Formal Logic and Deduction Systems

Software Formal Verification

Maria João Frade

Departmento de Informática
Universidade do Minho

2009/2010

What is a (formal) logic?

Logic is defined as the study of the principles of reasoning. One of its branches is symbolic logic, that studies formal logic.

- A formal logic is a language equipped with rules for deducing the truth of one sentence from that of another.
- A logic consists of
  - A *logical language* in which (well-formed) sentences are expressed.
  - A *semantics* that defines the intended interpretation of the symbols and expressions of the logical language.
  - A *proof system* that is a framework of rules for deriving valid judgments.
- Examples: propositional logic, first-order logic, higher-order logic, modal logic, ...

What is a logical language?

A logical language consists of

- *logical symbols* whose interpretations are fixed
- *non-logical symbols* whose interpretations vary

These symbols are combined together to form *well-formed formulas*.

Logic and computer science

- Logic and computer science share a symbiotic relationship
  - Logic provides language and methods for the study of theoretical computer science.
  - Computers provide a concrete setting for the implementation of logic.
- Formal logic makes it possible to calculate consequences at the symbolic level, so computers can be used to automate such symbolic calculations.
- Moreover, logic can be used to model the situations we encounter as computer science professionals, in such a way that we can reason about them formally.

Two branches of formal logic: *classical* and *intuitionistic*

- The classical understanding of logic is based on the notion of *truth*. The truth of a statement is "absolute" and independent of any reasoning, understanding, or action.
  - Statements are either true or false. ("false" $\leftrightsquigarrow$ "not true")
  - *tertium non datur* principle
    "$A \vee \neg A$" must hold no matter what the meaning of A is.
  - Accepts proof by contradiction.

- Intuitionistic logic is a branch of formal logic that rejects this guiding principle.
  - A statement A is "true" if we can prove it, or is "false" if we can show that if we have a proof of A we get a contradiction.
  - One judgement about a statement are based on the existence of a proof or "construction" of that statement.
  - To show "$A \vee \neg A$" one have to show A or $\neg A$. If neither of these can be shown, then the putative truth of the disjunction has no justification.

Classical logic *versus* intuitionistic logic

- Much of standard mathematics can be done within the framework of intuitionistic logic, but the task is very difficult, so mathematicians use methods of classical logic (as proofs by contradiction).

- However the philosophy behind intuitionistic logic is appealing for a computer scientist. For an intuitionist, a mathematical object (such as the solution of an equation) does not exist unless a finite construction (algorithm) can be given for that object.

Course overview

- Classical Propositional Logic
- Classical First-Order Logic
- Higher-Order Logic
- λ-Calculus
- Intuitionism and the Curry-Howard Isomorphism
- Calculus of Inductive Constructions

- The Coq proof-assistant

Bibliography


Michael Huth & Mark Ryan
Logic in Computer Science: Modelling and Reasoning About Systems
Cambridge University Press; 2nd edition (2004).


A First Course in Logic: An Introduction to Model Theory, Proof Theory, Computability, and Complexity
Shawn Hedman
Oxford (2004)


Aaron R. Bradley & Zohar Manna
The Calculus of Computation: Decision Procedures with Applications to Verification
Springer (2007)

Bibliography

Morten Heine Sørensen & Pawel Urzyczyn
Lectures on the Curry-Howard Isomorphism
Studies in Logic and the Foundations of Mathematics, 149. Elsevier (2004)

http://2020ok.com/books/35/lectures-on-the-curry-howard-isomorphism-37235.htm

Yves Bertot & Pierre Castéran
Interactive Theorem Proving and Program Development Coq'Art: The Calculus of Inductive Constructions
Springer (2004)

The Coq proof assistant
The latest version: Coq 8.2
http://coq.inria.fr/