FDD3023 Interactive Theorem Proving and Program Verification 7.5 credits

Interaktiv teorembevisning och programverifiering

This is a translation of the Swedish, legally binding, course syllabus.

Establishment

Course syllabus for FDD3023 valid from Spring 2020

Grading scale

P, F

Education cycle

Third cycle

Specific prerequisites

M.Sc. in Computer Science or equivalent.

Language of instruction

The language of instruction is specified in the course offering information in the course catalogue.

Intended learning outcomes

At the end of the course, the student should be able to

- Account for different foundations and technologies for interactive theorem proving
- Assess which types of program verification problems interactive theorem proving is suited to solve
- Account for the functionality and limitations of current interactive theorem provers
- Use an interactive theorem prover correctly in a small program verification project
- Be able to effectively use tools related to interactive theorem provers, such as editors and build systems
- Develop own formal models of software systems in an interactive theorem prover and account for limitations and applicability as well as express and formally prove important model properties in the tool
- Be able to design and carry out basic validation of own formal models
- Perform basic assessment of the benefits and costs of applying interactive theorem provers for verification of specific software systems

Course contents

Students will learn to model complex systems, encode their models and specifications in the formalism of an ITP, analyze and validate their models, and use the ITP to produce formal proofs that models satisfy their specifications.

After taking the course, students should be able to carry out their own modeling and verification projects in an ITP, and understand the possibilities and limitations of using ITPs for program verification.

Course structure

The course consists in one lecture per week, as well as a weekly exercise sheet that students must complete as homework in order to pass the course. The lecturers will be available to help with exercises during office hours and/or by appointment with individual students.

Course literature

- HOL4 guidebok (https://hol-theorem-prover.org/guidebook)
- HOL4 logik (http://sourceforge.net/projects/hol/files/hol/kananaskis-13/kananaskis-13-logic.pdf/download)

Examination

- EXA1 - Examination, 7.5 credits, grading scale: P, F

Based on recommendation from KTH's coordinator for disabilities, the examiner will decide how to adapt an examination for students with documented disability.

The examiner may apply another examination format when re-examining individual students.

If the course is discontinued, students may request to be examined during the following two academic years.

The examination consists of the homework assignments and a final project.

Other requirements for final grade

Completing all assignments as well as a successful review of the final project.

Ethical approach

- All members of a group are responsible for the group's work.
- In any assessment, every student shall honestly disclose any help received and sources used.
- In an oral assessment, every student shall be able to present and answer questions about the entire assignment and solution.