CS 510 Theorem Proving and Program Verification – Fall 2018

Instructor: Andrew Tolmach
120-23 FAB (503) 725-5492
email: tolmach@pdx.edu
Office Hours: MW 1-2pm & by appt.
Course web page: http://web.cecs.pdx.edu/~apt/cs510coq

Description

The course will be a hands-on introduction to interactive theorem proving and program verification using the Coq proof assistant. Program verification can be used to prove that programs will behave properly for all possible inputs and execution paths (unlike testing, which can only show correct behavior for particular inputs and executions). A proof assistant doesn't prove things itself; rather, it helps a human construct a proof more easily and reliably. We will begin by learning how to verify properties of very simple functional programs, and then progress to proofs about more interesting functional programs, imperative programs and other formal systems. If time permits, we will take a brief look at fully automated theorem provers, which work without direct human guidance.

Prerequisites

There are no official course prerequisites, but prior exposure to basic discrete mathematics and formal proof is essential. This course is all about the intersection between programming and mathematics, so you should feel comfortable with both. Undergraduates should have completed CS250, CS251 and preferably CS320 and CS350. (CS311 is also useful, but not expected.) Prior exposure to functional programming (e.g. CS457/557 or CS558) will also be very useful, but is not required.

Readings

There is no published textbook, but for the bulk of of the course, we will be using the on-line textbook Software Foundations, by Benjamin Pierce et al. This book is under continuous revision; the version we are using will be made available on the course web page as we proceed.

Requirements

There will be weekly homework exercises, a midterm and a final.

The course grade will be distributed as follows:

40%	Homework
25%	Midterm (in class)
35%	Final (possibly take-home – to be determined later)

Assignments and exams will contain problems at two levels: "standard" and "advanced." Students enrolled at the 500-level will be required to attempt the advanced questions; students at the 400-level are welcome to attempt the advanced questions too, but are not expected to do so.

Although it will not be formally assessed, class participation is strongly encouraged, and may affect borderline grades.

Computing Facilities

The course will require use of the Coq proof assistant. While the precise version we use doesn't matter too much, it will be easiest and safest if we all use the *same* version, namely version 8.8.1. This is (or will be) available on the CS linux lab machines as package `coq`. You will probably also want to install it yourself on your own laptop; see the course web page for pointers.

To interact with Coq, an IDE is a must; there are two choices of roughly equal quality. If you are an emacs user (or would like to become one), try the ProofGeneral environment (a general-purpose theorem proving IDE that has a Coq binding). Otherwise, you can use CoqIDE, which runs as a stand-alone tool on linux, MacOS, and Windows. See the course web page for pointers.

Individual Work

It is permitted (even encouraged) for you to work together on homework assignments. However, all homeworks must be prepared and submitted individually; the whole goal of the course is for you to become comfortable using the proof assistant yourself.

Exams must be completed individually without any collaboration. Plagiarism or collaborating on an exam will result in an automatic zero grade and the initiation of disciplinary action at the University level.

Disabilities

If you are a student with a disability in need of academic accommodations, you should register with Disability Services for Students and notify the instructor immediately to arrange for support services.

Title IX Reporting Obligations

Portland State is committed to fostering a safe, productive learning environment. Title IX and our school policy prohibit gender or sex-based discrimination and sexual misconduct (including harassment, domestic and dating violence, sexual assault, and stalking). We expect a culture of professionalism and mutual respect in our department and class. You may report any incident of discrimination or discriminatory harassment, including sexual harassment, to either the Office of Equity and Compliance (`https://www.pdx.edu/diversity/office-of-equity-compliance`) or the Office of the Dean of Student Life (`https://www.pdx.edu/dos/student-conduct-at-psu`).

Please be aware that members of the faculty have the responsibility to report any instances of sexual harassment, sexual violence and/or other forms of prohibited discrimination to PSU's Title IX Coordinator, the Office of Equity and Compliance or the Dean of Student Life and **cannot keep information confidential**. If you would rather share information about sexual harassment or sexual violence to a confidential employee who does not have this reporting responsibility, you can contact a confidential advocate at 503-725-5672 or by scheduling on-line (`psuwrc.youcanbook.me`) or another confidential employee found on the sexual misconduct resource webpage (`https://www.pdx.edu/sexual-assault/get-help`). For more information about your obligations and resources for sex/gender discrimination and sexual violence (Title IX), please complete the required student module Creating a Safe Campus in your D2L (`https://www.pdx.edu/sexual-assault/safe-campus-module`).

Tentative Schedule

This schedule is highly subject to change.

dates	*topics*
Sep 25 & 27	Introduction to Coq; Simple functional programs and proofs
Oct 2 & 4	Lists, polymorphism, higher-order functions
Oct 9 & 11	More Coq tactics; Logical connectives
Oct 16 & 18	More propositions
Oct 23 & 25	Proofs and computations; Coq automation
Oct 30	**Midterm**
Nov 1	Proofs of functional algorithms
Nov 6 & 8	More proofs of functional algorithms
Nov 13 & 15	Proofs of imperative programs; Hoare logic; invariants
Nov 20	Imperative program semantics
Nov 22	**No Class** Thanksgiving
Nov 27 & 29	Automated program provers
Dec 4	**Final Exam (5:30-7:20pm)** (if needed)