Diskrete Strukturen

Algebraische Strukturen

Algebra: $\langle S, f_1, \dots f_t \rangle$, S - nichtleere Menge $f_1, \dots, f_t$ Operatoren der Stelligkeit $m_1, \dots, m_t \in \mathbb{N}$

Signatur: Tupel $(m_1, \dots, m_t)$ $f_i : S^{m_i} \to S$

Hintereinanderausführung: $(f \circ g)(t) = f(g(t))$

Linksneutral $\Leftrightarrow$ $(\forall a \in S)[e \circ a = a]$; $(\forall a \in S)[a \circ e = a]$ rechtsn.

neutral: links- und rechtsneutral (eindeutig)

Linksinvers zu $a \Leftrightarrow x \circ a = e$; rechtsinvers zu a $a \circ x = e$

Inverses von a $\Leftrightarrow$ x ist links- u. rechtsinvers

assoziative Algebra: $(x \circ y) \circ z = x \circ (y \circ z)$

$\Rightarrow$ in assoz Algebren ist Inverses eindeutig

Unteralgebra von $(S, f_1, \dots, f_t)$: S' abgeschlossen unter $f_1, \dots, f_t$

$\mathbb{Z}_k := \{0, 1, 2, \dots, k-1\}$; $x \cdot_k y = \mathrm{mod}(x \cdot y, k)$

Homomorphismus: $A = \langle S, f_1, \dots, f_t \rangle$; $\tilde{A} = \langle \tilde{S}, \tilde{f}_1, \dots, \tilde{f}_t \rangle$, gleiche Signatur

$\hookrightarrow h : S \to \tilde{S}$ von A nach $\tilde{A}$ $\Rightarrow \tilde{f}_i(h(a_1), \dots, h(a_{m_i})) = h(\tilde{f}_i(a_1, \dots a_{m_i}))$

- existiert ein $h : S \to \tilde{S}$ $\Rightarrow \langle h(S), \tilde{f}_1, \dots, \tilde{f}_t \rangle$ Unteralg. von $\tilde{A}$

Isomorphismus: $h : S \to \tilde{S}$ ist bijektiv

Automorphismus: Isomorphismus $h : S \to \tilde{S}$ und $S = \tilde{S}$

gibt es Isomorph $A \to \tilde{A}$, so auch Isomorph $\tilde{A} \to A$

Typen von Algebren (E1) $\circ$ ist assoziativ
(E2) es gibt neutr. El $e \in S$
(E3) jedes El $a \in S$ besitzt eindeut. Inverses

Name	E1	E2	E3
Gruppoid			
Halbgruppe	X		
Monoid	X	X	
Gruppe	X	X	X
Loop		X	X
Gruppe mit 1		X	

abelsch $\circ$ ist kommutativ:
$a \circ b = b \circ a$
$\to$ Symmetrie entlang Diagonale

Ring $\langle S, + \rangle$ ist abelsche Gruppe mit neutr. Element $0 \in S$
$\langle S, \cdot \rangle$ ist Monoid mit neutralem Element $1 \in S$
für alle $a, b, c \in S$: $a(b+c) = (a \cdot b) + (a \cdot c)$ (distributiv)
$(b+c) \cdot a = (b \cdot a) + (c \cdot a)$

Körper $\langle S, + \rangle$ ist abelsche Gruppe mit neutr. Element $0 \in S$
$\langle S \setminus \{0\}, \cdot \rangle$ ist abelsche Gruppe mit neutr. Element $1 \in S$
für alle $a, b, c \in S$: $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$

- jeder Körper ist ein Ring

chin. Restsatz Für alle $m, n \in \mathbb{N}$ mit $ggT(m,n) = 1$ und $a \in \mathbb{Z}_m$ und $b \in \mathbb{Z}_n$ gibt es ein $t \in \mathbb{Z}_{m \cdot n}$ so dass
$t = \mathrm{mod}(a, m)$ und $t = \mathrm{mod}(b, n)$

allgemein $b_1, \dots, b_k \in \mathbb{N}$; $m_1, \dots, m_k \in \mathbb{N}$, $ggT(m_i, m_j) = 1$, $1 \leq i \leq j \leq k$ so gibt es genau ein $x \in \mathbb{Z}_{m_1 \cdot \ldots \cdot m_k}$ mit
$x = \mathrm{mod}(b_i, m_i)$

boolsche Algebra $A = \langle S, +, \cdot, \bar{\ } \rangle$, Sig $(2, 2, 1)$
$\langle S, + \rangle$ ist abelscher Monoid mit neutr. El $0 \in S$
$\langle S, \cdot \rangle$ ist abelscher Monoid mit neutral. El. $1 \in S$
für alle $a \in S$ gilt $a + \bar{a} = 1$ und $a \cdot \bar{a} = 0$
für alle $a, b, c \in S$ gilt $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$
$a + (b \cdot c) = (a+b) \cdot (a+c)$

Gruppenregeln

- Involutionsregel $a = (a^{-1})^{-1}$
- Kürzungsregeln $a \circ b = c \circ b \Leftrightarrow a = c$
  $b \circ a = b \circ c \Leftrightarrow a = c$
- Eind. Lsbk lin Gl $a \circ x = b \Leftrightarrow x = a^{-1} \circ b$
  $x \circ a = b \Leftrightarrow x = b \circ a^{-1}$

$a^0 = e$ | $a^m \circ a^n = a^{m+n}$
$a^n = a \circ a^{n-1}$ | $(a^n)^m = a^{m \cdot n}$
$a^{-n} = (a^{-1})^n$ | $a^m = a^n \Leftrightarrow a^{m-n} = e$

Ordnung $ord(a)$ ist kleinstes $r \in \mathbb{N}_+$ mit $a^r = e$
existiert r nicht, so ist $ord(a) = \infty$

- G endl Gruppe $\to$ alle $ord(a) < \infty$
  $ord(a) < \infty \Rightarrow$ $a^k = e \Leftrightarrow ord(a) \mid k$
- bei abelschen Gruppen mit $ord(a), ord(b) < \infty$ und $ggT(ord(a), ord(b)) = 1$ gilt: $ord(a \circ b) = ord(a) \cdot ord(b)$
- G abelsch, endl, $a \in G$ mit max ord $\Rightarrow ord(b) \mid ord(a)$ f.a. $b \in G$

Untergruppe: Unteralgebra $\langle H, \circ \rangle$ von Gruppe $\langle G, \circ \rangle$ ist Gruppe
$\to$ neutrale Elemente sind identisch

- G endl, H und K Untergruppen $\Rightarrow H \cap K$ Untergruppe
- G endl, $a \in G \Rightarrow S_a = \{e, a, a^2, \dots, a^{ord(a)-1}\}$ kleinste Untergruppe mit a

zyklische Gruppe $b \in G$, $G = \{b^i \mid i \in \mathbb{Z}\}$
b: erzeugendes Element / Generator, $\|G\| = ord(b)$

- $\|G\| = \infty \Rightarrow G$ isomorph zu $\langle \mathbb{Z}, + \rangle$
- $\|G\| = m < \infty \Rightarrow G$ — " — zu $\langle \mathbb{Z}_m, +_m \rangle$

eulersche Phi-Fkt $\varphi : \mathbb{N}_+ \to \mathbb{N}_+$: $\varphi(n) = \|\mathbb{Z}_n^*\|$ (Anzahl der zu n teilerfremden Zahlen)

$\mathbb{Z}_n^*$ - teilerfremd zu n

- $n \in \mathbb{N}$, $n \geq 2$, $a \in \mathbb{Z}_n^*$: $\mathrm{mod}(a^{\varphi(n)}, n) = 1$
- — " —, n ist Primzahl $\Leftrightarrow$ $\mathrm{mod}(a^{n-1}, n) = 1$ f.a. $a \in \mathbb{Z}_n \setminus \{0\}$

Körper

- $a \cdot 0 = 0 \cdot a = 0$
- $a \cdot b = 0 \Rightarrow a = 0$ od. $b = 0$
- $\langle \mathbb{Z}_n, +_n, \cdot_n \rangle$ ist Körper $\Leftrightarrow$ n ist Primzahl
- $K^* = K \setminus \{0\}$ ist zyklisch
- $n \in \mathbb{N}$, $n \geq 2$ gdw Körper mit $\|K\| = n$, wenn $n = p^k$ für geeign. Primzahl p und Zahl k, $\|K_1\| = \|K_2\| \Rightarrow K_1 \cong K_2$

Kombinatorik

Bijektion $f : A \to B$ gdw $\|A\| = \|B\|$

Summenregel $\|A_1 \cup \ldots \cup A_n\| = \sum_{j=1}^{n} \|A_j\|$, A_is paarweise disjunkt

Produktregel $\|A_1 \times \ldots \times A_n\| = \prod_{j=1}^{n} \|A_j\|$

Potenzregel $\|A\| = m$, $\|B\| = n$ $\Rightarrow$ es existieren n^m Fkt $f : A \to B$

Potenzmenge $\|A\| = n \Rightarrow \|\mathcal{P}(A)\| = 2^n$

Urnenmodelle	mit zurückl.	ohne zurücklegen
mit Reihenfolge	n^k	$n^{\underline{k}} = \frac{n!}{(n-k)!}$
ohne Reihenfolge	$\binom{n+k-1}{k}$	$\binom{n}{k} = \frac{n!}{k!(n-k)!}$

n - Anz Kugeln
k - Anz Züge

$\binom{n}{k_1, \dots, k_r} = \frac{n!}{k_1! \cdot \ldots \cdot k_r!}$

$\binom{n}{k} = \binom{n}{n-k}$, $\binom{n}{k} = 0$ für $k > n$

Pascal: $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$, $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$

$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$, $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

Vandermont $\binom{n+m}{k} = \sum_{j=0}^{k} \binom{n}{j} \binom{m}{k-j}$ $\to$ doppeltes Abzählen

Permutation $\|A\| = n$ $\pi : A \to A$, $A = \{1, \dots, n\} = [n]$, π ist bijektiv

Symmetrische Gruppe $\mathcal{S}_n = \{\pi \mid \pi : [n] \to [n]$ ist Permutation$\}$
$\|\mathcal{S}_n\| = n!$, $\sqrt{2\pi n}\left(\frac{n}{e}\right)^n < n! < \sqrt{2\pi n}\left(\frac{n}{e}\right)^n e^{\frac{1}{12n}}$, $e = 2{,}718281\ldots$

Matrixschreibweise $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots & n \\ \pi(1) & \pi(2) & \pi(3) & \pi(4) & \pi(5) & & \pi(n) \end{pmatrix}$

Tupelschreibweise: $(\pi(1), \pi(2), \pi(3), \dots, \pi(n))$

Zyklenschreibweise: $(\pi(1)\ \pi(2)\ \pi(3))(\dots)$, $(1\ 4\ 2) = (4\ 2\ 1) = (2\ 1\ 4)$

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 6 & 2 & 5 & 3 \end{pmatrix} = (4, 1, 6, 2, 5, 3) = (1, 4, 2)(3\ 6)(5)$

Stirlingzahlen 1. Art

$\sum_{k=1}^{n} s_{n,k} = \left[{n \atop k}\right] = n!$, $k>n: s_{n,k}=0$

$s_{n,k} = s_{n-1,k-1} + (n-1)s_{n-1,k}$ — $n>0: s_{n,0}=0$

$\hat{=}$ Anzahl Permutationen mit k Zykeln — $s_{0,0}=1$

Stirlingzahlen 2. Art

$S_{n,k} = \left\{{n \atop k}\right\}$ — $k>n: S_{n,k}=0$

$S_{n,k} = S_{n-1,k-1} + k \cdot S_{n-1,k}$ — $k=0: S_{n,0}=0$

$\hat{=}$ Anzahl k-Partitionen in n-elem. Menge — $S_{0,0}=1$

Bell-Zahl: Anzahl Partitionen in n-elem. Menge: $B_n = \sum_{k=0}^{n} S_{n,k}$

Inklusions-Exklusions-Prinzip: $\left\|\bigcup_{i=1}^{n} A_i\right\| = \sum_{\emptyset \neq K \subseteq \{1,\dots,n\}} (-1)^{1+\|K\|} \left\|\bigcap_{k\in K} A_k\right\|$

Schubfachschluss $\|A\| > \|B\| > 0$, $f: A \to B \Rightarrow \exists y \in B$ mit $\|f^{-1}(y)\| > 1$

allg. Schubfachschluss $A \to B \Rightarrow \exists y \in B$ mit $\|f^{-1}(y)\| \geq \left\lceil \frac{\|A\|}{\|B\|} \right\rceil$

$k>n$: $P_{n,k}=0$ — Zahl $=n$, anz Ziffern $=k$

$n\geq 1$: $P_{n,0}=0$

$P_{0,0}=1$

$1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$, $5! = 120$, $6! = 720$, $7! = 5040$, $8! = 40320$, $9! = 362880$, $10! = 3628800$

ungeordnete Zahlpart. $\# = P_{n,k} = \sum_{j=0}^{k} P_{n-k,j}$

geordnete Zahlpart. $\# = \binom{n-1}{k-1}$

Graphentheorie

$\|E\| = m$, $\|V\| = n$

Graph: Paar $G=(V,E)$, V endl., nichtleere Menge von Knoten, $E \subseteq \mathcal{P}_2(V) = \{\{x,y\} \mid x,y \in V \wedge x \neq y\}$

markiert: Namen spielen eine Rolle

Vollständiger Graph: K_n: n-Knoten, alle verbunden

Gittergraph: $M_{m,n}$: m Zeilen, n Spalten

Kreisgraph: C_n: n Knoten, zyklisch verbunden

Liniengraph: P_n: Pfad mit n+1 Knoten

Hyperwürfel: Q_d: d-Dimensionen, $V = \{0,1\}^d$, Kanten zu Knoten, die sich in genau 1 Komp. untersch.

Schleifen: Kanten, die Knoten mit sich selbst verbinden

Mehrfachkanten: mehrere Kanten zu 2 Knoten

Nachbarschaft: $N_G(v) = \{u \in V \mid \{v,u\} \in E\}$

Grad: $\deg(v) = \|N_G(v)\|$

$K_n: \deg(v) = n-1$; $C_n: \deg(v) = 2$; $Q_d: \deg(v) = d$

k-regulär $\Leftrightarrow$ f.a. $v \in V$ gilt $\deg(v) = k$

u,v **adjazent** $\Leftrightarrow e = \{u,v\} \in E$ (u,v Endknoten von e)

u,e **inzident** $\Leftrightarrow u \in E$ (u ist Endknoten von e)

- $\sum_{v\in V} \deg(v) = 2 \cdot \|E\|$
- Anzahl v mit ungeradem Grad ist gerade

Weg: der Länge k: Folge $W = \{v_0, e_1, v_1, \dots, v_{k-1}, e_k, v_k\}$, (v_0, v_k)-Weg (Startknoten v_0, innere Knoten, Endknoten v_k)

Pfad: Knotendisjunkter Weg (u,v paarweise versch.)

Kreis: Weg mit gl. Anfangs- und Endknoten

einfacher Kreis: Kreis ≥ 3, Knotendisjunkt

- Gibt es einen (u,v)-Weg, so gibt es einen (u,v)-Pfad

induzierter Teilgraph: Teilgraph in dem alle e drin sind

zusammenhängend: f.a. Knoten existiert (u,v)-Weg

Zusammenhangskomponente: zshg. Knotenmax. induzierter Teilgraph

- Jeder Graph enthält min $\|V\| - \|E\|$ Zshgkp
- in jedem zshg. $G=(V,E)$ gilt: $\|E\| \geq \|V\| - 1$

Abstand: $d_G(u,v)$ Länge des kürzesten Weges

Durchmesser: $\mathrm{diam}(G) = \max\{d_G(u,v) \mid u,v \in V\}$

Zentrum: ein Knoten, dessen max Abstand zu anderen Knoten minimal

Radius: $\mathrm{rad}(G) = \min_{u\in V} \max_{v \in V} d_G(u,v)$ max Abstand eines Knotens zum Zentrum

Baum: zshg, kreisfrei; **Wald:** Zshgk sind Bäume

Blatt: Baumknoten mit $\deg(v)=1$, Jeder Baum mit $\|V\| \geq 2$ enthält min 2 Blätter

- $T=(V,E)$ Baum mit $\|V\| \geq 2$, v Blatt $\Rightarrow T' = T \setminus \{v\}$ ist Baum
- $T=(V,E)$ gilt: $\|E\| = \|V\| - 1$; $T=(V,E)$, $T_1, \dots, T_k$ Komp. v. $T[V \setminus \{v\}]$, $\deg(v) = k$ — $T_1 \dots T_k$ Bäume
- $G=(V,E)$ zshg, C einf. Kreis mit Kante e $\Rightarrow G'(V, E \setminus \{e\})$ zshg.

Spannbaum $T=(V_T, E_T)$ von $G(V_G, E_G)$, falls $V_T = V_G$ und $E_T \subseteq E_G$

Cayley: $n \geq 2 \to$ es gibt n^{n-2} markierte Bäume

Prüfer-Code: entferne kl. Blatt, Knoten was dran hing aufschr.

Hamiltonkreis: enthält jeden Knoten genau 1mal; gilt f.a. nicht adjazenten Knoten $\deg(x) + \deg(v) \geq \|V\| \to$ G hat Hamiltonkreis

Eulertour: Kreis, der jede Kante genau 1mal enthält, $\deg(v)$ gerade f.a. v

planar: G kann kreuzungsfrei gez. werden; **eben:** ist so gez.

Gebiet/Facette: Zerschnitt der Ebene d. Kanten $\|F\| = \|E\| - \|V\| + 2$

- $\|V\| \geq 3$: $\|E\| \leq 3\|V\| - 6$
- G planar, wenn keine K_5 oder $K_{3,3}$ drin sind

Knotenfärbung: chromatische Zahl: $\chi(G)$ min k, so dass Knotenfärbung existiert

bipartit: kein einfacher Kreis ungerade Länge

- $T(V,E)$, $\|V\| \geq 2 \Rightarrow \chi(T) = 2$; G planar $\Rightarrow \chi(G) \leq 4$

Kantenfärbung: chromatischer Index: $\chi'(G)$ min k, so dass Kantenfärbung existiert

- $\Delta G \leq \chi'(G) \leq \Delta(G) + 1$, Δ max Grad

Matching: $M \subseteq E$, falls $e \cap f = \emptyset$ f.a. $e,f \in M$, $e \neq f$

perfekter Matching $\|M\| = \frac{1}{2}\|V\|$

Heiratssatz: $G = (A \uplus B, E)$ $\exists M$, $\|M\| = \|A\|$ gdw $\|N(X)\| \geq \|X\|$ f.a. $X \subseteq A$

- jeder k-reguläre, bipartite Graph enth. perf. Matching $\Rightarrow \chi'(G) = k$

Rekursionsgleichungen

Lineare R: $x_n = a_1 x_{n-1} + \dots + a_k x_{n-k} + b_k$ f.a. $n \geq k$

AB: $x_i = b_i$ f.a. $i \in \{0, \dots, k-1\}$

inhomog. lin. R. 1.O: $x_n = a x_{n-1}$, $x_0 = b_0 \Rightarrow x_n = b_0 a^n$

inhomog. lin. R. 1.O: $x_n = a x_{n-1} + b_1$, $x_0 = b_0$

$$\Rightarrow x_n = \begin{cases} b_0 \cdot a^n + b_1 \frac{a^n - 1}{a-1}, & a \neq 1 \\ b_0 + n b_1, & a = 1 \end{cases}$$

homog. lin R. 2.O.: $x_n = a_1 \cdot x_{n-1} + a_2 x_{n-2}$, $x_1 = b_1$, $x_0 = b_0$

$$A := \begin{cases} \frac{b_1 - b_0 \beta}{\alpha - \beta}, & \text{falls } \alpha \neq \beta \\ \frac{b_1 - b_0 \alpha}{\alpha}, & \text{falls } \alpha = \beta \end{cases}, \quad B := \begin{cases} \frac{b_1 - b_0 \alpha}{\alpha - \beta}, & \alpha \neq \beta \\ b_0, & \alpha = \beta \end{cases}, \quad x_n = \begin{cases} A\alpha^n - B\beta^n, & \alpha \neq \beta \\ (An + B)\alpha^n, & \alpha = \beta \end{cases}$$

formale Potenzreihe $A(x) = \sum_{k=0}^{\infty} a_k \cdot x^k$

Rechenregeln

(+) $\left(\sum_{k=0}^{\infty} a_k \cdot x^k\right) + \left(\sum_{k=0}^{\infty} b_k \cdot x^k\right) = \sum_{k=0}^{\infty} (a_k + b_k) x^k$

(·) $\left(\sum_{k=0}^{\infty} a_k \cdot x^k\right)\left(\sum_{k=0}^{\infty} b_k \cdot x^k\right) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k \cdot b_{n-k}\right) x^n$

(↑) $\sum_{k=0}^{\infty} a_k \cdot x^{m+k} = \sum_{k=m}^{\infty} a_{k} \cdot x^{m+k} = x^m \sum_{k=0}^{\infty} a_k x^k$

(↓) $\sum_{k=0}^{\infty} a_{k+m} \cdot x^k = x^{-m} \sum_{k=0}^{\infty} a_{k+m} \cdot x^{k+m} = x^{-m}\left(\sum_{k=0}^{\infty} a_k \cdot x^k - \sum_{k=0}^{m-1} a_k x^k\right)$

(f') $\left(\sum_{k=0}^{\infty}\right)' = \sum_{k=0}^{\infty} (a_k \cdot x^k)' = \sum_{k=0}^{\infty} k \cdot a_k \cdot x^{k-1} = \sum_{k=0}^{\infty} (k+1) a_{k+1} \cdot x^k$

Methode der erz. Funktion

1. Aufstellen der erz. Fkt als Potenzreihe
2. Anwenden der Rekursionsgleichung (Einsetzen)
3. Umformen nach erz. Fkt
4. Auflösen nach erz. Fkt. — $\frac{A}{1-\alpha x} + \frac{B}{1-\beta x}$
5. Ersetzen der neuen rechten Seite durch Potenzreihe (Taylor)
6. Koeffizientenvergleich — $F(x) = A \cdot \sum_{n=0}^{\infty} (\alpha x)^n + B \sum_{n=0}^{\infty} (\beta x)^n$

Taylor-Reihe $F(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(x_0)}{n!} \cdot z^n$

Folgeglied	Anfang	form. Potenzreihe	erz. Fkt
1	1,1,1,1,…	$\sum_{k=0}^{\infty} x^k$	$\frac{1}{1-x}$
k	0,1,2,3,…	$\sum_{k=0}^{\infty} k \cdot x^k$	$\frac{x}{(1-x)^2}$
α^k	$1, \alpha, \alpha^2, \dots$	$\sum_{k=0}^{\infty} \alpha^k \cdot x^k$	$\frac{1}{1-\alpha x}$
k^2	0,1,4,9	$\sum_{k=0}^{\infty} k^2 \cdot x^k$	$\frac{x(1+x)}{(1-x)^3}$
$\frac{1}{k}$	$0, 1, \frac{1}{2}, \frac{1}{3}$	$\sum_{k=0}^{\infty} \frac{1}{k} \cdot x^k$	$\ln \frac{1}{1-x}$
$\frac{1}{k!}$	$1, 1, \frac{1}{2}, \frac{1}{6}$	$\sum_{k=0}^{\infty} \frac{1}{k!} x^k$	e^x