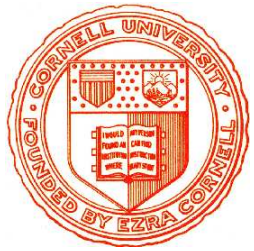
Automatisierte Logik und Programmierung

Einheit 11



Fortgeschrittene Konzepte der Typentheorie

1. “Nichtkonstruktive” Datentypen
2. Neuere Konstrukte
3. Ausblick

Mathematik benutzt nichtkonstruktive Konzepte

- **Mengentheoretische Operationen**
  - Teilmengenbildung $\{\, x{:}T \mid P[x] \,\}$
  - Vereinigung $S \cup T$ und Durchschnitt $S \cap T$ zweier Mengen
  - Vereinigung/Durchschnitt von Mengenfamilien $\bigcup_{x \in S} T[x]$, $\bigcap_{x \in S} T[x]$
  - Elemente dieser Typen sind Elemente der ursprünglichen Mengen
  - Informationen über Herkunft oder Selektionsprädikat sind nur implizit vorhanden (und nicht etwa in den Elementen gespeichert)
- **Äquivalenzklassen**
  - Äquivalenzrelation E induziert Klassen von Elementen eines Typs T
  - $[x]_E$ ist die Menge der zu x unter E äquivalenten Elemente
  - Menge der Klassen bildet einen neuen Typ $T//E$
  - Elemente von T sind Repräsentanten der Elemente von $T//E$
  - E induziert Gleichheit auf $T//E$: $[x]_E = [y]_E$ gilt g.d.w. $E(x, y)$

Mit bisherigen Typkonstrukten nicht simulierbar

Hilfreiche vordefinierte Typen

Konservative Definition gängiger Grundkonstrukte

- **Singulärer Typ:** $\texttt{Unit} \equiv 0 \in \mathbb{Z}$
  - Einziges Element ist Ax
  - Andere Bezeichnung: `t` ("der Wahrheitstyp" Gegenstück zu `f`)
- **Boolescher Datentyp:** $\mathbb{B} \equiv \texttt{Unit+Unit}$
  - $\mathsf{T} \equiv \mathsf{inl}(\mathsf{Ax})$, $\mathsf{F} \equiv \mathsf{inr}(\mathsf{Ax})$
  - if b then s else t $\equiv$ case b of $\mathsf{inl}(x) \mapsto s \mid \mathsf{inr}(y) \mapsto t$
  - Einbettung boolescher Werte in logische Prädikate durch Lifting:
    $\uparrow b \equiv$ `if` b `then t else f`
- **Rekursive Funktionen definiert durch Y-Kombinator**
  - $\mathsf{Y} \equiv$ `λf. (λx.f (x x)) (λx.f (x x))`
  - function $f(x) = t \equiv \mathsf{Y}(\lambda f.\lambda x.t)$ (geschlossener Term für f)
  - Nicht jede rekursiv definierte Funktion ist typisierbar
    Typ von function $f(x) = t$ muß im Kontext nachgewiesen werden

Teilmengenkonstrukt $\{x:S \mid P[x]\}$

- **Standardkonzept mit klarer intuitiver Bedeutung**
  - Ermöglicht natürliche Repräsentation von Teiltypen ($\mathbb{N}$, T `List`$^+$, ...) ohne ständige explizite Verwendung einschränkender Prädikate
  - z.B. $\forall \mathtt{n}:\mathbb{N}.\ \exists \mathtt{r}:\mathbb{N}.\ \mathtt{r}^2 \le \mathtt{n} < (\mathtt{r}+1)^2$ anstatt
    $\forall \mathtt{n}:\mathbb{Z}.\ 0 \le \mathtt{n} \ \Rightarrow\ \exists \mathtt{r}:\mathbb{Z}.\ 0 \le \mathtt{r} \wedge \mathtt{r}^2 \le \mathtt{n} < (\mathtt{r}+1)^2$
- **Konstruktive Interpretation von $\{x:S \mid P[x]\}$ schwierig**
  - Elemente sind Elemente aus $s \in S$, welche Eigenschaft $P[s]$ besitzen
  - Evidenz für $P[s]$ nur implizit vorhanden (kein Bestandteil des Elements)
- **Formale Ähnlichkeit zu $x:S \times P[x]$ nutzt wenig**
  - Elemente von $x:S \times P[x]$ sind Paare $\langle s, pf \rangle$ mit $s \in \{x:S \mid P[x]\}$
  - Evidenz $pf \in P[s]$ bleibt Bestandteil des Elements
  - Führt zu unnatürlichen Spezifikationen vieler Algorithmen
    Nullstellen finden $\{f{:}\mathbb{N}\to\mathbb{N} \mid \exists r{:}\mathbb{N}.\ f(r)=0\} \to \mathbb{N}$ (Suche nötig)
    würde zu $f{:}(\mathbb{N}\to\mathbb{N}) \times \exists r{:}\mathbb{N}.\ f(r)=0 \to \mathbb{N}$ (Projektion reicht)

$x:S \times P[x]$ ist zur Beschreibung von Teilmengen nicht geeignet

Der Teilmengenkonstruktor in der Typentheorie

- **Formalisierung der mengentheoretischen Aspekte**
  - Elemente von $\{x : S \mid P[x]\}$ sind Elemente von S
  - Es muß Evidenz für $P[s]$ geben, die aber nicht explizit bekannt ist
- **Sonderform des unabhängigen Konstruktors $\{S \mid P\}$**
  - Identisch mit S, wenn es Evidenz für P gibt, sonst leer
- **Häufigste Anwendung: Type-Squashing**
  - Definere $\downarrow P \equiv \{\mathsf{t} \mid P\}$

    Reduziert Struktur des Prädikats (Typs) P auf den "Wahrheitstyp" t
  - Wenn P nicht leer ist, enthält $\downarrow P$ nur das Element Ax

    Die Struktur der Elemente von P wird entfernt

    Alle Elemente von $\downarrow P$ sind gleich und besagen "P besitzt Evidenz"
  - Entfernt Überstrukturierung aus benutzerdefinierten Prädikaten

(siehe Folie 24)

Formulierung des Teilmengentyps

- **Ausdrücke**

  Kanonisch: $\{x:S \mid T\}$ S, T Terme, x Variable

  $\{S \mid T\}$ S, T Terme

  Nichtkanonisch: —

- **Reduktion von Ausdrücken**

  – entfällt, da keine nichtkanonische Elemente für den Teilmengenkonstruktor definiert

- **Urteile für Typ- und Elementgleichheit**

  $\{x_1:S_1 \mid T_1\} = \{x_2:S_2 \mid T_2\}$ falls $S_1{=}S_2$ und es gibt Terme p_1, p_2 und eine Variable x, die weder in T_1 noch in T_2 vorkommt, so daß

  $$p_1 \in \forall x:S_1 \,.\, T_1[x/x_1] \Rightarrow T_2[x/x_2]$$

  und $p_2 \in \forall x:S_1 \,.\, T_2[x/x_2] \Rightarrow T_1[x/x_1]$

  $\{x_1:S_1 \mid T_1\} = \{x_2:S_2 \mid T_2\} \in \mathbb{U}_j$ analog

  Prinzip der getrennten Definition von Typen kann nicht eingehalten werden

  $T = \{S_2 \mid T_2\}$ falls $T = \{x_2:S_2 \mid T_2\}$ für ein beliebiges $x_2 \in \mathcal{V}$

  $\{S_1 \mid T_1\} = T$ falls $\{x_1:S_1 \mid T_1\}{=}T$ für ein beliebiges $x_1 \in \mathcal{V}$

  $s = t \in \{x:S \mid T\}$ falls $\{x:S \mid T\}$ Typ und $s = t \in S$ und es gibt einen Term p mit der Eigenschaft $p \in T[s/x]$

Wichtige benutzerdefinierte Teilmengentypen

- **Zahlenmengen und -intervalle:**

$$\begin{aligned}
\mathbb{N} &\equiv \{\mathtt{i}:\mathbb{Z} \mid \mathtt{0}\leq\mathtt{i}\} \\
\mathbb{N}^{+} &\equiv \{\mathtt{i}:\mathbb{Z} \mid \mathtt{0}<\mathtt{i}\} \\
\{i\ldots\} &\equiv \{\mathtt{j}:\mathbb{Z} \mid i\leq\mathtt{j}\} \\
\{\ldots i\} &\equiv \{\mathtt{j}:\mathbb{Z} \mid \mathtt{j}\leq i\} \\
\{i..j\} &\equiv \{\mathtt{k}:\mathbb{Z} \mid i\leq\mathtt{k}\leq j\} \\
\{i..j^{-}\} &\equiv \{\mathtt{k}:\mathbb{Z} \mid i\leq\mathtt{k}<j\}
\end{aligned}$$

- **Listen**

$$T\,\mathsf{list}^{+} \equiv \{\mathtt{l}:T\,\mathsf{list} \mid \mathtt{l}\neq[] \in T\,\mathsf{list}\}$$

Behandlung von Teilmengen im Inferenzsystem

- **Verwaltung von implizitem Wissen erforderlich**
  - $\{x:T \mid P\}$ hat mehr Information als T und weniger als $x:T \times P$
    Nullstellenbestimmung ist verschieden aufwendig für Elemente von $\mathbb{N}\to\mathbb{N}$, $\{f{:}\mathbb{N}\to\mathbb{N} \mid \exists r{:}\mathbb{N}.\, f(r)=0\}$ und $f{:}(\mathbb{N}\to\mathbb{N})\times\exists r{:}\mathbb{N}.\, f(r)=0$
  - Für $s \in \{x:T \mid P\}$ wissen wir, daß $P[s]$ gilt, aber wir wissen nicht, wie die Evidenz für $P[s]$ konkret aussieht
  - In Beweisen müssen wir das Wissen $P[s]$ verwenden können, ohne die Evidenz für $P[s]$ algorithmisch einzusetzen

  Evidenz für $P[s]$ darf nicht im Extraktterm vorkommen

- **Unterstütze versteckte Hypothesen**
  - Erzeugung durch Dekomposition der Annahme $z{:}\{x:S \mid T\}$

$$\frac{H, z{:}\{x:S \mid T\}, H' \vdash C}{\texttt{setElimination}\ i\ y\ v\quad H, z{:}\{x:S \mid T\}, y{:}S, [\![v]\!]{:}T[y/x], H'[y/z] \vdash C[y/z]}\ \lfloor \text{ext}\ (\lambda y.\, t)\ z \rfloor \quad \lfloor \text{ext}\ t \rfloor$$

  - Freigabe der Hypothese nur in Teilzielen mit Extraktterm Ax
    (Gleichheiten, Kleiner-Relation)

Regeln für Teilmengentypen

$H \vdash \{x_1 : S_1 \mid T_1\} = \{x_2 : S_2 \mid T_2\} \in \mathbb{U}_j$ [Ax]
`setEquality` 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 $\{x : S \mid T\}$]
`setFormation` S x
$H \vdash S \in \mathbb{U}_j$ [Ax]
$H, x{:}S \vdash \mathbb{U}_j$ [ext T]

$H \vdash s = t \in \{x : S \mid T\}$ [Ax]
`set_memberEquality` j x'
$H \vdash s = t \in S$ [Ax]
$H \vdash T[s/x]$ [Ax]
$H, x'{:}S \vdash T[x'/x] \in \mathbb{U}_j$ [Ax]

$H \vdash \{x : S \mid T\}$ [ext s]
`set_memberFormation` j s x'
$H \vdash s \in S$ [Ax]
$H \vdash T[s/x]$ [Ax]
$H, x'{:}S \vdash T[x'/x] \in \mathbb{U}_j$ [Ax]

$H, z{:}\{x : S \mid T\}, H' \vdash C$ [ext $(\lambda y.\, t)\ z$]
`setElimination` i y v
$H, z{:}\{x : S \mid T\}, y{:}S, [\![v]\!]{:}T[y/x], H'[y/z] \vdash C[y/z]$ [ext t]

Die Regel `setEquality` *ist restriktiver als die Semantik auf Folie 5.*
Das macht sie unvollständig aber leichter anzuwenden.

Logische Interpretation des Teilmengentyps

- **$\{x:S \mid P[x]\}$ verhält sich wie ein Existenzquantor**
  - $\{x:S \mid P[x]\}$ ist genau dann nicht leer, wenn $\exists x{:}S.P[x]$ gültig ist
  - Elemente $s \in \{x:S \mid P[x]\}$ sind Zeugen für Gültigkeit von $\exists x{:}S.P[x]$
    Evidenz für $P[s]$ existiert, wird aber unterdrückt
  - $\{x:S \mid P[x]\}$ beschreibt nur den algorithmischen Aspekt des Quantors
  - $\forall$-$\exists$-Theorem auf Basis des Teilmengentyps liefern bessere Extraktterme
- **$\{P \mid Q\}$ verhält sich ähnlich wie die Konjunktion $P \wedge Q$**
  - $\{P \mid Q\}$ hat Elemente, wenn P und Q gültig sind
  - Elemente $p \in \{P \mid Q\}$ sind Elemente von P (partielle Evidenz)
    Evidenz für Q existiert, wird aber unterdrückt
  - $\{P \mid Q\}$ beschreibt eine nichtkommutative Konjunktion
  - $\{P \mid \mathsf{t}\}$ ist isomorph zu P
  - $\{\mathsf{t} \mid Q\}$ hat genau dann Elemente, wenn dies für Q gilt
    aber alle Elemente von $\{\mathsf{t} \mid Q\}$ sind gleich (“Squashing”)

Quadratwurzelalgorithmus mit Teilmengentypen

$\vdash \forall n{:}\mathbb{N}.\ \{r{:}\mathbb{N} \mid r^2 \le n < (r+1)^2\}$	allR
1. $n{:}\mathbb{N} \vdash \{r{:}\mathbb{N} \mid r^2 \le n < (r+1)^2\}$	NatInd4 1
1.1. $\vdash \{r{:}\mathbb{N} \mid r^2 \le 0 < (r+1)^2\}$	set_memberR ⌈0⌉ THEN Auto ✓
1.2. $i{:}\mathbb{N}, r{:}\mathbb{N}, r^2 \le i \div 4 < (r+1)^2 \vdash \{r{:}\mathbb{N} \mid r^2 \le i < (r+1)^2\}$	Decide ⌈$(2*r+1)^2 \le i$⌉ THEN Auto
1.2.1. $i{:}\mathbb{N}, r{:}\mathbb{N}, r^2 \le i \div 4 < (r+1)^2, (2*r+1)^2 \le i \vdash \{r{:}\mathbb{N} \mid r^2 \le i < (r+1)^2\}$	set_memberR ⌈2*r+1⌉ THEN Auto ✓
1.2.2. $i{:}\mathbb{N}, r{:}\mathbb{N}, r^2 \le i \div 4 < (r+1)^2, \neg((2*r+1)^2 \le i) \vdash \{r{:}\mathbb{N} \mid r^2 \le i < (r+1)^2\}$	set_memberR ⌈2*r⌉ THEN Auto ✓

- **Beweis hat die gleiche Struktur wie zuvor**
  - set_memberR ist Taktik für set_memberFormation
  - Versteckte Hypothese $r^2 \le i \div 4 < (r+1)^2$ wird für die Beweisziele $r^2 \le i$ und $i < (r+1)^2$ freigegeben,
  - Extrakt-Term enthält keine Beweiskomponenten
  - Effizienter Algorithmus für $\lfloor \sqrt{n} \rfloor$ wird ohne Projektion generiert

Durchschnittskonstruktor $\cap x:S.T[x]$

- **Durchschnitt einer Familie von Typen $T[x]$ mit $x \in S$**
  - Verallgemeinerung des einfachen Durchschnitts $S \cap T$ zweier Typen
  - Elemente sind Objekte, die für alle $x \in S$ zum Typ $T[x]$ gehören
  - Keine Abhängigkeit der Elemente von der Wahl eines konkreten $x \in S$
- **Strukturell ähnlich zu $x:S \to T[x]$** (aber andere Semantik)
  - Elemente von $x:S \to T[x]$ konstruieren für alle $x \in S$ ein $y \in T[x]$
  - $x \in S$ als Argument der Funktionen aus $x:S \to T[x]$ angegeben werden
  - Starke Abhängigkeit von $y \in T[x]$ von der Wahl des konkreten $x \in S$
- **Viele Anwendungen**
  - Record-Strukturen in Programmiersprachen
  - Definition eines Typs aller Terme der Typentheorie
  - Repräsentation eines echten Polymorphismus (ohne Abhängigkeiten)
  - Polymorphe Logik
  - "Guarded" Types

Formulierung des Durchschnittstyps

- **Ausdrücke**

  Kanonisch: $\cap x{:}S.T$ x Variable, S und T Terme

  Nichtkanonisch: —

- **Reduktion von Ausdrücken**

  – entfällt, da keine nichtkanonische Elemente für den Teilmengenkonstruktor definiert

- **Urteile für Typ- und Elementgleichheit**

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

  $\cap x_1{:}S_1.T_1 = \cap x_2{:}S_2.T_2 \in \mathbb{U}_j$ analog

  $t_1 = t_2 \in \cap x{:}S.T$ falls $\cap x{:}S.T$ *Typ* und
  $t_1{=}t_2 \in T[s/x]$ für alle Terme $s \in S$

Regeln für Durchschnittsbildung

$H \vdash \cap x_1{:}S_1.T_1 = \cap x_2{:}S_2.T_2 \in \mathbb{U}_j$ [Ax]
isectEquality 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 $\cap x : S\,.\,T$]
isectFormation x S
$H \vdash S \in \mathbb{U}_j$ [Ax]
$H, x{:}S \vdash \mathbb{U}_j$ [ext T]

$H \vdash t_1 = t_2 \in \cap x{:}S.T$ [Ax]
isect_memberEquality j x'
$H, x'{:}S \vdash t_1 = t_2 \in T[x'/x]$ [Ax]
$H \vdash S \in \mathbb{U}_j$ [Ax]

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

$H \vdash f_1 = f_2 \in T[t/x]$ [Ax]
isect_member_caseEquality $\cap x : S\,.\,T$ t
$H \vdash f_1 = f_2 \in \cap x{:}S.T$ [Ax]
$H \vdash t \in S$ [Ax]

$H, f{:}\cap x{:}S.T, H' \vdash C$ [ext $t[f, \mathsf{Ax}/y, z]$]
isectElimination i s y z
$H, f{:}\cap x{:}S.T, H' \vdash s \in S$ [Ax]
$H, f{:}\cap x{:}S.T, y{:}T[s/x], z{:}\, y{=}f \in T[s/x], H' \vdash C$ [ext t]

Anwendungen des Durchschnittstyps

- **Einfacher (binärer) Durchschnitt $S \cap T$**
  - Durchschnitt einer Mengenfamilie mit booleschem Index

    $S \cap T \equiv \cap \mathtt{b}{:}\mathbb{B}.\ \mathsf{if}\ \mathtt{b}\ \mathsf{then}\ S\ \mathsf{else}\ T$

  Achtung: $S \cap T$ ist nicht identisch mit $x{:}S \cap T$ mit T unabhängig von x
- **`Top`: Typ aller Terme der Typentheorie**
  - Leerer Durchschnitt hinterläßt keine Bedingungen an Elemente

    $\mathtt{Top} \equiv \cap \mathtt{x}{:}\{\}.\{\}$
  - Wegen $t \in \mathtt{Top}$, falls $t \in \{\}$ für alle $x \in \{\}$ gehört jeder Term t zu `Top`
- **Record Strukturen $\{l_1{:}T_1; ..; l_n{:}T_n\}$**
  - Durchschnitt einer Familie von Funktionen auf Labels l_i (Folie 26)
  - $\{l_1{:}T_1; ..; l_n{:}T_n\} \equiv \cap \mathtt{l}{:}\mathsf{Atom}.\ \mathsf{if}\ \mathtt{l}{=}l_1\ \mathsf{then}\ T_1\ \mathsf{else}$
    $\vdots \qquad\qquad \vdots$
    $\mathsf{if}\ \mathtt{l}{=}l_n\ \mathsf{then}\ T_n\ \mathsf{else}\ \mathtt{Top}$
- **Guarded types $\cap x{:}S.T$, wobei T unabhängig von x**
  - Isomorph zu `Top`, wenn S leer ist, und sonst isomorph zu T
  - Nützlich für Wohlgeformtheitsbeweise zu Mengenaussagen, die in pathologischen Fällen nicht einmal Typen wären (z.B. $x \in S \Rightarrow x \in T$)

Logische Interpretation des Durchschnittstyps

- **$\cap x{:}S.P[x]$ verhält sich wie ein Allquantor**
  - $\cap x{:}S.P[x]$ ist genau dann nicht leer, wenn $\forall x{:}S.P[x]$ gültig ist
  - Elemente $p \in \cap x{:}S.P[x]$ sind uniforme Evidenz für alle $P[s]$
  - Anders als bei $\forall x{:}S.P[x]$ wird Evidenz für $P[s]$ nicht aus s konstruiert
    algorithmischer Aspekt des Allquantors entfällt
  - Definition $\forall[x{:}S].P[x] \equiv \cap x{:}S.P[x]$ liefert polymorphe Logik
    Viele Quantoren in Theoremen können polymorph gewählt werden
    z.B. $\forall$`[i:`$\mathbb{Z}$`]. `$\forall$`[j:`$\mathbb{Z}$`]. i+j=j+i` $\in \mathbb{Z}$
- **Polymorphe Typdeklarationen sind möglich**
  - z.B. besagt $f \in \cap T{:}\mathbb{U}.\ T \to T$, daß f auf beliebigen Typen operiert
  - Typparameter T muß in Deklaration von f nicht verwendet werden
- **$P \cap Q$ verhält sich wie Konjunktion**
  - $P \cap Q$ ist genau dann nicht leer, wenn $P \wedge Q$ gültig ist
  - Elemente $p \in P \cap Q$ sind uniforme Evidenz für alle P und Q
  - Keine Paarbildung erforderlich

Vereinigungskonstruktor $\cup x:S.T[x]$

- **Vereinigung einer Familie von Typen $T[x]$ mit $x \in S$**
  - Verallgemeinerung der einfachen Vereinigung $S \cap T$ zweier Typen
  - Elemente sind Objekte y , die für ein $x \in S$ zum Typ $T[x]$ gehören
  - Keine Angabe eines konkreten $x \in S$ erforderlich
- **Strukturell ähnlich zu $x:S \times T[x]$** (aber andere Semantik)
  - Elemente von $x:S \times T[x]$ sind Paare (x, y) mit $x \in S$ und ein $y \in T[x]$
  - Starke Abhängigkeit von $y \in T[x]$ von der Wahl des konkreten $x \in S$
  - $x \in S$ muß als Teil des Elements mit angegeben werden
- **Nichttriviale Formalisierung**
  - Bei nicht disjunkten Typen muß Urteil der Elementgleichheit im Überlappingsbereich auf allen Typen übereinstimmen

Logische Interpretation des Vereinigungstyps

- **$\cup x{:}S.P[x]$ verhält sich wie ein Existensquantor**
  - $\cup x{:}S.P[x]$ ist genau dann nicht leer, wenn $\exists x{:}S.P[x]$ gültig ist
  - Elemente $p \in \cup x{:}S.P[x]$ sind Evidenz für ein $P[s]$
  - Anders als bei $\exists x{:}S.P[x]$ fehlt der Zeuge $s \in S$ für den $P[s]$ gilt algorithmischer Aspekt des Existenzquantors entfällt
  - $\exists[x{:}S].P[x] \equiv \cup x{:}S.P[x]$ liefert semi-klassischen Existenzquantor
- **$P \cup Q$ verhält sich wie Disjunktion**
  - $P \cup Q$ ist genau dann nicht leer, wenn $P \vee Q$ gültig ist
  - Elemente $p \in P \cup Q$ sind Evidenz für P oder für Q
  - Keine Kennzeichnung, welche der beiden Aussagen bewiesen wurde
  - $P[\vee]Q \equiv P \cup Q$ liefert semi-klassische Disjunktion

Quotiententypen

- **Modifikation der Gleichheit auf Typen**
  - Rationale Zahlen: Paare ganzer Zahlen mit $\langle z_1 , n_1 \rangle = \langle z_2 , n_2 \rangle$, falls $z_1 * n_2 = z_2 * n_1$
  - Reelle Zahlen: (rationale) Cauchyfolgen mit gleichem Grenzwert
  - Restklassenräume: $\mathbb{Z}$ `mod` k
- **Entspricht Faktorisierung modulo einer Äquivalenz**
  - Elemente s,t werden aus Typ T ausgewählt
  - Gleichheit von s und t wird über Äquivalenzrelation E neu definiert
  - Benutzerdefinierte Gleichheit wird in das Typsystem eingebettet

    Substitutions- und Gleichheitsregeln werden direkt anwendbar

Quotiententypen wichtig für formale Mathematik

Quotiententypen, formal

- **Ausdrücke**

  Kanonisch: $x\,,y : T//E$ E, T Terme, x, y Variablen

  Nichtkanonisch: —

- **Reduktion von Ausdrücken**

  – entfällt, da keine nichtkanonische Elemente für Quotiententypen definiert

- **Urteile für Typ- und Elementgleichheit**

  $x_1, y_1 : T_1//E_1$
  $= \; x_2, y_2 : T_2//E_2$ falls $T_1 = T_2$ und es gibt (verschiedene) Variablen x, y, z, die weder in E_1 noch in E_2 vorkommen, und Terme p_1, p_2, r,s und t mit der Eigenschaft

  $$p_1 \in \forall x{:}T_1\,.\,\forall y{:}T_1\,.\; E_1[x,y/x_1,y_1] \Rightarrow E_2[x,y/x_2,y_2]$$
  und $p_2 \in \forall x{:}T_1\,.\,\forall y{:}T_1\,.\; E_2[x,y/x_2,y_2] \Rightarrow E_1[x,y/x_1,y_1]$
  und $r \in \forall x{:}T_1\,.\,E_1[x,x/x_1,y_1]$
  und $s \in \forall x{:}T_1\,.\,\forall y{:}T_1\,.\; E_1[x,y/x_1,y_1] \Rightarrow E_1[y,x/x_1,y_1]$
  und $t \in \forall x{:}T_1\,.\,\forall y{:}T_1\,.\,\forall z{:}T_1\,.$
  $$E_1[x,y/x_1,y_1] \Rightarrow E_1[y,z/x_1,y_1] \Rightarrow E_1[x,z/x_1,y_1]$$

  $s = t \in x\,,y : T//E$ falls $x\,,y : T//E$ Typ und $s \in T$ und $t \in T$ und es gibt einen Term p mit der Eigenschaft $p \in E[s,t/x,y]$

Behandlung von Quotienten im Inferenzsystem

- **Gleichheit $E[s, t\,/\,x, y]$ ist implizites Wissen**
  - Wir wissen $E[s, t/x, y]$ wenn $s = t \in x, y : T//E$
  - In Beweisen müssen wir das Wissen $E[s, t/x, y]$ verwenden können, ohne die Evidenz für $E[s, t/x, y]$ algorithmisch einzusetzen

  Evidenz für $E[s, t/x, y]$ darf nicht im Extraktterm vorkommen

- **Versteckte Hypothesen erforderlich**
  - Dekomposition einer Quotientengleichheit muß versteckte Hypothesen generieren

$$
\begin{array}{l}
H, v{:}\, s = t \in x, y : T//E, H' \vdash C \qquad \lfloor \text{ext } u \rfloor \\
\quad \texttt{quotient\_equalityElimination } i\ j\ v' \\
\qquad H, v{:}\, s = t \in x, y : T//E, [\![v']\!]{:}E[s, t/x, y], H' \vdash C \qquad \lfloor \text{ext } u \rfloor \\
\qquad H, v{:}\, s = t \in x, y : T//E, H' \vdash E[s, t/x, y] \in \mathbb{U}_j \qquad \lfloor \text{Ax} \rfloor
\end{array}
$$

  - Freigabe versteckter Hypothesen wie zuvor

Regeln für Quotiententypen

$H \vdash \mathbb{U}_j$ [ext $x, y : T//E$]

quotientFormation T E x y z v v'

$H \vdash T \in \mathbb{U}_j$ [Ax]
$H, x{:}T, y{:}T \vdash E \in \mathbb{U}_j$ [Ax]
$H, x{:}T, \vdash E[x, x/x, y]$ [Ax]
$H, x{:}T, y{:}T, v{:}\, E[x, y/x, y] \vdash E[y, x/x, y]$ [Ax]
$H, x{:}T, y{:}T, z{:}T, v{:}\, E[x, y/x, y], v'{:}\, E[y, z/x, y] \vdash E[x, z/x, y]$ [Ax]

$H \vdash x_1, y_1 : T_1//E_1 = x_2, y_2 : T_2//E_2 \in \mathbb{U}_j$ [Ax]

quotientWeakEquality x y z v v'

$H \vdash T_1 = T_2 \in \mathbb{U}_j$ [Ax]
$H, x{:}T_1, y{:}T_1 \vdash E_1[x, y/x_1, y_1] = E_2[x, y/x_2, y_2] \in \mathbb{U}_j$ [Ax]
$H, x{:}T_1 \vdash E_1[x, x/x_1, y_1]$ [Ax]
$H, x{:}T_1, y{:}T_1, v{:}\, E_1[x, y/x_1, y_1] \vdash E_1[y, x/x_1, y_1]$ [Ax]
$H, x{:}T_1, y{:}T_1, z{:}T_1, v{:}\, E_1[x, y/x_1, y_1], v'{:}\, E_1[y, z/x_1, y_1] \vdash E_1[x, z/x_1, y_1]$ [Ax]

$H \vdash x_1, y_1 : T_1//E_1 = x_2, y_2 : T_2//E_2 \in \mathbb{U}_j$ [Ax]

quotientEquality

$H \vdash x_1, y_1 : T_1//E_1 \in \mathbb{U}_j$ [Ax]
$H \vdash x_2, y_2 : T_2//E_2 \in \mathbb{U}_j$ [Ax]
$H \vdash T_1 = T_2 \in \mathbb{U}_j$ [Ax]
$H, v{:}\, T_1{=}T_2{\in}\mathbb{U}_j, x{:}T_1, y{:}T_1 \vdash E_1[x, y/x_1, y_1] \Rightarrow E_2[x, y/x_2, y_2]$ [Ax]
$H, v{:}\, T_1{=}T_2{\in}\mathbb{U}_j, x{:}T_1, y{:}T_1 \vdash E_2[x, y/x_2, y_2] \Rightarrow E_1[x, y/x_1, y_1]$ [Ax]

$H \vdash s = t \in x, y : T//E$ [Ax]

quotient_memberWeakEquality j

$H \vdash x, y : T//E \in \mathbb{U}_j$ [Ax]
$H \vdash s = t \in T$ [Ax]

$H \vdash x, y : T//E$ [ext t]

quotient_memberFormation j

$H \vdash x, y : T//E \in \mathbb{U}_j$ [Ax]
$H \vdash T$ [ext t]

Regeln für Quotiententypen II

$H \vdash s = t \in x, y : T//E$ |Ax|
quotient_memberEquality j
$H \vdash x, y : T//E \in \mathbb{U}_j$ |Ax|
$H \vdash s \in T$ |Ax|
$H \vdash t \in T$ |Ax|
$H \vdash E[s, t/x, y]$ |Ax|

$H, v{:}\, s{=}t \in x, y : T//E, H' \vdash C$ |ext u|
quotient_equalityElimination i j v'
$H, v{:}\, s{=}t \in x, y : T//E, [\![v']\!]{:}E[s, t/x, y], H' \vdash C$ |ext u|
$H, v{:}\, s = t \in x, y : T//E, H' \vdash E[s, t/x, y] \in \mathbb{U}_j$ |Ax|

$H, z{:}\, x, y : T//E, H' \vdash s = t \in S$ |Ax|
quotientElimination i j x' y' v
$H, z{:}\, x, y : T//E, H', x'{:}T, y'{:}T \vdash E[x', y'/x, y] \in \mathbb{U}_j$ |Ax|
$H, z{:}\, x, y : T//E, H' \vdash S \in \mathbb{U}_j$ |Ax|
$H, z{:}\, x, y : T//E, H', x'{:}T, y'{:}T, v{:}\, E[x', y'/x, y] \vdash s[x'/z] = t[y'/z] \in S[x'/z]$ |Ax|

$H, z{:}\, x, y : T//E, H' \vdash s = t \in S$ |Ax|
quotientElimination_2 i j x' y' v
$H, z{:}\, x, y : T//E, H', x'{:}T, y'{:}T \vdash E[x', y'/x, y] \in \mathbb{U}_j$ |Ax|
$H, z{:}\, x, y : T//E, H' \vdash S \in \mathbb{U}_j$ |Ax|
$H, z{:}\, x, y : T//E, x'{:}T, y'{:}T, v{:}\, E[x', y'/x, y], H'[x'/z] \vdash s[x'/z] = t[y'/z] \in S[x'/z]$ |Ax|

Wichtige benutzerdefinierte Quotiententypen

- **Rationale Zahlen**

$x_1 =_q x_2 \equiv \mathsf{match}\ x_1\ \mathsf{with}\ \langle z_1, n_1\rangle \mapsto \mathsf{match}\ x_2\ \mathsf{with}\ \langle z_2, n_2\rangle \mapsto z_1 * n_2 = z_2 * n_1$

$\mathbb{Q} \equiv \mathtt{x,y} : \mathbb{Z} \times \mathbb{N}^+ // \mathtt{x} =_q \mathtt{y}$

$x_1 + x_2 \equiv \mathsf{match}\ x_1\ \mathsf{with}\ \langle z_1, n_1\rangle \mapsto \mathsf{match}\ x_2\ \mathsf{with}\ \langle z_2, n_2\rangle \mapsto \langle z_1 * n_2 + z_2 * n_1,\ n_1 * n_2\rangle$

$x_1 - x_2 \equiv \mathsf{match}\ x_1\ \mathsf{with}\ \langle z_1, n_1\rangle \mapsto \mathsf{match}\ x_2\ \mathsf{with}\ \langle z_2, n_2\rangle \mapsto \langle z_1 * n_2 - z_2 * n_1,\ n_1 * n_2\rangle$

$x_1 * x_2 \equiv \mathsf{match}\ x_1\ \mathsf{with}\ \langle z_1, n_1\rangle \mapsto \mathsf{match}\ x_2\ \mathsf{with}\ \langle z_2, n_2\rangle \mapsto \langle z_1 * z_2,\ n_1 * n_2\rangle$

$x_1 <_q x_2 \equiv \mathsf{match}\ x_1\ \mathsf{with}\ \langle z_1, n_1\rangle \mapsto \mathsf{match}\ x_2\ \mathsf{with}\ \langle z_2, n_2\rangle \mapsto z_1 * n_2 < z_2 * n_1$

- **Restklassenräume**

$x_1 = x_2\ \mathtt{mod}\ k \equiv k\ \mathtt{divides}\ x_1 - x_2$

$\mathbb{Z}\ \mathtt{mod}\ k \equiv \mathtt{x,y} : \mathbb{Z} // \mathtt{x} = \mathtt{y}\ \mathtt{mod}\ k$

Operationen auf $\mathbb{Z}$ mod k können direkt von $\mathbb{Z}$ übernommen werden

Behandlung überstrukturierter Prädikate

- **Manche Prädikate auf $\mathbb{Q}$ enthalten zu viel Struktur**
  - $x_1 <_q x_2$ muß im Quotiententyp (!) wohlgeformt sein
  - Gilt $x_1 <_q x_2 = x_1' <_q x_2'$, wenn $x_1 = x_1' \in \mathbb{Q}$ und $x_2 = x_2' \in \mathbb{Q}$?

    $z_1 * n_2 < z_2 * n_1 = z_1' * n_2' < z_2' * n_1'$ verlangt $z_1 * n_2 = z_1' * n_2' \in \mathbb{Z}$

    und $z_2 * n_1 = z_2' * n_1' \in \mathbb{Z}$

    Nicht gültig für $x_1 = \langle 2, 1\rangle$, $x_1' = \langle 4, 2\rangle$, $x_2 = x_2' = \langle 3, 1\rangle$
  - Unabhängigkeit vom Repräsentanten nicht mehr gegeben
  - Definition von $<_q$ enthält zu viel Struktur, wo nur "Wahrheit" nötig ist
- **Type-Squashing erforderlich** (neue Definition von $<_q$)

  $x_1 <_q x_2 \equiv \downarrow \mathsf{match}\ x_1\ \mathsf{with}\ \langle z_1, n_1\rangle \mapsto \mathsf{match}\ x_2\ \mathsf{with}\ \langle z_2, n_2\rangle \mapsto z_1 * n_2 < z_2 * n_1$

Behandlung überstrukturierter Prädikate

- **Manche Prädikate auf $\mathbb{Q}$ enthalten zu viel Struktur**
  - $x_1 <_q x_2$ muß im Quotiententyp (!) wohlgeformt sein
  - Gilt $x_1 <_q x_2 = x_1' <_q x_2'$, wenn $x_1 = x_1' \in \mathbb{Q}$ und $x_2 = x_2' \in \mathbb{Q}$?

    $z_1 * n_2 < z_2 * n_1 = z_1' * n_2' < z_2' * n_1'$ verlangt $z_1 * n_2 = z_1' * n_2' \in \mathbb{Z}$

    und $z_2 * n_1 = z_2' * n_1' \in \mathbb{Z}$

    Nicht gültig für $x_1 = \langle 2, 1\rangle$, $x_1' = \langle 4, 2\rangle$, $x_2 = x_2' = \langle 3, 1\rangle$
  - Unabhängigkeit vom Repräsentanten nicht mehr gegeben
  - Definition von $<_q$ enthält zu viel Struktur, wo nur "Wahrheit" nötig ist
- **Type-Squashing erforderlich** (neue Definition von $<_q$)

  $x_1 <_q x_2 \equiv \downarrow \mathsf{match}\ x_1\ \mathsf{with}\ \langle z_1, n_1\rangle \mapsto \mathsf{match}\ x_2\ \mathsf{with}\ \langle z_2, n_2\rangle \mapsto z_1 * n_2 < z_2 * n_1$
- **Alternative: $=_q$, $<_q$ als geliftete boolesche Operationen**

  $i_1 =_{\mathbb{Z}} i_2 \equiv \mathsf{if}\ i_1 = i_2\ \mathsf{then}\ \mathbf{T}\ \mathsf{else}\ \mathbf{F}$

  $i_1 <_{\mathbb{Z}} i_2 \equiv \mathsf{if}\ i_1 < i_2\ \mathsf{then}\ \mathbf{T}\ \mathsf{else}\ \mathbf{F}$

  $x_1 =_q x_2 \equiv \mathsf{match}\ x_1\ \mathsf{with}\ \langle z_1, n_1\rangle \mapsto \mathsf{match}\ x_2\ \mathsf{with}\ \langle z_2, n_2\rangle \mapsto \uparrow(z_1 * n_2 =_{\mathbb{Z}} z_2 * n_1)$

  $x_1 <_q x_2 \equiv \mathsf{match}\ x_1\ \mathsf{with}\ \langle z_1, n_1\rangle \mapsto \mathsf{match}\ x_2\ \mathsf{with}\ \langle z_2, n_2\rangle \mapsto \uparrow(z_1 * n_2 <_{\mathbb{Z}} z_2 * n_1)$

Definition Reeller Zahlen mit Quotiententypen

$$
\begin{array}{lcl}
x_1 \leq_q x_2 & \equiv & x_1 < x_2 \ \vee \ x_1 = x_2 \in \mathbb{Q} \\
z/n & \equiv & \langle z\,,n\rangle \\
|x| & \equiv & \mathsf{match}\ x\ \mathsf{with}\ \langle z\,,n\rangle \mapsto \mathsf{if}\ z<0\ \ \mathsf{then}\ \langle -z\,,n\rangle\ \ \mathsf{else}\ \langle z\,,n\rangle \\
\mathbb{R}_{pre} & \equiv & \{\mathtt{f}:\mathbb{N}^+\to\mathbb{Q} \mid \forall \mathtt{m},\mathtt{n}:\mathbb{N}^+.\ \ |\mathtt{f(n)-f(m)}| \ \leq\ \mathtt{1/m+1/n}\,\} \\
x_1 =_r x_2 & \equiv & \forall \mathtt{n}:\mathbb{N}^+.\ \ |x_1(\mathtt{n})\ -\ x_2(\mathtt{n})| \ \leq\ \mathtt{2/n} \\
\mathbb{R} & \equiv & \mathtt{x,y}:\mathbb{R}_{pre}/\!/\mathtt{x}=_r\mathtt{y} \\
x_1 + x_2 & \equiv & \lambda \mathtt{n}.\ x_1(\mathtt{n}) + x_2(\mathtt{n}) \\
x_1 - x_2 & \equiv & \lambda \mathtt{n}.\ x_1(\mathtt{n}) - x_2(\mathtt{n}) \\
|x| & \equiv & \lambda \mathtt{n}.\ |x(\mathtt{n})|
\end{array}
$$

Elegante Beweise erfordern viele Spezialtaktiken

Atomare Bezeichner

- **Verwaltung eindeutiger Namen**
  - Token: Textketten, die (anders als Strings) keine Struktur haben
  - Einzig mögliche Analyse ist Test auf Gleichheit von Token
  - Wichtig für Programmiersprachen und Sicherheitsprotokolle

---

- **Ausdrücke**

  Kanonisch: Atom

  "*token*" — *token* Text-Token

  Nichtkanonisch: if a=b then s else t — a, b, s, t Terme

- **Reduktion von Ausdrücken**

  if a=b then s else t $\xrightarrow{\beta}$ s, falls $a = b$, sonst t

- **Urteile für Typ- und Elementgleichheit**

  Atom = Atom

  "*token*" = "*token*" $\in$ Atom — *für alle token !* —

  Atom = Atom $\in \mathbb{U}_j$ — *für alle j !* —

Regeln für Atomare Bezeichner

$H \vdash \mathsf{Atom} = \mathsf{Atom} \in \mathbb{U}_j$ [Ax]
`atomEquality`

$H \vdash \mathbb{U}_j$ [ext Atom]
`atomFormation`

$H \vdash$ "*token*" = "*token*" $\in$ Atom [Ax]
`tokenEquality`

$H \vdash \mathsf{Atom}$ [ext "*token*"]
`tokenFormation "token"`

$H \vdash \mathsf{if}\ u_1{=}v_1\ \mathsf{then}\ s_1\ \mathsf{else}\ t_1 = \mathsf{if}\ u_2{=}v_2\ \mathsf{then}\ s_2\ \mathsf{else}\ t_2 \in T$ [Ax]
`atom_eqEquality` v
- $H \vdash u_1 = u_2 \in \mathsf{Atom}$ [Ax]
- $H \vdash v_1 = v_2 \in \mathsf{Atom}$ [Ax]
- $H, v{:}\ u_1{=}v_1 \in \mathsf{Atom} \vdash s_1 = s_2 \in T$ [Ax]
- $H, v{:}\ \neg(u_1{=}v_1 \in \mathsf{Atom}) \vdash t_1 = t_2 \in T$ [Ax]

$H \vdash \mathsf{if}\ u{=}v\ \mathsf{then}\ s\ \mathsf{else}\ t = t_2 \in T$ [Ax]
`atom_eqReduceTrue`
- $H \vdash s = t_2 \in T$ [Ax]
- $H \vdash u = v \in \mathsf{Atom}$ [Ax]

$H \vdash \mathsf{if}\ u{=}v\ \mathsf{then}\ s\ \mathsf{else}\ t = t_2 \in T$ [Ax]
`atom_eqReduceFalse`
- $H \vdash t = t_2 \in T$ [Ax]
- $H \vdash \neg(u = v \in \mathsf{Atom})$ [Ax]

Neuere Typkonstrukte

- **Abhängiger Durchschnitt $x:S\cap T[x]$** Bisher nur in MetaPRL
  - Element s muß zu S und gleichzeitig zu $T[s]$ gehören (Selbstreferenz!)
- **Squiggle-Equality $s\sim t$**
  - Einfacherer, syntaktischer Gleichheitstyp, ohne Abhängigkeit vom Typ
    $s\sim t$ gilt, wenn s und t zum gleichen Term reduzierbar sind
    oder in $\mathbb{Z}$ oder Atom semantisch gleich sind
  - Substitutionregel gilt auch für Terme die squiggle-gleich sind
- **Stark abhängige Funktionen $\{f \mid x:S\rightarrow T[f,x]\}$**
  - Selbstreferenz: Bildbereich hängt ab von Eingabe und Funktion f selbst
  - Mächtiger als abhängiger Durchschnitt, aber Beweise werden aufwendig
- **Aktuell in Entwicklung**
  - Logic of Events: Schließen über Kommunikation und verteilte Prozesse
  - Reflektion: Schließen über Beweisverfahren und das Meta-Level der CTT

Typentheorie im Rückblick

Inferenzkalkül für Mathematik & Programmierung

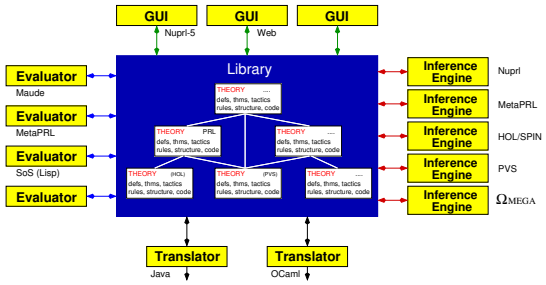
- **Ausdrucksstarkes Inferenzsystem**
  - Vereinheitlicht und erweitert Logik, λ-Kalkül und einfache Typentheorie
  - Formalisierung "natürlicher" Gesetze der zentralen Konzepte
  - Direkte Darstellung anstatt Simulation
  - Umfangreiche Theorie bestehend aus
    - Prädikatenlogik (höherer Stufe)
    - Mathematischen Grundkonzepten
    - Grundkonstrukten der Programmierung, einschließlich Rekursion
- **Praktische Probleme**
  - Beweise erfordern viel Schreibarbeit → *Interaktive Beweissysteme*
  - Beweise sind unübersichtlich (viele Regelanwendungen)
  - Beweise sind schwer zu finden (viele Regeln und Parameter)

→ *Automatisierung der Beweisführung*

Ausblick: Themen des zweiten Teils (Sommer 2017)

Konstruiere semiautomatische Beweissysteme

- **Aufbau von Beweissystemen**
  - Implementierung interaktiver Beweisassistenten
  - Das NuPRL Logical Programming Environment



- **Automatisierung des formalen Schließens**
  - Taktisches Beweisen
  - Entscheidungsprozeduren
  - Integration externer Systeme in den Inferenzmechanismus

- **Anwendungen & Demonstrationen**
  - Formalisierung mathematischen Wissens
  - Synthese effizienter Algorithmen aus formalen Spezifikationen

  ⋮