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 und Ordnungen

Erinnerung: Eine *Boolesche Algebra* $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ erfüllt folgende 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) $a \otimes \kappa(a) = 0$.

Boolesche Algebren und Ordnungen

Erinnerung: Eine *Halbordnung* kann aufgefasst werden als Struktur $(M, \leq)$, wobei $\leq$ eine binäre Relation auf M ist mit folgenden Eigenschaften:

Reflexivität

Transitivität

Antisymmetrie

Boolesche Algebren und Ordnungen

Satz: Auf einer B.A. $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ kann durch $a \leq b$ gdw. $a \oplus b = b$ eine Halbordnung auf B definiert werden (*von B.A. induzierte Halbordnung*).

Beweis: Reflexivität: $x \leq x = x$ bedeutet $x \oplus x = x$ (Idempotenz)

Transitivität: Annahme: $x \leq y$ und $y \leq z$. Das bedeutet:

$x \oplus y = y$ und $y \oplus z = z$ Mit der Assoziativität folgt:

$x \oplus z = x \oplus (y \oplus z) = (x \oplus y) \oplus z = y \oplus z = z$

Also gilt $x \leq z$, w.z.z.w.

Antisymmetrie: Annahme: $x \leq y$ und $y \leq x$, d.h.: $x \oplus y = y$ und $y \oplus x = x$. Wegen der Kommutativität folgt $x = y$.

Boolesche Algebren und Ordnungen

Die Betrachtung der dualen Booleschen Algebra liefert sofort eine weiter Halbordnung $\geq$ auf B. Also: $x \geq y$ gdw. $x \otimes y = y$.

Satz: $\forall x, y \in B : (x \leq y) \iff (y \geq x)$.

Beweis: Es gelte $x \leq y$, d.h.: $x \oplus y = y$.

Absorptionsgesetz $\rightsquigarrow x \otimes (x \oplus y) = x$, also $x \otimes y = x$ wegen $x \leq y$.

Also folgt $y \geq x$ aus $x \leq y$.

Das Dualitätsprinzip liefert die Umkehrung.

Folgerung: $\forall x, y \in B : (x \leq y) \iff (\kappa(y) \leq \kappa(x))$.

Boolesche Algebren und Ordnungen: Beispiele

Die Potenzmengenalgebra $(2^{\{0,1\}}, \cup, \cap, -, \emptyset, \{0,1\})$ hat als Grundmenge $2^{\{0,1\}} = \{\emptyset, \{0\}, \{1\}, \{0,1\}$.

$\emptyset \leq X$ für alle X, denn $\emptyset \cup X = X$.
$\{0,1\} \geq X$ für alle X, denn $\{0,1\} \cap X = X$ (dual).
$\{0\} \leq X$ gilt nur für $X = \{0\}$ und $X = \{0,1\}$.
$\{1\} \leq X$ gilt nur für $X = \{1\}$ und $X = \{0,1\}$.

Also gilt: $X \leq Y \iff X \subseteq Y$.

Boolesche Algebren: Teileralgebra als Beispiel

Wir wissen: $\mathcal{T}(6) = (\mathrm{T}(6), \mathrm{ggT}, \mathrm{kgV}, u_6, 6, 1)$ ist eine B.A.
Also: $x \leq_\mathrm{T} y$ gdw. $\mathrm{ggT}(x, y) = y$, d.h. $x \leq_\mathrm{T} y$ gdw. $y|x$.
Wir haben den Index T für die Halbordnung benutzt, da wir ja noch eine weitere Halbordnung $\leq$ auf Zahlmengen kennen, nämlich die gewöhnliche lineare.
Beachte: Aus $x \leq_\mathrm{T} y$ folgt $y \leq x$.
Die Umkehrung gilt aber im Allgemeinen nicht, da $\leq_\mathrm{T}$ nicht linear ist.
Veranschaulichung durch Hasse-Diagramme (Tafel).

Boolesche Algebren und Ordnungen: Weitere Eigenschaften

Satz: In der von einer Booleschen Algebra $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ induzierten Halbordnung $\leq$ gibt es stets ein kleinstes und ein größtes Element, nämlich 0 und 1.

Beweis: Dies folgt sofort aus $0 \oplus x = x$ (Neutralitätsgesetz) und $x \oplus 1 = 1$ (Dominanzgesetz).

In unseren Beispielen bedeutet dies:
$\emptyset$ ist das kleinste Element in einer Potenzmengenalgebra und die Gesamtmenge das größte.
6 ist das kleinste Element in der Teileralgebra $\mathcal{T}_6$, und 1 das größte.
Man veranschauliche sich dies wieder durch Hasse-Diagramme (Tafel).

Boolesche Algebren und Ordnungen: Weitere Eigenschaften

Satz: $x \leq y$ gdw. $x \otimes \kappa(y) = 0$ gdw. $\kappa(x) \oplus y = 1$.

Beweis: $x \leq y$ heißt nach Def. $x \oplus y = y$.
Komplementieren der beiden Seiten liefert mit dem De Morganschen Gesetz:
$\kappa(x) \otimes \kappa(y) = \kappa(y)$.
Multiplikation von links mit x liefert:
$x \otimes (\kappa(x) \otimes \kappa(y)) = x \otimes \kappa(y)$.
Das Assoziativitätsgesetz zusammen mit dem Komplementgesetz ergibt:
$0 = x \otimes \kappa(y)$, woraus nach De Morgan $\kappa(x) \oplus y = 1$ folgt.
Die Umkehrung folgt aus $0 = x \otimes \kappa(y)$ durch Addition von y:
$y = 0 \oplus y$ (linke Seite) sowie für die rechte:
$(x \otimes \kappa(y)) \oplus y = (x \oplus y) \otimes (\kappa(y) \oplus y) = (x \oplus y) \otimes 1 = x \oplus y$.
Welche Gesetze wurden verwendet ?

Boolesche Algebren und Ordnungen: Weitere Eigenschaften

Satz: $x \leq y$ gdw. $x \otimes \kappa(y) = 0$ gdw. $\kappa(x) \oplus y = 1$.

Interpretation des Satzes in der Logik:
$\kappa(x) \oplus y = 1$ bedeutet für Aussageformen p und q: $\neg p \vee q \equiv w$.
Daher entspricht $\leq$ z.B. bei der Ausdrucksalgebra der logischen Implikation $\Rightarrow$.
Transitivität der Halbordnung heißt daher: $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$.
Antisymmetrie der Halbordnung bedeutet: $((p \Rightarrow q) \wedge (q \Rightarrow p)) \Rightarrow (p \iff q)$.

Interpretation des Satzes in der Mengenlehre für $A, B \subseteq M$:
$A \subseteq B$ gdw. $A \cap (M \setminus B) = \emptyset$ gdw. $(M \setminus A) \cup B = M$.

Verbände als verallgemeinerte Boolesche Algebren

Eine Struktur $\mathcal{V} = (V; \sqcup, \sqcap)$ heißt *Verband* gdw. $\sqcup$ und $\sqcap$ zweistellige assoziative und kommutative Operationen auf der Grundmenge V sind, für die überdies die folgenden Verschmelzungsgesetze (Absorptionsgesetze) gelten:
$\forall a, b \in V : a \sqcap (a \sqcup b) = a \wedge a \sqcup (a \sqcap b) = a$

Satz: Jede Boolesche Algebra lässt sich als Verband begreifen.

Beispiel: $(\mathbb{R}, \min, \max)$ ist ein Verband, der keiner Booleschen Algebra entspricht.

Beispiel: Ist $(H, \times)$ eine Halbgruppe, so lässt sich auf der Menge aller Unterhalbgruppen durch $(A, B) \mapsto (A \cup B)^*$ (Erzeugnis der Vereinigung) und $(A, B) \mapsto A \cap B$ eine Verbandsstruktur aufprägen.

Wie in Booleschen Algebren gilt auch in Verbänden das *Dualitätsprinzip*.

Nochmal Morphis, Teilstrukturen und Erzeugnisse

Der Verband der Teiler von 6 ist ein Unterverband des Verbands der Teiler von 30.
Jedoch ist die Boolesche Algebra $\mathcal{T}(6)$ *keine* Unteralgebra von $\mathcal{T}(30)$.
Probleme: (1) Die Nullelemente sind verschieden.
(2) Der Komplementoperator von $\mathcal{T}(30)$ führt aus $\mathsf{T}(6)$ heraus: $\mathfrak{u}_{30}(6) = 5$.
Es gilt sogar: Die von $\mathsf{T}(6)$ in $\mathcal{T}(30)$ erzeugte B.A. ist gerade $\mathcal{T}(30)$.
Was ist $\{2\}^*$ in $\mathcal{T}(30)$? Da wir eine Teilalgebra suchen, gilt: $30, 1, 2, \mathfrak{u}_{30}(2) = 15 \in \{2\}^*$.
Überprüfe Abschlusseigenschaften: $\mathrm{ggT}(2, 15) = 1$ und $\mathrm{kgV}(2, 15) = 30$.
Die Unteralgebra $(\{1, 2, 15, 30\}, \mathrm{ggT}, \mathrm{kgV}, \mathfrak{u}_{30}, 30, 1)$ von $\mathcal{T}(30)$ ist zu $\mathcal{T}(6)$ isomorph.
Weitere isomorphe Unteralgebren sind die (B.A.-)Erzeugnisse $\{3\}^*$ und $\{5\}^*$.
Für die Verbandserzeugnisse des Teilerverbandes von 30 gilt hingegen: $\{2\}^* = \{2\}$ usf.

Verbände und Halbordnungen

Tatsächlich braucht man zur Definition einer Halbordnung nicht alle Eigenschaften einer Booleschen Algebra. Eine leichte Analyse des vorigen Beweises zeigt, dass wir nur noch folgendes Lemma zur Verallgemeinerung unserer früheren Aussage benötigen:

Lemma: $\sqcup$ und $\sqcap$ sind idempotente Operationen in einem Verband.

Beweis: Zweimaliges Anwenden des Verschmelzungsgesetzes liefert:
$a \sqcup a = a \sqcup (a \sqcap (a \sqcup b)) = a$.
Die andere Aussage folgt dual.

Satz: Auf einem Verband $\mathcal{V} = (V, \sqcup, \sqcap)$ kann durch $a \leq b$ gdw. $a \sqcup b = b$ eine Halbordnung auf V definiert werden, die *vom Verband induzierte Halbordnung* $H(\mathcal{V})$.

Aussagen über Verbände

Lemma: In einem Verband gilt: $a \leq b$ gdw. $a \sqcap b = a$.

Beweis: Aus $a \sqcap b = a$ folgt $a \sqcup b = (a \sqcap b) \sqcup b = b \sqcup (b \sqcap a) = b$. d.h. $a \leq b$.

Aus $a \sqcup b = b$ folgt $a \sqcap b = a \sqcap (a \sqcup b) = a$.

Lemma: (Verträglichkeit / Monotonie) In einem Verband gilt:

(1) $(a \leq b \wedge c \leq d) \implies ((a \sqcap c) \leq (b \sqcap d))$;

(2) $(a \leq b \wedge c \leq d) \implies ((a \sqcup c) \leq (b \sqcup d))$.

Beweis: $a \leq b$ bzw. $c \leq d$ gdw. $a = a \sqcap b$ bzw. $c = c \sqcap d$.

$\rightsquigarrow a \sqcap c = (a \sqcap b) \sqcap (c \sqcap d) = (a \sqcap c) \sqcap (b \sqcap d) \rightsquigarrow$ Beh. (1)

Beh. (2) zeigt man dual.

Beispiel: Es gibt fünf nicht-isomorphe Verbände über einer 5-elementigen Grundmenge. (Hasse-Diagramme an der Tafel)

Verbände und Halbordnungen

Die von Verbänden (und somit auch die von B.A.) induzierten Halbordnungen haben eine spezielle Eigenschaft:

Satz: Ist $\mathcal{V} = (V, \sqcup, \sqcap)$ ein Verband, so ist $H(\mathcal{V})$ eine Halbordnung, in der je zwei Elemente $a, b \in V$ eine untere Grenze $\inf(a, b)$ und eine obere Grenze $\sup(a, b)$ besitzen. Ferner gilt: $\inf(a, b) = a \sqcap b$ und $\sup(a, b) = a \sqcup b$.

Beweis: $a \sqcap b \leq a$, denn $(a \sqcap b) \sqcap a = a \sqcap (b \sqcap a) = a \sqcap (a \sqcap b) = (a \sqcap a) \sqcap b = a \sqcap b$.

$a \sqcap b \leq b$ analog.

Es sei u eine untere Schranke von $\{a, b\}$, also $u \sqcap a = u$ und $u \sqcap b = u$.

$u \sqcap (a \sqcap b) = (u \sqcap a) \sqcap b = u \sqcap b = u$, also $u \leq a \sqcap b$.

Dual folgen die Aussagen für die obere Grenze.

Verbände und Halbordnungen

Von der letzten Aussage gibt es eine Art Umkehrung:

Satz: Es sei $H = (V, \leq)$ eine Halbordnung, in der je zwei Elemente $a, b \in V$ eine untere Grenze $\inf(a, b)$ und eine obere Grenze $\sup(a, b)$ besitzen. Dann ist $V(H) = (V; \sup, \inf)$ ein Verband.

Beweis: Übungsaufgabe !

In gewissem (wenn auch nicht im strukturellen Sinne) sind daher Verbände und Halbordnungen mit unteren und oberen Grenzen dasselbe.
Es gilt überdies: $H(V(H)) = H$ und $V(H(\mathcal{V})) = \mathcal{V}$.
Ferner sind dann Verbandsmorphismen *ordnungserhaltend*, also Halbordnungsmorphis.

Beachte: $(\mathbb{N}, |)$ ist eine Halbordnung. $\rightsquigarrow (\mathbb{N}, \mathrm{kgV}, \mathrm{ggT})$ Verband.
$\rightsquigarrow \forall n \in \mathbb{N}, n > 0 : (T(n), \mathrm{kgV}, \mathrm{ggT})$ Unterverband.

Distributive Verbände

Gelten in einem Verband auch noch die von B.A. bekannten Distributivgesetze, so nennt man ihn *distributiv*. (Tatsächlich genügt das Einfordern eines der Distributivgesetze aufgrund des mächtigen Verschmelzungsgesetzes.)

Beispiel: $\forall n \in \mathbb{N}, n > 0 : (T(n), ggT, kgV)$ ist distributiver Verband.

Hinweis: Verbände sind nicht notwendig distributiv.
So sind zwei der fünf 5-elementigen Verbände nicht distributiv.
Ganz allgemein ist ein Verband genau dann distributiv, wenn er keinen der beiden genannten nicht-distributiven 5-elementigen Verbände als Teilverband enthält.

Ein Element a in einem distributiven Verband, das nicht kleinstes Element ist, heiß *irreduzibel* oder *unzerlegbar*, falls aus $a = x \sqcup y$ folgt $a = x$ oder $a = y$. (Bsp. Tafel)

Irreduzible Elemente in (distributiven) Verbänden muss es nicht geben

Für $A, B \subseteq \mathbb{N}$ definiere: $A \sim B$ gdw. A und B unterscheiden sich nur in endliche vielen Elementen.

Lemma: $(2^{\mathbb{N}}, \sim)$ ist eine Äquivalenzrelation.

Sei V die Menge der Äquivalenzklassen. $[A]$ sei die ÄK, in der A liegt.

Definiere auf V: $[A] \sqcup [B] := [A \cup B]$ und $[A] \sqcap [B] = [A \cap B]$.

Lemma: $\mathcal{V} = (V, \sqcup, \sqcap)$ ist ein distributiver Verband mit kleinstem Element $0 = [\emptyset]$ und größtem Element $1 = [\mathbb{N}]$.

Beweis: ... vor allem Wohldefiniertheit ...

Lemma: Im betrachteten Verband $\mathcal{V}$ gibt es keine irreduziblen Elemente.

Beweis: Grundidee: $[\mathbb{N}] = [\{n \in \mathbb{N} : 2|n\}] \sqcup [\{n \in \mathbb{N} : \neg(2|n)\}]$.

Wäre nämlich $[A] \neq 0$, so A unendlich, d.h., $A = \{n_0 < n_1 < n_2 < \dots\}$, also

$[A] = [\{n_j : 2|j\}] \sqcup [\{n_j : \neg(2|j)\}]$.

Komplemente in Verbänden

Sei $\mathcal{V} = (V, \sqcup, \sqcap)$ ein Verband mit größtem bzw. kleinstem Element 1 bzw. 0, also z.B. ein endlicher Verband. $y \in V$ heißt ein *Komplement* von $x \in V$ gdw. $x \sqcap y = 0$ und $x \sqcup y = 1$.

Wie an den 5-elementigen Verbänden ersichtlich, muss nicht jedes Element ein Komplement besitzen, und ebensowenig muss ein Komplement eindeutig bestimmt sein.

Satz: In einem distributiven Verband sind Komplemente, so sie existieren, eindeutig bestimmt.

Beweis: Aus $x \sqcap y_1 = x \sqcap y_2 (= 0)$ und $x \sqcup y_1 = x \sqcup y_2 (= 1)$ folgt:
$y_1 = y_1 \sqcup (x \sqcap y_1) = y_1 \sqcup (x \sqcap y_2) = (y_1 \sqcup x) \sqcap (y_1 \sqcup y_2) = (y_2 \sqcup x) \sqcap (y_1 \sqcup y_2) = y_2 \sqcup (x \sqcap y_1) = y_2 \sqcup (x \sqcap y_2) = y_2$.

Komplemente in Verbänden

Besitzt in einem Verband jedes Element ein Komplement, so heißt der Verband *komplementär*.
Ein komplementärer distributiver Verband wird auch *Boolescher Verband* genannt.

Satz: Jede Boolesche Algebra lässt sich als Boolescher Verband begreifen und umgekehrt.

Beweis: Nach den Aussagen der vorigen Vorlesung ist klar: B.A. $\leadsto$ B.V.
Für die Rückrichtung müssten wir die Gültigkeit der Axiome einer B.A. nachweisen, die wir geeignet zu einem vorgelegten B.V. definieren...

Atome in Verbänden

Betrachte einen Verband $\mathcal{V} = (V, \sqcup, \sqcap)$ mit kleinstem Element 0.
$p \in V$, $p \neq 0$, heißt *Atom* gdw. $\forall a \in V : 0 \leq a \leq p \Rightarrow (a = 0 \vee a = p)$.
Der duale Begriff es der eines *Hyperatoms*.

Satz: Es sei $\mathcal{V} = (V, \sqcup, \sqcap)$ ein Boolescher Verband, entsprechend einer B.A. $(V, \sqcup, \sqcap, \kappa, 0, 1)$. Dann ist p Atom gdw. p irreduzibel ist.

Beweis: (1) Es sei p ein Atom und betrachte $p = x \sqcup y$.

Per def. gilt: $x \leq x \sqcup y$. Da $x \sqcup y$ Atom, gilt $x = p$ oder $x = 0$. Falls nun $x = 0$, so $y = p$. Daher gilt: $x = p$ oder $y = p$, d.h., $p = x \sqcup y$ ist unzerlegbar.

(2) Ist p unzerlegbar, so ist zum einen $p \neq 0$.

Angenommen, p wäre kein Atom. Dann gäbe es ein q mit $0 < q < p$ (hierbei: $<:= \leq \cap \neq$).

Damit gilt: $p = q \sqcup p = (q \sqcup p) \sqcap 1 = (q \sqcup p) \sqcap (q \sqcup \kappa(q)) = q \sqcup (p \sqcap \kappa(q))$.

Da p irreduzibel und da $p \neq q$, folgt $p = p \sqcap \kappa(q)$, also $p \leq \kappa(q)$.

Da $\leq$ transitiv, folgt $q \leq \kappa(q)$, also $q = q \sqcap \kappa(q) = 0$ Widerspruch !