

Vorwort

Dieses Buch ist entstanden aus einer vom ersten Autor neu konzipierten Vorlesung für Erstsemester der Fächer Informatik und Wirtschaftsinformatik an der Universität Trier. Ziel dieser Vorlesung war es, die Hörer mit ihren recht unterschiedlichen mathematischen Vorkenntnissen und Fertigkeiten abzuholen und sie mit dem für ein erfolgreiches Studium der Informatik oder verwandter Studiengänge notwendigen mathematischen Rüstzeug auszustatten. Am Ende der Vorlesung sollten die Hörer dann in der Lage sein, in der exakten und streng formalisierten Denk- und Schreibweise der Mathematik zu argumentieren – eine Fähigkeit, ohne die eine erfolgreiche Arbeit in der Informatik unvorstellbar ist. Anders jedoch als in den üblichen Mathematikvorlesungen, bei denen die Hörer von vornherein mit dieser abstrakten mathematischen Denk- und Schreibweise konfrontiert werden, sollte diese hier behutsam eingeführt und eingeübt werden, um dem Schein, dass Mathematik schwer, manchmal zu schwer wäre, gleich von vornherein zu begegnen. Vorlesung und Buch beginnen deshalb im ersten Teil mit einer recht informellen, „erzählerischen“ Einführung in die Begriffswelt der Aussagenlogik und Mengenlehre und entwickeln dabei ein erstes belastbares Verständnis für den Sinn und Zweck exakter mathematischer Beschreibungen und Argumentationen. Die Bedeutung des mathematischen Beweisens wird erklärt und beim Sprechen über Relationen und Abbildungen systematisch eingeübt. Im zweiten Teil der Vorlesungen werden dann für die Informatik wichtige Beweistechniken, wie z.B. vollständige Induktion oder Abzähltechniken aus der Kombinatorik, mit einigen Anwendungen in der Stochastik vorgestellt. Der dritte Teil erörtert schließlich für die inzwischen mathematisch geschulten Leser einige grundlegende diskrete Strukturen, wie z.B. Graphen oder Boole'sche Algebren. Gleichsam spiralenförmig werden Begriffe, die in den ersten Kapiteln lediglich informell eingeführt wurden, in einem abschließenden Kapitel zur Aussagenlogik nun auf dem Niveau der exakten mathematischen Denk- und Schreibweise wieder aufgenommen und behandelt. Ausgestattet mit einer gesicherten Intuition haben Hörer und Leser nun auch in den höheren Gefilden mathematischer Betrachtungen eine gute Chance, sich zurechtzufinden und souverän zu bewegen.

Wir hoffen, mit einer solchen Aufbereitung des für einen Studenten oder anderen Interessierten der Informatik unerlässlichen mathematischen Stoffes eventuelle Defizite aus der mathematischen Vorbildung der Leser wettmachen und daraus resultierende Vorbehalte gegenüber einer weiterführenden Mathematikausbildung abbauen zu können.

Wir danken den Trierer Informatikstudenten für ihre zahlreichen Anregungen im Verlaufe der Vorlesungen, auch streckenweises Unverständnis hat uns geholfen, die Aufbereitung und Darstellung des Stoffes zu überdenken und am Stil der Darstellung zu feilen. Den Kollegen der Abteilung Informatik der Universität Trier sind wir sehr verbunden für gemeinsame Auffassungen zur Notwendigkeit einer soliden mathematischen Grundausbildung im Informatik- und Wirtschaftsinformatikstudium. Schließlich bedanken wir uns für die Unterstützung beim Zeichnen von Bildern und beim Korrekturlesen ganz herzlich bei Jochen Bern, Benjamin Boelter, Carsten Damm, Lilo Herbst, Lothar Jost und Harald Sack.

Trier, Februar 2000

Christoph Meinel
Martin Mundhenk

Vorwort zur dritten Auflage

In der dritten Auflage wurde ein Kapitel über Modulare Arithmetik mit den mathematischen Grundlagen der Kryptographie angefügt. Außerdem wurden Fehler und Unstimmigkeiten reduziert. Für die Hinweise dazu bedanken wir uns herzlich bei zahlreichen kritischen Lesern.

Potsdam/Jena, März 2006

Christoph Meinel
Martin Mundhenk

Inhaltsverzeichnis

Einleitung	11
I Grundlagen	17
1 Aussagen	19
1.1 Definition und Beispiele	19
1.2 Verknüpfungen von Aussagen	21
1.3 Tautologie und Kontradiktion	27
1.4 Aussageformen	31
1.5 Aussagen mit Quantoren	32
2 Mengen und Mengenoperationen	36
2.1 Mengen	36
2.2 Gleichheit von Mengen	39
2.3 Komplementäre Mengen	41
2.4 Die leere Menge	42
2.5 Teilmenge und Obermenge	43
2.6 Potenzmenge und Mengenfamilien	45
2.7 Vereinigung, Durchschnitt und Differenz von Mengen	47
2.8 Produkt von Mengen	52
2.9 Weitere Rechenregeln für Mengenoperationen	55
3 Mathematisches Beweisen	58
4 Relationen	63
4.1 Definition und erste Beispiele	63

4.2	Operationen auf Relationen	67
4.3	Wichtige Eigenschaften von Relationen	71
4.4	Äquivalenzrelationen und Klasseneinteilung	74
4.5	Rechnen mit Äquivalenzrelationen	80
4.6	Halbordnungsrelationen	83
5	Abbildungen und Funktionen	89
5.1	Definition und erste Beispiele	89
5.2	Surjektive, injektive und bijektive Abbildungen	94
5.3	Folgen und Mengenfamilien	100
5.4	Kardinalität von Mengen	103
	Quellen und weiterführende Literatur	108
II	Techniken	109
6	Grundlegende Beweisstrategien	111
6.1	Direkter Beweis	112
6.2	Beweis durch Kontraposition	114
6.3	Widerspruchs-Beweis	115
6.4	Äquivalenzbeweis	116
6.5	Beweis atomarer Aussagen	117
6.6	Beweis durch Fallunterscheidung	119
6.7	Beweis von Aussagen mit Quantoren	121
6.8	Kombinatorischer Beweis	124
7	Vollständige Induktion	128
7.1	Idee der vollständigen Induktion	129
7.2	Beispiele für Induktionsbeweise	130
7.3	Struktur von Induktionsbeweisen	133
7.4	Verallgemeinerte vollständige Induktion	135
7.5	Induktive Definitionen	136

8	Zählen	147
8.1	Grundlegende Zählprinzipien	147
8.2	Permutationen und Binomialkoeffizienten	152
8.3	Rechnen mit Binomialkoeffizienten	157
9	Diskrete Stochastik	166
9.1	Zufallsexperimente und Wahrscheinlichkeiten	166
9.2	Bedingte Wahrscheinlichkeit	174
9.3	Zufallsvariablen	176
9.4	Binomial-Verteilung und geometrische Verteilung	182
	Quellen und weiterführende Literatur	187
III	Strukturen	189
10	Boole'sche Algebra	191
10.1	Schaltfunktionen und Ausdrücke	191
10.2	Definition der Boole'schen Algebra	197
10.3	Beispiele Boole'scher Algebren	200
10.4	Eigenschaften Boole'scher Algebren	206
10.5	Halbordnungen in einer Boole'schen Algebra	210
10.6	Atome	213
10.7	Normalformen für Boole'sche Ausdrücke	216
10.8	Minimierung Boole'scher Ausdrücke	219
10.9	Der Isomorphie-Satz	221
10.10	Schaltkreis-Algebra	225
11	Graphen und Bäume	233
11.1	Grundbegriffe	234
11.2	Wege und Kreise in Graphen	241
11.3	Graphen und Matrizen	247
11.4	Isomorphismen auf Graphen	254
11.5	Bäume	258

12	Aussagenlogik	264
12.1	Boole'sche Algebra und Aussagenlogik	264
12.2	Normalformen	269
12.3	Erfüllbarkeitsäquivalente Formeln	271
12.4	Unerfüllbare Klauselmengen	276
12.5	Erfüllbarkeit von Hornklauseln	280
12.6	Resolution	283
12.7	Klauselmengen in 2KNF	291
13	Modulare Arithmetik	295
13.1	Die Teilbarkeitsrelation	296
13.2	Modulare Addition und Multiplikation	300
13.3	Modulares Rechnen	304
13.4	Der größte gemeinsame Teiler und der Algorithmus von Euklid	308
13.5	Der kleine Satz von Fermat	312
13.6	Verschlüsselung mit dem kleinen Satz von Fermat	316
13.7	Das RSA-Verfahren	322
	Quellen und weiterführende Literatur	324
	Index	327