LMSE 1

Logische Methoden des Software Engineerings

Vertiefungsmodul 1

Prof. Dr. Jakob Rehof

M.Sc. Andrej Dudenhefner

Lehrstuhl XIV, Software Engineering

Diese Vorlesung

- Intuitionistische Logik

- Natürliche Deduktion

Lesen und Übungen

- Lesen Kapitel 2.1 und 2.2 (Seite 23 - 28)
- Übungen
  - Aufgabe 2.7.3
  - Zeigen Sie mittels natürlicher Deduktion, dass die Formeln

    $$\varphi_1 = \neg(p \vee q) \rightarrow (\neg p \wedge \neg q)$$

    $$\varphi_2 = (\neg p \wedge \neg q) \rightarrow \neg(p \vee q)$$

    $$\varphi_3 = \neg\neg\neg p \rightarrow \neg p$$

    gültig sind.

Curry-Howard isomorphism

$$\frac{}{\Gamma, x : \tau \vdash x : \tau}\text{(var)}$$

$$\frac{\Gamma, x : \tau \vdash M : \sigma}{\Gamma \vdash \lambda x.M : \tau \to \sigma}(\to\text{I})$$

$$\frac{\Gamma \vdash M : \tau \to \sigma \qquad \Gamma \vdash N : \tau}{\Gamma \vdash M N : \sigma}(\to\text{E})$$

Curry-Howard isomorphism

$$\frac{}{\Gamma, \tau \vdash \tau}(\text{hyp})$$

$$\frac{\Gamma, \tau \vdash \sigma}{\Gamma \vdash \tau \to \sigma}(\text{DT})$$

$$\frac{\Gamma \vdash \tau \to \sigma \qquad \Gamma \vdash \tau}{\Gamma \vdash \sigma}(\text{MP})$$

Exercise 1

Let $\Gamma = \{\tau_1, \ldots, \tau_n\}$. *Prove that, if* $\Gamma \vdash \sigma$ *then* $\tau_1 \to \cdots \to \tau_n \to \sigma$ *is boolean tautology, when* $\to$ *is interpreted as implication.*

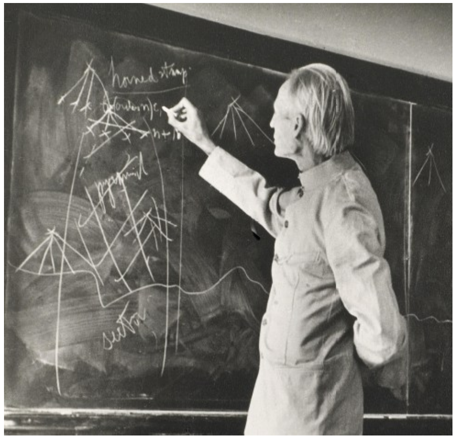
So, inhabitation is *provability* in intuitionistic propositional logic.

Intuitionistic logic

- *Classical logic* is about **truth**
- *Intuitionistic logic* is about **constructibility**
- Intuitionistic logic is therefore also called *constructive logic*
- All statements are classically regarded as either true or false: **p v –p** holds (*tertium non datur*)
  - „there is 7 seven‘s somewhere in the decimal representation of the number π“
  - „there are irrational p and q such that p^q is rational“

- Intuitionistic logic, in contrast, requires that we can *construct* the objects whose existence we assert and hence rejects the *tertium non datur* principle

Intuitionistic logic



- **L.E.J.Brouwer** (1881-1966)
- **Arend Heyting** (1898-1980)

- Glivenko
- Kolmogorov
- Gentzen
- Gödel
- ...

BHK-interpretation (informal constructive semantics)

- *A construction of* $\varphi_1 \wedge \varphi_2$ *consists of a construction of* φ_1 *and a construction of* φ_2*;*

- *A construction of* $\varphi_1 \vee \varphi_2$ *consists of a number* $i \in \{1, 2\}$ *and a construction of of* φ_i*;*

- *A construction of* $\varphi_1 \to \varphi_2$ *is a method (function) transforming every construction of* φ_1 *into a construction of* φ_2*;*

- *There is no possible construction of* $\bot$ *(where* $\bot$ *denotes falsity).*

BHK-interpretation (informal constructive semantics)

- *A construction of* $\varphi_1 \wedge \varphi_2$ *consists of a construction of* φ_1 *and a construction of* φ_2*;*
- *A construction of* $\varphi_1 \vee \varphi_2$ *consists of a number* $i \in \{1, 2\}$ *and a construction of of* φ_i*;*
- *A construction of* $\varphi_1 \to \varphi_2$ *is a method (function) transforming every construction of* φ_1 *into a construction of* φ_2*;*
- *There is no possible construction of* $\bot$ *(where* $\bot$ *denotes falsity).*

Negation $\neg\varphi$ is best understood as an abbreviation of an implication $\varphi \to \bot$. That is, we assert $\neg\varphi$ when the assumption of φ leads to an absurd. It follows that

- *A construction of* $\neg\varphi$ *is a method that turns every construction of* φ *into a non-existent object.*

BHK-interpretation (informal constructive semantics)

- *A construction of* $\varphi_1 \wedge \varphi_2$ *consists of a construction of* φ_1 *and a construction of* φ_2*;*
- *A construction of* $\varphi_1 \vee \varphi_2$ *consists of a number* $i \in \{1, 2\}$ *and a construction of of* φ_i*;*
- *A construction of* $\varphi_1 \rightarrow \varphi_2$ *is a method (function) transforming every construction of* φ_1 *into a construction of* φ_2*;*
- *There is no possible construction of* $\bot$ *(where* $\bot$ *denotes falsity).*

Note: This informal interpretation can be formalized in

- **recursion theory:** Kleene‘s notion of **realizability**
- **lambda calculus:** the **Curry-Howard isomorphism**

Natural deduction

$$\Phi ::= \bot \mid PV \mid (\Phi \to \Phi) \mid (\Phi \vee \Phi) \mid (\Phi \wedge \Phi).$$

$$\Gamma, \varphi \vdash \varphi \ (\mathrm{Ax})$$

$$\frac{\Gamma \vdash \varphi \quad \Gamma \vdash \psi}{\Gamma \vdash \varphi \wedge \psi} \ (\wedge\mathrm{I}) \qquad \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \varphi} (\wedge\mathrm{E}) \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \psi}$$

$$\frac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi} \quad (\vee\mathrm{I}) \quad \frac{\Gamma \vdash \psi}{\Gamma \vdash \varphi \vee \psi} \qquad \frac{\Gamma, \varphi \vdash \rho \quad \Gamma, \psi \vdash \rho \quad \Gamma \vdash \varphi \vee \psi}{\Gamma \vdash \rho} \ (\vee\mathrm{E})$$

$$\frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \to \psi} \ (\to \mathrm{I}) \qquad \frac{\Gamma \vdash \varphi \to \psi \quad \Gamma \vdash \varphi}{\Gamma \vdash \psi} (\to \mathrm{E})$$

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash \varphi} \ (\bot\mathrm{E})$$

Proof trees

2.2.5. Example. Let Γ abbreviate $\{\varphi \to (\psi \to \vartheta), \varphi \to \psi, \varphi\}$.

(i)

$$\dfrac{\varphi \vdash \varphi}{\vdash \varphi \to \varphi}\ (\to \mathrm{I})$$

(ii)

$$\dfrac{\dfrac{\varphi, \psi \vdash \varphi}{\varphi \vdash \psi \to \varphi}\ (\to \mathrm{I})}{\vdash \varphi \to (\psi \to \varphi)}\ (\to \mathrm{I})$$

(iii)

$$\dfrac{\dfrac{\dfrac{\dfrac{(\to \mathrm{E})\dfrac{\Gamma \vdash \varphi \to (\psi \to \vartheta) \quad \Gamma \vdash \varphi}{\Gamma \vdash \psi \to \vartheta} \qquad \dfrac{\Gamma \vdash \varphi \to \psi \quad \Gamma \vdash \varphi}{\Gamma \vdash \psi}(\to \mathrm{E})}{\Gamma \vdash \vartheta}(\to \mathrm{E})}{\varphi \to (\psi \to \vartheta), \varphi \to \psi \vdash \varphi \to \vartheta}(\to \mathrm{I})}{\varphi \to (\psi \to \vartheta) \vdash (\varphi \to \psi) \to (\varphi \to \vartheta)}(\to \mathrm{I})}{\vdash (\varphi \to (\psi \to \vartheta)) \to (\varphi \to \psi) \to (\varphi \to \vartheta)}(\to \mathrm{I})$$

Examples of classical tautologies

1. $\bot \to p$;
2. $((p \to q) \to p) \to p$;
3. $p \to \neg\neg p$;
4. $\neg\neg p \to p$;
5. $\neg\neg\neg p \to \neg p$;
6. $(\neg q \to \neg p) \to (p \to q)$;
7. $(p \to q) \to (\neg q \to \neg p)$;
8. $\neg(p \wedge q) \to (\neg p \vee \neg q)$;
9. $(\neg p \vee \neg q) \to \neg(p \wedge q)$;
10. $((p \leftrightarrow q) \leftrightarrow r) \leftrightarrow (p \leftrightarrow (q \leftrightarrow r))$;
11. $((p \wedge q) \to r) \leftrightarrow (p \to (q \to r))$;
12. $(p \to q) \leftrightarrow (\neg p \vee q)$;
13. $\neg\neg(p \vee \neg p)$.

Not all of these are intuitionistic theorems!

Example

-(p v q) → -p /\ -q

Write –p as p→0. We are to prove ((p v q) → 0) → ((p → 0) /\ (q → 0))

```
(p v q) → 0, p |-  p            (Ax)
--------------------------------- (vI)
(p v q) → 0, p |-  p v q                    (p v q) → 0, p |- (p v q) → 0          (Ax)
------------------------------------------------------------------------------------------  (→E)
                        (p v q) → 0, p |-  0
------------------------------------------------------------------------------------------- (→I)
                              (p v q) → 0  |-   p → 0
```

Similarly, we can prove (p v q) → 0 |- q → 0 by starting from (p v q) → 0, q |- q.

Therefore we have, by (/\I) (p v q) → 0 |- (p → 0) /\ (q → 0).

Then, by (→I) |- ((p v q) → 0) → ((p → 0) /\ (q → 0)).

Example

(-p /\ -q) → -(p v q)

Write –p as p→0. We are to prove ((p →0) /\ (q → 0)) → ((p v q) → 0)

((p →0) /\ (q → 0), (p v q) , p |- p (Ax)   ((p →0) /\ (q → 0), (p v q) , p |- p → 0 (/\E)

-- (→E)

[1] ((p →0) /\ (q → 0), (p v q) , p |- 0

Similarly, [2] ((p →0) /\ (q → 0), (p v q) , q |- 0.

Now, we have [3] ((p →0) /\ (q → 0), (p v q) |- p v q (Ax).

By [1], [2], [3] we conclude ((p →0) /\ (q → 0), (p v q) |- 0 by (vE).

Therefore, by (→E) conclude ((p →0) /\ (q → 0) |- (p v q) → 0.

Finally, by (→E) |- ((p →0) /\ (q → 0)) → ((p v q) → 0).

Example

$--- p \rightarrow -p$

Write –p as $p \rightarrow 0$. We are to prove $(((p \rightarrow 0) \rightarrow 0) \rightarrow 0) \rightarrow (p \rightarrow 0)$

$((p \rightarrow 0) \rightarrow 0) \rightarrow 0, p, p \rightarrow 0 \mid\!- \; p \rightarrow 0 \qquad ((p \rightarrow 0) \rightarrow 0) \rightarrow 0, p, p \rightarrow 0 \mid\!- \; p$

$((p \rightarrow 0) \rightarrow 0) \rightarrow 0, p, p \rightarrow 0 \mid\!- \; 0$

$((p \rightarrow 0) \rightarrow 0) \rightarrow 0, p \mid\!- \; (p \rightarrow 0) \rightarrow 0 \qquad ((p \rightarrow 0) \rightarrow 0) \rightarrow 0, p \mid\!- \; ((p \rightarrow 0) \rightarrow 0) \rightarrow 0$

$((p \rightarrow 0) \rightarrow 0) \rightarrow 0, p \mid\!- \; 0$

$((p \rightarrow 0) \rightarrow 0) \rightarrow 0 \mid\!- \; p \rightarrow 0$

$\mid\!- \; (((p \rightarrow 0) \rightarrow 0) \rightarrow 0) \rightarrow (p \rightarrow 0)$