

Informatik A

Prof. Dr. Norbert Fuhr

fuhr@uni-duisburg.de

auf Basis des Skripts von

Prof. Dr. Wolfram Luther und der Folien von Peter
Fankhauser

Teil I

Logik

Geschichte

- R. Descartes (17. Jhdt): klassische Euklidische Geometrie mit algebraischen Methoden
- G.W. Leibnitz (17. Jhdt): *lingua characteristica*, *calculus rator*
- Gottlob Frege (1879): *Begriffsschrift* Prädikatenlogik erster Stufe
- Skolem (1920): Beweisverfahren
- D. Hilbert, W. Ackermann (1928): Entscheidbarkeitsproblem
- Herbrand (1930): Entscheidbarkeit für korrekten mathematischen Satz
- Alan Turing, Alonzo Church (1936): Unentscheidbarkeit PL1
- Robinson (1954): automatisches Beweisverfahren (Resolutionsprinzip)
- Kowalski, Colmerauer (1972): Prolog

Teil I.1

Aussagenlogik

Aussagenlogik

Grundlagen

- **Aussage** (atomare Formel):
Satz der entweder wahr oder falsch ist
abgekürzt mit Großbuchstaben (A, B, \dots)
- **Beispiel**: Heute ist Sonntag
- **Interpretation**: Zuordnung eines Wahrheitswertes (w oder f) zu jeder Aussage
- **Operation**: Verknüpfung von Aussagen
- **Beispiel**: Heute ist Sonntag und es ist kalt.

Verknüpfungen

- **Negation**: einstellige Operation: $\neg A$ oder \overline{A}

	w	f
\neg	f	w

- **Konjunktion**: zweistellige Operation: $A \wedge B$

\wedge	w	f
w	w	f
f	f	f

- **Disjunktion**: zweistellige Operation: $A \vee B$

\vee	w	f
w	w	w
f	w	f

Formeln

Rekursive Konstruktion:

Literal	L	$::=$	A	Aussage
			$\neg A$	Negierte Aussage
Formel	F	$::=$	L	Literal
			$\neg F$	Negation
			$F \wedge F$	Konjunktion
			$F \vee F$	Disjunktion
			(F)	Klammerung

Beispiel

A ... Heute ist Montag.

B ... Heute ist Feiertag.

C ... Heute ist Vorlesung.

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

Weitere Verknüpfungen

- **Subjunktion:** $A \rightarrow B \equiv \neg A \vee B$

\rightarrow	w	f
w	w	f
f	w	w

- **Bijunktion:** $A \longleftrightarrow B \equiv (A \wedge B) \vee (\neg A \wedge \neg B)$

\longleftrightarrow	w	f
w	w	f
f	f	w

- **Antivalenz (xor):** $A \oplus B \equiv (A \wedge \neg B) \vee (\neg A \wedge B)$

\oplus	w	f
w	f	w
f	w	f

Klauseln

Klausel	K	$::=$	L	Literal
			$K \vee K$	Disjunktion
Konjunktive Form	KF	$::=$	(K)	Klausel
			$(K) \wedge KF$	Konjunktion von Klauseln
Konjunktion	D	$::=$	L	Literal
			$D \wedge D$	Konjunktion
Disjunktive Form	DF	$::=$	(D)	Konjunktion
			$(D) \vee DF$	Disjunktion von Konjunktionen

Beispiele:

$\neg A \vee B \vee C \dots KF$ und DF

$(\neg A \vee B \vee C) \wedge (\neg B \vee \neg C) \dots KF$

$(\neg A \wedge \neg B) \vee (\neg A \wedge \neg C) \vee (B \wedge \neg C) \vee (\neg B \wedge C) \dots DF$

Beweisverfahren

Begriffe

- **Modell**: Interpretation unter der eine Formel F wahr ist.
- **Unerfüllbare Formel**: Formel F , für die es kein Modell gibt.
- **Tautologie**: Formel F , für die jede Interpretation ein Modell ist.
 $\vdash F$

Beweis über Wahrheitstafeln

- Durchrechnen für alle Interpretationen

Axiomatische Verfahren

- Umformen bis zum Wahrheitswert w oder auf konjunktive Form mit mindestens einer Aussage $P \vee \neg P$ in jeder Klausel

Wahrheitstafel

Zu zeigen: $\vdash ((P \rightarrow Q) \wedge P) \rightarrow Q$

P	Q	$P \rightarrow Q$	$(P \rightarrow Q) \wedge P$	$((P \rightarrow Q) \wedge P) \rightarrow Q$
f	f	w	f	w
f	w	w	f	w
w	f	f	f	w
w	w	w	w	w

Syntaktische Umformung

Äquivalent sind die folgenden Formeln:

$$((P \rightarrow Q) \wedge P) \rightarrow Q$$

$$\neg((\neg P \vee Q) \wedge P) \vee Q$$

$$((P \wedge \neg Q) \vee \neg P) \vee Q$$

$$((P \vee \neg P) \wedge (\neg Q \vee \neg P)) \vee Q$$

$$(w \wedge (\neg P \vee \neg Q)) \vee Q$$

$$(\neg P \vee \neg Q) \vee Q$$

$$\neg P \vee w$$

$$w$$

Überführung in konjunktive Form

$$((P \rightarrow Q) \wedge P) \rightarrow Q$$

$$\neg((\neg P \vee Q) \wedge P) \vee Q$$

$$((P \wedge \neg Q) \vee \neg P) \vee Q$$

$$((P \vee \neg P) \wedge (\neg Q \vee \neg P)) \vee Q$$

$$((P \vee \neg P \vee Q) \wedge (\neg Q \vee Q \vee \neg P))$$

Äquivalenzregeln

Zwei Formeln F, G sind äquivalent; $F \equiv G$, wenn gilt: $\vdash F \longleftrightarrow G$

$(F \wedge F) \equiv F, (F \vee F) \equiv F$	Idempotenz
$(F \wedge G) \equiv (G \wedge F),$ $(F \vee G) \equiv (G \vee F)$	Kommutativität
$((F \wedge G) \wedge H) \equiv (F \wedge (G \wedge H)),$ $((F \vee G) \vee H) \equiv (F \vee (G \vee H))$	Assoziativität
$(F \wedge (F \vee G)) \equiv F, (F \vee (F \wedge G)) \equiv F$	Absorption
$(F \wedge (G \vee H)) \equiv ((F \wedge G) \vee (F \wedge H)),$ $(F \vee (G \wedge H)) \equiv ((F \vee G) \wedge (F \vee H))$	Distributivität
$\neg\neg F \equiv F$	Doppelnegation
$\neg(F \vee G) \equiv (\neg F \wedge \neg G),$ $\neg(F \wedge G) \equiv (\neg F \vee \neg G)$	de Morgansche Regeln
$F \rightarrow G \equiv \neg F \vee G$	bedingte Eliminierung
$F \wedge G \equiv F, F \vee G \equiv G,$ $F \wedge G \equiv G, F \vee G \equiv F,$	falls F unerfüllbar falls F Tautologie

Logisches Schließen

- Für S eine Menge von Formeln F_1, \dots, F_k und F eine Formel, ist F eine **logische Konsequenz** von S , in Zeichen $S \vdash F$, wenn jede Interpretation von S , die ein Modell von S ist, auch ein Modell von F ist.
- Regeln:

$$\begin{array}{l} F \vdash F \vee G \\ F \vdash G \rightarrow F \\ F \wedge G \vdash F \\ F \wedge G \vdash G \leftrightarrow F \\ (F \rightarrow G) \wedge (G \rightarrow H) \vdash F \rightarrow H \\ G \wedge (G \rightarrow F) \vdash F \\ \neg F \wedge (G \rightarrow F) \vdash \neg G \end{array} \quad \begin{array}{l} \\ \\ \\ \\ \text{Transitivität} \\ \text{Modus Ponens (Schlussregel)} \\ \text{Modus Tollens} \end{array}$$

Beispiel: Transitivität

A : (a ist eine gerade Zahl und b ist eine gerade Zahl)

B : ($a + b$ ist eine gerade Zahl)

B_1 : ($a = 2n$ und $b = 2m$, n, m ganze Zahlen)

B_2 : ($a + b = 2k$, k ganze Zahl)

A a und b sind gerade Zahlen

$A \rightarrow B_1$ Dann gibt es Zahlen n, m mit $a = 2n$ und $b = 2m$

$B_1 \rightarrow B_2$ Aus $a = 2n$ und $b = 2m$ folgt $a + b = 2(n + m) = 2k$

$B_2 \rightarrow B$ Aus $a + b = 2k$ folgt $a + b$ ist eine gerade Zahl

B Mit der Transitivität gilt B

Axiomensysteme

- **Theorie**: Menge von Axiomen \vdash Menge von Formeln
- **Korrektheit**: Jede Formel F , die aus einer Theorie T mit Hilfe von Axiomen AS abgeleitet wird ($T \vdash_{AS} F$) ist eine logische Konsequenz aus T ($T \vdash F$).
- **Vollständigkeit**: Jede Formel F , die eine logische Konsequenz aus T ist, ist auch tatsächlich mit Hilfe von AS ableitbar.
- **Konsistenz**: Es ist nicht sowohl F als auch $\neg F$ ableitbar.
- **Unabhängigkeit**: Kein Axiom ist die logische Konsequenz anderer Axiome.
- **Entscheidbarkeit**: Für alle Formeln gilt $T \vdash_{AS} F$ oder $T \vdash_{AS} \neg F$.
- Aussagenlogik ist entscheidbar und besitzt konsistente, vollständige und unabhängige Axiomensysteme.

Hilberts Axiomensystem der Aussagenlogik

- AS1: $A \vee A \rightarrow A$
- AS2: $A \rightarrow (A \vee B)$
- AS3: $(A \vee B) \rightarrow (B \vee A)$
- AS4: $(A \rightarrow B) \rightarrow ((C \vee A) \rightarrow (C \vee B))$

- Definition: $A \rightarrow B \equiv \neg A \vee B$
- Modus Ponens: $A \wedge (A \rightarrow B) \vdash B$
- Ersetzungsregel: $F[A/G]$ in der Formel F ersetze einige (alle) Vorkommen der Aussagenvariablen A durch die Formel G

Beispiel

Zeige: $\vdash (F \vee F) \longleftrightarrow F$

Beweis:

$$(F \vee F) \rightarrow F \quad \text{AS1.}$$

$$F \rightarrow (F \vee G) \quad \text{AS2,}$$

$$F \rightarrow (F \vee F) \quad \text{Ersetzungsregel } ((F \vee G)[G/F]).$$

Automatisches Beweisen

Resolution

- Modus Ponens:

$$\frac{P \quad P \rightarrow B}{B}$$

- Verallgemeinerung: $P \rightarrow B \equiv \neg P \vee B$

$$\frac{P \vee A_1 \vee A_2 \vee \dots \vee A_n \quad \neg P \vee B_1 \vee B_2 \vee \dots \vee B_m}{A_1 \vee A_2 \vee \dots \vee A_n \vee B_1 \vee B_2 \vee \dots \vee B_m \text{ Resolvente}}$$

- Um die Aussage A zu beweisen füge die Negation der Aussage $\neg A$ zu den Formeln der Theorie und versuche, durch Resolution die leere Klausel herzuleiten.

Beispiel

$$T = A \vee B, A \rightarrow \neg B, \neg A$$

Um B herzuleiten, fügen wir $\neg B$ zur Theorie dazu, und formen $A \rightarrow \neg B$ um.

Das ergibt:

$$T' = A \vee B, \neg A \vee \neg B, \neg A, \neg B$$

In Klauselform:

$$T' = (A, B), (\neg A, \neg B), \neg A, \neg B$$

B ist ein Resolvent von (A, B) und $\neg A$. Der Resolvent von B und $\neg B$ ist die leere Menge, daher ist T' unerfüllbar, daher folgt aus T B .

Teil I.2

Prädikatenlogik

Prädikatenlogik

Erweiterung der Aussagenlogik

- Konstante: a, b, c
- Variablen: x, y, z
- Funktionen: $f(a_1, \dots, a_k)$
- Prädikate: $P(a_1, \dots, a_k)$
- Quantoren: Allquantor ($\forall xF$), Existenzquantor ($\exists xF$)

Semantik

Interpretation:

Abbildung auf Domäne zur Zuordnung eines Wahrheitswertes

Beispiel

$$F : \forall x P(f(x, a), x).$$

- Domäne: natürliche Zahlen $\mathbb{N} := \{1, 2, 3, \dots\}$
- Konstante $a ::= 1$
- $f(x, a) ::= x * a$
- $P(x, y) ::= x = y$
- Interpretation: Für alle natürlichen Zahlen $x \in \mathbb{N}$ gilt $x \cdot 1 = x$.

Weitere Schlussregeln und Äquivalenzen

$\forall xF \vdash \exists xF$ für eine nichtleere Domäne

$$\forall xF \vee \forall xG \vdash \forall x(F \vee G)$$

$$\exists x(F \wedge G) \vdash \exists xF \wedge \exists xG$$

$$\neg \forall xF \equiv \exists x \neg F$$

$$\neg \exists xF \equiv \forall x \neg F$$

$$\forall x \forall y F \equiv \forall y \forall x F$$

$$\exists x \exists y F \equiv \exists y \exists x F$$

$$\forall x(F \wedge G) \equiv \forall xF \wedge \forall xG$$

$$\exists x(F \vee G) \equiv \exists xF \vee \exists xG$$

Entscheidbarkeit von PL1

- Die Wahrheitstafelmethode ist nicht übertragbar
- Erfüllbarkeit und Allgemeingültigkeit ist nicht entscheidbar
- PL1 ist **halbentscheidbar**: Unerfüllbare Formeln werden nach endlicher Zeit erkannt.

Beispiel: Peano-Axiome

1. $P(1)$

2. $\forall x (P(x) \rightarrow \exists y (P(y) \wedge Q(x, y)))$.

3. $\neg \exists x (P(x) \wedge Q(x, 1))$

4. $\forall x_1 \forall x_2 \forall y_1 \forall y_2 (P(x_1) \wedge P(x_2) \wedge Q(x_1, y_1) \wedge Q(x_2, y_2) \wedge \neg(x_1 = x_2) \rightarrow \neg(y_1 = y_2))$.

5. $\forall M (M(1) \wedge \forall x \forall y (P(x) \wedge P(y) \wedge M(x) \wedge Q(x, y) \rightarrow M(y)) \rightarrow (M \equiv P))$.

Interpretation

- $P(x)$... x ist eine natürliche Zahl
- $Q(x, y)$... $y = x + 1$; y ist Nachfolger von x
- M ... Prädikatenvariable (nicht möglich in PL1)