
Diskrete Mathematik

Karl-Heinz Zimmermann

Diskrete Mathematik

Books on Demand

Prof. Dr. Karl-Heinz Zimmermann
TU Hamburg-Harburg
21071 Hamburg
Germany

Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen
Nationalbibliografie; detaillierte bibliografische Daten sind im Internet
abrufbar über <http://dnb.ddb.de>.

Alle Rechte vorbehalten
©2006 Karl-Heinz Zimmermann, Autor

Herstellung und Verlag: Books on Demand GmbH, Norderstedt
Umschlaggestaltung: Wolfgang Brandt, TU Hamburg-Harburg
Gedruckt auf säure-, holz- und chlorfreiem Papier
Printed in Germany

ISBN 3-8334-5529-2

Für meinen Lehrer
Prof. Dr. Thomas Beth
16.11.1949 – 17.08.2005

Vorwort

Das Buch entstand aus einer viersemestrigen, jeweils zweistündigen Vorlesung über Diskrete Mathematik, die ich an der Technischen Universität Hamburg-Harburg für Studenten des Informatik-Ingenieurwesens in den letzten Jahren gehalten habe. Dieses Buch behandelt neben den Grundlagen der Diskreten Mathematik auch eine Reihe weiterführender Themen, deren Kenntnis heute von jedem Informatiker und Mathematiker erwartet wird. Es eignet sich für das Selbststudium und als Textbuch zum Gebrauch neben der Vorlesung.

Die Diskrete Mathematik ist die Mathematik der endlichen Mengen, besser gesagt, der endlichen Konfigurationen unter Nebenbedingungen. Dabei geht es u.a. um die Abzählung, Konstruktion und Existenz von Konfigurationen und das Rechnen mit Konfigurationen. Wichtige Teilgebiete der Diskreten Mathematik sind Kombinatorik, Graphentheorie, Verbandstheorie, Codierungstheorie, Kryptographie und kombinatorische Optimierung. Zudem stellt die Diskrete Mathematik Algorithmen und Datenstrukturen bereit und ist damit verknüpft mit der Theoretischen Informatik.

Im ersten Teil des Buches steht der Aufbau der modernen Mathematik im Vordergrund. Zunächst werden Grundbegriffe der mathematischen Logik und Mengenlehre dargestellt, soweit sie als sprachliches Gerüst der modernen Mathematik dienen. Anschließend werden Relationen, insbesondere Abbildungen, Äquivalenzen und Ordnungen, untersucht. Der erste Teil schließt mit dem Aufbau der natürlichen Zahlen sowie der Abzählbarkeit von Mengen.

Der zweite Teil führt in die elementare Kombinatorik ein. Zuerst werden Zählprinzipien vorgestellt, die grundlegend für den Aufbau der Kombinatorik sind. Danach wird die Abzählungstheorie der klassischen Abbildungstypen mit Nebenbedingungen entwickelt.

Im dritten Teil werden die klassischen euklidischen Ringe, der Ring der ganzen Zahlen und die Polynomringe, sowie die Restklassenringe modulo n untersucht. Die multiplikative Struktur dieser Ringe wird eingehender beleuchtet.

Im vierten Teil werden zuerst die grundlegenden Eigenschaften linearer Codes skizziert. Anschließend wird die Theorie der endlichen Körper entwickelt und wichtige Klassen linearer Codes vorgestellt.

Im fünften Teil wird die Verbandstheorie anhand der Ordnungstheorie aufgebaut. Als wichtiges Beispiel werden Begriffsverbände umfänglicher behandelt. Danach werden boolesche Verbände dargestellt und eine wichtige Klasse boolescher Verbände, Schaltalgebren, untersucht, mit deren Hilfe kombinatorische Schaltkreise beschrieben werden.

Der sechste Teil beginnt mit einer Einführung in die Graphentheorie. Dann werden grundlegende Algorithmen für Netzwerke präsentiert und Methoden vorgestellt, um komplexe Optimierungsprobleme näherungsweise zu lösen. Schließlich werden die Grundlagen der linearen Optimierung behandelt. Insbesondere wird gezeigt, dass die adressierten Netzwerk-Probleme durch lineare Programme gelöst werden können.

Im letzten Teil wird die kombinatorische Abzählungstheorie nach Pólya entwickelt und das Schubfachprinzip zur Ramsey-Theorie erweitert. Letztere gehört zu den wichtigsten Werkzeugen der existenziellen Kombinatorik.

Jedes Kapitel schließt mit einem anwendungszogenen Beispiel und einer Reihe von Selbsttestaufgaben. Lösungshinweise zu diesen Aufgaben findet der interessierte Leser auf meiner Homepage.

Das vorliegende Buch kann als Textbuch für Vorlesungen über Diskrete Mathematik dienen. Die folgende Tabelle liefert eine mögliche Zuordnung zwischen Vorlesungen und Kapiteln des Buches:

Vorlesung (zweistündig)	Kapitel
Diskrete Mathematik I	1 bis 11
Diskrete Mathematik II	12 bis 15 (teilweise 15.4), 19 bis 21
Diskrete Mathematik III	22 bis 24, 26
Diskrete Mathematik IV	15.4, 16 bis 18, 25

Danken möchte ich Dr. Prashant Batra, Stefan Goltz, Dr. Andreas Popp, Markus Volkmer und Dr. Otto Wohlmuth, die teils frühere Versionen des Manuskripts durchgesehen haben. Mein Dank gilt auch den Hörern meiner Vorlesungen, die durch ihr großes Interesse und ihre hilfreichen Kommentare an der Entstehung dieses Buches mitgewirkt haben. Danken möchte ich auch Wolfgang Brandt für die Gestaltung der Umschlagseite. Schließlich möchte ich dem Verlag *Books on Demand* meinen Dank für die gute Zusammenarbeit aussprechen.

Mathematische Notation

\underline{n}	$\{1, \dots, n\}$
\mathbb{N}	Menge der natürlichen Zahlen
\mathbb{N}_0	Menge der natürlichen Zahlen inklusive 0
\mathbb{Z}	Menge der ganzen Zahlen
\mathbb{Z}_n	Menge der Restklassen modulo n
\mathbb{Z}_n^*	Menge der Einheiten in \mathbb{Z}_n
\mathbb{Q}	Menge der rationalen Zahlen
\mathbb{R}	Menge der reellen Zahlen
\mathbb{R}_0^+	Menge der nichtnegativen reellen Zahlen
\mathbb{C}	Menge der komplexen Zahlen
\emptyset	leere Menge
$P(A)$	Potenzmenge von A
$ A $	Mächtigkeit von A
$\lfloor x \rfloor$	größte ganze Zahl kleiner gleich x
$\lceil x \rceil$	kleinste ganze Zahl größer gleich x

Inhaltsverzeichnis

Teil I Grundlagen

1	Grundlagen der Aussagenlogik	3
1.1	Aussagen	3
1.2	Aussageformen	4
1.3	Erfüllbarkeit und Gültigkeit	5
1.4	Äquivalenz	6
1.5	Schaltungsentwurf	8
2	Grundlagen der Prädikatenlogik	11
2.1	Objekte, Prädikate und Quantoren	11
2.2	Existentielle und universelle Quantifizierung	12
2.3	Variablen	14
2.4	Programmierung	15
2.5	Beweistechnik	18
3	Mengenlehre	23
3.1	Mengen und Elemente	23
3.2	Verknüpfung von Mengen	26
3.3	Mengensysteme	29
3.4	Axiomatische Mengenlehre	31
4	Relationen	37
4.1	Das kartesische Produkt	37
4.2	Der Relationsbegriff	39
4.3	Darstellung von Relationen	40
4.4	Komposition	41
4.5	Relationale Datenbanken	43

5	Homogene Relationen	47
5.1	Darstellung von homogenen Relationen	47
5.2	Äquivalenzen	48
5.3	Ordnungen	51
5.4	Hüllen	53
6	Abbildungen	55
6.1	Der Abbildungsbegriff	55
6.2	Spezielle Abbildungen	57
6.3	Familien, Folgen und Multimengen	59
6.4	Permutationen	62
6.5	Analyse von Algorithmen	66
7	Die natürlichen Zahlen	71
7.1	Vollständige Induktion	71
7.2	Arithmetik	72
7.3	Induktion und fundierte Mengen	76
7.4	Schleifenprogrammierung	77
8	Unendliche Mengen	81
8.1	Endliche und unendliche Mengen	81
8.2	Abzählbare und überabzählbare Mengen	82
8.3	Berechenbarkeit	86

Teil II Elementare Kombinatorik

9	Zählprinzipien	89
9.1	Elementare Zählprinzipien	89
9.2	Prinzip der doppelten Abzählung	90
9.3	Schubfachprinzip	91
9.4	Prinzip der Inklusion-Exklusion	92
10	Kombinationen und Permutationen	97
10.1	Kombinationen	97
10.2	Repetitionen	100
10.3	Permutationen	101
10.4	Permutationen und Zykeltypen	102
10.5	Variationen	104
11	Partitionen	109
11.1	Mengenpartitionen	109
11.2	Stirling-Zahlen	111
11.3	Zahlpartitionen	113

Teil III Arithmetik

12 Die ganzen Zahlen	119
12.1 Arithmetik der ganzen Zahlen	119
12.2 Ringe	121
12.3 Beispiele für Ringe	123
12.4 Homomorphismen	125
12.5 Schleifenparallelisierung	126
13 Teilbarkeitslehre	129
13.1 Division mit Rest	129
13.2 Der euklidische Algorithmus	131
13.3 Primfaktorisierung	133
13.4 Gödelisierung	135
14 Restklassenringe	137
14.1 Restklassenringe	137
14.2 Rechnen in Restklassenringen	140
14.3 Lineare Kongruenzsysteme	141
14.4 Kanonische Zerlegung von Restklassenringen	143
14.5 Modulares Rechnen	143
15 Einheiten in Restklassenringen	147
15.1 Einheiten und Nullteiler	147
15.2 Die Anzahl der Einheiten	149
15.3 Integritätsringe und Körper	151
15.4 Gruppen	152
15.5 RSA-Verfahren	159
16 Polynome	163
16.1 Polynomringe	163
16.2 Teilbarkeitslehre	165
16.3 Nullstellen	169
16.4 Irreduzible Polynome	172
16.5 Polynom-Interpolation	174
16.6 Divisionsschieberegister	176

Teil IV Codes

17 Lineare Codes	181
17.1 Linearcodes	181
17.2 Fehlerkorrigierende Linearcodes	184
17.3 Linearcodes von gleicher Qualität	191
17.4 Berechnung des Minimalabstandes	199

17.5	Schranken	201
17.6	Modifikation und Kombination	206
18	Endliche Körper	213
18.1	Körperweiterungen	213
18.2	Konstruktion und Eindeutigkeit	218
18.3	Existenz	222
18.4	Polynom-Faktorisierung	227
18.5	BCH-Codes	230
18.6	Reed-Solomon-Codes	231

Teil V Ordnungen und Verbände

19	Verbände	239
19.1	Der Verbandsbegriff	239
19.2	Ordnungsstrukturen als Verbände	241
19.3	Verbände als Ordnungsstrukturen	242
19.4	Unterverbände und Homomorphismen	244
19.5	Begriffsverbände	246
20	Boolesche Verbände	253
20.1	Distributive und komplementäre Verbände	253
20.2	Boolesche Algebren	256
20.3	Normalformen	257
20.4	Schaltalgebren	259
20.5	Kombinatorische Schaltkreise	264

Teil VI Graphen und Optimierung

21	Graphen	273
21.1	Grundbegriffe	273
21.2	Wege, Kreise und Zusammenhang	276
21.3	Planare Graphen	280
21.4	Datenstrukturen und Algorithmen	283
22	Netzwerke	287
22.1	Kürzeste Wege	287
22.2	Minimale Spannbäume	290
22.3	Maximale Flüsse	293
22.4	Die Sätze von Hall, König-Egerváry und Menger	299

23 Kombinatorische Optimierung	305
23.1 Komplexitätsklassen	305
23.2 Backtracking-Algorithmen	307
23.3 Heuristische Algorithmen	313
23.4 Greedy-Algorithmen und Matroide	319
23.5 Knotenfärbungen	322
24 Lineare Optimierung	327
24.1 Beispiele	327
24.2 Lineare Programme und Dualität	328
24.3 Der zulässige Bereich und die Rolle der Ecken	333
24.4 Ganzzahlige Programmierung	336
24.5 Das Simplex-Verfahren	340
<hr/>	
Teil VII Kombinatorik	
<hr/>	
25 Abzählende Kombinatorik	351
25.1 Gruppenoperationen	351
25.2 Das Lemma von Burnside	353
25.3 Färbungen	355
25.4 Zykelindikatorpolynome	356
25.5 Der Satz von Pólya	358
25.6 Anwendungen	360
26 Existenzielle Kombinatorik	367
26.1 Schubfachprinzip	367
26.2 Klassische Ramsey-Theorie	368
26.3 Untere Schranken	371
26.4 Verallgemeinerte Ramsey-Theorie	372
26.5 Graphische Ramsey-Theorie	374
26.6 Anwendung in der Kommunikationstechnik	375
Literaturverzeichnis	379
Sachverzeichnis	381