Inferenzmethoden

Teil I

Beweiskalküle

Formalisierung von Beweisen

Inferenzmethoden

Einheit 1

Formale Logik - kurzgefaßt

1. Syntax & Semantik der Prädikatenlogik
2. Inferenzkalküle für die Prädikatenlogik

Formale Kalküle

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

Beschreibung formaler Sprachen

- **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 Grundlagentheorien (Mengentheorie, Typentheorie)
  Mathematische Präzisierung der intuitiven Bedeutung

Syntax der Prädikatenlogik

- **(Abzählbare) Alphabete für erlaubte Symbole**
  - $\mathcal{V}$: Variablensymbole $x,y,z,a,b,c,\ldots$
  - $\mathcal{F}^i$: i-stellige Funktionssymbole, $\boldsymbol{\mathcal{F}} = \bigcup_{i=0}^{\infty}\mathcal{F}^i$ $f,g,h,\ldots$
  - $\mathcal{P}^i$: i-stellige Prädikatssymbole, $\boldsymbol{\mathcal{P}} = \bigcup_{i=0}^{\infty}\mathcal{P}^i$ $P,Q,R,\ldots$
- **Terme**
  - Variablen $x \in \mathcal{V}$, Konstante $f \in \mathcal{F}^0$ (atomare Terme)
  - $f(t_1,\ldots,t_n)$, wobei $t_1,..,t_n$ Terme, $f \in \mathcal{F}^n$
- **Formeln**
  - Konstante ff, Aussagenvariable $P \in \mathcal{P}^0$ (atomare Formeln)
  - $P(t_1,\ldots,t_n)$, wobei $t_1,..,t_n$ Terme, $P \in \mathcal{P}^n$
  - $\neg A$, $A \wedge B$, $A \vee B$, $A \Rightarrow B$, $\forall x\, A$, $\exists x\, A$, (A) (A, B Formeln, $x \in \mathcal{V}$)

Beispiele für Terme und Formeln

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

  Kontext bestimmt Rolle von Symbolen
- **Korrekte Formeln**
  - `(4=plus(2,3))` $\Rightarrow$ ff
  - `Sein` $\vee \neg$`Sein`, `lange_währt` $\Rightarrow$ `endlich_gut`
  - $\forall$`x` $\exists$`y` $\leq$`(*(y,y),x)` $\wedge$ `<(x,*(plus(y,1),plus(y,1)))`
- **Keine Formeln**
  - `plus(plus(2,3),4)` — Term
  - $\wedge$ `so_weiter` — Formel links von $\wedge$ fehlt
  - $\forall$`x x(4)=x` — Variable als Funktionszeichen
  - $\forall$`f f(4)=0` — Quantifizierung über Funktionszeichen (higher-order)

Konventionen sparen Klammern

$\exists$y gerade(y) $\land$ $\geq$(y,2) $\Rightarrow$ =(y,2) $\land$ >(y,20) **heißt?**

- $\exists$y (gerade(y) $\land$ $\geq$(y,2)) $\Rightarrow$ (=(y,2) $\land$ >(y,20)) ??
- $\exists$y gerade(y) $\land$ ($\geq$(y,2) $\Rightarrow$ (=(y,2) $\land$ >(y,20))) ??
- $\exists$y (gerade(y) $\land$ ($\geq$(y,2) $\Rightarrow$ =(y,2))) $\land$ >(y,20) ??

- **Prioritäten zwischen verschiedenen Konnektiven**

  $\neg$ bindet stärker als $\land$, dann folgt $\lor$, dann $\Rightarrow$, dann $\exists$, dann $\forall$.

$A \land \neg B$	entspricht	$A \land (\neg B)$
$A \land B \lor C$	entspricht	$(A \land B) \lor C$
$\exists x\ A \land B$	entspricht	$\exists x\ (A \land B)$

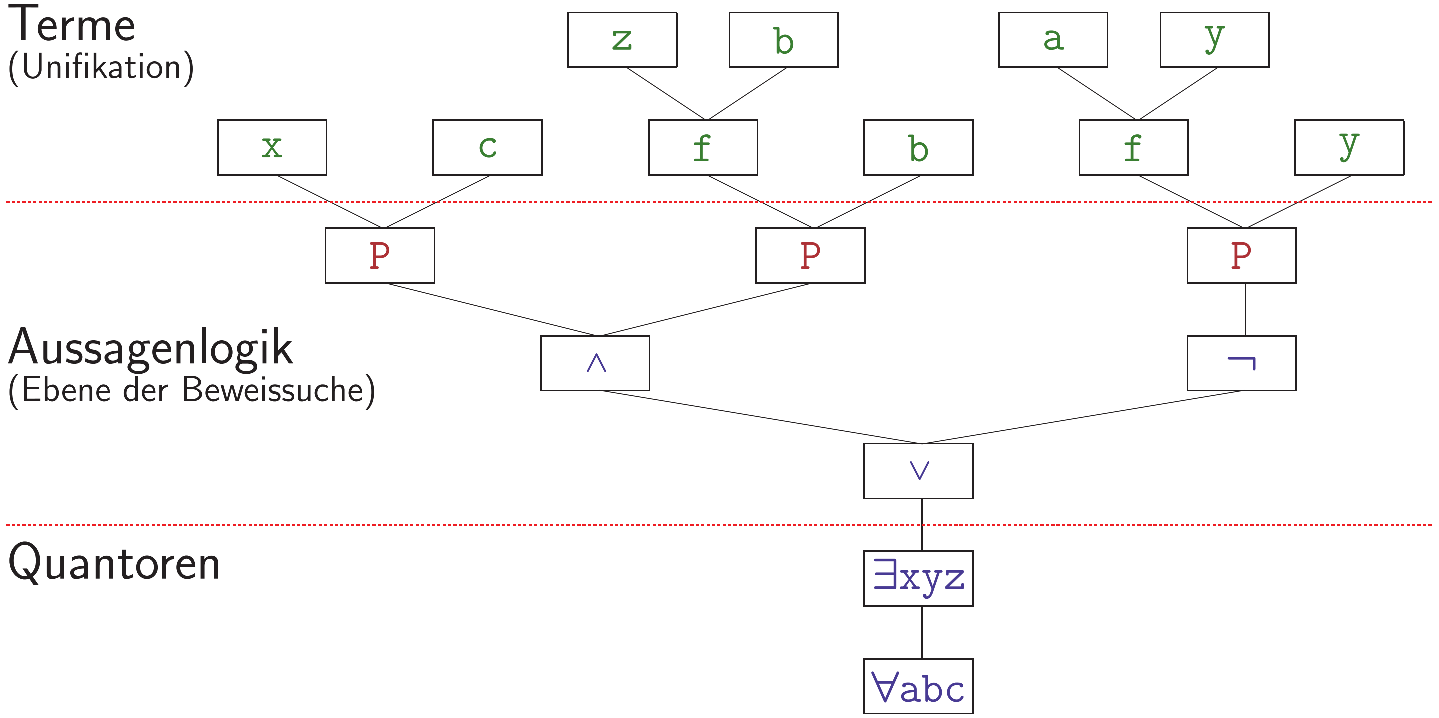
  Achtung: Unterschiedliche Konventionen in verschiedenen Lehrbüchern

- **Rechtsassoziativität bei Iteration von $\land$, $\lor$, $\Rightarrow$**
  - $A \Rightarrow B \Rightarrow C$ entspricht $A \Rightarrow (B \Rightarrow C)$

- **Keine Klammern bei Funktions-/Prädikatssymbolen**
  - Px entspricht $P(x)$ und fxy entspricht $f(x,y)$
  - $\exists xyz\, A$ entspricht $\exists x \exists y \exists z\, A$ und $\forall xyz\, A$ entspricht $\forall x \forall y \forall z\, A$

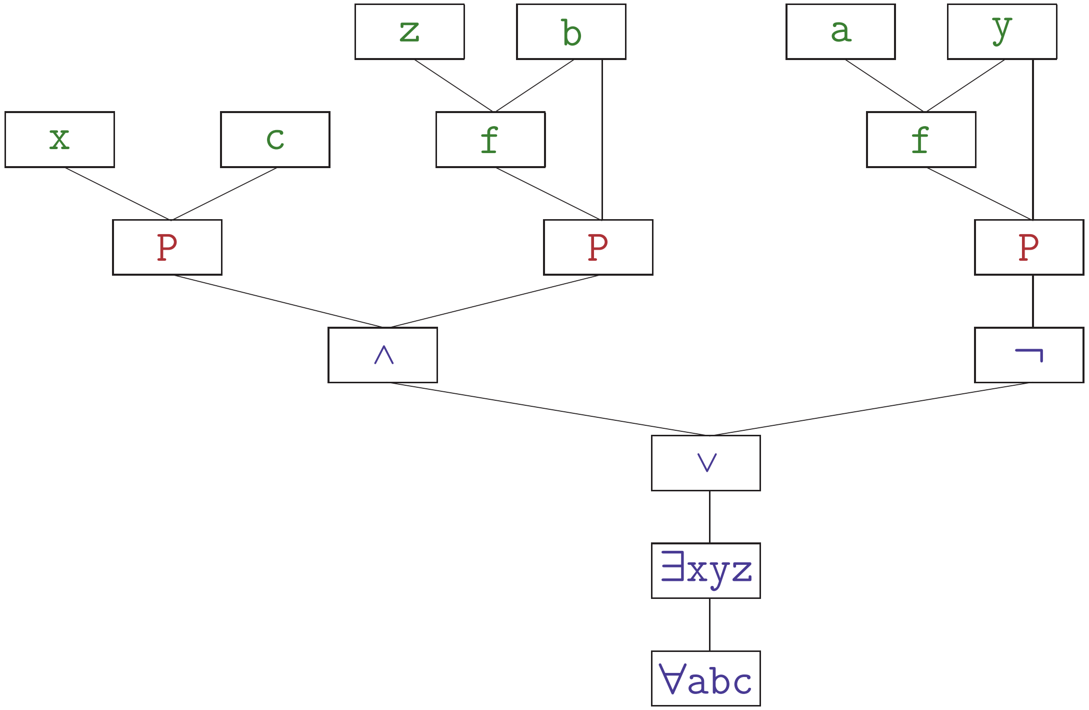
Formelbäume: Interne Darstellung von Formeln

- **Abstrakter Syntaxbaum, erzeugt durch Parsen der Formel**
- **Baumstruktur, annotiert mit Konnektiven und Symbolen**
- **Formelbaum für** $\forall abc\,\exists xyz\ Pxc \wedge P(fzb,b) \vee \neg P(fay,y)$



Gerichtete azyklische Graphen (DAG's)

- **Structure Sharing: Zusammenlegung identischer Teilbäume**
- **Effizientere Darstellung von Formeln ohne unnötige Kopien**
- **DAG für** $\forall$abc$\exists$xyz Pxc $\wedge$ P(fzb,b) $\vee$ $\neg$P(fay,y)



Semantik der Prädikatenlogik (I)
Interpretation in der Mengentheorie

- **Interpretation $\mathcal{I}$:**
  - **Universum $\mathcal{U}$ + Interpretationsfunktion ι**
- **Freie Wahl von ι auf elementaren Symbolen**
  - $\iota(x)$ Objekt aus $\mathcal{U}$ $\quad (x \in \mathcal{V})$
  - $\iota(f)$ n-stellige Funktion $\phi : \mathcal{U}^n \to \mathcal{U}$ $\quad (f \in \mathcal{F}^n)$
  - $\iota(P)$ Funktion $\Pi : \mathcal{U}^n \to \{\mathsf{wahr}, \mathsf{falsch}\}$ $\quad (P \in \mathcal{P}^n)$
- **Homomorphe Fortsetzung auf Terme und Formeln**
  - $\iota(f(t_1,\ldots,t_n)) = \iota(f)(\iota(t_1),\ldots,\iota(t_n))$
  - $\iota(\mathsf{ff}) = \mathsf{falsch}$
  - $\iota(P(t_1,\ldots,t_n)) = \iota(P)(\iota(t_1),\ldots,\iota(t_n))$.
  - $\iota((A)) = \iota(A)$

Semantik der Prädikatenlogik (II)

Fortsetzung von ι auf zusammengesetzte Formeln

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

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

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

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

$$\iota(\forall x\, A) = \begin{cases} \textsf{wahr} & \text{falls } \iota_x^u(A) = \textsf{wahr} \text{ für alle } u \in \mathcal{U} \\ \textsf{falsch} & \text{sonst} \end{cases}$$

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

$$\iota(\exists x\, A) = \begin{cases} \textsf{wahr} & \text{falls } \iota_x^u(A) = \textsf{wahr} \text{ für ein } u \in \mathcal{U} \\ \textsf{falsch} & \text{sonst} \end{cases}$$

Semantik der Prädikatenlogik (II) – klassisch
Fortsetzung von ι auf zusammengesetzte Formeln

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

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

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

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

$$\iota(\forall x\, A) = \begin{cases} \textsf{wahr} & \text{falls } \iota_x^u(A) = \textsf{wahr} \text{ für alle } u \in \mathcal{U} \\ \textsf{falsch} & \text{sonst} \end{cases}$$

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

$$\iota(\exists x\, A) = \begin{cases} \textsf{falsch} & \text{falls } \iota_x^u(A) = \textsf{falsch} \text{ für alle } u \in \mathcal{U} \\ \textsf{wahr} & \text{sonst} \end{cases}$$

Ist das wirklich dasselbe?

Interpretation von Formeln

Sei ι die "Standardinterpretation" und $\iota(\mathtt{x}) = \mathit{dreizehn}$

- $\iota(\leq\mathtt{(max(2,3,4),7)})$

  $= \iota(\leq)(\iota(\mathtt{max(2,3,4)}),\iota(\mathtt{7}))$

  $= \Pi_{\leq}(\iota(\mathtt{max})(\iota(\mathtt{2}),\iota(\mathtt{3}),\iota(\mathtt{4})),\ \mathit{sieben}))$

  $= \Pi_{\leq}(\phi_{max}(\mathit{zwei},\mathit{drei},\mathit{vier}),\ \mathit{sieben})$

  $= \Pi_{\leq}(\mathit{vier},\ \mathit{sieben})$

  $=$ wahr

- $\iota(\exists\mathtt{x}\ \leq\mathtt{(max(2,3,4),x)})$

  $=$ wahr gdw. $\iota_x^u(\leq\mathtt{(max(2,3,4),x)}) =$ wahr für ein $u \in \mathcal{U}$ ist

  $= \vdots$

  $=$ wahr gdw. $\Pi_{\leq}(\mathit{vier},\iota_x^u(\mathtt{x})) =$ wahr für eine Zahl u

  $=$ wahr gdw. $\Pi_{\leq}(\mathit{vier},u) =$ wahr für eine Zahl u

  $=$ wahr (wähle $u = \mathit{fünf}$)

Objekt- und Metasprache

Präsentation von Kalkülen hat zwei Sprachebenen

- **Objektsprache:**
  - Sprache des Kalküls, in dem formalisiert wird
  - Formale Sprache mit präzise definierter Syntax
  - Beispiel: $(\exists x\ P_1(x) \vee P_2(x)) \;\Rightarrow\; \neg(\forall x\ \neg P_1(x) \wedge \neg P_2(x))$
- **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* $(\exists x\ A \vee B)$ *folgt* $\neg(\forall x\ \neg A \wedge \neg B)$
- **Unterscheidung zuweilen durch Fonts / Farben**
  - Ansonsten aus Kontext eindeutig erkennbar

Modelle und Gültigkeit

- **Modell $\mathcal{M}$ von A** $(\mathcal{M} \models A)$
  - Interpretation $\mathcal{M} = (\iota, \mathcal{U})$ mit $\iota(A) = \mathsf{wahr}$
- **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)

Deduktionstheorem: $\boxed{\mathcal{E} \cup \{E\} \models F \text{ genau dann, wenn } \mathcal{E} \models E \Rightarrow F}$

- **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

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

$\forall x\ x<0$ erfüllbar, nicht gültig

$\exists x\ x>0$ erfüllbar, nicht gültig

$\neg(\exists x\ x>0)$ erfüllbar, nicht gültig

Symbole $\leq$, +, 3, 4, 1, > haben keine feste Bedeutung

Inferenzkalküle

Syntaktische Manipulation formaler Ausdrücke unter Berücksichtigung der Semantik

- **Inferenz:** Erzeugung von logischen Konsequenzen einer Formelmenge

  aus A *und* $A \Rightarrow B$ *folgt* B: $\quad \dfrac{A,\ \ A \Rightarrow B}{B}$

- **Regelschema** $\dfrac{A_1, \ldots, A_n}{C}$: *aus* $\underbrace{A_1 \text{ und } \ldots A_n}_{\textit{Prämissen}}$ *folgt* $\underbrace{C}_{\textit{Konklusion}}$
  - **Axiom**: Regel ohne Prämissen
  - $\Gamma \vdash_{rs} C$: Konkrete Anwendung des Regelschemas rs

- **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

Kalkülarten (I)

Kalküle sind Hilfsmittel, keine Beweismethode

- **Synthetisch**
  – Schlüsse von Axiomen zur Aussage
  – Bottom-up Vorgehensweise
  – Übliche Art, fertige Beweise zu präsentieren
- **Analytisch**
  – Schlüsse von Zielaussage zu notwendigen Voraussetzungen
  – Top-down Vorgehensweise
  – Hilfreicher für Entwicklung von Beweisen

KALKÜLARTEN (II)

- **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

  Sequenzenkalküle $\mathcal{LK}$, $\mathcal{LJ}$ (synthetisch)
  – Natürliche Inferenzregeln mit lokaler Verwaltung von Annahmen

  Refinement Logic (analytisch)
  – Analytischer Sequenzenkalkül, **gut für interaktive Beweissuche**

  Tableaux-Kalküle (analytisch)
  – Kompakte, unabhängig entstandene Variante des Sequenzenkalküls

- **Maschinennah: Resolutions-/Konnektionskalküle**
  – Maschinennahe analytische Kalküle, gut für automatisches Beweisen

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)	$(C \Rightarrow A) \Rightarrow ((C \Rightarrow B) \Rightarrow (C \Rightarrow A \wedge B))$	$\vdots$	$\vdots$

- **Nur eine Inferenzregel**

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

- **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	$\dfrac{A \quad B}{A \wedge B}$	$\wedge$-E	$\dfrac{A \wedge B}{A}$ $\quad$ $\dfrac{A \wedge B}{B}$
$\vee$-I	$\dfrac{A}{A \vee B}$ $\quad$ $\dfrac{B}{A \vee B}$	$\vee$-E	$\dfrac{A \vee B \quad \begin{matrix}[A]\\ C\end{matrix} \quad \begin{matrix}[B]\\ C\end{matrix}}{C}$
$\Rightarrow$-I	$\dfrac{\begin{matrix}[A]\\ B\end{matrix}}{A \Rightarrow B}$	$\Rightarrow$-E	$\dfrac{A \quad A \Rightarrow B}{B}$
$\neg$-I	$\dfrac{\begin{matrix}[A]\\ \mathsf{ff}\end{matrix}}{\neg A}$	$\neg$-E	$\dfrac{\neg A \quad A}{\mathsf{ff}}$
axiom	$\dfrac{}{A \vee \neg A}$	ff-E	$\dfrac{\mathsf{ff}}{A}$

  - 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: $((A \Rightarrow B) \land (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$
Beweis in $\mathcal{NK}$

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

Schematischer Beweis in Baumstruktur

$$\dfrac{\dfrac{\dfrac{\dfrac{[A] \quad \dfrac{[(A \Rightarrow B) \land (B \Rightarrow C)]}{(A \Rightarrow B)}\,\land\text{-}E}{B}\,\Rightarrow\text{-}E \qquad \dfrac{[(A \Rightarrow B) \land (B \Rightarrow C)]}{(B \Rightarrow C)}\,\land\text{-}E}{C}\,\Rightarrow\text{-}E}{(A \Rightarrow C)}\,\Rightarrow\text{-}I}{((A \Rightarrow B) \land (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)}\,\Rightarrow\text{-}I$$

Sequenzenkalküle

- **Modifikation von Natürlicher Deduktion**
  – Schließen über Aussagen mit Annahmen (Mengen von Formeln)
- **Grundkonzept Sequenz:** $\underbrace{\boldsymbol{A_1,..,A_n}}_{\text{Antezedent } \boldsymbol{\Gamma}} \vdash \underbrace{\boldsymbol{B_1,..,B_m}}_{\text{Sukzedent } \boldsymbol{\Phi}}$
  – Lesart "*Eine der Formeln B_i folgt aus den Annahmen $A_1,\ldots,A_n$*"
  – Zielsequenz $\vdash C$ ("*Formel C gilt ohne weitere Annahmen*")
- **Semantik entspricht** $A_1 \wedge \ldots \wedge A_n \;\Rightarrow\; B_1 \vee \ldots \vee B_m$
  – Homomorphe Fortsetzung von Interpretationen

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

- **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 ($-L$)

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

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

$\neg$-R	$\dfrac{\Gamma, A \vdash \Phi}{\Gamma \vdash \Phi, \neg A}$	$\neg$-L	$\dfrac{\Gamma \vdash \Phi, A}{\Gamma, \neg A \vdash \Phi}$
$\wedge$-R	$\dfrac{\Gamma \vdash \Phi, A \quad \Gamma \vdash \Phi, B}{\Gamma \vdash \Phi, A \wedge B}$	$\wedge$-L	$\dfrac{\Gamma, A \vdash \Phi}{\Gamma, A \wedge B \vdash \Phi} \quad \dfrac{\Gamma, B \vdash \Phi}{\Gamma, A \wedge B \vdash \Phi}$
$\vee$-R	$\dfrac{\Gamma \vdash \Phi, A}{\Gamma \vdash \Phi, A \vee B} \quad \dfrac{\Gamma \vdash \Phi, B}{\Gamma \vdash \Phi, A \vee B}$	$\vee$-L	$\dfrac{\Gamma, A \vdash \Phi \quad \Gamma, B \vdash \Phi}{\Gamma, A \vee B \vdash \Phi}$
$\Rightarrow$-R	$\dfrac{\Gamma, A \vdash \Phi, B}{\Gamma \vdash \Phi, A \Rightarrow B}$	$\Rightarrow$-L	$\dfrac{\Gamma \vdash \Phi, A \quad \Delta, B \vdash \Psi}{\Gamma, \Delta, A \Rightarrow B \vdash \Phi, \Psi}$
axiom	$\dfrac{}{A \vdash A}$	*Schnitt*	$\dfrac{\Gamma \vdash \Phi, A \quad A, \Delta \vdash \Psi}{\Gamma, \Delta \vdash \Phi, \Psi}$

  – 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

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \vdash A \qquad B \vdash B}{A,\ A \Rightarrow B \vdash B}\Rightarrow\!-L \qquad C \vdash C}{A,\ A \Rightarrow B,\ B \Rightarrow C \vdash C}\Rightarrow\!-L}{A,\ A \Rightarrow B,\ (A \Rightarrow B) \wedge (B \Rightarrow C) \vdash C}\wedge\!-L}{A,\ (A \Rightarrow B) \wedge (B \Rightarrow C) \vdash C}\wedge\!-L \text{ (mit Kontraktion)}}{(A \Rightarrow B) \wedge (B \Rightarrow C) \vdash A \Rightarrow C}\Rightarrow\!-R}{\vdash ((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow A \Rightarrow C}\Rightarrow\!-R
$$

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 $\dfrac{\Gamma, A \wedge B \vdash \Phi}{\Gamma, A, B \vdash \Phi} \quad \wedge L$
  - 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**: analytischer Sequenzenkalkül
  - Besonders geeignet für computergestützte interaktive Beweisführung

Refinement Logic: Analytische Sequenzenbeweise

Zielorientierte Beweisführung

- **Inferenzregel:** Abbildung von Beweisziel in Teilziele
  - Beweisziel: einzelne Sequenz, die zu beweisen ist
  - Teilziele: endliche (evtl. leere) Liste von Sequenzen, die nach Regelanwendung noch zu zeigen sind
  - Zugriff auf Hypothesen durch *Parameter*

$$\begin{array}{l} \Gamma \vdash C \;\; \texttt{BY} \;\; \mathit{rule} \\ \quad \Gamma_1 \vdash C_1 \\ \quad\quad \vdots \\ \quad \Gamma_n \vdash C_n \end{array}$$

$$\begin{array}{l} \Gamma, A \wedge B, \Delta \vdash C \;\; \texttt{BY andE} \;\; i \\ \quad \Gamma, A, B, \Delta \vdash C \end{array}$$

- **Beweis:** Baum mit Sequenzen und Regeln als Knoten
  - Nachfolger eines Knotens sind Teilziele der Regelanwendung auf Sequenz
  - unvollständig: manche Blätter ohne Regel
  - vollständig: Regeln der Blätter ohne Teilziele

- **Theorem:** Formel C mit vollständigem Beweis für $\vdash C$

Refinement Logic: Aussagenlogische Regeln

Elimination (links)		Introduktion (rechts)	
andE i	$\Gamma,\ A \wedge B,\ \Delta \vdash C$ $\Gamma,\ A,\ B,\ \Delta \vdash C$	$\Gamma \vdash A \wedge B$ $\Gamma \vdash A$ $\Gamma \vdash B$	andI
orE i	$\Gamma,\ A \vee B,\ \Delta \vdash C$ $\Gamma,\ A,\ \Delta \vdash C$ $\Gamma,\ B,\ \Delta \vdash C$	$\Gamma \vdash A \vee B$ $\Gamma \vdash A$ $\Gamma \vdash A \vee B$ $\Gamma \vdash B$	orI1 orI2
impE i	$\Gamma,\ A \Rightarrow B,\ \Delta \vdash C$ $\Gamma,\ A \Rightarrow B,\ \Delta \vdash A$ $\Gamma,\ \Delta,\ B \vdash C$	$\Gamma \vdash A \Rightarrow B$ $\Gamma,\ A \vdash B$	impI
notE i	$\Gamma,\ \neg A,\ \Delta \vdash C$ $\Gamma,\ \neg A,\ \Delta \vdash A$	$\Gamma \vdash \neg A$ $\Gamma,\ A \vdash \mathit{ff}$	notI
falseE i	$\Gamma,\ \mathit{ff},\ \Delta \vdash C$	$\Gamma \vdash P \vee \neg P$	magic

Die magic *Regel wird nur für klassische Logik benötigt*

Refinement Logic: Strukturelle Regeln

Regeln sind unabhängig von Prädikatenlogik

`hypothesis` i $\quad \Gamma,\ A,\ \Delta \vdash A$	$\Gamma,\ \Delta \vdash C$ $\quad$ `cut` i A $\quad \Gamma,\ \Delta \vdash A$ $\quad \Gamma,\ A,\ \Delta \vdash C$
`thin` i $\quad \Gamma,\ A,\ \Delta \vdash C$ $\quad \Gamma,\ \Delta \vdash C$	

- `hypothesis` : nötig für Abschluß von Beweisen ($\hat{=}$ *axiom*)
- `cut` : hilfreich für Strukturierung und Verkürzung (= *Schnitt*
- `thin` : nützlich bei großen Sequenzen (= *Ausdünnung*)

Formale Behandlung von Quantoren

Simuliere ι_x^u durch syntaktische Mechanismen

- **Semantische Analyse von Quantoren braucht ι_x^u**
  - $\iota(\forall x\ A)$ und $\iota(\exists x\ A)$ wird durch $\iota_x^u(A)$ erklärt
    - $\iota_x^u(A)$ muß für alle oder einen Wert u wahr werden
  - ι_x^u modifiziert die Interpretation ι für die gebundene Variable x
  - Syntaktisches Gegenstück ist Ersetzung der Variablen x in A durch Terme
- **Formales Konzept: Substitution $A[t/x]$**
  - Viele alternative Schreibweisen (sehr häufig $A\{x\backslash t\}$)
  - Vorkommen der Variablen x in A werden durch den Term t ersetzt
  - Hinreichend wenn jedes Objekt des Universums durch Terme beschreibbar
    - Reelle Zahlen, Funktionenräume etc. haben zu viele Objekte
  - Allquantor ist sonst nicht vollständig repräsentierbar

SUBSTITUTION $A[t/x]$ – WICHTIGE ASPEKTE

- **Substitution muß Semantik erhalten**
  - Die Namen quantifizierter Variablen dürfen keine Rolle spielen
    - $\exists x\ \ A(x)$ hat dieselbe Bedeutung wie $\exists y\ \ A(y)$
  - Keine Ersetzung von x durch t in $(\exists x\ \ x{\leq}4)[t/x]$
    - Das "äußere" x hat mit dem innerhalb des Quantors nichts zu tun
  - Keine Ersetzung von x durch y in $(\exists y\ \ x{<}y)[y/x]$
    - Durch die Ersetzung würde ein ungewollter Selbstbezug entstehen
- **Variablenvorkommen müssen identifizierbar sein**
  - Gebundenes Vorkommen x in A: x erscheint in Quantor, der A umfaßt
  - Freies Vorkommen x in A: x kommt in A vor, ohne gebunden zu sein
  - Notation $\boldsymbol{A[x]}$: Ausdruck A hat mögliche freie Vorkommen von x
  - A heißt geschlossen falls A keine freien Variablen enthält

Vorkommen von Variablen präzisiert

- x — die Variable x kommt frei vor; $y{\neq}x$ kommt nicht vor.
  ff: — die Variable x kommt nicht vor
- $f(t_1, \ldots, t_n)$ — freie Vorkommen von x in t_i bleiben frei
  $P(t_1, \ldots, t_n)$ — gebundene Vorkommen von x bleiben gebunden.
- $\neg A$, (A) — freie Vorkommen von x in A, B bleiben frei
  $A \wedge B$, $A \vee B$ — gebundene Vorkommen von x bleiben gebunden.
  $A \Rightarrow B$
- $\forall x\ A$ — beliebige Vorkommen von x in A werden gebunden
  $\exists x\ A$ — Vorkommen von $y{\neq}x$ in A bleiben unverändert.

$$\overbrace{\overbrace{(\forall x\ \underbrace{P(x)\ \wedge\ Q(x)}_{x\ \textit{frei}})}^{x\ \textit{gebunden}}\ \wedge\ \underbrace{R(x)}_{x\ \textit{frei}}}^{x\ \textit{frei und gebunden}}$$

Substitution $A[t/x]$ formal

Endliche Abbildung $\boldsymbol{\sigma}$ von Variablen in Terme

- $\boldsymbol{\sigma = [t_1, .., t_n/x_1, .., x_n]} \mathrel{\hat{=}} \sigma(x_1){=}t_1, \ldots, \sigma(x_n){=}t_n$
- $\boldsymbol{A\sigma}$: Anwendung von σ auf den Ausdruck A
- $\boldsymbol{\tau\,\sigma}$: Komposition von τ und σ (σ idempotent falls $\sigma\,\sigma = \sigma$)

$\lfloor x\rfloor[t/x]$	$= t$	$\lfloor x\rfloor[t/y]$	$= x$	$(y{\neq}x)$
$\lfloor f(t_1, .., t_n)\rfloor\sigma$	$= f(t_1\sigma, .., t_n\sigma)$	$\lfloor \mathsf{ff}\rfloor\sigma$	$= \mathsf{ff}$	
$\lfloor P(t_1, .., t_n)\rfloor\sigma$	$= P(t_1\sigma, .., t_n\sigma)$			
$\lfloor \neg A\rfloor\sigma$	$= \neg A\sigma$	$\lfloor A \wedge B\rfloor\sigma$	$= A\sigma \wedge B\sigma$	
$\lfloor A \vee B\rfloor\sigma$	$= A\sigma \vee B\sigma$	$\lfloor A \Rightarrow B\rfloor\sigma$	$= A\sigma \Rightarrow B\sigma$	
$\lfloor (A)\rfloor\sigma$	$= (A\sigma)$			
$\lfloor \forall x\ \ A\rfloor[t/x]$	$= \forall x\ \ A$	$\lfloor \exists x\ \ A\rfloor[t/x]$	$= \exists x\ \ A$	
$\lfloor \forall x\ \ A\rfloor[t/y]$	$= \lfloor \forall z\ \ A[z/x]\rfloor[t/y]$	$\lfloor \exists x\ \ A\rfloor[t/y]$	$= \lfloor \exists z\ \ A[z/x]\rfloor[t/y]$	*
$\lfloor \forall x\ \ A\rfloor[t/y]$	$= \forall x\ \ \lfloor A[t/y]\rfloor$	$\lfloor \exists x\ \ A\rfloor[t/y]$	$= \exists x\ \ \lfloor A[t/y]\rfloor$	**

*: *$y{\neq}x$, y frei in A, x frei in t, z neue Variable*

**: *$y{\neq}x$, y nicht frei in A oder x nicht frei in t*

Substitution ausgewertet

$$\lfloor(\forall y\ \mathtt{R(+(x,y))} \land \exists x\ \mathtt{x=y}) \land \mathtt{P(x)}\rfloor[\mathtt{-(y,4)/x}]$$

$$= \lfloor(\forall y\ \mathtt{R(+(x,y))} \land \exists x\ \mathtt{x=y})\rfloor[\mathtt{-(y,4)/x}]$$
$$\land\ \lfloor\mathtt{P(x)}\rfloor[\mathtt{-(y,4)/x}]$$

$$= (\forall z\ \lfloor\mathtt{R(+(x,z))} \land \exists x\ \mathtt{x=z}\rfloor[\mathtt{-(y,4)/x}])$$
$$\land\ \mathtt{P(-(y,4))}$$

$$= (\forall z\ \lfloor\mathtt{R(+(x,z))}\rfloor[\mathtt{-(y,4)/x}] \land \lfloor\exists x\ \mathtt{x=z}\rfloor[\mathtt{-(y,4)/x}])$$
$$\land\ \mathtt{P(-(y,4))}$$

$$= (\forall z\ \mathtt{R(+(-(y,4),z))} \land \exists x\ \mathtt{x=z}) \land \mathtt{P(-(y,4))}$$

Refinement Logic: Prädikatenlogische Regeln

Simuliere $\iota_x^u(A)$ durch $\iota(A[t/x])$

– $\iota(\forall x\ \ A)$ = wahr, wenn $\iota_x^u(A)$ = wahr für alle $u \in \iota(T)$

– $\forall x\ \ A$ ist gültig, wenn $A[x'/x]$ gültig ist für eine neue Variable x'

- Die Interpretation von x' ist nicht weiter festgelegt
  also muß A für jede Zuordnung eines Objekts u zu x' wahr sein

– $\iota(\exists x\ \ A)$ = wahr, wenn $\iota(A[t/x])$ = wahr für einen Term t

– $\exists x\ \ A$ ist gültig, wenn $A[t/x]$ gültig ist für einen Term t

Elimination (links)	Introduktion (rechts)
`allE` i t $\Gamma,\ \forall x\ \ A,\ \Delta \vdash C$ $\Gamma,\ \forall x\ \ A,\ A[t/x],\ \Delta \vdash C$	$\Gamma \vdash \forall x\ \ A$ `allI` * $\Gamma \vdash A[x'/x]$
`exE` i ** $\Gamma,\ \exists x\ \ A,\ \Delta \vdash C$ $\Gamma,\ A[x'/x],\ \Delta \vdash C$	$\Gamma \vdash \exists x\ \ A$ `exI` t $\Gamma \vdash A[t/x]$

**: Die Umbenennung $[x'/x]$ kann entfallen, wenn x nicht frei in Γ vorkommt*

***: Die Umbenennung $[x'/x]$ kann entfallen, wenn x nicht frei in C, Γ, Δ vorkommt*

KORREKTHEIT UND VOLLSTÄNDIGKEIT DES KALKÜLS

- **Alle Theoreme sind gültig**
  - C Theorem $\equiv\ \vdash C$ hat vollständigen Beweis
  - Beweis durch strukturelle Induktion über Beweisbaum
  - Blätter sind Regelanwendungen ohne Teilziele (`falseE`, `hypothesis`)
  - Knoten im Beweisbaum sind Regelanwendungen

  $\mapsto$ Es reicht, die "Korrektheit" aller Regeln zu zeigen

- **Alle gültigen Formeln sind beweisbar**
  - Beschreibe systematische Beweisprozedur
    - Erzeuge alle möglichen Substitutionen aller Quantoren (ineffizient!)
  - Zeige: wenn Prozedur nicht terminiert, ist die Formel widerlegbar

  $\mapsto$ Details aufwendig – mehr später bei Tableauxverfahren

Prädikatenlogik – Grenzen

- **Universelle Sprache mit wenigen Vorgaben**
  – Flexibel, aber zu wenig Struktur (nur logische Konnektive)
- **Keine Schlüsse über Werte von Termen möglich**
  – Interpretation von Gleichheit (z.B. `4+4=8`) ist nicht festgelegt
- **Kein Schließen über Datentypen möglich**
  – Welche Struktur und welche Elemente hat ein Datentyp?
  – Interpretation von $\forall x\ x{=}0 \lor x{\geq}1$ nicht festgelegt
- **Erweiterung durch Axiome unpraktisch**
  \+ alle guten Eigenschaften der Logik bleiben erhalten
  – Formales Schließen mühsam (zu viele Teilformeln)
- **Erweiterung von Semantik und Inferenzsystem**
  – Mehr Theorie: Korrektheit, Vollständigkeit etc. muß neu bewiesen werden
  \+ Formales Schließen "natürlich" und einfacher

Mehr in "Automatisierte Logik und Programmierung"