de Gruyter Lehrbuch

Jacobs/Jungnickel · Einführung in die Kombinatorik

Konrad Jacobs
Dieter Jungnickel

# Einführung in die Kombinatorik

2., völlig neu bearbeitete und erweiterte Auflage

Walter de Gruyter
Berlin · New York 2004

Konrad Jacobs
Abtsberg 25
96049 Bamberg

Dieter Jungnickel
Institut für Mathematik
Universität Augsburg
Universitätsstraße 14
86135 Augsburg

*Mathematics Subject Classification 2000:* 05-01

♾ Gedruckt auf säurefreiem Papier, das die US-ANSI-Norm über Haltbarkeit erfüllt.

ISBN 3-11-016727-1

*Bibliografische Information Der Deutschen Bibliothek*

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



Printed in Germany.
Umschlaggestaltung: Hansbernd Lindemann, Berlin.
Texterfassung in LaTeX und Konvertierung der Dateien: I. Zimmermann, Freiburg.
Druck und Bindung: Hubert & Co. GmbH & Co. KG, Göttingen.

# Vorwort zur zweiten Auflage

Seit dem Erscheinen der ersten Auflage dieses Buches sind nunmehr zwanzig Jahre vergangen. Für die Neuauflage haben Herr Kollege Jacobs und der Verlag de Gruyter mich um eine gründliche Überarbeitung gebeten. Ich habe dabei die im Vorwort zur ersten Auflage von Herrn Jacobs genannte Zielsetzung und den prinzipiellen Aufbau seines Buches respektiert, mich aber trotzdem nicht nur auf die Beseitigung von Druckfehlern und kleineren Irrtümern beschränkt. Neben verhältnismäßig geringfügigen Änderungen in der Darstellung und einigen vereinfachten Beweisen sowie vielen neuen Literaturhinweisen stehen die gründliche Umarbeitung mehrerer Kapitel (insbesondere die über Lateinische Quadrate, Codes, projektive Ebenen und Blockpläne) im Lichte neuerer Entwicklungen, was auch zu einigen umfangreichen Ergänzungen geführt hat. Insgesamt werden diese Teile nun doch systematischer präsentiert, wenn es auch dabei bleibt, daß eine vollständige Theorie im hier gesetzten Rahmen nicht geboten werden kann. Es sind so – wie ich denke – etliche weitere Rosinen zu dem von Herrn Jacobs angesprochenen Kuchen hinzugekommen, wie beispielsweise

- mehr Anwendungen aus der Codierungstheorie (Prüfziffersysteme, CRC-Codes),
- Anwendungen von Codes und projektiven Ebenen in der Kryptographie (Authentikation von Nachrichten, Zugangskontrolle zu geheimen Informationen),
- mehr über Blockpläne, zum Beispiel der Zusammenhang zur bekannten Hadamardschen Ungleichung, für die wir einen besonders kurzen Beweis eingeschlossen haben, und Differenzmengen, inklusive eines eleganten Beweises für den berühmten Hallschen Multiplikatorsatz,
- mehr über projektive Ebenen und Räume, insbesondere über Kollineationen (Satz von Singer) und interessante Unterstrukturen wie Unterebenen, Blockademengen und Bögen, wobei die Bögen einen verblüffenden Zusammenhang zur Codierungstheorie liefern,
- ein besonders kurzer und eleganter Beweis des Fünffarbensatzes,

um nur einige besondere Highlights zu nennen. Dabei haben natürlich auch meine persönlichen Interessen eine gewisse Rolle gespielt. Insgesamt hoffe ich aber, dem Geist der ersten Auflage treu geblieben zu sein und das Buch noch reichhaltiger und damit vielleicht auch noch eine Spur reizvoller gemacht zu haben.

Trotzdem bleiben notgedrungen viele wichtige Aspekte der Kombinatorik gänzlich außen vor, wie etwa die eminent wichtige Matroid-Theorie, die Theorie der Assoziationsschemata, die probabilistische Methode oder die extremale Kombinatorik. Für die Matroidtheorie sei der Leser auf die Bücher von Tutte [1971], Welsh [1976], Oxley [1992], Recski [1989] und White [1986], [1987], [1992] verwiesen. Zum Thema Assoziationsschemata empfehlen wir Bannai und Ito [1984] sowie Zieschang [1995], und zur probabilistischen Methode sollte man Erdős und Spencer [1974], Alon und Spencer [1992] sowie – für algorithmische Aspekte – Habib et al. [1998] konsultieren. Zur extremalen Kombinatorik vergleiche man Baranov und Stechkin [1995] sowie Jukna [2001]; für die extremale Graphentheorie ist nach wie vor das Buch von Bollobás [1978] die Standardreferenz.

Andere wichtige Aspekte kommen sicherlich ebenfalls etwas zu kurz; so spielen bei uns weder Algorithmen noch Anwendungen eine große Rolle, wenn sie auch gelegentlich angesprochen werden. Es sind aber gerade diese beiden Themen, die die enorme außermathematische Nützlichkeit der Kombinatorik erklären. Stellvertretend für viele mögliche Referenzen sei der an realen Anwendungen – etwa im VLSI-Design oder beim Entwurf von Kommunikations- und Verkehrsnetzwerken – interessierte Leser auf die Bücher von Lengauer [1990], Korte et al. [1990] sowie Bermond [1992] verwiesen. Auf diese Themen können wir leider gar nicht eingehen; immerhin werden wir zu Anwendungen in der Kryptographie im Text einiges sagen. Dagegen bleibt leider auch das vielfältig anwendbare „Traveling Salesman Problem“ auf der Strecke, das bestens dazu geeignet wäre, nahezu alle relevanten Aspekte der modernen kombinatorischen Optimierung kennenzulernen; dafür müssen wir unsere Leser auf die beiden wunderbaren Sammelwerke von Lawler et al. [1985] sowie Gutin und Punnen [2002] verweisen.

Ich danke dem Verlag de Gruyter und insbesondere Herrn Manfred Karbe für die gute Betreuung dieses Buchprojektes und die stets angenehme Zusammenarbeit. Mein ganz besonderer Dank gilt meinem früheren Studenten, Herrn Dr. Andreas Enge, der das Manuskript mit großer Aufmerksamkeit gelesen und zahlreiche Verbesserungsvorschläge gemacht hat. Die noch verbleibenden Irrtümer gehen ganz und gar zu meinen Lasten.

Augsburg, Juli 2003 *Dieter Jungnickel*

# Vorwort zur ersten Auflage

Es gibt verschiedene Arten, Kombinatorik zu lernen. Will man Berufs-Kombinatoriker werden, so kann man z. B.

(a) dem in der Rota-Schule gepflegten Trend zur Systematisierung kombinatorischer Schlußweisen folgen, wie etwa Rota [1975], Aigner [1979], Graver und Watkins [1977] oder

(b) versuchen, Kombinatorik im indisch-israelisch-ungarischen Stil (liebevoll-dynamisches Stellen und Lösen von Einzelproblemen im Lichte großer Leitideen) zu treiben und zur Einübung etwa das Buch von Lovàzs [1979] durcharbeiten.

Das Literaturverzeichnis gibt einen Einblick in die Fülle der veröffentlichten Lehrbücher und Monographien.

Das vorliegende Buch schließt soweit wie möglich an das Bändchen von Ryser [1963] an. Es wendet sich nicht so sehr an zukünftige Berufskombinatoriker, sondern vor allem an Mathematiker jeder Arbeitsrichtung, die einen knappen, vielseitigen Einblick in die Kombinatorik gewinnen und mit bescheidenem technischen Aufwand schnell an eine Vielzahl berühmter Resultate herankommen wollen. Damit sind insbesondere Studenten und auch Gymnasiallehrer angesprochen (die Kombinatorik wird wegen ihres Reizes und ihrer Direktheit in Zukunft eine wachsende Bedeutung im Schulunterricht haben).

Ich habe deshalb, bildlich gesprochen, versucht, einen möglichst kleinen Kuchen mit möglichst vielen Rosinen zu backen. Die Themenauswahl ist aus dem Inhaltsverzeichnis ersichtlich. Kürzer behandelt sind einige Themen, die an sich nicht zum klassischen Themenkanon der Kombinatorik gehören, z. B. das Diktatorproblem und einige Symmetrie-Eigenschaften der Morse-Folge 01101001... Der Versuchung, immer das allgemeinste mögliche Resultat zu beweisen, habe ich zu widerstehen gesucht. Auch auf die Einführung vereinheitlichender Begriffe (z. B. Inzidenzstruktur) habe ich absichtlich verzichtet. Die Kombinatorik ist bunt und soll bunt bleiben. Ich habe vor allem nach dem Typischen getrachtet. So lernt man z. B. die typische Arbeitsweise der Ray-Chaudhuri-Schule hier zweimal, bei der vollständigen Widerlegung der Eulerschen Vermutung über orthogonale lateinische Quadrate und bei der vollständigen Behandlung des Kirkman'schen Schulmädchenproblems im Falle der Dreierreihen, gründlich kennen. Dagegen habe ich die umfassenderen Existenzsätze für Blockpläne und auflösbare Blockpläne nur zitiert und nicht bewiesen. Verschiedene Großgebiete der modernen Kombinatorik – Graphentheorie, endliche Geometrie, Code-Theorie, Blockplan-Theorie – werden nur in typischen, aber, wie ich hoffe, gründlichen Kostproben vorgeführt; jedes dieser Gebiete würde ein eigenes Studium erfordern. Eine Reihe kombinatorischer Themen mußte aus Platzgründen entfallen (z.B. Such-Theorie, Matroid-Theorie, Fluktuationstheorie, Gittergas-Kombinatorik, topologische und wahrscheinlichkeitstheoretische Methoden, Hadamard-Matrizen, und auch die Permanententheorie, die mit dem Beweis der van-der-Waerden-Vermutung durch Egorychev [1981] und Falikman [1981] soeben einen schönen Schritt vorwärts getan hat, konnte ich nur streifen).

An verschiedenen Stellen habe ich Resultate aus anderen mathematischen Theorien genutzt, aus der Gruppentheorie, aus der Theorie der endlichen Körper, aus der elementaren Zahlentheorie, aus der Funktionentheorie. Diese Resultate werden am betr. Ort durch hoffentlich ausreichende Erläuterungen herangeholt.

Zwecks Pflege des Familiensinns unter Mathematikern habe ich das Literaturverzeichnis, soweit möglich und tunlich, mit Vornamen und Lebensdaten ausgestattet. Ich hoffe, es sind mir keine Fehler unterlaufen.

*Zur Bezeichnung:* Satz III.5.1 bedeutet: Satz 5.1 aus Kap. III § 5. Das Symbol □ bezeichnet das Ende eines Beweises.

Zahlreichen Freunden und Kollegen bin ich zu Dank verpflichtet. Mein Doktorvater, Herr Wilhelm Maak, dem ich dies Buch widme, hat mir vor langen Jahren einen ersten Zugang zur Kombinatorik eröffnet. Fachkundigen Rat haben mir vor allem Thomas Beth, Hillel Furstenberg, Dietrich Kölzow, Klaus Leeb, Volker Strehl und Benji Weiss gegeben; Maria Reményi hat den Text kritisch gelesen und verbessert. Für die Herstellung der Reinschrift danke ich den Sekretärinnen des Erlanger Mathematischen Instituts, voran Frau Helga Zech, und dem Verlag de Gruyter für die sorgfältige publikatorische Betreuung und die gute Zusammenarbeit.

Erlangen, April 1983 *Konrad Jacobs*

# Inhaltsverzeichnis

# I Das kleine Einmaleins der Kombinatorik

In diesem einführenden Kapitel wollen wir einige elementare Aussagen und Prinzipien der klassischen Kombinatorik kennenlernen. Nach einem kurzen Rückblick auf die wichtigsten Begriffe der Mengenlehre (der auch dazu dient, die von uns verwendete Notation festzulegen) stellen wir drei grundlegende Abzählprinzipien vor und leiten dann die einfachsten Anzahlaussagen für endliche Mengen her; danach betrachten wir mit dem Inklusions-Exklusions-Prinzip ein etwas schwierigeres Abzählverfahren, das von fundamentaler Bedeutung ist. Hier können wir dann bereits etliche anspruchsvollere Anwendungen behandeln.

## 1 Mengen

Die Kombinatorik beschäftigt sich überwiegend mit endlichen Mengen. Das Unendliche kommt aber sogleich ebenfalls in die Kombinatorik hinein, weil sie Sätze zu beweisen sucht, die für Mengen ohne Beschränkung der Mächtigkeit (also der Anzahl ihrer Elemente) gelten. Ferner bedient sich die Kombinatorik manchmal analytischer, topologischer oder stochastischer Methoden, wodurch sie es mit den reellen und den komplexen Zahlen oder auch mit topologischen Räumen zu tun bekommt; dieser Fall tritt besonders dann ein, wenn man sogenannte asymptotische Aussagen beweisen will. Schließlich lassen sich manche Fragestellungen und Ergebnisse der Kombinatorik von endlichen auf unendliche Mengen übertragen. In diesem Buch steht die Kombinatorik der endlichen Mengen im Vordergrund. Wo dieser Rahmen überschritten wird, werden wir die benötigten Hilfsmittel per Zitat ausdrücklich, aber ohne Beweis bereitstellen. Aber auch beim Umgang mit endlichen Mengen werden wir uns Resultate aus anderen Gebieten der Mathematik, insbesondere aus der Linearen Algebra, der Algebra der endlichen Körper und der Theorie der endlichen Gruppen – wieder per Zitat ohne Beweis – zu Nutze machen.

Wir setzen voraus, daß der Leser über gewisse Grundkenntnisse aus der naiven Mengenlehre, d. h. über Mengen und Abbildungen, verfügt. Es geht also nur noch darum, an gewisse Begriffsbildungen aus dieser Theorie zu erinnern und Bezeichnungen festzulegen. Die gesamte Kombinatorik ist, wie praktisch jeder Zweig der Mathematik, mit Hilfe der Begriffe „Menge“ und „Abbildung“ formulierbar. Die weiteren Abschnitte dieses Kapitels haben auch den Zweck, dies an einfachen Beispielen zu demonstrieren; dadurch soll insbesondere klar werden, daß zum Verständnis der Kombinatorik kein kombinatorischer Sonderverstand erforderlich ist. Dennoch werden wir später die konsequente Formulierung kombinatorischer Aussagen rein mit Hilfe der Begriffe „Menge“ und „Abbildung“ oft nicht voll durchführen, nämlich dann, wenn eine andere – beispielsweise verbale – Ausdrucksweise nach unserer Meinung besser geeignet ist, das Gemeinte klarzumachen. Von einem gewissen Stadium der Beschäftigung mit der Kombinatorik an sollte der Leser im Stande sein, mengentheoretischen Klartext selbstständig herzustellen, falls er dies wünscht. Folgende Mengen werden uns besonders beschäftigen:

$$\begin{aligned}
\mathbb{N} &= \{1, 2, 3, \dots\} = \text{die Menge der natürlichen Zahlen;}\\
\mathbb{Z} &= \{0, 1, -1, 2, -2, \dots\} = \{\dots, -1, 0, 1, \dots\}\\
&= \text{die Menge der ganzen Zahlen;}\\
\mathbb{Z}_+ &= \{0, 1, 2, \dots\} = \{m \mid m \in \mathbb{Z},\ m \geq 0\}\\
&= \mathbb{N} \cup \{0\} = \text{die Menge der ganzen Zahlen ab 0.}
\end{aligned}$$

Das Rechnen mit Kongruenzen (mod $m$) in $\mathbb{N}$ und $\mathbb{Z}$ wird als bekannt vorausgesetzt. Ferner benötigen wir immer wieder:

$$\begin{aligned}
\mathbb{Q} &= \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z},\ b \neq 0 \right\}\\
&= \text{die Menge (auch: der Körper) der rationalen Zahlen}
\end{aligned}$$

(womit wir eigentlich Äquivalenzklassen von Brüchen meinen, die Klassenbildung aber meist nicht explizit benützen);

$$\begin{aligned}
\mathbb{R} &= \text{die Menge (auch: der Körper) der reellen Zahlen;}\\
\mathbb{C} &= \text{die Menge (auch: der Körper) der komplexen Zahlen;}\\
GF(q) &= \text{der endliche Körper mit } q \text{ Elementen (wobei } q \text{ eine Primzahl-}\\
&\quad \text{potenz ist, vgl. § III.3).}
\end{aligned}$$

Mengen mit genau $r$ $(\in \mathbb{Z}_+)$ Elementen heißen auch *r-elementige Mengen* oder *r-Mengen*. Die *leere Menge* $\emptyset$ ist die einzige 0-Menge. Ist $M$ eine Menge und $r \in \mathbb{Z}_+$, so bezeichnet

$2^M$ die Menge aller Teilmengen von $M$ einschließlich der leeren Menge $\emptyset$;

$\binom{M}{r}$ die Menge der $r$-elementigen Teilmengen von $M$.

Man nennt $2^M$ auch die *Potenzmenge* von $M$. In der älteren Literatur findet man statt der hier verwendeten Bezeichnungen meist die Symbole $\mathcal{P}(M)$ bzw. $\mathcal{P}_r(M)$. Aus dem Zusammenhang sollte stets klar sein, ob wir mit $2^M$ gerade die Potenzmenge einer Menge oder aber eine Zahl meinen.

Die Mengenverknüpfungen $\cup$, $\cap$ und Symbole wie $\bigcup_{j=1}^n M_j$, $\bigcap_{k=1}^\infty M_k$, $\bigcup_{s\in I} M_s$ werden als bekannt vorausgesetzt. Sind $N$ und $M$ Mengen, so nennt man

$$
\begin{aligned}
M \setminus N &= \{x \mid x \in M,\ x \notin N\} \text{ die \textit{Differenz} von } M \text{ und } N\\
&\qquad \text{(in dieser Reihenfolge);}\\
M \triangle N &= (M \setminus N) \cup (N \setminus M) = (M \cup N) \setminus (M \cap N)\\
&\qquad \text{die \textit{symmetrische Differenz} von } M \text{ und } N.
\end{aligned}
$$

Eine Menge von Mengen wird auch als ein *Mengensystem* bezeichnet. Eine Abbildung einer nichtleeren Menge $I$ in eine Menge wird auch eine *Familie* genannt. $I$ heißt dann die *Indexmenge* der Familie. Ist $x_i$ das Bild von $i \in I$ unter dieser Abbildung, so schreibt man die Familie als $(x_i)_{i\in I}$. Bei speziellen $I$ verwendet man auch andere Schreib- und Sprechweisen:

$$
\begin{aligned}
(x_j)_{j\in\{1,2\}} &= (x_1, x_2) && \text{(\textit{geordnetes}) \textit{Paar}}\\
(y_k)_{k\in\{1,\dots,n\}} &= (y_1, \dots, y_n) && \textit{n-Tupel, n-Vektor}\\
(z_l)_{l\in\mathbb{Z}_+} &= (z_0, z_1, \dots) = z_0z_1\dots && \textit{Folge}\\
(y_m)_{m\in\mathbb{Z}} &= (\dots, u_{-1}, u_0, u_1, \dots)\\
&= \dots u_{-1}u_0u_1\dots && \textit{Folge}
\end{aligned}
$$

und dergleichen mehr. Dies alles gilt insbesondere bei *Mengenfamilien*, d. h. Abbildungen einer Indexmenge in eine Menge von Mengen. Ist $\mathcal{M}$ eine nichtleere Menge von Mengen, so bezeichnet

$\bigcup\limits_{M\in\mathcal{M}} M$ die *Vereinigung* aller Mengen aus $\mathcal{M}$, d. h. die Menge aller Elemente, die in mindestens einer Menge $M \in \mathcal{M}$ vorkommen;

$\bigcup\limits_{M\in\mathcal{M}} M$ den *Durchschnitt* aller Mengen aus $\mathcal{M}$, d. h. die Menge aller Elemente, die in jeder Menge $M \in \mathcal{M}$ vorkommen.

Ist $\mathcal{M} = \emptyset$, so setzt man $\bigcup_{M\in\mathcal{M}} M = \emptyset$; hat man sich entschlossen, nur Teilmengen einer festen Menge $X$ zu betrachten, definiert man $\bigcap_{M\in\emptyset} M = X$. Analoge Bezeichnungen werden für Mengenfamilien verwendet.