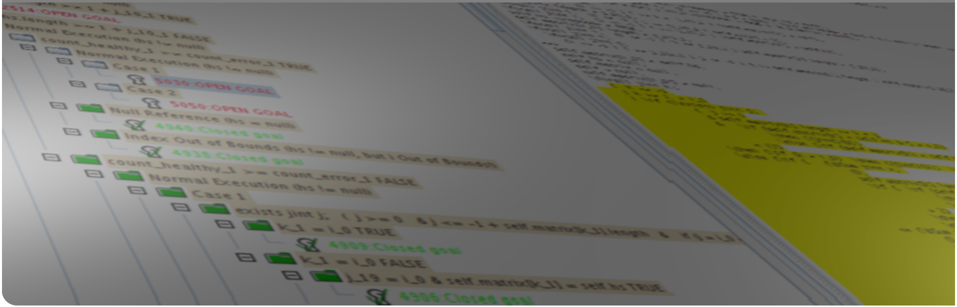
Karlsruhe Institute of Technology

Formale Systeme

Prof. Dr. Bernhard Beckert, WS 2018/2019

Hilbertkalkül

KIT – INSTITUT FÜR THEORETISCHE INFORMATIK



David Hilbert

Wesentlicher Begründer der axiomatischen Logik

David Hilbert $\star$1862, $\dagger$1943

- Einer der bedeutensten und einflußreichsten Mathematiker aller Zeiten

David Hilbert

Wesentlicher Begründer der axiomatischen Logik

David Hilbert $\star$1862, $\dagger$1943

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

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.

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:	$\forall x(\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \forall x \beta)$ $x \notin \mathit{Frei}(\alpha)$	($\forall$-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 $\neg, \to, \forall$

Ax1:	$\alpha \to (\beta \to \alpha)$		(Abschwächung)
Ax2:	$(\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma))$		(Verteilung von $\to$)
Ax3:	$(\neg\alpha \to \neg\beta) \to (\beta \to \alpha)$		(Kontraposition)
Ax4:	$\forall x \alpha \to \{x/t\}(\alpha)$	$\{x/t\}$ kollisionsfrei für α	(Instantiierung)
Ax5:	$\forall x(\alpha \to \beta) \to (\alpha \to \forall x \beta)$	$x \notin Frei(\alpha)$	($\forall$-Verschiebung)

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

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

Ax1, Ax2, Ax3 + Mp bilden den aussagenlogische Hilbertkalkül

Eine Ableitung $\vdash_{\mathbf{H0}} A \to A$

1. $(\underbrace{A}_{\alpha} \to ((\underbrace{A \to A}_{\beta}) \to \underbrace{A}_{\gamma})) \to$
$((\underbrace{A}_{\alpha} \to (\underbrace{A \to A}_{\beta})) \to (\underbrace{A}_{\alpha} \to \underbrace{A}_{\gamma}))$ Ax2

Eine Ableitung $\vdash_{\mathbf{H}0} A \to A$

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

Eine Ableitung $\vdash_{\mathbf{H0}} A \to A$

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

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

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

Eine Ableitung $\vdash_{\mathbf{H0}} A \to A$

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

Deduktionstheorem

Theorem (Deduktionstheorem)

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

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

Deduktionstheorem

Theorem (Deduktionstheorem)

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

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

Proof.

$\Rightarrow$

$$\begin{array}{lrcll}
\text{Es gelte} & M & \vdash & A \to B. & \text{Dann} \\
 & M \cup \{A\} & \vdash & A \to B. & \text{(erst recht)} \\
 & M \cup \{A\} & \vdash & A & \text{(trivialerweise)} \\
 & M \cup \{A\} & \vdash & B & \text{(Mp)}
\end{array}$$

$\square$

Deduktionstheorem

Theorem (Deduktionstheorem)

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

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

Proof.

$\Rightarrow$

$$\begin{array}{lrcll}
\text{Es gelte} & M & \vdash & A \to B. & \text{Dann} \\
& M \cup \{A\} & \vdash & A \to B. & \text{(erst recht)} \\
& M \cup \{A\} & \vdash & A & \text{(trivialerweise)} \\
& M \cup \{A\} & \vdash & B & \text{(Mp)}
\end{array}$$

$\Leftarrow$ siehe Skriptum. $\square$

Beispiel einer Ableitung mit Deduktionstheorem

Zeige, dass

$$(A \to B) \to ((B \to C) \to (A \to C))$$

eine Tautologie ist.

Beispiel einer Ableitung mit Deduktionstheorem

Zeige, dass

$$(A \to B) \to ((B \to C) \to (A \to C))$$

eine Tautologie ist.

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

Beispiel einer Ableitung mit Deduktionstheorem

Zeige, dass

$$(A \to B) \to ((B \to C) \to (A \to C))$$

eine Tautologie ist.

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

Beispiel einer Ableitung mit Deduktionstheorem

Zeige, dass

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

eine Tautologie ist.

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

Beispiel einer Ableitung mit Deduktionstheorem

Zeige, dass

$$(A \to B) \to ((B \to C) \to (A \to C))$$

eine Tautologie ist.

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

Beispiel einer Ableitung mit Deduktionstheorem

Zeige, dass

$$(A \to B) \to ((B \to C) \to (A \to C))$$

eine Tautologie ist.

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

Beispiel einer Ableitung mit Deduktionstheorem

Zeige, dass

$$(A \to B) \to ((B \to C) \to (A \to C))$$

eine Tautologie ist.

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

Beispiel einer Ableitung mit Deduktionstheorem

Zeige, dass

$$(A \to B) \to ((B \to C) \to (A \to C))$$

eine Tautologie ist.

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

Beispiel einer Ableitung mit Deduktionstheorem

Zeige, dass

$$(A \to B) \to ((B \to C) \to (A \to C))$$

eine Tautologie ist.

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

Vollständigkeit der PL1
GÖDEL 1931

Theorem

Σ sei eine Signatur der PL1.

Dann ist **H** *über Σ korrekt und vollständig:*
für alle $M \subseteq For_\Sigma$, $A \in For_\Sigma$ gilt:

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

Konsequenzen der Korrektheit und Vollständigkeit

Theorem (Kompaktheitsatz)

Für beliebige $M \subseteq For_\Sigma$, $A \in For_\Sigma$ gilt:

$$M \models A$$
$$\Leftrightarrow$$
$$E \models A \textit{ für eine endliche Teilmenge } E \subseteq M.$$

Konsequenzen der Korrektheit und Vollständigkeit

Theorem (Kompaktheitsatz)

Für beliebige $M \subseteq For_\Sigma$, $A \in For_\Sigma$ gilt:

$$M \models A$$
$$\Leftrightarrow$$
$$E \models A \text{ für eine endliche Teilmenge } E \subseteq M.$$

Theorem (Endlichkeitssatz)

Eine Menge $M \subseteq For_\Sigma$ hat genau dann ein Modell, wenn jede endliche Teilmenge von M ein Modell hat.

Konsequenzen der Korrektheit und Vollständigkeit

Theorem (Kompaktheitsatz)

Für beliebige $M \subseteq For_\Sigma$, $A \in For_\Sigma$ gilt:

$$M \models A$$
$$\Leftrightarrow$$
$$E \models A \text{ für eine endliche Teilmenge } E \subseteq M.$$

Theorem (Endlichkeitssatz)

Eine Menge $M \subseteq For_\Sigma$ 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

$$
\begin{array}{llll}
 & M & \models & A \\
\Leftrightarrow & M & \vdash & A \quad \text{(Korrektheit und Vollständigkeit)}
\end{array}
$$

Beweis des Kompaktheitsatzes

$$
\begin{array}{rcccl}
 & M & \models & A & \\
\Leftrightarrow & M & \vdash & A & \text{(Korrektheit und Vollständigkeit)} \\
\Leftrightarrow & E & \vdash & A & \text{für ein endliches } E \subseteq M \\
 & & & & \text{Endlichkeit von Ableitungen}
\end{array}
$$

Beweis des Kompaktheitsatzes

$$\begin{array}{lllll} & M & \models & A & \\ \Leftrightarrow & M & \vdash & A & \text{(Korrektheit und Vollständigkeit)} \\ \Leftrightarrow & E & \vdash & A & \text{für ein endliches } E \subseteq M \\ & & & & \text{Endlichkeit von Ableitungen} \\ \Leftrightarrow & E & \models & A & \text{für ein endliches } E \subseteq M \\ & & & & \text{Korrektheit u. Vollständigkeit} \end{array}$$