Logic

(Métodos Formais em Engenharia de Software)

Maria João Frade

Departmento de Informática
Universidade do Minho

2011/2012

Roadmap

- Classical Propositional Logic
- Classical First-Order Logic
- First-Order Theories
- **Natural Deduction**
  - natural deduction proof system for propositional and predicate logic; forward and backward reasoning
  - soundness; completeness; compactness
  - proof assistants; the Coq system

Natural Deduction

Introduction

- So far we have taken the "semantic" approach to logic. This, however, is not the only possible point of view.
- Instead of adopting the view based on the notion of truth, we can think of logic as a codification of reasoning. This alternative approach to logic, called "deductive", focuses directly on the deduction relation that is induced on formulas.
- A *proof system* (or *inference system*) consists of a set of basic rules for constructing derivations. Such a derivation is a formal object that encodes an explanation of why a given formula – the conclusion – is deducible from a set of assumptions.
- The rules that govern the construction of derivations are called *inference rules* and consist of zero or more *premises* and a single *conclusion*. Derivations have a tree-like shape. We use the standard notation of separating the premises from the conclusion by a horizontal line.

$$\frac{perm_1 \quad \ldots \quad perm_n}{concl}$$

Natural deduction

- The proof system we will present here is a formalisation of the reasoning used in mathematics, and was introduced by Gerhard Gentzen in the first half of the 20th century as a "natural" representation of logical derivations. It is for this reason called *natural deduction*.
- We choose to present the rules of natural deduction in sequent style.
- A *sequent* is a judgment of the form $\Gamma \vdash A$, where Γ is a set of formulas (the *context*) and A a formula (the *conclusion* of the sequent).
- A sequent $\Gamma \vdash A$ is meant to be read as "A can be deduced from the set of *assumptions* Γ", or simply "A is a consequence of Γ".

Natural deduction

The set of basic rules provided is intended to aid the translation of thought (mathematical reasoning) into formal proof.

For example, if F and G can be deduced from Γ, then $F \wedge G$ can also be deduced from Γ .

This is the "$\wedge$-introduction" rule

$$\frac{\Gamma \vdash F \quad \Gamma \vdash G}{\Gamma \vdash F \wedge G} \wedge_{\mathsf{I}}$$

There are two "$\wedge$-elimination" rules:

$$\frac{\Gamma \vdash F \wedge G}{\Gamma \vdash F} \wedge_{\mathsf{E1}} \qquad \frac{\Gamma \vdash F \wedge G}{\Gamma \vdash G} \wedge_{\mathsf{E2}}$$

Natural deduction

- This system is intended for human use, in the sense that
  - a person can guide the proof process;
  - the proof produced is highly legible, and easy to understand.

  This contrast with decision procedures that just produce a "yes/no" answer, and may not give insight into the relationship between the assumption and the conclusion.
- We present natural deduction in sequent style, because
  - it gives a clear representation of the discharging of assumptions;
  - it is closer to what one gets while developing a proof in a proof-assistant.

Natural deduction for PL

- An *instance* of an inference rule is obtained by replacing all occurrences of each meta-variable by a phrase in its range. An inference rule containing no premises is called an *axiom schema* (or simply, an *axiom*).

The proof system $\mathcal{N}_{\mathsf{PL}}$ of *natural deduction* for propositional logic is defined by the rules presented in the next slide. A *derivation* (or *proof*) in $\mathcal{N}_{\mathsf{PL}}$ is inductively defined by the following clause:

- If

$$\frac{\Gamma_1 \vdash A_1 \quad \ldots \quad \Gamma_n \vdash A_n}{\Gamma \vdash A}\ (\mathsf{R})$$

  is an instance of rule (R) of the proof system, and $\mathcal{D}_i$ is a derivation with conclusion $\Gamma_i \vdash A_i$ (for $1 \leq i \leq n$), then

$$\frac{\mathcal{D}_1 \quad \ldots \quad \mathcal{D}_n}{\Gamma \vdash A}\ (\mathsf{R})$$

A sequent $\Gamma \vdash A$ is *derivable* in $\mathcal{N}_{\mathsf{PL}}$ if it is the conclusion of some derivation.

System $\mathcal{N}_{\mathsf{PL}}$ for classical propositional logic

$$\frac{}{\Gamma \vdash \top}\ \text{true} \qquad \frac{A \in \Gamma}{\Gamma \vdash A}\ \text{assumption}$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ \wedge_{\mathsf{I}} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ \wedge_{\mathsf{E1}} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ \wedge_{\mathsf{E2}}$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ \vee_{\mathsf{I1}} \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ \vee_{\mathsf{I2}} \qquad \frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}\ \vee_{\mathsf{E}}$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\ \to_{\mathsf{I}} \qquad \frac{\Gamma \vdash A \quad \Gamma \vdash A \to B}{\Gamma \vdash B}\ \to_{\mathsf{E}}$$

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\ \neg_{\mathsf{I}} \qquad \frac{\Gamma \vdash A \quad \Gamma \vdash \neg A}{\Gamma \vdash \bot}\ \neg_{\mathsf{E}}$$

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A}\ \bot_{\mathsf{E}} \qquad \frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ \text{RAA}$$

Proof presentation

$\vdash \neg P \to (Q \to P) \to \neg Q$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg P, Q \to P, Q \vdash Q} \quad \dfrac{}{\neg P, Q \to P, Q \vdash Q \to P}\ \to_{\mathsf{E}}}{\neg P, Q \to P, Q \vdash P} \quad \dfrac{}{\neg P, Q \to P, Q \vdash \neg P}\ \neg_{\mathsf{E}}}{\neg P, Q \to P, Q \vdash \bot}}{\neg P, Q \to P \vdash \neg Q}\ \to_{\mathsf{I}}}{\neg P \vdash (Q \to P) \to \neg Q}\ \to_{\mathsf{I}}}{\vdash \neg P \to (Q \to P) \to \neg Q}\ \to_{\mathsf{I}}$$

- This example shows that even for such a reasonably simple formula, the size of the tree already poses a problem from the point of view of its representation.
- For that reason, we shall adopt an alternative format for presenting bigger proof trees.

Backward reasoning

- This presentation style in fact corresponds to a popular strategy for constructing derivations. In *backward reasoning* one starts with the conclusion sequent and chooses to apply a rule that can justify that conclusion; one then repeats the procedure on the resulting premises.

$\vdash \neg P \to (Q \to P) \to \neg Q$

$\vdash \neg P \to (Q \to P) \to \neg Q$ $\to_{\mathsf{I}}$
1. $\neg P \vdash (Q \to P) \to \neg Q$ $\to_{\mathsf{I}}$
1. $\neg P, Q \to P \vdash \neg Q$ $\neg_{\mathsf{I}}$
1. $\neg P, Q \to P, Q \vdash \bot$ $\neg_{\mathsf{E}}$
1. $\neg P, Q \to P, Q \vdash P$ $\to_{\mathsf{E}}$
1. $\neg P, Q \to P, Q \vdash Q$ assumption
2. $\neg P, Q \to P, Q \vdash Q \to P$ assumption
2. $\neg P, Q \to P, Q \vdash \neg P$ assumption

- In a proof-assistant the proof is usually developed backwards.

Forward reasoning

- If one prefers to present derivations in a forward fashion, which corresponds to constructing derivations using the *forward reasoning* strategy, then it is customary to simply give sequences of judgments, each of which is either an axiom or follows from a preceding judgment in the sequence, by an instance of an inference rule.

$\vdash \neg P \to (Q \to P) \to \neg Q$

	Judgment	Justification
1.	$\neg P, Q \to P, Q \vdash Q$	assumption
2.	$\neg P, Q \to P, Q \vdash Q \to P$	assumption
3.	$\neg P, Q \to P, Q \vdash P$	$\to_{\mathsf{E}}$ 1, 2
4.	$\neg P, Q \to P, Q \vdash \neg P$	assumption
5.	$\neg P, Q \to P, Q \vdash \bot$	$\neg_{\mathsf{E}}$ 3, 4
6.	$\neg P, Q \to P \vdash \neg Q$	$\neg_{\mathsf{I}}$ 5
7.	$\neg P \vdash (Q \to P) \to \neg Q$	$\to_{\mathsf{I}}$ 6
8.	$\vdash \neg P \to (Q \to P) \to \neg Q$	$\to_{\mathsf{I}}$ 7

In a proof-assistant

In a proof-assistant, the usual approach is to develop the proof by a method that is known as *goal directed proof*:

1. The user enters a statement that he wants to prove.
2. The system displays the formula as a formula to be proved, possibly giving a context of local facts that can be used for this proof.
3. The user enters a command (a basic rule or a *tactic*) to decompose the goal into simpler ones.
4. The system displays a list of formulas that still need to be proved.

When there are no more goals the proof is complete!

An example

$\vdash A \vee \neg A$ proved in backward direction

$\vdash A \vee \neg A$ RAA

1. $\neg(A \vee \neg A) \vdash \bot$ $\neg_E$

1. $\neg(A \vee \neg A) \vdash \neg(A \vee \neg A)$ assumption

2. $\neg(A \vee \neg A) \vdash A \vee \neg A$ $\vee_{I2}$

1. $\neg(A \vee \neg A) \vdash \neg A$ $\neg_I$

1. $\neg(A \vee \neg A), A \vdash \bot$ $\neg_E$

1. $\neg(A \vee \neg A), A \vdash A \vee \neg A$ $\vee_{I1}$

1. $\neg(A \vee \neg A), A \vdash A$ assumption

2. $\neg(A \vee \neg A), A \vdash \neg(A \vee \neg A)$ assumption

Admissible rule

An inference rule is *admissible* in a formal system if every judgement that can be proved making use of that rule can also be proved without it (in other words the set of judgements of the system is closed under the rule).

Weakening

The following rule, named *weakening*, is admissible in $\mathcal{N}_{PL}$

$$\frac{\Gamma \vdash A}{\Gamma, B \vdash A}$$

Derivable rule

An inference rule is said to be *derivable* in a proof system if the conclusion of the rule can be derived from its premisses using the other rules of the system.

Example of a derivable rule

	Judgment	Justification
1.	$\Gamma \vdash A \wedge B$	premise
2.	$\Gamma \vdash A$	$\wedge_{E1}$ 1
3.	$\Gamma \vdash B$	$\wedge_{E2}$ 1
4.	$\Gamma \vdash B \wedge A$	$\wedge_I$ 3, 2

Hence the rule $\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash B \wedge A}$ is a derivable.

Soundness, completeness and compactness of PL

Soundness

If $\Gamma \vdash F$, then $\Gamma \models F$.

Completeness

If $\Gamma \models F$, then $\Gamma \vdash F$.

Compactness

A (possible infinite) set of formulas Γ is satisfiable if and only if every finite subset of Γ is satisfiable.

Exercises

- Prove that $P \to Q \vdash \neg Q \to \neg P$ holds in $\mathcal{N}_{\mathsf{PL}}$.
- Prove that $\neg Q \to \neg P \vdash P \to Q$ holds in $\mathcal{N}_{\mathsf{PL}}$. (classical)
- Prove that the folowing rules are derivable in $\mathcal{N}_{\mathsf{PL}}$.
  1. $$\frac{\Gamma \vdash A \quad \Gamma, A \vdash B}{\Gamma \vdash B}\ \text{cut}$$
  2. $$\frac{\Gamma \vdash A}{\Gamma \vdash \neg\neg A}\ \neg\neg\text{I}$$
  3. $$\frac{\Gamma, A \vdash B \quad \Gamma, \neg A \vdash B}{\Gamma \vdash B}$$

Natural deduction for FOL

- We present here a natural deduction proof system for classical first-order logic in sequent style.
- Derivations in FOL will be similar to derivations in PL, except that we will have new proof rules for dealing with the quantifiers.
- More precisely, we overload the proof rules of PL, and we add introduction and elimination rules for the quantifiers. This means that the proofs developed for PL still hold in this proof system.

The proof system $\mathcal{N}_{\mathsf{FOL}}$ of natural deduction for first-order logic is defined by the rules presented in the next slide.

- An instance of an inference rule is obtained by replacing all occurrences of each meta-variable by a phrase in its range. In some rules, there may be side conditions that must be satisfied by this replacement. Also, there may be syntactic operations (such as substitutions) that have to be carried out after the replacement.

System $\mathcal{N}_{\mathsf{FOL}}$ for classical first-order logic

$$\frac{}{\Gamma \vdash \top}\ \text{true} \qquad \frac{\phi \in \Gamma}{\Gamma \vdash \phi}\ \text{assumption}$$

$$\frac{\Gamma \vdash \phi \quad \Gamma \vdash \psi}{\Gamma \vdash \phi \wedge \psi}\ \wedge_I \qquad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \phi}\ \wedge_{\text{E1}} \qquad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \psi}\ \wedge_{\text{E2}}$$

$$\frac{\Gamma \vdash \phi}{\Gamma \vdash \phi \vee \psi}\ \vee_{\text{I1}} \qquad \frac{\Gamma \vdash \psi}{\Gamma \vdash \phi \vee \psi}\ \vee_{\text{I2}} \qquad \frac{\Gamma \vdash \phi \vee \psi \quad \Gamma, \phi \vdash \theta \quad \Gamma, \psi \vdash \theta}{\Gamma \vdash \theta}\ \vee_{\text{E}}$$

$$\frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \to \psi}\ \to_{\text{I}} \qquad \frac{\Gamma \vdash \phi \quad \Gamma \vdash \phi \to \psi}{\Gamma \vdash \psi}\ \to_{\text{E}}$$

$$\frac{\Gamma, \phi \vdash \bot}{\Gamma \vdash \neg\phi}\ \neg_{\text{I}} \qquad \frac{\Gamma \vdash \phi \quad \Gamma \vdash \neg\phi}{\Gamma \vdash \bot}\ \neg_{\text{E}}$$

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash \phi}\ \bot_{\text{E}} \qquad \frac{\Gamma, \neg\phi \vdash \bot}{\Gamma \vdash \phi}\ \text{RAA}$$

System $\mathcal{N}_{\mathsf{FOL}}$ for classical first-order logic

Proof rules for quantifiers.

$$\frac{\Gamma \vdash \phi[y/x]}{\Gamma \vdash \forall x.\,\phi}\ \forall_{\mathsf{I}}\ \textbf{(a)} \qquad \frac{\Gamma \vdash \forall x.\,\phi}{\Gamma \vdash \phi[t/x]}\ \forall_{\mathsf{E}}$$

$$\frac{\Gamma \vdash \phi[t/x]}{\Gamma \vdash \exists x.\,\phi}\ \exists_{\mathsf{I}} \qquad \frac{\Gamma \vdash \exists x.\,\phi \quad \Gamma, \phi[y/x] \vdash \theta}{\Gamma \vdash \theta}\ \exists_{\mathsf{E}}\ \textbf{(b)}$$

(a) y must not occur free in either Γ or ϕ.

(b) y must not occur free in either Γ, ϕ or θ.

System $\mathcal{N}_{\mathsf{FOL}}$ for classical first-order logic

- Rule $\forall_{\mathsf{I}}$ tells us that if $\phi[y/x]$ can be deduced from Γ for a variable y that does not occur free in either Γ or ϕ, then $\forall x.\phi$ can also be deduced from Γ because y is fresh. The side condition (a) stating that y must not be free in ϕ or in any formula of Γ is crucial for the soundness of this rule. As y is a fresh variable we can think of it as an indeterminate term, which justifies that $\forall x.\phi$ can be deduced from Γ.
- Rule $\forall_{\mathsf{E}}$ says that if $\forall x.\phi$ can be deduced from Γ then the x in ϕ can be replaced by any term t assuming that t is free for x in ϕ (this is implicit in the notation). It is easy to understand that this rule is sound: if ϕ is true for all x, then it must be true for any particular term t.
- Rule $\exists_{\mathsf{I}}$ tells us that if it can be deduced from Γ that $\phi[t/x]$ for some term t which is free for x in ϕ (this proviso is implicit in the notation), then $\exists x.\phi$ can also be deduced from Γ.
- The second premise of rule $\exists_{\mathsf{E}}$ tells us that θ can be deduced if, additionally to Γ, ϕ holds for an indeterminate term. But the first premise states that such a term exists, thus θ can be deduced from Γ with no further assumptions.

An example

$(\exists x.\neg\psi) \rightarrow \neg\forall x.\psi$ is a theorem

$\vdash (\exists x.\neg\psi) \rightarrow \neg\forall x.\psi$ $\rightarrow_{\mathsf{I}}$

1. $\exists x.\neg\psi \vdash \neg\forall x.\psi$ $\neg_{\mathsf{I}}$

1. $\exists x.\neg\psi, \forall x.\psi \vdash \bot$ $\exists_{\mathsf{E}}$

1. $\exists x.\neg\psi, \forall x.\psi \vdash \exists x.\neg\psi$ assumption

2. $\exists x.\neg\psi, \forall x.\psi, \neg\psi[x_0/x] \vdash \bot$ $\neg_{\mathsf{E}}$

1. $\exists x.\neg\psi, \forall x.\psi, \neg\psi[x_0/x] \vdash \psi[x_0/x]$ $\forall_{\mathsf{E}}$

1. $\exists x.\neg\psi, \forall x.\psi, \neg\psi[x_0/x] \vdash \forall x.\psi$ assumption

2. $\exists x.\neg\psi, \forall x.\psi, \neg\psi[x_0/x] \vdash \neg\psi[x_0/x]$ assumption

Note that when the rule $\exists_{\mathsf{E}}$ is applied a fresh variable x_0 is introduced. The side condition imposes that x_0 must not occur free either in $\exists x.\neg\psi$ or in $\forall x.\psi$.

An example

Instead of explicitly write the substitutions, the following derivation adopts the convention to establish the converse implication.

$\phi(x_1, \ldots, x_n)$ to denote a formula having free variables $x_1, \ldots, x_n$ and $\phi(t_1, \ldots, t_n)$ denote the formula obtained by replacing each free occurrence of x_i in ϕ by the term t_i.

$(\neg\forall x.\psi(x)) \rightarrow \exists x.\neg\psi(x)$ is a theorem

$\vdash (\neg\forall x.\psi(x)) \rightarrow \exists x.\neg\psi(x)$ $\rightarrow_{\mathsf{I}}$

1. $\neg\forall x.\psi(x) \vdash \exists x.\neg\psi(x)$ RAA

1. $\neg\forall x.\psi(x), \neg\exists x.\neg\psi(x) \vdash \bot$ $\neg_{\mathsf{E}}$

1. $\neg\forall x.\psi(x), \neg\exists x.\neg\psi(x) \vdash \neg\forall x.\psi(x)$ assumption

2. $\neg\forall x.\psi(x), \neg\exists x.\neg\psi(x) \vdash \forall x.\psi(x)$ $\forall_{\mathsf{I}}$

1. $\neg\forall x.\psi(x), \neg\exists x.\neg\psi(x) \vdash \psi(x_0)$ RAA

1. $\neg\forall x.\psi(x), \neg\exists x.\neg\psi(x), \neg\psi(x_0) \vdash \bot$ $\neg_{\mathsf{E}}$

1. $\neg\forall x.\psi(x), \neg\exists x.\neg\psi(x), \neg\psi(x_0) \vdash \neg\exists x.\neg\psi(x)$ assumption

2. $\neg\forall x.\psi(x), \neg\exists x.\neg\psi(x), \neg\psi(x_0) \vdash \exists x.\neg\psi(x)$ $\exists_{\mathsf{I}}$

1. $\neg\forall x.\psi(x), \neg\exists x.\neg\psi(x), \neg\psi(x_0) \vdash \neg\psi(x_0)$ assumption

Soundness, completeness and compactness of $\mathcal{N}_{\mathsf{FOL}}$

Soundness

If $\Gamma \vdash \phi$, then $\Gamma \models \phi$.

Completeness

If $\Gamma \models \phi$, then $\Gamma \vdash \phi$.

Compactness

A (possible infinite) set of sentences Γ is satisfiable if and only if every finite subset of Γ is satisfiable.

Exercises

- Prove that the following sequents hold in $\mathcal{N}_{\mathsf{FOL}}$:
  1. $(\forall x.\phi(x)) \vee (\forall x.\psi(x)) \vdash \forall x.\phi(x) \vee \psi(x)$
  2. $\exists x.\exists y.\phi(x,y) \vdash \exists y.\exists x.\phi(x,y)$
- Show that the following rules are derivable in $\mathcal{N}_{\mathsf{FOL}}$:
  1. $$\frac{\Gamma, \forall x.\phi, \phi[t/x] \vdash \psi}{\Gamma, \forall x.\phi \vdash \psi}$$
  2. $$\frac{\Gamma, \phi[y/x] \vdash \psi}{\Gamma, \exists x.\phi \vdash \psi}$$ if y does not occur free in Γ or ψ

Proof checking mathematical statements

- Mathematics is usually presented in an informal but precise way.

> In situation Γ we have ψ.
> Proof. p. QED

- In Logic, Γ, ψ become formal objects and proofs can be formalized as a derivation (following some precisely given set of rules).

> $\Gamma \vdash_L \psi$
> Proof. p. QED

Proof-assistants

A *proof-assistant* is the combination of a *proof-checker* with a *proof-development system* to help on the formalization process and the interactive development of proofs.

In a proof-assistant, after formalizing the primitive notions of the theory (under study), the user develops the proofs interactively by means of (proof) *tactics*, and when a proof is finished a *"proof term"* (or simply a *"proof script"*) is created.

Machine assisted theorem proving:

- helps to deal with large problems;
- prevents us from overseeing details;
- does the bookkeeping of the proofs.

Proof-assistants

There are many proof-assistants for many different logics: fist-order logic, higher-order logic, modal logic, ...

We can mention as examples:

- Coq - http://coq.inria.fr/
- Isabelle - http://isabelle.in.tum.de/
- HOL - http://www.cl.cam.ac.uk/research/hvg/HOL
- Agda - http://wiki.portal.chalmers.se/agda/
- PVS - http://pvs.csl.sri.com/
- ...

The Coq proof-assistant

Demo

http://coq.inria.fr/