# Provas Formais e Verificação de Programas

## Descrição Breve

Assistentes de prova são ferramentas utilizadas para verificar a correção de programas. Ao contrário de ferramentas como verificadores de modelo e solucionadores SAT, os assistentes de prova são altamente interativos. Provas formais verificadas por máquina levam a programas confiáveis e matematicamente especificados e seguros.

Este curso introduz os estudantes à teoria e uso de assistentes de prova, usando Lean. Usaremos o Lean para verificar propriedades de programas funcionais e teoremas da matemática. Aprenderemos a teoria do raciocínio dedutivo e a lógica na qual essas ferramentas são baseadas.

## Descrição Estendida

Quando aprendemos a programar, frequentemente pensamos em termos de implementação de instruções: um programa é uma lista de passos que o computador deve executar para fazer o que queremos. Mas existem ideias importantes que faltam nessa perspectiva. Como especificamos precisamente o que queremos que o computador faça? E como verificamos que nossas instruções correspondem a essa especificação?

Linguagens foram desenvolvidas para oferecer uma estrutura unificada para especificação, implementação e verificação. Este curso trata da teoria e uso dessas linguagens, concentrando-se em Lean 4.

Lean é um "assistente de prova" e linguagem de programação. O tipo de verificação visto na maioria dos assistentes de prova não é probabilístico, como em grandes conjuntos de testes. Não é refutável, como comumente visto em verificadores de modelo e ferramentas similares. Nem é sempre automatizado. Parte da tarefa do programador é construir uma derivação, ou prova, que garanta formalmente que seu programa atenda à sua especificação.

Por causa desse foco na prova, um sistema como o Lean está na fronteira entre programação e matemática. É possível escrever e provar teoremas matemáticos da mesma forma que se escreve e verifica especificações de programas.

Este curso abordará uma variedade de tópicos relacionados à prova formal e verificação de programas. Examinaremos a teoria do raciocínio dedutivo e como ela é realizada na teoria dos tipos do Lean; paradigmas da programação funcional que facilitam a verificação; geração automática de provas; e aplicações dessas ferramentas na matemática pura. Mas, acima de tudo, aprenderemos a usar o Lean para escrever programas funcionais confiáveis e verificados. Este curso coloca a teoria do raciocínio dedutivo em prática.

## Objetivos do Curso

O principal objetivo deste curso é aprender como especificar e verificar propriedades de programas e objetos matemáticos na teoria dos tipos. Você aprenderá a usar o assistente de prova Lean para implementar programas funcionais, declarar suas propriedades importantes e verificar que essas propriedades são válidas. Ao mesmo tempo, você aprenderá a teoria subjacente a esses sistemas de raciocínio: do que consistem as provas dedutivas e porque elas são confiáveis.

Ao final deste curso, você deverá ser capaz de:

* Escrever programas funcionais executáveis em Lean.
* Especificar e verificar propriedades desses programas funcionais.
* Escrever e provar declarações matemáticas em Lean.
* Escrever meta-programas: táticas que buscam provas automaticamente.
* Explicar a semântica de programas funcionais.
* Distinguir objetos de prova (derivações, deduções) de outros tipos de verificações ou testes para correção de programas.

## Pré-requisitos

Recomendamos que os estudantes tenham cursado matemática discreta ou um curso de matemática baseado em provas. Familiaridade básica com programação funcional (por exemplo, Haskell, ML) é útil, mas não obrigatória.

## Livros Didáticos

Seguiremos "The Hitchhiker's Guide to Logical Verification" de Jasmin Blanchette et al.

## Avaliação

* 60%: Haverá uma tarefa de casa por capítulo do Guia do Mochileiro. Isso é aproximadamente semanal, embora algumas semanas não terão tarefas. As tarefas serão divulgadas nas segundas-feiras antes da aula e deverão ser entregues 8 dias depois, nas noites de terça-feira.
* 40%: Um "projeto de formalização" final individual ou prova dará aos alunos a oportunidade de implementar e verificar algo de seu próprio interesse no Lean. Disponibilizaremos ideias de projetos com antecedência, e os alunos são encorajados a consultar o instrutor.

## Colaboração

Os alunos são fortemente encorajados a trabalhar juntos nos problemas de exercício e a discutir as tarefas de casa. No entanto, as entregas escritas das tarefas devem ser seu próprio trabalho. Defendemos a política do "quadro branco apagado": discuta suas soluções com um colega, mas não faça referência a nenhuma nota escrita dessa conversa quando implementar suas soluções.

Uma boa regra é que suas discussões devem permanecer no nível conceitual. Pergunte "qual é a sintaxe para uma prova por indução", em vez de perguntar se sua prova por indução está correta.