Grundlagen der Programmierung

Ralf Möller, FH-Wedel

- Vorige Vorlesung:
  - Aussagenlogik (Boole'sche Logik)
- Inhalt dieser Vorlesung
  - Boole'sche Algebra
- Lernziele:
  - Ersetzbarkeitstheorem
  - Äquivalente Transformation von Ausdrücken

Wiederholung Aussagenlogik

- Syntax
  - Induktive Definition von Formeln
- Semantik
  - Bedeutung durch Elemente der Menge $\{0, 1\}$ bestimmt
  - Belegungsfunktion A: $\{A_1, A_2, A_3, A_4, \dots\} \rightarrow \{0, 1\}$
    - Anwendungen der Belegungsfunktion: Interpretation
  - Festlegung der Semantik der "Formelbildungsoperatoren"
    - Operatoren als Funktionen mit Urbild- und Bildbereich $\{0, 1\}$
    - "Wahrheitstabellen"
  - Modellbegriff
  - Entscheidungsprobleme

Begriff der induktiven Definition

- Zunächst einfachste Einheiten (Atome) festlegen
  - Beispiel: atomare Formeln der Aussagenlogik
- Dann erklären wie aus einfachen Einheiten komplexere Einheiten konstruiert werden können
  - Beispiel: Bildung allgemeiner Formeln wie $F \wedge G$, $F \vee G$, $\neg F$

Noch ein paar Abkürzungen ...

- Sei A eine beliebige atomare Formel (Variable)
- $\top$ stehe für $A \vee \neg A$
- $\perp$ stehe für $A \wedge \neg A$

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.

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: $R \rightarrow \neg S$
- Es regnet nicht: $\neg R$

$1 \rightarrow 1 = 1$
$1 \rightarrow 0 = 0$
$0 \rightarrow 1 = 1$
$0 \rightarrow 0 = 1$

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

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 $F \equiv G$.

Aufgaben

Gelten die folgenden Äquivalenzen?

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

Gelten die folgenden Aussagen?

				J/N	Gegenb.
Wenn	$(F \to G)$ gültig	dann	$F \models G$		
Wenn	$F \models G$	dann	$(F \to G)$ 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:

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

- Folgerung $\Longrightarrow$ Gültigkeit:

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

- 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

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

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

Boole'sche Algebra

- Äquivalenzen als "Transformationsgesetze"
  - Ersetzbarkeitstheorem
- Zentrale Frage:
  - Ist das alles Zufall?
  - Hängen die Gesetze irgendwie zusammen?
- Beispiel:
  - Nehmen wir an, die Äquivalenzen "Kommutativität" und "Distributivität" wurden bewiesen.
  - Muß man die anderen dann noch beweisen?
    Der Beweis über die Semantik ist aufwendig!

Boole'sche Algebra: Zentrale Idee

- Man nehme Operatoren, deren Semantik eine Funktion über einer Grundmenge M ist
  - Über die Elemente von M wollen wir nichts sagen!
  - Ein mögliches Beispiel ist nun M = {0, 1}
- Man nehme an, daß bezüglich der Operatoren gewisse Gesetze (sog. Axiome) gelten
- Nun zeige man, daß unter bestimmten Voraussetzungen andere Gesetze ebenfalls gelten

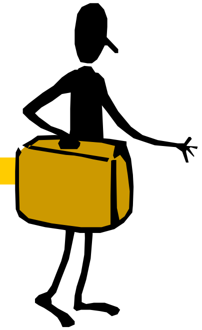
Boole'sche Algebra: Definition (Huntington)

- Grundmenge M
- Zwei zweistellige Operatoren: φ, ψ
- Zu jedem Operator gibt es in M ein neutrales Element {NULL, EINS} $\subseteq$ M, so daß gilt:
  - $x \ \varphi \ \mathrm{NULL} \equiv x$
  - $x \ \psi \ \mathrm{EINS} \equiv x$
- Zu jedem Element gibt es eindeutig ein Inverses: $\cdot^{-1}$
  - Für alle $x \in M$ gilt: $x^{-1} \in M$, $x \ \varphi \ x^{-1} = \mathrm{EINS}$, $x \ \psi \ x^{-1} = \mathrm{NULL}$
- Es gelten weiterhin
  das Kommutativgesetz und das Distributivgesetz

Boole'sche Algebra: Gesetze (Axiome)

- Kommutativgesetze
  - $x \varphi y \equiv y \varphi x$
  - $x \psi y \equiv y \psi x$
- Distributivgesetze
  - $x \varphi (y \psi z) \equiv (x \varphi y) \psi (x \varphi z)$
  - $x \psi (y \varphi z) \equiv (x \psi y) \varphi (x \psi z)$

Zusammenfassung, Kernpunkte



- Aussagenlogik (Boole'sche Logik)
  - Syntax, Formel
  - Semantik, Belegung, Modell
  - Entscheidungsprobleme
- Semantische und Syntaktische Verfahren zur Lösung von Inferenzproblemen
  - Erfüllbarkeit durch Wahrheitstabellen
  - Transformation von Formeln in äquivalente Formeln
- Einführung Boole'sche Algebra

Was kommt beim nächsten Mal?

- Fortsetzung Boole'sche Algebra
- Weitere syntaktische Verfahren zur Lösung von Entscheidungsproblemen