

Mathematik und Logik

Franz Binder

Institut für Algebra
Johannes Kepler Universität Linz

Vorlesung im 2006W

<http://www.algebra.uni-linz.ac.at/Students/Win/ml>

Inhalt

Aussagenlogik

Logische Implikation, \Rightarrow

Logische Konjunktion, \wedge

Logische Äquivalenz, \iff

Logische Disjunktion, \vee

Aussagenlogische Beweise

Logische Implikation, \Rightarrow

Logische Konjunktion, \wedge

Logische Disjunktion, \vee

Curry-Howard-Isomorphismus

Definition der Implikation, \Rightarrow

Formation

Sind P und Q Aussagen, dann bezeichnet $P \Rightarrow Q$ ebenfalls eine Aussage, die **Implikation** von P und Q .

Introduktion

Um $P \Rightarrow Q$ zu beweisen, muß man Q beweisen, wobei man einen Beweis von P voraussetzen darf.

Elimination

Hat man einen Beweis von $P \Rightarrow Q$, so reicht ein Beweis von P , um auch Q zu beweisen.

Schlußregeln

$$\frac{\begin{array}{|c|} \hline P \\ \hline \vdots \\ \hline Q \\ \hline \end{array}}{P \Rightarrow Q} \Rightarrow I$$

$$\frac{P \Rightarrow Q \quad P}{Q} \Rightarrow E$$

Definition der Konjunktion, \wedge

Formation

Sind P und Q Aussagen, dann bezeichnet $P \wedge Q$ ebenfalls eine Aussage, die **Konjunktion** von P und Q .

Introduktion

Um $P \wedge Q$ zu beweisen, muß man sowohl P als auch Q beweisen.

Elimination

Hat man einen Beweis von $P \wedge Q$ so auch einen Beweis von P , und auch einen Beweis von Q .

Schlußregeln

$$\frac{P \quad Q}{P \wedge Q} \wedge I$$

$$\frac{P \wedge Q}{P} \wedge E_0$$

$$\frac{P \wedge Q}{Q} \wedge E_1$$

Kommutativität der Konjunktion

Satz

Die logische Konjunktion ist kommutativ, d.h. die Aussage

$$A \wedge B \implies B \wedge A$$

ist allgemeingültig.

Beweis.

$$\frac{\boxed{\begin{array}{c} A \wedge B \\ \frac{\frac{A \wedge B}{B} \wedge \mathcal{E}_1 \quad \frac{A \wedge B}{A} \wedge \mathcal{E}_0}{B \wedge A} \wedge \mathcal{I} \end{array}}}{A \wedge B \implies B \wedge A} \implies \mathcal{I}$$



Definition der Äquivalenz, \iff

Notation

Die logische **Äquivalenz** wird mit $P \iff Q$ bezeichnet und ist lediglich eine Abkürzung für $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$.

Bemerkung

Zwei Aussagen sind äquivalent wenn sie vom logischen Standpunkt aus betrachtet gleichwertig sind.

Definition der Disjunktion, \vee

Formation

Sind P und Q Aussagen, dann bezeichnet $P \vee Q$ ebenfalls eine Aussage, die **Disjunktion** von P und Q .

Introduktion

Um $P \vee Q$ zu beweisen, genügt es, P zu beweisen, oder Q zu beweisen.

Elimination

Folgt irgendeine Aussage R sowohl aus P als auch aus Q , dann folgt sie auch aus $P \vee Q$ (Beweis durch Fallunterscheidung).

Schlußregeln

$$\frac{P}{P \vee Q} \vee I_0$$

$$\frac{Q}{P \vee Q} \vee I_1$$

$$\frac{P \Rightarrow R \quad Q \Rightarrow R}{P \vee Q \Rightarrow R} \vee E$$

Implikation, \Rightarrow

- ▶ Schlußregeln:

$$\frac{\begin{array}{c} x: P \\ \vdots \\ t[x]: Q \end{array}}{x \mapsto t[x]: P \Rightarrow Q} \Rightarrow \mathcal{I}$$

$$\frac{f: P \Rightarrow Q \quad x: P}{fx: Q} \Rightarrow \mathcal{E}$$

- ▶ Der Beweis einer Implikation ist ein **Algorithmus**,
- ▶ der für jeden Input vom Typ P einen Output vom Typ Q liefert.
- ▶ **Funktionsdatentyp**: Schreibweise: $P \rightarrow Q$ oder Q^P .
- ▶ **Konstruktor**: Abstraktion: (\mapsto) ;
- ▶ **Selektor**: Funktionsanwendung: `apply`.

Logische Konjunktion, \wedge

- ▶ Einführung und Elimination

$$\frac{x: P \quad y: Q}{(x, y): P \wedge Q} \wedge \mathcal{I}$$

$$\frac{z: P \wedge Q}{\text{fst } z: P} \wedge \mathcal{E}_0$$

$$\frac{z: P \wedge Q}{\text{snd } z: Q} \wedge \mathcal{E}_1$$

- ▶ Ein Beweis der Konjunktion $P \wedge Q$ ist ein **Paar**,
- ▶ dessen Komponenten die Typen P bzw. Q haben.
- ▶ **Verbunddatentyp (Direktes Produkt)**: $P \times Q$.
- ▶ **Konstruktor**: $(,): P \rightarrow Q \rightarrow P \times Q$;
- ▶ **Selektoren**: $\text{fst}: P \times Q \rightarrow P$, $\text{snd}: P \times Q \rightarrow Q$.

Kommutativität der Konjunktion

Satz

$$A \wedge B \implies B \wedge A.$$

- Beweis:

$$\frac{\frac{\frac{c: A \wedge B}{\text{snd } c: B} \wedge \mathcal{E}_1 \quad \frac{c: A \wedge B}{\text{fst } c: A} \wedge \mathcal{E}_0}{(\text{snd } c, \text{fst } c): B \wedge A} \wedge \mathcal{I}}{c \mapsto (\text{snd } c, \text{fst } c): A \wedge B \implies B \wedge A} \implies \mathcal{I}$$

- commute: $A \times B \rightarrow B \times A$, $c \mapsto (\text{snd } c, \text{fst } c)$,
- Intuitiver: $(a, b) \mapsto (b, a)$.
- Äquivalenz:
 $(c \mapsto (\text{snd } c, \text{fst } c), c \mapsto (\text{snd } c, \text{fst } c)): A \wedge B \iff B \wedge A.$

Logische Disjunktion, \vee

- ▶ **Introduktion und Elimination**

$$\frac{x: P}{\text{Left } x: P \vee Q} \vee I_0$$

$$\frac{y: Q}{\text{Right } y: P \vee Q} \vee I_1$$

$$\frac{f: P \Rightarrow R \quad g: Q \Rightarrow R}{\text{either } f g: P \vee Q \Rightarrow R} \vee E$$

- ▶ Ein Beweis der Disjunktion $P \vee Q$ ist einer von P oder von Q , *und als solcher gekennzeichnet.*
- ▶ **Disjunkte Vereinigung (Direkte Summe):** $P + Q$.
- ▶ **Konstruktoren:** Left: $P \rightarrow P + Q$, Right: $Q \rightarrow P + Q$;
- ▶ **Selektor:** either: $(P \rightarrow R) \rightarrow (Q \rightarrow R) \rightarrow (P + Q \rightarrow R)$.

Beispiel: $A \vee (B \wedge C) \Rightarrow A \vee B$

$$\frac{
 \frac{
 \frac{
 a: A
 }{
 \text{Left } a: A \vee B
 }{\vee \mathcal{I}_0}
 }{
 a \mapsto \text{Left } a: A \Rightarrow A \vee B
 }{\Rightarrow \mathcal{I}}
 \quad
 \frac{
 \frac{
 \frac{
 y: B \wedge C
 }{
 \text{fst } y: B
 }{\wedge \mathcal{E}_1}
 }{
 \text{Right}(\text{fst } y): A \vee B
 }{\vee \mathcal{I}_1}
 }{
 y \mapsto \text{Right}(\text{fst } y): B \wedge C \Rightarrow A \vee B
 }{\Rightarrow \mathcal{I}}
 }{
 \text{either}(a \mapsto \text{Left } a) (y \mapsto \text{Right}(\text{fst } y)): A \vee (B \wedge C) \Rightarrow A \vee B
 }{\vee \mathcal{E}}$$

Mit

$$f: A \vee (B \wedge C) \Rightarrow A \vee B$$

$$g: A \vee (B \wedge C) \Rightarrow A \vee C$$

erhalten wir auch:

$$(f, g): A \vee (B \wedge C) \Rightarrow (A \vee B) \wedge (A \vee C)$$

Es gibt auch: $h: (A \vee B) \wedge (A \vee C) \Rightarrow A \vee (B \wedge C)$

Curry-Howard-Isomorphismus

- ▶ Eine Aussage legt den Datentyp ihrer Beweise fest.
- ▶ Ein Datentyp entspricht der Aussage, daß es ein Objekt dieses Typs gibt.
- ▶ Jeder Algorithmus, der ein Objekt eines bestimmten Datentyps konstruiert, ist ein Beweis, daß es ein solches gibt.
- ▶ Aussagen entsprechen Programmspezifikationen.
- ▶ Beweise entsprechen Programmen.
- ▶ Man kann Aussagen beweisen, indem man ein Objekt vom passenden Typ konstruiert.
- ▶ Aus mathematischen Beweisen lassen sich verifizierte Programme extrahieren.
- ▶ *Fehlerfreie Software beliebiger Komplexität ist möglich.*