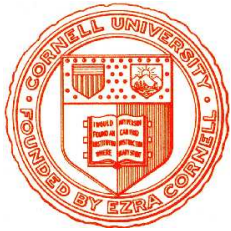


Automatisierte Logik und Programmierung

Einheit 3

Refinement Logic



1. Inferenzsystem

- Aussagenlogischer Kalkül
- Substitution und Quantorenregeln
- Gleichheitsbehandlung

2. Korrektheit und Vollständigkeit

3. Beweismethodik und Strategien

● 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)
- $H_1, \dots, H_n \vdash C$ heißt: *Konklusion C folgt aus Hypothesen $H_1, \dots, H_n$*

● 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

REFINEMENT LOGIC: GRUNDKONZEPTE PRÄZISIERT

● **Sequenz:** $H_1, \dots, H_n \vdash C$

- $\Gamma = H_1, \dots, H_n$ **Hypothesenliste**,
- H_i ist Formel oder **Deklaration** $x:T$ ($x \in \mathcal{V}, T \in \mathcal{T}$),
- C ist einzelne Formel (**Konklusion**)
- Semantik entspricht $H_1, \dots, H_n \Rightarrow C$
- Homomorphe Fortsetzung von Interpretationen

$$\iota(H_1, \dots, H_n \vdash C) = \begin{cases} \text{wahr} & \text{falls aus } \iota(H_1) = \text{wahr} \\ & \text{und } \dots \iota(H_n) = \text{wahr} \\ & \text{immer } \iota(C) = \text{wahr} \text{ folgt} \\ \text{falsch} & \text{sonst} \end{cases}$$

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

● **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**

$$\boxed{\begin{array}{c} \Gamma \vdash C \quad \text{BY rule} \\ \Gamma_1 \vdash C_1 \\ \vdots \\ \Gamma_n \vdash C_n \end{array}}$$

$$\boxed{\begin{array}{c} \Gamma, A \wedge B, \Delta \vdash C \quad \text{BY andE} \\ \Gamma, A, B, \Delta \vdash C \end{array}}$$

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

$$\begin{array}{l} \Gamma \vdash A \wedge B \text{ BY andI} \\ \Gamma \vdash A \\ \Gamma \vdash B \end{array}$$

● 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

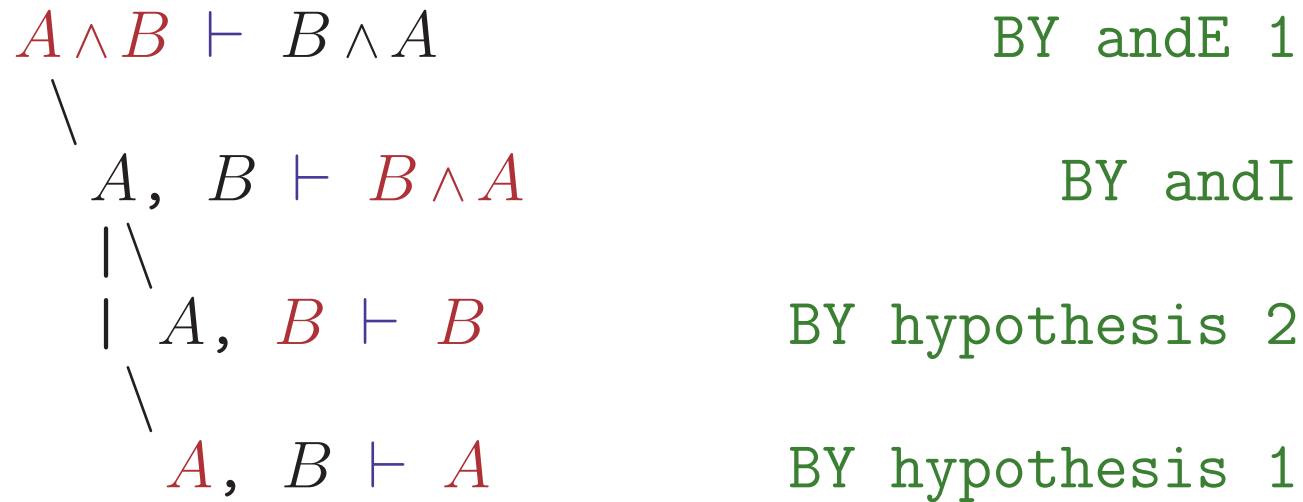
$$\begin{array}{l} \Gamma, A \wedge B, \Delta \vdash C \text{ BY andE } i \\ \Gamma, A, B, \Delta \vdash C \end{array}$$

● Hypothesenregel

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

$$\Gamma, C, \Delta \vdash C \text{ BY hypothesis } i$$

BEWEIS FÜR KOMMUTATIVITÄT VON $\wedge$



- **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 $\vdash C$

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

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

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

● 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

$$\frac{\Gamma, A \vee B, \Delta \vdash C \quad \text{BY orE}}{\Gamma, \Delta \vdash C}$$

BEWEIS FÜR DISTRIBUTIVITÄT VON $\wedge$ UND $\vee$

$A \wedge (B \vee C) \vdash (A \wedge B) \vee (A \wedge C)$	BY andE 1
$A, B \vee C \vdash (A \wedge B) \vee (A \wedge C)$	BY orE 2
$A, B \vdash (A \wedge B) \vee (A \wedge C)$	BY orI1
$A, B \vdash A \wedge B$	BY andI
$A, B \vdash A$	BY hypothesis 1
$A, B \vdash B$	BY hypothesis 2
$A, C \vdash (A \wedge B) \vee (A \wedge C)$	BY orI2
$A, C \vdash A \wedge C$	BY andI
$A, C \vdash A$	BY hypothesis 1
$A, C \vdash C$	BY hypothesis 2

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

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

● 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

$$\frac{\Gamma, A \Rightarrow B, \Delta \vdash C \text{ BY impE} \quad \Gamma, A \Rightarrow B, \Delta \vdash A}{\Gamma, \Delta, B \vdash C}$$

● Zerlegung einer Negation

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

CURRYING ZWISCHEN IMPLIKATION UND KONJUNKTION

$\vdash (A \wedge B \Rightarrow C) \Rightarrow (A \Rightarrow B \Rightarrow C)$	BY impI
$\backslash$ $A \wedge B \Rightarrow C \vdash A \Rightarrow B \Rightarrow C$	BY impI
$\backslash$ $A \wedge B \Rightarrow C, A \vdash B \Rightarrow C$	BY impI
$\backslash$ $A \wedge B \Rightarrow C, A, B \vdash C$	BY impE 1
$\begin{array}{l} \backslash \\ A \wedge B \Rightarrow C, A, B \vdash A \wedge B \end{array}$	BY andI
$\begin{array}{l} \quad \backslash \\ \quad A \wedge B \Rightarrow C, A, B \vdash A \end{array}$	BY hypothesis 2
$\begin{array}{l} \quad \quad \backslash \\ \quad \quad A \wedge B \Rightarrow C, A, B \vdash B \end{array}$	BY hypothesis 3
$\backslash$ $A, B, C \vdash C$	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

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

● Ausdünnen der Annahmen

- Hypothesen, die nicht gebraucht werden, können entfernt werden
- Beweise werden übersichtlicher

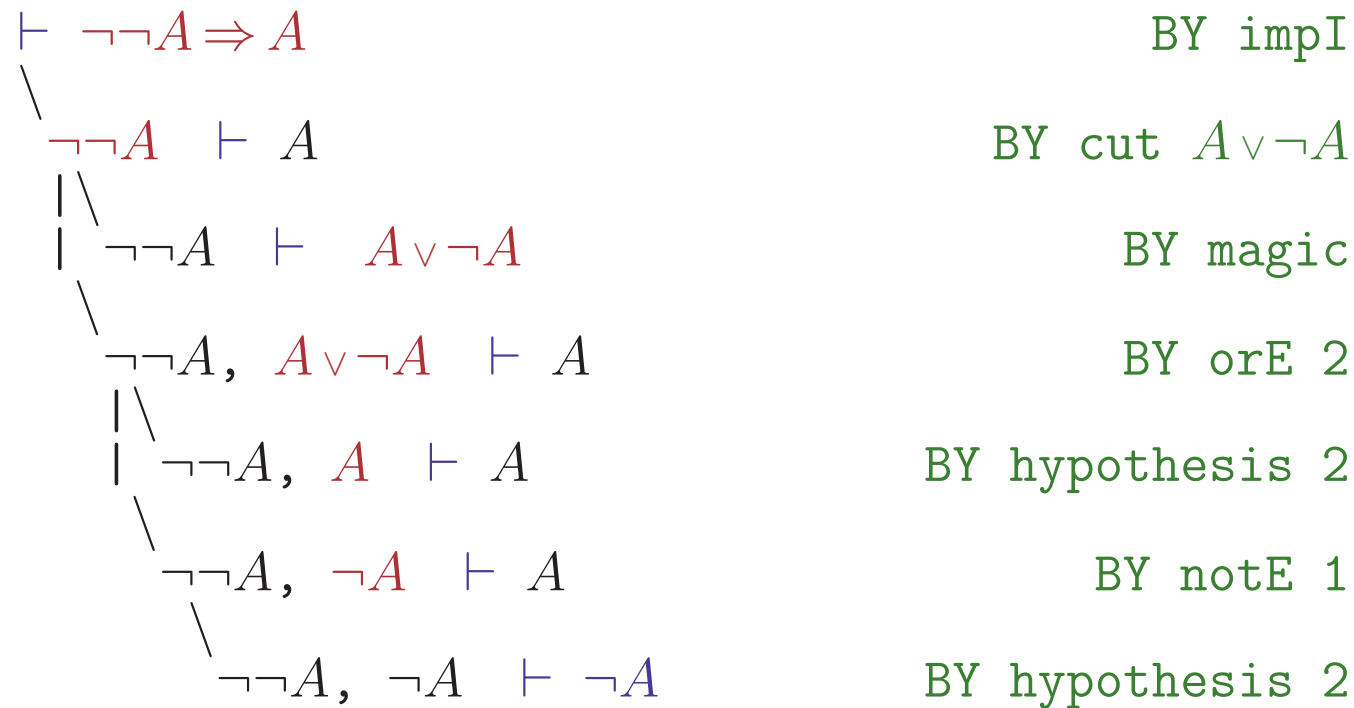
$$\frac{\Gamma, A, \Delta \vdash C}{\Gamma, \Delta \vdash C} \text{ BY thin } i$$

● 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>i</i>	$\begin{array}{c} \Gamma, A \wedge B, \Delta \vdash C \\ \Gamma, A, B, \Delta \vdash C \end{array}$	$\begin{array}{c} \Gamma \vdash A \wedge B \\ \Gamma \vdash A \\ \Gamma \vdash B \end{array}$	andI
orE <i>i</i>	$\begin{array}{c} \Gamma, A \vee B, \Delta \vdash C \\ \Gamma, A, \Delta \vdash C \\ \Gamma, B, \Delta \vdash C \end{array}$	$\begin{array}{c} \Gamma \vdash A \vee B \\ \Gamma \vdash A \\ \Gamma \vdash A \vee B \\ \Gamma \vdash B \end{array}$	orI1 orI2
impE <i>i</i>	$\begin{array}{c} \Gamma, A \Rightarrow B, \Delta \vdash C \\ \Gamma, A \Rightarrow B, \Delta \vdash A \\ \Gamma, \Delta, B \vdash C \end{array}$	$\begin{array}{c} \Gamma \vdash A \Rightarrow B \\ \Gamma, A \vdash B \end{array}$	impI
notE <i>i</i>	$\begin{array}{c} \Gamma, \neg A, \Delta \vdash C \\ \Gamma, \neg A, \Delta \vdash A \end{array}$	$\begin{array}{c} \Gamma \vdash \neg A \\ \Gamma, A \vdash \text{ff} \end{array}$	notI
falseE <i>i</i>	$\Gamma, \text{ff}, \Delta \vdash C$	$\Gamma \vdash P \vee \neg P$	magic
hypothesis <i>i</i>	$\Gamma, A, \Delta \vdash A$	$\begin{array}{c} \Gamma, \Delta \vdash C \\ \Gamma, \Delta \vdash A \end{array}$	cut <i>i</i> A
thin <i>i</i>	$\begin{array}{c} \Gamma, A, \Delta \vdash C \\ \Gamma, \Delta \vdash C \end{array}$	$\begin{array}{c} \Gamma, \Delta \vdash A \\ \Gamma, A, \Delta \vdash C \end{array}$	

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

Beweis braucht syntaktische Simulation von ι_x^u

- **Semantik von Quantoren verwendet ι_x^u**

- $\iota(\forall x:T.A)$ und $\iota(\exists x:T.A)$ 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
- Syntaktischer Beweis muß stattdessen Formel A modifizieren

- **Formales Konzept: Substitution $A[t/x]$**

- Viele alternative Schreibweisen (sehr häufig $A\{x \setminus t\}$)
- 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
 - $\exists x:T.A(x)$ hat dieselbe Bedeutung wie $\exists y:T.A(y)$
- Keine Ersetzung von x durch t in $(\exists x:\mathbb{N}.x \leq 4)[t/x]$
 - Das “äußere” x hat mit dem innerhalb des Quantors nichts zu tun
- Keine Ersetzung von x durch y in $(\exists y:\mathbb{N}.x < y)[y/x]$
 - 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 $A[x]$: 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
- $f(t_1, \dots, t_n)$ freie Vorkommen von x in t_i bleiben frei
 $t_1 = t_2$ gebundene Vorkommen von x bleiben gebunden.
 $P(t_1, \dots, t_n)$
- $\neg A, (A)$ freie Vorkommen von x in A, B bleiben frei
 $A \wedge B, A \vee B$ gebundene Vorkommen von x bleiben gebunden.
 $A \Rightarrow B$
- $\forall x:T. A$ beliebige Vorkommen von x in A werden gebunden
 $\exists x:T. A$ Vorkommen von $y \neq x$ in A bleiben unverändert.

$$\begin{array}{c}
 \text{x frei und gebunden} \\
 \hline
 \text{x gebunden} \\
 \hline
 (\forall \text{x:T. } \underbrace{P(\text{x}) \wedge Q(\text{x})}_{\text{x frei}}) \wedge \underbrace{R(\text{x})}_{\text{x frei}}
 \end{array}$$

SUBSTITUTION $A[t/x]$ FORMAL

Endliche Abbildung σ von Variablen in Terme

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

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

*: $y \neq x$, 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

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

REFINEMENT LOGIC: PRÄDIKATENLOGISCHE REGELN

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

- $\iota(\forall x:T.A) = \text{wahr}$, wenn $\iota_x^u(A) = \text{wahr}$ 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
- $\iota(\exists x:T.A) = \text{wahr}$, wenn $\iota(A[t/x]) = \text{wahr}$ 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 $i \ t$	$\Gamma, \forall x:T.A, \Delta \vdash C$ $\Gamma, \forall x:T.A, A[t/x], \Delta \vdash C$	$\Gamma \vdash \forall x:T.A$ $\Gamma, x':T \vdash A[x'/x]$	allI $*$
exE $i \ **$	$\Gamma, \exists x:T.A, \Delta \vdash C$ $\Gamma, x':T, A[x'/x], \Delta \vdash C$	$\Gamma \vdash \exists x:T.A$ $\Gamma \vdash A[t/x]$	exI t

$*$: 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

GLEICHHEITSBEHANDLUNG IM SEQUENZENKALKÜL

reflexivity

$$\Gamma \vdash t=t$$

symmetry

$$\begin{array}{l} \Gamma \vdash t_1=t_2 \\ \Gamma \vdash t_2=t_1 \end{array}$$

transitivity u

$$\begin{array}{l} \Gamma \vdash t_1=t_2 \\ \Gamma \vdash t_1=u \\ \Gamma \vdash u=t_2 \end{array}$$

substitution $t_1=t_2$

$$\begin{array}{l} \Gamma \vdash C \\ \Gamma \vdash t_1=t_2 \\ \Gamma \vdash C[t_2/t_1] \quad (\text{Termersetzung !}) \end{array}$$

Substitution subsumiert Regeln
für Transitivität und Symmetrie

SEQUENZENBEWEIS FÜR TRANSITIVITÄT DER GLEICHHEIT

$$\begin{array}{lcl} \vdash (t_1=u \wedge u=t_2) \Rightarrow t_1=t_2 & & \text{BY impI} \\ \swarrow & & \\ t_1=u \wedge u=t_2 \vdash t_1=t_2 & & \text{BY andE 1} \\ \swarrow & & \\ t_1=u, u=t_2 \vdash t_1=t_2 & & \text{BY substitution } t_1=u \\ \begin{array}{l} | \backslash \\ | \end{array} & & \\ \begin{array}{l} | \\ | \end{array} t_1=u, u=t_2 \vdash t_1=u & & \text{BY hypothesis 1} \\ \swarrow & & \\ t_1=u, u=t_2 \vdash u=t_2 & & \text{BY hypothesis 2} \end{array}$$

REFINEMENT LOGIC: KORREKTHEIT

ALLE THEOREME DER REFINEMENT LOGIC SIND GÜLTIG

- **C Theorem $\hat{=} \vdash C$ hat vollständigen Beweis**

- Knoten im Beweisbaum sind Regelanwendungen
- Blätter sind Regelanwendungen ohne Teilziele (**falseE**, **hypothesis**)

- **Strukturelle Induktion über Beweisbaum**

“Wenn $\Gamma \vdash C$ einen vollständigen Beweis hat, so ist $\Gamma \vdash C$ gültig”

- **Basisfall**: Anwendung von **falseE** oder **hypothesis** liefert keine Teilziele
- **Schrittfall**: Regelanwendung liefert Teilziele (mit vollständigem Beweis)

In beiden Fällen ist nur die **Korrektheit der angewandten Regel** zu zeigen

- *“ $\Gamma \vdash C$ ist gültig, wenn alle Teilziele $\Gamma_i \vdash C_i$ gültig sind”*

- **Beispiel: Korrektheit von **impI****

- Sei $\Gamma, A \vdash B$ gültig, ι beliebig
- dann ist $\iota(\Gamma, A \vdash B)$ =wahr
- also $\iota(B)$ =wahr, wann immer $\iota(\Gamma)$ =wahr und $\iota(A)$ =wahr
- also $\iota(A \Rightarrow B)$ =wahr, wann immer $\iota(\Gamma)$ =wahr
- also $\iota(\Gamma \vdash A \Rightarrow B)$ =wahr ✓

$\Gamma \vdash A \Rightarrow B$	BY impI
$\Gamma, A \vdash B$	

REFINEMENT LOGIC: VOLLSTÄNDIGKEIT

ALLE GÜLTIGEN FORMELN HABEN EINEN VOLLSTÄNDIGEN BEWEIS

- **Nicht jeder Sequenzenbeweisansatz terminiert**
... auch nicht wenn Formel gültig ist
- **Beschreibe systematische Beweisprozedur** (ineffizient!)
 - Methode zählt alle möglichen Substitutionen für alle Quantoren auf
 - Sequenzenbeweis ist unendlich, wenn Prozedur nicht terminieren kann
- **Systematische Prozedur liefert “Entscheidung”**
 - Unendliche Sequenzenbeweise haben offene Zweige
 - Offene Zweige in Sequenzenbeweisen sind **uniform widerlegbar**
 - Interpretiere jede atomare Formel links als **wahr**, rechts als **falsch**
- Gültige Formeln haben (endliche) vollständige Beweise** ✓
- **Details des Vollständigkeitsbeweises sind aufwendig**
 - **Hintikka Konstruktion** für Kalkül $\mathcal{LK}$ mit mehreren Konklusionen
 - Transformation: $\mathcal{LK}$ Beweise $\mapsto$ Sequenzenkalkül mit einer Konklusionen

TAKTIKEN UND BEWEISSTRATEGIEN

- **Konservative Erweiterung des Regelsystems**
 - Taktiken sind **definitorische Abkürzung** für komplexe Regelanwendungen
- **Erzeugung durch einfache Verknüpfung von Regeln**
 - Formale metasprachliche Ausdrücke liefern einfache Taktiksprache (**ML**)
 - r_1 **THEN** r_2 : Führe Regel r_2 direkt nach r_1 aus
 - r_1 **OR ELSE** r_2 : Führe Regel r_2 aus, wenn r_1 nicht anwendbar ist
 - Repeat** r : Führe Regel r solange wie möglich aus
 - Formulierung komplexer Taktiken und Beweisstrategien ebenfalls möglich
- **Keine Vergrößerung der Beweiskraft**
 - Beweise mit elementaren Regeln durch Expansion rekonstruierbar
 - Ermöglicht gleichzeitig ein kleines Grundinferenzsystem und flexible Präsentation von Beweisen (kürzer, bessere Struktur)

SEQUENZENKALKÜL: BEWEISMETHODIK

- **Kalkül garantiert Korrektheit formaler Beweise**

- Keine Methode um Beweise zu finden
- Systematische Beweisprozedur im Vollständigkeitsbeweis ist ineffizient

- **Es gibt Leitlinien für erfolgreiche Beweissuche**

- Versuche vorrangig Zweige abzuschließen (**falseE**, **hypothesis**)
- Verwende Dekompositionsregeln, die Formeln äquivalent aufbrechen
- Verwende **orE** vor **orI1** / **orI2**
- Verwende **exE** und **allI** vor **exI** und **allE**
- Wähle anwendbare Regel, welche die wenigsten Teilziele erzeugt

Methodik ist als Taktik **prover** programmierbar

- **Beweismethodik läßt Fragen offen**

- Auswahl der Substitution für Quantoren erfordert “Vorausschau”
- Maschinennahe Methoden finden Substitution durch **Unifikation**

Mehr dazu in der Vorlesung “Inferenzmethoden”

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 $\forall x:\mathbb{N}. x=0 \vee x\geq 1$ nicht festgelegt
- **Erweiterung durch Axiome unpraktisch**
 - + alle Eigenschaften der Logik bleiben erhalten
 - Formales Schließen mühsam (vgl. Hilberttyp-Kalküle)



Erweitere Semantik und Inferenzsystem

- + Formales Schließen “natürlich” und einfacher
- Mehr Theorie: Korrektheit, Vollständigkeit etc. neu zu beweisen