barkhauseninstitut.org

barkhausen institut

Foundations of Certified Programming Language and Compiler Design

Dr.-Ing. Sebastian Ertel

Composable Operating Systems Group, Barkhausen Institute

Outline

Lecture	Logic Coq/Lean	Formalisms	PL Haskell
1	Propositional and first-order logic		
2			Functional programming
3		Syntax and Semantics	
4			The untyped lambda calculus
5		Types	
6			The typed lambda calculus
7			Polymorphism
8		Curry-Howard	
9			Higher-order types
10			Dependent types

Goals

There are two reasons for studying logic:

1. For proving theorems in Coq.
2. For understanding the deep connection between logic and programming languages.

Syntax

Syntax:

A	$::=$		formulas:
	$\mid$	$P \mid Q \mid R$	propositional variables
	$\mid$	$A \Rightarrow A$	implication

Semantics

- Consider the folowing logical formula of propositions P, Q and R:

$$(P \Rightarrow Q) \Rightarrow ((Q \Rightarrow R) \Rightarrow (P \Rightarrow R))$$

- There exist two approaches to prove this formula.

[1] Alfred Tarski. "The semantic conception of truth: and the foundations of semantics". In: *Philosophy and phenomenological research* 4.3 (1944), pp. 341–376.
[2] Arend Heyting. *Intuitionism: an introduction*. Vol. 41. Elsevier, 1966.

Semantics

- Consider the folowing logical formula of propositions P, Q and R:

$$(P \Rightarrow Q) \Rightarrow ((Q \Rightarrow R) \Rightarrow (P \Rightarrow R))$$

- There exist two approaches to prove this formula.

denotational[1]

- Denotation: $t \triangleq$ `true` and $f \triangleq$ `false`
- If the value of the complete formula is `t` in all cases then the formula is said to be *valid*.
- This is referred to as *classical logic*.
- Example: truth table

P	Q	R	$P \Rightarrow Q$	$Q \Rightarrow R$	$P \Rightarrow R$	$(Q \Rightarrow R) \Rightarrow (P \Rightarrow R)$	
f	f	f	t	t	t	t	t
f	f	t	t	t	t	t	t
f	t	f	t	f	t	t	t
f	t	t	t	t	t	t	t
t	f	f	f	t	f	f	t
t	f	t	f	t	t	t	t
t	t	f	t	f	f	t	t
t	t	t	t	t	t	t	t

Semantics

- Consider the folowing logical formula of propositions P, Q and R:

$$(P \Rightarrow Q) \Rightarrow ((Q \Rightarrow R) \Rightarrow (P \Rightarrow R))$$

- There exist two approaches to prove this formula.

denotational[1]
- Denotation: $t \triangleq \texttt{true}$ and $f \triangleq \texttt{false}$
- If the value of the complete formula is `t` in all cases then the formula is said to be *valid*.
- This is referred to as *classical logic*.

constructive[2]
- Replaces the question “Is P true?” with “What are the proofs of P?”
- A proof for $P \Rightarrow Q$ is the process of constructing a proof of Q from a proof of P.
- This is called *intuitionistic logic* and was proposed in the early 20th century by Brouwer.

[1] Alfred Tarski. “The semantic conception of truth: and the foundations of semantics”. In: *Philosophy and phenomenological research* 4.3 (1944), pp. 341–376.

[2] Arend Heyting. *Intuitionism: an introduction*. Vol. 41. Elsevier, 1966.

Natural Deduction
Syntax

- Natural deduction is a formalism for proofs due to Gentzen[1].

Definition (Formulas/Propositions)

$$
\begin{array}{lcll}
X & \in & \mathcal{X} & \text{fixed countable infinite set of propositional variables} \\
A & ::= & & \\
 & | & X & \text{propositional variables} \\
 & | & A_1 \Rightarrow A_2 & \text{implication} \\
 & | & A_1 \wedge A_2 & \text{conjunction} \\
 & | & \top & \text{truth} \\
 & | & A_1 \vee A_2 & \text{disjunction} \\
 & | & \bot & \text{falsity} \\
 & | & \neg A_1 & \text{negation}
\end{array}
$$

[1] Gerhard Gentzen. “Untersuchungen Über Das Logische Schließen. I.”. In: *Mathematische Zeitschrift* 35 (1935), pp. 176–210.

Definition (Context)

A *context*

$$\Gamma = A_1, \ldots, A_n$$

is a list of n propositions.

Interpretation:

- The comma (,) in the specification of a context can be read as a “meta” conjunction.
- Do not confuse it with the logical conjunction $\wedge$ that appears in formulas!

Definition (Sequent/Judgement)

A *sequent* is a pair

$$\Gamma \vdash A$$

that consists of a context and a proposition.

Interpretation:

- The $\vdash$ in the specification of a judgement can be read as a “meta” implication.
- Do not confuse it with the logical implication $\Rightarrow$ that appears in formulas!

Definition (Inference Rule)

An *inference rule*

$$\frac{\Gamma \vdash A_1 \quad \ldots \quad \Gamma \vdash A_n}{\Gamma \vdash A}$$

consists of n sequents as premises and a concluding sequent.

Interpretation:

- deductively: from the proofs for each of the premises, we can deduce the conclusion
- inductively: for a proof of the conclusion, we need to construct proofs for each of the premises

The NJ System

Rules for Intuitionistic Natural Deduction

$$\frac{}{\Gamma, A, \Gamma' \vdash A}\ (ax)$$

Elimination rules

$$\frac{\Gamma \vdash A_1 \Rightarrow A_2 \quad \Gamma \vdash A_1}{\Gamma \vdash A_2}\ (\Rightarrow_E)$$

$$\frac{\Gamma \vdash A_1 \wedge A_2}{\Gamma \vdash A_1}\ (\wedge_E^l) \qquad \frac{\Gamma \vdash A_1 \wedge A_2}{\Gamma \vdash A_2}\ (\wedge_E^r)$$

$$\frac{\Gamma \vdash A_1 \vee A_2 \quad \Gamma, A_1 \vdash A_3 \quad \Gamma, A_2 \vdash A_3}{\Gamma \vdash A_3}\ (\vee_E)$$

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A_1}\ (\bot_E)$$

explosion principle

$$\frac{\Gamma \vdash \neg A_1 \quad \Gamma \vdash A_1}{\Gamma \vdash \bot}\ (\neg_E)$$

principle of non-contradiction

Introduction rules

$$\frac{\Gamma, A_1 \vdash A_2}{\Gamma \vdash A_1 \Rightarrow A_2}\ (\Rightarrow_I)$$

$$\frac{\Gamma \vdash A_1 \quad \Gamma \vdash A_2}{\Gamma \vdash A_1 \wedge A_2}\ (\wedge_I)$$

$$\frac{\Gamma \vdash A_1}{\Gamma \vdash A_1 \vee A_2}\ (\vee_I^l) \qquad \frac{\Gamma \vdash A_2}{\Gamma \vdash A_1 \vee A_2}\ (\vee_I^r)$$

$$\frac{\Gamma, A_1 \vdash \bot}{\Gamma \vdash \neg A_1}\ (\neg_I)$$

(incarnation of explosion principle)

$$\frac{}{\Gamma \vdash \top}\ (\top_I)$$

Consistency: There is at least one formula ($\bot$) that is not provable.

Intuitionistic vs Classic Logic

- Intuitionistic logic:

Intuitionist logic allows to extract so-called witnesses from proofs, e.g., from a proof of $A_1 \vee A_2$ we know which of the two propositions A_1 and A_2 actually holds.

- Classical logic:

$$\frac{}{\vdash \neg A \vee A} \text{ (excluded middle)}$$

Proofs

Proofs are defined inductively:

A sequent $\Gamma \vdash A$ is *provable* when it is the conclusion of a proof.

A formula A is *provable* when it is provable **without** hypothesis, i.e., the sequent $\vdash A$ is provable.

A proof is an inference rule (according to the definition above)

$$\frac{\dfrac{\pi_1}{\Gamma_1 \vdash A_1} \quad \dots \quad \dfrac{\pi_n}{\Gamma_n \vdash A_n}}{\Gamma \vdash A}$$

where all the premises are proofs themselves.

Examples

Proposition: $(A_1 \land A_2) \Rightarrow (A_1 \lor A_2)$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A_1 \land A_2 \vdash A_1 \land A_2}\,(ax)}{A_1 \land A_2 \vdash A_1}\,(\land_E)}{A_1 \land A_2 \vdash A_1 \lor A_2}\,(\lor_I^l)}{\vdash (A_1 \land A_2) \Rightarrow (A_1 \lor A_2)}\,(\Rightarrow_I)$$

Proposition: $(A_1 \lor A_2) \Rightarrow (A_2 \lor A_1)$

$$\dfrac{\dfrac{\dfrac{}{A_1 \lor A_2 \vdash A_1 \lor A_2}\,(ax) \qquad \dfrac{\dfrac{}{A_1 \lor A_2, A_2 \vdash A_2}\,(ax)}{A_1 \lor A_2, A_2 \vdash A_2 \lor A_1}\,(\lor_I^l) \qquad \dfrac{\dfrac{}{A_1 \lor A_2, A_1 \vdash A_1}\,(ax)}{A_1 \lor A_2, A_1 \vdash A_2 \lor A_1}\,(\lor_I^r)}{A_1 \lor A_2 \vdash A_2 \lor A_1}\,(\lor_E)}{\vdash (A_1 \lor A_2) \Rightarrow (A_2 \lor A_1)}\,(\Rightarrow_I)$$

What we have learned

- We know propositional logic and
- in particular natural deduction as a framework for proving propositions.
- We understand the difference between classical and intuitionistic logic
- and why it needs to be the foundation for theorem provers.