Isabelle/HOL Tutorial

Lectures at Universitetet i Oslo 2019

Jonathan Julian Huerta y Munive and Georg Struth

University of Sheffield

What is Isabelle/HOL?

Isabelle is

- a generic proof assistant
  - a formal specification language for mathematical theories
  - an interactive theorem prover based on a logical calculus
- developed mainly at Cambridge and München
- about 25 years old
- used by computer scientists and mathematicans world wide

Isabelle is

- a joy because it sometimes makes proving things easy
- a pain because it sometimes makes proving things hard

What is Isabelle/HOL?

specific characteristics

- Isabelle is an LCF-style theorem prover
- written in the functional programming language ML
- it has a small logical core and is therefore trustworthy
- it has stood the test of time
- users own the means of production
- Isabelle assists users in formalising proofs
- but aims at high level of proof automation

What is Isabelle/HOL?

HOL

- Isabelle offers different logics for theorem proving
- Isabelle/HOL is the most popular one
- it is based on classical typed higher-order logic
- it supports reasoning with sets, inductive sets, recursive functions,...

almost every formula you can write
you can write in Isabelle

What is Isabelle/HOL?

. . . almost every one:

- partially defined objects can be difficult to formalise
  - partial functions, matrices, categories . . .
- objects that are not recursively defined as well
  - graphs, automata, networks, . . .

What is Isabelle/HOL?

workflow

- three user interfaces
  - Isabelle jEdit (standard)
  - Proof General (outdated)
  - Visual Studio Code (in preparation)
- four modes of proof
  - interactive with natural deduction rules
  - automated with built-in provers, simplifiers, tactics
  - automated with external first-order theorem provers: sledgehammer
  - interactive with proof-scripting language Isar
- counterexample generators: nitpick/quickcheck
- type classes/locales allow building mathematical hierarchies
- large libraries of mathematical components have been implemented
- excellent documentation helps users

What is Isabelle/HOL?

users

- main applications in program verification/correctness
- increasing interest by mathematicians

alternatives

- Coq offers some advantages for programming mathematics
- Agda is popular with type theorists
- Mizar provides large mathematical libraries
- HOL is quite similar to Isabelle
- LEAN aims at combining lessons learned from Coq and Isabelle

Lecture Plan

- Monday
  - overview of Isabelle and jEdit
  - proofs from natural deduction to proof automation
  - definitions and abbreviations
- Tuesday
  - structured readable proofs with Isar
  - types, data types, recursive functions, proofs by induction
- Wednesday
  - theory engineering with type classes and locales
  - building verification components from algebraic principles
- Thursday
  - formalising Hoare logic
  - formalising predicate transformer semantics
- Friday
  - formalising structural operational semantics
  - an Isabelle component for hybrid systems verification

Exercise Plan

- there will be many basic tasks/exercises in class
- we have prepared a number of harder exercises for the afternoons
- we will distribute exercise sheets for them