GCMPSC 266

Formal Specification and Verification

Dick Kemmerer

Goals for the Course

- Each student familiar with basic verification techniques
- Capable of reading and evaluating verification literature
- Capable of pushing the frontiers of verification research

Prerequisites

CMPSCI 130AB

Formal Logic

Homework

Approximately Weekly
Late homework not accepted

Final Exam

Thursday, March 22, 2007 Noon-3:00pm

Detailed Synopsis and Review of Formal Methods Topic or Research Project

Grade Based On

Homework
Paper or Project
Final

Final Exam

Thursday March 19, 2009
Noon - 3:00pm

NO MAKEUP EXAMS

Office Hours

Tuesday 1:00 - 2:00pm
Thursday 1:00 - 2:00pm
and by appointment

Drop in anytime

For Thursday Read

"UNISEX: a UNIx-based Symbolic EXecutor for Pascal" by Kemmerer and Eckmann

Introduction to Verification

- What is it?
- Total vs. Partial Correctness
- Consistency vs. Correctness

Code Level Proofs

- Partial Correctness
- Total Correctness
- Consistency vs. Correctness

Entry Assertion - Conditions expected to be true upon entry to a program

Exit Assertion - Conditions that are expected to be true when the program is exited

Correctness Assertions - Bob Floyd

A procedure is said to be correct (with respect to its input and output assertions) if the truth of its input assertion upon procedure entry insures that if the procedure halts its output assertion will be true upon procedure exit.

Consider the case where we have an array A and we want to specify a procedure that sorts the first n+1 elements of A in ascending order.

We'll use entry and exit assertions to do the specifying