Einführung in die konstruktive Logik

Andreas Abel

Dezember 2005

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 $\perp$ 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 $\Gamma \vdash A$. Γ sei eine Menge von Aussagen.

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

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

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

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

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

4 Beweisterme

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

Γ sei eine Menge von Variable-Aussage-Paaren, geschrieben $x\!:\!A$.

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

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

$$\wedge\mathsf{I}\ \frac{\Gamma \vdash r : A \qquad \Gamma \vdash s : B}{\Gamma \vdash (r,\, s) : A \wedge B} \qquad \wedge\mathsf{E}_1\ \frac{\Gamma \vdash r : A \wedge B}{\Gamma \vdash r.1 : A} \qquad \wedge\mathsf{E}_2\ \frac{\Gamma \vdash r : A \wedge B}{\Gamma \vdash r.2 : B}$$

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

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

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

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

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 $\top\mathsf{E}$.

5 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).

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 1: Propositionale Formeln in Coq.

Tabelle 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 und B erzeugt.
- `split` kann auch angewendet werden, falls das Ziel von der Form $A_1 \rightarrow \cdots \rightarrow A_n \rightarrow C$ ist und C eine Konjuktion. Dann werden vor der Aufsplit-

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 2: Natürliches Schließen in Coq.

tung 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`
$r.1$	`proj1 r`
$r.2$	`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 3: 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.

6 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 1 (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 2 (Schnittregel) Die Regel

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

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

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

Definition 3 (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 4 Die beiden Regeln

$$\mathsf{weak}\ \frac{\Gamma \vdash t : A}{\Gamma, \Gamma' \vdash t : A} \qquad \mathsf{subst}\ \frac{\Gamma, x{:}A \vdash t : B \qquad \Gamma \vdash s : A}{\Gamma \vdash t(x := s) : B}$$

sind zulässig. Beweis siehe folgende Lemmata.

Lemma 5 (Abschwächung) *Wenn $\Gamma \vdash t : A$, dann $\Gamma, \Gamma' \vdash t : A$.*

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

Lemma 6 (Substitution) *Wenn* $\Gamma \vdash s : A$ *und* $\Gamma, x\!:\!A \vdash t : B$, *dann* $\Gamma \vdash t(x := s) : B$.

Proof. Durch Induktion über die zweite Herleitung. $\square$

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

7.1 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.

$$\dfrac{\dfrac{\begin{matrix}\vdots\\ \Gamma \vdash r : A\end{matrix} \qquad \begin{matrix}\vdots\\ \Gamma \vdash s : B\end{matrix}}{\Gamma \vdash (r, s) : A \wedge B}\,\wedge\mathsf{I}}{\Gamma \vdash (r, s).1 : A}\,\wedge\mathsf{E}_1 \qquad \longrightarrow \qquad \begin{matrix}\vdots\\ \Gamma \vdash r : A\end{matrix}$$

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

Implikation.

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

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

Zusammenfassung β-Reduktion.

$$\begin{array}{lllll}
(\beta_{\wedge 1}) & (r, s).1 & \longrightarrow & r \\
(\beta_{\wedge 2}) & (r, s).2 & \longrightarrow & s \\[1ex]
(\beta_{\Rightarrow}) & (\lambda x^A t)\, s & \longrightarrow & t(x := s)
\end{array}$$

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.

$$C \quad ::= \quad \lambda x.\bullet \mid \bullet\, s \mid r\, \bullet \mid (\bullet, r) \mid (s, \bullet) \mid \bullet.1 \mid \bullet.2$$

Theorem 7 (Subject reduction) *Wenn $\Gamma \vdash t : A$ und $t \longrightarrow t'$, dann auch $\Gamma \vdash t' : A$.*

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

7.2 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 8 (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.

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

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

$$\wedge\mathsf{I}\ \frac{\Gamma \vdash r \uparrow A \qquad \Gamma \vdash s \uparrow B}{\Gamma \vdash (r,\, s) \uparrow A \wedge B} \qquad \wedge\mathsf{E}_1\ \frac{\Gamma \vdash r \downarrow A \wedge B}{\Gamma \vdash r.1 \downarrow A} \qquad \wedge\mathsf{E}_2\ \frac{\Gamma \vdash r \downarrow A \wedge B}{\Gamma \vdash r.2 \downarrow B}$$

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

Theorem 9 (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 10 (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 11 (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.