ESPECIFICACION DEL COMPORTAMIENTO OBSERVABLE DE SISTEMAS SOFTWARE CONCURRENTES

por

Gonzalo León Serrano

Fernando Sáez Vacas

Laboratorio de Ordenadores, Ciber
nética y Teoría de Sistemas
E.T.S.I.Telecomunicación. Madrid.

RESUMEN

Se presenta en este trabajo un modelo de sistema y proceso concurrente junto con una herramienta de especificación del comportamiento dinámico del mismo. La herramienta, denominada expresiones de coordinación permite relacionar los eventos observables de un proceso mediante unos operadores basados en una semántica de red.

Un sistema concurrente se maneja algebráicamente mediante un conjunto de operaciones que permiten relacionar expresiones de coordinación y analizar el comportamiento del sistema.

1. INTRODUCCIÓN

El desarrollo de métodos de especificación formal de sistemas software y de los modelos que los forman, ha sido reconocido como una necesidad básica en la ingeniería del software (|FRANTA et al.,1980|)

En la especificación de sistemas software secuenciales, tanto las especificaciones axiomáticas, como las procedentes de abstracciones (ya sean datos o procedimientos) |LISKOV y BERZINS, 1979| parecen aportar resultados satisfactorios. El problema de la especificación de sistemas software concurrentes es, sin embargo, mucho más complejo.

La interacción entre los diferentes componentes (módulos, recursos, procesos, etc.) y los problemas derivados de su evolución dinámica invalidan las técnicas de especificación de sistemas secuenciales.

En un intento de superación de estos problemas podemos citar dos recientes enfoques:

- el desarrollo de una herramienta de especificación derivada de las redes de Petri y de las expresiones de camino denominada COSY (ver |LAUER et al., 1981|).
- la utilización de un lenguaje de descripción tipo-CSP (|HOARE, 1978|) y un modelo de verificación basado en una lógica temporal como CESAR (ver |QUEILLE y SIFAKIS, 1981|).

Todos estos enfoques,sin embargo, adolecen de la falta de un modelo previo (formalizado) de sistema concurrente a partir del cual derivar una técnica de especificación.

Otros autores, han intentado, dejando en un segundo plano el desarrollo de una herramienta software concreta, formalizar el concepto de proceso derivando una herramien

ta notacional. El trabajo más importante, a nuestro juicio, desarrollado en este sentido es el denominado CCS (ver |MILNE y MILNER, 1979|).

Estos autores parten de la concepción de un proceso como un conjunto de potencialidades de comunicación observables exteriormente; a partir de esta idea se define algebráicamente un conjunto básico de operaciones que permiten especificar sistemas complejos a partir de subsistemas más simples.

La limitación de su trabajo reside en la imposibilidad de tratar problemas dinámicos (como bloqueos o inaniciones) sobre la estructura del sistema construído. Su concepto de concurrencia es, asimismo, virtual (imbricación) y no real.

2. MODELO BASICO DE SISTEMA CONCURRENTE.

El trabajo desarrollado |LEON, 1982| ha tomado como base el enfoque de MILNE y MILNER incorporando conceptos derivados de la teoría de la concurrencia desarrollada en Bonn (GMD-ISF) por el grupo de trabajo dirigido por C.A. PETRI.

El modelo del sistema concurrente propuesto considera a un proceso como el elemento básico, y junto a un conjunto de enlaces que definen la interacción entre los procesos, el sistema es definido como una red de procesos.

Un proceso es definido como un conjunto de potenciales intercambios de información observables por otros procesos.

Por otro lado, y para dotar a nuestro modelo de los aspectos dinámicos necesarios para tratar el comportamiento de los procesos se le ha dotado de una semántica de red derivada de los sistemas Condición-Evento (C-E) |GENRICH et al., 1979|.

De acuerdo con estas consideraciones generales, las hipótesis básicas del modelo de proceso son:

a) Hipótesis de independencia temporal.

   No consideraremos el factor tiempo en el modelo excepto la existencia de un tiempo finito entre sucesivas comunicaciones observables.

b) Hipótesis de independencia del comportamiento local.

   Queremos indicar con ello la autonomía parcial de los procesos (consecuencia de su rol definido en el sistema) respecto al comportamiento global del sistema.

c) Hipótesis de sincronización de comunicaciones.

   La transmisión ó intercambio de información entre dos procesos participantes se efectúa de forma "sincronizada"; es decir, un proceso desea enviar una información y el otro recibirla.

   Los enlaces o canales de comunicación entre procesos son biunívocos; no hay, por tanto "difusión" de la información.

d) Hipótesis de infinitud

   Se refiere a la consideración cíclica indefinida de la vida de un proceso. Debido a esta hipótesis el conjunto de potenciales comunicaciones observables de un proceso es fijo.

e) Hipótesis de no-determinismo.

   Consideramos la existencia de situaciones no deterministas en el modelo de compostamiento de un proceso concurrente.

f) Hipótesis de abstracción organizativa.

   Pueden existir diversas organizaciones y/o comportamientos internos que presenten el mismo comportamiento externo. Esta situación obliga a considerar el modelo de proceso como el representante de una clase de proceso abstracta.

g) Hipótesis de abstracción interpretativa.

   Indica la necesidad de manejar en cada momento la información imprescindible a las conclusiones buscadas lo que obliga a modelar un proceso en diversos niveles de abstracción:

   - Nivel de proceso neutral: ¿Qué potencialidades de comunicación existen y cual es la relación entre ellas?.
   - Nivel de proceso controlado:

Incorporación de identificadores semánticos y clasificación de las puertas de comunicación en entrada y salida. Se modela, por tanto, el sentido del flujo de información.

Nivel de proceso valuado: Modela los valores intercambiados y las transformaciones sufridas por estos en el proceso, asociando expresiones (funciones de los valores de entrada) a las puertas de salida.

3. ESTRUCTURA JERARQUICA DE LA ESPECIFICACION.

3.1. Objetivos

La consideración de un sistema concurrente como un conjunto de procesos concurrentes (procesos en los cuales pueden existir comunicaciones observables independientemente) interconectados mediante un conjunto de enlaces (o canales) formando una red de procesos, nos sugiere la siguiente estructura de la especificación:

- una fase de especificación independiente de cada uno de los procesos concurrentes que van a formar parte del sistema.
- una fase de especificación del sistema concurrente a partir de los procesos especificados previamente.

La importancia de estas dos fases (y dentro de cada una de ellas los tres niveles descritos en la hipótesis de abstracción interpretativa) radica en disponer de un conjunto de herramientas de especificación jerarquizadas simplificando así la estructura global de la especificación.

3.2. Especificación de procesos concurrentes.

La especificación de procesos concurrentes se desarrolla utilizando una herramienta que hemos denominado: expresiones de coordinación.

Una expresión de coordinación es una herramienta notacional derivada de las expresiones de flujo [RIDDLE, et al., 1979] a las que se ha dotado de un conjunto de operadores que incrementan su potencia expresiva.

Desde un punto de vista formal, las expresiones de coordinación están basadas en una semántica de red derivada de los sistemas C-E [GENRICH et al., 1979].

Para comprender la interpretación asociada a las condiciones y eventos de un sistema C-E se han definido tres estados de una puerta de comunicación:

a) estado de reposo: No se desea efectuar ninguna transferencia de información.

b) estado cargado: La puerta está 'permitida localmente' (por el proceso al cual pertenece) a entablar comunicación.

c) estado activo: La comunicación se realiza entre las dos puertas en estado cargado.

De acuerdo con estos estados, las condiciones del sistema C-E representan el estado cargado de una puerta (el estado de reposo no es, digamos, observado exteriormente) mientras que los eventos representan los estados de actividad de la puerta.

Con esta interpretación, los operadores fundamentales de las expresiones de coordinación se corresponden con las siguientes redes C-E, siendo a_1 y a_2 potencialidades de comunicación observables y S^1 y S^2 subexpresiones de coordinación.

λ es la potencialidad de comunicación representante de todas las comunicaciones no-observables, (igualmente etiquetadas), pero que son necesarias para que de un sistema C-E se puedan extraer todos los comportamientos elementales asociados a los operadores de las expresiones de coordinación.

a) Operador secuencial (;) (a1;a2)

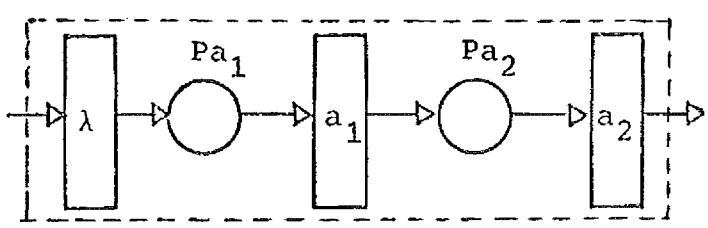

FIGURA 1

La potencialidad de comunicación a_1 pasa al estado activo y, seguidamente se permite (estado cargado correspondiente a la condición Pa_2) la comunicación a_2.

b) Operador concurrente (||)
(a1||a2)

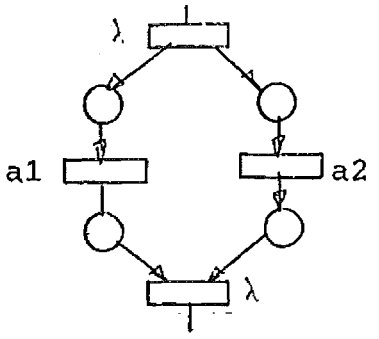

FIGURA 2

Las potencialidades de comunicación a_1 y a_2 son cargadas simultaneamente ya que esto puede hacerse localmente al proceso. Sin embargo, no tienen por qué realizarse simultáneamente ya que esto depende (debido a la hipótesis de comunicación sincronizada) de los procesos con los cuales intercambian información.

c) Operador no determinista (□)
(a1□a2)

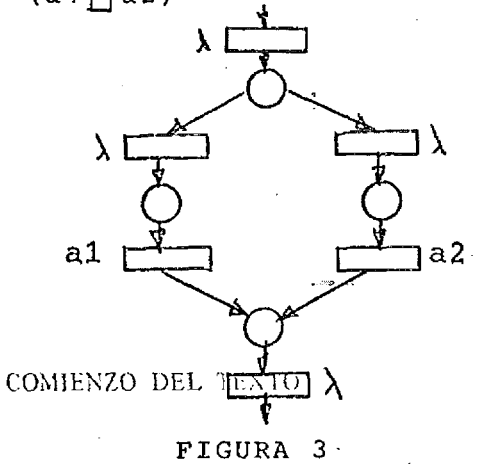

FIGURA 3

Sólo una de las potencialidades de comunicación se va a realizar. Esta situación expresa la idea de que con la información asociada al proceso no se puede determinar cual de ellas se va a realizar.

d) Operador cíclico (∞) $(S1)^{\infty}$

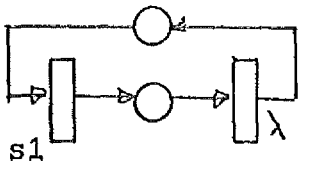

FIGURA 4

Obsérvese como, al representar los comportamientos elementales como una red C-E comenzando y finalizando por un evento, podemos sustituir una subexpresión de coordinación por un evento.

De acuerdo con estos comportamientos elementales el comportamiento dinámico de un proceso queda definido mediante una expresión de coordinación en la forma:

$$S_p = \delta_{\Sigma_p}(a1,\ldots,an,\lambda) \text{ con}$$

$$\Sigma_p = \{;,\ ||,\ \square,\ \infty\}$$

AUTORES

3.3. Especificación de sistemas concurrentes

La segunda fase de la especificación se refiere a expresar formalmente la interacción entre los procesos constituyentes. La imposibilidad de considerar globalmente (al menos de una forma general) un sistema concurrente obliga a disponer de un conjunto de operaciones que, no solo construyan un sistema a partir de procesos y enlaces entre ellos, sino que permitan disponer de visiones parciales del sistema.

a) Composición de procesos.

Considerada como operación binaria sobre las expresiones de coordinación de dos procesos:

$$S_p = S_{p1} \circ S_{p2} \mid \{enlaces\}$$

permite enlazar mediante un conjunto de enlaces las potencialidades de comunicación de dos procesos.

La semántica de red asociada a la operación de composición está basada en la compartición de eventos. Las potencialidades de comunicación pertenecientes al enlace se hacen coincidir en el tiempo y se asocian a un único evento (figura 5).

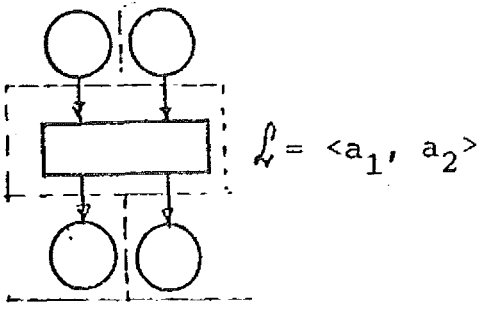

FIGURA 5

b) Descomposición de procesos

La operación de descomposición de procesos permite obtener una red de procesos cuyo comportamiento equivalente sea el del proceso original.

Esta operación nos permite utili-

zar procesos ya diseñados (cuyas expresiones de coordinación se conocen) como elementos en el diseño de procesos con comportamiento más complejo.

La operación de descomposición pone de manifiesto enlaces entre los procesos resultantes que podíamos considerar ocultos en el proceso original. En la figura 6 podemos ver el proceso original y la red resultante de la descomposición

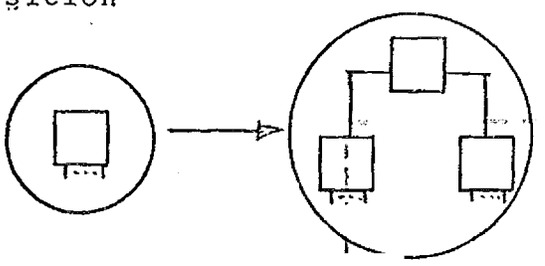

FIGURA 6

donde la sintaxis elegida es

$$S'_p = S_p \# (S1\ op) =$$

$$= S1 \circ S2 \circ SR \Big|_{\{\ell_{1r}, \ell_{2r}\}}$$

La descomposición puede ser de tres tipos:

1. Descomposición secuencial.
2. Descomposición concurrente.
3. Descomposición no determinística, dependiendo del operador elegido.

c) Reetiquetado de procesos.

Esta operación permite modificar la interpretación semántica asociada a las puertas de un proceso (a cualquier nivel de descripción del mismo) así como ocultar un conjunto de potencialidades de comunicación.

En el primer caso, el cambio en una expresión de coordinación de un subconjunto de potencialidades de comunicación por otro, o de las expresiones asociadas a unas puertas por otras, nos permite derivar de un mismo proceso abstracto diferentes "implementaciones".

En el segundo caso, la sustitución de una potencialidad de comunicación por un λ-evento supone ocultar (hacer no observable) esa comunicación.

Así: $S_p\ [a_i/b_i,\ a_j/\lambda]$

supone la sustitución de a_i por b_i y a_j por λ.

El conjunto de todas estas operaciones nos permiten realizar transformaciones algebráicas de los comportamientos de los procesos. No todas las operaciones de composición dan origen a una expresión de coordinación.

(1) FRANTA, W.R., BOEBERT, W.E. y BERG, H.K. "An approach to the specification of distributed software" en The use of formal specification of software. Informatik-Fachberichte nº 36. Springer-Verlag. Berlin 1980, pp. 197-236.

(2) GENRICH, H.J., LAUTENBACH, K. y THIAGARAJAN, P.S. "An overview of net theory". An advanced course on General net theory of processes and systems. Hamburg. Octubre 1979.

(3) HOARE, C.A.R. "Communicating sequential Processes". Com. ACM. 21,8 Ag.1978,pp.623-637.

(4) LAUER,P.E., SHIELDS,M.W. y COTRONIS,Y.Y. "Formal behavioural specification of concurrent systems without globality assumptions. Formalization of programming concepts. LNCS nº 107. Springer-Verlag. Berlin 1981. pp. 115-151.

(5) LEON,G. "Contribución a la modelación y especificación del comportamiento observable de sistemas concurrentes". Tesis Doctoral. ETSIT.Madrid, 1982.

(6) LISKOV,B. y BERZINS,J. "An appraisal of program specifications". Research Directions in software technology. (Peter Wegner ED.) MIT Press, 1979, pp. 276-301.

(7) MILNE,G. y MILNER,R. "Concurrent Processes and their syntax" J.ACM. 26,2 Abril, 1979, pp. 302-321.

(8) QUEILLE,J.P. y SIFAKIS, J. "Specification and verification of concurrent systems in CESAR. "Second European Workshop on Petri Nets and related Topics. Bad Honeff (Alemania) Sept. 1981, pp. 483-517.