Teil I: Formale Grundlagen der Informatik I

Endliche Automaten und formale Sprachen

Teil II: Formale Grundlagen der Informatik II

Logik in der Informatik

Martin Ziegler

Professor für Angewandte Logik

TU Darmstadt, Fachbereich Mathematik

Sommer 2011

(Folien wesentlich basierend auf Prof. M Otto)

Inhalt

Logik und Logik in der Informatik

- formalisierte Aussagen
  über Eigenschaften von Systemen
  → *Spezifikation*
- systematisches Nachprüfen
  von Eigenschaften von Systemen
  → *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
  → z.B. DB Abfragen
- systematische Auswertung
  → z.B. Abfrageauswertung
- logische Beziehungen & Kriterien
  – Implikation (→)/Subsumption (⊆)
  – Äquivalenzen (z.B. zur Abfrageoptimierung)
  – Leerheitstest

SYNTAX und **SEMANTIK**

Logik und Logik in der Informatik

- systematisches logisches Schließen;
  Deduktion, formales Beweisen
  → Wissensrepräsentation, KI
  → 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:

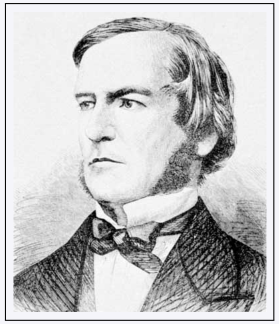
Verknüpfungen elementarer Aussagen mittels Boolescher logischer Verknüpfungen

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

$\mathbf{AL}(\mathcal{V})$, die Menge der AL-*Formeln über* $\mathcal{V}$
zu geg. 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.
$$\begin{array}{rcl} (\varphi \to \psi) & := & (\neg\varphi \vee \psi), \\ (\varphi \leftrightarrow \psi) & := & ((\neg\varphi \wedge \neg\psi) \vee (\varphi \wedge \psi)). \end{array}$$

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

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

AL Semantik Definition 1.4

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

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

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

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 φ
als Fortsetzung der Variablen-Belegung

AL Semantik: Wahrheitswerte

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

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* φ,
$\mathfrak{I}$ *ist Modell von* φ,
φ *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 φ auf $(b_1, \dots, b_n)$.

Wahrheitstafel:

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

Diese Information bestimmt die Semantik von φ 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 $\rightarrow$ Abschnitt 2.1

Folgerung, Äquivalenz, Allgemeingültigkeit, Erfüllbarkeit

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

für $\varphi, \psi \in \mathrm{AL}(\mathcal{V})$:
ψ *folgt aus* φ, wenn für *jede* $\mathcal{V}$-Interpretation $\mathfrak{I}$ gilt:
aus $\mathfrak{I} \models \varphi$ folgt $\mathfrak{I} \models \psi$.

Entsprechend $\Phi \models \psi$ für Formel*mengen* Φ

(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

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

grundlegende semantische Begriffe → Abschnitt 2.2

Folgerung, Äquivalenz, Allgemeingültigkeit, Erfüllbarkeit

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

$\varphi, \psi \in \mathrm{AL}(\mathcal{V})$ heißen *logisch äquivalent* (Schreibweise: $\varphi \equiv \psi$)
wenn für *alle* $\mathcal{V}$-Interpretationen $\mathfrak{I}$ gilt:
$\mathfrak{I} \models \varphi$ gdw. $\mathfrak{I} \models \psi$ d.h. identische Wahrheitstafeln!

Es gilt:
$\varphi \equiv \psi$ gdw. $\varphi \models \psi$ und $\psi \models \varphi$ gdw. $\models \varphi \leftrightarrow \psi$

Beispiele: $\neg\neg p \equiv p, \quad p \vee 0 \equiv p, \quad p \wedge 0 \equiv 0, \quad \dots$

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

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

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

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 $\Phi \subseteq \mathrm{AL}$:
Φ 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:

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

– wie?

– mit welchem Aufwand? (Komplexität)

– wie sieht ein Zertifikat aus für Un-/Erfüllbarkeit? ($\mathcal{P}$ vs. $\mathcal{NP}$)

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 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*

Disjunktionen von Konjunktionen von Literalen: **DNF**-Formeln
Konjunktionen 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: $\bigvee \emptyset \equiv 0$ (!)
$\bigwedge \emptyset \equiv 1$ (!)

Funktionale Vollständigkeit

Funktionale Vollständigkeit von AL_n für $\mathcal{B}_n$:

zu jedem $f \in \mathcal{B}_n$ existiert DNF-Formel $\varphi \in \mathrm{AL}_n$ mit $f = f_\varphi$.

($\Rightarrow$ bijektive Korrespondenz zw. $\mathcal{B}_n$ und $\mathrm{AL}_n/\!\equiv$)

Beweis:

betrachte $\varphi_f := \bigvee \{\varphi_{\mathbf{b}} \colon f(\mathbf{b}) = 1\}$

wo $\varphi_{\mathbf{b}} = \bigwedge \{p_i \colon b_i = 1\} \wedge \bigwedge \{\neg p_i \colon b_i = 0\}$

Korollar: Satz über DNF und KNF

$$\text{zu } \varphi \in \mathrm{AL}_n \text{ existieren stets: } \begin{cases} \text{DNF-Formel } \varphi_1 \in \mathrm{AL}_n \text{ mit } \varphi_1 \equiv \varphi, \\ \text{KNF-Formel } \varphi_2 \in \mathrm{AL}_n \text{ mit } \varphi_2 \equiv \varphi. \end{cases}$$

Dualität Konjunktion/Disjunktion

$\rightarrow$ Abschnitt 3.2

nützliche Umformungen/Rechenregeln

$\neg(\varphi_1 \wedge \varphi_2) \equiv \neg\varphi_1 \vee \neg\varphi_2$ verallgemeinert sich zu $\boxed{\neg(\bigwedge \Phi) \equiv \bigvee \Phi^\neg}$

wobei $\Phi^\neg := \{\neg\varphi \colon \varphi \in \Phi\}$

$\neg(\varphi_1 \vee \varphi_2) \equiv \neg\varphi_1 \wedge \neg\varphi_2$ verallgemeinert sich zu $\boxed{\neg(\bigvee \Phi) \equiv \bigwedge \Phi^\neg}$

für **KNF** $\overset{\neg}{\longleftrightarrow}$ **DNF:**

$$\boxed{\neg \underbrace{\bigwedge_{i=1}^{k} \big(\bigvee C_i\big)}_{\text{KNF}} \;\equiv\; \underbrace{\bigvee_{i=1}^{k} \big(\bigwedge C_i^\neg\big)}_{\text{DNF (*)}}}$$

$C_1, \dots, C_k$ (endl.) Mengen von Literalen
* Doppelnegationen in den $C_i^\neg$ eliminieren

Beispiel für exponentiellen "blow-up"

$$\boxed{\varphi_m = \varphi_m(p_1, \dots, p_{2m}) \;:=\; \bigwedge_{i=1}^m \neg(p_{2i-1} \leftrightarrow p_{2i}) \;\in \mathrm{AL}_{2m}}$$

- φ_m hat genau 2^m erfüllende Interpretationen in $\mathbb{B}^{2m}$
- KNF von Länge $\sim m$ (linear in m):
  $\varphi_m \equiv \bigwedge_{i=1}^m \big((p_{2i-1} \vee p_{2i}) \wedge (\neg p_{2i-1} \vee \neg p_{2i})\big)$
- DNF in Länge $\sim 2m2^m$ (exponentiell in m):
  $\varphi_m \equiv \bigvee \{\varphi_{\mathbf{b}} \colon \mathbf{b} \in \mathbb{B}^{2m}, \varphi_m[\mathbf{b}] = 1\}$
- **keine kürzere DNF:** $\begin{cases} \text{keine kürzeren Disjunktionsglieder!} \\ \text{keine redundanten Disjunktionsglieder!} \end{cases}$