

Formale Systeme

Hilbert-Kalkül

Prof. Dr. Bernhard Beckert | WS 2009/2010

KIT – INSTITUT FÜR THEORETISCHE INFORMATIK



Kalküle für die Aussagenlogik

Übersicht

- 1 Hilbert-Kalkül
- 2 Resolutionskalkül
- 3 Tableauekalkül
- 4 Sequenzenkalkül

Die Regel mit Schemavariablen α, β, γ

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

Eine Instanz mit

$$\alpha = \neg P_1$$

$$\beta = \mathbf{0}$$

$$\gamma = P_1 \wedge P_2$$

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

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 $(u_1, \dots, u_n, u_{n+1}) \in R$, so heißen

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

Wir schreiben meist

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

Die Instanzen von nullstelligen Regeln heißen auch *Axiome*.

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

Definition

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

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

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

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

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

Eine Formel A heisst *ableitbar* aus M , kurz

$$M \vdash A$$

genau dann, wenn es eine Ableitung (u_1, \dots, 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 $M \vdash_{\text{Kal}} u$.

David Hilbert ✱ 1862, † 1943

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



Definition

$$\text{Ax1: } \frac{}{\alpha \rightarrow (\beta \rightarrow \alpha)}$$

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

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

$$\text{Mp: } \frac{\alpha, \alpha \rightarrow \beta}{\beta} \quad (\text{Modus ponens})$$

Eine Ableitung für

$$\vdash_{H0} A \rightarrow A$$

- 1 $(\underbrace{A}_{\alpha} \rightarrow ((\underbrace{A \rightarrow A}_{\beta}) \rightarrow \underbrace{A}_{\gamma})) \rightarrow$
 $((\underbrace{A}_{\alpha} \rightarrow (\underbrace{A \rightarrow A}_{\beta})) \rightarrow (\underbrace{A}_{\alpha} \rightarrow \underbrace{A}_{\gamma}))$ Ax2
- 2 $A \rightarrow ((A \rightarrow A) \rightarrow A)$ Ax1
- 3 $(A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A)$ Mp auf (2),(1)
- 4 $A \rightarrow (A \rightarrow A)$ Ax1
- 5 $A \rightarrow A$ Mp auf (3),(4)

Theorem (Deduktionstheorem der Aussagenlogik)

Für beliebige Formelmengen M und Formeln A, B gilt:

$$M \vdash_{\text{H0}} A \rightarrow B \quad \Leftrightarrow \quad M \cup \{A\} \vdash_{\text{H0}} B$$

Proof.

\Rightarrow

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

Proof.

←

Es gelte: $M \cup \{A\} \vdash B$.

Sei (A_1, \dots, 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 $i \in \{1, \dots, m\}$:

$$M \vdash A \rightarrow A_i$$

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:

$$M \vdash A \rightarrow A_j.$$



- 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.

Proof.

←

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

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

also

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

□

Beispiel einer Ableitung mit Deduktionstheorem

$\{A \rightarrow B, B \rightarrow C, A\}$	\vdash	A	(triv.)
$\{A \rightarrow B, B \rightarrow C, A\}$	\vdash	$A \rightarrow B$	(triv.)
$\{A \rightarrow B, B \rightarrow C, A\}$	\vdash	B	(MP)
$\{A \rightarrow B, B \rightarrow C, A\}$	\vdash	$B \rightarrow C$	(triv.)
$\{A \rightarrow B, B \rightarrow C, A\}$	\vdash	C	(MP)
$\{A \rightarrow B, B \rightarrow C\}$	\vdash	$A \rightarrow C$	(DT)
$\{A \rightarrow B\}$	\vdash	$(B \rightarrow C) \rightarrow (A \rightarrow C)$	(DT)
	\vdash	$(A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$	(DT)

Theorem

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

① $M \vdash_{H0} A \Rightarrow M \models A$

Korrektheit von H0

② $M \models A \Rightarrow M \vdash_{H0} A.$

Vollständigkeit von H0

③ *Aus $M \models A$ folgt schon $E \models A$
für eine endliche Teilmenge E von M .*