CAS 707 — Formal Specification Techniques

7 January 2013

Outline

Instructor: Dr. Wolfram **Kahl,** Room: ITB-245, E-Mail: kahl@mcmaster.ca

Calendar Description

Topics include: Pre-/postconditions, refinement, state-based approaches, event based approaches, algebraic specifications, Petri nets, temporal logic, properties of programs, specification verification and validation.

Course Objective

The main objective is to introduce students to commonly used formal state-based, event-based, and algebraic techniques to specify and verify software systems. The course aims as well at fostering understanding of the mathematical foundations of these specification techniques, and the development of the skills needed to set up and manipulate mathematical models that mimic relevant features of software systems.

Course Pages: http://www.cas.mcmaster.ca/~kahl/CAS707/2013/

This is where you will find further information, announcements, and useful links.

It is the student's responsibility to be aware of the information in the course Web pages, and to check regularly for announcements.

Literature: The first book is concise treatment of Logic for CS with applications to formal specification; the other two cover a broad range of relevant topics; additional Literature will be listed on the course page.

- ***RSD***: José Bacelar Almeida, Maria João Frade, Jorge Sousa Pinto, Simão Melo de Sousa. *Rigorous Software Development — An Introduction to Program Verification.* Undergraduate Topics in Computer Science. Springer, London, 2011. URL *http://www.springerlink.com/content/978-0-85729-017-5/*.
- ***Logics of Specification Languages***. Monographs in Theoretical Computer Science. Dines Bjørner and Martin C. Henson (Eds.) ISBN: 978-3-540-74106-0 Online version available at http://www.springer.com/computer/foundations/book/978-3-540-74106-0
- ***Specification of Software Systems***, 2nd edition. V.S. Alagar and K. Periyasamy, ISBN: 978-0-85729-277-3 Online version available at http://www.springerlink.com/content/978-0-85729-276-6

Major Topics, not necessarily treated in that sequence:

- Foundations: Logic, Discrete Mathematics, Universal Algebra, Category Theory
- Algebraic Specification — CASL
- Hoare Logic, Contracts, and Refinement
- Model-Based Specification Techniques: VDM, Z, B
- Property-Oriented Specification Techniques
- Temporal and Event-Based Formalisms
- Model Checking

Grading:

- **Presentation Assignments** may involve any or all of the following:
  - reading additional material covering formal specification languages and tools
  - developing solutions to specified tasks, possibly using tool support
  - giving in-class presentations (slides are to submitted to the instructor as PDF for presentation at least **one hour before class**)
  - providing written summaries
  - providing exercise and exam questions about the presented material

  There will be several short presentations at the beginning of the course and possibly some longer presentations later. Some presentation assignments will allow group work.

  At the end of each class involving student presentations, **peer evaluation** will be conducted at least for the presentation aspects. The instructor reserves the right to override peer evaluation results if the process becomes flawed or manipulated.

- All **Presentation Assignments**:   42%
- **Attendance and participation**:   8%
- **Midterm Exam** (an **individual 5–10 minute oral examination** for each student):   10%
- **Final Exam** (an **individual 20 minute oral examination** for each student):   40%

Course Adaptation

The instructor and university reserve the right to modify elements of the course during the term.

The university may change the dates and deadlines for any or all courses in extreme circumstances. If either type of modification becomes necessary, reasonable notice and communication with the students will be given with explanation and the opportunity to comment on changes.

It is the responsibility of the student to check their McMaster email and course websites weekly during the term and to note any changes.

Academic Ethics

You are expected to exhibit honesty and use ethical behaviour in all aspects of the learning process. Academic credentials you earn are rooted in principles of honesty and academic integrity.

Academic dishonesty is to knowingly act or fail to act in a way that results or could result in unearned academic credit or advantage. This behaviour can result in serious consequences, e.g. the grade of zero on an assignment, loss of credit with a notation on the transcript (notation reads: "Grade of F assigned for academic dishonesty"), and/or suspension or expulsion from the university.

It is your responsibility to understand what constitutes academic dishonesty. For information on the various types of academic dishonesty please refer to the Academic Integrity Policy, located at http://www.mcmaster.ca/academicintegrity.

The following illustrates only three forms of academic dishonesty:

(1) Plagiarism, e.g. *the submission of work that is not one's own* or for which other credit has been obtained.

(2) Improper collaboration in group work.

(3) Copying or using unauthorised aids in tests and examinations.

Discrimination

The Faculty of Engineering is concerned with ensuring an environment that is free of all adverse discrimination. If there is a problem that cannot be resolved by discussion among the persons concerned, individuals are reminded that they should contact the Department Chair, the Sexual Harassment Office or the Human Rights Consultant, as soon as possible.