2.2 Ideale und Homomorphismen

Definition 2.9 Ein *Ideal* I der Boole'schen Algebra $\mathcal{A}$ ist eine nicht-leere Teilmenge $I \subseteq A$, 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 2.10 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

$$a \sim_I b :\Longleftrightarrow \exists a' \in I\ \exists b' \in I\ (a + a' = b + b'). \tag{3}$$

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

$$\begin{aligned}
0^B &:= [0]_I, \\
1^B &:= [1]_I \\
[a]_I +^B [c]_I &:= [a+c]_I && (4)\\
[a]_I \cdot^B [c]_I &:= [a \cdot c]_I && (5)\\
\overline{[a]_I}^B &:= [\overline{a}]_I && (6)
\end{aligned}$$

Damit dies wohldefiniert ist, also die rechten Seiten von (4) – (6) 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 $I = \mathit{kern}(h)$ ist. Für $I \subseteq \mathit{kern}(h)$ 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. $a \in \mathit{kern}(h)$. Ist umgekehrt $a \in \mathit{kern}(h)$, 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 $a \in I$. $\square$

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 2.11 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 2.12 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 2.13 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) $I = \mathit{kern}(h)$ 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 $h(a \cdot b) = 1$. Ist $h(a) = 0 = h(b)$, so ist $a + b \in I$, da I ein Ideal ist, also $h(a + b) = 0$.

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

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

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

(c) $\Rightarrow$ (d): (wird nachgetragen)

(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. $\Box$

Lemma 2.14 (Zorn'sches Lemma) Sei $(M, \leq)$ eine partielle Ordnung. Wenn jede durch $\leq$ total geordnete Teilmenge $K \subseteq M$ 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 2.15 Ist I ein echtes Ideal der Boole'schen Algebra $\mathcal{A}$, so gibt es 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 echtes Ideal $J \subseteq I$. Nach Lemma 2.13 ist J ein Primideal. $\Box$

Satz 2.16 (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 $\overline{a} \notin I$ 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.

$$a \in I \text{ und } b \notin I \quad \text{oder} \quad b \in I \text{ und } a \notin I \qquad \text{für ein Primideal } I. \tag{7}$$

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

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

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 ist hat $M(a,b)$ ein maximales Element, etwa $J(a,b)$. Nach Korollar 2.15 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 (7) gezeigt. □

2.4 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 2.17 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 2.18 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	$A\,a\,B$	$A \cdot \overline{B} = 0$	$\forall x(A(x) \rightarrow B(x))$
Einige A sind keine B	$A\,o\,B$	$A \cdot \overline{B} \neq 0$	$\exists x(A(x) \land \neg B(x))$
Alle A sind keine B	$A\,e\,B$	$A \cdot B = 0$	$\forall x(A(x) \rightarrow \neg B(x))$
Einige A sind B	$A\,i\,B$	$A \cdot B \neq 0$	$\exists x(A(x) \land B(x))$

Aristotes hatte in seiner Logik untersucht, welche Aussagen der Form

$$\alpha \land \beta \rightarrow \gamma$$

mit kategorischen Aussagen α, β, γ logisch allgemeingültig sind. Dies sind seine *Syllogismen*. Der Syllogismus „B<u>a</u>rb<u>a</u>r<u>a</u>“ ist die *Tautologie*

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

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).