

Prüfungsrelevante Verfahren, Sätze und Rechenregeln

2 Diskrete Strukturen

2.1 Mengenlehre und Kombinatorik

- zwei Mengen A und B sind gleich wenn sie die selben Elemente haben, d.h. wenn $A \subseteq B \wedge B \subseteq A$
- Beachte z.B. dass $\{\{1, 2\}, 7\} \not\subseteq \mathbb{N}$
- Schnitt und Vereinigung sind kommutativ, assoziativ, distributiv in beide Richtungen; für Beweise kann es nützlich sein sich die Definitionen dieser Operationen in Erinnerung zu rufen; $\overline{A \cup B} = \overline{A} \cap \overline{B}$, $\overline{A \cap B} = \overline{A} \cup \overline{B}$
- $A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$ heißt **kartesisches Produkt** oder **Produktmenge**; $|A \times B| = |A| \cdot |B|$
- **Potenzmenge** $\mathcal{P}(A)$ ist die Menge aller (auch unechten) Teilmengen von A , $|\mathcal{P}(A)| = 2^{|A|}$, es gilt stets $\emptyset \in \mathcal{P}(A)$
- $\binom{n}{k} = \frac{n!}{k!(n-k)!} = \binom{n}{n-k}$; $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$
- **Handschlaglemma**: Anzahl der Teilnehmer einer Konferenz, die einer ungeraden Anzahl von Teilnehmern die Hand geben, ist immer gerade

2.2 Abbildungen

- für $f : A \rightarrow B$, $A' \subseteq A$ heißt $f[A'] = \{f(a) \mid a \in A'\}$ Bild von A' unter f
- **injektiv**: $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$ ("für jedes $b \in B$ existiert höchstens ein $a \in A$ mit $f(a) = b$ ")
Beweise über Gegenbeispiel oder $f(a_1) = f(a_2)$ setzen
- **surjektiv**: $f[A] = B$ ("für jedes $b \in B$ existiert mindestens ein $a \in A$ mit $f(a) = b$ ")
Beweise über Gegenbeispiel oder Definitionsbereich der Umkehrfunktion untersuchen
- **bijektiv**: injektiv und surjektiv ("für jedes $b \in B$ existiert genau ein $a \in A$ mit $f(a) = b$ ")
- für f *injektiv* (!!) definieren wir $f^{-1} : f[A] \rightarrow A, b \mapsto f^{-1}(b) = a$ mit $f^{-1}(b) = a$ g.d.w. $f(a) = b$
- für $f : A \rightarrow B, g : B \rightarrow C$ ist **Komposition** $g \circ f : A \rightarrow C, x \mapsto g(f(x))$ (\Rightarrow von rechts nach links ausführen!!)

2.3 Permutationen

- **Permutation** von X ist bijektive Abbildung von X nach X , für $X = \{1, \dots, n\}$ ist S_n Menge aller Permutationen und $\pi \in S_n$ mit $\pi = \begin{pmatrix} 1 & \dots & n \\ \pi(1) & \dots & \pi(n) \end{pmatrix}$ und $|S_n| = n!$
- **k-Zyklus** = k-Tupel der Form (a_1, \dots, a_k) mit $\pi(a_k) = a_1, \pi(a_i) = a_{i+1}$, jedes Element von S_n kann als Komposition elementfremder Zyklen notiert werden: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = (1, 2, 3) \circ (4, 5) = (123)(45)$
- bei elementfremden Zyklen ist Reihenfolge egal: $(123)(45) = (45)(123)$; Elemente die auf sich selbst abgebildet werden heißen **Fixpunkte** und müssen nicht notiert werden: $(123)(4) = (123)$; mit welchem Element im Zyklus angefangen wird ist Egal: $(123)(45) = (312)(54)$
- **Transposition** = 2-Zyklus, jedes Element von S_n kann mit Transpositionen geschrieben werden als: $(a_1 \dots a_k) = (a_1 a_2)(a_2 a_3) \dots (a_{k-1} a_k)$ (nicht elementfremd \Rightarrow Reihenfolge wichtig!!)
- bei Komposition von Permutationen für jede Zahl von rechts nach links durchgehen: $\underbrace{(123)}_{(2)} \underbrace{(35)}_{(1)} = \underbrace{(1235)}_{(3)}$
5 wird in (1) auf 3 abgebildet, in (2) wird 3 auf 1 abgebildet, also $5 \rightarrow 3 \rightarrow 1$ und damit 5 \rightarrow 1 in (3)
- für $\alpha = (125)(38)(47)$ ist $\text{ord}(\alpha) = \text{kgV}(\underbrace{3, 2, 2}_{\text{ord der Zyklen}}) = 6 \Rightarrow \alpha^6 = \text{id}_X \Rightarrow \alpha^5 = \alpha^{-1}, \alpha^n = \alpha^{n \bmod 6}$
für α^{-1} kann man auch einfach Zeilen vertauschen

2.4 Beweis mittels vollständiger Induktion (Beispiel)

Beweis. Die Aussage A_n sei $\sum_{k=0}^n q^k = \frac{1-q^{n+1}}{1-q}$ mit $n \in \mathbb{N}, q \in \mathbb{R}, q \neq 1$.

$$(IA): n_0 = 0: \sum_{k=0}^0 q^k = q^0 = 1 = \frac{1-q^{0+1}}{1-q} \quad \text{w.A.} \\ \Rightarrow \text{Es gilt } A_0$$

$$(IV): \forall \tilde{n} : n_0 \leq \tilde{n} \leq n : \sum_{k=0}^{\tilde{n}} q^k = \frac{1-q^{\tilde{n}+1}}{1-q}$$

$$(IS): \sum_{k=0}^{n+1} q^k = \sum_{k=0}^n q^k + q^{n+1} \stackrel{(IV)}{=} \frac{1-q^{n+1}}{1-q} + q^{n+1} = \frac{1-q^{n+1} + (1-q)q^{n+1}}{1-q} \\ = \frac{1-q^{n+1} + q^{n+1} - q^{n+2}}{1-q} = \frac{1-q^{(n+1)+1}}{1-q}$$

\Rightarrow Damit ist die Behauptung für alle $n \in \mathbb{N}$ vollständig bewiesen □

- "Die Aussage A_n sei..." nur in VL und AuD Skript, *evtl.* wird sonst aber z.Z.: erwartet; IV muss auch nicht unbedingt notiert werden
- alles nochmal mit $(n+1)+1$ hinschreiben ist nicht nötig
- Varianten: $A_n \Rightarrow A_{n+1}$ / aus A_n folgt A_{n+1} für alle $n \in \mathbb{N}$
w.A. / Folglich gilt A_n für alle $n \in \mathbb{N}, n \geq n_0$
- Beachte dass oft auch nur für $n \in \mathbb{N}, n \geq k$ bewiesen wird (kein \tilde{n})!! und $n_0 = 0$ nicht immer gelten muss

2.5 Zahlentheorie

- $n \in \mathbb{N}, n \geq 1$ kann *eindeutig* geschrieben werden als $n = \prod_{i=1}^k p_i^{\alpha_i}$ (p_i prim, $\alpha_i \in \mathbb{N}$, "PFZ")
 \Rightarrow #Teiler von $n = \prod_i (\alpha_i + 1)$
- für $a, b \in \mathbb{N}$ gilt $a \mid b \Leftrightarrow \exists k : k \in \mathbb{N} \wedge ak = b$; $a \mid b_1 \wedge a \mid b_2 \Rightarrow a \mid (b_1 + b_2) \wedge a \mid (b_1 - b_2)$
- für $m, n \in \mathbb{Z}$ mit $n > 0$ gilt $\exists q, r : (q, r \in \mathbb{Z} \wedge m = nq + r \wedge 0 \leq r < n)$
 $m \bmod n := r$, für $a \bmod n = b \bmod n$ schreibe $a \equiv b \bmod n$
- **Homomorphieregel:** $(a \bmod n + b \bmod n) \bmod n = (a + b) \bmod n$ (analog für \cdot)
- $\text{kgV}(m, 0) = \text{kgV}(0, n) = 0$; $\text{ggT}(m, n) \cdot \text{kgV}(m, n) = m \cdot n$ (\Rightarrow kgV mit Euklid berechenbar)
- **Euklidischer Algorithmus:** für $m, n \in \mathbb{N}, m \leq n$!, immer weiter $\text{ggT}(m, n) = \text{ggT}(n \bmod m, m)$ berechnen;
 $\text{ggT}(m, n) = m$ falls $m \mid n$; $\text{ggT}(0, n) = n$; m, n teilerfremd $\Leftrightarrow \text{ggT}(m, n) = 1$
- **Lemma von Bézout:** $m, n \in \mathbb{N} \Rightarrow \exists a, b : a, b \in \mathbb{Z} \wedge \text{ggT}(m, n) = am + bn$ (a, b nicht eindeutig)
- **Erweiterter Euklidischer Algorithmus** am Beispiel ("EEA", keine offizielle Abkürzung):

	$\overbrace{1008}^m$	$\overbrace{499}^n$	$-q_i$					
1008	1	0			1008	1	0	
499	0	1			499	0	1	
$1008 \bmod 499 = 10$	1	$0 + 1 \cdot (-q_i) = -2$	$1008 = 499 \cdot 2 + 10 \Rightarrow -q_i = -2$	\Rightarrow	10	1	-2	-2
$499 \bmod 10 = 9$	-49	$1 + (-2)(-q_i) = 99$	$499 = 10 \cdot 49 + 9 \Rightarrow -q_i = -49$		9	-49	99	-49
$10 \bmod 9 = \underbrace{1}_{\text{ggT}}$	50	$-2 + 99(-q_i) = -101$	$10 = 9 \cdot 1 + 1 \Rightarrow -q_i = -1$		1	50	-101	-1
$9 \bmod 1 = 0$	STOP							

in m Spalte wird analog zu n Spalte gerechnet; EEA für $m, n \in \mathbb{Z}$: mit $|m|, |n|$ rechnen, dann Ergebnis anpassen
 $\Rightarrow \text{ggT}(1008, 499) = 1 = 50 \cdot 1008 - 101 \cdot 499$ (Bézout Koeffizienten $a = 50, b = -101$)

- **chinesischer Restsatz:** Seien $0 < n_1, \dots, n_k \in \mathbb{N}$ teilerfremd und seien $a_1, \dots, a_k \in \mathbb{Z}$. Dann existiert genau ein $x \in \{0, 1, \dots, \prod_{i=1}^k n_i - 1\}$ mit $x \equiv a_i \bmod n_i$ für alle $i = 1, \dots, k$
- für $k = 2$: Seien $0 < m, n \in \mathbb{N}$ teilerfremd und seien $a_1, a_2 \in \mathbb{N}$. Dann existiert genau ein $x \in \{0, 1, \dots, mn - 1\}$ mit $x \equiv a_1 \bmod m \wedge x \equiv a_2 \bmod n$; anschaulich heißt das, dass ein $m \times n$ Spielbrett eindeutig wie in VL durchnummeriert werden kann wenn $\text{ggT}(m, n) = 1$

2.6 Gruppentheorie

- Gruppe (G, \circ) (auch $(G; \circ, ^{-1}, e)$; dann Definition einfach anders formulieren) besteht aus Menge G und innerer Verknüpfung $\circ : G \times G \rightarrow G$, so dass: \circ assoziativ, es existiert **neutrales Element** $e \in G$ ($a \circ e = a = e \circ a$ für alle $a \in G$), es existiert **Inverses** $a^{-1} \in G$ zu jedem $a \in G$ (mit $a \circ a^{-1} = e = a^{-1} \circ a$)
- beweisen, dass es sich um eine Gruppe handelt z.B. per Tabelle möglich, oft kann man auch argumentieren dass Eigenschaften wie Assoziativität geerbt werden
- Gruppe heißt **abelsch**/kommutativ, falls \circ kommutativ ist
- $\mathbb{Z}_n = \{0, \dots, n-1\}$ bildet mit Addition mod n eine Gruppe; Menge aller Permutationen auf einer Menge kann als Gruppe aufgefasst werden, z.B. Eckenpermutationen eines Quadrates (" D_4 " / " D_8 ") (Komposition führt zu Drehungen, Spiegelungen und Identitätsabbildung)
- Nullteiler** mod n sind $a \in \mathbb{Z}_n \setminus \{0\}$ für die $b \in \mathbb{Z}_n \setminus \{0\}$ existiert mit $a \cdot b \equiv 0 \pmod n$
Einheiten mod n sind $a \in \mathbb{Z}_n$ für die $b \in \mathbb{Z}_n$ existiert mit $a \cdot b \equiv 1 \pmod n$, 1 ist immer eine Einheit
 m ist Einheit mod $n \Leftrightarrow m$ ist kein Nullteiler mod $n \Leftrightarrow \text{ggT}(m, n) = 1$
- Die Menge der Einheiten mod n heißt \mathbb{Z}_n^* und bildet eine Gruppe mit Multiplikation mod n ; es gilt mit PFZ, dass $\phi(n) := |\mathbb{Z}_n^*| = \prod_{i=1}^k (p_i^{\alpha_i} - p_i^{\alpha_i-1}) = \#$ zu n teilerfremde Zahlen die kleiner (-gleich) n sind
- eine multiplikative Gruppe ist **zyklisch**, falls $g \in G$ existiert mit $G = \{g^j \mid j \in \mathbb{Z}\}$, ein solches g heißt **Erzeuger** von G (Potenzrechengesetze ähnlich wie in \mathbb{N} , für additive Gruppen schreibe $G = \{jg \mid j \in \mathbb{Z}\}$); für Erzeuger gilt mit $|G| = n$, dass $G = \{g^j \mid j \in \mathbb{Z}_n\}$;
- Erzeuger von $(\mathbb{Z}_n, + \pmod n)$ sind genau die Elemente von $\mathbb{Z}_n^* \Rightarrow \# \text{ Erzeuger} = \phi(n)$
- Ein **Satz von Gauß**: für p prim ist $(\mathbb{Z}_p^*, \cdot \pmod n)$ zyklisch; $\# \text{ Erzeuger} = \phi(p-1) = \phi(\phi(p))$; diese Erzeuger heißen **Primitivwurzeln**

n	2	...	n
g_1^n			
\vdots			
g_n^n			

- "Finden Sie Erzeuger/Primitivwurzel/ist G zyklisch?": i.A. Tabelle erstellen ($n = |G|$)
sobald man für $j \neq 0$ auf $g^j = 1$ kommt kann man aufhören (da gilt $j \in \mathbb{Z}_n$ und damit immer schon $1 = g^0$)
- Inverses zu Einheit g von \mathbb{Z}_n berechnen: $\text{EEA}(n, g) \Rightarrow 1 = ag + bn \Rightarrow 1 \equiv ag \pmod n$
Achtung: evtl. ist $a \notin \mathbb{Z}_n$!!! (z.B. weil a negativ $\Rightarrow g^{-1} = n - a$)
- isomorph**=Strukturgleich ("man kann Elemente einfach umbenennen"), jede zyklische Gruppe ist isomorph entweder zu $(\mathbb{Z}, +)$ oder einem $(\mathbb{Z}_n, + \pmod n)$; als Beweis das zwei Gruppen nicht isomorph sind genügt z.B. " G_1 ist zyklisch, G_2 nicht"
- $U \subseteq G$ heißt **Untergruppe** von G falls $e \in U$; $a \circ b \in U$ für alle $a, b \in U$; $a^{-1} \in U$ für alle $a \in U$
- $\langle g \rangle := \{g^i \mid i \in \mathbb{Z}\}$ ist **von g erzeugte Untergruppe**
- $g \circ U = \{g \circ u \mid u \in U\}$ ist eine **(Links-)Nebenklasse** ("LNK") von U , $|g \circ U| = |U|$, 2 LNK sind entweder gleich oder disjunkt \Rightarrow jedes $g \in G$ liegt in genau einer LNK (nämlich $g \circ U$)
- Satz von Lagrange**: $|G| = |G : U| \cdot |U|$ ($|G : U| = \# \text{ LNK von } U \text{ in } G = \text{Index von } U \text{ in } G$)
 $|G|$ heißt Ordnung von G , $o(g) := |\langle g \rangle|$ Ordnung von g ; $g^{|G|} = e$
- "Finden Sie alle $\langle g \rangle$ ": ausnutzen welche Werte für $o(g)$ nach Lagrange nur möglich sind
"Finden Sie Untergruppen der Ordnung 2/3": U_2 enthält nur 1 und g mit $g^2 = 1$, U_3 enthält nur 1 und g_1, g_2 mit $g_1^2 = g_2, g_2^2 = g_1$ (\Rightarrow beides per Verknüpfungstafel lösbar)
- "Finden Sie die LNK von U ": per Verknüpfungstafel rechnen, ausnutzen dass LNK gleich oder disjunkt sind
- Satz von Euler-Fermat**: Seien $n \in \mathbb{N}, a \in \mathbb{Z}$ mit $\text{ggT}(a, n) = 1$. Dann gilt $a^{\phi(n)} \equiv 1 \pmod n$. (bei kleinem Fermat gilt n prim)
- für Beweise bieten sich oft Verknüpfungstafeln an, folgende Methoden helfen beim effizient rechnen: Kongruenz mit kleineren negativen Zahlen ausnutzen, für \circ kommutativ ist Tafel symmetrisch bzgl. Hauptdiagonale, Sudokuprinzip (jede Zahl nur ein mal pro Zeile/Spalte)
- dass $\text{ggT}(m, n) \geq 2$ kann man auch damit begründen, dass m, n beide z.B. 2 in PFZ haben, für ggT von kleinen Zahlen ist keine Begründung nötig
- Gleichungen in \mathbb{Z}_n : $123^{321} \cdot x \equiv 3^{321} \pmod{\phi(40)} \cdot x \equiv 3x \equiv 4 \pmod{40}$, mit $3^{-1} = 27$ folgt $x \equiv (27 \cdot 4) \pmod{40}$

2.7 Effizient potenzieren mod n

- andere Form von Euler-Fermat: $a^m \equiv a^{m \bmod \phi(n)} \pmod{n}$, gilt aber auch nur für $\text{ggT}(a, n) = 1$!!
- einfach die Zahlen Stück für Stück mit mod zerlegen

2.8 Kryptographie

- für p prim und g Primitivwurzel von \mathbb{Z}_p^* ist der **diskrete Logarithmus** von $x \in \mathbb{Z}_p^*$ zur Basis g die Zahl $m \in \{0, \dots, p-2\}$ mit $g^m \equiv x \pmod{p}$ ($m = \log_g(x)$); m kann nicht effizient berechnet werden, x aus g^m schon

• Diffie-Hellman-Merkle:

1. Alice und Bob einigen sich auf Primzahl p und Primitivwurzel g von \mathbb{Z}_p^*
2. Alice wählt geheime Zufallszahl a und berechnet $a' = g^a \pmod{p}$; Bob analog: $b' = g^b \pmod{p}$
3. beide teilen sich a' und b' mit und berechnen das Geheimnis $c = g^{ab} \pmod{p} = (a')^b \pmod{p} = (b')^a \pmod{p}$

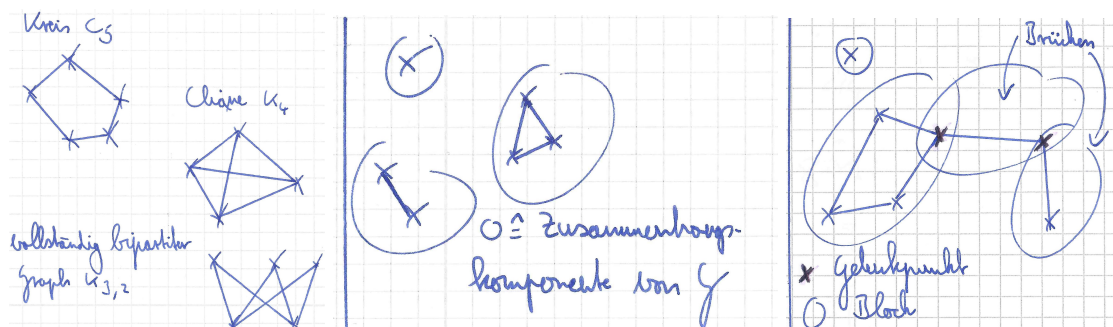
Um damit Nachricht $m \leq c$ zu verschlüsseln:

1. schreibe m und c binär als $m = m_1 \dots m_l, c = c_1 \dots c_k$
2. Alice verschickt $v_1 = m_1 + c_1 \pmod{2}, \dots, v_l = m_l + c_l \pmod{2}$; Bob berechnet $m_i = v_i + c_i \pmod{2}$

• RSA:

1. Bob wählt zufällig 2 verschiedene Primzahlen p, q und berechnet $n := pq$
2. Bob wählt zufällig $d \in \mathbb{Z}_{\phi(n)}^*$ und berechnet $i, h \in \mathbb{Z}$ mit $i \cdot d + h \cdot \phi(n) = \text{ggT}(d, \phi(n)) = 1$ (EEA)
3. n und i sind öffentliche Schlüssel und werden an Alice weitergegeben, d ist privater Schlüssel
4. Alice schickt $c = m^i \pmod{n}$ an Bob mit Nachricht m ($0 \leq m < n$)
5. Bob berechnet $m = c^d \pmod{n}$

2.9 Ungerichtete Graphen



- **Komplementgraph** $\bar{G} := \left(V, \binom{V}{2} \setminus E \right)$ (statt $\binom{V}{2}$ scheint $\{X \subset V : |X| = 2\}$ sicherer zu sein)
- $G_1 = (V_1, E_1), G_2 = (V_2, E_2)$ sind **isomorph**, wenn es eine Bijektion $f : V_1 \rightarrow V_2$ gibt, so dass $\{u, v\} \in E_1$ g.d.w. $\{f(u), f(v)\} \in E_2$ für alle $u, v \in V_1$. (d.h. es muss auch gelten $|E_1| = |E_2|$) ($G_1 \cong G_2$) ("sind G_1, G_2 gleich wenn man die Knoten in G_2 umbenennt?")
- **Subgraph** von G heißt ein Graph H mit $V(H) \subseteq V(G), E(H) \subseteq E(G)$. H heißt **induzierter Subgraph** von G , wenn $E(H) = E(G) \cap \binom{V(H)}{2}$ (also wenn aus G nur Knoten und nur die damit verbundenen Kanten gelöscht wurden), wir schreiben $H = G[V(H)]$
- ein Graph ist **k -färbbar**, wenn die Knoten so in k Farben angemalt werden könnten, dass 2 benachbarte Knoten nie die gleiche Farbe haben (z.B. C_n immer 3-färbbar, 2-färbbar g.d.w. n gerade) (i.A. einfach durch probieren lösen)
- G zweifärbbar (\Leftrightarrow bipartit) g.d.w. es in G keine ungeraden Kreise gibt; G ist **bipartit** g.d.w. disjunkte A, B (**Partitionsklassen**) existieren, so dass $V(G) = A \cup B \wedge \binom{A}{2} \cap E = \binom{B}{2} \cap E = \emptyset$
- Graph ohne Kreise = **Wald**; zusammenhängender Graph ohne Kreise = **Baum**, für Bäume gilt $|E| = |V| - 1$; Knoten mit $\deg = 1$ heißen **Blätter**

- "Geben Sie bis auf Isomorphie alle Bäume an für die gilt...." \Rightarrow alle Kombinationen von Knotengraden durchgehen, die bei gegebenem $|V|$ in Frage kommen
- G ist **k -fach zusammenhängend** wenn $G \setminus X = G[V \setminus X]$ zusammenhängend ist für alle $X \subseteq V$ mit $|X| = k-1$; G k -fach zusammenhängend $\Leftrightarrow G$ enthält für alle $a, b \in V$ mindestens k paarweise unabhängige Pfade von a nach b (unabhängig heißt haben nur Anfangs- und Endpunkt gemeinsam)
- ob k paarweise unabhängigen Pfade für k -fachen Zusammenhang vorliegen muss man i.A. für jedes Paar (a, b) einzeln prüfen, evtl. Aufwand verringern durch Symmetrien möglich, außerdem gilt $\min\{\deg(v) \mid v \in V\} \geq k$
- G ist **zweifach zusammenhängend** $\Leftrightarrow G$ kann aus einem Kreis durch sukzessives Anhängen von Pfaden konstruiert werden kann \Leftrightarrow es gibt keine Gelenkpunkte in $G \Leftrightarrow$ jeder Knoten liegt mit jedem anderen auf einem Kreis
- Sei A Menge der Gelenkpunkte von G , \mathcal{B} Menge der Blöcke, dann ist $(A \cup \mathcal{B}, \{\{a, B\} \mid a \in A, B \in \mathcal{B}, a \in B\})$ der **Blockgraph** von G ; Blockgraph ist ein Wald und für G zusammenhängend ein Baum
Blöcke können nicht als Kantenzüge angegeben werden, am besten einfach zeichnen!
- Pfade sind **disjunkt** wenn sie keine Knoten gemeinsam haben und **kantendisjunkt** falls sie keine Kanten gemeinsam haben; bei einem A - B -Pfad liegt nur der Anfangsknoten in A , nur der Endknoten in B
- **Satz von Menger:** Seien $A, B \subseteq V$. Dann ist die maximale Anzahl von paarweise disjunkten A - B -Pfaden in G gleich der Mächtigkeit einer kleinsten Knotenmenge, die A von B in G **trennt** (aus der also jeder A - B -Pfad einen Knoten enthält)
- **Kantengraph** $L(G)$ hat die Knotenmenge E und Kantenmenge $\{\{e, f\} \mid e, f \in E, |e \cap f| = 1\}$. Ist (u_0, \dots, u_n) Kantenzug/Pfad in G , so ist $(\{u_0, u_1\}, \dots, \{u_{n-1}, u_n\})$ Kantenzug/Pfad in $L(G)$
(für Kantenzüge gilt auch die Umkehrung)
- die maximale Anzahl von kantendisjunkten Pfaden von a nach b ist gleich der Mächtigkeit einer kleinsten Kantenmenge, die a von b **trennt** (trennt hat hier andere Bedeutung als bei Mengen: $F \subseteq E$ trennt a und b , wenn es in $(V, E \setminus F)$ keinen Kantenzug von a nach b gibt)
- G ist **k -fach kantenzusammenhängend**, falls für alle $F \subseteq E$ mit $|F| < k$ gilt $(V, E \setminus F)$ ist zusammenhängend; G k -fach kantenzusammenhängend \Leftrightarrow für je 2 $a, b \in V$ gibt es mindestens k kantendisjunkte Pfade von a nach b
- Ist G k -fach kantenzusammenhängend und $k \geq 2$, so ist $L(G)$ k -fach knotenzusammenhängend
- **offener Eulerzug** = Kantenzug, der jede Kante von G genau einmal durchläuft mit Anfangsknoten \neq Endknoten (Haus vom Nikolaus); **(geschlossener) Eulerzug** = Eulerzug bei dem Anfangs- und Endknoten gleich sind
- es gibt einen Eulerzug in $G \Leftrightarrow \forall v \in V : \deg(v)$ gerade; es gibt einen offenen Eulerzug in $G \Leftrightarrow$ es gibt genau 2 Knoten von ungeradem Grad in G
- $M \subseteq E$ heißt **Paarung** von G , falls die Element von M paarweise disjunkt sind. Für **perfekte Paarungen** gilt $2|M| = |V|$ (d.h. jeder Knoten taucht in genau einem Element von M auf). M ist eine **Paarung von $S \subseteq V$** , falls M Paarung von G und jedes Element von S in einer Kante von M auftaucht.
- Pfad in G heißt **alternierend** bzgl. M , falls er abwechselnd über Kanten aus M und $E \setminus M$ läuft; ein **alternierender** Pfad P heißt **augmentierend** bzgl. M , falls Start- und Endpunkt von P in keiner Kante aus M liegen (P beginnt und endet also auf Kante aus $E \setminus M$)
- **Lemma von Berge:** Eine Paarung M von G ist genau dann größtmöglich, wenn es keinen augmentierenden Pfad in G bzgl. M gibt.
- für $S \subseteq V$ heißt $N(S) = \{n \in V \mid \exists s \in S \text{ mit } s \text{ Nachbar von } n\}$ die **Nachbarschaft** von S
- Existiert eine Paarung M von S in G , so gilt $|N(S)| \geq |S|$
- **Heiratssatz von Hall:** Sei $\{A, B\}$ Bipartition von G . Dann gibt es genau dann eine Paarung von A in G , wenn $|N(S)| \geq |S|$ für alle $S \subseteq A$. $\Rightarrow k$ -reguläre (=jeder Knoten hat $\deg k$) bipartite Graphen haben eine perfekte Paarung
- Eine **Überdeckung** von G ist eine Teilmenge $U \subseteq V$, so dass jede Kante von G ein Element aus U enthält.
Satz von König: Die Größe einer minimalen Überdeckung von G ist gleich der Größe einer größten Paarung.
- Handschlaglemma für Graphen: $\sum_{v \in V} \deg(v) = 2|E|$ (=gerade!!, das ist wichtig für Beweise)

2.10 Gerichtete Graphen

- für $(u, v) \in E$ ist u Vorgänger von v , v Nachfolger von u
- für gerichtete Graphen gilt $E \subseteq V \times V$; $G^{-1} = (V, E^{-1})$ mit $E^{-1} = \{(y, x) \mid (x, y) \in E\}$ (Pfeile umkehren, hat die selben SZK wie G); $G[V'] = (V', E \cap (V' \times V'))$; "Schleifen" sind erlaubt ("Schleife" = gerichteter Kreis der Länge 1)
- Für $u, v \in V$ schreibe $u \preceq v$, falls es in G einen Pfad von u nach v gibt. \preceq ist transitive reflexive Hülle von $E \Rightarrow \preceq$ Quasiordnung auf V , \preceq Ordnung wenn es in G keine Kreise gibt
- Schreibe $u \sim v$ falls $u \preceq v \wedge v \preceq u$. Die Äquivalenzklassen von \sim heißen die **starken Zusammenhangskomponenten** von G ("SZK")

Algorithmen für gerichtete Graphen werden nicht geprüft

2.11 Aussagenlogik

- $\top / \perp =$ wahr/falsch; \wedge, \vee kommutativ, assoziativ, distributiv in beide Richtungen
De Morgansche Gesetze: $\neg(x \wedge y) = \neg x \vee \neg y, \neg(x \vee y) = \neg x \wedge \neg y$
- jeder **Ausdruck** A (=Verbindung von $\top, \perp, \neg, \wedge, \vee$, Variablensymbolen) definiert eine **boolsche Funktion** $f_A : \{0, 1\}^n \rightarrow \{0, 1\}$; A heißt **tautologisch/Tautologie** wenn $f_A(a_1, \dots, a_n) = 1$ für alle $a_1, \dots, a_n \in \{0, 1\}$
- schreibe $A \Rightarrow B$ für $\neg A \vee B$, $A \Leftrightarrow B$ für $(A \Rightarrow B) \wedge (B \Rightarrow A)$ (d.h. \Rightarrow ist immer wahr außer für $1 \Rightarrow 0$, \Leftrightarrow ist wahr für $1 \Leftrightarrow 1$ und $0 \Leftrightarrow 0$); es gilt $A \Rightarrow B$ äquivalent zu $\neg B \Rightarrow \neg A$ (**Kontraposition**)
- Ausdrücke A, B sind **äquivalent** wenn $f_A = f_B$ (d.h. wenn $A \Leftrightarrow B$ Tautologie); A **impliziert** B ($A \models B$) wenn jede erfüllende Belegung von A schon erfüllende Belegung von B ist (d.h. wenn $A \Rightarrow B$ Tautologie)
- **Darstellungssatz:** für jede n -stellige boolsche Funktion f existiert Ausdruck A in n Variablen, so dass $f_A = f$ (außerdem gilt f kann immer in KNF und DNF dargestellt werden)
- **disjunktive Normalform (DNF):** $\bigvee_i \bigwedge_j L_{ij}$; **konjunktive Normalform (KNF):** $\bigwedge_i \bigvee_j L_{ij}$
Beispiel: Sei f gegeben durch Tabelle. Es gilt $f = f_A = f_B$.

a_1, a_2	$f(a_1, a_2)$	
0,0	0	
0,1	1	$A = (\underbrace{\neg X_1 \wedge X_2}_{\text{Literal } L_{ij}}) \vee (\underbrace{X_1 \wedge X_2}_{\text{Klausel}})$
1,0	0	
1,1	1	

DNF

$B = (\underbrace{X_1 \vee X_2}_{\text{Klausel}}) \wedge (\underbrace{\neg X_1 \vee X_2}_{\text{Klausel}})$

KNF

- eine Aussage in **KNF (!!)** heißt **Horn**, falls jede Klausel maximal ein positives Literal (L_{ij} der Form X) enthält
- Algorithmus für **Horn-SAT**:
 1. suche nach Klausel der Gestalt X , lösche dann alle Literale der Gestalt $\neg X$
 2. falls dadurch leere Klausel entsteht **return NEIN**
 3. gehe zu 1. solange noch etwas gelöscht werden kann
 4. **return JA**

Beispiel: $A = (X_1 \vee \neg X_2 \vee \neg X_3) \wedge X_3$ Ausdruck ist Horn \Rightarrow Horn-SAT Algorithmus anwendbar
 X_3 ist eine Klausel $\Rightarrow \neg X_3$ streichen
 $A \Leftrightarrow (X_1 \vee \neg X_2) \wedge X_3 \Rightarrow$ JA (ist erfüllbar)

- erfüllende Belegung für Horn-SAT: Setze alle Variablen X mit Klausel der Gestalt X auf 1, alle anderen auf 0
- Beweise in Aussagenlogik über Ausdrücke umformen oder Wertetabelle (mit Zwischenschritten!!) oder Fallunterscheidung; gleiche Herangehensweise für "gesucht sind alle erfüllenden Belegungen", gilt z.B. Ausdruck $A = B$ müssen in Tabelle nur noch 2^{n-1} Belegungen geprüft werden

2.12 Relationen

- $R \subseteq A \times B$ heißt Relation, wir schreiben $(a, b) \in R$ oder aRb ; für Beweise sind oft Gegenbeispiele hilfreich
- mögliche Eigenschaften von $R \subseteq A \times A$: **reflexiv** (aRa für alle $a \in A$); **transitiv** ($aRb \wedge bRc \models aRc$ für alle $a, b, c \in A$); **symmetrisch** ($aRb \models bRa$ für alle $a, b \in A$); **antisymmetrisch** ($aRb \wedge bRa \models a = b$ für alle $a, b \in A$)
- R ist eine **Äquivalenzrelation** ("ÄR") falls gilt R reflexiv, symmetrisch, transitiv; R_1, R_2 ÄR $\models R_1 \cap R_2$ ÄR
- $a/R := \{b \in A \mid (a, b) \in R\}$ heißt **Äquivalenzklasse** ("ÄK") von a ("alles was mit a in Relation steht"); $A/R := \{a/R \mid a \in A\}$ Menge der ÄK; 2 ÄK sind entweder gleich oder disjunkt
- eine **Partition** von A ist eine Menge \mathcal{P} deren Elemente nichtleere Teilmengen von A sind, so dass gilt $\bigcup_{X \in \mathcal{P}} X = A$ und alle X sind gleich oder disjunkt; A/R ist eine Partition von A ; $\# \text{ÄR auf } A = \# \text{Partitionen von } A$
- Relationen können als gerichtete Graphen visualisiert werden; reflexiv=jeder Knoten hat Schlinge, transitiv= für jeden Pfad der Länge 2 gibt es Abkürzung, symmetrisch: wenn \rightarrow dann \Leftarrow , ÄK=Zusammenhangskomponenten; ÄR können auch als ungerichtete Graphen visualisiert werden
- Ordnung heißt man kann das sortieren \Rightarrow Graph darf keine gerichteten Kreise enthalten
- R ist eine **Ordnung** falls R reflexiv, antisymmetrisch, transitiv; **Quasiordnung** falls R reflexiv und transitiv
Beispiele: Teilbarkeitsrelation auf \mathbb{N} ; jede ÄR (nur Quasiordnung, keine Ordnung); \subseteq (i.A. nicht total)
- R ist **totale (Quasi-) Ordnung** falls R eine (Quasi-) Ordnung ist und je zwei Elemente x, y von A vergleichbar sind (d.h. $(x, y) \in R \vee (y, x) \in R$) Beispiele: \leq auf \mathbb{N} ; ÄR mit nur einer ÄK (nur totale Quasiordnung); $R = \{(a, b) \in \mathbb{C} \times \mathbb{C} : |a| \leq |b|\}$ (nur totale Quasiordnung)
- für R Ordnung auf A und $M \subseteq A$ heißt $x \in M \dots$
 - **maximales Element** von M , falls xRy schon $x = y$ impliziert für alle $y \in M$; **minimales Element** von M , falls yRx schon $y = x$ impliziert für alle $y \in M$
 - **größtest Element** von M , falls yRx für alle $y \in M$; **kleinstes Element** von M , falls xRy für alle $y \in M$
- gibt es ein größtes Element von M , so ist es eindeutig bestimmt und auch das einzige maximale Element von M ; analog für kleinstes
- für $R \subseteq A \times A$ ist $R \circ R = \{(a_1, a_3) \in A \times A \mid \text{es gibt } a_2 \in A \text{ mit } (a_1, a_2) \in R \wedge (a_2, a_3) \in R\}$; $R^0 = \{(a, a) \mid a \in A\}$, $R^1 = R, R^2 = R \circ R$ etc. (im gerichteten Graph entspricht R^k allen "Abkürzungen" für Wege der Länge k)
- für jede Relation R auf A existiert eine Quasiordnung auf A die R enthält. Sei R' die kleinste Quasiordnung die R enthält (**transitive reflexive Hülle**). Dann gilt $R' = \bigcup_{i \geq 0} R^i$ (das ganze berechnen bis $R^i = R^k$ für $i \geq k$, d.h. bis keinen neuen "Abkürzungen" mehr hinzukommen können)
- für jede Relation R auf A existiert eine transitive Relation auf A die R enthält. Sei R' die kleinste transitive Relation die R enthält (**transitive Hülle**). Dann gilt $R' = \bigcup_{i \geq 1} R^i$

Hinweis: In den Zusammenfassungen wird die Schreibweise x_1, \dots, x_n verwendet um Platz zu sparen, gebräuchlicher ist aber x_1, x_2, \dots, x_n

Immer angeben welche Sätze angewendet werden und warum sie anwendbar sind!

Bestimmen heißt Begründen! Nicht nur sagen "es gibt ungerade Kreise", sondern auch Beispiel angeben.