Provadores de Teoremas e suas Aplicações

Prof. Marcus Ramos
13 de Julho de 2018
UNIVASF

- Teoremas?
- Provas?
- Provadores de Teoremas?

Coisa de maluco?
Tem aplicação prática?
Por que eu deveria me interessar por isso?

Nova maneira de:

- Provar teoremas;
- Desenvolver software.

Provadores de Teoremas:

- Programa de computador;
- Várias plataformas;
- Verificação mecânica da correção de uma prova;
- Assistente interativo para elaboração de provas;
- Extração de programas;
- Linguagens e teorias;
- Existem vários disponíveis.

Vantagens para:

- Matemáticos;

- Cientistas da computação;
- Programadores;
- Engenheiros de software;
- Empresas de desenvolvimento de software e hardware;
- Usuários de programas, componentes e aplicativos.

Para os matemáticos:

- Formalização;
- Segurança;
- Publicação;
- Compartilhamento;
- Reutilização.

Mas...

O que a prova de teoremas tem a ver com o desenvolvimento de software?

Não são coisas completamente diferentes? Teoria e prática?

Tem tudo a ver!

Prova:

Argumentação incontestável sobre a validade de uma proposição.

Incontestável?
Proposição?

Teorema:

Proposição não-trivial acerca de alguma definição ou conjunto de definições.

Não-trivial?
Definição?

Teoria:

Definição (uma ou mais) e um conjunto de teoremas (ou lemas) que dizem respeito à(s) definição(ões).

Mas... provar teoremas e desenvolver sofware???

>>> Curry-Howard <<<

(Dedução Natural e Cálculo Lambda)

Se alguns requisitos forem observados,

A prova de um teorema se torna o programa que atende à uma certa especificação.

Provas ⇔ Programas
Proposições (ou Tipos) ⇔ Especificações

Conseqüência prática:

Provar um teorema é a mesma coisa que construir um programa!

Prova → Teorema (Proposição)

Programa → Especificação (Tipo)

Prova → Teorema (Proposição)

Programa → Especificação (Tipo)

Implicações:

- Programas certificados;
- Não há necessidade de testes;
- Corretos por construção;
- Maior confiabilidade.

Requisitos:

- Conhecer Provadores de Teoremas;
- Conhecer a teoria subjacente;
- Experiência;
- Força de vontade.

O mundo está mudando:

- Empresas de software estão usando Provadores de Teoremas;
- Elas estão contratando profissionais que sabem usá-los;
- Competitividade, produtividade e qualidade;
- Aplicações importantes;
- Mercado emergente.

Já mudou alguma coisa?

- Intel;
- Microsoft;
- Compiladores, sistemas operacionais, chips, smart cards etc;
- Visível na Europa e nos EUA;
- Imperceptível no Brasil;
- Oportunidades de carreira e de empreendimento.

O profissional do futuro precisa conhecer e saber usar a teoria. Provadores de Teoremas são apenas uma ferramenta.

Histórico pessoal:

- Linguagens Formais e Autômatos;
- Abordagem informal;
- Contato com Coq;
- Formalização matemática;
- França 2014;
- Portugal 2015;
- Doutorado 2016;
- Formalização de parte substancial da Teoria das Linguagens Livres de Contexto (~30.000 linhas de scripts escritas, ~600 teoremas e lemas provados).
- Continuidade.

Objetivos:

- Despertar o interesse pelo assunto;
- Temos um grupo de interessados?
- Estudar Provadores de Teoremas e Coq em particular;
- Entender o que é formalização matemática;
- Provar teoremas simples;
- Aprender como usar Coq para o desenvolvimento de software certificado;
- Incentivar o estudo continuado e a atuação na área, com pesquisas e publicações.

Próximos passos:

- Calendário de encontros;
- Planejamento das atividades;
- Avaliar pré-requisitos;
- Palestras e tutoriais;
- Colaboração em projeto de pesquisa.

Essencialmente:

- Muita teoria;
- Coq;
- Exemplos de uso e de aplicação;
- Estudos de casos;
- Formalização da Teoria das Linguagens Livres de Contexto;
- Slides e artigos já publicados;
- Muito estudo e muita dedicação.

Teoria:

- Lógica;
- Teoria de Provas;
- Dedução Natural;
- Cálculo Lambda (não-tipado e tipado);
- Teoria de Tipos;
- Curry-Howard;
- Construtivismo;
- Técnicas de prova (indução etc)
- etc.

Em resumo:

- Não é fácil;
- Aprendizado lento;
- Exige muita dedicação;
- Área ativa de pesquisa;
- Aplicações comerciais e acadêmicas de grande relevância;
- Muitas oportunidades;
- Tendência irreversível;
- É o futuro (da matemática e do desenvolvimento de software);
- Vai encarar?

Esta apresentação tem caráter apenas motivacional e introdutório. Para mais informações sobre o assunto, consultar (do autor):

- Slides WTA 2014;
- Slides Porto 2015;
- Tese 2016 + slides;
- Artigos diversos.

Além de uma grande quantidade de artigos, tutoriais e apresentações sobre o assunto disponíveis na Internet.

Obrigado!