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

CAS 707 — Formal Specification Techniques

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

Course Objective

The main objective is to introduce students to the application of logical formalisms in software specification and verification. The course aims as well to foster understanding of the mathematical foundations of these specification techniques, and the development of the skills needed to set up and manipulate mathematical models for relevant features of software systems.

Goals:

- Understanding of the motivation of mathematical approaches to software specification
- Knowledge of typical approaches to formal software specification and verification
- Ability to produce and evaluate formal software specifications
- Experience with a selection of current software specification formalisms and verification tools
- Knowlege of different logical formalisms, of the principles of related tool support, and associated selection criteria

Course Page: `https://www.cas.mcmaster.ca/~kahl/CAS707/2022/`

While most of the internal electronic information exchange for this course will be handled via **Avenue**, the course pages will contain useful links to external material, and will also serve as central fallback location for making information and material available outside Avenue, in particular in the case of Avenue accessibility problems.
It is the student's responsibility to be aware of the information on the course Avenue site, and, while Avenue is down, on the course web page, and to check regularly for announcements.

Outline

• Review of propositional and predicate logic and basic discrete math,	(CalcCheck, Using Z chapts. 1–10, parts of RSD chapt. 4)
• Model-based spacification (e.g., Z, B)	(e.g., Using Z)
• Hoare logic, verification condition generation	(Gordon, RSD)
• Specifying and verifying imperative programs	(Frama-C or other tools)
• Separation logic	(Gordon, Reynolds)
• Algebraic specification; specification by colimits	(e.g., Maude)
• Temporal logic, model-checking	(e.g., `nusmv`)
• Selection of other topics	(time permitting)

In several topics, mastering **mechanised techniques (tool support)** will be part of the course requirements.
Depending on the interests and preparation of the course participants, some of the above-listed topics may be replaced with other relevant topics.

Grading:

Assignments: There will be graded **Assignment Questions** (and possibly ungraded **Exercises**), essentially on a weekly basis for roughly the first two months.

Most assignments will be graded only summarily.

There may be individual assignments requiring short presentations.

Grade Calculation: All exam grades will be percentage grades.

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

- All **Assignments** together: 25%
- A **Project**, with deliverables typically including a handout, source files and presentation slides publicly submitted to Avenue, and a presentation held in class: 15%
- **Attendance, participation, and class preparation**: 5%
- **Midterm Exam** (**individual ≈10-minute oral examination** for each student in the week Feb. 28 to March 4): 15%
- **Final Exam** (**individual ≈20-minute oral examination** for each student): 40%

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

Literature

CALCCHECK `http://CalcCheck.McMaster.CA/`

"LADM": *A Logical Approach to Discrete Math*, by David Gries and Fred B. Schneider, Springer 1993, ISBN 3-540-94115-0 (the book motivating CALCCHECK)

"Using Z": *Using Z: Specification, Refinement, and Proof*, by Jim Woodcock and Jim Davies, Prentice Hall, 1996 (available on-line at `http://www.usingz.com/`).

Useful also as a **gentle** introduction to typed logic via natural deduction; also **covers basic discrete math** (sets, functions, relations…) extensively.

"RSD": *Rigorous Software Development — An Introduction to Program Verification*, by José Bacelar Almeida, Maria João Frade, Jorge Sousa Pinto, and Simão Melo de Sousa. Springer, London, 2011. DOI: 10.1007/978-0-85729-018-2 (available electronically via the McMaster library).

This is a useful reference for first-order logic for CS with applications to formal specification, including Hoare Logic.

"Gordon": *Hoare Logic*, by Mike Gordon; available on-line at `https://www.cl.cam.ac.uk/archive/mjcg/HL/`.

"Reynolds": *Introduction to Separation Logic*, by John C. Reynolds; available on-line at `https://www.cs.cmu.edu/afs/cs.cmu.edu/project/fox-19/member/jcr/www15818As2011/cs818A3-11.html`).

Also recommended:

"Huth-Ryan": *Logic in Computer Science, Modelling and Reasoning about Systems*, by Michael R. A. Huth and Mark D. Ryan, Cambridge University Press, 2nd edition 2004. `http://www.cs.bham.ac.uk/research/lics/`

Conventional untyped (single-sorted) presentation of logic via natural deduction; also includes chapters on Hoare logic and on temporal logic and model checking.

"Z Reference": *The Z Notation: A Reference Manual*, by J. M. Spivey, Prentice Hall, 1989 (out of print; available on-line at `http://spivey.oriel.ox.ac.uk/mike/zrm/`).

Classic "birthday book" specification in the introduction; far more accessible than the ISO standard for Z.

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

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 Integrity (see also page 4) — Course-Specific Notes

Academic credentials you earn are rooted in principles of honesty and academic integrity.

In the context of CAS 707, in particular the following behaviours constitute academic dishonesty:

1. *Plagiarism*, i.e., **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 have to produce your submissions for assignments yourself, and without collaboration (except where and as far as group work is explicitly allowed or specified by the assignment statement).

   - You are not allowed to copy & edit any portion of another student's work, nor from any websites, but you may use material from the course notes.
   - You are not allowed to give your solutions (or portions thereof) to another student.
   - You are not allowed to post full or partial homework or assignment solutions on discussion boards or websites (e.g., github, FaceBook, etc..).
   - You are not allowed to solicit solutions to the problem on on-line forums or purchasing solutions from on-line sources.
   - You are not allowed to submit a combined solution with a classmate.
   - You have to cite external sources that you have used.
3. **Accessing another students' Avenue or other relevant online account, or providing others access to your accounts.**
4. Meddling or attempting to meddle with online services used for course delivery.

Automatic Copyright of Course Materials

This is a reminder to students of copyright: In accordance with Canadian statutory and common law, any written or visual material that the instructor produces is automatically copyrighted. The instructor may pursue any violator of that copyright whether or not a notice is placed on the course material. Copyright does not dampen any ordinary use that colleagues or students make of the material.

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's Associate Chair for Undergraduate Studies, the Department Chair, the Sexual Harassment Office or the Human Rights Consultant, as soon as possible.

ACADEMIC INTEGRITY

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. **It is your responsibility to understand what constitutes academic dishonesty.**

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. For information on the various types of academic dishonesty please refer to the *Academic Integrity Policy*, located at https://secretariat.mcmaster.ca/university-policies-procedures-guidelines/

The following illustrates only three forms of academic dishonesty:

- plagiarism, e.g. the submission of work that is not one's own or for which other credit has been obtained.
- improper collaboration in group work.
- copying or using unauthorized aids in tests and examinations.

AUTHENTICITY / PLAGIARISM DETECTION

Some courses may use a web-based service (Turnitin.com) to reveal authenticity and ownership of student submitted work. For courses using such software, students will be expected to submit their work electronically either directly to Turnitin.com or via an online learning platform (e.g. A2L, etc.) using plagiarism detection (a service supported by Turnitin.com) so it can be checked for academic dishonesty.

Students who do not wish their work to be submitted through the plagiarism detection software must inform the Instructor before the assignment is due. No penalty will be assigned to a student who does not submit work to the plagiarism detection software. **All submitted work is subject to normal verification that standards of academic integrity have been upheld** (e.g., on-line search, other software, etc.). For more details about McMaster's use of Turnitin.com please go to www.mcmaster.ca/academicintegrity.

COURSES WITH AN ON-LINE ELEMENT

Some courses may use on-line elements (e.g. e-mail, Avenue to Learn (A2L), LearnLink, web pages, capa, Moodle, ThinkingCap, etc.). Students should be aware that, when they access the electronic components of a course using these elements, private information such as first and last names, user names for the McMaster e-mail accounts, and program affiliation may become apparent to all other students in the same course. The available information is dependent on the technology used. Continuation in a course that uses on-line elements will be deemed consent to this disclosure. If you have any questions or concerns about such disclosure please discuss this with the course instructor.

ONLINE PROCTORING

Some courses may use online proctoring software for tests and exams. This software may require students to turn on their video camera, present identification, monitor and record their computer activities, and/or lock/restrict their browser or other applications/software during tests or exams. This software may be required to be installed before the test/exam begins.

CONDUCT EXPECTATIONS

As a McMaster student, you have the right to experience, and the responsibility to demonstrate, respectful and dignified interactions within all of our living, learning and working communities. These expectations are described in the *Code of Student Rights & Responsibilities* (the "Code"). All students share the responsibility of maintaining a positive environment for the academic and personal growth of all McMaster community members, whether in person or online.

It is essential that students be mindful of their interactions online, as the Code remains in effect in virtual learning environments. The Code applies to any interactions that adversely affect, disrupt, or interfere with reasonable participation in University activities. Student disruptions or behaviours that interfere with university functions on online platforms (e.g. use of Avenue 2 Learn, WebEx or Zoom for delivery), will be taken very seriously and will be investigated. Outcomes may include restriction or removal of the involved students' access to these platforms.

ACADEMIC ACCOMMODATION OF STUDENTS WITH DISABILITIES

Students with disabilities who require academic accommodation must contact Student Accessibility Services (SAS) at 905-525-9140 ext. 28652 or sas@mcmaster.ca to make arrangements with a Program Coordinator. For further information, consult McMaster University's *Academic Accommodation of Students with Disabilities* policy.

REQUESTS FOR RELIEF FOR MISSED ACADEMIC TERM WORK

McMaster Student Absence Form (MSAF): In the event of an absence for medical or other reasons, students should review and follow the Academic Regulation in the Undergraduate Calendar "Requests for Relief for Missed Academic Term Work".

ACADEMIC ACCOMMODATION FOR RELIGIOUS, INDIGENOUS OR SPIRITUAL OBSERVANCES (RISO)

Students requiring academic accommodation based on religious, indigenous or spiritual observances should follow the procedures set out in the RISO policy. Students should submit their request to their Faculty Office ***normally within 10 working days*** of the beginning of term in which they anticipate a need for accommodation or to the Registrar's Office prior to their examinations. Students should also contact their instructors as soon as possible to make alternative arrangements for classes, assignments, and tests.

COPYRIGHT AND RECORDING

Students are advised that lectures, demonstrations, performances, and any other course material provided by an instructor include copyright protected works. The Copyright Act and copyright law protect every original literary, dramatic, musical and artistic work, including lectures by University instructors

The recording of lectures, tutorials, or other methods of instruction may occur during a course. Recording may be done by either the instructor for the purpose of authorized distribution, or by a student for the purpose of personal study. Students should be aware that their voice and/or image may be recorded by others during the class. Please speak with the instructor if this is a concern for you.

EXTREME CIRCUMSTANCES

The University reserves the right to change the dates and deadlines for any or all courses in extreme circumstances (e.g., severe weather, labour disruptions, etc.). Changes will be communicated through regular McMaster communication channels, such as McMaster Daily News, A2L and/or McMaster email.