Interactive Theorem Proving

Spring 2024
Lecture 1: Course Introduction

David Broman
Professor, KTH Royal Institute of Technology
Visiting Professor, Stanford University
Associate Director Faculty, Digital Futures

Elias Castegren
Assistant Professor, Uppsala University

Video Recording and Slides

We will…

- Record lectures by the teachers
- Remove questions and discussions
- Publish videos on Youtube

Hence, we would like that you only

- Ask questions in the Zoom chat, or
- Ask questions when we have Q/A sessions

All slides will be uploaded on the course page after the lecture

Proof Assistants and Interactive Theorem Provers

Why?

- Handwritten mathematical proofs: tedious to write and check
- Proof assistants assist in the process
- Proof checking becomes trivial!
- Learning to use proof assistants - not so trivial…

How are they used?

- To prove general mathematical theorems
- Formalize and prove properties of formal semantics
- Correctness of software (e.g., verified compilers)

Proof assistants

Coq, Isabelle/Isar, HOL, Agda, Lean, PVS, Idris, F*, Twelf, and many more…

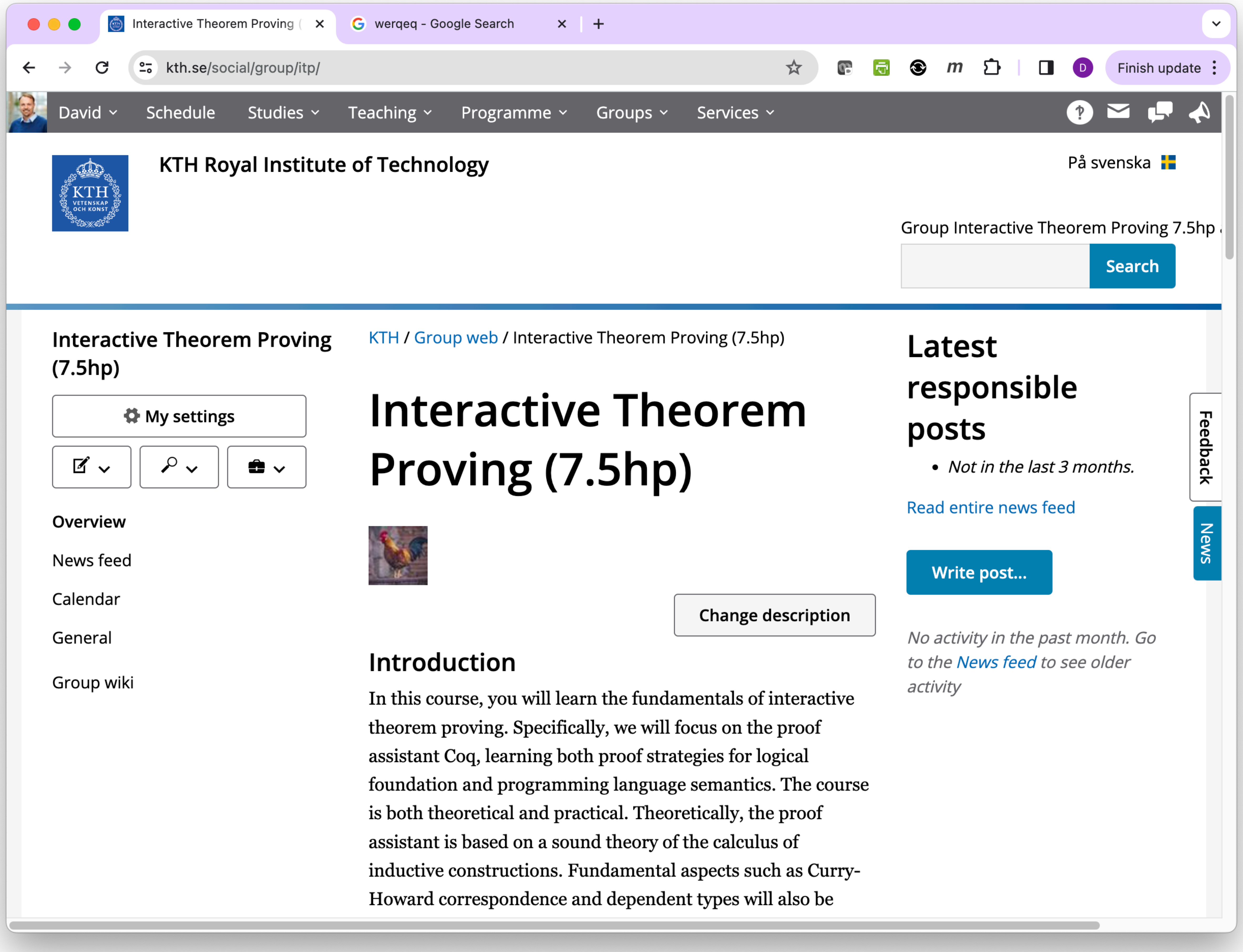
Part I
Course Information

Part II
Introduction to Coq

Part I

Course Information

Course Page



KTH Royal Institute of Technology

På svenska

Group Interactive Theorem Proving 7.5hp

Search

Interactive Theorem Proving (7.5hp)

My settings

Overview

News feed

Calendar

General

Group wiki

KTH / Group web / Interactive Theorem Proving (7.5hp)

Interactive Theorem Proving (7.5hp)

Change description

Introduction

In this course, you will learn the fundamentals of interactive theorem proving. Specifically, we will focus on the proof assistant Coq, learning both proof strategies for logical foundation and programming language semantics. The course is both theoretical and practical. Theoretically, the proof assistant is based on a sound theory of the calculus of inductive constructions. Fundamental aspects such as Curry-Howard correspondence and dependent types will also be

Latest responsible posts

- *Not in the last 3 months.*

Read entire news feed

Write post...

No activity in the past month. Go to the News feed to see older activity

Feedback

News

Course page with all info

https://www.kth.se/social/group/itp/

Learning Objectives

After the course, the student will be able to

- Construct proofs in Coq related to basic logic
- Apply proof assistant tactics
- Construct proofs in Coq related to programming language semantics
- Explain the concept of dependent types
- Explain the differences between different kinds of proof assistants
- Explain and reflect on ethical aspects of mathematics in computer science

Lecture and Seminars

Examiner and Course Organizer

David Broman

KTH Royal Institute of Technology

Teacher (Coq)

Elias Castegren,
Uppsala University

Guest lecture 1: Introduction to Agda

Teacher: Jeremy Siek, Indiana University, USA

Guest lecture 2: Introduction to HOL

Teacher: Magnus Myreen, Chalmers, Sweden

Potentially some
more guest lectures

Schedule (Tentative)

Note: please check the course website for the latest updates!

Lecture Seminar 1: Course Information and Introduction to Coq
Examiner: David Broman, Teacher: Elias Castegren
Date: Monday, April 15, 17.00-19.30 (Stockholm), 8 am-10.30 am (CA)

Lecture Seminar 2: Logical Foundations part 2 in Coq
Teacher: Elias Castegren
Date: Thursday, May 2, 17.00-19.00 (Stockholm), 8 am-10.00 am (CA)

Lecture Seminar 3: Programming Language Foundation part 1 in Coq
Teacher: Elias Castegren
Date: Thursday, May 23, 17.00-19.00 (Stockholm), 8 am-10.00 am (CA)

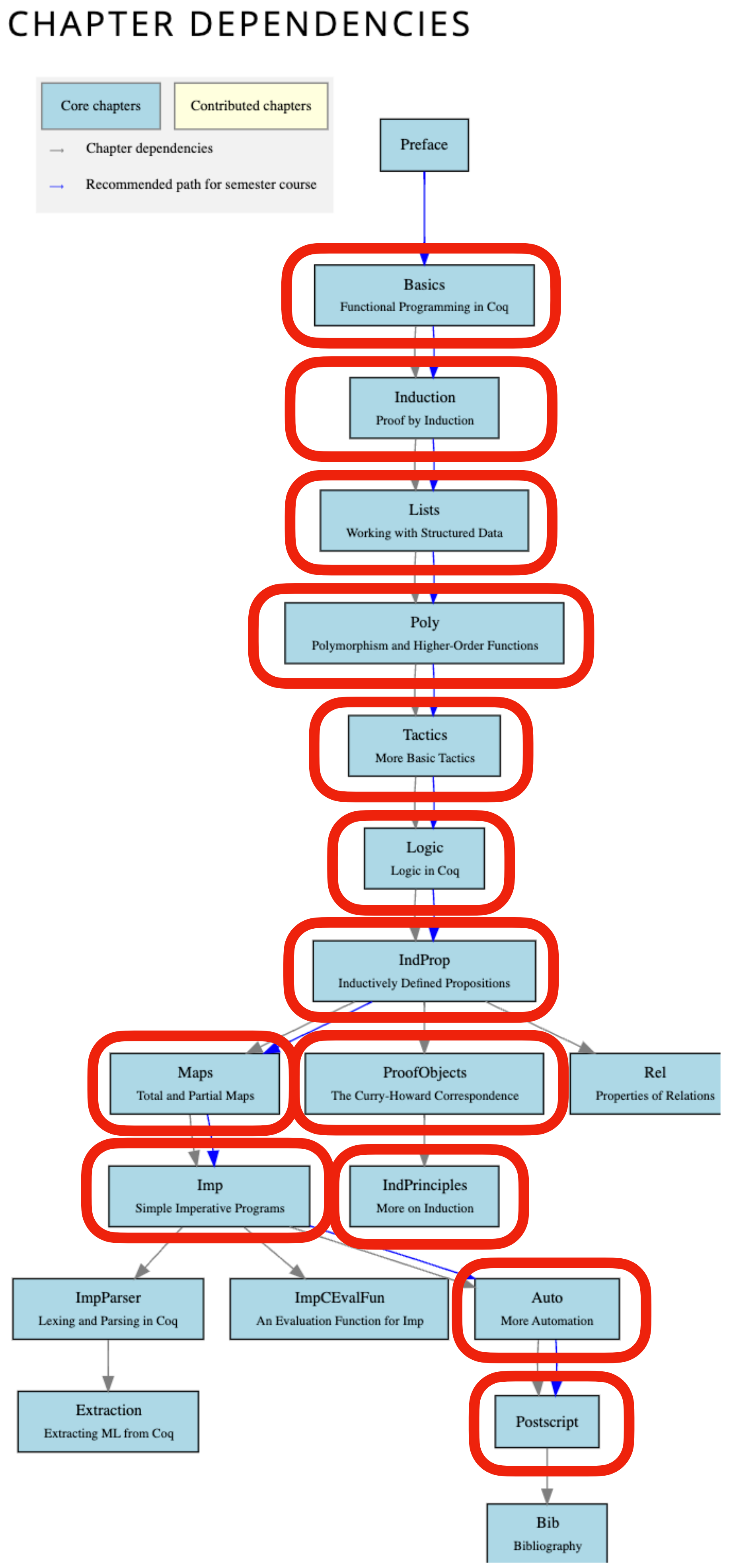
Lecture Seminar 4: Programming Language Foundation part 2 in Coq and Ethics
Teacher: Elias Castegren (Coq lecture)
Teacher: David Broman (Ethics discussion session)
Date: Thursday, June 13, 17.00-19.30 (Stockholm), 8 am-10.30 am (CA)

Guest Lecture 1: Introduction to Agda
Teacher: Jeremy Siek, Indiana University, USA
Date: TBD

Guest Lecture 2: Introduction to HOL
Teacher: Magnus Myreen, Chalmers, Sweden
Date: TBD

Lecture Seminar 5: Final student presentations
Teachers: David Broman and Elias Castegren
Tentative Date: Tuesday, June 25, 16.00-19.00

Home Assignments (Coq part 1)



Volume 1: Logical Foundation

https://softwarefoundations.cis.upenn.edu/lf-current/index.html

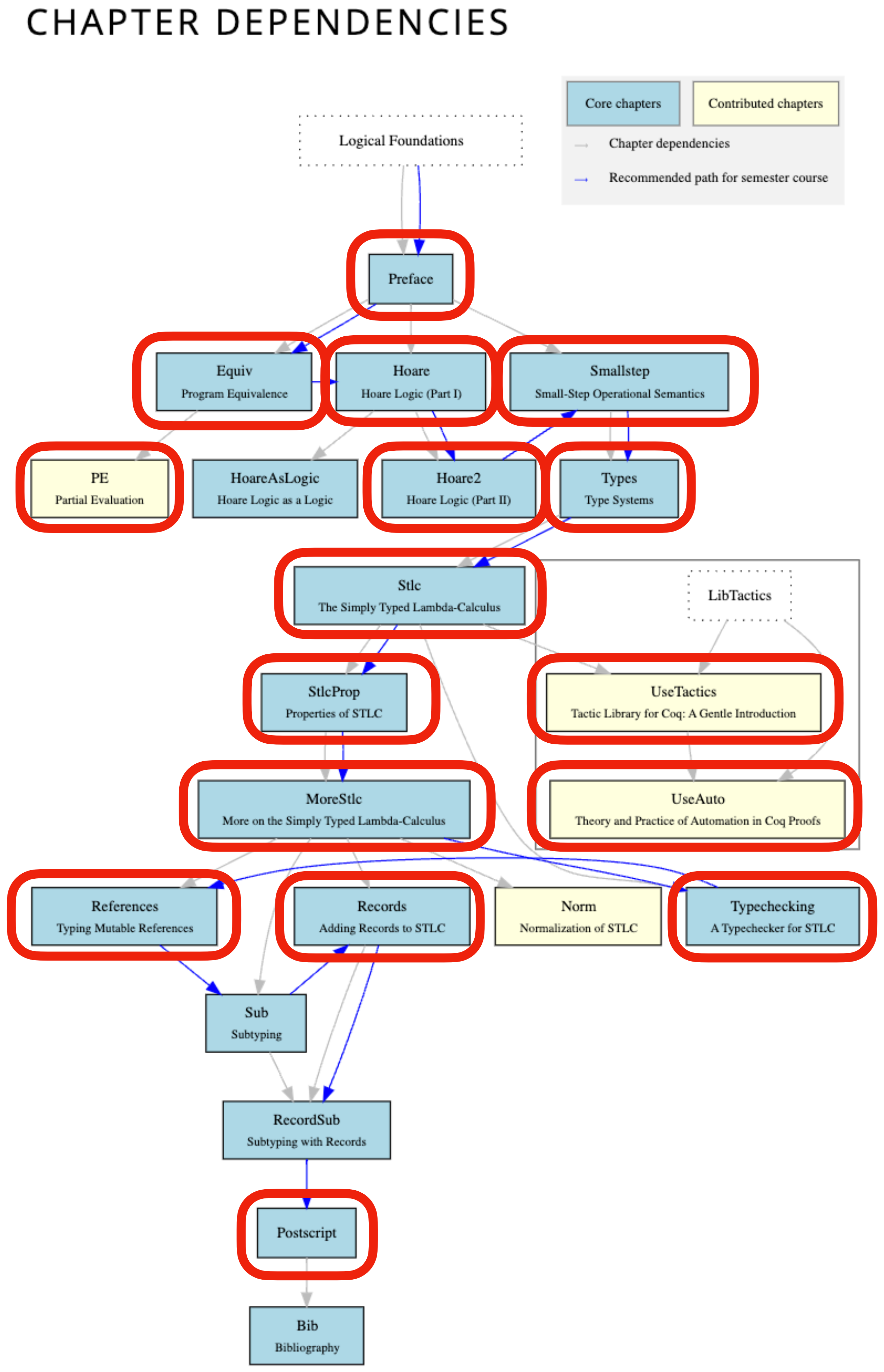
Do all chapters that follow the recommended path for the semester course (blue arrows, from Basics to postscript) in https://softwarefoundations.cis.upenn.edu/lf-current/deps.html.

In addition, chapters ProofObjects and IndPrinciples are included.

Within all chapters above:

- Do all exercises marked standard (non-optional and non-advanced)
- Do at least 10 optional exercises (in addition to the above)
- Do at least 4 advanced exercises (in addition to the above)

Home Assignments (Coq part 2)



Volume 2: Programming Language Foundation

https://softwarefoundations.cis.upenn.edu/plf-current/

Do all chapters in https://softwarefoundations.cis.upenn.edu/plf-current/deps.html, including core and contributed chapters, except: HoareAsLogic, Sub, RecordSub, and Norm

Within all chapters above:

Must do all exercises marked standard (non-optional and non-advanced)

Must do at least 10 optional exercises (in addition to the above)

Must do at least 4 advanced exercises (in addition to the above)

Home Assignments (Reflection Report)

Two days before the final seminar, you must submit a report

The report should be 3-5 pages, with font size 11, single column, and include comprehensive discussions and reflections on the following topics (as separate headlines):

- **Dependent types.** Explain in detail, reflect on its use.
- **Different proof assistants.** Give a short intro to each of them, discuss key differences and similarities. Include at least 3 proof assistants.
- **Ethical aspects.** Reflections on ethical aspects of mathematics in computer science. Reflect on the discussions from the seminar.

Details of how to submit all the assignments will be announced during the course.

Code of Honour

Note that you must follow KTH EECS Code of Honour
See this link

You are allowed to

- Discuss solutions with others

You are NOT allowed to

- Look at or copy any Coq solutions for the assignments
- Copy any text in the report, unless correctly quoted
- Use any AI tool for generating any text (it is OK to use tools like Grammarly for spelling and grammar checking)

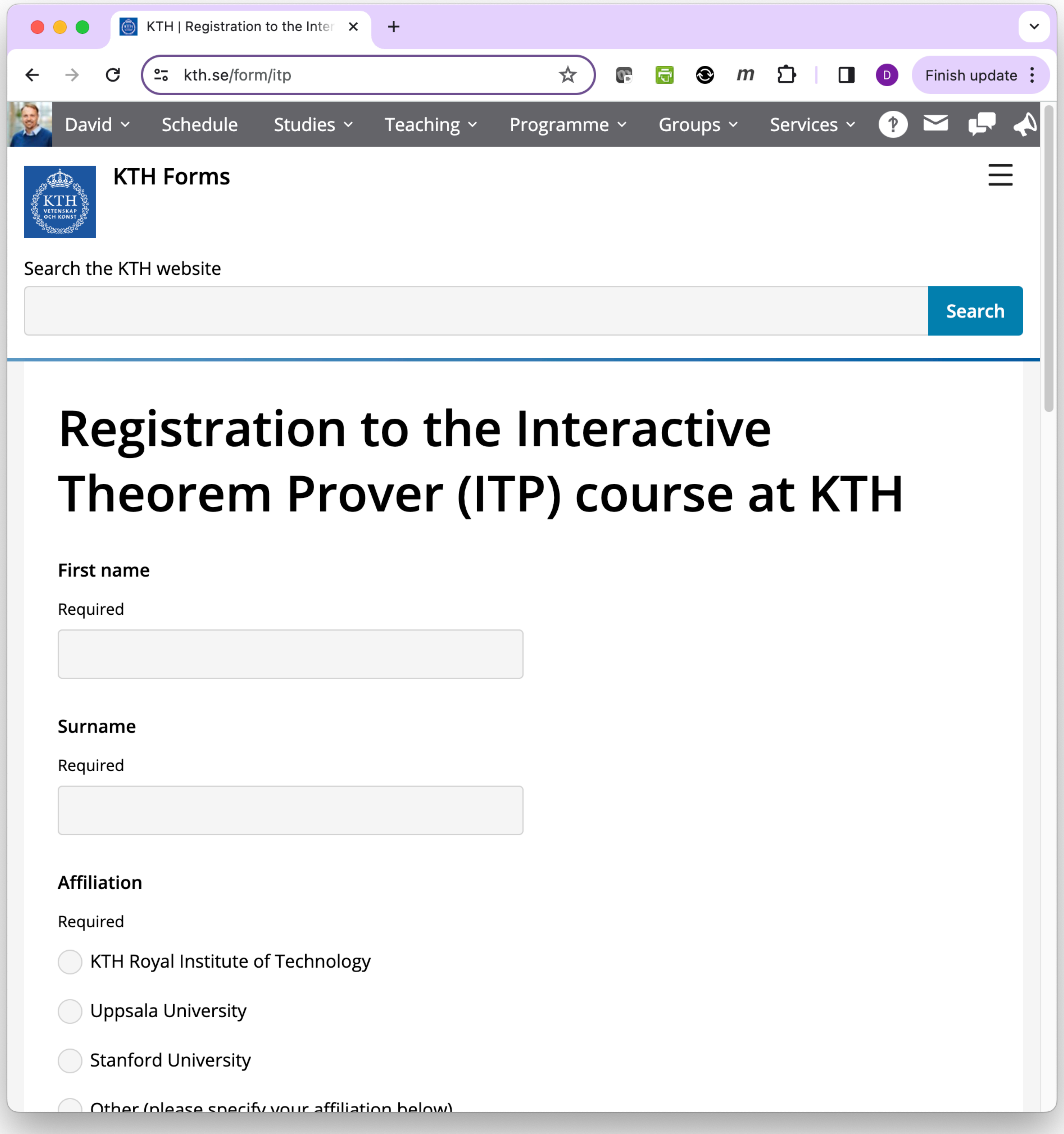
Examination

To be able to pass the course, you need to

- Solve **Coq assignments** from *Volume 1: Logical Foundation* and *Volume 2: Programming Language Foundation* from Software Foundations
- Write a 3-5 page **reflection report** discussion the concepts of dependent types, differences between different proof assistants, and reflections on ethical aspects of mathematics in computer science.
- Make an **oral presentation** at the final seminar, showing 1-2 advanced Coq proofs, as well as highlighting key aspects from the reflection document.

Attending lectures and seminars is optional but highly recommended.

Course Registration



Registration to the Interactive Theorem Prover (ITP) course at KTH

First name

Required

Surname

Required

Affiliation

Required

○ KTH Royal Institute of Technology

○ Uppsala University

○ Stanford University

○ Other (please specify your affiliation below)

Please register for the course (regardless if you take it for credits or not)

https://www.kth.se/form/itp

Course Slack Channels

After that you have registered, we will invite you to the Miking slack team.

Two relevant channels:

#itp-course-discussions

Q&A and discussion channels on any topics related to ITP and the course

#itp-course-info

Posts of general course info and news

Questions about the course organization?