Pontifícia Universidade Católica
do Rio de Janeiro

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

Pontifícia Universidade Católica
do Rio de Janeiro

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

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.

CDD: 004

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 agraciar.

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 separetely. 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

Lista de figuras

Lista de tabelas