Einführung in die konstruktive Logik

Andreas Abel

Oktober 2007

1 Motivation

Disjunktionseigenschaft. Wenn Aussage $A \vee B$ gilt, wüsste man gerne, ob nun A oder B wahr ist. Im Allgemeinen kann einem in der klassischen Logik dieser Wunsch jedoch nicht erfüllt werden. Das Gesetz vom ausgeschlossenen Dritten (lat. *tertium non datur* (TND), engl. *law of the excluded middle*) $A \vee \neg A$ gilt jedoch für beliebige Aussagen A, ohne dass man einen Beweis für A oder sein Gegenteil hätte. Spekulation: Das entspricht philosophisch der Postulation eines logisch allwissenden Gottes.

Man kann sich jedoch auch auf den Standpunkt des *Konstruktivisten* stellen: Wahr ist nur, was bewiesen ist. Dann erfordert die Wahrheit von $A \vee \neg A$ entweder einen Beweis von A oder von $\neg A$, also kann TND nicht allgemein gelten. Während die klassische Logik bereits im Altertum formalisiert wurde (Aristoteles), ist die konstruktive (oder *intuitionistische*) Logik eine Entwicklung des 20. Jahrhunderts, angestoßen durch die große Grundlagenkrise der Mathematik um 1900.

2 Brouwer-Heyting-Kolmogorov-Interpretation

Stellen wir uns nun auf den intuitionistischen Standpunkt. Was gilt nun als Beweis einer Aussage A? Kolmogorov [Kol32] sieht eine Aussage als Aufgabenstellung an und einen Beweis als eine Vorschrift, wie die Lösung zu erlangen ist.

- Ein Beweis von $A \wedge B$ ist ein Paar (p, q), wobei p ein Beweis von A und q ein Beweis von B ist.
- Ein Beweis von $A \vee B$ ist ein Paar (b, p), wobei b ein Bit ist und p ein Beweis von A, falls $b = 0$, und ein Beweis von B, falls $b = 1$.
- Ein Beweis von $A \Rightarrow B$ ist ein Programm f, dass einen beliebigen Beweis von A in einen Beweis von B transformiert.
- Ein Beweis von $\neg A$ ist ein Programm f, dass einen beliebigen Beweis von A in einen Beweis von $\bot$ transformiert.

- Der Beweis von $\top$ ist trivial.

Diese Definition kann auch als Vorschrift zur Vereinfachung von Aufgabenstellungen gelesen werden, z. B., "um die Aufgabe $A \wedge B$ zu lösen, löse sowohl A als auch B", "um die Aufgabe $A \vee B$ zu lösen, entscheide dich, entweder A oder B zu lösen". Die Aufgabe $\top$ kann als schon gelöst betrachtet werden. Die Aufgabe $\bot$ kann nicht weiter vereinfacht werden, d.h., es gibt keinen kanonischen Beweis von $\bot$.

Mehr zur BHK-Interpretation unter "Beweisterme".

Referenz: Andrei Kolmogorov, *Zur Deutung der intuitionistischen Logik* (1932) [Kol32].

3 Natürliches Schließen

Engl. natural deduction (ND).

Aussagen:

$$A, B, C ::= P \mid \top \mid \bot \mid A \wedge B \mid A \vee B \mid A \Rightarrow B.$$

Die Negation $\neg A$ ist definiert als $A \Rightarrow \bot$.

Der Kalkül des Natürlichen Schließens

$$\frac{\begin{array}{c}\overline{A}\\ \vdots\\ B\end{array}}{A \Rightarrow B}\Rightarrow\mathsf{I} \qquad \frac{A \Rightarrow B \qquad A}{B}\Rightarrow\mathsf{E}$$

$$\frac{A \qquad B}{A \wedge B}\wedge\mathsf{I} \qquad \frac{A \wedge B}{A}\wedge\mathsf{E}_1 \qquad \frac{A \wedge B}{B}\wedge\mathsf{E}_2$$

$$\frac{A}{A \vee B}\vee\mathsf{I}_1 \qquad \frac{B}{A \vee B}\vee\mathsf{I}_2$$

$$\frac{A \vee B \qquad \begin{array}{c}\overline{A}\\ \vdots\\ C\end{array} \qquad \begin{array}{c}\overline{B}\\ \vdots\\ C\end{array}}{C}\vee\mathsf{E}$$

$$\frac{}{\top}\top\mathsf{I} \qquad \frac{\bot}{C}\bot\mathsf{E}$$

Dabei entsprechen die Einführungsregeln (*introduction rules*) mit Namenssuffix I den BHK-Konstruktionsprinzipien für Beweise. Die Eliminationsregeln (*elimination rules*) mit Suffix E sind nötig, um hypothetische Beweise zu zerlegen,

um z.B. aus einem angenommenen Beweis von $A \wedge B$ einen Beweis von A zu machen. Einen Beweis mit einer I-Regel zu konstruieren und unmittelbar danach mit einer E-Regel wieder zu zerlegen, stellt einen Umweg dar, und kann abgekürzt werden (siehe Beweisreduktionen).

4 Natürliches Schließen in Tutch

Tutch (*tut*orial proof *ch*ecker) ist ein Beweisprüfer für natürliches Schließen zur Übungszwecken. Download und Dokumentation siehe:

```
http://www.tcs.ifi.lmu.de/~abel/tutch
```

Tutch ist in SML implementiert und benötigt einen aktuellen Standard ML of New Jersey Compiler zur Installation. Entwicklung eines Beweises in Tutch:

Formel	in Tutch
$\top$	`T`
$\bot$	`F`
$A \wedge B$	`A & B`
$A \vee B$	`A | B`
$A \Rightarrow B$	`A => B`
$\neg A$	`~ A`
$A \Leftrightarrow B$	`A <=> B`

Tabelle 1: Propositionale Formeln in Tutch.

Tutch kann auch unvollständige Beweise prüfen, meldet dann aber einen Fehler der auf die Lücke zeigt. Dieses Feature machen wir uns zunutze und entwickeln einen Beweis inkrementell:

```
proof andI : A => B => A & B =
begin

  A => B => A & B
end;
```

Dies ist die minimale Eingabe, die Tutch verarbeiten kann. `proof`, `begin`, `end` sind Schlüsselwörter. Wir entwickeln einen Beweis der Aussage `A => B => A & B` und geben ihm den Namen `andI`. Zwischen `begin` und `end` steht der Beweis als Liste von Aussagen, die letzte Aussage muss mit der zu beweisenden übereinstimmen.

Nach Aufruf von `tutch andI.tut` erhalten wir folgendes Ergebnis:

```
TUTCH 0.52 beta, $Date: 2002/10/24 19:25:49 $
[Opening file andI.tut]
Proving andI: A => B => A & B ...
andI.tut:4.3-4.18 Error:
```

```
Unjustified line .  |-  A => B => A & B
Assuming this line, checking remainder...
Proof incomplete
[Closing file andI.tut]
```

Die Datei ist also syntaktisch korrekt, aber der Beweis ist unvollständig. Um die Implikation `A => (B => A & B)` zu beweisen, nehmen wir `A` an und beweisen unter dieser Annahme `B => A & B`. In Tutch gibt es dafür die eckigen Klammern: Die erste Aussage nach der öffnenden Klammer ist die Annahme, die letzte Aussage vor der schliessenden Klammer die Konklusion.

```
proof andI: A => B => A & B =
begin
[ A;

  B => A & B ];
A => B => A & B
end;
```

Nun meldet Tutch:

```
Unjustified line A  |-  B => A & B
```

Weiter nehmen wir `B` an und beweisen `A & B`:

```
proof andI: A => B => A & B =
begin
[ A;
  [ B;
    A & B ];
  B => A & B ];
A => B => A & B
end;
```

Der Beweis ist fertig, da `A & B` aus den sichtbaren, darüberliegenden Aussagen durch Anwendung einer einzigen Regel, Und-Einführung, folgt. Mit `tutch -v andI.tut` erhalten wir ein Protokoll der Beweisprüfung:

```
Proving andI: A => B => A & B ...
  1  [ A;
  2    [ B;
  3      A & B ];              by AndI 1 2
  4    B => A & B ];           by ImpI 3
  5  A => B => A & B           by ImpI 4
QED
```

Tutch hat jede Aussage (außer den Annahmen) mit der Regel annotiert, die die Aussage beweist, mit den Nummern der Aussagen, die an diesem Schritt direkt beteiligt sind.

5 Natürliches Schließen mit expliziten Annahmen

Besonders wenn man etwas über den Kalkül des natürlichen Schließens zeigen möchte, ist es gut, die aktuell sichtbaren Annahmen zu jeder Zeit explizit zu nennen. Damit ergeben sich folgende Regeln:

Der Kalkül des Natürlichen Schließens mit expliziten Annahmen $\Gamma \vdash A$. Γ sei eine Menge von Aussagen, die aktuellen Annahmen (Hypothesen).

$$\frac{A \in \Gamma}{\Gamma \vdash A}\,\mathsf{hyp} \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\,{\Rightarrow}\mathsf{I} \qquad \frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}\,{\Rightarrow}\mathsf{E}$$

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\,{\wedge}\mathsf{I} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\,{\wedge}\mathsf{E}_1 \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\,{\wedge}\mathsf{E}_2$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\,{\vee}\mathsf{I}_1 \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\,{\vee}\mathsf{I}_2$$

$$\frac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}\,{\vee}\mathsf{E}$$

$$\frac{}{\Gamma \vdash \top}\,{\top}\mathsf{I} \qquad \frac{\Gamma \vdash \bot}{\Gamma \vdash C}\,{\bot}\mathsf{E}$$

Es ist eine Regel hyp hinzu gekommen, die besagt: Jede Annahme gilt als bewiesen. Die Regeln ${\Rightarrow}\mathsf{I}$ und ${\vee}\mathsf{E}$ fügen neue Annahmen hinzu (liest man die Regeln von unten nach oben), alle anderen Regeln lassen Γ unberührt.

6 Beweisterme

Nach der BHK-Interpretation ist ein Beweis ein Programm zur Lösung einer Aufgabe. Im Folgenden formalisieren wir diese Programme.

Beweisterme (Church-Stil):

$r, s, t ::= x \mid \lambda x^A.t \mid r\,s$	einfach getypter λ-Kalkül (für $\Rightarrow$)
$\mid (r, s) \mid \mathsf{fst}\,r \mid \mathsf{snd}\,r$	Paare und Projektionen (für $\wedge$)
$\mid \mathsf{inl}_B\,t \mid \mathsf{inl}_A\,t$	Injektionen und...
$\mid \mathsf{case}\,r\,\mathsf{of}\,\mathsf{inl}\,x^A \Rightarrow s \mid \mathsf{inr}\,y^B \Rightarrow t$	...Fallunterscheidung (für $\vee$)
$\mid ()$	leeres Tupel (für $\top$)
$\mid \mathsf{abort}_C\,r$	Ausnahme (*exception*) (für $\bot$)

Typisierung: Γ sei eine Menge von Variable-Aussage-Paaren, geschrieben $x : A$. Wir definieren induktiv ein Urteil $\Gamma \vdash t : C$ das besagt: *Unter den Annahmen Γ ist der Term t ein gültiger Beweis der Aussage C.*

$$\frac{(x:A) \in \Gamma}{\Gamma \vdash x : A}\,\mathsf{hyp}$$

$$\frac{\Gamma, x:A \vdash t : B}{\Gamma \vdash \lambda x^A.\, t : A \Rightarrow B}\Rightarrow\mathsf{I} \qquad \frac{\Gamma \vdash r : A \Rightarrow B \qquad \Gamma \vdash s : A}{\Gamma \vdash r\, s : B}\Rightarrow\mathsf{E}$$

$$\frac{\Gamma \vdash r : A \qquad \Gamma \vdash s : B}{\Gamma \vdash (r,\, s) : A \wedge B}\wedge\mathsf{I} \qquad \frac{\Gamma \vdash r : A \wedge B}{\Gamma \vdash \mathsf{fst}\, r : A}\wedge\mathsf{E}_1 \qquad \frac{\Gamma \vdash r : A \wedge B}{\Gamma \vdash \mathsf{snd}\, r : B}\wedge\mathsf{E}_2$$

$$\frac{\Gamma \vdash t : A}{\Gamma \vdash \mathsf{inl}_B\, t : A \vee B}\vee\mathsf{I}_1 \qquad \frac{\Gamma \vdash t : B}{\Gamma \vdash \mathsf{inr}_A\, t : A \vee B}\vee\mathsf{I}_2$$

$$\frac{\Gamma \vdash r : A \vee B \qquad \Gamma, x:A \vdash s : C \qquad \Gamma, y:B \vdash t : C}{\Gamma \vdash \mathsf{case}\, r\, \mathsf{of}\, \mathsf{inl}\, x^A \Rightarrow s \mid \mathsf{inr}\, y^B \Rightarrow t : C}\vee\mathsf{E}$$

$$\frac{}{\Gamma \vdash () : \top}\top\mathsf{I} \qquad \frac{\Gamma \vdash r : \bot}{\Gamma \vdash \mathsf{abort}_C\, r : C}\bot\mathsf{E}$$

Die Propositions-Annotationen in den Beweistermen zu $\Rightarrow\mathsf{I}$ und $\bot\mathsf{E}$ sind so gewählt, dass man die bewiesene Proposition C zu einem Beweisterm t durch strukturelle Rekursion über t mühelos reproduzieren kann.

Übung 1 Gegeben ein Typisierungskontext Γ und ein Beweisterm t im Church-Stil berechnet die Funktion $\mathsf{typeOf}(\Gamma \vdash t)$ die von t bewiesene Aussage A durch Rekursion über t. Falls t nicht wohlgetypt ist in Γ, wird $\emptyset$ zurückgegeben. Definieren Sie typeOf, in Anlehnung an obige Regeln.

In den Einführungsregeln (I, engl. *introduction*) erkennen wir die Definition eines kanonischen Beweises nach Brouwer-Heyting-Kolmogorov wieder. Es gibt keinen kanonischen Beweis der Absurdität, also keine Regel $\bot\mathsf{I}$. Die Beseitigungsregeln (E, engl. *elimination*) erklären, wie man vorhandene Beweise verwenden kann, um die Beweisaufgabe zu lösen. Auf den trivialen Beweis von $\top$ hat man keine Arbeit verwendet, kann ihn also auch nicht sinnvoll benutzen, deshalb keine Regel $\top\mathsf{E}$.

7 Beweisterme in Tutch

In Tutch werden Beweisterme sehr ähnlich geschrieben, es gibt die folgenden Unterschiede:

1. Keine Propositions-Annotationen.

2. $\lambda x.t$ wird geschrieben als `fn x => t` (wie in SML).

3. Fallunterscheidung wird mit `end` abgeschlossen, also

```
case r of inl x => s | inr y => t end
```

Ein Tutch-Beweis kann mit Beweistermen annotiert werden, die von Tutch dann auf Korrektheit geprüft werden. Z.B.

```
annotated proof andI : A => B => A & B =
begin
[ x : A;
  [ y : B;
    (x,y) : A & B ];
  fn y => (x,y) : B => A & B ];
fn x => fn y => (x,y) : A => B => A & B
end;
```

Das Schlüsselwort `annotated` zeigt an, dass nun jede Aussage einen Beweisterm erfordert. Annahmen werden mit Variablen annotiert, hergeleitete Aussagen mit einem zusammengesetzten Term. Dabei ist jeder Term ein voller Beweis für die dahinterstehende Aussage, dadurch ergibt sich eine gewaltige Redundanz: Jeder Teilbeweis muss vollständig wiederholt werden.

8 Coq

Das Beweissystem Coq basiert auf einem Kalkül ähnlich dem natürlichen Schließen.

```
Section Example1.

Variables (A B C: Prop).

Theorem currying : and A B -> C <-> A -> B -> C.
split.
 intros f a b.
 apply f.
 split. assumption. assumption.
intros f ab.
inversion ab.
apply f. assumption. assumption.
Qed.

Theorem orElim : or A B -> C <-> and (A -> C) (B -> C).
split.
 intros f.
 split.
  intros a. apply f. left. exact a.
 intros b. apply f. right. exact b.
intros gh d.
inversion_clear gh as [ g h ].
inversion_clear d as [ a | b ].
 apply g. assumption.
apply h. assumption.
Qed.

End Example1.
```

Eine Coq-Datei kann mehrere `Section`s enthalten, die jeweils lokale Annahmen (z.B: `Variables`) deklarieren dürfen. Das ist dem `theory`-Mechanismus von PVS ähnlich. Die Bibliothek `Coq.Init.Logic`, die automatisch geladen wird, enthält die Definition der logischen Konnektive. `Prop` ist der Typ der Aussagen (war `boolean` in PVS).

Tabelle 3 zeigt die den Beweisregeln des natürlichen Schließens entsprechende Coq-Taktiken. Die Entsprechung ist nicht eins-zu-eins, die `inversion`-Taktik entspricht eher einer Links-Regel des Sequenzenkalküls denn einer Eliminationsregel des natürlichen Schließens. Varianten:

- `intros x y z` führt gleich 3 Hypothesen ein.
- `apply f` führt auch mehrere $\Rightarrow$E-Schritte auf einmal aus, z.B., falls $f : A \Rightarrow B \Rightarrow C$ und das aktuelle Ziel C ist, dann werden zwei neue Ziele A

Formel	in Coq	Alternative
$\top$	`True`	
$\bot$	`False`	
$A \wedge B$	`A /\ B`	`and A B`
$A \vee B$	`A \/ B`	`or A B`
$A \Rightarrow B$	`A -> B`	
$\neg A$	`~ A`	`not A`
$A \Leftrightarrow B$	`A <-> B`	`iff A B`

Tabelle 2: Propositionale Formeln in Coq.

Regel	Coq-Taktik	Alternative
hyp	`exact x`	`assumption`
$\Rightarrow$I	`intros x`	
$\Rightarrow$E	`apply r`	
$\top$I	`split`	
$\wedge$I	`split`	
$\wedge$E	`inversion x`	`elim x`
$\vee$I$_1$	`left`	
$\vee$I$_2$	`right`	
$\vee$E	`inversion x`	`elim x`
$\bot$E	`inversion x`	`elim x`
weak	`clear x`	

Tabelle 3: Natürliches Schließen in Coq.

und B erzeugt.

- `split` kann auch angewendet werden, falls das Ziel von der Form $A_1 \to \cdots \to A_n \to C$ ist und C eine Konjuktion. Dann werden vor der Aufsplittung die Aussagen A_i als Hypotheses eingeführt. Dasselbe gilt analog für `left` und `right`.

- `inversion_clear h` zerlegt wie `inversion h` die Hypothese h in ihre Bestandteile, zusätzlich wird noch h entfernt. Beide Taktiken kann noch eine Liste von Bezeichnern `[ x1 ... xn ]` für die neuen Hypothesen mitgeliefert werden. Entstehen durch die Zerlegung mehrere Unterziele (wie z.B. bei $\vee$E), so müssen Bezeichner für jedes Unterziel mitgeliefert werden. Die Bezeichnerliste wird dann durch `|` entsprechend partitioniert.

- `elim x` kann auch auf Hypothesen der Form $A_1 \to \cdots \to A_n \to C$ und C Konjunktion, Disjunktion oder Falsum. Dann werden die A_i als neue Ziele hinzugefügt.

- `cut (A)` fügt die Annahme A hinzu, die dann separat noch bewiesen werden muss.

Beweisterme. Wurde `Theorem bla : A` in Coq bewiesen, so kann der Beweisterm mit `Print bla` (oder auch `Check bla`) eingesehen werden. In Coq können Beweisterme auch direkt eingegeben werden. Hier haben wir einige Aussagen mit Termen bewiesen, u.a. die des letzten Beispiels:

```
Section Example2.

Variables (A B C: Prop).

Definition curry  : (and A B -> C) -> A -> B -> C
  := fun f a b => f (conj a b).

Definition curry'
  := fun (f : and A B -> C) (a : A) (b : B) => f (conj a b).

Definition uncurry : (A -> B -> C) -> and A B -> C
  := fun f p => f (proj1 p) (proj2 p).

Definition join :  and (A -> C) (B -> C) -> or A B -> C
  := fun gh d =>
     match d with
     | or_introl a => proj1 gh a
     | or_intror b => proj2 gh b
     end.

Definition fsplit : (or A B -> C) -> and (A -> C) (B -> C)
```

```
  := fun f => conj (fun a => f (or_introl B a))
                   (fun b => f (or_intror A b)).

Definition abort : False -> C
  := fun h => match h with end.

Definition delay : C -> (True -> C)
  := fun c i => c.
Definition force : (True -> C) -> C
  := fun f => f I.

End Example2.
```

Die `Definition` eines Beweistermes kann entweder die zu beweisende Proposition mit angeben (Bsp. `curry`) oder vom System inferieren lassen (Bsp. `uncurry`). Dann müssen aber die Aussagen zu den (wenigstens einigen) Hypothesenvariablen angegeben werden. (Die Annotation der Variable `a` und `b` ist hier überflüssig.) Besondere Vorsicht ist bei `or_introl` und `or_intror` geboten: Sie

Beweisterm	in Coq
$\lambda x^A.\, t$	`fun (x : A) => t`
$r\, s$	`r s`
$()$	`I`
(r, s)	`conj r s`
$\mathsf{fst}\, r$	`proj1 r`
$\mathsf{snd}\, r$	`proj2 r`
$\mathsf{inl}\, r : A \vee B$	`or_introl B r`
$\mathsf{inr}\, r : A \vee B$	`or_intror A r`
$\mathsf{case}\, r\, \mathsf{of}\, \mathsf{inl}\, x^A \Rightarrow s \mid \mathsf{inr}\, y^B \Rightarrow t$	`match r with | or_introl x => s | or_intror y => t end`
$\mathsf{abort}_C\, r$	`match r return C with end`

Tabelle 4: Beweisterme in Coq.

benötigen als erstes Argument die Aussage der Disjunktion, die *nicht* vom Beweisterm (zweites Argument) beweisen wird. In einem `match`-Ausdruck muss dieses zusätzliche Argument aber wegelassen werden. Die $\bot$E-Term `abort` wird als Fallunterscheidung über 0 Alternativen repräsentiert. Die durch ein `match` zu beweisende Aussage `C` kann immer mit `return C` angegeben werden, muss aber nicht.

9 Herleitbare und zulässige Regeln

Wir verwenden J als Abkürzung für ein Urteil (engl. *judgement*), z.B. $\Gamma \vdash A$ oder $\Gamma \vdash t : A$.

Definition 2 (Herleitbare Regel) Eine Beweisregel

$$\frac{J_1 \dots J_n}{J}$$

heisst *herleitbar* (engl. *derivable*), falls es einen Beweisbaum von J mit Blättern $J_1, \dots, J_n$ gibt.

Beispiel 3 (Schnittregel) Die Regel

$$\frac{\Gamma \vdash A \qquad \Gamma, A \vdash B}{\Gamma \vdash B}\,\mathsf{cut}$$

ist im Kalkül des Natürlichen Schließens herleitbar. Wir geben eine Herleitung mit Beweistermen an:

$$\frac{\Gamma \vdash s : A \qquad \dfrac{\Gamma,\, x{:}A \vdash t : B}{\Gamma \vdash \lambda x^A.\, t : A \Rightarrow B}\Rightarrow\!\mathsf{I}}{\Gamma \vdash (\lambda x^A.\, t)\, s : B}\Rightarrow\!\mathsf{E}$$

Definition 4 (Zulässige Regel) Eine Beweisregel

$$\frac{J_1 \dots J_n}{J}$$

heisst *zulässig* (engl. *admissible*), falls aus den Herleitungen von $J_1, \dots, J_n$ eine Herleitung von J berechnet werden kann.

Beispiel 5 Die beiden Regeln

$$\frac{\Gamma \vdash t : A}{\Gamma, \Gamma' \vdash t : A}\,\mathsf{weak} \qquad \frac{\Gamma, x{:}A \vdash t : B \qquad \Gamma \vdash s : A}{\Gamma \vdash t[s/x] : B}\,\mathsf{subst}$$

sind zulässig. Beweis siehe folgende Lemmata.

Lemma 6 (Abschwächung) *Wenn* $\Gamma \vdash t : A$*, dann* $\Gamma, \Gamma' \vdash t : A$*.*

Proof. Durch Induktion über die Herleitung von $\Gamma \vdash t : A$. □

Lemma 7 (Substitution) *Wenn* $\Gamma \vdash s : A$ *und* $\Gamma, x : A \vdash t : B$*, dann* $\Gamma \vdash t[s/x] : B$*.*

Proof. Durch Induktion über die zweite Herleitung. □

10 Fragment $\Rightarrow\wedge\top$: Beweisreduktionen und normale Beweise

10.1 Beweisreduktionen

β-Reduktionen. Die Einführung eines logischen Konnektives, unmittelbar gefolgt von dessen Beseitigung, stellt einen Umweg im Beweis dar, der schematisch entfernt werden kann.

Konjunktion.

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ \Gamma \vdash r : A\end{array} \qquad \begin{array}{c}\vdots\\ \Gamma \vdash s : B\end{array}}{\Gamma \vdash (r,s) : A \wedge B}\,\wedge\mathsf{I}}{\Gamma \vdash \mathsf{fst}\,(r,s) : A}\,\wedge\mathsf{E}_1 \quad \longrightarrow \quad \begin{array}{c}\vdots\\ \Gamma \vdash r : A\end{array}$$

Analog für $\wedge\mathsf{I}$ gefolgt von $\wedge\mathsf{E}2$

Implikation.

$$\dfrac{\dfrac{\dfrac{}{\Gamma, x{:}A, \Gamma' \vdash x : A}\,\mathsf{hyp}}{\Gamma, x{:}A \vdash t : B}\,\Rightarrow\mathsf{I}}{\Gamma \vdash \lambda x t : A \to B} \qquad \begin{array}{c}\vdots\\ \Gamma \vdash s : A\end{array}}{\Gamma \vdash (\lambda x t)\, s : B}\,\Rightarrow\mathsf{E} \quad \longrightarrow \quad \begin{array}{c}\vdots\\ \Gamma, \Gamma' \vdash s : A\\ \vdots\\ \Gamma \vdash t[s/x] : B\end{array}$$

Tautologie. Für $\top$ gibt es keine Beseitigungsregel, daher keine β-Reduktion.

Zusammenfassung β-Reduktion.

$$\begin{array}{lll} (\beta_{\wedge 1}) & \mathsf{fst}\,(r,s) & \longrightarrow \; r \\ (\beta_{\wedge 2}) & \mathsf{snd}\,(r,s) & \longrightarrow \; s \\ \\ (\beta_{\Rightarrow}) & (\lambda x^A t)\, s & \longrightarrow \; t[s/x] \end{array}$$

Der jeweils linke Term heißt *Redex*, der rechte *Redukt*.

An jeder Stelle des Beweisbaumes darf eine Reduktion durchgeführt werden. Zu den fünf Reduktionsaxiomen kommt noch folgende Kongruenz-Regel hinzu:

$$\dfrac{t \longrightarrow t'}{C[t] \longrightarrow C[t']}$$

Dabei ist $C[\bullet]$ ein *Kontext*, also ein Term mit genau einem Loch $\bullet$, und $C[t]$ bezeichnet die Einsetzung des Terms t für das Loch. Es genügt, die Regel für Kontexte der Tiefe 1 anzunehmen.

$$C \quad ::= \quad \lambda x.\bullet \mid \bullet\, s \mid r\, \bullet \mid (\bullet, r) \mid (s, \bullet) \mid \mathsf{fst}\, \bullet \mid \mathsf{snd}\, \bullet$$

Theorem 8 (Subject reduction) *Wenn* $\Gamma \vdash t : A$ *und* $t \longrightarrow t'$*, dann auch* $\Gamma \vdash t' : A$*.*

Proof. Durch Induktion über die Herleitung von $t \longrightarrow t'$. □

10.2 Normale Beweise

Ein *normaler* Beweis ist ein Beweis ohne Umwege (β-Redexe). Ein *neutraler* Beweis kann in einen normalen Anstelle einer Hypothese eingesetzt werden, ohne dass ein Redex entsteht.

Definition 9 (Normal und neutral)

1. Ein Beweisterm t heißt normal, falls es keinen Term t' gibt, so dass $t \longrightarrow t'$.
2. Ein Beweisterm s heißt neutral, falls er zusätzlich nicht in einer Einführung endet. (Also keine λ-Abstraktion und kein Tupel ist.)

Charakterisierung der normalen und neutralen Beweise.

$$\begin{array}{ll} \Gamma \vdash t \downarrow A & t \text{ ist ein neutraler Beweis von } A \\ \Gamma \vdash t \uparrow A & t \text{ ist ein normaler Beweis von } A \end{array}$$

Die erste Regel besagt: Jeder neutrale Term ist auch normal.

$$\frac{\Gamma \vdash r \downarrow A}{\Gamma \vdash r \uparrow A}\,{\downarrow\uparrow} \qquad \frac{(x\!:\!A) \in \Gamma}{\Gamma \vdash x \downarrow A}\,\mathsf{hyp}$$

$$\frac{\Gamma, x\!:\!A \vdash t \uparrow B}{\Gamma \vdash \lambda x^A.\, t \uparrow A \Rightarrow B}\,{\Rightarrow}\mathsf{I} \qquad \frac{\Gamma \vdash r \downarrow A \Rightarrow B \qquad \Gamma \vdash s \uparrow A}{\Gamma \vdash r\, s \downarrow B}\,{\Rightarrow}\mathsf{E}$$

$$\frac{\Gamma \vdash r \uparrow A \qquad \Gamma \vdash s \uparrow B}{\Gamma \vdash (r,\, s) \uparrow A \wedge B}\,{\wedge}\mathsf{I} \qquad \frac{\Gamma \vdash r \downarrow A \wedge B}{\Gamma \vdash \mathsf{fst}\, r \downarrow A}\,{\wedge}\mathsf{E}_1 \qquad \frac{\Gamma \vdash r \downarrow A \wedge B}{\Gamma \vdash \mathsf{snd}\, r \downarrow B}\,{\wedge}\mathsf{E}_2$$

$$\frac{}{\Gamma \vdash () \uparrow \top}\,\top\mathsf{I}$$

Theorem 10 (Korrektheit) *Wenn* $\Gamma \vdash t \downarrow C$ *oder* $\Gamma \vdash t \uparrow C$*, dann ist* t *normal.*

Sei $\longrightarrow^*$ die reflexiv-transitive Hülle von $\longrightarrow$.

Theorem 11 (Normalisierung) *Wenn* $\Gamma \vdash t : A$*, dann gibt es ein* t' *mit* $t \longrightarrow^* t'$ *und* $\Gamma \vdash t \uparrow A$*.*

Anwendung: Wenn es keinen normalen Beweis einer Aussage gibt, so ist die Aussage im Kalkül des natürlichen Schließens überhaupt nicht beweisbar, also konstruktiv nicht gültig.

Beispiel 12 (Peirce-Formel) Die Formel $P \equiv ((A \Rightarrow B) \Rightarrow A) \Rightarrow A$ ist eine klassische Tautologie, aber konstruktiv nicht gültig. Man sieht leicht, dass ein normaler Beweis von P scheitern muss.

11 Volle Aussagenlogik: Beweisreduktionen und normale Beweise

Bei der Behandlung des natürlichen Schließens haben wir gesehen, dass Einführungsregeln dazu dienen, Beweise für größere Aussagen aus Beweisen kleinerer Aussagen zu konstruieren, und mit Eliminationsregeln hypothetische Beweise zerlegt werden können um sie für die Konstruktion von neuen Beweisen nutzbar zu machen. Der Kalkül allerdings erlaubt auch Umwege, d.h. die Konstruktion eines Beweises gefolgt von seiner sofortigen Zerlegung. Z.B.

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ \Gamma \vdash r : A\end{array} \qquad \begin{array}{c}\vdots\\ \Gamma \vdash s : B\end{array}}{\Gamma \vdash (r, s) : A \wedge B}\,\wedge\mathsf{I}}{\Gamma \vdash \mathsf{fst}\,(r, s) : A}\,\wedge\mathsf{E}_1$$

Im Folgenden zeigen wir, wie wir solche Umwege durch Beschränkung der Benutzung der I-Regeln auf die Konstruktionsphase und der E-Regeln auf die Zerlegungsphase verhindern können. Umwegsfreie Beweise bezeichnen wir als *normal*. Danach zeigen wir, wie wir Umwege in Beweisen durch Beweisreduktionen systematisch entfernen können.

11.1 Normale Beweise

Es wird sich zeigen, dass normale Beweisterme keiner Annotationen bedürfen, um aus Korrektheit geprüft zu werden. Wir können daher auf reine λ-Terme zurückfallen.

Beweisterme (Curry-Stil):

$$\begin{array}{rcl} r, s, t & ::= & x \mid \lambda x t \mid r\ s \\ & & \mid (r, s) \mid \mathsf{fst}\, r \mid \mathsf{snd}\, r \\ & & \mid \mathsf{inl}\, t \mid \mathsf{inl}\, t \mid \mathsf{case}\, r\ \mathsf{of}\ \mathsf{inl}\, x \Rightarrow s \mid \mathsf{inr}\, y \Rightarrow t \\ & & \mid () \\ & & \mid \mathsf{abort}\, r \end{array}$$

Wir versehen nun den Kalkül des natürlichen Schließens mit zwei *Modi*:

- Konstruktions-/Synthese-Modus: Wir beweisen eine zusammengesetzte Aussage durch Beweise (eines) ihrer Teile. Darunter fallen die Regeln $\Rightarrow\mathsf{I}$, $\wedge\mathsf{I}$, $\vee\mathsf{I}_1$, $\vee\mathsf{I}_2$, $\top\mathsf{I}$. Diesem Modus ist der Pfeil $\uparrow$ zugeordnet, der die Leserichtung der Regeln bei der Beweissuche andeuted: Von der Folgerung (*conclusion*) zu den Voraussetzungen (*premises*). In dieser Leserichtung wird die zu beweisende Aussage kleiner.
- Zerlegungs/Analyse-Modus: Wir zerlegen eine Annahme in ihre Teile. Vorzeigeinstanzen dieser Regel sind nur $\wedge\mathsf{E}_1$ und $\wedge\mathsf{E}_2$. Die Regel hyp macht

eine Annahme für die Analyse verfügbar. Durch die Regel $\downarrow\uparrow$ können wir den Modus wechseln. So kann eine (zerlegte) Annahme in Konstruktionen verwendet werden. Alternative Sichtweise: Komme ich in der Konstruktion nicht mehr weiter, z.B. weil die zu beweisende Formel atomar ist, so muss ich die Formel durch Analyse der Annahmen beweisen.

$$\frac{\Gamma \vdash r \downarrow A}{\Gamma \vdash r \uparrow A}\downarrow\uparrow \qquad \frac{(x{:}A) \in \Gamma}{\Gamma \vdash x \downarrow A}\,\mathsf{hyp}$$

$$\frac{\Gamma, x{:}A \vdash t \uparrow B}{\Gamma \vdash \lambda x t \uparrow A \Rightarrow B}\Rightarrow\!\mathsf{I} \qquad \frac{\Gamma \vdash r \downarrow A \Rightarrow B \qquad \Gamma \vdash s \uparrow A}{\Gamma \vdash r\, s \downarrow B}\Rightarrow\!\mathsf{E}$$

$$\frac{\Gamma \vdash r \uparrow A \qquad \Gamma \vdash s \uparrow B}{\Gamma \vdash (r,\, s) \uparrow A \wedge B}\wedge\mathsf{I} \qquad \frac{\Gamma \vdash r \downarrow A \wedge B}{\Gamma \vdash \mathsf{fst}\, r \downarrow A}\wedge\mathsf{E}_1 \qquad \frac{\Gamma \vdash r \downarrow A \wedge B}{\Gamma \vdash \mathsf{snd}\, r \downarrow B}\wedge\mathsf{E}_2$$

$$\frac{\Gamma \vdash t \uparrow A}{\Gamma \vdash \mathsf{inl}\, t \uparrow A \vee B}\vee\mathsf{I}_1 \qquad \frac{\Gamma \vdash t \uparrow B}{\Gamma \vdash \mathsf{inr}\, t \uparrow A \vee B}\vee\mathsf{I}_2$$

$$\frac{\Gamma \vdash r \downarrow A \vee B \qquad \Gamma, x{:}A \vdash s \uparrow C \qquad \Gamma, y{:}B \vdash t \uparrow C}{\Gamma \vdash \mathsf{case}\, r\, \mathsf{of}\, \mathsf{inl}\, x \Rightarrow s \mid \mathsf{inr}\, y \Rightarrow t \uparrow C}\vee\mathsf{E}$$

$$\frac{}{\Gamma \vdash () \uparrow \top}\top\mathsf{I} \qquad \frac{\Gamma \vdash r \downarrow \bot}{\Gamma \vdash \mathsf{abort}\, r \uparrow C}\bot\mathsf{E}$$

Die Mehrzahl der Eliminationsregeln ($\Rightarrow\!\mathsf{E}$, $\vee\mathsf{E}$, $\bot\mathsf{E}$) erwähnt beide Modi. Diese Regeln werden nun noch einzeln erklärt:

$\Rightarrow\!\mathsf{E}$ Um sich eine Hypothese der Form $A \Rightarrow B$ zunutze machen, d.h., zu zerlegen, muss man zuerst A beweisen. Dies muss unter Umständen durch Konstruktionen geschehen und erzeugt keine Umwege. Zum Beispiel wollen wir C aus A und $(A \vee B) \Rightarrow C$ beweisen. Aus der Annahme A konstruieren wir $A \vee B$ mit $\vee\mathsf{I}_1$, danach können wir die Annahme $(A \vee B) \Rightarrow C$ verwenden und erhalten C.

$$\dfrac{\dfrac{y \downarrow (A \vee B) \Rightarrow C \qquad \dfrac{\dfrac{x \downarrow A}{x \uparrow A}\downarrow\uparrow}{\mathsf{inl}\, x \uparrow A \vee B}\vee\mathsf{I}_1}{y\,(\mathsf{inl}\, x) \downarrow C}\Rightarrow\!\mathsf{E}}{y\,(\mathsf{inl}\, x) \uparrow C}\downarrow\uparrow$$

$\vee\mathsf{E}$ Hat man eine *Annahme* der Form $A \vee B$, kann man daraus nicht A oder B folgern, da man nicht weiss, welches der beiden wahr ist. (Ist $A \vee B$ jedoch *konstruiert*, kann man durch Inspektion des Beweises sehen ob A oder B wahr ist.) Will man nun die Annahme $A \vee B$ für den Beweis

einer dritten Aussage C verwenden, so muss man auf beide Möglichkeiten gefasst sein, d.h. man muss einen Beweis von C unter der Annahme von A bereitstellen, und einen Beweis von C unter der Annahme von B. Diese Beweise können im Allgemeinen konstruiert sein, daher der Modus $\uparrow$. Im Folgenden beweisen wir B aus den Annahmen $v : A$ und $x : B \vee (A \Rightarrow B)$.

$$\dfrac{x \downarrow B \vee (A \Rightarrow B) \qquad \dfrac{\dfrac{}{y \downarrow B}\,\mathsf{hyp}}{y \uparrow B}\downarrow\uparrow \qquad \dfrac{\dfrac{}{z \downarrow A \Rightarrow B}\,\mathsf{hyp} \qquad \dfrac{v \downarrow A}{v \uparrow A}\downarrow\uparrow}{z\,v \downarrow B}\Rightarrow\mathsf{E}}{z\,v \uparrow B}\downarrow\uparrow}{B}\vee\mathsf{E}$$

Die lokalen Annahmen y und z werden durch $\vee\mathsf{E}$ eingeführt.

$\bot\mathsf{E}$ Die Form dieser Regel ist analog zu $\vee\mathsf{E}$, wenn man das Falsum $\bot$ als *Disjunktion mit null Alternativen* betrachtet. Die Annahme $\bot$ ist nicht weiter zerlegbar; jedoch kann jede Aussage C durch aus $\bot$ trivial bewiesen werden: *ex falsum quot libet.*

Führen wir folgende Bezeichnungen ein: Falls $\Gamma \vdash t \uparrow C$ eine gültige Herleitung hat, so heisse der Beweisterm t *normal*. Falls $\Gamma \vdash t \downarrow C$ eine gültige Herleitung hat, so heisse t *neutral*.

Warum können wir hier mit Termen im Curry-Stil arbeiten, brauchen also die Annotationen, die Terme im Church-Stil bei sich tragen, nicht mehr? Nun, im Falle von $\lambda x^A.t$, $\mathsf{inl}_B\, t$, $\mathsf{inr}_A\, t$ und $\mathsf{abort}_C\, r$ befinden wir uns im Konstruktionsmodus, wissen also, welche Aussage wir gerade beweisen. Im Falle von $\mathsf{case}\, r\ \mathsf{of}\ \mathsf{inl}\, x^A \Rightarrow s \mid \mathsf{inr}\, y^B \Rightarrow t$ ist r von den Annahmen hergeleitet worden, es muss von der Form $A \vee B$ sein, also können wir A und B daraus ablesen.

Übung 13 (Bidirectional type-checking) Definieren Sie durch wechselseitige Rekursion über r Funktionen $\mathsf{check}(\Gamma, r, A)$ und $\mathsf{infer}(\Gamma, r)$. Dabei soll $\mathsf{check}(\Gamma, r, A)$ *wahr* zurückliefern gdw. $\Gamma \vdash r \uparrow A$, und $\mathsf{infer}(\Gamma, r)$ soll A zurückliefern gdw. $\Gamma \vdash r \downarrow A$.

11.2 Beweisreduktionen

Was ist nun von allgemeinen, nicht-normalen Beweisen $\Gamma \vdash t : C$ zu halten? Sie können durch Beweisreduktionen in normale überführt werden. Dies zeigen wir im Folgenden.

β-Reduktionen. Die Einführung eines logischen Konnektives, unmittelbar gefolgt von dessen Beseitigung, stellt einen Umweg im Beweis dar, der schematisch entfernt werden kann.

Konjunktion.

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ \Gamma \vdash r : A\end{array} \qquad \begin{array}{c}\vdots\\ \Gamma \vdash s : B\end{array}}{\Gamma \vdash (r, s) : A \wedge B}\,\wedge\mathsf{I}}{\Gamma \vdash \mathsf{fst}\,(r, s) : A}\,\wedge\mathsf{E}_1 \qquad \longrightarrow \qquad \begin{array}{c}\vdots\\ \Gamma \vdash r : A\end{array}$$

Analog für $\wedge\mathsf{I}$ gefolgt von $\wedge\mathsf{E}2$

Implikation.

$$\dfrac{\dfrac{\dfrac{}{\Gamma, x{:}A, \Gamma' \vdash x : A}\,\mathsf{hyp}}{\Gamma, x{:}A \vdash t : B}\,\Rightarrow\mathsf{I} \qquad \begin{array}{c}\vdots\\ \Gamma \vdash s : A\end{array}}{\Gamma \vdash (\lambda x t)\, s : B}\,\Rightarrow\mathsf{E} \qquad \longrightarrow \qquad \begin{array}{c}\vdots\\ \Gamma, \Gamma' \vdash s : A\\ \vdots\\ \Gamma \vdash t[s/x] : B\end{array}$$

Disjunktion.

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ \Gamma \vdash r : A\end{array}}{\Gamma \vdash \mathsf{inl}\, r : A \vee B}\,\vee\mathsf{I}_1 \qquad \dfrac{}{\Gamma, x{:}A, \Gamma' \vdash x : A}\,\mathsf{hyp} \qquad \begin{array}{c}\vdots\\ \Gamma \vdash x{:}A \vdash s : C\end{array} \qquad \dfrac{}{\Gamma, y{:}B, \Gamma' \vdash y : B}\,\mathsf{hyp} \qquad \begin{array}{c}\vdots\\ \Gamma \vdash y{:}B \vdash t : C\end{array}}{\Gamma \vdash \mathsf{case}\,\mathsf{inl}\, r\ \mathsf{of}\ \mathsf{inl}\, x \Rightarrow s \mid \mathsf{inr}\, y \Rightarrow t : C}\,\vee\mathsf{E}$$

$$\longrightarrow \qquad \begin{array}{c}\vdots\\ \Gamma, \Gamma' \vdash r : A\\ \vdots\\ \Gamma \vdash s[r/x] : C\end{array}$$

Analog für $\vee\mathsf{I}_2$ gefolgt von $\vee\mathsf{E}$.

Tautologie, Absurdität. Für $\top$ und $\bot$ gibt es jeweils nur entweder Einführungs- oder Beseitigungsregel, daher keine β-Reduktion.

Zusammenfassung β-Reduktion.

$$\begin{array}{lll}
(\beta_{\wedge 1}) & \mathsf{fst}\,(r, s) & \longrightarrow\ r\\
(\beta_{\wedge 2}) & \mathsf{snd}\,(r, s) & \longrightarrow\ s\\
(\beta_{\Rightarrow}) & (\lambda x t)\, s & \longrightarrow\ t[s/x]\\
(\beta_{\vee 1}) & \mathsf{case}\,\mathsf{inl}\, r\ \mathsf{of}\ \mathsf{inl}\, x \Rightarrow s \mid \mathsf{inr}\, y \Rightarrow t & \longrightarrow\ s[r/x]\\
(\beta_{\vee 2}) & \mathsf{case}\,\mathsf{inr}\, r\ \mathsf{of}\ \mathsf{inl}\, x \Rightarrow s \mid \mathsf{inr}\, y \Rightarrow t & \longrightarrow\ t[r/y]
\end{array}$$

Auswertungskontexte.

$$e ::= \bullet\, s \mid \mathsf{fst}\,\bullet \mid \mathsf{snd}\,\bullet \mid \mathsf{case}\,\bullet\,\mathsf{of}\,\mathsf{inl}\,x \Rightarrow s \mid \mathsf{inr}\,y \Rightarrow t \mid \mathsf{abort}_C\,\bullet$$

Permutations-Reduktionen.

$$\begin{array}{lll} (\pi_\vee) & e[\mathsf{case}\,r\,\mathsf{of}\,\mathsf{inl}\,x \Rightarrow s \mid \mathsf{inr}\,y \Rightarrow t] & \longrightarrow \quad \mathsf{case}\,r\,\mathsf{of}\,\mathsf{inl}\,x \Rightarrow e[s] \mid \mathsf{inr}\,y \Rightarrow e[t] \\ (\pi_\bot) & e[\mathsf{abort}\,r] & \longrightarrow \quad \mathsf{abort}\,r \end{array}$$

Bemerkung 14 Für Church-Terme wäre die Regel $e[\mathsf{abort}_C\,r] \longrightarrow \mathsf{abort}_X\,r$ so problematisch, es gibt allerdings einen sehr einfachen Algorithmus, der aus e und dem Typ A des Loches in e den Typ $X = e[A]$ des Kontextes e berechnet. Dieser funktioniert allerdings nur für wohlgetypte Terme.

$$\begin{array}{lcl} e[(A \Rightarrow B)\,s] & = & e[B] \\ e[\mathsf{fst}\,(A \wedge B)] & = & e[A] \\ e[\mathsf{snd}\,(A \wedge B)] & = & e[B] \\ e[\mathsf{abort}_A\,\bot] & = & e[A] \\ e[\mathsf{case}\,A \vee B\,\mathsf{of}\,\mathsf{inl}\,x^A \Rightarrow s \mid \mathsf{inr}\,y^B \Rightarrow t] & = & ??? \end{array}$$

Hier reichen sogar die Annotationen an case nicht!

Kongruenz. An jeder Stelle des Beweisbaumes darf eine Reduktion durchgeführt werden. Zu den fünf Reduktionsaxiomen kommt noch folgende Kongruenz-Regel hinzu:

$$\frac{t \longrightarrow t'}{C[t] \longrightarrow C[t']}$$

Dabei ist $C[\bullet]$ ein *Kontext*, also ein Term mit genau einem Loch $\bullet$, und $C[t]$ bezeichnet die Einsetzung des Terms t für das Loch.

Nun können wir die Begriffe *normal* und *neutral* noch einmal neu definieren, diesmal abstrakter: Ein *normaler* Beweis ist ein Beweis ohne Umwege. Ein *neutraler* Beweis kann in einen normalen Anstelle einer Hypothese eingesetzt werden, ohne dass ein Umweg entsteht.

Definition 15 (Normal und neutral)

1. Ein Beweisterm t heißt normal, falls es keinen Term t' gibt, so dass $t \longrightarrow t'$.
2. Ein Beweisterm s heißt neutral, falls dessen Einsetzung $t[s/x]$ in einen beliebigen normalen Term t wieder normal ist.

Die bisherigen Definitionen von normal und neutral waren korrekt, jedoch vollständig nur für wohlgetypte Terme.

Theorem 16 (Korrektheit)

1. *Wenn* $\Gamma \vdash t \downarrow C$ *oder* $\Gamma \vdash t \uparrow C$, *dann ist* t *normal.*
2. *Wenn* $\Gamma \vdash s \downarrow A$ *und* $\Gamma, x{:}A, \Gamma' \vdash t \uparrow C$, *dann ist* $\Gamma, \Gamma' \vdash t[s/x] \uparrow C$.

Lemma 17 (Subject reduction) *Wenn* $\Gamma \vdash t : A$ *und* $t \longrightarrow t'$*, dann auch* $\Gamma \vdash t' : A$*.*

Proof. Durch Induktion über die Herleitung von $\Gamma \vdash t : A$. □

Alternativ kann *subject reduction* auch über die Herleitung von $t \longrightarrow t'$ beweisen werden, dann sollte aber die Kongruenzregel verfeinert werden, dass nur Kontexte der Tiefe 1 zugelassen werden.

$$\begin{array}{rcl} c & ::= & \lambda x.\bullet \mid \bullet\, s \mid r\, \bullet \mid (\bullet, r) \mid (s, \bullet) \mid \mathsf{fst}\, \bullet \mid \mathsf{snd}\, \bullet \\ & \mid & \mathsf{case}\, \bullet\, \mathsf{of}\, \mathsf{inl}\, x \Rightarrow s \mid \mathsf{inr}\, y \Rightarrow r \mid \mathsf{case}\, r\, \mathsf{of}\, \mathsf{inl}\, x \Rightarrow \bullet \mid \mathsf{inr}\, s \Rightarrow t \\ & \mid & \mathsf{case}\, r\, \mathsf{of}\, \mathsf{inl}\, x \Rightarrow s \mid \mathsf{inr}\, y \Rightarrow \bullet \mid \mathsf{abort}\, \bullet \end{array}$$

12 Sequenzenkalkül

Teilformeleigenschaft.

Klassischer Sequenzenkalkül LK. Hat zwei ∨R Regeln, mit Kontraktion ist das äquivalent zu dem in PVS implementierten Sequenzenkalkül mit nur einer ∨R-Regel. Den intuitionistischen Sequenzenkalkül LJ erhält man aus LK durch Beschränkung der rechten Seite auf höchstens eine Formel, wobei die leere rechte Seite mit ⊥ gleichgesetzt wird. (Strukturregeln rechts fallen alle weg.)

Beweissuche mittels Sequenzenkalkül. Ein anderer Zugang zu schnittfreiem Sequenzenkalkül geht über normale ND-Beweise.

12.1 Sequenzenkalkül für Beweissuche

Intuitionistischer Sequenzenkalkül.

$$\frac{}{\Gamma, A \Longrightarrow A}\,\mathsf{hyp}$$

$$\frac{\Gamma, A \Rightarrow B, B \Longrightarrow C \qquad \Gamma, A \Rightarrow B \Longrightarrow A}{\Gamma, A \Rightarrow B \Longrightarrow C}\,{\Rightarrow}\mathsf{L} \qquad \frac{\Gamma, A \Longrightarrow B}{\Gamma \Longrightarrow A \Rightarrow B}\,{\Rightarrow}\mathsf{R}$$

$$\frac{\Gamma, A, B \Longrightarrow C}{\Gamma, A \wedge B \Longrightarrow C}\,{\wedge}\mathsf{L} \qquad \frac{\Gamma \Longrightarrow A \qquad \Gamma \Longrightarrow B}{\Gamma \Longrightarrow A \wedge B}\,{\wedge}\mathsf{R}$$

$$\frac{\Gamma, A \Longrightarrow C \qquad \Gamma, B \Longrightarrow C}{\Gamma, A \vee B \Longrightarrow C}\,{\vee}\mathsf{L} \qquad \frac{\Gamma \Longrightarrow A}{\Gamma \Longrightarrow A \vee B}\,{\vee}\mathsf{R}_1 \qquad \frac{\Gamma \Longrightarrow B}{\Gamma \Longrightarrow A \vee B}\,{\vee}\mathsf{R}_2$$

$$\frac{}{\Gamma, \bot \Longrightarrow C}\,\bot\mathsf{L} \qquad \frac{}{\Gamma \Longrightarrow \top}\,\top\mathsf{R}$$

Sequenzenkalkül als Produzent normaler Terme.

$$\frac{}{\Gamma,\ r \downarrow A \Longrightarrow r \uparrow A}\ \mathsf{hyp}$$

$$\frac{\Gamma,\ r \downarrow A \Rightarrow B,\ r\,s \downarrow B \Longrightarrow t \uparrow C \qquad \Gamma,\ r \downarrow A \Rightarrow B \Longrightarrow s \uparrow A}{\Gamma,\ r \downarrow A \Rightarrow B \Longrightarrow t \uparrow C}\ \Rightarrow\mathsf{L}$$

$$\frac{\Gamma,\ x \downarrow A \Longrightarrow t \uparrow B}{\Gamma \Longrightarrow \lambda x t \uparrow A \Rightarrow B}\ \Rightarrow\mathsf{R}$$

$$\frac{\Gamma,\ \mathsf{fst}\,r \downarrow A,\ \mathsf{snd}\,r \downarrow B \Longrightarrow t \uparrow C}{\Gamma,\ r \downarrow A \wedge B \Longrightarrow t \uparrow C}\ \wedge\mathsf{L} \qquad \frac{\Gamma \Longrightarrow t_1 \uparrow A \qquad \Gamma \Longrightarrow t_2 \uparrow B}{\Gamma \Longrightarrow (t_1, t_2) \uparrow A \wedge B}\ \wedge\mathsf{R}$$

$$\frac{\Gamma,\ x \downarrow A \Longrightarrow s \uparrow C \qquad \Gamma,\ x \downarrow B \Longrightarrow t \uparrow C}{\Gamma,\ r \downarrow A \vee B \Longrightarrow \mathsf{case}\,r\,\mathsf{of}\,\mathsf{inl}\,x \Rightarrow s \mid \mathsf{inr}\,y \Rightarrow t \uparrow C}\ \vee\mathsf{L}$$

$$\frac{\Gamma \Longrightarrow t \uparrow A}{\Gamma \Longrightarrow \mathsf{inl}\,t \uparrow A \vee B}\ \vee\mathsf{R}_1 \qquad \frac{\Gamma \Longrightarrow t \uparrow B}{\Gamma \Longrightarrow \mathsf{inr}\,t \uparrow A \vee B}\ \vee\mathsf{R}_2$$

$$\frac{}{\Gamma,\ r \downarrow \bot \Longrightarrow \mathsf{abort}\,r \uparrow C}\ \bot\mathsf{L} \qquad \frac{}{\Gamma \Longrightarrow () \uparrow \top}\ \top\mathsf{R}$$

13 Kripke-Modelle

Ein Aussagenlogisches Kripke-Modell ist ein Tripel $(K, \geq, \Vdash)$ so dass

- K ist eine nicht-leere Menge von Welten,
- $\geq$ ist partielle Präordnung auf K (reflexiv, transitiv),
- $\Vdash$ ist eine Relation zwischen Welten und Aussagenvariablen, $k \Vdash P$ bedeuted "k erfüllt P"
- die Erfüllungsrelation $\Vdash$ ist monoton, d.h.

$$k \Vdash P \quad \text{und} \quad k' \geq k \quad \text{implizieren} \quad k' \Vdash P$$

Die Erfüllungsrelation wird wie folgt auf Aussagen erweitert:

- $k \Vdash A \wedge B$ gdw. $k \Vdash A$ und $k \Vdash B$
- $k \Vdash A \vee B$ gdw. $k \Vdash A$ oder $k \Vdash B$
- $k \Vdash A \Rightarrow B$ gdw. für alle $k' \geq k$, wenn $k' \Vdash A$, dann $k' \Vdash B$
- $k \nVdash \bot$

Übung 18 Zeigen Sie: Falls $k \Vdash A$ und $k' \geq k$, dann $k' \Vdash A$.

14 Vollständigkeit

Literatur

[Kol32] Andrei Kolmogorov. Zur deutung der intuitionistischen logik. *Mathematische Zeitschrift*, 35:58–65, 1932.