2 Boole'sche Algebra

Im 19. Jahrhundert wurde die Begriffslogik des Aristoteles von den Mathematikern G.W.Boole, A. de Morgan und C.S.Peirce in die Form eines „Rechnens" mit Begriffen gebracht, die dem Rechnen mit Zahlen gleicht.

2.1 Axiome und grundlegende Eigenschaften

Definition 2.1 Eine *Boole'sche Algebra* $\mathcal{A} = (A, +, \cdot, ^{-}, 0, 1)$ besteht aus einer Menge $A \neq \emptyset$ mit Operationen und Elementen, so daß:

(a) $+, \cdot\ : A \times A \to A$ sind assoziativ, kommutativ und idempotent: für alle $a, b, c \in A$ gilt

$$\begin{aligned} a + (b + c) &= (a + b) + c \\ a + b &= b + a \\ a + a &= a \\ a \cdot (b \cdot c) &= (a \cdot b) \cdot c \\ a \cdot b &= b \cdot a \\ a \cdot a &= a, \end{aligned}$$

(b) $+$ und $\cdot$ sind distributiv zueinander: für alle $a, b, c \in A$ gilt

$$\begin{aligned} (a + b) \cdot c &= (a \cdot c) + (b \cdot c) \\ (a \cdot b) + c &= (a + c) \cdot (b + c), \end{aligned}$$

(c) 0, 1 sind neutrale Elemente für $+$ bzw. $\cdot$: für alle $a \in A$ gilt

$$\begin{aligned} a + 0 &= a \\ a \cdot 1 &= a, \end{aligned}$$

(d) $^{-} : A \to A$ ist der Übergang zum Komplement (Gegenteil): für alle $a \in A$

$$\begin{aligned} a + \overline{a} &= 1 \\ a \cdot \overline{a} &= 0. \end{aligned}$$

Die Anforderungen (a) – (d) an eine Boole'sche Algebra haben die Form von *universellen Gleichungen*, d.h. Aussagen $\forall a \forall b \forall c (s = t)$ mit geeigneten Termen s, t. Sie bilden ein *Axiomensystem* der Boole'schen Algebra, das wir mit BA bezeichnen.

Beispiel 2.2 Die Standardinterpretationen von BA sind:

(a) Die Algebra der Wahrheitswerte,

$$\mathbb{B} = (\{0,1\}, \max, \min, ^{-}, 0, 1)$$

mit $\overline{1} := 0$ und $\overline{0} := 1$. Schon Aristoteles betonte die Bedeutung des „tertium non datur", $a + \overline{a} = 1$, und des „ausgeschlossenen Widerspruchs", $a \cdot \overline{a} = 0$ als wichtigste Prinzipien der Logik.

(b) Die Potenzmengenalgebra einer Menge M,

$$2^M := (2^M, \cup, \cap, ^{-}, \emptyset, M)$$

mit $\overline{A} := M \setminus A := \{\, m \in M \mid m \notin A \,\}$.

Jede Boole'sche Algebra mit 8 Elementen ist isomorph zu 2^M für $M = \{a, b, c\}$ und kann wie folgt dargestellt werden:

Zu den Ecken x und y ist $x + y$ (bzw. $x \cdot y$) die erste Ecke, die man sowohl von x wie von y durch aufsteigende (bzw. absteigende) Linien erreicht. Das Komplement von x ist die „gegenüberliegende" Ecke, die man durch Spiegelung am Mittelpunkt erreicht, also $\overline{a} = a'$ usw.

Da nicht verlangt wird, daß $0 \neq 1$ ist, gibt es auch eine *triviale* Boole'sche Algebra, deren Individuenbereich aus nur einem Element besteht. Weitere Beispiele für Boole'sche Algebren kann man u.a. wie folgt konstruieren:

Proposition 2.3 Sei $\mathcal{A} = (A, +^A, \cdot^A, -^A, 0^A, 1^A)$ eine Boole'sche Algebra.

(a) Ist $\mathcal{A}' \subseteq \mathcal{A}$ eine Unteralgebra, so ist auch $\mathcal{A}'$ eine Boole'sche Algebra.

(b) Die aus $\mathcal{A}$ durch Vertauschen von $+$ und $\cdot$ sowie von 0 und 1 entstehende *duale* Algebra $\widetilde{\mathcal{A}} := (A, \cdot^A, +^A, -^A, 1^A, 0^A)$ ist eine Boole'sche Algebra.

(c) Sei neben $\mathcal{A}$ auch $\mathcal{B} = (B, +^B, \cdot^B, -^B, 0^B, 1^B)$ eine Boole'sche Algebra. Dann ist auch das *kartesische Produkt* von $\mathcal{A}$ und $\mathcal{B}$,

$$\mathcal{A} \times \mathcal{B} := (A \times B, +^{A \times B}, \cdot^{A \times B}, -^{A \times B}, 0^{A \times B}, 1^{A \times B}),$$

dessen Operationen ("komponentenweise") durch

$$\begin{array}{ccc}
\langle a,b\rangle +^{A\times B} \langle a',b'\rangle & := & \langle a +^A a', b +^B b'\rangle, \\
\langle a,b\rangle \cdot^{A\times B} \langle a',b'\rangle & := & \langle a \cdot^A a', b \cdot^B b'\rangle, \\
\overline{\langle a,b\rangle}^{A\times B} & := & \langle \overline{a}^A, \overline{b}^B\rangle, \\
0^{A\times B} & := & \langle 0^A, 0^B\rangle, \\
1^{A\times B} & := & \langle 1^A, 1^B\rangle
\end{array}$$

definiert sind, eine Boole'sche Algebra.

(d) Sei M eine Menge und $F := \{ f \mid f : M \to A \}$ die Menge der Funktionen von M nach A. Definiere („punktweise") folgende Operationen:

$$\begin{array}{ccc}
(f +^F g)(m) & := & f(m) +^A g(m), \\
(f \cdot^F g)(m) & := & f(m) \cdot^A g(m), \\
\overline{f}^F(m) & := & \overline{f(m)}^A, \\
0^F(m) & := & 0^A, \\
1^F(m) & := & 1^A,
\end{array}$$

Dann ist auch $\mathcal{F} := (F, +^F, \cdot^F, {}^{-F}, 0^F, 1^F)$ eine Boole'sche Algebra.

Beweis:

(a) Alle Axiome sind von der Form $\forall \vec{x} s(\vec{x}) = t(\vec{x})$ für geeignete Terme s und t. Wir hatten früher gezeigt, daß solche Aussagen beim Übergang von einer Struktur zu einer Unterstruktur „erhalten" bleiben.

(b) Sei $\widetilde{\varphi}$ *die zu* φ *duale* Formel, die aus φ entsteht, wenn man darin $+$ mit $\cdot$ und 0 mit 1 vertauscht. Offenbar gilt $\mathcal{A} \models \varphi$ genau dann, wenn $\widetilde{\mathcal{A}} \models \widetilde{\varphi}$, für jede Aussage φ. Nun beachte, daß für jedes Axiom φ die duale Aussage $\widetilde{\varphi}$ eines der anderen Axiome ist, und daß folglich jedes Axiom φ selbst die duale Aussage eines anderen Axioms ist, nämlich $\varphi = \widetilde{\widetilde{\varphi}}$. Also hat man für jedes Axiom φ:

$$\mathcal{A} \models \varphi \Rightarrow \mathcal{A} \models \widetilde{\varphi} \Rightarrow \widetilde{\mathcal{A}} \models \widetilde{\widetilde{\varphi}} \Rightarrow \widetilde{\mathcal{A}} \models \varphi.$$

(c) Das sieht man leicht durch Nachrechnen, da die Gleichungen ja in jeder Komponente gelten.

(d) Das sieht man ebenfalls leicht durch Nachrechnen.

□

Aus (b) folgt das *Dualitätsprinzip*

Die Aussage φ gilt in jeder Boole'schen Algebra genau dann, wenn $\widetilde{\varphi}$ in jeder Boole'schen Algebra gilt.

Proposition 2.4 Sei $\mathcal{A}$ eine Boole'sche Algebra. Sind $a, b \in A$ mit $a \cdot b = 0$ und $a + b = 1$, so ist $a = \overline{b}$.

Beweis:

$$\begin{aligned} a &= a \cdot 1 \\ &= a \cdot (b + \overline{b}) \\ &= (a \cdot b) + (a \cdot \overline{b}) \\ &= 0 + (a \cdot \overline{b}) \\ &= (b \cdot \overline{b}) + (a \cdot \overline{b}) \\ &= (b + a) \cdot \overline{b} \\ &= (a + b) \cdot \overline{b} \\ &= 1 \cdot \overline{b} \\ &= \overline{b}. \end{aligned}$$

□

Daraus folgen die als *de Morgan'sche Regeln* bekannten Gleichungen, die schon Wilhelm von Ockham im 14. Jahrhundert für die Logik gezeigt hat:

Lemma 2.5 (De Morgan) Für alle Elemente a, b einer Boole'schen Algebra gilt

$$\begin{aligned} \overline{a \cdot b} &= \overline{a} + \overline{b} \\ \overline{a + b} &= \overline{a} \cdot \overline{b} \end{aligned}$$

Beweis: Nach dem Dualitätsprinzip brauchen wir nur die erste Behauptung nachzuweisen. Nach Proposition 2.4 genügt es dafür zu zeigen:

$$(ab)(\overline{a} + \overline{b}) = 0, \qquad ab + (\overline{a} + \overline{b}) = 1,$$

denn dann folgt $\overline{a \cdot b} = \overline{a} + \overline{b}$. Die erste Gleichung erhält man durch

$$\begin{aligned} ab(\overline{a} + \overline{b}) &= ab\overline{a} + ab\overline{b} \\ &= a\overline{a}b + a0 \\ &= 0b + a0 \\ &= 0, \end{aligned}$$

und die zweite Gleichung durch

$$\begin{aligned} 1 &= 1 \cdot 1 \\ &= (a + \overline{a})(b + \overline{b}) \\ &= ab + a\overline{b} + \overline{a}b + \overline{a}\,\overline{b} \\ &= ab + a\overline{b} + \overline{a}b + \overline{a}\,\overline{b} + \overline{a}\,\overline{b} \end{aligned}$$

$$\begin{aligned}
&= ab + a\overline{b} + \overline{a}(b + \overline{b}) + \overline{a}\,\overline{b} \\
&= ab + \overline{a}(b + \overline{b}) + a\overline{b} + \overline{a}\,\overline{b} \\
&= ab + \overline{a}1 + (a + \overline{a})\overline{b} \\
&= ab + \overline{a} + 1\overline{b} \\
&= ab + \overline{a} + \overline{b}
\end{aligned}$$

Also sind ab und $\overline{a} + \overline{b}$ komplementär zu einander. □

Proposition 2.6 Ist $+ : A \times A \to A$ eine assoziative, kommutative und idempotente Abbildung, so ist die durch

$$a \leq b :\iff a + b = b \tag{13}$$

definierte Relation auf A eine partielle Ordnung.

Beweis:

(a) $\leq$ ist reflexiv: Da $+$ idempotent ist, gilt $a + a = a$, d.h. $a \leq a$.

(b) $\leq$ ist transitiv: Seien $a \leq b$ und $b \leq c$. Dann gilt

$$\begin{aligned}
a + c &= a + (b + c) && \text{da } b \leq c \\
&= (a + b) + c && \text{da } + \text{ assoziativ ist} \\
&= b + c && \text{da } a \leq b \\
&= c && \text{da } b \leq c,
\end{aligned}$$

also $a \leq c$. Damit ist $\leq$ transitiv.

(c) $\leq$ ist antisymmetrisch: Seien $a \leq b$ und $b \leq a$. Dann ist

$$\begin{aligned}
a &= b + a && \text{da } b \leq a \\
&= a + b && \text{da } + \text{ kommutativ ist} \\
&= b && \text{da } a \leq b \text{ ist.}
\end{aligned}$$

Also ist $\leq$ antisymmetrisch.

Nach (a) – (c) ist $\leq$ eine partielle Ordnung. □

Proposition 2.7 Sei $\mathcal{A}$ eine Boole'sche Algebra und $\leq^A$ die nach (13) aus $+^{\mathcal{A}}$ definierte partielle Ordnung. Dann gilt $0 \leq^A a \leq^A 1$ für jedes $a \in A$.

Beweis: Wegen $0 + a = a + 0 = a$ gilt $0 \leq a$. Wegen

$$a + 1 = a + (a + \overline{a}) = (a + a) + \overline{a} = a + \overline{a} = 1$$

gilt $a \leq 1$. Also ist 0 das kleinste und 1 das größte Element von A $\square$

Nimmt man in (13) statt + die Multiplikation $\cdot$, so erhält man ebenfalls eine partielle Ordnung,

$$a \geq b :\Longleftrightarrow\ a \cdot b = b. \tag{14}$$

In der Potenzmengenalgebra 2^M ist die nach (13) definierte partielle Ordnung die Teilmengenbeziehung, die nach (14) definierte die Obermengenbeziehung:

$$\begin{aligned} A \cup B = B \quad &\Longleftrightarrow \quad A \subseteq B, \\ A \cap B = B \quad &\Longleftrightarrow \quad A \supseteq B. \end{aligned}$$

Die beiden partiellen Ordnungen verhalten sich auch im allgemeinen so zu einander wie erwartet, d.h. $a \leq b$ gilt genau dann, wenn $b \geq a$ gilt:

Proposition 2.8 In jeder Boole'schen Algebra $\mathcal{A}$ gilt für alle a, b:

$$a + b = b \iff a \cdot b = a$$

Beweis: Sei $a + b = b$. Dann ist

$$ab = a(a + b) = aa + ab = a + ab = a(1 + b) = a1 = a.$$

Ist umgekehrt $a \cdot b = a$, so ist

$$a + b = ab + b = ab + 1b = (a + 1)b = 1b = b.$$

$\square$

Offenbar sind + und $\cdot$ monoton bezüglich $\leq$: ist z.B. $b \leq c$, so ist $ab \leq ac$, da

$$ab + ac = a(b + c) = ac.$$

Die Komplementbildung ist es natürlich nicht, sondern man hat

$$a \leq b \quad \Rightarrow \quad \overline{b} \leq \overline{a}.$$

Eine Boole'sche Algebra $\mathcal{A}$ kann man auch als Verallgemeinerung der 2-wertigen Logik verstehen: dann bedeutet $a = 1$, daß a wahr ist, $a = 0$, daß a falsch ist, und $a \leq b$, daß a logisch stärker ist als b, d.h. daß b aus a folgt.

2.2 Homomorphismen und Ideale

Proposition 2.9 Sei $h : \mathcal{A} \to \mathcal{B}$ ein Homomorphismus zwischen Boole'schen Algebren und $g : Var \to A$ eine Belegung. Dann ist für jede Formel φ

$$[\![\varphi]\!]^{\mathcal{B}}_{h \circ g} = h([\![\varphi]\!]^{\mathcal{A}}_g).$$

Beweis: durch Induktion über den Aufbau der aussagenlogischen Formeln.

$\varphi = \bot$: Da h ein Homomorphismus ist, ist $[\![\bot]\!]^{\mathcal{B}}_{h\circ g} = 0^{\mathcal{B}} = h(0^{\mathcal{A}}) = h([\![\bot]\!]^{\mathcal{A}}_g)$.

$\varphi = A_i$: Nach den Definitionen ist

$$[\![A_i]\!]^{\mathcal{B}}_{h\circ g} = (h \circ g)(A_i) = h(g(A_i)) = h([\![A_i]\!]^{\mathcal{A}}_g).$$

$\varphi = \neg\psi$: Nach Induktionsannahme gilt die Behauptung schon für ψ. Daher ist

$$[\![\neg\psi]\!]^{\mathcal{B}}_{h\circ g} = \overline{[\![\psi]\!]^{\mathcal{B}}_{h\circ g}}^{\mathcal{B}} = \overline{h([\![\psi]\!]^{\mathcal{A}}_g)}^{\mathcal{B}} = h(\overline{[\![\psi]\!]^{\mathcal{A}}_g}^{\mathcal{A}}) = h([\![\neg\psi]\!]^{\mathcal{A}}_g)$$

$\varphi = (\varphi_1 \wedge \varphi_2)$: Analog, mit der Induktionsannahme für φ_1 und φ_2 und weil h ein Homomorphismus ist. □

Definition 2.10 Ein *Ideal* I der Boole'schen Algebra $\mathcal{A}$ ist eine Teilmenge $\emptyset \neq I \subseteq A$, die „nach unten“ (d.h. unter $\geq$) und unter $+$ abgeschlossen ist:

(a) $0 \in I$,

(b) $\forall a, b \in A(b \leq a \in I \Rightarrow b \in I)$,

(c) $\forall a, b \in A(a \in I \wedge b \in I \Rightarrow a + b \in I)$.

Ein Ideal I von $\mathcal{A}$ heißt *echt*, wenn $I \neq A$.

Wegen (b) gilt für jedes Ideal I auf $\mathcal{A}$ und alle $a, b \in A$ offenbar:

$$\begin{aligned} a + b \in I &\quad\Rightarrow\quad a \in I, \\ a \in I &\quad\Rightarrow\quad a \cdot b \in I, \\ 1 \in I &\quad\Leftrightarrow\quad A = I. \end{aligned}$$

Satz 2.11 Sei $\mathcal{A}$ eine Boole'sche Algebra.

(a) Ist $h : \mathcal{A} \to \mathcal{B}$ ein Homomorphismus in eine Boole'sche Algebra $\mathcal{B}$, so ist $kern(h) := \{ a \in A \mid h(a) = 0^B \}$ ein Ideal von $\mathcal{A}$.

(b) Ist I ein Ideal von $\mathcal{A}$, so gibt es einen Homomorphismus $h : \mathcal{A} \to \mathcal{B}$ in eine Boole'sche Algebra $\mathcal{B}$, so daß $I = kern(h)$ ist.

Beweis:

(a) Nach den Homomorphismuseigenschaften von h gilt $h(0^A) = 0^B$, also $0 \in I$. Ist $b \leq a \in I$, so ist $0 \leq h(b) \leq h(a) = 0$, also auch $b \in I$. Sind $a, b \in I$, so ist $h(a + b) = h(a) + h(b) = 0 + 0 = 0$, also $a + b \in I$.

(b) Wir wollen $\mathcal{B}$ aus $\mathcal{A}$ durch zusammenfassen von Elementen in Äquivalenzklassen erhalten. Dazu definere

$$a \sim_I b :\iff \exists a' \in I \; \exists b' \in I \, (a + a' = b + b'). \tag{15}$$

Zuerst überprüfen wir, daß diese Relation eine Äquivalenzrelation ist: sie reflexiv, da $0 \in I$ und $a+0 = a+0$ gilt. Offensichtlich ist $\sim_I$ symmetrisch. Und $\sim_I$ ist transitiv, denn zu $a \sim_I b$, $b \sim_I c$ gibt es $a', b', b'', c' \in I$ mit

$$a + a' = b + b' \quad \text{und} \quad b + b'' = c + c',$$

also

$$a + (a' + b'') = (a + a') + b'' = b + b' + b'' = b' + (c + c') = c + (b' + c'),$$

und hier sind $(a + b''), (b' + c') \in I$, also $a \sim_I c$.

Wir nehmen nun

$$B := A/\!\sim_I \quad := \{\, [a]_I \mid a \in A \,\},$$

und schreiben für die Äquivalenzklasse von a bezüglich $\sim_I$ kurz

$$[a]_I := \{\, a' \in A \mid a \sim_I a' \,\}.$$

Um aus B eine Boole'sche Algebra $\mathcal{B}$ zu machen, setzen wir natürlich

$$\begin{aligned}
0^B &:= [0]_I, \\
1^B &:= [1]_I \\
[a]_I +^B [c]_I &:= [a + c]_I && (16) \\
[a]_I \cdot^B [c]_I &:= [a \cdot c]_I && (17) \\
\overline{[a]_I}^B &:= [\overline{a}]_I && (18)
\end{aligned}$$

Damit dies wohldefiniert ist, also die rechten Seiten von (16) – (18) nicht von der Wahl der Repräsentanten a, c abhängen, muß $\sim_I$ eine Kongruenzrelation sein. Um das zu überprüfen, seinen $a \sim_I b, c \sim_I d$ und dazu Elemente $a', b', c', d' \in I$ mit

$$a + a' = b + b' \quad \text{und} \quad c + c' = d + d'$$

gegeben. Wir zeigen zuerst, daß $[a + c]_I = [b + d]_I$ ist:

$$\begin{aligned}
(a + c) + (a' + c') &= (a + a') + (c + c') \\
&= (b + b') + (d + d') \\
&= (b + d) + (b' + d').
\end{aligned}$$

Da $(a' + c'), (b' + d') \in I$ sind, folgt hieraus $(a + c) \sim_I (b + d)$.

Die Behauptungen $[a \cdot c]_I = [b \cdot d]_I$ und $[\overline{a}]_I = [\overline{b}]_I$ bleiben als Übungsaufgaben.

Schließlich ist noch zu zeigen, daß $I = kern(h)$ ist. Für $I \subseteq kern(h)$ sei $a \in I$. Mit $a' := 0$ und $0' := a$ haben wir

$$a + a' = a + 0 = 0 + a = 0 + a'$$

mit $a', 0' \in I$, also $a \sim_I 0$ und daher $h(a) = [0]_I$, d.h. $a \in kern(h)$. Ist umgekehrt $a \in kern(h)$, so ist $h(a) = [a]_I = [0]_I$, also $a \sim_I 0$ und daher für geeignete $a', b' \in I$

$$a + a' = 0 + b' = b' \in I.$$

Da I nach unten abgeschlossen und $a \leq a + a' \in I$ ist, folgt $a \in I$. □

2.3 Der Stone'sche Darstellungssatz

In diesem Abschnitt wollen wir zeigen, daß jede Boole'sche Algebra (bis auf Isomorphie) eine Unteralgebra der Potenzmengenalgebra 2^M ist, für eine geeignete Menge M.

Definition 2.12 Ein *Primideal* auf $\mathcal{A}$ ist ein Ideal $I \subseteq A$ mit $I \neq A$ und

$$\forall a, b \in A(a \cdot b \in I \Rightarrow a \in I \vee b \in I).$$

Die Bezeichnung kommt daher, daß, wenn man $a \in I$ als "I teilt a" liest, die Primidealeigenschaft der Primzahleigenschaft entspricht.

Beispiel 2.13 Ist $\mathcal{A} = 2^M$ die Potenzmengenalgebra von M und $m \in M$, so ist

$$I := \{ A \subseteq M \mid m \notin A \}$$

ein Primideal von $\mathcal{A}$. Die Primeigenschaft besagt: ist $m \notin A \cap B$, so ist $m \notin A$ oder $m \notin B$.

Wichtig ist der Zusammenhang zwischen Primidealen und dem Komplement:

Lemma 2.14 Für echte Ideale $I \subset A$ sind äquivalent:

(a) I ist ein Primideal,

(b) Für alle $a \in A$ ist $a \in I$ genau dann, wenn $\overline{a} \notin I$,

(c) $I = kern(h)$ für einen Homomorphismus $h : \mathcal{A} \to \mathbb{B}$,

(d) I ist ein maximales echtes Ideal: es gibt kein Ideal J mit $I \subset J \subset A$.

Beweis: (a) $\Rightarrow$ (b): Sei I ein Primideal und $a \in A$. Da I ein echtes Ideal ist, ist $a + \overline{a} = 1 \notin I$, also wegen der Idealeigenschaften $a \notin I$ oder $\overline{a} \notin I$. Da I Primideal ist, ist andererseits wegen $a \cdot \overline{a} = 0 \in I$ auch $a \in I$ oder $\overline{a} \in I$. Zusammen ergibt das (b).

(b) $\Rightarrow$ (c): Damit I der Kern von h wird, müssen wir

$$h(a) := \begin{cases} 0, & \text{falls } a \in I \\ 1, & \text{sonst} \end{cases}$$

nehmen. Da $0 \in I$ ist, ist nach (b) $1 \notin I$, sodaß $h(0) = 0$ und $h(1) = 1$ wird. Wir zeigen zuerst, daß h monoton ist. Sei $a \leq b$. Ist $h(a) = 0$, so ist natürlich $h(a) \leq h(b)$. Ist $h(a) = 1$, so ist $a \notin I$, also $b \notin I$ wegen der Idealeigenschaft, und daher $h(b) = 1$, also auch $h(a) \leq h(b)$. Aus der Monotonie folgt

$$h(a \cdot b) \leq h(a) \leq h(a + b)$$

für alle $a, b \in A$. Falls $0 \in \{h(a), h(b)\}$, so ist also schon $h(a \cdot b) = h(a) \cdot h(b)$, und falls $1 \in \{h(a), h(b)\}$, so gilt schon $h(a + b) = h(a) + h(b)$. Ist $h(a) = 1 = h(b)$, also $a, b \notin I$, so ist $a \cdot b \notin I$ da I ein Primideal ist, also $h(a \cdot b) = 1 = h(a) \cdot h(b)$. Ist $h(a) = 0 = h(b)$, so ist $a + b \in I$, da I ein Ideal ist, also $h(a+b) = 0 = h(a) + h(b)$.

Schließlich ist $h(\overline{a}) = \overline{h(a)}$ nach der Voraussetzung (b), denn

$$h(\overline{a}) = 0 \iff \overline{a} \in I \iff a \notin I \iff h(a) = 1,$$

und analog $h(\overline{a}) = 1$ genau dann, wenn $h(a) = 0$.

(c) $\Rightarrow$ (d): Angenommen, es gebe ein Ideal J mit $I \subset J \neq A$. Dann gibt es $b \in J \setminus I$, und wegen $b \notin I = \mathit{kern}(h)$ ist $h(b) \neq 0$, also $h(b) = 1$ wegen $h(b) \in \mathbb{B}$. Da h ein Homomorphismus ist, ist $h(\overline{b}) = \overline{h(b)} = \overline{1} = 0$, also $\overline{b} \in I \subset J$. Da J ein Ideal ist, ist dann aber $1 = b + \overline{b} \in J$, und damit $J = A$.

(d) $\Rightarrow$ (a): Sei I ein maximales echtes Ideal von $\mathcal{A}$. Angenommen, $a \cdot b \in I$, aber $a \notin I$ und $b \notin I$. Die Menge

$$a + I := \{\, c \in A \mid \exists i \in I (c \leq a + i) \,\}$$

ist ein Ideal, da I eines ist und $+$ idempotent ist. Wegen $0 \in I$ und $a \notin I$ ist $I \neq (a + I)$, also $I = A$ und daher $1 = a + i_a$ für ein $i_a \in I$. Ebenso ist $I \neq b + I$ und deshalb $1 = b + i_b$ für ein $i_b \in I$. Daraus folgt

$$1 = (a + i_a) \cdot (b + i_b) = ab + ai_b + i_a b + i_a i_b \in I$$

wegen $ab \in I$ und weil mit $i \in I$ auch $c \cdot i \in I$ ist. □

Lemma 2.15 (Zorn'sches Lemma) Sei $(M, \leq)$ eine partielle Ordnung. Wenn jede durch $\leq$ total geordnete Teilmenge $\emptyset \neq K \subseteq M$ eine obere Schranke hat, dann hat M ein maximales Element.

Dieses Lemma kann man aus den bisher gemachten Annahmen über die Mengenbildungen nicht beweisen. Man braucht ein weiteres Axiom, das sogenannte „Auswahlaxiom“. Umgekehrt folgt das Auswahlaxiom aus dem Zorn'schen Lemma. Beides beweisen wir hier nicht. Das Zorn'sche Lemma ist aber einfach anzuwenden:

Korollar 2.16 Sei I ein echtes Ideal der Boole'schen Algebra $\mathcal{A}$. Es gibt ein Primideal J von $\mathcal{A}$ mit $I \subseteq J$.

Beweis: Betrachte die Menge

$$M := \{\, J \mid I \subseteq J, J \text{ ist echtes Ideal von } \mathcal{A} \,\},$$

partiell geordnet durch $\subseteq$. Jede durch $\subseteq$ total geordnete Teilmenge $\emptyset \neq K \subseteq M$ hat eine obere Schranke, nämlich $\bigcup K \in M$: da $K \neq \emptyset$, ist $0 \in \bigcup K$, und zu $a', b' \in \bigcup K$ mit $c \leq a'$ gibt es $J \in K$ mit $a', b' \in J$, also $c \in J$ und $a' + b' \in J \subseteq \bigcup K$. Nach dem Zorn'schen Lemma hat M ein maximales Element, also ein maximales Ideal $I \subseteq J$. Nach Lemma 2.14 ist J ein Primideal. □

Satz 2.17 (Stone'scher Darstellungssatz) Jede Boole'sche Algebra $\mathcal{A}$ ist isomorph zu einer Unteralgebra einer Boole'schen Algebra der Form 2^M.

Beweis: Sei M die Menge aller Primideale von $\mathcal{A}$. Definiere $h : A \to 2^M$ durch

$$h(a) := \{\, I \in M \mid a \notin I \,\} \in 2^M.$$

Beachte, daß für jedes Ideal I mit $a \in I$ auch $a \cdot b \in I$ ist, wegen $a \cdot b \leq a$. Für jedes Primideal ist $a \notin I$ genau dann, wenn $\overline{a} \in I$ ist. Daraus folgt, daß h ein Homomorphismus ist: sei I ein Primideal auf $\mathcal{A}$.

(a) $h(0) = \emptyset$: wegen $0 \in I$ ist $I \notin h(0)$.

(b) $h(1) = M$: wegen $1 \notin I$ ist $I \in h(1)$.

(c) für alle $a, b \in A$ gilt: $h(a + b) = h(a) \cup h(b)$:

$$\begin{aligned} (a+b) \notin I &\iff \overline{a+b} \in I, \\ &\iff \overline{a} \cdot \overline{b} \in I, \\ &\iff \overline{a} \in I \text{ oder } \overline{b} \in I, \quad \text{da } I \text{ Primideal ist} \\ &\iff a \notin I \text{ oder } b \notin I. \end{aligned}$$

(d) für alle $a, b \in A$ gilt: $h(a \cdot b) = h(a) \cap h(b)$:

$$\begin{aligned} (a \cdot b) \notin I &\iff \overline{a \cdot b} \in I \\ &\iff \overline{a} + \overline{b} \in I \\ &\iff \overline{a} \in I \text{ und } \overline{b} \in I \text{ (wegen } \overline{a}, \overline{b} \leq \overline{a} + \overline{b}) \\ &\iff a \notin I \text{ und } b \notin I. \end{aligned}$$

(e) für alle $a \in A$ gilt $h(\overline{a}) = M \setminus h(a)$.

$$\begin{aligned} \overline{a} \notin I &\iff a \in I \\ &\iff I \notin h(a). \end{aligned}$$

Es bleibt noch zu zeigen, daß h injektiv ist: Sei $a \neq b$. Zum Nachweis von $h(a) \neq h(b)$ zeigen wir, daß a und b „durch ein Primideal getrennt werden", d.h.

$$a \in I \text{ und } b \notin I \quad \text{oder} \quad b \in I \text{ und } a \notin I \qquad \text{für ein Primideal } I. \tag{19}$$

Wegen $a \neq b$ ist $a \not\leq b$ oder $b \not\leq a$, also etwa $a \not\leq b$. Dann ist $\overline{a} + b \neq 1$, denn sonst wäre

$$a + b = (a + b)(\overline{a} + b) = a\overline{a} + ab + b\overline{a} + bb = 0 + b(a + \overline{a}) + b = b,$$

also doch $a \leq b$. Wegen $1 \not\leq \overline{a} + b$ ist

$$I(a, b) := \{ c \in A \mid c \leq \overline{a} + b \}$$

ein echtes Ideal, und mit $\overline{a}+b \in I(a, b)$ sind $\overline{a} \in I(a, b)$ und $b \in I(a, b)$. Außerdem ist $a \notin I(a, b)$, da sonst $1 = a + \overline{a} \in I(a, b)$ wäre. Nun betrachte

$$M(a, b) := \{ J \mid I(a, b) \subseteq J, a \notin J, J \text{ ist ein Ideal} \}.$$

Ist $K \subseteq M(a, b)$ eine nichtleere total geordnete Teilmenge, so ist $\bigcup K$ eine obere Schranke von K, und $\bigcup K \in M(a, b)$. Nach dem Zorn'schen Lemma hat $M(a, b)$ ein maximales Element, etwa $J(a, b)$. Nach Korollar 2.16 gibt ein Primideal I mit $J(a, b) \subseteq I$. Wir haben $\overline{a}, b \in I(a, b) \subseteq J(a, b) \subseteq I$. Außerdem ist $a \notin I$, da sonst $1 = a + \overline{a} \in I$ wäre. Damit ist (19) gezeigt. □

2.4 Allgemeingültigkeit in allen Boole'schen Algebren

Wir haben die Formeln φ der klassischen Aussagenlogik bisher in der Algebra $\mathbb{B}$ der Wahrheitswerte ausgewertet, wobei die Operationen $+, \cdot, ^-, 0, 1$ durch $0^{\mathbb{B}}, 1^{\mathbb{B}}$ und die Wahrheitsfunktionen $+^{\mathbb{B}}, \cdot^{\mathbb{B}}$ und $^{-\mathbb{B}}$ interpretiert wurden. Insbesondere haben wir die Allgemeingültigkeit von Formeln und die logische Folgerung auf diese Interpretation zurückgeführt.

Aber ist es wirklich allgemein genug, wenn man nur die Interpretation in $\mathbb{B}$ berücksichtigt? Sollte man nicht auch mehr Wahrheitswerte und mehr Interpretationen von $+, \cdot, ^-$ zulassen?

Definition 2.18 Sei $\mathcal{K}$ die Klasse aller Boole'schen Algebren und T eine Menge von aussagenlogischen Formeln. Eine Formel φ ist eine *$\mathcal{K}$-Folgerung aus T*, kurz $T \models^{\mathcal{K}} \varphi$, wenn für jedes $\mathcal{A} \in \mathcal{K}$ und jede Belegung $g : \mathit{Var} \to A$ gilt:

wenn $[\![\psi]\!]_g^{\mathcal{A}} = 1^{\mathcal{A}}$ für alle $\psi \in T$, so ist auch $[\![\varphi]\!]_g^{\mathcal{A}} = 1^{\mathcal{A}}$.

Die Formel φ heißt *allgemeingültig in* $\mathcal{K}$, kurz: $\models^{\mathcal{K}} \varphi$, wenn $\emptyset \models^{\mathcal{K}} \varphi$. Eine Belegung $g : Var \to A$ in eine Algebra $\mathcal{A} \in \mathcal{K}$ *erfüllt* φ, wenn $[\![\varphi]\!]_g^{\mathcal{A}} = 1^{\mathcal{A}}$.

Wir wollen nun zeigen, daß die Allgemeingültigkeit und logische Folgerung, die allein mit der Interpretation $\mathbb{B}$ definiert wurden, schon die Allgemeingültigkeit und Folgerung bezüglich der Klasse aller Boole'schen Algebren nach sich zieht:

Satz 2.19 Sei $\mathcal{K}$ die Klasse aller Boole'schen Algebren, T eine Menge von Formeln und φ eine Formel der Aussagenlogik. Dann sind äquivalent:

(a) $T \models \varphi$

(b) $T \models^{\mathcal{K}} \varphi$

Beweis: (b) $\Rightarrow$ (a): Um $T \models \varphi$ zu zeigen, sei $g : Var \to \mathbb{B}$ eine Belegung über $\mathbb{B}$, die alle Formeln aus T erfüllt. Da $\mathbb{B} \in \mathcal{K}$ ist, gilt dann $[\![\varphi]\!]_g^{\mathbb{B}} = 1^{\mathbb{B}}$ nach (b).

(a) $\Rightarrow$ (b): (indirekt) Angenommen, $T \not\models^{\mathcal{K}} \varphi$. Dann gibt es eine Boole'sche Algebra $\mathcal{A}$ und eine Belegung $g : Var \to A$, so daß g jede Formel von T erfüllt, aber nicht φ. Um $T \not\models \varphi$ zu zeigen, müssen wir eine Belegung $g' : Var \to \mathbb{B}$ konstruieren, die T erfüllt, aber nicht φ.

Sei $b := [\![\varphi]\!]_g^{\mathcal{A}} \neq 1^{\mathcal{A}}$, also $1 \not\leq b$. Nach Korollar 2.16 gibt es oberhalb des echten Ideals $\{\, c \mid c \leq b \,\}$ ein Primideal $I \subseteq A$ mit $1 \notin I$ und $b \in I$. Nach Lemma 2.14 gibt es einen Homomorphismus $h : \mathcal{A} \to \mathbb{B}$ mit $I = kern(h)$. Für die Belegung $g' := h \circ g : Var \to \mathbb{B}$ gilt nach Proposition 2.9

$$[\![\psi]\!]_{g'}^{\mathbb{B}} = [\![\psi]\!]_{(h \circ g)}^{\mathbb{B}} = h([\![\psi]\!]_g^{\mathcal{A}})$$

für alle Formeln ψ. Insbesondere ist $[\![\psi]\!]_{g'}^{\mathbb{B}} = h([\![\psi]\!]_g^{\mathcal{A}}) = h(1^{\mathcal{A}}) = 1^{\mathbb{B}}$ für alle $\psi \in T$, aber $[\![\varphi]\!]_{g'}^{\mathbb{B}} = h([\![\varphi]\!]_g^{\mathcal{A}}) = h(b) = 0^{\mathbb{B}}$, da $b \in I = kern(h)$ war. □

2.5 Anwendungen der Boole'schen Algebra

Wo lassen sich Boole'sche Algebren in der Computerlinguistik anwenden? Da sich diese Theorie aus den Vorstellungen des Aristoteles über die Grundaussagen der (griechischen) Sprache entwickelt hat, erinnern wir zunächst daran, daß die Operationen $+$, $\cdot$ und $^{-}$ die umgangssprachlichen Aussagejunktoren „oder“, „und“ und „nicht“ interpretieren können.

Daneben können zumindest „und“ und „oder“ auch Ausdrücke anderer syntaktischer Art verbinden, etwa Verben, Nomina, Adjektive, Nominalphrasen, Verbalphrasen usw., und die Komplementbildung $^{-}$ findet man etwa bei der Bildung von Adjektiven und Nomina als Präfix, z.B. in „*un*schön", „*Un*tiefe".

Interpretiert man Verben, Nomina und Adjektive durch Relationen und Mengen von Objekten aus einer Menge M, so entsprechen den sprachlichen Koordinationspartikeln die Operationen $+, \cdot, ^{-}$ in gewissen Boole'schen Algebren der Form 2^M oder $2^{M\times M}$ oder Unteralgebren hiervon.

Hierbei spielen allem Anschein nach auch die in den Axiomen ausgedrückten Eigenschaften eine wichtige Rolle, insbesondere die Distributivgesetze. In vielen Fällen lassen sich Koordinierungen von Ausdrücken als „Abkürzungen" von Satzkoordinierungen verstehen:

Beispiel 2.20 Anwendungen von $(a + b)c = ac + bc$ bzw. $c(a + b) = ca + cb$:

(a)		Fritz will ((einen Aufsatz oder ein Buch) lesen)
	$\mapsto$	Fritz will ((einen Aufsatz lesen) oder (ein Buch lesen))
	$\mapsto$	(Fritz will einen Aufsatz lesen) oder (Fritz will ein Buch lesen)
(b)		(Intelligente (Männer und Frauen)) wissen es
	$\mapsto$	((intelligente Männer) und (intelligente Frauen)) wissen es
	$\mapsto$	((intelligente Männer wissen es) und (intelligente Frauen wissen es))

Bemerkung 2.21 Es gibt neben dem Boole'schen *und* auch ein „sequentielles" *und (dann)*, das z.B. nicht kommutativ ist:

	Er ((öffnete das Fenster) und (spuckte [dann] hinaus)
$\mapsto$	(Er öffnete das Fenster) und ([dann] (spuckte er hinaus))
$\neq$	Er ((spuckte zum Fenster hinaus) und (öffnete es))

Dieses sequentielle „und" wird normalerweise in Befehlen benutzt, wie im Neuen Testament: *Steh auf, nimm dein Bett, und geh!*. In Programmen schreibt man es als Semikolon, wie in $x := y + x\,;\, y := 0$.

Man kann nun das Rechnen mit Gleichungen zwischen Boole'schen Termen benutzen, um die Wahrheit von Aussagen einfacher Form nachzuprüfen. Boole hatte bemerkt, daß man die „kategorischen" Aussagen des Aristoteles durch (Un-)Gleichungen zwischen Mengen ausdrücken kann:

Aussageform	Aristotelisch	Boole'sch	quantorenlogisch
Alle A sind B	$A\,a\,B$	$A \cdot \overline{B} = 0$	$\forall x(A(x) \to B(x))$
Einige A sind keine B	$A\,o\,B$	$A \cdot \overline{B} \neq 0$	$\exists x(A(x) \wedge \neg B(x))$
Alle A sind keine B	$A\,e\,B$	$A \cdot B = 0$	$\forall x(A(x) \to \neg B(x))$
Einige A sind B	$A\,i\,B$	$A \cdot B \neq 0$	$\exists x(A(x) \wedge B(x))$

Aristotes hatte in seiner Logik untersucht, welche Aussagen der Form

$$\alpha \wedge \beta \to \gamma$$

mit kategorischen Aussagen α, β, γ logisch allgemeingültig sind. Dies sind seine *Syllogismen*. Der Syllogismus „B$\underline{\text{a}}$rb$\underline{\text{a}}$r$\underline{\text{a}}$" ist die *Tautologie*

$$A\,a\,B \wedge B\,a\,C \;\rightarrow\; A\,a\,C$$

und nicht, wie man seit Boethius (ca 400 n.Chr.) meint, die *Schlußregel*

$$\frac{\begin{array}{c}A\,a\,B\\ B\,a\,C\end{array}}{A\,a\,C}\,.$$

Die Schlußregel ist schwächer, da sie nur besagt: wenn die Obersätze *beweisbar* (bzw. bewiesen) sind, ist auch der Untersatz beweisbar (bzw. bewiesen).