Diskrete Strukturen
Großübung

Amelie Heindl

Lehrstuhl für Logik und Semantik

Technische Universität Berlin

Sommersemester 2024

Themenüberblick

Themenüberblick: Vorlesungswoche 11

- Äquivalenzrelationen
- Quotientenstrukturen
- Ordnungen
- Ketten
- Satz von Dilworth
- Verbände
- Monoide
- Homomorphismen
- Erkennung durch Monoide

Monoide

Monoide: Definitionen

In der Algebra beschäftigt man sich mit sogenannten algebraischen Strukturen, diese bestehen aus einer Menge, sowie Operationen auf den Elementen der Menge. Man unterscheidet verschiedene Arten von Strukturen nach Anzahl und Eigenschaften der Operationen. Wir lernen nun die einfachsten Strukturen kennen.

Magma

Sei M eine Menge und $\circ : M \times M \to M$ eine zweistellige Funktion. Dann ist $(M, \circ)$ ein Magma.

Halbgruppe

Sei $(S, \circ)$ ein Magma und sei $\circ$ assoziativ. Dann ist $(S, \circ)$ eine Halbgruppe.

- Assoziativität bedeutet, dass $(s \circ t) \circ u = s \circ (t \circ u)$ für alle $s, t, u \in S$ gilt.

Monoide: Definitionen

Monoid

Sei $(M, \circ)$ eine Halbgruppe und $e \in M$ ein Element, für das $m \circ e = e \circ m = m$ für alle $m \in M$ gilt. Dann ist $(M, \circ)$ ein Monoid.

- Das Element e wird neutrales Element von M bezüglich $\circ$ genannt.
- Das neutrale Element ist immer eindeutig. Angenommen $e, e' \in M$ wären neutral, dann gilt $e = e \circ e' = e'$.
- Teilweise wird ein Monoid $(M, \circ)$ auch als 3-Tupel $(M, \circ, e)$ angegeben oder nur mit M bezeichnet.
- Die Funktion wird meist in Infixnotation verwendet, also $s \circ t$ anstelle von $\circ(s, t)$ mit $s, t \in M$.
- Normalerweise bezeichnet man die Funktion als Operation oder Verknüpfung.

Monoide: Beispiele

Ist das eine Halbgruppe / ein Monoid?

Menge M	Operation $\circ$	Halbgruppe?	Monoid?
$\mathbb{N}^+$	$\cdot$	Ja	Ja (1 ist neutral)
$\mathbb{N}^+$	$+$	Ja	Nein
$\mathbb{N}$	$+$	Ja	Ja (0 ist neutral)
$\mathbb{N}$	$-$	Nein	Nein
$\mathbb{Z}$	$-$	Ja	Nein
$\mathbb{Z}$	min	Ja	Nein
$\mathbb{N}$	$\circ(a,b) := a^b$	Nein	Nein
$\mathscr{P}(\{a,b,c\})$	$\cup$	Ja	Ja ($\emptyset$ ist neutral)
$\{f : \mathbb{Z} \to \mathbb{Z} \mid f \text{ ist Funktion}\}$	Verkettung	Ja	Ja (id ist neutral)

Monoide: Grundlagen

Viele der grundlegenden Zahlenbereiche und Rechenarten bilden ein Monoid (beispielsweise $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ und $\mathbb{R}$ jeweils mit $+$ und $\cdot$).

Erkenntnisse über Monoide lassen sich damit in all diesen Zahlbereichen verwenden.

Es gibt auch abstrakte Monoide, die keinen bekannten Zahlenereich darstellen.

Beispiel: Sei $M = \{a, b, c, d\}$. Mit der Verknüpfung $\circ$, die durch folgende Verknüpfungstabelle gegeben ist, bildet $(M, \circ, a)$ ein Monoid:

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Monoide: Freie Monoide

Freie Monoide stellen einen Spezialfall von Monoiden dar.

Freies Monoid

Sei $(M, \circ)$ ein Monoid und $A \subset M$ eine Teilmenge. Dann heißt M frei über A, wenn sich jedes Element $m \in M$ eindeutig als Produkt $m = a_1 \circ a_2 \ldots \circ a_n$ darstellen lässt mit $a_1, \ldots, a_n \in A$.

Umgekehrt kann man auch zu jeder Menge A ein freies Monoid definieren.
In der Informatik betrachtet man hierbei vor Allem endliche Mengen A, diese werden dann auch Alphabet genannt.
Das freie Monoid $(A^*, \circ)$ zu A bildet man dann, indem man $A^* = \bigcup_{n \in \mathbb{N}} A^n$ als Menge wählt und die Konkatenation als Verknüpfung $\circ$. A^n enthält dabei alle n-elementigen Tupel von Elementen aus A (bzw. alle Wörter der Länge n mit Buchstaben aus A). Das leere Wort stellt das neutrale Element dar.

Homomorphismen

Homomorphismen: Grundlagen

Nun wären wir gerne in der Lage, Ähnlichkeiten zwischen algebraischen Strukturen feststellen zu können. Hierfür sind Morphismen (strukturerhaltende Abbildungen) nützlich.

Monoidhomomorphismus

Seien $(M_1, \circ_1)$ und $(M_2, \circ_2)$ Monoide. Sei $h : M_1 \to M_2$ eine Abbildung. Dann ist h ein Monoidhomomorphismus, falls

$$h(m \circ_1 m') = h(m) \circ_2 h(m')$$

für alle $m, m' \in M_1$ gilt.

Ein Homomorphismus ermöglicht es also, die Elemente eines Monoids auf die eines anderen Monoids abzubilden, wobei die "Verknüpfungseigenschaften" sich nicht ändern.

Homomorphismen: Grundlagen

- Neben Monoidhomomorphismen, kann man auch Homomorphismen für andere algebraische Strukturen (z.B. Gruppen) definieren.
- Für Mengen ist eine Homomorphismusdefinition nicht hilfreich, da es keine strukturellen Eigenschaften gibt, die erhalten werden könnten.
- Es gibt noch weitere Morphismen, die Spezialfälle von Homomorphismen, die weitere spezielle Eigenschaften erfüllen.

Monomorphismen	Injektive Homomorphismen
Epimorphismen	Surjektive Homomorphismen
Endomorphismen	Homomorphismen, bei denen Bildbereich und Definitionsbereich gleich sind
Isomorphismen	Bijektive Homomorphismen
Automorphismen	Bijektive Endomorphismen

Homomorphismen: Beispiel I

Wir betrachten die Monoide $(\{a,b\}^*, \circ, \varepsilon)$ und $(\mathbb{N}, +, 0)$, wobei $\circ$ die Konkatenation und ε das leere Wort ist. Wir definieren wir die Abbildung

$$h : \{a,b\}^* \to \mathbb{N}$$
$$w \mapsto |w|$$

h bildet also ein Wort auf seine Länge ab.
Nun wollen wir zeigen, dass h ein Homomorphismus ist.

- Es gilt $h(\varepsilon) = |\varepsilon| = 0$, somit ist die erste Bedingung erfüllt.
- Es gilt $h(w \circ w') = |w \circ w'| = |w| + |w'| = h(w) + h(w')$, somit ist die zweite Bedingung erfüllt.

Homomorphismen: Beispiele II

Ist das ein Monoidhomomorphismus?

Erstes Monoid	Zweites Monoid	Funktion h	Homomorphismus?
$(\mathbb{N}, +, 0)$	$(\mathbb{N}, +, 0)$	$n \mapsto n$	Ja
$(\mathbb{N}, +, 0)$	$(\mathbb{Z}, +, 0)$	$n \mapsto n$	Ja
$(\mathbb{Z}, \cdot, 1)$	$(\mathbb{Z}, +, 0)$	$z \mapsto 1$	Nein
$(\mathbb{N}, \cdot, 1)$	$(\{0,1\}, \cdot, 1)$	$n \mapsto n \bmod 2$	Ja
$(\mathbb{R}, +, 0)$	$(\mathbb{R}, \cdot, 1)$	$r \mapsto e^r$	Ja

Ordnungen

Ordnungen: Relationen

Vorletzte Woche haben wir Relationen betrachtet und die Eigenschaften, die sie Erfüllen müssen, um eine Äquivalenzrelation zu sein. Nun wollen wir eine weitere Art spezieller Relationen kennenlernen, die Ordnungsrelation, die andere Eigenschaften erfüllt.

Seien im Folgenden M eine Menge und $R \subseteq M \times M$ eine binäre Relation.

- Irreflexivität: R ist irreflexiv, falls $(m, m) \notin R$ für alle $m \in M$ gilt.
- Antisymmetrie: R ist antisymmetrisch, falls für alle $m, n \in M$ mit $m \neq n$ gilt, dass wenn $(m, n) \in R$ gilt, auch $(n, m) \notin R$ gilt.

Nun können wir Ordnungsrelationen definieren, die die Elemente einer Menge vergleichen und Ordnen sollen.

Ordnungen: Grundlagen

Partielle Ordnung

Sei M eine Menge und $R \subseteq M \times M$ eine Relation. Wenn R reflexiv, transitiv und antisymmetrisch ist, heißt R partielle Ordnung.

Strikte Partielle Ordnung

Sei M eine Menge und $R \subseteq M \times M$ eine Relation. Wenn R irreflexiv, transitiv und antisymmetrisch ist, heißt R strikte partielle Ordnung.

Ordnungen $R \subseteq M \times M$, für die entweder $(m, n) \in R$ oder $(n, m) \in R$ gilt, heißen lineare Ordnungen. In linearen Ordnungen sind also alle Elemente "vergleichbar".

Eine Menge M bildet mit einer auf ihr definierten partiellen Ordnung $\sqsubseteq$ eine Struktur $(M, \sqsubseteq)$, die partiell geordnete Menge genannt wird (oder poset nach dem englishen Ausdruck **p**artially **o**rdered **set**).

Ordnungen: Beispiele I

Partielle Ordnungen sind reflexiv, transitiv und antisymmetrisch.
Strikte partielle Ordnungen sind irreflexiv, transitiv und antisymmetrisch.

Ist das eine Ordnungsrelation?

Menge M	Relation R	Partielle Ordnung?	Strikte?
$\mathbb{N}$	$\leq$	Ja	Nein
$\mathbb{Z}$	$<$	Nein	Ja
$\mathbb{N}$	$\mid$	Ja	Nein
$\mathbb{Q}$	$=$	Nein	Nein
$\{a, b, c\}^*$	'Präfix sein von'	Ja	Nein
$\mathscr{P}(\{1, 2, 3, 4\})$	$\subsetneq$	Nein	Ja
DS Hausaufgaben Abgaben	'mehr Punkte erreicht als'	Nein	Ja

Ordnungen: Darstellung

Partielle Ordnungen lassen sich graphisch darstellen in Form von Hasse-Diagrammen. Dafür brauchen wir noch ein paar Definitionen.

Sei $(M, \sqsubseteq)$ eine partiell geordnete Menge und $m, m' \in M$ mit $m \neq m'$.

- $m \in M$ heißt Vorgänger von $m' \in M$, wenn $m \sqsubseteq m'$ gilt und kein Element $w \in M$ existiert mit $m \sqsubseteq w \sqsubseteq m'$ und $m \neq w \neq m'$.
- $m \in M$ heißt Nachfolger von $m' \in M$, wenn $m' \sqsubseteq m$ gilt und kein Element $w \in M$ existiert mit $m' \sqsubseteq w \sqsubseteq m$ und $m \neq w \neq m'$.

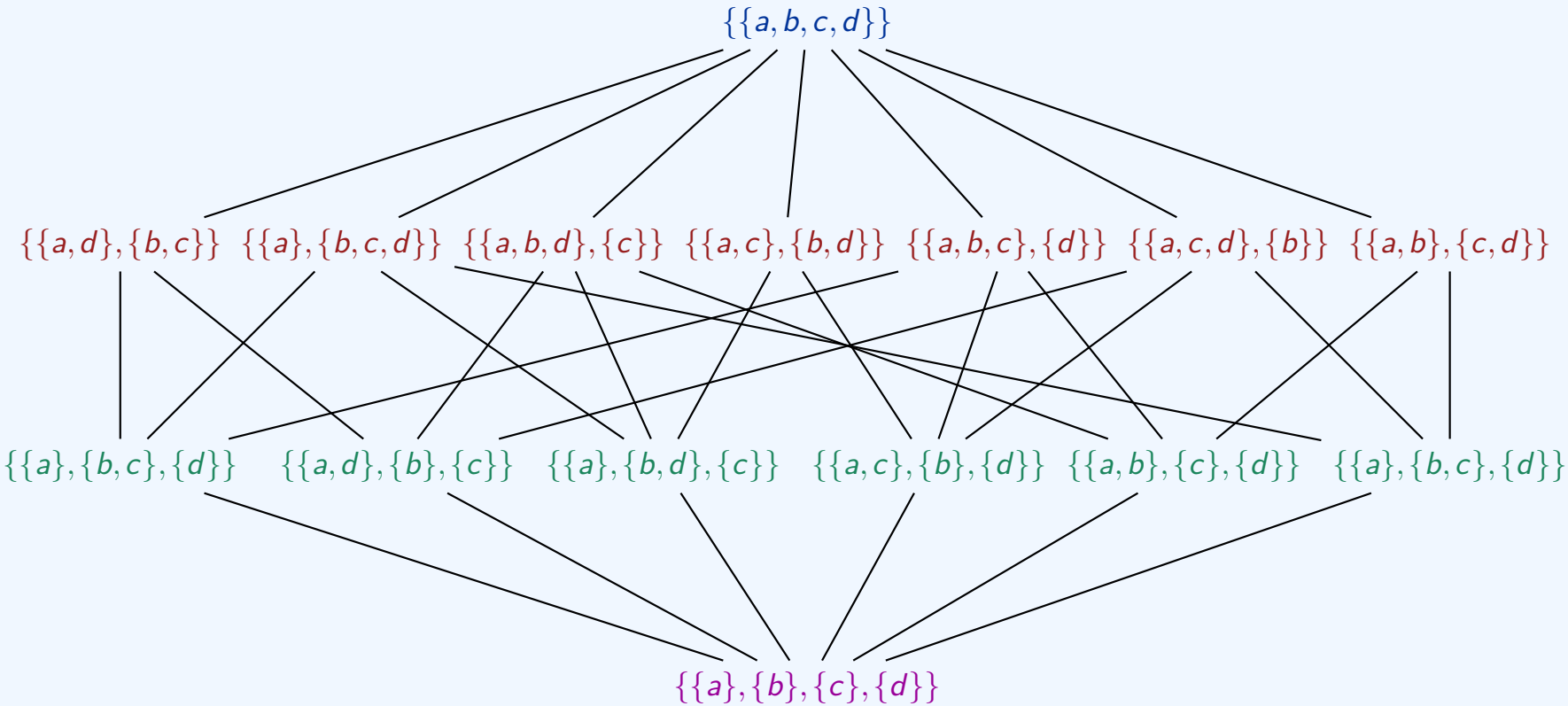
Vorgänger und Nachfolger folgen in der Ordnung also direkt aufeinander.

Ein Hasse-Diagramm für $(M, \sqsubseteq)$ wird nun erstellt, indem alle Elemente aus M aufgezeichnet werden und ein jedes Element mit seinen Nachfolgern verbunden wird. Zusätzlich sollen die Elemente dabei so angeordnet werden, dass alle Kanten von Vorgänger zu Nachfolger nach oben verlaufen.

Ordnungen: Beispiel II

Betrachten wir die Menge M aller Partitionen der Menge $\{a, b, c, d\}$. Nun definieren wir die Ordnungsrelation $\sqsubseteq$ durch: Für alle $m, m' \in M$ gilt $m \sqsubseteq m'$ genau dann, wenn für alle $s \in m$ ein $s' \in m'$ existiert mit $s \subseteq s'$ (also wenn die Partition m die Partition m' "verfeinert").

Dann ergibt sich folgendes Hasse-Diagramm:



Verbände

Verbände: Grundlagen

Nun wollen wir noch Verbände betrachten, die einen Spezialfall von Partiell geordneten Mengen darstellen.
Dafür brauchen wir folgende Definitionen. Sei $(M, \sqsubseteq)$ ein poset und seien $m, m' \in M$.

- Ein Element $s \in M$ ist eine obere Schranke für m, m', wenn $m \sqsubseteq s$ und $m' \sqsubseteq s$ gilt.
- Ein Element $s \in M$ ist eine untere Schranke für m, m', wenn $s \sqsubseteq m$ und $s \sqsubseteq m'$ gilt.
- Ein Element $s \in M$ ist ein Supremum für m, m', wenn s eine obere Schranke für m, m' ist und $s \sqsubseteq s'$ gilt für jede obere Schranke s' von m, m'.
- Ein Element $s \in M$ ist ein Infimum für m, m', wenn s eine untere Schranke für m, m' ist und $s' \sqsubseteq s$ gilt für jede untere Schranke s' von m, m'.

Verbände: Definition

Verband

Sei $(M, \sqsubseteq)$ eine partiell geordnete Menge. Falls es für alle Elemente $m, m' \in M$ ein Infimum und ein Supremum gibt, ist $(M, \sqsubseteq)$ ein Verband.

Da Verbände insbesondere auch partiell geordnete Mengen sind, lassen sie sich auch in Form von Hasse-Diagrammen darstellen.

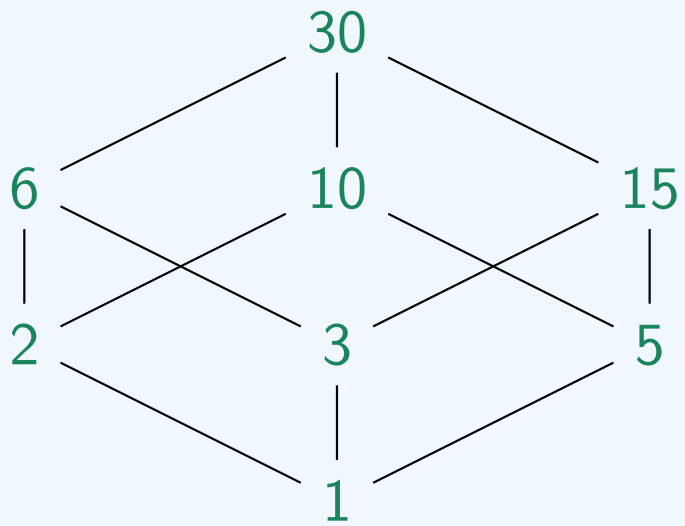
Besonders interessant an Verbänden ist, dass sie sich sowohl als Ordnungsstruktur (unsere Definition) als auch als algebraische Struktur mit zwei Verknüpfungen, die bestimmte Bedingungen erfüllen, definieren lassen.

Verbände: Beispiel I

Wir betrachten die Menge $M := \{n \in \mathbb{N}^+ \mid n|30\}$ aller Teiler von 30 und die partielle Ordnung $|$.

Für zwei Zahlen $m, n \in M$ ist das Supremum bezüglich $|$ stets $\mathrm{kgV}\{m, n\}$ und das Infimum $\mathrm{ggT}\{m, n\}$.

$(M, |)$ bildet einen Verband und lässt sich darstellen als:

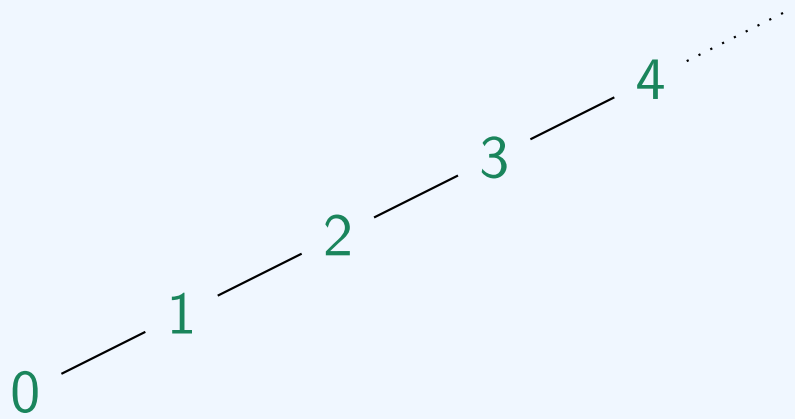


Verbände: Beispiel II

Wir betrachten die Menge $\mathbb{N}$ der natürlichen Zahlen und die partielle Ordnung $\leq$.

Für zwei Zahlen $m, n \in \mathbb{N}$ ist das Supremum bezüglich $\leq$ stets $\max\{m, n\}$ und das Infimum $\min\{m, n\}$.

$(\mathbb{N}, \leq)$ bildet einen Verband und lässt sich darstellen als:



Feedback, Fragen und Vorschläge zur Großübung gerne an:

a.heindl@tu-berlin.de