Course Code	Course Title
COMP 4901X	**Formal Reasoning about Programs**

Course Description

Modern software systems control a vast portion of our life and are often safety-critical, e.g. it would be catastrophic for an airplane autopilot or a medical device to have a bug. Thus, it is important to ensure that our software works correctly under all possible circumstances. With this goal in mind, this course introduces the well-known interactive proof assistant Coq and relies on it to develop simple ways of applying logical reasoning to programs in order to establish their correctness and safety. This is a hands-on course with 2 mini-project homeworks. Students who do not have the prerequisites but with equivalent background may seek approval from the instructor for enrollment in the course.

List of Topics

The tentative syllabus is as follows, course instructor might change it slightly based on the actual speed of the class:

1. Formal Semantics of Programs (Operational, Denotational, and Axiomatic)
2. Introduction to the Coq Proof Assistant
3. Inductive Types, Recursive Functions and Term Rewriting
4. Lambda calculus semantics
5. Hoare Logic
6. Formal Verification based on Hoare Logic (Safety, Liveness, Fairness and Termination Analyses)
7. Automation of the Analyses in 6 in Coq
8. Separation Logic and Reasoning about Heap-manipulating Programs
9. Incorrectness Logic
10. Operational Semantics for Concurrent Programs
11. Pi Calculus

Intended learning outcomes (ILOs) of the course:

Familiarity with and problem-solving ability in:

- The formal meaning of programs (operational semantics, small-step and big-step)
- Verifying the correctness of programs (model checking), specifically using the Coq proof assistant which is standard in both academia and industry
- Automated theorem proving using Coq
- Abstract Interpretation
- Data-flow Analysis
- Hoare Logic

Textbook / Reference books:(optional)

Formal Reasoning About Programs" by Adam Chlipala, MIT
http://adam.chlipala.net/frap/

Grading Scheme

Two Coding Homeworks: 25% each
Written Final Exam: 50%