UNSW Course Outline

COMP4161 Advanced Topics in Software Verification - 2024

Published on the 25 Aug 2024

General Course Information

Course Code : COMP4161
Year : 2024
Term : Term 3
Teaching Period : T3
Is a multi-term course? : No
Faculty : Faculty of Engineering
Academic Unit : School of Computer Science and Engineering
Delivery Mode : Multimodal
Delivery Format : Standard
Delivery Location : Kensington
Campus : Sydney
Study Level : Postgraduate, Undergraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

This course is about mechanical proof assistants, how they work, and what they can be used for. It presents specification and proof techniques used in industrial grade theorem provers, teaches the theoretical background to the techniques involved, and shows how to use a theorem prover

to conduct formal proofs in practice. The courses is intended to bring third/fourth year and postgraduate students into contact with the current research topics in the field of theorem proving and automated deduction and to teach them the necessary skills to successfully use industrial grade verification environments in modelling and verification.

Topics covered included: 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.

Note: experience with (first-order) logic and functional programming is required.

Course Aims

This course teaches you how to do mechanical, machine-assisted proofs---the gold standard of validation for software and mathematics. This provides exposure to an ironclad, principled way of developing safety-critical systems while knowing that you got it right. Students who have taken this course will be well equipped to work in proof engineering, or to undertake research in formal verification.

Course Learning Outcomes

Course Learning Outcomes
CLO1 : Write definitions in the theorem prover Isabelle/HOL
CLO2 : Formalise software verification problems
CLO3 : Prove theorems in an interactive proof assistant
CLO4 : Effectively use proof automation and automatic counter-example finding
CLO5 : Formally verify functional programs
CLO6 : Formally verify imperative programs, including small C programs

Course Learning Outcomes	Assessment Item
CLO1 : Write definitions in the theorem prover Isabelle/HOL	• Final exam • Assignments 1, 2 and 3
CLO2 : Formalise software verification problems	• Final exam • Assignments 1, 2 and 3
CLO3 : Prove theorems in an interactive proof assistant	• Final exam • Assignments 1, 2 and 3
CLO4 : Effectively use proof automation and automatic counter-example finding	• Final exam • Assignments 1, 2 and 3
CLO5 : Formally verify functional programs	• Final exam • Assignments 1, 2 and 3
CLO6 : Formally verify imperative programs, including small C programs	• Final exam • Assignments 1, 2 and 3

Learning and Teaching Technologies

Moodle - Learning Management System | EdStem | Echo 360 | Zoom | CSE Systems

Other Professional Outcomes

https://www.unsw.edu.au/engineering/student-life/student-resources/program-design

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
Final exam Assessment Format: Individual	50%	
Assignments 1, 2 and 3 Assessment Format: Individual	50%	

Assessment Details

Final exam

Assessment Overview

The individual take-home exam is done over approx. one day. Students will submit an Isabelle/HOL development that will be marked against assessment criteria.

Course Learning Outcomes

- CLO1 : Write definitions in the theorem prover Isabelle/HOL
- CLO2 : Formalise software verification problems
- CLO3 : Prove theorems in an interactive proof assistant
- CLO4 : Effectively use proof automation and automatic counter-example finding
- CLO5 : Formally verify functional programs
- CLO6 : Formally verify imperative programs, including small C programs

Assignment submission Turnitin type

This is not a Turnitin assignment

Generative AI Permission Level

No Assistance

This assessment is designed for you to complete without the use of any generative AI. You are not permitted to use any generative AI tools, software or service to search for or generate information or answers.
For more information on Generative AI and permitted use please see here.

Assignments 1, 2 and 3

Assessment Overview

Students will submit three individual written assignments. Submissions will consist of a small to medium scale Isabelle/HOL theory files and/or pdf files depending on the specific task, each solving a specified formal proof problem. Submissions will be marked against assessment criteria, and written feedback will be available online.

Course Learning Outcomes

- CLO1 : Write definitions in the theorem prover Isabelle/HOL
- CLO2 : Formalise software verification problems
- CLO3 : Prove theorems in an interactive proof assistant
- CLO4 : Effectively use proof automation and automatic counter-example finding
- CLO5 : Formally verify functional programs
- CLO6 : Formally verify imperative programs, including small C programs

Generative AI Permission Level

No Assistance

This assessment is designed for you to complete without the use of any generative AI. You are not permitted to use any generative AI tools, software or service to search for or generate information or answers.
For more information on Generative AI and permitted use please see here.

General Assessment Information

Grading Basis

Standard

Requirements to pass course

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.

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 0 : 2 September - 8 September	Other	Nothing
Week 1 : 9 September - 15 September	Lecture	Introduction, Lambda Calculus
Week 2 : 16 September - 22 September	Lecture	Proofs in Isabelle, Natural Deduction, HOL
Week 3 : 23 September - 29 September	Lecture	Term Rewriting
Week 4 : 30 September - 6 October	Lecture	Advanced Term Rewriting, Induction
Week 5 : 7 October - 13 October	Lecture	Recursive Datatypes and Primitive Recursion
Week 6 : 14 October - 20 October	Other	Flexibility week
Week 7 : 21 October - 27 October	Lecture	General Recursion
Week 8 : 28 October - 3 November	Lecture	Hoare Logic
Week 9 : 4 November - 10 November	Lecture	Weakest Preconditions, C Verification
Week 10 : 11 November - 17 November	Lecture	C Verification, Exam Prep

Attendance Requirements

Students are strongly encouraged to attend all classes and review lecture recordings.

General Schedule Information

The schedule is tentative and may evolve as the course proceeds.

Further information is on the course website at CSE https://www.cse.unsw.edu.au/~cs3161 .

Course Resources

Recommended Resources

See course website for a list of recommended reading.

Course Evaluation and Development

The course is evaluated every year using the myExperience system. Feedback on the course has been positive.

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
	Miki Tanaka					Yes	No
	COURSE EMAIL					No	Yes
	Thomas Sewell					No	No
	Robert Sison					No	No

Other Useful Information

Academic Information

I. Special consideration and supplementary assessment

If you have experienced an illness or misadventure beyond your control that will interfere with your assessment performance, you are eligible to apply for Special Consideration prior to, or within 3 working days of, submitting an assessment or sitting an exam.

Please note that UNSW has a Fit to Sit rule, which means that if you sit an exam, you are declaring yourself fit enough to do so and cannot later apply for Special Consideration.

For details of applying for Special Consideration and conditions for the award of supplementary assessment, please see the information on UNSW's Special Consideration page.

II. Administrative matters and links

All students are expected to read and be familiar with UNSW guidelines and polices. In particular, students should be familiar with the following:

- Attendance
- UNSW Email Address
- Special Consideration
- Exams
- Approved Calculators
- Academic Honesty and Plagiarism
- Equitable Learning Services

III. Equity and diversity

Those students who have a disability that requires some adjustment in their teaching or learning environment are encouraged to discuss their study needs with the course convener prior to, or at the commencement of, their course, or with the Equity Officer (Disability) in the Equitable Learning Services. Issues to be discussed may include access to materials, signers or note-takers, the provision of services and additional exam and assessment arrangements. Early notification is essential to enable any necessary adjustments to be made.

IV. Professional Outcomes and Program Design

Students are able to review the relevant professional outcomes and program designs for their streams by going to the following link: https://www.unsw.edu.au/engineering/student-life/student-resources/program-design.

Note: This course outline sets out the description of classes at the date the Course Outline is published. The nature of classes may change during the Term after the Course Outline is published. Moodle or your primary learning management system (LMS) should be consulted for the up-to-date class descriptions. If there is any inconsistency in the description of activities between the University timetable and the Course Outline/Moodle/LMS, the description in the Course Outline/Moodle/LMS applies.

Academic Honesty and Plagarism

UNSW has an ongoing commitment to fostering a culture of learning informed by academic integrity. All UNSW 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.*

Plagiarism is a type of intellectual theft. It can take many forms, from deliberate cheating to accidentally copying from a source without acknowledgement. UNSW has produced a website

with a wealth of resources to support students to understand and avoid plagiarism, visit: student.unsw.edu.au/plagiarism. The Learning Centre assists students with understanding academic integrity and how not to plagiarise. They also hold workshops and can help students one-on-one.

You are also reminded that careful time management is an important part of study and one of the identified causes of plagiarism is poor time management. Students should allow sufficient time for research, drafting and the proper referencing of sources in preparing all assessment tasks.

Repeated plagiarism (even in first year), plagiarism after first year, or serious instances, may also be investigated under the Student Misconduct Procedures. The penalties under the procedures can include a reduction in marks, failing a course or for the most serious matters (like plagiarism in an honours thesis or contract cheating) even suspension from the university. The Student Misconduct Procedures are available here:

www.gs.unsw.edu.au/policy/documents/studentmisconductprocedures.pdf

Submission of Assessment Tasks

Work submitted late without an approved extension by the course coordinator or delegated authority is subject to a late penalty of five percent (5%) of the maximum mark possible for that assessment item, per calendar day.

The late penalty is applied per calendar day (including weekends and public holidays) that the assessment is overdue. There is no pro-rata of the late penalty for submissions made part way through a day. This is for all assessments where a penalty applies.

Work submitted after five days (120 hours) will not be accepted and a mark of zero will be awarded for that assessment item.

For some assessment items, a late penalty may not be appropriate. These will be clearly indicated in the course outline, and such assessments will receive a mark of zero if not completed by the specified date. Examples include:

- Weekly online tests or laboratory work worth a small proportion of the subject mark;
- Exams, peer feedback and team evaluation surveys;
- Online quizzes where answers are released to students on completion;
- Professional assessment tasks, where the intention is to create an authentic assessment that

has an absolute submission date; and,
- Pass/Fail assessment tasks.

Faculty-specific Information

Engineering Student Support Services – The Nucleus - enrolment, progression checks, clash requests, course issues or program-related queries

Engineering Industrial Training – Industrial training questions

UNSW Study Abroad – study abroad student enquiries (for inbound students)

UNSW Exchange – student exchange enquiries (for inbound students)

UNSW Future Students – potential student enquiries e.g. admissions, fees, programs, credit transfer

Phone

(+61 2) 9385 8500 – Nucleus Student Hub

(+61 2) 9385 7661 – Engineering Industrial Training

(+61 2) 9385 3179 – UNSW Study Abroad and UNSW Exchange (for inbound students)

School Contact Information

CSE Help! - on the Ground Floor of K17

- For assistance with coursework assessments.

The Nucleus Student Hub - https://nucleus.unsw.edu.au/en/contact-us

- Course enrolment queries.

Grievance Officer - grievance-officer@cse.unsw.edu.au

- If the course convenor gives an inadequate response to a query or when the courses convenor does not respond to a query about assessment.

Student Reps - stureps@cse.unsw.edu.au

- If some aspect of a course needs urgent improvement. (e.g. Nobody responding to forum

queries, cannot understand the lecturer)

You should **never** contact any of the following people directly:

- Vice Chancellor

- Pro-vice Chancellor Education (PVCE)

- Head of School

- CSE administrative staff

- CSE teaching support staff

They will simply bounce the email to one of the above, thereby creating an unnecessary level of indirection and a delay in the response.