Universität Hamburg Department Mathematik

Boolesche Algebra

Hans Joachim Oberle

Vorlesung an der TUHH im Wintersemester 2006/07

Montags, 9:45 - 11:15 Uhr, 14täglich

TUHH, DE 22, Audimax 2

http://www.math.uni-hamburg.de/home/oberle/vorlesungen.html

Literatur.

R. Haggarty: Diskrete Mathematik für Informatiker.
Pearson Studium, München, 2004.
ISBN: 3 8273 7095 7.

R. Lidl, G. Pilz: Angewandte abstrakte Algebra I, II.
BI Wissenschaftsverlag, Mannheim, 1982.
Englische Ausgabe (2. Auflage): Springer, New York, 1997.

E. Mendelson: Boolesche Algebra und logische Schaltungen.
Schaums Outline, McGraw-Hill, Hamburg, 1982.
ISBN: 0 07 092033 8.

H.J. Oberle: Boolesche Algebra.
Skript der Universität Hamburg, Hamburg, 1990.

1. Aussagen

Definition (1.1)

Aussagen sind Sätze, die entweder *wahr* oder *falsch* sind.

Tertium non datur (Es gibt keine dritte Möglichkeit)!

Ist A eine Aussage, so bezeichnet $w(A)$ ihren *Wahrheitswert*, $w(A) = 1$ falls A eine wahre Aussage ist und $w(A) = 0$ andernfalls.

Beispiele:

"Hamburg ist die Hauptstadt Deutschlands" - "$1 + 1 = 2$" - "Es regnet" - "Wie geht es dir?" (ist keine Aussage!) - "$x > 5$" (ist keine Aussage!)

Definition (1.2)

Aussagenformen sind sprachliche Gebilde mit Leerstellen (Aussagevariablen). Dort können *Subjekte (Dinge)*, *Prädikate (Eigenschaften)* oder *Aussagen* eingesetzt werden. Wenn man einsetzt, erhält man eine Aussage. I.Allg. muss wohldefiniert werden, was eingesetzt werden darf!

Beispiele (1.3):

- $P(x)$ sei "x ist die Hauptstadt von Deutschland"; $P(x)$ ist eine Aussageform (keine Aussage!); für die Variable x dürfen wir Städtenamen einsetzen.
P(München) (ist eine Aussage) ist falsch, P(Berlin) ist wahr.

- $Q(z) :\Leftrightarrow z > 3$. Wir setzen reelle Zahlen ein, $z \in \mathbb{R}$.
$Q(11)$ ist wahr, $Q(-2)$ ist falsch.

Verknüpfung von Aussagen durch Junktoren (1.4):
Seien A und B Aussagen. Dann werden die folgenden Aussagen definiert

- Negation $\neg A$ (“nicht A”)
- Konjunktion $A \wedge B$ (“A und B”)
- Disjunktion $A \vee B$ (“A oder B”)
- Implikation $A \Rightarrow B$ (“wenn A, dann B”)
- Äquivalenz $A \Leftrightarrow B$ (“A ist äquivalent zu B”)

Wahrheitswertetabellen (1.5) (Definition der Junktoren)

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
w	w	f	w	w	w	w
w	f	f	f	w	f	f
f	w	w	f	w	w	f
f	f	w	f	f	w	w

Die Implikation wird allgemeiner als im normalen Sprachgebrauch üblich definiert (dort gibt es immer einen Zusammenhang zwischen Prämisse und Konklusion). Wichtig (und gewöhnungsbedürftig): Wenn die Prämisse falsch ist, ist die Implikation immer wahr!

Beispiele (1.6):

$A :\Leftrightarrow$ "Es regnet.", $B :\Leftrightarrow$ "Es ist Montag.",
$\neg B \Leftrightarrow$ "Es ist nicht Montag."
$(A \wedge B) \Leftrightarrow$ "Es regnet und es ist Montag."
$(A \vee B) \Leftrightarrow$ "Es regnet oder es ist Montag"
$(A \Rightarrow B) \Leftrightarrow$ "Immer wenn es regnet, ist Montag."
$(B \Rightarrow A) \Leftrightarrow$ "Wenn Montag ist, dann regnet es."
$(B \Rightarrow (1+1=2))$ ist eine wahre Aussage, da $1+1=2$ wahr ist (die Aussage ist also an jedem Wochentag wahr).

Dies sind aber nicht alle möglichen Verknüpfungen zweier Aussagen, es gibt genau $2^4 = 16$ verschiedene Junktoren.

A	B	o_1	o_2	o_3	o_4	o_5	o_6	o_7	o_8	o_9	o_{10}	o_{11}	o_{12}	o_{13}	o_{14}	o_{15}	o
w	w	w	f	w	f	w	f	w	f	w	f	w	f	w	f	w	
w	f	w	w	f	f	w	w	f	f	w	w	f	f	w	w	f	
f	w	w	w	w	w	f	f	f	f	w	w	w	w	f	f	f	
f	f	w	w	w	w	w	w	w	w	f	f	f	f	f	f	f	

Beispiele:
o_4 entspricht der *Negation*, o_9 entspricht der *Disjunktion*.

Satz (1.7): Alle 16 Junktoren lassen sich mit den elementaren Junktoren Negation $\neg$, Konjunktion $\wedge$ und Disjunktion $\vee$ darstellen. D.h. es gibt Aussageformen $w_i(A, B)$, welche nur diese Verknüpfungen verwenden, so dass

$$Ao_iB \;\Leftrightarrow\; w_i(A, B), \quad i = 1, \ldots, 16$$

Beweis:

$$
\begin{array}{lcl}
A \ o_1 \ B & \Leftrightarrow & A \vee (\neg A) \\
A \ o_2 \ B & \Leftrightarrow & \neg(A \wedge B) \\
A \ o_3 \ B & \Leftrightarrow & B \vee (\neg A) \\
A \ o_4 \ B & \Leftrightarrow & \neg A \\
A \ o_5 \ B & \Leftrightarrow & A \vee (\neg B) \\
A \ o_6 \ B & \Leftrightarrow & \neg B \\
A \ o_7 \ B & \Leftrightarrow & (A \wedge B) \vee ((\neg A) \wedge (\neg B)) \\
A \ o_8 \ B & \Leftrightarrow & \neg(A \vee B) \\
A \ o_9 \ B & \Leftrightarrow & A \vee B \\
A \ o_{10} \ B & \Leftrightarrow & (A \wedge (\neg B)) \vee (B \wedge (\neg A)) \\
A \ o_{11} \ B & \Leftrightarrow & B \\
A \ o_{12} \ B & \Leftrightarrow & (\neg A) \wedge B \\
A \ o_{13} \ B & \Leftrightarrow & A \\
A \ o_{14} \ B & \Leftrightarrow & A \wedge (\neg B) \\
A \ o_{15} \ B & \Leftrightarrow & A \wedge B \\
A \ o_{16} \ B & \Leftrightarrow & A \wedge (\neg A) \qquad \square
\end{array}
$$

Definition (1.8):

NAND Verknüpfung: $A|B \quad :\Leftrightarrow \quad \neg(A \wedge B)$
NOR Verknüpfung: $A \nabla B \quad :\Leftrightarrow \quad \neg(A \vee B)$
Die NAND-Verknüpfung heißt auch *Sheffer-Operator*, die NOR-Verknüpfung auch *Pierce-Operator*.

Satz (1.9): Alle 16 Junktoren lassen sich mit der NAND-Verknüpfung darstellen. Analoges gilt für die NOR-Verknpfung.
Insbesondere bedeutet dies, dass sich *jede* Verknüpfung zweier Aussagen allein als Komposition von NAND-Verknüpfungen (oder NOR-Verknüpfungen) dargestellt lässt.

Beweis:

$$\begin{aligned} \neg A &\Leftrightarrow A|A \\ A \wedge B &\Leftrightarrow (A|B)|(A|B) \\ A \vee B &\Leftrightarrow (A|A)|(B|B) \qquad \square \end{aligned}$$

Beispiel (1.10): $A \circ_7 B \;\Leftrightarrow\; (A \wedge B) \vee ((\neg A) \wedge (\neg B)) \;\Leftrightarrow$

$((A|B)|(A|B)|(A|B)|(A|B))|(((A|A)|(B|B))|((A|A)|(B|B))|((A|A)|(B|B))|((A|A)|(B|B$

Definition (1.11): Aussageformen, in denen die Leerstellen Aussagevariablen sind, heißen *Formeln der Aussagenlogik*. Formeln heißen *erfüllbar*, falls die Variablen so durch Aussagen ersetzt werden können, dass eine wahre Aussage entsteht.

Beispiel: $A \wedge (\neg A)$ ist nicht erfüllbar.

Definition (1.12): Eine Formel heißt *allgemeingültig* oder auch eine *Tautologie*, falls bei *jeder* Ersetzung der Leerstellen durch Aussagen eine wahre Aussage entsteht.

Beispiel: $A \vee (\neg A)$ ist eine Tautologie.

Wichtige Tautologien (1.13):

a.)	$A \vee \neg A$	Ausgeschlossenes Drittes
b.)	$\neg(A \wedge \neg A)$	Satz vom Widerspruch
c.)	$\neg\neg A \Leftrightarrow A$	Doppelte Verneinung
d.)	$\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$	Regel von de Morgan I
e.)	$\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$	Regel von de Morgan II
f.)	$(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$	Kontraposition
g.)	$(A \Rightarrow B) \wedge A \Rightarrow B$	modus ponens
h.)	$(A \Rightarrow B) \wedge \neg B \Rightarrow \neg A$	modus tollens
i.)	$(A \Rightarrow B) \Leftrightarrow (B \vee \neg A)$	
j.)	$(A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow (A \Rightarrow C)$	modus barbara
k.)	$A \wedge (B \wedge C) \Leftrightarrow (A \wedge B) \wedge C$	Assoziativgesetz I
l.)	$A \vee (B \vee C) \Leftrightarrow (A \vee B) \vee C$	Assoziativgesetz II
m.)	$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$	Distributivgesetz I
n.)	$A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$	Distributivgesetz II

Klammerregeln: Es wird vereinbart: Junktoren niedrigeren *Rangs* werden zuerst ausgeführt. Bei gleichem Rang wird von links nach rechts abgearbeitet.

Junktor	Rang
$\Leftrightarrow$	5
$\Rightarrow$	4
$\vee$	3
$\wedge$	2
$\neg$	1

Beispiel:

mit Klammerung	ohne Klammerung
$(\neg(\neg(A \wedge C))) \vee (\neg A)$	$\neg\neg(A \wedge C) \vee \neg A$
$(A \vee (\neg B)) \wedge (C \wedge (\neg A))$	$(A \vee \neg B) \wedge (C \wedge \neg A)$
$((A \vee (\neg B)) \wedge C) \wedge (\neg A)$	$(A \vee \neg B) \wedge C \wedge \neg A$
$(\neg A) \Rightarrow (B \Rightarrow (\neg(A \vee C)))$	$\neg A \Rightarrow (B \Rightarrow \neg(A \vee C))$

Nachweis von Tautologien:

- *Semantisches Verfahren.* Man stellt die Wahrheitswertetafel auf und belegt die auftretenden Aussagevariablen mit allen möglichen Kombinationen von Wahrheitswerten.

- *Syntaktisches Verfahren.* Man versucht, die Formel, die man als Tautologie nachweisen will, durch Anwendung bekannter Tautologien, vgl. (1.13), direkt umzuformen.

Beispiel: Zeige: $\neg p \Rightarrow (p \Rightarrow q)$ ist eine Tautologie.

$$\begin{aligned} \neg p \Rightarrow (p \Rightarrow q) \quad &\Leftrightarrow \quad [(p \Rightarrow q) \vee \neg\neg p] \\ &\Leftrightarrow \quad [(q \vee \neg p) \vee p] \\ &\Leftrightarrow \quad [q \vee (\neg p \vee p)] \end{aligned}$$

Erläuterung: Es wird der Reihe nach angewendet (1.13) i), i), c) und l). Da $(\neg p \vee p)$ nach (1.13) a) stets wahr ist, ist auch die letzte Formel eine Tautologie! $\square$

Aussagenkalkül.

Betrachtet man nur Aussagen und Aussagenverknüpfungen mit den obigen Junktoren, so erhält man den *Aussagenkalkül*. Genauer besteht der Aussagenkalkül aus *Axiomen*, das sind grundlegende Tautologien und Regeln, wie man durch Umformung aus diesen neue Tautologien gewinnt. Es gilt der

Vollständigkeitssatz des Aussagenkalküls.

Jede korrekte Formel (Tautologie) ist mit den Regeln des Aussagenkalküls ableitbar.

Für die Darstellung der meisten mathematischen Sachverhalte reichen jedoch die bisherigen Sprachelemente nicht aus!

Quantoren.

In mathematischer Sprechweise werden die Quantoren folgendermassen definiert

- Allquantor oder Generalisator: $\forall\, x \in \Omega \;:\; A(x)$

“Für alle x aus der Menge/Klasse Ω ist die Aussage $A(x)$ wahr.”

- Existenzquantor oder Partikularisator: $\exists\, x \in \Omega \;:\; A(x)$

“Es gibt (mindestens) ein x in Ω, so dass $A(x)$ wahr ist.”

- Existenz und Eindeutigkeit: $\exists_1\, x \in \Omega \;:\; A(x)$

“Es gibt genau ein x in Ω, so dass $A(x)$ wahr ist.”

Man beachte: "$\forall\, x \in \Omega \ : \ A(x)$" oder "$\exists\, y \in \Omega \ : \ A(y)$" sind *Aussagen*. Die Variablen x, y werden durch die Quantoren gebunden. Insbesondere sind die Aussagen $\forall\, x \in \Omega \ : \ A(x)$ und $\forall\, z \in \Omega \ : \ A(z)$ gleichbedeutend!

Beispiele:

$\forall\, x \in \mathbb{R} \ : \ x = 3$ ist falsch.

$\exists\, x \in \mathbb{R} \ : \ x = 3$ ist wahr.

$\exists_1\, x \in \mathbb{R} \ : \ x = 3$ ist wahr.

$\forall\, z \in \mathbb{R} \ : \ z + 1 \in \mathbb{R}$ ist wahr.

$\forall\, y \in \mathbb{R} \ : \ y \geq |y|$ ist falsch.

Verneinungsregel: $\neg\,(\forall\, x \in \Omega : \ A(x)) \ \Leftrightarrow \ \exists\, x \in \Omega : \ (\neg A(x))$

Erweitert man den Aussagenkalkül durch die Sprachelemente “Quantoren”, “Subjekte” und “Prädikatsvariable” (Eigenschaften), so erhält man den *Prädikatenkalkül ersten Stufe*. Auch hier sind genau die korrekten Formeln aus dem Axiomensystem ableitbar. Das ist der Inhalt des **Vollständigkeitssatzes von Kurt Gödel (1930)**.

Eine weitere Erweiterung der Sprachelemente, bei der auch Prädikate von Prädikaten und Quantoren über Prädikatsvariblen zugelassen sind, führt zu einem *Prädikatenkalkülen höherer Stufe*. Dieser ist allerdings stets unvollständig, **Unvollständigkeitssatz von Gödel (1931)**. Mehr noch, es gibt keinen (endlichen) Algorithmus, mit dem man entscheiden kann, ob eine vorgegebene Formel allgemeingültig ist, **Unentscheidbarkeitssatz von Alan Turing und Alonzo Church (1936)**.

Kurt Gödel
(1906-1978)

Alan Turing
(1912-1954)