

Formale Systeme

Prof. Dr. Bernhard Beckert, WS 2015/2016

Hilbertkalkül

KIT – INSTITUT FÜR THEORETISCHE INFORMATIK

David Hilbert

Wesentlicher Begründer der axiomatischen Logik

David Hilbert ★ 1862, † 1943

- ▶ Einer der bedeutendsten und einflußreichsten Mathematiker aller Zeiten



David Hilbert

Wesentlicher Begründer der axiomatischen Logik

David Hilbert ★ 1862, † 1943

- ▶ Einer der bedeutendsten und einflußreichsten Mathematiker aller Zeiten
- ▶ Professor in Königsberg und Göttingen



David Hilbert

Wesentlicher Begründer der axiomatischen Logik

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.



Hilbertkalkül

Axiome und Regeln

Axiome sind Schemata!

x : Variable, t : Term, α, β, γ : Formeln

Zur Vereinfachung:

Beschränkung auf logische Operatoren $\neg, \rightarrow, \forall$

Hilbertkalkül

Axiome und Regeln

Axiome sind Schemata!

x : Variable, t : Term, α, β, γ : Formeln

Zur Vereinfachung:

Beschränkung auf logische Operatoren $\neg, \rightarrow, \forall$

Ax1: $\alpha \rightarrow (\beta \rightarrow \alpha)$ (Abschwächung)

Ax2: $(\alpha \rightarrow (\beta \rightarrow \gamma)) \rightarrow ((\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma))$ (Verteilung von $\rightarrow$)

Ax3: $(\neg\alpha \rightarrow \neg\beta) \rightarrow (\beta \rightarrow \alpha)$ (Kontraposition)

Ax4: $\forall x\alpha \rightarrow \{x/t\}(\alpha)$ $\{x/t\}$ kollisionsfrei für α (Instantiierung)

Ax5: $\forall x(\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \forall x\beta)$ $x \notin \text{Frei}(\alpha)$ ($\forall$ -Verschiebung)

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

Gen:
$$\frac{\alpha}{\forall x\alpha}$$
 (Generalisierung)

Hilbertkalkül

Axiome und Regeln

Axiome sind Schemata!

x : Variable, t : Term, α, β, γ : Formeln

Zur Vereinfachung:

Beschränkung auf logische Operatoren $\neg, \rightarrow, \forall$

Ax1: $\alpha \rightarrow (\beta \rightarrow \alpha)$ (Abschwächung)

Ax2: $(\alpha \rightarrow (\beta \rightarrow \gamma)) \rightarrow ((\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma))$ (Verteilung von $\rightarrow$)

Ax3: $(\neg\alpha \rightarrow \neg\beta) \rightarrow (\beta \rightarrow \alpha)$ (Kontraposition)

Ax4: $\forall x\alpha \rightarrow \{x/t\}(\alpha)$ $\{x/t\}$ kollisionsfrei für α (Instantiierung)

Ax5: $\forall x(\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \forall x\beta)$ $x \notin \text{Frei}(\alpha)$ ($\forall$ -Verschiebung)

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

Gen:
$$\frac{\alpha}{\forall x\alpha}$$
 (Generalisierung)

Ax1, Ax2, Ax3 + Mp bilden den aussagenlogische Hilbertkalkül

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

$$\begin{aligned} 1. & \left(\underbrace{A}_{\alpha} \rightarrow \left(\underbrace{(A \rightarrow A)}_{\beta} \rightarrow \underbrace{A}_{\gamma} \right) \right) \rightarrow \\ & \left(\left(\underbrace{A}_{\alpha} \rightarrow \underbrace{(A \rightarrow A)}_{\beta} \right) \rightarrow \left(\underbrace{A}_{\alpha} \rightarrow \underbrace{A}_{\gamma} \right) \right) \end{aligned}$$

Ax2

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

1.
$$\underbrace{A}_{\alpha} \rightarrow ((\underbrace{A \rightarrow A}_{\beta}) \rightarrow \underbrace{A}_{\gamma}) \rightarrow$$
$$((\underbrace{A}_{\alpha} \rightarrow \underbrace{A \rightarrow A}_{\beta})) \rightarrow (\underbrace{A}_{\alpha} \rightarrow \underbrace{A}_{\gamma}) \quad \text{Ax2}$$
2. $A \rightarrow ((A \rightarrow A) \rightarrow A) \quad \text{Ax1}$

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

1.
$$\underbrace{A}_{\alpha} \rightarrow ((\underbrace{A \rightarrow A}_{\beta}) \rightarrow \underbrace{A}_{\gamma}) \rightarrow$$
$$((\underbrace{A}_{\alpha} \rightarrow \underbrace{A \rightarrow A}_{\beta})) \rightarrow (\underbrace{A}_{\alpha} \rightarrow \underbrace{A}_{\gamma}) \quad \text{Ax2}$$
2. $A \rightarrow ((A \rightarrow A) \rightarrow A) \quad \text{Ax1}$
3. $(A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A) \quad \text{Mp auf (2),(1)}$

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

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

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

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

Theorem (Deduktionstheorem)

Sei M ein Formelmengen, A, B Formeln, wobei A keine freien Variablen enthält. Dann gilt:

$$M \vdash_{\mathbf{H}} A \rightarrow B \quad \Leftrightarrow \quad M \cup \{A\} \vdash_{\mathbf{H}} B$$

Theorem (Deduktionstheorem)

Sei M eine Formelmengen, A, B Formeln, wobei A keine freien Variablen enthält. Dann gilt:

$$M \vdash_H A \rightarrow B \quad \Leftrightarrow \quad M \cup \{A\} \vdash_H B$$

Proof.

$\Rightarrow$

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



Theorem (Deduktionstheorem)

Sei M eine Formelmengen, A, B Formeln, wobei A keine freien Variablen enthält. Dann gilt:

$$M \vdash_H A \rightarrow B \quad \Leftrightarrow \quad M \cup \{A\} \vdash_H B$$

Proof.

$\Rightarrow$

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

$\Leftarrow$ siehe Skriptum.



Beispiel einer Ableitung mit Deduktionstheorem

Zeige, dass

$$(A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$$

eine Tautologie ist.

Beispiel einer Ableitung mit Deduktionstheorem

Zeige, dass

$$(A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$$

eine Tautologie ist.

$$\{A \rightarrow B, B \rightarrow C, A\} \quad \vdash \quad A \quad \text{(triv.)}$$

Beispiel einer Ableitung mit Deduktionstheorem

Zeige, dass

$$(A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$$

eine Tautologie ist.

$$\begin{array}{lll} \{A \rightarrow B, B \rightarrow C, A\} & \vdash & A & \text{(triv.)} \\ \{A \rightarrow B, B \rightarrow C, A\} & \vdash & A \rightarrow B & \text{(triv.)} \end{array}$$

Beispiel einer Ableitung mit Deduktionstheorem

Zeige, dass

$$(A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$$

eine Tautologie ist.

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

Beispiel einer Ableitung mit Deduktionstheorem

Zeige, dass

$$(A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$$

eine Tautologie ist.

$\{A \rightarrow B, B \rightarrow C, A\}$	$\vdash$	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.)

Beispiel einer Ableitung mit Deduktionstheorem

Zeige, dass

$$(A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$$

eine Tautologie ist.

$\{A \rightarrow B, B \rightarrow C, A\}$	$\vdash$	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)

Beispiel einer Ableitung mit Deduktionstheorem

Zeige, dass

$$(A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$$

eine Tautologie ist.

$\{A \rightarrow B, B \rightarrow C, A\}$	$\vdash$	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)

Beispiel einer Ableitung mit Deduktionstheorem

Zeige, dass

$$(A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$$

eine Tautologie ist.

$\{A \rightarrow B, B \rightarrow C, A\}$	$\vdash$	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)

Beispiel einer Ableitung mit Deduktionstheorem

Zeige, dass

$$(A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$$

eine Tautologie ist.

$\{A \rightarrow B, B \rightarrow C, A\}$	$\vdash$	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)

Vollständigkeit der PL1

GÖDEL 1931

Theorem

Σ sei eine Signatur der PL1.

Dann ist **H** über Σ korrekt und vollständig:
für alle $M \subseteq \text{For}_\Sigma$, $A \in \text{For}_\Sigma$ gilt:

$$M \models A \iff M \vdash_{\mathbf{H}} A$$

Konsequenzen der Korrektheit und Vollständigkeit

Theorem (Kompaktheitsatz)

Für beliebige $M \subseteq \text{For}_\Sigma$, $A \in \text{For}_\Sigma$ gilt:

$$M \models A$$

$$\Leftrightarrow$$

$E \models A$ für eine endliche Teilmenge $E \subseteq M$.

Konsequenzen der Korrektheit und Vollständigkeit

Theorem (Kompaktheitsatz)

Für beliebige $M \subseteq \text{For}_\Sigma$, $A \in \text{For}_\Sigma$ gilt:

$$M \models A$$

$$\Leftrightarrow$$

$E \models A$ für eine endliche Teilmenge $E \subseteq M$.

Theorem (Endlichkeitssatz)

Eine Menge $M \subseteq \text{For}_\Sigma$ hat genau dann ein Modell, wenn jede endliche Teilmenge von M ein Modell hat.

Konsequenzen der Korrektheit und Vollständigkeit

Theorem (Kompaktheitsatz)

Für beliebige $M \subseteq \text{For}_\Sigma$, $A \in \text{For}_\Sigma$ gilt:

$$M \models A$$

$$\Leftrightarrow$$

$E \models A$ für eine endliche Teilmenge $E \subseteq M$.

Theorem (Endlichkeitssatz)

Eine Menge $M \subseteq \text{For}_\Sigma$ hat genau dann ein Modell, wenn jede endliche Teilmenge von M ein Modell hat.

Der Endlichkeitssatz ist der Spezialfall $A = 0$ des Kompaktheitssatzes.

Beweis des Kompaktheitsatzes

$$M \models A$$

$$M \models A$$

$$\Leftrightarrow M \vdash A \quad (\text{Korrektheit und Vollständigkeit})$$

$$M \models A$$

$$\Leftrightarrow M \vdash A \quad (\text{Korrektheit und Vollständigkeit})$$

$$\Leftrightarrow E \vdash A \quad \text{für ein endliches } E \subseteq M$$

Endlichkeit von Ableitungen

$$M \models A$$

$$\Leftrightarrow M \vdash A \quad (\text{Korrektheit und Vollständigkeit})$$

$$\Leftrightarrow E \vdash A \quad \text{für ein endliches } E \subseteq M$$

Endlichkeit von Ableitungen

$$\Leftrightarrow E \models A \quad \text{für ein endliches } E \subseteq M$$

Korrektheit u. Vollständigkeit