
Vorwort

Wenn sich Studierende der Informatik oder verwandter Fächer in den ersten Wochen ihres Studiums befinden, wundern sie sich häufig, wie viele Lehrveranstaltungen der Mathematik sie besuchen müssen. Die Zusammenhänge zwischen diesen Vorlesungen und der Informatik sind den Studierenden am Anfang oft ziemlich rätselhaft. Ein Anliegen dieses Buchs ist es daher, den Stellenwert der Mathematik für die Informatik deutlich zu machen. Dies wollen wir erreichen, indem wir die mathematischen Sachverhalte nicht nur gut verständlich und präzise darstellen, sondern auch viele ihrer Anwendungen in der Informatik ausführlich beschreiben.

Im ersten Studienjahr hören Informatikerinnen und Informatiker in der Regel Vorlesungen zur Analysis und linearen Algebra. Entsprechend gibt es viele Bücher für Studienanfänger, die diese Themen fundiert behandeln (siehe beispielsweise [33, 34, 60, 70]). Zur Auffrischung der Kenntnisse stellen wir in diesem Buch die betreffenden Inhalte der beiden Bereiche nur kurz dar. Wir behandeln vor allem den Stoff von Mathematikveranstaltungen, die im zweiten oder in späteren Studienjahren gehört werden.

Kap. 1 gibt eine Einführung in die Logik, die eine zentrale Rolle in der Mathematik spielt. Wir gehen auf die Aussagen- und Prädikatenlogik ein sowie auf die Anwendung in der Programmverifikation und der logischen Programmierung. Mengen, Relationen und Funktionen betrachten wir in Kap. 2. In diesem Zusammenhang behandeln wir unter anderem relationale Datenbanken und die funktionale Programmierung. Zahlensysteme und die Mächtigkeit von Mengen untersuchen wir in Kap. 3. Ein wichtiges Thema für die Informatik ist hier die Darstellung von Zahlen in Rechnern. Dem Algorithmus, einem zentralen Begriff der Informatik, widmen wir uns in Kap. 4. Um die Komplexität von Algorithmen zu untersuchen, sind die Begriffe Folgen, Reihen und stetige Funktionen aus der Analysis notwendig, die kurz wiederholt werden. Danach können wir auf die Größenordnung von Funktionen eingehen, mit deren Hilfe die Beschränkung der Rechenzeit oder des Platzbedarfs von Algorithmen ausgedrückt werden können. Mit der Darstellung von Rekurrenzgleichungen und erzeugenden Funktionen gelingt es uns, für wichtige Typen von Algorithmen, zu denen etwa die binäre Suche oder Quicksort gehören, die Zeitkomplexität zu bestimmen. Außerdem erläutern wir das mathematische Konzept der Matroide. Mit ihrer Hilfe können wir das Verhalten von „gierigen“ Algorithmen beschreiben.

Kap. 5 gibt einen ersten Einblick in die Graphentheorie. Ihrer Anwendung in der Informatik geben wir breiten Raum. Die Graphentheorie ist eine wichtige Grundlage für Datenstrukturen, die das Speichern und das schnelle Wiederfinden von Daten ermöglichen. Kap. 6 beschäftigt sich zunächst mit den Grundlagen der Zahlentheorie wie Teilbarkeit und Primzahlen. Danach betrachten wir die modulare Arithmetik, mit deren Hilfe wir das RSA-Public-Key-Kryptosystem ausführlich untersuchen können. Als eine weitere Anwendung in der Kryptografie stellen wir ein Secret-Sharing-Verfahren vor.

Nachdem wir in Kap. 6 in Zusammenhang mit der modularen Arithmetik schon die ersten algebraischen Begriffe erwähnt haben, untersuchen wir die Algebra in den Kap. 7 bis 9 systematisch. Den Anfang machen die einfachen algebraischen Strukturen Halbgruppen und Monoide in Kap. 7. Speziell betrachten wir freie Monoide. Unter anderem zeigen wir, wie sie in der Informatik zur Beschreibung von formalen Sprachen und Programmiersprachen, etwa durch Grammatiken, eingesetzt werden können. Kap. 8 widmet sich der Gruppentheorie. Dabei wird als eine Anwendung von zyklischen Gruppen das ElGamal-Public-Key-Verschlüsselungsverfahren behandelt. Ringe, Polynomringe und Körper untersuchen wir in Kap. 9. Besonders wichtig sind endliche Körper und ihre multiplikativen Gruppen. Diese Gruppen sind zyklisch und können beim ElGamal-Public-Key-Verschlüsselungsverfahren eingesetzt werden, was wir an einem Beispiel erläutern.

In Kap. 10 geben wir in den Abschn. 10.1 bis 10.5 eine Kurzdarstellung der linearen Algebra. Dadurch sind wir in der Lage, weitere wichtige Anwendungen der Mathematik in der Informatik zu beschreiben. Als Erstes betrachten wir in diesem Zusammenhang in Abschn. 10.6 das Information-Retrieval, bei dem es darum geht, aus einer Datenbank Informationen zurückzugewinnen. In fast allen einführenden Büchern zur linearen Algebra fehlt die für viele Anwendungen – nicht nur in der Informatik – wichtige Singulärwertzerlegung von Matrizen, die wir daher ausführlich in Abschn. 10.7 behandeln. In Abschn. 10.8 wenden wir sie in der Computergrafik an. Die Algebra und die Lineare Algebra sind in der Codierungstheorie von besonderer Bedeutung. Bei der Übertragung von Nachrichten über Funk, Telefon oder das Internet werden Zeichen geeignet codiert. Im ausführlichen Abschn. 10.9 geben wir daher eine erste Einführung in lineare Codes. Danach behandeln wir in Abschn. 10.10 einige Secret-Sharing-Verfahren, die sowohl Methoden der linearen Algebra als auch der Gruppentheorie verwenden. Im letzten Abschn. 10.11 zeigen wir, wie die unterschiedlichen algebraischen Strukturen aus den Kap. 7 bis 10 durch den Begriff einer allgemeinen oder mehrsortigen Algebra einheitlich beschrieben werden können. Wir weisen darauf hin, dass in der Informatik mehrsortige Algebren auch für die Spezifikation abstrakter Datentypen besonders wichtig sind.

Gegenstand von Kap. 11 ist die Wahrscheinlichkeitstheorie. Zunächst stellen wir die wichtigsten Grundbegriffe der Kombinatorik dar. Danach behandeln wir Wahrscheinlichkeitsräume, diskrete und stetige Zufallsvariable sowie einige ihrer Anwendungen in der Informatik, etwa die Analyse von Algorithmen. Die Untersuchung stetiger Zufallsvariablen setzt Basiskenntnisse der Integralrechnung voraus. Die notwendigen Begriffe und Aussagen werden daher kurz zusammengestellt. Den Abschluss des Buchs bildet eine Einführung in die Theorie stochastischer Prozesse. Schwerpunkt dieses Abschnitts sind

Markow-Ketten, deren Anwendung wir an einem Beispiel aus dem Gebiet der Betriebssysteme (Bediensysteme) erläutern.

Unser Buch kann als Grundlage für verschiedene Mathematikvorlesungen für Informatiker dienen. In den Bachelorstudiengängen der Informatik und der Mathematik ist es üblich, Module aus zweistündigen bis vierstündigen Vorlesungen mit einer Übung zu bilden. So sind unseres Erachtens die beiden Kapitel über Graphentheorie und Grundlagen der Zahlentheorie für eine zweistündige Vorlesung über diskrete Strukturen geeignet. Die Kap. 7 bis 9 und zusätzlich aus Kap. 10 die Abschn. 10.9 über lineare Codes, 10.10 über Secret-Sharing-Verfahren und 10.11 über allgemeine Algebra sind für eine dreistündige Vorlesung, eventuell auch zwei zweistündige Vorlesungen zur Algebra zu verwenden. Das Kap. 11 kann als Begleitung einer zweistündigen Vorlesung zur Wahrscheinlichkeitstheorie dienen. Die ersten vier Kapitel des Buchs liefern allgemeine Grundlagen der Mathematik mit einigen Anwendungen in der Informatik, über die eine entsprechende Vorlesung angeboten werden könnte. Diese Kapitel sind aber für jede Leserin und jeden Leser geeignet, sich mit mathematischen Grundlagen vertraut zu machen oder diese wieder aufzufrischen. Beim Lesen anderer Kapitel des Buchs kann es nützlich sein, gelegentlich zu diesen Grundlagen zurückzugehen. Die Gegenstände der Abschn. 4.3 (Größenordnung von Funktionen), 4.4 (Rekurrenzgleichungen und erzeugende Funktionen) und 4.5 (Matroide) können auch im Rahmen einer Vorlesung über Algorithmen verwendet werden.

Zum Selbststudium eignet sich das Buch ebenfalls sehr gut. Die Kap. 7 bis 10 sollten in dieser Reihenfolge gelesen werden. Aus Kap. 7 sind allerdings nur die wichtigsten Definitionen für die folgenden Kapitel notwendig. Für das Verständnis von Kap. 11 muss die Leserin oder der Leser einige Grundlagen der Analysis kennen, die in den Abschn. 4.1 und 4.2 zu finden sind. Die übrigen Kapitel können unabhängig voneinander gelesen werden. Jedoch wird ein gewisses intuitives Verständnis der Logik und Mengenlehre vorausgesetzt.

Dieses Buch stellt die wichtigsten Grundlagen der Mathematik für Informatiker zusammen. Es ist klar, dass wir nicht die gesamte Mathematik, die auf irgendeine Art für die Informatik von Bedeutung ist, behandeln können. Die eine Informatikerin wird beispielsweise noch etwas über numerische Mathematik wissen wollen, die zweite über Statistik und ein dritter Informatiker benötigt noch weitergehende Kenntnisse der Graphentheorie. Auf der Basis dieses Buchs sollte es aber möglich sein, sich in spezielle Mathematikbücher zu diesen Themen einzuarbeiten.

Zu jedem Kapitel gibt es Übungsaufgaben. Die Lösungen sind auf der [WWW-Seite](http://www.tu-braunschweig.de/ips/staff/struckmann/mathematik)

<http://www.tu-braunschweig.de/ips/staff/struckmann/mathematik>

des Buchs zu finden. Da nicht damit zu rechnen ist, dass das Buch vollständig fehlerfrei ist, haben wir unter dieser URL ebenfalls eine Fehlerliste eingerichtet. Wir bitten die Leser, uns Fehler mitzuteilen, die dort noch nicht aufgeführt sind, seien es nun Tipp-, Rechtschreib- oder auch logische Fehler.

Besonders bedanken möchten wir uns bei *Frau Dipl.-Math. Katrin Wätjen* für das Korrekturlesen des Buchs. Einige Monate lang hat sie dieser Aufgabe einen großen Teil ihrer Freizeit gewidmet. Ihre kritischen Anmerkungen haben zu vielen Verbesserungen geführt. Außerdem möchten wir *Prof. Dr. Arnfried Kemnitz* danken, der mehrere Kapitel Korrektur gelesen hat, sowie *Dr. Andreas Rüdinger* und *Bianca Alton* von Elsevier Deutschland (Spektrum Akademischer Verlag) für ihre Unterstützung bei der Abfassung und Veröffentlichung dieses Buchs.

In dieser zweiten Auflage des Buches haben wir Kap. 12 mit dem Gegenstand Algorithmen und Programme eingefügt. Zwar werden in verschiedenen vorhergehenden Kapiteln spezielle Algorithmen betrachtet, hier wird jedoch eine allgemeinere Darstellung von Algorithmen und ihre Umsetzung in Programmiersprachen behandelt. Es wird auf die Formulierung, die Komplexität und Korrektheit von Algorithmen eingegangen. Weitere Aspekte in diesem Kapitel sind Berechenbarkeitsfragen und Rekursionen als spezielle Algorithmen.

Wir bedanken uns bei Frau Dorothea Glaunsinger und Herrn Hermann Engesser vom Springer-Verlag, die diese zweite Auflage unseres Buches betreut haben.

Braunschweig, im April 2016

Werner Struckmann, Dietmar Wätjen

Mathematik für Informatiker
Grundlagen und Anwendungen
Struckmann, W.; Wätjen, D.
2016, XI, 551 S. 97 Abb.,
ISBN: 978-3-662-49870-5