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

Algebraische Strukturen — Motivation

Informatik und Mathematik als *Strukturwissenschaften*.
Endziel mathematischer / informatischer Analyse / Modellbildung:
Konzentration auf das Wesentliche
Grundlage aximatischer Methodik: nicht unnötiges wiederholtes Nachweisen derselben Eigenschaften
Diese Vorgehensweise selbst wird (mit verschiedenen Stoßrichtungen) untersucht in den Theorien der *universellen Algebra*, *Kategorientheorie* und *Beweistheorie*.

Beispiele wichtiger Strukturen

Ein *Graph* G ist gegeben durch ein Paar (V, E), wobei V die *Knotenmenge* und $E \subseteq V \times V$ die *Kantenrelation* ist.

Eine *Halbgruppe* H ist gegeben durch ein Paar $(X, \circ)$, wobei X die Grundmenge und $\circ$ eine assoziative Operation auf X ist, d.h., $\circ : X \times X \to X$ (üblicherweise in Infixnotation geschrieben).

Beispiel: $(\{w, f\}, \wedge)$ ist eine Halbgruppe, ebenso $(\{w, f\}, \vee)$.
Beispiel: Für jede Menge M ist $(2^M, \cup)$ eine Halbgruppe, ebenso $(2^M, \cap)$.

Strukturen, ganz allgemein, werden *syntaktisch* beschrieben durch

1. eine oder auch mehrere Grundmengen

2. Operationen (evtl. auch nullstellige, also Konstanten) und / oder

3. Relationen / Funktionen auf den Grundmengen.

Üblicherweise gibt es noch eine Liste von Eigenschaften, die die beschriebenen Objekte erfüllen müssen, z.B. die Assoziativität im Falle einer Halbgruppe.

Dieser abstrakte Zugang ist sehr gut geeignet zur sauberen Beschreibung von Datentypen und Phänomenen bei der objektorientierten Programmierung, siehe FH-Skript zu OO.

Der funktionale Standpunkt ist manchmal einfacher als der relationale.

Bekannt: Funktionen als spezielle Relationen

Umgekehrt ist eine (z.B. binäre) Relation auch eine Menge $R \subseteq M \times N$.
Diese definiert Abbildungen R_1 und R_2 durch $R_1((x,y)) = x$ und $R_2((x,y)) = y$.
Also können wir alternativ Graphen auffassen als Struktur $G = (V, E; \alpha, \omega)$, wobei
V die Knotenmenge
E die Kantenmenge
α die Anfangsknotenabbildung $\alpha : E \to V$ und
ω die Endknotenabbildung $\omega : E \to V$ ist.

Im Folgenden gehen wir daher davon aus, dass Strukturen durch Mengen und Funktionen gegeben sind; Operationen sind ja ebenfalls Abbildungen.

Teilstrukturen

Es sei $S = (M_1, \ldots, M_n; f_1, \ldots, f_m)$ eine Struktur mit den Mengen M_i und den Funktionen f_j.

S' heißt *Teilstruktur* oder *Unterstruktur* von S gdw. $S' = (M'_1, \ldots, M'_{n'}; f'_1, \ldots, f'_{m'})$ mit $n' = n$, $m' = m$ und $M'_i \subseteq M_i$ für $i = 1, \ldots, n$ sowie f'_j ergibt sich aus f_j durch geeignete Restriktionen; ist z.B. $f_j : M_{k_j} \to M_{\ell_j}$, so ist $f'_j : M'_{k_j} \to M'_{\ell_j}$ mit $f'_j(x) = f_j(x)$ für alle $x \in M'_{k_j}$.
Wesentlich zum Nachweis der Teilstruktureigenschaft ist, ob $f_j(x) \in M'_{\ell_j}$ liegt.

Beispiel: Graphen (an der Tafel)
Beispiel: $(\{f\}, \wedge)$ ist eine Unterhalbgruppe von $(\{w, f\}, \wedge)$.

Morphismen

Wir nennen zwei Strukturen *gleichartig*, wenn sie die gleiche Anzahl von Mengen und Abbildungen besitzen und die Abbildungen die entsprechenden Mengen miteinander verknüpfen; außerdem sollen beide Strukturen dieselben Eigenschaften erfüllen.

Ein *Morphismus* (of auch: *Homomorphismus* oder kurz *Morphi*) ist eine *strukturerhaltende Abbildung* zwischen zwei gleichartigen Strukturen. Die erklären wir am besten an unseren Beispielen.
Die Teilstruktureigenschaft von S' bzgl. S kann man auch dadurch beschreiben, dass die Identität (als Einbettung) ein Morphi ist.
Insbesondere in der Kategorientheorie beliebt: Darstellung durch *kommutatives Diagramm*.
Morphismen auf gleichartigen Strukturen bilden mit der Hintereinanderausführung eine Halbgruppe.

Morphismen—Beispiele

Es seien $G_1 = (V_1, E_1, \alpha_1, \omega_1)$ und $G_2 = (V_2, E_2, \alpha_2, \omega_2)$ zwei Graphen. Ein *Graph(homo)morphismus* ist eine Abbildung (genauer: ein Paar von Abbildungen) $h = (h_V, h_E)$ mit $h_V : V_1 \to V_2$ und $h_E : E_1 \to E_2$, für die gilt: $\alpha_2(h_E(e)) = h_V(\alpha_1(e))$ und $\omega_2(h_E(e)) = h_V(\omega_1(e))$.

Es seien $H_1 = (M_1, \circ_1)$ und $H_2 = (M_2, \circ_2)$ zwei Halbgruppen. Ein *Halbgruppenmorphismus* ist eine Abbildung $h : M_1 \to M_2$ mit $h(x \circ_1 y) = h(x) \circ_2 h(y)$.
Konkret: $H_1 = (\{w, f\}, \wedge)$ und $H_2 = (\{w, f\}, \vee)$ mit $h : w \mapsto f$ und $f \mapsto w$.
$h(w \wedge w) = h(w) = f = f \vee f = h(w) \vee h(w)$.
$h(w \wedge f) = h(f) = w = f \vee w = h(w) \vee h(f)$.
$h(f \wedge f) = h(f) = w = w \vee w = h(f) \vee h(f)$.

Morphismen—praktisch gesehen

Graphen kann man als Modell für Schaltnetze nehmen.
Um solch ein Netz zu realisieren, versucht man meist, eine Darstellung desselben in einem *orthogonalen planaren Layout* zu finden.
Dabei werden die einzelnen Gatter (die elementare Schaltfunktionen wie UND oder ODER darstellen), gedanklich an Gitterpunkten der Zahlenebene angebracht, und die Leiterbahnen entlang achsenparalleler Linien.
Um Laufzeitprobleme zu vermeiden, sollten benachbarte Gatter auch auf dem Gitter benachbart sein.

Kurz gesagt: Wir suchen einen Morphismus von unserem gegebenen Graphen G in den Gittergraphen

$$(\mathbb{Z}^2, \{((i,j),(i',j')) \mid (i = i' \wedge |j - j'| = 1) \vee (j = j' \wedge |i - i'| = 1)\}).$$

Aus physikalischen Gründen sollte der Morphismus injektiv sein.

Morphismus-Jargon

Ein injektiver Morphismus heißt auch *Monomorphismus*.
Ein surjektiver Morphismus heißt auch *Epimorphismus*.
Ein bijektiver Morphi wird auch *Isomorphismus* genannt.
Ein Isomorphismus von einer Struktur auf sich selbst heißt auch *Automorphismus*.

Satz: Die Umkehrabbildung eines Isomorphismus ist wiederum ein Isomorphismus. Man sagt daher auch, zwei Strukturen seien *isomorph*.

Hinweis: Eigentlich müssten wir bei jedem Morphismus anmerken, auf welche Struktur er sich bezieht. Das vermeiden wir aber aus schreibtechnischen Gründen; sonst müssten wir später immer von Boolesche-Algebren-Epimorphismen reden...

Monoide—eine weitere Struktur

Ein *Monoid* kann beschrieben werden durch ein Tripel $M = (X, \circ, 1)$. Dabei ist $(X, \circ)$ eine Halbgruppe und $1 \in X$ ein *Einselement* oder *neutrales Element*, d.h., $\forall x \in X : 1 \circ x = x \circ 1 = x$.

Beispiel: $(\{w, f\}, \wedge, w)$ ist ein Monoid. $(\{w\}, \wedge, w)$ ist ein Untermonoid davon, nicht aber $(\{f\}, \wedge, f)$. Man kann den Halbgruppenmorphismus zwischen H_1 und H_2 aus dem vorigen Beispiel auch als Monoidmorphismus begreifen. Beachte: neutrale Elemente müssen aufeinander abgebildet werden.

Satz: In einer Halbgruppe gibt es höchstens ein Einselement.

Beweis: Es seien 1 und $1'$ Einselemente. Also gilt: $1 = 1 \circ 1' = 1'$; das erste Gleichheitszeichen gilt, da $1'$ Einselement ist, und das zweite, da 1 Einselement ist.

Monoide—weitere Beispiele

Ist $H = (M, \circ)$ eine Halbgruppe, so kann man H durch *Adjunktion* eines *formalen Einselements* 1 zu einem Monoid machen, indem man die Verknüpfung $\circ$ erweitert auf $M' = M \cup \{1\}$ durch $x \circ 1 = 1 \circ x = x$ für alle $x \in M'$.
Offenbar ist dann $(M', \circ, 1)$ ein Monoid.
Beispiel: Jede Operation auf einer einstelligen Menge definiert eine Halbgruppe (sogar ein Monoid) $(\{x\}, \cdot, x)$. Adjunktion von 1 als (neuem) Einselement liefert ein Monoid mit folgender *Verknüpfungstafel*:

$\cdot$	x	1
x	x	x
1	x	1

; diese ist *isomorph* zu H_1.

Beispiel: $(\mathbb{N}, \max)$ und $(\mathbb{N}, \min)$ sind Halbgruppen. $(\mathbb{N}, \max)$ besitzt das Einselement 0. $(\mathbb{N}, \min)$ besitzt kein Einselement, das zu adjungierende Einselement wird meist ∞ genannt.

Monoide—weitere Beispiele

Bislang waren alle betrachteten Monoide kommutativ. Das muss nicht sein.

Beispiel: Auf der Menge $M = \{a, b\}$ gibt es folgende Relationen:
$\mathcal{R} = \{ R_0 = \emptyset, R_1 = \{(a,a)\}, R_2 = \{(b,b)\}, R_3 = \{(a,b)\}, R_4 = \{(b,a)\}, R_5 = R_1 \cup R_2, R_6 = R_1 \cup R_3, R_7 = R_1 \cup R_4, R_8 = R_2 \cup R_3, R_9 = R_2 \cup R_4, R_{10} = R_3 \cup R_4, R_{11} = \overline{R_1}, R_{12} = \overline{R_2}, R_{13} = \overline{R_3}, R_{14} = \overline{R_4}, R_{15} = M \times M \}$.
$(\mathcal{R}, \circ, R_{15})$ bildet ein Monoid.
Wegen $R_3 \circ R_4 = R_1 \neq R_2 = R_4 \circ R_3$ ist es nicht kommutativ.

Gruppen sind spezielle Monoide

Eine *Gruppe* ist beschrieben durch $G = (X, \circ, 1, \iota)$, wobei $(X, \circ, 1)$ ein Monoid ist und $\iota : X \to X$ der Inversenoperator, d.h. $a \circ \iota(a) = \iota(a) \circ a = 1$. $\iota(a)$ heißt auch *Inverses* von a.

Beispiel: $\mathcal{N} = (\mathbb{N}, +, 0)$ ist ein Monoid, aber keine Gruppe. Nur die 0 besitzt ein Inverses.
$\mathcal{Z} = (\mathbb{Z}, +, 0, -)$ ist eine Gruppe, deren unterliegendes Monoid $\mathcal{N}$ als Teilmonoid enthält.

Manche Monoide besitzen ein *absorbierendes Element* 0, auch *Nullelement* genannt, mit der Eigenschaft $\forall x 0 = 0x = 0$. Monoide mit Nullelement sind keine Gruppen.

Ein wichtiges Beispiel für Gruppen liefern die Automorphismen einer Struktur (mit der Hintereinanderausführung als Operation).
Beispiel: Die Automorphismengruppe des vollständigen Graphen mit n Knoten heißt auch Permutationsgruppe (symmetrische Gruppe). Nach dem Satz von Cayley ist jede Gruppe zu einer Untergruppe einer symmetrischen Gruppe isomorph.

Wir basteln uns weitere Monoide (entsprechend für Halbgruppen und Gruppen)

Es seien $\mathcal{M}_i = (M_i, \circ_i, 1_i)$ Monoide für $i = 1, 2$.

Satz: $\mathcal{M} := \mathcal{M}_1 \times \mathcal{M}_2 := (M_1 \times M_2, \circ, (1_1, 1_2))$ mit $(m_1, m_2) \circ (n_1, n_2) := (m_1 \circ_1 n_1, m_2 \circ_2 n_2)$ ist ein Monoid.

Beispiel: $(\mathbb{Z}, +, 0)$ ist ein Monoid. Für festes $n \in \mathbb{N} \setminus \{0\}$ ist $\mod n$ ein Morphi in das Monoid $\mathcal{Z}_n := (\mathbb{Z}_n, +_n, 0)$ mit $a +_n b = (a + b) \mod n$. $\mathcal{Z}_2 \times \mathcal{Z}_3$ ist isomorph zu $\mathcal{Z}_6$.

Satz: $2^{\mathcal{M}_1} := (2^{M_1}, \circ_1, \{1_1\})$ mit $N \circ_1 N' := \{n \circ_1 n' \mid n \in N, n' \in N'\}$ ist ein Monoid (*Komplexprodukt*).

Erzeugnis (entsprechend für Halbgruppen und Gruppen)

Es sei $\mathcal{M} = (M, \circ, 1)$ Monoid und $X \subseteq M$. Wir sagen $X \Rightarrow X'$ für $X' \subseteq M$ gdw.
$x \in X' \iff x \in X \vee x = 1 \vee \exists y, z \in X : x = y \circ z$.
Wir reparieren sozusagen, was X noch daran fehlt, ein Monoid zu sein.

Die reflexive transitive Hülle von $\Rightarrow$ werde wieder mit $\Rightarrow^*$ bezeichnet.
Entsprechend bezeichnet X^* die eindeutig bestimmte Teilmenge von M mit der Eigenschaft $X \Rightarrow^* X^*$. X^* heißt auch *Erzeugnis* von X oder von X erzeugt.
Im Falle von Halbgruppen schreibt man auch X^+ für das Erzeugnis.
Satz: Jedes Erzeugnis X^* ist ein Untermonoid von $\mathcal{M}$.

Beispiel: In $\mathcal{Z}$ gilt: $\{0, 1\}^*$ ist isomorph zu $\mathcal{N}$.

Freies Erzeugnis (für Halbgruppen, Monoide und Gruppen)

Eine weitere uns vertraute Operation ist das cartesische Mengenprodukt
Allgemein macht es aus einem n-Tupel und einem m-Tupel ein $(n+m)$-Tupel.
Wir können dabei von der Grundmenge (also 1-Tupeln) aus starten und immer mehr und längere Tupel hinzugewinnen, wenn wir analog zur Erzeugnisbildung vorgehen.
Bezeichnet M^n die Menge der n-Tupel über der Menge M, so gilt: $M^+ = \bigcup_{n \geq 1} M^n$.
Wie vorher gesehen gilt: M^+ ist gegen cartesische Mengenproduktbildung abgeschlossen; letztere Operation heißt auch *Konkatenation*.
Folgerung: $(M^+, \cdot)$ ist eine Halbgruppe, die von M *frei erzeugte HG*.
Ist M endlich, so heißt M auch *Alphabet* und $w \in M^*$ *Wort*.
Durch Adjunktion des neutralen Elementes λ (genannt *leeres Wort*) entsteht das frei erzeugte Monoid $M^* = M^+ \cup \{\lambda\}$.
Beispiel: $\{a\}^*$ ist isomorph zu $(\mathbb{N}, +, 0)$ (Unärzähler, siehe Peano-Axiome).

Erzeugendensysteme (entsprechend für Halbgruppen und Gruppen)

Es sei $\mathcal{M} = (M, \circ, 1)$ Monoid und $X \subseteq M$. X heißt *Erzeugendensystem* für $\mathcal{M}$ gdw. $X^* = M$.
Ist h ein Morphi mit Definitionsbereich M, so genügt es, h auf einem Erzeugendensystem X zu kennen: Da sich jedes Element $y \in M$ als Produkt $y = x_1 \circ x_2 \circ \cdots \circ x_n$ darstellen lässt, gilt $h(y) = h(x_1)h(x_2)\ldots h(x_n)$ aufgrund der Morphi-Eigenschaft.

Beispiel: M ist ein Erzeugendensystem für M^*.
Betrachte $h : M^* \to \{a\}^*$, definiert durch $x \mapsto a$ für $x \in M$.
Bezeichne $\phi : \{a\}^* \to \mathcal{N}$ den erwähnten Monoidisomorphismus, so heißt $\ell : M^* \to \mathcal{N}, m \mapsto \phi(h(m))$ auch *Länge(nfunktion)* für M^*.
ℓ ist ebenfalls ein Morphi, d.h., $\ell(m \cdot n) = \ell(m) + \ell(n)$.