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

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 zu $\mathcal{A}$ *duale* Algebra $\widetilde{\mathcal{A}} := (A, \cdot^A, +^A, -^A, 1^A, 0^A)$, die aus $\mathcal{A}$ durch Vertauschen von $+$ und $\cdot$ sowie von 0 und 1 entsteht, 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

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

definiert sind, eine Boole'sche Algebra.

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.

□

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

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

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

$$a \leq b : \Longleftrightarrow\ a + b = b \tag{1}$$

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 Ist $\mathcal{A}$ eine Boole'sche Algebra und $\leq^A$ die nach (1) 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 □

Nimmt man in (1) statt $+$ die Multiplikation $\cdot$, so erhält man ebenfalls eine partielle Ordnung,

$$a \geq b : \Longleftrightarrow \; a \cdot b = b. \tag{2}$$

In der Potenzmengenalgebra 2^M ist die nach (1) definierte partielle Ordnung die Teilmengenbeziehung, die nach (2) 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

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

□

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.