



**Jefferson de Barros Santos**

**Infraestrutura para provedores interativos de  
teoremas na Web**

**Dissertação de Mestrado**

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Pós-graduação em Informática do Departamento de Informática da PUC-Rio

Orientador: Prof. Edward Hermann Haeusler

Rio de Janeiro  
Março de 2010



**Jefferson de Barros Santos**

**Infraestrutura para Provedores Interativos de  
Teoremas na Web**

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre pelo Programa de Pós-graduação em Informática do Departamento de Informática do Centro Técnico e Científico da PUC-Rio. Aprovada pela Comissão Examinadora abaixo assinada.

**Prof. Edward Hermann Haeusler**  
Orientador

Departamento de Informática – PUC-Rio

**Prof. Daniel Schwabe**

Departamento de Informática – PUC-Rio

**Prof<sup>a</sup> Marcelo da Silva Corrêa**

Universidade Federal Fluminense – UFF

**Prof<sup>a</sup> Alex de Vasconcellos Garcia**  
Instituto Militar de Engenharia – IME

**Prof. José Eugenio Leal**  
Coordenador Setorial do Centro  
Técnico Científico – PUC-Rio

Rio de Janeiro, 24 de março de 2010

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

### Jefferson de Barros Santos

Graduou-se Bacharel em Informática pela PUC-Rio. Desenvolve software profissionalmente desde 1995 e, atualmente é analista de sistemas da PUC-Rio, trabalhando com os sistemas administrativos da universidade. Atua como professor em cursos de extensão e especialização desta instituição em áreas como Gerência de Projetos e Desenvolvimento Ágil de Software.

#### Ficha Catalográfica

Santos, Jefferson de Barros

Infraestrutura para provedores interativos de teoremas na Web / Jefferson de Barros Santos; orientador: Edward Hermann Haeusler. — 2010.

89 f.: il. ; 30 cm

Dissertação (Mestrado) - Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Informática, Rio de Janeiro, 2010.

Inclui bibliografia

1. Informática – Teses. 2. Prova automática de teoremas;. 3. Provedores interativos;. 4. Interfaces gráficas;. 5. Web services.. I. Haeusler, Edward Hermann. II. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Informática. III. Título.

CDD: 004

Esta dissertação é dedicada em especial a meus pais, Maria de Fátima e Helio, pelo amor, carinho e por todo o esforço que fizeram para apoiar os meus estudos. Amo vocês!

## Agradecimentos

Aos meus filhos, Lara e Caio. A primeira, que compartilhou o pai com os estudos durante tanto tempo e tantas vezes me revigorou, com seu sorriso, carinho e frases engraçadas. O segundo, que nasceu duas semanas depois da minha defesa, também dividiu o pai com livros e pesquisas enquanto ainda estava na barriga da mamãe. Vocês são tudo pra mim.

À minha esposa, Paula, pelo amor, paciência e tolerância. Por ter aguentado um marido ausente em tantos momentos e por sempre ter admirado e apoiado o caminho que escolhi.

Ao meu orientador, professor Edward Hermann Haeusler, pelos ensinamentos, incentivo, compreensão e amizade. Por ter me feito acreditar que eu seria capaz de contribuir para a pesquisa em Teoria da Computação, mesmo não sendo minha área de pesquisa original.

Aos professores membros da banca por todos os comentários que ajudaram a melhorar bastante o texto final que aqui apresento.

Aos meus companheiros de estudo, Cecília e Pedro, que dividiram comigo essa caminhada e me ajudaram em muitos momentos.

Ao meu chefe e amigo, Gustavo Miranda, por ter sido um grande incentivador e ter me dado as condições necessárias para conciliar trabalho e mestrado.

Aos meus companheiros de trabalho da equipe do SGU da PUC-Rio. Vocês vivenciaram alguns dos momentos mais importantes da minha vida e, de alguma maneira, todos contribuíram para que eu conseguisse concluir esse mestrado.

E a Deus, por ter colocado todas essas pessoas em minha vida e por ter me permitido chegar até aqui. Obrigado.

## Resumo

Santos, Jefferson de Barros; Haeusler, Edward Hermann. **Infraestrutura para provadores interativos de teoremas na Web.** Rio de Janeiro, 2010. 89p. Dissertação de Mestrado — Departamento de Informática, Pontifícia Universidade Católica do Rio de Janeiro.

Prova automática de teoremas consiste na prova de teoremas matemáticos por intermédio de programas de computador. Dependendo da linguagem lógica em uso, o processo de provar uma determinada fórmula pode não ser computável. Além disso, dependendo do cálculo dedutivo empregado, a busca por uma prova envolve lidar com a possibilidade de aplicação de longas sequências de axiomas e regras de inferência. Tudo isso reforça a necessidade da intervenção humana no processo de prova em sistemas denominados provadores interativos de teoremas ou assistentes de prova. Em um cenário típico, um usuário interage com a máquina de prova através de uma interface gráfica, normalmente implementada como um aplicativo desktop. Recentemente, porém, muitos aplicativos deste tipo passaram a ser oferecidos para seus usuários através da web. Esta forma de disponibilizar software evita que o usuário final se preocupe com questões de instalação e configuração e possibilita o acesso ao sistema de qualquer computador, com qualquer sistema operacional, bastando ter disponível uma conexão com a Internet. Nesta dissertação, estudamos possibilidades de uso da web como plataforma para a construção de ambientes interativos para prova de teoremas. Nossa proposta é estudar os diferentes modelos de interação entre usuário e ambientes de prova automatizados e verificar como estes modelos podem ser adaptados para a web. Como resultado, apresentamos uma ferramenta gráfica para visualização e manipulação direta de provas formais na web como uma interface alternativa entre usuários e provadores.

## Palavras-chave

Prova automática de teoremas; Provadores interativos; Interfaces gráficas; Web services.

## Abstract

Santos, Jefferson de Barros; Haeusler, Edward Hermann. **Infrastructure for Web-based Interactive Theorem Provers**. Rio de Janeiro, 2010. 89p. MSc Dissertation — Departamento de Informática, Pontifícia Universidade Católica do Rio de Janeiro.

Automatic theorem proving consists of proving mathematical theorems by means of computer programs. Depending on the logic used, the process of proving a formula is not computable. Moreover, depending of the deductive system applied to, the search for a proof can involve the application of long sequences of axioms and inference rules, reinforcing the need of human intervention in the proof process. Such systems are known as interactive theorem provers or proof assistants. In a typical scenario, the user interacts with the prover through a graphical interface, usually a desktop application. Recently, however, applications like those started to be delivered to users through the web. This way of software deployment avoids that final users have to deal with complex activities like prover installation and configuration and allows this user to access the system from different machines with a simple Internet connection. In this research we study the use of web as a platform for interactive theorem proving environments construction. Our purpose is to study some interaction models between user and automated proof environments and verify how these models can be adapted to work as a web application. As a result we show a graphical tool for visualization and direct manipulation of formal proofs on web to work as an alternative interface between user and proving machines.

## Keywords

Automatic theorem proving; Interactive provers; Graphical interfaces; Web services.

## Sumário

1	Introdução	<b>12</b>
1.1	Descrição do Problema	12
1.2	Objetivo desta Dissertação	13
1.3	Organização desta Dissertação	14
2	Conceitos Fundamentais sobre Prova de Teoremas	<b>16</b>
2.1	Linguagens Lógicas	16
2.2	Semântica	19
2.3	Sistemas Dedutivos	21
2.4	Dedução Natural	23
2.5	Cálculo de Sequentes	25
2.6	Tableaux	28
3	Provadores de Teoremas	<b>32</b>
3.1	Fundamentos	32
3.2	Provadores Orientados a Objetivos	34
3.3	Problemas no Uso de Provadores de Teoremas	35
4	Interfaces para Provadores de Teoremas	<b>37</b>
4.1	Premissa Básica: Separação Interface-Provador	38
4.2	Representação de Provas	39
4.3	Modelos de Interação Humano-Computador	40
4.4	Componentes Básicos de Interfaces para Provadores	46
4.5	Requisitos de Interfaces para Provadores	53
4.6	Outros Trabalhos Relacionados	55
4.7	Principais Ferramentas	55
5	Uma Interface Web para Provadores Interativos	<b>62</b>
5.1	O Processo de Prova	63
5.2	A Web como Plataforma para Interfaces para Provadores	64
5.3	Arquitetura Geral da Solução	67
5.4	Implementando o Protocolo de Comunicação como Web Service	70
5.5	Desenvolvimento da Interface Web	75
5.6	Modelos de Interação na Interface Web	76
5.7	Scripts de Prova	79
6	Conclusões e Trabalhos Futuros	<b>81</b>
	Referências Bibliográficas	<b>84</b>

## Lista de figuras

3.1	Provedores apoiados por Verificadores de Prova	36
4.1	O processo de prova representado como uma árvore	39
4.2	A visão de prova como programação	43
4.3	Exemplo de linguagem imperativa em scripts de prova	52
4.4	Exemplo de linguagem declarativa em scripts de prova	52
4.5	Arquitetura Geral do Proof General Kit	60
5.1	Etapa 1 - Informar o Objetivo Inicial	64
5.2	Etapa 2 - Provedor iniciado com o objetivo inicial	64
5.3	Etapa 3 - Lista de regras disponíveis no objetivo escolhido	65
5.4	Etapa 4 - Regra aplicada e apresentação de nova lista de regras	65
5.5	Etapa 5 - Prova concluída	66
5.6	Arquitetura do HemeraWeb	68
5.7	Operações suportadas pelo Web Service	73
5.8	A arquitetura MVC	76
5.9	Árvore de Estado da Prova no HemeraWeb	78
5.10	Biblioteca de Scripts de um Usuário no HemeraWeb	80
5.11	Estados dos Scripts de Prova	80

## Lista de tabelas

2.1	Dedução Natural para Primeira Ordem Clássica	24
2.2	Regras do Tableaux para Lógica Proposicional Clássica	29

*O mesmo homem não pode atravessar o mesmo rio, porque o homem de ontem não é o mesmo homem, nem o rio de ontem é o mesmo de hoje.*

**Heráclito**, filósofo grego pré-socrático.