Intuitionistische Logik

Typen und Terme

Sequenzenkalkül mit einer Zielformel

- Sequenz des SCSC (single conclusion sequential calculus) hat Form

  $$\Gamma \vdash p$$

  wobei p eine Aussage und Γ eine Menge von Aussagen.

- Die Symmetrie

  - Antezedent --- Succzedent
  - $\wedge$ --- $\vee$
  - $\forall$ --- $\exists$

  geht verloren !

- Statt einer $\bullet$-L $\bullet$-R Regel für jeden Operator $\bullet$ gibt es für den äußeren Operator in p

  - $\bullet$ -Einführungsregeln ($\bullet$-intro)
  - $\bullet$ -Eliminationsregeln ($\bullet$-elim)

Axiom

- Das einzige Axiom ist auch hier

$$\frac{}{\Gamma, \varphi \vdash \varphi}\ ax$$

Strukturregeln

- Die Strukturregeln entsprechen den Strukturregeln im Sequenzenkalkül, die sich nur auf die linke Seite beziehen:

$$\frac{\Gamma, \varphi \vdash \psi}{\Gamma, \varphi, \Delta \vdash \psi}$$

weakening

$$\frac{\Gamma, \varphi_1, \varphi_2 \vdash \psi}{\Gamma, \varphi_2, \varphi_1 \vdash \psi}$$

Perm

$$\frac{\Gamma, \varphi, \varphi \vdash \psi}{\Gamma, \varphi \vdash \psi}$$

Kontraktion

Regeln für $\wedge$

- Die Regeln für $\wedge$:

$$\frac{\Gamma \vdash \varphi_1,\ \Gamma \vdash \varphi_2}{\Gamma \vdash \varphi_1 \wedge \varphi_2}\ \wedge\text{-intro}$$

$$\frac{\Gamma \vdash \varphi_1 \wedge \varphi_2}{\Gamma \vdash \varphi_1}\ \wedge\text{-elim-l} \qquad \frac{\Gamma \vdash \varphi_1 \wedge \varphi_2}{\Gamma \vdash \varphi_2}\ \wedge\text{-elim-r}$$

Regeln für $\rightarrow$

- Die Regeln für $\rightarrow$

$$\frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \rightarrow \psi}$$

$\rightarrow$-intro

$$\frac{\Gamma \vdash \varphi \rightarrow \psi \qquad \Gamma \vdash \varphi}{\Gamma \vdash \psi}$$

$\rightarrow$-elim-2

Regeln für $\vee$

- Die Regeln für $\vee$:

$$\frac{\Gamma \vdash \varphi_1}{\Gamma \vdash \varphi_1 \vee \varphi_2} \vee\text{-intro-l} \qquad \frac{\Gamma \vdash \varphi_2}{\Gamma \vdash \varphi_1 \vee \varphi_2} \vee\text{-intro-r}$$

$$\frac{\Gamma \vdash \varphi_1 \vee \varphi_2 \quad \Gamma, \varphi_1 \vdash \psi, \quad \Gamma, \varphi_2 \vdash \psi}{\Gamma \vdash \psi} \vee\text{-elim}$$

Regel für $\bot$

- Regel für $\bot$

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash \varphi}$$

$\bot$ - elim

- Es gibt keine Intro-Regel für $\bot$

Negation

- Die Negation von φ wird „als Makro“ definiert:

$$\neg \varphi := \varphi \rightarrow \bot$$

- Mit den Regeln für $\rightarrow$ erhält man damit die abgeleiteten Regeln

$$\frac{\Gamma, \varphi \vdash \bot}{\Gamma \vdash \neg \varphi}\ \neg\text{-intro} \qquad \frac{\Gamma \vdash \neg \varphi}{\Gamma, \varphi \vdash \bot}\ \neg\text{-elim}$$

Tertium non datur

- Die bisherigen Regeln definieren den *intuitionistischen Aussagenkalkül.*
- Die folgenden Regeln lassen sich damit nicht herleiten:

- Tertium non datur (principle of excluded middle):

$$\frac{}{\Gamma \vdash \varphi \vee \neg\varphi}$$

PEM

- Reductio ad absurdum (Widerspruchsbeweis):

$$\frac{}{\Gamma \vdash \neg\neg\varphi \rightarrow \varphi}$$

RAA

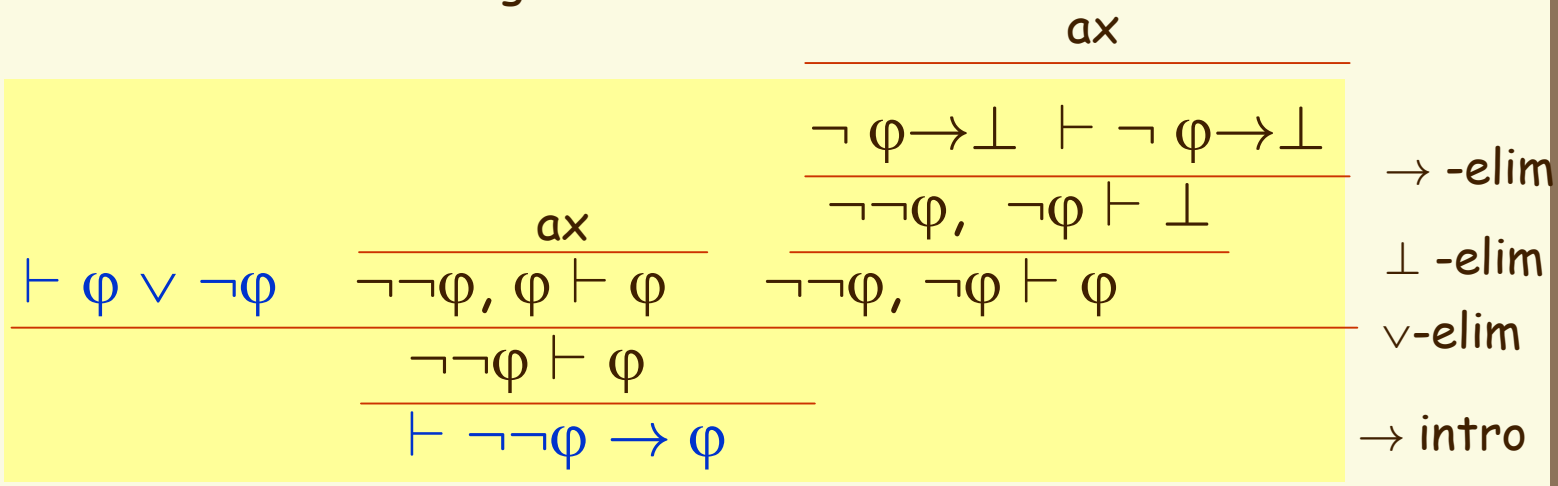
Zusammenhänge

- Im Intuitionistischen Aussagenkalkül lässt sich beweisen:

  $\vdash (\varphi \vee \neg\varphi) \quad \leftrightarrow \quad (\neg\neg\varphi \rightarrow \varphi)$

  Tertium non Datur und Widerspruchsbeweis sind also äquivalent

  - Beweis der Richtung „$\rightarrow$“:



Intuitionistisch (nicht) beweisbareAussagen

- Folgende Aussagen sind intuitionistisch nicht beweisbar

  $\varphi \vee \neg \varphi$ (tertium non datur)

  $\neg\neg\varphi \rightarrow \varphi$ (reductio ad absurdum)

  $\neg(\varphi \wedge \psi) \leftrightarrow \neg\varphi \vee \neg\psi$ (deMorgan– $\wedge$)

  $\neg\varphi \vee \psi \leftrightarrow (\varphi \rightarrow \psi)$

  $((\varphi \rightarrow \psi) \rightarrow \varphi) \rightarrow \varphi$ (Peirce-Formel)

- Folgende Aussagen sind intuitionistisch beweisbar

  $\varphi \rightarrow \neg\neg \varphi$

  $\neg\neg\neg \varphi \rightarrow \neg\varphi$

  $\neg(\varphi \vee \psi) \leftrightarrow \neg\varphi \wedge \neg\psi$ (deMorgan– $\vee$)

Intuitionistische Prädikatenlogik

- Die Regeln für den $\forall$-Quantor sind offensichtlich

$$\frac{\Gamma \vdash \varphi(x),\ x \notin FV(\Gamma)}{\Gamma \vdash \forall x.\varphi(x)}$$

$\forall$ -intro

$$\frac{\Gamma \vdash \forall x.\varphi(x)}{\Gamma \vdash \varphi(t)}$$

$\forall$ -elim

Intuitionistische Prädikatenlogik

- Der Existenzquantor ist eine Form der (unendlichen) Disjunktion.

$$\frac{\Gamma \vdash \varphi(t)}{\Gamma \vdash \exists x.\varphi(x)}$$

$\exists$ -intro

$$\frac{\Gamma \vdash \exists x.\varphi(x) \quad \Gamma,\varphi(x) \vdash \psi \quad x \notin FV(\Gamma)}{\Gamma \vdash \psi}$$

$\exists$ -elim

Was gilt – was gilt nicht

- Es gilt:

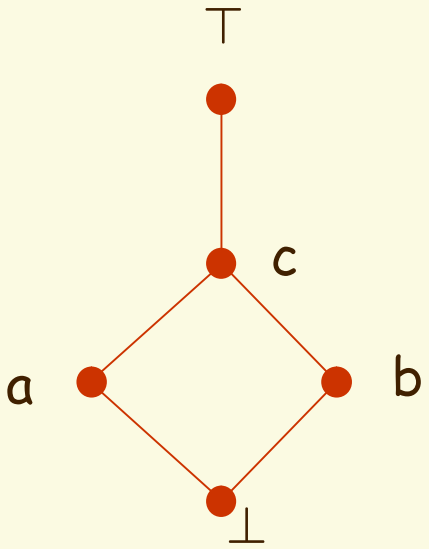
$$\neg\, \exists x.\phi(x) \quad \leftrightarrow \quad \forall x.\neg\, \phi(x)$$

- Es gilt **nicht**:

$$\neg\, \forall x.\phi(x) \quad \leftrightarrow \quad \exists x.\neg\, \phi(x)$$

Wie zeigt man Nicht-Beweisbarkeit ?

- Ersetze bool={⊥, ⊤} durch eine Heyting-Algebra, z.B. H={⊥, ⊤, a, b, c } mit der Ordnung der Figur.
  - Wir definieren ∨, ∧, → durch
    - $x \vee y = \min \{z \mid x \leq z, y \leq z\}$
    - $x \wedge y = \max \{ z \mid z \leq x, z \leq y\}$
    - $x \to y = \max \{ z \mid x \wedge z \leq y \}$



Operationstafel für „→"

→	⊥	a	b	c	⊤
⊥	⊤	⊤	⊤	⊤	⊤
a	b	⊤	b	⊤	⊤
b	a	a	⊤	⊤	⊤
c	⊥	a	b	⊤	⊤
⊤	⊥	a	b	c	⊤

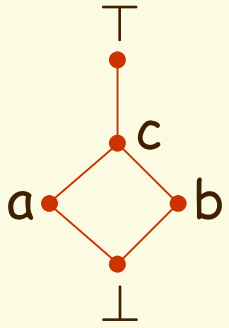
Insbesondere folgt:

$\neg c = c \to \bot = \bot$
$\neg\neg c = \bot \to \bot = \top$

Für alle $x \neq c$ gilt
$\neg\neg x = x$

Wie zeigt man Nicht-Beweisbarkeit ?

- Jede Abbildung ρ: At $\to$ H der aussagelogischen Variablen
  At in H kann auf aussagelogischen Formeln fortgesetzt werden:
  - $[\![X]\!]_\rho$:= $\rho(X)$, falls X aussagenlogische Variable
  - $[\![P \wedge Q]\!]_\rho$:= $[\![P]\!]_\rho \wedge [\![Q]\!]_\rho$
  - $[\![P \vee Q]\!]_\rho$:= $[\![P]\!]_\rho \vee [\![Q]\!]_\rho$
  - $[\![P \to Q]\!]_\rho$:= $[\![P]\!]_\rho \to [\![Q]\!]_\rho$
  - $[\![\bot]\!]_\rho$:= $\bot$



- Zeige durch Inspektion aller intuitionischen Regeln:
  - Wenn eine Sequenz $\phi_1,\ldots,\phi_n \vdash \psi$ intuitionistisch herleitbar ist, dann gilt

    $[\![\phi_1]\!]_\rho \wedge \ldots \wedge [\![\phi_n]\!]_\rho \leq [\![\psi]\!]_\rho$
  - Wähle jetzt z.B. die Abb. $\rho(A) = c$. Es folgt:

    $[\![\neg\neg A]\!]_\rho = [\![(A\to\bot)\to\bot]\!]_\rho = (c\to\bot)\to\bot = \top \not\leq c = [\![A]\!]_\rho$

Ist Intuitionismus schwächer als Klassische Logik ?

- Einerseits
  - Intuitionistische Beweise sind „glaubhafter"
  - Intuitionistische Existenzbeweise liefern immer einen *Zeugen* (witness).
  - Jeder intuitionistische Beweis für $P \rightarrow Q$ liefert einen Algorithmus, der einen Beweis von P in einen Beweis von Q transformiert.
  - Beweise sind konstruktiv (kein „deus ex machina")

- Andererseits
  - es gibt Sätze, die man intuitionistisch nicht beweisen kann
  - $\phi \vee \neg \phi$ ist nützlich, (aber ein bisschen dubios)
  - Klassisch kann man beweisen: $\exists\, p,q \in \mathbb{R}\text{-}\mathbb{Q}.\ p^q \in \mathbb{Q}$,
    (aber liefert der Beweis irgendeine Information?
  - Ähnlich kann man klassisch z.B. beweisen:
    $\exists\, x \in \mathbb{N}.\ x < 10 \leftrightarrow \forall\, k >= 4. \exists\, p,q \in \mathbb{N}.\ Prim(p) \wedge Prim(q) \wedge 2*k=p+q.$
    Aber niemand kennt x !

Ist klassische Logik nützlicher ?

- Jeder Satz, der intuitionistisch beweisbar ist, ist auch klassisch beweisbar
- Es gibt klassisch wahre Sätze, die intuitionistisch nicht beweisbar sind.

o Aber man kann zeigen:

- **Ist φ ein klassisch wahrer aussagenlogischer Satz, dann ist $\neg\neg\varphi$ intuitionistisch beweisbar**
- **Für die Prädikatenlogik muss noch das Axiom (DNS)**
  $\forall x.\ \neg\neg\phi(x) \leftrightarrow \neg\neg\forall x.\phi(x)$
- **hinzugenommen werden**
- Damit kann ein intuitionistischer Beweiskalkül genausogut auch für Beweise der klassischen Logik hergenommen werden.

Was hat man von Intuitionismus

- In der Informatik interessiert man sich hauptsächlich für Objekte, die man konstruieren kann
  - für Funktionen nur, wenn man eine Vorschrift (Algorithmus) hat, diese zu berechnen
  - für Beweise nur, wenn sie das angeblich existierende Element auch liefern.
- Es gibt eine eindeutige Entsprechung zwischen Typtheorie und intuitionistischer Logik
  - Curry-Howard-Isomorphismus
  - Ein intuitionistischer Beweis, dass man eine Folge ordnen kann, liefert automatisch einen Algorithmus („proofs as programs")
    - wenn der Beweis korrekt ist, ist der Algorithmus beweisbar korrekt
- Neuere Anwendungen
  - proof-carrrying code
  - trusted code

Vergleich: Typtheorie Intuitionismus

- p : P interpretieren wir jetzt als: p ist ein Beweis für T

  - $p : P_1 \wedge P_2$ — p ist von der Form (p_1,p_2) mit $p_1: P_1$, $p_2:P_2$
  - $p : P_1 \vee P_2$ — p ist von der form $(1,p_1)$ oder $(2,p_2)$ mit $p_1:P_1$ und $p_2:P_2$
  - $p: P \to Q$, — p ist ein Algorithmus, der einem Beweis von P einen Beweis von Q zuordnet
  - $p: \neg P$ — $p : P \to \bot$
  - $p: \bot$ — niemals

- In dieser Interpretation entsprechen sich Formeln und Typen:

  - $P \to Q \approx [P \to Q]$
  - $P \wedge Q \approx P \times Q$
  - $P \vee Q \approx P + Q$
  - $\bot \approx \emptyset$