

Logik

Aussagenlogik

Logische Implikation,  $\Rightarrow$   
Logische Konjunktion,  $\wedge$   
Logische Äquivalenz,  
 $\Leftrightarrow$   
Logische Disjunktion,  $\vee$

Prädikatenlogik

Allquantor,  $\forall$   
Existenzquantor,  $\exists$

Datentypen

Logische Implikation,  $\Rightarrow$   
Logische Konjunktion,  $\wedge$   
Logische Disjunktion,  $\vee$   
Curry-Howard-  
Isomorphismus

# Mathematik und Logik

2007W

Institut für Algebra  
Johannes Kepler Universität Linz

Vorlesung im 2007W

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

Logik

Aussagenlogik

Logische Implikation,  $\Rightarrow$   
Logische Konjunktion,  $\wedge$   
Logische Äquivalenz,  
 $\Leftrightarrow$   
Logische Disjunktion,  $\vee$

Prädikatenlogik

Allquantor,  $\forall$   
Existenzquantor,  $\exists$

Datentypen

Logische Implikation,  $\Rightarrow$   
Logische Konjunktion,  $\wedge$   
Logische Disjunktion,  $\vee$   
Curry-Howard-  
Isomorphismus

## Inhalt

### Logik

#### Aussagenlogik

Logische Implikation,  $\Rightarrow$   
Logische Konjunktion,  $\wedge$   
Logische Äquivalenz,  $\Leftrightarrow$   
Logische Disjunktion,  $\vee$

#### Prädikatenlogik

Allquantor,  $\forall$   
Existenzquantor,  $\exists$

#### Datentypen

Logische Implikation,  $\Rightarrow$   
Logische Konjunktion,  $\wedge$   
Logische Disjunktion,  $\vee$   
Curry-Howard-Isomorphismus

# Aussagen

Logik

Aussagenlogik

- Logische Implikation,  $\Rightarrow$
- Logische Konjunktion,  $\wedge$
- Logische Äquivalenz,  $\Leftrightarrow$
- Logische Disjunktion,  $\vee$

Prädikatenlogik

- Allquantor,  $\forall$
- Existenzquantor,  $\exists$

Datentypen

- Logische Implikation,  $\Rightarrow$
- Logische Konjunktion,  $\wedge$
- Logische Disjunktion,  $\vee$
- Curry-Howard-Isomorphismus

Die **mathematische Logik** verwendet mathematische Methoden, um das logische Denken formal zu beschreiben.

- ▶ Populäre Definition: Eine Aussage ist ein Satz, der entweder falsch oder wahr ist.
- ▶ Problem: Wie definiert man *wahr* und *falsch*?
- ▶ Ein **Beweis** stellt sicher, daß eine Aussage wahr ist.
- ▶ DEFINITION: Eine **Aussage** ist eine Konstruktion, durch welche festgelegt wird, wie ihre Beweise zu konstruieren sind.
- ▶ Eine Aussage, die wir nicht beweisen können, muß nicht unbedingt falsch sein.

# Definition der Implikation, $\Rightarrow$

Logik

Aussagenlogik

- Logische Implikation,  $\Rightarrow$
- Logische Konjunktion,  $\wedge$
- Logische Äquivalenz,  $\Leftrightarrow$
- Logische Disjunktion,  $\vee$

Prädikatenlogik

- Allquantor,  $\forall$
- Existenzquantor,  $\exists$

Datentypen

- Logische Implikation,  $\Rightarrow$
- Logische Konjunktion,  $\wedge$
- Logische Disjunktion,  $\vee$
- Curry-Howard-Isomorphismus

## 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

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

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

## 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

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

$$\frac{P \wedge Q}{P} \wedge \mathcal{E}_0$$

$$\frac{P \wedge Q}{Q} \wedge \mathcal{E}_1$$

## Kommutativität der Konjunktion

### SATZ

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

$$A \wedge B \Rightarrow B \wedge A$$

ist allgemeingültig.

### BEWEIS.

$$\frac{\frac{A \wedge B}{B} \wedge \mathcal{E}_1 \quad \frac{A \wedge B}{A} \wedge \mathcal{E}_0}{B \wedge A} \wedge \mathcal{I} \Rightarrow \mathcal{I}$$

$$A \wedge B \Rightarrow B \wedge A$$



## Logik

## Aussagenlogik

Logische Implikation,  $\Rightarrow$ Logische Konjunktion,  $\wedge$ Logische Äquivalenz,  
 $\Leftrightarrow$ Logische Disjunktion,  $\vee$ 

## Prädikatenlogik

Allquantor,  $\forall$ Existenzquantor,  $\exists$ 

## Datentypen

Logische Implikation,  $\Rightarrow$ Logische Konjunktion,  $\wedge$ Logische Disjunktion,  $\vee$ Curry-Howard-  
IsomorphismusDefinition der Äquivalenz,  $\Leftrightarrow$ 

## NOTATION

Die logische **Äquivalenz** wird mit  $P \Leftrightarrow Q$  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.

## Logik

## Aussagenlogik

Logische Implikation,  $\Rightarrow$ Logische Konjunktion,  $\wedge$ Logische Äquivalenz,  
 $\Leftrightarrow$ Logische Disjunktion,  $\vee$ 

## Prädikatenlogik

Allquantor,  $\forall$ Existenzquantor,  $\exists$ 

## Datentypen

Logische Implikation,  $\Rightarrow$ Logische Konjunktion,  $\wedge$ Logische Disjunktion,  $\vee$ Curry-Howard-  
IsomorphismusDefinition 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

$$\frac{P}{P \vee Q} \vee \mathcal{I}_0$$

$$\frac{Q}{P \vee Q} \vee \mathcal{I}_1$$

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

Logik

Aussagenlogik

Logische Implikation,  $\Rightarrow$

Logische Konjunktion,  $\wedge$

Logische Äquivalenz,  
 $\Leftrightarrow$

Logische Disjunktion,  $\vee$

Prädikatenlogik

Allquantor,  $\forall$

Existenzquantor,  $\exists$

Datentypen

Logische Implikation,  $\Rightarrow$

Logische Konjunktion,  $\wedge$

Logische Disjunktion,  $\vee$

Curry-Howard-  
Isomorphismus

# Allquantor, $\forall$

- ▶ Sei  $X$  ein Datentyp, und  $P[x]$  für jedes  $x \in X$  eine Aussage. Dann bezeichnet  $\forall_{x \in X} P[x]$  eine **All-Aussage**.
- ▶ Die All-Aussage drückt eine universelle Quantifizierung aus.
- ▶ Ein Beweis von  $\forall_{x \in X} P[x]$  konstruiert für jedes beliebige  $x \in X$  einen Beweis von  $P[x]$ .
- ▶ Praktisch: Es sei  $\forall_{x \in X} P[x]$  zu beweisen. Vorgangsweise: Annahme  $x \in X$ ; beweise  $P[x]$ .
- ▶ Hängt  $P[x]$  nicht von  $x$  ab, dann liegt eine normale Implikation vor:  $\forall_{x \in X} P$  ist dasselbe wie  $X \rightarrow P$ .

Logik

Aussagenlogik

Logische Implikation,  $\Rightarrow$

Logische Konjunktion,  $\wedge$

Logische Äquivalenz,  
 $\Leftrightarrow$

Logische Disjunktion,  $\vee$

Prädikatenlogik

Allquantor,  $\forall$

Existenzquantor,  $\exists$

Datentypen

Logische Implikation,  $\Rightarrow$

Logische Konjunktion,  $\wedge$

Logische Disjunktion,  $\vee$

Curry-Howard-  
Isomorphismus

# Allquantor, Einführung und Elimination

- ▶ Um  $\forall_{x \in X} P[x]$  zu beweisen, muß man  $P[x]$  für ein beliebiges  $x \in X$  beweisen.
- ▶  $\forall$ -Einführung:

$$\frac{\begin{array}{c} x \in X \\ \boxed{\vdots} \\ P[x] \end{array}}{\forall_{x \in X} P[x]} \forall\mathcal{I}$$

- ▶ Wurde  $\forall_{x \in X} P[x]$  bewiesen, und ist  $a \in X$ , dann hat man einen Beweis von  $P[a]$ .
- ▶  $\forall$ -Elimination:

$$\frac{\forall_{x \in X} P[x] \quad a \in X}{P[a]} \forall\mathcal{E}$$

Logik

Aussagenlogik

- Logische Implikation,  $\Rightarrow$
- Logische Konjunktion,  $\wedge$
- Logische Äquivalenz,  $\Leftrightarrow$
- Logische Disjunktion,  $\vee$

Prädikatenlogik

- Allquantor,  $\forall$
- Existenzquantor,  $\exists$

Datentypen

- Logische Implikation,  $\Rightarrow$
- Logische Konjunktion,  $\wedge$
- Logische Disjunktion,  $\vee$
- Curry-Howard-Isomorphismus

# Allquantor, Beispiel

$$\begin{array}{c}
 \forall x \in X A[x] \vee \forall y \in Y B[y] \\
 \boxed{\begin{array}{c} x \in X \\ \boxed{\begin{array}{c} y \in Y \\ \boxed{\begin{array}{c} \vdots \\ A[x] \vee B[y] \end{array}} \\ \forall y \in Y (A[x] \vee B[y]) \quad \forall I \end{array}} \\ \forall x \in X \forall y \in Y (A[x] \vee B[y]) \quad \forall I \end{array}} \\
 \hline
 \forall x \in X A[x] \vee \forall y \in Y B[y] \Rightarrow \forall x \in X \forall y \in Y (A[x] \vee B[y]) \quad \Rightarrow I
 \end{array}$$

Logik

Aussagenlogik

- Logische Implikation,  $\Rightarrow$
- Logische Konjunktion,  $\wedge$
- Logische Äquivalenz,  $\Leftrightarrow$
- Logische Disjunktion,  $\vee$

Prädikatenlogik

- Allquantor,  $\forall$
- Existenzquantor,  $\exists$

Datentypen

- Logische Implikation,  $\Rightarrow$
- Logische Konjunktion,  $\wedge$
- Logische Disjunktion,  $\vee$
- Curry-Howard-Isomorphismus

# Allquantor: Beispiel (Fortsetzung)

Annahmen:  $\forall x \in X A[x] \vee \forall y \in Y B[y]$ ,  $x \in X$ ,  $y \in Y$   
 Zu beweisen:

$$\begin{array}{c}
 \forall x \in X A[x] \qquad \forall y \in Y B[y] \\
 \boxed{\begin{array}{c} \vdots \\ A[x] \vee B[y] \end{array}} \qquad \boxed{\begin{array}{c} \vdots \\ A[x] \vee B[y] \end{array}} \\
 \hline
 \forall x \in X A[x] \vee \forall y \in Y B[y] \Rightarrow A[x] \vee B[y] \quad \forall E
 \end{array}$$

Die beiden Fälle:

$$\begin{array}{c}
 \forall x \in X A[x] \quad x \in X \quad \forall E \\
 \hline
 A[x] \\
 \hline
 A[x] \vee B[y] \quad \forall I_0
 \end{array}$$

$$\begin{array}{c}
 \forall y \in Y B[y] \quad y \in Y \quad \forall E \\
 \hline
 B[y] \\
 \hline
 A[x] \vee B[y] \quad \forall I_1
 \end{array}$$

Logik

Aussagenlogik

Logische Implikation,  $\Rightarrow$

Logische Konjunktion,  $\wedge$

Logische Äquivalenz,  
 $\Leftrightarrow$

Logische Disjunktion,  $\vee$

Prädikatenlogik

Allquantor,  $\forall$

Existenzquantor,  $\exists$

Datentypen

Logische Implikation,  $\Rightarrow$

Logische Konjunktion,  $\wedge$

Logische Disjunktion,  $\vee$

Curry-Howard-  
Isomorphismus

# Existenzquantor, $\exists$

- ▶ Sei  $X$  ein Datentyp, und  $P[x]$  für jedes  $x \in X$  eine Aussage. Dann bezeichnet  $\exists_{x \in X} P[x]$  eine **Existenz-Aussage**.
- ▶ Die Existenzaussage drückt eine existenzielle Quantifizierung aus.
- ▶ Ein Beweis von  $\exists_{x \in X} P[x]$  konstruiert ein  $a \in X$  und einen Beweis von  $P[a]$ .
- ▶ Praktisch: Es sei  $\exists_{x \in X} P[x]$  zu beweisen. Vorgangsweise: Man wählt ein passendes  $a \in X$ , und versucht damit  $P[a]$  zu beweisen.
- ▶ Hängt  $P[x]$  nicht von  $x$  ab, dann liegt eine normale Konjunktion vor:  $\exists_{x \in X} P$  ist dasselbe wie  $X \wedge P$ .

Logik

Aussagenlogik

Logische Implikation,  $\Rightarrow$

Logische Konjunktion,  $\wedge$

Logische Äquivalenz,  
 $\Leftrightarrow$

Logische Disjunktion,  $\vee$

Prädikatenlogik

Allquantor,  $\forall$

Existenzquantor,  $\exists$

Datentypen

Logische Implikation,  $\Rightarrow$

Logische Konjunktion,  $\wedge$

Logische Disjunktion,  $\vee$

Curry-Howard-  
Isomorphismus

# Existenzquantor: Einführung und Elimination

- ▶ Um  $\exists_{x \in X} P[x]$  zu beweisen, muß man ein  $a \in X$  finden und damit  $P[a]$  beweisen.
- ▶  $\exists$ -Einführung: 
$$\frac{a \in X \quad P[a]}{\exists_{x \in X} P[x]} \exists\mathcal{I}$$
- ▶ Wurde  $\exists_{x \in X} P[x]$  bewiesen, so kann man für's weitere annehmen, daß es ein soches Objekt gibt.
- ▶  $\exists$ -Elimination:

$$\frac{\exists_{x \in X} P[x] \quad \begin{array}{|c|} \hline y \in X \quad P[y] \\ \hline \vdots \\ \hline Q \\ \hline \end{array}}{Q} \exists\mathcal{E}$$

Logik

Aussagenlogik

Logische Implikation,  $\Rightarrow$

Logische Konjunktion,  $\wedge$

Logische Äquivalenz,

$\iff$

Logische Disjunktion,  $\vee$

Prädikatenlogik

Allquantor,  $\forall$

Existenzquantor,  $\exists$

Datentypen

Logische Implikation,  $\Rightarrow$

Logische Konjunktion,  $\wedge$

Logische Disjunktion,  $\vee$

Curry-Howard-  
Isomorphismus

# Implikation, $\Rightarrow$

- ▶ Schlußregeln:

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

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

- ▶ 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:  $\text{apply}$ .

Logik

Aussagenlogik

Logische Implikation,  $\Rightarrow$

Logische Konjunktion,  $\wedge$

Logische Äquivalenz,

$\iff$

Logische Disjunktion,  $\vee$

Prädikatenlogik

Allquantor,  $\forall$

Existenzquantor,  $\exists$

Datentypen

Logische Implikation,  $\Rightarrow$

Logische Konjunktion,  $\wedge$

Logische Disjunktion,  $\vee$

Curry-Howard-  
Isomorphismus

# Logische Konjunktion, $\wedge$

- ▶ Introduction und Elimination

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

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

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

- ▶ 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**:  $(, ) \in P \rightarrow Q \rightarrow P \times Q$ ;
- ▶ **Selektoren**:  $\text{fst} \in P \times Q \rightarrow P$ ,  $\text{snd} \in P \times Q \rightarrow Q$ .

Logik

Aussagenlogik

Logische Implikation,  $\Rightarrow$

Logische Konjunktion,  $\wedge$

Logische Äquivalenz,  $\Leftrightarrow$

Logische Disjunktion,  $\vee$

Prädikatenlogik

Allquantor,  $\forall$

Existenzquantor,  $\exists$

Datentypen

Logische Implikation,  $\Rightarrow$

Logische Konjunktion,  $\wedge$

Logische Disjunktion,  $\vee$

Curry-Howard-  
Isomorphismus

# Kommutativität der Konjunktion

## SATZ

$$A \wedge B \Rightarrow B \wedge A.$$

► Beweis:

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

$$c \mapsto (\text{snd } c, \text{fst } c) \in A \wedge B \Rightarrow B \wedge A$$

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

Logik

Aussagenlogik

Logische Implikation,  $\Rightarrow$

Logische Konjunktion,  $\wedge$

Logische Äquivalenz,  $\Leftrightarrow$

Logische Disjunktion,  $\vee$

Prädikatenlogik

Allquantor,  $\forall$

Existenzquantor,  $\exists$

Datentypen

Logische Implikation,  $\Rightarrow$

Logische Konjunktion,  $\wedge$

Logische Disjunktion,  $\vee$

Curry-Howard-  
Isomorphismus

# Logische Disjunktion, $\vee$

► Einführung und Elimination

$$\frac{x \in P}{\text{Left } x \in P \vee Q} \vee \mathcal{I}_0 \quad \frac{y \in Q}{\text{Right } y \in P \vee Q} \vee \mathcal{I}_1$$

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

- 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:**  $\text{Left} \in P \rightarrow P + Q, \text{Right} \in Q \rightarrow P + Q;$
- **Selektor:**  $\text{either} \in (P \rightarrow R) \rightarrow (Q \rightarrow R) \rightarrow (P + Q \rightarrow R).$

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

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

$$\text{either } (a \mapsto \text{Left } a) (y \mapsto \text{Right } (\text{fst } y)) \in A \vee (B \wedge C) \Rightarrow A \vee B$$

Mit

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

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

erhalten wir auch:

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

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

## 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.*