logical verification lecture 1
2011 03 29
first-order propositional logic

who

Femke van Raamsdonk

T446

femke at cs.vu.nl

what

- 12 lectures: theory
  Tuesdays 13.30–15.15 in F637
  Fridays 13.30–15.15 in F654

- 12 practical works: Coq and exercises
  Thursdays 09.00–10.45 in P323
  Fridays 09.00–10.45 in P323
  (I arrive later)

- final test

material

- course notes via the webpage

- slides via the webpage

- exercises and old exams via the webpage

- Coq exercises via prover.cs.ru.nl

topic

computer science

formal methods

proof assistants

type theory and Coq

proof assistants or interactive theorem provers

a computer program (the proof checker) verifies a theory

proof assistant = proof checker + user interaction

proof assistants

- Coq
- PVS
- ACL2
- HOL/Isabelle
- Mizar

Coq

a functional programming language and a reasoning framework based on higher order logic to perform proofs on the programs

Standard ML

defined by Robin Milner (1934–2010), Tofte, Harper
first real language with a mathematical semantics

big achievements in interactive theorem proving

- four colour theorem
  Georges Gonthier
- verified C-compiler
  Xavier Leroy
- operating system microkernel
  Gerwin Klein

this course

- Curry-Howard-De Bruijn isomorphism
  logic $\leftrightarrow$ λ-calculus
- proof checker Coq

first-order propositional logic

a sequence of (strict) inclusions:

$$\begin{array}{c}\text{minimal logic (ML)}\\ \subset \\ \text{minimal logic plus } \bot \\ \subset \\ \text{full intuitionistic logic (IL)} \\ \subset \\ \text{classical logic (CL)}\end{array}$$

minimal logic (ML)

only $\rightarrow$

minimal logic: formulas

a propositional variable:
a

implication:
$(A \rightarrow B)$

natural deduction: two kinds of logical rules

- introduction rules
- elimination rules

minimal logic: implication

implication introduction rule

$$\frac{B}{A \rightarrow B}\ I[x] \rightarrow$$

implication elimination rule

$$\frac{A \rightarrow B \qquad A}{B}\ E \rightarrow$$

minimal logic: assumption

assumption rule

$$A$$

tautologies

(not only for ML)

A is a tautology
if there is a proof of A without open assumptions
(all assumptions are cancelled)

minimal logic: examples of tautologies

- $A \to A$
- $A \to B \to A$
- $((A \to B) \to (C \to D)) \to C \to B \to D$
- permutation
  $(A \to B \to C) \to (B \to A \to C)$
- weak law of Peirce
  $(((((A \to B) \to A) \to A) \to B) \to B)$

minimal logic plus falsum

ML + $\bot$

$\bot$ is a connective without arguments

what are the rules for $\bot$?

ML plus falsum: falsum elimination rule

$$\frac{\bot}{A}\ E\bot$$

ML plus falsum: negation

negation is defined: $\neg A := A \to \bot$

ML plus falsum: examples of tautologies

- contraposive
  $(A \to B) \to (\neg B \to \neg A)$
- many negations
  $\neg\neg(\neg\neg A \to A)$

intuitionistic logic (IL)

$\mathrm{ML} + \bot + \top + \wedge + \vee$

every connective comes with its natural deduction rules

intuitionistic logic: introduction rule for true

$$\top$$

intuitionistic logic: rules for conjunction

conjunction introduction rule

$$\frac{A \qquad B}{A \wedge B}\ I\wedge$$

conjunction elimination rules

$$\frac{A \wedge B}{A}\ E\wedge \qquad \frac{A \wedge B}{B}\ E\wedge$$

intuitionistic logic: rules for disjunction

disjunction introduction rules

$$\frac{A}{A \vee B}\ I\vee \qquad \frac{B}{A \vee B}\ I\vee$$

disjunction elimination rule

$$\frac{A \vee B \qquad A \rightarrow C \qquad B \rightarrow C}{C}$$

intuitionistic logic: examples of tautologies

- $A \vee B \rightarrow B \vee A$
- $A \wedge B \rightarrow B \wedge A$

classical logic

start with intuitionistic logic

add a classical axiom
(more later)

further reading

- intuitionism
- ten questions about intuitionism
- interactive theorem proving

overview: propositional logic

- minimal logic (ML)
  $(((((A \to B) \to A) \to A) \to B) \to B)$
- ML + $\bot$
  $(A \to B) \to (\neg B \to \neg A)$
- intuitionistic logic
  $A \vee B \to (A \to C) \to (B \to C) \to C$
- classical logic
  $A \vee \neg A$