CONCORRÊNCIA E SINCRONIZAÇÃO PARA LÓGICA DINÂMICA DE PROCESSOS

Vera Lúcia Prudência dos Santos

TESE SUBMETIDA AO CORPO DOCENTE DA COORDENAÇÃO DOS PROGRAMAS DE PÓS-GRADUAÇÃO DE ENGENHARIA DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE DOUTOR EM CIÊNCIAS EM ENGENHARIA DE SISTEMAS E COMPUTAÇÃO.

Aprovada por:

Prof. Mário Roberto Folhadela Benevides, Ph.D.

Prof. Edward Hermann Haeusler, D.Sc.

Prof. Fábio Protti, D.Sc.

Prof. Ruy José Guerra Barreto de Queiroz, Ph.D.

Profa. Sheila Regina Murgel Veloso, D.Sc.

RIO DE JANEIRO, RJ – BRASIL

ABRIL DE 2005

SANTOS, VERA LÚCIA PRUDÊNCIA DOS

Concorrência e Sincronização para Lógica Dinâmica de Processos [Rio de Janeiro] 2005

XI, 165p. 29,7 cm (COPPE/UFRJ, D.Sc., Engenharia de Sistemas e Computacão, 2005)

Tese – Universidade Federal do Rio de Janeiro, COPPE

1 - CCS

2 - Lógica Modal

3 - Lógica Dinâmica Proposicional

4 - Lógica para CCS

5 - Lógica Dinâmica de Concorrência

I. COPPE/UFRJ II. Título (série)

À Deus.

Agradecimentos

Ao professor Mário Benevides pela orientação, pelas sugestões, ensinamentos, pelo apoio e confiança na execução deste trabalho.

Aos professores membros da banca examinadora.

Ao meu esposo Adriano, pelo amor que sempre me dedicou, pela paciência e por compreender os momentos de ausência e de ansiedade.

Ao meu irmão Luciano pela ajuda sempre que precisei.

Aos meus pais, João e Helena, e as minhas irmãs, Eliana, Kall e Marcela pelo carinho e pela força que sempre me deram.

Aos amigos da COPPE: Daniele, Gilvan, Rodrigo, Alfredo, Jurandir, Geci, Roseli, Paulinho, Renata, Elder, por estarem sempre presentes.

Aos funcionários do programa de Engenharia de Sistemas e Computação, em especial Solange, Cláudia Prata, Lúcia, Sueli, Lourdes, Julinho e Dona Gersina (in memorian).

Aos meus padrinhos do Rio, Guaraci e Hildete, pelo apoio que me deram sempre que precisei.

Aos amigos distantes, em especial Zane, Cristóvão, Haroldo, Rita, Vadeci, Valnir, Valcir e Aninha.

Ao CNPq, pelo suporte financeiro.

" ... por isso sigo caminhando, sempre em frente,

incansável, na certeza de ir até

onde Deus disser: É até aqui. "

José Rodrigues Lustoza

Resumo da Tese apresentada à COPPE/UFRJ como parte dos requisitos necessários para a obtenção do grau de Doutor em Ciências (D.Sc.)

CONCORRÊNCIA E SINCRONIZAÇÃO PARA LÓGICA DINÂMICA DE PROCESSOS

Vera Lúcia Prudência dos Santos

Abril/2005

Orientador: Mário Roberto Folhadela Benevides

Programa: Engenharia de Sistemas e Computação

Apresentamos uma Lógica Dinâmica Proposicional que usa termos CCS como programas. O mecanismo de comunicação é baseado em CCS com ações de comunicação e a ação silenciosa (τ) representando ações internas. Provamos a completude com respeito à classe de modelos finitos Kripke. Diferentemente da Lógica Dinâmica de Concorrência com canais, a nossa lógica é decidível.

Abstract of Thesis presented to COPPE/UFRJ as a partial fulfillment ofthe requirements for the degree of Doctor of Science (D.Sc.)

Concurrency and Sinchronisation for Process Propositional Dynamic Logic

Vera Lúcia Prudência dos Santos

April/2005

Advisor: Mário Roberto Folhadela Benevides

Department: Systems and Computation Engineering

This work presents a Propositional Dynamic Logic which uses CCS terms as programs. The communication mechanism is based on CCS with communication actions and the silent action (τ) representing internal actions. We prove completeness with respect to a class of finite Kripke models. Unlike Concurrent PDL (with channels) our logic is decidable.

Índice

Lista de Figuras

Capítulo 1

Introdução

Neste trabalho apresentamos mecamismos de Concorrência e Sincronização para Lógica Dinâmica. Este tema foi inspirado no CCS [MIL89] e na lógica dinâmica proposicional [HAR84].

A teoria de CCS (Calculus of Communication Systems) surgiu na década de 80, e estuda processos via sistema de axiomas nos quais noções como execução seqüencial, execução paralela, escolha, comunicação, etc., são formalizadas pelos significados de operadores e equações. Seu objetivo principal consiste em especificar e verificar processos concorrentes.

O estudo da lógica dinâmica proposicional tem exibido uma área de pesquisa na qual os conceitos e métodos da lógica, computabilidade, complexidade e autômatos e teoria da linguagem formal são utilizados para se obter uma lógica para raciocinar sobre propriedades de programas.

Através do estudo desses dois assuntos, observamos que o CCS trata o comportamento observável de um sistema, e que a lógica dinâmica proposicional trata propriedades de programas. A partir disso nos motivamos a desenvolver uma lógica que estude os agentes do CCS como programas da lógica dinâmica proposicional.

Este trabalho propõe uma lógica dinâmica cujos programas são termos CCS. A

idéia principal é raciocionar sobre propriedades de especificações de sistemas concorrentes especificados em CCS.

A seguir apresentamos a organização do trabalho.

No Capítulo 2 temos uma revisão bibliográfica na qual apresentamos uma visão geral do CCS, baseado em [MIL89], onde abordamos o simbolismo, as definições básicas, a sintaxe, a semântica, as leis equacionais, bisimulação, dentre outros tópicos. Uma visualização da Lógica Dinâmica Proposicional baseada em [BRV02], onde apresentamos a sintaxe, a semântica, a definição de modelos canônicos para prova de completude. Em seguida, temos um estudo da Lógica Modal para CCS, baseada em [HC96], onde mencionamos a lógica de Hennessy-Milner para CCS, cujas fórmulas expressam propriedades de agentes. O poder diferenciador dessa lógica é limitado pela equivalência de bissimulação: dois processos bissimilares têm as mesmas propriedades modais. Além disso, apresentamos Comunicação em Lógica Dinâmica de Concorrência, introduzida por [PEL87a] como uma extensão de lógica dinâmica regular que tenta prover uma estrutura para raciocínio sobre programas concorrentes no modelo *and/or*. Apresentamos também uma linguagem lógica e o modelo correspondente que permite representar comunicação entre dois processos executando em paralelo - *channel - Concurrent Propositional Dynamic Logic (channel-CPDL).*

No Capítulo 3 apresentamos os resultados da nossa Lógica Dinâmica Proposicional para Programas CCS com concorrência e sincronização. Definimos a linguagem, o modelo, o frame, o esquema de axiomas, a prova de corretude e a prova de completude para cada operador introduzido na lógica.

No capítulo 4 apresentamos alguns exemplos com aplicaçẽs da nossa lógica.

No Capítulo 5 apresentamos a conclusão da tese e propostas para trabalhos futuros.

Capítulo 2

Revisão Bibliográfica

2.1 CCS

Comunicação e concorrência são noções complementares, ambas essenciais no entendimento de sistemas dinâmicos complexos. Sistemas são compostos de várias partes, cada uma atuando concorrentemente com, ou independentemente das outras partes.

Cada noção é a suposição de que cada uma das várias partes do sistema tem sua própria identidade, que persiste no decorrer do tempo, chamaremos essas partes de agentes. Sem essa suposição, dificilmente seríamos capazes de diferenciar os eventos do comportamento do sistema.

Usaremos o termo *agente* para representar qualquer sistema cujo comportamento consiste em ações discretas. Cada ação de um agente é uma interação com seus agentes vizinhos e portanto, gerando uma *comunicação* ou ocorre independentemente deles, podendo ocorrer *concorrentemente* com outras ações.

Uma parte essencial de uma teoria de sistemas complexos é uma noção precisa e tratável de *comportamento*. O que importa quando instalamos um microprocessador num sistema não são seus atributos físicos como peso, cheiro e cor, nem

sua constituição interna, mas simplesmente a maneira como este interage com o resto do sistema. Portanto, é razoável definirmos o comportamento de um sistema como sendo sua inteira capacidade de comunicação. Ou seja, o comportamento de um sistema é exatamente o que é observável, e para observar um sistema basta comunicar-se com ele.

2.1.1 Simbolismo

Existem cinco operadores básicos para construção de expressões para agentes no CCS, que são: Prefixação, Soma, Composição, Restrição e Rerrotulação.

Considere o agente C, uma célula que pode conter um único dado:

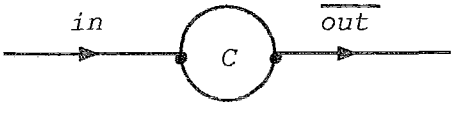

Figura 2.1: Célula simples

O diagrama mostra que a célula tem duas portas, mas não define o comportamento da célula. Devemos supor que:

- quando vazio, C pode aceitar um item na porta com rótulo *in*;
- quando um item estiver armazenado, C pode liberá-lo na porta com rótulo $\overline{out}$.

OBS: Os rótulos das portas de saída sempre terão uma sobrebarra para serem diferenciados das portas de entrada.

2.1.2 Prefixação

Usando o operador prefixação $(\cdot)$, que caracteriza seqüencialidade, escrevemos o comportamento de C como segue:

$$C = in(x) \cdot C'(x)$$

$$C'(x) = \overline{out}(x) \cdot C$$

O comportamento de C pode ser definido também por uma equação simples:

$$C = in(x) \cdot \overline{out}(x) \cdot C$$

Neste caso, C é descrito como um buffer de capacidade um.

Veremos, na Figura 4.2 o que acontece se juntarmos duas ou mais cópias de C. Isto é, representamos o resultado pela expressão de agente C^C.

Figura 2.2: Duas cópias da célula C

2.1.3 Soma

O operador binário (+) combina duas expressões de agentes como alternativas, enquanto que $(\cdot)$ prefixa uma ação numa expressão de agente simples. P + Q significa que o agente irá se comportar ou como P ou como Q. Se um dos dois começa a ser executado o outro é descartado.

Exemplo 2.1.3.1 : *Considere uma máquina de vender cartões telefônicos. Suponha que um cartão com 60 unidades custe 5,00 reais e um cartão com 20 unidades custe 1,00 real, e somente essas notas podem ser usadas.*

Uma maneira natural de definir a máquina de vendas, V, de acordo com sua interação com o ambiente em suas cinco portas (5r, 1r, 60u, 20u, retirar) é:

$$V = 5r \cdot 60u \cdot retirar \cdot V + 1r \cdot 20u \cdot retirar \cdot V$$

2.1.4 Composição

Exemplo 2.1.4.1 : *Suponha que desejamos receber uma confirmação do destinatário para o transmissor a respeito de cada valor enviado.*

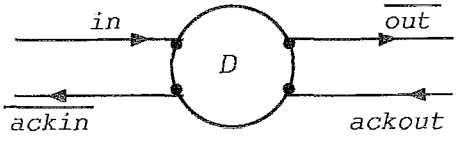

Figura 2.3:

D notificará o agente que lhe enviou o dado, somente depois de ter enviado o valor e recebido sua confirmação. Assim, definimos D como segue:

$$D = in(x) \cdot \overline{out}(x) \cdot ackout \cdot \overline{ackin} \cdot D$$

Observe que não existem valores nas ações *ackout* e $\overline{ackin}$; essas ações representam sincronizações puras entre agentes.

Neste caso, podemos definir um combinador de ligação (|), então podemos fazer a combinação de n cópias de D,

que definiremos por:

Figura 2.4:

$$D^n = D \mid D \mid \ldots \mid D$$

O operador binário de combinação é representado por $\mid$. Intuitivamente, o agente $P \mid Q$ é um sistema no qual P e Q procedem independentemente, mas também podem interagir através de portas complementares.

Nenhuma porta é internalizada pela composição, isto é, todas as portas permanecem abertas para novos links. A composição é comutativa e associativa, portanto não importa a ordem dos componentes.

2.1.5 Restrição

É um operador unário sobre agentes, representado por $A\backslash L$, significando que as portas em L (conjunto de portas rotuladas) do agente A não estão disponíveis para comunicação externa.

Note que a restrição $\backslash L$ internaliza tanto as portas em L quanto seus complementos.

2.1.6 Rerrotulação

Seja l um rótulo qualquer e $\overline{l}$ o seu complemento. Dizemos que uma função f de rótulo para rótulo é uma função de rerrotulação se ela preserva o complemento, ou seja:

Se $f(l) = l'$ então $f(\overline{l}) = \overline{l'}$.

Para cada função rerrotulação f, o operador rerrotulação $[f]$, pós-fixado para um agente, tem o efeito de rerrotular as portas do agente como imposta por f.

Escrevemos $l'_1/l_1 \ldots l'_n/l_n$, para a função rerrotulação f para a qual $f(l_i) = l'_i$ e $f(\overline{l_i}) = \overline{l'_i}$, para $i = 1, \ldots n$, caso contrário $f(l) = l$

2.1.7 Definições Básicas

Sincronização

Sincronizações sozinhas não são suficientes para descrever sistemas, cujo comportamento futuro depende de informações recebidas.

Para expressar esta dependência usamos uma expressão condicional, cuja condição contém variáveis que aguardam por valores de entrada, além disso, uma variável deve ocorrer anteriormente como um parâmetro numa entrada pré-fixada, que representa comunicação por passagem de valor. No CCS, sincronização e soma trabalham juntas dando o poder para expressar a comunicação de valores de qualquer tipo.

Ação e Transição

Sejam $\mathring{A} = \{a, b, c, \ldots\}$ um conjunto infinito de *nomes* e $\overline{\mathring{A}} = \{\overline{a}, \overline{b}, \overline{c}, \ldots\}$ um conjunto infinito de *co-nomes*. Então $\mathcal{L} = \mathring{A} \cup \overline{\mathring{A}}$ o conjunto de rótulos observáveis.

Os agentes serão identificados por estados. A transição de um estado para outro estado é acompanhada por uma ação e escrevemos como indicado abaixo:

$$P \xrightarrow{l} Q$$

Os agentes compostos $P \mid Q$ possuem transições, que são consideradas separadamente para P e para Q.

Exemplo 2.1.7.1 : *Suponha que os agentes A e B são dados, onde a, b, c são nomes de portas diferentes:*

Figura 2.5:

$A \stackrel{\text{def}}{=} a \cdot A' \quad B \stackrel{\text{def}}{=} c \cdot B'$
$A' \stackrel{\text{def}}{=} \overline{c} \cdot A \quad B' \stackrel{\text{def}}{=} \overline{b} \cdot B$

Agora, considere o agente composto $A \mid B$:

Figura 2.6:

A primeira regra de transição diz que: se o agente A pode fazer uma ação sozinho então A também pode fazer uma ação no contexto $A \mid B$, deixando o agente B inalterado, o mesmo valendo para B. Portanto,

$A \xrightarrow{a} A'$ inferimos $A \mid B \xrightarrow{a} A' \mid B$

O mesmo acontece pelo fato da porta c de A está ligada com a porta $\overline{c}$ de B, temos:

$A' \xrightarrow{\overline{c}} A$ inferimos $A' \mid B \xrightarrow{\overline{c}} A \mid B$

Isto não representa a comunicação entre A' e B, em vez disso, representa a possibilidade que A' pode se comunicar com um terceiro agente através da porta $\overline{c}$, deixando o agente B inalterado.

Para representar uma comunicação *handshake* (aperto de mão), que consite de ações simultâneas por ambas as partes, definimos uma outra regra de transição a seguir:

$A' \xrightarrow{\bar{c}} A$ e $B \xrightarrow{c} B'$ inferimos $A' \mid B \xrightarrow{?} A \mid B'$

Isto incorpora a idéia que A e B mudam de estado simultâneamente, com a composição sendo preservada. Mas, o que escrevemos no lugar de "?"?

A resposta para esta questão é muito importante para o nosso cálculo. Consideramos que "?" representa uma ação *perfeita* para o agente $A' \mid B$, além disso, esta ação perfeita origina-se de qualquer par $(b, \bar{b})$ de ações complementares pelos componentes de uma agente composto, já que a ação é interna para tal agente composto.

Assim, é suficiente introduzir uma ação perfeita simples, que denotamos por τ, para representar todas as comunicações *handshake* (aperto de mão). Note que, a ação τ não tem complemento.

Devemos definir $Act = \mathcal{L} \cup \{\tau\}$, como o conjunto de todas as ações possíveis. Então podemos deduzir a seguinte regra para o exemplo acima.

$A' \xrightarrow{\bar{c}} A$ e $B \xrightarrow{c} B'$ inferimos $A' \mid B \xrightarrow{\tau} A \mid B'$

O comportamento dos sistemas compostos ignora suas ações internas, pois τ não representa uma comunicação potencial e também não é observável diretamente.

Dizemos que dois sistemas são equivalentes quando eles exibem os mesmos modelos de ações externas.

Uma seqüência de ações internas

$$P \xrightarrow{\tau} P_1 \xrightarrow{\tau} \cdots \xrightarrow{\tau} P_n$$

é equivalente a uma simples ação interna

$$P \xrightarrow{\tau} P_n$$

e isto permite simplificações consideráveis da expressão do agente P via equações algébricas apropriadas.

Veremos agora o efeito da restrição da porta c ($\backslash c$) no agente $(A \mid B)\backslash c$, mostrado na Figura 2.7, onde as portas rotuladas c e $\overline{c}$ desaparecem significa que o agente composto restrito $(A \mid B) \setminus c$ pode não realizar as ações, embora ele possa realizar uma ação τ que resulta da comunicação $(c, \overline{c})$ entre seus componentes.

Figura 2.7:

A regra geral para restrição é a seguinte:

Se $P \xrightarrow{\alpha} P'$ então $P \setminus L \xrightarrow{\alpha} P' \setminus L$ tal que $\alpha, \overline{\alpha} \notin L$

Todas as transições que podem ocorrer no sistema $(A \mid B)\backslash c$ serão representadas numa árvore infinita, que chamaremos de árvore de *transição* ou árvore de *derivação*:

Podemos ver que a árvore se repete. Podemos resumir a ação comportamento do sistema num grafo de transição 2.9:

Vemos que o comportamento do agente $(A \mid B) \setminus c$ é igual a C_1, onde definimos os agentes $C_0, \cdots, C_3$ por:

$$C_0 \stackrel{\text{def}}{=} \overline{b} \cdot C_1 + a \cdot C_2$$

$$C_1 \stackrel{\text{def}}{=} a \cdot C_3$$

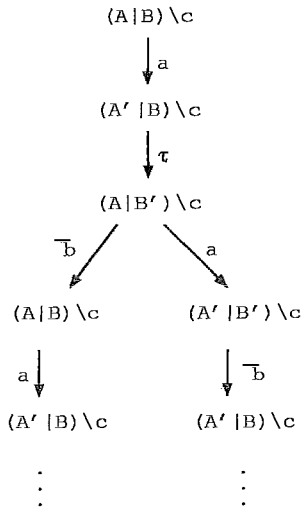

Figura 2.8:

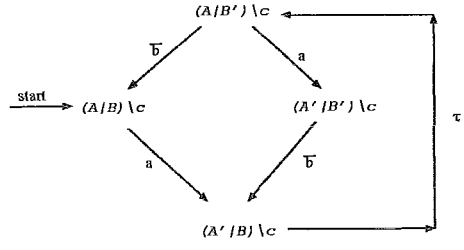

Figura 2.9:

$C_2 \stackrel{\text{def}}{=} \overline{b} \cdot C_3$

$C_3 \stackrel{\text{def}}{=} \tau \cdot\cdot C_0$

A Sintaxe

Nas seções anteriores já definimos $\mathcal{L} = \mathring{A} \cup \overline{\mathring{A}}$, o conjunto de rótulos observáveis, onde $\mathring{A} = \{a, b, c, \cdots\}$ é o conjunto de *nomes* (portas que aceitam eventos) e $\overline{\mathring{A}} = \{\overline{a}, \overline{b}, \overline{c}, \cdots\}$ é o conjunto de *co-nomes* (portas que podem oferecer eventos). Temos também que as ações l e l' agem sobre $\mathcal{L}$. Definimos também a ação *perfeita* ou

silenciosa τ e o conjunto de ações $Act = \mathcal{L} \cup \{\tau\}$, com as ações α e β agindo sobre Act.

Devemos usar K, L como subconjuntos de $\mathcal{L}$, e devemos usar $\overline{L}$ para representar o conjunto de complementos de rótulos em L. Uma *função rerrotulação* f, é uma função de $\mathcal{L}$ em $\mathcal{L}$ tal que $f(\bar{l}) = \overline{f(l)}$. E estendendo f para o conjunto Act temos que $f(\tau) = \tau$.

Seja $\Xi = \{E, F, \cdots\}$, o conjunto de *expressões de agentes*. Ξ é o menor conjunto que inclue $\mathcal{K}$ e contém as seguintes expressões, onde E e E_i estão em Ξ:

- $\alpha \cdot E$, uma prefixação ($\alpha \in Act$);
- $\sum_{i \in I} E_i$, uma soma (I é um conjunto de índices);
- $E_1 | E_2$, uma composição;
- $E \backslash L$, uma restrição (L $\subseteq \mathcal{L}$);
- $E[f]$, uma rerrotulação (f é uma função rerrotulação)

Na expressão de soma, significa o somatório de todas as expressões E_i com i agindo sobre I, e podemos reescrevê-la da seguinte forma: $\sum\{E_i : i \in I\}$.

A Semântica

Para entendermos o significado da linguagem básica do CCS, devemos usar a noção geral de *sistema de transição rotulado*:

$$(S, T, \{\xrightarrow{t} : t \in T\})$$

onde S é um conjunto de estados, T é um conjunto de rótulos e $\xrightarrow{t} \subseteq S \times S$ para cada $t \in T$ é uma relação transição.

No sistema de transição devemos tomar S como sendo Ξ (conjunto de expressões de agentes) e T como Act (conjunto de ações).

A semântica para Ξ consiste na definição de cada relação transição $\stackrel{\alpha}{\rightarrow}$ sobre Ξ. Devemos definir as transições de cada agente composto em termos das transições de seus componentes. Na seção anterior, por exemplo, indicamos que, de $A \stackrel{a}{\rightarrow} A'$ inferimos $A \mid B \stackrel{a}{\rightarrow} A' \mid B$. A regra geral que nos permite essa inferência será:

$$\frac{E \stackrel{\alpha}{\rightarrow} E'}{E \mid F \stackrel{\alpha}{\rightarrow} E' \mid F}$$

Assim, podemos observar que a semântica pa CCS é feita através de um conjunto de regras de inferência, obtidas a partir de ações atômicas, que são definidas por indução na estrutura das expressões de comportamento. Apresentamos abaixo as regras de transição para os operadores do nosso cálculo (usaremos os nomes **Act**, **Sum**, **Com**, **Res**, **Rel** e **Con** para indicar que as regras estão associadas respectivamente com Prefixação, Soma, Composição, Restrição, Rerrotulação e com Constantes.)

Prefixação:

$$\mathbf{Act} = \frac{}{\beta \cdot E \stackrel{\beta}{\rightarrow} E}$$

Soma:

$$\mathbf{Sum_j} = \frac{E_j \stackrel{\beta}{\rightarrow} E'_j}{\sum_{i \in I} E_i \stackrel{\beta}{\rightarrow} E'_j} (j \in J)$$

De $E_1 \stackrel{\beta}{\rightarrow} E'_1$ inferimos $E_1 + E_2 \stackrel{\beta}{\rightarrow} E'_1$

Composição:

$$\mathbf{Com_1} = \frac{E \stackrel{\beta}{\rightarrow} E'}{E|F \stackrel{\beta}{\rightarrow} E'|F}$$

De $E \stackrel{\beta}{\rightarrow} E'$ inferimos $E|F \stackrel{\beta}{\rightarrow} E'|F$

$$\mathbf{Com_2} = \frac{F \stackrel{\beta}{\rightarrow} F'}{E|F \stackrel{\beta}{\rightarrow} E|F'}$$

De $F \xrightarrow{\beta} F'$ inferimos $E|F \xrightarrow{\beta} E|F'$

$$\mathbf{Com_3} = \frac{E \xrightarrow{l} E' F \xrightarrow{\bar{l}} F'}{E|F \xrightarrow{\tau} E'|F'}$$

De $E \xrightarrow{\bar{l}} E'$ e $F \xrightarrow{\bar{l}} F'$ inferimos $E|F \xrightarrow{\tau} E'|F'$

Restrição:

$$\mathbf{Res} = \frac{E \xrightarrow{\beta} E'}{E\backslash L \xrightarrow{\beta} E'\backslash L}(\beta, \bar{\beta} \notin L)$$

Rerrotulação:

$$\mathbf{Rel} = \frac{E \xrightarrow{\beta} E'}{E[f] \xrightarrow{f(\beta)} E'[f]}$$

Constante:

$$\mathbf{Con} = \frac{P \xrightarrow{\beta} P'}{A \xrightarrow{\beta} P'}(A \stackrel{\text{def}}{=} P)$$

2.1.8 Leis Equacionais

Nesta seção apresentamos a classificação das leis equacionais que usaremos no nosso cálculo:

- As leis *dinâmicas* , que envolvem somente os combinadores dinâmicos (Prefixação, Soma e Constantes). Essas leis podem ser consideradas como uma álgebra de grafos de transição.

- As leis *estáticas* que envolvem somente os combinadores estáticos (Composição, Restrição e Rerrotulação). Essas leis podem ser consideradas como uma álgebra de grafos de fluxo.

- As leis de *expansão* que representam todas as possibilidades de ações que um sistema composto pode executar.

As Leis Dinâmicas

As leis dinâmicas para soma são as seguintes:

Proposição 2.1.1 *: Leis monóides:*

1. $P + Q = Q + P$
2. $P + (Q + R) = (P + Q) + R$
3. $P + P = P$
4. $P + 0 = P$

Abaixo temos as leis dinâmicas para prefixação, e baseia-se no significado das ações silenciosas τ:

Proposição 2.1.2 *: Leis τ:*

1. $\alpha \cdot \tau \cdot P = \alpha \cdot P$
2. $P + \tau \cdot P = \tau \cdot P$
3. $\alpha \cdot (P + \tau \cdot Q) + \alpha \cdot Q = \alpha \cdot (P + \tau \cdot Q)$

Definição 2.1.1 *:* $P \stackrel{\alpha}{\Rightarrow} P'$ *se* $P(\stackrel{\tau}{\rightarrow})^* \stackrel{\alpha}{\rightarrow} (\stackrel{\tau}{\rightarrow})^* P'$.

Nesta definição usamos $(\stackrel{\tau}{\rightarrow})^*$, o fechamento transitivo reflexivo de $\stackrel{\tau}{\rightarrow}$, que significa: *zero ou mais ações* τ. Note que, $\stackrel{\tau}{\Rightarrow}$ significa *uma ou mais ações* τ.

Corolário 2.1.1 *:* $P + \tau \cdot (P + Q) = \tau \cdot (P + Q)$

Leis de Expansão

Freqüentemente, um sistema de concorrência é expressado como uma composição restrita, na seguinte forma:

$$(P_1 \mid ... \mid P_n) \setminus L$$

Uma composição restrita de componentes rerrotulados origina-se muitas vezes do que devemos chamar de uma *standard concurrent form* (scf), que se escreve:

$$(P_1[f_1] \mid ... \mid P_n[f_n]) \setminus L$$

Muitas vezes, os agentes P_i serão puramente seqüenciais, isto é, serão definidos usando somente prefixação e soma. A lei de expansão está interessada nas ações imediatas de um agente na *standard concurrent form.* Essas ações serão de dois tipos:

- O primeiro tipo é devido a uma ação α de um componente simples, P_i, então a sfc terá uma ação $f_i(\alpha)$, e a derivativa será uma nova sfc:

  $$(P_1[f_1] \mid ... \mid P_i'[f_i] \mid ... \mid P_n[f_n]) \setminus L$$

  isto é, somente o i-ésimo componente da expressão muda.

- O segundo tipoé uma ação τ, uma comunicação resultante de ações l_1 por P_i e l_2 por P_j $(i \leq i < j \leq n)$, tal que $f_i(l_1) = \overline{f_j(l_2)}$. Então a derivativa será uma nova scf:

  $$(P_1[f_1] \mid ... \mid P_i'[f_i] \mid .... \mid P_j'[f_j] \mid ... \mid P_n[f_n]) \setminus L$$

na qual temos dois componentes mudando.

Com este resultado preliminar podemos definir a lei formalmente.

Proposição 2.1.3 : *A lei de expansão:*

Seja $P \equiv (P_1[f_1] \mid \cdots \mid P_n[f_n]) \setminus L$ *com* $n \geq 1$. *Então*

$$P = \sum\{f_i(\alpha) \cdot (P_1[f_1] \mid \cdots \mid P_i'[f_i] \mid \cdots \mid P_n[f_n]) \setminus L :$$

$$P_i \xrightarrow{\alpha} P_i', f_i(\alpha) \notin L \cup \overline{L}\} +$$

$$\sum\{\tau \cdot (P_1[f_1] \mid \cdots \mid P_i'[f_i] \mid \cdots \mid P_j'[f_j] \cdots \mid P_n[f_n]) \setminus L :$$

$$P_i \xrightarrow{l_1} P_i', P_j \xrightarrow{l_2} P_j', f_i(l_1) = \overline{f_j(l_2)}, i < j\}$$

Um uso freqüente da lei de expansão é quando todas as funções de rerrotulação f_i são funções identidade Id, então temos a vantagem da lei $P[Id] = P$.

Corolário 2.1.2 :

Seja $P \equiv (P_1 \mid \cdots \mid P_n)\setminus L$ *com* $n \geq 1$. *Então*

$$P = \sum\{\alpha \cdot (P_1 \mid \cdots \mid P_i' \mid \cdots \mid P_n)\setminus L :$$

$$P_i \xrightarrow{\alpha} P_i', \alpha \notin L \cup \overline{L}\} +$$

$$\sum\{\tau \cdot (P_1 \mid \cdots \mid P_i' \mid \cdots \mid P_j' \cdots \mid P_n)\setminus L :$$

$$P_i \xrightarrow{l} P_i',\ P_j \xrightarrow{l} P_j', i < j\}$$

Leis Estáticas

O conjunto de axiomas para os operadores estáticos é correto e completo para grafos de fluxo; isto é, são axiomas que podem ser deduzidos exatamente daquelas equações que são verdadeiras na interpretação do grafo de fluxo.

Abaixo, apresentamos os três grupos de equações: Composição, Restrição e Rerrotulação.

Proposição 2.1.4 *: Leis de composição:*

1. $P \mid Q = Q \mid P$
2. $P \mid (Q \mid R) = (P \mid Q) \mid R$
3. $P \mid 0 = P$

Note que 0, na interpretação de um grafo de fluxo, representa o grafo de fluxo vazio.

Proposição 2.1.5 *: Leis de restrição:*

1. $P\backslash L = P$ *se* $\mathcal{L}(P) \cap (L \cup \overline{L}) = \emptyset$
2. $P\backslash K\backslash L = P\backslash(K \cup L)$
3. $P[f]\backslash L = P\backslash f^{-1}(L)[f]$
4. $(P \mid Q)\backslash L = P\backslash L \mid Q\backslash L$ *se* $\mathcal{L}(P) \cap \overline{\mathcal{L}(Q)} \cap (L \cup \overline{L}) = \emptyset$

Proposição 2.1.6 *: Leis de rerrotulação:*

1. $P[Id] = P$
2. $P[f] = P[f']$ *se* $f\lceil\mathcal{L}(P) = f'\lceil\ \mathcal{L}(P)$

3. $P[f][f'] = P[f' \circ f]$

4. $(P \mid Q)[f] = P[f] \mid Q[f]$ *se* $f\lceil(L \cup \overline{L})$ *é uma função um para um, onde* $L = \mathcal{L}(P \mid Q)$

Id é a função identidade. f e f' tem efeito sobre P, a notação $f\lceil D$ significa a função f restrita ao domínio D, no item (4) é necessário garantir que $[f]$ é aplicado a P e Q separadamente.

2.1.9 Bissimulação

Nesta seção daremos uma noção de equivalência entre agentes, baseado na idéia de que dois agentes P e Q são distintos, se a distinção pode ser detectada por um agente externo interagindo com cada um deles. Em toda seção devemos tratar a ação interna τ , como qualquer outra ação, e isto produzirá uma relação de equivalência que chamaremos de *equivalência forte*, na qual devemos distinguir entre $a \cdot \tau \cdot 0$ e $a \cdot 0$.

A seguir, mostramos a necessidade da noção de igualdade forte, introduzimos a importância da idéia de *bisimulação forte*, pois equivalência forte é definida usando essa noção.

Bissimulação Forte

Definição 2.1.2 : *Uma relação binária* $S \subseteq P \times P$ *sobre agentes é uma* **bissimulação forte** *se* $(P, Q) \in S$ *implica, para todo* $\alpha \in Act$, *em:*

i. Sempre que $P \xrightarrow{\alpha} P'$ *então, para algum* Q', $Q \xrightarrow{\alpha} Q'$ *e* $(P', Q') \in S$

ii. Sempre que $Q \xrightarrow{\alpha} Q'$ *então, para algum* P', $P \xrightarrow{\alpha} P'$ *e* $(P', Q') \in S$

Figura 2.10:

Exemplo 2.1.9.1 *: Considere o exemplo dado anteriormente:*

Quando dizemos que o agente $(A \mid B) \setminus c$ *se comporta igual ao agente* C_1*, dados pelas seguintes equações:*

$$C_0 \stackrel{\text{def}}{=} \overline{b} \cdot C_1 + a \cdot C_2$$
$$C_1 \stackrel{\text{def}}{=} a \cdot C_3$$
$$C_2 \stackrel{\text{def}}{=} \overline{b} \cdot C_3$$
$$C_3 \stackrel{\text{def}}{=} \tau \cdot C_0$$

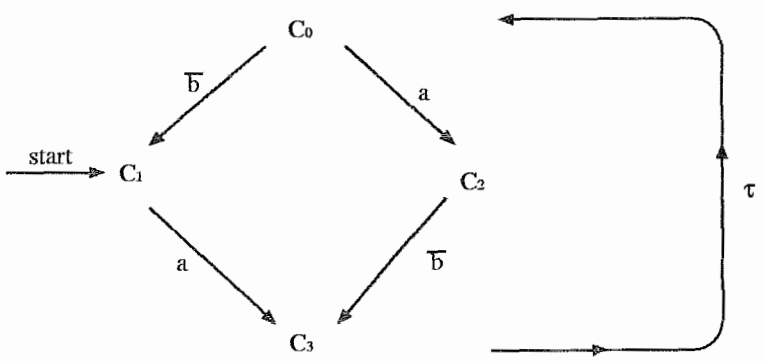

Figura 2.11:

estamos afirmando que a seguinte relação S *é uma bissimulação forte:*

$$S = \{((A \mid B)\backslash c, C_1), ((A' \mid B)\backslash c, C_3), ((A \mid B')\backslash c, C_0), ((A' \mid B')\backslash c, C_2)\}$$

Isto é fácil comprovar, basta checar todas as possíveis derivações de cada um dos oito agentes, como por exemplo:

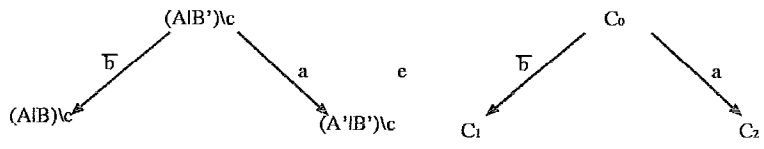

Figura 2.12:

Proposição 2.1.7 : *Assuma que cada S_i, $i = 1, 2, \ldots$, é uma bissimulção forte. Então as seguintes relações são bissimulações fortes:*

1. *Idp (identidade)*

2. *S_i^{-1} (inverso)*

3. *$S_1 S_2$ (composição)*

4. *$\cup_{i \in I} S_i$ (união)*

Prova. Provaremos somente (3).

Suponha que $(P, R) \in S_1 S_2$. Então para algum Q temos

$$(P, Q) \in S_1 \text{ e } (Q, R) \in S_2$$

Seja $P \xrightarrow{\alpha} P'$. Então para algum Q', como $(P, Q) \in S_1$, temos

$$Q \xrightarrow{\alpha} Q' \text{ e } (P', Q') \in S_1$$

Já que, $(Q, R) \in S_2$ para algum R', temos

$$R \xrightarrow{\alpha} R' \text{ e } (Q', R') \in S_2$$

Conseqüentemente, $(P', R') \in S_1 S_2$. Similarmente, se $R \xrightarrow{\alpha} R'$, então podemos encontrar P' tal que, $P \xrightarrow{\alpha} P'$ e $(P', R') \in S_1 S_2$. □

Definição 2.1.3 : *P e Q são* **equivalentes forte** *ou* **bissimilares forte** *$(P \sim Q)$, se $(P,Q) \in S$ para alguma bissimulação forte S. Isto pode ser expressado como segue:*

$$\sim = \cup\{S : S \text{ é uma bissimulação } \}$$

$\sim$ é uma bissimulação forte e é uma relação de equivalência.

Definição 2.1.4 : *S é uma bissimulação forte sobre $\sim$ se PSQ implica, para todo $\alpha \in Act$, em:*

i. Sempre que $P \xrightarrow{\alpha} P'$ então, para algum Q', $Q \xrightarrow{\alpha} Q'$ e $P' \sim S \sim Q'$

ii. Sempre que $Q \xrightarrow{\alpha} Q'$ então, para algum P', $P \xrightarrow{\alpha} P'$ e $P' \sim S \sim Q'$

2.1.10 Equivalência de Observação

Definição 2.1.5 : *Se $t \in Act^*$ então $\hat{t} \in \mathcal{L}^*$ é uma seqüência obtida pela remoção de todas as ocorrências τ de t.*

Note que $\hat{\tau^n} = \varepsilon$ (a seqüência vazia).

Definição 2.1.6 : *Se $t = \alpha_1 \cdots \alpha_n \in Act^*$, então escrevemos $E \xrightarrow{t} E'$ se $E \xrightarrow{\alpha_1} \cdots \xrightarrow{\alpha_n} E'$.*

Definimos abaixo um novo sistema de transição rotulado:

$$(\Xi, \mathcal{L}^*, \{\stackrel{s}{\Rightarrow}, s \in \mathcal{L}^*\})$$

sobre expressões de agentes, nos quais as relações transição $\stackrel{s}{\Rightarrow}$ são definidas a seguir. Definimos também $\stackrel{t}{\Rightarrow}$ para todo $t \in Act^*$, isto é, as seqüências que podem conter τ.

Definição 2.1.7 : *Se* $t = \alpha_1, \cdots, \alpha_n \in Act^*$ *então* $E \stackrel{t}{\Rightarrow} E'$ *se*

$$E(\tau)^* \stackrel{\alpha_1}{\Rightarrow} (\tau)^* \cdots (\tau)^* \stackrel{\alpha_n}{\Rightarrow} (\tau)^* E'$$

Escreve-se $E \stackrel{t}{\Rightarrow}$ *significando* $E \stackrel{t}{\Rightarrow} E'$ *para algum* E'.

Definição 2.1.8 : *Se* $t \in Act^*$, *então* E' *é uma* **t-descendente** *de* E *se e somente se* $E \stackrel{\hat{t}}{\Rightarrow} E'$ *para algum* E'.

Vamos fazer a diferença entre as três relações $\stackrel{t}{\rightarrow}$, $\stackrel{t}{\Rightarrow}$ e $\stackrel{\hat{t}}{\Rightarrow}$, para $t \in Act^*$.

Cada relação especifica uma seqüência de ações com o mesmo conteúdo observável de t, mas as possibilidades das intervenções das ações τ são diferentes.

$\stackrel{t}{\rightarrow}$ especifica exatamente as ações τ ocorrendo em t;

$\stackrel{t}{\Rightarrow}$ especifica o número mínimo de ações τ ocorrendo em t;

$\stackrel{\hat{t}}{\Rightarrow}$ não especifica nada sobre as ações τ

Portanto, $P \stackrel{t}{\rightarrow} P'$ implica $P \stackrel{t}{\Rightarrow} P'$ e $P \stackrel{t}{\Rightarrow} P'$ implica $P \stackrel{\hat{t}}{\Rightarrow} P'$.

Definição 2.1.9 : *Uma relação binária* $S \subseteq P \times P$ *sobre agentes, é uma* **bissimulação (fraca)** *se* $(P, Q) \in S$ *implica, para todo* $\alpha \in Act$, *em:*

i. Sempre que $P \stackrel{\alpha}{\rightarrow} P'$ *então, para algum* Q', $Q \stackrel{\hat{\alpha}}{\Rightarrow} Q'$ *e* $(P', Q') \in S$

ii. Sempre que $Q \stackrel{\alpha}{\rightarrow} Q'$ *então, para algum* P', $P \stackrel{\hat{\alpha}}{\Rightarrow} P'$ *e* $(P', Q') \in S$

Exemplo 2.1.10.1 : *Sejam os agentes* C_0 *e* D , *representados pelos grafos abaixo:*

É facil checar que

$$S = \{(C_0, D), (C_1, D_1), (C_2, D_2), (C_3, D)\}$$

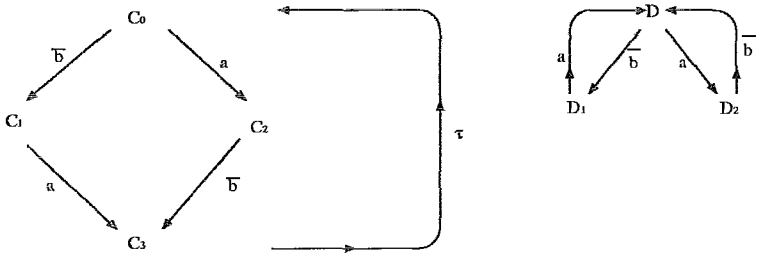

Figura 2.13:

é uma bissimulação, embora não possa existir uma bissimulação forte contendo o par (C_3, D).

Definição 2.1.10 : P *e* Q *são* **equivalentes-observação** *ou* **fracamente bissimilares** $(P \simeq Q)$, *se* $(P, Q) \in S$ *para alguma bissimulação (fraca)* S. *Isto é,*

$$\simeq = \cup\{S : S \text{ é uma bissimulação } \}$$

2.2 Lógica Dinâmica Proposicional (LDP)

A *Lógica Dinâmica Proposicional* (LDP), é um ramo importante da lógica modal que envolve modalidades unárias. A linguagem de PDL possui uma coleção infinita de operadores modais, cada um desses operadores tem a seguinte forma: $\langle\pi\rangle$, onde π denota um programa (não-determinístico).

A interpretação de $\langle\pi\rangle\phi$ é *"alguma execução de π no estado atual leva para um estado em que ϕ é verdadeiro"*, o que significa que seu dual $[\pi]\phi$ declara que *"toda execução de π num estado atual leva para um estado em que ϕ é verdadeiro."*

Programas complexos são construídos dos programas básicos com a ajuda de operações sobre programas. Usando operadores modais para refletir esta estrutura, obtemos uma linguagem poderosa e flexível.

2.2.1 Sintaxe

Suponha que temos algum conjunto fixo de programas básicos $a, b, c, ...$ Seja Π o menor conjunto de programas básicos construído sobre eles usando os construtores de programas $\cup, ;, *$ e $?$.

Seja um conjunto de diamonds $\langle\pi\rangle$ indexado por uma coleção de programas Π e os programas gerados desta base usando os construtores de programas, onde:

Escolha: Se π_1 e π_2 são programas, então $\pi_1 \cup \pi_2$ também é um programa.

O significado de $\pi_1 \cup \pi_2$ é executar não-deterministicamente π_1 ou π_2.

Composição: Se π_1 e π_2 são programas então $\pi_1; \pi_2$ também é um programa.

Este programa primeiro executa π_1 e então executa π_2.

Iteração: Se π é um programa então π^* também é um programa.

π^* é um programa que executa π um número finito de vezes.

Teste: Se ϕ é uma fórmula, então $\phi?$ é um programa.

Este programa testa se ϕ é verdadeira. Se for, então continua; se não for, falha.

Interpretando essas definições utilizando os operadores temos que:

Se $\langle\pi_1\rangle$ e $\langle\pi_2\rangle$ são operadores modais, então $\langle\pi_1 \cup \pi_2\rangle$, $\langle\pi_1;\pi_2\rangle$ e $\langle\pi^*\rangle$ também são.

Com esta notação podemos descrever propriedades de execução de programas:

$$\langle\pi^*\rangle\phi \longleftrightarrow \phi \vee \langle\pi;\pi^*\rangle\phi$$

Dizemos que o próximo estado possui a informação ϕ, pode ser alcançado pela execução de π um número finito de vezes, se e somente se já temos a informação ϕ no estado corrente ou podemos executar π uma vez e então encontrar um próximo estado que possui a informação ϕ depois de um número finito de repetições de π.

O construtor teste tem uma sintaxe não usual, ele nos permite fazer uma modalidade de uma fórmula. Intuitivamente, esta modalidade acessa o estado atual se esse estado satisfaz ϕ. Ou seja, $\langle\phi?\rangle\psi$ simplesmente significa $\phi \wedge \psi$. Podemos usar o operador teste para fazer programas interessantes, como por exemplo:

$(p?;a) \cup (\neg p?;b)$ é "Se p então a senão b"

Estamos interessados somente na LDP regular, isto é, vamos trabalhar somente com três construtores de programas que são: $\cup, ;, *$.

Definição 2.2.1 *: Um frame para LDP é um sistema de transição* $\mathcal{F} = (W, R_\pi)_{\pi\in\Pi}$, *mas só estamos interessados em frames-LDP regulares, isto é, frames tais que para todos os programas* π *temos:*

$R_{\pi_1 \cup \pi_2} = R_{\pi_1} \cup R_{\pi_2}$

$R_{\pi_1;\pi_2} = R_{\pi_1}; R_{\pi_2}$

$R_{\pi^*} = (R_\pi)^*$

2.2.2 Axiomatização

Definição 2.2.2 *: A* **lógica dinâmica proposional normal** *contém os seguintes axiomas:*

1. $[\pi](p \to q) \to ([\pi]p \to [\pi]q)$
2. $\langle\pi\rangle p \leftrightarrow \neg[\pi]\neg p$
3. $[\pi_1;\pi_2]p \leftrightarrow [\pi_1][\pi_2]p$
4. $[\pi_1 \cup \pi_2]p \leftrightarrow [\pi_1]p \wedge [\pi_2]p$
5. $[\pi^*]p \leftrightarrow p \wedge [\pi][\pi^*]p$
6. $[\pi^*](p \to [\pi]p) \to (p \to [\pi^*]p)$

e é fechada sob

Modus Ponens:

$$\frac{\vdash_\Lambda \phi, \vdash_\Lambda \phi \to \psi}{\vdash_\Lambda \psi}$$

Generalização:

($\vdash_\Lambda \phi$ implica $\vdash_\Lambda [\pi]\phi$ para todo programa π)

Substituição Uniforme:

$$\frac{\vdash_\Lambda \phi}{\vdash_\Lambda \sigma \cdot \phi}$$

E chamamos esta a menor lógica proposicional normal.

Na nossa lógica usaremos, $\vdash \phi$ para significar que ϕ é um teorema de LDP, consistência chamaremos de consistência-LDP e assim por diante. Note que LDP não é uma lógica compacta. Seja Σ um conjunto definido como abaixo:

$$\{\langle\alpha^*\rangle p, \neg p, \neg\langle\alpha\rangle p, \neg\langle\alpha\rangle\langle\alpha\rangle p, \neg\langle\alpha\rangle\langle\alpha\rangle\langle\alpha\rangle p, \cdots\}$$

Qualquer subconjunto finito de Σ é satisfatível em um frame-LDP em um único ponto, mas o próprio Σ não é.

A corretude é direta. Basta checar que os axiomas realmente são válidos em todos os frames-LDP regulares.

A completude será provada com a ajuda de modelos canônicos finitos.

Dizemos que um conjunto de fórmulas Σ é **fechado sob subfórmulas** se, para todo $\phi \in \Sigma$, se ψ é uma subfórmula de ϕ então $\psi \in \Sigma$.

2.2.3 Modelos Canônicos

Nesta seção introduziremos a noção de modelos canônicos para LDP. Trabalharemos com a linguagem de lógica dinâmica proposicional regular, definida anteriormente. Vimos também que um frame desta linguagem é um sistema de transição $\mathcal{F}= (W, R_\pi)_{\pi\in\Pi}$, onde:

$$R_{\pi_1\cup\pi_2} = R_{\pi_1} \cup R_{\pi_2}$$

$$R_{\pi_1;\pi_2} = R_{\pi_1}; R_{\pi_2}$$

$R_{\pi^*} = (R_\pi)^*$

Dizemos que uma fórmula ϕ é uma validade-LDP ($\models \phi$) se ela é válida em todos os frames-LDP.

Definição 2.2.3 (Fecho de Fischer-Ladner): *Se Σ é qualquer conjunto de fórmulas então $FL(\Sigma)$ (o Fecho de Fischer-Ladner de Σ) é o menor conjunto que é fechado sob subfórmulas e satisfaz as seguintes restrições adicionais:*

1. *Se $\langle \pi_1; \pi_2 \rangle \phi \in FL(\Sigma)$ então $\langle \pi_1 \rangle \langle \pi_2 \rangle \phi \in FL(\Sigma)$*

2. *Se $\langle \pi_1 \cup \pi_2 \rangle \phi \in FL(\Sigma)$ então $\langle \pi_1 \rangle \phi \vee \langle \pi_2 \rangle \phi \in FL(\Sigma)$*

3. *Se $\langle \pi^* \rangle \phi \in FL(\Sigma)$ então $\langle \pi \rangle \langle \pi^* \rangle \phi \in FL(\Sigma)$*

Note que, se Σ é finito, então $FL(\Sigma)$ também é finito.

Definimos $\neg FL(\Sigma)$, o *fecho de $FL(\Sigma)$ sob negações simples*, como sendo o menor conjunto tal que, se $\phi \in FL(\Sigma)$ e ϕ não é da forma $\neg\psi$ então $\neg\phi \in \neg FL(\Sigma)$. Isto é, para todo $\phi \in \neg FL(\Sigma)$ existe um $\psi \in \Sigma$ tal que ψ é equivalente a $\neg\phi$.

Definição 2.2.4 (Átomos): *Seja Σ um conjunto de fórmulas. Um conjunto de fórmulas $\mathcal{A}$ é um* **átomo** *sobre Σ se ele é um subconjunto maximal consistente de $\neg FL(\Sigma)$. Isto é, $\mathcal{A}$ é um átomo sobre Σ se $\mathcal{A} \subseteq \neg FL(\Sigma)$ então $\mathcal{A}$ é consistente, e se $\mathcal{A} \subset \mathcal{B} \subseteq \neg FL(\Sigma)$ então $\mathcal{B}$ é inconsistente. $At(\Sigma)$ é o conjunto de todos os átomos sobre Σ.*

Lema 2.2.1 : *Seja Σ qualquer conjunto de fórmulas, e $\mathcal{A}$ qualquer elemento de $At(\Sigma)$. Então*

1. *Se $\neg\phi \in \mathcal{A}$ então $\phi \notin \mathcal{A}$.*

2. *Se* $\phi \in \mathcal{A}$ *e* ψ *é equivalente a* $\neg\phi$ *então* $\psi \notin \mathcal{A}$.

3. *Para todo* $\phi \wedge \psi \in \neg FL(\Sigma)$: $\phi \wedge \psi \in \mathcal{A}$ *se e somente se* $\phi \in \mathcal{A}$ *e* $\psi \in \mathcal{A}$.

4. *Para todo* $\langle \pi_1; \pi_2 \rangle \phi \in \neg FL(\Sigma)$: $\langle \pi_1; \pi_2 \rangle \phi \in \mathcal{A}$ *se e somente se* $\langle \pi_1 \rangle \langle \pi_2 \rangle \phi \in \mathcal{A}$.

5. *Para todo* $\langle \pi_1 \cup \pi_2 \rangle \phi \in \neg FL(\Sigma)$: $\langle \pi_1 \cup \pi_2 \rangle \phi \in \mathcal{A}$ *se e somente se* $\langle \pi_1 \rangle \phi \vee \langle \pi_2 \rangle \phi \in \mathcal{A}$.

6. *Para todo* $\langle \pi^* \rangle \phi \in \neg FL(\Sigma)$: $\langle \pi^* \rangle \phi \in A$ *se e somente se* $\langle \pi \rangle \langle \pi^* \rangle \phi \in \mathcal{A}$.

Prova.: A prova é bastante simples. Provaremos o caso 3 e os outros casos são similares, direta da definição de $\mathcal{A}$ ser maximal consistente.

($\Rightarrow$) Se $\phi \wedge \psi \in A$ então $\phi \in \mathcal{A}$ e $\psi \in \mathcal{A}$. Da definição 2.2.4 temos que $\mathcal{A} \subseteq \neg FL(\Sigma)$, assim se $\phi \wedge \psi \in \mathcal{A}$ e $\mathcal{A} \subseteq \neg FL(\Sigma)$ então $\phi \wedge \psi \in \neg FL(\Sigma)$, e $\phi \in \neg FL(\Sigma)$ e $\psi \in \neg FL(\Sigma)$, consequentemente $\phi \in \mathcal{A}$ e $\psi \in \mathcal{A}$.

($\Leftarrow$) Se $\phi \in \mathcal{A}$ e $\psi \in \mathcal{A}$ então $\phi \wedge \psi \in \mathcal{A}$. Da definição 2.2.4 temos que $\mathcal{A} \subseteq \neg FL(\Sigma)$. Então $\phi \in \neg FL(\Sigma)$ e $\psi \in \neg FL(\Sigma)$, assim $\phi \wedge \psi \in \neg FL(\Sigma)$. Logo, $\phi \wedge \psi \in \mathcal{A}$. □

Átomos são generalizações diretas de conjuntos maximais consistentes (MCS_s). Note, por exemplo, que se escolhemos Σ para ser um conjunto de fórmulas, então $At(\Sigma)$ é somente o conjunto de todos MSC_s.

Lema 2.2.2 : *Seja* M *o conjunto de todos os* MCS_s, *e* Σ *qualquer conjunto de sentenças. Então* $At(\Sigma) = \{\Gamma \cap \neg FL(\Sigma) \mid \Gamma \in M\}$.

O próximo lema é análogo ao Lema de Lindenbaum.

Lema 2.2.3 *Se $\phi \in \neg FL(\Sigma)$ e ϕ é consistente, então existe um $\mathcal{A} \in At(\Sigma)$ tal que $\phi \in \mathcal{A}$.*

Prova.: Existem duas maneiras de provar isto. Poderíamos aplicar simplesmente o Lema de Lindenbaum: como ϕ é consistente, existe um MCS_s que contém ϕ. Assim, pelo lema anterior, $M \cap \neg FL(\Sigma)$ é um átomo contendo ϕ. Porém, é mais fácil considerármos uma prova finitária.

Note que a informação em um átomo A pode ser representada por uma única fórmula $\bigwedge_{\phi \in A} \phi = \hat{\mathcal{A}}$.

Escreveremos tais conjunções de átomos como $\hat{\mathcal{A}}$. Obviamente, $\hat{\mathcal{A}} \notin \mathcal{A}$. Usando esta notação, construimos o átomo desejado da seguinte forma:

Enumere os elementos de $\neg FL(\Sigma)$ como $\sigma_1, \cdots, \sigma_m$. Considere $\mathcal{A}_1$ como sendo $\{\sigma_1\}$. Suponha que $\mathcal{A}_n$ está definido, onde $n < m$. Temos então que,

$$\vdash \hat{\mathcal{A}}_n \leftrightarrow (\hat{\mathcal{A}}_n \wedge \sigma_{n+1}) \vee (\hat{\mathcal{A}}_n \wedge \neg\sigma_{n+1}).$$

como isto é uma tautologia proposicional, então ou $\mathcal{A}_n \cup \{\sigma_{n+1}\}$ ou $\mathcal{A}_n \cup \{\neg\sigma_{n+1}\}$ é consistente.

Seja $\mathcal{A}_{n+1}$ uma extensão consistente. Pelo fato de $\neg FL(\Sigma)$ ser fechado somente sob negações simples, se $\mathcal{A}_n \cup \{\neg\sigma_{n+1}\}$ é a possibilidade consistente, podemos formar a extensão $\mathcal{A}_n \cup \{\tau\}$, onde $\neg\tau$ é σ_{n+1}. Seja $\mathcal{A}$ igual a $\mathcal{A}_m$. Então $\mathcal{A}$ é um átomo contendo ϕ. □

Lema 2.2.4 *: Para qualquer coleção finita de fórmulas Σ, $\vdash \bigvee_{\mathcal{A} \in At(\Sigma)} \hat{\mathcal{A}}$.*

Definição 2.2.5 (Modelo Canônico sobre Σ): *Seja Σ um conjunto de fórmulas. O* **modelo canônico sobre** Σ *é a tripla $(At(\Sigma), \{S_\pi^\Sigma\}_{\pi \in \Pi}, V^\Sigma)$, onde para cada*

variável proposicional p, $V^{\Sigma}(p) = \{\mathcal{A} \in At(\Sigma) \mid p \in \mathcal{A}\}$, *e para todo átomo* $\mathcal{A}$, $\mathcal{B} \in At(\Sigma)$ *e todo programa* π, $\mathcal{A}S_{\pi}^{\Sigma}\mathcal{B}$ *se* $\hat{\mathcal{A}} \wedge \langle\pi\rangle\hat{\mathcal{B}}$ *é consistente.* V^{Σ} *é chamado a* **valoração canônica** *e* S_{π} *são as* **relações canônicas**.

Com as preliminares estabelecidas, vamos retornar ao resultado da completude. Dada uma sentença consistente ϕ, precisamos satisfazer ϕ em um modelo-PDL regular. E é natural tentar construir o modelo requerido de átomos. Como primeiro passo, vamos dar uma definição precisa do que é um modelo-PDL regular construído de átomos.

Definição 2.2.6 (Modelo-LDP Regular sobre Σ): *Seja* Σ *um conjunto de fórmulas. Para todos os programas básicos* a, *defina* R_a^{Σ} *como sendo* S_a^{Σ}. *Para todos os programas complexos, defina indutivamente as relações-LDP* R_{π}^{Σ} *na maneira usual usando uniões, composições e fechamento transitivo reflexivo. Finalmente, defina* $\mathcal{B}$, *o modelo-LDP sobre* Σ *como sendo* $(At(\Sigma), \{R_{\pi}^{\Sigma}\}_{\pi \in \Pi}, V^{\Sigma})$, *onde* V^{Σ} *é a valoração canônica.*

Uma questão fundamental é a seguinte:

O modelo canônico sobre Σ é o modelo-LDP regular sobre Σ?

Infelizmente não. Apesar disso, é possível provar um Lema da Existência para modelos-LDP.

Lema 2.2.5 (Lema da Existência para Programas Básicos): *Seja* $\mathcal{A} \in At(\Sigma)$ *e* a *um programa básico. Então para todas as fórmulas* $\langle a\rangle\psi$ *em* $\neg FL(\Sigma)$, $\langle a\rangle\psi \in \mathcal{A}$ *se e somente se existe um* $\mathcal{B} \in At(\Sigma)$ *tal que* $\mathcal{A}R_a\mathcal{B}$ *e* $\psi \in \mathcal{B}$.

Prova.: ($\Leftarrow$) Suponha que existe um $\mathcal{B} \in At(\Sigma)$ tal que $\mathcal{A}R_a\mathcal{B}$ e $\psi \in \mathcal{B}$. Como R_a e S_a são idênticas para programas básicos, temos $\mathcal{A}S_a\mathcal{B}$, então $\hat{\mathcal{A}} \wedge \langle a \rangle \hat{\mathcal{B}}$ é consistente. Como ψ é uma das conjunções de $\hat{\mathcal{B}}$ então $\hat{\mathcal{A}} \wedge \langle a \rangle \psi$ é consistente. Como $\langle a \rangle \psi$ está em $\neg FL(\Sigma)$, deve estar também em $\mathcal{A}$, visto que $\mathcal{A}$ é um átomo e conseqüentemente, maximal consistente em $\neg FL(\Sigma)$.

($\Rightarrow$) Suponha $\langle a \rangle \psi \in \mathcal{A}$. Vamos construir um átomo $\mathcal{B}$ apropriado por escolhas forçadas. Enumere as fórmulas em $\neg FL(\Sigma)$ como $\sigma_1, ..., \sigma_m$. Defina $\mathcal{B}_0$ como sendo $\{\psi\}$. Suponha como hipótese indutiva que $\mathcal{B}_n$ é definido tal que $\hat{\mathcal{A}} \wedge \langle a \rangle \hat{\mathcal{B}}_n$ é consistente (onde $0 \leq n \leq m$). Temos,

$$\vdash \langle a \rangle \hat{\mathcal{B}}_n \leftrightarrow \langle a \rangle ((\hat{\mathcal{B}}_n \wedge \sigma_{n+1}) \vee (\hat{\mathcal{B}}_n \wedge \neg \sigma_{n+1}))$$

então,

$$\vdash \langle a \rangle \hat{\mathcal{B}}_n \leftrightarrow (\langle a \rangle (\hat{\mathcal{B}}_n \wedge \sigma_{n+1}) \vee \langle a \rangle (\hat{\mathcal{B}}_n \wedge \neg \sigma_{n+1}))$$

Portanto, ou para $\mathcal{B}' = \mathcal{B}_n \cup \{\sigma_{n+1}\}$ ou para $\mathcal{B}' = \mathcal{B}_n \cup \{\neg \sigma_{n+1}\}$ temos que, $\hat{\mathcal{A}} \wedge \langle a \rangle \hat{\mathcal{B}}$ é consistente.

Escolha $\mathcal{B}_{n+1}$ como sendo a expansão consistente, e faça $\mathcal{B}$ ser $\mathcal{B}_m$. Logo, $\mathcal{B}$ é o átomo que procuramos. □

Os axiomas 5 e 6 não podem dar a identidade desejada entre S_π e R_π. Mas, esses axiomas são fortes o bastante para garantir que $S_\pi \subseteq R_\pi$ para programas arbitrários π. Esta inclusão nos permite comprimir uma prova do Lema da Existência.

Lema 2.2.6 : *Para todos os programas* π, $S_{\pi^*} \subseteq R_{\pi^*}$.

Prova.: Precisamos mostrar que para todos os programas π que: se $\mathcal{A}S_{\pi^*}\mathcal{B}$ então existe uma seqüência finita de átomos $\mathcal{C}_0, ..., \mathcal{C}_n$ tal que $\mathcal{A} = \mathcal{C}_0 S_\pi \mathcal{C}_1, ..., \mathcal{C}_{n-1} S_\pi \mathcal{C}_n = \mathcal{B}$.

Seja $\mathcal{D}$ o conjunto de todos os átomos alcançáveis de $\mathcal{A}$ por tal seqüência. Mostraremos que $\mathcal{B} \in \mathcal{D}$.

Defina δ como sendo $\bigvee_{\mathcal{D} \in \mathcal{D}} \hat{\mathcal{D}}$.

Note que $\delta \wedge \langle \pi \rangle \neg \delta$ é inconsistente. No caso contrário, $\delta \wedge \langle \pi \rangle \hat{\mathcal{E}}$ seria consistente para ao menos um átomo $\mathcal{E}$ não alcançável por $\mathcal{A}$ em muitos casos finitos S_π, o que significa que $\hat{\mathcal{D}} \wedge \langle \pi \rangle \hat{\mathcal{E}}$ é consistente para ao menos um $\mathcal{D} \in \hat{\mathcal{D}}$, o que significa que $\mathcal{E} \in \mathcal{D}$, que não é verdade.

Como $\delta \wedge \langle \pi \rangle \neg \delta$ é inconsistente, temos $\vdash \delta \rightarrow [\pi]\delta$, conseqüentemente, pela generalização temos, $\vdash [\pi^*](\delta \rightarrow [\pi]\delta)$.

Pelo axioma 6, $\vdash \delta \rightarrow [\pi^*]\delta$. Como $\mathcal{A} S_{\pi^*} \hat{\mathcal{A}}$, $\hat{\mathcal{A}}$ é um dos disjuntos em δ, então $\vdash \hat{\mathcal{A}} \rightarrow \delta$ e conseqüentemente, $\vdash \hat{\mathcal{A}} \rightarrow [\pi^*]\delta$.

Como nossa suposição inicial foi que: $\hat{\mathcal{A}} \wedge \langle \pi^* \rangle \hat{\mathcal{B}}$ é consistente, então $\hat{\mathcal{A}} \wedge \langle \pi^* \rangle (\hat{\mathcal{B}} \wedge \delta)$ é consistente também. Mas isto significa que para um dos disjuntos $\hat{\mathcal{D}}$ de δ, $\hat{\mathcal{B}} \wedge \hat{\mathcal{D}}$ é consistente. Como $\mathcal{B}$ e $\mathcal{D}$ são átomos, $\mathcal{B} = \mathcal{D}$ e conseqüentemente $\mathcal{B} \in \mathcal{D}$. ■

Com este lema, podemos provar diretamente a inclusão desejada.

Lema 2.2.7 : *Para todos os programas* π, $S_\pi \subseteq R_\pi$.

Prova.: Por indução na estrutura de π.

Caso base:É imediato por termos definido R_a como sendo S_a para todos os programas básicos a.

Suponha que $\mathcal{A} S_{\pi_1;\pi_2} \mathcal{B}$, isto é, $\hat{\mathcal{A}} \wedge \langle \pi_1; \pi_2 \rangle \hat{\mathcal{B}}$, é consistente.

Pelo axioma 3, $\hat{\mathcal{A}} \wedge \langle \pi_1 \rangle \langle \pi_2 \rangle \hat{\mathcal{B}}$, também é consistente.

Usando o argumento de "escolha forçada", podemos construir um átomo $\mathcal{C}$ tal que $\hat{\mathcal{A}} \wedge \langle \pi_1 \rangle \hat{\mathcal{C}}$ e $\hat{\mathcal{C}} \wedge \langle \pi_2 \rangle \hat{\mathcal{B}}$ consistentes. Segue que $\mathcal{A} R_{\pi_1;\pi_2} \mathcal{B}$.

Uma argumentação similar usando o axioma 5, mostra que $S_{\pi_1 \cup \pi_2} \subseteq R_{\pi_1 \cup \pi_2}$. □

Agora, podemos provar o Lema da Existência para programas arbitrários.

Lema 2.2.8 (Lema da Existência): *Para todos os átomos $\mathcal{A}$ e todas as fórmulas $\langle \pi \rangle \psi \in \neg FL(\Sigma)$, $\langle \pi \rangle \psi \in \mathcal{A}$ se e somente se existe um $\mathcal{B}$ tal que $\mathcal{A} R_\pi \mathcal{B}$ e $\psi \in \mathcal{B}$.*

Prova.: ($\Rightarrow$) Suponha $\langle \pi \rangle \psi \in \mathcal{A}$. Podemos construir um átomo $\mathcal{B}$ tal que $\mathcal{A} S_\pi \mathcal{B}$ pela "escolha forçada". Já provamos que $S_\pi \subseteq R_\pi$, então $\mathcal{A} R_\pi \mathcal{B}$ também já está provado.

($\Leftarrow$) Indução na estrutura de π.

O caso base é exatamente o Lema da Existência para programas básicos, então:

Suponha que π tem a forma $\pi_1; \pi_2$, e além disso, suponha $\mathcal{A} R_{\pi_1;\pi_2} \mathcal{B}$ e $\psi \in \mathcal{B}$.

Então existe um átomo $\mathcal{C}$ tal que $\mathcal{A} R_{\pi_1} \mathcal{C}$ e $\mathcal{C} R_{\pi_2} \mathcal{B}$ e $\psi \in B$. Pelo Lema 2.2.1, $\langle \pi_2 \rangle \psi \in \neg FL(\Sigma)$, conseqüentemente, pela hipótese indutiva $\langle \pi_2 \rangle \psi \in \mathcal{C}$. Similarmente, como $\langle \pi_1 \rangle \langle \pi_2 \rangle \psi \in \neg FL(\Sigma)$, $\langle \pi_1 \rangle \langle \pi_2 \rangle \psi \in \mathcal{A}$.

Conseqüentemente, pelo Lema 2.2.1, $\langle \pi_1; \pi_2 \rangle \psi \in \mathcal{A}$ como exigido.

Suponha que $\mathcal{A} R_{\pi^*} \mathcal{B}$ e $\psi \in \mathcal{B}$. Isto significa que existe um seqüência finita de átomos $\mathcal{C}_0, \cdots, \mathcal{C}_n$ tal que $\mathcal{A} = \mathcal{C}_0 R_\pi \mathcal{C}_1, ..., \mathcal{C}_n R_\pi \mathcal{C}_{n+1} = \mathcal{B}$.

Por uma indução em n provamos que $\langle \pi^* \rangle \psi \in \mathcal{C}_i$ para todo i, o resultado exigido para $\mathcal{A} = \mathcal{C}_0$ é imediato deles.

Caso Base: $n = 0$

Isto significa $\mathcal{A} = \mathcal{B}$. Do axioma 5 temos que $\vdash \langle \pi^* \rangle \psi \leftrightarrow \psi \vee \langle \pi \rangle \langle \pi^* \rangle \psi$ e consequentemente que $\vdash \psi \rightarrow \langle \pi^* \rangle \psi$. Então, $\langle \pi^* \rangle \psi \in \mathcal{A}$.

Passo indutivo: Suponha que o resultado vale para $n \leq k$, e que

$$\mathcal{A} = \mathcal{C}_0 R_\pi \mathcal{C}_1, \cdots, \mathcal{C}_n R_\pi \mathcal{C}_{k+1} = \mathcal{B}$$

Pela hipótese indutiva, $\langle \pi^* \rangle \psi \in \mathcal{C}_1$. Conseqüentemente, $\langle \pi \rangle \langle \pi^* \rangle \psi \in \mathcal{A}$, para $\langle \pi \rangle \langle \pi^* \rangle \psi \in \neg FL(\Sigma)$. Mas, $\vdash \langle \pi^* \rangle \psi \leftrightarrow \psi \vee \langle \pi \rangle \langle \pi^* \rangle \psi$. Portanto, $\langle \pi^* \rangle \psi \in \mathcal{A}$.

Isto completa a subindução, e estabelece o resultado exigido para $\langle \pi^* \rangle$. E também completa a indução principal e portanto a prova do lema. □

Lema 2.2.9 (Lema da Verdade): *Seja $\mathcal{B}$ o modelo-LDP sobre Σ. Para todos os átomos $\mathcal{A}$ e todos $\psi \in \neg FL(\Sigma)$, $\mathcal{B}, \mathcal{A} \models \psi$ se e somente se $\psi \in \mathcal{A}$.*

Prova.: Indução no número de conectivos O caso base segue da definição de valoração canônica sobre Σ. O caso booleano segue do lema 2.2.1 das propriedades dos átomos. Finalmente, o Lema da Existência nos leva ao passo das modalidades no modo geral. ■

Teorema 2.2.1 : *LDP é fracamente completa com relação à classe de todos os frames-LDP.*

Prova.: Seja Σ um conjunto de fórmulas. Se Σ é consistente, pelo Lema de Lindenbaum, podemos estendê-lo para Σ^+ que é um MCS_s. Como $\Sigma \subseteq \Sigma^+$ então $\Sigma^+ \in At(\Sigma)$ e pelo Lema da Verdade se $\Sigma = \{\alpha_1, ..., \alpha_n\}$, $\alpha_i \in \Sigma^+$ se e somente se $\mathcal{M}, \Sigma^+ \models \alpha_i$, $\forall i$. Logo, $\mathcal{M}, \Sigma^+ \models \Sigma$. □

2.3 Lógica para CCS

Considere dois agentes CCS não equivalentes:

$$a \cdot 0 + \tau \cdot b \cdot 0 \neq a \cdot 0 + b \cdot 0$$

O primeiro agente é diferente do segundo agente porque ele pode evoluir silenciosamente para o agente $b \cdot 0$ que é incapaz de responder a ação a.

Geralmente, quando dois agentes não são equivalentes (no sentido forte ou fraco) queremos exibir uma propriedade que um agente tem, mas o outro não. Utilizaremos uma lógica modal (Hennessy-Milner), cujas fórmulas expressam propriedades de agentes. O poder diferenciador dessa lógica é limitado pela equivalência bissimulação: dois processos bissimilares tem as mesmas propriedades modais.

A propriedade *safety* (segurança) é *nada ruim nunca acontece*, enquanto que uma propriedade *liveness* (vivo) expressa *alguma coisa boa em algum momento acontece.*

A propriedade *safety* crucial de uma exclusão mútua é que nenhum dos dois processos estão sempre em suas seções críticas ao mesmo tempo. E uma propriedade importante de *liveness* é que sempre que um processo solicita execução em sua seção crítica então eventualmente é permitido.

Propriedades de sistemas cíclicos podem também ser expressas: Um exemplo é uma especificação CCS de um escalonador, ele deve realizar uma seqüência de ações $a_1, \ldots, a_n$ ciclicamente, iniciando em a_1.

2.3.1 Lógica de Hennessy-Milner

Processos de CCS geram sistemas de transição rotulados, estruturas que encapsulam seus procedimentos. Estes têm a forma:

$$(\mathcal{P}, \{\xrightarrow{a} | \ a \in \mathring{A}\})$$

onde,

$\mathcal{P}$ é um conjunto não vazio de agentes;

$\mathring{A}$ é um conjunto de ações;

$\xrightarrow{a}$ é a relação transição a para cada $a \in \mathring{A}$.

Lógicas modais são interpretadas em tais sistemas. Seja K um subconjunto de $\mathring{A}$, então a seguinte definição de sintaxe especifica fórmulas da lógica Hennessy-Milner (uma lógica modal particular):

$$\varphi = tt \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid [K]\varphi$$

onde,

Uma fórmula ou é a fórmula constante verdade tt ou é a negação de uma fórmula $\neg\varphi$, ou uma conjunção de fórmulas $\varphi_1 \wedge \varphi_2$, ou uma fórmula modalizada $[K]\varphi$ (φ é válida depois da execução de qualquer ação em K.)

Assuma um sistema de transição fixo $(\mathcal{P}, \{\xrightarrow{a} | \ a \in \mathring{A}\})$. Para qualquer fórmula φ da lógica Hennessy-Milner podemos definir quando um processo $E \in \mathcal{P}$ satisfaz a propriedade φ ($E \models \varphi$) e se E falha tendo a propriedade φ ($E \not\models \varphi$).

A relação satisfação $\models$ é definida indutivamente na estrutura das fórmulas abaixo:

1. $E \models tt$

2. $E \models \neg\varphi$ se e somente se $E \not\models \varphi$

3. $E \models \varphi \wedge \psi$ se e somente se $E \models \varphi$ e $E \models \psi$

4. $E \models [K]\varphi$ se e somente se $\forall E' \in \mathcal{P}\ \forall a \in K$ se $E \xrightarrow{a} E'$ então $E' \models \varphi$

Assim, podemos descrever as fórmulas acima do seguinte modo:

1. Todo processo em P tem a propriedade tt;

2. Um processo tem a propriedade $\neg\varphi$ quando ele não tem a propriedade φ;

3. Um processo tem a propriedade $\varphi \wedge \psi$ quando ele tem as propriedades φ e ψ;

4. Um processo satisfaz $[K]\varphi$ se depois de toda execução de qualquer ação em K, todo processo resultante tem a propriedade φ.

Temos o operador dual de $[K]$ que é $\langle K\rangle$:

$$\langle K\rangle\varphi \stackrel{\text{def}}{=} \neg[K]\neg\varphi$$

Este operador expressa: após uma execução de uma ação em K.

$$E \models \langle K\rangle\varphi \text{ se e somente se } \exists E' \in \mathcal{P}, \exists a \in K,\ E \xrightarrow{a} E' \text{ e } E' \models \varphi$$

Outros operadores que também são utilizados são a disjunção e a fórmula falsa (ff):

$$ff \stackrel{\text{def}}{=} \neg tt$$

$$\varphi \vee \psi \stackrel{\text{def}}{=} \neg(\neg\varphi \wedge \neg\psi)$$

Abaixo, temos algumas abreviações importantes:

$$[a_1, \ldots, a_n] \text{ para } [\{a_1, \ldots, a_n\}]$$

$$[-K] \text{ para } [\mathring{A} - K]$$

$$[-] \text{ para } [\mathring{A}]$$

Uma semântica alternativa da lógica Hennessy-Milner define indutivamente para cada fórmula B, o subconjunto $\|A\| \in \mathcal{P}$ tendo a propriedade A como segue:

$$\|tt\| = \mathcal{P}$$

$$\|\neg A\| = \mathcal{P} - \|A\|$$

$$\|A \wedge B\| = \|A\| \cap \|B\|$$

$$\|[K]A\| = \overline{[K]}\|A\|$$

$\overline{[K]}$ é o agente transformador para qualquer $\mathcal{P}' \subseteq \mathcal{P}$:

$$\overline{[K]}\mathcal{P}' = \{E \in \mathcal{P} | \, \forall E' \in \mathcal{P}, \forall a \in K \text{ se } E \xrightarrow{a} E' \text{ então } E' \in \mathcal{P}'\}$$

Claramente, $E \models A$ se e somente se $E \in \|A\|$. O agente transformador dual para $\overline{[K]}$, $\overline{\langle K \rangle}$, associado com $\langle K \rangle$, é definido como segue:

$$\overline{\langle K \rangle}\mathcal{P}' = \{E \in \mathcal{P} | \, \exists E' \in \mathcal{P}', \exists a \in K, E \xrightarrow{a} E'\}$$

2.3.2 Capacidade e Necessidade

Nesta seção veremos as classes de propriedades que são expressas com a lógica de Hennessy-Milner.

Primeiro considere a fórmula modal simples $\langle K \rangle tt$ que expressa uma *capacidade* de realizar uma ação em K:

$$E \models \langle K \rangle tt \text{ se e somente se } \exists E' \in \mathcal{P} \exists a \in K E \xrightarrow{a} E'$$

Agora considere a fórmula $[K]ff$ que expressa *incapacidade* de realizar qualquer ação em K. K expressa *deadlock* quando ele é igual ao conjunto de ações $\mathring{A}$, ou seja, ele expressa incapacidade de realizar qualquer ação.

Exemplo 2.3.2.1 : *Considere uma máquina de vender cartões telefônicos. Suponha que um cartão com 60 unidades custe 5,00 reais e um cartão com 20 unidades custe 1,00 real, e somente essas notas podem ser usadas.*

$$V = 5r \cdot 60u \cdot Retirar \cdot V + 1r \cdot 20u \cdot Retirar \cdot V$$

$$V \models \langle 5r \rangle tt$$

(V pode aceitar 5,00 reais, mas um botão não pode ser apertado antes que o dinheiro seja depositado), portanto

$$V \models [60u, 20u]ff$$

$$V \models [5r]([20u]ff \wedge \langle 60u \rangle tt)$$

(Depois que $5r$ *é depositado o botão* $20u$ *não pode ser apertado, já o botão* $60u$ *pode ser apertado.)*

$$V \models [5r, 1r][5r, 1r]ff$$

(Depois que uma nota é depositada nenhuma outra nota (5r ou 1r) pode ser depositada.)

$$V \models [60u, 20u]\langle Retirar \rangle tt$$

(Depois que uma nota é depositada e o botão é apertado, um cartão pode ser retirado.)

Podemos provar a seguinte propriedade:

$V \models [5r]([20u]ff \wedge \langle 60u\rangle tt)$ *se e somente se*

$60u \cdot Retirar \cdot V \models [20u]ff \wedge \langle 60u\rangle tt$

como $\{60u \cdot Retirar \cdot V\} = \{E \mid V \xrightarrow{5r} E\}$ *se e somente se*

$60u \cdot Retirar \cdot V \models [20u]ff$ *e*

$60u \cdot Retirar \cdot V \models \langle 60u\rangle tt$

Observamos que $60u \cdot Retirar \cdot V$ *é capaz de realizar* $60u$*, mas não é capaz de realizar* $20u$*.*

Note que não é necessário computar, ou mesmo conhecer o sistema de transição para V *no processo de checagem de uma propriedade. A prova acima permanece válida para qualquer máquina de venda* V *na seguinte forma:*

$$V \stackrel{\text{def}}{=} 5r \cdot 60u \cdot E_1 + 1r \cdot 20u \cdot E_2$$

Ações nos operadores modais podem conter valores como, por exemplo, a célula simples abaixo:

$$C \stackrel{\text{def}}{=} in(x) \cdot \overline{out}(x) \cdot C$$

tem a propriedade $[in(v)]\langle\overline{out}(v)\rangle tt$.

Exemplo 2.3.2.2 *: Seja uma célula simples que entra um número* x *e sai o seu quadrado,* $x \in N$*.*

$$SQ \stackrel{\text{def}}{=} in(x) \cdot \overline{out}(x^2) \cdot SQ$$

Fazendo a verificação para $x = 3$ *temos:*

$$SQ = [in(3)] \cdot \langle \overline{out}(9) \rangle tt$$

A lógica modal pode expressar *necessidade* também. A propriedade que E pode apenas realizar a ação a, é dada por:

$$E \models \langle - \rangle tt \wedge [-a] ff$$

onde,

$\langle - \rangle tt$ afirma que alguma ação pode acontecer.

$[-a] ff$ diz que qualquer ação além de a é impossível.

Exemplo 2.3.2.3 : *A propriedade modal* $A = \langle\langle \varepsilon \rangle\rangle [[a]] ff$ *diferencia os dois agentes abaixo:*

$$a \cdot 0 + \tau \cdot b \cdot 0 \models A$$

$$a \cdot 0 + b \cdot 0 \not\models A$$

Uma segunda lógica modal nos permite expressar capacidades e incapacidades de agentes para realizar ações com respeito às relações de transição $\Rightarrow$.

Podemos definir, por exemplo, a propriedade de existir *deadlock* (incapacidade de realizar uma ação observável):

$$Deadlock \stackrel{\text{def}}{=} [[-\varepsilon]] ff$$

Para expressar *necessidade* precisamos saber o seguinte:

Qualquer agente E tem a propriedade $\langle\langle - \rangle\rangle tt$ porque $E \stackrel{\varepsilon}{\Rightarrow} E$. Pela mesma razão nenhum agente tem a propriedade $[[-a]] ff$ quando a é observável.

Para fazer a representação que E deve realizar a, podemos tentar através da fórmula abaixo:

$$\langle\langle -\varepsilon \rangle\rangle tt \wedge [[-\{a, \varepsilon\}]] ff$$

2.4 Comunicação em Lógica Dinâmica de Concorrência

Neste capítulo apresentamos uma linguagem lógica e o modelo correspondente que permite representar comunicação entre dois processos executando em paralelo - *channel - Concurrent Propositional Dynamic Logic (channel-CPDL)*, proposta por David Peleg em [PEL87b].

channel-CPDL é uma dentre as extensões da Lógica Dinâmica Proposicional Concorrente (Concurrent Propositional Dynamic Logic-CPDL) que visam incorporar mecanismos de comunicação aos programas concorrentes.

2.4.1 Lógica Dinâmica Proposicional Concorrente

Lógica Dinâmica de Concorrência (CDL) foi introduzida por [PEL87b] como uma extensão de lógica dinâmica regular que tenta prover uma estrutura para raciocínio sobre programas concorrentes no modelo *and/or*.

Um dos modelos mais estudados de computação concorrente é aquele da árvore *and/or*. Esta visão analisa concorrência na sua forma mais pura através da noção dual de não determinismo.

Podemos mostrar um processo no modelo *and/or* através de uma árvore cujos arcos representam ações atômicas. Não determinismo é introduzido pela permissão de um nó que possui várias ramificações, mas requer que o processo execute todas as possíveis continuações em paralelo. Este é o conceito clássico de decomposição *and/or* que ocorre em computabilidade, lógica, teoria dos jogos, etc.

Sintaxe

A sintaxe é aquela de LDP com a adição de um operador de concorrência $\cap$ nos programas.

Definição 2.4.1 : *Seja* $\Phi = \{P_1, ..., P_n\}$ *um conjunto de fórmulas atômicas e* $\Psi = \{a_1, ..., a_n\}$ *um conjunto de programas atômicos:*

1. *Todo* P_i *é uma fórmula;*
2. *Se* A *e* B *são fórmulas e* α *é uma programa então* $A \vee B$, $\neg A$ *e* $\langle\alpha\rangle A$ *são fórmulas;*
3. *Todo* a_i *é um programa;*
4. *Se* α *e* β *são programas e* A *é uma fórmula, então* $\alpha \cup \beta$, $\alpha \cap \beta$, $\alpha;\beta$, α^* *e* $A?$ *são programas.*

Semântica

Definição 2.4.2 : *Um modelo para CPDL é uma tripla* $\mathcal{M} = \langle S, \pi, \rho\rangle$, *onde:*

- S *é um conjunto de estados;*
- π *interpreta um subconjunto* $\pi(P)$ *de* S *para toda fórmula atômica* P *e*
- ρ *interpreta um subconjunto* $\rho(a)$ *de* $S \times 2^S$ *para todo programa atômico* a.

Intuitivamente, $(s, U) \in \rho(\alpha)$ para $s \in S$ e $U \subseteq S$ se α pode ser executado de s e alcançar todos os estados de U em paralelo. Então a fórmula $\langle\alpha\rangle A$ vale num estado s se e somente se existe um conjunto $U \subseteq S$ tal que $(s, U) \in \rho(\alpha)$ e cada estado em U satisfaz A.

Definição 2.4.3 : *Extensão de π e ρ para fórmulas e programas através das regras seguintes:*

$\pi(A \vee B) = \pi(A) \cup \pi(B)$,

$\pi(\neg A) = S - \pi(A)$,

$\pi(\langle\alpha\rangle A) = \{s \mid \exists U((s,U) \in \rho(\alpha) \wedge U \subseteq \pi(A))\}$ *e*

$\rho(A?) = \{(s,\{s\}) \mid s \in \pi(A)\}$,

$\rho(\alpha \cup \beta) = \rho(\alpha) \cup \rho(\beta)$,

$\rho(\alpha \cap \beta) = \{(s,U) \mid \exists V,W((s,V) \in \rho(\alpha) \wedge (s,W) \in \rho(\beta) \wedge U = V \cup W)\}$,

$\rho(\alpha;\beta) = \rho(\alpha).\rho(\beta)$,

$\rho(\alpha^*) = min\{R \mid R \subseteq S \times 2^S \wedge R = \rho(true?) \cup \rho(\alpha).R\}$,

onde $R_1.R_2$ *é definido (para qualquer* $R_1, R_2 \subseteq S \times 2^S$*) como*

$\{(s,U) \mid \exists s_1,U_1,s_2,U_2,...((s,\{s_1,s_2,...\}) \in R_1 \wedge \forall i(s_i,U_i) \in R_2 \wedge U = \bigcup_i U_i)\}$

A definição de $\langle\alpha\rangle A$ diz que existe uma computação de α tal que A vale em todos os seus estados finais. Uma escolha alternativa poderia fazer $\langle\alpha\rangle A$ sempre que existe uma computação de α tal que A é verdadeira em algum dos estados finais.

2.4.2 Modelo de Computação em Árvore

Veremos uma construção equivalente para interpretação ρ de programas, baseada na noção de uma trec ou computação tipo árvore. Esta construção provê as bases técnicas para estender CDL para trabalhar com comunicação.

Definição 2.4.4 : *Uma seq é um programa LDP (determinístico) que não contém* $\cup$ *ou* $*$*, isto é, uma seqüência de programas atômicos e testes concatenados.*

A função de *trecs* em programas concorrentes é análoga das *seqs* em programas regulares. Uma *trec* descreve uma execução determinística específica de um programa que pode ser ou não concorrente.

Definição 2.4.5 : *Uma trec ou uma árvore de computação é um programa CPDL que não possui* $\cup$ *ou* $*$.

O conjunto de *trecs* pode ser definido como o fecho de programas atômicos e testes sob concatenação e $\cap$.

Definição 2.4.6 : *Uma trec* α *é dita estar na forma de árvore se é definida indutivamente da seguinte forma:*

1. *true?* *é uma trec,*
2. *se* α *e* β *são trecs,* a *é uma programa atômico e* A *é uma fórmula, então* $\alpha \cap \beta$, $a;\alpha$ *e* $A?;\alpha$ *são trecs.*

Uma *trec* na forma de árvore pode ser representada como uma árvore cujos arcos são rotulados pelos programas atômicos e testes da *trec* e cada $\cap$ corresponde a uma divisão em dois ramos. As folhas desta árvore correspondem aos estados finais dos diferentes processos paralelos gerados pela *trec*.

Toda trec pode ser transformada para forma de árvore. Por exemplo, se α e β estão na forma de árvore então $\alpha;\beta$ pode ser transformada para forma de árvore pela junção da árvore de representação β a toda folha da árvore de representação α. Isto corresponde a aplicação repetida da seguinte regra de transformação:

$$(\theta \cap \gamma);\delta \Rightarrow \theta;\delta \cap \gamma;\delta$$

Note que esta regra é válida para programas CPDL em geral e também com $\cup$ em vez de $\cap$. Porém, se δ é uma folha então ambas as transformações não são verdadeiras. Conseqüentemente, uma trec não pode ser decomposta em um conjunto de seqs paralelas separadas completamente.

A semântica de um programa α (não determinístico) PDL sequencial pode ser definida com base num conjunto $\tau(\alpha)$ de seq (determinístico), descrevendo as possíveis execuções de α tal que $\rho(\alpha) = \bigcup_{\beta \in \tau(\alpha)} \rho(\beta)$.

Analogamente, a semântica de um programa concorrente α (não determinístico) pode ser baseada numa coleção de trecs (determinísticas). Todo programa α está associado com um conjunto de trecs $\tau(\alpha)$ representando todas as suas possíveis execuções.

Definição 2.4.7 : *O conjunto de trecs $\tau(\alpha)$ de um programa α é definido por:*

1. $\tau(a_i) = \{a_i\}$, *para programas atômicos* a_i,

2. $\tau(A?) = \{A?\}$, *para testes* $A?$,

3. $\tau(\alpha \cup \beta) = \tau(\alpha) \cup \tau(\beta)$,

4. $\tau(\alpha \cap \beta) = \{\gamma \cap \delta \mid \gamma \in \tau(\alpha) \text{ e } \delta \in \tau(\beta)\}$,

5. $\tau(\alpha;\beta) = \{\theta \mid \exists \gamma, \delta_1, ..., \delta_k (\gamma \in \tau(\alpha), \delta_1, ..., \delta_k \in \tau(\beta),$ *γ tem k folhas e θ é obtido pela atribuição de cada δ_i a uma das folhas de γ*$), k > 0\}$,

6. $\tau(\alpha^*)$ *é o conjunto minimal construído pelas seguintes regras:*

   a. $true? \in \tau(\alpha^*)$

   b. *Para todo γ, δ e θ, se $\gamma \in \tau(\alpha^*)$, $\delta \in \tau(\alpha)$ e θ é obtido pela junção de δ a uma das folhas de γ, então $\theta \in \tau(\alpha^*)$ também.*

Note que $\tau(\alpha)$ contém somente *trecs* na forma de árvore,e para qualquer *trec* α, $\tau(\alpha)$ contém alguma forma de árvore equivalente a α.

2.4.3 Channel-CPDL

Na semântica de *trecs*, um programa CPDL pode ser descrito como uma árvore onde não existem ligações entre os ramos. A execução de um programa CPDL se inicia em um certo estado comum s, mas uma vez que se divide em dois ou mais processos paralelos, esses processos avançam separadamente, sem sincronização ou ligação.

Não podemos fazer uso de uma semântica de programas como esta para viabilizar a comunicação entre processos, tendo em vista que deve existir alguma ligação entre os diferentes ramos. Conseqüentemente, é interessante considerar super-estados representando cortes na árvore de computação e as definições semânticas referem-se simultâneamente a todos os estados no corte e todos os programas operando em diferentes ramos.

As principais funções a serem exercidas na comunicação num ambiente concorrente podem ser caracterizadas como:

1. Sincronização de processos;
2. Troca de informação entre processos;
3. Transmissão de informações, mensagens e resultados finais para algum processo principal.

A comunicação em *channel-CPDL* é feita através de canais estabelecidos entre dois processos, de forma bem próxima ao que ocorre em várias linguagens concorrentes. A notação utilizada á parecida com aquela usada no CCS [MIL89].

Dadas as necessidades de interação entre processos de ramos distintos em uma *trec*, [PEL87b] propõe para *channel-CPDL* uma semântica de super-estados. Os super-estados representam cortes transversais na árvore de computação. As definições semânticas envolvem simultâneamente todos os estados no corte e todos os programas operando em diferentes ramos.

Os cortes representam conjuntos de estados locais, sendo que qualquer configuração de estados é permitida, desde que restrições de sincronismo impostas pelos mecanismos de comunicação não sejam violadas.

Sintaxe de Channel-CPDL

Definição 2.4.8 *: A sintaxe é baseada em CPDL, com as seguintes adições para a comunicação:*

- *A linguagem tem uma coleção de canais* $\{C_i\}$,
- *Em adição a programas atômicos e testes, as seguintes operações atômicas são permitidas:*

  $C!0(resp.C!1) \Rightarrow$ *transmite 0 (resp.1) sobre o canal* C

  $C?0(resp.C?1) \Rightarrow$ *recebe 0 (resp.1) sobre o canal* C

As operações $C!0$, $C!1$ correspondem respectivamente ao envio de um bit com valor 0 e envio de um bit com valor 1 através do canal C. Analogamente, as operações $C?0$, $C?1$ correspondem ao recebimento de um bit com valor 0 ou 1 em C. Para que um processo possa realizar uma operação de envio é necessário que outro processo realize simultaneamente a respectiva operação de recebimento.

Como cada canal de comunicação C liga apenas dois processos, então quando uma operação de comunicação é realizada, sincroniza dois processos envolvidos, se um processo tenta realizar a ação de envio antes de o respectivo processo destinatário da mensagem a ação de recebimento, o primeiro fica bloqueado aguardando que o segundo faça o recebimento da mensagem e vice-versa.

Os comandos de comunicação podem ser usados por um processo para transferir, por exemplo, o valor de um predicado P no seu estado corrente (pela execução de $P?; C!1 \cup (\neg P)?; C!0$) e em um outro processo onde pode-se tomar uma decisão com base na mensagem enviada (pela execução de $C?0; \alpha \cup C?1; \beta$).

Semântica de Channel-CPDL

Uma definição formal da semântica de channel-CPDL é mais complexa se comparada àquela de CPDL, como um resultado de ter que trabalhar simultâneamente com super estados (conjunto de estados simultâneos) ao invés de trabalhar cada ramo de execução separadamente.

Esta restrição é uma consequência da introdução dos operadores de comunicação, que por serem realizados simultâneamente impedem que sua avaliação seja feita em separado sem introduzir novos objetos semânticos. Se existem canais em comum entre diferentes ramos, pode ser que haja estados a partir dos quais os programas não possam ser executados em separado. Assim sendo, é necessário que as regras semânticas considerem os processos concorrentes que estejam sendo executados em paralelo. Isto é feito através de super-processos.

O modelo para *channel-CPDL* provê uma interpretação $\rho(a) \subseteq S \times 2^S$ para programas atômicos a , por isso nos limitamos a modelos sequenciais [PEL87a]. Essa definição tem que ser estendida para super processos. Usamos a seguinte notação:

Um super estado é denotado por $\overline{s} = [s_1 \mid ... \mid s_n]$

- quando $n = 1$ identificamos s_1 com $[s_1]$,

- quando $\overline{s}$ é conhecido podemos nos referir a uma porção dele por $[s_i \mid ... \mid s_{i+k}]$ como $\overline{s}(i, i+k)$,

- dois super estados podem ser combinados para formar um super estado maior. Isto é denotado por $[s_1 \mid ... \mid s_n] \mid [q_1 \mid ... \mid q_n] = [s_1 \mid ... \mid s_n \mid q_1 \mid ... \mid q_n]$,

- o tamanho de $\overline{s}$, denotado por $\mid \overline{s} \mid$, é o número n de estados paralelos em $\overline{s}$.

Um super processo é denotado por $\overline{\alpha} = [\alpha_1 \mid ... \mid \alpha_n]$

- podemos descrever uma porção dele por $\overline{\alpha}(i, i+k)$,

- identificamos α_1 com $[\alpha_1]$,

- um super processo $\overline{\alpha} = [\alpha_1 \mid ... \mid \alpha_n]$, $\rho(\overline{\alpha}) \subseteq S^n \times (\bigcup_{i>=n} S^i)$, isto é, $\rho(\overline{\alpha})$ consiste de tuplas $(\overline{s}, \overline{s}')$ com $\mid \overline{s} \mid = n$ e $\mid \overline{s}' \mid \geq n$

Conservamos a natureza da árvore em programas determinísticos, as *trecs*, e a forma de decomposição de programas gerais em *trecs*. Assim, temos as transformações descritas na seção 6.3, incluindo:

1. $(\theta \cap \gamma); \delta \Rightarrow \theta; \delta \cap \gamma; \delta$ e

2. $(\theta \cup \gamma); \delta \Rightarrow \theta; \delta \cup \gamma; \delta$

Primeiro definimos o conjunto de *trecs* $\tau(\alpha)$ associado a cada programa α. Em seguida, definimos $\rho(\overline{\alpha})$ para um super processo $\overline{\alpha}$ consistindo somente de *trecs* na forma de árvore.

Neste ponto, a interpretação semântica das operações do canal de comunicação

obrigam algumas conexões de sincronização entre ramos separados das *trecs*, portanto esses ramos não são mais independentes e as *trecs* perdem sua natureza árvore.

1. $\rho(true?) = \{(s, s) \mid s \in S\}$.

2. Se $\alpha_i = a.\beta, (s_i, s') \in \rho(a)$ e $(\overline{s}(1, i-1) \mid s' \mid (\overline{s}(i+1, n), \overline{r}) \in \rho((\overline{\alpha}(1, i-1) \mid \beta \mid (\overline{\alpha}(i+1, n))$ então $(\overline{s}, \overline{r}) \in \rho(\overline{\alpha})$.

3. Se $\alpha_i = C!1; \beta_1$, $\alpha_j = C?1; \beta_2$, $j > i$ e $(\overline{s}, \overline{r}) \in \rho(\overline{\alpha}(1, i-1) \mid \beta_1 \mid \overline{\alpha}(i+1, j-1) \mid \beta_2 \mid \overline{\alpha}(j+1, n))$ então $(\overline{s}, \overline{r}) \in \rho(\overline{\alpha})$.

   Similarmente, quando $j < i$, e quando a mensagem é 0 (zero) em ambos os lados.

4. Se $\alpha_i = A?; \beta$, $s_i \in \pi(A)$ e $(\overline{s}, \overline{r}) \in \rho(\overline{\alpha}(1, i-1) \mid \beta \mid \overline{\alpha}(i+1, n))$ então $(\overline{s}, \overline{r}) \in \rho(\overline{\alpha})$.

5. Se $\alpha_i = \beta \cap \gamma$ e $(\overline{s}(1, i-1) \mid s_i \mid s_i \mid \overline{s}(i+1, n), \overline{r}) \in \rho(\overline{\alpha}(1, i-1) \mid \beta \mid \gamma \mid \overline{\alpha}(i+1, n))$ então $(\overline{s}, \overline{r}) \in \rho(\overline{\alpha})$.

Para todo $\overline{\alpha}$, $\rho(\overline{\alpha})$ contém precisamente aqueles pares $(\overline{s}, \overline{r})$ introduzidos pelas regras acima.

A definição de ρ é estendida para qualquer super processo $\overline{\alpha}$ por

$$\rho([\alpha_1 \mid ... \mid \alpha_n]) = \bigcup_{\beta_i \in \tau(\alpha_i)} \rho([\beta_1 \mid ... \mid \beta_n])$$

A interpretação de fórmulas tem que ser modificada de acordo com:

$$\pi(\langle\alpha\rangle A) = \{s' \mid \exists \overline{s}(\overline{s} = [s_1 \mid ... \mid s_n], (s', \overline{s}) \in \rho(\alpha) \text{ e } \forall i, 1 \leq i \leq n(s_i \in \pi(A)))\}$$

A definição da semântica de programas apresentada em *channel-CPDL* difere daquela dada para programas concorrentes sem comunicação (CPDL).

Em *channel-CPDL* interpretamos a execução de programa como partindo de um único estado para um multiconjunto de estados. Assim, permitimos que um programa a se divida e atinja dois ou mais estados em sua execução. A escolha de diferentes semânticas porém não afeta a interpretação de formúlas. É possível demonstrar que:

Se $tt = true? \cap true?, \alpha = tt; a$ e $\rho(a) = \{(s_0, s_1), (s_0, s_2)\}$.

Então pelas regras anteriores, temos:

$$\rho(tt) = \rho(true?) \text{ e } \rho(\alpha) = \{(s_0, \{s_1\}), (s_0, \{s_2\})\}$$

enquanto que, de acordo com a interpretação de multiconjuntos, temos:

$$\rho_{mult}(\alpha) = \{(s_0, [s_1 \mid s_1]), (s_0, [s_1 \mid s_2]), (s_0, [s_2 \mid s_1]), (s_0, [s_2 \mid s_2])\}$$

O que significa a possibilidade de α se dividir e alcançar dois estados diferentes.

1. $\rho(\alpha) \subseteq \rho_{mult}(\alpha)$ para todo programa α (identificando como um multiconjunto U com o conjunto $set(U)$, consistindo precisamente de seus elementos) e,

2. $(s, U) \in \rho_{mult}(\alpha) \Rightarrow \exists U' (U' \subseteq set(U), (s, U') \in \rho(\alpha)$, para todo programa α.

Esas duas observações servem para provar que para qualquer fórmula A, $\pi(A) = \pi_{mult}(A)$.

Para essa interpretação de fórmulas devemos notar que na semântica dois programas α e β em contextos separados ($\langle\alpha\rangle A$ e $\langle\beta\rangle B$) estão totalmente desligados e nenhuma comunicação é possível entre eles. Além disso, mesmo a fórmula anexada A não tem nenhum modo de se referir ao canal α, e o mesmo se aplica para testes em α. Isto significa, que axiomas CPDL válidos, tais como:

$\langle \alpha \cap \beta \rangle A \equiv \langle \alpha \rangle A \wedge \langle \beta \rangle A$ e

$\langle \alpha ; \beta \rangle A \equiv \langle \alpha \rangle \langle \beta \rangle A$

não valem mais em channel-CPDL. Por exemplo,

$\langle C!0 \cap C?0 \rangle true$ é sempre verdade, enquanto que $\langle C!0 \rangle true \wedge \langle C?0 \rangle true$ é sempre falso.

Os dois exemplos a seguir foram retirados de [PEL87b].

Exemplo: Contagem de folha

Seja a fórmula,

$$even_1 : \langle ((a \cap b)^* ; leaf? ; ((\neg P)? \cup (P? ; C!1))) \cap (C?1 ; C?1)^* \rangle true$$

onde,

$$leaf : \neg \langle a \cup b \rangle true$$

Considerando modelos na forma de árvores binárias finitas completa a/b (onde cada nó tem apenas zero ou dois ramos, a e b), a fórmula $even_1$ contempla exatamente os modelos nos quais existe um número par de folhas satisfazendo P.

O programa principal de $even_1$ se divide em vários processos paralelos, um para cada ramo da árvore. Cada um desses processos compartilha uma folha, teste P, e envia uma mensagem se P é verdade. Um processo separado recebe essas mensagens e computa a paridade do número de mensagens recebidas.

Para calcular as árvores binárias parciais, isto é, nas quais um nó pode ter um filho, substituimos o subprograma $(a \cap b)^*$ por:

$$((\langle a\rangle true \wedge \langle b\rangle true)?; (a \cap b)$$

$$\cup(\langle a\rangle true \wedge \neg\langle b\rangle true)?; a$$

$$\cup(\neg\langle a\rangle true \wedge \langle b\rangle true)?; b)^*$$

Este programa, quando aplicado a uma árvore binária finita a/b, conta o número dos diferentes caminhos levando até as folhas que satisfazem P.

Considere o modelo abaixo:

Figura 2.14:

onde, em cada estado, exatamente um dos arcos é denotado por a e um por b.

Estes exemplos demonstram processos independentes enviando mensagens (relatórios de execução) para um processo de contagem principal.

Exemplo: Problema da Correspondência de Post - (PCP)

Este exemplo é baseado nas idéias usadas em [DHS83], que mostra a indecibilidade de LDP + $\{\alpha^i\beta\gamma^i \mid i \geq 0\}$, pela redução ao Problema da Correspondência de Post (PCP) ao seu problema de satisfabilidade.

Os modelos considerados neste exemplo são cada um na forma de um caminho finito $p_{\mathcal{M}} = (s_0, s_1, ..., s_m)$ conectados por um programa atômico a com um predicado atômico P interpretado sobre os estados do modelo.

Cada modelo $\mathcal{M}$ representa uma palavra $z_{\mathcal{M}} = \sigma_1...\sigma_m$ para cada $1 \leq i \leq m$, $\sigma_i = 1$ se $s_i \models P$, caso contrário $\sigma_i = 0$.

Sejam $\tilde{x} = (x_1, ..., x_m)$, $\tilde{y} = (y_1, ..., y_m)$, instâncias PCP. Construiremos uma

fórmula *channel-CPDL* $correspond_{\tilde{x},\tilde{y}}$, que é satisfeita no modelo $\mathcal{M}$ se e somente se a palavra representada $z_{\mathcal{M}}$ é uma solução para a instância PCP $(\tilde{x}, \tilde{y})$ dada.

A fórmula $correspond_{\tilde{x},\tilde{y}}$ dispara dois processos, um para achar e verificar a x-partição da palavra e outro para a y-partição da palavra. Os processos usam canais C_i, $(1 \leq i \leq n)$, nessa ordem, para forçar as aplicações simultâneas de palavras x_i e y_i.

A fórmula $correspond_{\tilde{x},\tilde{y}}$ é construída como segue:

Para qualquer palavra $x_i = w_{i,1}...w_{i,n_i}$ construa um programa $\alpha_i = a_{i,1}; ...; a_{i,n_i}; C_i!1$, onde

$$a_{i,j} = \begin{cases} a; P?, & w_{i,j} = 1 \\ a; (\neg P)?, & w_{i,j} = 0 \end{cases}$$

Para qualquer palavra $y_i = v_{i,1}...v_{i,n_i}$, construa um programa $\beta_i = b_{i,1}; ...; b_{i,n_i}; C_i!1$.

Seja

$$\alpha = (\bigcup_{1 \leq i \leq n} \alpha_i)^*$$

e

$$\beta = (\bigcup_{1 \leq i \leq n} \beta_i)^*$$

Assim, definimos

$$correspond_{\tilde{x},\tilde{y}} : \langle \alpha \cup \beta \rangle leaf$$

$correspond_{\tilde{x},\tilde{y}}$ declara que α e β podem ser executados em paralelo no caminho $p_{\mathcal{M}}$ o que implica que $p_{\mathcal{M}}$ pode ser decomposto em k partes correspondendo a uma sequência de k palavras x_i, e alternativamente, em k partes correspondendo a uma sequência de k palavras y_i, com mesmos índices. Isto significa que o modelo, de fato, representa uma solução para a instância PCP dada.

Decidibilidade

O exemplo acima pode ser usado para provar que o problema da validade para *channel-CPDL* é indecídivel, por uma redução para o Problema da Correspondência de Post (PCP).

Para uma dada instância PCP, podemos construir uma fórmula *channel-CPDL* $pcp_{x,y}$ que é satisfatível se e somente se a dada instância tem solução. Especificamente, é necessário forçar o modelo para ser da forma desejada de um caminho simples (ou vários isomorfos) e então declarar $correspond_{\tilde{x},\tilde{y}}$.

Portanto, a capacidade de sincronizar dois processos paralelos torna o problema da validade de *channel-CPDL* indecídivel.

Capítulo 3

Lógica Dinâmica Proposicional para Programas CCS

3.1 Introdução

No capítulo anterior apresentamos uma lógica para CCS (Lógica de Henessy-Milner) e a lógica dinâmica proposicional. A partir desses dois estudos propomos neste capítulo uma Lógica Dinâmica Proposicional para Programas CCS (LDP-CCS) usando os operadores do CCS. Os operadores serão inseridos um a um mostrando a sintaxe, a semântica, o esquema de axiomas, as provas de corretude e completude.

3.2 Linguagem e Modelos

Definição 3.2.1 : *A linguagem de* **LDP-CCS com Composição Paralela com Sincronização** *consiste de um conjunto* Φ *de símbolos proposicionais,* $\Phi = \{p, q, ...\}$, *um conjunto de nomes* $\mathring{A} = \{a, b, ...\}$, *um conjunto de co-nomes* $\overline{\mathring{A}} = \{\overline{a}, \overline{b}, ...\}$, *um conjunto de ações* $Act = \mathring{A} \cup \overline{\mathring{A}} \cup \{\tau\}$, *uma família de operadores modais* $[\,]$ *e dois operadores CCS:* $\cdot$, $+$ *e* $|$. *As fórmulas são definidas como segue:*

$$\varphi ::= p \mid \bot \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \rightarrow \varphi_2 \mid \neg\varphi \mid [K]\varphi \mid [E]\varphi$$

$$\alpha ::= a \mid \overline{a} \mid \tau$$

$E ::= 0 \mid \alpha \cdot E \mid E_1 + E_2 \mid E_1 \mid E_2$

onde,

$K \subseteq Act.$

Definição 3.2.2 : *Um* **frame** *para a LDP-CCS é* $\mathcal{F} = (W, Z, R_\alpha, R_E)$ *onde:*

W *é um conjunto não vazio de estados;*

Z *é um conjunto de estados finais,* $Z \subseteq W$, *onde*

$$\forall \alpha \in Act \; e \; \forall w (w \in Z \Leftrightarrow \neg \exists w', wR_\alpha w')$$

R_α *é uma relação binária para cada programa básico* α ;

R_E *é uma relação binária para cada programa* E, *onde:*

$R_{\alpha \cdot E} = R_\alpha ; R_E$

$R_{E_1 + E_2} = R_{E_1} \cup R_{E_2}$

$R_0 = \{(x, x) \mid x \in Z\}$

$R_{E_1 | E_2}$ *satisfaz as seguintes condições:*

i. $R_{E_1|E_2} = R_{E_2|E_1}$ *(comutativa)*

ii. $R_{(E_1|E_2)|E_3} = R_{E_1|(E_2|E_3)}$ *(associativa)*

iii. $R_{E|0} = R_E$

iv. $R_{(E_1+E_2)|E_3} = R_{(E_1|E_3)+(E_2|E_3)}$

v. $R_{(\alpha.E_1)|E_2} \supseteq R_{\alpha.(E_1|E_2)}$

vi. $R_{(\alpha_1.E_1)|(\alpha_2.E_2)} = R_{\alpha_1.(E_1|\alpha_2.E_2)+\alpha_2.(\alpha_1.E_1|E_2)}$

vii. $R_{((\alpha.E_1)|(\overline{\alpha}.E_2))} = R_{\alpha.(E_1|\overline{\alpha}.E_2)+\overline{\alpha}.(\alpha.E_1|E_2)+\tau.(E_1|E_2)}$

Definição 3.2.3 : *Um* **modelo** *para a LDP-CCS com Composição Paralela com Sincronização é* $\mathcal{M} = (W, S, R_\alpha, R_E, V)$, *onde* V *é uma função valoração mapeando símbolos proposicionais em subconjuntos de* W.

Definição 3.2.4 : *Seja* $\mathcal{M} = (W, Z, R_\alpha, R_E, V)$ *um modelo e* $w \in W$. *Definimos a noção de* **satisfação** *de uma fórmula* φ *num modelo* $\mathcal{M}$ *em um estado* w, $\mathcal{M},w \models \varphi$, *pode ser definida indutivamente como segue:*

1. $(\mathcal{M},w) \models p$ *se e somente se* $p \in V(p)$.
2. $(\mathcal{M},w) \models \bot$ *se e somente se* $w \in W$.
3. $(\mathcal{M},w) \models \neg\varphi$ *se e somente se* $(\mathcal{M},w) \not\models \varphi$.
4. $(\mathcal{M},w) \models \varphi_1 \wedge \varphi_2$ *se e somente se* $(\mathcal{M},w) \models \varphi_1$ *e* $(\mathcal{M},w) \models \varphi_2$.
5. $(\mathcal{M},w) \models [K]\varphi$ *se e somente se* $\forall w' \in W$ *e* $\forall \alpha \in K$, *se* $wR_\alpha w'$ *então* $(\mathcal{M},w') \models \varphi$.
6. $(\mathcal{M},w) \models [E]\varphi$ *se e somente se* $\forall w' \in W$, *se* $wR_E w'$ *então* $(\mathcal{M},w') \models \varphi$.

Se $(\mathcal{M},w) \models \varphi$ para todo estado w, dizemos que φ é válido no modelo $\mathcal{M}$, $\mathcal{M} \models \varphi$. E se φ é válida em todos os modelos $\mathcal{M}$, dizemos que φ é válida, $\models \varphi$.

3.3 Axiomatização

1. todas as tautologias
2. $[K](\varphi \rightarrow \psi) \rightarrow [K]\varphi \rightarrow [K]\psi$
3. $[E](\varphi \rightarrow \psi) \rightarrow [E]\varphi \rightarrow [E]\psi$

4. $[\alpha \cdot E]\varphi \leftrightarrow [\alpha][E]\varphi$

5. $[E_1 + E_2]\varphi \leftrightarrow [E_1]\varphi \wedge [E_2]\varphi$

6. $[0 + E_1]\varphi \rightarrow [E_1]\varphi$

7. $\varphi \wedge [\mathring{A}]\bot \rightarrow \langle 0\rangle\varphi$ (reflexividade de R_0)

8. $[\mathring{A}]\bot \wedge \langle 0\rangle\varphi \rightarrow [0]\varphi$ (R_0 é funcional)

9. $[\mathring{A}]\bot \leftrightarrow \langle 0\rangle\top$

10. $[E_1 \mid E_2]\varphi \leftrightarrow [E_2 \mid E_1]\varphi$

11. $[(E_1 \mid E_2) \mid E_3]\varphi \leftrightarrow [E_1 \mid (E_2 \mid E_3)]\varphi$

12. $[E \mid 0]\varphi \leftrightarrow [E]\varphi$

13. $[(E_1 + E_2) \mid E_3]\varphi \leftrightarrow [(E_1 \mid E_3) + (E_2 \mid E_3)]\varphi$

14. $[\alpha.(E_1 \mid E_2)]\varphi \rightarrow [(\alpha.E_1) \mid E_2]\varphi$

15. $[(\alpha_1.E_1) \mid (\alpha_2.E_2)]\varphi \leftrightarrow [\alpha_1.(E_1 \mid \alpha_2.E_2)]\varphi \wedge [\alpha_2.(\alpha_1.E_1 \mid E_2)]\varphi$

16. $[(\alpha.E_1) \mid (\overline{\alpha}.E_2)]\varphi \leftrightarrow [\alpha.(E_1 \mid \overline{\alpha}.E_2)]\varphi \wedge [\overline{\alpha}.(\alpha.E_1 \mid E_2)]\varphi \wedge [\tau.(E_1 \mid E_2)]\varphi$

Regras de Inferência:

Substituição Uniforme:

$$\frac{\vdash \varphi}{\vdash \varphi(\beta_1/p_1, \cdots, \beta_n/p_n)}$$

Modus Ponens:

$$\frac{\varphi, \varphi \rightarrow \psi}{\psi}$$

Generalização:

$$\frac{\vdash \varphi}{\vdash [K]\varphi}, \quad \frac{\vdash \varphi}{\vdash [E]\varphi}$$

Um **teorema** é um conjunto de fórmulas Γ se e somente se existe uma seqüência $\varphi_1, ..., \varphi_n$ de fórmulas tal que φ_i é um teorema ou pertence a Γ ou é consequencia das anteriores pela aplicação das regras modus ponens ou substituição.

Lema 3.3.1 : $\vdash [\alpha](\varphi \wedge [\mathring{A}]\bot) \rightarrow [\alpha \cdot 0]\varphi$

Prova. Suponha $\varphi \wedge [\mathring{A}]\bot$.

$\vdash (\varphi \wedge [\mathring{A}]\bot) \rightarrow \langle 0\rangle\varphi$ (pelo axioma 7)

$\vdash (\varphi \wedge [\mathring{A}]\bot) \rightarrow ([\mathring{A}]\bot \wedge \langle 0\rangle\varphi)$ (cálculo proposicional)

$\vdash (\varphi \wedge [\mathring{A}]\bot) \rightarrow [0]\varphi$ (pelo axioma 8)

$\vdash [\alpha]((\varphi \wedge [\mathring{A}]\bot) \rightarrow [0]\varphi)$ (generalização)

$\vdash [\alpha](\varphi \wedge [\mathring{A}]\bot) \rightarrow [\alpha][0]\varphi$ (K)

$\vdash [\alpha](\varphi \wedge [\mathring{A}]\bot) \rightarrow [\alpha \cdot 0]\varphi$ (pelo axioma 4) □

3.4 Corretude

Considere F como sendo a classe de frames $\mathcal{F}= (W, Z, R_\alpha, R_E)$, onde as relações R_α, R_E, são descritas na definicão 3.2.2. Seja $\mathcal{M}$ um modelo para $\mathcal{F}$.

Definição 3.4.1 :

- *Uma fórmula φ é válida em um estado w de um frame $\mathcal{F}$, $\mathcal{F}$,$w \models \varphi$, se e somente se φ é verdadeira em todo modelo $(\mathcal{F}, V)$ baseado em $\mathcal{F}$ no estado w.*

- *φ é válida em um frame $\mathcal{F}$, $\mathcal{F} \models \varphi$, se e somente se φ é válida em todo estado de $\mathcal{F}$.*

- *φ é válida numa classe de frames F, $F \models \varphi$, se e somente se ela é válida em cada frame $\mathcal{F} \in F$.*

Teorema 3.4.1 : *Todo teorema do Esquema de Axiomas é válido na classe de frames F .*

Temos que provar que:

- Todo axioma do Esquema de Axiomas é válido na classe de frames F.
- As regras de inferência preservam validade na classe de frames F.

Lema 3.4.1 : *Para todas as fórmulas e todos os programas:*

1. $F \models [K](\varphi \to \psi) \to [K]\varphi \to [K]\psi$
2. $F \models [E](\varphi \to \psi) \to [E]\varphi \to [E]\psi$
3. $F \models [\alpha \cdot E]\varphi \leftrightarrow [\alpha][E]\varphi$
4. $F \models [E_1 + E_2]\varphi \leftrightarrow [E_1]\varphi \wedge [E_2]\varphi$
5. $F \models [0 + E_1]\varphi \to [E_1]\varphi$
6. $F \models \varphi \wedge [\mathring{A}]\bot \to \langle 0\rangle\varphi$
7. $F \models [\mathring{A}]\bot \wedge \langle 0\rangle\varphi \to [0]\varphi$
8. $F \models [\mathring{A}]\bot \leftrightarrow \langle 0\rangle\top$
9. $F \models [E_1 \mid E_2]\varphi \leftrightarrow [E_2 \mid E_1]\varphi$
10. $F \models [(E_1 \mid E_2) \mid E_3]\varphi \leftrightarrow [E_1 \mid (E_2 \mid E_3)]\varphi$

11. $F \models [E \mid 0]\varphi \leftrightarrow [E]\varphi$

12. $F \models [(E_1 + E_2) \mid E_3]\varphi \leftrightarrow [(E_1 \mid E_3) + (E_2 \mid E_3)]\varphi$

13. $F \models [\alpha.(E_1 \mid E_2)]\varphi \rightarrow [(\alpha.E_1) \mid E_2]\varphi$

14. $F \models [(\alpha_1.E_1) \mid (\alpha_2.E_2)]\varphi \leftrightarrow [\alpha_1.(E_1 \mid \alpha_2.E_2)]\varphi \wedge [\alpha_2.(\alpha_1.E_1 \mid E_2)]\varphi$

15. $F \models [(\alpha.E_1) \mid (\overline{\alpha}.E_2)]\varphi \leftrightarrow [\alpha.(E_1 \mid \overline{\alpha}.E_2)]\varphi \wedge [\overline{\alpha}.(\alpha.E_1 \mid E_2)]\varphi \wedge [\tau.(E_1 \mid E_2)]\varphi$

Prova.

1. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$$(\mathcal{M}, w) \not\models [K](\varphi \rightarrow \psi) \rightarrow [K]\varphi \rightarrow [K]\psi$$

Então,

(1) $(\mathcal{M}, w) \models [K](\varphi \rightarrow \psi)$ e

(2) $(\mathcal{M}, w) \not\models [K]\varphi \rightarrow [K]\psi$

(1) se e somente se $\forall w' \in W$ e $\forall \alpha \in K$ se $wR_\alpha w'$ então (3) $(\mathcal{M}, w') \models (\varphi \rightarrow \psi)$.

(2) se e somente se (4) $(\mathcal{M}, w) \models [K]\varphi$ e (5) $(\mathcal{M}, w) \not\models [K]\psi$.

(4) se e somente se $\forall w' \in W$ e $\forall \alpha \in K$ se $wR_\alpha w'$ então (6) $(\mathcal{M}, w') \models \varphi$.

De (3) e (6) e pela definição de satisfação,, $\forall w' \in W$, $(\mathcal{M}, w') \models \psi$, se e somente se $(\mathcal{M}, w') \models [K]\psi$. O que contraria (5).

2. Segue do mesmo modo do item 1.

3. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$(\mathcal{M}, w) \not\models [\alpha \cdot E]\varphi \leftrightarrow [\alpha][E]\varphi$

Então,

(1) $(\mathcal{M}, w) \not\models [\alpha \cdot E]\varphi \rightarrow [\alpha][E]\varphi$ ou

(2) $(\mathcal{M}, w) \not\models [\alpha][E]\varphi \rightarrow [\alpha \cdot E]\varphi$

(1) se e somente se (3) $(\mathcal{M}, w) \models [\alpha \cdot E]\varphi$ e (4) $(\mathcal{M}, w) \not\models [\alpha][E]\varphi$.

(3) se e somente se $\forall w', w'' \in W$ se $wR_{\alpha \cdot E}w''$, então $(\mathcal{M}, w'') \models \varphi$.

Como $R_{\alpha \cdot E} = R_\alpha; R_E$, pela definição 3.2.2, então se $\forall w'' \in W, wR_\alpha; R_E w''$ então $(\mathcal{M}, w'') \models \varphi$.

(4) se e somente se (5) $(\mathcal{M}, w) \models \langle\alpha\rangle\langle E\rangle\neg\varphi$.

(5) se e somente se $\exists w', w'' \in W$ tal que $wR_\alpha w'$ e $w' R_E w''$, e $(\mathcal{M}, w'') \models \neg\varphi$.

Então existe um $w'' \in W$ tal que $wR_\alpha; R_E w''$ e $(\mathcal{M}, w'') \models \neg\varphi$. O que contradiz (3).

Ou

(2) se e somente se (6) $(\mathcal{M}, w) \models [\alpha][E]\varphi$ e (7) $(\mathcal{M}, w) \not\models [\alpha \cdot E]\varphi$.

(6) se e somente se $\forall w', w'' \in W$ se $wR_\alpha w'$ e $w' R_E w''$, então $(\mathcal{M}, w'') \models \varphi$.

Como $R_\alpha; R_E = R_{\alpha \cdot E}$, pela definição 3.2.2, então se $\forall w'' \in W, wR_\alpha; R_E w''$ então $(\mathcal{M}, w'') \models \varphi$.

(7) se e somente se (8) $(\mathcal{M}, w) \models \langle\alpha \cdot E\rangle\neg\varphi$.

(8) se e somente se $\exists w', w'' \in W$ tal que $wR_{\alpha \cdot E}w''$, e $(\mathcal{M}, w'') \models \neg\varphi$.

Como $R_{\alpha \cdot E} = R_\alpha; R_E$, pela definição 3.2.2 então $\exists w', w'' \in W$ tal que $wR_\alpha w'; w' R_E w''$ e $(\mathcal{M}, w'') \models \neg\varphi$. O que contradiz (6).

4. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$(\mathcal{M}, w) \not\models [E_1 + E_2]\varphi \leftrightarrow [E_1]\varphi \wedge [E_2]\varphi$

Então,

(1) $(\mathcal{M}, w) \not\models [E_1 + E_2]\varphi \rightarrow [E_1]\varphi \wedge [E_2]\varphi$ ou

(2) $(\mathcal{M}, w) \not\models [E_1]\varphi \wedge [E_2]\varphi \rightarrow [E_1 + E_2]\varphi$

(1) se e somente se (3) $(\mathcal{M}, w) \models [E_1 + E_2]\varphi$ e (4) $(\mathcal{M}, w) \not\models [E_1]\varphi \wedge [E_2]\varphi$.

(3) se e somente se $\forall w' \in W$ se $wR_{E_1+E_2}w'$ então $(\mathcal{M}, w') \models \varphi$.

Como $R_{E_1+E_2} = R_{E_1} \cup R_{E_2}$, pela definição 3.2.2, então $\forall w' \in W$ se $wR_{E_1}w'$ ou $wR_{E_2}w'$ então $(\mathcal{M}, w') \models \varphi$.

(4) se e somente se (5) $(\mathcal{M}, w) \models \langle E_1\rangle\neg\varphi \vee \langle E_2\rangle\neg\varphi$.

(5) se e somente se (6) $(\mathcal{M}, w) \models \langle E_1\rangle\neg\varphi$ ou (7) $(\mathcal{M}, w) \models \langle E_2\rangle\neg\varphi$.

(6) se e somente se $\exists w' \in W$ tal que $wR_{E_1}w'$ e $(\mathcal{M}, w') \models \neg\varphi$. Ou

(7) se e somente se $\exists w' \in W$ tal que $wR_{E_2}w'$ e $(\mathcal{M}, w') \models \neg\varphi$.

Como $R_{E_1+E_2} = R_{E_1} \cup R_{E_2}$, pela definição 3.2.2, então $\exists w'$ tal que $wR_{E_1+E_2}w'$ e $(\mathcal{M}, w') \models \neg\varphi$. O que contradiz (3).

ou

(2) se e somente se (8) $(\mathcal{M}, w) \models [E_1]\varphi \wedge [E_2]\varphi$ e (9) $(\mathcal{M}, w) \not\models [E_1 + E_2]\varphi$.

(8) se e somente se (10) $(\mathcal{M}, w) \models [E_1]\varphi$ e (11) $(\mathcal{M}, w) \models [E_2]\varphi$.

(10) se e somente se $\forall w' \in W$ se $wR_{E_1}w'$ então $(\mathcal{M}, w') \models \varphi$ e

(11) se e somente se $\forall w' \in W$ se $wR_{E_2}w'$ então $(\mathcal{M}, w') \models \varphi$.

(9) se e somente se (12) $(\mathcal{M}, w) \models \langle E_1 + E_2\rangle\neg\varphi$.

(12) se e somente se $\exists w' \in W$ tal que $wR_{E_1+E_2}w'$ então $(\mathcal{M}, w') \models \neg\varphi$.

Como $R_{E_1+E_2} = R_{E_1} \cup R_{E_2}$, pela definição 3.2.2, então $\exists w'$ tal que $wR_{E_1}w'$ ou $wR_{E_2}w'$ e $(\mathcal{M}, w') \models \neg\varphi$. O que contradiz (10) e (11).

5. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$$(\mathcal{M}, w) \not\models [0 + E_1]\varphi \rightarrow [E_1]\varphi$$

Então,

(1) $(\mathcal{M}, w) \models [0 + E_1]\varphi$ e

(2) $(\mathcal{M}, w) \not\models [E_1]\varphi$

(1) se e somente se $\forall w' \in W$ se $wR_{0+E_1}w'$ e $wR_{E_1}w'$ então $(\mathcal{M}, w') \models \varphi$.

Como $R_{0+E_1} = R_{E_1}$, pela definição 3.2.2, pois R_0 é reflexiva, então $\forall w' \in W, wR_{E_1}w'$ e $(\mathcal{M}, w') \models \varphi$.

(2) se e somente se (3) $(\mathcal{M}, w) \models \langle E_1\rangle\neg\varphi$.

(3) se e somente se $\exists w' \in W$ tal que $wR_{E_1}w'$ então $(\mathcal{M}, w') \models \neg\varphi$. O que contradiz (1).

6. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$$(\mathcal{M}, w) \not\models \varphi \wedge [\mathring{A}]\bot \rightarrow \langle 0\rangle\varphi$$

Então,

(1) $(\mathcal{M}, w) \models \varphi \wedge [\mathring{A}]\bot$ e

(2) $(\mathcal{M}, w) \not\models \langle 0\rangle\varphi$

(1) se e somente se (3) $(\mathcal{M}, w) \models \varphi$ e (4) $(\mathcal{M}, w) \models [\mathring{A}]\bot$.

(2) se e somente se (5) $(\mathcal{M}, w) \models [0]\neg\varphi$.

De (4) temos que $\forall\alpha \in Act\ \neg\exists w'\ wR_\alpha w'$ (pela definição de Z)

(5) se e somente se $\forall w \in Z$ e como R_0 é reflexiva, temos que wR_0w, $(\mathcal{M}, w) \models \neg\varphi$. O que contradiz (3).

7. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$$(\mathcal{M}, w) \not\models [\mathring{A}]\bot \wedge \langle 0\rangle\varphi \rightarrow [0]\varphi$$

Então,

(1) $(\mathcal{M}, w) \models [\mathring{A}]\bot \wedge \langle 0\rangle\varphi$ e

(2) $(\mathcal{M}, w) \not\models [0]\varphi$

(1) se e somente se (3) $(\mathcal{M}, w) \models [\mathring{A}]\bot$ e (4) $(\mathcal{M}, w) \models \langle 0\rangle\varphi$.

De (3) temos que $\forall\alpha \in Act\ \neg\exists w'\ wR_\alpha w'$ (pela definição de Z).

(4) se e somente se $\forall w \in W, wR_0w$, reflexividade de R_0, então $(\mathcal{M}, w) \models \varphi$.

(2) se e somente se (5) $(\mathcal{M}, w) \not\models \langle 0\rangle\neg\varphi$ (5) se e somente se $\forall w \in W, wR_0w$ então $(\mathcal{M}, w) \models \neg\varphi$. O que contradiz (4).

8. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$$(\mathcal{M}, w) \not\models [\mathring{A}]\bot \leftrightarrow \langle 0\rangle\top$$

(1) $(\mathcal{M}, w) \not\models [\mathring{A}]\bot \rightarrow \langle 0\rangle\top$ e

(2) $(\mathcal{M}, w) \not\models \langle 0\rangle\top \rightarrow [\mathring{A}]\bot$

(1) se e somente se (3) $(\mathcal{M}, w) \models [\mathring{A}]\bot$ e (4) $(\mathcal{M}, w) \not\models \langle 0\rangle\top$.

(3) temos que $\forall\alpha \in Act\ \neg\exists w'\ wR_\alpha w'$ (pela definição de Z).

(4) se e somente se não existe w' tal que wR_0w'. O que contradiz ().

(2) se e somente se (6) $(\mathcal{M}, w) \models \langle 0 \rangle \top$ e (7) $(\mathcal{M}, w) \not\models [\mathring{A}] \bot$.

(6) se (8) wR_0w.

(7) se e somente se $(\mathcal{M}, w) \models \langle \mathring{A} \rangle \top$ se e somente se

$\exists \alpha \in Act$ tal que $wR_\alpha w'$

se e somente se $w \notin Z \Rightarrow (w, w) \notin R_0$. O que contradiz (1).

9. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$$(\mathcal{M}, w) \not\models [E_1 \mid E_2]\varphi \leftrightarrow [E_2 \mid E_1]\varphi$$

Então,

(1) $(\mathcal{M}, w) \not\models [E_1 \mid E_2]\varphi \rightarrow [E_2 \mid E_1]\varphi$ ou

(2) $(\mathcal{M}, w) \not\models [E_2 \mid E_1]\varphi \rightarrow [E_1 \mid E_2]\varphi$

(1) se e somente se (3) $(\mathcal{M}, w) \models [E_1 \mid E_2]\varphi$ e (4) $(\mathcal{M}, w) \not\models [E_2 \mid E_1]\varphi$.

(3) se e somente se $\forall w' \in W$ se $wR_{E_1|E_2}w'$ então $(\mathcal{M}, w') \models \varphi$.

Como $R_{E_1|E_2} = R_{E_2|E_1}$, pela definição 3.2.2, então $\forall w' \in W, wR_{E_2|E_1}w'$ e $(\mathcal{M}, w') \models \varphi$.

(4) se e somente se (5) $(\mathcal{M}, w) \models \langle E_2 \mid E_1 \rangle \neg\varphi$.

(5) se e somente se $\exists w' \in W$ tal que $wR_{E_2|E_1}w'$ e $(\mathcal{M}, w') \models \neg\varphi$. O que contraria (3).

(2) se e somente se (6) $(\mathcal{M}, w) \models [E_2 \mid E_1]\varphi$ e (7) $(\mathcal{M}, w) \not\models [E_1 \mid E_2]\varphi$.

(6) se e somente se $\forall w' \in W$ se $wR_{E_2|E_1}w'$ então $(\mathcal{M}, w') \models \varphi$.

(7) se e somente se (8) $(\mathcal{M}, w) \models \langle E_1 \mid E_2 \rangle \neg\varphi$.

(8) se e somente se $\exists w' \in W$ tal que $wR_{E_1|E_2}w'$, como $R_{E_1|E_2} = R_{E_2|E_1}$, pela definição

3.2.2, e $(\mathcal{M}, w') \models \neg\varphi$. O que contraria (6).

10. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$$(\mathcal{M}, w) \not\models [(E_1 \mid E_2) \mid E_3]\varphi \leftrightarrow [E_1 \mid (E_2 \mid E_3)]\varphi$$

Então,

(1) $(\mathcal{M}, w) \not\models [(E_1 \mid E_2) \mid E_3]\varphi \rightarrow [E_1 \mid (E_2 \mid E_3)]\varphi$ ou

(2) $(\mathcal{M}, w) \not\models [E_1 \mid (E_2 \mid E_3)]\varphi \rightarrow [(E_1 \mid E_2) \mid E_3]\varphi$

(1) se e somente se (3) $(\mathcal{M}, w) \models [(E_1 \mid E_2) \mid E_3]\varphi$ e (4) $(\mathcal{M}, w) \not\models [E_1 \mid (E_2 \mid E_3)]\varphi$.

(3) se e somente se $\forall w' \in W$ se $wR_{(E_1|E_2)|E_3}w'$ então $(\mathcal{M}, w') \models \varphi$.

Como $R_{(E_1|E_2)|E_3} = R_{E_1|(E_2|E_3)}$, pela definição 3.2.2, então $\forall w' \in W$, $wR_{E_1|(E_2)|E_3)}w'$ então $(\mathcal{M},w') \models \varphi$.

(4) se e somente se (5) $(\mathcal{M}, w) \models \langle E_1 \mid (E_2 \mid E_3)\rangle\neg\varphi$.

(5) se e somente se $\exists w' \in W$ tal que $wR_{E_1|(E_2|E_3)}w'$ e $(\mathcal{M}w') \models \neg\varphi$. O que contraria (3).

(2) se e somente se (6) $(\mathcal{M}, w) \models [E_1 \mid (E_2 \mid E_3)]\varphi$ e (7) $(\mathcal{M}, w) \not\models [(E_1 \mid E_2) \mid E_3]\varphi$.

(6) se e somente se $\forall w' \in W$ se $wR_{E_1|(E_2|E_3)}w'$ e $(\mathcal{M}w') \models \varphi$.

(7) se e somente se (8) $(\mathcal{M}, w) \models \langle(E_1 \mid E_2) \mid E_3\rangle\neg\varphi$.

(8) se e somente se $\exists w' \in W$ tal que $wR_{(E_1|E_2)|E_3}w'$ e como $R_{(E_1|E_2)|E_3} = R_{E_1|(E_2|E_3)}$, pela definição 3.2.2, e $(\mathcal{M}w') \models \neg\varphi$. O que contraria (6).

11. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$(\mathcal{M}, w) \not\models [0 \mid E]\varphi \leftrightarrow [E]\varphi$

Então,

(1) $(\mathcal{M}, w) \not\models [0 \mid E]\varphi \rightarrow [E]\varphi$ ou

(2) $(\mathcal{M}, w) \not\models [E]\varphi \rightarrow [0 \mid E]\varphi$

(1) se e somente se (3) $(\mathcal{M}, w) \models [0 \mid E]\varphi$ e (4) $(\mathcal{M}, w) \not\models [E]\varphi$.

(3) $w \in W$, se $wR_{E|0}w'$ então $(\mathcal{M},w') \models \varphi$.

Como $R_{0|E} = R_E$, pela definição 3.2.2, então $\forall w' \in W$, wR_Ew' e $(\mathcal{M},w') \models \varphi$.

(4) se e somente se (5) $(\mathcal{M}, w) \models \langle E\rangle\neg\varphi$.

(5) se e somente se $\exists w' \in W$ tal que wR_Ew', e $(\mathcal{M},w') \models \neg\varphi$. O que contraria (3).

(2) se e somente se (6) $(\mathcal{M}, w) \models [E]\varphi$ e (7) $(\mathcal{M}, w) \not\models [0 \mid E]\varphi$.

(6) se e somente se $\forall w' \in W$ se wR_Ew' então $(\mathcal{M}, w') \models \varphi$.

(7) se e somente se (8) $(\mathcal{M}, w) \models \langle 0 \mid E\rangle\neg\varphi$.

(8) se e somente se $\exists w' \in W$ tal que $wR_{0|E}w'$, e como $R_{0|E} = R_E$, pela definição 3.2.2, e $(\mathcal{M}, w') \models \neg\varphi$. O que contraria (5).

12. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$(\mathcal{M}, w) \not\models [(E_1 + E_2) \mid E_3]\varphi \leftrightarrow [(E_1 \mid E_3) + (E_2 \mid E_3)]\varphi$

(1) $(\mathcal{M}, w) \not\models [(E_1 + E_2) \mid E_3]\varphi \rightarrow [(E_1 \mid E_3) + (E_2 \mid E_3)]\varphi$ ou

(2) $(\mathcal{M}, w) \not\models [(E_1 \mid E_3) + (E_2 \mid E_3)]\varphi \rightarrow [(E_1 + E_2) \mid E_3]\varphi$

(1) se e somente se (3) $(\mathcal{M}, w) \models [(E_1+E_2) \mid E_3]\varphi$ e (4) $(\mathcal{M}, w) \not\models [(E_1 \mid E_3)+(E_2 \mid E_3)]\varphi$.

(3) se e somente se $\forall w' \in W$ se $wR_{(E_1+E_2)|E_3}w'$ então $(\mathcal{M}, w') \models \varphi$.

Como $R_{(E_1+E_2)|E_3} = R_{(E_1|E_3)+(E_2|E_3)}$, pela definição 3.2.2, então se $\forall w' \in W$, $wR_{(E_1|E_3)+(E_2|E_3)}w'$ então $(\mathcal{M}, w') \models \varphi$.

(4) se e somente se (5) $(\mathcal{M}, w) \models \langle (E_1 \mid E_3) + (E_2 \mid E_3) \rangle \neg\varphi$.

(5) se e somente se $\exists w' \in W$ tal que $wR_{(E_1|E_3)+(E_2|E_3)}w'$ e $(\mathcal{M}, w') \models \neg\varphi$. O que contradiz (3).

(2) se e somente se (6) $(\mathcal{M}, w) \models [(E_1 \mid E_3)+(E_2 \mid E_3)]\varphi$ e (7) $(\mathcal{M}, w) \not\models [(E_1+E_2) \mid E_3]\varphi$.

(6) se e somente se $\forall w' \in W$ se $wR_{(E_1|E_3)+(E_2|E_3)}w'$ então $(\mathcal{M}, w') \models \varphi$.

(7) se e somente se (8) $(\mathcal{M}, w) \models \langle (E_1 + E_2) \mid E_3 \rangle \neg\varphi$.

(8) se e somente se $\exists w' \in W$ tal que $wR_{(E_1+E_2)|E_3}w'$ e como $R_{(E_1+E_2)|E_3} = R_{(E_1|E_3)+(E_2|E_3)}$, pela definição 3.2.2, e $(\mathcal{M}, w') \models \neg\varphi$. O que contradiz (6).

13. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$$(\mathcal{M}, w) \not\models [\alpha.(E_1 \mid E_2)]\varphi \rightarrow [(\alpha.E_1) \mid E_2]\varphi$$

Então,

(1) $(\mathcal{M}, w) \models [\alpha.(E_1 \mid E_2)]\varphi$ e

(2) $(\mathcal{M}, w) \not\models [(\alpha.E_1) \mid E_2]\varphi$

(1) se e somente se $\forall w' \in W$ se $wR_{\alpha.(E_1|E_2)}w'$ então $(\mathcal{M}, w') \models \varphi$.

Como $R_{(\alpha.E_1)|E_2} \supseteq R_{\alpha.(E_1|E_2)}$, pela definição 3.2.2, então $\forall w' \in W, wR_{(\alpha.E_1)|E_2}w'$ e $(\mathcal{M}, w') \models \varphi$.

(2) se e somente se (3) $(\mathcal{M}, w) \models \langle (\alpha.E_1) \mid E_2 \rangle \neg\varphi$.

(3) se e somente se $\exists w' \in W$ tal que $wR_{(\alpha.E_1)|E_2}w'$ e $(\mathcal{M}, w') \models \neg\varphi$. O que contradiz (1).

14. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$$(\mathcal{M}, w) \not\models [(\alpha_1.E_1) \mid (\alpha_2.E_2)]\varphi \leftrightarrow [\alpha_1.(E_1 \mid \alpha_2.E_2)]\varphi \wedge [\alpha_2.(\alpha_1.E_1 \mid E_2)]\varphi$$

Então,

(1) $(\mathcal{M}, w) \not\models [(\alpha_1.E_1) \mid (\alpha_2.E_2)]\varphi \rightarrow [\alpha_1.(E_1 \mid \alpha_2.E_2)]\varphi \wedge [\alpha_2.(\alpha_1.E_1 \mid E_2)]\varphi$ ou

(2) $(\mathcal{M}, w) \not\models [\alpha_1.(E_1 \mid \alpha_2.E_2)]\varphi \wedge [\alpha_2.(\alpha_1.E_1 \mid E_2)]\varphi \rightarrow [(\alpha_1.E_1) \mid (\alpha_2.E_2)]\varphi$

(1) se e somente se (3) $(\mathcal{M}, w) \models [(\alpha_1.E_1) \mid (\alpha_2.E_2)]\varphi$ e (4) $(\mathcal{M}, w) \not\models [\alpha_1.(E_1 \mid \alpha_2.E_2)]\varphi \wedge [\alpha_2.(\alpha_1.E_1 \mid E_2)]\varphi$.

(3) se e somente se $\forall w' \in W$ se $wR_{(\alpha_1.E_1)|(\alpha_2.E_2)}w'$ então $(\mathcal{M}, w') \models \varphi$.

Como $R_{(\alpha_1.E_1)|(\alpha_2.E_2)} = R_{\alpha_1.(E_1|\alpha_2.E_2)+\alpha_2.(\alpha_1.E_1|E_2)}$, pela definição 3.2.2,então $\forall w' \in W$ $wR_{\alpha_1.(E_1|\alpha_2.E_2)+\alpha_2.(\alpha_1.E_1|E_2)}w'$ e $(\mathcal{M}, w') \models \varphi$.

(4) se e somente se (5) $(\mathcal{M}, w) \not\models [\alpha_1.(E_1 \mid \alpha_2.E_2)]\varphi$ e (6) $(\mathcal{M}, w) \not\models [\alpha_2.(\alpha_1.E_1 \mid E_2)]\varphi$.

(5) se e somente se (7) $(\mathcal{M}, w) \models \langle\alpha_1.(E_1 \mid \alpha_2.E_2)\rangle\neg\varphi$.

(7) se e somente se $\exists w' \in W$ tal que $wR_{\alpha_1.(E_1|\alpha_2.E_2)}w'$ e $(\mathcal{M}, w') \models \neg\varphi$. O que contradiz (3).

(6) se e somente se (8) $(\mathcal{M}, w) \models \langle\alpha_2.(\alpha_1.E_1 \mid E_2)\rangle\neg\varphi$.

(8) se e somente se $\exists w' \in W$ tal que $wR_{\alpha_2.(\alpha_1.E_1|E_2)}w'$ e como $R_{(\alpha_1.E_1)|(\alpha_2.E_2)} =$

$R_{\alpha_1.(E_1|\alpha_2.E_2)+\alpha_2.(\alpha_1.E_1|E_2)}$, pela definição 3.2.2, e $(\mathcal{M}, w') \models \neg\varphi$. O que contradiz (3).

(2) se e somente se (9) $(\mathcal{M}, w) \not\models [\alpha_1.(E_1 \mid \alpha_2.E_2)]\varphi \wedge [\alpha_2.(\alpha_1.E_1 \mid E_2)]\varphi$ e (10) $(\mathcal{M}, w) \not\models [(\alpha_1.E_1) \mid (\alpha_2.E_2)]\varphi$.

(9) se e somente se (11) $(\mathcal{M}, w) \models [\alpha_1.(E_1 \mid \alpha_2.E_2)]\varphi$ e (12) $(\mathcal{M}, w) \models [\alpha_2.(\alpha_1.E_1 \mid E_2)]\varphi$.

(11) se e somente se $\forall w' \in W$ se $wR_{\alpha_1.(E_1|\alpha_2.E_2)}w'$ então $(\mathcal{M}, w') \models \varphi$.(*)

(12) se e somente se $\forall w' \in W$ se $wR_{\alpha_2.(\alpha_1.E_1|E_2)}w'$ então $(\mathcal{M}, w') \models \varphi$.(**)

Como $R_{(\alpha_1.E_1)|(\alpha_2.E_2)} = R_{\alpha_1.(E_1|\alpha_2.E_2)+\alpha_2.(\alpha_1.E_1|E_2)}$, pela definição 3.2.2, então $\forall w' \in W$ $wR_{\alpha_1.(E_1|\alpha_2.E_2)+\alpha_2.(\alpha_1.E_1|E_2)}w'$ então $(\mathcal{M}, w') \models \varphi$.

(10) se e somente se (13) $(\mathcal{M}, w) \models \langle(\alpha_1.E_1) \mid (\alpha_2.E_2)\rangle\neg\varphi$.

(13) se somente se $\exists w' \in W$ tal que $wR_{(\alpha_1.E_1)|(\alpha_2.E_2)}w'$ e $(\mathcal{M}, w') \models \neg\varphi$. O que contradiz (*) e (**).

15. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$$(\mathcal{M}, w) \not\models [(\alpha.E_1) \mid (\overline{\alpha}.E_2)]\varphi \leftrightarrow [\alpha.(E_1 \mid \overline{\alpha}.E_2)]\varphi \wedge [\overline{\alpha}.(\alpha.E_1 \mid E_2)]\varphi \wedge [\tau.(E_1 \mid E_2)]\varphi$$

Então,

(1) $(\mathcal{M}, w) \not\models [(\alpha.E_1) \mid (\overline{\alpha}.E_2)]\varphi \rightarrow [\alpha.(E_1 \mid \overline{\alpha}.E_2)]\varphi \wedge [\overline{\alpha}.(\alpha.E_1 \mid E_2)]\varphi \wedge [\tau.(E_1 \mid E_2)]\varphi$ ou

(2) $(\mathcal{M}, w) \not\models [\alpha.(E_1 \mid \overline{\alpha}.E_2)]\varphi \wedge [\overline{\alpha}.(\alpha.E_1 \mid E_2)]\varphi \wedge [\tau.(E_1 \mid E_2)]\varphi \rightarrow [(\alpha.E_1) \mid (\overline{\alpha}.E_2)]\varphi$

(1) se e somente se (3) $(\mathcal{M}, w) \models [(\alpha.E_1) \mid (\overline{\alpha}.E_2)]\varphi$ e (4) $(\mathcal{M}, w) \not\models [\alpha.(E_1 \mid \overline{\alpha}.E_2)]\varphi \wedge [\overline{\alpha}.(\alpha.E_1 \mid E_2)]\varphi \wedge [\tau.(E_1 \mid E_2)]\varphi$.

(3) se e somente se $\forall w' \in W$ se $wR_{((\alpha.E_1)|(\overline{\alpha}.E_2))}w'$ então $(\mathcal{M}, w') \models \varphi$.

Como $R_{((\alpha.E_1)|(\overline{\alpha}.E_2))} = R_{\alpha.(E_1|\overline{\alpha}.E_2)+\overline{\alpha}.(\alpha.E_1|E_2)+\tau.(E_1|E_2)}$, pela definição 3.2.2, então $\forall w' \in W, wR_{\alpha.(E_1|\overline{\alpha}.E_2)+\overline{\alpha}.(\alpha.E_1|E_2)+\tau.(E_1|E_2)}w'$ e $(\mathcal{M}, w') \models \varphi$.

(4) se e somente se (5) $(\mathcal{M}, w) \models \langle\alpha.(E_1 \mid \overline{\alpha}.E_2)\rangle\neg\varphi \vee \langle\overline{\alpha}.(\alpha.E_1 \mid E_2)\rangle\neg\varphi \vee \langle\tau.(E_1 \mid E_2)\rangle\neg\varphi$.

(5) se e somente se $\exists w' \in W$ tal que $wR_{\alpha.(E_1|\overline{\alpha}.E_2)+\overline{\alpha}.(\alpha.E_1|E_2)+\tau.(E_1|E_2)}w'$ e $(\mathcal{M}, w') \models \neg\varphi$. O que contraria (3).

(2) se e somente se (6) $(\mathcal{M}, w) \models [\alpha.(E_1 \mid \overline{\alpha}.E_2)]\varphi \wedge [\overline{\alpha}.(\alpha.E_1 \mid E_2)]\varphi \wedge [\tau.(E_1 \mid E_2)]\varphi$ e (7) $(\mathcal{M}, w) \not\models [(\alpha.E_1) \mid (\overline{\alpha}.E_2)]\varphi$.

(6) se e somente se $\forall w' \in W$ se $wR_{\alpha.(E_1|\overline{\alpha}.E_2)+\overline{\alpha}.(\alpha.E_1|E_2)+\tau.(E_1|E_2)}w'$ então $(\mathcal{M}, w') \models \varphi$.

(7) se e somente se (8) $(\mathcal{M}, w) \models \langle(\alpha.E_1) \mid (\overline{\alpha}.E_2)\rangle\neg\varphi$.

(8) se e somente se $\exists w' \in W$ tal que $wR_{((\alpha.E_1)|(\overline{\alpha}.E_2))}w'$ e como $R_{((\alpha.E_1)|(\overline{\alpha}.E_2))} = R_{\alpha.(E_1|\overline{\alpha}.E_2)+\overline{\alpha}.(\alpha.E_1|E_2)+\tau.(E_1|E_2)}$, pela definição 3.2.2, e $(\mathcal{M}, w') \models \neg\varphi$. O que contraria (6). □

Lema 3.4.2 : *Para todas as fórmulas e todos os programas α e E tal que,*

1. *Se $\mathcal{M} \models \varphi$ e $\mathcal{M} \models \varphi \rightarrow \psi$ então $\mathcal{M} \models \psi$*

2. *Se $\mathcal{M} \models \varphi$ então $\mathcal{M} \models [\alpha]\varphi$*

3. *Se $\mathcal{M} \models \varphi$ então $\mathcal{M} \models [E]\varphi$*

Prova.

1. Suponha que $\mathcal{M} \models \varphi$, $\mathcal{M} \models \varphi \rightarrow \psi$ e $\mathcal{M} \not\models \psi$. Uma vez que $\varphi \rightarrow \psi \equiv \neg(\varphi \wedge \neg\psi)$,

segue que $\mathcal{M} \models \neg(\varphi \wedge \neg\psi)$, se e somente se $\mathcal{M} \not\models \varphi \wedge \neg\psi$. Temos também, por hipótese, que $\mathcal{M} \models \varphi$ e $\mathcal{M} \models \neg\psi$, ou seja, $\mathcal{M} \models \varphi \wedge \neg\psi$. O que é uma contradição. Logo, $\mathcal{M} \models \psi$.

2. Suponha que $\mathcal{M} \models \varphi$ e $\mathcal{M} \not\models [\alpha]\varphi$. Então $\mathcal{M} \models \neg[\alpha]\varphi$, isto é, existe um estado w e um estado w' tal que $wR_\alpha w'$ e $\mathcal{M}, w' \models \neg\varphi$, o que contradiz a hipótese de que φ é verdadeira em todos os estados de $\mathcal{M}$, $\mathcal{M} \models \varphi$. Logo, $\mathcal{M} \models [\alpha]\varphi$.

3. Suponha que $\mathcal{M} \models \varphi$ e $\mathcal{M} \not\models [E]\varphi$. Então existe um estado w tal que $\mathcal{M}$,$w \models \neg[E]\varphi$, isto é, existe um estado w e um estado w' tal que $wR_E w'$ e $\mathcal{M}, w' \models \neg\varphi$, o que contradiz a hipótese de que φ é verdadeira em todos os estados de $\mathcal{M}$, $\mathcal{M} \models \varphi$. Logo, $\mathcal{M} \models [E]\varphi$. □

3.5 Completude

Nesta seção apresentaremos a prova do teorema da completude para a LDP-CCS com Composição Paralela com Sincronização.

Considere a classe de frames $F = (W, Z, R_\alpha, R_E)$.

Teorema 3.5.1 : *Toda fórmula válida na classe de frames F é um teorema do sistema de axiomas da LDP-CCS com Composição Paralela com Sincronização.*

Prova. Na prova do teorema usaremos a técnica do modelo canônico, isto é, construiremos um modelo canônico para a LDP-CCS com Composição Paralela com Sincronização e depois mostraremos que o frame do modelo canônico esta na classe F.

O modelo canônico tem a propriedade que toda fbf α é verdade no modelo canônico se e somente se ela é um teorema do sistema.

Mostrando que o frame do modelo canônico está na classe F, e fazendo α válida em F, então α será válida no frame do modelo canônico, e conseqüentemente, α será um teorema do sistema de axiomas da LDP-CCS com Composição Paralela com Sincronização.

Precisamos fazer o seguinte:

1. Construir o modelo canônico para a LDP-CCS com Composição Paralela com Sincronização;

2. Provar que o frame do modelo canônico está na classe F, e para isso temos que provar que o frame do modelo canônico é prefixado, é de soma e é de composição para as relações canônicas.

Construiremos o modelo canônico e então provaremos dois lemas que correspondem aos ítens (1) e (2) acima. O teorema 3.5.1 segue desses dois lemas.

Definição 3.5.1 : *Seja* $\mathcal{F}^c = (W^c, Z^c, R^c_\alpha, R^c_E)$ *um frame canônico para a LDP-CCS com Composição Paralela com Sincronização, onde:*

1. W^c *contém todos os conjuntos maximais consistentes sob a LDP-CCS com Composição Paralela com Sincronização;*

2. *As relações canônicas para* $w, w' \in W^c$ *são:*

$$(wR^c_\alpha w') \text{ se e somente se } \forall\varphi\ ([\alpha]\varphi \in w \text{ então } \varphi \in w')$$
$$(wR^c_E w') \text{ se e somente se } \forall\varphi\ ([E]\varphi \in w \text{ então } \varphi \in w')$$

3. *Seja* $Z^c \subseteq W^c$ *o conjunto dos estados tal que,*

$$Z^c = \{w \in W^c \mid [\acute{A}]\bot \in w\}$$

Definição 3.5.2 : *O modelo canônico $\mathcal{M}^c$ para a LDP-CCS com Composição Paralela com Sincronização é um par $\mathcal{M}^c = (\mathcal{F}^c, V^c)$ sobre $\mathcal{F}^c$, onde para cada $p \in \Phi$, $V^c(p, w) = 1$ se e somente se $p \in w$.*

Lema 3.5.1 : *Seja $\mathcal{M}^c = (W^c, R^c_\alpha, R^c_E, V^c)$ o modelo canônico definido para a LDP-CCS com Composição Paralela com Sincronização.*

1. *Se $\neg[\alpha]\varphi \in w$ então existe v tal que $(wR^c_\alpha v)$ e $\neg\varphi \in v$*

2. *Se $\neg[E]\varphi \in w$ então existe v tal que $(wR^c_E v)$ e $\neg\varphi \in v$*

Prova.

1. Suponha $\neg[\alpha]\varphi \in w$. Construiremos um v tal que $(wR^c_\alpha v)$ e $\neg\varphi \in v$.

Seja $v' = \{\neg\varphi\} \cup \{\psi | [\alpha]\psi \in w\}$.

Provaremos que v' é consistente. Então é suficiente tomar qualquer extensão maximal de v' como o conjunto v.

Entretanto, pela construção, v é um conjunto maximal consistente tal que $(wR^c_\alpha v)$ e $\neg\varphi \in v$, isto é, para todo ψ, se $[\alpha]\psi \in w$ então $\psi \in v$ e $\neg\varphi \in v$.

Agora é necessário provar que $v' = \{\neg\varphi\} \cup \{\psi | [\alpha]\psi \in w\}$ é consistente.

Suponha que v' é inconsistente. Então existem $\psi_1, ..., \psi_n$ tal que

$\vdash (\psi_1 \wedge ... \wedge \psi_n) \rightarrow \varphi$ (definição de consistência)

$\vdash [\alpha]((\psi_1 \wedge ... \wedge \psi_n) \rightarrow \varphi)$ (generalização por $[\alpha]$)

$\vdash [\alpha](\psi_1 \wedge ... \wedge \psi_n) \rightarrow [\alpha]\varphi$

$\vdash [\alpha]\psi_1 \wedge ... \wedge [\alpha]\psi_n \rightarrow [\alpha](\psi_1 \wedge ... \wedge \psi_n)$

$\vdash [\alpha]\psi_1 \wedge ... \wedge [\alpha]\psi_n \rightarrow [\alpha]\varphi$

Como $[\alpha]\psi_1 \wedge ... \wedge [\alpha]\psi_n \in w$ então $[\alpha]\varphi \in w$. Mas, pela hipótese, temos que $\neg[\alpha]\varphi \in w$, o que é uma contradição. Pois, w é maximal consistente. Conseqüentemente, v' é consistente.

2. Feito da mesma forma do item 1. □

Lema 3.5.2 *:*

1. *Se* $\forall w(\forall w'((wR^c_\alpha w') \Rightarrow \varphi \in w')) \Rightarrow [\alpha]\varphi \in w$.

2. *Se* $\forall w(\forall w'((wR^c_E w') \Rightarrow \varphi \in w') \Rightarrow [E]\varphi \in w$.

Prova.

1. Suponha que $\forall w, w' \in W^c((wR^c_\alpha w') \Rightarrow \varphi \in w')$ e não é o caso que $[\alpha]\varphi \in w$.

Então dado que w é maximal consistente, $\neg[\alpha]\varphi \in w$.

Mostramos no lema 3.5.1 que se $\neg[\alpha]\varphi \in w$ então $\exists w'((wR^c_\alpha w')$ e $\neg\varphi \in w')$. Mas, pela hipótese, $\forall w'((wR^c_\alpha w') \Rightarrow \varphi \in w')$.

Então temos que $\neg\varphi \in w'$ e $\varphi \in w'$, o que gera uma contradição, pois w' é um conjunto maximal consistente.

Conseqüentemente, de $\forall w'((wR^c_\alpha w' \Rightarrow \varphi \in w')$ concluímos que $[\alpha]\varphi \in w$.

2. Segue do mesmo modo do item anterior. □

Lema 3.5.3 **(Lema da Verdade)***: Para toda fórmula* φ *e todo* $w \in W^c$, $\varphi \in w$ *se e somente se* $(\mathcal{M}^c, w) \models \varphi$.

Prova. Provaremos usando indução no tamanho da fórmula φ.

H.I.: Para toda fórmula φ com $\mid \varphi \mid \leq n$ o lema vale.

Provaremos que o lema vale para a base e então que ele vale para as fórmulas com $\mid \varphi \mid = n+1$.

1) Base: $\varphi = p \in \Phi$

$(\mathcal{M}^c, w) \models p$ se e somente se $w \in V(p)$ (satisfatibilidade)

se e somente se $p \in w$ (def. de modelo canônico).

2) Conjunção: $\varphi_1 \wedge \varphi_2$

$(\mathcal{M}^c, w) \models \varphi_1 \wedge \varphi_2$ se e somente se $(\mathcal{M}^c, w) \models \varphi_1$ e

$(\mathcal{M}^c, w) \models \varphi_2$ (satisfatibilidade)

se e somente se $\varphi_1 \in w$ e $\varphi_2 \in w$ (H.I)

se e somente se $\varphi_1 \wedge \varphi_2 \in w$ (maximalidade de w)

3) Negação: $\neg\varphi$

$(\mathcal{M}^c, w) \models \neg\varphi$ se e somente se $(\mathcal{M}^c, w) \not\models \varphi$ (satisfatibilidade)

$\Rightarrow \varphi \notin w$ (H.I)

$\Rightarrow \neg\varphi \in w$ (maximalidade de w)

4) Programa básico: $[\alpha]\varphi$

$(\mathcal{M}^c, w) \models [\alpha]\varphi \Leftrightarrow \forall w'((wR_\alpha w') \Rightarrow (\mathcal{M}^c, w') \models \varphi)$ (satisfatibilidade)

$\Leftrightarrow \forall w'\ ((wR^c_\alpha w') \Rightarrow \varphi \in w')$ (H.I)

$\Leftrightarrow [\alpha]\varphi \in w$ (pelo lema 3.5.2).

5) Programa composto: $[E]\varphi$

$(\mathcal{M}^c, w) \models [E]\varphi \Leftrightarrow \forall w'\ ((wR_E w') \Rightarrow (\mathcal{M}^c, w') \models \varphi)$ (satisfatibilidade)

$\Leftrightarrow \forall w'(wR^c_E w') \Rightarrow \varphi \in w')$ (H.I)

$\Leftrightarrow [E]\varphi \in w$ (pelo lema 3.5.2).

□

Lema 3.5.4 : *Para* $w, w' \in W^c$, $wR^c_{\alpha\cdot E}w' \Leftrightarrow wR_\alpha; R_E w'$.

Prova.

$(\Leftarrow)$ $wR_\alpha; R_E w'$

Suponha NÃO $wR^c_{\alpha\cdot E}w' \Leftrightarrow$ NÃO $([\alpha \cdot E]\varphi \in w \Rightarrow \varphi \in w')$

$[\alpha \cdot E]\varphi \in w$ e $\neg\varphi \in w'$ (*)

$\Leftrightarrow [\alpha][E]\varphi \in w$ (pelo axioma 4 e maximalidade)

Pelo lema da verdade, $(\mathcal{M}^c, w) \models [\alpha][E]\varphi$

se e somente se $\forall v$, $wR_\alpha v \Rightarrow (\mathcal{M}^c, v) \models [E]\varphi \Rightarrow \forall w'$, $vR_E w' \Rightarrow (\mathcal{M}^c, w') \models \varphi$

Como $wR_\alpha; R_E w'$ então $(\mathcal{M}^c, w') \models \varphi \Leftrightarrow \varphi \in w'$. O que contraria (*).

$(\Rightarrow)$ $wR^c_{\alpha\cdot E}w'$

Sabemos que, $\langle\alpha \cdot E\rangle\varphi \in w$ e $\varphi \in w'$ para alguma fórmula φ.

Pelo lema da verdade, $(\mathcal{M}^c, w) \models \langle\alpha \cdot E\rangle\varphi$ e $(\mathcal{M}^c, w') \models \varphi$

Pelo axioma 4, $(\mathcal{M}^c, w) \models \langle\alpha\rangle\langle E\rangle\varphi$

se e somente se $\exists v$ tal que $wR_\alpha v$ e $(\mathcal{M}^c, v) \models \langle E\rangle\varphi$ se e somente se $\exists u$ tal que $vR_E u$

e $(\mathcal{M}^c, u) \models \varphi$ (*)

Suponha NÃO $wR_\alpha; R_E w'$, então

NÃO $\exists r(wR_\alpha r \wedge rR_E w')$. O que contraria (*). □

Lema 3.5.5 : *Para* $w, w' \in W^c$, $wR^c_{E_1+E_2}w' \Leftrightarrow w(R_{E_1} \cup R_{E_2})w'$.

Prova.

($\Leftarrow$) Suponha $w(R_{E_1} \cup R_{E_2})w'$ e NÃO $wR^c_{E_1+E_2}w'$.

NÃO $([E_1 + E_2]\varphi \Rightarrow \varphi \in w')$

$[E_1 + E_2]\varphi \in w$ e $\neg\varphi \in w'$ (*)

Pelo axioma 5, $[E_1]\varphi \wedge [E_2]\varphi \in w$

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [E_1]\varphi \wedge [E_2]\varphi$ se e somente se

$(\mathcal{M}^c, w) \models [E_1]\varphi$ e $(\mathcal{M}^c, w) \models [E_2]\varphi$ se e somente se

$\forall v$, $wR_{E_1}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$ e $\forall v$, $wR_{E_2}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$

$\forall v$, $w(R_{E_1} \cup R_{E_2})v \Rightarrow (\mathcal{M}^c, v) \models \varphi$.

Como $w(R_{E_1} \cup R_{E_2})w'$ então $(\mathcal{M}^c, w') \models \varphi$ se e somente se

$\varphi \in w'$. O que contradiz (*).

($\Rightarrow$) $wR^c_{E_1+E_2}w'$ e NÃO $w(R_{E_1} \cup R_{E_2})w'$.

NÃO $wR^c_{E_1}w'$ e NÃO $wR^c_{E_2}w'$ Se e somente se existe φ tal que $[E_1]\varphi \in w$ e $\varphi \notin w'$

e existe ψ tal que $[E_2]\psi \in w$ e $\psi \notin w'$

$[E_1]\varphi \wedge [E_2]\psi \in w$ e $\varphi \notin w'$ e $\psi \notin w' \Rightarrow$

$[E_1](\varphi \vee \psi) \wedge [E_2](\varphi \vee \psi) \in w$ e $\neg\varphi \in w'$ e $\neg\psi \in w'$.

se e somente se $[E_1 + E_2](\varphi \vee \psi) \in w$ e $(\neg\varphi \wedge \neg\psi) \in w'$ e $\neg(\varphi \vee \psi) \in w'$ (*)

se e somente se pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [E_1 + E_2](\varphi \vee \psi)$.

se e somente se $\forall v$, $wR^c_{E_1+E_2}v \Rightarrow (\mathcal{M}^c, v) \models \varphi \vee \psi$.

Como $wR^c_{E_1+E_2}w'$ então $(\mathcal{M}^c, w') \models \varphi \vee \psi$.

Se e somente se $\varphi \vee \psi \in w'$. O que contradiz (*). □

Lema 3.5.6 *: Para* $w, w' \in W^c$, $wR^c_{0+E_1}w' \Leftrightarrow wR_{E_1}w'$.

Prova.

($\Leftarrow$) Suponha $wR^c_{E_1}w'$ e NÃO $wR^c_{0+E_1}w'$.

Se e somente se NÃO $([0+E_1]\varphi \Rightarrow \varphi \in w')$.

Se e somente se $[0+E_1]\varphi \in w$ e $\neg\varphi \in w$. (*)

Pelo axioma 6, $[E_1]\varphi$.

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [E_1]\varphi$

Se e somente se $\forall v$, $wR^c_{E_1}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$.

Como $wR^c_{E_1}w'$ então $(\mathcal{M}^c, w') \models \varphi$ se e somente se $\varphi \in w'$. O que contradiz (*).

($\Rightarrow$) Suponha $wR^c_{0+E_1}w'$ e NÃO $wR^c_{E_1}w'$.

Se e somente se $\exists\varphi$ tal que $[E_1]\varphi \in w$ e $\varphi \notin w$. (*)

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [0+E_1]\varphi$.

Se e somente se $\forall v$, $wR^c_{0+E_1}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$.

Como $wR^c_{0+E_1}w'$ então $(\mathcal{M}^c, w') \models \varphi$ se e somente se $\varphi \in w'$. O que contradiz (*).

□

Lema 3.5.7 : $\forall\alpha \in Act$ *e* $\forall w(w \in Z^c \Leftrightarrow \neg\exists w', wR_\alpha w')$.

Prova.

($\Rightarrow$) Suponha que $w \in Z^c$.

Suponha que existe uma ação $\alpha \in Act$ tal que $wR_\alpha w'$.

Pela definição de Z^c, $[\mathcal{A}]\bot \in w$ para alguma φ.

Pelo axioma 7, $[\mathring{A}]\bot \in w$ e pelo lema da verdade, $(\mathcal{M}^c, w) \models [\mathring{A}]\bot$, $\forall\alpha \in Act$, α, $\alpha \neq 0$ e $\forall w'$ tal que $wR_\alpha w'$, $(\mathcal{M}^c, w') \models \bot$. O que é um absurdo. Logo, $\neg\exists\alpha \in Act$ tal que $wR_\alpha w'$ e $w \in Z^c$.

($\Leftarrow$) Suponha que $\neg\exists w' wR_\alpha w'$ se e somente se para toda φ

$[\alpha]\varphi \in w$ e $\varphi \notin w'$, em particular vale para $\bot$

$[\alpha]\bot$ para qualquer α. Logo,

$[\alpha_1]\bot \wedge [\alpha_2]\bot \wedge \cdots \wedge [\alpha_n]\bot \in w$ se e somente se

$[\mathring{A}]\bot \in w$ e portanto $w \in Z^{\mathbf{c}}$. □

Lema 3.5.8 *: $R_0^c \subseteq Z \times Z$.*

Prova.

Suponha $xR_0^c y \Leftrightarrow \forall\varphi\ \varphi \in y \Rightarrow \langle 0\rangle\varphi \in x$

$\top \in y$, logo $\langle 0\rangle\top \in x$ e

pelo axioma 9, $[\mathring{A}]\bot \in x$, logo $x \in Z$

pelo axioma 7, $\langle 0\rangle[\mathring{A}]\bot \in x$ e

pelo axioma 8, $[0][\mathring{A}]\bot \in x$ e

pelo lema da verdade, $(\mathcal{M}^c, x) \models [0][\mathring{A}]\bot$ se e somente se

$\forall z$ se $xR_0^c z \Rightarrow (\mathcal{M}^c, z) \models [\mathring{A}]\bot$

como $xR_0^c y$ então $(\mathcal{M}^c, y) \models [\mathring{A}]\bot$ e

pelo lema da verdade, $[\mathring{A}]\bot \in y$. Logo, $y \in Z$. □

Lema 3.5.9 *: R_0^c é reflexiva.*

Prova.:

Suponha que R_0^c não é reflexiva. Então para algum x, $\neg(xR_0^c x)$.

$xR_0^c y$ se e somente se $\forall\varphi\ \varphi \in y \Rightarrow \langle 0\rangle\varphi \in x$.

$\exists\varphi$ tal que $\varphi \in x$ e $\neg\langle 0\rangle\varphi \in x$. (*)

Como $x \in Z$ (por 4) então $[\mathring{A}]\bot \in x$.

Pelo axioma 7, se $\langle 0\rangle\varphi \in x$. O que contraria (*). □

Lema 3.5.10 : *R_0 é funcional.*

Prova.

Suponha que R_0 não é funcional, como R_0 é reflexiva para algum x e y.

xR_0x e xR_0y e $x \neq y$.

(1) $\forall\varphi\ xR_0x$ se e somente se $[0]\varphi \in x \Rightarrow \varphi \in x$.

(2) $\forall\psi\ xR_0y$ se e somente se $\psi \in y \Rightarrow \langle 0\rangle\psi \in x$.

De (3) $x \neq y$ e ambos são conjuntos maximais consistentes, logo para alguma fórmula

(4) $\theta \in y$ e $\theta \notin x \Leftrightarrow \neg\theta \in x$. (*)

De (4) e (2) $\langle 0\rangle\theta \in x$, como por 4, $R_0 \subseteq Z \times Z$

$x \in S$ e portanto, $[\mathring{A}]\bot \in x$ e $[\mathring{A}]\bot \wedge \langle 0\rangle\theta \in x$ e pelo axioma 8,

$\Rightarrow [0]\theta \in x$, de (1), $\theta \in x$. O que contraria (*). □

Lema 3.5.11 : $R_0 = \{(x,x) \mid x \in Z\}$

Prova.

De 4 sabemos que $R_0 \subseteq Z \times Z$, falta mostrar que $x \in Z \Rightarrow xR_0x$.

Suponha que $x \in Z$ (1) e NÃO xR_0x (2).

(1) $\Rightarrow [\mathring{A}]\bot \in x$, $\exists\varphi\ [0]\varphi \in x$ e $\varphi \notin x$ (*)

pelo axioma 7, $\vdash [\mathring{A}]\bot \rightarrow (\neg\varphi \rightarrow \langle 0\rangle\neg\varphi)$

$\vdash [\mathring{A}]\bot \rightarrow ([0]\varphi \rightarrow \varphi)$

$\vdash [\mathring{A}]\bot \wedge [0]\varphi \rightarrow \varphi$

de (1) e (2) $[\mathring{A}]\bot \wedge [0]\varphi \in x$ e pelo axioma 7, $\varphi \in x$. O que contraria (*). □

Lema 3.5.12 : *Para $w, w' \in W^c$, $wR^c_{E_1|E_2}w' \Leftrightarrow wR^c_{E_2|E_1}w'$.*

Prova.

($\Leftarrow$) Suponha $wR^c_{E_2|E_1}w'$ e NÃO $wR^c_{E_1|E_2}w'$.

Se e somente se NÃO $([E_1 \mid E_2]\varphi \in w \Rightarrow \varphi \in w')$.

Se e somente se $[E_1 \mid E_2]\varphi \in w$ e $\neg\varphi \in w'$. (*)

Pelo axioma 10, $[E_2 \mid E_1]\varphi \in w$.

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [E_2 \mid E_1]\varphi$

Se e somente se $\forall v \in W^c$, $wR^c_{E_2|E_1}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$

Como $wR_{E_2|E_1}w'$ então $(\mathcal{M}^c, w') \models \varphi$. O que contradiz (*).

($\Rightarrow$) Suponha $wR^c_{E_1|E_2}w'$ e NÃO $wR^c_{E_2|E_1}w'$.

Se e somente se $\exists\varphi$ tal que $[E_2 \mid E_1]\varphi \in w$ e $\varphi \notin w'$.

Se e somente se $[E_1 \mid E_2]\varphi \in w$ e $\neg\varphi \notin w'$.(*)

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [E_2 \mid E_1]\varphi$

Se e somente se $\forall v$, $wR^c_{E_1|E_2}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$.

Como $wR^c_{E_1|E_2}w'$ então $(\mathcal{M}^c, w') \models \varphi$.

Se e somente se $\varphi \in w'$. O que contradiz (*). □

Lema 3.5.13 : *Para* $w, w' \in W^c$, $wR^c_{(E_1|E_2)|E_3}w' \Leftrightarrow wR^c_{E_1|(E_2|E_3)}w'$.

Prova.

$\Leftarrow$ Suponha $wR^c_{(E_1|E_2)|E_3}w'$ e NÃO $wR^c_{E_1|(E_2|E_3)}w'$.

Se e somente se NÃO $([E_1 \mid (E_2 \mid E_3)]\varphi \in w \Rightarrow \varphi \in w')$.

Se e somente se $[E_1 \mid (E_2 \mid E_3)]\varphi \in w$ e $\neg\varphi \in w'$. (*)

Pelo axioma 11, $[E_1 \mid (E_2 \mid E_3)]\varphi \in w$.

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [E_1 \mid (E_2 \mid E_3)]\varphi$

Se e somente se $\forall v \in W^c$, $wR^c_{E_1|(E_2|E_3)}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$

Como $wR_{E_1|(E_2|E_3)}w'$ então $(\mathcal{M}^c, w') \models \varphi$. O que contradiz (*).

($\Rightarrow$) Suponha $wR^c_{E_1|(E_2|E_3)}w'$ e NÃO $wR^c_{(E_1|E_2)|E_3}w'$.

Se e somente se $\exists\varphi$ tal que $[(E_1 \mid E_2) \mid E_3]\varphi \in w$ e $\varphi \notin w'$.

Se e somente se $[(E_1 \mid E_2) \mid E_3]\varphi \in w$ e $\neg\varphi \notin w'$.(*)

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [(E_1 \mid E_2) \mid E_3]\varphi$

Se e somente se $\forall v$, $wR^c_{(E_1|E_2)|E_3}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$.

Como $wR^c_{(E_1|E_2)|E_3}w'$ então $(\mathcal{M}^c, w') \models \varphi$.

Se e somente se $\varphi \in w'$. O que contradiz (*). □

Lema 3.5.14 : *Para* $w, w' \in W^c$, $wR^c_{E|0}w' \Leftrightarrow wR^c_E w'$.

Prova.

($\Leftarrow$) Suponha $wR^c_E w'$ e NÃO $wR^c_{E|0}w'$.

Se e somente se NÃO $([E \mid 0]\varphi \in w \Rightarrow \varphi \in w')$.

Se e somente se $[E \mid 0]\varphi \in w$ e $\neg\varphi \in w'$. (*)

Pelo axioma 12, $[E]\varphi \in w$.

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [E]\varphi$.

Se e somente se $\forall v \in W^c$, $wR^c_E v \Rightarrow (\mathcal{M}^c, v) \models \varphi$

Como $wR_E w'$ então $(\mathcal{M}^c, w') \models \varphi$. O que contradiz (*).

($\Rightarrow$) Suponha $wR^c_{E|0}w'$ e NÃO $wR^c_E w'$.

Se e somente se $\exists\varphi$ tal que $[E]\varphi \in w$ e $\varphi \notin w'$.

Se e somente se $[E]\varphi \in w$ e $\neg\varphi \notin w'$.(*)

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [E]\varphi$

Se e somente se $\forall v$, $wR^c_E v \Rightarrow (\mathcal{M}^c, v) \models \varphi$.

Como $wR^c_{E|0}w'$ então $(\mathcal{M}^c, w') \models \varphi$.

Se e somente se $\varphi \in w'$. O que contradiz (*). □

Lema 3.5.15 : *Para* $w, w' \in W^c$, $wR^c_{(E_1+E_2)|E_3}w' \Leftrightarrow wR^c_{(E_1|E_3)+(E_2|E_3)}w'$.

Prova.

($\Leftarrow$) Suponha $wR^c_{(E_1|E_3)+(E_2|E_3)}w'$ e NÃO $wR^c_{(E_1+E_2)|E_3}w'$.

Se e somente se NÃO $([(E_1 + E_2) \mid E_3]\varphi \in w \Rightarrow \varphi \in w')$.

Se e somente se $[(E_1 + E_2) \mid E_3]\varphi \in w$ e $\neg\varphi \in w'$. (*)

Pelo axioma 13, $[(E_1 \mid E_3) + (E_2 \mid E_3)]\varphi \in w$.

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [(E_1 \mid E_3) + (E_2 \mid E_3)]\varphi$

Se e somente se $\forall v \in W^c$, $wR^c_{(E_1|E_3)+(E_2|E_3)}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$

Como $wR_{(E_1|E_3)+(E_2|E_3)}w'$ então $(\mathcal{M}^c, w') \models \varphi$. O que contradiz (*).

($\Rightarrow$) Suponha $wR^c_{(E_1+E_2)|E_3}w'$ e NÃO $wR^c_{(E_1|E_3)+(E_2|E_3)}w'$.

Se e somente se $\exists\varphi$ tal que $[(E_1 + E_2) \mid E_3]\varphi \in w$ e $\varphi \notin w'$.

Se e somente se $[(E_1 + E_2) \mid E_3]\varphi \in w$ e $\neg\varphi \notin w'$.(*)

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [(E_1 + E_2) \mid E_3]\varphi$

Se e somente se $\forall v \in W^c$, $wR^c_{(E_1+E_2)|E_3}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$.

Como $wR^c_{(E_1|E_2)|E_3}w'$ então $(\mathcal{M}^c, w') \models \varphi$.

Se e somente se $\varphi \in w'$. O que contradiz (*). □

Lema 3.5.16 : *Para* $w, w' \in W^c$, $wR_{\alpha.(E_1|E_2)}w' \Rightarrow wR_{(\alpha.E_1)|E_2}w'$.

Prova.

Suponha $wR_{\alpha.(E_1|E_2)}w'$ e NÃO $wR_{(\alpha.E_1)|E_2}w'$.

Se e somente se $\exists\varphi$ tal que $[(\alpha.E_1) \mid E_2]\varphi \in w$ e $\varphi \notin w'$.

Se e somente se $[(\alpha.E_1) \mid E_2]\varphi \in w$ e $\neg\varphi \in w'$. (*)

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [(\alpha.E_1) \mid E_2]\varphi$.

Se e somente se $\forall v \in W^c$, $wR_{\alpha.(E_1|E_2)}v \Rightarrow$, $(\mathcal{M}^c, v) \models \varphi$.

Como $wR_{\alpha.(E_1|E_2)}w'$ então $(\mathcal{M}^c, w') \models \varphi$.

Se e somente se $\varphi \in w'$. O que contradiz (*). □

Lema 3.5.17 *:*

Para $w, w' \in W^c$, $wR_{(\alpha_1.E_1)|(\alpha_2.E_2)}w' \Leftrightarrow wR_{\alpha_1.(E_1|\alpha_2.E_2)+\alpha_2.(\alpha_1.E_1|E_2)}w'$.

Prova.

($\Leftarrow$) Suponha $wR_{\alpha_1.(E_1|\alpha_2.E_2)+\alpha_2.(\alpha_1.E_1|E_2)}w'$ e NÃO $wR_{(\alpha_1.E_1)|(\alpha_2.E_2)}w'$

Se e somente se NÃO $([(\alpha_1.E_1) \mid (\alpha_2.E_2)]\varphi \in w \Rightarrow \varphi \in w')$.

Se e somente se $[(\alpha_1.E_1) \mid (\alpha_2.E_2)]\varphi \in w$ e $\neg\varphi \in w'$. (*)

Pelo axioma 15, $[\alpha_1.(E_1 \mid \alpha_2.E_2)]\varphi \wedge [\alpha_2.(\alpha_1.E_1 \mid E_2)]\varphi$.

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [\alpha_1.(E_1 \mid \alpha_2.E_2)]\varphi \wedge [\alpha_2.(\alpha_1.E_1 \mid E_2)]\varphi$.

Se e somente se $\forall v \in W^c$, $wR_{\alpha_1.(E_1|\alpha_2.E_2)+\alpha_2.(\alpha_1.E_1|E_2)}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$.

Como $wR_{\alpha_1.(E_1|\alpha_2.E_2)+\alpha_2.(\alpha_1.E_1|E_2)}w'$ então $(\mathcal{M}^c, w') \models \varphi$. O que contradiz (*).

($\Rightarrow$) Suponha $wR_{(\alpha_1.E_1)|(\alpha_2.E_2)}w'$ e NÃO $wR_{\alpha_1.(E_1|\alpha_2.E_2)+\alpha_2.(\alpha_1.E_1|E_2)}w'$

Se e somente se $\exists\varphi$ tal que $[\alpha_1.(E_1 \mid \alpha_2.E_2)]\varphi \wedge [\alpha_2.(\alpha_1.E_1 \mid E_2)]\varphi \in w$ e $\neg\varphi \in w'$

Se e somente se $[\alpha_1.(E_1 \mid \alpha_2.E_2)]\varphi \wedge [\alpha_2.(\alpha_1.E_1 \mid E_2)]\varphi \in w$ e $\neg\varphi \in w'$. (*)

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [\alpha_1.(E_1 \mid \alpha_2.E_2)]\varphi \wedge [\alpha_2.(\alpha_1.E_1 \mid E_2)]\varphi$

Se e somente se $\forall v \in W^c$, $wR_{(\alpha_1.E_1)|(\alpha_2.E_2)}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$.

Como $wR_{(\alpha_1.E_1)|(\alpha_2.E_2)}w'$ então $(\mathcal{M}^c, w') \models \varphi$.

Se e somente se $\varphi \in w'$. O que contradiz (*). □

Lema 3.5.18 *:*

Para $w, w' \in W^c$, $wR_{(\alpha.E_1)|(\overline{\alpha}.E_2)}w' \Leftrightarrow (w, w') \in R_{\alpha.(E_1|\overline{\alpha}.E_2)+\overline{\alpha}.(\alpha.E_1|E_2)+\tau.(E_1|E_2)}$.

Prova.

($\Leftarrow$) Suponha $wR_{\alpha.(E_1|\overline{\alpha}.E_2)+\overline{\alpha}.(\alpha;E_1|E_2)+\tau.(E_1|E_2)}w'$ e NÃO $wR_{(\alpha.E_1)|(\overline{\alpha}.E_2)}w'$

Se e somente se NÃO $([(\alpha.E_1) \mid (\overline{\alpha}.E_2)]\varphi \in w \Rightarrow \varphi \in w')$.

Se e somente se $[(\alpha.E_1) \mid (\overline{\alpha}.E_2)]\varphi \in w$ e $\neg\varphi \in w'$. (*)

Pelo axioma 16, $[(\alpha.(E_1 \mid \overline{\alpha}.E_2)]\varphi \wedge [\overline{\alpha}.(\alpha; E_1 \mid E_2)]\varphi \wedge [\tau.(E_1 \mid E_2)]\varphi \in w$.

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [\alpha.(E_1 \mid \overline{\alpha}.E_2)]\varphi \wedge [\overline{\alpha}.(\alpha; E_1 \mid E_2)]\varphi \wedge [\tau.(E_1 \mid E_2)]\varphi$.

Se e somente se $\forall v \in W^c$, $wR_{\alpha.(E_1|\overline{\alpha}.E_2)+\overline{\alpha}.(\alpha.E_1|E_2)+\tau.(E_1|E_2)}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$

Como $wR_{\alpha.(E_1|\overline{\alpha}.E_2)+\overline{\alpha}.(\alpha.E_1|E_2)+\tau.(E_1|E_2)}w' \Rightarrow (\mathcal{M}^c, w') \models \varphi$. O que contradiz (*).

($\Rightarrow$) Suponha $wR_{(\alpha.E_1)|(\overline{\alpha}.E_2)}w'$ e NÃO $wR_{\alpha.(E_1|\overline{\alpha}.E_2)+\overline{\alpha}.(\alpha.E_1|E_2)+\tau.(E_1|E_2)}w'$

Se e somente se $\exists\varphi$ tal que $[\alpha.(E_1 \mid \overline{\alpha}.E_2)]\varphi \wedge [\overline{\alpha}.(\alpha.E_1 \mid E_2)]\varphi \wedge [\tau.(E_1 \mid E_2)]\varphi \in w$ e $\varphi \notin w'$.

Se e somente se $[\alpha.(E_1 \mid \overline{\alpha}.E_2)]\varphi \wedge [\overline{\alpha}.(\alpha.E_1 \mid E_2)]\varphi \wedge [\tau.(E_1 \mid E_2)]\varphi \in w$ e $\neg\varphi \in w'$.(*)

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [(\alpha.E_1) \mid (\overline{\alpha}.E_2)]\varphi$.

Se e somente se $\forall v \in W^c$, $wR_{((\alpha.E_1)|(\overline{\alpha}.E_2))}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$

Como $wR_{((\alpha.E_1)|(\overline{\alpha}.E_2))}w'$ então $(\mathcal{M}^c, w') \models \varphi$.

Se e somente se $\varphi \in w'$. O que contradiz (*). □

3.6 Adicionando Restrição

3.6.1 Sintaxe

Definição 3.6.1 : *A linguagem* **LDP-CCS com Composição Paralela com Sincronização e Restrição** *é definida usando os mesmos símbolos e operadores da definição 3.2.1 com o acréscimo do operador CCS:* $\backslash$.

$$\varphi ::= p \mid \bot \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \rightarrow \varphi_2 \mid \neg\varphi \mid [K]\varphi \mid [E]\varphi$$

$$\alpha ::= a \mid \overline{a} \mid \tau$$

$$E ::= 0 \mid \alpha \cdot E \mid E_1 + E_2 \mid E_1|E_2 \mid E \setminus L$$

onde, $K \subseteq Act$, $\mathcal{L} \subseteq \mathring{A} \cup \overline{\mathring{A}}$ *e* $L \subseteq \mathcal{L}$.

3.6.2 Semântica

Definição 3.6.2 : *Um* **frame** *para a LDP-CCS com Composição com Sincronização e Restrição é* $\mathcal{F} = (W, Z, R_\alpha, R_E)$, *onde:*

W *é um conjunto não vazio de estados;*

Z *é um conjunto de estados finais,* $Z \subseteq W$, *onde*

$$\forall \alpha \in Act \text{ e } \forall w (w \in Z \Leftrightarrow \neg\exists w', wR_\alpha w')$$

R_α *é uma relação binária para cada programa básico* α ;

R_E *é uma relação binária para cada programa composto* E, *onde:*

$R_{(\alpha \cdot E)\backslash L} = R_\alpha ; R_{E\backslash L}$ *se* $\alpha \notin L$

$R_{(\alpha \cdot E)\backslash L} = R_0$ *se* $\alpha \in L$

$R_{(E_1+E_2)\backslash L} = R_{E_1\backslash L} \cup R_{E_2\backslash L}$

$R_0 = \{(x, x) \mid x \in Z\}$

$R_{(E_1|E_2)\backslash L}$ *satisfaz as seguintes condições:*

i. $R_{(E_1|E_2)\backslash L} = R_{(E_2|E_1)\backslash L}$ *(comutativa)*

ii. $R_{((E_1|E_2)|E_3)\backslash L} = R_{(E_1|(E_2|E_3))\backslash L}$ *(associativa)*

iii. $R_{(E|0)\backslash L} = R_{(E)\backslash L}$

iv. $R_{((E_1+E_2)|E_3)\backslash L} = R_{((E_1|E_3)+(E_2|E_3))\backslash L}$

v. $R_{((\alpha.E_1)|E_2)\backslash L} \supseteq R_{(\alpha.(E_1|E_2))\backslash L}$, *se* $\alpha \notin L$

vi. $R_{((\alpha.E_1)|E_2)\backslash L} = R_{(0|E_2)\backslash L}$, *se* $\alpha \in L$

vii. $R_{((\alpha_1.E_1)|(\alpha_2.E_2))\backslash L} = R_{(\alpha_1.(E_1|\alpha_2.E_2)+\alpha_2.(\alpha_1.E_1|E_2))\backslash L}$, *se* $\alpha_1, \alpha_2 \notin L$

viii. $R_{((\alpha.E_1)|(\overline{\alpha}.E_2))\backslash L} = R_{(\alpha.(E_1|\overline{\alpha}.E_2)+\overline{\alpha}.(\alpha.E_1|E_2)+\tau.(E_1|E_2))\backslash L}$, *se* $\alpha, \overline{\alpha} \notin L$

ix. $R_{(\alpha.E)\backslash L} = R_0$, *se* $\alpha \in L$

x. $R_{((\alpha.E_1)|(\overline{\alpha}.E_2))\backslash L} = R_{\tau.(E_1|E_2)}$, *se* $\alpha \in L$

Definição 3.6.3 : *Um* **modelo** *para a LDP-CCS com Composição Paralela com Sincronização e Restrição é* $\mathcal{M} = (W, Z, R_\alpha, R_E, V)$, *onde* V *é uma função valoração mapeando símbolos proposicionais em subconjuntos de* W.

Definição 3.6.4 : *Seja* $\mathcal{M} = (W, Z, R_\alpha, R_E, V)$ *um modelo e* $w \in W$. *Definimos a noção de* **satisfação** *de uma fórmula* φ *num modelo* $\mathcal{M}$ *em um estado* w, $(\mathcal{M},w) \models \varphi$, *como segue:*

1. $(\mathcal{M},w) \models p$ *se e somente se* $p \in V(p)$.

2. $(\mathcal{M},w) \models \bot$ *se e somente se* $w \notin W$.

3. $(\mathcal{M},w) \models \neg\varphi$ *se e somente se* $(\mathcal{M},w) \not\models \varphi$.

4. $(\mathcal{M},w) \models \varphi_1 \wedge \varphi_2$ *se e somente se* $(\mathcal{M},w) \models \varphi_1$ *e* $(\mathcal{M},w) \models \varphi_2$.

5. $(\mathcal{M},w) \models [K]\varphi$ *se e somente se* $\forall w' \in W$ *e* $\forall \alpha \in K$, *se* $wR_\alpha w'$ *então* $(\mathcal{M},w') \models \varphi$.

6. $(\mathcal{M},w) \models [E]\varphi$ *se e somente se* $\forall w' \in W$, *se* $wR_E w'$ *então* $(\mathcal{M},w') \models \varphi$.

Se $(\mathcal{M},w) \models \varphi$ para todo estado w, dizemos que φ é válido no modelo $\mathcal{M}$, $\mathcal{M} \models \varphi$. E se φ é válida em todos os modelos $\mathcal{M}$, dizemos que φ é válida, $\models \varphi$.

3.6.3 Axiomatização

1. todas as tautologias

2. $[K](\varphi \to \psi) \to [K]\varphi \to [K]\psi$

3. $[E](\varphi \to \psi) \to [E]\varphi \to [E]\psi$

4. $[(\alpha \cdot E) \setminus L]\varphi \leftrightarrow [\alpha][E \setminus L]\varphi$, se $\alpha \notin L$

5. $[(E_1 + E_2) \setminus L]\varphi \leftrightarrow [E_1 \setminus L]\varphi \wedge [E_2 \setminus L]\varphi$

6. $[(0 + E_1) \setminus L]\varphi \to [E_1 \setminus L]\varphi$

7. $\varphi \wedge [\mathring{A}]\bot \to \langle 0\rangle\varphi$ (reflexividade de R_0)

8. $[\mathring{A}]\bot \wedge \langle 0\rangle\varphi \to [0]\varphi$ (R_0 é funcional)

9. $[\alpha](\varphi \wedge [\mathring{A}]\bot) \to [\alpha \cdot 0]\varphi$

10. $[\mathring{A}]\bot \leftrightarrow \langle 0\rangle\top$

11. $[(E_1 \mid E_2) \setminus L]\varphi \leftrightarrow [(E_2 \mid E_1) \setminus L]\varphi$

12. $[((E_1 \mid E_2) \mid E_3) \setminus L]\varphi \leftrightarrow [(E_1 \mid (E_2 \mid E_3)) \setminus L]\varphi$

13. $[(E \mid 0) \setminus L]\varphi \leftrightarrow [E \setminus L]\varphi$

14. $[((E_1 + E_2) \mid E_3) \setminus L]\varphi \leftrightarrow [((E_1 \mid E_3) + (E_2 \mid E_3)) \setminus L]\varphi$

15. $[((\alpha.E_1) \mid E_2) \setminus L]\varphi \rightarrow [(\alpha.(E_1 \mid E_2)) \setminus L]\varphi$, se $\alpha \notin L$

16. $[((\alpha.E_1) \mid E_2) \setminus L]\varphi \rightarrow [(0 \mid E_2) \setminus L]\varphi$, se $\alpha \in L$

17. $[((\alpha_1.E_1) \mid (\alpha_2.E_2)) \setminus L]\varphi \leftrightarrow [(\alpha_1.(E_1 \mid \alpha_2.E_2)]\varphi \wedge [\alpha_2.(\alpha_1.E_1 \mid E_2)) \setminus L]\varphi$, se $\alpha_1, \alpha_2 \notin L$

18. $[((\alpha.E_1) \mid (\overline{\alpha}.E_2)) \setminus L]\varphi \leftrightarrow [(\alpha.(E_1 \mid \overline{\alpha}.E_2)) \setminus L]\varphi \wedge [(\overline{\alpha}.(\alpha; E_1 \mid E_2)) \setminus L]\varphi \wedge [(\tau.(E_1 \mid E_2)) \setminus L]\varphi$, se $\alpha, \overline{\alpha} \notin L$

19. $[(\alpha \cdot E) \setminus L]\varphi \leftrightarrow [0]\varphi$, se $\alpha \in L$

20. $[((\alpha.E_1) \mid (\overline{\alpha}.E_2)) \setminus L]\varphi \leftrightarrow [\tau.(E_1 \mid E_2)]\varphi$, se $\alpha, \overline{\alpha} \in L$

Regras de Inferência:

Substituição Uniforme:

$$\frac{\vdash \varphi}{\vdash \varphi(\beta_1/p_1, \cdots, \beta_n/p_n)}$$

Modus Ponens:

$$\frac{\varphi, \varphi \rightarrow \psi}{\psi}$$

Generalização:

$$\frac{\vdash \varphi}{\vdash [K]\varphi} \quad \frac{\vdash \varphi}{\vdash [E]\varphi}$$

3.6.4 Corretude

Considere um frame $\mathcal{F} = (W, Z, R_\alpha, R_E)$, onde as relações R_α e R_E, são descritas na definição 3.6.2. Seja $\mathcal{M}$ um modelo para $\mathcal{F}$.

Teorema 3.6.1 *: Todo teorema do Esquema de Axiomas é válido na classe de frames F.*

Prova. Temos que provar que:

- Todo axioma do Esquema de Axiomas é válido na classe de frames F.
- As regras de inferência preservam validade na classe de frames F.

Lema 3.6.1 *: Para todas as fórmulas e todos os programas:*

1. $F \models [K](\varphi \to \psi) \to [K]\varphi \to [K]\psi$
2. $F \models [E](\varphi \to \psi) \to [E]\varphi \to [E]\psi$
3. $F \models [(\alpha \cdot E) \setminus L]\varphi \leftrightarrow [\alpha][E \setminus L]\varphi$, *se* $\alpha \notin L$
4. $F \models [(E_1 + E_2) \setminus L]\varphi \leftrightarrow [E_1 \setminus L]\varphi \wedge [E_2 \setminus L]\varphi$
5. $F \models [(0 + E_1) \setminus L]\varphi \to [E_1 \setminus L]\varphi$
6. $F \models \varphi \wedge [\mathring{A}]\bot \to \langle 0\rangle\varphi$ *(reflexividade de* R_0*)*
7. $F \models [\mathring{A}]\bot \wedge \langle 0\rangle\varphi \to [0]\varphi$ *(*R_0 *é funcional)*
8. $F \models [\alpha](\varphi \wedge [\mathring{A}]\bot) \to [\alpha \cdot 0]\varphi$
9. $F \models [\mathring{A}]\bot \leftrightarrow \langle 0\rangle\top$

10. $F \models [(E_1 \mid E_2) \setminus L]\varphi \leftrightarrow [(E_2 \mid E_1) \setminus L]\varphi$

11. $F \models [((E_1 \mid E_2) \mid E_3) \setminus L]\varphi \leftrightarrow [(E_1 \mid (E_2 \mid E_3)) \setminus L]\varphi$

12. $F \models [(E \mid 0) \setminus L]\varphi \leftrightarrow [E \setminus L]\varphi$

13. $F \models [((E_1 + E_2) \mid E_3) \setminus L]\varphi \leftrightarrow [((E_1 \mid E_3) + (E_2 \mid E_3)) \setminus L]\varphi$

14. $F \models [((\alpha.E_1) \mid E_2) \setminus L]\varphi \rightarrow [(\alpha.(E_1 \mid E_2)) \setminus L]\varphi$, *se* $\alpha \notin L$

15. $F \models [((\alpha.E_1) \mid E_2) \setminus L]\varphi \rightarrow [(0 \mid E_2) \setminus L]\varphi$, *se* $\alpha \in L$

16. $F \models [((\alpha_1.E_1) \mid (\alpha_2.E_2)) \setminus L]\varphi \leftrightarrow [(\alpha_1.(E_1 \mid \alpha_2.E_2) \setminus L]\varphi \wedge [(\alpha_2.(\alpha_1.E_1 \mid E_2)) \setminus L]\varphi$, *se* $\alpha_1, \alpha_2 \notin L$

17. $F \models [((\alpha.E_1) \mid (\overline{\alpha}.E_2)) \setminus L]\varphi \leftrightarrow [(\alpha.(E_1 \mid \overline{\alpha}.E_2)) \setminus L]\varphi \wedge [(\overline{\alpha}.(\alpha.E_1 \mid E_2)) \setminus L]\varphi \wedge [(\tau.(E_1 \mid E_2)) \setminus L]\varphi$, *se* $\alpha, \overline{\alpha} \notin L$

18. $F \models [(\alpha \cdot E) \setminus L]\varphi \leftrightarrow [0]\varphi$, *se* $\alpha \in L$

19. $F \models [((\alpha.E_1) \mid (\overline{\alpha}.E_2)) \setminus L]\varphi \leftrightarrow [\tau.(E_1 \mid E_2)]\varphi$, *se* $\alpha, \overline{\alpha} \in L$

Prova.

1. Idem prova 1. do lema 3.4.1.

2. Idem prova 2. do lema 3.4.1.

3. Suponha, por contradição, que existe um modelo $\mathcal{M} = (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$$(\mathcal{M}, w) \not\models [(\alpha \cdot E) \setminus L]\varphi \leftrightarrow [\alpha][E \setminus L]\varphi, \text{ se } \alpha \notin L$$

Então,

(1) $(\mathcal{M}, w) \not\models [(\alpha \cdot E) \setminus L]\varphi \rightarrow [\alpha][E \setminus L]\varphi$, se $\alpha \notin L$ ou

(2) $(\mathcal{M}, w) \not\models [\alpha][E \setminus L]\varphi \rightarrow [(\alpha \cdot E) \setminus L]\varphi$, se $\alpha \notin L$

(1) se e somente se (3) $(\mathcal{M}, w) \models [(\alpha \cdot E) \setminus L]\varphi$ e (4) $(\mathcal{M}, w) \not\models [\alpha][E \setminus L]\varphi$.

(3) se e somente se $\forall w', w'' \in W$ se $wR_{(\alpha \cdot E)\setminus L}w''$, se $\alpha \notin L$, então $(\mathcal{M}, w'') \models \varphi$.

Como $R_{(\alpha \cdot E)\setminus L} = R_\alpha; R_{E\setminus L}$, pela definição 3.6.2, então se $\forall w'' \in W, wR_\alpha; R_{E\setminus L}w''$ então $(\mathcal{M}, w'') \models \varphi$.

(4) se e somente se (5) $\mathcal{M}, w \models \langle\alpha\rangle\langle E \setminus L\rangle\neg\varphi$.

(5) se e somente se $\exists w', w'' \in W$ tal que $wR_\alpha w'$ e $w'R_{E\setminus L}w''$, então $(\mathcal{M}, w'') \models \neg\varphi$.

Então existe um $w'' \in W$ tal que $wR_\alpha; R_{E\setminus L}w''$ e $(\mathcal{M}, w'') \models \neg\varphi$. O que contradiz (3).

Ou (2) se e somente se (6) $(\mathcal{M}, w) \models [\alpha][E \setminus L]\varphi$ e (7) $(\mathcal{M}, w) \not\models [(\alpha \cdot E) \setminus L]\varphi$.

(6) se e somente se $\forall w', w'' \in W$ se $wR_\alpha w'$ e $w'R_{E\setminus L}w''$, então $(\mathcal{M}, w'') \models \varphi$.

Como $R_\alpha; R_{E\setminus L} = R_{(\alpha \cdot E)\setminus L}$, pela definição 3.6.2, então se $\forall w'' \in W, wR_\alpha; R_{E\setminus L}w''$ então $(\mathcal{M}, w'') \models \varphi$.

(7) se e somente se (8) $(\mathcal{M}, w) \models \langle(\alpha \cdot E) \setminus L\rangle\neg\varphi$.

(8) se e somente se $\exists w', w'' \in W$ tal que $wR_{(\alpha \cdot E)\setminus L}w''$, então $(\mathcal{M}, w'') \models \neg\varphi$. O que contradiz (6).

4. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$$(\mathcal{M}, w) \not\models [(E_1 + E_2) \setminus L]\varphi \leftrightarrow [E_1 \setminus L]\varphi \wedge [E_2 \setminus L]\varphi$$

Então,

(1) $(\mathcal{M}, w) \not\models [(E_1 + E_2) \setminus L]\varphi \rightarrow [E_1 \setminus L]\varphi \wedge [E_2 \setminus L]\varphi$ ou

(2) $(\mathcal{M}, w) \not\models [E_1 \setminus L]\varphi \wedge [E_2 \setminus L]\varphi \rightarrow [(E_1 + E_2) \setminus L]\varphi$

(1) se e somente se (3) $(\mathcal{M}, w) \models [(E_1 + E_2) \setminus L]\varphi$ e (4) $(\mathcal{M}, w) \not\models [E_1 \setminus L]\varphi \wedge [E_2 \setminus L]\varphi$.

(3) se e somente se $\forall w' \in W$ se $wR_{(E_1+E_2)\setminus L}w'$ então $(\mathcal{M}, w') \models \varphi$.

Como $R_{(E_1+E_2)\setminus L} = R_{E_1\setminus L} \cup R_{E_2\setminus L}$, pela definição 3.6.2, então $\forall w' \in W$ se $wR_{E_1\setminus L}w'$ ou $wR_{E_2\setminus L}w'$ então $(\mathcal{M}, w') \models \varphi$.

(4) se e somente se (5) $(\mathcal{M}, w) \models \langle E_1 \setminus L\rangle\neg\varphi$ ou (6) $(\mathcal{M}, w) \models \langle E_2 \setminus L\rangle\neg\varphi$.

(5) se e somente se $\exists w' \in W$ tal que $wR_{E_1\setminus L}w'$ e $(\mathcal{M}, w') \models \neg\varphi$. O que contradiz (3). Ou

(6) se e somente se $\exists w' \in W$ tal que $wR_{E_2\setminus L}w'$ e $(\mathcal{M}, w') \models \neg\varphi$. O que contradiz (3).

ou (2) se e somente se (7) $(\mathcal{M}, w) \models [E_1 \setminus L]\varphi \wedge [E_2 \setminus L]\varphi$ e (8) $(\mathcal{M}, w) \not\models [(E_1 + E_2) \setminus L]\varphi$.

(7) se e somente se (9) $(\mathcal{M}, w) \models [E_1 \setminus L]\varphi$ e (10) $(\mathcal{M}, w) \models [E_2 \setminus L]\varphi$.

(9) se e somente se $\forall w' \in W$ se $wR_{E_1\setminus L}w'$ então $(\mathcal{M}, w') \models \varphi$ e

(10) se e somente se $\forall w' \in W$ se $wR_{E_2\setminus L}w'$ então $(\mathcal{M}, w') \models \varphi$.

(8) se e somente se (11) $(\mathcal{M}, w \models)\langle(E_1 + E_2) \setminus L\rangle\neg\varphi$.

(11) se e somente se $\exists w' \in W$ tal que $wR_{(E_1+E_2)\setminus L}w'$ então $(\mathcal{M}, w') \models \neg\varphi$. Como $R_{(E_1+E_2)\setminus L} = R_{E_1\setminus L} \cup R_{E_2\setminus L}$, pela definição 3.6.2, então $\exists w'$ tal que $wR_{E_1}w'$ ou $wR_{E_2}w'$ e $(\mathcal{M}, w') \models \neg\varphi$. O que contradiz (9) e (10).

5. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$$(\mathcal{M}, w) \not\models [(0 + E_1) \setminus L]\varphi \rightarrow [E_1 \setminus L]\varphi$$

Então,

(1) $(\mathcal{M}, w) \models [(0 + E_1) \setminus L]\varphi$ e

(2) $(\mathcal{M}, w) \not\models [E_1 \setminus L]\varphi$

(1) se e somente se$\forall w' \in W$ se $wR_{(0+E_1)\setminus L}w'$ então $(\mathcal{M}, w') \models \varphi$.

Como $R_{(0+E_1)\setminus L} = R_{E_1\setminus L}$, pela definição 3.6.2, pois R_0 é reflexiva, então $\forall w' \in W, wR_{E_1\setminus L}w'$ e $(\mathcal{M}, w') \models \varphi$.

(2) se e somente se (3) $(\mathcal{M}, w) \models \langle E_1 \setminus L\rangle\neg\varphi$.

(3) se e somente se $\exists w' \in W$ tal que $wR_{E_1\setminus L}w'$ e $(\mathcal{M}, w') \models \neg\varphi$. O que contraria (1).

6. Idem prova 6. do lema 3.4.1.

7. Idem prova 7. do lema 3.4.1.

8. Idem prova 8. do lema 3.4.1.

9. Idem prova 9. do lema 3.4.1.

10. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$$(\mathcal{M}, w) \not\models [(E_1 \mid E_2) \setminus L]\varphi \leftrightarrow [(E_2 \mid E_1) \setminus L]\varphi$$

Então,

(1) $(\mathcal{M}, w) \not\models [(E_1 \mid E_2) \setminus L]\varphi \rightarrow [(E_2 \mid E_1) \setminus L]\varphi$ ou

(2) $(\mathcal{M}, w) \not\models [(E_2 \mid E_1) \setminus L]\varphi \rightarrow [(E_1 \mid E_2) \setminus L]\varphi$

(1) se e somente se (3) $(\mathcal{M}, w) \models [(E_1 \mid E_2) \setminus L]\varphi$ e (4) $(\mathcal{M}, w) \not\models [(E_2 \mid E_1) \setminus L]\varphi$.

(3) se e somente se $\forall w' \in W$ se $wR_{(E_1|E_2)\setminus L}w'$ então $(\mathcal{M}, w') \models \varphi$.(*)

Como $R_{(E_1|E_2)\setminus L} = R_{(E_2|E_1)\setminus L}$, pela definição 3.6.2, então $\forall w' \in W, wR_{(E_2|E_1)\setminus L}w'$ e $(\mathcal{M}, w') \models \varphi$.

(4) se e somente se (5) $(\mathcal{M}, w) \models \langle(E_2 \mid E_1) \setminus L\rangle\neg\varphi$.

(5) se e somente se $\exists w' \in W$ tal que $wR_{(E_2|E_1)\setminus L}w'$ e $(\mathcal{M}, w') \models \neg\varphi$. O que contraria (*).

(2) se e somente se (6) $(\mathcal{M}, w) \models [(E_2 \mid E_1) \setminus L]\varphi$ e (7) $(\mathcal{M}, w) \not\models [(E_1 \mid E_2) \setminus L]\varphi$.

(6) se e somente se $\forall w' \in W$ se $wR_{(E_2|E_1)\setminus L}w'$ então $(\mathcal{M}, w') \models \varphi$.(**)

(7) se e somente se (8) $\mathcal{M}, w \models \langle(E_1 \mid E_2) \setminus L\rangle\neg\varphi$.

(8) se e somente se $\exists w' \in W$ tal que $wR_{(E_1|E_2)\setminus L}w'$,, como $R_{E_1|E_2} = R_{E_2|E_1}$, pela definição 3.6.2, e $(\mathcal{M}, w') \models \neg\varphi$. O que contraria (**).

11. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$$(\mathcal{M}, w) \not\models [((E_1 \mid E_2) \mid E_3) \setminus L]\varphi \leftrightarrow [(E_1 \mid (E_2 \mid E_3)) \setminus L]\varphi$$

Então,

(1) $(\mathcal{M}, w) \not\models [((E_1 \mid E_2) \mid E_3) \setminus L]\varphi \rightarrow [(E_1 \mid (E_2 \mid E_3)) \setminus L]\varphi$ ou

(2) $(\mathcal{M}, w) \not\models [(E_1 \mid (E_2 \mid E_3)) \setminus L]\varphi \rightarrow [((E_1 \mid (E_2) \mid E_3) \setminus L]\varphi$

(1) se e somente se (3) $(\mathcal{M}, w) \models [((E_1 \mid (E_2) \mid E_3) \setminus L]\varphi$ e (4) $(\mathcal{M}, w) \not\models [(E_1 \mid (E_2 \mid E_3)) \setminus L]\varphi$.

(3) se e somente se $\forall w' \in W$ se $wR_{((E_1|E_2)|E_3)\setminus L}w'$ então $(\mathcal{M}, w') \models \varphi$.(*)

Como $R_{((E_1|E_2)|E_3)\setminus L} = R_{(E_1|(E_2|E_3))\setminus L}$, pela definição 3.6.2, então $\forall w' \in W$, $wR_{(E_1|(E_2)|E_3))\setminus L}w'$ então $(\mathcal{M},w') \models \varphi$.

(4) se e somente se (5) $(\mathcal{M}, w) \models \langle(E_1 \mid (E_2 \mid E_3)) \setminus L\rangle\neg\varphi$.

(5) se e somente se $\exists w' \in W$ tal que $wR_{(E_1|(E_2|E_3))\setminus L}w'$ e $(\mathcal{M}, w') \models \neg\varphi$. O que contraria (*).

(2) se e somente se (6) $(\mathcal{M}, w) \models [(E_1 \mid (E_2 \mid E_3)) \setminus L]\varphi$ e (7) $(\mathcal{M}, w) \not\models [((E_1 \mid E_2) \mid E_3) \setminus L]\varphi$.

(6) se e somente se $\forall w' \in W$ se $wR_{(E_1|(E_2|E_3))\setminus L}w'$ então $(\mathcal{M}, w') \models \varphi$. (**)

(7) se e somente se (8) $(\mathcal{M}, w) \models \langle((E_1 \mid E_2) \mid E_3) \setminus L\rangle\neg\varphi$.

(8) se e somente se $\exists w' \in W$ tal que $wR_{((E_1|E_2)|E_3)\setminus L}w'$ e como $R_{((E_1|E_2)|E_3)\setminus L} = R_{(E_1|(E_2|E_3))\setminus L}$, pela definição 3.6.2, e $(\mathcal{M}, w') \models \neg\varphi$. O que contraria (**).

12. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$$(\mathcal{M}, w) \not\models [(0 \mid E) \setminus L]\varphi \leftrightarrow [E \setminus L]\varphi$$

Então,

(1) $(\mathcal{M}, w) \not\models [(0 \mid E) \setminus L]\varphi \rightarrow [E \setminus L]\varphi$ e

(2) $(\mathcal{M}, w) \not\models [E \setminus L]\varphi \rightarrow [(0 \mid E) \setminus L]\varphi$

(1) se e somente se (3) $(\mathcal{M}, w) \models [(0 \mid E) \setminus L]\varphi$ e (4) $(\mathcal{M}, w) \not\models [E \setminus L]\varphi$.

(3) se e somente se $w \in W$, se $wR_{(E|0)\setminus L}w'$ então $(\mathcal{M},w') \models \varphi$.(*)

Como $R_{(0|E)\setminus L} = R_{E\setminus L}$, pela definição 3.6.2, então $\forall w' \in W$, $wR_{E\setminus L}w'$ e $(\mathcal{M},w') \models \varphi$.

(4) se e somente se (5) $(\mathcal{M}, w) \models \langle E \setminus L\rangle\neg\varphi$.

(5) se e somente se $\exists w' \in W$ tal que $wR_{E\setminus L}w'$, e $(\mathcal{M},w') \models \neg\varphi$. O que contraria (*).

(2) se e somente se (6) $(\mathcal{M}, w) \models [E \setminus L]\varphi$ e (7) $(\mathcal{M}, w) \not\models [(0 \mid E) \setminus L]\varphi$.

(6) se e somente se $\forall w' \in W$ se $wR_{E\setminus L}w'$ então $(\mathcal{M}, w') \models \varphi$.(**)

(7) se e somente se (8) $(\mathcal{M}, w) \models \langle (0 \mid E) \setminus L \rangle \neg\varphi$.

(8) se e somente se $\exists w' \in W$ tal que $R_{(0|E)\setminus L} = R_{E\setminus L}$, pela definição 3.6.2, então $wR_{(0|E)\setminus L}w'$ e $(\mathcal{M}, w') \models \neg\varphi$. O que contraria (**).

13. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$$(\mathcal{M}, w) \not\models [((E_1 + E_2) \mid E_3) \setminus L]\varphi \leftrightarrow [((E_1 \mid E_3) + (E_2 \mid E_3)) \setminus L]\varphi$$

Então

(1) $(\mathcal{M}, w) \not\models [((E_1 + E_2) \mid E_3) \setminus L]\varphi \rightarrow [((E_1 \mid E_3) + (E_2 \mid E_3)) \setminus L]\varphi$ ou

(2) $(\mathcal{M}, w) \not\models [((E_1 \mid E_3) + (E_2 \mid E_3)) \setminus L]\varphi \rightarrow [((E_1 + E_2) \mid E_3) \setminus L]\varphi$

(1) se e somente se $(\mathcal{M}, w) \models [((E_1 + E_2) \mid E_3) \setminus L]\varphi$ e (4) $(\mathcal{M}, w) \models [((E_1 \mid E_3) + (E_2 \mid E_3) \setminus L]\varphi$.

(3) se e somente se $\forall w' \in W$ se $wR_{((E_1+E_2)|E_3)\setminus L}w'$ então $(\mathcal{M}, w') \models \varphi$.(*)

Como $R_{((E_1+E_2)|E_3)\setminus L} = R_{((E_1|E_3)+(E_2|E_3))\setminus L}$, pela definição 3.6.2, então se $\forall w' \in W$, $wR_{((E_1|E_3)+(E_2|E_3))\setminus L}w'$ então $(\mathcal{M}, w') \models \varphi$.

(4) se e somente se (5) $(\mathcal{M}, w) \models \langle ((E_1 \mid E_3) + (E_2 \mid E_3)) \setminus L \rangle \neg\varphi$.

(5) se e somente se $\exists w' \in W$ tal que $wR_{((E_1|E_3)+(E_2|E_3))\setminus L}w'$ e $(\mathcal{M}, w') \models \neg\varphi$. O que contradiz (*).

(2) se e somente se (6) $(\mathcal{M}, w) \models [((E_1 \mid E_3) + (E_2 \mid E_3)) \setminus L]\varphi$ e (7) $(\mathcal{M}, w) \not\models [((E_1 + E_2) \mid E_3) \setminus L]\varphi$.

(6) se e somente se $\forall w' \in W$ se $wR_{((E_1|E_3)+(E_2|E_3))\setminus L}w'$ então $(\mathcal{M}, w') \models \varphi$.(**)

(7) se e somente se (8) $(\mathcal{M}, w) \models \langle ((E_1 + E_2) \mid E_3) \setminus L \rangle \neg\varphi$.

(8) se e somente se $\exists w' \in W$ tal que $wR_{((E_1+E_2)|E_3)\setminus L}w'$ e como $R_{((E_1+(E_2)|E_3)\setminus L} =$

$R_{((E_1|E_3)+(E_2|E_3))\setminus L}$, pela definição 3.6.2, e $(\mathcal{M}, w') \models \neg\varphi$. O que contradiz (**).

14. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$$(\mathcal{M}, w) \not\models [(\alpha \cdot (E_1 \mid E_2)) \setminus L]\varphi \rightarrow [((\alpha.(E_1) \mid E_2) \setminus L]\varphi$$

Então,

(1) $(\mathcal{M}, w) \models [(\alpha.(E_1 \mid E_2)) \setminus L]\varphi$ e

(2) $(\mathcal{M}, w) \not\models [((\alpha.E_1) \mid E_2) \setminus L]\varphi$

(1) se e somente se $\forall w' \in W$ se $wR_{(\alpha.(E_1|E_2))\setminus L}w'$ então $(\mathcal{M}, w') \models \varphi$. (*)

Como $R_{((\alpha.E_1)|E_2)\setminus L} \supseteq R_{(\alpha.(E_1|E_2))\setminus L}$, pela definição 3.6.2, então $\forall w' \in W, wR_{((\alpha.E_1)|E_2)\setminus L}w'$ e $(\mathcal{M}, w') \models \varphi$.

(2) se e somente se (3) $\mathcal{M}, w \models \langle((\alpha.E_1) \mid E_2) \setminus L\rangle\neg\varphi$.

(3) se e somente se $\exists w' \in W$ tal que $wR_{((\alpha.E_1)|E_2)\setminus L}w'$ e $(\mathcal{M}, w') \models \neg\varphi$. O que contradiz (*).

15. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$$(\mathcal{M}, w) \not\models [((\alpha.E_1) \mid E_2) \setminus L]\varphi \rightarrow [(0 \mid E_2) \setminus L]\varphi, \text{ se } \alpha \in L$$

Então,

(1) $(\mathcal{M}, w) \models [((\alpha.E_1) \mid E_2) \setminus L]\varphi$ e

(2) $(\mathcal{M}, w) \not\models [(0 \mid E_2) \setminus L]\varphi$

(1) se e somente se $\forall w' \in W$ se $wR_{((\alpha.E_1)|E_2)\setminus L}w'$, se $\alpha \in L$, então $(\mathcal{M}, w') \models \varphi$. (*)

Como $R_{((\alpha.E_1)|E_2)\setminus L} = R_{(0|E_2)\setminus L}$, se $\alpha \in L$, pela definição 3.6.2, então $\forall w' \in W, wR_{(0|E_2)\setminus L}w'$ e $(\mathcal{M}, w') \models \varphi$.

(2) se e somente se (3) $(\mathcal{M}, w) \models \langle(0 \mid E_2) \setminus L\rangle\neg\varphi$.

(3) se e somente se $\exists w' \in W$ tal que $wR_{(0|E_2)\setminus L}w'$ e $(\mathcal{M}, w') \models \neg\varphi$. O que contradiz (*).

16. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$$(\mathcal{M}, w) \not\models [((\alpha_1.E_1) \mid (\alpha_2.E_2)) \setminus L]\varphi \leftrightarrow [(\alpha_1.(E_1 \mid \alpha_2.E_2)) \setminus L]\varphi \wedge [(\alpha_2.(\alpha_1.E_1 \mid E_2)) \setminus L]\varphi$$

Então,

$$(1)\ (\mathcal{M}, w) \not\models [((\alpha_1.E_1) \mid (\alpha_2.E_2)) \setminus L]\varphi \rightarrow [(\alpha_1.(E_1 \mid \alpha_2.E_2)) \setminus L]\varphi \wedge [(\alpha_2.(\alpha_1.E_1 \mid E_2)) \setminus L]\varphi \text{ ou}$$

$$(2)\ (\mathcal{M}, w) \not\models [(\alpha_1.(E_1 \mid \alpha_2.E_2)) \setminus L]\varphi \wedge [(\alpha_2.(\alpha_1.E_1 \mid E_2)) \setminus L]\varphi \rightarrow [((\alpha_1.E_1) \mid (\alpha_2.E_2)) \setminus L]\varphi$$

(1) se e somente se (3) $(\mathcal{M}, w) \models [((\alpha_1.E_1) \mid (\alpha_2.E_2)) \setminus L]\varphi$ e (4) $(\mathcal{M}, w) \not\models [(\alpha_1.(E_1 \mid \alpha_2.E_2)) \setminus L]\varphi \wedge [(\alpha_2.(\alpha_1.E_1 \mid E_2)) \setminus L]\varphi$.

(3) se e somente se $\forall w' \in W$ se $wR_{((\alpha_1.E_1)|(\alpha_2.E_2))\setminus L}w'$ então $(\mathcal{M}, w') \models \varphi$. (*)

Como $R_{((\alpha_1.E_1)|(\alpha_2.E_2))\setminus L} = R_{(\alpha_1.(E_1|\alpha_2.E_2)+\alpha_2.(\alpha_1.E_1|E_2))\setminus L}$, pela definição 3.6.2, então $\forall w' \in W\ wR_{(\alpha_1.(E_1|\alpha_2.E_2)+\alpha_2.(\alpha_1.E_1|E_2))\setminus L}w'$ e $(\mathcal{M}, w') \models \varphi$.

(4) se e somente se (5) $(\mathcal{M}, w) \not\models [(\alpha_1.(E_1 \mid \alpha_2.E_2)) \setminus L]\varphi$ e (6) $(\mathcal{M}, w) \not\models [(\alpha_2.(\alpha_1.E_1 \mid E_2)) \setminus L]\varphi$.

(5) se e somente se (7) $(\mathcal{M}, w) \models \langle(\alpha_1.(E_1 \mid \alpha_2.E_2)) \setminus L\rangle\neg\varphi$.

(7) se e somente se $\exists w' \in W$ tal que $wR_{(\alpha_1.(E_1|\alpha_2.E_2))\setminus L}w'$ e $(\mathcal{M}, w') \models \neg\varphi$. O que contradiz (*).

(6) se e somente se (8) $(\mathcal{M}, w) \models \langle(\alpha_2.(\alpha_1.E_1 \mid E_2)) \setminus L\rangle\neg\varphi$.

(8) se e somente se $\exists w' \in W$ tal que $wR_{(\alpha_2.(\alpha_1.E_1|E_2))\setminus L}w'$ e $(\mathcal{M}, w') \models \neg\varphi$. O que contradiz (*).

(2) se e somente se (9) $(\mathcal{M}, w) \not\models [(\alpha_1.(E_1 \mid \alpha_2.E_2)) \setminus L]\varphi \wedge [(\alpha_2.(\alpha_1.E_1 \mid E_2)) \setminus L]\varphi$ e (10) $(\mathcal{M}, w) \not\models [((\alpha_1.E_1) \mid (\alpha_2.E_2)) \setminus L]\varphi$.

(9) se e somente se (11) $(\mathcal{M}, w) \models [(\alpha_1.(E_1 \mid \alpha_2.E_2)) \setminus L]\varphi$ e (12) $(\mathcal{M}, w) \models [(\alpha_2.(\alpha_1.E_1 \mid E_2)) \setminus L]\varphi$.

(11) se e somente se $\forall w' \in W$ se $wR_{(\alpha_1.(E_1|\alpha_2.E_2))\setminus L}w'$ então $\mathcal{M}, w' \models \varphi$.(*)

(12) se e somente se $\forall w' \in W$ se $wR_{(\alpha_2.(\alpha_1.E_1|E_2))\setminus L}w'$ então $(\mathcal{M}, w') \models \varphi$.(**)

Como $R_{((\alpha_1.E_1)|(\alpha_2.E_2))\setminus L} = R_{(\alpha_1.(E_1|\alpha_2.E_2)+\alpha_2.(\alpha_1.E_1|E_2))\setminus L}$, pela definição 3.6.2, então $\forall w' \in W\ wR_{(\alpha_1.(E_1|\alpha_2.E_2)+\alpha_2.(\alpha_1.E_1|E_2))\setminus L}w'$ então $(\mathcal{M}, w') \models \varphi$.

(10) se e somente se (13) $(\mathcal{M}, w) \models \langle((\alpha_1.E_1) \mid (\alpha_2.E_2)) \setminus L\rangle\neg\varphi$.

(13) se somente se $\exists w' \in W$ tal que $wR_{((\alpha_1.E_1)|(\alpha_2.E_2))\setminus L}w'$ e $(\mathcal{M}, w') \models \neg\varphi$. O que contradiz (*) e (**).

17. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$$(\mathcal{M}, w) \not\models [(\alpha.E_1) \mid (\overline{\alpha}.E_2) \setminus L]\varphi \leftrightarrow [(\alpha.(E_1 \mid \overline{\alpha}.E_2)) \setminus L]\varphi \wedge [(\overline{\alpha}.(\alpha.E_1 \mid E_2)) \setminus L]\varphi \wedge [(\tau.(E_1 \mid E_2)) \setminus L]\varphi$$

Então,

(1) $(\mathcal{M}, w) \not\models [((\alpha.E_1) \mid (\overline{\alpha}.E_2)\backslash L]\varphi \rightarrow [(\alpha.(E_1 \mid \overline{\alpha}.E_2))\backslash L]\varphi \wedge [(\overline{\alpha}.(\alpha.E_1 \mid E_2)) \setminus L]\varphi \wedge [(\tau.(E_1 \mid E_2)) \setminus L]\varphi$ ou

(2) $(\mathcal{M}, w) \not\models [(\alpha.(E_1 \mid \overline{\alpha}.E_2)) \setminus L]\varphi \wedge [(\overline{\alpha}.(\alpha; E_1 \mid E_2)) \setminus L]\varphi \wedge [(\tau.(E_1 \mid E_2)) \setminus L]\varphi \rightarrow [((\alpha.E_1) \mid (\overline{\alpha}.E_2)) \setminus L]\varphi$

(1) se e somente se (3) $(\mathcal{M}, w) \models [((\alpha.E_1) \mid (\overline{\alpha}.E_2)) \setminus L]\varphi$ e (4) $(\mathcal{M}, w) \not\models [(\alpha.(E_1 \mid \overline{\alpha}.E_2)) \setminus L]\varphi \wedge [(\overline{\alpha}.(\alpha.E_1 \mid E_2)) \setminus L]\varphi \wedge [(\tau.(E_1 \mid E_2)) \setminus L]\varphi$.

(3) se e somente se $\forall w' \in W$ se $wR_{(((\alpha.E_1)|(\overline{\alpha}.E_2)))\backslash L}w'$ então $(\mathcal{M}, w') \models \varphi$.(*)

Como $R_{((\alpha.E_1)|(\overline{\alpha}.E_2))\backslash L} = R_{(\alpha.(E_1|\overline{\alpha}.E_2)+\overline{\alpha}.(\alpha.E_1|E_2)+\tau.(E_1|E_2))\backslash L}$, pela definição 3.6.2, então $\forall w' \in W, wR_{(\alpha.(E_1|\overline{\alpha}.E_2)+\overline{\alpha}.(\alpha.E_1|E_2)+\tau.(E_1|E_2))\backslash L}w'$ e $(\mathcal{M}, w') \models \varphi$.

(4) se e somente se (5) $(\mathcal{M}, w) \models \langle(\alpha.(E_1 \mid \overline{\alpha}.E_2)) \setminus L\rangle\neg\varphi \vee \langle(\overline{\alpha}.(\alpha.E_1 \mid E_2)) \setminus L\rangle\neg\varphi \vee \langle(\tau.(E_1 \mid E_2)) \setminus L\rangle\neg\varphi$.

(5) se e somente se $\exists w' \in W$ tal que $wR_{(\alpha.(E_1|\overline{\alpha}.E_2)+\overline{\alpha}.(\alpha.E_1|E_2)+\tau.(E_1|E_2))\backslash L}w'$ e $(\mathcal{M}, w') \models \neg\varphi$. O que contraria (*).

(2) se e somente se (6) $(\mathcal{M}, w) \models [(\alpha.(E_1 \mid \overline{\alpha}.E_2)) \setminus L]\varphi \wedge [(\overline{\alpha}.(\alpha.E_1 \mid E_2)) \setminus L]\varphi \wedge [(\tau.(E_1 \mid E_2)) \setminus L]\varphi$ e (7) $(\mathcal{M}, w) \not\models [((\alpha.E_1) \mid (\overline{\alpha}.E_2)) \setminus L]\varphi$.

(6) se e somente se $\forall w' \in W$ se $wR_{(\alpha.(E_1|\overline{\alpha}.E_2)+\overline{\alpha}.(\alpha.E_1|E_2)+\tau.(E_1|E_2))\backslash L}w'$ então $(\mathcal{M}, w') \models \varphi$. (**)

(7) se e somente se (8) $(\mathcal{M}, w) \models \langle((\alpha.E_1) \mid (\overline{\alpha}.E_2)) \setminus L\rangle\neg\varphi$.

(8) se e somente se $\exists w' \in W$ tal que $wR_{(((\alpha.E_1)|(\overline{\alpha}.E_2)))\backslash L}w'$ e como $R_{(((\alpha.E_1)|(\overline{\alpha}.E_2)))\backslash L} = R_{(\alpha.(E_1|\overline{\alpha}.E_2)+\overline{\alpha}.(\alpha.E_1|E_2)+\tau.(E_1|E_2))\backslash L}$, pela definição 3.6.2, então $(\mathcal{M}, w') \models \neg\varphi$. O que contraria (**).

18. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$$(\mathcal{M}, w) \not\models [(\alpha.E) \setminus L]\varphi \leftrightarrow [0]\varphi, \text{ se } \alpha \in L$$

Então

(1) $(\mathcal{M}, w) \not\models [(\alpha.E) \setminus L]\varphi \rightarrow [0]\varphi$, se $\alpha \in L$ ou

(2) $(\mathcal{M}, w) \not\models [0]\varphi \rightarrow [(\alpha.E) \setminus L]\varphi$, se $\alpha \in L$

(1) se e somente se (3) $(\mathcal{M}, w) \models [(\alpha.E) \setminus L]\varphi$ e (4) $(\mathcal{M}, w) \not\models [0]\varphi$.

(3) se e somente se $\nexists w' \in W$ tal que $wR_{(\alpha.E)\setminus L}w'$, se $\alpha \in L$ e pela definição 3.6.2, $R_{(\alpha.E)\setminus L} = R_0$, se $\alpha \in L$ e como R_0 é reflexiva temos que $(\mathcal{M}, w) \models \varphi$. (*)

(4) se e somente se (5) $(\mathcal{M}, w) \models \langle 0\rangle\neg\varphi$

(5) se e somente se $\forall w \in W$ se wR_0w então $(\mathcal{M}, w) \models \neg\varphi$. O que contradiz (*).

(2) se e somente se (6) $(\mathcal{M}, w) \models [0]\varphi$ e (7) $(\mathcal{M}, w) \not\models [(\alpha.E) \setminus L]\varphi$, se $\alpha \in L$

(6) se e somente se $\forall w \in W$ se wR_0w então $(\mathcal{M}, w) \models \varphi$. (*)

(7) se e somente se (8) $(\mathcal{M}, w) \models \langle(\alpha.E) \setminus L\rangle\neg\varphi$, se $\alpha \in L$.

(8) se e somente se $\nexists w' \in W$ tal que $wR_{(\alpha.E)\setminus L}w'$, se $\alpha \in L$ e pela definição 3.6.2, $R_{(\alpha.E)\setminus L} = R_0$, se $\alpha \in L$ e como R_0 é reflexiva temos que $(\mathcal{M}, w) \models \neg\varphi$. O que contradiz (*).

19. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$$(\mathcal{M}, w) \not\models [((\alpha.E_1) \mid (\overline{\alpha}.E_2)) \setminus L]\varphi \leftrightarrow [\tau.(E_1 \mid E_2)]\varphi, \text{ se } \alpha, \overline{\alpha} \in L$$

Então

(1) $(\mathcal{M}, w) \not\models [((\alpha.E_1) \mid (\overline{\alpha}.E_2)) \setminus L]\varphi \rightarrow [\tau.(E_1 \mid E_2)]\varphi$, se $\alpha, \overline{\alpha} \in L$ ou

(2) $(\mathcal{M}, w) \not\models [\tau.(E_1 \mid E_2)]\varphi \rightarrow [((\alpha.E_1) \mid (\overline{\alpha}.E_2)) \setminus L]\varphi$, se $\alpha, \overline{\alpha} \in L$

(1) se e somente se (3) $(\mathcal{M}, w) \models [((\alpha.E_1) \mid (\overline{\alpha}.E_2)) \setminus L]\varphi$ e (4) $(\mathcal{M}, w) \not\models [\tau.(E_1 \mid E_2)]\varphi$.

(3) se e somente se $\forall w' \in W$ se $wR_{((\alpha.E_1)|(\overline{\alpha}.E_2))\setminus L}w'$, se $\alpha \in L$, então $(\mathcal{M}, w') \models \varphi$. (*)

Como $R_{((\alpha.E_1)|(\overline{\alpha}.E_2))\setminus L} = R_{\tau.(E_1|E_2)}$, se $\alpha \in L$, pela definição 3.6.2, então $\forall w' \in W, wR_{\tau.(E_1|E_2)}w'$ e $(\mathcal{M}, w') \models \varphi$.

(4) se e somente se (5) $(\mathcal{M}, w) \models \langle\tau.(E_1 \mid E_2\rangle\neg\varphi$.

(5) se e somente se $\exists w' \in W$ tal que $wR_{\tau.(E_1|E_2}w'$ e $(\mathcal{M}, w') \models \neg\varphi$. O que contradiz (*).

(2) se e somente se (6) $(\mathcal{M}, w) \models [\tau.(E_1 \mid E_2)]\varphi$ e (7) $(\mathcal{M}, w) \not\models [((\alpha.E_1) \mid (\overline{\alpha}.E_2)) \setminus L]\varphi$, se $\alpha, \overline{\alpha} \in L$.

(6) se e somente se $\forall w' \in W$ se $wR_{\tau.(E_1|E_2}w'$ então $(\mathcal{M}, w') \models \varphi$. (*)

(7) se e somente se (8) $(\mathcal{M}, w) \models \langle((\alpha.E_1) \mid (\overline{\alpha}.E_2)) \setminus L\rangle\neg\varphi$.

(8) se e somente se $\exists w' \in W$ tal que $wR_{((\alpha.E_1)|(\overline{\alpha}.E_2))\setminus L}w'$ e como $R_{((\alpha.E_1)|(\overline{\alpha}.E_2))\setminus L} = R_{\tau.(E_1|E_2)}$, se $\alpha \in L$, pela definição 3.6.2,então $(\mathcal{M}, w') \models \neg\varphi$. O que contradiz (*).

□

□

Lema 3.6.2 : *Para todas as fórmulas e todos os programas α e E tal que,*

1. *Se $\mathcal{M} \models \varphi$ e $\mathcal{M} \models \varphi \rightarrow \psi$ então $\mathcal{M} \models \psi$*

2. *Se* $\mathcal{M} \models \varphi$ *então* $\mathcal{M} \models [\alpha]\varphi$

3. *Se* $\mathcal{M} \models \varphi$ *então* $\mathcal{M} \models [E]\varphi$

Prova.: Idem prova do lema 3.4.2.

□

3.6.5 Completude

Nesta seção apresentaremos a prova do teorema da completude para a LDP-CCS com Composição Paralela com Sincronização e Restrição.

Considere a classe de frames $F = (W, Z, R_\alpha, R_E)$.

Teorema 3.6.2 : *Toda fórmula válida na classe de frames* F *é um teorema do sistema de axiomas da LDP-CCS com Composição Paralela com Sincronização e Restrição.*

Prova. Na prova do teorema usaremos a técnica do modelo canônico, isto é, construiremos um modelo canônico para a LDP-CCS com Composição Paralela com Sincronização e Restrição e depois mostraremos que o frame do modelo canônico esta na classe F.

O modelo canônico tem a propriedade que toda fbf α é verdade no modelo canônico se e somente se ela é um teorema do sistema.

Mostrando que o frame do modelo canônico está na classe F, e fazendo α válida em F, então α será válida no frame do modelo canônico, e conseqüentemente, α será um teorema do sistema de axiomas da LDP-CCS com Composição Paralela com Sincronização e Restrição.

Precisamos fazer o seguinte:

1. Construir o modelo canônico para a LDP-CCS com Composição Paralela com Sincronização e Restrição;

2. Provar que o frame do modelo canônico está na classe F, e para isso temos que provar que o frame do modelo canônico é prefixado, é de soma, é de composição e é de restrição para as relações canônicas.

Construiremos o modelo canônico e então provaremos dois lemas que correspondem aos ítens (1) e (2) acima. o teorema 3.6.2 segue desses dois lemas.

Definição 3.6.5 : *Seja* $\mathcal{F}^c = (W^c, Z^c, R^c_\alpha, R^c_E,)$ *um frame canônico para a LDP-CCS com Composição Paralela com Sincronização e Restrição, onde:*

1. W^c *contém todos os conjuntos maximais consistentes sob a LDP-CCS com Composição Paralela com Sincronização e Restrição;*

2. *As relações canônicas para* $w, w' \in W^c$ *são:*

$$(wR^c_\alpha w') \text{ se e somente se } \forall w, w' \ ([K]\varphi \in w \text{ então } \varphi \in w')$$
$$(wR^c_E w') \text{ se e somente se } \forall w, w' \ ([E]\varphi \in w \text{ então } \varphi \in w')$$

3. *Seja* $Z^c \subseteq W^c$ *o conjunto dos estados tal que,*

$$Z^c = \{w \in W^c \mid [\mathring{A}]\bot \in w\}$$

Definição 3.6.6 : *O modelo canônico* $\mathcal{M}^c$ *para a LDP-CCS com Composição Paralela com Sincronização e Restrição é um par* $\mathcal{M}^c = (\mathcal{F}^c, V^c)$ *sobre* $\mathcal{F}^c$, *onde para cada* $p \in \Phi$, $V^c(p, w) = 1$ *se e somente se* $p \in w$.

Lema 3.6.3 : *Seja* $\mathcal{M}^c = (W^c, R^c_\alpha, R^c_E, V^c)$ *o modelo canônico definido para a LDP-CCS com Composição Paralela com Sincronização e Restrição.*

1. *Se* $\neg[K]\varphi \in w$ *então existe* v *tal que* $((wR^c_\alpha v$ *e* $\neg\varphi \in v)$

2. *Se* $\neg[E]\varphi \in w$ *então existe* v *tal que* $(wR^c_E v$ *e* $\neg\varphi \in v)$

Prova. Idem prova do Lema 3.5.1. □

Lema 3.6.4 *:*

1. *Se* $\forall w, w' \in W^c((wR^c_\alpha w') \Rightarrow \varphi \in w')$ *então* $[K]\varphi \in w$.

2. *Se* $\forall w, w' \in W^c((wR^c_E w') \Rightarrow \varphi \in w')$ *então* $[E]\varphi \in w$.

Prova.

1. Suponha que $\forall w, w' \in W^c((wR^c_\alpha w') \Rightarrow \varphi \in w')$ e não é o caso que $[\alpha]\varphi \in w$.

Então dado que w é maximal consistente, $\neg[\alpha]\varphi \in w$.

Mostramos no lema 3.5.1 que se $\neg[\alpha]\varphi \in w$ então $\exists w'((wR^c_\alpha w')$ e $\neg\varphi \in w')$. Mas, pela hipótese, $\forall w'((wR^c_\alpha w') \Rightarrow \varphi \in w')$.

Então temos que $\neg\varphi \in w'$ e $\varphi \in w'$, o que gera uma contradição, pois w' é um conjunto maximal consistente.

Conseqüentemente, de $\forall w'((wR^c_\alpha w' \Rightarrow \varphi \in w')$ concluímos que $[\alpha]\varphi \in w$.

2. Suponha que $\forall w, w' \in W^c((wR^c_E w') \Rightarrow \varphi \in w')$ e não é o caso que $[E]\varphi \in w$.

Então dado que w é maximal consistente, $\neg[E]\varphi \in w$.

Mostramos no lema 3.5.1 que se $\neg[E]\varphi \in w$ então $\exists w'((wR^c_E w')$ e $\neg\varphi \in w')$. Mas, pela hipótese, $\forall w'((wR^c_E w') \Rightarrow \varphi \in w')$.

Então temos que $\neg\varphi \in w'$ e $\varphi \in w'$, o que gera uma contradição, pois w' é um conjunto maximal consistente.

Conseqüentemente, de $\forall w'((wR^c_E w' \Rightarrow \varphi \in w')$ concluímos que $[E]\varphi \in w$. □

Lema 3.6.5 (Lema da Verdade): *Para toda fórmula φ e todo $w \in W^c$, $\varphi \in w$ se e somente se $(\mathcal{M}^c, w) \models \varphi$.*

Prova. Idem prova do Lema 3.5.3. □

Lema 3.6.6 : *Para $wR^c_{(\alpha \cdot E)\setminus L}w' \Leftrightarrow wR^c_\alpha; R^c_{E\setminus L}w'$.*

Prova.

($\Leftarrow$) $wR^c_\alpha; R^c_{E\setminus L}w'$

Suponha NÃO $wR^c_{(\alpha \cdot E)\setminus L}w' \Leftrightarrow$ NÃO $([(\alpha \cdot E) \setminus L]\varphi \in w \Rightarrow \varphi \in w')$

$[(\alpha \cdot E) \setminus L]\varphi \in w$ e $\neg\varphi \in w'$ (*)

$\Leftrightarrow [\alpha][E \setminus L]\varphi \in w$ (pelo axioma 4 e maximalidade)

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [\alpha][E \setminus L]\varphi$

se e somente se $\forall v$, $wR^c_\alpha v \Rightarrow (\mathcal{M}^c, v) \models [E \setminus L]\varphi \Rightarrow \forall w'$, $vR^c_{E\setminus L}w' \Rightarrow (\mathcal{M}^c, w') \models \varphi$

Como $wR^c_\alpha; R^c_{E\setminus L}w'$ então $(\mathcal{M}^c, w') \models \varphi \Leftrightarrow \varphi \in w'$. O que contraria (*).

($\Rightarrow$) $wR^c_{(\alpha \cdot E)\setminus L}w'$

Sabemos que, $\langle(\alpha \cdot E) \setminus L\rangle\varphi \in w$ e $\varphi \in w'$ para alguma fórmula φ.

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models \langle(\alpha \cdot E) \setminus L\rangle\varphi$ e $(\mathcal{M}^c, w') \models \varphi$

Pelo axioma 4, $(\mathcal{M}^c, w) \models \langle\alpha\rangle\langle E \setminus L\rangle\varphi$

se e somente se $\exists v$ tal que $wR^c_\alpha v$ e $(\mathcal{M}^c, v) \models \langle E \setminus L\rangle\varphi$ se e somente se $\exists u$ tal que $vR^c_E u$ e $(\mathcal{M}^c, u) \models \varphi$ (*)

Suponha NÃO $wR^c_\alpha; R^c_{E\setminus L}w'$, então

NÃO $\exists r(wR^c_\alpha r \wedge rR^c_{E\setminus L}w')$. O que contraria (*). □

Lema 3.6.7 : *Para $wR^c_{(E_1+E_2)\setminus L}w' \Leftrightarrow wR^c_{E_1\setminus L}w' \cup wR^c_{E_2\setminus L}w'$.*

Prova.

($\Leftarrow$) Suponha $w(R^c_{E_1\setminus L} \cup R^c_{E_2\setminus L})w'$ e NÃO $wR^c_{(E_1+E_2)\setminus L}w'$.

NÃO $([(E_1 + E_2) \setminus L]\varphi \Rightarrow \varphi \in w')$

$[(E_1 + E_2) \setminus L]\varphi \in w$ e $\neg\varphi \in w'$ (*)

Pelo axioma 5, $[E_1 \setminus L]\varphi \wedge [E_2 \setminus L]\varphi \in w$

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [E_1 \setminus L]\varphi \wedge [E_2 \setminus L]\varphi$ se e somente se

$(\mathcal{M}^c, w) \models [E_1 \setminus L]\varphi$ e $(\mathcal{M}^c, w) \models [E_2 \setminus L]\varphi$ se e somente se

$\forall v,\ wR^c_{E_1\setminus L}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$ e $\forall v,\ wR^c_{E_2\setminus L}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$

$\forall v,\ w(R^c_{E_1\setminus L} \cup R^c_{E_2\setminus L})v \Rightarrow (\mathcal{M}^c, v) \models \varphi$.

Como $w(R^c_{E_1\setminus L} \cup R^c_{E_2\setminus L})w'$ então $(\mathcal{M}^c, w') \models \varphi$ se e somente se

$\varphi \in w'$. O que contradiz (*).

$(\Rightarrow)$ $wR^c_{(E_1+E_2)\setminus L}w'$ e NÃO $w(R_{E_1\setminus L} \cup R_{E_2\setminus L})w'$.

NÃO $wR^c_{E_1\setminus L}w'$ e NÃO $wR^c_{E_2\setminus L}w'$ Se e somente se existe φ tal que $[E_1 \setminus L]\varphi \in w$ e

$\varphi \notin w'$ e existe ψ tal que $[E_2 \setminus L]\psi \in w$ e $\psi \notin w'$

$[E_1 \setminus L]\varphi \wedge [E_2 \setminus L]\psi \in w$ e $\varphi \notin w'$ e $\psi \notin w' \Rightarrow$

$[E_1 \setminus L](\varphi \vee \psi) \wedge [E_2 \setminus L](\varphi \vee \psi) \in w$ e $\neg\varphi \in w'$ e $\neg\psi \in w'$.

se e somente se $[(E_1 + E_2) \setminus L](\varphi \vee \psi) \in w$ e $(\neg\varphi \wedge \neg\psi) \in w'$ e $\neg(\varphi \vee \psi) \in w'$ (*)

se e somente se pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [(E_1 + E_2) \setminus L](\varphi \vee \psi)$.

se e somente se $\forall v,\ wR^c_{(E_1+E_2)\setminus L}v \Rightarrow (\mathcal{M}^c, v) \models \varphi \vee \psi$.

Como $wR^c_{(E_1+E_2)\setminus L}w'$ então $(\mathcal{M}^c, w') \models \varphi \vee \psi$.

Se e somente se $\varphi \vee \psi \in w'$. O que contradiz (*). □

Lema 3.6.8 : *Para* $wR^c_{(E_1|E_2)\setminus L}w' \Leftrightarrow wR^c_{(E_2|E_1)\setminus L}w'$.

Prova.

$(\Leftarrow)$ Suponha $wR^c_{(E_2|E_1)\setminus L}w'$ e NÃO $wR^c_{(E_1|E_2)\setminus L}w'$.

Se e somente se NÃO $([(E_1 \mid E_2) \setminus L]\varphi \in w \Rightarrow \varphi \in w')$.

Se e somente se $[(E_1 \mid E_2) \setminus L]\varphi \in w$ e $\neg\varphi \in w'$. (*)

Pelo axioma 11, $[(E_2 \mid E_1) \setminus L]\varphi \in w$.

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [(E_2 \mid E_1) \setminus L]\varphi$

Se e somente se $\forall v \in W^c$, $wR^c_{(E_2|E_1)\setminus L}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$

Como $wR_{(E_2|E_1)\setminus L}w'$ então $(\mathcal{M}^c, w') \models \varphi$. O que contradiz (*).

($\Rightarrow$) Suponha $wR^c_{(E_1|E_2)\setminus L}w'$ e NÃO $wR^c_{(E_2|E_1)\setminus L}w'$.

Se e somente se $\exists\varphi$ tal que $[(E_2 \mid E_1) \setminus L]\varphi \in w$ e $\varphi \notin w'$.

Se e somente se $[(E_1 \mid E_2) \setminus L]\varphi \in w$ e $\neg\varphi \notin w'$.(*)

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [(E_2 \mid E_1) \setminus L]\varphi$

Se e somente se $\forall v$, $wR^c_{E_1|E_2}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$.

Como $wR^c_{(E_1|E_2)\setminus L}w'$ então $(\mathcal{M}^c, w') \models \varphi$.

Se e somente se $\varphi \in w'$. O que contradiz (*). □

Lema 3.6.9 : *Para* $wR^c_{((E_1|E_2)|E_3)\setminus L}w' \Leftrightarrow wR^c_{(E_1|(E_2|E_3))\setminus L}w'$.

Prova.

($\Leftarrow$) Suponha $wR^c_{((E_1|E_2)|E_3)\setminus L}w'$ e NÃO $wR^c_{(E_1|(E_2|E_3)\setminus L}w'$.

Se e somente se NÃO $([(E_1 \mid (E_2 \mid E_3)) \setminus L]\varphi \in w \Rightarrow \varphi \in w')$.

Se e somente se $[(E_1 \mid (E_2 \mid E_3)) \setminus L]\varphi \in w$ e $\neg\varphi \in w'$. (*)

Pelo axioma 12, $[(E_1 \mid (E_2 \mid E_3)) \setminus L]\varphi \in w$.

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [(E_1 \mid (E_2 \mid E_3)) \setminus L]\varphi$

Se e somente se $\forall v \in W^c$, $wR^c_{(E_1|(E_2|E_3))\setminus L}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$

Como $wR_{(E_1|(E_2|E_3)\setminus L}w'$ então $(\mathcal{M}^c, w') \models \varphi$. O que contradiz (*).

($\Rightarrow$) Suponha $wR^c_{(E_1|(E_2|E_3))\setminus L}w'$ e NÃO $wR^c_{((E_1|E_2)|E_3)\setminus L}w'$.

Se e somente se $\exists\varphi$ tal que $[((E_1 \mid E_2) \mid E_3) \setminus L]\varphi \in w$ e $\varphi \notin w'$.

Se e somente se $[((E_1 \mid E_2) \mid E_3) \setminus L]\varphi \in w$ e $\neg\varphi \notin w'$.(*)

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [((E_1 \mid E_2) \mid E_3) \setminus L]\varphi$

Se e somente se $\forall v$, $wR^c_{((E_1|E_2)|E_3)\setminus L}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$.

Como $wR^c_{(E_1|(E_2|E_3))\setminus L}w'$ então $(\mathcal{M}^c, w') \models \varphi$.

Se e somente se $\varphi \in w'$. O que contradiz (*). □

Lema 3.6.10 *: Para* $wR^c_{(E|0)\setminus L}w' \Leftrightarrow wR^c_{E\setminus L}w'$.

Prova.

($\Leftarrow$) Suponha $wR^c_{E\setminus L}w'$ e NÃO $wR^c_{(E|0)\setminus L}w'$.

Se e somente se NÃO $([(E \mid 0) \setminus L]\varphi \in w \Rightarrow \varphi \in w')$.

Se e somente se $[(E \mid 0) \setminus L]\varphi \in w$ e $\neg\varphi \in w'$. (*)

Pelo axioma 13, $[E \setminus L]\varphi \in w$.

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [E \setminus L]\varphi$.

Se e somente se $\forall v \in W^c$, $wR^c_{E\setminus L}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$

Como $wR_{E\setminus L}w'$ então $(\mathcal{M}^c, w') \models \varphi$. O que contradiz (*).

($\Rightarrow$) Suponha $wR^c_{(E|0)\setminus L}w'$ e NÃO $wR^c_{E\setminus L}w'$.

Se e somente se $\exists\varphi$ tal que $[E \setminus L]\varphi \in w$ e $\varphi \notin w'$.

Se e somente se $[E \setminus L]\varphi \in w$ e $\neg\varphi \notin w'$.(*)

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [E \setminus L]\varphi$

Se e somente se $\forall v$, $wR^c_E v \Rightarrow (\mathcal{M}^c, v) \models \varphi$.

Como $wR^c_{(E|0)\setminus L}w'$ então $(\mathcal{M}^c, w') \models \varphi$.

Se e somente se $\varphi \in w'$. O que contradiz (*). □

Lema 3.6.11 : *Para* $wR^c_{((E_1+E_2)|E_3)\backslash L}w' \Leftrightarrow wR^c_{(((E_1|E_2)+(E_2+E_3))\backslash L}w'$.

Prova.

($\Leftarrow$) Suponha $wR^c_{(((E_1|E_2)|(E_2|E_3))\backslash L}w'$ e NÃO $wR^c_{((E_1+(E_2)|E_3)\backslash L}w'$.

Se e somente se NÃO $([((E_1 + E_2) \mid E_3) \setminus L]\varphi \in w \Rightarrow \varphi \in w')$.

Se e somente se $[((E_1 + E_2) \mid E_3) \setminus L]\varphi \in w$ e $\neg\varphi \in w'$. (*)

Pelo axioma 14, $[((E_1 \mid E_2) + (E_2 \mid E_3)) \setminus L]\varphi \in w$.

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [((E_1 \mid E_2) + (E_2 \mid E_3)) \setminus L]\varphi$

Se e somente se $\forall v \in W^c$, $wR^c_{(((E_1|(E_2)+(E_2|E_3)))\backslash L}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$

Como $wR_{((E_1|(E_2)+(E_2|E_3))\backslash L}w'$ então $(\mathcal{M}^c, w') \models \varphi$. O que contradiz (*).

($\Rightarrow$) Suponha $wR^c_{((E_1+(E_2)|E_3)\backslash L}w'$ e NÃO $wR^c_{((E_1|E_2)+(E_2|E_3))\backslash L}w'$.

Se e somente se $\exists\varphi$ tal que $[((E_1 + E_2) \mid E_3) \setminus L]\varphi \in w$ e $\varphi \notin w'$.

Se e somente se $[((E_1 + E_2) \mid E_3) \setminus L]\varphi \in w$ e $\neg\varphi \notin w'$.(*)

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [((E_1 + E_2) \mid E_3) \setminus L]\varphi$

Se e somente se $\forall v \in W^c$, $wR^c_{((E_1+E_2)|E_3)\backslash L}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$.

Como $wR^c_{((E_1|(E_2)|E_3)\backslash L}w'$ então $(\mathcal{M}^c, w') \models \varphi$.

Se e somente se $\varphi \in w'$. O que contradiz (*). □

Lema 3.6.12 : *Para* $wR_{((\alpha.E_1)|E_2)\backslash L}w' \Rightarrow wR_{(\alpha;(E_1|E_2))\backslash L}w'$, *se* $\alpha \notin L$.

Prova.

Suponha $wR_{((\alpha.E_1)|E_2)\backslash L}w'$ e NÃO $wR_{(\alpha.(E_1|E_2))\backslash L}w'$.

Se e somente se $\exists\varphi$ tal que $[(\alpha.E_1 \mid E_2) \setminus L]\varphi \in w$ e $\varphi \notin w'$.

Se e somente se $[(\alpha.E_1 \mid E_2) \setminus L]\varphi \in w$ e $\neg\varphi \in w'$. (*)

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [(\alpha.(E_1 \mid E_2) \setminus L]\varphi$.

Se e somente se $\forall v \in W^c$, $wR_{((\alpha.E_1)|E_2)\setminus L}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$

Como $wR_{((\alpha.E_1)|E_2)\setminus L}w'$ então $(\mathcal{M}^c, w') \models \varphi$.

Se e somente se $\varphi \in w'$. O que contradiz (*). □

Lema 3.6.13 : *Para* $wR_{((\alpha.E_1)|E_2)\setminus L}w' \Rightarrow wR_{(0|E_2)\setminus L}w'$, *se* $\alpha \in L$.

Prova.

Suponha $wR_{((\alpha.E_1)|E_2)\setminus L}w'$ e NÃO $wR_{(0|E_2)\setminus L}w'$.

Se e somente se $\exists\varphi$ tal que $[(0 \mid E_2) \setminus L]\varphi \in w$ e $\varphi \notin w'$.

Se e somente se $[(\alpha.E_1 \mid E_2) \setminus L]\varphi \in w$ e $\neg\varphi \in w'$. (*)

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [(\alpha.(E_1 \mid E_2) \setminus L]\varphi$.

Se e somente se $\forall v \in W^c$, $wR_{((\alpha.E_1)|E_2)\setminus L}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$

Como $wR_{((\alpha.E_1)|E_2)\setminus L}w'$ então $(\mathcal{M}^c, w') \models \varphi$.

Se e somente se $\varphi \in w'$. O que contradiz (*). □

Lema 3.6.14 : *Para* $wR_{((\alpha_1.E_1)|(\alpha_2.E_2))\setminus L}w' \Leftrightarrow wR_{(\alpha_1.(E_1|\alpha_2.E_2)+\alpha_2.(\alpha_1.E_1|E_2))\setminus L}w'$, *se* $\alpha_1, \alpha_2 \notin L$.

Prova.

($\Leftarrow$) Suponha $wR_{(\alpha_1.(E_1|\alpha_2.E_2)+\alpha_2.(\alpha_1.E_1|E_2))\setminus L}w'$ e NÃO $wR_{((\alpha_1.E_1)|(\alpha_2.E_2))\setminus L}w'$

Se e somente se NÃO $([((\alpha_1.(E_1) \mid (\alpha_2.E_2)) \setminus L]\varphi \in w \Rightarrow \varphi \in w')$.

Se e somente se $[((\alpha_1.(E_1) \mid (\alpha_2.E_2)) \setminus L]\varphi \in w$ e $\neg\varphi \in w'$. (*)

Pelo axioma 17, $[(\alpha_1.(E_1 \mid \alpha_2.E_2)) \setminus L]\varphi \wedge [(\alpha_2.(\alpha_1.E_1 \mid E_2)) \setminus L]\varphi$.

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [(\alpha_1.(E_1 \mid \alpha_2.E_2)) \setminus L]\varphi \wedge [(\alpha_2.(\alpha_1.E_1 \mid E_2)) \setminus L]\varphi$.

Se e somente se $\forall v \in W^c$, $wR_{(\alpha_1.(E_1|\alpha_2.E_2)+\alpha_2.(\alpha_1.E_1|E_2))\setminus L}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$.

Como $wR_{(\alpha_1.(E_1|\alpha_2.E_2)+\alpha_2.(\alpha_1.E_1|E_2))\setminus L}w'$ então $(\mathcal{M}^c, w') \models \varphi$. O que contradiz (*).

($\Rightarrow$) Suponha $wR_{((\alpha_1.E_1)|(\alpha_2.E_2))\setminus L}w'$ e NÃO $wR_{(\alpha_1.(E_1|\alpha_2.E_2)+\alpha_2.(\alpha_1.E_1|E_2))\setminus L}w'$

Se e somente se $\exists\varphi$ tal que $[(\alpha_1.(E_1 \mid \alpha_2.E_2)) \setminus L]\varphi \wedge [(\alpha_2.(\alpha_1.E_1 \mid E_2)) \setminus L]\varphi \in w$ e $\varphi \notin w'$

Se e somente se $[(\alpha_1.(E_1 \mid \alpha_2.E_2)) \setminus L]\varphi \wedge [(\alpha_2.(\alpha_1.E_1 \mid E_2)) \setminus L]\varphi \in w$ e $\neg\varphi \in w'$. (*)

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [(\alpha_1.(E_1 \mid \alpha_2.E_2)) \setminus L]\varphi \wedge [(\alpha_2.(\alpha_1.E_1 \mid E_2)) \setminus L]\varphi$

Se e somente se $\forall v \in W^c$, $wR_{((\alpha_1.E_1)|(\alpha_2.E_2))\setminus L}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$.

Como $wR_{((\alpha_1.E_1)|(\alpha_2.E_2))\setminus L}w'$ então $(\mathcal{M}^c, w') \models \varphi$.

Se e somente se $\varphi \in w'$. O que contradiz (*). □

Lema 3.6.15 : *Para* $wR_{((\alpha.E_1)|(\overline{\alpha}.E_2))\setminus L}w' \Leftrightarrow wR_{(\alpha.(E_1|\overline{\alpha}.E_2)+\overline{\alpha}.(\alpha;E_1|E_2)+\tau.(E_1|E_2))\setminus L}w'$, *se* $\alpha, \overline{\alpha} \notin L$.

Prova.

($\Leftarrow$) Suponha $wR_{(\alpha.(E_1|\overline{\alpha}.E_2)+\overline{\alpha}.(\alpha;E_1|E_2)+\tau.(E_1|E_2))\setminus L}w'$ e NÃO $wR_{((\alpha.E_1)|(\overline{\alpha}.E_2))\setminus L}w'$.

Se e somente se NÃO $([((\alpha.E_1) \mid (\overline{\alpha}.E_2)) \setminus L]\varphi \in w \Rightarrow \varphi \in w')$

Se e somente se $[((\alpha.E_1) \mid (\overline{\alpha}.E_2)) \setminus L]\varphi \in w$ e $\neg\varphi \in w'$. (*)

Pelo axioma 18, $[(\alpha.(E_1 \mid \overline{\alpha}.E_2)) \setminus L]\varphi \wedge [(\overline{\alpha}.(\alpha.E_1 \mid E_2)) \setminus L]\varphi \wedge [(\tau.(E_1 \mid E_2)) \setminus L]\varphi$

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [(\alpha.(E_1 \mid \overline{\alpha}.E_2)) \setminus L]\varphi \wedge [(\overline{\alpha}.(\alpha.E_1 \mid E_2)) \setminus L]\varphi \wedge [(\tau.(E_1 \mid E_2)) \setminus L]\varphi$

Se e somente se $\forall v \in W^c$, $wR_{(\alpha.(E_1|\overline{\alpha}.E_2)+\overline{\alpha}.(\alpha;E_1|E_2)+\tau.(E_1|E_2))\setminus L}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$

Como $wR_{(\alpha.(E_1|\overline{\alpha}.E_2)+\overline{\alpha}.(\alpha.E_1|E_2)+\tau.(E_1|E_2))\setminus L}w'$, então $(\mathcal{M}^c, w') \models \varphi$. O que contradiz (*).

($\Rightarrow$) Suponha $wR_{((\alpha.E_1)|(\overline{\alpha}.E_2))\setminus L}w'$ e NÃO $wR_{(\alpha.(E_1|\overline{\alpha}.E_2)+\overline{\alpha}.(\alpha.E_1|E_2)+\tau.(E_1|E_2))\setminus L}w'$

Se e somente se $\exists\varphi$ tal que $[(\alpha.(E_1 \mid \overline{\alpha}.E_2)) \setminus L]\varphi \wedge [(\overline{\alpha}.(\alpha.E_1 \mid E_2)) \setminus L]\varphi \wedge [(\tau.(E_1 \mid E_2)) \setminus L]\varphi$ e $\varphi \notin w'$

Se e somente se $[(\alpha.(E_1 \mid \overline{\alpha}.E_2))\backslash L]\varphi \wedge [(\overline{\alpha}.(\alpha.E_1 \mid E_2))\backslash L]\varphi \wedge [(\tau.(E_1 \mid E_2))\backslash L]\varphi \in w$ e $\neg\varphi \in w'$. (*)

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [(\alpha.(E_1 \mid \overline{\alpha}.E_2)) \setminus L]\varphi \wedge [(\overline{\alpha}.(\alpha.E_1 \mid E_2)) \setminus L]\varphi \wedge [(\tau.(E_1 \mid E_2)) \setminus L]\varphi$

Se e somente se $\forall v \in W^c$, $wR_{((\alpha.E_1)|(\overline{\alpha}.E_2))\backslash L}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$.

Como $wR_{((\alpha.E_1)|(\overline{\alpha}.E_2))\backslash L}w'$ então $(\mathcal{M}^c, w') \models \varphi$.

Se e somente se $\varphi \in w'$. O que contradiz (*). □

Lema 3.6.16 *: Para $wR_{(\alpha.E)\backslash L}w \Leftrightarrow wR_0w$, se $\alpha \in L$.*

Prova.

($\Leftarrow$) Suponha $wR_{(\alpha.E)\backslash L}w$ e NÃO wR_0w, se $\alpha \in L$

Se e somente se $[(\alpha.E) \setminus L]\varphi \in w$ se $\alpha \in L$, então $\varphi \notin w'$.

Pelo axioma 19, $[0]\varphi$

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [0]\varphi$.

Por definição, $S \subseteq W$ e $w \in S$, como R_0 é reflexiva e funcional então wR_0w e não é o caso de wR_0w' para algum w'

Logo, $\nexists w' \in W^c$ tal que wR_0w' e $\varphi \notin w'$.

($\Rightarrow$) Suponha wR_0w e NÃO $wR_{(\alpha.E)\backslash L}w$

Se e somente se $\exists\varphi$ tal que $[(\alpha.E) \setminus L]\varphi$ se $\alpha \in L$, então $\varphi \notin w$.

Se e somente se $[(\alpha.E) \setminus L]\varphi \in w$ se $\alpha \in L$ e $\neg\varphi \in w$. (*)

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [(\alpha.E) \setminus L]\varphi$

Se e somente se $\forall w \in W^c$, wR_0w, pela reflexividade de R_0, $\Rightarrow (\mathcal{M}^c, w) \models \varphi$.

Se e somente se $\varphi \in w$. O que contradiz (*). □

Lema 3.6.17 : *Para* $wR_{((\alpha.E_1)|(\overline{\alpha}.E_2))\setminus L}w' \Leftrightarrow wR_{\tau.(E_1|E_2)}w'$, *se* $\alpha \in L$.

Prova.

($\Leftarrow$) Suponha $wR_{((\alpha.E_1)|(\overline{\alpha}.E_2))\setminus L}w'$ e NÃO $wR_{\tau.(E_1|E_2)}w'$

Se e somente se NÃO $([((\alpha.E_1) \mid (\overline{\alpha}.E_2)) \setminus L]\varphi \in w \Rightarrow \varphi \in w')$

Se e somente se $[((\alpha.E_1) \mid (\overline{\alpha}.E_2)) \setminus L]\varphi \in w$ e $\neg\varphi \in w'$. (*)

Pelo axioma 20, $[\tau.(E_1 \mid E_2)]\varphi$, se $\alpha \in L$

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [\tau.(E_1 \mid E_2)]\varphi$, se $\alpha \in L$

Se e somente se $\forall v \in W^c$, $wR_{\tau.(E_1|E_2)}v$, se $\alpha \in L \Rightarrow (\mathcal{M}^c, v) \models \varphi$

Como $wR_{\tau.(E_1|E_2)}w'$, se $\alpha \in L$, então $(\mathcal{M}^c, w') \models \varphi$. O que contradiz (*).

($\Rightarrow$) Suponha $wR_{\tau.(E_1|E_2)}w'$ e NÃO $wR_{((\alpha;E_1)|(\overline{\alpha}.E_2))\setminus L}w'$

Se e somente se $\exists\varphi$ tal que $[((\alpha.E_1) \mid (\overline{\alpha}.E_2)) \setminus L]\varphi \in w$ e $\varphi \notin w'$

Se e somente se $[((\alpha.E_1) \mid (\overline{\alpha}.E_2)) \setminus L]\varphi \in w$ e $\neg\varphi \in w'$. (*)

Pelo Lema da Verdade, $(\mathcal{M}^c, w) \models [((\alpha.E_1) \mid (\overline{\alpha}.E_2)) \setminus L]\varphi$

Se e somente se $\forall v \in W^c$, $wR_{((\alpha.E_1)|(\overline{\alpha}.E_2))\setminus L}v \Rightarrow (\mathcal{M}^c, v) \models \varphi$

Como $wR_{((\alpha.E_1)|(\overline{\alpha}.E_2))\setminus L}w'$ então $(\mathcal{M}^c, w') \models \varphi$.

Se e somente se $\varphi \in w'$. O que contradiz (*). □

Definição 3.6.7 : *Seja* E *um programa. O conjunto das transições de* E, $T(E)$ *é definido como segue:*

i.

$$E = (\alpha \cdot E) \setminus L \Rightarrow \begin{cases} T(E) = 0, & \text{se } \alpha \in L \\ T(E) = \{\langle \alpha, E_1 \rangle\}, & \text{se } \alpha \notin L \end{cases}$$

ii. $E = (E_1 + E_2) \setminus L \Rightarrow T(E) = T(E_1 \setminus L) \cup T(E_2 \setminus L)$

iii. $E = (E_1 \mid E_2) \setminus L \Rightarrow \forall \langle \alpha_1, E_1' \rangle \in T(E_1)$ *e* $\langle \alpha_2, E_2' \rangle \in T(E_2)$

iv. $T(E) := 0$,

$$\textit{Se } \alpha_1 \notin L \textit{ então } T(E) := T(E) \cup \{\langle \alpha_1, E_1' \rangle\}$$

$$\textit{Se } \alpha_2 \notin L \textit{ então } T(E) := T(E) \cup \{\langle \alpha_2, E_2' \rangle\}$$

$$\textit{Se } \alpha_1 = \alpha \textit{ e } \alpha_2 = \overline{\alpha} \textit{ então } T(E) := T(E) \cup \{\langle \tau, (E_1' \mid E_2') \rangle\}$$

Lema 3.6.18 $\vdash \langle E \rangle \varphi \leftrightarrow \langle \alpha_1, E_1 \rangle \varphi \vee \cdots \vee \langle \alpha_n, E_n \rangle \varphi$, $R_E = R_{\alpha_1.E_1 + \cdots + \alpha_n.E_n}$, *onde* $\langle \alpha_i, E_i \rangle \in T(E)$.

Prova. Usando o axioma 14, podemos ter várias vezes o seguinte:

$$\langle E \rangle \varphi \leftrightarrow \langle F_1^1 \mid \cdots \mid F_{n_1}^1 + F_1^2 \mid \cdots \mid F_{n_2}^2 + \cdots + F_1^k \mid \cdots \mid F_{n_k}^k \rangle \varphi$$

onde cada F_i^j ou é 0 ou é um processo $\alpha_i^j \cdot G_i^j$.

Usando o axioma 13, podemos eliminar os 0's e aplicando o axioma 5 obtemos:

$$\langle E \rangle \varphi \leftrightarrow \langle \alpha_1^1 \cdot G_1^1 \mid \cdots \mid \alpha_{m_1}^1 \cdot G_{m_1}^1 \rangle \varphi \vee \cdots \vee \langle \alpha_1^k \cdot G_1^k \mid \cdots \mid \alpha_{m_k}^k \cdot G_{m_k}^k \rangle \varphi$$

Para cada termo da definição podemos fazer o seguinte:

$$\langle \alpha_1^j \cdot G_1^j \mid \cdots \mid \alpha_{m_j}^j \cdot G_{m_j}^j \rangle \varphi$$

Para cada α_i^j se ele pertence a L e se algum outro α_l^j é seu complemento, geramos a seguinte fórmula, usando o axioma 20:

$$\langle \tau \cdot (\alpha_1^j \cdot G_1^j \mid \cdots \mid G_i^j \mid \cdots \mid G_l^j \mid \cdots \mid \alpha_{m_j}^j \cdot G_{m_j}^j) \rangle \varphi$$

Se $\alpha_i^j \in L$, mas seu complemento não ocorre no termo então eliminamos $\alpha_i^j \cdot G_i^j$ da composição.

Se $\alpha_l^j \notin L$ então aplicamos o axioma 17 e obtemos:

$$\langle E \rangle \varphi \leftrightarrow \langle \alpha_1 \cdot E_1 \rangle \varphi \vee \cdots \vee \langle \alpha_n \cdot E_n \rangle \varphi$$

A prova do item (ii) análoga ao (i), só que usando a regra correspondente. □

3.7 Adicionando Iteração

Estendemos a linguagem da LDP-CCS com Composição Paralela e Iteração com Sincronização com o operador CCS de Iteração: $*$. A LDP-CCS com Composição Paralela e Iteração com Sincronização é definida como segue:

3.7.1 Linguagem, Frames e Modelos

Definição 3.7.1 *: A* **LDP-CCS com Composição Paralela e Iteração com Sincronização** *é definida usando os mesmos símbolos da definição 3.6.1:*

$$\varphi ::= p \mid \top \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \rightarrow \varphi_2 \mid \neg\varphi \mid [K]\varphi \mid [E]\varphi$$

$$\alpha ::= a \mid \overline{a} \mid \tau$$

$$E ::= 0 \mid i \mid \alpha \cdot E \mid E \cdot 0 \mid E_1 + E_2 \mid (E_1|E_2) \mid E^*$$

onde, $K \subseteq Act$, $\mathcal{L} \subseteq \mathring{A} \cup \overline{\mathring{A}}$ *e* $L \subseteq \mathcal{L}$.

Definição 3.7.2 *: Um* **frame** *para LDP-CCS com Composição Paralela e Iteração com Sincronização é* $\mathcal{F} = (W, Z, R_\alpha, R_E)$

onde:

W *é um conjunto de estados finitos;*

Z *é um conjunto de estados finais,* $Z \subseteq W$, *onde*

$$\forall \alpha \in Act \text{ e } \forall w (w \in Z \Leftrightarrow \neg\exists w', w R_\alpha w')$$

R_α *é uma relação binária para cada programa básico* α;

R_E *é uma relação binária para cada programa composto* E, *onde:*

$$R_{\alpha \cdot E} = R_\alpha ; R_E$$

$$R_{E \cdot 0} = R_E ; R_0$$

$R_{E_1+E_2} = R_{E_1} \cup R_{E_2}$

$R_0 = \{(x,x) \mid x \in Z\}$

$R_i = \{(x,x) \mid x \in W\}$

$R_{(E_1|E_2)\setminus L}$ *satisfaz as seguintes condições:*

i. $R_{E_1|E_2} = R_{E_2|E_1}$ *(comutativa)*

ii. $R_{(E_1|E_2)|E_3} = R_{E_1|(E_2|E_3)}$ *(associativa)*

iii. $R_{E|0} = R_E$

iv. $R_{(E_1+E_2)|E_3} = R_{(E_1|E_3)+(E_2|E_3)}$

v. $R_{\alpha_1 \cdot E_1|\alpha_2 \cdot E_2|\cdots|\alpha_n \cdot E_n} =$

$R_{\sum_{i=1}^{n} \alpha_i(\alpha_1 \cdot E_1|\cdots|E_i|\cdots|\alpha_n \cdot E_n)+\tau(\alpha_1 \cdot E_1|\cdots|E_i|\cdots|E_j|\cdots|\alpha_n \cdot E_n)}$, *para todo* $\alpha_i = \overline{\alpha_j}$

vi. $R_{(E_1|E_2^*)} = R_{(E_1 \cdot 0|E_2)^*}$ *e* $R_{E_2 \cdot E_2^* \cdot E_1} = \emptyset$

Definição 3.7.3 : *Um* **modelo** *para a LDP-CCS com composição paralela e iteração com sincronização é* $\mathcal{M} = (W, Z, R_\alpha, R_E, V)$, *onde* V *é uma função valoração mapeando símbolos proposicionais em subconjuntos de* V. E, *para todo estado* $w, w' \in W$ *e todo programa* α *e* E, $wR_\alpha w'$ *e* $wR_E w'$.

Definição 3.7.4 : *Seja* $\mathcal{M} = (W, Z, R_\alpha, R_E, V)$ *um modelo e* $w \in W$. *Definimos a noção de* **satisfação** *de uma fórmula* φ *num modelo* $\mathcal{M}$ *em um estado* w, $(\mathcal{M},w) \models \varphi$, *como segue:*

1. $(\mathcal{M},w) \models p$ *se e somente se* $p \in V(p)$.

2. $(\mathcal{M},w) \models \bot$ *se e somente se* $w \in W$.

3. $(\mathcal{M},w) \models \neg\varphi$ *se e somente se* $\mathcal{M},w \not\models \varphi$.

4. $(\mathcal{M},w) \models \varphi_1 \wedge \varphi_2$ *se e somente se* $(\mathcal{M},w) \models \varphi_1$ *e* $(\mathcal{M},w) \models \varphi_2$.

5. $(\mathcal{M},w) \models [K]\varphi$ *se e somente se* $\forall w' \in W$ *e* $\forall \alpha \in K$, $wR_\alpha w'$ *e* $(\mathcal{M},w') \models \varphi$.

6. $(\mathcal{M},w) \models [E]\varphi$ *se e somente se* $\forall w' \in W$, $wR_E w'$ *e* $(\mathcal{M},w') \models \varphi$.

Se $\mathcal{M},w \models \varphi$ para todo estado w, dizemos que φ é válida no modelo $\mathcal{M}$, $\mathcal{M} \models \varphi$. E se φ é válida em todos os modelos $\mathcal{M}$, dizemos que φ é válida, $\models \varphi$.

3.7.2 Axiomatização

Axiomas

1. todas as tautologias
2. $[K](\varphi \to \psi) \to [K]\varphi \to [K]\psi$
3. $[E](\varphi \to \psi) \to [E]\varphi \to [E]\psi$
4. $[\alpha \cdot E]\varphi \leftrightarrow [\alpha][E]\varphi$
5. $[E_1 + E_2]\varphi \leftrightarrow [E_1]\varphi \wedge [E_2]\varphi$
6. $[0 + E_1]\varphi \to [E_1]\varphi$
7. $\varphi \wedge [\mathring{A}]\bot \to \langle 0\rangle\varphi$ (reflexividade de R_0)
8. $[\mathring{A}]\bot \wedge \langle 0\rangle\varphi \to [0]\varphi$ (R_0 é funcional)
9. $[\alpha](\varphi \wedge [\mathring{A}]\bot) \to [\alpha \cdot 0]\varphi$
10. $[\mathring{A}]\bot \leftrightarrow \langle 0\rangle\top$

11. $[i]\varphi \rightarrow \varphi$

12. $[E_1 \mid E_2]\varphi \leftrightarrow [E_2 \mid E_1]\varphi$

13. $[(E_1 \mid E_2) \mid E_3]\varphi \leftrightarrow [E_1 \mid (E_2 \mid E_3)]\varphi$

14. $[E \mid 0]\varphi \leftrightarrow [E]\varphi$

15. $[(E_1 + E_2) \mid E_3]\varphi \leftrightarrow [((E_1 \mid E_3) + (E_2 \mid E_3)]\varphi$

16. $\langle \alpha_1 \cdot E_1 \mid \alpha_2 \cdot E_2 \mid \cdots \mid \alpha_n \cdot E_n \rangle \varphi \leftrightarrow \langle \sum_{i=1}^{n} \alpha_i (\alpha_1 \cdot E_1 \mid \cdots \mid E_i \mid \cdots \mid \alpha_n \cdot E_n) + \tau(\alpha_1 \cdot E_1 \mid \cdots \mid E_i \mid \cdots \mid E_j \mid \cdots \mid \alpha_n \cdot E_n \rangle \varphi$, para todo $\alpha_i = \overline{\alpha_j}$

17. $\langle E_1 \mid E_2^* \rangle \varphi \leftrightarrow \langle (E_1 \cdot 0 \mid E_2)^* \rangle \varphi \wedge [E_2][E_2^*][E_1]\bot$

Regras de Inferência:

Substituição Uniforme:

$$\frac{\vdash \varphi}{\vdash \varphi(\beta_1/p_1, \cdots, \beta_n/p_n)}$$

Modus Ponens:

$$\frac{\varphi, \varphi \rightarrow \psi}{\psi}$$

Generalização:

$$\frac{\vdash \varphi}{\vdash [K]\varphi}, \quad \frac{\vdash \varphi}{\vdash [E]\varphi}$$

3.7.3 Corretude

Considere um frame $\mathcal{F} = (W, Z, R_\alpha, R_E)$, onde as relações R_α e R_E, são descritas na definição 3.7.2. Seja $\mathcal{M}$ modelo sobre $\mathcal{F}$.

Teorema 3.7.1 *: Todo teorema do sistema axiomático é válido na classe de frames F.*

Prova. Temos que provar que:

- Todo axioma do Esquema de Axiomas é válido na classe de frames F.
- As regras de inferência preservam validade na classe de frames F.

Lema 3.7.1 *: Para todas as fórmulas e todos os programas:*

1. $F \models [K](\varphi \to \psi) \to [K]\varphi \to [K]\psi$
2. $F \models [E](\varphi \to \psi) \to [E]\varphi \to [E]\psi$
3. $F \models [\alpha \cdot E]\varphi \leftrightarrow [\alpha][E]\varphi$, *se* $\alpha \notin L$
4. $F \models [E_1 + E_2]\varphi \leftrightarrow [E_1]\varphi \wedge [E_2]\varphi$
5. $F \models [0 + E_1]\varphi \to [E_1]\varphi$
6. $F \models \varphi \wedge [\mathring{A}]\bot \to \langle 0\rangle\varphi$ *(reflexividade de* R_0*)*
7. $F \models [\mathring{A}]\bot \wedge \langle 0\rangle\varphi \to [0]\varphi$ *(*R_0 *é funcional)*
8. $F \models [\alpha](\varphi \wedge [\mathring{A}]\bot) \to [\alpha \cdot 0]\varphi$
9. $F \models [\mathring{A}]\bot \leftrightarrow \langle 0\rangle\top$
10. $F \models [i]\varphi \to \varphi$
11. $F \models [E_1 \mid E_2]\varphi \leftrightarrow [E_2 \mid E_1]\varphi$
12. $F \models [(E_1 \mid E_2) \mid E_3]\varphi \leftrightarrow [E_1 \mid (E_2 \mid E_3)]\varphi$
13. $F \models [E \mid 0]\varphi \leftrightarrow [E]\varphi$
14. $F \models [(E_1 + E_2) \mid E_3]\varphi \leftrightarrow [(E_1 \mid E_3) + (E_2 \mid E_3)]\varphi$

15. $F \models \langle \alpha_1 \cdot E_1 \mid \alpha_2 \cdot E_2 \mid \cdots \mid \alpha_n \cdot E_n \rangle \varphi \leftrightarrow \langle \sum_{i=1}^{n} \alpha_i (\alpha_1 \cdot E_1 \mid \cdots \mid E_i \mid \cdots \mid \alpha_n \cdot E_n) + \tau(\alpha_1 \cdot E_1 \mid \cdots \mid E_i \mid \cdots \mid E_j \mid \cdots \mid \alpha_n \cdot E_n) \rangle \varphi$, *para todo* $\alpha_i = \overline{\alpha_j}$

16. $F \models \langle E_1 \mid E_2^* \rangle \varphi \leftrightarrow \langle (E_1 \cdot 0 \mid E_2)^* \rangle \varphi \wedge [E_2][E_2^*][E_1]\bot$

Prova.

1. Idem prova 1. do lema 3.4.1.

2. Idem prova 2. do lema 3.4.1.

3. Idem prova 3. do lema 3.4.1.

4. Idem prova 4. do lema 3.4.1.

5. Idem prova 5. do lema 3.4.1.

6. Idem prova 6. do lema 3.4.1.

7. Idem prova 7. do lema 3.4.1.

8. Idem prova 8. do lema 3.4.1.

9. Idem prova 9. do lema 3.4.1.

10. Idem prova 10. do lema 3.4.1.

11. Suponha, por contradição, que existe um modelo $\mathcal{M} = (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$$\mathcal{M}, w \not\models [i]\varphi \rightarrow \varphi$$

Então,

(1) $\mathcal{M}, w \models [i]\varphi$ e

(2) $\mathcal{M}, w \not\models \varphi$

(1) se e somente se $\forall w \in W$ e wR_iw e $\mathcal{M}, w \models \varphi$.

(2) se e somente se $\mathcal{M}, w \models \neg\varphi$. O que contradiz (1).

12. Idem prova 12. do lema 3.4.1.

13. Idem prova 13. do lema 3.4.1.

14. Idem prova 14. do lema 3.4.1.

15. Idem prova 14. do lema 3.4.1.

16. Suponha, por contradição, que existe um modelo $\mathcal{M}= (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$\mathcal{M}, w \not\models \langle \alpha_1 \cdot E_1 \mid \alpha_2 \cdot E_2 \mid \cdots \mid \alpha_n \cdot E_n \rangle \varphi \leftrightarrow \langle \sum_{i=1}^{n} \alpha_i (\alpha_1 \cdot E_1 \mid \cdots \mid E_i \mid \cdots \mid \alpha_n \cdot E_n) + \tau(\alpha_1 \cdot E_1 \mid \cdots \mid E_i \mid \cdots \mid E_j \mid \cdots \mid \alpha_n \cdot E_n \rangle \varphi$, para todo $\alpha_i = \overline{\alpha_j}$

Então,

(1) $\mathcal{M}, w \not\models \langle \alpha_1 \cdot E_1 \mid \alpha_2 \cdot E_2 \mid \cdots \mid \alpha_n \cdot E_n \rangle \varphi \rightarrow \langle \sum_{i=1}^{n} \alpha_i (\alpha_1 \cdot E_1 \mid \cdots \mid E_i \mid \cdots \mid \alpha_n \cdot E_n) + \tau(\alpha_1 \cdot E_1 \mid \cdots \mid E_i \mid \cdots \mid E_j \mid \cdots \mid \alpha_n \cdot E_n \rangle \varphi$, para todo $\alpha_i = \overline{\alpha_j}$.

(2) $\mathcal{M}, w \not\models \langle \sum_{i=1}^{n} \alpha_i (\alpha_1 \cdot E_1 \mid \cdots \mid E_i \mid \cdots \mid \alpha_n \cdot E_n) + \tau(\alpha_1 \cdot E_1 \mid \cdots \mid E_i \mid \cdots \mid E_j \mid \cdots \mid \alpha_n \cdot E_n \rangle \varphi \rightarrow \langle \alpha_1 \cdot E_1 \mid \alpha_2 \cdot E_2 \mid \cdots \mid \alpha_n \cdot E_n \rangle \varphi$, para todo $\alpha_i = \overline{\alpha_j}$.

(1) se e somente se (3) $\mathcal{M}, w \models \langle \alpha_1 \cdot E_1 \mid \alpha_2 \cdot E_2 \mid \cdots \mid \alpha_n \cdot E_n \rangle \varphi$ e (4) $\mathcal{M}, w \not\models \langle \sum_{i=1}^{n} \alpha_i (\alpha_1 \cdot E_1 \mid \cdots \mid E_i \mid \cdots \mid \alpha_n \cdot E_n) + \tau(\alpha_1 \cdot E_1 \mid \cdots \mid E_i \mid \cdots \mid E_j \mid \cdots \mid \alpha_n \cdot E_n \rangle \varphi$, para todo $\alpha_i = \overline{\alpha_j}$.

(3) se e somente se $\forall w' \in W$ se $w R_{\alpha_1 \cdot E_1 \mid \alpha_2 \cdot E_2 \mid \cdots \mid \alpha_n \cdot E_n} w'$ então $\mathcal{M}, w' \models \varphi$.

(4) se e somente se (5) $\mathcal{M}, w \models [\sum_{i=1}^{n} \alpha_i (\alpha_1 \cdot E_1 \mid \cdots \mid E_i \mid \cdots \mid \alpha_n \cdot E_n) + \tau(\alpha_1 \cdot E_1 \mid \cdots \mid E_i \mid \cdots \mid E_j \mid \cdots \mid \alpha_n \cdot E_n] \neg \varphi$, para todo $\alpha_i = \overline{\alpha_j}$.

(5) se e somente se $\forall w' \in W$ se $R_{\alpha_1 \cdot E_1 \mid \alpha_2 \cdot E_2 \mid \cdots \mid \alpha_n \cdot E_n} =$

$R_{\sum_{i=1}^{n} \alpha_i(\alpha_1 \cdot E_1 | \cdots | E_i | \cdots | \alpha_n \cdot E_n) + \tau(\alpha_1 \cdot E_1 | \cdots | E_i | \cdots | E_j | \cdots | \alpha_n \cdot E_n)}$, para todo $\alpha_i = \overline{\alpha_j}$, pela definição 3.7.2, então $wR_{\sum_{i=1}^{n} \alpha_i(\alpha_1 \cdot E_1 | \cdots | E_i | \cdots | \alpha_n \cdot E_n) + \tau(\alpha_1 \cdot E_1 | \cdots | E_i | \cdots | E_j | \cdots | \alpha_n \cdot E_n)} w'$ e $\mathcal{M}, w' \models \neg\varphi$. O que contradiz (3).

(2) se e somente se (6) $\mathcal{M}, w \models \langle \sum_{i=1}^{n} \alpha_i(\alpha_1 \cdot E_1 \mid \cdots \mid E_i \mid \cdots \mid \alpha_n \cdot E_n) + \tau(\alpha_1 \cdot E_1 \mid \cdots \mid E_i \mid \cdots \mid E_j \mid \cdots \mid \alpha_n \cdot E_n \rangle \varphi$ e (7) $\mathcal{M}, w \not\models \langle \alpha_1 \cdot E_1 \mid \alpha_2 \cdot E_2 \mid \cdots \mid \alpha_n \cdot E_n \rangle \varphi$.

(6) se e somente se $\forall w' \in W$ se $wR_{\sum_{i=1}^{n} \alpha_i(\alpha_1 \cdot E_1 | \cdots | E_i | \cdots | \alpha_n \cdot E_n) + \tau(\alpha_1 \cdot E_1 | \cdots | E_i | \cdots | E_j | \cdots | \alpha_n \cdot E_n)} w'$ e $\mathcal{M}, w' \models \neg\varphi$.

(7) se e somente se (8) $\mathcal{M}, w \models [\alpha_1 \cdot E_1 \mid \alpha_2 \cdot E_2 \mid \cdots \mid \alpha_n \cdot E_n] \neg\varphi$.

(8) se e somente se $\forall w' \in W$ se $R_{\alpha_1 \cdot E_1 | \alpha_2 \cdot E_2 | \cdots | \alpha_n \cdot E_n} = R_{\sum_{i=1}^{n} \alpha_i(\alpha_1 \cdot E_1 | \cdots | E_i | \cdots | \alpha_n \cdot E_n) + \tau(\alpha_1 \cdot E_1 | \cdots | E_i | \cdots | E_j | \cdots | \alpha_n \cdot E_n)}$, para todo $\alpha_i = \overline{\alpha_j}$, pela definição 3.7.2, então $wR_{\alpha_1 \cdot E_1 | \alpha_2 \cdot E_2 | \cdots | \alpha_n \cdot E_n} w'$ e $\mathcal{M}, w' \models \neg\varphi$. O que contradiz (6).

17. Suponha, por contradição, que existe um modelo $\mathcal{M} = (\mathcal{F}, V)$ com um mundo possível $w \in W$ tal que

$$\mathcal{M}, w \not\models \langle E_1 \mid E_2^* \rangle \varphi \leftrightarrow \langle (E_1 \cdot 0 \mid E_2)^* \rangle \varphi \wedge [E_2][E_2^*][E_1] \bot$$

Então,

(1) $\mathcal{M}, w \not\models \langle E_1 \mid E_2^* \rangle \varphi \leftrightarrow \langle (E_1 \cdot 0 \mid E_2)^* \rangle \varphi \wedge [E_2][E_2^*][E_1] \bot$ e

(2) $\mathcal{M}, w \not\models \langle (E_1 \cdot 0 \mid E_2)^* \rangle \varphi \wedge [E_2][E_2^*][E_1] \bot \rightarrow \langle E_1 \mid E_2^* \rangle \varphi$

(1) se e somente se (3) $\mathcal{M}, w \models \langle E_1 \mid E_2^* \rangle \varphi \wedge [E_2][E_2^*][E_1] \bot$ e (4) $\mathcal{M}, w \not\models \langle (E_1 \cdot 0 \mid E_2)^* \rangle \varphi \wedge [E_2][E_2^*][E_1] \bot$

(3) se e somente se $\forall w' \in W$ se $wR_{(E_1 | E_2^*)} w'$ então $\mathcal{M}, w' \models \varphi$.(*)

Como $R_{(E_1 | E_2^*)} = R_{(E_1 \cdot 0 | E_2)^*}$ e $R_{E_2 \cdot E_2^* \cdot E_1} = \emptyset$, pela definição 3.7.2, então se $\forall w' \in W$,

$wR_{(E_1 \cdot 0 | E_2)^*} w'$ e $R_{E_2 \cdot E_2^* \cdot E_1} =$ então $(\mathcal{M}, w') \models \varphi$.

(4) se e somente se (5) $\mathcal{M}, w \models [(E_1 \cdot 0 \mid E_2)^*] \neg\varphi \vee \langle E_2 \rangle \langle E_2^* \rangle \langle E_1 \rangle \top$.

(5) se e somente se $\forall w' \in W$ se $wR_{(E_1 \cdot 0 | E_2)^*} w'$ e $R_{E_2 \cdot E_2^* \cdot E_1} = \emptyset$ então $(\mathcal{M}, w') \models \neg\varphi$.

O que contradiz (*).

(2) se e somente se (8) $\mathcal{M}, w \models \langle (E_1 \cdot 0 \mid E_2)^* \rangle \varphi \wedge [E_2][E_2^*][E_1] \bot$ e (9) $\mathcal{M}, w \not\models \langle E_1 \mid E_2^* \rangle \varphi$.

(8) se e somente se $\forall w' \in W$ se $wR_{(E_1 \cdot 0 | E_2)^*} w'$ e $R_{E_2 \cdot E_2^* \cdot E_1} = \emptyset$ então $(\mathcal{M}, w') \models \neg\varphi$.

(*)

(9) se e somente se (10) $\mathcal{M}, w \models [E_1 \mid E_2^*] \neg\varphi$.

(10) se e somente se $\forall w' \in W$ se $wR_{(E_1 | E_2^*)} w'$, como $R_{(E_1 | E_2^*)} = R_{(E_1 \cdot 0 | E_2)^*}$ e $R_{E_2 \cdot E_2^* \cdot E_1} = \emptyset$, pela definição 3.7.2, então $\mathcal{M}, w' \models \neg\varphi$. O que contradiz (*).

□

Lema 3.7.2 : *Para todas fbfs $\varphi \in A$ e todos os programas K_i e E_i tal que $i = 1, 2, ..., n$:*

1. *Se $F \models \varphi$ e $F \models \varphi \rightarrow \psi$ então $F \models \psi$*

2. *Se $F \models \varphi$ então $F \models [K]\varphi$ com $K \neq 0$*

3. *Se $F \models \varphi$ então $F \models [E]\varphi$ com $E \neq 0$*

Prova. Idem prova do lema 3.6.2. □

3.7.4 Completude

Modelos Canônicos PDL

A construção do modelo canônico é o mesmo usado em LDP. Primeiro, definimos o Fecho de Fisher e Ladner $F_{FL}(\Sigma)$ para um conjunto Σ de fórmulas e então definimos

o conjunto de átomos de Σ, $At(\Sigma)$.

Definição 3.7.5 (Fecho de Fischer e Ladner). *Seja Σ um conjunto de fórmulas e $Act_\Sigma = \{\alpha_1, \cdots, \alpha_n\}$ o conjunto de todos os programas básicos ocorrendo nas fórmulas de Σ. O* **fecho** *de Σ, notação $F_{FL}(\Sigma)$, é o menor conjunto de fórmulas satisfazendo as seguintes condições:*

1. *$F_{FL}(\Sigma)$ é fechado sob subfórmulas*
2. *Se $\varphi \wedge [\mathring{A}]\bot \in F_{FL}(\Sigma)$ então $\langle 0\rangle\varphi \in F_{FL}(\Sigma)$*
3. *Se $\langle \alpha \cdot E\rangle\varphi \in F_{FL}(\Sigma)$, então $\langle\alpha\rangle\langle E\rangle\varphi \in F_{FL}(\Sigma)$*
4. *Se $\langle E_1 + E_2\rangle\varphi \in F_{FL}(\Sigma)$, então $\langle E_1\rangle\varphi \wedge \langle E_2\rangle\varphi \in F_{FL}(\Sigma)$*
5. *Se $\langle E_1 \mid E_2\rangle\varphi \in F_{FL}(\Sigma)$, então $\langle E_2 \mid E_1\rangle\varphi \in F_{FL}(\Sigma)$*
6. *Se $\langle (E_1 \mid E_2) \setminus L\rangle\varphi \in F_{FL}(\Sigma)$, então $\langle (E_2 \mid E_1) \setminus L\rangle\varphi \in F_{FL}(\Sigma)$*
7. *Se $\langle E^*\rangle\varphi \in F_{FL}(\Sigma)$, então $\langle E\rangle\langle E^*\rangle\varphi \in F_{FL}(\Sigma)$*

É fácil verificar que se Σ é um conjunto finito de fórmulas, então o fechamento $F_{FL}(\Sigma)$ of Σ também é finito. Assumimos que Σ é finito.

Definição 3.7.6 *: Seja Σ um conjunto fórmulas. Um conjunto de fórmulas $\mathcal{A}$ é dito ser um* **átomo de** *Σ se ele é um subconjunto maximal consistente de $F_{FL}(\Sigma)$. O conjunto de todos os átomos de Σ é denotado por $At(\Sigma)$.*

Lema 3.7.3 *: Seja Σ um conjunto de fórmulas. Se $\phi \in F_{FL}(\Sigma)$ e ϕ é consistente então existe um átomo $\mathcal{A} \in At(\Sigma)$ tal que $\phi \in \mathcal{A}$.*

Prova. Podemos construir o átomo $\mathcal{A}$ como segue. Primeiro, enumeramos os elementos de $F_{FL}(\Sigma)$ como $\varphi_1, \cdots, \varphi_n$. Iniciamos a construção fazendo $\mathcal{A}_1 = \{A\}$, então para $1 < i < n$, sabemos que

$$\vdash \mathcal{A}_i \leftrightarrow (\mathcal{A}_n \wedge \varphi_{i+1}) \vee (\mathcal{A}_n \wedge \neg\varphi_{i+1})$$

é uma tautologia e, consequentemente, ou $\mathcal{A}_i \wedge \varphi_{i+1}$ ou $\mathcal{A}_i \wedge \neg\varphi_{i+1}$ é consistente. Tomamos $\mathcal{A}_{i+1}$ como a união de $\mathcal{A}_i$ com o membro consistente da disjunção anterior. Seja $\mathcal{A} = \mathcal{A}_n$. Então $\mathcal{A}$ é um átomo contendo φ. □

Definição 3.7.7 *: Seja Σ um conjunto de fórmulas. As* **relações canônicas sobre** *Σ S_E^Σ em $At(\Sigma)$ são definidas como segue: $\mathcal{A}S_E^\Sigma\mathcal{B}$ se e somente se $\bigwedge \mathcal{A} \wedge \langle E \rangle \bigwedge \mathcal{B}$ é consistente.*

Definição 3.7.8 *: Seja Σ um conjunto de fórmulas. O* **modelo canônico sobre** *Σ é uma tupla $\mathcal{M}^\Sigma = \langle At(\Sigma), Z^\Sigma, S_E^\Sigma, \mathbf{V}^\Sigma \rangle$, onde para todos os símbolos proposicionais p e para todos os átomos $\mathcal{A} \in At(\Sigma)$ temos*

- $\mathbf{V}^\Sigma(p) = \{\mathcal{A} \in At(\Sigma) \mid p \in \mathcal{A}\}$;
- $Z^\Sigma = \{\mathcal{A} \in At(\Sigma) \mid [\mathring{A}]\bot \in \mathcal{A}\}$.

Lema 3.7.4 *As seguintes propriedades sobre a relação S_0 valem:*

1. $S_0^\Sigma \subseteq Z^\Sigma \times Z^\Sigma$;
2. S_0^Σ *é reflexiva;*
3. S_0^Σ *é funcional.*

Prova.

1. $S_0^\Sigma \subseteq Z^\Sigma \times Z^\Sigma$.

Suponha que $\mathcal{A}S_0\mathcal{B}$.

$\bigwedge \mathcal{A} \wedge \langle 0 \rangle \bigwedge \mathcal{B}$ é consistente. *

$\bigwedge \mathcal{A} \wedge \langle 0 \rangle \top$ é consistente, pela maximalidade.

$\langle 0 \rangle \top \in \mathcal{A}$ e pelo axiomo 9, $[\mathring{A}]\bot \in \mathcal{A}$, então $\mathcal{A} \in Z^\Sigma$.

Suponha que $\mathcal{B} \notin Z^\Sigma$, então $[\mathring{A}]\bot \notin \mathcal{B}$. **

$\vdash [\mathring{A}]\top \wedge \langle 0 \rangle [\mathring{A}]\bot \rightarrow [0][\mathring{A}]\bot$, axioma 7

$\vdash [\mathring{A}]\bot \wedge \langle 0 \rangle [\mathring{A}]\bot$

como $[\mathring{A}]\bot \in \mathcal{A}$ então $\mathcal{A} \wedge [0][\mathring{A}]\bot$ é consistente também.

De * e ** $\bigwedge \mathcal{A} \wedge \langle 0 \rangle \neg [\mathring{A}]\bot$ é consistente, isto é uma contradição.

2. S_0^Σ é reflexiva.

Por (1.), $S_0^\Sigma \subseteq Z^\Sigma \times Z^\Sigma$.

Suponha que $\mathcal{A} \in Z^\Sigma$, então $[\mathring{A}]\bot \in \mathcal{A}$

Pelo axioma 6, $\vdash \bigwedge \mathcal{A} \wedge [\mathring{A}]\bot \rightarrow \langle 0 \rangle \wedge \mathcal{A}$.

então $\bigwedge \mathcal{A} \wedge \langle 0 \rangle \wedge \mathcal{A}$ é consistente.

Portanto, $\mathcal{A}S_0^\Sigma\mathcal{A}$.

3. S_0^Σ is funcional.

Por (1.) e (2.), sabemos que $S_0^\Sigma \subseteq Z^\Sigma \times Z^\Sigma$ e S_0^Σ é reflexiva.

Suponha que S_0^Σ não é funcional, então existe $\mathcal{A}$ e $\mathcal{B}$ tal que $\mathcal{A}S_0^\Sigma\mathcal{B}$ e $\mathcal{A} \neq \mathcal{B}$. Mas se $\mathcal{A} \neq \mathcal{B}$ então para alguma fórmula $\varphi \in F_{FL}$, $\varphi \in \mathcal{A}$

mas $\varphi \notin \mathcal{B}$ e portanto $\neg\varphi \in \mathcal{B}$

pelo axioma 6, $\bigwedge \mathcal{A} \wedge \langle 0 \rangle \varphi$ é consistente e

Pelo axioma 7, $\bigwedge \mathcal{A} \wedge [0]\varphi$ é também consistente

mas $\bigwedge \mathcal{A} \wedge \langle 0 \rangle \wedge \mathcal{B}$ é também consistente

mas isto é uma contradição, porque $\neg\varphi \in \mathcal{B}$. □

Dizemos que $\mathbf{V}^{\Sigma}$ é a *valoração canônica.*

Definição 3.7.9 (Modelo Regular LDP-CCS sobre Σ): *Seja Σ um conjunto de fórmulas. Definimos um modelo LDP-CCS sobre Σ como $\mathcal{N} = \langle At(\Sigma), Y, R_E, \mathbf{V} \rangle$ tal que $Y := Z$ e para todo programa básico α, $R_\alpha := S_\alpha$. A relação $R_0 := S_0$ e as relações R_E são definidas indutivamente de acordo com a definição 3.7.2 e $\mathbf{V}$ é a valoração canônica.*

Lema 3.7.5 (Lema da Existência para Programas Básicos): *Seja $\mathcal{A} \in At(\Sigma)$ um átomo e α um programa básico então para toda fórmula $\langle\alpha\rangle\phi \in F_{FL}(\Sigma)$, $\langle\alpha\rangle\phi \in \mathcal{A}$ sse existe um $\mathcal{B} \in At(\Sigma)$ tal que $\mathcal{A}R_\alpha\mathcal{B}$ e $\phi \in \mathcal{B}$.*

Prova.

($\Leftarrow$) Suponha que existe $\mathcal{B} \in At(\Sigma)$ tal que $\mathcal{A}R_\alpha\mathcal{B}$ e $\phi \in \mathcal{B}$.

Como R_α e S_α são idênticas para programas básicos, $\mathcal{A}S_\alpha\mathcal{B}$, então $\bigwedge \mathcal{A} \wedge \langle\alpha\rangle \bigwedge \mathcal{B}$ é consistente. Como ϕ é uma das conjunções em $\bigwedge \mathcal{B}$, $\bigwedge \mathcal{A} \wedge \langle\alpha\rangle\phi$ é consistente. Como $\langle\alpha\rangle\phi$ está em $F_{FL}(\Sigma)$ deve está também em $\mathcal{A}$, como $\mathcal{A}$ é um átomo e consequentemente maximal consistente em $F_{FL}(\Sigma)$.

($\Rightarrow$) Suponha $\langle\alpha\rangle\phi \in \mathcal{A}$.

Vamos construir um átomo apropriado $\mathcal{B}$ por escolhas forçadas. Enumere as fórmulas

em $F_{FL}(\Sigma)$ como $\psi_1, \cdots, \psi_m$. Define-se $\mathcal{B}_0$ como sendo $\{\neg\phi\}$.

Suponha como hipótese indutiva que $\mathcal{B}_n$ é definido tal que $\bigwedge \mathcal{A} \wedge \langle\alpha\rangle \bigwedge \mathcal{B}_n$ é consistente, onde $0 \leq n < m$. Temos que

$$\vdash \langle\alpha\rangle \bigwedge \mathcal{B}_n \leftrightarrow \langle\alpha\rangle(\bigwedge \mathcal{B}_n \wedge \psi_{n+1}) \vee (\bigwedge \mathcal{B}_n \wedge \neg\psi_{n+1}) \text{ então}$$

$$\vdash \langle\alpha\rangle \bigwedge \mathcal{B}_n \leftrightarrow (\langle\alpha\rangle(\bigwedge \mathcal{B}_n \wedge \psi_{n+1}) \vee \langle\alpha\rangle(\bigwedge \mathcal{B}_n \wedge \neg\psi_{n+1}))$$

Portanto, ou para $\mathcal{B}' = \mathcal{B}_n \cup \{\psi_{n+1}\}$ ou para $\mathcal{B}' = \mathcal{B}_n \cup \{\neg\psi_{n+1}\}$ temos que $\bigwedge \mathcal{A} \wedge \langle\alpha\rangle\mathcal{B}'$ é consistente. Escolhemos $\mathcal{B}_{n+1}$ para ser esta expansão consistente, e faça $\mathcal{B}$ ser $\mathcal{B}_m$ é o átomo procurado. □

Lema 3.7.6 : *Sejam $\mathcal{A}, \mathcal{B} \in At(\Sigma)$. Então*

Se $\mathcal{A}S_{E^*}\mathcal{B}$ então $\mathcal{A}(S_E)^*\mathcal{B}$.

Prova. Suponha que $\mathcal{A}S_{E^*}\mathcal{B}$.

Precisamos mostrar que para todos os programas E, se $\mathcal{A}S_{E^*}\mathcal{B}$ então existe uma sequência finita de átomos $C_0, \cdots, C_n$ tal que $\mathcal{A} = C_0 S_E C_1, \cdots, C_{n-1} S_E C_n = \mathcal{B}$. Seja $\mathcal{D}$ o conjunto de todos os átomos alcançáveis de $\mathcal{A}$ por tal sequência. Mostraremos que $\mathcal{B} \in \mathcal{D}$. Definimos ϕ como sendo $\bigvee_{D\in\mathcal{D}} D$. É difícil ver que $\phi \wedge \langle E\rangle\neg\phi$ é inconsistente. Então $\phi \wedge \langle E\rangle F$ deveria ser consistente em ao menos um átomo F não em $\mathcal{D}$, o que significaria que $D \wedge \langle E\rangle F$ era consistente para ao menos um $D \in \mathcal{D}$. Mas então por DS_EF, F poderia ser alcançado de A em uma quantidade finita de passos S_E, o que implicaria que $F \in \mathcal{D}$, o que não é.

Como $\phi \wedge \langle E\rangle\neg\phi$ é inconsistente, $\vdash \phi \rightarrow [E]\phi$, pela generalização $\vdash [E^*](\phi \rightarrow [E]\phi)$. Pelo axioma 18, $\vdash \phi \rightarrow [E^*]\phi$. Agora, como $AS_{E^*}A$, A é um dos disjuntos em ϕ, assim, $\vdash A \rightarrow \phi$ e, portanto, $\vdash A \rightarrow [E^*]\phi$.

Como a suposição inicial era que $A \wedge \langle E^* \rangle B$ é consistente, segue que $A \wedge \langle E^* \rangle (B \wedge \phi)$ é consistente também.

Mas isto significa que para um dos disjuntos D de ϕ, $B \wedge D$ é consistente. Como B e D são átomos, $B = D$ e consequentemente $B \in \mathcal{D}$. E, pela definição $\mathcal{D}$, temos $\mathcal{A}(S_E)^*\mathcal{B}$. □

Lema 3.7.7 : *Seja $\mathcal{A} \in At(\Sigma)$ e $\langle E \rangle \varphi \in F_{FL}(\Sigma)$. Então $\langle E \rangle \varphi \in \mathcal{A}$ se e somente se existe $\mathcal{B} \in At(\Sigma)$ tal que $\mathcal{A} S_E \mathcal{B}$ e $\varphi \in \mathcal{B}$.*

Prova.

($\Rightarrow$) Suponha que $\langle E \rangle \varphi \in \mathcal{A}$.

Pela definição 3.7.6, temos que $\bigwedge \mathcal{A} \wedge \langle E \rangle \varphi$ é consistente.

Usando a tautologia, pelo raciocínio modal, $\vdash \varphi \leftrightarrow ((\varphi \wedge \phi) \vee (\varphi \wedge \neg\phi))$, temos que ou $\bigwedge \mathcal{A} \wedge \langle E \rangle (\varphi \wedge \phi)$ é consistente ou $\bigwedge \mathcal{A} \wedge \langle E \rangle (\varphi \wedge \neg\phi)$ é consistente.

Portanto, por escolhas apropriadas de ϕ, para todas as fórmulas $\phi \in F_{FL}$, podemos construir um átomo $\mathcal{B}$ tal que $\varphi \in \mathcal{B}$ and $\bigwedge \mathcal{A} \wedge \langle E \rangle (\varphi \wedge \bigwedge \mathcal{B})$ é consistente e pela definição 3.7.7, $\mathcal{A} S_E \mathcal{B}$.

($\Leftarrow$) Suponha que existe um $\mathcal{B}$ tal que $\varphi \in \mathcal{B}$ e $\mathcal{A} S_E \mathcal{B}$. Então $\bigwedge \mathcal{A} \wedge \langle E \rangle \wedge \bigwedge \mathcal{B}$ é consistente e também que $\bigwedge \mathcal{A} \wedge \langle E \rangle \varphi$ é consistente. Mas $\langle E \rangle \varphi \in F_{FL}$ e pela maximalidade $\langle E \rangle \varphi \in \mathcal{A}$. □

Lema 3.7.8 : *Seja $\mathcal{A} \in At(\Sigma)$ e $\langle E^* \rangle \varphi \in F_{FL}$. Então $\langle E^* \rangle \varphi \in \mathcal{A}$ se e somente se existe um $\mathcal{B} \in At(\Sigma)$ tal que $\mathcal{A}(S_E)^*\mathcal{B}$ e $\varphi \in \mathcal{B}$.*

Prova.

($\Rightarrow$) Suponha $\langle E^* \rangle \varphi \in \mathcal{A}$.

Pelo lema 3.7.7, existe um átomo $\mathcal{B}$ tal que $\mathcal{A}S_{E^*}\mathcal{B}$ e pelo lema 3.7.6 temos que $\mathcal{A}(S_E)^*\mathcal{B}$.

($\Leftarrow$) Suponha que para algum $\mathcal{B}$, $\mathcal{A}(S_E)^*\mathcal{B}$ e $\varphi \in \mathcal{B}$. Então, para algum n $\mathcal{A} = \mathcal{A}_1 S_E \cdots S_E \mathcal{A}_n = \mathcal{B}$. Podemos provar por indução em $1 < k < n$.

$k = 2$: $\mathcal{A}S_E\mathcal{B}$ e $\varphi \in \mathcal{B}$. Pelo lema 3.7.7 $\langle E\rangle\varphi \in \mathcal{A}$. Do axiom 21, sabemos que $\vdash \langle E\rangle\varphi \rightarrow \langle E^*\rangle\varphi$ e pela definição de F_{FL} e maximalidade temos que $\langle E^*\rangle\varphi \in \mathcal{A}$.

$k > 2$: Pela hipótese de indução $\langle E^*\rangle\varphi \in \mathcal{A}_2$, e sabemos que $\mathcal{A}_1 S_E \mathcal{A}_2$, pelo lema 3.7.7 temos $\langle E\rangle\langle E^*\rangle\varphi \in \mathcal{A}_1$. Do axioma 22, obtemos $\vdash \langle E\rangle\langle E^*\rangle\varphi \rightarrow \langle E^*\rangle\varphi$ pela definição de F_{FL} e maximalidade temos $\langle E^*\rangle\varphi \in \mathcal{A}$.

□

Definição 3.7.10 : *O comprimento de um agente* $\mid E \mid$ *é definido como o número de ações e operadores sem contar os* $\cdot 0$.

Lema 3.7.9 : *Seja* $E = E_1 \mid E_2$ *e* $\mid E \mid = m$. *Então*

a. $\vdash \langle E\rangle\varphi \leftrightarrow \langle(\langle F_1\rangle\varphi \wedge \phi_1) \vee (\langle F_2\rangle\varphi \wedge \phi_2) \vee \cdots \vee (\langle F_n\rangle\varphi \wedge \phi_n)$
onde para cada termo F_i *da forma* $F_i^l \mid \cdots \mid (F_i^l)^*$ *e* $\phi_i = [F_i^l][F_i^l)^*][[F_i^1 \mid \cdots \mid [F_i^{l-1}]\bot$, *caso contrário* $\phi_i = \top$

b. $R_E = R_{F_1+\cdots+F_n}$ *e* $R_{E_2 \cdot E_2^* \cdot E_1} = \emptyset$, *onde cada* F_i *do tipo* $F_i = (E_1 \cdot 0 \mid E_2)^*$ *é ou*

   1. $F_i = G_1^i \mid \cdots \mid G_{n_1}^i$ *e* $\mid F_i \mid < n$ *ou*

   2. $F_i = (H_i)^*$ *e* $\mid H_i \mid < n$ *ou*

   3. $F_i = \alpha \cdot C_i$ *e* $\mid C_i \mid < n$

Prova.: *a*. Indução no número de composição paralela.

Base: $n = 1$, temos várias possibilidades:

1. $E_1 = D_1 + D_1'$
2. $E_2 = D_2 + D_2'$
3. $E_1 = \alpha_1 \cdot D_1$
4. $E_2 = \alpha_2 \cdot D_2$
5. $E_1 = (D_1)^*$
6. $E_2 = (D_2)^*$

Nos casos 1. e 2. se um dos dois ou ambos for uma soma, podemos aplicar o axioma da distribuição da $\mid$ sobre a soma:

$$\vdash \langle (E_1 \mid (E_2 + E_3)) \rangle \varphi \leftrightarrow \langle E_1 \mid E_2 + E_1 \mid E_3 \rangle \varphi$$

e transformando E numa soma onde cada parcela tem comprimento menor que n.

Isto cobre os casos 1 $\mid$ 2, 1 $\mid$ 4, 1 $\mid$ 6, 3 $\mid$ 2 e 5 $\mid$ 2.

Caso 5 $\mid$ 4, onde $E_1 = \alpha_1 \cdot D_1$ e $E_2 = (D_2^*)$

$\langle E \rangle \varphi \leftrightarrow \langle E_1 \mid E_2 \rangle \varphi \leftrightarrow \langle \alpha_1 \cdot D_1 \mid D_2^* \rangle \varphi \wedge [D_2^*][E_1]\bot$

Pelo axioma 17, $\langle E \rangle \varphi \leftrightarrow \langle (\alpha \cdot D \centerdot 0 \mid D_2)^* \rangle \varphi \wedge [D_2^*][E_1]\bot$ e $\mid \alpha \cdot D \centerdot 0 \mid D_2 \mid < \mid E \mid$.

Caso 3 $\mid$ 6 é análogo ao 5 $\mid$ 4.

Caso 5 $\mid$ 6 é análogo ao 5 $\mid$ 4.

Caso 3 $\mid$ 4, onde $E_1 = \alpha_1 \cdot D_1$ e $E_2 = \alpha_2 \centerdot D_2$

$\langle \alpha_1 \cdot D_1 \mid \alpha_2 \cdot D_2 \rangle \varphi \leftrightarrow \langle \alpha_1 \cdot (D_1 \mid \alpha_2 \centerdot D_2) + \alpha_2 \cdot (\alpha_1 \centerdot D_1 \mid \alpha_2 \cdot D_2) \rangle \varphi$ e

$\mid D_1 \mid \alpha_2 \cdot D_2 \mid < \mid E \mid$ e $\mid \alpha_1 \cdot D_1 \mid \alpha_2 \cdot D_2 \mid < \mid E \mid$

H.I. vale para agentes com $k < n$ composições paralelas.

Suponha que E tem n composições paralelas

$$E = E_1 \mid E_2 \mid \cdots \mid E_{n+1}$$

$\langle E \rangle \varphi \rightarrow \langle E_1 \mid E_2 \mid \cdots \mid E_{n+1} \rangle \varphi$.

Temos vários casos:

1. Se um dos E_i's $1 \leq i \leq n+1$ for uma soma aplicando a distribuição da $\mid$ sobre a $+$ e obtemos duas parcelas de composição paralela com comprimento menor que $\mid E \mid$.

2. Se um dos E_i's for D_i^*, usando comutatividade e associatividade pelo axioma 17

$\langle E \rangle \varphi \leftrightarrow \langle (D_i \mid (E_1 \mid \cdots \mid E_i \mid E_{i+1} \mid \cdots \mid E_{n+1}) \cdot 0)^* \rangle \varphi \wedge [D_i][D_i^*][E_1 \mid \cdots \mid E_i \mid E_{i+1} \mid \cdots \mid E_{n+1}]\bot$ e $\mid D_1 \mid (E_1 \mid \cdots \mid E_i \mid E_{i+1} \mid \cdots \mid E_{n+1}) \mid < \mid E \mid$.

3. Todos os E_i's são do tipo $\alpha_i \cdot D_i$.

Usando o axioma 16, $\langle \alpha_1 \cdot D_1 \mid \alpha_2 \cdot D_2 \mid \cdots \mid \alpha_n \cdot D_n \rangle \varphi \leftrightarrow$

$\alpha_1 \cdot (D_1 \mid \alpha_2 \cdot D_2 \mid \cdots \mid \alpha_n \cdot D_n) + \cdots + \alpha_n \cdot (\alpha_1 \cdot D_1 \mid \cdots \mid D_n) + \tau \cdot (\alpha_1 \cdot D_1 \mid \cdots \mid D_n) \rangle \varphi$

e

$\mid \alpha_1 \cdot D_1 \mid \cdots \mid D_i \mid \cdots \mid \alpha_n \cdot D_n \mid < \mid E \mid$ para todo i, $1 \leq i \leq n$.

b. Análoga ao caso *a.*. □

Lema 3.7.10 : $S_E \subseteq R_E$.

Prova.

Pela indução no tamanho de $\mid E \mid$.

Base: $n = 0$, $E = 0$ e $E = i$. Neste caso, por definição $S_E = R_E$.

H.I. Vale para $\mid E \mid < m$:

1. $E = \alpha \cdot E_1$

Suponha que $\mathcal{A}S_{\alpha \cdot E}\mathcal{B}$, isto é, $\mathcal{A} \wedge \langle \alpha \cdot E \rangle \mathcal{B}$ é consistente. Pelo axioma 4, $\mathcal{A} \wedge \langle \alpha \rangle \langle E \rangle \mathcal{B}$ é consistente também. Usando um argumento de escolhas forçadas podemos construir um átomo $\mathcal{C}$ tal que $\mathcal{A} \wedge \langle \alpha \rangle \mathcal{C}$ e $\mathcal{C} \wedge \langle E \rangle \mathcal{B}$ são ambos consistente. Mas pela hipótese de indução $\mathcal{A}R_{\alpha}\mathcal{C}$ e $\mathcal{C}R_{E}\mathcal{B}$. Segue que $\mathcal{A}R_{\alpha \cdot E}\mathcal{B}$ como requerido.

2. $E = E_1 + E_2$

Suponha que $\mathcal{A}S_{E_1+E_2}\mathcal{B}$, isto é, $\mathcal{A} \wedge \langle E_1 + E_2 \rangle \mathcal{B}$ é consistente. Pelo axioma 5, $\mathcal{A} \wedge \langle E_1 \rangle \mathcal{B}$ é consistente ou $\mathcal{A} \wedge \langle E_2 \rangle \mathcal{B}$ é consistente. Mas pela hipótese de indução $\mathcal{A}R_{E_1}\mathcal{B}$ ou $\mathcal{A}R_{E_2}\mathcal{B}$. Segue que $\mathcal{A}R_{E_1+E_2}\mathcal{B}$, como requerido.

3. $E = E_1^*$

Foi provado no lema 3.7.6.

4. $E = E_1 \mid E_2$

Suponha $\mathcal{A}S_{E_1|E_2}\mathcal{B}$ se e somente se $\bigwedge \mathcal{A} \wedge \langle E_1 \mid E_2 \rangle \wedge \mathcal{B}$ é consistente.

Pelo lema 3.7.9, $\bigvee(\bigwedge \mathcal{A} \wedge \langle F_1 + \cdots + F_n \rangle \wedge \mathcal{B} \wedge \phi_i)$ é consistente.

Aplicando o axioma 5, $\vdash \langle E_1 + E_2 \rangle \varphi \leftrightarrow \langle E_1 \rangle \vee \langle E_2 \rangle \varphi$ e distribuindo $\wedge$ sobre $\vee$, temos que $\bigvee(\wedge \mathcal{A} \wedge \langle F_i \rangle \wedge \mathcal{B} \wedge \phi_i)$.

Logo ou $\bigvee(\wedge \mathcal{A} \wedge \langle F_i \rangle \wedge \mathcal{B}$ é consistente, logo $\mathcal{A} \wedge \langle F_i \rangle \wedge \mathcal{B}$ é consistente e $\mathcal{A} \wedge \phi_i$ é consistente.

Ou $\mathcal{A}S_{F_i}\mathcal{B}$ ou $\cdots$ ou $\mathcal{A}S_{F_i}\mathcal{B}$.

Logo, temos três casos:

1. $F_i = G_1^i \mid \cdots \mid G_{n_1}^i$ e $\mid F_i \mid < n$ e $\phi_i = \top$, logo pela H.I., $\mathcal{A}R_{F_i}\mathcal{B}$ ou

2. $F_i = (H_i)^*$,$H_i = E_1 \cdot 0 \mid E_2$ e $\phi_i = [E_2][E_2^*][E_1]\bot$, logo $R_{E_2 \cdot E_2^* \cdot E_1} = \emptyset$ e portanto

$\mathcal{A} \wedge \phi$ é consistente.

Logo $\mathcal{A}S_{H_i^*}\mathcal{B}$.

Pelo lema 3.7.6, $\mathcal{A}(S_{H_i})^*\mathcal{B}$.

Pela H.I., $S_{H_i} \subseteq R_{Hi}$, logo $\mathcal{A}(R_{H_i})^*\mathcal{B}$.

Pela definição, $(R_{H_i})^* = R_{H_i^*}$ e portanto,

$\mathcal{A}R_{H_i^*}\mathcal{B}$, logo $\mathcal{A}R_{F_i}\mathcal{B}$ ou

3. $F_i = \alpha_i \cdot H_i$, logo $\mathcal{A}S_{\alpha_i \cdot H_i}\mathcal{B}$.

   Pelo lema 3.7.6, $\mathcal{A}(S_{\alpha_i}; S_{H_i})\mathcal{B}$.

   Como $S_\alpha = R_\alpha$ e pela H.I., $S_{H_i} \subseteq R_{H_i}$, temos que $\mathcal{A}(R_{\alpha_i}; R_{H_i})\mathcal{B}$.

   Pela definição, $\mathcal{A}R_{\alpha_i \cdot H_i}\mathcal{B}$, portanto, $\mathcal{A}R_{F_i}\mathcal{B}$.

Logo, $\mathcal{A}(R_{F_1} \cup R_{F_2} \cup \cdots \cup R_{F_m})\mathcal{B}$.

Pela definição de R, $\mathcal{A}(R_{F_1} + R_{F_2} + \cdots + R_{F_m})\mathcal{B}$ e $R_{E_2 \cdot E_2^* \cdot E_1} = \emptyset$, para todo $F_i = (E_1 \cdot 0 \mid E_2)^*$.

Pelo lema 3.7.9, $\mathcal{A}R_E\mathcal{B}$.

□

Lema 3.7.11 (Lema da Existência): *Para todos os átomos $\mathcal{A}$ e todas as fórmulas $\langle E \rangle \phi \in F_{FL}(\Sigma)$, $\langle E \rangle \phi \in \mathcal{A}$ sse existe um $\mathcal{B}$ tal que $\mathcal{A}R_E\mathcal{B}$ e $\phi \in \mathcal{B}$.*

Prova.

($\Rightarrow$) Suponha que $\langle E \rangle \phi \in \mathcal{A}$. Pelo lema 3.7.7, existe um átomo $\mathcal{B} \in At(\Sigma)$ tal que $\mathcal{A}S_E\mathcal{B}$ e $\varphi \in \mathcal{B}$. Mas provamos no lema 3.7.9 que se $\mathcal{A}S_E\mathcal{B}$ então $\mathcal{A}R_E\mathcal{B}$ também.

($\Leftarrow$) Procedemos pela indução na estrutura de E.

- O caso base é o Lema da Existência para programas básicos e no caso do programa 0 segue do fato que $R_0 = S_0$.

- Suponha que E tem a forma $\langle \alpha \cdot E \rangle \phi$ e, além disso, suponha que $\mathcal{A} R_{\alpha \cdot E} \mathcal{B}$ e $\phi \in \mathcal{B}$. Então existe um átomo $\mathcal{C}$ tal que $\mathcal{A} R_\alpha \mathcal{C}$ e $\mathcal{C} R_E \mathcal{B}$ e $\phi \in \mathcal{B}$. Pela hipótese de indução, $\langle E \rangle \phi \in C$ e $\langle \alpha \rangle \langle E \rangle \phi \in F_{FL}(\Sigma)$, $\langle \alpha \rangle \langle E \rangle \phi \in \mathcal{A}$. Portanto, $\langle \alpha \cdot E \rangle \phi \in \mathcal{A}$ como requerido.

- Suponha que E tem a forma $\langle E_1 + E_2 \rangle \phi$, e, além disso, suponha que $\mathcal{A} R_{E_1 + E_2} \mathcal{B}$ e $\phi \in \mathcal{B}$. Pela definição da relação R, $\mathcal{A} R_{E_1} \mathcal{B}$ ou $\mathcal{A} R_{E_2} \mathcal{B}$ e $\phi \in \mathcal{B}$. Pela hipótese de indução, $\langle E_1 \rangle \phi \in \mathcal{A}$ ou $\langle E_2 \rangle \phi \in \mathcal{A}$. Então $\langle E_1 \rangle \phi \vee \langle E_2 \rangle \phi \in \mathcal{A}$. Portanto, $\langle E_1 + E_2 \rangle \phi \in \mathcal{A}$. Como requerido.

- Suponha que E tem a forma $\langle E_1 \mid E_2 \rangle \phi$ e além disso, suponha que $\mathcal{A} R_{E_1 | E_2} \mathcal{B}$ e $\phi \in \mathcal{B}$. Pela definição da relação R, $\mathcal{A} R_{E_2 | E_1} \mathcal{B}$ e $\phi \in \mathcal{B}$. Pela hipótese de indução, $\langle E_2 \mid E_1 \rangle \phi \in \mathcal{A}$. Então $\langle E_1 \mid E_2 \rangle \phi \in \mathcal{A}$ como requerido.

- Suponha que E tem a forma $\langle (E_1 \mid E_2) \mid E_3 \rangle \phi$ e além disso, suponha que $R_{(E_1 | E_2) | E_3} \mathcal{B}$ e $\phi \in \mathcal{B}$. Pela definição da relação R, $R_{E_1 | (E_2 | E_3)} \mathcal{B}$ e $\phi \in \mathcal{B}$. Pela hipótese de indução, $\langle E_1 \mid (E_2 \mid E_3) \rangle \phi \in \mathcal{A}$. Então $\langle (E_1 \mid E_2) \mid E_3 \rangle \phi \in \mathcal{A}$ como requerido.

- Suponha que E tem a forma $\langle E \mid 0 \rangle \phi$ e além disso, suponha que $R_{E|0} \mathcal{B}$ e $\phi \in \mathcal{B}$. Pela definição da relação R, $\mathcal{A} R_E \mathcal{B}$ e $\phi \in \mathcal{B}$. Pela hipótese de indução, $\langle E \rangle \phi \in \mathcal{A}$. Então $\langle E \mid 0 \rangle \phi \in \mathcal{A}$, como requerido.

- Suponha que E tem a forma $\langle (E_1 + E_2) \mid E_3 \rangle \phi$ e além disso, suponha que $R_{(E_1 + E_2) | E_3} \mathcal{B}$ e $\phi \in \mathcal{B}$. Pela definição da relação R, $\mathcal{A} R_{(E_1 | E_3) + (E_2 | E_3)} \mathcal{B}$ e $\phi \in \mathcal{B}$.

Pela hipótese de indução, $\langle (E_1 \mid E_3) + (E_2 \mid E_3) \rangle \phi \in \mathcal{A}$. Então $\langle (E_1 + E_2) \mid E_3 \rangle \phi \in \mathcal{A}$, como requerido.

- Suponha que $\mathcal{A} R_{E^*} \mathcal{B}$ e $\phi \in \mathcal{B}$. Isto significa que existe uma sequência finita de átomos $\mathcal{C}_0 \cdots \mathcal{C}_n$ tal que $\mathcal{A} = \mathcal{C}_0 R_E \mathcal{C}_1 \cdots \mathcal{C}_n R_E \mathcal{C}_{n+1} = \mathcal{B}$. Por uma subindução em n provamos que $\langle E^* \rangle \phi \in \mathcal{C}_i$, para todo i, o resultado requerido para $\mathcal{A} = \mathcal{C}_0$ é então imediato.

  Caso Base: $n = 0$. Isto significa que $\mathcal{A} = \mathcal{B}$. Do axioma 17, temos que $\vdash \langle E^* \rangle \phi \leftrightarrow \phi \vee \langle E \rangle \langle E^* \rangle \phi$ e consequentemente que $\vdash \phi \rightarrow \langle E^* \rangle \phi$. Portanto, $\langle E^* \rangle \phi \in \mathcal{A}$.

  Passo Indutivo: Suponha que o resultado é válido para $n \leq k$, e que $\mathcal{A} = \mathcal{C}_0 R_E \mathcal{C}_1 \cdots \mathcal{C}_n R_E \mathcal{C}_{k+1} = \mathcal{B}$.

  Pela hipótese de indução, $\langle E^* \rangle \phi \in \mathcal{C}_1$. Consequentemente, $\langle E \rangle \langle E^* \rangle \phi \in \mathcal{A}$, por $\langle E \rangle \langle E^* \rangle \phi \in F_{FL}(\Sigma)$. Usando o axioma 17, temos que $\vdash \langle E \rangle \langle E^* \rangle \phi \rightarrow \langle E^* \rangle \phi$. Portanto, $\langle E^* \rangle \phi \in \mathcal{A}$. Isto completa a subindução e estabelece o resultado requerido para $\langle E^* \rangle$. Isto também completa a indução principal e portanto a prova do lema.

□

Lema 3.7.12 (Lema da Verdade): *Seja $\mathcal{M} = (W, Z_E, V)$ um modelo finito construído sobre uma fórmula ϕ pela construção apresentada acima. Para todos os átomos $\mathcal{A}$ e todos $\varphi \in F_{FL}(\phi)$, $\mathcal{M}, \mathcal{A} \models \varphi$ se e somente se $\varphi \in \mathcal{A}$.*

Prova. Por indução na estrutura de φ.

- Fórmulas atômica e operadores Booleanos diretamente da definição de V;

- Modalidade $\langle x \rangle$, para $x \in \{\alpha, \alpha \cdot E, E_1 + E_2, 0, E_1 \mid E_2, (E_1 \mid E_2) \setminus L, E^*\}$

  ($\Rightarrow$) Suponha $\mathcal{M}, \mathcal{A} \models \langle x \rangle \varphi$, então existe $\mathcal{A}'$ tal que $\mathcal{A} R_x \mathcal{A}'$ e $\mathcal{M}, \mathcal{A}' \models \varphi$. Pela hipótese de indução $\varphi \in \mathcal{A}'$, pelo lema 3.7.7, para o caso que $x = E^*$ usamos o lema 3.7.11, temos que $\langle x \rangle \varphi \in \mathcal{A}$.

  ($\Leftarrow$) Suponha $\mathcal{M}, \mathcal{A} \not\models \langle x \rangle \varphi$. Para todos $\mathcal{A}'$, $\mathcal{A} S_x \mathcal{A}'$ e $\mathcal{M}, \mathcal{A}' \not\models \varphi$. Pela hipótese de indução $\varphi \notin \mathcal{A}'$, pelo lema 3.7.7, para o caso que $x = E^*$ usamos o lema 3.7.11, temos $\langle x \rangle \varphi \notin \mathcal{A}$.

□

Teorema 3.7.2 (Completude para Modelos Finitos): *LDP-CCS com Composição Paralela e Iteração com Sincronização é completa com respeito à classe de modelos finitos.*

Prova. Para toda fórmula consistente φ podemos construir um modelo canônico e então usamos a construção para fazer um modelo finito $\mathcal{M}_\varphi$. Pelo lema 3.7.3, existe um átomo $\mathcal{A} \in At(\Sigma)$ tal que $\varphi \in \mathcal{A}$, e pelo **Lema da Verdade**, $\mathcal{M}, \mathcal{A} \models \varphi$. Portanto, nosso sistema modal é completo com respeito à classe de modelos finitos.
□

Capítulo 4

Exemplos

4.1 Exemplo1: Máquina de Vendas

Considere uma máquina de vendas:

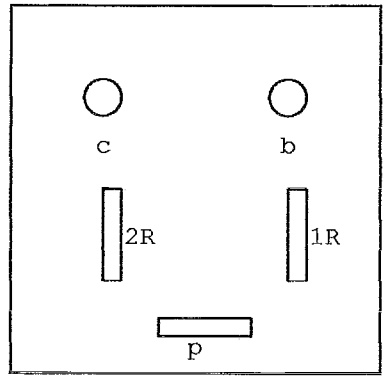

Figura 4.1: Máquina de Vendas

$$M \stackrel{\text{def}}{=} 1(v \cdot p \cdot M + 1 \cdot a \cdot p \cdot M) + 2 \cdot a \cdot p \cdot M$$

ESTADOS:

V = luz vermelha está acesa;

A = luz amarela está acesa;

P = chocolate pequeno está diponível;

G = chocolate grande está disponível.

AÇÕES ($\mathcal{A}$):

1 = colocar moeda de um real;

2 = colocar duas moedas de um real;

v = escolher chocolate pequeno;

a = escolher chocolate grande;

p = pegar chocolate grande ou pequeno;

ESPECIFICAÇÃO:

$(\neg V \wedge \neg A) \rightarrow [1]V$

$(\neg V \wedge \neg A) \rightarrow [1][1]A$

$(\neg V \wedge \neg A) \rightarrow [2]A$

$A \rightarrow [a]G$

$V \rightarrow [v]P$

$P \vee G \rightarrow [p](\neg V \wedge \neg A)$

$$M \equiv (1 \cdot (v \cdot p + 1 \cdot a \cdot p) + 2 \cdot a \cdot p)^*$$

PROPRIEDADES:

1. $[1 \cdot 0]V$

2. $[1 \cdot 1 \cdot 0]A$

3. $[2 \cdot a \cdot 0]G$

4. $[1 \cdot 1 \cdot a]G$

5. $(\neg V \wedge \neg A) \rightarrow [M](\neg V \wedge \neg A)$

6. $(\neg V \wedge \neg A) \rightarrow [M]\langle K\rangle \top$

Podemos provar as propriedades acima como segue:

1. $[1 \cdot 0]V$

   Prova. $[1] \rightarrow [1]V$

   $[1]V$

   $[1 \cdot 0]V$ □

2. $[1 \cdot 1 \cdot 0]A$

   Prova. $1 \rightarrow [1]A$ (especificação)

   $[1](1 \rightarrow [1]A)$ (necessidade)

   $[1]a \rightarrow [1][1]A$ (K)

   $[1][1]A$ (MP)

   $[1 \cdot 1 \cdot 0]A$ (axioma 4) □

3. $[2 \cdot a \cdot 0]G$

   Prova.

   $a \rightarrow [a]G$ (especificação)

   $[2](a \rightarrow [a]G)$ (necessidade)

   $[2]a \rightarrow [2][a]G$ (K)

   $[2][a]G$ (MP)

   $[2 \cdot a]G$ (axioma 5)

   $[2 \cdot a \cdot 0]G$ (axioma 4) □

4. $(\neg V \wedge \neg A) \rightarrow [M](\neg V \wedge \neg A)$

Prova.

$\neg(V \wedge A)$

$\neg([a]G \wedge [v]P)$

$P \vee G$

$[p](\neg V \wedge \neg A)$

$[M](\neg V \wedge \neg A)$ □

4.2 Exemplo2: Máquina de Vendas com Troco

Considere uma máquina de vendas:

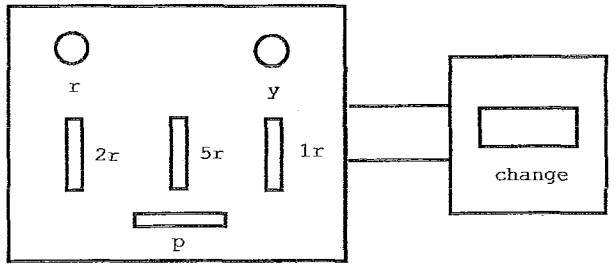

Figura 4.2: Máquina de Vendas com Troco

ESTADOS:

R = luz vermelha está acesa;

Y = luz amarela está acesa;

S = chocolate pequeno está disponível;

B = chocolate grande está disponível.

C = troco está disponível.

AÇÕES

1 = colocar moeda de um real;

2 = colocar duas moedas de um real;

5 = colocar uma nota de cinco reais;

s = escolher chocolate pequeno;

b = escolher chocolate grande;

c = pegar chocolate grande ou pequeno;

ch = apanhar o troco.

ESPECIFICAÇÃO:

$(\neg R \wedge \neg Y) \rightarrow [1]R$

$(\neg R \wedge \neg Y) \rightarrow [1][1]Y$

$(\neg R \wedge \neg Y) \rightarrow [2]Y$

$(\neg R \wedge \neg Y) \rightarrow [5](R \wedge Y)$

$(R \wedge Y) \rightarrow [s \cdot 4]S \wedge [b \cdot 3]B$

$Y \rightarrow [b]B$

$R \rightarrow [s]S$

$S \vee B \rightarrow [c](\neg R \wedge \neg Y)$

$(\neg R \wedge \neg Y) \rightarrow [\tau]C$

$C \rightarrow [5 \cdot 3 \cdot b]B + [5 \cdot 4 \cdot s]S$

$V \equiv (1 \cdot (s \cdot c + 1 \cdot b \cdot c) + 2 \cdot b \cdot c)^*$

$V' \equiv (1 \cdot (s \cdot c + 1 \cdot b \cdot c) + 2 \cdot b \cdot c)^* + 5(s \cdot \overline{4} + b \cdot \overline{3})$

$CH \equiv (3 \cdot c' + 4 \cdot c')$

$$V_{CH} \equiv (V' \mid CH)^*$$

PROPRIEDADES:

1. $[1 \cdot 0]R$
2. $[1 \cdot 1 \cdot 0]Y$
3. $[2 \cdot y \cdot 0]B$
4. $[1 \cdot 1 \cdot y]B$

5. $[5 \cdot 3 \cdot r \cdot 0]S$

6. $[5 \cdot 4 \cdot y \cdot 0]B$

7. $(\neg R \wedge \neg Y) \rightarrow [V](\neg R \wedge \neg Y)$

8. $(\neg R \wedge \neg Y) \rightarrow [V]\langle K \rangle \top$

9. $(\neg R \wedge \neg Y) \rightarrow [V' \mid CH](\neg R \wedge \neg Y)$

10. $(\neg R \wedge \neg Y) \rightarrow [V_{CH}](\neg R \wedge \neg Y)$

11. $(\neg R \wedge \neg Y) \rightarrow [V_{CH}]\langle K \rangle \top$

4.3 Exemplo3: Cruzamento

Esse exemplo representa uma abstração de concorrência de um cruzamento consistindo em:

$$C \stackrel{\text{def}}{=} (R \mid T \mid S)$$

ESTADOS:

R = estrada para carros;

T = estrada com trilhos;

S = sinal que indica se o cruzamento está liberado para o trem ou para o carro;

AÇÕES:

c = carro se aproximando;

t = trem se aproximando;

l = barra levantada;

a = barra abaixada;

v = indica sinal verde para o trem;

r = indica sinal vermelho para o carro;

cc = carro cruzando;

tc = trem cruzando;

CO-AÇÕES:

$\overline{l}$ = barra levantada;

$\overline{a}$ = barra abaixada;

$\overline{v}$ = indica sinal verde para o trem;

$\overline{r}$ = indica sinal vermelho para o carro;

$\overline{cc}$ = carro cruzando;

$\overline{tc}$ = trem cruzando;

ESTADO INICIAL:

Inicialmente as barras estão abaixadas e o sinal está verde para o trem.

$R \stackrel{\text{def}}{=} c \cdot l \cdot cc \cdot \overline{a} \cdot R$

$T \stackrel{\text{def}}{=} t \cdot v \cdot tc \cdot \overline{r} \cdot T$

$S \stackrel{\text{def}}{=} \overline{v} \cdot r \cdot S + \overline{l} \cdot a \cdot S$

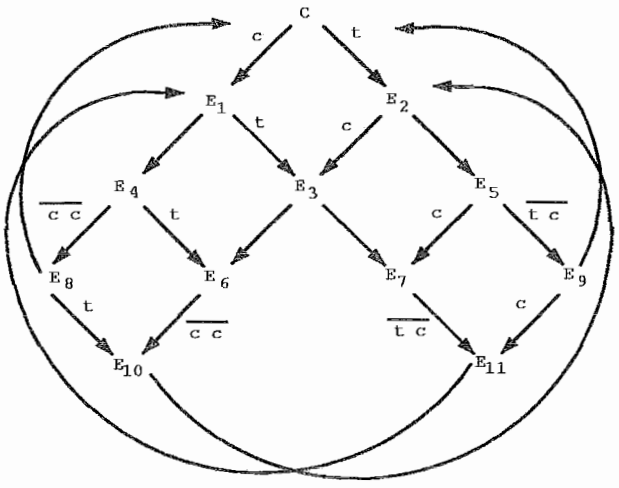

Figura 4.3: Cruzamento

De acordo com a figura acima, podemos definir os agentes do seguinte modo:

$C = E_1 + E_2$

$E_1 = t \cdot E_3 + \tau \cdot E_4$

$E_2 = c \cdot E_3 + \tau \cdot E_5$

$E_3 = \tau \cdot E_6 + \tau \cdot E_7$

$E_4 = \overline{cc} \cdot E_8 + t \cdot E_6$

$E_5 = c \cdot E_7 + \overline{tc} \cdot E_9$

$E_6 = \overline{cc} \cdot E_{10}$

$E_7 = \overline{tc} \cdot E_{11}$

$E_8 = t \cdot E_{10} + \tau \cdot C$

$E_9 = c \cdot E_{11} + \tau \cdot C$

$E_{10} = \tau \cdot E_2$

$E_{11} = \tau \cdot E_1$

$L = \{v, r, l, a\}$

$E_0 \equiv C$

$E_1 \equiv [(l \cdot \overline{cc} \cdot \overline{a} \cdot R \mid T \mid S] \setminus L$

$E_2 \equiv [R \mid v \cdot \overline{tc} \cdot \overline{r} \cdot T \mid S] \setminus L$

$E_3 \equiv [l \cdot \overline{cc} \cdot a \cdot R \mid v \cdot \overline{tc} \cdot \overline{r} \cdot T \mid S] \setminus L$

$E_4 \equiv [\overline{cc} \cdot \overline{a} \cdot R \mid T \mid a \cdot S] \setminus L$

$E_5 \equiv [R \mid \overline{tc} \cdot \overline{r} \cdot T \mid r \cdot S] \setminus L$

$E_6 \equiv [\overline{cc} \cdot \overline{a} \cdot R \mid v \cdot \overline{tc} \cdot \overline{r} \cdot T \mid a \cdot S] \setminus L$

$E_7 \equiv [l \cdot \overline{cc} \cdot \overline{a} \cdot R \mid \overline{tc} \cdot \overline{r} \cdot T \mid r \cdot S] \setminus L$

$E_8 \equiv [\overline{a} \cdot R \mid T \mid a \cdot S] \setminus L$

$E_9 \equiv [R \mid \overline{r} \cdot T \mid r \cdot S] \setminus L$

$E_{10} \equiv [\overline{a} \cdot R \mid v \cdot \overline{tc} \cdot \overline{r} \cdot T \mid a \cdot S] \setminus L$

$E_{11} \equiv [l \cdot \overline{cc} \cdot \overline{a} \cdot R \mid \overline{r} \cdot T \mid r \cdot S] \setminus L$

ESPECIFICAÇÃO:

1. $[(R \mid T \mid S) \setminus L]\varphi \rightarrow [c][(l \cdot \overline{cc} \cdot \overline{a} \cdot R \mid T \mid S) \setminus L]\varphi + [l][[(R \mid v \cdot \overline{tc} \cdot \overline{r} \cdot T \mid S) \setminus L)]\varphi$

2. $[(l \cdot \overline{cc} \cdot \overline{a} \cdot R \mid T \mid S) \setminus L] \to [\tau][(\overline{cc} \cdot \overline{a} \cdot R \mid T \mid a \cdot S) \setminus L]\varphi + [t][(l \cdot \overline{cc} \cdot a \cdot R \mid v \cdot \overline{tc} \cdot \overline{r} \cdot T \mid S) \setminus L]\varphi$

3. $[R \mid v \cdot \overline{tc} \cdot \overline{r} \cdot T \mid S) \setminus L] \to [c][(l \cdot \overline{cc} \cdot a \cdot R \mid v \cdot \overline{tc} \cdot \overline{r} \cdot T \mid S) \setminus L]\varphi + [\tau][([R \mid \overline{tc} \cdot \overline{r} \cdot T \mid r \cdot S) \setminus L]\varphi$

4. $[l \cdot \overline{cc} \cdot a \cdot R \mid v \cdot \overline{tc} \cdot \overline{r} \cdot T \mid S) \setminus L]\varphi \to [\tau][(\overline{cc} \cdot \overline{a} \cdot R \mid v \cdot \overline{tc} \cdot \overline{r} \cdot T \mid a \cdot S) \setminus L]\varphi + [\tau][(l \cdot \overline{cc} \cdot \overline{a} \cdot R \mid \overline{tc} \cdot \overline{r} \cdot T \mid r \cdot S) \setminus L]\varphi$

5. $[\overline{cc} \cdot \overline{a} \cdot R \mid T \mid a \cdot S) \setminus L]\varphi \to [cc][(\overline{a} \cdot R \mid T \mid a \cdot S) \setminus L]\varphi + [t][(\overline{cc} \cdot \overline{a} \cdot R \mid v \cdot \overline{tc} \cdot \overline{r} \cdot T \mid a \cdot S) \setminus L]\varphi$

6. $[R \mid \overline{tc} \cdot \overline{r} \cdot T \mid r \cdot S) \setminus L]\varphi \to [c][(l \cdot \overline{cc} \cdot \overline{a} \cdot R \mid \overline{tc} \cdot \overline{r} \cdot T \mid r \cdot S) \setminus L]\varphi + [tc][[R \mid \overline{r} \cdot T \mid r \cdot S) \setminus L]\varphi$

7. $[\overline{cc} \cdot \overline{a} \cdot R \mid v \cdot \overline{tc} \cdot \overline{r} \cdot T \mid a \cdot S) \setminus L]\varphi \to [cc][(\overline{a} \cdot R \mid v \cdot \overline{tc} \cdot \overline{r} \cdot T \mid a \cdot S) \setminus L]\varphi$

8. $[l \cdot \overline{cc} \cdot \overline{a} \cdot R \mid \overline{tc} \cdot \overline{r} \cdot T \mid r \cdot S) \setminus L]\varphi \to [tc][(l \cdot \overline{cc} \cdot \overline{a} \cdot R \mid \overline{r} \cdot T \mid r \cdot S) \setminus L]\varphi$

9. $[\overline{a} \cdot R \mid T \mid a \cdot S) \setminus L]\varphi \to [\tau][((R \mid T \mid S) \setminus L]\varphi + [t][(\overline{a} \cdot R \mid v \cdot \overline{tc} \cdot \overline{r} \cdot T \mid a \cdot S) \setminus L]\varphi$

10. $[(R \mid \overline{r} \cdot T \mid r \cdot S) \setminus L]\varphi \to [\tau][((R \mid T \mid S) \setminus L]\varphi + [c][(l \cdot \overline{cc} \cdot \overline{a} \cdot R \mid \overline{r} \cdot T \mid r \cdot S) \setminus L]\varphi$

11. $[(\overline{a} \cdot R \mid v \cdot \overline{tc} \cdot \overline{r} \cdot T \mid a \cdot S) \setminus L]\varphi \to [\tau][(R \mid v \cdot \overline{tc} \cdot \overline{r} \cdot T \mid S) \setminus L]\varphi$

12. $[(l \cdot \overline{cc} \cdot \overline{a} \cdot R \mid \overline{r} \cdot T \mid r \cdot S) \setminus L]\varphi \to [\tau][(l \cdot \overline{cc} \cdot \overline{a} \cdot R \mid T \mid S) \setminus L]\varphi$

13. $(E_1.t.E_3.\tau.E_7.\overline{tc}.E_{11}.\tau.E_1)^*$

14. $(E_2.c.E_3.\tau.E_6.\overline{cc}.E_{10}.\tau.E_2)^*$

15. $(E_0.c.E_1.\tau.E_4.\overline{cc}.E_8.\tau.E_0)^*$

16. $(E_0.t.E_2.\tau.E_5.\overline{tc}.E_9.\tau.E_0)^*$

PROPRIEDADES:

1. $[c \cdot l \cdot cc \cdot \overline{a} \cdot 0]R$

2. $[t \cdot v \cdot tc \cdot \overline{r} \cdot 0]T$

3. $[\overline{v} \cdot r \cdot 0]S$

4. $[\overline{l} \cdot a \cdot 0]S$

5. $R \rightarrow [v][cc]C$

6. $T \rightarrow [r][tc]C$

7. $(\neg R \wedge \neg T) \rightarrow [c](R \wedge \neg T) \wedge [t](\neg R \wedge T)$

8. $(\neg R \wedge \neg T) \rightarrow [C]\langle K\rangle \top$

9. $(\neg R \wedge \neg T) \rightarrow [C](\neg R \wedge \neg T)$

10. $[c]\langle K\rangle \bot \wedge [c][\overline{cc}]R$ - a propriedade *liveness* acontece, pois sempre que um carro se aproxima do cruzamento, eventualmente ele cruza;

11. a propriedade *deadlock* não acontece, pois não é o caso do trem ficar esperando o carro passar;

12. $\neg([\overline{tc}]T \wedge [\overline{cc}]R)$ - a propriedade *safety* acontece, pois nunca é possível um trem e um carro atravessarem ao mesmo tempo.

Capítulo 5

Conclusão

Este trabalho apresenta resultados sobre a Lógica Dinâmica Proposicional para Programas CCS.

Apresentamos a linguagem e o sistema axiomático. Fornecemos as provas de Corretude e Completude para este sistema. Mostramos também alguns exemplos contendo propriedades da lógica apresentada e suas respectivas provas.

Provamos que a Lógica Dinâmica Proposicional para Programas CCS é completa com respeito a classe de modelos finitos LPD-CCS. Consequentemente, nossa lógica tem a propriedade de modelo finito e, portanto, toda fórmula ψ pode ser satisfeita em um estado de um modelo com no máximo $2^{|\psi|}$, onde $|\psi|$ é o número de símbolos de ψ.

Um procedimento simples de decisão para o problema de satisfabilidade de nossa lógica pode ser: Dada uma fórmula ψ, construimos todos os modelos Kripke com no máximo $2^{|\psi|}$ estados, verificando se eles pertencem a classe apropriada e testando de ψ é satisfeita em algum estado desse modelo. Existem aproximadamente $2^{2^{|\psi|}}$ modelos desse tipo. Além disso, este algoritmo estabelece um tempo exponencial duplo de limite superior para o problema da satisfabilidade de nossa lógica.

O problema de satisfabilidade para LPD é EXPTIME-completo [LAN04]. Isto

produz um tempo exponencial de limite inferior para o problema da satisfabilidade da nossa lógica.

Acreditamos que as contribuições deste trabalho se dão no sentido de combinar duas áreas de estudo: Álgebra de Processos e Lógica Dinâmica, chegando numa lógica que expressa todas as propriedades desejadas das duas áreas. A Lógica Dinâmica Proposicional para Programas CCS nos dá possibilidade de trabalhar com propriedades de programas através dos operadores do cálculo CCS.

Como desenvolvimento de futuros trabalhos gostaríamos de citar algumas linhas de pesquisa:

1. Investigar algumas extensões de LPD-CCS para uma LPD para programas π-calculus.

2. Estabelecer um resultado de complexidade preciso para o problema de satisfabilidade para LPD para Programas CCS.

3. Desenvolver um provador automático de teoremas.

4. Verificar formalmente um protocolo de comunicação utilizando LPD para Programas CCS.

Referências Bibliográficas

[BRV02] P. BLACKBURN, de M. RIJKE, and Y. VENEMA. *Modal Logic.* Cambridge University Press, Amsterdam, 2002.

[BV95] P. BLACKBURN and Y. VENEMA. Dynamic squares. *Journal Philosophical Logic*, 24:469–523, 1995.

[COS92] M. M. COSTA. *Introdução à Lógica Modal Aplicada à Computação.* Instituto de Informática da UFRGS, GRAMADO - RS, 1992.

[DHS83] A. PNUELI D. HAREL and J. STAVI. Propositional dynamic logic of nonregular programs. *J. Computer System Science*, 26:222–243, 1983.

[END72] H. B. ENDERTON. *A Mathematical Introduction Logic.* Academic Press, 1972.

[GS91] J. GROENENDIJK and M. STOKHOF. Dynamic predicate logic. *Linguistics and Philosophy*, 14:39–100, 1991.

[HAR84] DAVID HAREL. Dynamic logic. *Handbook of Philosophical Logic, in Gabbay and Guenthner, eds.*, pages 497–604, 1984.

[HC96] G. HUGHES and M. CRESSWEL. *A New Introduction to Modal Logic.* Routledge, London, 1996.

[LAN04] MARTIN LANGE. A lower complexity bound for propositional dynamic logic with intersection. *Institut fur Informatik, University of Munich*, pages 1–11, 2004.

[MIL89] R. MILNER. *Communication and Concurrency*. Prentice Hall International, London - Uk, 1989.

[PAR85] ROHIT PARIKH. The logic of games and its applications. *Annals of Discrete Mathematics*, 24:111–140, 1985.

[PEL87a] DAVID PELEG. Communication in concurrent dynamic logic. *Journal of Computer and System Sciences*, 35:23–58, 1987.

[PEL87b] DAVID PELEG. Concurrent dynamic logic. *Journal of the Association for Computing Machinery*, 34:450–479, 1987.

[PEL87c] DAVID PELEG. Concurrent program schemes and their logics. *Theorical Computer Science*, 55:1–45, 1987.

[SG98] V. B. SHEHTMAN and D. M. GABBAY. Products of modal logic, part 1. *L. J. of the IGPL- no. 01*, 6:73–146, 1998.

[STI94a] C. STIRLING. An introduction to modal and temporal logics for ccs. *Dept. of Computer Science - University of Edingurgh, UK*, pages 1–25, 1994.

[STI94b] C. STIRLING. Modal and temporal logics for processes. *Dept. of Computer Science - University of Edingurgh, UK*, 1994.

[VEN94] Y. VENEMA. A crash course in arrow logic. *Logic Group Preprint Series*, (107), 1994.

[VIS95] A. VISSER. Relational validity and dynamic predicate logic. *Utrecht Research Institute for Philosophy*, pages 1–8, 1995.