Diskrete Mathematik für Informatiker

Rebecca Busch

Universität Siegen

Wintersemester 2016/2017

Übersicht über die Themen

- Mengentheoretische Grundlagen
- Aussagenlogik & Prädikatenlogik
- Beweisprinzipien
- Kombinatorik: Abzählen von Mengen
- Kombinatorik: Einfache Identitäten
- Kombinatorik: Der Binomische Lehrsatz
- Graphentheorie: Grundbegriffe
- Graphentheorie: Planare Graphen
- Graphentheorie: Färbungen von Graphen
- Graphentheorie: Matchings
- Graphentheorie: Euler- und Hamiltonpfade
- Algebraische Strukturen: Monoide und Gruppen
- Zahlentheorie
- Zahlentheorie: RSA-Verschlüsselung
- Zahlentheorie: Fibonacci-Zahlen
- Algebraische Strukturen: Ringe und Körper

Bemerkungen

Es folgen ein paar Themen, die bereits in der Vorlesung behandelt wurden. Die Themen sind **nicht** vollständig und in der Klausur können Aufgaben zu allen Bereichen aus der Vorlesung vorkommen! Diese Themen sind also lediglich ein Einstieg in ihre Vorbereitungen zur Klausur! Ich wünsche ihnen viel Erfolg in den Vorbereitungen und ein gutes Gelingen in der Klausur!

Mengentheoretische Grundlagen

Mengen

- $\mathbb{N} = \{0, 1, 2, 3, 4, 5, \ldots\}$ (Menge der natürlichen Zahlen)
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ (Menge der ganzen Zahlen)
- $\mathbb{Q} = \{\frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{Z}, q \neq 0\}$ (Menge der rationalen Zahlen)
- $P = \{n \in \mathbb{N} \mid n \geq 2, n \text{ ist nur durch 1 und } n \text{ teilbar}\}$ (Menge der Primzahlen)
- $\mathbb{R}$ (Menge der rationalen Zahlen + Menge der irrationalen Zahlen)
- $\mathbb{C} = \{x + i \cdot y \mid x, y \in \mathbb{R}\}$ (Menge der komplexen Zahlen)
- $\mathbb{Z}_n$ (Menge der ganzen Zahlen mod n)
- $2^A = \{B \mid B \subseteq A\}$ (Potenzmenge oder Menge aller Teilmengen)

Mengentheoretische Grundlagen

Definition (Relationen und Funktionen)

Seien A und B Mengen.

Eine Relation von A nach B ist eine Teilmenge $R \subseteq A \times B$.

Eine (binäre) Relation auf A ist eine Teilmenge $R \subseteq A \times A$.

Eine Funktion (oder Abbildung) von A (dem Definitionsbereich) nach B (dem Wertebereich) ist eine Relation $f \subseteq A \times B$, so dass für alle $a \in A$ genau ein $b \in B$ mit $(a, b) \in f$ existiert. Wir schreiben dann auch $f(a) = b$.

Wir schreiben auch $f : A \to B$ für eine Funktion f von A nach B.

Definition (injektive/surjektive/bijektive Funktionen)

Eine Funktion $f : A \to B$ is injektiv, falls für alle $a, b \in A$ gilt:
Wenn $a \neq b$ gilt, muss auch $f(a) \neq f(b)$ gelten
(verschiedene Elemente werden auf verschieden Elemente abgebildet).

Eine Funktion $f : A \to B$ is surjektiv, falls für alle $b \in B$ ein $a \in A$ mit $f(a) = b$ existiert (jedes Element aus B wird durch f getroffen).
Äquivalent: $f(A) = B$.

Eine Funktion $f : A \to B$ is bijektiv, falls sie injektiv und surjektiv ist.
Wir sagen auch, dass f eine Bijektion ist.

Definition (Umkehrfunktion)

Für eine bijektive Funktion $f : A \to B$ kann man die Umkehrfunktion $f^{-1} : B \to A$ definieren durch folgende Vorschrift:

$$f^{-1}(b) = a \text{ genau dann, wenn } f(a) = b$$

Mengentheoretische Grundlagen

Definition ((ir)reflexive/(anti)symmetrische/transitive Relationen)

Sei A eine Menge und $R \subseteq A \times A$ eine Relation auf A.

- R ist reflexiv, falls aRa für alle $a \in A$ gilt.
- R ist irreflexiv, falls kein $a \in A$ mit aRa existiert.
- R ist symmetrisch, falls für alle $a, b \in A$ gilt:
  Wenn aRb, dann auch bRa.
- R ist antisymmetrisch, falls für alle $a, b \in A$ gilt:
  Wenn aRb und bRa, dann $a = b$.
- R ist transitiv, falls für alle $a, b, c \in A$ gilt:
  Wenn aRb und bRc, dann auch aRc.

Mengentheoretische Grundlagen

- **Der direkte Beweis:** Wir zeigen: Wenn A gilt, dann gilt auch B.$(A \to B)$
- **Der Äquivalenzbeweis:** Wir zeigen: Wenn A gilt, dann gilt auch B und wenn B gilt, dann gilt auch A.$((A \to B) \wedge (B \to A))$
- **Der Widerspruchsbeweis:** Wir zeigen: Wenn B nicht gilt, dann gilt A auch nicht.$(\neg B \to \neg A)$
- **Beweis durch vollständige Induktion**

Satz 5(Prinzip der vollständigen Induktion)

Sei $A \subseteq \mathbb{N}$. Angenommen es gilt

- $0 \in A$ und
- für alle $n \in A$ gilt auch $n + 1 \in A$.

Dann gilt $A = \mathbb{N}$.

Zahlentheorie: RSA-Verschlüsselung

RSA-Verfahren:

1. Der Empfänger E wählt zwei (große — z. B. 1000 Bits lange) verschiedene Primzahlen p und q (werden geheim gehalten).
2. E berechnet $n = p \cdot q$ und $\varphi(n) = (p-1) \cdot (q-1)$.
3. E berechnet zwei Zahlen k und ℓ mit $\mathrm{ggT}(k, \varphi(n)) = 1$ und $k \cdot \ell \equiv 1 \mod \varphi(n)$.
4. Öffentlicher Kodierungsschlüssel: n und k
5. Geheimer Dekodierschlüssel: ℓ.
6. Nachrichten sind Elemente aus $\mathbb{Z}_n$
7. Verschlüsseln: $m \mapsto (m^k \bmod n)$ für $m \in \mathbb{Z}_n$
8. Entschlüsseln: $m \mapsto (m^\ell \bmod n)$ für $m \in \mathbb{Z}_n$

Satz 56 (Korrektheit des RSA-Verfahrens)

Es gilt $(m^k)^\ell \equiv m \mod n$ für alle $m \in \mathbb{Z}_n$.

Kombinatorik: Der Binomische Lehrsatz

Satz 23 (Binomischer Lehrsatz)

Für alle natürlichen Zahlen $n \geq 0$ und alle reellen Zahlen $x, y \in \mathbb{R}$ gilt:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Satz 23 (etwas verändert: Binomischer Lehrsatz)

Für alle natürlichen Zahlen $n \geq 0$ und alle reellen Zahlen $x, y \in \mathbb{R}$ gilt:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

Kombinatorik: Einfache Identitäten

Satz 21 (Symmetrie der Binomialkoeffizienten)

Es gilt $\binom{n}{k} = \binom{n}{n-k}$.

Satz 20 (Additionseigenschaft der Binomialkoeffizienten)

Es gilt $\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$.

Satz 22 (Vandermondische Identität)

Es gilt:

$$\sum_{j=0}^{k} \binom{m}{j} \cdot \binom{n}{k-j} = \binom{m+n}{k}.$$

Algebraische Strukturen: Monoide und Gruppen

Definition (Monoid, Gruppe)

Ein Monoid ist ein Paar $(A, \circ)$, wobei gilt:

- A ist eine beliebige Menge.
- $\circ : A \times A \to A$ ist eine 2-stellige Operation auf A; anstatt $\circ(a, b)$ schreiben wir $a \circ b$.
- $\circ$ ist assoziativ, d. h. $\forall a, b, c \in A : (a \circ b) \circ c = a \circ (b \circ c)$.
- Es existiert ein neutrales Element e bzgl. $\circ$, d. h. $\exists e \in A \; \forall a \in A : a \circ e = e \circ a = a$.

Ein Monoid $(A, \circ)$ ist eine Gruppe, falls für jedes $a \in A$ ein Inverses existiert: $\forall a \in A \; \exists b \in A : a \circ b = b \circ a = e$ (wobei e neutral ist).

Algebraische Strukturen: Monoide und Gruppen

Definition (Kommutative Monoide und Gruppen)

Ein Monoid (eine Gruppe) $(A, \circ)$ ist kommutativ, falls für alle $a, b \in A$ gilt: $a \circ b = b \circ a$.

Kommutative Gruppen nennt man auch Abelsche Gruppen.

Definition (zykliche Gruppen)

Eine Gruppe $(G, \circ)$ ist zyklisch, falls ein $g \in G$ existiert mit $G = \{g^n \mid n \in \mathbb{Z}\}$.

Das Element g bezeichnen wir dann auch als einen Erzeuger von G.

Definition (Untergruppen)

Sei $\mathbb{G} = (G, \circ)$ eine Gruppe. Eine nicht-leere Teilmenge $U \subseteq G$ ist eine Untergruppe von $\mathbb{G}$, wenn gilt:

$$\forall a \in U : a^{-1} \in U \quad \text{und} \quad \forall a, b \in U : a \circ b \in U$$

Graphentheorie: Grundbegriffe

Definition (isomorphe Graphen)

Zwei Graphen $G_1 = (V_1, E_1)$ und $G_2 = (V_2, E_2)$ sind isomorph, falls es eine bijektive Abbildung $f : V_1 \to V_2$ gibt mit

$$\forall x, y \in V_1 : \{x, y\} \in E_1 \iff \{f(x), f(y)\} \in E_2$$

Definition (planare Graphen)

Ein Graph $G = (V, E)$ ist planar, wenn er in die Ebene so eingezeichnet werden kann, dass sich die Kanten nicht schneiden.

Definition (planare Graphen)

Ein Graph G ist planar, falls er eine planare Einbettung (p, ℓ) in den $\mathbb{R}^2$ hat.

Graphentheorie: Planare Graphen

Eine planare Einbettung des Graphen $G = (V, E)$ in den $\mathbb{R}^2$ ist ein Paar (p, ℓ), wobei gilt:

- $p : V \to \mathbb{R}^2$ ist injektiv und ordnet jedem Knoten einen Punkt des $\mathbb{R}^2$ zu.
- $\ell : E \to 2^{\mathbb{R}^2}$ ordnet jeder Kante $\{x, y\} \in E$ einen Linienzug $\ell(x, y)$ mit den Endpunkten $p(x)$ und $p(y)$ zu, so dass für alle Kanten $\{u, v\}, \{x, y\} \in E$ mit $\{u, v\} \neq \{x, y\}$ gilt:

$$(\ell(u, v) \setminus \{p(u), p(v)\}) \cap \ell(x, y) = \emptyset$$

Graphentheorie

Weitere wichtige Begriffe in der Graphentheorie sind:

- bipatit
- Zusammenhangskomponente
- Facette
- k-Färbung von G / Färbungszahl $\chi(G)$
- Maximalgrad $\Delta(G)$
- d-regulär
- Matching / Matchingzahl $\mu(G)$
- M-satuiert / M- alternierender Weg / M- erweiternd
- Knotenüberdeckung / $\gamma(G)$
- Eulerpfad / Eulerkreis
- Hamiltonpfad / Hamiltonkreis