



## Einführung in die Theoretische Informatik

David Drexel      Alexander Maringele  
Julian Fodor      David Obwaller  
Alexander Lochmann      Jonas Schöpf  
Georg Moser      **Manuel Schneckenreither**

cbr.uibk.ac.at

## Zusammenfassung

## Zusammenfassung der letzten LVA

### Beispiel

Wenn das Kind schreit, hat es Hunger  
Das Kind schreit  
Also, hat das Kind Hunger

### Fakt

*Korrektheit dieser Schlussfigur ist unabhängig von den konkreten Aussagen*

### Definition (*Modus Ponens*)

Wenn  $A$ , dann  $B$   
 $A$  gilt  
Also, gilt  $B$

## Inhalte der Lehrveranstaltung

### Einführung in die Logik

Syntax & Semantik der Aussagenlogik, Formales Beweisen, Konjunktive und Disjunktive Normalformen

### Einführung in die Algebra

Boolesche Algebra, Universelle Algebra, Logische Schaltkreise

### Einführung in die Theorie der Formalen Sprachen

Grammatiken und Formale Sprachen, Reguläre Sprachen, Kontextfreie Sprachen

### Einführung in die Berechenbarkeitstheorie

Algorithmisch unlösbare Probleme, Turing Maschinen, Registermaschinen

### Einführung in die Programmverifikation

Prinzipien der Analyse von Programmen, Verifikation nach Hoare

# Syntax der Aussagenlogik

## Definition

Sei **AT** eine Menge von **atomaren Formeln** (oder **Atomen**), deren Elemente mit  $p, q, r, \dots$  bezeichnet werden

## Definition

**Wahrheitswertsymbole:**

True    False

**Junktoren:**

$\neg$     $\wedge$     $\vee$     $\rightarrow$

# Aussagenlogische Formeln

## Definition

Die **Formeln** der Aussagenlogik sind induktiv definiert:

- 1 Eine atomare Formel  $p$  ist eine **Formel**,
- 2 ein Wahrheitswertsymbol (True, False) ist eine **Formel**, und
- 3 wenn  $A$  und  $B$  **Formeln** sind, dann sind auch die folgenden **Formeln**:

$\neg A$      $(A \wedge B)$      $(A \vee B)$      $(A \rightarrow B)$

## Beispiel

Der folgende Ausdruck  $A$  ist eine Formel

$((p \rightarrow \neg q) \rightarrow (\neg q \rightarrow \neg p))$

# Präzedenzen

## Konvention

Wir verwenden die folgende Präzedenz:

$\neg > \vee, \wedge > \rightarrow$      $\rightarrow$  ist rechts-assoziativ:  $p \rightarrow (q \rightarrow r)$

## Beispiel

$\neg p \wedge q \rightarrow r \vee s$  statt  $((\neg p \wedge q) \rightarrow (r \vee s))$

# Wahrheitswertbelegung

## Definition

- 1 **T** und **F** bezeichnen die beiden betrachteten **Wahrheitswerte**
- 2 **Belegung**  $v$ :  $AT \rightarrow \{T, F\}$  assoziiert Atome mit Wahrheitswerten

## Beispiel

Betrachte die Atome  $p, q$  und  $r$ , sowie die folgende Belegung:

$$v(a) := \begin{cases} T & a = p \\ F & a = q \\ F & a = r \end{cases}$$

Wir schreiben auch  $v(p) = T, v(q) = F, v(r) = F$

## Definition

- 1 **Atome** sind Platzhalter für konkrete Aussagen
- 2 **Junktoren** sind formale Zeichen, die Aussagen verbinden

$\neg$                        $\wedge$                        $\vee$                        $\rightarrow$   
 Negation      Konjunktion      Disjunktion      Implikation

- 3 Die Bedeutung wird durch **Wahrheitstafeln** definiert

$\neg$	
T	F
F	T

$\wedge$	T	F
T	T	F
F	F	F

$\vee$	T	F
T	T	T
F	T	F

$\rightarrow$	T	F
T	T	F
F	T	T

## Beispiel

Der allgemeine Aussage „Wenn  $p$ , dann  $q$ “ kann nun konzise ausgedrückt werden:

$$p \rightarrow q$$

## Semantik der Aussagenlogik

### Definition

Erweiterung der Belegung  $v$  zu einem **Wahrheitswert** für Formeln:

$$\bar{v}(p) = v(p) \quad \bar{v}(\text{True}) = T \quad \bar{v}(\text{False}) = F$$

$$\bar{v}(\neg A) = \begin{cases} T & \bar{v}(A) = F \\ F & \bar{v}(A) = T \end{cases}$$

$$\bar{v}(A \wedge B) = \begin{cases} T & \bar{v}(A) = \bar{v}(B) = T \\ F & \text{sonst} \end{cases}$$

$$\bar{v}(A \vee B) = \begin{cases} F & \bar{v}(A) = \bar{v}(B) = F \\ T & \text{sonst} \end{cases}$$

$$\bar{v}(A \rightarrow B) = \begin{cases} T & \bar{v}(A) = F \text{ oder } \bar{v}(B) = T \\ F & \text{sonst} \end{cases}$$

## Wahrheitstabelle

### Beispiel

Sei  $v(p) = T$ ,  $v(q) = F$ , dann  $\bar{v}(A) = \bar{v}((p \rightarrow \neg q) \rightarrow (\neg q \rightarrow \neg p)) = F$

### Definition

Sei  $A$  eine Formel; die **Wahrheitstabelle von  $A$**  listet alle relevanten Belegungen  $v$  zusammen mit dem Wahrheitswert  $\bar{v}(A)$  auf

### Beispiel

Betrachte die Formel:

$$(p \rightarrow \neg q) \rightarrow (\neg q \rightarrow \neg p)$$

Wir stellen die folgende Wahrheitstabelle auf:

$p$	$q$	$(p \rightarrow \neg q)$	$(\neg q \rightarrow \neg p)$	$(p \rightarrow \neg q) \rightarrow (\neg q \rightarrow \neg p)$
T	T	F	T	T
T	F	T	F	F
F	T	T	T	T
F	F	T	T	T

## Definition

sei  $A$  eine Formel

- 1 wenn Belegung  $v$  existiert, sodass  $\bar{v}(A) = T$ , heißt  $A$  **erfüllbar**
- 2 wenn **keine** solche Belegung existiert, heißt  $A$  **unerfüllbar**
- 3 wenn für **alle** Belegungen  $v$ ,  $\bar{v}(A) = T$ , heißt  $A$  **gültig** oder **Tautologie**

## Definition

Die **Konsequenzrelation**  $\{A_1, \dots, A_n\} \models B$  gilt, gdw. für alle Belegungen  $v$ :

$$\bar{v}(A_1) = T, \dots, \bar{v}(A_n) = T \text{ impliziert } \bar{v}(B) = T$$

- Wir schreiben  $\models A$  statt  $\emptyset \models A$ ; außerdem schreiben wir  $A_1, \dots, A_n \models B$  statt  $\{A_1, \dots, A_n\} \models B$
- Gilt  $\emptyset \models A$  dann ist  $A$  eine Tautologie

## Satz

Eine Formel  $A$  ist eine Tautologie gdw.  $\neg A$  unerfüllbar

## Beweis.

- 1 Wir zeigen die Richtung von links nach rechts:
  - angenommen  $\bar{v}(A) = T$ , für alle Belegungen  $v$
  - also  $\bar{v}(\neg A) = F$ , für alle Belegungen  $v$
  - somit ist  $\neg A$  unerfüllbar
- 2 Wir zeigen die Richtung von rechts nach links:
  - angenommen  $\neg A$  ist unerfüllbar
  - $\bar{v}(\neg A) = F$ , für alle Belegungen  $v$
  - also  $\bar{v}(A) = T$ , für alle Belegungen  $v$  und somit gültig

## Definition (Äquivalenz)

$A \equiv B$ , wenn  $A \models B$  und  $B \models A$  gilt

## Satz

$A \equiv B$  gilt gdw.  $(A \rightarrow B) \wedge (B \rightarrow A)$  eine Tautologie

## Beweis.

Wir zeigen die Richtung von links nach rechts:

- $(A \rightarrow B) \wedge (B \rightarrow A)$  gültig gdw.  $(A \rightarrow B)$  gültig und  $(B \rightarrow A)$  gültig
- Angenommen  $A \models B$ ; dann gilt für alle Belegungen  $v$ :

$$\bar{v}(A) = T \text{ impliziert } \bar{v}(B) = T$$

- $\bar{v}(A \rightarrow B) = T$  für alle  $v$
- $(A \rightarrow B)$  ist gültig
- ähnlich folgt aus  $B \models A$ , dass  $(B \rightarrow A)$  gültig

## Assoziativität und Kommutativität von Junktoren

- Konjunktion und Disjunktion sind assoziativ und kommutativ
- Wir unterscheiden nicht zwischen:

$$(A \wedge B) \wedge C \\ A \wedge B$$

$$A \wedge (B \wedge C) \\ B \wedge A$$

$$A \wedge B \wedge C$$

## Definition

- 1  $\bigwedge_{i=1}^n A_i = A_1 \wedge \dots \wedge A_n \quad n \geq 1$
- 2  $\bigwedge_{i=1}^0 A_i = \text{True}$
- 3  $\bigvee_{i=1}^n A_i = A_1 \vee \dots \vee A_n \quad n \geq 1$
- 4  $\bigvee_{i=1}^0 A_i = \text{False}$

## Äquivalenzen I

### Lemma (Elementare Äquivalenzen)

$$\begin{array}{llll} \neg\neg A \equiv A & A \vee \text{True} \equiv \text{True} & A \wedge \text{True} \equiv A & A \rightarrow \text{True} \equiv \text{True} \\ A \vee \text{False} \equiv A & A \wedge \text{False} \equiv \text{False} & A \rightarrow \text{False} \equiv \neg A & \\ A \vee A \equiv A & A \wedge A \equiv A & \text{True} \rightarrow A \equiv A & \\ A \vee \neg A \equiv \text{True} & A \wedge \neg A \equiv \text{False} & \text{False} \rightarrow A \equiv \text{True} & \\ & & A \rightarrow A \equiv \text{True} & \end{array}$$

### Lemma (Distributivgesetze und Andere)

$$\begin{array}{ll} A \rightarrow B \equiv \neg A \vee B & \neg(A \rightarrow B) \equiv A \wedge \neg B \\ A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C) & A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C) \end{array}$$

## Äquivalenzen II

### Lemma (Absorptionsgesetze)

$$\begin{array}{ll} A \wedge (A \vee B) \equiv A & A \vee (A \wedge B) \equiv A \\ A \wedge (\neg A \vee B) \equiv A \wedge B & A \vee (\neg A \wedge B) \equiv A \vee B \end{array}$$

### Lemma (Gesetze von de Morgan)

$$\neg(A \wedge B) \equiv \neg A \vee \neg B \quad \neg(A \vee B) \equiv \neg A \wedge \neg B$$

## Gleiches durch Gleiches Ersetzen

### Definition

Eine **Teilformel**  $A$  einer Formel  $B$  ist ein Teilausdruck von  $B$ , der wiederum eine Formel ist

### Satz

- 1  $A, B$  Formeln und  $E, F$  Teilformeln von  $A, B$
- 2 Gelte  $E \equiv F$
- 3  $B$  ist das Resultat der Ersetzung von  $E$  durch  $F$  in  $A$

Dann gilt  $A \equiv B$

### Beispiel

Wir betrachten die folgende Äquivalenz

$$p \rightarrow q \equiv \neg p \vee q$$

mit der folgenden Formel

$$(p \rightarrow q) \wedge r$$

Nun gilt

$$\underline{(p \rightarrow q)} \wedge r \equiv \underline{(\neg p \vee q)} \wedge r$$