Teil I: Formale Grundlagen der Informatik I

Endliche Automaten und formale Sprachen

# Teil II: Formale Grundlagen der Informatik II

# Logik in der Informatik

Martin Otto

Professor für Mathematische Logik
und Grundlagen der Informatik

TUD, Fachbereich Mathematik

Sommer 2015

## Inhalt

## Logik und Logik in der Informatik

- formalisierte Aussagen
  über Eigenschaften von Systemen
  $\to$ *Spezifikation*
- systematisches Nachprüfen
  von Eigenschaften von Systemen
  $\to$ *Verifikation, model checking*
- logische Beziehungen & Kriterien
  – Folgerungen
  – Äquivalenzen
  – Erfüllbarkeit/Allgemeingültigkeit

**SYNTAX** und **SEMANTIK**



## Logik und Logik in der Informatik

- formalisierte Eigenschaften
  von Elementen in Strukturen
  $\to$ z.B. DB Abfragen
- systematische Auswertung
  $\to$ z.B. Abfrageauswertung
- logische Beziehungen & Kriterien
  – Implikation ($\to$)/Subsumption ($\subseteq$)
  – Äquivalenzen (z.B. zur Abfrageoptimierung)
  – Leerheitstest

**SYNTAX** und **SEMANTIK**

## Logik und Logik in der Informatik

- systematisches logisches Schließen;
  Deduktion, formales Beweisen
  $\rightarrow$ Wissensrepräsentation, KI
  $\rightarrow$ automatisches/interaktives Beweisen, ...

**SYNTAX und SEMANTIK**

---

**historisch:** Grundlagen der Mathematik
formales Beweisen und seine Rechtfertigung

**von Grundlagenfragen der Mathematik zu:**
Fragen der Berechenbarkeit/Entscheidbarkeit (Church, Turing)
Kernfragen der theoretischen Informatik (vorweggenommen)

*seither:* immer neue praktische Anwendungen in der Informatik



## Literatur

**Burris: Logic for Mathematics and Computer Science**
Prentice-Hall 1998.

**Ben-Ari: Mathematical Logic for Computer Science**
Springer 1993.

**Ebbinghaus, Flum, Thomas:**
**Einführung in die mathematische Logik**
Spektrum 1998.

**Schöning: Logik für Informatiker**
Spektrum 2000.

# Teil 1: Aussagenlogik, AL

## Gegenstandsbereich:

Verknüpfungen elementarer Aussagen mittels
Boolescher logischer Verknüpfungen

Boolesche Verknüpfungen (Junktoren): $\neg, \wedge, \vee, \rightarrow, \ldots$

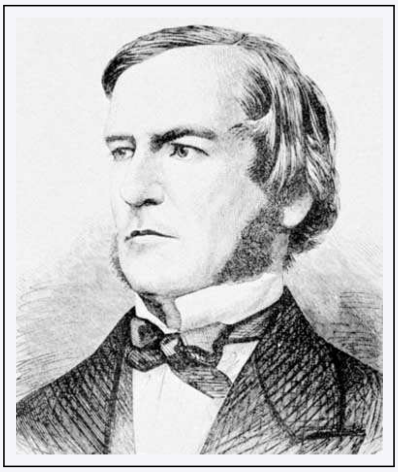
**Wesentlich:**

- strukturierte Formalisierung komplexerer Eigenschaften
- modulare Semantik
- kombinatorisch-algebraischer Charakter der Logik (Boole)
- korrekte und vollständige Beweiskalküle





# George Boole (1815–1864)



**Algebraisierung/Mathematisierung der Logik**

z.B. The Mathematical Analysis of Logic,
Being an Essay Towards a Calculus of Deductive Reasoning
1847

An Investigation of the Laws of Thought, 1854

## AL Syntax

Definition 1.1

Symbole: $0, 1;\ p, q, r, \ldots, p_1, p_2, \ldots;\ \neg, \wedge, \vee, \ldots;\ (,)$

$\mathbf{AL}(\boldsymbol{\mathcal{V}})$, die Menge der $\mathrm{AL}$-*Formeln über* $\mathcal{V}$
zu geg. $\mathrm{AL}$-Variablenmenge $\mathcal{V}$, induktiv erzeugt:

| | |
|---|---|
| atomare Formeln: | 0, 1, $p$ in $\mathrm{AL}(\mathcal{V})$ (wobei $p \in \mathcal{V}$). |
| Negation: | für $\varphi \in \mathrm{AL}(\mathcal{V})$ ist auch $\neg\varphi \in \mathrm{AL}(\mathcal{V})$. |
| Konjunktion: | für $\varphi, \psi \in \mathrm{AL}(\mathcal{V})$ ist auch $(\varphi \wedge \psi) \in \mathrm{AL}(\mathcal{V})$. |
| Disjunktion: | für $\varphi, \psi \in \mathrm{AL}(\mathcal{V})$ ist auch $(\varphi \vee \psi) \in \mathrm{AL}(\mathcal{V})$. |

Übung: Kontextfreie Grammatik (für $\mathrm{AL}(\mathcal{V}_n)$)





## AL Syntax

evtl. weitere Junktoren, offiziell hier nur als Abkürzungen:

z.B.
$$\begin{aligned}(\varphi \rightarrow \psi) &:= (\neg\varphi \vee \psi),\\ (\varphi \leftrightarrow \psi) &:= ((\neg\varphi \wedge \neg\psi) \vee (\varphi \wedge \psi)).\end{aligned}$$

statt allg. $\mathrm{AL}(\mathcal{V})$ oft auch für standardisierte Variablenmengen:

$$\begin{aligned}\mathrm{AL} &:= \mathrm{AL}(\mathcal{V}), & \mathcal{V} &= \{p_i : i \geqslant 1\}\\ \mathrm{AL}_n &:= \mathrm{AL}(\mathcal{V}_n), & \mathcal{V}_n &= \{p_i : 1 \leqslant i \leqslant n\}\end{aligned}$$

## AL Semantik — Definition 1.4

**Interpretationen**
von *Belegungen* der $\mathrm{AL}$-Variablen
zu *Wahrheitswerten* für $\mathrm{AL}$-Formeln: Wahrheitswerte in $\mathbb{B} = \{0,1\}$

$\mathcal{V}$-Interpretation (Belegung):

$$\boxed{\begin{array}{rcl} \mathfrak{I}\colon \mathcal{V} & \longrightarrow & \mathbb{B} \\ p & \longmapsto & \mathfrak{I}(p) \end{array}}$$

$$\mathfrak{I} \text{ interpretiert } p \text{ als } \begin{cases} \text{“wahr”} & \text{wenn } \mathfrak{I}(p) = 1, \\ \text{“falsch”} & \text{wenn } \mathfrak{I}(p) = 0. \end{cases}$$

zur Definition der Semantik von Formeln $\varphi \in \mathrm{AL}(\mathcal{V})$
über geg. $\mathcal{V}$-Interpretation $\mathfrak{I}$:

definiere Wahrheitswertfunktion
$$\begin{array}{rcl} {}^{\mathfrak{I}}\colon \mathrm{AL}(\mathcal{V}) & \longrightarrow & \mathbb{B} \\ \varphi & \longmapsto & \varphi^{\mathfrak{I}} \end{array}$$

induktiv über den Aufbau der Formeln $\varphi$
als Fortsetzung der Variablen-Belegung





## AL Semantik: Wahrheitswerte

Wahrheitswerte für Formeln $\varphi \in \mathrm{AL}(\mathcal{V})$
bzgl. einer geg. $\mathcal{V}$-Interpretatation $\mathfrak{I}$

**Funktion $\varphi \longmapsto \varphi^{\mathfrak{I}}$ induktiv:**

| | |
|---|---|
| atomare Formeln: | $0^{\mathfrak{I}} := 0$; $1^{\mathfrak{I}} := 1$; $p^{\mathfrak{I}} := \mathfrak{I}(p)$. |
| Negation: | $(\neg\varphi)^{\mathfrak{I}} := 1 - \varphi^{\mathfrak{I}}$. |
| Konjunktion: | $(\varphi \wedge \psi)^{\mathfrak{I}} := \min(\varphi^{\mathfrak{I}}, \psi^{\mathfrak{I}})$. |
| Disjunktion: | $(\varphi \vee \psi)^{\mathfrak{I}} := \max(\varphi^{\mathfrak{I}}, \psi^{\mathfrak{I}})$. |

## AL Semantik: Modellbeziehung

aus Funktion $\varphi \longmapsto \varphi^{\mathfrak{I}}$ definiere:

$\boxed{\mathfrak{I} \textit{ erfüllt } \varphi \quad \text{gdw. } \varphi^{\mathfrak{I}} = 1}$

Schreibweise: $\mathfrak{I} \models \varphi$.

Sprechweisen: $\mathfrak{I}$ *erfüllt* $\varphi$,
$\mathfrak{I}$ *ist Modell von* $\varphi$,
$\varphi$ *ist wahr unter* $\mathfrak{I}$.

Für Formelmengen $\Phi \subseteq \mathrm{AL}(\mathcal{V})$ entsprechend:

$\mathfrak{I} \models \Phi$ gdw. $\mathfrak{I} \models \varphi$ für alle $\varphi \in \Phi$.





## AL Semantik: Wahrheitstafeln

für $\varphi \in \mathrm{AL}_n$ schreiben wir auch $\varphi = \varphi(p_1, \dots, p_n)$

für $(b_1, \dots, b_n) \in \mathbb{B}^n$ sei

$$\varphi[b_1, \dots, b_n] := \begin{cases} \varphi^{\mathfrak{I}} \text{ für Interpretation } \mathfrak{I} \\ \text{mit } (\mathfrak{I}(p_i) = b_i)_{i=1,\dots,n} \end{cases}$$

der Wahrheitswert von $\varphi$ auf $(b_1, \dots, b_n)$.

**Wahrheitstafel:**

Wertetabelle der Funktion $\begin{cases} \mathbb{B}^n & \longrightarrow & \mathbb{B} \\ (b_1, \dots, b_n) & \longmapsto & \varphi[b_1, \dots, b_n] \end{cases}$

Diese Information bestimmt die Semantik von $\varphi$ vollständig!

## AL Semantik: Wahrheitstafeln

Semantik der Junktoren anhand ihrer Wahrheitstafeln:

| $p$ | $\neg p$ |
|---|---|
| 0 | 1 |
| 1 | 0 |

| $p$ | $q$ | $p \wedge q$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

| $p$ | $q$ | $p \vee q$ |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 1 |

| $p$ | $q$ | $p \rightarrow q$ |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 1 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

| $p$ | $q$ | $p \leftrightarrow q$ |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |





## grundlegende semantische Begriffe → Abschnitt 2.1

Folgerung, Äquivalenz, Allgemeingültigkeit, Erfüllbarkeit

### (1) Folgerungsbeziehung $\varphi \models \psi$

für $\varphi, \psi \in \mathrm{AL}(\mathcal{V})$:
$\psi$ *folgt aus* $\varphi$, wenn für *alle* $\mathcal{V}$-Interpretationen $\mathfrak{I}$ gilt:
$\mathfrak{I} \models \varphi \;\Rightarrow\; \mathfrak{I} \models \psi$.

Entsprechend $\Phi \models \psi$ für Formelmengen $\Phi$

### (2) Allgemeingültigkeit $\models \varphi$

$\varphi \in \mathrm{AL}(\mathcal{V})$ *allgemeingültig*, wenn für *alle* $\mathcal{V}$-Interpretationen $\mathfrak{I}$ gilt:
$\mathfrak{I} \models \varphi$.

**Beispiele**

$\varphi \models \varphi \vee \psi, \qquad \varphi \models (\varphi \wedge \psi) \vee (\varphi \wedge \neg\psi), \qquad \models \varphi \vee \neg\varphi$

## grundlegende semantische Begriffe → Abschnitt 2.2

Folgerung, Äquivalenz, Allgemeingültigkeit, Erfüllbarkeit

### (3) Logische Äquivalenz $\varphi \equiv \psi$

$\varphi, \psi \in \mathrm{AL}(\mathcal{V})$ *logisch äquivalent*,
wenn für *alle* $\mathcal{V}$-Interpretationen $\mathfrak{I}$ gilt:
$\mathfrak{I} \models \varphi$ gdw. $\mathfrak{I} \models \psi$.

d.h.: identische Wahrheitstafeln!

Schreibweise: $\varphi \equiv \psi$

**sämtlich äquivalent:** $\left\{ \begin{array}{l} \varphi \equiv \psi \\ \models \varphi \leftrightarrow \psi \\ \varphi \models \psi \ \text{ und } \ \psi \models \varphi \end{array} \right.$





## Beispiele: logische Äquivalenzen = Identitäten in BA

$\neg\neg p \equiv p, \quad p \vee 0 \equiv p, \quad p \wedge 0 \equiv 0, \quad \ldots$

$p \vee q \equiv q \vee p, \quad (p \vee q) \vee r \equiv p \vee (q \vee r), \quad \ldots$

$(p \vee q) \equiv \neg(\neg p \wedge \neg q), \quad (p \wedge q) \equiv \neg(\neg p \vee \neg q)$

$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r), \quad p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

## grundlegende semantische Begriffe → Abschnitt 2.3

Folgerung, Äquivalenz, Allgemeingültigkeit, Erfüllbarkeit

### Erfüllbarkeit

$\varphi \in \mathrm{AL}(\mathcal{V})$ *erfüllbar*,
wenn es *mindestens eine* $\mathcal{V}$-Interpretation $\mathfrak{I}$ *gibt* mit $\mathfrak{I} \models \varphi$.

analog für Formelmengen $\Phi \subseteq \mathrm{AL}$:
$\Phi$ erfüllbar, wenn $\mathfrak{I} \models \Phi$ für mindestens ein $\mathfrak{I}$.

**wichtig:**

$\boxed{\varphi \text{ erfüllbar} \quad \text{gdw.} \quad \neg\varphi \textit{ nicht } \text{allgemeingültig}}$





## Erfüllbarkeit

### Zentrale Rolle der Erfüllbarkeit (SAT):

- $\models \varphi$ gdw. $\neg\varphi$ *nicht* erfüllbar.
- $\varphi \models \psi$ gdw. $\varphi \wedge \neg\psi$ *nicht* erfüllbar.
- $\Phi \models \psi$ gdw. $\Phi \cup \{\neg\psi\}$ *nicht* erfüllbar.
- $\varphi \equiv \psi$ gdw. weder $\varphi \wedge \neg\psi$ noch $\neg\varphi \wedge \psi$ erfüllbar.

### AL Erfüllbarkeitsproblem (SAT(AL)) entscheidbar:

$\mathrm{SAT}(\mathrm{AL}) = \{\varphi \in \mathrm{AL} \colon \varphi \text{ erfüllbar } \}$ entscheidbar

– wie?

– mit welchem Aufwand? (Komplexität)

## AL und Boolesche Funktionen → Abschnitt 3

$\mathcal{B}_n$: die Menge aller $n$-stelligen Booleschen Funktionen

$$\begin{array}{rcl} f : \mathbb{B}^n & \longrightarrow & \mathbb{B} \\ (b_1, \dots, b_n) & \longmapsto & f(b_1, \dots, b_n) \end{array}$$

speziell für $\varphi \in \mathrm{AL}_n$:

$$\boxed{\left.\begin{array}{rcl} f_\varphi : \mathbb{B}^n & \longrightarrow & \mathbb{B} \\ (b_1, \dots, b_n) & \longmapsto & \varphi[b_1, \dots, b_n] \end{array}\right\} \in \mathcal{B}_n}$$

beachte: $f_\varphi = f_\psi$ gdw. $\varphi \equiv \psi$

also: $\begin{array}{rcl} \mathrm{AL}_n /\!\equiv & \longrightarrow & \mathcal{B}_n \\ [\varphi]_\equiv & \longmapsto & f_\varphi \end{array}$ injektiv!

**Fragen:**

- wieviele $n$-stellige Boolesche Funktionen gibt es?; $|\mathcal{B}_n| =$?
- ist jedes $f \in \mathcal{B}_n$ durch $\mathrm{AL}$-Formel $\varphi \in \mathrm{AL}_n$ darstellbar?





## Disjunktive und konjunktive Normalformen, DNF, KNF

Nomenklatur: $p$ bzw. $\neg p$ (für $p \in \mathcal{V}$) heißen *Literale*

**D**isjunktionen von Konjunktionen von Literalen: **DNF**-Formeln
**K**onjunktionen von Disjunktionen von Literalen: **KNF**-Formeln

“große” Konjunktion/Disjunktion (Schreibweisen):

für endliche Formelmenge $\Phi = \{\varphi_1, \dots, \varphi_n\}$:

$\bigwedge \Phi := \bigwedge_{i=1}^n \varphi_i = \varphi_1 \wedge \ldots \wedge \varphi_n$

$\bigvee \Phi := \bigvee_{i=1}^n \varphi_i = \varphi_1 \vee \ldots \vee \varphi_n$

Konvention: auch *leere* Disjunktionen/Konjunktionen zulässig

mit der Interpretation: $\bigvee \emptyset \equiv 0$ (!)

$\bigwedge \emptyset \equiv 1$ (!)