UMA LÓGICA MODAL BIDIMENSIONAL PARA REPRESENTAÇÃO DO CONHECIMENTO EM SISTEMAS DISTRIBUÍDOS MULTIAGENTES

Vania Costa

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. Eduard Hermann Haeusler, D.Sc.

Prof. Fábio Protti, D.Sc.

Prof. Marcelo Finger, Ph.D.

Profa. Sheila Regina Murgel Veloso, D.Sc.

RIO DE JANEIRO, RJ - BRASIL
DEZEMBRO DE 2002

COSTA, VANIA

Uma lógica modal bidimensional para representação do conhecimento em sistemas distribuídos multiagentes [Rio de Janeiro] 2002

VII, 100p. 29,7 cm (COPPE/UFRJ, D. Sc., Engenharia de Sistemas e Computação, 2002)

Tese - Universidade Federal do Rio de Janeiro, COPPE

1. Lógicas Epistêmicas
2. Lógicas Multidimensionais
3. Sistemas Distribuídos

I. COPPE/UFRJ II. Título (série)

Agradecimentos

Nenhum trabalho verdadeiramente digno é realizado por uma só pessoa. Portanto, quero expressar os meus mais sinceros agradecimentos a todos aqueles que de alguma forma contribuíram para a realização desta dissertação.

Aos meus familiares, principalmente as minhas irmãs Vanda Costa e Vanise Costa, agradeço pelo incentivo em todos os momentos difíceis que atravessamos no decorrer destes últimos anos.

Agradeço o apoio e o entusiasmo dos meus amigos, aqueles poucos amigos verdadeiros, que torcem sempre, e que desejam compartilhar as minhas vitórias.

Obrigada a todos os professores, funcionários e colegas da COPPE pela colaboração, pelo encorajamento e pela paciência ao longo de todo este aprendizado.

Especiais agradecimentos ao meu orientador, o professor Mário Benevides, pelas sugestões, correções e ensinamentos valiosos que permitiram a execução deste trabalho.

Finalmente, gostaria de agradecer aos meus mentores espirituais - os indivíduos que, apesar de invisíveis aos olhos, muito me ajudaram e seguem sempre comigo.

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

UMA LÓGICA MODAL BIDIMENSIONAL PARA REPRESENTAÇÃO DO CONHECIMENTO EM SISTEMAS DISTRIBUÍDOS MULTIAGENTES

Vania Costa

Dezembro/2002

Orientador: Mário Benevides

Programa: Engenharia de Sistemas e Computação

Fazemos uma nova abordagem do estudo do conhecimento como uma ferramenta para raciocinar sobre comunicação em sistemas distribuídos assíncronos. Elaboramos uma revisão do trabalho de Joseph Y. Halpern, Yoram Moses, Ronald Fagin e Moshe Y. Vardi sobre o uso da lógica modal para representar o conhecimento de agentes que se comunicam numa rede através de troca de mensagens. A maioria dos resultados do referido trabalho, principalmente a formalização das noções de *conhecimento mútuo* e *conhecimento comum*, são aplicados a sistemas síncronos, uma idealização dos sistemas distribuídos reais. Portanto, formalizar outros conceitos de conhecimento para ambientes assíncronos foi a motivação inicial desta tese. Exibimos um modelo para sistemas distribuídos assíncronos e discutimos os resultados de Prakash Panangaden e Kim Taylor: uma semântica formal para um tipo de conhecimento comum alcançável assincronamente, o chamado *conhecimento comum concorrente*. Contudo, até o momento nenhum sistema axiomático havia sido apresentado para a semântica de Panangaden & Taylor. Investigamos os resultados em lógicas modais multidimensionais, de Dov M. Gabbay e Valentin Shehtman, buscando um formalismo que permitisse tratar os diferentes níveis de conhecimento no modelo de sistemas distribuídos assíncronos que adotamos. Introduzimos, então, uma nova perspectiva dos conceitos de conhecimento individual, conhecimento iterativo e conhecimento em um grupo de agentes baseada no produto de lógicas modais, ou lógicas multidimensionais. Apresentamos uma lógica bidimensional de conhecimento para sistemas distribuídos assíncronos e definimos um sistema axiomático para esta lógica. Fornecemos também as provas de corretude e completude para a lógica bidimensional de conhecimento. Exemplos do uso da lógica bidimensional para modelar conhecimento comum concorrente são apresentados. Finalmente, extensões e futuros desenvolvimentos da semântica bidimensional de conhecimento são sugeridos.

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

A TWO-DIMENSIONAL MODAL LOGIC FOR KNOWLEDGE REPRESENTATION IN MULTI-AGENT DISTRIBUTED SYSTEMS

Vania Costa

December/2002

Advisor: Mário Benevides

Department: Computer Science

We propose a new approach for studying knowledge as a tool to reason about communication in asynchronous distributed systems. We elaborated a revision of Joseph Y. Halpern, Yoram Moses, Ronald Fagin and Moshe Y. Vardi's work on the use of modal logic to represent the agents' knowledge that communicate one another in a network through messages passing. Most of the results of the referred work, mainly the formalization of the notions of mutual knowledge and common knowledge, are applied to synchronous systems, a theoretical approach of distributed systems. Therefore, the initial motivation for this dissertation was to formalize other concepts of knowledge for asynchronous environments. We exhibited a model for distributed asynchronous systems and we discuss Prakash Panangaden and Kim Taylor's results: a formal semantics for a type of common knowledge reachable in asynchronous contexts, the so-called concurrent common knowledge. However, up to now no axiomatic system was defined for the semantics of Panangaden and Taylor. We investigated the results in multidimensional modal logics, of Dov M. Gabbay and Valentin Shehtman, looking for a formalism to treat the different knowledge levels in the model of asynchronous distributed systems that we adopted. We introduced a new perspective of the concepts of individual knowledge, interactive knowledge and agents' group knowledge based on the product of modal logics, or multidimensional logics. We presented a two-dimensional logic of knowledge for asynchronous distributed systems and we defined an axiomatic system for this logic. We also supplied the proofs of soundness and completeness for the two-dimensional logic of knowledge. Examples of the use of the two-dimensional logic to model concurrent common knowledge are presented. Finally, extensions and futures developments of the two-dimensional semantics of knowledge are suggested.

Conteúdo

Capítulo 1

Introdução

"... a faculdade de julgar com acerto e de discernir o verdadeiro do falso, que é propriamente o que se chama o bom senso ou a razão, é naturalmente igual em todos os homens; e, portanto, a diversidade de nossas opiniões não provêm de serem umas mais razoáveis do que as outras, mas somente de conduzirmos os nossos pensamentos por diversas vias e de não considerarmos as mesmas coisas."

R. Descartes, Discurso sobre o Método

1.1 Motivação

Uma das hipóteses mais aceitas na pesquisa em Inteligência Artificial (IA) é que a inteligência requer conhecimento e cognição. Segundo esta visão, a meta principal da IA seria o estudo da conceitualização do mundo e deveria começar com teorias a nível de conhecimento. Portanto, uma teoria em IA seria a especificação do conhecimento subjacente à cognição, isto é, ao mecanismo de controle da performance num sistema inteligente. Abrangeria o conhecimento necessário à execução de toda atividade sensitiva e informativa, tal como o uso da linguagem, resolução de problemas, decisões, percepção e algum tipo de atividade motora. Assim sendo, uma teoria em IA estrutura-se na teoria de representação do conhecimento subentendida. Na verdade, o interesse pelas teorias de conhecimento está presente em muitos outros campos da ciência, e remonta à época da Grécia antiga, quando os filósofos questionavam sobre o que realmente era possível conhecer, ou ainda, o que significa dizer que alguém sabe alguma coisa.

Neste trabalho, fazemos uma abordagem do estudo do conhecimento, ou epistemologia, como uma ferramenta para raciocinar sobre comunicação em

sistemas distribuídos multiagentes de troca de mensagens. Por sistema distribuído, entendemos um conjunto de processadores ou agentes, interligados através de uma rede de canais de comunicação. Para representar conhecimento neste ambiente utilizamos uma abordagem lógica. A contribuição principal desta tese, é uma lógica modal bidimensional para representar conhecimento de agentes neste tipo de ambiente distribuído de troca de mensagens.

Uma proposição p é de conhecimento mútuo ou de conhecimento de todos num grupo de agentes se cada agente conhece p. O conhecimento mútuo implica, simplesmente, no conhecimento que cada agente atribui a qualquer outro agente. Suponha, por exemplo, que cada participante de um congresso chega para uma conferência sabendo que o palestrante chegará atrasado. O fato de que o palestrante chegará atrasado é de conhecimento mútuo entre os participantes, mas cada participante pode pensar que somente ele próprio sabe disso. Contudo, se um dos participantes anuncia no auditório: "O professor palestrante me disse que chegará atrasado", então, supondo-se que o anunciante está dizendo a verdade, cada participante sabe agora que cada outro participante sabe que o palestrante chegará atrasado, e cada partipante sabe que cada participante sabe que cada participante sabe que o palestrante chegará atrasado, e assim por diante. Ou seja, a declaração do participante torna o fato que era mutuamente conhecido num fato de conhecimento comum.

O conhecimento comum é um fenômeno presente em muitas situações na nossa vida social. Para coordenar ações, estabelecer acordos, e em outros comportamentos típicos, os indivíduos necessitam de um conhecimento prévio ou da compreensão mútua ou ainda do conhecimento comum de certos fatos. Muitas vezes, quando uma interação em particular é mal sucedida, atribui-se a falha ao fato de que os agentes não tinham o conhecimento comum necessário que resultaria em sucesso. Se um casal se perde em um shopping, eles têm uma boa chance de se reencontrarem devido ao conhecimento comum prévio dos gostos e preferências mútuas, levando-os a procurarem um pelo outro nas lojas onde o outro gosta de frequentar. Num caso mal sucedido, um motorista pode causar um acidente ao cruzar o sinal vermelho, e tentar explicar ao guarda que cometeu a infração por não ter visto, ou seja, por não saber que o sinal estava vermelho, embora todos os outros motoristas o soubessem.

Apesar da importância do conhecimento comum nas interações sociais, é notável que só recentemente filósofos e cientistas tenham se voltado para a análise mais detalhada do conceito. O filósofo escocês David Hume (1711-1776) foi talvez o primeiro a fazer referência explícita ao papel do conhecimento mútuo em ações coordenadas. No seu "*A Treatise of Human Nature*"

(1740), Hume argumentava que a condição necessária para ações coordenadas era a de que todos os agentes conhecessem o comportamento esperado uns dos outros. Segundo Hume, sem esta condição as convenções sociais desapareceriam. Muito mais tarde, em 1953, o matemático John E. Littlewood (1885-1977) apresentou alguns exemplos do tipo de raciocínio usado no conhecimento comum. Na década de 60, os economistas Thomas Schelling (1921) e John Harsanyi (1920-2000) defenderam que algo como o conhecimento comum era necessário para explicar certas inferências que as pessoas fazem sobre as outras. Contudo, foi o filósofo David K. Lewis (1941-2001) quem primeiro forneceu uma análise explícita do conhecimento comum na monografia "*Convention*" (1969). Stephen Schiffer, Robert Aumann e Gilbert Harman, durante a década de 70, deram, independentemente, definições alternativas de conhecimento comum. John Barwise (1942-2000), em 1989, forneceu uma formulação precisa da descrição intuitiva de Harman. A análise de Shiffer do conhecimento comum como uma hierarquia de declarações epistêmicas se tornou um padrão na literatura. As descrições de Lewis, Aumann e Barwise todas implicam na abordagem hiérárquica de Schiffer.

A análise e as aplicações do conhecimento comum e conceitos relacionados de conhecimento em ambientes multiagentes tornou-se um campo de pesquisa muito ativo. Na década de 80, diversos trabalhos foram desenvolvidos no esforço de definir uma lógica formal que descrevesse o conhecimento de agentes que se comunicam através de troca de mensagens numa rede. Uma contribuição importante para a formalização da lógica do conhecimento deve-se a Joseph Y. Halpern, Yoram Moses e Ronald Fagin, em meados da década de 80, quando foram publicados os trabalhos "Knowledge and common knowledge in a distributed environment", em 84, revisto em 90 [17], e "A formal model of knowledge, action and communication in distributed systems: preliminary report" , em 85 [14], revisto em 89 [16]. Seguiram-se outros artigos nos anos seguintes e, finalmente em 95, uma compilação do trabalho da década foi publicado no livro "Reasoning About Knowledge" de R. Fagin, J. Y. Halpern, Y. Moses e M. Y. Vardi [20]. Os conceitos de conhecimento formalizados por Halpern et al. [20] são aplicados, principalmente, a sistemas síncronos, uma idealização dos sistemas distribuídos reais. Num sistema síncrono, os agentes têm uma base de tempo comum, um relógio global, que permite ações coordenadas simultâneas. A obtenção de conhecimento comum está, neste caso, vinculada a possibilidade de os agentes realizarem tais ações coordenadas simultâneas, e portanto só é alcançado em ambientes síncronos.

A nossa motivação inicial era a de estender, redefinir ou buscar outras perspectivas dos conceitos de conhecimento formalizados até então, a fim construir uma lógica para representar outros tipos de conhecimento que os agentes pudessem alcançar em um ambiente assíncrono de troca de mensa-

gens. Encontramos no *conhecimento comum concorrente* [31] a definição de um tipo de acordo alcançável em sistemas distribuídos assíncronos. Para ilustrar o conceito de conhecimento comum concorrente, suponha que estamos assistindo a partida final do Campeonato Mundial de Futebol, e o nosso país é um dos times que disputam o título. Todos os ouvintes estão desejosos de comemorar a vitória, e esperam o gol decisivo da partida. Podemos supor que existe uma pequena, porém perceptível, diferença de tempo na chegada das imagens nas televisões do país, ou seja, suponha que a imagem chega primeiro em alguns lugares e alguns segundos depois em outros. Logo que acontece o gol da vitória, alguns pontos do país já começam a festejar a conquista do título, sabendo que em todo o país, mais cedo ou mais tarde, todos saberão da vitória. Portanto, em cada lugar do país, todos sabem que, em algum momento mais cedo ou mais tarde, todos saberão da vitória, e todos sabem que todos estão cientes disso, e todos sabem que todos sabem e assim por diante. Neste caso, o conhecimento dos ouvintes sobre o gol da vitória não é simultâneo, porém todos sabem que em algum momento mais cedo ou mais tarde todos os outros tomaram ou tomarão conhecimento da conquista. Assim sendo, podemos dizer que vitória do time é de conhecimento comum concorrente entre todos os torcedores.

Com o objetivo de modelar o conhecimento alcançável em contextos assíncronos, como o *conhecimento comum concorrente*, buscamos outra semântica para definir conhecimento. Tomamos como ponto de partida o modelo de Lamport [25] de sistemas assíncronos que descreve um algoritmo distribuído do ponto de vista de execuções assíncronas e estados globais (ou cortes consistentes). Consideramos, então, uma abordagem onde os estados de conhecimento constituem um par execução-corte.

Para formalizar o conhecimento em estados representados por pares bidimensionais, utilizamos uma lógica modal multidimensional, neste caso, bidimensional. Nas lógicas modais multidimensionais os estados (ou mundos possíveis) são n-uplas, representando n dimensões onde as fórmulas lógicas são avaliadas. Intuitivamente, o que desejamos é que o conhecimento dos agentes seja avaliado num estado que se constitui no par ordenado (r, c), representando execuções assíncronas (*runs*) e estados globais (*consistent cuts*). A idéia de combinar lógicas não é uma novidade, na verdade é uma técnica naturalmente utilizada em lógicas aplicadas. Porém, só recentemente lógicos e outros pesquisadores da ciência da computação têm divulgado resultados neste sentido. A fundamentação da pesquisa em lógicas multidimensionais pode ser encontrada em Segerberg [32]. Uma referência importante nesta área tende a ser o livro "Many-dimensional modal logics: theory and applications" de D.Gabbay, A.Kurucz, F.Wolter e M.Zakharyaschev, que encontra-se, no momento, em fase final para publicação [11].

1.2 Organização da Tese

Esta tese está organizada da seguinte maneira:

- O capítulo 2 deste trabalho é uma revisão dos principais resultados obtidos em lógicas epistêmicas ou lógicas de conhecimento. Notadamente, discutimos os resultados de Halpern, Fagin, Moses e Vardi no que diz respeito à formalização do conhecimento de um grupo de agentes num sistema distribuído.

- No capítulo 3, apresentamos uma semântica para modelar conhecimento em sistemas distribuídos assíncronos com base nos conceitos de causalidade de eventos e estados globais [25]. Definimos o conhecimento em função do que chamamos de *visão passada* do agente. Utilizamos esta semântica para definir a comunicação e os estados de conhecimento dos agentes no sistema formal que estamos propondo. É importante lembrar que utilizamos indistintamente os termos processo, processador e agente. Além disso, adotamos o modelo de sistemas distribuídos assíncronos confiáveis, onde os canais são infalíveis, a ordem de processamento das mensagens é *fifo (first in first out)*, e o tempo de entrega é finito, embora indeterminado.

- Discutimos os resultados sobre comunicação em ambientes assíncronos de P. Panangaden e K. Taylor [31] no capítulo 4. Define-se aí uma semântica formal para um tipo de conhecimento alcançável em sistemas assíncronos, o *conhecimento comum concorrente*. Além disso, são apresentadas condições suficientes para alcançar conhecimento comum concorrente, e um algoritmo que garante a obtenção do mesmo.

- O capítulo 5 resume a investigação sobre o trabalho em lógicas modais multidimensionais. Abordamos somente os assuntos necessários para compreensão dos capítulos seguintes, mas a pesquisa nesta área é muito mais abrangente. Tomamos como base, principalmente, os resultados de Dov M. Gabbay e Valentin Shehtman [33].

- Nos capítulos restantes, ou seja, a partir do capítulo 6, encontra-se a nossa proposta para uma lógica que descreve o conhecimento em ambientes distribuídos multiagentes. No capítulo 6 introduzimos o conceito de *subproduto fechado de lógicas modais*, um sistema semântico polimodal bidimensional. Desenvolvemos o subproduto fechado de lógicas modais a partir do produto de lógicas modais, porém com duas inovações. Restringimos a avaliação das fórmulas a um subconjunto de pontos

introduzindo uma relação unária que determina o que chamamos de pontos ou pares admissíveis. Além disso, criamos uma relação adicional, a do fecho transitivo sobre as relações originais. Desta forma, definimos o conhecimento como uma propriedade *interdimensional*. Na interpretação para sistemas distribuídos, significa que o conhecimento é avaliado em todos os pares (r, c) (execuções e cortes consistentes) indistinguíveis sob o ponto de vista do agente. Apresentamos um exemplo para ilustrar esta interpretação.

- Propomos, ainda no capítulo 6, um sistema axiomático para a lógica bidimensional de conhecimento, o sistema $\mathcal{S}_m^2$. Na verdade, o sistema $\mathcal{S}_m^2$ pode ser visto como uma extensão do produto bidimensional de $S5_m$, acrescido de axiomas para o conhecimento definido como o fecho das relações básicas, e portanto, como uma propriedade bidimensional.

- O capítulo 7 contem as provas de corretude e completude para o sistema $\mathcal{S}_m^2$. Provamos que o sistema $\mathcal{S}_m^2$ possui a propriedade f.m.p. (*finite model property*) e, portanto, é decidível.

- No capítulo 8, introduzimos o sistema $\mathcal{C}_m^2$ para conhecimento comum concorrente. Propriedades como o *conhecimento mútuo concorrente* e o *conhecimento comum concorrente* são formalizadas. Provamos que o sistema $\mathcal{C}_m^2$ é correto e completo e apresentamos exemplos para ilustrar estados de conhecimento concorrente.

- Conclusões e propostas para futuros trabalhos são apresentadas no capítulo 9.

Capítulo 2

Lógicas de Conhecimento em um Grupo de Agentes

As lógicas epistêmicas, ou lógicas de conhecimento, visam descrever propriedades sobre o conhecimento de um grupo de agentes. Em particular, as lógicas modais de conhecimento descrevem como um agente raciocina sobre o mundo e sobre o conhecimento de outros agentes com os quais ele interage.

A aplicação de tais lógicas é bastante ampla, desde a Economia até a Inteligência Artificial. Estamos interessados, principalmente, na aplicação das lógicas modais de conhecimento a sistemas distribuídos, onde o *grupo de agentes* é representado por processadores infalíveis que se comunicam através de troca de mensagens numa rede com canais confiáveis.

A idéia intuitiva das lógicas de conhecimento, como de costume, é a mesma de outras lógicas modais, baseia-se numa semântica de mundos possíveis: "*A intuição é que se um agente não tem conhecimento completo sobre o mundo, ele vai considerar um número de mundos possíveis. Estes são seus candidatos para a maneira que o mundo realmente é.*" [20].

Diz-se que o agente conhece um fato p se p é verdade em todos os mundos que o agente considera possíveis. Com base neste conceito de conhecimento, os autores em [20] apresentaram um sistema semântico e o sistema axiomático correspondente $\mathcal{K}_m$, onde m representa o número de agentes, e o operador modal K_i representa o conhecimento que o agente i possui em relação aos mundos que ele considera possíveis.

Na verdade, o sistema $\mathcal{K}_m$ é o clássico sistema $\mathcal{K}$ da lógica modal proposicional, porém com m operadores modais, ou seja, é uma lógica polimodal proposicional com operadores K_i, onde $i = 1, \ldots, m$, representa o agente.

Assim como ocorre na lógica modal proposicional, também foram apresentadas em [20] extensões do sistema polimodal $\mathcal{K}_m$. Impondo-se restrições sobre a relação de possibilidade, originaram-se, então, os outros sistemas

polimodais proposicionais, a saber, $\mathcal{T}_m$, $\mathcal{S}4_m$ e $\mathcal{S}5_m$.

Discutimos brevemente a sintaxe e a semântica para as lógicas modais de conhecimento, o sistema $\mathcal{K}_m$ e suas respectivas extensões $\mathcal{T}_m$, $\mathcal{S}4_m$ e $\mathcal{S}5_m$.

Em seguida, introduzimos as noções de conhecimento num grupo de agentes, tais como o significa dizer que um fato é de conhecimento comum no grupo. Apresentamos, então, a semântica e o sistema axiomático $\mathcal{S}5_m^C$ para conhecimento em grupo.

Terminamos este capítulo analisando a relação existente entre comunicação num sistema distribuído e o conhecimento que pode ser adquirido pelos agentes. Reproduzimos uma série de exemplos de problemas conhecidos, tais como o *Problema do Ataque Coordenado* e o *Problema dos Maridos Infiéis*, a fim de avaliar os níveis de conhecimento que podem ser alcançados de acordo com a comunicação (síncrona ou assíncrona, canais confiáveis ou com falhas) estabelecida entre os agentes. Uma variação bastante conhecida do *Problema dos Maridos Infiéis* é o *Problema das Crianças com Lama na Testa*, porém, já que ambos os problemas ilustram as mesmas circunstâncias de comunicação, optamos pelo problema menos ingênuo.

2.1 Sintaxe para as Lógicas de Conhecimento

A linguagem das lógicas de conhecimento num grupo de m agentes é a mesma linguagem de uma lógica proposicional polimodal, com m operadores modais K_i, $i = 1, \ldots, m$. Neste caso, $K_i p$ é interpretado como "o agente i *conhece* o fato p".

As fórmulas bem formadas (f.b.f) da linguagem são definidas por indução, como de costume. Muitas vezes faremos referência às fórmulas bem formadas da linguagem simplesmente como *fórmulas.*

Definição 2.1.1 *Lógica L_m.*

Seja a lógica L_m o menor conjunto de fórmulas contendo o conjunto de primitivas Prop, fechado sob negação, conjunção e os operadores modais K_i, onde $i = 1, \ldots, m$.

Logo, se α e β são fórmulas da linguagem, então $\neg\alpha, (\alpha \wedge \beta)$ e $K_i\alpha$, para $i = 1, \ldots, m$, também são fórmulas.

Para simplificar a leitura, omitiremos os parênteses sempre que não houver dúvidas sobre o escopo das fórmulas. Além disso, utilizaremos as seguintes abreviaturas da lógica proposicional:

$\alpha \vee \beta$ para $\neg(\neg\alpha \wedge \neg\beta)$;

$\alpha \rightarrow \beta$ para $\neg\alpha \vee \beta$;

$\alpha \leftrightarrow \beta$ para $(\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha)$.

2.2 Semântica para as Lógicas de Conhecimento

Levando-se em conta que o conhecimento K_i de um agente i é definido a partir dos mundos que ele considera possíveis, a semântica utilizada é, naturalmente, a semântica proposicional de mundos possíveis de Kripke.

Definição 2.2.1 *Frame F.*
Um frame $F = (W, R_i)$ é uma estrutura relacional onde:

1. *W é o conjunto de estados ou mundos possíveis;*
2. *$R_i \subseteq W \times W$ é uma relação binária em W, dita relação de possibilidade, onde $i = 1, 2, \ldots, m$.*

Definição 2.2.2 *Modelo M.*
Um modelo M sobre $F = (W, R_i)$ é um par $M = (F, v)$, onde $v : Prop \rightarrow 2^W$ é uma função de atribuição de valores de verdade às primitivas de $Prop$. Para cada $p \in Prop$, $v(p)$ é o conjunto dos estados $w, w \in W$, onde p é verdadeira.

Definição 2.2.3 *Satisfazibilidade em L_m.*
Seja L_m a lógica com m operadores modais K_i, $i = 1, \ldots, m$. Uma fórmula $\alpha \in L_m$ é verdadeira em (M, w), $(M, w) \models \alpha$, quando:

1. *$(M, w) \models p \Leftrightarrow w \in v(p)$, onde $p \in Prop$;*
2. *$(M, w) \models \alpha \wedge \beta \Leftrightarrow (M, w) \models \alpha$ e $(M, w) \models \beta$;*
3. *$(M, w) \models \neg\alpha \Leftrightarrow (M, w) \not\models \alpha$;*
4. *$(M, w) \models K_i\alpha \Leftrightarrow \forall w'((wR_iw') \Rightarrow (M, w') \models \alpha)$.*

Dizemos que:

- *Uma fórmula α é satisfatível se existe um estado w e um modelo M tal que α é verdadeira em (M, w), $(M, w) \models \alpha$.*
- *Uma fórmula α é verdadeira em um modelo M, $M \models \alpha$, quando é verdadeira em todos os mundos de M.*
- *Uma fórmula α é válida num frame F, $F \models \alpha$, se é válida em todos os modelos sobre F.*
- *Uma fórmula α é válida numa classe de frames $\mathbf{F}$ se é válida em cada frame $F \in \mathbf{F}$.*

2.3 Sistemas Axiomáticos de Conhecimento

2.3.1 O Sistema Axiomático $\mathcal{K}_m$

Analogamente aos sistemas da lógica modal, o sistema básico para as lógicas polimodais de conhecimento é o sistema $\mathcal{K}_m$.

Definição 2.3.1 *Sistema $\mathcal{K}_m$ [20].*
Seja G o grupo de m agentes. O sistema $\mathcal{K}_m$ consiste de dois axiomas e três regras de inferência.
Axiomas:

A0 *Todas as tautologias do cálculo proposicional*

A1 $(K_i\alpha \wedge K_i(\alpha \rightarrow \beta)) \rightarrow K_i\beta$, *para todo* $i \in G$

Regras:

R0 *De* $\vdash \alpha$ *derive toda substituição uniforme de* α

R1 *De* $\vdash \alpha, \alpha \rightarrow \beta$ *derive* β *(modus ponens)*

R2 *De* $\vdash \alpha$ *derive* $K_i\alpha$, *para todo* $i \in G$ *(generalização do conhecimento)*

Teorema 2.3.2 *Corretude e Completude de $\mathcal{K}_m$ [20].*
Seja $\mathbf{F}_m$ a classe de todos os frames de Kripke para m agentes.
$\mathcal{K}_m$ é uma axiomatização correta e completa em relação a classe de frames $\mathbf{F}_m$.

A prova do teorema 2.3.2 pode ser encontrada em [20].

2.3.2 Outros Sistemas Axiomáticos de Conhecimento

A seguir apresentamos outros axiomas que caracterizam o conhecimento, conforme o tipo de restrição sobre as relações R_i.

A2 $K_i\alpha \rightarrow \alpha$, para todo $i \in G$

É conhecido como o *axioma do conhecimento* e expressa a idéia de que somente fatos verdadeiros são conhecidos pelos agentes.

A3 $K_i\alpha \rightarrow K_iK_i\alpha$, para todo $i \in G$

É dito o *axioma da introspecção positiva*, representando a propriedade de que o agente sabe que sabe α.

A4 $\neg K_i\alpha \rightarrow K_i\neg K_i\alpha$, para todo $i \in G$

É chamado o *axioma da introspecção negativa*, indicando que o agente sabe que não sabe α.

Os axiomas $A2$, $A3$ e $A4$ são válidos se as relações R_i forem, respectivamente, reflexivas, transitivas e euclidianas.

Assim sendo, com a adição destes axiomas, originam-se as extensões de $\mathcal{K}_m$, conforme a seguir:

- $\mathcal{T}_m$ é $\mathcal{K}_m$ acrescido do axioma $A2$.
- $\mathcal{S}4_m$ é $\mathcal{T}_m$ acrescido do axioma $A3$.
- $\mathcal{S}5_m$ é $\mathcal{S}4_m$ acrescido do axioma $A4$.

Teorema 2.3.3 *Corretude e Completude de $\mathcal{K}_m, \mathcal{T}_m, \mathcal{S}4_m$ e $\mathcal{S}5_m$ [20].*

Sejam $\mathbf{F}_m^r, \mathbf{F}_m^{rt}$ e $\mathbf{F}_m^{rts}$ as classes de frames para m agentes onde as relações de possibilidade são, respectivamente, reflexivas, reflexivas-transitivas e reflexivas-transitivas-simétricas.

1. *$\mathcal{T}_m$ é uma axiomatização correta e completa em relação a classe de frames $\mathbf{F}_m^r$.*
2. *$\mathcal{S}4_m$ é uma axiomatização correta e completa em relação a classe de frames $\mathbf{F}_m^{rt}$.*
3. *$\mathcal{S}5_m$ é uma axiomatização correta e completa em relação a classe de frames $\mathbf{F}_m^{rts}$.*

Uma prova do teorema 2.3.3 também pode ser encontrada em [20].

2.4 Estados de Conhecimento Relacionados ao Grupo de Agentes

Uma série de estados de conhecimento surgem naturalmente quando se pensa no grupo de agentes como um todo. Em sistemas multiagentes é importante, em muitas situações, analisar o que todos os agentes sabem em um determinado estado global do sistema. Por exemplo, se todos já sabem quem é o líder no grupo. Neste caso, dizemos que o líder é de conhecimento de todos ou de *conhecimento mútuo.*

Em outras situações, o conhecimento mútuo sobre um fato não é condição suficiente para certas ações. Pode ser necessário avaliar não somente o que

todo mundo sabe, mas também o que todo mundo sabe que todo mundo sabe. Neste caso, o agente precisa considerar não somente os fatos que são verdadeiros no estado corrente, mas também o conhecimento que os outros agentes no grupo têm sobre estes fatos. Diz-se que um fato é de *conhecimento comum* no grupo quando todo mundo sabe este fato, e todo mundo sabe que todo mundo sabe este fato, e além disso, todo mundo sabe que todo mundo sabe que todo mundo sabe, e assim sucessivamente. O conhecimento sobre as convenções entre todos os membros de uma comunidade é um exemplo de conhecimento comum, uma vez que, para todo fato convencionado, todo mundo sabe este fato, e todo mundo sabe que todo mundo sabe, e todo mundo sabe que todo mundo sabe que todo mundo sabe, e assim por diante.

Se o conhecimento comum é o que todo mundo sabe, e todo mundo sabe que todo mundo sabe, e assim sucessivamente, pode-se dizer que este tipo de conhecimento é o que qualquer pessoa comum possui. E, no entanto, do ponto de vista de comunicação num sistema distribuído, é o nível de conhecimento mais difícil de ser alcançado, conforme veremos.

Por outro lado, pode-se pensar no conhecimento obtido quando se une o conhecimento de todos os membros do grupo. Neste caso, diz-se que o grupo tem o *conhecimento distribuído* sobre um fato, ou seja, quando a união do conhecimento de todos permite deduzir este fato, mesmo que nenhum membro do grupo conheça tal fato individualmente. Contrariamente ao que é de conhecimento comum, o conhecimento distribuído poderia ser visto como o conhecimento de alguém que tudo sabe, digamos um mestre ou um sábio.

As contribuições mais interessantes e originais em [20] surgem na formalização para raciocinar sobre estes estados de conhecimento relacionados ao grupo de agentes. Para tanto, os autores acrescentaram à linguagem modal operadores de conhecimento em um grupo, tais como:

- D_G para o conhecimento distribuído;
- A_G para o conhecimento de alguém;
- E_G para o conhecimento mútuo;
- C_G para o conhecimento comum.

A seguir, encontra-se a semântica para alguns estados de conhecimento identificados num grupo de agentes, a saber, o conhecimento mútuo e o conhecimento comum sobre um determinado fato.

Definição 2.4.1 *Lógica* L_m^C.

Seja G *o grupo de* m *agentes. Considere* L_m^C *como sendo* L_m *com a adição dos operadores* E_G *e* C_G.

Logo, se α é uma fórmula de L_m^C, então $E_G\alpha$ e $C_G\alpha$ também são.

Definição 2.4.2 *Satisfazibilidade em L_m^C.*

Seja L_m^C a lógica com m operadores modais K_i, $i = 1, \ldots, m$, e os operadores E_G e C_G. Uma fórmula $\alpha \in L_m^C$ é verdadeira em (M, w), $(M, w) \models \alpha$, quando:

1. $(M, w) \models p \Leftrightarrow w \in v(p)$, *onde* $p \in Prop$;
2. $(M, w) \models \alpha \wedge \beta \Leftrightarrow (M, w) \models \alpha$ *e* $(M, w) \models \beta$;
3. $(M, w) \models \neg\alpha \Leftrightarrow (M, w) \not\models \alpha$;
4. $(M, w) \models K_i\alpha \Leftrightarrow \forall w'((wR_iw') \Rightarrow (M, w') \models \alpha)$;
5. $(M, w) \models E_G\alpha \Leftrightarrow \forall w'((wR_iw') \Rightarrow (M, w') \models K_i\alpha)$;
6. $(M, w) \models C_G\alpha \Leftrightarrow (M, w) \models E_G^k\alpha$ *para todo* $k \geq 1$. [1]

2.5 Sistemas Axiomáticos para Conhecimento em Grupo

Quaisquer dos sistemas $\mathcal{K}_m$, $\mathcal{T}_m$, $\mathcal{S}4_m$ ou $\mathcal{S}5_m$ podem ser estendidos a sistemas que refletem as propriedades dos estados de conhecimento no grupo de agentes. Sejam $\mathcal{K}_m^C$, $\mathcal{T}_m^C$, $\mathcal{S}4_m^C$ e $\mathcal{S}5_m^C$ respectivamente tais extensões com os axiomas e regras para conhecimento mútuo e conhecimento comum.

Em particular, apresentamos o sistema $\mathcal{S}5_m^C$, que é $\mathcal{S}5_m$ acrescido dos axiomas e regras para conhecimento no grupo.

Definição 2.5.1 *Sistema $\mathcal{S}5_m^C$.*

Seja G o grupo de m agentes. O sistema $\mathcal{S}5_m^C$, consiste de sete axiomas e quatro regras de inferência.

Axiomas:

A0 *Todas as tautologias do cálculo proposicional*

A1 $(K_i\alpha \wedge K_i(\alpha \rightarrow \beta)) \rightarrow K_i\beta$, *para todo* $i \in G$

A2 $K_i\alpha \rightarrow \alpha$, *para todo* $i \in G$

A3 $K_i\alpha \rightarrow K_iK_i\alpha$, *para todo* $i \in G$

[1] Para $k = 1$ $E_G^1\alpha = E_G\alpha$; para $k = 2$ $E_G^2\alpha = E_GE_G\alpha$; para $k = 3$ $E_G^3\alpha = E_GE_GE_G\alpha$; e assim por diante.

A4 $\neg K_i\alpha \rightarrow K_i\neg K_i\alpha$, *para todo* $i \in G$

A5 $E_G\alpha \leftrightarrow \bigwedge_{i\in G} K_i\alpha$

A6 $C_G\alpha \rightarrow E_G(\alpha \wedge C_G\alpha)$

Regras:

R0 *De* $\vdash \alpha$ *derive toda substituição uniforme de* α

R1 *De* $\vdash \alpha, \alpha \rightarrow \beta$ *derive* β *(modus ponens)*

R2 *De* $\vdash \alpha$ *derive* $K_i\alpha$, *para todo* $i \in G$ *(generalização do conhecimento)*

R3 *De* $\vdash \alpha \rightarrow E_G(\alpha \wedge \beta)$ *derive* $\alpha \rightarrow C_G\beta$ *(regra da indução)*

Teorema 2.5.2 *Corretude e Completude de* $\mathcal{K}_m^C$, $\mathcal{T}_m^C$, $\mathcal{S}4_m^C$ *e* $\mathcal{S}5_m^C$ *[20].*

- $\mathcal{K}_m^C$ *é uma axiomatização correta e completa em relação a classe de frames* $\mathbf{F}_m$.
- $\mathcal{T}_m^C$ *é uma axiomatização correta e completa em relação a classe de frames* $\mathbf{F}_m^r$.
- $\mathcal{S}4_m^C$ *é uma axiomatização correta e completa em relação a classe de frames* $\mathbf{F}_m^{rt}$.
- $\mathcal{S}5_m^C$ *é uma axiomatização correta e completa em relação a classe de frames* $\mathbf{F}_m^{rts}$.

Uma prova do teorema 2.3.3 é encontrada em [20].

2.6 Comunicação e Conhecimento em Ambientes Distribuídos

Segundo Halpern et al. [17], "*a comunicação num sistema distribuído pode ser vista como o ato de transformar o estado de conhecimento do sistema*". Assim sendo, a evolução da comunicação entre os agentes pode ser entendida como a ascensão numa hierarquia de estados de conhecimento, ou seja, como certos fatos verdadeiros passam de um estado de conhecimento distribuído até se tornar de conhecimento comum entre os agentes.

Nesta abordagem, de que a comunicação num sistema distribuído evolui segundo uma hierarquia de estados de conhecimento no grupo, é possível

identificar, através de uma análise da semântica dos operadores de conhecimento em grupo, esta exata hierarquia. Logo, se p é um fato verdadeiro, a seguinte hierarquia pode ser observada:

$C_G p \rightarrow E_G^k p \rightarrow E_G p \rightarrow A_G p \rightarrow D_G p \rightarrow p$

Neste caso, observa-se que o conhecimento comum sobre o fato p corresponde ao nível mais alto nesta hierarquia, o último estado a ser alcançado. No entanto, sob certas circunstâncias, o conhecimento comum sobre um fato pode não ser nunca alcançado, conforme ilustra o *Problema do Ataque Coordenado*, que discutiremos adiante.

Por outro lado, existem resultados supreendentes, tal como a relação existente entre conhecimento comum e sistemas síncronos: somente em sistemas síncronos, onde a comunicação entre os agentes permite ações simultâneas coordenadas, o conhecimento comum de certos fatos pode ser obtido durante uma execução. O *Problema dos Maridos Infiéis* será utilizado para ilustrar este resultado.

2.6.1 O Problema do Ataque Coordenado

Um resultado importante relacionado a comunicação num sistema distribuído e os estados de conhecimento atingíveis diz respeito ao tipo de canal de comunicação:

Se existem falhas nos canais de comunicação, então o conhecimento comum não é atingido.

Um problema que ilustra este resultado é conhecido como o *Problema do Ataque Coordenado*. A seguir temos uma descrição do mesmo.

> Suponha que duas divisões de um exército estão posicionadas respectivamente em dois topos de montanha a observar um inimigo que se encontra no vale. Sabe-se que, para vencer a batalha, as duas divisões devem atacar o inimigo simultaneamente. Como não havia planos para o ataque, o general da primeira divisão idealizou coordenar um ataque simultâneo em algum momento do dia seguinte. Neste caso, nenhum dos dois generais atacaria o inimigo sem a certeza de que o outro general também estaria atacando. A comunicação entre os generais é feita através de mensageiros que normalmente levam uma hora para sair de uma divisão e chegar a outra. No entanto, existe a possibilidade do mensageiro se perder na escuridão, ou, até mesmo, ser capturado pelo inimigo.

A pergunta é: *Quanto tempo será necessário para coordenar este ataque?*

Para responder a esta pergunta, façamos o seguinte raciocínio intuitivo. Considere que A representa o general da primeira divisão, e que B representa o outro general. Suponha que o general A envie ao general B a seguinte mensagem: "Atacar a meia noite". O general B não irá atacar visto que A não tem conhecimento de que B recebeu a mensagem. Desta forma, B envia um mensageiro que confirme que a mensagem foi recebida. Mais uma vez, A não irá atacar sem que seja confirmado a B que o seu mensageiro chegou com a mensagem. Seguindo este raciocínio, observa-se que sempre haverá a necessidade de uma confirmação. Logo, os generais nunca irão chegar a fazer um ataque simultâneo.

Teorema 2.6.1 *Conhecimento Comum e Falhas nos Canais. [17]*
Não existe um algoritmo para obter conhecimento comum se a comunicação não é garantida.

A prova deste teorema é encontrada em [17], porém outra versão mais elaborada do mesmo pode ser encontrada em [20]. Além disso, uma análise completa sobre a relação do conhecimento comum e o tipo de acordo que pode ser obtido em sistemas com falhas em processos (SBA - *Simultaneous Byzantine Agreement*) também é apresentada em [20].

2.6.2 Conhecimento Comum e Ações Coordenadas

Uma condição bem aceita, desde filósofos até pesquisadores da ciência da computação, é a de que *é a publicação de um fato que o torna de conhecimento comum no grupo.* De uma forma geral, existiriam duas formas de se publicar um fato:

1. O fato faz parte das convenções de uma comunidade. No contexto de sistemas distribuídos, as convenções entre os agentes corresponderiam às informações iniciais comuns, inseridas antes da execução do sistema.

2. O fato é anunciado de forma que todos os agentes estejam presentes. Em sistemas distribuídos, para simular a presença usando troca de mensagens, é preciso fazer com que os agentes tomem conhecimento do fato simultaneamente.

A simultaneidade é alcançada num sistema se existe um algoritmo que garanta que todos os membros do sistema vão executar uma ação coordenada simultaneamente. É demonstrado em [17], que a simultaneidade não pode ser alcançada em sistemas assíncronos, onde o tempo de entrega das mensagens é finito porém indeterminado.

Portanto, como a simultaneidade não pode ser alcançada em tais sistemas, não é possível a obtenção de conhecimento comum de um fato durante a execução de um algoritmo, conforme é apresentado nos dois lemas e no teorema a seguir.

Lema 2.6.2 *Conhecimento Comum e Simultaneidade [17].*
Se o conhecimento comum de um fato é alcançado durante uma execução, todos os agentes o fazem simultaneamente.

Lema 2.6.3 *Entrega de Mensagens e Simultaneidade [17].*
Se não há limite nos tempos de entrega das mensagens, então a simultaneidade não é alcançada.

Teorema 2.6.4 *Conhecimento Comum e a Entrega de Mensagens [17].*
Se a comunicação é garantida, mas não há limite nos tempos de entrega das mensagens, então não existe um algoritmo para alcançar conhecimento comum.

Estes resultados foram revistos e publicados em [20].

A partir deste resultado, verificamos que o tipo de comunição é essencial para determinar se o conhecimento comum das fórmulas pode ser alcançado. "*Uma fórmula que é de conhecimento comum em algum instante deve ser também de conhecimento comum no instante onde nenhuma mensagem foi entregue.*" [20]

Isto não implica, contudo, que nenhum fato jamais possa se tornar de conhecimento comum. Por exemplo, em sistemas síncronos, adota-se a hipótese de que os agentes têm acesso a um relógio global. Na verdade, a hipótese sobre a existência de um relógio global significa que o tempo é de conhecimento comum entre os agentes. Além disso, como os agentes podem realizar ações coordenadas, outros estados de conhecimento podem ser atingidos, possivelmente o conhecimento comum de fatos e fórmulas.

2.6.3 O Problema dos Maridos Infiéis

Para ilustrar a relação entre conhecimento e ações coordenadas, vamos apresentar o "*quebra-cabeça dos maridos infiéis*" e algumas de suas variações, de acordo com o tipo de canal de comunicação que está sendo considerado.

O objetivo é analisar o conhecimento que um agente pode obter apenas observando as ações tomadas por outros agentes, as quais se relacionam a um fato que é de conhecimento comum. A seguir, fornecemos a descrição do problema e alguns resultados em três situações distintas, a saber, para a comunicação síncrona, assíncrona, e com limite no tempo de entrega das mensagens.

Caso Síncrono

Em uma cidade chamada Mamajorca, as rainhas faziam campanha contra o problema da infidelidade masculina. Os fatos de conhecimento comum em Mamajorca eram:

1. As rainhas eram pessoas perfeitamente confiáveis.
2. As mulheres sempre obedeciam a rainha.
3. Todas as mulheres eram capazes de ouvir um tiro disparado em Mamajorca.

A rainha Henrieta I, a fim de acabar com a infidelidade masculina, chamou todas as mulheres casadas na praça da cidade e anunciou: "Existe no mínimo um marido infiel nesta cidade. Embora nenhuma de vocês antes desta reunião tenha o conhecimento se seu marido é ou não infiel, cada uma tem o conhecimento sobre a fidelidade dos outros maridos. Todas estão proibidas de discutir este assunto com qualquer outra pessoa. Contudo, se alguma de vocês concluir que seu próprio marido é infiel, esta deve atirar no mesmo à meia-noite do dia da descoberta". Após esta declaração, 39 noites se passaram, e na quadragésima noite, tiros foram ouvidos.

A pergunta é: *Quantos maridos infiéis haviam?*

Para raciocinar intuitivamente sobre o que ocorre, considere inicialmente a existência de apenas um marido infiel. Sua esposa após a leitura do documento, não conhecendo outro marido infiel conclui sobre a infidelidade de seu marido e atira na primeira noite. Ao considerar dois maridos infiéis, suas esposas têm o conhecimento de apenas um marido infiel e esperam ouvir um tiro na primeira noite. Como isto não acontece, elas concluem sobre a infidelidade de seus maridos e atiram na segunda noite. Baseando-se nestes argumentos, a conclusão do problema para um número k de maridos infiéis é:

Teorema 2.6.5 *Se existem k maridos infiéis, no instante em que a rainha leu o documento, então as esposas traídas atirarão em seus maridos na noite do k-ésimo dia.*

Uma prova deste teorema se dá por indução no número k de maridos infiéis.

1. Para $k = 1$, já foi visto que o teorema é válido.

2. Suponha a validade do teorema para $k = n$. Deseja-se provar a validade para $k = n + 1$. Assuma que existem $n + 1$ maridos infiéis. Logo, suas esposas tem o conhecimento de n maridos infiéis e esperam ouvir tiros na n-ésima noite. Como esta noite passou em silêncio, elas concluem a existência de mais um marido infiel, que seria seu próprio marido. Assim, por indução, na $(n + 1)$-ésima noite serão ouvidos $n + 1$ tiros.

Seja a proposição p : "Existe no mínimo um marido infiel na cidade." Na verdade, se existe mais de um marido infiel, este não é nenhum fato novo para as esposas na cidade, uma vez que cada uma delas conhece sobre a infidelidade dos maridos das outras. Porém, o anúncio da rainha torna este fato de conhecimento comum, o que permite que, a cada noite em silêncio, as esposas possam concluir ao mesmo tempo sobre a infidelidade de mais um marido.

Neste caso, o conhecimento comum é obtido de acordo com as ações das esposas: uma vez que a primeira noite passou-se em silêncio, foi adquirido o conhecimento comum de no mínimo dois maridos infiéis. Com a segunda noite de silêncio, torna-se de conhecimento comum a existência de no mínimo três maridos infiéis, e, ao continuar o processo, o conhecimento de k maridos infiéis é obtido após $k - 1$ noites em silêncio. O importante é que este conhecimento comum foi obtido sem nenhuma comunicação entre as esposas.

É interessante também observar que, antes do anúncio da rainha, $E_G^{k-1}p$ era verdade, enquanto que $E_G^k p$ não era. Para verificar isto, considere o caso de $k = 3$ maridos infiéis. Logo, cada esposa traída sabia exatamente sobre a infidelidade de 2 maridos infiéis, e sabia também que cada uma destas esposas traídas sabia sobre a infidelidade do marido da outra, o que torna $E_G^2 p$ verdade. Porém, quando o fato de que existe pelo menos um marido infiel na cidade é anunciado, tornam-se verdadeiras as fórmulas do tipo $E_G^k p$ para $k \geq 1$. Em particular, $E_G^3 p$ é suficiente para que cada uma das 3 esposas traídas possa concluir sobre a infidelidade do próprio marido. Na verdade, é possível demonstrar que para k esposas traídas, $E_G^k p$ é suficiente para garantir que cada esposa possa concluir sobre a infidelidade do próprio marido.

Caso Assíncrono

> Suponha que Henrieta II, sucessora de Henrieta I, para continuar combatendo o mesmo problema, implantou um sistema de correios para evitar a reunião na praça, garantindo que todas as cartas enviadas chegariam num tempo finito, porém indeterminado, em todas as casas de Mamajorca. A primeira carta tratava deste sistema de correios. A segunda carta enviada era uma cópia fiel do documento de Henrieta I.

Esta segunda idéia foi um fracasso, pois o sistema de correios implantado, no qual o tempo de entrega das mensagens é indeterminado, as esposas traídas não terão o conhecimento de que as outras esposas já receberam ou não a carta.

Teorema 2.6.6 *Se existe mais de um marido infiel, então, ao usar um canal assíncrono para a emissão das instruções, nenhum marido infiel sofrerá um tiro.*

Prova.

Quando existe um marido infiel, sua esposa, ao receber a carta, irá atirar a meia-noite do mesmo dia. O problema aparece no caso de $k > 1$ maridos infiéis. Neste caso, não haverá tiros porque as k esposas traídas imaginarão sempre que seus maridos são fiéis e que as $k - 1$ esposas traídas que elas conhecem ainda não receberam a carta da rainha. Sendo a carta da rainha de conhecimento comum eventual, uma esposa nunca poderá determinar se as noites em silêncio são resultantes da reação das outras esposas ao receber a carta ou do fato delas ainda não terem recebido a carta. Assim sendo, mesmo após $k-1$ noites em silêncio, não será possível concluir sobre k maridos infiéis, ou seja, o conhecimento comum sobre k maridos infiéis nunca será obtido.

Caso com Limite de Entrega nas Mensagens

> Para evitar os problemas de Henrieta II, Henrieta III melhora o sistema de correios de modo que seja de conhecimento comum que qualquer carta enviada pela rainha chega a casa de suas súditas em, no máximo, um dia. Assim, a primeira carta enviada tratava desta melhoria e a segunda era uma cópia fiel do documento de Henrieta I.

Proposição 2.6.7 *No caso com limite de entrega de d dias, uma esposa que conhece k maridos infiéis terá o conhecimento de que seu próprio marido é infiel se kd noites em silêncio se passarem após o dia no qual ela recebeu a carta da rainha.*

Apesar desta idéia ser mais eficiente que a anterior, ela não chegou a ser tão boa quanto a idéia inicial. Continuavam ocorrendo injustiças. Por exemplo, considere duas esposas a_1 e a_2 e $d = 2$. Suponha que a_1 tem o conhecimento de que o marido de a_2 é infiel, e que a_1 recebeu a carta na segunda-feira. À meia-noite de terça-feira a_2 atirou em seu marido. Devido a ausência de um calendário, a_1 não pode concluir sobre a fidelidade de seu marido, pois existem duas possibilidades:

1. O marido de a_1 é fiel e a_2 recebeu a carta na terça-feira e, não conhecendo outro marido infiel, atirou em seu marido.

2. O marido de a_1 é infiel, a_2 recebeu a carta no domingo e espera domingo e segunda para ouvir um tiro de a_1, mas como não aconteceu, concluiu que seu marido era infiel e atirou na noite de terça-feira.

Teorema 2.6.8 *Considere como o primeiro dia significativo o dia em que uma esposa traída recebe a carta. As esposas traídas que receberam a carta da rainha no primeiro dia significativo atirarão em seus maridos* $(k-1)d$ *dias após esse dia, onde* k *é o número de maridos infiéis. Todas as outras esposas permanecerão na dúvida quanto a fidelidade de seus maridos.*

A solução para as injustiças ocorridas é apresentada na proposição e no teorema a seguir.

Proposição 2.6.9 *Num sistema com limite de entrega de* d *dias, se toda esposa esperar* n *dias a partir do dia em que ela descobre sobre a infidelidade de seu marido, então a esposa que tem o conhecimento de* k *maridos infiéis saberá que seu próprio marido é infiel se* $k(d+n)$ *noites silenciosas passarem a partir do dia em que ela recebeu a carta.*

Teorema 2.6.10 *Se a espera é longa o suficiente, ou seja,* $n = d-1$, *então a esposa traída atira em seu marido sem deixar dúvidas quanto ao problema da infidelidade.*

Com base nesses resultados, verifica-se o conhecimento comum exige sempre alguma espécie de sincronismo para ser alcançado.

Outros conceitos de conhecimento comum alcançáveis em sistemas distribuídos foram definidos, tal como o ϵ-conhecimento comum [17] [20], e o conhecimento comum concorrente [31]. Estamos interessados particularmente neste último, o conhecimento comum concorrente, uma vez que constitui um tipo de conhecimento comum alcançável em sistemas distribuídos assíncronos.

Capítulo 3

Conhecimento em Sistemas Distribuídos Assíncronos

Apresentamos uma semântica para sistemas distribuídos assíncronos baseada nas noções de ordenação de eventos e estados globais. Esta semântica utiliza o modelo introduzido por Lamport [25] que tornou-se um padrão na área de sistemas distribuídos para tratar de tempo em ambientes assíncronos.

Dado o modelo para sistemas assíncronos, definimos uma interpretação de conhecimento dos agentes: o conhecimento é dado pelo que chamamos de *visão passada do agente*, isto é, todos os eventos que aconteceram até o momento para este agente. A interpretação considera os estados de conhecimento indistinguíveis sob o ponto de vista do agente, ou seja, todos os cortes consistentes onde o agente sabe as mesmas coisas, neste caso, onde ele tem a mesma visão passada. Com esta interpretação de conhecimento é possível também analisar a evolução da comunicação entre os agentes, identificando que estados de conhecimento em grupo podem ser alcançados.

3.1 Modelo para Sistemas Distribuídos Assíncronos

Antes de apresentar o modelo para sistemas distribuídos assíncronos propriamente dito, introduzimos alguns conceitos básicos.

Definição 3.1.1 *Sistema Distribuído de Troca de Mensagens.*

"Um sistema distribuído é uma coleção finita de processadores conectados por uma rede de comunicação. A comunicação é alcançada através do envio de mensagens ao longo de canais da rede." [16]

Definição 3.1.2 *Algoritmo Distribuído.*

Um algoritmo distribuído é um protocolo que especifica as ações de cada agente quando do recebimento de uma mensagem.

"Um protocolo determina que mensagens podem ser enviadas como função do estado interno do processador. Mesmo quando o protocolo é determinístico, o sistema pode se comportar não-deterministicamente, devido a incertezas nos tempos de entrega das mensagens e a possíveis falhas na entrega." [20]

Definição 3.1.3 *Sistema Distribuído Síncrono.*

"Um sistema distribuído síncrono é aquele em que todos os processadores do sistema funcionam segundo um relógio global comum, a que todos têm acesso. Uma característica normalmente associada a sistemas distribuídos síncronos diz respeito ao tempo para que uma mensagem enviada por um nó a um de seus vizinhos seja entregue: se o sistema é síncrono, uma mensagem enviada no início de um ciclo (ou passo) do relógio global chega ao seu destino (um vizinho de sua origem) antes do início do próximo ciclo. Sistemas distribuídos síncronos constituem apenas uma abstração teórica, não existem na prática."

Definição 3.1.4 *Sistema Distribuído Assíncrono.*

"Sistemas distribuídos reais são sistemas assíncronos, isto é, sistemas cuja principal característica é a ausência completa de uma base de tempo comum a todos os processadores que o compõem. Além disso, sistemas assíncronos são geralmente modelados de tal forma que mensagens sofram atrasos finitos, porém indeterminados, durante seu trânsito entre dois vizinhos no sistema."

Doravante, as definições são relativas à *sistemas distribuídos assíncronos*, onde não existe a noção de tempo global, a comunicação é garantida, e o tempo de entrega das mensagens é finito porém indeterminado.

Definição 3.1.5 *Evento.*

Os eventos refletem a troca de mensagens entre os agentes. O evento é o elemento básico nas definições de tempo para sistemas assíncronos.

Um evento pode ser definido como uma tupla $e = [a_i, t_i, s_i, s'_i, M, \mathcal{M}]$, *onde:*

1. a_i - *agente i para o qual ocorre o evento e*
2. t_i - *tempo local do agente i em que ocorre o evento e*
3. s_i - *estado local do agente i que antecede o evento e*

4. s_i' - *estado local do agente i que sucede o evento e*

5. M - *mensagem recebida pelo agente i associada ao evento e (pode não ser definida para o agente inicial)*

6. $\mathcal{M}$ - *mensagens enviadas pelo agente i em decorrência do evento e*

Definição 3.1.6 *Execução de um Algoritmo.*
Dado um algoritmo distribuído assíncrono $\mathcal{A}$, cada execução $r(\mathcal{A})$ é um conjunto $E_{r(\mathcal{A})}$ de eventos que descrevem uma computação distribuída deste algoritmo.

Definição 3.1.7 *Ação de um Agente.*
Uma ação é vista como um transformador de estados. É uma função de estados locais em estados locais.
Seja M uma mensagem. Embora ações internas aos processadores também sejam possíveis, consideramos somente dois tipos de ações:

1. $send_i^j(M)$ - *o agente i envia a mensagem M ao agente j;*

2. $receive_i^j(M)$ - *o agente i recebe a mensagem M de um agente $j \neq i$.*

A seguir fornecemos o modelo para sistemas distribuídos assíncronos que será usado em todos os exemplos de aplicação no restante deste trabalho.

Definição 3.1.8 *Modelo de Sistema Assíncrono.*
Dado um algoritmo distribuído $\mathcal{A}$, considere o seguinte sistema para computar $\mathcal{A}$:

1. *Uma rede com m agentes infalíveis ($m \geq 2$), conectados por canais* fifo *confiáveis;*

2. *Um conjunto R de execuções assíncronas de $\mathcal{A}$;*

3. *Um conjunto E de eventos em todas as execuções de $\mathcal{A}$;*

4. *Um conjunto C de cortes consistentes (definição 3.1.13) em todas as execuções de $\mathcal{A}$.*

Neste modelo, uma execução r de um algoritmo distribuído $\mathcal{A}$ é ilustrada por um *grafo de precedência de eventos.* Considere o diagrama da figura 3.1 como uma possível execução do algoritmo distribuído PIF (*propagation of information with feedback*) [2] para três agentes.

A finalidade do algoritmo PIF é tornar uma mensagem M conhecida de todos os agentes do sistema e, supondo que apenas um único agente inicia o algoritmo, informar esse agente quando M já tiver atingido todos os outros.

A seguir, uma descrição do algoritmo PIF.

Algoritmo de Propagação de Informação com Realimentação

1. Regra para o iniciador:

   Envie M para todos os vizinhos e, ao receber de todos os vizinhos, conclua que todos os outros já receberam M.

2. Regra para os outros agentes

   Ao receber M pela primeira vez, seja a_k este vizinho que enviou M pela primeira vez; envie M a todos os vizinhos exceto a_k;

   Ao ter recebido M de todos os vizinhos, envie M a a_k.

Cada vértice no grafo de precedência da figura 3.1 representa um evento, quando os agentes enviam a mensagem M a um ou mais de seus vizinhos, e as setas orientadas representam a ordem em que os eventos ocorreram.

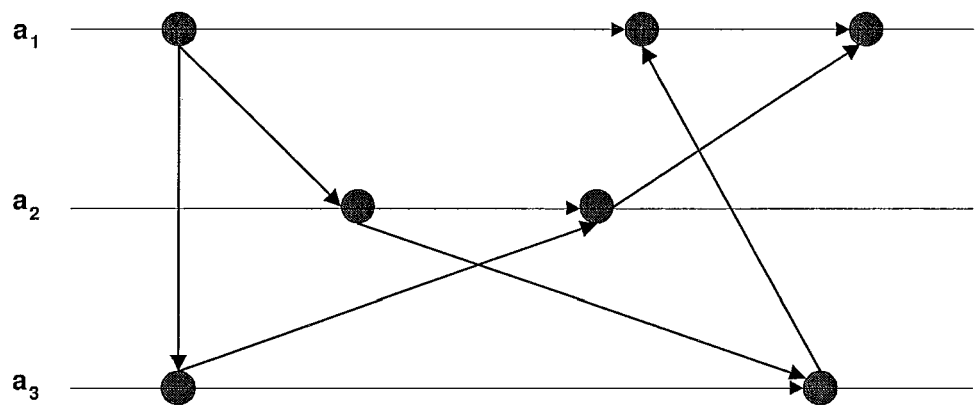

Figura 3.1: Algoritmo PIF com 3 Agentes - Grafo de Precedência de Eventos

Assim sendo, podemos falar de tempo em termos de relações de causalidade entre os eventos. Considere as seguintes relações:

1. A relação binária denotada por $\rightarrow$ cujo significado intuitivo é *aconteceu imediatamente antes*, ou seja, para dois eventos e e e', a notação $e \rightarrow e'$ é lida como "e aconteceu imediatamente antes de e'";

2. A relação binária $\rightarrow^+$ interpretada como *aconteceu antes*; representamos $e \rightarrow^+ e'$ quando e aconteceu antes de e'.

Definição 3.1.9 *Relações de Causalidade entre Eventos.*
Dados e, e', sejam as seguintes relações de causalidade:

- *e aconteceu imediatamente antes de e', $e \rightarrow e'$, se e somente se uma das duas condições ocorre:*

  1. *e, e' ocorreram para o mesmo agente i e, para os instantes $t_i < t'_i$, não existe nenhum outro evento e'' ocorrendo para i num instante t''_i tal que $t_i < t''_i < t'_i$;*
  2. *e, e' ocorreram para agentes distintos i e j, e a mensagem recebida por j no evento e' foi enviada por i no evento e, ou seja, $e = [a_i, t_i, s_i, s'_i, M_e, \mathcal{M}_e]$, $e' = [a_j, t_j, s_j, s'_j, M_{e'}, \mathcal{M}_{e'}]$, $M_{e'} \in \mathcal{M}_e$.*

- *e aconteceu antes de e', $e \rightarrow^+ e'$, se a relação $\rightarrow^+$ é o fecho transitivo da relação $\rightarrow$, ou seja, quando ocorre uma das duas condições:*

  1. $e \rightarrow e'$
  2. $\exists e_1, \ldots, e_k$ *para algum* $k > 0$ *tais que* $e \rightarrow e_1, \ldots, e_{k-1} \rightarrow e_k \rightarrow e'$.

Observe que a relação *aconteceu antes* ($\rightarrow^+$) é irreflexiva e transitiva, logo, é uma ordem parcial sobre os eventos.

A relação *aconteceu antes*, pode ser utilizada para definir o passado e o futuro de um evento em uma execução

Definição 3.1.10 *Passado e Futuro de Eventos.*
Seja $E_{r(\mathcal{A})}$ o conjunto de eventos de uma execução $r(\mathcal{A})$. Define-se o passado e o futuro de $e \in E_{r(\mathcal{A})}$ como:
Passado(e) $= \{e' \in E_{r(\mathcal{A})} | e' \rightarrow^+ e\}$;
Futuro (e) $= \{e' \in E_{r(\mathcal{A})} | e \rightarrow^+ e'\}$.

Considere $E_{r(\mathcal{A})}$ o conjunto de eventos de uma execução $r(\mathcal{A})$. A figura 3.2 é uma representação dos conjuntos $\rightarrow$, $\rightarrow_+$ e $E_{r(\mathcal{A})} \times E_{r(\mathcal{A})}$.

A relação *aconteceu antes*, também pode ser utilizada para definir eventos concorrentes.

Definição 3.1.11 *Concorrência de Eventos.*
Dois eventos e, e' são concorrentes se e somente se e não aconteceu antes de e' e e' não aconteceu antes de e, ou seja:
$\neg(e' \rightarrow^+ e) \wedge \neg(e \rightarrow^+ e')$.

Definição 3.1.12 *Estado do Sistema.*
Um estado do sistema é definido por:

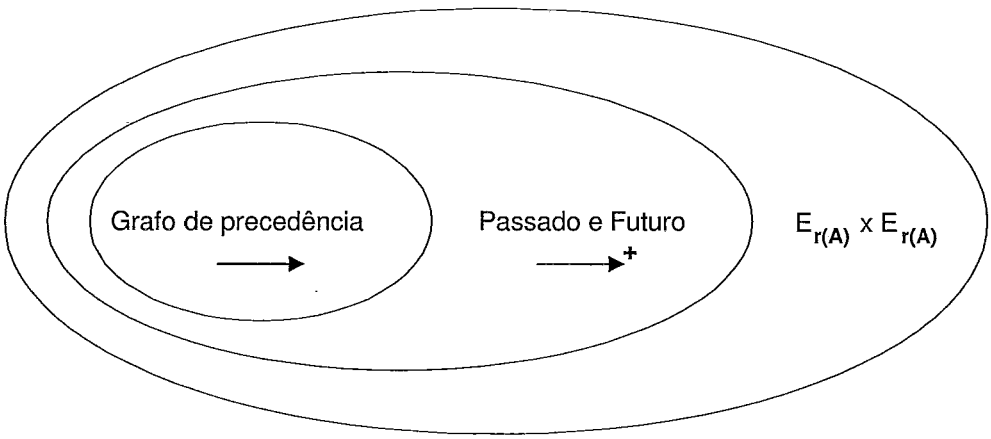

Figura 3.2: Relação entre Conjuntos de Eventos

1. *Para cada agente i, o estado local de i;*

2. *Para cada par (i, j), um conjunto de mensagens representando as mensagens em trânsito do agente i para o agente j.*

Nem todo estado do sistema é consistente com a ordem de entrega de mensagens entre os agentes. Intuitivamente, um *estado global* é um estado do sistema que "faz sentido", refletindo o estado local de cada agente, o conjunto de mensagens em trânsito, e onde *não existem mensagens do futuro para o passado.*

Definição 3.1.13 *Corte Consistente.*

Seja $E_{r(\mathcal{A})}$ o conjunto de eventos da execução $r(\mathcal{A})$. Um estado global ou corte consistente c em $r(\mathcal{A})$ é representado por uma partição de $E_{r(\mathcal{A})}$ em dois conjuntos E_P e E_F tais que:

se $e \in E_P$ então Passado(e) $\subseteq E_P$.

Um corte consistente c também pode ser definido em relação aos eventos no futuro:

se $e \in E_F$ então Futuro(e) $\subseteq E_F$.

Logo, um corte consistente divide o grafo de eventos em dois conjuntos de eventos, E_P e E_F, ditos, respectivamente, passado e futuro em relação ao corte c.

O grafo da figura 3.3 ilustra duas partições ou dois estados do sistema, sendo que apenas um deles é um estado global.

Outra forma de definir um estado global é considerar uma ordem total dos eventos de $E_{r(\mathcal{A})}$, representada por $\rightarrow^t$, consistente com uma ordem parcial

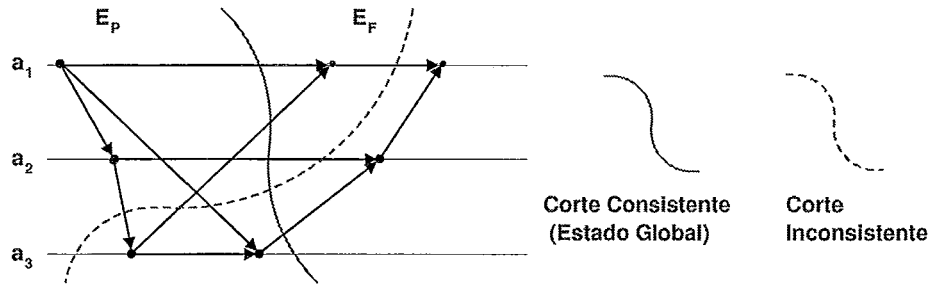

Figura 3.3: Corte Consistente

da relação *aconteceu antes*. Logo, uma ordem total $\rightarrow^t$ é uma trajetória orientada envolvendo todos os eventos de $E_{r(\mathcal{A})}$, onde $\rightarrow^t$ não contraria $\rightarrow^+$ e, para todo e, $e' \in E_{r(\mathcal{A})}$ ou $e \rightarrow^t e'$ ou $e' \rightarrow^t e$.

Desta forma, dada uma ordem total $\rightarrow^t$ consistente com $\rightarrow^+$, existem $|E_{r(\mathcal{A})}| + 1$ estados de sistema, cada um deles estabelecendo uma partição que divide $E_{r(\mathcal{A})}$ em dois conjuntos E_P e E_F, tal que $e \rightarrow^+ e'$ para todo $e \in E_P$ e $e' \in E_F$.

Definição 3.1.14 *Estado Global e Ordem Total de Eventos.*

Um estado de sistema é um estado global se e somente se existe uma ordem total $\rightarrow^t$ consistente com $\rightarrow^+$, tal que aquele estado de sistema é um dos $|E_{r(\mathcal{A})}| + 1$ estados dados por $\rightarrow^t$.

3.2 Interpretação do Conhecimento em Sistemas Assíncronos

As interpretações epistêmicas ou de conhecimento descritas em [17] e [20] referem-se a um par (r, t) onde t é um instante de tempo numa execução r, ou seja, são interpretações para sistemas síncronos onde existe uma base de tempo comum entre os agentes.

Entretanto, desejamos definir o que é uma interpretação do conhecimento no contexto do modelo para sistemas distribuídos assíncronos da seção 3.1, isto é, o que seria o conhecimento dos agentes nos possíveis estados globais do sistema.

Existem diferentes maneiras de definir uma interpretação epistêmica ou de conhecimento para um agente num determinado estado global. Uma das formas é fazer do conhecimento do agente uma função do seu estado local. Na interpretação baseada no estado local, se é possível a um agente chegar a

um estado através de duas histórias diferentes, então não é possível distinguir estas duas histórias passadas.

Como queremos que o agente não esqueça os fatos passados, podemos dizer que o conhecimento de um agente em um determinado corte consistente do sistema é caracterizado pela sua *visão passada*. Intuitivamente, dizemos que a *visão passada* de um agente em relação ao corte considerado é o conjunto de eventos que aconteceram para ele no seu passado, até o corte atual.

Definição 3.2.1 *Visão Passada do Agente em Relação a um Corte.*

Dado um corte consistente c representado pela partição E_P e E_F , a visão passada do agente i em relação ao corte c é o conjunto de eventos que ocorreram para o agente i em E_P, ou seja:

$V_P(i, c) = \{e_i | e_i \in E_P\}$

Definição 3.2.2 *Visão Futura do Agente em Relação a um Corte.*

Dado um corte consistente c representado pela partição E_P e E_F, a visão futura do agente i em relação ao corte c é o conjunto de eventos que ocorreram para o agente i em E_F, ou seja:

$V_F(i, c) = \{e_i | e_i \in E_F\}$

O estado local de um agente, bem como sua visão passada ou visão futura em relação a um corte podem ser usados para definir o que se entende como conhecimento do agente. Utilizamos o conhecimento baseado na visão passada do agente i em relação a um corte c como o conhecimento que queremos associar ao operador de conhecimento K_i na lógica que apresentamos.

Definição 3.2.3 *Interpretação de Conhecimento do Agente Baseado na Visão Passada.*

Dado um estado global atual do sistema, um agente considera como estados possíveis todos os outros estados globais onde ele tem a mesma visão passada que no estado global atual.

Seja α uma fórmula bem formada. Um agente conhece α se, em todos os estados onde ele tem a mesma visão passada, esta implica na veracidade de α.

No conhecimento baseado na visão passada, o agente não esquece os fatos que já ocorreram em sua história. Assim sendo, dizemos que o agente tem *perfect recall*, ou seja, ele não esquece o que já sabia, tudo que aconteceu sob o seu ponto de vista. Neste caso, o agente não esquece os fatos, mas a ordem em que eles ocorreram não importa. Para considerar a ordem que os eventos ocorreram, bastaria tomar a história local de eventos, ou seja, a sequência de eventos que ocorreram para o agente até o corte considerado.

Considerando a definição 3.2.3 para conhecimento do agente, observamos que, quando um agente tem a mesma visão passada em dois cortes distintos, ele terá o conhecimento dos mesmos fatos nos dois pontos [1]. Neste caso, dizemos que ambos os cortes são indistinguíveis do ponto de vista do agente.

3.3 Semântica para Sistemas Distribuídos Assíncronos

Como de costume, utilizamos uma semântica baseada em estruturas de Kripke para representar o conhecimento dos agentes no modelo de sistemas distribuídos assíncronos adotado.

Neste caso, consideramos:

1. Os estados ou mundos possíveis como pares (r, c), representando um corte c numa execução assíncrona r;

2. Os fatos básicos do sistema são as primitivas;

3. A função de atribuição de valores-verdade é uma função que preserva o conhecimento dos agentes, ou seja, o que o agente conhece é função do conjunto de eventos da sua visão passada em relação ao estado atual.

4. A relação de possibilidade é uma relação de equivalência refletindo a indistinguibilidade dos cortes do ponto de vista do agente: para um agente i, um estado (r', c') é indistinguível em relação ao estado atual (r, c), se e somente se a visão passada do agente i é a mesma em c e c', ou seja, $V_P(i, c) = V_P(i, c')$.

Considere a sintaxe para uma lógica polimodal de conhecimento como na seção 2.1, onde o operador K_i representa o conhecimento do agente i. A semântica para lógicas de conhecimento em sistemas assíncronos onde os estados são pares (r, c) é redefinida como segue.

Definição 3.3.1 *Satisfazibilidade em L_m.*

Seja L_m a lógica com m operadores modais K_i, $i = 1, \ldots, m$. Uma fórmula $\alpha \in L_m$ é verdadeira em $[M, (r, c)]$, $[M, (r, c)] \models \alpha$, quando:

1. $[M, (r, c)] \models p \Leftrightarrow (r, c) \in v(p)$, *onde* $p \in Prop$;

2. $[M, (r, c)] \models \alpha \wedge \beta \Leftrightarrow [M, (r, c)] \models \alpha$ *e* $[M, (r, c)] \models \beta$;

[1] Veja exemplo da seção 6.4

3. $[M,(r,c)] \models \neg\alpha \Leftrightarrow [M,(r,c)] \not\models \alpha$;

4. $[M,(r,c)] \models K_i\alpha \Leftrightarrow \forall(r',c')((r,c)R_i(r',c') \Rightarrow [M,(r',c')] \models \alpha)$.

Esta é a semântica básica que, doravante, utilizaremos para representar o conhecimento dos agentes num ambiente distribuído assíncrono.

Capítulo 4

Conhecimento Comum Concorrente

Como foi visto anteriormente, o conhecimento comum requer ações simultâneas e, portanto, não pode ser alcançado em sistemas assíncronos. Portanto, um dos nossos objetivos é o de investigar outros tipos de conhecimento em grupo que possam de fato ser atingidos em ambientes assíncronos.

O conceito de *conhecimento comum concorrente* definido em [31] é o correspondente em sistemas assíncronos ao conhecimento comum, ou seja, é um tipo de acordo alcançável em ambientes reais, onde não existe uma base de tempo comum ou um relógio global. Uma das aplicações importantes do conhecimento comum concorrente refere-se à execução das chamadas *ações distribuídas ou concorrentes*: ações executadas após um corte consistente. Assim como ocorre na relação existente entre ações simultâneas e o conhecimento comum para sistemas síncronos, demonstra-se em [31] que o conhecimento comum concorrente é uma condição necessária e suficiente para executar *ações concorrentes*.

O modelo de sistemas assíncronos utilizado por Panangaden et al. [31] é o mesmo apresentado no capítulo 3. A idéia de tempo é descrita em termos de relações de causalidade entre eventos e possíveis estados globais consistentes com estas relações. Neste caso, o agente considera indistinguíveis todos os estados globais que incluem o seu estado local. Assim sendo, a semântica captura a estrutura essencial de sistemas puramente assíncronos.

4.1 Semântica para Conhecimento Comum Concorrente

A relação de indistinguibilidade em [31] associa ao conhecimento do agente o seu estado local atual: "*Dois cortes são indistinguíveis para um processo i se eles contém o mesmo estado local para o processo i*". Logo, em qualquer estado da história de um processo i, i não pode determinar qual dos possíveis cortes consistentes incluindo seu estado atual é o estado global atual.

Para tratar de conhecimento do grupo num primeiro nível de acordo, é preciso definir o que seria o análogo ao conhecimento mútuo do sistema síncrono, ou seja, o que significa dizer que todos têm *conhecimento mútuo concorrente* de um fato. Informalmente, Panangaden et al. dizem que "*todo mundo concorrentemente sabe que uma fórmula é verdadeira se todos os agentes sabem que ela é verdadeira em algum estado global possível (ou corte consistente) indistinguível*". A intuição é a de que todos os agentes sabem que em algum momento mais cedo ou mais tarde naquela execução o fato se torna verdadeiro (veja o exemplo do Campeonato de Futebol apresentado no capítulo introdutório desta dissertação).

Uma semântica formal para a lógica de conhecimento comum concorrente foi definida em [31], embora nenhum sistema axiomático tenha sido apresentado. Na verdade, a sintaxe e semântica utilizadas são, essencialmente, as mesmas já vistas anteriormente, na seção 3.3, porém com a adição de operadores modais para conhecimento comum concorrente.

Seja G o grupo de m processadores. A seguir, apresentamos o significado de cada operador na lógica para conhecimento comum concorrente [31]:

- $K_i\alpha$ representa "o processo i conhece α", ou seja, α é verdade em todos os possíveis estados globais que incluem o estado local de i.
- $P_i\alpha$ representa "existe algum estado global consistente *na mesma execução* que inclui o estado local de i, no qual α é verdade".
- $E_C\alpha$ representa o "conhecimento mútuo concorrente de α". $E_C\alpha$ é dado por: $E_C\alpha = \bigwedge K_iP_i\alpha, i \in G$
- $C_C\alpha$ representa "α é de conhecimento comum concorrente".

O conhecimento comum concorrente implica que "todo mundo concorrentemente sabe, e todo mundo concorrentemente sabe que todo mundo concorrentemente sabe", e assim por diante. Ou seja:

$C_C\alpha \rightarrow E_C\alpha \wedge E_C^2\alpha \wedge E_C^3\alpha \wedge \ldots$

A seguir, introduzimos a semântica formal para o *conhecimento comum concorrente.*

Seja $v : Prop \rightarrow 2^W$ a função de atribuição de valores de verdade às primitivas do conjunto $Prop$, conforme discutida anteriormente. Ou seja, para cada $p \in Prop$, $v(p)$ é o conjunto dos estados $w, w \in W$, onde p é verdadeira.

Considere $\sim_i$ a relação de indistinguibilidade entre dois estados (r, c) e (r', c') sob o ponto de vista de um agente i.

Definição 4.1.1 *Satisfazibilidade em* $\mathcal{L}_m^C$.

Seja $\mathcal{L}_m^C$ *a lógica com m operadores modais* K_i, $i = 1, \ldots, m$, *e os operadores para conhecimento comum concorrente* P_i, E_C *e* C_C. *Uma fórmula* $\alpha \in \mathcal{L}_m^C$ *é verdadeira em* $[M, (r, c)]$, $[M, (r, c)] \models \alpha$, *quando:*

1. $[M, (r, c)] \models p \Leftrightarrow (r, c) \in v(p)$, *onde* $p \in Prop$;
2. $[M, (r, c)] \models \alpha \wedge \beta \Leftrightarrow [M, (r, c)] \models \alpha$ *e* $[M, (r, c)] \models \beta$;
3. $[M, (r, c)] \models \neg\alpha \Leftrightarrow [M, (r, c)] \not\models \alpha$;
4. $[M, (r, c)] \models K_i\alpha \Leftrightarrow \forall(r', c')((r, c) \sim_i (r', c') \Rightarrow [M, (r', c')] \models \alpha)$;
5. $[M, (r, c)] \models P_i\alpha \Leftrightarrow \exists(r, c')((r, c) \sim_i (r, c')$ *e* $[M, (r, c')] \models \alpha)$;
6. $[M, (r, c)] \models E_C\alpha \Leftrightarrow [M, (r, c)] \models K_iP_i\alpha$;
7. $[M, (r, c)] \models C_C\alpha \Leftrightarrow [M, (r, c)] \models E_C^k\alpha$ *para todo* $k \geq 1$. [1]

Observa-se que, na lógica para conhecimento comum concorrente, os estados de conhecimento do grupo são definidos no contexto de sistemas puramente assíncronos, ou seja, as fórmulas são avaliadas em um corte consistente de uma execução assíncrona. Além disso, existe um operador adicional, o operador P_i, cuja função é semelhante a de uma modalidade temporal, e que poderia ser traduzido como *mais cedo ou mais tarde num corte consistente daquela execução.* Desta forma, qualquer aplicação onde os processos precisam chegar a um acordo sobre uma propriedade de um estado global consistente do sistema podem ser entendidas em termos de conhecimento comum concorrente.

[1] Para $k = 1$ $E_C^1\alpha = E_C\alpha$; para $k = 2$ $E_C^2\alpha = E_CE_C\alpha$; para $k = 3$ $E_C^3\alpha = E_CE_CE_C\alpha$; e assim por diante.

4.2 Conhecimento Comum Concorrente e Ponto Fixo

Analogamente à caracterização de conhecimento comum em termos de ponto fixo [20], é apresentada em [31] uma semântica para definir o conhecimento comum concorrente usando ponto fixo.

Intuitivamente, a idéia é mostrar que o conhecimento comum concorrente pode ser pensado como uma situação em que todos os agentes concorrentemente sabem que a situação é verdadeira e é de conhecimento comum concorrente. Ou seja, o conhecimento comum concorrente é definido como o maior ponto fixo da equação $X = E_C(\alpha \wedge X)$.

Para definir o significado das fórmulas foi introduzida uma variável proposicional X à linguagem. Além disso, define-se para cada fórmula na linguagem estendida uma função que mapeia conjuntos de estados em conjuntos de estados , conforme a seguir.

Definição 4.2.1 *Conhecimento Comum Concorrente e Ponto Fixo.*

Seja W o conjunto de cortes consistentes de todas as execuções de um algoritmo A num sistema distribuído assíncrono. Seja Z um subconjunto de W. O significado de uma fórmula é dado indutivamente pela seguinte função $\int$:

1. $\int[p](Z) = \{(r,c) \in Z | (r,c) \in v(p)\}$, *onde* $p \in Prop$
2. $\int[\neg\phi](Z) = W - \int[\phi](Z)$
3. $\int[\phi \wedge \psi](Z) = \int[\phi](Z) \cap \int[\psi](Z)$
4. $\int[X](Z) = Z$
5. $\int[K_i\phi](Z) = \{(r,c) \in W \mid \forall(r',c') \in W((r',c') \sim_i (r,c) \Rightarrow (r',c') \in \int[\phi](Z))\}$
6. $\int[P_i\phi](Z) = \{(r,c) \in W \mid \exists(r,c') \in W((r,c') \sim_i (r,c) \wedge (r,c') \in \int[\phi](Z))\}$

Se uma fórmula não possui variável livre, então seu significado é uma função constante. Neste caso, o valor de verdade da semântica é recuperado definindo:

$[M,(r,c)] \models \phi \Leftrightarrow (r,c) \in \int[\phi](\emptyset)$.

Para garantir a monotonicidade de $\int[\phi](Z)$, as ocorrências da variável livre X em ϕ devem ser positivas, isto é, devem estar no escopo de um número par de sinais de negação.

Assim sendo, define-se o maior ponto fixo, $\nu X.\phi$, como:
$\int[\nu X.\phi](Z) = \bigcup\{B \mid \int[\phi](B) = B\}$
E o conhecimento comum concorrente, $C_C\phi$, é visto como um caso especial da equação acima, como segue:
$C_C\phi = \nu X.E_C(\phi \wedge X)$
É demonstrado em [31] que a regra de indução para o conhecimento comum concorrente é correta em relação à semântica definida, conforme assegura o seguinte teorema.

Teorema 4.2.2 *Se* $M \models \phi \Rightarrow E_C(\phi \wedge \psi)$ *então* $M \models \phi \Rightarrow C_C(\psi)$.

Logo, a semântica apresentada define o conhecimento comum concorrente em termos de ponto fixo, conforme desejado, e garante que:
$C_C\phi \Leftrightarrow E_C(\phi \wedge C_C\phi)$.

4.3 Obtenção de Conhecimento Comum Concorrente

O objetivo aqui é mostrar que, assim como existe um resultado em [20] dizendo que, se o conhecimento comum é alcançado, todos os agentes o fazem simultaneamente, para o conhecimento comum concorrente vale um teorema análogo. Além disso, uma condição geral suficiente para que o conhecimento comum concorrente seja alcançado no sistema é apresentada.

Para tanto, é importante a noção do que significa um processo *atingir* ou *alcançar* uma fórmula. Intuitivamente, diz-se que um processo i atinge uma fórmula ϕ num determinado corte de uma execução do sistema se o seu estado local implica que i sabe ϕ e que no *passado*, i não sabia ϕ.

Demonstra-se em [31] que, se o $C_C\phi$ é alcançado em uma execução, então todos os processos aprendem $P_iC_C\phi$ ao longo de um corte consistente.

Teorema 4.3.1 *Se o* $C_C\phi$ *é atingido na execução* r*, então o conjunto de estados locais nos quais os processos aprendem* $P_iC_C\phi$ *forma um corte consistente em* r *[31].*

Este teorema é importante na medida em que traça um paralelo entre o conhecimento comum e o conhecimento comum concorrente. Se, por um lado, em sistemas assíncronos ações simultâneas de qualquer tipo são impossíveis, por outro lado, é possível executar *ações concorrentes* que ocorrem ao longo de um corte consistente, onde as pré-condições destas ações são de conhecimento comum concorrente entre os agentes.

Outro resultado importante em [31] diz respeito à condição suficiente para obter $C_G\phi$. Para tanto, define-se o conjunto τ de *cortes localmente distinguíveis*: "A fim de alcançar $C_G\phi$, é suficiente que o sistema possua um conjunto τ de cortes, pelo menos um por execução, com a seguinte propriedade: quando um estado local de qualquer processo está em um corte de τ em alguma execução, então o mesmo estado local deste processo está em algum corte de τ em toda execução na qual ele ocorre" [31]. Intuitivamente, a idéia é que o processo sabe que o seu estado local é um elemento de um dos cortes de τ.

Definição 4.3.2 *Corte Localmente Distinguível.*

Um conjunto τ de cortes de um sistema é localmente distinguível se:

$\forall r \exists c((r,c) \in \tau)$ *e*

$[\forall i = 1, \ldots, m, \forall (r,c) \in \tau \forall (r',c')$

$((r',c') \sim_i (r,c) \Rightarrow (\exists d((r',d) \in \tau \text{ e } (r',d) \sim_i (r,c)))]$

Para melhor compreender esta definição, sugere-se considerar uma fórmula $in\tau$ tal que $[M,(r,c)] \models in\tau \Leftrightarrow (r,c) \in \tau$. Assim sendo, a segunda condição acima para um conjunto de cortes localmente distinguível é simplesmente:

$in\tau \rightarrow E_G(in\tau)$

O teorema a seguir estabelece que, qualquer sistema que possua um conjunto de cortes locamente distinguível onde ϕ é verdadeira, alcança conhecimento comum concorrente de ϕ.

Teorema 4.3.3 *Condição para Obtenção de Conhecimento Comum Concorrente [31].*

Se um sistema tem um conjunto τ de cortes localmente distinguíveis tal que:

$\forall (r,c) \in \tau \; [M,(r,c)] \models \phi$ *então*

$\forall (r,c) \in \tau \; [M,(r,c)] \models C_G\phi$.

A prova deste teorema encontra-se em [31].

4.4 Algoritmo para Conhecimento Comum Concorrente

Em [31] são apresentados dois algoritmos para obtenção de conhecimento comum concorrente: o primeiro requer que os canais sejam *fifo*, o segundo não possui esta restrição. Como o modelo de sistemas assíncronos que adotamos supõe canais *fifo*, vamos reproduzir aqui somente o primeiro algoritmo,

que utilizaremos mais tarde nos exemplos de aplicações para conhecimento comum concorrente.

Antes porém, algumas observações são feitas a respeito dos fatos que podem tornar-se de conhecimento comum concorrente em um sistema assíncrono. O requisito fundamental para que um fato possa tornar-se de conhecimento comum concorrente é que este seja um fato *localmente controlável*, conforme as definições a seguir.

Definição 4.4.1 *Fato Local.*
Um fato ϕ é local a um agente i num modelo M se:
$M \models \phi \rightarrow K_i\phi$

Definição 4.4.2 *Fato Localmente Controlável.*
Um fato ϕ é localmente controlável se, toda vez que o agente i sabe ϕ em qualquer estado do sistema, i pode evitar que ϕ torne-se falso para qualquer número finito de eventos.

Segundo Panangaden et al., "Qualquer fato que torne-se conhecido por algum processo e seja localmente controlável por este processo pode tornar-se de conhecimento comum concorrente entre todos os processos" [31].

Um fato *estável*, aquele que uma vez verdadeiro permanece sempre verdadeiro, é outro exemplo de um fato que torna-se de conhecimento comum concorrente entre todos os agentes. Por isso, propriedades globais estáveis, tais como *deadlock* e terminação global de um algoritmo distribuído, são candidatas a serem descritas em termos de conhecimento comum concorrente.

Para a descrição seguinte do algoritmo de obtenção de conhecimento comum concorrente, considere que a expressão *estado de corte* refere-se ao estado local de um determinado processo no corte atual.

Algoritmo para Obter Conhecimento Comum Concorrente

1. O iniciador I, em algum ponto em sua história local onde I conhece ϕ, manda a mensagem $send_I^j(\phi)$ para todo vizinho j, e, imediatamente, alcança seu estado de corte. Depois de mandar a primeira mensagem e até alcançar seu estado de corte, I não recebe mensagens, e evita que ϕ seja falsificado.

2. Todos os outros processos i, ao receberem a mensagem $send_j^i(\phi)$ pela primeira vez, mandam a mensagem $send_i^k(\phi)$ para todos os vizinhos $k \neq j$, ou seja, exceto aquele vizinho do qual receberam a mensagem pela primeira vez, e , imediatamente, alcançam seu estado de corte. Depois de mandar a primeira mensagem e até alcançar seu estado de corte, i não recebe mensagens.

É demonstrado em [31] que, se um sistema assíncrono com canais *fifo* confiáveis, no qual ϕ é um fato localmente controlável por um dos agentes, implementa o algoritmo acima, então todos os agentes alcançam conhecimento comum concorrente de ϕ.

Discute-se também em [31] a relação existente entre o conhecimento comum concorrente e as chamadas *ações concorrentes* - ações que são executadas imediatamente após um corte consistente. Demonstra-se que o conhecimento comum concorrente de certas pré-condições é uma condição necessária e suficiente para que ações concorrentes possam ser executadas num algoritmo distribuído.

Esta relação entre o conhecimento comum concorrente e ações concorrentes é importante devido à predominância de tais ações em sistemas distribuídos assíncronos. Por exemplo, ações concorrentes são executadas em algoritmos para gravar *checkpoints*, algoritmos para recuperação de bancos de dados, em algoritmos para gravar *snapshots* para detecção de propriedades globais, entre outros. Na verdade, uma nova análise do algoritmo para *snapshots* de Chandy-Lamport utilizando o conceito de conhecimento comum concorrente é desenvolvida em [31].

Capítulo 5

Lógicas Modais Multidimensionais

Muitos formalismos modais são usados para raciocinar sobre tempo, conhecimento, crenças, ações e espaço independentemente. Contudo o que se verifica na prática é que todas estas entidades existem em interação íntima: conhecimento, crenças e regiões do espaço podem mudar com o passar do tempo e de acordo com certas ações; agentes em um sistema multiagente podem ter suas próprias bases de conhecimento que são atualizadas ao longo do tempo, e assim sucessivamente. O intuito é poder combinar, por exemplo, lógicas epistêmicas, temporais, e outras a fim de obter uma lógica apropriada para descrever as propriedades de todas as entidades envolvidas.

Acreditamos que o motivo pelo qual não foi apresentado um sistema de axiomas para a lógica de conhecimento comum concorrente em [31] reside no fato da semântica definida ser insuficiente para avaliar as fórmulas no contexto do par (r, c) - representando o corte consistente c na execução assíncrona r. Propomos que o par (r, c) seja interpretado sob uma ótica bidimensional, como uma composição de dois contextos ou dimensões originais - uma dimensão de execuções assíncronas e outra de cortes consistentes - onde as propriedades em cada uma destas dimensões podem ser avaliadas em separado. Por isso, propomos utilizar uma lógica bidimensional para modelar conhecimento em ambientes assíncronos.

Neste capítulo discutiremos as lógicas multidimensionais: uma técnica que combina duas ou mais lógicas a fim de capturar as interações entre as diversas entidades, resultando num formalismo que, muitas vezes, aumenta o poder expressivo das lógicas isoladas. Abordamos, particularmente, as lógicas modais multidimensionais, discutimos os conceitos de *fusões de lógicas modais* e de *produto de lógicas modais*. Além disso, reproduzimos alguns resultados importantes acerca de como axiomatizar este produto [33].

5.1 Fusões

A formação de fusões, ou junções independentes, é talvez o mais simples e freqüente método usado para combinar lógicas.

Definição 5.1.1 *Fusão de Lógicas Modais.*
Seja L_1 uma lógica n-modal, L_2 uma lógica m-modal. Sua fusão é a lógica $n+m-$modal $L_1 \oplus L_2 = \mathcal{K}_{n+m} + L_1 + L_2^{+n}$, onde L_2^{+n} corresponde ao conjunto das fórmulas $n+m-$modais obtidas das fórmulas de L_2 substituindo-se o operador modal $\Box_j$ de L_2 por $\Box_{j+n}$.

Nenhum axioma que contenha os operadores modais de ambas as linguagens é requerido para axiomatizar a fusão de L_1 e L_2, ou seja, os operadores modais permanecem independentes.

A formação de fusões é uma operação binária associativa sobre lógicas, portanto, pode-se definir a fusão de n lógicas de um modo direto, para qualquer número natural $n \geq 2$. Por exemplo, temos:
$\mathcal{K}_m = \mathcal{K} \oplus \mathcal{K} \oplus \ldots \oplus \mathcal{K}$ (m vezes);
$\mathcal{S}5_m = \mathcal{S}5 \oplus \mathcal{S}5 \oplus \ldots \oplus \mathcal{S}5$ (m vezes);
e assim por diante.

Portanto, as lógicas epistêmicas $\mathcal{K}_m$ e suas respectivas extensões $\mathcal{T}_m$, $\mathcal{S}4_m$ e $\mathcal{S}5_m$ discutidas no capítulo 2 são, na realidade, fusões de lógicas modais.

Fusões de lógicas tem sido estudadas durante um tempo relativamente longo. O primeiro resultado explícito sobre fusões foi obtido por Thomason (1980), que provou que fusões de lógicas modais consistentes são extensões conservativas de seus componentes. Resultados adicionais que mostram que muitas propriedades importantes das lógicas são preservadas sob fusões foram obtidos por Kracht e Wolter [36], Finger e Gabbay [10], Wolter [37], entre outros.

As fusões de lógicas modais têm também uma interpretação semântica muito natural, pelo menos para lógicas que são Kripke completas. Considere duas classes $\mathbf{F}_1$ e $\mathbf{F}_2$ de m- e n-frames, respectivamente, fechadas sob uniões disjuntas e cópias isomórficas. A fusão $\mathbf{F}_1 \oplus \mathbf{F}_2$ é a classe de todos os n + m-frames da forma:
$(W, R_1 ..., R_m, S_1, ..., S_n)$ tal que $(W, R_1 ..., R_m) \in \mathbf{F}_1$ e $(W, S_1, ..., S_n) \in \mathbf{F}_2$.

Assim, $\mathbf{F}_1 \oplus \mathbf{F}_2$ consiste de combinações arbitrárias de frames de $\mathbf{F}_1$ e $\mathbf{F}_2$ que compartilham o mesmo conjunto de mundos. Claramente, se $\mathbf{F}_1$ e $\mathbf{F}_2$ determinam lógicas L_1 e L_2, respectivamente, então todos os frames em $\mathbf{F}_1 \oplus \mathbf{F}_2$ validam a fusão $L_1 \oplus L_2$. Porém, não é trivial provar o inverso, ou seja, que $\mathbf{F}_1 \oplus \mathbf{F}_2$ caracteriza $L_1 \oplus L_2$.

Um teorema importante sobre preservação de propriedades em fusões de lógicas diz que a fusão de duas lógicas decidíveis é também decidível. No entanto, este resultado é válido para fusões de lógicas modais proposicionais, mas não vale quando combinamos, por exemplo, lógicas de primeira ordem [11].

Em geral, as seguintes propriedades são transferidas das lógicas para suas fusões:

- Kripke completude
- f.m.p.
- decidibilidade
- interpolação uniforme

5.2 Produto de Lógicas Modais

Do ponto de vista semântico, as fusões não modificam a *dimensão* das lógicas: os mundos ou estados nos frames continuam sendo vistos como pontos sem nenhuma *característica multidimensional*. A formação de produtos cartesianos de diversas estruturas é uma maneira padrão de fazer uma abordagem multidimensional do mundo. Portanto, nada mais natural do que pensar no produto cartesiano de lógicas modais para capturar os aspectos multidimensionais da interação de operadores modais.

"*Lógicas modais multidimensionais correspondem ao produto de frames de Kripke.*" [33]

Definição 5.2.1 *Produto de Frames.*

Sejam L_1 e L_2 lógicas proposicionais polimodais com m operadores. Considere $F_1 = (W_1, R_i)$ e $F_2 = (W_2, R_j)$ dois frames proposicionais para L_1 e L_2, respectivamente. O produto dos frames é o frame $F_1 \times F_2 = (W_1 \times W_2, R_i^h, R_j^v))$, onde:

$R_i^h = \{((x,z),(y,z))|xR_iy\}$;

$R_j^v = \{((z,x),(z,y))|xR_jy\}$.

O frame $F_1 \times F_2$ é dito frame-produto.

Naturalmente, esta definição pode ser estendida para o produto de n lógicas modais.

Os subscritos h e v remetem a intuição de considerarmos R_i^h como sendo a relação de acessibilidade horizontal e R_j^v a relação vertical de acessibilidade no frame-produto.

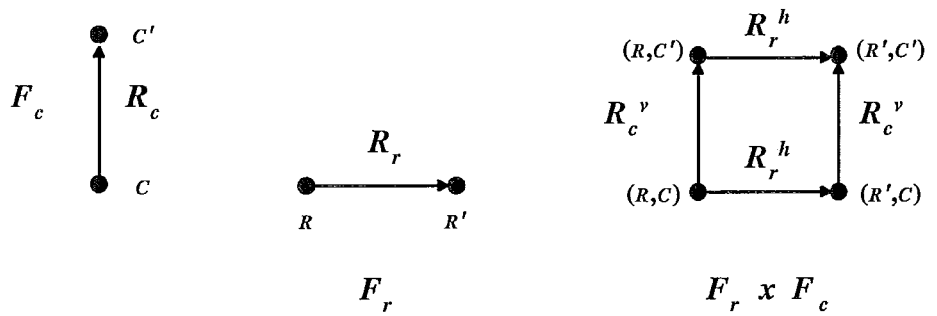

Figura 5.1: Produto de Frames

Definição 5.2.2 *Produto Semântico de Lógicas Modais.*

Sejam L_1 e L_2 lógicas proposicionais polimodais com m operadores. Considere $\mathbf{F}(L_1)$ a classe de frames validando L_1 e $\mathbf{F}(L_2)$ a classe de frames validando L_2.

Analogamente, todas as fórmulas válidas em um certo frame F constituem a lógica modal $\mathbf{L}(F)$. A lógica modal $\mathbf{L}(\mathbf{F})$ para uma classe de frames $\mathbf{F}$ é definida como a interseção $\bigcap\{\mathbf{L}(F) \mid F \in \mathbf{F}\}$.

O produto das lógicas L_1 e L_2 é a lógica $L_1 \times L_2$ obtida através de $\mathbf{L}(\mathbf{F}(L_1) \times \mathbf{F}(L_2))$.

É intuitivo pensar que o produto das lógicas sempre contem suas fusões, ou seja, $L_1 \oplus L_2 \subseteq L_1 \times L_2$. Na verdade, esta inclusão é própria. Contudo, os operadores modais de cada lógica não são afetados por suas interações, ou seja, o produto das lógicas é uma extensão conservativa das lógicas componentes [11].

5.3 Axiomatização do Produto de Lógicas Modais

O problema da axiomatização do produto de lógicas modais consiste em: dadas as lógicas modais L_1, L_2, ..., L_n, respectivamente, axiomatizar a lógica $L_1 \times L_2 \times \ldots \times L_n$. Comparado a fusão de lógicas modais, onde a axiomatização é direta e uma série de propriedades são preservadas, a axiomatização do produto de lógicas não é trivial. Em geral, a dificuldade depende muito do número de dimensões do produto: pouco resultados foram obtidos sobre produtos de três dimensões ou mais.

Contudo, os resultados em [33] mostram que, em muitos casos, o produto de duas lógicas modais pode ser facilmente axiomatizado. Para tanto,

verifique que as seguintes propriedades são observadas em frames-produto.

1. comutatividade a esquerda: $\forall x \forall y \forall z(xR^v y \wedge yR^h z \rightarrow \exists w(xR^h w \wedge wR^v z))$
2. comutatividade a direita: $\forall x \forall y \forall z(xR^h y \wedge yR^v z \rightarrow \exists w(xR^v w \wedge wR^h z))$
3. propriedade Church-Rosser: $\forall x \forall y \forall z(xR^v y \wedge xR^h z \rightarrow \exists w(yR^h w \wedge zR^v w))$

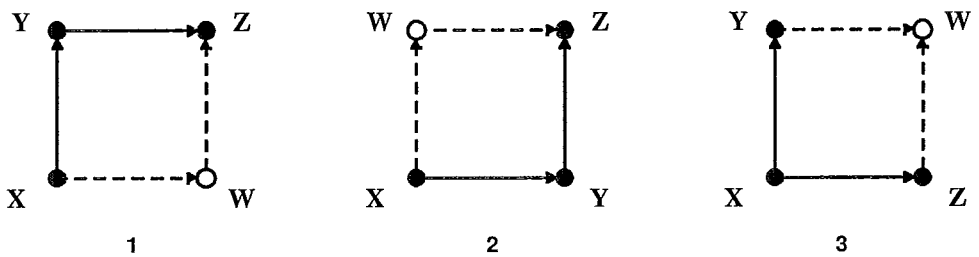

Figura 5.2: Propriedades do Produto de Frames

Estas propriedades também podem ser expressas por fórmulas modais. Chamaremos de lógicas comutativas as lógicas cujo produto possui estas propriedades, conforme a definição a seguir.

Definição 5.3.1 *Produtos Comutativos.*
Para as lógicas L_1 n-modal e L_2 m-modal, seja:
$[L_1, L_2] = L_1 \oplus L_2 + C^1_{ij} + C^2_{ij}$, *onde:*
$C^1_{ij} = (\Box_i \Box_{j+n} p \leftrightarrow \Box_{j+n} \Box_i p)$,
$C^2_{ij} = (\Diamond_i \Box_{j+n} p \rightarrow \Box_{j+n} \Diamond_i p)$,
$1 \leq i \leq n$, $1 \leq j \leq m$.
Diremos que o produto das lógicas L_1, L_2 é comutativo *se $L_1 \times L_2 = [L_1, L_2]$.*

Na verdade, é demonstrado em [33] que, em geral, $[L_1, L_2] \subseteq L_1 \times L_2$.

O produto de lógicas modais com certas características é *comutativo*, conforme veremos a seguir.

Definição 5.3.2 *Fórmulas Fechadas e Lógicas Fechadas.*
Uma n-modal fórmula é fechada se é uma 0-fórmula, ou seja, se não contem letras proposicionais.
Uma lógica n-modal é fechada se é axiomatizada por um conjunto de fórmulas n−modais fechadas.

Definição 5.3.3 *Lógica Canônica.*

Uma lógica modal é dita canônica se é válida em todos os seus frames canônicos.

Proposição 5.3.4 *Toda lógica fechada é canônica.*

Definição 5.3.5 *Fórmulas PTC e Lógicas PTC.*

Uma fórmula modal é pseudo-transitiva se é da forma:

$\nabla_1 \Box_k p \rightarrow \triangle_2 p$, *onde* $p \in Prop$, $\nabla_1 = \Diamond_i, \ldots, \Diamond_j$, $\triangle_2 = \Box_m, \ldots, \Box_n$ *são sequências de operadores modais (possivelmente vazias).*

Uma fórmula PTC é uma fórmula que ou é fechada ou é pseudo-transitiva.

Uma lógica PTC é uma lógica modal axiomatizada por um conjunto de fórmulas PTC.

Proposição 5.3.6 *Toda lógica PTC é canônica [33].*

Teorema 5.3.7 *Axiomatização do Produto de Lógicas Modais PTC [33].*

A lógica resultante do produto de todo par de lógicas PTC é comutativa.

Ou seja, se L_1 , L_2 são lógicas PTC - lógicas axiomatizáveis por um conjunto de fórmulas pseudo-transitivas ou fechadas - então $L_1 \times L_2 = [L_1, L_2]$.

Proposição 5.3.8 *Se as lógicas L_1 e L_2 são canônicas, então $[L_1, L_2]$ é canônica e $[L_1, L_2] = \mathbf{L}([\mathbf{F}(L_1), \mathbf{F}(L_2)])$.*

Provas para todas as proposições desta seção podem ser encontradas em [33].

Muitas lógicas modais conhecidas são PTC, tais como $\mathcal{D}, \mathcal{K}4, \mathcal{S}4, \mathcal{T}, \mathcal{B}, \mathcal{S}5$, e outras. Portanto, produtos bidimensionais tais como $\mathcal{T} \times \mathcal{T}$, $\mathcal{S}4 \times \mathcal{S}4$, $\mathcal{S}5 \times \mathcal{S}5$ são *comutativos.*

O nosso interesse é, particularmente, pelo produto $\mathcal{S}5 \times \mathcal{S}5$. Temos então, pelos resultados apresentados, que o produto $\mathcal{S}5 \times \mathcal{S}5$ é comutativo, e portanto a lógica resultante é axiomatizada por $[\mathcal{S}5, \mathcal{S}5]$. Além disso, como $\mathcal{S}5$ é canônica, pela proposição 5.3.8, o produto $\mathcal{S}5 \times \mathcal{S}5$ é canônico.

A lógica polimodal bidimensional que apresentamos para o conhecimento de agentes em sistemas assíncronos é, na verdade, uma extensão polimodal de $[\mathcal{S}5, \mathcal{S}5]$, conforme veremos nos capítulos seguintes.

Capítulo 6

Lógica Bidimensional de Conhecimento em Sistemas Distribuídos

Definimos o *subproduto fechado de lógicas modais* introduzindo dois aspectos novos sobre o produto de lógicas modais. O primeiro aspecto diz respeito a noção de *pares admissíveis*, ou seja, a restrição sobre determinados pontos gerando, desta forma, o que chamamos de *subproduto das lógicas*. O segundo aspecto trata da introdução da relação do fecho transitivo sobre as relações originais, produzindo o que denominamos um *produto fechado*. As duas características adicionais do *subproduto fechado de lógicas modais* constituem contribuições originais para a área de lógicas multidimensionais.

Apresentamos, então, as definições semânticas e o sistema axiomático $\mathcal{S}_m^2$ para uma lógica bidimensional de conhecimento no contexto de execuções assíncronas e cortes consistentes de um algoritmo distribuído. A semântica bidimensional e o sistema axiomático $\mathcal{S}_m^2$ não têm precedentes no campo das lógicas epistêmicas. As lógicas epistêsmicas tratam, em geral, de sistemas polimodais, onde cada operador modal refere-se ao conhecimento de um agente. Na lógica bidimensional que apresentamos a novidade está no contexto de avaliação das fórmulas, que são pares (r, c) de execuções e cortes.

Ilustramos o conhecimento que pode ser modelado pelo sistema $\mathcal{S}_m^2$ através de um exemplo com o algoritmo distribuído PIF (*propagation of information with feedback*) para três agentes.

6.1 Subproduto Fechado de Lógicas Modais

O *subproduto fechado de lógicas modais* é semelhante ao produto de lógicas modais, porém com duas características adicionais.

Em primeiro lugar, definimos um conjunto chamado de conjunto de *estados admissíveis* que é, na verdade, um subconjunto de todos os estados resultantes do produto cartesiano. A interpretação destes *estados admissíveis* no contexto de sistemas assíncronos é associada ao fato de que nem todos os pares (r, c) de execuções e cortes fazem sentido. Ou seja, nem todos os cortes consistentes estão presentes em todas as execuções, e vice-versa.

De um modo geral, os estados ou mundos possíveis no frame produto constituem o conjunto W de todos os pares obtidos do produto cartesiano dos dois conjuntos X e Y de estados dos frames básicos. Contudo, nem sempre todos os pares (x, y) são interessantes sob o ponto de vista de uma aplicação. Por isso, definimos o subconjunto $A \subseteq W = X \times Y$, que é dito o *conjunto de pares admissíveis*, a fim de restringir o foco, dando origem ao que chamamos de *subproduto* dos frames originais.

Além disso, definimos um operador modal bidimensional K_i associado à relação do fecho transitivo sob a união das relações básicas. Este operador modal representa as propriedades do conhecimento dos agentes no contexto (r, c) de execuções e cortes. Esta é uma nova interpretação do conhecimento dos agentes em ambientes assíncronos, que conduz a uma semântica distinta de todas as apresentadas até então.

Para se ter uma idéia de como a nova relação do fecho transitivo potencializa o subproduto das lógicas, repare que, no produto convencional não era possível falar de propriedades *interdimensionais*. De acordo com a definição 5.2.1, as relações no produto de lógicas constituem projeções das relações originais: observamos que, fixando-se uma ordenada e variando-se a outra tem-se o efeito de *projetar uma dimensão*. Assim, cada par de pontos relacionados define, na verdade, um passo horizontal ou vertical no plano. No subproduto fechado de lógicas, temos a mesma noção de passos horizontais e/ou verticais, e adicionalmente, a possibilidade de darmos *saltos interdimensionais*, através da relação obtida do fecho transitivo sob a união das duas relações básicas.

Definição 6.1.1 *Subproduto Fechado Semântico de Frames Modais.*

Considere os frames $F_1 = (X, R_i)$ *e* $F_2 = (Y, R_j)$ *para* L_1 *e* L_2, *respectivamente. O* subproduto fechado *dos frames* F_1 *e* F_2 *em relação a* A *é o frame* $F_1 \otimes F_2 = (W, \simeq_i, \approx_j, \sim_k, A)$, *onde:*

1. $W = X \times Y$ *: é o conjunto de todos os estados* (x, y);

2. $A \subseteq W = X \times Y$: *é um subconjunto dos estados* (x, y);

3. $\simeq_i = \{((x,z),(y,z))|xR_iy\}$;

4. $\approx_j = \{((z,x),(z,y))|xR_jy\}$;

5. $\sim_k = (\simeq_i \cup \approx_j)^*$, onde $(\simeq_i \cup \approx_j)^*$ denota o fecho transitivo sob a união de $\simeq_i$ e $\approx_j$.

Definição 6.1.2 *Subproduto Fechado Semântico de Lógicas Modais.*

Sejam L_1 *e* L_2 *lógicas polimodais,* $\mathbf{F}(L_1)$ *a classe de frames validando* L_1 *e* $\mathbf{F}(L_2)$ *a classe de frames validando* L_2. *O subproduto fechado das lógicas* L_1 *e* L_2 *é a lógica* $\mathbf{L}(\mathbf{F}(L_1) \otimes \mathbf{F}(L_2))$.

Definição 6.1.3 *Modelo sobre o Subproduto de Frames Modais.*

Um modelo M *sobre* $F = F_H \otimes F_V$ *é um par* $M = (F, v)$, *onde* v *é uma função de atribuição de valores de verdade às primitivas de* $Prop = Prop_H \cup Prop_V$. *Para cada* $p \in Prop$, $v(p)$ *é o conjunto dos pares* (x, y) *onde* p *é verdadeira, ou seja,* $v(p) : Prop \longrightarrow 2^{X \times Y}$.

6.2 Semântica Bidimensional

Propomos uma semântica para lógicas de conhecimento em sistemas distribuídos assíncronos sob esta nova perspectiva, onde o contexto (r, c) de execuções assíncronas e cortes consistentes no qual as fórmulas são avaliadas é visto como o produto de duas lógicas básicas, L_H e L_V, correspondendo às dimensões horizontal e vertical, respectivamente.

- A lógica L_H é interpretada, por exemplo, no contexto onde o corte é fixo e variam-se as execuções, ou seja, é possível avaliar as propriedades do conhecimento em cortes comuns a diversas execuções.

- A lógica L_V é interpretada no contexto onde a execução é fixa e variam-se os cortes, a fim de avaliar as propriedades do conhecimento em cortes consistentes de uma execução assíncrona dada.

Definição 6.2.1 *Lógica* L_H.

Seja a lógica L_H *o menor conjunto de fórmulas contendo o conjunto de primitivas* $Prop_H$, *fechado sob negação, conjunção e os operadores modais* H_i, *onde* $i = 1, \ldots, m$.

Definição 6.2.2 *Lógica* L_V.

Seja a lógica L_V *o menor conjunto de fórmulas contendo o conjunto de primitivas* $Prop_V$, *fechado sob negação, conjunção e os operadores modais* V_i, *onde* $i = 1, \ldots, m$.

6.2.1 Relações de Possibilidade

Tendo em vista que a semântica para sistemas assíncronos é baseada na semântica de mundos possíveis de Kripke, temos, como de costume, relações de possibilidade ou de acessibilidade. Uma vez que os estados possíveis para um agente são dados por uma relação de equivalência refletindo a indistinguibilidade dos estados globais sob o ponto de vista do agente, considere, para a semântica bidimensional, que as relações de possibilidade são **relações de equivalência**, cuja interpretação é a seguinte:

- A relação de equivalência $\simeq_i$ associamos à dimensão horizontal. No contexto de sistemas distribuídos assíncronos, supomos que a dimensão horizontal representa o conjunto R de execuções assíncronas do sistema para m agentes. Portanto, para $r_1 \in R$ e $r_2 \in R$, temos que $(r_1, c) \simeq_i (r_2, c)$ é lido como "as execuções r_1 e r_2 são indistinguíveis sob o ponto de vista do agente i" ou "nas execuções r_1 e r_2 o agente i tem a mesma visão passada em relação ao corte c considerado".

- A relação de equivalência $\approx_j$ para a dimensão vertical. Neste caso, supomos que a dimensão vertical representa uma enumeração do conjunto C de estados globais ou cortes consistentes possíveis em todas as execuções do sistema. Logo, para $c_1 \in C$ e $c_2 \in C$, $(r, c_1) \approx_j (r, c_2)$ significa que "para o agente j os cortes c_1 e c_2 da execução r são indistinguíveis" ou "nos cortes c_1 e c_2 o agente j tem a mesma visão passada".

- A relação de equivalência $\sim_k$ para o *subproduto fechado* das dimensões básicas. Esta relação constitui o fecho transitivo sob a união das duas relações anteriores, permitindo o que chamamos de *saltos inter-dimensionais*. Então, para dois estados (r_1, c_1) e (r_2, c_2), a relação $(r_1, c_1) \sim_k (r_2, c_2)$ indica que "para o agente k, o corte c_1 na execução r_1 é indistinguível do corte c_2 na execução r_2" ou que "em (r_1, c_1) e em (r_2, c_2) o agente k tem a mesma visão passada".

Doravante, utilizaremos o mesmo subscrito i para as relações e operadores modais, uma vez que temos m agentes, e portanto, o subproduto de duas lógicas m-modais.

6.2.2 Operadores Modais de Conhecimento

Para cada relação de equivalência definida temos um operador modal associado. Considerando a interpretação de conhecimento baseada na visão

passada dos agentes como definida em 3.2.1 e 3.2.3, o significado dos operadores modais é o seguinte:

- $H_i\varphi$ indica que "o agente i conhece φ em todas as execuções indistinguíveis para o corte atual".
- $V_i\varphi$ indica que "o agente i conhece φ em todos os cortes indistinguíveis na execução atual".
- $K_i\varphi$ indica que "o agente i conhece φ em todos os estados (r, c) indistinguíveis para ele". Ou seja, φ é verdadeira em todos os pares (r, c) onde o agente tem a mesma visão passada. Para simplificar, diremos que $K_i\varphi$ representa simplesmente que "o agente i tem o conhecimento de φ".

6.2.3 Interpretação de Conhecimento Bidimensional

Desejamos interpretar a lógica bidimensional polimodal L_m^2 como o subproduto fechado das lógicas L_H e L_V. A lógica L_m^2 é utilizada para representar o conhecimento em sistemas distribuídos multiagentes assíncronos de modo que é possível definir propriedades de cada contexto em separado, de execuções e de cortes, e também do contexto (r, c) bidimensional resultante.

Definição 6.2.3 *Lógica Bidimensional* L_m^2.
Seja a lógica L_m^2 *o menor conjunto de fórmulas bem formadas contendo a constante* Δ, *o conjunto de primitivas* $Prop = Prop_H \cup Prop_V$, *fechado sob negação, conjunção e os operadores modais* $\overline{H}_i$, H_i, $\overline{V}_i$, V_i, Q_i *e* K_i, *onde* $i = 1, \ldots, m$.

Em resumo, para a lógica L_m^2, desejamos a seguinte interpretação de Kripke:

- Os mundos possíveis são pares (r, c) onde r é uma execução assíncrona e c um corte consistente (ou estado global) na execução r;
- Os fatos básicos do sistema constituem o conjunto de primitivas $Prop = Prop_H \cup Prop_V$;
- A função de atribuição de valores-verdade v é uma função que preserva o conhecimento dos agentes, ou seja, o que o agente conhece é função do conjunto de eventos da sua visão passada em relação ao estado atual;
- As relações $\simeq_i$ e $\approx_i$ são relações de equivalência onde:

1. $(r,c) \simeq_i (r',c)$ se e somente se a visão passada do agente i é a mesma em (r,c) e em (r',c);
2. $(r,c) \approx_i (r,c')$ se e somente se a visão passada do agente i é a mesma em (r,c) e em (r,c');

- A relação $\sim_i$ é o fecho transitivo sob a união das duas relações de equivalência básicas $\simeq_i$ e $\approx_i$.

6.2.4 Satisfazibilidade em L_m^2

Finalmente, podemos formalizar o que significa, no contexto bidimensional (r,c) de execuções assíncronas e cortes consistentes, dizer que uma fórmula $\alpha \in L_m^2$ é verdadeira.

Definição 6.2.4 *Satisfazibilidade em L_m^2.*
Seja $F = (W, \simeq_i, \approx_i, \sim_i, A)$ um frame para L_m^2 e seja M um modelo sobre F. Uma fórmula $\alpha \in L_m^2$ é verdadeira em $[M,(r,c)]$, $[M,(r,c)] \models \alpha$, para $(r,c) \in W = R \times C$, quando:

1. $[M,(r,c)] \models p \Leftrightarrow (r,c) \in v(p)$, *onde* $p \in Prop$;
2. $[M,(r,c)] \models \alpha \wedge \beta \Leftrightarrow [M,(r,c)] \models \alpha$ *e* $[M,(r,c))] \models \beta$;
3. $[M,(r,c)] \models \neg\alpha \Leftrightarrow [M,(r,c)] \not\models \alpha$;
4. $[M,(r,c)] \models \overline{H}_i\alpha \Leftrightarrow \forall(r',c')\{((r,c) \simeq_i (r',c')) \Rightarrow [M,(r',c')] \models \alpha\}$;
5. $[M,(r,c)] \models \overline{V}_i\alpha \Leftrightarrow \forall(r',c')\{((r,c) \approx_i (r',c')) \Rightarrow [M,(r',c')] \models \alpha\}$;
6. $[M,(r,c)] \models \Delta \Leftrightarrow (r,c) \in A \subseteq W = R \times C$;
7. $[M,(r,c)] \models H_i\alpha \Leftrightarrow [M,(r,c)] \models \Delta$ *e* $[M,(r,c)] \models \overline{H}_i\alpha$;
8. $[M,(r,c)] \models V_i\alpha \Leftrightarrow [M,(r,c)] \models \Delta$ *e* $[M,(r,c)] \models \overline{V}_i\alpha$;
9. $[M,(r,c)] \models Q_i\alpha \Leftrightarrow [M,(r,c)] \models H_i\alpha$ *e* $[M,(r,c)] \models V_i\alpha$;
10. $[M,(r,c)] \models K_i\alpha \Leftrightarrow [M,(r,c)] \models \Delta$ *e* $\forall(r',c')\{((r,c) \sim_i (r',c')) \Rightarrow [M,(r',c')] \models \alpha\}$.

6.3 Sistema Axiomático $\mathcal{S}_m^2$

Quando as relações de possibilidade são relações de equivalência, sabemos que lógicas como L_H e L_V são axiomatizáveis por $\mathcal{S}5_m$ [20]. Além disso, sabemos que o produto $\mathcal{S}5_m \times \mathcal{S}5_m$ é comutativo, e portanto, axiomatizado por $[\mathcal{S}5_m, \mathcal{S}5_m]$, conforme a definição 5.3.1.

Propomos, então, uma axiomatização da lógica bidimensional L_m^2 como sendo os axiomas do produto comutativo $\mathcal{S}5_m \times \mathcal{S}5_m$, para as dimensões horizontal e vertical, acrescida de axiomas que caracterizam as propriedades do operador modal bidimensional K_i.

Considere $\mathcal{S}_m^2$ o sistema axiomático para a lógica bidimensional L_m^2 constituído dos seguintes axiomas e regras.

Axiomas.

0 Todas as tautologias do cálculo proposicional

1 $(\overline{H}_i\alpha \wedge \overline{H}_i(\alpha \rightarrow \beta)) \rightarrow \overline{H}_i\beta$

2 $\overline{H}_i\alpha \rightarrow \alpha$

3 $\overline{H}_i\alpha \rightarrow \overline{H}_i\overline{H}_i\alpha$

4 $\neg\overline{H}_i\alpha \rightarrow \overline{H}_i\neg\overline{H}_i\alpha$

5 $(\overline{V}_i\alpha \wedge \overline{V}_i(\alpha \rightarrow \beta)) \rightarrow \overline{V}_i\beta$

6 $\overline{V}_i\alpha \rightarrow \alpha$

7 $\overline{V}_i\alpha \rightarrow \overline{V}_i\overline{V}_i\alpha$

8 $\neg\overline{V}_i\alpha \rightarrow \overline{V}_i\neg\overline{V}_i\alpha$

9 $(K_i\alpha \wedge K_i(\alpha \rightarrow \beta)) \rightarrow K_i\beta$

10 $K_i\alpha \rightarrow \alpha$

11 $K_i\alpha \rightarrow K_iK_i\alpha$ [1]

12 $\neg K_i\alpha \rightarrow K_i\neg K_i\alpha$

13 $\overline{H}_i\overline{V}_j\alpha \leftrightarrow \overline{V}_j\overline{H}_i\alpha$

14 $\neg\overline{H}_i\neg\overline{V}_j\alpha \rightarrow \overline{V}_j\neg\overline{H}_i\neg\alpha$

[1] Este axioma é obtido dos axiomas 19 e 20.

15 $\neg\overline{V}_i\neg\overline{H}_j\alpha \rightarrow \overline{H}_j\neg\overline{V}_i\neg\alpha$

16 $H_i\alpha \leftrightarrow \Delta \wedge \overline{H}_i\alpha$

17 $V_i\alpha \leftrightarrow \Delta \wedge \overline{V}_i\alpha$

18 $Q_i\alpha \leftrightarrow H_i\alpha \wedge V_i\alpha$

19 $K_i\alpha \leftrightarrow Q_iK_i\alpha$

20 $K_i(\alpha \rightarrow Q_i\alpha) \rightarrow (\alpha \rightarrow K_i\alpha)$

onde $i, j = 1, \ldots, m$.

Regras.

R0 De $\vdash \alpha$ derive toda substituição uniforme para α

R1 De $\vdash \alpha, \alpha \rightarrow \beta$ derive β (modus ponens)

R2 De $\vdash \alpha$ derive $\overline{H}_i\alpha$ (*generalização horizontal*)

R3 De $\vdash \alpha$ derive $\overline{V}_i\alpha$ (*generalização vertical*)

R4 De $\vdash \alpha$ derive $K_i\alpha$ (*generalização bidimensional*)

6.4 Exemplo de Conhecimento em um Sistema Assíncrono

Para ilustrar o tipo de conhecimento caracterizado por $\mathcal{S}_m^2$, considere um sistema assíncrono com 3 agentes, rodando o algoritmo distribuído para propagação da informação com realimentação (PIF). Assumimos o agente a_1 como iniciador do algoritmo. Lembramos também que $send_i^j(M)$ significa que "o agente i manda a mensagem M para o agente j" e $receive_i^j(M)$ que "o agente i recebe a mensagem M do agente j". Para uma descrição do algoritmo PIF, consulte a seção 3.1.

Primeiramente definimos o conjunto E de eventos que caracterizam o envio e/ou recebimento da mensagem M entre os agentes. Os eventos têm o mesmo significado independente da execução.

$E = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$ onde:

1. e_1 - $send_1^2(M)$, $send_1^3(M)$
2. e_2 - $receive_2^1(M)$, $send_2^3(M)$

3. e_3 - $receive_3^2(M)$, $send_3^1(M)$

4. e_4 - $receive_3^1(M)$, $send_3^2(M)$

5. e_5 - $receive_2^3(M)$, $send_2^1(M)$

6. e_6 - $receive_1^3(M)$

7. e_7 - $receive_1^2(M)$

Portanto, temos os conjuntos E_i, $i = 1, 2, 3$ de eventos possíveis para os agentes a_1, a_2 e a_3, respectivamente:
$E_1 = \{e_1, e_6, e_7\}$
$E_2 = \{e_2, e_5\}$
$E_3 = \{e_3, e_4\}$
As diferentes execuções resultam das combinações na ordem em que os eventos acontecem para cada agente. Assim sendo, enumeramos as possíveis execuções, dando origem ao conjunto $R = \{r_1, r_2, r_3, r_4, r_5, r_6\}$. As figuras 6.1 e 6.2 contêm os gráfos de precedência para as possíveis execuções do conjunto R, com os respectivos cortes consistentes, tendo o agente a_1 como iniciador do algoritmo.

Enumeramos os possíveis estados globais ou cortes consistentes que ocorrem nas execuções do conjunto R. Neste caso, consideramos a definição 3.1.13 de corte consistente para todas as execuções assíncronas do sistema, ou seja, cada estado global é uma partição dos eventos em dois conjuntos, resultando nos 16 cortes a seguir [2]:

c_1 $E_P = \{e_1\}$; $E_F = \{e_2, e_3, e_4, e_5, e_6, e_7\}$

c_2 $E_P = \{e_1, e_2\}$; $E_F = \{e_3, e_4, e_5, e_6, e_7\}$

c_3 $E_P = \{e_1, e_2, e_3\}$; $E_F = \{e_4, e_5, e_6, e_7\}$

c_4 $E_P = \{e_1, e_2, e_3, e_4\}$; $E_F = \{e_5, e_6, e_7\}$

c_5 $E_P = \{e_1, e_2, e_3, e_4, e_5\}$; $E_F = \{e_6, e_7\}$

c_6 $E_P = \{e_1, e_2, e_3, e_4, e_5, e_6\}$; $E_F = \{e_7\}$

c_7 $E_P = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$; $E_F = \{\}$

c_8 $E_P = \{e_1, e_2, e_3, e_6\}$; $E_F = \{e_4, e_5, e_7\}$

[2] O corte c_0: $E_P = \{\}$; $E_F = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$ correspondente ao estado inicial não foi considerado.

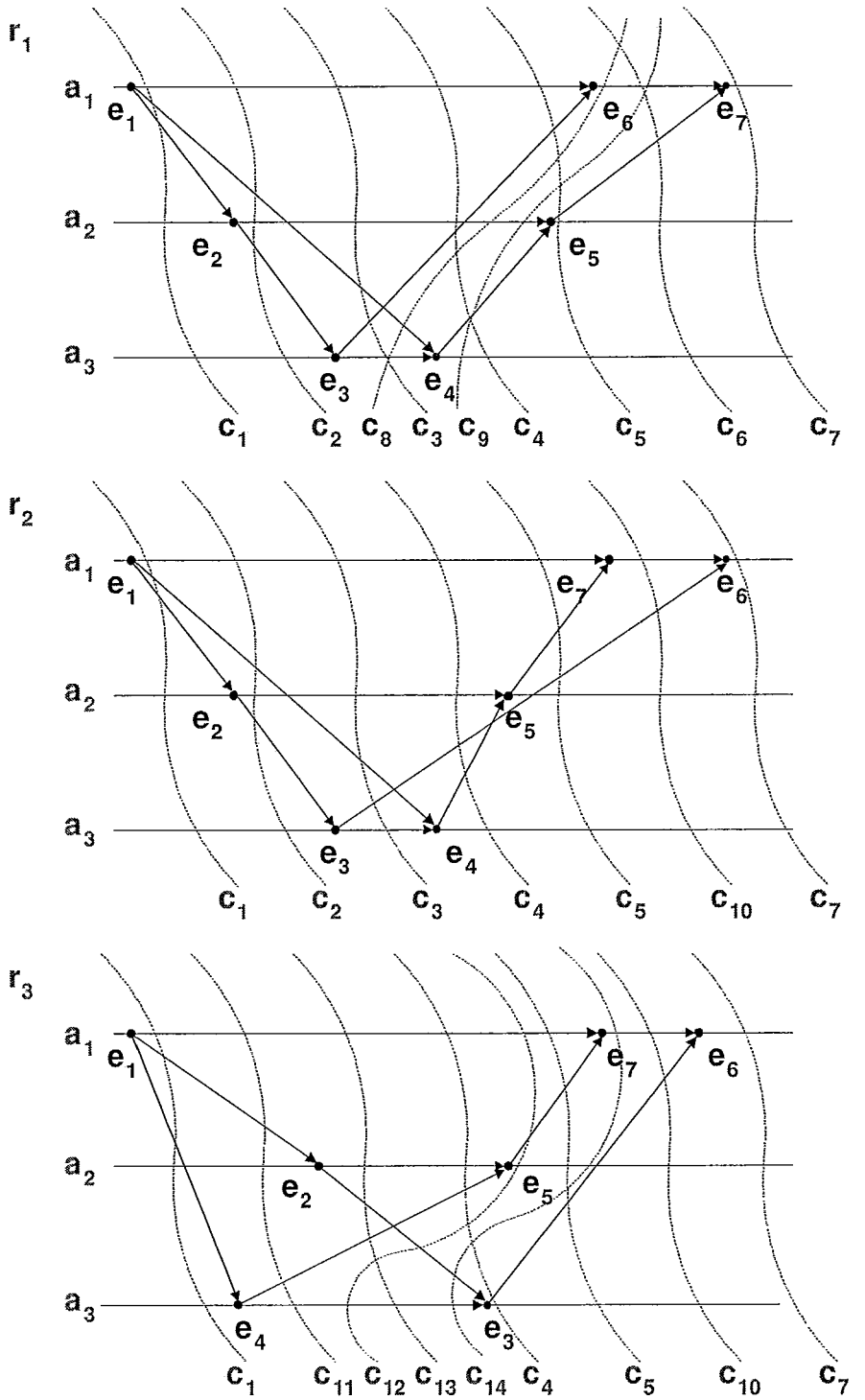

Figura 6.1: Algoritmo PIF com 3 Agentes - Grafos de Precedência para Execuções r_1, r_2, r_3

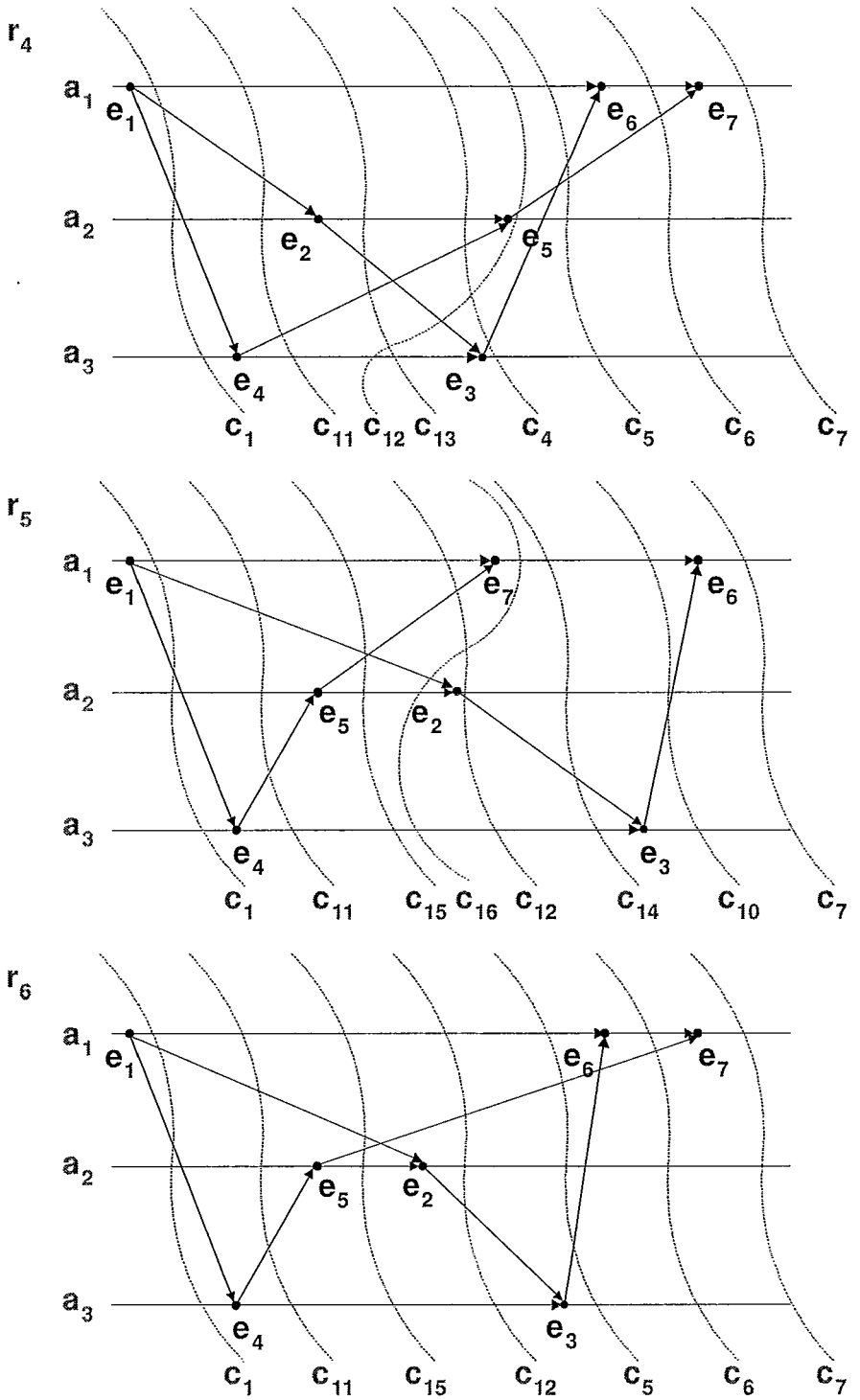

Figura 6.2: Algoritmo PIF com 3 Agentes - Grafos de Precedência para Execuções r_4, r_5, r_6

c_9 $E_P = \{e_1, e_2, e_3, e_6, e_4\}$; $E_F = \{e_5, e_7\}$

c_{10} $E_P = \{e_1, e_2, e_3, e_4, e_5, e_7\}$; $E_F = \{e_6\}$

c_{11} $E_P = \{e_1, e_4\}$; $E_F = \{e_2, e_3, e_5, e_6, e_7\}$

c_{12} $E_P = \{e_1, e_2, e_4, e_5\}$; $E_F = \{e_3, e_6, e_7\}$

c_{13} $E_P = \{e_1, e_2, e_4\}$; $E_F = \{e_3, e_5, e_6, e_7\}$

c_{14} $E_P = \{e_1, e_2, e_4, e_5, e_7\}$; $E_F = \{e_3, e_6\}$

c_{15} $E_P = \{e_1, e_4, e_5\}$; $E_F = \{e_2, e_3, e_6, e_7\}$

c_{16} $E_P = \{e_1, e_4, e_5, e_7\}$; $E_F = \{e_2, e_3, e_6\}$

Consideramos a interpretação epistêmica baseada na visão passada, conforme definida em 3.2.1 e 3.2.3. Neste caso, o estado local de cada agente é dado pelo conjunto de eventos que ocorreram para o agente até o corte atual. Logo, temos os seguintes conjuntos de estados ou visões passadas possíveis para cada agente:

$V_P(1, c_i) = \{e_1\}$, $i = 1, 2, 3, 4, 5, 11, 12, 13, 15$;
$V_P(1, c_j) = \{e_1, e_6\}$, $j = 6, 8, 9$;
$V_P(1, c_k) = \{e_1, e_7\}$, $k = 10, 14, 16$;
$V_P(1, c_l) = \{e_1, e_6, e_7\}$, $l = 7$;
$V_P(2, c_i) = \{\}$, $i = 1, 11$;
$V_P(2, c_j) = \{e_2\}$, $j = 2, 3, 4, 8, 9, 13$;
$V_P(2, c_k) = \{e_5\}$, $k = 15, 16$;
$V_P(2, c_l) = \{e_2, e_5\}$, $l = 5, 6, 7, 10, 12, 14$;
$V_P(3, c_i) = \{\}$, $i = 1, 2$;
$V_P(3, c_j) = \{e_3\}$, $j = 3, 8$;
$V_P(3, c_k) = \{e_4\}$, $k = 11, 12, 13, 14, 15, 16$;
$V_P(3, c_l) = \{e_3, e_4\}$, $l = 4, 5, 6, 7, 9, 10$.

Como a relação de equivalência que definimos diz que dois cortes são indistinguíveis sob o ponto de vista de um agente quando o agente tem a mesma visão passada em ambos os cortes, significa que cada conjunto de cortes i, j, k e l forma uma classe de equivalência de conhecimento do agente, ou seja, em cada conjunto de cortes i, j, k e l o agente *sabe* as mesmas coisas, aconteceram os mesmos eventos para ele.

Considerando a dimensão horizontal como a de execuções r e a vertical como a de cortes c, apresentamos gráficos que representam as classes de equivalência de conhecimento i, j, k e l dos agentes. Os gráficos são, na verdade,

uma espécie de redução reflexiva-transitiva das classes de equivalência de conhecimento, ou seja, não foram desenhadas ligações reflexivas ou transitivas dadas por $\simeq_i$, $\approx_i$, ou $\sim_i$. Construímos 6 gráficos: os 3 gráficos das figuras 6.3, 6.4, 6.5 representam o conhecimento bidimensional e os complementos em relação ao produto cartesiano, ou seja, as linhas cheias referem-se ao conhecimento associado ao operador K_i para os cortes admissíveis, enquanto que as linhas pontilhadas representam os complementos relativos aos operadores $\overline{H}_i$ e $\overline{V}_i$, avaliados em todos os pontos do produto cartesiano $R \times C$. Os 3 gráficos restantes não apresentam os complementos em relação ao produto cartesiano, mas apenas os pares admissíveis, são menos carregados e as classes de equivalência podem ser melhor visualizadas.

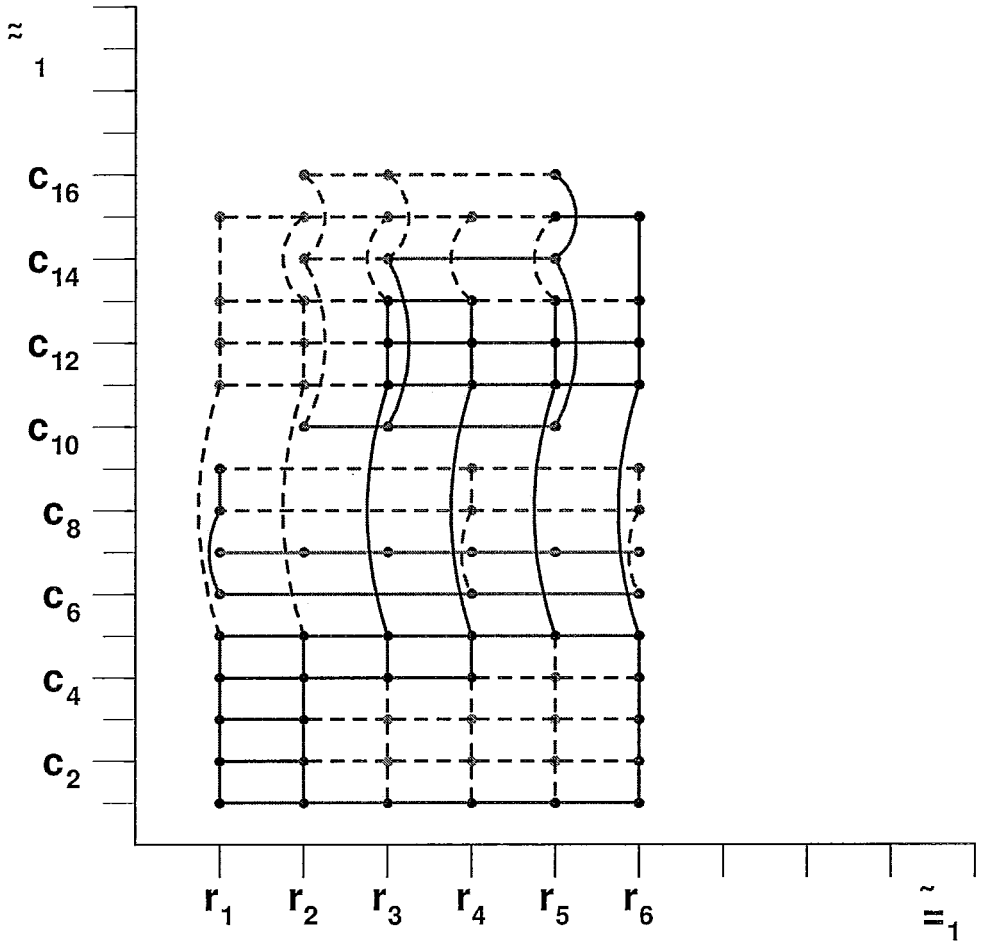

Figura 6.3: Classes de Equivalência de Conhecimento para o Agente 1

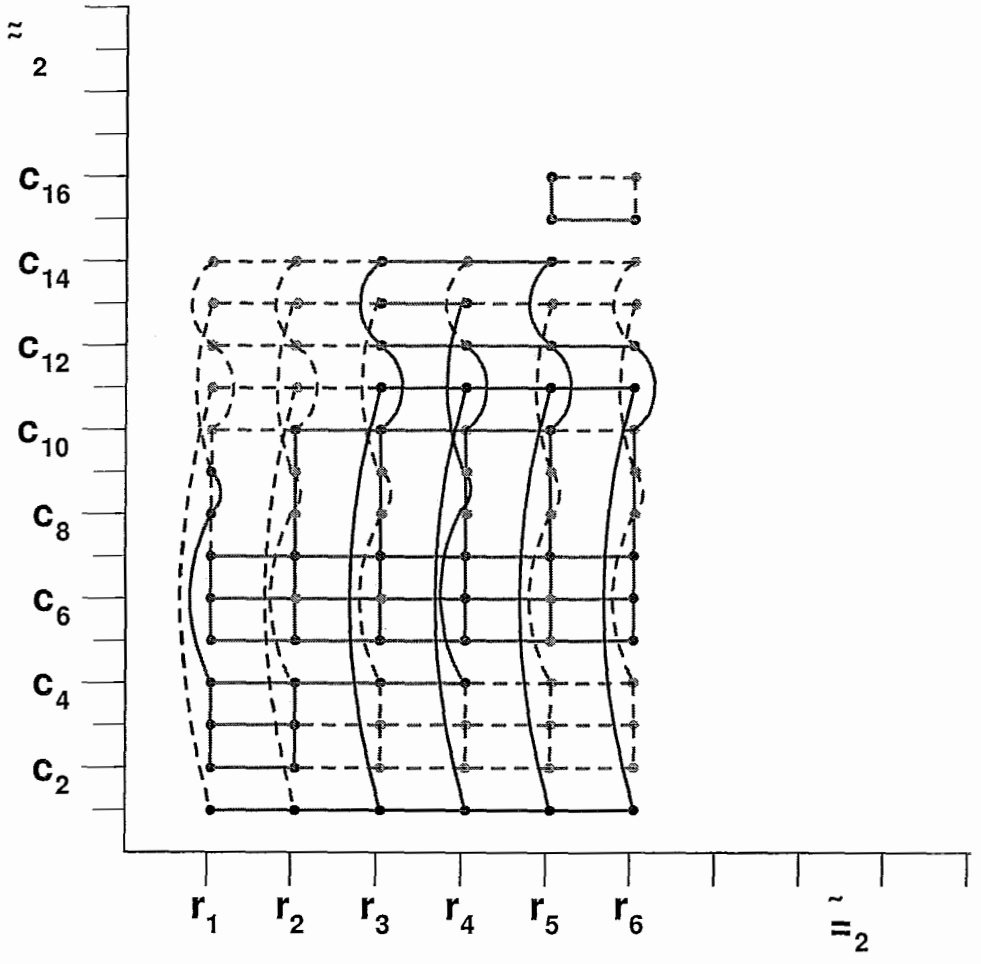

Figura 6.4: Classes de Equivalência de Conhecimento para o Agente 2

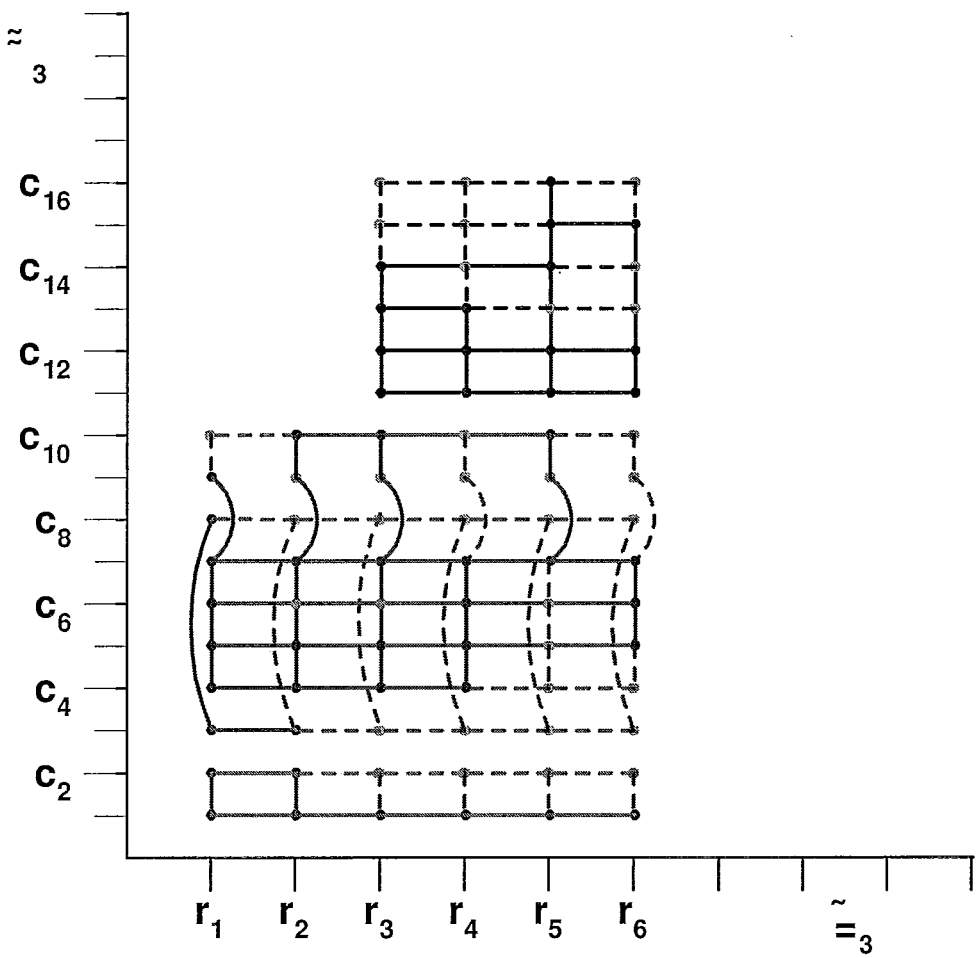

Figura 6.5: Classes de Equivalência de Conhecimento para o Agente 3

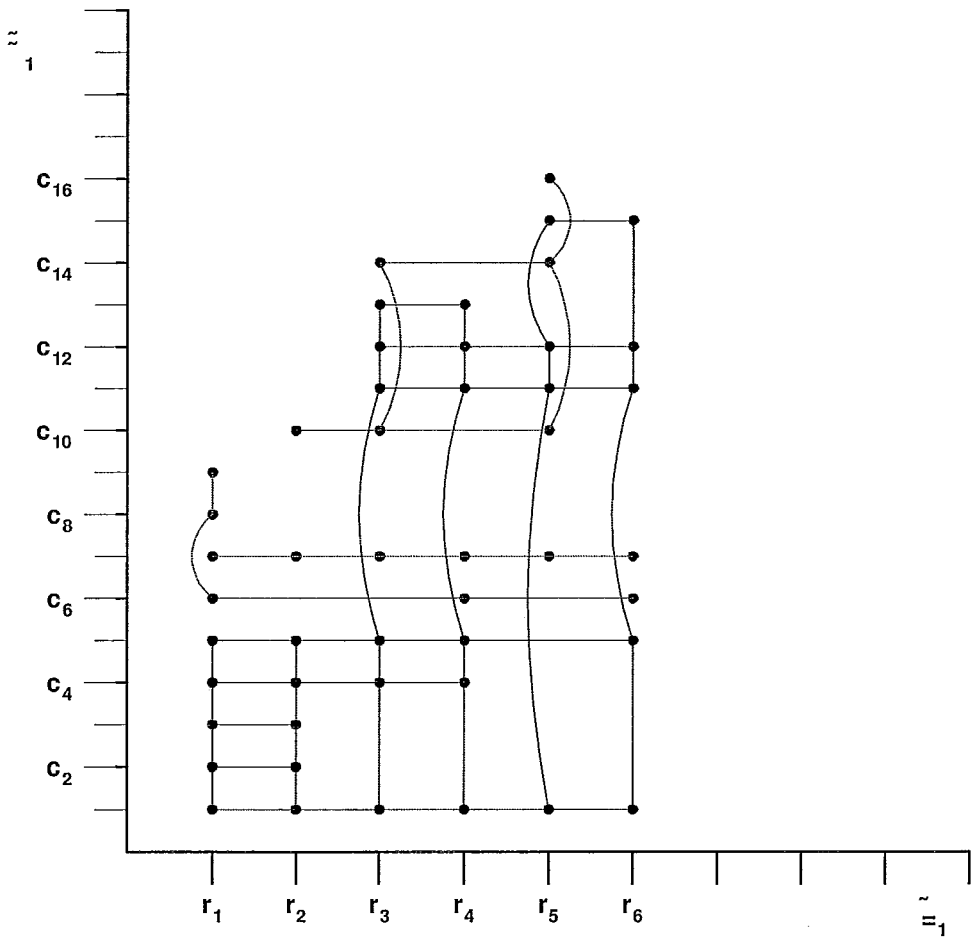

Figura 6.6: Classes de Equivalência de Conhecimento para o Agente 1 (pares admissíveis)

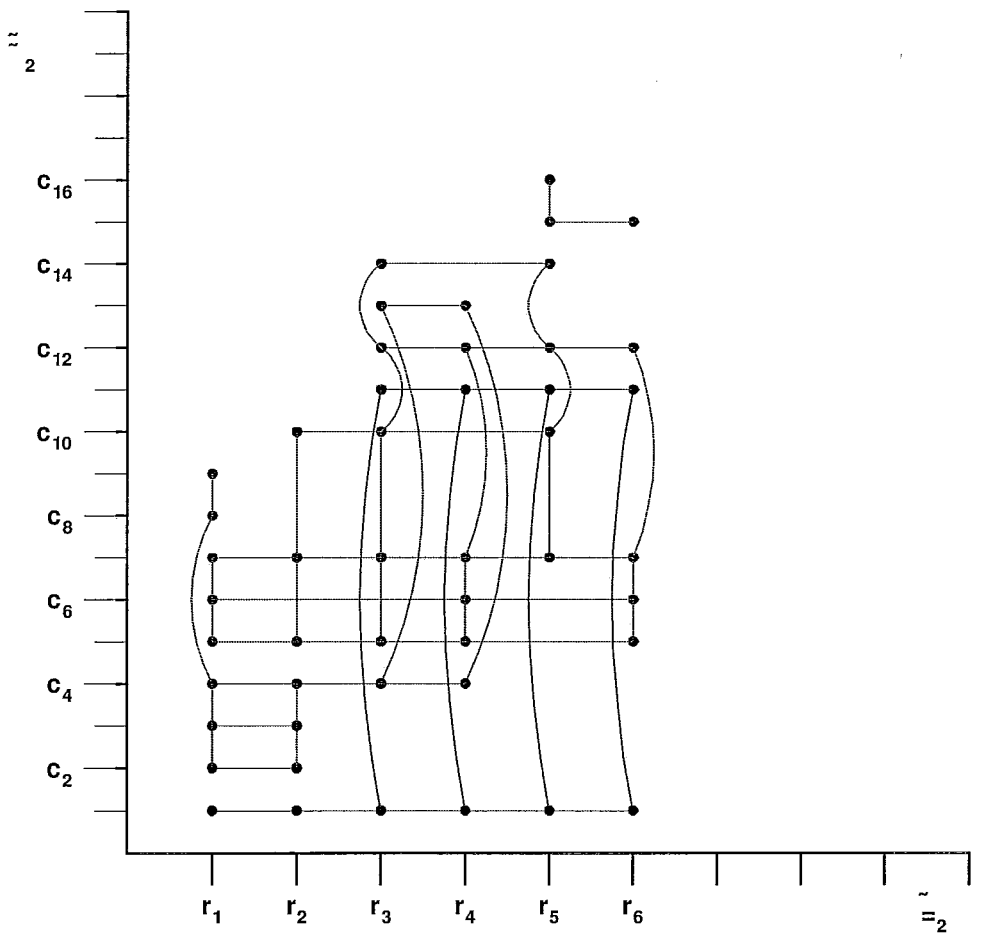

Figura 6.7: Classes de Equivalência de Conhecimento para o Agente 2 (pares admissíveis)

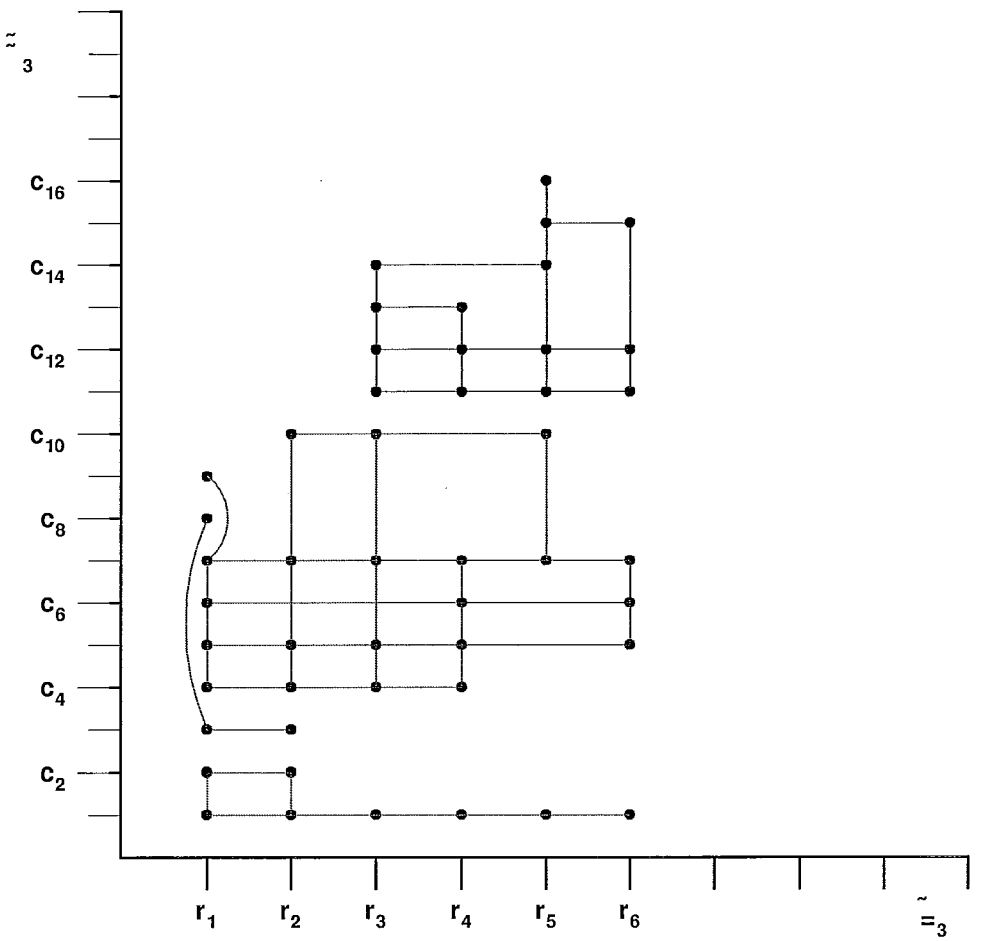

Figura 6.8: Classes de Equivalência de Conhecimento para o Agente 3 (pares admissíveis)

Capítulo 7

Corretude e Completude de $\mathcal{S}_m^2$

Neste capítulo apresentamos as provas de corretude e completude para o sistema $\mathcal{S}_m^2$. Fornecemos uma prova da propriedade f.m.p. para $\mathcal{S}_m^2$, ou seja, mostramos que o sistema é caracterizado por uma classe de modelos finitos. Como consequência, temos que $\mathcal{S}_m^2$ é decidível.

Para dar uma prova formal de decidibilidade para $\mathcal{S}_m^2$ seria preciso mostrar que existe um procedimento efetivo que, para qualquer f.b.f. $\varphi \in L_m^2$, determina, em num número finito de passos, se φ é um teorema do sistema. Contudo, existe uma conexão bem conhecida entre as propriedades de decidibilidade e f.m.p. (finite model property): se um sistema é finitamente axiomatizável e tem a propriedade de modelos finitos, então é decidível. Neste caso, para provar a decidibilidade de $\mathcal{S}_m^2$, é suficiente mostrar que $\mathcal{S}_m^2$ tem a propriedade de modelos finitos.

7.1 Corretude para $\mathcal{S}_m^2$

Desejamos provar a corretude do sistema $\mathcal{S}_m^2$ em relação à classe de frames que correspondem a subprodutos fechados de duas lógicas modais $\mathcal{S}5_m$. Para tanto, é preciso demonstrar que todos os axiomas do sistema $\mathcal{S}_m^2$ são válidos nesta classe de frames e que as regras de inferência preservam a validade.

Definição 7.1.1 *Classe de frames* **F**.

Seja **F** *a classe de frames* $F = (W, \simeq_i, \approx_i, \sim_i, A)$, *onde* $W = R \times C$, $A \subseteq W$, *as relações* $\simeq_i, \approx_i$ *são relações de equivalência e* $\sim_i$ *é o fecho transitivo sob estas duas primeiras, conforme a definição 6.1.1. Ou seja,* **F** *é a classe de frames de subprodutos fechados de duas dimensões onde as relações originais são relações de equivalência.*

Lema 7.1.2 *Seja* M *um modelo sobre* $F \in \mathbf{F}$.

Para toda fórmula bem formada (f.b.f.) α *e* $\beta \in L_m^2$, *e todo* $i, j = 1, 2, \ldots, m$:

1 $M \models (\overline{H}_i\alpha \wedge \overline{H}_i(\alpha \rightarrow \beta)) \rightarrow \overline{H}_i\beta$

2 $M \models \overline{H}_i\alpha \rightarrow \alpha$

3 $M \models \overline{H}_i\alpha \rightarrow \overline{H}_i\overline{H}_i\alpha$

4 $M \models \neg\overline{H}_i\alpha \rightarrow \overline{H}_i\neg\overline{H}_i\alpha$

5 $M \models (\overline{V}_i\alpha \wedge \overline{V}_i(\alpha \rightarrow \beta)) \rightarrow \overline{V}_i\beta$

6 $M \models \overline{V}_i\alpha \rightarrow \alpha$

7 $M \models \overline{V}_i\alpha \rightarrow \overline{V}_i\overline{V}_i\alpha$

8 $M \models \neg\overline{V}_i\alpha \rightarrow \overline{V}_i\neg\overline{V}_i\alpha$

9 $M \models (K_i\alpha \wedge K_i(\alpha \rightarrow \beta)) \rightarrow K_i\beta$

10 $M \models K_i\alpha \rightarrow \alpha$

11 $M \models K_i\alpha \rightarrow K_iK_i\alpha$

12 $M \models \neg K_i\alpha \rightarrow K_i\neg K_i\alpha$

13 $M \models \overline{H}_i\overline{V}_j\alpha \leftrightarrow \overline{V}_j\overline{H}_i\alpha$

14 $M \models \neg\overline{H}_i\neg\overline{V}_j\alpha \rightarrow \overline{V}_j\neg\overline{H}_i\neg\alpha$

15 $M \models \neg\overline{V}_i\neg\overline{H}_j\alpha \rightarrow \overline{H}_j\neg\overline{V}_i\neg\alpha$

16 $M \models H_i\alpha \leftrightarrow \Delta \wedge \overline{H}_i\alpha$

17 $M \models V_i\alpha \leftrightarrow \Delta \wedge \overline{V}_i\alpha$

18 $M \models Q_i\alpha \leftrightarrow H_i\alpha \wedge V_i\alpha$

19 $M \models K_i\alpha \leftrightarrow Q_iK_i\alpha$

20 $M \models K_i(\alpha \rightarrow Q_i\alpha) \rightarrow (\alpha \rightarrow K_i\alpha)$

Prova do Lema 7.1.2.

1 Se $[M, (r, c)] \models (\overline{H}_i\alpha \wedge \overline{H}_i(\alpha \rightarrow \beta))$, então para todo estado (r', c') tal que $((r, c) \simeq_i (r', c'))$ temos $[M, (r', c')] \models \alpha$ e $[M, (r', c')] \models \alpha \rightarrow \beta$. Se $[M, (r', c')] \models \alpha$ e $[M, (r', c')] \models \neg\alpha \vee \beta$ $(\alpha \rightarrow \beta \equiv \neg\alpha \vee \beta)$, então $[M, (r', c')] \models \beta$, para todo (r', c'). Portanto, $[M, (r, c)] \models \overline{H}_i\beta$.

2 Se $[M,(r,c)] \models \overline{H}_i\alpha$, então para todo (r',c') tal que $((r,c) \simeq_i (r',c'))$, $[M,(r',c')] \models \alpha$. Uma vez que $\simeq_i$ é reflexiva, segue que $((r,c) \simeq_i (r,c))$. Logo, $[M,(r,c)] \models \alpha$.

3 Suponha que $[M,(r,c)] \models \overline{H}_i\alpha$. Considere um estado (r',c') tal que $((r,c) \simeq_i (r',c'))$ e um (r'',c'') tal que $((r',c') \simeq_i (r'',c''))$. Uma vez que $\simeq_i$ é transitiva, então $((r,c) \simeq_i (r'',c''))$, e portanto $[M,(r'',c'')] \models \alpha$. Se temos $[M,(r'',c'')] \models \alpha$ para todo (r'',c'') tal que $((r',c') \simeq_i (r'',c''))$, então $[M,(r',c')] \models \overline{H}_i\alpha$. Assim, para todo (r',c') tal que $((r,c) \simeq_i (r',c'))$, temos $[M,(r',c')] \models \overline{H}_i\alpha$. Logo, $[M,(r,c)] \models \overline{H}_i\overline{H}_i\alpha$.

4 Suponha que $[M,(r,c)] \models \neg\overline{H}_i\alpha$. Então, existe algum (r',c') tal que $((r,c) \simeq_i (r',c'))$ e $[M,(r',c')] \models \neg\alpha$. Suponha que existe (r'',c'') tal que $((r,c) \simeq_i (r'',c''))$. Uma vez que $\simeq_i$ é simétrica, segue que $((r'',c'') \simeq_i (r,c))$. Como $((r,c) \simeq_i (r',c'))$, e $\simeq_i$ é transitiva, temos também que $((r'',c'') \simeq_i (r',c'))$. Segue que $[M,(r'',c'')] \models \neg\overline{H}_i\alpha$, para todo (r'',c''). Logo, $[M,(r,c)] \models \overline{H}_i\neg\overline{H}_i\alpha$.

Uma vez que $\approx_i$ e $\sim_i$ também são relações de equivalência, as provas de 5, 6, 7, 8 e 9, 10, 11, 12 são análogas às provas 1, 2, 3, 4 acima.

Como 13, 14, 15 são os axiomas de Shehtman e Gabbay para o produto de lógicas pseudo-transitivas ou fechadas, as provas de corretude e completude podem ser encontradas em [33].

16 Segue direto da regra semântica 7, definição 6.2.4.

17 Segue direto da regra semântica 8, definição 6.2.4.

18 Segue direto da regra semântica 9, definição 6.2.4.

19 Para provar que $M \models K_i\alpha \leftrightarrow Q_iK_i\alpha$ é válido, provaremos que $M \models K_i\alpha \rightarrow Q_iK_i\alpha$ e $M \models Q_iK_i\alpha \rightarrow K_i\alpha$.

$M \models K_i\alpha \rightarrow Q_iK_i\alpha$ (direção $\rightarrow$). Suponha que $[M,(r,c)] \models K_i\alpha$. Uma vez que $\sim_i$ é, por definição, o fecho transitivo sob a união de $\simeq_i$ e $\approx_i$, é fácil checar que $[M,(r,c)] \models K_i\alpha \rightarrow Q_i\alpha$. Portanto, substitutindo α por $K_i\alpha$, temos que $[M,(r,c)] \models K_iK_i\alpha \rightarrow Q_iK_i\alpha$. Pelo axioma 11 (cuja validade já provamos) temos também que $M \models K_i\alpha \rightarrow K_iK_i\alpha$. Então, temos $[M,(r,c)] \models K_i\alpha$, $[M,(r,c)] \models K_i\alpha \rightarrow K_iK_i\alpha$ e $[M,(r,c)] \models K_iK_i\alpha \rightarrow Q_iK_i\alpha$. Consequentemente, podemos aplicar *modus ponens* duas vezes [1] e concluir que $[M,(r,c)] \models Q_iK_i\alpha$.

[1] Veja a prova do lema 7.1.3 para a validade da regra *modus ponens*

$M \models Q_i K_i \alpha \rightarrow K_i \alpha$ (direção $\leftarrow$). Suponha que $[M,(r,c)] \models Q_i K_i \alpha$. Então, $[M,(r,c)] \models H_i K_i \alpha$ e $[M,(r,c)] \models V_i K_i \alpha$. Já que as relações $\simeq_i$ e $\approx_i$ são reflexivas, concluímos, para ambos os casos, que $[M,(r,c)] \models K_i \alpha$. Logo, $M \models Q_i K_i \alpha \rightarrow K_i \alpha$.

20 Suponha que $[M,(r,c)] \models K_i(\alpha \rightarrow Q_i \alpha)$ e $[M,(r,c)] \models \alpha$. Uma vez que $\sim_i$ é reflexiva, então $[M,(r,c)] \models (\alpha \rightarrow Q_i \alpha)$. Como $[M,(r,c)] \models (\alpha \rightarrow Q_i \alpha)$ e $[M,(r,c)] \models \alpha$, temos $[M,(r,c)] \models Q_i \alpha$, isto é, $[M,(r,c)] \models H_i \alpha$ e $[M,(r,c)] \models V_i \alpha$. Usando o axioma 19, provado no ítem anterior, se $[M,(r,c)] \models K_i(\alpha \rightarrow Q_i \alpha)$ então $[M,(r,c)] \models Q_i K_i(\alpha \rightarrow Q_i \alpha)$, e portanto $[M,(r,c)] \models H_i K_i(\alpha \rightarrow Q_i \alpha)$ e $[M,(r,c)] \models V_i K_i(\alpha \rightarrow Q_i \alpha)$. Logo, seguindo a direção horizontal, para todo (r',c') tal que $((r,c) \simeq_i (r',c'))$ temos $[M,(r',c')] \models K_i(\alpha \rightarrow Q_i \alpha)$. Sabemos também que $[M,(r,c)] \models H_i \alpha$ e, portanto, podemos concluir que $[M,(r',c')] \models \alpha$. Da mesma forma, para todo (r'',c'') que é verticalmente alcançável de (r,c), temos $[M,(r'',c'')] \models K_i(\alpha \rightarrow Q_i \alpha)$ e $[M,(r'',c'')] \models \alpha$. Logo, para todo (r',c') e (r'',c'') que é alcançável em um passo a partir de (r,c) podemos refazer o raciocínio e sempre concluir α para qualquer outro estado que é alcançável horizontalmente ou verticalmente a partir de (r',c') ou (r'',c''). Portanto, por indução, para todo (r_j,c_j) alcançável partindo-se de (r,c) num caminho de passos horizontais e/ou verticais, temos $[M,(r_j,c_j)] \models \alpha$. Logo, $[M,(r,c)] \models K_i \alpha$.

$\triangle$

Lema 7.1.3 *Para toda fórmula bem formada α e $\beta \in L_m^2$, e todo $i = 1,2,\ldots,m$:*

1 *Se $M \models \alpha$ e $M \models \alpha \rightarrow \beta$, então $M \models \beta$*

2 *Se $M \models \alpha$, então $M \models \overline{H}_i \alpha$*

3 *Se $M \models \alpha$, então $M \models \overline{V}_i \alpha$*

4 *Se $M \models \alpha$, então $M \models K_i \alpha$*

Prova do Lema 7.1.3.

1 Suponha que $M \models \alpha$, $M \models \alpha \rightarrow \beta$ e $M \not\models \beta$. Uma vez que $\alpha \rightarrow \beta \equiv \neg(\alpha \wedge \neg\beta)$, segue que $M \models \neg(\alpha \wedge \neg\beta)$ se e somente se $M \not\models \alpha \wedge \neg\beta$. Temos também, por hipótese, que $M \models \alpha$ e $M \models \neg\beta$, ou seja, $M \models \alpha \wedge \neg\beta$, o que é uma contradição. Logo, $M \models \beta$.

2 Suponha $M \models \alpha$ e $M \not\models \overline{H}_i\alpha$. Então, $M \models \neg\overline{H}_i\alpha$, isto é, existe um estado (r', c') tal que $(r, c) \simeq_i (r', c')$ e $[M, (r', c')] \models \neg\alpha$, o que contradiz a hipótese de que α é verdadeira em todos os estados de M, $M \models \alpha$. Logo, $M \models \overline{H}_i\alpha$.

3 Análogo ao ítem 2 para $\overline{V}_i\alpha$.

4 Análogo ao ítem 2 para $K_i\alpha$.

$\triangle$

Teorema 7.1.4 *Todo teorema de $\mathcal{S}_m^2$ é valido na classe de frames* **F**.

Prova do teorema 7.1.4.
É preciso provar que:

1. Todo axioma de $\mathcal{S}_m^2$ é valido na classe de frames **F**.

2. As regras $R1$ a $R4$ preservam a validade na classe de frames **F**.

Na verdade, 1. e 2. seguem diretamente dos lemas 7.1.2 e 7.1.3, respectivamente.
$\triangle$

7.2 Modelos Finitos para $\mathcal{S}_m^2$

Para provar a completude de $\mathcal{S}_m^2$ é necessário mostrar que toda fórmula válida na classe de frames **F** é um teorema de $\mathcal{S}_m^2$. Ou, de forma equivalente, é preciso provar que para toda fórmula φ $\mathcal{S}_m^2$-consistente existe um modelo baseado em um frame $F \in \mathbf{F}$ que satisfaz φ.

Na verdade, vamos provar que $\mathcal{S}_m^2$ tem a propriedade f.m.p., ou seja, mostraremos que para toda f.b.f. $\varphi \in L_m^2$ é possível construir um modelo finito que satisfaz φ.

Considere novamente a classe **F** de frames $F = (W, \simeq_i, \approx_i, \sim_i, A)$, onde $W = R \times C$, $A \subseteq W$ e as relações originais $\simeq_i, \approx_i$ são de equivalência.

Logo, precisamos:

1. Construir uma espécie de modelo canônico finito baseado numa f.b.f. qualquer $\varphi \in L_m^2$;

2. Provar que φ é verdadeira em algum estado deste modelo finito, ao qual chamaremos de φ-modelo;

3. Provar que o frame do φ-modelo está na classe **F**, isto é, que o frame do φ-modelo é reflexivo-transitivo-simétrico para as relações canônicas e que corresponde a um frame de um subproduto fechado.

A seguir, definimos o modelo canônico finito para φ, o φ-modelo, e então provamos os lemas 7.2.5 e 7.2.9 que correspondem a 2 e 3 acima.

O φ-modelo finito é, de fato, baseado nas subfórmulas de φ, porque, para produzir um modelo que satisfaz φ, só precisamos considerar os valores-verdade para suas subfórmulas.

Definição 7.2.1 *Subfórmulas de $\varphi \in L^2_m$.*

Considere $\varphi \in L^2_m$. Seja $Sub(\varphi)$ o conjunto $\{\alpha | \alpha$ é uma subfórmula de $\varphi\}$, mais as fórmulas:

1 $\Delta \wedge \overline{H}_i\alpha$ *para cada subfórmula* $H_i\alpha$ *de* φ*;*

2 $\Delta \wedge \overline{V}_i\alpha$ *para cada subfórmula* $V_i\alpha$ *de* φ*;*

3 $H_i\alpha \wedge V_i\alpha$ *para cada subfórmula* $Q_i\alpha$ *de* φ*;*

4 $Q_iK_i\alpha$ *para cada subfórmula* $K_i\alpha$ *de* φ*.*

Seja $Sub^+(\varphi)$ o conjunto $Sub(\varphi) \cup \{\neg\alpha | \alpha \in Sub(\varphi)\}$.

Definição 7.2.2 *Conjunto φ-maximal $\mathcal{S}^2_m$-consistente.*

Um conjunto Γ de f.b.f. é φ-maximal $\mathcal{S}^2_m$-consistente se e somente se $\Gamma \subseteq Sub^+(\varphi)$ e:

1. *Para toda $\alpha \in Sub(\varphi)$ ou $\alpha \in \Gamma$ ou $\neg\alpha \in \Gamma$ (φ-maximalidade);*

2. *Se $\Gamma = \{\gamma_1, \ldots, \gamma_n\}$ então não ocorre $\vdash \neg(\gamma_1 \wedge \ldots \gamma_n)$ ($\mathcal{S}^2_m$-consistência).*

Definição 7.2.3 *φ-frame finito.*

Seja $F^\varphi = (W^\varphi, \simeq^\varphi_i, \approx^\varphi_i, \sim^*_i, A^\varphi)$ o φ-frame finito para a f.b.f. $\varphi \in L^2_m$, onde:

1. *W^φ contem todos os conjuntos φ-maximais $\mathcal{S}^2_m$-consistentes;*

2. *As relações para w e $w' \in W^\varphi$ são:*

   1 $(w \simeq^\varphi_i w') \Leftrightarrow \forall\alpha(\overline{H}_i\alpha \in w \Leftrightarrow \overline{H}_i\alpha \in w')$

   2 $(w \approx^\varphi_i w') \Leftrightarrow \forall\alpha(\overline{V}_i\alpha \in w \Leftrightarrow \overline{V}_i\alpha \in w')$

   3 $(w \sim^*_i w') \Leftrightarrow (w, w') \in (\simeq^\varphi_i \cup \approx^\varphi_i)^*$, onde $(\simeq^\varphi_i \cup \approx^\varphi_i)^*$ denota o fecho transitivo sob a união de $\simeq^\varphi_i$ e $\approx^\varphi_i$

4 $A^{\varphi}(w) \Leftrightarrow \Delta \in w$

Definição 7.2.4 *φ-modelo finito.*

O φ-modelo finito M^{φ} para $\varphi \in L_m^2$ é um par $M^{\varphi} = (F^{\varphi}, v^{\varphi})$ sobre F^{φ} onde, para cada $p \in Prop = Prop_H \cup Prop_V$, $w \in v^{\varphi}(p) \Leftrightarrow p \in w$.

Lema 7.2.5 *Truth Lemma.*

Seja φ uma f.b.f. em L_m^2. Para toda $\alpha \in Sub(\varphi)$, e todo $w \in W^{\varphi}$: $\alpha \in w \Leftrightarrow (M^{\varphi}, w) \models \alpha$.

Prova do lema 7.2.5.

A prova é por indução no comprimento das subfórmulas $\alpha \in Sub(\varphi)$.

Hipótese de indução: para toda subfórmula $\alpha \in Sub(\varphi)$ com $|\alpha| \leq n$ vale o lema 7.2.5.

Provamos que o lema vale para a base ($\alpha \in Prop$) e então que também vale para $|\alpha| = n + 1$.

1. Base: $\alpha = p \in Prop$.

$(M^{\varphi}, w) \models p$	$\Leftrightarrow w \in v^{\varphi}(p)$	*satisfazibilidade*
	$\Leftrightarrow p \in w$	*definição do φ-modelo*

2. Conjunção: $\alpha \wedge \beta$.

$(M^{\varphi}, w) \models \alpha \wedge \beta$	$\Leftrightarrow (M^{\varphi}, w) \models \alpha$ e $(M^{\varphi}, w) \models \beta$	*satisfazibilidade*
	$\Leftrightarrow \alpha \in w$ e $\beta \in w$	*hipótese de indução*
	$\Leftrightarrow w \vdash \alpha$ e $w \vdash \beta$	*$\mathcal{S}_m^2$-consistência de w*
	$\Leftrightarrow w \vdash \alpha \wedge \beta$	
	$\Leftrightarrow \alpha \wedge \beta \in w$	*$\mathcal{S}_m^2$-consistência de w*

3. Negação: $\neg\alpha$.

$(M^{\varphi}, w) \models \neg\alpha$	$\Leftrightarrow (M^{\varphi}, w) \not\models \alpha$	*satisfazibilidade*
	$\Leftrightarrow \alpha \notin w$	*hipótese de indução*
	$\Leftrightarrow \neg\alpha \in w$	*φ-maximalidade de w*

4. Horizontal: $\overline{H}_i\alpha$.

$(M^{\varphi}, w) \models \overline{H}_i\alpha$	$\Leftrightarrow \forall w'((w \simeq_i^{\varphi} w') \Rightarrow (M^{\varphi}, w') \models \alpha)$	*satisfazibilidade*
	$\Leftrightarrow \forall w'((w \simeq_i^{\varphi} w') \Rightarrow \alpha \in w')$	*hipótese de indução*
	$\Leftrightarrow \overline{H}_i\alpha \in w$	*proposição 7.2.6*

5. Vertical: $\overline{V}_i\alpha$.

   Análogo ao ítem anterior.

6. Bidimensional: $K_i\alpha$.

$$
\begin{array}{lll}
(M^\varphi, w) \models K_i\alpha & \Leftrightarrow \forall w'((w \sim_i^* w') \Rightarrow (M^\varphi, w') \models \alpha) & \textit{satisfazibilidade} \\
& \Leftrightarrow \forall w'((w \sim_i^* w') \Rightarrow \alpha \in w') & \textit{hipótese de indução} \\
& \Leftrightarrow K_i\alpha \in w & \textit{proposição 7.2.6}
\end{array}
$$

7. Restrição: Δ.

$$
\begin{array}{lll}
(M^\varphi, w) \models \Delta & \Leftrightarrow w \in A^\varphi & \textit{satisfazibilidade} \\
& \Leftrightarrow \Delta \in w & \textit{definição de } A^\varphi
\end{array}
$$

8. Horizontal restrito: $H_i\alpha$.

$$
\begin{array}{lll}
\text{(Direção } \Rightarrow\text{)} & & \\
H_i\alpha \in w & \Rightarrow \Delta \wedge \overline{H}_i\alpha \in w & \textit{definição 7.2.1} \\
& \Rightarrow w \vdash \Delta \wedge \overline{H}_i\alpha & \mathcal{S}_m^2\textit{-consistência de } w \\
& \Rightarrow w \vdash \Delta \text{ e } w \vdash \overline{H}_i\alpha & \\
& \Rightarrow \Delta \in w \text{ e } \overline{H}_i\alpha \in w & \mathcal{S}_m^2\textit{-consistência de } w \\
& \Rightarrow (M^\varphi, w) \models \Delta \text{ e } (M^\varphi, w) \models \overline{H}_i\alpha & \textit{itens 4 e 7} \\
& \Rightarrow (M^\varphi, w) \models H_i\alpha & \textit{satisfazibilidade} \\
\text{(Direção } \Leftarrow\text{)} & & \\
(M^\varphi, w) \models H_i\alpha & \Rightarrow (M^\varphi, w) \models \Delta \text{ e } (M^\varphi, w) \models \overline{H}_i\alpha & \textit{satisfazibilidade} \\
& \Rightarrow \Delta \in w \text{ e } \overline{H}_i\alpha \in w & \textit{itens 4 e 7} \\
& \Rightarrow w \vdash \Delta \text{ e } w \vdash \overline{H}_i\alpha & \mathcal{S}_m^2\textit{-consistência de } w \\
& \Rightarrow w \vdash \Delta \wedge \overline{H}_i\alpha & \\
& \Rightarrow w \vdash H_i\alpha & \textit{axioma 16} \\
& \Rightarrow H_i\alpha \in w & \mathcal{S}_m^2\textit{-consistência de } w
\end{array}
$$

9. Vertical restrito: $V_i\alpha$.

   Análogo ao ítem anterior.

10. Passo interdimensional: $Q_i\alpha$

$$
\begin{array}{lll}
\text{(Direção } \Rightarrow\text{)} & & \\
Q_i\alpha \in w & \Rightarrow H_i\alpha \wedge V_i\alpha \in w & \textit{definição 7.2.1} \\
& \Rightarrow w \vdash H_i\alpha \wedge V_i\alpha & \mathcal{S}_m^2\textit{-consistência de } w \\
& \Rightarrow w \vdash H_i\alpha \text{ e } w \vdash V_i\alpha &
\end{array}
$$

	$\Rightarrow H_i\alpha \in w$ e $V_i\alpha \in w$	$\mathcal{S}^2_m$-*consistência de* w
	$\Rightarrow (M^\varphi, w) \models H_i\alpha$ e $(M^\varphi, w) \models V_i\alpha$	*itens 8 e 9*
	$\Rightarrow (M^\varphi, w) \models Q_i\alpha$	*satisfazibilidade*
(Direção $\Leftarrow$)		
$(M^\varphi, w) \models Q_i\alpha$	$\Rightarrow (M^\varphi, w) \models H_i\alpha$ e $(M^\varphi, w) \models V_i\alpha$	*satisfazibilidade*
	$\Rightarrow H_i\alpha \in w$ e $V_i\alpha \in w$	*itens 8 e 9*
	$\Rightarrow w \vdash H_i\alpha$ e $w \vdash V_i\alpha$	$\mathcal{S}^2_m$-*consistência de* w
	$\Rightarrow w \vdash H_i\alpha \wedge V_i\alpha$	
	$\Rightarrow w \vdash Q_i\alpha$	*axioma 18*
	$\Rightarrow Q_i\alpha \in w$	$\mathcal{S}^2_m$-*consistência of* w

$\triangle$

Proposição 7.2.6 *Para todo* w *e* $w' \in W^\varphi$*:*

1. $\overline{H}_i\alpha \in w \Leftrightarrow \forall w'((w \simeq_i^\varphi w') \Rightarrow \alpha \in w')$;
2. $\overline{V}_i\alpha \in w \Leftrightarrow \forall w'((w \approx_i^\varphi w') \Rightarrow \alpha \in w')$;
3. $K_i\alpha \in w \Leftrightarrow \forall w'((w \sim_i^* w') \Rightarrow \alpha \in w')$.

Prova da Proposição 7.2.6

1. $\overline{H}_i\alpha \in w \Leftrightarrow \forall w'((w \simeq_i^\varphi w') \Rightarrow \alpha \in w')$.

   (Direção $\Rightarrow$) $\overline{H}_i\alpha \in w \Rightarrow \forall w'((w \simeq_i^\varphi w') \Rightarrow \alpha \in w')$.

   Suponha $\overline{H}_i\alpha \in w$ e não é o caso que $\forall w'((w \simeq_i^\varphi w') \Rightarrow \alpha \in w')$:

   $\Rightarrow \exists w' \neg((w \simeq_i^\varphi w') \Rightarrow \alpha \in w')$
   $\Rightarrow \exists w' \neg(\neg(w \simeq_i^\varphi w')$ ou $\alpha \in w')$
   $\Rightarrow \exists w'((w \simeq_i^\varphi w')$ e $\neg\alpha \in w')$

   Pela definição de $\simeq_i^\varphi$, junto com a hipótese que $\overline{H}_i\alpha \in w$, temos também:

$\Rightarrow \overline{H}_i\alpha \in w'$	*definição de* $\simeq_i^\varphi$
$\Rightarrow w' \vdash \overline{H}_i\alpha$	$\mathcal{S}^2_m$-*consistência de* w'
$\Rightarrow w' \vdash \alpha$	axioma 2
$\Rightarrow \alpha \in w'$	$\mathcal{S}^2_m$-*consistência de* w'

Mas, como w' é um conjunto φ-maximal $\mathcal{S}_m^2$-consistente, $\neg\alpha \in w'$ e $\alpha \in w'$ é uma contradição.

Assim sendo, de $\overline{H}_i\alpha \in w$, concluímos $\forall w'((w \simeq_i^{\varphi} w') \Rightarrow \alpha \in w')$.

(Direção $\Leftarrow$) $\forall w'((w \simeq_i^{\varphi} w') \Rightarrow \alpha \in w') \Rightarrow \overline{H}_i\alpha \in w$.

Suponha$\forall w'((w \simeq_i^{\varphi} w') \Rightarrow \alpha \in w')$ e não é o caso que $\overline{H}_i\alpha \in w$. Logo, dado que w é um conjunto φ-maximal $\mathcal{S}_m^2$-consistente, $\neg\overline{H}_i\alpha \in w$.

Mostramos no lema 7.2.8 que se $\neg\overline{H}_i\alpha \in w \Rightarrow \exists w'((w \simeq_i^{\varphi} w')$ e $\neg\alpha \in w')$. Contudo, por hipótese, $\forall w'((w \simeq_i^{\varphi} w') \Rightarrow \alpha \in w')$. Logo, temos $\neg\alpha \in w'$ e $\alpha \in w'$, o que é uma contradição, porque w' é um conjunto φ-maximal $\mathcal{S}_m^2$-consistente.

Consequentemente, de $\forall w'((w \simeq_i^{\varphi} w') \Rightarrow \alpha \in w')$ concluímos $\overline{H}_i\alpha \in w$.

2. $\overline{V}_i\alpha \in w \Leftrightarrow \forall w'((w \approx_i^{\varphi} w') \Rightarrow \alpha \in w')$.

   Análogo ao ítem anterior.

3. $K_i\alpha \in w \Leftrightarrow \forall w'((w \sim_i^{*} w') \Rightarrow \alpha \in w')$.

   Considere as seguintes abreviações:

   $h_i\alpha := \neg H_i\neg\alpha$

   $v_i\alpha := \neg V_i\neg\alpha$

   $q_i\alpha := \neg Q_i\neg\alpha$

   $k_i\alpha := \neg K_i\neg\alpha$

   Portanto, damos a prova para:

   $k_i\alpha \in w \Leftrightarrow \exists w'((w \sim_i^{*} w')$ e $\alpha \in w')$

   (Direção $\Leftarrow$) $\exists w'((w \sim_i^{*} w')$ e $\alpha \in w') \Rightarrow k_i\alpha \in w$.

   A prova é por indução no comprimento n do caminho entre w e w'. Seja $\{w_0, w_1, w_2, \ldots, w_n\}$, onde $w = w_0$, $w' = w_n$, um caminho entre w e w' tal que $(w_i \simeq_i^{\varphi} w_{i+1})$ ou $(w_i \approx_i^{\varphi} w_{i+1})$, para todo $i = 0, \ldots, n-1$.

   Suponha que $\exists w'((w \sim_i^{*} w')$ e $\alpha \in w') \Rightarrow k_i\alpha \in w$, para uma sequência $\{w_0, w_1, w_2, \ldots, w_n\}$, onde $w = w_0$, $w' = w_n$, e $n \leq k$.

   Para $n = 1$:

$$
\begin{array}{lll}
\exists w'((w \sim_i^{*} w') \text{ e } \alpha \in w') & & \\
\quad \Rightarrow \exists w'(((w \simeq_i^{\varphi} w') \text{ ou } (w \approx_i^{\varphi} w')) \text{ e } \alpha \in w') & & \textit{definição de } \sim_i^{*} \\
\quad \Rightarrow h_i\alpha \in w \text{ ou } v_i\alpha \in w & & \textit{definições de } \simeq_i^{\varphi} \textit{ e } \approx_i^{\varphi} \\
\quad \Rightarrow w \vdash h_i\alpha \text{ ou } w \vdash v_i\alpha & & \mathcal{S}_m^2\textit{-consistência de } w
\end{array}
$$

$\Rightarrow w \vdash h_i\alpha \vee v_i\alpha$

$\Rightarrow w \vdash q_i\alpha$ *axioma 18*

$\Rightarrow w \vdash k_i\alpha$ *teorema* $K_i\alpha \rightarrow Q_i\alpha$

$\Rightarrow k_i\alpha \in w$ $\mathcal{S}_m^2$*-consistência de* w

Para $n = k+1$, existe uma sequência $\{w_0, \ldots, w_k, w_{k+1}\}$ tal que $(w_i \simeq_i^{\varphi} w_{i+1})$ ou $(w_i \approx_i^{\varphi} w_{i+1})$, para todo $i = 0, \ldots, k$, onde $w = w_0$, $w' = w_{k+1}$, e $\alpha \in w'$.

Como no caso de $n = 1$, para os dois últimos $\{w_k, w_{k+1}\}$, temos que $h_i\alpha \in w_k$ ou $v_i\alpha \in w_k$. Pela hipótese de indução, para a subsequência $\{w_0, \ldots, w_k\}$, a proposição vale. Então, concluímos:

$\{w_0, \ldots, w_k, w_{k+1}\}$, onde $w = w_0$, $w' = w_{k+1}$ e $\alpha \in w'$

$\Rightarrow k_ih_i\alpha \in w$ ou $k_iv_i\alpha \in w$ *hipótese de indução*

$\Rightarrow w \vdash k_ih_i\alpha$ ou $w \vdash k_iv_i\alpha$ $\mathcal{S}_m^2$*-consistência de* w

$\Rightarrow w \vdash k_ih_i\alpha \vee k_iv_i\alpha$

$\Rightarrow w \vdash k_iq_i\alpha$ *axioma 18*

$\Rightarrow w \vdash k_i\alpha$ *axioma 19*

$\Rightarrow k_i\alpha \in w$ $\mathcal{S}_m^2$*-consistência de* w

(Direção $\Rightarrow$) $k_i\alpha \in w \Rightarrow \exists w'((w \sim_i^* w')$ e $\alpha \in w')$.

Definição 7.2.7 *Seja a relação* $\sim_i^{\varphi}$ *como segue:*
$(w \sim_i^{\varphi} w') \Leftrightarrow \forall\alpha(K_i\alpha \in w \Leftrightarrow \alpha \in w')$.

O que queremos provar segue imediatamente de:

A : $k_i\alpha \in w \Rightarrow \exists w'((w \sim_i^{\varphi} w')$ e $\alpha \in w')$

B : $\sim_i^{\varphi} \subseteq \sim_i^*$

A prova para A é idêntica à do ítem 1.

Para a prova de B, suponha que $(w \sim_i^{\varphi} w')$. Como $w \in W^{\varphi}$ e $w' \in W^{\varphi}$ são conjuntos φ-maximal $\mathcal{S}_m^2$-consistentes, suas conjunções também são conjuntos finitos de fórmulas em L_m^2. Sejam $\hat{w}$ e $\hat{w'}$ as conjunções de fórmulas em w e w', respectivamente.

Considere o conjunto $V = \{v \mid w \sim_i^* v\}$ de estados alcançáveis a partir de w em caminhos finitos de passos horizontais e/ou verticais, isto é, todas as sequências $\{w_0, \ldots, w_n\}$ tais que $(w_i \simeq_i^{\varphi} w_{i+1})$ ou $(w_i \approx_i^{\varphi}$

w_{i+1}), para todo $i = 0, \ldots, n-1$, e $w = w_0$, $v = w_n$. Seja γ a disjunção de tais estados, $\gamma = \bigvee_{v \in V} \hat{v}$. Vamos mostrar que $w' \in V$.

Note que $\gamma \wedge q_i \neg\gamma$ é inconsistente com w, caso contrário $\gamma \wedge q_i \hat{w''}$ seria consistente para pelo menos um estado $w'' \notin V$, o que significaria que $\hat{v} \wedge q_i \hat{w''}$ seria consistente para pelo menos um $v \in V$, e portanto que $(v \sim_i^* w'')$, o que implicaria em $w'' \in V$, o que não ocorre.

Portanto, $\gamma \rightarrow Q_i\gamma$ é consistente. Pela regra de generalização de K_i, temos que $\vdash K_i(\gamma \rightarrow Q_i\gamma)$. Pelo axioma 20, temos então $\vdash \gamma \rightarrow K_i\gamma$. Como $w \in V$, então $\vdash \hat{w} \rightarrow \gamma$, e consequentemente $\vdash \hat{w} \rightarrow K_i\gamma$. Pela definição de $\sim_i^{\varphi}$, temos que $\hat{w} \wedge k_i \hat{w'}$ é consistente, e segue que $\hat{w} \wedge k_i(\hat{w'} \wedge \gamma)$ é consistente também. Mas isso significa que para um dos $\hat{v}$ da disjunção γ, $\hat{w'} \wedge \gamma$ é consistente. Comos w' e v são átomos, $w' = v$ e portanto $w' \in V$.

$\triangle$

Lema 7.2.8 *Considere $M^{\varphi} = (W^{\varphi}, \simeq_i^{\varphi}, \approx_i^{\varphi}, \sim_i^*, A^{\varphi}, v^{\varphi})$ o φ-modelo finito.*

1. *Se $\neg\overline{H}_i\alpha \in w$, então existe um v tal que $(w \simeq_i^{\varphi} v)$ e $\neg\alpha \in v$.*
2. *Se $\neg\overline{V}_i\alpha \in w$, então existe um v tal que $(w \approx_i^{\varphi} v)$ e $\neg\alpha \in v$.*

Prova do lema 7.2.8

A prova é a análoga para ambos os ítens, então vamos provar somente para $\overline{H}_i\alpha$.

Suponha que $\neg\overline{H}_i\alpha \in w$. Vamos construir um v tal que $(w \simeq_i^{\varphi} v)$ e $\neg\alpha \in v$.

Seja $v' = \{\neg\alpha\} \cup \{\overline{H}_i\psi \mid \overline{H}_i\psi \in w\}$.

Provaremos que v' é consistente. Logo, é suficiente tomar qualquer extensão φ-maximal $\mathcal{S}_m^2$-consistente de v' como o conjunto v que estamos procurando. Por construção, v será um conjunto φ-maximal $\mathcal{S}_m^2$-consistente tal que $(w \simeq_i^{\varphi} v)$, ou seja, para todo ψ, se $\overline{H}_i\psi \in w$, então $\overline{H}_i\psi \in v$, e $\neg\alpha \in v$.

Agora é preciso provar que $v' = \{\neg\alpha\} \cup \{\overline{H}_i\psi \mid \overline{H}_i\psi \in w\}$ é consistente.

Suponha que v' é inconsistente. Então, existem $\psi_1, \ldots, \psi_n$ tais que:

1.	$\vdash (\overline{H}_i\psi_1 \wedge \ldots \wedge \overline{H}_i\psi_n) \rightarrow \alpha$	*def. de consistência*
2.	$\vdash \overline{H}_i((\overline{H}_i\psi_1 \wedge \ldots \wedge \overline{H}_i\psi_n) \rightarrow \alpha)$	*generalização $\overline{H}_i$*
3.	$\vdash \overline{H}_i(\overline{H}_i\psi_1 \wedge \ldots \wedge \overline{H}_i\psi_n) \rightarrow \overline{H}_i\alpha$	*axioma 1*
4.	$\vdash \overline{H}_i\overline{H}_i\psi_1 \wedge \ldots \wedge \overline{H}_i\overline{H}_i\psi_n \rightarrow \overline{H}_i(\overline{H}_i\psi_1 \wedge \ldots \wedge \overline{H}_i\psi_n)$	
5.	$\vdash \overline{H}_i\overline{H}_i\psi_1 \wedge \ldots \wedge \overline{H}_i\overline{H}_i\psi_n \rightarrow \overline{H}_i\alpha$	*3. e 4.*
6.	$\vdash \overline{H}_i\psi_1 \wedge \ldots \wedge \overline{H}_i\psi_n \rightarrow \overline{H}_i\alpha$	*axioma 3*

Como $\overline{H}_i\psi_1 \wedge \ldots \wedge \overline{H}_i\psi_n \in w$, então $\overline{H}_i\alpha \in w$. Mas, por hipótese, também temos que $\neg\overline{H}_i\alpha \in w$, o que é uma contradição, porque w é um conjunto φ-maximal $\mathcal{S}5^2_m$-consistente. Consequentemente, v' é consistente.

$\triangle$

Lema 7.2.9 *O frame finito F^φ pertence a classe* **F**.

A *O frame F^φ é reflexivo-transitivo-simétrico para $\simeq_i^\varphi$, $\approx_i^\varphi$ e $\sim_i^*$.*

B *O frame F^φ corresponde a um frame de um subproduto fechado.*

Prova do lema 7.2.9, parte A.

É fácil verificar que as relações $\simeq_i^\varphi$ e $\approx_i^\varphi$ são, por definição, relações reflexivas, transitivas e simétricas, então F^φ é reflexivo-transitivo-simétrico para ambas $\simeq_i^\varphi$ e $\approx_i^\varphi$. Dado que $\sim_i^*$ é o fecho transitivo sob $\simeq_i^\varphi$ e $\approx_i^\varphi$, então F^φ também é reflexivo-transitivo-simétrico para $\sim_i^*$.

Prova do lema 7.2.9, parte B.

Como dissemos anteriormente, se as relações de possibilidade são definidas como relações de equivalência, então lógicas polimodais como L_H e L_V são axiomatizáveis por $\mathcal{S}5_m$ [20].

Sabemos que, pelos resultados apresentados no capítulo 5, o produto $\mathcal{S}5_m \times \mathcal{S}5_m$ é comutativo, e portanto a lógica resultante é axiomatizada por $[\mathcal{S}5_m, \mathcal{S}5_m]$.

Neste caso, o sistema axiomático $[\mathcal{S}5_m, \mathcal{S}5_m]$ é constituído dos seguintes axiomas e regras:

Axiomas.

0 Todas as tautologias do cálculo proposicional

1 $(\overline{H}_i\alpha \wedge \overline{H}_i(\alpha \rightarrow \beta)) \rightarrow \overline{H}_i\beta$

2 $\overline{H}_i\alpha \rightarrow \alpha$

3 $\overline{H}_i\alpha \rightarrow \overline{H}_i\overline{H}_i\alpha$

4 $\neg\overline{H}_i\alpha \rightarrow \overline{H}_i\neg\overline{H}_i\alpha$

5 $(\overline{V}_i\alpha \wedge \overline{V}_i(\alpha \rightarrow \beta)) \rightarrow \overline{V}_i\beta$

6 $\overline{V}_i\alpha \rightarrow \alpha$

7 $\overline{V}_i\alpha \rightarrow \overline{V}_i\overline{V}_i\alpha$

8 $\neg\overline{V}_i\alpha \rightarrow \overline{V}_i\neg\overline{V}_i\alpha$

13 $\overline{H}_i\overline{V}_j\alpha \leftrightarrow \overline{V}_j\overline{H}_i\alpha$

14 $\neg\overline{H}_i\neg\overline{V}_j\alpha \rightarrow \overline{V}_j\neg\overline{H}_i\neg\alpha$

15 $\neg\overline{V}_i\neg\overline{H}_j\alpha \rightarrow \overline{H}_j\neg\overline{V}_i\neg\alpha$

onde $i, j = 1, \ldots, m$.

Regras.

R0 De $\vdash \alpha$ derive toda substituição uniforme para α

R1 De $\vdash \alpha, \alpha \rightarrow \beta$ derive β (modus ponens)

R2 De $\vdash \alpha$ derive $\overline{H}_i\alpha$ (*generalização horizontal*)

R3 De $\vdash \alpha$ derive $\overline{V}_i\alpha$ (*generalização vertical*)

Além disso, como a lógica de $\mathcal{S}5_m$ é canônica, pela proposição 5.3.8, o produto $\mathcal{S}5_m \times \mathcal{S}5_m$ é canônico.

Logo, o subframe $F^{\varphi}_{\times} = (W^{\varphi}, \simeq^{\varphi}_i, \approx^{\varphi}_i)$ do frame F^{φ}, constituído apenas das relações horizontais e verticais, é um frame produto.

Portanto, para provar que o frame F^c é um subproduto, restaria mostrar que a relação canônica do fecho $\sim^*_i$ está bem definida, ou seja:

$K_i\alpha \in w \Leftrightarrow \forall w'((w \sim^*_i w') \Rightarrow \alpha \in w')$.

Mas isto já foi provado no ítem 3 da proposição 7.2.6.

$\triangle$

7.3 Model-Checking

Em geral, o problema de verificar se uma fórmula φ é verdadeira num frame de Kripke é conhecido como *model-checking problem*. Apresentamos uma prova de que, para toda f.b.f. $\varphi \in L^2_m$, é possível construir um modelo finito M^{φ} que satisfaz φ. Como M^{φ} é finito, então existe um procedimento efetivo para checar se φ é verdadeira em M^{φ}. O próximo passo seria, então, verificar a quantidade de recursos, tempo e/ou memória, necessários para decidir se a fórmula é verdadeira.

Proposição 7.3.1 *Seja uma fórmula $\varphi \in L^2_m$, $\mid \varphi \mid$ o comprimento de φ e $\parallel W^{\varphi} \parallel$ o tamanho do frame F^{φ}.*

Existe um algoritmo que, dado o modelo M^{φ} sobre o frame F^{φ} e um estado $w \in F^{\varphi}$ determina, num tempo $O(\parallel W^{\varphi} \parallel \times \mid \varphi \mid)$, se $M^{\varphi} \models \varphi$.

Prova. Sejam $\varphi_1, \ldots, \varphi_n$ as subfórmulas de φ ordenadas por tamanho, ou seja, $\varphi_n = \varphi$ e se φ_i é uma subfórmula de φ_j então $i < j$. Existem no máximo $\mid \varphi \mid$ subfórmulas de φ, logo temos que $n \leq \mid \varphi \mid$. Podemos rotular cada estado em M^φ com φ_j ou $\neg\varphi_j$, dependendo se φ_j é verdadeira ou não em w, e isto pode ser feito num tempo $O((n+c)\times \parallel W^\varphi \parallel)$, onde c é uma constante que se refere ao tempo adicional para rotular as subfórmulas com os operadores modais.

$\triangle$

Capítulo 8

Lógica Bidimensional para Conhecimento Comum Concorrente

Sabemos que o conhecimento comum requer ações simultâneas e portanto não pode ser alcançado durante a execução de um algoritmo distribuído num sistema assíncrono, onde tais ações não são possíveis. Assim sendo, procuramos identificar outros conceitos de conhecimento em grupo que capturassem as características do modelo para sistemas assíncronos descrito no capítulo 3.

Encontramos no conhecimento comum concorrente o tipo de acordo procurado, ou seja, um tipo de conhecimento em grupo alcançável em ambientes assíncronos. Vimos também que uma semântica formal para conhecimento comum concorrente foi definida em [31], porém não foi apresentado um sistema axiomático correspondente.

Com a nova abordagem que propomos de interpretar os pares de estados (r, c) - execução assíncrona r e corte consistente c - sob uma perpectiva bidimensional, como o produto de duas lógicas modais, a avaliação das fórmulas da linguagem do conhecimento comum concorrente torna-se natural, em consequência da própria definição semântica. Por exemplo, a interpretação das fórmulas que envolvem o operador P_i no contexto de uma lógica bidimensional é direta: a fórmula $P_i\alpha$ significa que existe um corte indistinguível sob o ponto de vista do agente i, na mesma execucão, onde α é verdadeira. Logo, o operador P_i corresponde, de fato, ao dual do operador V_i da lógica bidimensional de conhecimento.

Desta forma, propomos uma axiomatização do conhecimento comum concorrente: o sistema $\mathcal{C}_m^2$, que é, na verdade, uma extensão do sistema $\mathcal{S}_m^2$ apresentado anteriormente.

Neste capítulo apresentamos o sistema $\mathcal{C}_m^2$ e as respectivas provas de corretude e completude. Introduzimos uma interpretação grafo-teórica do conhecimento comum concorrente que é crucial para a prova de corretude de $\mathcal{C}_m^2$. Para ilustrar, terminamos com alguns exemplos de conhecimento comum concorrente.

8.1 Incorporando Conhecimento Mútuo Concorrente e Conhecimento Comum Concorrente

Já temos todos os elementos para definir uma lógica bidimensional para conhecimento comum concorrente. Para tanto, vamos reunir aqui tudo o que foi dito até então sobre semântica bidimensional para sistemas distribuídos assíncronos e conhecimento concorrente.

A linguagem da lógica para conhecimento comum concorrente é a mesma da lógica bidimensional de conhecimento acrescida dos operadores E_C, para conhecimento mútuo concorrente, e C_C, para conhecimento comum concorrente. A lógica bidimensional para conhecimento comum concorrente é definida como segue.

Definição 8.1.1 *Lógica Bidimensional para Conhecimento Comum Concorrente LC_m^2.*

Seja a lógica LC_m^2 o menor conjunto de fórmulas bem formadas contendo a constante Δ, o conjunto de primitivas $Prop = Prop_H \cup Prop_V$, fechado sob negação, conjunção e os operadores modais H_i, V_i, K_i, E_C e C_C onde $i = 1, \ldots, m$.

A definição de satisfazibilidade em LC_m^2 é a mesma de L_m^2 acrescida de três regras para os operadores P_i (na realidade o dual de V_i), E_C e C_C, conforme abaixo.

Definição 8.1.2 *Satisfazibilidade em LC_m^2.*

Seja $F = (W, \simeq_i, \approx_i, \sim_i)$ um frame para LC_m^2 e seja M um modelo sobre F. Uma fórmula $\alpha \in LC_m^2$ é verdadeira em $[M, (r, c)]$, $[M, (r, c)] \models \alpha$, para $(r, c) \in W = R \times C$, quando:

1. $[M, (r, c)] \models p \Leftrightarrow (r, c) \in v(p)$, *onde* $p \in Prop$;
2. $[M, (r, c)] \models \alpha \wedge \beta \Leftrightarrow [M, (r, c)] \models \alpha$ *e* $[M, (r, c))] \models \beta$;
3. $[M, (r, c)] \models \neg\alpha \Leftrightarrow [M, (r, c)] \not\models \alpha$;

4. $[M,(r,c)] \models \overline{H}_i\alpha \Leftrightarrow \forall(r',c')\{((r,c) \simeq_i (r',c')) \Rightarrow [M,(r',c')] \models \alpha\}$;

5. $[M,(r,c)] \models \overline{V}_i\alpha \Leftrightarrow \forall(r',c')\{((r,c) \approx_i (r',c')) \Rightarrow [M,(r',c')] \models \alpha\}$;

6. $[M,(r,c)] \models \Delta \Leftrightarrow (r,c) \in A \subseteq W = R \times C$;

7. $[M,(r,c)] \models H_i\alpha \Leftrightarrow [M,(r,c)] \models \Delta$ *e* $[M,(r,c)] \models \overline{H}_i\alpha$;

8. $[M,(r,c)] \models V_i\alpha \Leftrightarrow [M,(r,c)] \models \Delta$ *e* $[M,(r,c)] \models \overline{V}_i\alpha$;

9. $[M,(r,c)] \models Q_i\alpha \Leftrightarrow [M,(r,c)] \models H_i\alpha$ *e* $[M,(r,c)] \models V_i\alpha$;

10. $[M,(r,c)] \models K_i\alpha \Leftrightarrow [M,(r,c)] \models \Delta$ *e* $\forall(r',c')\{((r,c) \sim_i (r',c')) \Rightarrow [M,(r',c')] \models \alpha\}$;

11. $[M,(r,c)] \models P_i\alpha \Leftrightarrow [M,(r,c)] \models \neg V_i \neg\alpha$;

12. $[M,(r,c)] \models E_C\alpha \Leftrightarrow [M,(r,c)] \models \bigwedge K_iP_i\alpha$;

13. $[M,(r,c)] \models C_C\alpha \Leftrightarrow [M,(r,c)] \models E_C^k\alpha$ *para todo* $k \geq 1$.

8.2 Sistema Axiomático $\mathcal{C}_m^2$

Uma axiomatização da lógica bidimensional LC_m^2 é dada pelo sistema $\mathcal{S}_m^2$ (apresentado no capítulo 6, seção 6.3) acrescido dos axiomas para conhecimento mútuo concorrente E_C, e conhecimento comum concorrente C_C. A este novo sistema damos o nome de $\mathcal{C}_m^2$.

Portanto, considere $\mathcal{C}_m^2$ o sistema axiomático para a lógica bidimensional de conhecimento comum concorrente, LC_m^2, constituído dos seguintes axiomas e regras.

Axiomas.

0 Todas as tautologias do cálculo proposicional

1 $(\overline{H}_i\alpha \wedge \overline{H}_i(\alpha \rightarrow \beta)) \rightarrow \overline{H}_i\beta$

2 $\overline{H}_i\alpha \rightarrow \alpha$

3 $\overline{H}_i\alpha \rightarrow \overline{H}_i\overline{H}_i\alpha$

4 $\neg\overline{H}_i\alpha \rightarrow \overline{H}_i\neg\overline{H}_i\alpha$

5 $(\overline{V}_i\alpha \wedge \overline{V}_i(\alpha \rightarrow \beta)) \rightarrow \overline{V}_i\beta$

6 $\overline{V}_i\alpha \rightarrow \alpha$

7 $\overline{V}_i\alpha \rightarrow \overline{V}_i\overline{V}_i\alpha$

8 $\neg\overline{V}_i\alpha \rightarrow \overline{V}_i\neg\overline{V}_i\alpha$

9 $(K_i\alpha \wedge K_i(\alpha \rightarrow \beta)) \rightarrow K_i\beta$

10 $K_i\alpha \rightarrow \alpha$

11 $K_i\alpha \rightarrow K_iK_i\alpha$ [1]

12 $\neg K_i\alpha \rightarrow K_i\neg K_i\alpha$

13 $\overline{H}_i\overline{V}_j\alpha \leftrightarrow \overline{V}_j\overline{H}_i\alpha$

14 $\neg\overline{H}_i\neg\overline{V}_j\alpha \rightarrow \overline{V}_j\neg\overline{H}_i\neg\alpha$

15 $\neg\overline{V}_i\neg\overline{H}_j\alpha \rightarrow \overline{H}_j\neg\overline{V}_i\neg\alpha$

16 $H_i\alpha \leftrightarrow \Delta \wedge \overline{H}_i\alpha$

17 $V_i\alpha \leftrightarrow \Delta \wedge \overline{V}_i\alpha$

18 $Q_i\alpha \leftrightarrow H_i\alpha \wedge V_i\alpha$

19 $K_i\alpha \leftrightarrow Q_iK_i\alpha$

20 $K_i(\alpha \rightarrow Q_i\alpha) \rightarrow (\alpha \rightarrow K_i\alpha)$

21 $P_i\alpha \leftrightarrow \neg V_i\neg\alpha$

22 $E_C\alpha \leftrightarrow \bigwedge K_iP_i\alpha$

23 $C_C\alpha \leftrightarrow E_C(\alpha \wedge C_C\alpha)$

onde $i, j = 1, \ldots, m$.

Regras.

R0 De $\vdash \alpha$ derive toda substituição uniforme para α

R1 De $\vdash \alpha, \alpha \rightarrow \beta$ derive β (modus ponens)

R2 De $\vdash \alpha$ derive $\overline{H}_i\alpha$ (*generalização horizontal*)

R3 De $\vdash \alpha$ derive $\overline{V}_i\alpha$ (*generalização vertical*)

R4 De $\vdash \alpha$ derive $K_i\alpha$ (*generalização bidimensional*)

R5 De $\vdash \alpha \rightarrow E_C(\alpha \wedge \beta)$ derive $\alpha \rightarrow C_C\beta$ (*regra da indução*)

[1] Este axioma é obtido dos axiomas 19 e 20.

8.3 Corretude para $\mathcal{C}^2_m$

Vamos provar a corretude do sistema $\mathcal{C}^2_m$ em relação à classe de frames que correspondem a subprodutos fechados de lógicas modais $S5_m$. Como vimos anteriormente, é preciso demonstrar que todos os axiomas do sistema são válidos nesta classe e que as regras de inferência preservam a validade.

Repetimos a seguir a definição da classe de frames para a qual desejamos provar a corretude de $\mathcal{C}^2_m$ e a seguir enunciamos e provamos os dois lemas da corretude.

Definição 8.3.1 *Classe de frames* **F**.

Seja **F** *a classe de frames* $F = (W, \simeq_i, \approx_i, \sim_i, A)$, *onde* $W = R \times C$, $A \subseteq W$, *as relações* $\simeq_i, \approx_i$ *são relações de equivalência e* $\sim_i$ *é o fecho transitivo sob as duas primeiras, conforme a definição 6.1.1. Ou seja,* **F** *é a classe de frames de subprodutos fechados de duas dimensões onde as relações básicas são relações de equivalência.*

Lema 8.3.2 *Seja* M *um modelo sobre* F.

Para toda fórmula bem formada (f.b.f.) α *e* $\beta \in LC^2_m$, *e todo* $i, j = 1, 2, \ldots, m$:

1 $M \models (\overline{H}_i\alpha \wedge \overline{H}_i(\alpha \rightarrow \beta)) \rightarrow \overline{H}_i\beta$

2 $M \models \overline{H}_i\alpha \rightarrow \alpha$

3 $M \models \overline{H}_i\alpha \rightarrow \overline{H}_i\overline{H}_i\alpha$

4 $M \models \neg\overline{H}_i\alpha \rightarrow \overline{H}_i\neg\overline{H}_i\alpha$

5 $M \models (\overline{V}_i\alpha \wedge \overline{V}_i(\alpha \rightarrow \beta)) \rightarrow \overline{V}_i\beta$

6 $M \models \overline{V}_i\alpha \rightarrow \alpha$

7 $M \models \overline{V}_i\alpha \rightarrow \overline{V}_i\overline{V}_i\alpha$

8 $M \models \neg\overline{V}_i\alpha \rightarrow \overline{V}_i\neg\overline{V}_i\alpha$

9 $M \models (K_i\alpha \wedge K_i(\alpha \rightarrow \beta)) \rightarrow K_i\beta$

10 $M \models K_i\alpha \rightarrow \alpha$

11 $M \models K_i\alpha \rightarrow K_iK_i\alpha$

12 $M \models \neg K_i\alpha \rightarrow K_i\neg K_i\alpha$

13 $M \models \overline{H}_i\overline{V}_j\alpha \leftrightarrow \overline{V}_j\overline{H}_i\alpha$

14 $M \models \neg\overline{H}_i\neg\overline{V}_j\alpha \rightarrow \overline{V}_j\neg\overline{H}_i\neg\alpha$

15 $M \models \neg\overline{V}_i\neg\overline{H}_j\alpha \rightarrow \overline{H}_j\neg\overline{V}_i\neg\alpha$

16 $M \models H_i\alpha \leftrightarrow \Delta \wedge \overline{H}_i\alpha$

17 $M \models V_i\alpha \leftrightarrow \Delta \wedge \overline{V}_i\alpha$

18 $M \models Q_i\alpha \leftrightarrow H_i\alpha \wedge V_i\alpha$

19 $M \models K_i\alpha \leftrightarrow Q_iK_i\alpha$

20 $M \models K_i(\alpha \rightarrow Q_i\alpha) \rightarrow (\alpha \rightarrow K_i\alpha)$

21 $M \models P_i\alpha \leftrightarrow \neg V_i\neg\alpha$

22 $M \models E_C\alpha \leftrightarrow \bigwedge K_iP_i\alpha$

23 $M \models C_C\alpha \leftrightarrow E_C(\alpha \wedge C_C\alpha)$

Prova do Lema 8.3.2.

As provas para os ítens 1 a 20 foram dadas no capítulo 7, seção 7.1. Os ítens 21 e 22 seguem imediatamente das regras semânticas 11 e 12, respectivamente.

Portanto, falta apenas o ítem 23: $M \models C_C\alpha \leftrightarrow E_C(\alpha \wedge C_C\alpha)$.

Para a prova do ítem 23, utilizamos uma caracterização grafo-teórica de conhecimento comum concorrente, no sentido que propomos pensar no conhecimento concorrente em termos de pontos alcançáveis e caminhos traçados por estes pontos. Tal caracterização é enunciada na Proposição 8.3.4 adiante. Primeiramente, apresentamos algumas definições.

Considere W_Δ o conjunto de pontos (r, c) tal que $M, (r, c) \models \Delta$. Sejam $w, w', w'', w_n \in W_\Delta, n \geq 0$.

Definimos a seguir um ponto w' como sendo, respectivamente, K_i-alcançável, V_i-alcançável, K_iV_i-alcançável e KV-alcançável a partir de w em n KV-passos.

Definição 8.3.3 *K_i-alcançável, V_i-alcançável, K_iV_i-alcançável e KV-alcançável em n KV-passos.*

1. *w' é K_i-alcançável a partir de w se e somente se $w \sim_i^* w'$;*

2. *w' é V_i-alcançável a partir de w se e somente se $w \approx_i^* w'$;*

3. *w' é K_iV_i-alcançável a partir de w se e somente se existe um w'' tal que $w \sim_i^* w''$ e $w'' \approx_i^* w'$;*

4. *w' é KV-alcançável a partir de w em n KV-passos se e somente se existem pontos $w_0, w_1, \ldots, w_n$ tais que, $w = w_0$, $w' = w_n$, e para todo j, $0 \leq j \leq n-1$ temos w_{j+1} é K_iV_i-alcançável a partir de w_j, $i \in \{1, 2, \ldots, m\}$.*

Proposição 8.3.4 *Interpretação grafo-teórica de conhecimento comum concorrente.*

a) $M, w \models E_C\alpha$ se e somente se, para todo $i \in \{1, 2, \ldots, m\}$:
para todo w' K_iV_i-alcançável a partir de w, temos que $M, w' \models \alpha$;

b) $M, w \models E_C^k\alpha$ se e somente se, para todo $i \in \{1, 2, \ldots, m\}$:
para todo w' KV-alcançável a partir de w em k KV-passos temos que $M, w' \models \alpha$;

c) $M, w \models C_C\alpha$ se e somente se, para todo $i \in \{1, 2, \ldots, m\}$:
para todo w' KV-alcançável a partir de w em n KV-passos, para qualquer $n > 0$, temos que $M, w' \models \alpha$.

Prova da Proposição 8.3.4.
A parte *a*) segue da definição de conhecimento mútuo concorrente. Lembrando que $M, w \models E_C^{k+1}\alpha \Leftrightarrow M, w \models E_C(E_C^k\alpha)$, a parte *b*) segue direto por indução em k. A parte *c*) é imediata a partir de *b*) e da definição de conhecimento comum concorrente.
$\triangle$

Vamos utilizar a caracterização grafo-teórica do conhecimento comum concorrente da proposição 8.3.4 para concluir a prova do lema 8.3.2.

23: $M \models C_C\alpha \leftrightarrow E_C(\alpha \wedge C_C\alpha)$.
Direção $\rightarrow$:
Supor que $M, w \models C_C\alpha$. Logo, $M, w' \models \alpha$ para todo w' KV-alcançável a partir de w em n KV-passos, $n > 0$. Em particular, se w'' é KV-alcançável a partir de w em um KV-passo temos que $M, w'' \models \alpha$ e $M, w' \models \alpha$ para todo w' KV-alcançável a partir de w'' em n KV-passos, $n > 0$. Portanto, $M, w'' \models \alpha \wedge C_C\alpha$ para todo w'' KV-alcançável a partir de w em um KV-passo. Logo, $M, w \models E_C(\alpha \wedge C_C\alpha)$.
Direção $\leftarrow$:
Supor que $M, w \models E_C(\alpha \wedge C_C\alpha)$. Seja w' KV-alcançável a partir de w em n KV-passos, $n > 0$, e seja w'' um ponto no caminho de w' tal que w''

é o primeiro ponto KV-alcançável a partir de w em um KV-passo. Já que $M, w \models E_C(\alpha \wedge C_C\alpha)$, segue que $M, w'' \models \alpha \wedge C_C\alpha$. Assim sendo, temos dois casos: ou $w' = w''$ ou w' é KV-alcançável a partir de w'' em n KV-passos. No primeiro caso, $M, w' \models \alpha$, uma vez que $M, w'' \models \alpha$. No segundo caso, pela proposição 8.3.4 e o fato de que $M, w'' \models C_C\alpha$, temos que $M, w' \models \alpha$. Então, para todo w' KV-alcançável a partir de w em n KV-passos, $n > 0$, temos que $M, w' \models \alpha$. Logo, $M, w \models C_C\alpha$.

△

Lema 8.3.5 *Para toda fórmula bem formada α e $\beta \in LC_m^2$, e todo $i = 1, 2, \ldots, m$:*

1 *Se $M \models \alpha$ e $M \models \alpha \rightarrow \beta$, então $M \models \beta$*

2 *Se $M \models \alpha$, então $M \models \overline{H}_i\alpha$*

3 *Se $M \models \alpha$, então $M \models \overline{V}_i\alpha$*

4 *Se $M \models \alpha$, então $M \models K_i\alpha$*

5 *Se $M \models \alpha \rightarrow E_C(\alpha \wedge \beta)$, então $M \models \alpha \rightarrow C_C\beta$*

Prova do Lema 8.3.5.

As provas dos ítens 1 a 4 foram dadas no capítulo 7, seção 7.1.

Segue então a prova do ítem

5: Se $M \models \alpha \rightarrow E_C(\alpha \wedge \beta)$, então $M \models \alpha \rightarrow C_C\beta$

Supor que $M, w \models \alpha \rightarrow E_C(\alpha \wedge \beta)$ e $M, w \models \alpha$. Vamos provar por indução em n que para todo w' KV-alcançável a partir de w em n KV-passos, $n > 0$, temos que $M, w' \models \alpha \wedge \beta$, e, portanto, que $M, w \models C_C(\alpha \wedge \beta)$.

Caso $n = 1$.

Supor w' KV-alcançável a partir de w em um KV-passo. Uma vez que $M, w \models \alpha \rightarrow E_C(\alpha \wedge \beta)$ e $M, w \models \alpha$ então $M, w \models E_C(\alpha \wedge \beta)$. Como w' é KV-alcançável a partir de w em um KV-passo, pela proposição 8.3.4, temos que $M, w' \models \alpha \wedge \beta$.

Caso $n = n' + 1$.

Se $n = n' + 1$, então existe um w' KV-alcançável a partir de w em n' KV-passos tal que w'' é KV-alcançável a partir de w' em um KV-passo. Pela hipótese de indução, temos que $M, w' \models \alpha \wedge \beta$. O mesmo argumento do caso base, $n = 1$, mostra que $M, w'' \models \alpha \wedge \beta$, pois $M \models \alpha \rightarrow E_C(\alpha \wedge \beta)$.

△

8.4 Completude para $\mathcal{C}_m^2$

O operador C_C para conhecimento comum concorrente, assim como o operador para conhecimento comum, também é infinitário se consideramos sua definição como uma conjunção infinita. Poderíamos pensar, então, que não é possível caracterizá-lo através de um conjunto finito de axiomas. Porém, a caracterização do conhecimento comum concorrente através de ponto fixo, conforme o axioma 23 do sistema $\mathcal{C}_m^2$, além de correta, segundo o que já demonstramos, é também completa, conforme provaremos a seguir. Neste caso, mostraremos que toda fórmula $\mathcal{C}_m^2$-consistente é satisfatível em relação a classe de frames de subprodutos fechados.

Considere novamente a classe $\mathbf{F}$ como a classe de frames do tipo $F = (W, \simeq_i, \approx_i, \sim_i, A)$, onde $W = R \times C$, $A \subseteq W$, as relações $\simeq_i, \approx_i$ são relações de equivalência e $\sim_i$ é o fecho transitivo sob as relações básicas.

Para a prova de completude vamos construir modelos finitos. Ou seja, vamos provar que $\mathcal{C}_m^2$ tem a propriedade f.m.p.

A demonstração é essencialmente igual à da seção 7.2, faltando apenas a prova para as fórmulas contendo os operadores de conhecimento concorrente E_C e C_C. Portanto, vamos repetir as definições necessárias, com algumas alterações, e apresentar as provas para E_C e C_C.

Definição 8.4.1 *Subfórmulas de $\varphi \in LC_m^2$.*

Considere $\varphi \in LC_m^2$. Seja $Sub(\varphi)$ o conjunto $\{\alpha | \alpha$ é uma subfórmula de $\varphi\}$, mais as fórmulas:

1 $\Delta \wedge \overline{H}_i\alpha$ *para cada subfórmula* $H_i\alpha$ *de* φ*;*

2 $\Delta \wedge \overline{V}_i\alpha$ *para cada subfórmula* $V_i\alpha$ *de* φ*;*

3 $H_i\alpha \wedge V_i\alpha$ *para cada subfórmula* $Q_i\alpha$ *de* φ*;*

4 $Q_iK_i\alpha$ *para cada subfórmula* $K_i\alpha$ *de* φ*;*

5 $K_iP_i\alpha$ *para cada subfórmula* $E_C\alpha$ *de* φ*;*

6 $E_C(\alpha \wedge C_C\alpha)$ *para cada subfórmula* $C_C\alpha$ *de* φ*.*

Seja $Sub^+(\varphi)$ o conjunto $Sub(\varphi) \cup \{\neg\alpha | \alpha \in Sub(\varphi)\}$.

Definição 8.4.2 *Conjunto φ-maximal $\mathcal{C}_m^2$-consistente.*

Um conjunto Γ de f.b.f. é φ-maximal $\mathcal{C}_m^2$-consistente se e somente se $\Gamma \subseteq Sub^+(\varphi)$ e:

1. *Para toda $\alpha \in Sub(\varphi)$ ou $\alpha \in \Gamma$ ou $\neg\alpha \in \Gamma$ (φ-maximalidade);*

2. *Se* $\Gamma = \{\gamma_1, \ldots, \gamma_n\}$ *então não ocorre* $\vdash \neg(\gamma_1 \wedge \ldots \gamma_n)$ *(C_m^2-consistência).*

Definição 8.4.3 *φ-frame finito.*

Seja $F^\varphi = (W^\varphi, \simeq_i^\varphi, \approx_i^\varphi, \sim_i^*, A^\varphi)$ *o φ-frame finito para a f.b.f.* $\varphi \in LC_m^2$, *onde:*

1. W^φ *contem todos os conjuntos φ-maximal C_m^2-consistentes;*

2. *As relações para* w *e* $w' \in W^\varphi$ *são:*

   1 $(w \simeq_i^\varphi w') \Leftrightarrow \forall\alpha(\overline{H}_i\alpha \in w \Leftrightarrow \overline{H}_i\alpha \in w')$

   2 $(w \approx_i^\varphi w') \Leftrightarrow \forall\alpha(\overline{V}_i\alpha \in w \Leftrightarrow \overline{V}_i\alpha \in w')$

   3 $(w \sim_i^* w') \Leftrightarrow (w, w') \in (\simeq_i^\varphi + \approx_i^\varphi)^*$, onde $(\simeq_i^\varphi + \approx_i^\varphi)^*$ denota o fecho transitivo sob a união de $\simeq_i^\varphi$ e $\approx_i^\varphi$

   4 $A^\varphi(w) \Leftrightarrow \Delta \in w$

Definição 8.4.4 *φ-modelo finito.*

O φ-modelo finito M^φ para $\varphi \in LC_m^2$ é um par $M^\varphi = (F^\varphi, v^\varphi)$ sobre F^φ onde, para cada $p \in Prop = Prop_H \cup Prop_V$, $w \in v^\varphi(p) \Leftrightarrow p \in w$.

Lema 8.4.5 *Truth Lemma.*

Seja φ qualquer f.b.f. em LC_m^2. Para toda $\alpha \in Sub(\varphi)$, e todo $w \in W^\varphi$: $\alpha \in w \Leftrightarrow (M^\varphi, w) \models \alpha$.

Prova do lema 8.4.5.

Como vimos, a prova é por indução no comprimento das subfórmulas $\alpha \in Sub(\varphi)$.

Hipótese de indução: para toda subfórmula $\alpha \in Sub(\varphi)$ com $|\alpha| \leq n$ vale o lema 8.4.5.

Provaremos que o lema vale para a base ($\alpha \in Prop$) e então que também vale para $|\alpha| = n+1$. Os argumentos para os casos em que α é uma proposição primitiva (caso base), uma conjunção, uma negação, ou das formas $\overline{H}_i\alpha$, $\overline{V}_i\alpha$, Δ, $H_i\alpha$, $V_i\alpha$, $Q_i\alpha$ ou $K_i\alpha$ são idênticas as provas da seção 7.2. A seguir, a prova para os casos $E_C\alpha$ e $C_C\alpha$. Vale lembrar que $P_i\alpha$ é uma abreviação para $\neg V_i \neg\alpha$.

1. Conhecimento mútuo concorrente: $E_C\alpha \in w \Leftrightarrow (M^\varphi, w) \models E_C\alpha$.

   (Direção $\Rightarrow$)

   $E_C\alpha \in w \quad \Rightarrow K_iP_i\alpha \in w \quad$ *w é φ-maximal C_m^2-consistente*

   $\Rightarrow (M^\varphi, w) \models K_iP_i\alpha \quad$ *ítem 6 do lema 7.2.5*

$$
\begin{array}{lll}
 & \Rightarrow (M^{\varphi}, w) \models E_C\alpha & \textit{satisfazibilidade} \\
\text{(Direção } \Leftarrow\text{)} & & \\
(M^{\varphi}, w) \models E_C\alpha \Rightarrow & (M^{\varphi}, w) \models K_iP_i\alpha & \textit{satisfazibilidade, para todo } i \\
 & \Rightarrow K_iP_i\alpha \in w & \textit{ítem 6 do lema 7.2.5} \\
 & \Rightarrow w \vdash K_iP_i\alpha & \textit{C^2_m-consistência de } w \\
 & \Rightarrow w \vdash E_C\alpha & \textit{axioma 22} \\
 & \Rightarrow E_C\alpha \in w & \textit{C^2_m-consistência de } w
\end{array}
$$

2. Conhecimento comum concorrente : $C_C\alpha \in w \Leftrightarrow (M^{\varphi}, w) \models C_C\alpha$.

   Direção ($\Rightarrow$): $C_C\alpha \in w \Rightarrow (M^{\varphi}, w) \models C_C\alpha$.

   Vamos provar que:

   (*) Se $C_C\alpha \in w$ então, para todo w' KV-alcançável a partir de w em n KV-passos, para qualquer $n > 0$, temos que $\alpha \in w'$ e $C_C\alpha \in w'$.

   Pela hipótese de indução principal, temos $\alpha \in w' \Leftrightarrow (M^{\varphi}, w') \models \alpha$. A proposição 8.3.4 garante que, para todo w' KV-alcançável a partir de w em n KV-passos, para qualquer $n > 0$, temos $(M^{\varphi}, w') \models \alpha \Leftrightarrow (M^{\varphi}, w) \models C_C\alpha$. Logo, teremos provado $C_C\alpha \in w \Rightarrow (M^{\varphi}, w) \models C_C\alpha$.

   A prova de (*) é por por indução em n.

   Caso base: $n = 1$.

   Seja w' KV-alcançável a partir de w em um KV-passo. Suponha que $C_C\alpha \in w$. Então:

$$
\begin{array}{lll}
C_C\alpha \in w & \Rightarrow E_C(\alpha \wedge C_C\alpha) \in w & \textit{w é φ-maximal C^2_m-consistente} \\
 & \Rightarrow (M^{\varphi}, w) \models E_C(\alpha \wedge C_C\alpha) & \textit{ítem 1 acima} \\
 & \Rightarrow \alpha \wedge C_C\alpha \in w' & \textit{proposição 8.3.4} \\
 & \Rightarrow w' \vdash \alpha \wedge C_C\alpha & \textit{C^2_m-consistência de } w \\
 & \Rightarrow w' \vdash \alpha \text{ e } w' \vdash C_C\alpha & \\
 & \Rightarrow \alpha \in w' \text{ e } C_C\alpha \in w' & \textit{C^2_m-consistência de } w
\end{array}
$$

   Hipótese de indução: $n = n'$

   - Se $C_C\alpha \in w$ então, para todo w' KV-alcançável a partir de w em n' KV-passos, para qualquer $n' > 0$, temos que $\alpha \in w'$ e $C_C\alpha \in w'$.

Provaremos para $n = n' + 1$.

Seja w'' KV-alcançável a partir de w em $n' + 1$ KV-passos. Então existe w' tal que w' é KV-alcançável a partir de w em n' KV-passos e w'' é KV-alcançável a partir de w' em um KV-passo. Pela hipótese de indução, ambos $\alpha \in w'$ e $C_G\alpha \in w'$. O mesmo argumento usado para o caso base pode então ser usado para mostrar que $\alpha \in w''$ e $C_G\alpha \in w''$.

Direção ($\Leftarrow$): $(M^\varphi, w) \models C_G\alpha \Rightarrow C_G\alpha \in w$.

Suponha $(M^\varphi, w) \models C_G\alpha$. Como $w \in W^\varphi$ é φ-maximal $\mathcal{C}_m^2$-consistente, a conjunção das subfórmulas em w também é uma fórmula finita em LC_m^2. Seja $\hat{w}$ a conjunção das fórmulas em w.

Considere o conjunto $V = \{v \in W^\varphi | (M^\varphi, v) \models C_G\alpha\}$ de estados que satisfazem $C_G\alpha$. Seja γ a disjunção de tais estados, $\gamma = \bigvee_{v \in V} \hat{v}$. Como V é finito, então γ é uma fórmula de LC_m^2 e pode ser vista como a fórmula que caracteriza os estados onde $C_G\alpha$ é verdadeira.

Observe que $\gamma \rightarrow E_G(\alpha \wedge \gamma)$ é $\mathcal{C}_m^2$-consistente, portanto, temos que $\vdash \gamma \rightarrow E_G(\alpha \wedge \gamma)$. Pela regra da indução R5, temos então $\vdash \gamma \rightarrow C_G\alpha$. Como $w \in V$, então $\vdash \hat{w} \rightarrow \gamma$, e consequentemente $\vdash \hat{w} \rightarrow C_G\alpha$ (**). Logo, $C_G\alpha \in w$, pois $\neg C_G\alpha$ junto com (**) faria w $\mathcal{C}_m^2$-inconsistente.

$\triangle$

8.5 Exemplos de Conhecimento Comum Concorrente

1. Broadcast de Mensagens

   Um dos exemplos do uso de conhecimento comum concorrente envolve a difusão ou *broadcast* de informações. Em geral, a difusão de uma série de mensagens em sequência não garante que elas cheguem na mesma ordem em todos os pontos da rede, mesmo que os canais sejam *fifo*, pois as mensagens podem seguir por rotas distintas e com diferentes velocidades de transmissão. Contudo, em [31] temos um teorema relacionando uma condição suficiente para garantir que as mensagens cheguem na ordem correta em todos os nós.

Teorema 8.5.1 *Ordenação de Broadcast.*

Considere que $\rho(\phi_k)$ significa que "a mensagem ϕ_k foi recebida por todos os agentes".

Se o agente i sabe $P_i(\rho(\phi_k))$ antes de iniciar o broadcast de ϕ_{k+1} então ϕ_k chega antes de ϕ_{k+1} em todos os agentes.

A prova para este teorema encontra-se em [31]. A idéia intuitiva da prova é a seguinte: considere c' o corte indistinguível para i onde vale $\rho(\phi_k)$; se uma mensagem ϕ_{k+1} enviada por i chegasse a j antes da mensagem ϕ_k, então o corte c' não seria consistente!

O teorema acima não implica que todos os outros processos além do iniciador também sabem que receberam as mensagens na ordem correta. Contudo, se for de conhecimento comum que $K_i P_i(\rho(\phi_k))$ é uma pré-condição para o iniciador começar o broadcast da mensagem ϕ_{k+1}, então todos os processos saberão que todas as mensagens chegam na ordem certa.

Este exemplo ilustra uma situação onde $K_i(\rho(\phi_k))$ não precisa ser alcançado, apenas um conhecimento mais fraco, $K_i P_i(\rho(\phi_k))$ é suficiente para executar uma ação. Uma vez que não é necessário saber que todas as mensagens foram recebidas no estado atual, mas, ao invés disso, é suficiente saber $P_i(\rho(\phi_k))$, o tempo de latência na espera por mensagens de confirmação é eliminado.

Assim sendo, o algoritmo para alcançar conhecimento comum concorrente apresentado na seção 4.3 pode ser usado para garantir que múltiplas mensagens enviadas a todos os processos cheguem na ordem correta. Neste caso, o fato $\rho(\phi_k)$ torna-se de conhecimento comum concorrente.

2. Algoritmo para Propagação de Informação com Feedback

   Como o algoritmo PIF que apresentamos na seção 3.1 é um algoritmo para difusão de informações, que implementa o algoritmo para obtenção de conhecimento comum concorrente, temos que o conhecimento comum concorrente de $\rho(\phi_k)$ é alcançado por todos os agentes antes do final do algoritmo. Para provar isto, basta encontrar um conjunto τ de cortes localmente distinguíveis onde vale $\rho(\phi_k)$. Na verdade, existe uma série de tais conjuntos, mas considere, por exemplo um conjunto $\tau = (c_4, c_{12})$. É fácil verificar nas figuras 6.1 e 6.2 que estes cortes são de fato localmente distinguíveis e que satisfazem $\rho(\phi_k)$. Logo, embora o conhecimento comum de $\rho(\phi_k)$, ou seja, o conhecimento comum de que todos receberam a mensagem nunca seja alcançado, $C_C(\rho(\phi_k))$ é alcançado, isto é, o conhecimento comum concorrente de que todos recebem a mensagem é obtido muito antes do final de qualquer execução.

3. Replicação de Dados

Neste exemplo utiliza-se o resultado da ordenação de mensagens obtido no exemplo sobre broadcast de mensagens para construir um algoritmo que mantém a consistência de atualizações em dados replicados.

Seja x um dado replicado e x_M a cópia de x para o site mestre, que chamaremos de agente M. Suponha que M, necessita fazer uma série de atualizações $Op_1, Op_2, \ldots$ em x de modo que todas as atualizações ocorram na mesma ordem em todas as cópias de x. Considere ψ_k como sendo "a operação Op_k foi executada por M". No primeiro exemplo acima vimos que o algoritmo para alcançar conhecimento comum concorrente apresentado na seção 4.3 pode ser usado para garantir que múltiplas mensagens enviadas a todos os processos cheguem na ordem correta. Logo, um protocolo que implemente o referido algoritmo onde cada processo executa a operação Op_k imediatamente após alcançar seu estado de corte, ou seja, depois de aprender $C_C\rho(\psi_k)$, resolve o problema.

Supondo canais *fifo* e tomando o algoritmo para obtenção de conhecimento comum concorrente da seção 4.3 como base, temos o seguinte algoritmo:

Algoritmo para Atualização de Dados Replicados

- O mestre M, depois de executar a operação Op_k e antes de executar a operação Op_{k+1}, manda a mensagem $send_M^j(\psi_k)$ para todo vizinho j, e, imediatamente, alcança seu estado de corte. Depois de mandar a primeira mensagem e até alcançar seu estado de corte, M não recebe mensagens.
- Todos os outros processos i, ao receberem a mensagem $send_j^i(\psi_k)$ pela primeira vez, mandam a mensagem $send_i^k(\psi_k)$ para todos os vizinhos $k \neq j$, ou seja, exceto aquele vizinho do qual receberam a mensagem pela primeira vez, e , imediatamente, alcançam seu estado de corte. Depois de mandar a primeira mensagem e até alcançar seu estado de corte, i não recebe mensagens.

Este algoritmo é muito mais eficiente quando comparado com os métodos convencionais de ordenação de operações, que, em geral, requerem um número ilimitado de mensagens, uma vez que associam a cada operação um número de ordem, e armazenam as operações até que números mais baixos sejam processados.

Contudo, é importante notar que mesmo o conhecimento comum concorrente das operações não garante que múltiplas atualizações concorrentes de outros sites sejam efetuadas na ordem correta: se o agente i torna ϕ_1 de conhecimento comum concorrente e o agente j torna ϕ_2 de conhecimento comum concorrente, alguns agentes podem executar Op_1 enquanto outros executam Op_2 primeiro. Desta forma, o algoritmo apresentado é útil somente em atualizações do tipo *master-slave*.

Capítulo 9

Conclusão

Este trabalho apresenta resultados sobre lógicas epistêmicas e lógicas multidimensionais com aplicações na área de sistemas distribuídos multiagentes. Apresentamos os sistemas axiomáticos S_m^2 e C_m^2 para lógicas modais bidimensionais de conhecimento e conhecimento comum concorrente, respectivamente. Fornecemos as provas de corretude e completude para estes sistemas. Provas para a propriedade de modelos finitos também são apresentadas, donde concluímos que os respectivos problemas de provabilidade e validade para estas lógicas são decidíveis.

Acreditamos que uma das contribuições práticas mais interessantes desta dissertação é a formalização de uma nova abordagem epistêmica para ambientes distribuídos mais próximos da realidade, ou seja, para ambientes assíncronos multiagentes de troca de mensagens. Muitos ambientes reais, como a maioria das aplicações para a Internet, constituem ambientes distribuídos assíncronos onde o conceito de conhecimento comum concorrente de alguns fatos pode ser usado como pré-requisito para a especificação de certas ações concorrentes. Por exemplo, se o problema em questão envolve disseminação de informações, o conhecimento comum concorrente de certos fatos pode ser usado como pré-condição. Sabe-se que o conhecimento comum concorrente pode ser usado como um tipo de acordo apropriado em qualquer algoritmo distribuído que envolva a análise de propriedades de um estado global. É possível que o conceito de conhecimento comum concorrente tenha um espectro de aplicabilidade que vai além da área de algoritmos distribuídos.

As contribuições teóricas deste trabalho se dão, principalmente, no sentido de ampliar o campo de pesquisa das lógicas epistêmicas numa direção que está se tornando uma tendência em lógica: a de combinar lógicas a fim de melhor expressar as propriedades desejadas. A lógica bidimensional de conhecimento abre a possibilidade de modelar conhecimento iterativo num ambiente assíncrono, porque sua semântica é baseada na noção de cortes

consistentes (ou estados globais) e execuções assíncronas, características do modelo amplamente divulgado de Lamport [25]. Além disso, o uso do produto de lógicas multidimensionais para lidar com o conhecimento é um diferencial em relação a abordagem das lógicas epistêmicas tradicionais. A idéia de termos duas lógicas, cada uma para tratar de um ponto de vista distinto - pontos de vista de execuções e cortes - e utilizar o produto das lógicas para modelar o conhecimento dos agentes é uma contribuição nova. Para tanto, definimos o conhecimento como o fecho transitivo das relações do produto, criando o conceito de subproduto fechado de lógicas modais.

A interpretação da lógica bidimensional de conhecimento no contexto de sistemas distribuídos multiagentes é apenas uma de, talvez, diversas outras interpretações possíveis para este formalismo. Podemos supor uma interpretação para simulações financeiras na bolsa de valores, onde os agentes têm diferentes possibilidades de compra e venda de ações. O conhecimento comum concorrente sobre a venda ou compra de certas ações por determinados agentes pode decidir sobre a compra ou venda de outras ações, já que todos sabem que, mais cedo ou mais tarde, todos os outros agentes da bolsa saberão de todas as movimentações. Provavelmente, qualquer situação onde o conhecimento de determinados fatos é alcançado por todos os agentes não simultaneamente, porém *mais cedo ou mais tarde*, pode ser descrito em termos de algo como o conhecimento comum concorrente e, portanto, formalizado através da lógica que apresentamos.

Como desenvolvimentos futuros deste trabalho gostaríamos de citar algumas linhas de pesquisa. A primeira diz respeito a uma versão temporal da lógica bidimensional de conhecimento. Na verdade, não estamos sugerindo acrescentar mais uma dimensão temporal, pois o estado onde as fórmulas são avaliadas já possui um componente temporal, isto é, os cortes consistentes. O que desejamos é estender a presente lógica acrescentando operadores modais de tempo a fim de permitir as noções de *antes* e *depois* relativas ao corte consistente (ou estado global atual), o que pode aumentar significativamente o poder expressivo da lógica.

Uma segunda vertente de desenvolvimento deste trabalho seria considerar uma extensão híbrida da lógica bidimensional de conhecimento. A idéia é acrescentar operadores nominais, isto é, dar *nome* aos estados, e, talvez, operadores para quantificação sobre os estados [4], o que permitiria falar de estados específicos e de determinadas propriedades sobre alguns ou mesmo sobre todos os estados. Por exemplo, gostaríamos de ter expressividade para formalizar as propriedades do conjunto de *cortes localmente distinguíveis* descritos na seção 4.3, que é uma condição suficiente para atingir conhecimento comum concorrente.

Bibliografia

[1] Aumann, R. J. (1976). *Agreeing to disagree.* In: Annals of statistics v. 4, n. 6, pp. 1236-1239.

[2] Barbosa, V. C. (1996). *An Introduction to Distributed Algorithms.* MIT Press, Massachusets, U.S.A.

[3] Barwise, J. (1989). *On the model theory of common knowledge.* In: The situation in logic, CSLI lecture notes, pp. 201-220, Center for the Study of Language and Information, Stanford University, U.S.A.

[4] Blackburn, P., Tzakova, M. (1999). *Hybrid languages and temporal logic* Logic Journal of the IGPL, v.7., pp. 27-54.

[5] Chellas, B. (1980). *Modal Logic, An Introduction.* Cambridge UP, Cambridge, U.K.

[6] Costa, V., Benevides, M. R., and Barbosa, V. C. (1999). *Rumo a uma lógica bidimensional de conhecimento em sistemas distribuídos assíncronos.* XII Encontro Brasileiro de Lógica 99, pp. 95-103, Itatiaia, RJ.

[7] Costa, V. and Benevides, M. R. (2002). *A two-dimensional modal logic for knowledge representation in asynchronous multi-agent systems.* In: Proceedings of the International Conference on Artificial Intelligence (IC-AI'02) vol. III. H.R. Arabnia and Youngsong Mun Editors, Las Vegas, Nevada, USA.

[8] Duc H.N. (2001). *Resource-bounded reasoning about knowledge.* Ph.D. Dissertation, Universidade de Leipzig, Alemanha.

[9] Finger M., Gabbay D. (1992). *Adding a temporal dimension to a logical system.* Journal of Logic Language and Information v. 1, pp. 203-233.

[10] Finger M., Gabbay D. (1996). *Combining temporal logic systems.* Notre Dame Journal of Formal Logic, v. 37(2), pp. 204-232.

[11] Gabbay D., Kurucz A., Wolter F., Zakharyaschev M. *Many-dimensional modal logics: theory and applications* (in preparation, to appear with Elsevier Science), url: www.dcs.kcl.ac.uk/staff/mz/GKWZ/gkwz.html.

[12] Geanakoplos, J. D. (1992) *Common Knowledge.* Journal of Economic Perspectives 6, pp. 53-82.

[13] Gerbrandy, J. (1997) *Dynamic Epistemis Logic.* In: ILLC Research Report, Amsterdam University, NL.

[14] Halpern, J. Y. e Fagin, R. (1985). *A formal model of knowledge, action, and communication in distributed systems: preliminary report.* In: Proceedings of the ACM Symposium on Principles of Distributed Computing, pp. 224-236.

[15] Halpern, J. Y. (1986). *Reasoning about Knowledge: an overview.* In: Proceedings of the 1st Conference on Theoretical Aspects of Reasoning about Knowledge, pp. 1-17, Monterey, CA, U.S.A.

[16] Halpern, J. Y. and Fagin, R. (1989). *Modelling knowledge and action in distributed systems.* Distributed Computing 3(4), pp. 159-177.

[17] Halpern, J. Y. and Y. Moses (1990). *Knowledge and common knowledge in a distributed environment.* Journal of the ACM, v. 37 n. 3, pp. 549-587.

[18] Halpern, J. Y. and Y. Moses (1992). *A guide to completeness and complexity for modal logics of knowledge and belief.* Artificial Intelligence 54, pp. 319-379.

[19] Halpern, J. Y. and L. D. Zuck (1992). *A little knowledge goes a long way: knowledge-based derivations and correctness proofs for a family of protocols.* Journal of the ACM v. 39 n. 3, pp. 449-478.

[20] Halpern, J. Y., R. Fagin, Y. Moses and M. Y. Vardi (1995). *Reasoning about knowledge.* MIT Press, Massachusets, U.S.A.

[21] Hintikka, J. (1962). *Knowledge and belief.* Cornell UP, Ithaca, NY, U.S.A.

[22] Hintikka, J. (1986). *Reasoning About Knowledge in Philosophy: The Paradigm of Epistemic Logic.* In: Proceedings of the 1st Conference on Theoretical Aspects of Reasoning about Knowledge, pp. 63-80, Monterey, CA, U.S.A.

[23] Hoek W. van der, Thijsse E. (2002). *A General Approach to Multi-Agent Minimal Knowledge.* accepted for Studia Logica, 2002.

[24] Hughes, G. E, Cresswell, M.J. (1996). *A New Introduction to Modal Logic.* Routledge, London and New York.

[25] Lamport, L. (1978). *Time, clocks and the ordering of events in a distributed system.* Communications of the ACM v. 21 n. 7, pp. 558-565.

[26] Lamport, L., Chandy, M. (1985). *Distributed Snapshots: Determining Global States of a Distributed System.* ACM Transactions on Computer Systems v. 3, n. 1, pp.63-75. *Time, clocks and the ordering of events in a distributed system.* Communications of the ACM v. 21 n. 7, pp. 558-565.

[27] Lehmann, D. (1984). *Knowledge, common knowledge and related puzzles.* In: Proceedings of 3rd ACM Symposium on Principles of Distributed Computing, pp. 62-67, Vancouver, BC, Canada.

[28] Lehmann, D., Kraus, S. (1988). *Knowledge, belief and time.* Theoretical Computer Science, 58 n. 1-3, pp. 155-174.

[29] Lewis, D. (1969). *Convention.* Harvard University Press Cambridge, MA, U.K.

[30] Meyden, R. van der (1998). *Common Knowledge and Update in Finite Environments.* Information and Computation v. 140, n. 2, pp. 115-157. A preliminary version of this paper appeared in Proceedings of the Conference on Theoretical Aspects of Reasoning about Knowledge, Pacific Grove CA, March 1994.

[31] Panangaden, P. and K. Taylor (1992). *Concurrent Common Knowledge: defining agreement for asynchronous systems.* Distributed Computing 6, pp. 73-93.

[32] Segerberg, K. (1973). *Two-dimensional modal logics.* Journal of Philosophical Logic, v. 2, pp. 77-96.

[33] Shehtman, V. B. and D. M. Gabbay (1998). *Products of Modal Logics, part 1.* L. J. of the IGPL, v. 6, n. 1, pp. 73-146.

[34] Shehtman, V. B. (1998). *Two-dimensional modal logics and relativised quantifiers.* Advances in Modal Logics II. Uppsala, Sweden.

[35] Schiffer, S. R. (1972). *Meaning.* Clarendon, Oxford, U.K.

[36] Wolter, F. and M. Kracht (1991). *Properties of independently axiomatizable bimodal logics.* The Journal of Symbolic Logic, v. 56, n. 4, pp. 1469-1485.

[37] Wolter, F. (1994). *What is the upper part of the lattice of bimodal logics?* Studia Logica, v. 53, n. 2, pp. 234-241.