Fachhochschule Nordwestschweiz
Hochschule für Wirtschaft

Boolesche Algebra

Ein algebraischer Ansatz - konsequent verfolgt

Studie

Autor: Helmut Vetter
Ort, Datum: Arlesheim, 02.09.2014

Diese Arbeit wurde mit TexLive erstellt.

Boolesche Algebra
Ein algebraischer Ansatz - konsequent verfolgt

Autor
Vetter, Helmut
Schillerweg 2
CH-4144 Arlesheim
061 599 51 09
helmut.vetter@fhnw.ch

Auftraggeberschaft
Fachhochschule für Wirtschaft
Tanner, Christian

Arlesheim, September 2014

Ehrenwörtliche Erklärung
Ich versichere, dass ich die vorliegende Arbeit selbstständig und ohne Benutzung anderer als der im Literaturverzeichnis angegebenen Quellen und Hilfsmittel angefertigt habe.

Die wörtlich oder inhaltlich den im Literaturverzeichnis aufgeführten Quellen und Hilfsmitteln entnommenen Stellen sind in der Arbeit als Zitat bzw. Paraphrase kenntlich gemacht.

Diese Arbeit ist noch nicht veröffentlicht worden. Sie ist somit weder anderen Interessenten zugänglich gemacht noch einer anderen Prüfungsbehörde vorgelegt worden.

Arlesheim, 02.09.2014

Helmut Vetter

Management Summary

Steht das Symbol x für "weisse Dinge", y für "Schafe", so bedeutet xy weisse Schafe. $y - xy$ sind die Schafe, die nicht weisse Schafe sind. Dies ist dasselbe wie $y(1 - x)$ die Schafe, die nicht weiss sind.

Aufgrund solcher Formalisierung hat George Boole 1854 gezeigt, dass man in der Logik - ähnlich wie mit Zahlen - rechnen kann.

Ausgehend von einem Axiomensystem sollen in dieser Arbeit die Rechengesetze der "Booleschen Algebra" hergeleitet werden.

Im Anhang wird gezeigt dass die Aussagenlogik und die Mengenlehre diesem Axiomensystem genügen und folgerichtig die Rechengesetze der "Booleschen Algebra" für diese gelten.

Inhaltsverzeichnis

1 Problemstellung

George Boole zeigte vor rund 160 Jahren, dass man mit Aussagen - ähnlich wie mit Zahlen - rechnen kann.
Hier soll dies in kompakter Form dargestellt werden. Der axiomatische Aufbau folgt dem Buch von G. Whitesitt "Boolesche Algebra und ihre Anwendungen".
Aufgebaut wird das System in den Kapiteln 4 und 5 auf der Konjunktion (und, hier: $\cdot$) der Disjunktion (oder, hier: $+$) und der Negation (nicht, hier: $'$). Die Konstante 1 steht für die Tautologie, 0 für die Kontradiktion.
In Anhang (Kapitel 8) wird die Gültigkeit der Axiome (Definition 1) für Aussagenlogik und Mengenlehre gezeigt.
In Kapitel 6 erfolgt die Definition weiterer zweistelliger Operationen und eine Übersicht über die verwendeten Symbole in der Aussagenlogik, der Mengenlehre und der Informatik.
In Kapitel 7 wird der Anschluss an die Theorie der Ringe hergestellt.

2 Aussagenlogik

Eine Aussage ist ein sprachliches Gebilde, von dem objektiv festgestellt werden kann, ob es wahr (w bzw. 1) oder falsch (f bzw. 0) ist. Man spricht von der Eigenschaft der "Zweiwertigkeit".
Die Aussagenlogik definiert wie sich die Wahrheitswerte bei der Verknüpfung zweier Aussagen mittels den Partikeln "und" (and bzw. $\wedge$), "oder" (or bzw. $\vee$) und "nicht" (not bzw. $\neg$) zu einer neuen Aussage verhalten.

Formal besteht somit die Aussagenlogik
1) aus der Menge $\{0,1\}$
mit auf ihr definierten Operationen
2a) und $\wedge : \{0,1\}^2 \to \{0,1\}$, via $(x,y) \mapsto x \wedge y$
2b) oder $\vee : \{0,1\}^2 \to \{0,1\}$, via $(x,y) \mapsto x \vee y$
2c) nicht $\neg : \{0,1\} \to \{0,1\}$, via $x \mapsto \neg x$

Die Wirkungsweise der Operationen können (wie beim 1x1 der Zahlen) in Wertetabellen dargestellt werden...

oder ($\vee$)		
a	b	$a \vee b$
0	0	0
0	1	1
1	0	1
1	1	1

und ($\wedge$)		
a	b	$a \wedge b$
0	0	0
0	1	0
1	0	0
1	1	1

nicht ($\neg$)	
a	$\neg a$
0	1
1	0

Damit ist alles definiert!

Wie in der Standardalgebra können Terme in äquivalente (=gleichwertige) Terme umformt werden (Beispiel Standardalgebra: $x \cdot (1+y) = x + xy$). In der Algebra der Aussagenlogik gilt beispielsweise die Identität $x \wedge x = x$

Wie in der Standardalgebra wird man in der Algebra der Aussagenlogik eine Reihe von Grundgesetzen (=Axiome) deklarieren, auf deren Basis man die Umwandlung von Termen in äquivalente Terme nachweisen kann.

An unserm Beispiel aus der Standardalgebra sieht die Ableitung der Äquivalenz der beiden Terme $x(1+y)$ und $x+xy$ wie folgt aus:
Verwendet werden das Distributivgesetz (D) $a(b+c) = ab + ac$; und die Eigenschaft der Zahl 1 als neutrales Element der Multiplikation (N) $a \cdot 1 = a$:

$x(1+y) \overset{\text{D}}{=} x1 + xy \overset{\text{N}}{=} x + xy$ qed.

Die formale Definition einer Boolschen Algebra erfolgt in Kapitel 5. Im Anhang (Kapitel 8) erfolgt der Nachweis, dass die Algebra der Aussagenlogik die Axiome einer Boolschen Algebra erfüllt, also eine Boolsche Algebra ist.

3 Mengenlehre

Die Mengenlehre ist eng verknüpft mit der Aussagenlogik.

Formal ist der Zusammenhang folgender...
Gegeben sei eine Grundmenge Ω.
Grundlegend ist die Bijektion $f : \operatorname{Pot}\Omega \to \{0,1\}^\Omega$, die jeder Teilmenge von Ω den Vektor in $\{0,1\}^\Omega$ zuordnet, der genau an den Stellen x eine 1 hat, für die gilt $x \in \Omega$.
Beispiel: $\Omega := \{1,2,3\}$. Für die Teilmenge $\{1,3\}$ ist $f(\{1,3\}) = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$; für die Teilmenge $\{\}$ ist $f(\{\}) = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$; für die Teilmenge $\{1,2,3\}$ ist $f(\{1,2,3\}) = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ usw.

Die Operationen der Aussagenlogik lassen sich durch komponentenweises Anwenden von der Menge $\{0,1\}$ auf die Menge $\{0,1\}^\Omega$ übertragen.
Beispiel: $\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \wedge \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \vee \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$, $\neg \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$.
Auf diese Weise überträgt sich die Eigenschaft eine Boolsche Algebra zu sein, von der Aussagenlogik auf jedes $\{0,1\}^\Omega$ und wie nachfolgend gezeigt auf die Mengenalgebra der Teilmengen von Ω.

Definition der Operationen zwischen Teilmengen von Ω via die Bijektion $f : \operatorname{Pot}\Omega \to \{0,1\}^\Omega$:
Schnittmenge: $A \cap B = f^{-1}(f(A) \wedge f(B))$
Vereinigungsmenge: $A \cup B = f^{-1}(f(A) \vee f(B))$
Komplement: $\overline{A} = f^{-1}(\neg f(A))$

4 Formale Definition einer Booleschen Algebra

Gegeben ist eine Menge R und auf dieser zwei zweistellige Operationen s bzw. "$+$" und m bzw. "$\cdot$":
$s : (a,b) \mapsto s(a,b) =: a + b$ und $m : (a,b) \mapsto m(a,b) =: a \cdot b =: ab$
zudem eine einstellige Operation i bzw. "$'$"
$i : a \mapsto i(a) =: a'$
und zwei Konstanten $0 \neq 1$.
Man spricht kurz von der Struktur $(R, \cdot, +, ', 0, 1)$

Konventionen: Statt $m(a,b)$ schreibt man $a \cdot b$ oder kürzer ab. Statt $s(a,b)$ schreibt man $a + b$. Statt $i(a)$ schreibt man a'.
Diese Kurzschriften machen eine Rangfolge der Operationen sinnvoll, um Klammern zu sparen:
"$'$" hat den Vorrang vor "$\cdot$" und "$+$" beim Zugriff auf ein Argument.
"$\cdot$" hat den Vorrang vor "$+$" beim Zugriff auf ein Argument.
Greift von beiden Seiten dieselbe Operation auf ein Argument zu, so hat die weiter links stehende Operation den Vorrang vor der weiter rechts stehenden.

Beispiel Im Term $a + b \cdot c'$ hat somit
beim Zugriff auf c die Operation "$'$" den Vorrang vor der Operation "$\cdot$";
und beim Zugriff auf b die Operation "$\cdot$" den Vorrang vor der Operation "$+$".

Dies liesse sich explizit mit Klammern schreiben als $a + (b \cdot (c'))$

Definition 1 Boolesche Algebra $(R, +, \cdot, ', 0, 1)$
Es sollen folgende Axiome K.1 bis I.2 gelten:

	1	2
K	$a + b = b + a$	$ab = ba$
D	$a + bc = (a + b)(a + c)$	$a(b + c) = ab + ac$
N	$a + 0 = a$	$a1 = a$
I	$a + a' = 1$	$aa' = 0$

Bemerkung Aussagenlogik
Via Wahrheitstafeln lässt sich zeigen, dass diese Axiome (Definition 1) für die Aussagenlogik gelten, wenn man $+$ als $\vee$, $\cdot$ als $\wedge$, $'$ als $\neg$ interpretiert. Siehe Anhang im Kapitel 8.

Bemerkung Mengenlehre
Via Kapitel 3 oder via Venndiagramme gemäss anhang im Kapitel 8 lässt sich zeigen, dass diese Axiome (Definition 1) für die Mengenlehre gelten, wenn man $+$ als Vereinigung, $\cdot$ als Schnitt, $'$ als Komplement interpretiert.

5 Identitäten in einer Booleschen Algebra

Es werden jetzt eine Reihe von Identitäten aus den Axiomen (Definition 1) hergeleitet. Die Gesetze treten jeweils paarweise auf, was sich schlussendlich im Dualitätsprinzip (Satz 12) zusammenfassen lässt.

Satz 1

	1	2
S1	$a + a = a$	$aa = a$

Beweis 1

S1.1: $a \overset{\text{N.1}}{=} a + 0 \overset{\text{I.2}}{=} a + aa' \overset{\text{D.1}}{=} (a + a)(a + a') \overset{\text{I.1}}{=} (a + a)1 \overset{\text{N.2}}{=} a + a$ qed.

S1.2: $a \overset{\text{N.2}}{=} a1 \overset{\text{I.1}}{=} a(a + a') \overset{\text{D.2}}{=} aa + aa' \overset{\text{I.2}}{=} aa + 0 \overset{\text{N.1}}{=} aa$ qed.

Satz 2

	1	2
S2	$a + 1 = 1$	$a0 = 0$

Beweis 2

S2.1: $1 \overset{\text{I.1}}{=} a + a' \overset{\text{N.2}}{=} a + a'1 \overset{\text{D.1}}{=} (a + a')(a + 1) \overset{\text{I.1}}{=} 1(a + 1) \overset{\text{K.2}}{=} (a + 1)1 \overset{\text{N.2}}{=} a + 1$ qed.

S2.2: $0 \overset{\text{I.2}}{=} aa' \overset{\text{N.1}}{=} a(a' + 0) \overset{\text{D.2}}{=} aa' + a0 \overset{\text{I.2}}{=} 0 + a0 \overset{\text{K.1}}{=} a0 + 0 \overset{\text{N.1}}{=} a0$ qed.

Satz 3

	1	2
S3	$a + ax = a$	$a(a + x) = a$

Beweis 3

S3.1: $a \overset{\text{N.2}}{=} a1 \overset{\text{S2.1}}{=} a(x + 1) \overset{\text{D.2}}{=} ax + a1 \overset{\text{N.2}}{=} ax + a \overset{\text{K.1}}{=} a + ax$ qed.

S3.2: $a \overset{\text{N.1}}{=} a + 0 \overset{\text{S2.2}}{=} a + x0 \overset{\text{D.1}}{=} (a + x)(a + 0) \overset{\text{N.1}}{=} (a + x)a \overset{\text{K.2}}{=} a(a + x)$ qed.

Satz 4

S4	Gilt $a+x=1$ und $ax=0$, dann ist $x=a'$

Beweis 4

S4: $a' \overset{N.2}{=} a'1 \overset{Vor}{=} a'(a+x) \overset{D.2}{=} a'a+a'x \overset{K.2}{=} aa'+a'x \overset{I.2}{=} 0+a'x \overset{Vor}{=} ax+a'x \overset{K.2}{=} xa+xa' \overset{D.2}{=} x(a+a') \overset{I.1}{=} x1 \overset{N.2}{=} x$ qed.

Satz 5

	1	2
S5	$ax+a'x=x$	(a+x)(a'+x)=x

Beweis 5

S5.1: $x \overset{N.2}{=} x1 \overset{I.1}{=} x(a+a') \overset{D.2}{=} xa+xa' \overset{K.2}{=} ax+a'x$ qed.

S5.2: $x \overset{N.1}{=} x+0 \overset{I.2}{=} x+aa' \overset{D.1}{=} (x+a)(x+a') \overset{K.1}{=} (a+x)(a'+x)$ qed.

Satz 6 Assoziativgesetze

	1	2
S6=A	$a+(b+c)=(a+b)+c$	$a(bc)=(ab)c$

Beweis 6

H1: $a((a+b)+c)=a(a+(b+c))$

Beweis H1: $a((a+b)+c) \overset{D.2}{=} a(a+b)+ac \overset{S3.2}{=} a+ac \overset{S3.1}{=} a \overset{N.1}{=} a+0 \overset{S2.2}{=} a+((b+c)0) \overset{D.1}{=} (a+(b+c))(a+0) \overset{N.1}{=} (a+(b+c))a \overset{K.2}{=} a(a+(b+c))$ qed.

H2: $a'((a+b)+c)=a'(a+(b+c))$

Beweis H2: $a'((a+b)+c) \overset{D.2}{=} a'(a+b)+a'c \overset{D.2}{=} (a'a+a'b)+a'c \overset{K.2}{=} (aa'+a'b)+a'c \overset{I.2}{=} (0+a'b)+a'c \overset{K.1}{=} (a'b+0)+a'c \overset{N.1}{=} a'b+a'c \overset{D.2}{=} a'(b+c) \overset{N.1}{=} a'(b+c)+0 \overset{K.1}{=} 0+a'(b+c) \overset{I.2}{=} aa'+a'(b+c) \overset{K.2}{=} a'a+a'(b+c) \overset{D.2}{=} a'(a+(b+c))$ qed.

S6.1: $a+(b+c) \overset{S5.1}{=} a(a+(b+c))+a'(a+(b+c)) \overset{H.1/2}{=} a((a+b)+c)+a'((a+b)+c)) \overset{S5.1}{=} (a+b)+c$ qed.

H3: $a+(ab)c=a+a(bc)$

Beweis H3: $a+(ab)c \overset{D.1}{=} (a+ab)(a+c) \overset{S3.1}{=} a(a+c) \overset{S3.2}{=} a \overset{N.2}{=} a1 \overset{S2.1}{=} a(bc+1) \overset{K.1}{=} a(1+bc) \overset{D.2}{=} a1+a(bc) \overset{N.2}{=} a+a(bc)$ qed.

H4: $a'+(ab)c=a'+a(bc)$

Beweis H4: $a'+(ab)c \overset{D.1}{=} (a'+ab)(a'+c) \overset{D.1}{=} ((a'+a)(a'+b))(a'+c) \overset{K.1}{=} ((a+a')(a'+b))(a'+c) \overset{I.1}{=} (1(a'+b))(a'+c) \overset{K.2}{=} ((a'+b)1)(a'+c) \overset{N.2}{=} (a'+b)(a'+c) \overset{D.1}{=} a'+bc \overset{N.2}{=} (a'+bc)1 \overset{K.2}{=} 1(a'+bc) \overset{I.1}{=} (a+a')(a'+bc) \overset{K.1}{=} (a'+a)(a'+bc) \overset{D.1}{=} a'+a(bc)$ qed.

S6.2: $a(bc) \overset{S5.2}{=} (a+a(bc))(a'+a(bc)) \overset{H.3/4}{=} (a+(ab)c))(a'+(ab)c)) \overset{S5.2}{=} (ab)c$ qed.

Satz 7

	1	2
S7	$0'=1$	$1'=0$

Beweis 7

S7.1: $0+1 \overset{K.1}{=} 1+0 \overset{N.1}{=} 1$ und $01 \overset{N.2}{=} 0 \overset{S4}{\Rightarrow} 1=0'$ qed.

S7.2: $1+0 \overset{N.1}{=} 1$ und $10 \overset{K.2}{=} 01 \overset{N.2}{=} 0 \overset{S4}{\Rightarrow} 0=1'$ qed.

Satz 8

S8	$a'' = a$

Beweis 8

S8: $a' + a \overset{K.1}{=} a + a' \overset{I.1}{=} 1$ und $a'a \overset{K.2}{=} aa' \overset{I.2}{=} 0 \overset{S4}{\Rightarrow} a = a''$ qed.

Satz 9 deMorgan's Gesetze

	1	2
S9	$(a+b)' = a'b'$	$(ab)' = a' + b'$

Beweis 9

S9.1: $(a+b) + a'b' \overset{A.1}{=} a + (b + a'b') \overset{D.1}{=} a + (b+a')(b+b') \overset{I.1}{=} a + (b+a')1 \overset{N.2}{=} a + (b+a') \overset{K.1}{=}$
$a + (a'+b) \overset{A.1}{=} (a+a') + b \overset{I.1}{=} 1 + b \overset{K.1}{=} b + 1 \overset{S2.1}{=} 1$
und $(a+b)(a'b') \overset{K.2}{=} (a'b')(a+b) \overset{D.2}{=} (a'b')a + (a'b')b \overset{K.2}{=} (b'a')a + (a'b')b \overset{A.2}{=} b'(a'a) + a'(b'b) \overset{K.2}{=}$
$b'(aa') + a'(bb') \overset{I.2}{=} b'0 + a'0 \overset{S2.2}{=} 0 + 0 \overset{N.1}{=} 0$
$\overset{S4}{\Rightarrow} a'b' = (a+b)'$ qed.

S9.2: $ab + (a'+b') \overset{A.1}{=} (ab+a') + b' \overset{K.1}{=} (a'+ab) + b' \overset{D.1}{=} (a'+a)(a'+b) + b' \overset{K.1}{=} (a+a')(a'+b) + b' \overset{I.1}{=} 1(a'+b) + b' \overset{K.2}{=}$
$(a'+b)1 + b' \overset{N.2}{=} (a'+b) + b' \overset{A.1}{=} a' + (b+b') \overset{I.1}{=} a' + 1 \overset{S2.1}{=} 1$
und $(ab)(a'+b') \overset{D.2}{=} (ab)a' + (ab)b' \overset{K.2}{=} (ba)a' + (ab)b' \overset{A.2}{=} b(aa') + a(bb') \overset{I.2}{=} b0 + a0 \overset{S2.2}{=} 0 + 0 \overset{N.1}{=} 0$
$\overset{S4}{\Rightarrow} a' + b' = (ab)'$ qed.

Satz 10

S10.1	Das Resultat einer mehrgliedrigen Summe ist unabhängig von der Reihenfolge der Ausführung der einzelnen Additionen
S10.2	Das Resultat eines mehrgliedrigen Produkts ist unabhängig von der Reihenfolge der Ausführung der einzelnen Multiplikationen

Beweis 10

S10.1: Beweis durch Induktion nach der Anzahl n der Summanden der Summe.
Verankerung: In den Fällen $n = 1$ und $n = 2$ ist nichts zu beweisen.
V=Voraussetzung: Der Satz sei für $n \geq 2$ Summanden bewiesen.
Jetzt sei eine Summe mit $n + 1 \geq 3$ Summanden gegeben, mit vorgegebener Ausführreihenfolge der n Additionen.
Die letzte Addition $S_1 + S_2 \overset{V}{=} S_1 + (S_2' + a_{n+1}) \overset{A.1}{=} (S_1 + S_2') + a_{n+1} \overset{V}{=} (\ldots((a_1 + a_2) + a_3)\ldots + a_n) + a_{n+1}$
liefert also immer dasselbe. qed.

S10.2: Beweis durch Induktion nach der Anzahl n der Faktoren des Produkts.
Verankerung: In den Fällen $n = 1$ und $n = 2$ ist nichts zu beweisen.
V=Voraussetzung: Der Satz sei für $n \geq 2$ Faktoren bewiesen.
Jetzt sei ein Produkt mit $n + 1 \geq 3$ Faktoren gegeben, mit vorgegebener Ausführreihenfolge der n Multiplikationen.
Das letzte Produkt $P_1P_2 \overset{V}{=} P_1(P_2'a_{n+1}) \overset{A.2}{=} (P_1P_2')a_{n+1} \overset{V}{=} (\ldots((a_1a_2)a_3)\ldots a_n)a_{n+1}$
liefert also immer dasselbe. qed.

Bemerkung: Die Summe S_2' bzw. das Produkt P_2' können dabei auch leer sein. Beachte die Definitionen Leere Summe $:= 0$, Leeres Produkt $:= 1$.

Satz 11

S11.1	Das Resultat einer mehrgliedrigen Summe ist unabhängig von der Reihenfolge der Summanden
S11.2	Das Resultat eines mehrgliedrigen Produkts ist unabhängig von der Reihenfolge der Faktoren

Beweis 11

S11.1: Beweis durch Induktion nach der Anzahl n der Summanden der Summe.

Verankerung: Im Fall $n = 1$ ist nichts zu beweisen.

V=Voraussetzung: Der Satz sei für $n \geq 1$ Summanden bewiesen.

Jetzt sei eine Summe mit $n + 1 \geq 2$ Summanden in beliebiger Reihenfolge gegeben.

$S \overset{\text{S10.1}}{=} S_1 + (a_{n+1} + S_2) \overset{\text{K.1}}{=} S_1 + (S_2 + a_{n+1}) \overset{\text{A.1}}{=} (S_1 + S_2) + a_{n+1} \overset{\text{V}}{=} (\ldots((a_1 + a_2) + a_3) \ldots + a_n) + a_{n+1}$

liefert also immer dasselbe. qed.

S11.2: Beweis durch Induktion nach der Anzahl n der Faktoren des Produkts.

Verankerung: Im Fall $n = 1$ ist nichts zu beweisen.

V=Voraussetzung: Der Satz sei für $n \geq 1$ Faktoren bewiesen.

Jetzt sei ein Produkt mit $n + 1 \geq 2$ Faktoren in beliebiger Reihenfolge gegeben.

$P \overset{\text{S10.2}}{=} P_1(a_{n+1}P_2) \overset{\text{K.2}}{=} P_1(P_2a_{n+1}) \overset{\text{A.2}}{=} (P_1P_2)a_{n+1} \overset{\text{V}}{=} (\ldots((a_1a_2)a_3) \ldots a_n)a_{n+1}$

liefert also immer dasselbe. qed.

Bemerkung: Die Summen S_1 oder S_2 bzw. die Produkte P_1 oder P_2 können dabei auch leer sein. Beachte die Definitionen Leere Summe $:= 0$, Leeres Produkt $:= 1$. Satz 12 Dualitätsprinzip

Die Struktur $(R, +, \cdot, ', 0, 1)$ geht via $j : a \mapsto a'$ isomorph über in die Struktur $(R, \cdot, +, ', 1, 0)$

Beweis 12

Dies folgt aus den Aussagen:

- j ist Bijektion

  j ist injektiv: Es sei $j(a) = j(b)$, dann $a \overset{\text{S8}}{=} a'' \overset{\text{Def}}{=} (j(a))' \overset{\text{Vor}}{=} (j(b))' \overset{\text{Def}}{=} b'' \overset{\text{S8}}{=} b$ qed.

  j ist surjektiv: Es ist $a \overset{\text{S8}}{=} a'' \overset{\text{Def}}{=} j(a')$ qed.
- $j(a + b) \overset{\text{Def}}{=} (a + b)' \overset{\text{S9.1}}{=} a'b' \overset{\text{Def}}{=} j(a)j(b)$ qed.
- $j(ab) \overset{\text{Def}}{=} (ab)' \overset{\text{S9.2}}{=} a' + b' \overset{\text{Def}}{=} j(a) + j(b)$ qed.
- $j(a') \overset{\text{Def}}{=} a'' \overset{\text{Def}}{=} j(a)'$ qed.
- $j(0) \overset{\text{Def}}{=} 0' \overset{\text{S7.1}}{=} 1$ qed.
- $j(1) \overset{\text{Def}}{=} 1' \overset{\text{S7.2}}{=} 0$ qed.

6 Weitere Operationen

Definitionen

1	$a \rightarrow b := a' + b$
2	$a \leftrightarrow b := ab + a'b'$
3	$a \oplus b := ab' + a'b$
4	$a \dagger b := (ab)' = a' + b'$

Namen und Symbol in Logik und Informatik (Programmiersprache "C") und Mengenlehre:

Boolesche Algebra	Logik	Informatik	Mengenlehre
$a \cdot b$	$a \wedge b$ [Konjunktion, AND, und]	$a\&b$	$A \cap B$ [Schnittmenge]
$a + b$	$a \vee b$ [Disjunktion, OR, oder]	$a\|b$	$A \cup B$ [Vereinigungsmenge]
a'	$\neg a$ [Negation, NOT, nicht]	$!a$	$\overline{A}$ [Komplement]
$a \oplus b$	$a \oplus b$ [XOR, entweder oder]	$!(a == b)$	$A \Delta B$ [Symmetrische Differenz]
$a \dagger b$	$a \dagger b$ [NAND, nicht beide]	$!(a\&b)$	$\overline{A \cap B} = \overline{A} \cup \overline{B}$
$a \rightarrow b$	$a \rightarrow b$ [Implikation, IF THEN, wenn dann]	$(a <= b)$	$\overline{A} \cup B$; Resultat ist Ω, genau dann wenn $A \subseteq B$ [Teilmenge]
$a \leftrightarrow b$	$a \leftrightarrow b$ [Äquivalenz, genau dann wenn]	$(a == b)$	$(A \cap B) \cup (\overline{A} \cap \overline{B})$, Resultat ist Ω, genau dann wenn $A = B$ [Gleichheit]

Zu den letzten beiden Punkte in der Spalte Mengenlehre beachte man auch die Ausführungen in Kapitel 3.

Satz 13

Alle Operationen einer Booleschen Algebra können durch die einzige Operation $\dagger$ ausgedrückt werden!

Beweis 13

1) $a \dagger a \overset{\text{Def}}{=} (aa)' \overset{\text{S1.2}}{=} a'$ qed.

2) $(a \dagger a) \dagger (b \dagger b) \overset{1)}{=} a' \dagger b' \overset{\text{Def}}{=} (a'b')' \overset{\text{S9.2}}{=} a'' + b'' \overset{\text{S8}}{=} a + b$ qed.

3) $(a \dagger b) \dagger (a \dagger b) \overset{\text{Def}}{=} (ab)' \dagger (ab)' \overset{\text{Def}}{=} ((ab)'(ab)')' \overset{\text{S1.2}}{=} (ab)'' \overset{\text{S8}}{=} ab$ qed.

7 Boolesche Ringe

Definition Ring

Ein Ring $(R, +, \cdot, n, 0, 1)$ ist eine Menge mit zwei zweistelligen Operationen $+$ und $\cdot$, einer einstelligen Operation n und zwei Konstanten $0 \neq 1$ die den folgenden Axiomen genügt.

- $(R, +, n, 0)$ ist abelsche Gruppe:
  RK.1 Kommutativgesetz: $a + b = b + a$
  RA.1 Assoziativgesetz: $a + (b + c) = (a + b) + c$
  RN.1 Neutrales Element 0: $a + 0 = a$
  RI.1 Inverses Element $n(a)$ zu a mit: $a + n(a) = 0$
- $(R, \cdot, 1)$ ist kommutativ und assoziativ mit Eins:
  RK.2 Kommutativgesetz: $a \cdot b = b \cdot a$
  RA.2 Assoziativgesetz: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
  RN.2 Neutrales Element 1: $a \cdot 1 = a$
- RD Distributivgesetz: $a \cdot (b + c) = a \cdot b + a \cdot c$

Bemerkung: Um die Notationen zu verkürzen schreibt man kurz ab statt $a \cdot b$; und um Klammern zu sparen, regelt man für den Zugriff der Operationen auf ein Element: $\cdot$ hat Vorrang vor $+$.
Beispiel: So bedeutet $a + bc$ in expliziter Form $a + (b \cdot c)$.

Satz 14

S14.1	In einem Ring ist das Resultat einer mehrgliedrigen Summe unabhängig von der Reihenfolge der Summanden
S14.2	In einem Ring ist das Resultat eines mehrgliedrigen Podukts unabhängig von der Reihenfolge der Fakoren

Beweis 14

Wie bei Satz 10 und 11. Verwendet wird lediglich das Assoziativ- und das Kommutativgesetz. qed.

Satz 15

In einem Ring gilt für jedes $a \in R$, dass $a0 = 0$

Beweis 15

$a0 + a0 \overset{\text{RD}}{=} a(0+0) \overset{\text{RN.1}}{=} a0$ addieren von $n(a0)$ auf beiden Seiten ergibt $a0 = 0$

Definition Vielfache

Für ein Element a des Ringes $(R, +, \cdot, n, 0, 1)$ und $x \in \mathbb{N}_0$ definiert man

$$xa := x \cdot a := \begin{cases} (x-1) \cdot a + a & \text{, für } x \geq 1 \\ 0 & \text{, für } x = 0 \end{cases}$$

$$a^x := \begin{cases} a^{x-1} \cdot a & \text{, für } x \geq 1 \\ 1 & \text{, für } x = 0 \end{cases}$$

Definition Boolescher Ring

Eine Boolescher Ring $(R, +, \cdot, n, 0, 1)$ ist ein Ring mit der zusätzlichen Eigenschaft

RB: $a^2 = a$ für jedes $a \in R$

Satz 16

Sei R ein Booleschen Ring. Dann gilt:	
1	für jedes $a \in R$ ist $2a = 0$
2	$n(a) = a$
3	jedes endlich erzeugte Ideal in R ist Hauptideal
4	für jedes maximale Ideal $m \subseteq R$ ist R/m isomorph zu $\mathbb{Z}/(2)$

Beweis 16

1) $a + 1 \overset{\text{RB}}{=} (a+1)^2 \overset{\text{Def}}{=} (a+1)(a+1) \overset{\text{RD}}{=} (a+1)a + (a+1)1 \overset{\text{RK.2}}{=} a(a+1) + (a+1)1 \overset{\text{RN.2}}{=} a(a+1) + (a+1) \overset{\text{RD}}{=}$
$(a^2 + a) + (a+1) \overset{\text{RB}}{=} (a+a) + (a+1) \overset{\text{S14.1}}{=} 3a + 1$ addiert man beidseitig $n(a) + n(1)$,
so erhält man $0 = 2a$ qed.

2) $n(a) \overset{\text{RN.1}}{=} n(a) + 0 \overset{1)}{=} n(a) + 2a \overset{\text{Def}}{=} n(a) + (a+a) \overset{\text{RA.1}}{=} (n(a) + a) + a \overset{\text{RK.1}}{=}$
$(a + n(a)) + a \overset{\text{RI.1}}{=} 0 + a \overset{\text{RK.1}}{=} a + 0 \overset{\text{RN.1}}{=} a$ qed.

3) Es reicht $(a, b) = (a) + (b) = (a + b + ab)$ zu zeigen. Dies erlaubt es, die Anzahl $n > 1$ der Erzeugenden eines Ideales um eins auf $n - 1$ zu reduzieren.

sicher ist $(a + b + ab) \subseteq (a, b)$.

$a(a + b + ab) \overset{\text{RD}}{=} a^2 + ab + a^2 b \overset{\text{RB}}{=} a + ab + ab \overset{\text{Def}}{=} a + 2(ab) \overset{1)}{=} a + 0 \overset{\text{RN.1}}{=} a$ zeigt $a \in (a + b + ab)$

$b(a + b + ab) \overset{\text{RD}}{=} ba + b^2 + bab \overset{\text{S14.2}}{=} ba + b^2 + b^2 a \overset{\text{RB}}{=} ba + b + ba \overset{\text{R14.1}}{=} b + 2(ba) \overset{1)}{=} b + 0 \overset{\text{RN.1}}{=} b$

zeigt $b \in (a + b + ab)$ qed.

4) $K := R/m$ ist ein Körper mit der Booleschen Eigenschaft! Sei $a \in K$, so

$0 \overset{1)}{=} 2a \overset{\text{Def}}{=} a + a \overset{1)}{=} a + a^2 = a(1 + a)$

Da ein Körper keine echten Nullteiler hat, ist $a = 0$ oder $1 + a = 0$ via beidseitiges Addieren von $n(1) \overset{2)}{=} 1$ folgt $a = 1$. Somit ist $a \in \{0, 1\}$ und da a beliebig in K war also $K = \{0, 1\}$. Jeder Körper mit 2 Elementen ist aber

isomorph zu $\mathbb{Z}/(2)$ qed.

Satz 17

Eine Boolesche Algebra $(R, +, \cdot, ', 0, 1)$ ist stets auch Boolescher Ring $(R, \oplus, \cdot, n, 0, 1)$.

Beweis 17

Definiere:

$a \oplus b := ab' + a'b$

Die Operation $\cdot$ ist in beiden Strukturen gleich definiert!

$n(a) := a$

Jetzt werden die Ringaxiome nachgewiesen:

RK.1: $a \oplus b \overset{\text{Def}}{=} ab' + a'b \overset{\text{K.1}}{=} a'b + ab' \overset{\text{K.2}}{=} ba' + b'a \overset{\text{Def}}{=} b \oplus a$ qed.

RA.1 Linke Seite: $a \oplus (b \oplus c) \overset{\text{Def}}{=} a \oplus (bc' + b'c) \overset{\text{Def}}{=} a(bc' + b'c)' + a'(bc' + b'c) \overset{\text{S9.1}}{=}$

$a((bc')'(b'c)') + a'(bc' + b'c) \overset{\text{S9.2}}{=} a((b' + c'')(b'' + c')) + a'(bc' + b'c) \overset{\text{S8}}{=} a((b' + c)(b + c')) + a'(bc' + b'c) \overset{\text{D.2}}{=}$

$a((b' + c)b + (b' + c)c') + a'bc' + a'b'c \overset{\text{K.2}}{=} a(b(b' + c) + c'(b' + c)) + a'bc' + a'b'c \overset{\text{D.2}}{=}$

$a((bb' + bc) + (c'b' + c'c)) + a'bc' + a'b'c \overset{\text{K.2}}{=} a((bb' + bc) + (b'c' + cc')) + a'bc' + a'b'c \overset{\text{I.2}}{=}$

$a((0 + bc) + (b'c' + 0)) + a'bc' + a'b'c \overset{\text{K.1}}{=} a((bc + 0) + (b'c' + 0)) + a'bc' + a'b'c \overset{\text{N.1}}{=}$

$a(bc + b'c') + a'bc' + a'b'c \overset{\text{D.2}}{=} abc + ab'c' + a'bc' + a'b'c$

RA.1 Rinke Seite: $(a \oplus b) \oplus c \overset{\text{Def}}{=} (ab' + a'b) \oplus c \overset{\text{Def}}{=} (ab' + a'b)c' + (ab' + a'b)'c \overset{\text{S9.1}}{=}$

$(ab' + a'b)c' + ((ab')'(a'b)')c \overset{\text{S9.2}}{=} (ab' + a'b)c' + ((a' + b'')(a'' + b'))c \overset{\text{S8}}{=} (ab' + a'b)c' + ((a' + b)(a + b'))c \overset{\text{D.2}}{=}$

$(ab' + a'b)c' + ((a' + b)a + (a' + b)b'))c \overset{\text{K.2}}{=} c'(ab' + a'b) + c(a(a' + b) + b'(a' + b))) \overset{\text{D.2}}{=}$

$c'ab' + c'a'b + c(aa' + ab + b'a' + b'b) \overset{\text{K.2}}{=} c'ab' + c'a'b + c(aa' + ab + b'a' + bb') \overset{\text{I.2}}{=}$

$c'ab' + c'a'b + c(0 + ab + b'a' + 0) \overset{\text{S11.1}}{=} c'ab' + c'a'b + c(ab + b'a' + 0 + 0) \overset{\text{N.1}}{=}$

$c'ab' + c'a'b + c(ab + b'a') \overset{\text{D.2}}{=} c'ab' + c'a'b + cab + cb'a' \overset{\text{S11.2}}{=} ab'c' + a'bc' + abc + b'a'c \overset{\text{S11.1}}{=}$

$abc + ab'c' + a'bc' + a'b'c$ qed.

RN.1: $a \oplus 0 \overset{\text{Def}}{=} a0' + a'0 \overset{\text{S7.1}}{=} a1 + a'0 \overset{\text{N.2}}{=} a + a'0 \overset{\text{S2.2}}{=} a + 0 \overset{\text{N.1}}{=} a$ qed.

RI.1: $a \oplus n(a) \overset{\text{Def}}{=} a \oplus a \overset{\text{Def}}{=} a'a + aa' \overset{\text{K.2}}{=} aa' + aa' \overset{\text{I.2}}{=} 0 + 0 \overset{\text{N.1}}{=} 0$ qed.

RK.2: $ab \overset{\text{K.2}}{=} ba$ qed.

RA.2: $a(bc) \overset{\text{A.2}}{=} (ab)c$ qed.

RN.2: $a1 \overset{\text{N.2}}{=} a$ qed.

RD Linke Seite: $a(b \oplus c) \overset{\text{Def}}{=} a(bc' + b'c) \overset{\text{D.2}}{=} a(bc') + a(b'c) \overset{\text{S11.2}}{=} abc' + ab'c$

RD Rechte Seite: $ab \oplus ac \overset{\text{Def}}{=} ab \oplus ac \overset{\text{Def}}{=} ab(ac)' + (ab)'ac \overset{\text{S9.2}}{=} (ab)(a' + c') + (a' + b')(ac) \overset{\text{K.2}}{=}$

$(ab)(a' + c') + (ac)(a' + b') \overset{\text{D.2}}{=} (ab)a' + (ab)c' + (ac)a' + (ac)b' \overset{\text{S11.2}}{=} baa' + abc' + caa' + ab'c \overset{\text{I.2}}{=}$

$b0 + abc' + c0 + ab'c \overset{\text{S2.2}}{=} 0 + abc' + 0 + ab'c \overset{\text{S11.1}}{=} abc' + ab'c + 0 + 0 \overset{\text{N.1}}{=} abc' + ab'c$ qed.

RB: $aa \overset{\text{S1.2}}{=} a$ qed.

Satz 18

Eine Boolescher Ring $(R, \oplus, \cdot, n, 0, 1)$ ist stets auch Boolesche Algebra $(R, +, \cdot, ', 0, 1)$.

Beweis 18

Definiere:

$a + b := a \oplus b \oplus ab$

Die Operation $\cdot$ ist in beiden Strukturen gleich definiert!

$a' := a \oplus 1$

Jetzt werden die Axiome der Booleschen Algebra nachgewiesen:

K.1: $a + b \overset{\text{Def}}{=} a \oplus b \oplus ab \overset{\text{S14.1}}{=} b \oplus a \oplus ab \overset{\text{RK.2}}{=} b \oplus a \oplus ba \overset{\text{Def}}{=} b \oplus a$ qed.

K.2: $ab \overset{\text{RK.1}}{=} ba$ qed.

D.1 Linke Seite $a + bc \overset{\text{Def}}{=} a \oplus bc \oplus abc$

D.1 Rechte Seite $(a + b)(a + c) \overset{\text{Def}}{=} (a \oplus b \oplus ab)(a \oplus c \oplus ac) \overset{\text{RD}}{=}$

$(a \oplus b \oplus ab)a \oplus (a \oplus b \oplus ab)c \oplus (a \oplus b \oplus ab)(ac) \overset{\text{RK.2}}{=}$

$a(a \oplus b \oplus ab) \oplus c(a \oplus b \oplus ab) \oplus (ac)(a \oplus b \oplus ab) \overset{\text{RD}}{=}$

$aa \oplus ab \oplus aab \oplus ca \oplus cb \oplus cab \oplus aca \oplus acb \oplus acab \overset{\text{S14.2}}{=}$

$a^2 \oplus ab \oplus ac \oplus bc \oplus a^2b \oplus a^2c \oplus 2abc \oplus a^2bc \overset{\text{RB}}{=}$

$a \oplus ab \oplus ac \oplus bc \oplus ab \oplus ac \oplus 2abc \oplus abc \overset{\text{S14.1}}{=}$

$a \oplus 2ab \oplus 2ac \oplus bc \oplus 3abc \overset{\text{S16.1}}{=} a \oplus bc \oplus abc$ qed.

D.2: Linke Seite $a(b + c) \overset{\text{Def}}{=} a(b \oplus c \oplus bc) \overset{\text{RD}}{=} ab \oplus ac \oplus abc$

D.2: Rechte Seite $ab + ac \overset{\text{Def}}{=} ab \oplus ac \oplus abac \overset{\text{S14.2}}{=} ab \oplus ac \oplus a^2bc \overset{\text{RB}}{=} ab \oplus ac \oplus abc$ qed.

N.1: $a + 0 \overset{\text{Def}}{=} a \oplus 0 \oplus a0 \overset{\text{S15}}{=} a \oplus 0 \oplus 0 \overset{\text{RN.1}}{=} a$ qed.

N.2: $a1 \overset{\text{Def}}{=} a1 \overset{\text{RN}}{=} a$ qed.

I.1: $a + a' \overset{\text{Def}}{=} a \oplus a' \oplus aa' \overset{\text{Def}}{=} a \oplus (a \oplus 1) \oplus a(a \oplus 1) \overset{\text{RD}}{=}$

$a \oplus (a \oplus 1) \oplus (a^2 \oplus a1) \overset{\text{S14.1}}{=} 1 \oplus a \oplus a \oplus a1 \oplus a^2 \overset{\text{RN.2}}{=} 1 \oplus 2a \oplus a \oplus a^2 \overset{\text{RB}}{=}$

$1 \oplus 3a \oplus a = 1 \oplus 4a \overset{\text{S16.1}}{=} 1$ qed.

I.2: $aa' \overset{\text{Def}}{=} a(a \oplus 1) \overset{\text{RD}}{=} a^2 \oplus a1 \overset{\text{RN.2}}{=} a^2 \oplus a \overset{\text{RB}}{=} a \oplus a = 2a \overset{\text{S16.1}}{=} 0$ qed.

8 Anhang

8.1 Aussagenlogik

8.1.1 Definitionen der Operationen OR (oder, $+$), AND (und, $\cdot$), NOT (nicht, $'$) via Wahrheitstafel

Bemerkung: 0=falsch, 1=wahr.

OR ($+$)		
a	b	$a + b$
0	0	0
0	1	1
1	0	1
1	1	1

AND ($\cdot$)		
a	b	ab
0	0	0
0	1	0
1	0	0
1	1	1

NOT ($'$)	
a	a'
0	1
1	0

8.1.2 Nachweis der Axiome K1 bis I2 für die Aussagenlogik

Axiom K1			
a	b	$a+b$	$b+a$
0	0	0	0
0	1	1	1
1	0	1	1
1	1	1	1

Axiom K2			
a	b	ab	ba
0	0	0	0
0	1	0	0
1	0	0	0
1	1	1	1

Axiom D1							
a	b	c	bc	$a+bc$	$a+b$	$a+c$	$(a+b)(a+c)$
0	0	0	0	0	0	0	0
0	0	1	0	0	0	1	0
0	1	0	0	0	1	0	0
0	1	1	1	1	1	1	1
1	0	0	0	1	1	1	1
1	0	1	0	1	1	1	1
1	1	0	0	1	1	1	1
1	1	1	1	1	1	1	1

Axiom D2							
a	b	c	$b+c$	$a(b+c)$	ab	ac	$ab+ac$
0	0	0	0	0	0	0	0
0	0	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	1	1	1	0	0	0	0
1	0	0	0	0	0	0	0
1	0	1	1	1	0	1	1
1	1	0	1	1	1	0	1
1	1	1	1	1	1	1	1

Axiom N1		
a	0	$a+0$
0	0	0
1	0	1

Axiom N2		
a	1	$a1$
0	1	0
1	1	1

Axiom I1		
a	a'	$a+a'$
0	1	1
1	0	1

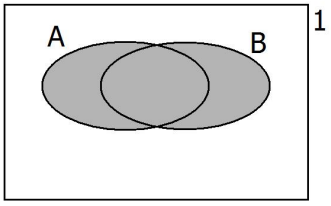
Axiom I2		
a	a'	aa'
0	1	0
1	0	0

8.2 Mengenlehre

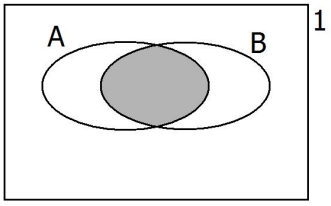
8.2.1 Definitionen der Operationen Vereinigung (+), Schnitt (·), Komplement (′) via Venndiagramm

Bemerkung: 0=leere Menge, 1=Grundmenge Ω

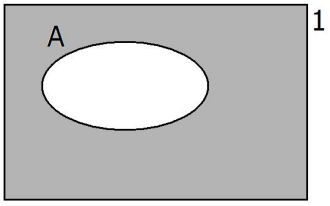
Vereinigung $A \cup B \quad (A+B)$



Schnitt $A \cap B \quad (A \cdot B)$



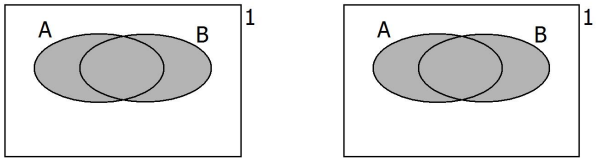
Komplement $\overline{A} \quad (A')$



8.2.2 Nachweis der Axiome K1 bis I2 für die Mengenlehre

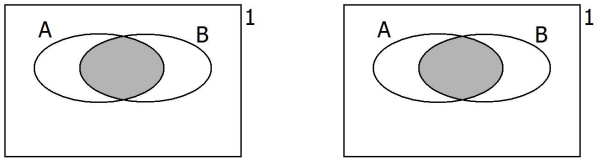
Axiom K1

$A + B = B + A$



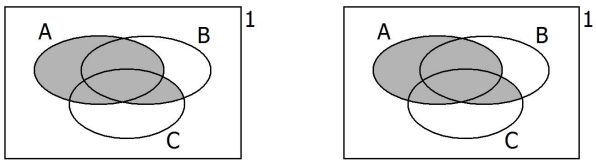
Axiom K2

$AB = BA$



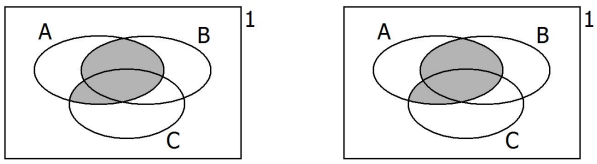
Axiom D1

$A + BC = (A + B)(A + C)$



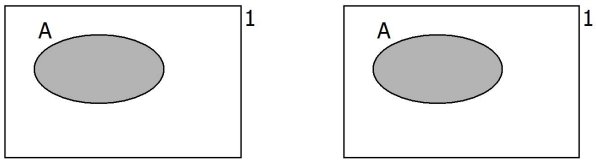
Axiom D2

$A(B + C) = AB + AC$



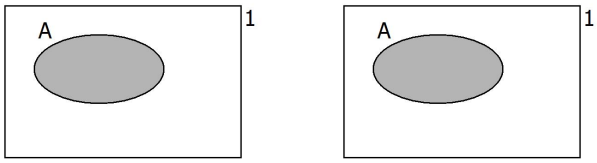
Axiom N1

$A + 0 = A$



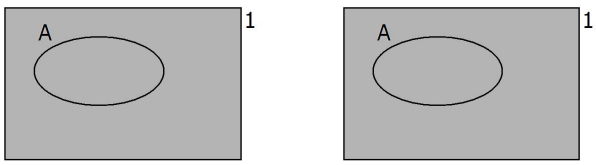
Axiom N2

$A1 = A$



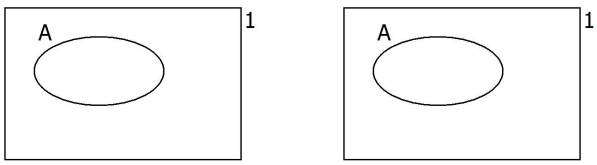
Axiom I1

$A + A' = 1$



Axiom I2

$AA' = 0$



Literaturverzeichnis

Whitesitt, J. E. (1973): Boolesche Algebra und ihre Anwendungen.
4. Nachdruck. Leipzig: VEB Verlag Enzyklopädie

Boole, George (1958): The Laws of Thought.
Nachdruck. New York: Dover Classics

Meschkowski, Herbert (1967): Denkweisen grosser Mathematiker.
2., überarbeitete Auflage. Braunschweig: Vieweg Verlag