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

1.10.1 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.

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

Analog für $\wedge\mathsf{I}$ gefolgt von $\wedge\mathsf{E2}$

Implikation.

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

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

Zusammenfassung β-Reduktion.

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

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:

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

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. 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 $\Gamma \vdash t' : A$.*

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

1.10.2 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)

1. *$\Gamma \vdash t \downarrow C$ gdw. $\Gamma \vdash t : C$ und t neutral.*
2. *$\Gamma \vdash t \uparrow C$ gdw. $\Gamma \vdash t : C$ und t normal.*

Beweis. Simultan durch Induktion nach t. □

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 $\Gamma \vdash t \uparrow A$.*

Beweis. Wir definieren ein Maß auf Beweisen, das mit jedem Reduktionsschritt abnimmt. Dies kann nicht die Termgröße sein, den durch die Entfernung des Redexes $(\lambda x t)\, s$ kann der Term größer werden (Verdopplung von s. Z.B.: Der Redex von $(\lambda f \lambda x.\, f\,(f\,(f\,x)))\,(\lambda y.y)$ ist $\lambda x.\,(\lambda y.y)\,((\lambda y.y)\,((\lambda y.y)\,x))$. Es sind neue Redexe entstanden, die jedoch von geringerem *Rang* sind, wobei der Rang der Typ der substitutierten Variable ist. Sei $f : A \Rightarrow A$, dann ist der Rang des ursprünglichen Redexes $A \Rightarrow A$, die neuen Redexe $(\lambda y.y)\,\_$ haben nur Rang A, den Typen von y.

Wir definieren die Ordnung einer Aussage A rekursiv durch $|\top| = |P| = 0$, $|A \Rightarrow B| = \max(1 + |A|, |B|)$ und $|A \wedge B| = \max(|A|, |B|)$. Der Rang eines Redexes der Form $(\lambda x^A t)\, s$ sei $|A|$, ein Redex der Form $\mathsf{fst}\,(r, s) : A$ habe den Rang $|A|$. Gegeben ein Term t, sei $\#(t, 0)$ die Größe von t (Anzahl der Knoten in der Baumdarstellung von t) und $\#(t, n+1)$ die Anzahl der Redexe vom Rang n in t. Wir setzen $t > t'$ falls es ein $n \geq 0$ gibt mit $\#(t, n) > \#(t', n)$ und $\#(t, m) \geq \#(t', m)$ für alle $m > n$. Die so definierte (lexikographische) Ordnung ist wohlfundiert. Wir zeigen nun: Wenn $\Gamma \vdash t : A$ und $t \longrightarrow t'$ entfernt einen Redex r, dessen Rang den Rang jedes Redexes r' in einem echten Subterm von r übersteigt, dann $t > t'$. Damit erreicht man die Normalform in endlich vielen Schritten.

Einen solchen Redex findet man immer, jeder innerste Redex (also dessen Subterme keinen Redex enthalten), ist geeignet.

Reduzieren wir einen $\wedge$-Redex, z.B. $(t fst\,(r, s))\, t \longrightarrow r\, t$, so wird der Term kleiner. Es kann zwar ein neuer Redex, z.B. $r\,t$, entstanden sein, dessen Rang ist jedoch kleiner.

Der kritische Fall ist der $\Rightarrow$-Redex $(\lambda x^A t)\, s \longrightarrow t[s/x]$. Falls s keine Einführung ist, entstehen keine neuen Redexe, wir haben zwar den Term vergrößert und Redexe von in s vervielfacht, jedoch haben sie einen Rang $< |A|$. Ist s eine Einführung, können zusätzlich noch neue Redexe entstehen, diese haben jedoch kleineren Rang. Z.B. sei $s = \lambda y^B.s'$, dann ist zwingenderweise $A = B \Rightarrow C$, und enthalte t eine Subterm $x\,r$. Dann ensteht der neue Redex $(\lambda y^B.s')\, r$, jedoch nur vom Rang $|B|$. □

Alternativ können wir das Theorem auch direkt durch Induktion über t zeigen [JM03]. Für den Applikationsfall brauchen wir $\Gamma \vdash r \uparrow A \Rightarrow B$ und $\Gamma \vdash s \uparrow A$ impliziert $r\,s \longrightarrow^* t'$ und $\Gamma \vdash t' \uparrow B$. Dies folgt aus dem Substitutionslemma:

Lemma 12 (Substitution) *Wenn $\Gamma, x : A, \Gamma' \vdash t \uparrow C$ und $\Gamma \vdash s \uparrow A$, dann $t[s/x] \longrightarrow^* t'$ und $\Gamma, \Gamma' \vdash t' \uparrow C$.*

Beweis. Wir beweisen dies durch lexikographische Induktion über $(|A|, t)$, simultan mit: Wenn $\Gamma, x : A, \Gamma' \vdash t \downarrow C$ und $\Gamma \vdash s \uparrow A$, dann $t[s/x] \longrightarrow^* t'$ und entweder $\Gamma, \Gamma' \vdash t' \downarrow C$, oder $\Gamma, \Gamma' \vdash t' \uparrow C$ und $|C| \leq |A|$.

Im Fall $t = x$ ist $t[s/x] = s$ schon normal und $C = A$.

Im Fall $t = y$ ist $t[s/x] = y$ neutral.

Im Fall $t = t_1\, t_2$ gilt nach Induktionshypothese $t_1[s/x] \longrightarrow^* t_1'$ und $t_2[s/x] \longrightarrow^* t_2'$ mit $\Gamma, \Gamma' \vdash t_2' \uparrow A$. Falls $\Gamma, \Gamma' \vdash t_1' \downarrow B \Rightarrow C$, dann gilt sofort $\Gamma, \Gamma' \vdash t_1'\, t_2' \downarrow C$. Andernfalls ist $t_1' = \lambda yr$ für ein r und $\Gamma, \Gamma', y : B \vdash r \uparrow C$. Da $|B \Rightarrow C| < |A|$ nach Ind.hyp., also $|B| < |A|$, können wir die Ind.hyp. erneut anwenden und erhalten $r[t_2'/y] \longrightarrow^* r'$ und $\Gamma, \Gamma' \vdash r' \uparrow C$. Insgesamt $t_1\, t_2[s/x] \longrightarrow^* t_1' t_2' = (\lambda y.r)\, t_2' \longrightarrow r[t_2'/y] \longrightarrow^* r'$.

Die übrigen Fälle sind unproblematisch. □

Anwendung des Normalisierungs-Satzes: 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 13 (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.

1.11 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.

1.11.1 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):

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

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 $\Rightarrow$I, $\wedge$I, $\vee\mathsf{I}_1$, $\vee\mathsf{I}_2$, $\top$I. Diesem Modus ist der Pfeil $\uparrow$ zugeordnet, der die Leserichtung der Regeln bei der Beweissuche andeutet: 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.

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

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

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

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

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

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

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

$\Rightarrow$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.

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

$\vee$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 $x : B \lor (A \Rightarrow B)$.

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

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

$\bot\mathsf{E}$ Die Form dieser Regel ist analog zu $\lor\mathsf{E}$, 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 $A \lor B$ sein, also können wir A und B daraus ablesen.

Übung 14 (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. $\Gamma \vdash r \downarrow A$.

1.11.2 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.

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

Analog für $\wedge\mathsf{I}$ gefolgt von $\wedge\mathsf{E2}$

Implikation.

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

Disjunktion.

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

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

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.

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

Auswertungskontexte.

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

Permutations-Reduktionen.

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

Bemerkung 15 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.

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

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 16 (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 17 (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 18 (Subject reduction) *Wenn* $\Gamma \vdash t : A$ *und* $t \longrightarrow t'$, *dann auch* $\Gamma \vdash t' : A$.

Beweis. 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.

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

1.12 Sequenzenkalkül

Teilformeleigenschaft.

Klassischer Sequenzenkalkül LK. Hat zwei $\vee$R Regeln, mit Kontraktion ist das äquivalent zu dem in PVS implementierten Sequenzenkalkül mit nur einer $\vee$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 $\bot$ gleichgesetzt wird. (Strukturregeln rechts fallen alle weg.)

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

1.12.1 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.

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

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

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

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

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

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

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