Formale Systeme

Prof. Dr. Bernhard Beckert

Fakultät für Informatik
Universität Karlsruhe (TH)

Winter 2008/2009

Kalküle für die Aussagenlogik
Übersicht

1. Hilbert-Kalkül
2. Resolutionskalkül
3. Tableaukalkül
4. Sequenzenkalkül

Beispiel einer Beweisregel

Die Regel mit Schemavariablen α,β,γ

$$\frac{\alpha \vee \beta, \beta \rightarrow \gamma, \gamma \rightarrow \alpha}{\alpha}$$

Eine Instanz mit

$$\begin{array}{rcl} \alpha & = & \neg P_1 \\ \beta & = & \mathbf{0} \\ \gamma & = & P_1 \wedge P_2 \end{array}$$

$$\frac{\neg P_1 \vee \mathbf{0}, \mathbf{0} \rightarrow (P_1 \wedge P_2), (P_1 \wedge P_2) \rightarrow \neg P_1}{\neg P_1}$$

Beweisregeln, abstrakt

Definition

Für ein $n \in \mathbb{N}$ ist eine *n-stellige Regel* R eine entscheidbare, $n+1$-stellige Relation über der Menge der Formeln.
Ist $(u_1, \ldots, u_n, u_{n+1}) \in R$, so heißen

- $(u_1, \ldots, u_n, u_{n+1})$ eine *Instanz* von R
- $u_1, \ldots, u_n$ die *Prämissen* dieser Instanz
- u_{n+1} die *Conclusio* dieser Instanz.

Wir schreiben meist

$$\frac{u_1, \ldots, u_n}{u_{n+1}}$$

Die Instanzen von nullstelligen Regeln heissen auch *Axiome*.

Ableitungen, abstrakt

Sei eine Formelmenge L, eine Menge M von Voraussetzungen und eine Menge von Regeln festgelegt.

Definition

Eine *Ableitung* aus M ist eine Folge $(u_1, \ldots, u_m)$ von Formeln in L, so dass für jedes $i \in \{1, \ldots, m\}$ gilt:

- u_i ist Axiom; oder
- $u_i \in M$; oder
- es gibt eine Instanz

$$\frac{u_{j_1}, \ldots, u_{j_n}}{u_i}$$

  einer Regel mit $j_1, \ldots, j_n < i$

Man beachte, dass u_1 ein Axiom oder ein Element von M sein muss.

Ableitbarkeit, abstrakt

Eine Formel A heisst *ableitbar* aus M, kurz

$$M \vdash A$$

genau dann, wenn es eine Ableitung $(u_1, \ldots, u_m)$ gibt mit $u_m = A$.

- Für $\emptyset \vdash u$ schreiben wir $\vdash u$, für $\{v\} \vdash u$ schreiben wir $v \vdash u$.
- Falls erforderlich wird der Kalkül in der Notation mit angezeigt, also $M \vdash_{Kal} u$.

David Hilbert

Wesentlicher Begründer der axiomatischen Logik

David Hilbert $\star$ *1862,* † *1943*

- Einer der bedeutensten und einflußreichsten Mathematiker aller Zeiten
- Professor in Königsberg und Göttingen
- Wichtige Beiträge zu
  - Logik
  - Funktionalanalysis
  - Zahlentheorie
  - Mathematische Grundlagen der Physik
  - uvm.

Die Regeln des Hilbertkalküls

Definition

Ax1: $$\frac{}{\alpha \to (\beta \to \alpha)}$$

Ax2: $$\frac{}{(\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma))}$$

Ax3: $$\frac{}{(\neg\alpha \to \neg\beta) \to (\beta \to \alpha)}$$

Mp: $$\frac{\alpha, \alpha \to \beta}{\beta}$$ (Modus ponens)

Eine Ableitung für $\vdash_{\mathbf{H0}} A \rightarrow A$

$$
\begin{array}{lll}
1. & (\underbrace{A}_{\alpha} \rightarrow ((\underbrace{A \rightarrow A}_{\beta}) \rightarrow \underbrace{A}_{\gamma})) \rightarrow & \\
 & ((\underbrace{A}_{\alpha} \rightarrow (\underbrace{A \rightarrow A}_{\beta})) \rightarrow (\underbrace{A}_{\alpha} \rightarrow \underbrace{A}_{\gamma})) & \text{Ax2} \\
2. & A \rightarrow ((A \rightarrow A) \rightarrow A) & \text{Ax1} \\
3. & (A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A) & \text{Mp auf (2),(1)} \\
4. & A \rightarrow (A \rightarrow A) & \text{Ax1} \\
5. & A \rightarrow A & \text{Mp auf (3),(4)}
\end{array}
$$

Deduktionstheorem

Theorem (Deduktionstheorem der Aussagenlogik)

Für beliebige Formelmengen M und Formeln A, B gilt:

$$M \vdash_{\mathbf{H0}} A \to B \quad \Leftrightarrow \quad M \cup \{A\} \vdash_{\mathbf{H0}} B$$

Proof.

$\Rightarrow$

Es gelte	M	$\vdash$	$A \to B$.	Dann
	$M \cup \{A\}$	$\vdash$	$A \to B$.	(erst recht)
	$M \cup \{A\}$	$\vdash$	A	(trivialerweise)
	$M \cup \{A\}$	$\vdash$	B	(Mp)

$\square$

Deduktionstheorem (Forts.)

Proof.

$\Leftarrow$

Es gelte: $M \cup \{A\} \vdash B$.
Sei $(A_1, \ldots, A_m)$ Ableitung von B aus $M \cup \{A\}$.
Ziel: $M \vdash A \rightarrow B$, d. h. $M \vdash A \rightarrow A_m$.
Wir zeigen für alle $i \in \{1, \ldots, m\}$:

$$M \vdash A \rightarrow A_i$$

durch Induktion über i.
Sei i mit $1 \leq i \leq m$ gegeben.
Nehmen wir also an, dass für alle $j < i$ schon gezeigt ist: $M \vdash A \rightarrow A_j$. $\square$

Deduktionstheorem (2. Forts.)

1.Fall:	$A_i \in M \cup$ Ax1 $\cup$ Ax2 $\cup$ Ax3.	Dann gilt:
	$M \vdash A_i$	(trivial)
	$M \vdash A_i \rightarrow (A \rightarrow A_i)$	(Ax1)
	$M \vdash A \rightarrow A_i$	(Mp)

2.Fall: $A_i = A$.

Wir haben $M \vdash A \rightarrow A$ schon gezeigt.

Deduktionstheorem (3. Forts.)

Proof.

$\Leftarrow$

3.Fall: Es gibt $j < i$ und $k < i$ mit $A_k = A_j \rightarrow A_i$.

Nach obiger Annahme (Induktionsvoraussetzung) wissen wir:

$M \vdash A \rightarrow A_j$
$M \vdash A \rightarrow (A_j \rightarrow A_i)$

Man hat ferner

$$M \vdash (A \rightarrow (A_j \rightarrow A_i)) \rightarrow (A \rightarrow A_j) \rightarrow (A \rightarrow A_i)) \qquad \text{(Ax2)}$$

also

$$M \vdash A \rightarrow A_i \qquad \text{(2mal Mp).}$$

□

Beispiel einer Ableitung mit Deduktionstheorem

$$
\begin{array}{lcll}
\{A \to B, B \to C, A\} & \vdash & A & \text{(triv.)} \\
\{A \to B, B \to C, A\} & \vdash & A \to B & \text{(triv.)} \\
\{A \to B, B \to C, A\} & \vdash & B & \text{(MP)} \\
\{A \to B, B \to C, A\} & \vdash & B \to C & \text{(triv.)} \\
\{A \to B, B \to C, A\} & \vdash & C & \text{(MP)} \\
\{A \to B, B \to C\} & \vdash & A \to C & \text{(DT)} \\
\{A \to B\} & \vdash & (B \to C) \to (A \to C) & \text{(DT)} \\
 & \vdash & (A \to B) \to ((B \to C) \to (A \to C)) & \text{(DT)}
\end{array}
$$

Metatheoreme zu H0

Theorem

Sei M eine Menge aussagenlogischer Formeln, A eine aussagenlogische Formel.

1. $M \vdash_{\mathbf{H0}} A \quad \Rightarrow \quad M \models A$ — *Korrektheit von H0*
2. $M \models A \Rightarrow M \vdash_{\mathbf{H0}} A.$ — *Vollständigkeit von H0*
3. *Aus* $M \models A$ *folgt schon* $E \models A$ *für eine endliche Teilmenge* E *von* M.