



Carlos Bazilio Martins

**Análise Formal de Protocolos e Algoritmos
Distribuídos: Uma Abordagem Baseada em
Linguagem**

Tese de Doutorado

Tese apresentada ao Programa de Pós-Graduação em Informática do Departamento de Informática da PUC-Rio como requisito parcial para obtenção do título de Doutor em Informática.

Orientador: Prof. Edward Hermann Haeusler

Rio de Janeiro
Setembro de 2005



Carlos Bazilio Martins

**Análise Formal de Protocolos e Algoritmos
Distribuídos: Uma Abordagem Baseada em
Linguagem**

Tese apresentada ao Programa de Pós-Graduação em Informática do Departamento de Informática do Centro Técnico Científico da PUC–Rio como requisito parcial para obtenção do título de Doutor em Informática. Aprovada pela Comissão Examinadora abaixo assinada.

Prof. Edward Hermann Haeusler

Orientador

Departamento de Informática — PUC–Rio

Prof. Raimundo José de Araújo Macêdo

Departamento de Ciência da Computação - UFBA

Prof. Mario Roberto Folhadela Benevides

Instituto de Matemática - UFRJ

Prof. Christiano de Oliveira Braga

Instituto de Computação - UFF

Prof. Markus Endler

Departamento de Informática - PUC-Rio

Prof. Renato Fontoura de Gusmão Cerqueira

Departamento de Informática - PUC-Rio

Prof. José Eugênio Leal

Coordenador Setorial do Centro Técnico Científico — PUC–Rio

Rio de Janeiro, 09 de Setembro de 2005

Todos os direitos reservados. É proibida a reprodução total ou parcial do trabalho sem autorização da universidade, do autor e do orientador.

Carlos Bazilio Martins

Graduou-se em Computação na Universidade Federal Fluminense (UFF), onde obteve bolsas de pesquisa na área Orientação à Objetos e Otimização em Grafos, além de monitorias nas disciplinas de Compiladores e Linguagens Formais. Obteve o título de Mestre em Computação na Pontifícia Universidade Católica (PUC-RJ), e sua dissertação se concentrava nas áreas de Linguagem de Programação e Programação Concorrente. Em paralelo, trabalhou com pesquisas em transformações de código legado na própria instituição.

Ficha Catalográfica

Martins, Carlos Bazilio

Análise Formal de Protocolos e Algoritmos Distribuídos: Uma Abordagem Baseada em Linguagem / Carlos Bazilio Martins; orientador: Edward Hermann Haeusler. — Rio de Janeiro : PUC-Rio, Departamento de Informática, 2005.

v., 119 f: il. ; 29,7 cm

1. Tese (doutorado) - Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Informática.

Inclui referências bibliográficas.

1. Informática – Tese. 2. Especificação Formal. 3. Verificação Formal. 4. Protocolos. 5. Algoritmos Distribuídos. I. Haeusler, Edward Hermann. II. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Informática. III. Título.

Agradecimentos

Ao CNPq e à PUC-Rio, pelos auxílios concedidos, sem os quais este trabalho não poderia ter sido realizado.

Ao tio Hermann, como seus pupilos costumam chamá-lo. Muito do que sei hoje devo a você. Como todo meu professor, jamais será esquecido. Considero isso um prêmio, o qual há alguns anos atrás você me deu a oportunidade de agradecer.

Agradeço também aos professores Markus Endler e Christiano Braga, que forneceram importantes contribuições para o enriquecimento deste trabalho.

Aos colegas de trabalho, Vaston, Davi, Fernando, Rademaker, os demais e, em especial, a Geiza. O dia-a-dia definitivamente não seria o mesmo sem vocês! :-)

Aos amigos colecionados ao longo de toda essa jornada desde minha graduação na UFF, passando pelo mestrado e agora no doutorado na PUC-Rio. Sem vocês, nada disso seria possível. Ou, no máximo, seria possível com muito menos graça.

À minha mãe que, contrariando sua própria criação, seus exemplos familiares, exemplos no trabalho, contrariando tudo e todos, abdicou de boa parte de sua vida para poder chamar seu filho de Doutor, sem nem mesmo saber ao certo o que isso representaria.

Às outras mulheres da minha vida (minhas tia, irmã e meu coração) que, só pelo fato de existirem, de uma maneira ou de outra, já eram incentivo suficiente para que eu terminasse este trabalho.

Resumo

Martins, Carlos Bazilio; Haeusler, Edward Hermann. **Análise Formal de Protocolos e Algoritmos Distribuídos: Uma Abordagem Baseada em Linguagem**. Rio de Janeiro, 2005. 119p. Tese de Doutorado — Departamento de Informática, Pontifícia Universidade Católica do Rio de Janeiro.

Neste trabalho propomos uma arquitetura para a verificação formal de protocolos e algoritmos distribuídos. Esta pode ser vista como uma camada mais abstrata sobre o processo tradicional de verificação formal, onde temos a especificação e propriedade a serem verificadas, o verificador e o resultado retornado por este. O objetivo é simplificar o processo de especificação e verificação formal de protocolos e algoritmos distribuídos através de um ambiente mais dedicado. A parte principal desta arquitetura é a linguagem de especificação LEP, que contém construções de domínio-específico para simplificar a especificação destes sistemas. Outra característica desta linguagem é separar as especificações da topologia e do protocolo propriamente dito. Acreditamos que esta separação é válida pois torna mais clara a intenção das partes e ainda permite, por exemplo, o reuso de uma topologia entre diferentes especificações de protocolos. Assim, visamos oferecer uma linguagem cujos exemplos de especificações devem se assemelhar às descrições de algoritmos encontradas nos livros didáticos. Além disso, de forma a se ter a entrada e a saída da arquitetura compatíveis, propomos um pós-processamento da saída dos verificadores formais de forma a obter a saída no nível de abstração de LEP.

Palavras-chave

Especificação Formal. Verificação Formal. Protocolos. Algoritmos Distribuídos.

Abstract

Martins, Carlos Bazilio; Haeusler, Edward Hermann. **Formal Analysis of Protocols and Distributed Algorithms: a Based-Language Approach**. Rio de Janeiro, 2005. 119p. PhD Thesis — Department of Informática, Pontifícia Universidade Católica do Rio de Janeiro.

In this work we propose an architecture for the formal verification of protocols and distributed algorithms. This can be seen as a more abstract layer over the ordinary process of formal verification, where we have just the specification of the protocol and properties to be verified, and the formal tool. Our goal is to simplify the specification and formal verification of protocols and distributed algorithms through a dedicated environment. The core of the architecture is its input specification language (LEP), which provides domain-specific constructions for simplifying the specification of those systems. With LEP the specification of the protocol and the specification of the topology to be referred to the protocol are given separately. We feel that this division improves the legibility of both and allows the reuse of the specification of a topology among distinct protocols. Using this approach we try to offer a language whose specifications should be similar to the descriptions of the algorithms found on the didactic books. Moreover, in order to have the input and output of the architecture compatible, we also propose a way of processing the result of the formal verification tool. Then we could have the result on the abstract level of LEP.

Keywords

Formal Specification. Formal Verification. Protocols. Distributed Algorithms.

Sumário

1	Introdução	11
1.1	Organização da Tese	14
2	Formas de Validação	15
2.1	Simulação	15
2.2	Verificação Formal	15
2.3	Nossa Visão	17
3	Arquitetura Proposta	19
3.1	Descrição	20
3.2	LEP	21
3.3	Semântica Formal das Traduções	37
4	Estudos de Caso	53
4.1	Protocolos Analisados	53
4.2	Comparação entre LEP e outras linguagens	65
5	Discussão sobre Otimização dos Modelos	68
5.1	Modelo Mínimo	70
5.2	Limitante Superior	74
6	Trabalhos Relacionados	79
6.1	Propostas Similares	79
6.2	Linguagens de Especificação	80
6.3	Ferramentas Utilizadas	82
6.4	Trabalhos Afins	83
7	Conclusão	86
A	Definições	99
A.1	Gramática de Atributos	99
A.2	Gramática de Grafos	99
A.3	Gramática de Grafos com Atributos	100
B	Gramática de LEP em BNF	101
C	Especificações do Algoritmo de Eleição de um Líder	107
C.1	LEP	107
C.2	SDL	109
C.3	Promela	109
C.4	NuSMV	110
C.5	Murphi	113
C.6	CDL	114
C.7	XL	115

Lista de figuras

3.1	Modelo tradicional de verificação	19
3.2	Descrição geral da arquitetura	20
3.3	Especificações de topologias em LEP	24
3.4	Gramática de Grafos para a topologia totalmente conectada	26
3.5	Derivação da Gramática de Grafos para a topologia totalmente conectada	27
3.6	Declaração de um módulo em LEP	28
3.7	Eleição de um líder numa rede arbitrária em LEP	31
3.8	Algoritmo de consenso especificado em LEP	32
3.9	Especificação simplificada do DSR em LEP	33
3.10	Ambiente do Modelo de Comunicação de LEP	34
3.11	Algoritmo de consenso especificado em LEP	46
3.12	Trecho gerado da tradução do módulo comandante para o Código Intermediário	47
3.13	Trecho do código da especificação do comandante em Promela	48
3.14	Contra-exemplo no formato MSC retornado pelo Spin	49
3.15	Versão textual de parte do contra-exemplo retornado pelo Spin	50
3.16	Contra-exemplo retornado pelo SMV (<i>commandLEP</i> é o mesmo que <i>codePositionLEP</i>)	51
4.1	MSC de um cenário do RDP	54
4.2	Topologia inicial de RDP em LEP	56
4.3	Estação móvel do RDP em LEP	56
4.4	Estação base do RDP em LEP	57
4.5	Abstração dos proxies do RDP em LEP	58
4.6	Módulo servidor do RDP em LEP	58
4.7	Estação móvel do RDP com inicialização não-determinística	59
4.8	Mecanismo para a descoberta de rotas	60
4.9	Declaração das variáveis locais e da mensagem que inicia o protocolo DSR	62
4.10	Tratamento da mensagem de descoberta de rota	63
4.11	Tratamento da mensagem que retorna a rota obtida para o nó origem	63
4.12	Tratamento da mensagem que envia pacote sobre rota já calculada	64
4.13	Tratamento de mensagens de erro enviadas quando uma conexão é quebrada	64
4.14	Número de Comandos nas especificações do algoritmo de Eleição de um Líder em diferentes linguagens	66
5.1	Modelo para a verificação do protocolo DSR	68
5.2	Modelo para a verificação do protocolo RDP	69
5.3	Eleição de um líder numa rede arbitrária em LEP	72
5.4	Conjunto de dependências para a especificação da figura 5.3	72
5.5	Ocorrência da propriedade <i>any?win</i> no conjunto em destaque	72
5.6	Nó sincronizável com o nó <i>c?win</i> em destaque	73
5.7	Nós sincronizáveis com o nó <i>c?msg</i>	73

5.8	Traços de um modelo gerados por um verificador de modelos	75
5.9	Algoritmo de consenso especificado em LEP	77
6.1	Hierarquia para padrões de especificação de propriedades	83
7.1	Especificação de um leilão em LEP	89
B.1	Sequências no tempo onde as fórmulas são válidas	106
C.1	Especificação da versão original do Algoritmo de Eleição de um Líder em LEP	108
C.2	Especificação da versão otimizada do Algoritmo de Eleição de um Líder em LEP	108
C.3	Especificação de Eleição de um Líder em SDL	109
C.4	Especificação de Eleição de um Líder em Promela	111
C.5	Especificação de Eleição de um Líder em SMV	112
C.6	Especificação de Eleição de um Líder em SMV	112
C.7	Especificação de Eleição de um Líder em SMV	113
C.8	Constantes, Tipos e Variáveis utilizadas na especificação da Eleição de um Líder em $\text{Mur}\varphi$	114
C.9	Funções para manipulação dos canais de mensagens da especificação da Eleição de um Líder em $\text{Mur}\varphi$	115
C.10	Regras que descrevem o comportamento de um nó na especificação da Eleição de um Líder em $\text{Mur}\varphi$	116
C.11	Estado inicial da especificação da Eleição de um Líder em $\text{Mur}\varphi$	116
C.12	Especificação de Eleição de um Líder em CDL	117
C.13	Especificação de Eleição de um Líder em XL	118

Lista de tabelas

3.1	Negação dos pronomes como agentes	47
4.1	Tabela de Comparação entre LEP e Promela (NUM-TRANS contém o número de transições - <i>Pré-condição</i> → <i>Ação</i> - existentes no módulo onde o pronome <i>everyone</i> ocorre)	67