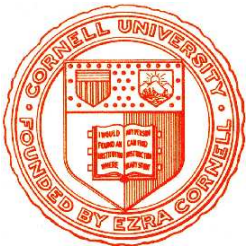


Automatisierte Logik und Programmierung

Einheit 9

Formale Inferenz in der Typentheorie



1. Verifikation und Evidenzkonstruktion
2. Universen und Gleichheitstypen
3. Formale Regeln und Beweise
4. Einbettung der Prädikatenlogik
5. Entwurfsentscheidungen im Rückblick

Beweisen durch Verfeinerung typentheoretischer Urteile

- **Syntaktische Simulation semantischer Schlüsse**
 - Formaler Nachweis, daß bestimmte Urteile gefällt werden können
 - Inferenzregeln ersetzen semantische Argumente
- **Beweise operieren zielorientiert**
 - Oberstes Beweisziel ist die Behauptung, daß ein bestimmtes Urteil tatsächlich gefällt werden kann
 - Inferenzregeln verfeinern ein Ziel in Teilziele, welche den Voraussetzungen für das Fällen des semantischen Urteils entsprechen
 - Verfeinerungskalkül unterstützt Suche nach Beweisen
- **Beweisziele müssen hypothetische Urteile repräsentieren**
 - Syntaktisches Gegenstück ist Sequenz $x_1:T_1, \dots, x_n:T_n \vdash J$
 - Initialsequenz $\vdash J$ beschreibt Urteil ohne Annahmen

UNTERSTÜTZUNG FÜR ALLE ASPEKTE DES SCHLIESSENS

- **Es gibt verschiedene Zielrichtungen formaler Beweise**
 - Typzugehörigkeitsprüfung: zeige $t \in T$ (Type-Checking, Verifikation)
 - Gleichheitsschließen: zeige $s=t \in T$ (Auswertung von Programmen)
 - Witness-Finding zeige Existenz eines Terms t mit $t \in T$
(Synthese von Programmen, Evidenz für logische Aussagen, vgl. §3)
 - Schließen über Typ-Sein und Typ-Gleichheit
- **Beweiskalkül muß einheitlichen Formalismus anbieten**
 - Gleichheitsurteile subsumieren Typ-Sein und Typzugehörigkeit
 - **Universen** können Typ-Eigenschaft syntaktisch darstellen (Folie 3)
aber Girard's Paradox muß vermieden werden
 - Alle vier Urteilklassen sind durch Gleichheitsurteil $s=t \in T$ darstellbar
- **Gleichheit kann Witness-Finding nicht darstellen**
 - Kalkül soll Evidenz/Programme konstruieren und nicht nur überprüfen
 - Beweisziel $\vdash T$ (*Konstruiere Element des Typs T*) wäre die beste Form
 - Urteil $s=t \in T$ kann durch Gleichheitstyp repräsentiert werden (Folie 5)

Syntaktische Repräsentation des Konzepts “Typ-Sein”

- **Typ-Sein ist ein semantisches Konzept**
 - Beschreibung der Rolle eines Ausdrucks als Repräsentant eines Typs
 - Abhängigkeiten werden semantisch charakterisiert
 $x:S \rightarrow T \text{ Typ}$, falls $S \text{ Typ}$ und $T[s/x] \text{ Typ}$ für alle $s \in S$
 - Voraussetzungen beziehen sich immer auf konkrete Typen
Typ-wertige Funktionen sind nicht erforderlich (aber nützlich)
- **Beweiskalkül benötigt syntaktische Simulation**
 - $T \text{ Typ}$ könnte syntaktisch durch $T \in \mathbb{U}$ beschrieben werden
 - Ausdruck \mathbb{U} ist Repräsentant des Universums aller Typen
- **Semantik muß Ausdruck \mathbb{U} eine Bedeutung geben**
 - Formulierung $T \in \mathbb{U}$ verlangt, daß \mathbb{U} selbst ein Typ ist (§8, Folie 10)
 - $\mathbb{U} \in \mathbb{U}$ darf nicht gelten, also ist \mathbb{U} Element eines höheren Universums
 - Liefert Universenhierarchie $\mathbb{U} = \mathbb{U}_1 \in \mathbb{U}_2 \in \mathbb{U}_3 \in \dots$
 - Klassifizierung des Typs typ-wertiger Funktionen $f:S \rightarrow \mathbb{U}_i$ verlangt
kumulative Universenhierarchie: $\mathbb{U} = \mathbb{U}_1 \subseteq \mathbb{U}_2 \subseteq \mathbb{U}_3 \subseteq \dots$

Syntaktische Repräsentation der Typ-Eigenschaft

- **Ausdrücke**

Kanonisch: \mathbb{U}_j j natürliche Zahl oder Variable

Nichtkanonisch: —

- **Reduktion von Ausdrücken**

– entfällt, da keine spezifischen Terme für Universen existieren

- **Urteile für Typ- und Elementgleichheit**

$S = T$ falls $S=T \in \mathbb{U}_j$

$\mathbb{U}_i = \mathbb{U}_j$ falls i identisch mit j (*als natürliche Zahl bzw. Variable*)

$x_1:S_1 \rightarrow T_1 = x_2:S_2 \rightarrow T_2 \in \mathbb{U}_j$ falls $S_1=S_2 \in \mathbb{U}_j$ und $T_1[s_1/x_1]=T_2[s_2/x_2] \in \mathbb{U}_j$
für alle Terme s_1, s_2 mit $s_1=s_2 \in S_1$.

$x_1:S_1 \times T_1 = x_2:S_2 \times T_2 \in \mathbb{U}_j$ falls $S_1=S_2 \in \mathbb{U}_j$ und $T_1[s_1/x_1]=T_2[s_2/x_2] \in \mathbb{U}_j$
für alle Terme s_1, s_2 mit $s_1=s_2 \in S_1$.

⋮

$\{\} = \{\} \in \mathbb{U}_j$

— *analog für alle anderen Datentypen* —

— *für alle j !* —

$\mathbb{U}_i = \mathbb{U}_k \in \mathbb{U}_j$

falls i identisch mit k und k kleiner als j (*als Zahl*)

Kumulativität wird dadurch erreicht, daß Basistypen zu jedem \mathbb{U}_j gehören

Integration von Gleichheit in logische Aussagen

- **Fundamental für fast alle mathematischen Schlüsse**
 - Die meisten logischen Prädikate sind durch Gleichheiten zu beschreiben
- **Nicht dasselbe wie definitorische Gleichheit $A \equiv B$**
 - Definitorische Gleichheit ist ein syntaktisch-linguistisches Konzept
Zwei Ausdrücke werden als **identisch** deklariert
 - Propositionale Gleichheit ist **Gleichheit von Werten**, z.B. $2+2 = 2^2$
- **Nicht dasselbe wie Gleichheitsurteile $s=t \in T$**
 - Gleichheitsurteile stellen die Gültigkeit einer Gleichheit fest
 - Propositionale Gleichheiten sind nur Behauptungen, die auch ungültig sein können, z.B. $2+2 = 3$
 - Propositionale Gleichheiten können mit Konnektiven verbunden werden

- **Essentiell für Argumente mit Gleichheitsannahmen**

- Viele Typdefinitionen haben Voraussetzungen, in den hypothetische Urteile mit Gleichheitsannahmen verwendet werden

$\lambda x_1.t_1 = \lambda x_2.t_2 \in x:S \rightarrow T$ falls $t_1[s_1/x_1] = t_2[s_2/x_2] \in T[s_1/x]$ für alle $s_1 = s_2 \in S$

- Logische Schlüsse verwenden zuweilen komplexe Gleichheitsannahmen
“Aus $\forall x:\mathbb{N}. f(x)=x \Rightarrow f(x+1)=x+1$ und $f(0)=0$ folgt $\forall n:\mathbb{N}. f(n)=n$ ”
- Hypothetische Urteile benötigen mehr als Typzugehörigkeitsannahmen

- **Propositionale Gleichheit als Datentyp**

- Die Annahme $s=t \in T$ bedeutet in Wirklichkeit die Annahme, Evidenz für diese Gleichheit zu besitzen, also ein Element eines Gleichheitstyps
- Die konkrete Evidenz ist eigentlich irrelevant
- Ein Gleichheitstyp ermöglicht eine Formulierung komplexer Annahmen

- **Definiere Gleichheitstyp $s=t$ in T**

- Syntaktische Darstellung ist bewußt ähnlich zum Gleichheitsurteil
- Es gibt nur ein kanonisches Element Ax , das nicht von s, t, T abhängt
- Es gibt keine nichtkanonischen Terme (Evidenz wird nicht analysiert)

FORMULIERUNG EINES GLEICHHEITSTYPS

Schließen mit Werten von Ausdrücken

- **Ausdrücke***

Kanonisch: $s=t \text{ in } T$ s, t und T Terme

Ax

Nichtkanonisch: —

- **Reduktion von Ausdrücken**

– entfällt, da keine nichtkanonischen Terme für Gleichheitstypen

- **Urteile für Typ- und Elementgleichheit**

$s_1=t_1 \text{ in } T_1 = s_2=t_2 \text{ in } T_2$ falls $T_1=T_2$, $s_1=s_2 \in T_1$, und $t_1=t_2 \in T_1$

$Ax = Ax \in s=t \text{ in } T$ falls $s=t \in T$

*: In Nuprl wird der Gleichheitstyp als $s=t \in T$ dargestellt (\in statt **in**)

Wir verwenden diese Form, wenn keine Gefahr der Verwechslung mit Urteilen besteht

ANWENDUNGEN DER PROPOSITIONALEN GLEICHHEIT

- **Der leere Datentyp kann konservativ definiert werden**

- $\{\} \equiv X:\mathbb{U} \rightarrow (X=X \rightarrow X \text{ in } \mathbb{U})$ kann keine Elemente haben

- **Seltsame Eigenschaften von $\{\}$ gelten auch für Simulation**

Für jeden Typ T gilt $\lambda z. (\lambda x. x x) (\lambda x. x x) \in \{\} \rightarrow T$

- Es gilt $t = \lambda z. (\lambda x. x x) (\lambda x. x x) \in \{\} \rightarrow T$ für jedes beliebige T , da

- $t \in \{\} \rightarrow T$ falls $\{\} \rightarrow T$ Typ und $(\lambda x. x x) (\lambda x. x x) \in T$ für alle $s \in \{\}$

- Sei s Element von $\{\} = X:\mathbb{U} \rightarrow (X=X \rightarrow X \text{ in } \mathbb{U})$

- Dann ist $s(T)$ Element von $T=T \rightarrow T$ in \mathbb{U} und reduziert zu Ax

- $Ax \in T=T \rightarrow T$ in \mathbb{U} bedeutet $T = T \rightarrow T \in \mathbb{U}$, also $T = T \rightarrow T$

- Es ist $(\lambda x. x x) (\lambda x. x x) \in T$, wenn $\lambda x. x x$ zu T und zu $T \rightarrow T$ gehört

- $\lambda x. x x \in T \rightarrow T = T$ gilt, falls $x x \in T$ für alle $x \in T$

- $x x \in T$ gilt, falls $x \in T \rightarrow T$ und $x \in T$

- Wegen $T = T \rightarrow T$ und der Annahme $x \in T$ ist beides der Fall

- **Universen und Gleichheit ermöglichen einheitliche Form**
 - Aufgabe von Beweisen wird, Elemente eines Typs zu konstruieren
Beweisziel ist Nachweis von $\vdash T$ “*Typ T besitzt Elemente*”
 - Verifikation von Gleichheiten und Typzugehörigkeit ist simulierbar
Beweisziel wird Nachweis von z.B. $\vdash s=t$ in T
Tatsächliche Aufgabe ist also, Evidenz für $s=t \in T$ zu finden
- **Konstruktion von Elementen durch Verfeinerung**
 - Beweisziel $\vdash T$ wird in Teilziele zerlegt
 - In atomaren Zielen kann ein Element von T direkt konstruiert werden
 - Ansonsten wird Element aus denen der Unterziele zusammengesetzt
 - Konkretes Element des Hauptziels kann erst beschrieben werden, wenn der Beweis vollständig vollendet wurde
 - Element kann (nachträglich) aus Beweis **extrahiert** werden
- **Darstellung von Beweiszielen (in Regeln) ist $\vdash T$ [ext t]**
 - Ziel ist einen noch unbekanntem Term t mit $t \in T$ zu konstruieren

Sechs Arten von Aufgaben können realisiert werden

- **Verifikation: Evidenz für das Fällen von Urteilen**

- *Typ-Sein* “ $T \text{ Typ}$ ”: $\vdash T=T \text{ in } \mathbb{U}_j \text{ [ext } p]$
(Für ein frei gewähltes j zeige Existenz eines Terms p mit $p \in T=T \text{ in } \mathbb{U}_j$)
- *Typgleichheit* “ $S=T$ ”: $\vdash S=T \text{ in } \mathbb{U}_j \text{ [ext } p]$
- *Typzugehörigkeit* “ $t \in T$ ”: $\vdash t=t \text{ in } T \text{ [ext } p]$
- *Elementgleichheit* “ $s=t \in T$ ”: $\vdash s=t \text{ in } T \text{ [ext } p]$

- **Synthese: Konstruktion von Termen**

- *Konstruktion von Datentypen*: $\vdash \mathbb{U}_j \text{ [ext } T]$
- *Konstruktion von Elementen eines Typs*: $\vdash T \text{ [ext } t]$
(Zeige Existenz eines Terms t mit $t \in T$)

(NEUE) DARSTELLUNG VON SEQUENZEN IM KALKÜL

- **Sequenz:** $H \vdash T$ [ext t]

“Unter der Annahme, daß x_i Variablen vom Typ T_i sind, ist T nicht leer (inhabited)”

– $H = x_1:T_1, \dots, x_n:T_n[x_1, \dots, x_{n-1}]$ **Hypothesenliste**, T, t Terme

– $x_i:T_i$ **Deklaration** “ x_i ist Variable vom Typ T_i ” (x_i Variable, T_i Term)

– Notation T [ext t] drückt aus, daß t unbekannt (und unsichtbar) ist

Geschlossene Sequenz:

– Jede freie Variable x in T oder T_i ist zuvor durch $x:T_j$ deklariert

Reine Sequenz:

– Geschlossene Sequenz, in der jede Variable nur einmal deklariert ist

Initialesequenz: Geschlossene Sequenz der Form $\vdash T$ ohne Hypothesen

- **Evidenzterm für $H \vdash T$**

– Term t mit freien Variablen aus den x_i , so daß $t \in T$ gilt,

wenn alle x_i mit Elementen $t_i \in T_i$ instantiiert werden

Eine Sequenz ist **gültig**, wenn es einen Evidenzterm für sie gibt

Definition direkt umsetzbar in Implementierung

INFERENZREGELN SIMULIEREN DEFINITION DER URTEILE

● Verfeinerung eines Verifikationsziels (Gleichheitstyp in Nuprl Darstellung)

$$H \vdash \lambda x_1. t_1 = \lambda x_2. t_2 \in x : S \rightarrow T$$

$$H \vdash S \in \mathbb{U}_j$$

$$H, x' : S \vdash t_1[x'/x_1] = t_2[x'/x_2] \in T[x'/x] \quad \text{lambdaEquality } j \ x'$$

$\lambda x_1. t_1 = \lambda x_2. t_2 \in x : S \rightarrow T$, falls $x : S \rightarrow T$ Typ und $t_1[s_1/x_1] = t_2[s_2/x_2] \in T[s_1/x]$ für alle s_1, s_2 mit $s_1 = s_2 \in S$

- Regel vereinfacht $x : S \rightarrow T$ Typ zu “ S Typ und $T[s_1/x]$ Typ für alle $s_1 \in S$ ”
- Letzteres ist bewiesen, wenn $t_1[s_1/x_1] = t_2[s_2/x_2] \in T[s_1/x]$ gezeigt ist
- S Typ wird durch Wahl des Universums (nur!) hinreichend repräsentiert

● Aufbau von Evidenz

$$H \vdash x : S \rightarrow T \quad \text{[ext } \lambda x'. t]$$

$$H, x' : S \vdash T[x'/x] \quad \text{[ext } t]$$

$$H \vdash S \in \mathbb{U}_j \quad \text{[Ax]} \quad \text{lambdaFormation } j \ x'$$

- Evidenz für Teilziele wird zu Evidenz für Hauptziel zusammengesetzt
 - Evidenz für Verifikation von $S \in \mathbb{U}_j$ hat keine konstruktive Bedeutung
- [ext Ax] wird kurz als [Ax] geschrieben (oder ganz weggelassen)

(NEUE) DARSTELLUNG VON REGELN

- **(Verfeinerungs-)Regel** (dec, val)

- dec **Dekomposition**: Abbildung von Sequenzen in Liste von Sequenzen (Verfeinerung eines **Beweisziels** in Liste von **Teilzielen**)
- val **Validierung**: Abbildung von Liste von Sequenzen und Termen in Terme (Konstruktion von **Evidenz** für Beweisziel aus Evidenzen für Teilziele)
- Regeln werden als **Regelschemata** dargestellt mit Metavariablen als Platzhaltern für Formeln und Evidenzterme
- Konkrete Regeln entstehen hieraus durch Instantiierung der Metavariablen

- **Korrektheit einer Regel** $r = (dec, val)$

Sei $S_0 = H \vdash T$ eine reine Sequenz und seien $S_i = H_i \vdash T_i$ die Resultate der Anwendung von dec auf S_0 . Dann gilt

- Alle Teilzielsequenzen S_i sind rein
- Wenn alle S_i gültig sind, dann ist auch S_0 gültig
- Sind t_i Evidenzterme für S_i , dann ist $t = val(S_0, (S_i, t_i))$ Evidenzterm für S_0

KORREKTHEIT DER REGEL λ Formation

$$H \vdash x:S \rightarrow T \quad [\text{ext } \lambda x'.t]$$

$$H, x':S \vdash T[x'/x] \quad [\text{ext } t]$$

$$H \vdash S \in \mathbb{U}_j \quad [\text{Ax}]$$

λ Formation j x'

- Sei $S_0 = H \vdash x:S \rightarrow T$ eine reine Sequenz und $S_1 = H, x':S \vdash T[x'/x]$ und $S_2 = H \vdash S \in \mathbb{U}_j$
- Alle freien Variablen in H und in $x:S \rightarrow T$ sind genau einmal deklariert. In T kommt x eventuell frei vor, in S nicht. x' ist neu und in $T[x'/x]$ genau einmal deklariert. Damit sind S_1 und S_2 rein.
- Sei t Evidenzterme für S_1 und $t' = \text{Ax}$ Evidenzterm für S_2 . Dann ist $t \in T[s/x]$ ($= T[x'/x][s/x']$) für alle $s \in S$.

Per Definition ist dann auch $\lambda x'.t \in x:S \rightarrow T$ und damit ist auch $\lambda x'.t = \text{val}(S_0, (S_1, t), (S_2, \text{Ax}))$ Evidenzterm für S_0 .

Es folgt, daß S_0 gültig ist, wenn S_1 und S_2 gültig sind

DARSTELLUNG VON BEWEISEN NAHEZU UNVERÄNDERT

● Beweise

- Jede Sequenz $S = H \vdash C$ ist **unvollständiger** Beweis mit **Wurzel** S
- $(S, r, [\pi_1, \dots, \pi_n])$ ist Beweis mit Wurzelsequenz S ,
wenn $r = (dec, val)$ eine korrekte Regel ist und π_i Beweise für alle
Sequenzen S_i sind, die durch Anwendung von dec auf S entstehen
- **vollständiger Beweis**: Beweis ohne unvollständige Teilbeweise
- **Theorem**: vollständiger Beweis, dessen Wurzel eine **Initiaalsequenz** ist

● Extrakterm $ext(\pi)$ eines vollständigen Beweises

- $ext(S, (dec, val), [\pi_1, \dots, \pi_n]) = val([S, (S_1, ext(\pi_1)), \dots, (S_n, ext(\pi_n))])$,
wobei S_i Wurzeln der π_i
- Für $\pi = (S, (dec, val), [])$ liefert dies den Spezialfall $ext(\pi) = val([S])$

(vgl. §3, Folie 21)

Jeder Datentyp benötigt vier Arten von Regeln

• Typ-Formationsregeln:

- Wann sind zwei Typen gleich (typEquality) $H \vdash S = T \in \mathbb{U}_j^*$
- Wie ist ein Typ zusammengesetzt? (typFormation) $H \vdash \mathbb{U}_j \text{ [ext } T]$

• Kanonische Regeln:

- Wann sind kanonische Elemente gleich? (elementEquality) $H \vdash s = t \in T^*$
- Wie sind Elemente zusammengesetzt? $(\text{elementFormation})$ $H \vdash T \text{ [ext } t]$

• Nichtkanonische Regeln:

- Wann sind nichtkanonische Elemente gleich? $(\text{nichtkanonischEquality})$ $H \vdash s = t \in T^*$
- Wie kann man Elemente des Typs nutzen? (typElimination) $H, x:S, H' \vdash T \text{ [ext } t]$

• Berechnungsregeln:

- Reduktion von Redizes in Gleichheit $(\text{nichtkanonischReduce})$ $H \vdash \text{redex} = t \in T^*$

• Spezielle Regeln

*: Evidenz für Verifikationsziele $\vdash s = t \in T$ ist grundsätzlich ohne konstruktive Bedeutung (Ax)

REFINEMENT REGELN FÜR DEN FUNKTIONENRAUM

● Gleichheitsregel für Funktionenräume

– Funktionenräume sind gleich, wenn Argument- und Bildtypen gleich

$$H \vdash x_1:S_1 \rightarrow T_1 = x_2:S_2 \rightarrow T_2 \in \mathbb{U}_j \quad \text{[Ax]}$$

$$H \vdash S_1 = S_2 \in \mathbb{U}_j \quad \text{[Ax]}$$

$$H, x:S_1 \vdash T_1[x/x_1] = T_2[x/x_2] \in \mathbb{U}_j \quad \text{[Ax]}$$

functionEquality x

● Formationsregel für Funktionenräume (wird nicht mehr verwendet)

– Funktionenraum wird als Evidenz für \mathbb{U}_j konstruiert

$$H \vdash \mathbb{U}_j \quad \text{[ext } x:S \rightarrow T]$$

$$H \vdash S \in \mathbb{U}_j \quad \text{[Ax]}$$

$$H, x:S \vdash \mathbb{U}_j \quad \text{[ext } T]$$

functionFormation $x \ S$

● Gleichheits-/Formationsregeln für kanonische Funktionen

$$H \vdash \lambda x_1. t_1 = \lambda x_2. t_2 \in x:S \rightarrow T$$

$$H \vdash S \in \mathbb{U}_j$$

$$H, x':S \vdash t_1[x'/x_1] = t_2[x'/x_2] \in T[x'/x]$$

lambdaEquality $j \ x'$

$$H \vdash x:S \rightarrow T \quad \text{[ext } \lambda x'. t]$$

$$H, x':S \vdash T[x'/x] \quad \text{[ext } t]$$

$$H \vdash S \in \mathbb{U}_j \quad \text{[Ax]}$$

lambdaFormation $j \ x'$

REFINEMENT REGELN FÜR DEN FUNKTIONENRAUM II

- **Gleichheitsregel für Funktionsapplikationen** (nichtkanonisch)
 - Applikationen sind gleich, wenn Funktionen und Argumente gleich

$$H \vdash f_1 t_1 = f_2 t_2 \in T[t_1/x] \quad \text{[Ax]}$$

$$H \vdash f_1 = f_2 \in x:S \rightarrow T \quad \text{[Ax]}$$

$$H \vdash t_1 = t_2 \in S \quad \text{[Ax]}$$

applyEquality $x:S \rightarrow T$

- **Erzeugung nichtkanonischer Elemente**

$$H, f: x:S \rightarrow T, H' \vdash C \quad \text{[ext } t[fs, Ax/y, z]\text{]}$$

$$H, f: x:S \rightarrow T, H' \vdash s \in S \quad \text{[Ax]}$$

$$H, f: x:S \rightarrow T, y:T[s/x], z: y=f s \in T[s/x], H' \vdash C \quad \text{[ext } t\text{]}$$

functionElimination

$i \ s \ y \ z$

- Regel arbeitet auf Hypothesenliste anstatt der Konklusion
- Regel zeigt, wie Element f des Funktionenraums verwendet wird
- Evidenzterm enthält Applikation von f auf angegebenes $s \in S$
- **Reduktionsregel**
 - Redex auf linker Seite einer Gleichheit wird durch Kontraktum ersetzt

$$H \vdash (\lambda x.t) s = t_2 \in T \quad \text{[Ax]}$$

$$H \vdash t[s/x] = t_2 \in T \quad \text{[Ax]}$$

applyReduce

SONDERREGELN

● Regel für Extensionalität von Funktionen

– Funktionen sind gleich, wenn sie auf allen Argumenten gleich sind

Die Regel `lambdaEquality` sichert dies nur für λ -Abstraktionen

$$\begin{array}{ll} H \vdash f_1 = f_2 \in x:S \rightarrow T & [\text{ext } t] \\ H, x':S \vdash f_1 x' = f_2 x' \in T[x'/x] & [\text{ext } t] \\ H \vdash S \in \mathbb{U}_j & [\text{Ax}] \\ H \vdash f_1 \in x_1:S_1 \rightarrow T_1 & [\text{Ax}] \\ H \vdash f_2 \in x_2:S_2 \rightarrow T_2 & [\text{Ax}] \end{array}$$

`functionExtensionality`

$j \ x_1:S_1 \rightarrow T_1 \ x_2:S_2 \rightarrow T_2 \ x'$

– f_1, f_2 können auf Obermengen von S und $T[x]$ definiert sein

– Evidenz für punktweise Gleichheit (meist `Ax`) wird weitergereicht

● Gleichheitsregel für deklarierte Variablen

$$H, x:T, H' \vdash x = x \in T \quad [\text{Ax}] \quad \text{hypothesisEquality } i$$

– Reflexivität gilt nur für Elemente eines Typs (vgl. `declaration` aus §6)

● Formation von Extraktermen aus deklarierten Variablen

$$H, x:T, H' \vdash T \quad [\text{ext } x] \quad \text{hypothesis } i$$

– Eine Variablendeklaration vom Typ T ist Evidenz für T (vgl. `axiom` aus §3)

VIELE REGELN BENÖTIGEN STEUERUNGSPARAMETER

Angabe von Daten, die für Teilziel oder Extraktterm benötigt werden, aber im Beweisziel nicht auftauchen

- **Position i einer Hypothese**

$$H, x:T, H' \vdash T \quad \text{[ext } x] \quad \text{hypothesis } i$$

– Benutzer muß angeben, auf welche Hypothese die Regel zugreifen soll

- **Name x einer neu zu erzeugenden Variablen**

$$\begin{array}{l} H \vdash x_1:S_1 \rightarrow T_1 = x_2:S_2 \rightarrow T_2 \in \mathbb{U}_j \quad \text{[Ax]} \\ H \vdash S_1 = S_2 \in \mathbb{U}_j \quad \text{[Ax]} \\ H, x:S_1 \vdash T_1[x/x_1] = T_2[x/x_2] \in \mathbb{U}_j \quad \text{[Ax]} \end{array} \quad \text{functionEquality } x$$

– Automatische Namenszeugung wäre mehr als nur Pattern Matching

- **Level j des Universums eines (Teil-)typs**

$$\begin{array}{l} H \vdash \lambda x_1. t_1 = \lambda x_2. t_2 \in x:S \rightarrow T \quad \text{[Ax]} \\ H \vdash S \in \mathbb{U}_j \quad \text{[Ax]} \\ H, x':S \vdash t_1[x'/x_1] = t_2[x'/x_2] \in T[x'/x] \quad \text{[Ax]} \end{array} \quad \text{lambdaEquality } j \quad x'$$

– Notwendig für Teilziele, die Typ-Sein eines Ausdrucks prüfen müssen

STEUERUNGSPARAMETER FÜR INFERENZREGELN (II)

- **Term s** , der als spezifische Instanz gebraucht wird

$$\begin{array}{l}
 H, f: x:S \rightarrow T, H' \vdash C \quad \text{[ext } t[f s, Ax/y, z]\text{]} \\
 H, f: x:S \rightarrow T, H' \vdash s \in S \quad \text{[Ax]} \\
 H, f: x:S \rightarrow T, y:T[s/x], z: y=f s \in T[s/x], H' \vdash C \quad \text{[ext } t\text{]}
 \end{array}$$

functionElimination

i s y z

– Term kann Funktionsargument sein oder Variable instantiieren

- **Typ T** eines Teilterms des Beweiszieles

$$\begin{array}{l}
 H \vdash f_1 t_1 = f_2 t_2 \in T[t_1/x] \quad \text{[Ax]} \\
 H \vdash f_1 = f_2 \in x:S \rightarrow T \quad \text{[Ax]} \\
 H \vdash t_1 = t_2 \in S \quad \text{[Ax]}
 \end{array}$$

applyEquality $x:S \rightarrow T$

– Teilterme, die in Unterzielen isoliert auftreten, benötigen einen Typ

- **Abhängigkeit** eines Terms C von einer Variablen x

$$\begin{array}{l}
 H \vdash C[s/x] \quad \text{[ext } u\text{]} \\
 H \vdash s = t \in T \quad \text{[Ax]} \\
 H \vdash C[t/x] \quad \text{[ext } u\text{]} \\
 H, x:T \vdash C \in \mathbb{U}_j \quad \text{[Ax]}
 \end{array}$$

substitution $j \ s=t \in T \ x \ C$

– Ermöglicht Verallgemeinerung einer instantiierten Form des Terms C

ANWENDUNG DER REGELN FÜR DEN FUNKTIONENRAUM

● Konstruktion eines Terms in $x:S \rightarrow (Tx \rightarrow Tx)$

– Deklarationen $S:\mathbb{U}, T:S \rightarrow \mathbb{U}$ sind vorgegeben

$S:\mathbb{U}, T:S \rightarrow \mathbb{U} \vdash x:S \rightarrow (Tx \rightarrow Tx)$	$[\text{ext } \lambda x. (\lambda p. p)]$	lambdaFormation 1 x
1. $S:\mathbb{U}, T:S \rightarrow \mathbb{U}, x:S \vdash Tx \rightarrow Tx$	$[\text{ext } \lambda p. p]$	lambdaFormation 1
1.1. $S:\mathbb{U}, T:S \rightarrow \mathbb{U}, x:S, p:Tx \vdash Tx$	$[\text{ext } p]$	hypothesis 4
1.2. $S:\mathbb{U}, T:S \rightarrow \mathbb{U}, x:S \vdash Tx \in \mathbb{U}$	$[\text{Ax}]$	applyEquality $S \rightarrow \mathbb{U}$
1.2.1. $S:\mathbb{U}, T:S \rightarrow \mathbb{U}, x:S \vdash T \in S \rightarrow \mathbb{U}$	$[\text{Ax}]$	hypothesisEquality 2
1.2.2. $S:\mathbb{U}, T:S \rightarrow \mathbb{U}, x:S \vdash x \in S$	$[\text{Ax}]$	hypothesisEquality 3
2. $S:\mathbb{U}, T:S \rightarrow \mathbb{U}, x:S \vdash S \in \mathbb{U}$	$[\text{Ax}]$	hypothesisEquality 1

– Extraktterm wird nach Vollendung des Beweises generiert

– Gleichheitsziele tragen nicht zum Extraktterm bei

FORMALER BEWEIS EINER TYPZUGEHÖRIGKEIT

$T:\mathbb{U} \vdash (\lambda f.\lambda x. fx)(\lambda z.z) \in T \rightarrow T$	<code>applyEquality (T→T)→(T→T)</code>
1. $T:\mathbb{U} \vdash \lambda f.\lambda x. fx \in (T \rightarrow T) \rightarrow (T \rightarrow T)$	<code>lambdaEquality 1 f</code>
1.1. $T:\mathbb{U}, f:T \rightarrow T \vdash \lambda x. fx \in T \rightarrow T$	<code>lambdaEquality 1 x</code>
1.1.1. $T:\mathbb{U}, f:T \rightarrow T, x:T \vdash fx \in T$	<code>applyEquality T→T</code>
1.1.1.1. $T:\mathbb{U}, f:T \rightarrow T, x:T \vdash f \in T \rightarrow T$	<code>hypothesisEquality 2</code>
1.1.1.2. $T:\mathbb{U}, f:T \rightarrow T, x:T \vdash x \in T$	<code>hypothesisEquality 3</code>
1.1.2. $T:\mathbb{U}, f:T \rightarrow T \vdash T \in \mathbb{U}$	<code>hypothesisEquality 1</code>
1.2. $T:\mathbb{U} \vdash T \rightarrow T \in \mathbb{U}$	<code>functionEquality x</code>
1.2.1. $T:\mathbb{U} \vdash T \in \mathbb{U}$	<code>hypothesisEquality 1</code>
1.2.2. $T:\mathbb{U}, x:T \vdash T \in \mathbb{U}$	<code>hypothesisEquality 1</code>
2. $T:\mathbb{U} \vdash \lambda z.z \in T \rightarrow T$	<code>lambdaEquality 1 z</code>
2.1. $T:\mathbb{U}, z:T \vdash z \in T$	<code>hypothesisEquality 2</code>
2.2. $T:\mathbb{U} \vdash T \in \mathbb{U}$	<code>hypothesisEquality 1</code>

FORMALE ANALYSE VON $\lambda x.x x$

- **Es gilt $\lambda x.x x \notin S \rightarrow T$ für alle Typen S, T**
 - Semantisches Argument in Einheit 8 hat gezeigt, daß das Urteil $\lambda x.x x \in S \rightarrow T$ nicht gefällt werden kann

- **Beweisansätze bleiben unvollständig**

$S:\mathbb{U}, T:\mathbb{U} \vdash \lambda x.x x \in S \rightarrow T$	<code>lambdaEquality 1 x</code>
1. $S:\mathbb{U}, T:\mathbb{U}, x:S \vdash x x \in T$	<code>applyEquality S → T</code>
1.1. $S:\mathbb{U}, T:\mathbb{U}, x:S \vdash x \in S \rightarrow T$	<code>????</code>
1.2. $S:\mathbb{U}, T:\mathbb{U}, x:S \vdash x \in S$	<code>hypothesisEquality 3</code>

- Beweis kann nicht abgeschlossen werden
- Auch alternative Beweisversuche führen nicht zum Erfolg
- **$\lambda x.x x \notin S \rightarrow T$ ist formal nicht beweisbar**
 - Man könnte nur zeigen, daß aus der Annahme $\lambda x.x x \in S \rightarrow T$ jede beliebige Aussage folgen würde

VOLLSTÄNDIGER REGELSATZ FÜR FUNKTIONENRAUM

$H \vdash x_1:S_1 \rightarrow T_1 = x_2:S_2 \rightarrow T_2 \in \mathbb{U}_j$ [Ax]
functionEquality x
 $H \vdash S_1 = S_2 \in \mathbb{U}_j$ [Ax]
 $H, x:S_1 \vdash T_1[x/x_1] = T_2[x/x_2] \in \mathbb{U}_j$ [Ax]

$H \vdash \mathbb{U}_j$ [ext $x:S \rightarrow T$]
functionFormation $x S$
 $H \vdash S \in \mathbb{U}_j$ [Ax]
 $H, x:S \vdash \mathbb{U}_j$ [ext T]

$H \vdash \lambda x_1.t_1 = \lambda x_2.t_2 \in x:S \rightarrow T$ [Ax]
lambdaEquality $j x'$
 $H, x':S \vdash t_1[x'/x_1] = t_2[x'/x_2] \in T[x'/x]$ [Ax]
 $H \vdash S \in \mathbb{U}_j$ [Ax]

$H \vdash x:S \rightarrow T$ [ext $\lambda x'.t$]
lambdaFormation $j x'$
 $H, x':S \vdash T[x'/x]$ [ext t]
 $H \vdash S \in \mathbb{U}_j$ [Ax]

$H \vdash f_1 t_1 = f_2 t_2 \in T[t_1/x]$ [Ax]
applyEquality $x:S \rightarrow T$
 $H \vdash f_1 = f_2 \in x:S \rightarrow T$ [Ax]
 $H \vdash t_1 = t_2 \in S$ [Ax]

$H, f:x:S \rightarrow T, H' \vdash C$ [ext $t[fs, Ax/y, z]$]
functionElimination $i s y z$
 $H, f:x:S \rightarrow T, H' \vdash s \in S$ [Ax]
 $H, f:x:S \rightarrow T, y:T[s/x], z:y=f s \in T[s/x], H' \vdash C$ [ext t]

$H \vdash (\lambda x.t) s = t_2 \in T$ [Ax]
applyReduce
 $H \vdash t[s/x] = t_2 \in T$ [Ax]

$H \vdash f_1 = f_2 \in x:S \rightarrow T$ [ext t]
functionExtensionality $j x_1:S_1 \rightarrow T_1 x_2:S_2 \rightarrow T_2 x'$
 $H, x':S \vdash f_1 x' = f_2 x' \in T[x'/x]$ [ext t]
 $H \vdash S \in \mathbb{U}_j$ [Ax]
 $H \vdash f_1 \in x_1:S_1 \rightarrow T_1$ [Ax]
 $H \vdash f_2 \in x_2:S_2 \rightarrow T_2$ [Ax]

WARUM HABEN REGELN WOHLGEFORMTHEITSZIELE ?

Ohne diese Ziele wären seltsame Beweise möglich

• Verzicht auf $\vdash S \in \mathbb{U}_j$ in lambdaEquality

$$\boxed{\begin{array}{l} H \vdash \lambda x_1. t_1 = \lambda x_2. t_2 \in x : S \rightarrow T \\ H, x' : S \vdash t_1[x'/x_1] = t_2[x'/x_2] \in T[x'/x] \end{array}} \quad \text{lambdaEquality } x'$$

– Modifizierte Regel würde Beweis für unsinnige Aussage ermöglichen

$$\vdash \lambda x. T \in x : (\lambda y. y) \rightarrow \mathbb{B} \quad \text{lambdaEquality } x$$

1. $x : (\lambda y. y) \vdash T \in \mathbb{B}$ *wäre beweisbar mit Regeln für \mathbb{B}*

• Verzicht auf $\vdash C \in \mathbb{U}_j$ in substitution

$$\boxed{\begin{array}{l} H \vdash C[s/x] \quad \text{[ext } u\text{]} \\ H \vdash s = t \in T \quad \text{[Ax]} \\ H \vdash C[t/x] \quad \text{[ext } u\text{]} \end{array}} \quad \text{substitution } s=t \in T \quad x \quad C$$

– Modifizierte Regel würde Beweis mit unsinnigen Argumenten ermöglichen

$$\vdash \text{if } 1+1=2 \text{ then } \mathbb{B} \text{ else } \lambda y. y$$

1. $\vdash 1+1=2 \in \mathbb{N}$ *substitution $1+1=2 \in \mathbb{N} \quad x \quad \text{if } x=2 \text{ then } \mathbb{B} \text{ else } \lambda y. y$*

2. $\vdash \text{if } 2=2 \text{ then } \mathbb{B} \text{ else } \lambda y. y$

– Unterziele sind ok, aber $\text{if } x=2 \text{ then } \mathbb{B} \text{ else } \lambda y. y$ ist für $x \neq 2$ kein Typ

REGELN FÜR PRODUKTRAUM

Regeln ergeben sich direkt aus Semantikdefinition in §8

$$H \vdash x_1:S_1 \times T_1 = x_2:S_2 \times T_2 \in \mathbb{U}_j \quad [\text{Ax}]$$

productEquality x'

$$H \vdash S_1 = S_2 \in \mathbb{U}_j \quad [\text{Ax}]$$

$$H, x':S_1 \vdash T_1[x'/x_1] = T_2[x'/x_2] \in \mathbb{U}_j \quad [\text{Ax}]$$

$$H \vdash \mathbb{U}_j \quad [\text{ext } x:S \times T]$$

productFormation $x S$

$$H \vdash S \in \mathbb{U}_j \quad [\text{Ax}]$$

$$H, x:S \vdash \mathbb{U}_j \quad [\text{ext } T]$$

$$H \vdash \langle s_1, t_1 \rangle = \langle s_2, t_2 \rangle \in x:S \times T \quad [\text{Ax}]$$

pairEquality $j x'$

$$H \vdash s_1 = s_2 \in S \quad [\text{Ax}]$$

$$H \vdash t_1 = t_2 \in T[s_1/x] \quad [\text{Ax}]$$

$$H, x':S \vdash T[x'/x] \in \mathbb{U}_j \quad [\text{Ax}]$$

$$H \vdash x:S \times T \quad [\text{ext } \langle s, t \rangle]$$

pairFormation $j s x'$

$$H \vdash s \in S \quad [\text{Ax}]$$

$$H \vdash T[s/x] \quad [\text{ext } t]$$

$$H, x':S \vdash T[x'/x] \in \mathbb{U}_j \quad [\text{Ax}]$$

$$H \vdash \text{match } e_1 \text{ with } \langle x_1, y_1 \rangle \mapsto t_1 = \text{match } e_2 \text{ with } \langle x_2, y_2 \rangle \mapsto t_2 \in C[e_1/z] \quad [\text{Ax}]$$

spreadEquality $z C x:S \times T s t y$

$$H \vdash e_1 = e_2 \in x:S \times T \quad [\text{Ax}]$$

$$H, s:S, t:T[s/x], y: e_1 = \langle s, t \rangle \in x:S \times T \vdash t_1[s, t/x_1, y_1] = t_2[s, t/x_2, y_2] \in C[\langle s, t \rangle/z] \quad [\text{Ax}]$$

$$H \vdash \text{match } \langle s, t \rangle \text{ with } \langle x, y \rangle \mapsto u = t_2 \in T \quad [\text{Ax}]$$

spreadReduce

$$H \vdash u[s, t/x, y] = t_2 \in T \quad [\text{Ax}]$$

$$H, z: x:S \times T, H' \vdash C \quad [\text{ext match } z \text{ with } \langle s, t \rangle \mapsto u]$$

productElimination $i s t$

$$H, z: x:S \times T, s:S, t:T[s/x] H'[\langle s, t \rangle/z] \vdash C[\langle s, t \rangle/z] \quad [\text{ext } u]$$

REGELN FÜR UNABHÄNGIGE RÄUME SIND EINFACHER

$$H \vdash x_1:S_1 \rightarrow T_1 = x_2:S_2 \rightarrow T_2 \in \mathbb{U}_j \quad \text{[Ax]}$$

functionEquality x

$$H \vdash S_1 = S_2 \in \mathbb{U}_j \quad \text{[Ax]}$$

$$H, x:S_1 \vdash T_1[x/x_1] = T_2[x/x_2] \in \mathbb{U}_j \quad \text{[Ax]}$$

$$H \vdash S_1 \rightarrow T_1 = S_2 \rightarrow T_2 \in \mathbb{U}_j \quad \text{[Ax]}$$

independent_functionEquality

$$H \vdash S_1 = S_2 \in \mathbb{U}_j \quad \text{[Ax]}$$

$$H \vdash T_1 = T_2 \in \mathbb{U}_j \quad \text{[Ax]}$$

$$H, f:x:S \rightarrow T, H' \vdash C \quad \text{[ext } t[f s, \text{Ax}/y, z]\text{]}$$

functionElimination $i \ s \ y \ z$

$$H, f:x:S \rightarrow T, H' \vdash s \in S \quad \text{[Ax]}$$

$$H, f:x:S \rightarrow T, y:T[s/x], z:y=f s \in T[s/x], H' \vdash C \quad \text{[ext } t\text{]}$$

$$H, f:S \rightarrow T, H' \vdash C \quad \text{[ext } t[f s, /y]\text{]}$$

independent_functionElimination $i \ y$

$$H, f:S \rightarrow T, H' \vdash S \quad \text{[ext } s\text{]}$$

$$H, f:S \rightarrow T, y:T, H' \vdash C \quad \text{[ext } t\text{]}$$

$$H \vdash x_1:S_1 \times T_1 = x_2:S_2 \times T_2 \in \mathbb{U}_j \quad \text{[Ax]}$$

productEquality x'

$$H \vdash S_1 = S_2 \in \mathbb{U}_j \quad \text{[Ax]}$$

$$H, x':S_1 \vdash T_1[x'/x_1] = T_2[x'/x_2] \in \mathbb{U}_j \quad \text{[Ax]}$$

$$H \vdash S_1 \times T_1 = S_2 \times T_2 \in \mathbb{U}_j \quad \text{[Ax]}$$

independent_productEquality

$$H \vdash S_1 = S_2 \in \mathbb{U}_j \quad \text{[Ax]}$$

$$H \vdash T_1 = T_2 \in \mathbb{U}_j \quad \text{[Ax]}$$

$$H \vdash x:S \times T \quad \text{[ext } \langle s, t \rangle\text{]}$$

pairFormation $j \ s \ x'$

$$H \vdash s \in S \quad \text{[Ax]}$$

$$H \vdash T[s/x] \quad \text{[ext } t\text{]}$$

$$H, x':S \vdash T[x'/x] \in \mathbb{U}_j \quad \text{[Ax]}$$

$$H \vdash S \times T \quad \text{[ext } \langle s, t \rangle\text{]}$$

independent_pairFormation

$$H \vdash S \quad \text{[ext } s\text{]}$$

$$H \vdash T \quad \text{[ext } t\text{]}$$

$$H \vdash \langle s_1, t_1 \rangle = \langle s_2, t_2 \rangle \in x:S \times T \quad \text{[Ax]}$$

pairEquality $j \ x'$

$$H \vdash s_1 = s_2 \in S \quad \text{[Ax]}$$

$$H \vdash t_1 = t_2 \in T[s_1/x] \quad \text{[Ax]}$$

$$H, x':S \vdash T[x'/x] \in \mathbb{U}_j \quad \text{[Ax]}$$

$$H \vdash \langle s_1, t_1 \rangle = \langle s_1, t_1 \rangle \in S \times T \quad \text{[Ax]}$$

independent_pairEquality

$$H \vdash s_1 = s_2 \in S \quad \text{[Ax]}$$

$$H \vdash t_1 = t_2 \in T \quad \text{[Ax]}$$

FORMALER BEWEIS EINER TYPZUGEHÖRIGKEIT II

$S:\mathbb{U}, T:\mathbb{U} \vdash \lambda p. \text{match } p \text{ with } \langle x, y \rangle \mapsto x \in (S \times T) \rightarrow S$
lambdaEquality 1 p

1. $S:\mathbb{U}, T:\mathbb{U}, p:S \times T \vdash \text{match } p \text{ with } \langle x, y \rangle \mapsto x \in S$
productElimination 3 s t

1.1. $S:\mathbb{U}, T:\mathbb{U}, p:S \times T, s:S, t:T \vdash \text{match } \langle s, t \rangle \text{ with } \langle x, y \rangle \mapsto x \in S$
spreadReduce

1.1.1. $S:\mathbb{U}, T:\mathbb{U}, p:S \times T, s:S, t:T \vdash s \in S$
hypothesisEquality 3

Alternativer Beweis mit spreadEquality

$S:\mathbb{U}, T:\mathbb{U} \vdash \lambda p. \text{match } p \text{ with } \langle x, y \rangle \mapsto x \in (S \times T) \rightarrow S$
lambdaEquality 1 p

1. $S:\mathbb{U}, T:\mathbb{U}, p:S \times T \vdash \text{match } p \text{ with } \langle x, y \rangle \mapsto x \in S$
spreadEquality z S S×T s t z

1.1. $S:\mathbb{U}, T:\mathbb{U}, p:S \times T \vdash p \in S \times T$
hypothesisEquality 3

1.2. $S:\mathbb{U}, T:\mathbb{U}, p:S \times T, s:S, t:T, p = \langle s, t \rangle \in S \times T \vdash s \in S$
hypothesisEquality 4

VOLLSTÄNDIGER REGELSATZ FÜR SUMMENTYP

$H \vdash S_1 + T_1 = S_2 + T_2 \in \mathbb{U}_j$ [Ax] unionEquality $H \vdash S_1 = S_2 \in \mathbb{U}_j$ [Ax] $H \vdash T_1 = T_2 \in \mathbb{U}_j$ [Ax]	$H \vdash \mathbb{U}_j$ [ext $S+T$] unionFormation $H \vdash \mathbb{U}_j$ [ext S] $H \vdash \mathbb{U}_j$ [ext T]
$H \vdash \text{inl}(s_1) = \text{inl}(s_2) \in S+T$ [Ax] inlEquality j $H \vdash s_1 = s_2 \in S$ [Ax] $H \vdash T \in \mathbb{U}_j$ [Ax]	$H \vdash S+T$ [ext $\text{inl}(s)$] inlFormation j $H \vdash S$ [ext s] $H \vdash T \in \mathbb{U}_j$ [Ax]
$H \vdash \text{inr}(t_1) = \text{inr}(t_2) \in S+T$ [Ax] inrEquality j $H \vdash t_1 = t_2 \in T$ [Ax] $H \vdash S \in \mathbb{U}_j$ [Ax]	$H \vdash S+T$ [ext $\text{inr}(t)$] inrFormation j $H \vdash T$ [ext t] $H \vdash S \in \mathbb{U}_j$ [Ax]
$H \vdash \text{case } e_1 \text{ of } \text{inl}(x_1) \mapsto u_1 \mid \text{inr}(y_1) \mapsto v_1 = \text{case } e_2 \text{ of } \text{inl}(x_2) \mapsto u_2 \mid \text{inr}(y_2) \mapsto v_2 \in C[e_1/z]$ [Ax] decideEquality $z \ C \ S+T \ s \ t \ y$ $H \vdash e_1 = e_2 \in S+T$ [Ax] $H, s:S, y: e_1 = \text{inl}(s) \in S+T \vdash u_1[s/x_1] = u_2[s/x_2] \in C[\text{inl}(s)/z]$ [Ax] $H, t:T, y: e_1 = \text{inr}(t) \in S+T \vdash v_1[t/y_1] = v_2[t/y_2] \in C[\text{inr}(t)/z]$ [Ax]	
$H, z:S+T, H' \vdash C$ [ext case z of $\text{inl}(x) \mapsto u \mid \text{inr}(y) \mapsto v$] unionElimination $i \ x \ y$ $H, z:S+T, x:S, H'[\text{inl}(x)/z] \vdash C[\text{inl}(x)/z]$ [ext u] $H, z:S+T, y:T, H'[\text{inr}(y)/z] \vdash C[\text{inr}(y)/z]$ [ext v]	
$H \vdash \text{case } \text{inl}(s) \text{ of } \text{inl}(x) \mapsto u \mid \text{inr}(y) \mapsto v = t_2 \in T$ [Ax] decideReduceLeft $H \vdash u[s/x] = t_2 \in T$ [Ax]	$H \vdash \text{case } \text{inr}(t) \text{ of } \text{inl}(x) \mapsto u \mid \text{inr}(y) \mapsto v = t_2 \in T$ [Ax] decideReduceRight $H \vdash v[t/y] = t_2 \in T$ [Ax]

FORMALER BEWEIS EINER TYPZUGEHÖRIGKEIT III

```
S:U, T:U ⊢ λz. case z of inl(x) ↦ x | inr(y) ↦ (y, y)
    ∈ z:S+T → case z of inl(x) ↦ S | inr(y) ↦ T×T
    lambdaEquality 1 z THEN unionElimination 3 s t

1. S:U, T:U, z:S+T, s:S ⊢ case inl(s) of inl(x) ↦ x | inr(y) ↦ (y, y)
    ∈ case inl(s) of inl(x) ↦ S | inr(y) ↦ T×T
    decideReduceLeft

1.1. S:U, T:U, z:S+T, s:S ⊢ s
    ∈ case inl(s) of inl(x) ↦ S | inr(y) ↦ T×T
    subst* case inl(s) of inl(x) ↦ S | inr(y) ↦ T×T = S ∈ U
    THENL [ decideReduceLeft THEN hypothesisEquality 1
    ; hypothesisEquality 4]

2. S:U, T:U, z:S+T, y:T ⊢ case inr(t) of inl(x) ↦ x | inr(y) ↦ (y, y)
    ∈ case inr(t) of inl(x) ↦ S | inr(y) ↦ T×T
    decideReduceRight
    THEN subst* case inr(t) of inl(x) ↦ S | inr(y) ↦ T×T = T×T ∈ U
    THENL [ decideReduceRight THEN ...; hypothesisEquality 4]
```

* `subst` ist eine Taktik auf Basis der Regel `substitution`, die Parameter automatisch bestimmt

REGELSATZ FÜR {}, UNIVERSEN, GLEICHHEIT

$$\Gamma \vdash \{\} = \{\} \in \mathbb{U}_j \quad \text{[Ax]}$$

voidEquality

$$\Gamma \vdash \text{any}(s) = \text{any}(t) \in T \quad \text{[Ax]}$$

anyEquality

$$\Gamma \vdash s = t \in \{\} \quad \text{[Ax]}$$

$$H \vdash \mathbb{U}_j = \mathbb{U}_j \in \mathbb{U}_k \quad \text{[Ax]}$$

universeEquality ($j < k$)

$$H \vdash T \in \mathbb{U}_k \quad \text{[Ax]}$$

cumulativity j ($j < k$)

$$H \vdash T \in \mathbb{U}_j \quad \text{[Ax]}$$

$$H \vdash s_1 = t_1 \in T_1 = s_2 = t_2 \in T_2 \in \mathbb{U}_j \quad \text{[Ax]}$$

equalityEquality

$$H \vdash T_1 = T_2 \in \mathbb{U}_j \quad \text{[Ax]}$$

$$H \vdash s_1 = s_2 \in T_1 \quad \text{[Ax]}$$

$$H \vdash t_1 = t_2 \in T_1 \quad \text{[Ax]}$$

$$H \vdash \text{Ax} = \text{Ax} \in s = t \in T \quad \text{[Ax]}$$

axiomEquality

$$H \vdash s = t \in T \quad \text{[Ax]}$$

$$H, z: s = t \in T, H' \vdash C \quad \text{[ext } u_i]$$

equalityElimination i

$$H, z: s = t \in T, H'[\text{Ax}/z] \vdash C[\text{Ax}/z] \quad \text{[ext } u_i]$$

$$H, x:T, H' \vdash x = x \in T \quad \text{[Ax]}$$

hypothesisEquality i

$$\Gamma \vdash \mathbb{U}_j \quad \text{[ext } \{\}]$$

voidFormation

$$\Gamma, z: \{\}, H' \vdash C \quad \text{[ext any}(z)]$$

voidElimination i

$$H \vdash \mathbb{U}_k \quad \text{[ext } \mathbb{U}_j]$$

universeFormation j ($j < k$)

$$H \vdash \mathbb{U}_j \quad \text{[ext } s = t \in T]$$

equalityFormation T

$$H \vdash T \in \mathbb{U}_j \quad \text{[Ax]}$$

$$H \vdash T \quad \text{[ext } s]$$

$$H \vdash T \quad \text{[ext } t]$$

$$H \vdash C[s/x] \quad \text{[ext } u_i]$$

substitution j $s=t \in T$ x C

$$H \vdash s = t \in T \quad \text{[Ax]}$$

$$H \vdash C[t/x] \quad \text{[ext } u_i]$$

$$H, x:T \vdash C \in \mathbb{U}_j \quad \text{[Ax]}$$

$$H \vdash s = t \in T \quad \text{[Ax]}$$

equality (Entscheidungsprozedur)

EFFEKTE VON $\{\}$ SIND IM KALKÜL BEWEISBAR

- $\{\} \rightarrow T$ ist Typ, auch wenn T kein Typ ist

- Ausdruck ist für $T = \lambda x. \lambda y. y$ oder $T = 0 = 1 \in 2$ typisierbar

$\vdash \{\} \rightarrow (\lambda x. \lambda y. y) \in \mathbb{U}$	functionEquality x
1. $\vdash \{\} \in \mathbb{U}$	voidEquality
2. $x:\{\} \vdash \lambda x. \lambda y. y \in \mathbb{U}$	voidElimination 1

- Der Term $t = \lambda z. (\lambda x. x x) (\lambda x. x x)$ wird typisierbar

$T:\mathbb{U} \vdash \lambda z. (\lambda x. x x) (\lambda x. x x) \in \{\} \rightarrow T$	lambdaEquality 1 z
1. $T:\mathbb{U}, z:\{\} \vdash (\lambda x. x x) (\lambda x. x x) \in T$	voidElimination 2
2. $T:\mathbb{U} \vdash \{\} \rightarrow T \in \mathbb{U}$	functionEquality x
2.1. $T:\mathbb{U} \vdash \{\} \in \mathbb{U}$	voidEquality
2.2. $T:\mathbb{U}, x:\{\} \vdash T \in \mathbb{U}$	hypothesisEquality 1

- **Starke Normalisierbarkeit gilt nur für Extrakterme**

- Regeln erzeugen keine Terme mit Selbstreferenz

WEITERE REGELN

$$\frac{H, x:T, H' \vdash T}{\text{hypothesis } i} \quad \text{[ext } x]$$

$$\frac{H, H' \vdash C}{\text{cut } i \ T \ x} \quad \text{[ext } (\lambda x. t) \ s]$$

$$\frac{H, H' \vdash T}{H, x:T, H' \vdash C} \quad \begin{array}{l} \text{[ext } s] \\ \text{[ext } t] \end{array}$$

$$\frac{H, z:T, H' \vdash C}{\text{hyp_replacement } i \ S \ j} \quad \text{[ext } t]$$

$$\frac{H, z:S, H' \vdash C}{H, z:T, H' \vdash T = S \in \mathbb{U}_j} \quad \begin{array}{l} \text{[ext } t] \\ \text{[Ax]} \end{array}$$

$$\frac{H \vdash C}{\text{lemma "theorem-name"}} \quad \text{[ext } t]$$

$$\frac{H \vdash C}{\text{instantiate } \Gamma' \ C' \ \sigma} \quad \text{[ext } t[\sigma]]$$

$$\frac{H' \vdash C'}{\text{[ext } t]}$$

$$\frac{H \vdash C}{\text{unfold } \textit{def-name}} \quad \text{[ext } t]$$

$$\frac{H \vdash C_{\downarrow}}{\text{[ext } t]}$$

$$\frac{H, z:T, H' \vdash C}{\text{unfoldHyp } i \ \textit{def-name}} \quad \text{[ext } t]$$

$$\frac{H, z:T_{\downarrow}, H' \vdash C}{\text{[ext } t]}$$

$$\frac{H, x:T, H' \vdash C}{\text{thin } i} \quad \text{[ext } t]$$

$$\frac{H, H' \vdash C}{\text{[ext } t]}$$

$$\frac{H \vdash T}{\text{introduction } t} \quad \text{[ext } t]$$

$$\frac{H \vdash t \in T}{\text{[Ax]}}$$

$$\frac{H \vdash t \in T}{\text{extract "theorem-name"}} \quad \text{[Ax]}$$

$$\frac{H \vdash C}{\text{rename } y \ x} \quad \text{[ext } t[y/x]]$$

$$\frac{\Gamma[x/y] \vdash C[x/y]}{\text{[ext } t]}$$

$$\frac{H \vdash C_{\downarrow}}{\text{fold } \textit{def-name}} \quad \text{[ext } t]$$

$$\frac{H \vdash C}{\text{[ext } t]}$$

$$\frac{H, z:T_{\downarrow}, H' \vdash C}{\text{foldHyp } i \ \textit{def-name}} \quad \text{[ext } t]$$

$$\frac{H, z:T, H' \vdash C}{\text{[ext } t]}$$

WIE SOLL MAN SICH DAS ALLES MERKEN?

WIR HABEN JETZT BEREITS 59 REGELN

- **Viele Regeln folgen der Struktur von Termen**
 - Formations- und Eliminationsregeln zerlegen Typen
 - Gleichheitsregeln zerlegen kanonische/nichtkanonische
 - Reduktionsregeln führen Ein-Schritt Berechnungen aus
 - **Fasse gleichartige Regeln unter einem Namen zusammen**
 - **D** i : Dekomposition eines Terms in Hypothese i (Konklusion $\hat{=} 0$)
 - **EqD** i : Dekomposition einer Gleichheit in Hypothese i
 - **ReduceEquands** i : Evaluation eines Redex in Hypothese i
- Damit sind die meisten Regeln abgedeckt (Details im Nuprl Manual S. 154ff)
- **Bestimme Parameter automatisch, wenn möglich**
 - Neue Variablennamen sind leicht zu erzeugen
 - Universenlevel / Typ von Termen ist oft durch Typechecking zu finden
 - Ansonsten müssen Parameter explizit angegeben werden

Implementierung als Taktiken, die Regeln aufrufen \mapsto ALuP II

- **Logik kann in Typentheorie eingebettet werden**
 - Prinzip “*Propositionen als Datentypen*” macht Aussagen zu Typen
 - Gleichheit ist das grundlegende Prädikat
 - Logische Konnektive entsprechen Typkonstruktoren (vgl. §3, Folie 24)
 - *Curry-Howard Isomorphie* stellt Bezug zwischen Inferenzregeln her
 - Regeln für $\wedge, \vee, \Rightarrow, \neg, \forall, \exists$ entsprechen denen für $\rightarrow, \times, +, \{ \}$
- **Logik wird konservative Erweiterung der Typentheorie**
 - Konnektive sind durch definitorische Gleichheiten definierbar
 - Inferenzregeln sind als Taktiken “programmierbar”
 - Logik kann als Bibliothekskonzept eingeführt werden

Eine echte Erweiterung des Kalküls ist nicht erforderlich

DEFINITORISCHE GLEICHUNGEN FÜR LOGISCHE KONZEPTE

and	$P \wedge Q$	\equiv	$P \times Q$
or	$P \vee Q$	\equiv	$P + Q$
implies	$P \Rightarrow Q$	\equiv	$P \rightarrow Q$
not	$\neg P$	\equiv	$P \rightarrow \{\}$
false	f	\equiv	$\{\}$
exists	$\exists x:T. P[x]$	\equiv	$x:T \times P[x]$
all	$\forall x:T. P[x]$	\equiv	$x:T \rightarrow P[x]$
prop	\mathbb{P}_i	\equiv	\mathbb{U}_i

CURRY-HOWARD ISOMORPHIE: $\Rightarrow, \neg, \forall$ VS. $\rightarrow, \{\}$

$H \vdash A \Rightarrow B$ [ext $\lambda a. b$]
 impliesR
 $H, a:A \vdash B$ [ext b]

$H \vdash x:S \rightarrow T$ [ext $\lambda x'. t$]
 lambdaFormation $j \ x'$
 $H, x':S \vdash T[x'/x]$ [ext t]
 $H \vdash S \in \mathbb{U}_j$ [Ax]

$H \vdash (\forall x)B$ [ext $\lambda x'. b$]
 allR
 $H, x':\mathbb{U} \vdash B[x'/x]$ [ext b]

$H \vdash \neg A$ [ext $\lambda a. b$]
 notR
 $H, a:A \vdash \text{f}$ [ext b]

$H, f:A \Rightarrow B, H' \vdash C$ [ext $c[f a/b]$]
 impliesL i
 $H, f:A \Rightarrow B, H' \vdash A$ [ext a]
 $H, b:B, H' \vdash C$ [ext c]

$H, f:x:S \rightarrow T, H' \vdash C$ [ext $t[fs, \text{Ax}/y, z]$]
 functionElimination $i \ s \ y \ z$
 $H, f:x:S \rightarrow T, H' \vdash s \in S$ [Ax]
 $H, f:x:S \rightarrow T, y:T[s/x], z:y=f \ s \in T[s/x], H' \vdash C$ [ext t]

$H, f:(\forall x)B, H' \vdash C$ [ext $c[f(t)/b]$]
 allL $i \ t$
 $H, f:(\forall x)B, b:B[t/x], H' \vdash C$ [ext c]

$H, f:\neg A, H' \vdash C$ [ext $\text{any}(f(a))$]
 notL
 $H, f:\neg A, H' \vdash A$ [ext a]

$\Gamma, z:\{\}, H' \vdash C$ [ext $\text{any}(z)$]
 voidElimination i

CURRY-HOWARD ISOMORPHIE: \wedge, \vee, \exists VS. $\times, +$

$H \vdash A \wedge B$ [ext (a, b)]
andR
 $H \vdash A$ [ext a]
 $H \vdash B$ [ext b]

$H \vdash (\exists x)B$ [ext (t, b)]
exR t
 $H \vdash B[t/x]$ [ext b]

$H, x:A \wedge B, H' \vdash C$ [ext $c[x.1, x.2/a, b]$]
andL i
 $H, a:A, b:B, H' \vdash C$ [ext c]

$H, z:(\exists x)B, H' \vdash C$ [ext $c[z.1, z.2/x', b]$]
exL i
 $H, x':\mathbb{U}, b:B[x'/x], H' \vdash C$ [ext c]

$H \vdash A \vee B$ [ext $\text{inl}(a)$]
orR1
 $H \vdash A$ [ext a]

$H \vdash A \vee B$ [ext $\text{inr}(b)$]
orR2
 $H \vdash B$ [ext b]

$H, x:A \vee B, H' \vdash C$
[ext $\text{case } x \text{ of } \text{inl}(a) \rightarrow c_1 \mid \text{inr}(b) \rightarrow c_2$]
orL i
 $H, a:A, H' \vdash C$ [ext c_1]
 $H, b:B, H' \vdash C$ [ext c_2]

$H \vdash x:S \times T$ [ext $\langle s, t \rangle$]
pairFormation j s x'
 $H \vdash s \in S$ [Ax]
 $H \vdash T[s/x]$ [ext t]
 $H, x':S \vdash T[x'/x] \in \mathbb{U}_j$ [Ax]

$H, z:x:S \times T, H' \vdash C$ [ext $\text{match } z \text{ with } \langle s, t \rangle \mapsto u$]
productElimination i s t
 $H, z:x:S \times T, s:S, t:T[s/x] H'[\langle s, t \rangle/z] \vdash C[\langle s, t \rangle/z]$ [ext u]

$H \vdash S + T$ [ext $\text{inl}(s)$]
inlFormation j
 $H \vdash S$ [ext s]
 $H \vdash T \in \mathbb{U}_j$ [Ax]

$H \vdash S + T$ [ext $\text{inr}(t)$]
inrFormation j
 $H \vdash T$ [ext t]
 $H \vdash S \in \mathbb{U}_j$ [Ax]

$H, z:S + T, H' \vdash C$ [ext $\text{case } z \text{ of } \text{inl}(x) \mapsto u \mid \text{inr}(y) \mapsto v$]
unionElimination i x y
 $H, z:S + T, x:S, H'[\text{inl}(x)/z] \vdash C[\text{inl}(x)/z]$ [ext u]
 $H, z:S + T, y:T, H'[\text{inr}(y)/z] \vdash C[\text{inr}(y)/z]$ [ext v]

LOGISCHE REGELN ALS KONSERVATIVE ERWEITERUNG

• Logische Regeln entsprechen Beweisfragmenten

```
H ⊢ A ⇒ B           [ext λa.b]
impliesR
H, a:A ⊢ B           [ext b]
```

```
H ⊢ A ⇒ B           [ext λa.b]
unfold implies
1. H ⊢ A → B        [ext λa.b]
   lambdaFormation 1 a
1.1. H, a:A ⊢ B      [ext b]
1.2. H ⊢ A ∈ U      [Ax]
     fold prop
1.2.1. H ⊢ A ∈ P    [Ax]
       Auto
```

- Wohlgeformtheit der Aussage A wird implizit vorausgesetzt
- In der Typentheorie muß $A \in \mathbb{P}$ explizit bewiesen werden
- Taktik `Auto` kann Wohlgeformtheit für “einfache” Aussagen beweisen

• Implementierung von `impliesR` als Taktik

```
– impliesR ≡      unfold implies
                    THEN lambdaFormation 1 a
                    THENL [Id; fold prop THEN Auto]
```

- Taktik `Id` läßt aktuelles Ziel unverändert, a ist neuer Name (↦ Alup II)
- Verwendung von `fold prop` kann entfallen, da `Auto` auch $A \in \mathbb{U}$ löst

IMPLEMENTIERUNG DER REGEL `impliesL`

• Beweisfragment für `impliesL` ist komplex

$$\begin{array}{l}
 H, f:A \Rightarrow B, H' \vdash C \quad [\text{ext } c[f a/b]] \\
 \text{impliesL } i \\
 H, f:A \Rightarrow B, H' \vdash A \quad [\text{ext } a] \\
 H, b:B, H' \vdash C \quad [\text{ext } c]
 \end{array}$$

$$\begin{array}{l}
 H, f:A \Rightarrow B, H' \vdash C \quad [\text{ext } (\lambda x.c[f x/b]) a] \\
 \text{cut } i \ A \ x \\
 1. \ H, f:A \Rightarrow B, H' \vdash A \quad [\text{ext } a] \\
 2. \ H, f:A \rightarrow B, x:A, H' \vdash C \quad [\text{ext } c[f s/b]] \\
 \quad \text{unfoldHyp } i \ \text{implies} \\
 2.1. \ H, f:A \rightarrow B, x:A, H' \vdash C \quad [\text{ext } c[f x/b]] \\
 \quad \quad \text{functionElimination } i \ x \ b \ z \\
 2.1.1. \ H, f:A \rightarrow B, x:A, H' \vdash x \in A \quad [\text{Ax}] \\
 \quad \quad \text{hypothesisEquality } i+1 \\
 2.1.2. \ H, f:A \rightarrow B, x:A, b:B, \\
 \quad \quad \quad z : b=f x \in B, H' \vdash C \quad [\text{ext } c] \\
 \quad \quad \quad \text{thin } i \ \text{THEN thin } i \ \text{THEN thin } i+1 \\
 2.1.2.1. \ H, b:B, H' \vdash C \quad [\text{ext } c]
 \end{array}$$

– `functionElimination` benötigt explizit einen Term $a \in A$

– Regel `cut` ermöglicht, diesen separat konstruieren zu lassen

– Regel `thin` eliminiert Hypothesen, die nicht gebraucht werden

• Implementierung von `impliesL` als Taktik

– `impliesL i` \equiv `cut i A x`
`THENL [Id; unfoldHyp i implies`
`THEN functionElimination i`
`THENL [Id; hypothesisEquality i+1 THEN thin i`
`THEN thin i THEN thin i+1]]`

– Term A muß aus Kontext bestimmt werden, x ist neuer Name (\mapsto Alup II)

DAS AUSWAHLAXIOM IST FORMAL BEWEISBAR

$$(\forall x:S. \exists y:T. P(x, y)) \Rightarrow \exists f:S \rightarrow T. \forall x:S. P(x, f(x))$$

$\vdash \forall S, T: \mathbb{U}_j. \forall P: S \times T \rightarrow \mathbb{P}_j. (\forall x:S. \exists y:T. P(x, y)) \Rightarrow \exists f:S \rightarrow T. \forall x:S. P(x, f(x))$
Repeat allR

1. $S: \mathbb{U}_j, T: \mathbb{U}_j, P: S \times T \rightarrow \mathbb{P}_j \vdash (\forall x:S. \exists y:T. P(x, y)) \Rightarrow \exists f:S \rightarrow T. \forall x:S. P(x, f(x))$
impliesR

1.1... , $h: (\forall x:S. \exists y:T. P(x, y)) \vdash \exists f:S \rightarrow T. \forall x:S. P(x, f(x))$
exR $\lambda x. (h x).1$

1.1.1... , $h: (\forall x:S. \exists y:T. P(x, y)) \vdash \forall x:S. P(x, (\lambda x. (h x).1) x)$
allR THEN reduce

1.1.1.1... , $h: (\forall x:S. \exists y:T. P(x, y)), x:S \vdash P(x, (h x).1)$
allL 4 x

1.1.1.1.1... , $h: (\forall x:S. \exists y:T. P(x, y)), x:S, p: (\exists y:T. P(x, y)) \vdash P(x, p.1)$
exL 5

1.1.1.1.1.1... , $h: (\forall x:S. \exists y:T. P(x, y)), x:S, y:T, z:P(x, y) \vdash P(x, (y, z).1)$
reduce THEN hypothesisEquality 7

● Aussage ist konstruktiv

- Die Funktion f kann aus einer Evidenz der $\forall\exists$ -Aussage extrahiert werden
- Grundlage für Synthese von Programmen aus Beweisen

METALOGISCHE ASPEKTE

- **Wichtige Sätze der Refinement Logik sind leicht zu zeigen**
 - *Ist $H \vdash C$ in RL beweisbar, dann gibt es einen Beweis ohne Schnittregel*
Nachweis des **Schnitteliminationssatzes** durch Normalisierung der Evidenz
 - *RL ist konsistent*
Andernfalls gäbe es einen schnittfreien Beweis für die Sequenz $\vdash f$
- **Typisierbarkeit**
 - Typisierbare Terme können **nichttypisierbare Teilterme** enthalten
 - Typzugehörigkeit und Typsein ist i.a. **nicht entscheidbar**
 - Objekt- und Typausdrücke können nichtterminierende Terme sein
 - Halteproblem wird Teil des Typisierbarkeitsproblems
 - **Wohlgeformtheitsziele im Beweiskalkül sind unvermeidbar**
- **Normalisierbarkeits- und Konfluenzaussagen**
 - Manche typisierbare Terme sind weder stark noch schwach normalisierbar
 - Wegen Festlegung auf **Lazy Evaluation** ist Konfluenz irrelevant
 - **Extrahierbare Terme sind stark normalisierbar und konfluent**

ENTWURFSENTSCHEIDUNGEN IM RÜCKBLICK

- **Beweisführung ist analytisch mit Verfeinerungsregeln**
 - Unterstützt die (maschinelle) Suche nach Beweisen
- **Urteile werden durch Konklusionen T [ext t] dargestellt**
 - Ermöglicht Konstruktion von Evidenzen für Typen und Aussagen
- **Gleichheit ist ein Datentyp und extensional**
 - Unterstützt Typzugehörigkeits- und Gleichheitsbeweise
- **Typ-Sein wird durch eine Universenhierarchie repräsentiert**
 - Jedes Universum für sich ist eine unvollständige Repräsentation
- **Logische Aussagen werden als Datentypen repräsentiert**
 - Curry-Howard Isomorphie zwischen Konnektiven und Typkonstruktoren