overview

practicalities

introduction

minimal prop1

minimal logic plus falsum

full intuitionistic propositional logic

further reading

who

Jasmin Christian Blanchette (T437)
Femke van Raamsdonk (T446)

j.c.blanchette at vu.nl
f.van.raamsdonk at vu.nl

what

• 12 lectures: theory
  Mondays 13:30–15:15 in S655 (weeks 14, 15, 17–21)
  Thursdays 13:30–15:15 in S655 (weeks 14, 16, 19–21)

• 12 practical works: Coq and exercises
  Tuesdays 15:30–17:15 in P337 (weeks 14–21)
  Fridays 11:00–12:45 in P337 (weeks 14, 16, 19, 20)
tests

- 5 practical works Coq
  grade: pass or fail

- written exam
  Thursday 1 June 2017, 15:15–18:00 in M143

material

- course notes via the webpage
- slides via the webpage
- exercises and some 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

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

Coq

to perform proofs on the programs

a functional programming language
and a reasoning framework based on higher-order logic

Standard ML

defined by Robin Milner (1934–2010), Tofte, Harper

first real language with a mathematical semantics

big achievements in interactive theorem proving

- **four color theorem** (in Coq)
  Georges Gonthier et al.

- **verified C compiler** (in Coq)
  Xavier Leroy et al.

- **operating system microkernel** (in Isabelle/HOL)
  Gerwin Klein et al.

- **Kepler conjecture** (in HOL Light and Isabelle/HOL)
  Thomas Hales et al.
this course

- Curry–Howard–De Bruijn isomorphism
  logic ↔ \( \lambda \)-calculus
- Coq proof checker

first-order propositional logic (prop1)

a sequence of (strict) inclusions:

- minimal logic (ML)
- minimal logic plus \( \perp \)
- full intuitionistic logic (IL)
- classical logic (CL)

minimal logic (ML)

minmal logic: formulas

only \( \rightarrow \)

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

implication elimination rule
\[ \frac{A \rightarrow B \quad A}{B} \ \text{E} \rightarrow \]

minimal logic: assumption

assumption rule
\[ A \]

tautologies (general, not only minimal logic)

A is a tautology
if there is a proof of A without open assumptions
(all assumptions are canceled)
minimal prop1: 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
  \( (((((A \rightarrow B) \rightarrow A) \rightarrow A) \rightarrow B) \rightarrow B) \)

apply and implication elimination

\[ \frac{A \rightarrow B}{B} \quad \frac{A}{E} \]

goal: \( B \)
assumption: \( x : A \rightarrow B \)
tactic: apply \( x \)
new goal: \( A \)

NB: apply versus assumption

intro and implication introduction

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

goal: \( A \rightarrow B \)
tactic: intro \( x \)
new goal: \( B \)

proof normalization: detour

introduction immediately followed by an elimination

\[ \frac{\dot{C}}{A \rightarrow C \quad I[x] \rightarrow} \quad \frac{\ddot{A}}{\dot{A} \quad E \rightarrow} \]
proof normalization: detour elimination

\[
\begin{array}{c}
\vdash C \\
\hline
\frac{A}{A \rightarrow C} \quad \frac{I[x]}{C} \\
\hline
\frac{E}{A \rightarrow E}
\end{array}
\]

is replaced by

\[
\begin{array}{c}
\vdash \frac{A}{C} \\
\hline
\frac{E}{A}
\end{array}
\]

where every occurrence of the assumption \( A^x \) is replaced by the proof

\[
\vdash \frac{A}{C}
\]

proof normalization: normal proof

proof without a detour

\[
\begin{array}{c}
\vdash C \\
\hline
\frac{I[x]}{C} \\
\hline
\frac{I[y]}{E}
\end{array}
\]

reduces to

\[
\begin{array}{c}
\vdash C \\
\hline
\frac{I[y]}{E}
\end{array}
\]
minimal logic plus falsum

ML + ⊥

⊥ is a connective without arguments

what are the rules for ⊥?

ML plus falsum: falsum elimination rule

\[ \frac{\bot}{A} E\bot \]

ML plus falsum: negation

negation is defined: \( \neg A := A \rightarrow \bot \)

ML plus falsum: examples of tautologies

- contrapositive
  \[ (A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A) \]
- many negations
  \[ \neg \neg A \rightarrow A \]
ML plus falsum: Coq

\[ \bot \]
\[ \frac{A}{\bot} \quad E \bot \]

goal: \( A \)
tactic: elimtype False
new goal: \( \bot \)

intuitionistic logic: introduction rule for true

\[ \top \]

intuitionistic logic: rules for conjunction

conjunction introduction rule

\[ \frac{A \land B}{A} \quad I \land \]

conjunction elimination rules

\[ \frac{A \land B}{A} \quad E \land \]
\[ \frac{A \land B}{B} \quad E \land \]
split and conjunction introduction

\[ \frac{A}{A \land B} \quad \frac{B}{A \land B} \quad \text{I}_\land \]

goal: \( A \land B \)
tactic: split
new goals: \( A \) and \( B \)

elim and conjunction elimination

\[ \frac{A \land B}{A} \quad \text{E}_\land \quad \frac{A \land B}{B} \quad \text{E}_\land \]

goal: \( A \)
assumption: \( x : A \land B \)
tactic: elim \( x \)
new goal: \( A \to B \to A \)

(after two intros we have \( A \) and \( B \) available as hypothesis)

intuitionistic logic: rules for disjunction

disjunction introduction rules

\[ \frac{A}{A \lor B} \quad \text{I}_\lor \quad \frac{B}{A \lor B} \quad \text{I}_\lor \]

disjunction elimination rule

\[ \frac{A \lor B \quad A \to C \quad B \to C}{C} \]

goal: \( A \lor B \)
tactic: left
new goal: \( A \)
elim and disjunction elimination

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

goal: $C$

assumption: $x : A \lor B$

tactic: elim $x$

new goals: $A \rightarrow C$ and $B \rightarrow C$

intuitionistic logic: examples of tautologies

- $A \lor B \rightarrow B \lor A$
- $A \land B \rightarrow B \land A$

overview: first-order propositional logic

- minimal logic (ML)
  $((((A \rightarrow B) \rightarrow A) \rightarrow B) \rightarrow B)$

- ML + ⊥
  $(A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A)$

- intuitionistic logic
  $A \lor B \rightarrow (A \rightarrow C) \rightarrow (B \rightarrow C) \rightarrow C$

- classical logic
  $A \lor \neg A$

further reading

- Luitzen E.J. Brouwer
- Arend Heyting
- Development of intuitionistic logic