COMP4011/8011
Advanced Topics in
Formal Methods and Programming Languages

– Software Verification with Isabelle/HOL –

Peter Höfner

July 24, 2024

Section 0

Admin

Lecturer

- **A/Prof. Peter Höfner**
  CSIT, Room N234 (Building 108)
  Peter.Hoefner@anu.edu.au
  +61 2 6125 0159

  Consultation
  after the lecture, or by appointment

Lectures

- Tuesday 10:00-11:30, Rm G51 Haydon-Allen Bldg
  Wednesday 9:00-10:30, Rm G52 Haydon-Allen Bldg
- Q/A session in Week 12 or 13

- **Etiquette**
  - tailored for in-person attendance
  - engage
  - feel free to ask questions
  - we reject behaviour that strays into harassment, no matter how mild

DropIns

- not mandatory
- Thursday 11:00-13:30, Rm G51 Haydon-Allen Bldg
- from Week 2 onwards

- **Summary**
  - your chance to discuss problems
  - discuss home work
  - discuss exercises from lectures
  - **no structured activity**
    (nothing will happen without your input)
  - except: oral discussion of your assignments

Plan/Schedule I

Resources

web: `https://cs.anu.edu.au/courses/comp4011-itp/`
wattle: `https://wattlecourses.anu.edu.au/course/view.php?id=44081`
edstem: `https://edstem.org/`
(you will be registered at the end of the week)

Workload

The average student workload is 130 hours for a six unit course.
That is roughly **11 hours/week**.
`https://policies.anu.edu.au/ppl/document/ANUP_000691`

Plan/Schedule II

Assessment criteria

- Quizz: 0% (for feedback only)
- Assignments: 45%, 3 assignments
- Take-home exam: 55% (55 marks) **[hurdle]**
- **hurdle:** minimum of 35% in the final exam

Assessments (tentative)

No	Hand Out	Hand In	Marks
0	23/07	26/07	0
1		16/08	15
2		04/10	15
3		12/10	15
4		tbc	55

About the Course I

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 interactive theorem provers (Isabelle/HOL), teaches the theoretical background to the techniques involved, and shows how to use a theorem prover to conduct formal proofs in practice.

About the Course II

Topics (tentative)

The following schedule is tentative and likely to change.

	Topic
0	Admin
1	Introduction
2	Lambda Calculus
3	Proofs in Isabelle, Natural Deduction, HOL
4	Term Rewriting
5	Induction
6	Recursive Datatypes and Primitive Recursion
7	General Recursion
8	Hoare Logic
9	Weakest Preconditions
10	Advanced Topics in Software Verification
11	Guest lectures and Exam Preparation

About the Course IV

Disclaimer

This is first time I offer this course.

The material in these notes has been drawn from several different sources, including the books and similar courses at some other universities. In particular, it is based on a course offered by UNSW and Proofcraft.

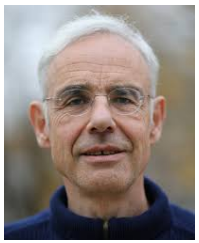
As it is a newly designed course, changes in timetabling are quite likely.

Feedback (oral, email, survey, . . .) is highly appreciated.

Credits



Gerwin Klein, June Andronick, Johannes Åman Pohjola



Tobias Nipkow, Larry Paulson, Makarius Wenzel


David Basin, Burkhardt Wolff

Academic Integrity

- never misrepresent the work of others as your own
- if you take ideas from elsewhere (including tools) you must say so with utmost clarity

Generative AI

- introduction of fundamental concepts
- use of any Generative AI tools is not permitted

Reading Material

- Tobias Nipkow and Gerwin Klein: Concrete Semantics
  `http://www.concrete-semantics.org`

Further Reading

- Tobias Nipkow, Lawrence C. Paulson, Markus Wenzel: Isabelle/HOL – A Proof Assistant for Higher-Order Logic
- Apostolos Doxiadis, Christos H. Papadimitriou, Alecos Papadatos, Annie Di Donna. Logicomix: An Epic Search for Truth
- Hendrik Pieter Barendregt. The Lambda Calculus, its Syntax and Semantics
- Alonzo Church. A formulation of the simple theory of types
- Michael J. C. Gordon and Tom F. Melham (eds), Introduction to HOL. Cambridge University Press
- Franz Baader and Tobias Nipkow. Term Rewriting and All That
- ...

Software

- Isabelle (Australian download mirror)
  `https://proofcraft.systems/isabelle/index.html`
- Isabelle theory library
  `https://isabelle.in.tum.de/library/`
- The Archive of Formal Proofs
  `https://www.isa-afp.org`

Exercise 1

Install Isabelle
Feel free to bring your laptop into lectures and dropins.