Especificação e verificação em CCS de sistemas de comunicação (*)

Wanderley Lopes de Souza
Bernardo Gonçalves Riso (**)
Adalberto F. M. Filho

GRC/DSC/CCT/Universidade Federal da Paraíba
Av. Aprígio Veloso, 882
58.100 – Campina Grande (Pb)

Sumário

Neste trabalho é explorada a utilização de "Calculus of Communicating Systems (CCS)" para a especificação formal de sistemas de comunicação e para a verificação da consistência entre especificações, de um mesmo sistema, realizadas em diferentes níveis de abstração. A atividade de validação, aqui empregada, utiliza o conceito de equivalência de observação, que é formalmente definido na própria álgebra CCS.

1. Introdução

Durante o ciclo de desenvolvimento de um sistema de comunicação, as especificações formais, além de facilitar a própria construção do sistema, devem ser referências confiáveis para as atividades de validação e implementação. Para que esse objetivo possa ser atingido, é necessário que a técnica de descrição formal (TDF) utilizada, seja: abstrata, expressiva e analítica [LoSt 88].

O termo validação refere-se a qualquer atividade, que vise aumentar o grau de confiabilidade da entidade (especificação, design ou implementação) que está sendo analisada. No caso da especificação final dessa entidade ser atingida através de refinamentos sucessivos, a validação do design procurará detectar, a cada passo, inconsistências entre a nova especificação e a sua precedente (mais abstrata).

(*) realizado com auxílio fornecido pelo CNPq
(**) lotado no CEC/CTC/Universidade Federal de Santa Catarina

As atividades de validação seguem, normalmente, uma das seguintes filosofias: verificação ou teste.

O teste, frequentemente aplicado a implementações, procura provar a conformidade de uma entidade em relação a sua especificação, através da execução controlada dessa entidade e através da observação de seu comportamento. Para que essa filosofia possa ser empregada em especificações e designs, é necessário prever algum tipo de execução dessas entidades [JaBo 83].

A verificação utiliza algum tipo de raciocínio lógico, para analisar se uma entidade possui ou não determinadas propriedades que lhe são requeridas. A verificação de especificações e designs, em CCS, utiliza o mesmo princípio de observação de comportamento, sendo que a diferença, em relação ao teste, é que esse princípio é expresso algebricamente e as provas, que asseguram a equivalência de observação de comportamento entre entidades, são realizadas matematicamente.

2. CCS: uma álgebra para a especificação de sistemas comunicantes

As metodologias utilizadas para a descrição dos sistemas computacionais procuram:

(a) determinar um modelo que se comporta como o sistema, obtendo-se uma representação, com um certo nível de detalhamento, do próprio sistema, ou

(b) descrever o comportamento do sistema, visto por um observador externo, o que permite a sua abstração completa (uma verdadeira caixa preta).

Os autômatos se enquadram na primeira categoria, enquanto que CCS, apresentado em [Miln 80], pertence à segunda categoria. Para uma melhor compreensão do conceito de observabilidade e das diferenças entre esses dois modelos, sugere-se, ao leitor interessado, que consulte [Lope 87].

Em CCS um sistema é representado através de um agente (processo) ou através da composição de agentes. A comunicação entre um agente e o seu ambiente (ou entre dois agentes) é síncrona. Isto é, só ocorrerá quando, simultaneamente, um agente oferecer (ou aceitar) um evento e o seu ambiente (ou outro agente) aceitar (ou oferecer) esse mesmo evento. Nessa comunicação poderá ocorrer (ou não) passagem de valores.

Num sistema composto, uma comunicação entre dois de seus agentes é

uma **ação atômica** (indivisível) de todo o sistema, sendo que o observador é capaz de "observar" uma única ação atômica por vez. Se num determinado instante mais de uma ação atômica é possível, uma escolha não-determinística é realizada. Portanto, essa álgebra não é capaz de expressar uma concorrência no sentido mais amplo do termo.

Uma especificação em CCS é na realidade uma descrição dos eventos de um sistema passíveis de ocorrer. Esse sistema representa um termo da álgebra sujeito a manipulações, que podem transformá-lo em outro termo com outra estrutura ("intension") mas com idêntico comportamento ("extension").

2.1. Sintaxe de CCS (Anexo 1)

Os termos da álgebra CCS são expressões de comportamento, que utilizam rótulos ("labels") para representar as portas dos agentes onde ocorrem os eventos. Esses rótulos são assim definidos:

- $\Lambda = \Delta \cup \bar{\Delta}$ é o conjunto de rótulos visíveis ao observador, sendo que $\Delta = \{\alpha,\beta,\ldots\}$ representa as portas que podem aceitar eventos e o conjunto de co-rótulos $\bar{\Delta} = \{\bar{\alpha},\bar{\beta},\ldots\}$ representa as portas que podem oferecer eventos. As comunicações entre os agentes de um sistema, são indicadas pelo rótulo τ
- os rótulos podem estar vinculados a conjuntos ("tuples")de variáveis $(x_1,\ldots,x_n)$, enquanto que os co-rótulos podem estar vinculados a conjuntos de expressões de valor $(E_1,\ldots,E_n)$. Numa comunicação, para que haja passagem de valores, é necessário que os tipos de variáveis e das expressões de valor envolvidos sejam compatíveis. Entretanto, é omitida, em CCS, uma definição formal desses tipos.

A cada expressão de comportamento B é associada uma espécie ("sort") L(B), que é um subconjunto de rótulos$\subseteq\Lambda$. É associado também um conjunto de variáveis livres FV(B), que são variáveis às quais não foram ainda atribuídos valores. $B\{E_1/x_1,\ldots,E_n/x_n\}$, abreviadamente $B\{\bar{E}/\bar{x}\}$, é o resultado da substituição de todas as ocorrências livres das variáveis $x_i (1\leq i\leq n)$, em B, pelas suas respectivas expressões de valor E_i.

As operações CCS, que permitem as manipulações com as expressões de comportamento, podem ser classificadas em:

(a) dinâmicas, que descrevem os comportamentos dos agentes de uma forma não determinística. São também chamadas de operações básicas, já que qualquer agente CCS pode ser reduzido a uma expres-

são de comportamento constituída somente dessas operações

- nula (NIL): expressa uma "não ação"
- soma (+): indica uma escolha não determinística
- ação ($\alpha\tilde{x}$, $\bar{\alpha}\tilde{E}$ ou τ).

(b) estáticas, que fixam uma estrutura de ligação entre os comportamentos dos agentes de um sistema

- composição (|): combina agentes, sendo que pode ocorrer comunicação entre eles
- restrição ($\backslash\alpha$): esconde portas do observador. A combinação de | com $\backslash\alpha$ permite restringir os eventos, que podem ocorrer em α, às comunicações τ (que passam a ser ações internas)
- rerotulação ([S]): permite a troca dos nomes dos rótulos. Essa troca é definida pela operação S (e.g., $S=\alpha\beta/\gamma\delta$ significa trocar γ por α e δ por β)
- identificador (b[$\tilde{E}$]): permite a parametrização das expressões de comportamento
- condição (if E then B else B'): indica uma escolha a ser realizada em função do valor assumido pela expressão booleana E.

A precedência entre os operadores CCS é:

restrição e rerotulação > ação > composição > soma.

2.2. Semântica de CCS (Anexo 2)

A semântica de CCS é definida através de um conjunto de regras de inferência, obtidas a partir de ações atômicas $\xrightarrow{\mu v}$, que por sua vez são definidas, por indução, na estrutura das expressões de comportamento. Portanto, todas as ações atômicas, de uma expressão de comportamento composta, podem ser inferidas a partir das ações atômicas de seus componentes.

$B \xrightarrow{\mu v} B'$: B através de $\xrightarrow{\mu v}$ pode transformar-se em B', onde $\mu \in A \cup \{\tau\}$ e v é um valor de tipo apropriado a μ. Para o caso particular de $\xrightarrow{\tau}$, o valor v de tipo apropriado a τ é $\emptyset$ ("0-tuple").

Por exemplo, a partir de $B_1 \xrightarrow{\mu v} B_1'$ infere-se que $(B_1+B_2) \xrightarrow{\mu v} B_1'$ e a partir de $B_2 \xrightarrow{\mu v} B_2'$ infere-se que $(B_1+B_2) \xrightarrow{\mu v} B_2'$. Portanto, para cada operação CCS, que possibilita a obtenção de uma expressão de comportamento, é necessá-

rio uma (ou um conjunto de) regra(s) de inferência.

2.3. Equivalência de observação de comportamento ($\approx$)

A definição formal de $\approx$ é feita através de uma sequência decrescente de relações de equivalência. Sejam B,B', C e C' expressões de comportamento e $B \stackrel{s}{\Rightarrow} B'$ a forma abreviada de $B \xrightarrow{\tau^{m_0}.\mu_1 v_1.\tau^{m_1}\ldots\mu_k v_k.\tau^{m_k}} B'$ para $k,m_1,\ldots,m_k \geq 0$. Então:

$B \approx_0 C$ é sempre verdadeiro

$B \approx_{k+1} C$ se para todo $s \in (\Lambda x V)^*$

(i) se $B \stackrel{s}{\Rightarrow} B'$ então $\exists\ C' \mid C \stackrel{s}{\Rightarrow} C'$ e $B' \approx_k C'$ e

(ii) se $C \stackrel{s}{\Rightarrow} C'$ então $\exists\ B' \mid B \stackrel{s}{\Rightarrow} B'$ e $B' \approx_k C'$

$B \approx C$ se para $\forall\ k \geq 0$, $B \approx_k C$

obs: $\Lambda x V$ representa o produto cartesiano do conjunto de rótulos Λ pelo conjunto de valores V; * representa uma potência inteira.

Em [Miln 80] alguns capítulos são dedicados ao estabelecimento e prova das propriedades relativas à equivalência de observação. Para se chegar a esse conjunto de propriedades, algumas relações, "mais fortes" (menos abrangentes) que $\approx$, foram definidas: equivalência direta ($\equiv$), equivalência forte ($\sim$) e congruência ($\approx^c$).

Uma vez que $\approx$ é uma relação mais abrangente que $\equiv$, $\sim$ e $\approx^c$, as propriedades válidas para essas três últimas relações são também válidas para a primeira. Na próxima seção desse artigo, as seguintes propriedades serão utilizadas:

(2.1.) Teorema da expansão (te). Seja a expressão de comportamento $B = (B_1 | \ldots | B_m) \backslash A$, onde cada B_i é uma somatória de guardas $g(\alpha\tilde{x}, \bar{\alpha}\tilde{E}$ ou $\tau)$ e A um conjunto de nomes de rótulos (e co-rótulos). Então:

$B \sim \sum\{g.((B_1|\ldots|B_i'|\ldots|B_m)\backslash A);\ g.B_i' \text{ é um termo da somatória de } B_i \text{ e } name(g) \notin A\}$

$+ \sum\{\tau.((B_1|\ldots|B_i'\{\tilde{E}/\tilde{x}\}|\ldots|B_j'|\ldots|B_m)\backslash A);\ \alpha\tilde{x}.B_i' \text{ é um termo da somatória de } B_i,\ \bar{\alpha}\tilde{E}.B_j' \text{ é um termo da somatória de } B_j \text{ e } i \neq j\}$

obs: aplicando-se sucessivamente o te é possível transformar qualquer expressão de comportamento num conjunto de ações e somas

(2.2.) $B \simeq \tau.B$ (absorção de τ)

(2.3.) $B+\tau.B \simeq^C \tau.B$ (absorção de B)

(2.4.) se $B \simeq C$ então $g.B \simeq^C g.C$

Para uma melhor compreensão dessas relações e de toda a álgebra CCS, recomenda-se uma leitura aprofundada de [Miln 80].

3. Definição de um sistema de comunicação em CCS

Nesta seção é exemplificada a utilização de CCS, através das especificações de um serviço de comunicação e de seu refinamento. A conformidade entre essas duas especificações é verificada através da relação de equivalência de observação.

Seja S um sistema composto por três agentes: produtor de dados (P), serviço de comunicação de dados (SC) e consumidor de dados (C) (Fig. 3.1).

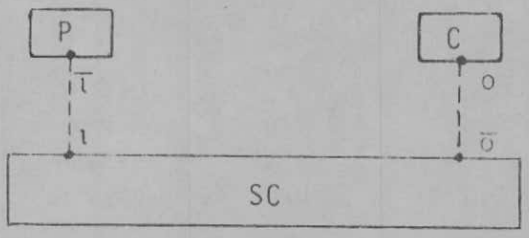

Fig. 3.1 - Sistema produtor-consumidor

O SC é confiável, de modo que os dados produzidos por P são entregues íntegros a C e na sequência correta. SC pode ser especificado em CCS através de um identificador de comportamento (SC), cuja expressão de comportamento é

$$SC \Leftarrow i.d.\bar{o}.d.SC \qquad (3.1)$$

onde i e $\bar{o}$ representam, respectivamente, as portas de entrada e saída e d representa uma variável de tipo apropriado ao dado que será transmitido do produtor para o consumidor.

Para oferecer SC, pode-se especificar um protocolo que utiliza o bit alternante. Como existem várias versões desse protocolo, será utilizada a versão apresentada em [Boch 78]. Nessa versão, três módulos são especificados através de máquinas de estados finitas (MEF): o emissor (E), o receptor (R) e o meio de comunicação (M) (Fig. 3.2).

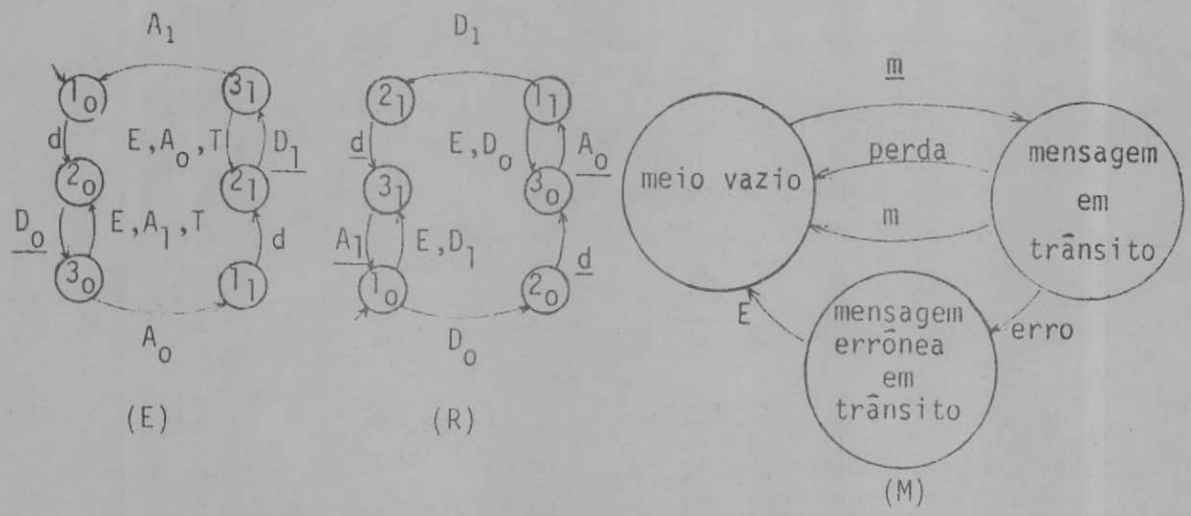

Fig. 3.2 - MEFs relativas aos módulos E, R e M

Em relação ao meio M são consideradas as possibilidades de perda e corrupção de mensagens (dados e confirmação), mas não é levado em conta o atraso de transmissão. Além disso, num determinado instante, somente uma mensagem pode estar transitando em M.

Esse mesmo protocolo pode ser descrito, em CCS, considerando-se os mesmos módulos, agora tratados como agentes, especificados através dos identificadores de comportamento $E(b_e)$, $R(b_r)$ e M (Fig. 3.3).

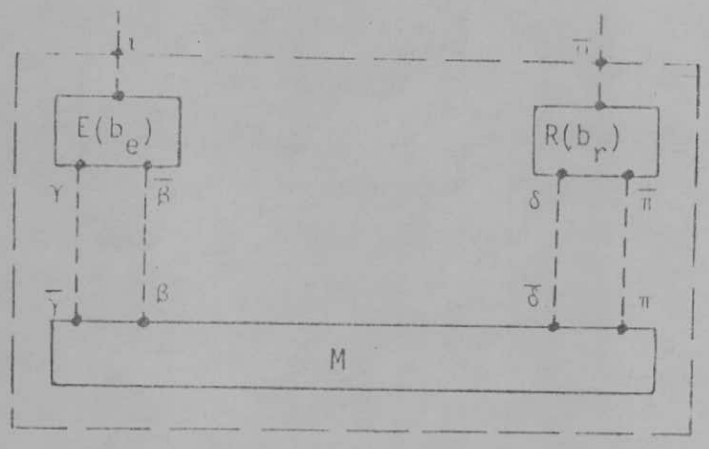

Fig. 3.3 - Agentes relativos ao protocolo do bit alternante

$E(b_e)$ e $R(b_r)$ são parametrizados em b_e e b_r, respectivamente, sendo que essas variáveis guardam o valor do bit alternante (0 ou 1) e são utilizadas para realizar o controle de sequenciamento das mensagens.

$E(b_e)$ recebe dados do produtor através da porta ι e entrega uma men

sagem de dados na porta $\overline{\beta}$. Essa mensagem é composta dos dados recebidos (d), do bit alternante (b_e) e de algum tipo de informação adicional (não representada), que permite detectar se houve ou não corrupção da mesma. Após o envio da mensagem de dados, $E(b_e)$ aguarda a mensagem de confirmação correspondente na porta γ. Caso essa mensagem chegue, esteja íntegra e traga o bit alternante esperado, $E(b_e)$ poderá receber novos dados do produtor. Em qualquer outro caso, $E(b_e)$ retransmitirá a mesma mensagem de dados.

$R(b_r)$ recebe as mensagens de dados através da porta δ. Se uma mensagem é íntegra e traz o bit esperado, $R(b_r)$ entrega os dados através da porta $\overline{\sigma}$ e envia a mensagem de confirmação correspondente. Caso contrário, $R(b_r)$ retransmitirá a última mensagem de confirmação. A mensagem de confirmação é composta da confirmação (c), do bit alternante (b) e de algum tipo de informação adicional (não representada) que permite detectar se houve ou não corrupção da mesma. O valor de b representa sempre o bit alternante da última mensagem de dados recebida corretamente.

M, após receber uma mensagem de dados na porta β, poderá entregá-la (íntegra ou corrompida) na porta $\overline{\delta}$ ou poderá simplesmente perdê-la. De modo semelhante, após receber uma mensagem de confirmação na porta π, poderá entregá-la (íntegra ou corrompida) na porta $\overline{\gamma}$ ou poderá simplesmente perdê-la. Supõe-se que M não pode perder ou corromper a mesma mensagem indefinidamente.

$E(b_e)$ pode ser especificado em CCS através da seguinte expressão de comportamento

$$E(b_e) \Leftarrow \iota d.E' \tag{3.2}$$

onde a expressão de comportamento E' pode ser deduzida através do seguinte conjunto de equações:

$$E' = \overline{\beta} d b_e \,.\, (E' + \gamma x b_x.E'') \tag{3.3}$$

$$E'' = \underline{\text{if}}\ p(x,b_x)\ \underline{\text{then}}\ E((b_e + 1) \bmod 2)\ \underline{\text{else}}\ E' \tag{3.4}$$

onde $p(x,b_x)$ é um predicado habilitador, que verifica a integridade da mensagem de confirmação e verifica se o valor do bit alternante é o esperado.

$R(b_r)$ pode ser especificado em CCS através da seguinte expressão de comportamento

$$R(b_r) \Leftarrow \delta y b_y.R' \tag{3.5}$$

onde a expressão de comportamento R' pode ser deduzida através do seguinte conjunto de equações:

$$R' = \underline{\text{if}}\ q(y,b_y)\ \underline{\text{then}}\ \overline{\sigma}d.\overline{\pi}cb_r.R((b_r+1) \bmod 2)\ \ \underline{\text{else}}\ R'' \qquad (3.6)$$

$$R'' = \overline{\pi}c((b_r+1) \bmod 2).\ R(b_r) \qquad (3.7)$$

obs: cb_r em (3.6) e $c((b_r+1) \bmod 2)$ em (3.7) representam a confirmação da última mensagem de dados recebida corretamente; $q(y,b_y)$ é um predicado habilitador, que verifica a integridade da mensagem de dados e verifica se o valor do bit alternante é o esperado.

M pode ser especificado em CCS através da seguinte expressão de comportamento

$$M \Leftarrow \beta z b_z.M' \qquad (3.8)$$

onde a expressão de comportamento M' pode ser deduzida através do seguinte conjunto de equações:

$$M' = \overline{\delta}vb_v.M'' + M \qquad (3.9)$$

$$M'' = \pi wb_w.(\overline{\gamma}ub_u.M + M) \qquad (3.10)$$

obs: no conjunto de expressões que definem $E(b_e)$, $R(b_r)$ e M, a seguinte notação foi adotada: x, b_x, y, b_y, z, b_z, w e b_w representam variáveis livres, enquanto que d, c, b_e, b_r, v, b_v, u e b_u representam variáveis não-livres, isto é, variáveis que já assumiram seus respectivos valores.

A composição dos três agentes, acima especificados, define um novo serviço de comunicação entre o produtor e o consumidor, cuja expressão de comportamento é dada por

$$BA \Leftarrow E(b_e) \mid M \mid R(b_r) \qquad (3.11)$$

sendo que para $L = \{\beta,\overline{\beta},\gamma,\overline{\gamma},\delta,\overline{\delta},\pi,\overline{\pi}\}$

$$SC' = BA \setminus L \qquad (3.12)$$

é equivalente, em termos de observação, a SC.

3.1. Equivalência de observação ($\approx$) entre SC e SC'

Pode-se verificar que $SC \approx SC'$ através da aplicação do teorema da expansão (te) (2.1) na expressão de comportamento relativa a SC' e utilizando as propriedades da relação de equivalência de observação.

Demonstração:

Substituindo-se BA por sua expressão de comportamento

$$SC' = (E(b_e) | M \mid R(b_r)) \setminus L \qquad (3.13)$$

e utilizando (3.2), (3.5) e (3.8),

$$SC' = (\imath d.E' | \beta z b_z.M' | \delta y b_y.R') \setminus L \qquad (3.14)$$

De acordo com o te e uma vez que a única ação atômica possível na expressão de comportamento (3.14) é $\xrightarrow{\imath d}$ (β e δ estão restritos)

$$SC' \sim \imath d.((E' | \beta_z b_z.M' | \delta y b_y.R') \setminus L) \qquad (3.15)$$

que por sua vez pode ser reescrito, utilizando-se (3.3), como

$$SC' \sim \imath d.((\bar{\beta} d b_e.(E' + \gamma x b_x.E") | \beta z b_z.M' | \delta y b_y.R') \setminus L) \qquad (3.16)$$

Aplicando-se novamente o te e uma vez que a única ação atômica possível em (3.16) é $\xrightarrow{\tau}$ (resultado da sincronização de $\bar{\beta} d b_e$ com $\beta z b_z$)

$$SC' \sim \imath d.\tau_\beta.(((E' + \gamma x b_x.E") | M'(db_e/zb_z) | \delta y b_y.R') \setminus L) \qquad (3.17)$$

obs: para facilitar a compreensão dos leitores, as ações internas $\xrightarrow{\tau}$, serão indexadas com o "nome" das portas onde ocorreu a sincronização.

Realizando-se as devidas substituições de E' e $M'(db_e/zb_z)$ (M' é definido em (3.9)) em (3.17)

$$\begin{aligned} SC' \sim \imath d.\tau_\beta.(((&\bar{\beta} d b_e.(E' + \gamma x b_x.E") + \gamma x b_x.E") | \\ &(\bar{\delta} v b_v.M"(db_e/zb_z) + M) | \\ &\delta y b_y.R') \setminus L) \end{aligned} \qquad (3.18)$$

obs: uma vez que a expressão de comportamento de M é guardada por $\beta z b_z$, z e b_z não são variáveis livres de M, o que implica que $M(db_e/zb_z) = M$.

Procedendo-se a uma nova substituição de M em (3.18)

$$\begin{aligned} SC' \sim \imath d.\tau_\beta.(((&\bar{\beta} d b_e.(E' + \gamma x b_x.E") + \gamma x b_x.E") | \\ &(\bar{\delta} v b_v.M"(db_e/zb_z) + \beta z b_z.M') | \\ &\delta y b_y.R') \setminus L) \end{aligned} \qquad (3.19)$$

De acordo com o te, duas ações internas são possíveis em (3.19):

- $\xrightarrow{\tau_\delta}$, que corresponde à entrega de uma mensagem de dados ao receptor ou
- $\xrightarrow{\tau_\beta}$, que corresponde à retransmissão, por parte do emissor, da mensagem de dados anterior (o meio perdeu a mensagem de dados).

Portanto, (3.19) pode ser reescrita como

$$SC' \sim \imath d.\tau_{\beta}.(\tau_{\delta}.(((\bar{\beta}db_e.(E'+\gamma xb_x.E") + \gamma xb_x.E")|$$
$$M"(db_e/zb_z)| R'(vb_v/yb_y))\setminus L)$$
$$+ \tau_{\beta}.(((E'+\gamma xb_x.E")|M'(db_e/zb_z)|$$
$$\delta yb_y.R')\setminus L)) \qquad (3.20)$$

que por sua vez pode ser condensada em

$$SC' \sim \imath d.\tau_{\beta}.(\tau_{\delta}.B_1 + \tau_{\beta}.B_2) \qquad (3.21)$$

onde B_1 e B_2 representam as expressões de comportamento relativas, respectivamente, ao primeiro e segundo membros da operação soma de (3.20).

Aplicando-se sucessivamente o te em (3.21)

$$SC' \sim \imath d.\tau_{\beta}.(\tau_{\delta}.B_1$$
$$+ \tau_{\beta}.(\tau_{\delta}.B_1$$
$$+ \tau_{\beta}.(\tau_{\delta}.B_1$$
$$+ \tau_{\beta}.(\ldots \quad \ldots)))) \qquad (3.22)$$

obs: (3.22) expressa a possibilidade da ocorrência de um número infinito de retransmissões de mensagens de dados. Como é suposto que o meio eventualmente entregará uma mensagem de dados, eventualmente ocorrerá a ação interna $\overset{\tau}{\underline{\delta}}$, e o comportamento de SC' passará a ser expresso por B_1.

Aplicando-se sucessivamente as propriedades (2.2), (2.3) e (2.4) em (3.22)

$$SC' = \imath d.\tau_{\beta}.\tau_{\delta}.B_1$$
$$= \imath d.B_1 \qquad (3.23)$$

com
$$B_1 = ((\bar{\beta}db_e.(E'+\gamma xb_x.E") + \gamma xb_x.E")|$$
$$M"(db_e/zb_z)|R'(vb_v/yb_y))\setminus L \qquad (3.24)$$

Realizando-se as devidas substituições de $M"(db_e/zb_z)$ e $R'(vb_v/yb_y)$ em (3.24)

$$B_1 = ((\bar{\beta}db_e.(E'+\gamma xb_x.E") + \gamma xb_x.E")|\ \pi wb_w.(\bar{\gamma}ub_u.M + M)|$$
$$\underline{\text{if}}\ q(v,b_v)\ \underline{\text{then}}\ \bar{o}d.\bar{\pi}cb_r.\ R((b_r+1) \bmod 2)$$
$$\underline{\text{else}}\ \bar{\pi}c((b_r+1) \bmod 2).\ R(b_r))\setminus L \qquad (3.25)$$

Em função do valor assumido por $q(v,b_v)$, B_1 poderá ser reescrito como:

(a) se $q(v,b_v)$ = false, então B_1 passará a ser descrito por

$$B_1' = ((\bar{\beta}db_e.(E'+\gamma xb_x.E") + \gamma xb_x.E")| \pi wb_w.(\bar{\gamma}ub_u.M + M)|$$
$$\bar{\pi}c((b_r+1) \bmod 2).R(b_r))\setminus L \qquad (3.25a)$$

significando que a mensagem de dados recebida não é íntegra ou não traz o bit esperado. Nesse caso não haverá dados à disposição do consumidor.

De acordo com o **te** e uma vez que a única ação interna possível em (3.25a) é $\xrightarrow{\tau_\pi}$

$$B_1' \sim \tau_\pi.(((\bar{\beta}db_e.(E'+\gamma xb_x.E") + \gamma xb_x.E")|$$
$$(\bar{\gamma}ub_u.M + M)| R(B_r))\setminus L) \qquad (3.26a)$$

significando que uma mensagem de confirmação relativa à última mensagem de dados corretamente recebida foi enviada.

Utilizando-se a definição de M em (3.26a)

$$B_1' \sim \tau_\pi.(((\bar{\beta}db_e.(E'+\gamma xb_x.E") + \gamma xb_x.E")|$$
$$(\bar{\gamma}ub_u.\beta zb_z.M' + \beta zb_z.M')| R(b_r))\setminus L) \qquad (3.27a)$$

que de acordo com o **te** pode ser transformado em

$$B' \sim \tau_\pi.(\tau_\gamma.((E"(ub_u/xb_x)| \beta zb_z.M'| R(b_r))\setminus L)$$
$$+ \tau_\beta.(((E' + \gamma xb_x.E")| M'(db_e/zb_z)| R(b_r))\setminus L)) \qquad (3.28a)$$

onde $E"(ub_u/xb_x) = E'$, uma vez que $p(x,b_x)$ = false (a mensagem de reconhecimento recebida pelo emissor não é a esperada).

Utilizando-se em (3.28a) a equação (3.3)

$$B_1' \sim \tau_\pi.(\tau_\gamma.((\bar{\beta}db_e.(E' + \gamma xb_x.E")| \beta zb_z.M'| R(b_r))\setminus L)$$
$$+ \tau_\beta.(((E' + \gamma xb_x.E")| M'(db_e/zb_z)| R(b_r))\setminus L)) \qquad (3.29a)$$

e aplicando o **te** em (3.29a)

$$B_1' \sim \tau_\pi.(\tau_\gamma.\tau_\beta.(((E' + \gamma xb_x.E")| M'(db_e/zb_z)| R(b_r))\setminus L)$$
$$+ \tau_\beta.(((E' + \gamma xb_x.E")| M'(db_e/zb_z)| R(b_r))\setminus L)) \qquad (3.30a)$$

Utilizando-se (3.5) e aplicando-se sucessivamente as propriedades

(2.2), (2.3) e (2.4) em (3.30a)

$$B_1' \simeq ((E' + \gamma x b_x.E'')|\ M'(db_e/zb_z)|\delta y b_y.R')\setminus L \qquad (3.31a)$$

Combinando-se as relações (3.31a) a (3.17), para esse caso

$$SC' \simeq \imath d.\tau_\beta.B_1'$$

$$\simeq \imath d.B_1' \qquad (3.32a)$$

onde B_1' passará a ser descrito por B_1 (3.25).

Como eventualmente o receptor receberá uma mensagem de dados íntegra e com o bit esperado, isso implicará que eventualmente

(b) $q(v,b_v)$ = true, então B_1 passará a ser descrito por

$$B_1'' = ((\bar{\beta}db_e.(E' + \gamma x b_x.E'') + \gamma x b_x.E'')|\ \pi w b_w.(\bar{\gamma}ub_u.M + M)|$$
$$\bar{o}d.\bar{\pi}cb_r.R((b_r+1) \bmod 2))\setminus L \qquad (3.25b)$$

Em (3.25b) a única ação atômica possível é $\underline{\bar{o}d}$ (os dados estão à disposição do consumidor). Aplicando-se sucessivamente te

$$B_1'' \sim \bar{o}d.(((\bar{\beta}db_e.(E' + \gamma x b_x.E'') + \gamma x b_x.E'')|\ \pi w b_w.(\bar{\gamma}ub_u.M + M)|$$
$$\bar{\pi}cb_r.\ R((b_r+1) \bmod 2))\setminus L) \qquad (3.26b)$$

$$B_1'' \sim \bar{o}d.\tau_\pi.(((\bar{\beta}db_e.(E' + \gamma x b_x.E'') + \gamma x b_x.E'')|$$
$$(\bar{\gamma}ub_u.M + M)|\ R((b_r+1) \bmod 2))\setminus L)$$
$$\sim \bar{o}d.\tau_\pi.(((\bar{\beta}db_e.(E' + \gamma x b_x.E'') + \gamma x b_x.E'')|$$
$$(\bar{\gamma}ub_u.\ \beta zb_z.M' + \beta zb_z.M')|\ R((b_r+1) \bmod 2))\setminus L) \qquad (3.27b)$$

$$B_1'' \sim \bar{o}d.\tau_\pi.(\tau_\gamma.((E''(ub_u/xb_x)|\ \beta zb_z.M'|\ R((b_r+1) \bmod 2))\setminus L)$$
$$+ \tau_\beta.(((E' + \gamma x b_x.E'')|\ M'(db_e/zb_z)|$$
$$R((b_r+1) \bmod 2))\setminus L)) \qquad (3.28b)$$

onde o segundo termo da operação "soma" mais externa de (3.28b) reflete a possibilidade de perda da mensagem de confirmação e a consequente retransmissão da mensagem de dados.

A relação (3.28b) pode ser condensada em

$$B_1'' \sim \bar{o}d.\tau_\pi.(\tau_\gamma.\ B_3 + \tau_\beta.\ B_4) \qquad (3.29b)$$

Desenvolvendo-se B_4

$$B_4 = ((E' + \gamma x b_x . E'') \mid M'(d b_e / z b_z) \mid R((b_r+1) \bmod 2)) \setminus L \qquad (3.30b)$$

e considerando que o meio eventualmente entregará uma mensagem de dados ao receptor, chega-se a uma relação semelhante a (3.25)

$$B_4 = ((\bar{\beta} d b_e . (E' + \gamma x b_x . E'') + \gamma x b_x . E'') \mid \pi w b_w . (\bar{\gamma} u b_u . M + M) \mid$$
$$\underline{\text{if}}\ q(v,b_v)\ \underline{\text{then}}\ \bar{o}d .\ \bar{\pi} c b_r .\ R((b_r+1) \bmod 2)$$
$$\underline{\text{else}}\ \bar{\pi} c((b_r+1) \bmod 2) .\ R(b_r)) \setminus L \qquad (3.31b)$$

onde, necessariamente, $q(v,b_v)$ = false. Isto porque, mesmo que a mensagem esteja íntegra, os dados relativos a essa mensagem já foram entregues ao consumidor e, portanto, não traz o bit esperado. Consequentemente, recai-se no caso (a) e a expressão de comportamento de B_4 é a indicada em (3.25a), isto é, para esse caso,

$$B_4 \simeq B_1' \qquad (3.32b)$$

Como eventualmente o meio entregará uma mensagem de confirmação ao emissor, então, eventualmente

$$B_1'' \simeq \bar{o}d . \tau_\pi . \tau_\gamma . B_3 \qquad (3.33b)$$

Desenvolvendo-se B_3

$$B_3 = (E''(u b_u / x b_x) \mid \beta z b_z .\ M' \mid R((b_r+1) \bmod 2)) \setminus L \qquad (3.34b)$$

e utilizando a equação (3.4),

$$B_3 = (\underline{\text{if}}\ p(u,b_u)\ \underline{\text{then}}\ E((b_e+1) \bmod 2)\ \underline{\text{else}}\ E' \mid$$
$$\beta z b_z .\ M' \mid R((b_r+1) \bmod 2)) \setminus L \qquad (3.35b)$$

Em função do valor assumido por $p(u,b_u)$, B_3 poderá ser reescrito como

(i) se $p(u,b_u)$ = false, então B_3 passará a ser descrito por

$$B_3' = (E' \mid \beta z b_z . M' \mid R((b_r+1) \bmod 2)) \setminus L \qquad (3.35bi)$$

significando que a mensagem de confirmação não é íntegra e a mensagem de dados será retransmitida.

O desenvolvimento de (3.35bi) é análogo ao desenvolvimento de (3.15), que gera, por sua vez, a expressão de comportamento B_1 definida em (3.24). Uma vez que o receptor não entregará os dados relativos à mensagem de

dados retransmitida

$$B_3' \simeq B_1' \qquad (3.36bi)$$

Como eventualmente a mensagem de confirmação estará íntegra, eventualmente

(ii) $p(u,b_u)$ = true, então B_3 passará a ser descrito por

$B_3'' = (E((b_e+1) \bmod 2)|\, M \,|\, R((b_r+1) \bmod 2)) \setminus L$

significando que o emissor poderá receber novos dados do produtor.

$$B_3'' = B_3 = SC' \qquad (3.35bii)$$

Utilizando-se (3.33b) e (3.35bii)

$$B_1'' \simeq \bar{o}d.\tau_\pi.\tau_\gamma.SC'$$
$$\simeq \bar{o}d.SC' \qquad (3.36b)$$

Como no caso (b) $B_1'' = B_1$, substituindo-se (3.36b) em (3.23) obtém-se

$$\boxed{SC' \simeq id.\bar{o}d.SC'} \qquad (3.37)$$

que é uma expressão de comportamento equivalente, em termos de observação, à expressão de comportamento de SC (3.1). Portanto,

$$\boxed{SC \simeq SC'} \quad \text{c.q.d.}$$

4. Refinamentos sucessivos de um mesmo sistema em CCS

A descrição de sistemas através de CCS permite ao projetista:

(a) realizar diversas especificações de um mesmo sistema em diferentes níveis de abstração e

(b) a cada refinamento do sistema, provar que a nova especificação comporta-se de modo equivalente à especificação obtida no nível de abstração imediatamente superior.

Na seção anterior foram especificados o sistema de comunicação SC e o seu primeiro refinamento SC' e foi demonstrado, de forma exaustiva, que $SC \simeq SC'$. Nesta seção é simplesmente realizado um novo refinamento para esse

sistema (SC"), sendo que a demonstração da equivalência entre SC' e SC" é deixada a cargo do leitor.

Nesta nova especificação, $E(b_e)$ será considerado composto de um transmissor $Tr(b_e)$ e um temporizador Te (Fig. 4.1), M será considerado composto de dois meios de comunicação simplex (M_1,M_2) e um sumidouro de mensagens (S) (Fig. 4.2), enquanto que $R(b_r)$ será mantido inalterado.

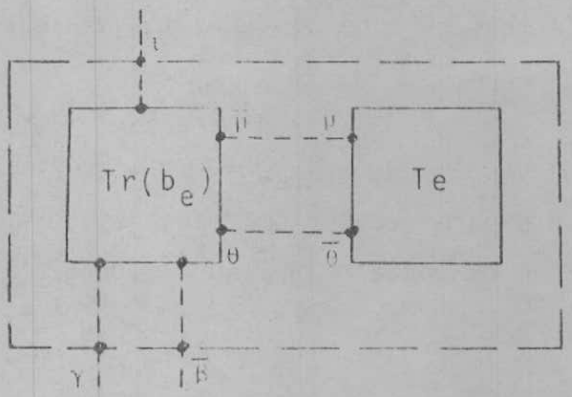

Fig. 4.1 - Refinamento de $E(b_e)$

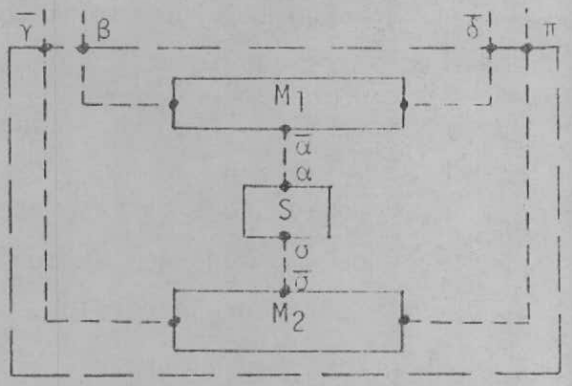

Fig. 4.2 - Refinamento de M

$Tr(b_e)$ comporta-se de modo análogo a $E(b_e)$, sendo que a diferença básica está na possibilidade da ocorrência, em $Tr(b_e)$, dos seguintes eventos: inicialização do temporizador Te através de um sincronismo em $\bar{\mu}$ e fim da temporização através de um sincronismo em θ.

$$Tr(b_e) \Leftarrow \iota d.Tr' \tag{4.1}$$

$$Tr' = \bar{\beta} db_e.\bar{\mu}.(\iota x b_x.Tr'' + \theta.Tr') \tag{4.2}$$

$$Tr'' = \underline{\text{if}}\ p(x,b_x)\ \underline{\text{then}}\ Tr((b_e+1) \bmod 2)\ \ \underline{\text{else}}\ Tr' \tag{4.3}$$

obs: é interessante observar em (4.2), que o estouro do temporizador só terá efeito sobre $Tr(b_e)$, quando ocorrer antes da chegada de uma mensagem de confirmação.

O temporizador Te, após ser inicializado em μ, aguarda t_{max} unidades inteiras de tempo para sinalizar o fim da temporização em $\bar{\theta}$. Te pode ser reinicializado a qualquer momento por $Tr(b_e)$.

$$Te \Leftarrow \mu.Te'(0) \tag{4.4}$$

$$Te' = \underline{\text{if}}\ p(t)\ \underline{\text{then}}\ (Te + Te'(t+1))\ \ \underline{\text{else}}\ \bar{\theta}.\ Te \tag{4.5}$$

onde p(t) é um predicado habilitador que verifica se o número de unidades inteiras $t < t_{max}$.

M_1 recebe uma mensagem de dados em β e pode entregá-la ao consumidor (íntegra ou corrompida) na porta $\overline{\delta}$, ou pode entregá-la ao sumidouro na porta $\overline{\alpha}$. M_1 só pode transportar uma mensagem de dados por vez, sendo que é suposto que M_1 não pode perder ou corromper a mesma mensagem de dados indefinidamente.

$$M_1 \Leftarrow \beta z b_z . (\overline{\delta} v b_v . M_1 + \overline{\alpha} v b_v . M_1) \tag{4.6}$$

M_2 é um meio de comunicação de mensagens de confirmação, cujo comportamento é análogo ao de M_1.

$$M_2 \Leftarrow \pi w b_w . (\overline{\gamma} u b_u . M_2 + \overline{\sigma} u b_u . M_2) \tag{4.7}$$

O sumidouro S está sempre pronto para receber uma mensagem de dados na porta α, ou uma mensagem de confirmação na porta σ. Qualquer mensagem recebida por S é considerada perdida.

$$S \Leftarrow \alpha v b_v . S + \sigma u b_u . S \tag{4.8}$$

obs: no conjunto de expressões que definem $Tr(b_e)$, Te, M_1, M_2 e S foi adotada uma notação semelhante à utilizada para definir $E(b_e)$, $R(b_r)$ e M.

A composição do agente $Tr(b_e)$ com o agente Te define um sistema "emissor composto", que para $L_1 = \{\mu, \overline{\mu}, \theta, \overline{\theta}\}$ oferece um serviço

$$SE = (Tr(b_e) \mid Te) \setminus L_1 \tag{4.9}$$

e pode-se provar que $SE \simeq E(b_e)$.

A composição dos agentes M_1, M_2 e S define um sistema "meio de comunicação composto", que para $L_2 = \{\alpha, \overline{\alpha}, \sigma, \overline{\sigma}\}$ oferece um serviço

$$SM = (M_1 \mid M_2 \mid S) \setminus L_2 \tag{4.10}$$

e pode-se provar que $SM \simeq M$.

Uma vez provadas essas duas equivalências, a demonstração da equivalência do novo serviço de comunicação,

$$SC'' = (SE \mid SM \mid R(b_r)) \setminus L \tag{4.11}$$

em relação a SC' e SC, é mera decorrência.

Novos refinamentos são possíveis. Por exemplo, pode-se melhorar a especificação do comportamento de Te e pode-se definir como as mensagens de dados em M_1 e as mensagens de confirmação em M_2 são corrompidas.

A cada novo refinamento é importante que uma nova prova, que garan-

ta a equivalência entre as especificações, seja realizada. Portanto, para os sistemas de comunicação reais, bem mais complexos que o apresentado neste trabalho, é evidente a necessidade de automatização (parcial ou plena) do procedimento de demonstração.

5. Conclusão

Neste artigo procurou-se utilizar as potencialidades da álgebra CCS para a especificação e verificação formais de sistemas de comunicação. Para tal, após uma apresentação sumária dessa técnica, a mesma foi utilizada em diferentes especificações de um mesmo sistema, demonstrando assim o seu alto grau de abstração.

A verificação da equivalência de observação, entre as duas primeiras especificações, foi realizada detalhadamente, a fim de demonstrar o poder de análise de CCS e também para que o leitor sentisse a complexidade desse tipo de prova e a consequente necessidade de sua automatização. A verificação da terceira especificação, assim como as sugestões para novos refinamentos, foram deixadas como exercícios aos interessados.

CCS é um cálculo voltado para a descrição da dinâmica da comunicação entre processos. Os aspectos estáticos envolvidos nas interações, tais como os tipos de dados, não são definidos de forma precisa. Portanto, para que seja possível uma completa definição desses processos, é necessário complementar essa álgebra.

Cabe salientar ainda o reduzido número de operadores CCS (oito), que pode dificultar as descrições de serviços e protocolos complexos. Por exemplo, existe somente uma operação (composição) capaz de expressar comunicação e pseudoconcorrência. A adição de novos operadores, assim como certas mudanças na sintaxe, poderiam tornar essa álgebra mais expressiva e facilitar a legibilidade das especificações de tais sistemas.

6. Referências

[Boch 78] G.v. Bochmann, "Finite state description of communication protocols", Computer Networks, Vol 2, Nº 4/5, 1978, pp. 361-372.

[JaBo 83] C. Jard, G.v. Bochmann, "An approach to testing specifications", anais do ACM SIGSOFT/SIGPLAN Software Engineering Symposium on High-Level Debugging, Pacific Grove (USA), 1983, pp. 53-59.

[Lope 87] W. Lopes de Souza, "LOTOS: Uma técnica para a descrição formal de

serviços e protocolos de comunicação", anais do 5º Simpósio Brasileiro de Redes de Computadores, São Paulo (SP), 1987, pp. 121-144.

[LoSt 88] W. Lopes de Souza, S. Stiubiener, "Especificação e validação de protocolos", rel. técnico Nº 01/88, GRC/UFPb, Campina Grande (Pb), 1988.

[Miln 80] R. Milner, "A Calculus of Communicating Systems", ed. G. Goos e J. Hartmanis, Springer-Verlag, 1980.

Anexo 1: sintaxe das expressões de comportamento CCS

	expressão B"	espécie L(B")	variáveis livres FV(B")
operações nula (inaction)	NIL	$\varnothing$	$\varnothing$
soma (summation)	B+B'	$L(B) \cup L(B')$	$FV(B) \cup FV(B')$
ação (action)	$\alpha x_1,\ldots,x_n.B$ $\overline{\alpha} E_1,\ldots,E_n.B$ $\tau.B$	$L(B) \cup \{\alpha\}$ $L(B) \cup \{\overline{\alpha}\}$ $L(B)$	$FV(B)-\{x_1,\ldots,x_n\}$ $FV(B) \cup \bigcup_i FV(E_i)$ $FV(B)$
composição (composition)	$B \mid B'$	$L(B) \cup L(B')$	$FV(B) \cup FV(B')$
restrição (restriction)	$B \setminus \alpha$	$L(B)-\{\alpha,\overline{\alpha}\}$	$FV(B)$
rerotulação (relabelling)	$B[S]$	$S(L(B))$	$FV(B)$
identificador (identifier)	$b(E_1,\ldots,E_{n(b)})$	$L(b)$	$\bigcup_i FV(E_i)$
condição (conditional)	if E then B else B'	$L(B) \cup L(B')$	$FV(E) \cup FV(B) \cup FV(B')$

Anexo 2: semântica de CCS expressa através de regras de inferência

1. nula (Inaction)

   NIL não permite ações atômicas

2. soma (Sum →)

   (1) $\dfrac{B_1 \xrightarrow{\mu v} B_1'}{B_1+B_2 \xrightarrow{\mu v} B_1'}$ (2) $\dfrac{B_2 \xrightarrow{\mu v} B_2'}{B_1+B_2 \xrightarrow{\mu v} B_2'}$

3. ação (Act →)

   (1) $\alpha x_1,\ldots,x_n.B \xrightarrow{\alpha(v_1,\ldots,v_n)} B\{v_1/x_1,\ldots,v_n/x_n\}$

   (2) $\bar{\alpha} v_1,\ldots,v_n.B \xrightarrow{\bar{\alpha}(v_1,\ldots,v_n)} B$

   (3) $\tau.B \xrightarrow{\tau} B$

4. composição (Com →)

   (1) $\dfrac{B_1 \xrightarrow{\mu v} B_1'}{B_1|B_2 \xrightarrow{\mu v} B_1'|B_2}$ (2) $\dfrac{B_2 \xrightarrow{\mu v} B_2'}{B_1|B_2 \xrightarrow{\mu v} B_1|B_2'}$

   (3) $\dfrac{B_1 \xrightarrow{\lambda v} B_1' \text{ e } B_2 \xrightarrow{\bar{\lambda} v} B_2'}{B_1|B_2 \xrightarrow{\tau} B_1'|B_2'}$

5. restrição (Res →) $\dfrac{B \xrightarrow{\mu v} B'}{B\backslash\alpha \xrightarrow{\mu v} B'\backslash\alpha}$, $\mu \notin \{\alpha,\bar{\alpha}\}$

6. rerotulação (Rel →) $\dfrac{B \xrightarrow{\mu v} B'}{B[S] \xrightarrow{(S\mu)v} B'[S]}$ obs: por convenção $S\tau = \tau$

7. identificação (Ide →) $b(x_1,\ldots,x_{n(b)}) \Leftarrow B_b$ onde $FV(B_b) \subseteq \{x_1,\ldots,x_{n(b)}\}$

   $\dfrac{B_b\{v_1/x_1,\ldots,v_{n(b)}/x_{n(b)}\} \xrightarrow{\mu v} B'}{b(v_1,\ldots,v_{n(b)}) \xrightarrow{\mu v} B'}$

8. condição (Con →)

   (1) $\dfrac{B_1 \xrightarrow{\mu v} B_1'}{(\underline{\text{if}}\ \text{true}\ \underline{\text{then}}\ B_1\ \underline{\text{else}}\ B_2) \xrightarrow{\mu v} B_1'}$ (2) $\dfrac{B_2 \xrightarrow{\mu v} B_2'}{(\underline{\text{if}}\ \text{false}\ \underline{\text{then}}\ B_1\ \underline{\text{else}}\ B_2) \xrightarrow{\mu v} B_2'}$