

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 $\emptyset \in \mathcal{P}(A)$
- $\binom{n}{k} = \frac{n!}{k!(n-k)!}$
- **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)

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 $n = \prod_{i=1}^k p_i^{\alpha_i}$ mit p_i prim, $\alpha_i \in \mathbb{N} \Rightarrow \# \text{Teiler} = \prod_i (\alpha_i + 1)$
- 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)
- $\text{ggT}(0, 0) = 0$; $\text{kgV}(m, 0) = \text{kgV}(0, n) = 0$; $\text{ggT}(m, n) \cdot \text{kgV}(m, n) = m \cdot n$; m, n teilerfremd für $\text{ggT}(m, n) = 1$
- **Euklidischer Algorithmus** (EA, keine offizielle Abkürzung):
- **Erweiterter Euklidischer Algorithmus** (EEA, keine offizielle Abkürzung):
- **Lemma von Bézout**
- **Al Kashi's Trick**
- **chinesischer Restsatz**

2.6 Gruppentheorie

2.7 Kryptographie

- **diskreter Logarithmus:**
- **Diffie-Hellman-Merkle:**
- **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 $i \cdot d + h \cdot \phi(n) = \text{ggT}(d, \phi(n)) = 1$ (EEA)
3. n und i sind öffentliche Schlüssel und werden an Alice weitergegeben, d ist privater Schlüssel
4. Alice schickt $c = m^i \bmod n$ an Bob mit Nachricht m ($0 \leq m < n$)
5. Bob berechnet $m = c^d \bmod n$ (Potenzieren mit Al Kashi oder Euler-Fermat oder Zahl zerlegen)

2.8 Ungerichtete Graphen

2.9 Gerichtete Graphen

2.10 Aussagenlogik

2.11 Relationen