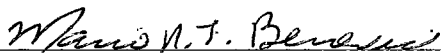


UMA LÓGICA MODAL BIDIMENSIONAL PARA REPRESENTAÇÃO
DO CONHECIMENTO EM SISTEMAS DISTRIBUÍDOS
MULTIAGENTES

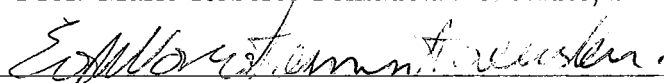
Vania Costa

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.

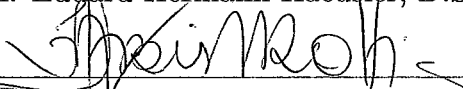
Aprovada por:



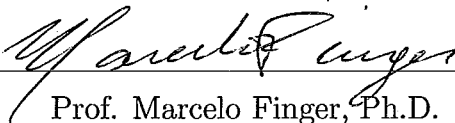
Prof. Mário Roberto Folhadela Benevides, Ph.D.



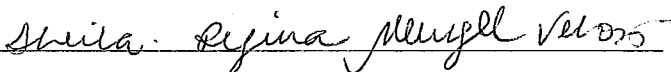
Prof. Eduard Hermann Haeusler, D.Sc.



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 correte 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

1	Introdução	1
1.1	Motivação	1
1.2	Organização da Tese	5
2	Lógicas de Conhecimento em um Grupo de Agentes	7
2.1	Sintaxe para as Lógicas de Conhecimento	8
2.2	Semântica para as Lógicas de Conhecimento	9
2.3	Sistemas Axiomáticos de Conhecimento	10
2.3.1	O Sistema Axiomático \mathcal{K}_m	10
2.3.2	Outros Sistemas Axiomáticos de Conhecimento	10
2.4	Estados de Conhecimento Relacionados ao Grupo de Agentes .	11
2.5	Sistemas Axiomáticos para Conhecimento em Grupo	13
2.6	Comunicação e Conhecimento em Ambientes Distribuídos . . .	14
2.6.1	O Problema do Ataque Coordenado	15
2.6.2	Conhecimento Comum e Ações Coordenadas	16
2.6.3	O Problema dos Maridos Infieis	17
3	Conhecimento em Sistemas Distribuídos Assíncronos	22
3.1	Modelo para Sistemas Distribuídos Assíncronos	22
3.2	Interpretação do Conhecimento em Sistemas Assíncronos . . .	28
3.3	Semântica para Sistemas Distribuídos Assíncronos	30
4	Conhecimento Comum Concorrente	32
4.1	Semântica para Conhecimento Comum Concorrente	33
4.2	Conhecimento Comum Concorrente e Ponto Fixo	35
4.3	Obtenção de Conhecimento Comum Concorrente	36
4.4	Algoritmo para Conhecimento Comum Concorrente	37
5	Lógicas Modais Multidimensionais	40
5.1	Fusões	41
5.2	Produto de Lógicas Modais	42

5.3	Axiomatização do Produto de Lógicas Modais	43
6	Lógica Bidimensional de Conhecimento em Sistemas Distribuídos	46
6.1	Subproduto Fechado de Lógicas Modais	47
6.2	Semântica Bidimensional	48
6.2.1	Relações de Possibilidade	49
6.2.2	Operadores Modais de Conhecimento	49
6.2.3	Interpretação de Conhecimento Bidimensional	50
6.2.4	Satisfazibilidade em L_m^2	51
6.3	Sistema Axiomático \mathcal{S}_m^2	52
6.4	Exemplo de Conhecimento em um Sistema Assíncrono	53
7	Corretude e Completude de \mathcal{S}_m^2	65
7.1	Corretude para \mathcal{S}_m^2	65
7.2	Modelos Finitos para \mathcal{S}_m^2	69
7.3	Model-Checking	78
8	Lógica Bidimensional para Conhecimento Comum Concorrente	80
8.1	Incorporando Conhecimento Mútuo Concorrente e Conhecimento Comum Concorrente	81
8.2	Sistema Axiomático \mathcal{C}_m^2	82
8.3	Corretude para \mathcal{C}_m^2	84
8.4	Completude para \mathcal{C}_m^2	88
8.5	Exemplos de Conhecimento Comum Concorrente	91
9	Conclusão	95

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 estruturava-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 participante 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 Schiffer 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 hierárquica 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.Zakharyashev, 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 \mathcal{S}_m , acrescido de axiomas para o conhecimento definido como o fecho das relações básicas, e portanto, como uma propriedade bidimensional.
- O capítulo 7 contém 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 $i = 1, \dots, m$, 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 Infieis*, 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 Infieis* 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 , $i = 1, \dots, m$. 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 $i = 1, \dots, m$.

Logo, se α e β são fórmulas da linguagem, então $\neg\alpha$, $(\alpha \wedge \beta)$ e $K_i\alpha$, para $i = 1, \dots, m$, 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 $i = 1, 2, \dots, m$.

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 , $i = 1, \dots, m$. 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 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 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.
- $\mathcal{S4}_m$ é \mathcal{T}_m acrescido do axioma A3.
- $\mathcal{S5}_m$ é $\mathcal{S4}_m$ acrescido do axioma A4.

Teorema 2.3.3 *Corretude e Completude de $\mathcal{K}_m, \mathcal{T}_m, \mathcal{S4}_m$ e $\mathcal{S5}_m$ [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. $\mathcal{S4}_m$ é uma axiomatização correta e completa em relação a classe de frames \mathbf{F}_m^{rt} .
3. $\mathcal{S5}_m$ 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 convencionalizado, 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 , $i = 1, \dots, m$, 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 $i \in G$

¹Para $k = 1$ $E_G^1\alpha = E_G\alpha$; 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 $\mathcal{K}_m^C, \mathcal{T}_m^C, \mathcal{S}_m^4$ e \mathcal{S}_m^5 [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}_m^4 é uma axiomatização correta e completa em relação a classe de frames \mathbf{F}_m^{rt} .
- \mathcal{S}_m^5 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:

$$C_{Gp} \rightarrow E_{Gp}^k \rightarrow E_{Gp} \rightarrow A_{Gp} \rightarrow D_{Gp} \rightarrow p$$

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 surpreendentes, 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 Infieis* 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 comunicação 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.

