

# Einführung in die Theoretische Informatik

## Woche 2

Harald Zankl

Institut für Informatik @ UIBK  
Wintersemester 2014/2015



Zusammenfassung

## Zusammenfassung der letzten LVA

### Beispiel

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

### Fakt

*Die 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:**

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

## Syntax der Aussagenlogik (2)

### 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

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

auch **Formeln**

### Beispiel

Der Ausdruck  $((p \rightarrow \neg q) \rightarrow (\neg q \rightarrow \neg p))$  ist eine Formel

### Konvention

Wir verwenden die folgende Präzedenz:

$$\neg > \vee, \wedge > \rightarrow \quad \rightarrow \text{ ist rechts-assoziativ: } A \rightarrow (B \rightarrow C)$$

## Semantik der Aussagenlogik

### 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  $v(p) = T$ ,  $v(q) = F$ ,  $v(r) = F$ .

## Semantik der Aussagenlogik (2)

### Definition

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



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

$\neg$	$\wedge$	$\vee$	$\rightarrow$																						
<table border="1" style="display: inline-table; border-collapse: collapse;"><tr><td>T</td><td>F</td></tr><tr><td>F</td><td>T</td></tr></table>	T	F	F	T	<table border="1" style="display: inline-table; border-collapse: collapse;"><tr><td>T</td><td>F</td></tr><tr><td>T</td><td>F</td></tr><tr><td>F</td><td>F</td></tr></table>	T	F	T	F	F	F	<table border="1" style="display: inline-table; border-collapse: collapse;"><tr><td>T</td><td>F</td></tr><tr><td>T</td><td>T</td></tr><tr><td>F</td><td>F</td></tr></table>	T	F	T	T	F	F	<table border="1" style="display: inline-table; border-collapse: collapse;"><tr><td>T</td><td>F</td></tr><tr><td>T</td><td>F</td></tr><tr><td>F</td><td>T</td></tr></table>	T	F	T	F	F	T
T	F																								
F	T																								
T	F																								
T	F																								
F	F																								
T	F																								
T	T																								
F	F																								
T	F																								
T	F																								
F	T																								

### Beispiel

Die allgemeine Aussage „Wenn  $p$ , dann  $q$ “ schreiben wir:

$$p \rightarrow q$$

## Semantik der Aussagenlogik (3)

### Definition

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

$$\begin{aligned} \bar{v}(p) &= v(p) & \bar{v}(\neg A) &= \begin{cases} T & \bar{v}(A) = F \\ F & \bar{v}(A) = T \end{cases} \\ \bar{v}(\text{True}) &= T & \bar{v}(A \wedge B) &= \begin{cases} T & \bar{v}(A) = \bar{v}(B) = T \\ F & \text{sonst} \end{cases} \\ \bar{v}(\text{False}) &= F & \bar{v}(A \vee B) &= \begin{cases} F & \bar{v}(A) = \bar{v}(B) = F \\ T & \text{sonst} \end{cases} \\ & & \bar{v}(A \rightarrow B) &= \begin{cases} T & \bar{v}(A) = F \text{ oder } \bar{v}(B) = T \\ F & \text{sonst} \end{cases} \end{aligned}$$

### Beispiel

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

## Wahrheitstabelle

### 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

## Eigenschaften

### Definition

Eine Formel  $A$  heißt

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

### Beispiel

- erfüllbar:  $p$ ,  $q$ ,  $p \wedge q$
- unerfüllbar:  $p \wedge \neg p$
- Tautologie:  $p \vee \neg p$ ,  $\neg(p \wedge \neg p)$

### Satz

*Wenn eine Formel  $A$  gültig ist, dann ist  $A$  auch erfüllbar.*

## 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



## Konsequenz und Äquivalenz

## Konsequenz und Äquivalenz von Formeln

## Definition (Konsequenz)

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

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

## Beispiel

$$p \not\models q \quad p, q \models q \quad p \wedge q \models q \quad p \not\models p \wedge q \quad p \rightarrow q \models \neg p \vee q \quad \models p \vee \neg p$$

## Definition (Äquivalenz)

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

## Beispiel

$$p \not\equiv q \quad p \wedge q \not\equiv q \quad p \not\equiv p \wedge q \quad p \rightarrow q \equiv \neg p \vee q$$

# Assoziativität und Kommutativität von Junktoren

## Fakt

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

$$\begin{array}{ccc} (A \wedge B) \wedge C & A \wedge (B \wedge C) & A \wedge B \wedge C \\ A \wedge B & B \wedge A & \end{array}$$

## Definition

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

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

## Äquivalenzen II

Lemma (Kommutativ- und Assoziativgesetze)

$$\begin{aligned} A \wedge B &\equiv B \wedge A & A \vee B &\equiv B \vee A \\ A \wedge (B \wedge C) &\equiv (A \wedge B) \wedge C & A \vee (B \vee C) &\equiv (A \vee B) \vee C \end{aligned}$$

Lemma (Absorptionsgesetze)

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

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 Seien  $A, B$  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

Seien  $A = (p \rightarrow q) \wedge r$  und  $B = (\neg p \vee q) \wedge r$ .

Da  $p \rightarrow q \equiv \neg p \vee q$  gilt  $(p \rightarrow q) \wedge r \equiv (\neg p \vee q) \wedge r$ .