Certified Programming with Dependent Types
CAS 763

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

Quick Introduction

Dependent types are everywhere in mathematics — you probably don't even notice them. But can you implement a matrix multiplication function in C, C++, Java, Rust, Go, Standard ML, OCaml, or Haskell 2010 such that the *type system* will catch attempts to multiply a 3-by-4 matrix with a 2-by-5 matrix? Dependent types can encode such constraints, and much more: Via the Curry-Howard correspondence, specifications expressed as logical formulae can be turned into types, so that the type checker can be used to guarantee data-type invariants and program correctness: Programs that are not proven correct then won't even compile!

The course CAS 763 will help you to learn the dependently-typed programming language Agda, practice formalising the mathematics needed for expressing datatype invariants and program specifications, and also acquire knowledge and understanding of the relevant foundations.

Previous experience with Haskell wold be useful, but is not strictly necessary. Familiarity with basic propositional and predicate logic is essentially assumed.

Calendar Description

Type systems featuring types depending on values empower not only logics that can capture common mathematical formalisations more naturally than conventional first-order or higher-order logics; they also empower programming languages where specifications may be incorporated into the type of programs, and well-typed programs are thus guaranteed to satisfy these specifications.

Students will learn at least one dependently-typed programming language in depth. The course will also cover associated foundations, including relevant type theories and the Curry-Howard correspondence, as well as useful patterns of formalising, programming, and proving in dependently-typed programming languages.

Topics

The main language for this course will be Agda2 (usually simply referred to as "Agda").

- Brief review of conventional logic, using CALCCHECK
- Basic functional programming with pattern matching in Agda
- The Curry-Howard correspondence: Formulae as types, proofs as data
- Proving properties of functional programs
- Indexed datatypes
- Simple certified programs: Incorporating specifications into types
- Invariant-carrying datatypes
- Representing typed data: Expression languages, logics and programming languages
- Dependently-typed programming patterns: Universes, Views
- Category-theoretic abstractions as typed interfaces
- Other dependently-typed languages, e.g., Coq and Idris.

Learning Objectives

Precondition

Students are expected to have achieved the following learning objectives **before** taking this course:

1. Students should know and understand
   a) Propositional logic and predicate logic
   b) Principles of typed expressions and statically typed programming languages
   c) Basic concepts and theorems about sets, functions and relations
   d) Standard kinds of algebras
   e) Basic datastructures and algorithms
   f) Basics of functional programming
2. Students should be able to
   a) Translate moderate complex mathematical prose into predicate-logic definitions and formulae
   b) Construct derivations in some proof system for predicate logic
   c) Routinely use structural induction for proofs where appropriate
   d) Quickly acquire a new programming paradigm

Postcondition

Students are expected to achieve the following learning objectives at the end of this course:

1. Students should know and understand
   a) The difference in expressiveness dependent types bring to logic
   b) The difference in expressiveness dependent types bring to programming languages
   c) The Curry-Howard correspondence
   d) The syntax and tpying principles of the Agda2 programming language
   e) The reduction semantics of the Agda2 programming language
   f) Commonly used programming patterns in dependently-typed languages, including universes, views
   g) An overview of dependently-typed languages currently available
2. Students should be able to
   a) Design and implement dependently-typed data structures
   b) Express specifications as types in a dependently-typed language
   c) Implement functions that "prove their own correctness"
   d) Design module interfaces that guarantee correct implementations
   e) Fluently use the Agda2 programming language to formalise specifications and produce certified implementations.

Course Page:

```
http://www.cas.mcmaster.ca/~kahl/DepTyp/2021/
```

This and the Avenue course page are where you will find further information, announcements, and useful links. It is the student's responsibility to be aware of the information on the course web page and Avenue site, and to check regularly for announcements.

Grading:

Assignments: In the first part of the course, there will be weekly **Assignments** to support the learning of the Agda programming language. Solutions will need to be submitted electronically.

Paper Presentations and Projects: In the later part of the course, you will be assigned topics for presentation that will start with seminar-style paper presentations, and may also involve exploring other languages and systems, or completing a larger, individual programming assignment. Evaluation will be based both on the project work (to be submitted electronically) including documentation quality, and on the presentation; details TBA.

Grade Calculation: All exam grades will be percentage grades.

For every student, the course grade is calculated as a weighted average:
- All **Assignments**: 50%
- **Paper Presentations or Projects**: 10% + 15% + 25%

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

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

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.**
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.

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.