# Verificación Formal y Refinamientos en $P/PML$

Javier R. Diaz

**Director:** Gabriel A. Baum

*A mis padres, Mariana, Seba y amigos.*

# Agradecimientos

En primer lugar, agradezco a mis padres Graciela y Jorge su apoyo incondicional (¡y paciencia!) durante todos mis años de estudio, esto es, ha sido y será muy importante para mí, por eso este trabajo ha sido dedicado a ellos.

Quiero agradecer especialmente al Prof. Gabriel A. Baum (el director de esta tesis) y al Dr. Marcelo F. Frias por estar siempre dispuestos a ofrecerme guía durante todo el desarrollo de este trabajo.

Finalmente, estoy muy agradecido con la familia Prado León por su cálida amistad, realmente me sentí en casa durante mi estancia en la ciudad de México, donde la mayor parte de este trabajo fue realizada.

Javier R. Díaz
La Plata, 2001

# Prefacio

Los métodos formales permiten al ingeniero de software especificar, desarrollar y verificar un sistema basado en computadora mediante la aplicación de una notación matemática rigurosa. Estos métodos proporcionan un mecanismo para detectar y corregir más fácilmente los problemas de ambigüedad, incompletitud e inconsistencia asociados a los métodos tradicionales de especificación. Además, sirven como base para la verificación de programas y la derivación de programas.

En el contexto de las aplicaciones industriales, existen distintos métodos formales propuestos que permiten la modelización de los elementos de este tipo de sistemas. La lógica $P/PML$ (*Product/Process Modelling Logic*)[4] es un método formal desarrollado para la especificación y construcción de sistemas industriales de tiempo real. Esta lógica es una extensión de la lógica dinámica de primer orden [11] agregando (a) acciones atómicas arbitrarias en lugar de sólo asignación, (b) variables sobre procesos que permiten especificar sistemas parcialmente, (c) un combinador de paralelismo y (d) restricciones de tiempo sobre los procesos.

En este trabajo se estudiarán los aspectos de *verificación* y *derivación* formal de procesos en la lógica $P/PML$. En la primer parte se definirá el formalismo $P/PML$, su sintaxis y semántica, y se darán algunos ejemplos de procesos en esta lógica. En la segunda parte de este trabajo se explorará el concepto de verificación formal de procesos en $P/PML$, tratándose el aspecto de corrección parcial. Como resultado, se desarrollará un sistemas formal de prueba que permitirán verificar la corrección parcial de procesos con respecto a especificaciones lógicas. En la tercer parte de este trabajo se explorará el segundo concepto mencionado antes, el de derivación formal de procesos en la lógica $P/PML$, desarrollándose como resultado un cálculo de refinamientos que permitirá derivar procesos a partir de especificaciones lógicas. Por último, se presentarán las conclusiones acerca de este trabajo y se citarán algunas posibles extensiones a desarrollar en el futuro.

# Contenido

# Parte I

# La Lógica $P/PML$

# Capítulo 1

# La Lógica $P/PML$

## 1.1 Introducción

La lógica $P/PML$ (*Product/Process Modelling Logic*) [4] es un formalismo orientado a la especificación de procesos industriales con un componente de tiempo real. Este formalismo ve al mundo como un modelo en términos de dos (y sólo dos) tipos de entidades: productos y procesos. Un *producto* es una descripción de una entidad del mundo real en términos de atributos medibles. Un *proceso* es una descripción de una entidad del mundo real en términos de cómo transforma su producto de entrada en el producto de salida y de sus restricciones de tiempo. Los procesos se construyen a partir de los métodos (procesos atómicos) de una máquina abstracta que modela las capacidades básicas de la organización cuyos procesos industriales se están modelizando. Estas capacidades básicas pueden ser de máquinas (computadoras, prensas, cintas transportadoras), o de personas (programadores, ingenieros, vendedores), o incluso (sub)organizaciones. La lógica $P/PML$ es una extensión de la lógica dinámica de primer orden [11] agregando (a) acciones atómicas arbitrarias (que representan los métodos de la máquina abstracta) en lugar de sólo asignación, (b) variables sobre procesos para poder especificar abstractamente los procesos que estamos interesados en construir, (c) un combinador que nos permite expresar paralelismo de procesos, y (d) restricciones de tiempo asociadas a los procesos que nos permita razonar acerca del tiempo (tiempo de ejecución de procesos, caminos críticos, etc.). La semántica de $P/PML$ se basa en la semántica algebraica de la lógica dinámica de primer orden, adaptándola para incluir los aspectos mencionados antes. Con respecto al tiempo dentro del formalismo, cada acción básica es suplementada con una especificación de cotas de tiempo superior e inferior. Estas cotas tienen la siguiente interpretación: La cota inferior se interpreta como el mínimo tiempo que debe pasar antes de que sucedan los efectos de la acción, y la cota superior da un tiempo máximo para que los efectos de la acción se establezcan. Las especificaciones de los procesos también tendrán asociadas cotas superiores e inferiores, y se espera que las implementaciones para ellos satisfagan estas restricciones de tiempo.

La algebraización de la lógica $P/PML$ se obtiene usando "*omega-closure fork-algebras*" [3, 4]. Con ello es posible razonar acerca de $P/PML$ en un marco ecuacional. El razonamiento ecuacional basado en sustituciones de iguales por iguales es el tipo de manipulación que se realiza en muchos sistemas de procesamiento de información.

## 1.2 Sintaxis de $P/PML$

DEFINICION 1.2.1 Una *signatura de objeto* es un par $\langle A, \Sigma \rangle$ tal que

1. $\Sigma = \langle S, F, P \rangle$ es una signatura de primer orden multisort con conjunto de sorts $S$, conjunto de símbolos de función $F$ y conjunto de símbolos de predicado $P$. Entre los sorts, se distinguirá un sort llamado *sort de tiempo*, denotado por $T$.
2. $A$ es un conjunto de *símbolos de acción*. A cada $a \in A$ se asocia un par $\langle s_1, s_2 \rangle \in (S^*)^2$ llamado su *aridad*. Se denotará la aridad de entrada de $a$ por $ia(a)$ y la aridad de salida de $a$ por $oa(a)$.

■

Se denotará por $IndVar$ al conjunto de las variables individuales y por $RelVar$ al conjunto de variables relacionales. A cada $X \in RelVar$ se asocia una aridad $\langle s_1, s_2 \rangle \in (S^*)^2$. Se define $ia(X) = s_1$ y $oa(X) = s_2$. Con respecto al sort de tiempo $T$, se asumirá que se disponen de algunas constantes distinguidas tales como $\epsilon$, $\infty$, etc., como así también de algunos símbolos de función y de predicado usuales, tales como $\leq$, $+$, etc.

DEFINICION 1.2.2 Dada una signatura de objeto $\mathcal{S} = \langle A, \langle S, F, P \rangle \rangle$, los conjuntos de *términos relacionales* y *fórmulas* en $\mathcal{S}$ son los conjuntos más pequeños $RT(\mathcal{S})$ y $For(\mathcal{S})$ tales que

1. $A \cup RelVar \subseteq RT(\mathcal{S})$.
2. Si $t \in S^*$, entonces $1'_t \in RT(\mathcal{S})$. Se define $ia(1'_t) = oa(1'_t) = t$.
3. Si $r \in RT(\mathcal{S})$ y $ia(r) = oa(r)$, entonces $r^* \in RT(\mathcal{S})$. Se define $ia(r^*) = oa(r^*) = ia(r)$.
4. Si $r, s \in RT(\mathcal{S})$, $ia(r) = ia(s)$ y $oa(r) = oa(s)$, entonces $r+s \in RT(\mathcal{S})$ y $r \cdot s \in RT(\mathcal{S})$. Se define $ia(r+s) = ia(r \cdot s) = ia(r)$ y $oa(r+s) = oa(r \cdot s) = oa(r)$.
5. Si $r, s \in RT(\mathcal{S})$ y $oa(r) = ia(s)$, entonces $r;s \in RT(\mathcal{S})$. Se define $ia(r;s) = ia(r)$ y $oa(r;s) = oa(s)$.
6. Si $\alpha \in For(\mathcal{S})$ es una fórmula de primer orden sin cuantificadores y con variables libres [1] $x_1, \ldots, x_n$ con $x_i$ de sort $s_i$, entonces $\alpha? \in RT(\mathcal{S})$ y $ia(\alpha?) = oa(\alpha?) = s_1 \ldots s_n$.
7. El conjunto de fórmulas atómicas de primer orden en la signatura $\Sigma$ está contenido en $For(\mathcal{S})$.
8. Si $\alpha \in For(\mathcal{S})$, entonces $\neg\alpha \in For(\mathcal{S})$.
9. Si $\alpha, \beta \in For(\mathcal{S})$, entonces $\alpha \vee \beta \in For(\mathcal{S})$.
10. Si $\alpha \in For(\mathcal{S})$ y $x$ es una variable individual de sort $s$, entonces $(\exists x : s)\, \alpha \in For(\mathcal{S})$.
11. Si $\alpha \in For(\mathcal{S})$, $t \in RT(\mathcal{S})$ con $ia(t) = s_1 \ldots s_m$ y $oa(t) = {s'}_1 \ldots {s'}_n$, $\vec{x} = x_1, \ldots, x_m$ con $x_i$ de sort $s_i$, $\vec{y} = y_1, \ldots, y_n$ distintas con $y_i$ de sort ${s'}_i$ y $l$, $u$ son expresiones de sort $T$, entonces $\left[\vec{x}\ {}_l t^u\ \vec{y}\right] \alpha \in For(\mathcal{S})$ y $\left\langle \vec{x}\ {}_l t^u\ \vec{y} \right\rangle \alpha \in For(\mathcal{S})$.

[1] En una acción de la forma $\alpha?$, las variables libres de $\alpha$ deben entenderse como 'parámetros formales' de la acción.

■

Se denotará por $GRT(\mathcal{S})$ al conjunto de todos los términos relacionales *base*, es decir, los términos en $RT(\mathcal{S})$ donde no ocurren variables relacionales.

DEFINICION 1.2.3 Dados $R \in RT(\mathcal{S})$ con $ia(R) = s_1 \dots s_m$ y $oa(R) = s'_1 \dots s'_n$, $\vec{x} = x_1, \dots, x_m$ con $x_i$ de sort $s_i$, $\vec{y} = y_1, \dots, y_n$ distintas con $y_i$ de sort $s'_i$, y $l$, $u$ expresiones de sort $T$, una expresión de la forma $\vec{x}\ R\ \vec{y}$ se denomina *término de acción* y una expresión de la forma $\vec{x}\ {}_l R^u\ \vec{y}$ se denomina *término de acción temporal*. En el caso de que $R \in GRT(\mathcal{S})$, se los llama *término de acción base* y *término de acción temporal base*, respectivamente.

■

## 1.3 Semántica de $P/PML$

DEFINICION 1.3.1 Dada una signatura de objeto $\mathcal{S} = \langle A, \langle S, F, P \rangle \rangle$, una *estructura de objeto para* $\mathcal{S}$ es una estructura $\mathcal{A} = \langle \mathbf{S}, \mathbf{A}, \mathbf{F}, \mathbf{P} \rangle$ que satisface

1. $\mathbf{S}$ es una familia $S$-indizada de conjuntos no vacíos, donde el conjunto $\mathsf{T}$ es el $T$-ésimo elemento de $\mathbf{S}$. En general, el conjunto correspondiente al sort $s$ se denotará por $\mathsf{s}$.
2. $\mathbf{A}$ es una familia $A$-indizada de relaciones binarias que satisface las restricciones de tipo de los símbolos de $A$, es decir, si $ia(a) = s_1 \dots s_m \in S^*$ y $oa(a) = s'_1 \dots s'_n \in S^*$, entonces $a^{\mathcal{A}}$ (como se denotará al $a$-ésimo elemento de $\mathbf{A}$) está contenido en $(\mathsf{s}_1 \times \cdots \times \mathsf{s}_m) \times (\mathsf{s'}_1 \times \cdots \times \mathsf{s'}_n)$.
3. A cada $f : s_1 \dots s_k \to s$ en $F$ se le asocia una función $f^{\mathcal{A}} : \mathsf{s}_1 \times \cdots \times \mathsf{s}_k \to \mathsf{s} \in \mathbf{F}$.
4. A cada $p$ de aridad $s_1 \dots s_k$ en $P$ se le asocia una relación $p^{\mathcal{A}} \subseteq \mathsf{s}_1 \times \cdots \times \mathsf{s}_k \in \mathbf{P}$.

■

Con respecto al dominio $\mathsf{T}$ asociado al sort de tiempo $T$, no se profundizará en las diferentes posibilidades para modelar el tiempo, sino que se elegirá más bien alguna representación adecuada (con respecto a la aplicación que se tenga en mente), como por ejemplo el campo de los números racionales o reales, extendido con un elemento máximo $\infty$.

DEFINICION 1.3.2 Sea $\mathcal{S}$ una signatura de objeto y $\mathcal{A}$ una estructura de objeto para $\mathcal{S}$. Se define una *valuación de las variables individuales* como una función $\nu : IndVar \to \bigcup_i \mathsf{s}_i$ que satisface las restricciones de tipo de las variables en $IndVar$, es decir, si $x$ es una variable individual de sort $s$, entonces $\nu(x) \in \mathsf{s}$.

■

NOTACION 1.3.3 Dada una valuación de las variables individuales $\nu$ y un arreglo de variables $\vec{x} = x_1, \dots, x_n$, por $\nu(\vec{x})$ se denotará la tupla $\langle \nu(x_1), \dots, \nu(x_n) \rangle$.

DEFINICION 1.3.4 Sea $\mathcal{S}$ una signatura de objeto y $\mathcal{A}$ una estructura de objeto para $\mathcal{S}$. Se define una *valuación de las variables relacionales* como una función $\mu : RelVar \to GRT$ que satisface las restricciones de tipo de las variables en $RelVar$, es decir, si $X$ es una variable relacional entonces $X$ y $\mu(X)$ tienen la misma aridad.

■

Se asumirá que las acciones atómicas tienen asignada una cota inferior y superior de tiempo, a saber $l_a \in \mathsf{T}$ y $u_a \in \mathsf{T}$ con $l_a \leq u_a$ para cada acción $a \in A$. A partir de las cotas de las acciones atómicas es posible definir cotas para acciones complejas de una forma bastante natural.

DEFINICION 1.3.5 Sea $\mathcal{S}$ una signatura de objeto, $\mathcal{A}$ una estructura de objeto y $\mu$ una valuación relacional. Las funciones

$$\mathsf{l}_\mu : RT(\mathcal{S}) \cup For(\mathcal{S}) \to \mathsf{T}$$

y

$$\mathsf{u}_\mu : RT(\mathcal{S}) \cup For(\mathcal{S}) \to \mathsf{T}$$

se definen como sigue[2]:

1. Si $a \in A$, entonces $\mathsf{l}(a) = l_a$ y $\mathsf{u}(a) = u_a$.
2. Si $R = X \in RelVar$, entonces $\mathsf{l}(R) = \mathsf{l}(\mu(X))$ y $\mathsf{u}(R) = \mathsf{u}(\mu(X))$.
3. Si $R = 1'_t$, con $t \in S^*$, entonces $\mathsf{l}(R) = \epsilon$ y $\mathsf{u}(R) = \epsilon$ ($\epsilon$ es una constante de sort $\mathsf{T}$ que representa una pequeña cantidad de tiempo).
4. Si $R = S^*$, entonces $\mathsf{l}(R) = 0$ y $\mathsf{u}(R) = \infty$.
5. Si $R = S + T$, entonces $\mathsf{l}(R) = \min\{\mathsf{l}(S), \mathsf{l}(T)\}$ y $\mathsf{u}(R) = \max\{\mathsf{u}(S), \mathsf{u}(T)\}$
6. Si $R = S \cdot T$, entonces $\mathsf{l}(R) = \max\{\mathsf{l}(S), \mathsf{l}(T)\}$ y $\mathsf{u}(R) = \max\{\mathsf{u}(S), \mathsf{u}(T)\}$.
7. Si $R = S;T$, entonces $\mathsf{l}(R) = \mathsf{l}(S)$ y $\mathsf{u}(R) = \mathsf{u}(S) + \mathsf{u}(T)$.
8. Si $R = \alpha?$ con $\alpha \in For(\mathcal{S})$ de primer orden sin cuantificadores, entonces $\mathsf{l}(R) = \mathsf{l}(\alpha)$ y $\mathsf{u}(R) = \mathsf{u}(\alpha) + \epsilon$ [3].
9. Si $\alpha = p(t_1, \ldots, t_n)$, entonces $\mathsf{l}(\alpha) = l_p \in \mathsf{T}$ y $\mathsf{u}(\alpha) = u_p \in \mathsf{T}$ con $l_p \leq u_p$.
10. Si $\alpha = \neg\beta$, entonces $\mathsf{l}(\alpha) = \mathsf{l}(\beta)$ y $\mathsf{u}(\alpha) = \mathsf{u}(\beta)$.
11. Si $\alpha = \beta \vee \gamma$, entonces $\mathsf{l}(\alpha) = \min\{\mathsf{l}(\beta), \mathsf{l}(\gamma)\}$ y $\mathsf{u}(\alpha) = \max\{\mathsf{u}(\beta), \mathsf{u}(\gamma)\}$.

■

DEFINICION 1.3.6 Sea $\mathcal{S}$ una signatura de objeto, $\mathcal{A}$ una estructura de objeto para $\mathcal{S}$ y $\mu$ una valuación relacional. Dadas dos valuaciones de las variables individuales $\nu$ y $\nu'$ y un término de acción $\vec{x}\ R\ \vec{y}$, por $\nu\left(\vec{x}\ R\ \vec{y}\right)\nu'$ se denotará el hecho que

1. $\left\langle \nu(\vec{x}), \nu'(\vec{y}) \right\rangle \in R^{\mathcal{A}}_{\mu}$ (la denotación del término relacional $R$, formalmente definida en Def. 1.3.7),
2. para cada variable $z$ que no ocurre en $\vec{y}$, $\nu'(z) = \nu(z)$ .

[2] Para reducir notación se denotará a $\mathsf{l}_\mu$ y $\mathsf{u}_\mu$ por $\mathsf{l}$ y $\mathsf{u}$ respectivamente. Sólo se considerarán fórmulas de primer orden sin cuantificadores, ya que son las únicas usadas para construir acciones de la forma $\alpha?$

[3] Por simplicidad, en la práctica se asumirá que $\mathsf{l}(\alpha?) = \mathsf{u}(\alpha?) = \epsilon$

■

Nótese que en el item 2 de Def. 1.3.6 se está adoptando una posición de *mínimo cambio*, en el sentido de que los valores de las variables no mencionadas explícitamente en el término se mantienen intactos.

La semántica de las fórmulas se define relativa a valuaciones de las variables individuales y de las variables relacionales. En la siguiente definición, la notación $\mathcal{A} \models_{P/PML} \alpha[\nu][\mu]$ ha de leerse *"La fórmula $\alpha$ se satisface en la estructura de objeto $\mathcal{A}$ con las valuaciones $\nu$ y $\mu$".*

DEFINICION 1.3.7 Sea $\mathcal{S} = \langle A, \langle S, F, P \rangle \rangle$ una signatura de objeto y $\mathcal{A} = \langle \mathbf{S}, \mathbf{A}, \mathbf{F}, \mathbf{P} \rangle$ una estructura de objeto para $\mathcal{S}$. Sea $\nu$ una valuación de las variables individuales y $\mu$ una valuación de las variables relacionales. Entonces:

1. Si $a \in A$, entonces $a_\mu^{\mathcal{A}}$ es el elemento con índice $a$ en $\mathbf{A}$.
2. Si $R \in RelVar$, entonces $R_\mu^{\mathcal{A}} = (\mu(R))_\mu^{\mathcal{A}}$.
3. Si $R = 1'_t$, con $t = s_1 \ldots s_k \in S^*$, entonces $R_\mu^{\mathcal{A}} = \{ \langle \langle a_1, \ldots, a_k \rangle, \langle a_1, \ldots, a_k \rangle \rangle : a_i \in \mathsf{s}_i \}$.
4. Si $R = S^*$, con $S \in RT(\mathcal{S})$, entonces $R_\mu^{\mathcal{A}}$ es la clausura reflexiva-transitiva de la relación binaria $S_\mu^{\mathcal{A}}$.
5. Si $R = S + T$, con $S, T \in RT(\mathcal{S})$, entonces $R_\mu^{\mathcal{A}} = S_\mu^{\mathcal{A}} \cup T_\mu^{\mathcal{A}}$.
6. Si $R = S \cdot T$, con $S, T \in RT(\mathcal{S})$, entonces $R_\mu^{\mathcal{A}} = S_\mu^{\mathcal{A}} \cap T_\mu^{\mathcal{A}}$.
7. Si $R = S;T$, con $S, T \in RT(\mathcal{S})$, entonces $R_\mu^{\mathcal{A}}$ es la composición de las relaciones binarias $S_\mu^{\mathcal{A}}$ y $T_\mu^{\mathcal{A}}$.
8. Si $R = \alpha?$ con $\alpha \in For(\mathcal{S})$ sin cuantificadores y con variables libres $\vec{x} = x_1, \ldots, x_n$ con $x_i$ de sort $s_i$, entonces $R_\mu^{\mathcal{A}} = \left\{ \left\langle \nu'(\vec{x}), \nu'(\vec{x}) \right\rangle : \nu' \text{ es una valuación y } \mathcal{A} \models_{P/PML} \alpha[\nu'][\mu] \right\}$
9. Si $\varphi = p(t_1, \ldots, t_n)$ con $p \in P$, entonces $\mathcal{A} \models_{P/PML} \varphi[\nu][\mu]$ si $\langle {t_1}_\nu^{\mathcal{A}}, \ldots, {t_n}_\nu^{\mathcal{A}} \rangle \in p^{\mathcal{A}}$.
10. Si $\varphi = \neg\alpha$, entonces $\mathcal{A} \models_{P/PML} \varphi[\nu][\mu]$ si $\mathcal{A} \not\models_{P/PML} \alpha[\nu][\mu]$.
11. Si $\varphi = \alpha \vee \beta$, entonces $\mathcal{A} \models_{P/PML} \varphi[\nu][\mu]$ si $\mathcal{A} \models_{P/PML} \alpha[\nu][\mu]$ ó $\mathcal{A} \models_{P/PML} \beta[\nu][\mu]$.
12. Si $\varphi = (\exists x : s)\alpha$, entonces $\mathcal{A} \models_{P/PML} \varphi[\nu][\mu]$ si existe $a \in \mathsf{s}$ tal que $\mathcal{A} \models_{P/PML} \alpha[\nu_x^a][\mu]$ ($\nu_x^a$, como es usual, denota la valuación que concuerda con $\nu$ en todas las variables distintas a $x$, y satisface $\nu_x^a(x) = a$).
13. Si $\varphi = \left[\vec{x}\ {}_l R^u\ \vec{y}\right] \alpha$, entonces $\mathcal{A} \models_{P/PML} \varphi[\nu][\mu]$ si
    (a) $l_\nu^{\mathcal{A}} \leq \mathsf{l}(R)$, $u_\nu^{\mathcal{A}} \geq \mathsf{u}(R)$, y
    (b) para toda valuación $\nu'$ tal que $\nu \left(\vec{x}\ R\ \vec{y}\right) \nu'$ entonces $\mathcal{A} \models_{P/PML} \varphi[\nu'][\mu]$.
14. Si $\varphi = \left\langle \vec{x}\ {}_l R^u\ \vec{y} \right\rangle \alpha$, entonces $\mathcal{A} \models_{P/PML} \varphi[\nu][\mu]$ si

(a) $l_\nu^{\mathcal{A}} \leq \mathsf{l}(R)$, $u_\nu^{\mathcal{A}} \geq \mathsf{u}(R)$, y

(b) existe una valuación $\nu'$ tal que $\nu \left( \vec{x} \; R \; \vec{y} \right) \nu'$ y $\mathcal{A} \models_{P/PML} \varphi[\nu'][\mu]$.

■

Nótese que a diferencia de la lógica dinámica, en $P/PML$ deben incluirse ambos operadores modales como primitivos, ya que por su definición no existe dualidad entre ellos. Intuitivamente, una fórmula $\left[ \vec{x} \; {}_l R^u \; \vec{y} \right] \alpha$ especifica que el proceso $R$ satisface las restricciones de tiempo $l$,$u$ y que toda ejecución terminante de $R$ con entradas $\vec{x}$ y salidas $\vec{y}$ establece la poscondición $\alpha$ al terminar. Una fórmula $\left\langle \vec{x} \; {}_l R^u \; \vec{y} \right\rangle \alpha$ especifica que el proceso $R$ satisface las restricciones de tiempo $l$,$u$ y que es posible ejecutar la acción $R$ con entradas $\vec{x}$ y salidas $\vec{y}$ estableciendo la poscondición $\alpha$ al terminar. Con respecto a la acción de testeo, y con el objetivo de simplificar, se asumirá que el orden de las variables libres en una acción de este tipo es el orden de ocurrencia de dichas variables en la fórmula, leída de izquierda a derecha. Así, por ejemplo, para la acción de testeo $R = (x > 0 \wedge b = \mathsf{t} \vee z = 1)?$ se tendrá que $ia(R) = oa(R) = Nat \; Bool \; Nat$ y

$$R_\mu^{\mathcal{A}} = \{ \langle \langle n, b, m \rangle, \langle n, b, m \rangle \rangle : n, m \in \mathsf{Nat}, \; b \in \mathsf{Bool}, \; n > 0, \; b = \mathsf{t} \text{ ó } m = 1 \}.$$

## 1.4 Un ejemplo: *La máquina vendedora*

En esta sección se presentará un ejemplo que servirá para ilustrar el tipo de problemas que pueden especificarse utilizando la lógica $P/PML$ y cómo las características de tiempo real de esta lógica juegan un rol decisivo en la elección de implementaciones de procesos. Supóngase que un fabricante de máquinas vendedoras de caramelos quiere fabricar máquinas con las siguientes características: Si la máquina tiene caramelos, entonces, luego de que el dinero ha sido depositado, se entrega el caramelo. Si la máquina está vacía, entonces, en caso de que la máquina pueda ser reabastecida a tiempo, debería reabastecerse. Caso contrario, el dinero debería ser devuelto al cliente. Además, la transacción debe completarse en a lo sumo 3 minutos (pues el fabricante cree que un consumidor puede esperar dicho tiempo sin perder la paciencia). Se modelizará el estado interno de la máquina utilizando las variables $\#\$$, $\#P$, $\$r$ y $Pr$ que representan la cantidad de dinero en la máquina, la cantidad de caramelos que quedan en la máquina, si el dinero fue devuelto al cliente, y si el caramelo fue en efecto dado al cliente, respectivamente. Así, es posible especificar el comportamiento de la máquina mediante la siguiente fórmula $P/PML$

$$pre \Rightarrow \left[ \langle \#\$, \#P, \$r, Pr \rangle \; {}_0 VM^{3m} \; \langle \#\$, \#P, \$r, Pr \rangle \right] post$$

donde $pre$ es

$$\#\$ = x_0 \wedge \#P = P_0 \wedge \$r = \mathsf{f} \wedge Pr = \mathsf{f},$$

$post$ es[4]

$$P_0 = 0 \Rightarrow \begin{pmatrix} \#\$ = x_0 + 1 \wedge \#P = MP - 1 \wedge \$r = \mathsf{f} \wedge Pr = \mathsf{t} \\ \vee \\ \#\$ = x_0 \wedge \#P = 0 \wedge \$r = \mathsf{t} \wedge Pr = \mathsf{f} \end{pmatrix}$$
$$P_0 > 0 \Rightarrow \#\$ = x_0 + 1 \wedge \#P = P_0 - 1 \wedge \$r = \mathsf{f} \wedge Pr = \mathsf{t}$$

[4] $MP$ es una constante que representa la máxima cantidad de caramelos que la máquina puede almacenar.

y $VM$ es una variable relacional que representa el proceso que implementará el comportamiento de la máquina. Supóngase que, como restricción, este proceso debe construirse usando algunas de las siguientes acciones atómicas:

- *Accept*\$ (que acepta el dinero introducido en la máquina. Su cota inferior de tiempo es 0 y la cota superior de tiempo es 3 segundos.)
- *Return*\$ (que devuelve el dinero al cliente, siempre que la máquina tenga dinero. Su cota inferior de tiempo es 0 y la cota superior de tiempo es 4 segundos).
- *GiveProduct* (que entrega el caramelo al cliente, siempre que la máquina tenga caramelos. Su cota inferior de tiempo es 0 y la cota superior de tiempo es 10 segundos).
- *AskForReplenish* (que reabastece totalmente la máquina. Su cota inferior de tiempo es 0 y la cota superior de tiempo se discutirá a continuación).

Si la máquina ha de colocarse en el lobby de un hotel, parece plausible que en cuanto la máquina se vacíe, un empleado la reabastecerá (resultando un proceso que es más conveniente para el fabricante), y, por lo tanto, una cota superior de tiempo para la acción de reabastecimiento podría ser 2 minutos. Por lo tanto, el siguiente proceso muestra una implementación factible [5]:

$$(\#P > 0?; Accept\$; GiveProduct) + (\#P = 0?; Accept\$; AskForReplenish; GiveProduct)$$

Si la máquina ha de colocarse en una estación de subterráneo, entonces puede esperarse que la máquina no sea reabastecida más de una vez al día. Entonces, la cota superior de tiempo para la acción de reabastecimiento podría ser 24 horas. En este caso, el proceso descrito anteriormente no satisface la especificación, pero el siguiente sí:

$$(\#P > 0?; Accept\$; GiveProduct) + (\#P = 0?; Accept\$; Return\$)$$

[5] En rigor, la acción de testeo $\#P > 0?$ ocurrente en las implementaciones es una abreviatura de la acción $(\#\$ = \#\$ \wedge \#P > 0 \wedge \$r = \$r \wedge Pr = Pr)?$ y análogamente para la acción $\#P = 0?$.

# Parte II

# Verificación Formal en $P/PML$

# Capítulo 2

# Corrección Parcial en $P/PML$

## 2.1 Especificaciones y corrección en $P/PML$

La verificación de programas es una técnica que permite probar formalmente (de forma similar a una prueba tradicional de un teorema matemático) la correctitud de un programa. Las pruebas de corrección de programas son en general bastante tediosas pero, a diferencia de los métodos que utilizan casos de prueba, demuestran la ausencia de errores. Esto es particularmente importante para algunas aplicaciones donde la presencia de errores de programa puede tener consecuencias de alto impacto, tales como sistemas de monitoreo de pacientes, controladores de reactores nucleares, etc. Dadas las características del formalismo $P/PML$, resulta importante desarrollar un marco riguroso en el cual sea posible el estudio del aspecto de verificación formal de procesos en $P/PML$. Como primer paso al discutir sobre la corrección de procesos en $P/PML$ con respecto a especificaciones, es necesario definir en forma intuitiva el significado de 'especificación' y 'corrección'. En general, se entiende por especificación a una descripción del comportamiento deseado de un programa. Formalmente, se suele representar a una especificación como un par de predicados de la lógica de primer orden, llamados 'precondición' y 'poscondición', que caracterizan los conjuntos de estados antes y después de la ejecución del programa respectivamente. En general, una especificación se suele denotar

$$[\alpha, \beta]$$

donde $\alpha$ y $\beta$ son fórmulas de la lógica de primer orden (precondición y poscondición respectivamente). Otras veces (por ejemplo [14]) se incluye además una lista de las variables (llamada *frame*) cuyos valores está permitido cambiar. En este caso, se suele denotar

$$w : [\alpha, \beta]$$

donde $w$ es una lista de variables. En cualquier caso, aunque esta noción de estados antes y después de la ejecución de un proceso existe en $P/PML$, se tendrá un concepto de 'especificación' diferente. Durante su ejecución, un proceso toma los productos que contienen las variables de entrada, realiza alguna clase de transformación con los mismos y finalmente deposita los productos resultantes en las variables de salida. Por lo tanto, se deberán considerar las variables de entrada y de salida como parte de la especificación de un proceso. Por otro lado, una especificación en $P/PML$ debería incluir

además cotas de tiempo para la ejecución del proceso. Así, una especificación en $P/PML$ tendrá la forma

$$\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l}$$

donde $\alpha$ y $\beta$ son fórmulas de la lógica de primer orden (la precondición y poscondición, respectivamente), $\vec{x}, \vec{y}$ son las variables de entrada y salida (respectivamente), y $l, u$ son las cotas inferior y superior de tiempo (respectivamente). Intuitivamente, se desea interpretar la corrección parcial en $P/PML$ de la siguiente manera: Un proceso es correcto parcialmente con respecto a una especificación si toda ejecución terminante del proceso con variables de entrada y salida especificadas y que comienza en un estado que satisface la precondición termina en un estado que satisface la poscondición, cumpliendo las restricciones de tiempo. Formalmente, dados un proceso $R$ y una especificación $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l}$, se denota el hecho de que $R$ es parcialmente correcto con respecto a $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l}$ de la siguiente forma

$$\{\alpha\}\ \vec{x}\ {}_{l}R^{u}\ \vec{y}\ \{\beta\}$$

Así, por ejemplo, la fórmula $\{x = 0\}\,\langle\, x\,\rangle_{0}\, Inc; Dup^{2}\,\langle\, y, z\,\rangle\,\{y = z = 1\}$ establece que el proceso $Inc; Dup$ es parcialmente correcto con respecto a la especificación $\langle\, x\,\rangle, \langle\, y, z\,\rangle : [x = 0,\ y = z = 1]\ {}^{2}_{0}$.

## 2.2 La lógica de Hoare

Para razonar formalmente sobre la corrección parcial de procesos en $P/PML$, se presentará una lógica de Hoare y un cálculo para esta lógica, basados en los que se presentan en [12]. La definición de esta lógica de Hoare se construye sobre la lógica multisort de primer orden.

DEFINICION 2.2.1 (Sintaxis de la lógica de Hoare) Sea $\mathcal{S}$ una signatura de objeto. Una *fórmula de Hoare* sobre $\mathcal{S}$ es una expresión de la forma

$$\{\alpha\}\ \vec{x}\ {}_{l}R^{u}\ \vec{y}\ \{\beta\}$$

donde $\alpha, \beta \in For(\mathcal{S})$ son fórmulas de primer orden con $Var(\beta) \subseteq \vec{y}$, y $\vec{x}\ {}_{l}R^{u}\ \vec{y}$ es un término de acción temporal base.

■

El conjunto de todas las fórmulas de Hoare sobre $\mathcal{S}$ se denotará por $HFor(\mathcal{S})$. Nótese que en la definición anterior, las variables libres que ocurren en la fórmula $\beta$ deben aparecer en $\vec{y}$. La motivación de esta restricción deriva de un problema de composicionalidad que se explicará más adelante, pero debe aclararse que esta restricción no implica una disminución importante en la expresividad de la lógica, puesto que el uso de constantes lógicas en las fórmulas está permitido. Así, por ejemplo, la expresión

$$\{true\}\,\langle\, x\,\rangle_{0}\, Inc^{1}\,\langle\, y\,\rangle\,\{y = x + 1\}$$

no es una fórmula de Hoare, y debería reescribirse utilizando una constante lógica como sigue

$$\{x = X\}\,\langle\, x\,\rangle_{0}\, Inc^{1}\,\langle\, y\,\rangle\,\{y = X + 1\}.$$

La única disminución de expresividad consiste en que resulta imposible realizar aserciones sobre la propiedad de mínimo cambio en la ejecución de procesos. Por ejemplo, la expresión

$$\{y = 0\}\,\langle\, x\,\rangle_{0}\, Inc^{1}\,\langle\, x\,\rangle\,\{y = 0\}$$

no es una fórmula de Hoare. En consecuencia, la propiedad de mínimo cambio deberá asumirse en esta lógica de Hoare.

Los únicos objetos sintácticos en la lógica de Hoare serán las fórmulas de Hoare, por lo tanto la semántica de esta lógica sólo requiere describir el significado de las fórmulas de Hoare

DEFINICION 2.2.2 (Semántica de la lógica de Hoare) Sean $\mathcal{S}$ una signatura de objeto y $\mathcal{A}$ una estructura de objeto para $\mathcal{S}$. Dados una valuación $\nu$ de las variables individuales y $\{\alpha\}\ \vec{x}\ {}_l R^u\ \vec{y}\ \{\beta\} \in HFor(\mathcal{S})$ se dice que la fórmula de Hoare $\{\alpha\}\ \vec{x}\ {}_l R^u\ \vec{y}\ \{\beta\}$ se *satisface* en la estructura de objeto $\mathcal{A}$ por la valuación $\nu$, denotado por

$$\models_{\mathcal{A}} \{\alpha\}\ \vec{x}\ {}_l R^u\ \vec{y}\ \{\beta\}[\nu],$$

siempre que $\mathcal{A} \models_{P/PML} \alpha \Rightarrow \left[\vec{x}\ {}_l R^u\ \vec{y}\right] \beta[\nu][id]$[1].

■

Una fórmula de Hoare $\{\alpha\}\ \vec{x}\ {}_l R^u\ \vec{y}\ \{\beta\}$ se dice que es *válida* en una estructura de objeto $\mathcal{A}$, denotado por

$$\models_{\mathcal{A}} \{\alpha\}\ \vec{x}\ {}_l R^u\ \vec{y}\ \{\beta\},$$

siempre que $\models_{\mathcal{A}} \{\alpha\}\ \vec{x}\ {}_l R^u\ \vec{y}\ \{\beta\}[\nu]$ para toda valuación $\nu$. Una fórmula de Hoare se dice que es *lógicamente válida*, denotado por

$$\models \{\alpha\}\ \vec{x}\ {}_l R^u\ \vec{y}\ \{\beta\},$$

siempre que $\models_{\mathcal{A}} \{\alpha\}\ \vec{x}\ {}_l R^u\ \vec{y}\ \{\beta\}$ para toda estructura de objeto $\mathcal{A}$. Una estructura de objeto $\mathcal{A}$ se dice que es un *modelo* de un conjunto $W \subseteq For(\mathcal{S}) \cup HFor(\mathcal{S})$ de fórmulas de primer orden y fórmulas Hoare, si $\models_{\mathcal{A}} w$ para toda $w \in W$. Una fórmula de Hoare se dice que es una *consecuencia lógica* de un conjunto $W$ de fórmulas de primer orden y fórmulas Hoare, denotado por

$$W \models \{\alpha\}\ \vec{x}\ {}_l R^u\ \vec{y}\ \{\beta\},$$

siempre que $\models_{\mathcal{A}} \{\alpha\}\ \vec{x}\ {}_l R^u\ \vec{y}\ \{\beta\}$ para todo modelo $\mathcal{A}$ de $W$. El conjunto de todas las consecuencias lógicas de $W$ se denota por $Cn(W)$. Un conjunto no vacío $T \subseteq HFor(\mathcal{S})$ se dice que es una *teoría* (sobre $\mathcal{S}$) cuando existe al menos un modelo para $T$ y además $Cn(T) \subseteq T$.

EJEMPLO 2.2.1 Sea $\mathcal{A}$ una estructura de objeto y $\nu$ una valuación tal que $\nu(x) = 1$. Entonces

$$\models_{\mathcal{A}} \{true\}\ \langle x \rangle\ {}_\epsilon (z = z)?^\epsilon\ \langle x \rangle\ \{x = 1\}[\nu]$$

ya que se cumple que $\mathcal{A} \models_{P/PML} true \Rightarrow [\langle x \rangle\ {}_\epsilon (z = z)?^\epsilon\ \langle x \rangle]\ (x = 1)[\nu]$.

■

EJEMPLO 2.2.2 Sea $\mathcal{A}$ una estructura de objeto donde $Inc^{\mathcal{A}} = \{\langle n, n+1 \rangle : n \in \mathsf{Nat}, n \geq 0\}$. Entonces

$$\models_{\mathcal{A}} \{x \leq 0\}\ \langle x \rangle\ {}_0 Inc^\infty\ \langle y \rangle\ \{y = 1\}$$

pues es cierto que $\models_{\mathcal{A}} \{x \leq 0\}\ \langle x \rangle\ {}_0 Inc^\infty\ \langle y \rangle\ \{y = 1\}[\nu]$ para toda valuación $\nu$.

[1] Puesto que $R \in GRT(\mathcal{S})$, de ahora en más escribiremos $\mathcal{A} \models_{P/PML} \varphi[\nu]$ en lugar de $\mathcal{A} \models_{P/PML} \varphi[\nu][id]$ y $R^{\mathcal{A}}$ en vez de $R^{\mathcal{A}}_{id}$.

■

EJEMPLO 2.2.3 Sea $\alpha \in For(\mathcal{S})$. Entonces

$$\models \{\alpha\} \langle x \rangle_0 1'_{Int}; 1'_{Int}{}^{3*\epsilon} \langle x \rangle \{\alpha\}$$

ya que se tiene $\models_{\mathcal{A}} \{\alpha\} \langle x \rangle_0 1'_{Int}; 1'_{Int}{}^{3*\epsilon} \langle x \rangle \{\alpha\}$ para toda estructura de objeto $\mathcal{A}$.

■

EJEMPLO 2.2.4 Sea $W$ el conjunto $\{X+1 > X, \{x = X\} \langle x \rangle_0 Inc^1 \langle y \rangle \{y = X+1\}\}$. Entonces se tiene que

$$W \models \{x = X\} \langle x \rangle_0 Inc^1 \langle y \rangle \{y > X\}$$

puesto que, siendo $\mathcal{A}$ un modelo de $W$, se cumple que $\models_{\mathcal{A}} \{x = X\} \langle x \rangle_0 Inc^1 \langle y \rangle \{y > X\}$.

■

## 2.3 El cálculo de Hoare

En esta sección se desarrollará un cálculo (infinitario) para la lógica de Hoare presentada en la sección anterior, denominado 'cálculo de Hoare'. El propósito de este cálculo es el de derivar las fórmulas de Hoare 'verdaderas'. Así, el cálculo de Hoare no dependerá de una estructura de objeto específica, sino que incluirá solamente los axiomas y reglas que son válidos en toda estructura de objeto. Por supuesto, en la práctica se está interesado en las fórmulas de Hoare válidas en alguna estructura de objeto $\mathcal{A}$ en particular. Este tema será tratado en la siguiente sección.

Formalmente, el cálculo de Hoare sobre una signatura de objeto $\mathcal{S} = \langle A, \langle S, F, P \rangle \rangle$ es un cálculo sobre $For(\mathcal{S}) \cup HFor(\mathcal{S})$ que consiste de los siguientes esquemas de axioma y reglas de deducción[2]:

(i) *Axioma ACT1*: Para todo $a \in A$

$$\boxed{\{true\} \vec{x}_0 a^\infty \vec{y} \{true\}}$$

(ii) *Axioma ACT2*: Para todo $a \in A$

$$\boxed{\{false\} \vec{x}_0 a^\infty \vec{y} \{false\}}$$

(iii) *Axioma SKIP*

$$\boxed{\{\alpha\} \vec{x}_\epsilon 1'_t{}^\epsilon \vec{x} \{\alpha\}}$$

(iv) *Axioma TEST*: Siendo $\vec{z}$ las variables libres de $\gamma$

$$\boxed{\{\gamma[\vec{x}/\vec{z}] \Rightarrow \alpha\} \vec{x}_\epsilon \gamma?^\epsilon \vec{x} \{\alpha\}}$$

[2]En adelante, se denotará por $\alpha[\vec{e}/\vec{x}]$ la sustitución simultánea de las ocurrencias libres de las variables $\vec{x}$ por las expresiones $\vec{e}$ en la fórmula $\alpha$.

(v) *Regla CONS*

$$\frac{\alpha \Rightarrow \gamma, \qquad \{\gamma\}\ \vec{x}\ {}_{l}R^{u}\ \vec{y}\ \{\delta\}, \qquad \delta \Rightarrow \beta}{\{\alpha\}\ \vec{x}\ {}_{l}R^{u}\ \vec{y}\ \{\beta\}}$$

(vi) *Regla VAR*

$$\frac{\{\alpha\}\ \vec{z}\ {}_{l}R^{u}\ \vec{w}\ \{\beta\}}{\{\alpha[\vec{x}/\vec{z}]\}\ \vec{x}\ {}_{l[\vec{x}/\vec{z}]}R^{u[\vec{x}/\vec{z}]}\ \vec{y}\ \{\beta[\vec{y}/\vec{w}]\}}$$

(vii) *Regla TIME*

$$\frac{\alpha \Rightarrow l \leq v, \qquad \{\alpha\}\ \vec{x}\ {}_{v}R^{w}\ \vec{y}\ \{\beta\}, \qquad \alpha \Rightarrow w \leq u}{\{\alpha\}\ \vec{x}\ {}_{l}R^{u}\ \vec{y}\ \{\beta\}}$$

(viii) *Regla SEC*: Si $Var(w) \cap \vec{z} = \emptyset$

$$\frac{\{\alpha\}\ \vec{x}\ {}_{l}S^{u}\ \vec{z}\ \{\gamma\}, \quad \{\gamma\}\ \vec{z}\ {}_{v}T^{w}\ \vec{y}\ \{\beta\}}{\{\alpha\}\ \vec{x}\ {}_{l}\ S;T\ {}^{u+w}\ \vec{y}\ \{\beta\}}$$

(ix) *Regla CHC*

$$\frac{\{\alpha\}\ \vec{x}\ {}_{l}S^{u}\ \vec{y}\ \{\beta\}, \qquad \{\alpha\}\ \vec{x}\ {}_{v}T^{w}\ \vec{y}\ \{\beta\}}{\{\alpha\}\ \vec{x}\ {}_{min\{l,v\}}S+T^{max\{u,w\}}\ \vec{y}\ \{\beta\}}$$

(x) *Regla PAR*

$$\frac{\{\alpha\}\ \vec{x}\ {}_{l}S^{u}\ \vec{y}\ \{\beta\}, \qquad \{\alpha\}\ \vec{x}\ {}_{v}T^{w}\ \vec{y}\ \{\gamma\}}{\{\alpha\}\ \vec{x}\ {}_{max\{l,v\}}S\cdot T^{max\{u,w\}}\ \vec{y}\ \{\beta \wedge \gamma\}}$$

(xi) *Regla ITE*

$$\frac{\left\{\{\alpha\}\ \vec{x}\ {}_{l}S^{i\ u}\ \vec{y}\ \{\beta\}\right\}_{i<\omega}}{\{\alpha\}\ \vec{x}\ {}_{0}S^{*\infty}\ \vec{y}\ \{\beta\}}$$

Antes de continuar, se comentará el 'significado' de estos axiomas y reglas. Los axiomas $ACT1$ y $ACT2$ establecen verdades acerca de la ejecución de acciones atómicas en general. Los axiomas $SKIP$ y $TEST$, junto con las reglas $SEC$, $CHC$, $PAR$ e $ITE$, caracterizan el comportamiento de los constructos de $P/PML$. La regla $CONS$ permite relacionar las fórmulas Hoare con las fórmulas de primer orden de la teoría bajo consideración. La regla $VAR$ permite sustituir las variables de entrada y salida de una fórmula Hoare, sin alterar su significado. Finalmente, la regla $TIME$ permite razonar acerca del tiempo de ejecución de procesos. A esta altura, es posible explicar la razón por la cual se impuso la restricción sintáctica sobre las fórmulas Hoare establecida en la Def. 2.2.1. Sin

esta restricción, sería posible derivar fórmulas Hoare no válidas. Por ejemplo, a partir de las fórmulas válidas (en alguna interpretación estándar de los números enteros)

$$\{true\}\,\langle x\rangle_{\epsilon}\,1'_{Int}{}^{\epsilon}\,\langle z\rangle\,\{z=x\}\ \text{y}\ \{z=x\}\,\langle z\rangle_{\epsilon}\,1'_{Int}{}^{\epsilon}\,\langle y\rangle\,\{z=x\}$$

y aplicando la regla $SEC$ se obtendría la fórmula

$$\{true\}\,\langle x\rangle_{\epsilon}\,1'_{Int};1'_{Int}{}^{\epsilon+\epsilon}\,\langle y\rangle\,\{z=x\}$$

la cual no es válida puesto que viola la propiedad de mínimo cambio. Por otro lado, la restricción sintáctica $Var(w)\cap\vec{z}=\emptyset$ en la regla $SEC$ se introduce para evitar otras inconsistencias. Por ejemplo, a partir de las fórmulas válidas en alguna interpretación estándar de los números enteros

$$\{u=\epsilon\}\,\langle u\rangle_{\epsilon}\,1'_{T}{}^{u}\,\langle z\rangle\,\{z=\epsilon\}\ \text{y}\ \{z=\epsilon\}\,\langle z\rangle_{\epsilon}\,1'_{T}{}^{z}\,\langle u\rangle\,\{u=\epsilon\}$$

y aplicando la regla $SEC$ sin restricciones se obtendría la fórmula

$$\{u=\epsilon\}\,\langle u\rangle_{\epsilon}\,1'_{T};1'_{T}{}^{u+z}\,\langle u\rangle\,\{u=\epsilon\}$$

que claramente no es válida.

Es útil extender los axiomas y reglas (que son un tanto incómodos) mediante reglas derivadas. La aplicación de una regla derivada reemplaza varias aplicaciones de los axiomas y reglas originales, reduciendo así la longitud de la deducción. Por ejemplo, la siguiente es una regla derivada para acciones *skip*:

(i') *Regla SKIP'*

$$\frac{\alpha\Rightarrow l\leq\epsilon,\qquad \alpha\Rightarrow\beta[\vec{x}/\vec{y}],\qquad \alpha\Rightarrow\epsilon\leq u}{\{\alpha\}\ \vec{x}\ {}_{l}\,1'_{t}{}^{u}\ \vec{y}\ \{\beta\}}$$

Esta regla derivada resulta de la siguiente deducción (a partir de $\alpha\Rightarrow l\leq\epsilon$, $\alpha\Rightarrow\beta[\vec{x}\,/\,\vec{y}]$, $\alpha\Rightarrow\epsilon\leq u$ y de una teoría arbitraria):

| | | |
|---|---|---|
| (1) | $\{\beta\}\ \vec{y}\ {}_{\epsilon}\,1'_{t}{}^{\epsilon}\ \vec{y}\ \{\beta\}$ | Por Ax. $SKIP$ |
| (2) | $\{\beta[\vec{x}/\vec{y}]\}\ \vec{x}\ {}_{\epsilon}\,1'_{t}{}^{\epsilon}\ \vec{y}\ \{\beta\}$ | Por Re. $VAR$ a (1) |
| (3) | $\beta\Rightarrow\beta$ | Por lógica |
| (4) | $\alpha\Rightarrow\beta[\vec{x}/\vec{y}]$ | Por hipótesis |
| (5) | $\{\alpha\}\ \vec{x}\ {}_{\epsilon}\,1'_{t}{}^{\epsilon}\ \vec{y}\ \{\beta\}$ | Por Re. $CONS$ a (2),(3),(4) |
| (6) | $\alpha\Rightarrow l\leq\epsilon$ | Por hipótesis |
| (7) | $\alpha\Rightarrow\epsilon\leq u$ | Por hipótesis |
| (8) | $\{\alpha\}\ \vec{x}\ {}_{l}\,1'_{t}{}^{u}\ \vec{y}\ \{\beta\}$ | Por Re. $TIME$ a (5),(6),(7) |

Otro ejemplo de regla derivada es la siguiente regla para composiciones no determinísticas, la cual resulta de $n-1$ aplicaciones de la regla $CHC$ y de la asociatividad de $min$ y $max$:

(ii') *Regla CHC'*: Para $n \geq 2$

$$\frac{\alpha \Rightarrow l \leq min_i\{l_i\},\ \{\alpha\}\ \vec{x}\ {}_{l_1}S_1{}^{u_1}\ \vec{y}\ \{\beta\}, \ldots, \{\alpha\}\ \vec{x}\ {}_{l_n}S_n{}^{u_n}\ \vec{y}\ \{\beta\},\ \alpha \Rightarrow max_i\{u_i\} \leq u}{\{\alpha\}\ \vec{x}\ {}_{l}S_1 + \ldots + S_n{}^{u}\ \vec{y}\ \{\beta\}}$$

Similarmente pueden establecerse otras reglas derivadas. El cálculo resultante permite trabajar 'hacia atrás' durante el proceso de prueba, lo cual es más natural y puede ser útil para desarrollar un sistema automático de verificación basado en 'condiciones de verificación'.

## 2.4 Consistencia y completitud relativa

Ahora se investigará si el cálculo de Hoare desarrollado resulta ser consistente y completo. Recuérdese que el propósito del cálculo es el de derivar fórmulas de Hoare válidas en una estructura de objeto en particular. Por lo tanto, para obtener resultados significativos se debe apelar a las fórmulas de primer orden válidas en la estructura de objeto $\mathcal{A}$ (es decir, a la teoría $Th(\mathcal{A})$). Además, puesto que una estructura de objeto incluye acciones atómicas que constituyen la máquina abstracta de una aplicación en particular, también deberá apelarse a algún conjunto de fórmulas de Hoare válidas en $\mathcal{A}$ acerca de acciones atómicas de $\mathcal{A}$. Más adelante se discutirá este tema en profundidad, al abordar la investigación de la completitud del cálculo.

Primero se probará la consistencia del cálculo, en una versión un tanto más general que la que se requiere.

TEOREMA 2.4.1 (***Consistencia del Cálculo de Hoare***) *Sea* $\mathcal{S} = \langle A, \langle S, F, P \rangle \rangle$ *una signatura de objeto. Entonces para todo* $W \subseteq For(\mathcal{S}) \cup HFor(\mathcal{S})$ *y* $\{\alpha\}\ \vec{x}\ {}_{l}R^{u}\ \vec{y}\ \{\beta\} \in HFor(\mathcal{S})$

$$\textit{si } W \vdash \{\alpha\}\ \vec{x}\ {}_{l}R^{u}\ \vec{y}\ \{\beta\} \textit{ entonces } W \models \{\alpha\}\ \vec{x}\ {}_{l}R^{u}\ \vec{y}\ \{\beta\}.$$

*Prueba.* Supóngase que $W \vdash h$. Se probará que $W \models h$ por inducción sobre la longitud $k$ de la deducción de $h$.

(a) *Paso base:* Si $k = 0$ entonces se tienen varios casos.

Caso 1: $h \in W$. Luego, por definición de consecuencia lógica, se tiene que $W \models h$.

Caso 2: $h$ es el axioma $ACT1$. Sean $\nu, \nu'$ valuaciones de las variables individuales. Luego

$W \models h$ sii $\models_{\mathcal{M}} h$ para todo modelo $\mathcal{M}$ de $W$ (Definición)

sii $\mathcal{M} \models_{P/PML} true \Rightarrow \left[\vec{x}\ {}_{0}a^{\infty}\ \vec{y}\right] true[\nu]$ (Def. 2.2.2)

sii $\mathsf{l}(a) \geq 0, \mathsf{u}(a) \leq \infty$ y si $\nu(\vec{x}\ a\ \vec{y})\nu'$ entonces $\mathcal{M} \models_{P/PML} true[\nu']$ (Definición)

sii **true** (Lógica)

Caso 3: $h$ es el axioma $ACT2$. Sean $\nu, \nu'$ valuaciones de las variables individuales. Luego

$$
\begin{aligned}
W \models h \text{ sii } & \models_{\mathcal{M}} h \text{ para todo modelo } \mathcal{M} \text{ de } W && \text{(Definición)}\\
\text{sii } & \mathcal{M} \models_{P/PML} false \Rightarrow \left[\vec{x}\ {}_0 a^{\infty}\ \vec{y}\right] false[\nu] && \text{(Def. 2.2.2)}\\
\text{sii } & \mathcal{M} \models_{P/PML} false[\nu] \text{ entonces } \mathcal{M} \models_{P/PML} \left[\vec{x}\ {}_0 a^{\infty}\ \vec{y}\right] false[\nu] && \text{(Definición)}\\
\text{sii } & \textbf{true} && \text{(Lógica)}
\end{aligned}
$$

Caso 4: $h$ es el axioma $SKIP$. Sean $\nu, \nu'$ valuaciones de las variables individuales. Luego

$$
\begin{aligned}
W \models h \text{ sii } & \models_{\mathcal{M}} h \text{ para todo modelo } \mathcal{M} \text{ de } W && \text{(Definición)}\\
\text{sii } & \mathcal{M} \models_{P/PML} \alpha \Rightarrow \left[\vec{x}\ {}_{\epsilon} 1'_t{}^{\epsilon}\ \vec{x}\right] \alpha[\nu] && \text{(Def. 2.2.2)}\\
\text{sii } & \mathcal{M} \models_{P/PML} \alpha[\nu] \text{ entonces } \mathsf{l}(1'_t) \geq \epsilon, \mathsf{u}(1'_t) \leq \epsilon \text{ y}\\
& \quad \nu(\vec{x}\ 1'_t\ \vec{x})\nu' \text{ implica } \mathcal{M} \models_{P/PML} \alpha[\nu'] && \text{(Definición)}\\
\text{sii } & \mathcal{M} \models_{P/PML} \alpha[\nu] \text{ entonces } \epsilon \geq \epsilon, \epsilon \leq \epsilon \text{ y}\\
& \quad \nu = \nu' \text{ implica } \mathcal{M} \models_{P/PML} \alpha[\nu'] && \text{(Definición)}\\
\text{sii } & \textbf{true} && \text{(Lógica)}
\end{aligned}
$$

Caso 5: $h$ es el axioma $TEST$. Sean $\nu, \nu'$ valuaciones de las variables individuales. Luego

$$
\begin{aligned}
W \models h \text{ sii } & \models_{\mathcal{M}} h \text{ para todo modelo } \mathcal{M} \text{ de } W && \text{(Definición)}\\
\text{sii } & \mathcal{M} \models_{P/PML} (\gamma[\vec{x}/\vec{z}] \Rightarrow \alpha) \Rightarrow \left[\vec{x}\ {}_{\epsilon}\gamma?^{\epsilon}\ \vec{x}\right] \alpha[\nu] && \text{(Def. 2.2.2)}\\
\text{sii } & \mathcal{M} \models_{P/PML} \gamma[\vec{x}/\vec{z}] \Rightarrow \alpha[\nu] \text{ entonces } \mathsf{l}(\gamma?) \geq \epsilon, \mathsf{u}(\gamma?) \leq \epsilon \text{ y}\\
& \quad \nu(\vec{x}\ \gamma?\ \vec{x})\nu' \text{ implica } \mathcal{M} \models_{P/PML} \alpha[\nu'] && \text{(Definición)}\\
\text{sii } & \mathcal{M} \models_{P/PML} \gamma[\vec{x}/\vec{z}] \Rightarrow \alpha[\nu] \text{ entonces } \epsilon \geq \epsilon, \epsilon \leq \epsilon \text{ y}\\
& \quad \nu = \nu', \mathcal{M} \models_{P/PML} \gamma[\vec{x}/\vec{z}][\nu] \text{ implican } \mathcal{M} \models_{P/PML} \alpha[\nu'] && \text{(Definición)}\\
\text{sii } & \textbf{true} && \text{(Lógica)}
\end{aligned}
$$

(b) *Paso inductivo:* Supóngase que si $W \vdash h$ en una deducción de longitud $k < m$ con $m > 1$ entonces $W \models h$. Luego, si $W \vdash h$ en una deducción de longitud $k = m$, se tienen varios casos:

Caso 1: $h$ es consecuencia de aplicar la regla $CONS$. Luego $h$ tiene la forma $\{\alpha\}\ \vec{x}\ {}_l R^u\ \vec{y}\ \{\beta\}$, y además $W \vdash \alpha \Rightarrow \gamma$, $W \vdash \{\gamma\}\ \vec{x}\ {}_l R^u\ \vec{y}\ \{\delta\}$ y $W \vdash \delta \Rightarrow \beta$, cada una en una deducción de menos de $k$ pasos. Luego, $\{\alpha \Rightarrow \gamma, \delta \Rightarrow \beta\} \subseteq W$, por lo tanto $W \models \alpha \Rightarrow \gamma$ y $W \models \delta \Rightarrow \beta$. Por hipótesis inductiva, $W \models \{\gamma\}\ \vec{x}\ {}_l R^u\ \vec{y}\ \{\delta\}$. Sean $\nu, \nu'$ valuaciones de las variables

individuales, y $h'$ la fórmula $\{\gamma\}\ \vec{x}\ {}_{l}R^{u}\ \vec{y}\ \{\delta\}$. Entonces

$W \models h'$ sii $\models_{\mathcal{M}} h'$ para todo modelo $\mathcal{M}$ de $W$ (Definición)

sii $\mathcal{M} \models_{P/PML} \gamma \Rightarrow \left[\vec{x}\ {}_{l}R^{u}\ \vec{y}\right] \delta[\nu]$ (Def. 2.2.2)

sii $\mathcal{M} \models_{P/PML} \gamma[\nu]$ entonces $\mathsf{l}(R) \geq l_{\nu}^{\mathcal{M}}, \mathsf{u}(R) \leq u_{\nu}^{\mathcal{M}}$ y
$\nu(\vec{x}\ R\ \vec{y})\nu'$ implica $\mathcal{M} \models_{P/PML} \delta[\nu']$ (Definición)

ent. $\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces $\mathsf{l}(R) \geq l_{\nu}^{\mathcal{M}}, \mathsf{u}(R) \leq u_{\nu}^{\mathcal{M}}$ y
$\nu(\vec{x}\ R\ \vec{y})\nu'$ implica $\mathcal{M} \models_{P/PML} \beta[\nu']$ (Hip. y Lógica)

sii $\mathcal{M} \models_{P/PML} \alpha \Rightarrow \left[\vec{x}\ {}_{l}R^{u}\ \vec{y}\right] \beta[\nu]$ (Def. 2.2.2)

sii $\models_{\mathcal{M}} h$ (Definición)

sii $W \models h$ (Definición)

Caso 2: $h$ es consecuencia de aplicar la regla $VAR$. Luego $h$ tiene la forma $\{\alpha[\vec{x}\ /\ \vec{z}]\}\ \vec{x}\ {}_{l[\vec{x}/\vec{z}]}R^{u[\vec{x}/\vec{z}]}\ \vec{y}\ \{\beta[\vec{y}/\vec{w}]\}$, y además $W \vdash \{\alpha\}\ \vec{z}\ {}_{l}R^{u}\ \vec{w}\ \{\beta\}$, en una deducción de menos de $k$ pasos. Por hipótesis inductiva, $W \models \{\alpha\}\ \vec{z}\ {}_{l}R^{u}\ \vec{w}\ \{\beta\}$. Sean $\nu, \nu'$ valuaciones de las variables individuales, y $h'$ la fórmula $\{\alpha\}\ \vec{z}\ {}_{l}R^{u}\ \vec{w}\ \{\beta\}$. Entonces

$W \models h'$ sii $\models_{\mathcal{M}} h'$ para todo modelo $\mathcal{M}$ de $W$ (Definición)

sii $\mathcal{M} \models_{P/PML} \alpha \Rightarrow \left[\vec{z}\ {}_{l}R^{u}\ \vec{w}\right] \beta[\nu]$ (Def. 2.2.2)

sii $\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces $\mathsf{l}(R) \geq l_{\nu}^{\mathcal{M}}, \mathsf{u}(R) \leq u_{\nu}^{\mathcal{M}}$ y
$\nu(\vec{z}\ R\ \vec{w})\nu'$ implica $\mathcal{M} \models_{P/PML} \beta[\nu']$ (Definición)

ent. $\mathcal{M} \models_{P/PML} \alpha[\vec{x}/\vec{z}][\nu]$ entonces
$\mathsf{l}(R) \geq l[\vec{x}/\vec{z}]_{\nu}^{\mathcal{M}}, \mathsf{u}(R) \leq u[\vec{x}/\vec{z}]_{\nu}^{\mathcal{M}}$ y
$\nu(\vec{x}\ R\ \vec{y})\nu'$ implica $\mathcal{M} \models_{P/PML} \beta[\vec{y}/\vec{w}][\nu']$ (Lóg. y $Var(\beta) \subseteq \vec{w}$)

sii $\mathcal{M} \models_{P/PML} \alpha[\vec{x}/\vec{z}] \Rightarrow \left[\vec{x}\ {}_{l[\vec{x}/\vec{z}]}R^{u[\vec{x}/\vec{z}]}\ \vec{y}\right] \beta[\vec{y}/\vec{w}][\nu]$ (Def. 2.2.2)

sii $\models_{\mathcal{M}} h$ (Definición)

sii $W \models h$ (Definición)

Caso 3: $h$ es consecuencia de aplicar la regla $TIME$. Luego $h$ tiene la forma $\{\alpha\}\ \vec{x}\ {}_{l}R^{u}\ \vec{y}\ \{\beta\}$, y además $W \vdash \alpha \Rightarrow l \leq v$, $W \vdash \{\alpha\}\ \vec{x}\ {}_{v}R^{w}\ \vec{y}\ \{\beta\}$ y $W \vdash \alpha \Rightarrow w \leq u$, cada una en una deducción de menos de $k$ pasos. Luego, $\{\alpha \Rightarrow l \leq v, \alpha \Rightarrow w \leq u\} \subseteq W$, por lo tanto $W \models \alpha \Rightarrow l \leq v$ y $W \models \alpha \Rightarrow w \leq u$. Por hipótesis inductiva, $W \models \{\alpha\}\ \vec{x}\ {}_{v}R^{w}\ \vec{y}\ \{\beta\}$.

Sean $\nu, \nu'$ valuaciones de las variables individuales, y $h'$ la fórmula $\{\alpha\}\ \vec{x}\ {}_v R^w\ \vec{y}\ \{\beta\}$. Entonces

$W \models h'$ sii $\models_{\mathcal{M}} h'$ para todo modelo $\mathcal{M}$ de $W$ (Definición)

sii $\mathcal{M} \models_{P/PML} \alpha \Rightarrow \left[\vec{x}\ {}_v R^w\ \vec{y}\right] \beta[\nu]$ (Def. 2.2.2)

sii $\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces $\mathsf{l}(R) \geq v_\nu^{\mathcal{M}}, \mathsf{u}(R) \leq w_\nu^{\mathcal{M}}$ y

$\nu(\vec{x}\ R\ \vec{y})\nu'$ implica $\mathcal{M} \models_{P/PML} \delta[\nu']$ (Definición)

ent. $\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces

$\mathsf{l}(R) \geq v_\nu^{\mathcal{M}} \geq l_\nu^{\mathcal{M}}, \mathsf{u}(R) \leq w_\nu^{\mathcal{M}} \leq u_\nu^{\mathcal{M}}$ y

$\nu(\vec{x}\ R\ \vec{y})\nu'$ implica $\mathcal{M} \models_{P/PML} \beta[\nu']$ (Hip. y Lógica)

sii $\mathcal{M} \models_{P/PML} \alpha \Rightarrow \left[\vec{x}\ {}_l R^u\ \vec{y}\right] \beta[\nu]$ (Lóg. y Def. 2.2.2)

sii $\models_{\mathcal{M}} h$ (Definición)

sii $W \models h$ (Definición)

Caso 4: $h$ es consecuencia de aplicar la regla $SEC$. Luego $h$ tiene la forma $\{\alpha\}\ \vec{x}\ {}_l S;T^{\ u+w}\ \vec{y}\ \{\beta\}$, y además $W \vdash \{\alpha\}\ \vec{x}\ {}_l S^u\ \vec{z}\ \{\gamma\}$ y $W \vdash \{\gamma\}\ \vec{z}\ {}_v T^w\ \vec{y}\ \{\beta\}$ con $Var(w) \cap \vec{z} = \emptyset$, cada una en una deducción de menos de $k$ pasos. Por hipótesis inductiva, $W \models \{\alpha\}\ \vec{x}\ {}_l S^u\ \vec{z}\ \{\gamma\}$ y $W \models \{\gamma\}\ \vec{z}\ {}_v T^w\ \vec{y}\ \{\beta\}$. Sean $\nu_1, \nu_2, \nu_3, \nu_4$ valuaciones de las variables individuales, y $\mathcal{M}$ un modelo de $W$. Entonces, por definición, se tiene que

(1) $\mathcal{M} \models_{P/PML} \alpha[\nu_1]$ entonces $\mathsf{l}(S) \geq l_{\nu_1}^{\mathcal{M}}, \mathsf{u}(S) \leq u_{\nu_1}^{\mathcal{M}}$ y

$\left\langle \nu_1(\vec{x}), \nu_2(\vec{z}) \right\rangle \in S^{\mathcal{M}}, \nu_1(z) = \nu_2(z)$ con $z \notin \vec{z}$ implica $\mathcal{M} \models_{P/PML} \gamma[\nu_2]$

y

(2) $\mathcal{M} \models_{P/PML} \gamma[\nu_3]$ entonces $\mathsf{l}(T) \geq v_{\nu_3}^{\mathcal{M}}, \mathsf{u}(T) \leq w_{\nu_3}^{\mathcal{M}}$ y

$\left\langle \nu_3(\vec{z}), \nu_4(\vec{y}) \right\rangle \in T^{\mathcal{M}}, \nu_3(z) = \nu_4(z)$ con $z \notin \vec{y}$ implica $\mathcal{M} \models_{P/PML} \beta[\nu_4]$.

En particular, para $\nu_2 = \nu_3$ desde 1 y 2 por lógica se tiene que

$\mathcal{M} \models_{P/PML} \alpha[\nu_1]$ entonces $\mathsf{l}(S) \geq l_{\nu_1}^{\mathcal{M}}, \mathsf{u}(S) \leq u_{\nu_1}^{\mathcal{M}}$ y

$\left\langle \nu_1(\vec{x}), \nu_2(\vec{z}) \right\rangle \in S^{\mathcal{M}}, \nu_1(z) = \nu_2(z)$ con $z \notin \vec{z}, \mathsf{l}(T) \geq v_{\nu_2}^{\mathcal{M}}, \mathsf{u}(T) \leq w_{\nu_2}^{\mathcal{M}}$,

$\left\langle \nu_2(\vec{z}), \nu_4(\vec{y}) \right\rangle \in T^{\mathcal{M}}, \nu_2(z) = \nu_4(z)$ con $z \notin \vec{y}$ implican $\mathcal{M} \models_{P/PML} \beta[\nu_4]$.

Por hipótesis se tenía que $Var(w) \cap \vec{z} = \emptyset$, luego por lógica y definición se tiene que

$\mathcal{M} \models_{P/PML} \alpha[\nu_1]$ entonces $\mathsf{l}(S;T) = \mathsf{l}(S) \geq l_{\nu_1}^{\mathcal{M}}, \mathsf{u}(S;T) = \mathsf{u}(S) + \mathsf{u}(T) \leq (u+w)_{\nu_1}^{\mathcal{M}}$ y

$\left\langle \nu_1(\vec{x}), \nu_4(\vec{y}) \right\rangle \in (S;T)^{\mathcal{M}}, \nu_1(z) = \nu_2(z)$ con $z \notin \vec{z}, \nu_2(z) = \nu_4(z)$ con $z \notin \vec{y}$

implican $\mathcal{M} \models_{P/PML} \beta[\nu_4]$.

La condición de mínimo cambio $\nu_1(z) = \nu_4(z)$ con $z \notin \vec{y}$ no puede asegurarse, pero no se la considera debido al problema de composicionalidad explicado en la Sección 2.3. Luego, por definición se tiene que $\mathcal{M} \models_{P/PML} \alpha \Rightarrow \left[\vec{x}\ {}_l\ S;T\ {}^{u+w}\ \vec{y}\right] \beta[\nu]$, y por Def. 2.2.2 que $W \models h$.

Caso 5: $h$ es consecuencia de aplicar la regla $CHC$. Luego $h$ tiene la forma

$$\{\alpha\}\ \vec{x}\ {}_{min\{l,v\}}\ S+T\ {}^{max\{u,w\}}\ \vec{y}\ \{\beta\},$$

y además $W \vdash \{\alpha\}\ \vec{x}\ {}_lS^u\ \vec{y}\ \{\beta\}$ y $W \vdash \{\alpha\}\ \vec{x}\ {}_vT^w\ \vec{y}\ \{\beta\}$, cada una en una deducción de menos de $k$ pasos. Por hipótesis inductiva, $W \models \{\alpha\}\ \vec{x}\ {}_lS^u\ \vec{y}\ \{\beta\}$ y $W \models \{\alpha\}\ \vec{x}\ {}_vT^w\ \vec{y}\ \{\beta\}$. Sean $\nu, \nu'$ valuaciones de las variables individuales, y $\mathcal{M}$ un modelo de $W$. Entonces, por definición, se tiene que

(1) $\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces $\mathsf{l}(S) \geq l_\nu^{\mathcal{M}}, \mathsf{u}(S) \leq u_\nu^{\mathcal{M}}$ y
$\left\langle \nu(\vec{x}), \nu'(\vec{y}) \right\rangle \in S^{\mathcal{M}}, \nu'(z) = \nu(z)$ con $z \notin \vec{y}$ implica $\mathcal{M} \models_{P/PML} \beta[\nu']$

y

(2) $\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces $\mathsf{l}(T) \geq v_\nu^{\mathcal{M}}, \mathsf{u}(T) \leq w_\nu^{\mathcal{M}}$ y
$\left\langle \nu(\vec{x}), \nu'(\vec{y}) \right\rangle \in T^{\mathcal{M}}, \nu'(z) = \nu(z)$ con $z \notin \vec{y}$ implica $\mathcal{M} \models_{P/PML} \beta[\nu']$

Desde 1 y 2 por lógica se tiene que

$\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces $\mathsf{l}(S) \geq l_\nu^{\mathcal{M}}, \mathsf{u}(S) \leq u_\nu^{\mathcal{M}}, \mathsf{l}(T) \geq v_\nu^{\mathcal{M}}, \mathsf{u}(T) \leq w_\nu^{\mathcal{M}}$ y
$\left\langle \nu(\vec{x}), \nu'(\vec{y}) \right\rangle \in S^{\mathcal{M}}$ ó $\left\langle \nu(\vec{x}), \nu'(\vec{y}) \right\rangle \in T^{\mathcal{M}}, \nu(z) = \nu'(z)$ con $z \notin \vec{y}$
implican $\mathcal{M} \models_{P/PML} \beta[\nu']$.

Luego, por definición se tiene que

$\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces
$\mathsf{l}(S+T) = min\{\mathsf{l}(S), \mathsf{l}(T)\} \geq min\{l, v\}_\nu^{\mathcal{M}}, \mathsf{u}(S+T) = max\{\mathsf{u}(S), \mathsf{u}(T)\} \leq max\{u, w\}_\nu^{\mathcal{M}}$ y
$\left\langle \nu(\vec{x}), \nu'(\vec{y}) \right\rangle \in (S+T)^{\mathcal{M}}, \nu(z) = \nu'(z)$ con $z \notin \vec{y}$ implica $\mathcal{M} \models_{P/PML} \beta[\nu']$.

Así, por definición se tiene que $\mathcal{M} \models_{P/PML} \alpha \Rightarrow \left[\vec{x}\ {}_{min\{l,v\}}\ S+T\ {}^{max\{u,w\}}\ \vec{y}\right] \beta[\nu]$, y por Def. 2.2.2 que $W \models h$.

Caso 6: $h$ es consecuencia de aplicar la regla $PAR$. Luego $h$ tiene la forma

$$\{\alpha\}\ \vec{x}\ {}_{max\{l,v\}}\ S \cdot T\ {}^{max\{u,w\}}\ \vec{y}\ \{\beta \wedge \gamma\},$$

y además $W \vdash \{\alpha\}\ \vec{x}\ {}_lS^u\ \vec{y}\ \{\beta\}$ y $W \vdash \{\alpha\}\ \vec{x}\ {}_vT^w\ \vec{y}\ \{\gamma\}$, cada una en una deducción de menos de $k$ pasos. Por hipótesis inductiva, $W \models \{\alpha\}\ \vec{x}\ {}_lS^u\ \vec{y}\ \{\beta\}$ y $W \models \{\alpha\}\ \vec{x}$

${}_vT^w\ \vec{y}\ \{\gamma\}$. Sean $\nu, \nu'$ valuaciones de las variables individuales, y $\mathcal{M}$ un modelo de $W$. Entonces, por definición, se tiene que

(1) $\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces $\mathsf{l}(S) \geq l_\nu^{\mathcal{M}}, \mathsf{u}(S) \leq u_\nu^{\mathcal{M}}$ y
$\left\langle \nu(\vec{x}), \nu'(\vec{y}) \right\rangle \in S^{\mathcal{M}}, \nu'(z) = \nu(z)$ con $z \notin \vec{y}$ implica $\mathcal{M} \models_{P/PML} \beta[\nu']$

y

(2) $\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces $\mathsf{l}(T) \geq v_\nu^{\mathcal{M}}, \mathsf{u}(T) \leq w_\nu^{\mathcal{M}}$ y
$\left\langle \nu(\vec{x}), \nu'(\vec{y}) \right\rangle \in T^{\mathcal{M}}, \nu'(z) = \nu(z)$ con $z \notin \vec{y}$ implica $\mathcal{M} \models_{P/PML} \gamma[\nu']$

Desde 1 y 2 por lógica se tiene que

$\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces $\mathsf{l}(S) \geq l_{\nu_1}^{\mathcal{M}}, \mathsf{u}(S) \leq u_\nu^{\mathcal{M}}, \mathsf{l}(T) \geq v_\nu^{\mathcal{M}}, \mathsf{u}(T) \leq w_\nu^{\mathcal{M}}$ y
$\left\langle \nu(\vec{x}), \nu'(\vec{y}) \right\rangle \in S^{\mathcal{M}}$ y $\left\langle \nu(\vec{x}), \nu'(\vec{y}) \right\rangle \in T^{\mathcal{M}}, \nu(z) = \nu'(z)$ con $z \notin \vec{y}$
implican $\mathcal{M} \models_{P/PML} \beta[\nu']$ y $\mathcal{M} \models_{P/PML} \gamma[\nu']$.

Luego, por definición se tiene que

$\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces
$\mathsf{l}(S{\cdot}T) = max\{\mathsf{l}(S), \mathsf{l}(T)\} \geq max\{l, v\}_\nu^{\mathcal{M}}, \mathsf{u}(S{\cdot}T) = max\{\mathsf{u}(S), \mathsf{u}(T)\} \leq max\{u, w\}_\nu^{\mathcal{M}}$ y
$\left\langle \nu(\vec{x}), \nu'(\vec{y}) \right\rangle \in (S{\cdot}T)^{\mathcal{M}}, \nu(z) = \nu'(z)$ con $z \notin \vec{y}$ implica $\mathcal{M} \models_{P/PML} \beta \wedge \gamma[\nu']$.

Así, por definición se tiene que $\mathcal{M} \models_{P/PML} \alpha \Rightarrow \left[\vec{x}\ {}_{max\{l,v\}}\ S{\cdot}T\ {}^{max\{u,w\}}\ \vec{y}\right] \beta \wedge \gamma[\nu]$, y por Def. 2.2.2 que $W \models h$.

Caso 7: $h$ es consecuencia de aplicar la regla $ITE$. Luego $h$ tiene la forma $\{\alpha\}\ \vec{x}\ {}_0S^{*\infty}\ \vec{y}\ \{\beta\}$, y además $W \vdash \{\alpha\}\ \vec{x}\ {}_iS^{i\,u}\ \vec{y}\ \{\beta\}$ para todo $i < \omega$ en una deducción de menos de $k$ pasos. Por hipótesis inductiva, $W \models \{\alpha\}\ \vec{x}\ {}_iS^{i\,u}\ \vec{y}\ \{\beta\}$ para todo $i < \omega$. Sean $\nu, \nu'$ valuaciones de las variables individuales, y $\mathcal{M}$ un modelo de $W$. Entonces, por definición, se tiene que

$\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces $\mathsf{l}(S^i) \geq l_\nu^{\mathcal{M}}, \mathsf{u}(S^i) \leq u_\nu^{\mathcal{M}}$ y
$\left\langle \nu(\vec{x}), \nu'(\vec{x}) \right\rangle \in (S^i)^{\mathcal{M}}, \nu'(z) = \nu(z)$ con $z \notin \vec{x}$ implica $\mathcal{M} \models_{P/PML} \beta[\nu']$

para todo $i < \omega$. Luego, por lógica y definición se tiene que

$\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces $\mathsf{l}(S^j) \geq l_\nu^{\mathcal{M}}, \mathsf{u}(S^j) \leq u_\nu^{\mathcal{M}}$ y
$\left\langle \nu(\vec{x}), \nu'(\vec{y}) \right\rangle \in (S^j)^{\mathcal{M}}, \nu(z) = \nu'(z)$ con $z \notin \vec{y}$ implica $\mathcal{M} \models_{P/PML} \beta[\nu']$

para algún $j < \omega$, y por definición se tiene que

$\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces $\mathsf{l}(S^*) \geq 0, \mathsf{u}(S^*) \leq \infty$ y
$\left\langle \nu(\vec{x}), \nu'(\vec{y}) \right\rangle \in (S^*)^{\mathcal{M}}, \nu(z) = \nu'(z)$ con $z \notin \vec{y}$ implica $\mathcal{M} \models_{P/PML} \beta[\nu']$.

Así, por definición se tiene que $\mathcal{M} \models_{P/PML} \alpha \Rightarrow \left[\vec{x}\ {}_0 S^{*\infty}\ \vec{y}\right] \beta[\nu]$, y por Def. 2.2.2 que $W \models h$.

■

A continuación se estudiará la completitud del cálculo de Hoare presentado. Se denotará por $HTh(\mathcal{A})$ al conjunto de fórmulas de Hoare válidas en $\mathcal{A}$. Es fácil ver que $HTh(\mathcal{A})$ es una teoría. Ahora bien, el propósito del cálculo es el de derivar fórmulas de Hoare a partir de una estructura de objeto $\mathcal{A}$ en particular, por lo tanto parece razonable investigar la completitud del cálculo a partir del conjunto de fórmulas $Th(\mathcal{A}) \cup HTh(\mathcal{A})$. Por otro lado, para encontrar un resultado válido en cuanto a la completitud, es necesario restringir la atención a cierto tipo de interpretaciones. Estas estucturas de objeto se llamarán *expresivas* (Ver [11, 13]). Una estructura de objeto $\mathcal{A}$ se dirá que es expresiva (para $P/PML$) si para todo término de acción temporal base $\vec{x}\ {}_l R^u\ \vec{y}$ y $\varphi \in For(\mathcal{S})$ de primer orden, existe una fórmula de primer orden $\psi_L \in For(\mathcal{S})$ tal que $\mathcal{A} \models_{P/PML} \psi_L \Leftrightarrow \left[\vec{x}\ {}_l R^u\ \vec{y}\right] \varphi$. En los ejemplos prácticos de las secciones posteriores, se asumirá que se razona sobre estructuras de objeto expresivas.

Ahora se probará que el cálculo de Hoare es completo sólo si se consideran interpretaciones expresivas.

TEOREMA 2.4.2 (***Completitud del Cálculo de Hoare***) *Sean $\mathcal{S} = \langle A, \langle S, F, P\rangle\rangle$ una signatura de objeto y $\mathcal{A}$ una estructura de objeto expresiva para $\mathcal{S}$. Entonces para todo $\{\alpha\}\ \vec{x}\ {}_l R^u\ \vec{y}\ \{\beta\} \in HFor(\mathcal{S})$*

$$\textit{si } Th(\mathcal{A}) \cup HTh(\mathcal{A}) \models \{\alpha\}\ \vec{x}\ {}_l R^u\ \vec{y}\ \{\beta\} \textit{ entonces } Th(\mathcal{A}) \cup HTh(\mathcal{A}) \vdash \{\alpha\}\ \vec{x}\ {}_l R^u\ \vec{y}\ \{\beta\}.$$

*Prueba.* Sea $W$ el conjunto $Th(\mathcal{A}) \cup HTh(\mathcal{A})$ y $h$ una fórmula de Hoare $\{\alpha\}\ \vec{x}\ {}_l R^u\ \vec{y}\ \{\beta\}$. Supóngase que $W \models h$. Se probará que $W \vdash h$ por inducción estructural sobre $R$.

(a) *Paso base:* Se tienen varios casos.

Caso 1: $R \equiv a$ con $a \in A$. Por definición, $h \in HTh(\mathcal{A})$. Luego, es obvio que $W \vdash h$.

Caso 2: $R \equiv 1'_t$. Sean $\nu, \nu'$ valuaciones de las variables individuales. Luego

$$\begin{aligned}
&W \models h \text{ sii } \models_{\mathcal{M}} h \text{ para todo modelo } \mathcal{M} \text{ de } W && \text{(Definición)}\\
&\quad \text{sii } \mathcal{M} \models_{P/PML} \alpha \Rightarrow \left[\vec{x}\ {}_l 1'_t{}^u\ \vec{y}\right] \beta[\nu] && \text{(Def. 2.2.2)}\\
&\quad \text{sii } \mathcal{M} \models_{P/PML} \alpha[\nu] \text{ entonces } \mathsf{l}(1'_t) \geq l^{\mathcal{M}}_{\nu}, \mathsf{u}(1'_t) \leq u^{\mathcal{M}}_{\nu} \text{ y}\\
&\qquad \nu(\vec{x}\ 1'_t\ \vec{y})\nu' \text{ implica } \mathcal{M} \models_{P/PML} \beta[\nu'] && \text{(Definición)}\\
&\quad \text{sii } \mathcal{M} \models_{P/PML} \alpha[\nu] \text{ entonces } \epsilon \geq l^{\mathcal{M}}_{\nu}, \epsilon \leq u^{\mathcal{M}}_{\nu} \text{ y}\\
&\qquad \nu' = \nu^{\nu(\vec{x})}_{\vec{y}} \text{ implica } \mathcal{M} \models_{P/PML} \beta[\nu'] && \text{(Definición)}\\
&\quad \text{ent. } \mathcal{M} \models_{P/PML} \alpha \Rightarrow l \leq \epsilon,\ \mathcal{M} \models_{P/PML} \alpha \Rightarrow \epsilon \leq u \text{ y}\\
&\qquad \mathcal{M} \models_{P/PML} \alpha \Rightarrow \beta[\vec{x}/\vec{y}] && \text{(Lógica)}\\
&\quad \text{sii } W \models \alpha \Rightarrow l \leq \epsilon,\ W \models \alpha \Rightarrow \epsilon \leq u \text{ y}\\
&\qquad W \models \alpha \Rightarrow \beta[\vec{x}/\vec{y}] && \text{(Definición)}
\end{aligned}$$

ent. $\{\alpha \Rightarrow l \leq \epsilon, \alpha \Rightarrow \epsilon \leq u, \alpha \Rightarrow \beta[\vec{x}/\vec{y}]\} \subseteq Th(\mathcal{A})$ (Def. y Lóg.)

ent. $W \vdash \alpha \Rightarrow l \leq \epsilon$, $W \vdash \alpha \Rightarrow \epsilon \leq u$ y

$W \vdash \alpha \Rightarrow \beta[\vec{x}/\vec{y}]$. (Definición)

Así, se tiene que la deducción

| | | |
|---|---|---|
| (1) | $\{\beta\}\ \vec{y}\ {}_{\epsilon}1'_{t}{}^{\epsilon}\ \vec{y}\ \{\beta\}$ | $(SKIP)$ |
| (2) | $\{\beta[\vec{x}/\vec{y}]\}\ \vec{x}\ {}_{\epsilon}1'_{t}{}^{\epsilon}\ \vec{y}\ \{\beta\}$ | $(VAR)$ |
| (3) | $\alpha \Rightarrow \beta[\vec{x}/\vec{y}]$ | (Hipótesis) |
| (4) | $\{\alpha\}\ \vec{x}\ {}_{\epsilon}1'_{t}{}^{\epsilon}\ \vec{y}\ \{\beta\}$ | $(CONS$ 2,3) |
| (5) | $\alpha \Rightarrow l \leq \epsilon$ | (Hipótesis) |
| (6) | $\alpha \Rightarrow \epsilon \leq u$ | (Hipótesis) |
| (7) | $\{\alpha\}\ \vec{x}\ {}_{l}1'_{t}{}^{u}\ \vec{y}\ \{\beta\}$ | $(TIME$ 4,5,6) |

es una deducción para $h$ desde $W$. Por lo tanto $W \vdash h$.

Caso 3: $R \equiv \gamma?$. Sean $\nu, \nu'$ valuaciones de las variables individuales. Luego

$W \models h$ sii $\models_{\mathcal{M}} h$ para todo modelo $\mathcal{M}$ de $W$ (Definición)

sii $\mathcal{M} \models_{P/PML} \alpha \Rightarrow \left[\vec{x}\ {}_{l}\gamma?{}^{u}\ \vec{y}\right]\beta[\nu]$ (Def. 2.2.2)

sii $\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces $\mathrm{l}(\gamma?) \geq l_{\nu}^{\mathcal{M}}, \mathrm{u}(\gamma?) \leq u_{\nu}^{\mathcal{M}}$ y

$\nu(\vec{x}\ \gamma?\ \vec{y})\nu'$ implica $\mathcal{M} \models_{P/PML} \beta[\nu']$ (Definición)

sii $\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces $\epsilon \geq l_{\nu}^{\mathcal{M}}, \epsilon \leq u_{\nu}^{\mathcal{M}}$ y

$\nu' = \nu_{\vec{y}}^{\nu(\vec{x})}$ y $\mathcal{M} \models_{P/PML} \gamma[\vec{y}/\vec{z}][\nu']$ implica $\mathcal{M} \models_{P/PML} \beta[\nu']$ (Definición)

ent. $\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces $\epsilon \geq l_{\nu}^{\mathcal{M}}, \epsilon \leq u_{\nu}^{\mathcal{M}}$ y

$\mathcal{M} \models_{P/PML} \gamma[\vec{y}/\vec{z}][\vec{x}/\vec{y}][\nu]$ implica $\mathcal{M} \models_{P/PML} \beta[\vec{x}/\vec{y}][\nu]$ (Lógica)

ent. $\mathcal{M} \models_{P/PML} \alpha \Rightarrow l \leq \epsilon$, $\mathcal{M} \models_{P/PML} \alpha \Rightarrow \epsilon \leq u$ y

$\mathcal{M} \models_{P/PML} \alpha \Rightarrow (\gamma[\vec{y}/\vec{z}] \Rightarrow \beta)[\vec{x}/\vec{y}]$ (Lógica)

sii $W \models \alpha \Rightarrow l \leq \epsilon$, $W \models \alpha \Rightarrow \epsilon \leq u$ y

$W \models \alpha \Rightarrow (\gamma[\vec{y}/\vec{z}] \Rightarrow \beta)[\vec{x}/\vec{y}]$ (Definición)

ent. $\{\alpha \Rightarrow l \leq \epsilon, \alpha \Rightarrow \epsilon \leq u, \alpha \Rightarrow (\gamma[\vec{y}/\vec{z}] \Rightarrow \beta)[\vec{x}/\vec{y}]\} \subseteq Th(\mathcal{A})$ (Def. y Lóg.)

ent. $W \vdash \alpha \Rightarrow l \leq \epsilon$, $W \vdash \alpha \Rightarrow \epsilon \leq u$ y

$W \vdash \alpha \Rightarrow (\gamma[\vec{y}/\vec{z}] \Rightarrow \beta)[\vec{x}/\vec{y}]$. (Definición)

Así, se tiene que la deducción

| | | |
|---|---|---|
| (1) | $\{\gamma[\vec{y}/\vec{z}] \Rightarrow \beta\}\ \vec{y}\ {}_{\epsilon}\gamma?^{\epsilon}\ \vec{y}\ \{\beta\}$ | $(TEST)$ |
| (2) | $\{(\gamma[\vec{y}/\vec{z}] \Rightarrow \beta)[\vec{x}/\vec{y}]\}\ \vec{x}\ {}_{\epsilon}\gamma?^{\epsilon}\ \vec{y}\ \{\beta\}$ | $(VAR)$ |
| (3) | $\alpha \Rightarrow (\gamma[\vec{y}/\vec{z}] \Rightarrow \beta)[\vec{x}/\vec{y}]$ | (Hipótesis) |
| (4) | $\{\alpha\}\ \vec{x}\ {}_{\epsilon}\gamma?^{\epsilon}\ \vec{y}\ \{\beta\}$ | $(CONS$ 2,3) |
| (5) | $\alpha \Rightarrow l \leq \epsilon$ | (Hipótesis) |
| (6) | $\alpha \Rightarrow \epsilon \leq u$ | (Hipótesis) |
| (7) | $\{\alpha\}\ \vec{x}\ {}_{l}\gamma?^{u}\ \vec{y}\ \{\beta\}$ | $(TIME$ 4,5,6) |

es una deducción para $h$ desde $W$. Por lo tanto $W \vdash h$.

(b) *Paso inductivo:* Supóngase que la propiedad es verdadera para $S, T \in GRT(\mathcal{S})$ y que $W \models h$. Luego, se tienen varios casos:

Caso 1: $R \equiv S;T$. Sean $\nu, \nu'$ valuaciones de las variables individuales. Luego

$W \models h$ sii $\models_{\mathcal{M}} h$ para todo modelo $\mathcal{M}$ de $W$ (Definición)

sii $\mathcal{M} \models_{P/PML} \alpha \Rightarrow \left[\vec{x}\ {}_{l}S;T^{u}\ \vec{y}\right]\beta[\nu]$ (Def. 2.2.2)

sii $\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces $\mathsf{l}(S;T) \geq l_{\nu}^{\mathcal{M}}, \mathsf{u}(S;T) \leq u_{\nu}^{\mathcal{M}}$ y
$\nu(\vec{x}\ S;T\ \vec{y})\nu'$ implica $\mathcal{M} \models_{P/PML} \beta[\nu']$ (Definición)

sii $\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces $\mathsf{l}(S) \geq l_{\nu}^{\mathcal{M}}, \mathsf{u}(S) + \mathsf{u}(T) \leq u_{\nu}^{\mathcal{M}}$ y
$\left\langle \nu(\vec{x}), \nu'(\vec{y}) \right\rangle \in (S;T)^{\mathcal{M}}, \nu(z) = \nu'(z)$ con $z \notin \vec{y}$
implica $\mathcal{M} \models_{P/PML} \beta[\nu']$. (Definición)

Así, se tiene por un lado que

$\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces $\mathsf{l}(S) \geq l_{\nu}^{\mathcal{M}}$ y $\mathsf{u}(S) + \mathsf{u}(T) \leq u_{\nu}^{\mathcal{M}}$
sii $W \models \alpha \Rightarrow l \leq \mathsf{l}(S)$ y $W \models \alpha \Rightarrow \mathsf{u}(S) + \mathsf{u}(T) \leq u$ (Lógica)
ent. $\{\alpha \Rightarrow l \leq \mathsf{l}(S), \alpha \Rightarrow \mathsf{u}(S) + \mathsf{u}(T) \leq u\} \subseteq Th(\mathcal{A})$ (Def. y Lóg.)
ent. $W \vdash \alpha \Rightarrow l \leq \mathsf{l}(S)$ y $W \vdash \alpha \Rightarrow \mathsf{u}(S) + \mathsf{u}(T) \leq u$ (Definición)

y por otro lado que

(*)
$\mathcal{M} \models_{P/PML} \alpha[\nu]$ implica que si existe $\mathsf{s}$ tal que
$\left\langle \nu(\vec{x}), \mathsf{s} \right\rangle \in S^{\mathcal{M}}, \left\langle \mathsf{s}, \nu'(\vec{y}) \right\rangle \in T^{\mathcal{M}}, \nu'(z) = \nu(z)$ con $z \notin \vec{y}$ ent. $\mathcal{M} \models_{P/PML} \beta[\nu']$.

Por otro lado, como $\mathcal{A}$ es expresiva se tiene que existe una fórmula de primer orden $\psi$ tal que $\mathcal{A} \models_{P/PML} \psi \Leftrightarrow \left[\vec{z}\ {}_{\mathsf{l}(T)} T^{\mathsf{u}(T)}\ \vec{y}\right] \beta$. De aquí, por lógica y definición se tiene que

(**) $\mathcal{M} \models_{P/PML} \psi[\nu]$ siempre que
$\left\langle \nu(\vec{z}), \nu'(\vec{y}) \right\rangle \in T^{\mathcal{M}}, \nu'(z) = \nu(z)$ con $z \notin \vec{y}$ implica $\mathcal{M} \models_{P/PML} \beta[\nu']$.

Supóngase ahora que $\mathcal{M} \models_{P/PML} \alpha[\nu]$ y que $\left\langle \nu(\vec{x}), \nu'(\vec{z}) \right\rangle \in S^{\mathcal{M}}, \nu'(z) = \nu(z)$ con $z \notin \vec{z}$. Luego por lógica y * se tiene que

$$\left\langle \nu'(\vec{z}), \nu''(\vec{y}) \right\rangle \in T^{\mathcal{M}}, \nu''(z) = \nu'(z) \text{ con } z \notin \vec{y} \text{ implica } \mathcal{M} \models_{P/PML} \beta[\nu'']$$

siendo $v''$ una valuación de las variables individuales. Luego por lógica y ** se tiene que $\mathcal{M} \models_{P/PML} \psi[\nu']$. Así, por lógica y definición se llega a $\mathcal{M} \models_{P/PML} \alpha \Rightarrow \left[\vec{x}\ {}_{\mathsf{l}(S)} S^{\mathsf{u}(S)}\ \vec{z}\right] \psi$ y de allí que $W \models \{\alpha\}\ \vec{x}\ {}_{\mathsf{l}(S)} S^{\mathsf{u}(S)}\ \vec{z}\ \{\psi\}$. Además, de un párrafo anterior se deduce, por lógica y definición, que $W \models \{\psi\}\ \vec{z}\ {}_{\mathsf{l}(T)} T^{\mathsf{u}(T)}\ \vec{y}\ \{\beta\}$. Así, por hipótesis inductiva, se tiene que $W \vdash \{\alpha\}\ \vec{x}\ {}_{\mathsf{l}(S)} S^{\mathsf{u}(S)}\ \vec{z}\ \{\psi\}$ y $W \vdash \{\psi\}\ \vec{z}\ {}_{\mathsf{l}(T)} T^{\mathsf{u}(T)}\ \vec{y}\ \{\beta\}$. Finalmente, se tiene que la deducción

| | | |
|---|---|---|
| (1) | $\{\alpha\}\ \vec{x}\ {}_{\mathsf{l}(S)} S^{\mathsf{u}(S)}\ \vec{z}\ \{\psi\}$ | (Hipótesis) |
| (2) | $\{\psi\}\ \vec{z}\ {}_{\mathsf{l}(T)} T^{\mathsf{u}(T)}\ \vec{y}\ \{\beta\}$ | (Hipótesis) |
| (3) | $\{\alpha\}\ \vec{x}\ {}_{\mathsf{l}(S)} S;T^{\mathsf{u}(S)+\mathsf{u}(T)}\ \vec{y}\ \{\beta\}$ | ($SEC$ 1,2) |
| (4) | $\alpha \Rightarrow l \leq \mathsf{l}(S)$ | (Hipótesis) |
| (5) | $\alpha \Rightarrow \mathsf{u}(S) + \mathsf{u}(T) \leq u$ | (Hipótesis) |
| (6) | $\{\alpha\}\ \vec{x}\ {}_{l} S;T^{u}\ \vec{y}\ \{\beta\}$ | ($TIME$ 3,4,5) |

es una deducción para $h$ desde $W$. Por lo tanto $W \vdash h$.

Caso 2: $R \equiv S+T$. Sean $\nu, \nu'$ valuaciones de las variables individuales. Luego

$W \models h$ sii $\models_{\mathcal{M}} h$ para todo modelo $\mathcal{M}$ de $W$ (Definición)

sii $\mathcal{M} \models_{P/PML} \alpha \Rightarrow \left[\vec{x}\ {}_{l} S+T^{u}\ \vec{y}\right] \beta[\nu]$ (Def. 2.2.2)

sii $\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces $\mathsf{l}(S+T) \geq l_{\nu}^{\mathcal{M}}, \mathsf{u}(S+T) \leq u_{\nu}^{\mathcal{M}}$ y
$\nu(\vec{x}\ S+T\ \vec{y})\nu'$ implica $\mathcal{M} \models_{P/PML} \beta[\nu']$ (Definición)

sii $\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces
$min\{\mathsf{l}(S), \mathsf{l}(T)\} \geq l_{\nu}^{\mathcal{M}}, max\{\mathsf{u}(S), \mathsf{u}(T)\} \leq u_{\nu}^{\mathcal{M}}$ y
$\left\langle \nu(\vec{x}), \nu'(\vec{y}) \right\rangle \in (S+T)^{\mathcal{M}}, \nu(z) = \nu'(z)$ con $z \notin \vec{y}$
implica $\mathcal{M} \models_{P/PML} \beta[\nu']$. (Definición)

Así, se tiene por un lado que

$\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces $min\{\mathsf{l}(S), \mathsf{l}(T)\} \geq l_\nu^{\mathcal{M}}$ y $max\{\mathsf{u}(S), \mathsf{u}(T)\} \leq u_\nu^{\mathcal{M}}$
sii $W \models \alpha \Rightarrow l \leq min\{\mathsf{l}(S), \mathsf{l}(T)\}$ y $W \models \alpha \Rightarrow max\{\mathsf{u}(S), \mathsf{u}(T)\} \leq u$ (Lógica)
ent. $\{\alpha \Rightarrow l \leq min\{\mathsf{l}(S), \mathsf{l}(T)\}, \alpha \Rightarrow max\{\mathsf{u}(S), \mathsf{u}(T)\} \leq u\} \subseteq Th(\mathcal{A})$ (Def. y Lóg.)
ent. $W \vdash \alpha \Rightarrow l \leq min\{\mathsf{l}(S), \mathsf{l}(T)\}$ y $W \vdash \alpha \Rightarrow max\{\mathsf{u}(S), \mathsf{u}(T)\} \leq u$ (Definición)

y por otro lado que

$\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces
$\left\langle \nu(\vec{x}), \nu'(\vec{y}) \right\rangle \in S^{\mathcal{M}}$ ó $\left\langle \nu(\vec{x}), \nu'(\vec{y}) \right\rangle \in T^{\mathcal{M}}, \nu'(z) = \nu(z)$ con $z \notin \vec{y}$
implica $\mathcal{M} \models_{P/PML} \beta[\nu']$.

De aquí, por lógica, se tiene que

(1) $\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces
$\left\langle \nu(\vec{x}), \nu'(\vec{y}) \right\rangle \in S^{\mathcal{M}}, \nu'(z) = \nu(z)$ con $z \notin \vec{y}$ implica $\mathcal{M} \models_{P/PML} \beta[\nu']$

y

(2) $\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces
$\left\langle \nu(\vec{x}), \nu'(\vec{y}) \right\rangle \in T^{\mathcal{M}}, \nu'(z) = \nu(z)$ con $z \notin \vec{y}$ implica $\mathcal{M} \models_{P/PML} \beta[\nu']$.

Así, desde 1 y 2 por definición y lógica se llega a $\mathcal{M} \models_{P/PML} \alpha \Rightarrow \left[\vec{x}\ {}_{\mathsf{l}(S)} S^{\mathsf{u}(S)}\ \vec{y}\right] \beta$ y $\mathcal{M} \models_{P/PML} \alpha \Rightarrow \left[\vec{x}\ {}_{\mathsf{l}(T)} T^{\mathsf{u}(T)}\ \vec{y}\right] \beta$, y de allí a $W \models \{\alpha\}\ \vec{x}\ {}_{\mathsf{l}(S)} S^{\mathsf{u}(S)}\ \vec{y}\ \{\beta\}$ y $W \models \{\alpha\}\ \vec{x}\ {}_{\mathsf{l}(T)} T^{\mathsf{u}(T)}\ \vec{y}\ \{\beta\}$. Luego, por hipótesis inductiva, se tiene que $W \vdash \{\alpha\}\ \vec{x}\ {}_{\mathsf{l}(S)} S^{\mathsf{u}(S)}\ \vec{y}\ \{\beta\}$ y $W \vdash \{\alpha\}\ \vec{x}\ {}_{\mathsf{l}(T)} T^{\mathsf{u}(T)}\ \vec{y}\ \{\beta\}$. Finalmente, se tiene que la deducción

(1) $\{\alpha\}\ \vec{x}\ {}_{\mathsf{l}(S)} S^{\mathsf{u}(S)}\ \vec{y}\ \{\beta\}$ (Hipótesis)
(2) $\{\alpha\}\ \vec{x}\ {}_{\mathsf{l}(T)} T^{\mathsf{u}(T)}\ \vec{y}\ \{\beta\}$ (Hipótesis)
(3) $\{\alpha\}\ \vec{x}\ {}_{min\{\mathsf{l}(S),\mathsf{l}(T)\}} S{+}T^{max\{\mathsf{u}(S),\mathsf{u}(T)\}}\ \vec{y}\ \{\beta\}$ ($CHC$ 1,2)
(4) $\alpha \Rightarrow l \leq min\{\mathsf{l}(S), \mathsf{l}(T)\}$ (Hipótesis)
(5) $\alpha \Rightarrow max\{\mathsf{u}(S), \mathsf{u}(T)\} \leq u$ (Hipótesis)
(6) $\{\alpha\}\ \vec{x}\ {}_{l} S{+}T^{u}\ \vec{y}\ \{\beta\}$ ($TIME$ 3,4,5)

es una deducción para $h$ desde $W$. Por lo tanto $W \vdash h$.

Caso 3: $R \equiv S{\cdot}T$. Sean $\nu, \nu'$ valuaciones de las variables individuales. Luego

$$
\begin{array}{ll}
W \models h \text{ sii } \models_{\mathcal{M}} h \text{ para todo modelo } \mathcal{M} \text{ de } W & \text{(Definición)} \\
\quad \text{sii } \mathcal{M} \models_{P/PML} \alpha \Rightarrow \left[\vec{x}\ {}_{l} S{\cdot}T^{u}\ \vec{y}\right]\beta[\nu] & \text{(Def. 2.2.2)} \\
\quad \text{sii } \mathcal{M} \models_{P/PML} \alpha[\nu] \text{ entonces } \mathsf{l}(S{\cdot}T) \geq l_{\nu}^{\mathcal{M}}, \mathsf{u}(S{\cdot}T) \leq u_{\nu}^{\mathcal{M}} \text{ y} & \\
\qquad \nu(\vec{x}\ S{\cdot}T\ \vec{y})\nu' \text{ implica } \mathcal{M} \models_{P/PML} \beta[\nu'] & \text{(Definición)} \\
\quad \text{sii } \mathcal{M} \models_{P/PML} \alpha[\nu] \text{ entonces} & \\
\qquad max\{\mathsf{l}(S), \mathsf{l}(T)\} \geq l_{\nu}^{\mathcal{M}}, max\{\mathsf{u}(S), \mathsf{u}(T)\} \leq u_{\nu}^{\mathcal{M}} \text{ y} & \\
\qquad\quad \left\langle \nu(\vec{x}), \nu'(\vec{y}) \right\rangle \in (S{\cdot}T)^{\mathcal{M}}, \nu(z) = \nu'(z) \text{ con } z \notin \vec{y} & \\
\qquad\quad\quad \text{implica } \mathcal{M} \models_{P/PML} \beta[\nu']. & \text{(Definición)}
\end{array}
$$

Así, se tiene por un lado que

$$
\begin{array}{ll}
\mathcal{M} \models_{P/PML} \alpha[\nu] \text{ entonces } max\{\mathsf{l}(S), \mathsf{l}(T)\} \geq l_{\nu}^{\mathcal{M}} \text{ y } max\{\mathsf{u}(S), \mathsf{u}(T)\} \leq u_{\nu}^{\mathcal{M}} & \\
\quad \text{sii } W \models \alpha \Rightarrow l \leq max\{\mathsf{l}(S), \mathsf{l}(T)\} \text{ y } W \models \alpha \Rightarrow max\{\mathsf{u}(S), \mathsf{u}(T)\} \leq u & \text{(Lógica)} \\
\quad \text{ent. } \{\alpha \Rightarrow l \leq max\{\mathsf{l}(S), \mathsf{l}(T)\}, \alpha \Rightarrow max\{\mathsf{u}(S), \mathsf{u}(T)\} \leq u\} \subseteq Th(\mathcal{A}) & \text{(Def. y Lóg.)} \\
\quad \text{ent. } W \vdash \alpha \Rightarrow l \leq max\{\mathsf{l}(S), \mathsf{l}(T)\} \text{ y } W \vdash \alpha \Rightarrow max\{\mathsf{u}(S), \mathsf{u}(T)\} \leq u & \text{(Definición)}
\end{array}
$$

y por otro lado que

$$
\begin{array}{l}
\mathcal{M} \models_{P/PML} \alpha[\nu] \text{ entonces} \\
\quad \left\langle \nu(\vec{x}), \nu'(\vec{y}) \right\rangle \in S^{\mathcal{M}} \text{ y } \left\langle \nu(\vec{x}), \nu'(\vec{y}) \right\rangle \in T^{\mathcal{M}}, \nu'(z) = \nu(z) \text{ con } z \notin \vec{y} \\
\qquad \text{implica } \mathcal{M} \models_{P/PML} \beta[\nu'].
\end{array}
$$

De aquí, por lógica, se tiene que

(1) $\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces
$\left\langle \nu(\vec{x}), \nu'(\vec{y}) \right\rangle \in S^{\mathcal{M}}, \nu'(z) = \nu(z) \text{ con } z \notin \vec{y}$ implica $\mathcal{M} \models_{P/PML} \beta[\nu']$

ó bien

(2) $\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces
$\left\langle \nu(\vec{x}), \nu'(\vec{y}) \right\rangle \in T^{\mathcal{M}}, \nu'(z) = \nu(z) \text{ con } z \notin \vec{y}$ implica $\mathcal{M} \models_{P/PML} \beta[\nu']$.

Así, desde 1 y 2 por definición y lógica se llega a $\mathcal{M} \models_{P/PML} \alpha \Rightarrow \left[\vec{x}\ {}_{\mathsf{l}(S)} S^{\mathsf{u}(S)}\ \vec{y}\right]\beta$ ó $\mathcal{M} \models_{P/PML} \alpha \Rightarrow \left[\vec{x}\ {}_{\mathsf{l}(T)} T^{\mathsf{u}(T)}\ \vec{y}\right]\beta$, y de allí a $W \models \{\alpha\}\ \vec{x}\ {}_{\mathsf{l}(S)} S^{\mathsf{u}(S)}\ \vec{y}\ \{\beta\}$ ó $W \models \{\alpha\}\ \vec{x}\ {}_{\mathsf{l}(T)} T^{\mathsf{u}(T)}\ \vec{y}\ \{\beta\}$. Supóngase que $W \models \{\alpha\}\ \vec{x}\ {}_{\mathsf{l}(S)} S^{\mathsf{u}(S)}\ \vec{y}\ \{\beta\}$. Es cierto que $W \models \{\alpha\}\ \vec{x}\ {}_{\mathsf{l}(T)} T^{\mathsf{u}(T)}\ \vec{y}\ \{true\}$. Luego, por hipótesis inductiva, se tiene que

$W \vdash \{\alpha\}\ \vec{x}\ {}_{\mathsf{l}(S)}S^{\mathsf{u}(S)}\ \vec{y}\ \{\beta\}$ y $W \vdash \{\alpha\}\ \vec{x}\ {}_{\mathsf{l}(T)}T^{\mathsf{u}(T)}\ \vec{y}\ \{true\}$. Así, se tiene que la deducción

| | | |
|---|---|---|
| (1) | $\{\alpha\}\ \vec{x}\ {}_{\mathsf{l}(S)}S^{\mathsf{u}(S)}\ \vec{y}\ \{\beta\}$ | (Hipótesis) |
| (2) | $\{\alpha\}\ \vec{x}\ {}_{\mathsf{l}(T)}T^{\mathsf{u}(T)}\ \vec{y}\ \{true\}$ | (Hipótesis) |
| (3) | $\{\alpha\}\ \vec{x}\ {}_{max\{\mathsf{l}(S),\mathsf{l}(T)\}}S{\cdot}T^{max\{\mathsf{u}(S),\mathsf{u}(T)\}}\ \vec{y}\ \{\beta \wedge true\}$ | ($PAR$ 1,2) |
| (4) | $\beta \wedge true \Rightarrow \beta$ | (Lógica) |
| (5) | $\{\alpha\}\ \vec{x}\ {}_{max\{\mathsf{l}(S),\mathsf{l}(T)\}}S{\cdot}T^{max\{\mathsf{u}(S),\mathsf{u}(T)\}}\ \vec{y}\ \{\beta\}$ | ($CONS$ 3,4) |
| (6) | $\alpha \Rightarrow l \leq max\{\mathsf{l}(S),\mathsf{l}(T)\}$ | (Hipótesis) |
| (7) | $\alpha \Rightarrow max\{\mathsf{u}(S),\mathsf{u}(T)\} \leq u$ | (Hipótesis) |
| (8) | $\{\alpha\}\ \vec{x}\ {}_{l}S{\cdot}T^{u}\ \vec{y}\ \{\beta\}$ | ($TIME$ 5,6,7) |

es una deducción para $h$ desde $W$. Similarmente se prueba en el caso de que $W \models \{\alpha\}\ \vec{x}\ {}_{\mathsf{l}(T)}T^{\mathsf{u}(T)}\ \vec{y}\ \{\beta\}$. Por lo tanto $W \vdash h$.

Caso 4: $R \equiv S^*$. Sean $\nu, \nu'$ valuaciones de las variables individuales. Luego

| | |
|---|---|
| $W \models h$ sii $\models_{\mathcal{M}} h$ para todo modelo $\mathcal{M}$ de $W$ | (Definición) |
| sii $\mathcal{M} \models_{P/PML} \alpha \Rightarrow \left[\vec{x}\ {}_{l}S^{*\,u}\ \vec{y}\right]\beta[\nu]$ | (Def. 2.2.2) |
| sii $\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces $\mathsf{l}(S^*) \geq l_\nu^{\mathcal{M}}, \mathsf{u}(S^*) \leq u_\nu^{\mathcal{M}}$ y $\nu(\vec{x}\ S^*\ \vec{y})\nu'$ implica $\mathcal{M} \models_{P/PML} \beta[\nu']$ | (Definición) |
| sii $\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces $0 \geq l_\nu^{\mathcal{M}}, \infty \leq u_\nu^{\mathcal{M}}$ y $\left\langle \nu(\vec{x}), \nu'(\vec{y}) \right\rangle \in (S^*)^{\mathcal{M}}, \nu(z) = \nu'(z)$ con $z \notin \vec{y}$ implica $\mathcal{M} \models_{P/PML} \beta[\nu']$. | (Definición) |

Así, se tiene por un lado que

| | |
|---|---|
| $\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces $0 \geq l_\nu^{\mathcal{M}}$ y $\infty \leq u_\nu^{\mathcal{M}}$ | |
| sii $W \models \alpha \Rightarrow l \leq 0$ y $W \models \alpha \Rightarrow \infty \leq u$ | (Lógica) |
| ent. $\{\alpha \Rightarrow l \leq 0, \alpha \Rightarrow \infty \leq u\} \subseteq Th(\mathcal{A})$ | (Def. y Lóg.) |
| ent. $W \vdash \alpha \Rightarrow l \leq 0$ y $W \vdash \alpha \Rightarrow \infty \leq u$ | (Definición) |

y por otro lado, aplicando lógica y definición, que

$\mathcal{M} \models_{P/PML} \alpha[\nu]$ entonces
$\left\langle \nu(\vec{x}), \nu'(\vec{y}) \right\rangle \in (S^i)^{\mathcal{M}}, \nu'(z) = \nu(z)$ con $z \notin \vec{y}$ implica $\mathcal{M} \models_{P/PML} \beta[\nu']$

para $i < \omega$. Así, nuevamente por definición y lógica se llega a $\mathcal{M} \models_{P/PML} \alpha \Rightarrow \left[\vec{x}\ {}_{\mathsf{l}(S^i)}S^{i\,\mathsf{u}(S^i)}\ \vec{y}\right]\beta$ para $i < \omega$ y de allí a $W \models \{\alpha\}\ \vec{x}\ {}_{\mathsf{l}(S^i)}S^{i\,\mathsf{u}(S^i)}\ \vec{y}\ \{\beta\}$. Luego,

por lo demostrado en el caso 1, se tiene que $W \vdash \{\alpha\} \stackrel{\rightarrow}{x}_{\mid(S^i)} S^{i\,\mathsf{u}(S^i)} \stackrel{\rightarrow}{y} \{\beta\}$. Finalmente, se tiene que la deducción

| | | |
|---|---|---|
| (1) | $\{\alpha\} \stackrel{\rightarrow}{x}_{\mid(S^i)} S^{i\,\mathsf{u}(S^i)} \stackrel{\rightarrow}{y} \{\beta\},\ i < \omega$ | (Hipótesis) |
| (2) | $\{\alpha\} \stackrel{\rightarrow}{x}_{0} S^{*\,\infty} \stackrel{\rightarrow}{y} \{\beta\}$ | $(ITE\ 1)$ |
| (3) | $\alpha \Rightarrow l \leq 0$ | (Hipótesis) |
| (4) | $\alpha \Rightarrow \infty \leq u$ | (Hipótesis) |
| (5) | $\{\alpha\} \stackrel{\rightarrow}{x}_{l} S^{*\,u} \stackrel{\rightarrow}{y} \{\beta\}$ | $(TIME\ 2,3,4)$ |

es una deducción para $h$ desde $W$. Por lo tanto $W \vdash h$.

■

Se ha visto en esta última sección que existe un cálculo consistente y completo para el conjunto de fórmulas de Hoare que son consecuencia lógica del conjunto $Th(\mathcal{A}) \cup HTh(\mathcal{A})$ donde $\mathcal{A}$ es una estructura de objeto expresiva. Hasta aquí, la aplicación del cálculo de Hoare a una teoría dada consiste en considerar las derivaciones en el cálculo a partir de esta teoría. Sin embargo, es interesante notar que existe una forma alternativa de aplicar el cálculo de Hoare cuando la teoría $HTh(\mathcal{A})$ es *axiomatizable*. Una teoría $HTh(\mathcal{A})$ se dice que es axiomatizable cuando existe un conjunto decidible $W \subseteq HFor(\mathcal{S})$ tal que $HTh(\mathcal{A})$ es el conjunto de todas las fórmulas de Hoare derivables desde $Th(\mathcal{A}) \cup W$ en el cálculo de Hoare. En tal caso, el cálculo de Hoare se aumenta con los axiomas de la teoría (es decir, $W$). Las derivaciones de interés son entonces las derivaciones en este cálculo extendido a partir de $Th(\mathcal{A})$. Esta visión alternativa no fue adoptada aquí porque sólo es aplicable a teorías axiomatizables (sin embargo en los ejemplos prácticos se usará, ya que las teorías involucradas serán axiomatizables).

EJEMPLO 2.4.1 Considérese la interpretación usual $\mathcal{I}$ de la aritmética de Peano, donde además se incluye una única acción atómica $Inc$ tal que $Inc^{\mathcal{I}} = \{\langle n, n+1\rangle : n \in \mathsf{Nat}\}$ con $l_{Inc} = 0$ y $u_{Inc} = 1$. Luego, la teoría $HTh(\mathcal{I})$ es axiomatizable con el esquema de axioma $\{\alpha[x+1/x]\}\langle x\rangle_0 Inc^1 \langle x\rangle \{\alpha\}$. Así, por ejemplo se tiene que la fórmula de Hoare

$$\{y = 0\}\langle y\rangle_0 Inc; Inc^3 \langle z\rangle \{z + 1 = 3\}$$

es derivable desde $Th(\mathcal{I})$ en el cálculo extendido según la siguiente deducción:

| | | |
|---|---|---|
| (1) | $\{x+1+1=3\}\langle x\rangle_0 Inc^1 \langle x\rangle \{x+1=3\}$ | (Axioma) |
| (2) | $\{x+1+1+1=3\}\langle x\rangle_0 Inc^1 \langle x\rangle \{x+1+1=3\}$ | (Axioma) |
| (3) | $\{x+1+1+1=3\}\langle x\rangle_0 Inc; Inc^{1+1} \langle x\rangle \{x+1=3\}$ | $(SEC\ 1,2)$ |
| (4) | $x = 0 \Rightarrow x+1+1+1=3$ | $(Th(\mathcal{I}))$ |
| (5) | $\{x=0\}\langle x\rangle_0 Inc; Inc^{1+1} \langle x\rangle \{x+1=3\}$ | $(CONS\ 3,4)$ |
| (6) | $x = 0 \Rightarrow 1+1 \leq 3$ | $(Th(\mathcal{I}))$ |
| (7) | $\{x=0\}\langle x\rangle_0 Inc; Inc^3 \langle x\rangle \{x+1=3\}$ | $(TIME\ 5,6)$ |
| (8) | $\{y=0\}\langle y\rangle_0 Inc; Inc^3 \langle z\rangle \{z+1=3\}$ | $(VAR\ 7)$ |

■

Por otro lado, y por razones de generalidad, no se ha asumido que la teoría $Th(\mathcal{A})$ es axiomatizable (por ejemplo, es conocido que la aritmética de Peano no es axiomatizable en el cálculo de predicados de primer orden). En caso de serlo, el cálculo de Hoare se aumenta con los axiomas y reglas de deducción del cálculo de la lógica multisort y con los axiomas de $Th(\mathcal{A})$. Las derivaciones de interés son entonces las derivaciones en este cálculo extendido a partir del conjunto vacío.

## 2.5 Otras reglas derivadas

En esta sección se presentarán reglas derivadas para cierta clase especial de procesos similares a los comandos guardados de Dijkstra [7], que pueden ser útiles en la práctica. Estos procesos se definen a partir de los procesos prmitivos de $P/PML$ de la siguiente forma:

$$\begin{array}{ll}
\textbf{if } []i \bullet \gamma_i \to S_i \textbf{ fi} & \equiv_{def} \ \gamma_1?;S_1 + \ldots + \gamma_n?;S_n \\
\textbf{do } []i \bullet \gamma_i \to S_i \textbf{ od} & \equiv_{def} \ (\textbf{if } []i \bullet \gamma_i \to S_i \textbf{ fi})^*;\neg\gamma_1?;\ldots;\neg\gamma_n? \\
\textbf{if } \gamma \textbf{ then } S \textbf{ else } T & \equiv_{def} \textbf{ if } \gamma \to S \ [] \ \neg\gamma \to T \textbf{ fi} \\
\textbf{while } \gamma \textbf{ do } S & \equiv_{def} \textbf{ do } \gamma \to S \textbf{ od}
\end{array}$$

A partir de esta definición, se obtienen las siguientes reglas derivadas para las dos primeros tipos de procesos:

(iii') *Regla IF*: Siendo $\vec{z_i}$ las variables libres de $\gamma_i$

$$\frac{\{\gamma_i[\vec{x}/\vec{z_i}] \wedge \alpha\} \ \vec{x} \ {}_{l_i} S_i{}^{u_i} \ \vec{y} \ \{\beta\}, \ i = 1..n}{\{\alpha\} \ \vec{x} \ {}_{\epsilon}\textbf{if } []i \bullet \gamma_i \to S_i \textbf{ fi}^{\epsilon + max_i\{u_i\}} \ \vec{y} \ \{\beta\}}$$

(iv') *Regla DO*: Siendo $\vec{z_i}$ las variables libres de $\gamma_i$

$$\frac{\{\gamma_i[\vec{x}/\vec{z_i}] \wedge \psi \wedge t = t_0\} \ \vec{x} \ {}_{l_i} S_i{}^{u_i} \ \vec{x} \ \{\psi \wedge t < t_0\}, \ i = 1..n}{\{\psi\} \ \vec{x} \ {}_{\epsilon}\textbf{do } []i \bullet \gamma_i \to S_i \textbf{ od}^{t * max_i\{u_i\}} \ \vec{x} \ \{\neg(\bigvee_i \gamma_i[\vec{x}/\vec{z_i}]) \wedge \psi\}}$$

La regla derivada $IF$ resulta de la siguiente deducción (a partir de sus premisas y de una teoría arbitraria):

| | | |
|---|---|---|
| (1) | $\{\gamma_i[\vec{x}/\vec{z_i}] \wedge \alpha\} \ \vec{x} \ {}_{l_i} S_i{}^{u_i} \ \vec{y} \ \{\beta\}, \ i = 1..n$ | (Hipótesis) |
| (2) | $\{\gamma_i[\vec{x}/\vec{z_i}] \Rightarrow \gamma_i[\vec{x}/\vec{z_i}] \wedge \alpha\} \ \vec{x} \ {}_{\epsilon}\gamma_i?^{\epsilon} \ \vec{x} \ \{\gamma_i[\vec{x}/\vec{z_i}] \wedge \alpha\}, \ i = 1..n$ | $(TEST)$ |
| (3) | $\alpha \Rightarrow \Big(\gamma_i[\vec{x}/\vec{z_i}] \Rightarrow \gamma_i[\vec{x}/\vec{z_i}] \wedge \alpha\Big)$ | (Lógica) |
| (4) | $\{\alpha\} \ \vec{x} \ {}_{\epsilon}\gamma_i?^{\epsilon} \ \vec{x} \ \{\gamma_i[\vec{x}/\vec{z_i}] \wedge \alpha\}, \ i = 1..n$ | $(CONS$ 2,3) |
| (5) | $\{\alpha\} \ \vec{x} \ {}_{\epsilon}\gamma_i?;S_i{}^{\epsilon+u_i} \ \vec{y} \ \{\beta\}, \ i = 1..n$ | $(SEC$ 1,4) |
| (6) | $\alpha \Rightarrow \epsilon \leq min\{\epsilon, \ldots, \epsilon\}$ | (Aritmética) |

(7) $\alpha \Rightarrow max_i\{\epsilon + u_i\} \leq \epsilon + max_i\{u_i\}$ (Aritmética)

(8) $\{\alpha\}\ \vec{x}\ _{\epsilon}\mathbf{if}\ []i \bullet \gamma_i \rightarrow S_i\ \mathbf{fi}^{\epsilon + max_i\{u_i\}}\ \vec{y}\ \{\beta\}$ ($CHC'$ 5,6,7)

Para probar que la regla $DO$ es derivada, se usará el siguiente lema:

LEMA 2.5.1 *La fórmula de Hoare*

$$\{\psi\}\ \vec{x}\ _0(\mathbf{if}\ []i \bullet \gamma_i \rightarrow S_i\ \mathbf{fi})^{k\ \infty}\ \vec{x}\ \{\psi\},\ k \geq 0$$

*es derivable a partir de las fórmulas de Hoare* $\{\gamma_i[\vec{x}/\vec{z_i}] \wedge \psi \wedge t = t_0\}\ \vec{x}\ _{l_i} S_i^{\ u_i}\ \vec{x}\ \{\psi \wedge t < t_0\},\ i = 1..n$ *y de una teoría arbitraria.*

*Prueba.* Ver Apéndice A. ■

La regla derivada $DO$ resulta entonces de la siguiente deducción (a partir de sus premisas y de una teoría arbitraria): Siendo $\varphi$ la fórmula $\neg(\bigvee_i \gamma_i[\vec{x}/\vec{z_i}]) \wedge \psi$,

(1) $\{\neg\gamma_n[\vec{x}/\vec{z_n}] \Rightarrow \varphi\}\ \vec{x}\ _{\epsilon}\neg\gamma_n?^{\epsilon}\ \vec{x}\ \{\varphi\}$ ($TEST$)

...

($n$) $\{\neg\gamma_1[\vec{x}/\vec{z_1}] \Rightarrow (\neg\gamma_2[\vec{x}/\vec{z_2}] \Rightarrow (\ldots\varphi))\}\ \vec{x}\ _{\epsilon}\neg\gamma_1?^{\epsilon}\ \vec{x}\ \{\neg\gamma_2[\vec{x}/\vec{z_2}] \Rightarrow (\ldots\varphi)\}$ ($TEST$)

(a) $\{\neg\gamma_1[\vec{x}/\vec{z_1}] \Rightarrow (\neg\gamma_2[\vec{x}/\vec{z_2}] \Rightarrow (\ldots\varphi))\}\ \vec{x}\ _{\epsilon}\neg\gamma_1?;\ldots;\neg\gamma_n?^{\epsilon+\cdots+\epsilon}\ \vec{x}\ \{\varphi\}$ ($SEC$ $1,\ldots,n$)

(b) $\psi \Rightarrow (\neg\gamma_1[\vec{x}/\vec{z_1}] \Rightarrow (\neg\gamma_2[\vec{x}/\vec{z_2}] \Rightarrow (\ldots\varphi)))$ (Lógica)

(c) $\{\psi\}\ \vec{x}\ _{\epsilon}\neg\gamma_1?;\ldots;\neg\gamma_n?^{\epsilon+\cdots+\epsilon}\ \vec{x}\ \{\varphi\}$ ($CONS$ a,b)

(d) $\{\gamma_i[\vec{x}/\vec{z_i}] \wedge \psi \wedge t = t_0\}\ \vec{x}\ _{l_i} S_i^{\ u_i}\ \vec{x}\ \{\psi \wedge t < t_0\},\ i = 1..n$ (Hipótesis)

(e) $\{\psi\}\ \vec{x}\ _0(\mathbf{if}\ []i \bullet \gamma_i \rightarrow S_i\ \mathbf{fi})^{k\ \infty}\ \vec{x}\ \{\psi\},\ k \geq 0$ (Lem. 2.5.1)

(f) $\{\psi\}\ \vec{x}\ _0(\mathbf{if}\ []i \bullet \gamma_i \rightarrow S_i\ \mathbf{fi})^{*\ \infty}\ \vec{x}\ \{\psi\}$ ($ITE$ e)

(g) $\{\psi\}\ \vec{x}\ _0\mathbf{do}\ []i \bullet \gamma_i \rightarrow S_i\ \mathbf{od}^{\infty+\epsilon+\cdots+\epsilon}\ \vec{x}\ \{\varphi\}$ ($SEC$ c,f)

Nótese que las cotas de tiempo en la regla $DO$ no pueden derivarse, sino que se asumen como válidas. A partir de estas reglas pueden obtenerse inmediatamente reglas para los dos últimos tipos de procesos, ya que son casos especiales de las reglas $IF$ y $DO$.

(v') *Regla IFT*: Siendo $\vec{z}$ las variables libres de $\gamma$

$$\frac{\{\gamma[\vec{x}/\vec{z}] \wedge \alpha\}\ \vec{x}\ _l S^u\ \vec{y}\ \{\beta\} \qquad \{\neg\gamma[\vec{x}/\vec{z}] \wedge \alpha\}\ \vec{x}\ _v T^w\ \vec{y}\ \{\beta\}}{\{\alpha\}\ \vec{x}\ _{\epsilon}\mathbf{if}\ \gamma\ \mathbf{then}\ S\ \mathbf{else}\ T^{\epsilon + max\{u,w\}}\ \vec{y}\ \{\beta\}}$$

(vi') *Regla WD*: Siendo $\vec{z}$ las variables libres de $\gamma$

$$\frac{\{\gamma[\vec{x}/\vec{z}] \wedge \psi \wedge t = t_0\}\ \vec{x}\ _l S^u\ \vec{x}\ \{\psi \wedge t < t_0\}}{\{\psi\}\ \vec{x}\ _{\epsilon}\mathbf{while}\ \gamma\ \mathbf{do}\ S^{t*u}\ \vec{x}\ \{\neg\gamma[\vec{x}/\vec{z}] \wedge \psi\}}$$

## 2.6 Ejemplos

En esta sección se darán algunos ejemplos de pruebas de corrección parcial de procesos en $P/PML$ utilizando el cálculo de Hoare presentado en las secciones anteriores. Para los ejemplos, se asumirá la existencia de una estructura de objeto $\mathcal{A}$ (sobre una signatura $\mathcal{S}$ adecuada) que contiene sólo las siguientes acciones atómicas:

- *Inc* (que toma como entrada un número entero y lo retorna incrementado en 1, con $\mathsf{l}(Inc) = 0$ y $\mathsf{u}(Inc) = 1$).
- *Dec* (que toma como entrada un número entero positivo y lo retorna decrementado en 1, con $\mathsf{l}(Dec) = 0$ y $\mathsf{u}(Dec) = 1$).
- *Neg* (que toma como entrada un número entero y lo retorna negado, con $\mathsf{l}(Neg) = \epsilon$ y $\mathsf{u}(Neg) = 2 * \epsilon$).
- *Decby*2 (que toma como entrada un número entero y lo retorna decrementado en 2, con $\mathsf{l}(Decby2) = 0$ y $\mathsf{u}(Decby2) = 2$.)
- *Join* (que toma como entrada un par de números enteros y retorna uno de ellos, con $\mathsf{l}(Join) = 0$ y $\mathsf{u}(Join) = 0$).
- *Sum* (que toma como entrada un par de números enteros y retorna la suma de ellos, con $\mathsf{l}(Sum) = 0$ y $\mathsf{u}(Sum) = 2$).
- *Swap* (que toma como entrada un par de números enteros y los intercambia, con $\mathsf{l}(Swap) = 1$ y $\mathsf{u}(Swap) = 4$).
- $Zerofst$ (que toma como entrada un par de números enteros y setea en 0 la primer componente, con $\mathsf{l}(Zerofst) = 0$ y $\mathsf{u}(Zerofst) = 2$).
- $Zerosnd$ (que toma como entrada un par de números enteros y setea en 0 la segunda componente, con $\mathsf{l}(Zerosnd) = 1$ y $\mathsf{u}(Zerosnd) = 3$).
- $Decfst$ (que toma como entrada un par de números enteros y decrementa en 1 la primer componente, con $\mathsf{l}(Decfst) = 0$ y $\mathsf{u}(Decfst) = 2$).
- *Decsnd* (que toma como entrada un par de números enteros y decrementa en 1 la segunda componente, con $\mathsf{l}(Decsnd) = 0$ y $\mathsf{u}(Decsnd) = 3$).
- *Flip* (que arroja una moneda y retorna la cadena "hd" ó "tl", con $\mathsf{l}(Flip) = 2$ y $\mathsf{u}(Flip) = 3$).

En este caso particular, la teoría $HTh(\mathcal{A})$ es axiomatizable con los siguientes esquemas de axioma: Siendo $\alpha \in For(\mathcal{S})$, $x, y, z, w$ variables de sort *Int*, $c$ una variable de sort *Coin* y $s$ una variable de sort *String*,

- *Axioma Inc*:
$$\{\alpha[x + 1/y]\} \langle x \rangle_0 Inc^1 \langle y \rangle \{\alpha\}$$
- *Axioma Dec*:
$$\{\alpha[x - 1/y]\} \langle x \rangle_0 Dec^1 \langle y \rangle \{\alpha\}$$

- *Axioma Neg*:
$$\{\alpha[-x/y]\}\,\langle\, x\,\rangle_{\,\epsilon}\, Neg^{2*\epsilon}\,\langle\, y\,\rangle\,\{\alpha\}$$
- *Axioma Decby2*:
$$\{\alpha[x-2/y]\}\,\langle\, x\,\rangle_{\,0}\, Decby2^{\,2}\,\langle\, y\,\rangle\,\{\alpha\}$$
- *Axioma Join*:
$$\{\alpha[x/z]\wedge\alpha[y/z]\}\,\langle\, x,y\,\rangle_{\,0}\, Join^{\,0}\,\langle\, z\,\rangle\,\{\alpha\}$$
- *Axioma Sum*:
$$\{\alpha[x+y/z]\}\,\langle\, x,y\,\rangle_{\,0}\, Sum^{\,2}\,\langle\, z\,\rangle\,\{\alpha\}$$
- *Axioma Swap*:
$$\{\alpha[y,x/z,w]\}\,\langle\, x,y\,\rangle_{\,1}\, Swap^{\,4}\,\langle\, z,w\,\rangle\,\{\alpha\}$$
- *Axioma Zerofst*:
$$\{\alpha[0,y/z,w]\}\,\langle\, x,y\,\rangle_{\,0}\, Zerofst^{\,2}\,\langle\, z,w\,\rangle\,\{\alpha\}$$
- *Axioma Zerosnd*:
$$\{\alpha[x,0/z,w]\}\,\langle\, x,y\,\rangle_{\,1}\, Zerosnd^{\,3}\,\langle\, z,w\,\rangle\,\{\alpha\}$$
- *Axioma Decfst*:
$$\{\alpha[x-1,y/z,w]\}\,\langle\, x,y\,\rangle_{\,0}\, Decfst^{\,2}\,\langle\, z,w\,\rangle\,\{\alpha\}$$
- *Axioma Decsnd*:
$$\{\alpha[x,y-1/z,w]\}\,\langle\, x,y\,\rangle_{\,0}\, Decsnd^{\,3}\,\langle\, z,w\,\rangle\,\{\alpha\}$$
- *Axioma Flip*:
$$\{\alpha[\mathsf{hd}/s]\wedge\alpha[\mathsf{tl}/s]\}\,\langle\, c\,\rangle_{\,2}\, Flip^{\,3}\,\langle\, s\,\rangle\,\{\alpha\}$$

EJEMPLO 2.6.1 Se quiere probar que

$$Th(\mathcal{A})\vdash\{true\}\,\langle\, coin\,\rangle_{\,1}\, Flip;s=\mathsf{hd}?^{\,\epsilon+4}\,\langle\, res\,\rangle\,\{res=\mathsf{hd}\}.$$

La siguiente es una deducción de la fórmula desde $Th(\mathcal{A})$:

| | | |
|---|---|---|
| (1) | $\{res=\mathsf{hd}\Rightarrow res=\mathsf{hd}\}\,\langle\, res\,\rangle_{\,\epsilon}\, s=\mathsf{hd}?^{\,\epsilon}\,\langle\, res\,\rangle\,\{res=\mathsf{hd}\}$ | $(TEST)$ |
| (2) | $true\Rightarrow(res=\mathsf{hd}\Rightarrow res=\mathsf{hd})$ | (Lógica) |
| (3) | $\{true\}\,\langle\, res\,\rangle_{\,\epsilon}\, s=\mathsf{hd}?^{\,\epsilon}\,\langle\, res\,\rangle\,\{res=\mathsf{hd}\}$ | $(CONS$ 1,2) |
| (4) | $\{true\}\,\langle\, coin\,\rangle_{\,2}\, Flip^{\,3}\,\langle\, res\,\rangle\,\{true\}$ | $(Flip)$ |
| (5) | $\{true\}\,\langle\, coin\,\rangle_{\,2}\, Flip;s=\mathsf{hd}?^{\,3+\epsilon}\,\langle\, res\,\rangle\,\{res=\mathsf{hd}\}$ | $(SEC$ 3,4) |
| (6) | $true\Rightarrow 1\leq 2$ | (Aritmética) |
| (7) | $true\Rightarrow 3+\epsilon\leq\epsilon+4$ | (Aritmética) |
| (8) | $\{true\}\,\langle\, coin\,\rangle_{\,1}\, Flip;s=\mathsf{hd}?^{\,\epsilon+4}\,\langle\, res\,\rangle\,\{res=\mathsf{hd}\}$ | $(TIME$ 5,6,7) |

■

EJEMPLO 2.6.2 Se quiere probar que

$$Th(\mathcal{A}) \vdash \{x = 1 \wedge y = 2\} \langle x, y \rangle_1 Swap; Sum; (Inc + Dec)^7 \langle x \rangle \{even(x)\}.$$

La siguiente es una deducción de la fórmula desde $Th(\mathcal{A})$:

| | | |
|---|---|---|
| (1) | $\{even(x+1)\} \langle x \rangle_0 Inc^1 \langle x \rangle \{even(x)\}$ | $(Inc)$ |
| (2) | $\{even(x-1)\} \langle x \rangle_0 Dec^1 \langle x \rangle \{even(x)\}$ | $(Dec)$ |
| (3) | $odd(x) \Rightarrow even(x+1)$ | (Aritmética) |
| (4) | $\{odd(x)\} \langle x \rangle_0 Inc^1 \langle x \rangle \{even(x)\}$ | $(CONS$ 1,3) |
| (5) | $odd(x) \Rightarrow even(x-1)$ | (Aritmética) |
| (6) | $\{odd(x)\} \langle x \rangle_0 Dec^1 \langle x \rangle \{even(x)\}$ | $(CONS$ 2,5) |
| (7) | $\{odd(x)\} \langle x \rangle_{min\{0,0\}} Inc + Dec^{max\{1,1\}} \langle x \rangle \{even(x)\}$ | $(CHC$ 4,6) |
| (8) | $\{odd(x+y)\} \langle x, y \rangle_0 Sum^2 \langle x \rangle \{odd(x)\}$ | $(Sum)$ |
| (9) | $\{odd(x+y)\} \langle x, y \rangle_0 Sum; (Inc + Dec)^{2+max\{1,1\}} \langle x \rangle \{even(x)\}$ | $(SEC$ 7,8) |
| (10) | $\{odd(y+x)\} \langle x, y \rangle_1 Swap^4 \langle x, y \rangle \{odd(x+y)\}$ | $(Swap)$ |
| (11) | $\{odd(y+x)\} \langle x, y \rangle_1 Swap; Sum; (Inc + Dec)^{4+2+max\{1,1\}} \langle x \rangle \{even(x)\}$ | $(SEC$ 9,10) |
| (12) | $x = 1 \wedge y = 2 \Rightarrow odd(y+x)$ | (Aritmética) |
| (13) | $\{x = 1 \wedge y = 2\} \langle x, y \rangle_1 Swap; Sum; (Inc + Dec)^{4+2+max\{1,1\}} \langle x \rangle \{even(x)\}$ | $(CONS$ 11,12) |
| (14) | $x = 1 \wedge y = 2 \Rightarrow 4 + 2 + max\{1,1\} \leq 7$ | (Aritmética) |
| (15) | $\{x = 1 \wedge y = 2\} \langle x, y \rangle_1 Swap; Sum; (Inc + Dec)^7 \langle x \rangle \{even(x)\}$ | $(TIME$ 13,14) |

■

EJEMPLO 2.6.3 Se quiere probar que

$$Th(\mathcal{A}) \vdash \{true\} \langle x, y \rangle_1 (Zerofst \cdot Zerosnd); Join; Inc^{*\,\infty} \langle w \rangle \{w \geq 0\}.$$

Para ello, se usará el siguiente lema:

LEMA 2.6.1 $Th(\mathcal{A}) \vdash \{w = 0\} \langle w \rangle_0 Inc^{k\,\infty} \langle w \rangle \{w \geq 0\}$, *con* $k \geq 0$.

*Prueba.* Por inducción sobre $k$. Para $k = 0$, se tiene la siguiente deducción:

| | | |
|---|---|---|
| (1) | $w = 0 \Rightarrow 0 \leq \epsilon$ | (Aritmética) |
| (2) | $w = 0 \Rightarrow \epsilon \leq \infty$ | (Aritmética) |
| (3) | $w = 0 \Rightarrow w \geq 0$ | (Aritmética) |
| (4) | $\{w = 0\} \langle w \rangle_0 1'_{Int}{}^{\infty} \langle w \rangle \{w \geq 0\}$ | $(SKIP'$ 1,2,3) |

Supongamos que el enunciado es verdadero para $k$ con $k \geq 0$. Para $k+1$ se tiene la siguiente deducción:

| | | |
|---|---|---|
| (1) | $\{w+1 \geq 0\}\,\langle w \rangle_0\, Inc^1\, \langle w \rangle\, \{w \geq 0\}$ | $(Inc)$ |
| (2) | $w \geq 0 \Rightarrow w+1 \geq 0$ | (Aritmética) |
| (3) | $\{w \geq 0\}\,\langle w \rangle_0\, Inc^1\, \langle w \rangle\, \{w \geq 0\}$ | $(CONS$ 1,2) |
| (4) | $\{w = 0\}\,\langle w \rangle_0\, Inc^{k^\infty}\, \langle w \rangle\, \{w \geq 0\}$ | (Hipótesis Inductiva) |
| (5) | $\{w = 0\}\,\langle w \rangle_0\, Inc^{k+1^{\infty+1}}\, \langle w \rangle\, \{w \geq 0\}$ | $(SEC$ 3,4) |
| (6) | $w = 0 \Rightarrow \infty + 1 \leq \infty$ | (Aritmética) |
| (7) | $\{w = 0\}\,\langle w \rangle_0\, Inc^{k+1^\infty}\, \langle w \rangle\, \{w \geq 0\}$ | $(TIME$ 5,6) |

■

Así, la siguiente es una deducción de la fórmula desde $Th(\mathcal{A})$:

| | | |
|---|---|---|
| (1) | $\{w = 0\}\,\langle w \rangle_0\, Inc^{k^\infty}\, \langle w \rangle\, \{w \geq 0\},\ k \geq 0$ | (Lem. 2.6.1) |
| (2) | $\{w = 0\}\,\langle w \rangle_0\, Inc^{*^\infty}\, \langle w \rangle\, \{w \geq 0\}$ | $(ITE$ 1) |
| (3) | $\{x = 0 \wedge y = 0\}\,\langle x,y \rangle_0\, Join^0\, \langle w \rangle\, \{w = 0\}$ | $(Join)$ |
| (4) | $\{x = 0 \wedge y = 0\}\,\langle x,y \rangle_0\, Join; Inc^{*^{0+\infty}}\, \langle w \rangle\, \{w \geq 0\}$ | $(SEC$ 2,3) |
| (5) | $\{0 = 0\}\,\langle x,y \rangle_0\, Zerofst^2\, \langle x,y \rangle\, \{x = 0\}$ | $(Zerofst)$ |
| (6) | $\{0 = 0\}\,\langle x,y \rangle_1\, Zerosnd^3\, \langle x,y \rangle\, \{y = 0\}$ | $(Zerosnd)$ |
| (7) | $\{0 = 0\}\,\langle x,y \rangle_{max\{0,1\}}\, Zerofst \cdot Zerosnd^{max\{2,3\}}\, \langle x,y \rangle\, \{x = 0 \wedge y = 0\}$ | $(PAR$ 5,6) |
| (8) | $\{0 = 0\}\,\langle x,y \rangle_{max\{0,1\}}\, (Zerofst \cdot Zerosnd); Join; Inc^{*^u}\, \langle w \rangle\, \{w \geq 0\}$ donde $u$ es $max\{2,3\}+0+\infty$ | $(SEC$ 4,7) |
| (9) | $true \Rightarrow 0 = 0$ | (Aritmética) |
| (10) | $\{true\}\,\langle x,y \rangle_{max\{0,1\}}\, (Zerofst \cdot Zerosnd); Join; Inc^{*^u}\, \langle w \rangle\, \{w \geq 0\}$ | $(CONS$ 8,9) |
| (11) | $true \Rightarrow 1 \leq max\{0,1\}$ | (Aritmética) |
| (12) | $true \Rightarrow max\{2,3\}+0+\infty \leq \infty$ | (Aritmética) |
| (13) | $\{true\}\,\langle x,y \rangle_1\, (Zerofst \cdot Zerosnd); Join; Inc^{*^\infty}\, \langle w \rangle\, \{w \geq 0\}$ | $(TIME$ 10,11,12) |

■

EJEMPLO 2.6.4 Se quiere probar que

$$Th(\mathcal{A}) \vdash \{x = X\}\,\langle x \rangle_\epsilon\, \mathbf{if}\ x > 0 \rightarrow 1'_{Int}\ []\ x < 0 \rightarrow neg\ \mathbf{fi}^{3*\epsilon}\, \langle y \rangle\, \{y = |X|\}.$$

La siguiente es una deducción de la fórmula desde $Th(\mathcal{A})$:

| | | |
|---|---|---|
| (1) | $\{x = \|X\|\}\,\langle x\rangle_{\epsilon}\, 1'_{Int}{}^{\epsilon}\,\langle x\rangle\,\{x = \|X\|\}$ | $(SKIP)$ |
| (2) | $x = X \wedge x > 0 \Rightarrow x = \|X\|$ | (Aritmética) |
| (3) | $\{x = X \wedge x > 0\}\,\langle x\rangle_{\epsilon}\, 1'_{Int}{}^{\epsilon}\,\langle x\rangle\,\{x = \|X\|\}$ | $(CONS\ 1{,}2)$ |
| (4) | $\{x = X \wedge x > 0\}\,\langle x\rangle_{\epsilon}\, 1'_{Int}{}^{\epsilon}\,\langle y\rangle\,\{y = \|X\|\}$ | $(VAR\ 3)$ |
| (5) | $\{-x = \|X\|\}\,\langle x\rangle_{\epsilon}\, neg^{2*\epsilon}\,\langle y\rangle\,\{y = \|X\|\}$ | $(Neg)$ |
| (6) | $x = X \wedge x < 0 \Rightarrow -x = \|X\|$ | Aritmética |
| (7) | $\{x = X \wedge x < 0\}\,\langle x\rangle_{\epsilon}\, neg^{2*\epsilon}\,\langle y\rangle\,\{y = \|X\|\}$ | $(CONS\ 5{,}6)$ |
| (8) | $\{x = X\}\,\langle x\rangle_{\epsilon}\,\mathbf{if}\ x > 0 \to 1'_{Int}\ []\ x < 0 \to neg\ \mathbf{fi}^{\epsilon + max\{\epsilon, 2*\epsilon\}}\,\langle y\rangle\,\{y = \|X\|\}$ | $(IF\ 4{,}7)$ |
| (9) | $x = X \Rightarrow \epsilon + max\{\epsilon, 2*\epsilon\} \leq 3*\epsilon$ | (Artimética) |
| (10) | $\{x = X\}\,\langle x\rangle_{\epsilon}\,\mathbf{if}\ x > 0 \to 1'_{Int}\ []\ x < 0 \to neg\ \mathbf{fi}^{3*\epsilon}\,\langle y\rangle\,\{y = \|X\|\}$ | $(TIME\ 8{,}9)$ |

■

EJEMPLO 2.6.5 Sea $DecToEq$ el proceso

$$\mathbf{do}\ u > v \to Decfst\ []\ z < w \to Decsnd\ \mathbf{od}.$$

Se quiere probar que

$$Th(\mathcal{A}) \vdash \{true\}\,\langle x, y\rangle_{\epsilon}\, DecToEq^{|x-y|*3}\,\langle x, y\rangle\,\{x = y\}.$$

La siguiente es una deducción de la fórmula desde $Th(\mathcal{A})$:

| | | |
|---|---|---|
| (1) | $\{true \wedge |x - 1 - y| < t_0\}\,\langle x, y\rangle_0\, Decfst^2\,\langle x, y\rangle\,\{true \wedge |x - y| < t_0\}$ | $(Decfst)$ |
| (2) | $x > y \wedge true \wedge |x - y| = t_0 \Rightarrow true \wedge |x - 1 - y| < t_0$ | (Aritmética) |
| (3) | $\{x > y \wedge true \wedge |x - y| = t_0\}\,\langle x, y\rangle_0\, Decfst^2\,\langle x, y\rangle\,\{true \wedge |x - y| < t_0\}$ | $(CONS\ 1{,}2)$ |
| (4) | $\{true \wedge |x - y - 1| < t_0\}\,\langle x, y\rangle_0\, Decsnd^3\,\langle x, y\rangle\,\{true \wedge |x - y| < t_0\}$ | $(Decsnd)$ |
| (5) | $x < y \wedge true \wedge |x - y| = t_0 \Rightarrow true \wedge |x - y - 1| < t_0$ | (Aritmética) |
| (6) | $\{x < y \wedge true \wedge |x - y| = t_0\}\,\langle x, y\rangle_0\, Decsnd^3\,\langle x, y\rangle\,\{true \wedge |x - y| < t_0\}$ | $(CONS\ 4{,}5)$ |
| (7) | $\{true\}\,\langle x, y\rangle_{\epsilon}\, DecToEq^{|x-y|*max\{2,3\}}\,\langle x, y\rangle\,\{\neg(x > y \vee x < y) \wedge true\}$ | $(DO\ 3{,}6)$ |
| (8) | $true \Rightarrow |x - y| * max\{2, 3\} \leq |x - y| * 3$ | (Aritmética) |
| (9) | $\{true\}\,\langle x, y\rangle_{\epsilon}\, DecToEq^{|x-y|*3}\,\langle x, y\rangle\,\{\neg(x > y \vee x < y) \wedge true\}$ | $(TIME\ 7{,}8)$ |
| (10) | $\neg(x > y \vee x < y) \wedge true \Rightarrow x = y$ | (Aritmética) |
| (11) | $\{true\}\,\langle x, y\rangle_{\epsilon}\, DecToEq^{|x-y|*3}\,\langle x, y\rangle\,\{x = y\}$ | $(CONS\ 9{,}10)$ |

■

EJEMPLO 2.6.6 En este ejemplo se probará la corrección parcial del segundo proceso que implementa la máquina vendedora de caramelos presentado en la Sección 1.4. Siendo $\mathcal{A}$ la estructura de objeto para este problema, se tiene que $HTh(\mathcal{A})$ es axiomatizable con los siguientes esquemas de axioma:[3]

[3]Para reducir notación se escribirá, por ejemplo, $[\#\$ + 1/\#\$']$ en lugar de $[\#\$ + 1, \#P, \$r, Pr/\#\$', \#P', \$r', Pr']$, asumiendo así que las variables restantes no se cambian.

Siendo $\alpha \in For(\mathcal{S})$, $\#\$, \#P, \#\$', \#P'$ variables de sort $Nat$ y $\$r, Pr, \$r', Pr'$ variables de sort $Bool$,

- *Axioma Accept$*:

$$\{\alpha[\#\$ + 1/\#\$']\} \langle \#\$, \#P, \$r, Pr \rangle_0 Accept\$^{3s} \langle \#\$', \#P', \$r', Pr' \rangle \{\alpha\}$$

- *Axioma Return$*:

$$\{\#\$ > 0 \Rightarrow \alpha[\#\$ - 1, \mathsf{t}/\#\$', \$r']\} \langle \#\$, \#P, \$r, Pr \rangle_0 Return\$^{4s} \langle \#\$', \#P', \$r', Pr' \rangle \{\alpha\}$$

- *Axioma GiveProduct*:

$$\{\#P > 0 \Rightarrow \alpha[\#P - 1, \mathsf{t}/\#P', Pr']\} \langle \#\$, \#P, \$r, Pr \rangle_0 GiveProduct^{10s} \langle \#\$', \#P', \$r', Pr' \rangle \{\alpha\}$$

- *Axioma AskForReplenish*:

$$\{\alpha[MP/\#P']\} \langle \#\$, \#P, \$r, Pr \rangle_0 AskForReplenish^{24h} \langle \#\$', \#P', \$r', Pr' \rangle \{\alpha\}$$

Se quiere probar que la fórmula de Hoare

$$\{\#\$ = x_0 \wedge \#P = P_0 \wedge \$r = \mathsf{f} \wedge Pr = \mathsf{f}\}$$
$$\langle \#\$, \#P, \$r, Pr \rangle$$
$$_0\ (\#P > 0?; Accept\$; GiveProduct) + (\#P = 0?; Accept\$; Return\$)^{3m}$$
$$\langle \#\$, \#P, \$r, Pr \rangle$$
$$\left\{ P_0 = 0 \Rightarrow \begin{pmatrix} \#\$ = x_0 + 1 \wedge \#P = MP - 1 \wedge \$r = \mathsf{f} \wedge Pr = \mathsf{t} \\ \vee \\ \#\$ = x_0 \wedge \#P = 0 \wedge \$r = \mathsf{t} \wedge Pr = \mathsf{f} \end{pmatrix} \right\}$$
$$P_0 > 0 \Rightarrow \#\$ = x_0 + 1 \wedge \#P = P_0 - 1 \wedge \$r = \mathsf{f} \wedge Pr = \mathsf{t}$$

es derivable desde $Th(\mathcal{A})$ en el cálculo de Hoare extendido con los axiomas anteriores. Por $Vending$, $m$, $pre$ y $post$ se denotarán el proceso, la tupla $\langle \#\$, \#P, \$r, Pr \rangle$, la precondición y la poscondición de la fórmula de Hoare, respectivamente. Así, la siguiente es una deducción de esta fórmula desde $Th(\mathcal{A})$:

| | | |
|---|---|---|
| (1) | $\{\#P > 0 \Rightarrow post[\#P - 1, \mathsf{t}/\#P, Pr]\} m_0 GiveProduct^{10s} m\{post\}$ | ($GiveProduct$) |
| (2) | $mid_1 \Rightarrow (\#P > 0 \Rightarrow post[\#P - 1, \mathsf{t}/\#P, Pr])$ | (Aritmética) |
| | donde $mid_1 \equiv \#P > 0 \Rightarrow (P_0 = 0 \Rightarrow \#\$ = x_0 + 1 \wedge \#P = MP \wedge \$r = \mathsf{f})$ $\wedge\ (P_0 > 0 \Rightarrow \#\$ = x_0 + 1 \wedge \#P = P_0 \wedge \$r = \mathsf{f})$ | |
| (3) | $\{mid_1\} m_0 GiveProduct^{10s} m\{post\}$ | ($CONS$ 1,2) |
| (4) | $\{mid_1[\#\$ + 1/\#\$]\} m_0 Accept\$^{3s} m\{mid_1\}$ | ($Accept\$$) |
| (5) | $\#P > 0 \wedge pre \Rightarrow mid_1[\#\$ + 1/\#\$]$ | (Aritmética) |
| (6) | $\{\#P > 0 \wedge pre\} m_0 Accept\$^{3s} m\{mid_1\}$ | ($CONS$ 4,5) |
| (7) | $\{\#P > 0 \wedge pre\} m_0 Accept\$; GiveProduct^{3s+10s} m\{post\}$ | ($SEC$ 3,6) |

(8) $\{\#\$ > 0 \Rightarrow post[\#\$ - 1, \mathsf{t}/\#\$, \$r]\} m_0\, Return\$^{4s} m\{post\}$ ($Return\$$)

(9) $mid_2 \Rightarrow (\#\$ > 0 \Rightarrow post[\#\$ - 1, \mathsf{t}/\#\$, \$r])$ (Aritmética)
donde $mid_2 \equiv \#\$ > 0 \Rightarrow (\#\$ = x_0 + 1 \wedge \#P = 0 \wedge Pr = \mathsf{f})$

(10) $\{mid_2\} m_0\, Return\$^{4s} m\{post\}$ ($CONS$ 8,9)

(11) $\{mid_2[\#\$ + 1/\#\$]\} m_0\, Accept\$^{3s} m\{mid_2\}$ ($Accept\$$)

(12) $\#P = 0 \wedge pre \Rightarrow mid_2[\#\$ + 1/\#\$]$ (Aritmética)

(13) $\{\#P = 0 \wedge pre\} m_0\, Accept\$^{3s} m\{mid_2\}$ ($CONS$ 11,12)

(14) $\{\#P = 0 \wedge pre\} m_0\, Accept\$; Return\$^{3s+4s} m\{post\}$ ($SEC$ 10,13)

(15) $\{\#P > 0 \Rightarrow \#P > 0 \wedge pre\} m_\epsilon\, \#P > 0?^{\epsilon} m\{\#P > 0 \wedge pre\}$ ($TEST$)

(16) $pre \Rightarrow (\#P > 0 \Rightarrow \#P > 0 \wedge pre)$ (Lógica)

(17) $\{pre\} m_\epsilon\, \#P > 0?^{\epsilon} m\{\#P > 0 \wedge pre\}$ ($CONS$ 15,16)

(18) $\{pre\} m_\epsilon\, \#P > 0?; Accept\$; GiveProduct^{\epsilon+3s+10s} m\{post\}$ ($SEC$ 7,17)

(19) $\{\#P = 0 \Rightarrow \#P > 0 \wedge pre\} m_\epsilon\, \#P = 0?^{\epsilon} m\{\#P = 0 \wedge pre\}$ ($TEST$)

(20) $pre \Rightarrow (\#P = 0 \Rightarrow \#P = 0 \wedge pre)$ (Lógica)

(21) $\{pre\} m_\epsilon\, \#P = 0?^{\epsilon} m\{\#P = 0 \wedge pre\}$ ($CONS$ 19,20)

(22) $\{pre\} m_\epsilon\, \#P = 0?; Accept\$; Return\$^{\epsilon+4s+10s} m\{post\}$ ($SEC$ 14,21)

(23) $\{pre\} m_{min\{\epsilon,\epsilon\}}\, Vending^{max\{\epsilon+3s+10s, \epsilon+4s+10s\}} m\{post\}$ ($CHC$ 18,22)

(24) $pre \Rightarrow 0 \leq min\{\epsilon, \epsilon\}$ (Aritmética)

(25) $pre \Rightarrow max\{\epsilon + 3s + 10s, \epsilon + 4s + 10s\} \leq 3m$ (Aritmética)

(26) $\{pre\} m_0\, Vending^{3m} m\{post\}$ ($TIME$ 23,24,25)

■

# Parte III

# Refinamientos en $P/PML$

# Capítulo 3

# Cálculo de Refinamientos en $P/PML$

## 3.1 Introducción

En la segunda parte de este trabajo se ha estudiado el aspecto de verificación formal de procesos en la lógica $P/PML$. En esta tercer parte, se introducirá la visión opuesta a la verificación de programas: el concepto de *derivación de programas*. La tarea de un programador puede ser vista como la construcción de un programa $S$ a partir de una especificación $[P, Q]$ de forma tal que $S$ satisfaga dicha especificación. Las teorías de derivación de programas presentan reglas para 'calcular' programas a partir de sus especificaciones. Estas teorías permiten una sistematización del proceso de desarrollo de programas, produciendo artefactos de software correctos. Varias teorías han sido desarrolladas en este aspecto, como por ejemplo la teoría de las precondiciones más débiles de E.W. Dijkstra [7]. Otro ejemplo importante de este tipo de formalismos es el cálculo de refinamientos [2, 14], que formaliza el enfoque de refinamiento paso a paso ("stepwise refinement") para la construcción de programas [15]. En el cálculo de refinamientos, los programas se derivan en un lenguaje de amplio espectro que incluye tanto construcciones ejecutables como no ejecutables. Una derivación típicamente comienza con una especificación (en general, no ejecutable), y progresa vía un número de formas intermedias que combinan tanto construcciones ejecutables como no ejecutables, terminando con un programa conteniendo sólo construcciones ejecutables. En cada paso de derivación, se toman decisiones que acercan al programa a una forma ejecutable, posiblemente dando lugar a ciertas obligaciones de prueba. Estas obligaciones de prueba pueden descargarse a medida que aparecen, de forma que el programa y su prueba se desarrollan simultáneamente, como recomienda Gries [9]. La notación usual utilizada en el cálculo de refinamientos es:

$$R \sqsubseteq S$$

donde $R, S$ son programas del lenguaje de programación. En general, una fórmula de la forma $R \sqsubseteq S$ (que suele leerse como "$S$ refina a $R$") establece que $S$ es en un sentido 'mejor' que $R$ (más eficiente, más ejecutable, etc.). El enfoque acerca de refinamientos en $P/PML$ adoptado aquí difiere con el enfoque presentado en [5], basándose más bien en el que aparece en [8]. Este enfoque sigue el estilo de refinamiento desarrollado por Morgan, pero está fundado en la lógica de Hoare presentada en la segunda parte de este trabajo. En rigor, se indentifica una especificación con el conjunto de sus posibles

implementaciones, y el refinamiento se representa como manipulaciones sobre conjuntos de procesos. El proceso de refinamiento consistirá entonces de una secuencia de pasos que realizan decisiones de diseño sistemáticas para reducir los conjuntos de posibles implementaciones hasta alcanzar una única implementación. Así, un refinamiento de una especificación $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l}$ a una implementación $R$ se denotará por

$$\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l} \sqsubseteq R.$$

Por ejemplo, la fórmula $\langle x \rangle, \langle y, z \rangle : [x = 0,\ y = z = 1]\ {}^{2}_{0} \sqsubseteq Inc; Dup$ establece que la especificación $\langle x \rangle, \langle y, z \rangle : [x = 0,\ y = z = 1]\ {}^{2}_{0}$ puede refinarse a la implementación $Inc; Dup$.

## 3.2 La lógica de refinamientos

Para razonar formalmente sobre refinamientos en $P/PML$, se presentará una lógica de refinamientos y un cálculo para esta lógica, que serán desarrollados siguiendo el enfoque adoptado en la segunda parte del trabajo. Este cálculo permitirá derivar refinamientos preservando la corrección parcial. Nuevamente, la definición de esta lógica se construye sobre la lógica multisort de primer orden.

DEFINICION 3.2.1 Sea $\mathcal{S}$ una signatura de objeto. Una *especificación* sobre $\mathcal{S}$ es una expresión de la forma

$$\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l}$$

donde $\alpha, \beta \in For(\mathcal{S})$ son fórmulas de primer orden con $Var(\beta) \subseteq \vec{y}$, $\vec{x} = x_1 \ldots x_m$ con $x_i$ de sort $s_i$, $\vec{y} = y_1 \ldots y_n$ distintas con $y_i$ de sort $s'_i$ y $l, u$ expresiones de sort $T$. Se define $ia(\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l}) = s_1 \ldots s_m$ y $oa(\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l}) = s'_1 \ldots s'_n$

■

El conjunto de todas las especificaciones sobre $\mathcal{S}$ se denotará por $Spec(\mathcal{S})$. Nótese que, al igual que en el caso de las fórmulas de Hoare de la segunda parte del trabajo, se debe aplicar la misma restricción sintáctica sobre la poscondición en una especificación. Formalizado el concepto de especificación, es necesario definir el lenguaje de amplio espectro en el cual se derivan los refinamientos. Para ello, se extenderá la definición de término relacional para incluir especificaciones, es decir, se considerará que $Spec(\mathcal{S}) \subseteq RT(\mathcal{S})$. Por convención, $Spec(\mathcal{S}) \nsubseteq GRT(\mathcal{S})$. Finalmente, se define la sintaxis de las fórmulas de la lógica de refinamientos.

DEFINICION 3.2.2 (Sintaxis de la lógica de refinamientos) Sea $\mathcal{S}$ una signatura de objeto. Una *fórmula de refinamiento* sobre $\mathcal{S}$ es una expresión de la forma

$$R \sqsubseteq S$$

donde $R, S \in RT(\mathcal{S})$ tales que $ia(R) = ia(S)$ y $oa(R) = oa(S)$.

■

El conjunto de todas las fórmulas de refinamiento sobre $\mathcal{S}$ se denotará por $RFor(\mathcal{S})$. Los únicos objetos sintácticos en la lógica de refinamientos serán las fórmulas de refinamiento, por lo tanto la semántica de esta lógica sólo requiere describir el significado de este tipo de fórmulas. Para ello se debe primero asociar un término relacional con el conjunto de sus posibles implementaciones.

DEFINICION 3.2.3 Sean $\mathcal{S}$ una signatura de objeto, $\mathcal{A}$ una estructura de objeto para $\mathcal{S}$ y $R \in RT(\mathcal{S})$. La función

$$\wp : RT(\mathcal{S}) \to \mathcal{P}\,(GRT(\mathcal{S}))$$

se define como sigue:

1. $\wp(a) = \{a\}$, si $a \in A \cup \{\, 1'_t : t \in S^* \,\} \cup \{\, \alpha? : \alpha \in For(\mathcal{S}) \,\}$.
2. $\wp(\vec{x}, \vec{y} : [\alpha,\ \beta]\,{}_l^u) = \left\{ R \in GRT(\mathcal{S}) : Th(\mathcal{A}) \cup HTh(\mathcal{A}) \vdash \{\alpha\}\ \vec{x}\ {}_l R^u\ \vec{y}\ \{\beta\} \right\}$.
3. $\wp(S^*) = \{\, s^* : s \in \wp(S) \,\}$
4. $\wp(S \odot T) = \{\, s \odot t : s \in \wp(S) \wedge t \in \wp(T) \,\}$, si $\odot \in \{;, +, \cdot\}$.

■

EJEMPLO 3.2.1 Sea $\mathcal{A}$ una estructura de objeto donde las acciones atómicas $Inc$ y $Dec$ incrementan y decrementan en 1 su entrada, respectivamente. Entonces

$$\begin{aligned}
&\wp(\langle x \rangle,\langle y \rangle : [x = 0,\ y = 0]\,{}_0^\infty \cdot Dec) \\
&\quad = \left\{ r \cdot Dec : r \in \wp(\vec{x}, \vec{y} : [x = 0,\ y = 0]\,{}_0^\infty) \right\} \\
&\quad = \{1'_{Int} \cdot Dec,\ 1'_{Int}; 1'_{Int} \cdot Dec,\ 1'_{Int} + 1'_{Int} \cdot Dec,\ true? \cdot Dec,\ x = 0? \cdot Dec,\ Inc; Dec \cdot Dec,\ \ldots\}.
\end{aligned}$$

■

Una propiedad importante que la función $\wp$ satisface es la monotonicidad con respecto a la inclusión de conjuntos.

PROPIEDAD 3.2.4 *Sean $S, S', T, T' \in RT(\mathcal{S})$ tales que $\wp(S') \subseteq \wp(S)$ y $\wp(T') \subseteq \wp(T)$. Entonces*

1. *$\wp(S'^*) \subseteq \wp(S^*)$, y*
2. *$\wp(S' \odot T') \subseteq \wp(S \odot T)$, si $\odot \in \{;, +, \cdot\}$.*

*Prueba.* Véase Apéndice A. ■

Finalmente, se define la semántica de las fórmulas de refinamiento.

DEFINICION 3.2.5 (Semántica de la lógica de refinamientos) Sea $\mathcal{S}$ una signatura de objeto y $\mathcal{A}$ una estructura de objeto para $\mathcal{S}$. Dada $R \sqsubseteq S \in RFor(\mathcal{S})$ se dice que la fórmula de refinamiento $R \sqsubseteq S$ es *válida* en $\mathcal{A}$, denotado por

$$\models_{\mathcal{A}} R \sqsubseteq S,$$

siempre que $\wp(S) \subseteq \wp(R)$.

■

Los conceptos de validez lógica, modelo, consecuencia lógica y teoría para fórmulas de refinamiento se definen en forma análoga a lo expuesto en la Sección 2.2 de la segunda parte del trabajo.

EJEMPLO 3.2.2 Sea $\mathcal{A}$ una estructura de objeto donde $Inc^{\mathcal{A}} = \{\langle n, n+1\rangle : n \in \mathsf{Nat}, n \geq 0\}$. Entonces

$$\models_{\mathcal{A}} \langle x\rangle,\langle y\rangle : [x \leq 0,\ y = 1]\ {}^{\infty}_{0} \sqsubseteq Inc$$

pues es cierto que $Inc \in \wp(\langle x\rangle,\langle y\rangle : [x \leq 0,\ y = 1]\ {}^{\infty}_{0})$.

■

EJEMPLO 3.2.3 Sea $\alpha \in For(\mathcal{S})$. Entonces

$$\models \langle x\rangle,\langle x\rangle : [\alpha,\ \alpha]\ {}^{3*\epsilon}_{0} \sqsubseteq 1'_{Int}; 1'_{Int}$$

ya que se tiene $\models_{\mathcal{A}} \langle x\rangle,\langle x\rangle : [\alpha,\ \alpha]\ {}^{3*\epsilon}_{0} \sqsubseteq 1'_{Int}; 1'_{Int}$ para toda estructura de objeto $\mathcal{A}$.

■

EJEMPLO 3.2.4 Sea $W$ el conjunto $\{X + 1 > X, \langle x\rangle,\langle y\rangle : [x = X,\ y = X + 1]\ {}^{1}_{0} \sqsubseteq Inc\}$. Entonces se tiene que

$$W \models \langle x\rangle,\langle y\rangle : [x = X,\ y > X]\ {}^{1}_{0} \sqsubseteq Inc$$

puesto que, siendo $\mathcal{A}$ un modelo de $W$, se cumple que $\models_{\mathcal{A}} \langle x\rangle,\langle y\rangle : [x = X,\ y > X]\ {}^{1}_{0} \sqsubseteq Inc$.

■

## 3.3 El cálculo de refinamientos

En esta sección se desarrollará un cálculo para la lógica de refinamientos presentada en la sección anterior, denominado 'cálculo de refinamientos'. El propósito de este cálculo es el de derivar fórmulas de refinamiento 'verdaderas'. Por lo tanto, el cálculo de refinamientos no dependerá de una estructura de objeto específica, sino que incluirá solamente axiomas y reglas que son válidos en toda estructura de objeto. Por supuesto, en la práctica se está interesado en las fórmulas de refinamiento válidas en alguna estructura de objeto $\mathcal{A}$ en particular. Este tema será tratado en la siguiente sección.

Formalmente, el cálculo de refinamientos sobre una signatura de objeto $\mathcal{S} = \langle A, \langle S, F, P\rangle\rangle$ es un cálculo sobre $For(\mathcal{S}) \cup RFor(\mathcal{S})$ que consiste de los siguientes esquemas de axioma y reglas de deducción:

(i) *Axioma SKIP*

$$\boxed{\vec{x}, \vec{x} : [\alpha,\ \alpha]\ {}^{\epsilon}_{\epsilon} \sqsubseteq 1'_{t}}$$

(ii) *Axioma TEST*: Siendo $\vec{z}$ las variables libres de $\gamma$

$$\boxed{\vec{x}, \vec{x} : [\gamma[\vec{x}/\vec{z}] \Rightarrow \alpha,\ \alpha]\ {}^{\epsilon}_{\epsilon} \sqsubseteq \gamma?}$$

(iii) *Regla CONS*

$$\boxed{\frac{\gamma \Rightarrow \alpha, \qquad \delta \Leftarrow \beta}{\vec{x}, \vec{y} : [\gamma,\ \delta]\ {}^{u}_{l} \sqsubseteq \vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l}}}$$

(iv) *Regla VAR*: Si $\vec{z}$ son variables distintas o bien $\vec{x}=\vec{z}$

$$\frac{}{\vec{x},\vec{y} : [\alpha[\vec{x}/\vec{z}],\ \beta[\vec{y}/\vec{w}]]\ {}^{u[\vec{x}/\vec{z}]}_{l[\vec{x}/\vec{z}]} \sqsubseteq \vec{z},\vec{w} : [\alpha,\ \beta]\ {}^{u}_{l}}$$

(v) *Regla TIME*

$$\frac{\alpha \Rightarrow v \leq l, \qquad \alpha \Rightarrow w \geq u}{\vec{x},\vec{y} : [\alpha,\ \beta]\ {}^{w}_{v} \sqsubseteq \vec{x},\vec{y} : [\alpha,\ \beta]\ {}^{u}_{l}}$$

(vi) *Regla SEC*: Si $Var(w) \cap \vec{z} = \emptyset$

$$\frac{}{\vec{x},\vec{y} : [\alpha,\ \beta]\ {}^{u+w}_{l} \sqsubseteq \vec{x},\vec{z} : [\alpha,\ \gamma]\ {}^{u}_{l}; \vec{z},\vec{y} : [\gamma,\ \beta]\ {}^{w}_{v}}$$

(vii) *Regla CHC*

$$\frac{}{\vec{x},\vec{y} : [\alpha,\ \beta]\ {}^{max\{u,w\}}_{min\{l,v\}} \sqsubseteq \vec{x},\vec{y} : [\alpha,\ \beta]\ {}^{u}_{l} + \vec{x},\vec{y} : [\alpha,\ \beta]\ {}^{w}_{v}}$$

(viii) *Regla PAR*

$$\frac{}{\vec{x},\vec{y} : [\alpha,\ \beta \wedge \gamma]\ {}^{max\{u,w\}}_{max\{l,v\}} \sqsubseteq \vec{x},\vec{y} : [\alpha,\ \beta]\ {}^{u}_{l} \cdot \vec{x},\vec{y} : [\alpha,\ \gamma]\ {}^{w}_{v}}$$

(ix) *Regla ITE*

$$\frac{}{\vec{x},\vec{x} : [\alpha,\ \alpha]\ {}^{\infty}_{0} \sqsubseteq \left(\vec{x},\vec{x} : [\alpha,\ \alpha]\ {}^{u}_{l}\right)^{*}}$$

(x) *Regla REF*

$$\frac{}{R \sqsubseteq R}$$

(xi) *Regla TRAN*

$$\frac{R \sqsubseteq S \qquad S \sqsubseteq T}{R \sqsubseteq T}$$

(xii) *Regla MNSEC*

$$\frac{R \sqsubseteq R' \qquad S \sqsubseteq S'}{R;S \sqsubseteq R';S'}$$

(xiii) *Regla MNCHC*

$$\frac{R \sqsubseteq R' \qquad S \sqsubseteq S'}{R+S \sqsubseteq R'+S'}$$

(xiv) *Regla MNPAR*

$$\frac{R \sqsubseteq R' \qquad S \sqsubseteq S'}{R \cdot S \sqsubseteq R' \cdot S'}$$

(xv) *Regla MNITE*

$$\frac{R \sqsubseteq R'}{R^* \sqsubseteq R'^*}$$

Las reglas $REF$, $TRAN$, $MNSEC$, $MNCHC$, $MNPAR$ y $MNITE$ se agregan para que el enfoque de refinamientos sucesivos funcione. Las reglas $REF$ y $TRAN$ establecen la reflexividad y transitividad de $\sqsubseteq$ respectivamente, asegurando que cada término relacional es un refinamiento de los anteriores a lo largo de una derivación. Las reglas $MNSEC$, $MNCHC$, $MNPAR$ y $MNITE$ establecen la monotonicidad de $\sqsubseteq$ con respecto a los constructos ;, $+$, $\cdot$ y $*$, permitiendo refinar individualmente los componentes de un término.

De forma similar a lo realizado con el cálculo de Hoare en la segunda parte, es posible extender los axiomas y reglas del cálculo de refinamientos mediante reglas derivadas. Por ejemplo, la siguiente es una regla derivada para acciones *skip*:

(i') *Regla SKIP'*

$$\frac{\alpha \Rightarrow l \leq \epsilon, \qquad \alpha \Rightarrow \beta[\vec{x}/\vec{y}], \qquad \alpha \Rightarrow \epsilon \geq u}{\vec{x}, \vec{y} : [\alpha,\ \beta]_l^u \sqsubseteq 1'_t}$$

## 3.4 Consistencia y completitud relativa

En esta sección se investigarán la consistencia y completitud del cálculo de refinamientos desarrollado. Debe recordarse que el propósito del cálculo es el de derivar refinamientos válidos en una estructura de objeto en particular. Por lo tanto, para obtener resultados significativos se debe apelar a las fórmulas de primer orden válidas en la estructura de objeto $\mathcal{A}$, o sea, a la teoría $Th(\mathcal{A})$. Además, está claro que debe apelarse también a las fórmulas de refinamiento válidas en $\mathcal{A}$, conjunto que se denotará por $RTh(\mathcal{A})$. Es fácil ver que $RTh(\mathcal{A})$ es una teoría. Así, resulta razonable entonces investigar la consistencia y completitud del cálculo a partir del conjunto de fórmulas $Th(\mathcal{A}) \cup RTh(\mathcal{A})$.

Primero se demostrará la consistencia del cálculo.

TEOREMA 3.4.1 (***Consistencia del Cálculo de Refinamientos***) *Sea $\mathcal{S} = \langle A, \langle S, F, P \rangle \rangle$ una signatura de objeto y $\mathcal{A}$ una estructura de objeto para $\mathcal{S}$. Entonces para todo $R \sqsubseteq S \in RFor(\mathcal{S})$*

$$\textit{si } Th(\mathcal{A}) \cup RTh(\mathcal{A}) \vdash R \sqsubseteq S \textit{ entonces } Th(\mathcal{A}) \cup RTh(\mathcal{A}) \models R \sqsubseteq S.$$

*Prueba.* Sean $W$ y $W'$ los conjuntos $Th(\mathcal{A}) \cup RTh(\mathcal{A})$ y $Th(\mathcal{A}) \cup HTh(\mathcal{A})$ respectivamente, y $r$ una fórmula de refinamiento. Supóngase que $W \vdash r$. Se probará que $W \models r$ por inducción sobre la longitud $k$ de la deducción de $r$.

(a) *Paso base:* Si $k = 0$ entonces se tienen varios casos.

Caso 1: $r \in RTh(\mathcal{A})$. Luego, por definición de consecuencia lógica, se tiene que $W \models r$.

Caso 2: $r$ es el axioma $SKIP$. Luego

$$\begin{aligned}
W \models r \text{ sii } &\models_{\mathcal{M}} r \text{ para todo modelo } \mathcal{M} \text{ de } W && \text{(Definición)}\\
\text{sii } &\wp(1'_t) \subseteq \wp(\vec{x}, \vec{x} : [\alpha,\ \alpha]\ {}^{\epsilon}_{\epsilon}) && \text{(Def. 3.2.5)}\\
\text{sii } &1'_t \in \left\{ R \in GRT(\mathcal{S}) : W' \vdash \{\alpha\}\ \vec{x}\ {}_{\epsilon}R^{\epsilon}\ \vec{x}\ \{\alpha\} \right\} && \text{(Def. 3.2.3)}\\
\text{sii } &W' \vdash \{\alpha\}\ \vec{x}\ {}_{\epsilon}1'_t{}^{\epsilon}\ \vec{x}\ \{\alpha\} && \text{(Conjuntos)}\\
\text{sii } &\textbf{true} && (SKIP)
\end{aligned}$$

Caso 3: $r$ es el axioma $TEST$. Luego

$$\begin{aligned}
W \models r \text{ sii } &\models_{\mathcal{M}} r \text{ para todo modelo } \mathcal{M} \text{ de } W && \text{(Definición)}\\
\text{sii } &\wp(\gamma?) \subseteq \wp(\vec{x}, \vec{x} : [\gamma[\vec{x}/\vec{z}] \Rightarrow \alpha,\ \alpha]\ {}^{\epsilon}_{\epsilon}) && \text{(Def. 3.2.5)}\\
\text{sii } &\gamma? \in \left\{ R \in GRT(\mathcal{S}) : W' \vdash \{\gamma[\vec{x}/\vec{z}] \Rightarrow \alpha\}\ \vec{x}\ {}_{\epsilon}R^{\epsilon}\ \vec{x}\ \{\alpha\} \right\} && \text{(Def. 3.2.3)}\\
\text{sii } &W' \vdash \{\gamma[\vec{x}/\vec{z}] \Rightarrow \alpha\}\ \vec{x}\ {}_{\epsilon}\gamma?^{\epsilon}\ \vec{x}\ \{\alpha\} && \text{(Conjuntos)}\\
\text{sii } &\textbf{true} && (TEST)
\end{aligned}$$

(b) *Paso inductivo:* Supóngase que si $W \vdash r$ en una deducción de longitud $k < m$ con $m > 1$ entonces $W \models r$. Luego, si $W \vdash r$ en una deducción de longitud $k = m$, se tienen varios casos:

Caso 1: $r$ es consecuencia de aplicar la regla $CONS$. Luego $r$ tiene la forma $\vec{x}, \vec{y} : [\gamma,\ \delta]\ {}^{u}_{l} \sqsubseteq \vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l}$, y además $W \vdash \gamma \Rightarrow \alpha$ y $W \vdash \delta \Leftarrow \beta$, cada una en una deducción de menos de $k$ pasos. Luego, $\{\gamma \Rightarrow \alpha, \delta \Leftarrow \beta\} \subseteq Th(\mathcal{A})$, por lo tanto $W' \models \gamma \Rightarrow \alpha$ y $W' \models \delta \Leftarrow \beta$. Entonces

$$\begin{aligned}
\wp(\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l}) &= \left\{ R \in GRT(\mathcal{S}) : W' \vdash \{\alpha\}\ \vec{x}\ {}_{l}R^{u}\ \vec{y}\ \{\beta\} \right\} && \text{(Def. 3.2.3)}\\
&\subseteq \left\{ R \in GRT(\mathcal{S}) : W' \vdash \{\gamma\}\ \vec{x}\ {}_{l}R^{u}\ \vec{y}\ \{\delta\} \right\} && \text{(Hipótesis y } CONS)\\
&= \wp(\vec{x}, \vec{y} : [\gamma,\ \delta]\ {}^{u}_{l}) && \text{(Def. 3.2.3)}
\end{aligned}$$

Caso 2: $r$ es consecuencia de aplicar la regla $VAR$. Luego $r$ tiene la forma

$$\vec{x}, \vec{y} : [\alpha[\vec{x}/\vec{z}],\ \beta[\vec{y}/\vec{w}]]\ {}^{u[\vec{x}/\vec{z}]}_{l[\vec{x}/\vec{z}]} \sqsubseteq \vec{z}, \vec{w} : [\alpha,\ \beta]\ {}^{u}_{l}.$$

Entonces

$$\begin{aligned}
&\wp(\vec{z},\vec{w} : [\alpha,\ \beta]\,{}_{l}^{u}) \\
&\quad = \left\{ R \in GRT(\mathcal{S}) : W' \vdash \{\alpha\}\ \vec{z}\ {}_{l}R^{u}\ \vec{w}\ \{\beta\} \right\} && \text{(Def. 3.2.3)} \\
&\quad \subseteq \left\{ R \in GRT(\mathcal{S}) : W' \vdash \{\alpha[\vec{x}/\vec{z}]\}\ \vec{x}\ {}_{l[\vec{x}/\vec{z}]}R^{u[\vec{x}/\vec{z}]}\ \vec{y}\ \{\beta[\vec{y}/\vec{w}]\} \right\} && (VAR) \\
&\quad = \wp(\vec{x},\vec{y} : [\alpha[\vec{x}/\vec{z}],\ \beta[\vec{y}/\vec{w}]]\,{}_{l[\vec{x}/\vec{z}]}^{u[\vec{x}/\vec{z}]}) && \text{(Def. 3.2.3)}
\end{aligned}$$

Caso 3: $r$ es consecuencia de aplicar la regla $TIME$. Luego $r$ tiene la forma $\vec{x},\vec{y} : [\alpha,\ \beta]\,{}_{v}^{w} \sqsubseteq \vec{x},\vec{y} : [\alpha,\ \beta]\,{}_{l}^{u}$, y además $W \vdash \alpha \Rightarrow v \leq l$ y $W \vdash \alpha \Rightarrow w \geq u$, cada una en una deducción de menos de $k$ pasos. Luego, $\{\alpha \Rightarrow v \leq l, \alpha \Rightarrow w \geq u\} \subseteq Th(\mathcal{A})$, por lo tanto $W' \models \alpha \Rightarrow v \leq l$ y $W' \models \alpha \Rightarrow w \geq u$. Entonces

$$\begin{aligned}
\wp(\vec{x},\vec{y} : [\alpha,\ \beta]\,{}_{l}^{u}) &= \left\{ R \in GRT(\mathcal{S}) : W' \vdash \{\alpha\}\ \vec{x}\ {}_{l}R^{u}\ \vec{y}\ \{\beta\} \right\} && \text{(Def. 3.2.3)} \\
&\subseteq \left\{ R \in GRT(\mathcal{S}) : W' \vdash \{\alpha\}\ \vec{x}\ {}_{v}R^{w}\ \vec{y}\ \{\beta\} \right\} && \text{(Hipótesis y } TIME) \\
&= \wp(\vec{x},\vec{y} : [\alpha,\ \beta]\,{}_{v}^{w}) && \text{(Def. 3.2.3)}
\end{aligned}$$

Caso 4: $r$ es consecuencia de aplicar la regla $SEC$. Luego $r$ tiene la forma $\vec{x},\vec{y} : [\alpha,\ \beta]\,{}_{l}^{u+w} \sqsubseteq \vec{x},\vec{z} : [\alpha,\ \gamma]\,{}_{l}^{u};\vec{z},\vec{y} : [\gamma,\ \beta]\,{}_{v}^{w}$, con $Var(w) \cap \vec{z} = \emptyset$. Entonces

$$\begin{aligned}
&\wp(\vec{x},\vec{z} : [\alpha,\ \gamma]\,{}_{l}^{u};\vec{z},\vec{y} : [\gamma,\ \beta]\,{}_{v}^{w}) \\
&\quad = \left\{ r;s : r \in \wp(\vec{x},\vec{z} : [\alpha,\ \gamma]\,{}_{l}^{u}) \wedge s \in \wp(\vec{z},\vec{y} : [\gamma,\ \beta]\,{}_{v}^{w}) \right\} && \text{(Def. 3.2.3)} \\
&\quad = \left\{ r;s \in GRT(\mathcal{S}) : W' \vdash \{\alpha\}\ \vec{x}\ {}_{l}r^{u}\ \vec{z}\ \{\gamma\} \wedge W' \vdash \{\gamma\}\ \vec{z}\ {}_{v}s^{w}\ \vec{y}\ \{\beta\} \right\} && \text{(Def. 3.2.3)} \\
&\quad \subseteq \left\{ r;s \in GRT(\mathcal{S}) : W' \vdash \{\alpha\}\ \vec{x}\ {}_{l}r;s^{u+w}\ \vec{y}\ \{\beta\} \right\} && (SEC) \\
&\quad \subseteq \wp(\vec{x},\vec{y} : [\alpha,\ \beta]\,{}_{l}^{u+w}) && \text{(Def. 3.2.3)}
\end{aligned}$$

Caso 5: $r$ es consecuencia de aplicar la regla $CHC$. Luego $r$ tiene la forma $\vec{x},\vec{y} : [\alpha,\ \beta]\,{}_{min\{l,v\}}^{max\{u,w\}} \sqsubseteq \vec{x},\vec{y} : [\alpha,\ \beta]\,{}_{l}^{u} + \vec{x},\vec{y} : [\alpha,\ \beta]\,{}_{v}^{w}$. Entonces

$$\begin{aligned}
&\wp(\vec{x},\vec{y} : [\alpha,\ \beta]\,{}_{l}^{u} + \vec{x},\vec{y} : [\alpha,\ \beta]\,{}_{v}^{w}) \\
&\quad = \left\{ r+s : r \in \wp(\vec{x},\vec{y} : [\alpha,\ \beta]\,{}_{l}^{u}) \wedge s \in \wp(\vec{x},\vec{y} : [\alpha,\ \beta]\,{}_{v}^{w}) \right\} && \text{(Def. 3.2.3)} \\
&\quad = \left\{ r+s \in GRT(\mathcal{S}) : W' \vdash \{\alpha\}\ \vec{x}\ {}_{l}r^{u}\ \vec{y}\ \{\beta\} \wedge W' \vdash \{\alpha\}\ \vec{x}\ {}_{v}s^{w}\ \vec{y}\ \{\beta\} \right\} && \text{(Def. 3.2.3)} \\
&\quad \subseteq \left\{ r+s \in GRT(\mathcal{S}) : W' \vdash \{\alpha\}\ \vec{x}\ {}_{min\{l,v\}}r+s^{max\{u,w\}}\ \vec{y}\ \{\beta\} \right\} && (CHC) \\
&\quad \subseteq \wp(\vec{x},\vec{y} : [\alpha,\ \beta]\,{}_{min\{l,v\}}^{max\{u,w\}}) && \text{(Def. 3.2.3)}
\end{aligned}$$

Caso 6: $r$ es consecuencia de aplicar la regla $PAR$. Luego $r$ tiene la forma $\overrightarrow{x}, \overrightarrow{y} : [\alpha,\ \beta \wedge \gamma]\ {}^{max\{u,w\}}_{max\{l,v\}} \sqsubseteq \overrightarrow{x}, \overrightarrow{y} : [\alpha,\ \beta]\ {}^{u}_{l} \cdot \overrightarrow{x}, \overrightarrow{y} : [\alpha,\ \gamma]\ {}^{w}_{v}$. Entonces

$$
\begin{aligned}
&\wp(\overrightarrow{x}, \overrightarrow{y} : [\alpha,\ \beta]\ {}^{u}_{l} \cdot \overrightarrow{x}, \overrightarrow{y} : [\alpha,\ \gamma]\ {}^{w}_{v}) \\
&\quad = \left\{ r \cdot s : r \in \wp(\overrightarrow{x}, \overrightarrow{y} : [\alpha,\ \beta]\ {}^{u}_{l}) \wedge s \in \wp(\overrightarrow{x}, \overrightarrow{y} : [\alpha,\ \gamma]\ {}^{w}_{v}) \right\} && \text{(Def. 3.2.3)} \\
&\quad = \left\{ r \cdot s \in GRT(\mathcal{S}) : W' \vdash \{\alpha\}\ \overrightarrow{x}\ {}_{l}r^{u}\ \overrightarrow{y}\ \{\beta\} \wedge W' \vdash \{\alpha\}\ \overrightarrow{x}\ {}_{v}s^{w}\ \overrightarrow{y}\ \{\gamma\} \right\} && \text{(Def. 3.2.3)} \\
&\quad \subseteq \left\{ r \cdot s \in GRT(\mathcal{S}) : W' \vdash \{\alpha\}\ \overrightarrow{x}\ {}_{max\{l,v\}}r \cdot s^{max\{u,w\}}\ \overrightarrow{y}\ \{\beta \wedge \gamma\} \right\} && (PAR) \\
&\quad \subseteq \wp(\overrightarrow{x}, \overrightarrow{y} : [\alpha,\ \beta \wedge \gamma]\ {}^{max\{u,w\}}_{max\{l,v\}}) && \text{(Def. 3.2.3)}
\end{aligned}
$$

Caso 7: $r$ es consecuencia de aplicar la regla $ITE$. Luego $r$ tiene la forma $\overrightarrow{x}, \overrightarrow{x} : [\alpha,\ \alpha]\ {}^{\infty}_{0} \sqsubseteq \left(\overrightarrow{x}, \overrightarrow{x} : [\alpha,\ \alpha]\ {}^{u}_{l}\right)^{*}$. Entonces

$$
\begin{aligned}
&\wp(\left(\overrightarrow{x}, \overrightarrow{x} : [\alpha,\ \alpha]\ {}^{u}_{l}\right)^{*}) \\
&\quad = \left\{ r^{*} : r \in \wp(\overrightarrow{x}, \overrightarrow{x} : [\alpha,\ \alpha]\ {}^{u}_{l})) \right\} && \text{(Def. 3.2.3)} \\
&\quad = \left\{ r^{*} \in GRT(\mathcal{S}) : W' \vdash \{\alpha\}\ \overrightarrow{x}\ {}_{l}r^{u}\ \overrightarrow{x}\ \{\alpha\} \right\} && \text{(Def. 3.2.3)} \\
&\quad \subseteq \left\{ r^{*} \in GRT(\mathcal{S}) : W' \vdash \{\alpha\}\ \overrightarrow{x}\ {}_{l}r^{i\,u}\ \overrightarrow{x}\ \{\alpha\},\ i \geq 0 \right\} && (SKIP,SEC) \\
&\quad \subseteq \left\{ r^{*} \in GRT(\mathcal{S}) : W' \vdash \{\alpha\}\ \overrightarrow{x}\ {}_{0}r^{*\,\infty}\ \overrightarrow{x}\ \{\alpha\} \right\} && (ITE) \\
&\quad \subseteq \wp(\overrightarrow{x}, \overrightarrow{x} : [\alpha,\ \alpha]\ {}^{\infty}_{0}) && \text{(Def. 3.2.3)}
\end{aligned}
$$

Caso 8: $r$ es consecuencia de aplicar la regla $REF$. Luego $r$ tiene la forma $R \sqsubseteq R$. Es obvio que $\wp(R) \subseteq \wp(R)$. Así, se deduce que $W \models R \sqsubseteq R$.

Caso 9: $r$ es consecuencia de aplicar la regla $TRAN$. Luego $r$ tiene la forma $R \sqsubseteq T$, y además $W \vdash R \sqsubseteq S$ y $W \vdash S \sqsubseteq T$, cada una en una deducción de menos de $k$ pasos. Luego, por hipótesis inductiva $W \models R \sqsubseteq S$ y $W \models S \sqsubseteq T$. Por Def. 3.2.3 se tiene que $\wp(S) \subseteq \wp(R)$ y $\wp(T) \subseteq \wp(S)$. Así, se deduce que $\wp(T) \subseteq \wp(R)$, y de allí que $W \models R \sqsubseteq T$.

Caso 10: $r$ es consecuencia de aplicar la regla $MNSEC$. Luego $r$ tiene la forma $R;S \sqsubseteq R';S'$, y además $W \vdash R \sqsubseteq R'$ y $W \vdash S \sqsubseteq S'$, cada una en una deducción de menos de $k$ pasos. Luego, por hipótesis inductiva $W \models R \sqsubseteq R'$ y $W \models S \sqsubseteq S'$. Por Def. 3.2.3 se tiene que $\wp(R') \subseteq \wp(R)$ y $\wp(S') \subseteq \wp(S)$. Luego, por Prp. 3.2.4 se deduce que $\wp(R';S') \subseteq \wp(R;S)$, y de allí que $W \models R;S \sqsubseteq R';S'$.

Caso 11: $r$ es consecuencia de aplicar la regla $MNCHC$, $MNPAR$ ó $MNITE$. La demostración es análoga al caso anterior.

■

A continuación se estudiará la completitud del cálculo de refinamientos presentado. En este momento hay un punto importante a considerar. La intención del cálculo de refinamientos consiste en

comenzar con una especificación inicial y refinarla (mediante la sucesiva aplicación de las regla de refinamiento) hasta llegar a una implementación concreta. Sin embargo, la relación de refinamiento, como fue definida en Def. 3.2.5, admite ciertos refinamientos válidos que no son de interés de acuerdo a la intención del cálculo (como por ejemplo refinamiento a sí mismo, o bien refinamiento de acciones atómicas). Por lo tanto, para encontrar un resultado válido en cuanto a la completitud del cálculo, es necesario considerar sólo los refinamientos de interés. Así, resultará suficiente demostrar que todos los refinamientos válidos interesantes pueden probarse en el cálculo. Por otro lado, será necesario también restringirse a las estructuras de objeto expresivas.

Ahora se probará que el cálculo de refinamientos es completo en el sentido expuesto anteriormente. Primero se probará un lema que será utilizado en la demostración de completitud. Este lema establece que si se refina una especificación a una implementación, ésta será correcta con respecto a dicha especificación, y recíprocamente.

LEMA 3.4.2 *Sea* $S \in GRT(\mathcal{S})$. *Luego*

$$Th(\mathcal{A}) \cup RTh(\mathcal{A}) \models \vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l} \sqsubseteq S \text{ si y sólo si } Th(\mathcal{A}) \cup HTh(\mathcal{A}) \models \{\alpha\}\ \vec{x}\ {}_{l}S^{u}\ \vec{y}\ \{\beta\}.$$

*Prueba.* Véase Apéndice A. ■

TEOREMA 3.4.3 (***Completitud del Cálculo de Refinamientos***) *Sean* $\mathcal{S} = \langle A, \langle S, F, P \rangle \rangle$ *una signatura de objeto y* $\mathcal{A}$ *una estructura de objeto expresiva para* $\mathcal{S}$. *Entonces para todo* $R \in Spec(\mathcal{S})$ *y* $S \in GRT(\mathcal{S})$

$$\text{si } Th(\mathcal{A}) \cup RTh(\mathcal{A}) \models R \sqsubseteq S \text{ entonces } Th(\mathcal{A}) \cup HTh(\mathcal{A}) \vdash R \sqsubseteq S.$$

*Prueba.* Sean $W$ y $W'$ los conjuntos $Th(\mathcal{A}) \cup RTh(\mathcal{A})$ y $Th(\mathcal{A}) \cup HTh(\mathcal{A})$ respectivamente, y $r$ una fórmula de refinamiento $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l} \sqsubseteq S$ con $S \in GRT(\mathcal{S})$. Supóngase que $W \models r$. Se probará que $W \vdash r$ por inducción estructural sobre $S$.

(a) *Paso base:* Se tienen varios casos.

Caso 1: $S \equiv a$ con $a \in A$. Por definición, $r \in RTh(\mathcal{A})$. Luego, es obvio que $W \vdash r$.

Caso 2: $S \equiv 1'_t$. Si $W \models r$ entonces por Lem. 3.4.2 se tiene que $W' \models \{\alpha\}\ \vec{x}\ {}_{l}1'_t{}^{u}\ \vec{y}\ \{\beta\}$. Luego, por la demostración de Teo. 2.4.2 se tiene que $W \vdash \alpha \Rightarrow l \leq \epsilon$, $W \vdash \alpha \Rightarrow \epsilon \leq u$ y $W \vdash \alpha \Rightarrow \beta[\vec{x}/\vec{y}]$. Así, se tiene que la deducción

| | | |
|---|---|---|
| (1) | $\alpha \Rightarrow l \leq \epsilon$ | (Hipótesis) |
| (2) | $\alpha \Rightarrow \epsilon \leq u$ | (Hipótesis) |
| (3) | $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l} \sqsubseteq \vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\epsilon}_{\epsilon}$ | ($TIME$ 1,2) |
| (4) | $\alpha \Rightarrow \beta[\vec{x}/\vec{y}]$ | (Hipótesis) |
| (5) | $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\epsilon}_{\epsilon} \sqsubseteq \vec{x}, \vec{y} : [\beta[\vec{x}/\vec{y}],\ \beta]\ {}^{\epsilon}_{\epsilon}$ | ($CONS$ 4) |
| (6) | $\vec{x}, \vec{y} : [\beta[\vec{x}/\vec{y}],\ \beta]\ {}^{\epsilon}_{\epsilon} \sqsubseteq \vec{x}, \vec{x} : [\beta[\vec{x}/\vec{y}],\ \beta[\vec{x}/\vec{y}]]\ {}^{\epsilon}_{\epsilon}$ | ($VAR$) |
| (7) | $\vec{x}, \vec{x} : [\beta[\vec{x}/\vec{y}],\ \beta[\vec{x}/\vec{y}]]\ {}^{\epsilon}_{\epsilon} \sqsubseteq 1'_t$ | ($SKIP$) |
| (8) | $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l} \sqsubseteq 1'_t$ | ($TRAN$ 3,5,6,7) |

es una deducción para $r$ desde $W$. Por lo tanto $W \vdash r$.

Caso 3: $S \equiv \gamma?$. Si $W \models r$ entonces por Lem. 3.4.2 se tiene que $W' \models \{\alpha\}\ \vec{x}\ {}_l\gamma?^u\ \vec{y}\ \{\beta\}$. Luego, por la demostración de Teo. 2.4.2 se tiene que $W \vdash \alpha \Rightarrow l \leq \epsilon$, $W \vdash \alpha \Rightarrow \epsilon \leq u$ y $W \vdash \alpha \Rightarrow (\gamma[\vec{y}/\vec{z}] \Rightarrow \beta)[\vec{x}/\vec{y}]$. Sea $\psi$ la fórmula $\gamma[\vec{x}/\vec{z}] \Rightarrow \beta[\vec{x}/\vec{y}]$. Así, se tiene que la deducción

| | | |
|---|---|---|
| (1) | $\alpha \Rightarrow l \leq \epsilon$ | (Hipótesis) |
| (2) | $\alpha \Rightarrow \epsilon \leq u$ | (Hipótesis) |
| (3) | $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l} \sqsubseteq \vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\epsilon}_{\epsilon}$ | ($TIME$ 1,2) |
| (4) | $\alpha \Rightarrow \psi$ | (Hip. y Lógica) |
| (5) | $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\epsilon}_{\epsilon} \sqsubseteq \vec{x}, \vec{y} : [\psi,\ \beta]\ {}^{\epsilon}_{\epsilon}$ | ($CONS$ 4) |
| (6) | $\vec{x}, \vec{y} : [\psi,\ \beta]\ {}^{\epsilon}_{\epsilon} \sqsubseteq \vec{x}, \vec{x} : [\psi,\ \beta[\vec{x}/\vec{y}]]\ {}^{\epsilon}_{\epsilon}$ | ($VAR$) |
| (7) | $\vec{x}, \vec{x} : [\psi,\ \beta[\vec{x}/\vec{y}]]\ {}^{\epsilon}_{\epsilon} \sqsubseteq \gamma?$ | ($TEST$) |
| (8) | $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l} \sqsubseteq \gamma?$ | ($TRAN$ 3,5,6,7) |

es una deducción para $r$ desde $W$. Por lo tanto $W \vdash r$.

(b) *Paso inductivo:* Supóngase que la propiedad es verdadera para $S, T \in GRT(\mathcal{S})$ y que $W \models r$. Luego, se tienen varios casos:

Caso 1: $R \equiv S;T$. Si $W \models r$ entonces por Lem. 3.4.2 se tiene que $W' \models \{\alpha\}\ \vec{x}\ {}_l S;T^u\ \vec{y}\ \{\beta\}$. Luego, por la demostración de Teo. 2.4.2 se tiene que

$$W \vdash \alpha \Rightarrow l \leq \mathsf{l}(S),\ W \vdash \alpha \Rightarrow \mathsf{u}(S) + \mathsf{u}(T) \leq u$$

y

$$W' \models \{\alpha\}\ \vec{x}\ {}_{\mathsf{l}(S)}S^{\mathsf{u}(S)}\ \vec{z}\ \{\psi\},\ W' \models \{\psi\}\ \vec{z}\ {}_{\mathsf{l}(T)}T^{\mathsf{u}(T)}\ \vec{y}\ \{\beta\}.$$

Luego por Lem. 3.4.2 se tiene que

$$W \models \vec{x}, \vec{z} : [\alpha,\ \psi]\ {}^{\mathsf{u}(S)}_{\mathsf{l}(S)} \sqsubseteq S,\ W \models \vec{z}, \vec{y} : [\psi,\ \beta]\ {}^{\mathsf{u}(T)}_{\mathsf{l}(T)} \sqsubseteq T$$

y por hipótesis inductiva que

$$W \vdash \vec{x}, \vec{z} : [\alpha,\ \psi]\ {}^{\mathsf{u}(S)}_{\mathsf{l}(S)} \sqsubseteq S,\ W \vdash \vec{z}, \vec{y} : [\psi,\ \beta]\ {}^{\mathsf{u}(T)}_{\mathsf{l}(T)} \sqsubseteq T.$$

Así, se tiene que la deducción

| | | |
|---|---|---|
| (1) | $\alpha \Rightarrow l \leq \mathsf{l}(S)$ | (Hipótesis) |
| (2) | $\alpha \Rightarrow \mathsf{u}(S) + \mathsf{u}(T) \leq u$ | (Hipótesis) |
| (3) | $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l} \sqsubseteq \vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\mathsf{u}(S)+\mathsf{u}(T)}_{\mathsf{l}(S)}$ | ($TIME$ 1,2) |
| (4) | $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\mathsf{u}(S)+\mathsf{u}(T)}_{\mathsf{l}(S)} \sqsubseteq \vec{x}, \vec{z} : [\alpha,\ \psi]\ {}^{\mathsf{u}(S)}_{\mathsf{l}(S)}; \vec{z}, \vec{y} : [\psi,\ \beta]\ {}^{\mathsf{u}(T)}_{\mathsf{l}(T)}$ | ($SEC$) |
| (5) | $\vec{x}, \vec{z} : [\alpha,\ \psi]\ {}^{\mathsf{u}(S)}_{\mathsf{l}(S)} \sqsubseteq S$ | (Hipótesis) |

(6) $\vec{z}, \vec{y} : [\psi,\ \beta]\ {}^{\mathsf{u}(T)}_{\mathsf{l}(T)} \sqsubseteq T$ (Hipótesis)

(7) $\vec{x}, \vec{z} : [\alpha,\ \psi]\ {}^{\mathsf{u}(S)}_{\mathsf{l}(S)}; \vec{z}, \vec{y} : [\psi,\ \beta]\ {}^{\mathsf{u}(T)}_{\mathsf{l}(T)} \sqsubseteq S;T$ ($MNSEC$ 5,6)

(8) $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l} \sqsubseteq S;T$ ($TRAN$ 3,4,7)

es una deducción para $r$ desde $W$. Por lo tanto $W \vdash r$.

Caso 2: $R \equiv S+T$. Si $W \models r$ entonces por Lem. 3.4.2 se tiene que $W' \models \{\alpha\}\ \vec{x}\ {}_{l}S+T^{u}\ \vec{y}\ \{\beta\}$. Luego, por la demostración de Teo. 2.4.2 se tiene que

$$W \vdash \alpha \Rightarrow l \leq min\{\mathsf{l}(S), \mathsf{l}(T)\},\ W \vdash \alpha \Rightarrow max\{\mathsf{u}(S), \mathsf{u}(T)\} \leq u$$

y

$$W' \models \{\alpha\}\ \vec{x}\ {}_{\mathsf{l}(S)}S^{\mathsf{u}(S)}\ \vec{y}\ \{\beta\},\ W' \models \{\alpha\}\ \vec{x}\ {}_{\mathsf{l}(T)}T^{\mathsf{u}(T)}\ \vec{y}\ \{\beta\}.$$

Luego por Lem. 3.4.2 se tiene que

$$W \models \vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\mathsf{u}(S)}_{\mathsf{l}(S)} \sqsubseteq S,\ W \models \vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\mathsf{u}(T)}_{\mathsf{l}(T)} \sqsubseteq T$$

y por hipótesis inductiva que

$$W \vdash \vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\mathsf{u}(S)}_{\mathsf{l}(S)} \sqsubseteq S,\ W \vdash \vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\mathsf{u}(T)}_{\mathsf{l}(T)} \sqsubseteq T.$$

Sean $v$ y $w$ los términos $min\{\mathsf{l}(S), \mathsf{l}(T)\}$ y $max\{\mathsf{u}(S), \mathsf{u}(T)\}$ respectivamente. Así, se tiene que la deducción

(1) $\alpha \Rightarrow l \leq v$ (Hipótesis)

(2) $\alpha \Rightarrow w \leq u$ (Hipótesis)

(3) $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l} \sqsubseteq \vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{w}_{v}$ ($TIME$ 1,2)

(4) $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{w}_{v} \sqsubseteq \vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\mathsf{u}(S)}_{\mathsf{l}(S)} + \vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\mathsf{u}(T)}_{\mathsf{l}(T)}$ ($CHC$)

(5) $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\mathsf{u}(S)}_{\mathsf{l}(S)} \sqsubseteq S$ (Hipótesis)

(6) $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\mathsf{u}(T)}_{\mathsf{l}(T)} \sqsubseteq T$ (Hipótesis)

(7) $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\mathsf{u}(S)}_{\mathsf{l}(S)} + \vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\mathsf{u}(T)}_{\mathsf{l}(T)} \sqsubseteq S+T$ ($MNCHC$ 5,6)

(8) $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l} \sqsubseteq S+T$ ($TRAN$ 3,4,7)

es una deducción para $r$ desde $W$. Por lo tanto $W \vdash r$.

Caso 3: $R \equiv S \cdot T$. Si $W \models r$ entonces por Lem. 3.4.2 se tiene que $W' \models \{\alpha\}\ \vec{x}\ {}_{l}S \cdot T^{u}\ \vec{y}\ \{\beta\}$. Luego, por la demostración de Teo. 2.4.2 se tiene que

$$W \vdash \alpha \Rightarrow l \leq max\{\mathsf{l}(S), \mathsf{l}(T)\},\ W \vdash \alpha \Rightarrow max\{\mathsf{u}(S), \mathsf{u}(T)\} \leq u$$

y

$$W' \models \{\alpha\}\ \vec{x}\ {}_{\mathsf{l}(S)}S^{\mathsf{u}(S)}\ \vec{y}\ \{\beta\},\ W' \models \{\alpha\}\ \vec{x}\ {}_{\mathsf{l}(T)}T^{\mathsf{u}(T)}\ \vec{y}\ \{true\}.$$

Luego por Lem. 3.4.2 se tiene que

$$W \models \vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\mathsf{u}(S)}_{\mathsf{l}(S)} \sqsubseteq S,\ W \models \vec{x}, \vec{y} : [\alpha,\ true]\ {}^{\mathsf{u}(T)}_{\mathsf{l}(T)} \sqsubseteq T$$

y por hipótesis inductiva que

$$W \vdash \vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\mathsf{u}(S)}_{\mathsf{l}(S)} \sqsubseteq S,\ W \vdash \vec{x}, \vec{y} : [\alpha,\ true]\ {}^{\mathsf{u}(T)}_{\mathsf{l}(T)} \sqsubseteq T.$$

Sean $v$ y $w$ los términos $max\{\mathsf{l}(S), \mathsf{l}(T)\}$ y $max\{\mathsf{u}(S), \mathsf{u}(T)\}$ respectivamente. Así, se tiene que la deducción

| | | |
|---|---|---|
| (1) | $\alpha \Rightarrow l \leq v$ | (Hipótesis) |
| (2) | $\alpha \Rightarrow w \leq u$ | (Hipótesis) |
| (3) | $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l} \sqsubseteq \vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{w}_{v}$ | ($TIME$ 1,2) |
| (4) | $\beta \wedge true \Rightarrow \beta$ | (Lógica) |
| (5) | $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{w}_{v} \sqsubseteq \vec{x}, \vec{y} : [\alpha,\ \beta \wedge true]\ {}^{w}_{v}$ | ($CONS$ 4) |
| (6) | $\vec{x}, \vec{y} : [\alpha,\ \beta \wedge true]\ {}^{w}_{v} \sqsubseteq \vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\mathsf{u}(S)}_{\mathsf{l}(S)} \cdot \vec{x}, \vec{y} : [\alpha,\ true]\ {}^{\mathsf{u}(T)}_{\mathsf{l}(T)}$ | ($PAR$) |
| (7) | $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\mathsf{u}(S)}_{\mathsf{l}(S)} \sqsubseteq S$ | (Hipótesis) |
| (8) | $\vec{x}, \vec{y} : [\alpha,\ true]\ {}^{\mathsf{u}(T)}_{\mathsf{l}(T)} \sqsubseteq T$ | (Hipótesis) |
| (9) | $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\mathsf{u}(S)}_{\mathsf{l}(S)} \cdot \vec{x}, \vec{y} : [\alpha,\ true]\ {}^{\mathsf{u}(T)}_{\mathsf{l}(T)} \sqsubseteq S \cdot T$ | ($MNPAR$ 7,8) |
| (10) | $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l} \sqsubseteq S \cdot T$ | ($TRAN$ 3,5,6,9) |

es una deducción para $r$ desde $W$. Por lo tanto $W \vdash r$.

Caso 4: $R \equiv S^*$. Si $W \models r$ entonces por Lem. 3.4.2 se tiene que $W' \models \{\alpha\}\ \vec{x}\ {}_{l}S^{*\,u}\ \vec{y}\ \{\beta\}$. Luego, por la demostración de Teo. 2.4.2 se tiene que

$$W \vdash \alpha \Rightarrow l \leq 0,\ W \vdash \alpha \Rightarrow \infty \leq u,\ \alpha \Rightarrow \beta[\vec{x}/\vec{y}]$$

y

$$W' \models \{\beta[\vec{x}/\vec{y}]\}\ \vec{x}\ {}_{l}S^{u}\ \vec{x}\ \{\beta[\vec{x}/\vec{y}]\}.$$

Luego por Lem. 3.4.2 se tiene que $W \models \vec{x}, \vec{x} : [\beta[\vec{x}/\vec{y}],\ \beta[\vec{x}/\vec{y}]]\ {}^{u}_{l} \sqsubseteq S$ y por hipótesis

inductiva que $W \vdash \vec{x}, \vec{x} : [\beta[\vec{x}/\vec{y}],\ \beta[\vec{x}/\vec{y}]]\ {}^{u}_{l} \sqsubseteq S$. Así se tiene que la deducción

| | | |
|---|---|---|
| (1) | $\alpha \Rightarrow l \leq 0$ | (Hipótesis) |
| (2) | $\alpha \Rightarrow \infty \leq u$ | (Hipótesis) |
| (3) | $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l} \sqsubseteq \vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\infty}_{0}$ | ($TIME$ 1,2) |
| (4) | $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\infty}_{0} \sqsubseteq \vec{x}, \vec{x} : [\alpha,\ \beta[\vec{x}/\vec{y}]]\ {}^{\infty}_{0}$ | ($VAR$) |
| (5) | $\alpha \Rightarrow \beta[\vec{x}/\vec{y}]$ | (Hipótesis) |
| (6) | $\vec{x}, \vec{x} : [\alpha,\ \beta[\vec{x}/\vec{y}]]\ {}^{\infty}_{0} \sqsubseteq \vec{x}, \vec{x} : [\beta[\vec{x}/\vec{y}],\ \beta[\vec{x}/\vec{y}]]\ {}^{\infty}_{0}$ | ($CONS$ 5) |
| (7) | $\vec{x}, \vec{x} : [\beta[\vec{x}/\vec{y}],\ \beta[\vec{x}/\vec{y}]]\ {}^{\infty}_{0} \sqsubseteq (\vec{x}, \vec{x} : [\beta[\vec{x}/\vec{y}],\ \beta[\vec{x}/\vec{y}]]\ {}^{u}_{l})^{*}$ | ($ITE$) |
| (8) | $\vec{x}, \vec{x} : [\beta[\vec{x}/\vec{y}],\ \beta[\vec{x}/\vec{y}]]\ {}^{u}_{l} \sqsubseteq S$ | (Hipótesis) |
| (9) | $(\vec{x}, \vec{x} : [\beta[\vec{x}/\vec{y}],\ \beta[\vec{x}/\vec{y}]]\ {}^{u}_{l})^{*} \sqsubseteq S^{*}$ | ($MNITE$ 8) |
| (10) | $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l} \sqsubseteq S^{*}$ | ($TRAN$ 3,4,6,7,8) |

es una deducción para $r$ desde $W$. Por lo tanto $W \vdash r$.

■

Se ha visto en esta última sección que existe un cálculo consistente y completo (en el sentido expuesto) para el conjunto de fórmulas de refinamiento que son consecuencia lógica del conjunto $Th(\mathcal{A}) \cup RTh(\mathcal{A})$ donde $\mathcal{A}$ es una estructura de objeto expresiva. De forma análoga al cálculo de Hoare de la segunda parte del trabajo, existe una forma alternativa de aplicar el cálculo de refinamientos cuando la teoría es *axiomatizable*. Se dice que una teoría $RTh(\mathcal{A})$ es axiomatizable cuando existe un conjunto decidible $W \subseteq RFor(\mathcal{S})$ tal que $RTh(\mathcal{A})$ es el conjunto de todas las fórmulas de refinamiento derivables desde $Th(\mathcal{A}) \cup W$ en el cálculo de refinamientos. En tal caso, el cálculo de refinamientos se aumenta con los axiomas de la teoría (es decir, $W$). Las derivaciones de interés son entonces las derivaciones en este cálculo extendido a partir de $Th(\mathcal{A})$. Esta visión alternativa no fue adoptada aquí porque sólo es aplicable a teorías axiomatizables, sin embargo, en los ejemplos prácticos se usará, ya que las teorías involucradas serán axiomatizables.

EJEMPLO 3.4.1 Considérese la interpretación usual $\mathcal{I}$ de la aritmética de Peano, donde además se incluye una única acción atómica $Inc$ tal que $Inc^{\mathcal{I}} = \{\, \langle\, n, n+1 \,\rangle : n \in \mathsf{Nat}, n \geq 0 \,\}$ con $l_{Inc} = 0$ y $u_{Inc} = 1$. Luego, la teoría $RTh(\mathcal{I})$ es axiomatizable con el esquema de axioma $\langle\, x \,\rangle,\langle\, x \,\rangle : [\alpha[x+1/x],\ \alpha]\ {}^{1}_{0} \sqsubseteq Inc$. Así, por ejemplo se tiene que la fórmula

$$\langle\, y \,\rangle,\langle\, z \,\rangle : [y = 0,\ z + 1 = 3]\ {}^{3}_{0} \sqsubseteq Inc; Inc$$

es derivable desde $Th(\mathcal{I})$ en el cálculo extendido según la siguiente deducción:

| | | |
|---|---|---|
| (1) | $\langle\, y \,\rangle,\langle\, z \,\rangle : [y = 0,\ z + 1 = 3]\ {}^{3}_{0} \sqsubseteq \langle\, x \,\rangle,\langle\, x \,\rangle : [x = 0,\ x + 1 = 3]\ {}^{3}_{0}$ | ($VAR$) |
| (2) | $x = 0 \Rightarrow 1 + 1 \leq 3$ | ($Th(\mathcal{I})$) |
| (3) | $\langle\, x \,\rangle,\langle\, x \,\rangle : [x = 0,\ x + 1 = 3]\ {}^{3}_{0} \sqsubseteq \langle\, x \,\rangle,\langle\, x \,\rangle : [x = 0,\ x + 1 = 3]\ {}^{1+1}_{0}$ | ($TIME$ 2) |
| (4) | $\langle\, x \,\rangle,\langle\, x \,\rangle : [x = 0,\ x + 1 = 3]\ {}^{1+1}_{0}$ $\sqsubseteq \langle\, x \,\rangle,\langle\, x \,\rangle : [x = 0,\ x = 1]\ {}^{1}_{0}\, ;\, \langle\, x \,\rangle,\langle\, x \,\rangle : [x = 1,\ x + 1 = 3]\ {}^{1}_{0}$ | ($SEC$) |
| (5) | $x = 0 \Rightarrow x + 1 = 1$ | ($Th(\mathcal{I})$) |

| | | |
|---|---|---|
| (6) | $\langle x \rangle,\langle x \rangle : [x = 0,\ x = 1]\ {}^{1}_{0} \sqsubseteq \langle x \rangle,\langle x \rangle : [x + 1 = 1,\ x = 1]\ {}^{1}_{0}$ | ($CONS$ 5) |
| (7) | $\langle x \rangle,\langle x \rangle : [x + 1 = 1,\ x = 1]\ {}^{1}_{0} \sqsubseteq Inc$ | (Axioma) |
| (8) | $\langle x \rangle,\langle x \rangle : [x = 0,\ x = 1]\ {}^{1}_{0} \sqsubseteq Inc$ | ($TRAN$ 6,7) |
| (9) | $x = 1 \Rightarrow x + 1 + 1 = 3$ | ($Th(\mathcal{I})$) |
| (10) | $\langle x \rangle,\langle x \rangle : [x = 1,\ x + 1 = 3]\ {}^{1}_{0} \sqsubseteq \langle x \rangle,\langle x \rangle : [x + 1 + 1 = 3,\ x + 1 = 3]\ {}^{1}_{0}$ | ($CONS$ 9) |
| (11) | $\langle x \rangle,\langle x \rangle : [x + 1 + 1 = 3,\ x + 1 = 3]\ {}^{1}_{0} \sqsubseteq Inc$ | (Axioma) |
| (12) | $\langle x \rangle,\langle x \rangle : [x = 1,\ x + 1 = 3]\ {}^{1}_{0} \sqsubseteq Inc$ | ($TRAN$ 10,11) |
| (13) | $\langle x \rangle,\langle x \rangle : [x = 0,\ x = 1]\ {}^{1}_{0}; \langle x \rangle,\langle x \rangle : [x = 1,\ x + 1 = 3]\ {}^{1}_{0} \sqsubseteq Inc; Inc$ | ($MNSEC$ 8,12) |
| (14) | $\langle y \rangle,\langle z \rangle : [y = 0,\ z + 1 = 3]\ {}^{3}_{0} \sqsubseteq Inc; Inc$ | ($TRAN$ 1,3,4,13) |

■

Por otro lado, y por razones de generalidad, tampoco aquí se ha asumido que la teoría $Th(\mathcal{A})$ es axiomatizable. En caso de serlo, el cálculo de refinamientos se aumenta con los axiomas y reglas de deducción del cálculo de la lógica multisort y con los axiomas de $Th(\mathcal{A})$. Las derivaciones de interés son entonces las derivaciones en este cálculo extendido a partir del conjunto vacío.

## 3.5 Otras reglas derivadas

A continuación se presentan reglas derivadas para la clase especial de procesos (similares a los comandos guardados de Dijkstra) definida en la Sección 2.5. Las siguientes son reglas derivadas para los dos primeros tipos de procesos:

(ii') *Regla IF*: Siendo $\vec{z_i}$ las variables libres de $\gamma_i$

$$\frac{}{\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\epsilon + max_i\{u_i\}}_{\epsilon} \sqsubseteq \textbf{if } []i \bullet \gamma_i \rightarrow \vec{x}, \vec{y} : [\gamma_i[\vec{x}/\vec{z_i}] \wedge \alpha,\ \beta]\ {}^{u_i}_{l_i} \textbf{ fi}}$$

(iii') *Regla DO*: Siendo $\vec{z_i}$ las variables libres de $\gamma_i$

$$\frac{}{\vec{x}, \vec{x} : [\psi,\ \neg(\bigvee_i \gamma_i[\vec{x}/\vec{z_i}]) \wedge \psi]\ {}^{t * max_i\{u_i\}}_{\epsilon} \sqsubseteq \textbf{do } []i \bullet \gamma_i \rightarrow \vec{x}, \vec{x} : [\gamma_i[\vec{x}/\vec{z_i}] \wedge \psi \wedge t = t_0,\ \psi \wedge t < t_0]\ {}^{u_i}_{l_i} \textbf{ od}}$$

(iv') *Regla MNIF*

$$\frac{R_i \sqsubseteq R_i',\ i = 1..n}{\textbf{if } []i \bullet \gamma_i \rightarrow R_i \textbf{ fi} \sqsubseteq \textbf{if } []i \bullet \gamma_i \rightarrow R_i' \textbf{ fi}}$$

(v') *Regla MNDO*

$$\frac{R_i \sqsubseteq R_i' \; i = 1..n}{\mathbf{do}\ []i \bullet \gamma_i \to R_i\ \mathbf{od} \sqsubseteq \mathbf{do}\ []i \bullet \gamma_i \to R_i'\ \mathbf{od}}$$

La regla derivada $IF$ resulta de la siguiente deducción (a partir de sus premisas y de una teoría arbitraria):

(1) $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\epsilon+max\{u_i\}}_{\epsilon} \sqsubseteq \vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\epsilon+u_1}_{\epsilon} + \ldots + \vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\epsilon+u_n}_{\epsilon}$ $(CHC)$

(2) $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\epsilon+u_i}_{\epsilon} \sqsubseteq \vec{x}, \vec{x} : [\alpha,\ \gamma_i[\vec{x}/\vec{z_i}] \wedge \alpha]\ {}^{\epsilon}_{\epsilon}; \vec{x}, \vec{y} : [\gamma_i[\vec{x}/\vec{z_i}] \wedge \alpha,\ \beta]\ {}^{u_i}_{\epsilon}$ $(SEC)$

(3) $\alpha \Rightarrow (\gamma_i[\vec{x}/\vec{z_i}] \Rightarrow \gamma_i[\vec{x}/\vec{z_i}] \wedge \alpha)$ (Lógica)

(4) $\vec{x}, \vec{x} : [\alpha,\ \gamma_i[\vec{x}/\vec{z_i}] \wedge \alpha]\ {}^{\epsilon}_{\epsilon} \sqsubseteq \vec{x}, \vec{x} : [\gamma_i[\vec{x}/\vec{z_i}] \Rightarrow \gamma_i[\vec{x}/\vec{z_i}] \wedge \alpha,\ \gamma_i[\vec{x}/\vec{z_i}] \wedge \alpha]\ {}^{\epsilon}_{\epsilon}$ $(CONS\ 3)$

(5) $\vec{x}, \vec{x} : [\gamma_i[\vec{x}/\vec{z_i}] \Rightarrow \gamma_i[\vec{x}/\vec{z_i}] \wedge \alpha,\ \gamma_i[\vec{x}/\vec{z_i}] \wedge \alpha]\ {}^{\epsilon}_{\epsilon} \sqsubseteq \gamma_i?$ $(TEST)$

(6) $\vec{x}, \vec{x} : [\alpha,\ \gamma_i[\vec{x}/\vec{z_i}] \wedge \alpha]\ {}^{\epsilon}_{\epsilon} \sqsubseteq \gamma_i?$ $(TRAN\ 4{,}5)$

(7) $\vec{x}, \vec{y} : [\gamma_i[\vec{x}/\vec{z_i}] \wedge \alpha,\ \beta]\ {}^{u_i}_{\epsilon} \sqsubseteq \vec{x}, \vec{y} : [\gamma_i[\vec{x}/\vec{z_i}] \wedge \alpha,\ \beta]\ {}^{u_i}_{\epsilon}$ $(REF)$

(8) $\vec{x}, \vec{x} : [\alpha,\ \gamma_i[\vec{x}/\vec{z_i}] \wedge \alpha]\ {}^{\epsilon}_{\epsilon}; \vec{x}, \vec{y} : [\gamma_i[\vec{x}/\vec{z_i}] \wedge \alpha,\ \beta]\ {}^{u_i}_{\epsilon}$
$\sqsubseteq \gamma_i?; \vec{x}, \vec{y} : [\gamma_i[\vec{x}/\vec{z_i}] \wedge \alpha,\ \beta]\ {}^{u_i}_{\epsilon}$ $(MNSEC\ 6{,}7)$

(9) $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\epsilon+u_i}_{\epsilon} \sqsubseteq \gamma_i; \vec{x}, \vec{y} : [\gamma_i[\vec{x}/\vec{z_i}] \wedge \alpha,\ \beta]\ {}^{u_i}_{\epsilon}$ $(TRAN\ 2{,}8)$

(10) $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\epsilon+u_1}_{\epsilon} + \ldots + \vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\epsilon+u_n}_{\epsilon}$
$\sqsubseteq \mathbf{if}\ []i \bullet \gamma_i \to \vec{x}, \vec{y} : [\gamma_i[\vec{x}/\vec{z_i}] \wedge \alpha,\ \beta]\ {}^{u_i}_{l_i}\ \mathbf{fi}$ $(MNCHC\ 9)$

(11) $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\epsilon+max\{u_i\}}_{\epsilon} \sqsubseteq \mathbf{if}\ []i \bullet \gamma_i \to \vec{x}, \vec{y} : [\gamma_i[\vec{x}/\vec{z_i}] \wedge \alpha,\ \beta]\ {}^{u_i}_{l_i}\ \mathbf{fi}$ $(TRAN\ 1{,}10)$

La regla derivada $MNIF$ resulta de la siguiente deducción:

(1) $R_i \sqsubseteq R_i'$ (Hipótesis)

(2) $\gamma_i? \sqsubseteq \gamma_i?$ $(REF)$

(3) $\gamma_i?; R_i \sqsubseteq \gamma_i?; R_i'$ $(MNSEC\ 1{,}2)$

(4) $\mathbf{if}\ []i \bullet \gamma_i \to R_i\ \mathbf{fi} \sqsubseteq \mathbf{if}\ []i \bullet \gamma_i \to R_i'\ \mathbf{fi}$ $(MNCHC\ 3)$

La regla derivada $DO$ resulta de la siguiente deducción (a partir de sus premisas y de una teoría arbitraria):

(1) $\vec{x}, \vec{x} : [\psi,\ \neg(\bigvee_i \gamma_i[\vec{x}/\vec{z_i}]) \wedge \psi]\ {}^{\infty}_{0}$

$\sqsubseteq \vec{x}, \vec{x} : [\psi,\ \psi]\ {}^{\infty}_{0}; \vec{x}, \vec{x} : [\psi,\ \neg(\bigvee_i \gamma_i[\vec{x}/\vec{z_i}]) \wedge \psi]\ {}^{\infty}_{0}$ $(SEC)$

(2) $\vec{x}, \vec{x} : [\psi,\ \psi]\ {}^{\infty}_{0} \sqsubseteq (\vec{x}, \vec{x} : [\psi,\ \psi]\ {}^{\infty}_{0})^*$ $(ITE)$

(3) $\vec{x}, \vec{x} : [\psi,\ \psi]\ {}^{\infty}_{0} \sqsubseteq \textbf{if}\ []i \bullet \gamma_i \rightarrow \vec{x}, \vec{y} : [\gamma_i[\vec{x}/\vec{z_i}] \wedge \psi,\ \psi]\ {}^{u_i}_{l_i}\ \textbf{fi}$ $(IF)$

(4) $\gamma_i[\vec{x}/\vec{z_i}] \wedge \psi \Rightarrow \gamma_i[\vec{x}/\vec{z_i}] \wedge \psi \wedge t = t_0$ (Lógica)

(5) $\psi \wedge t < t_0 \Rightarrow \psi$ (Lógica)

(6) $\vec{x}, \vec{y} : [\gamma_i[\vec{x}/\vec{z_i}] \wedge \psi,\ \psi]\ {}^{u_i}_{l_i} \sqsubseteq \vec{x}, \vec{y} : [\gamma_i[\vec{x}/\vec{z_i}] \wedge \psi \wedge t = t_0,\ \psi \wedge t < t_0]\ {}^{u_i}_{l_i}$ $(CONS\ 4{,}5)$

(7) $\textbf{if}\ []i \bullet \gamma_i \rightarrow \vec{x}, \vec{y} : [\gamma_i[\vec{x}/\vec{z_i}] \wedge \psi,\ \psi]\ {}^{u_i}_{l_i}\ \textbf{fi}$

$\sqsubseteq \textbf{if}\ []i \bullet \gamma_i \rightarrow \vec{x}, \vec{y} : [\gamma_i[\vec{x}/\vec{z_i}] \wedge \psi \wedge t = t_0,\ \psi \wedge t < t_0]\ {}^{u_i}_{l_i}\ \textbf{fi}$ $(MNIF\ 6)$

(8) $\vec{x}, \vec{x} : [\psi,\ \psi]\ {}^{\infty}_{0} \sqsubseteq \textbf{if}\ []i \bullet \gamma_i \rightarrow \vec{x}, \vec{y} : [\gamma_i[\vec{x}/\vec{z_i}] \wedge \psi \wedge t = t_0,\ \psi \wedge t < t_0]\ {}^{u_i}_{l_i}\ \textbf{fi}$ $(TRAN\ 3{,}7)$

(9) $(\vec{x}, \vec{x} : [\psi,\ \psi]\ {}^{\infty}_{0})^*$

$\sqsubseteq (\textbf{if}\ []i \bullet \gamma_i \rightarrow \vec{x}, \vec{y} : [\gamma_i[\vec{x}/\vec{z_i}] \wedge \psi \wedge t = t_0,\ \psi \wedge t < t_0]\ {}^{u_i}_{l_i}\ \textbf{fi})^*$ $(MNITE\ 3)$

(10) $\vec{x}, \vec{x} : [\psi,\ \psi]\ {}^{\infty}_{0}$

$\sqsubseteq (\textbf{if}\ []i \bullet \gamma_i \rightarrow \vec{x}, \vec{y} : [\gamma_i[\vec{x}/\vec{z_i}] \wedge \psi \wedge t = t_0,\ \psi \wedge t < t_0]\ {}^{u_i}_{l_i}\ \textbf{fi})^*$ $(TRAN\ 2{,}9)$

(11) $\vec{x}, \vec{x} : [\psi,\ \neg(\bigvee_i \gamma_i[\vec{x}/\vec{z_i}]) \wedge \psi]\ {}^{\infty}_{0} \sqsubseteq \vec{x}, \vec{x} : [\psi,\ \neg\gamma_1[\vec{x}/\vec{z_1}] \wedge \psi]\ {}^{\infty}_{0}; \ldots;$

$\vec{x}, \vec{x} : [\neg \bigvee_{i=1}^{n-1} \gamma_i[\vec{x}/\vec{z_i}] \wedge \psi,\ \neg \bigvee_i \gamma_i[\vec{x}/\vec{z_i}] \wedge \psi]\ {}^{\infty}_{0}$ $(SEC)$

(12) $\psi \Rightarrow (\neg\gamma_1[\vec{x}/\vec{z_1}] \Rightarrow \neg\gamma_1[\vec{x}/\vec{z_1}] \wedge \psi)$ (Lógica)

(13) $\vec{x}, \vec{x} : [\psi,\ \neg\gamma_1[\vec{x}/\vec{z_1}] \wedge \psi]\ {}^{\infty}_{0}$

$\sqsubseteq \vec{x}, \vec{x} : [\neg\gamma_1[\vec{x}/\vec{z_1}] \Rightarrow \neg\gamma_1[\vec{x}/\vec{z_1}] \wedge \psi,\ \neg\gamma_1[\vec{x}/\vec{z_1}] \wedge \psi]\ {}^{\infty}_{0}$ $(CONS\ 12)$

(14) $\vec{x}, \vec{x} : [\neg\gamma_1[\vec{x}/\vec{z_1}] \Rightarrow \neg\gamma_1[\vec{x}/\vec{z_1}] \wedge \psi,\ \neg\gamma_1[\vec{x}/\vec{z_1}] \wedge \psi]\ {}^{\infty}_{0} \sqsubseteq \neg\gamma_1?$ $(TEST)$

(15) $\vec{x}, \vec{x} : [\psi,\ \neg\gamma_1[\vec{x}/\vec{z_1}] \wedge \psi]\ {}^{\infty}_{0} \sqsubseteq \neg\gamma_1?$ $(TRAN\ 13{,}14)$

$\ldots$

(16) $\vec{x}, \vec{x} : [\neg \bigvee_{i=1}^{n-1} \gamma_i[\vec{x}/\vec{z_i}] \wedge \psi,\ \neg \bigvee_i \gamma_i[\vec{x}/\vec{z_i}] \wedge \psi]\ {}^{\infty}_{0} \sqsubseteq \neg\gamma_n?$ $(TEST)$

(17) $\vec{x}, \vec{x} : [\psi,\ \neg\gamma_1[\vec{x}/\vec{z_1}] \wedge \psi]\ {}^{\infty}_{0}; \ldots;$

$\vec{x}, \vec{x} : [\neg \bigvee_{i=1}^{n-1} \gamma_i[\vec{x}/\vec{z_i}] \wedge \psi,\ \neg \bigvee_i \gamma_i[\vec{x}/\vec{z_i}] \wedge \psi]\ {}^{\infty}_{0}$

$\sqsubseteq \neg\gamma_1?; \ldots; \neg\gamma_n?$ $(MNSEC\ 15{,}16)$

(18) $\vec{x}, \vec{x} : [\psi,\ \neg(\bigvee_i \gamma_i[\vec{x}/\vec{z_i}]) \wedge \psi]\ {}^{\infty}_{0} \sqsubseteq \neg\gamma_1?; \ldots; \neg\gamma_n?$ $(TRAN\ 11{,}17)$

(19) $\vec{x}, \vec{x} : [\psi,\ \psi]\ {}^{\infty}_{0}; \vec{x}, \vec{x} : [\psi,\ \neg(\bigvee_i \gamma_i[\vec{x}/\vec{z_i}]) \wedge \psi]\ {}^{\infty}_{0}$

$\sqsubseteq$ **do** $[]i \bullet \gamma_i \rightarrow \vec{x}, \vec{y} : [\gamma_i[\vec{x}/\vec{z_i}] \wedge \psi \wedge t = t_0,\ \psi \wedge t < t_0]\ {}^{u_i}_{l_i}$ **od** ($MNSEC$ 10,18)

(20) $\vec{x}, \vec{x} : [\psi,\ \neg(\bigvee_i \gamma_i[\vec{x}/\vec{z_i}]) \wedge \psi]\ {}^{\infty}_{0}$

$\sqsubseteq$ **do** $[]i \bullet \gamma_i \rightarrow \vec{x}, \vec{y} : [\gamma_i[\vec{x}/\vec{z_i}] \wedge \psi \wedge t = t_0,\ \psi \wedge t < t_0]\ {}^{u_i}_{l_i}$ **od** ($TRAN$ 1,19)

La regla derivada $MNDO$ resulta de la siguiente deducción:

| | | |
|---|---|---|
| (1) | $R_i \sqsubseteq R'_i$ | (Hipótesis) |
| (2) | **if** $[]i \bullet \gamma_i \rightarrow R_i$ **fi** $\sqsubseteq$ **if** $[]i \bullet \gamma_i \rightarrow R'_i$ **fi** | ($MNIF$ 1) |
| (3) | (**if** $[]i \bullet \gamma_i \rightarrow R_i$ **fi**)$^*$ $\sqsubseteq$ (**if** $[]i \bullet \gamma_i \rightarrow R'_i$ **fi**)$^*$ | ($MNITE$ 2) |
| (4) | $\neg\gamma_1?; \ldots; \neg\gamma_n? \sqsubseteq \neg\gamma_1?; \ldots; \neg\gamma_n?$ | ($REF$) |
| (5) | **do** $[]i \bullet \gamma_i \rightarrow R_i$ **od** $\sqsubseteq$ **do** $[]i \bullet \gamma_i \rightarrow R'_i$ **od** | ($MNSEC$ 3,4) |

Aquí también, nótese que las cotas de tiempo en la regla $DO$ no pueden derivarse, pero se asumen como verdaderas. En forma inmediata es posible obtener reglas derivadas para los dos últimos tipos de procesos.

(vi') *Regla IFT*: Siendo $\vec{z}$ las variables libres de $\gamma$

$$\frac{}{\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{\epsilon+max\{u,w\}}_{\epsilon} \sqsubseteq \textbf{if } \gamma \textbf{ then } \vec{x}, \vec{y} : [\gamma[\vec{x}/\vec{z}] \wedge \alpha,\ \beta]\ {}^{u}_{l} \textbf{ else } \vec{x}, \vec{y} : [\neg\gamma[\vec{x}/\vec{z}] \wedge \alpha,\ \beta]\ {}^{w}_{v}}$$

(vii') *Regla WD*: Siendo $\vec{z}$ las variables libres de $\gamma$

$$\frac{}{\vec{x}, \vec{x} : [\psi,\ \neg\gamma[\vec{x}/\vec{z}] \wedge \psi]\ {}^{t*u}_{\epsilon} \sqsubseteq \textbf{while } \gamma \textbf{ do } \vec{x}, \vec{x} : [\gamma[\vec{x}/\vec{z}] \wedge \psi \wedge t = t_0,\ \psi \wedge t < t_0]\ {}^{u}_{l}}$$

(viii') *Regla MNIFT*

$$\frac{R \sqsubseteq R' \qquad S \sqsubseteq S'}{\textbf{if } \gamma \textbf{ then } R \textbf{ else } S \sqsubseteq \textbf{if } \gamma \textbf{ then } R' \textbf{ else } S'}$$

(ix') *Regla MNWD*

$$\frac{R \sqsubseteq R'}{\textbf{while } \gamma \textbf{ do } R \sqsubseteq \textbf{while } \gamma \textbf{ do } R'}$$

## 3.6 Ejemplos

En esta sección se darán algunos ejemplos de refinamiento de procesos en $P/PML$ usando el cálculo de refinamientos presentado en las secciones previas. Para simplificar las derivaciones, no se hará uso explícito de las reglas $REF$, $TRAN$ ni de las reglas de monotonicidad. Además, no se harán explícitas las premisas para las reglas $CONS$ y $TIME$. Para los ejemplos, se asumirá la existencia de una estructura de objeto $\mathcal{A}$ (sobre una signatura $\mathcal{S}$ adecuada) que contiene sólo las acciones atómicas descriptas en la Sección 2.6. Esta estructura de objeto representa la máquina abstracta sobre la cual se deberán construir los procesos que implementen las especificaciones. En este caso en particular, la teoría $RTh(\mathcal{A})$ es axiomatizable con los siguientes esquemas de axioma: Siendo $\alpha \in For(\mathcal{S})$, $x, y, z, w$ variables de sort $Int$, $c$ una variable de sort $Coin$ y $s$ una variable de sort $String$,

- *Axioma Inc*:
$$\langle x \rangle, \langle y \rangle : [\alpha[x+1/y],\ \alpha]\ {}^{1}_{0} \sqsubseteq Inc$$
- *Axioma Dec*:
$$\langle x \rangle, \langle y \rangle : [\alpha[x-1/y],\ \alpha]\ {}^{1}_{0} \sqsubseteq Dec$$
- *Axioma Neg*:
$$\langle x \rangle, \langle y \rangle : [\alpha[-x/y],\ \alpha]\ {}^{2*\epsilon}_{\epsilon} \sqsubseteq Neg$$
- *Axioma Decby2*:
$$\langle x \rangle, \langle y \rangle : [\alpha[x-2/y],\ \alpha]\ {}^{2}_{0} \sqsubseteq Decby2$$
- *Axioma Join*:
$$\langle x, y \rangle, \langle z \rangle : [\alpha[x/z] \wedge \alpha[y/z],\ \alpha]\ {}^{0}_{0} \sqsubseteq Join$$
- *Axioma Sum*:
$$\langle x, y \rangle, \langle z \rangle : [\alpha[x+y/z],\ \alpha]\ {}^{2}_{0} \sqsubseteq Sum$$
- *Axioma Swap*:
$$\langle x, y \rangle, \langle z, w \rangle : [\alpha[y, x/z, w],\ \alpha]\ {}^{4}_{1} \sqsubseteq Swap$$
- *Axioma Zerofst*:
$$\langle x, y \rangle, \langle z, w \rangle : [\alpha[0, y/z, w],\ \alpha]\ {}^{2}_{0} \sqsubseteq Zerofst$$
- *Axioma Zerosnd*:
$$\langle x, y \rangle, \langle z, w \rangle : [\alpha[x, 0/z, w],\ \alpha]\ {}^{3}_{1} \sqsubseteq Zerosnd$$
- *Axioma Decfst*:
$$\langle x, y \rangle, \langle z, w \rangle : [\alpha[x-1, y/z, w],\ \alpha]\ {}^{2}_{0} \sqsubseteq Decfst$$
- *Axioma Decsnd*:
$$\langle x, y \rangle, \langle z, w \rangle : [\alpha[x, y-1/z, w],\ \alpha]\ {}^{3}_{0} \sqsubseteq Decsnd$$
- *Axioma Flip*:
$$\langle c \rangle, \langle s \rangle : [\alpha[\mathsf{hd}/s] \wedge \alpha[\mathsf{tl}/s],\ \alpha]\ {}^{3}_{2} \sqsubseteq Flip$$

EJEMPLO 3.6.1 Se quiere derivar un proceso desde la especificación

$$\langle coin\rangle,\langle res\rangle{:}[true,\ res = \mathsf{hd}]\ {}^{\epsilon+4}_{1}.$$

La siguiente es una derivación de una implementación desde $Th(\mathcal{A})$:

$$\begin{array}{lll}
 & \langle coin\rangle,\langle res\rangle{:}[true,\ res = \mathsf{hd}]\ {}^{\epsilon+4}_{1} & \\
 & \quad \sqsubseteq \langle coin\rangle,\langle res\rangle{:}[true,\ true]\ {}^{4}_{1};\ \langle res\rangle,\langle res\rangle{:}[true,\ res = \mathsf{hd}]\ {}^{\epsilon}_{\epsilon} & (TIME, SEC) \\
(1) & \langle coin\rangle,\langle res\rangle{:}[true,\ true]\ {}^{4}_{1} & \\
 & \quad \sqsubseteq Flip & (TIME, Flip) \\
(2) & \langle res\rangle,\langle res\rangle{:}[true,\ res = \mathsf{hd}]\ {}^{\epsilon}_{\epsilon} & \\
 & \quad \sqsubseteq s = \mathsf{hd}? & (CONS, TEST)
\end{array}$$

Así, se tiene que el proceso $Flip;s = \mathsf{hd}?$ es una implementación correcta.

■

EJEMPLO 3.6.2 Se quiere derivar un proceso desde la especificación

$$\langle x, y\rangle,\langle x\rangle{:}[x = 1 \wedge y = 2,\ even(x)]\ {}^{7}_{1}.$$

La siguiente es una derivación de una implementación desde $Th(\mathcal{A})$:

$$\begin{array}{lll}
\langle x, y\rangle,\langle x\rangle{:}[x = 1 \wedge y = 2,\ even(x)]\ {}^{7}_{1} & & \\
\quad \sqsubseteq \langle x, y\rangle,\langle x, y\rangle{:}[x = 1 \wedge y = 2,\ odd(x + y)]\ {}^{4}_{1};\ \langle x, y\rangle,\langle x\rangle{:}[odd(x + y),\ even(x)]\ {}^{3}_{1} & (SEC,TIME) & \\
(1) & & \\
\langle x, y\rangle,\langle x, y\rangle{:}[x = 1 \wedge y = 2,\ odd(x + y)]\ {}^{4}_{1} & & \\
\quad \sqsubseteq \langle x, y\rangle,\langle x, y\rangle{:}[odd(y + x),\ odd(x + y)]\ {}^{4}_{1} & (CONS) & \\
\quad \sqsubseteq Swap & (Swap) & \\
(2) & & \\
\langle x, y\rangle,\langle x\rangle{:}[odd(x + y),\ even(x)]\ {}^{3}_{1} & & \\
\quad \sqsubseteq \langle x, y\rangle,\langle x\rangle{:}[odd(x + y),\ odd(x)]\ {}^{2}_{0};\ \langle x\rangle,\langle x\rangle{:}[odd(x),\ even(x)]\ {}^{1}_{0} & (SEC,TIME) & \\
(3) & & \\
\langle x, y\rangle,\langle x\rangle{:}[odd(x + y),\ odd(x)]\ {}^{2}_{0} & & \\
\quad \sqsubseteq Sum & (Sum) & \\
(4) & & \\
\langle x\rangle,\langle x\rangle{:}[odd(x),\ even(x)]\ {}^{1}_{0} & & \\
\quad \sqsubseteq \langle x\rangle,\langle x\rangle{:}[odd(x),\ even(x)]\ {}^{1}_{0} + \langle x\rangle,\langle x\rangle{:}[odd(x),\ even(x)]\ {}^{1}_{0} & (CHC,TIME) & \\
(5) & & \\
\langle x\rangle,\langle x\rangle{:}[odd(x),\ even(x)]\ {}^{1}_{0} & & \\
\quad \sqsubseteq \langle x\rangle,\langle x\rangle{:}[even(x + 1),\ even(x)]\ {}^{1}_{0} & (CONS) & \\
\quad \sqsubseteq Inc & (Inc) &
\end{array}$$

(6)

$\langle x \rangle,\langle x \rangle : [odd(x),\ even(x)]\ {}^{1}_{0}$

$\sqsubseteq \langle x \rangle,\langle x \rangle : [even(x-1),\ even(x)]\ {}^{1}_{0}$ $(CONS)$

$\sqsubseteq Dec$ $(Dec)$

Así, se tiene que el proceso $Swap;Sum;(Inc + Dec)$ es una implementación correcta.

■

EJEMPLO 3.6.3 Se quiere derivar un proceso desde la especificación

$$\langle x, y \rangle,\langle w \rangle : [true,\ w \geq 0]\ {}^{\infty}_{1}.$$

La siguiente es una derivación de una implementación desde $Th(\mathcal{A})$:

$\langle x, y \rangle,\langle w \rangle : [true,\ w \geq 0]\ {}^{\infty}_{1}$

$\sqsubseteq \langle x, y \rangle,\langle x, y \rangle : [true,\ x = 0 \wedge y = 0]\ {}^{3}_{1}; \langle x, y \rangle,\langle w \rangle : [x = 0 \wedge y = 0,\ w \geq 0]\ {}^{\infty}_{0}$ $(SEC,TIME)$

(1)

$\langle x, y \rangle,\langle x, y \rangle : [true,\ x = 0 \wedge y = 0]\ {}^{3}_{1}$

$\sqsubseteq \langle x, y \rangle,\langle x, y \rangle : [true,\ x = 0]\ {}^{2}_{0} \cdot \langle x, y \rangle,\langle x, y \rangle : [true,\ y = 0]\ {}^{3}_{1}$ $(PAR,TIME)$

(2)

$\langle x, y \rangle,\langle x, y \rangle : [true,\ x = 0]\ {}^{2}_{0}$

$\sqsubseteq \langle x, y \rangle,\langle x, y \rangle : [0 = 0,\ x = 0]\ {}^{2}_{0}$ $(CONS)$

$\sqsubseteq Zerofst$ $(Zerofst)$

(3)

$\langle x, y \rangle,\langle x, y \rangle : [true,\ y = 0]\ {}^{3}_{1}$

$\sqsubseteq \langle x, y \rangle,\langle x, y \rangle : [0 = 0,\ y = 0]\ {}^{3}_{1}$ $(CONS)$

$\sqsubseteq Zerosnd$ $(Zerosnd)$

(4)

$\langle x, y \rangle,\langle w \rangle : [x = 0 \wedge y = 0,\ w \geq 0]\ {}^{\infty}_{0}$

$\sqsubseteq \langle x, y \rangle,\langle w \rangle : [x = 0 \wedge y = 0,\ w = 0]\ {}^{0}_{0}; \langle w \rangle,\langle w \rangle : [w = 0,\ w \geq 0]\ {}^{\infty}_{0}$ $(SEC,TIME)$

(5)

$\langle x, y \rangle,\langle w \rangle : [x = 0 \wedge y = 0,\ w = 0]\ {}^{0}_{0}$

$\sqsubseteq Join$ $(Join)$

(6)

$\langle w \rangle,\langle w \rangle : [w = 0,\ w \geq 0]\ {}^{\infty}_{0}$

$\sqsubseteq \langle w \rangle,\langle w \rangle : [w \geq 0,\ w \geq 0]\ {}^{\infty}_{0}$ $(CONS)$

$\sqsubseteq (\langle w \rangle,\langle w \rangle : [w \geq 0,\ w \geq 0]\ {}^{1}_{0})^{*}$ $(ITE)$

(7)
$\langle w \rangle,\langle w \rangle : [w \geq 0,\ w \geq 0]\ {}^{1}_{0}$

$\sqsubseteq \langle w \rangle,\langle w \rangle : [w+1 \geq 0,\ w \geq 0]\ {}^{1}_{0}$ $(CONS)$

$\sqsubseteq Inc$ $(Inc)$

Así, se tiene que el proceso $(Zerofst \cdot Zerosnd); Join; Inc^*$ es una implementación correcta.

■

EJEMPLO 3.6.4 Se quiere derivar un proceso desde la especificación

$$\langle x \rangle,\langle y \rangle : [true,\ y = 0]\ {}^{x*2}_{\epsilon}.$$

La siguiente es una derivación de una implementación desde $Th(\mathcal{A})$:

$\langle x \rangle,\langle y \rangle : [true,\ y = 0]\ {}^{x*2}_{\epsilon}$

$\sqsubseteq \langle x \rangle,\langle x \rangle : [true,\ x = 0]\ {}^{x*2}_{\epsilon}$ $(VAR)$

$\sqsubseteq \langle x \rangle,\langle x \rangle : [true,\ \neg(x \neq 0)]\ {}^{x*2}_{\epsilon}$ $(CONS)$

$\sqsubseteq$ **while** $z \neq 0$ **do** $\langle x \rangle,\langle x \rangle : [x \neq 0 \wedge true \wedge x = x_0,\ true \wedge x < x_0]\ {}^{2}_{0}$ $(WD)$

(1) $\langle x \rangle,\langle x \rangle : [x \neq 0 \wedge true \wedge x = x_0,\ true \wedge x < x_0)]\ {}^{2}_{0}$

$\sqsubseteq \langle x \rangle,\langle x \rangle : [true \wedge x - 2 < x_0,\ true \wedge x < x_0)]\ {}^{2}_{0}$ $(CONS)$

$\sqsubseteq Decby2$ $(Decby2)$

Así, se tiene que el proceso **while** $z \neq 0$ **do** $Decby2$ es una implementación correcta.

■

EJEMPLO 3.6.5 En este ejemplo se derivará una implementación para el problema de la máquina vendedora de caramelos presentado en la Sección 1.4. Siendo $\mathcal{A}$ la estructura de objeto para este problema, se tiene que $RTh(\mathcal{A})$ es axiomatizable con los siguientes esquemas de axioma:

Siendo $\alpha \in For(\mathcal{S})$, $\#\$, \#P, \#\$', \#P'$ variables de sort $Nat$ y $\$r, Pr, \$r', Pr'$ variables de sort $Bool$,

- *Axioma Accept$*:

$$\langle \#\$, \#P, \$r, Pr \rangle,\langle \#\$', \#P', \$r', Pr' \rangle : [\alpha[\#\$ + 1/\#\$'],\ \alpha]\ {}^{3s}_{0} \sqsubseteq Accept\$$$

- *Axioma Return$*:

$$\langle \#\$, \#P, \$r, Pr \rangle,\langle \#\$', \#P', \$r', Pr' \rangle : [\#\$ > 0 \Rightarrow \alpha[\#\$ - 1, \mathtt{t}/\#\$', \$r'],\ \alpha]\ {}^{4s}_{0} \sqsubseteq Return\$$$

- *Axioma GiveProduct*:

$$\langle \#\$, \#P, \$r, Pr \rangle,\langle \#\$', \#P', \$r', Pr' \rangle : [\#P > 0 \Rightarrow \alpha[\#P - 1, \mathtt{t}/\#P', Pr'],\ \alpha]\ {}^{10s}_{0} \sqsubseteq GiveProduct$$

- *Axioma AskForReplenish*:

$$\langle \#\$, \#P, \$r, Pr \rangle, \langle \#\$', \#P', \$r', Pr' \rangle : [\alpha[MP/\#P'],\ \alpha]\ {}^{24h}_{0} \sqsubseteq AskForReplenish$$

Sean $m$ y $m'$ las tuplas $\langle \#\$, \#P, \$r, Pr \rangle$ y $\langle \#\$', \#P', \$r', Pr' \rangle$, $pre$ la fórmula $\#\$ = x_0 \wedge \#P = P_0 \wedge \$r = \mathsf{f} \wedge Pr = \mathsf{f}$, y $post$ la fórmula

$$P_0 = 0 \Rightarrow \begin{pmatrix} \#\$ = x_0 + 1 \wedge \#P = MP - 1 \wedge \$r = \mathsf{f} \wedge Pr = \mathsf{t} \\ \vee \\ \#\$ = x_0 \wedge \#P = 0 \wedge \$r = \mathsf{t} \wedge Pr = \mathsf{f} \end{pmatrix}$$
$$P_0 > 0 \Rightarrow \#\$ = x_0 + 1 \wedge \#P = P_0 - 1 \wedge \$r = \mathsf{f} \wedge Pr = \mathsf{t}$$

Se quiere derivar un proceso desde la especificación

$$m, m : [pre,\ post]\ {}^{3m}_{0}.$$

La siguiente es una derivación de una implementación desde $Th(\mathcal{A})$:

$m, m : [pre,\ post]\ {}^{3m}_{0}$

$\sqsubseteq$ **if** $(IF, TIME)$

$\#P = 0 \rightarrow m, m : [\#P = 0 \wedge pre,\ post]\ {}^{3s+4s}_{0}\ []$

$\#P > 0 \rightarrow m, m : [\#P > 0 \wedge pre,\ post]\ {}^{3s+10s}_{0}$

**fi**

(1) $m, m : [\#P = 0 \wedge pre,\ post]\ {}^{3s+4s}_{0}$

$\sqsubseteq m, m' : [\#P = 0 \wedge pre,\ mid_1]\ {}^{3s}_{0}; m', m : [mid_1,\ post]\ {}^{4s}_{0}$ $(SEC)$

donde $mid_1 \equiv \#\$' = x_0 + 1 \wedge \#P' = P_0 = 0 \wedge \$r' = \mathsf{f} \wedge Pr' = \mathsf{f}$

(2) $m, m' : [\#P = 0 \wedge pre,\ mid_1]\ {}^{3s}_{0}$

$\sqsubseteq m, m' : [mid_1[\#\$ + 1/\#\$'],\ mid_1]\ {}^{3s}_{0}$ $(CONS)$

$\sqsubseteq Accept\$$ $(Accept\$)$

(3) $m', m : [mid_1,\ post]\ {}^{4s}_{0}$

$\sqsubseteq m', m : [\#\$' > 0 \wedge post[\#\$' - 1, \mathsf{t}/\#\$, \$r],\ post]\ {}^{4s}_{0}$ $(CONS)$

$\sqsubseteq Return\$$ $(Return\$)$

(4) $m, m : [\#P > 0 \wedge pre,\ post]\ {}^{3s+10s}_{0}$

$\sqsubseteq m, m' : [\#P > 0 \wedge pre,\ mid_2]\ {}^{3s}_{0}; m', m : [mid_2,\ post]\ {}^{10s}_{0}$ $(SEC)$

donde $mid_2 \equiv \#\$' = x_0 + 1 \wedge \#P' = P_0 > 0 \wedge \$r' = \mathsf{f} \wedge Pr' = \mathsf{f}$

(5) $m, m' : [\#P > 0 \wedge pre,\ mid_2]\ {}^{3s}_{0}$

$\sqsubseteq m, m' : [mid_2[\#\$ + 1/\#\$'],\ mid_2]\ {}^{3s}_{0}$ $(CONS)$

$\sqsubseteq Accept\$$ $(Accept\$)$

(6) $m', m : [mid_2,\ post]\ {}^{10s}_{0}$

$\sqsubseteq m', m : [\#P' > 0 \wedge post[\#P' - 1, \mathsf{t}/\#P, Pr],\ post]\ {}^{10s}_{0}$ $(CONS)$

$\sqsubseteq GiveProduct$ $(GiveProduct)$

Así, se tiene que el proceso **if** $\#P = 0 \rightarrow Accept\$;Return\$$ [] $\#P > 0 \rightarrow Accept\$;GiveProduct$ **fi** es una implentación correcta del problema de la máquina vendedora.

■

## 3.7 Un caso de estudio: *El problema del control de la caldera de vapor*

En [6] se derivó una implementación $P/PML$ para el problema del control de la caldera de vapor a partir de una especificación simplificada (basada en la especificación informal dada en [1]). En esta sección, se revisitará el problema del control de la caldera de vapor y se derivará una implementación para este problema, utilizando el cálculo de refinamientos que se ha desarrollado. En este caso, se considerará una especificación más compleja que la se trató en [6]. Basándose en la especificación de requerimientos informal dada en [1], se considerarán los siguientes elementos:

- Se tendrán en cuenta las distintas clases de fallas de los dispositivos físicos (fallas en en los dispositivos de medición del nivel del agua y del vapor y fallas en los controladores de las bombas).
- Se considerarán los cinco diferentes modos de operación del programa, a saber: inicialización, normal, degradado, rescate y parada de emergencia.
- Para ilustrar el comportamiento del sistema entero, se modelarán como procesos tanto el entorno físico como el programa controlador.
- Se modelará un protocolo abstracto de pasaje de mensajes entre las unidades físicas (el entorno) y el programa controlador, usando variables de estado compartidas.

### 3.7.1 Modelo del sistema

A continuación se modelará el sistema de acuerdo con la especificación informal, presentando las constantes y variables de estado del sistema que se usarán.

**Constantes:**

- $C$: Capacidad total de agua en la caldera de vapor.
- $M_1$: Límite mínimo de la cantidad de agua.
- $M_2$: Límite máximo de la cantidad de agua.
- $N_1$: Cantidad de agua mínima normal a mantenerse durante la operación regular.
- $N_2$: Cantidad de agua máxima normal a mantenerse durante la operación regular.
- $W$: Máxima cantidad de vapor a la salida de la caldera.
- $U_1$: Gradiente máximo de aumento de la cantidad de vapor.

- $U_2$: Gradiente máximo de disminución de la cantidad de vapor.
- $P$: Capacidad nominal de cada bomba.
- $E$: Capacidad nominal de la válvula de evacuación.

Se asumirá que $0 < M_1 < N_1 < N_2 < M_2 < C$.

**Sensores:**

- $q$: Cantidad real corriente de agua en la caldera.
- $v$: Cantidad real corriente de vapor saliendo de la caldera.
- $e$: Cantidad real corriente de agua saliendo de la caldera a través de la válvula de evacuación.
- $p_1, \ldots, p_4$: Capacidad real corriente de cada bomba.

**Actuadores:**

- *mode*: Modo de operación actual del programa controlador.
- *pumps*: Estado actual de las bombas. Sus posibles valores son on y off.
- *valve*: Estado actual de la válvula de evacuación. Sus posible valores son open y closed.
- *stop*: Si el sistema ha sido detenido o no.

**Indicadores:**

- *q_gauge*: Indicador del nivel de agua. Sus posibles valores son ok y failed.
- *v_gauge*: Indicador del nivel de vapor. Sus posibles valores son ok y failed.
- $p_1$*_gauge*, $\ldots$, $p_4$*_gauge*: Indicadores de bombas. Sus posibles valores son ok y failed.

**Medidas transmitidas:**

- *trans_q*: Medida transmitida del nivel de agua.
- *trans_v*: Medida transmitida del nivel de vapor.
- *trans_*$p_1, \ldots,$ *trans_*$p_4$: Medida transmitida de la capacidad de cada bomba.

**Medidas ajustadas:**

- $qa_1$: Medida ajustada mínima del nivel de agua.
- $qa_2$: Medida ajustada máxima del nivel de agua.

Además, se usarán las siguientes funciones y predicados definidos a continuación:

$$
\begin{array}{ll}
q\_min(q,v,p,e) & \triangleq q - v * 5 - \frac{1}{2} * U_1 * 25 + p - e \\
q\_max(q,v,p,e) & \triangleq q - v * 5 - \frac{1}{2} * U_2 * 25 + p - e \\
q\_variation(q,v,p,e,q') & \triangleq q\_min(q,v,p,e) \leq q' \leq q\_max(q,v,p,e) \wedge 0 \leq q' \leq C \\
v\_variation(v,v') & \triangleq v - U_2 * 5 \leq v' \leq v + U_1 * 5 \wedge 0 \leq v' \leq W \\
checkValve(valve) & \triangleq \begin{cases} E * 5 & \text{si } valve = \mathsf{open} \\ 0 & \text{c.c.} \end{cases} \\
choose(\alpha, x) & \triangleq \forall n : n \geq 0 \Rightarrow \alpha[n/x] \\
transmit(\alpha, gauge, t, val) & \triangleq (gauge = \mathsf{ok} \Rightarrow \alpha[val/t]) \wedge (gauge = \mathsf{failed} \Rightarrow choose(\alpha, t))
\end{array}
$$

### 3.7.2 La máquina abstracta

A continuación se definirá la máquina abstracta sobre la cual se derivará una implementación para el problema del control de la caldera de vapor. Para este propósito, se usarán las acciones atómicas definidas más adelante. Para simplificar, llamaremos "estado del sistema" a la tupla formada por todas las variables de estado mencionadas en la sección anterior. Así, se considerarán todas las acciones atómicas como tranformadores de estado. También, se asumirá que las sustituciones que aparecen en los axiomas para las acciones atómicas sólo cambian las variables mencionadas explíctamente y no alterar el resto. Se supondrá que $\epsilon = 0$ seg., y que $\mathsf{l}(a) = 0$ seg. y $\mathsf{u}(a) = 1$ seg., para cada acción atómica $a$.

**Acciones atómicas del entorno físico:** Las siguientes son las acciones atómicas de la máquina abstracta que se usarán para construir un proceso que representará el entorno físico.

- *Update_q*: Actualiza la medida del nivel de agua, de acuerdo a la dinámica del sistema.
- *Update_v*: Actualiza la medida del nivel de vapor, de acuerdo a la dinámica del sistema.
- $Update\_p_1, \ldots, Update\_p_4$: Actualiza la medida de capacidad de cada bomba, de acuerdo a la dinámica del sistema.
- *Update_e*: Actualiza la medida de la válvula de evacuación, de acuerdo a la dinámica del sistema.
- *Break_q_gauge*: Rompe el indicador del nivel de agua, haciendo insegura su medida.
- *Repair_q_gauge*: Repara el indicador del nivel de agua.
- *Break_v_gauge*: Rompe el indicador del nivel de vapor, haciendo insegura su medida.

- *Repair_v_gauge*: Repara el indicador del nivel de vapor.
- $Break\_p_1\_gauge, \ldots, Break\_p_4\_gauge$: Rompe cada indicador de bomba, haciendo insegura su medida.
- $Repair\_p_1\_gauge, \ldots, Repair\_p_4\_gauge$: Repara cada indicador de bomba.
- $Transmit\_q$: Transmite la medida actual del nivel de agua, siempre que el indicador del nivel de agua no esté roto. En caso contrario, no puede fiarse del valor transmitido.
- $Transmit\_v$: Transmite la medida actual del nivel de vapor, siempre que el indicador del nivel de vapor no esté roto. En caso contrario, no puede fiarse del valor transmitido.
- $Transmit\_p_1, \ldots, Transmit\_p_4$: Transmite la medida de la capacidad de cada bomba, siempre que el indicador de bomba no esté roto. En caso contrario, no puede fiarse del valor transmitido.

Los axiomas asociados a estas acciones atómicas son los siguientes: Siendo $s, s'$ dos estados del sistema,

- *Axioma Update_q*:

$$s, s' : [\forall q_0 : q\_variation(q, v, p_1 + p_2 + p_3 + p_4, e, q_0) \Rightarrow \alpha[q_0/q'],\ \alpha]\ {}^{1}_{0} \sqsubseteq Update\_q$$

- *Axioma Update_v*:

$$s, s' : [\forall v_0 : v\_variation(v, v_0) \Rightarrow \alpha[v_0/v'],\ \alpha]\ {}^{1}_{0} \sqsubseteq Update\_v$$

- *Axioma Update_$p_i$* (para todo $i = 1..4$):

$$s, s' : [\forall p_i^0 : 0 \leq p_i^0 \leq P * 5 \Rightarrow \alpha[p_i^0/p_i'],\ \alpha]\ {}^{1}_{0} \sqsubseteq Update\_p_i$$

- *Axioma Update_e*:

$$s, s' : [\alpha[checkValve(valve)/e'],\ \alpha]\ {}^{1}_{0} \sqsubseteq Update\_e$$

- *Axioma Break_q_gauge*:

$$s, s' : [\alpha[\mathsf{failed}/q\_gauge'],\ \alpha]\ {}^{1}_{0} \sqsubseteq Break\_q\_gauge$$

- *Axioma Repair_q_gauge*:

$$s, s' : [\alpha[\mathsf{ok}/q\_gauge'],\ \alpha]\ {}^{1}_{0} \sqsubseteq Repair\_q\_gauge$$

- *Axioma Break_v_gauge*:

$$s, s' : [\alpha[\mathsf{failed}/v\_gauge'],\ \alpha]\ {}^{1}_{0} \sqsubseteq Break\_v\_gauge$$

- *Axioma Repair_v_gauge*:

$$s, s' : [\alpha[\mathsf{ok}/v\_gauge'],\ \alpha]\ {}^{1}_{0} \sqsubseteq Repair\_v\_gauge$$

- *Axioma* $Break\_p_i\_gauge$ (para todo $i = 1..4$):

$$s, s' : [\alpha[\mathsf{failed}/p_i\_gauge'],\ \alpha]\ {}^{1}_{0} \sqsubseteq Break\_p_i\_gauge$$

- *Axioma* $Repair\_p_i\_gauge$ (para todo $i = 1..4$):

$$s, s' : [\alpha[\mathsf{ok}/p_i\_gauge'],\ \alpha]\ {}^{1}_{0} \sqsubseteq Repair\_p_i\_gauge$$

- *Axioma* $Transmit\_q$:

$$s, s' : [transmit(\alpha, q\_gauge, trans\_q', q),\ \alpha]\ {}^{1}_{0} \sqsubseteq Transmit\_q$$

- *Axioma* $Transmit\_v$:

$$s, s' : [transmit(\alpha, v\_gauge, trans\_v', v),\ \alpha]\ {}^{1}_{0} \sqsubseteq Transmit\_v$$

- *Axioma* $Transmit\_p_i$ (para todo $i = 1..4$):

$$s, s' : [transmit(\alpha, p_i\_gauge, trans\_p_i', p_i),\ \alpha]\ {}^{1}_{0} \sqsubseteq Transmit\_p_i$$

**Acciones atómicas del programa controlador:** Las siguientes son las acciones atómicas de la máquina abstracta que se usarán para construir un proceso que represente el programa controlador

- $Estimate\_qa_1\_ok$: Estima la medida ajustada $qa_1$, siempre que el indicador del nivel de agua no esté roto.
- $Estimate\_qa_1\_failed$: Estima la medida ajustada $qa_1$, siempre que el indicador del nivel de agua esté roto.
- $Estimate\_qa_2\_ok$: Estima la medida ajustada $qa_2$, siempre que el indicador del nivel de agua no esté roto.
- $Estimate\_qa_2\_failed$: Estima la medida ajustada $qa_1$, siempre que el indicador del nivel de agua esté roto.
- $GoToOperatingMode$: Cambia el modo actual a modo operativo.
- $GoToEmergencyMode$: Cambia el modo actual a modo de parada de emergencia.
- $OpenValve$: Abre la válvula de evacuación.
- $CloseValve$: Cierra la válvula de evacuación.
- $SwitchOnPumps$: Enciende las bombas.
- $SwitchOffPumps$: Apaga las bombas.
- $StopSystem$: Detiene el sistema.

Los axiomas asociados a estas acciones atómicas son los siguientes: Siendo $s, s'$ dos estados del sistema,

- *Axioma* $Estimate\_qa_1\_ok$:

$$s, s' : [q\_gauge = \mathsf{ok} \wedge \alpha[trans\_q/qa_1'],\ \alpha]\ {}^{1}_{0} \sqsubseteq Estimate\_qa_1\_ok$$

- *Axioma* $Estimate\_qa_1\_failed$:

$$s, s' : [q\_gauge = \mathsf{failed} \wedge \alpha[q\_min(qa_1, trans\_v, \sum trans\_p_i, 0)/qa_1'],\ \alpha]\ {}^{1}_{0} \sqsubseteq estimate\_qa_1\_Failed$$

- *Axioma* $Estimate\_qa_2\_ok$:

$$s, s' : [q\_gauge = \mathsf{ok} \wedge \alpha[trans\_q/qa_2'],\ \alpha]\ {}^{1}_{0} \sqsubseteq Estimate\_qa_2\_ok$$

- *Axioma* $Estimate\_qa_2\_failed$:

$$s, s' : [q\_gauge = \mathsf{failed} \wedge \alpha[q\_max(qa_2, trans\_v, \sum trans\_p_i, 0)/qa_2'],\ \alpha]\ {}^{1}_{0} \sqsubseteq Estimate\_qa_2\_failed$$

- *Axioma* $GoToOperatingMode$:

$$s, s' : [\alpha[\mathsf{oper}/mode],\ \alpha]\ {}^{1}_{0} \sqsubseteq GoToOperatingMode$$

- *Axioma* $GoToEmergencyMode$:

$$s, s' : [\alpha[\mathsf{emer}/mode],\ \alpha]\ {}^{1}_{0} \sqsubseteq GoToEmergencyMode$$

- *Axioma* $OpenValve$:

$$s, s' : [\alpha[\mathsf{open}/valve],\ \alpha]\ {}^{1}_{0} \sqsubseteq OpenValve$$

- *Axioma* $CloseValve$:

$$s, s' : [\alpha[\mathsf{closed}/valve],\ \alpha]\ {}^{1}_{0} \sqsubseteq CloseValve$$

- *Axioma* $SwitchOnPumps$:

$$s, s' : [\alpha[\mathsf{on}/pumps],\ \alpha]\ {}^{1}_{0} \sqsubseteq SwitchOnPumps$$

- *Axioma* $SwitchOffPumps$:

$$s, s' : [\alpha[\mathsf{off}/pumps],\ \alpha]\ {}^{1}_{0} \sqsubseteq SwitchOffPumps$$

- *Axioma* $StopSystem$:

$$s, s' : [\alpha[\mathsf{t}/stop],\ \alpha]\ {}^{1}_{0} \sqsubseteq StopSystem$$

### 3.7.3 Especificación del problema y derivación de una implementación

Aquí se dará una especificación formal del problema del control de la caldera de vapor desde la cual se derivará (a través de refinamientos) una implementación $P/PML$. Debe aclararse que no se incluirán todos los requerimientos en la especificación inicial, sino que eventualmente se incluirán a través de pasos de refinamiento subsecuentes. Sea *pre* la fórmula

$$mode = M_0 \wedge q = q_0 \wedge v = v_0 \wedge valve = V_0 \wedge pumps = P_0 \wedge qa_1 = qa_1^0 \wedge qa_2 = qa_2^0$$

y *post* la fórmula

$$M_0 = \mathsf{init} \wedge q\_gauge = \mathsf{ok} \wedge trans\_q > N_2 \Rightarrow valve = \mathsf{open}$$
$$M_0 = \mathsf{init} \wedge q\_gauge = \mathsf{ok} \wedge trans\_q < N_1 \Rightarrow pumps = \mathsf{on}$$
$$M_0 = \mathsf{init} \wedge q\_gauge = \mathsf{ok} \wedge V_0 = \mathsf{closed} \wedge P_0 = \mathsf{off} \wedge N_1 \leq trans\_q \leq N_2 \Rightarrow mode = \mathsf{oper}$$
$$M_0 = \mathsf{init} \wedge q\_gauge = \mathsf{failed} \Rightarrow mode = \mathsf{emer}$$
$$M_0 = \mathsf{oper} \wedge (Normal \vee Degraded) \wedge M_1 \leq trans\_q < N_1 \Rightarrow pumps = \mathsf{on}$$
$$M_0 = \mathsf{oper} \wedge (Normal \vee Degraded) \wedge N_2 < trans\_q \leq M_2 \Rightarrow pumps = \mathsf{off}$$
$$M_0 = \mathsf{oper} \wedge (Normal \vee Degraded) \wedge (trans\_q < M_1 \vee trans\_q > M_2) \Rightarrow mode = \mathsf{emer}$$
$$M_0 = \mathsf{oper} \wedge Rescue \wedge M_1 \leq qa_1 \wedge qa_2 \leq N_2 \Rightarrow pumps = \mathsf{on}$$
$$M_0 = \mathsf{oper} \wedge Rescue \wedge N_1 \leq qa_1 \wedge qa_2 \leq M_2 \Rightarrow pumps = \mathsf{off}$$
$$M_0 = \mathsf{oper} \wedge Rescue \wedge (M_1 > qa_1 \vee qa_2 > M_2 \vee (qa_1 < N_1 \wedge N_2 > qa_2)) \Rightarrow mode = \mathsf{emer}$$
$$M_0 = \mathsf{oper} \wedge Emergency \Rightarrow mode = \mathsf{emer}$$
$$M_0 = \mathsf{emer} \Rightarrow stop = \mathsf{t}$$

donde las fórmulas *Normal*, *Degraded*, *Rescue* y *Emergency* se definen como

$$Normal \triangleq q\_gauge = \mathsf{ok} \wedge v\_gauge = \mathsf{ok} \wedge p_1\_gauge = \mathsf{ok} \wedge \cdots \wedge p_4\_gauge = \mathsf{ok}$$
$$Degraded \triangleq q\_gauge = \mathsf{ok} \wedge (v\_gauge = \mathsf{failed} \vee p_1\_gauge = \mathsf{failed} \vee \cdots \vee p_4\_gauge = \mathsf{failed})$$
$$Rescue \triangleq q\_gauge = \mathsf{failed} \wedge v\_gauge = \mathsf{ok} \wedge p_1\_gauge = \mathsf{ok} \wedge \cdots \wedge p_4\_gauge = \mathsf{ok}$$
$$Emergency \triangleq q\_gauge = \mathsf{failed} \wedge (v\_gauge = \mathsf{failed} \vee p_1\_gauge = \mathsf{failed} \vee \cdots \vee p_4\_gauge = \mathsf{failed})$$

Así, la implementación para el problema del control de la caldera de vapor se derivará a partir de la especificación

$$SystemCycle \triangleq s, s{:}[pre,\ post]\ {}^{5}_{0}.$$

**Refinamiento de** *SystemCycle*: Se abreviará $mode = M_0 \wedge valve = V_0 \wedge pumps = P_0 \wedge qa_1 = qa_1^0 \wedge qa_2 = qa_2^0$ por $pre_1$. Como primer paso en la derivación, se refinará la especificación *SystemCycle*. Se ha mencionado que, para ilustrar el sistema completo, se modelarán tanto tanto el entorno físico como el programa controlador. Se considerará un modelo estrictamente secuencial del ciclo entorno-controlador. Por lo tanto, se refinará *SystemCycle* como

$$SystemCycle \sqsubseteq Environment; Controller$$

donde las especificaciones *Environment* y *Controller* se definen como

$$Environment \triangleq s, s{:}[pre,\ mid_1]\ {}^{2}_{0}$$
$$Controller \triangleq s, s{:}[mid_1,\ post]\ {}^{3}_{0}$$

y la fórmula $mid_1$ es

$$pre_1 \wedge \begin{pmatrix} q\_gauge = \mathsf{ok} \Rightarrow trans\_q = q \\ v\_gauge = \mathsf{ok} \Rightarrow trans\_v = v \\ p_1\_gauge = \mathsf{ok} \Rightarrow trans\_p_1 = p_1 \\ \dots \\ p_4\_gauge = \mathsf{ok} \Rightarrow trans\_p_4 = p_4 \end{pmatrix}$$

La fórmula $mid_1$ establece que siempre que las unidades físicas funcionan correctamente, las medidas transmitidas al controlador son las medidas reales. Como puede verse, en este paso de refinamiento se ha introducido el protocolo de comunicación entre el entorno físico y el programa controlador.

**Refinamiento de *Environment*:** Ahora, se refinará la especificación *Environement*. El comportamiento del entorno físico comienza actualizando las medidas de las unidades físicas de acuerdo a la dinámica del sistema (que representa la evolución del sistema luego de un período de cinco segundos), y luego se trasmiten las medidas actuales al controlador. Por la tanto, se refinará *Environment* como

$$Environment \sqsubseteq Update;Transmit$$

donde las especificaciones *Update* y $Transmit$ se definen como

$$Update \triangleq s, s{:}[pre,\ mid_2]\ {}^{1}_{0}$$
$$Transmit \triangleq s, s{:}[mid_2,\ mid_1]\ {}^{1}_{0}$$

y la fórmula $mid_2$ es

$$pre_1 \wedge \begin{pmatrix} q\_variation(q_0, p_1 + p_2 + p_3 + p_4, e, q) \\ v\_variation(v_0, v) \\ e = checkValve(valve) \\ 0 \leq p_1, \dots, p_4 \leq P * 5 \end{pmatrix}$$

La fórmula $mid_2$ establece que las medidas reales han sido actualizadas de acuerdo con la dinámica del sistema. El requerimiento introducido en este paso de refinamiento trata de la evolución del entorno físico luego de ciclo de tiempo de cinco segundos.

**Refinamiento de *Update*:** Ahora, se refinará la especificación *Update*. En esta etapa, se considerará también la posibilidad de daños en las unidades físicas. Ya que la actualización de las variables del entorno puede ejecutarse simultáneamente (representando la evolución paralela del entorno), se refinará *Update* como

$$Update \sqsubseteq UpdateMeasures \cdot UpdateGauges$$

donde las especificaciones $UpdateMeasures$ y $UpdateGauges$ se definen como

$$UpdateMeasures \triangleq s, s{:}[pre,\ mid_2]\ {}^{1}_{0}$$
$$UpdateGauges \triangleq s, s{:}[pre,\ mid_3]\ {}^{1}_{0}$$

y la fórmula $mid_3$ es

$$pre_1 \wedge \begin{pmatrix} q\_gauge = \mathsf{ok} \vee q\_gauge = \mathsf{failed} \\ v\_gauge = \mathsf{ok} \vee v\_gauge = \mathsf{failed} \\ p_1\_gauge = \mathsf{ok} \vee p_1\_gauge = \mathsf{failed} \\ \dots \\ p_4\_gauge = \mathsf{ok} \vee p_4\_gauge = \mathsf{failed} \end{pmatrix}$$

Como lo establece la fórmula $mid_3$, en este paso de refinamiento se ha introducido la posibilidad de fallas de las unidades físicas durante la actualización de las medidas. Así, es posible que varias unidades puedan dañarse antes de trasmitir información al controlador.

**Refinamiento de $UpdateMeasures$:** Ahora, se refinará la especificación $UpdateMeasures$. Como se mencionó antes, la actualización de las medidas puede ejecutarse simultánemente, por lo tanto se refina $UpdateMeasures$ como

$$UpdateMeasures \sqsubseteq Upd\_q \cdot Upd\_v \cdot Upd\_e \cdot Upd\_p_1 \cdot \ldots \cdot Upd\_p_4$$

donde las especificaciones se definen como

$$\begin{aligned}
Upd_q &\triangleq s, s{:}[pre,\ pre_1 \wedge q_variation(q_0, \textstyle\sum p_i, e, q)]\ {}^{1}_{0} \\
Upd_v &\triangleq s, s{:}[pre,\ pre_1 \wedge v_variation(v_0, v)]\ {}^{1}_{0} \\
Upd_e &\triangleq s, s{:}[pre,\ pre_1 \wedge e = checkValve(valve)]\ {}^{1}_{0} \\
Upd_p_1 &\triangleq s, s{:}[pre,\ pre_1 \wedge 0 \leq p_1 \leq P * 5]\ {}^{1}_{0} \\
&\dots \\
Upd_p_4 &\triangleq s, s{:}[pre,\ pre_1 \wedge 0 \leq p_4 \leq P * 5]\ {}^{1}_{0}
\end{aligned}$$

Como puede verse, se ha decompuesto la especificación $UpdateMeasures$ en varias especificaciones en paralelo representando la actualización de las medidas dentro de cada unidad física. Ahora se refinará $Upd\_q$. Sea $\psi$ la fórmula

$$\forall n : q\_variation(q, \textstyle\sum p_i, e, n) \Rightarrow pre_1 \wedge q\_variation(q_0, \sum p_i, e, n)$$

Por lo tanto, la especificación $Upd\_q$ puede refinarse a una implementación de la siguiente forma:

$$\begin{aligned}
&Upd_q \\
&\quad \sqsubseteq s, s{:}[\psi,\ pre_1 \wedge q_variation(q_0, \textstyle\sum p_i, e, q)]\ {}^{1}_{0} && (CONS) \\
&\quad \sqsubseteq Update_q && (Update_q)
\end{aligned}$$

Similarmente, se puede probar que

$$\begin{aligned} Upd\_v &\sqsubseteq Update\_v \\ Upd\_e &\sqsubseteq Update\_e \\ Upd\_p_1 &\sqsubseteq Update\_p_1 \\ &\dots \\ Upd\_p_4 &\sqsubseteq Update\_p_4 \end{aligned}$$

Así, se ha llegado a una implementación para la especificación $UpdateMeasures$.

**Refinamiento de** $UpdateGauges$**:** Ahora, se refinará la especificación $UpdateGauges$. Como se mencionó antes, se modelará el posible daño de las unidades físicas en paralelo, por lo tanto se refina $UpdateGauges$ como

$$UpdateGauges \sqsubseteq Update\_q\_gauge \cdot Update\_v\_gauge \cdot Update\_p_1\_gauge \cdot \dots \cdot Update\_p_4\_gauge$$

donde las especificaciones se definen como

$$\begin{aligned} Update\_q\_gauge &\triangleq s, s' : [pre,\ pre_1 \wedge (q\_gauge = \mathsf{ok} \vee q\_gauge = \mathsf{failed})]\ {}^{1}_{0} \\ Update\_v\_gauge &\triangleq s, s' : [pre,\ pre_1 \wedge (v\_gauge = \mathsf{ok} \vee v\_gauge = \mathsf{failed})]\ {}^{1}_{0} \\ Update\_p_1\_gauge &\triangleq s, s' : [pre,\ pre_1 \wedge (p_1\_gauge = \mathsf{ok} \vee p_1\_gauge = \mathsf{failed})]\ {}^{1}_{0} \\ &\dots \\ Update\_p_4\_gauge &\triangleq s, s' : [pre,\ pre_1 \wedge (p_4\_gauge = \mathsf{ok} \vee p_4\_gauge = \mathsf{failed})]\ {}^{1}_{0} \end{aligned}$$

En este paso de refinamiento, se ha descompuesto la especificación $UpdateGauges$ en varios procesos representando el posible daño de cada unidad física. A continuación, se refinará $Update\_q\_gauge$ a una implementación. Sea $\psi$ la fórmula $q\_gauge = \mathsf{ok} \vee q\_gauge = \mathsf{failed}$. Entonces,

$$\begin{aligned} & Update\_q\_gauge \\ & \quad \sqsubseteq s, s' : [pre,\ pre_1 \wedge \psi]\ {}^{1}_{0} + s, s' : [pre,\ pre_1 \wedge \psi]\ {}^{1}_{0} && (CHC) \\ (1) \quad & s, s' : [pre,\ pre_1 \wedge \psi]\ {}^{1}_{0} \\ & \quad \sqsubseteq s, s' : [(pre_1 \wedge \psi)[\mathsf{ok}/q\_gauge],\ pre_1 \wedge \psi]\ {}^{1}_{0} && (CONS) \\ & \quad \sqsubseteq Repair\_q\_gauge && (Repair\_q\_gauge) \\ (2) \quad & s, s' : [pre,\ pre_1 \wedge \psi]\ {}^{1}_{0} \\ & \quad \sqsubseteq s, s' : [(pre_1 \wedge \psi)[\mathsf{failed}/q\_gauge],\ pre_1 \wedge \psi]\ {}^{1}_{0} && (CONS) \\ & \quad \sqsubseteq Break\_q\_gauge && (Break\_q\_gauge) \end{aligned}$$

Similarmente, se puede probar que

$$\begin{aligned} Update\_q\_gauge &\sqsubseteq Repair\_v\_gauge + Break\_v\_gauge \\ Update\_p_1\_gauge &\sqsubseteq Repair\_p_1\_gauge + Break\_p_1\_gauge \\ &\dots \\ Update\_p_4\_gauge &\sqsubseteq Repair\_p_4\_gauge + Break\_p_4\_gauge \end{aligned}$$

Así, se ha llegado a una implementación para la especificación $UpdateGauges$.

**Refinamiento de $Transmit$:** Ahora, se refinará la especificación $Transmit$. Se modelará el hecho de que la trasmisión es simultánea, por lo tanto se refina $Transmit$ como

$$\begin{aligned} Transmit &\sqsubseteq s, s:[pre_1,\ mid_1]\,{}^{1}_{0} && (CONS)\\ &\sqsubseteq Tra\_q \cdot Tra\_v \cdot Tra\_p_1 \cdot \ldots \cdot Tra\_p_4 && (PAR) \end{aligned}$$

donde las especificaciones se definen como

$$\begin{aligned} Tra\_q &\triangleq s, s:[pre,\ pre_1 \wedge (q\_gauge = \mathsf{ok} \Rightarrow trans\_q = q)]\,{}^{1}_{0}\\ Tra\_v &\triangleq s, s:[pre,\ pre_1 \wedge (v\_gauge = \mathsf{ok} \Rightarrow trans\_v = v)]\,{}^{1}_{0}\\ Tra\_p_1 &\triangleq s, s:[pre,\ pre_1 \wedge (p_1\_gauge = \mathsf{ok} \Rightarrow trans\_p_1 = p_1)]\,{}^{1}_{0}\\ &\ldots\\ Tra\_p_4 &\triangleq s, s:[pre,\ pre_1 \wedge (p_4\_gauge = \mathsf{ok} \Rightarrow trans\_p_4 = p_4)]\,{}^{1}_{0} \end{aligned}$$

En este paso de refinamiento, se ha descompuesto la especificación $Transmit$ en varias especificaciones en paralelo representando la transmisión de las medidas actuales al controlador. Ahora, se refinará $Tra\_q$ a una implementación. Sea $\psi$ la fórmula $pre_1 \wedge (q\_gauge = \mathsf{ok} \Rightarrow trans\_q = q)$. Entonces,

$$\begin{aligned} Tra\_q &\sqsubseteq s, s:[transmit(\psi, q\_gauge, trans\_q, q),\ \psi]\,{}^{1}_{0} && (CONS)\\ &\sqsubseteq Transmit\_q && (Transmit\_q) \end{aligned}$$

Similarmente, se puede probar que

$$\begin{aligned} Tra\_v &\sqsubseteq Transmit\_v\\ Tra\_p_1 &\sqsubseteq Transmit\_p_1\\ &\ldots\\ Tra\_p_4 &\sqsubseteq Transmit\_p_4 \end{aligned}$$

Así, se ha llegado a una implementación para la especificación $Transmit$.

**Refinamiento de $Controller$:** Se abreviará $mode = M_0 \wedge valve = V_0 \wedge pumps = P_0$ por $pre_2$. Ahora, se refinará la especificación $Controller$. El comportamiento del controlador comienza estimando el nivel de agua mínimo y máximo en la caldera (teniendo en cuenta si la información transmitida por el entorno no es fiable debido a la falla del indicador del nivel de agua), y luego se toman las acciones de control correspondientes. Así, se refina $Controller$ como

$$\begin{aligned} Controller &\sqsubseteq s, s:[pre_1,\ post]\,{}^{3}_{0} && (CONS)\\ &\sqsubseteq Estimate; Control && (SEC) \end{aligned}$$

donde las especificaciones $Estimate$ y $Control$ se definen como

$$\begin{aligned} Estimate &\triangleq s, s:[pre_1,\ mid_4]\,{}^{1}_{0}\\ Control &\triangleq s, s:[mid_4,\ post]\,{}^{2}_{0} \end{aligned}$$

y la fórmula $mid_4$ es

$$pre_2 \wedge \begin{pmatrix} q\_gauge = \mathsf{ok} \Rightarrow qa_1 = trans\_q \wedge qa_2 = trans\_q \\ q\_gauge = \mathsf{failed} \Rightarrow \begin{pmatrix} qa_1 = q\_min(qa_1^0, trans\_v, \sum trans\_p_i, 0) \\ qa_2 = q\_max(qa_2^0, trans\_v, \sum trans\_p_i, 0) \end{pmatrix} \end{pmatrix}$$

La fórmula $mid_4$ establece que las medidas ajustadas $qa_1$ y $qa_2$ han sido calculadas correctamente. En este paso de refinamiento, se ha introducido la estimación del nivel de agua cuando se detecta una falla en el indicador de nivel de agua.

**Refinamiento de** *Estimate*: Ahora, se refinará la especificación *Estimate*. Aquí, se calcula una estimación del nivel de agua mínimo y máximo. Es posible realizar estimaciones de $qa_1$ y $qa_2$ simultánemante, por lo tanto se refina *Estimate* como

$$Estimate \sqsubseteq Estimate\_qa_1 \cdot Estimate\_qa_2$$

donde la especificaciones $Estimate\_qa_1$ y $Estimate\_qa_2$ se definen como

$$Estimate\_qa_1 \triangleq s, s{:}[pre_1,\ mid_5]\ {}^{1}_{0}$$
$$Estimate\_qa_2 \triangleq s, s{:}[pre_1,\ mid_6]\ {}^{1}_{0}$$

la fórmula $mid_5$ es

$$pre_2 \wedge \begin{pmatrix} q\_gauge = \mathsf{ok} \Rightarrow qa_1 = trans\_q \\ q\_gauge = \mathsf{failed} \Rightarrow qa_1 = q\_min(qa_1^0, trans\_v, \sum trans\_p_i, 0) \end{pmatrix}$$

y la fórmula $mid_6$ es

$$pre_2 \wedge \begin{pmatrix} q\_gauge = \mathsf{ok} \Rightarrow qa_2 = trans\_q \\ q\_gauge = \mathsf{failed} \Rightarrow qa_2 = q\_max(qa_2^0, trans\_v, \sum trans\_p_i, 0) \end{pmatrix}$$

En este paso de refinamiento, se ha decompuesto *Estimate* en dos especificaciones en paralelo que realizan las estimaciones. Ahora, se refinará $Estimate\_qa_1$ a una implementación. Así

$Estimate\_qa_1$

$\sqsubseteq$ **if** $q\_gauge = \mathsf{ok}$ — $(IFT)$

**then** $s, s{:}[q\_gauge = \mathsf{ok} \wedge pre_1,\ mid_5]\ {}^{1}_{0}$

**else** $s, s{:}[q\_gauge = \mathsf{failed} \wedge pre_1,\ mid_5]\ {}^{1}_{0}$

(1) $s, s{:}[q\_gauge = \mathsf{ok} \wedge pre_1,\ mid_5]\ {}^{1}_{0}$

$\sqsubseteq s, s{:}[q\_gauge = \mathsf{ok} \wedge mid_5[trans\_q/qa_1],\ mid_5]\ {}^{1}_{0}$ — $(CONS)$

$\sqsubseteq Estimate\_qa_1\_ok$ — $(Estimate\_qa_1\_ok)$

(2) $s, s{:}[q\_gauge = \mathsf{failed} \wedge pre_1,\ mid_5]\ {}^{1}_{0}$

$\sqsubseteq s, s{:}[q\_gauge = \mathsf{failed} \wedge mid_5\sigma,\ mid_5]\ {}^{1}_{0}$ — $(CONS)$

donde $\sigma \equiv [q\_min(qa_1, trans\_v, \sum trans\_p_i, 0)/qa_1]$

$\sqsubseteq Estimate\_qa_1\_failed$ — $(Estimate\_qa_1\_failed)$

Similarmente, puede probarse que

$$Estimate\_qa_2 \sqsubseteq \textbf{if } q\_gauge = \mathsf{ok} \textbf{ then } Estimate\_qa_2\_ok \textbf{ else } Estimate\_qa_2\_failed$$

Así, se ha llegado a una implementación para la especificación *Estimate*.

**Refinamiento de** *Control***:** Ahora, se refinará la especificación *Control*. Se debe monitorear el sistema y tomar las acciones de control correspondientes para mantener el nivel de agua entre los niveles apropiados. Así, se refina *Control* como

$Control$
$\sqsubseteq$ $(CONS)$
$s, s{:}[pre_2,\ post]\ {}^{2}_{0}$
$\sqsubseteq$ $(IF)$
**if**

$mode = \mathsf{init} \wedge q\_gauge = \mathsf{ok} \wedge trans\_q > N_2 \rightarrow Init1\ []$
$mode = \mathsf{init} \wedge q\_gauge = \mathsf{ok} \wedge trans\_q < N_1 \rightarrow Init2\ []$
$mode = \mathsf{init} \wedge q\_gauge = \mathsf{ok} \wedge valve = \mathsf{open} \wedge N_1 \leq trans\_q \leq N_2 \rightarrow Init3\ []$
$mode = \mathsf{init} \wedge q\_gauge = \mathsf{ok} \wedge pumps = \mathsf{on} \wedge N_1 \leq trans\_q \leq N_2 \rightarrow Init4\ []$
$mode = \mathsf{init} \wedge q\_gauge = \mathsf{ok} \wedge valve = \mathsf{closed} \wedge pumps = \mathsf{off} \wedge N_1 \leq trans\_q \leq N_2 \rightarrow Init5\ []$
$mode = \mathsf{init} \wedge q\_gauge = \mathsf{failed} \rightarrow Init6\ []$
$mode = \mathsf{oper} \wedge (Normal \vee Degraded) \wedge M_1 \leq trans\_q < N_2 \rightarrow Oper1[]$
$mode = \mathsf{oper} \wedge (Normal \vee Degraded) \wedge N_1 < trans\_q \leq M_2 \rightarrow Oper2[]$
$mode = \mathsf{oper} \wedge (Normal \vee Degraded) \wedge (trans\_q < M_1 \vee trans\_q > M_2) \rightarrow Oper3[]$
$mode = \mathsf{oper} \wedge Rescue \wedge M_1 \leq qa_1 \wedge qa_2 \leq N_2 \rightarrow Oper4[]$
$mode = \mathsf{oper} \wedge Rescue \wedge N_1 \leq qa_1 \wedge qa_2 \leq M_2 \rightarrow Oper5[]$
$mode = \mathsf{oper} \wedge Rescue \wedge (M_1 > qa_1 \vee qa_2 > M_2 \vee (qa_1 < N_1 \wedge N_2 > qa_2)) \rightarrow Oper6[]$
$mode = \mathsf{oper} \wedge Emergency \rightarrow Oper7[]$
$mode = \mathsf{emer} \rightarrow Emer$

**fi**

En este paso de refinamiento, se ha descompuesto *Control* en varias especificaciones guardadas representando las acciones de control que deben tomarse. Para reducir la notación, se abrevian las guardas en el proceso anterior etiquetándolas con el nombre de la especificación correspondiente en minúsculas. Así, las especificaciones se definen como

$$
\begin{aligned}
Init1 &\triangleq s, s' : [init1 \wedge pre_2,\ post]\ {}^{2}_{0} \\
&\ldots \\
Init6 &\triangleq s, s' : [init6 \wedge pre_2,\ post]\ {}^{2}_{0} \\
Oper1 &\triangleq s, s' : [oper1 \wedge pre_2,\ post]\ {}^{2}_{0} \\
&\ldots \\
Oper7 &\triangleq s, s' : [oper7 \wedge pre_2,\ post]\ {}^{2}_{0} \\
Emer &\triangleq s, s' : [emer \wedge pre_2,\ post]\ {}^{2}_{0}
\end{aligned}
$$

Como puede verse, cada especificación se hace cargo de las acciones de control a realizarse cuando su guarda es verdadera. Ahora, se refinará $Init1$ a una implementación. Se tiene que

$$
\begin{aligned}
&Init1 \\
&\quad \sqsubseteq s, s' : [post[\mathsf{open}/valve],\ post]\ {}^{2}_{0} && (CONS) \\
&\quad \sqsubseteq s, s' : [post[\mathsf{open}/valve],\ post]\ {}^{1}_{0} && (TIME) \\
&\quad \sqsubseteq OpenValve && (OpenValve)
\end{aligned}
$$

Similarmente, puede probarse que

$$
\begin{aligned}
Init2 &\sqsubseteq switchOnPumps \\
Init3 &\sqsubseteq closeValve \\
Init4 &\sqsubseteq switchOffPumps \\
Init5 &\sqsubseteq goToOperatingMode \\
Init6 &\sqsubseteq goToEmergencyMode \\
Oper1 &\sqsubseteq switchOnPumps \\
Oper2 &\sqsubseteq switchOffPumps \\
Oper3 &\sqsubseteq goToEmergencyMode \\
Oper4 &\sqsubseteq switchOnPumps \\
Oper5 &\sqsubseteq switchOffPumps \\
Oper6 &\sqsubseteq goToEmergencyMode \\
Oper7 &\sqsubseteq goToEmergencyMode \\
Emer &\sqsubseteq StopSystem
\end{aligned}
$$

Así, se ha llegado a una implementación para la especificación $Control$.

# Capítulo 4

# Conclusiones y trabajo futuro

En este trabajo se han tratado los aspectos de verificación formal y derivación formal de procesos en la lógica $P/PML$. En la primer parte, se ha estudiado el aspecto de corrección parcial de procesos en $P/PML$. Como resultado de este estudio, ha sido desarrollado un sistema lógico que permite probar en forma rigurosa y sistemática la corrección parcial de un proceso con respecto a una especificación. El cálculo desarrollado tiene la importante propiedad de ser consistente y (relativamente) completo. Además, a través de los ejemplos presentados puede verse que es bastante simple razonar acerca de la corrección parcial en $P/PML$ usando el cálculo.

En la segunda parte de este trabajo, se ha estudiado el aspecto de derivación formal de procesos en $P/PML$. Como resultado, se ha desarrollado un cálculo de refinamientos que permite derivar procesos (parcialmente correctos) a partir de especificaciones. Dicho cálculo resulta ser consistente y "completo" (en un sentido). Además, se ha elegido el problema del control de la caldera de vapor para testear el cálculo con un caso de estudio complejo, mostrando su aplicabilidad y versatilidad.

Como trabajo futuro podría estudiarse el aspecto de verificación automática de procesos en $P/PML$, basándose en el cálculo de Hoare presentado en este trabajo, y a partir de allí el desarrollo de una herramienta automática de verificación para $P/PML$. Otros aspectos a estudiar son la corrección total de procesos en $P/PML$ y el desarrollo de un cálculo de refinamientos que permita derivar procesos totalmente correctos.

# Bibliografía


[1] Abrial J. R., Börger E. and Langmaack H., *Formal Methods for Industrial Applications: Specifying and Programming the Steam Boiler Control*, Springer-Verlag, 1996.

[2] Back R.J.R. y von Wright J., *Refinement Calculus: A Systematic Introduction*, Springer-Verlag, 1998.

[3] Baum G. A., Frias M. F. y Haeberer A. M., *Fork Algebras in Algebra, Logic and Computer Science*, Fundamenta Informaticae Vol. 32, 1997.

[4] Baum G. A., Frias M. F. y Maibaum T. S. E., *A Logic for Real-Time Systems Specification, Its Algebraic Semantics and Equational Calculus*, en Proceedings of AMAST'98, LNCS 1548, Springer-Verlag, pp. 91-105, 1998.

[5] Baum G. A., Frias M. F. y Maibaum T. S. E., *Adding Refinements to $P/PML$.*

[6] Baum G. A., Frias M. F. y Diaz J. R., *A $P/PML$ Solution for the Steam-Boiler Control Problem*, en Proceedings del WAIT'2000, 29 JAIIO, pp.13-29, 2000.

[7] Dijkstra E. W., *A Discipline of Programming*, Prentice Hall, Englewood Cliffs, 1976.

[8] Gordon M., *Specification and Verification I*, 1999.

[9] Gries D., *The Science of Programming*, Springer-Verlag, 1981.

[10] Hamilton A.G., *Logic for Mathematicians*, Cambridge University Press, 1981.

[11] Harel D., Dynamic Logic, *Handbook of Philosophical Logic. II: Extensions of Classical Logic*, D. Reidel, 1984.

[12] Hoare C. A. R., An Axiomatic Basis for Computer Programming, *Communications of the ACM*, 12:576-580, 1969.

[13] Loeckx, L. y Sieber K., *The Foundations of Program Verification*, John Wiley & Sons, 1984.

[14] Morgan C., *Programming from Specifications, Second Edition*, Prentice Hall, 1998.

[15] Wirth N., Program development by stepwise refinement, *Communications of the ACM*, 1971.

# Apéndice A

# Pruebas

LEMA A.0.1 *La fórmula de Hoare*

$$\{\psi\}\ \vec{x}\ _0(\textbf{if}\ []i \bullet \gamma_i \rightarrow S_i\ \textbf{fi})^{k\ \infty}\ \vec{x}\ \{\psi\},\ k \geq 0$$

*es derivable a partir de las fórmulas de Hoare* $\{\gamma_i[\vec{x}/\vec{z_i}] \wedge \psi \wedge t = t_0\}\ \vec{x}\ _{l_i} S_i^{\ u_i}\ \vec{x}\ \{\psi \wedge t < t_0\},\ i = 1..n$ *y de una teoría arbitraria.*

*Prueba.* Se denota por $IF$ al proceso **if** $[]i \bullet \gamma_i \rightarrow S_i$ **fi**. Se probará el enunciado por inducción sobre $k$. Supóngase que $k = 0$. Entonces, se tiene la siguiente deducción:

| | | |
|---|---|---|
| (1) | $\{\psi\}\ \vec{x}\ _\epsilon 1'_t{}^\epsilon\ \vec{x}\ \{\psi\}$ | $(SKIP)$ |
| (2) | $\psi \Rightarrow 0 \leq \epsilon$ | (Aritmética) |
| (3) | $\psi \Rightarrow \epsilon \leq \infty$ | (Aritmética) |
| (4) | $\{\psi\}\ \vec{x}\ _0 1'_t{}^\infty\ \vec{x}\ \{\psi\}$ | $(TIME$ 1,2,3) |

Supóngase que el enunciado es verdadero para $k$ con $k \geq 0$. Entonces se tiene la siguiente deducción:

| | | |
|---|---|---|
| (1) | $\{\gamma_i[\vec{x}/\vec{z_i}] \wedge \psi \wedge t = t_0\}\ \vec{x}\ _{l_i} S_i^{\ u_i}\ \vec{x}\ \{\psi \wedge t < t_0\},\ i = 1..n$ | (Hipótesis) |
| (2) | $\{\psi \wedge t = t_0\}\ \vec{x}\ _\epsilon IF^{\epsilon + max_i\{u_i\}}\ \vec{x}\ \{\psi \wedge t < t_0\}$ | $(IF$ 1) |
| (3) | $\{\psi\}\ \vec{x}\ _0 IF^{k\ \infty}\ \vec{x}\ \{\psi\}$ | (Hipótesis Inductiva) |
| (4) | $\psi \wedge t < t_0 \Rightarrow \psi$ | (Lógica) |
| (5) | $\{\psi \wedge t < t_0\}\ \vec{x}\ _0 IF^{k\ \infty}\ \vec{x}\ \{\psi\}$ | $(CONS$ 3,4) |
| (6) | $\{\psi \wedge t = t_0\}\ \vec{x}\ _\epsilon IF^{k+1\ \epsilon + max_i\{u_i\} + \infty}\ \vec{x}\ \{\psi\}$ | $(SEC$ 2,5) |
| (7) | $\psi \Rightarrow \psi \wedge t = t_0$ | (Lógica) |

| | | |
|---|---|---|
| (8) | $\{\psi\}\ \vec{x}\ {}_{\epsilon} IF^{k+1}\ {}^{\epsilon+max_i\{u_i\}+\infty}\ \vec{x}\ \{\psi\}$ | ($CONS$ 6,7) |
| (9) | $\psi \Rightarrow 0 \leq \epsilon$ | (Aritmética) |
| (10) | $\psi \Rightarrow \epsilon + max_i\{u_i\} + \infty \leq \infty$ | (Aritmética) |
| (11) | $\{\psi\}\ \vec{x}\ {}_{0} IF^{k+1}\ {}^{\infty}\ \vec{x}\ \{\psi\}$ | ($TIME$ 8,9,10) |

■

PROPIEDAD A.0.2 *Sean $S, S', T, T' \in RT(\mathcal{S})$ tales que $\wp(S') \subseteq \wp(S)$ y $\wp(T') \subseteq \wp(T)$. Entonces*

1. *$\wp(S'^*) \subseteq \wp(S^*)$, y*
2. *$\wp(S' \odot T') \subseteq \wp(S \odot T)$, si $\odot \in \{;, +, \cdot\}$.*

*Prueba.*

1. Si $s^* \in \wp(S'^*)$ entonces por Def. 3.2.3 se tiene que $s \in \wp(S')$. Luego por hipótesis, $s \in \wp(S)$ y nuevamente por Def. 3.2.3 se tiene $s^* \in \wp(S^*)$.
2. Si $s \odot t \in \wp(S' \odot T')$ entonces por Def. 3.2.3 se tiene que $s \in \wp(S')$ y $t \in \wp(T')$. Luego por hipótesis, $s \in \wp(S)$ y $t \in \wp(T)$. Nuevamente por Def. 3.2.3 se tiene $s \odot t \in \wp(S \odot T)$.

■

LEMA A.0.3 *Sea $S \in GRT(\mathcal{S})$. Luego*

$$Th(\mathcal{A}) \cup RTh(\mathcal{A}) \models \vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l} \sqsubseteq S \text{ si y sólo si } Th(\mathcal{A}) \cup HTh(\mathcal{A}) \models \{\alpha\}\ \vec{x}\ {}_{l} S^{u}\ \vec{y}\ \{\beta\}.$$

*Prueba.* Sean $W$ y $W'$ los conjuntos $Th(\mathcal{A}) \cup RTh(\mathcal{A})$ y $Th(\mathcal{A}) \cup HTh(\mathcal{A})$ respectivamente, y $r$ la fórmula $\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l} \sqsubseteq S$.

| | |
|---|---|
| $W \models r$ sii $\models_{\mathcal{M}} r$ para todo modelo $\mathcal{M}$ de $W$ | (Definición) |
| sii $\wp(S) \subseteq \wp(\vec{x}, \vec{y} : [\alpha,\ \beta]\ {}^{u}_{l})$ | (Def. 3.2.5) |
| sii $S \in \left\{ R \in GRT(\mathcal{S}) : W' \vdash \{\alpha\}\ \vec{x}\ {}_{l} R^{u}\ \vec{y}\ \{\beta\} \right\}$ | (Def. 3.2.3) |
| sii $W' \vdash \{\alpha\}\ \vec{x}\ {}_{l} S^{u}\ \vec{y}\ \{\beta\}$ | (Conjuntos) |
| sii $W' \models \{\alpha\}\ \vec{x}\ {}_{l} S^{u}\ \vec{y}\ \{\beta\}$ | (Teo. 2.4.1,2.4.2) |

■