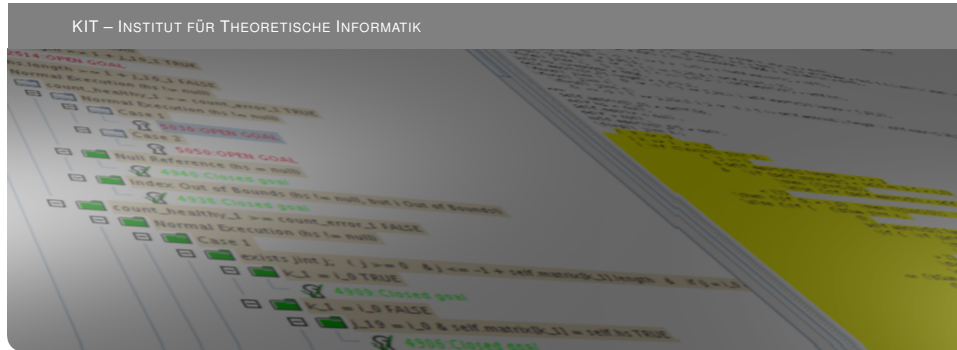


# Formale Systeme

Prof. Dr. Bernhard Beckert, WS 2014/2015

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,  $\alpha, \beta, \gamma$ : Formeln

Zur Vereinfachung:

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

# Hilbertkalkül

## Axiome und Regeln

Axiome sind Schemata!

$x$ : Variable,  $t$ : Term,  $\alpha, \beta, \gamma$ : 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  $\alpha$  (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,  $\alpha, \beta, \gamma$ : 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  $\alpha$  (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 $\vdash_{H0} A \rightarrow A$

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

Ax2

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

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

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

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

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

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

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

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

## Theorem (Deduktionstheorem)

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

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

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

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

## 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.

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

# Beispiel einer Ableitung mit Deduktionstheorem

Zeige, dass

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

eine Tautologie ist.

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

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

# 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)

# 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

$\Sigma$  sei eine Signatur der PL1.

Dann ist  $\mathbf{H}$  über  $\Sigma$  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  $A = \mathbf{0}$  des Kompaktheitssatzes.

# Beweis des Kompaktheitsatzes

$$M \models A$$

# Beweis des Kompaktheitsatzes

$$M \models A$$

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

$$M \models A$$

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

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

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