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

$\boxed{\textbf{SYNTAX} \text{ und } \textbf{SEMANTIK}}$

Logik und Logik in der Informatik

- systematisches logisches Schließen;
  Deduktion, formales Beweisen
  → Wissensrepräsentation, KI
  → automatisches/interaktives Beweisen, ...

$\boxed{\textbf{SYNTAX} \text{ und } \textbf{SEMANTIK}}$

---

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)
danach: immer neue praktische Anwendungen in der Informatik

Logik und Logik in der Informatik

- formalisierte Eigenschaften

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

$\boxed{\textbf{SYNTAX} \text{ und } \textbf{SEMANTIK}}$

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 98.

Schöning: Logik für Informatiker
Spektrum 2000.

Teil 1: Aussagenlogik, AL

Gegenstandsbereich:

Verknüpfungen elementarer Aussagen mittels Boolescher logischer Verknüpfungen

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

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

Syntax der Aussagenlogik AL

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

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

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

evtl. weitere Junktoren, offiziell als Abkürzungen:
z.B. $(\varphi \rightarrow \psi) := (\neg\varphi \vee \psi)$,
$(\varphi \leftrightarrow \psi) := \big((\neg\varphi \wedge \neg\psi) \vee (\varphi \wedge \psi)\big)$.

über Standard-Variablen: $\mathsf{AL} := \mathsf{AL}(\mathcal{V}), \quad \mathcal{V} = \{p_i \colon i \geqslant 1\}$
$\mathsf{AL}_n := \mathsf{AL}(\mathcal{V}_n), \quad \mathcal{V}_n = \{p_i \colon 1 \leqslant i \leqslant n\}$

Semantik der Aussagenlogik AL

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

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

$\mathfrak{I}$ interpretiert p 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 $\varphi \in$ AL($\mathcal{V}$)
über geg. $\mathcal{V}$-Interpretation $\mathfrak{I}$:

Wahrheitswertfunktion $\quad {}^{\mathfrak{I}}\colon \mathsf{AL}(\mathcal{V}) \longrightarrow \mathbb{B}$
$\qquad \varphi \longmapsto \varphi^{\mathfrak{I}}$

induktiv über den Aufbau der Formeln φ definiert!

Semantik: Wahrheitswerte für Formeln $\varphi \in$ AL($\mathcal{V}$)
bzgl. einer $\mathcal{V}$-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:	$(\varphi \vee \psi)^{\mathfrak{I}} := \max(\varphi^{\mathfrak{I}}, \psi^{\mathfrak{I}})$.

Modellbeziehung

$\mathfrak{I}$ *erfüllt* φ 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 $\Phi \subseteq$ AL($\mathcal{V}$) entsprechend:
$\mathfrak{I} \models \Phi$ gdw. $\mathfrak{I} \models \varphi$ für alle $\varphi \in \Phi$.

Semantik und 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 $(b_1, \dots, b_n)$.

Wahrheitstafeln

die Wertetabelle der Funktion

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

bestimmt die Semantik von φ vollständig!

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

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. $\mathfrak{I} \models \psi$. [identische Wahrheitstafeln!]

Schreibweise: $\varphi \equiv \psi$

sämtlich äquivalent: $\varphi \equiv \psi$
$\models \varphi \leftrightarrow \psi$
$\varphi \models \psi$ und $\psi \models \varphi$

Beispiele (vgl. Identitäten in Booleschen Algebren)

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

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

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

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

Grundlegende semantische Begriffe

Folgerung, Äquivalenz, Allgemeingültigkeit, Erfüllbarkeit

Folgerungsbeziehung $\varphi \models \psi$

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

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

Allgemeingültigkeit $\models \varphi$

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

Beispiele

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

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 $\mathfrak{I}$.

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

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.

$\mathrm{SAT}(\mathrm{AL}) = \{\varphi \in \mathrm{AL} : \varphi \text{ erfüllbar }\}$ entscheidbar (wie?)