

Software Foundations

CIS500
Spring 2013

<http://www.seas.upenn.edu/~cis500>

Introductions



Benjamin Pierce
bcpierce@cis



Arthur Azevedo de Amorim
aarthur@cis



Marco Gaboardi
gaboardi@cis

Overview

Reliability

Approaches to Reliability

- Social
 - Extreme programming, etc.
- Methodological
 - Design patterns, APIs, etc.
- Mathematical ←————— *This course*
 - “formal methods”...

Software Foundations

- Mathematical underpinnings for reliable software

Five Interwoven Threads

1. basic tools from **logic** for making and justifying precise claims about programs;
2. the use of **proof assistants** to construct rigorous logical arguments;
3. the idea of **functional programming**, both as a method of programming and as a bridge between programming and logic;
4. techniques for formal **verification** of properties of specific programs; and
5. the use of **type systems** for establishing well-behavedness guarantees for all programs in a given programming language

Logic

- “The calculus of computer science”

Proof Assistants

- Rigorous support for *checking* proofs
- Semi-automatic support for *writing* proofs
- Coq

- Logic \rightarrow hacking :-)

Functional Programming

- Key ideas:
 - *pure* computation
 - “persistent” data structures
 - functions as data (“first-class functions”)
- An attractive way of programming
 - Easier reasoning
 - Better scaling / parallelization
- A bridge to logic

Program Verification

- “Does this program sort lists?”
 - “Does this one correctly steer the plane?”
- “Do these programs behave the same?”
 - “Does this optimizer *always* produce programs that behave the same (as the ones it started with)?”

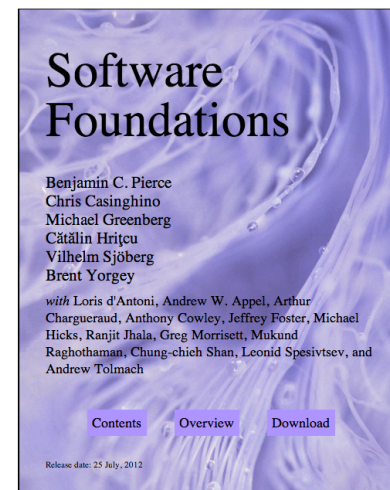
Type Systems

- The world's most popular *lightweight formal method*
- Extremely effective in detecting bugs and helping structure complex software

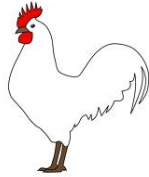
(over to Coq...)

Things to Do

Textbook



Coq

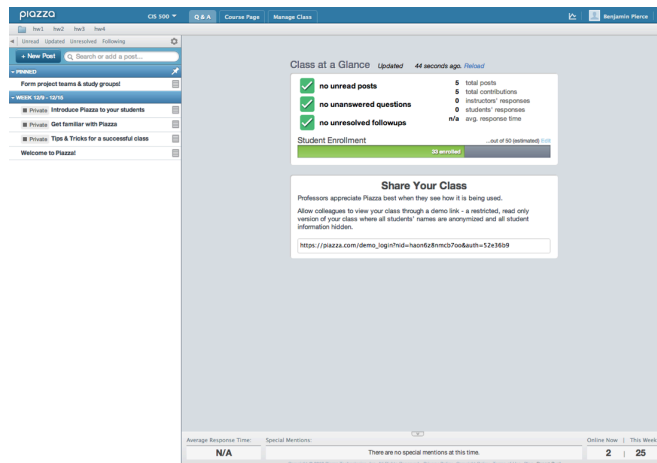


Available on CETS systems;
easy to install on your own machine

Clickers



Piazza



<https://piazza.com/upenn/spring2013/cis500>

Summary

- Now:
 - Register for Piazza group: <https://piazza.com/upenn/spring2013/cis500>
 - Check that you can sign into cis500 page on Blackboard
 - Read through the “Logistics” section of the handout
- By Monday:
 - Buy a “clicker” at the bookstore
 - Read chapters Preface and Basics
- By Wednesday:
 - download and install Coq on your machine (or use the one on CETS machines)
 - download file Basics.v from course web page
 - complete all non-optional exercises
 - submit via Blackboard by noon on Wednesday

Course Logistics

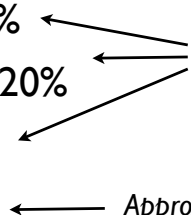
Collaboration

- Collaboration on homework assignments *encouraged*
- Studying with other people is an excellent way to internalize the material
- Feel free to form study teams (of size at most 3, ideally 2)

Homework

- Small part of your grade, but a large part of your understanding — impossible to perform well on exams without seriously grappling with the homework
- Submit one assignment per study group
- Late policy: Late homeworks lose 25% of their value for each day (or partial day) after the announced deadline

Evaluation

- First midterm: 20%
 - Second midterm: 20%
 - Final exam: 40%
 - Homework: 20%
- Dates TBA*
- Approximately weekly*
- 

(Lack of) Extra Credit

- Grade improvements can only be obtained by sitting in on the course next year and turning in all homeworks and exams.
(If you are doing this to improve your grade from last year, please drop me an email so I know who you are.)
- There will be no extra credit projects, either during the semester or after the course ends. Concentrate your efforts on this course, now.