Diskrete Strukturen und Logik

WiSe 2006/07 in Trier

Henning Fernau
Universität Trier
fernau@informatik.uni-trier.de

$\boxed{\text{Diskrete Strukturen und Logik}}$ Gesamtübersicht

- Organisatorisches
- Einführung
- Logik & Mengenlehre
- Beweisverfahren
- Kombinatorik: Die Kunst des Zählens
- algebraische Strukturen

aus der letzten Vorlesung

Aussagen und Aussageformen

Verknüpfung von Aussagen (Junktoren)

einfache Rechenregeln

skizzierte Anwendung: Programmverifikation

. . . heute (und morgen) . . .

Tautologien und Kontradiktionen

Prädikatenlogik

Aussageverbindungen

Sind p_1, ..., p_n Aussagen, so können wir diese unter Verwendung der vorher eingeführten Verknüpfungen zu einer sog. *Aussageverbindung* $a(p_1, \ldots, p_n)$ kombinieren.

Im Allgemeinen gilt: Abhängig von den Wahrheitswerten der Aussagen p_i kann man $a(p_1, \ldots, p_n)$ somit einen Wahrheitswert zuordnen.

Beispiel: $a(p, q) = ((p \vee \neg q) \wedge (p \implies q))$ ist wahr, falls p und q wahr sind, aber falsch, falls p wahr und q falsch ist.

Tautologien und Kontradiktionen

Eine Aussageverbindung $a(p_1, \ldots, p_n)$ von n Aussagen p_1, p_2, ..., p_n heißt *Tautologie* (bzw. *Kontradiktion*), wenn sie unabhängig von den Wahrheitswerten der Aussagen p_i stets falsch (bzw. wahr) ist.

Beispiel: $p \vee \neg p$: *Prinzip vom ausgeschlossenen Dritten* Tautologie
Beispiel: $p \wedge \neg p$: *Prinzip vom ausgeschlossenen Widerspruch* Kontradiktion

Beweis: Wahrheitstafel !

Beispiel: $((p \Rightarrow q) \wedge (q \Rightarrow p)) \iff (p \iff q)$ Tautologie

Hinweis: Äquivalenzen beweist man daher durch Nachrechnen von zwei Implikationsrichtungen.

Beispiele für Tautologien

1. $(p \Rightarrow \neg p) \Rightarrow \neg p$
2. $(p \wedge (p \Rightarrow q)) \Rightarrow q$
3. $(p \wedge q) \Rightarrow p$, $(p \wedge q) \rightarrow q$
4. $p \Rightarrow (p \vee q)$, $q \Rightarrow (p \vee q)$
5. $(p \Rightarrow q) \Rightarrow [(q \Rightarrow r) \Rightarrow (p \Rightarrow r)]$
6. $((p \Rightarrow q) \wedge (q \Rightarrow r) \wedge p) \Rightarrow r$

Hinweis: Beweisverfahren fußen oft auf Tautologien

Beweise für Tautologien Z.B. 5. mit (kombinierter, gekürzter) Wahrheitstafel

p	q	r	$A = p \Rightarrow q$	$B = q \Rightarrow r$	$C = p \Rightarrow r$	$D = B \Rightarrow C$	$A \Rightarrow D$
w	w	w	w	w	w	w	w
w	w	f	w	f	f	w	w
w	f	$?$	f	$?$	$?$	$?$	w
f	w	w	w	w	w	w	w
f	w	f	w	f	w	w	w
f	f	$?$	w	w	w	w	w

“Abkürzungsregel:” Ist die Prämisse falsch, so ist die Implikation wahr.

$\boxed{\textbf{Logische Äquivalenz}}$ von Aussageverbindungen

Zwei Aussageverbindungen $a_1(p_1, \ldots, p_n)$ und $a_2(p_1, \ldots, p_n)$ mit denselben Aussagen $p_1, \ldots, p_n$ heißen *logisch äquivalent*, falls die Aussageverbindung

$$a_1(p_1, \ldots, p_n) \iff a_2(p_1, \ldots, p_n)$$

eine Tautologie ist.

Schreibweise: $a_1(p_1, \ldots, p_n) \equiv a_2(p_1, \ldots, p_n)$

Viele bislang gefundene Rechenregeln und Tautologien lassen sich so schreiben (s. nächste Folie).

Logische Äquivalenzen — Beispiele

1. Kommutativgesetze: $(p \wedge q) \equiv (q \wedge p)$; $(p \vee q) \equiv (q \vee p)$.

2. Assoziativgesetze: $(p \wedge (q \wedge r)) \equiv ((p \wedge q) \wedge r)$; $(p \vee (q \vee r)) \equiv ((p \vee q) \vee r)$.

3. Distributivgesetze: $(p \wedge (q \vee r)) \equiv ((p \wedge q) \vee (p \wedge r))$; $(p \vee (q \wedge r)) \equiv ((p \vee q) \wedge (p \vee q))$.

4. Gesetze von de Morgan: $\neg(p \wedge q) \equiv (\neg p \vee \neg q)$; $\neg(p \vee q) \equiv (\neg p \wedge \neg q)$.

5. Identitätsgesetze: $(p \vee f) \equiv p$, $(p \wedge t) \equiv p$.

6. Umkehrschluss: $(p \Rightarrow q) \equiv (\neg q \Rightarrow \neg p)$.

7. Auflösen der Implikation: $(p \Rightarrow q) \equiv (\neg p \vee q)$.

8. Auflösen der Äquivalenz: $(p \iff q) \equiv ((p \Rightarrow q) \wedge (q \Rightarrow p)) \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$.

Logische Äquivalenzen — Beweise

1. Wahrheitstafelbeweis (vollständige Fallunterscheidung), z.B. für Umkehrschluss

2. Ausnutzung bekannter Tautologien (also durch Umformungen), z.B. für 8b:

$$
\begin{aligned}
(p \iff q) &\equiv^{8a} ((p \Rightarrow q) \land (q \Rightarrow p)) \\
&\equiv^{7} ((\neg p \lor q) \land (\neg q \lor p)) \\
&\equiv^{3} ((\neg p \lor q) \land \neg q) \lor ((\neg p \lor q) \land p) \\
&\equiv^{1,3} ((\neg p \land \neg q) \lor (q \land \neg q)) \lor ((\neg p \land p) \lor (q \land p)) \\
&\equiv^{1,2,5} (p \land q) \lor (\neg p \land \neg q)
\end{aligned}
$$

Noch mehr logische Äquivalenzen

1. $((p \Rightarrow q) \wedge (r \Rightarrow q)) \equiv (p \vee r) \Rightarrow q$.
2. $(p \vee (q \wedge \neg q)) \equiv p$;
   $(p \wedge (q \vee \neg q)) \equiv p$.
3. Dominanz: $p \wedge f \equiv f$; $p \vee t \equiv t$.
4. Negationsgesetze: $p \wedge \neg p \equiv f$; $p \vee \neg p \equiv t$.
5. Doppelte Negation: $\neg\neg p \equiv p$.
6. Idempotenzgesetze: $p \wedge p \equiv p$; $p \vee p \equiv p$.
7. Absorptionsgesetze: $(p \wedge (p \vee q)) \equiv p$; $(p \vee (p \wedge q)) \equiv p$.

Abtrennungsregel *modus ponens* (Schlussketten)

Ist p wahr sowie $p \Rightarrow q$, so auch q.

In Zeichen: $(p \wedge (p \Rightarrow q)) \Rightarrow q$. (z.B.: Wahrheitstafelbeweis)

Sind allgemein $p_1, \ldots, p_n$ Aussagen und
sind p_1 und $p_i \Rightarrow p_{i+1}$ wahr für $i = 1, \ldots, n-1$,
so ist p_n wahr.

Hierfür schreibt man abkürzend (wenn auch nicht ganz korrekt):
$(p_1 \wedge (p_1 \Rightarrow p_2 \Rightarrow \ldots \Rightarrow p_n)) \Rightarrow p_n$

Ähnlich notiert man manchmal Ketten von Äquivalenzen (s.o.(!))

Eine Knobelaufgabe

Gespensterknobelei

Die entsprechenden Dateien finden Sie original hier.

Aufgabe: Wie können wir das Problem modellieren und lösen ?