Diskrete Strukturen

Vorlesung 10: Boolesche Algebren und Gruppen

18. Dezember 2018

Organisation

Bonusserie und alte Prüfungen:

- werden wir noch diese Woche publizieren

Organisation

Bonusserie und alte Prüfungen:

- werden wir noch diese Woche publizieren

Prüfung:

- Freitag, den 22. Februar 2019 von 10–11 Uhr
  im AudiMax, HS 3, HS 9
- Abmeldungen noch bis zum 12. Januar 2019, 9 Uhr möglich
- schriftlich, 60 min
- Hilfsmittel: nur ein beschriebenes oder bedrucktes DIN-A4-Blatt

Nächste Termine — Modul “Diskrete Strukturen”

Hörsaalübung (Mo. 9:15)	Vorlesung (Di. 17:15)
17.12. Hörsaalübung 5. Übungswoche	18.12. Boolesche Algebren, Gruppen
24.12. Frohe Weihnachten	25.12. Frohe Weihnachten
31.12. Guten Rutsch	1.1. Gesundes Neues
7.1.	8.1. Körper (5. Abgabe + 6. Übungsblatt)
14.1. Hörsaalübung 6. Übungswoche	15.1. Graphen und Bäume
21.1.	22.1. Planarität von Graphen (6. Abgabe + 7. Übungsblatt)
28.1. Hörsaalübung 7. Übungswoche	29.1. Färbbarkeit von Graphen
4.2. Tutorium (Klausurvorbereitung)	5.2. Arithmetik

Vorlesungsstruktur

1. Mathematische Grundlagen
   - Aussagen- und Prädikatenlogik
   - Naive Mengenlehre
   - Relationen und Funktionen
2. Diskrete Strukturen
   - Algebraische Strukturen
   - Bäume und Graphen
   - Arithmetik

Heutige Vorlesung

- Eigenschaften von Booleschen Algebren
- Atome und Isomorphiesatz
- Definition kommutative Gruppe
- Grundlegende Eigenschaften von kommutativen Gruppen

Bitte Fragen direkt stellen!

Definition (§9.9 Komplement und Boolesche Algebra)

Sei $(M, \preceq)$ ein Verband mit kleinstem Element $\perp$ (von M) und größtem Element $\top$ (von M).

- Sei $x \in M$. Ein Element $y \in M$ heißt Komplement von x gdw. $x \wedge y = \perp$ und $x \vee y = \top$.

Definition (§9.9 Komplement und Boolesche Algebra)

Sei $(M, \preceq)$ ein Verband mit kleinstem Element $\bot$ (von M) und größtem Element $\top$ (von M).

- 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.

Definition (§9.9 Komplement und Boolesche Algebra)

Sei $(M, \preceq)$ ein Verband mit kleinstem Element $\bot$ (von M) und größtem Element $\top$ (von M).

- 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.
- Der Verband $(M, \preceq)$ heißt Boolesche Algebra gdw. er komplementiert und distributiv ist und $\bot \neq \top$ gilt.

§10.1 Definition (Atom)

Sei $(M, \preceq)$ eine Boolesche Algebra mit kleinstem Element $\bot$.
Ein Element $x \in M$ ist ein Atom gdw.

- $x \neq \bot$ und
- für alle $y \in M$ mit $y \preceq x$ gilt $y \in \{\bot, x\}$.

§10.1 Definition (Atom)

Sei $(M, \preceq)$ eine Boolesche Algebra mit kleinstem Element $\perp$.
Ein Element $x \in M$ ist ein Atom gdw.

- $x \neq \perp$ und
- für alle $y \in M$ mit $y \preceq x$ gilt $y \in \{\perp, x\}$.

Notizen:

- Atome sind die (direkten) Nachbarn des kleinsten Elements $\perp$ im Hasse-Diagramm
- Atome sind genau die minimalen Elemente in $M \setminus \{\perp\}$

Beispiele

- Boolesche Algebra der Wahrheitswerte

Atome: $\{1\}$ 1 Atom

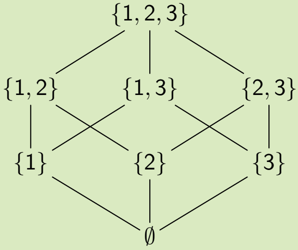
Algebraische Strukturen — Boolesche Algebren

Beispiele

- Boolesche Algebra der Wahrheitswerte

Atome: $\{1\}$ 1 Atom

- Potenzmenge von $M = \{1, 2, 3\}$



Atome: $\{\{1\}, \{2\}, \{3\}\}$ 3 Atome

§10.2 Theorem

Sei $(M, \preceq)$ eine Boolesche Algebra mit endlichem M und kleinstem Element $\perp$. Es gelten:

1. $a \wedge m \in \{\perp, a\}$ für jedes $m \in M$ und jedes Atom $a \in M$
2. $a \wedge b = \perp$ für alle Atome $a, b \in M$ mit $a \neq b$
3. für jedes $m \in M \setminus \{\perp\}$ existiert ein Atom $a \in M$ mit $a \preceq m$

§10.2 Theorem

Sei $(M, \preceq)$ eine Boolesche Algebra mit endlichem M und kleinstem Element $\bot$. Es gelten:

1. $a \wedge m \in \{\bot, a\}$ für jedes $m \in M$ und jedes Atom $a \in M$
2. $a \wedge b = \bot$ für alle Atome $a, b \in M$ mit $a \neq b$
3. für jedes $m \in M \setminus \{\bot\}$ existiert ein Atom $a \in M$ mit $a \preceq m$

Beweis (direkt; 1/2).

1. Offenkundig gilt $a \wedge m \preceq a$. Da a Atom ist, gilt $a \wedge m \in \{\bot, a\}$.

§10.2 Theorem

Sei $(M, \preceq)$ eine Boolesche Algebra mit endlichem M und kleinstem Element $\perp$. Es gelten:

1. $a \wedge m \in \{\perp, a\}$ für jedes $m \in M$ und jedes Atom $a \in M$
2. $a \wedge b = \perp$ für alle Atome $a, b \in M$ mit $a \neq b$
3. für jedes $m \in M \setminus \{\perp\}$ existiert ein Atom $a \in M$ mit $a \preceq m$

Beweis (direkt; 1/2).

1. Offenkundig gilt $a \wedge m \preceq a$. Da a Atom ist, gilt $a \wedge m \in \{\perp, a\}$.
2. Wenn a und b Atome sind, dann folgen aus $a \wedge b \preceq a$ und $a \wedge b \preceq b$ sowohl $a \wedge b \in \{\perp, a\}$ als auch $a \wedge b \in \{\perp, b\}$. Da $a \neq b$, muss $a \wedge b = \perp$ gelten.

Beweis (direkt; 2/2).

3. Sei $m_0 \in M \setminus \{\perp\}$ beliebig.
   - Falls m_0 ein Atom ist, dann gilt $m_0 \preceq m_0$.

Beweis (direkt; 2/2).

3. Sei $m_0 \in M \setminus \{\bot\}$ beliebig.
   - Falls m_0 ein Atom ist, dann gilt $m_0 \preceq m_0$.
   - Falls m_0 kein Atom ist, dann existiert $m_1 \in M$ mit $m_1 \preceq m_0$ und $m_1 \notin \{\bot, m_0\}$. Wir schreiben $x \succ y$ gdw. $y \preceq x$ und $x \neq y$.

Beweis (direkt; 2/2).

3. Sei $m_0 \in M \setminus \{\perp\}$ beliebig.
   - Falls m_0 ein Atom ist, dann gilt $m_0 \preceq m_0$.
   - Falls m_0 kein Atom ist, dann existiert $m_1 \in M$ mit $m_1 \preceq m_0$ und $m_1 \notin \{\perp, m_0\}$. Wir schreiben $x \succ y$ gdw. $y \preceq x$ und $x \neq y$. Also $m_0 \succ m_1$. Mit m_1 können wir das Argument wiederholen und damit eine Kette

$$m_0 \succ m_1 \succ m_2 \succ m_3 \succ \cdots$$

     konstruieren. Dies Kette muss mit einem Atom m_i mit $m_i \preceq m_0$ terminieren, da M endlich ist. □

Notizen:

- Infimum mit einem Atom a kann nur kleinstes Element $\perp$ oder a liefern
- Infimum mit zwei verschiedenen Atomen ist immer das kleinste Element $\perp$ (denn Atome sind unvergleichbar)
- Jedes Element (außer $\perp$) liegt über einem Atom

§10.3 Theorem

Sei $(M, \preceq)$ eine Boolesche Algebra mit endlichem M, kleinstem Element $\bot$ und größtem Element $\top$. Seien $m \in M$ und $A_m = \{a \in M \mid a \text{ Atom}, a \preceq m\}$ die Menge der kleineren Atome. Dann gilt $m = \sup A_m$.

§10.3 Theorem

Sei $(M, \preceq)$ eine Boolesche Algebra mit endlichem M, kleinstem Element $\bot$ und größtem Element $\top$. Seien $m \in M$ und $A_m = \{a \in M \mid a \text{ Atom}, a \preceq m\}$ die Menge der kleineren Atome. Dann gilt $m = \sup A_m$.

Beweis (direkt; 1/2).

Wir beweisen die Aussage zunächst für $m = \top$. Da $\top$ das größte Element ist, enthält $A_\top$ alle Atome $A_\top = \{a_1, \dots, a_k\}$. Nehmen wir nun an, dass $\top \neq \sup A_\top$. Dann gilt auch $\top^c = \bot \neq (\sup A_\top)^c = a_1^c \wedge \cdots \wedge a_k^c$ aufgrund der Eindeutigkeit der Komplemente.

§10.3 Theorem

Sei $(M, \preceq)$ eine Boolesche Algebra mit endlichem M, kleinstem Element $\bot$ und größtem Element $\top$. Seien $m \in M$ und $A_m = \{a \in M \mid a \text{ Atom}, a \preceq m\}$ die Menge der kleineren Atome. Dann gilt $m = \sup A_m$.

Beweis (direkt; 1/2).

Wir beweisen die Aussage zunächst für $m = \top$. Da $\top$ das größte Element ist, enthält $A_\top$ alle Atome $A_\top = \{a_1, \dots, a_k\}$. Nehmen wir nun an, dass $\top \neq \sup A_\top$. Dann gilt auch $\top^c = \bot \neq (\sup A_\top)^c = a_1^c \wedge \dots \wedge a_k^c$ aufgrund der Eindeutigkeit der Komplemente. Da $a_1^c \wedge \dots \wedge a_k^c \neq \bot$ existiert gemäß §10.2 ③ ein Atom $a_i \in A_\top$, so dass $a_i \preceq a_1^c \wedge \dots \wedge a_k^c$.

$$a_i = a_i \wedge a_1^c \wedge \dots \wedge a_k^c = a_i \wedge a_i^c \wedge \dots = \bot$$

da $a_i \in A_\top$. Also ist $a_i = \bot$ kein Atom. Widerspruch.

Beweis (direkt; 2/2).

Also gilt $\top = \sup A_\top$. Sei nun m beliebig. Es gilt gemäß §10.2[1]

$$
\begin{aligned}
m = \top \wedge m = \left(\sup A_\top\right) \wedge m &= (a_1 \vee \cdots \vee a_k) \wedge m \\
&= (a_1 \wedge m) \vee \cdots \vee (a_k \wedge m) = \underbrace{(a_1 \wedge m)}_{\in\{a_1, \perp\}} \vee \cdots \vee \underbrace{(a_k \wedge m)}_{\in\{a_k, \perp\}}
\end{aligned}
$$

Beweis (direkt; 2/2).

Also gilt $\top = \sup A_\top$. Sei nun m beliebig. Es gilt gemäß §10.2[1]

$$m = \top \wedge m = \left(\sup A_\top\right) \wedge m = (a_1 \vee \cdots \vee a_k) \wedge m$$
$$= (a_1 \wedge m) \vee \cdots \vee (a_k \wedge m) = \underbrace{(a_1 \wedge m)}_{\in\{a_1, \bot\}} \vee \cdots \vee \underbrace{(a_k \wedge m)}_{\in\{a_k, \bot\}}$$

Für jedes $1 \leq i \leq k$ gilt $a_i \wedge m = a_i$ gdw. $a_i \preceq m$. Sei $A_m = \{a_{j_1}, \ldots, a_{j_n}\}$.
Also gilt

$$m = (a_{j_1} \wedge m) \vee \cdots \vee (a_{j_n} \wedge m) = a_{j_1} \vee \cdots \vee a_{j_n} = \sup A_m \qquad \square$$

Beweis (direkt; 2/2).

Also gilt $\top = \sup A_\top$. Sei nun m beliebig. Es gilt gemäß §10.2[1]

$$m = \top \wedge m = \left(\sup A_\top\right) \wedge m = (a_1 \vee \cdots \vee a_k) \wedge m$$
$$= (a_1 \wedge m) \vee \cdots \vee (a_k \wedge m) = \underbrace{(a_1 \wedge m)}_{\in\{a_1, \perp\}} \vee \cdots \vee \underbrace{(a_k \wedge m)}_{\in\{a_k, \perp\}}$$

Für jedes $1 \leq i \leq k$ gilt $a_i \wedge m = a_i$ gdw. $a_i \preceq m$. Sei $A_m = \{a_{j_1}, \dots, a_{j_n}\}$. Also gilt

$$m = (a_{j_1} \wedge m) \vee \cdots \vee (a_{j_n} \wedge m) = a_{j_1} \vee \cdots \vee a_{j_n} = \sup A_m$$ □

Notizen:

- jedes Element einer endlichen Booleschen Algebra lässt sich also als Supremum von Atomen darstellen
- wie wir gleich zeigen, ist diese Darstellung sogar eindeutig

§10.4 Theorem

Sei $(M, \preceq)$ eine Boolesche Algebra mit endlichem M und kleinstem Element $\perp$. Weiterhin sei A die Menge aller Atome von $(M, \preceq)$. Für alle $X \subseteq A$ und $Y \subseteq A$ mit $X \neq Y$ gilt $\sup X \neq \sup Y$.

§10.4 Theorem

Sei $(M, \preceq)$ eine Boolesche Algebra mit endlichem M und kleinstem Element $\perp$. Weiterhin sei A die Menge aller Atome von $(M, \preceq)$. Für alle $X \subseteq A$ und $Y \subseteq A$ mit $X \neq Y$ gilt $\sup X \neq \sup Y$.

Beweis (indirekt).

Seien $X \subseteq A$ und $Y \subseteq A$ Teilmengen der Atome mit $X \neq Y$, so dass $\sup X = \sup Y$. O.B.d.A. existiert $a \in X$, so dass $a \notin Y$. Also gilt unter Nutzung von §10.2❷

$$\begin{aligned} a &= a \vee \perp = (a \wedge a) \vee \sup\{\perp\} \\ &= (a \wedge a) \vee \sup\{a \wedge x \mid x \in X \setminus \{a\}\} \\ &= a \wedge \sup X = a \wedge \sup Y \\ &= \sup\{a \wedge y \mid y \in Y\} = \sup\{\perp\} = \perp \end{aligned}$$

Also gilt $a = \perp$, womit a kein Atom ist. Widerspruch. $\square$

Notizen:

- jedes Element hat Darstellung als Supremum von Atomen
- verschiedene Mengen von Atomen liefern verschiedene Suprema

Notizen:

- jedes Element hat Darstellung als Supremum von Atomen
- verschiedene Mengen von Atomen liefern verschiedene Suprema

§10.5 Theorem

Eine endliche Boolesche Algebra $(M, \preceq)$ mit n Atomen besitzt genau 2^n Elemente (d.h. $|M| = 2^n$)

Notizen:

- jedes Element hat Darstellung als Supremum von Atomen
- verschiedene Mengen von Atomen liefern verschiedene Suprema

§10.5 Theorem

Eine endliche Boolesche Algebra $(M, \preceq)$ mit n Atomen besitzt genau 2^n Elemente (d.h. $|M| = 2^n$)

Beweis (direkt).

Sei A die Menge der Atome. Dann ist $\sup\colon \mathcal{P}(A) \to M$ injektiv gemäß §10.4. Also $2^n = 2^{|A|} = |\mathcal{P}(A)| \leq |M|$.

Notizen:

- jedes Element hat Darstellung als Supremum von Atomen
- verschiedene Mengen von Atomen liefern verschiedene Suprema

§10.5 Theorem

Eine endliche Boolesche Algebra $(M, \preceq)$ mit n Atomen besitzt genau 2^n Elemente (d.h. $|M| = 2^n$)

Beweis (direkt).

Sei A die Menge der Atome. Dann ist $\sup : \mathcal{P}(A) \to M$ injektiv gemäß §10.4. Also $2^n = 2^{|A|} = |\mathcal{P}(A)| \leq |M|$. Sei $f : M \to \mathcal{P}(A)$, so dass $f(m) = A_m$ wie in §10.3. Diese Funktion ist auch injektiv und damit $|M| \leq |\mathcal{P}(A)| = 2^n$, womit $|M| = 2^n$ folgt. □

Notizen:

- Isomorphismus ist Bijektion
  die alle Relationen und Operationen “erhält”
- gleiches “Rechnen” in isomorphen Strukturen
- isomorphe Strukturen unterscheiden sich nur in der Benennung der Elemente der Grundmenge

Motivation:

- wir zeigen noch, dass alle endlichen Booleschen Algebren isomorph zu Potenzmengenalgebren sind

$\rightarrow$ Isomorphiesatz von Stone

Marshall Harvey Stone (* 1903; † 1989)

- amer. Mathematiker
- Funktionsanalysis und Boolesche Algebren
- begeisterter Reisender und starb auf Reise

§10.6 Theorem (Isomorphiesatz von Stone)

Sei $\mathcal{M} = (M, \preceq)$ eine endliche Boolesche Algebra mit Atomen A.
Dann sind $\mathcal{M}$ und $(\mathcal{P}(A), \subseteq)$ isomorph.

§10.6 Theorem (Isomorphiesatz von Stone)

Sei $\mathcal{M} = (M, \preceq)$ eine endliche Boolesche Algebra mit Atomen A. Dann sind $\mathcal{M}$ und $(\mathcal{P}(A), \subseteq)$ isomorph.

Beweis (direkt; 1/2).

Für jedes $m \in M$, sei $A_m = \{a \in A \mid a \preceq m\}$. Wir definieren die Funktion $\varphi \colon M \to \mathcal{P}(A)$ durch $\varphi(m) = A_m$ für alle $m \in M$.

- injektiv: *(Kontraposition)* Seien $x, y \in M$, so dass $A_x = \varphi(x) = \varphi(y) = A_y$. Gemäß §10.3 gilt dann $x = \sup A_x = \sup A_y = y$.

§10.6 Theorem (Isomorphiesatz von Stone)

Sei $\mathcal{M} = (M, \preceq)$ eine endliche Boolesche Algebra mit Atomen A.
Dann sind $\mathcal{M}$ und $(\mathcal{P}(A), \subseteq)$ isomorph.

Beweis (direkt; 1/2).

Für jedes $m \in M$, sei $A_m = \{a \in A \mid a \preceq m\}$. Wir definieren die Funktion $\varphi\colon M \to \mathcal{P}(A)$ durch $\varphi(m) = A_m$ für alle $m \in M$.

- injektiv: *(Kontraposition)* Seien $x, y \in M$, so dass $A_x = \varphi(x) = \varphi(y) = A_y$. Gemäß §10.3 gilt dann $x = \sup A_x = \sup A_y = y$.
- surjektiv: Sei $X \subseteq A$ eine Teilmenge der Atome. Da A endlich ist, existiert $m = \sup X$. Also gilt $\varphi(m) = X$ aufgrund von §10.4.

§10.6 Theorem (Isomorphiesatz von Stone)

Sei $\mathcal{M} = (M, \preceq)$ eine endliche Boolesche Algebra mit Atomen A. Dann sind $\mathcal{M}$ und $(\mathcal{P}(A), \subseteq)$ isomorph.

Beweis (direkt; 1/2).

Für jedes $m \in M$, sei $A_m = \{a \in A \mid a \preceq m\}$. Wir definieren die Funktion $\varphi\colon M \to \mathcal{P}(A)$ durch $\varphi(m) = A_m$ für alle $m \in M$.

- injektiv: *(Kontraposition)* Seien $x, y \in M$, so dass $A_x = \varphi(x) = \varphi(y) = A_y$. Gemäß §10.3 gilt dann $x = \sup A_x = \sup A_y = y$.
- surjektiv: Sei $X \subseteq A$ eine Teilmenge der Atome. Da A endlich ist, existiert $m = \sup X$. Also gilt $\varphi(m) = X$ aufgrund von §10.4.
- Also ist φ bijektiv.

Beweis (direkt; 2/2).

Es bleibt zu zeigen, dass die Struktur erhalten wird. Sei $x, y \in M$ beliebig. Z.zg.

$$x \preceq y \qquad \text{gdw.} \qquad \varphi(x) \subseteq \varphi(y)$$

($\rightarrow$) Sei $x \preceq y$. Es gilt $\varphi(x) = A_x$ und $a \preceq x$ für alle $a \in A_x$. Also auch $a \preceq y$ und damit $a \in A_y = \varphi(y)$. Also $\varphi(x) \subseteq \varphi(y)$.

Beweis (direkt; 2/2).

Es bleibt zu zeigen, dass die Struktur erhalten wird. Sei $x, y \in M$ beliebig. Z.zg.

$$x \preceq y \qquad \text{gdw.} \qquad \varphi(x) \subseteq \varphi(y)$$

($\rightarrow$) Sei $x \preceq y$. Es gilt $\varphi(x) = A_x$ und $a \preceq x$ für alle $a \in A_x$. Also auch $a \preceq y$ und damit $a \in A_y = \varphi(y)$. Also $\varphi(x) \subseteq \varphi(y)$.

($\leftarrow$) Sei $\varphi(x) \subseteq \varphi(y)$. Dann gilt $A_x \subseteq A_y$ und damit gemäß §10.3

$$\begin{aligned} x &= \sup A_x \preceq \sup A_x \vee \sup(A_y \setminus A_x) \\ &= \sup\bigl(A_x \cup (A_y \setminus A_x)\bigr) = \sup A_y = y \end{aligned}$$

Beweis (direkt; 2/2).

Es bleibt zu zeigen, dass die Struktur erhalten wird. Sei $x, y \in M$ beliebig. Z.zg.

$$x \preceq y \qquad \text{gdw.} \qquad \varphi(x) \subseteq \varphi(y)$$

($\rightarrow$) Sei $x \preceq y$. Es gilt $\varphi(x) = A_x$ und $a \preceq x$ für alle $a \in A_x$. Also auch $a \preceq y$ und damit $a \in A_y = \varphi(y)$. Also $\varphi(x) \subseteq \varphi(y)$.

($\leftarrow$) Sei $\varphi(x) \subseteq \varphi(y)$. Dann gilt $A_x \subseteq A_y$ und damit gemäß §10.3

$$\begin{aligned} x &= \sup A_x \preceq \sup A_x \vee \sup(A_y \setminus A_x) \\ &= \sup\big(A_x \cup (A_y \setminus A_x)\big) = \sup A_y = y \end{aligned}$$

Also sind $\mathcal{M}$ und $(\mathcal{P}(A), \subseteq)$ isomorph. □

Notizen:

- jede endliche Boolesche Algebra ist
  isomorph zu einer Potenzmengenalgebra
- die Gesetze der endlichen Potenzmengenalgebra $(\mathcal{P}(M), \subseteq)$
  gelten auch in allen Booleschen Algebren dieser Größe

Notizen:

- jede endliche Boolesche Algebra ist
  isomorph zu einer Potenzmengenalgebra
- die Gesetze der endlichen Potenzmengenalgebra $(\mathcal{P}(M), \subseteq)$
  gelten auch in allen Booleschen Algebren dieser Größe

$\rightarrow$ Rechnen in endlichen Booleschen Algebren
= Rechnen mit Teilmengen einer endlichen Menge

Frage

Gilt diese Isomorphie auch für unendliche Boolesche Algebren?

Frage

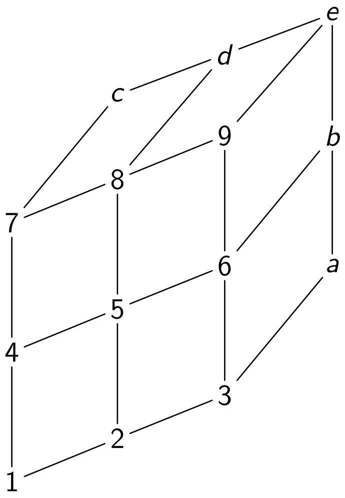
Gilt diese Isomorphie auch für unendliche Boolesche Algebren?

Beobachtungen:

- jede unendliche Potenzmengenalgebra ist überabzählbar (d.h. nicht abzählbar)
  - ist die Menge M endlich, dann ist $\mathcal{P}(M)$ auch endlich
  - ist die Menge M abzählbar unendlich, dann ist $|\mathcal{P}(M)| > |M|$ (§8.6) und damit überabzählbar
- es gibt aber abzählbar unendliche Boolesche Algebren (und sogar solche ohne Atome)

$\rightarrow$ nicht jede Boolesche Algebra ist isomorph zu einer Potenzmengenalgebra

Ist dies eine Boolesche Algebra?



Wiederholung (§9.12 Boolesche Algebra)

Eine algebraische Struktur $(M, \sqcap, \sqcup, \cdot^*, \bot, \top)$ des Typs $(0, 2, 1, 2)$, so dass für alle $x, y \in M$

- $\sqcap$ und $\sqcup$ kommutativ, distributiv und assoziativ sind,
- $x \sqcup (x \sqcap y) = x$ und $x \sqcap (x \sqcup y) = x$, Absorption
- und $x \sqcap x^* = \bot$ und $x \sqcup x^* = \top$. Komplemente

liefert eine Boolesche Algebra.

Wiederholung (§9.12 Boolesche Algebra)

Eine algebraische Struktur $(M, \sqcap, \sqcup, \cdot^*, \bot, \top)$ des Typs $(0, 2, 1, 2)$, so dass für alle $x, y \in M$

- $\sqcap$ und $\sqcup$ kommutativ, distributiv und assoziativ sind,
- $x \sqcup (x \sqcap y) = x$ und $x \sqcap (x \sqcup y) = x$, Absorption
- und $x \sqcap x^* = \bot$ und $x \sqcup x^* = \top$. Komplemente

liefert eine Boolesche Algebra.

Motivation:

- hat zwei binäre Funktionen (und eine unäre Funktion und 2 Konstanten)
- wir schauen uns zunächst nur die Eigenschaften der binären Funktion $\sqcup$ an

Wiederholung (§9.12 Boolesche Algebra)

Eine algebraische Struktur $(M, \sqcap, \sqcup, \cdot^*, \bot, \top)$ des Typs $(0, 2, 1, 2)$, so dass für alle $x, y \in M$

- $\sqcap$ und $\sqcup$ kommutativ, distributiv und assoziativ sind,
- $x \sqcup (x \sqcap y) = x$ und $x \sqcap (x \sqcup y) = x$, Absorption
- und $x \sqcap x^* = \bot$ und $x \sqcup x^* = \top$. Komplemente

liefert eine Boolesche Algebra.

Motivation:

- hat zwei binäre Funktionen
  (und eine unäre Funktion und 2 Konstanten)
- wir schauen uns zunächst nur die Eigenschaften
  der binären Funktion $\sqcup$ an

Beispiele

- ganze Zahlen $(\mathbb{Z}, +, (-\cdot), 0)$ mit Addition
  - $x + y = y + x$ für alle $x, y \in \mathbb{Z}$ (Kommutativität)
  - $x + (y + z) = (x + y) + z$ für alle $x, y, z \in \mathbb{Z}$ (Assoziativität)
  - $x + (-x) = 0$ für alle $x \in \mathbb{Z}$ (Inverse)

Algebraische Strukturen — Kommutative Gruppen

Beispiele

- ganze Zahlen $(\mathbb{Z}, +, (-\cdot), 0)$ mit Addition
  - $x + y = y + x$ für alle $x, y \in \mathbb{Z}$ (Kommutativität)
  - $x + (y + z) = (x + y) + z$ für alle $x, y, z \in \mathbb{Z}$ (Assoziativität)
  - $x + (-x) = 0$ für alle $x \in \mathbb{Z}$ (Inverse)
  - außerdem gilt: $0 + x = x$ für alle $x \in \mathbb{Z}$

Beispiele

- ganze Zahlen $(\mathbb{Z}, +, (-\cdot), 0)$ mit Addition
  - $x + y = y + x$ für alle $x, y \in \mathbb{Z}$ (Kommutativität)
  - $x + (y + z) = (x + y) + z$ für alle $x, y, z \in \mathbb{Z}$ (Assoziativität)
  - $x + (-x) = 0$ für alle $x \in \mathbb{Z}$ (Inverse)
  - außerdem gilt: $0 + x = x$ für alle $x \in \mathbb{Z}$
- rationale Zahlen $(\mathbb{Q} \setminus \{0\}, \cdot, \cdot^{-1}, 1)$ mit Multiplikation
  - $x \cdot y = y \cdot x$ für alle $x, y \in \mathbb{Q} \setminus \{0\}$ (Kommutativität)
  - $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ für alle $x, y, z \in \mathbb{Q} \setminus \{0\}$ (Assoziativität)
  - $x \cdot x^{-1} = 1$ für alle $x \in \mathbb{Q} \setminus \{0\}$ (Inverse)
  - außerdem gilt: $1 \cdot x = x$ für alle $x \in \mathbb{Q} \setminus \{0\}$

§10.7 Definition (kommutative Gruppe)

Eine algebraische Struktur $(M, \oplus, \cdot^*, e)$ des Typs $(0, 1, 1, 1)$ ist eine kommutative (oder: Abelsche) Gruppe, gdw.

- $\oplus$ kommutativ und assoziativ ist,
  $x \oplus y = y \oplus x$ für alle $x, y \in M$ und
  $x \oplus (y \oplus z) = (x \oplus y) \oplus z$ für alle $x, y, z \in M$
- $e \oplus x = x$ für alle $x \in M$ und (neutrales Element)
- $x \oplus x^* = e$ für alle $x \in M$. (Inverse)

Niels Henrik Abel (* 1802; † 1829)

- norw. Mathematiker
- Begründer der Gruppentheorie
- verstarb mit 26 Jahren an Lungentuberkulose

Notizen:

- wir betrachten nur kommutative Gruppen (oder Abelsche Gruppen)
- es gibt allerdings auch nicht-kommutative Gruppen
  (für die im Wesentlichen die gleichen Bedingungen ohne die Kommutativität von $\oplus$ gelten; d.h. es gelten zusätzlich

$$x \oplus e = x \qquad \text{und} \qquad x^* \oplus x = e \qquad\qquad \text{für alle } x)$$

- kommutative Gruppen werden manchmal auch "multiplikativ" geschrieben $(M, \odot, \cdot^{-1}, 1)$

§10.8 Theorem

Seien $(M, \oplus, \cdot^*, e)$ und $(M, \oplus, \cdot^\dagger, e)$ zwei kommutative Gruppen mit gleicher binärer Operation $\oplus$ und gleichem neutralen Element e. Dann gilt $x^* = x^\dagger$ für alle $x \in M$. (d.h. die Inversen sind eindeutig bestimmt)

§10.8 Theorem

Seien $(M, \oplus, \cdot^*, e)$ und $(M, \oplus, \cdot^\dagger, e)$ zwei kommutative Gruppen mit gleicher binärer Operation $\oplus$ und gleichem neutralen Element e. Dann gilt $x^* = x^\dagger$ für alle $x \in M$. (d.h. die Inversen sind eindeutig bestimmt)

Beweis (direkt).

Unter Anwendung der Gesetze gilt für alle $x \in M$

$$x^* = e \oplus x^* = \underbrace{(x \oplus x^\dagger)}_{e} \oplus x^* = (x^\dagger \oplus x) \oplus x^*$$

$$= x^\dagger \oplus \underbrace{(x \oplus x^*)}_{e} = x^\dagger \oplus e = x^\dagger$$

□

§10.8 Theorem

Seien $(M, \oplus, \cdot^*, e)$ und $(M, \oplus, \cdot^\dagger, e)$ zwei kommutative Gruppen mit gleicher binärer Operation $\oplus$ und gleichem neutralen Element e. Dann gilt $x^* = x^\dagger$ für alle $x \in M$. (d.h. die Inversen sind eindeutig bestimmt)

Beweis (direkt).

Unter Anwendung der Gesetze gilt für alle $x \in M$

$$x^* = e \oplus x^* = \underbrace{(x \oplus x^\dagger)}_{e} \oplus x^* = (x^\dagger \oplus x) \oplus x^*$$

$$= x^\dagger \oplus \underbrace{(x \oplus x^*)}_{e} = x^\dagger \oplus e = x^\dagger \qquad \square$$

Notizen:

- da eindeutig wird die unäre Funktion $\cdot^*$ oft nicht angegeben

§10.9 Theorem

Seien $(M, \oplus, e)$ und $(M, \oplus, u)$ zwei kommutative Gruppen mit gleicher binärer Operation $\oplus$. Dann gilt $e = u$.

(d.h. das neutrale Element ist eindeutig bestimmt)

§10.9 Theorem

Seien $(M, \oplus, e)$ und $(M, \oplus, u)$ zwei kommutative Gruppen mit gleicher binärer Operation $\oplus$. Dann gilt $e = u$.

(d.h. das neutrale Element ist eindeutig bestimmt)

Beweis (direkt).

Unter Anwendung der Gesetze gilt

$$\underbrace{e = u \oplus e}_{\text{Neutralität } u} = \underbrace{e \oplus u = u}_{\text{Neutralität } e}$$

□

§10.9 Theorem

Seien $(M, \oplus, e)$ und $(M, \oplus, u)$ zwei kommutative Gruppen mit gleicher binärer Operation $\oplus$. Dann gilt $e = u$.

(d.h. das neutrale Element ist eindeutig bestimmt)

Beweis (direkt).

Unter Anwendung der Gesetze gilt

$$\underbrace{e = u \oplus e}_{\text{Neutralität } u} = \underbrace{e \oplus u = u}_{\text{Neutralität } e} \qquad \square$$

Notizen:

- aufgrund der Eindeutigkeit werden die unäre Funktion $\cdot^*$ und das neutrale Element e oft nicht angegeben

§10.10 Definition (kommutative Gruppe [erneut])

Eine algebraische Struktur $(M, \oplus)$ des Typs $(0, 1, 0, 0)$ ist eine kommutative Gruppe, gdw.

- $\oplus$ kommutativ und assoziativ ist und
  $x \oplus y = y \oplus x$ für alle $x, y \in M$ und
  $x \oplus (y \oplus z) = (x \oplus y) \oplus z$ für alle $x, y, z \in M$
- ein Element $e \in M$ existiert, so dass
  - $e \oplus x = x$ für alle $x \in M$ und (neutrales Element)
  - für alle $x \in M$ ein $y \in M$ existiert, so dass $x \oplus y = e$. (Inverse)

Notizen:

- jedes Element muss ein Inverses besitzen
- Inverse verschiedener Elemente sind verschieden

Beispiele

- $(\mathbb{N}, +)$ ist keine kommutative Gruppe
  - das neutrale Element ist 0 denn $0 + n = n$ für alle $n \in \mathbb{N}$
  - aber für 1 gibt es kein Inverses,
    denn es gibt kein $n \in \mathbb{N}$, so dass $1 + n = 0$

Beispiele

- $(\mathbb{N}, +)$ ist keine kommutative Gruppe
  - das neutrale Element ist 0 denn $0 + n = n$ für alle $n \in \mathbb{N}$
  - aber für 1 gibt es kein Inverses,
    denn es gibt kein $n \in \mathbb{N}$, so dass $1 + n = 0$
- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$ und $(\mathbb{R} \setminus \{0\}, \cdot)$
  sind kommutative Gruppen

Beispiele

- $(\mathbb{N}, +)$ ist keine kommutative Gruppe
  - das neutrale Element ist 0 denn $0 + n = n$ für alle $n \in \mathbb{N}$
  - aber für 1 gibt es kein Inverses,
    denn es gibt kein $n \in \mathbb{N}$, so dass $1 + n = 0$
- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$ und $(\mathbb{R} \setminus \{0\}, \cdot)$
  sind kommutative Gruppen
- $(\mathbb{Q}, \cdot)$ ist keine kommutative Gruppe
  - das neutrale Element ist 1 denn $1 \cdot q = q$ für alle $q \in \mathbb{Q}$
  - aber für 0 gibt es kein Inverses,
    denn es gibt kein $q \in \mathbb{Q}$, so dass $0 \cdot q = 1$

Frohe Weihnachten und einen guten Start in 2019!

- Atome und Isomorphiesatz von Stone
- Einführung Gruppen

Fünfte Aufgabenserie bereits im AlmaWeb verfügbar