

# Automatisierte Logik und Programmierung

## Teil I

### Formalisierung



# Automatisierte Logik und Programmierung

## Einheit 2



## Grundkonzepte formaler Kalküle



### 1. Syntax und Semantik

... am Beispiel der Prädikatenlogik

### 2. Konzeptionelle Betrachtungen

- Definitorische Erweiterung
- Objekt- und Metasprache
- Klassische vs. intuitionistische Mathematik
- Evidenzsemantik

### 3. Prinzipien formaler Beweisführung

## Simulation semantischer Schlußfolgerungen durch Regeln für symbolische Manipulation

- **Regelanwendung ohne Nachdenken**

- Umgeht Mehrdeutigkeiten der natürlichen Sprache
- Erlaubt schematische Lösung mathematischer Probleme

Beispiele: Differentialkalkül, Fourier-Transformationen,  
Computer Algebra, Formale Logik

- **Kernbestandteile:**

- Formale Sprache (Syntax + Semantik)
- Ableitungssystem (Axiome + Inferenzregeln)

- **Wichtige Eigenschaften logischer Kalküle**

- Korrekt, vollständig, automatisierbar
- Leicht verständlich, ausdrucksstark, ggf. konstruktiv

# KALKÜLE IN DIESER VERANSTALTUNG

- **Prädikatenlogik**

- Schlußfolgerungen aus der logischen Struktur einer Aussage

- **$\lambda$ -Kalkül**

- Schließen über das Resultat von Berechnungen

- **Einfache Typentheorie**

- Prinzipien des Schließens über Eigenschaften von Algorithmen

- **Konstruktive (intuitionistische) Typentheorie**

- Uniformer Kalkül für Logik, Berechnung und Programmeigenschaften
- Formalisiert Grundkonzepte von Mathematik und Programmierung
- Fundamentale Theorie: konstruktive Auslegung + direkte Semantik
- Implementiert im Nuprl System

- **Syntax:** Präzisierung des **Vokabulars**
  - Formale **Struktur** der Sprache (Notation, textliche Erscheinungsform)
  - Beschreibbar durch **mathematische Definitionsgleichungen** oder durch **formale Grammatiken**
- **Semantik:** Präzisierung der **Bedeutung** von Text
  - Interpretation syntaktisch korrekter Ausdrücke in informaler **Zielsprache**  
Beschreibbar durch **Interpretationsfunktion**: Quellsymbole  $\mapsto$  Zielobjekte  
*... aber was ist die Bedeutung der Zielsprache?*
  - **Direkte Semantik** für Grundagentheorien (**Mengentheorie**, **Typentheorie**)  
Mathematische Präzisierung der intuitiven Bedeutung

# FORMALISIERUNG UMGANGSSPRACHLICHER AUSSAGEN

*Studenten, die im Hauptstudium mindestens 120 Leistungspunkte erreichen, haben die Diplomhauptprüfung bestanden*

## Mögliche Formalisierungen

- DPO-14.3 *ohne Struktur*
- 120-Leistungspunkte  $\Rightarrow$  Diplom-bestanden *Aussagenlogik*
- $\forall \text{student. Leistungspunkte-erreicht}(\text{student}, 120)$   
 $\Rightarrow \text{Diplom-bestanden}(\text{student})$  *zu viel Text*
- $\forall s. (lp(s) > 120) \Rightarrow D(s)$  *typisch Prädikatenlogik*
- $\forall s : \text{Student. } (lp(s) > 120) \Rightarrow D(s)$  *Prädikatenlogik mit Sorten*

# ANFORDERUNGEN AN EINE FORMALISIERUNGSSPRACHE

- Kurz, prägnant, **maschinenlesbar**
- **Frei wählbare Symbole** für Prädikate, Operatoren, Platzhalter für Objekte
- Fest definierte Symbole für logische Bezüge (**Konnektive, Quantoren**)
- Eventuell fest definierte Symbole für wichtige Standardkonzepte (**Gleichheit, ...**)
- Eventuell Klassifizierung von Bereichen bzw. (**Daten-)**typen in Quantoren

# SYNTAX DER PRÄDIKATENLOGIK MIT SORTEN UND GLEICHHEIT

## ● (Abzählbare) **Alphabete** für erlaubte Symbole

- $\mathcal{V}$ : Variablensymbole  $x, y, z, \dots$
- $\mathcal{F}^i$ :  $i$ -stellige Funktionssymbole,  $\mathcal{F} = \bigcup_{i=0}^{\infty} \mathcal{F}^i$   $f, g, h, \dots, a, b, c, \dots$
- $\mathcal{P}^i$ :  $i$ -stellige Prädikatssymbole,  $\mathcal{P} = \bigcup_{i=0}^{\infty} \mathcal{P}^i$   $P, Q, R, \dots$
- $\mathcal{T}$ : Bereichssymbole (Typen / Sorten)  $S, T, \dots$

## ● **Terme**: Formalisierung mathematischer **Objekte**

- Variablen  $x \in \mathcal{V}$ , Konstante  $f \in \mathcal{F}^0$  (atomare Terme)
- $f(t_1, \dots, t_n)$ , wobei  $t_1, \dots, t_n$  Terme,  $f \in \mathcal{F}^n$

## ● **Formeln**: Formalisierung mathematischer **Aussagen**

- Konstante **ff**, Aussagenvariable  $P \in \mathcal{P}^0$  (atomare Formeln)
- $t_1 = t_2$ ,  $P(t_1, \dots, t_n)$ , wobei  $t_1, t_2, \dots, t_n$  Terme,  $P \in \mathcal{P}^n$
- $\neg A$ ,  $A \wedge B$ ,  $A \vee B$ ,  $A \Rightarrow B$ ,  $\forall x:T. A$ ,  $\exists x:T. A$ ,  $(A)$   
wobei  $A, B$  Formeln,  $x \in \mathcal{V}$ ,  $T \in \mathcal{T}$



# BEISPIELE FÜR TERME UND FORMELN

## ● Korrekte Terme

- $x$   $x \in \mathcal{V}$
- $24$   $24 \in \mathcal{F}^0$
- $\text{vater}(\text{peter})$   $\text{peter} \in \mathcal{V}, \text{vater} \in \mathcal{F}^1$
- $\text{max}(2,3,4), \text{max}(\text{plus}(4,\text{plus}(5,5)),23,5)$

Kontext bestimmt Rolle von Symbolen

## ● Korrekte Formeln

- $(4=\text{plus}(2,3)) \Rightarrow \text{ff}$
- $\text{Sein} \vee \neg \text{Sein}, \text{lange\_währt} \Rightarrow \text{endlich\_gut}$
- $\forall x:\mathbb{N}. \exists y:\mathbb{Z}. \leq(* (y,y), x) \wedge <(x, *( \text{plus}(y,1), \text{plus}(y,1)))$

## ● Keine Formeln

- $\text{plus}(\text{plus}(2,3),4)$  Term
- $\wedge \text{so\_weiter}$  Formel links von  $\wedge$  fehlt
- $\forall x:\mathbb{N}. x(4)=x$  Variable als Funktionszeichen
- $\forall f:F. f(4)=0$  Quantifizierung über Funktionszeichen (higher-order)
- $\forall x. x=x$  Typsymbol fehlt (unsortierte Prädikatenlogik)

## KONVENTIONEN SPAREN KLAMMERN

$\exists y:\mathbb{N}. \text{gerade}(y) \wedge \geq(y,2) \Rightarrow y=2 \wedge >(y,20)$  heißt?

- $\exists y:\mathbb{N}. (\text{gerade}(y) \wedge \geq(y,2)) \Rightarrow (y=2 \wedge >(y,20))$  ??
- $\exists y:\mathbb{N}. \text{gerade}(y) \wedge (\geq(y,2) \Rightarrow (y=2 \wedge >(y,20)))$  ??
- $\exists y:\mathbb{N}. (\text{gerade}(y) \wedge (\geq(y,2) \Rightarrow y=2)) \wedge >(y,20)$  ??

### ● Prioritäten zwischen verschiedenen Konnektiven

- $\neg$  bindet stärker als  $\wedge$ , dann folgt  $\vee$ , dann  $\Rightarrow$ , dann  $\exists$ , dann  $\forall$ .

$A \wedge \neg B$  entspricht  $A \wedge (\neg B)$

$A \wedge B \vee C$  entspricht  $(A \wedge B) \vee C$

$\exists x:T. A \wedge B$  entspricht  $\exists x:T. (A \wedge B)$

Achtung: Unterschiedliche Konventionen in verschiedenen Lehrbüchern

### ● Rechtsassoziativität bei Iteration von $\wedge$ , $\vee$ , $\Rightarrow$

- $A \Rightarrow B \Rightarrow C$  entspricht  $A \Rightarrow (B \Rightarrow C)$

### ● Keine Klammern bei Funktions-/Prädikatssymbolen

- $Px$  entspricht  $P(x)$  und  $fxy$  entspricht  $f(x,y)$

- **Konservative Erweiterung der Objektsprache**

- Neues Konstrukte sind **definitorische Abkürzung** für existierende objektsprachliche Ausdrücke (ggf. mit Parametern)
- Beispiel: **Äquivalenz** in der Prädikatenlogik

$$A \Leftrightarrow B \equiv (A \Rightarrow B) \wedge (B \Rightarrow A)$$

- Bedeutung wird auf Semantik bestehender Konstrukte abgestützt

- **Erlaubt kleinen Grundformalismus**

- Einfache Syntax und Semantik
- Einfaches Inferenzsystem
- Eigenschaften leicht beweisbar

- **Erhöht Flexibilität des Formalismus**

- Ergibt **umfangreiche formale Sprache**
- Erlaubt **freiere Syntax**

## Präsentation von Kalkülen hat zwei Sprachebenen

### ● Objektsprache:

- Sprache des Kalküls, in dem formalisiert wird
- Formale Sprache mit präzise definierter Syntax
- Beispiel:  $(\exists x:T. P_1(x) \vee P_2(x)) \Rightarrow \neg(\forall x:T. \neg P_1(x) \wedge \neg P_2(x))$

### ● Metasprache:

- Sprache, um Aussagen über den Kalkül zu machen
  - Beschreibung von Syntax, Semantik, Eigenschaften des Kalküls
- Natürliche, oft stark schematisierte Sprache
- Enthält Objektsprache, angereichert um syntaktische Metavariablen
- Beispiel: *aus*  $(\exists x:T. A \vee B)$  *folgt*  $\neg(\forall x:T. \neg A \wedge \neg B)$

### ● Unterscheidung zuweilen durch Fonts / Farben

- Ansonsten aus Kontext eindeutig erkennbar

# SEMANTIK DER PRÄDIKATENLOGIK (I)

## INTERPRETATION IN DER MENGENTHEORIE

- **Interpretation  $\mathcal{I}$ :**

- Universum  $\mathcal{U}$  + Interpretationsfunktion  $\iota$

- **Freie Wahl von  $\iota$  auf elementaren Symbolen**

- $\iota(x)$  Objekt aus  $\mathcal{U}$   $(x \in \mathcal{V})$
- $\iota(f)$   $n$ -stellige Funktion  $\phi : \mathcal{U}^n \rightarrow \mathcal{U}$   $(f \in \mathcal{F}^n)$
- $\iota(T)$  Teilmenge von  $\mathcal{U}$   $(T \in \mathcal{T})$
- $\iota(P)$  Funktion  $\Pi : \mathcal{U}^n \rightarrow \{\text{wahr, falsch}\}$   $(P \in \mathcal{P}^n)$

- **Homomorphe Fortsetzung auf Terme und Formeln**

- $\iota(f(t_1, \dots, t_n)) = \iota(f)(\iota(t_1), \dots, \iota(t_n))$
- $\iota(\text{ff}) = \text{falsch}$
- $\iota(t_1 = t_2) = \text{wahr, falls } \iota(t_1) \text{ und } \iota(t_2) \text{ in } \mathcal{U} \text{ gleich (sonst falsch)}$
- $\iota(P(t_1, \dots, t_n)) = \iota(P)(\iota(t_1), \dots, \iota(t_n))$ .
- $\iota((A)) = \iota(A)$

# SEMANTIK DER PRÄDIKATENLOGIK (II)

## FORTSETZUNG VON $\iota$ AUF ZUSAMMENGESETZTE FORMELN

$$\iota(\neg A) = \begin{cases} \text{wahr} & \text{falls } \iota(A) = \text{falsch} \\ \text{falsch} & \text{sonst} \end{cases}$$

$$\iota(A \wedge B) = \begin{cases} \text{wahr} & \text{falls } \iota(A) = \text{wahr} \text{ und } \iota(B) = \text{wahr} \\ \text{falsch} & \text{sonst} \end{cases}$$

$$\iota(A \vee B) = \begin{cases} \text{wahr} & \text{falls } \iota(A) = \text{wahr} \text{ oder } \iota(B) = \text{wahr} \\ \text{falsch} & \text{sonst} \end{cases}$$

$$\iota(A \Rightarrow B) = \begin{cases} \text{wahr} & \text{falls aus } \iota(A) = \text{wahr} \text{ immer } \iota(B) = \text{wahr} \text{ folgt} \\ \text{falsch} & \text{sonst} \end{cases}$$

$$\iota(\forall x:T.A) = \begin{cases} \text{wahr} & \text{falls } \iota_x^u(A) = \text{wahr} \text{ für alle } u \in \iota(T) \\ \text{falsch} & \text{sonst} \end{cases}$$

$\iota_x^u(x) = u, \text{ sonst } \iota_x^u = \iota$

$$\iota(\exists x:T.A) = \begin{cases} \text{wahr} & \text{falls } \iota_x^u(A) = \text{wahr} \text{ für ein } u \in \iota(T) \\ \text{falsch} & \text{sonst} \end{cases}$$

# SEMANTIK DER PRÄDIKATENLOGIK (II) – KLASSISCH

## FORTSETZUNG VON $\iota$ AUF ZUSAMMENGESETZTE FORMELN

$$\iota(\neg A) = \begin{cases} \text{wahr} & \text{falls } \iota(A) = \text{falsch} \\ \text{falsch} & \text{sonst} \end{cases}$$

$$\iota(A \wedge B) = \begin{cases} \text{wahr} & \text{falls } \iota(A) = \text{wahr} \text{ und } \iota(B) = \text{wahr} \\ \text{falsch} & \text{sonst} \end{cases}$$

$$\iota(A \vee B) = \begin{cases} \text{falsch} & \text{falls } \iota(A) = \text{falsch} \text{ und } \iota(B) = \text{falsch} \\ \text{wahr} & \text{sonst} \end{cases}$$

$$\iota(A \Rightarrow B) = \begin{cases} \text{falsch} & \text{falls } \iota(A) = \text{wahr} \text{ und } \iota(B) = \text{falsch} \\ \text{wahr} & \text{sonst} \end{cases}$$

$$\iota(\forall x:T.A) = \begin{cases} \text{wahr} & \text{falls } \iota_x^u(A) = \text{wahr} \text{ für alle } u \in \iota(T) \\ \text{falsch} & \text{sonst} \end{cases}$$

$\iota_x^u(x) = u, \text{ sonst } \iota_x^u = \iota$

$$\iota(\exists x:T.A) = \begin{cases} \text{falsch} & \text{falls } \iota_x^u(A) = \text{falsch} \text{ für alle } u \in \iota(T) \\ \text{wahr} & \text{sonst} \end{cases}$$

Ist das wirklich dasselbe?

# INTUITIONISTISCHE VS. KLASSISCHE MATHEMATIK

- Was genau heißt **oder**, **wann immer**, **es gibt**?
  - Gilt  $A \vee B$ , wenn man angeben kann, welches von beiden wahr ist?
  - Gilt  $A \Rightarrow B$ , wenn man zeigen kann, wie  $B$  aus  $A$  folgt?
  - Gilt  $\exists x. A$ , wenn man ein  $x$  angeben kann, für das  $A$  wahr ist?
- Gesetz vom ausgeschlossenen Dritten:  $A \vee \neg A$ 
  - Heißt “Eine Aussage ist wahr oder ihr Gegenteil ist wahr”
  - Grundannahme der “klassischen” Mathematik – aber unbeweisbar
  - Nicht identisch mit: “Eine Aussage ist wahr oder falsch”
- **Intuitionistische** (konstruktive) Mathematik
  - Versteht alle mathematischen Aussagen konstruktiv
  - Ist für Schließen über Algorithmen naheliegender
  - Gesetz vom ausgeschlossenen Dritten wird Entscheidbarkeitsaussage
  - Formaler Unterschied gering aber Beweise werden z.T. komplizierter



# NICHTKONSTRUKTIVE MATHEMATISCHE GESETZE

- $\neg\neg A \Rightarrow A$ 
  - Wenn das Gegenteil falsch ist, dann muß eine Aussage nicht wahr sein
  - Der Widerspruchsbeweis sagt nicht, warum die Aussage wahr sein soll
  - Äquivalent zu  $A \vee \neg A$
- $A \Rightarrow B \Rightarrow \neg A \vee B$ 
  - Wenn wir wissen warum eine Aussage aus einer anderen folgt, dann wissen wir noch nicht ob die erste falsch oder die zweite wahr ist
- $\neg(\neg A \wedge \neg B) \Rightarrow A \vee B$ 
  - Wenn zwei Aussagen nicht gleichzeitig falsch sind, dann ist noch nicht klar, welche von beiden wahr ist.
- $\neg(\forall x:T. \neg P(x)) \Rightarrow \exists x:T. P(x)$ 
  - Wenn eine Aussage nicht für alle Elemente falsch ist, dann wissen wir noch nicht, für welches sie wahr ist

# INTERPRETATION VON FORMELN

Sei  $\iota$  die “Standardinterpretation” und  $\iota(\mathbf{x}) = \text{dreizehn}$

- $\iota(\leq(\max(2,3,4),7))$   
 $= \iota(\leq)(\iota(\max(2,3,4)),\iota(7))$   
 $= \Pi_{\leq}(\iota(\max)(\iota(2),\iota(3),\iota(4)), \text{sieben}))$   
 $= \Pi_{\leq}(\phi_{\max}(\text{zwei},\text{drei},\text{vier}), \text{sieben}))$   
 $= \Pi_{\leq}(\text{vier}, \text{sieben}))$   
 $= \text{wahr}$
- $\iota(\exists \mathbf{x}:\mathbb{N}. \leq(\max(2,3,4),\mathbf{x}))$   
 $= \text{wahr}$  gdw.  $\iota_x^u(\leq(\max(2,3,4),\mathbf{x})) = \text{wahr}$  für ein  $u \in \iota(\mathbb{N})$  ist  
 $= :$   
 $= \text{wahr}$  gdw.  $\Pi_{\leq}(\text{vier},\iota_x^u(\mathbf{x})) = \text{wahr}$  für eine Zahl  $u$   
 $= \text{wahr}$  gdw.  $\Pi_{\leq}(\text{vier},u) = \text{wahr}$  für eine Zahl  $u$   
 $= \text{wahr}$  (wähle  $u = \text{fünf}$ )

# MODELLE UND GÜLTIGKEIT

- **Modell  $\mathcal{M}$  von  $A$**   **$(\mathcal{M} \models A)$** 
  - Interpretation  $\mathcal{M} = (\iota, \mathcal{U})$  mit  $\iota(A) = \text{wahr}$
- **$A$  gültig** jede Interpretation ist ein Modell für  $A$
- **$A$  erfüllbar** es gibt ein Modell für  $A$
- **$A$  widerlegbar** es gibt ein Modell für  $\neg A$
- **$A$  widersprüchlich** es gibt kein Modell für  $A$
- **$A$  folgt logisch aus Formelmenge  $\mathcal{E}$**   **$(\mathcal{E} \models A)$** 
  - Aus  $\mathcal{I} \models E$  für alle  $E \in \mathcal{E}$  folgt  $\mathcal{I} \models A$  (semantisch gültiger Schluß)
- **Theorie  $\mathcal{T}$** 
  - Erfüllbare Formelmenge mit allen Formeln, die daraus logisch folgen

# GÜLTIGKEIT VON FORMELN

$$(\leq(4, +(3, 1))) \Rightarrow \leq(+(3, 1), 4)) \Rightarrow \leq(+(3, 1), 4)$$

erfüllbar, nicht gültig

$$\leq(4, +(3, 1)) \wedge \neg \leq(4, +(3, 1))$$

unerfüllbar

$$(\leq(4, +(3, 1)) \wedge \leq(+(3, 1), 4)) \Rightarrow \leq(+(3, 1), 4) \quad \text{gültig}$$

$$\forall x:\mathbb{N}. x < 0$$

erfüllbar, nicht gültig

$$\exists x:\mathbb{N}. x > 0$$

erfüllbar, nicht gültig

$$\neg(\exists x:\mathbb{N}. x > 0)$$

erfüllbar, nicht gültig

**Symbole  $\leq$ ,  $+$ ,  $3$ ,  $4$ ,  $1$ ,  $\mathbb{N}$ ,  $>$  haben keine feste Bedeutung**

## EINE ALTERNATIVE FORM, SEMANTIK ZU DEFINIEREN

- **Interpretation in Zielsprache ist unintuitiv**
  - Bedeutung der Zielsprache muß präzisiert werden
  - Für grundlegende Objektsprachen sollte man dies besser direkt tun
- **Mengentheorie ist keine konstruktive Zielsprache**
  - Objekte haben keine Standardrepräsentation
  - Operationen auf Struktur von Objekten sind nicht beschreibbar
- **Direkte Semantik präzisiert Intuition**
  - **Urteile** weisen Basiskonzepten intuitiv verständliche Bedeutung zu
    - Explizite Urteile erklären Bedeutung atomarer Konstrukte
    - Homomorphe Fortsetzung auf komplexe Konstrukte
  - Beschreibung verbal oder in formaler Metasprache
    - Formale Semantik erleichtert Entwicklung von Inferenzregeln  
ist aber selbst kein Beweissystem

# BEISPIEL: EVIDENZSEMANTIK FÜR PRÄDIKATENLOGIK

## Welche Evidenz gibt es für Gültigkeit von Formeln?

- **Atomare Formeln sind intuitiv gültig oder widersprüchlich**
  - Gebe **explizite Evidenz** für Gültigkeit von  $4 = +(1,3), \dots$
  - Gebe **explizite Evidenz** für Widersprüchlichkeit von  $0=1, \dots$
  - Unbeweisbare oder uninterpretierte Formeln sind **ohne Evidenz**
- **Evidenz für komplexe Formeln wird konstruktiv aufgebaut**
  - $e$  Evidenz für Widersprüchlichkeit von  $A \mapsto e$  Evidenz für  $\neg A$
  - $e_a, e_b$  Evidenzen für  $A$  bzw.  $B \mapsto (e_a, e_b)$  Evidenz für  $A \wedge B$
  - $e_a$  Evidenz für  $A \mapsto \text{inl}(e_a)$  Evidenz für  $A \vee B$
  - $e_b$  Evidenz für  $B \mapsto \text{inr}(e_b)$  Evidenz für  $A \vee B$
  - $e_b$  Evidenz für  $B$  wenn  $e_a$  Evidenz für  $A \mapsto \lambda e_a. e_b$  Evidenz für  $A \Rightarrow B$
  - $e_a[a]$  Evidenz für  $A[a] \mapsto (a, e_a[a])$  Evidenz für  $\exists x:T. A$
  - $e_a[a]$  Evidenz für  $A[a]$  für alle  $a$  in  $T \mapsto \lambda a. e_a[a]$  Evidenz für  $\forall x:T. A$

**Aufwendiger, aber präziser als modelltheoretische Semantik**

- **Erlaubte Symbole**

- $+$ ,  $-$ ,  $*$ ,  $/$ ,  $0$ ,  $1$ ,  $2$ ,  $3$ , ... sowie  $\mathbb{Z}$ ,  $\in$ , Variablen und logische Konnektive

- **Terme:**

- Variablen  $x$  oder Konstanten  $0$ ,  $1$ ,  $2$ ,  $3$ , ...
- Funktionsanwendungen  $-t$ ,  $t_1+t_2$ ,  $t_1-t_2$ ,  $t_1*t_2$ ,  $t_1/t_2$

- **Formeln:**

- atomare Formel:  $t \in \mathbb{Z}$
- zusammengesetzte Formeln wie in der Prädikatenlogik

- **Formale Urteile für atomare Formeln**

- $0 \in \mathbb{Z}$ ,  $1 \in \mathbb{Z}$ ,  $2 \in \mathbb{Z}$ , ...
- $-t \in \mathbb{Z}$  falls  $t \in \mathbb{Z}$
- $t_1+t_2 \in \mathbb{Z}$ ,  $t_1-t_2 \in \mathbb{Z}$ ,  $t_1*t_2 \in \mathbb{Z}$ ,  $t_1/t_2 \in \mathbb{Z}$  falls  $t_1 \in \mathbb{Z}$  und  $t_2 \in \mathbb{Z}$

- **Urteile für zusammengesetzte Formeln wie zuvor**

## Syntaktische Manipulation formaler Ausdrücke unter Berücksichtigung der Semantik

- **Konversion:** Umformung in semantisch äquivalente Ausdrücke

$$\begin{array}{lll} 4+5 & \rightarrow & 9 \\ A \wedge (A \vee B) & \rightarrow & A \\ d/dx(u + v) & \rightarrow & du/dx + dv/dx \end{array}$$

- Konversion ist **werterhaltende** Termersetzung

- **Inferenz:** Erzeugung logischer Konsequenzen einer Formelmenge

$$\text{aus } A \text{ und } A \Rightarrow B \text{ folgt } B: \quad \frac{A, A \Rightarrow B}{B}$$

- Inferenz erhält **Gültigkeit** von Aussagen aber erlaubt **Abschwächung**
- Inferenz ist vielseitiger für logisches Schließen



# GRUNDKONZEPTE VON (INFERENZ)KALKÜLEN

- **Regelschema**  $\frac{A_1, \dots, A_n}{C}$  : aus  $\underbrace{A_1 \text{ und } \dots A_n}_{\text{Prämissen}}$  folgt  $\underbrace{C}_{\text{Konklusion}}$ 
  - **Axiom**: Regel ohne Prämissen
  - $\Gamma \vdash_{rs} C$ : Konkrete Anwendung des Regelschemas  $rs$
- **Ableitung**
  - Folge von Formeln  $F_1, \dots, F_k$  wobei Formel  $F_i$  durch Anwendung eines Regelschemas auf einige der Formeln  $F_1, \dots, F_{i-1}$  entsteht
- **Theorem**
  - Formel, die sich durch Anwendung endlich vieler Regeln ableiten läßt
- **Wahrheit ist nicht dasselbe wie Beweisbarkeit**
  - **Korrektheit** eines Kalküls: alle Theoreme sind gültig  
... einer Regel: Gültigkeit der Konklusion folgt aus Gültigkeit der Prämissen
  - **Vollständigkeit**: alle gültigen Aussagen sind Theoreme
    - unmöglich für ausdrucksstarke Theorien (Arithmetik, Analysis, ...)

## Kalküle sind Hilfsmittel, keine Beweismethode

### ● Synthetisch

- Bottom-up Vorgehensweise
- Schlüsse von Axiomen zur Aussage
- Übliche Art, fertige Beweise zu präsentieren

$$\frac{\frac{\frac{[A \wedge B]}{B} \wedge -E \quad \frac{[A \wedge B]}{A} \wedge -E}{B \wedge A} \wedge -I}{(A \wedge B) \Rightarrow (B \wedge A)} \Rightarrow -I$$

### ● Analytisch

$$\begin{array}{l} \vdash A \wedge B \Rightarrow B \wedge A \quad \text{BY impI} \\ \quad \backslash \\ \quad A \wedge B \vdash B \wedge A \quad \text{BY andE 1} \\ \quad \quad \backslash \\ \quad \quad A, B \vdash B \wedge A \quad \text{BY andI} \\ \quad \quad \quad \backslash \\ \quad \quad \quad A, B \vdash B \quad \text{BY hypothesis 2} \\ \quad \quad \quad \quad \backslash \\ \quad \quad \quad \quad A, B \vdash A \quad \text{BY hypothesis 1} \end{array}$$

- Schlüsse von Zielaussage zu notwendigen Voraussetzungen
- Top-down Vorgehensweise, hilfreicher für Entwicklung von Beweisen

# KALKÜLARTEN

- **Axiom-orientiert: Frege–Hilbert–Kalküle**

- Sehr mächtig, aber aufwendige Beweissuche (synthetisch)

- **Konnektivorientiert**

**Natürliches Schließen**  $\mathcal{NK}, \mathcal{NJ}$  (synthetisch)

- Einfache Regeln für Einführung und Analyse von Konnektiven
- Separate globale Verwaltung von noch offenen Annahmen

**Sequenzkalküle**  $\mathcal{LK}, \mathcal{LJ}$  (synthetisch)

- Natürliche Inferenzregeln mit lokaler Verwaltung von Annahmen

**Tableaux-Kalküle** (analytisch)

- Kompakte, unabhängig entstandene Variante des Sequenzkalküls

**Refinement Logic** (analytisch)

- Analytischer Sequenzkalkül, **gut für interaktive Beweissuche**

- **Maschinennah: Resolutions-/Konnektionskalküle**

- Maschinennahe analytische Kalküle, gut für automatisches Beweisen

# ANHANG

# FREGE–HILBERT–KALKÜLE

## ● Sehr viele Axiomenschemata

- |                                                                                                        |                                                                                  |
|--------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| (A1) $A \Rightarrow A$                                                                                 | (A11) $(A \wedge B \vee C) \Rightarrow (A \vee C) \wedge (B \vee C)$             |
| (A2) $A \Rightarrow (B \Rightarrow A)$                                                                 | (A12) $(A \vee C) \wedge (B \vee C) \Rightarrow (A \wedge B \vee C)$             |
| (A3) $(A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))$                 | (A13) $(A \vee B) \wedge C \Rightarrow (A \wedge C \vee B \wedge C)$             |
| (A4) $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$ | (A14) $(A \wedge C \vee B \wedge C) \Rightarrow (A \vee B) \wedge C$             |
| (A5) $A \Rightarrow A \vee B$                                                                          | (A15) $(A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$                |
| (A6) $A \Rightarrow B \vee A$                                                                          | (A16) $A \wedge \neg A \Rightarrow B$                                            |
| (A7) $(A \Rightarrow C) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \vee B \Rightarrow C))$          | (A17) $(A \wedge (A \Rightarrow B)) \Rightarrow B$                               |
| (A8) $A \wedge B \Rightarrow A$                                                                        | (A18) $(A \wedge C \Rightarrow B) \Rightarrow (C \Rightarrow (A \Rightarrow B))$ |
| (A9) $A \wedge B \Rightarrow B$                                                                        | (A19) $(A \Rightarrow (A \wedge \neg A)) \Rightarrow \neg A$                     |
| (A10) $(C \Rightarrow A) \Rightarrow ((C \Rightarrow B) \Rightarrow (C \Rightarrow A \wedge B))$       | $\vdots$                                                                         |

## ● Nur eine Inferenzregel

$$(\text{mp}) \quad \frac{A, A \Rightarrow B}{B}$$

## ● Beweise mathematisch elegant aber unnatürlich

- (1)  $A \wedge B \Rightarrow A$  (A8)
- (2)  $A \wedge B \Rightarrow B$  (A9)
- (3)  $(A \wedge B \Rightarrow B) \Rightarrow ((A \wedge B \Rightarrow A) \Rightarrow (A \wedge B \Rightarrow B \wedge A))$  (A10)
- (4)  $(A \wedge B \Rightarrow A) \Rightarrow (A \wedge B \Rightarrow B \wedge A)$  (mp mit (2), (3))
- (5)  $(A \wedge B \Rightarrow B \wedge A)$  (mp mit (1), (4))

# NATÜRLICHE DEDUKTION $\mathcal{NK}$

- **Lesbare, kompaktifizierte Beweisdarstellung**
  - Beweisbaum mit Formeln und schematischen Inferenzregeln als Übergänge
  - Globale Verwaltung temporärer Annahmen
  - Synthetischer Aufbau (ungünstig für Suche nach Beweisen)
- **Inferenzfiguren gruppiert nach logischen Symbolen**
  - **Einführungsregel**: Welche Voraussetzungen machen eine Formel gültig?
  - **Eliminationsregel**: Was folgt aus einer gegebenen Formel?

|                  |                                                                 |                      |                  |                                                                                                              |                        |
|------------------|-----------------------------------------------------------------|----------------------|------------------|--------------------------------------------------------------------------------------------------------------|------------------------|
| $\wedge -I$      | $\frac{A \quad B}{A \wedge B}$                                  |                      | $\wedge -E$      | $\frac{A \wedge B}{A}$                                                                                       | $\frac{A \wedge B}{B}$ |
| $\vee -I$        | $\frac{A}{A \vee B}$                                            | $\frac{B}{A \vee B}$ | $\vee -E$        | $\frac{A \vee B \quad \begin{array}{c} [A] \\ C \end{array} \quad \begin{array}{c} [B] \\ C \end{array}}{C}$ |                        |
| $\Rightarrow -I$ | $\frac{\begin{array}{c} [A] \\ B \end{array}}{A \Rightarrow B}$ |                      | $\Rightarrow -E$ | $\frac{A \quad A \Rightarrow B}{B}$                                                                          |                        |
| $\neg -I$        | $\frac{\begin{array}{c} [A] \\ \text{ff} \end{array}}{\neg A}$  |                      | $\neg -E$        | $\frac{\neg A \quad A}{\text{ff}}$                                                                           |                        |
| <i>axiom</i>     | $\overline{A \vee \neg A}$                                      |                      | $\text{ff} -E$   | $\frac{\text{ff}}{A}$                                                                                        |                        |

- Einziges Axiom  $A \vee \neg A$  nur für klassische Logik erforderlich

## BEISPIEL: $((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$ MATHEMATISCHER BEWEIS

1. Wir nehmen an  $(A \Rightarrow B) \wedge (B \Rightarrow C)$  sei erfüllt
2. Wir nehmen weiter an, daß  $A$  gilt.
3. Aus der ersten Annahme folgt  $(A \Rightarrow B)$
4. und mit der zweiten dann auch  $B$ .
5. Aus der ersten Annahme folgt auch, daß  $(B \Rightarrow C)$  gilt
6. und mit der vierten dann auch  $C$ .
7. Es ergibt sich, daß  $C$  unter der Annahme  $A$  gilt. Also folgt  $A \Rightarrow C$
8. Insgesamt folgt  $A \Rightarrow C$  unter der Annahme  $(A \Rightarrow B) \wedge (B \Rightarrow C)$ .  
Damit gilt die Behauptung:  $((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$

# BEISPIEL: $((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$

## BEWEIS IN $\mathcal{NK}$

1.  $(A \Rightarrow B) \wedge (B \Rightarrow C)$  Annahme
2.  $A$  Annahme
3.  $(A \Rightarrow B)$   $\wedge$ -E mit (1)
4.  $B$   $\Rightarrow$ -E mit (2) und (3)
5.  $(B \Rightarrow C)$   $\wedge$ -E mit (1)
6.  $C$   $\Rightarrow$ -E mit (4) und (5)
7.  $(A \Rightarrow C)$   $\Rightarrow$ -I mit (2) und (6) — (2) entfällt
8.  $(A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow (A \Rightarrow C)$   $\Rightarrow$ -I mit (1) und (7) — (1) entfällt

### Schematischer Beweis in Baumstruktur

$$\begin{array}{c}
 \frac{\frac{[A] \quad \frac{[(A \Rightarrow B) \wedge (B \Rightarrow C)]}{(A \Rightarrow B)} \wedge\text{-}E}{B} \Rightarrow\text{-}E \quad \frac{[(A \Rightarrow B) \wedge (B \Rightarrow C)]}{(B \Rightarrow C)} \wedge\text{-}E}{C} \Rightarrow\text{-}E}{(A \Rightarrow C)} \Rightarrow\text{-}I}{((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)} \Rightarrow\text{-}I
 \end{array}$$



# SEQUENZENKALKÜLE

- **Modifikation von Natürlicher Deduktion**

- Schließen über Aussagen mit Annahmen (Mengen von Formeln)

- Grundkonzept **Sequenz**:  $\underbrace{A_1, \dots, A_n}_{\text{Antezedent } \Gamma} \vdash \underbrace{B_1, \dots, B_m}_{\text{Sukzedent } \Phi}$

- Lesart “*Eine der Formeln  $B_i$  folgt aus den Annahmen  $A_1, \dots, A_n$* ”
- **Zielsequenz**  $\vdash C$  (“*Formel  $C$  gilt ohne weitere Annahmen*”)

- **Semantik entspricht**  $A_1 \wedge \dots \wedge A_n \Rightarrow B_1 \vee \dots \vee B_m$

- Homomorphe Fortsetzung von Interpretationen

$$\iota(A_1, \dots, A_n \vdash B_1, \dots, B_m) = \begin{cases} \text{wahr} & \text{falls aus } \iota(A_1) = \text{wahr} \\ & \text{und } \dots \iota(A_n) = \text{wahr} \\ & \text{immer } \iota(B_1) = \text{wahr} \\ & \text{oder } \dots \iota(B_m) = \text{wahr folgt} \\ \text{falsch} & \text{sonst} \end{cases}$$

- Begriffe **Modell, Gültigkeit, Erfüllbarkeit** analog

# INFERENZ IN SEQUENZENKALKÜLEN

- **Synthetische Beweise** wie bei  $\mathcal{NK}$

- Lokale Sicht: keine globale Verwaltung von Annahmen nötig

- **Regeln manipulieren Sequenzen statt Formeln**

- Eliminationsregeln  $\mapsto$  Einführungsregeln links für Antezedent ( $-L$ )

$$\frac{A \wedge B}{A} \wedge -E \quad \text{wird zu} \quad \frac{\Gamma, A \vdash \Phi}{\Gamma, A \wedge B \vdash \Phi} \wedge -L$$

- Einführungsregeln  $\mapsto$  Einführungsregeln rechts für Sukzedent ( $-R$ )

|                  |                                                                                                                               |                  |                                                                                                               |
|------------------|-------------------------------------------------------------------------------------------------------------------------------|------------------|---------------------------------------------------------------------------------------------------------------|
| $\neg -R$        | $\frac{\Gamma, A \vdash \Phi}{\Gamma \vdash \Phi, \neg A}$                                                                    | $\neg -L$        | $\frac{\Gamma \vdash \Phi, A}{\Gamma, \neg A \vdash \Phi}$                                                    |
| $\wedge -R$      | $\frac{\Gamma \vdash \Phi, A \quad \Gamma \vdash \Phi, B}{\Gamma \vdash \Phi, A \wedge B}$                                    | $\wedge -L$      | $\frac{\Gamma, A \vdash \Phi \quad \Gamma, B \vdash \Phi}{\Gamma, A \wedge B \vdash \Phi}$                    |
| $\vee -R$        | $\frac{\Gamma \vdash \Phi, A}{\Gamma \vdash \Phi, A \vee B} \quad \frac{\Gamma \vdash \Phi, B}{\Gamma \vdash \Phi, A \vee B}$ | $\vee -L$        | $\frac{\Gamma, A \vdash \Phi \quad \Gamma, B \vdash \Phi}{\Gamma, A \vee B \vdash \Phi}$                      |
| $\Rightarrow -R$ | $\frac{\Gamma, A \vdash \Phi, B}{\Gamma \vdash \Phi, A \Rightarrow B}$                                                        | $\Rightarrow -L$ | $\frac{\Gamma \vdash \Phi, A \quad \Delta, B \vdash \Psi}{\Gamma, \Delta, A \Rightarrow B \vdash \Phi, \Psi}$ |
| <i>axiom</i>     | $\frac{}{A \vdash A}$                                                                                                         | <i>Schnitt</i>   | $\frac{\Gamma \vdash \Phi, A \quad A, \Delta \vdash \Psi}{\Gamma, \Delta \vdash \Phi, \Psi}$                  |

- Mehrere Sukzedentenformeln nur für klassische Logik erforderlich

- Originalformulierung des Kalküls  $\mathcal{LK}$  verwendet **Listen von Formeln**

Kalkül benutzt **strukturelle Regeln** zur Simulation von Formelmengen

# SEQUENZENBEWEIS FÜR $((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$

1.  $A \vdash A$  Axiom
2.  $B \vdash B$  Axiom
3.  $A, A \Rightarrow B \vdash B$   $\Rightarrow$ -E mit (1), (2)
4.  $C \vdash C$  Axiom
5.  $A, A \Rightarrow B, B \Rightarrow C \vdash C$   $\Rightarrow$ -E mit (3), (4)
6.  $A, (A \Rightarrow B) \wedge (B \Rightarrow C) \vdash C$   $\wedge$ -E
7.  $(A \Rightarrow B) \wedge (B \Rightarrow C) \vdash A \Rightarrow C$   $\Rightarrow$ -I
8.  $\vdash (A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow (A \Rightarrow C)$   $\Rightarrow$ -I

## Schematischer Beweis in Baumstruktur

$$\begin{array}{c}
 \frac{A \vdash A \quad B \vdash B}{A, A \Rightarrow B \vdash B} \Rightarrow -L \quad C \vdash C \\
 \hline
 \frac{A, A \Rightarrow B, B \Rightarrow C \vdash C}{A, A \Rightarrow B, (A \Rightarrow B) \wedge (B \Rightarrow C) \vdash C} \wedge -L \\
 \hline
 \frac{A, A \Rightarrow B, (A \Rightarrow B) \wedge (B \Rightarrow C) \vdash C}{A, (A \Rightarrow B) \wedge (B \Rightarrow C) \vdash C} \wedge -L \text{ (mit Kontraktion)} \\
 \hline
 \frac{A, (A \Rightarrow B) \wedge (B \Rightarrow C) \vdash C}{(A \Rightarrow B) \wedge (B \Rightarrow C) \vdash A \Rightarrow C} \Rightarrow -R \\
 \hline
 \frac{(A \Rightarrow B) \wedge (B \Rightarrow C) \vdash A \Rightarrow C}{\vdash ((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow A \Rightarrow C} \Rightarrow -R
 \end{array}$$

# KONSTRUKTIVE VS. KLASSISCHE BEWEISKALKÜLE

- $\mathcal{NK}$  und  $\mathcal{LK}$  haben intuitionistische Varianten

- $\mathcal{NJ}$ : Kalkül verwendet nur konnektionsbezogene Inferenzregeln  
Keine gesonderten Axiome erforderlich
- $\mathcal{LJ}$ : Sukzedent enthält genau eine Formel (“single conclusioned”)  
Regeln dürfen nie zwei oder mehr Sukzedentenformeln erzeugen

- Die intuitionistische Form erscheint natürlicher

- Die Grundform der Kalküle liefert immer die konstruktive Logik
- Nichtkonstruktive Schlüsse erfordern besondere Konstrukte
  - $\mathcal{NK}$ : gesondertes “künstliches” Axiom  $A \vee \neg A$  wird hinzugefügt
  - $\mathcal{LK}$ : zu beweisende Schlußfolgerung steht nicht eindeutig fest  
... man kann mitten im Beweis das Beweisziel wechseln
- Nichtkonstruktive Beweise sind allerdings zuweilen erheblich kürzer

# SYNTHETISCHE VS. ANALYTISCHE BEWEISKALKÜLE

- **Synthetische Form unterstützt Beweispräsentation**

- Beweis führt von Annahmen zum Endergebnis
- Offen bleibt, wie man zu den anfänglichen Annahmen kommt

- **Analytische Form unterstützt Beweissuche**

- Umkehrung der Inferenzregeln bzw. ihrer Lesart 
$$\frac{\Gamma, A \wedge B \vdash \Phi}{\Gamma, A, B \vdash \Phi} \quad \wedge L$$
- Geeigneter zur **Entwicklung** von Beweisen
  - Suche hinreichende Voraussetzungen für Gültigkeit einer Aussage
  - Iterativer Prozess **verfeinert** Beweisziel in Teilziele, bis keine unbewiesenen Voraussetzungen übrigbleiben
  - **Sequenzen enthalten alle beweisrelevanten Informationen** für eine lokale Durchführung dieses Prozesses,
- Synthetischer Beweis ist Umkehrung des fertigen Beweisbaums

→ **Refinement Logic:** (Konstruktiver) analytischer Sequenzenkalkül

- Besonders geeignet für **computergestützte interaktive Beweisführung**