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, $x \in \mathcal{V}$)

Konventionen sparen Klammern

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

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

- **Prioritäten zwischen verschiedenen Konnektiven**

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

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

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

  $\exists x\ A \wedge B$ entspricht $\exists x\ (A \wedge B)$

  Achtung: Unterschiedliche Konventionen in verschiedenen Lehrbüchern

- **Rechtsassoziativität bei Iteration von $\wedge$, $\vee$, $\Rightarrow$**

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

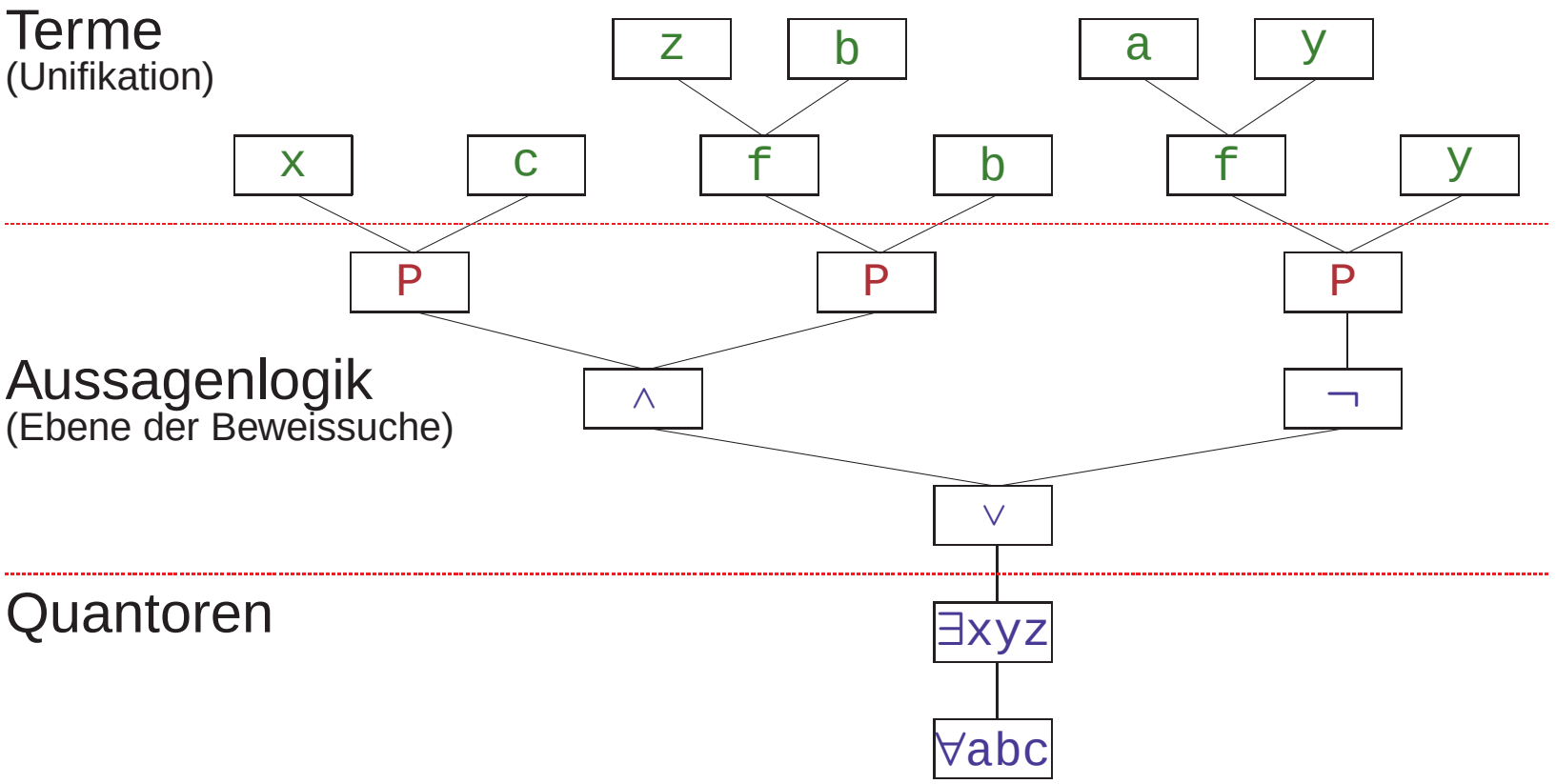
- **Keine Klammern bei Funktions-/Prädikatssymbolen**

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

  – $\exists xyz\ A$ 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** $\forall abc\,\exists xyz\;\; Pxc \wedge P(fzb,b) \vee \neg P(fay,y)$



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 $\mathcal{U}$ $(x \in \mathcal{V})$
  - $\iota(f)$ n-stellige Funktion $\varphi : \mathcal{U}^n \to \mathcal{U}$ $(f \in \mathcal{F}^n)$
  - $\iota(P)$ Funktion $\Pi : \mathcal{U}^n \to \{\mathsf{wahr}, \mathsf{falsch}\}$ $(P \in \mathcal{P}^n)$
- **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

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

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

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

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

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

$\iota^u_x(x) = u$, sonst $\iota^u_x = \iota$

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

Semantik der Prädikatenlogik (II) – klassisch

Fortsetzung von ι auf zusammengesetzte Formeln

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

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

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

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

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

$\iota^u_x(x) = u$, sonst $\iota^u_x = \iota$

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

Ist das wirklich dasselbe?

Modelle und Gültigkeit

- **Modell $\mathcal{M}$ von A** **($\mathcal{M} \models A$)**
  - Interpretation $\mathcal{M} = (\iota, \mathcal{U})$ mit $\iota(A) =$ 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: $\mathcal{E} \cup \{E\} \models F$ genau dann, wenn $\mathcal{E} \models E \Rightarrow F$

- **Theorie $\mathcal{T}$**
  - Erfüllbare Formelmenge mit allen Formeln, die daraus logisch folgen

Syntaktische Manipulation formaler Ausdrücke unter Berücksichtigung der Semantik

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

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

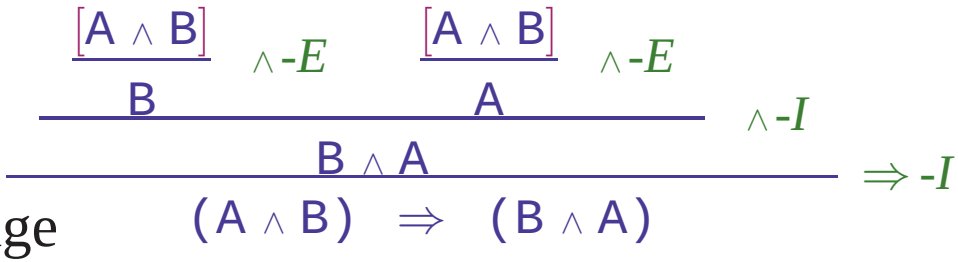
- **Regelschema** $\dfrac{A_1, \ldots, A_n}{C}$: *aus* $\underbrace{A_1 \ und \ \ldots A_n}_{Prämissen}$ *folgt* $\underbrace{C}_{Konklusion}$
  - **Axiom**: Regel ohne Prämissen
  - $\Gamma \vdash_{rs} C$: Konkrete Anwendung des Regelschemas rs
- **Theorem**
  - Formel, die sich durch Anwendung endlich 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

Kalküle sind Hilfsmittel, keine Beweismethode

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



- **Analytisch**

```
⊢ A∧B ⇒ B∧A   BY impI
  \ A∧B ⊢ B∧A   BY andE 1
    \ A, B ⊢ B∧A   BY andI
      |\ A, B ⊢ B   BY hypothesis 2
       \ A, B ⊢ A   BY hypothesis 1
```

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

Verdichtung entfernt Redundanz aus Beweisen

- **Formale Logik und Semantik** ✓
  - Repräsentation mathematischer Aussagen in präziser Sprache
  - Beweise sind mathematische Argumente auf Basis der Semantik
- **Kalkül des natürlichen Schließens ($\mathcal{NK}$)** ↦ "Angewandte Logik"
  - Schematische Inferenzfiguren für logische Konnektive
- **Sequenzenkalküle ($\mathcal{LK}$, Refinement Logic)** ↦ nächste Folien
  - Lokale Verwaltung von Annahmen vereinfacht Anwendung von Regeln
  - Analytische Formulierung unterstützt Beweissuche
- **Tableaux-Kalküle** ↦ §2
  - Zusammenfassung strukturell gleichartiger Inferenzregeln in Klassen
- **Matrix-Kalküle** ↦ §3
  - Kompakte Beweisrepräsentation durch Beweisführung im Formelbaum
  - Gezielte Auswahl beweisrelevanter Teilformeln durch Konnektionen
  - Gezielte Instantiierung von Quantoren durch Unifikation

Resolutionskalküle entstanden durch eine andersartige Entwicklung

Sequenzenkalküle

- **Schließen über Aussagen mit Annahmen**
  - Lokale Sicht: keine globale Verwaltung der Annahmen nötig
- **Grundkonzept Sequenz:** $\underbrace{A_1, \ldots, A_n}_{\text{Antezedent } \Gamma} \vdash \underbrace{B_1, \ldots, B_m}_{\text{Sukzedent } \Phi}$
  - 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** $A_1 \wedge \ldots \wedge A_n \Rightarrow B_1 \vee \ldots \vee B_m$

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

  - Begriffe Modell, Gültigkeit, Erfüllbarkeit analog
- **Synthetische und analytische Form möglich**
  - Synthetische Form $\mathcal{LK}$ für Beweispräsentation
  - Analytische Form Refinement Logic für interaktive Beweissuche

Synthetische Sequenzenkalküle ($\mathcal{LK}$)

$$\neg\text{–}R\ \frac{\Gamma, A \vdash \Phi}{\Gamma \vdash \Phi, \neg A} \qquad \neg\text{–}L\ \frac{\Gamma \vdash \Phi, A}{\Gamma, \neg A \vdash \Phi}$$

$$\wedge\text{–}R\ \frac{\Gamma \vdash \Phi, A \quad \Gamma \vdash \Phi, B}{\Gamma \vdash \Phi, A \wedge B} \qquad \wedge\text{–}L\ \frac{\Gamma, A \vdash \Phi}{\Gamma, A \wedge B \vdash \Phi} \quad \frac{\Gamma, B \vdash \Phi}{\Gamma, A \wedge B \vdash \Phi}$$

$$\vee\text{–}R\ \frac{\Gamma \vdash \Phi, A}{\Gamma \vdash \Phi, A \vee B} \quad \frac{\Gamma \vdash \Phi, B}{\Gamma \vdash \Phi, A \vee B} \qquad \vee\text{–}L\ \frac{\Gamma, A \vdash \Phi \quad \Gamma, B \vdash \Phi}{\Gamma, A \vee B \vdash \Phi}$$

$$\Rightarrow\text{–}R\ \frac{\Gamma, A \vdash \Phi, B}{\Gamma \vdash \Phi, A \Rightarrow B} \qquad \Rightarrow\text{–}L\ \frac{\Gamma \vdash \Phi, A \quad \Delta, B \vdash \Psi}{\Gamma, \Delta, A \Rightarrow B \vdash \Phi, \Psi}$$

$$\textit{axiom}\ \frac{}{A \vdash A} \qquad \textit{Schnitt}\ \frac{\Gamma \vdash \Phi, A \quad A, \Delta \vdash \Psi}{\Gamma, \Delta \vdash \Phi, \Psi}$$

- **Beweiszeilen verwalten alle Annahmen und Zielformeln**
  - Mehrere Sukzedentenformeln nur für klassische Logik erforderlich
- **Sequenzenbeweis für** $((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \vdash A \quad B \vdash B}{A, A \Rightarrow B \vdash B}\Rightarrow\text{–}L \quad C \vdash C}{A, A \Rightarrow B, B \Rightarrow C \vdash C}\Rightarrow\text{–}L}{A, A \Rightarrow B, (A \Rightarrow B) \wedge (B \Rightarrow C) \vdash C}\wedge\text{–}L}{A, (A \Rightarrow B) \wedge (B \Rightarrow C) \vdash C}\wedge\text{–}L\ (+\text{ Kontraktion!})}{(A \Rightarrow B) \wedge (B \Rightarrow C) \vdash A \Rightarrow C}\Rightarrow\text{–}R}{\vdash ((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow A \Rightarrow C}\Rightarrow\text{–}R$$

Zielorientierte Beweisführung

- **Inferenzregel:** Abbildung von Beweisziel in Teilziele

$$\frac{\Gamma_1 \vdash C_1 \quad \cdots \quad \Gamma_n \vdash C_n}{\Gamma \vdash C \text{ BY } \mathit{rule}}$$

  – 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*

$$\frac{\Gamma, A, B, \Delta \vdash C}{\Gamma, A \wedge B, \Delta \vdash C \text{ BY andE } i}$$

  – Nur eine Formel im Sukzedenten (Sonderregel für klassische Logik)

- **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 die Sequenz $\vdash C$

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	$\Gamma,\ \neg A,\ \Delta \vdash C$ $\Gamma,\ \neg A,\ \Delta \vdash A$	$\Gamma \vdash \neg A$ $\Gamma,\ A \vdash \mathsf{ff}$	`notI`
`falseE` i	$\Gamma,\ \mathsf{ff},\ \Delta \vdash C$	$\Gamma \vdash P \vee \neg P$	`magic`

Die `magic` Regel wird für Schließen in klassischer Logik benötigt

Refinement Logic: Strukturelle Regeln

Regeln sind unabhängig von Prädikatenlogik

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

- `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

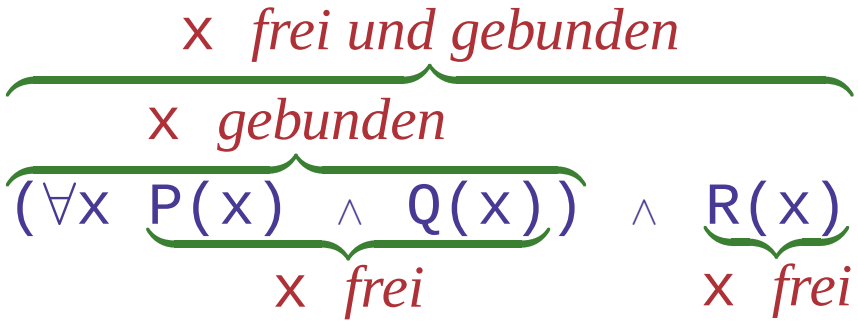
Simuliere ι_x^u durch syntaktische Mechanismen

- **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
- **Variablen**vorkommen **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
  - A heißt geschlossen falls A keine freien Variablen enthält

  Substitution ersetzt nur freie Variablen und bindet keine freien Variablen



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 $u \in \mathcal{U}$

– $\forall x\ A$ 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**
  - Beweis durch strukturelle Induktion über Beweisbaum
    (C Theorem $\equiv$ $\vdash$ C hat vollständigen Beweis)
  - Blätter sind Regelanwendungen ohne Teilziele (`falseE`, `hypothesis`)
  - Knoten im Beweisbaum sind Regelanwendungen
  - Es reicht, die "Korrektheit" aller Regeln einzeln zu zeigen $\mapsto$ Übung
- **Alle gültigen Formeln sind beweisbar**
  - Beschreibe systematische Beweisprozedur
    - Erzeuge alle möglichen Substitutionen aller Quantoren (ineffizient!)
  - Zeige: wenn Prozedur nicht terminiert, ist die Formel widerlegbar
  - Details aufwendig – mehr später bei Tableauxverfahren

ANHANG

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

Frege–Hilbert–Kalküle

- **Sehr viele Axiomenschemata**

(A1) $A \Rightarrow A$
(A2) $A \Rightarrow (B \Rightarrow A)$
(A3) $(A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C))$
(A4) $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$
(A5) $A \Rightarrow A \vee B$
(A6) $A \Rightarrow B \vee A$
(A7) $(A \Rightarrow C) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \vee B \Rightarrow C))$
(A8) $A \wedge B \Rightarrow A$
(A9) $A \wedge B \Rightarrow B$
(A10) $(C \Rightarrow A) \Rightarrow ((C \Rightarrow B) \Rightarrow (C \Rightarrow A \wedge B))$

(A11) $(A \wedge B \vee C) \Rightarrow (A \vee C) \wedge (B \vee C)$
(A12) $(A \vee C) \wedge (B \vee C) \Rightarrow (A \wedge B \vee C)$
(A13) $(A \vee B) \wedge C \Rightarrow (A \wedge C \vee B \wedge C)$
(A14) $(A \wedge C \vee B \wedge C) \Rightarrow (A \vee B) \wedge C$
(A15) $(A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$
(A16) $A \wedge \neg A \Rightarrow B$
(A17) $(A \wedge (A \Rightarrow B)) \Rightarrow B$
(A18) $(A \wedge C \Rightarrow B) \Rightarrow (C \Rightarrow (A \Rightarrow B))$
(A19) $(A \Rightarrow (A \wedge \neg A)) \Rightarrow \neg A$
$\vdots$ $\vdots$

- **Nur eine Inferenzregel**

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

- **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*	$\dfrac{A \wedge B}{A} \qquad \dfrac{A \wedge B}{B}$
$\vee$-*I*	$\dfrac{A}{A \vee B}$	$\dfrac{B}{A \vee B}$	$\vee$-*E*	$\dfrac{A \vee B \qquad \begin{matrix}[A]\\ C\end{matrix} \qquad \begin{matrix}[B]\\ C\end{matrix}}{C}$
$\Rightarrow$-*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: $((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$
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

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

Sequenzenkalküle

- **Modifikation von Natürlicher Deduktion**
  - Schließen über Aussagen mit Annahmen (Mengen von Formeln)
- **Grundkonzept Sequenz:** $\underbrace{A_1, \ldots, A_n}_{\text{Antezedent } \Gamma} \vdash \underbrace{B_1, \ldots, B_m}_{\text{Sukzedent } \Phi}$
  - 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** $A_1 \wedge \ldots \wedge A_n \Rightarrow B_1 \vee \ldots \vee B_m$

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

- **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 ($\text{–}L$)

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

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

$$\neg\text{–}R\ \frac{\Gamma, A \vdash \Phi}{\Gamma \vdash \Phi, \neg A} \qquad \neg\text{–}L\ \frac{\Gamma \vdash \Phi, A}{\Gamma, \neg A \vdash \Phi}$$

$$\wedge\text{–}R\ \frac{\Gamma \vdash \Phi, A \quad \Gamma \vdash \Phi, B}{\Gamma \vdash \Phi, A \wedge B} \qquad \wedge\text{–}L\ \frac{\Gamma, A \vdash \Phi}{\Gamma, A \wedge B \vdash \Phi} \quad \frac{\Gamma, B \vdash \Phi}{\Gamma, A \wedge B \vdash \Phi}$$

$$\vee\text{–}R\ \frac{\Gamma \vdash \Phi, A}{\Gamma \vdash \Phi, A \vee B} \quad \frac{\Gamma \vdash \Phi, B}{\Gamma \vdash \Phi, A \vee B} \qquad \vee\text{–}L\ \frac{\Gamma, A \vdash \Phi \quad \Gamma, B \vdash \Phi}{\Gamma, A \vee B \vdash \Phi}$$

$$\Rightarrow\text{–}R\ \frac{\Gamma, A \vdash \Phi, B}{\Gamma \vdash \Phi, A \Rightarrow B} \qquad \Rightarrow\text{–}L\ \frac{\Gamma \vdash \Phi, A \quad \Delta, B \vdash \Psi}{\Gamma, \Delta, A \Rightarrow B \vdash \Phi, \Psi}$$

$$\textit{axiom}\ \frac{}{A \vdash A} \qquad \textit{Schnitt}\ \frac{\Gamma \vdash \Phi, A \quad A, \Delta \vdash \Psi}{\Gamma, \Delta \vdash \Phi, \Psi}$$

  - 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

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

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 $\dfrac{\Gamma, A \wedge B \vdash \Phi}{\Gamma, A, B \vdash \Phi}\ \wedge L$
  - 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

$\mapsto$ **Refinement Logic:** (Konstruktiver) analytischer Sequenzenkalkül

- Besonders geeignet für computergestützte interaktive Beweisführung

Refinement Logic

Beweisführung durch schrittweise Verfeinerung

- **Analytischer Kalkül**
  - Zielorientiertes Vorgehen durch Top-Down Entwicklung von Beweisen
  - Inferenzregeln zerlegen Beweisziel in "leichtere" Teilaufgaben
- **Sequenzenkalkül**
  - In jedem Beweis(teil-)ziel sind alle Annahmen explizit genannt
  - Technisch: Schließen über Sequenzen (Mengen von Formeln)
  - $H_1,..,H_n \vdash C$ heißt: *"Konklusion C folgt aus Hypothesen $H_1,..,H_n$"*
- **Computergerechte Formalisierung**
  - Hypothesen dargestellt als Liste von Formeln
  - Regeln greifen auf konkrete Hypothesen durch Parameter zu
- **Konstruktive Auslegung**
  - Inferenzregeln zerlegen zusammengesetzte Formeln in ihre Bestandteile bis Konklusion C direkt aus einer Annahme H_i folgt (d.h. $C = H_i$)
  - Klassisches Schließen ermöglicht durch Hinzunahme einer Sonderregel

Beweisregeln folgen direkt aus Semantik

- **Zerlegung einer Konjunktion in der Konklusion**
  - $A \wedge B$ ist gültig wenn A gültig ist und B gültig ist
  - Um $A \wedge B$ zu zeigen, genügt es
    A zu beweisen und B zu beweisen
  - Die Hypothesenliste Γ ändert sich dabei nicht

$\Gamma \vdash A \wedge B$ BY andI
  $\Gamma \vdash A$
  $\Gamma \vdash B$

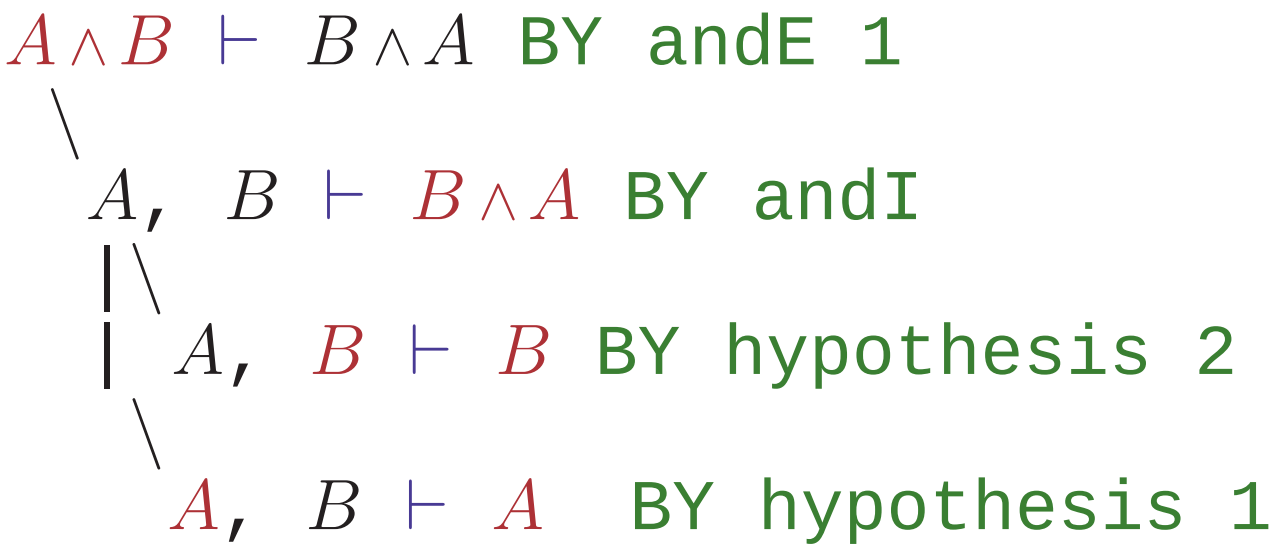
- **Zerlegung einer Konjunktion in den Hypothesen**
  - Wenn eine Aussage C aus den Annahmen A und B folgt,
    dann folgt sie auch aus $A \wedge B$
  - Um $A \wedge B \vdash C$ zu zeigen, genügt es
    $A, B \vdash C$ zu beweisen
  - Die restlichen Hypothesen ändern sich nicht
  - Beweisregel muß Position von $A \wedge B$ angeben

$\Gamma, A \wedge B, \Delta \vdash C$ BY andE i
  $\Gamma, A, B, \Delta \vdash C$

- **Hypothesenregel**
  - Wenn die Konklusion C in den Hypothesen vorkommt,
    dann ist sie bewiesen

$\Gamma, C, \Delta \vdash C$ BY hypothesis i

Beweis für Kommutativität von $\wedge$



Schliessen über Disjunktionen

- **Zerlegung einer Disjunktion in der Konklusion**
  - $A \vee B$ ist gültig wenn A gültig ist oder wenn B gültig ist
  - Um $A \vee B$ zu zeigen, genügt es entweder A oder B zu beweisen
  - Mit der Wahl der Beweisregel wird eine Entscheidung getroffen
  - Die Hypothesenliste ändert sich nicht

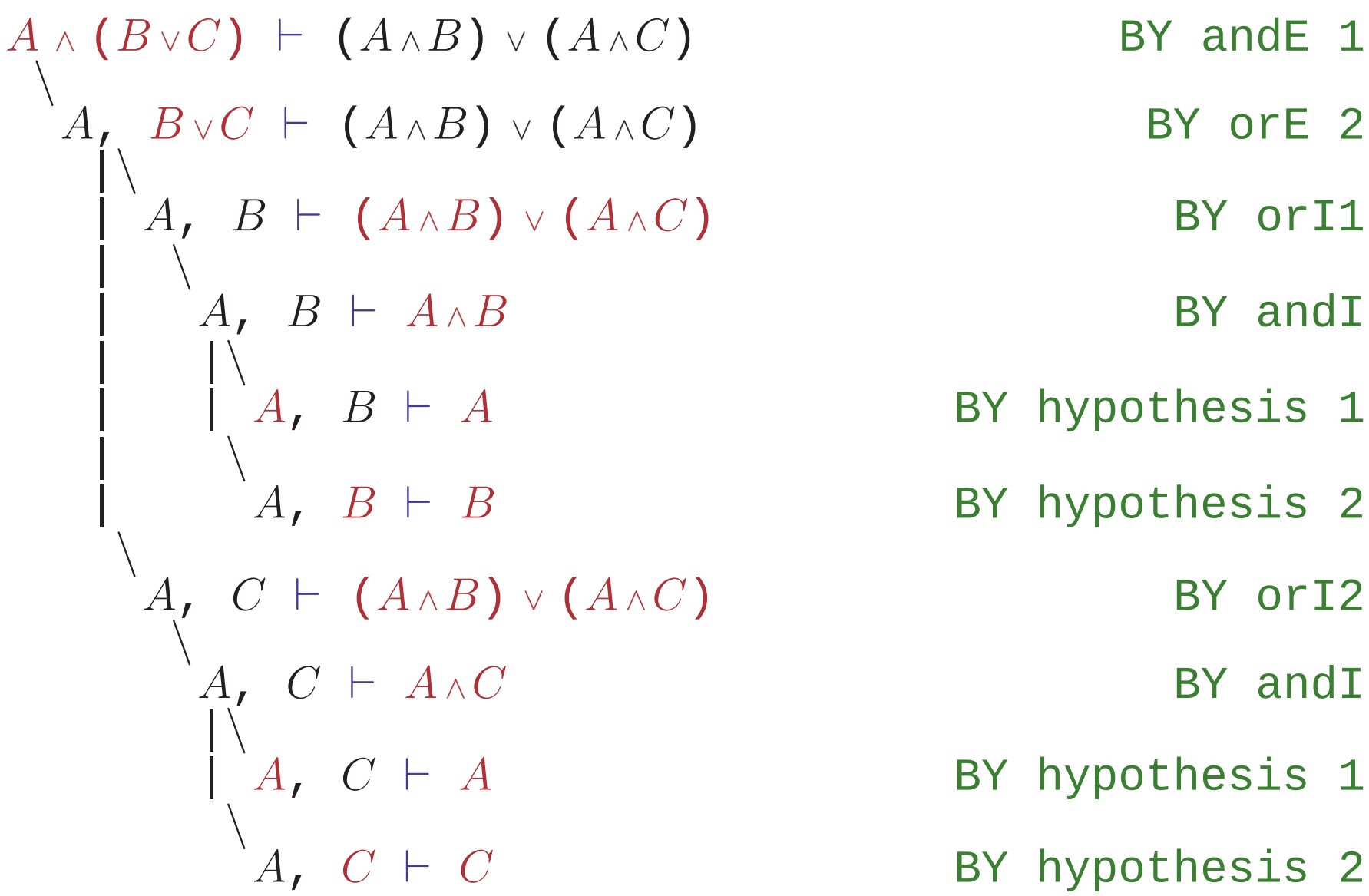
$$\frac{\Gamma \vdash A \vee B \ \texttt{BY orI1}}{\Gamma \vdash A}$$

$$\frac{\Gamma \vdash A \vee B \ \texttt{BY orI2}}{\Gamma \vdash B}$$

- **Zerlegung einer Disjunktion in den Hypothesen**
  - Wenn eine Aussage C aus der Annahmen A und aus der Annahme B folgt, dann folgt sie auch aus $A \vee B$
  - Um $A \vee B \vdash C$ zu zeigen, muß man $A \vdash C$ und $B \vdash C$ beweisen
  - Die restlichen Hypothesen ändern sich nicht
  - Beweisregel muß Position von $A \vee B$ angeben

$$\frac{\Gamma, A \vee B, \Delta \vdash C \ \texttt{BY orE } i}{\Gamma, A, \Delta \vdash C \qquad \Gamma, B, \Delta \vdash C}$$

Beweis für Distributivität von $\wedge$ und $\vee$



Implikation und Negation

- **Zerlegung einer Implikation in der Konklusion**
  - $A \Rightarrow B$ ist gültig wenn B unter der Annahme A gültig ist
  - Um $A \Rightarrow B$ zu zeigen, genügt es A anzunehmen und B zu beweisen
  - Die Beweisregel verschiebt A in die Hypothesen

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\ \texttt{BY impI}$$

- **Zerlegung einer Implikation in den Hypothesen**
  - Wenn eine Aussage C aus der Annahme B folgt und A gültig ist, dann folgt C aus $A \Rightarrow B$
  - Um $A \Rightarrow B \vdash C$ zu zeigen, muß man $B \vdash C$ und $\vdash A$ beweisen
  - Die restlichen Hypothesen ändern sich nicht
  - Beweisregel muß $A \Rightarrow B$ erhalten

$$\frac{\Gamma, A \Rightarrow B, \Delta \vdash A \qquad \Gamma, \Delta, B \vdash C}{\Gamma, A \Rightarrow B, \Delta \vdash C}\ \texttt{BY impE } i$$

- **Zerlegung einer Negation**
  - $\neg A$ ist dasselbe wie $A \Rightarrow \mathsf{ff}$
  - Die Regeln für Negation entsprechen denen der Implikation
  - Jede Aussage folgt unter der Annahme ff ($\mathsf{ff} \vdash C$ ist gültig)

Currying zwischen Implikation und Konjunktion

$\vdash (A \wedge B \Rightarrow C) \Rightarrow (A \Rightarrow B \Rightarrow C)$ BY impI

$A \wedge B \Rightarrow C \vdash A \Rightarrow B \Rightarrow C$ BY impI

$A \wedge B \Rightarrow C,\ A \vdash B \Rightarrow C$ BY impI

$A \wedge B \Rightarrow C,\ A,\ B \vdash C$ BY impE 1

$A \wedge B \Rightarrow C,\ A,\ B \vdash A \wedge B$ BY andI

$A \wedge B \Rightarrow C,\ A,\ B \vdash A$ BY hypothesis 2

$A \wedge B \Rightarrow C,\ A,\ B \vdash B$ BY hypothesis 3

$A,\ B,\ C \vdash C$ BY hypothesis 3

Sonstige Inferenzregeln

- **Einfügen von Zwischenbehauptungen**
  - C ist gültig wenn A gilt und C aus der Annahme A folgt
  - Um C zu zeigen, kann man eine Zwischenbehauptung A beweisen und C unter der Annahme A beweisen
  - A kann eine beliebige "Schnitt"-Formel sein
  - Inferenzregel muß A als Parameter haben
  - Beweise werden signifikant kürzer, wenn A mehrfach benutzt wird

$$\frac{\Gamma \vdash A \qquad \Gamma, A \vdash C}{\Gamma \vdash C \text{ BY cut } A}$$

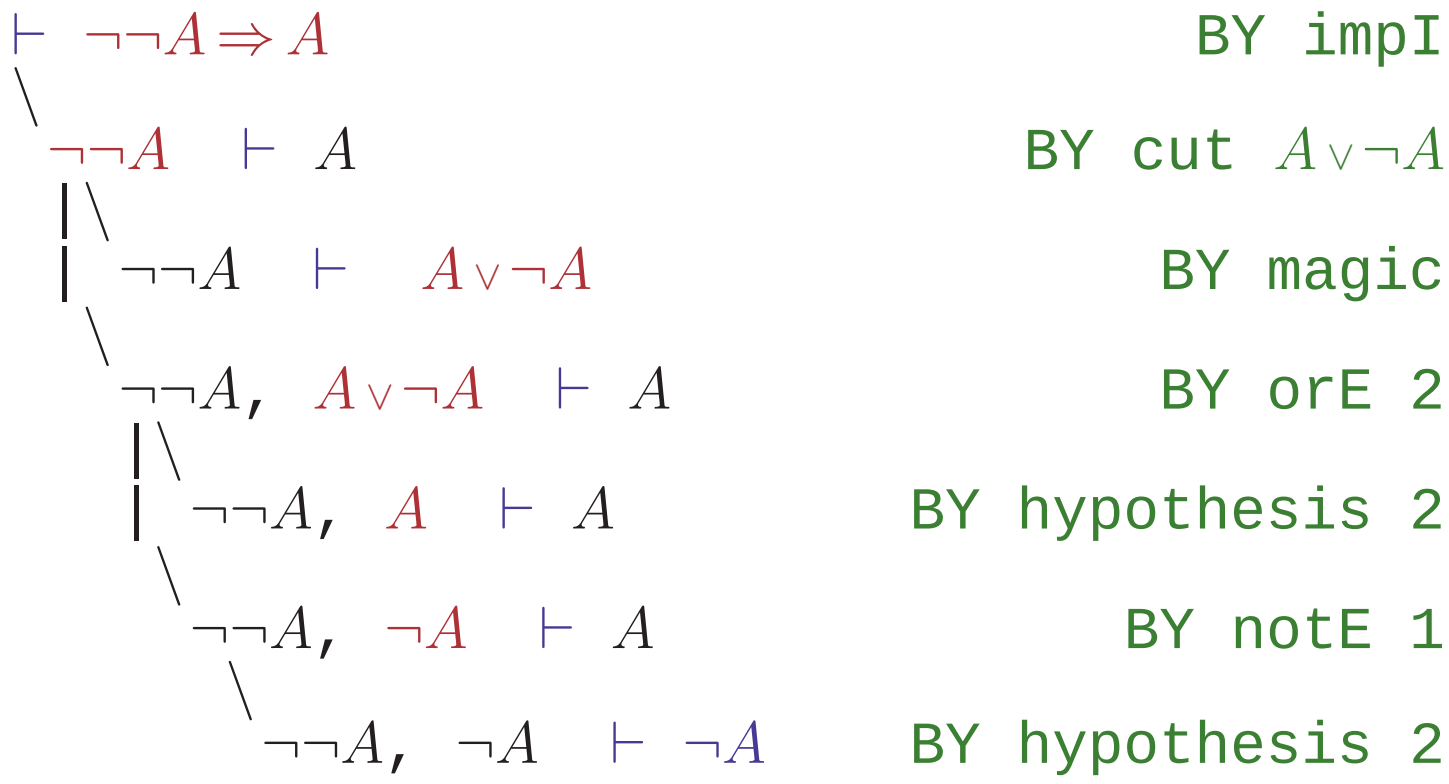
- **Ausdünnen der Annahmen**
  - Hypothesen, die nicht gebraucht werden, können entfernt werden
  - Beweise werden übersichtlicher

$$\frac{\Gamma, \Delta \vdash C}{\Gamma, A, \Delta \vdash C \text{ BY thin } i}$$

- **Klassisches Schließen**
  - Das Gesetz vom Ausgeschlossenen Dritten wird als gültig postuliert

$$\Gamma \vdash A \vee \neg A \text{ BY magic}$$

Klassische Behandlung der doppelten Negation



Refinement Logic: Aussagenlogische Regeln

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	$\Gamma,\ \neg A,\ \Delta \vdash C$ $\Gamma,\ \neg A,\ \Delta \vdash A$	$\Gamma \vdash \neg A$ $\Gamma,\ A \vdash \mathsf{ff}$	notI
falseE i	$\Gamma,\ \mathsf{ff},\ \Delta \vdash C$	$\Gamma \vdash P \vee \neg P$	magic
hypothesis i thin i	$\Gamma,\ A,\ \Delta \vdash A$ $\Gamma,\ A,\ \Delta \vdash C$ $\Gamma,\ \Delta \vdash C$	$\Gamma,\ \Delta \vdash C$ $\Gamma,\ \Delta \vdash A$ $\Gamma,\ A,\ \Delta \vdash C$	cut i A

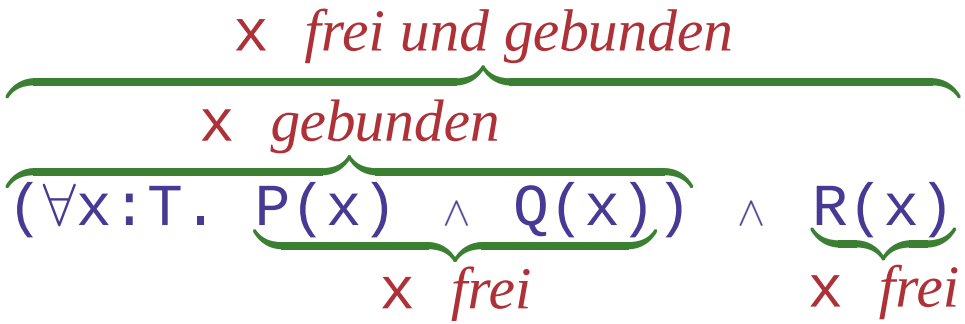
Formale Behandlung von Quantoren

- **Zerlegung eines Allquantors in der Konklusion**
  - $\forall x{:}T.A$ ist gültig wenn $\iota_x^u(A)$ für jeden möglichen Wert u wahr ist
  - Um $\forall x{:}T.A$ zu zeigen, nimmt man an $x{:}T$ sei beliebig aber fest und beweist dann A für dieses x
  - Der Name x ist ein Platzhalter für einen beliebigen Wert u
  - Wenn der Name x in den Hypothesen bereits vorkommt, wählt man einen neuen Namen y und ersetzt x in A durch y
- **Zerlegung eines Existenzquantors**
  - $\exists x{:}T.A$ ist gültig wenn $\iota_x^u(A)$ für einen Wert u wahr ist
  - Um $\exists x{:}T.A$ zu zeigen, beschreibt man einen konkreten Wert durch einen Term t und beweist A für diesen Term
  - Formal muß der Name x in A durch den Term t ersetzt werden

Simuliere ι_x^u syntaktisch durch Substitution $A[t/x]$

Vorkommen von Variablen präzisiert

- x — die Variable x kommt frei vor; $y{\neq}x$ kommt nicht vor.
  ff: — die Variable x kommt nicht vor
- $f(t_1, ..., t_n)$, $t_1{=}t_2$, $P(t_1, ..., t_n)$ — freie Vorkommen von x in t_i bleiben frei; gebundene Vorkommen von x bleiben gebunden.
- $\neg A$, (A), $A \wedge B$, $A \vee B$, $A \Rightarrow B$ — freie Vorkommen von x in A, B bleiben frei; gebundene Vorkommen von x bleiben gebunden.
- $\forall x{:}T\,.\,A$, $\exists x{:}T\,.\,A$ — beliebige Vorkommen von x in A werden gebunden; Vorkommen von $y{\neq}x$ in A bleiben unverändert.



Substitution $A[t/x]$ formal

Endliche Abbildung σ 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 $\sigma\,\sigma = \sigma$)

$\lfloor x \rfloor[t/x]$	$= t$	$\lfloor x \rfloor[t/y]$	$= x$ $(y{\neq}x)$
$\lfloor f(t_1, .., t_n) \rfloor\sigma$	$= f(t_1\sigma, .., t_n\sigma)$	$\lfloor \mathsf{ff} \rfloor\sigma$	$= \mathsf{ff}$
$\lfloor P(t_1, .., t_n) \rfloor\sigma$	$= P(t_1\sigma, .., t_n\sigma)$	$\lfloor t_1 = t_2 \rfloor\sigma$	$= t_1\sigma = t_2\sigma$
$\lfloor \neg A \rfloor\sigma$	$= \neg A\sigma$	$\lfloor A \wedge B \rfloor\sigma$	$= A\sigma \wedge B\sigma$
$\lfloor A \vee B \rfloor\sigma$	$= A\sigma \vee B\sigma$	$\lfloor A \Rightarrow B \rfloor\sigma$	$= A\sigma \Rightarrow B\sigma$
$\lfloor (A) \rfloor\sigma$	$= (A\sigma)$		
$\lfloor \forall x:T\,.\,A \rfloor[t/x]$	$= \forall x:T\,.\,A$	$\lfloor \exists x:T\,.\,A \rfloor[t/x]$	$= \exists x:T\,.\,A$
$\lfloor \forall x:T\,.\,A \rfloor[t/y]$	$= \lfloor \forall z:T\,.\,A[z/x] \rfloor[t/y]$	$\lfloor \exists x:T\,.\,A \rfloor[t/y]$	$= \lfloor \exists z:T\,.\,A[z/x] \rfloor[t/y]$ *
$\lfloor \forall x:T\,.\,A \rfloor[t/y]$	$= \forall x:T\,.\,\lfloor A[t/y] \rfloor$	$\lfloor \exists x:T\,.\,A \rfloor[t/y]$	$= \exists x:T\,.\,\lfloor A[t/y] \rfloor$ **

*: *$y{\neq}x$, 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

$$
\begin{aligned}
&\lfloor(\forall y{:}T.\ R(+(x,y)) \wedge \exists x{:}T.\, x{=}y) \wedge P(x)\rfloor[-(y,4)/x] \\
=\ &\lfloor(\forall y{:}T.\ R(+(x,y)) \wedge \exists x{:}T.\, x{=}y)\rfloor[-(y,4)/x] \\
&\quad \wedge \lfloor P(x)\rfloor[-(y,4)/x] \\
=\ &(\forall z{:}T.\ \lfloor R(+(x,z)) \wedge \exists x{:}T.\, x{=}z\rfloor[-(y,4)/x]) \\
&\quad \wedge P(-(y,4)) \\
=\ &(\forall z{:}T.\ \lfloor R(+(x,z))\rfloor[-(y,4)/x] \wedge \lfloor\exists x{:}T.\, x{=}z\rfloor[-(y,4)/x]) \\
&\quad \wedge P(-(y,4)) \\
=\ &(\forall z{:}T.\ R(+(-(y,4),z)) \wedge \exists x{:}T.\, x{=}z) \wedge P(-(y,4))
\end{aligned}
$$

Refinement Logic: Prädikatenlogische Regeln

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

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

– $\forall x:T\,.\,A$ 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

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

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

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

Beweis für Distributivität von $\wedge$ und $\forall$

$\forall x{:}T.\,P(x) \wedge Q(x) \vdash (\forall x{:}T.\,P(x)) \wedge (\forall x{:}T.\,Q(x))$ BY andI

- $\forall x{:}T.\,P(x) \wedge Q(x) \vdash \forall x{:}T.\,P(x)$ BY allI
  - $\forall x{:}T.\,P(x) \wedge Q(x),\ x{:}T \vdash P(x)$ BY allE 1 x
    - $\forall x{:}T.\,P(x) \wedge Q(x),\ x{:}T,\ P(x) \wedge Q(x) \vdash P(x)$ BY andE 3
      - $\forall x{:}T.\,P(x) \wedge Q(x),\ x{:}T,\ P(x),\ Q(x) \vdash P(x)$ BY hypothesis 3
- $\forall x{:}T.\,P(x) \wedge Q(x) \vdash \forall x{:}T.\,Q(x)$ BY allI
  - $\forall x{:}T.\,P(x) \wedge Q(x),\ x{:}T \vdash Q(x)$ BY allE 1 x
    - $\forall x{:}T.\,P(x) \wedge Q(x),\ x{:}T,\ P(x) \wedge Q(x) \vdash Q(x)$ BY andE 3
      - $\forall x{:}T.\,P(x) \wedge Q(x),\ x{:}T,\ P(x),\ Q(x) \vdash Q(x)$ BY hypothesis 4