Automatisches Beweisen

Viorica Sofronie-Stokkermans (sofronie@mpi-sb.mpg.de)

Webseite:

www.mpi-sb.mpg.de/∼sofronie/teaching/autreas-trier.html

Inhalt

Aussagenlogik

- Syntax, Semantik
- OBDDs, DPLL-Algorithmus

Prädikatenlogik 1. Stufe

- Syntax, Semantik, Modelltheorie, . . .
- Resolution, Tableaux

Ziele

- Einführung in der Logik
- Einführung in das automatische Beweisen
- Beweissysteme

  Korrektheit, Vollständigkeit, Komplexität, Implementierung
- Effiziente Algorithmen für spezifische deduktive Probleme
- Praktische Anwendungen

Literatur

Uwe Schöning: Logik für Informatiker, Spektrum

Melvin Fitting: First-Order Logic and Automated Theorem Proving, Springer

Spezialartikel zu den einzelnen Kapiteln.

Teil 1: Aussagenlogik

- Eine Logik der Wahrheitswerten
- Entscheidbar (NP-vollständig)
- Wichtig für Hardware Anwendungen (Boolesche Schaltkreise) und Model Checking

1.1 Syntax

- Aussagenvariablen
- Logische Verknüpfungen
  $\Rightarrow$ Boolesche Kombinationen

Aussagenvariablen

Sei Π eine Menge von Aussagenvariablen.

Wir verwenden die Buchstaben P, Q, R, S, um Aussagenvariablen zu bezeichnen

Aussagenformeln

F_Π Menge der Formeln über Π:

$$
\begin{array}{rcll}
F, G, H & ::= & \bot & \text{(Falsum)} \\
& \mid & \top & \text{(Verum)} \\
& \mid & P, \quad P \in \Pi & \text{(atomische Formel)} \\
& \mid & \neg F & \text{(Negation)} \\
& \mid & (F \wedge G) & \text{(Konjunktion)} \\
& \mid & (F \vee G) & \text{(Disjunktion)} \\
& \mid & (F \implies G) & \text{(Implikation)} \\
& \mid & (F \equiv G) & \text{(Äquivalenz)}
\end{array}
$$

Konventionen zur Notation

- Klammereinsparungen werden nach folgenden Regeln vorgenommen:
  - $\neg \quad >_p \quad \vee \quad >_p \quad \wedge \quad >_p \quad \Longrightarrow \quad >_p \quad \equiv$ (Präzedenzen),
  - $\vee$ und $\wedge$ sind assoziativ und kommutativ,
  - $\Longrightarrow$ ist rechtsassoziativ.

Terminologie

Eine Formel F, die als Teil einer Formel G auftritt,
heißt Teilformel von G.

F ist eine Teilformel von F

$$\left.\begin{array}{l} F = \neg G \text{ und} \\ H \text{ Teilformel von } G \end{array}\right\} \rightarrow \quad H \text{ Teilformel von } F$$

$$\left.\begin{array}{l} F = F_1 \ \rho \ F_2 \\ (\text{wo } \rho \in \{\vee, \wedge, \Rightarrow, \Leftrightarrow\}) \\ H \text{ Teilformel von } F_1 \text{ oder } F_2 \end{array}\right\} \rightarrow \quad H \text{ Teilformel von } F$$

1.2. Semantik

Klassische Logik:

zwei Wahrheitswerte “wahr” (1) und “falsch” (0) .

(Es existieren auch mehrwertige Logiken: mehr als zwei Wahrheitswerte)

Boole'sche Funktionen

Boole'sche Funktion $\quad f : \{0,1\}^n \to \{0,1\}$

$$B_\neg : \{0,1\} \to \{0,1\} \qquad B_\neg(0) = 1; \quad B_\neg(1) = 0$$

$$B_\vee : \{0,1\}^2 \to \{0,1\} \qquad B_\vee(x,y) = 0 \quad \text{gdw} \quad x = 0 \text{ und } y = 0$$

$$B_\wedge : \{0,1\}^2 \to \{0,1\} \qquad B_\wedge(x,y) = 1 \quad \text{gdw} \quad x = 1 \text{ und } y = 1$$

$$B_\Rightarrow : \{0,1\}^2 \to \{0,1\} \qquad B_\Rightarrow(x,y) = 0 \quad \text{gdw} \quad x = 1 \text{ und } y = 0$$

$$B_\Leftrightarrow : \{0,1\}^2 \to \{0,1\} \qquad B_\Leftrightarrow(x,y) = 1 \quad \text{gdw} \quad x = y$$

Wertbelegungen

Aussagenvariablen für sich haben keine Bedeutung.

Hierfür müssen Wertebelegungen (Valuationen) explizit oder implizit aus dem Kontext zur Verfügung stehen.

Eine Valuation ist eine Abbildung

$$\mathcal{A} : \Pi \to \{0, 1\}$$

wo $\{0, 1\}$ die Menge der Wahrheitswerte ist.

Wahrheitswert einer Formel in $\mathcal{A}$

Sei $\mathcal{A} : \Pi \to \{0, 1\}$ eine Π-Valuation. $\mathcal{A}^* : F_\Pi \to \{0, 1\}$ wird induktiv über Aufbau von F wie folgt definiert:

$$\begin{aligned}
\mathcal{A}^*(\bot) &= 0 \\
\mathcal{A}^*(\top) &= 1 \\
\mathcal{A}^*(P) &= \mathcal{A}(P) \\
\mathcal{A}^*(\neg F) &= 1 - \mathcal{A}^*(F) \\
\mathcal{A}^*(F \rho G) &= \mathrm{B}_\rho(\mathcal{A}^*(F), \mathcal{A}^*(G)) \\
&\quad \text{wo } \mathrm{B}_\rho \text{ die Boolesche Funktion assoziiert mit } \rho
\end{aligned}$$

Wir schreiben normalerweise $\mathcal{A}$ statt $\mathcal{A}^*$.

1.3 Modelle, Gültigkeit, Erfüllbarkeit

Gültigkeit und Erfüllbarkeit

F gilt in $\mathcal{A}$ ($\mathcal{A}$ ist Modell von F):

$$\mathcal{A} \models F \;\; :\Leftrightarrow \;\; \mathcal{A}(F) = 1$$

F ist (allgemein-) gültig (oder eine Tautologie):

$$\models F \;\; :\Leftrightarrow \;\; \mathcal{A} \models F, \;\text{ für alle } A : \Pi \to \{0, 1\}$$

F heißt erfüllbar gdw. es $\mathcal{A} : \Pi \to \{0, 1\}$ gibt, so daß $\mathcal{A} \models F$.

Sonst heißt F unerfüllbar (oder eine Kontradiktion).

Folgerung und Äquivalenz

F impliziert G (oder G folgt aus F), i.Z. $F \models G$

$$:\Leftrightarrow \quad \text{für alle } \mathcal{A} : \Pi \to \{0,1\} \text{ gilt: } \mathcal{A} \models F \Longrightarrow \mathcal{A} \models G.$$

F und G sind äquivalent

$$:\Leftrightarrow \quad \text{für alle } \mathcal{A} : \Pi \to \{0,1\} \text{ gilt: } \mathcal{A} \models F \text{ gdw. } A \models G.$$

Proposition 1.1 *$F \models G$ gdw. $(F \implies G)$ ist gültig*

Proposition 1.2 *F und G äquivalent gdw. $(F \equiv G)$ ist gültig.*

Erweiterung auf Formelmengen N in natürlicher Weise, z.B.:

$$N \models G \quad :\Leftrightarrow \quad \text{für alle } \mathcal{A} : \Pi \to \{0,1\} \text{ gilt:}$$
$$\text{falls } \mathcal{A} \models F, \text{ für alle } F \in N,$$
$$\text{so} \quad \mathcal{A} \models G.$$

Gültigkeit vs. (Un-)Erfüllbarkeit

Nachweis von Gültigkeit (und damit Folgerung oder Äquivalenz) durch (Un-)Erfüllbarkeitstest:

Proposition 1.3

$$F \textit{ gültig} \quad \Leftrightarrow \quad \neg F \textit{ unerfüllbar}$$

Frage: $N \models G$ kann ähnlicherweise durch Unerfüllbarkeit nachgewiesen werden. Wie?

Gültigkeit vs. (Un-)Erfüllbarkeit

Nachweis von Gültigkeit (und damit Folgerung oder Äquivalenz) durch (Un-)Erfüllbarkeitstest:

Proposition 1.4

$$N \models G \qquad \Leftrightarrow \qquad N \cup \{\neg G\} \ \textit{unerfüllbar}$$