McMaster University
Department of Computing and Software
Dr. W. Kahl

Outline

COMP SCI 3EA3 — Software Specification and Correctness

6 September 2012

Instructor: Dr. Wolfram **Kahl,** Department of Computing and Software, ITB-245
E-Mail: kahl@cas.mcmaster.ca

Calendar Description:

Formal specifications in software development; logical formalisms; functional and relational specifications; completeness and consistency of specifications; verification; validation; presentation of information; tool supported verification.

Goals:

- Understanding of the motivation of mathematical approaches to software specification
- Understanding of the essence of logical formalisms
- Translation skills between natural language and logical formalisms
- Knowledge of important proof systems for propositional logic and first-order predicate logic, and skills in producing formal proofs
- Ability to evaluate formal software specifications
- Knowlege of different logical formalisms, of the principles of related tool support, and associated selection criteria
- Knowledge of typical approaches to formal software specification and verification

Course Pages: http://www.cas.mcmaster.ca/~kahl/CS3EA3/2012/

This is the main entry point where you find further information, especially concerning tutorial organization and software installation. Electronic versions of the assignment sheets will also be kept there, and/or on the course's **Avenue** site.

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

Schedule:

Lectures: Tuesday, Thursday, Friday 14:30–15:20, JHE-A101

Tutorial: Thursday, 9:30–10:20, starting 13 September, usually room T13-106.
The tutorial normally discusses student work on exercise problems, or prepares aspects of assignments.
Every student is expected to complete the scheduled work, i.e., exercise problems or necessary reading, ***before*** the corresponding tutorial session.
Occasionally, special sessions in computer-equipped labs may be announced on course pages.

Office Hours: TBA, and by appointment.

Students are expected to attend all lectures and tutorials.

Literature:

Main Textbooks:

LADM: David Gries, Fred B. Schneider. *A Logical Approach to Discrete Math.* Springer, 1993. ISBN: 978-0387941158 ***(Used in CS1FC3 in 2011)***

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/.*
(Available as electronic ressource via the McMaster library)

"Using Z" — Introduction to the Z Specification Notation
Jim Woodcock, Jim Davies. *Using Z: Specification, Refinement, and Proof*. Prentice Hall, 1996. URL *http://www.usingz.com/*. ISBN 0-13-948472-8
- Out of print; **available on-line**.
- Useful as an introduction to logic via natural deduction; also covers basic discrete math (sets, functions, relations…) extensively.

A Logic Textbook that also treats Model Checking:
Michael Huth, Mark Ryan. *Logic in Computer Science, Modelling and Reasoning about Systems.* Cambridge University Press. Second edition, 2004.
- Conventional untyped (single-sorted) presentation of logic via natural deduction; also includes chapters on Hoare logic and on temporal logic.

Specification and Verification in the Software Development Context:
Carlo Ghezzi, Mehdi Jazayeri, Dino Mandrioli. *Fundamentals of Software Engineering.* Prentice Hall. 2nd ed., 2003.

Additional material may be handed out or made available electronically via the course pages.

Outline:

(With relevant textbook chapters indicated — not all textbook contents will be covered in detail. Times are rough estimates.)

- Introduction (0.5 weeks, RSD 1–2)
- Review of logical notation (0.5 weeks, LADM 1–4,8–11, Using Z 2–4)
- Introduction to Hoare logic (2 weeks, LADM 1.6, 10, 12.6)
- Theory of propositional logic, and related tools (2 weeks, RSD 3)
- Theory of predicate Logic, and related tools (3 weeks, RSD 4)
- Hoare logic in depth (2.5 weeks, RSD 5–7)
- Specification of modular systems (1 week, RSD 8)
- Larger applications (1 week, e.g. RSD 9–10)

In several topics, mastering **mechanised techniques (tool support)** will be part of the course requirements.

Grading:

All examinations in this course will be **Closed Book**. That is, no written or printed material nor a calculator nor other electronic aids may be used during the examinations.

> After notations, presentation rules, and basic definitions and proof rules have been introduced in class, **students are expected to know them at all times**.

Assignments

There will be graded **Assignment Questions**, and ungraded **Exercises**, essentially on a weekly basis. ***It is essential that you meet the deadlines*** for the assigments; there is no credit for documents handed in after the deadline, except with properly documented accommodation reasons. *If you cannot hand in your assignment on time* **due to (e.g.) illness reasons**:

- Hand your assignment in as soon as possible. If the assignment in question required handing in paper, hand your solution either to the instructor, or to the TA, or to Tina in the departmental office. (Last resort outside office hours: Insert into the drop box in front of the departmental office ITB-202.) For electronic submission, there will be a "Late Dropbox" on Avenue.

  We will make note of the time of your submission, which must be **before** solutions are discussed in class or tutorial.
- Follow the usual procedures for missed work with your Associate Dean's office. **The outcome of that process will decide whether/how the late submission can be counted.**

Accomodations for **missed work**,

including **late assignments**, require the corresponding form from the Associate Dean's office. Where you use the electronic system, note that you are still **required** to get in touch with the instructor to actually be granted any accomodation.

Final Exam

The **final examination** will be scheduled by the Registrar's Office in the usual way. It will be a closed book examination of three hours duration and cover the material of **all** lectures, tutorials, handouts, and assignments.

Midterms

In addition, there will be **two midterm examinations**, details to be announced.

Grade Calculation

All exam grades will be percentage grades.

For every student, the course grade is calculated as a weighted average:

- For n being the number of assignments this course will have had, 30% of the weight are given to your $(n-1)$ best assignments;
- those midterms that are better than the final count 20% each, and those midterms that are not better than the final count 10% each;
- the remaining weight (between 30% and 50%) is given to the final.
- Some exercise sheets or assignments may contain ***bonus questions***; marks for solutions to these will be added to the final mark *for those who have passed the course.*

The course grade will be converted from a percentage grade to a letter grade according to the scale of the Registrar's Office.

The instructor reserves the right to conduct any deferred exams orally.

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 four 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) ***Collaboration where individual work is expected.***

> **You hoave to produce your submissions for assignment questions yourself, and without collaboration** (except where and as far as group work is explicitly allowed or specified by the assignment statement).
>
> For each assignment question there will normally be exercise questions similar to it — you ***are allowed*** to collaborate on these ***exercise questions***. (The tutorials are typically not expected to cover all exercise questions.)

(3) Improper collaboration in group work.

(4) ***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.