Diskrete Strukturen und Logik

WiSe 2006/07 in Trier

Henning Fernau
Universität Trier
fernau@informatik.uni-trier.de

Diskrete Strukturen und Logik Gesamtübersicht

- Organisatorisches
- Einführung
- Logik & Mengenlehre
- Beweisverfahren
- Kombinatorik: Die Kunst des Zählens
- algebraische Strukturen

Boolesche Algebren

Syntax (Aussehen)

Eine *Boolesche Algebra* ist beschrieben durch ein 6-Tupel $\mathcal{B} = (\mathrm{B}, \oplus, \otimes, \kappa, 0, 1)$:

B: Grundmenge

$\oplus, \otimes : \mathrm{B} \times \mathrm{B} \to \mathrm{B}$: zweistellige Verknüpfungen auf B

$\oplus$: *Addition*; $\otimes$: *Multiplikation*

$\kappa : \mathrm{B} \to \mathrm{B}$: einstellige Operation auf B: *Komplement*

$0, 1 \in \mathrm{B}$: Konstanten (nullstellige Operationen)

Boolesche Algebren: geforderte Eigenschaften

$0 \neq 1$
Kommutativgesetze: (1) $\forall a, b \in B : a \oplus b = b \oplus a$, (2) $\forall a, b \in B : a \otimes b = b \otimes a$.
Distributivgesetze: (1) $\forall a, b, c \in B : a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ und (2) $\forall a, b, c \in B : a \oplus (b \otimes c) = (a \oplus b) \otimes (a \oplus c)$
Neutralitätsgesetze: (1) 0 ist *rechtsneutrales Element* bzgl. $\oplus$, d.h.: $a \oplus 0 = a$ und (2) 1 ist *rechtsneutrales Element* bzgl. $\otimes$, d.h.: $a \otimes 1 = a$
Komplementgesetze: (1) $\kappa(a)$ ist das *Komplement* von a, d.h.: (1) $a \oplus \kappa(a) = 1$ und (2) $a \otimes \kappa(a) = 0$.

0 heiß auch *Nullelement*, 1 *Einselement* von $\mathcal{B}$.

Boolesche Algebren: ein Beispiel

$(\{w, f\}, \vee, \wedge, \bar{\ }, f, w)$ ist eine Boolesche Algebra.
In der Schreibweise
$(\{0, 1\}, +, \cdot, \bar{\ }, 0, 1)$ heißt sie auch *Schaltalgebra*.

Satz: Die Schaltalgebra ist (bis auf Isomorphie) die kleinste Boolesche Algebra.

Beweis: Die Eigenschaften einer Booleschen Algebra sind für die Schaltalgebra bekannt.
Da $0 \neq 1$ stets zwei verschiedene Elemente mit definierten Eigenschaften sind, folgt die Minimalität und Eindeutigkeit.

$\leadsto$ Unsere Theorie hat ein Modell (ist also nicht leer) !

Potenzmengenalgebren: ein weiteres Beispiel

Aus unserer 8. Vorlesung wissen wir:
Satz: Für jede Menge $M \neq \emptyset$ bildet $(2^M, \cup, \cap, \bar{\ }, \emptyset, M)$ eine Boolesche Algebra, die so genannte *Potenzmengenalgebra* (über M). (Das Komplement ist bezüglich M zu verstehen.)

Beweis: Möglicherweise noch unbekannt: das Komplementgesetz. Das bedeutet jetzt für $A \subseteq M$: $A \cup \bar{A} = M$ und $A \cap \bar{A} = \emptyset$.

Satz: Die Potenzmengenalgebra einer einelementigen Menge ist isomorph zur Schaltalgebra.

Boolesche Algebren: Teileralgebra als Beispiel

$T(n) = \{k \in \mathbb{N} \mid k|n\}$: Teiler von n.
$\mathrm{kgV}(a, b)$: das kleinste gemeinsame Vielfache von a und b
$\mathrm{ggT}(a, b)$: der größte gemeinsame Teiler von a und b
Erinnerung: $\mathrm{kgV}(a, b) = ab/\,\mathrm{ggT}(a, b)$; $((t|a) \wedge (t'|a')) \implies (\mathrm{ggT}(t, t')|\,\mathrm{ggT}(a, a'))$.
Definiere für $a \in T(n)$: $u_n(a) := n/a$.

Problem: Ist, für $n \geq 2$, $\mathcal{T}(n) = (T(n), \mathrm{ggT}, \mathrm{kgV}, u_n, n, 1)$ stets eine Boolesche Algebra ?
Beachte fehlerhafte Benennung der neutralen Elemente im M/M.
Wenn ja, nennen wir sie *Teileralgebra*.
Beobachte: Die betrachtete Schaltalgebra ist zu $\mathcal{T}(2)$ isomorph:
$\mathrm{ggT}(1, 1) = \mathrm{ggT}(1, 2) = \mathrm{ggT}(2, 1) = 1$, $\mathrm{ggT}(2, 2) = 2$.
$\mathrm{kgV}(1, 1) = 1$, $\mathrm{kgV}(1, 2) = \mathrm{kgV}(2, 1) = \mathrm{kgV}(2, 2) = 2$.

Überprüfe geforderte Eigenschaften

$0 \neq 1$: Da $n \geq 2$, gilt $1 \neq n$. ✓

Kommutativgesetze: (1) $\forall a, b \in B : a \oplus b = b \oplus a$, (2) $\forall a, b \in B : a \otimes b = b \otimes a$. Nach Def. von kgV und ggT kommt es offenbar nicht auf die Reihenfolge der Argumente an. ✓

Neutralitätsgesetze: (1) 0 ist *rechtsneutrales Element* bzgl. $\oplus$, d.h.: $a \oplus 0 = a$ und (2) 1 ist *rechtsneutrales Element* bzgl. $\otimes$, d.h.: $a \otimes 1 = a$
ad (1): Dies bedeutet in unserem Fall: $\forall a|n : \mathrm{ggT}(a, n) = a$.
ad (2): Dies bedeutet in unserem Fall: $\forall a|n : \mathrm{kgV}(a, 1) = a$.✓

Überprüfe geforderte Eigenschaften

Distributivgesetze: (1) $\forall a, b, c \in B : a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ und (2) $\forall a, b, c \in B : a \oplus (b \otimes c) = (a \oplus b) \otimes (a \oplus c)$

ad (1): Dies bedeutet in unserem Fall:

$\forall a, b, c \in T(n) : \mathrm{kgV}(a, \mathrm{ggT}(b, c)) = \mathrm{ggT}(\mathrm{kgV}(a, b), \mathrm{kgV}(a, c))$.

$\mathrm{kgV}(a, \mathrm{ggT}(b, c)) = a\,\mathrm{ggT}(b, c)/\,\mathrm{ggT}(a, b, c)$ versus

$\mathrm{ggT}(\mathrm{kgV}(a, b), \mathrm{kgV}(a, c)) = \mathrm{ggT}(ab/\,\mathrm{ggT}(a, b), ac/\,\mathrm{ggT}(a, c))$

Sind diese Ausdücke immer gleich ?? Wir prüfen zunächst Beispiele:

$a = 2$, $b = 6$, $c = 3$:

$\mathrm{kgV}(a, \mathrm{ggT}(b, c)) = \mathrm{kgV}(2, \mathrm{ggT}(6, 3)) = \mathrm{kgV}(2, 3) = 6.$

$\mathrm{ggT}(\mathrm{kgV}(a, b), \mathrm{kgV}(a, c)) = \mathrm{ggT}(\mathrm{kgV}(2, 6), \mathrm{kgV}(2, 3)) = \mathrm{ggT}(6, 6) = 6.$ $\checkmark$

$a = 3$, $b = 6$, $c = 9$:

$\mathrm{kgV}(a, \mathrm{ggT}(b, c)) = \mathrm{kgV}(3, \mathrm{ggT}(6, 9)) = \mathrm{kgV}(3, 3) = 3.$

$\mathrm{ggT}(\mathrm{kgV}(a, b), \mathrm{kgV}(a, c)) = \mathrm{ggT}(\mathrm{kgV}(3, 6), \mathrm{kgV}(3, 9)) = \mathrm{ggT}(6, 9) = 3.$ $\checkmark$

Überprüfe geforderte Eigenschaften: Distributivgesetze (allgemein)

Betrachte Zahl t mit $t| \operatorname{kgV}(a, \operatorname{ggT}(b, c))$.

t lässt sich schreiben als $t = pq$ mit $p|a$ und $q| \operatorname{ggT}(b, c)$.

Wegen $p|a$ gilt: $p| \operatorname{kgV}(a, x)$ für jedes x, und somit $p| \operatorname{ggT}(\operatorname{kgV}(a, b), \operatorname{kgV}(a, c))$.

$q| \operatorname{ggT}(b, c)$. $\rightsquigarrow (q|b) \wedge (q|c) \rightsquigarrow (q| \operatorname{kgV}(a, b)) \wedge (q| \operatorname{kgV}(a, c))$

$\rightsquigarrow t| \operatorname{ggT}(\operatorname{kgV}(a, b), \operatorname{kgV}(a, c))$ mit $t = pq$; insbesondere $t = \operatorname{kgV}(a, \operatorname{ggT}(b, c))$.

$\checkmark$

Umgekehrt: Betrachte Zahl t mit $t| \operatorname{ggT}(\operatorname{kgV}(a, b), \operatorname{kgV}(a, c))$.

Dann gilt: $t| \operatorname{kgV}(a, b)$ und $t| \operatorname{kgV}(a, c)$.

t lässt sich schreiben als $t = pq$ mit $p|a$ und $q|b$.

t lässt sich schreiben als $t = p'q'$ mit $p'|a$ und $q'|c$.

Mit $p'' = \operatorname{kgV}(p, p')$ haben wir eine weitere Darstellung $t = p''q''$ mit $p''|a$.

Aus der Aufteilung der Primfaktoren von t ergibt sich sofort: $q'' = \operatorname{ggT}(q, q')$.

Es gilt: $q''| \operatorname{ggT}(b, c)$, denn $((q|b) \wedge (q'|c)) \implies (\operatorname{ggT}(q, q')| \operatorname{ggT}(b, c))$.

Aus $p''|a$ und $q''| \operatorname{ggT}(b, c)$ folgt für $t = p''q''$: $t| \operatorname{kgV}(a, \operatorname{ggT}(b, c))$. $\checkmark$

Überprüfe geforderte Eigenschaften

Distributivgesetze: (1) $\forall a, b, c \in B : a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ und (2) $\forall a, b, c \in B : a \oplus (b \otimes c) = (a \oplus b) \otimes (a \oplus c)$

ad (2): Dies bedeutet in unserem Fall:

$\forall a, b, c \in T(n) : ggT(a, kgV(b, c)) = kgV(ggT(a, b), ggT(a, c))$.

Der Beweis folgt ganz analog.

Überprüfe geforderte Eigenschaften: Komplementgesetze

(1) $\kappa(a)$ ist das *Komplement* von a, d.h.: (1) $a \oplus \kappa(a) = 1$ und (2) $a \otimes \kappa(a) = 0$.
(1) bedeutet: $\mathrm{ggT}(a, u_n(a)) = \mathrm{ggT}(a, n/a) = 1$.
Das gilt nur für jedes $a|n$, falls es keine Quadratzahl größer 1 gibt, die n teilt.
(2) sieht man entsprechend.

Alles zusammen genommen zeigen unsere Überlegungen:

Satz: $\mathcal{T}(n)$ ist eine Boolesche Algebra genau dann, wenn es keine Zahl größer 1 gibt, deren Quadrat n teilt.

Ausdruck-Algebra

Erinnerung: Wir hatten früher wohlgeformte aussagenlogische Ausdrücke samt der Belegungsfunktion β betrachtet. Wir nannten zwei w.a.A. α, α' äquivalent, falls $\beta(\alpha) = \beta(\alpha')$.
Es sei A_n die Menge aller Äquivalenzklassen von w.a.A. mit Variablenmenge $X_n = \{x_1, \ldots, x_n\}$.
Die Äquivalenzklasse von α werde $[\alpha]$ notiert.
Definiere: $[\alpha] \sqcup [\alpha'] := [(\alpha) \vee (\alpha')]$, $[\alpha] \sqcap [\alpha'] := [(\alpha) \wedge (\alpha')]$, $C_n([\alpha]) := [\neg\alpha]$.

Satz: Für jedes $n \in \mathbb{N}$ ist $\mathcal{A}_n = (A_n, \sqcup, \sqcap, C_n, [f], [w])$ eine Boolesche Algebra. Diese ist für $n = 0$ zur Schaltalgebra isomorph.

Beweis: Zu überlegen: Wohldefiniertheit.

BAs aus BAs: Funktionenalgebren

Es sei $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ eine Boolesche Algebra.
$B_n := B^{B^n}$ bezeichne die *n-stelligen Booleschen Funktionen*.
Definiere für $f, g \in B_n$ folgende Operationen:
$(f \star g)(x_1, \ldots, x_n) := f(x_1, \ldots, x_n) \oplus g(x_1, \ldots, x_n)$
$(f \odot g)(x_1, \ldots, x_n) := f(x_1, \ldots, x_n) \otimes g(x_1, \ldots, x_n)$
$(\Gamma(f))(x_1, \ldots, x_n) := \kappa(f(x_1, \ldots, x_n))$
0 und 1 sollen der Einfachheit halber auch die n-stelligen Funktionen bezeichnen, die konstant 0 bzw. 1 liefern.
Satz: Für $n \in \mathbb{N}$ ist $\mathcal{B}_n = (B_n, \star, \odot, \Gamma, 0, 1)$ eine Boolesche Algebra. Diese ist für $n = 0$ zu $\mathcal{B}$ isomorph.

Beweis: Tafel

Der Plan für die nächste Zeit:

Wir haben jetzt heute viele Modelle für Boolesche Algebren kennengelernt. Insbesondere für die Schaltalgebra und die Potenzmengenalgebren wissen wir bereits viele weitere Eigenschaften.

Natürliche mathematische Fragen:
— Gelten diese Eigenschaften allgemein ?
— Können wir vielleicht sogar weitere Eigenschaften herausbekommen ?