Software is increasingly becoming the vehicle of modern civilization, playing a crucial role in our society. All activities including telecommunications, transportation, and banking rely on software systems. Consequently, the problem of making software reliable and secure has become one of today’s most important challenges. Studies estimate that bugs in software cost businesses worldwide about $175 billion annually. In addition, software failures can lead to loss of life in safety-critical systems such as airbag-deployment systems and aircraft collision-avoidance systems.

The goal of this course is to learn essential techniques that enable the construction of highly reliable software. As we will see in this course, formal specification techniques allow for the construction of automated verification tools that can perform tests on specifications and corresponding code to find errors in requirements, models, designs, and implementations. In this course, we will study a collection of techniques for formal software development, spanning from high-level semantic modeling to coding and debugging. The study will be done not in the abstract, however, but through the use of actual tools supporting these techniques.

Prerequisites

Grades of C- or above in Software Engineering I, or consent of instructor.
Familiarity with basic set theory and propositional and first-order logic will be helpful.

Web Page

Students are expected to check the course web site on a regular basis (at least every other day) for announcements regarding the course.

Performance Objectives

- Students will be able to write verification-oriented models of non-trivial systems
- Students will be able to express desirable properties of systems in formal requirements notations
• Students will be able to use verification tools to determine whether design models satisfy their desired properties
• Students will understand the algorithms underlying verification tools and the strengths and limitations of those algorithms

Textbook and Reading Material

There is no required textbook for this course. Reading materials will be available on the course web site. They will include several papers on formal software specification and verification, a number of papers on how to use the specification/verification tools adopted in the course, and various class notes.

Grading Policy

The weighting of items in grade determination will be the following:

<table>
<thead>
<tr>
<th>Item</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class Participation</td>
<td>20%</td>
</tr>
<tr>
<td>Homeworks</td>
<td>40%</td>
</tr>
<tr>
<td>Midterm</td>
<td>20%</td>
</tr>
<tr>
<td>Final Exam</td>
<td>20%</td>
</tr>
</tbody>
</table>

The midterm will be held on 3/5/2007 during class time (subject to change). The final exam will be held as per university schedule. The following grading scale will be used: A – 90; BA – 85; B – 80; CB – 75; C – 70; DC – 65; D –60.

Course Policies

Assigned Readings: You are expected to do all the assigned readings.

Additional Readings and discussions: You are urged to consult sources other than the prescribed readings. You are also encouraged to discuss the course topics with your classmates.

Homework assignments: You are allowed and encouraged to discuss the homework assignments with your classmates, but you are not allowed to share solutions. Since the homework counts as a significant portion of your grade, it is expected that the submitted work be strictly your own. (The following rule of thumb will help you not to cross the line: discuss the assignments together but do not take any written notes; go home and write the solution by yourself.)

Cheating: Copying someone else's work or sharing solutions will result in a zero on the assignment for the first offense and an F in the course for the second offense.
Late submissions: Your solutions to written assignments are to be submitted in class, before the class starts. Late written assignments can be handed in during office hours or in class. Alternatively, they can be put in the instructor's mailbox. In that case, you must notify the instructor by email at once. Late assignments will be graded according to the following policy:

- 15% of the actual score will be taken off for assignments submitted between 0 and 24 hours after the deadline.
- 35% of the actual score will be taken off for assignments submitted between 24 and 48 hours after the deadline.
- No assignments will be accepted after that.

Attendance: Students are expected to attend all classes. Your knowledge and therefore your grade depends on it. You are responsible for all announcements and material covered during class even if you did not attend. In that case, check with the instructor or with your classmates.

Extra credit: No extra-credit homeworks or tests will be given on an individual basis (although they may be given to the whole class).

Missed exams: If you miss an exam (Midterm or Final Exam), the decision as to whether or not it is made up and how it is made up will be made on an individual basis. To be excused there must be significant circumstances beyond the student’s control. Generally this will require documentation, such as a doctor’s note in the case of illness. Normally, if the absence from an exam is excused, the average of the other exam and class participation will be used to replace it. If it is unexcused, 70% of the average of the other exam and class participation will be used. At most one missed exam, excused or unexcused, will be made up in this way. You must inform the instructor before the exam if there are circumstances beyond your control that will cause missing an exam.

Use of Electronic Devices: You are expected to stay alert and pay attention to the directions/announcements in the class. Cellphones, PDAs, and other electronic devices should NOT be used during the lecture and should be turned-off. If available, please do bring your laptop to the class. Web-surfing of non-course related material is NOT permitted during the class. In order to maintain the integrity of the classroom and if I feel it is distracting you or others, I may ask you to turn-off your laptop.

Incomplete Grades: Please note that the incomplete grade - I - is intended for the student who has missed a relatively small portion of work due to circumstances beyond his/her control. In general, performance on work done must be at a level of C or better in order to qualify for an incomplete. An I grade will not be given to replace an otherwise low or failing grade in the class.

Academic Honesty
The following statement has been approved and distributed by the Western Michigan University Faculty Senate:
You are responsible for making yourself aware of and understanding the policies and procedures in the Undergraduate (pp. 274-276) [Graduate (pp. 25-27)] Catalog that pertain to Academic Honesty. These policies include cheating, fabrication, falsification and forgery, multiple submission, plagiarism, complicity and computer misuse. If there is reason to believe you have been involved in academic dishonesty, you will be referred to the Office of Student Conduct. You will be given the opportunity to review the charge(s). If you believe you are not responsible, you will have the opportunity for a hearing. You should consult with me if you are uncertain about an issue of academic honesty prior to the submission of an assignment or test.

Unless otherwise told, you may not bring aids to exams. Submission of another person’s work in part or whole is not permitted. Learning can certainly occur with discussion of class material and assignments with other students, and we will be doing considerable collaborative activity, but at all times take care that you don’t represent the work of another as your own.

• If you are copying another’s work in part or whole, either by hand or electronically, you are going too far.

• If two or more people are working so closely together that the outcomes, particularly on significant portions of computer programs, are essentially line-by-line the same in logical structure, they are going too far.

• You should not give your completed work to someone else or accept another’s completed work to “review or look at” in either hardcopy or electronic form. This too easily facilitates copying.

Easy availability of information, material, source codes, lecture notes etc on the Internet may make it possible to find solutions to your assignments on the Internet or elsewhere. It is okay to refer to those, understand them and use them to enhance your solutions, generate your own ideas etc. However, you must give proper and full credit to original authors of the work, if you include their ideas and/or solutions. Failing to do so is part of academic and professional dishonesty. It will not be tolerated in this class. Do not give in to temptations.

If you are found responsible for violation of academic honesty in the course, you will receive a penalty up to and including an E grade in the class.

Topic Outline

The outline is tentative and will be adjusted as necessary during the course of the semester.

• Introduction
  o The role of formal methods in software engineering
• Mathematical Background
  o Sets and relations
o Propositional and First-order Logic
  o Computational Tree Logic
• Alloy Specifications
  o Introduction to Alloy
  o Alloy Basics
  o Modeling and Analyzing Using Alloy/ACA
  o Alloy Case Studies
• Formal Verification
  o CTL Model Checking
  o BDDs and SAT
  o Symbolic Model Checking
• Design by Contract
  o Light-weight specifications
  o Extended Static Checking
  o Introduction to ESC/Java
  o Annotating and checking Java code with ESC/Java

Acknowledgement

In order to provide the highest quality course, I will use substantial material adapted from the road-tested and highly successful course CIS 771 at Kansas State. This material is generously provided by Matthew Dwyer and John Hatcliff.