UNIVERSITÄT
LEIPZIG

Vorlesung 11 - Distributive Verbände, allgemeine algebraische Strukturen, Boolesche Algebren

# Diskrete Strukturen (WS 2024-25)

Łukasz Grabowski

Mathematisches Institut

- eine geordnete Menge $(M, \leq)$ heißt Verband gdw. für alle $x, y \in M$ wir haben dass $x \vee y$ (infimum) und $x \wedge y$ (supremum) existieren. Z.B. $(P(X), \subseteq)$ ist ein Verband.
- Verband $(M, \leq)$ gibt uns eine Menge mit zwei Operationen $(M, \vee, \wedge)$, die kommutativ, assoziativ, und absorbtiv sind. Umgekehrt jede solche Menge $(M, \vee, \wedge)$ gibt uns ein Verband $(M, \leq)$. D.H. es gibt zwei äquivalente Wege wie mein ein Verband definieren/betrachten kann.

- Distributive Verbände sind solche wo für alle $x, y, z \in M$ gilt

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

und

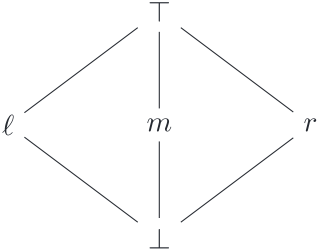
$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$

- Total geordnete Mengen, $(P(X), \subseteq)$ sind distributive Verbände.

- Sei $(V, \vee, \wedge)$ ein Verband. Ein Unterverband ist eine Menge $W \subset V$ mit der Eigenschaft dass für alle $x, y \in W$ haben wir $x \vee y \in W$ und $x \wedge y \in W$.
- Ein Unterverband von $(P(X), \cap, \cup)$ heißt Mengenverband. Mengenverbände sind distributiv.
- VORSICHT: Jede Menge $Q \subset P(X)$ hat eine Ordnungsrelation die sie su einer geordneten Mengen macht. Manchmanl ist so eine Menge $(Q, \subseteq)$ ein Verband, aber kein Unterverband. Z.B. $Q := \{\emptyset, \{1\}, \{1, 2\}, \{3\}, \{1, 2, 3\}\}$.
  - ▶ Es geht darum dass die Operationen $\vee$ and $\wedge$ müssen in einem Unterverband gleich sein als im ursprünglichen Verband.
  - ▶ Also $Q$ is zwar ein Verband aber kein Unterverband von $\mathcal{P}(\{1, 2, 3\}$.

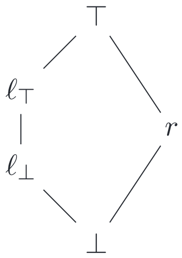
- Wir sagen dass zwei Verbände $(V, \vee, \wedge)$ und $(V', \vee', \wedge')$ sind isomorph gdw. es gibt eine bijektion $\varphi\colon V \to V'$ mit der Eigenschaft dass für alle $x, y \in V$ haben wir $\varphi(x \vee y) = \varphi(x) \vee' \varphi(y)$ und $\varphi(x \wedge y) = \varphi(x) \wedge' \varphi(y)$.
- Äquivalent gesagt, zwei Verbände $(V, \geq)$ und $(V', \geq')$ sind isomporh gdw. es gibt eine bijektion $\varphi\colon V \to V'$ mit der Eigenschaft dass für alle $x, y \in V$ haben wir $x \leq y \iff \varphi(x) \leq' \varphi(y)$.
- Noch anders, äquivalent, gesagt, zwei Verbände sind isomorph, wenn sie "gleiche" Hasse-diagramme haben, wobei "gleiche" bedeutet dass der einzig mögliche Unterschied sind die Namen von Knoten.

- nicht-distributiver Verband $M_3$:




- $\ell \vee (m \wedge r) = l$ und $(\ell \vee m) \wedge (\ell \vee r) = \top$.

- nicht-distributiver Verband $N_5$:




- $\ell_\top \wedge (\ell_\perp \vee r) = \ell_\top$ und $(\ell_\top \wedge \ell_\perp) \vee (\ell_\top \wedge r) = \ell_\perp$.

**Satz.** Sei $\mathcal{V} = (V, \vee, \wedge)$ ein Verband. Dann ist $\mathcal{V}$ distributiv gdw. kein Unterverband von $\mathcal{V}$ isomorph zu den Verbänden $M_3$ oder $N_5$ ist.

**Beweis.**

- Wir zeigen in der Vorlesung nur eine, die "einfache", Richtung. D.h. wir nehmen an, dass es gibt ein Unterverband von $\mathcal{V}$, der entweder zu $M_3$ oder zu $N_5$ isomorph ist.
- Für die andere Richtung, sehe Skript.
- Sei $U \subseteq V$ eine Teilmenge, die ein Unterverband von $V$ ist, und der isomorph zu $M_3$ ist.
- Sei $\varphi\colon V \to M_3$ ein Isomorphismus. Seien $x := \varphi^{-1}(\ell)$, $y := \varphi^{-1}(m)$, $z := \varphi^{-1}(r)$.
- Wir sehen jetzt dass

$$x \vee (y \wedge z) \neq (x \vee y) \wedge (x \vee z).$$

**Satz.** Sei $\mathcal{V} = (V, \vee, \wedge)$ ein Verband. Dann ist $\mathcal{V}$ distributiv gdw. kein Unterverband von $\mathcal{V}$ isomorph zu den Verbänden $M_3$ oder $N_5$ ist.

**Beweis.** (Fortsetzung) In der Tat,

$$\varphi(x \vee (y \wedge z)) = \ell \vee (m \wedge r) = \ell$$

und

$$\varphi((x \vee y) \wedge (x \vee z)) = (\ell \vee m) \wedge (\ell \vee r) = \top.$$

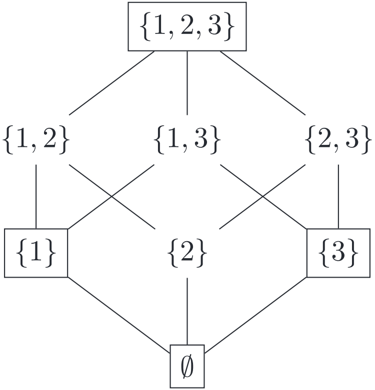
- Ähnilich beweisen wir dass wenn $U$ isomorph zu $N_5$ ist dann auch $\mathcal{V}$ nicht distributivist.

- Motivation: $(U, \leq)$, $(U, \vee, \wedge)$, $(U, \equiv)$,...
- In algemeinen, wenn wir eine algebraische Struktur definieren, benutzen wir
  - $R_1, \ldots, R_k \subseteq U \times U$ Relationen auf $U$,
  - $f_1, \ldots, f_\ell \colon U \times U \to U$ binäre (zweistellige) Funktionen auf $U$,
  - $g_1, \ldots, g_m \colon U \to U$ unäre (einstellige) Funktionen auf $U$ und
  - $c_1, \ldots, c_n \in U$ Elemente (auch: Konstanten) von $U$.
- Wir können so eine algebraische Struktur schreiben als $(U, \langle R_1, \ldots R_k \rangle, \langle f_1, \ldots, f_l \rangle, \langle g_1, \ldots, g_m \rangle, \langle c_1, \ldots, c_n \rangle)$. Wir sagen dass sie des Typs $(k,\ l,\ m,\ n)$ ist.

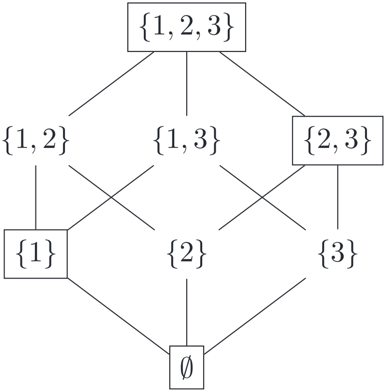
- Jede Äquivalenzrelation $\equiv$ auf $M$ liefert eine algebraische Struktur $(M, \equiv) = \big(M, \langle\equiv\rangle, \langle\rangle, \langle\rangle, \langle\rangle\big)$ des Typs $(1,\ 0,\ 0,\ 0)$.
- Jede teilweise geordnete Menge $(M, \preceq)$ mit einer Relation $\preceq\ \subseteq M \times M$ ist eine algebraische Struktur des Typs $(1, 0, 0, 0)$.
- Jede Potenzmenge $\mathcal{P}(M)$ liefert eine algebraische Struktur $\big(\mathcal{P}(M), \subseteq, \cup, \cap, \cdot^c, \emptyset, M\big)$ des Typs $(1, 2, 1, 2)$.
- Man kann jetzt definieren Isomorphismum von Strukturen, und Unterstrukturen ganz generel (sehe Skript). Diese algemeine Definitionen sind für die Klausur nicht erforderlich. Isomorphismen und Unterstrukturen müssen jedoch in allen von uns untersuchten Sonderfällen verstanden werden.

Wir betrachten den Verband $\mathcal{O} = (\mathcal{P}(\{1, 2, 3\}), \cup, \cap)$.

- keine Unterstruktur:



- Unterstruktur:



- Sei $(M, \preceq)$ ein Verband mit kleinstem Element $\bot$ und größtem Element $\top$ und sei $x \in M$.
- Ein Element $y \in M$ heißt **Komplement** von $x$ gdw. $x \wedge y = \bot$ und $x \vee y = \top$.
- Der Verband $(M, \preceq)$ heißt **komplementiert** gdw. für jedes $x \in M$ ein Komplement $y \in M$ von $x$ existiert.
- Ein Verband $(M, \preceq)$ heißt **Boolesche Algebra** gdw. er distributiv und komplemetiert ist, und zusätzlich $\bot \neq \top$.
- Beispiel: $(P(X), \subseteq)$, $X \neq \emptyset$.
- Die Komplemente sind im Allgemeinen in Verbänden nicht eindeutig. Z.B. das Element $\ell$ im Verband $M_3$ hat die Komplemente $m$ und $r$.

**Satz.** Sei $(M, \preceq)$ ein distributiver Verband mit kleinstem Element $\bot$ und größtem Element $\top$. Für jedes $x \in M$ existiert höchstens ein Komplement von $x$.

**Beweis.** Sei $x \in M$ und seien $y, z \in M$ Komplemente von $x$.

- Wir zeigen erst $y = y \wedge z$:

$$y = \top \wedge y = (x \vee z) \wedge y = (x \wedge y) \vee (z \wedge y) = \bot \vee (z \wedge y) = y \wedge z$$

- Aber auch $z = y \wedge z$:

$$z = \top \wedge z = (x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z) = \bot \vee (y \wedge z) = y \wedge z$$

- Also $y = y \wedge z = z$. □

Boolesche Algebren sind als Modelle der Aussagenlogik entstanden (Komplement ist die Abstraktion der Negation).

- Als Beispiel betrachten wir der Verband der Wahrheitswerte (isomorph zu $\mathcal{P}(\{1\})$): $\big(\{0,\ 1\}, \{(0,0),\ (0,1),\ (1,1)\}\big)$

**Satz.** Sei $(M, \preceq)$ eine Boolesche Algebra mit kleinstem Element $\perp$ und größtem Element $\top$. Dann gelten

- $(x^c)^c = x$ für alle $x \in M$, und
- (Morganische Gesetze) $(x \wedge y)^c = x^c \vee y^c$ und $(x \vee y)^c = x^c \wedge y^c$ für alle $x, y \in M$.

**Beweis.**

- Per Definition ist $(x^c)^c$ das Komplement von $x^c$. Also $(x^c)^c \wedge x^c = \top$ und $(x^c)^c \vee x^c = \perp$. Durch Eindeutigkeit des Komplements es folgt $(x^c)^c = x$.

- Wir zeigen z.B. das Gesetz $(x \vee y)^c = x^c \wedge y^c$.
- Wir zeigen, dass $(x \vee y) \wedge (x^c \wedge y^c) = \bot$ und $(x \vee y) \vee (x^c \wedge y^c) = \top$. Aufgrund der Eindeutigkeit des Komplements ist dann $(x \vee y)^c = x^c \wedge y^c$ bewiesen.
- Es gilt

$$(x \vee y) \wedge (x^c \wedge y^c) = (x \wedge x^c \wedge y^c) \vee (y \wedge x^c \wedge y^c)$$

$$= (\bot \wedge y^c) \vee (\bot \wedge x^c) = \bot \vee \bot = \bot$$

- Es gilt auch

$$(x \vee y) \vee (x^c \wedge y^c) = (x \vee y \vee x^c) \wedge (x \vee y \vee y^c)$$

$$= (\top \vee y) \vee (\top \vee x) = \top \vee \top = \top$$

□

Wie Verbände, lassen sich auch Boolsche Algebren operationell charakterisieren.

**Satz.** Sei $(M, \sqcap, \sqcup, \cdot^*, \bot, \top)$ eine algebraische Struktur des Typs $(0, 2, 1, 2)$, so dass

- $\sqcap$ und $\sqcup$ assoziativ, kommutativ, distributiv und absorptiv sind, und
- Die operation $\cdot^*$ jedes Element $x \in M$ auf sein Komplement abbildet, d.H.

$$x \sqcap x^* = \bot \qquad \text{und} \qquad x \sqcup x^* = \top \ .$$

Dann ist $(M, \preceq)$, mit $x \preceq y$ gdw. $x = x \sqcap y$, eine Boolesche Algebra.

**Beweis.** Folgt aus der Charakterisierung von Verbänden. □

UNIVERSITÄT
LEIPZIG

# VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

**Łukasz Grabowski**
Mathematisches Institut

grabowski@math.uni-leipzig.de