COMP 4161: Advanced Topics in Software Verification

Data61 Advanced Course, Session 2/2018

- Home
- Course Outline
- Lectures
- Assignments
- Exam
- Reading
- Forum

Course Outline

Staff

Lecturer (LiC): Gerwin Klein
Email: gerwin.klein at data61.csiro.au
Phone: +61 2 9490 5878
Office: Level 3, Building K17
Consultations: by appointment

Lecturer: June Andronick
Email: june.andronick at data61.csiro.au
Phone: +61 2 8306 0581
Office: Level 3, Building K17
Consultations: by appointment

Lecturer: Christine Rizkallah
Email: c.rizkallah at unsw.edu.au
Office: Level 3, Building K17
Consultations: by appointment

Lecturer: Miki Tanaka
Email: miki.tanaka at data61.csiro.au
Office: Level 3, Building K17
Consultations: by appointment

Course Goal

To educate students in advanced topics in software verification. Topics include higher order logic, natural deduction, lambda calculus, term rewriting, data types and recursive functions, induction principles, calculational reasoning, mathematical proofs, decision procedures for a variety of logical domains, and proofs about programs.

Learning Outcomes

At the end of the course, successful students will be able to

- write definitions in the theorem prover Isabelle/HOL
- formalise software verification problems
- prove theorems in an interactive proof assistant
- effectively use proof automation and automatic counter-example finding
- formally verify functional programs
- formally verify imperative programs, including small C programs

Parallel Teaching

advanced UG + PG

Course Prerequisites

48 Units of Credit. In addition, experience with (first-order) logic or functional programming is required. The course is intended for 4th year or post graduate students. Second and third year students can participate with permission of the lecturer.

Course Exclusions

None

Constituents

- Lecture: the lecture will cover the following main topics: higher order logic, natural deduction, lambda calculus, term rewriting, data types and recursive functions, induction principles, mathematical proofs, and proofs about programs.
- Tutorials: there are no tutorials for this lecture
- Assignments: there will be three assignments. Penalty for late submission of assignments will be 4% (of the worth of the assignment) subtracted from the raw mark per day of being late. In other words, earned marks will be lost. For example, assume an assignment worth 25 marks is marked as 20, but had been submitted two days late. The late penalty will be 2 marks, resulting in a mark of 18 being awarded. No assignments will be accepted later than one week after the deadline.

Preliminary Course Schedule

Week	Topic
1	Introduction and Admin, Lambda Calculus
2	Typed Lambda Calculus, Proofs in Isabelle, Natural Deduction
3	HOL
4	Term Rewriting
5	Induction
6	Recursive Datatypes and Primitive Recursion
7	General Recursion
8	Hoare Logic
9	C verification
10	Writing Automated Proof Methods
11	Isar: Structured Proofs
12	Typeclasses and Locales

Course philosophy and teaching strategies

The learning focus in this course is primarily on lectures and assignments. The first two assignments are intended to give early feedback and to test your preparedness for the final exam. While marks are assigned to the assignments, their primary purpose is to give you concrete tasks with deadlines to help you structure your learning.

Assessment

- Assignments: There will be three written assignments. Assignment 1 will be due in week 3, assignment 2 in week 8, and assignment 3 in week 11.
- Exam: The final exam will be a take-home exam with Isabelle/HOL proofs and questions on the lecture material.
- Supplementary Exam: If you cannot attend the Final Exam because of illness or misadventure, you must submit a Special Consideration request, with documentation, through MyUNSW within 48 hours of the exam. If your request is reasonable, then you will be awarded a Supplementary Exam.
- Final Mark: the class mark consists of the assignments (each 1/3). The arithmetic mean of the class mark and exam mark is used to determine the final mark. To pass the course, a minimum of 40% is necessary in each component. If both the class mark and the exam mark are greater or equal to 40%, the final mark will be `(class mark + exam mark) / 2` otherwise `minimum ((class mark + exam mark) / 2, 44)`

Text and Reference Books

See the page on reading material. The main textbook is Concrete Semantics, also available online.

Continual course improvement

Feedback from the last evaluation of this course was positive and we intend to maintain the same style and content. One issue raised by students was the lack of textbook. This is now available.

Student Conduct

The **Student Code of Conduct** (Information, Policy) sets out what the University expects from students as members of the UNSW community. As well as the learning, teaching and research environment, the University aims to provide an environment that enables students to achieve their full potential and to provide an experience consistent with the University's values and guiding principles. A condition of enrolment is that students *inform themselves* of the University's rules and policies affecting them, and conduct themselves accordingly.

In particular, students have the responsibility to observe standards of equity and respect in dealing with every member of the University community. This applies to all activities on UNSW premises and all external activities related to study and research. This includes behaviour in person as well as behaviour on social media, for example Facebook groups set up for the purpose of discussing UNSW courses or course work. Behaviour that is considered in breach of the Student Code Policy as discriminatory, sexually inappropriate, bullying, harassing, invading another's privacy or causing any person to fear for their personal safety is serious misconduct and can lead to severe penalties, including suspension or exclusion from UNSW.

If you have any concerns, you may raise them with your lecturer, or approach the School Ethics Officer, Grievance Officer, or one of the student representatives.

Plagiarism

Plagiarism is defined as using the words or ideas of others and presenting them as your own. UNSW and CSE treat plagiarism as academic misconduct, which means that it carries penalties as severe as being excluded from further study at UNSW. There are several on-line sources to help you understand what plagiarism is and how it is dealt with at UNSW:

- Plagiarism and Academic Integrity
- UNSW Plagiarism Procedure

Make sure that you read and understand these. Ignorance is not accepted as an excuse for plagiarism. In particular, you are also responsible that your assignment files are not accessible by anyone but you by setting the correct permissions in your CSE directory and code repository, if using. Note also that plagiarism includes paying or asking another person to do a piece of work for you and then submitting it as your own work.

UNSW has an ongoing commitment to fostering a culture of learning informed by academic integrity. All UNSW staff and students have a responsibility to adhere to this principle of academic integrity. Plagiarism undermines academic integrity and is not tolerated at UNSW. Plagiarism at UNSW is defined as using the words or ideas of others and passing them off as your own.

If you haven't done so yet, please take the time to read the full text of

- UNSW's policy regarding academic honesty and plagiarism

The pages below describe the policies and procedures in more detail:

- Student Code Policy
- Student Misconduct Procedure
- Plagiarism Policy Statement
- Plagiarism Procedure

You should also read the following page which describes your rights and responsibilities in the CSE context:

- Essential Advice for CSE Students

Further information

- Students enrolled in this course are expected to attend all classes.
- The use of School of Computer Science and Engineering computing laboratories is subject to rules described in the Yellow Form, which you acknowledge (electronic) receipt of when you receive your computing account. The Yellow Form also outlines what to do in case illness or misadventure that affects your assessment, and supplementary examinations procedures within the School of Computer Science and Engineering.
- UNSW Occupational Health and Safety policies and responsibilities.