Tornando LOTOS Apta para Especificar Sistemas Tempo Real

Murilo S. de Camargo* e Jean-Marie Farines

LCMI - EEL - CTC
Universidade Federal de Santa Catarina
Caixa Postal 476 - 88.040-900 - Florianópolis - S.C.
Telefone: (0482) 31-9202 - Fax: (0482) 34-9770
E-mail: {murilo,farines}@lcmi.ufsc.br

Sumário: *Neste artigo é apresentada uma extensão da linguagem LOTOS Básico [3] com capacidade para representar e tratar restrições de tempo associadas à ações (tais ações são referenciadas como ações temporizadas). Estas restrições, especificadas como intervalos de tempo, têm uma influência direta no modo que as ações podem ser oferecidas e sincronizadas. Uma característica importante do modelo proposto é o caráter "imperativo" que foi dado às restrições de tempo, daí o nome RT_LOTOS (Real Time LOTOS). Ações específicas são introduzidas no modelo para expressar violações temporais que são a conseqüência das ações não realizadas. Assim, o modelo apresentado torna-se particularmente atraente para especificação formal de sistemas tempo real. Um novo operador, preempção temporal, é definido na linguagem para permitir ao usuário expressar o comportamento do sistema na presença de violações temporais. Após ter apresentado a semântica completa de RT_LOTOS alguns pequenos exemplos são propostos para ilustrar os principais conceitos deste modelo.*

Palavras-chave: especificação formal, verificação, sistemas distribuídos, tempo real, sistemas multimídia

1 Introdução

A necessidade de representar e analisar sistemas nos quais o tempo tem um papel fundamental como é o caso para Sistemas Tempo Real Críticos ou para Sistemas Multimídia, leva a procura de novos modelos temporizados ou a extensão dos existentes através do uso explícito do tempo.

Neste trabalho, é apresentada uma proposta de extensão da linguagem de especificação formal Basic LOTOS [3, 12] destinada a representar aplicações tempo real. O modelo proposto é chamado RT_LOTOS (Real Time LOTOS). A escolha de LOTOS

*Professor do Depto. de Informática e Estatística da UFSC, em doutoramento no LCMI-EEL-UFSC

como modelo de base se deve principalmente ao seu conhecido poder de expressão e de análise, e a sua conseqüente utilização para representar e analisar Sistemas de Comunicação e aplicações distribuídas. Neste artigo, a álgebra de processos RT_LOTOS é apresentada formalmente e são discutidas as escolhas feitas para sua semântica, tanto do ponto de vista das potencialidades de representação como de análise e verificação.

O presente artigo é organizado como segue: A seção 2 apresenta uma sinopse intuitiva do modelo RT_LOTOS. Na seção 3 é descrita a sintaxe e semântica informal do modelo. Na seção 4 é apresentada a definição completa da álgebra de processos RT_LOTOS incluindo a definição de sua semântica operacional estrutural e a generalização para o modelo de relações de bissimulação clássicas. A seção 5 mostra como as restrições temporais básicas podem ser representadas no modelo e também são apresentados alguns exemplos de aplicações. Na seção 6 é apresentado um comentário sobre algumas das várias técnicas de verificação possíveis para álgebras de processos temporizados. Finalmente na seção 7, o modelo proposto é relacionado com outros existentes e também são apresentados os comentários finais e perspectivas futuras para o trabalho.

2 A visão intuitiva de RT_LOTOS

Nesta seção é apresentada a visão intuitiva que serviu de base para propor uma nova extensão temporal para a linguagem LOTOS. Para continuar em conformidade com Basic LOTOS, chamaremos *Act* o conjunto das ações observáveis e i a ação interna.

Afim de possibilitar a definição de restrições temporais em uma especificação escolhemos definir ações temporizadas associando intervalos de tempo às ações observáveis. Estes intervalos, da forma, $[t_{min},t_{max}]$, determinam em que instante as diferentes ações podem ser oferecidas ao seu ambiente. Se nenhum intervalo é associado explicitamente à uma dada ação observável, faz-se a hipótese de que o intervalo $[0,\infty]$ está associado a esta ação. Em outras palavras, as ações observáveis não temporizadas são consideradas como não urgentes.

O fato de associar um tempo máximo t_{max} à uma ação não implica que se deseja forçar a urgência de uma tal ação temporizada, pois procuramos manter o paradigma das álgebras de processos no qual a aceitação de uma ação observável depende de seu ambiente. Na nossa proposta objetiva-se indicar que se a ação $[t_{min},t_{max}]a$ não pôde se realizar durante o intervalo especificado, então ela não poderá o ser fora deste intervalo. Para poder caracterizar esta situação, define-se um conjunto de ações especiais, chamado Act^*. Estas ações especiais, chamadas violações temporais, têm por objetivo notificar, quando da execução de uma especificação, que ações temporizadas não puderam se realizar dentro dos intervalos que lhes foram associados. Assim, chama-se a^* a ação especial caracterizando a violação temporal associada à não realização de uma certa ação temporizada $[t_{min}, t_{max}]a$. O interesse de poder dispor destas ações especiais reside na possibilidade de representar em uma especificação tratamentos de exceção à serem realizados quando da ocorrência de tais violações temporais. Para realizar isso, introduz-se um novo operador, chamado de operador de preempção temporal, destinado a exprimir os tratamentos de exceção desejados.

Como poderá ser observado na descrição formal da semântica de RT_LOTOS, permitiu-se também a ocultação de ações observáveis temporizadas. Para manter

a coerência do modelo, optou-se por permitir a associação de restrições temporais também à ação interna i sem que seja aumentada a complexidade da semântica. Todavia, devem ser notadas com relação a temporização da ação i duas diferenças fundamentais que caracterizam a urgência da ação interna i:

- na falta de uma temporização explícita da ação interna i ela é considerada como sendo temporizada pelo intervalo temporal $[0,0]$,
- além disso não é definida violação temporal associada à $[t_{min}, t_{max}]i$, dado que i deve, necessariamente, realizar-se no intervalo $[t_{min}, t_{max}]$.

Finalmente, procuramos definir RT_LOTOS como uma extensão estrita de Basic LOTOS. Para convencer-se disso é suficiente associar intervalos temporais $[0,\infty]$ às ações observáveis e de não mais considerar, na semântica operacional, as regras de progressão do tempo. Além disso, o fato de considerar intervalos temporais $[0,\infty]$ para todas as ações tornam sem nenhum efeito as regras da semântica operacional tratando das violações temporais.

3 Descrição da sintaxe e dos operadores de RT_LOTOS

3.1 Sintaxe de RT_LOTOS

Os termos de RT_LOTOS são gerados pela sintaxe apresentada a seguir. Observe-se que esta é uma extensão direta da sintaxe de Basic LOTOS.

$E ::=$	$stop$	(* inação *)
$\mid$	$exit$	(* terminação com sucesso *)
$\mid$	$[t_{min}, t_{max}]a; E$	(* prefixação *)
$\mid$	$[t_{min}, t_{max}]i; E$	(* prefixação *)
$\mid$	$E[\,]E'$	(* escolha *)
$\mid$	$E\|[L]\|E'$	(* composição paralela *)
$\mid$	$hide\ L\ in\ E$	(* ocultação *)
$\mid$	$E >> F$	(* composição seqüencial *)
$\mid$	$E [> F$	(* preempção *)
$\mid$	$E <L] \{a_1{:}Q_1, \cdots, a_n{:}Q_n\}$	(* preempção temporal *)
$\mid$	$P[a_1, \cdots, a_n]$	(* instanciação de processos *)

O símbolo $\mathcal{E}$ será usado para denotar o conjunto dos termos gerados pela sintaxe de RT_LOTOS. Além disso, cometer-se-á, na continuação do texto, o abuso de linguagem clássico confundindo expressões de comportamento e processos para qualificar os termos gerados por esta sintaxe.

3.2 Descrição informal dos operadores de RT_LOTOS

A descrição informal dos termos de RT_LOTOS é dada a seguir.

"*stop*" representa um processo que não faz nada, exceto deixar o tempo progredir.

"*exit*" representa o processo de terminação com sucesso clássica de LOTOS. A ação δ da semântica de *exit* não é urgente.

"$[t_{min}, t_{max}]a; E$" representa um processo no qual a ação a só pode ser oferecida dentro do intervalo de tempo $[t_{min}, t_{max}]$; antes de t_{min} a ação sofre um atraso deixando o tempo apenas progredir, e depois de t_{max} o oferecimento da ação "caduca", deixando de existir. Se no intervalo de tempo a ação a é realizada, então $[t_{min}, t_{max}]a; E$ passa a se comportar como E. Se a ação a ficou oferecida até o instante t_{max} e não foi realizada, então ocorre a violação temporal a^* neste instante e o processo passa a se comportar como o processo *stop*.

"$E[\,]F$" representa a escolha entre os processos E e F. O processo se comporta como E ou como F, com a escolha sendo realizada no instante da realização de uma primeira ação $a \in Act$; isto significa que a realização de uma ação de violação temporal a^* não decide uma escolha.

"$E|[L]|F$" representa o operador de composição paralela de dois processos. Cada um dos dois processos pode realizar, de modo independente, as ações que não pertençam ao conjunto L, sendo que para as ações no conjunto L os processos devem se sincronizar. As sincronizações ocorrem desde que elas sejam possíveis, isto é, se ambos os processos oferecem uma ação para se sincronizar, então esta ação é realizada imediatamente. Ou seja, estamos atribuíndo uma semântica de progresso máximo[1] às *ações sincronizáveis*. No caso de um dos dois processos não oferecer a ação sincronizável até a expiração do intervalo de tempo da ação oferecida ocorrerá uma ação de violação temporal associada a ação cujo intervalo temporal expirou; o comportamento subseqüente continuará sendo a composição paralela do processo que segue a violação temporal com o processo que não ofereceu a ação à sincronizar.

"hide L in E" representa um processo que transforma as ações observáveis em L em invisíveis (e urgentes).

"$E >> F$" representa a composição seqüencial de dois processos E e F. Sua interpretação informal é que se o processo E termina com sucesso, e não por causa de um deadlock prematuro, então a execução do processo F é possível.

"$E\ [> F$" representa um processo que se comporta como E, mas que pode ser interrompido a qualquer instante pela realização de uma ação de F. Se E termina sem que o processo F comece, então "$E\ [> F$" também termina. Mas, se uma ação de F ocorre antes do término de E, então a execução do processo E é abandonada e o controle passa para o processo F.

"$E < L]\,\{a_1 : Q_1, \cdots, a_n : Q_n\}$" representa o operador de preempção temporal. Este operador possui aridade $n + 1$ onde $n < \infty$ é a cardinalidade do conjunto L, i.e. $|L| = n$. Os "$a_i : Q_i$" têm o seguinte propósito: os "a_i" são rótulos identificadores e "Q_i" são processos; "a_i" indica que é o processo "Q_i" que tratará uma eventual violação temporal "a_i^*". Para simplificar a explanação considere-se o processo $P = E < L]\,\{a_1 : Q_1, \cdots, a_n : Q_n\}$. Assim, o processo P começa pela execução de E. Se E termina sem ocorrências de violações temporais a^* tal que $a \in L$, então o processo P termina. Mas, se durante a execução de E ocorrer uma violação temporal a_i^* com

[1] Diz-se que um modelo possui semantica de progresso máximo ou retardo mínimo para uma dada ação se ela ocorre tão logo esteja pronta para tal [16].

$a_i \in L$, então a execução do processo E é abandonada e o processo Q_i é iniciado no seu lugar.

$P[a_1/a'_1, \cdots, a_n/a'_n]$ representa uma instanciação do processo $P[a'_1, \cdots, a'_n]$ em que as ações a'_i têm seu nome trocado para a_i, para $i = 1, \cdots, n$.

4 A álgebra de processos RT_LOTOS

Esta seção é dedicada à definição formal da álgebra de processos RT_LOTOS.

Uma álgebra de processos é definida [16] como uma quádrupla $(OP, \mathcal{L}, R_{\mathcal{L}}^{OP}, \sim)$ onde

- OP é um conjunto de operadores definindo a linguagem da álgebra de processos
- $\mathcal{L}$ é um conjunto de nomes de transições
- $R_{\mathcal{L}}^{OP}$ é um conjunto de regras da semântica operacional estrutural *à la Plotkin* [18] associando os termos da álgebra de processos com sistemas de transições rotuladas em $\mathcal{L}$ (modelos)
- $\sim \subseteq AP \times AP$ é uma equivalência comportamental sobre modelos.

No caso de uma álgebra de processos temporizada aumenta-se o conjunto $\mathcal{L}$ unindo-se a ele os elementos de um domínio de tempo D, obtendo-se um conjunto de ações estendido $\mathcal{L} \cup D$. Definem-se, para cada operador da álgebra, regras de inferência rotuladas por elementos deste domínio de acordo com a semântica que se quer atribuir à álgebra temporizada. Entretanto, é necessário assumir como hipótese básica que o domínio de tempo considerado seja *enumerável* para que o sistema de transições rotuladas subjacente à esta álgebra de processos seja bem definido. Esta hipótese não é demasiadamente restritiva visto que conjuntos densos (como é o caso dos números racionais) e esparsos (como por exemplo os números naturais) a satisfazem.

Os elementos que compõem a álgebra de processos RT_LOTOS são definidos nas próximas seções na seguinte ordem. Inicialmente, é definido o domínio de tempo a ser considerado. A seguir, é apresentado o conjunto de ações de RT_LOTOS. Depois, são apresentadas as regras da semântica operacional estrutural. Finalmente, são apresentadas algumas bissimulações desenvolvidas para RT_LOTOS, dentre elas uma congruência.

4.1 O Domínio de Tempo Considerado

Em RT_LOTOS, nem a sintaxe, nem a semântica dependem de um domínio de tempo particular. Como em [13], a única hipótese feita aqui é que o domínio de tempo seja enumerável o que garante que o modelo semântico subjacente seja um Sistema de Transições Rotuladas. Procedendo desta maneira, pode-se considerar tanto domínios de tempo *esparsos* (inteiros naturais) quanto *densos* (racionais).

Seja D o domínio de tempo. D^ω denota o conjunto $D \cup \{\omega\}$ onde ω é um conjunto não pertencente a D e tal que $\forall d \in D,\ d < \omega$ e $\omega + d = \omega$.

4.2 As Ações de RT_LOTOS

As ações de RT_LOTOS podem ser agrupadas em dois grandes conjuntos:

- as ações clássicas de LOTOS, a saber as *ações observáveis* pertencentes ao conjunto Act, a *ação interna* i e a *ação de término com sucesso* δ
- as ações específicas de RT_LOTOS que são *violações temporais* a^* que pertencem ao conjunto Act^*, sabendo que existe uma bijeção entre Act e Act^*.

RT_LOTOS permite temporizar as ações observáveis e também a ação interna. A ação δ e as violações temporais a^*, sendo devidas a ocorrências de operações especificadas na linguagem mas não sendo diretamente manipuláveis nesta, não podem ser temporizadas.

Os conjuntos de ações são definidos da seguinte maneira: $Act^i = Act \cup \{i\}$, $Act^\delta = Act \cup \{\delta\}$ e $Act^{i,\delta} = Act \cup \{i\} \cup \{\delta\}$.

Seja a uma ação pertencendo ao conjunto Act^i. RT_LOTOS permite temporizar uma tal ação escrevendo $[t_{min}, t_{max}]a$ com t_{min} e t_{max} ($t_{min} \leq t_{max}$) pertencendo ao domínio de tempo D^ω considerado.

t_{min}, é o limite inferior do intervalo de tempo, e caracteriza o retardo mínimo durante o qual a ação a deve ser apresentada (ou sensibilizada) antes de ser realmente oferecida a seu ambiente. A partir do cumprimento deste retardo, a ação pode se realizar durante um intervalo de tempo igual a $[0, t_{max} - t_{min}]$. No final deste intervalo de tempo o comportamento será diferente dependendo do tipo da ação (se observável a ou interna i). Se a é uma ação observável, a não ocorrência de a dentro do intervalo estabelecido provocará a realização de uma ação especial, a ação a^* caracterizando a violação do intervalo de tempo associado a a. De outra maneira, se a é a ação interna i, então a progressão do tempo é suspensa até a realização de i ou de uma outra oferecida no mesmo instante e que esteja em conflito com i como é no caso do operador de escolha.

Do ponto de vista semântico, constata-se que assim que as ações observáveis só podem realizar-se durante o intervalo de tempo que lhes é associado. Além disso, a ação i torna-se "*autônoma*" quando do expiração de seus intervalos de tempo. Como em outros modelos temporizados [12, 13], a ação δ não é urgente enquanto que uma violação temporal é autônoma por definição.

Além disso, e em conformidade com a semântica padrão de LOTOS, todas as ocorrências de ações são consideradas atômicas e instantâneas.

4.3 Semântica Operacional

A semântica operacional é apresentada no estilo SOS (*Structured Operational Semantics*) de Plotkin [18] e compreende:

- um conjunto de regras de inferência para as ações clássicas de RT-LOTOS
- um conjunto de regras de inferência para as violações temporais
- um conjunto de regras de inferência para a progressão do tempo

4.3.1 Notação

Doravante, para simplificar o texto, utilizaremos:

- $E \xrightarrow{a}$ significando que existe em E uma ação a pronta a se realizar.
- $E \not\xrightarrow{a}$ significando que não existe em E uma ação a que esteja pronta a se realizar.
- $[t]$ significando $[t,t]$ para $t \in D^{\omega}$
- i significando $[0,0]i$
- $a;E$ significando $[0,\omega]a;E$
- $E|||F$ significando $E|[\emptyset]|F$ (entrelaçamento total das ações)
- $E||F$ significando $E|[Act]|F$ (sincronização total das ações)
- $E < a]F$ denotando o caso particular de $E < a]\{a : F\}$

4.3.2 Regras Semânticas dos Operadores

As regras semânticas dos operadores de RT_LOTOS são apresentadas nas tabelas 1 e 2.

Na tabela 1, a regra In diz que o operador *stop* não bloqueia a progressão do tempo.

As regras Ter-1 e Ter-2 referem-se ao operador *exit* sendo que a última das duas regras expressa a não urgência da ação δ.

As regras com o prefixo Pre descrevem o comportamento do operador de prefixação ";". A regra Pre-1.a diz que uma ação a pode ser realizada durante toda a duração do intervalo temporal $[0,t]$; A regra Pre-1.b tem por objetivo exprimir uma violação temporal, denotada a^*, indicando que a ação a não pôde ser realizada dentro da restrição temporal imposta. O processo resultante torna-se *stop*, e no caso da necessidade de fazer sentir este fato dentro da especificação, essa violação temporal pode ser tratada por um mecanismo de exceção *ad hoc* através do operador $E < L]\{a_1 : Q_1, a_2 : Q_2, \cdots, a_n : Q_n\}$, onde $a \in L$. Observe-se ainda que a ação i pode também ser temporizada. Tão logo o intervalo de tempo associado com ela torna-se $[0,0]$, ela torna-se uma ação urgente; como conseqüência, não existe violação temporal associada com a ação i.

As regras com prefixo Esc descrevem o operador de escolha. A regra Esc-1.b estipula que se uma violação temporal afeta o processo E (i.e. E oferece a ação a^*), então esta violação temporal *não* resolve a escolha.

As regras com o prefixo Par descrevem o comportamento do operador de composição paralela dependendo se sincronizações podem ou não ocorrer, e dependendo da ocorrência de violações temporais. As regras Par-1.a tratam os casos de sincronização de ações e as Par-1.b tratam o caso do entrelaçamento das ações. A regra Par-2 define a progressão do tempo para este operador.

No final da tabela 1 tem-se ainda as regras Oc que definem a semântica do operador de Ocultação. Sobre as regras deste operador vale o seguinte comentário. Mesmo que

a regra Oc-2 imponha urgência na ocorrência das ações que são oferecidas, existe um não-determinismo entre a ocorrência de um a ou um a^* quando da especificação de uma expressão como $[t,t]a;E$. É para tratar situações como esta que as regras Oc-1.b.i e Oc-1.b.ii foram estabelecidas. Observe-se que a única possibilidade de ocorrência de um a^* acontece quando atribuímos um intervalo pontual, do tipo $[t,t]$, numa prefixação da ação a. Assim, as regras do Oc-1.b.i e Oc-1.b.ii tratam exclusivamente este caso. Em todas as outras situações a urgência imposta pela regra Oc-2 é mandatória, e as ações ocorrem tão logo elas sejam possíveis.

Na tabela 2, as regras com prefixo Seq estabelecem a semântica do operador de composição paralela. Vale o comentário seguinte. A regra Seq-2, que define a progressão do tempo, estabelece o único caso de urgência da ação δ. Ou seja, se a ação δ pode ocorrer num processo E, então ela ocorrerá imediatamente no processo $E \gg F$.

As regras do operador de preempção têm o prefixo Preem.

O operador de tratamento de violações temporais é descrito pelas regras iniciadas com PreemTem. Observa-se pela regra PreemTem-1.bi que a ocorrência de uma violação temporal a_j^* no processo "E", com $a_j \in L$, faz com que "$E < L]\{a_1 : Q_1, a_2 : Q_2, \cdots, a_n : Q_n\}$" torne-se, silenciosamente, o processo "Q_j" que estava associado a ação a_j. E pela regra PreemTem-1.b.ii tem-se que se uma ação $b \notin L$, então violações temporais b^* no processo "E" não provocam nenhuma transformação no processo "$E < L]\{a_1 : Q_1, a_2 : Q_2, \cdots, a_n : Q_n\}$".

Finalmente, concluindo a tabela 2 tem-se as regras Inst que descrevem o operador de instanciação de processos.

4.4 Bissimulações em RT_LOTOS

Nesta seção são definidas bissimulações temporais dentro do contexto de RT_LOTOS. Tendo em vista a hipótese feita sobre o domínio do tempo (ou seja, que o domínio do tempo é enumerável), o modelo subjacente é o usual Sistema de Transições Rotuladas (STR). No caso de tempo denso, o STR deverá ser infinito (número infinito de estados e ramificações); mas isto não caracteriza um problema para o enfoque deste trabalho, pois dá-se apenas o significado de bissimulações temporais e não propõem-se algoritmos para estas bissimulações.

4.4.1 Bissimulação Temporal Forte

A definição da bissimulação temporal forte corresponde à definição da bissimulação forte clássica, onde as violações temporais e os arcos temporizados de D^ω são considerados como ações quaisquer.

Definição 1 Seja $\mathcal{L} = Act^{i,\delta} \cup Act^* \cup D^\omega$ um conjunto de ações. Então, define-se a função $\mathcal{F}$, sobre subconjuntos de $\mathcal{E} \times \mathcal{E}$ (isto é, relações binárias sobre expressões de comportamento), como segue. Se $\mathcal{R} \subseteq \mathcal{E} \times \mathcal{E}$, então $(P,Q) \in \mathcal{F}(\mathcal{R})$ se, e somente se, para toda ação $a \in \mathcal{L}$:

1. sempre que $P \xrightarrow{a} P'$ então, para algum Q', $Q \xrightarrow{a} Q'$ e $(P',Q') \in \mathcal{R}$, e

In	$\frac{-}{stop \xrightarrow{t} stop}$ $(t \in D^{\omega})$
Ter-1	$\frac{-}{exit \xrightarrow{\delta} stop}$
Ter-2	$\frac{-}{exit \xrightarrow{t} exit}$ $(t \in D^{\omega})$
Pre-1.a	$\frac{-}{[0,t]a;E \xrightarrow{a} E}$ $(t \in D^{\omega})$ $(a \in Act^{i})$
Pre-1.b	$\frac{-}{[0,0]a;E \xrightarrow{a^{\bullet}} stop}$ $(a \in Act)$
Pre-2.a	$\frac{-}{[0,t+s]a;E \xrightarrow{s} [0,t]a;E}$ $(t,s \in D^{\omega}$ e $s>0)$ $(a \in Act^{i})$
Pre-2.b	$\frac{-}{[t_1+s,t_2+s]a;E \xrightarrow{s} [t_1,t_2]a;E}$ $(s,t_1,t_2 \in D^{\omega}$ e $s>0)$ $(a \in Act^{i})$
Esc-1.a	$\frac{E \xrightarrow{a} E'}{E[\,]F \xrightarrow{a} E' \quad F[\,]E \xrightarrow{a} E'}$ $(a \in Act^{i,\delta})$
Esc-1.b	$\frac{E \xrightarrow{a^{\bullet}} E'}{E[\,]F \xrightarrow{a^{\bullet}} E'[\,]F \quad F[\,]E \xrightarrow{a^{\bullet}} F[\,]E'}$ $(a \in Act)$
Esc-2	$\frac{E \xrightarrow{t} E', \quad F \xrightarrow{t} F'}{E[\,]F \xrightarrow{t} E'[\,]F'}$ $(t \in D^{\omega})$
Par-1.a.i	$\frac{E \xrightarrow{a} E', \; F \xrightarrow{a} F'}{E\|[L]\|F \xrightarrow{a} E'\|[L]\|F'}$ $(a \in L \cup \{\delta\})$
Par-1.a.ii.A	$\frac{E \xrightarrow{a^{\bullet}} E', \; F \xrightarrow{a^{\bullet}} F'}{E\|[L]\|F \xrightarrow{a^{\bullet}} E'\|[L]\|F'}$ $(a \in L)$
Par-1.a.ii.B	$\frac{(E \xrightarrow{a^{\bullet}} E') \wedge (F \not\xrightarrow{g} \vee F \not\xrightarrow{a^{\bullet}})}{E\|[L]\|F \xrightarrow{a^{\bullet}} E'\|[L]\|F \quad F\|[L]\|E \xrightarrow{a^{\bullet}} F\|[L]\|E'}$ $(a \in L)$
Par-1.b.i	$\frac{E \xrightarrow{a} E'}{E\|[L]\|F \xrightarrow{a} E'\|[L]\|F \quad F\|[L]\|E \xrightarrow{a} F\|[L]\|E'}$ $(\delta \neq a \notin L)$
Par-1.b.ii	$\frac{E \xrightarrow{a^{\bullet}} E'}{E\|[L]\|F \xrightarrow{a^{\bullet}} E'\|[L]\|F \quad F\|[L]\|E \xrightarrow{a^{\bullet}} F\|[L]\|E'}$ $(a \notin L)$
Par-2	$\frac{(E \xrightarrow{t} E' \wedge F \xrightarrow{t} F'), (\forall a \in L \;\; E \not\xrightarrow{a} \wedge F \not\xrightarrow{a})}{E\|[L]\|F \xrightarrow{t} E'\|[L]\|F'}$ $(t \in D^{\omega})$
Oc-1.a.i	$\frac{E \xrightarrow{a} E'}{\text{hide } L \text{ in } E \xrightarrow{a} \text{hide } L \text{ in } E'}$ $(a \notin L)$
Oc-1.a.ii	$\frac{E \xrightarrow{a} E'}{\text{hide } L \text{ in } E \xrightarrow{i} \text{hide } L \text{ in } E'}$ $(a \in L)$
Oc-1.b.i	$\frac{E \xrightarrow{a^{\bullet}} E'}{\text{hide } L \text{ in } E \xrightarrow{a^{\bullet}} \text{hide } L \text{ in } E'}$ $(a \notin L)$
Oc-1.b.ii	$\frac{E \xrightarrow{a^{\bullet}} E'}{\text{hide } L \text{ in } E \xrightarrow{i} \text{hide } L \text{ in } E'}$ $(a \in L)$
Oc-2	$\frac{E \xrightarrow{t} E', \; (\forall a \in L \;\; E \not\xrightarrow{g})}{\text{hide } L \text{ in } E \xrightarrow{t} \text{hide } L \text{ in } E'}$ $(t \in D^{\omega})$

Tabela 1: Semântica operacional de RT_LOTOS: parte I

Seq-1.a.i	$\frac{E \xrightarrow{a} E'}{E \gg F \xrightarrow{a} E' \gg F}$	$(a \in Act^{i})$
Seq-1.a.ii	$\frac{E \xrightarrow{\delta} E'}{E \gg F \xrightarrow{i} F}$	
Seq-1.b	$\frac{E \xrightarrow{a^*} E'}{E \gg F \xrightarrow{a^*} E' \gg F}$	$(a \in Act)$
Seq-2	$\frac{E \not\xrightarrow{\delta}, \; E \xrightarrow{t} E'}{E \gg F \xrightarrow{t} E' \gg F}$	$(t \in D^{\omega})$
Preem-1.a.i	$\frac{E \xrightarrow{a} E'}{E \,[\!> F \xrightarrow{a} E' \,[\!> F}$	$(a \in Act^{i})$
Preem-1.a.ii	$\frac{F \xrightarrow{a} F'}{E \,[\!> F \xrightarrow{a} F'}$	$(a \in Act^{i,\delta})$
Preem-1.a.iii	$\frac{E \xrightarrow{\delta} E'}{E \,[\!> F \xrightarrow{\delta} E'}$	
Preem-1.b.i	$\frac{F \xrightarrow{a^*} F'}{E \,[\!> F \xrightarrow{a^*} E \,[\!> F'}$	$(a \in Act)$
Preem-1.b.ii	$\frac{E \xrightarrow{a^*} E'}{E \,[\!> F \xrightarrow{a^*} E \,[\!> F}$	$(a \in Act)$
Preem-2	$\frac{E \xrightarrow{t} E', \; F \xrightarrow{t} F'}{E \,[\!> F \xrightarrow{t} E' \,[\!> F'}$	$(t \in D^{\delta})$
PreemTem-1.a	$\frac{E \xrightarrow{a} E'}{E \lhd L] \{a_1{:}Q_1, a_2{:}Q_2, \cdots, a_n{:}Q_n\} \xrightarrow{a} E' \lhd L] \{a_1{:}Q_1, a_2{:}Q_2, \cdots, a_n{:}Q_n\}}$	$(a \in Act^{i,\delta})$
PreemTem-1.b.i	$\frac{E \xrightarrow{a_j^*} E'}{E \lhd L] \{a_1{:}Q_1, a_2{:}Q_2, \cdots, a_n{:}Q_n\} \xrightarrow{i} Q_j}$	$(a_j \in L)$
PreemTem-1.b.ii	$\frac{E \xrightarrow{b^*} E'}{E \lhd L] \{a_1{:}Q_1, a_2{:}Q_2, \cdots, a_n{:}Q_n\} \xrightarrow{b^*} E' \lhd L] \{a_1{:}Q_1, a_2{:}Q_2, \cdots, a_n{:}Q_n\}}$	$(b \in Act - L)$
PreemTem-2	$\frac{E \xrightarrow{t} E'}{E \lhd L] \{a_1{:}Q_1, a_2{:}Q_2, \cdots, a_n{:}Q_n\} \xrightarrow{t} E' \lhd L] \{a_1{:}Q_1, a_2{:}Q_2, \cdots a_n{:}Q_n\}}$	$(t \in D^{\omega})$
Inst-1.a	$\frac{E[a_1/a'_1, \cdots, a_n/a'_n] \xrightarrow{a} E', \; P[a'_1, \cdots, a'_n] := E}{P[a_1, \cdots, a_n] \xrightarrow{a} E'}$	$(a \in Act^{i,\delta})$
Inst-1.b	$\frac{E[a_1/a'_1, \cdots, a_n/a'_n] \xrightarrow{a^*} E', \; P[a'_1, \cdots, a'_n] := E}{P[a_1, \cdots, a_n] \xrightarrow{a^*} E'}$	$(a \in Act)$
Inst-2	$\frac{E[a_1/a'_1, \cdots, a_n/a'_n] \xrightarrow{t} E', \; P[a'_1, \cdots, a'_n] := E}{P[a_1, \cdots, a_n] \xrightarrow{t} E'}$	$(t \in D^{\omega})$

Tabela 2: Semântica operacional de RT_LOTOS: parte II

2. sempre que $Q \xrightarrow{a} Q'$ então, para algum P', $P \xrightarrow{a} P'$ e $(P', Q') \in \mathcal{R}$

$\mathcal{R}$ é chamada uma bissimulação temporal forte se, e somente se, $\mathcal{R} \subseteq \mathcal{F}(\mathcal{R})$. Se $(P, Q) \in \mathcal{R}$ para alguma bissimulação temporal $\mathcal{R}$, então P e Q são ditos fortemente bissimilares temporais, em símbolos $P \sim_t Q$. Como usual, isto pode ser expresso como: $\sim_t = \bigcup\{\mathcal{R} : \mathcal{R}$ é uma bissimulação temporal forte$\}$. □

Proposição 1 Seja $\mathcal{L} = Act^{i,\delta} \cup Act^* \cup D^\omega$ e seja $\mathcal{R} \subseteq \mathcal{E} \times \mathcal{E}$ uma bissimulação temporal forte. Então $(P, Q) \in \mathcal{R}$ implica que:

1. sempre que $P \xrightarrow{a} P'$ então, para algum Q', $Q \xrightarrow{a} Q'$ e $(P', Q') \in \mathcal{R}$, e
2. sempre que $Q \xrightarrow{a} Q'$ então, para algum P', $P \xrightarrow{a} P'$ e $(P', Q') \in \mathcal{R}$

Prova: Por hipótese, $\mathcal{R}$ é uma bissimulação temporal forte, então $\mathcal{R} \subseteq \mathcal{F}(\mathcal{R})$ o que implica que $(P, Q) \in \mathcal{F}(\mathcal{R})$, logo, tem-se (1) e (2). □

Proposição 2 A Relação $\sim_t$ tem as seguintes propriedades:

1. $\sim_t$ é a maior bissimulação temporal forte
2. $\sim_t$ é uma relação de equivalência

Prova: A demonstração da proposição acima é completamente similar à demonstração de propriedades equivalentes realizadas em [Milner 89], pp. 90-91. □

Proposição 3 A equivalência temporal forte é substitutiva sob todos os operadores RT_LOTOS. Em outras palavras, sejam P_1, P_2, Q, e $Q_1, \cdots, Q_n$ expressões de comportamento e $P_1 \sim_t P_2$. Então

(1) $[t_1, t_2]a; P_1 \sim_t [t_1, t_2]a; P_2$
(2) $P_1[]Q \sim_t P_2[]Q$
(3) $P_1|[L]|Q \sim_t P_2|[L]|Q$
(4) $hideLinP_1 \sim_t hideLinP_2$
(5) $P_1 >> Q \sim_t P_2 >> Q$
(6) $P_1 [> Q \sim_t P_2 [> Q$
(7) $P_1 < L] \{a_1 : Q_1, \cdots, a_n : Q_n\} \sim_t P_2 < L] \{a_1 : Q_1, \cdots, a_n : Q_n\}$

Prova: A prova de (7) é dada a seguir, os outros itens podem ser provados de maneira semelhante.

Seja $\mathcal{S} = \{(P_1 < L] \{a_1 : Q_1, \cdots, a_n : Q_n\}, P_2 < L] \{a_1 : Q_1, \cdots, a_n : Q_n\}) : P_1 \sim P_2\}$. Serão discutidos os seguintes casos:

1. $P_1 \xrightarrow{a} P'_1$ tal que $a \in D^\omega \cup Act^{i,\delta}$:
   como $P_1 \sim_t P_2$, então existe uma derivação $P_2 \xrightarrow{a} P'_2$ tal que $P'_1 \sim_t P'_2$. Também, as regras de transição implicam que
   $P_1 < L] \{a_1 : Q_1, \cdots, a_n : Q_n\} \xrightarrow{a} P'_1 < L] \{a_1 : Q_1, \cdots, a_n : Q_n\}$ e
   $P_2 < L] \{a_1 : Q_1, \cdots, a_n : Q_n\} \xrightarrow{a} P'_2 < L] \{a_1 : Q_1, \cdots, a_n : Q_n\}$, e assim
   $(P'_1 < L] \{a_1 : Q_1, \cdots, a_n : Q_n\}, P'_2 < L] \{a_1 : Q_1, \cdots, a_n : Q_n\}) \in \mathcal{S}$.

2. $P_1 \xrightarrow{a^*} P'_1$, como $P_1 \sim_t P_2$, então existe uma derivação $P_2 \xrightarrow{a^*} P'_2$ tal que $P'_1 \sim_t P'_2$. Existem dois casos:

   (a) $a^* \notin L$, e então tem-se as derivações:
   $P_1 < L]\,\{a_1{:}Q_1, \cdots, a_n{:}Q_n\} \xrightarrow{a^*} P'_1 < L]\,\{a_1{:}Q_1, \cdots, a_n{:}Q_n\}$ e
   $P_2 < L]\,\{a_1{:}Q_1, \cdots, a_n{:}Q_n\} \xrightarrow{a^*} P'_2 < L]\,\{a_1{:}Q_1, \cdots, a_n{:}Q_n\}$, e tem-se
   $(P'_1 < L]\,\{a_1{:}Q_1, \cdots, a_n{:}Q_n\}, P'_2 < L]\,\{a_1{:}Q_1, \cdots, a_n{:}Q_n\}) \in \mathcal{S}$

   (b) $a^* \in L$, com $a^* = a_k^*$ para algum $k \in \{1, \cdots, n\}$, e então tem-se as derivações:
   $P_1 < L]\,\{a_1{:}Q_1, \cdots, a_n{:}Q_n\} \xrightarrow{i} Q_k$ e $P_2 < L]\,\{a_1{:}Q_1, \cdots, a_n{:}Q_n\} \xrightarrow{i} Q_k$ que satisfaz o requisito.

Por um argumento simétrico, completa-se a prova de que $\mathcal{S}$ é uma bissimulação temporal forte. □

4.4.2 Bissimulação Temporal Direta

Poder-se-ia definir também uma bissimulação temporal fraca que correspondesse à definição de bissimulação fraca clássica, em que violações temporais e os arcos temporizados de D^ω são considerados como ações quaisquer. As definições, proposições e provas seriam similares às clássicas (e só não serão apresentadas aqui por restrição de espaço). Entretanto, nos parece mais interessante por permitir observar a progressão do tempo e a realização de ações que ocorrem satisfazendo suas restrições de tempo definir a bissimulação temporal direta que corresponde à definição de bissimulação fraca clássica, onde os arcos temporizados de D^ω são considerados como ações quaisquer, e as violações temporais são consideradas como ações internas i. Utiliza-se o termo bissimulação temporal direta, denotado por $\overset{*}{\approx}$, pois esta bissimulação se abstrai das violações temporais, não existindo conseqüentemente mais notificações de que não ocorrem dentro de seus respectivos intervalos de tempo.

Definição 2 Define-se a relação de transição $\rightsquigarrow \subset \mathcal{E} \times \mathcal{E}$ como:

1. $E \overset{a}{\rightsquigarrow} F$ se, e somente se $E(\xrightarrow{\rho})^* \xrightarrow{a} (\xrightarrow{\rho})^* F$, onde $(\xrightarrow{\rho})^*$ representa zero ou mais ocorrências da transição $(\xrightarrow{\rho})$, $a \in Act$ e $\rho \in Act^* \cup \{i\}$.

2. $E \overset{d}{\rightsquigarrow} F$ se, e somente se $E(\xrightarrow{\rho})^* \xrightarrow{d_1} (\xrightarrow{\rho})^* F \cdots (\xrightarrow{\rho})^* \xrightarrow{d_n} (\xrightarrow{\rho})^*$, onde $d_i \in D^\omega$ para $i \leq n$, $d = \sum_{i \leq n} d_i$ e $\rho \in Act^* \cup \{i\}$. □

Seja $\mathcal{L}^\circ = Act^\delta \cup D^\omega \cup \{\varepsilon\}$ e considere $\rightsquigarrow$, então obtém-se um sistema de transições rotuladas padrão:

$$\langle \mathcal{E}, \mathcal{L}^\circ, \{\overset{a}{\rightsquigarrow} : a \in \mathcal{L}^\circ\} \rangle.$$

Sob este sistema pode-se estabelecer a noção de equivalência temporal direta.

Definição 3 Seja $\mathcal{L}^\circ = Act^\delta \cup D^\omega \cup \{\varepsilon\}$ o conjunto de ações. Então, define-se a função $\mathcal{F}^\circ$, sobre subconjuntos de $\mathcal{E} \times \mathcal{E}$ (isto é, relações binárias sobre expressões de comportamento), como segue. Se $\mathcal{R} \subseteq \mathcal{E} \times \mathcal{E}$, então $(P, Q) \in \mathcal{F}^\circ(\mathcal{R})$ se, e somente se, para toda ação $a \in \mathcal{L}^\circ$:

1. sempre que $P \xrightarrow{a} P'$ então, para algum Q', $Q \overset{a}{\rightsquigarrow} Q'$ e $(P', Q') \in \mathcal{R}$, e

2. sempre que $Q \xrightarrow{a} Q'$ então, para algum P', $P \overset{a}{\rightsquigarrow} P'$ e $(P', Q') \in \mathcal{R}$

$\mathcal{R}$ é chamada uma bissimulação temporal fraca se, e somente se, $\mathcal{R} \subseteq \mathcal{F}^{\circ}(\mathcal{R})$. Se $(P, Q) \in \mathcal{R}$ para alguma bissimulação temporal fraca $\mathcal{R}$, então P e Q são ditos fracamente bissimilares temporais, em símbolos $P \dot{\approx}_t Q$. Como usual, isto pode ser expresso como: $\dot{\approx}_t = \bigcup\{\mathcal{R} : \mathcal{R}$ é uma bissimulação temporal direta$\}$. □

Proposição 4 Seja $\mathcal{L}^{\circ} = Act^{\delta} \cup Act^{c} \cup D^{\omega} \cup \{\epsilon\}$ e seja $\mathcal{R} \subseteq \mathcal{E} \times \mathcal{E}$ uma bissimulação temporal direta. Então $\langle P, Q \rangle \in \mathcal{R}$ implica que:

1. sempre que $P \xrightarrow{a} P'$ então, para algum Q', $Q \overset{a}{\rightsquigarrow} Q'$ e $(P', Q') \in \mathcal{R}$, e

2. sempre que $Q \xrightarrow{a} Q'$ então, para algum P', $P \overset{a}{\rightsquigarrow} P'$ e $(P', Q') \in \mathcal{R}$

Prova: Por hipótese, $\mathcal{R}$ é uma bissimulação temporal fraca, então $\mathcal{R} \subseteq \mathcal{F}^{\circ}(\mathcal{R})$ o que implica que $(P, Q) \in \mathcal{F}^{\circ}(\mathcal{R})$, logo, tem-se (1) e (2). □

Proposição 5 Dadas as relações binárias R, R_1 and R_2, então sejam:

$R^{-1} = \{(Q, P) : (P, Q) \in R\}$

$R_1 R_2 = \{(P, S) :$ para algum $Q, (P, Q) \in R_1$ e $(Q, S) \in R_2\}$.

Assuma que cada R_i $(i = 1, 2, \cdots)$ é uma bissimulação temporal direta. Então todas as seguintes relações também são bissimulações temporais diretas.

(1) $Id_{\mathcal{E}}$ (3) $R_1 R_2$

(2) R_i^{-1} (4) $\bigcup_{i \in I} R_i$

Prova: (1), (2) e (4) são óbvios, prova-se (3).

Seja $(P, S) \in R_1 R_2$, então para algum Q tem-se $(P, Q) \in R_1$ e $(Q, S) \in R_2$.

Agora seja $P \overset{a}{\rightsquigarrow} P'$. Então para algum Q' tem-se que $Q \overset{a}{\rightsquigarrow} Q'$ e $(P', Q') \in R_1$, pois $(P, Q) \in R_1$.

Também como $(Q, S) \in R_2$ tem-se, para algum S', que $S \overset{a}{\rightsquigarrow} S'$.

Assim, $(P', S') \in R_1 R_2$. Similarmente, se $S \overset{a}{\rightsquigarrow} S'$, pode-se encontrar P' tal que $P \overset{a}{\rightsquigarrow} P'$ e $(P', S') \in R_1 R_2$. □

Proposição 6 A relação $\dot{\approx}_t$ tem as seguintes propriedades:

1. $\dot{\approx}_t$ é a maior bissimulação temporal direta

2. $\dot{\approx}_t$ é uma relação de equivalência

Prova: (1) segue diretamente da definição 3 e da proposição 4, e (2) deriva diretamente da proposição 5. □

Para ilustrar a bissimulação temporal direta, considere-se o exemplo seguinte:

```
E = [p-d,p+d]a; stop ||| [p,p]i;E
F = ([p-d,p+d]a; stop <a] {a:(i;stop)} ||| [p,p]i;F
```

Os processos E e F estão em bissimulação temporal direta, mas não em estão em bissimulação temporal fraca. Isto deve-se ao fato de que o processo F transforma a ocorrência da violação temporal a^* em uma ação interna i.

Abstraindo-se dos arcos temporizados de D^ω e da ação interna i, pode-se definir ainda o conceito de bissimulação fraca que considera unicamente as ações observáveis. A definição da bissimulação fraca no contexto de RT_LOTOS tem como maior interesse a utilização desta linguagem formal em situações onde o tempo não afeta a correção do sistema. Visto que RT_LOTOS é uma extensão direta de LOTOS Básico, a bissimulação fraca também pode ser usada para inferir propriedades deste modelo.

Com a apresentação d as bissimulações acima fica então completamente definida a álgebra de processos temporizada RT_LOTOS.

5 Discussão sobre as representações das restrições temporais básicas em RT_LOTOS

Nesta seção, discutiremos as principais características de RT_LOTOS do ponto de vista temporal, destacando a expressividade, facilidade de uso e alto poder intuitivo e simplificador das escolhas feitas pelos autores e dos operadores subseqüentes introduzidos no modelo LOTOS. Algumas operações temporais (delay, timeout, watchdogs, periodicidade) exemplificarão estas características. A seguir, apresentaremos alguns exemplos de comportamentos e situações que são de grande interesse em sistemas tempo real críticos e outros sistemas dependentes do tempo como por exemplo os sistemas multimídia, e mostraremos como RT_LOTOS pode representar tais situações.

5.1 Operações básicas

Restrição de Tempo Em RT_LOTOS, a imposição de restrições temporais às ocorrências de ações é feita de maneira clara e direta pela simples atribuição de um intervalo de tempo a uma ação, da forma "$[t_{min}, t_{max}]a$". A ação só poderá ocorrer depois de ser retardada durante t_{min} unidades de tempo e antes de expirar o tempo máximo t_{max} no qual ela poderia se realizar. Entretanto, não há nenhuma exigência da ação a ter que ocorrer dentro daquele intervalo.

Violação temporal A ocorrência da ação temporizada $[t_{min}, t_{max}]a$ depende sempre do ambiente e este pode não estar apto a realizá-la dentro do intervalo. Neste caso, a ação a não ocorrerá, sendo violada a restrição de tempo imposta a ação. Um evento que sinaliza a ocorrência de tal violação de tempo faz parte da semântica de RT_LOTOS. O tratamento das violações de tempo é facultativa podendo ser realizada pelo operador de tratamento de exceções temporais discutido abaixo.

Tratamento de exceção temporal RT_LOTOS possui um poderoso operador de tratamento de exceções temporais, que permite tratar com modularidade e simplicidade os eventos relacionados à não ocorrência, dentro dos intervalos estabelecidos, de ações em um processo. O operador de tratamento de exceções temporais (ou preempção temporal) pode ser considerado como um processo supervisor de alto nível que, a cada instante, está apto a detectar a ocorrência de uma violação temporal e tratá-la imediatamente através da desabilitação do processo que a gerou, e a inicial-

ização de um processo específico para tratamento desta.

Retardo ("delay") Um retardo de $t \in D^{\omega}$ unidades de tempo imposto a um processo P pode ser representado por:

```
Q:=[t]i;P
```

Processo periódico Sejam Q um processo e $t \in D^{\omega}$ uma quantidade de tempo, então um processo P que representa o lançamento do processo Q a cada período de tempo t pode ser representado por:

```
P:=Q|||[t]i;P
```

Timeout Sejam P e Q dois comportamentos, e $t \in D^{\omega}$. Então, um *timeout* é um mecanismo dependente do tempo que se comporta como P, se uma ação inicial de P ocorre até o instante t, ou como Q após o tempo t. No nosso modelo, um mecanismo de *timeout* pode ser modelado como:

```
P [] [t]i;Q
```

O modelo RT_LOTOS também permite representar um mecanismo que trata timeouts diferentes em um conjunto de ações particulares dentro de um processo arbitrário. Como exemplo, seja a uma ação especificada (em possivelmente diferentes pontos) de um processo P com intervalo(s) de tempo do tipo $[t_{min}, t_{max}]$, com $t_{max} < \infty$ e seja Q um outro comportamento (um tratador de exceções, por exemplo). Então, o processo

```
P <a] {a:Q }
```

comporta-se como P se nenhuma ação de violação temporal a^* ocorrer durante a realização neste processo. No caso da ocorrência de uma violação temporal a^* (isto é, a não realização de a dentro do(s) intervalo(s) de tempo associado(s) a ela), então o processo P é descontinuado e o processo Q é iniciado.

Watchdog Em RT_LOTOS um mecanismo de *watchdog* pode ser modelado utilizando o operador de preempção, da maneira que segue:

```
P [> [t]i;Q
```

onde P e Q representam respectivamente o comportamento normal e o de exceção e $t \in D^{\omega}$. O processo resultante se comporta como P até o instante t, após o que P é abortado, e Q é iniciado.

5.2 Alguns exemplos simples de aplicação

Uma situação hipotética em um Sistema Tempo-Real: Considere-se um processo P de um sistema tempo-real em que uma dada ação a seja considerada imprescindível e devendo satisfazer restrições de tempo do tipo $[t_{min}, t_{max}]$ em cada uma das suas ocorrências no processo. Deseja-se representar o seguinte comportamento: uma eventual não realização da ação a por violação da restrição de tempo no processo P deve provocar a realização das três etapas seguintes:

1. a instância do processo P, em execução, deve ser abortada,
2. um processo de recuperação Q deve ser lançado, e em seguida
3. uma outra instância do processo P deve ter início.

De forma genérica, a especificação de um tal comportamento em RT_LOTOS pode ser facilmente representada por:

```
P <a] {a:(Q >> P)}
```

Assim, na primeira vez que ocorrer uma violação temporal (ação a^*) no processo P o processo "`(Q >> P)`" será iniciado. No caso da não ocorrência de a^* em P o processo "`(Q >> P)`" nunca terá inicio, e se P terminar, então o processo "`P <a] {a:(Q >> P)}`" terminará também.

Fluxo periódico com "*jitter*": Deseja-se especificar um fluxo periódico infinito com *jitter* (neste exemplo não são considerados derivas permanentes oriundas de atrasos), sendo que a ação a representa a unidade de informação do fluxo [20].

Um tal fluxo periódico de período p com jitter d ($d < \frac{p}{2}$) pode ser especificado pelo seguinte processo:

```
fluxo := [p-d,p+d]a;stop ||| [p]i;fluxo
```

A recursão define a repetição do processo *fluxo* a cada p unidades de tempo pois a ação interna i é urgente após o retardo de p unidades de tempo. Por outro lado, a ação a pode ocorrer em qualquer tempo dentro do intervalo $[p-d, p+d]$, que caracteriza o "jitter" associado a ocorrência de uma instância de uma unidade de informação. A não ocorrência da ação a dentro deste intervalo induz a ocorrência da violação temporal a^* no final do intervalo. Como consequência ainda, ocorrências de a^* caracterizam perdas de unidades de informação que podem ser tratadas num nível superior.

Fluxo com relações de dependência entre unidades de informação: Deseja-se agora especificar um fluxo onde são definidas certas relações de dependência entre unidades de informação. Este tipo de abordagem é usado em geral quando considera-se um fluxo de vídeo compactado. Neste caso, um *frame* veicula as informações que caracterizam as modificações de uma imagem com relação a uma imagem de referência. Numa tal situação, pode ser útil evitar de entregar *frames* que dependam de *frames* de referência que não puderam ter sido encaminhados previamente.

Uma especificação de alto-nível de um tal fluxo de vídeo pode ser expressa em RT_LOTOS pelo processo `video` no qual faz-se a hipótese de que a ação `m` modela um *frame* de referência (*master frame*) e que as ações `a` e `b` caracterizam *frames* que dependem do *frame* de referência.

```
video := [t]m;[t]a;[t]b;video <m] [2t]i;video
```

Se deseja-se ocultar a ocorrência das violações temporais associadas às ações `a` e `b`, o processo `video` pode ser especificado da seguinte maneira:

```
video := (([t]m;[t]a;[t]b;video <m] [2t]i;video) <a] [t]b;video) <b] video)
```

6 Verificação de sistemas tempo-real

Nesta seção apresentaremos de maneira informal alguns importantes aspectos relacionados à verificação de sistemas tempo-real. Após ter apresentado as diferentes técnicas de verificação em sistemas que não dependem do tempo, abordaremos as dificuldades de tratamento do tempo em técnicas convencionais, as potencialidades de algumas técnicas emergentes de verificação de sistemas tempo-real e a sua relação com o modelo RT_LOTOS.

As técnicas de verificação são geralmente divididas em técnicas de verificação de equivalências e de verificação de modelos.

As técnicas de verificação fundadas em equivalências são baseadas no confronto de duas especificações do sistema a verificar: uma primeira descrevendo os detalhes de realização dos procedimentos necessários para realizar um objetivo; e uma segunda, mais simples, que descreve um comportamento mais abstrato do objetivo a realizar. Os Sistemas de Transições Rotuladas das duas especificações são então testadas para determinar se os comportamentos são equivalentes.

Verificação de modelos ("*model-checking*") é um método de verificação de sistemas concorrentes em que fórmulas de uma lógica devem ser provadas ou não sobre um modelo de um modelo de grafos de estados do comportamento do sistema. Nestas técnicas dois modelos diferentes são usados em geral. Um primeiro modelo é usado para descrever o sistema como modelo de especificação (em geral usam-se máquinas de estados finitos, redes de Petri, ou autômatos). Deste modelo são gerados grafos que representam os estados alcançáveis pelo sistema. O segundo modelo é uma lógica (modal, em geral) que permite expressar asserções sobre propriedades do sistema que podem ser provadas ou refutadas (Por exemplo, em [8], Cavalli e Horn utilizam verificação de modelos de uma lógica temporal em máquinas de estados finitos como técnica de verificação).

A aplicação dessas técnicas num contexto onde o tempo intervém direta e explicitamente não é trivial. Como já foi comentado na seção 4, a representação de sistemas dependentes do tempo em Sistemas de Transições Rotuladas implica em adicionar um número muito elevado de transições para denotar a progressão do tempo. Por exemplo, para representar um mecanismo de timeout onde o tempo de espera é de 2 unidades de tempo (ex.: a;E[][2]i;F), teríamos que ter três ramificações representando as possibilidades de realização de a nos instantes 0,1 e 2 no caso do domínio de tempo ser o dos números naturais; ou teríamos um número infinito de ramificações para representar as possibilidades de ocorrência de a transições de progressão do tempo caso o domínio de tempo fosse o dos números racionais positivos. Este exemplo mostra a possibilidade de crescimento elevada, com relação ao número de estados, que a introdução do tempo provoca nos Sistemas de Transições Rotuladas, sobretudo quando deseja-se utilizar um modelo de tempo denso.

A partir da discussão acima, pode-se concluir que, pelo menos com as técnicas atuais, técnicas de verificação baseadas em Sistemas de Transições Rotuladas não são, em geral, de grande utilidade para tratamento de sistemas dependentes do tempo. Em particular, apesar da sua importância na definição completa de uma Álgebra de Processo Temporizada as bissimulações com tempo que podem ser definidas para uma álgebra de processos temporizadas parecem difíceis de serem verificadas quando

o domínio de tempo for denso.

Contudo, a problemática de verificação para tempo real não é recente e outras técnicas de verificação para este tipo de sistemas são descritas na bibliografia. Em particular, as técnicas de verificação baseadas em grafos e autômatos temporizados descritas em [1] e [2] têm um importância diferenciada no contexto de RT_LOTOS; isto é, ambas as técnicas são fundadas em modelos próximos e foi mostrado que é possível transladar álgebras de processos temporizadas para estes modelos [17].

A técnica descrita em [1] baseia-se na utilização de algoritmos de *model checking* num contexto de tempo real e os autores combinam o uso da lógica temporal tempo-real TCTL e o modelo de grafos temporizados. Já a técnica apresentada em [2] é centrada na utilização de algoritmos de verificação da inclusão de ω-linguagens, e os autores combinam o uso de autômatos temporizados (extensões temporizadas dos autômatos de Büchi e Muller) e algoritmos e propriedades de inclusão de ω-linguagens aceitas por esses.

A utilização desse tipo de abordagem como técnica de verificação de sistemas tempo real nos parece promissora e com o objetivo de tornar possível a utilização destas técnicas a partir de especificações em RT_LOTOS, já se definiu uma translação da semântica de RT_LOTOS no modelo de grafos temporizados [7]. Estudos de aplicações desta técnica de verificação estão sendo realizados.

7 Comentários finais e perspectivas

Neste artigo foi apresentada uma extensão temporal da técnica de descrição formal LOTOS, RT_LOTOS. Outra propostas similares, T-LOTOS [4] de Bolognesi e Lucidi e Timed LOTOS [13] de Leduc e Léonard vem sendo desenvolvidas nestes últimos anos. Em particular, o debate entre T-LOTOS e Timed LOTOS gerou toda uma discussão sobre a urgência ou a ausência de urgência que é necessário associar à realização das ações observáveis. Nossa proposição foi em grande parte inspirada por esse debate, tomando como ponto de partida o fato de que as ações observáveis temporizadas não são urgentes (como em Timed LOTOS), mas que não poderiam também serem oferecidas eternamente como em Timed LOTOS. Daí surgiu a idéia de introduzir o conceito de violação temporal que conduziu naturalmente ao novo operador de preempção temporal dando desta forma o caráter tempo real à linguagem. Em seguida associou-se restrições de tempo às ações, como em TIC-LOTOS [19] de Quemada e Azcorra, ao invés de introduzir um operador de retardo (*delay*)como em Timed LOTOS. Esta é a intuição de base que reveste a abordagem proposta que, de um ponto de vista conceitual, parece estar mais próximo de Timed LOTOS que de T-LOTOS. Em particular, como em Timed LOTOS, a única hipótese que foi feita sobre o domínio de tempo é que ele seja enumerável. As diferenças essenciais entre RT_LOTOS e Timed LOTOS são:

- intervalos de tempo são associados diretamente às ações ao invés do operador de retardo Δ de Timed LOTOS, o que permite evitar a introdução na semântica de uma ação suplementar θ como em Timed LOTOS
- a caracterização de violações temporais em RT_LOTOS, as quais podem ser observadas em níveis mais altos da especificação (se elas não forem ocultadas) ou

tratadas explicitamente pelo operador de preempção temporal; como mostrado em alguns exemplos anteriores, o conceito de violação temporal permite obter especificações simples quando restrições de tempo-real devem ser cumpridas.

- a possibilidade de temporizar a ação interna em RT_LOTOS, preservando sua característica de urgência uma vez que seu intervalo temporal chegue ao fim.

Os resultados apresentados neste artigo são uma evolução natural de três outros trabalhos dos autores que introduziram o modelo RT_LOTOS [6, 9, 10]. Entre outras diferenças com as versões anteriores, o presente artigo não mais atribui distribuições de probabilidade aos intervalos das ações como em [6] e, em relação aos dois últimos, é modificada a semântica dos operadores de prefixação e de preempção temporal, tornando-os mais intuitivos e gerais, e introduzidas as relações de bissimulação de comportamento.

Recentemente, Leduc e Léonard apresentaram uma nova versão do modelo Timed LOTOS [14] que difere substancialmente da anterior. Esta nova versão introduz no modelo ações temporizadas (análogo à RT_LOTOS) e elimina o operador de retardo Δ, entre outras características, mostrando a justeza das escolhas feitas na nossa proposta.

Muitas são as perspectivas de continuação do presente trabalho. Por exemplo, do ponto de vista formal nos parece interessante o estudo do modelo RT_LOTOS sem a hipótese de atomicidade das ações; isto é, atribuindo durações às ações. Isto é possível através da redefinição da semântica do modelo dentro de um contexto de paralelismo verdadeiro, como por exemplo a semântica de causalidade [11]. Um estudo de RT_LOTOS dentro deste contexto tem sido realizado pelos autores. Do ponto de vista prático, outra perspectiva muito interessante e próxima é a utilização das técnicas de verificação descritas em [1] E [2] tendo RT_LOTOS como linguagem de especificação, e como já foi dito no final da seção anterior, esta abordagem vem sendo estudada pelos autores.

Referências

[1] Alur, R.; Courcoubetis, C. e Dill, D., *Model Checking for Real-Time Systems*. In Proceedings of the Fifth IEEE Symposium on Logic in Computer Science, 1990.

[2] Alur, R. e Dill, D., *The Theory of Timed Automata*. In Proceedings of REX Workshop "Real time: Theory in Pratice", LNCS 600, 1992.

[3] Bolognesi, T. e Brinksma, Ed. *Introduction to the ISO Specification Language LOTOS*, Computer Networks and ISDN Systems (NORTH-HOLLAND), No. 14, 1987, pp. 25-59.

[4] Bolognesi, T. e Lucidi, F. , *LOTOS-Like Process Algebras with Urgent or Timed Interactions*. In Proccedings of the IFIP TC6/WG6.1 4th International Conference on Formal Description Techniques, FORTE'91, North-Holland, 1992.

[5] Bolognesi, T. e Lucidi, F. , *Timed Process Algebras with Urgent Interactions and a Unique Powerful Binary Operator*. In Proceedings of REX Workshop "Real time: Theory in Pratice", LNCS 600.

[6] Camargo, M. S. de; Farines, J.-M., *Uma Variante do Modelo LOTOS Básico com Tempo Estocástico para Especificação e Avaliação de Desempenho em Sistemas*

Distribuídos Dependentes do Tempo", anais do 10 Simpósio Brasileiro de Redes de Computadores, Recife, Abril, 1992, pp. 192-207.

[7] Camargo, M.S. de; Farines, J.-M., *A Translação de RT_LOTOS para o Modelo de Grafos Temporizados: uma Abordagem para Verificação de Sistemas Tempo Real*, Relatório Técnico RT 93-31, LCMI-UFSC, Florianópolis, Dezembro, 1993.

[8] Cavalli, A.R. e Horn, F, *Proof of Specification Properties by Using Finite State Machines and Temporal Logic*, Em IFIP - Protocol Specification, Testing, and Verification Proceedings, H. Rudin e C.H. West (eds), 1987.

[9] Courtiat, J.P. and De Camargo, M.S. and Saïdouni, D.E *RT_LOTOS: A Time Extension of LOTOS for the Specification of Real-Time Systems*, LAAS Report 93158, May 1993, submitted for publication.

[10] Courtiat, J.P. and De Camargo, M.S. and Saïdouni, D.E, *RT_LOTOS: LOTOS Temporisé pour la Spécification de Systèmes Temps Réel* , actes du congrés CFIP'93, Montréal, Canadá, Setembro 1993.

[11] Coelho Da Costa, R. da, e Courtiat, J.P. *A true concurrency semantics for LOTOS*, In Proceedings of the IFIP TC6/WG6.1 5th Int. Conf. on Formal Description Techniques -FORTE'92-, North-Holland, 1992.

[12] *LOTOS, A Formal Description Technique Based on the Ordering of Observational Behaviour*, ISO IS 8807, Novembre, 1988.

[13] Leduc, G. e Léonard, L. *A Timed LOTOS Supporting a Dense Time Domain and Including New Timed Operators*, In Proccedings of the IFIP TC6/WG6.1 5th International Conference on Formal Description Techniques, FORTE'92, North-Holland, 1993.

[14] Leduc, G. e Léonard, L. *Comment rendre LOTOS apte à spécifier des systèmes temps réel?*, actes du congrés CFIP'93, Montréal, Canadá, Setembro 1993.

[15] R Milner, *Communication and Concurrency*, C.A.R Hoare Series Editor, Prentice Hall, 1989.

[16] Nicollin, X. e Sifakis, J., *An Overview and Syntesis on Timed Process Algebras*, In Proceedings of REX Workshop "Real time: Theory in Pratice", LNCS 600, 1992.

[17] Nicollin, X. e Sifakis, J. e Yovine, S., *From ATP to Timed Graphs and Hybrid Systems*, In Proceedings of REX Workshop "Real time: Theory in Pratice", LNCS 600, 1992.

[18] Plotkin, G.D., *A Structural Approach to Operational Semantics*, Report DAIMI-FN19, Computer Science Dept., Århus University, Dinamarca, 1981.

[19] Quemada, J, e Azcorra, A, and Frutos, D., *A Timed Calculus for LOTOS*, In Proccedings of the IFIP TC6/WG6.1 2nd International Conference on Formal Description Techniques, FORTE'89, North-Holland, 1990.

[20] Carmo, L. F. R. C e de Saqui, P, e Courtiat, J. P. *Basic Synchronization Concepts in Multimedia Systems*, 3rd International Workshop on Network and Operating System Support for Digital Audio and Video, San Diego, November 92.