

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

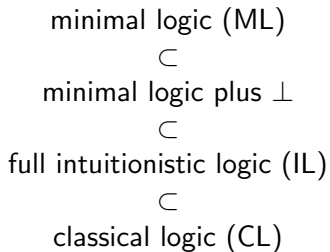
- four colour theorem
Georges Gonthier
- verified C-compiler
Xavier Leroy
- operating system microkernel
Gerwin Klein

this course

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

first-order propositional logic

a sequence of (strict) inclusions:



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

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

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

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

minimal logic plus falsum

ML + \perp

\perp is a connective without arguments

what are the rules for \perp ?

ML plus falsum: falsum elimination rule

$$\frac{\perp}{A} E_{\perp}$$

ML plus falsum: negation

negation is defined: $\neg A := A \rightarrow \perp$

ML plus falsum: examples of tautologies

- contrapositive

$$(A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A)$$

- many negations

$$\neg\neg(\neg\neg A \rightarrow A)$$

intuitionistic logic (IL)

ML + \perp + \top + \wedge + \vee

every connective comes with its natural deduction rules

intuitionistic logic: introduction rule for true

T

intuitionistic logic: rules for conjunction

conjunction introduction rule

$$\frac{A \quad B}{A \wedge B} I_{\wedge}$$

conjunction elimination rules

$$\frac{A \wedge B}{A} E_{\wedge} \quad \frac{A \wedge B}{B} E_{\wedge}$$

intuitionistic logic: rules for disjunction

disjunction introduction rules

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

disjunction elimination rule

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

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)

overview: propositional logic

- minimal logic (ML)

$$((((A \rightarrow B) \rightarrow A) \rightarrow A) \rightarrow B) \rightarrow B$$

- ML + \perp

$$(A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A)$$

- intuitionistic logic

$$A \vee B \rightarrow (A \rightarrow C) \rightarrow (B \rightarrow C) \rightarrow C$$

- classical logic

$$A \vee \neg A$$

further reading

- intuitionism
- ten questions about intuitionism
- interactive theorem proving