Computational Logic
Algorithmische Logik

Boolesche Logik und Algebra

Ralf Moeller
Hamburg Univ. of Technology

Eine Logelei: Supermann existiert nicht!

Wenn Supermann das Böse verhindern kann und will, dann wird er es tun. Wenn Supermann das Böse nicht verhindern kann, dann ist er machtlos; wenn er es nicht verhindern will, dann ist er böswillig. Supermann verhindert das Böse nicht. Wenn Supermann existiert, ist er weder machtlos noch böswillig. Darum existiert Supermann nicht.

Folgerung und Äquivalenz

Eine Formel G heißt eine *Folgerung* der Formeln $F_1, \ldots, F_k$ falls für jede Belegung, die sowohl zu $F_1, \ldots, F_k$ als auch zu G passend ist, gilt:

> Wenn $\mathcal{A}$ Modell von $\{F_1, \ldots, F_k\}$ ist, dann ist $\mathcal{A}$ auch Modell von G.

Wir schreiben $F_1, \ldots, F_k \models G$, falls G eine Folgerung von $F_1, \ldots, F_k$ ist.

Zwei Formeln F und G heißen (*semantisch*) *äquivalent*, falls für alle Belegungen $\mathcal{A}$, die sowohl für F als auch für G passend sind, gilt $\mathcal{A}(F) = \mathcal{A}(G)$. Hierfür schreiben wir $F \equiv G$.

Motivation für Wahrheitstabelle von $\rightarrow$

- Wir betrachten folgende Formeln
  - Wenn es regnet,
    scheint die Sonne nicht: $R \rightarrow \neg S$
  - Es regnet: R
- Daraus folgt: Die Sonne scheint nicht!
  - Also: $\{R \rightarrow \neg S, R\} \models \neg S$
  - Wie sehen die Modelle von $\{R \rightarrow \neg S, R\}$ aus?
  - R hat den Wert 1,
  - Wie wird $R \rightarrow \neg S$ auf 1 abgebildet?
  - $\neg S$ muß auf 1 abgebildet werden (qed)

$1 \rightarrow 1 = 1$

$1 \rightarrow 0 = 0$

$0 \rightarrow 1 = 1$

$0 \rightarrow 0 = 1$

Zweites Beispiel:

- Wenn es regnet,
  scheint die Sonne nicht: $R \to \neg S$
- Es regnet nicht: $\neg R$

$1 \to 1 = 1$

$1 \to 0 = 0$

$0 \to 1 = 1$

$0 \to 0 = 1$

- Folgt daraus: Die Sonne scheint nicht?
  - $\{R \to \neg S, \neg R\} \models \neg S$?
  - Wie sehen die Modelle von $\{R \to \neg S, \neg R\}$ aus?
  - R hat den Wert 0, da $\neg R$ auf 1 abgebildet werden soll
  - Wenn $R \to \neg S$ auf 1 abgebildet werden soll, dann bleiben die dritte und vierte Zeile, somit kann in den Modellen von $\{R \to \neg S, \neg R\}$ auch $\neg S$ auf 0 abgebildet werden (wir wählen die Variante aus Zeile 4)

Schlußmuster

- Wir haben gesehen:
  - $\{P, P \rightarrow Q\} \models Q$ (Name für Schlußmuster: Modus Ponens)
- Folgendes können wir auch zeigen:
  - $\{Q, \neg P \rightarrow \neg Q\} \models P$ (Name für Schlußmuster: Modus Tollens)
- Oder auch:
  - $\{\neg Q, P \rightarrow Q\} \models \neg P$ (Name für Schlußmuster: Kontraposition)

Aufgaben

Gelten die folgenden Äquivalenzen?

$$
\begin{aligned}
(A \rightarrow B) \rightarrow C &\equiv A \rightarrow (B \rightarrow C) \\
(A \rightarrow B) \rightarrow C &\equiv (A \wedge B) \rightarrow C \\
(A \leftrightarrow B) \leftrightarrow C &\equiv A \leftrightarrow (B \leftrightarrow C)
\end{aligned}
$$

Gelten die folgenden Aussagen?

				J/N	Gegenb.
Wenn	$(F \rightarrow G)$ gültig	dann	$F \models G$		
Wenn	$F \models G$	dann	$(F \rightarrow G)$ gültig		
Wenn	$(F \leftrightarrow G)$ gültig	dann	$F \equiv G$		
Wenn	$F \equiv G$	dann	$(F \leftrightarrow G)$ gültig		

Die Hauptprobleme

- Modellprüfung

  Sei F eine Formel und sei $\mathcal{A}$ eine passende Belegung. Gilt $\mathcal{A}(F) = 1$?

- Erfüllbarkeit

  Sei F eine Formel. I st F erfüllbar ?

- Gültigkeit

  Sei F eine Formel. Ist F gültig ?

- Folgerung

  Seien F und G Formeln. Gilt $F \models G$?

- Äquivalenz

  Seien F und G Formeln. Gilt $F \equiv G$?

Aufgabe

Welche Probleme lassen sich auf welche reduzieren?

- Gültigkeit $\Longleftrightarrow$ (Nicht)Erfüllbarkeit:

$$F \text{ gültig gdw. } \neg F \text{ nicht erfüllbar}$$
$$F \text{ erfüllbar gdw. } \neg F \text{ nicht gültig}$$

- Gültigkeit $\Longrightarrow$ Folgerung:

$$F \text{ gültig gdw. } \mathrm{T} \models F$$

- Folgerung $\Longrightarrow$ Gültigkeit:

$$F \models G \text{ gdw. } F \to G \text{ gültig}$$

- Gültigkeit $\Longrightarrow$ Äquivalenz:

$$F \text{ gültig gdw. } F \equiv T$$

- Äquivalenz $\Longrightarrow$ Gültigkeit:

$$F \equiv G \text{ gdw. } F \leftrightarrow G \text{ gültig}$$

Lösung des Erfüllbarkeitsproblems

- Gegeben sei eine aussagenlogische Formel F, deren Erfüllbarkeit zu prüfen ist
- In der Formel kommen atomare Formeln (Variablen) vor
- Teste für alle Belegungsmöglichkeiten der atomaren Formeln den Wahrheitswert
- Wenn sich eine Belegung finden läßt, so daß der Wahrheitswert von F sich zu 1 berechnet, ist F erfüllbar (semantische Beweismethoden)
- Man muß bei n Variablen 2^n Möglichkeiten prüfen

Gesucht wird ein mechanisches Verfahren

- Wir definieren einen Operator $\vdash$
- $\{F1, F2, ..., Fk\} \vdash G$
- Ansprüche an $\vdash$
- Korrektheit
  - Wenn $\{F1, F2, ..., Fk\} \vdash G$ dann $\{F1, F2, ..., Fk\} \vDash G$
- Vollständigkeit
  - Wenn $\{F1, F2, ..., Fk\} \vDash G$ dann $\{F1, F2, ..., Fk\} \vdash G$

Lösung des Äquivalenzproblems

- Es soll gezeigt werden, daß eine Formel F äquivalent zu einer Formel G ist.
- $F \equiv G$ gdw. $(F \leftrightarrow G)$ gültig gdw. $\neg(F \leftrightarrow G)$ nicht erfüllbar
- Man muß im schlimmsten Fall 2^n verschiedene Belegungsmöglichkeiten testen
- Frage: Geht das nicht direkt durch Umformung der syntaktischen Einheiten für F und G, so daß F syntaktisch in G überführt wird?

Ersetzbarkeitstheorem

Satz (Ersetzbarkeitstheorem)
Seien F und G äquivalente Formeln. Sei H eine Formel mit (mindestens) einem Vorkommen der Teilformel F. Dann ist H äquivalent zu H', wobei H' aus H hervorgeht, indem (irgend) ein Vorkommen von F in H durch G ersetzt wird.

Beweisprinzipien: Induktion

- Behauptung: $\mathcal{B}$(F) gilt für jede Formel F
- Beweis:
  - 1. Man zeige, es gilt $\mathcal{B}(A_i)$ für jede atomare Formel A_i.
  - 2. Man zeige unter der (Induktions-)Annahme, daß $\mathcal{B}$(F) und $\mathcal{B}$(G) gelten, folgt, daß $\mathcal{B}(F \wedge G)$, $\mathcal{B}(F \vee G)$, $\mathcal{B}(\neg F)$ gelten

Beweis: (Ersetzbarkeitstheorem)

Beweis (durch Induktion über den Formelaufbau von H):

Induktionsanfang: Falls H eine atomare Formel ist, dann kann nur $H = F$ sein. Und damit ist klar, daß H äquivalent zu H' ist, denn $H' = G$.

Induktionsschritt: Falls F gerade H selbst ist, so trifft dieselbe Argumentation wie im Induktionsanfang zu. Sei also angenommen, F ist eine Teilformel von H mit $F \neq H$. Dann müssen wir drei Fälle unterscheiden.

Fall 1: H hat die Bauart $H = \neg H_1$.
Nach Induktionsvoraussetzung ist H_1 äquivalent zu $H_1^{'}$, wobei $H_1^{'}$ aus H_1 durch Ersetzung von F durch G hervorgeht. Nun ist aber $H^{'} = \neg H_1^{'}$. Aus der (semantischen) Definition von „$\neg$“ folgt dann, daß H und $H^{'}$ äquivalent sind.
Fall 2: H hat die Bauart $H = (H_1 \vee H_2)$.
Dann kommt F entweder in H_1 oder H_2 vor. Nehmen wir den ersteren Fall an (der zweite ist völlig analog). Dann ist nach Induktionssannahme H_1 wieder äquivalent zu $H_1^{'}$, wobei $H_1^{'}$ aus H_1 durch Ersetzung von F durch G hervorgeht. Mit der Definition von „$\vee$“ ist dann klar, daß $H \equiv (H_1^{'} \vee H_2) = H^{'}$.
Fall 3: H hat die Bauart $H = (H_1 \wedge H_2)$.
Diesen Fall beweist man völlig analog zu *Fall 2*.

Äquivalenzen

Satz

Es gelten die folgenden Äquivalenzen:

$$
\begin{array}{rcll}
(F \wedge F) & \equiv & F & \\
(F \vee F) & \equiv & F & \text{(Idempotenz)} \\
(F \wedge G) & \equiv & (G \wedge F) & \\
(F \vee G) & \equiv & (G \vee F) & \text{(Kommutativität)} \\
((F \wedge G) \wedge H) & \equiv & (F \wedge (G \wedge H)) & \\
((F \vee G) \vee H) & \equiv & (F \vee (G \vee H)) & \text{(Assoziativität)} \\
F \wedge (F \vee G)) & \equiv & F & \\
F \vee (F \wedge G)) & \equiv & F & \text{(Absorption)} \\
F \wedge (G \vee H)) & \equiv & ((F \wedge G) \vee (F \wedge H)) & \\
F \vee (G \wedge H)) & \equiv & ((F \vee G) \wedge (F \vee H)) & \text{(Distributivität)} \\
\neg\neg F & \equiv & F & \text{(Doppelnegation)}
\end{array}
$$

Weitere Äquivalenzen

$$
\begin{aligned}
\neg(F \wedge G) &\equiv (\neg F \vee \neg G) & \\
\neg(F \vee G) &\equiv (\neg F \wedge \neg G) & \text{(deMorgansche Regeln)} \\
(F \vee G) &\equiv F, \text{ falls } F \text{ Tautologie} & \\
(F \wedge G) &\equiv G, \text{ falls } F \text{ Tautologie} & \text{(Tautologieregeln)} \\
(F \vee G) &\equiv G, \text{ falls } F \text{ unerfüllbar} & \\
(F \wedge G) &\equiv F, \text{ falls } F \text{ unerfüllbar} & \text{(Unerfüllbarkeitsregeln)}
\end{aligned}
$$