Computational Logic

# Einführung in die Theoretische Informatik

## Woche 3

Harald Zankl

Institut für Informatik @ UIBK
Wintersemester 2014/2015

# 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

$$\neg A \qquad (A \wedge B) \qquad (A \vee B) \qquad (A \to B)$$

auch Formeln

## Definition

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

## 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 $A \equiv B$*

# 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.*

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

2. *A ist unerfüllbar gdw.*

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

## Beispiel

Wir betrachten die Formel $F$

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

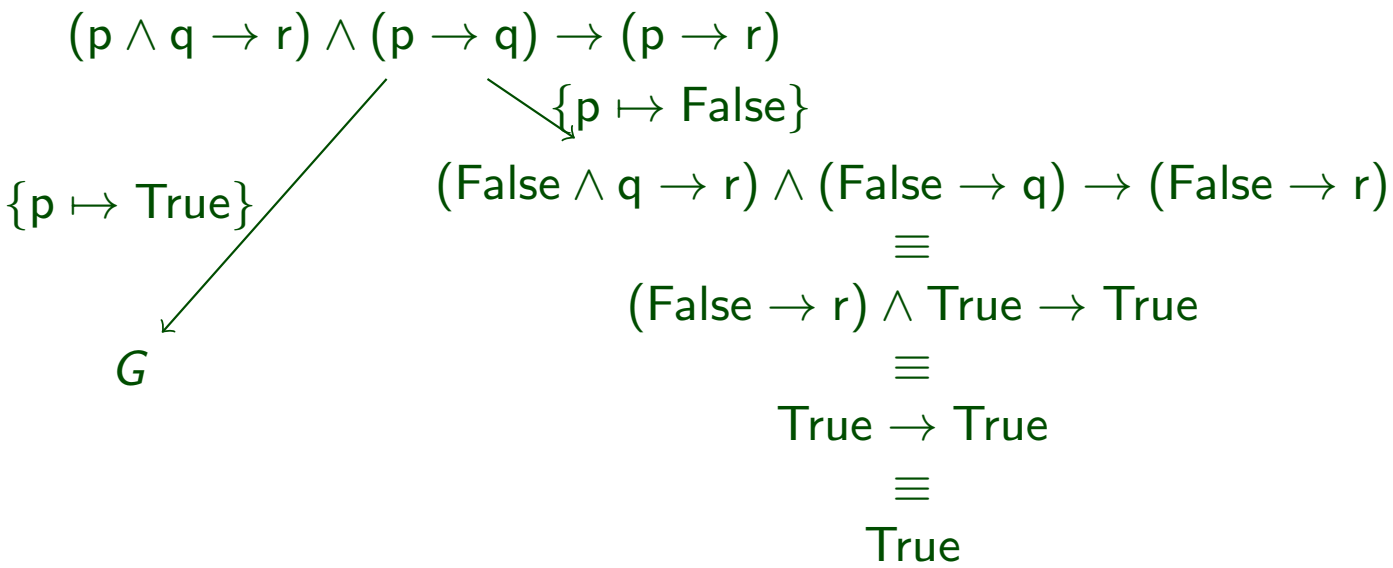
Laut der Methode von Quine ist $F$ eine Tautologie.

## Beispiel

Methode von Quine liefert die folgenden Anforderungen

1. $(\text{True} \wedge q \to r) \wedge (\text{True} \to q) \to (\text{True} \to r) =: G$ ist Tautologie
2. $(\text{False} \wedge q \to r) \wedge (\text{False} \to q) \to (\text{False} \to r)$ ist Tautologie

Anforderungen in Baumform:




Übrige Anforderungen

3. $G$ ist Tautologie

# Beispiel (Fortsetzung)

$$\overbrace{(\text{True} \wedge q \to r) \wedge (\text{True} \to q) \to (\text{True} \to r)}^{G}$$
$$\equiv$$
$$(q \to r) \wedge q \to r$$

$\{q \mapsto \text{True}\}$

$$(\text{True} \to r) \wedge \text{True} \to r$$
$$\equiv$$
$$r \wedge \text{True} \to r$$
$$\equiv$$
$$r \to r$$
$$\equiv$$
$$\text{True}$$

$\{q \mapsto \text{False}\}$

$$(\text{False} \to r) \wedge \text{False} \to r$$
$$\equiv$$
$$\text{True} \wedge \text{False} \to r$$
$$\equiv$$
$$\text{False} \to r$$
$$\equiv$$
$$\text{True}$$

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

# Formales Beweisen

## *Modus Ponens*

$$\frac{A \to B \quad A}{B}\ MP$$

## Definition

Axiome für die Aussagenlogik nach Frege und Łukasiewicz

(1) $A \to (B \to A)$

(2) $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$

(3) $(\neg A \to \neg B) \to (B \to A)$

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

1. Ein Beweis von $B$ aus $\mathcal{G}$ ist eine Sequenz
$$B_1, \ldots, B_\ell \text{ mit } B_\ell = B$$
sodass für alle $1 \leqslant i \leqslant \ell$ 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 $B_{i_2}$, $i_1, i_2 < i$
2. $B$ heißt beweisbar aus den Prämissen $\mathcal{G}$, wenn es einen Beweis von $B$ aus $\mathcal{G}$ gibt

## Definition

1. Die Beweisbarkeitsrelation $A_1, \ldots, A_n \vdash B$ gilt, gdw. $B$ aus $\{A_1, \ldots, A_n\}$ beweisbar ist.
2. Wenn $\vdash B$, dann nennen wir $B$ beweisbar.

## Beispiel

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

$$
\begin{array}{ll}
(1) & A \to (B \to A) \\
(2) & (A \to (B \to C)) \to ((A \to B) \to (A \to C)) \\
(3) & (\neg A \to \neg B) \to (B \to A) \\
(MP) & \dfrac{A \to B \quad A}{B}
\end{array}
$$

| | | |
|---|---|---|
| 1 | $\neg p$ | Prämisse |
| 2 | $\neg p \to (\neg q \to \neg p)$ | Axiom (1) |
| 3 | $\neg q \to \neg p$ | 1, 2, *MP* |
| 4 | $(\neg q \to \neg p) \to (p \to q)$ | Axiom (3) |
| 5 | $p \to q$ | 3, 4, *MP* |

# Korrektheit und Vollständigkeit

## Satz

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

$$A_1, \ldots, A_n \models B \quad \textit{gdw.} \quad A_1, \ldots, A_n \vdash B \ .$$

## Satz (Deduktionstheorem)

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

## Beispiel

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

| $p$ | $q$ | $\neg p \to (p \to q)$ |
|---|---|---|
| T | T | T |
| T | F | T |

| $p$ | $q$ | $\neg p \to (p \to q)$ |
|---|---|---|
| F | T | T |
| F | F | T |

Nun zeigen wir die Gültigkeit mit folgenden Beweis:

| | | |
|---|---|---|
| 1 | $\neg p$ | Prämisse |
| 2 | $\neg p \to (\neg q \to \neg p)$ | Axiom (1) |
| 3 | $\neg q \to \neg p$ | 1, 2, *MP* |
| 4 | $(\neg q \to \neg p) \to (p \to q)$ | Axiom (3) |
| 5 | $p \to q$ | 3, 4, *MP* |
| 6 | $\neg p \to (p \to q)$ | 1, 5, *Deduktionstheorem* |

## Beweis des Deduktionstheorems.

Angenommen $B$ wird mit dem Beweis

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

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

*$A \to B_k$ ist ohne die Prämisse $A$ beweisbar*

1. Basis: $k = 1$; dann gilt $B_1 = B_k = A$ und die Behauptung, da $A \to A$ beweisbar

2. Schritt: $k > 1$; die Induktionshypothese besagt

   *Für alle $l < k$ ist $A \to B_l$ 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 $B_i$, $B_j = (B_i \to B_k)$

## 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 | $B_k \to (A \to B_k)$ | Axiom (1) |
| 3 | $A \to B_k$ | 1, 2, MP |

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

  Wir verwenden folgenden Beweis:

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

# Konjunktive und Disjunktive Normalform

## Definition

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

## Definition

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

$$\mathrm{TV}(f) := \{(s_1, \ldots, s_n) \mid f(s_1, \ldots, s_n) = \mathsf{T}\}$$

## 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* $f : \{\mathsf{T}, \mathsf{F}\}^n \to \{\mathsf{T}, \mathsf{F}\}$ *eine Wahrheitsfunktion mit* $\mathrm{TV}(f) \neq \varnothing$, $\mathrm{TV}(f) \neq \{\mathsf{T}, \mathsf{F}\}^n$
- *Seien* $p_1, \ldots, p_n$ *atomare Formeln*
- *Sei DNF* $D$ *definiert als:*

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

  *wobei* $A_i = p_i$, *wenn* $s_i = \mathsf{T}$ *und* $A_i = \neg p_i$ *sonst*
- *Sei KNF* $K$ *definiert als:*

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

  *wobei* $B_j = p_j$, *wenn* $s_j = \mathsf{F}$ *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:
   - $\mathrm{TV}(f) = \varnothing$
   - $\mathrm{TV}(f) = \{\mathsf{T}, \mathsf{F}\}^n$
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:

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

| p | q | p $\oplus$ q | Disjunktion |
|---|---|---|---|
| F | F | F | $p_1 \vee p_2$ |
| T | T | F | $\neg p_1 \vee \neg p_2$ |

KNF

$$(p_1 \vee p_2) \wedge (\neg p_1 \vee \neg p_2)$$