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 $\{\{1,2\},7\} \nsubseteq \mathbb{N}$
- 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 $\emptyset \in \mathcal{P}(A)$
- $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$
- **Handschlaglemma:** Anzahl der Teilnehmer einer Konferenz, die einer ungeraden Anzahl von Teilnehmern die Hand geben, ist immer gerade

2.2 Abbildungen

- für $f : A \to B, A' \subseteq A$ 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 $\boldsymbol{f^{-1}}$ **:** $f[A] \to A, b \mapsto f^{-1}(b) = a$ mit $f^{-1}(b) = a$ g.d.w. $f(a) = b$
- für $f : A \to B, g : B \to C$ ist **Komposition** $g \circ f : A \to C, x \mapsto g(f(x))$ ($\Rightarrow$ von rechts nach links ausführen!!)

2.3 Permutationen

- **Permutation** von X ist bijektive Abbildung von X nach X, für $X = \{1, \ldots, n\}$ ist S_n Menge aller Permutationen und $\pi \in S_n$ mit $\pi = \begin{pmatrix} 1 & \ldots & n \\ \pi(1) & \ldots & \pi(n) \end{pmatrix}$ und $|S_n| = n!$
- **k-Zyklus** = k-Tupel der Form $(a_1, \ldots, a_k)$ 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:
  $(a_1, \ldots, a_k) = (a_1 a_2)(a_2 a_3) \ldots (a_{k-1} a_k)$ (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 $5 \to 3 \to 1$ und damit $5 \to 1$ in *(3)*

2.4 Beweis mittels vollständiger Induktion (Beispiel)

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

(IA): $n_0 = 0$: $\sum_{k=0}^{0} q^k = q^0 = 1 = \dfrac{1-q^{0+1}}{1-q}$ w.A.

$\Rightarrow$ Es gilt A_0

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

(IS): $\sum_{k=0}^{n+1} q^k = \sum_{k=0}^{n} q^k + q^{n+1} \overset{\text{(IV)}}{=} \dfrac{1-q^{n+1}}{1-q} + q^{n+1} = \dfrac{1-q^{n+1}+(1-q)q^{n+1}}{1-q}$

$= \dfrac{1-q^{n+1}+q^{n+1}-q^{n+2}}{1-q} = \dfrac{1-q^{(n+1)+1}}{1-q}$

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

- "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 $a \mid b \Leftrightarrow \exists k : k \in \mathbb{N} \wedge ak = b$; $\quad a \mid b_1 \wedge a \mid b_2 \Rightarrow a \mid (b_1 + b_2) \wedge a \mid (b_1 - b_2)$
- 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 $\cdot$)
- $\mathrm{kgV}(m,0) = \mathrm{kgV}(0,n) = 0$; $\mathrm{ggT}(m,n) \cdot \mathrm{kgV}(m,n) = m \cdot n$ ($\Rightarrow$ kgV mit Euklid berechenbar)
- **Euklidischer Algorithmus:** immer weiter $\mathrm{ggT}(m,n) = \mathrm{ggT}(n \bmod m, m)$ berechnen; $\mathrm{ggT}(m,n) = m$ falls $m \mid n$; $\mathrm{ggT}(0,n) = n$; m, n teilerfremd $\Leftrightarrow \mathrm{ggT}(m,n) = 1$
- **Lemma von Bézout:** $m, n \in \mathbb{N} \Rightarrow \exists a, b : a, b \in \mathbb{Z} \wedge \mathrm{ggT}(m,n) = am + bn$
- **Erweiterter Euklidischer Algorithmus** am Beispiel ("EEA", keine offizielle Abkürzung):

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

$\Rightarrow$

	1008	499	$-q_i$
1008	1	0	
499	0	1	
10	1	-2	-2
9	-49	99	-49
1	50	-101	-1

in m Spalte wird analog zu n Spalte gerechnet, das ganze bis in der linken Spalte 0 stehen würde

$\Rightarrow \mathrm{ggT}(1008, 499) = 1 = 50 \cdot 1008 - 101 \cdot 499$ (Bézout Koeffizienten $a = 50, b = -101$)

- **chinesischer Restsatz:** Seien $0 < n_1, \ldots, n_k \in \mathbb{N}$ teilerfremd und seien $a_1, \ldots, a_k \in \mathbb{Z}$. Dann existiert genau ein $x \in \left\{0, 1, \ldots, \prod_{i=1}^{k} n_i - 1\right\}$ mit $x \equiv a_i \bmod n_i$ für alle $i = 1, \ldots, k$
- für $k = 2$: Seien $0 < m, n \in \mathbb{N}$ teilerfremd und seien $a_1, a_2 \in \mathbb{N}$. Dann existiert genau ein $x \in \{0, 1, \ldots, mn-1\}$ 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 $\mathrm{ggT}(m,n) = 1$

2.6 Gruppentheorie

- Gruppe $(G, \circ)$ (auch $(G; \circ, ^{-1}, e)$; dann Definition einfach anders formulieren) besteht aus Menge G und innerer Verknüpfung $\circ : G \times G \to G$ so dass: $\circ$ assoziativ, es existiert **neutrales Element** e ($a \circ e = a = e \circ a$ für alle $a \in G$), es existiert **Inverses** a^{-1} zu jedem $a \in G$ ($a \circ a^{-1} = e = a^{-1} \circ a$)
- Gruppe heißt **abelsch**/kommutativ, falls $\circ$ kommutativ ist
- $\mathbb{Z}_n = \{0, \ldots, n-1\}$ bildet mit Addition mod n eine Gruppe; Symmetrien eines Quadrates ("D_4"/"D_8")/Dreiecks etc. bilden ebenfalls eine Gruppe (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 $a \cdot b \equiv 0 \bmod n$
  Einheiten mod n sind $a \in \mathbb{Z}_n$ für die $b \in \mathbb{Z}_n$ existiert mit $a \cdot b \equiv 1 \bmod n$; 1 ist immer eine Einheit
  m ist Einheit mod $n \Leftrightarrow$ m ist kein Nullteiler mod $n \Leftrightarrow \mathrm{ggT}(m, n) = 1$
- 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
- multiplikative Gruppe ist **zyklisch** falls $g \in G$ existiert mit $G = \left\{g^j \mid j \in \mathbb{Z}\right\}$ (Potenzrechengesetze ähnlich wie in $\mathbb{N}$, für additive Gruppen schreibe $G = \{jg \mid j \in \mathbb{Z}\}$); Erzeuger sind $g \in G, |G| = n$ so dass $G = \left\{g^j \mid j \in \mathbb{Z}_n\right\}$; Erzeuger von $\mathbb{Z}_n$ sind genau die Elemente von $\mathbb{Z}_n^* \Rightarrow \#$ Erzeuger$= \phi(n)$
- für p prim ist $(\mathbb{Z}_p^*, \cdot \bmod n)$ zyklisch; $\#$ Erzeuger$= \phi(p-1)$; diese Erzeuger heißen **Primitivwurzeln**
- **Isomorph**=Strukturgleich ("man kann Elemente einfach umbenennen"), jede zyklische Gruppe ist isomorph entweder zu $(\mathbb{Z}, +)$ oder einem $(\mathbb{Z}_n, + \bmod n)$; 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 $a \in U$
- $\langle g \rangle := \left\{g^i \mid i \in \mathbb{Z}\right\}$ 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:** $|G| = |G : U| \cdot |U|$ ($|G : U| = \#$ LNK von U in G=Index von U in G)
  $|G|$ heißt Ordnung von G, $\mathrm{o}(g) := |\langle g \rangle|$ Ordnung von g
- **Satz von Euler-Fermat:** Seien $n \in \mathbb{N}, a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$. Dann gilt $a^{\phi(n)} \equiv 1 \bmod n$. (bei kleinem Fermat gilt n prim)
- für Beweise bieten sich oft Verknüpfungstafeln an, folgende Methoden helfen beim effizient rechnen:

2.7 Effizient potenzieren mod n

- andere Form von Euler-Fermat: $a^m \equiv a^{m \bmod \phi(n)}$ mod n, gilt aber auch nur für $\mathrm{ggT}(a, n) = 1$!!
- 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 $m \in \{0, \ldots, p-2\}$ mit $g^m \equiv x \bmod p$ ($m = \log_g(x)$); 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 $a' = g^a \bmod p$; Bob analog: $b' = g^b \bmod p$
  3. beide teilen sich a' und b' mit und berechnen das Geheimnis $c = g^{ab} \bmod p = (a')^b \bmod p = (b')^a \bmod p$

  Um damit Nachricht $m \leq c$ zu verschlüsseln:
  1. schreibe m und c binär als $m = m_1 \ldots m_l, c = c_1 \ldots c_k$
  2. Alice verschickt $v_1 = m_1 + c_1 \bmod 2, \ldots, v_l = m_l + c_l \bmod 2$; Bob berechnet $m_i = v_i + c_i \bmod 2$
- **RSA:**
  1. Bob wählt zufällig 2 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 $i \cdot d + h \cdot \phi(n) = \mathrm{ggT}(d, \phi(n)) = 1$ (EEA)
  3. n und i sind öffentliche Schlüssel und werden an Alice weitergegeben, d ist privater Schlüssel
  4. Alice schickt $c = m^i \bmod n$ an Bob mit Nachricht m ($0 \leq m < n$)
  5. Bob berechnet $m = c^d \bmod n$

2.9 Ungerichtete Graphen

2.10 Gerichtete Graphen

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** $f_A : \{0,1\}^n \to \{0,1\}$; A heißt **tautologisch/Tautologie** wenn $f_A(a_1, \ldots, a_n) = 1$ für alle $a_1, \ldots, a_n \in \{0,1\}$
- 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 war 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 $A \Rightarrow B$ Tautologie
- **Darstellungssatz:** für jede n-stellige boolsche Funktion f existiert Ausdruck A in n Variablen, so dass $f_A = f$
- **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
1,0	0
1,1	1

$$A = \underbrace{(\underbrace{\neg X_1}_{\textbf{Literal } L_{ij}} \wedge X_2) \vee \underbrace{(X_1 \wedge X_2)}_{\textbf{Klausel}}}_{\text{DNF}} \quad B = \underbrace{(X_1 \vee X_2) \wedge (\neg X_1 \vee X_2)}_{\text{KNF}}$$

- 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; danach `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
  $A \Leftrightarrow (X_1 \vee \neg X_2) \wedge X_3 \quad \Rightarrow$ JA (ist erfüllbar)
- Beweise in Aussagenlogik über Ausdrücke umformen oder Wertetabelle

2.12 Relationen