

PROCEDIMIENTOS DE DECISION PARA LA EQUIVALENCIA Y LA CONGRUENCIA OBSERVACIONAL DE TERMINOS REGULARES DE CCS

A. SORIANO

UNIVERSIDAD CENTRAL DE VENEZUELA

RESUMEN

Se presenta la descripción de procedimientos de decisión para la equivalencia y la congruencia observacional de CCS. Dichos procedimientos de decisión se basan en transformaciones realizadas sobre los sistemas de transiciones que representan los comportamientos descritos por los términos, y en la noción de bisimulación. Estas transformaciones son de dos tipos: unas correspondientes a la eliminación de bucles y cadenas de acciones no visibles y la otras correspondientes a la eliminación de duplicidades de un mismo comportamiento.

INTRODUCCION.

Actualmente con el desarrollo de los sistemas distribuidos y la concepción de lenguajes de programación capaces de expresar el paralelismo, es posible construir sistemas cada vez más poderosos y rápidos. Sin embargo, estos sistemas son cada vez más complejos, de allí que hoy por hoy en la concepción de sistemas comunicantes, es indispensable de realizar una fase de verificación que permita garantizar la fiabilidad de los sistemas.

La verificación de sistemas comunicantes es hoy en día un campo activo de investigación. En el presente trabajo nos interesamos por el problema de la verificación automática de sistemas comunicantes regulares.

Verificar la descripción de un sistema consiste en compararla con una especificación. Desde un punto de vista teórico, es posible distinguir entre dos tratamientos diferentes. Un tratamiento basado en la lógica [AS 79] [Pn 77] [Ab 79] donde las propiedades a verificar se representan por un conjunto de aserciones sobre el comportamiento. Este tratamiento permite verificar propiedades generales de los sistemas como por ejemplo la ausencia de abrazo mortal. El otro tratamiento se basa en teorías algebraicas [Mi 80] [Mi 83] [BK 85] [AB 84] [BH 84] en las que las descripciones de los sistemas y sus especificaciones se escriben como términos de un álgebra y las pruebas se realizan en base a una noción de equivalencia entre los términos del álgebra; este enfoque permite verificar propiedades específicas de los sistemas, como por ejemplo, la especificación del servicio de un protocolo de comunicación. En lo sucesivo, consideraremos esta segunda forma de especificación.

En la literatura, hay varios ejemplos de verificación de sistemas comunicantes basados en un álgebra [Mi 80] [BK 84] [Ko 85]. Pero el problema principal en este tipo de pruebas está ligado a la manipulación de términos, y cuando más complejos son los sistemas, más aumenta cantidad de cálculo necesaria para la verificación; de ahí la necesidad de su automatización.

Este trabajo se orienta en esta dirección y su objetivo es el describir

un procedimiento de decisión para la equivalencia y la congruencia observacional de términos regulares del cálculo CCS de Milner [Mi 80].

CCS [Mi 80] es un cálculo para la descripción, la especificación y la verificación de sistemas comunicantes asincronos. Este cálculo está basado en dos ideas principales: la observación y la comunicación sincrónica.

Informalmente, en CCS, puede describirse el comportamiento observable de un sistema (noción de observación). Es a partir de esta noción de observación que se definen los criterios de comparación de sistemas (equivalencia y congruencia observacional).

La descripción de un sistema puede hacerse también por composición paralela (operación que se escribe como $\parallel$) de procesos que se comunican entre ellos. La comunicación de procesos se considera como una acción indivisible del sistema (idea de comunicación sincronizada), esta acción se denomina comunicación interna y se denota por τ .

De una manera mas formal, las verificaciones de sistemas comunicantes consisten en transformar y comparar un término que describe un sistema con su especificación representada por otro término.

Recientemente, se han publicado trabajos [HM 85] [BK 85] [Mi 85] en los que se presenta una axiomatización completa para la equivalencia y la congruencia observacional, sin embargo, es importante disponer de procedimientos de verificación automatizables.

Este trabajo se orienta en este sentido y en él se describen procedimientos de decisión para la equivalencia y la congruencia observacional de términos regulares de CCS. Los procedimientos que se describen se basan en la aplicación de transformaciones ad-hoc definidas sobre *relaciones de transición* representando los comportamientos de los términos CCS y en la noción de *bisimulación*.

El trabajo consiste de tres partes: en la primera parte se realiza una descripción del álgebra de CCS y la definición y axiomatización de la equivalencia y la congruencia observacional, en la segunda parte se describen los procedimientos de decisión de la equivalencia y la congruencia observacional y por último se da una conclusión.

I.- CCS: "Calcul of Communicating Systems".

CCS es un álgebra de términos provista de una relación de congruencia. La semántica operacional de su lenguaje le permite interpretar los términos como procesos (sistemas de transición comunicantes). La relación de congruencia permite la comparación de los términos.

En este trabajo, nos restringimos al álgebra de procesos que representa los comportamientos regulares.

I.1.- Álgebra para CCS.

Sea:

- D , un conjunto de nombres de *acciones* o *puertos de comunicación* cuyos elementos se identifican por letras minúsculas,
- $\sim D$, un conjunto de nombres de *puertos* llamados *complementarios* cuyos

- elementos son los elementos de D precedidos por el símbolo " $\sim$ ",
- una biyección:
 $\alpha \longleftrightarrow \sim\alpha$, donde $\alpha \in D$,
 $\sim\alpha \in \sim D$,
 se dice que " $\sim\alpha$ " es el *puerto complementario* de " α ",
 ésto nos permite definir la interacción entre procesos,
 - τ , ($\tau \in D$ et $\tau \in \sim D$) una etiqueta que representa una *acción no observable* resultante de una comunicación interna entre α y $\sim\alpha$, $\alpha \in D$,
 - P , el conjunto de etiquetas de puertos de comunicación, $P = D \cup \sim D$,
 - $P_\tau = P \cup \{\tau\}$,
 - F , el conjunto de funciones de redefinición f tales que:
 $f: L \subseteq P \longrightarrow M \subseteq P$
 f es una biyección,
 f respeta los complementos definidos por la biyección,
 - Y , el conjunto de variables de comportamiento,
 - las firmas, $\Sigma_1 = (P_\tau, \text{nil}, +)$
 $\Sigma_2 = (P_\tau, \text{nil}, +, \parallel, [], \backslash)$

donde:

nil es una constante,
 $+$ et $\parallel$ son operadores binarios,
 $\forall \alpha \in P_\tau$ α , $\forall f \in F$ $[f]$, $\forall \alpha \in P$ $\backslash \alpha$, son operadores unarios.

Los operadores $+$ y $\parallel$ son operadores infijos, α es un operador prefijo, $[f]$ y $\backslash \alpha$ son operadores postfixos. El símbolo "." se utiliza como separador después del operador α , por ejemplo se escribe $\alpha.\text{nil}$ y no αnil .

La prioridad es creciente para los operadores $+$ y $\parallel$, $[f]$ y $\backslash \alpha$, α . Los operadores $+$, $\parallel$, $[f]$ y $\backslash \alpha$ son asociativos a izquierda y el operador α es asociativo a derecha.

Representamos por:

- T_f , el álgebra de firma Σ_2 . Los elementos de T_f se llaman *términos finitos*.
 Se dice que un término finito está escrito en *forma de suma* si:
 - sea $t = \text{nil}$,
 - sea $t = \sum_{i \in I} \alpha_i.t_i$ y cada t_i es un término finito escritos en forma de suma.
- T_s , es el subconjunto de términos finitos en forma de suma. ($T_s \subseteq T_f$).
- $\Pi[\Sigma_1, Y]$, el álgebra de firma $\Sigma_1 \cup Y$. ($T_s \subseteq \Pi[\Sigma_1, Y]$).
- $\Pi[\Sigma_2, Y]$, el álgebra de firma $\Sigma_2 \cup Y$. ($\Pi[\Sigma_1, Y] \subseteq \Pi[\Sigma_2, Y]$ y $T_f \subseteq \Pi[\Sigma_2, Y]$).

Los elementos de $\Pi[\Sigma_1, Y]$ y los de $\Pi[\Sigma_2, Y]$ son expresiones a

partir de las cuales se construyen los términos que definen comportamientos infinitos.
 T_r , el conjunto de pares de la forma: $u = (t, E)$
 donde $t \in \Pi[\Sigma_2, Y]$,

E es un conjunto de ecuaciones de la forma: $\{v_i = t_i\}_{i=1, \dots, n}$
 donde $v_i \in Y$ y $t_i \in \Pi[\Sigma_1, Y]$ y $\forall i, j \ i \neq j \Rightarrow v_i \neq v_j$. Se dice que t_i
 es la *definición* de v_i .

Los elementos de T_r definen los comportamientos infinitos. Los
 pares $(t, \emptyset) \in T_r$ (*términos finitos*) sont escritos simplemente t . ($T_f \subseteq T_r$).

Para los términos de T_r se introducen las nociones de *variable*
útil, *variable inútil*, *variable libre*, *término cerrado*, *variable no*
guardada, *término guardado* y *término bien guardado*. Estas
 nociones se utilizan para definir los términos regulares.

Para $t \in \Pi[\Sigma_2, Y]$, sea $\text{var}(t)$ el conjunto de variables de t .

Para un término $u = (t, E)$, se dice que una variable v es *útil* si y
 solamente si $v \in \bigcup_{j=0}^{\text{card}(E)} \rho^j(\text{var}(t))$, donde $\rho(X)$ se define como:

$$\rho(X) = \{z \mid v_i \in X \text{ y } v_i = t_i \text{ y } z \in \text{var}(t_i)\},$$

ρ^0 es la identidad

$$\rho^{k+1}(X) = \rho(\rho^k(X)), \text{ para } k > 1.$$

Se dice que una variable v est *inútil* en un término $u = (t, E)$ si y
 solamente si $\exists t_i$ tal que $v = t_i$ pertenece a E y v no es una variable útil
 del término u .

Se dice que una variable v es *libre* en un término $(t, E) \in T_r$ si y
 solamente sino existe j tal que $v = t_j \in E$.

Se dice que un término es *cerrado* si y solamente si no contiene
 variables libres.

Se dice que una variable v *no es guardada* en un término $u = (t, E)$
 si y solamente si v aparece en t o en la definición de una variable útil
 de u sin estar precedida por una acción.

Se dice que un término $u = (t, E)$ es *guardado* si y solamente si
 toda variable no guardada del término puede reemplazarse por nil o
 por una expresion de la forma $\sum \alpha_i t_i$, oar substitución repetida de
 variables por sus definiciones.

Se dice que un término $u = (t, E)$ es *bien guardado* si y solamente
 si él es guardado y toda variable guardada por τ en él, puede ser
 reemplazada por nil o por una expresión de la forma
 $\sum_{i=1, \dots, n} \alpha_i t_i$, $\alpha_k \neq \tau$.

Sobre los términos de T_r definimos los operadores α , $+$, $\parallel$, $!$, $[f]$
 de la manera siguiente:

$$\alpha(t, E) = (\alpha t, E)$$

$$(t_1, E_1) + (t_2, E_2) = (t_1 + t_2, E_1 \cup E_2), \quad \text{si } \exists x_i \in Y \text{ tal que } x_i = t_i \in E_1 \\ \text{y } x_i = t'_i \in E_2$$

$$(t_1, E_1) \parallel (t_2, E_2) = (t_1 \parallel t_2, E_1 \cup E_2), \quad \text{si } \exists x_i \in Y \text{ tal que } x_i = t_i \in E_1 \\ \text{y } x_i = t'_i \in E_2$$

$$(t, E)\alpha = (t\alpha, E)$$

$$(t, E)\eta = (t\eta, E)$$

- T_r , es el subconjunto de términos cerrados y guardados de T_r .

Los elementos de T_r son los términos regulares de CCS.

I.2.- Semántica operacional de los operadores.

La semántica operacional [PI 81] de CCS se da a través de relaciones de transición $\xrightarrow{\alpha}$, $\alpha \in P_r$. Estas relaciones son las más pequeñas relaciones binarias sobre T_r definidas por las reglas:

$$\frac{t \xrightarrow{\alpha} t'}{(t, E) \xrightarrow{\alpha} (t', E)}$$

$$\frac{v = t' \in E \text{ et } t[t'_i/v_i] \xrightarrow{\alpha} t''}{(t, E) \xrightarrow{\alpha} (t'', E)}$$

$$(\alpha): \quad \alpha.t \xrightarrow{\alpha} t \quad (\text{ACCION})$$

$$(1) \quad \frac{t_1 \xrightarrow{\alpha} t'_1}{t_1 + t_2 \xrightarrow{\alpha} t'_1} \quad (\text{ESCOGENCIA NO DETERMINISTA})$$

$$(2) \quad \frac{t_2 \xrightarrow{\alpha} t'_2}{t_1 + t_2 \xrightarrow{\alpha} t'_2}$$

$$\begin{array}{ll}
 \text{(ID)} & \frac{t_1 \xrightarrow{\alpha} t'_1}{t_1 \parallel t_2 \xrightarrow{\alpha} t'_1 \parallel t_2} \\
 (1) & \\
 & \frac{t_2 \xrightarrow{\alpha} t'_2}{t_1 \parallel t_2 \xrightarrow{\alpha} t_1 \parallel t'_2} \quad (\text{COMPOSICION PARALELA}) \\
 (2) & \\
 & \frac{t_1 \xrightarrow{\alpha} t'_1, t_2 \xrightarrow{\alpha} t'_2}{t_1 \parallel t_2 \xrightarrow{\alpha} t'_1 \parallel t'_2} \\
 (3) & \\
 \text{(I)} & \frac{t \xrightarrow{\alpha} t', \alpha \neq \beta}{t\beta \xrightarrow{\alpha} t'} \quad (\text{BORRADO}) \\
 \text{(II)} & \frac{t \xrightarrow{\alpha} t'}{\eta\eta \xrightarrow{f(\alpha)} t[\eta]} \quad (\text{REDEFINICION})
 \end{array}$$

Notación:

- Sea $s = \alpha_1 \dots \alpha_n, n \geq 0$ y $\alpha_i \in P$
 entonces $p(\xrightarrow{\tau})^* \xrightarrow{\alpha_1} (\xrightarrow{\tau})^* \dots \xrightarrow{\alpha_n} (\xrightarrow{\tau})^* p$
 se escribe como $p = s \Rightarrow p'$.
- $t(\xrightarrow{\tau})^* t'$ se escribe como $t \Rightarrow t'$.
- $t(\xrightarrow{\tau})^+ t'$ se escribe como $t = \tau \Rightarrow t'$.

I.3.- Relaciones de equivalencia y de congruencia.

R. Milner define relaciones de equivalencia y de congruencia sobre T_P . Estas relaciones definen criterios de comparación entre términos. A continuación se presentan tres relaciones definidas para T_P . Estas relaciones son:

- la congruencia fuerte
- la equivalencia observacional
- la congruencia observacional

1.3.1. Congruencia Fuerte.

Sean: $p, q \in T_r$.

R una relación binaria sobre T_r y $F(R)$ la función:

$(p, q) \in F(R)$ ssi (i) $p \xrightarrow{\alpha} p'$ implica $\exists q' (q \xrightarrow{\alpha} q' \text{ y } (p', q') \in R)$ y
(ii) $q \xrightarrow{\alpha} q'$ implica $\exists p' (p \xrightarrow{\alpha} p' \text{ y } (p', q') \in R)$.

Definición 1.1.

Se dice que R es una *bisimulación* si y solamente si $R \subseteq F(R)$.

Definición 1.2.

La *equivalencia fuerte* (escrita $\sim$) se define como la más grande relación de bisimulación, es decir:

$$\sim = \cup \{ R \subseteq T_r \times T_r \mid R \subseteq F(R) \}.$$

La relación $\sim$ existe y es única porque F es monótona en el reticulado de las relaciones binarias con la inclusión de conjuntos ($\subseteq$).

Para los términos pertenecientes a T_r , la axiomatización de la *equivalencia fuerte* esta dada por: $(A_1)-(A_{16})$ de la Tabla 1. Esta relación de equivalencia es una relación de congruencia para los operadores α , $+$ et $\parallel$. En lo sucesivo se denominará *congruencia fuerte*.

1.3.2.- Equivalencia Observacional.

La equivalencia observacional se define exactamente como la congruencia fuerte, excepto que se utilizan las relaciones $\xrightarrow{\alpha} \Rightarrow$ et $\Rightarrow$ en lugar de $\xrightarrow{\alpha}$ et $\rightarrow$. La equivalencia observacional se escribe como $\approx$.

Proposición 1.1.

Para dos términos $t_1, t_2 \in T_r$, $t_1 \approx t_2$ si y solamente si se verifican las condiciones siguientes:

- (i) $t_1 \xrightarrow{\alpha} t'_1$ implica $(\alpha = \tau \text{ y } t'_1 \approx t_2)$
o $\exists t'_2 (t_2 \xrightarrow{\alpha} t'_2 \text{ y } t'_1 \approx t'_2)$
- (ii) $t_2 \xrightarrow{\alpha} t'_2$ implica $(\alpha = \tau \text{ y } t'_2 \approx t_1)$
o $\exists t'_1 (t_1 \xrightarrow{\alpha} t'_1 \text{ y } t'_1 \approx t'_2)$.

Proposición 1.2.

$p \sim q$ implica $p \approx q$.

La relación de equivalencia observacional no es una relación de congruencia. Por ejemplo: $a.nil \approx \tau.a.nil$ pero, $b.nil + a.nil \not\approx a.nil$

observacionalmente equivalente a $b.nil + \tau.a.nil$.

Para términos pertenecientes a T_F , La equivalencia observacional esta axiomatizada por: $(A_1)-(A_{20})$ de la Tabla 1.

1.3.3.- Congruencia Observacional.

La *congruencia observacional* (escrita $\approx^C$) se define como la mayor relación de congruencia para los operadores α , $+$ et $\parallel$ incluida en la equivalencia observacional.

Proposition 1.3.

Para dos términos $t_1, t_2 \in T_F$, $t_1 \approx^C t_2$ si y solamente si $\forall \alpha \in P_T$ se verifican la condiciones siguientes:

- (1) $t_1 \xrightarrow{\alpha} t'_1$ implica $\exists t'_2 (t_2 \xrightarrow{\alpha} t'_2 \text{ y } t'_1 \approx t'_2)$
- (2) $t_2 \xrightarrow{\alpha} t'_2$ implica $\exists t'_1 (t_1 \xrightarrow{\alpha} t'_1 \text{ y } t'_1 \approx t'_2)$

En la proposición siguiente, damos una nueva caracterización para la congruencia observacional. Esta caracterización se utilizará en la definición del procedimiento de decisión de la congruencia observacional.

Proposition 1.4.

Para dos términos $t_1, t_2 \in T_F$, $t_1 \approx^C t_2$ si y solamente si se verifican las condiciones siguientes:

- $t_1 \approx t_2$,
- $t_1 \xrightarrow{\tau} t'_1$ implica $\exists t'_2$ tal que $t_2 \xrightarrow{\tau} t'_2 \text{ y } t'_1 \approx t'_2$,
- $t_2 \xrightarrow{\tau} t'_2$ implica $\exists t'_1$ tal que $t_1 \xrightarrow{\tau} t'_1 \text{ y } t'_1 \approx t'_2$.

Para los términos pertenecientes a T_F , la axiomatización de la equivalencia observacional está dada por: $(A_1)-(A_{19})$ de la Tabla 1.

Milner a demostrado la completitud de una axiomatización para la congruencia observacional para los términos recursivos. Esta axiomatización está definida para términos recursivos escritos de manera diferente a la nuestra, sin embargo, los axiomas y reglas de inferencia de nuestro formalismo pueden obtenerse de los suyos por transformaciones sintácticas. De esta manera, una axiomatización completa para la congruencia observacional de términos de T_F está dada por los axiomas $(A_1)-(A_{19})$ de la Tabla 1 y los axiomas y reglas de inferencia dados en la Tabla 2.

Cabe destacar que los axiomas (A_6) , (A_7) , (A_{12}) , (A_{14}) , (A_{16}) indicando las propiedades de asociatividad, conmutatividad y distributividad de los operadores $\parallel$, $\mid$ y $[\]$ no pueden deducirse de los otros axiomas; pero en lo sucesivo no se utilizarán dichos axiomas porque todas sus instancias pueden deducirse.

TABLA 1:

(I):	(A ₁):	$t_1 + (t_2 + t_3) = (t_1 + t_2) + t_3$
	(A ₂):	$t_1 + t_2 = t_2 + t_1$
	(A ₃):	$t + t = t$
	(A ₄):	$t + \text{nil} = t$
	(A ₅):	Si t_1 y t_2 son de la forma: $t_1 = \sum_{i=1, \dots, n} \alpha_i \cdot t_i \quad \text{et} \quad t_2 = \sum_{j=1, \dots, n} \beta_j \cdot t_j$ entonces: $t_1 \parallel t_2 = \sum \alpha_i \cdot (t_i \parallel t_2) + \sum \beta_j \cdot (t_1 \parallel t_j) + \sum \tau \cdot (t_i \parallel t_j)$ $\alpha_i = \sim \beta_i \wedge \sim \alpha_j = \beta_j \wedge i=1, \dots, n \wedge j=1, \dots, n$
(II):	(A ₆):	$t_1 \parallel t_2 = t_2 \parallel t_1$
	(A ₇):	$t_1 \parallel (t_2 \parallel t_3) = (t_1 \parallel t_2) \parallel t_3$
	(A ₈):	$t \parallel \text{nil} = t$
	(A ₉):	$(\alpha.t) \parallel \eta = \eta(\alpha) \cdot (t \parallel \eta)$
	(A ₁₀):	$(t_1 + t_2) \parallel \eta = t_1 \parallel \eta + t_2 \parallel \eta$
(III):	(A ₁₁):	$\text{nil} \parallel \eta = \text{nil}$
	(A ₁₂):	$(t_1 \parallel t_2) \parallel \eta = t_1 \parallel \eta \parallel t_2 \parallel \eta$
	(I):	$(A_{13}): (\alpha.t) \beta = \begin{cases} \text{nil} & \text{si } \alpha = \beta \text{ o } \alpha = \sim \beta \\ \alpha.(t\beta) & \text{si no} \end{cases}$
	(A ₁₄):	$(t_1 + t_2) \alpha = t_1 \alpha + t_2 \alpha$
	(A ₁₅):	$\text{nil} \alpha = \text{nil}$
(IV):	(A ₁₆):	$\eta \alpha_1 \alpha_2 = \eta \alpha_2 \alpha_1$
	(A ₁₇):	$t + \tau.t = \tau.t$
	(A ₁₈):	$\alpha.(t_1 + \tau.t_2) = \alpha.(t_1 + \tau.t_2) + \alpha.t_2$
	(A ₁₉):	$\alpha.\tau.t = \alpha.t$
	(A ₂₀):	$\tau.t = t$

TABLA 2:

	$t_1 = t_2$
(1):	$(t, E \cup \{x_1=t_1\}) = (t, E \cup \{x_2=t_2\})$
(2):	$(t, E \cup \{x_1=t_1, x_2=t_2\}) = (t, E \cup \{x_1=t_1, x_2=t_2[t_1/x_1]\})$
(3):	$\frac{(z_i, E) = (t_i[z_j/x_j]_{j=1, \dots, n}, E)}{(z_i, E) = (x_i, \{x_j=t_j\}_{j=1, \dots, n})} \quad \text{var}(t_j) \{x_1, \dots, x_n\}$
(4):	$\frac{x \notin \text{útil}(t, E)}{(t, E) = (t, E \cup \{x=t_1\})}$
(5):	$(t, E \cup \{x=\tau.x+t_1\}) = (t, E \cup \{x=\tau.t_1\})$
(6):	$(t, E \cup \{x=\tau.(x+t_1)+t_2\}) = (t, E \cup \{x=\tau.x+t_1+t_2\})$

II. Verificación de términos regulares

En esta parte, se presenta un procedimiento de decisión para la congruencia fuerte, la equivalencia observacional y la congruencia observacional de términos que describen comportamientos regulares (*términos regulares*).

Este procedimiento utiliza la noción de *sistema de transiciones* para representar las derivaciones de los términos y la noción de *bisimulación* para compararlos. A partir de estas nociones y basándose en la propiedad I.1., se obtiene directamente un procedimiento de decisión para la congruencia fuerte. Considerando las proposiciones I.2. y I.4. definimos las *transformaciones ED* y *Q* que permiten decidir respectivamente la equivalencia y la congruencia observacional por *simulación*.

Para decidir cada una de las equivalencias que se han definido sobre T_P , procedemos en tres etapas:

1. Construcción del *sistema de transiciones* asociado a cada término a comparar.
2. Aplicación de transformaciones ad hoc sobre los sistemas de

transición construidos.

3. Decidir la equivalencia correspondiente por bisimulación entre los sistemas de transiciones transformados.

II.1.- Construcción de sistemas de transiciones.

Definición II.1.

Un sistema de transiciones S_u asociado a un término $u=(t,E) \in T_r$ se define de la manera siguiente:

$$S_u = (Q, \cup_{\alpha \in P_r} R_\alpha, t)$$

donde:

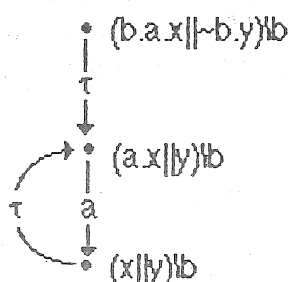
Q es un conjunto de estados correspondiente al conjunto de términos obtenidos por derivación a partir de u ,

$R_\alpha \subseteq Q \times Q$ se define como: $(q', q'') \in R_\alpha$ si y solamente si $(t', E) \xrightarrow{\alpha} (t'', E)$ y $q' = (t', E)$ y $q'' = (t'', E)$.

Para indicar $(p, q) \in R_\alpha$ se utiliza también $p \xrightarrow{\alpha} q$ y de manera análoga se utilizan las notaciones $=\alpha \Rightarrow$ et $\Rightarrow$.

u es el estado inicial del sistema.

Por ejemplo, el sistema de transiciones asociado al término: $((b.a.x || \sim b.y) \backslash b, \{x=b.a.x, y=\sim b.y\})$, es:



Es posible extender las relaciones $\sim$, $\approx$ et $\approx^C$ definidas sobre los términos, a los sistemas de transiciones correspondientes; es decir, para los términos $t_1, t_2 \in T_r$,

- (i) $t_1 \sim t_2$ si y solamente si $S_{t_1} \sim S_{t_2}$
- (ii) $t_1 \approx t_2$ si y solamente si $S_{t_1} \approx S_{t_2}$
- (iii) $t_1 \approx^C t_2$ si y solamente si $S_{t_1} \approx^C S_{t_2}$

II.2.- Transformaciones de sistemas de transiciones.

En esta parte, se definen las transformaciones $E\mathcal{D}$ y $\mathcal{A}\mathcal{D}$. Se dan algunas propiedades interesantes de dichas transformaciones y su utilización para decidir la equivalencia y la congruencia observacional de términos de T_r .

2.1.- Transformación EO.

Teóricamente, para decidir la equivalencia observacional de términos regulares, es suficiente construir para cada término el sistema de transiciones $O(S)$ que representa las relaciones $\Rightarrow_{\alpha}$ para $\alpha \in P$ y $\Rightarrow$ para la acción τ y decidir la equivalencia por bisimulación entre los sistemas de transiciones construidos (proposition 1.2).

Definición II.2.

Si $S=(Q, \cup_{\alpha \in P} R_{\alpha}, q_0)$ entonces $\mathcal{L}(S)=(Q, \cup_{\alpha \in P} R'_{\alpha}, q_0)$ es el sistema de transiciones que para todo $\alpha \in P$ se verifican las condiciones siguientes:

- $q \xrightarrow{\alpha} q'$ es una transición de $\mathcal{L}(S)$ si y solamente si $q \Rightarrow_{\alpha} q'$ es una derivación de S
- $q \xrightarrow{\tau} q'$ es una transición de $\mathcal{L}(S)$ si y solamente si $q \Rightarrow q'$ es una derivación de S ($\xrightarrow{\tau}$ es reflexiva en $\mathcal{L}(S)$).

Siguiendo la terminología de Bergstra y Klop [BK 85], llamaremos *saturation* esta transformación de S en $\mathcal{L}(S)$.

Por ejemplo, si se quiere decidir la equivalencia observacional de los términos u y v definidos como:

$$u = ((x||y)d, \{x=d.\sim d.x+a.c.nil, y=\sim d.(b.nil+d.y)\})$$

$$v = ((x||y)d, \{x=d.(b.nil+a.\sim d.nil), y=\sim d.d.c.nil\})$$

- Se construyen los sistemas de transiciones S_u y S_v (Figuras S_u et S_v).

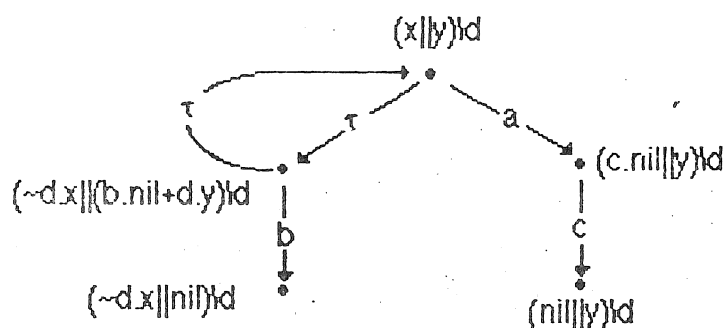


Figura S_u

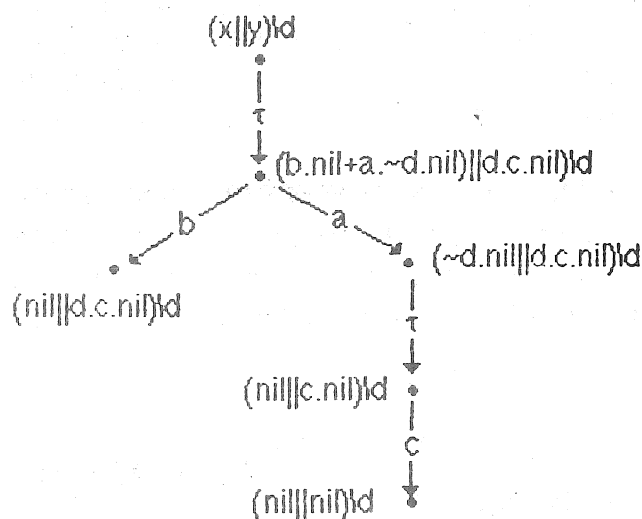


Figura S_V

- A partir de S_U y de S_V , se construyen los sistemas de transiciones $\mathcal{L}(S_U)$ y $\mathcal{L}(S_V)$ (Figura R).
- Se calcula la relación de bisimulación R entre los sistemas $\mathcal{L}(S_U)$ y $\mathcal{L}(S_V)$; dicha relación se ilustra en la Figura R. Se concluye que $u \approx v$.

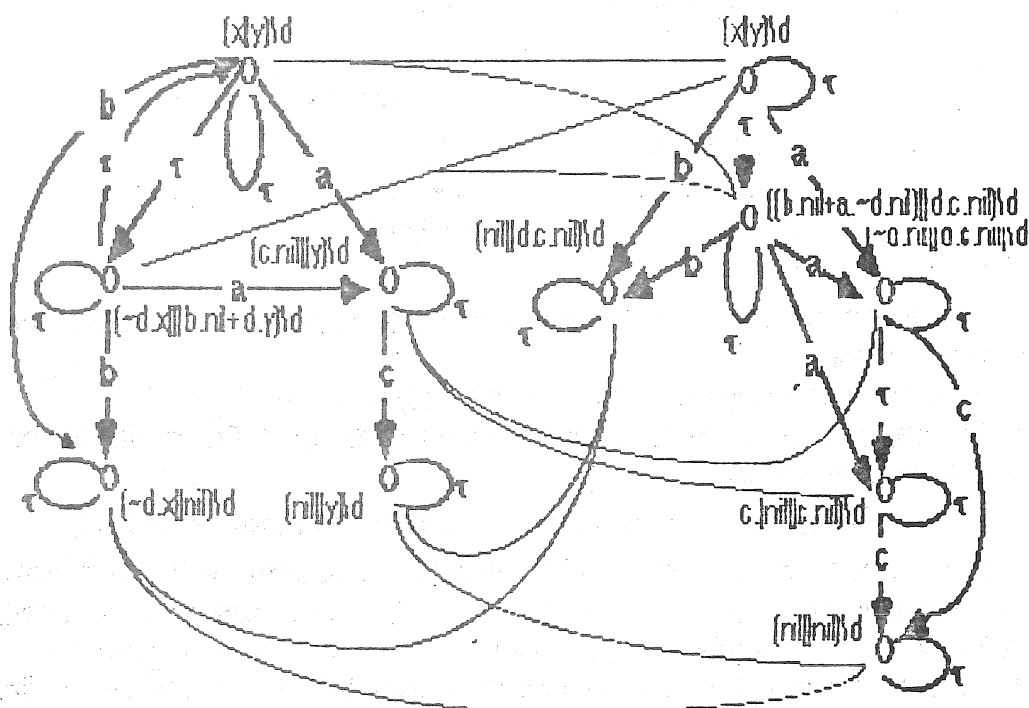


Figura R.

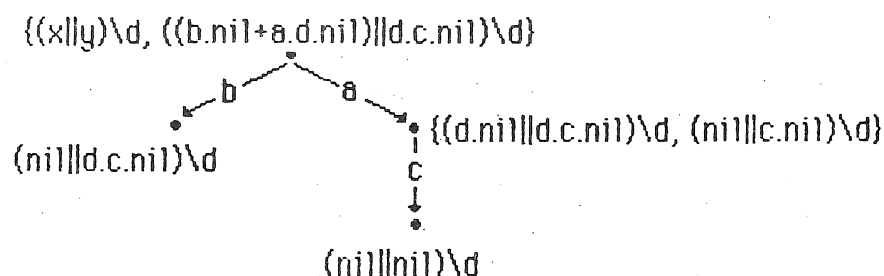
Teniendo en cuenta que la saturación agrega transiciones al sistema, es interesante intentar reducir el sistema inicial antes de la aplicación de dicha transformación.

De hecho, en ciertos casos, es posible de reducir una cantidad considerable de los estados (sub-términos) y de las transiciones (derivaciones) a

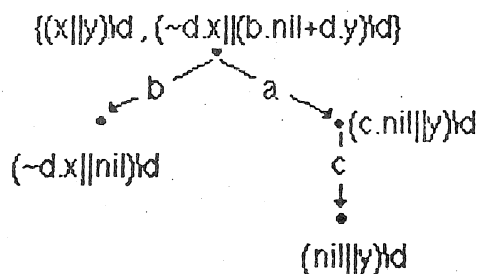
tratar. Estas reducciones pueden definirse de una manera sintáctica a través de reglas de reescritura a aplicarse a los sistemas de transiciones. Estas reducciones permiten en ciertos casos reducir de manera considerable la cantidad de cálculo necesaria para decidir la equivalencia observacional de términos.

Las reducciones que se proponen corresponden a:

- la eliminación de 'cadenas de acciones no observables' (*reducciones*): en el ejemplo anterior, para el sistema de transiciones asociado al término y , esta reducción produce el sistema de transiciones:



- la eliminación de circuitos de acciones no observables: en el ejemplo anterior, para el sistema de transiciones asociado al término u , esta reducción produce el sistema de transiciones:



De esta manera, para la verificación de la equivalencia observacional del ejemplo anterior:

- se construyen los sistemas de transiciones ilustrados en la Figura R'.
- se calcula la relación de bisimulación R' ilustrada en la Figura R'. Así es posible concluir que $u \approx v$.

A continuación, se definen las transformaciones *reducciones* y *reducciones* sobre los sistemas de transiciones asociados a los términos. Enunciamos las propiedades de preservación de la equivalencia observacional. Se define la transformación EO y se enuncia la proposición que garantiza la decidibilidad de la equivalencia observacional de dos términos por bisimulación aplicando la transformación EO a los sistemas de transiciones asociados a dichos términos.

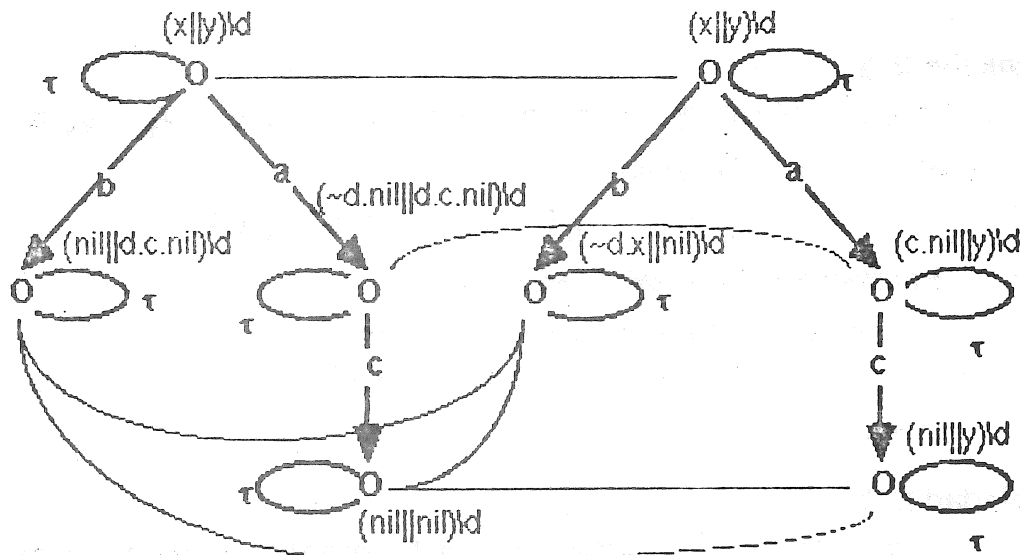


Figura R'

Definición II.3.

Para un sistema de transiciones $S = (Q, \cup_{\alpha \in P_{\tau}} R_{\alpha}, \tau)$,

- Se dice que una transición $p \xrightarrow{\tau} q$ es una *cadena de τ* en S si y solamente si ella es la única transición posible a partir del estado p .
- Se dice que $p_1 \xrightarrow{\tau} p_2, \dots, p_n \xrightarrow{\tau} p_1 \in R_{\tau}$ y $p_1 \xrightarrow{\tau} p_1 \in R_{\tau}$ constituyen *circuitos de τ* en S .

Propiedad II.1.

Todo par de sistemas de transiciones S_1, S_2 verifica:

$S_1 \approx S_2$ si y solamente si $O(S_1) \sim O(S_2)$.

Definición II.4.

La eliminación de las cadenas de τ de un sistema de transiciones

$S_u = (Q, \cup_{\alpha \in P_{\tau}} R_{\alpha}, u)$, consiste en:

- eliminar toda transición $t \xrightarrow{\tau} t' \in R_{\tau}$, si ella es la única transición posible a partir del estado t ,
- la substitución del estado t' por el estado t en el sistema resultante.

Propiedad II.2.

La transformación τ -cadenas preserva la equivalencia observacional. Es decir, dos sistemas de transiciones S_1 y S_2 son observacionalmente equivalentes si y solamente si después de la aplicación de la transformación τ -cadenas ellos son observacionalmente equivalentes.

Definición II.5.

Para un sistema de transiciones $S_U = (Q, \cup_{\alpha \in P_T} P_{\alpha}, u)$, la eliminación de circuitos de τ

$$t_1 \xrightarrow{\tau} t_2, \dots, t_n \xrightarrow{\tau} t_1 \in R_{\tau} \quad \text{o} \quad t_1 \xrightarrow{\tau} t_1 \in R_{\tau}$$

(transformación τ -circuitos) consiste en:

- eliminar toda transición $t_i \xrightarrow{\tau} t_j$ del circuito,
- la substitución de cada estado del circuito por t_1 en el sistema resultante.

Propiedad II.3.

La transformación τ -circuitos preserva la equivalencia observacional.

Définition 1. II.6.

Para todo sistema de transiciones S , la transformación EO se define como $EO(S) = O(S')$ donde S' es el sistema obtenido por aplicación de las transformaciones τ -cadenas y τ -circuitos sobre S .

Proposition 1. II.1.

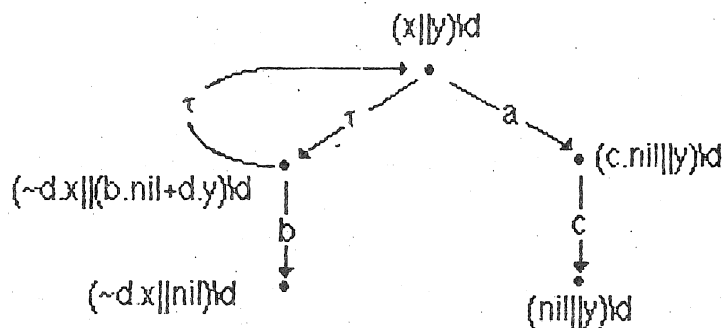
Para todo par de términos t_1, t_2 de T_T

$t_1 \approx t_2$ si y solamente si $EO(S_{t_1}) \sim EO(S_{t_2})$.

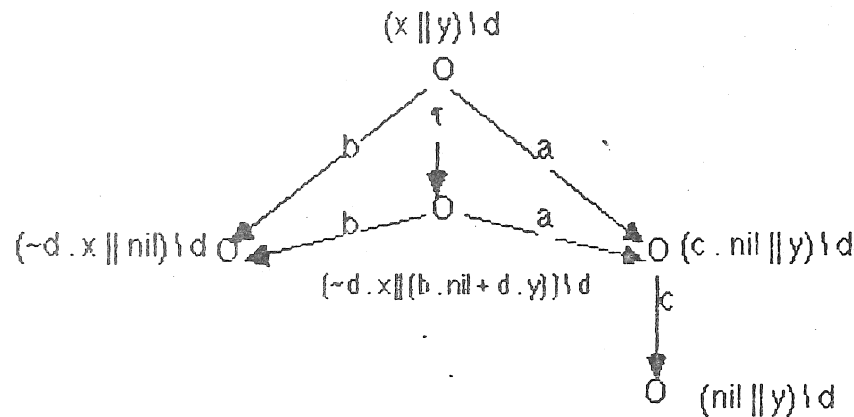
II.2.2.- Transformación EO .

De manera similar, se define una transformación (transformación EO) sobre los sistemas de transiciones que permite decidir la congruencia observacional por simulación de los sistemas de transiciones obtenidos por aplicación de la transformación EO .

Por ejemplo, el sistema de transiciones:



asociado al término $u = ((x||y)Id, \{x=d.\sim d.x+a.c.nil, y=\sim d.(b.nil+d.y)\})$ por aplicación de la transformación EO , se transforma en:



Definición II. 7.

Para todo sistema de transiciones $S=(Q, \cup_{\alpha \in P_{\tau}} R_{\alpha}, q_0)$, la transformación $\mathcal{A}$ procede en tres etapas:

- 1.- Construcción del sistema de transiciones $S'=(Q', \cup_{\alpha \in P_{\tau}} R'_{\alpha}, q'_0)$ por aplicación de las transformaciones τ -cadenas y τ -circuitos sobre el sistema S .
- 2.- Si durante la construcción del sistema S' , se elimina alguna τ -transición que parte del estado inicial q_0 , se agrega un nuevo estado inicial $q \in Q'$, y una transición $q \xrightarrow{\tau} q'_0$ para obtener el sistema de transiciones S'' .
- 3.- Transformación de S'' en un sistema S''' tal que $\forall \alpha \in P_{\tau} q \xrightarrow{\alpha} q'$ es una transición de S''' si y solamente si $q \xrightarrow{\alpha} q'$ es una derivación de S'' . Cabe indicar que la relación $\xrightarrow{\tau}$ no se hace reflexiva como en el caso de la equivalencia observacional.

Proposición II. 2.

La transformación $\mathcal{A}$ preserva la congruencia observacional.

Prueba.

Por la proposición II. 3 y por la definición de la transformación $\mathcal{A}$, se obtiene:

$$S_{t1} \approx S_{t2} \text{ si y solamente si } \mathcal{A}(S_{t1}) \approx \mathcal{A}(S_{t2})$$

es decir $\mathcal{A}$ preserva la equivalencia observacional.

Sea $S_{ti} = (Q_{ti}, \cup_{\alpha \in P_{\tau}} R_{\alpha, ti}, q_{i0})$ para $i = 1, 2$

$$\mathcal{A}(S_{ti}) = (Q'_{ti}, \cup_{\alpha \in P_{\tau}} R'_{\alpha, ti}, q'_{i0}) \text{ para } i = 1, 2$$

Si en S_{ti} hay una τ -transición $q_{i0} \xrightarrow{\tau} q_{ti}$ que forma parte de un circuito o de una cadena de τ , es decir que es eliminada en el paso 1 de la transformación $\mathcal{A}$ se agrega una transición $q'_{i0} \xrightarrow{\tau} q'_{ti}$ en el paso 2, donde $q'_{ti} \in Q'$ es el estado inicial del sistema después de la transformación $\mathcal{A}$. Así, por

construcción de $\mathcal{CO}(S_{ti})$ para $i=1,2$ se tiene que:

$$(1) \quad q_{i0} \xrightarrow{\tau} q_{ti} \in R_{\tau ti} \text{ implica } \exists q'_{ti} \in Q'_{ti} \quad q'_{i0} \xrightarrow{\tau} q'_{ti} \in R'_{\tau ti} \text{ y } q'_{ti} \approx q_{ti}$$

$$q'_{i0} \xrightarrow{\tau} q'_{ti} \in R'_{\tau ti} \text{ implica } \exists q_{ti} \in Q_{ti} \quad q_{i0} \xrightarrow{\tau} q_{ti} \in R_{\tau ti} \text{ y } q'_{ti} \approx q_{ti}$$

por (1) y la proposición I.4. se obtiene que $S_{ti} \approx^C \mathcal{CO}(S_{ti})$,

asi, $S_{t1} \approx^C S_{t2}$ si y solamente si $\mathcal{CO}(S_{t1}) \approx^C \mathcal{CO}(S_{t2})$. ♦

Para decidir la congruencia observacional, no es suficiente verificar si los sistemas $\mathcal{CO}(S_{ti})$ obtenidos a partir de S_{ti} se bisimulan; en efecto, la relación de transición debe ser reflexiva en algunos casos. Por ejemplo, para decidir la congruencia observacional de los términos $b.a.nil$ y $b.(a.a.nil + a.nil)$ por bisimulación, es necesario considerar la relación $\xrightarrow{\tau}$ reflexiva. Pero, es fácil ver que si se considera la relación $\xrightarrow{\tau}$ reflexiva, no es posible distinguir por bisimulación los términos $a.nil$ y $\tau.a.nil$; de esta manera, ella no debe ser considerada como reflexiva para el estado inicial. De igual modo, si suponemos la relación $\xrightarrow{\tau}$ reflexiva para todos los estados excepto para el estado inicial, no es posible de verificar por bisimulación que los términos $(a.b.x, x=a.b.x)$ y $(x, x=a.b.x)$ son observacionalmente congruentes.

Por esta razón, introducimos la noción de *r-bisimulación* entre sistemas de transiciones. Esta noción es una variante de la noción de bisimulación; ella se diferencia únicamente por el hecho de que se considera reflexiva la relación $\xrightarrow{\tau}$ de manera asimétrica:

- para el estado inicial q_0 no se agrega jamás un bucle $q_0 \xrightarrow{\tau} q_0$,
- en cada etapa, para la verificación de la condición (i) de la bisimulación, se considera reflexiva la relación $\xrightarrow{\tau}$ únicamente para el segundo sistema de transiciones excepto para el estado inicial e inversamente para la verificación de la condición (ii).

Definición II.8.

Para $S_i = (Q_i, \cup_{\alpha \in P_{\tau}} R_{\alpha}, q_{i0})$, $i=1,2$ se dice que S_1 et S_2 *r-bisimulan* (escrito como $S_1 \sim^r S_2$) si y solamente si el mayor punto fijo $R \subseteq Q_1 \times Q_2$ de la funcional F_r contiene el par (q_{10}, q_{20}) .

La funcional F_r se define como:

$$F_r(R) = \{(p, q) \mid p R q \text{ y}$$

$$\text{y } \forall \alpha \neq \tau \text{ (si } p \xrightarrow{\alpha} p' \text{ entonces } \exists q' \in Q_2 (q \xrightarrow{\alpha} q' \text{ y } p' R q'))$$

$$\text{y si } q \xrightarrow{\alpha} q' \text{ entonces } \exists p' \in Q_1 (p \xrightarrow{\alpha} p' \text{ y } p' R q'))$$

$$\text{y si } p \xrightarrow{\tau} p' \text{ entonces } ((p = q_{10} \text{ y } (p', q) \in R) \text{ o}$$

$$\exists q' \in Q_2 (q = \tau \Rightarrow q' \text{ y } p' R q'))$$

$$\text{y si } q \xrightarrow{\tau} q' \text{ entonces } ((q = q_{20} \text{ y } (p, q') \in R) \text{ o}$$

$$\exists p' \in Q_1 (p = \tau \Rightarrow p' \text{ y } p' R q'))\}.$$

Proposición II.4.

Para todo término t_1, t_2 de T_r

$t_1 \approx^c t_2$ si y solamente si $\alpha(S_{t_1}) \sim \alpha(S_{t_2})$. ♦

CONCLUSION

El objetivo de este trabajo fué el de definir métodos de verificación de sistemas comunicantes descritos en CCS.

Se realizó un estudio del cálculo CCS sin transmisión de valor. Para los términos regulares, se definieron procedimientos de decisión para la congruencia fuerte, la equivalencia observacional y la congruencia observacional. Estos procedimientos de decisión se basan en transformaciones y comparaciones de sistemas de transiciones representando los comportamientos descritos por los términos.

Estos resultados pueden ser aplicados sin muchas variaciones a otros cálculos, como por ejemplo a ACP [BK 84].

REFERENCIAS

- [Ab 79] Abrahamson K.
Modal Logic of concurrent non deterministic programs.
Semantics of Concurrent Computation Proceedings.
Lecture Notes in Computer Science 70. Springer-Verlag.
1979.
- [AB 84] Austy D., Boudol G.
Algèbre de processus et synchronisation.
TCS 30 pp. 91-131.
- [AS 79] Abrial J. R., Schuman S. A.
Non deterministic system verification.
Lecture Notes in Computer Science 70. Springer-Verlag.
1979.
- [BH 84] Brookes S. D., Hoare C. A. R., Roscoe A. W.
Theory of communicating sequential processes.
JACM. 31 (3). Juillet 1984.
- [BK 84] Bergstra J. A., Klop J. W.
Verification of an alternating bit protocol by means of process algebra.
Centre for Mathematics and Computers.
Departement of Computer Science.
Rapport CS-R8404. Mars 1984. Amsterdam.
- [BK 85] Bergstra J. A., Klop J. W.
A complete inference system for regular processes with silent moves.
Centre for Mathematics and Computers.

- Departement of Computer Science.
Rapport CS-R8420. Mars 1984. Amsterdam.
- [HM 85] Hennessy M., Milner R.
Algebraic laws for nondeterminism and concurrency.
JACM. 32(1). pp. 137-161. Janvier 1985.
- [Ko 85] Koomen C.J.
Algebraic specification and verification of communication protocols.
Science of Computer Programming 5. pp 1-36. 1985.
- [Mi 80] Milner R.
A calculus of communicating systems.
Lecture Notes in Computer Science 92.
Springer-Verlag. 1980.
- [Mi 83] Milner R.
Calculi for synchrony and asynchrony.
T.C.S. 25; pp. 267-310. 1983.
- [Mi 85] Milner R.
A complete axiomatisation for observational congruence of finite state behaviors.
Manuscript non publié, décembre 1985.
- [Pl 81] Plotkin G.
A structural approach to operational semantics.
Aarhus University. Denmark.
DAIMI FN-19. Septembre 1981.
- [Pn 77] Pnueli A.
The temporal logic of concurrent programs.
19th. FOCS. 1977.
- [So 87] Soriano A.
VENUS: UN OUTIL D'AIDE A LA VERIFICATION DES SYSTEMES COMMUNICANTES.
Tesis de doctorado. INPG. Francia. 1987.
- [SY 85] Soriano A. y Voiron J.
CONCEPCION ET MISE EN OEUVRE D'UN SYSTEME DE PREUVE POUR UN SOUS ENSEMBLE DE CCS SANS TRANSMISSION DE VALEURS.
Panel '85. EXPODATA.
V Congresso da Sociedade Brasileira de Computacao.
XI Conferencia Latino Americana de Informatica. Brasil. 1985.