

# Einführung in die Theoretische Informatik

Woche 3

Harald Zankl

Institut für Informatik @ UIBK  
Wintersemester 2014/2015



## Zusammenfassung

### Definition (Äquivalenz)

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

### Lemma (Distributivgesetze)

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

### Lemma (Gesetze von de Morgan)

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

### 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  $A \equiv B$

## Zusammenfassung der letzten LVA

### 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**

### Definition

Erweiterung der Belegung  $v$  zu einem **Wahrheitswert**  $\bar{v}$  für Formeln anhand der Wahrheitstafeln für die Junktoren

## Inhalte der Lehrveranstaltung

### 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

## Methode von Quine

## Lemma

Sei  $A$  eine Formel und  $p$  ein Atom in  $A$ .

1  $A$  ist eine Tautologie gdw.

$A\{p \mapsto \text{True}\}$  ist Tautologie und  $A\{p \mapsto \text{False}\}$  ist Tautologie

2  $A$  ist unerfüllbar gdw.

$A\{p \mapsto \text{True}\}$  unerfüllbar und  $A\{p \mapsto \text{False}\}$  unerfüllbar

## Beispiel

Wir betrachten die Formel  $F$

$$F := (p \wedge q \rightarrow r) \wedge (p \rightarrow q) \rightarrow (p \rightarrow r)$$

Laut der Methode von Quine ist  $F$  eine Tautologie.

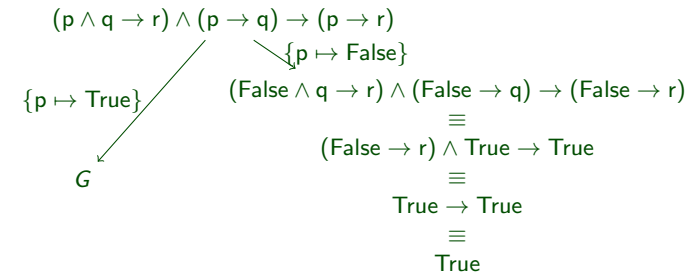
## Beispiel

Methode von Quine liefert die folgenden Anforderungen

1  $(\text{True} \wedge q \rightarrow r) \wedge (\text{True} \rightarrow q) \rightarrow (\text{True} \rightarrow r) =: G$  ist Tautologie

2  $(\text{False} \wedge q \rightarrow r) \wedge (\text{False} \rightarrow q) \rightarrow (\text{False} \rightarrow r)$  ist Tautologie

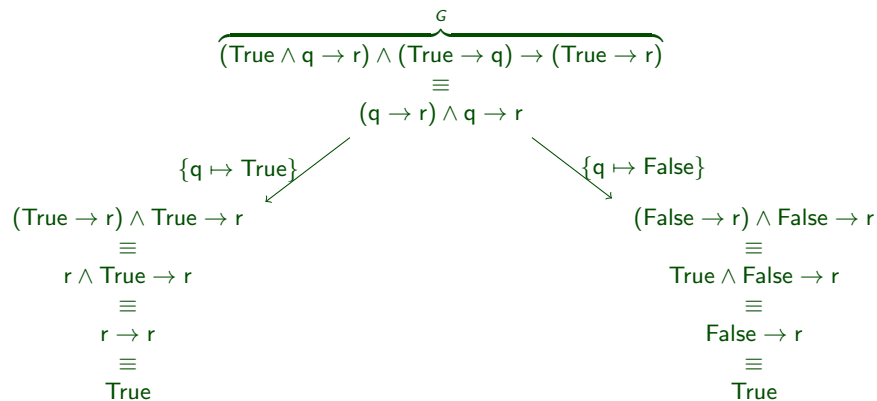
Anforderungen in Baumform:



Übrige Anforderungen

3  $G$  ist Tautologie

## Beispiel (Fortsetzung)



Es gibt keine weiteren Anforderungen mehr, also ist  $F$  eine Tautologie

## Formales Beweisen

## Modus Ponens

$$\frac{A \rightarrow B \quad A}{B} \text{MP}$$

## Definition

Axiome für die Aussagenlogik nach Frege und Łukasiewicz

- (1)  $A \rightarrow (B \rightarrow A)$
- (2)  $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$
- (3)  $(\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)$

Die Axiome sind Schemata, das heißt  $A$ ,  $B$  und  $C$  können für beliebige Formeln stehen

## Formaler Beweis (Ableitung, Herleitung, Deduktion)

### Definition

Sei  $\mathcal{G}$  eine endliche Menge von Formeln (Prämissen),  $B$  eine Formel

- Ein **Beweis** von  $B$  aus  $\mathcal{G}$  ist eine Sequenz

$$B_1, \dots, B_\ell \text{ mit } B_\ell = B$$

sodass für alle  $1 \leq i \leq \ell$  eine der folgenden Alternativen gilt:

- $B_i \in \mathcal{G}$
- $B_i$  ist eine Instanz eines der Axiome
- $B_i$  folgt mit MP aus  $B_{i_1}$  und  $B_{i_2}$ ,  $i_1, i_2 < i$

- $B$  heißt **beweisbar** aus den Prämissen  $\mathcal{G}$ , wenn es einen Beweis von  $B$  aus  $\mathcal{G}$  gibt

### Definition

- Die **Beweisbarkeitsrelation**  $A_1, \dots, A_n \vdash B$  gilt, gdw.  $B$  aus  $\{A_1, \dots, A_n\}$  beweisbar ist.
- Wenn  $\vdash B$ , dann nennen wir  $B$  **beweisbar**.

## Korrektheit und Vollständigkeit

### Satz

Die Axiome (1), (2), (3) mit Inferenzregel MP sind **korrekt** und **vollständig** für die Aussagenlogik:

$$A_1, \dots, A_n \models B \text{ gdw. } A_1, \dots, A_n \vdash B.$$

### Satz (Deduktionstheorem)

Sei  $B$  mit Hilfe der Prämisse  $A$  beweisbar, dann existiert ein Beweis von  $A \rightarrow B$ , der  $A$  nicht als Prämisse hat.

### Beispiel

Wir suchen einen Beweis für  $\neg p \vdash p \rightarrow q$ :

- $A \rightarrow (B \rightarrow A)$
  - $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$
  - $(\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)$
- $$(MP) \frac{A \rightarrow B \quad A}{B}$$

1	$\neg p$	Prämisse
2	$\neg p \rightarrow (\neg q \rightarrow \neg p)$	Axiom (1)
3	$\neg q \rightarrow \neg p$	1, 2, MP
4	$(\neg q \rightarrow \neg p) \rightarrow (p \rightarrow q)$	Axiom (3)
5	$p \rightarrow q$	3, 4, MP

### Beispiel

Wir betrachten die Tautologie  $\neg p \rightarrow (p \rightarrow q)$ :

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

Nun zeigen wir die Gültigkeit mit folgenden Beweis:

1	$\neg p$	Prämisse
2	$\neg p \rightarrow (\neg q \rightarrow \neg p)$	Axiom (1)
3	$\neg q \rightarrow \neg p$	1, 2, MP
4	$(\neg q \rightarrow \neg p) \rightarrow (p \rightarrow q)$	Axiom (3)
5	$p \rightarrow q$	3, 4, MP
6	$\neg p \rightarrow (p \rightarrow q)$	1, 5, Deduktionstheorem

## Beweis des Deduktionstheorems.

Angenommen  $B$  wird mit dem Beweis

$$B_1, \dots, B_\ell = B$$

nachgewiesen; oBdA. gilt  $B_1 = A$ ; wir zeigen die folgende Aussage mit Induktion nach  $k$  ( $1 \leq k \leq \ell$ ):

$A \rightarrow B_k$  ist ohne die Prämisse  $A$  beweisbar

**1** BASIS:  $k = 1$ ; dann gilt  $B_1 = B_k = A$  und die Behauptung, da  $A \rightarrow A$  beweisbar

**2** SCHRITT:  $k > 1$ ; die Induktionshypothese besagt

Für alle  $l < k$  ist  $A \rightarrow B_l$  ohne die Prämisse  $A$  beweisbar

Fallunterscheidung:

- sei  $B_k = A$  (wir argumentieren wie im Basisfall)
- sei  $B_k$  ein Axiom oder eine Prämisse  $\neq A$
- $B_k$  folgt mit MP aus  $B_i, B_j = (B_i \rightarrow B_k)$

## Beweis des Deduktionstheorems.

- Fall  $B_k$  ein Axiom oder eine Prämisse  $\neq A$

Wir verwenden folgenden Beweis:

1	$B_k$	Axiom oder Prämisse $\neq A$
2	$B_k \rightarrow (A \rightarrow B_k)$	Axiom (1)
3	$A \rightarrow B_k$	1, 2, MP

- Fall  $B_k$  folgt mit MP aus  $B_i, B_j = (B_i \rightarrow B_k)$

Wir verwenden folgenden Beweis:

1	Beweis von $A \rightarrow B_i$	IH
2	Beweis von $A \rightarrow (B_i \rightarrow B_k)$	IH
3	$(A \rightarrow (B_i \rightarrow B_k)) \rightarrow (A \rightarrow B_i) \rightarrow (A \rightarrow B_k)$	Axiom (2)
4	$(A \rightarrow B_i) \rightarrow (A \rightarrow B_k)$	2, 3, MP
5	$A \rightarrow B_k$	1, 4, MP



## Konjunktive und Disjunktive Normalform

## Definition

Eine **Wahrheitsfunktion**  $f: \{T, F\}^n \rightarrow \{T, F\}$  ist eine Funktion, die  $n$  Wahrheitswerten einen Wahrheitswert zuordnet

## Definition

Sei  $f: \{T, F\}^n \rightarrow \{T, F\}$  eine Wahrheitsfunktion; wir definieren:

$$\text{TV}(f) := \{(s_1, \dots, s_n) \mid f(s_1, \dots, s_n) = T\}$$

## Definition

- 1** Ein **Literal** ist ein Atom  $p$  oder die Negation eines Atoms  $\neg p$
- 2** Eine Formel  $A$  ist in **disjunktiver Normalform (DNF)**, wenn  $A$  eine Disjunktion von Konjunktionen von Literalen ist
- 3** Eine Formel  $A$  ist in **konjunktiver Normalform (KNF)**, wenn  $A$  eine Konjunktion von Disjunktionen von Literalen ist

## Lemma

- Sei  $f: \{T, F\}^n \rightarrow \{T, F\}$  eine Wahrheitsfunktion mit  $\text{TV}(f) \neq \emptyset, \text{TV}(f) \neq \{T, F\}^n$
- Seien  $p_1, \dots, p_n$  atomare Formeln
- Sei DNF  $D$  definiert als:

$$D := \bigvee_{(s_1, \dots, s_n) \in \text{TV}(f)} \bigwedge_{i=1}^n A_i$$

wobei  $A_i = p_i$ , wenn  $s_i = T$  und  $A_i = \neg p_i$  sonst

- Sei KNF  $K$  definiert als:

$$K := \bigwedge_{(s_1, \dots, s_n) \notin \text{TV}(f)} \bigvee_{j=1}^n B_j$$

wobei  $B_j = p_j$ , wenn  $s_j = F$  und  $B_j = \neg p_j$  sonst

- Die Wahrheitstabellen von  $D$  und  $K$  entsprechen der Wahrheitsfunktion  $f$

## Satz

- 1 Jede Wahrheitsfunktion kann als DNF oder KNF ausgedrückt werden
- 2 Jede Formel mit  $n$  Atomen induziert eine Wahrheitsfunktion in  $n$  Variablen

## Beweis.

- 1 Es fehlen die Fälle mit trivialer Wahrheitsfunktion:
  - $TV(f) = \emptyset$
  - $TV(f) = \{T, F\}^n$
- 2 Setze  $D = K := p \wedge \neg p$  im ersten Fall
- 3 Setze  $D = K := p \vee \neg p$  im zweiten Fall



## Folgerung

Für jede Formel  $A$  existiert eine DNF  $D$  und eine KNF  $K$ , sodass  $A \equiv D \equiv K$  gilt.

## Beispiel

Die folgende Operation ( $\oplus$ ) wird XOR genannt:

p	q	$p \oplus q$
F	F	F
F	T	T
T	F	T
T	T	F

Wir erstellen die KNF:

$$TV(\oplus) = \{(F, T), (T, F)\}$$

p	q	$p \oplus q$	Disjunktion	KNF
F	F	F	$p_1 \vee p_2$	
T	T	F	$\neg p_1 \vee \neg p_2$	$(p_1 \vee p_2) \wedge (\neg p_1 \vee \neg p_2)$