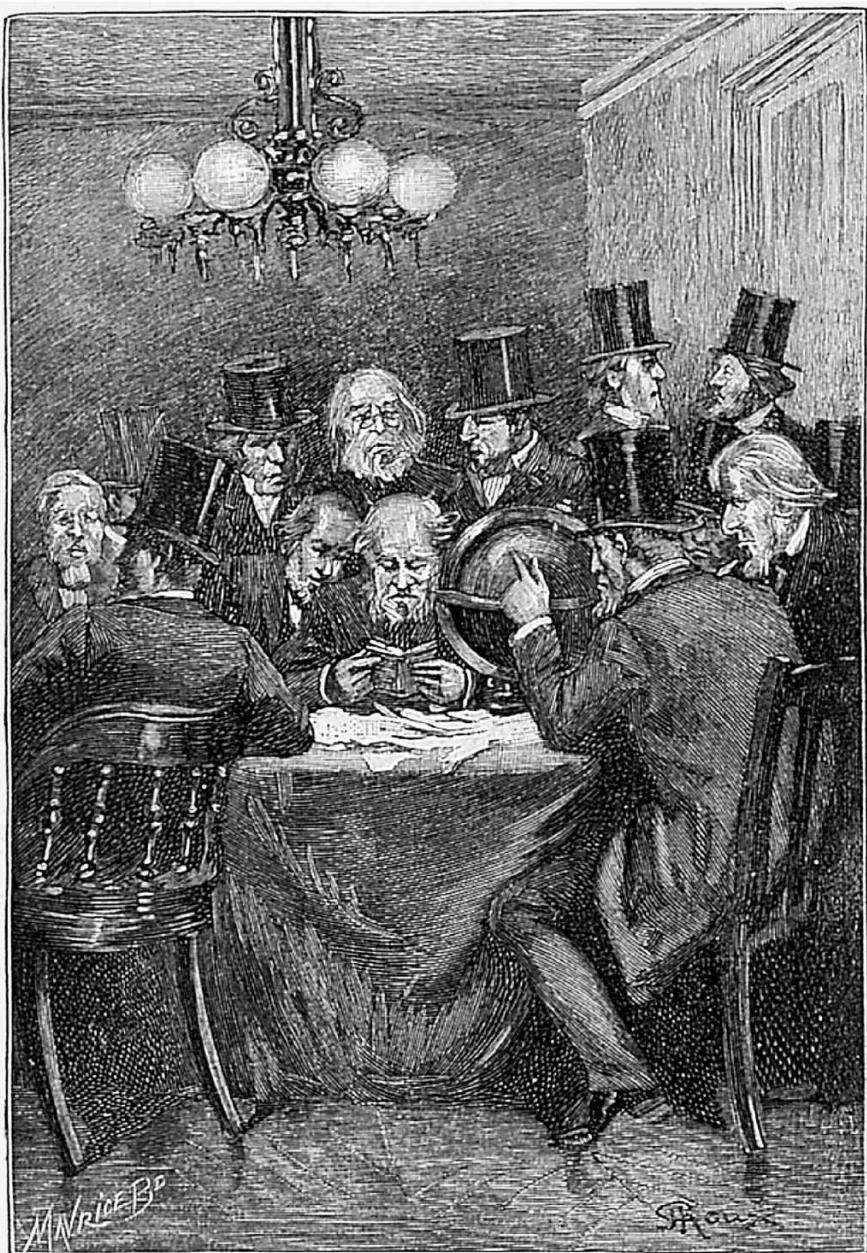


# Springer-Lehrbuch



„Nur Mathematiker wussten dieses Werk zu würdigen...“

Illustration von G. Roux aus der tschechischen Ausgabe von *Sans dessous* von Jules Verne, erschienen bei J. R. Vilimek, Prag, 1931 (Deutscher Titel: *Der Schuss am Kilimandscharo*).

Jiří Matoušek · Jaroslav Nešetřil

---

# Diskrete Mathematik

Eine Entdeckungsreise

Übersetzt von Hans Mielke



Springer

Professor Dr. Jiří Matoušek  
Professor Dr. Jaroslav Nešetřil  
Karls-Universität  
Institut für Angewandte Mathematik  
und  
Institut für Theoretische Informatik  
Malostranské nám. 25  
11800 Prag, Tschechien  
E-mail: matousek@kam.mff.cuni.cz  
E-mail: nesetril@kam.mff.cuni.cz

*Übersetzer*  
Dr. Hans Mielke  
Freie Universität Berlin  
E-mail: mielke@math.fu-berlin.de

---

© Jiří Matoušek and Jaroslav Nešetřil 1998, 2007  
This 2nd edition of the German translation of *Invitation to Discrete Mathematics* is published by arrangement with Oxford University Press.  
Diese 2. Auflage der deutschen Übersetzung von *Invitation to Discrete Mathematics* erscheint mit freundlicher Genehmigung von Oxford University Press.

---

#### Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

---

#### Mathematics Subject Classification (2000): 05-01, 68-01, 68Rxx

---

ISBN 978-3-540-30150-9 2. Aufl. Springer Berlin Heidelberg New York  
ISBN 978-3-540-42386-7 1. Aufl. Springer-Verlag Berlin Heidelberg New York

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland vom 9. September 1965 in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtsgesetzes.

Springer ist ein Unternehmen von Springer Science+Business Media

[springer.de](http://springer.de)

© Springer-Verlag Berlin Heidelberg 2002, 2007

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürfen. Text und Abbildungen wurden mit größter Sorgfalt erarbeitet. Verlag und Autor können jedoch für eventuell verbreitete fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Herstellung: LE-TeX Jelonek, Schmidt & Vöckler GbR, Leipzig  
Umschlaggestaltung: WMXDesign GmbH, Heidelberg

Gedruckt auf säurefreiem Papier 46/3180/YL - 5 4 3 2 1 0

# Vorwort zur zweiten Auflage in deutscher Sprache

---

Dies ist die zweite Auflage der „Entdeckungsreise“. Zum Stoff der ersten Auflage hinzugekommen sind Kapitel 2 über Halbordnungen, Abschnitt 4.7 über den Satz von Turán, zwei Beweise der Cauchy–Schwarzschen Ungleichung in Abschnitt 7.3, ein weiterer Beweis der Determinantenformel für die Anzahl der aufspannenden Bäume in Abschnitt 8.5, eine geometrische Interpretation der Konstruktion der reellen projektiven Ebene in Abschnitt 9.2 sowie das kurze Kapitel 11 über den Satz von Ramsey. Außerdem haben wir einige Kleinigkeiten geändert und natürlich eine Reihe von Fehlern korrigiert, auf die uns freundliche Leser aufmerksam gemacht haben (einige dieser Fehler sind bereits in den Nachdrucken der ersten Auflage behoben). Sie sehen, es lohnt sich die zweite Auflage zu erwerben anstatt verbilligten Restexemplaren der ersten Auflage nachzujagen... .

*Prag  
Juni 2007*

J. M.  
J. N.

# Ein Wort zur deutschen Übersetzung

---

Das Buch, das Sie in Händen halten, basiert auf der englischen Ausgabe, die bei Oxford University Press erschienen ist. Wir haben eine Reihe von (wie wir meinen) Verbesserungen vorgenommen: Einige Stellen sind geändert, verschiedene Fehler korrigiert, manche Lücke geschlossen. Das Kapitel über die Cayley–Formel für die Anzahl der aufspannenden Bäume ist um einen weiteren Beweis ergänzt (der ganz neu ist und vielleicht der einfachste überhaupt); der Anhang mit den algebraischen Grundbegriffen ist um geometrische Interpretationen einiger Begriffe der linearen Algebra bereichert. Unser Übersetzer Hans Mielke von der FU Berlin hat hervorragende Arbeit geleistet. Einige der Verbesserungsvorschläge stammen von ihm, und wir glauben, dass seine Übersetzung den Geist unseres Buches wiedergibt.

Ziel und Zweck dieses Buches sind im Vorwort ausführlich dargelegt; an dieser Stelle möchten wir noch hinzufügen, dass wir das Buch vor dem Hintergrund der Tradition der europäischen Universität konzipiert und geschrieben haben. Aus diesem Grunde finden wir eine Übersetzung ins Deutsche besonders passend.

*Prag  
Dezember 2001*

J. M.  
J. N.

# Vorwort

---

Wozu hat eine Einführung in die diskrete Mathematik ein so langes Vorwort? Was wollen wir überhaupt sagen? Es gibt viele Wege zur diskreten Mathematik. Zunächst wollen wir Wegweiser aufstellen, denen wir beim Schreiben zu folgen versucht haben; der Leser mag dann über unseren Erfolg entscheiden. Außerdem geben wir einige eher technische Hinweise, wie man nach diesem Buch eine Vorlesung halten kann, zu den Übungsaufgaben, zur Literatur usw.

Hier nun also einige Leitgedanken, die dieses Buch vielleicht von anderen mit ähnlichem Titel und Inhalt unterscheiden.

- *Mathematisches Denken entwickeln.* Unser Hauptziel, wichtiger als das Vermitteln mathematischer Fakten, ist beim Studienten Verständnis für mathematische Begriffe, Definitionen und Beweise zu wecken und ihn (oder sie!) zu befähigen, Probleme zu lösen, die mehr als nur Standardrezepte erfordern, sowie mathematische Gedanken präzise auszudrücken. Mathematische Denkgewohnheiten sind in vielen Lebensbereichen von Vorteil, z.B. beim Programmieren oder bei der Entwicklung komplexer Anlagen.<sup>1</sup> Viele private (gut zahlende) Firmen scheinen das zu wissen. Sie interessieren sich nicht wirklich dafür, ob der Bewerber vollständige Induktion im Schlaf kann, aber sie wünschen sich, dass er gewohnt ist, sich komplexe Konzepte in kurzer Zeit anzueignen — mathematische Sätze sind dafür offenbar ein hervorragendes Training. Die Wahl des speziellen Gebiets für dieses Training ist dabei nebensächlich — wenn Sie sich für Algebra begeistern, werden wir sicher nicht versuchen Sie für Kombinatorik abzuwerben! Aber wir glauben, dass diskrete Mathematik für eine erste Annäherung an die Mathematik besonders geeignet ist, denn die Probleme und Begriffe sind elementarer als zum Beispiel in der Analysis, die von Anfang an mit tiefliegenderen Ideen startet.

---

<sup>1</sup>Man sollte aber auch nicht vergessen, dass es in anderen Lebensbereichen besser ist, typische Verhaltensweisen eines Mathematikers abzulegen.

- *Methoden, Techniken, Prinzipien.* In modernen universitären Lehrplänen versteht man unter diskreter Mathematik gewöhnlich die Mathematik endlicher Mengen, oft einschließlich verschiedener Gebiete wie Logik, endliche Automaten, lineares Programmieren oder Rechnerarchitektur. Wir haben den Rahmen eher eng gesteckt; das Buch ist im Wesentlichen eine Einführung in die Kombinatorik und Graphentheorie. Wir konzentrieren uns auf relativ wenige grundlegende Methoden und Prinzipien, um den Reichtum mathematischer Techniken schon auf dieser elementaren Ebene vorzuführen; die Wahl der Themen ist dem untergeordnet.
- *Genuss.* Wir haben dieses Buch für Leser geschrieben, die Mathematik genießen können, doch unser kühnster Wunsch ist, dem einen oder anderen Leser, dem dieser Genuss bisher nicht zugänglich war, dabei zu helfen, gegenüber der Mathematik positive Gefühle zu entwickeln. Unserer Ansicht nach ist dies überhaupt der Schlüssel: Wohlgefallen an einer eleganten mathematischen Idee und manchmal das Gefühl des Triumphs, wenn diese Idee schwierig zu verstehen oder zu entdecken war. Nicht alle Menschen haben diese Gabe, so wie nicht jeder Musik genießen kann, aber ohne sie ist das Studium der Mathematik wohl eher langweilig.
- *Alle Karten auf den Tisch.* Wir versuchen kein Argument unter den Tisch fallen zu lassen und gegenüber dem Leser mathematisch ehrlich zu sein. Wenn wir schreiben etwas sei leicht zu sehen, meinen wir das auch, und wenn der Leser es nicht sehen kann, ist irgendetwas falsch — vielleicht haben wir die Schwierigkeit falsch eingeschätzt, aber das Problem könnte auch beim Leser liegen, der vielleicht den vorangegangenen Text noch nicht ganz verstanden hat. Wann immer möglich versuchen wir alles zu beweisen und nicht auf Ergebnisse anderer Gebiete zurückzugreifen (manchmal finden sich Beweise zu Hilfssätzen in den Übungsaufgaben, dann aber mit Lösungshinweisen), und wenn wir einen Beweis einmal nicht vollständig führen können (wie z.B. einige Ergebnisse über ebene Graphen), betonen wir dies und gestehen, welche Schritte wir nicht begründen.
- *Informatik.* Heutzutage spezialisieren sich viele Studenten der diskreten Mathematik zugleich in Informatik. Wir glauben dennoch, dass auch Menschen, die nichts über Computer wissen oder

gar Computerhasser sind, freien Zugang zur diskreten Mathematik haben sollten. Wir haben es deshalb vermieden, das Buch mit Begriffen und Beispielen aus der Informatik zu überfrachten. Wir haben aber auch die Informatiker nicht vergessen und deshalb Abschnitte über effiziente Algorithmen und ihre Laufzeitanalyse sowie einige Aufgaben (siehe unten) eingefügt.

- *Blick über den Tellerrand.* Der ausgewählte Stoff bietet an mehreren Stellen die Möglichkeit, Konzepte anderer Zweige der Mathematik an Beispielen vorzuführen. Indem wir einerseits darauf achten, nicht zu viel Stoff aufzunehmen, haben wir andererseits den Raum, auf solche Querverbindungen hinzuweisen. Unserer Erfahrung nach mögen Studenten solche Anwendungen, vorausgesetzt sie werden sorgfältig genug durchgeführt und nicht nur in einem Satz abgehandelt.

**Voraussetzungen und Zielgruppe.** In den meisten Teilen des Buches setzen wir nicht viel mehr als das gewöhnliche mathematische Schulwissen voraus. Einige etwas abstraktere Begriffe, die zwar in der gesamten Mathematik gebräuchlich sind, aber über das Schulwissen hinausgehen, erklären wir im ersten Kapitel. An einigen Stellen benötigen wir etwas Algebra, wie sie im Grundstudium vermittelt wird. Die für uns wichtigsten Ergebnisse aus der Algebra haben wir in einem Anhang zusammengetragen. Es gibt zwar auch einige wenige Ausflüge in die Analysis (wobei uns Begriffe wie Grenzwert, Ableitung, Stetigkeit usw. begegnen), aber wir denken, dass die meisten Studenten, die eine Vorlesung über diskrete Mathematik besuchen, über Grundkenntnisse in Analysis verfügen.

Der Leserkreis kann sowohl Studienanfänger der Mathematik oder Informatik mit dem üblichen Schulwissen umfassen als auch fortgeschrittenere Studenten bis zum Hauptstudium. Auch für gebildete Nichtmathematiker wie Biologen oder Chemiker kann dieses Buch eine nützliche Quelle sein. Dem mathematisch fortgeschrittenen Leser mag dieses Buch als schnelle Einführung in die Kombinatorik dienen.

**Lehre.** Dieses Buch basiert auf einer Vorlesung im Grundstudium Mathematik und Informatik, die wir seit vielen Semestern an der Karls–Universität in Prag halten. Der zweite Autor hat Teile der Vorlesung auch schon an der Universität Chicago, an der Universität Bonn und an der Simon–Fraser–Universität in Vancouver

gehalten. Bei der Vorlesung in Prag (13 Wochen mit je einer 90-minütigen Vorlesung und einem 90-minütigen Tutorium) behandeln wir gewöhnlich die Kapitel 1–9, wobei wir einige Abschnitte nur streifen und andere auslassen (zum Beispiel 3.6, 4.5 4.5, 5.5, 8.3–8.5, 9.2). Während wir im Buch manchmal mehrere Beweise zu einem Satz angeben, haben wir in der Vorlesung immer nur einen Beweis präsentiert und gelegentlich andere Beweise in den Tutorien besprochen. Manchmal haben wir auch zwei Sitzungen zu erzeugenden Funktionen (Abschnitte 12.1–12.3) oder eine Sitzung zum Zyklenraum eines Graphen (13.4) eingeschoben.

Für das Buch haben wir den Stoff unserer Vorlesung mit viel zusätzlichem, auch weiter führenden Material ergänzt, und wir hoffen, dass der Leser auch solche Teile beachtet, die für die Klausurvorbereitung nicht unbedingt nötig sind. Einige Kapitel können auch als Einführung in weiterführende Vorlesungen dienen (über die probabilistische Methode oder Anwendungen der linearen Algebra).

Das Kleingedruckte signalisiert in diesem Buch Abschnitte, die wir unbedingt in das Buch aufnehmen wollten, die wir aber nicht ganz so wichtig finden. Dabei handelt es sich um zusätzliche Erklärungen sowie um Bemerkungen oder Beispiele, die sich zum Teil auf einem höheren Niveau als der Haupttext bewegen. In jedem Fall sollte der Haupttext auch ohne das Kleingedruckte verständlich sein.

Wir haben in die Übungsaufgaben viele zusätzliche Information eingeschmuggelt, so dass sich ein Blick in die Aufgaben auch dann lohnt, wenn man sie nicht zu lösen beabsichtigt.

**Zu den Aufgaben.** Die meisten Abschnitte schließen mit einer kleineren oder größeren Sammlung von Übungsaufgaben. Einige von ihnen knüpfen nur lose an das Thema des Abschnitts an und dienen eher dem Spaß und der mathematischen Allgemeinbildung. Zur Lektüre des Buches gehört es aber in jedem Fall, wenigstens einige der Aufgaben zu lösen, auch wenn uns klar ist, dass das Tempo des modernen Lebens und die menschliche Natur es dem Leser kaum erlauben werden, alle (oder fast alle) der 477 Aufgaben zu lösen (obwohl das wahrscheinlich der schnellste Weg wäre, sich den Stoff anzueignen).

Reine Routine-Aufgaben, bei denen nur irgendein „Rezept“ anzuwenden ist, wie zum Beispiel „Wenden Sie den soeben besprochenen Algorithmus auf den folgenden Graphen an“, stellen wir kaum. Wir gehen davon aus, dass der Leser sein Verständnis selbst überprüft.

Wir haben die Aufgaben nach Schwierigkeitsgrad in drei Klassen

eingeteilt (kein, ein oder zwei Sterne). Wir stellen uns vor, dass ein guter Student, der den Stoff eines bestimmten Abschnitts verstanden hat, in der Lage sein sollte die Mehrzahl der „sternlosen“ Aufgaben zu lösen, wenn auch nicht unbedingt mühelos. Für die Aufgaben mit einem Stern braucht man meistens eine pfiffige Idee oder ein wenig mathematisches Wissen (aus der Analysis zum Beispiel). Für die Aufgaben mit zwei Sternen schließlich braucht man schon einen ziemlich schlauen Einfall. Die meisten Aufgaben haben kurze Lösungen; unseres Wissens nach sind lange, mühselige Rechnungen stets vermeidbar. Die Klassifikation nach dem Schwierigkeitsgrad beruht natürlich auf unserer subjektiven Einschätzung, und eine Aufgabe, die für den einen leicht ist, kann für einen anderen unüberwindliche Schwierigkeiten aufweisen. Also verzweifeln Sie nicht, wenn Sie eine Aufgabe ohne Stern mal nicht lösen können!

Einige Aufgaben sind mit *Inf* als Aufgaben aus der Informatik gekennzeichnet. Meistens handelt es sich um Probleme beim Entwurf effizienter Algorithmen, für die manchmal elementare Kenntnisse über Datenstrukturen notwendig sind. Die vorgestellten Algorithmen können auch programmiert und getestet werden, etwa in einem weiter führenden Programmierkurs. Einige der Informatikaufgaben mit einem Stern sind (zum Teil erprobte) Vorschläge für Projekte, für die man sowohl ein Gefühl für Mathematik braucht als auch algorithmische Kniffe und Programmierkenntnisse.

Hinweise zu vielen der Aufgaben geben wir in einem eigenen Kapitel am Ende des Buches. Es sind wirklich nur Hinweise und keine vollständigen Lösungen, und obwohl das Nachlesen der Hinweise die Freude an der (selbstständigen) Lösung des Problems trübt, mag es für viele Studenten schon eine Herausforderung sein, eine Lösung vollständig und ordentlich aufzuschreiben.

**Zur Literatur.** Im Literaturverzeichnis sind nicht alle Quellen der Ideen und Ergebnisse aufgeführt, die in diesem Buch zusammengetragen sind. An dieser Stelle möchten wir aber als besonders wichtige Quelle die große Sammlung gelöster kombinatorischer Probleme von Lovász [9] nennen und empfehlen. Sie ist ein hervorragendes Buch für das tiefere Studium der Kombinatorik und zugleich eine Enzyklopädie vieler Ergebnisse und Methoden. Wenn man ein neues Kombinatorikbuch schreibt, kommt man um diese Problemsammlung nicht herum, zum Beispiel ist eine nicht unbedeutende Anzahl unserer schwierigeren Aufgaben (den weniger schwierigen Teilen) die-

ser Sammlung entnommen oder zumindest von ihr inspiriert. Das Buch von Biggs [3] ist eine hübsche Einführung in die Kombinatorik mit einer etwas anderen Schwerpunktsetzung als unser Buch. Die Bücher von Van Lint und Wilson [8] und Cameron [5] sind etwas fortgeschritten, vielleicht wie eine Fortsetzung zu unserem Buch. Die wunderbare Einführung in die Graphentheorie von Bollobás [4] wurde wahrscheinlich mit ähnlichen Zielen geschrieben wie unser Buch, aber das Tempo ist nicht ganz so gemütlich und es deckt viel mehr Stoff über Graphen ab. Brandneu und auf Hauptstudiumsniveau<sup>2</sup> ist das Buch von Diestel [2]. Die Kunst des kombinatorischen Zählens und der asymptotischen Analyse ist hervorragend in dem beliebten Buch von Graham, Knuth und Patashnik [7] dargestellt (auch in Knuths Monographie [44]). Von Flajolet und Sedgewick [6] wird wohl bald ein weiteres umfassendes und modernes Buch zu diesem Thema in Druck gehen. Haben Sie eine spezielle Frage zur Kombinatorik, dann ist das *Handbook of Combinatorics* [41] ein guter erster Griff. Weitere Literaturhinweise finden sich hier und dort in unserem Text. Es gibt eine sehr große Zahl Kombinatorikbücher, wir nennen nur einige unserer Lieblingswerke.

**Zum Stichwortverzeichnis.** Bei den meisten mathematischen Begriffen, besonders bei grundlegenden (wie Relation oder Graph), verweist das Stichwortverzeichnis nur auf die Definition. Mathematische Symbole aus lateinischen Buchstaben (wie  $C_n$ ) befinden sich am Anfang der Einträge mit dem entsprechenden Buchstaben. Spezielle Symbole (wie  $X \setminus Y$ ,  $G \cong H$ ) oder Symbole, die griechische Buchstaben enthalten, sind am Anfang des Stichwortverzeichnisses aufgeführt.

**Danksagungen.** Dieses Buch ist aus einem Manuskript in tschechischer Sprache entstanden, das wir im Laufe unserer Vorlesungstätigkeit in Prag entwickelt haben. Wir danken unseren Kollegen vom Institut für angewandte Mathematik der Karls-Universität, unseren Assistenten und unseren Studenten für ihre Anregungen und hilfreichen Kommentare zum Text und zu den Aufgaben. Insbesondere danken wir Pavel Socha, Eva Matoušková, Tomáš Holan und Robert Babilon, die eine Reihe von Fehlern in der tschechischen Version gefunden haben. Martin Klazar und Jiří Otta haben einige dutzend Probleme und Aufgaben zusammengetragen; diese Liste

---

<sup>2</sup>Und auf Deutsch erhältlich!

war der Keim unserer Aufgabensammlung. Unserem Kollegen Jan Kratochvíl verdanken wir wertvolle Anregungen, die er uns aufgrund seiner Erfahrungen mit eben dieser Vorlesung geben konnte. Tomáš Kaiser hat uns bei der Übersetzung eines Kapitels ins Englische tatkräftig unterstützt. Adam Dingle und Tim Childers waren uns in einem frühen Stadium der englischen Übersetzung behilflich. Jan Nekovář ist von den Gipfeln der Zahlentheorie herabgestiegen um uns bei der Suche nach einem passenden Beweis für Tatsache 12.7.1 auf die Sprünge zu helfen.

Mehrere Menschen haben die englische Version in verschiedenen Entwicklungsstadien gelesen und uns wertvolle Hinweise gegeben. Unser besonderer Dank gilt Jeff Stopple, der uns in Prag besucht hat, das gesamte Manuskript sorgfältig gelesen hat und mit uns seine Lehrerfahrung geteilt hat. Viel verdanken wir Mari Inaba und Helena Nešetřilová, deren sehr nützliche und spezielle Bemerkungen anders waren als die meisten anderen. Uns unbekannte Referenten von Oxford University Press haben uns mit ihren Kommentaren ebenfalls sehr geholfen. Den letzten Schliff hat das Buch während eines Aufenthalts des ersten Autors an der ETH Zürich bekommen. Die Atmosphäre bei Emo Welzl und den Mitgliedern seiner Arbeitsgruppe war sehr angenehm und freundlich, auch noch nachdem jeder von ihnen gebeten wurde ein Kapitel zu lesen. Für ihre Hilfe danken wir Hans-Martin Will, Beat Trachsler, Bernhard von Stengel, Lutz Kettner, Joachim Giesen, Bernd Gärtner, Johannes Blömer und Arthur Andrzejak sehr herzlich. Wir danken auch Hee-Kap Ahn, der ebenfalls ein Kapitel gelesen hat.

Viele Leser haben in der ersten Auflage Fehler gefunden (und gemeldet!) Die vollständige Liste finden Sie auf der weiter unten erwähnten Internet–Seite mit den Errata, hier nennen wir die besonders fleißigen Helfer Mel Hausner, Emo Welzl, Hans Mielke und Bernd Bischl.

Wir bedanken uns bei Karel Horák, der dem ersten Autor beim Kampf mit dem Layout des Buches mit professionellem Rat beigestanden hat (leider scheinen die Zeiten vorbei zu sein, wo Bücher von Schriftsetzern gesetzt wurden) und bei Jana Chlebíková für ihre lange Liste von Tippfehlern.

Fast alle Abbildungen hat der erste Autor mit dem Grafik–Editor Ipe 5.0 gezeichnet. Im Namen der Menschheit danken wir Otfried Cheong (geb. Schwarzkopf) für sein Programm.

Schließlich möchten wir noch die überaus freundliche und kompetente Hilfe von Sönke Adlung bei der Herausgabe des Buches erwähnen. Im letzten Stadium der Bearbeitung des Buches war es ein Vergnügen, mit Julia Tompson zusammen zu arbeiten.

**Eine abschließende Bitte.** Ein längerer mathematischer Text enthält in aller Regel eine nicht unerhebliche Anzahl von Fehlern. Viele von ihnen haben wir bereits korrigiert, aber unweigerlich immer noch etliche übersehen. Wir bitten daher alle Leser, die auf Fehler, unklare Formulierungen, falsche Hinweise zu den Übungsaufgaben und ähnliches stoßen, uns diese mitzuteilen.<sup>3</sup>

---

<sup>3</sup>Wir bitten, dieses Buch betreffende Post an `matousek@kam.mff.cuni.cz` zu senden. Eine Internetseite zu diesem Buch mit Errata–Liste ist über die Adresse <http://www.ms.mff.cuni.cz/acad/kam/idm> erreichbar.

# Inhaltsverzeichnis

---

<b>1</b>	<b>Grundlagen</b>	<b>1</b>
1.1	Eine kleine Problemsammlung	2
1.2	Notation	8
1.3	Vollständige Induktion	18
1.4	Funktionen	28
1.5	Relationen	35
1.6	Äquivalenz und andere spezielle Relationen	40
<b>2</b>	<b>Ordnungen</b>	<b>47</b>
2.1	Ordnungen und wie man sie zeichnen kann	47
2.2	Ordnungen und lineare Ordnungen	53
2.3	Die Teilmengenrelation	57
2.4	Groß heißt lang oder dick	59
<b>3</b>	<b>Zahltheorie</b>	<b>64</b>
3.1	Funktionen und Teilmengen	64
3.2	Permutationen	70
3.3	Binomialkoeffizienten	73
3.4	Näherungen: Eine Einführung	85
3.5	Näherungen: Fakultät	93
3.6	Näherungen: Binomialkoeffizienten	101
3.7	Inklusion–Exklusion	106
3.8	Vertauschte Hüte	112
<b>4</b>	<b>Graphen</b>	<b>119</b>
4.1	Definition eines Graphen; Isomorphismus	119
4.2	Teilgraphen, Komponenten, Adjazenzmatrix	129
4.3	Gradfolgen	136
4.4	Eulersche Graphen	142
4.5	Gerichtete Eulersche Graphen	151
4.6	2-Zusammenhang	156
4.7	Dreiecksfreie Graphen: ein Extremalproblem	163

<b>5 Bäume</b>	168
5.1 Definition und Charakterisierungen	168
5.2 Isomorphismen von Bäumen	175
5.3 Aufspannende Bäume eines Graphen	182
5.4 Minimal aufspannende Bäume	188
5.5 Die Algorithmen von Jarník und Borůvka	195
<b>6 Graphen in der Ebene</b>	201
6.1 Zeichnungen in die Ebene und andere Flächen	201
6.2 Kreise in ebenen Graphen	209
6.3 Die Euler–Formel	217
6.4 Das Vier–Farben–Problem	227
<b>7 Die Methode des Doppelten Abzählens</b>	240
7.1 Paritätsargumente	240
7.2 Der Satz von Sperner	250
7.3 Ein Problem der extremalen Graphentheorie	258
<b>8 Die Anzahl aufspannender Bäume</b>	264
8.1 Die Cayley–Formel	264
8.2 Ein Beweis mit Gradfolgen	266
8.3 Ein Beweis mit Wirbeltieren	268
8.4 Ein Beweis mit dem Prüfer-Code	270
8.5 Beweise mit Determinanten	274
8.6 Der zurzeit wohl einfachste Beweis	285
<b>9 Endliche projektive Ebenen</b>	289
9.1 Definition und grundlegende Eigenschaften	289
9.2 Existenz endlicher projektiver Ebenen	300
9.3 Orthogonale lateinische Quadrate	306
9.4 Kombinatorische Anwendungen	310
<b>10 Wahrscheinlichkeit und probabilistische Beweise</b>	314
10.1 Beweis durch Zählen	314
10.2 Endliche Wahrscheinlichkeitsräume	321
10.3 Zufallsvariable und Erwartungswert	333
10.4 Einige Anwendungen	339
<b>11 Ramsey–Theorie</b>	350
11.1 Eine Party zu sechst	351
11.2 Der Satz von Ramsey für Graphen	352
11.3 Eine untere Schranke für die Ramsey–Zahlen	355

<b>12 Erzeugende Funktionen</b>	358
12.1 Polynome	358
12.2 Potenzreihen	362
12.3 Fibonacci-Zahlen und der goldene Schnitt	375
12.4 Binäre Bäume	383
12.5 Würfeln	388
12.6 Zufallswege	389
12.7 Zahlpartitionen	393
<b>13 Anwendungen der Linearen Algebra</b>	401
13.1 Designs	401
13.2 Die Fisher–Ungleichung	407
13.3 Überdeckungen mit bipartiten Graphen	411
13.4 Der Zyklenraum eines Graphen	414
13.5 Ströme und Schnitte	418
13.6 Probabilistisches Testen	423
<b>Anhang: Grundlagen aus der Algebra</b>	435
<b>Literatur</b>	445
<b>Hinweise zu ausgewählten Übungen</b>	451
<b>Stichwortverzeichnis</b>	475



# 1

## Grundlagen

---

In diesem ersten Kapitel wollen wir anhand einiger ausgewählter Probleme die Natur der Fragestellungen kennen lernen, die in diesem Buch behandelt werden. Wir führen wichtige Begriffe, Schreibweisen und Techniken ein, die meisten davon sind sehr einfach und spielen in vielen mathematischen Disziplinen eine Rolle. Wir gehen davon aus, dass der Leser einige davon schon kennt (oder zumindest von ihnen gehört hat) und werden daher hauptsächlich exakte Definitionen für die Begriffe angeben und versuchen, sie mit Hilfe diverser Diagramme und Bilder lebendig werden zu lassen.

In Abschnitt 1.1 stellen wir verschiedene Probleme vor, die wir später genauer studieren werden, und machen uns ein paar Gedanken zum Stellenwert mathematischer Probleme u.ä.

In Abschnitt 1.2 tragen wir Schreibweisen zusammen. Wir führen die üblichen Symbole für Operationen mit Mengen oder Zahlen ein, etwa  $\cup$  für die Vereinigung von Mengen oder  $\sum$  für die Summe einer Folge von Zahlen. Die meisten dieser Symbole sind Standard und der Leser sollte in der Lage sein diesen Abschnitt zu überfliegen und später bei Bedarf nachzuschlagen.

In Abschnitt 1.3 diskutieren wir die vollständige Induktion, ein wichtiges Werkzeug um Aussagen zu beweisen, besonders in der diskreten Mathematik. An dieser Stelle geht es hauptsächlich um das Grundverständnis des Prinzips — Gelegenheit, das Prinzip (auch in Variationen) zu sehen und zu üben werden wir in den folgenden Kapiteln noch häufig haben. Wir machen uns auch ein paar Gedanken über mathematische Beweise im Allgemeinen.

In Abschnitt 1.4 erklären wir den Begriff der Funktion und definieren spezielle Typen von Funktionen, nämlich die injektiven, die surjektiven und die bijektiven Funktionen, die uns immer wieder begegnen werden.

## 2 Grundlagen

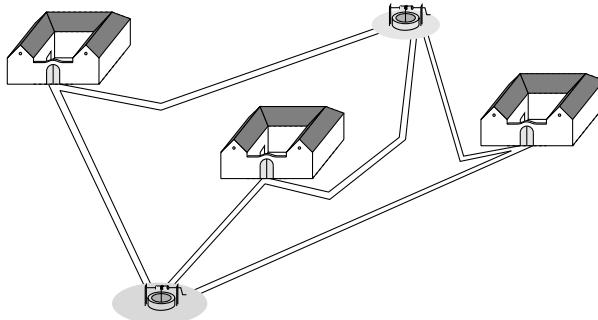
Die Abschnitte 1.5 und 1.6 behandeln Relationen und spezielle Typen von Relationen, nämlich Äquivalenz- und Ordnungsrelationen. Auch sie gehören zu den wirklich wichtigen „Vokabeln“ der Mathematik. Weil dies aber so einfache und allgemeine Konzepte sind, die erst durch die Fülle interessanter konkreter Beispiele mit Leben erfüllt werden, könnte ein Leser sie zunächst für „zu abstrakt“ halten — eine höfliche Umschreibung für „zu langweilig“. In diesem Fall sollten Sie diese Abschnitte nur überfliegen und bei Bedarf später noch einmal zurückblättern. (Das ist ungefähr so, wie wenn man eine Sprache lernt: Die Konjugation der Verben „sein“ und „haben“ zu lernen ist nicht besonders aufregend; wenn man über die ersten Schritte hinausgekommen ist, ist es aber undenkbar, nur mit den Formen „ich bin“ und „er ist“ auszukommen. Das ist also der Zweck dieses Kapitels: Wir eignen uns die *Sprache* der Mathematik an.)

### 1.1 Eine kleine Problemsammlung

Werfen wir also einen Blick auf einige der Probleme, mit denen wir uns in diesem Buch beschäftigen werden. Wir formulieren sie hier in populärer Form, vielleicht kennen Sie das eine oder andere als Knobelaufgabe.

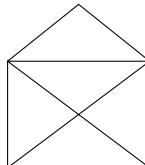
Recht bekannt ist das Problem von den drei Häusern und den drei Brunnen: Vor langer Zeit in einem fernen Königreich standen drei Häuser in einem Tal, und es waren drei Brunnen ganz in der Nähe, und ihr Wasser war rein und klar. Es war ein friedliches Tal, so lange bis die Zwietracht dort einkehrte. Die drei Höfe fielen in Feindschaft, und der Streit wollte kein Ende nehmen, und an Versöhnung war nicht zu denken. Die Menschen auf jedem der Höfe bestanden darauf, drei direkte Pfade zu den drei Brunnen zu haben, Pfade, welche die der Nachbarn nicht kreuzen sollten. Wenn es von jedem Hof aus diese Wege gäbe, dann wären alle zufrieden und in dem Tal könnte wieder Frieden einkehren. Doch bis zum heutigen Tage herrscht dort die Zwietracht. Kann es jemals wieder Frieden geben?

Mit nur zwei Brunnen ist das Problem einfach:

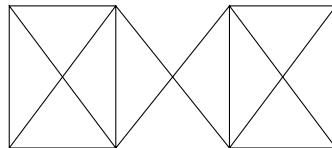


Aber mit drei Brunnen ist es hoffnungslos (es sei denn, diese stolzen Männer und Frauen wären bereit Tunnel oder Brücken zu benutzen, was eher unwahrscheinlich ist). Können Sie das als ein mathematisches Problem formulieren und beweisen, dass es keine Lösung hat?

Im Kern handelt dieses Problem vom Zeichnen in der Ebene. Auch viele andere Probleme, die wir in diesem Buch studieren werden, können als Zeichenprobleme formuliert werden. Ist es möglich, das folgende Bild zu zeichnen ohne den Stift abzusetzen und dabei jede Linie nur einmal zu ziehen?



Und wie ist es bei diesem Bild?

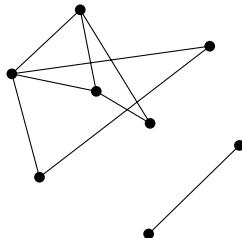


Warum nicht? Ein Beweis, dass etwas nicht geht, ist im Allgemeinen schwieriger zu erbringen als zu zeigen, dass es geht. Denn ist die Antwort ja, dann genügt es zu zeigen, wie es geht. Ist die Antwort aber nein, dann muss man sich etwas überlegen. Gibt es eine einfache Methode, Bilder, die man ohne Absetzen zeichnen kann, von solchen zu unterscheiden, bei denen es nicht geht? (Und gibt es hübsche Geschichten, die dieses und die folgenden Probleme illustrieren?)

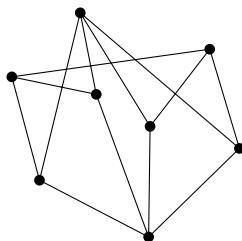
Für die folgenden Probleme zeichnen wir acht Punkte in die Ebene, sodass keine drei von ihnen auf einer Geraden liegen. (Die Zahl acht ist hier beliebig; im Allgemeinen würden wir  $n$  solche Punkte

## 4 Grundlagen

betrachten.) Verbinden Sie einige dieser Punkte durch gerade Linien, dann könnten sie das folgende Bild erhalten:

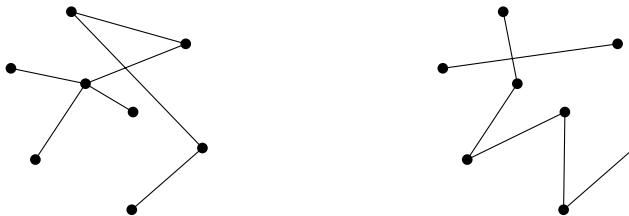


Wie viele Linien können Sie höchstens ziehen, wenn Sie kein Dreieck erzeugen wollen? (Dabei sollen nur solche Dreiecke zählen, deren drei Ecken auf Punkten liegen.) Das folgende Bild hat 13 Linien:



Können Sie bei acht Punkten mehr als dreizehn Linien ziehen, sodass kein Dreieck entsteht? Wahrscheinlich schon. Aber können Sie auch beweisen, dass ihr Resultat das Bestmögliche ist?

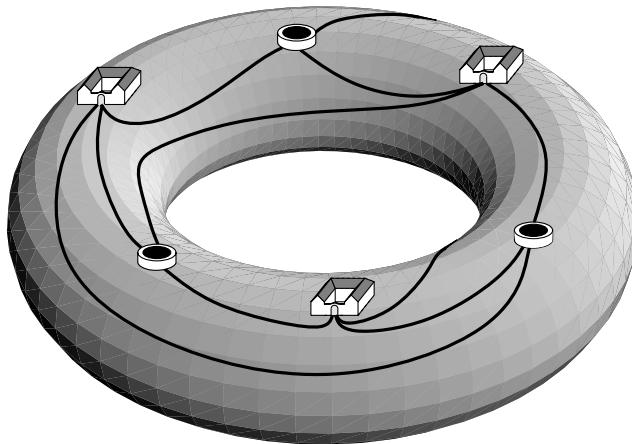
Als Nächstes wollen wir einige Linien so zwischen den Punkten ziehen, dass man von jedem Punkt aus jeden anderen erreichen kann, wobei man nur entlang der Linien gehen darf und nur an den Punkten die Richtung wechseln kann. Das Bild unten links ist also eine zulässige Lösung, das rechte Bild nicht:



Wie viele Linien müssen wir mindestens zeichnen? Wie viele verschiedene Lösungen mit dieser minimalen Linienanzahl gibt es? Und wie finden wir eine Lösung, bei der die Gesamtlänge der eingezeichneten Linien möglichst klein ist?

Alle diese Aufgaben sind eingekleidete Versionen einfacher elementarer Fragen der *Graphentheorie*, die ein Viertel dieses Buches

ausmacht (Kapitel 4, 5 und 6). Bei den obigen Problemen mit acht Punkten in der Ebene sieht man schnell ein, dass es überhaupt keine Rolle spielt, wo man die einzelnen Punkte zeichnet; es kommt lediglich darauf an, welche Paare von Punkten wir durch Linien verbinden und welche nicht. Die meisten Gebiete der Graphentheorie behandeln Probleme, die man zwar geometrisch veranschaulichen kann, in denen die Geometrie aber nicht wirklich eine Rolle spielt. Das Problem mit den Brunnen und Häusern aber gehört zu dem im Kern geometrischen Teil der Graphentheorie. Für dieses Problem ist wesentlich, dass die Wege in der Ebene gebaut werden sollen. Lägen die Häuser und die Brunnen nicht in einem Tal, sondern auf einem winzigen Planeten von der Form eines Spritzkuchen, dann könnte man die Wege anlegen:



Ein weiteres wichtiges Thema in diesem Buch ist das *kombinatorische Zählen*, behandelt in den Kapiteln 3 und 12. Dort beginnen Probleme für gewöhnlich: „Auf wie viele Arten kann man...?“ Eine Frage dieser Art haben wir in der Serie von Problemen mit den acht Punkten erwähnt (eine interessante Frage — das ganze Kapitel 8 ist ihr gewidmet). Vermutlich haben Sie schon eine Menge solcher Probleme gesehen; fügen wir noch eines hinzu: Auf wie viele Arten kann man  $n$  identische Münzen in Gruppen aufteilen? Vier Münzen kann man zum Beispiel auf fünf Arten aufteilen:  $1 + 1 + 1 + 1$  (vier Gruppen mit je einer Münze),  $1 + 1 + 2$ ,  $1 + 3$ ,  $2 + 2$  und  $4$  (alle vier Münzen bilden eine Gruppe, ein Grenzfall, den die meisten Menschen vielleicht nicht als „Aufteilung“ bezeichnen würden). Für dieses Problem werden wir keine exakte Formel angeben können;

## 6 Grundlagen

zwar gibt es so eine Formel, aber ihre Herleitung würde weit über den Rahmen dieses Buches hinausgehen. Immerhin werden wir wenigstens Schranken für die gesuchte Anzahl berechnen. Diese Anzahl ist eine Funktion von  $n$ , und wir können durch Abschätzungen ein Verständnis dafür entwickeln, wie stark diese Funktion verglichen mit einfachen und gut bekannten Funktionen wie  $n^2$  oder  $2^n$  wächst. Der Vergleich komplizierter Funktionen mit einfachen ist Thema der *asymptotischen Analyse*, die wir auch streifen werden und die in vielen Gebieten wichtig ist, z.B. wenn man verschiedene Algorithmen, die das gleiche Problem lösen, miteinander vergleichen will.

Auch wenn die vorgestellten Probleme wie Knobelaufgaben aussehen, so kann man doch jedes von ihnen als Startpunkt einer Theorie mit zahlreichen inner- und außermathematischen Anwendungen ansehen.

Es ist tatsächlich verdammt schwierig, ein gutes mathematisches Problem von einem schlechten zu unterscheiden, und oft kann man die Qualität eines Problems erst im Nachhinein beurteilen, wenn das Problem gelöst und die Konsequenzen verstanden sind. Zunächst müssen wir natürlich klären, was wir unter einem guten Problem verstehen wollen. Ein Problem ist gut, wenn uns seine Lösung zu neuen Einsichten, Methoden oder gar einer neuen Theorie führt. Viele Probleme der Unterhaltungsmathematik sind in diesem Sinn nicht gut, auch wenn ihre Lösung vielleicht beachtliche Fähigkeiten oder Intuition verlangt.

Ein pragmatischer Leser wendet vielleicht ein, dass die oben gestellten Probleme aus praktischer Sicht völlig nutzlos sind. Ist es nicht Zeitverschwendug, fragt der Skeptiker, eine ganze Vorlesung darüber zu hören, wo ich doch so viele nützliche Dinge lernen könnte, die meiner Karriere förderlich wären? Einwände dieser Art sind nicht selten, man kann sie nicht einfach übergehen — und wäre es nur, weil sie oft von den Menschen erhoben werden, die die Forschungsgelder verteilen.

Eine mögliche Antwort ist die, dass wir zu jedem dieser Unterhaltungsprobleme ein Pendant von großer praktischer Bedeutung finden. So muss z.B. ein Briefträger allen Haushalten in seinem Bezirk die Post bringen, also jede Straße mindestens einmal entlanglaufen. Was ist der kürzeste Weg für den Postboten? Kann man diesen in vertretbarer Zeit mit einem Supercomputer berechnen? Oder gar mit einem Personalcomputer? Das Botenproblem ist im Kern ein Problem über das Zeichnen von Linien in der Ebene ohne den Stift abzusetzen.

Ein weiteres Beispiel: Wenn für einen Schaltkreis die Positionen der Komponenten auf der Platine schon feststehen, kann man sie dann so verdrahten, dass die Verbindungen auf der Oberfläche der Platine verlaufen ohne sich zu kreuzen? Und welche Verteilung der Komponenten und der Verdrahtung auf der Platine beansprucht den geringsten Platz?

Dies sind typische Fragen des VLSI<sup>1</sup> Designs. Kennt man sich mit dem Brunnenproblem aus (vornehm gesprochen: mit Graphentheorie), dann findet man sich wesentlich leichter mit dem Design integrierter Schaltkreise zurecht.

Diese „praktischen Probleme“ gehören auch zur Graphentheorie, gepaart mit dem Design effizienter Algorithmen. Das vorliegende Buch verspricht keine Lösungen zu solch komplexen Problemen; um aber fortgeschrittene Bücher über diese Themen zu verstehen oder gar selbst eine Idee beizutragen, ist es ratsam zunächst die zu Grunde liegenden Konzepte zu begreifen.

Diese Probleme sind also nur scheinbar nutzlos. Aber kommt es darauf überhaupt an? Die fruchtbarste mathematische Forschung war nur selten durch praktische Ziele motiviert. Einige großartige Ideen haben erst kürzlich Anwendungen gefunden. Mathematik hat beachtliche Anwendungen, doch der Versuch die mathematische Forschung auf die direkt anwendbaren Teile zu beschneiden, hinterlässt einen leblosen Torso, dem der größte Teil der kreativen Kraft genommen ist.

Aufgaben sind in diesem Abschnitt wohl überflüssig — können Sie einige, vielleicht alle der hier vorgestellten Probleme lösen? Selbst wenn sie nur unvollständige Ergebnisse erhalten oder vielleicht gar keine, es wird Ihnen eine große Hilfe für das Weiterlesen sein, wenn sie es versuchen.

Was *ist* denn nun diskrete Mathematik? So fragt sich der Leser vielleicht nicht ganz zu Unrecht. Das Adjektiv „diskret“ ist hier als Gegensatz zu „kontinuierlich“ gemeint. Die Objekte der diskreten Mathematik (z.B. die natürlichen Zahlen) sind klar voneinander getrennt, und eine jede ist von den anderen wohlunterscheidbar; wir können sie als einzelne „Individuen“ wahrnehmen (so wie Bäume in einem nahen Wald). Im Gegensatz dazu gehen bei einem typischen „kontinuierlichen“ Objekt (z.B. den reellen Zahlen) die einzelnen Punkte ineinander über (wie Bäume in einem Wald, von einem hoch fliegenden Flugzeug aus gesehen). Wir können unsere Aufmerksamkeit auf einen bestimmten Punkt richten, doch es gibt immer ganz nahe dabei noch viele weitere Punkte, die wir nicht alle zugleich als Individuen wahrnehmen können.

Nach dieser Erklärung könnte man auch solche Teile der Mathematik wie Algebra oder Mengenlehre als „diskret“ bezeichnen. Doch gewöhnlich versteht man unter Diskreter Mathematik den Teil der Mathematik, der von endlichen Mengen handelt. An vielen Universitäten wird in der Vorlesung über Diskrete Mathematik das Gebiet recht weit gefasst: Man behandelt neben Kombinatorik, Zähltheorie und Graphentheorie auch Logik, Mengenlehre und theoretische Informatik (endliche Automaten, formale Sprachen, z.T. sogar Rechnerarchitektur). Wir

---

<sup>1</sup>Englisch: Very Large Scale Integration (Entwurf von Computer-Chips u.ä.)

bevorzugen eine etwas engere Definition, und so hätten wir dies Buch auch „Eine Einführung in Kombinatorik und Graphentheorie“ nennen können. Doch die Vorlesung, aus der dieses Buch entstanden ist, hieß nun einmal „Diskrete Mathematik“. Wir haben uns entschieden es dabei zu belassen.

## 1.2 Notation

**Zahlbereiche.** Für die Menge aller natürlichen Zahlen, d.h. für die Menge  $\{1, 2, 3, \dots\}$ , reservieren wir das Symbol  $\mathbb{N}$ . Die Buchstaben  $n, m, k, i, j, p$  und manchmal auch andere bezeichnen in der Regel natürliche Zahlen.

Ausgehend von den natürlichen Zahlen können wir andere wohlbekannte Zahlbereiche konstruieren: die ganzen, die rationalen und die reellen Zahlen (auch die komplexen Zahlen, aber die werden wir kaum benutzen).

Die *ganzen Zahlen* erhalten wir aus den natürlichen, indem wir die negativen Zahlen und die Null hinzunehmen. Die Menge aller ganzen Zahlen bezeichnen wir mit  $\mathbb{Z}$ .

Die *rationalen Zahlen* sind die Brüche mit ganzzahligem Zähler und Nenner. Normalerweise bezeichnet man diese Menge mit  $\mathbb{Q}$ , doch in diesem Buch brauchen wir kein Symbol für sie. Die Konstruktion der Menge  $\mathbb{R}$  aller *reellen Zahlen* ist komplizierter und wird gewöhnlich in einführenden Kursen zur Analysis behandelt. Wichtige Beispiele für reelle Zahlen, die nicht rational sind, sind Zahlen wie  $\sqrt{2}$ , wichtige Konstanten wie  $\pi$  und allgemein Zahlen, bei denen hinter dem Komma unendlich viele nicht periodische Ziffern folgen, z.B.  $0,12112111211112\dots$

Das *abgeschlossene Intervall* zwischen  $a$  und  $b$  auf der reellen Achse wird mit  $[a, b]$  bezeichnet, das *offene Intervall* mit den gleichen Endpunkten schreiben wir als  $(a, b)$ .

**Operationen mit Zahlen.** Die meisten Symbole für Operationen mit Zahlen wie  $+$  für die Addition,  $\sqrt{\phantom{x}}$  für die Quadratwurzel usw. sind allgemein bekannt. Die Division schreiben wir manchmal als Bruch und manchmal mit einem Schrägstrich, also entweder  $\frac{a}{b}$  oder  $a/b$ .

Wir führen noch zwei etwas weniger bekannte Funktionen ein. Ist  $x$  eine reelle Zahl, so bezeichnet  $\lfloor x \rfloor$  die Zahl „ $x$  abgerundet“, d.h. die

größte ganze Zahl, die kleiner oder gleich  $x$  ist<sup>2</sup>. Analog schreiben wir  $\lceil x \rceil$ , für „ $x$  aufgerundet“, die kleinste ganze Zahl größer gleich  $x$ . Zum Beispiel ist  $\lceil 0,999 \rceil = 0$ ,  $\lceil -0,1 \rceil = -1$ ,  $\lceil 0,01 \rceil = 1$ ,  $\lceil \frac{17}{3} \rceil = 6$ ,  $\lceil \sqrt{2} \rceil = 1$ .

Später werden wir noch weitere Operationen und Funktionen für Zahlen einführen, die eine wichtige kombinatorische Bedeutung haben und die wir uns etwas genauer ansehen werden, z.B.  $n!$  und  $\binom{n}{k}$ .

**Summen und Produkte.** Sind  $a_1, a_2, \dots, a_n$  reelle Zahlen, so schreibt man ihre Summe  $a_1 + a_2 + \dots + a_n$  oft kürzer mit dem Summationszeichen  $\sum$ , als

$$\sum_{i=1}^n a_i.$$

Diese Notation erinnert an die FOR-Schleife in vielen Programmiersprachen. Es folgen noch ein paar Beispiele:

$$\sum_{j=2}^5 \frac{1}{2j} = \frac{1}{4} + \frac{1}{6} + \frac{1}{8} + \frac{1}{10}$$

$$\sum_{i=2}^5 \frac{1}{2j} = \frac{1}{2j} + \frac{1}{2j} + \frac{1}{2j} + \frac{1}{2j} = \frac{2}{j}$$

$$\begin{aligned} \sum_{i=1}^n \sum_{j=1}^n (i+j) &= \sum_{i=1}^n ((i+1) + (i+2) + \dots + (i+n)) \\ &= \sum_{i=1}^n (ni + (1+2+\dots+n)) \\ &= n \left( \sum_{i=1}^n i \right) + n(1+2+\dots+n) \\ &= 2n(1+2+\dots+n). \end{aligned}$$

Analog zur Summenschreibweise mit  $\sum$  (das ist der griechische Buchstabe „Sigma“, er steht für Summe) gibt es die Produktschreibweise  $\prod$  (das griechische „Pi“). Ein Beispiel mag genügen:

---

<sup>2</sup>Hauptsächlich in der älteren Literatur wird häufig  $[x]$  statt  $\lfloor x \rfloor$  geschrieben („die Gaußklammer“).

$$\prod_{i=1}^n \frac{i+1}{i} = \frac{2}{1} \cdot \frac{3}{2} \cdot \dots \cdot \frac{n+1}{n} = n+1.$$

**Mengen.** Ein anderer elementarer Begriff, den wir ständig brauchen werden, ist der einer Menge. Wahrscheinlich kennen Sie Mengen schon aus der Schule (dank der permanenten Modernisierung des Schulsystems vielleicht sogar aus der Grundschule). Mengen werden gewöhnlich mit großen Buchstaben bezeichnet:

$$A, B, \dots, X, Y, \dots, M, N, \dots$$

und so weiter, ihre Elemente bezeichnet man meist mit kleinen Buchstaben:  $a, b, \dots, x, y, \dots, m, n, \dots$

Die Tatsache, dass eine Menge  $X$  ein Element  $x$  enthält, wird traditionell mit dem Symbol  $\in$  bezeichnet, dem stilisierten griechischen Buchstaben  $\varepsilon$  („Epsilon“). Wir lesen  $x \in X$  als „ $x$  ist ein Element von  $X$ “, „ $x$  gehört zu  $X$ “, „ $x$  ist in  $X$ “ oder ähnlich.

An dieser Stelle sollten wir erwähnen, dass das Konzept einer Menge und das Symbol  $\in$  *Grundbegriffe* sind in dem Sinne, dass wir sie nicht mittels anderer „elementarerer“ Begriffe definieren können (anders als etwa bei den rationalen Zahlen, die wir ja mit Hilfe der ganzen Zahlen definiert haben). Zum Verständnis des Konzepts „Menge“ bauen wir in diesem Buch auf die Intuition, unterstützt durch zahlreiche Beispiele. Zu Beginn des 20. Jahrhunderts hat sich allerdings herausgestellt, dass der naive Umgang mit „intuitiven Mengen“ in verschiedene absonderliche Situationen führt, zu den sogenannten *Paradoxien*.<sup>3</sup> Um Paradoxien zu umgehen wurde die gesamte Mengenlehre auf einer formalen Basis ganz neu aufgebaut, alle Eigenschaften von Mengen werden aus einigen wenigen, präzise formulierten Grundannahmen, den *Axiomen*, abgeleitet. Da die Mengen, die wir betrachten, fast immer endlich sein werden, brauchen wir uns vor Paradoxien nicht zu fürchten. Wir können also gut mit dem intuitiven Mengenbegriff leben.

Die Menge mit den Elementen 1, 37, und 55 wird als  $\{1, 37, 55\}$  geschrieben. Die Bezeichnungen  $\{37, 1, 55\}$  und  $\{1, 37, 1, 55, 55, 1\}$  drücken die gleiche Menge aus, d.h. das mehrfache Auftreten des

<sup>3</sup>Das berühmteste ist vielleicht das Russellsche Paradoxon. Eine mögliche Formulierung ist die mit dem Barbier bei der Armee. Er hat die Pflicht all jene Soldaten zu rasieren, die sich nicht selbst rasieren — muss er sich nun selbst rasieren oder nicht? Dieses Paradoxon kann auch in exakter mathematischer Sprache formuliert werden und impliziert die Inkonsistenz von intuitiv harmlosen Dingen wie z.B. der „Menge aller Mengen“.

gleichen Elements interessiert uns nicht und wird ignoriert. Ein Element kann nicht „zweimal“ in der gleichen Menge sein! Die drei Punkte in  $\{2, 4, 6, 8, \dots\}$  bedeuten „und weiter nach dem gleichen Muster“, in diesem Fall ist also die Menge aller geraden Zahlen gemeint. Das Bildungsmuster sollte auf den ersten Blick ersichtlich sein. Man erkennt zum Beispiel  $\{2^1, 2^2, 2^3, \dots\}$  leicht als die Menge aller Potenzen von 2, die Schreibweise  $\{2, 4, 8, \dots\}$  ist hingegen weniger klar.

**Geordnete und ungeordnete Paare.** Wir wissen schon, dass das Symbol  $\{x, y\}$  die Menge bezeichnet, die die Elemente  $x$  und  $y$  und sonst nichts enthält. In diesem speziellen Fall nennt man die Menge  $\{x, y\}$  auch das *ungeordnete Paar* von  $x$  und  $y$ . Das Paar  $\{x, y\}$  ist das gleiche wie  $\{y, x\}$ , und wenn  $x = y$  ist, dann enthält  $\{x, y\}$  genau ein Element.

Wir führen auch gleich die Notation  $(x, y)$  für das *geordnete Paar* von  $x$  und  $y$  ein. In diesem Fall ist die Reihenfolge der Elemente  $x$  und  $y$  wesentlich. Das bedeutet konkret:

$$(x, y) = (z, t) \text{ dann und nur dann wenn } x = z \text{ und } y = t. \quad (1.1)$$

Es ist interessant, wie man geordnete Paare mithilfe ungeordneter Paare definieren kann:

$$(x, y) = \{\{x\}, \{x, y\}\}.$$

Überprüfen Sie, dass die so definierten geordneten Paare die Bedingung (1.1) erfüllen! Im weiteren können wir  $(x, y)$  dann wie einen Grundbegriff verwenden.

Analog schreiben wir  $(x_1, x_2, \dots, x_n)$  für das *geordnete n-Tupel*<sup>4</sup> der Elemente  $x_1, x_2, \dots, x_n$ . Ein Spezialfall dieser Konvention ist, den Punkt in der Ebene mit Koordinaten  $x$  und  $y$  als  $(x, y)$  zu schreiben (und genauso für Punkte oder Vektoren im höherdimensionalen Raum).

**Mengendefinitionen.** Die interessanteren (und komplizierteren) Mengen definiert man normalerweise aus schon vorhandenen mittels einer Regel. Die Menge aller Quadrate natürlicher Zahlen können wir so schreiben:

$$\{i^2 : i \in \mathbb{N}\}$$

---

<sup>4</sup>Ein Paar ist ein 2-Tupel, ein 3-Tupel heißt Tripel, ein 4-Tupel manchmal Quadrupel — aber spätestens an dieser Stelle gehen die Namen aus und man spricht von  $n$ -Tupeln.

## 12 Grundlagen

oder auch

$$\{n \in \mathbb{N}: \text{ es gibt ein } k \in \mathbb{N} \text{ so dass } k^2 = n\}$$

oder mit dem Symbol  $\exists$  für „es gibt ein“:

$$\{n \in \mathbb{N}: \exists k \in \mathbb{N} (k^2 = n)\}.$$

Ein weiteres Beispiel ist die formale Definition des offenen Intervalls  $(a, b)$ , das wir weiter oben eingeführt haben:

$$(a, b) = \{x \in \mathbb{R}: a < x < b\}.$$

Hier haben wir ein schönes Beispiel für die mehrfache Belegung mathematischer Symbole:  $(a, b)$  kann zum einen das offene Intervall bedeuten, aber auch das geordnete Paar bestehend aus  $a$  und  $b$ . Welche dieser zwei verschiedenen Bedeutungen im konkreten Fall gemeint ist, muss man dem Kontext entnehmen — was in aller Regel keine besondere Mühe kostet. Diese Mehrfachbelegung von Symbolen ist keineswegs unüblich in der Mathematik, viele Symbole werden mit verschiedenen Bedeutungen benutzt. Eine dritte Bedeutung:  $(a, b)$  bezeichnet oft den größten gemeinsamen Teiler zweier natürlicher Zahlen  $a$  und  $b$  (diese Bedeutung werden wir in diesem Buch jedoch vermeiden).

**Die leere Menge.** Eine besonders wichtige Menge ist die, die überhaupt kein Element enthält. Es gibt genau eine solche Menge, man nennt sie die *leere Menge* und bezeichnet sie mit  $\emptyset$  oder  $\{\}$ . Wir weisen darauf hin, dass die leere Menge Element einer anderen Menge sein kann. Beispielsweise ist  $\{\emptyset\}$  die Menge, die die leere Menge enthält und sonst keine weiteren Elemente; das ist etwas anderes als  $\emptyset$ !

**Mengensysteme.** Als Mathematiker gehen wir viel mit Mengen um, deren Elemente wiederum Mengen sind. Zum Beispiel könnten wir die Menge

$$M = \{\{1, 2\}, \{1, 2, 3\}, \{2, 3, 4\}, \{4\}\},$$

definieren, die als Elemente vier Mengen mit natürlichen Zahlen enthält, oder genauer: vier Teilmengen der Menge  $\{1, 2, 3, 4\}$ . Gerade in der diskreten Mathematik begegnen uns solche Mengen sehr häufig, sie heißen *Mengensysteme* oder *Mengenfamilien*. Wir sagen also, dass  $M$  ein Mengensystem auf der Menge  $\{1, 2, 3, 4\}$  ist. Oft machen wir diese Situation dadurch kenntlich, dass wir Mengensysteme mit geschwungenen Buchstaben bezeichnen, etwa mit  $\mathcal{M}$ .

Solch eine Unterscheidung konsequent zu verfolgen ist allerdings schwierig — wie würden wir eine Menge bezeichnen, die Mengen von Mengen enthält?

Das Mengensystem aller möglichen Teilmengen einer Menge  $X$  nennen wir die *Potenzmenge* von  $X$  und bezeichnen sie mit dem Symbol<sup>5</sup>  $2^X$ . Eine andere gebräuchliche Bezeichnung der Potenzmenge ist  $\mathcal{P}(X)$ .

**Mächtigkeit.** Ein Großteil dieses Buches ist dem Zählen diverser Objekte gewidmet. Folglich ist die Anzahl der Elemente einer endlichen Menge  $X$  ein wichtiges Konzept für uns. Wir verwenden das gleiche Symbol wie für den Betrag einer Zahl:  $|X|$ .

**Eine noch allgemeinere Summenschreibweise.** Manchmal ist es vorteilhaft, Summen noch allgemeiner aufzuschreiben als einfach nach dem Muster  $\sum_{i=1}^n a_i$ . Zum Beispiel soll

$$\sum_{i \in \{1, 3, 5, 7\}} i^2$$

die Summe  $1^2 + 3^2 + 5^2 + 7^2$  bezeichnen. Unter das Summationszeichen schreiben wir die Laufvariable und die Menge, deren Werte sie nacheinander annehmen soll. Diese Schreibweise lässt uns reichlich Freiheit, die wir auch nutzen wollen. Wir können den Summationsbereich auch mit Worten beschreiben:

$$\sum_{\substack{i: 1 \leq i \leq 10 \\ i \text{ Primzahl}}} i = 2 + 3 + 5 + 7.$$

Wenn der Summationsbereich leer ist, dann definieren wir den Wert der Summe als 0, gleichgültig, was konkret hinter dem Summationszeichen steht. Zwei Beispiele sollen das illustrieren:

$$\sum_{i=1}^0 (i + 10) = 0, \quad \sum_{\substack{i \in \{2, 4, 6, 8\} \\ i \text{ ungerade}}} i^4 = 0.$$

Diese „Mengennotation“ können wir entsprechend auch für Produkte verwenden. Ein leeres Produkt, wie etwa  $\prod_{j: 2 \leq j < 1} 2^j$ , hat per Definition stets den Wert 1 (*nicht* 0 wie die leere Summe).

---

<sup>5</sup>Diese Notation mag auf den ersten Blick sonderbar anmuten, sie hat jedoch Tradition und als Begründung soll uns genügen, dass die Anzahl ihrer Elemente  $2^{|X|}$  ist; siehe Proposition 3.1.2.

**Mengenoperationen.** Mit Hilfe der elementaren Relation  $\in$  („ist Element von“) können wir weitere Relationen und sogar Operationen zwischen Mengen definieren. Zum Beispiel sind zwei Mengen  $X$  und  $Y$  gleich, wenn sie dieselben Elemente besitzen. Wir schreiben dann  $X = Y$ .

Andere Relationen zwischen Mengen können ähnlich einfach definiert werden. Für zwei Mengen  $X$  und  $Y$  bedeutet etwa  $X \subseteq Y$  (in Worten: „ $X$  ist eine Teilmenge von  $Y$ “), dass jedes Element aus  $X$  auch zu  $Y$  gehört.

Mit der Schreibweise  $X \subset Y$  wird manchmal die Tatsache ausgedrückt, dass  $X$  eine Teilmenge von  $Y$  ist, die aber nicht gleich  $Y$  ist. Diese Unterscheidung zwischen  $\subseteq$  und  $\subset$  wird jedoch in der Literatur nicht einheitlich gehandhabt, einige Autoren verwenden  $\subset$  sogar synonym mit unserem  $\subseteq$ . Es kommt übrigens auch das Zeichen  $\subsetneq$  vor — was mag das bedeuten?

Die Schreibweisen  $X \cup Y$  (die Vereinigungsmenge von  $X$  und  $Y$ ) und  $X \cap Y$  (die Schnittmenge von  $X$  und  $Y$ ) kann man so definieren:

$$X \cup Y = \{z: z \in X \text{ oder } z \in Y\}, \quad X \cap Y = \{z: z \in X \text{ und } z \in Y\}.$$

Wollen wir betonen, dass die Mengen  $X$  und  $Y$ , deren Vereinigung wir bilden, disjunkt sind, d.h. keine gemeinsamen Elemente haben, dann schreiben wir die Vereinigung als  $X \dot{\cup} Y$ . Der Ausdruck  $X \setminus Y$  ist die *Differenz* der Mengen  $X$  und  $Y$ , d.h. die Menge aller Elemente von  $X$ , die nicht zugleich in  $Y$  enthalten sind.

Große Symbole  $\cup$  und  $\cap$  werden im gleichen Sinne benutzt wie die Symbole  $\sum$  und  $\prod$ . Sind also  $X_1, X_2, \dots, X_n$  Mengen, dann kann man ihre Vereinigung kompakt als

$$\bigcup_{i=1}^n X_i \tag{1.2}$$

schreiben; analog für Schnittmengen.

Beachten Sie, dass diese Schreibweise nur deshalb möglich (d.h. eindeutig) ist, weil die Operationen  $\cup$  und  $\cap$  *assoziativ* sind; d.h. es gilt

$$X \cap (Y \cap Z) = (X \cap Y) \cap Z$$

und

$$X \cup (Y \cup Z) = (X \cup Y) \cup Z$$

für jedes Tripel  $X, Y, Z$  von Mengen. Das bedeutet, dass es gleichgültig ist, wie man die Vereinigung von 3 (oder allgemeiner  $n$ ) Mengen „beklammert“. Daher kann der gemeinsame Wert wie in (1.2) bezeichnet werden. Die Operationen  $\cup$  und  $\cap$  sind auch *kommutativ*, d.h. sie genügen den Bedingungen

$$X \cap Y = Y \cap X,$$

$$X \cup Y = Y \cup X.$$

Neben Kommutativität und Assoziativität erfüllen die Operationen  $\cup$  und  $\cap$  eine dritte wichtige Eigenschaft, die *Distributivität*. Für je drei Mengen  $X, Y, Z$  gilt

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z),$$

$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z).$$

Die Gültigkeit dieser beiden Gleichungen überprüft man, indem man zeigt, dass ein Element genau dann zu der Menge auf der linken Seite gehört, wenn es auch zur Menge auf der rechten Seite gehört. Das ist die Standardmethode um Mengengleichheit zu beweisen: Zwei Mengen  $A$  und  $B$  sind genau dann gleich, wenn sowohl  $A \subseteq B$  als auch  $B \subseteq A$  gelten. Auch das Distributivgesetz kann für beliebige Anzahlen von Mengen formuliert werden. Zum Beispiel

$$A \cap \left( \bigcup_{i=1}^n X_i \right) = \bigcup_{i=1}^n (A \cap X_i);$$

$$A \cup \left( \bigcap_{i=1}^n X_i \right) = \bigcap_{i=1}^n (A \cup X_i).$$

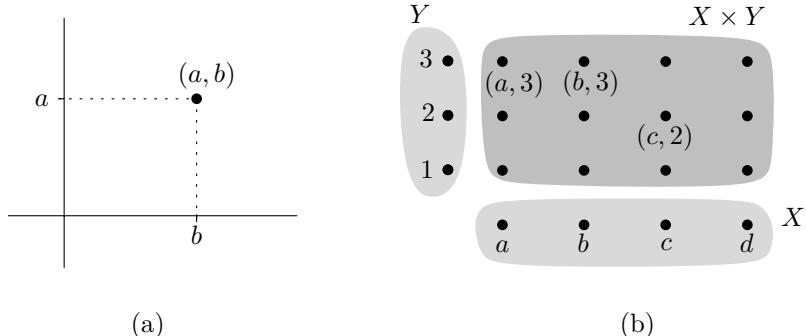
Gleichungen dieser Art kann man mit vollständiger Induktion beweisen, die in Abschnitt 1.3 behandelt wird. Weitere wichtige Regeln für Mengen sind die *de Morganschen Gesetze*

$$X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B) \quad \text{und} \quad X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$$

sowie ihre Verallgemeinerungen

$$X \setminus \left( \bigcup_{i=1}^n A_i \right) = \bigcap_{i=1}^n (X \setminus A_i)$$

$$X \setminus \left( \bigcap_{i=1}^n A_i \right) = \bigcup_{i=1}^n (X \setminus A_i).$$



**Abb. 1.1** Das kartesische Produkt: (a)  $\mathbb{R} \times \mathbb{R}$ ; (b)  $X \times Y$  für endliche Mengen  $X, Y$ .

Die letzte Operation, die wir hier einführen wollen, ist das *kartesische Produkt* zweier Mengen  $X$  und  $Y$ , das mit  $X \times Y$  bezeichnet wird. Das kartesische Produkt von  $X$  und  $Y$  ist die Menge aller geordneten Paare der Form  $(x, y)$ , wobei  $x \in X$  und  $y \in Y$ . Formal heißt das

$$X \times Y = \{(x, y) : x \in X, y \in Y\}.$$

Mit dem kartesischen Produkt haben wir ein Beispiel einer Operation, die nicht kommutativ ist: Im Allgemeinen sind  $X \times Y$  und  $Y \times X$  nicht gleich.

Der Name „kartesisches Produkt“ kommt von einer geometrischen Interpretation. Wählen wir nämlich  $X = Y = \mathbb{R}$ , dann können wir  $X \times Y$  interpretieren als die Menge aller Punkte in der Ebene, denn jeder Punkt in der Ebene ist eindeutig bestimmt durch ein geordnetes Paar reeller Zahlen, seine kartesischen Koordinaten<sup>6</sup> — die  $x$ -Koordinate und die  $y$ -Koordinate (Abb. 1.1(a)). Diese geometrische Sichtweise ist zuweilen auch für kartesischen Produkte solcher Mengen von Nutzen, deren Elemente keine Zahlen sind (Abb. 1.1(b)).

Das kartesische Produkt einer Menge mit sich selbst, also  $X \times X$ , wird auch mit  $X^2$  bezeichnet.

## Aufgaben

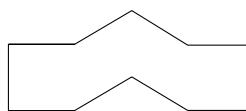
- Welche der folgenden Formeln sind richtig?

(a)  $\lfloor \frac{(n+1)^2}{2} \rfloor = \lfloor \frac{n^2}{2} \rfloor + n,$

---

<sup>6</sup>Die kartesischen Koordinaten hat René Descartes erfunden, der sich latinisiert Cartesius nannte.

- (b)  $\lfloor \frac{n+k}{2} \rfloor = \lfloor \frac{n}{2} \rfloor + \lfloor \frac{k}{2} \rfloor$ ,
- (c)  $\lceil (\lfloor x \rfloor) \rceil = \lceil x \rceil$  (wobei  $x$  eine beliebige reelle Zahl ist),
- (d)  $\lceil (\lfloor x \rfloor + \lfloor y \rfloor) \rceil = \lceil x \rceil + \lceil y \rceil$ .
2. \*Beweisen Sie, dass die Gleichung  $\lfloor \sqrt{x} \rfloor = \lfloor \sqrt{\lfloor x \rfloor} \rfloor$  für jede positive reelle Zahl  $x$  gilt.
3. (a) Definieren Sie, was eine „Beklammerung“ einer Vereinigung von  $n$  Mengen  $\bigcup_{i=1}^n X_i$  ist. Definieren Sie analog auch „Beklammerungen“ einer Summe von  $n$  Zahlen  $\sum_{i=1}^n a_i$ .
- (b) Beweisen Sie, dass je zwei Beklammerungen des Schnittes  $\bigcap_{i=1}^n X_i$  das gleiche Resultat ergeben.
- (c) Auf wieviele Arten kann man die Vereinigung  $A \cup B \cup C \cup D$  von 4 Mengen beklammen?
- (d) \*\*Suchen Sie nach einer Formel oder einer anderen Methode um die Anzahl der Beklammerungen einer Vereinigung von  $n$  Mengen  $\bigcup_{i=1}^n X_i$  zu zählen.
4. Wahr oder falsch? Wenn  $2^X = 2^Y$  für zwei Mengen  $X$  und  $Y$  gilt, dann muss  $X = Y$  sein.
5. Darf man bei kartesischen Produkten „kürzen“? Das soll heißen: Wenn  $X \times Y = X \times Z$  für drei Mengen  $X, Y, Z$  gilt, folgt daraus  $Y = Z$ ?
6. Zeigen Sie, dass für je zwei Mengen  $A, B$  gilt:
- $$(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B).$$
7. \*Betrachten Sie die Zahlen von 1 bis 1000. Zeigen Sie, dass sich unter je 501 von ihnen zwei Zahlen finden, von denen eine die andere teilt.
8. Mit diesem Problem können Sie Ihr Talent testen, einfache aber „versteckte“ Lösungen zu finden. Unterteilen Sie die folgende Figur in 7 kongruente Teile. Kongruent heißt, dass die Teile durch Verschieben, Drehen und eventuell Spiegeln zur Deckung gebracht werden können. Alle Außenseiten in der Figur haben Länge 1, die Winkel haben 90, 120 und 150 Grad.



### 1.3 Vollständige Induktion

Angenommen, wir wollen eine Summe wie  $1 + 2 + 2^2 + 2^3 + \cdots + 2^n = \sum_{i=0}^n 2^i$  berechnen (und haben die Formel für geometrische Reihen gerade nicht im Kopf). Wir könnten vermuten, dass es für diese Summe eine allgemeine Formel gibt, mit der man für jedes  $n$  ganz schnell die Summe weiß. Um die Formel zu raten würden wir wohl die Summe für ein paar kleine Werte  $n$  berechnen und darauf kommen, dass die Summe wahrscheinlich den Wert  $2^{n+1} - 1$  ergibt. Wie aber können wir beweisen, dass es so ist? Denn selbst, wenn wir diese Formel für eine Million verschiedene  $n$  überprüft haben, beim eine-million-und-ersten Wert für  $n$  könnte es anders sein. Die Korrektheit einer solchen Formel kann man mit der so genannten *vollständigen Induktion* beweisen. In unserem Beispiel würden wir so vorgehen:

1. Die Formel  $\sum_{i=0}^n 2^i = 2^{n+1} - 1$  ist richtig für  $n = 1$ , das sieht man direkt:  $2^0 + 2^1 = 2^2 - 1$ .
2. Nehmen wir einmal an, die Formel stimmt für einen Wert  $n = n_0$ . Wir beweisen, dass sie dann auch für  $n = n_0 + 1$  richtig ist. Es ist nämlich

$$\sum_{i=0}^{n_0+1} 2^i = \left( \sum_{i=0}^{n_0} 2^i \right) + 2^{n_0+1},$$

und die eingeklammerte Summe ist nach unserer Annahme (dass nämlich die Formel für  $n = n_0$  gilt) gleich  $2^{n_0+1} - 1$ . Daher ist

$$\sum_{i=0}^{n_0+1} 2^i = 2^{n_0+1} - 1 + 2^{n_0+1} = 2 \cdot 2^{n_0+1} - 1 = 2^{n_0+2} - 1.$$

Das ist genau die zu beweisende Formel für  $n = n_0 + 1$ .

Damit ist die Gültigkeit der Gleichung für beliebiges  $n$  bewiesen: Nach Schritt 1 ist die Formel für  $n = 1$  wahr, und wenn wir dieses Wissen in Schritt 2 hineinstecken (d.h.  $n_0 = 1$  setzen), erhalten wir daraus die Gültigkeit der Formel für  $n = 2$ . Mit diesem Wissen erhalten wir nun aus Schritt 2, dass die Formel für  $n = 3$  gilt, und indem wir so fortfahren, auch für jede weitere natürliche Zahl. Ganz wesentlich für das Argument ist, dass der konkrete Wert von  $n_0$  in Schritt 2 beliebig ist. Wir zeigen den Schritt von  $n_0$  auf  $n_0 + 1$  mit einem Schlag für alle natürlichen Zahlen  $n_0$ .

Schritt 2 bei dieser Art von Beweis nennt man den *Induktions-schritt*. Die Annahme, dass die zu beweisende Aussage für irgend-einen Wert  $n = n_0$  schon gilt, nennt man die *Induktionsannahme*, auch *Induktionsvoraussetzung*.

Eine der möglichen allgemeinen Formulierungen des Prinzips der vollständigen Induktion ist die folgende:

**1.3.1 Hilfssatz.** Es sei  $X$  eine Menge natürlicher Zahlen mit den folgenden beiden Eigenschaften:

- (i) Die Zahl 1 gehört zu  $X$ .
- (ii) Ist eine natürliche Zahl  $n$  Element von  $X$ , dann ist auch  $n + 1$  Element von  $X$ . ( $n \in X \Rightarrow n + 1 \in X$ .)

Dann enthält  $X$  alle natürlichen Zahlen ( $X = \mathbb{N}$ ).

In Anwendungen dieses Schemas ist  $X$  die Menge aller Zahlen  $n$ , für welche die Aussage  $A(n)$ , die gerade bewiesen werden soll, wahr ist.

Es gibt viele Varianten der vollständigen Induktion. Soll eine Aussage etwa nur für alle  $n \geq 2$  bewiesen werden (möglicherweise ist sie falsch für  $n = 1$ ), dann ist als erstes die Gültigkeit der Aussage für  $n = 2$  nachzuweisen. Als Induktionsvoraussetzung ist es manchmal vorteilhaft (oder notwendig), die Gültigkeit der Aussage nicht nur für  $n = n_0$ , sondern für alle  $n \leq n_0$  anzunehmen. Ein Verständnis dafür, was alles möglich ist, liefern am besten Beispiele.

Vollständige Induktion kann man entweder als grundlegende Eigen-schaft der natürlichen Zahlen auffassen (als Axiom, sie also ohne Beweis akzeptieren), oder man kann sie aus der folgenden anderen grundlegen-den Eigenschaft (Axiom) herleiten: *Jede nicht leere Menge natürlicher Zahlen besitzt ein kleinstes Element*. Diese Eigenschaft hat einen Na-men: Man sagt, die normale Ordnung der natürlichen Zahlen nach der Größe ist eine *Wohlordnung*. Ja, das Prinzip der vollständigen Induk-tion und das Wohlordnungsprinzip sind sogar äquivalent<sup>7</sup>, und jedes von ihnen könnte man als eines der Grundaxiome für die Theorie der natürlichen Zahlen nehmen.

*Beweis von Hilfssatz 1.3.1 aus dem Wohlordnungsprinzip.* Wir führen diesen Beweis indirekt: Nehmen wir einmal an, es gibt eine Menge  $X$ , die (i) und (ii) erfüllt, aber nicht alle natürlichen Zahlen enthält. Daraus werden wir einen Widerspruch ableiten. Sei  $Y$  die Menge derje-nigen natürlichen Zahlen, die nicht in  $X$  enthalten sind. Nach unserer

---

<sup>7</sup>sofern man annimmt, dass jede natürliche Zahl  $n > 1$  einen eindeutigen Vorgänger  $n - 1$  besitzt.

Annahme ist  $Y \neq \emptyset$ , also gibt es nach dem Wohlordnungsprinzip eine kleinste Zahl in  $Y$ , nennen wir sie  $n_0$ . Nun wissen wir aus (i), dass  $n_0 > 1$  ist, und weil  $n_0$  die kleinste Zahl ist, die nicht in  $X$  ist, muss die Zahl  $n_0 - 1$  in  $X$  enthalten sein. Daraus folgt aber mit (ii), dass  $n_0$  doch ein Element von  $X$  ist, ein Widerspruch.  $\square$

Eine Anmerkung noch: Diese Argumentation (beginnend mit „Sei  $n_0$  die kleinste Zahl, welche die zu beweisende Aussage verletzt“ einen Widerspruch herzuleiten, dass es nämlich eine noch kleinere „böse“ Zahl geben muss) wird manchmal anstelle von vollständiger Induktion benutzt. Man spricht von der „Suche nach dem kleinsten Verbrecher“, und im Grunde machen beide Verfahren das Gleiche. Welche Variante Verwendung findet, ist eine Frage des konkreten Problems und des persönlichen Geschmacks.

Vollständige Induktion ist eine unserer wichtigsten Beweismethoden, wir werden sehr oft Beweise mittels vollständiger Induktion führen. Daher wird es in den folgenden Kapiteln noch reichlich Beispiele und Aufgaben dazu geben.

**Die Natur mathematischer Beweise.** Mathematische Beweise sind eine erstaunliche Erfindung. Sie erlauben, die Wahrheit einer Aussage über jeden Zweifel zu erheben, sogar wenn die Aussage eine so komplizierte Situation beschreibt, dass sie sich der Anschauung entzieht. Man kann wohl kaum direkt einsehen, dass es keine zwei natürlichen Zahlen  $m, n$  gibt, für die  $\frac{m}{n} = \sqrt{2}$ , und doch können wir uns dieser Tatsache absolut sicher sein, weil sie sich mit einer Folge einfacher logischer Schlüsse beweisen lässt.

Eines der Hauptziele dieses Buches ist, dem Leser die Schönheit und Eleganz mathematischen Beweisens vor Augen zu führen. Wir wünschen uns, dass auch Sie die Befriedigung erfahren, die ein gelungener Beweis erzeugen kann — sei er nun aus einem Buch oder sogar ein eigener.

Ein möglicher Einwand ist, dass die meisten Studenten im späteren Beruf wohl nie solche Beweise brauchen werden. Wir glauben, dass man sich durch das Beweisen mathematischer Sätze nützliche Denkgewohnheiten antrainiert, etwa den Gebrauch klarer und präziser Begriffe, exaktes Formulieren von Gedanken und Aussagen und dass man keine Möglichkeiten übersieht, die vielleicht nicht ganz offensichtlich sind. Solche Gewohnheiten sind z.B. dann von unschätzbarem Wert, wenn man Software schreiben will, die nicht gleich abstürzt, wenn ein Fall eintritt, den man nicht eingeplant hat.

Beweise zu finden und aufzuschreiben ist teils Technik, teils eine Kunst.<sup>8</sup> Am besten lernt man das, indem man sich viele korrekte und „gute“ Beweise anschaut und versteht; dann muss man es selbst versuchen, wobei man eigentlich jemand braucht, der die Fehler in den eigenen Beweisen aufzeigt. Die falschen Beispiele sind sehr wichtig, und weil die Kommunikation durch ein Buch nur in eine Richtung verläuft, haben wir uns entschlossen, in diesem Buch auch einige falsche Beweise zu zeigen, d.h. Beweisversuche von Studenten, die nach unserer Erfahrung typische Fehler enthalten. Diese absichtlich falschen Beweise sind in einer anderen Schrift gesetzt. Im Rest dieses Abschnitts diskutieren wir ein paar häufige Fehlerquellen. (Die möglichen Fehlerarten in Beweisen sind zahlreich, wir streben keine enzyklopädische Vollständigkeit an und keine Klassifikation.)

Eine häufige Situation ist, dass der Anfänger das Problem nicht richtig versteht. Manchmal sind es Feinheiten in der Formulierung des Problems, die leicht zu übersehen sind, und ein Missverständnis ist nicht unbedingt Schuld des Studenten, der Autor des Problems kann sehr wohl Mehrdeutigkeiten übersehen haben. Das einzige Mittel gegen diese Art Missverständnis ist äußerste Aufmerksamkeit beim Lesen und Verstehen eines Problems, bevor man versucht es zu lösen. Testen Sie zuerst, ob das Problem in dem Sinn, in dem Sie es verstehen, sinnvoll ist. Ist die Lösung verdächtig einfach? Was könnte es noch heißen?

Eine mögliche Fehlerquelle ist der unkritische Gebrauch von Taschenrechnern und Computern. Auf die Frage, auf wie viele Nullen die dezimale Darstellung der Zahl  $50! = 50 \cdot 49 \cdot 48 \cdots \cdot 1$  endet, antwortete ein Student: 60, weil ein Taschenrechner mit einem 8-stelligen Display  $50! = 3,04140 \cdot 10^{64}$  berechnet. Nun, ein etwas besserer Rechner oder Computer, der Zahlen mit beliebig vielen Ziffern handhaben kann, würde dieses Problem korrekt lösen und berechnen, dass

$$50! = 304140932017133780436126081660647688443776415689605120000000000000$$

auf zwölf Nullen endet. Manche Softwaresysteme können sogar selbst eine Formel für die Summe  $1^2 \cdot 2^1 + 2^2 \cdot 2^2 + 3^2 \cdot 2^3 + \cdots + n^2 2^n$  finden oder die Anzahl binärer Bäume auf  $n$  Ecken (siehe Abschnitt 12.4) bestimmen. Doch natürlich können auch die Programmierer solcher Systeme Fehler machen,<sup>9</sup> daher ist es besser die Ergebnisse noch einmal zu überprüfen.

<sup>8</sup>Wir werden in diesem Buch nicht den Versuch unternehmen zu erklären, was ein guter Beweis ist!

<sup>9</sup>Und sogar die Computer selbst können sich „irren“: Erinnern Sie sich noch an den Fehler in der Fließkommaeinheit des Pentium Prozessors?

Außerdem sind die Fähigkeiten dieser Systeme noch sehr beschränkt; die künstliche Intelligenz müsste noch einige Fortschritte machen, bevor Computer eine Formel für die Anzahl der Nullen am Ende von  $n!$  entdecken und beweisen können, oder einen Ernst zu nehmenden Teil der Probleme in diesem Buch lösen können.

Im Prinzip kann man Beweise so detailliert und so formal aufschreiben, dass sie automatisch durch einen Computer überprüft werden können. Ist ein solcher Beweis falsch, dann muss irgend ein Schritt eindeutig falsch sein, doch leider ist es sehr aufwändig und nicht praktikabel, Beweise vollständig zu formalisieren. Alle Beweise in Lehrbüchern und alle Lösungen zu Aufgaben sind bis zu einem gewissen Grade informell.

Kleinere Ungenauigkeiten mögen nötig sein, will man einen Beweis vernünftig darstellen, doch allzuleicht verbergen sie auch Fehler. Eine gute Regel beim Schreiben und Überprüfen von Beweisen ist, dass *in einem korrekten Beweis jede Aussage wirklich richtig sein sollte*. Oft entdeckt man Fehler in einem Beweis, indem man eine falsche Aussage, einen Fehler in einer Rechnung oder eine Aussage, die sinnlos ist, isoliert („seien  $\ell_1$  und  $\ell_2$  zwei beliebige Geraden im dreidimensionalen Raum, und sei  $\rho$  eine Ebene, die beide enthält...“). Sind sie erst einmal entdeckt und ans Tageslicht gebracht, sind solche Fehler für (fast) jeden offensichtlich. Trotzdem kommen Sie häufig vor. Wenn man über einem Beweis brütet und plötzlich eine Idee hat, die zum Ziel zu führen scheint, und denkt: DAS ist es, dann vergisst man gewöhnlich jede Vorsicht und ist bereit den blanken Unsinn niederzuschreiben. (Leider ist die erste Idee, die einem in den Sinn kommt, meist Unsinn und kein Geniestreich, zumindest nach unserer Erfahrung mit dem Lösen von Problemen.)

Ein besonders häufiger Fehler, der wahrscheinlich jedem Matematiker schon einmal unterlaufen ist, ist einen Fall zu übersehen. Der Beweis funktioniert für einige Objekte, für die er konzipiert ist, doch nicht in anderen Fällen, die der Autor übersehen hat. Fallunterscheidungen sehen in jeder konkreten Situation anders aus, dennoch findet man immer wieder die gleichen Fehler. Teilen einer Gleichung durch  $x - y$  ist nur für  $x \neq y$  erlaubt, der Fall  $x = y$  muss gesondert behandelt werden. Auf den Schnittpunkt zweier Geraden darf man in einem Beweis nur zurückgreifen, wenn die Geraden nicht parallel sind. Es ist fahrlässig aus  $a > b$  auf  $a^2 > b^2$  zu schließen, wenn man nichts über das Vorzeichen von  $a$  und  $b$  weiß, usw.

Viele Beweise gerade von Anfängern sind auch deshalb falsch, weil richtige Sätze falsch angewendet werden. Eine Aussage scheint aus einem Satz (aus der Vorlesung oder aus einem Lehrbuch) zu folgen, aber in Wirklichkeit sagt der Satz etwas anderes, oder einige der Voraussetzungen sind nicht gegeben. Da wir bisher keine nennenswerten Sätze behandelt haben, wollen wir ein künstliches geometrisches Beispiel geben: „Weil  $ABC$  ein gleichschenkliges Dreieck ist, bei dem die Seiten, die an  $A$  stoßen, die gleiche Länge haben, gilt  $|AB|^2 + |AC|^2 = |BC|^2$  nach dem Satz des Pythagoras.“ Ist nicht im Satz des Pythagoras von einem rechten Winkel die Rede?

Häufig beruhen Fehler und Missverständnisse darauf, dass man sich unbemerkt auf unbewiesene Behauptungen stützt.

Viele Beweise, auch korrekte und sogar solche in Lehrbüchern, enthalten unbewiesene Aussagen, man erkennt sie anhand von Schlüsselworten wie „offensichtlich“. In einem ehrlichen Beweis sollte die Bedeutung solcher Worte idealerweise sein: „Ich, der Autor dieses Beweises, sehe wie man diese Aussage streng beweist, und weil sie mir einfach genug zu sein scheint, vertraue ich darauf, dass Sie, mein Leser, ohne allzu große Anstrengung die Details selbst ausfüllen können.“ In vielen Zeitschriftenartikeln bekommt der Leser jedoch den Eindruck, dass der Autor eher so etwas denkt wie: „Ich sehe so ungefähr, wie man das beweisen könnte, weil ich schon jahrelang an diesem Problem arbeite, und wenn Sie es nicht sehen, dann ist das Ihr Problem.“ Teile von Beweisen auszulassen, die „klar“ scheinen, ist also eine hochgradig schwierige soziale Angelegenheit, und man sollte immer sehr vorsichtig dabei sein. Und Studenten sollten sich nicht wundern, wenn ihr Lehrer darauf besteht, dass solche „offensichtlichen“ Teile im Detail bewiesen werden. Denn was wäre ein besserer Platz Fehler in einem Beweis zu verstecken als in den Teilen, die fehlen?

Ein ernsteres Problem betrifft Teile eines Beweises, die unbeabsichtigt ausgelassen sind. Meistens ist die Aussage, deren Beweis fehlt, nicht einmal explizit formuliert.<sup>10</sup> Es kann eine sehr anspruchsvolle Aufgabe sein, den Autor eines Beweises davon zu überzeugen, dass etwas damit falsch ist, besonders dann, wenn die unbewiesene Aussage wirklich wahr ist.

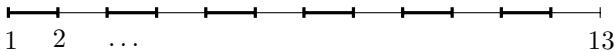
Ein typischer unvollständiger Anfängerbeweis in der diskreten Mathematik besteht darin, dass ein Spezialfall für den allgemeinen Fall

<sup>10</sup>Die Ansprüche an die Genauigkeit eines Beweises sind im Laufe der Zeit gestiegen; selbst wenn man die Beweise der größten Mathematiker vergangener Jahrhunderte betrachtet, können nur die wenigsten den heutigen Maßstäben standhalten.

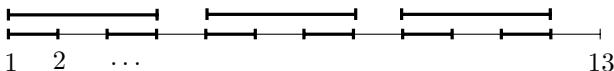
gehalten wird. Als ein Beispiel lassen Sie uns die folgende Aufgabe aus einer Mathematikolympiade betrachten:

**1.3.2 Problem.** Sei  $n > 1$  eine ganze Zahl. Sei  $M$  eine Menge abgeschlossener Intervalle. Die Endpunkte  $u, v$  eines jeden Intervalls  $[u, v] \in M$  seien natürliche Zahlen mit  $1 \leq u < v \leq n$ . Angenommen, für je zwei verschiedene Intervalle  $I, I' \in M$  tritt einer der folgenden Fälle ein:  $I \cap I' = \emptyset$  oder  $I \subset I'$  oder  $I' \subset I$  (d.h. je zwei Intervalle überlappen ganz oder gar nicht). Zeigen Sie, dass  $|M| \leq n - 1$ .

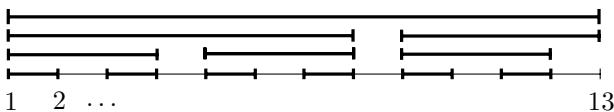
**Ein Beweisversuch.** Um  $M$  so groß wie möglich zu machen fügen wir als erstes möglichst viele Einheitsintervalle ein, wie in dem folgenden Bild:



Diese  $\lfloor n/2 \rfloor$  Intervalle sind alle disjunkt. Nun muss jedes andere Intervall in  $M$  mindestens zwei dieser Einheitsintervalle enthalten (oder für ungerades  $n$  eventuell das letzte Einheitsintervall plus den letzten Punkt, der noch übrig bleibt). Um also möglichst viele Intervalle zu erhalten fügen wir die nächste „Schicht“ kürzestmöglicher Intervalle hinzu, und zwar so:



Auf diese Weise fahren wir fort, Schicht um Schicht hinzufügend, bis wir schließlich als letzte Schicht das gesamte Intervall  $[1, n]$  hinzufügen:



Es bleibt zu zeigen, dass die so konstruierte Menge  $M$  höchstens  $n - 1$  Intervalle enthält. Wir beobachten, dass jedes Intervall in der  $k$ -ten Schicht einen Punkt der Form  $i + \frac{1}{2}$ ,  $1 \leq i \leq n - 1$  enthält, der in keinem der Intervalle der vorangegangenen Schichten enthalten ist, weil der Zwischenraum zwischen den zwei Intervallen in der vorigen Schicht noch nicht überdeckt war, bevor die  $k$ -te Schicht hinzugefügt wurde. Deshalb ist  $|M| \leq n - 1$  wie behauptet.  $\square$

Dieser „Beweis“ sieht ziemlich clever aus (die Art, die Intervalle in dem speziellen  $M$  zu zählen, das in dem Beweis konstruiert wird, ist sogar sehr elegant). Was ist also falsch daran? Nun, wir haben gezeigt, dass *ein spezielles*  $M$  die geforderte Ungleichung  $|M| \leq n - 1$  erfüllt. Der Beweis will suggerieren, dass dieses spezielle  $M$  der schlimmstmögliche Fall ist, dass kein anderes  $M$  mehr Intervalle haben kann, aber tatsächlich zeigt er nichts dergleichen. Zum Beispiel argumentiert der erste Schritt, dass ein  $M$  mit der maximal möglichen Zahl von Intervallen  $\lfloor n/2 \rfloor$  Einheitsintervalle enthalten sollte. Aber das ist nicht wahr,

wie die Menge  $M = \{[1, 2], [1, 3], [1, 4], \dots, [1, n]\}$  zeigt. Obigen „Beweis“ zu „retten“, indem man an den verschiedenen Schritten herumbastelt, ist wahrscheinlich schwieriger, als einen anderen, korrekten Beweis zu finden. Auch wenn der oben gezeigte „Beweis“ einige nützliche Hinweise enthält (die Zählidee am Ende des Beweises kann so modifiziert werden, dass sie für jedes  $M$  funktioniert), ist er ziemlich weit davon entfernt eine gültige Lösung der Aufgabe zu sein.

Dieses „Beweisschema“ hat offensichtlich eine große Anziehungs-kraft: zu behaupten, dieses Objekt  $X$  muss das Schlimmste sein, und dann zu zeigen, dass dieses spezielle  $X$  tut, was es soll. Doch die Behauptung, dass nichts schlimmer sein kann als dieses  $X$ , wird nicht bewiesen (obwohl es meist ziemlich plausibel aussieht, dass wir bei der Konstruktion dieses  $X$  den schlimmsten Fall in Bezug auf die zu beweisende Aussage konstruieren).

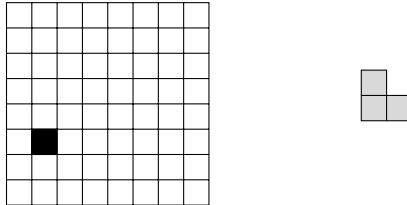
Eine Variante dieses Fehlers taucht häufig in Induktionsbeweisen auf. In den Abschnitten 5.1 und 6.3 geben wir Beispiele dazu.

## Aufgaben

1. Beweisen Sie die folgenden Formeln mittels vollständiger Induktion:
  - (a)  $1 + 2 + 3 + \dots + n = n(n + 1)/2$
  - (b)  $\sum_{i=1}^n i \cdot 2^i = (n - 1)2^{n+1} + 2$ .
2. Die Zahlen  $F_0, F_1, F_2, \dots$  sind wie folgt definiert:  $F_0 = 0$ ,  $F_1 = 1$ ,  $F_{n+2} = F_{n+1} + F_n$  für  $n = 0, 1, 2, \dots$ . Beweisen Sie, dass für jedes  $n \geq 0$  die Formel  $F_n \leq ((1 + \sqrt{5})/2)^{n-1}$  gilt (siehe auch Abschnitt 12.3). Übrigens: Fällt Ihnen auf, dass die Zahlen  $F_i$  durch Induktion definiert sind? Induktive Definitionen nennt man auch *rekursiv*.
3. (a) Stellen Sie sich vor, Sie zeichnen  $n$  Geraden in die Ebene, und zwar so, dass keine zwei parallel sind und dass sich keine drei in einem gemeinsamen Punkt schneiden. Zeigen Sie, dass die Ebene dadurch in exakt  $n(n + 1)/2 + 1$  Teile zerschnitten wird.  
 (b) \*Analog zur vorigen Übung: Wir betrachten  $n$  Ebenen im dreidimensionalen Raum, von denen keine zwei parallel sind, keine drei sich in einer Geraden schneiden und keine vier einen gemeinsamen Punkt haben. In wieviele Gebiete zerteilen diese Ebenen den Raum?
4. Beweisen Sie den *Satz von de Moivre* mit Induktion:  $(\cos \alpha + i \sin \alpha)^n = \cos(n\alpha) + i \sin(n\alpha)$ . Dabei ist  $i$  die imaginäre Einheit.
5. Im alten Ägypten schrieb man Brüche als Summe von Brüchen mit Zähler 1. Zum Beispiel ist  $\frac{3}{5} = \frac{1}{2} + \frac{1}{10}$ . Untersuchen Sie folgenden Algorithmus um einen Bruch  $\frac{m}{n}$  auf diese Gestalt zu bringen ( $1 \leq m < n$ ): Schreiben Sie den Bruch  $\frac{1}{\lceil n/m \rceil}$ , berechnen Sie  $\frac{m}{n} - \frac{1}{\lceil n/m \rceil}$ , und solange das nicht Null ist, wiederholen Sie diesen Schritt. Beweisen

Sie, dass dieser Algorithmus stets nach einer endlichen Anzahl von Schritten fertig wird.

6. \*Betrachten Sie ein  $2^n \times 2^n$  „Schachbrett“, aus dem ein beliebiges Feld entfernt wurde, etwa so wie in dem folgenden Bild (mit  $n = 3$ ):



Beweisen Sie, dass man jedes solche Schachbrett ohne Lücken oder Überlappungen mit L-förmigen Steinen belegen kann, die jeweils drei Felder bedecken.

7. Sei  $n \geq 2$  eine natürliche Zahl. Wir betrachten folgendes Spiel: Zwei Spieler schreiben gemeinsam eine Folge von Nullen und Einsen auf. Sie beginnen mit einer leeren Zeile und ziehen abwechselnd. Ein Zug besteht darin, an das Ende der Zeile eine 0 oder eine 1 zu schreiben. Ein Spieler verliert, wenn die von ihm hinzugefügte Ziffer einen Block der Länge  $n$  erzeugt, der in der Folge schon einmal vorkommt (auch wenn die beiden Positionen überlappen). Für  $n = 4$  könnte eine Folge so aussehen: 00100001101011110011 (der zweite Spieler hat verloren, weil durch den letzten Zug 0011 wiederholt wird).
- (a) Beweisen Sie, dass dieses Spiel stets nach endlich vielen Schritten ein Ende findet.
  - (b) \*Angenommen,  $n$  ist ungerade. Zeigen Sie, dass der zweite Spieler (also der den zweiten Zug macht) eine Gewinnstrategie hat.
  - (c) \*Zeigen Sie, dass für  $n = 4$  der erste Spieler eine Gewinnstrategie hat. Für alle geraden  $n > 4$  ist das Problem, welcher Spieler eine Gewinnstrategie hat, ungelöst.
8. \*Auf einem unendlich großen Blatt Karopapier sind  $n$  Kästchen schwarz, alle anderen sind weiß. Zu den Zeitpunkten  $t = 1, 2, \dots$  werden alle Kästchen nach der folgenden Regel neu gefärbt: Jedes Kästchen erhält die Farbe, die in dem Tripel bestehend aus sich selbst sowie den Nachbarn oben und rechts am häufigsten (also mindestens zwei mal) vorkommt. Zeigen Sie, dass nach dem Zeitpunkt  $t = n$  alle Kästchen weiß sind.
9. Ein Teilchen befindet sich zur Zeit 0 im Punkt 0 auf der Zahlengeraden. Dieses Teilchen zerfällt in zwei Teile, die in entgegengesetzte Richtungen auseinanderfliegen und nach 1 Sekunde im Abstand 1 vom ursprünglichen Teilchen anhalten. Innerhalb der nächsten Sekunde

zerfallen diese beiden Teilchen, emittieren jeweils zwei neue Teilchen, die in verschiedene Richtungen auseinanderfliegen und im Abstand 1 vom Punkt des Zerfalls anhalten, und so weiter. Immer wenn sich zwei Teilchen treffen, vernichten sie sich gegenseitig (ohne dass etwas übrigbleibt). Wie viele Teilchen wird es zum Zeitpunkt  $2^{11} + 1$  geben?

10. \*Sei  $M \subseteq \mathbb{R}$  eine Menge reeller Zahlen, in der jede nicht leere Teilmenge von  $M$  eine kleinste und eine größte Zahl enthält. Beweisen Sie, dass  $M$  endlich ist.
11. Wir werden die folgende Aussage mit vollständiger Induktion beweisen: *Seien  $\ell_1, \ell_2, \dots, \ell_n$  verschiedene Geraden in der Ebene, von denen keine zwei parallel sind ( $n \geq 2$ ). Dann haben alle diese Geraden einen Punkt gemeinsam.*
  1. Für  $n = 2$  ist die Aussage wahr, denn je 2 nichtparallele Geraden schneiden sich.
  2. Angenommen, die Aussage gilt für  $n = n_0$ . Seien nun  $n = n_0 + 1$  Geraden  $\ell_1, \dots, \ell_n$  mit den geforderten Eigenschaften gegeben. Nach Induktionsvoraussetzung haben die ersten  $n_0$  dieser Geraden (also  $\ell_1, \ell_2, \dots, \ell_{n-1}$ ) einen gemeinsamen Punkt; nennen wir ihn einmal  $x$ . Genauso haben auch die  $n_0$  Geraden  $(\ell_1, \ell_2, \dots, \ell_{n-2}, \ell_n)$  einen Punkt gemeinsam; wir nennen ihn  $y$ . Die Gerade  $\ell_1$  liegt in beiden Gruppen, enthält also sowohl  $x$  als auch  $y$ . Das trifft auch auf  $\ell_{n-2}$  zu. Nun schneiden sich aber  $\ell_1$  und  $\ell_{n-2}$  in einem eindeutigen Punkt, also muss  $x = y$  sein. Deshalb haben alle Geraden  $\ell_1, \dots, \ell_n$  einen gemeinsamen Punkt, nämlich  $x$ .

Irgendetwas ist faul daran. Nur was?

12. Seien  $n_1, n_2, \dots, n_k$  natürliche Zahlen, jede von ihnen mindestens 1, und sei  $n_1 + n_2 + \dots + n_k = n$ . Zeige, dass  $n_1^2 + n_2^2 + \dots + n_k^2 \leq (n - k + 1)^2 + k - 1$ .

„Lösung“: Der Ausdruck  $\sum_{i=1}^k n_i^2$  wird besonders groß, wenn wir alle bis auf ein  $n_i$  auf 1 setzen und einen (das ergibt sich daraus) auf  $n - k + 1$ . In diesem Fall ist die Summe der Quadrate genau  $(n - k + 1)^2 + k - 1$ .

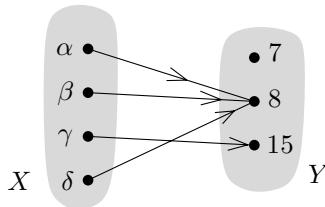
Warum ist das kein akzeptabler Beweis? \*Geben Sie einen korrekten Beweis.

13. \*Geben Sie einen korrekten Beweis für das Problem 1.3.2 an.
14. \*Seien  $n > 1$  und  $k$  zwei gegebene natürliche Zahlen und  $I_1, I_2, \dots, I_m$  abgeschlossene (nicht notwendig verschiedene) Intervalle mit der Eigenschaft, dass bei jedem Intervall  $I_j = [u_j, v_j]$  die Zahlen  $u_j$  und  $v_j$  natürliche Zahlen mit  $1 \leq u_j < v_j \leq n$  sind, und dass außerdem keine Zahl in mehr als  $k$  der Intervalle  $I_1, \dots, I_m$  enthalten ist. Welches ist der größtmögliche Wert für  $m$ ?

## 1.4 Funktionen

Der Begriff der Funktion ist grundlegend in der Mathematik. Die heutige Sichtweise von Funktionen hat sich erst langsam entwickelt. Lange Zeit hat man nur reelle oder komplexe Funktionen betrachtet, und was eine richtige Funktion sein wollte, musste sich durch eine Formel wie  $f(x) = x^2 + 4$ ,  $f(x) = \sqrt{\sin(x/\pi)}$ ,  $f(x) = \int_0^x (\sin t/t)dt$ , oder  $f(x) = \sum_{n=0}^{\infty} (x^n/n!)$  ausdrücken lassen. Aus moderner Sicht darf eine reelle Funktion jeder reellen Zahl eine beliebige andere Zahl als Funktionswert zuordnen.

Nehmen wir uns einmal zwei beliebige Mengen. Anschaulich ist eine Funktion wie ein Automat, in den man ein Element aus  $X$  hineinsteckt und der einem dafür ein eindeutig bestimmtes Element aus  $Y$  herausgibt. Wir können uns ein Bild von einer Funktion machen, indem wir die Mengen  $X$  und  $Y$  zeichnen und von jedem Element  $x$  aus  $X$  ausgehend einen Pfeil zu demjenigen Element  $y$  aus  $Y$  zeichnen, das der Automat ausgibt, wenn man  $x$  eingeworfen hat:



Unsere erste Beobachtung ist, dass von jedem Element in  $X$  genau ein Pfeil ausgeht, während in die Elemente aus  $Y$  kein, ein oder mehrere Pfeile hineinführen. Solch eine Zeichnung einer Funktion wollen wir als *Pfeildiagramm* bezeichnen.

Jetzt gießen wir diese Anschauung in eine mathematische Definition und stützen uns dabei auf Objekte, die wir schon kennen, auf Mengen und geordnete Paare.

**1.4.1 Definition.** Eine Funktion  $f$  aus einer Menge  $X$  in eine Menge  $Y$  ist eine Menge geordneter Paare  $(x, y)$  mit  $x \in X$  und  $y \in Y$  (mit anderen Worten, eine Teilmenge des kartesischen Produkts  $X \times Y$ ) mit der Eigenschaft, dass zu jedem  $x \in X$  genau ein Paar mit erster Komponente  $x$  in  $f$  enthalten ist.

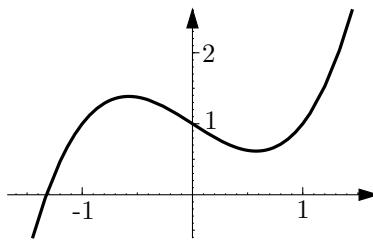
Mengen, Abbildungen und Relationen sind wichtige Grundbegriffe in der Mathematik. Jeder dieser Begriffe lässt sich durch jeden anderen definieren. In der Regel geht man von Mengen aus und definiert damit Abbildungen und Relationen, weil „Menge“ das elementarste der drei

Konzepte ist. Man könnte aber genausogut mit einem der anderen beiden Begriffe beginnen.

Dass das geordnete Paar  $(x, y)$  in  $f$  ist, codiert uns also, dass die Funktion  $f$  uns die Zahl  $y$  gibt, wenn sie  $x$  bekommt. Wir schreiben dafür  $y = f(x)$ , und wir sagen,  $f$  bildet  $x$  auf  $y$  ab,  $f$  ordnet dem Wert  $x$  den Wert  $y$  zu oder  $y$  ist das *Bild* von  $x$ .

Die Beispieldfunktion im Bild oben etwa besteht aus den geordneten Paaren  $(\alpha, 8)$ ,  $(\beta, 8)$ ,  $(\gamma, 15)$  und  $(\delta, 8)$ .

So abstrakt diese Definition auf den ersten Blick aussieht, sie entspricht doch der Art und Weise, wie wir (z.B. in der Schule) am häufigsten Funktionen zeichnen: Der *Graph* einer Funktion wie in Abb. 1.1 ist ein Bild des kartesischen Produkts  $X \times Y$ , in dem die Punkte  $(x, f(x))$  markiert sind. Die folgende Abbildung zeigt den Graphen derjenigen Funktion  $f: \mathbb{R} \rightarrow \mathbb{R}$ , die durch  $f(x) = x^3 - x + 1$  gegeben ist:



Dass  $f$  eine Funktion aus einer Menge  $X$  in eine Menge  $Y$  ist, wird mit folgender Schreibweise abgekürzt:

$$f: X \rightarrow Y .$$

Und die Tatsache, dass die Funktion  $f$  einem Element  $x$  ein Element  $y$  zuordnet, wird auch als

$$f: x \mapsto y .$$

geschrieben. Wir könnten stattdessen auch einfach  $y = f(x)$  schreiben. Wozu also diese neue Schreibweise? Der Vorteil des Symbols  $\mapsto$  ist, dass wir so über eine Funktion reden können, ohne ihr einen Namen zu geben. (In der Programmiersprache LISP oder der Mathematiksoftware Mathematica gibt es zum Beispiel namenlose Funktionen.) Es ist nicht korrekt, zu sagen: „Betrachten Sie die Funktion  $x^2$ “, weil wir nicht dazu sagen, was die Variable ist. In diesem speziellen Fall können wir uns ziemlich sicher sein, dass die Funktion  $x \mapsto x^2$  gemeint ist, aber wenn es heißt: „Betrachten Sie die Funktion  $zy^2 + 5z^3y$ “, dann ist nicht klar, ob der Ausdruck von  $x$  oder von  $z$  abhängen soll — oder von beiden. Wenn man hingegen  $y \mapsto zy^2 + 5z^3y$  schreibt, dann ist klar, dass wir die Abhängigkeit von  $y$  untersuchen und  $z$  als Parameter ansehen wollen.

Gleichbedeutend mit dem Wort „Funktion“ ist „Abbildung“.

Für die Menge  $\{f(x) : x \in X\}$  aller Funktionswerte der Funktion  $f$  schreiben wir auch  $f(X)$ . Klar, dass es zu einem so wichtigen Begriff wie „Funktion“ viele weitere Abkürzungen, Schreibweisen und Namen gibt (z.B. nennt man  $X$  den *Definitionsbereich* und  $Y$  den *Wertebereich* von  $f$ ), doch wir wollen unsere Terminologie auf das notwendige beschränken.

Wir sollten aber unbedingt erwähnen, dass man Funktionen hintereinander ausführen kann.

**1.4.2 Definition (Komposition von Funktionen).** Sind  $f: X \rightarrow Y$  und  $g: Y \rightarrow Z$  zwei Funktionen, dann können wir eine neue Funktion  $h: X \rightarrow Z$  definieren, deren Werte durch

$$h(x) = g(f(x))$$

für jedes  $x \in X$  gegeben sind. In Worten: Um den Wert von  $h(x)$  zu berechnen wenden wir zunächst die Funktion  $f$  auf  $x$  an und danach die Funktion  $g$  auf das Ergebnis.

Die Funktion  $h$  (bitte überprüfen Sie, dass  $h$  wirklich eine Funktion ist) heißt die Verknüpfung oder Komposition oder Hintereinanderausführung der Funktionen  $g$  und  $f$  und wird mit  $g \circ f$  bezeichnet. Das heißt, für jedes  $x \in X$  ist

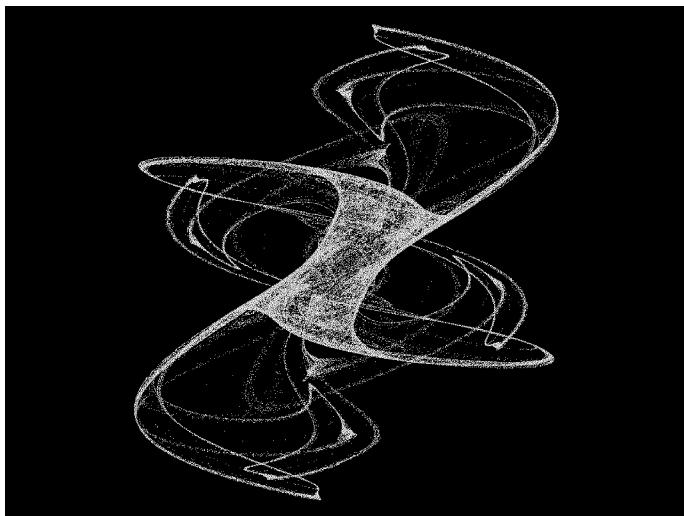
$$(g \circ f)(x) = g(f(x)).$$

Die Verknüpfung von Funktionen ist assoziativ, aber nicht kommutativ. Selbst wenn  $g \circ f$  wohldefiniert ist, kann man nicht einmal darauf zählen, dass  $f \circ g$  auch definiert ist. Damit zwei Funktionen verknüpft werden können, muss die „mittlere“ Menge  $Y$  die gleiche sein (zumindest muss der Wertebereich von  $f$  im Definitionsbereich von  $g$  enthalten sein, damit  $g$  überhaupt angewendet werden kann.)

Die Verknüpfung von Funktionen kann sehr interessant, sogar aufregend werden. Betrachten wir zum Beispiel die Abbildung  $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$  von der Ebene in sich selbst, die durch

$$f: (x, y) \mapsto \left( \sin(ax) + b \sin(ay), \sin(cx) + d \sin(cy) \right)$$

mit  $a = 2,879879$ ,  $b = 0,765145$ ,  $c = -0,966918$ ,  $d = 0,744728$  gegeben ist. Auf den ersten Blick sieht diese Funktion nicht besonders interessant aus, vielleicht sehen die Konstanten ein bisschen kompliziert aus. Startet man jedoch mit dem Punkt  $p = (0,1; 0,1)$  und markiert die ersten hunderttausend oder million Punkte der Folge  $p, f(p),$



**Abb. 1.2** „Des Königs Traum“. Die Formel für dieses Fraktal ist dem Buch von C. Pickover entnommen: *Chaos in Wonderland*, St Martin’s Press, New York 1994.

$f(f(p)), f(f(f(p))), \dots$ , dann erhält man ein Bild wie in Abb. 1.2.<sup>11</sup> Es handelt sich dabei um ein so genanntes *Fraktal*; es scheint keine allgemein akzeptierte mathematische Definition von Fraktalen zu geben. Man versteht darunter im Allgemeinen komplizierte Punktmengen, die durch relativ einfache Funktionen erzeugt werden. Der Leser findet viele farbige und ausgeklügelte Bilder verschiedener Fraktale in Büchern oder im Internet. Fraktale sind nicht nur hübsch anzusehen (und geeignet, unendlich viel Zeit zu kosten, wenn man mit ihnen auf einem Computer experimentiert), sie sind auch wichtig bei der Beschreibung zahlreicher Naturphänomene.

Nach diesem Abstecher wenden wir uns wieder den grundlegenden Definitionen zu Funktionen zu.

**1.4.3 Definition (Wichtige Typen von Funktionen).** Eine Funktion  $f: X \rightarrow Y$  heißt

- injektiv, wenn aus  $x \neq y$  folgt, dass  $f(x) \neq f(y)$ ,
- surjektiv wenn es zu jedem  $y \in Y$  (mindestens) ein  $x \in X$  gibt, für das  $f(x) = y$  gilt, und

---

<sup>11</sup> Natürlich erzeugt man solche Bilder mit dem Computer, und da Computer nur eine eingeschränkte Rechengenauigkeit besitzen, kann man in Wahrheit nur eine Näherung an die Abbildung berechnen.

- bijektiv, oder eine Bijektion, wenn  $f$  sowohl injektiv als auch surjektiv ist.

In einem Pfeildiagramm einer Funktion erkennt man die verschiedenen Typen wie folgt:

- bei einer injektiven Funktion kommt bei jedem Punkt  $y \in Y$  höchstens ein Pfeil an,
- bei einer surjektiven Funktion kommt bei jedem Punkt  $y \in Y$  mindestens ein Pfeil an, und
- bei einer bijektiven Funktion, kommt bei jedem Punkt  $y \in Y$  genau ein Pfeil an.

Um hervorzuheben, dass eine Abbildung  $f: X \rightarrow Y$  injektiv ist, verwendet man zuweilen die Schreibweise

$$f: X \hookrightarrow Y.$$

Das Symbol  $\hookrightarrow$  ist eine Kombination aus dem Teilmengensymbol  $\subset$  und dem Abbildungspfeil  $\rightarrow$ . Denn wenn  $f: X \hookrightarrow Y$  eine injektive Funktion ist, dann kann man die Menge  $Z = f(X)$  als „Kopie“ der Menge  $X$  innerhalb von  $Y$  ansehen (weil ja  $f$  als Abbildung  $X \rightarrow Z$  eine Bijektion ist). Man kann sich also eine injektive Abbildung  $f: X \hookrightarrow Y$  als eine Art verallgemeinerte Teilmengenbeziehung von  $X$  in  $Y$  vorstellen.

Natürlich gibt es auch spezielle Schreibweisen für surjektive und bijektive Funktionen, doch deren Gebrauch ist noch weit weniger einheitlich als bei injektiven Funktionen. Wir werden sie nicht verwenden.

Weil wir am Zählen von Objekten interessiert sind, werden Bijektionen für uns von ganz besonderer Bedeutung sein. Denn wenn  $X$  und  $Y$  zwei Mengen sind, zwischen denen eine Bijektion  $f: X \rightarrow Y$  existiert, dann haben  $X$  und  $Y$  die gleiche Anzahl von Elementen. Sehen wir uns einmal ein ganz einfaches Beispiel für diese Vorgehensweise an (raffiniertere kommen später).

**1.4.4 Beispiel.** Wieviele Folgen der Länge 8 gibt es, die aus Ziffern zwischen 0 und 9 bestehen? Wieviele von ihnen enthalten eine gerade Anzahl ungerader Ziffern?

**Lösung.** Die Antwort auf die erste Frage ist  $10^8$ . Eine leichte Art das einzusehen ist, sich klarzumachen, dass jede Folge aus 8 Ziffern als Zahl zwischen 0 und  $10^8 - 1$  angesehen werden kann, und dass umgekehrt jede Zahl zwischen 0 und  $10^8 - 1$  im Dezimalsystem geschrieben höchstens 8 Stellen hat, sie also gegebenenfalls von links mit Nullen aufgefüllt werden kann, so dass sie eine 8-Ziffern-Folge ergibt. Dieses Vorgehen definiert eine Bijektion zwischen der Menge  $\{0, 1, \dots, 10^8 - 1\}$  und der Menge aller 8-Ziffern-Folgen.

Wahrscheinlich war diese Bijektion etwas zu einfach (oder besser: zu gewohnt) um irgendwen zu beeindrucken. Wie steht es aber mit jenen

Ziffernfolgen der Länge 8, die gerade viele ungerade Ziffern enthalten? Sei  $G$  (wie „gerade“) die Menge all dieser Folgen, und  $U$  seien alle anderen, also die mit ungerade vielen ungeraden Ziffern. Wir betrachten eine Folge  $g \in G$  und konstruieren daraus eine andere Folge  $f(g)$ , indem wir die erste Ziffer von  $g$  ändern: Aus 0 machen wir 1, aus der 1 die 2, ..., aus der 8 die 9 und aus der 9 die 0. Man prüft leicht nach, dass die neue Folge  $f(g)$  eine ungerade Anzahl ungerader Ziffern hat, dass  $f$  also eine Abbildung von  $G$  nach  $U$  ist. Aus zwei verschiedenen Folgen  $g, g' \in G$  erhalten wir mit der beschriebenen Modifikation auch zwei verschiedene Folgen  $f(g), f(g') \in U$ , also ist  $f$  injektiv. Außerdem erhalten wir jede Folge  $u \in U$  als ein  $f(g)$ , wir müssen ja nur die erste Ziffer „zurück ändern“, also 1 durch 0 ersetzen oder 2 durch 1, ..., 9 durch 8 und 0 durch 9. Also ist  $f$  auch surjektiv, mithin bijektiv und  $|G| = |U|$ . Da  $|G| + |U| = 10^8$  ist, erhalten wir als Ergebnis  $|G| = 5 \cdot 10^7$ .

□

Im nun folgenden Hilfssatz beweisen wir ein paar einfache Eigenschaften über Funktionen.

**Hilfssatz.** Seien  $f: X \rightarrow Y$  und  $g: Y \rightarrow Z$  Funktionen. Dann gilt:

- (i) Sind  $f$  und  $g$  injektiv, dann ist auch  $g \circ f$  injektiv.
- (ii) Sind  $f$  und  $g$  surjektiv, dann ist auch  $g \circ f$  surjektiv.
- (iii) Sind  $f$  und  $g$  bijektiv, dann ist auch  $g \circ f$  bijektiv.
- (iv) Zu jeder Funktion  $f: X \rightarrow Y$  kann man eine Menge  $Z$ , eine injektive Funktion  $h: Z \rightarrow Y$  sowie eine surjektive Funktion  $g: X \rightarrow Z$  finden, so dass  $f = h \circ g$ . (Das bedeutet, dass sich jede Funktion als Verknüpfung einer injektiven mit einer surjektiven Funktion schreiben lässt.)

*Beweis.* Die Teile (i), (ii) und (iii) folgen direkt aus den Definitionen. Als ein Beispiel beweisen wir (ii).

Wir müssen zeigen, dass es zu jedem  $z \in Z$  ein  $x \in X$  gibt, für das  $(g \circ f)(x) = z$  ist. Sei also  $z \in Z$  beliebig. Weil  $g$  surjektiv ist, existiert ein  $y \in Y$  mit  $g(y) = z$ . Und weil  $f$  surjektiv ist, existiert ein  $x \in X$  mit  $f(x) = y$ . Dieses  $x$  ist genau das, wonach wir suchen, denn  $(g \circ f)(x) = g(f(x)) = g(y) = z$ .

Der interessante Teil ist (iv). Sei  $Z = f(X) \subseteq Y$ . Wir definieren die Abbildungen  $g: X \rightarrow Z$  und  $h: Z \rightarrow Y$  wie folgt:

$$\begin{aligned} g(x) &= f(x) && \text{für } x \in X \\ h(z) &= z && \text{für } z \in Z. \end{aligned}$$

Nun haben  $Z$ ,  $g$  und  $h$  die gewünschten Eigenschaften:  $Z \subseteq Y$ ,  $g$  ist surjektiv,  $h$  ist injektiv und  $f = h \circ g$ . □

Ein Vorschlag: Führen Sie jetzt den Beweis für die verbliebenen zwei Teile des Satzes; das fördert das Verständnis der in diesem Abschnitt eingeführten Begriffe.

**Umkehrfunktion.** Ist  $f: X \rightarrow Y$  eine Bijektion, dann können wir eine Funktion  $g: Y \rightarrow X$  definieren durch  $g(y) = x$ , wobei  $x$  das eindeutige Element von  $X$  mit  $y = f(x)$  ist. Die so definierte Funktion  $g$  heißt die *Umkehrfunktion* von  $f$ , sie wird gewöhnlich mit  $f^{-1}$  bezeichnet. Bildlich gesprochen erhält man die Umkehrfunktion, indem man einfach die Richtung aller Pfeile umkehrt. Eine weitere äquivalente Definition der Umkehrfunktion finden Sie in Aufgabe 4. Sie sieht etwas komplizierter aus, ist von einem „höheren“ Standpunkt aus jedoch vorteilhaft.

## Aufgaben

1. Zeigen Sie: Ist  $X$  eine endliche Menge, so ist eine Funktion  $f: X \rightarrow X$  genau dann injektiv, wenn sie surjektiv ist.
2. Finden Sie ein Beispiel für:
  - (a) Eine injektive Funktion  $f: \mathbb{N} \hookrightarrow \mathbb{N}$ , die nicht surjektiv ist.
  - (b) Eine surjektive Funktion  $f: \mathbb{N} \rightarrow \mathbb{N}$ , die nicht injektiv ist.
3. Entscheiden Sie, welche der folgenden Funktionen  $\mathbb{Z} \rightarrow \mathbb{Z}$  injektiv und welche surjektiv sind:  $x \mapsto 1 + x$ ,  $x \mapsto 1 + x^2$ ,  $x \mapsto 1 + x^3$ ,  $x \mapsto 1 + x^2 + x^3$ . Ist die Antwort eine andere, wenn wir die Funktionen als Funktionen von  $\mathbb{R}$  nach  $\mathbb{R}$  auffassen? (Vielleicht wollen Sie die Graphen der Funktionen skizzieren.)
4. Zu einer Menge  $X$  definieren wir die *Identitätsabbildung*  $\text{id}_X: X \rightarrow X$  durch  $\text{id}_X(x) = x$  für alle  $x \in X$ . Sei  $f: X \rightarrow Y$  eine Funktion. Beweisen Sie:
  - (a) Es existiert genau dann eine Funktion  $g: Y \rightarrow X$  mit  $g \circ f = \text{id}_X$ , wenn  $f$  injektiv ist.
  - (b) Es existiert genau dann eine Funktion  $g: Y \rightarrow X$  mit  $f \circ g = \text{id}_Y$ , wenn  $f$  surjektiv ist.
  - (c) Es existiert genau dann eine Funktion  $g: Y \rightarrow X$ , für die sowohl  $g \circ f = \text{id}_X$  gilt als auch  $f \circ g = \text{id}_Y$ , wenn  $f$  bijektiv ist.
  - (d) Ist  $f: X \rightarrow Y$  eine Bijektion, dann sind die folgenden drei Bedingungen äquivalent für eine Funktion  $g: Y \rightarrow X$ :
    - (i)  $g = f^{-1}$ ,
    - (ii)  $g \circ f = \text{id}_X$ , und
    - (iii)  $f \circ g = \text{id}_Y$ .

5. (a) Wenn  $g \circ f$  eine surjektive Funktion ist, muss dann  $g$  surjektiv sein?  
Muss  $f$  surjektiv sein?  
(b) Wenn  $g \circ f$  eine injektive Funktion ist, muss dann  $g$  injektiv sein?  
Muss  $f$  injektiv sein?
6. Beweisen Sie, dass die folgenden zwei Eigenschaften für eine Funktion  $f: X \rightarrow Y$  äquivalent sind:  
(i)  $f$  ist injektiv.  
(ii) Für jede beliebige Menge  $Z$  und zwei beliebige verschiedene Funktionen  $g_1: Z \rightarrow X$  und  $g_2: Z \rightarrow X$  sind die Funktionen  $f \circ g_1$  und  $f \circ g_2$  ebenfalls verschieden.  
(Überlegen Sie sich zuerst, was es heißt, dass zwei Funktionen gleich sind und was es heißt, dass sie verschieden sind.)
7. Normalerweise begreift man die Anzahl der Elemente einer Menge als etwas intuitiv Gegebenes und verzichtet auf eine Definition. Wenn man sich für die logischen Grundlagen der Mathematik interessiert, definiert man die Mächtigkeit einer Menge über Bijektionen:  $|X| = n$  bedeutet, dass es eine Bijektion zwischen  $X$  und der Menge  $\{1, 2, \dots, n\}$  gibt. (Es existieren auch alternative Definitionen für die Mächtigkeit einer Menge, wir wollen uns mit dieser begnügen.)
  - (a) Beweisen Sie: Haben  $X$  und  $Y$  (bezüglich dieser Definition) die gleiche Mächtigkeit, dann existiert eine Bijektion von  $X$  nach  $Y$ .
  - (b) Beweisen Sie: Wenn  $X$  (bezüglich dieser Definition) die Mächtigkeit  $n$  hat und es eine Bijektion zwischen  $X$  und  $Y$  gibt, dann hat auch  $Y$  die Mächtigkeit  $n$ .
  - (c) \*Beweisen Sie, dass eine Menge nach dieser Definition nicht zwei verschiedene Mächtigkeiten  $m$  und  $n$ ,  $m \neq n$ , haben kann. Achten Sie darauf, nicht die intuitive Vorstellung von „Größe“ einer Menge zu benutzen, sondern nur die Definition mit der Bijektion. Gehen Sie induktiv vor.

## 1.5 Relationen

Es ist bemerkenswert, wie viele mathematische Konzepte mithilfe von Mengen und ein paar mengentheoretischen Konstruktionen ausgedrückt werden können. Das ist nicht nur bemerkenswert, es ist auch überraschend, weil es die Mengenlehre und auch das Konzept einer Menge noch nicht besonders lange gibt. Noch vor hundert Jahren waren Mengen nicht allgemein als seriöse Mathematik akzeptiert. Heute ist die Mengenlehre die Sprache der Mathematik (und der Mathematiker) geworden. Diese gemeinsame Sprache hilft, die Mathematik in ihrer ganzen Vielfalt als ein auf gemeinsamen Grundlagen ruhendes Ganzes zu begreifen.

Wir werden sehen, wie kompliziertere mathematische Konzepte mit einfachsten mengentheoretischen Mitteln realisiert werden können. Der Schlüsselbegriff der Relation,<sup>12</sup> den wir nun einführen, ist eine gemeinsame Verallgemeinerung so verschiedener Begriffe wie Äquivalenz, Funktion oder Ordnung.

**1.5.1 Definition.** Eine Relation ist eine Menge geordneter Paare.<sup>13</sup> Sind  $X$  und  $Y$  Mengen, so nennt man jede Teilmenge des kartesischen Produkts  $X \times Y$  eine Relation zwischen  $X$  und  $Y$ . Der wichtigste Spezialfall ist  $X = Y$ ; wir sprechen dann von einer Relation auf  $X$ , was also eine beliebige Teilmenge  $R \subseteq X \times X$  ist.

Wenn ein geordnetes Paar  $(x, y)$  zu einer Relation  $R$  gehört, wenn also  $(x, y) \in R$  ist, dann sagen wir,  $x$  und  $y$  stehen bezüglich  $R$  in Relation zueinander, und wir schreiben  $xRy$ .

Wir haben schon einmal Objekte als Teilmenge eines kartesischen Produkts definiert, nämlich Funktionen. Eine Funktion ist also eine spezielle Relation, bei der wir verlangen, dass jedes  $x \in X$  zu genau einem  $y \in Y$  in Relation steht. In allgemeinen Relationen kann ein  $x \in X$  zu mehreren Elementen aus  $Y$  in Relation stehen oder auch zu keinem.

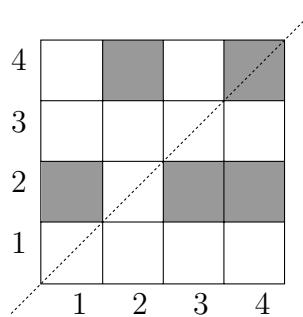
Viele Symbole, die dem Leser geläufig sind, können in diesem Sinne als Relationen aufgefasst werden. Zum Beispiel sind  $=$  und  $\geq$  beides Relationen auf der Menge  $\mathbb{N}$  der natürlichen Zahlen. Die erste besteht aus den Paaren  $(1, 1), (2, 2), (3, 3), \dots$ , die zweite aus den Paaren  $(1, 1), (2, 1), (2, 2), (3, 1), (3, 2), (3, 3), (4, 1), \dots$ . Anstatt des gewohnten  $5 \geq 2$  könnten wir also auch  $(5, 2) \in \geq$  schreiben; das werden wir natürlich in der Regel nicht tun. Wir müssten uns dann übrigens festlegen, auf welcher Menge wir die Relation  $\geq$  betrachten: Als Relation auf  $\mathbb{R}$  wäre es eine andere Menge geordneter Paare.

Interessante Beispiele für Relationen sind Verwandtschaftsverhältnisse wie „ist Mutter von“, „ist Vater von“, „ist Vetter von“. Dies sind Relationen auf der Menge aller Menschen, in der Regel wohl definiert, wenn auch im Einzelfall nicht immer leicht zu bestimmen.

Eine Relation  $R$  auf einer Menge  $X$  kann man auf (mindestens) zwei verschiedene Weisen veranschaulichen. Die erste Methode ist in Abb. 1.3 dargestellt. Die kleinen Quadrate korrespondieren zu den geordneten Paaren im kartesischen Produkt; die Quadrate, bei

<sup>12</sup>Als mathematisches Objekt; es gibt das Wort auch in der normalen Sprache.

<sup>13</sup>Um genauer zu sein könnten wir sagen eine *zweistellige Relation* (weil Paare von Elementen in Relation zueinander gesetzt werden). Man betrachtet auch  $n$ -stellige Relationen für  $n \neq 2$ .



**Abb. 1.3** Eine bildliche Darstellung der Relation  $R = \{(1, 2), (2, 1), (2, 2), (3, 2), (4, 2)\}$  auf der Menge  $\{1, 2, 3, 4\}$ .

denen die entsprechenden geordneten Paare in Relation stehen, sind markiert. Diese Sorte Bild betont die Definition einer Relation auf  $X$  und zeigt die Relation sozusagen als Ganzes.

Dieses Bild ist von der Idee her der Beschreibung einer Relation auf einer Menge  $X$  durch eine Matrix sehr ähnlich.<sup>14</sup> Eine Relation  $R$  auf einer  $n$ -elementigen Menge  $X = \{x_1, x_2, \dots, x_n\}$  lässt sich vollständig durch die  $n \times n$  Matrix  $A = (a_{ij})$  beschreiben, wobei

$$\begin{aligned} a_{ij} &= 1 && \text{wenn } (x_i, x_j) \in R \\ a_{ij} &= 0 && \text{wenn } (x_i, x_j) \notin R. \end{aligned}$$

Die Matrix  $A$  heißt *Adjazenzmatrix* der Relation  $R$ . Für die Relation in Abb. 1.3 sieht die Adjazenzmatrix zum Beispiel so aus:

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

Diese Matrix ist im Vergleich zu Abb. 1.3 um 90 Grad gedreht. Das kommt daher, dass man bei einem Matrixelement den ersten Index als Nummer der Zeile auffasst (von oben gezählt) und den zweiten Index als Spaltennummer, während man bei kartesischen Koordinaten die erste Koordinate als horizontale Position interpretiert und die zweite als vertikale (von unten gezählt). Beides sind willkürliche Konventionen,

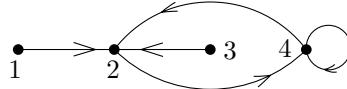
---

<sup>14</sup>Eine  $n \times m$  Matrix ist eine Tabelle mit  $n$  Zeilen und  $m$  Spalten. Im Anhang finden Sie die Definition und elementare Eigenschaften von Matrizen, sie gehören zum Stoff der linearen Algebra. Hier verwenden wir Matrizen allerdings lediglich zur Buchhaltung: Zu gegebener Zeile und Spalte können wir einen Wert aus der Tabelle ablesen.

aber es ist vernünftig, dabei zu bleiben — sonst erzeugt man eine babylonische Sprachverwirrung.

Die Adjazenzmatrix eignet sich auch dazu, Relationen auf endlichen Mengen im Computer zu speichern.

Dies ist ein weiteres Bild der gleichen Relation wie in Abb. 1.3:



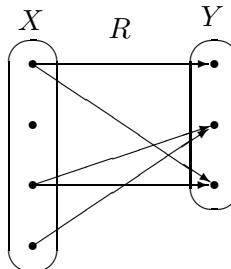
Die Punkte entsprechen den Elementen aus  $X$ . Wenn ein geordnetes Paar  $(x, y)$  zu der Relation  $R$  gehört, dann zeichnen wir einen Pfeil von  $x$  zu  $y$ :

$$x \longrightarrow y$$

und in dem Fall, dass  $x = y$  ist, eine Schlinge:



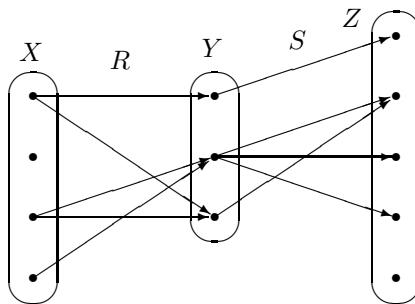
Ähnlich kann man eine Relation zwischen verschiedenen Mengen  $X$  und  $Y$  darstellen:



Diese Darstellung haben wir in Abschnitt 1.4 für Funktionen benutzt.

**Verknüpfung von Relationen.** Seien  $X, Y, Z$  Mengen, sei  $R \subseteq X \times Y$  eine Relation zwischen  $X$  und  $Y$ , und sei  $S \subseteq Y \times Z$  eine Relation zwischen  $Y$  und  $Z$ . Die *Verknüpfung der Relationen  $R$  und  $S$*  ist die Relation  $T \subseteq X \times Z$ , die wie folgt definiert ist: Für gegebenes  $x \in X$  und  $z \in Z$  gilt  $xTz$  genau dann, wenn es ein  $y \in Y$  gibt, so dass  $xRy$  und  $ySz$ . Die Verknüpfung zweier Relationen  $R$  und  $S$  wird meist mit  $R \circ S$  bezeichnet.

Die Verknüpfung von Relationen lässt sich schön mit einem Pfeildiagramm illustrieren. In der folgenden Skizze gehört ein Paar  $(x, z)$  immer dann zur Relation  $R \circ S$ , wenn man entlang der Pfeile von  $x$  (über irgendein  $y$ ) zu  $z$  gelangen kann.



Haben Sie es bemerkt? Die Verknüpfung von Relationen ist genauso definiert wie die von Funktionen, aber die Schreibweisen sind in einem wesentlichen Detail verschieden! Für Relationen wird die Verknüpfung in der Regel „von links nach rechts“ geschrieben, für Funktionen meist „von rechts nach links“. Sind  $f: X \rightarrow Y$  und  $g: Y \rightarrow Z$  Funktionen, dann schreibt man ihre Verknüpfung  $g \circ f$ , doch wenn wir  $f$  und  $g$  als Relationen auffassen, dann schreiben wir  $f \circ g$  für die gleiche Sache! Beide Schreibweisen haben einen Sinn, und eigentlich könnte man sich auf eine einheitliche Notation einigen. Die Unterschiede sind historisch bedingt, und es scheint am wenigsten Verwirrung zu stiften, wenn man das akzeptiert und es nicht zu ändern versucht. In diesem Buch werden wir fast ausschließlich Funktionen verknüpfen.

Wie bei Funktionen ist die Verknüpfung auch nicht für zwei beliebige Relationen definiert. Um zwei Relationen verknüpfen zu können müssen sie die „mittlere Menge“ (in der Definition hieß sie  $Y$ ) gemein haben. Insbesondere kann es also vorkommen, dass  $R \circ S$  definiert ist,  $S \circ R$  aber sinnlos ist! Wenn aber  $R$  und  $S$  beides Relationen auf der gleichen Menge  $X$  sind, dann ist ihre Verknüpfung stets definiert. Doch selbst in diesem Fall hängt das Resultat der Verknüpfung von der Reihenfolge ab, und im Allgemeinen ist  $R \circ S$  von  $S \circ R$  verschieden — siehe Aufgabe 2.

## Aufgaben

1. Beschreiben Sie die Relation  $R \circ R$ ; dabei steht  $R$  für
  - (a) die Gleichheitsrelation „=“ auf der Menge  $\mathbb{N}$  aller natürlichen Zahlen,
  - (b) die Relation „kleiner oder gleich“ ( $\leq$ ) auf  $\mathbb{N}$ ,
  - (c) die Relation „echt kleiner“ ( $<$ ) auf  $\mathbb{N}$ ,
  - (d) die Relation „echt kleiner“ ( $<$ ) auf der Menge  $\mathbb{R}$  aller reellen Zahlen.
2. Finden Sie zwei Relationen  $R$  und  $S$  auf einer Menge  $X$ , so dass  $R \circ S \neq S \circ R$ .
3. Zu einer gegebenen Relation  $R$  auf einer Menge  $X$  definieren wir induktiv das Symbol  $R^n$  durch  $R^1 = R$  und  $R^{n+1} = R \circ R^n$ .

- (a) Beweisen Sie: Ist  $X$  endlich und  $R$  eine Relation auf  $X$ , dann gibt es  $r, s \in \mathbb{N}$ ,  $r < s$ , so dass  $R^r = R^s$  ist.
- (b) Finden Sie eine Relation  $R$  auf einer endlichen Menge, für die  $R^n \neq R^{n+1}$  ist für jedes  $n \in \mathbb{N}$ .
- (c) Zeigen Sie, dass für unendliches  $X$  die Behauptung aus (a) nicht richtig ist (d.h. dass es (mindestens) eine Relation  $R$  auf  $X$  gibt, so dass alle Relationen  $R^n$ ,  $n \in \mathbb{N}$ , verschieden sind).
4. (a) Seien  $X = \{x_1, x_2, \dots, x_n\}$  und  $Y = \{y_1, y_2, \dots, y_m\}$  endliche Mengen, und sei  $R \subseteq X \times Y$  eine Relation. Erweitern Sie die Definition der Adjazenzmatrix auf diesen Fall.
- (b) \*Seien  $X, Y, Z$  endliche Mengen sowie  $R \subseteq X \times Y$  und  $S \subseteq Y \times Z$  Relationen, und seien  $A_R$  und  $A_S$  ihre Adjazenzmatrizen. Wenn Sie bei der Definition der Adjazenzmatrix in (a) alles richtig gemacht haben, dann sollte das Matrixprodukt  $A_R A_S$  definiert sein. Finden Sie den Zusammenhang zwischen der Verknüpfung  $R \circ S$  der beiden Relationen und dem Matrixprodukt  $A_R A_S$  heraus und beschreiben Sie ihn.
5. Beweisen Sie, dass die Verknüpfung von Relationen assoziativ ist: Sind  $R, S, T$  Relationen, so dass  $(R \circ S) \circ T$  definiert ist, dann ist auch  $R \circ (S \circ T)$  definiert und ist gleich  $(R \circ S) \circ T$ .

## 1.6 Äquivalenz und andere spezielle Relationen

Jede Sprache hat Ihren eigenen Charakter. Manche Sprachen sind vokalreich, andere fallen durch Konsonantenhäufung auf. Bei manchen ist die Grammatik einfach, bei anderen die Aussprache. Mit der Mathematik ist es ähnlich. Zwar hat ihr Formalismus einige grundlegende Eigenschaften, er ist exakt und es kommt oft auf Kleingkeiten an (manchmal vielleicht zu sehr), doch die verschiedenen Gebiete der Mathematik unterscheiden sich in Stil und Sprache. Ein Beispiel: Die Algebra steht in dem Ruf, besonders viele Definitionen und Schreibweisen zu benötigen, die noch dazu in großer Zahl an den Anfang gestellt werden, vor die Darstellung des „eigentlichen“ Themas. Viele dieser algebraischen Konzepte sind jedoch auch in anderen Gebieten von Bedeutung und gehören damit zum allgemeinen mathematischen Vokabular. Hier zeigen wir exemplarisch, wie solche Begriffe normalerweise eingeführt werden. Dieser Abschnitt behandelt spezielle Typen von Relationen und gehört damit im Wesentlichen zur Algebra.

Funktionen sind für uns Relationen mit besonderen Eigenschaften. Um auch Äquivalenzen und Ordnungen als besondere Relationen charakterisieren zu können, identifizieren wir nun vier Eigenschaften, die eine Relation haben kann, oder auch nicht. Jede dieser

Eigenschaften hat einen eigenen Namen, und zusammen ermöglichen sie, die neben den Funktionen wichtigsten Relationen zu definieren.

**1.6.1 Definition.** Wir nennen eine Relation  $R$  auf einer Menge  $X$

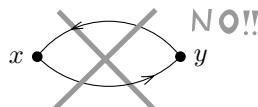
- reflexiv, wenn  $xRx$  für alle  $x \in X$ ;
- symmetrisch, wenn aus  $xRy$  folgt, dass  $yRx$  ist, für alle  $x, y \in X$ ;
- antisymmetrisch<sup>15</sup> wenn  $xRy$  und  $yRx$  nur für  $x = y$  gleichzeitig zutreffen;
- transitiv, wenn aus  $xRy$  und  $yRz$  folgt, dass  $xRz$  ist, für alle  $x, y, z \in X$ .

In einer Zeichnung wie in Abb. 1.3 erkennt man die Reflexivität einer Relation daran, dass sie alle Quadrate auf der Diagonalen (durch die gepunktete Linie angedeutet) enthält. In einem Pfeildiagramm hängt bei einer reflexiven Relation an jedem Punkt eine Schlinge.

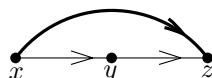
Bei symmetrischen Relationen ist die schachbrettartige Darstellung (wie in Abb. 1.3) achsensymmetrisch zu den Diagonalen. In einem Pfeildiagramm hat jeder Pfeil einen „Zwilling“, der in die andere Richtung zeigt:



Ganz anders bei antisymmetrischen Relationen, dort ist diese Situation ausgeschlossen:



Die Transitivität lässt sich besser am Pfeildiagramm erklären. Wenn es die Pfeile  $x \rightarrow y$  und  $y \rightarrow z$  gibt, dann muss es auch den Pfeil  $x \rightarrow z$  geben:



Die Pfeilchen-Bilder zur Illustration von Reflexivität, Symmetrie, Antisymmetrie und Transitivität nutzen aus, dass diese Eigenschaften im Prinzip leicht nachzuprüfen sind, weil sie „lokal“ sind, d.h. sich jeweils nur auf Paare oder Tripel von Elementen beziehen.

---

<sup>15</sup>Manchmal nennt man diese Eigenschaft auch *schwach antisymmetrisch*, während bei einer *stark antisymmetrischen* Relation  $xRy$  und  $yRx$  nie gleichzeitig zutreffen, d.h.  $xRx$  ist ausgeschlossen.

Eine alternative Beschreibung dieser Eigenschaften verwendet die Verknüpfungsoperation für Relationen (siehe Abschnitt 1.5) sowie die beiden folgenden Begriffe:

Die *inverse Relation*  $R^{-1}$  einer gegebenen Relation  $R$  ist  $R^{-1} = \{(y, x) : (x, y) \in R\}$ . Man dreht also einfach alle Pfeile in  $R$  in die entgegengesetzte Richtung.

Das Symbol  $\Delta_X$  bezeichne die kleinste reflexive Relation auf einer Menge  $X$ :

$$\Delta_X = \{(x, x) : x \in X\}.$$

Die Relation  $\Delta_X$  nennen wir hier die *Diagonale* (auf der Menge  $X$ ). Dieser Name ist durch die Adjazenzmatrix–Darstellung von Relationen motiviert (siehe Abschnitt 1.5). Bei  $\Delta_X$  handelt es sich um die Gleichheitsrelation, die zugleich eine Funktion ist und in dem Zusammenhang *Identität* genannt wird.

Nach diesen Vorbereitungen können wir Definition 1.6.1 kompakter formulieren:

- (1)  $R$  ist reflexiv, wenn  $\Delta_X \subseteq R$ .
- (2)  $R$  ist symmetrisch, wenn  $R = R^{-1}$ .
- (3)  $R$  ist antisymmetrisch, wenn  $R \cap R^{-1} \subseteq \Delta_X$ .
- (4)  $R$  ist transitiv, wenn  $R \circ R \subseteq R$ .

Nun sind wir so weit, Äquivalenz, Ordnung und lineare Ordnung zu definieren.

### 1.6.2 Definition.

- Eine Relation  $R$  auf einer Menge  $X$  heißt eine Äquivalenzrelation auf  $X$ , wenn sie reflexiv, symmetrisch und transitiv ist.
- Eine Relation  $R$  auf einer Menge  $X$  heißt eine Ordnung auf  $X$ , wenn sie reflexiv, antisymmetrisch und transitiv ist.
- Eine Relation  $R$  auf einer Menge  $X$  heißt eine lineare Ordnung (auch totale Ordnung) auf  $X$ , wenn sie eine Ordnung ist mit der zusätzlichen Eigenschaft  $R \cup R^{-1} = X \times X$  (mit anderen Worten, für je zwei Elemente  $x, y \in X$  gilt mindestens eine der Beziehungen  $xRy$  oder  $yRx$ ).

Auf den ersten Blick mag der Unterschied zwischen diesen drei Begriffen gering und unbedeutend erscheinen. Doch der Eindruck täuscht, und wir nutzen die Gelegenheit, Ihnen einzuschärfen: In einer mathematischen Definition zählt jedes Wort. Die Begriffe Äquivalenz und Ordnung sind in Wahrheit so verschieden, dass sie für

gewöhnlich getrennt behandelt werden. So wollen auch wir vorgehen: Im Rest dieses Abschnitts untersuchen wir Äquivalenzrelationen, Ordnungen kommen später dran, in Kapitel 2.

Um ein Gefühl für die Bedeutung dieser Begriffe zu bekommen, geben wir zunächst einige Beispiele; einige werden später genauer diskutiert. Wir betrachten drei Relationen auf der Menge  $\mathbb{N}$  aller natürlichen Zahlen:

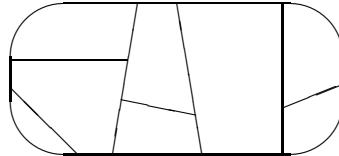
- Die Relation  $R$ , bei der  $xRy$  ist, wenn  $x - y$  eine gerade Zahl ist, ist eine Äquivalenzrelation (aber keine Ordnung).
- Die Relation  $|$ , bei der  $x|y$  ist, wenn  $x$  ein Teiler von  $y$  ist, d.h. es gibt eine natürliche Zahl  $q$  mit  $qx = y$ , ist eine Ordnung (aber keine Äquivalenzrelation und keine lineare Ordnung).
- Die Relation  $\leq$ , bei der  $x \leq y$  die übliche Bedeutung hat, d.h. dass die Zahl  $x$  kleiner oder gleich  $y$  ist, ist eine lineare Ordnung (und damit auch eine Ordnung, aber keine Äquivalenzrelation).

Wir möchten Sie ausdrücklich ermuntern, im Detail nachzuvollziehen, dass diese drei Relationen die jeweiligen Bedingungen in Definition 1.6.2 erfüllen.

**Äquivalenzrelationen.** Der Sinn des Begriffs der Äquivalenz ist, in der jeweiligen Situation auszudrücken, welche Objekte „vom gleichen Typ“ sind. Das Konzept der Äquivalenzrelation ist eine Verallgemeinerung von Begriffen, die Gleichheit, Isomorphie, Ähnlichkeit usw. ausdrücken. Äquivalenzrelationen bezeichnet man oft mit Symbolen, die so ähnlich wie  $=$  aussehen, z.B.  $\equiv$ ,  $\simeq$ ,  $\approx$ ,  $\cong$ . Vielleicht möchten Sie jetzt ein Weilchen darüber nachdenken, weshalb die drei Eigenschaften Reflexivität, Symmetrie und Transitivität sinnvoll sind für eine Relation, die so etwas wie „vom gleichen Typ sein“ ausdrücken soll.

Wir wollen uns einige Beispiele aus der Geometrie ansehen. Mit  $X$  bezeichnen wir die Menge aller Dreiecke in der Ebene. Eine Möglichkeit ist, zwei Dreiecke äquivalent zu nennen, wenn sie kongruent sind (d.h. sie können mit Verschiebungen und Drehungen ineinander überführt werden). Eine zweite Möglichkeit ist, zwei Dreiecke äquivalent zu nennen, wenn sie ähnlich sind (d.h. sie können mit Verschiebungen und Drehungen sowie Streckung oder Stauchung ineinander überführt werden; mit anderen Worten, die entsprechenden Winkel sind gleich). Eine dritte Äquivalenzrelation erhalten wir, wenn wir jedes Dreieck nur zu sich selbst äquivalent nennen.

Auch wenn eine Äquivalenzrelation  $R$  auf einer Menge  $X$  eine spezielle Relation ist und wir sie also mit den beiden oben beschriebenen Methoden darstellen können, werden wir meistens ein Bild wie das folgende verwenden:



Der Schlüssel zu dieser Sorte Zeichnung ist der Begriff der *Äquivalenzklasse*. Sei  $R$  eine Äquivalenzrelation auf einer Menge  $X$  und sei  $x$  ein Element von  $X$ . Mit  $R[x]$ , bezeichnen wir die Menge aller Elemente  $y \in X$ , die zu  $x$  äquivalent sind, also  $R[x] = \{y \in X : xRy\}$ .  $R[x]$  heißt die *Äquivalenzklasse von  $x$  unter der Relation  $R$* .

**1.6.3 Hilfssatz.** Für jede Äquivalenzrelation  $R$  auf  $X$  gilt

- (i)  $R[x] \neq \emptyset$  für alle  $x \in X$ .
- (ii) Für je zwei Elemente  $x, y \in X$  ist entweder  $R[x] = R[y]$  oder  $R[x] \cap R[y] = \emptyset$ .
- (iii) Eine Äquivalenzrelation  $R$  ist durch ihre Äquivalenzklassen eindeutig bestimmt.

Bevor wir zum Beweis schreiten, sollten wir klären, was (iii) konkret bedeutet. Gemeint ist: Sind  $R$  und  $S$  zwei Äquivalenzrelationen auf der gleichen Menge  $X$ , und gilt für jedes  $x \in X$  die Gleichheit  $R[x] = S[x]$ , dann ist  $R = S$ .

*Beweis.* Wir müssen nur die drei Bedingungen für Äquivalenzrelationen anwenden.

- (i) Die Menge  $R[x]$  enthält  $x$ , weil  $R$  eine reflexive Relation ist.
- (ii) Seien  $x, y$  zwei Elemente. Wir unterscheiden zwei Fälle:
  - (a) Wenn  $xRy$  gilt, dann wollen wir  $R[x] = R[y]$  beweisen. Wir zeigen zunächst  $R[x] \subseteq R[y]$ . Sei  $z \in R[x]$ , dann gilt  $xRz$  (nach Definition von  $R[x]$ ), dann wissen wir, dass auch  $zRx$  (wegen der Symmetrie von  $R$ ) und deshalb gilt  $zRy$  (wegen der Transitivität von  $R$ ) und also  $yRz$  (wieder wegen der Symmetrie). Daher gilt auch  $z \in R[y]$ . Wir haben also  $R[x] \subseteq R[y]$  gezeigt. Jetzt wenden wir noch einmal die Symmetrie an und erhalten, dass aus  $xRy$  stets  $R[x] = R[y]$  folgt.

- (b) Wenn  $xRy$  nicht gilt, dann zeigen wir, dass  $R[x] \cap R[y] = \emptyset$ , und zwar mit einem Widerspruchsbeweis. Angenommen, es gibt ein  $z \in R[x] \cap R[y]$ , dann ist  $xRz$  und  $zRy$  (wieder haben wir die Symmetrie ausgenutzt), und also  $xRy$  (weil  $R$  transitiv ist). Das ist aber ein Widerspruch zu unserer Annahme oben.
- (iii) Dieser Teil gilt, weil die Äquivalenzklassen die Relation  $R$  wie folgt bestimmen:

$$xRy \text{ genau dann, wenn } \{x, y\} \subseteq R[x]. \quad \square$$

Dieser Hilfssatz garantiert, dass die Äquivalenzklassen einer Äquivalenzrelation eine *Partition* der Menge  $X$  bilden, d.h. dass sie disjunkte Teilmengen von  $X$  sind und dass ihre Vereinigung  $X$  ist. Umgekehrt bestimmt jede Partition von  $X$  eine eindeutige Äquivalenzrelation auf  $X$ . Das bedeutet, es gibt eine bijektive Abbildung zwischen der Menge der Äquivalenzrelationen auf  $X$  und der Menge aller Partitionen von  $X$ . Deshalb kann man eine Äquivalenzrelation durch die zugehörige Partition darstellen – wie im Bild oben.

## Aufgaben

1. Wie erkennen Sie Reflexivität, Symmetrie und Transitivität einer Relation anhand ihrer Adjazenzmatrix?
2. \*Zeigen Sie, dass für eine Relation  $R$  auf einer Menge  $X$  genau dann  $R \circ R^{-1} = \Delta_X$  gilt, wenn  $R$  reflexiv und antisymmetrisch ist.
3. Beweisen Sie, dass eine Relation  $R$  genau dann transitiv ist, wenn  $R \circ R \subseteq R$ .
4. (a) Zeigen Sie: Für jede Relation  $R$  ist die Relation  $T = R \cup R \circ R \cup R \circ R \circ R \cup \dots$  (die Vereinigung aller wiederholten Verknüpfungen von  $R$  mit sich selbst) transitiv.  
 (b) Zeigen Sie: Jede transitive Relation, die  $R$  als Teilmenge enthält, enthält auch  $T$ .  
 (c) Zeigen Sie: Ist  $|X| = n$ , dann ist  $T = R \cup R \circ R \cup \dots \cup \underbrace{R \circ R \circ \dots \circ R}_{(n-1)\times}$

*Bemerkung.* Die Relation  $T$  aus (a) und (b) ist die kleinste transitive Relation, die  $R$  enthält;  $T$  heißt der *transitive Abschluss* von  $R$ .

5. Seien  $R$  und  $S$  zwei beliebige Äquivalenzrelationen auf einer Menge  $X$ . Entscheiden Sie, welche der folgenden Relationen dann ebenfalls Äquivalenzrelationen sein müssen (wenn ja, beweisen Sie, dass es so ist; wenn nein, geben Sie ein Gegenbeispiel).

- (a)  $R \cap S$   
 (b)  $R \cup S$   
 (c)  $R \setminus S$   
 (d)  $R \circ S$ .
6. Beschreiben Sie alle Relationen auf einer Menge  $X$ , die zugleich Äquivalenzrelation und Ordnung sind.
7. Gegeben seien zwei beliebige Ordnungen  $R$  und  $S$  auf einer Menge  $X$ . Entscheiden Sie, welche der folgenden Relationen auf jeden Fall Ordnungen sind:
- (a)  $R \cap S$   
 (b)  $R \cup S$   
 (c)  $R \setminus S$   
 (d)  $R \circ S$ .
8. (a) Angenommen  $R$  ist eine transitive Relation auf der Menge  $\mathbb{Z}$  der ganzen Zahlen, und wir wissen, dass für je zwei ganze Zahlen  $a, b \in \mathbb{Z}$  mit  $|a - b| = 2$  die Relation  $aRb$  erfüllt ist. Ist *jedes*  $R$ , dass diese Bedingung erfüllt, notwendig eine Äquivalenzrelation? (Bedenken Sie, dass auch solche Zahlenpaare in  $R$  sein könnten, die nicht durch die gegebenen Bedingungen dazu gezwungen sind!)
- (b) Angenommen  $R$  ist eine transitive Relation auf  $\mathbb{Z}$  und wir wissen, dass für je zwei Zahlen  $a, b \in \mathbb{Z}$ , mit  $|a - b| \in \{3, 4\}$  die Relation  $aRb$  gilt. Ist dann  $R$  notwendig eine Äquivalenzrelation?
9. Eine Äquivalenzrelation  $\sim$  auf der Menge  $\mathbb{Z}$  heißt eine *Kongruenzrelation*, wenn die folgende Bedingung für alle  $a, x, y \in \mathbb{Z}$  gilt: Ist  $x \sim y$ , dann ist auch  $a + x \sim a + y$ .
- (a) Sei  $q \neq 0$  eine ganze Zahl. Wir definieren eine Relation  $\equiv_q$  auf  $\mathbb{Z}$ , indem wir  $x \equiv_q y$  setzen, wenn  $q$  ein Teiler von  $x - y$  ist. Prüfen Sie, dass  $\equiv_q$  eine Kongruenzrelation ist.
- (b) \*Beweisen Sie, dass jede Kongruenzrelation auf  $\mathbb{Z}$  entweder von der Form  $\equiv_q$  ist (für irgendein  $q$ ) oder die Gleichheitsrelation  $\{(x, x) : x \in \mathbb{Z}\}$ .
- (c) Wenn wir die Bedingung „ $a + x \sim a + y$ “ in der Definition einer Kongruenzrelation durch „ $ax \sim ay$ “ ersetzen würden, wäre die Behauptung (a) dann immer noch wahr? \*Und wie stünde es um die Behauptung in (b)?

# 2

# Ordnungen

---

Keine Frage, dass der Leser mit der Ordnung der natürlichen Zahlen (sowie der anderen Zahlbereiche) nach der Größe vertraut ist (die „ganz normale“ Ordnung). Diese Ordnung ist eine Relation, sie sagt etwas über Paare von Zahlen aus. Gewöhnlich verwendet man für sie das Zeichen „ $\leq$ “ („kleiner oder gleich“). Auch auf anderen Mengen kann man Relationen definieren, die wesentliche Eigenschaften mit der gewohnten Ordnung der natürlichen Zahlen gemein haben. So wie zuvor die Äquivalenzrelationen werden wir Ordnungsrelationen durch drei Eigenschaften definieren; dann können wir auf jeder Menge Ordnungen definieren, z.B. auf der Menge aller Worte in einer bestimmten Sprache, und zwar ganz verschiedene, auch völlig verrückte Ordnungen.

Die allgemeine Definition einer Ordnungsrelation haben wir bereits in Definition 1.6.1 eingeführt: Eine Relation  $R$  heißt eine Ordnung, wenn sie reflexiv, antisymmetrisch und transitiv ist. Ergänzend bemerken wir, dass für eine Menge  $X$  zusammen mit einer Ordnungsrelation  $R$  auf  $X$  das Paar  $(X, R)$  als *geordnete Menge* bezeichnet wird.

Geordnete Mengen haben zahlreiche interessante Eigenschaften. Einige erwähnen wir in diesem Kapitel, andere werden uns später begegnen, vor allem in Kapitel 7.

## 2.1 Ordnungen und wie man sie zeichnen kann

Wir beginnen mit einigen Bemerkungen zur Schreibweise. Für Ordnungen verwendet man häufig die Zeichen  $\preceq$  und  $\leq$ . Das erste ist vor allem dann nützlich, wenn wir eine Ordnung der natürlichen Zahlen verwenden wollen, welche nicht die natürliche ist, oder allgemeiner wenn wir auf einer Menge zwei verschiedene Ordnungen zugleich betrachten.

Wenn wir eine Ordnung  $\preceq$  haben, dann können wir von ihr die „strikte Ungleichheit“,  $\prec$ , wie folgt ableiten:  $a \prec b$  genau dann, wenn  $a \preceq b$  und  $a \neq b$ . Des Weiteren können wir die „umgekehrte Ordnung“  $\succeq$  erklären:  $a \succeq b$  genau dann, wenn  $b \preceq a$ .

**Lineare Ordnungen und Halbordnungen.** Wir erinnern uns: Eine Relation  $R$  heißt lineare Ordnung, wenn  $R$  eine Ordnung ist, in der je zwei Elemente  $x, y$  vergleichbar sind, d.h.  $xRy$  oder  $yRx$  gilt.

Um zu betonen, dass wir von einer Ordnungsrelation sprechen, die nicht unbedingt linear zu sein braucht, benutzen wir auch die Namen *Halbordnung* oder *partielle Ordnung*. Mit einer partiellen Ordnung meinen wir also genau das Gleiche wie mit einer Ordnung (ohne weitere Adjektive), sie kann auch linear sein. Analog dazu gebraucht man das Wort *partiell geordnete Menge*. Als Abkürzung für dieses lange Wort hat sich das Kunstwort *Poset* eingebürgert. Es ist vom englischen Ausdruck *partially ordered set* abgeleitet.

**Beispiele.** Wir haben schon verschiedene Beispiele geordneter Mengen erwähnt; das waren  $(\mathbb{N}, \leq)$ ,  $(\mathbb{R}, \leq)$  und ähnliche, wobei  $\leq$  für die gewohnte Ordnung steht.

Man prüft leicht nach, dass, wenn  $R$  eine Ordnung auf einer Menge  $X$  ist und wenn  $Y \subseteq X$  eine Teilmenge von  $X$  ist, die Relation  $R \cap Y^2$  (die Einschränkung von  $R$  auf  $Y$ ) eine Ordnung auf  $Y$  ist. Wir ordnen die Elemente von  $Y$  genauso wie vorher und lassen die anderen einfach weg. So erhalten wir viele weitere Beispiele für geordnete Mengen, nämlich verschiedene Teilmengen der reellen Zahlen mit der gewohnten Ordnung. Dies erweist sich als ein recht allgemeines Beispiel für linear geordnete Mengen, wie Sie in Aufgabe 2.3.6 sehen werden.

Worte sind im Lexikon alphabetisch sortiert; diese Idee wird bei der *lexikographischen Ordnung* aufgegriffen. Zunächst betrachten wir den Spezialfall  $X = \mathbb{N} \times \mathbb{N}$ , die Menge aller geordneten Paare  $(a_1, a_2)$  natürlicher Zahlen. Wir definieren die lexikographische Ordnung  $\leq_{\text{lex}}$  auf  $X$  wie folgt:  $(a_1, a_2) \leq_{\text{lex}} (b_1, b_2)$ , wenn entweder  $a_1 < b_1$  ist, oder wenn  $a_1 = b_1$  und  $a_2 \leq b_2$ . Für die allgemeine Definition seien  $(X_1, \leq_1), (X_2, \leq_2), \dots, (X_n, \leq_n)$  irgendwelche linear geordneten Mengen, dann definieren wir die lexikographische Ordnung  $\leq_{\text{lex}}$  auf dem kartesischen Produkt  $X_1 \times X_2 \times \dots \times X_n$  so:

$$(a_1, a_2, \dots, a_n) \leq_{\text{lex}} (b_1, b_2, \dots, b_n)$$

gelte, wenn  $(a_1, a_2, \dots, a_n) = (b_1, b_2, \dots, b_n)$ , oder wenn es einen Index  $i \in \{1, 2, \dots, n\}$  gibt, so dass  $a_j = b_j$  für alle  $j < i$ , aber  $a_i <_i b_i$ .

Es ist einsichtig, dass die alphabetische Ordnung der Worte im Lexikon in diesem Sinne eine lexikographische Ordnung ist, auch wenn bei genauerer Betrachtung eine Reihe von Komplikationen auftreten, beispielsweise sind nicht alle Worte gleich lang. Und dann gibt es noch Feinheiten wie die, dass man „van Beethoven“ unter B findet.

**Beispiele für Halbordnungen.** Wie sehen Ordnungen aus, die nicht linear sind? Ein Beispiel ist die Relation  $\Delta_X = \{(x, x) : x \in X\}$  (die Gleichheitsrelation oder Diagonale). Sie erfüllt die Kriterien für eine Ordnung, ist jedoch für  $|X| > 1$  keine lineare Ordnung.

Nun kommen wir zu interessanteren Halbordnungen.

**2.1.1 Beispiel.** Nehmen wir einmal an, wir wollen einen Kühlschrank kaufen. Wir könnten uns die unüberschaubare Fülle verschiedener Modelle durch eine mathematische Abstraktion vereinfachen, indem wir lediglich auf drei objektive Daten achten, nämlich auf den Preis, auf den Stromverbrauch und auf die Größe des Innenraums. Wenn wir zwei Modelle vergleichen, von denen das erste teurer ist, mehr Strom verbraucht und außerdem weniger hineinpasst, dann stufen wir den zweiten als besser ein — eine deutliche Mehrheit der Kühlschränkäufer würde wohl zustimmen. Andere Situationen sind nicht so deutlich, z.B. wenn das eine Modell kleiner, dafür aber billiger ist als das andere, oder wenn das eine Modell zwar teurer ist, dafür aber weniger Strom verbraucht.

Diese Relation „eindeutig schlechter sein“ (bezeichnen wir sie mit  $\preceq$ ) ist also eine partielle Ordnung auf der Menge aller Kühlschrankmodelle, oder mathematisch gesehen auf der Menge aller Tripel  $(p, s, i)$  reeller Zahlen ( $p$  steht für den Preis,  $s$  für den Stromverbrauch und  $i$  für die Größe des Innenraums):

$$(p_1, s_1, i_1) \preceq (p_2, s_2, i_2) \text{ genau dann wenn} \\ p_1 \geq p_2, s_1 \geq s_2, \text{ und } i_1 \leq i_2. \quad (2.1)$$

Das nächste Beispiel haben wir bereits angesprochen:

**2.1.2 Beispiel.** Für natürliche Zahlen  $a, b$  bedeutet das Symbol  $a|b$ , dass  $a$  ein Teiler von  $b$  ist. Mit anderen Worten, es gibt eine natürliche Zahl  $c$ , so dass  $b = ac$ . Die Relation „|“ ist eine partielle Ordnung auf  $\mathbb{N}$ . Der Aufforderung, dies nachzuprüfen, sind fleißige Leser bereits oben gefolgt.

**2.1.3 Beispiel.** Sei  $X$  eine Menge. Die Teilmengenrelation „ $\subseteq$ “ ist eine partielle Ordnung auf der Menge  $2^X$  aller Teilmengen von  $X$ .

**Geordnete Mengen zeichnen.** Ordnungen auf endlichen Mengen kann man mit Pfeildiagrammen veranschaulichen, so wie jede andere Relation auf einer endlichen Menge. In der Regel wird so ein Pfeildiagramm aber sehr viele Pfeile enthalten, eine lineare Ordnung von 10 Elementen hätte zum Beispiel  $10 + 9 + \dots + 1 = 55$  Pfeile und Schlingen. Einige der Pfeile kann man jedoch aus der Transitivität erschließen: wenn wir  $x \preceq y$  und  $y \preceq z$  wissen, dann ist auch  $x \preceq z$ , also können wir den Pfeil von  $x$  nach  $z$  weglassen. Wir brauchen auch nicht die Schlingen einzuziehen, weil wir wissen, dass die sowieso da sind. In endlichen Ordnungen ist die ganze Information schon durch die Relation „unmittelbarer Vorgänger“ gegeben, die wir jetzt definieren wollen.

Sei  $(X, \preceq)$  eine geordnete Menge. Wir nennen ein Element  $x \in X$  einen *unmittelbaren Vorgänger* eines Elements  $y \in X$ , wenn gilt:

- $x \prec y$  und
- es gibt kein  $t \in X$  mit  $x \prec t \prec y$ .

Für die Dauer des nächsten Absatzes wollen wir diese Relation „unmittelbarer Vorgänger“ mit  $\triangleleft$  bezeichnen.

Die Behauptung, eine Ordnung  $\preceq$  könne schon aus der Kenntnis der unmittelbaren Vorgänger ( $\triangleleft$ ) rekonstruiert werden, lässt sich wie folgt präzisieren:

**2.1.4 Hilfssatz.** Sei  $(X, \preceq)$  eine endliche geordnete Menge und sei  $\triangleleft$  die zugehörige Relation „unmittelbarer Vorgänger“. Für irgend zwei Elemente  $x, y \in X$  gilt genau dann  $x \prec y$ , wenn es eine Kette von Elementen  $x_1, x_2, \dots, x_k \in X$  gibt, so dass  $x \triangleleft x_1 \triangleleft \dots \triangleleft x_k \triangleleft y$  ist (wobei  $k = 0$  nicht ausgeschlossen ist, das hieße dann  $x \triangleleft y$ ).

*Beweis.* Die eine Richtung ist einfach: Wenn  $x \triangleleft x_1 \triangleleft \dots \triangleleft x_k \triangleleft y$  ist, dann ist auch  $x \preceq x_1 \preceq \dots \preceq x_k \preceq y$  (weil die Relation „unmittelbarer Vorgänger“ in der Ordnungsrelation enthalten ist) und wegen der Transitivität von  $\preceq$  gilt dann  $x \preceq y$ .

Die andere Richtung ist auch nicht besonders schwer, wir zeigen sie induktiv. Dazu formulieren wir die Aussage noch einmal neu (auf Induktion zurechtgeschnitten):

**Lemma.** Seien  $x, y \in X$ ,  $x \prec y$ , zwei Elemente, für die es höchstens  $n$  Elemente  $t \in X$  gibt, die  $x \prec t \prec y$  erfüllen (d.h. die „zwischen“  $x$  und  $y$  liegen). Dann gibt es  $x_1, x_2, \dots, x_k \in X$  so dass  $x \triangleleft x_1 \triangleleft \dots \triangleleft x_k \triangleleft y$ . Für  $n = 0$  bedeutet die Voraussetzung in diesem Lemma, dass es kein  $t$  gibt, für das  $x \prec t \prec y$  ist, dass also  $x \triangleleft y$  ist. Das bedeutet, dass die Aussage stimmt (mit  $k = 0$ ).

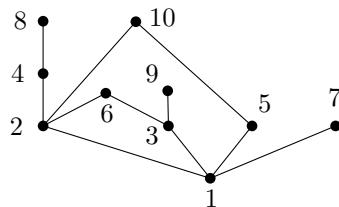
Nehmen wir nun an, das Lemma ist richtig für alle  $n$  bis zu einem

$n_0$ . Wir haben nun  $x, y \in X$  mit  $x \prec y$ , so dass die Menge  $M_{xy} = \{t \in X: x \prec t \prec y\}$  die Mächtigkeit  $n = n_0 + 1$  hat. Wir wählen ein Element  $u \in M_{xy}$  aus und betrachten die Mengen  $M_{xu} = \{t \in X: x \prec t \prec u\}$  und  $M_{uy}$ . Aus der Transitivität von  $\prec$  folgt, dass  $M_{xu} \subset M_{xy}$  ist und  $M_{uy} \subset M_{xy}$ . Sowohl  $M_{xu}$  als auch  $M_{uy}$  haben mindestens ein Element weniger als  $M_{xy}$  (weil  $u \notin M_{xu}$ ,  $u \notin M_{uy}$ ) und nach Induktionsvoraussetzung finden wir Elemente  $x_1, \dots, x_k$  und  $y_1, \dots, y_\ell$  derart, dass  $x \triangleleft x_1 \triangleleft \dots \triangleleft x_k \triangleleft u$  und  $u \triangleleft y_1 \triangleleft \dots \triangleleft y_\ell \triangleleft y$  gilt. Indem wir diese beiden „Ketten“ aneinanderfügen, erhalten wir die gewünschte Folge, die  $x$  und  $y$  verbindet.  $\square$

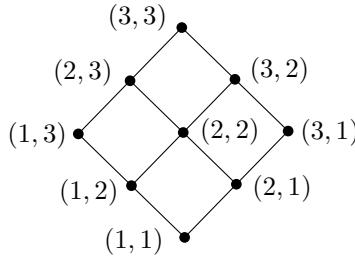
Nach obigem Hilfssatz genügt es, die Relation „unmittelbarer Vorgänger“ zu zeichnen. Wenn wir dann noch die Konvention beachten, dass alle Pfeile im Diagramm nach oben gerichtet sind (das bedeutet wenn  $x \prec y$ , dann ist  $y$  weiter oben als  $x$ ), dann brauchen wir noch nicht einmal die Pfeilspitzen einzuziehen — es genügt dann, Linien zwischen den Punkten zu zeichnen. Ein solches Bild einer partiellen Ordnung heißt *Hasse-Diagramm*. Das folgende Bild zeigt eine lineare Ordnung auf sieben Elementen, etwa  $(\{1, 2, \dots, 7\}, \leq)$ :



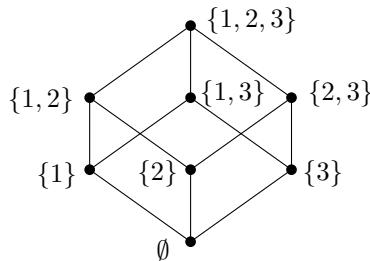
Die nächste Figur zeigt die Menge  $\{1, 2, \dots, 10\}$ , geordnet mit der Teilbarkeitsrelation (siehe Beispiel 2.1.2):



In der nächsten Abbildung sehen wir ein Hasse-Diagramm der Menge  $\{1, 2, 3\} \times \{1, 2, 3\}$ , wobei die Ordnung  $\preceq$  durch die folgende Regel gegeben ist:  $(a_1, b_1) \preceq (a_2, b_2)$  genau dann wenn  $a_1 \leq a_2$  und  $b_1 \leq b_2$ .



Zum Abschluss zeigen wir noch ein Hasse-Diagramm einer Potenzmenge: So stellt sich ein Mathematiker die Menge aller Teilmengen von  $\{1, 2, 3\}$ , geordnet durch Inklusion, vor:



Weitere Beispiele (und Konzepte) bezüglich Posets finden sich in den Aufgaben.

## Aufgaben

1. Überprüfen Sie, dass die Relation (2.1) in Beispiel 2.1.1 wirklich eine Ordnung definiert.
2. \*Sei  $R$  eine Relation auf einer Menge  $X$ , so dass es keine endliche Folge  $x_1, x_2, \dots, x_k$  von Elementen aus  $X$  gibt, für die  $x_1Rx_2, x_2Rx_3, \dots, x_{k-1}Rx_k, x_kRx_1$  ist (so ein  $R$  heißt *azyklisch*). Zeigen Sie, dass es eine Ordnung  $\preceq$  auf  $X$  gibt, für die  $R \subseteq \preceq$  ist. Wenn es Ihnen hilft, dann können Sie annehmen, dass  $X$  endlich ist.
3. Zeigen Sie, dass Hilfssatz 2.1.4 für unendliche Mengen nicht gilt.
4. Zwei Posets  $(X, \leq)$  und  $(Y, \preceq)$  heißen *isomorph*,<sup>1</sup> wenn es eine Bijektion  $f: X \rightarrow Y$  gibt, so dass für alle  $x, y \in X$  genau dann  $x \leq y$  gilt, wenn  $f(x) \preceq f(y)$ .
  - (a) Zeichnen Sie Hasse-Diagramme für alle nicht isomorphen Posets auf drei Elementen (d.h. für jeden Isomorphietyp eines).

---

<sup>1</sup>aus dem Griechischen: von gleicher Gestalt; die beiden Posets „sehen als Ordnungen gleich aus“.

- (b) Zeigen Sie, dass je zwei lineare Ordnungen auf  $n$  Elementen isomorph sind. (Eine andere Sprechweise dafür ist, dass es „bis auf Isomorphie“ nur eine solche Ordnung gibt.)
- (c) Finden Sie zwei nicht isomorphe lineare Ordnungen auf der Menge der natürlichen Zahlen.
- (d) Finden Sie unendlich viele nicht isomorphe lineare Ordnungen auf  $\mathbb{N}$ ? \*Für Leser, die etwas über die Mächtigkeit unendlicher Mengen wissen: Überabzählbar viele?

## 2.2 Ordnungen und lineare Ordnungen

Jede lineare Ordnung ist auch eine Halbordnung. Die Umkehrung („jede Halbordnung ist linear“) ist offenbar falsch, wie wir in mehreren Beispielen gesehen haben. Es gilt jedoch der folgende wichtige Satz:

**2.2.1 Satz.** *Sei  $(X, \preceq)$  ein endliches Poset. Dann existiert eine lineare Ordnung  $\leq$  auf  $X$ , so dass aus  $x \preceq y$  auch  $x \leq y$  folgt.*

Jede Halbordnung lässt sich also zu einer linearen Ordnung erweitern, die dann als *lineare Erweiterung* der Halbordnung bezeichnet wird.

Bevor wir Satz 2.2.1 beweisen, führen wir noch einen wichtigen Begriff ein.

**2.2.2 Definition.** *Sei  $(X, \preceq)$  eine geordnete Menge. Ein Element  $a \in X$  heißt minimales Element von  $(X, \preceq)$ , wenn es kein  $x \in X$  mit der Eigenschaft  $x \prec a$  gibt. Ein maximales Element  $a$  ist analog definiert (es gibt kein  $x \succ a$ ).*

Es gilt:

**2.2.3 Satz.** *Jedes endliche Poset  $(X, \preceq)$  hat mindestens ein minimales Element.*

**Beweis.** Wir wählen ein beliebiges  $x_0 \in X$ . Ist  $x_0$  bereits minimal, so sind wir fertig. Ist  $x_0$  nicht minimal in  $(X, \preceq)$ , dann gibt es ein  $x_1 \prec x_0$ . Ist nun  $x_1$  minimal, so sind wir fertig, andernfalls gibt es ein  $x_2 \prec x_1$ , und so weiter. Nach endlich vielen Schritten erreichen wir ein minimales Element, denn andernfalls hätte  $X$  unendlich viele verschiedene Elemente  $x_0, x_1, x_2, \dots$ .  $\square$

Für unendliche Mengen ist Satz 2.2.3 nichts weiter als falsch. Zum Beispiel hat die Menge  $(\mathbb{Z}, \leq)$  der ganzen Zahlen mit ihrer natürlichen Ordnung kein minimales Element.

Vielleicht ist dem Leser dieser (algorithmisch motivierte) Beweis von Satz 2.2.3 suspekt. Statt in die Details zu gehen, fügen wir eine andere Formulierung der gleichen Beweisidee an.

**Zweiter Beweis.** Wir betrachten die geordnete Menge  $(X, \preceq)$  und wählen ein  $x \in X$ , für das die Menge  $L_x = \{y : y \preceq x\}$  die kleinstmögliche Anzahl von Elementen hat. Ist  $|L_x| = 1$ , dann sind wir fertig, denn dann ist  $L_x = \{x\}$  und somit  $x$  ein minimales Element. Nun zeigen wir, dass  $|L_x| > 1$  unmöglich ist. In diesem Fall gibt es nämlich ein  $y \in L_x$ ,  $y \neq x$ , und dann ist  $|L_y| < |L_x|$ , was jedoch der Wahl des Elements  $x$  widerspricht.  $\square$

Die Existenz eines minimalen Elements (Satz 2.2.3) nutzen wir gleich im nächsten Beweis aus.

**Beweis von Satz 2.2.1 (Existenz der linearen Erweiterung).** Wir führen Induktion über  $|X|$ . Für  $|X| = 1$  ist nichts zu beweisen, es gibt nur eine Ordnung auf  $X$  und die ist bereits linear. Betrachten wir also eine geordnete Menge  $(X, \preceq)$  mit  $|X| > 1$ . Sei  $x_0 \in X$  ein minimales Element in  $(X, \preceq)$ . Wir setzen  $X' = X \setminus \{x_0\}$  und bezeichnen die Restriktion der Relation  $\preceq$  auf die Menge  $X'$  mit  $\preceq'$ . Wir wissen, dass  $(X', \preceq')$  eine geordnete Menge ist, und deshalb gibt es laut Induktionsvoraussetzung eine lineare Ordnung  $\leq'$  von  $X'$ , so dass für alle  $x, y \in X'$  aus  $x \preceq' y$  folgt, dass auch  $x \leq' y$ . Wir definieren eine Relation  $\leq$  auf der Menge  $X$  wie folgt:

$$\begin{aligned} x_0 \leq y &\quad \text{für jedes } y \in X'; \\ x \leq y &\quad \text{wenn} \quad x \leq' y. \end{aligned}$$

Offensichtlich folgt aus  $x \preceq y$  stets  $x \leq y$ . Dass  $\leq$  wirklich eine lineare Ordnung ist, mag der Leser selbst überprüfen.  $\square$

Die Existenz linearer Erweiterungen ist eine wichtige und nützliche Tatsache. In vielen Anwendungen muss eine gegebene Halbordnung (mit dem Rechner) zu einer linearen Ordnung erweitert werden. Dieses algorithmische Problem läuft unter dem Namen *topologische Sortierung*.

Satz 2.2.1 über die Existenz linearer Erweiterungen gilt auch für unendliche Mengen, lässt sich dann aber nicht mehr so einfach beweisen. In gewissem Sinne lässt er sich dann gar nicht mehr beweisen, weil man ihn als eines der Axiome der Mengenlehre ansehen kann, etwa so wie das Auswahlaxiom, mit dem er verwandt ist (aber nicht äquivalent).

Wir beschließen diesen Abschnitt mit einer Warnung. Der Begriff „minimales Element“ darf nicht mit dem scheinbar ähnlichen

*kleinsten Element* (auch *Minimum* genannt) verwechselt werden. Die Ähnlichkeit ist rein sprachlicher Natur, die Begriffe selbst sind sehr verschieden, wie die folgende Definition zeigt.

**2.2.4 Definition.** Sei  $(X, \preceq)$  eine geordnete Menge. Ein Element  $a \in X$  heißt kleinstes Element von  $(X, \preceq)$ , wenn  $a \preceq x$  für alle  $x \in X$ . Ein größtes Element ist analog definiert.

Ein kleinstes Element ist offenbar auch minimal. Beispielsweise ist in der Menge der natürlichen Zahlen, geordnet durch die Teilbarkeitsrelation, d.h.  $(\mathbb{N}, |)$ , die Zahl 1 ein kleinstes Element und ein minimales Element. Ein minimales Element ist jedoch nicht zwangsläufig ein kleinstes Element: Betrachten wir z.B. eine mindestens zweielementige Menge  $X$  mit der Gleichheitsrelation (also  $(X, \Delta_X)$ ), dann sind keine zwei Elemente vergleichbar, jedes Element ist minimal, aber es gibt kein kleinstes Element. Ein weiteres Beispiel ist  $(\mathbb{N} \setminus \{1\}, |)$ , die natürlichen Zahlen größer 1 mit der Teilbarkeitsrelation. Dort gibt es kein kleinstes Element, aber unendlich viele minimale Elemente; davon handelt Aufgabe 7.

## Aufgaben

1. (a) Zeigen Sie, dass ein größtes Element stets maximal ist.  
 (b) Finden Sie ein Beispiel für ein Poset mit maximalem aber ohne größtes Element.  
 (c) Finden Sie ein Poset ohne kleinstes und ohne minimales Element, aber mit größtem Element.
2. (a) Betrachten Sie die Menge  $\{1, 2, \dots, n\}$ , geordnet durch die Teilbarkeitsrelation  $|$  (siehe Beispiel 2.1.2). Was ist die maximal mögliche Anzahl von Elementen einer Menge  $X \subseteq \{1, 2, \dots, n\}$ , die durch  $|$  linear geordnet ist (solch eine Menge, eine linear geordnete Teilmenge einer partiell geordneten Menge, heißt *Kette*)?  
 (b) Beantworten Sie die gleiche Frage für die Potenzmenge  $2^{\{1, 2, \dots, n\}}$ , geordnet durch die Relation  $\subseteq$  (siehe Beispiel 2.1.3).
3. Mit  $\text{le}(X, \preceq)$  bezeichnen wir die Anzahl der linearen Erweiterungen eines Poset  $(X, \preceq)$ . Beweisen Sie:  
 (a)  $\text{le}(X, \preceq) = 1$  genau dann, wenn  $\preceq$  eine lineare Ordnung ist;  
 (b)  $\text{le}(X, \preceq) \leq n!$ , wobei  $n = |X|$  (vielleicht möchten Sie zunächst Kapitel 3 lesen).
4. Beweisen Sie, dass ein kleinstes Element, wenn es überhaupt existiert, eindeutig bestimmt ist.

## 56 Ordnungen

5. Beweisen Sie, dass ein minimales Element in einer linear geordneten Menge auch das kleinste Element ist.
6. Beweisen oder widerlegen Sie: Wenn ein Poset  $(X, \preceq)$  nur ein einziges minimales Element hat, dann ist es zugleich ein kleinstes Element.
7. (a) Beweisen Sie, dass das Poset  $(\mathbb{N} \setminus \{1\}, |)$  unendlich viele minimale Elemente besitzt. Wie werden sie normalerweise genannt?  
 (b) Wie viele minimale Elemente besitzt die geordnete Menge  $(X, |)$ , wenn  $X = \{4k + 2 : k \geq 2\}$ ? Es sei angemerkt, dass die entsprechende Frage für die Menge  $\{4k + 1 : k \geq 2\}$  mit der Teilbarkeitsordnung deutlich schwieriger ist.
8. Es sei  $(X, R)$  eine partiell geordnete Menge. Beweisen Sie:
  - (a) Auch  $(X, R^{-1})$  ist partiell geordnet.
  - (b) Ein Element  $x \in X$  ist genau dann maximal in  $(X, R)$ , wenn  $x$  minimal in  $(X, R^{-1})$  ist.
  - (c) Ein Element  $x \in X$  ist genau dann das größte Element von  $(X, R)$ , wenn  $x$  das kleinste Element von  $(X, R^{-1})$  ist.

Weil  $(R^{-1})^{-1} = R$ , gibt es die Begriffe für geordnete Mengen immer in symmetrischen Paaren, etwa minimales und maximales Element, kleinstes und größtes Element, etc. Daher betrachten wir Definitionen und Beweise oft für nur einen der Begriffe in einem solchen Paar. Zum Beispiel genügt es, Satz 2.2.3 über die Existenz eines minimalen Elements zu beweisen, der entsprechende Satz über die Existenz eines maximalen Elements folgt ganz von selbst — den Beweis „übersetzt“ man einfach. Diese Methode nennt man das *Dualitätsprinzip* für geordnete Mengen.

9. Sei  $(X, \preceq)$  ein Poset und  $A \subseteq X$  eine Teilmenge. Ein Element  $s \in X$  heißt *Supremum* der Menge  $A$ , wenn folgendes gilt:

- $a \preceq s$  für alle  $a \in A$ ,
- wenn  $a \preceq s'$  für alle  $a \in A$  ist, wobei  $s'$  ein Element der Menge  $X$  ist, dann ist  $s \preceq s'$ .

Ein Supremum  $s$  kann in  $A$  enthalten sein, muss aber nicht. Das *Infimum* einer Teilmenge  $A \subseteq X$  ist analog definiert, nur dass alle Ungleichungen in die andere Richtung gehen.

- (a) Zeigen Sie, dass jede Teilmenge  $A \subseteq X$  höchstens ein Supremum und höchstens ein Infimum hat. (Das Supremum von  $A$  wird, wenn es existiert, mit  $\sup A$  bezeichnet. Entsprechend bezeichnet  $\inf A$  das Infimum.)
- (b) Welches Element ist das Supremum der leeren Menge (nach der eben angegebenen Definition)?

- (c) Geben Sie ein Beispiel für ein Poset an, in dem jede nichtleere Teilmenge ein Infimum hat, es jedoch nichtleere Teilmengen gibt, die kein Supremum haben.
- (d) \*Sei  $(X, \preceq)$  ein Poset, in dem jede Teilmenge (einschließlich der leeren) ein Supremum besitzt. Zeigen Sie, dass dann jede Teilmenge auch ein Infimum hat.
10. Betrachten Sie das Poset  $(\mathbb{N}, |)$  (geordnet mit Teilbarkeitsrelation).
- Entscheiden Sie, ob jede nichtleere Teilmenge von  $\mathbb{N}$  ein Supremum besitzt.
  - Entscheiden Sie, ob jede nichtleere endliche Teilmenge von  $\mathbb{N}$  ein Supremum besitzt.
  - Entscheiden Sie, ob jede nichtleere Teilmenge ein Infimum besitzt.

## 2.3 Die Teilmengenrelation

In Abschnitt 1.4 haben wir die Beschreibung einer Äquivalenzrelation auf einer Menge  $X$  durch eine Partition der Menge eingeführt. Diese Entsprechung ist bijektiv, wir können Partitionen also als eine andere Darstellung von Äquivalenzrelationen ansehen. Gibt es etwas vergleichbares für Halbordnungen?

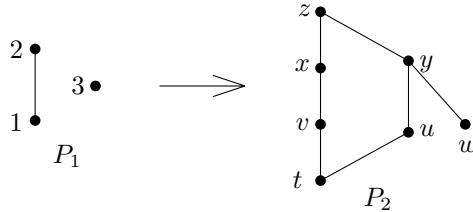
Die Antwort scheint nein. Der Begriff der Ordnung erscheint so viel reicher und komplexer zu sein als der der Äquivalenz, deshalb widmen wir ihm ein eigenes Kapitel. Dennoch zeigen wir in diesem Abschnitt, dass jede Halbordnung gewissermaßen durch die Teilmengenrelation  $\subseteq$  gegeben ist, auf eine irgendwie vertraute Weise. Zur Formulierung dieses Ergebnisses verwenden wir die folgende Definition.

**2.3.1 Definition.** Es seien  $(X, \preceq)$  und  $(X', \preceq')$  geordnete Mengen. Eine Abbildung  $f: X \rightarrow X'$  heißt eine Einbettung von  $(X, \preceq)$  in  $(X', \preceq')$ , wenn die folgenden Bedingungen erfüllt sind:

- $f$  ist eine injektive Abbildung;
- $f(x) \preceq' f(y)$  gilt genau dann, wenn  $x \preceq y$ .

An dieser Stelle ist eine Bemerkung angebracht. Ist eine Einbettung  $f$  surjektiv, dann ist sie ein Isomorphismus, wie schon in Aufgabe 2.1.4 angesprochen. Während ein Isomorphismus zweier geordneter Mengen die Tatsache ausdrückt, dass sie „genauso aussehen“, sagt uns eine Einbettung von  $(X, \preceq)$  in  $(X', \preceq')$ , dass ein *Teilbereich* von  $(X', \preceq')$ , nämlich  $\{f(x): x \in X\}$ , „genauso aussieht“ wie  $(X, \preceq)$ .

Die folgende Zeichnung zeigt zwei Posets:



Beispiele für Einbettungen von  $P_1$  in  $P_2$  sind die Abbildungen  $f: 1 \mapsto v, 2 \mapsto x, 3 \mapsto y$  und  $f': 1 \mapsto t, 2 \mapsto x, 3 \mapsto w$ , wohingegen weder  $g: 1 \mapsto t, 2 \mapsto v, 3 \mapsto y$  noch  $g': 1 \mapsto x, 2 \mapsto w, 3 \mapsto u$  Einbettungen sind.

**2.3.2 Satz.** Für jede geordnete Menge  $(X, \preceq)$  existiert eine Einbettung in die geordnete Menge  $(2^X, \subseteq)$ .

**Beweis.** Dieser Beweis beruht darauf, dass man eine solche Einbettung sehr leicht angeben kann. Wir definieren die Abbildung  $f: X \rightarrow 2^X$  durch  $f(x) = \{y \in X: y \preceq x\}$ . Nun zeigen wir, dass dies wirklich eine Einbettung ist.

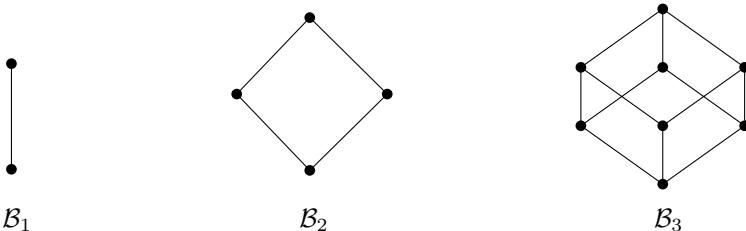
1.  $f$  ist injektiv. Denn wenn  $f(x) = f(y)$ , dann folgt (wegen  $x \in f(x)$  und  $y \in f(y)$ ) aus der Definition von  $f$ , dass sowohl  $x \preceq y$  als auch  $y \preceq x$ , und somit ist (wegen der Antisymmetrie von  $\preceq$ )  $x = y$ .
2. Wenn  $x \preceq y$ , dann ist auch  $f(x) \subseteq f(y)$ . Denn wenn  $z \in f(x)$ , dann ist  $z \preceq x$ , und wegen der Transitivität von  $\preceq$  ist  $z \preceq y$ . Letzteres bedeutet aber, dass  $z \in f(y)$ .
3. Wenn  $f(x) \subseteq f(y)$ , dann ist  $x \preceq y$ . Denn wenn  $f(x) \subseteq f(y)$ , dann ist  $x \in f(y)$ , und folglich  $x \preceq y$ .  $\square$

Die Abbildung  $f$  ist uns bereits im Beweis von Satz 2.2.3 begegnet, die Menge  $f(x)$  hieß dort  $L_x$ . Es kommt häufiger vor, dass das gleiche Ding in anderem Kontext einen anderen Namen hat. Die Mengen  $L_x$  werden relativ oft benötigt und haben Namen wie „Ideal“ oder „Unterhalbmenge“.

Dieser Satz gilt übrigens auch für unendliche Mengen.

Die geordneten Mengen  $(2^X, \subseteq)$  sind also universell in dem Sinne, dass jede geordnete Menge in ihnen enthalten ist. Es verwundert daher nicht, dass sie sehr gründlich untersucht sind und dass besondere Schreibweisen für sie definiert sind. Speziell für  $X =$

$\{1, 2, \dots, n\}$  wird die Menge  $(2^X, \subseteq)$  oft mit  $\mathcal{B}_n$  bezeichnet. Die Hasse-Diagramme von  $\mathcal{B}_1$ ,  $\mathcal{B}_2$  und  $\mathcal{B}_3$  sehen so aus:



Je nach Kontext (und den zusätzlichen Eigenschaften, die gerade interessieren) bezeichnet man die geordneten Mengen  $\mathcal{B}_n$  als Boolesche Algebra, Boolesches Gitter,  $n$ -dimensionalen Würfel, usw.

## Aufgaben

1. Wie viele lineare Erweiterungen hat  $\mathcal{B}_2$ , und wie sieht es bei  $\mathcal{B}_3$  aus?
2. Führen Sie nochmals den Beweis von Satz 2.3.2, diesmal unter Verwendung von *Oberhalbmenigen*, d.h. Mengen der Gestalt  $U_x = \{y: xRy\}$ .
3. Geben Sie ein Beispiel für eine geordnete Menge an, die sich in ein  $\mathcal{B}_n$  mit  $n < |X|$  einbetten lässt.
4. \*Beweisen Sie, dass jedes endliche Poset in  $(\mathbb{N}, |)$  eingebettet werden kann.
5. \*Beweisen Sie, dass sich nicht jedes endliche Poset in die geordnete Menge mit Tripeln reeller Zahlen aus Beispiel 2.1.1 einbetten lässt.
6. (a) Beschreiben Sie eine Einbettung der Menge  $\{1, 2\} \times \mathbb{N}$  mit der lexicographischen Ordnung in die geordnete Menge  $(\mathbb{Q}, \leq)$  der rationalen Zahlen mit der gewohnten Ordnung.  
 (b) Ersetzen Sie in (a) die Menge  $\{1, 2\} \times \mathbb{N}$  durch  $\mathbb{N} \times \mathbb{N}$  (lexikographisch geordnet) und lösen Sie diese Abwandlung.  
 (c)\* Beweisen Sie, dass *jede* abzählbare linear geordnete Menge in  $(\mathbb{Q}, \leq)$  eingebettet werden kann.
7. \*Beweisen Sie, dass jede Teilmenge des Poset  $\mathcal{B}_n$  sowohl ein Supremum als auch ein Infimum hat (die Definitionen stehen in Aufgabe 2.2.9).
8. Wie viele Einbettungen von  $P_1$  in  $P_2$  gibt es, wenn  $P_1$  und  $P_2$  die Posets aus dem Bild vor Satz 2.3.2 sind?

## 2.4 Groß heißt lang oder dick

Sei  $(X, \preceq)$  ein endliches Poset, das wir mit dem Buchstaben  $P$  abkürzen wollen. In diesem Abschnitt haben wir es fast immer mit

nur einer geordneten Menge zu tun, die aber beliebig gewählt sein darf. Die hier zu untersuchenden Begriffe werden in den folgenden Definitionen eingeführt.

**2.4.1 Definition.** Eine Menge  $A \subseteq X$  heißt unabhängig in  $P$ , wenn für keine zwei (verschiedenen) Elemente  $x, y \in A$  gilt, dass  $x \preceq y$ .

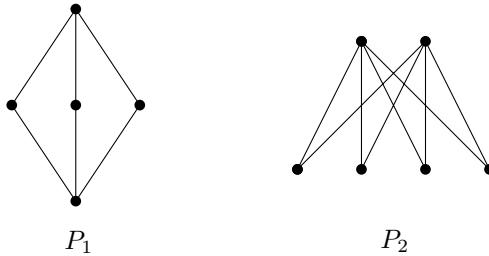
Eine unabhängige Menge wird auch als *Antikette* bezeichnet.

Wir nennen zwei Elemente  $x$  und  $y$  *vergleichbar*, wenn  $x \preceq y$  oder  $y \preceq x$  gilt, andernfalls *unvergleichbar*. Mit dieser Terminologie sagt die obige Definition also, eine Menge ist unabhängig, wenn keine zwei Elemente vergleichbar sind.

Wir schreiben  $\alpha(P)$  für die maximale Größe einer unabhängigen Menge in  $P$ . Als Formel:

$$\alpha(P) = \max\{|A| : A \text{ unabhängig in } P\}.$$

**2.4.2 Beispiel.** Für die abgebildeten Mengen  $P_1$  und  $P_2$



ist  $\alpha(P_1) = 3$ ,  $\alpha(P_2) = 4$ .

**2.4.3 Beobachtung.** Die Menge aller minimalen Elemente von  $P$  ist unabhängig.

**2.4.4 Definition.** Eine Menge  $A \subseteq X$  heißt eine Kette von  $P$ , wenn je zwei ihrer Elemente vergleichbar sind (in  $P$ ).

Anders ausgedrückt, bilden die Elemente von  $A$  eine linear geordnete Teilmenge von  $P$ . Mit  $\omega(P)$  bezeichnen wir die maximale Größe einer Kette in  $P$ . Für die geordneten Mengen  $P_1$  und  $P_2$  von oben ist  $\omega(P_1) = 3$ ,  $\omega(P_2) = 2$ .

Man prüft leicht nach, dass  $\omega(\mathcal{B}_n) = n + 1$ . Die Bestimmung von  $\alpha(\mathcal{B}_n)$  ist deutlich schwieriger; wir werden diese Frage in Kapitel 7 beantworten.

Die obigen Beispiele legen nahe, sich  $\alpha(P)$  als eine Art abstrakte „Dicke“ vorzustellen und bei  $\omega(P)$  an so etwas wie „Länge“ zu denken.

Der folgende Satz kommt eher unschuldig daher, ebenso wie sein Beweis. Er hat jedoch weit reichende Konsequenzen.

**2.4.5 Satz.** *Für jede endliche geordnete Menge  $P = (X, \preceq)$  ist*

$$\alpha(P) \cdot \omega(P) \geq |X|.$$

(Der Leser sollte sich angewöhnen, neue Behauptungen zunächst an einfachen Beispielen „auszuprobieren“. Gilt dieser Satz 2.4.5 für die oben stehenden Beispiele?)

**Beweis.** Wir definieren Mengen  $X_1, X_2, \dots, X_t$  mit Induktion:  $X_1$  sei die Menge aller minimalen Elemente der geordneten Menge  $P$ . Im Induktionsschritt seien  $X_1, \dots, X_\ell$  bereits definiert, und  $X'_\ell = X \setminus \bigcup_{i=1}^\ell X_i$  bezeichne die Menge aller Elemente, die zu keiner der Mengen  $X_1, \dots, X_\ell$  gehören. Wenn  $X'_\ell$  die leere Menge ist, setzen wir  $t = \ell$  und beenden die Konstruktion. Andernfalls, wenn  $X'_\ell \neq \emptyset$ , stehe  $\preceq'$  für die Ordnung  $\preceq$  eingeschränkt auf  $X'_\ell$ , und wir definieren  $X_{\ell+1}$  als die Menge aller minimalen Elemente in  $(X'_\ell, \preceq')$ . Der Beweis ist fertig, wenn wir die folgenden Behauptungen zeigen können:

- (1) Die Mengen  $X_1, \dots, X_t$  bilden eine Partition von  $X$ .
- (2) Jedes  $X_i$  ist eine unabhängige Menge in  $P$ .
- (3)  $\omega(P) \geq t$ .

Die Behauptungen (1) und (2) folgen unmittelbar aus der Definition der Mengen  $X_1, X_2, \dots, X_t$  und aus Beobachtung 2.4.3. Daher genügt es, (3) zu beweisen.

Mit einer Art umgekehrter Induktion ( $k = t, t-1, \dots, 2, 1$ ) identifizieren wir Elemente  $x_i \in X$ , so dass die Menge  $\{x_1, x_2, \dots, x_t\}$  eine Kette bildet. Wir wählen  $x_t \in X_t$  beliebig. Weil  $x_t \notin X_{t-1}$ , muss es ein  $x_{t-1} \in X_{t-1}$  geben, für das  $x_{t-1} \prec x_t$ . Auf diesem Argument beruht der ganze Beweis: Sind  $x_t \in X_t, x_{t-1} \in X_{t-1}, \dots, x_{k+1} \in X_{k+1}$  schon konstruiert, dann ist  $x_{k+1} \notin X_k$ , und daher gibt es ein  $x_k \in X_k$  mit  $x_k \prec x_{k+1}$ .

Die so konstruierte Menge  $\{x_1, \dots, x_t\}$  ist eine Kette. Deshalb ist  $\omega(P) \geq t$ . (Es ist sogar  $\omega(P) = t$ ; das brauchen wir aber nicht und überlassen es dem Leser als leichte Übung.)  $\square$

Satz 2.4.5 hat eine Reihe hübscher Anwendungen, was der folgende berühmte Beweis illustrieren mag.

**2.4.6 Satz (Erdős–Szekeres–Lemma).** *Eine beliebige Folge  $(x_1, \dots, x_{n^2+1})$  reeller Zahlen enthält stets eine monotone Teilfolge der Länge  $n + 1$ .*

Zunächst lassen Sie uns die Begriffe dieses Satzes explizit definieren. Eine *Teilfolge* der Länge  $m$  ist durch Indizes  $i_1, \dots, i_m$  bestimmt,  $i_1 < i_2 < \dots < i_m$ , und hat die Form  $(x_{i_1}, x_{i_2}, \dots, x_{i_m})$ . Eine solche Folge heißt *monoton* wenn  $x_{i_1} \leq x_{i_2} \leq \dots \leq x_{i_m}$  oder  $x_{i_1} \geq x_{i_2} \geq \dots \geq x_{i_m}$ . Z.B. enthält die Folge  $(3, 5, 6, 2, 8, 1, 4, 7)$  die monotonen Teilfolgen  $(3, 5, 6, 8)$  (mit  $i_1 = 1, i_2 = 2, i_3 = 3$  und  $i_4 = 5$ ) und  $(6, 2, 1)$  (mit  $i_1 = 3, i_2 = 4, i_3 = 6$ ), sowie viele weitere.

**Beweis von Satz 2.4.6.** Gegeben sei eine Folge  $(x_1, \dots, x_{n^2+1})$  von  $n^2 + 1$  reellen Zahlen. Wir setzen  $X = \{1, 2, \dots, n^2 + 1\}$  und definieren eine Relation  $\preceq$  auf  $X$  durch

$$i \preceq j \text{ genau dann, wenn sowohl } i \leq j \text{ als auch } x_i \leq x_j.$$

Es ist nicht schwer zu sehen, dass die Relation  $\preceq$  eine (partielle) Ordnung auf der Menge  $X$  ist. Daher gilt  $\alpha(X, \preceq) \cdot \omega(X, \preceq) \geq n^2 + 1$ , und folglich ist  $\alpha(X, \preceq) > n$  oder  $\omega(X, \preceq) > n$ . Nun überprüft man leicht, dass eine Kette  $i_1 \prec i_2 \prec \dots \prec i_m$  in der Ordnung  $\preceq$  einer nicht fallenden Teilfolge  $x_{i_1} \leq x_{i_2} \leq \dots \leq x_{i_m}$  entspricht (es ist ja  $i_1 < i_2 < \dots < i_m$ ), während eine unabhängige Menge  $\{i_1, i_2, \dots, i_m\}$  einer fallenden Teilfolge entspricht (wenn wir die Schreibweise so wählen, dass  $i_1 < i_2 < \dots < i_m$ , dann erhalten wir  $x_{i_1} > x_{i_2} > \dots > x_{i_m}$ , denn wenn wir z.B.  $x_{i_1} \leq x_{i_2}$  und  $i_1 < i_2$  hätten, dann wäre  $i_1 \prec i_2$ ).  $\square$

## Aufgaben

1. (a)  $\preceq_i$ ,  $i = 1, \dots, k$ , seien Ordnungen auf einer Menge  $X$ . Beweisen Sie, dass  $\bigcap_{i=1}^k \preceq_i$  wieder eine Ordnung auf  $X$  ist (zur Erinnerung:  $\preceq_i$  ist eine Relation und daher eine Teilmenge von  $X \times X$ ).
  - (b) \*Beweisen Sie, dass sich jede Halbordnung  $\preceq$  auf einer Menge  $X$  als Schnitt von *linearen* Ordnungen von  $X$  schreiben lässt.
2. Beweisen Sie, dass  $\omega(\mathcal{B}_n) = n + 1$ .
3. Finden Sie eine Folge reeller Zahlen der Länge 17, die keine monotone Teilfolge der Länge 5 enthält.
4. Beweisen Sie die folgende stärkere Form von Satz 2.4.6:  $k, \ell$  seien natürliche Zahlen. Jede Folge natürlicher Zahlen der Länge  $k\ell + 1$  enthält eine nicht fallende Teilfolge der Länge  $k + 1$  oder eine fallende Teilfolge der Länge  $\ell + 1$ .

5. (a) Beweisen Sie, dass Satz 2.4.5, ebenso wie die vorige Aufgabe, in folgendem Sinn optimal sind: Für alle  $k$  und  $\ell$  gibt es eine  $n$ -elementige, partiell geordnete Menge  $P$  mit  $n$  Elementen, so dass  $n = k\ell$ ,  $\alpha(P) = k$  und  $\omega(P) = \ell$ .  
 (b) \*Gegeben  $k, \ell \geq 1$ , geben Sie eine reelle Zahlenfolge der Länge  $k\ell$ , die keine nicht fallende Teilfolge der Länge  $k + 1$  und keine fallende Teilfolge der Länge  $\ell + 1$  enthält.
6. (a) Wir betrachten zwei Folgen  $a = (a_1, \dots, a_n)$  und  $b = (b_1, \dots, b_n)$  mit verschiedenen reellen Zahlen. Zeigen Sie, dass es immer Indizes  $i_1, \dots, i_k$ ,  $1 \leq i_1 < \dots < i_k \leq n$ , mit  $k = \lceil n^{1/4} \rceil$  gibt, so dass die dadurch bestimmte Teilfolge sowohl in  $a$  als auch in  $b$  steigend oder fallend ist (alle vier Kombinationen sind erlaubt, z.B. „steigend in  $a$ , fallend in  $b$ “, „fallend in  $a$ , fallend in  $b$ “, usw.).  
 (b) \*Zeigen Sie, dass die Schranke für  $k$  in (a) im allgemeinen nicht verbessert werden kann.
7. \*\*(Satz von Dilworth) Sei  $(X, \preceq)$  ein endliches Poset. Zeigen Sie, dass  $X$  als (disjunkte) Vereinigung von höchstens  $\alpha = \alpha(X, \preceq)$  Ketten geschrieben werden kann.



# 3

## Zähltheorie

---

In diesem Kapitel wollen wir Fragen nach der Anzahl gewisser Konfigurationen nachgehen, etwa auf wie viele Arten man  $n$  verschiedene Postkarten an  $n$  Freunde versenden kann oder wie viele Abbildungen es aus einer  $n$ -elementigen Menge in eine  $m$ -elementige Menge gibt. Wir beginnen mit einfachen Beispielen, bei denen man kaum mehr als den gesunden Menschenverstand benötigt, vielleicht noch eine clevere Idee, jedenfalls kein Spezialwissen. Die fortgeschrittenen Techniken kommen dann später.

### 3.1 Funktionen und Teilmengen

Wir beginnen mit dem versprochenen Postkartenproblem.

**Problem.** Professor X<sup>1</sup> geht nach einem arbeitsreichen Kurzbesuch im mathematischen Institut in Niederfuchsingen noch im Ort spazieren und beschließt, jedem seiner fünf Freunde Alice, Bob, Arthur, Merlin und HAL-9000 eine Postkarte zu schicken. Ein Händler verkauft 26 verschiedene Ansichtskarten. Wie viele Möglichkeiten hat Professor X, seinen fünf Freunden Postkarten zu schicken?

Weil er die Postkarte für jeden Freund auf 26 Arten auswählen kann, und weil die fünf Wahlmöglichkeiten voneinander unabhängig sind, ist die Antwort auf diese Frage  $26^5$ . In einer etwas abstrakteren Sprache haben wir die Anzahl aller Abbildungen aus einer fünfelementigen Menge (die Freunde) in eine 26-elementige Menge (die verschiedenen Postkarten) bestimmt. Hier ist noch ein eng verwandtes Problem:

---

<sup>1</sup>Ähnlichkeiten mit real existierenden Professoren sind rein zufällig und haben nichts zu bedeuten.

**Problem.** Wie viele verschiedene Worte gibt es, die aus fünf Buchstaben bestehen? (Wir benutzen die 26 Buchstaben des Alphabets und verlangen nicht, dass die Worte etwas bedeuten<sup>2</sup>.)

Weil jeder der fünf Buchstaben unabhängig von den anderen auf 26 Arten gewählt werden kann, sieht man unschwer ein, dass die Antwort wieder  $26^5$  ist. Und tatsächlich, ein Wort mit fünf Buchstaben kann als Abbildungen aus der Menge  $\{1, 2, \dots, 5\}$  in die Menge  $\{a, b, \dots, z\}$  aufgefasst werden: Für jede der fünf Positionen im Wort, nummeriert von 1 bis 5, geben wir den Buchstaben an dieser Position an. Umformulierungen dieser Art gehören zu den wichtigsten Techniken der Zähltheorie; man *codiert* eine Sorte Objekte durch eine andere Sorte.

Um das hässliche Wort „ $n$ -elementig“ weitgehend zu vermeiden, schreiben wir kurz „ $n$ -Menge“ und meinen damit „eine Menge, die  $n$  Elemente enthält.“

Als Nächstes zählen wir also die Abbildungen aus einer  $n$ -Menge in eine  $m$ -Menge. Dazu perfektionieren wir den Gedankengang von vorhin — eigentlich schreiben wir ihn nur sauber auf.

**3.1.1 Hilfssatz.** Sei  $N$  eine  $n$ -Menge (möglicherweise leer, d.h. wir erlauben  $n = 0, 1, 2, \dots$ ) und sei  $M$  eine  $m$ -Menge,  $m \geq 1$ . Dann ist die Anzahl aller möglichen Abbildungen  $f: N \rightarrow M$  gleich  $m^n$ .

*Beweis.* Wir führen Induktion nach  $n$ . Beginnen wir mit  $n = 0$ . Welches sind die Abbildungen  $f$  von der Menge  $N = \emptyset$  in die Menge  $M$ ? Nach Definition einer Abbildung ist  $f$  eine Menge mit geordneten Paaren  $(x, y)$ , wobei  $x \in N = \emptyset$  und  $y \in M$ . Weil die leere Menge aber keine Elemente enthält, kann  $f$  kein solches geordnetes Paar enthalten, und folglich muss  $f$  selbst die leere Menge sein. Andererseits erfüllt  $f = \emptyset$  in diesem Fall die Definition einer Abbildung, die verlangt, dass für jedes  $x \in N$  eine gewisse Bedingung erfüllt sein soll; es gibt aber keine Elemente  $x \in N$ . Also gibt es genau eine Abbildung  $f: \emptyset \rightarrow M$ . Das ist genau, was auch die Formel sagt, denn  $m^0 = 1$  für jedes  $m \geq 1$ . Damit stimmt die Formel für den Fall  $n = 0$ , das ist der Induktionsanfang.

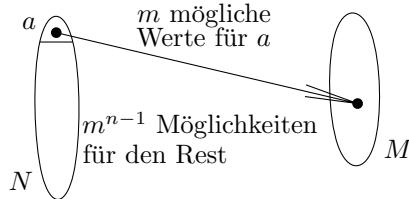
Die Frage, ob eine Abbildung von der leeren Menge in eine andere Menge sinnvoll ist und ob wir sie überhaupt betrachten sollen, ist berechtigt. Man kann die Induktion problemlos auch mit  $n = 1$  starten.

---

<sup>2</sup>Wer will schon ausschließen, dass ein Wort wie *ywizp* nicht in irgendeiner exotischen Sprache, vielleicht auf Tralfamadorisch, doch etwas bedeutet?

Doch die Erfahrung lehrt, dass es in mathematischen Überlegungen oft vorteilhaft ist, solche „Grenzfälle“ genau zu untersuchen und die Definition ganz exakt anzuwenden. Auf diese Weise vermeidet man im weiteren Verlauf der Untersuchungen lästige Ausnahmen und Fallunterscheidungen oder gar Lücken und Fehler in Beweisen. Aus dem gleichen Grund definiert man die „leere Summe“ als 0 oder setzt  $x^0 = 1$  für  $x \neq 0$  usw.

Nehmen wir als Nächstes an, der Hilfssatz ist schon für alle  $n \leq n_0$  und für alle  $m \geq 1$  bewiesen (Induktionsannahme). Für den Induktionsschritt setzen wir  $n = n_0 + 1$  und betrachten eine  $n$ -Menge  $N$  und eine  $m$ -Menge  $M$ . Wir wählen ein beliebiges Element  $a \in N$ . („Beliebig“ heißt, es ist egal, welches Element wir wählen; nach der Wahl ist es aber fest, d.h. wir dürfen nicht später im Beweis ein anderes Element  $a$  nennen.) Eine Abbildung  $f: N \rightarrow M$  anzugeben ist das Gleiche, wie einen Wert  $f(a) \in M$  festzulegen sowie eine Abbildung  $f': N \setminus \{a\} \rightarrow M$ . Den Wert  $f(a)$  können wir auf  $m$  verschiedene Arten wählen, die Abbildung  $f'$  nach Induktionsvoraussetzung auf  $m^{n-1}$  Arten. Jede Wahl von  $f(a)$  kann mit jeder Wahl von  $f'$  kombiniert werden und keine zwei Kombinationen geben die gleiche Funktion  $f$ , also gibt es insgesamt  $m \cdot m^{n-1} = m^n$  verschiedene  $f$ . Fassen wir das ganze Argument noch einmal im Bild zusammen:



□

**3.1.2 Hilfssatz.** Eine  $n$ -Menge  $X$  hat stets genau  $2^n$  Teilmengen (für alle  $n \geq 0$ ).

Dies ist ein weiteres einfaches und wichtiges Zählresultat. Wir geben zwei Beweise.

**Erster Beweis (Induktion).** Für  $X = \emptyset$  gibt es genau eine Teilmenge, nämlich  $\emptyset$ , und das ist, was die Formel auch sagt:  $2^0 = 1$ .

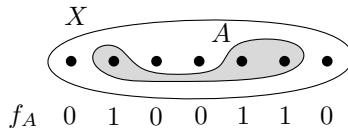
Haben wir eine  $(n+1)$ -Menge  $X$ , dann betrachten wir ein (beliebiges) Element  $a \in X$  und unterteilen die Teilmengen von  $X$  in zwei Klassen: in die Teilmengen, die  $a$  enthalten, und jene, die  $a$  nicht enthalten. Die zweite Klasse sind genau die Teilmengen der

$n$ -Menge  $X \setminus \{a\}$ , davon gibt es  $2^n$  viele (nach Induktionsvoraussetzung). Für jede Teilmenge  $A$  der ersten Klasse betrachten wir die Menge  $A' = A \setminus \{a\}$ . Dies ist eine Teilmenge von  $X \setminus \{a\}$ . Offensichtlich erhält man jede Teilmenge  $A' \subseteq X \setminus \{a\}$  von genau einer Menge  $A$  aus der ersten Klasse, nämlich von  $A' \cup \{a\}$ . Mit anderen Worten: Es gibt eine Bijektion zwischen allen Teilmengen der ersten und der zweiten Klasse. Also hat auch die erste Klasse  $2^n$  Teilmengen, insgesamt erhalten wir  $2^n + 2^n = 2^{n+1}$  Teilmengen der  $(n+1)$ -Menge  $X$ , wie behauptet.  $\square$

**Zweiter Beweis (Rückführung auf ein bekanntes Resultat).** Bertachten wir eine beliebige Teilmenge  $A$  einer gegebenen  $n$ -Menge  $X$ . Wir definieren eine Abbildung  $f_A: X \rightarrow \{0, 1\}$ . Für ein Element  $x \in X$  setzen wir

$$f_A(x) = \begin{cases} 1 & \text{falls } x \in A \\ 0 & \text{falls } x \notin A. \end{cases}$$

(Diese Abbildung wird in der Mathematik oft betrachtet, sie heißt die *charakteristische Funktion* der Menge  $A$ .) Im Bild sieht das so aus:



Verschiedene Mengen  $A$  haben verschiedene charakteristische Funktionen  $f_A$ , und umgekehrt legt jede Abbildung  $f: X \rightarrow \{0, 1\}$  eindeutig eine Teilmenge  $A \subseteq X$  mit  $f = f_A$  fest. Also ist die Anzahl der Teilmengen von  $X$  gleich der Anzahl aller Funktionen  $X \rightarrow \{0, 1\}$ , und die ist nach Hilfssatz 3.1.1 gleich  $2^n$ .  $\square$

Nun ein etwas komplizierteres Ergebnis:

**3.1.3 Hilfssatz.** Sei  $n \geq 1$ . Jede  $n$ -Menge hat genau  $2^{n-1}$  Teilmengen mit ungerade vielen Elementen sowie  $2^{n-1}$  Teilmengen mit gerade vielen Elementen.

*Beweis.* Der Einfachheit halber werden wir eine Menge mit ungerade vielen Elementen ungerade nennen. Wir benutzen Hilfssatz 3.1.2. Halten wir ein Element  $a \in X$  fest. Wir können eine Teilmenge  $A \subseteq X \setminus \{a\}$  nach folgender Regel zu einer ungeraden Teilmenge  $A' \subseteq X$  ergänzen: ist  $|A|$  ungerade, so setzen wir  $A' = A$ , und ist  $|A|$

gerade, so setzen wir  $A' = A \cup \{a\}$ . Man überzeugt sich leicht (bitte tun Sie es!), dass dies eine Bijektion zwischen dem System aller Teilmengen von  $X \setminus \{a\}$  und dem System aller ungeraden Teilmengen von  $X$  definiert. Also ist die Anzahl aller ungeraden Teilmengen von  $X$  gleich  $2^{n-1}$ .

Für die Teilmengen mit gerade vielen Elementen kann man den Beweis genau so führen, oder man argumentiert einfach, dass jede Teilmenge, die nicht ungerade ist, gerade viele Elemente enthalten muss. Daraus berechnet man, dass es  $2^n - 2^{n-1} = 2^{n-1}$  viele Teilmengen mit gerade vielen Elementen gibt.  $\square$

### Injektive Abbildungen.

**Problem.** Nachdem Professor X eine Weile darüber nachgedacht hat, welche der zirka zwölf Millionen Möglichkeiten, seinen fünf Freunden Postkarten zu senden, wohl die beste wäre, geht er wieder zu dem Händler um die Karten zu kaufen. Doch der Händler hat bereits alle Postkarten verkauft und will gerade schließen. Er hat aber von jeder der 26 Postkarten noch ein Ansichtsexemplar, und er lässt sich überreden, Professor X fünf davon zu je 5 Euro zu überlassen. Jetzt muss Professor X neu entscheiden, für wen er welche Postkarte kauft. Wieviele Möglichkeiten hat er nun?

Professor X macht sich klar, dass er die injektiven Abbildungen aus einer 5-elementigen Menge in eine 26-elementige Menge zählen muss. Das ist das gleiche, wie die Worte mit 5 Buchstaben zu zählen, bei denen alle Buchstaben verschieden sind.

**3.1.4 Hilfssatz.** Seien  $n, m \geq 0$ , dann gibt es genau

$$m(m-1)\dots(m-n+1) = \prod_{i=0}^{n-1} (m-i)$$

injektive Abbildungen aus einer gegebenen  $n$ -Menge in eine gegebene  $m$ -Menge.

*Beweis.* Wieder wenden wir Induktion nach  $n$  an (und zwar knapper und versierter als bisher). Für  $n = 0$ : Die leere Abbildung ist injektiv, also gibt es genau eine injektive Abbildung; da wir das leere Produkt als 1 definiert haben (wie praktisch!), ist die angegebene Formel für  $n = 0$  richtig.

Für  $n > m$  gibt es keine injektive Abbildung, auch das sagt die Formel richtig voraus; denn einer der Faktoren in dem Produkt ist 0.

Betrachten wir nun eine  $n$ -Menge  $N$ ,  $n \geq 1$ , und eine  $m$ -Menge  $M$ ,  $m \geq n$ . Wir wählen ein beliebiges Element  $a \in N$  und dazu einen Funktionswert  $f(a) \in M$ , einen von  $m$  möglichen. Nun müssen wir noch eine injektive Abbildung aus der Menge  $N \setminus \{a\}$  in die Menge  $M \setminus \{f(a)\}$  wählen. Nach Induktionsvoraussetzung haben wir dafür  $(m-1)(m-2) \dots (m-n+1)$  Möglichkeiten. Insgesamt gibt es also  $m(m-1)(m-2) \dots (m-n+1)$  injektive Abbildungen  $f: N \rightarrow M$ . (Gibt es dazu kein Bild? Nun, Sie können nicht erwarten, in einem Buch dieser Preisklasse *alles* zu finden.)  $\square$

Bei dem zweiten Postkartenproblem und den Worten mit 5 Buchstaben haben wir es schon erwähnt: Eine injektive Abbildung aus einer  $n$ -Menge in eine  $m$ -Menge können wir auch als Auswahl von  $n$  Elementen aus einer  $m$ -Menge interpretieren, wobei die Reihenfolge der gewählten Elemente von Bedeutung ist (d.h. wir konstruieren ein  $n$ -Tupel). So eine Auswahl bezeichnet man manchmal als *Variation ohne Wiederholung von  $n$  Elementen aus  $m$  Elementen*.

## Aufgaben

- Sei  $X = \{x_1, x_2, \dots, x_n\}$  eine  $n$ -Menge. Beschreiben Sie eine Codierung der Teilmengen von  $X$  als Worte der Länge  $n$ , die nur die Buchstaben  $a$  und  $b$  enthalten. Schließen Sie daraus, dass die Anzahl der Teilmengen von  $X$  gleich  $2^n$  ist. (Vgl. den zweiten Beweis von Hilfsatz 3.1.2.)
- Bestimmen Sie die Anzahl der geordneten Paare  $(A, B)$  mit der Eigenschaft  $A \subseteq B \subseteq \{1, 2, \dots, n\}$ .
- Sei  $N$  eine  $n$ -Menge und  $M$  eine  $m$ -Menge. Definieren Sie eine Bijektion zwischen der Menge aller Abbildungen  $f: N \rightarrow M$  und dem  $n$ -fachen kartesischen Produkt  $M^n$ .
- Gibt es unter den Zahlen  $1, 2, \dots, 10^{10}$  mehr, die in Dezimalschreibweise eine 9 enthalten, oder gibt es mehr, die keine 9 enthalten?
- (a) Wie viele  $(n \times n)$  Matrizen mit Einträgen aus  $\{0, 1, \dots, q-1\}$  gibt es?  
(b) \*Sei  $q$  eine Primzahl. Wie viele nicht singuläre Matrizen gibt es über dem Körper mit  $q$  Elementen? (Anders ausgedrückt: Wie viele der Matrizen aus Aufgabenteil (a) haben eine Determinante, die nicht durch  $q$  teilbar ist?)

6. \*Zeigen Sie, dass eine natürliche Zahl  $n \geq 1$  genau dann eine ungerade Anzahl von Teilern (einschließlich 1 und  $n$  selbst) hat, wenn  $\sqrt{n}$  eine ganze Zahl ist.

## 3.2 Permutationen

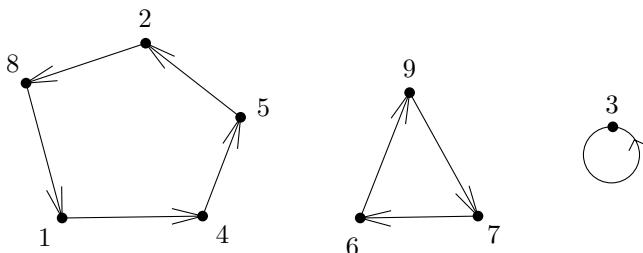
Eine bijektive Abbildung einer endlichen Menge  $X$  in sich selbst heißt eine *Permutation* der Menge  $X$ .

Sind die Elemente aus  $X$  irgendwie angeordnet, dann können wir eine Permutation auch als Umsortieren der Elemente von  $X$  in eine neue Reihenfolge auffassen. Wenn wir z.B. die Menge  $X = \{a, b, c, d\}$  betrachten, dann ist eine mögliche Permutation  $p$  durch  $p(a) = b$ ,  $p(b) = d$ ,  $p(c) = c$  und  $p(d) = a$  gegeben. Eine der üblichen Schreibweisen für Permutationen ist die folgende zweizeilige Form:

$$\begin{pmatrix} a & b & c & d \\ b & d & c & a \end{pmatrix}.$$

In der ersten Zeile sind die Elemente von  $X$  aufgelistet, und unter einem Element  $x \in X$  aus der ersten Zeile steht in der zweiten Zeile das Element  $p(x)$ . Das ist also eine Wertetabelle mit zwei Klammern außen. In den meisten Fällen ist es bequem mit  $X = \{1, 2, \dots, n\}$  zu arbeiten. Mit der Konvention, dass in der ersten Zeile die Zahlen  $1, 2, \dots, n$  in der natürlichen Reihenfolge stehen, können wir uns darauf beschränken, lediglich die zweite Zeile zu schreiben. Dann steht  $(2 \ 4 \ 3 \ 1)$  z.B. für die Permutation  $p$  mit  $p(1) = 2$ ,  $p(2) = 4$ ,  $p(3) = 3$  und  $p(4) = 1$ . Dies nennen wir die einzeilige Schreibweise.

Oft ist die Zyklenschreibweise zur Darstellung einer Permutation praktisch. Am einfachsten versteht man, was ein Zyklus einer Permutation ist, anhand eines Pfeildiagramms (wie in Abschnitt 1.5 eingeführt). Für eine Permutation  $p: X \rightarrow X$  repräsentieren wir die Elemente von  $X$  als Punkte, und wir zeichnen einen Pfeil immer von  $x$  nach  $p(x)$ . Für die Permutation  $p = (4 \ 8 \ 3 \ 5 \ 2 \ 9 \ 6 \ 1 \ 7)$  (dies ist die oben eingeführte einzeilige Form) sieht das Bild so aus:



In jedem Punkt beginnt genau ein Pfeil (weil  $p$  eine Funktion ist) und endet genau ein Pfeil (mindestens einer, weil  $p$  surjektiv ist, und höchstens einer, weil  $p$  injektiv ist). Überlegen Sie sich doch einmal, warum das Bild einer Permutation so aussehen muss: Es besteht aus mehreren disjunkten Mengen von Punkten, die untereinander durch Pfeile kreisförmig verbunden sind. In einer solchen Gruppe von Punkten kann man zyklisch entlanglaufen, deshalb nennt man sie die *Zyklen* der Permutation. (Wenn Sie mit dieser bildlichen Definition eines Zyklus nicht ganz zufrieden sind, in Aufgabe 2 finden Sie eine formale Definition.) In Zyklendarstellung kann man die oben abgebildete Permutation  $p$  auch  $p = ((1, 4, 5, 2, 8)(3)(6, 9, 7))$  schreiben, das ist die Zyklenschreibweise. In jeder inneren Klammer sind die Elemente eines Zyklus in der durch die Pfeile gegebenen Reihenfolge aufgelistet; um die Schreibweise eindeutig zu machen beginnt man in der Regel mit dem kleinsten Element eines Zyklus.

Permutationen sind ebenso nützlich wie elementar. Zum Beispiel beim Entwurf und der Analyse von Sortieralgorithmen. Einige effiziente Algorithmen für Probleme auf Graphen oder mit geometrischen Objekten sortieren als erstes die Eingabe zufällig um, d.h. sie wenden eine zufällige Permutation an. In der Gruppentheorie, die in fast allen Gebieten der Mathematik und auch in der modernen Physik eine herausragende Rolle spielt, sind Permutationsgruppen (mit der Hintereinanderausführung als Gruppenoperation) eines der Grundobjekte. Die Tatsache, dass Gleichungen vom Grad 5 nicht mehr allgemein lösbar sind, lässt sich auf Eigenschaften der Gruppe aller Permutationen von 5 Elementen zurückführen. Der Zauberwürfel, ein in den frühen 80er Jahren des 20. Jahrhunderts weit verbreitetes Spielzeug, ist ein hübsches Beispiel einer komplizierten Permutationsgruppe. Will man das Mischen von Spielkarten mathematisch analysieren, muss man Permutationen untersuchen. Und all dies ist nur ein kleiner Ausschnitt der vielfältigen Anwendungen von Permutationen.

Die Anzahl der Permutationen einer  $n$ -Menge ist laut Hilfssatz 3.1.4 gleich  $n(n-1)\dots\cdot 2 \cdot 1$ . Diese Zahl ist eine Funktion von  $n$ , man bezeichnet sie mit  $n!$  und nennt sie  *$n$  Fakultät*. Zusammengefasst:

$$n! = n(n-1)\cdot\dots\cdot 2\cdot 1 = \prod_{j=0}^{n-1} (n-j) = \prod_{i=1}^n i.$$

In dem speziellen Fall  $n = 0$  haben wir  $0! = 1$  (denn  $0!$  ist als leeres Produkt definiert).

## Aufgaben

1. Wie viele Permutationen von  $\{1, 2, \dots, n\}$  bestehen aus einem einzigen Zyklus?
2. Gegeben sei eine Permutation  $p: X \rightarrow X$ ; mit  $p^k$  bezeichnen wir die Permutation, die wir durch  $k$ -fache Anwendung von  $p$  erhalten, genauer:  $p^1 = p$  und  $p^k = p \circ p^{k-1}$ . Definieren Sie folgendermaßen eine Relation  $\approx$  auf der Menge  $X$ : Genau dann ist  $i \approx j$ , wenn es eine Zahl  $k \geq 1$  gibt mit  $p^k(i) = j$ . Beweisen Sie, dass  $\approx$  eine Äquivalenzrelation auf  $X$  ist, und dass die Äquivalenzklassen gerade die Zyklen von  $p$  sind.
3. Sei  $p$  eine Permutation, und sei  $p^k$  definiert wie in Aufgabe 2. Die kleinste natürliche Zahl  $k \geq 1$ , für die  $p^k = \text{id}$  ist, nennen wir die *Ordnung* der Permutation  $p$ . (Dabei ist  $\text{id}$  die identische Permutation, die jedes Element auf sich selbst abbildet.)
  - (a) Bestimmen Sie die Ordnung der Permutation  $(2 \ 3 \ 1 \ 5 \ 4 \ 7 \ 8 \ 9 \ 6)$ .
  - (b) Zeigen Sie, dass die Ordnung jeder Permutation  $p$  einer endlichen Menge wohldefiniert ist, und \*finden Sie eine Methode, die Ordnung einer Permutation aus den Längen ihrer Zyklen zu berechnen.
4. *Inf* Schreiben Sie ein Programm, das alle Permutationen der Menge  $\{1, 2, \dots, n\}$  auflistet, jede genau einmal. Achten Sie darauf, dass ihr Programm keinen übertriebenen Speicherbedarf hat, denn für große  $n$  wird  $n!$  astronomisch groß. \*Können Sie erreichen, dass die Gesamtzahl der Operationen zur Erzeugung der Permutationen proportional zu  $n!$  ist? Die Operationen zur Ausgabe der Permutationen sollen nicht mitgezählt werden.
5. (Die nächste Aufgabe ist etwas schwieriger — wenn Sie die ersten zwei Abschnitte dieses Kapitels zu leicht und vielleicht ein wenig langweilig fanden: hier ist Futter für Ihre grauen Zellen.) Sei  $p$  eine Permutation der Menge  $\{1, 2, \dots, n\}$ . Wir schreiben  $p$  in der einzeiligen Schreibweise, und in der so entstandenen Zahlenfolge markieren wir die *aufsteigenden Segmente*, z.B. (4 5 7 2 6 8 3 1). Mit  $f(n, k)$  bezeichnen wir die Anzahl der Permutationen einer  $n$ -Menge mit genau  $k$  aufsteigenden Teilstücken.
  - (a) \*Zeigen Sie, dass  $f(n, k) = f(n, n + 1 - k)$  ist, und folgern Sie daraus, dass die durchschnittliche Anzahl aufsteigender Segmente einer Permutation  $(n + 1)/2$  ist (wobei der Durchschnitt über alle Permutationen der Menge  $\{1, 2, \dots, n\}$  gemeint ist).
  - (b) \*Beweisen Sie die Rekursion
 
$$f(n, k) = k \cdot f(n - 1, k) + (n + 1 - k) f(n - 1, k - 1).$$
  - (c) Bestimmen Sie mit Hilfe von (b) die Anzahl der Permutationen von  $\{1, 2, \dots, n\}$  mit 2 aufsteigenden Segmenten, mit 3 aufsteigenden Segmenten und \*mit  $k$  aufsteigenden Segmenten.

(d) \*Berechnen Sie für eine zufällig gewählte Permutation  $\pi$  der Menge  $\{1, 2, \dots, n\}$  die Wahrscheinlichkeit dafür, dass das erste aufsteigende Segment die Länge  $k$  hat. Zeigen Sie, dass die durchschnittliche Länge des ersten aufsteigenden Segments für große  $n$  gegen  $e - 1$  strebt.

*Bemerkung.* Diese und ähnliche Fragen sind in der Analyse verschiedener Sortieralgorithmen von Bedeutung.

6. Sei  $\pi$  eine Permutation der Menge  $\{1, 2, \dots, n\}$ . Ein geordnetes Paar  $(i, j) \in \{1, 2, \dots, n\} \times \{1, 2, \dots, n\}$  nennen wir eine *Inversion* von  $\pi$ , wenn  $i < j$  und  $\pi(i) > \pi(j)$ .
  - (a) Beweisen Sie, dass die Menge  $I(\pi)$  aller Inversionen eine transitive Relation auf  $\{1, 2, \dots, n\}$  ist.
  - (b) Beweisen Sie, dass auch das Komplement von  $I(\pi)$  transitiv ist.
  - (c) <sup>Inf</sup> Über einen Sortieralgorithmus  $A$  erfahren Sie Folgendes: Als Eingabe werden  $n$  Zahlen akzeptiert; diese werden in aufsteigender (genauer: in nicht fallender) Reihenfolge ausgegeben; in jedem Schritt kann der Algorithmus  $A$  nur ein Paar benachbarter Zahlen austauschen. Zeigen Sie, dass es Eingaben gibt, für die der Algorithmus  $A$  mindestens  $cn^2$  Schritte benötigt, wobei  $c > 0$  eine geeignete Konstante ist.
  - (d) <sup>\*Inf</sup> Fällt Ihnen eine Methode ein, die Anzahl der Inversionen einer gegebenen Permutation von  $\{1, 2, \dots, n\}$  in wesentlich weniger als  $n^2$  Schritten zu berechnen? (Es gibt verschiedene Lösungen, siehe z.B. Knuth [44].)
7. (a) \*Welches ist die größte Zehnerpotenz, die die Zahl  $70!$  teilt? Mit anderen Worten: Mit wie vielen Nullen endet die Zahl  $70!$  im Dezimalsystem?
  - (b) \*Suchen Sie nach einer allgemeinen Formel für die größte Zahl  $k$ , für die  $n!$  durch  $p^k$  teilbar ist, wenn  $p$  eine vorgegebene Primzahl ist.
8. Zeigen Sie: Für  $k, n \geq 1$  teilt  $(k!)^n$  die Zahl  $(kn)!$ .

### 3.3 Binomialkoeffizienten

Seien  $n$  und  $k$  ganze Zahlen,  $n \geq k \geq 0$ . Der *Binomialkoeffizient*  $\binom{n}{k}$  (lies: „ $n$  über  $k$ “<sup>3</sup>) ist eine Funktion der Variablen  $n$  und  $k$ ; er ist definiert durch

$$\binom{n}{k} = \frac{n(n-1)(n-2)\dots(n-k+1)}{k(k-1)\cdot\dots\cdot2\cdot1} = \frac{\prod_{i=0}^{k-1}(n-i)}{k!}. \quad (3.1)$$

---

<sup>3</sup>Auf englisch sagt man für  $\binom{n}{k}$  „ $n$  choose  $k$ “; den englischen Ausdruck „ $n$  over  $k$ “ gibt es auch, er bezeichnet den Bruch  $\frac{n}{k}$ .

Vielleicht ist Ihnen eine andere Formulierung bekannt:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Unter den gegebenen Voraussetzungen sind diese beiden Formen äquivalent. Allerdings hat die erste einige Vorteile. Die numerische Berechnung von  $\binom{n}{k}$  ist mit (3.1) einfacher, man erhält auch weniger große Zwischenergebnisse beim Rechnen. Außerdem ist (3.1) sogar dann erklärt, wenn  $n$  eine beliebige reelle Zahl ist; in dem speziellen Fall, dass  $n$  eine natürliche Zahl ist, aber  $n < k$ , ergibt sich  $\binom{n}{k} = 0$ . Mehr dazu in Kapitel 12.

Die wichtigste kombinatorische Interpretation des Binomialkoeffizienten  $\binom{n}{k}$  ist die als *Anzahl aller  $k$ -elementigen Teilmengen einer  $n$ -Menge*. Das beweisen wir gleich, doch wir erleichtern uns das Leben, indem wir eine Schreibweise einführen, die nach dem nächsten Hilfssatz sehr intuitiv sein wird.

**3.3.1 Definition.** Sei  $X$  eine Menge und sei  $k$  eine nicht negative ganze Zahl. Mit

$$\binom{X}{k}$$

bezeichnen wir die Menge aller  $k$ -elementigen Teilmengen der Menge  $X$ .

Zum Beispiel ist  $\binom{\{a,b,c\}}{2} = \{\{a,b\}, \{a,c\}, \{b,c\}\}$ . Die Bedeutung von  $\binom{x}{k}$  hat ab jetzt also zwei Bedeutungen, je nachdem, ob  $x$  eine Zahl ist oder eine Menge. Was nun folgt, setzt diese beiden Bedeutungen zueinander in Beziehung:

**3.3.2 Hilfssatz.** Eine endliche Menge  $X$  hat  $\binom{|X|}{k}$   $k$ -elementige Teilmengen.

Als Formel:

$$\left| \binom{X}{k} \right| = \binom{|X|}{k}.$$

*Beweis.* Setze  $n = |X|$ . Wir zählen alle *geordneten*  $k$ -Tupel (d.h. ohne Wiederholung) von Elementen aus  $X$  auf zwei verschiedene Arten. Einerseits wissen wir aus Hilfssatz 3.1.4 (und der darauf folgenden Bemerkung), dass die Anzahl der geordneten  $k$ -Tupel  $n(n-1)\dots(n-k+1)$  ist. Andererseits können wir aus einer  $k$ -elementigen Teilmenge  $M \in \binom{X}{k}$  auf  $k!$  verschiedene Arten geordnete

$k$ -Tupel erzeugen, und jedes geordnete  $k$ -Tupel erhalten wir so aus genau einer  $k$ -elementigen Teilmenge  $M$ . Also ist

$$n(n-1)\dots(n-k+1) = k! \left| \binom{X}{k} \right|.$$

□

**Eine völlig andere Fragestellung führt auch auf die Binomialkoeffizienten.** Auf wie viele verschiedene Arten lässt sich eine ganze Zahl  $m \geq 0$  als Summe von genau  $r$  ganzen Zahlen  $i_1 \geq 0, i_2 \geq 0, \dots, i_r \geq 0$  schreiben? Die Reihenfolge der Summanden soll dabei eine Rolle spielen. Für  $n = 3$  und  $r = 2$  gibt es z.B. die vier Möglichkeiten  $3 = 0 + 3$ ,  $3 = 1 + 2$ ,  $3 = 2 + 1$  und  $3 = 0 + 3$ . Anders gesagt: Wir möchten die Anzahl der geordneten  $r$ -Tupel  $(i_1, i_2, \dots, i_r)$  nicht negativer ganzer Zahlen bestimmen, die folgende Gleichung erfüllen:

$$i_1 + i_2 + \dots + i_r = m. \quad (3.2)$$

Diese Anzahl ist der Binomialkoeffizient  $\binom{m+r-1}{r-1}$ . Dafür gibt es unter anderem den folgenden verblüffenden Beweis.

Stellen wir uns  $r$  Schachteln vor, nummeriert von 1 bis  $r$  (das soll heißen, wir können die Schachteln voneinander unterscheiden). Außerdem haben wir  $m$  gleichartige Kugeln (d.h. wir können die Kugeln nicht voneinander unterscheiden). Nun verteilen wir die Kugeln irgendwie auf die Schachteln und bezeichnen die Anzahl der Kugeln in den Schachteln mit  $i_1, i_2, \dots, i_r$ . Wir nehmen an, dass jede der Schachteln groß genug ist um alle  $m$  Kugeln aufzunehmen. Die möglichen Verteilungen der Kugeln auf die Schachteln codieren uns gerade die Lösungen von Gleichung (3.2). Zu der Lösung  $0 + 1 + 0 + 3 + 1 + 2 = 7$  (für  $m = 7$  und  $r = 6$ ) gehört z.B. die Verteilung



Uns interessiert also, auf wie viele Arten wir  $m$  ununterscheidbare Kugeln auf  $r$  unterscheidbare Schachteln verteilen können. Im nächsten Bild lassen wir einfach den Boden und die linke und rechte Außenwand weg; es bleiben  $m$  Kugeln und  $r - 1$  Trennwände übrig:



Durch diese „Vereinfachung“ ist keine Information verloren gegangen, das neue Bild beschreibt immer noch eindeutig eine Verteilung von Kugeln auf Schachteln. Eine solche Verteilung auszuwählen ist also gleichbedeutend damit, die Position der Trennwände zwischen den Kugeln festzulegen. Analysieren wir diese Situation:  $m + r - 1$  Objekte, Kugeln und Trennwände, sind in einer Reihe angeordnet, und wir dürfen bestimmen, an welche Stellen Kugeln und an welche Stellen Trennwände sollen. Dazu legen wir die  $r - 1$  Stellen für die Trennwände fest, und das können wir auf  $\binom{m+r-1}{r-1}$  Arten tun.  $\square$

**Einfache Eigenschaften der Binomialkoeffizienten.** Eine ganz wichtige Formel ist

$$\binom{n}{k} = \binom{n}{n-k}. \quad (3.3)$$

Dass sie stimmt, sieht man direkt an der oben schon erwähnten Formel  $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ . Die kombinatorische Bedeutung von Gleichung (3.3) ist, dass die Anzahl der  $k$ -elementigen Teilmengen einer  $n$ -Menge die gleiche ist wie die der Teilmengen mit  $n - k$  Elementen. Klar, es sind nur verschiedene Sichtweisen der gleichen Situation: Einmal wählt man  $k$  Elemente für die Teilmenge aus, das andere Mal wählt man die  $n - k$  Elemente, die nicht in die Teilmenge sollen. Oder, korrekt gesprochen, es gibt eine Bijektion zwischen den  $k$ - und den  $n - k$ -elementigen Teilmengen einer  $n$ -Menge, nämlich die Abbildung, die jeder Menge ihr Komplement zuordnet.

Die folgende Formel ist nach Pascal benannt und ist die definierende Eigenschaft des *Pascalschen Dreiecks* (siehe unten).

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}. \quad (3.4)$$

Unser Beweis beruht auf einer kombinatorischen Interpretation. Die rechte Seite ist gleich der Anzahl der  $k$ -elementigen Teilmengen einer  $n$ -Menge  $X$ . Wir wählen ein Element  $a \in X$  und teilen die  $k$ -elementigen Teilmengen von  $X$  in zwei Gruppen ein, je nachdem, ob sie das Element  $a$  enthalten oder nicht. Die Teilmengen, die  $a$  nicht enthalten, sind genau die  $k$ -elementigen Teilmengen von  $X \setminus \{a\}$ , also  $\binom{n-1}{k}$  viele. Aus den  $k$ -elementigen Teilmengen  $A \subseteq X$ , die das Element  $a$  enthalten, entfernen wir das Element  $a$  und erhalten so genau die  $(k-1)$ -elementigen Teilmengen  $A' \subseteq X \setminus \{a\}$ . (Bitte überzeugen Sie sich, dass man auf diese Weise eine Bijektion erhält zwischen

allen  $k$ -elementigen Teilmengen von  $X$ , die das Element  $a$  enthalten, und allen  $(k-1)$ -elementigen Teilmengen  $X \setminus \{a\}$ .) Davon gibt es  $\binom{n-1}{k-1}$ . Zusammen heißt das, dass die Anzahl aller  $k$ -elementigen Teilmengen von  $X$  gleich  $\binom{n-1}{k} + \binom{n-1}{k-1}$  ist.  $\square$

Gleichung (3.4) hängt eng mit dem so genannten *Pascalschen Dreieck* zusammen:

$$\begin{array}{ccccccc}
 & & & & 1 & & \\
 & & & & 1 & 1 & \\
 & & & & 1 & 2 & 1 \\
 & & & & 1 & 3 & 3 & 1 \\
 & & & & 1 & 4 & 6 & 4 & 1 \\
 1 & 5 & 10 & 10 & 5 & 1 \\
 \vdots & & \vdots & & \vdots & &
 \end{array}$$

Ganz oben steht eine 1, und aus einer Zeile konstruiert man die darunter folgende so: Unter je zwei aufeinanderfolgenden Zahlen schreibe ihre Summe. Ergänze am Rand Einsen. Diese Konstruktionsvorschrift ist sozusagen eine Definition mittels vollständiger Induktion; solch eine Definition nennt man eine *rekursive Definition*. Mit vollständiger Induktion und unter Ausnutzen von Gleichung (3.4) kann man ganz einfach zeigen, dass in der  $(n+1)$ -ten Zeile die Binomialkoeffizienten  $\binom{n}{0}, \binom{n}{1}, \dots, \binom{n}{n}$  stehen.

**Der Binomialsatz.** Sicher erinnern Sie sich noch (mit Schrecken oder mit Sympathie?) an die *binomischen Formeln*. Die eine ist  $(a+b)^2 = a^2 + 2ab + b^2$ , wissen Sie die beiden anderen noch? Der nun folgende Binomialsatz ist eine Verallgemeinerung für beliebige Exponenten; wir zeigen ihn hier in leicht vereinfachter Form. Sie können ihn z.B. mit Induktion und Gleichung (3.4) beweisen.

**3.3.3 Satz (Binomialsatz).** Für jede ganze Zahl  $n \geq 0$  gilt

$$(1+x)^n = \sum_{k=0}^n \binom{n}{k} x^k$$

(dies ist eine Aussage über die Gleichheit zweier Polynome in der Variablen  $x$ ; insbesondere gilt die Gleichheit für jede reelle Zahl, die man für  $x$  einsetzt).

Aus dem Binomialsatz können wir viele weitere Eigenschaften der Binomialkoeffizienten herleiten. Die vielleicht einfachste erhält man, indem man  $x = 1$  setzt:

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n. \quad (3.5)$$

Kombinatorisch betrachtet ist dies nichts anderes, als alle Teilmengen einer  $n$ -Menge zu zählen. Auf der linken Seite sind sie nach Mächtigkeiten zusammengefasst.

**Zweiter Beweis von Hilfssatz 3.1.3 (von der Anzahl der Teilmengen mit ungerader Mächtigkeit).** Setzen wir im Binomial-  
satz  $x = -1$  ein, erhalten wir

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \cdots = \sum_{k=0}^n (-1)^k \binom{n}{k} = 0. \quad (3.6)$$

Addieren wir dies und Gleichung (3.5), dann erhalten wir

$$2 \left[ \binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots \right] = 2^n.$$

In den eckigen Klammern steht die Gesamtzahl der geraden Teilmengen einer  $n$ -Menge. Deshalb hat eine  $n$ -Menge insgesamt  $2^{n-1}$  gerade Teilmengen. Die anderen Teilmengen sind die ungeraden, das sind  $2^n - 2^{n-1}$  viele.  $\square$

**Weitere Identitäten mit Binomialkoeffizienten.** Man kennt buchstäblich tausende von Formeln und Identitäten mit Binomialkoeffizienten, ganze Bücher sind ihnen gewidmet. Hier führen wir eine weitere Formel mit einem hübschen kombinatorischen Beweis vor. Weitere Formeln und Methoden, neue Formeln abzuleiten, kommen in den Aufgaben und in Kapitel 12.

### 3.3.4 Hilfssatz.

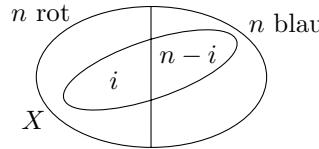
$$\sum_{i=0}^n \binom{n}{i}^2 = \binom{2n}{n}.$$

*Beweis.* Der erste Trick ist, die Symmetrie (3.3) der Binomialkoeffizienten auszunutzen und die Summe als

$$\sum_{i=0}^n \binom{n}{i} \binom{n}{n-i}$$

zu schreiben. Nun zeigen wir, dass diese Summe die  $n$ -elementigen Teilmengen einer  $2n$ -Menge zählt (was die rechte Seite der zu beweisenden Gleichung offenbar auch tut). Betrachten Sie eine  $2n$ -Menge

$X$  und färben Sie  $n$  der Elemente rot und die anderen  $n$  blau. Eine  $n$ -elementige Teilmenge von  $X$  auszuwählen ist nun das Gleiche, wie  $i$  rote und  $n - i$  blaue Elemente auszusuchen,  $i \in \{0, 1, \dots, n\}$ :



Für festes  $i$  gibt es  $\binom{n}{i}$  Möglichkeiten für die roten Elemente und (unabhängig davon)  $\binom{n}{n-i}$  Möglichkeiten für die blauen. Insgesamt können wir eine  $n$ -elementige Teilmenge von  $X$  auf  $\sum_{i=0}^n \binom{n}{i} \binom{n}{n-i}$  Arten auswählen.  $\square$

**Multinomialkoeffizienten und der Multinomialsatz.** Dies ist eine der häufigsten Aufgaben in amerikanischen Lehrbüchern: Wie viele verschiedene Worte (die nichts zu bedeuten brauchen) kann man aus den Buchstaben des Wortes MISSISSIPPI bilden? Anders ausgedrückt, wie viele Möglichkeiten haben wir, diese Buchstaben umzuordnen? Stellen Sie sich zuerst vor, dass wir alle Buchstaben in dem Wort irgendwie unterscheiden können, dass wir also 4 verschiedene S haben usw. Im Schriftbild werden wir sie durch Indizes kennzeichnen:  $M_1I_1S_1S_2I_2S_3S_4I_3P_1P_2I_4$ . Wir haben also elf verschiedene Buchstaben, die auf  $11!$  Arten umgeordnet werden können. Betrachten wir einmal ein (beliebiges) Wort, das von einem MISSISSIPPI ohne Indizes stammt, etwa SIPISMSIPIS. Aus wie vielen Worten mit Indizes erhalten wir es durch Streichen der Indizes? Die Indizes der vier S können in  $4!$  verschiedenen Anordnungen sein, die vier I unabhängig davon ebenfalls in  $4!$  Anordnungen, die zwei P in  $2!$  und schließlich das eine M in  $1!$  Anordnungen. Das Wort SIPISMSIPIS kann also (wie jedes andere Wort mit den Buchstaben aus MISSISSIPPI) auf  $4!4!2!1!$  Arten entstehen. Die Anzahl der Worte ohne Indizes, die Lösung für unser Ausgangsproblem, ist also  $11!/(4!4!2!1!)$ .

Mit dem gleichen Argument erhält man das folgende allgemeine Ergebnis: Wenn wir  $m$  Sorten von Objekten haben, jeweils  $k_i$  ununterscheidbare von der  $i$ -ten Sorte (wobei  $k_1 + k_2 + \dots + k_m = n$ ), dann ist die Anzahl verschiedener Anordnungen dieser Objekte durch den Ausdruck

$$\frac{n!}{k_1!k_2!\dots k_m!}$$

gegeben, den man gewöhnlich kurz

$$\binom{n}{k_1, k_2, \dots, k_m}$$

schreibt und als *Multinomialkoeffizienten* bezeichnet. Im Spezialfall  $m = 2$  erhalten wir einen Binomialkoeffizienten, d.h.  $\binom{n}{k, n-k}$  ist das Gleiche wie  $\binom{n}{k}$ . Der Name „Multinomialkoeffizient“ hat mit folgendem Satz zu tun:

**3.3.5 Satz (Multinomialsatz).** *Die folgende Gleichung gilt für beliebige reelle Zahlen  $x_1, x_2, \dots, x_m$  und jede natürliche Zahl  $n \geq 1$ :*

$$(x_1 + x_2 + \dots + x_m)^n = \sum_{\substack{k_1 + \dots + k_m = n \\ k_1, \dots, k_m \geq 0}} \binom{n}{k_1, k_2, \dots, k_m} x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}.$$

Die Summe auf der rechten Seite dieser Formel enthält in der Regel ziemlich viele Summanden (summiert wird über alle möglichen Arten,  $n$  als Summe von  $m$  nicht negativen ganzen Zahlen zu schreiben). Doch in den meisten Fällen verwendet man den Satz, um den Koeffizienten eines bestimmten Terms zu bestimmen. Z.B. sehen wir mühelos, dass der Koeffizient von  $x^2y^3z^5$  in  $(x+y+z)^{10}$  gleich  $\binom{10}{2,3,5} = 2520$  ist.

Den Multinomialsatz kann man mit Induktion nach  $n$  beweisen (siehe Aufgabe 26). Ein anderen, natürlicheren Beweis kann man mit den Methoden in Kapitel 12 führen.

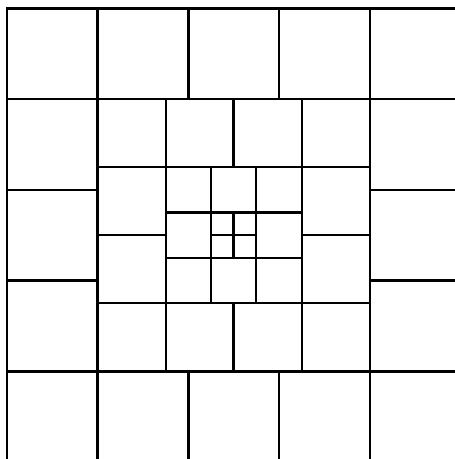
## Aufgaben

1. Verpacken Sie das Problem, alle  $k$ -elementigen Teilmengen einer  $n$ -Menge zu zählen, in eine Geschichte mit Postkarten.
2. Beweisen Sie die Pascal-Rekursion (3.4) durch Umformungen aus der Definition (3.1) der Binomialkoeffizienten.
3. (a) Beweisen Sie die Formel

$$\binom{r}{r} + \binom{r+1}{r} + \binom{r+2}{r} + \dots + \binom{n}{r} = \binom{n+1}{r+1} \quad (3.7)$$

durch Induktion über  $n$  (für beliebiges, aber festes  $r$ ). Was ist die Aussage dieser Formel für  $r = 1$ ?

- (b) \*Finden Sie für die gleiche Formel einen kombinatorischen Beweis.
4. \*Berechnen Sie die Summe  $\sum_{k=m}^n \binom{k}{m} \binom{n}{k}$  für natürliche Zahlen  $m \leq n$  (d.h. finden Sie eine einfache Formel, in der keine Summe mehr vorkommt).
  5. Berechnen Sie (d.h. finden Sie eine einfache Formel, in der keine Summe mehr vorkommt)
    - (a)  $\sum_{k=1}^n \binom{k}{m} \frac{1}{k}$ ,
    - (b) \*  $\sum_{k=0}^n \binom{k}{m} k$ .



**Abb. 3.1** Ein grafischer Beweis der Formel für  $1^3 + 2^3 + \cdots + n^3$ .

6. \*\*Beweisen Sie:

$$\sum_{k=0}^m \binom{m}{k} \binom{n+k}{m} = \sum_{k=0}^m \binom{n}{k} \binom{m}{k} 2^k.$$

7. \*Wie viele *monotone* Funktionen  $f: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$  gibt es? Monoton heißt, dass für  $i < j$  auch  $f(i) \leq f(j)$  ist.
8. Wie viele Summanden stehen auf der rechten Seite der Formel für  $(x_1 + \cdots + x_m)^n$  im Multinomialsatz?
9. \*Wie viele  $k$ -elementige Teilmengen von  $\{1, 2, \dots, n\}$  gibt es, die keine zwei aufeinanderfolgenden Zahlen enthalten?
10. (a) Berechnen Sie die Summen  $\sum_{i=2}^n i(i-1)$  und  $\sum_{i=1}^n i^2$  unter Verwendung von Formel (3.7) für  $r = 2$ .  
 (b) Berechnen Sie  $\sum_{i=1}^n i^3$  mit (a) und nochmaliger Anwendung von (3.7) für  $r = 3$ .  
 (c) \*Leiten Sie das Ergebnis aus (b) ein weiteres Mal her, diesmal mit Hilfe von Abbildung 3.1 (die Figur ist für den Fall  $n = 4$  gezeichnet).
11. Beweisen Sie den Binomialsatz mit Induktion über  $n$ .
12. Für eine reelle Zahl  $x$  und eine natürliche Zahl  $n$  bezeichne das Symbol  $x^n$  das Produkt  $x(x-1)(x-2)\dots(x-n+1)$  (die so genannte *n-te fallende Faktorielle von x*). Beweisen Sie mittels Induktion das folgende Analogon zum Binomialsatz:

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

13. Beweisen Sie die *Leibniz-Formel* für die Differenziation eines Produkts. Es seien  $u, v$  reelle Funktionen einer Variable und  $f^{(k)}$  stehe für die  $k$ -te Ableitung einer Funktion  $f$ . Dann gilt

$$(uv)^{(n)} = \sum_{k=0}^n \binom{n}{k} u^{(k)} v^{(n-k)}$$

(unter der Voraussetzung, dass alle in der Formel auftauchenden Ableitungen existieren). Der Fall  $n = 1$  ist die Formel  $(uv)' = u'v + uv'$  für die erste Ableitung eines Produkts, die Sie als bekannt voraussetzen dürfen.

14. *Inf* Schreiben Sie ein Programm, das alle  $k$ -elementigen Teilmengen der Menge  $\{1, 2, \dots, n\}$  auflistet, jede genau einmal. Achten Sie auf den Speicherbedarf, damit Sie auch dann mit dem vorhandenen Speicher auskommen, wenn  $\binom{n}{k}$ , die Anzahl dieser Teilmengen, sehr groß ist.\* Gelingt es Ihnen, die Gesamtzahl der Schritte des Algorithmus proportional zu  $\binom{n}{k}$  zu halten, wenn die für die Ausgabe notwendigen Operationen nicht gezählt werden?
15. Sei  $p$  eine Primzahl und seien  $n, k$  natürliche Zahlen.
- Zeigen Sie, dass  $\binom{p}{k}$  für  $k < p$  durch  $p$  teilbar ist.
  - Zeigen Sie, dass  $\binom{n}{p}$  genau dann durch  $p$  teilbar ist, wenn  $\lfloor n/p \rfloor$  durch  $p$  teilbar ist.
16. (a) \*Zählen Sie die Teilmengen einer  $n$ -Menge, deren Mächtigkeit ein Vielfaches von 4 ist. Verwenden Sie dazu den Binomialsatz.  
(b) \*Zählen Sie die Teilmengen einer  $n$ -Menge, deren Mächtigkeit ein Vielfaches von 3 ist.
17. Wir haben  $n$  Sorten von Objekten, und wir möchten die Anzahl der Möglichkeiten bestimmen, ein  $k$ -Tupel von Objekten auszuwählen. Wir interessieren uns dabei für verschiedene Varianten: Wir können geordnete oder ungeordnete  $k$ -Tupel auswählen, und wir können von jeder Sorte genau ein Objekt haben oder aber beliebig viele, nicht unterscheidbare. Tragen Sie die richtigen Formeln in die folgende Tabelle ein:

	Nur 1 Objekt von jeder Sorte	Beliebig viele Objekte von jeder Sorte
Geordnete $k$ -Tupel		
Ungeordnete $k$ -Tupel		

18. Wir haben  $k$  Kugeln, die wir in  $n$  (nummerierte) Schachteln verteilen. Tragen Sie die Formeln für die Anzahl der möglichen Aufteilungen für verschiedene Varianten des Problems in die folgende Tabelle ein:

	Höchstens 1 Kugel in jede Schachtel	Beliebig viele Kugeln in jede Schachtel
Kugeln unterscheidbar (verschieden gefärbt)		
Kugeln ununterscheidbar		

19. \*Sieben Elfen und 5 Kobolde sollen sich so in einer Reihe aufstellen, dass keine zwei Kobolde nebeneinander stehen. Auf wie viele Arten können sie das tun?
20. Bei einem Festmahl werden 13 Platten angerichtet. Es gibt 5 (ununterscheidbare) Hummer und 8 (ebenso ununterscheidbare) gefüllte Schnecken. Uns interessiert die Anzahl der Möglichkeiten, die Schnecken und Hummer einen nach dem anderen auf die Platten zu verteilen. Die Reihenfolge des Arrangierens ist wesentlich. (Also wie viele Drehbücher gibt es: „Lege eine Schnecke auf Platte Nr. 3. Richte einen Hummer auf Platte Nr. 11 an...“?) Auf wie viele Arten geht das,
- (a) wenn es keine weiteren Vorschriften gibt und z.B. auch alles auf der gleichen Platte angerichtet werden darf?
  - (b) wenn keine Platte leer bleiben darf?
21. Zeichnen Sie ein Dreieck  $ABC$ . Zeichnen Sie  $n$  verschiedene Punkte auf der Seite  $AB$  ein (alle verschieden von  $A$  und  $B$ ) und verbinden Sie alle durch eine gerade Linie mit der Ecke  $C$ . Zeichnen Sie auch auf der Seite  $AC$   $n$  Punkte ein, die Sie mit  $B$  verbinden.
- (a) Wie viele Schnittpunkte entstehen zwischen den neu eingezeichneten Linien? In wie viele Gebiete wird das Dreieck dadurch unterteilt?
  - (b) \*Zeichnen Sie auf der Seite  $BC$  weitere  $n$  Punkte ein, die Sie mit  $A$  verbinden. Wie viele Schnittpunkte gibt es nun (unter der Voraussetzung, dass sich keine drei Linien in einem Punkt schneiden)?
  - (c) \*In wie viele Gebiete ist das Dreieck in der Situation (b) unterteilt?
22. Untersuchen Sie ein konvexes  $n$ -Eck, in dem sich keine drei Diagonalen in einem gemeinsamen Punkt schneiden. Zeichnen Sie alle Diagonalen ein (d.h. verbinden Sie je zwei Eckpunkte durch eine Linie).
- (a) \*Wie viele Schnittpunkte erzeugen die Diagonalen?
  - (b) \*In wie viele Teile wird das Vieleck durch die Diagonalen geteilt?
23. (Cayley–Problem) \*Betrachten Sie ein reguläres konvexes  $n$ -Eck  $P$  mit Ecken  $A_1, A_2, \dots, A_n$ . Auf wie viele Arten kann man von diesen  $n$  Ecken  $k$  Stück auswählen, von denen keine zwei benachbart sind (mit

anderen Worten: Keine Seite des  $k$ -Ecks mit den ausgewählten Eckpunkten ist zugleich eine Seite des  $n$ -Ecks)? Hinweis: Berechnen Sie zuerst die Anzahl der Möglichkeiten, bei denen  $A_1$  mit ausgewählt wird.

24. \*Betrachten Sie ein regelmäßiges  $n$ -Eck. Unterteilen Sie es durch Diagonalen, die sich gegenseitig nicht schneiden, in Dreiecke (d.h. *triangulieren* Sie es), und zwar so, dass jedes der Dreiecke mindestens eine Seite hat, die auch schon im ursprünglichen  $n$ -Eck eine Außenseite war.

- (a) Wie viele Diagonalen müssen Sie einzeichnen? Wie viele Dreiecke entstehen?  
 (b) \*Wie viele solche Triangulierungen gibt es?

25. (a) Was ist der Koeffizient von  $x^2y^3z$  im Polynom  $(2x - y^2 + 3z)^6$ ? Was ist der Koeffizient von  $x^2y^2z$ ?  
 (b) Bestimmen Sie den Koeffizienten von  $x^2y^8z$  in  $(2x + y^2 - 5z)^7$ .  
 (c) Was ist der Koeffizient von  $u^2v^3z^3$  in  $(3uv - 2z + u + v)^7$ ?

26. (a) Beweisen Sie die Gleichung

$$\binom{n}{k_1, k_2, \dots, k_m} = \binom{n-1}{k_1-1, k_2, k_3, \dots, k_m} + \binom{n-1}{k_1, k_2-1, k_3, \dots, k_m} + \dots + \binom{n-1}{k_1, k_2, \dots, k_{m-1}, k_m-1}$$

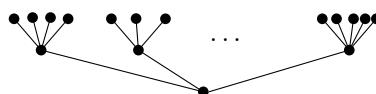
$$(n \geq 1, k_1 + \dots + k_m = n, k_i \geq 1).$$

- (b) Beweisen Sie den Multinomialssatz durch Induktion nach  $n$ .

27. Bestimmen Sie die Anzahl linearer Fortsetzungen der folgenden partiellen Ordnungen:

- (a)  $X$  ist disjunkte Vereinigung von Mengen  $X_1, X_2, \dots, X_k$  der Größe  $r_1, r_2, \dots, r_k$ . Jedes  $X_i$  ist durch  $\preceq$  linear geordnet, und keine zwei Elemente aus verschiedenen  $X_i$  sind vergleichbar.

- (b) \*Das Hasse-Diagramm von  $(X, \preceq)$  ist ein Baum wie im folgenden Bild. Die Wurzel hat  $k$  Kinder, von denen am  $i$ -ten  $r_i$  Blätter hängen.



## 3.4 Näherungen: Eine Einführung

Wenn wir eine Frage der Form „Wie viel?“ stellen, dann hoffen wir oft auf eine exakte Zahl als Antwort. So ist es z.B. für eine Millionärin angenehm zu wissen, dass sie exakt 107 343 726,12 Doublezons<sup>4</sup> besitzt. Auch bei mathematischen Zählproblemen ist das so: Eine exakte Formel empfindet man als besonders schöne Lösung, doch oft ist es schwierig eine solche anzugeben. Glücklicherweise ist das in vielen Fällen gar nicht notwendig, in vielen Fällen ist eine ungefähre Kenntnis der Lösung ausreichend. Den meisten Menschen genügt es, ihren Kontostand zwischen 4000 und 4100 Doublezons zu wissen. Häufig genügt sogar eine Abschätzung in eine Richtung: wenn wir wissen, dass ein Computerprogramm mindestens  $10^{10}$  Tage benötigt um ein Problem optimal zu lösen, dann können wir uns die Mühe sparen, genauer zu bestimmen, ob es mehr oder weniger als  $10^{12}$  Tage laufen würde.

Zuweilen fällt es schwer exakte Ergebnisse herzuleiten. Manchmal ist die Berechnung möglich, aber sehr aufwändig, manchmal übersteigt sie unsere Fähigkeiten. Wenn wir uns mit einer Näherung zufrieden geben, dann sparen wir möglicherweise Zeit und Arbeit, und — vielleicht noch wichtiger — wir erweitern den Bereich der Probleme, die wir überhaupt angehen können.

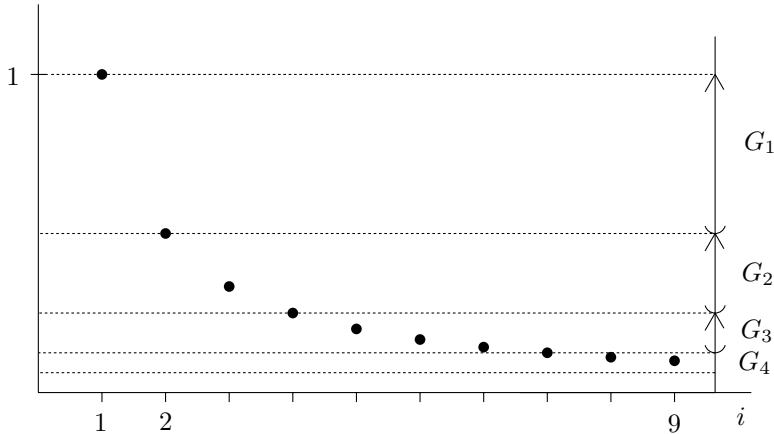
Außerdem kann eine exakte Lösung schwer zu fassen sein, so dass ein Vergleich mit anderen Größen schwer fällt. Ist die Antwort einfach eine Zahl („Wie viele Platonische Körper gibt es?“ — 5; siehe Abschnitt 6.3), gibt es natürlich keine Probleme beim Vergleich mit anderen Zahlen; die Situation ist aber ganz anders, wenn die Lösung eine Formel ist, die von einer oder gar mehreren Variablen abhängt. Solch eine Formel definiert eine Funktion, und wir möchten gerne verstehen, „wie groß“ diese Funktion ist. Die gängige Vorgehensweise ist, die in Frage kommende Funktion mit einfachen, bekannten Funktionen zu vergleichen. Wir beginnen mit einem besonders wichtigen Beispiel.

**3.4.1 Beispiel (Die harmonischen Zahlen).** Die folgende Summe ist in Mathematik und Informatik von großer Bedeutung:

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} = \sum_{i=1}^n \frac{1}{i}.$$

---

<sup>4</sup>Doublezon ist eine Währung aus dem Buch *L'Écume des jours* (Deutsche Übersetzung: *Der Schaum der Tage*) von Boris Vian.



**Abb. 3.2** Aufteilung der Folge  $(\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \dots)$  in Gruppen von gleicher Größenordnung.

Die Zahl  $H_n$  heißt die  $n$ -te *harmonische Zahl*. Man kann beweisen, dass es unmöglich ist diese Summe zu vereinfachen (es gibt keine „geschlossene Form“). Wir hätten gern eine Vorstellung davon, wie sich  $H_n$  mit wachsendem  $n$  verhält. Insbesondere möchten wir entscheiden, ob  $H_n \rightarrow \infty$  für  $n \rightarrow \infty$ .

**Eine einfache Näherung.** In diesem Fall ist es eine gute Idee, die einzelnen Summanden (also die Glieder der Folge  $\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \dots$ ) derart in Gruppen aufzuteilen, dass die Terme in jeder Gruppe von „gleicher Größenordnung“ sind. Wir legen fest, dass die  $k$ -te Gruppe  $G_k$  aus denjenigen Zahlen  $\frac{1}{i}$  besteht, für die

$$\frac{1}{2^k} < \frac{1}{i} \leq \frac{1}{2^{k-1}}$$

ist (siehe Abb. 3.2).

Das heißt,  $G_k$  enthält die  $2^{k-1}$  Zahlen

$$\frac{1}{2^{k-1}}, \frac{1}{2^{k-1}+1}, \frac{1}{2^{k-1}+2}, \dots, \frac{1}{2^k-1}.$$

Also gilt für die Summe der Terme in jeder Gruppe  $G_k$

$$\sum_{x \in G_k} x \leq |G_k| \max G_k = 2^{k-1} \frac{1}{2^{k-1}} = 1,$$

und ebenso

$$\sum_{x \in G_k} x \geq |G_k| \min G_k > 2^{k-1} \frac{1}{2^k} = \frac{1}{2}.$$

Der Term  $\frac{1}{i}$  gehört zu der Gruppe  $G_k$  mit  $2^{k-1} \leq i < 2^k$ , d.h. mit  $k = \lfloor \log_2 i \rfloor + 1$ . Deshalb kann  $H_n$  nicht größer sein als die Summe der Zahlen in den ersten  $\lfloor \log_2 n \rfloor + 1$  Gruppen, und wir haben

$$H_n = \sum_{i=1}^n \frac{1}{i} \leq \sum_{k=1}^{\lfloor \log_2 n \rfloor + 1} 1 \leq \log_2 n + 1.$$

Entsprechend erhalten wir die untere Schranke

$$H_n > \sum_{k=1}^{\lfloor \log_2 n \rfloor} \frac{1}{2} \geq \frac{1}{2} \lfloor \log_2 n \rfloor.$$

Wir schließen daraus, dass  $H_n \rightarrow \infty$  über alle Schranken wächst, aber recht langsam, etwa so langsam wie die Logarithmusfunktion. Diese Näherung ist für beliebig große Werte  $n$  brauchbar; wir bekommen durch sie eine Vorstellung von der Größe von  $H_n$ , denn wir brauchen nur den Logarithmus zu berechnen. Das Verhältnis zwischen oberer und unterer Schranke ist etwa 2, und das um so genauer, je größer  $n$  ist.

Für eine etwas pfiffigere, genauere Näherung von  $H_n$  verweisen wir auf Aufgabe 3.5.13.

Zugegeben: Es sieht so aus, als hätten wir in diesem konkreten Beispiel einfach Glück gehabt. Es scheint wie ein Wunder, dass es möglich ist die Funktion  $H_n$  recht gut durch Vielfache der Logarithmusfunktion anzunähern. Doch die Erfahrung zeigt, dass dieses Glück keine Ausnahme ist, und dass sich Funktionen (in einer Variable  $n$ ) für gewöhnlich ziemlich genau durch Allerweltsfunktionen wie  $n$ ,  $n^2$ ,  $n^{35/13}$ ,  $2^n$ ,  $3 \cdot 26^n$ ,  $3^{n^2/2}$ ,  $\ln n$ ,  $\frac{3}{11}n(\ln n)^2$  usw. annähern lassen. Allerdings ist es nicht immer einfach solche Näherungen zu bestimmen. Im Folgenden stellen wir einige Techniken vor, die bei der Suche hilfreich sein können.

**Asymptotischer Vergleich von Funktionen.** Was wir in obigem Beispiel gezeigt haben, könnten wir so beschreiben: „Die Funktion  $H_n$  ist kleiner als die Funktion  $\log_2 n + 1$ .“ Das soll heißen: Für alle  $n \in \mathbb{N}$  gilt die Ungleichung  $H_n \leq \log_2 n + 1$ . Wenn wir hingegen die Funktionen  $f(n) = 5n$  und  $g(n) = n^2$  betrachten, dann

ist (in diesem Sinne) keine von beiden „kleiner“ als die andere, denn weil  $f(1) = 5 > g(1) = 1$ , aber  $f(6) = 30 < g(6) = 36$ , gilt keine der Ungleichungen  $f(n) \leq g(n)$  und  $f(n) \geq g(n)$  für alle  $n$ . Trotzdem ist intuitiv klar (spätestens nachdem man die Funktionsgraphen skizziert hat), dass  $g$  „viel schneller wächst“ als  $f$ : Außer für einige kleine Werte von  $n$  ist  $g(n)$  stets größer als  $f(n)$ , nach anfänglichen Startschwierigkeiten läuft  $g$  davon.

In Mathematik und theoretischer Informatik vergleicht man Funktionen auf den natürlichen Zahlen meist in Bezug auf ihr *asymptotisches Verhalten*, d.h. für  $n \rightarrow \infty$ ; ihr Verhalten bei kleinen  $n$  ignoriert man. Diese Vorgehensweise bezeichnet man als *asymptotische Analyse*. Wir sprechen vom *asymptotischen Verhalten* einer Funktion oder einfach von ihrer *Asymptotik*, wenn wir sie für  $n \rightarrow \infty$  mit einfachen Funktionen vergleichen.

Angenommen  $f$  und  $g$  sind reelle Funktionen einer Variable  $n$ . Wir führen das Symbol  $f \preceq g$  ein, das bedeuten soll, dass es eine Zahl  $n_0$  gibt, so dass für alle  $n \geq n_0$  die Ungleichung  $f(n) \leq g(n)$  erfüllt ist; „letzten Endes wird  $g$  größer als  $f$ “. Im Beispiel oben würden wir also  $5n \preceq n^2$  schreiben.

Man kann die Relation  $\preceq$  als eine Art „weiches  $\leq$ “ zwischen den betrachteten Funktionen ansehen. Wenn  $f \preceq g$ , dann können wir uns sicher sein, dass  $g(n)$  größer ist als  $f(n)$ , wenn nur  $n$  groß genug ist, doch im Allgemeinen wissen wir nicht, wie groß  $n$  sein muss. Die Schreibweise  $\preceq$  unterschlägt einen Teil der Information. Dies ist einerseits eine Stärke, oft zeigt man die  $\preceq$ -Relation zwischen zwei Funktionen viel leichter als die „harte“ Relation  $\leq$ , bei der man sich genau überlegen muss, für welche  $n$  sie gilt. Auf der anderen Seite kann sich der „Benutzer“ auch betrogen fühlen: Stellen wir uns einmal vor, jemand verkauft uns einen Apparat (eine Black Box), der für jede Zahl  $n$ , die man eingibt, eine Zahl  $f(n)$  berechnet und anzeigt. Der Verkäufer garantiert uns, dass  $f(n) \preceq n$ . Wenn wir das Gefühl haben, dass er uns mit dieser Garantie betrogen hat, haben wir keine Chance das jemals zu beweisen. Denn wie viele  $n$  wir auch finden, für die  $f(n) > n$  ist, der Verkäufer kann immer behaupten, dass die Zahl  $n_0$ , auf die sich die Garantie bezieht, eben doch noch größer sei als alle unsere Beispiele.

Die Schreibweise  $f \preceq g$  ist keine Standardnotation. Sie ist aber ein erster Schritt in Richtung auf die gängigen Schreibweisen im nächsten Abschnitt, die noch etwas mehr Information unterdrücken und deshalb noch einfacher handzuhaben sind.

**Die „Oh“-Notation.** Wir führen nun die am meisten gebrauchte Schreibweise zum Vergleich der Größenordnung von Funktionen ein.

**3.4.2 Definition.** Seien  $f, g$  reelle Funktionen in einer Variable, definiert auf den natürlichen Zahlen. Wir schreiben

$$f(n) = O(g(n))$$

um auszudrücken, dass es Konstanten  $n_0$  und  $C$  gibt, so dass für alle  $n \geq n_0$  die Ungleichung  $|f(n)| \leq C \cdot g(n)$  gilt. Will man  $f(n) = O(g(n))$  laut lesen, sagt man „ $f$  ist  $O$  von  $g$ “ oder „ $f$  ist groß- $O$  von  $g$ “ (es gibt auch ein klein- $O$ ).

Die Information, die diese Schreibweise versteckt, ist der Wert der Konstanten  $C$ . Sie könnte 0,001 oder 10 oder  $10^{10}$  sein — sicher ist nur, dass so eine Konstante  $C$  existiert. Intuitiv bedeutet die Notation  $f(n) = O(g(n))$ , dass  $f$  nicht nennenswert schneller wächst als  $g$ ; eine äquivalente Formulierung ist, dass  $f(n)/g(n)$  nicht beliebig groß wird, sondern beschränkt ist. Eine typische Aussage in unserer neuen Schreibweise wäre z.B.  $10n^2 + 5n = O(n^2)$ .

Die  $O()$ -Notation ist jedoch nicht ohne Tücken: Am schlimmsten ist vielleicht, dass das Gleichheitszeichen „=“ missbraucht wird um etwas auszudrücken, das eher eine Ungleichung ist. Die Aussage  $f(n) = O(g(n))$  garantiert uns, dass  $f(n)$  nicht „gar zu groß“ wird; sie gibt *keine* Mindestgröße für  $f(n)$  an. Z.B. ist  $n + 5 = O(n^2)$  genauso wahr wie  $n + 5 = O(n)$ , wenn auch nicht ganz so aussagekräftig. Diese Asymmetrie äußert sich darin, dass rechts und links eine Rolle spielen. Auf keinen Fall darf man  $O(f(n)) = g(n)$  schreiben! Die  $O()$ -Notation ist keine schöne Schreibweise, aber sie ist praktisch, und vor allem: sie wird oft verwendet.

Komplizierte Ausdrücke werden einfacher mit der  $O()$ -Notation:

$$(7n^2 + 6n + 2)(n^3 - 3n + 2^8) = O(n^5). \quad (3.8)$$

Wieso? Zwei Grundregeln im Umgang mit der  $O()$ -Notation sind die folgenden: Gelten  $f_1(n) = O(g_1(n))$  und  $f_2(n) = O(g_2(n))$ , dann gilt auch  $f_1(n) + f_2(n) = O(g_1(n) + g_2(n))$ , und entsprechend für die Multiplikation  $f_1(n)f_2(n) = O(g_1(n)g_2(n))$  (Aufgabe 6). Weil offensichtlich  $n = O(n^2)$  und  $1 = O(n^2)$  gelten, ergibt die wiederholte Anwendung dieser beiden Regeln  $7n^2 + 6n + 2 = O(n^2 + n^2 + n^2) = O(n^2)$ , und  $n^3 - 3n + 2^8 = O(n^3)$ . Schließlich erhalten wir (nach einer letzten Anwendung der Multiplikationsregel) Gleichung (3.8). Ist es nicht praktisch, dass wir das Produkt der beiden Klammern gar nicht ausrechnen mussten?

Mit ein wenig Übung kann man Abschätzungen und Vereinfachungen wie in (3.8) einfach so hinschreiben ohne allzu viel nachdenken zu müssen, indem man schnell den dominierenden Term in einem Ausdruck ausmacht und alles andere in dem  $O()$  versteckt. Meist ist gar nicht mehr nötig als die folgenden einfachen Regeln:

**3.4.3 Tatsache (Nützliche asymptotische Ungleichungen).** Es seien  $C, a, \alpha, \beta > 0$  irgendwelche reellen Zahlen unabhängig von  $n$ . Es gilt

- (i)  $n^\alpha = O(n^\beta)$  wenn  $\alpha \leq \beta$  („ein großer Exponent dominiert einen kleineren“),
- (ii)  $n^C = O(a^n)$  für jedes  $a > 1$  („eine Exponentialfunktion dominiert jedes Polynom“),
- (iii)  $(\ln n)^C = O(n^\alpha)$  für jedes  $\alpha > 0$  („ein Polynom dominiert Logarithmen“).

(All diese Ungleichungen gelten auch für die  $\preceq$ -Relation.)

Teil (i) ist trivial, für Teil (ii) berufen wir uns auf die Analysis („einfache Übung“), und Teil (iii) leitet man aus (ii) durch Logarithmieren her.

Beim Vergleichen von Funktionen ist die  $O()$ -Notation hilfreich, im Gegensatz zum Vergleich mittels  $\preceq$  ermöglicht sie eine Aussage über die Größenordnung der Differenz. Z.B. bedeutet  $f(n) = g(n) + O(\sqrt{n})$ , dass die Funktion  $f$  sich von  $g$  höchstens um einen „Fehler“ der Größenordnung  $\sqrt{n}$  unterscheidet, d.h. dass  $f(n) - g(n) = O(\sqrt{n})$ . Ein konkretes Beispiel:  $\binom{n}{2} = n(n-1)/2 = \frac{1}{2}n^2 + O(n)$ .

Nun sehen wir uns einmal ein Beispiel an, in dem wir eine relativ komplizierte Summe abschätzen.

**3.4.4 Beispiel.** Wir betrachten  $f(n) = 1^3 + 2^3 + 3^3 + \dots + n^3$ . Gesucht ist eine gute asymptotische Näherung an  $f(n)$ .

In diesem Fall findet man sogar eine geschlossene Form für  $f(n)$  (siehe Aufgabe 3.3.10), aber man muss bereit sein dafür zu arbeiten.<sup>5</sup> Doch wir finden mit sehr viel geringerem Aufwand recht gute asymptotische Abschätzungen für  $f(n)$ . Dazu bemerken wir zunächst, dass  $f(n) \leq n \cdot n^3 = n^4$ . Andererseits ist die Hälfte der Summanden größer als  $(n/2)^3$ , deshalb ist  $f(n) \geq (n/2)^4 = n^4/16$ . Als erste Näherung sehen wir also schon, dass sich  $f(n)$  bis auf einen relativ kleinen Faktor in etwa wie die Funktion  $n^4$  verhält.

---

<sup>5</sup>Zumindest, wenn man es von Hand ausrechnen möchte; mit vielen Computeralgebra-Systemen ist es ein Kinderspiel.

Wir verbessern diese Abschätzung mit Hilfe der Summationsformel (3.7) (Aufgabe 3.3.3) mit  $r = 3$ :

$$\binom{3}{3} + \binom{4}{3} + \binom{5}{3} + \cdots + \binom{n}{3} = \binom{n+1}{4}.$$

Wir setzen  $g(k) = \binom{k}{3}$ . Dann ist  $g(k) = \frac{k(k-1)(k-2)}{3!} = \frac{k^3}{6} + O(k^2)$ . Also gilt

$$\begin{aligned} f(n) &= \sum_{k=1}^n k^3 = \sum_{k=1}^n 6g(k) + \sum_{k=1}^n [k^3 - 6g(k)] \\ &= 6\binom{n+1}{4} + O\left(\sum_{k=1}^n k^2\right) = \frac{n^4}{4} + O(n^3). \end{aligned}$$

Dabei haben wir die folgende Tatsache benutzt: Sind  $f, g$  Funktionen und ist  $f(n) = O(g(n))$ , dann ist  $\sum_{k=1}^n f(k) = O(\sum_{k=1}^n g(k))$ . Das ist nicht schwer zu beweisen.

**Weitere Bemerkungen.** Eine ähnliche „groß-Oh“-Notation ist auch für Funktionen mehrerer Variablen gebräuchlich. So bedeutet z.B.  $f(m, n) = O(g(m, n))$ , dass es Konstanten  $m_0, n_0$  und  $C$  gibt, so dass für alle  $m \geq m_0$  und  $n \geq n_0$  gilt:  $|f(m, n)| \leq C \cdot g(m, n)$ .

Es gibt noch einige weitere übliche Schreibweisen um die Größenordnung von Funktionen zu vergleichen. Sie sind sehr bequem, denn wenn man sich erst einmal an sie gewöhnt hat, dann ersetzt ein einzelnes Zeichen einen Ausdruck wie: „Es gibt eine Konstante  $c > 0$ , so dass für alle  $n \in \mathbb{N} \dots$  gilt.“ Wir wollen nicht in die Details gehen, sondern lediglich die gebräuchlichsten Symbole in der folgenden Tabelle zusammenstellen.

---

Notation	Definition	Bedeutung
$f(n) = o(g(n))$	$\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 0$	$f$ wächst viel langsamer als $g$
$f(n) = \Omega(g(n))$	$g(n) = O(f(n))$	$f$ wächst mindestens so schnell wie $g$
$f(n) = \Theta(g(n))$	$f(n) = O(g(n))$ und $f(n) = \Omega(g(n))$	$f$ und $g$ sind etwa von gleicher Größenordnung
$f(n) \sim g(n)$	$\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 1$	$f(n)$ und $g(n)$ sind fast gleich

---

Zum Abschluss wenden wir uns der Frage zu, wofür eine Aussage wie  $f(n) = O(g(n))$  gut ist. Da sie uns keine Auskunft über die

versteckte Konstante gibt, können wir nie für ein bestimmtes  $n$  eine Abschätzung für  $f(n)$  erhalten. Darauf gibt es mehrere Antworten. Zum einen interessiert in der Mathematik meist nicht das einzelne  $n$ , sondern es genügt zu wissen, dass die eine Funktion nicht wesentlich schneller wächst als die andere. Auf diese Art kann man z.B. die Existenz eines Objekts beweisen, ohne es zu konstruieren (siehe Kapitel 10 für eine solche Beweismethode). Eine andere mögliche Antwort ist, dass man die in der  $O()$ -Notation versteckte Konstante in vielen Fällen herausfinden kann, wenn man möchte. Man muss dafür die ganze Rechnung in  $O()$ -Notation noch einmal sehr genau durchgehen und über die Konstanten in allen Abschätzungen Rechenschaft ablegen. Das ist für gewöhnlich umständlich, aber möglich. Als Faustregel (mit unzähligen Ausnahmen) kann man sagen, wenn ein einfacher Beweis zu einer  $O()$ -Abschätzung führt, dann ist die versteckte Konstante nicht gar zu groß. Wenn wir zwei Funktionen  $f(n) = O(n)$  und  $g(n) = \Omega(n^2)$  haben, dann ist  $f(n)$  typischerweise kleiner als  $g(n)$  (sogar für mittelgroße  $n$ ). Weitere Bemerkungen zur  $O()$ -Notation in Verbindung mit Algorithmen folgen in Abschnitt 5.3.

## Aufgaben

1. Überzeugen Sie sich, dass die oben eingeführte Relation  $\preceq$  eine transitive Relation auf der Menge aller Funktionen  $f: \mathbb{N} \rightarrow \mathbb{R}$  ist. Finden Sie ein Beispiel für Funktionen  $f$  und  $g$ , für die weder  $f \preceq g$  noch  $g \preceq f$  gilt.
2. Finden Sie positive, monoton wachsende Funktionen  $f(n)$  und  $g(n)$ , die für alle natürlichen Zahlen  $n$  definiert sind und für die weder  $f(n) = O(g(n))$  noch  $g(n) = O(f(n))$  gilt.
3. Erklären Sie die Bedeutung der folgenden Behauptungen und klären Sie, welche davon wahr sind.
  - (a)  $n^2 = O(n^2 \ln n)$
  - (b)  $n^2 = o(n^2 \ln n)$
  - (c)  $n^2 + 5n \ln n = n^2(1 + o(1)) \sim n^2$
  - (d)  $n^2 + 5n \ln n = n^2 + O(n)$
  - (e)  $\sum_{i=1}^n i^8 = \Theta(n^9)$
  - (f)  $\sum_{i=1}^n \sqrt{i} = \Theta(n^{3/2})$ .
4. Was bedeuten:  $f(n) = O(1)$ ,  $g(n) = \Omega(1)$ ,  $h(n) = n^{O(1)}$ ? Wie kann man diese Aussagen mit wenigen Worten fassen?

5. \*Ordnen Sie die folgenden Funktionen nach ihrem Wachstum und drücken Sie die Ordnung mittels der in diesem Abschnitt eingeführten Notation aus:  $n \ln n$ ,  $(\ln \ln n)^{\ln n}$ ,  $(\ln n)^{\ln \ln n}$ ,  $n \cdot e^{\sqrt{\ln n}}$ ,  $(\ln n)^{\ln n}$ ,  $n \cdot 2^{\ln \ln n}$ ,  $n^{1+1/(\ln \ln n)}$ ,  $n^{1+1/\ln n}$ ,  $n^2$ .
6. Zeigen Sie, dass aus  $f_1(n) = O(g_1(n))$  und  $f_2(n) = O(g_2(n))$  folgt, dass  $f_1(n) + f_2(n) = O(g_1(n) + g_2(n))$  und  $f_1(n)f_2(n) = O(g_1(n)g_2(n))$ .

### 3.5 Näherungen: Fakultät

In diesem Abschnitt soll es um Näherungen für die Funktion  $n!$  (sprich:  $n$  Fakultät) gehen. Auf den ersten Blick mag es erscheinen, als würde uns die Definition der Fakultät selbst, also die Formel  $n! = n(n - 1) \dots \cdot 2 \cdot 1$ , alles über sie erzählen, was uns jemals interessieren könnte. Für kleine Werte von  $n$  kann  $n!$  sehr schnell mit einem Computer ausgerechnet werden, und für größere  $n$  denkt man vielleicht, dass die Werte der Fakultät zu groß sind, um in der „Wirklichkeit“ vorzukommen. Z. B. ist  $70! > 10^{100}$ , wie die meisten Besitzer eines Taschenrechners mit  $\boxed{n!}$ -Knopf wohl wissen. Doch in mathematischen Betrachtungen müssen wir die Größenordnung der Funktion  $n!$  oft mit anderen Funktionen vergleichen, auch für sehr große Werte von  $n$ . Dabei ist die Definition selbst nicht besonders hilfreich, und auch eine Auswertung von  $n!$  durch einen Computer ist keine Alternative. Was wir brauchen, sind Abschätzungen, die  $n!$  durch einfachere Funktionen beschränken.

Will man ein Problem angehen, dann ist es gewöhnlich eine gute Strategie zunächst nach sehr einfachen Lösungen zu suchen, die man allmählich verbessert. Als Abschätzung für  $n!$  ist ein sehr einfacher Ansatz, den wir einmal ausprobieren wollen, die Ungleichung

$$n! = \prod_{i=1}^n i \leq \prod_{i=1}^n n = n^n.$$

Und für eine sehr einfache untere Schranke können wir schreiben

$$n! = \prod_{i=2}^n i \geq \prod_{i=2}^n 2 = 2^{n-1}.$$

D.h.  $n!$  liegt irgendwo zwischen den Funktionen  $2^{n-1}$  und  $n^n$ . In vielen Fällen brauchen wir gar nicht mehr Information über  $n!$ . Doch in anderen Fällen, etwa in Beispiel 3.5.1 unten, brauchen wir genauere

Kenntnisse. Ist  $n!$  „näher an“  $n^n$  oder an  $2^{n-1}$ ? Wächst die Funktion  $\frac{n^n}{n!}$  über alle Schranken, und wenn: wie schnell tut sie das?

Bis zu einem gewissen Grade kann man auch diese Frage mit sehr einfachen Betrachtungen beantworten (ähnlich zum ersten Teil der Lösung von Beispiel 3.4.4). Ist  $n$  gerade, dann ist die Hälfte der Zahlen in der Menge  $\{1, 2, \dots, n\}$  höchstens  $\frac{n}{2}$ , und die andere Hälfte ist mindestens  $\frac{n}{2}$ . Daher gilt für gerades  $n$  einerseits

$$n! \geq \prod_{i=n/2+1}^n i > \prod_{i=n/2+1}^n \frac{n}{2} = \left(\frac{n}{2}\right)^{n/2} = \left(\sqrt{\frac{n}{2}}\right)^n \quad (3.9)$$

und andererseits

$$n! \leq \left(\prod_{i=1}^{n/2} \frac{n}{2}\right) \left(\prod_{i=n/2+1}^n n\right) = \frac{n^n}{2^{n/2}}. \quad (3.10)$$

Für ungerades  $n$  muss man ein bisschen vorsichtiger sein, doch es stellt sich heraus, dass diese beiden Formeln  $n! > \left(\sqrt{n/2}\right)^n$  und  $n! \leq n^n/2^{n/2}$  auch für alle ungeraden  $n \geq 3$  gelten (Aufgabe 1). Aus Gleichung (3.9) lesen wir ab, dass  $n!$  wesentlich schneller wächst als  $2^n$ ; tatsächlich wächst  $n!$  früher oder später schneller als jede Funktion  $C^n$  für eine feste Zahl  $C$ . Gleichung (3.10) erzählt uns, dass  $n^n$  noch schneller wächst als  $n!$ .

Es folgt ein einfaches Beispiel, in dem die Frage nach dem Vergleich von  $n^n$  und  $n!$  ganz natürlich auftaucht.

**3.5.1 Beispiel.** Von  $n$  Personen zieht jede zufällig eine Karte aus einem Stapel mit  $n$  Karten, merkt sich die Karte, und steckt sie zurück in den Stapel. Wie groß ist die Wahrscheinlichkeit, dass keine zweite Person die gleiche Karte zieht? Gibt es eine ernstzunehmende Chance, oder ist es eher unwahrscheinlich? Mathematisch gesprochen: Wie groß ist die Wahrscheinlichkeit, dass eine zufällige Abbildung der Menge  $\{1, 2, \dots, n\}$  in sich selbst eine Permutation ist?

Die Anzahl aller Abbildungen ist  $n^n$ , die Anzahl der Permutationen ist  $n!$ , also ist die gesuchte Wahrscheinlichkeit  $n!/n^n$ . Aus der oberen Schranke (3.10) berechnen wir

$$\frac{n!}{n^n} \leq \frac{n^n/2^{n/2}}{n^n} = 2^{-n/2}.$$

Also ist die Wahrscheinlichkeit höchstens  $2^{-n/2}$ , und außer wenn  $n$  sehr klein ist, ist das betrachtete Ereignis extrem unwahrscheinlich. Aus

präziseren Abschätzungen für  $n!$ , die wir im Weiteren herleiten werden, werden wir sehen, dass die gesuchte Wahrscheinlichkeit sich in etwa wie die Funktion  $e^{-n}$  verhält.

**Eine einfache Näherung nach Gauß.** Wir zeigen eine elegante Näherung, die (3.9) und (3.10) ähnelt, aber etwas stärker ist. Der Beweis ist auch von historischem Interesse, weil er von dem großen Mathematiker Gauß erfunden wurde, und wir lernen dabei eine wichtige, oft nützliche Gleichung kennen.

**3.5.2 Satz.** Für jedes  $n \geq 1$  gilt

$$n^{n/2} \leq n! \leq \left(\frac{n+1}{2}\right)^n.$$

Wir beginnen den Beweis mit der Ungleichung vom arithmetischen und geometrischen Mittel zweier Zahlen. Für positive Zahlen  $a, b$  definieren wir den *arithmetischen Mittelwert* von  $a$  und  $b$  als  $\frac{a+b}{2}$ , und den *geometrischen Mittelwert*<sup>6</sup> von  $a$  und  $b$  als  $\sqrt{ab}$ .

**3.5.3 Lemma (Ungleichung vom arithmetischen und geometrischen Mittel).** Für je zwei positive reelle Zahlen  $a$  und  $b$  ist das geometrische Mittel höchstens so groß wie das arithmetische Mittel.

*Beweis.* Es gilt  $(\sqrt{a} - \sqrt{b})^2 \geq 0$ , weil das Quadrat jeder reellen Zahl positiv ist. Daraus erhalten wir durch Ausmultiplizieren der linken Seite  $a - 2\sqrt{ab} + b \geq 0$ ; wir addieren  $2\sqrt{ab}$  zu beiden Seiten dieser Ungleichung, dividieren durch 2 und erhalten  $\sqrt{ab} \leq \frac{a+b}{2}$ . Dies ist die zu beweisende Ungleichung.  $\square$

*Beweis von Satz 3.5.2.* Die Idee ist, jede Zahl  $i \in \{1, 2, \dots, n\}$  zusammen mit ihrer „Cousine“  $n+1-i$  zu betrachten und jedes Produkt  $i(n+1-i)$  nach oben und nach unten abzuschätzen. Während  $i$  die Werte  $1, 2, \dots, n$  durchläuft, durchläuft  $n+1-i$  die Werte  $n, n-1, \dots, 1$ . Das Produkt

$$\prod_{i=1}^n i(n+1-i)$$

enthält deshalb jeden Faktor  $j \in \{1, 2, \dots, n\}$  genau zweimal, hat also den Wert  $(n!)^2$ . Also gilt

$$n! = \prod_{i=1}^n \sqrt{i(n+1-i)}. \quad (3.11)$$

---

<sup>6</sup>Ist  $g$  der geometrische Mittelwert von  $a$  und  $b$ , dann besitzt ein Rechteck mit den Seitenlängen  $a$  und  $b$  den gleichen Flächeninhalt wie ein Quadrat mit der Seitenlänge  $g$ . Das ist wohl der Grund für den Namen „geometrischer“ Mittelwert.

Setzen wir in der Ungleichung vom arithmetischen und geometrischen Mittel  $a = i$  und  $b = n + 1 - i$ , erhalten wir

$$\sqrt{i(n+1-i)} \leq \frac{i+n+1-i}{2} = \frac{n+1}{2},$$

und mit (3.11)

$$n! = \prod_{i=1}^n \sqrt{i(n+1-i)} \leq \prod_{i=1}^n \frac{n+1}{2} = \left(\frac{n+1}{2}\right)^n,$$

womit die obere Schranke in Satz 3.5.2 bewiesen ist.

Um die untere Schranke für  $n!$  zu beweisen, genügt es,  $i(n+1-i) \geq n$  für alle  $i = 1, 2, \dots, n$  zu beweisen. Für  $i = 1$  und  $i = n$  berechnen wir direkt  $i(n+1-i) = n$ . Für  $2 \leq i \leq n-1$  steht da ein Produkt zweier Zahlen, von denen die größere mindestens  $\frac{n}{2}$  und die kleinere mindestens 2 ist; also ist  $i(n+1-i) \geq n$  für alle  $i$ . Damit ist  $n! \geq \sqrt{n^n} = n^{n/2}$ , was wir beweisen wollten.  $\square$

Nachdem wir nun einige Abschätzungen für  $n!$  kennen, können wir weiter bohren und uns z.B. fragen, ob  $(\frac{n+1}{2})^n/n!$  gegen unendlich strebt, wenn ja wie schnell, usw. Wir lassen ein paar Schritte aus (das ist so in Büchern) von diesem langsamem Prozess des Sich-Vortastens und beweisen Schranken, die  $n!$  bis auf einen Faktor von  $n$  abschätzen (bedenken Sie, dass in den bisherigen Abschätzungen unsere Unsicherheit noch mindestens exponentiell in  $n$  war). In diesen Abschätzungen begegnet uns die so genannte *Eulersche Zahl*  $e = 2,718281828\dots$ , die Basis des natürlichen Logarithmus. Das Studium dieser bemerkenswerten Zahl gehört in das Gebiet der Analysis, hier benötigen wir nur das Folgende:

**3.5.4 Tatsache.** *Für jede reelle Zahl  $x$  gilt*

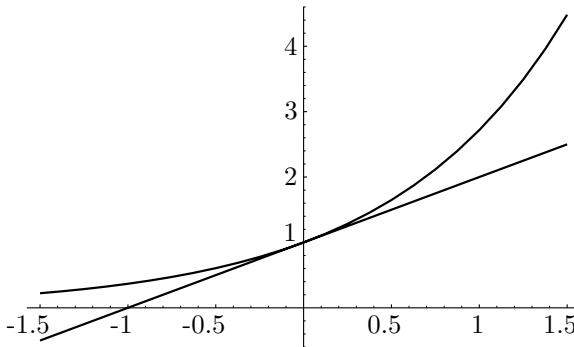
$$1 + x \leq e^x$$

(siehe Abb. 3.3).

Diese Tatsache gehört unbedingt zum Repertoire eines jeden, der sich an asymptotischen Abschätzungen versucht. Hier benutzen wir sie zum Beweis des folgenden Satzes:

**3.5.5 Satz.** *Für jedes  $n \geq 1$  ist*

$$e \left(\frac{n}{e}\right)^n \leq n! \leq en \left(\frac{n}{e}\right)^n.$$



**Abb. 3.3** Die Funktionen  $y = 1+x$  und  $y = e^x$  in der Nähe des Ursprungs.

**Erster Beweis (Induktion).** Wir beweisen nur die obere Schranke  $n! \leq en(n/e)^n$  und überlassen die untere dem Leser als Aufgabe 9. Für  $n = 1$  wird die rechte Seite der Gleichung 1, also gilt die Ungleichung. Nehmen wir an, dass die Ungleichung für  $n - 1$  schon bewiesen ist, und wir zeigen Sie nun für  $n$ . Es gilt

$$n! = n \cdot (n-1)! \leq n \cdot e(n-1) \left( \frac{n-1}{e} \right)^{n-1}$$

nach Induktionsvoraussetzung. Wir formen die rechte Seite um:

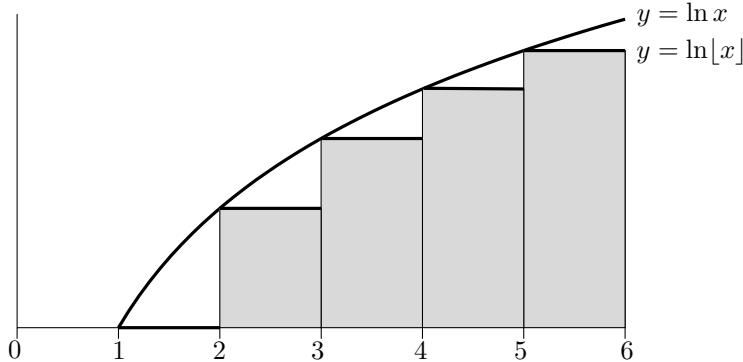
$$\left[ en \left( \frac{n}{e} \right)^n \right] \cdot \left( \frac{n-1}{n} \right)^n e.$$

In den eckigen Klammern haben wir schon die obere Schranke für  $n!$ , die wir beweisen möchten. Es genügt also zu zeigen, dass der andere Teil in diesem Ausdruck nicht größer werden kann als 1. Mit Umformen und Ausnutzen von Tatsache 3.5.4 erhalten wir

$$e \left( \frac{n-1}{n} \right)^n = e \left( 1 - \frac{1}{n} \right)^n \leq e \left( e^{-1/n} \right)^n = e \cdot e^{-1} = 1.$$

□

Übrigens ist Tatsache 3.5.4 die *einige* Eigenschaft der Zahl  $e$ , die wir im Beweis verwendet haben; der Zahlenwert von  $e$  hat beispielsweise gar keine Rolle gespielt. Nun ist es allerdings so, dass  $e$  durch Tatsache 3.5.4 charakterisiert ist: Ist  $a$  eine reelle Zahl mit der Eigenschaft  $1+x \leq a^x$  für alle  $x \in \mathbb{R}$ , dann muss  $a = e$  sein. Existenz und Eindeutigkeit einer reellen Zahl  $e$  mit eben dieser Eigenschaft beweist man in der Analysis.



**Abb. 3.4** Vergleich der Fläche unter der Treppenfunktion mit der Fläche unter der Kurve (Näherung durch ein Integral).

**Zweiter Beweis von Satz 3.5.5 (mit einem Integral).** Wieder zeigen wir nur die obere Schranke. Wir beginnen mit der Form  $n! = 1 \cdot 2 \cdot \dots \cdot n$  und wenden auf beide Seiten den natürlichen Logarithmus (d.h. den Logarithmus zur Basis  $e$ ) an. So erhalten wir

$$\ln n! = \ln 1 + \ln 2 + \dots + \ln n.$$

Den Ausdruck auf der rechten Seite können wir als Inhalt der Fläche auffassen, die von der  $x$ -Achse, von der Treppenfunktion  $x \mapsto \lfloor \ln x \rfloor$ , der linken Begrenzung  $x = 1$  und der rechten Begrenzung  $x = n + 1$  eingeschlossen wird; siehe Abbildung 3.4.

Weil in diesem Intervall  $\lfloor \ln x \rfloor \leq \ln x$  ist, ist der Flächeninhalt unter der Treppenfunktion nicht größer als der Flächeninhalt unter der Funktion  $x \mapsto \ln x$  im Intervall  $[1, n + 1]$ . Diesen können wir durch ein Integral ausdrücken:

$$\ln n! \leq \int_1^{n+1} \ln x \, dx = (n+1) \ln(n+1) - n$$

(diese Rechnung ist eine elementare Integrationsaufgabe). Weitere Umformung ergibt

$$n! \leq e^{(n+1) \ln(n+1) - n} = \frac{(n+1)^{n+1}}{e^n}.$$

Das ist noch nicht die Form, die wir wünschen; doch wenn wir diese Ungleichung für  $n-1$  statt  $n$  anwenden, erhalten wir die gesuchte Formel

$$n! = n \cdot (n-1)! \leq n \cdot \frac{n^n}{e^{n-1}} = en \left(\frac{n}{e}\right)^n.$$

□

Ein aufmerksamer Leser mag sich fragen, woher beim zweiten Beweis die Zahl  $e$  auftaucht. Es sieht fast so aus, als hätten wir  $e$  künstlich eingeführt, indem wir die Rechnung mit dem natürlichen Logarithmus von  $n!$  begonnen haben, das heißt mit dem Logarithmus zur Basis  $e$ . Es stellt sich allerdings heraus, dass  $e$  auch dann in der vorkommt, wenn wir den Logarithmus zu irgendeiner anderen Basis wählen. Aber die Rechnung wird dann komplizierter.

Wir möchten unbedingt eine noch wesentlich präzisere Näherung für  $n!$  angeben, die unter dem Namen *Stirling Formel* bekannt ist. Für die Funktion

$$f(n) = \sqrt{2\pi n} \left(\frac{n}{e}\right)^n,$$

wobei  $\pi = 3,1415926535\dots$  der Flächeninhalt des Einheitskreises ist, gilt  $f(n) \sim n!$ . Ausgeschrieben heißt das

$$\lim_{n \rightarrow \infty} \frac{f(n)}{n!} = 1.$$

Wenn wir also  $n!$  durch  $f(n)$  abschätzen, dann strebt der relative Fehler dieser Näherung für  $n \rightarrow \infty$  gegen 0. Ein Beispiel: Für  $n = 8$  ist der Fehler etwa 1%. Übrigens liegt die Stirling Formel ungefähr „in der Mitte“ zwischen den beiden Abschätzungen aus Satz 3.5.5 (siehe auch Aufgabe 10). Der Beweis der Stirling Formel verlangt eine ganze Portion mehr Analysis, deshalb passt er nicht so recht in dieses Buch und wir lassen ihn einfach aus. Wenn Sie ihn dennoch kennen lernen möchten, können Sie z.B. im Knuth [44] nachlesen.

## Aufgaben

1. (a) Zeigen Sie, dass die Formel  $n! > \left(\sqrt{n/2}\right)^n$  für alle ungeraden  $n \geq 1$  gilt (vgl. Gleichung (3.9)).  
 (b) Zeigen Sie, dass für ungerades  $n \geq 3$  sogar  $n! \leq n^n/2^{n/2}$  ist.
2. Beweisen Sie mit Hilfe von Tatsache 3.5.4, dass
  - (a)  $(1 + \frac{1}{n})^n \leq e$  für alle  $n \geq 1$  und
  - (b) \*  $(1 + \frac{1}{n})^{n+1} \geq e$  für alle  $n \geq 1$ .
  - (c) Schließen Sie aus (a) und (b), dass  $\lim_{n \rightarrow \infty} (1 + \frac{1}{n})^n = e$ .
  - (d) Zeigen Sie  $(1 - \frac{1}{n})^n \leq \frac{1}{e} \leq (1 - \frac{1}{n})^{n-1}$ .
3. (Hier werden Analysiskenntnisse vorausgesetzt!) \*Beweisen Sie Tatsache 3.5.4.
4. Zeigen Sie:  $\sqrt[n]{n}$  konvergiert gegen 1 für  $n \rightarrow \infty$ . \*Beweisen Sie unter Verwendung von Tatsache 3.5.4, dass  $\sqrt[n]{n} - 1 \geq \frac{\ln n}{n}$  ist für alle  $n \geq 1$ .

5. Welche der folgenden Aussagen sind wahr?
- $n! \sim ((n+1)/2)^n$ ,
  - $n! \sim ne(n/e)^n$ ,
  - $n! = O((n/e)^n)$ ,
  - $\ln(n!) = \Omega(n \ln n)$ ,
  - $\ln(n!) \sim n \ln n$ .
6. (a) Für welche Paare  $(a, b)$ ,  $a, b > 0$ , gilt die Gleichung  $\sqrt{ab} = (a+b)/2$ ?  
 (b) Der *harmonische Mittelwert* zweier positiver reellen Zahlen  $a, b$  ist definiert als  $2ab/(a+b)$ . Vermuten Sie, gestützt auf Beispiele, eine Ungleichung, die das harmonische Mittel mit dem geometrischen und arithmetischen Mittel in Beziehung setzt und \*beweisen Sie sie.
7. Es seien  $x_1, x_2, \dots, x_n$  positive reelle Zahlen. Ihr *arithmetisches Mittel* ist  $(x_1 + x_2 + \dots + x_n)/n$ , ihr *geometrisches Mittel* ist  $\sqrt[n]{x_1 x_2 \dots x_n}$ . Mit  $AG(n)$  bezeichnen wir die Aussage: „Für jedes  $n$ -Tupel  $x_1, x_2, \dots, x_n$  positiver reeller Zahlen ist der geometrische Mittelwert kleiner oder gleich dem arithmetischen Mittelwert.“ Beweisen Sie  $AG(n)$  für alle  $n$  mit der folgenden etwas eigenartigen Induktion:
- Zeigen Sie, dass aus  $AG(n)$  für jedes  $n$   $AG(2n)$  folgt.
  - \*Zeigen Sie, dass aus  $AG(n)$  für jedes  $n > 1$   $AG(n-1)$  folgt.
  - Erklären Sie, warum mit (a) und (b) die Gültigkeit von  $AG(n)$  für alle  $n$  gezeigt ist.
8. (Berechnung der Zahl  $\pi$ ) \*Definieren Sie zwei Folgen  $\{a_0, a_1, a_2, \dots\}$  und  $\{b_0, b_1, b_2, \dots\}$  wie folgt:  $a_0 = 2$ ,  $b_0 = 4$ ,  $a_{n+1} = \sqrt{a_n b_n}$ ,  $b_{n+1} = 2a_{n+1}b_n/(a_{n+1} + b_n)$ . Beweisen Sie, dass beide Folgen gegen  $\pi$  konvergieren. Hinweis: Die beiden Folgen haben eine Beziehung zu regulären Vielecken mit  $2^n$  Seiten, die ganz im Einheitskreis drin liegen und dabei möglichst groß sind bzw. die den Einheitskreis ganz enthalten und dabei möglichst klein sind.
- Bemerkung.* Diese Methode  $\pi$  zu berechnen, die auf Archimedes zurückgeht, ist nicht besonders effizient. Hier ist ein Beispiel eines wesentlich schnelleren Algorithmus:  $x_1 = 2^{-3/4} + 2^{-5/4}$ ,  $y_1 = 2^{1/4}$ ,  $\pi_0 = 2 + \sqrt{2}$ ,  $\pi_n = \pi_{n-1}(x_n + 1)/(y_n + 1)$ ,  $y_{n+1} = (y_n \sqrt{x_n} + 1/\sqrt{x_n})/(y_n + 1)$ ,  $x_{n+1} = (\sqrt{x_n} + 1/\sqrt{x_n})/2$ . Die  $\pi_n$  konvergieren sehr schnell gegen  $\pi$ . Diesen und weitere  $\pi$ -Algorithmen finden Sie mitsamt der zugrunde liegenden Theorie in Borwein und Borwein [17].
9. Beweisen Sie die untere Schranke  $n! \geq e(n/e)^n$  aus Satz 3.5.5
- mit Induktion (verwenden Sie geschickt Tatsache 3.5.4) und
  - mit einem Integral.

10. (Hier werden Analysiskenntnisse vorausgesetzt!) \*Beweisen Sie die folgende obere Schranke für die Fakultät (sie ist schon recht nah an der Stirling Formel):  $n! \leq e\sqrt{n}(n/e)^n$ . Sehen Sie sich dazu den zweiten Beweis von Satz 3.5.5 noch einmal an; vom Flächeninhalt unter der Kurve  $y = \ln x$  müssen Sie die Fläche geeigneter Dreiecke subtrahieren.
11. Beweisen Sie die *Bernoulli Ungleichung*: Für jede natürliche Zahl  $n$  und für jede reelle Zahl  $x \geq -1$  gilt  $(1+x)^n \geq 1 + nx$ .
12. Beweisen Sie, dass für  $n = 1, 2, \dots$

$$2\sqrt{n+1} - 2 < 1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} \leq 2\sqrt{n} - 1.$$

13. Sei  $H_n$  definiert wie in Beispiel 3.4.1:  $H_n = \sum_{i=1}^n \frac{1}{i}$ .
  - (a) \*Beweisen Sie die Ungleichungen  $\ln n < H_n \leq \ln n + 1$  durch Induktion über  $n$  (verwenden Sie Tatsache 3.5.4).
  - (b) Lösen Sie (a) nochmals mit Hilfe von Integralen.

## 3.6 Näherungen: Binomialkoeffizienten

Im letzten Abschnitt haben wir das Verhalten der Funktion  $n!$  näher untersucht, in diesem werden wir auf ähnliche Weise die Funktion

$$\binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k(k-1)\dots\cdot 2\cdot 1} = \prod_{i=0}^{k-1} \frac{n-i}{k-i} \quad (3.12)$$

studieren. Aus der Definition von  $\binom{n}{k}$  erhalten wir sofort

$$\binom{n}{k} \leq n^k,$$

was für viele Anwendungen ausreichend ist. Ist  $k > \frac{n}{2}$ , so sollte man in einem ersten Schritt die Gleichung  $\binom{n}{k} = \binom{n}{n-k}$  anwenden.

Um eine untere Schranke für  $\binom{n}{k}$  zu finden, sehen wir uns die Definition des Binomialkoeffizienten als ein Produkt von Brüchen an, wie eben in (3.12). Für  $n \geq k > i \geq 0$  ist  $\frac{n-i}{k-i} \geq \frac{n}{k}$ , und daher ist

$$\binom{n}{k} \geq \left(\frac{n}{k}\right)^k.$$

Man erhält ziemlich gute obere und untere Schranke für  $\binom{n}{k}$  aus der Stirling Formel, mittels der Gleichung  $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ . Diese Schranken sind allerdings ein wenig unhandlich in Berechnungen, und außerdem haben wir die Stirling Formel gar nicht bewiesen. Wir wollen ein paar gute, wenn auch weniger genaue Näherungen mit verschiedenen Methoden herleiten (das Hauptziel ist dabei natürlich, diese Methoden vorzuführen).

**3.6.1 Satz.** Für jedes  $n \geq 1$  und für jedes  $k$ ,  $1 \leq k \leq n$ , ist

$$\binom{n}{k} \leq \left(\frac{en}{k}\right)^k.$$

*Beweis.* Wir zeigen sogar eine stärkere Ungleichung:

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{k} \leq \left(\frac{en}{k}\right)^k.$$

Wir beginnen mit der Behauptung des Binomialsatzes, dass für eine beliebige reelle Zahl  $n$

$$\binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n = (1+x)^n$$

ist. Im Weiteren nehmen wir außerdem an, dass  $0 < x < 1$ . Durch Weglassen einiger Summanden auf der linken Seite erhalten wir

$$\binom{n}{0} + \binom{n}{1}x + \cdots + \binom{n}{k}x^k \leq (1+x)^n,$$

und Division durch  $x^k$  führt auf

$$\frac{1}{x^k} \binom{n}{0} + \frac{1}{x^{k-1}} \binom{n}{1} + \cdots + \binom{n}{k} \leq \frac{(1+x)^n}{x^k}.$$

Jeder der Binomialkoeffizienten auf der linken Seite ist mit einem Faktor versehen, der mindestens 1 ist (wir nahmen ja an, dass  $x < 1$  ist), und also kann die linke Seite nicht größer werden, wenn wir alle diese Faktoren durch 1 ersetzen. Wir erhalten

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{k} \leq \frac{(1+x)^n}{x^k}.$$

Die Zahl  $x \in (0, 1)$  kann noch beliebig gewählt werden, wir tun es so, dass die rechte Seite möglichst klein wird. Ein guter Wert ist  $x = \frac{k}{n}$ . Setzen wir diesen Wert auf der rechten Seite ein, erhalten wir

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{k} \leq \left(1 + \frac{k}{n}\right)^n \left(\frac{n}{k}\right)^k.$$

Schließlich benutzen wir noch Tatsache 3.5.4 und bekommen

$$\left(1 + \frac{k}{n}\right)^n \leq \left(e^{k/n}\right)^n = e^k,$$

woraus die Ungleichung in Satz 3.6.1 folgt.  $\square$

Der Trick, den wir in diesem Beweis benutzt haben, stammt aus dem Umkreis der *erzeugenden Funktionen*, der vielleicht mächtigsten bekannten Technik für asymptotische Abschätzungen. In Kapitel 12 werden wir etwas über erzeugende Funktionen lernen, doch die ganze Stärke dieses Zugangs zu asymptotischen Schranken kann man erst würdigen, wenn man sich auch in der Funktionentheorie auskennt.

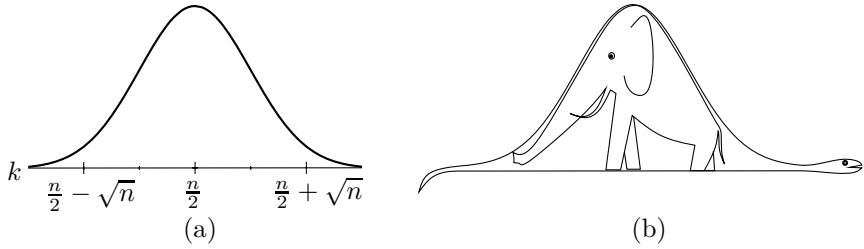
**Der Binomialkoeffizient  $\binom{n}{\lfloor n/2 \rfloor}$ .** Aus der Definition des Binomialkoeffizienten können wir problemlos die folgende Formel ableiten:

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

Für  $k \leq n/2$  ist daher  $\binom{n}{k} > \binom{n}{k-1}$ , und für  $k \geq n/2$  erhalten wir  $\binom{n}{k} > \binom{n}{k+1}$ . Für festes  $n$  sind deshalb die „mittleren“ Binomialkoeffizienten die größten; ist  $n$  gerade, so ist  $\binom{n}{n/2}$  größer als alle anderen, und für ungerades  $n$  sind  $\binom{n}{\lfloor n/2 \rfloor}$  und  $\binom{n}{\lceil n/2 \rceil}$  die größten Binomialkoeffizienten  $\binom{n}{k}$ .

Das Verhalten des Binomialkoeffizienten  $\binom{n}{k}$  als Funktion von  $k$  ist in Abb. 3.5(a) illustriert (für festes  $n$  und  $k$  nahe  $n/2$ ). Der Graph der Funktion  $\binom{n}{k}$  ist eigentlich gar keine „richtige“ durchgehende Kurve (weil  $\binom{n}{k}$  nur für ganzzahlige  $k$  definiert ist), doch wenn  $n$  sehr groß ist, dann hat man so viele Punkte, dass sie den Eindruck einer Kurve vermitteln. Die „Höhe“ dieser glockenförmigen Kurve ist genau  $\binom{n}{\lfloor n/2 \rfloor}$ , und die „Breite“ der Glocke auf halber Höhe ist etwa  $1,5\sqrt{n}$ . Die Skalen der vertikalen und der horizontalen Achse sind also sehr verschieden: Die horizontale Achse zeigt einen  $k$ -Bereich der Länge  $3\sqrt{n}$ , während der vertikale Bereich  $\binom{n}{\lfloor n/2 \rfloor}$  ist (wir werden bald sehen, dass das beinahe  $2^n$  ist).

Wenn Sie die Funktionen  $x \mapsto e^{-x^2/2}$  zeichnen, erhalten Sie eine Kurve, die genauso aussieht wie die, die wir für die Binomialkoeffizienten gezeichnet haben, abgesehen vielleicht von einer verschiedenen Beschriftung der Achsen. Das ist so, weil die Kurve  $e^{-x^2/2}$ , die so genannte *Gaußkurve*, ein Grenzwert von Kurven von Binomialkoeffizienten für  $n \rightarrow \infty$  ist (in einem genau definierten Sinne). Die Gaußkurve spielt in Wahrscheinlichkeitstheorie, Statistik und manchem anderen Gebiet eine wichtige Rolle. Sie beschreibt z. B. eine typische Verteilung von



**Abb. 3.5** Ein Graph von  $\binom{n}{k}$  als Funktion von  $k$  in der Nähe von  $\frac{n}{2}$  (a), oder vielleicht ein Hut, oder vielleicht auch eine gewaltige Boa Constrictor, die gerade einen Elefanten verdaut (b) (siehe [30]).

Fehlern in physikalischen Messungen, den Prozentsatz von Tagen mit einer gegebenen Maximaltemperatur in einer längeren Zeitperiode usw. In der Statistik nennt man die Verteilung, die durch die Gaußkurve gegeben wird, die *Normalverteilung*. Die Gaußkurve ist eines jener allgegenwärtigen mathematischen Objekte, die in vielen, oft unerwarteten Zusammenhängen auftauchen (auch die Eulersche Zahl  $e$  ist ein solches Objekt, das man immer wieder trifft). Mehr über die Gaußkurve und ähnliche Dinge können Sie in einem Lehrbuch der Wahrscheinlichkeitstheorie finden (Wir empfehlen Grimmett und Stirzaker [21] oder auf Deutsch das Buch von Krengel [24]).

Wie groß ist der größte Binomialkoeffizient  $\binom{n}{\lfloor n/2 \rfloor}$ ? Oft ist die folgende einfache Abschätzung ausreichend:

$$\frac{2^n}{n+1} \leq \binom{n}{\lfloor n/2 \rfloor} \leq 2^n.$$

Die obere Schranke folgt aus der Gleichung  $\sum_{k=0}^n \binom{n}{k} = 2^n$ , die untere Schranke ebenfalls, weil  $\binom{n}{\lfloor n/2 \rfloor}$  der größte der  $n+1$  Binomialkoeffizienten  $\binom{n}{k}$  ist, deren Summe  $2^n$  ist.

Wir zeigen noch eine wesentlich bessere Abschätzung. Um die Notation übersichtlich zu halten, beschränken wir uns auf gerade Zahlen  $n$  und schreiben  $n = 2m$ .

**3.6.2 Hilfssatz.** Für alle  $m \geq 1$  ist

$$\frac{2^{2m}}{2\sqrt{m}} \leq \binom{2m}{m} \leq \frac{2^{2m}}{\sqrt{2m}}.$$

*Beweis.* Die Beweise der beiden Ungleichungen sind ähnlich. Betrachten wir die Zahl

$$P = \frac{1 \cdot 3 \cdot 5 \cdots (2m-1)}{2 \cdot 4 \cdot 6 \cdots 2m}$$

(in diesem Schritt ist die ganze Beweisidee versteckt). Weil

$$P = \frac{1 \cdot 3 \cdot 5 \cdots (2m-1)}{2 \cdot 4 \cdot 6 \cdots 2m} \cdot \frac{2 \cdot 4 \cdots (2m)}{2 \cdot 4 \cdots (2m)} = \frac{(2m)!}{2^{2m}(m!)^2},$$

können wir schreiben

$$P = \frac{1}{2^{2m}} \binom{2m}{m}.$$

Wir wollen also beweisen, dass

$$\frac{1}{2\sqrt{m}} \leq P \leq \frac{1}{\sqrt{2m}}.$$

Für die obere Schranke betrachten wir das Produkt

$$\left(1 - \frac{1}{2^2}\right) \left(1 - \frac{1}{4^2}\right) \cdots \left(1 - \frac{1}{(2m)^2}\right),$$

das man auch so schreiben kann:

$$\left(\frac{1 \cdot 3}{2^2}\right) \left(\frac{3 \cdot 5}{4^2}\right) \cdots \left(\frac{(2m-1)(2m+1)}{(2m)^2}\right) = (2m+1)P^2.$$

Das Produkt muss aber kleiner als 1 sein, also ist  $(2m+1)P^2 < 1$ , und deshalb  $P \leq 1/\sqrt{2m}$ .

Für die untere Schranke betrachten wir das Produkt

$$\left(1 - \frac{1}{3^2}\right) \left(1 - \frac{1}{5^2}\right) \cdots \left(1 - \frac{1}{(2m-1)^2}\right)$$

und drücken es in der Form

$$\left(\frac{2 \cdot 4}{3^2}\right) \left(\frac{4 \cdot 6}{5^2}\right) \cdots \left(\frac{(2m-2)(2m)}{(2m-1)^2}\right) = \frac{1}{2 \cdot (2m) \cdot P^2}$$

aus, womit wir  $P \geq 1/(2\sqrt{m})$  erhalten.  $\square$

Wenn man sowohl  $(2m)!$  als auch  $m!$  mit der Stirling Formel approximiert, erhält man ein noch genaueres Ergebnis:

$$\binom{2m}{m} \sim \frac{2^{2m}}{\sqrt{\pi m}}.$$

Abschätzungen dieser Art haben einen interessanten Bezug z.B. zur Zahlentheorie. Einer der berühmtesten mathematischen Sätze ist die folgende Aussage über die Dichte der Primzahlen:

**3.6.3 Satz (Primzahlsatz).** *Mit  $\pi(n)$  bezeichnen wir die Anzahl der Primzahlen, die nicht größer sind als  $n$ . Es gilt*

$$\pi(n) \sim \frac{n}{\ln n}$$

(d.h.  $\lim_{n \rightarrow \infty} \pi(n) \ln n / n = 1$ ).

Man kennt verschiedene Beweise für diesen Satz; sie alle haben gemeinsam, ziemlich kompliziert zu sein. Im vorletzten Jahrhundert<sup>7</sup> hat Tschebyschew einen einfachen Beweis für das folgende schwächere Ergebnis gefunden:

$$\pi(n) = \Theta\left(\frac{n}{\ln n}\right),$$

d.h. für alle  $n$  und gewisse Konstanten  $c_2 \geq c_1 > 0$  ist  $c_1 n / \ln n \leq \pi(n) \leq c_2 n / \ln n$ . Der Beweis beruht zum Teil auf den Abschätzungen  $\frac{2^{2m}}{2m+1} \leq \binom{2^m}{m} \leq 2^{2m}$  (siehe Aufgabe 2). Tschebyschew hat auch das so genannte *Bertrandsche Postulat* bewiesen: Für jede Zahl  $n \geq 1$  gibt es eine Primzahl  $p$  mit  $n < p \leq 2n$ . Der vielleicht einfachste bekannte Beweis macht unter anderem von den Abschätzungen aus Hilfssatz 3.6.2 Gebrauch. Wenn Sie mehr über diese interessanten Zusammenhänge erfahren möchten, dann können Sie sie z.B. in Chandrasekhar [38] nachlesen.

## Aufgaben

1. (a) Beweisen Sie die Abschätzung  $\binom{n}{k} \leq (en/k)^k$  mit Induktion nach  $k$ .  
 (b) Beweisen Sie die Abschätzung aus (a) direkt aus Satz 3.5.5.
2. (Tschebyschews Abschätzung von  $\pi(n)$ )
  - (a) Zeigen Sie, dass das Produkt aller Primzahlen  $p$  mit  $m < p \leq 2m$  höchstens  $\binom{2^m}{m}$  ist.
  - (b) \*Beweisen Sie die Abschätzung  $\pi(n) = O(n/\ln n)$  mit Hilfe von (a), wobei  $\pi(n)$  die gleiche Bedeutung hat wie im Primzahlsatz 3.6.3.
  - (c) \*Sei  $p$  eine Primzahl, und seien  $m, k$  natürliche Zahlen. Zeigen Sie: Wenn  $p^k$  die Zahl  $\binom{2^m}{m}$  teilt, dann ist  $p^k \leq 2m$ .
  - (d) Beweisen Sie mit (c), dass  $\pi(n) = \Omega(n/\ln n)$ .

## 3.7 Inklusion–Exklusion

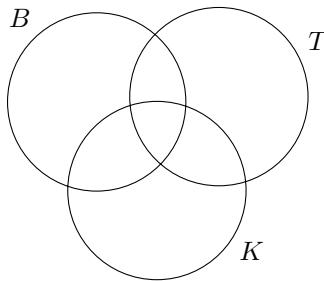
Die Geschichte von der Stadt mit den drei Vereinen ist so etwas wie das Standardbeispiel für Inklusion–Exklusion mit endlichen Mengen:

**3.7.1 Beispiel.** In der Stadt N. gibt es drei Vereine. Der Tennisclub hat 20 Mitglieder, die Briefmarkengruppe 15 und der Kleintierzüchterverein 8. Zwei der Tennisspieler und drei Briefmarkensammler züchten auch Kleintiere, sechs Einwohner spielen Tennis und sammeln Briefmarken, und ein ganz besonders eifriger Mensch engagiert sich in allen drei Vereinen. Wie viele Menschen sind insgesamt am Vereinsleben in N. beteiligt?

---

<sup>7</sup>Das ist die korrekte Übersetzung von „Within the past century“.

Zur Einstimmung bestimmen wir die Anzahl der Einwohner von N., die Mitglied im Tennisclub oder im Kleintierzüchterverein (oder in beiden) sind. Dazu haben wir die Anzahl der Tennisspieler und die der Kleintierzüchter zusammenzählen und dann die Anzahl jener Menschen abzuziehen, die in beiden Vereinen aktiv sind, denn die wurden ja zweifach gezählt bei der Summenbildung. Als Formel haben wir  $|T \cup K| = |T| + |K| - |T \cap K| = 20 + 8 - 2 = 26$ . Wenn Sie sich nicht durch die leicht kindische Fragestellung entmutigen lassen,<sup>8</sup> dann finden Sie mit ähnlichen Argumenten heraus, dass die Antwort für alle drei Vereine 33 ist. Bei der Suche nach der Lösung ist ein Bild hilfreich:



Das Prinzip der Inklusion–Exklusion erlaubt uns, das Vereinsproblem für größere Städte (mit mehr als drei Vereinen) zu lösen. Immer, wenn wir die Mächtigkeit einer Vereinigung mehrerer Mengen berechnen wollen und uns die Mächtigkeiten aller möglichen Schnitte dieser Mengen bekannt sind, können wir dieses Prinzip anwenden. Für zwei Mengen  $T$  und  $K$  haben wir die Formel oben hergeleitet, für drei Mengen  $T$ ,  $K$  und  $B$  lautet sie

$$|B \cup T \cup K| = |B| + |T| + |K| - |B \cap T| - |B \cap K| - |T \cap K| + |B \cap T \cap K|.$$

In Worten ausgedrückt: Wir erhalten die Mächtigkeit der Vereinigung, indem wir zuerst die Mächtigkeiten der drei Mengen addieren, dann die Mächtigkeiten aller paarweisen Schnittmengen subtrahieren und schließlich die Mächtigkeit des Schnitts aller drei Mengen addieren. Wir werden gleich sehen, dass diese Methode mit einer kleinen Anpassung für jede beliebige (endliche) Anzahl  $n$  von Mengen  $A_1, A_2, \dots, A_n$  funktioniert. Man erhält nämlich die Mächtigkeit  $|A_1 \cup A_2 \cup \dots \cup A_n|$  ihrer Vereinigung, indem man zuerst die Mächtigkeiten der einzelnen Mengen addiert, dann die Mächtigkeiten der

---

<sup>8</sup>Zweifellos ein Zeichen besonderer mathematischer Begabung!

paarweisen Schnitte subtrahiert, die Mächtigkeiten der Schnitte von je drei Mengen addiert, die Mächtigkeiten der vierfachen Schnitte wieder subtrahiert, usw.; im letzten Schritt addieren (wenn  $n$  ungerade) oder subtrahieren (wenn  $n$  gerade) wir die Mächtigkeit des Schnitts aller  $n$  Mengen.

Wie schreibt man das als Formel? Vielleicht so:

$$\begin{aligned} |A_1 \cup A_2 \cup \cdots \cup A_n| &= |A_1| + |A_2| + \cdots + |A_n| \\ -|A_1 \cap A_2| - |A_1 \cap A_3| - \cdots - |A_1 \cap A_n| - |A_2 \cap A_3| - \cdots - |A_{n-1} \cap A_n| \\ +|A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| \\ + \cdots + (-1)^{n-1} |A_1 \cap A_2 \cap \cdots \cap A_n|. \end{aligned}$$

Das ist ziemlich umständlich, und ehrlich: Die *Regel* wird in dieser Formulierung nicht besonders deutlich. Die folgende Variante ist schon etwas geschickter:

$$\begin{aligned} |A_1 \cup A_2 \cup \cdots \cup A_n| &= \sum_{i=1}^n |A_i| - \sum_{1 \leq i_1 < i_2 \leq n} |A_{i_1} \cap A_{i_2}| \\ &\quad + \sum_{1 \leq i_1 < i_2 < i_3 \leq n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| \\ &\quad - \cdots + (-1)^{n-1} |A_1 \cap A_2 \cap \cdots \cap A_n|. \end{aligned}$$

Wenn wir nun noch die Notation  $\binom{X}{k}$  für die Menge aller  $k$ -elementigen Teilmengen der Menge  $X$  erinnern, und wenn wir eine Schreibweise analog zu  $\sum$  erfinden, die mehrfache Vereinigungen und Schnitte ausdrückt, dann erhält die Formel eine recht elegante Gestalt:

**3.7.2 Satz (Prinzip der Inklusion–Exklusion).** Für endliche Mengen  $A_1, A_2, \dots, A_n$  gilt

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{k=1}^n (-1)^{k-1} \sum_{I \in \binom{\{1, 2, \dots, n\}}{k}} \left| \bigcap_{i \in I} A_i \right|. \quad (3.13)$$

Falls Ihnen nicht klar ist, wieso diese Formel die oben in Worte gefasste Regel ausdrückt, dann empfehlen wir Ihnen, sich die Zeit zu nehmen und Schritt für Schritt den Fall  $n = 3$  auszuarbeiten. Sie wären nicht der erste, der einen Moment der Ruhe und Überlegung benötigt. Achten Sie besonders darauf, Mengen und Zahlen sauber zu unterscheiden.

Es geht übrigens noch kürzer: Auch die folgende (teuflisch kompakt formulierte) Formel beschreibt das Prinzip der Inklusion–Exklusion:

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{\emptyset \neq I \subseteq \{1, 2, \dots, n\}} (-1)^{|I|-1} \left| \bigcap_{i \in I} A_i \right|. \quad (3.14)$$

**Erster Beweis des Prinzips der Inklusion–Exklusion: Induktion.** Wir führen Induktion nach  $n$ , der Anzahl der Mengen  $A_i$ . Den Induktionsanfang machen wir bei  $n = 2$ , denn wir werden im Induktionsschritt eben diesen Fall brauchen. Dass die Formel für  $n = 2$  gilt, haben wir aber schon in dem einleitenden Beispiel mit den Vereinen gesehen. (für  $n = 1$  ist sie auch richtig, was sagt denn dann Gleichung (3.7.2) aus?) Kommen wir nun zum Induktionsschritt. Unsere Induktionsannahme ist, dass die Formel für  $n - 1$  beliebige Mengen gültig ist.

$$\left| \bigcup_{i=1}^n A_i \right| = \left| \left( \bigcup_{i=1}^{n-1} A_i \right) \cup A_n \right| = \left| \bigcup_{i=1}^{n-1} A_i \right| + |A_n| - \left| \left( \bigcup_{i=1}^{n-1} A_i \right) \cap A_n \right|$$

(an dieser Stelle benötigen wir die Inklusion–Exklusion für zwei Mengen, d.h. die Gleichung  $|A \cup B| = |A| + |B| - |A \cap B|$  mit  $A = A_1 \cup \dots \cup A_{n-1}$ ,  $B = A_n$ )

$$= \left| \bigcup_{i=1}^{n-1} A_i \right| + |A_n| - \left| \bigcup_{i=1}^{n-1} (A_i \cap A_n) \right|$$

(wir haben auch die Distributivität des Schnitts ausgenutzt:  $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$ ; nun wenden wir die Induktionsannahme zweimal an, einmal für  $|A_1 \cup \dots \cup A_{n-1}|$  und einmal für  $|A'_1 \cup \dots \cup A'_{n-1}|$ , wobei  $A'_i = A_i \cap A_n$ )

$$\begin{aligned} &= \left( \sum_{k=1}^{n-1} (-1)^{k-1} \sum_{I \in \binom{\{1, 2, \dots, n-1\}}{k}} \left| \bigcap_{i \in I} A_i \right| \right) + |A_n| - \\ &\quad \left( \sum_{k=1}^{n-1} (-1)^{k-1} \sum_{I \in \binom{\{1, 2, \dots, n-1\}}{k}} \left| \bigcap_{i \in I \cup \{n\}} A_i \right| \right). \end{aligned}$$

Wir sind fast fertig. In der ersten Summe addieren wir (schon mit dem richtigen Vorzeichen) die Mächtigkeiten aller Schnitte, bei denen die Menge  $A_n$  keine Rolle spielt. In der zweiten Summe kommen

die Mächtigkeiten aller Schnitt vor, in denen  $A_n$  auftaucht, und der Schnitt von  $k+1$  Mengen (d.h.  $k$  der Mengen  $A_1, \dots, A_{n-1}$  sowie  $A_n$ ) erhält das Vorzeichen  $-(-1)^{k-1} = (-1)^k$ . Der Term  $|A_n|$  ist in der zweiten Summe nicht enthalten, er taucht aber gesondert zwischen den beiden Summen auf. Unterm Strich kommt jede Mächtigkeit eines Schnitts von  $k$  der Mengen  $A_1, \dots, A_n$  genau einmal vor in diesem Ausdruck, und zwar mit dem Vorzeichen  $(-1)^{k-1}$ , genau wie in Gleichung (3.13). Damit ist unser Induktionsbeweis beendet. Ohne eine vernünftige, kompakte Schreibweise würde man sich in diesem Beweis wohl schwer zurecht finden.  $\square$

**Zweiter Beweis des Prinzips der Inklusion–Exklusion: mittels Zählen.** Betrachten wir ein beliebiges Element  $x \in A_1 \cup \dots \cup A_n$ . Sein Beitrag zur Zahl auf der linken Seite von Gleichung (3.13) ist 1. Wir untersuchen nun seinen Beitrag zur rechten Seite. Dafür benennen wir die Anzahl der Mengen  $A_i$ , die  $x$  enthalten, mit  $j$ . Und wir nehmen o.B.d.A.<sup>9</sup> an, dass  $x$  in den Mengen  $A_1, A_2, \dots, A_j$  enthalten ist und in  $A_{j+1}, \dots, A_n$  nicht.

Das Element  $x$  taucht in der Schnittmenge von je  $k$  der Mengen  $A_1, A_2, \dots, A_j$  auf und sonst nicht. Weil es  $\binom{j}{k}$   $k$ -elementige Teilmengen einer  $j$ -Menge gibt, ist  $x$  in  $\binom{j}{k}$  Schnittmengen von  $k$  der Mengen enthalten. Die Mächtigkeiten der Schnitte von  $k$  Mengen werden mit dem Vorzeichen  $(-1)^{k-1}$  gezählt, also ist der Beitrag des Elements  $x$  zur rechten Seite der Inklusions–Exklusions–Formel (3.13)

$$j - \binom{j}{2} + \binom{j}{3} - \dots + (-1)^{j-1} \binom{j}{j}.$$

Nach Formel (3.6) ist die alternierende Summe der Binomialkoeffizienten 0, der obige Ausdruck ist also 1. Damit haben wir herausgefunden, dass jedes Element  $x$  auch zur rechten Seite der Gleichung (3.13) den Beitrag 1 leistet, und die Formel ist bewiesen.  $\square$

**Und noch ein Beweis.** Wenn man will, kann man das Prinzip der Inklusion–Exklusion auch als Konsequenz der folgenden Methode, ein Produkt auszumultiplizieren, ansehen:

---

<sup>9</sup>O.B.d.A. steht für „ohne Beschränkung der Allgemeinheit“; diese Floskel benutzt man, um uninteressante Schwierigkeiten in der Notation zu vermeiden. In diesem Fall brauchen wir die  $A_i$  nur umzusortieren, um  $x \in A_1, A_2, \dots, A_j$  zu erreichen. Beispiel: Ist  $n = 3$ ,  $j = 1$ ,  $x \in A_2$ ,  $x \notin A_1, A_3$ , sortieren wir einfach um:  $A'_1 = A_2$ ,  $A'_2 = A_1$ ,  $A'_3 = A_3$ . Nun rechnen wir mit den  $A'_i$  weiter.

$$(1 + x_1)(1 + x_2) \dots (1 + x_n) = \sum_{I \subseteq \{1, 2, \dots, n\}} \left( \prod_{i \in I} x_i \right). \quad (3.15)$$

Bitte machen Sie sich bewusst, was diese Formel aussagt (z.B. indem Sie sie für  $n = 1, 2, 3$  ausführlich aufschreiben) und warum sie gilt.

Um nun das Prinzip der Inklusion–Exklusion zu beweisen, setzen wir  $A = A_1 \cup A_2 \cup \dots \cup A_n$ , und  $f_i: A \rightarrow \{0, 1\}$  seien die charakteristischen Funktionen der Mengen  $A_i$ , d.h.  $f_i(a) = 1$  für  $a \in A_i$  und sonst  $f_i(a) = 0$ . Für jedes  $a \in A$  gilt  $\prod_{i=1}^n (1 - f_i(a)) = 0$  (nicht wahr?), und wenn wir in (3.15)  $x_i = -f_i(a)$  setzen, erhalten wir

$$\sum_{I \subseteq \{1, 2, \dots, n\}} (-1)^{|I|} \prod_{i \in I} f_i(a) = 0.$$

Wir addieren alle diese Gleichungen (für jedes  $a \in A$  eine), sortieren die Summanden um und erhalten

$$\begin{aligned} 0 &= \sum_{a \in A} \left( \sum_{I \subseteq \{1, 2, \dots, n\}} (-1)^{|I|} \prod_{i \in I} f_i(a) \right) \\ &= \sum_{I \subseteq \{1, 2, \dots, n\}} (-1)^{|I|} \left( \sum_{a \in A} \prod_{i \in I} f_i(a) \right). \end{aligned} \quad (3.16)$$

Mit der richtigen Interpretation der Funktion  $\prod_{i \in I} f_i(a)$  sind wir nun fertig: Es handelt sich um die charakteristische Funktion der Menge  $\bigcap_{i \in I} A_i$ , und deshalb ist  $\sum_{a \in A} \prod_{i \in I} f_i(a) = |\bigcap_{i \in I} A_i|$ . Insbesondere ist für  $I = \emptyset$  das Produkt  $\prod_{i \in \emptyset} f_i(a)$  das leere Produkt, das als 1 definiert ist, also ist  $\sum_{a \in A} \prod_{i \in \emptyset} f_i(a) = \sum_{a \in A} 1 = |A|$ . Gleichung (3.16) bedeutet also

$$|A| + \sum_{\emptyset \neq I \subseteq \{1, 2, \dots, n\}} (-1)^{|I|} \left| \bigcap_{i \in I} A_i \right| = 0,$$

was gerade das Prinzip der Inklusion–Exklusion in der Form (3.14) ist.  $\square$

**Die Bonferroni–Ungleichungen.** Manchmal sind wir in der Situation, die Mächtigkeiten aller Schnitte von bis zu  $m$  Mengen zu kennen, nicht jedoch die Mächtigkeiten von Schnitten von mehr als  $m$  Mengen. In diesem Fall können wir die Mächtigkeit der Vereinigung aller Mengen nicht exakt bestimmen (jedenfalls nicht mit Inklusion–Exklusion). Die so genannten *Bonferroni–Ungleichungen* sagen uns etwas über den Fehler, den wir machen, wenn wir alle Terme mit  $k > m$  auf der rechten Seite der Inklusions–Exklusions–Formel (3.13) weglassen: Der Fehler,

den wir so machen, hat das gleiche Vorzeichen wie der erste Term, den wir weglassen. Als Formel geschrieben ergibt sich für jedes gerade  $q$

$$\sum_{k=1}^q (-1)^{k-1} \sum_{I \in \binom{\{1, 2, \dots, n\}}{k}} \left| \bigcap_{i \in I} A_i \right| \leq \left| \bigcup_{i=1}^n A_i \right| \quad (3.17)$$

und für jedes ungerade  $q$

$$\sum_{k=1}^q (-1)^{k-1} \sum_{I \in \binom{\{1, 2, \dots, n\}}{k}} \left| \bigcap_{i \in I} A_i \right| \geq \left| \bigcup_{i=1}^n A_i \right|. \quad (3.18)$$

Wenn in Beispiel 3.7.1 also nicht bekannt ist, wie viele eifrige Einwohner von N. in allen drei Vereinen aktiv sind, dann können wir dennoch sagen, dass mindestens 32 Menschen am Vereinsleben der Stadt teilhaben (und höchstens 43, natürlich). Wir beweisen die Bonferroni–Ungleichungen hier nicht.

## Aufgaben

1. Erklären Sie, warum die Gleichungen (3.13) und (3.14) dieselbe Gleichung ausdrücken.
2. \*Beweisen Sie die Bonferroni–Ungleichungen. Wenn Ihnen der allgemeine Fall zu kompliziert erscheint, versuchen Sie wenigstens die Fälle  $q = 1$  und  $q = 2$ .
3. (Sieb des Eratosthenes) Wie viele Zahlen bleiben in  $\{1, 2, \dots, 1000\}$  übrig, wenn man alle Vielfachen von 2, 3, 5 und 7 wegstreicht?
4. Wie viele Zahlen zwischen 1 und 100 sind durch keine Quadratzahl (außer 1) teilbar?
5. \*Wie viele Anordnungen der Buchstaben A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P gibt es, aus denen man durch Streichen von Buchstaben keines der Worte BAD, DACH oder APO erhält? Wie sieht es aus, wenn wir auch MAHLEN verbieten?
6. Auf wie viele Arten können vier Amerikaner, drei Russen und fünf Chinesen eine Schlange bilden, in der keine der Nationalitäten einen Block bildet?

## 3.8 Vertauschte Hüte

**3.8.1 Problem (Die zerstreute Garderobenfrau).** Zu einem Empfang sind  $n$  Herren geladen. Sie alle tragen Zylinder, und sie alle geben ihre Zylinder an der Garderobe ab. Bei der Rückgabe ist die

Garderobenfrau nicht ganz bei der Sache — sei es, dass sie an diesem Tag zerstreut ist, sei es, dass sie halb blind ist nach jahrzehntelangem Dienst in der schlecht beleuchteten Garderobe — und gibt die Zylinder nach dem Zufallsprinzip zurück. Mit welcher Wahrscheinlichkeit bekommt keiner der Herren den richtigen Zylinder zurück?

In dieser Form ist das Problem natürlich ein Spiel, aber der mathematische Kern ist bemerkenswert; vor ein paar hundert Jahren haben sich die besten Mathematiker damit beschäftigt. Erst einmal formulieren wir das Problem mit Permutationen. Wenn wir die Herren als Nummern  $1, 2, \dots, n$  ansehen und ihre Hüte auch, dann erzeugt die Garderobenfrau durch ihr Tun eine zufällige Permutation  $\pi$  auf der Menge  $\{1, 2, \dots, n\}$ , wobei  $\pi(i)$  die Nummer des Hutes ist, den Herr Nr.  $i$  bei der Ausgabe erhält. Die Frage ist also, wie groß ist die Wahrscheinlichkeit, dass  $\pi(i) \neq i$  für alle  $i \in \{1, 2, \dots, n\}$  gilt? Ein Index  $i$  mit  $\pi(i) = i$  heißt ein *Fixpunkt* der Permutation  $\pi$ . Wir fragen also: Wie wahrscheinlich ist es, dass eine zufällig ausgewählte Permutation *fixpunktfrei* ist, also keinen Fixpunkt hat? Jede der  $n!$  möglichen Permutationen ist gleich wahrscheinlich, so wie die Garderobenfrau die Hüte zurückgibt. Bezeichnen wir die Anzahl der fixpunktfreien Permutationen<sup>10</sup> einer  $n$ -Menge mit  $D(n)$ , dann ist die gesuchte Zahl also  $D(n)/n!$ .

Mit Hilfe des Prinzips der Inklusion–Exklusion leiten wir nun eine Formel für  $D(n)$  her. Eigentlich werden wir die „bösen“ Permutationen zählen, d.h. die mit mindestens einem Fixpunkt. Sei  $S_n$  die Menge aller Permutationen von  $\{1, 2, \dots, n\}$ , und für  $i = 1, 2, \dots, n$  definieren wir  $A_i = \{\pi \in S_n : \pi(i) = i\}$ . Die „bösen“ Permutationen sind genau die in der Vereinigung aller  $A_i$ .

An dieser Stelle empfehlen wir, die Definition der Mengen  $A_i$  noch einmal ganz genau anzusehen. Die Elemente sind Permutationen, nicht Zahlen — dies ist eine häufige Quelle von Missverständnissen.

Wenn wir das Prinzip der Inklusion–Exklusion anwenden wollen, müssen wir die Mächtigkeiten der  $k$ -fachen Schnitte von Mengen  $A_i$  ausdrücken. Man sieht leicht, dass  $|A_i| = (n - 1)!$  ist, denn wenn  $\pi(i) = i$  fix ist, können wir eine beliebige Permutation der übrigen  $n - 1$  Zahlen wählen. Welche Permutationen liegen in  $A_1 \cap A_2$ ? Gerade die mit 1 und 2 als Fixpunkt (die übrigen Zahlen dürfen beliebig permutiert werden), also ist  $|A_1 \cap A_2| = (n - 2)!$ . Allgemein gilt für beliebige  $i_1 < i_2 < \dots < i_k$ , dass  $|A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_k}| =$

---

<sup>10</sup>Solche Permutationen werden manchmal Dérangements genannt.

$(n - k)!$ , und wenn wir dies in die Inklusions–Exklusions–Formel einsetzen, erhalten wir

$$|A_1 \cup \dots \cup A_n| = \sum_{k=1}^n (-1)^{k-1} \binom{n}{k} (n - k)! = \sum_{k=1}^n (-1)^{k-1} \frac{n!}{k!}.$$

Wir erinnern uns, dass wir die „bösen“ Permutationen (mit mindestens einem Fixpunkt) gezählt haben, deshalb ist

$$D(n) = n! - |A_1 \cup \dots \cup A_n| = n! - \frac{n!}{1!} + \frac{n!}{2!} - \dots + (-1)^n \frac{n!}{n!},$$

was wir auch so schreiben können:

$$D(n) = n! \left( 1 - \frac{1}{1!} + \frac{1}{2!} - \dots + (-1)^n \frac{1}{n!} \right). \quad (3.19)$$

In der Analysis lernt man, dass die Reihe in der Klammer für  $n \rightarrow \infty$  gegen  $e^{-1}$  konvergiert (dabei ist  $e$  die Eulersche Zahl), und zwar sehr schnell. Damit haben wir die Näherung  $D(n) \approx n!/e$ , und die Wahrscheinlichkeit in unserem Garderobenproblem konvergiert gegen die Konstante  $e^{-1} = 0,36787\dots$ . Ist es nicht erstaunlich, dass die Wahrscheinlichkeit in so geringem Maße von der Anzahl der Herren abhängt?

**Die Eulersche  $\varphi$ –Funktion.** Die nach dem Mathematiker Leonhard Euler benannte Funktion, die meist mit  $\varphi$  bezeichnet wird, spielt eine wichtige Rolle in der Zahlentheorie. Für eine natürliche Zahl  $n$  ist  $\varphi(n)$  als die Anzahl der natürlichen Zahlen  $m \leq n$  definiert, die zu  $n$  relativ prim sind; als Formel

$$\varphi(n) = |\{m \in \{1, 2, \dots, n\}: \text{ggT}(n, m) = 1\}|.$$

Hier steht  $\text{ggT}(n, m)$  für den größten gemeinsamen Teiler von  $n$  und  $m$ ; das ist die größte natürliche Zahl die sowohl  $n$  als auch  $m$  teilt. Als Beispiel für eine Anwendung des Prinzips der Inklusion–Exklusion finden wir eine Formel, die es erlaubt,  $\varphi(n)$  schnell zu berechnen, vorausgesetzt wir kennen die Primfaktoren von  $n$ .

Der einfachste Fall ist, wenn  $n = p$  eine Primzahl ist. Dann ist jedes  $m < p$  relativ prim zu  $p$ , und also ist  $\varphi(p) = p - 1$ .

Der nächste Schritt in Richtung auf eine allgemeine Lösung ist der Fall, dass  $n = p^\alpha$  ( $\alpha \in \mathbb{N}$ ) eine Primzahlpotenz ist. Dann sind die Zahlen, die nicht relativ prim zu  $p^\alpha$  sind, Vielfache von  $p$ , d.h.  $p, 2p, 3p, \dots, p^{\alpha-1}p$ , und es gibt  $p^{\alpha-1}$  solche Vielfache, die nicht größer als  $p^\alpha$  sind (allgemein ist, wenn  $d$  ein Teiler einer Zahl  $n$  ist, die Anzahl

der Vielfachen von  $d$ , die nicht größer sind als  $n$ , gleich  $n/d$ ). Deshalb bleiben  $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1 - 1/p)$  Zahlen übrig, die relativ prim zu  $p^\alpha$  sind.

Ein beliebiges  $n$  kann in der Form

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

geschrieben werden, wobei  $p_1, p_2, \dots, p_r$  verschiedene Primzahlen sind und  $\alpha_i \in \mathbb{N}$ . Die „bösen“  $m \leq n$ , die nichts zu  $\varphi(n)$  beitragen, sind alle Vielfachen von den Primzahlen  $p_1, \dots, p_r$ . Wir bezeichnen die Menge aller Vielfachen von  $p_i$  mit  $A_i = \{m \in \{1, 2, \dots, n\} : p_i | m\}$ . Es ist dann  $\varphi(n) = n - |A_1 \cup A_2 \cup \dots \cup A_r|$ . Das Prinzip der Inklusion–Exklusion verlangt, dass wir die Mächtigkeiten der Schnittmengen von den  $A_i$  herausfinden. Der Schnitt von  $A_1$  und  $A_2$  z.B. enthält alle Zahlen, die sowohl durch  $p_1$  als auch durch  $p_2$  teilbar sind; das sind gerade die Vielfachen von  $p_1 p_2$ , und deshalb ist  $|A_1 \cap A_2| = n/(p_1 p_2)$ . Das gleiche Argument ergibt auch

$$|A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_k}| = \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_k}}.$$

Schauen wir uns zunächst die Fälle  $r = 2$  und  $r = 3$  an. Für  $n = p_1^{\alpha_1} p_2^{\alpha_2}$  haben wir

$$\begin{aligned} \varphi(n) &= n - |A_1 \cup A_2| = n - |A_1| - |A_2| + |A_1 \cap A_2| \\ &= n - \frac{n}{p_1} - \frac{n}{p_2} + \frac{n}{p_1 p_2} = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right). \end{aligned}$$

Für  $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}$  erhalten wir analog

$$\begin{aligned} \varphi(n) &= n - \frac{n}{p_1} - \frac{n}{p_2} - \frac{n}{p_3} + \frac{n}{p_1 p_2} + \frac{n}{p_1 p_3} + \frac{n}{p_2 p_3} - \frac{n}{p_1 p_2 p_3} \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \left(1 - \frac{1}{p_3}\right). \end{aligned}$$

Jetzt kann man die allgemeine Formel raten.

**3.8.2 Satz.** Für  $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$  ist

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right). \quad (3.20)$$

*Beweis.* Für eine beliebige Zahl  $r$  erhalten wir mit dem Prinzip der Inklusion–Exklusion (geschickterweise verwenden wir die kurze Form (3.14))

$$\varphi(n) = n - \sum_{\emptyset \neq I \subseteq \{1, 2, \dots, r\}} (-1)^{|I|-1} \frac{n}{\prod_{i \in I} p_i} = n \cdot \sum_{I \subseteq \{1, 2, \dots, r\}} \frac{(-1)^{|I|}}{\prod_{i \in I} p_i}.$$

Wir behaupten, dass diese beängstigende Formel gleich der rechten Seite von Gleichung (3.20) ist. Das folgt aus Formel (3.15) zum Ausmultiplizieren des Produkts  $(1+x_1)(1+x_2)(1+x_3)\dots$ , wenn man  $x_i = -1/p_i$ ,  $i = 1, 2, \dots, r$  einsetzt.  $\square$

## Aufgaben

1. An einem Ball nehmen  $n$  Ehepaare teil. Auf wieviele Arten können sie  $n$  Paare bilden, wenn keine Dame mit ihrem Gatten tanzt?
2. (a) Bestimmen Sie die Anzahl der Permutationen mit genau einem Fixpunkt.  
 (b) Bestimmen Sie die Anzahl der Permutationen mit genau  $k$  Fixpunkten.
3. Was ist „faul“ an dem folgenden induktiven „Beweis“, dass  $D(n) = (n-1)!$  für alle  $n \geq 2$ ? Finden Sie den Fehler! Für  $n = 2$  gilt die Formel, also nehmen wir  $n \geq 3$  an. Sei  $\pi$  eine fixpunktfreie Permutation von  $\{1, 2, \dots, n-1\}$ . Wir möchten sie zu einer fixpunktfreien Permutation  $\pi'$  von  $\{1, 2, \dots, n\}$  ergänzen. Wir wählen eine Zahl  $i \in \{1, 2, \dots, n-1\}$  und definieren  $\pi'(n) = \pi(i)$ ,  $\pi'(i) = n$  und  $\pi'(j) = \pi(j)$  für  $j \neq i, n$ . Dies definiert eine Permutation von  $\{1, 2, \dots, n\}$ , und man prüft leicht nach, dass sie fixpunktfrei ist. Für jedes der  $D(n-1) = (n-2)!$  möglichen  $\pi$  kann der Index  $i$  auf  $n-1$  Arten gewählt werden. Also ist  $D(n) = (n-2)! \cdot (n-1) = (n-1)!$ .
4. \*Beweisen Sie die Gleichung

$$D(n) = n! - nD(n-1) - \binom{n}{2}D(n-2) - \cdots - \binom{n}{n-1}D(1) - 1.$$

5. (a) \*Beweisen Sie die Rekursion  $D(n) = (n-1)[D(n-1) + D(n-2)]$ . Beweisen Sie induktiv Formel (3.19) für  $D(n)$ .  
 (b) \*Berechnen Sie die Formel für  $D(n)$  direkt aus der Rekursion aus (a). Benutzen Sie die Hilfsfolge  $a_n = D(n) - nD(n-1)$ .
6. Wie viele Permutationen der Zahlen  $1, 2, \dots, 10$  gibt es, die keine gerade Zahl auf sich selbst abbilden?
7. (Anzahl der surjektiven Funktionen) Nun ist es an der Zeit, die Anzahl der *surjektiven* Abbildungen einer  $m$ -Menge in eine  $n$ -Menge zu bestimmen (was wir bisher vermieden haben). Berechnen Sie sie
  - (a) für  $m = 2$
  - (b) für  $m = 3$ .
  - (c) \*Finden Sie eine Formel für allgemeines  $m$ ; überprüfen Sie Ihr Ergebnis für  $m = n = 10$  (was ist das Ergebnis für  $n = m$ ?). Warnung:

Die resultierende Formel ist eine Summe, keine „schöne“ Formel wie ein Binomialkoeffizient.

- (d) \*Zeigen Sie, wenn möglich ohne auf (c) zurückzugreifen, dass die Anzahl der surjektiven Abbildungen in eine  $m$ -Menge durch  $m!$  teilbar ist.
8. (a) \*Auf wie viele Arten kann man  $n$  Personen in  $k$  Gruppen aufteilen (oder: Wie viele Äquivalenzrelationen mit  $k$  Äquivalenzklassen gibt es auf einer  $n$ -Menge)? Suchen Sie zuerst nach einer Lösung des Problems für  $k = 2, 3$  und  $k = n - 1, n - 2$ . Für allgemeines  $k$  ist die gesuchte Antwort eine Summe.
- (b) Wie viele Äquivalenzrelationen gibt es auf einer  $n$ -Menge? (Das Ergebnis ist eine Doppelsumme.)
- (c) \*Das Ergebnis aus (b) wird als die  $n$ -te Bell-Zahl  $B_n$  bezeichnet. Beweisen Sie die folgende (überraschende) Formel:

$$B_n = \frac{1}{e} \sum_{i=0}^{\infty} \frac{i^n}{i!}.$$

9. \*Beweisen Sie die folgende Formel für die Eulersche  $\varphi$ -Funktion: Sind  $m$  und  $n$  relativ prim, dann gilt  $\varphi(mn) = \varphi(m)\varphi(n)$ . Damit haben Sie auch einen weiteren Beweis für Gleichung (3.20), denn dass sie für Primzahlpotenzen gilt, wissen Sie; und für andere natürliche Zahlen hilft Ihnen die neue Formel weiter.
10. \*Beweisen Sie, dass für jede beliebige natürliche Zahl  $n$  die Gleichung  $\sum_{d|n} \varphi(d) = n$  gilt (die Summe läuft über alle natürlichen Zahlen  $d$ , die  $n$  teilen).
11. (a) Wie viele Teiler hat die Zahl  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ ? ( $p_1, p_2, \dots, p_r$  sind lauter verschiedene Primzahlen.)
- (b) Zeigen Sie: Die *Summe* aller Teiler der Zahl  $n$  (wie in (a) gegeben) ist
- $$\prod_{i=1}^r \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$
- (c) \*\*Eine Zahl  $n$  heißt *perfekt*, wenn die Summe aller ihrer Teiler ( $n$  ausgenommen)  $n$  ergibt. Z.B. ist  $6 = 1 + 2 + 3$  perfekt. Beweisen Sie, dass jede gerade perfekte Zahl die Gestalt  $2^q(2^{q+1} - 1)$  hat, wobei  $q \geq 1$  eine natürliche Zahl ist und  $2^{q+1} - 1$  eine Primzahl.

*Bemerkung.* Es ist keine einzige ungerade perfekte Zahl bekannt, aber niemand kann beweisen, dass es keine gibt.

12. (a) \*Bestimmen Sie zu einer gegebenen natürlichen Zahl  $N$  die Wahrscheinlichkeit dafür, dass zwei unabhängig gewählte Zahlen  $m, n \in \{1, 2, \dots, N\}$  relativ prim sind.  
(b) \*Beweisen Sie, dass der Grenzwert der Wahrscheinlichkeit aus (a) für  $N \rightarrow \infty$  gleich dem unendlichen Produkt  $\prod_p (1 - 1/p^2)$  ist, wobei  $p$  über alle Primzahlen läuft. (Es sei erwähnt, dass dieses Produkt den Wert  $6/\pi^2$  hat; man kann das aus Tatsache 12.7.1 beweisen.)
13. (a) Bestimmen Sie die Anzahl der Graphen ohne Ecken vom Grad 0 auf einer vorgegebenen Eckenmenge  $V$  (die Definitionen finden Sie in den Abschnitten 4.1 und 4.3).  
(b) Bestimmen Sie die Anzahl aller Graphen auf der Eckenmenge  $V$  mit mindestens zwei Ecken vom Grad 0 und mit genau zwei Ecken vom Grad 0.
14. \*Auf wie viele Arten kann man  $n$  Ehepaare so um einen runden Tisch mit  $2n$  Stühlen setzen, dass kein Paar nebeneinander sitzt?



# 4

# Graphen

---

## 4.1 Definition eines Graphen; Isomorphismus

Die Struktur vieler praktisch motivierten oder auch mathematischer Probleme kann man sich oft durch ein Schema veranschaulichen, das aus zwei Sorten von Dingen besteht:

- aus einer (endlichen) Menge von Punkten und
- aus Linien, die Paare von Punkten miteinander verbinden.

Die Punkte könnten z.B. Gäste einer Geburtstagsfeier sein, von denen zwei immer dann durch eine Linie miteinander verbunden sind, wenn die beiden Gäste einander kennen. Oder die Punkte repräsentieren Straßenkreuzungen in einer Stadt und die Verbindungslinien die Straßen. Auch Nahverkehrs- oder Eisenbahnnetze werden oft in dieser Form dargestellt (siehe Abb. 4.1), und elekrotechnische Pläne haben oft einen ähnlichen Charakter. In all diesen Fällen werden die Punkte gewöhnlich *Ecken* (oder auch *Knoten*) genannt und die verbindenden Linien heißen *Kanten*.<sup>1</sup>

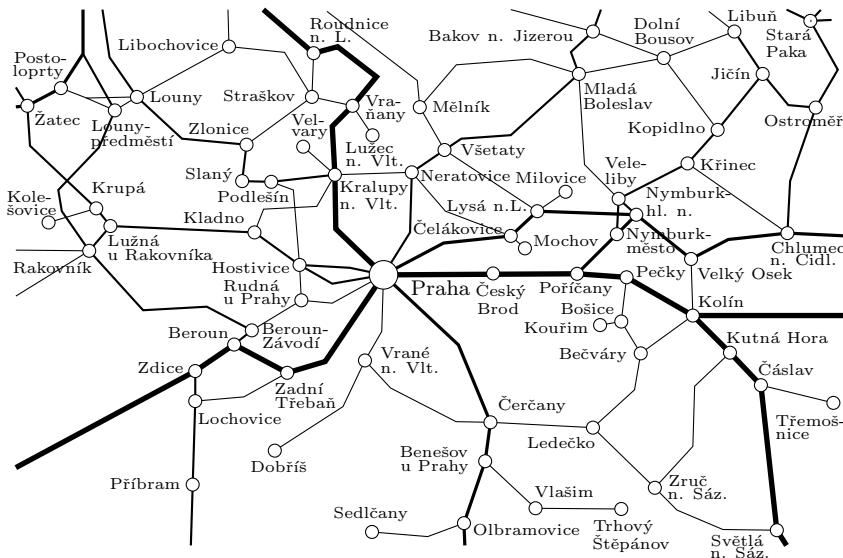
Wir lassen die Länge, die Form und andere Eigenschaften der Verbindungslinien außer Acht und fokussieren allein darauf, welche Paare von Punkten verbunden sind und welche nicht — das ist ein Graph. Diese einfache Idee ist einer der Schlüsselbegriffe der Diskreten Mathematik.

**4.1.1 Definition.** Ein Graph<sup>2</sup>  $G$  ist ein geordnetes Paar  $(V, E)$ ; dabei ist  $V$  eine Menge und  $E$  ist eine Menge 2-elementiger Teilmengen von  $V$ . Die Elemente der Menge  $V$  heißen Ecken des Graphen  $G$  und die Elemente von  $E$  heißen Kanten von  $G$ .

---

<sup>1</sup>Woher diese Namen kommen, wird in Abschnitt 6.3 klar werden.

<sup>2</sup>Was wir hier einfach Graph nennen, heißt manchmal etwas ausführlicher ein *einfacher ungerichteter Graph*, in Abgrenzung von anderen, ähnlichen Konzepten; mit einigen werden wir uns später noch auseinandersetzen.



**Abb. 4.1** Ausschnitt aus einem Plan des tschechischen Eisenbahnnetzes (ca.  $150 \times 100$  km um Prag).

Es wäre wohl natürlicher, die Eckenmenge mit  $E$  und die Kantenmenge mit  $K$  zu bezeichnen. Die hier verwendeten Bezeichnungen haben sich aber durchgesetzt, weil „Ecke“ auf englisch „vertex“ (Plural: „vertices“) heißt, und „Kante“ heißt „edge“. Es bestand also die Wahl, hier die englischen Anfangsbuchstaben zu wählen oder Sie in Verwirrung zu stürzen, sobald Sie ein englisches Buch aufschlagen.

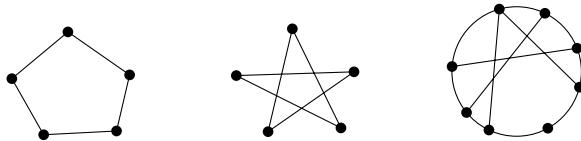
Fast alle in diesem Buch betrachteten Graphen werden eine endliche Eckenmenge haben. In den wenigen Fällen, in denen unendliche Graphen vorkommen, werden wir das ausdrücklich erwähnen.

Wenn dir deutlich machen wollen, dass ein Graph  $G$  die Eckenmenge  $V$  und die Kantenmenge  $E$  hat, dann schreiben wir  $G = (V, E)$ . Wenn wir uns auf die Eckenmenge eines schon gegebenen Graphen  $G$  beziehen wollen, dann schreiben wir  $V(G)$ . Analog schreiben wir  $E(G)$  für die Kantenmenge eines Graphen  $G$ . Eine nützliche Schreibweise ist außerdem  $\binom{V}{2}$  für die Menge aller zweielementigen Teilmengen von  $V$  (siehe Abschnitt 3.3.1 für den Hintergrund). Kurz können wir sagen, dass ein Graph ein Paar  $(V, E)$  mit  $E \subseteq \binom{V}{2}$  ist.

Die folgende Terminologie erklärt sich fast von selbst: Ist  $\{u, v\}$  eine Kante eines Graphen  $G$ , dann sagen wir, dass die Ecken  $u$  und  $v$

*adjazent* in  $G$  oder dass  $u$  ein *Nachbar* von  $v$  ist (und  $v$  ein Nachbar von  $u$ ).

Gerne stellt man Graphen durch Zeichnungen in der Ebene dar. Die Ecken des Graphen zeichnet man als Punkte (oder ganz kleine Kreise) in die Ebene und die Kanten werden durch (gerade oder gebogene) Linien zwischen den Endpunkten repräsentiert. Auf diese Art erhalten wir Bilder wie diese:



Der Name „Graph“ kommt wahrscheinlich gerade von dieser Möglichkeit der Zeichnung. (Das Wort „Graph“ ist hier in einer ganz anderen Bedeutung benutzt als in „Graph einer Funktion“ — sicherlich haben Sie das selbst auch schon bemerkt.)

Die Zeichnung eines Graphen spielt jedoch nur eine untergeordnete Rolle. Es gibt viele Möglichkeiten einen Graphen zu repräsentieren, und ein Computer wird ihn sicherlich nicht als Zeichnung speichern. Ein und derselbe Graph kann auf vielerlei Arten gezeichnet werden. Die beiden ersten der obigen Beispiele zeigen z. B. den gleichen Graphen mit Eckenmenge  $\{1, 2, 3, 4, 5\}$  und den Kanten  $\{1, 2\}, \{2, 3\}, \{3, 4\}, \{4, 5\}, \{5, 1\}$ .

Eine Zeichnung eines Graphen ist oft eine große Hilfe für das Verständnis. Sie können kaum zu viele Zeichnungen machen. Viele Konzepte sind durch Bilder motiviert, und dementsprechend hilft Ihnen ein Bild, Intuition zu entwickeln.

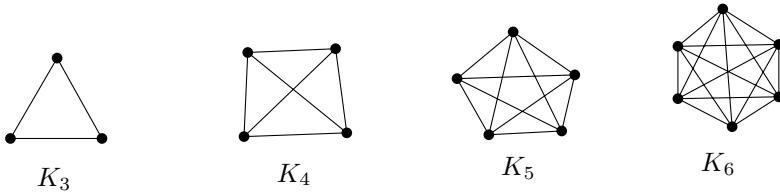
Eine Zeichnung eines Graphen ist in der Regel dann besonders übersichtlich, wenn sich die Kanten möglichst wenig überkreuzen. Kreuzungen können fälschlich für Ecken gehalten werden, und bei manchen elektronischen Schaltkreisen sowie in einer Reihe anderer Situationen sind Kreuzungen nicht zulässig. Dieser Gedanke führt zum Studium einer wichtigen Graphenklasse, den so genannten ebenen Graphen (siehe Kapitel 6).

Die Eisenbahnkarte in Abb. 4.1 illustriert auch, dass das Konzept eines Graphen eine Abstraktion ist und Situationen aus dem richtigen Leben vereinfacht. Das historisch gewachsene Eisenbahnnetz ähnelt der Zeichnung eines Graphen, aber es gibt da z. B. ein paar Stellen, wo sich die Gleise außerhalb der Bahnhöfe treffen. Außerdem verlieren wir durch die Beschränkungen auf Bahnhöfe und Verbindungen eine ganze Menge anderer Information (Zustand der Gleise, ob eine Strecke ein-

oder mehrgleisig ausgebaut ist, welche Gleise durch einen Bahnhof hindurch führen und welche daran vorbeigeführt werden, Streckenlänge, Bahnhofspläne, usw.). Wenn man vor der Aufgabe stünde, ein Eisenbahnenetz mathematisch zu modellieren, und man kennt das Konzept eines Graphen nicht, dann würde man wahrscheinlich auf etwas viel Komplizierteres kommen. Und tatsächlich werden Graphen in Anwendungen oft durch weitere Informationen ergänzt. Das Konzept Graph ist sehr nützlich als Ausgangspunkt für solche mathematischen Modelle, und wenn wir einen Graphen als wesentlichen Bestandteil des Modells verwenden, dann steht uns mit einem Mal eine gut entwickelte mathematische Theorie zur Verfügung.

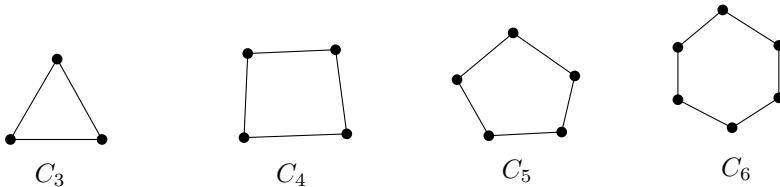
**Wichtige Graphen.** An dieser Stelle führen wir einige spezielle Typen von Graphen ein, die eine wichtige Rolle in der Graphentheorie spielen und für die sich eine Standardterminologie herausgebildet hat.

*Der vollständige Graph  $K_n$ :*  $V = \{1, 2, \dots, n\}$ ,  $E = \binom{V}{2}$ .

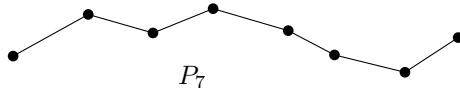


Den  $K_{23}$  in Abb. 4.2 bilden wir mit allen 253 Kanten hauptsächlich aus Gründen der Ästhetik ab.

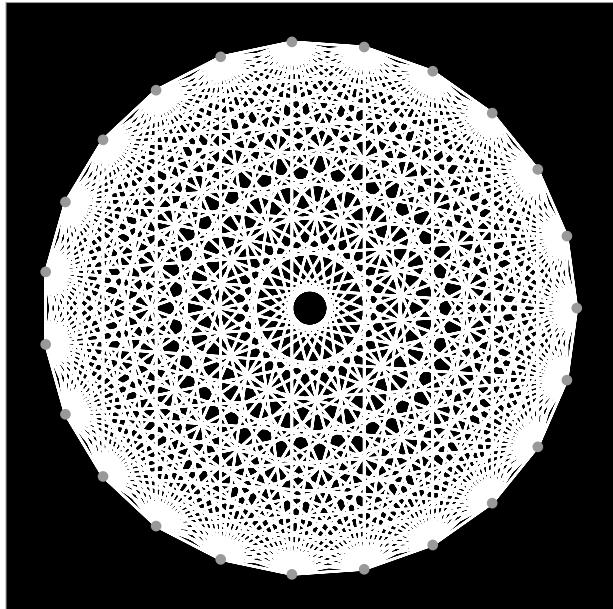
*Der Kreis  $C_n$ :*  $V = \{1, 2, \dots, n\}$ ,  
 $E = \{\{i, i+1\} : i = 1, 2, \dots, n-1\} \cup \{\{1, n\}\}$ .



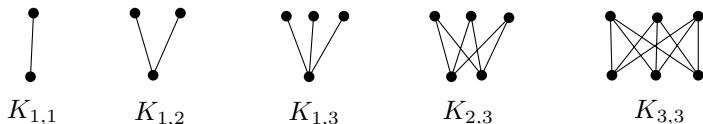
*Der Weg  $P_n$ :*  $V = \{0, 1, \dots, n\}$ ,  $E = \{\{i-1, i\} : i = 1, 2, \dots, n\}$ .



*Der vollständige bipartite Graph  $K_{n,m}$ :*  
 $V = \{u_1, \dots, u_n\} \cup \{v_1, \dots, v_m\}$ ,  
 $E = \{\{u_i, v_j\} : i = 1, 2, \dots, n, j = 1, 2, \dots, m\}$ .



**Abb. 4.2** Der vollständige Graph  $K_{23}$ .



Hier scheint eine Erklärung angebracht. Das Wort „bi-partit“ bedeutet „aus zwei Teilen bestehend“. Allgemein heißt ein Graph  $G$  *bipartit*, wenn man die Menge  $V(G)$  so in zwei disjunkte Mengen  $V_1$  und  $V_2$  aufteilen kann, dass jede Kante von  $G$  eine Ecke aus  $V_1$  mit einer Ecke aus  $V_2$  verbindet. In Symbolen:  $E(G) \subseteq \{\{v, v'\}: v \in V_1, v' \in V_2\}$ . Die Mengen  $V_1$  und  $V_2$  heißen manchmal *Klassen* von  $G$ .

**Isomorphie von Graphen.** Wir sehen zwei Graphen  $G$  und  $G'$  als identisch (oder gleich) an, wenn sie die gleiche Eckenmenge und die gleiche Kantenmenge haben, d.h.  $G = G'$  bedeutet  $V(G) = V(G')$  und  $E(G) = E(G')$ . Aber viele Graphen unterscheiden sich „nur“ in den Namen ihrer Ecken und Kanten und haben ansonsten die gleiche „Struktur“. Für solche Fälle haben wir das Konzept des Isomorphismus.

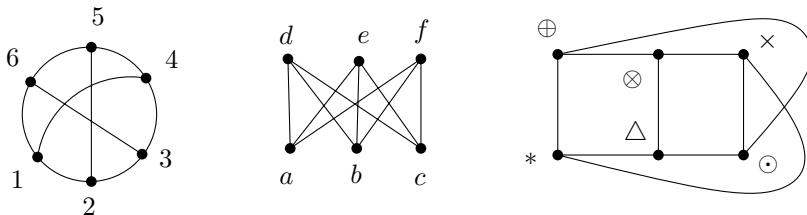
**4.1.2 Definition.** Zwei Graphen  $G = (V, E)$  und  $G' = (V', E')$  heißen *isomorph*, wenn es eine Bijektion  $f: V \rightarrow V'$  gibt, so dass

$$\{x, y\} \in E \quad \text{genau dann, wenn} \quad \{f(x), f(y)\} \in E'$$

für alle  $x, y \in V$ ,  $x \neq y$  gilt. So eine Funktion  $f$  heißt ein Isomorphismus der Graphen  $G$  und  $G'$ . Wenn  $G$  und  $G'$  isomorph sind, schreiben wir  $G \cong G'$ .

Ein Isomorphismus bildet also adjazente Ecken auf adjazente Ecken und nicht adjazente Ecken auf nicht adjazente Ecken ab; man kann sich das als „Umbenennen der Ecken“ eines Graphen vorstellen. Die Relation  $\cong$  („isomorph sein“) ist eine Äquivalenzrelation (auf jeder Menge von Graphen) (siehe Aufgabe 7).

**Problem.** Die folgenden drei Bilder zeigen isomorphe Graphen. Finden Sie Isomorphismen!



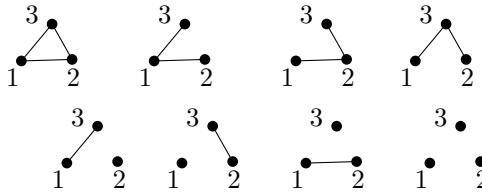
*Lösung.* Alle drei Graphen sind isomorph zu  $K_{3,3}$ . Ein Isomorphismus zwischen den ersten beiden Graphen ist z.B.  $1 \mapsto a$ ,  $2 \mapsto d$ ,  $3 \mapsto b$ ,  $4 \mapsto e$ ,  $5 \mapsto c$ ,  $6 \mapsto f$  (es gibt mehrere andere Möglichkeiten!). Die Isomorphismen zwischen dem ersten und dritten sowie zwischen dem zweiten und dritten Graphen sollten Sie selbst finden.

**Warnung.** Die Definition eines Isomorphismus ist eigentlich ganz einfach; ein Isomorphismus zwischen  $G$  und  $G'$  ist jedoch *nicht irgendeine* Bijektion zwischen  $V$  und  $V'$  und auch nicht *irgendeine* Bijektion zwischen  $E$  und  $E'$ . Wir schlagen vor, dass Sie jetzt einmal die Definition aus dem Gedächtnis niederschreiben, um sich zu vergewissern, dass Sie sie wirklich verstanden haben (sie ist sehr wichtig!).

**Test auf Isomorphie.** Bei kleinen Bildern ist es gewöhnlich nicht besonders schwierig herauszufinden, ob sie zu isomorphen Graphen gehören oder nicht (auch wenn das obige Problem zeigt, dass die Bilder ganz und gar nicht ähnlich aussehen müssen). Doch das Problem zu entscheiden, ob zwei gegebene Graphen isomorph sind oder nicht, ist im Allgemeinen schwierig, kein effizienter Algorithmus ist bekannt (d.h. keiner, der für alle Fälle schnell funktioniert). Man vermutet sogar, dass es gar keinen solchen effizienten Algorithmus gibt. Die Schwierigkeit liegt darin, zu beweisen, dass zwei gegebene Graphen auf  $n$  Ecken nicht isomorph sind. Um dies mit Hilfe der Definition nachzuprüfen

müssen wir uns vergewissern, dass keine der  $n!$  möglichen Bijektionen auf der Eckenmenge ein Isomorphismus ist. Natürlich kann man das oft abkürzen und Isomorphie ganz einfach ausschließen. Wenn zwei Graphen z.B. verschieden viele Kanten haben, dann können Sie nicht isomorph sein, weil ein Isomorphismus die Anzahl der Kanten erhält. Allgemeiner: wenn wir einem Graphen eine Zahl oder einen Vektor zuordnen können, derart dass isomorphe Graphen stets denselben Wert erhalten, können wir diese manchmal dafür verwenden, nicht isomorphe Graphen zu unterscheiden (Beispiele folgen später). Aber bis jetzt hat man noch keine schnelle Methode gefunden, die *immer* erfolgreich ist.

**Anzahl nicht isomorpher Graphen.** Sei  $V$  die Menge  $\{1, 2, \dots, n\}$ . Einen Graphen mit Eckenmenge  $V$  zu wählen bedeutet, ein beliebige Teilmenge  $E \subseteq \binom{V}{2}$  auszuwählen. Die Menge  $\binom{V}{2}$  hat  $\binom{n}{2}$  Elemente, deshalb gibt es auf der Eckenmenge  $V$  genau  $2^{\binom{n}{2}}$  verschiedene Graphen. Allerdings sind einige dieser Graphen isomorph, es gibt also wesentlich weniger als  $2^{\binom{n}{2}}$  paarweise nicht isomorphe Graphen auf  $n$  Ecken. Für  $V = \{1, 2, 3\}$  haben wir z.B. die folgenden  $8 = 2^{\binom{3}{2}}$  verschiedenen Graphen:



Unter diesen 8 Graphen finden wir jedoch nur 4 nicht isomorphe:



Wie viele paarweise nicht isomorphe Graphen gibt es auf  $n$  Ecken für allgemeines  $n$ ? Anders gefragt: In wie viele Äquivalenzklassen zerlegt die Äquivalenzrelation  $\cong$  die Menge aller Graphen auf der Eckenmenge  $V = \{1, 2, \dots, n\}$ ? Diese Zahl zu bestimmen ist nicht leicht (siehe z.B. Harary und Palmer [22]), doch mit dem folgenden einfachen (und cleveren!) Trick erhalten wir zumindest eine akzeptable Abschätzung. Einerseits ist die Anzahl nicht isomorpher Graphen auf  $n$  Ecken sicherlich nicht größer als die Anzahl aller verschiedenen Graphen auf  $V$ , d.h.  $2^{\binom{n}{2}}$ . Betrachten wir nun einen bestimmten Graphen  $G$  mit Eckenmenge  $V$ . Wie viele verschiedene Graphen  $G'$  auf  $V$  sind zu  $G$  isomorph? Ist  $G$  zum Beispiel der Graph



auf der Eckenmenge  $\{1, 2, 3\}$ , dann gibt es drei solche isomorphen Graphen. Ist  $G'$  so ein zu  $G$  isomorpher Graph, dann existiert nach Definiti-

on eine Bijektion  $f: V \rightarrow V$ , die ein Isomorphismus zwischen  $G$  und  $G'$  ist. Die Anzahl aller möglichen Bijektionen  $f: V \rightarrow V$  ist  $n!$ , also ist  $G$  zu höchstens  $n!$  verschiedenen Graphen auf der Menge  $V$  isomorph. (Im Allgemeinen sind es weniger! In unserem speziellen Beispiel für  $n = 3$  hatten wir  $3! = 6$  Bijektionen, aber nur 3 verschiedene Graphen, die isomorph zu  $G$  sind — können Sie das erklären?) Anders ausgedrückt besteht jede Äquivalenzklasse von  $\cong$  auf der Menge aller Graphen mit Eckenmenge  $V$  aus höchstens  $n!$  Graphen, und deshalb ist die Anzahl der Äquivalenzklassen mindestens

$$\frac{2^{\binom{n}{2}}}{n!}.$$

Das heißt aber, dass es mindestens so viele paarweise nicht isomorphe Graphen auf  $n$  Ecken gibt.

Wir behaupten, dass das Wachstum dieser Funktion von  $n$  nicht wesentlich langsamer ist als das von  $2^{\binom{n}{2}}$ . Um das zu sehen, wenden wir auf beide Funktionen den Logarithmus an und formen die resultierenden Ausdrücke geeignet um. Wir verwenden die offensichtliche Abschätzung  $n! \leq n^n$ :

$$\log_2 \left[ 2^{\binom{n}{2}} \right] = \binom{n}{2} = \frac{n^2}{2} \left( 1 - \frac{1}{n} \right),$$

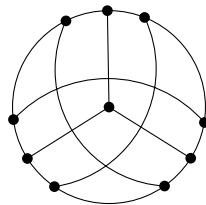
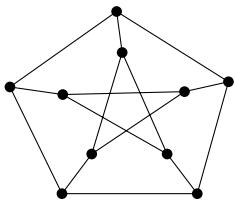
$$\begin{aligned} \log_2 \frac{2^{\binom{n}{2}}}{n!} &= \binom{n}{2} - \log_2 n! \geq \frac{1}{2}n^2 - \frac{1}{2}n - n \log_2 n \\ &= \frac{n^2}{2} \left( 1 - \frac{1}{n} - \frac{2 \log_2 n}{n} \right). \end{aligned}$$

Wir sehen, dass sich die Logarithmen der beiden Funktionen für großes  $n$  ungefähr wie die Funktion  $\frac{1}{2}n^2$  verhalten: Der relative Fehler, den wir machen, wenn wir die Logarithmen durch  $\frac{1}{2}n^2$  ersetzen, konvergiert gegen 0 für  $n \rightarrow \infty$ . (In Abschnitt 3.4 haben wir uns ausführlicher mit Abschätzungen für das Wachstum von Funktionen auseinandergesetzt.) Insbesondere ist die Anzahl nicht isomorpher Graphen auf  $n$  Ecken (für hinreichend großes  $n$ ) sehr viel größer als  $2^n$ .

In den eben angestellten Betrachtungen haben wir bewiesen, dass es viele nicht isomorphe Graphen gibt, erstaunlicherweise ohne auch nur ein Paar nicht isomorpher Graphen zu konstruieren. In Kapitel 10 werden wir ähnliche Methoden systematischer diskutieren. Viele nicht isomorphe Graphen explizit zu konstruieren ist gar nicht so einfach — siehe Aufgabe 8.

## Aufgaben

1. (a) Geben Sie einen Isomorphismus der folgenden Graphen an:



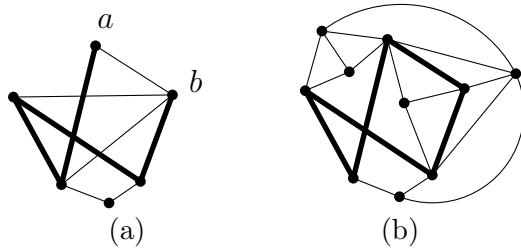
- (b) \*Zeigen Sie, dass die beiden Graphen oben isomorph zu dem folgenden Graphen sind: Die Eckenmenge ist  $\binom{\{1,2,\dots,5\}}{2}$  (ungeordnete Zahlenpaare) und zwei Ecken  $\{i, j\}$  und  $\{k, \ell\}$  ( $i, j, k, \ell \in \{1, 2, \dots, 5\}$ ) bilden genau dann eine Kante, wenn  $\{i, j\} \cap \{k, \ell\} = \emptyset$ .

*Bemerkung.* Dieser Graph heißt der *Petersen-Graph* und ist ein ganz besonderer Graph; er ist relativ klein und überschaubar, jedoch ein Gegenbeispiel zu vielen Vermutungen und ein Spezialfall in vielen Sätzen. Er ist das kleinste (nicht triviale) Mitglied in der Familie der so genannten *Kneser-Graphen*, die viele weitere Beispiele von Graphen mit interessanten Eigenschaften enthält. Die Eckenmenge eines Kneser-Graph ist  $\binom{\{1,2,\dots,n\}}{k}$  für natürliche Zahlen  $n > k \geq 1$ , und Kanten entsprechen leeren Schnitten.

2. Welche der folgenden Aussagen über Graphen  $G$  und  $H$  sind wahr? Begründen Sie Ihre Antworten!
  - (i)  $G$  und  $H$  sind genau dann isomorph, wenn für jede Abbildung  $f: V(G) \rightarrow V(H)$  und für je zwei Ecken  $u, v \in V(G)$  gilt:  $\{u, v\} \in E(G) \Leftrightarrow \{f(u), f(v)\} \in V(H)$ .
  - (ii)  $G$  und  $H$  sind genau dann isomorph, wenn es eine bijektive Abbildung  $f: E(G) \rightarrow E(H)$  gibt.
  - (iii) Wenn es eine Bijektion  $f: V(G) \rightarrow V(H)$  gibt, so dass jede Ecke  $u \in V(G)$  den gleichen Grad wie  $f(u)$  hat, dann sind  $G$  und  $H$  isomorph.
  - (iv) Wenn  $G$  und  $H$  isomorph sind, dann gibt es eine bijektive Abbildung  $f: V(G) \rightarrow V(H)$ , so dass jede Ecke  $u \in V(G)$  den gleichen Grad wie  $f(u)$  hat.
  - (v) Sind  $G$  und  $H$  isomorph, so gibt es eine Bijektion  $f: E(G) \rightarrow E(H)$ .
  - (vi)  $G$  und  $H$  sind genau dann isomorph, wenn es eine Abbildung  $f: V(G) \rightarrow V(H)$  gibt, so dass für je zwei Ecken  $u, v \in V(G)$  gilt:  $\{u, v\} \in E(G) \Leftrightarrow \{f(u), f(v)\} \in E(H)$ .
  - (vii) Zu jedem Graphen auf  $n$  Ecken gibt es einen isomorphen Graphen auf der Eckenmenge  $\{1, 2, \dots, n\}$ .
  - (viii) Jeder Graph auf  $n \geq 1$  Ecken ist zu unendlich vielen anderen Graphen isomorph.
3. Ein *Automorphismus* eines Graphen  $G = (V, E)$  ist ein Isomorphismus zwischen  $G$  und  $G$ , d.h. eine Bijektion  $f: V \rightarrow V$ , so dass genau dann

$\{u, v\} \in E$ , wenn  $\{f(u), f(v)\} \in E$ . Ein Graph heißt *asymmetrisch*, wenn er als Automorphismus nur die identische Abbildung zulässt (die jede Ecke auf sich selbst abbildet).

- (a) Finden Sie ein Beispiel eines asymmetrischen Graphen mit mindestens zwei Ecken.
- (b) Zeigen Sie, dass es keinen asymmetrischen Graphen  $G$  mit  $1 < |V(G)| \leq 5$  gibt.
- 4. Zeigen Sie, dass ein Graph  $G$  mit  $n$  Ecken genau dann asymmetrisch ist (siehe Aufgabe 3), wenn  $n!$  verschiedene Graphen auf der Eckenmenge  $V(G)$  zu  $G$  isomorph sind.
- 5. Wir nennen einen Graphen  $G = (V, E)$  *eckentransitiv*, wenn für je zwei Ecken  $v, v' \in V$  ein Automorphismus  $f: V \rightarrow V$  von  $G$  existiert (siehe Aufgabe 3) mit  $f(v) = v'$ . Analog heißt  $G$  *kantentransitiv*, wenn für je zwei Kanten  $e, e' \in E$  ein Automorphismus  $f: V \rightarrow V$  existiert mit  $f(e) = e'$  (wenn  $e = \{u, v\}$ , dann steht  $f(e)$  für die Menge  $\{f(u), f(v)\}$ ).
  - (a) Beweisen Sie, dass der Graph in Aufgabe 1 eckentransitiv ist.
  - (b) Entscheiden Sie, ob jeder eckentransitive Graph auch kantentransitiv ist.
  - (c) Konstruieren Sie einen Graph, der kantentransitiv ist, aber nicht eckentransitiv.
  - (d) \*Zeigen Sie, dass jeder Graph aus (c) notwendig bipartit ist.
- 6. Wie viele Graphen auf der Eckenmenge  $\{1, 2, \dots, 2n\}$  sind isomorph zu dem Graphen, der aus  $n$  eckendisjunkten Kanten besteht (d.h. mit Kantenmenge  $\{\{1, 2\}, \{3, 4\}, \dots, \{2n-1, 2n\}\}$ )?
- 7. \*Sei  $V$  eine endliche Menge.  $\mathcal{G}$  bezeichne die Menge aller möglichen Graphen mit Eckenmenge  $V$ . Überprüfen Sie, dass  $\cong$  („isomorph sein“) eine Äquivalenzrelation auf  $\mathcal{G}$  ist.
- 8. \*Konstruieren Sie möglichst viele paarweise nicht isomorphe Graphen mit Eckenmenge  $\{1, 2, \dots, n\}$  ( $n$  sei eine sehr große Zahl). Finden Sie mehr als  $n^2$  davon? Wenigstens  $2^{n/10}$ , oder vielleicht wesentlich mehr?
- 9. (a) <sup>CS</sup> Zeichnen Sie die Logarithmen der Funktionen  $2^{\binom{n}{2}}$  und  $2^{\binom{n}{2}}/n!$  in einem vernünftigen Bereich.
  - (b) \*;<sup>CS</sup> Schreiben Sie ein Programm, das für gegebenes  $n$  die Anzahl nicht isomorpher Graphen auf  $n$  Ecken berechnet. (Warnung: Nur mit einer cleveren Idee werden Sie in der Lage sein, mit halbwegs großen  $n$  fertig zu werden!). Zeichnen Sie für die Werte von  $n$ , die Sie handhaben können, die berechneten Zahlen in die Zeichnung aus (a) ein.



**Abb. 4.3** Ein Beispiel (a) eines Teilgraphen und (b) eines induzierten Teilgraphen.

(c) \*Wenn Sie (b) in den Griff bekommen haben, dann sollten die berechneten Zahlen darauf hinweisen, dass die untere Schranke  $2^{\binom{n}{2}}/n!$  für die Anzahl nicht isomorpher Graphen viel näher an der Wahrheit liegt als die obere Schranke  $2^{\binom{n}{2}}$ . Die Herleitung der oberen Schranke war ohnehin ein wenig zu einfach; können Sie sie verbessern?

## 4.2 Teilgraphen, Komponenten, Adjazenzmatrix

Die nächste Definition handelt davon, was heißen soll, „ein Graph ist in einem anderen enthalten“. Es stellt sich heraus, dass es mindestens zwei sinnvolle Möglichkeiten gibt, diese Vorstellung zu präzisieren.

**4.2.1 Definition.** Seien  $G$  und  $G'$  Graphen. Wir nennen  $G$  einen Teilgraphen von  $G'$ , wenn  $V(G) \subseteq V(G')$  und  $E(G) \subseteq E(G')$ . Wir nennen  $G$  einen induzierten Teilgraphen von  $G'$ , wenn  $V(G) \subseteq V(G')$  und  $E(G) = E(G') \cap \binom{V(G')}{2}$ .

Wir fassen diese Definition in Worte: Ein induzierter Teilgraph eines Graphen  $G'$  entsteht durch das Löschen einiger Ecken von  $G'$  und aller Kanten, die eine der gelöschten Ecken enthalten. Um einen Teilgraph zu erhalten, dürfen wir zusätzlich noch weitere Kanten löschen, auch wenn keine ihrer Endenken entfernt wurde. Abbildung 4.3(a) zeigt einen Graph und einen zum Weg  $P_4$  isomorphen Teilgraphen, der durch die dickeren Linien gekennzeichnet ist. Dieser Teilgraph ist nicht induziert (wegen der Kante  $\{a, b\}$ ). Abbildung 4.3(b) zeigt einen induzierten Teilgraph, isomorph zum Kreis  $C_5$ ; wie jeder induzierte Teilgraph ist er natürlich zugleich ein Teilgraph.

**Wege und Kreise.** Ein Teilgraph eines Graphen  $G$ , der isomorph zu einem Weg  $P_t$  ist, wird ein *Weg im Graphen G* genannt; siehe

Abb. 4.3(a). Einen Weg in einem Graphen  $G$  kann man als eine Folge

$$(v_0, e_1, v_1, \dots, e_t, v_t),$$

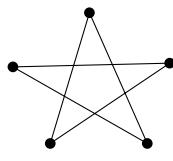
paarweise verschiedener Ecken  $v_0, v_1, \dots, v_t$  des Graphen  $G$  auffassen, so dass für alle  $i = 1, 2, \dots, t$  die Paare  $e_i = \{v_{i-1}, v_i\} \in E(G)$  sind. Das ist wie das Tagebuch eines Reisenden, der den Weg von einem Ende zum anderen zurücklegt und die besuchten Ecken und Kanten notiert.<sup>3</sup> Genauer sagen wir, der Weg  $(v_0, e_1, v_1, \dots, e_t, v_t)$  sei ein *Weg von  $v_0$  nach  $v_n$  der Länge  $t$* . Wir erlauben auch den Extremfall  $t = 0$ , d.h. einen Weg der Länge Null, der nur aus einer einzigen Ecke besteht.

Analog nennen wir einen Teilgraphen von  $G$ , der zu einem Kreis  $C_t$  ( $t \geq 3$ ) isomorph ist, einen *Kreis in  $G$* ; siehe Abb. 4.3(b). Ein Kreis in einem Graphen  $G$  kann also als eine Folge

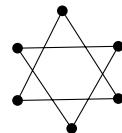
$$(v_0, e_1, v_1, e_2, \dots, e_{t-1}, v_{t-1}, e_t, v_0)$$

aufgefasst werden; dabei sind  $v_0, v_1, \dots, v_{t-1}$  paarweise verschiedene Ecken des Graphen  $G$ ,  $e_i = \{v_{i-1}, v_i\} \in E(G)$  für  $i = 1, 2, \dots, t-1$  und zusätzlich  $e_t = \{v_{t-1}, v_0\} \in E(G)$ . Die Zahl  $t \geq 3$  heißt die Länge des Kreises.

**Zusammenhang, Komponenten.** Wir nennen einen Graphen  $G$  *zusammenhängend*, wenn  $G$  für je zwei Ecken  $x, y \in V(G)$  einen Weg von  $x$  nach  $y$  enthält. Diagramm (a) zeigt ein Beispiel eines zusammenhängenden Graphen,



(a)



(b)

während (b) eine Zeichnung eines unzusammenhängenden Graphen ist.

Zusammenhang kann man auch geringfügig anders definieren. Zunächst führen wir ein Konzept ähnlich dem Weg in einem Graphen

---

<sup>3</sup>Weil wir nur einfache Graphen zulassen, ist das Notieren der Kanten nicht unbedingt notwendig, denn sie können aus der Folge der Ecken rekonstruiert werden. Die hier gegebene Definition ist zweckmäßig, wenn Mehrfachkanten (mehrere Kanten zwischen den gleichen zwei Ecken) erlaubt sind.

ein. Sei  $G = (V, E)$  ein Graph. Eine Folge  $(v_0, e_1, v_1, e_2, \dots, e_t, v_t)$  heißt ein *Spaziergang* in  $G$  (ausführlicher ein *Spaziergang der Länge  $t$  von  $v_0$  nach  $v_t$* ), wenn  $e_i = \{v_{i-1}, v_i\} \in E$  für alle  $i = 1, \dots, t$ . In einem Spaziergang dürfen Kanten und Ecken wiederholt vorkommen, was in einem Weg verboten war. Ein Spaziergang ist das Tagebuch eines Menschen, der kreuz und quer durch eine Gegend reist und sich nichts daraus macht, wenn er einen Ort mehrmals besucht oder eine Strecke mehrfach zurücklegt.

Als Nächstes definieren wir eine Relation  $\sim$  auf der Menge  $V(G)$ : Genau dann sei  $x \sim y$ , wenn es einen Spaziergang von  $x$  nach  $y$  in  $G$  gibt. Es ist eine ziemlich einfache Übung zu überprüfen, dass  $\sim$  eine Äquivalenzrelation ist. Sei  $V = V_1 \dot{\cup} V_2 \dot{\cup} \dots \dot{\cup} V_k$  die Partition der Eckenmenge  $V$  in die Äquivalenzklassen von  $\sim$ . Die von den Mengen  $V_i$  induzierten Teilgraphen von  $G$  heißen die *Komponenten* des Graphen  $G$ . Die folgende Beobachtung setzt diese Definition einer Komponente mit der vorigen Definition eines zusammenhängenden Graphen in Beziehung.

**4.2.2 Beobachtung.** *Jede Komponente eines Graphen ist zusammenhängend; ein Graph ist genau dann zusammenhängend, wenn er nur eine einzige Komponente hat.*

*Beweis.* Dass ein zusammenhängender Graph nur eine Komponente hat, ist klar. Für die andere Richtung: Je zwei Ecken  $x, y$  in der gleichen Komponente eines Graphen  $G$  können mit einem Spaziergang verbunden werden. Ein Spaziergang von  $x$  nach  $y$  mit kürzest möglicher Länge muss ein Weg sein.  $\square$

Diese Definition einer „Komponente“ mittels Spaziergängen mag etwas umständlich erscheinen, weshalb haben wir den ersten Ansatz mit den Wegen nicht weiter verfolgt? Dann würde man die Relation  $\sim'$  zu Grunde legen, wobei  $x \sim' y$  ist, wenn es einen Weg von  $x$  nach  $y$  gibt. Aus den obigen Überlegungen folgt, dass  $\sim'$  tatsächlich die gleiche Relation ist wie  $\sim$ . Doch der Beweis, dass  $\sim'$  eine Äquivalenzrelation ist, ist ziemlich verworkt; der Ansatz mit den Spaziergängen vermeidet einige Schwierigkeiten technischer Natur.

Es ist relativ einfach zu entscheiden, ob ein gegebener Graph zusammenhängend ist und gegebenenfalls die Komponenten zu bestimmen. Auf die Beschreibung konkreter Algorithmen wollen wir uns an dieser Stelle nicht einlassen, man findet sie in fast jedem Lehrbuch über Algorithmen. Meist stellt man sich vor, dass man in einem Graphen (oder

spannender formuliert: in einem Labyrinth) alle Ecken und Kanten „finden“ möchte; deshalb spricht man von „Suchalgorithmen“. Die beiden bekanntesten Algorithmen dieser Art sind die so genannte *Tiefensuche* und die *Breitensuche* (englisch *depth-first search* und *breadth-first search*).

**Abstand in Graphen.** Sei  $G = (V, E)$  ein zusammenhängender Graph. Wir definieren den *Abstand*  $d_G(v, v')$  zweier Ecken  $v, v' \in V(G)$  als die Länge eines kürzesten Weges von  $v$  nach  $v'$  in  $G$ .

Der Abstand  $d_G$  ist also eine Funktion  $d_G: V \times V \rightarrow \mathbb{R}$ , die *Abstandsfunktion* oder *Metrik* von  $G$ . Die Metrik von  $G$  hat folgende Eigenschaften:

1.  $d_G(v, v') \geq 0$ , und  $d_G(v, v') = 0$  dann und nur dann, wenn  $v = v'$ ;
2. (Symmetrie)  $d_G(v, v') = d_G(v', v)$  für je zwei Ecken  $v, v'$ ;
3. (Dreiecksungleichung) Für je drei Ecken  $v, v', v'' \in V(G)$  ist  $d_G(v, v'') \leq d_G(v, v') + d_G(v', v'')$ .

Diese drei Eigenschaften prüft man leicht mit der Definition der Abstandsfunktion  $d_G(v, v')$  nach. Jede Abbildung  $d: V \times V \rightarrow \mathbb{R}$ , die die Eigenschaften 1–3 erfüllt, heißt eine *Metrik* auf der Menge  $V$ , und die Menge  $V$  zusammen mit einer solchen Abbildung  $d$  heißt ein *metrischer Raum*. Die Metrik  $d_G$  eines Graphen hat darüber hinaus die folgenden speziellen Eigenschaften:

4.  $d_G(v, v')$  ist stets eine ganze Zahl
5. Ist  $d_G(v, v'') > 1$ , dann gibt es eine dritte Ecke  $v'$ ,  $v \neq v' \neq v''$ , für die  $d_G(v, v') + d_G(v', v'') = d_G(v, v'')$ .

Die Bedingungen 1–5 genügen schon um eine Funktion als Abstandsfunktion eines Graphen mit Eckenmenge  $V$  zu charakterisieren (siehe Aufgabe 7).

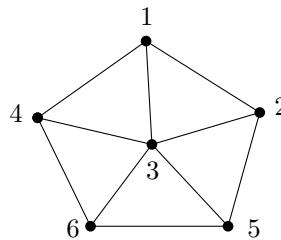
**Darstellungen eines Graphen.** Bisher haben wir Graphen durch eine Zeichnung repräsentiert, wenn wir nicht die Ecken- und Kantenmenge direkt aufgeschrieben haben. Es gibt viele weitere Möglichkeiten, einen Graphen darzustellen. Eine Zeichnung ist (bei Graphen von überschaubarer Größe) für Menschen besonders übersichtlich; andere Darstellungen sind insbesondere dann vorteilhaft, wenn wir Graphen in einem Computer speichern und manipulieren wollen. Eine sehr einfache und gebräuchliche Darstellung ist die *Adjazenzmatrix*:

**4.2.3 Definition.** Sei  $G = (V, E)$  ein Graph mit  $n$  Ecken. Wir ordnen die Ecken in beliebiger Reihenfolge  $v_1, v_2, \dots, v_n$ . Die Adjazenzmatrix von  $G$  ist die  $n \times n$  Matrix  $A_G = (a_{ij})_{i,j=1}^n$ , die von der gewählten Reihenfolge der Ecken abhängt und wie folgt definiert ist:

$$a_{ij} = \begin{cases} 1 & \text{wenn } \{v_i, v_j\} \in E \\ 0 & \text{sonst.} \end{cases}$$

In Abschnitt 1.5 haben wir auf ähnliche Art die Adjazenzmatrix einer Relation definiert. Die Adjazenzmatrix eines Graphen ist immer eine symmetrische quadratische Matrix mit Einträgen 0 und 1, auf der Hauptdiagonalen steht nur 0. Die andere Richtung gilt auch: Jede Matrix mit diesen Eigenschaften ist die Adjazenzmatrix eines Graphen.

**Beispiel.** Der Graph  $G =$



hat die Adjazenzmatrix

$$A_G = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Wir betonen nochmals, dass die Adjazenzmatrix von der gewählten Reihenfolge der Ecken eines Graphen abhängig ist.

Vielleicht denken Sie nun, dass diese Matrixdarstellung nur für Computer von Interesse ist, und dass wir menschlichen Wesen nichts davon haben, einen Graphen als eine Matrix anzusehen; schließlich codieren der Graph und die Adjazenzmatrix die gleiche Information. Um zu illustrieren, wie nützlich eine alternative Darstellung eines Graphen für uns sein kann, schauen wir uns die folgende einfache Verbindung zwischen der Matrixmultiplikation und der Abstandsfunktion des Graphen an.

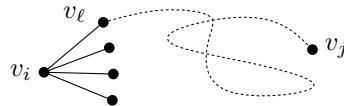
**4.2.4 Hilfssatz.** Sei  $G = (V, E)$  ein Graph mit Eckenmenge  $V = \{v_1, v_2, \dots, v_n\}$  und sei  $A = A_G$  seine Adjazenzmatrix. Mit  $A^k$  bezeichnen wir die  $k$ -te Potenz der Adjazenzmatrix (bezüglich der ganz normalen Matrixmultiplikation aus der linearen Algebra, d.h. die Matrix  $B = A^2$  hat die Einträge  $b_{ij} = \sum_{k=1}^n a_{ik}a_{kj}$ ). Mit  $a_{ij}^{(k)}$  bezeichnen

wir den Eintrag der Matrix  $A^k$  an der Stelle  $(i, j)$ . Dann ist  $a_{ij}^{(k)}$  die Anzahl der Spaziergänge in  $G$ , die bei der Ecke  $v_i$  beginnen, bei  $v_j$  enden und Länge genau  $k$  haben.

Induktionsbeweise haben oft die Eigenschaft, zwar einen korrekten, oft einfachen Beweis abzugeben, jedoch den Kern des Problems zu verstecken. Der Binomialsatz 3.3.3 ist z.B. so ein Fall. In dem nun folgenden Beweis ist Induktion genau das richtige, man sieht nicht nur, *dass* die Aussage wahr ist, sondern auch genau, *weshalb*.

*Beweis.* Wir führen Induktion nach  $k$ . Dass es einen Spaziergang der Länge 1 zwischen zwei Ecken gibt, bedeutet gerade, dass diese Ecken durch eine Kante miteinander verbunden sind, und deshalb ist der Hilfsatz für  $k = 1$  lediglich eine Umformulierung der Definition der Adjazenzmatrix.

Sei nun  $k > 1$  und seien  $v_i, v_j$  zwei beliebige (evtl. gleiche) Ecken. Jeder Spaziergang der Länge  $k$  von  $v_i$  nach  $v_j$  besteht aus einer Kante von  $v_i$  zu irgendeinem Nachbarn  $v_\ell$  von  $v_i$  und einem Spaziergang der Länge  $k - 1$  von  $v_\ell$  nach  $v_j$ :



Nach Induktionsvoraussetzung ist die Anzahl der Spaziergänge der Länge  $k - 1$  von  $v_\ell$  nach  $v_j$  gleich  $a_{\ell j}^{(k-1)}$ . Also ist die Anzahl der Spaziergänge der Länge  $k$  von  $v_i$  nach  $v_j$  gleich

$$\sum_{\{v_i, v_\ell\} \in E(G)} a_{\ell j}^{(k-1)} = \sum_{\ell=1}^n a_{i\ell} a_{\ell j}^{(k-1)}.$$

Das ist aber gerade der  $(i, j)$ -Eintrag im Produkt der Matrizen  $A$  und  $A^{k-1}$ , d.h.  $a_{ij}^{(k)}$ .  $\square$

**4.2.5 Folgerung.** Der Abstand zwischen je zwei Ecken  $v_i, v_j$  genügt der Gleichung

$$d_G(v_i, v_j) = \min\{k \geq 0: a_{ij}^{(k)} \neq 0\}.$$

Dieses Ergebnis hat überraschende Anwendungen. Z.B. gibt es Algorithmen, die für alle Eckenpaare in einem gegebenen Graphen den Abstand berechnen, indem sie trickreiche Algorithmen für Matrixmultiplikation verwenden (einige werden in Aho, Hopcroft, Ullman [12] beschrieben). So erhält man unerwartet schnelle Methoden zur Berechnung der Metrik  $d_G$ . Die Aufgaben 10 und 11 deuten weitere Anwendungen an.

Abschließend noch eine Bemerkung: Die Adjazenzmatrix ist nicht immer die beste Computerdarstellung eines Graphen. Speziell für

Graphen mit wenigen (d.h. deutlich weniger als  $\binom{n}{2}$ ) Kanten ist es in der Regel besser, für jede Ecke die Liste ihrer Nachbarn zu speichern. Für die schnelle Implementierung mancher Algorithmen sind oft andere, kompliziertere Darstellungen in Gebrauch.

## Aufgaben

1. Beweisen Sie, dass das Komplement eines unzusammenhängenden Graphen  $G$  zusammenhängend ist. (Das *Komplement* eines Graphen  $G = (V, E)$  ist der Graph  $(V, \binom{V}{2} \setminus E)$ .)
2. Was ist die größtmögliche Anzahl von Kanten in einem Graphen mit  $n$  Ecken und  $k$  Komponenten?
3. *Inf* Entwerfen Sie einen Algorithmus, der die Komponenten eines gegebenen Graphen  $G$  bestimmt. (Wenn  $G$  ein Graph mit  $n$  Ecken und  $m$  Kanten ist, dann sollten Sie mit  $O(n + m)$  Schritten auskommen.)
4. \*Beweisen Sie, dass ein Graph  $G$  genau dann bipartit ist, wenn er keine Kreise ungerader Länge enthält.
5. \*Beschreiben Sie alle Graphen, die keinen Weg (nicht notwendig induziert!) der Länge 3 enthalten.
6. \*Wenn Sie die vorige Aufgabe gelöst haben: Beschreiben Sie alle Graphen, die keinen Weg der Länge 4 enthalten.
7. Zeigen Sie: Wenn eine Funktion  $d: V \times V \rightarrow \mathbb{N} \cup \{0\}$  die Bedingungen 1–5 oben erfüllt, dann existiert ein Graph  $G = (V, E)$ , dessen Metrik  $d_G(v, v') = d(v, v')$  ist (für je zwei Ecken aus  $V$ ).
8. Überlegen Sie, wie man den „Durchmesser“ und den „Radius“ eines Graphen definieren könnte (so, dass die Definitionen mit der intuitiven Vorstellung dieser Begriffe übereinstimmen).
9. (a) Finden Sie einen zusammenhängenden Graphen auf  $n$  Ecken, für den jede Potenz  $A_G^1, A_G^2, \dots$  der Adjazenzmatrix mindestens eine 0 enthält.  
 (b) Sei  $G$  ein Graph auf  $n$  Ecken,  $A = A_G$  seine Adjazenzmatrix und  $I_n$  die  $n \times n$  Einheitsmatrix (alle Einträge der Hauptdiagonalen sind 1, der Rest ist 0). Beweisen Sie, dass  $G$  genau dann zusammenhängend ist, wenn die Matrix  $(I_n + A)^{n-1}$  keine 0 enthält.  
 (c) Welche Einträge der Matrix  $(I_n + A)^{n-1}$  sind 0, wenn der Graph  $G$  nicht zusammenhängend ist?
10. Zeigen Sie, dass ein Graph  $G$  genau dann ein Dreieck (d.h. einen  $K_3$ ) enthält, wenn es Indizes  $i$  und  $j$  gibt, so dass in beiden Matrizen  $A_G$  und  $A_G^2$  der  $(i, j)$ -Eintrag ungleich 0 ist. Dabei sei  $A_G$  die Adjazenzmatrix von  $G$ .

*Bemerkung.* In Verbindung mit Algorithmen für schnelle Matrixmultiplikation führt diese Beobachtung auf die schnellste bekannte Methode, um festzustellen, ob ein gegebener Graph ein Dreieck enthält; sie ist wesentlich schneller als der  $O(n^3)$ -Algorithmus, auf den man zuerst kommt.

11. \*Sei  $G$  ein Graph. Beweisen Sie die folgende Formel für die Anzahl der (nicht notwendig induzierten) Kreise der Länge 4 in  $G$ :

$$\frac{1}{8} \left( \text{Spur}(A_G^4) - 2|E(G)| - 4 \sum_{v \in V(G)} \binom{\deg_G(v)}{2} \right).$$

Hierbei ist  $A_G^4$  die vierte Potenz der Adjazenzmatrix und mit  $\text{Spur}(A_G^4)$  bezeichnet man die Summe der Hauptdiagonaleinträge von  $A_G^4$ . Die Zahlen  $\deg_G(v)$  werden erst im folgenden Abschnitt definiert. Übrigens ergibt sich aus dieser Formel ein  $O(n^3)$ -Algorithmus zum Bestimmen der Anzahl der Kreise der Länge 4, oder sogar ein noch schnellerer Algorithmus, wenn man schnelle Matrixmultiplikation verwendet.

12. Beweisen Sie, dass zwei Graphen  $G$  und  $G'$  genau dann isomorph sind, wenn es eine Permutationsmatrix  $P$  gibt, für die

$$A_{G'} = P A_G P^T.$$

Hier ist  $A_G$  die Adjazenzmatrix von  $G$  und  $P^T$  ist die zu  $P$  transponierte Matrix. Eine Matrix  $P$  heißt eine *Permutationsmatrix*, wenn ihre Einträge 0 und 1 sind und in jeder Zeile und jeder Spalte genau eine 1 steht.

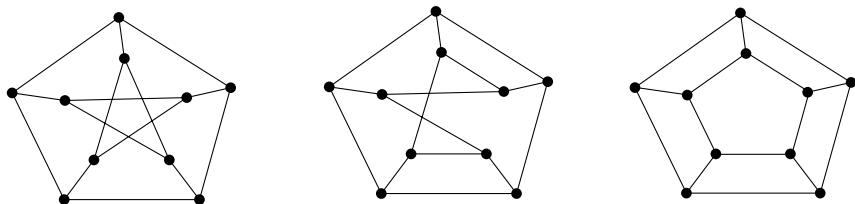
### 4.3 Gradfolgen

Sei  $G$  ein Graph, und sei  $v$  eine Ecke von  $G$ . Die Anzahl der Kanten von  $G$ , welche die Ecke  $v$  enthalten, wird  $\deg_G(v)$  abgekürzt. Die Zahl  $\deg_G(v)$  heißt der *Grad* von  $v$  in  $G$ .

Bezeichnen wir die Ecken von  $G$  mit  $v_1, v_2, \dots, v_n$  (in irgendeiner beliebigen Reihenfolge). Die Folge

$$(\deg_G(v_1), \deg_G(v_2), \dots, \deg_G(v_n))$$

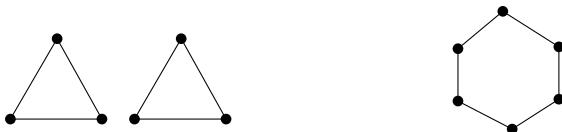
heißt eine *Gradfolge* des Graphen  $G$ . Für die verschiedenen möglichen Anordnungen der Ecken erhalten wir im Allgemeinen als Gradfolge ein und desselben Graphen verschiedene Zahlenfolgen, die sich in der Reihenfolge ihrer Glieder unterscheiden. Wir werden also zwei Gradfolgen als „gleich“ ansehen, wenn die eine aus der anderen durch Umordnen der Folgenglieder hervorgeht (um das exakt



**Abb. 4.4** Drei zusammenhängende nicht isomorphe Graphen mit der selben Gradfolge.

aufzuschreiben, würde man eine Äquivalenzrelation definieren...). Unsere Standardreihenfolge für Gradfolgen soll die aufsteigende sein (genauer: die nicht fallende), mit dem kleinsten Grad zuerst.

Man sieht leicht, dass zwei isomorphe Graphen die gleiche Gradfolge haben, dass also zwei Graphen mit unterschiedlichen Gradfolgen notwendig nicht isomorph sind. Graphen mit der gleichen Gradfolge brauchen jedoch nicht isomorph zu sein! Z.B. haben die Graphen



beide die Gradfolge  $(2, 2, 2, 2, 2, 2)$ , aber sie sind offensichtlich nicht isomorph, weil der eine zusammenhängend ist und der andere nicht. Alle drei Graphen in Abb. 4.4 haben die gleiche Gradfolge, nämlich  $(3, 3, 3, 3, 3, 3, 3, 3, 3, 3)$ , aber keine zwei von ihnen sind isomorph (der Beweis ist etwas schwieriger; siehe Aufgabe 1). Trotz dieser negativen Beispiele ist die Gradfolge ein wichtiges und leicht berechenbares Charakteristikum eines Graphen, und sie hilft oft bei der Unterscheidung nicht isomorpher Graphen.

Man interessiert sich dafür, welche Zahlenfolgen als Gradfolge eines Graphen vorkommen (auch wenn dieses Problem vielleicht nicht zu den allerwichtigsten der Graphentheorie gehört). Eine ganz einfache Bedingung ist durch die folgende Beobachtung gegeben:

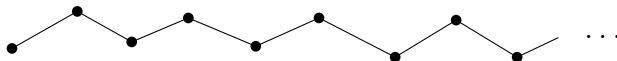
**4.3.1 Hilfssatz.** Für jeden Graphen  $G = (V, E)$  ist

$$\sum_{v \in V} \deg_G(v) = 2|E|.$$

*Beweis.* Der Grad einer Ecke  $v$  ist die Anzahl der Kanten, die  $v$  enthalten. Jede Kante enthält zwei Ecken, also ergibt das Aufsummieren aller Grade zweimal die Anzahl der Kanten. (Im Bild: Zeichnen Sie die Kanten als Doppelpfeile ein, d.h. als Linie mit „Spitzen“ an beiden Enden. Wie viele Pfeilspitzen zeichnen Sie insgesamt? An jeder Kante sind zwei Spitzen, also  $2|E|$ . Anders gezählt: An einer Ecke  $v$  kommen  $\deg_G(v)$  Spitzen an, also  $\sum_{v \in V} \deg_G(v)$ ).  $\square$

**4.3.2 Folgerung (Handshake Lemma).** In jedem Graph ist die Anzahl der Ecken ungeraden Grades eine gerade Zahl. (Oder: Die Anzahl der Gäste auf einer Geburtstagsfeier, die ungerade vielen anderen Gästen zur Begrüßung die Hand gegeben haben, ist immer gerade — auf jeder endlichen Party.)

Für Feste mit unendlich vielen Gästen ist das Handshake Lemma nicht wahr. Ein einseitig unendlicher Weg hat genau eine Ecke ungeraden Grades:



Das Handshake Lemma (Folgerung 4.3.2) und ähnlich einfache notwendige Bedingungen reichen nicht aus zur Charakterisierung der Folgen, die als Gradfolge eines Graphen vorkommen können (siehe Aufgabe 2). Eine vollständige Charakterisierung der Gradfolgen ist nicht ganz einfach, man verwendet dazu so genannte Flüsse in Netzwerken, die in diesem Buch nicht vorkommen. Wir erklären hier einen einfachen Algorithmus, der entscheidet, ob eine gegebene Folge ganzer Zahlen eine Gradfolge eines Graphen ist oder nicht. Der Algorithmus ist eine einfache Konsequenz des folgenden Resultats.

**4.3.3 Satz (Satz über Gradfolgen).** Sei  $D = (d_1, d_2, \dots, d_n)$  eine Folge natürlicher Zahlen,  $n > 1$ . Wir nehmen an,  $d_1 \leq d_2 \leq \dots \leq d_n$ , und definieren die Folge  $D' = (d'_1, \dots, d'_{n-1})$  durch

$$d'_i = \begin{cases} d_i & \text{für } i < n - d_n \\ d_i - 1 & \text{für } i \geq n - d_n. \end{cases}$$

Für  $D = (1, 1, 2, 2, 2, 3, 3)$  z.B. ist  $D' = (1, 1, 2, 1, 1, 2)$ . Dann ist  $D$  genau dann Gradfolge eines Graphen, wenn  $D'$  Gradfolge eines Graphen ist.

*Beweis.* Die eine Richtung ist einfach. Angenommen,  $D'$  ist Gradfolge eines Graphen  $G' = (V', E')$ , wo  $V' = \{v_1, v_2, \dots, v_{n-1}\}$  und

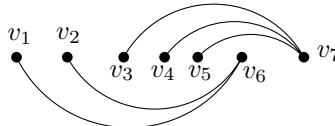
$\deg_G(v_i) = d'_i$  für alle  $i = 1, 2, \dots, n - 1$ . Wir fügen eine neue Ecke  $v_n$  hinzu, verschieden von  $v_1, \dots, v_{n-1}$ , und definieren einen neuen Graphen  $G = (V, E)$  durch

$$V = V' \cup \{v_n\}$$

$$E = E' \cup \{\{v_i, v_n\} : i = n - d_n, n - d_n + 1, \dots, n - 1\}.$$

In Worten heißt das: Die neue Ecke  $v_n$  ist mit den letzten  $d_n$  Ecken  $v_{n-d_n}, \dots, v_{n-1}$  von  $G'$  verbunden. Der neue Graph  $G$  ist so konstruiert, dass er offensichtlich die Gradfolge  $D$  hat. (Das dürfte die beste Methode sein, sich diesen Satz zu merken, indem man sich diese Konstruktion merkt.)

Die andere Richtung ist schwerer zu beweisen, wenn  $D$  eine Gradfolge ist, dass dann auch  $D'$  eine Gradfolge ist. Nehmen wir also an, dass  $D$  eine Gradfolge eines Graphen ist. Leider können wir die obige Konstruktion, mit der von  $D'$  zu  $D$  übergegangen sind, im Allgemeinen nicht umkehren; wenn wir eine Ecke größten Grades abpfücken, dann könnte es nämlich sein, dass sie mit anderen Ecken verbunden ist, als für unsere Konstruktion nötig wäre. Die folgende Abbildung zeigt ein Beispiel:



Wie betrachten also die Menge  $\mathcal{G}$  aller Graphen auf der Eckenmenge  $\{v_1, \dots, v_n\}$ , in denen der Grad von Ecke  $v_i$  gleich  $d_i$  ist,  $i = 1, 2, \dots, n$ . Wir beweisen die folgende Behauptung:

**Behauptung.** Die Menge  $\mathcal{G}$  enthält einen Graphen  $G_0$ , in dem die Ecke  $v_n$  genau zu den Ecken  $v_{n-d_n}, v_{n-d_n+1}, \dots, v_{n-1}$  benachbart ist, d.h. zu den letzten  $d_n$  Ecken.

Wenn wir solch einen Graphen  $G_0$  haben (wie in der Behauptung), dann ist schon klar, dass der Graph  $G' = (\{v_1, \dots, v_{n-1}\}, E')$ , wobei  $E' = \{e \in E(G_0) : v_n \notin e\}$ , die Gradfolge  $D'$  hat (d.h. wir können die Ecke  $v_n$  aus  $G_0$  entfernen), und das beweist den Satz über Gradfolgen. Es bleibt also nur noch, die Behauptung zu beweisen.

Wenn  $d_n = n - 1$  ist, dann ist  $v_n$  mit allen anderen Ecken verbunden und jeder Graph aus  $\mathcal{G}$  erfüllt die Behauptung. Angenommen,  $d_n < n - 1$ . Wir definieren für einen Graphen  $G \in \mathcal{G}$  die Zahl  $j(G)$

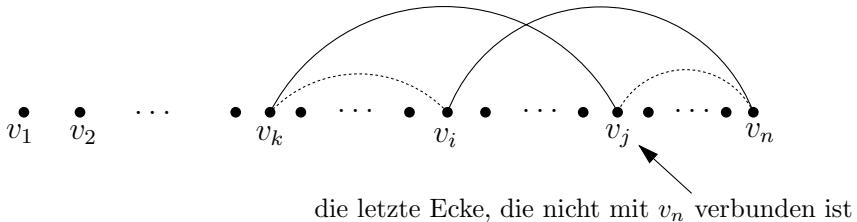


Abb. 4.5 Zum Beweis des Gradfolgen-Satzes.

als den größten Index  $j \in \{1, 2, \dots, n-1\}$ , für den  $\{v_j, v_n\} \notin E(G)$  ist. Sei  $G_0 \in \mathcal{G}$  ein Graph mit kleinstmöglichem Wert  $j(G)$ . Wir beweisen, dass  $j(G_0) = n - d_n - 1$  ist, und daraus sehen wir schon, dass  $G_0$  die Behauptung erfüllt.

Wir werden die Annahme  $j = j(G_0) > n - d_n - 1$  zum Widerspruch führen. Die Ecke  $v_n$  muss mit  $d_n$  Ecken benachbart sein, von denen höchstens  $d_n - 1$  einen größeren Index als  $v_j$  haben können. Deshalb gibt es einen Index  $i < j$ , für den  $v_i$  zu  $v_n$  adjazent ist, also ist  $\{v_j, v_n\} \notin E(G_0)$ ,  $\{v_i, v_n\} \in E(G_0)$  (vergleiche Abb. 4.5). Weil  $\deg_{G_0}(v_i) \leq \deg_{G_0}(v_j)$  ist, gibt es eine Ecke  $v_k$ , die mit  $v_j$  benachbart ist, aber nicht mit  $v_i$ . In dieser Situation betrachten wir einen neuen Graphen  $G' = (V, E')$ , wobei

$$E' = (E(G_0) \setminus \{\{v_i, v_n\}, \{v_j, v_k\}\}) \cup \{\{v_j, v_n\}, \{v_i, v_k\}\}.$$

Man prüft leicht nach, dass auch der Graph  $G'$  die Gradfolge  $D$  hat, und weil  $j(G') \leq j(G_0) - 1$  ist, erhalten wir einen Widerspruch zur Wahl von  $G_0$ . Damit ist die Behauptung bewiesen, also auch Satz 4.3.3.  $\square$

Wie schon gesagt ergibt sich aus diesem Satz eine einfache Methode zu entscheiden, ob eine gegebene Folge Gradfolge eines Graphen ist. Zur Illustration folgt ein konkretes Beispiel.

**Problem.** Entscheiden Sie, ob es einen Graphen mit Gradfolge  $(1, 1, 1, 2, 2, 3, 4, 5, 5)$  gibt.

*Lösung.* Wir reduzieren die gegebene Folge durch wiederholte Anwendung des Gradfolgensatzes 4.3.3:

$$(1, 1, 1, 2, 2, 3, 4, 5, 5)$$

$$(1, 1, 1, 1, 1, 2, 3, 4)$$

$$(1, 1, 1, 0, 0, 1, 2); \text{ umsortiert } (0, 0, 1, 1, 1, 2)$$

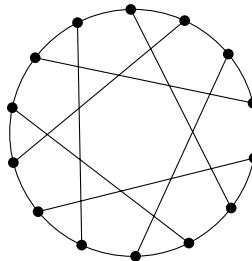
$(0, 0, 1, 1, 0, 0)$ ; umsortiert  $(0, 0, 0, 0, 1, 1)$   
 $(0, 0, 0, 0, 0)$ .

Da die letzte Folge ein Gradfolge eines Graphen ist (von dem Graph mit 5 Ecken und ohne Kanten), schließen wir, dass auch die ursprüngliche Folge eine Gradfolge ist. Konstruieren Sie einen solchen Graph!

## Aufgaben

1. Zeigen Sie, dass die drei Graphen in Abb. 4.4 paarweise nicht isomorph sind.
2. Konstruieren Sie ein Beispiel einer Folge der Länge  $n$ , in der jedes Folgenglied eine der Zahlen  $1, 2, \dots, n - 1$  ist, die eine gerade Anzahl ungerader Glieder hat und die dennoch nicht Gradfolge eines Graphen ist.
3. Wo im Beweis des Gradfolgensatzes haben wir die Annahme  $d_1 \leq d_2 \leq \dots \leq d_n$  gebraucht? Zeigen Sie, dass die Behauptung nicht mehr richtig ist, wenn wir diese Annahme weglassen.
4. Finden Sie ein kleinstmögliches Beispiel (mit kleinstmöglicher Eckenzahl) zweier zusammenhängender, nicht isomorpher Graphen mit der selben Gradfolge.
5. Zeichnen Sie alle nicht isomorphen Graphen auf sieben Ecken mit der Gradfolge  $(6, 3, 3, 3, 3, 3, 3)$ . Beweisen Sie, dass Sie keinen ausgelassen haben!
6. Geben Sie ein möglichst kleines Beispiel eines Graph mit 6 Ecken vom Grad 3, die anderen Ecken sollen Grad  $\leq 2$  haben, und mit 12 Kanten.
7. Sei  $G$  ein Graph mit 9 Ecken vom Grad 5 oder 6. Beweisen Sie, dass er mindestens 5 Ecken von Grad 6 hat oder mindestens 6 Ecken von Grad 5.
8. (a) Für welche  $n \geq 2$  gibt es einen Graphen, dessen Gradfolge aus  $n$  verschiedenen Zahlen besteht?  
(b) \*Für welche  $n$  gibt es einen Graphen auf  $n$  Ecken, dessen Gradfolge  $n - 1$  verschiedene Zahlen enthält (d.h. genau zwei Ecken haben den selben Grad)?
9. Sei  $G$  ein Graph, in dem alle Ecken mindestens den Grad  $d$  haben. Beweisen Sie, dass  $G$  einen (nicht notwendig induzierten) Weg der Länge  $d$  enthält.
10. \*Sei  $G$  ein Graph mit Maximalgrad 3. Beweisen Sie, dass die Ecken von  $G$  so mit zwei Farben gefärbt werden können (jede Ecke erhält eine Farbe), dass es keinen Weg der Länge 2 gibt, dessen 3 Ecken alle die gleiche Farbe erhalten.

11. \*\*Sei  $G$  ein Graph mit Minimalgrad 3. Zeigen Sie, dass  $G$  einen Kreis enthält, der nicht induziert ist (d.h. der eine *Sehne* enthält).
12. Ein Graph  $G$  heißt *k-regulär*, wenn alle seine Ecken den Grad  $k$  haben. Bestimmen Sie alle Paare  $(k, n)$ , für die es einen  $k$ -regulären Graphen auf  $n$  Ecken gibt.
13. Zeichnen Sie alle nicht isomorphen 3-regulären Graphen auf sechs Ecken.
14. Finden Sie einen 3-regulären asymmetrischen Graphen (siehe Aufgabe 4.1.3).
15. (a) Zeigen Sie, dass der Graph aus Abb. 9.3 zu dem folgenden isomorph ist:



- (b) \*Beweisen Sie, dass jeder 3-reguläre Graph mit 14 Ecken, der keinen Kreis der Länge 5 oder kleiner enthält, isomorph zu dem Graphen in (a) ist (dieser Graph heißt der *Heawood-Graph*). Wenn Ihnen dazu nichts einfällt, sollten Sie es nach der Bearbeitung von Kapitel 9 noch einmal versuchen.
16. \*Sei  $G$  ein zusammenhängender Graph, in dem je zwei verschiedene Ecken  $u, v$  entweder 0 oder 5 gemeinsame Nachbarn haben. Beweisen Sie, dass  $G$   $k$ -regulär ist für eine Zahl  $k$ .
  17. \*\* Beweisen Sie, dass jeder Graph mit einer geraden Eckenanzahl zwei Ecken mit einer geraden Anzahl gemeinsamer Nachbarn hat.

## 4.4 Eulersche Graphen

Dies hier ist eines der ältesten Probleme im Zusammenhang mit dem Zeichnen von Graphen.

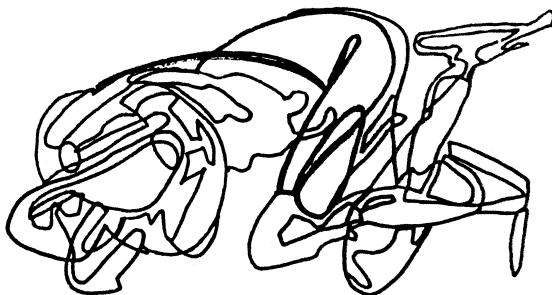
**Problem.** Zeichnen Sie einen gegebenen Graphen  $G = (V, E)$  in einem einzigen geschlossenen Zug, d.h. ohne den Stift abzusetzen. (Jede Kante soll nur einmal gezogen werden.)

Mathematisch kann man das so formalisieren: Finden Sie einen geschlossenen Spaziergang  $(v_0, e_1, v_1, \dots, e_{m-1}, v_{m-1}, e_m, v_0)$ , der alle Ecken und alle Kanten enthält, jede Kante genau einmal, die Ecken dürfen mehrfach vorkommen. („Geschlossen“ heißt, dass die erste und die letzte Ecke die gleiche sind.) So ein Spaziergang heißt eine *geschlossene Euler-Tour* in  $G$ , und ein Graph, der eine geschlossene Euler-Tour besitzt, heißt *Eulersch*.

Hier ein Beispiel eines Graphen, den man mit einer durchgehenden Linie zeichnen kann:



und noch eines:



Es stellt sich heraus, dass man Eulersche Graphen durch eine einfache „lokale“ Bedingung, die lediglich die Eckengrade verwendet, charakterisieren kann.

**4.4.1 Satz (Charakterisierung Eulerscher Graphen).** Ein Graph  $G = (V, E)$  ist genau dann Eulersch, wenn er zusammenhängend ist und alle Ecken geraden Grad haben.

*Erster Beweis.* Die eine Richtung ist recht einfach zu zeigen. Klar ist, dass ein Eulerscher Graph zusammenhängend sein muss. Der Grund, dass alle Eckengrade gerade sein müssen, ist, dass eine Rundtour aus jeder Ecke, in die sie hineinführt, auch wieder herausführen muss. Genauer: Wenn wir eine Richtung vorgeben, in der die Euler-Tour durchlaufen wird, und uns eine Ecke  $v \in V(G)$  ansehen, dann führen einige der Kanten in  $v$  hinein und andere führen hinaus — und zwar gleich viele, weil uns die Tour eine Bijektion definiert.

Die andere Richtung ist etwas anspruchsvoller. Um den Beweis übersichtlich zu halten, definieren wir eine *Tour* in  $G$  als einen Spaziergang, bei dem keine Kante wiederholt wird (Ecken dürfen hingegen wiederholt werden). Wir betrachten eine Tour  $T = (v_0, e_1, v_1, \dots, e_m, v_m)$  größtmöglicher Länge  $m$  in  $G$ . Wir beweisen, dass

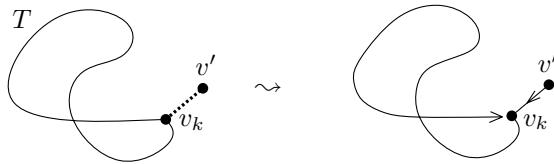
- (i)  $v_0 = v_m$ , und
- (ii)  $\{e_i : i = 1, 2, \dots, m\} = E$ .

*Ad (i).* Ist  $v_0 \neq v_m$ , dann ist die Ecke  $v_0$  zu einer ungeraden Anzahl von Kanten der Tour  $T$  inzident. Weil aber der Grad  $\deg_G(v_0)$  gerade ist, gibt es eine Kante  $e \in E(G)$ , die zu  $v_0$  inzident ist und nicht in  $T$  enthalten. Also könnten wir die Tour  $T$  um diese Kante verlängern — ein Widerspruch.

*Ad (ii).* Wir wissen schon, dass  $v_0 = v_m$  ist. Wir schreiben  $V(T)$  für die Menge der Ecken, die in  $T$  vorkommen und  $E(T)$  für die Menge der Kanten in  $T$ . Zuerst zeigen wir, dass  $V(T) = V$  ist. Wir nehmen an,  $V(T) \neq V$ . Weil  $G$  zusammenhängend ist, gibt es eine Kante der Form  $e = \{v_k, v'\} \in E(G)$ , wobei  $v_k \in V(T)$  und  $v' \notin V(T)$ . In diesem Fall hat die Tour

$$(v', e, v_k, e_{k+1}, v_{k+1}, \dots, v_{m-1}, e_m, v_0, e_1, v_1, \dots, e_k, v_k)$$

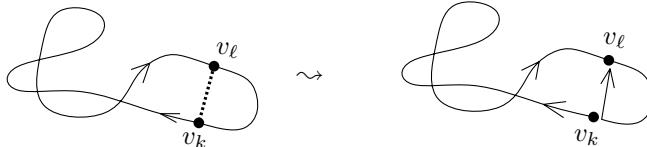
die Länge  $m + 1$  — ein Widerspruch. Im Bild sieht das so aus:



Wenn  $V(T) = V$ , aber  $E(T) \neq E$ , betrachten wir eine Kante  $e \in E \setminus E(T)$  und schreiben  $e = \{v_k, v_\ell\}$ . Analog zum vorigen Fall führt die neue Tour

$$(v_k, e_{k+1}, v_{k+1}, \dots, v_{m-1}, e_m, v_0, e_1, v_1, \dots, e_k, v_k, e, v_\ell)$$

zu einem Widerspruch. Im Bild:



Damit ist Satz 4.4.1 bewiesen.  $\square$

Der wesentliche Trick in dem Beweis ist, sich die *längstmögliche* Tour anzusehen; der Rest ist mehr oder weniger Routine. Diesen Trick sollten Sie sich merken, er kommt zuweilen wieder vor (in diesem Buch z.B. in Aufgabe 4.3.11 oder in Lemma 5.1.3). Varianten davon (betrachte ein „extremes“ unter den in Frage kommenden Objekten) sind sehr häufig nützlich.

**Zweiter Beweis von Satz 4.4.1.** Wir beschränken uns auf den Beweis, dass jeder zusammenhängende Graph, dessen Ecken alle geraden Grad haben, eine geschlossene Euler–Tour besitzt; die andere Richtung ist einfach, ein Beweis soll uns genügen. Wir starten mit folgendem Lemma:

**4.4.2 Lemma.** Sind bei einem Graphen  $G = (V, E)$  alle Eckengrade gerade, dann lässt sich die Kantenmenge  $E$  derart in disjunkte Teilmengen  $E_1, E_2, \dots, E_k$  partitionieren, dass jedes  $E_i$  die Kantenmenge eines Kreises ist.

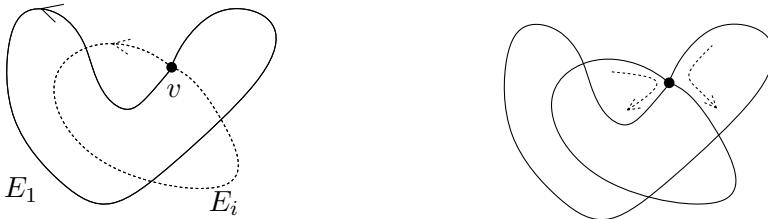
**Beweis des Lemmas.** Wir führen Induktion nach  $|E|$ . Für  $E = \emptyset$  stimmt die Aussage des Lemma. Im Induktionsschritt genügt es, zu zeigen, dass  $G$  mindestens einen Kreis enthält. Denn wenn wir die Kantenmenge eines in  $G$  enthaltenen Kreises mit  $E_1$  bezeichnen, dann hat auch der Graph  $(V, E \setminus E_1)$  nur gerade Grade, und daher lässt sich seine Kantenmenge gemäß Induktionsannahme in Kreise partitionieren.

Wir suchen also einen Kreis in  $G$  und dürfen dabei annehmen, dass  $E \neq \emptyset$ . Dazu konstruieren wir einen Weg in  $G$ . Wir starten mit einer beliebigen Ecke  $v_0$  mit Grad größer Null, wählen eine angrenzende Kante  $e_1$  und haben mit  $(v_0, e_1, v_1)$  den Anfang unseres Weges. Haben wir bereits einen Weg  $(v_0, e_1, \dots, v_{i-1}, e_i, v_i)$  konstruiert, dann schauen wir nach, ob  $v_i$  mit einer der anderen Ecken  $v_j$  des bis hier konstruierten Weges benachbart ist,  $0 \leq j \leq i-2$ . Wenn ja, dann bildet die Kante  $\{v_i, v_j\}$  zusammen mit dem Wegstück zwischen  $v_j$  und  $v_i$  den gesuchten Kreis. Ist  $v_i$  mit keiner der anderen Ecken  $v_j$  benachbart,  $0 \leq j \leq i-2$ , dann können wir den Weg mit einer Kante  $e_{i+1} = \{v_i, v_{i+1}\}$  verlängern, weil  $v_{i-1}$  nicht der einzige Nachbar von  $v_i$  sein kann. Denn andernfalls hätte  $v_i$  den (ungeraden) Grad 1.

In einem endlichen Graphen kann es keinen Weg unendlicher Länge geben, deshalb finden wir auf diese Weise früher oder später einen Kreis.  $\square$

Nun beenden wir den Beweis von Satz 4.4.1. Gegeben sei ein zusammenhängender Graph  $G = (V, E)$ , dessen Grade alle gerade sind. Dann zerlegen wir  $E$  in disjunkte Kreise  $E_1, E_2, \dots, E_k$ , ganz so wie im eben bewiesenen Lemma. Wir werden diese Kreise zu einer geschlossenen Euler-Tour verbinden, indem wir mit einem Kreis beginnen und die übrigen sukzessive hinzufügen. Genauer gesagt, beweisen wir folgendes: *Es sei  $G = (V, E)$  ein zusammenhängender Graph, dessen Kantenmenge  $E$  sich als disjunkte Vereinigung von  $\ell > 1$  Mengen  $E_1, E_2, \dots, E_\ell$  schreiben lässt, die jeweils in einer geschlossenen Tour durchlaufen werden können. Dann gibt es einen Index  $i \neq 1$ , so dass auch  $E_1 \cup E_i$  in einer geschlossenen Tour durchlaufen werden kann.*

Wiederholte Anwendung dieser Aussage erlaubt uns, die anfänglich  $k$  disjunkten Kreise zu einer geschlossenen Euler-Tour zusammenzusetzen. Zum Beweis der Aussage bezeichnen wir mit  $V_i$  die Menge all jener Ecken, die in mindestens einer Kante von  $E_i$  enthalten sind. Nun müssen wir nur noch die Existenz eines  $i \neq 1$  beweisen, für das  $V_1 \cap V_i \neq \emptyset$  ist, denn dann können wir (wie im folgenden Bild) die beiden geschlossenen Touren mit Kantenmengen  $E_1$  und  $E_i$  zu einer einzigen geschlossenen Tour verbinden.



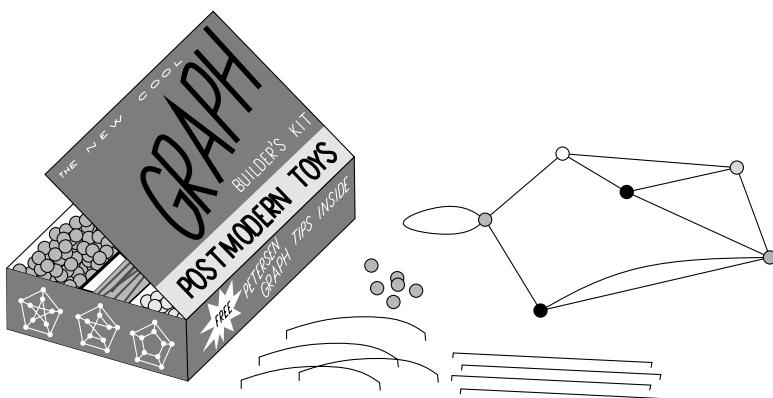
Nehmen wir also das Gegenteil an:  $V_1 \cap (V_2 \cup V_3 \cup \dots \cup V_k) = \emptyset$ . Dies bedeutet jedoch, dass es keine Kante gibt, die zwischen den Eckenmengen  $V_1$  und  $V_2 \cup V_3 \cup \dots \cup V_k$  verläuft (jede Kante von  $G$  liegt ja in einem  $E_i$ ), und somit ist  $G$  nicht zusammenhängend — ein Widerspruch.  $\square$

**Bemerkung zu Mehrfachkanten.** Wir haben die Kanten in einem Graphen als 2-elementige Teilmengen der Eckenmenge definiert, und wir werden dieser Definition in diesem Buch fast immer

treu bleiben. Das bedeutet jedoch unter anderem, dass zwei Ecken durch höchstens eine Kante verbunden sein können. In manchen Anwendungen ist es jedoch natürlich zuzulassen, dass zwei Ecken durch mehrere verschiedene Kanten, so genannte *Mehrfachkanten*, verbunden sind. Man spricht dann von *Multigraphen*. In diesem Fall brauchen wir natürlich eine neue mathematische Definition von Kanten, und da gibt es verschiedene Möglichkeiten.

Wir könnten die Kanten statt als Menge als eine Funktion auffassen, die jedem Paar  $\{u, v\}$  von Ecken eine nicht negative ganze Zahl  $m(u, v)$ , die *Vielfachheit* der Kante  $\{u, v\}$ , zuordnet.  $m(u, v) = 0$  würde also bedeuten, dass die Kante in dem Graph nicht vorhanden ist,  $m(u, v) = 1$  wäre eine „gewöhnliche“ (Einfach-) Kante, und  $m(u, v) > 1$  hieße, dass der Graph  $m(u, v)$  „Kopien“ der Kante  $\{u, v\}$  enthält. Ein Multigraph ist dann ein geordnetes Paar  $(V, m)$ , wobei  $m: \binom{V}{2} \rightarrow \{0, 1, 2, \dots\}$ .

Ein anderer, in gewisser Weise eleganterer Ansatz, Mehrfachkanten einzuführen, ist Kanten als „abstrakte“ Objekte anzusehen, d.h.  $E$  als eine endliche Menge anzusehen, disjunkt von der Eckenmenge  $V$ . Für jede Kante  $e \in E$  bestimmen wir dann das Paar der Enden von  $e$ . Das gleiche Eckenpaar kann bei mehreren Kanten vorkommen. Formal ist dann ein Graph mit Mehrfachkanten ein geordnetes Tripel  $(V, E, \varepsilon)$ , wobei  $V$  und  $E$  disjunkte Mengen sind und  $\varepsilon: E \rightarrow \binom{V}{2}$  eine Abbildung, welche sich die Enden der Kanten „merkt“. Man kann sich das so vorstellen: Wir haben einen Graphen-Bausatz mit einem Vorrat an Ecken und Kanten; die Abbildung  $\varepsilon$  ist dann die Bastelanleitung, die uns sagt, wie wir für einen bestimmten Graphen die Ecken und Kanten zusammenfügen müssen:



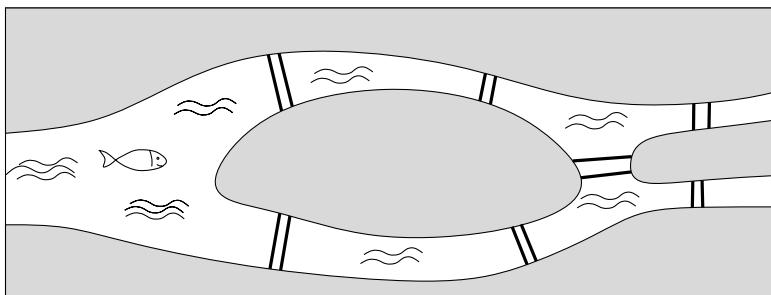
Zuweilen ist es nützlich, in einem Graphen auch *Schlingen* (englisch *loops*) zuzulassen, d.h. Kanten, die bei der gleichen Ecke beginnen und enden. Auch Schlingen kann man formal auf verschiedene Arten einführen. Am einfachsten ist es, eine Schlinge an einer Ecke  $v$  als die 1-elementige Menge  $\{v\}$  in der Kantenmenge  $E$  zu repräsentieren (in der die normalen Kanten 2-elementige Mengen sind). In Multigraphen kann man Schlingen zulassen, indem man  $\varepsilon$  als Abbildung in die Menge  $\binom{V}{2} \cup V$  auffasst; eine Schlinge  $e$  wird von  $\varepsilon$  auf ihre eindeutige Endstelle abgebildet.

Noch eine weitere Abwandlung der Graphen, die so genannten *gerichteten Graphen*, werden in Abschnitt 4.5 behandelt.

Wie wir Mehrfachkanten und Schlingen genau formalisieren, spielt fast nie eine Rolle, vorausgesetzt wir entscheiden uns für eine Methode und bleiben dabei.

## Aufgaben

- Der folgende Übersichtsplan zeigt eine Stadt mit sieben Brücken:



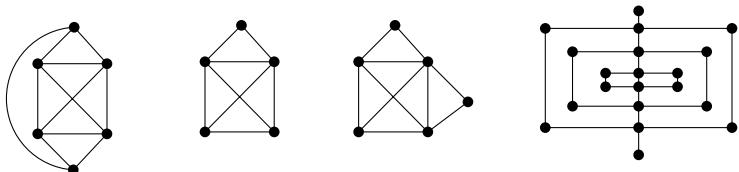
- Zeigen Sie, dass es nicht möglich ist durch die Stadt zu spazieren, jede Brücke genau einmal zu überschreiten und zum Ausgangspunkt zurückzukommen (Schwimmen ist verboten). Kann man genau einmal über jede Brücke gehen, wenn nicht verlangt wird, zum Ausgangspunkt zurückzukehren?

Dies ist eine historische Motivation für die Eulerschen Graphen. Der Plan stellt (in bewundernswerter Genauigkeit) einen Teil der Stadt Königsberg, Královec, Królewiec oder Kaliningrad dar — alle diese Namen hatte sie in ihrer bewegten Geschichte — und das Problem wurde 1736 durch Euler gelöst. Finden Sie die Stadt in einem modernen Atlas?

- Wie viele Brücken müssen die Königsberger noch bauen (und wo), damit eine Euler-Tour existiert?

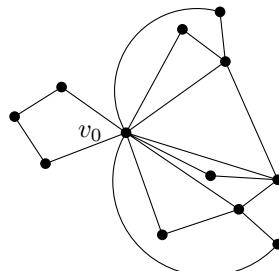
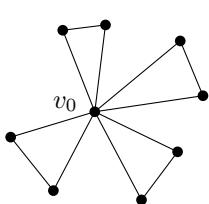
*Bemerkung.* Menschen, die das Konzept eines Graphen nicht kennen, könnten versuchen, das Königsberger Brückenproblem praktisch zu lösen, indem sie wirklich durch die Stadt spazieren. (Wäre doch eine Idee für das Königsberger Gastronomiegewerbe, mal einen Wettbewerb auszuschreiben.) Wenn Sie sich je in einer fremden Stadt durchschlagen mussten, werden Sie uns wahrscheinlich zustimmen, dass die Chance, die (negative) Antwort auf diese Weise herauszufinden, verschwindend gering ist. So gesehen ist Eulers Genie und die Einfachheit des Graphenmodells für diese Situation wirklich bewundernswert.

2. Charakterisieren Sie die Graphen, welche eine (nicht unbedingt geschlossene) Tour enthalten, die alle Kanten enthält.
3. Zeichnen Sie die folgenden Graphen mit einer durchgehenden Linie:

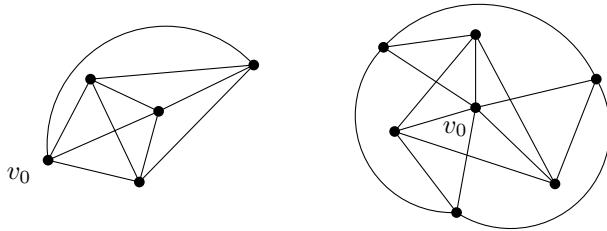


4. (a) Formulieren Sie auf der Grundlage des ersten Beweises von Satz 4.4.1 einen Algorithmus, der in einem gegebenen Graphen eine geschlossene Euler-Tour findet.  
 (b) *Inf* Wie schnell ist ihr Algorithmus aus (a) (d.h. wie viele Schritte benötigt er schlimmstenfalls für einen Graphen mit  $n$  Ecken und  $m$  Kanten)?  
 (c) *Inf* Bearbeiten Sie (a) und (b) nochmals, diesmal auf Grundlage des zweiten Beweises. Welcher der beiden Algorithmen hat die bessere Komplexität?
5. Prüfen Sie, dass Satz 4.4.1 auch für Graphen mit Schlingen und Mehrfachkanten gilt (was ist die geeignete Definition für den Grad einer Ecke in solchen Graphen?).
6. Charakterisieren Sie die Folgen nicht negativer ganzer Zahlen, die als Gradfolgen von Graphen auftreten können, wenn Schlingen und Mehrfachkanten erlaubt sind. (Eine Schlinge erhöht den Grad der Ecke um 2.)
7. Ein *Hamiltonscher Kreis* in einem Graphen  $G$  ist ein Kreis, der alle Ecken von  $G$  enthält. Die Idee ist der Eulerschen Tour sehr ähnlich, doch es stellt sich heraus, dass sie viel komplizierter zu handhaben ist. So ist z.B. kein effizienter Algorithmus bekannt, der entscheidet, ob ein Graph einen Hamiltonschen Kreis besitzt oder nicht. Diese und die zwei folgenden Aufgaben sind eine winzige Einführung in diesen Begriff (ein weiteres hübsches Ergebnis wird in Aufgabe 5.3.3 erwähnt).

- (a) Entscheiden Sie, welche der Graphen in Abb. 6.1 einen Hamiltonschen Kreis besitzen. Versuchen Sie, Ihre Behauptungen zu beweisen!
- (b) Konstruieren Sie zwei zusammenhängende Graphen mit der selben Gradfolge, einen mit und einen ohne Hamiltonschen Kreis.
8. Für einen Graph  $G$  bezeichnet man mit  $L(G)$  den so genannten *Kantengraph* von  $G$  (englisch *line graph*), der durch  $L(G) = (E, \{\{e, e'\} : e, e' \in E(G), e \cap e' \neq \emptyset\})$  gegeben ist. Sind die folgenden Aussagen für jeden Graphen  $G$  wahr?
- (a)  $G$  ist genau dann zusammenhängend, wenn  $L(G)$  zusammenhängend ist.
- (b)  $G$  ist genau dann Eulersch, wenn  $L(G)$  einen Hamiltonschen Kreis besitzt (siehe Aufgabe 7 für eine Definition des Hamiltonschen Kreises).
9. (a) \*Beweisen Sie, dass jeder Graph  $G$  mit  $n$  Ecken und Minimalgrad  $\frac{n}{2}$  einen Hamiltonschen Kreis besitzt (siehe Aufgabe 7 für eine Definition des Hamiltonschen Kreises).
- (b) \*Genügt es, in (a) Minimalgrad  $\lfloor n/2 \rfloor$  anzunehmen?
10. Wir nennen einen Graphen  $G = (V, E)$  *zufällig Eulersch* von der Ecke  $v_0$  aus, wenn jede maximale Tour, die bei  $v_0$  startet, schon eine geschlossene Eulersche Tour in  $G$  ist. Das heißt, wenn wir bei  $v_0$  beginnen und eine Kante nach der anderen zeichnen, dann können wir immer eine beliebige Fortsetzungskante wählen unter allen noch nicht gezeichneten, ohne in eine Sackgasse zu laufen. (Es wäre praktisch, wenn Galerien oder Zoos zufällig Eulersch wären, doch leider sind sie es selten. Das Ergebnis aus (c) unten deutet an, warum das so ist.)
- (a) Beweisen Sie, dass die folgenden Graphen zufällig Eulersch sind:



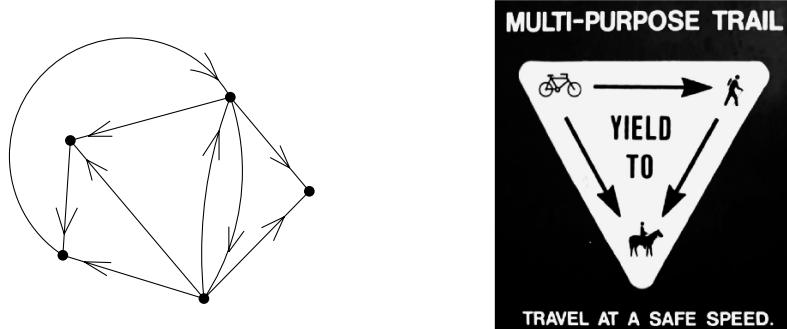
- (b) Zeigen Sie, dass die nächsten Graphen nicht zufällig Eulersch sind:



(c) \*Beweisen Sie die folgende Charakterisierung zufällig Eulerscher Graphen. Ein zusammenhängender Graph  $G = (V, E)$ , dessen Ecken alle geraden Grad haben, ist genau dann von einer Ecke  $v_0$  aus zufällig Eulersch, wenn der Graph  $(V \setminus \{v_0\}, \{e \in E : v_0 \notin e\})$  keinen Kreis enthält.

## 4.5 Gerichtete Eulersche Graphen

Bisher haben wir nur „ungerichtete“ Graphen betrachtet — die Kanten waren ungeordnete Paare von Ecken. Es gibt jedoch viele Situationen, in denen so etwas wie Einbahnstraßen vorkommen:



Um solche Situationen zu modellieren, führt man gerichtete Graphen ein, in denen jede Kante eine Richtung hat.

**4.5.1 Definition.** Ein gerichteter Graph  $G$  ist ein Paar  $(V, E)$ , wobei  $E$  eine Teilmenge des Kartesischen Produkts  $V \times V$  ist. Die geordneten Paare  $(x, y) \in E$  heißen gerichtete Kanten. Wir sagen, dass eine gerichtete Kante  $e = (x, y)$  den Kopf  $y$  und den Fuß  $x$  hat, oder<sup>4</sup> dass  $e$  eine Kante von  $x$  nach  $y$  ist.

<sup>4</sup>Hier noch etwas Terminologie: Oft wird das Kunstwort *Digraph* verwendet, das aus dem englischen Wort *directed graph* abgeleitet ist. Eine gerichtete Kante heißt oft *arc*. Statt „gerichtet“ sagt man oft „orientiert“, und ein *orientierter Graph* ist oft ein spezieller gerichteter Graph, in dem die gerichteten Kanten  $(x, y)$  und  $(y, x)$  nicht zugleich vorkommen dürfen (also ein einfacher Graph, in dem jede Kante eine Orientierung erhält).

Weiter könnten wir gerichtete Graphen mit Mehrfachkanten einführen, und für jedes andere Konzept oder Problem auf ungerichteten Graphen könnten wir das gerichtete Analogon untersuchen. Manchmal sind die Ergebnisse für gerichtete Graphen einfache Abwandlungen der Ergebnisse für ungerichtete Graphen. In anderen Problemen unterscheiden sich die gerichteten und ungerichteten Fälle wesentlich, und in aller Regel ist die gerichtete Version die kompliziertere. In diesem Buch befassen wir uns fast ausschließlich mit ungerichteten Graphen. Machen wir hier eine Ausnahme: Wir führen gerichtete Eulersche Graphen ein und beschreiben eine interessante Anwendung.

Einem aufmerksamen Leser ist vielleicht aufgefallen, dass ein gerichteter Graph  $G = (V, E)$  eine Relation auf der Menge  $V$  ist. Beide Konzepte sind üblich, und beide haben ihre Berechtigung, denn je nach Problemstellung ist die eine oder die andere Formulierung handlicher.

Es ist recht natürlich, eine *gerichtete Tour* in einem gerichteten Graphen  $G = (V, E)$  als eine Folge

$$(v_0, e_1, v_1, e_2, \dots, e_m, v_m)$$

zu definieren, wobei  $e_i = (v_{i-1}, v_i) \in E$  für  $i = 1, 2, \dots, m$  und  $e_i \neq e_j$  für  $i \neq j$ . Entsprechend können wir gerichtete Spaziergänge, gerichtete Wege und gerichtete Kreise definieren.

Wir nennen einen gerichteten Graphen  $(V, E)$  *Eulersch*, wenn er eine geschlossene gerichtete Tour zulässt, die alle Ecken enthält und jede gerichtete Kante genau einmal benutzt. Auch für diese gerichtete Variante Eulerscher Graphen gibt es eine attraktive Charakterisierung. Bevor wir das Resultat formulieren, erweitern wir noch unser Vokabular.

Für eine gegebene Ecke  $v$  in einem gerichteten Graphen  $G = (V, E)$  bezeichnen wir die Anzahl der gerichteten Kanten, die in  $v$  enden (d.h. die  $v$  als Kopf haben), mit  $\deg_G^+(v)$ . Analog dazu steht  $\deg_G^-(v)$  für die Anzahl gerichteter Kanten, die aus  $v$  herausführen. Die Zahl  $\deg_G^+(v)$  heißt der *Eingrad* von  $v$  und  $\deg_G^-(v)$  heißt der *Ausgrad* von  $v$ .

Zu jedem gerichteten Graphen  $G = (V, E)$  kann man den zu Grunde liegenden ungerichteten Graphen  $\bar{G} = (V, \bar{E})$  definieren, wobei

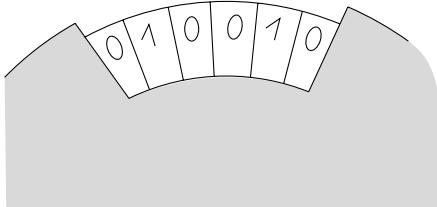
$$\bar{E} = \{\{x, y\}: (x, y) \in E \text{ oder } (y, x) \in E\}.$$

Es folgt nun die versprochene Charakterisierung gerichteter Eulerscher Graphen.

**4.5.2 Hilfssatz.** Ein gerichteter Graph ist genau dann Eulersch, wenn der zu Grunde liegende ungerichtete Graph zusammenhängend<sup>5</sup> ist und wenn  $\deg_G^+(v) = \deg_G^-(v)$  ist für jede Ecke  $v \in V(G)$ .

Der Beweis dieses Hilfssatzes ist dem Beweis von Satz 4.4.1 sehr ähnlich und daher eine geeignete Aufgabe.

**Eine Anwendung.** Auf den Rand eines Rades soll eine Folge von  $n$  Ziffern 0 und 1 geschrieben werden. Durch ein Sichtfenster sehen wir  $k$  aufeinanderfolgende Ziffern:



Die Folge von  $n$  Ziffern soll so gewählt werden, dass die Position des Rades aus den  $k$  im Fenster sichtbaren Ziffern stets eindeutig bestimmt werden kann, egal in welcher Stellung sich das Rad befindet. (Sie können sich z.B. vorstellen, dass auf diese Art die Winkelstellung einer Radarschüssel kontrolliert werden soll.) Für ein gegebenes  $k$  möchten wir ein Rad mit möglichst großem  $n$  herstellen (damit die Winkelstellung möglichst genau kontrolliert werden kann). Eine mathematische Formulierung des Problems ist die folgende:

**Problem.** Finde eine möglichst lange zyklische Folge von Ziffern 0 und 1, so dass sich kein  $k$ -Tupel von aufeinanderfolgenden Ziffern an einer anderen Stelle wiederholt.

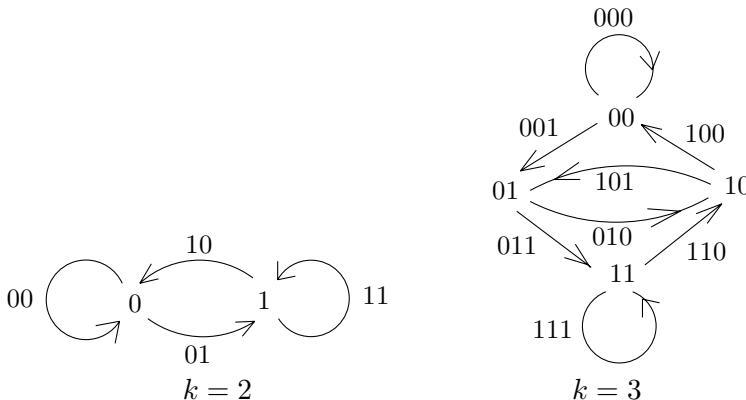
Mit  $\ell(k)$  bezeichnen wir die größtmögliche Anzahl von Ziffern in so einer Folge für ein gegebenes  $k$ . Wir beweisen das folgende überraschende Ergebnis:

**Hilfssatz.** Für jedes  $k \geq 1$  ist  $\ell(k) = 2^k$ .

*Beweis.* Da es nur  $2^k$  viele Ziffernfolgen der Länge  $k$  aus 0 und 1 gibt, kann die zyklische Folge nicht länger sein als  $2^k$ . Es bleibt zu

---

<sup>5</sup>Ein gerichteter Graph, dessen zu Grunde liegender ungerichteter Graph zusammenhängend ist, heißt *schwach zusammenhängend* (ein Polizist, der die Einbahnstraßenschilder nicht beachten muss, kann von jeder Ecke zu jeder anderen). Ein gerichteter Graph heißt *stark zusammenhängend*, wenn man von jeder Ecke über einen gerichteten Weg zu jeder anderen gelangen kann.



**Abb. 4.6** Der gerichtete Graph in dem Problem mit der zyklischen Ziffernfolge.

zeigen, dass die Länge  $2^k$  tatsächlich erreicht werden kann; wir konstruieren eine Folge der Länge  $2^k$  mit der gewünschten Eigenschaft. Der Fall  $k = 1$  ist einfach, wir können also  $k \geq 2$  annehmen.

Definieren Sie einen Graphen  $G = (V, E)$  wie folgt:

- $V$  ist die Menge aller Folgen der Länge  $k - 1$  aus 0 und 1 (also  $|V| = 2^{k-1}$ ).
- Die gerichteten Kanten sind alle Paare von Ziffernfolgen der Länge  $(k - 1)$  von der Form

$$((a_1, \dots, a_{k-1}), (a_2, \dots, a_k)).$$

Die gerichteten Kanten korrespondieren bijektiv zu den Ziffernfolgen der Länge  $k$

$$(a_1, a_2, \dots, a_k),$$

und deshalb ist  $|E| = 2^k$ . Im Folgenden wollen wir für die gerichtete Kante  $((a_1, \dots, a_{k-1}), (a_2, \dots, a_k))$  kürzer  $(a_1, a_2, \dots, a_k)$  schreiben. Das sollte keine Verwirrung stiften.

Man sieht schnell, dass  $\deg_G^-(v) = \deg_G^+(v) = 2$  für jede Ecke  $v \in V$ . Der  $G$  zu Grunde liegende ungerichtete Graph ist zusammenhängend, weil wir jede Folge in die Nullfolge verwandeln können, indem wir wiederholt die letzte Ziffer weglassen und vorne eine Null ergänzen. Daher ist  $G$  ein gerichteter Eulerscher Graph. Beispiele für  $k = 2$  und  $k = 3$  sind in Abb. 4.6 gezeigt.

Sei  $|E| = 2^k = K$  und sei  $(e^1, \dots, e^K)$  die Folge der Kanten in irgendeiner gerichteten Euler-Tour von  $G$ . Jede Kante  $e^i$  hat die

Form  $e^i = (a_1^i, \dots, a_k^i)$ . Die gewünschte zyklische Folge der Länge  $K$  aus Ziffern 0 und 1 können wir als  $(a_1^1, a_1^2, \dots, a_1^K)$  definieren. Das heißt, wir nehmen einfach den ersten Eintrag aus jedem  $e^i$ . In dieser Folge entspricht jede Teilfolge von  $k$  aufeinanderfolgenden Ziffern einer gerichteten Kante der Euler–Tour, und weil in der Tour keine gerichtete Kante wiederholt wird, kommt keine der  $k$ -ziffrigen Teilfolgen mehrmals vor. Damit ist  $\ell(k) = 2^k$  bewiesen.

Aus dem Graphen in Abb. 4.6 finden wir z.B. für  $k = 2$  eine Tour 00, 01, 11, 10 und die zugehörige zyklische Folge 0011; für  $k = 3$  ist eine Tour 000, 001, 011, 111, 110, 101, 010, 100 und die zugehörige zyklische Folge ist 00011101.  $\square$

Die in obigem Beweis konstruierten Graphen heißen die *De Bruijn Graphen*. Obwohl sie exponentiell groß sind in  $k$ , kann man die Nachbarn einer gegebenen Ecke schnell finden. Andere Graphen mit ähnlichen Eigenschaften sind die  *$k$ -dimensionalen Würfel*: Die Eckenmenge besteht wieder aus allen Folgen der Länge  $k$ , die aus 0 und 1 bestehen, und zwei Folgen sind dann adjazent, wenn sie sich in genau einer Koordinate unterscheiden. Wenn Sie die Würfelgraphen für  $k \leq 3$  aufzeichnen, dann verstehen Sie den Namen.

## Aufgaben

1. Beweisen Sie Hilfssatz 4.5.2.
2. Entwerfen Sie einen Algorithmus, der in einem gerichteten Graphen eine gerichtete Euler–Tour findet.
3. Welche gerichteten Graphen können ohne den Stift abzusetzen in einem (nicht unbedingt geschlossenen) Zug gezeichnet werden? Jede gerichtete Kante muss genau einmal gezogen werden, und zwar in der Richtung vom Fuß zum Kopf.
4. Sei  $G = (V, E)$  ein Graph. Eine *Orientierung* von  $G$  ist ein orientierter Graph  $G' = (V, E')$ , der dadurch entsteht, dass jede Kante  $\{u, v\} \in E$  entweder durch die gerichtete Kante  $(u, v)$  oder durch die gerichtete Kante  $(v, u)$  ersetzt wird. Anders gesagt:  $G'$  ist eine Orientierung von  $G$ , wenn  $G$  der  $G'$  zu Grunde liegende ungerichtete Graph ist.
  - (a) Beweisen Sie: Wenn alle Grade von  $G$  gerade sind, dann existiert eine Orientierung  $H$  von  $G$ , so dass  $\deg_H^+(v) = \deg_H^-(v)$  ist für alle Ecken  $v \in V(G)$ .
  - (b) Beweisen Sie, dass ein gerichteter Graph  $G$ , bei dem  $\deg_G^+(v) = \deg_G^-(v)$  für alle Ecken  $v$  gilt, genau dann stark zusammenhängend ist, wenn er schwach zusammenhängend ist.

5. \*Sei  $G = (V, E)$  ein gerichteter Graph und sei  $w: E \rightarrow \mathbb{R}$  eine Funktion, die jeder Kante eine reelle Zahl zuordnet. Eine auf der Eckenmenge definierte Funktion  $p: V \rightarrow \mathbb{R}$  heißt *Potenzial* für  $w$ , wenn  $w(e) = p(v) - p(u)$  ist für jede gerichtete Kante  $e = (u, v)$ . Beweisen Sie, dass genau dann ein Potenzial für  $w$  existiert, wenn die Summe der Werte von  $w$  über die Kanten jedes beliebigen gerichteten Kreises in  $G$  0 ist.
6. \*Beweisen Sie, dass die folgenden zwei Bedingungen für einen stark zusammenhängenden gerichteten Graphen  $G$  äquivalent sind:
  - (i)  $G$  enthält einen gerichteten Kreis gerader Länge.
  - (ii) die Ecken von  $G$  können so mit zwei Farben gefärbt werden (jede Ecke erhält eine Farbe), dass es für jede Ecke  $u$  eine gerichtete Kante  $(u, v)$  gibt, so dass  $v$  eine andere Farbe hat als  $u$ .
7. \*\*Ritter aus zwei verfeindeten Burgen sitzen um einen runden Tisch bei Friedensverhandlungen. Die Anzahl der Ritter, zu deren Rechten ein Feind sitzt, ist die gleiche wie die Anzahl der Ritter, zu deren Rechten ein Verbündeter sitzt. Beweisen Sie, dass die Gesamtzahl der Ritter durch 4 teilbar ist.
8. \*Ein *Turnier* ist ein gerichteter Graph, in dem für je zwei verschiedene Ecken  $u, v$  genau eine der gerichteten Kanten  $(u, v)$  und  $(v, u)$  in dem Graph enthalten ist. Beweisen Sie, dass es in jedem Turnier einen gerichteten Weg gibt, der durch alle Ecken führt (so ein Weg heißt *Hamiltonsch*).
9. \*Beweisen Sie, dass es in jedem Turnier (Definition siehe Aufgabe 8) eine Ecke  $v$  gibt, die von jeder anderen Ecke aus durch einen gerichteten Weg der Länge höchstens 2 erreicht werden kann. Eine amüsante Interpretation ist die folgende: Zwischen je zwei von  $n$  Personen besteht eine Dominanzrelation. Eine Person, die alle anderen dominiert, heißt *Diktator*. Eine Person  $P$  heißt *graue Eminenz*, wenn für alle Personen  $Q \neq P$ , die  $P$  nicht dominiert, eine dritte Person  $R$  existiert, die von  $P$  dominiert wird und die selbst  $Q$  dominiert (also  $P \rightarrow Q$  oder es existiert ein  $R$  mit  $P \rightarrow R \rightarrow Q$ ). Nicht in jeder Gruppe von Personen gibt es einen Diktator; aber wenn Sie die Aufgabe gelöst haben, dann wissen Sie: Es gibt immer eine graue Eminenz!

## 4.6 2-Zusammenhang

Ein Graph  $G$  heißt  *$k$ -fach eckenzusammenhängend*, wenn er mindestens  $k + 1$  Ecken hat und nach Entfernen von beliebigen  $k - 1$  Ecken immer noch zusammenhängend ist. Ein Graph  $G$  heißt  *$k$ -fach kanten-zusammenhängend*, wenn er nach Entfernen von beliebigen  $k - 1$  Kanten immer noch zusammenhängend ist. Die größte Zahl  $k$ , für die  $G$   $k$ -fach

eckenzusammenhängend ist, heißt die (*Ecken-*) *Zusammenhangszahl* von  $G$ , und analog wird die *Kantenzusammenhangszahl* definiert.

Wenn ein Graph ein Eisenbahnnetz, Nahverkehrslinien, Telefonleitungen oder ähnliches repräsentiert, dann darf man bei höherem Zusammenhang auf eine gewisse Robustheit hoffen, dass das System auch in einer kritischen Situation noch halbwegs funktioniert, wenn ein oder mehrere Knoten oder Verbindungen nicht ordnungsgemäß arbeiten. Die Begriffe Ecken- und Kantenzusammenhang sind von recht großer theoretischer und praktischer Bedeutung in der Graphentheorie. Ein verwandtes Konzept ist das der so genannten *Flüsse in Netzwerken*, die wir in diesem Buch jedoch nicht untersuchen. Hier wollen wir unser Augenmerk auf 2-fachen Eckenzusammenhang richten, der in einem Kapitel über ebene Graphen eine Rolle spielt; außerdem dient er uns zur Illustration einiger Beweismethoden und Konstruktionen.

Statt von 2-fachem Eckenzusammenhang werden wir kürzer von 2-Zusammenhang sprechen. Der Übersicht halber wiederholen wir noch einmal die Definition:

**4.6.1 Definition (2-Zusammenhang).** Ein Graph  $G$  mit mindestens drei Ecken heißt 2-zusammenhängend, wenn er nach Entfernen einer — egal welcher! — Ecke zusammenhängend bleibt.

Anders ausgedrückt: Ein Graph  $G$  mit mindestens drei Ecken ist nicht 2-zusammenhängend, wenn es eine Ecke gibt, deren Entfernung aus  $G$  mehrere Komponenten erzeugt. Es ist leicht zu sehen, dass ein 2-zusammenhängender Graph auch zusammenhängend ist (hier brauchen wir die Bedingung, dass ein 2-zusammenhängender Graph mindestens drei Ecken hat — klar?). In diesem Abschnitt geben wir alternative Beschreibungen 2-zusammenhängender Graphen. Bevor wir damit beginnen, führen wir die Notation für ein paar graphentheoretische Operationen ein. Dadurch werden einige Formeln wesentlich einfacher, und auch im Folgenden wird es von Nutzen sein.

**4.6.2 Definition (Ein paar Operationen mit Graphen).** Sei  $G = (V, E)$  ein Graph. Wir definieren diverse neue Graphen, die durch Veränderungen an  $G$  entstehen:

- (Entfernen einer Kante)

$$G - e = (V, E \setminus \{e\}),$$

wobei  $e \in E$  eine Kante von  $G$  ist;

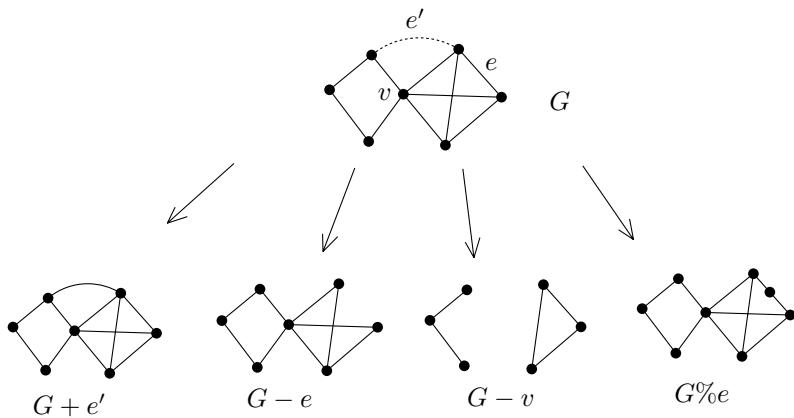


Abb. 4.7 Beispiele für Graphenoperationen.

- (Einfügen einer neuen Kante)

$$G + \bar{e} = (V, E \cup \{\bar{e}\}),$$

wobei  $\bar{e} \in \binom{V}{2} \setminus E$  ein Paar von Ecken ist, das in  $G$  keine Kante ist (eine „Nicht-Kante von  $G$ “);

- (Entfernen einer Ecke)

$$G - v = (V \setminus \{v\}, \{e \in E: v \notin e\}),$$

wobei  $v \in V$  (wir entfernen die Ecke  $v$  und alle Kanten, die  $v$  als einen Endpunkt haben);

- (Unterteilen einer Kante)

$$G\%e = \left( V \cup \{z\}, (E \setminus \{\{x, y\}\}) \cup \{\{x, z\}, \{z, y\}\} \right),$$

wobei  $e = \{x, y\} \in E$  eine Kante ist und  $z \notin V$  eine neue Ecke (wir „zeichnen eine neue Ecke  $z$ “ mitten auf die Kante  $\{x, y\}$ ).

Wir nennen einen Graphen  $G'$  eine Unterteilung des Graphen  $G$ , wenn  $G'$  isomorph zu einem Graphen ist, der aus  $G$  durch eine Folge von Kantenunterteilungen entsteht.

Abbildung 4.7 zeigt Beispiele der eben definierten Operationen.  
Nun zurück zum 2-Zusammenhang. Hier ist die erste bemerkenswerte Charakterisierung:

**4.6.3 Satz.** Ein Graph  $G$  ist genau dann 2-zusammenhängend, wenn es zu je zwei Ecken in  $G$  einen Kreis in  $G$  gibt, der diese zwei Ecken enthält.

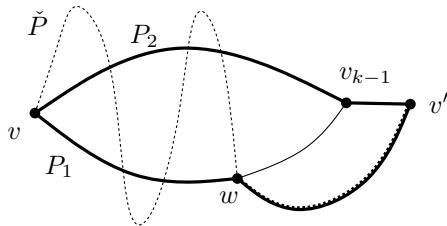
Dieser Satz ist ein Spezialfall eines sehr wichtigeren allgemeineren Satzes, dem *Satz von Menger*, der folgendes aussagt: Sind  $x$  und  $y$  zwei Ecken in einem  $k$ -fach ecken-zusammenhängenden Graphen, dann gibt es ein System von  $k$  Wegen zwischen  $x$  und  $y$ , die paarweise disjunkt sind (bis auf die gemeinsamen Enden  $x$  und  $y$  natürlich).

*Beweis.* Die Bedingung ist zweifellos hinreichend, damit  $G$  2-zusammenhängend ist, denn wenn zwei Ecken  $v, v'$  auf einem gemeinsamen Kreis liegen, dann gibt es zwischen ihnen zwei Wege, die außer den Enden keine Ecke gemeinsam haben. Daher können  $v$  und  $v'$  nicht durch Entfernen einer einzelnen Ecke in verschiedene Komponenten fallen.

Nun zum Beweis der anderen Richtung. Wir werden die Existenz eines gemeinsamen Kreises für  $v$  und  $v'$  durch Induktion nach  $d_G(v, v')$ , dem Abstand der Ecken  $v$  und  $v'$ , beweisen.

Für den Induktionsanfang sei  $d_G(v, v') = 1$ . Das heißt, dass  $\{v, v'\} = e \in E(G)$ . Wegen des 2-Zusammenhangs von  $G$  ist der Graph  $G - e$  zusammenhängend (Vorsicht!  $e$  ist eine Kante und keine Ecke, aber wäre  $G - e$  nicht zusammenhängend, dann wäre auch mindestens einer der Graphen  $G - v$ ,  $G - v'$  nicht zusammenhängend). Deshalb gibt es in dem Graphen  $G - e$  einen Weg von  $v$  nach  $v'$ , und dieser Weg bildet zusammen mit der Kante  $e$  den gesuchten Kreis, der  $v$  und  $v'$  enthält.

Als Induktionsvoraussetzung nehmen wir an, dass jedes Eckenpaar im Abstand kleiner als  $k$  auf einem gemeinsamen Kreis liegt, für ein  $k \geq 2$ . Betrachten Sie zwei Ecken  $v, v' \in V$  mit Abstand  $k$ . Sei  $P = (v = v_0, e_1, v_1, \dots, e_k, v_k = v')$  ein kürzester Weg von  $v$  nach  $v'$ . Weil  $d_G(v, v_{k-1}) = k - 1$  ist, gibt es einen Kreis, der  $v$  und  $v_{k-1}$  enthält. Dieser Kreis besteht aus zwei Wegen  $P_1$  und  $P_2$  zwischen  $v$  und  $v_{k-1}$ . Betrachten wir nun den Graph  $G - v_{k-1}$ . Er ist zusammenhängend und enthält daher einen Weg  $\check{P}$  von  $v$  nach  $v'$ , der natürlich nicht  $v_{k-1}$  enthält. Sei  $w$  die letzte Ecke auf dem Weg  $\check{P}$  (wenn man von  $v$  nach  $v'$  geht), die zu einem der Wege  $P_1, P_2$  gehört, wie in folgender Abbildung:



Ohne Beschränkung der Allgemeinheit können wir annehmen, dass  $w$  eine Ecke von  $P_1$  ist. Den gesuchten Kreis, der  $v$  und  $v'$  enthält, kann man nun aus dem Weg  $P_2$ , aus dem Teil des Weges  $P_1$  zwischen  $v$  und  $w$  und aus dem Teil des Weges  $\check{P}$  zwischen  $w$  und  $v'$  bilden (in der Abbildung durch eine dicke Linie gekennzeichnet).  $\square$

#### 4.6.4 Beobachtung.

*Ein Graph  $G$  ist genau dann 2-zusammenhängend, wenn jede Unterteilung von  $G$  2-zusammenhängend ist.*

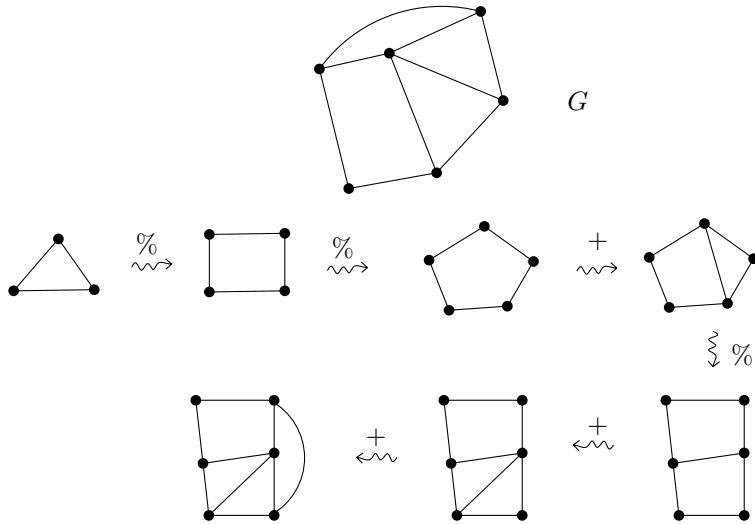
*Beweis.* Es genügt zu zeigen, dass für jede Kante  $e \in E(G)$  der Graph  $G$  genau dann 2-zusammenhängend ist, wenn  $G\%e$  2-zusammenhängend ist. Ist  $v \in V(G)$  eine Ecke von  $G$ , dann sieht man leicht, dass  $G - v$  genau dann zusammenhängend ist, wenn  $(G\%e) - v$  zusammenhängend ist. Deshalb folgt aus dem 2-Zusammenhang von  $G\%e$ , dass auch  $G$  2-zusammenhängend ist. Für die andere Richtung müssen wir noch zeigen, dass für einen 2-zusammenhängenden Graphen  $G$  auch  $(G\%e) - z$  zusammenhängend ist, wobei  $z$  die neu hinzugefügte Ecke ist. Das folgt aus der Tatsache (die wir in dem vorangegangenen Beweis begründet haben), dass  $G - e$  zusammenhängend ist, wenn  $G$  2-zusammenhängend ist.  $\square$

Die nächste Charakterisierung 2-zusammenhängender Graphen ist besonders brauchbar in Beweisen. Wir zeigen, wie 2-zusammenhängende Graphen aus einfacheren Graphen zusammengesetzt sind.

#### 4.6.5 Satz (Erzeugen 2-zusammenhängender Graphen).

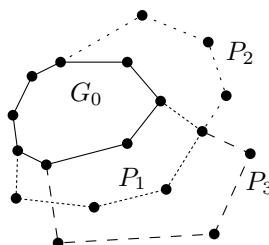
*Ein Graph  $G$  ist genau dann 2-zusammenhängend, wenn er aus einem Dreieck (d.h. aus einem  $K_3$ ) durch wiederholtes Unterteilen von Kanten und Hinzufügen von Kanten erzeugt werden kann.*

So eine Konstruktion kann z.B. so aussehen:



*Beweis.* Jeder Graph, der durch Unterteilen und Hinzufügen von Kanten aus  $K_3$  entsteht, ist offensichtlich 2-zusammenhängend. Es bleibt also zu zeigen, dass wir jeden 2-zusammenhängenden Graphen so aufbauen können.

Was wir tatsächlich zeigen werden, ist, dass wir jeden 2-zusammenhängenden Graphen durch eine ein wenig andere Konstruktion erzeugen können. Wir beginnen mit einem Kreis  $G_0$ , und wenn wir einen Graphen  $G_{i-1}$  schon gebaut haben, dann erzeugen wir einen Graphen  $G_i$ , indem wir einen Weg  $P_i$  hinzufügen, der zwei Ecken des Graphen  $G_{i-1}$  verbindet. Nur die Endencken des Weges  $P_i$  sind Ecken aus  $G_{i-1}$ , während alle Kanten und alle inneren Ecken neu hinzukommen. Wie in der folgenden Zeichnung angedeutet,

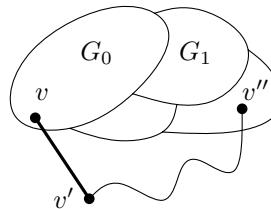


„kleben“ wir sozusagen sukzessive „Öhrchen“ an den Graphen  $G$  an (und so eine Zerlegung eines Graphen heißt wirklich eine *Ohrenzerlegung*, englisch *ear decomposition*).

Weil man das Hinzufügen eines Weges durch das Hinzufügen und Unterteilen von Kanten simulieren kann,<sup>6</sup> genügt es zu zeigen, dass jeder 2-zusammenhängende Graph  $G$  durch wiederholtes Ankleben von Ohren erzeugt werden kann.

Sehen wir uns einen beliebigen Kreis  $G_0$  in  $G$  an. Wir nehmen an, dass Graphen  $G_j = (E_j, V_j)$  für  $j \leq i$  mit den oben beschriebenen Eigenschaften schon definiert sind. Ist  $G_i = G$ , dann sind wir fertig; wir nehmen also weiter an, dass  $E_i \neq E(G)$  ist. Weil  $G$  zusammenhängend ist, gibt es eine Kante  $e \in E(G) \setminus E_i$ , so dass  $e \cap V_i \neq \emptyset$ .

Wenn beide Enden von  $e$  in  $V_i$  liegen, dann setzen wir  $G_{i+1} = G_i + e$ . Andernfalls sei  $e = \{v, v'\}$ , wobei  $v \in V_i$ ,  $v' \notin V_i$ :



Betrachten wir den Graphen  $G - v$ . Er ist zusammenhängend (weil  $G$  2-zusammenhängend ist) und deshalb gibt es einen Weg  $P$ , der die Ecke  $v'$  mit einer Ecke  $v'' \in V_i$  verbindet, wobei  $v''$  die einzige Ecke auf dem Weg  $P$  ist, die zu  $V_i$  gehört (zum Beispiel hat ein kürzester Weg zwischen  $v'$  und  $V_i$  in  $G - v$  diese Eigenschaft). Nun können wir den Graphen  $G_{i+1}$  definieren als  $G_i$ , dem wir die Kante  $e$  und den Weg  $P$  hinzufügen, d.h.  $V_{i+1} = V_i \cup V(P)$ ,  $E_{i+1} = E_i \cup \{e\} \cup E(P)$ .  $\square$

## Aufgaben

1. Beweisen Sie, dass es zu je zwei Kanten eines 2-zusammenhängenden Graphen einen Kreis gibt, der beide enthält.
2. Sei  $G$  ein *kritisch 2-zusammenhängender Graph*; das bedeutet, dass  $G$  2-zusammenhängend ist, aber kein Graph  $G - e$  für  $e \in E(G)$  ist 2-zusammenhängend.
  - (a) Beweisen Sie, dass mindestens eine Ecke von  $G$  Grad 2 hat.

---

<sup>6</sup>Ein bisschen aufpassen muss man hier schon: sind  $v, v' \in V(G_{i-1})$  schon durch eine Kante verbunden, wenn wir einen neuen Weg zwischen ihnen einfügen wollen, dann dürfen wir nicht einfach damit beginnen die Kante  $\{v, v'\}$  hinzuzufügen (zumindest dann nicht, wenn wir keine Mehrfachkanten erlauben). In diesem Fall müssen wir die Kante  $\{v, v'\}$  zuerst unterteilen, dann die Kante  $\{v, v'\}$  neu hinzufügen, und dann eventuell weitere Unterteilungen vornehmen.

- (b) Finden Sie für jedes  $n$  ein Beispiel eines kritisch 2-zusammenhängenden Graphen mit einer Ecke vom Grad mindestens  $n$ .
- (c) \*Geben Sie für jedes  $n$  ein Beispiel eines kritisch 2-zusammenhängenden Graphen mit einer Ecke vom Grad  $\geq n$ , die von allen Ecken vom Grad 2 mindestens den Abstand  $n$  hat.
3. (a) Ist es wahr, dass jeder kritisch 2-zusammenhängende Graph (siehe Aufgabe 2) aus einem Kreis aufgebaut werden kann, indem man nach und nach „Ohren“ (Wege der Länge mindestens 2) anklebt?
- (b) Ist es wahr, dass jeder kritisch 2-zusammenhängende Graph durch Ankleben von Ohren aus einem Kreis aufgebaut werden kann, und zwar so, dass jeder im Laufe der Konstruktion entstehenden Graphen auch kritisch 2-zusammenhängend ist?
4. Beweisen Sie, dass jeder 2-zusammenhängende Graph eine stark zusammenhängende Orientierung (siehe Abschnitt 4.5) besitzt.
5. \*Bestimmen Sie die (Ecken-) Zusammenhangszahl des  $k$ -dimensionalen Würfels. Der  $k$ -dimensionale Würfel wurde am Ende von Abschnitt 4.5 definiert.
6. \*Sei  $d \geq 3$  eine ganze Zahl und  $G$  ein  $d$ -regulärer (jede Ecke hat Grad  $d$ ),  $d$ -kantenzusammenhängender Graph. Beweisen Sie, dass solch ein  $G$  *tough*<sup>7</sup> ist, was bedeutet, dass das Entfernen von  $k$  Ecken aus  $G$  höchstens  $k$  Komponenten erzeugt (für alle  $k \geq 1$ ).
7. (Satz von Mader) \*\*Sei  $G$  ein Graph auf  $n$  Ecken, so dass  $|E(G)| \geq (2k-3)(n-k+1)+1$ , wobei  $k$  eine natürliche Zahl mit  $2k-1 \leq n$  ist. Beweisen Sie mit Induktion nach  $n$ , dass  $G$  einen  $k$ -fach eckenzusammenhängenden Teilgraphen hat.

## 4.7 Dreiecksfreie Graphen: ein Extremalproblem

Wir betrachten einen Graphen  $G$  auf  $n$  Ecken. Was wissen wir über die Kantenzahl? Das ist einfach, wir kennen die Antwort: Jede ganze Zahl zwischen 0 und  $\binom{n}{2}$  ist möglich. Die maximal („extremal“) mögliche Zahl der Kanten in einem Graph auf  $n$  Ecken ist  $\binom{n}{2}$ , und jeder Graph mit dieser Kantenzahl ist isomorph zum vollständigen Graphen  $K_n$ .

In diesem Abschnitt wollen wir ein anspruchsvollereres, „echtes“ Extremalproblem angehen. Wie viele Kanten kann ein Graph auf  $n$  Ecken haben, wenn wir wissen, dass er kein Dreieck (also keinen zu  $K_3$  isomorphen Untergraphen) enthält? Wieder interessiert uns die

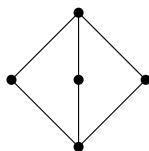
---

<sup>7</sup>Tough (sprich: taff) heißt auf Englisch zäh, hart.

*maximal* mögliche Kantenzahl eines solchen Graphen, die wir mit  $T(n)$  bezeichnen.

Die Werte  $T(1) = 0$ ,  $T(2) = 1$  und  $T(3) = 2$  sind klar. Man sieht auch leicht ein, dass  $T(4) = 4$  ist: die Ungleichung  $T(4) \geq 4$  demonstriert der Kreis  $C_4$  der Länge 4, und die Ungleichung  $T(4) < 5$  folgt zum Beispiel daraus, dass ein Graph mit 4 Ecken und 5 Kanten bis auf Isomorphie eindeutig bestimmt ist und ein Dreieck enthält.

Doch was ist  $T(5)$ ? Der Kreis  $C_5$  der Länge 5 zeigt, dass  $T(5) \geq 5$  ist. Dieser Graph mag auch bestmöglich scheinen, denn durch Hinzufügen einer weiteren Kante entsteht zwangsläufig ein Dreieck. Doch der Schein trügt: tatsächlich ist  $T(5) \geq 6$ , wie der folgende Graph zeigt:



Wir werden sehen, dass *dieser* Graph wirklich maximal viele Kanten enthält. Im nun folgenden Satz zeigen wir nicht nur  $T(5) = 6$ , sondern bestimmen  $T(n)$  für alle  $n$  exakt.

**4.7.1 Satz.** Für jede natürliche Zahl  $n$  ist  $T(n) = \lfloor \frac{n^2}{4} \rfloor$ .

Zur Erinnerung:  $\lfloor x \rfloor$  bezeichnet die größte ganze Zahl, die kleiner oder gleich der reelle Zahl  $x$  ist („Abrunden“).

**Beweis.** Zunächst zeigen wir die (deutlich einfachere) Ungleichung  $T(n) \geq \lfloor \frac{n^2}{4} \rfloor$ . Dafür genügt es, geeignete dreiecksfreie Graphen anzugeben. Wir machen die folgende Definition etwas allgemeiner als nötig, das wird sich später auszahlen. Zu disjunkten Mengen  $X$  und  $Y$  bezeichne  $K_{X,Y}$  den Graphen mit Eckenmenge  $X \cup Y$  und Kantenmenge  $\{\{x,y\} : x \in X, y \in Y\}$ . Der Graph  $K_{X,Y}$  heißt vollständiger bipartiter Graph, und wenn  $a = |X|$  und  $b = |Y|$ , dann ist  $K_{X,Y}$  isomorph zu  $K_{a,b}$  wie in Abschnitt 4.1 definiert. Ein bipartiter Graph enthält keine Dreiecke, und der Graph  $K_{a,b}$  hat  $ab$  Kanten. Schauen Sie sich nochmal den Graphen an, mit dem wir  $T(5) \geq 6$  gezeigt haben — er ist isomorph zu  $K_{2,3}$ .

Für unseren Beweis müssen wir nun noch Werte  $a, b$  angeben, so dass  $a + b = n$  und  $a \cdot b = \lfloor \frac{n^2}{4} \rfloor$ ; wir versuchen es mit der möglichst gleichmäßigen Aufteilung  $a = \lfloor \frac{n}{2} \rfloor$  und  $b = n - a$ . Wir unterscheiden zwei Fälle,  $n$  gerade oder  $n$  ungerade. Zuerst sei  $n$  ungerade, d.h.

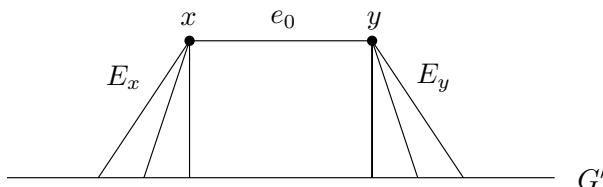
$n = 2k + 1$ . In diesem Fall ist  $a = k$ ,  $b = k + 1$  und  $ab = k^2 + k$ . Andererseits ist  $\lfloor \frac{n^2}{4} \rfloor = \lfloor \frac{(2k+1)^2}{4} \rfloor = \lfloor k^2 + k + \frac{1}{4} \rfloor = k^2 + k = ab$ . Der zweite Fall, dass  $n$  gerade ist, ist eine Spur einfacher und daher dem Leser überlassen. Damit haben wir gezeigt:  $T(n) \geq \lfloor \frac{n^2}{4} \rfloor$ .

Nun zeigen wir die schwierigere Ungleichung  $T(n) \leq \lfloor \frac{n^2}{4} \rfloor$ . Weil  $T(n)$  eine ganze Zahl ist, brauchen wir nur  $T(n) \leq \frac{n^2}{4}$  zu zeigen. Wir führen eine etwas ungewöhnliche Induktion über  $n$ . Wie wir bereits wissen, gilt die Aussage für  $n \leq 4$ . Im Induktionsschritt beweisen wir die folgende Implikation:

$$T(n) \leq \frac{n^2}{4} \quad \Rightarrow \quad T(n+2) \leq \frac{(n+2)^2}{4}.$$

Es sei also  $G = (V, E)$  ein dreiecksfreier Graph mit  $n+2$  Ecken. Unser Ziel ist,  $|E| \leq \frac{(n+2)^2}{4}$  zu zeigen. Wir wählen eine beliebige Kante  $e_0 = \{x, y\} \in E$ , setzen  $V' = V \setminus \{x, y\}$  und bezeichnen den von  $V'$  induzierten Teilgraphen von  $G$  mit  $G' = (V', E')$ . Der Graph  $G'$  ist dreiecksfrei, folglich haben wir nach Induktionsvoraussetzung  $|E'| \leq \frac{n^2}{4}$ .

$E_x$  sei die Menge der Kanten von  $G$ , die mit der Ecke  $x$  inzident sind,  $E_x = \{e \in E : x \in e \in E, e \neq e_0\}$ . Analog definieren wir die Menge  $E_y$ . Damit haben wir  $E = E' \cup (E_x \cup E_y) \cup \{e_0\}$  und  $|E| = |E'| + |E_x \cup E_y| + 1$ . Eine entscheidende Erkenntnis ist nun, dass eine Kante aus  $E_x$  keine gemeinsame Ecke mit einer Kante aus  $E_y$  haben kann, und dass deshalb  $|E_x \cup E_y| \leq n$  ist.



Zusammenfassend haben wir gezeigt, dass  $|E| \leq \frac{n^2}{4} + n + 1 = \frac{(n+2)^2}{4}$ .  $\square$

Wir können sogar noch mehr aus dem obigen Beweis herausholen. Wir führen folgende Schreibweise ein: Wir nennen einen Graphen  $G = (V, E)$  auf  $n$  Ecken *extremal*, wenn er kein Dreieck enthält und  $\lfloor \frac{n^2}{4} \rfloor$  Kanten hat. Wir wissen bereits, dass  $K_{\lfloor n/2 \rfloor, n - \lfloor n/2 \rfloor}$  extremal ist.

**4.7.2 Satz.** Für jede Eckenzahl  $n$  ist jeder extremale Graph stets isomorph zu  $K_{a,b}$  mit  $a = \lfloor \frac{n}{2} \rfloor$ ,  $b = n - \lfloor \frac{n}{2} \rfloor$ .

Der vollständige bipartite Graph mit möglichst gleich großen Klassen ist also jeweils der einzige extreme Graph. Diese bemerkenswerte Tatsache war wesentliche Inspirationsquelle einer ganzen Theorie: Der *extremalen Graphentheorie*. Weiteren Beispielen werden wir in Abschnitt 7.3 begegnen. Auch den Satz von Sperner (siehe Abschnitt 7.2) kann man als ein Ergebnis der extremalen Graphentheorie ansehen.

**Beweis von Satz 4.7.2.** Weil wir genauso wie im Beweis von Satz 4.7.1 vorgehen, legen wir unser Augenmerk hauptsächlich auf diejenigen Argumente, aus denen die Eindeutigkeit des extremalen Graphen folgt. Wieder stimmt die Aussage für  $n = 1, 2, 3$ , wir können mühelos alle extremalen Graphen betrachten. Im Induktionsschritt berufen wir uns auf die Eindeutigkeit des extremalen Graphen auf  $n$  Ecken, unser Ziel ist, die Eindeutigkeit für  $n + 2$  Ecken zu zeigen.

Sei also  $G = (V, E)$  ein dreiecksfreier Graph auf  $n + 2$  Ecken und mit  $\lfloor \frac{(n+2)^2}{4} \rfloor$  Kanten. Wir wählen eine beliebige Kante  $e_0 = \{x, y\}$  und betrachten den Graphen  $G' = (V', E')$  mit  $V' = V \setminus \{x, y\}$  und  $E' = E \cap \binom{V'}{2}$ . Weil  $|E| = \lfloor \frac{n^2}{4} \rfloor + n + 1$  und weil  $|E'| \leq \lfloor \frac{n^2}{4} \rfloor$  und  $|E_x \cup E_y| \leq n$  (siehe den Beweis von Satz 4.7.1), folgt, dass  $|E'| = \lfloor \frac{n^2}{4} \rfloor$  sein muss. Daher ist  $G'$  extremal und folglich isomorph zu  $K_{a,b}$ , wobei  $a = \lfloor \frac{n}{2} \rfloor$  und  $b = n - a$ . Also ist  $G' = K_{X,Y}$  für eine geeignete Partition von  $V'$  in zwei Mengen  $X$  und  $Y$ ,  $|X| = a$ ,  $|Y| = b$ . Wir bemerken, dass  $x$  nur mit  $X$  oder  $Y$  verbunden sein kann, nicht mit beiden, und entsprechend  $y$ . Doch weil  $|E_x| + |E_y| = n$ , muss eine der folgenden zwei Möglichkeiten zutreffen: Entweder ist  $x$  mit allen Ecken aus  $X$  verbunden und  $y$  mit allen Ecken aus  $Y$ , oder  $x$  ist mit allen  $Y$ -Ecken verbunden und  $y$  mit allen  $X$ -Ecken. Eine kurze Überlegung zeigt, dass diese beiden Möglichkeiten isomorphe Graphen ergeben.  $\square$

Wir beschließen diesen Abschnitt mit der Skizze eines weiteren Beweises von Satz 4.7.1. Eigentlich beweisen wir einen geringfügig anderen Satz:

**4.7.3 Satz.** Sei  $G = (V, E)$  ein dreiecksfreier Graph. Dann gibt es eine Partition von  $V$  in zwei Klassen  $X$  und  $Y$ , so dass für jede Ecke  $x \in V$  gilt:  $d_G(x) \leq d_{K_{X,Y}}(x)$ .

Zunächst zeigen wir, wie Satz 4.7.1 aus Satz 4.7.3 folgt: Aus der Ungleichung in Satz 4.7.3 folgern wir, dass die Kantenzahl von  $G$  nicht größer sein kann als die Kantenzahl von  $K_{X,Y}$  (denn die Kantenzahl ist die doppelte Gradsumme), und somit genügt es zu zeigen, dass ein Graph  $K_{a,b}$  mit  $a+b = n$  höchstens  $\lfloor \frac{n^2}{4} \rfloor$  Kanten hat (siehe Aufgabe 1).

**Beweis von Satz 4.7.3.** Sei  $G = (V, E)$  ein dreiecksfreier Graph. Wir suchen uns eine Ecke  $x_0 \in V$  mit maximalem Grad in  $G$ . Wir setzen  $Y = \{y: \{x_0, y\} \in E\}$  und  $X = V \setminus Y$ . Es ist  $x_0 \in X$ , und für jedes  $x \in X$  haben wir  $d_{K_{X,Y}}(x) = |Y| = d_G(x_0) \geq d_G(x)$ , womit die behauptete Ungleichung für alle  $x \in X$  gezeigt ist. Als nächstes bemerken wir, dass keine zwei Ecken aus  $Y$  adjazent sind, weil alle Ecken in  $Y$  mit  $x_0$  benachbart sind,  $G$  aber kein Dreieck enthält. Deshalb liegen alle Nachbarn eines jeden  $y \in Y$  in  $X$ , und wir haben  $d_G(y) \leq |X| \leq d_{K_{X,Y}}(y)$ .  $\square$

## Aufgaben

- Bestimmen Sie natürliche Zahlen  $a$  und  $b$  mit  $a + b = n$ , für die der Ausdruck  $a \cdot b$  maximal wird.
- Bestimmen Sie zu gegebenen natürlichen Zahlen  $k$  und  $n$  alle Werte natürlicher Zahlen  $a_1, \dots, a_k$ , für die  $\sum_{i=1}^k a_i = n$  ist und das Produkt  $a_1 \cdot a_2 \cdot \dots \cdot a_k$  maximal wird.
- Ein vollständiger  $k$ -partiter Graph  $K(V_1, V_2, \dots, V_k)$  auf der Eckenmenge  $V$  ist durch eine Partition  $V_1, \dots, V_k$  der Eckenmenge  $V$  gegeben, seine Kanten sind alle Eckenpaare  $\{x, y\}$ , wo  $x$  und  $y$  in verschiedenen Klassen der Partition liegen. Formal:  $K(V_1, \dots, V_k) = (V, E)$ , wobei genau dann  $\{x, y\} \in E$ , wenn  $x \neq y$  und  $|\{x, y\} \cap V_i| \leq 1$  für alle  $i = 1, \dots, k$ . Beweisen Sie (unter Verwendung von Aufgabe 2), dass die maximale Kantenzahl eines vollständigen  $k$ -partiten Graphen auf einer gegebenen Eckenmenge bei möglichst gleich großen Klassen erreicht wird, d.h. wenn  $\left| |V_i| - |V_j| \right| \leq 1$  für alle  $i, j$ . Wie viele Kanten hat so ein Graph  $K(V_1, \dots, V_k)$ ?
- \*Beweisen Sie, dass für jedes  $k \geq 1$  und für jeden Graph  $G = (V, E)$ , der keinen  $K_{k+1}$  als Teilgraph enthält, eine Partition  $V_1, \dots, V_k$  von  $V$  existiert, so dass keine Ecke  $x$  einen größeren Eckengrad in  $G$  hat als in  $K(V_1, \dots, V_k)$  (dies ist ein Analogon zu Satz 4.7.3). Auf diese Art lässt sich Satz 4.7.1 verallgemeinern, wobei man statt des Dreiecks  $K_3$  den vollständigen Graphen  $K_k$  für beliebiges (aber festes)  $k$  betrachtet. Das ist der berühmte Satz von Turán.



# 5

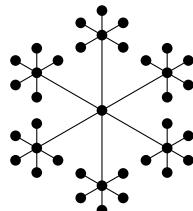
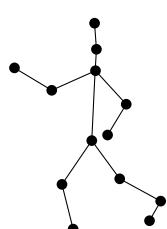
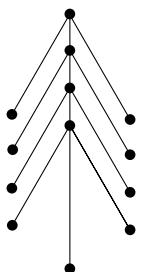
# Bäume

---

## 5.1 Definition und Charakterisierungen

Wie jedes andere Fach hat auch die Mathematik ihre eigene Sprache entwickelt. Dabei haben auch sehr abstrakte und schwer fassbare Konzepte Namen erhalten, die in der normalen Sprache schon vergeben sind (wenn Sie bis hier gelesen haben, dann ist Ihnen das natürlich schon aufgefallen). Eine geschickte Wahl des Namens für ein neues Konzept kann durchaus von Bedeutung sein. Ein guter Name kann auf einer intuitiven Ebene helfen, wesentliche Eigenschaften eines Objekts zu vermitteln, die der formalen Definition nicht ohne weiteres anzusehen sind. Und ein unpassender Name kann einen sehr verwirren. Es gibt Namen, die heutzutage etwas unlogisch klingen, wenn man ihre zuweilen verwinkelte Geschichte nicht kennt. Zum Beispiel sind „Ringe“ in der Mathematik weder rund noch aus Gold, und man wundert sich schon, wenn ein Ding in der Ebene „Ecke“ heißt (Sie werden sich nicht mehr wundern, wenn Sie Kapitel 6 gelesen haben). In diesem Kapitel stellen wir Ihnen ein einfaches und ganz fundamentales graphentheoretisches Konzept vor, den Baum, und Sie können Sich ein Bild davon machen, was für ein passender Name den Mathematikern damit eingefallen ist.

In der Graphentheorie ist ein Baum ein Graph ähnlich denen in den folgenden Zeichnungen:



Diese Bilder sollen ein Gefühl dafür vermitteln, was ein Baum in der Graphentheorie ist. Aber wir brauchen natürlich eine exakte Definition. Wie könnte sie aussehen? Bitte versuchen Sie jetzt, bevor Sie weiterlesen, eine Definition zu formulieren.

Die gebräuchlichste Definition ist vielleicht die folgende:

**5.1.1 Definition.** Ein Baum ist ein zusammenhängender Graph, der keinen Kreis enthält.

Haben Sie „Baum“ anders definiert? Dann gibt es mindestens zwei Möglichkeiten: Vielleicht waren die Bilder oben doch nicht so intuitiv, vielleicht haben Sie aber auch eine der vielen äquivalenten Definitionen gefunden. Bald werden wir vier weitere Möglichkeiten vorstellen.

Dann werden wir fünf verschiedene potenzielle Definitionen für das gleiche Objekt haben. Wozu soll das gut sein? Zuerst einmal ist die gerade eben gegebene Definition in mehrerlei Hinsicht nicht besonders geeignet. Es ist z.B. nicht klar, wie man testen kann, ob ein Graph ein Baum ist oder nicht. Zum Testen des Zusammenhangs gibt es einen einfachen Algorithmus, aber die Nichtexistenz eines Kreises nachzuweisen scheint problematisch. Die alternativen Beschreibungen, zu denen wir gleich kommen werden, lassen sich z.T. direkt in Algorithmen zur Erkennung von Bäumen umsetzen. Fünf äquivalente Definitionen, das bedeutet auch: Wir dürfen uns eine der Definitionen aussuchen, die anderen vier sind dann äquivalente Charakterisierungen und geben interessante Eigenschaften von Bäumen, die in Anwendungen vielleicht nützlich sind.

Zweitens ist der Beweis, dass die verschiedenen Definitionen äquivalent sind, nach unserer Erfahrung sehr gut geeignet, das selbstständige Formulieren eigener Beweise zu üben. Die diversen Implikationen in dem Beweis sind nicht unglaublich schwierig, aber auch nicht ganz einfach. Bei dem Versuch einer dieser Implikationen zu beweisen hat man jede Menge Möglichkeiten, Fehler zu machen und zu entdecken, Lücken zu finden und zu schließen. Der Beweis, den wir am Ende dieses Abschnitts geben, soll auch zeigen, wie man vorgehen kann, wenn man die Äquivalenz gleich mehrerer Aussagen zeigen will.

Drittens sind die äquivalenten Charakterisierungen von Bäumen einfach und zeigen zugleich Beispiele „guter“ Charakterisierungen eines mathematischen Objekts; wichtige (und schwierige) Sätze in verschiedenen Gebieten haben formal eine ähnliche Struktur.

Es folgen die angekündigten äquivalenten Definitionen für Bäume. Die erstaunlichste ist vielleicht die Version, dass man unter den zusammenhängenden Graphen einen Baum einfach durch Zählen der Ecken und Kanten erkennt.

**5.1.2 Satz (Charakterisierungen für Bäume).** Die folgenden Bedingungen sind alle äquivalent für einen Graph  $G = (V, E)$ :

(i)  $G$  ist ein Baum.

(ii) (eindeutige Wege)

Zu je zwei Ecken  $x, y \in V$  gibt es genau einen Weg von  $x$  nach  $y$ .

(iii) (minimal zusammenhängender Graph)

Der Graph  $G$  ist zusammenhängend, und wenn man eine Kante  $e \in E$  entfernt (egal welche), dann ist der resultierende Graph  $G - e$  nicht mehr zusammenhängend.

(iv) (maximal kreisfreier Graph)

Der Graph  $G$  enthält keinen Kreis, und wenn man eine Kante  $e \in \binom{V}{2} \setminus E$  hinzufügt, dann enthält der resultierende Graph  $G + e$  einen Kreis.

(v) (Euler-Formel)

$G$  ist zusammenhängend und  $|V| = |E| + 1$ .

Dieser Satz beschreibt nicht nur verschiedene Eigenschaften von Bäumen, wie etwa „jeder Baum auf  $n$  Ecken hat  $n - 1$  Kanten“, sondern er zählt Eigenschaften auf, die zu Definition 5.1.1 äquivalent sind; er sagt z.B. „ein Graph auf  $n$  Ecken ist genau dann ein Baum, wenn er zusammenhängend ist und  $n - 1$  Kanten hat“.

Die große Schwierigkeit beim Beweis der Äquivalenzen in Satz 5.1.2 liegt für Anfänger darin, dass man leicht dazu neigt, unbewiesene Aussagen zu behaupten. Man schaut sich eine Äquivalenz intensiv an — und hält sie dann für klar; oder man begründet sie mit etwas, das man für klar hält, andere (z.B. der Professor) aber nicht. (Dieses Problem hat man überhaupt in der Graphentheorie.) Deshalb gibt es alle möglichen Lücken in solchen Beweisen. Schauen wir uns ein (hypothetisches) Beispiel an.

Die folgende Implikation soll bewiesen werden: „Ist  $G$  ein Baum, dann gibt es zwischen je zwei Ecken in  $G$  genau einen Weg.“ Die meisten Menschen bemerken schnell, dass es zwischen je zwei Ecken in  $G$  mindestens einen Weg gibt. Dann könnte sich zwischen einem Schüler und seiner Lehrerin, die gemeinsam den Beweis erarbeiten, etwa der folgende Dialog entwickeln:

S.: „Wir führen einen Widerspruchsbeweis. Wenn  $u$  und  $v$  zwei Ecken in  $G$  sind, zwischen denen es zwei verschiedene Wege gibt, dann enthält  $G$  einen Kreis. Also stimmt die Behauptung.“

L.: „Aber warum muss es einen Kreis geben in  $G$ , wenn zwischen  $u$  und  $v$  zwei verschiedene Wege verlaufen?“

S.: „Naja, weil die zwei Wege zusammen einen Kreis enthalten.“

Für die Lehrerin ist das keine einfache Situation: Die Behauptung ist richtig und der „Beweis durch ein Bild“ ist ganz einfach; doch es fehlt der Beweis.

L: „Aber warum? Wir brauchen doch einen Beweis! In dem Bild, ja, da ist tatsächlich ein Kreis, und ich kenne auch keinen Graph, der keinen Kreis enthält und doch zwei verschiedene Wege zwischen  $u$  und  $v$ . Aber ist es nicht denkbar, dass es irgendwo Außerirdische gibt, viel intelligenter als du und ich und alle anderen Menschen zusammen, die so einen Graphen konstruieren können?“

(Über Vorschläge für didaktischere, überzeugendere Argumente würden wir uns freuen.) Einen hieb- und stichfesten Beweis zu führen ist tatsächlich nicht völlig trivial, aber das Hauptproblem ist, zu vermitteln, *dass* wirklich etwas zu beweisen *ist*. Sie werden sehen, dass wir in unserem Beweis von Satz 5.1.2 weiter unten dieses direkte Argument lieber vermeiden.

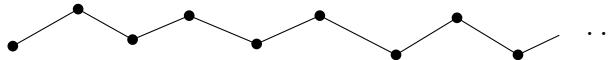
Wir gehen nun an den Beweis von Satz 5.1.2. Gerade bei einem Satz wie diesem, bei dem so viele Aussagen zu beweisen sind, ist es wichtig den Beweis gut zu organisieren. Wir führen Induktion über die Eckenzahl, „pflücken“ im Induktionsschritt eine Ecke vom Grad 1 ab und können dann die Induktionsvoraussetzung anwenden. Den Grundstein dafür legen wir in den zwei nun folgenden Lemmas.

Wir nennen eine Ecke vom Grad 1 in einem Graphen  $G$  ein *Blatt* von  $G$ . Unser Ausgangspunkt ist die folgende fast offensichtliche Beobachtung:

**5.1.3 Lemma (Blatt–Lemma).** *Jeder Baum mit mindestens zwei Ecken enthält mindestens zwei Blätter.*

*Beweis.* Sei  $P = (v_0, e_1, v_1, \dots, e_t, v_t)$  ein längstmöglicher Weg in einem Baum  $T = (V, E)$ . Die Länge dieses Weges  $P$  ist mindestens 1, anders gesagt ist  $v_0 \neq v_t$ . Wir behaupten, dass sowohl  $v_0$  als auch  $v_t$  Blätter sind. Um das zu beweisen führen wir die gegenteilige Annahme zum Widerspruch. Wenn  $v_0$  kein Blatt ist (für  $v_t$  alles analog), dann gibt es eine Kante  $e = \{v_0, v\}$ , welche die Ecke  $v_0$  enthält und nicht die erste Kante  $e_1 = \{v_0, v_1\}$  aus dem Weg  $P$  ist. Entweder ist  $v$  eine der Ecken  $v = v_i$  ( $i \geq 2$ ) auf dem Weg  $P$  (in diesem Fall bildet die Kante  $e$  gemeinsam mit dem Abschnitt  $v_0, e_1, v_1, \dots, e_i, v_i$  von  $P$  einen Kreis), oder  $v \notin \{v_0, \dots, v_t\}$  (in diesem Fall können wir  $P$  um die Kante  $e$  verlängern). In beiden Fällen erhalten wir einen Widerspruch.  $\square$

Wir sollten erwähnen, dass das Blatt-Lemma nicht für unendliche Bäume gilt. Der Beweis scheitert daran, dass es in unendlichen Bäumen nicht unbedingt einen Weg maximaler Länge gibt. Der „einseitig unendliche Weg“ hat zum Beispiel nur ein Blatt



und der „zweiseitig unendliche Weg“ hat gar keines:



Wir werden aber nur endliche Graphen betrachten.

Wir erinnern noch einmal an eine Notation aus Abschnitt 4.6: Wenn  $G = (V, E)$  ein Graph ist und  $v$  eine Ecke von  $G$ , dann steht  $G - v$  für den Graphen, der entsteht, wenn man aus  $G$  die Ecke  $v$  entfernt und mit ihr alle inzidenten Kanten. In dem Fall, dass  $v$  ein Blatt in einem Baum  $T$  ist, entsteht  $T - v$  durch Entfernen der Ecke  $v$  und der einen Kante, die  $v$  enthält.

**5.1.4 Lemma.** Sei  $G$  ein Graph und  $v$  ein Blatt in  $G$ . Dann sind die folgenden zwei Aussagen äquivalent:

- (i)  $G$  ist ein Baum
- (ii)  $G - v$  ist ein Baum.

*Beweis.* Zuerst beweisen wir die Implikation  $(i) \Rightarrow (ii)$ . Der Graph  $G$  sei also ein Baum, dann möchten wir zeigen, dass  $G - v$  auch ein Baum ist. Wir betrachten zwei Ecken  $x, y$  in  $G - v$ . Weil  $G$  zusammenhängend ist, gibt es in  $G$  einen Weg zwischen  $x$  und  $y$ . Dieser Weg kann außer  $x$  und  $y$  keine Ecke vom Grad 1 enthalten, also insbesondere nicht  $v$ . Deshalb liegt er vollständig in  $G - v$ , und wir schließen, dass  $G - v$  zusammenhängend ist. Weil  $G$  keinen Kreis enthält, kann offensichtlich auch  $G - v$  keinen Kreis enthalten und ist somit ein Baum.

Nun ist noch die Richtung  $(ii) \Rightarrow (i)$  zu zeigen. Sei  $G - v$  ein Baum. Wenn wir das Blatt  $v$  wieder anhängen, kann kein Kreis entstehen. Außerdem müssen wir den Zusammenhang von  $G$  nachweisen, aber der ist auch offensichtlich: alle Ecken außer  $v$  sind schon in  $G - v$  in der gleichen Komponente, und in  $G$  erreicht man von  $v$  aus jede andere Ecke  $x$ , indem man zuerst von  $v$  zu dem einzigen Nachbarn  $v'$  geht und dann von  $v'$  nach  $x$  den Weg nimmt, der diese beiden Ecken schon in  $G - v$  verbindet.  $\square$

Dieses Lemma gestattet uns, einen Baum durch wiederholtes Abpflücken von Blättern kleiner und kleiner zu machen. Dieses Hilfsmittel können wir gleich sehr gut gebrauchen.

*Beweis von Satz 5.1.2.* Wir beweisen, dass jede der Aussagen (ii)–(v) zu (i) äquivalent ist. Damit ist dann die Äquivalenz all dieser Aussagen gezeigt.<sup>1</sup> Die Beweise gehen mit Induktion über die Anzahl der Ecken von  $G$ , wobei wir Lemma 5.1.4 ausnutzen. Für den Induktionsanfang stellen wir fest, dass die Aussagen alle für den Graph mit nur einer einzigen Ecke gelten.

Zuerst zeigen wir, dass aus (i) alle Aussagen (ii)–(v) folgen. Dazu sei  $G$  ein Baum mit mindestens zwei Ecken,  $v$  sei eines seiner Blätter und  $v'$  sei der eindeutige Nachbar von  $v$  in  $G$ . Als Induktionsvoraussetzung dürfen wir annehmen, dass für den Graphen  $G - v$  (ii)–(v) gelten.

Die Gültigkeit der Aussagen (ii), (iii) und (v) für  $G$  folgt nun sehr leicht. Wir sind versucht zu schreiben, es sei offensichtlich; doch es ist wohl besser, wenn wir Sie bitten, die Details selbst auszuarbeiten.

Um die Gültigkeit von (iv) zu zeigen brauchen wir nicht einmal die Induktionsvoraussetzung für  $G - v$ . Weil  $G$  zusammenhängend ist, können je zwei Ecken  $x, y \in V(G)$  durch einen Weg miteinander verbunden werden, und wenn  $\{x, y\} \notin E(G)$ , dann bildet dieser Weg zusammen mit der Kante  $\{x, y\}$  einen Kreis. Das beweist (i)  $\Rightarrow$  (iv).

Nun werden wir beweisen, dass aus jeder der Bedingungen (ii)–(v) folgt, dass  $G$  ein Baum ist. In (ii) und (iii) nehmen wir schon an, dass  $G$  zusammenhängend ist. Außerdem kann ein Graph, der (ii) oder (iii) erfüllt, keinen Kreis enthalten. Für (ii) ist das so, weil zwei Ecken, die auf einem Kreis liegen, durch zwei verschiedene Wege miteinander verbunden werden können, und für (iii), weil das Weglassen einer Kante in einem Kreis den Graphen zusammenhängend lässt. Also haben wir schon die Äquivalenz von (i)–(iii) gezeigt.

Um die Implikation (iv)  $\Rightarrow$  (i) zu beweisen, genügt der Nachweis, dass  $G$  zusammenhängend ist. Dazu können wir das Argument aus dem Beweis von (i)  $\Rightarrow$  (iv) einfach umdrehen. Wenn zwei Ecken  $x, y \in V(G)$  nicht direkt durch eine Kante verbunden sind, dann enthält der Graph  $G + \{x, y\}$  einen Kreis, und dieser Kreis ohne die Kante  $\{x, y\}$  ist ein Weg von  $x$  nach  $y$  in  $G$ .

Schließlich beweisen wir noch die Implikation (v)  $\Rightarrow$  (i) durch Induktion über die Eckenzahl. Betrachten wir also einen zusammen-

---

<sup>1</sup>Das ist so, weil „Äquivalenz“ eine Äquivalenzrelation ist.

hängenden Graphen  $G$  mit  $|V| = |E| + 1 \geq 2$ . Die Summe aller Eckengrade ist dann  $2|V| - 2$  (warum?). Das bedeutet, dass nicht alle Ecken Grad 2 oder größer haben können, und weil alle Grade mindestens 1 sind (wegen des Zusammenhangs!), gibt es eine Ecke  $v$  vom Grad genau 1, also ein Blatt in  $G$ . Der Graph  $G' = G - v$  ist auch zusammenhängend und erfüllt  $|V(G')| = |E(G')| + 1$ , ist also nach Induktionsvoraussetzung ein Baum. Deshalb ist auch  $G$  ein Baum.  $\square$

## Aufgaben

1. Zeichnen Sie alle Bäume auf der Eckenmenge  $\{1, 2, 3, 4\}$  sowie alle paarweise nicht isomorphen Bäume auf 6 Ecken (d.h. aus jeder Äquivalenzklasse einen Vertreter).
2. Beweisen Sie, dass jeder kreisfreie Graph  $G = (V, E)$ , der die Gleichung  $|V| = |E| + 1$  erfüllt, ein Baum ist.
3. \*Sei  $n \geq 3$ . Beweisen Sie, dass ein Graph  $G$  auf  $n$  Ecken genau dann ein Baum ist, wenn er nicht isomorph zum  $K_n$  ist und das Hinzufügen einer beliebigen (noch nicht vorhandenen) Kante zwischen zwei der  $n$  Ecken genau einen Kreis erzeugt.
4. Beweisen Sie, dass ein Graph auf  $n$  Ecken mit  $c$  Komponenten mindestens  $n - c$  Kanten hat.
5. Zeigen Sie: Ein Baum, der eine Ecke vom Grad  $k$  enthält, hat mindestens  $k$  Blätter.
6. Sei  $T$  ein Baum mit  $n$  Ecken,  $n \geq 2$ . Für jede positive ganze Zahl  $i$  bezeichne  $p_i$  die Anzahl der Ecken vom Grad  $i$  in  $T$ . Beweisen Sie, dass

$$p_1 - p_3 - 2p_4 - \cdots - (n - 3)p_{n-1} = 2.$$

(Das ergibt einen alternativen Beweis des Blatt-Lemmas 5.1.3.)

7. König Uxamhwiashurh hatte vier Söhne, zehn seiner männlichen Nachkommen hatten je drei Söhne, 15 hatten zwei Söhne und alle anderen starben kinderlos. Wie viele männliche Nachkommen hatte König Uxamhwiashurh?
8. Betrachten Sie einmal die folgenden zwei Bedingungen an eine Folge  $(d_1, d_2, \dots, d_n)$  positiver ganzer Zahlen ( $n \geq 1$ ):
  - (i) Es gibt einen Baum mit Gradfolge  $(d_1, d_2, \dots, d_n)$ .
  - (ii)  $\sum_{i=1}^n d_i = 2n - 2$ .
 Ziel ist, die Äquivalenz dieser beiden Bedingungen zu beweisen (dann haben wir eine simple Methode, die Gradfolgen von Bäumen zu erkennen).

(a) Warum folgt (ii) aus (i)?

(b) Was ist faul mit dem folgenden „Beweis“ der Implikation (ii) $\Rightarrow$ (i)? Wir führen Induktion nach  $n$ . Der Induktionsanfang  $n = 1$  ist leicht zu prüfen. Die Implikation gelte also für ein  $n \geq 1$ , wir möchten sie nun für  $n+1$  beweisen. Ist  $D = (d_1, d_2, \dots, d_n)$  eine Folge positiver ganzer Zahlen mit  $\sum_{i=1}^n d_i = 2n - 2$ , dann wissen wir nach Induktionsvoraussetzung, dass es einen Baum  $T$  auf  $n$  Ecken mit  $D$  als Gradfolge gibt. Wir fügen eine weitere Ecke  $v$  zu  $T$  hinzu, verbinden sie durch eine Kante mit einer Ecke von  $T$  und erhalten so einen Baum  $T'$  auf  $n + 1$  Ecken. Sei  $D'$  die Gradfolge von  $T'$ . Wir wissen, dass die Eckenzahl um 1 angestiegen ist und die Summe der Eckengrade um 2 (die neue Ecke hat Grad 1 und der Grad von einer der alten Ecken hat sich um 1 erhöht). Deshalb erfüllt die Folge  $D'$  Bedingung (ii) und ist Gradfolge eines Baumes, nämlich von  $T'$ . Damit ist auch der Induktionsschritt bewiesen.

(c) \*Beweisen Sie (ii) $\Rightarrow$ (i).

9. Wir zeigen Ihnen noch einen Beweis dafür, dass jeder zusammenhängende Graph  $G = (V, E)$  mit  $|V| = |E| + 1$  ein Baum ist (das ist die Implikation (v) $\Rightarrow$ (i) in Satz 5.1.2). Was ist falsch daran?

Weil der Graph nach Voraussetzung zusammenhängend ist, brauchen wir lediglich zu beweisen, dass er keinen Kreis enthält. Wir führen Induktion über die Eckenzahl. Für  $|V| = 1$  besteht der Graph nur aus einer einzelnen Ecke und keiner Kante, und die Behauptung gilt ( $1 = 0 + 1$ ). Wir nehmen also als Induktionsvoraussetzung an, dass die Implikation für jeden Graphen  $G = (V, E)$  auf  $n$  Ecken gilt. Wir wollen sie nun auch für Graphen  $G' = (V', E')$  beweisen, die aus  $G$  durch Hinzufügen einer neuen Ecke entstehen. Damit die Behauptung  $|V'| = |E'| + 1$  auch für  $G'$  gilt, müssen wir auch eine neue Kante hinzufügen, und weil wir annehmen, dass  $G'$  zusammenhängend ist, muss diese neue Kante die neue Ecke mit einer Ecke in  $V$  verbinden. Daher hat die neue Ecke Grad 1 und kann nicht in einem Kreis liegen. Und weil  $G$  keinen Kreis hat (nach Induktionsvoraussetzung) kann auch  $G'$  keinen Kreis enthalten, womit der Induktionsschritt bewiesen ist.

## 5.2 Isomorphismen von Bäumen

Wie schon in Abschnitt 4.1 erwähnt ist kein Algorithmus bekannt, der schnell testet, ob zwei gegebene Graphen isomorph sind oder nicht. Für einige spezielle Graphenklassen gibt es jedoch effiziente Algorithmen. Eine dieser Klassen sind die Bäume. Viele (vielleicht die meisten) algorithmischen Probleme sind für Bäume relativ einfach, auch wenn sie für allgemeine Graphen schwer anzugehen sind.

In diesem Abschnitt führen wir einen schnellen und einfachen Algorithmus vor, der zwei gegebene Bäume  $T$  und  $T'$  auf Isomorphie

testet. Ist ein Baum  $T$  gegeben, dann berechnet der Algorithmus eine Folge von Nullen und Einsen der Länge  $2n$ , die wir als den *Code* des Baums  $T$  bezeichnen. Isomorphe Bäume führen zu identischen Folgen, während nicht isomorphe Bäume verschiedene Folgen erhalten. Auf diese Weise ist der Test auf Isomorphie bei Bäumen auf einen einfachen Vergleich zweier Folgen zurückgeführt.

Als Nächstes legen wir die Terminologie für eine Reihe von Konzepten fest. In der algorithmischen Graphentheorie ist das recht nützlich, weil viele Konzepte aus verschiedenen Anwendungen motiviert sind und die Namensgebung entsprechend uneinheitlich ist.

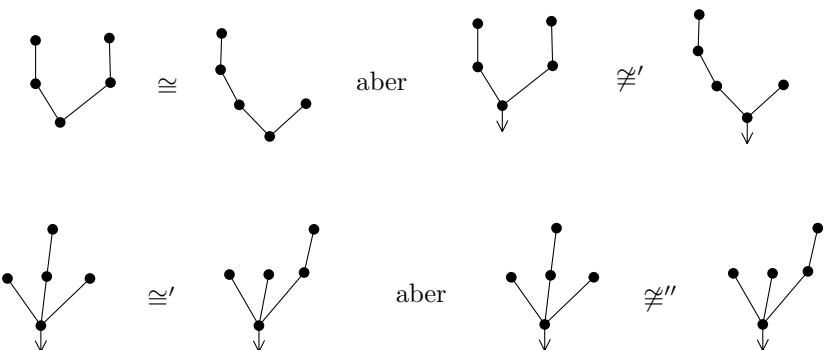
Ein *Wurzelbaum* ist ein Paar  $(T, r)$  aus einem Baum  $T$  und einer vor den anderen ausgezeichneten Ecke  $r \in V(T)$ , der *Wurzel* von  $T$ . Ist  $\{x, y\} \in E(T)$  eine Kante und liegt die Ecke  $x$  auf dem eindeutigen Weg von  $y$  zur Wurzel, dann nennen wir  $x$  den *Vater* von  $y$  (in dem betrachteten Wurzelbaum) und  $y$  einen *Sohn* von  $x$ .

Ein *gepflanzter Baum* ist ein Wurzelbaum  $(T, r)$  zusammen mit einer Zeichnung eben dieses Baums in die Ebene. In dieser Zeichnung ist die Wurzel durch einen nach unten gerichteten Pfeil gekennzeichnet und die Söhne einer Ecke liegen alle über ihrem Vater.

Vielleicht bevorzugen Sie die folgende Variante. Eine ebene Zeichnung eines Baumes wird, abgesehen von stetigen Verformungen der Ebene, vollständig beschrieben durch die Ordnung (von links nach rechts) der Söhne aller Ecken. Ein gepflanzter Baum ist also ein Wurzelbaum, in dem jeder Ecke  $v$  eine lineare Ordnung ihrer Söhne zugewiesen wurde. Formal könnten wir einen gepflanzten Baum auch als ein Tripel  $(T, r, \nu)$  schreiben, wobei  $\nu$  eine Menge linearer Ordnungen ist, eine lineare Ordnung der Söhne für jede Ecke.

Für jeden der oben definierten Baumtypen definiert man, was ein Isomorphismus ist. Wir erinnern daran, dass eine Abbildung  $f: V(T) \rightarrow V(T')$  ein Isomorphismus zwischen Bäumen  $T$  und  $T'$  ist, wenn  $f$  eine Bijektion ist (d.h. injektiv und surjektiv), für die genau dann  $\{x, y\} \in E(T)$  ist, wenn  $\{f(x), f(y)\} \in E(T')$ . Wenn ein solcher Isomorphismus existiert, schreiben wir  $T \cong T'$ . Ein *Isomorphismus von Wurzelbäumen*  $(T, r)$  und  $(T', r')$  ist ein Isomorphismus  $f$  der Bäume  $T$  und  $T'$  mit der zusätzlichen Eigenschaft, dass  $f(r) = r'$ . Wir drücken dies als  $(T, r) \cong' (T', r')$  aus. Ein *Isomorphismus gepflanzter Bäume* ist ein Isomorphismus von Wurzelbäumen, der zusätzlich bei jeder Ecke die Ordnung der Söhne erhält. Wenn zwei gepflanzte Bäume in diesem Sinne isomorph sind, schreiben wir  $(T, r, \nu) \cong'' (T', r', \nu')$ .

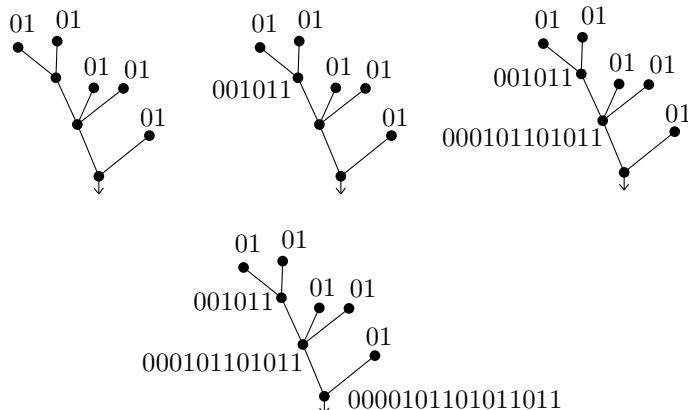
Die Definitionen von  $\cong$ ,  $\cong'$  und  $\cong''$  sind jeweils stärker als die vorige. Das sieht man am besten an den folgenden kleinen Beispielen:



Die Definition des Isomorphismus gepflanzter Bäume ist die mit den meisten Bedingungen, folglich ist die Codierung dieser Bäume am einfachsten. Die folgende Methode ordnet jeder Ecke in einem gepflanzten Baum einen Code zu. Der Code des ganzen Baums ist dann als der Code der Wurzel definiert.

- K1. Jedes Blatt außer der Wurzel erhält den Code 01.
- K2. Sei  $v$  eine Ecke mit den Söhnen  $v_1, v_2, \dots, v_t$  (von links nach rechts). Wenn  $A_i$  der Code des Sohnes  $v_i$  ist, dann erhält die Ecke  $v$  den Code  $0A_1A_2\dots A_t1$ .

Der Prozess, wie ein Code Schritt für Schritt aufgebaut wird, sieht so aus:



Isomorphe gepflanzte Bäume erhalten deshalb den gleichen Code, weil wir bei der Konstruktion des Codes ausschließlich Eigenschaften ver-

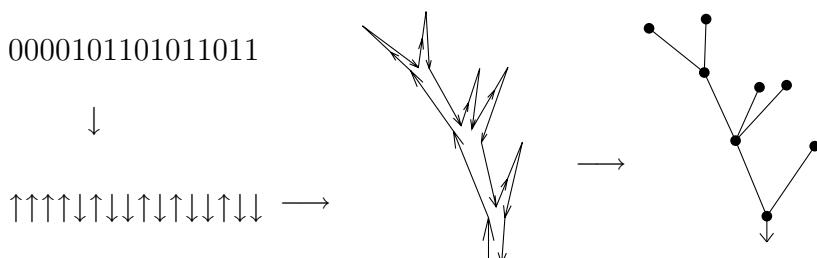
wendet haben, die unter Isomorphismen gepflanzter Bäume erhalten bleiben.

Nun zeigen wir, wie wir den ursprünglichen gepflanzten Baum aus dem Code rekonstruieren können. Auf diese Art beweisen wir, dass nicht isomorphe gepflanzte Bäume verschiedene Codes erhalten. Wir führen Induktion über die Länge des Codes.

Der kürzest mögliche Code, 01, gehört zu dem gepflanzten Baum mit einer einzelnen Ecke. (Nach K2: Die Wurzel hat keine Söhne, deshalb wird bei 0...1 nichts für die Punkte eingesetzt.) Im Induktionsschritt untersuchen wir einen Code  $k$  der Länge  $2(n+1)$ . Dieser Code hat die Form  $0A1$ , wobei  $A = A_1A_2\dots A_t$  eine Verkettung der Codes mehrerer gepflanzter Bäume ist (im Extremfall  $t = 1$  ist  $A$  einfach Code eines gepflanzten Baums). Den Teil  $A_1$  identifiziert man als das kürzeste Anfangsstück der Folge  $A$ , das gleich viele Nullen und Einsen enthält. Analog ist  $A_2$  das nächste minimale Segment mit gleich vielen Nullen und Einsen, und so weiter. Nach Induktionsvoraussetzung gehört jedes  $A_i$  zu einem eindeutigen gepflanzten Baum. Der gepflanzte Baum, der durch den Code  $k$  beschrieben wird, hat eine Wurzel  $r$ , und diese Wurzel hat als Söhne die Wurzeln  $r_1, r_2, \dots, r_t$  der gepflanzten Bäume, die durch die Folgen  $A_1$  bis  $A_t$  codiert sind (von links nach rechts). Also bestimmt der Code einen gepflanzten Baum eindeutig.

**Decodieren mit der Pfeilmethode.** Wir müssen unbedingt noch vorführen, wie man sich diesen Code ganz anschaulich vorstellen kann. Dann wird auch das Decodieren zum Kinderspiel.

In einer gegebenen Codefolge ersetzen wir jede 0 durch einen Pfeil „ $\uparrow$ “ und jede 1 durch einen Pfeil „ $\downarrow$ “. Dann lesen wir diese Folge von Pfeilen als Anweisungen, wie wir den Baum zeichnen sollen. Immer wenn wir auf einen „ $\uparrow$ “ stoßen, zeichnen wir eine Kante vom aktuellen Punkt aufwärts (und zwar weiter rechts als die anderen von diesem Punkt aus schon gezeichneten Teile). Bei einem „ $\downarrow$ “ folgen wir einer schon gezeichneten Kante abwärts. Das ganze sieht dann ungefähr so aus:



(Diese Prozedur zeichnet auch den Pfeil an der Wurzel, denn ein Baum mit nur einer Ecke hat den Code 01.) Etwas verspielt formuliert kann man also sagen: Der Code eines gepflanzten Baums beschreibt den Weg einer Raupe, die den Baum entlang kriecht.

Wir haben die Isomorphismen gepflanzter Bäume so genau studiert, weil sich der Algorithmus für gepflanzte Bäume leicht zu einem Algorithmus für Wurzelbäume erweitern lässt. Wir erzeugen den Code eines Wurzelbaums  $(T, r)$  ganz ähnlich wie für gepflanzte Bäume, als einzige Änderung befolgen wir statt Regel K2 die folgende Modifikation:

K2'. Wenn jeder Sohn  $w$  einer Ecke  $v$  schon einen Code  $A(w)$  hat, dann ordnen wir die Söhne  $w_1, w_2, \dots, w_t$  so, dass  $A(w_1) \leq A(w_2) \leq \dots \leq A(w_t)$ . Die Ecke  $v$  erhält dann den Code  $0\ A_1\ A_2\dots A_t\ 1$ , wobei  $A_i = A(w_i)$ .

Hier bedeutet  $A \leq B$ , dass die Folge  $A$  in irgendeiner vorher festgelegten Ordnung aller endlichen 0-1-Folgen vor  $B$  kommt. Üblich ist z.B. die so genannte *lexikographische Ordnung*. Dabei werden zwei (verschiedene) Folgen  $A = (a_1, a_2, \dots, a_n)$  und  $B = (b_1, b_2, \dots, b_m)$  so miteinander verglichen:

- Wenn  $A$  ein Anfangsstück von  $B$  ist, dann  $A < B$ . Wenn  $B$  ein Anfangsstück von  $A$  ist, dann  $B < A$ . (Zum Beispiel ist  $0010 < 00100$  und  $0 < 0111$ .)
- Andernfalls sei  $j$  der kleinste Index mit  $a_j \neq b_j$ . Wenn  $a_j < b_j$  ist, dann  $A < B$ , und wenn  $a_j > b_j$  ist, dann  $A > B$ . (Zum Beispiel ist  $011 < 1$  und  $10011 < 10110$ .)

Wir müssen prüfen, dass zwei Wurzelbäume genau dann isomorph sind, wenn sie den gleichen Code haben. Der Beweis ist ganz ähnlich wie bei gepflanzten Bäumen, deshalb „überlassen wir ihn der geneigten Leserin zur Übung.“

Nun kommen wir zur Codierung von Bäumen ohne Wurzel.<sup>2</sup> Unsere Aufgabe würde wesentlich vereinfacht, wenn wir eine Ecke finden würden, die die Rolle der Wurzel übernehmen kann; so eine Ecke müsste unter jedem Isomorphismus erhalten bleiben. Für Bäume kann man so eine ausgezeichnete Ecke tatsächlich finden (nun, nicht immer, aber die Ausnahmefälle sind leicht zu charakterisieren und

---

<sup>2</sup>Manchmal wird der Begriff *freier Baum* benutzt, wenn besonders betont werden soll, dass die Rede von einem Baum ohne Wurzel ist.

auch nicht besonders schwer in den Griff zu bekommen). Die relevanten Definitionen sind auch in anderem Kontext nützlich, deshalb formulieren wir sie allgemein für Graphen und nicht nur für Bäume.

Für eine Ecke  $v$  in einem Graphen  $G$  bezeichne das Symbol  $\text{ex}_G(v)$  das Maximum der Abstände von  $v$  zu allen anderen Ecken von  $G$ . Die Zahl  $\text{ex}_G(v)$  heißt die *Exzentrizität* der Ecke  $v$  in dem Graphen  $G$ . Die Idee dabei ist, dass die Ecken mit kleiner Exzentrizität zentral gelegen sind, während die mit großer Exzentrizität „im äußeren Bereich“ von  $G$  liegen.

Mit  $C(G)$  bezeichnen wir die Menge aller Ecken von  $G$  mit minimaler Exzentrizität. Die Menge  $C(G)$  heißt das *Zentrum*<sup>3</sup> von  $G$ . Am Beispiel eines Kreises (und vieler anderer Graphen) sieht man, dass das Zentrum manchmal aus der gesamten Eckenmenge besteht. Aber für Bäume gilt

**Hilfssatz.** *Für jeden Baum  $T$  hat  $C(T)$  höchstens zwei Ecken. Wenn  $C(T)$  aus zwei Ecken  $x$  und  $y$  besteht, dann ist  $\{x, y\}$  eine Kante.*

*Beweis.* Wir beschreiben eine Methode, das Zentrum eines Baums zu finden. Gegeben sei ein Baum  $T = (V, E)$ . Wenn  $T$  zwei oder weniger Ecken hat, dann ist die gesamte Eckenmenge das Zentrum und der Hilfssatz gilt. Ansonsten sei  $T' = (V', E')$  der Baum, der aus  $T$  durch Abreißen aller Blätter entsteht:

$$\begin{aligned} V' &= \{x \in V : \deg_T(x) > 1\}, \\ E' &= \{\{x, y\} \in E : \deg_T(x) > 1 \text{ und } \deg_T(y) > 1\}. \end{aligned}$$

Klarerweise ist  $V(T') \neq \emptyset$  (denn nicht alle Ecken von  $T$  können Blätter sein). Des Weiteren sind die entferntesten Ecken von jeder Ecke  $v$  aus notwendig Blätter, deshalb erhalten wir für jedes  $v \in V'$

$$\text{ex}_T(v) = \text{ex}_{T'}(v) + 1.$$

Insbesondere ist  $C(T') = C(T)$ . Wenn  $T'$  mindestens drei Ecken hat, wiederholen wir die eben beschriebene Konstruktion, wenn nicht, dann haben wir das Zentrum von  $T$  gefunden.  $\square$

Wir können nun den Code eines Baums  $T$  beschreiben.

---

<sup>3</sup>Die Exzentrizität der Ecken im Zentrum heißt der *Radius* des Graphen  $G$ .

- Wenn das Zentrum von  $T$  aus einer einzelnen Ecke  $v$  besteht, dann definieren wir den Code von  $T$  als den Code des Wurzelbaums  $(T, v)$ .
- Wenn das Zentrum von  $T$  aus einer Kante  $e = \{x_1, x_2\}$  besteht, betrachten wir den Graph  $T - e$ . Dieser Graph hat genau zwei Komponenten  $T_1$  und  $T_2$ ; dabei wählen wir die Namen  $T_1, T_2$  so, dass  $x_i \in V(T_i)$  ist. Der Buchstabe  $A$  bezeichne den Code des Wurzelbaums  $(T_1, x_1)$  und der Buchstabe  $B$  den Code des Wurzelbaums  $(T_2, x_2)$ . Wenn in der lexikographischen Ordnung  $A \leq B$  ist, dann codieren wir den Baum  $T$  durch den Code des Wurzelbaums  $(T, x_1)$ , und wenn  $A \geq B$  ist, dann codieren wir  $T$  durch den Code von  $(T, x_2)$ .

Jetzt sind wir in der Lage, jeden Baum durch eine 0-1-Folge zu codieren.

Das Decodieren geht genauso wie bei den gepflanzten Bäumen (und erlaubt unter anderem, die „kanonische“ Zeichnung eines Baums zu definieren). Weil ein Isomorphismus ein Zentrum auf ein Zentrum abbildet und weil wir schon gesehen haben, dass die Codierung für Wurzelbäume funktioniert, ist leicht einzusehen, dass zwei Bäume genau dann den gleichen Code haben, wenn sie isomorph sind.

Das Ziel bei der Beschreibung von Bäumen durch Zahlenfolgen war, Bäume einfach auf Isomorphie testen zu können. Die Algorithmen für die verschiedenen Typen von Bäumen, die in diesem Abschnitt erklärt wurden, können so implementiert werden, dass die Anzahl der elementaren Rechenschritte (etwa Computerinstruktionen) durch eine lineare Funktion in der Eingabegröße (z.B. Summe der Eckenzahlen der beiden Bäume) beschränkt ist.

Man kennt noch weitere Graphenklassen, für die man das Isomorphieproblem effizient entscheiden kann. Die vielleicht wichtigsten Beispiele sind die Klasse aller ebenen Graphen und die Klasse aller Graphen, deren Maximalgrad durch eine kleine Konstante beschränkt ist. In diesen Fällen sind die bekannten Algorithmen jedoch schon ziemlich kompliziert.

## Aufgaben

1. (a) Finden Sie einen *asymmetrischen* Baum, d.h. einen Baum auf mindestens 2 Ecken, der nur einen einzigen Automorphismus zulässt (der dann natürlich die Identität sein muss). (Für die Definition von Automorphismus siehe Aufgabe 4.1.3).

- (b) Finden Sie die kleinstmögliche Eckenzahl, die ein Baum wie in (a) haben kann (d.h. beweisen Sie, dass kein kleinerer Baum asymmetrisch sein kann).
2. Finden Sie zwei nicht isomorphe Bäume mit der gleichen Gradfolge.
  3. Ein Wurzelbaum heißt *binär*, wenn jede innere Ecke (d.h. die kein Blatt ist) genau zwei Söhne hat.
    - (a) Zeichnen Sie alle nicht isomorphen binären Bäume mit 9 Ecken.
    - (b) Charakterisieren Sie die Codes binärer Bäume.
  4. Beweisen Sie im Detail, dass isomorphe Bäume (ohne Wurzel) durch die oben beschriebene Prozedur den gleichen Code erhalten, und dass nicht isomorphe Bäume verschiedene Codes bekommen.
  5.  $^{*,\text{Inf}}$  Seien  $A_1, \dots, A_t$  Folgen von Nullen und Einsen (möglicherweise von verschiedenen Längen). Mit  $n$  bezeichnen wir die Summe ihrer Längen. Entwerfen Sie einen Algorithmus, der diese Folgen in  $O(n)$  Schritten lexikographisch sortiert. Dabei darf in einem Schritt nur auf ein Glied einer Folge  $A_i$  zugegriffen werden; es ist nicht erlaubt, eine ganze 0-1-Folge mit einem Mal zu manipulieren.
  6. Beweisen Sie, dass es höchstens  $4^n$  paarweise nicht isomorphe Bäume auf  $n$  Ecken gibt.
  7. Sei  $T = (V, E)$  ein Baum und  $v$  eine Ecke von  $T$ . Sei

$$\tau(v) = \max(|V(T_1)|, |V(T_2)|, \dots, |V(T_k)|),$$

wobei  $T_1, \dots, T_k$  alle Komponenten des Graphen  $T - v$  sind. Das *Zentroid* des Baums  $T$  ist die Menge aller Ecken  $v \in V$  mit minimalem  $\tau(v)$ .

- (a) \*Beweisen Sie, dass das Zentroid eines Baums entweder aus einer einzelnen Ecke oder aus zwei durch eine Kante verbundenen Ecken besteht.
- (b) Ist das Zentroid immer identisch mit dem Zentrum?
- (c) Beweisen Sie: Wenn  $v$  eine Ecke im Zentroid ist, dann ist  $\tau(v) \leq \frac{2}{3}|V(T)|$ .

### 5.3 Aufspannende Bäume eines Graphen

Ein aufspannender Baum ist eine der elementaren Graphenkonstruktionen:

**5.3.1 Definition.** Sei  $G = (V, E)$  ein Graph. Ein beliebiger Baum der Form  $(V, E')$ , mit  $E' \subseteq E$ , heißt ein aufspannender Baum des Graphen  $G$ . So ein aufspannender Baum ist ein Teilgraph von  $G$ , der ein Baum ist und alle Ecken von  $G$  enthält.

Offensichtlich kann nur ein zusammenhängender Graph  $G$  einen aufspannenden Baum haben. Es ist nicht schwer zu zeigen, dass jeder zusammenhängende Graph einen aufspannenden Baum besitzt. Wir beweisen das, indem wir zwei (schnelle) Algorithmen angeben, die in einem gegebenen zusammenhängenden Graphen einen aufspannenden Baum finden. In den folgenden Abschnitten werden wir Varianten dieser Algorithmen benötigen, deshalb wollen wir sie genau untersuchen.

**5.3.2 Algorithmus (Aufspannender Baum 1).** Sei  $G = (V, E)$  ein Graph mit  $n$  Ecken und  $m$  Kanten. Wir ordnen die Kanten von  $G$  in einer beliebigen Reihenfolge  $(e_1, e_2, \dots, e_m)$  an. Der Algorithmus konstruiert schrittweise Kantenmengen  $E_0, E_1, \dots \subseteq E$ .

Sei  $E_0 = \emptyset$ . Wenn die Menge  $E_{i-1}$  schon bestimmt ist, dann berechnen wir die Menge  $E_i$  wie folgt:

$$E_i = \begin{cases} E_{i-1} \cup \{e_i\} & \text{wenn der Graph } (V, E_{i-1} \cup \{e_i\}) \text{ keinen Kreis} \\ E_{i-1} & \text{sonst.} \end{cases} \quad [\text{enthält,}]$$

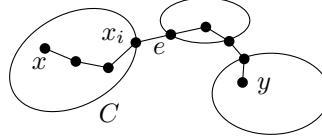
Der Algorithmus stoppt, wenn entweder  $E_i$  schon  $n - 1$  Kanten hat oder wenn  $i = m$ , d.h. wenn alle Kanten aus  $G$  schon abgearbeitet sind. Mit  $E_t$  bezeichnen wir die Menge, mit der der Algorithmus stoppt, und mit  $T$  den Graphen  $(V, E_t)$ .

**5.3.3 Hilfssatz (Korrekttheit von Algorithmus 5.3.2).** Wenn Algorithmus 5.3.2 einen Graph  $T$  mit  $n - 1$  Kanten erzeugt, dann ist  $T$  ein aufspannender Baum von  $G$ . Wenn es  $k < n - 1$  Kanten in  $T$  gibt, dann ist der Graph  $G$  nicht zusammenhängend und hat  $n - k$  Komponenten.

*Beweis.* So wie die Mengen  $E_i$  gebildet werden, kann der Graph  $G$  keinen Kreis enthalten. Ist  $k = |E(T)| = n - 1$ , dann ist  $T$  ein Baum nach Aufgabe 5.1.2, und somit ein aufspannender Baum von  $G$ . Ist  $k < n - 1$ , dann ist  $T$  nicht zusammenhängend und jede Komponente ist ein Baum (so einen Graph nennt man einen *Wald*). Man sieht leicht, dass er  $n - k$  Komponenten hat.

Wir beweisen mit Widerspruch, dass die Eckenmengen der Komponenten des Graphen  $T$  mit den Eckenmengen der Komponenten des Graphen  $G$  übereinstimmen. Angenommen, das ist nicht wahr, d.h. es gibt zwei Ecken  $x$  und  $y$ , die in der gleichen Komponente von

$G$  aber in verschiedenen Komponenten von  $T$  liegen. Mit  $C$  bezeichnen wir die Komponente von  $T$ , in der die Ecke  $x$  liegt, und wir betrachten in dem Graphen  $G$  einen Weg  $(x = x_0, e_1, x_1, e_2, \dots, e_\ell, x_\ell = y)$  von  $x$  nach  $y$ , wie in dem folgenden Bild:



Sei  $i$  der letzte Index, für den  $x_i$  in der Komponente  $C$  enthalten ist. Offensichtlich ist  $i < \ell$ , also ist  $x_{i+1} \notin C$ . Die Kante  $e = \{x_i, x_{i+1}\}$  gehört deshalb nicht zum Graphen  $T$ , und so muss sie zu irgend einem Zeitpunkt mit einigen der schon für  $T$  ausgewählten Kanten einen Kreis bilden (sonst würde sie der Algorithmus ja dazunehmen). Deshalb enthält auch der Graph  $T + e$  einen Kreis; das aber ist unmöglich, weil  $e$  zwei verschiedene Komponenten von  $T$  miteinander verbindet. So erhalten wir den Widerspruch.  $\square$

**Komplexität des Algorithmus.** Wir haben gerade gezeigt, dass Algorithmus 5.3.2 stets tut, was wir von ihm erwarten, nämlich einen aufspannenden Baum des gegebenen Graphen zu berechnen. Aber wenn wir tatsächlich mit dem Problem konfrontiert sind, in verhältnismäßig großen Graphen aufspannende Bäume zu finden, sollten wir dann die Zeit (oder das Geld) aufbringen diesen Algorithmus zu programmieren?

So eine Frage zu beantworten ist nicht ganz einfach, man vergleicht Algorithmen nach verschiedenen, zuweilen widersprüchlichen Kriterien. Zum Beispiel ist die Einfachheit und Klarheit eines Algorithmus ein wichtiges Kriterium (denn komplizierte oder obskure Algorithmen führen allzu leicht zu Programmierfehlern), aber auch die Robustheit (welchen Einfluss haben Rundungsfehler oder kleinen Ungenauigkeiten in den Eingabedaten auf die Korrektheit des Ergebnisses?), Speicherbedarf und vieles mehr. Das vielleicht gebräuchlichste Maß für die Komplexität eines Algorithmus ist seine *Zeitkomplexität*, womit die Anzahl der elementaren Operationen (wie Additionen, Multiplikationen, Vergleiche zweier Zahlen usw.) gemeint ist, die der Algorithmus zur Lösung des eingegebenen Problems durchführen muss. In den allermeisten Fällen betrachtet man die *Worst-Case-Komplexität*, das ist die Anzahl der Operationen, die schlimmstenfalls nötig ist. Man darf sich „den schlimmstmöglichen Fall“ als eine Eingabe vorstellen, die sich der Erzfeind ausgedacht hat um einem das Leben möglichst schwer (und den Algorithmus möglichst langsam) zu machen. Die Zeitkomplexität ist eine Funktion, die von der „Größe der Eingabe“ abhängt. Bei der Berechnung eines aufspannenden Baums kann man die Größe der Eingabe

z.B. durch die Summe von Eckenzahl und Kantenzahl des Eingabe-graphen ausdrücken. Statt „Worst–Case–Zeitkomplexität“ werden wir einfach „Komplexität“ sagen, denn andere Komplexitätstypen (sinnvoll ist z.B. auch die durchschnittliche Anzahl von Operationen) werden wir nicht diskutieren.

Nur selten kann man die Komplexität eines Algorithmus exakt bestimmen. Um auch nur davon träumen zu können, müssten wir genau festlegen, welches die elementaren Operationen sind (das hieße auch, dass wir uns damit auf einen bestimmten Computer beschränken würden), und außerdem müssten wir den Algorithmus bis ins kleinste Detail beschreiben; im Wesentlichen hieße das, dass wir ein konkretes Programm untersuchen. Doch selbst wenn man diese Einschränkungen in Kauf nehmen wollte, wäre die genaue Bestimmung der Komplexität schon für sehr einfache Algorithmen recht aufwändig. Deshalb analysiert man die Komplexität von Algorithmen in den meisten Fällen nur asymptotisch. Typische Aussagen sind dann von der Form, ein Algorithmus habe die Komplexität  $O(n^{3/2})$ , ein anderer  $O(n \log n)$  und so weiter (hier ist  $n$  ein Parameter, der die Größe der Eingabe misst).

Um die Güte eines Algorithmus wirklich beurteilen zu können, ist es meist notwendig, so eine theoretische Analyse durch Testläufe mit verschiedenen Eingabedaten auf einem Rechner zu ergänzen. Wenn die asymptotische Analyse etwa eine Komplexität von  $O(n^2)$  für den einen Algorithmus ergibt und  $O(n \log^4 n)$  für den anderen, dann scheint auf den ersten Blick der zweite Algorithmus klar überlegen, weil die Funktion  $n \log^4 n$  viel langsamer wächst als  $n^2$ . Wenn aber die exakte Komplexität des ersten Algorithmus  $n^2 - 5n$  ist und die des zweiten  $20n(\log_2 n)^4$ , dann käme die Überlegenheit des zweiten Algorithmus erst für  $n > 5 \cdot 10^6$  zum Tragen, und so eine Überlegenheit ist vom praktischen Gesichtspunkt aus wertlos.

Wir wollen nun die asymptotische Komplexität von Algorithmus 5.3.2 schätzen. Wir haben den Algorithmus aber auf einem „high level“ beschrieben. Das bezieht sich auf die Tatsache, dass wir zum Beispiel einen Test benutzen, ob eine gegebene Menge von Kanten einen Kreis enthält, was man beim besten Willen nicht als eine elementare Operation auffassen kann. Die Komplexität des Algorithmus wird also auch davon abhängen, wie geschickt wir solch komplexe Operationen mittels elementaren Operationen zu realisieren in der Lage sind.

Wenn wir über unseren Algorithmus 5.3.2 nachdenken, fällt auf, dass es nicht nötig ist, all die Kantenmengen  $E_i$  zu speichern, sondern dass sie alle durch ein und die selbe Variable repräsentiert werden können (etwa durch eine Liste von Kanten), die sukzessive die Werte  $E_0, E_1, \dots$  hat. Die einzige Frage von Bedeutung ist, wie wir effizient testen können, ob das Hinzufügen einer neuen Kante  $e_i$  einen Kreis erzeugt oder nicht. Dies ist die entscheidende Beobachtung: Genau dann entsteht ein Kreis, wenn die beiden Enden der Kante  $e_i$  zur glei-

chen Zusammenhangskomponente des Graphen  $(V, E_{i-1})$  gehören. Wir müssen also das folgende Problem lösen:

**5.3.4 Problem (UNION–FIND Problem).** Sei  $V = \{1, 2, \dots, n\}$  eine Menge von Ecken. Anfangs ist die Menge  $V$  in 1-elementige Äquivalenzklassen partitioniert (d.h. keine zwei verschiedenen Ecken werden als äquivalent angesehen). Wie kann man diese Äquivalenzrelation auf  $V$  (mit anderen Worten: eine Partition von  $V$  in Äquivalenzklassen) so in einer geeigneten Datenstruktur speichern, dass die folgenden zwei Typen von Operationen effizient ausgeführt werden können:

- (i) (UNION) Mache zwei gegebene nicht äquivalente Ecken  $i, j \in V$  äquivalent, d.h. ersetze die zwei Klassen, die sie enthalten, durch ihre Vereinigung.
- (ii) (Test auf Äquivalenz — FIND) Gegeben zwei Ecken  $i, j \in V$ , entscheide, ob sie zu diesem Zeitpunkt äquivalent sind oder nicht.

Eine neue Anfrage (UNION oder FIND) erreicht den Algorithmus erst, nachdem er die vorige Operation abgearbeitet hat.

Unser Algorithmus 5.3.2 zum Auffinden eines aufspannenden Baums benötigt höchstens  $n - 1$  UNION-Operationen und höchstens  $m$  FIND-Operationen.

Wir beschreiben eine recht einfache Lösung für Problem 5.3.4. Anfangs kennzeichnen wir alle Ecken in  $V$  mit verschiedenen Markierungen, z.B. mit  $1, 2, \dots, n$ . Wir werden dafür Sorge tragen, dass die Markierungen immer so verteilt sind, dass zwei Ecken genau dann äquivalent sind, wenn sie die gleiche Markierung haben. Der Äquivalenztest FIND ist damit ein simpler Vergleich zweier Markierungen. Um zwei Klassen durch ihre Vereinigung zu ersetzen, müssen wir die Markierungen für die Elemente in einer der Klassen austauschen. Wenn wir die Elemente einer jeden Klasse außerdem noch in einer Liste speichern, dann ist die für das neue Markieren nötige Zeit proportional zur Größe derjenigen Klasse, deren Markierungen ausgetauscht werden.

Als eine sehr grobe Abschätzung der Laufzeit können wir so vorgehen: Keine Klasse hat mehr als  $n$  Elemente, also benötigt eine einzelne UNION-Operation nie mehr als  $O(n)$  Zeit. Für  $n - 1$  UNION-Operationen und  $m$  FIND-Operationen erhalten wir also die Schranke  $O(n^2 + m)$ . Eine billige Verbesserung ist, sich auch noch die Größe jeder Klasse zu merken und die Markierungen immer in der kleineren Klasse zu wechseln. Für diesen Algorithmus kann man eine viel bessere Schranke herleiten:  $O(n \log n + m)$  (Aufgabe 1). Die beste bekannte Lösung für Problem 5.3.4 stammt von Tarjan und benötigt höchstens  $O(n\alpha(n) + m)$  Schritte für  $m$  FIND- und  $n - 1$  UNION-Operationen (siehe z.B. Aho, Hopcroft und Ullman [12]), wobei  $\alpha(n)$  eine Funktion von  $n$  ist, die wir hier nicht definieren wollen; wir merken lediglich an, dass  $\alpha(n)$  zwar ins Unendliche wächst mit  $n \rightarrow \infty$ , aber extrem langsam, viel langsamer als Funktionen wie  $\log \log n$ ,  $\log \log \log n$  usw. Für

praktische Zwecke ist die oben beschriebene Lösung (mit Ummarkieren der jeweils kleineren Menge) wahrscheinlich vollauf ausreichend.

Wir präsentieren einen weiteren Algorithmus für aufspannende Bäume, der vielleicht noch einfacher ist.

**5.3.5 Algorithmus (Aufspannender Baum 2).** Gegeben sei ein Graph  $G = (V, E)$  mit  $n$  Ecken und  $m$  Kanten. Wir werden sukzessive Eckenmengen  $V_0, V_1, V_2, \dots \subseteq V$  und Kantenmengen  $E_0, E_1, E_2, \dots \subseteq E$  konstruieren. Wir setzen  $E_0 = \emptyset$  und  $V_0 = \{v\}$ , wobei  $v$  eine beliebige Ecke ist.

Wenn  $V_{i-1}$  und  $E_{i-1}$  schon konstruiert sind, finden wir eine Kante  $e_i = \{x_i, y_i\} \in E(G)$ , so dass  $x_i \in V_{i-1}$  und  $y_i \in V \setminus V_{i-1}$ , und wir setzen  $V_i = V_{i-1} \cup \{y_i\}$ ,  $E_i = E_{i-1} \cup \{e_i\}$ . Wenn es keine solche Kante gibt, endet der Algorithmus und gibt den bisher konstruierten Graphen  $T = (V_t, E_t)$  aus.

**5.3.6 Hilfssatz (Korrektheit von Algorithmus 5.3.5).** Wenn der Algorithmus mit einem Graph  $T$  mit  $n$  Ecken endet, dann ist  $T$  ein aufspannender Baum von  $G$ . Ansonsten ist  $G$  ein nicht zusammenhängender Graph und  $T$  ist ein aufspannender Baum derjenigen Komponente von  $G$ , welche die Anfangsecke  $v$  enthält.

*Beweis.* Der Graph  $T$  ist ein Baum, weil er zusammenhängend ist und die richtige Anzahl von Kanten und Ecken hat. Hat  $T$  genau  $n$  Ecken, dann ist er ein aufspannender Baum.; nehmen wir also an,  $T$  habe  $\bar{n} < n$  Ecken. Es bleibt zu zeigen, dass  $V(T)$  die Eckenmenge einer Komponente von  $G$  ist.

Nehmen wir das Gegenteil an: Es gebe ein  $x \in V(T)$  und ein  $y \notin V(T)$ , die durch einen Weg im Graphen  $G$  verbunden sind. Wie im Beweis von Hilfssatz 5.3.3 finden wir auf diesem Weg eine Kante  $e = \{x_j, y_j\} \in E(G)$ , so dass  $x_j \in V(T)$  und  $y_j \in V \setminus V(T)$ . Der Algorithmus hätte also die Kante  $e$  und die Ecke  $y_j$  zu dem Baum hinzufügen können statt mit dem Baum  $T$  aufzuhören. Dieser Widerspruch beendet den Beweis.  $\square$

**Bemerkung.** Die Details des eben beschriebenen Algorithmus können so ausgearbeitet werden, dass die Laufzeit  $O(n + m)$  ist (siehe Aufgabe 2).

## Aufgaben

1. Beweisen Sie: Wenn das Problem 5.3.4 mit der beschriebenen Methode (stets die Markierungen in der kleineren Klasse zu ändern) gelöst

wird, dann ist die totale Komplexität von  $n - 1$  UNION-Operationen höchstens  $O(n \log n)$ .

2. *\*.Inf* Arbeiten Sie die Details von Algorithmus 5.3.5 so aus, dass die Laufzeit im schlimmsten Fall  $O(n+m)$  ist. (Dazu benötigen Sie Kenntnisse einfacher listenartiger Datenstrukturen.)
3. In Aufgabe 4.4.7 haben wir einen Hamiltonschen Kreis in einem Graphen  $G$  definiert als einen Kreis, der alle Ecken von  $G$  enthält. Für einen Graphen  $G$  und eine natürliche Zahl  $k \geq 1$  definieren wir den Graph  $G^{(k)}$  als den Graph mit Eckenmenge  $V(G)$ , in dem zwei (verschiedene) Ecken genau dann durch eine Kante verbunden sind, wenn ihr Abstand in  $G$  höchstens  $k$  ist.
  - (a) \*Beweisen Sie, dass für jeden Baum  $T$  der Graph  $T^{(3)}$  einen Hamiltonschen Kreis besitzt.
  - (b) Schließen Sie mit Hilfe von (a), dass  $G^{(3)}$  einen Hamiltonschen Kreis besitzt für jeden zusammenhängenden Graphen  $G$ .
  - (c) Finden Sie einen zusammenhängenden Graphen  $G$ , so dass  $G^{(2)}$  keinen Hamiltonschen Kreis besitzt.

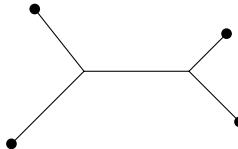
## 5.4 Minimal aufspannende Bäume

Stellen Sie sich eine Karte ihres bevorzugten Ausflugsgebiets vor (mit vielleicht 30–40 Dörfern). Einige der Dörfer sind durch Schotterwege miteinander verbunden, und zwar so, dass man jedes Dorf von jedem anderen aus entlang der Schotterstraßen erreichen kann. Das Verkehrsamt beschließt, einige dieser Wege zu asphaltierten Landstraßen auszubauen, auf denen man zügig vorankommt. Die finanziellen Mittel sind aber knapp, deshalb soll das ganze möglichst wenig kosten — am Ende soll es aber möglich sein, von jedem Dorf aus in jedes andere zu fahren nur unter Benutzung von Landstraßen. Dies ist ein fundamentales Graphenproblem, wir suchen einen *minimal aufspannenden Baum*. Dieser Abschnitt ist der Lösung dieses Problems gewidmet.

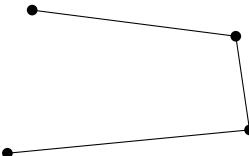
Wenn Sie sich nicht angesprochen fühlen, weil ihr bevorzugtes Ausflugsgebiet schon lange ein dichtes Netz an Bundes- und Landstraßen aufweist, dann dürfen Sie sich ein weniger entwickeltes Land vorstellen oder eine andere natürliche Formulierung des zu Grunde liegenden mathematischen Problems erfinden.

Wir nehmen unausgesprochen an, dass die existierenden Wege keine Kreuzungen außerhalb der Dörfer haben und dass die neuen Straßen

(wegen der Eigentumsverhältnisse?) nur an Stelle der alten gebaut werden dürfen. Sonst könnte es eine billigere Lösung sein, vier Orte so zu verbinden:



und nicht so



Wenn wir die erste Lösung zulassen, erhalten wir ein anderes algorithmisches Problem (das des *Steiner-Baums*), welches sich als sehr viel schwieriger erweist als das des minimal aufspannenden Baums.

Eine mathematische Formulierung der Suche nach einem minimal aufspannenden Baum erfordert, die Definition eines Graphen ein wenig zu erweitern: Wir werden Graphen mit *gewichteten Kanten* betrachten. Das bedeutet, dass für jede Kante  $e \in E$  eine Zahl  $w(e)$  gegeben ist, genannt das *Gewicht* der Kante  $e$ . Das Gewicht einer Kante ist normalerweise eine nicht negative ganze oder reelle Zahl. Ein Graph  $G = (V, E)$  zusammen mit einer Gewichtsfunktion  $w$  auf seinen Kanten,  $w: E \rightarrow \mathbb{R}$ , wird manchmal als *Netzwerk* bezeichnet.

Nun sind wir in der Lage, unser Problem aus dem Straßenbau in der Sprache der Graphentheorie zu formulieren:

**Problem.** Gegeben ein zusammenhängender Graph  $G = (V, E)$  mit einer nicht negativen Gewichtsfunktion  $w$  auf den Kanten, finde einen aufspannenden zusammenhängenden Teilgraphen  $(V, E')$ , für den die Summe

$$w(E') = \sum_{e \in E'} w(e) \quad (5.1)$$

den minimalen Wert annimmt.

Man sieht leicht, dass sich unter den Lösungen dieses Problems stets mindestens ein aufspannender Baum von  $G$  befindet. Wenn die Gewichte strikt positiv sind, dann muss *jede* Lösung ein aufspannender Baum sein. Wenn zum Beispiel alle Kanten das Gewicht 1 haben, dann sind die Lösungen des Problems genau die aufspannenden

Bäume des Graphen, und der Ausdruck (5.1) nimmt als minimalen Wert  $|V| - 1$  an.

Deshalb können wir uns auf das folgende Problem beschränken:

**5.4.1 Problem (Minimal aufspannender Baum).** Finde für einen zusammenhängenden Graphen  $G = (V, E)$  mit einer Gewichtsfunktion  $w$  auf den Kanten einen aufspannenden Baum  $T = (V, E')$  mit kleinstmöglichem Wert  $w(E')$ .

Dem aufmerksamen Leser wird nicht entgangen sein, dass wir negative Gewichte hier zulassen. Die Algorithmen, die wir untersuchen wollen, lösen sogar das allgemeinere Problem mit beliebigen Gewichten. Das ist gar nicht selbstverständlich: Viele Graphenprobleme, die mit nicht negativen Gewichten einfach sind, verwandeln sich in algorithmisch schwere Probleme, wenn wir Gewichte mit beliebigem Vorzeichen zulassen. Ein Beispiel eines solchen Problems ist, einen kürzesten Weg in einem Netzwerk zu finden, wobei die Länge eines Weges als die Summe seiner Kantengewichte definiert ist.

Ein gegebener Graph kann sehr viele aufspannende Bäume besitzen (siehe Kapitel 8) und es sieht vielleicht schwierig aus, den besten zu finden. Es ist aber nicht so schwer, eine einfache Modifikation der Algorithmen aus dem vorigen Abschnitt funktioniert. Wir stellen Ihnen mehrere Algorithmen vor; ein einfacher (und weit verbreiterter) ist der folgende:

**5.4.2 Algorithmus (Der Greedy<sup>4</sup>–Algorithmus (Kruskal)).** Die Eingabe ist ein zusammenhängender Graph  $G = (V, E)$  mit einer Gewichtsfunktion  $w$  auf den Kanten. Wir sortieren die Kanten  $e_1, e_2, \dots, e_m$  nach Gewicht, so dass

$$w(e_1) \leq w(e_2) \leq \dots \leq w(e_n).$$

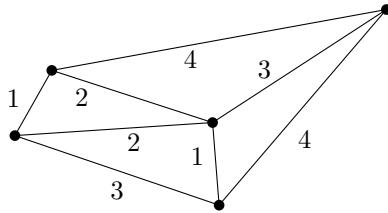
Mit dieser Anordnung der Kanten ist Algorithmus 5.3.2 auszuführen.

Bevor wir die Korrektheit dieses Algorithmus beweisen, was nicht ganz leicht ist, wollen wir den Algorithmus an einem kleinen Beispiel illustrieren.

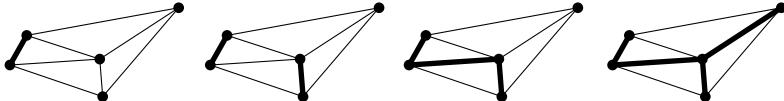
**Beispiel.** Wir wenden den Greedy–Algorithmus auf das folgende Netzwerk an:

---

<sup>4</sup>Englisch greedy = gierig.



Einen möglichen Ablauf des Algorithmus zeigt das nächste Diagramm:



**5.4.3 Hilfssatz (Korrektheit des Greedy–Algorithmus).** *Algorithmus 5.4.2 findet einen minimal aufspannenden Baum.*

*Beweis.* Dieser Beweis ist zwar nicht wirklich tiefgründig, aber er scheint eine konzentrierte Aufmerksamkeit zu verlangen; andernfalls unterlaufen einem sehr leicht Fehler (beide Autoren haben ihre Erfahrungen damit gesammelt).

Sei  $T$  der aufspannende Baum, den der Algorithmus findet, und sei  $\check{T}$  irgendein anderer aufspannender Baum des Graphen  $G = (V, E)$ . Zu zeigen ist, dass  $w(E(T)) \leq w(E(\check{T}))$ . Wir ordnen die Kanten  $e'_1, e'_2, \dots, e'_{n-1}$  von  $T$  nach Gewicht, so dass  $w(e'_1) \leq w(e'_2) \leq \dots \leq w(e'_{n-1})$  ist (die Kante  $e'_i$  ist zugleich ein  $e_j$  aus dem Algorithmus, sie hat nun also zwei verschiedene Namen!). Analog seien  $\check{e}_1, \dots, \check{e}_{n-1}$  die Kanten von  $\check{T}$ , geordnet nach aufsteigendem Gewicht.

Wir zeigen, dass für  $i = 1, \dots, n-1$  sogar gilt

$$w(e'_i) \leq w(\check{e}_i). \quad (5.2)$$

Das zeigt dann natürlich, dass  $T$  ein minimal aufspannender Baum ist. Angenommen, Gleichung (5.2) ist nicht wahr und  $i$  ist der kleinste Index, für den sie verletzt ist, d.h.  $w(e'_i) > w(\check{e}_i)$ . Wir betrachten die Mengen

$$\begin{aligned} E' &= \{e'_1, \dots, e'_{i-1}\}, \\ \check{E} &= \{\check{e}_1, \dots, \check{e}_i\}. \end{aligned}$$

Die Graphen  $(V, E')$  und  $(V, \check{E})$  enthalten keine Kreise, es gelten  $|E'| = i - 1$  und  $|\check{E}| = i$ .

Wenn wir zeigen können, dass es eine Kante  $e \in \check{E}$  gibt, für die der Graph  $(V, E' \cup \{e\})$  keinen Kreis enthält, haben wir einen Widerspruch. Denn dann ist  $w(e) \leq w(\check{e}_i) < w(e'_i)$ , und das heißt, dass wir einen Fehler gemacht haben, als wir die Kante  $e$  in dem Algorithmus getestet haben. Es gab keinen Grund,  $e$  zu verwerfen und nicht auszuwählen, und wir hätten sie an Stelle der Kante  $e'_i$  nehmen sollen (wenn nicht schon früher).

Deshalb genügt es, folgendes zu zeigen: *Sind  $E', \check{E} \subseteq \binom{V}{2}$  zwei Kantenmengen, so dass der Graph  $(V, \check{E})$  keinen Kreis enthält und  $|E'| < |\check{E}|$ , dann gibt es eine Kante  $e \in \check{E}$ , die zwei Ecken aus verschiedenen Komponenten des Graphen  $(V, E')$  miteinander verbindet.* Das zeigen wir mit einem einfachen Zählargument. Seien  $V_1, \dots, V_s$  die Eckenmengen der Komponenten des Graphen  $(V, E')$ . Für  $j = 1 \dots s$  ist

$$\left| E' \cap \binom{V_j}{2} \right| \geq |V_j| - 1,$$

und wenn wir diese Ungleichungen über alle  $j$  summieren, erhalten wir  $|E'| \geq n - s$ . Andererseits ist

$$\left| \check{E} \cap \binom{V_j}{2} \right| \leq |V_j| - 1,$$

weil  $\check{E}$  keinen Kreis enthält, und deshalb liegen höchstens  $n - s$  Kanten aus  $\check{E}$  innerhalb der Komponenten  $V_j$ . Weil wir aber  $|\check{E}| > |E'|$  angenommen haben, gibt es eine Kante  $e \in \check{E}$ , die zwischen zwei verschiedenen Komponenten verläuft.  $\square$

Der hier vorgestellte Algorithmus von Kruskal ist ein Prototyp des so genannten *Greedy–Algorithmus*. „Greedy“ heißt „gierig“, und das ist genau das Charakteristische an dem Algorithmus: In jedem Schritt wählen wir unter allen noch in Frage kommenden Kanten diejenige, die den größten Gewinn verspricht (hier: unter den Kanten, die keinen Kreis erzeugen, die mit den geringsten Kosten). Ganz allgemein nennt man solche Strategien „greedy“, bei denen man in jedem Schritt die Wahl trifft, die in diesem Moment die günstigste scheint, ohne zu bedenken, ob diese Entscheidung spätere Nachteile nach sich zieht. Für viele Probleme ist diese kurzsichtige Strategie völlig unbrauchbar. Beim Schachspiel z.B. würde das (in der einfachsten Form) bedeuten, dass ein Spieler wann immer möglich Figuren schlägt, und zwar stets die wertvollste. Mit so einer naiven Strategie verliert man aber schnell.

Es ist vielleicht etwas überraschend, dass der Greedy–Algorithmus für minimal aufspannende Bäume korrekt arbeitet. Die Greedy–Strategie ist auch für viele andere Probleme nützlich (ganz besonders, wenn

wir keine bessere Idee haben). Oft liefert sie zumindest eine gute Näherungslösung. Probleme, für die der Greedy–Algorithmus garantiert eine optimale Lösung liefert, werden in der so genannten *Matroidtheorie* behandelt. Ein gutes Lehrbuch darüber ist Oxley [28].

## Aufgaben

1. Analog zum minimal aufspannenden Baum ist der *maximal aufspannende Baum* definiert. Formulieren Sie den Greedy–Algorithmus für dieses Problem und zeigen Sie, dass er stets eine ein optimale Lösung findet.
2. Beweisen Sie: Ist  $T = (V, E')$  ein aufspannender Baum von einem Graphen  $G = (V, E)$  und ist  $e$  eine beliebige Kante aus  $E \setminus E'$ , dann enthält der Graph  $T + e$  genau einen Kreis.
3. Beweisen Sie: Ist  $T$  ein aufspannender Baum eines Graphen  $G$ , dann gibt es für jede Kante  $e \in E(G) \setminus E(T)$  eine Kante  $e' \in E(T)$ , so dass  $(T - e') + e$  wiederum ein aufspannender Baum von  $G$  ist.
4. Sei  $G$  ein zusammenhängender Graph mit einer Gewichtsfunktion  $w$  auf den Kanten. Beweisen Sie, dass der minimal aufspannende Baum von  $G$  eindeutig bestimmt ist, wenn  $w$  injektiv ist.
5. \*Sei  $G$  ein zusammenhängender Graph mit einer Gewichtsfunktion  $w$  auf den Kanten. Beweisen Sie, dass es für jeden minimal aufspannenden Baum  $T$  von  $G$  eine Anordnung der Kanten gibt, mit der der Greedy–Algorithmus den Baum  $T$  als Lösung ausgibt.
6. Seien  $w$  und  $w'$  zwei Gewichtsfunktionen auf den Kanten eines Graphen  $G = (V, E)$ . Angenommen, für je zwei Kanten  $e_1, e_2 \in E$  ist genau dann  $w(e_1) < w(e_2)$ , wenn  $w'(e_1) < w'(e_2)$  ist. Beweisen Sie, dass  $(V, E')$  genau dann ein minimal aufspannender Baum von  $G$  für die Gewichtsfunktion  $w$  ist, wenn  $(V, E')$  ein minimal aufspannender Baum von  $G$  für die Gewichtsfunktion  $w'$  ist. (Das bedeutet, dass die Lösung des Problems, einen minimal aufspannenden Baum zu finden, nur von der Reihenfolge der Kantengewichte abhängt.)
7. *Inf* Schauen Sie sich noch einmal die Diskussion von Algorithmus 5.3.2 im vorangegangenen Abschnitt an, um die Details für den Greedy–Algorithmus so zu regeln, dass seine Komplexität  $O((n+m) \log n)$  ist.
8. Betrachten Sie eine Menge  $V$  von  $n$  Punkten in der Ebene. Definieren Sie eine Gewichtsfunktion auf der Kantenmenge des vollständigen Graphen auf  $V$ : Das Gewicht einer Kante  $\{x, y\}$  ist der Abstand der Punkte  $x$  und  $y$ .
  - (a) \*Zeigen Sie, dass kein minimal aufspannender Baum dieses Netzwerks eine Ecke vom Grad 7 oder höher hat.

- (b) \*Zeigen Sie, dass es einen minimal aufspannenden Baum gibt, dessen Kanten nicht kreuzen.
9. \*Sei  $V$  eine Menge von  $n > 1$  Punkten im Einheitsquadrat in der Ebene und  $T$  ein minimal aufspannender Baum von  $V$  (d.h. von dem vollständigen Graphen mit den Abständen als Kantengewichte, wie in Aufgabe 8). Zeigen Sie, dass die Gesamtlänge der Kanten in  $T$  höchstens  $10\sqrt{n}$  ist. (Die Konstante 10 kann man noch wesentlich verbessern; die beste bekannte Abschätzung ist etwa  $1,4\sqrt{n} + O(1)$ .)
10. Sei  $G = (V, E)$  ein Graph und  $w$  eine nicht negative Gewichtsfunktion auf den Kanten.
- (a) \*Jede Menge  $E' \subseteq E$  paarweise disjunkter Kanten (d.h. ohne gemeinsame Ecken) heißt ein *Matching* in dem Graphen  $G$ . Bezeichnen Sie mit  $\nu_w(G)$  den maximal möglichen Wert von  $w(E')$  für ein Matching  $E' \subseteq E$ . Ein Greedy–Algorithmus zum Auffinden eines maximalen Matchings funktioniert ähnlich wie Kruskals Algorithmus für einen maximal aufspannenden Baum, d.h. er geht die Kanten eine nach der anderen in der Reihenfolge absteigender Gewichte durch und wählt eine Kante, wenn sie mit den anderen schon gewählten Kanten keine Ecke gemeinsam hat. Zeigen Sie, dass dieser Algorithmus immer ein Matching mit Gewicht mindestens  $\frac{1}{2}\nu_w(G)$  findet.
- (b) Zeigen Sie, dass die Schranke in (a) nicht verbessert werden kann; das heißt, für jede Konstante  $\alpha > \frac{1}{2}$  gibt es eine Eingabe, bei der der Greedy–Algorithmus ein Matching mit Gewicht kleiner als  $\alpha \nu_w(G)$  findet.
11. Eine Menge  $C \subseteq E$  in einem Graph  $G = (V, E)$  heißt eine (*Kanten–Bedeckung*), wenn jede Ecke  $v \in V$  in mindestens einer Kante  $e \in C$  enthalten ist (d.h. die Kanten aus  $C$  bedecken alle Ecken). Sie möchten mit einem Greedy–Algorithmus eine kleine Kantenbedeckung finden: Wenn es Kanten gibt, die zwei unbedeckte Ecken enthalten, dann wählen Sie eine beliebige solche, andernfalls wählen Sie irgendeine Kante, die eine noch unbedeckte Ecke bedeckt. Sie wiederholen diesen Vorgang solange, bis alle Ecken bedeckt sind. Zeigen Sie, dass die Anzahl der Kanten in einer so konstruierten Bedeckung
- (a) höchstens zwei mal so groß ist wie eine kleinste Bedeckung,
- (b) \*\*sogar höchstens  $\frac{3}{2}$  mal so groß ist wie eine kleinste Bedeckung.
12. \*Eine Menge  $D \subseteq V$  in einem Graph  $G = (V, E)$  heißt *dominierend*, wenn  $\bigcup_{e \in E: e \cap D \neq \emptyset} e = V$  (d.h. jede Ecke aus  $V$ , die nicht schon in  $D$  ist, ist zu einer Ecke aus  $D$  benachbart). Wir suchen auf Greedy–Art eine kleine dominierende Menge: Wir wählen stets eine Ecke, die mit möglichst vielen noch nicht versorgten Ecken benachbart ist. Zeigen Sie, dass es für jede Zahl  $C$  einen Graphen gibt, für den  $|D_G| \geq C|D_M|$  ist, wobei  $D_G$  eine dominierende Menge ist, die

der Greedy–Algorithmus ausgewählt hat, und  $D_M$  eine dominierende Menge minimaler Größe. (Beginnen Sie, indem Sie Beispiele für kleine Werte von  $C$  finden.)

## 5.5 Die Algorithmen von Jarník und Borůvka

Was wir als „Jarník–Algorithmus“ bezeichnen ist besser bekannt unter dem Namen „Algorithmus von Prim“. Während der Artikel von Prim aber von 1957 datiert, hat Jarník den gleichen Algorithmus bereits 1930 elegant und präzise beschrieben (womit er die Arbeit von Borůvka fortsetzte, der 1928 den ersten dokumentierten Algorithmus zum Finden eines minimal aufspannenden Baums publiziert hat), und so halten wir es für angemessener, dem ersten Erfinder die Ehre der Namensgebung zuzugestehen.

Heutzutage kann man den Jarník–Algorithmus als eine einfache Erweiterung von Algorithmus 5.3.5 ansehen.

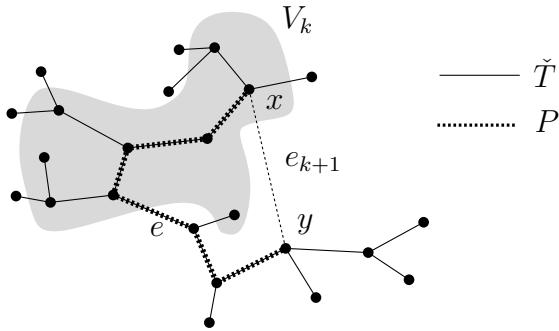
**5.5.1 Algorithmus (Jarník–Algorithmus).** Gehe wie in Algorithmus 5.3.5 vor und wähle als jeweils nächste Kante  $e_i$  eine Kante von kleinstmöglichem Gewicht aus der Menge  $\{\{x,y\} \in E(G) : x \in V_{i-1}, y \notin V_{i-1}\}$ .

**5.5.2 Hilfssatz (Korrektheit des Jarník–Algorithmus).** Der Algorithmus von Jarník findet einen minimal aufspannenden Baum in jedem zusammenhängenden Netzwerk.

*Beweis.* Sei  $T = (V, E')$  der vom Jarník–Algorithmus konstruierte aufspannende Baum, die Kanten in  $E'$  seien nummeriert von  $e_1$  bis  $e_{n-1}$  in der Reihenfolge ihres Hinzufügens zu  $T$ . Wir führen den Beweis indirekt (d.h. einen Widerspruchsbeweis): Angenommen,  $T$  ist kein minimal aufspannender Baum.

Sei  $T'$  ein minimal aufspannender Baum. Sei  $k(T')$  derjenige Index  $k$ , für den die Kanten  $e_1, e_2, \dots, e_k$  alle zu  $E(T')$  gehören, aber  $e_{k+1} \notin E(T')$  ist. Wir wählen unter allen minimal aufspannenden Bäumen einen Baum  $\check{T} = (V, \check{E})$  mit möglichst großem  $k = k(\check{T})$  aus.

Sehen wir uns nun den Moment genauer an, in dem der Algorithmus die Kante  $e_{k+1}$  zu  $T$  hinzufügt. Sei  $T_k = (V_k, E_k)$  der Baum, den die Kanten  $e_1, \dots, e_k$  aufspannen. Dann hat  $e_{k+1}$  die Form  $\{x, y\}$  mit  $x \in V(T_k)$  und  $y \notin V(T_k)$ . Der Graph  $\check{T} + e_{k+1}$  enthält einen Kreis  $C$  (weil er zusammenhängend ist und mehr als  $n - 1$  Kanten hat), und  $C$  enthält die Kante  $e_{k+1}$  (siehe auch Aufgabe 5.4.2).



**Abb. 5.1** Zum Korrektheitsbeweis des Jarník–Algorithmus.

Der Kreis  $C$  besteht aus der Kante  $e_{k+1} = \{x, y\}$  plus einem Weg  $P$ , der die Ecken  $x$  und  $y$  im aufspannenden Baum  $\check{T}$  verbindet. Mindestens eine Kante auf dem Weg  $P$  hat ein Ende in der Menge  $V_k$  und das andere Ende außerhalb von  $V_k$ . Sei  $e$  eine solche Kante. Offensichtlich ist  $e \neq e_{k+1}$ , und außerdem wissen wir, dass  $e \in \check{E}$  ist und  $e_{k+1} \notin \check{E}$ ; die Situation sieht ungefähr wie in Abb. 5.1 aus. Die Kanten  $e$  und  $e_{k+1}$  verbinden jede eine Ecke aus  $V_k$  mit einer Ecke, die nicht in  $V_k$  liegt, und aus der Kantenauswahlregel des Algorithmus folgt, dass  $w(e_{k+1}) \leq w(e)$ .

Wir betrachten nun den Graphen  $T' = (\check{T} + e_{k+1}) - e$ . Dieser Graph hat  $n - 1$  Kanten und ist, wie man leicht nachprüft, zusammenhängend; folglich ist er ein aufspannender Baum. Es ist  $w(E(T')) = w(\check{E}) - w(e) + w(e_{k+1}) \leq w(\check{E})$ , und deshalb ist auch  $T'$  ein minimal aufspannender Baum, jedoch mit  $k(T') > k(\check{T})$ . Dieser Widerspruch zu der Wahl von  $\check{T}$  beweist den Hilfssatz 5.5.2.

*Warnung.* Dies ist ein weiterer Beweis, dem eine gewisse Robustheit abgeht: Wenn man einen der Schritte etwas anders ansetzt, dann muss man schon Glück haben, damit der Beweis trotzdem funktioniert.  $\square$

**Der Algorithmus von Borůvka.** Der erste, der einen Algorithmus für minimal aufspannende Bäume angegeben hat, war Borůvka. Wie so oft in den Wissenschaften war die erste Idee nicht die einfachste — sowohl Kruskals als auch (ganz besonders) Jarníks Algorithmus sind konzeptuell einfacher. Und doch war es Borůvkas Algorithmus, der erst kürzlich als Startpunkt für den theoretisch schnellsten bekannten Algorithmus für minimal aufspannende Bäume diente (Karger, Klein und Tarjan [43]). Der neue schnelle Algorithmus ist ziemlich kompliziert

und benutzt einige weitere Ideen (die wir hier nicht weiter verfolgen werden) um die Berechnung zu beschleunigen.

**5.5.3 Algorithmus (Der Borůvka–Algorithmus).** Die Eingabe ist ein Graph  $G = (V, E)$  mit Kantengewichtsfunktion  $w$ . Wir müssen davon ausgehen, dass verschiedene Kanten verschiedene Gewichte erhalten, dass die Gewichtsfunktion also injektiv ist. Diese Voraussetzung ist nicht sonderlich restriktiv, denn man kann jede Gewichtsfunktion (auf einer endlichen Menge) „injektiv machen“, ganz einfach indem man die Gewichte um ganz kleine Beträge ändert, wodurch sich das Gewicht eines minimal aufspannenden Baums auch nur um einen ganz kleinen Betrag ändert. (Alternativ kann man den Algorithmus so abwandeln, dass er mit beliebigen Gewichten funktioniert, indem man eine einfache Regel hinzufügt; siehe Aufgabe 6 unten.)

Dieser Algorithmus konstruiert Schritt für Schritt Kantenmengen  $E_0, E_1, \dots \subseteq E$ , er beginnt mit  $E_0 = \emptyset$ .

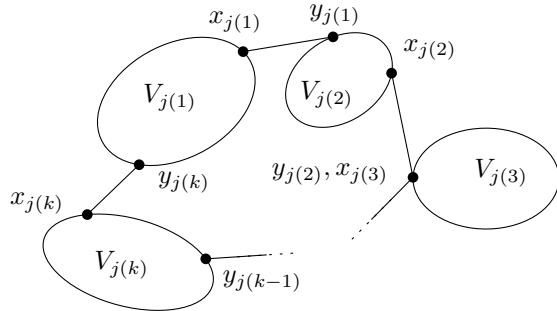
Angenommen, die Menge  $E_{i-1}$  ist schon berechnet;  $(V_1, \dots, V_t)$  sei die Partition der Eckenmenge, die durch die Komponenten des Graphen  $(V, E_{i-1})$  gegeben ist. (Um ganz genau zu sein, müsste diese Partition auch noch einen Index  $i$  haben, weil sie in jedem Schritt eine andere ist. Wir lassen diesen Index  $i$  hier um der Übersicht willen weg.) Für jede Menge  $V_j$  von dieser Partition bestimmen wir die Kante  $e_j = \{x_j, y_j\}$  (mit  $x_j \in V_j, y_j \notin V_j$ ), deren Gewicht minimal ist unter allen Kanten der Form  $\{x, y\}$ ,  $x \in V_j, y \in V \setminus V_j$  (es kann passieren, dass  $e_j = e_{j'}$  ist für  $j \neq j'$ ). Wir setzen  $E_i = E_{i-1} \cup \{e_1, \dots, e_t\}$ . Der Algorithmus endet, wenn der Graph  $(V, E_i)$  eine Komponente hat.

Man könnte diesen Algorithmus als „Blasen–Algorithmus“ bezeichnen. Der Graph  $G$  wird durch „Blasen“ überdeckt, und in jedem Schritt wird eine Blase mit der nächsten benachbarten vereinigt.

Den Korrektheitsbeweis dieses Algorithmus werden wir nicht führen (das dürfen Sie in einer der Aufgaben nachholen). Wir zeigen nur, dass der konstruierte Graph keinen Kreis hat (was, anders als bei den anderen Algorithmen, nicht ganz offensichtlich ist). Angenommen, in Schritt  $i$  entsteht ein Kreis. Das bedeutet, es gibt paarweise verschiedene Indizes  $j(1), j(2), \dots, j(k)$ , für die

$$\begin{array}{ll} x_{j(1)} \in V_{j(1)}, & y_{j(1)} \in V_{j(2)} \\ x_{j(2)} \in V_{j(2)}, & y_{j(2)} \in V_{j(3)} \\ \vdots & \\ x_{j(k-1)} \in V_{j(k-1)}, & y_{j(k-1)} \in V_{j(k)} \\ x_{j(k)} \in V_{j(k)}, & y_{j(k)} \in V_{j(1)}. \end{array}$$

In einem Bild sieht das etwa so aus:

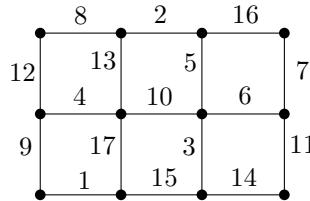


Weil verschiedene Kanten verschiedene Gewichte haben, hat die Kante  $e_{j(\ell)}$  stets das kleinste Gewicht unter allen Kanten, die aus der Komponente  $V_{j(\ell)}$  herausführen, insbesondere gilt dann

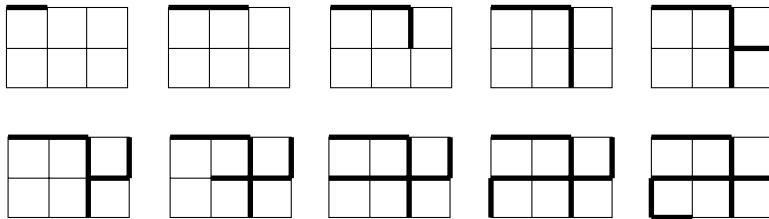
$$w(e_{j(1)}) < w(e_{j(2)}) < \dots < w(e_{j(k)}) < w(e_{j(1)}).$$

Das kann aber nicht sein, also findet der Boruvka–Algorithmus einen aufspannenden Baum von  $G$ . Zu zeigen, dass er einen minimal aufspannenden Baum findet, kostet etwas mehr Mühe.  $\square$

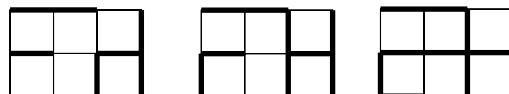
**Beispiel.** Betrachten Sie das folgende Netzwerk (die Zahlen neben den Kanten sind die Gewichte):



Der Jarník–Algorithmus verläuft folgendermaßen, wenn er in der oberen linken Ecke startet:



Kruskals Algorithmus benötigt 17 Schritte (doch nur in zehn von ihnen wird eine neue Kante hinzugefügt). Der Boruvka–Algorithmus hingegen ist recht kurz:



Aber in jedem Schritt steckt viel mehr Arbeit.

## Aufgaben

1. (Allgemeiner Algorithmus für aufspannende Bäume) Betrachten Sie den folgenden Algorithmus zur Bestimmung eines minimal aufspannenden Baums. Die Eingabe ist ein zusammenhängender Graph  $G = (V, E)$  mit Gewichtsfunktion  $w$ . Setzen Sie  $E_0 = \emptyset$ . Wenn  $E_{i-1}$  schon definiert ist, wählen Sie eine beliebige Komponente  $V_i$  des Graphen  $(V, E_{i-1})$ , nehmen Sie eine Kante  $e_i$  von minimalem Gewicht unter den Kanten mit einer Ecke in  $V_i$  und der anderen Ecke nicht in  $V_i$ , und setzen Sie  $E_i = E_{i-1} \cup \{e_i\}$ . Beweisen Sie, dass  $(V, E_{n-1})$  ein minimal aufspannender Baum ist. (Orientieren Sie sich am Korrektheitsbeweis für den Algorithmus von Jarník.)

Zeigen Sie, dass daraus die Korrektheit sowohl von Kruskals als auch von Jarníks Algorithmus folgt.

2. („Umgekehrter“ Greedy–Algorithmus) Betrachten Sie folgenden Algorithmus zur Bestimmung eines minimal aufspannenden Baums. Die Eingabe ist ein zusammenhängender Graph  $G = (V, E)$  mit Gewichtsfunktion  $w$ . Ordnen Sie die Kanten  $e_1, \dots, e_m$  so, dass  $w(e_1) \geq \dots \geq w(e_m)$ . Setzen Sie  $E_0 = E$  und

$$E_i = \begin{cases} E_{i-1} \setminus \{e_i\} & \text{wenn der Graph } (V, E_{i-1} \setminus \{e_i\}) \\ & \text{zusammenhängend ist,} \\ E_i & \text{sonst.} \end{cases}$$

Beweisen Sie, dass  $(V, E_m)$  ein minimal aufspannender Baum von  $G$  ist.

3. \*Weisen Sie die Korrektheit des Borůvka–Algorithmus nach.
4. <sup>Inf</sup> Füllen Sie die Details des Jarník–Algorithmus so aus, dass seine Komplexität  $O((m+n)\log n)$  ist (Sie sollten sich ein wenig mit Datenstrukturen auskennen).
5. (a) Beweisen Sie, dass der Borůvka–Algorithmus höchstens  $O(\log n)$  Phasen durchläuft, d.h. der Graph  $(V, E_i)$  ist schon für ein  $i = O(\log n)$  zusammenhängend.  
 (b) <sup>Inf</sup> Füllen Sie die Details von Borůvkas Algorithmus so aus, dass seine Komplexität höchstens  $O((m+n)\log n)$  ist.
6. (Tie-breaking in Borůvkas Algorithmus) Wenn eine beliebige Gewichtsfunktion auf den Kanten eines Graphen  $G = (V, E)$  gegeben ist, dann wählen wir (ein für alle mal) eine beliebige Ordnung  $e_1, e_2, \dots, e_m$  der Kanten und definieren  $e_i \triangleleft e_j$ , wenn entweder  $w(e_i) < w(e_j)$  ist oder wenn  $w(e_i) = w(e_j)$  und zugleich  $i \leq j$ .  
 (a) Formulieren Sie den Borůvka–Algorithmus mit der (linearen) Kan tenordnung  $\triangleleft$  an Stelle der einfachen (partiellen) Ordnung  $\leq$  nach Gewicht.

- (b) Weisen Sie nach, dass der Algorithmus aus (a) einen aufspannenden Baum von  $G$  berechnet.
- (c) Beweisen Sie, dass der Algorithmus aus (a) einen minimal aufspannenden Baum von  $G$  (bezüglich der Gewichtsfunktion  $w$ ) berechnet (passen Sie den Beweis aus Aufgabe 3 entsprechend an).



# 6

## Graphen in der Ebene

---

### 6.1 Zeichnungen in die Ebene und andere Flächen

Oft ist es von Vorteil, Graphen zu zeichnen. Wie Sie sehen, sind die meisten Graphen in diesem Buch durch eine Zeichnung angegeben (und nicht etwa als Liste der Ecken und Kanten). Doch bisher haben wir keine Eigenschaften von Graphen studiert, die mit ihren Zeichnungen zu tun haben. In diesem Kapitel wollen wir die Zeichnungen selbst genauer untersuchen. Unser Hauptinteresse gilt dabei jenen Graphen, die so in die Ebene gezeichnet werden können, dass sich keine Kanten kreuzen. Solche Graphen nennt man *eben* oder *planar*.

Aus den zahlreichen Bildern auf den vorangegangenen Seiten und aus der informellen Definition aus Abschnitt 4.1 haben Sie wahrscheinlich schon eine recht gute Vorstellung davon, was mit der Zeichnung eines Graphen gemeint ist. So eine Intuition ist ausreichend, wenn wir zeigen möchten, dass ein bestimmter Graph eben ist — wir müssen dann ja nur eine kreuzungsfreie Zeichnung angeben. Wenn wir aber einen wirklichen Beweis geben wollen, dass ein bestimmter Graph *nicht* eben ist, dann kommen wir ohne eine mathematische Definition von „Zeichnung“ nicht aus. Die gesamte moderne Mathematik fußt auf einigen wenigen grundlegenden Begriffen und Axiomen der Mengenlehre — zumindest versucht die große Mehrheit der Mathematiker sicherzustellen, dass es so ist. So modelliert man z.B. eine „Ebene“ als das kartesische Produkt  $\mathbb{R} \times \mathbb{R}$ . Jede reelle Zahl kann man als eine gewisse Teilmenge der rationalen Zahlen definieren, die rationalen Zahlen kann man aus den natürlichen Zahlen aufbauen, und schließlich fasst man die natürlichen Zahlen als gewisse Mengen auf, die man aus der leeren Menge konstruiert. (In der „normalen“ Mathematik kommt das selten zum Tragen, aber wenn Sie in ein Buch über Grundlagen der Mathematik schauen, dann werden Sie das dort so finden.)

Um formal definieren zu können, was wir unter einer Zeichnung verstehen wollen, beginnen wir so: Eine *einfache Kurve* ist eine Teilmenge  $\alpha$  der Ebene von der Form  $\alpha = \gamma([0, 1]) = \{\gamma(x) : x \in [0, 1]\}$ ,

wobei  $\gamma: [0, 1] \rightarrow \mathbb{R}^2$  eine injektive stetige Abbildung aus dem abgeschlossenen Intervall  $[0, 1]$  in die Ebene ist. Die Punkte  $\gamma(0)$  und  $\gamma(1)$  heißen die *Endpunkte* der einfachen Kurve  $\alpha$ . (Wenn  $\gamma$  nicht injektiv ist, dann schneidet  $\alpha$  sich selbst und die Kurve heißt nicht mehr einfach.)

So furchteinflößend diese Definition auf den ersten Blick aussehen mag, sie ist doch recht nah an der intuitiven Idee von einer durchgehenden gezeichneten Linie. Das Intervall  $[0, 1]$  darf man sich als den Zeitabschnitt vorstellen, in dem wir die Linie vom Punkt  $\gamma(0)$  zum Punkt  $\gamma(1)$  ziehen. Dann ist  $\gamma(t)$  die Position der Bleistiftspitze zur Zeit  $t$ . Die Stetigkeit der Abbildung  $\gamma$  bedeutet, dass wir den Stift nicht absetzen, und die Injektivität sagt, dass die Linie sich nicht selbst schneidet.

**6.1.1 Definition.** Mit einer Zeichnung oder einer Einbettung eines Graphen  $G = (V, E)$  meinen wir eine Zuordnung, die jeder Ecke  $v$  des Graphen  $G$  einen Punkt  $b(v)$  in der Ebene zuordnet und jeder Kante  $e = \{v, v'\} \in E$  eine einfache Kurve  $\alpha(e)$  in der Ebene mit Endpunkten  $b(v)$  und  $b(v')$ . Wir verlangen, dass die Abbildung  $b$  injektiv ist (verschiedene Ecken werden durch verschiedene Punkte in der Ebene repräsentiert), und dass keiner der Punkte  $b(v)$  auf einer der Kurven  $\alpha(e)$  liegt, außer wenn  $v$  eine Endecke der Kante  $e$  ist. Ein Graph zusammen mit einer Einbettung heißt ein topologischer Graph<sup>1</sup> oder auch eingebetteter Graph.

Eine Zeichnung eines Graphen  $G$ , in der sich die zu zwei verschiedenen Kanten gehörenden Kurven nur in Endpunkten treffen oder gar nicht, wird ebene Zeichnung genannt. Ein Graph  $G$  heißt eben oder planar, wenn er mindestens eine ebene Zeichnung hat.

Diese formale Definition der Zeichnung eines Graphen haben wir gegeben, um Ihnen vorzuführen, dass sich auch so ein anschaulicher Begriff wie „Zeichnung“ elementar in den logischen Aufbau der Mathematik fügt. Wir werden die weitere Theorie der ebenen Graphen jedoch nicht so streng fortführen. Dafür müssten wir Begriffe und Resultate über ebene einfache Kurven aus der *Topologie* verwenden, und wenn wir alles lückenlos beweisen wollten, bräuchten wir schon eine erstaunlich komplizierte Maschinerie. Außerdem sind die Beweise von Aussagen, die „anschaulich klar“ sind, oft überraschend schwierig. Aus diesen Gründen werden wir uns im Folgenden auf unsere (auf Ihre!) Intuition verlassen, und wir werden Sie an der einen oder anderen Stelle bitten, eine (wahre!) Aussage ohne Beweis zu akzeptieren. Eine strenge Behandlung des Themas finden Sie z.B. in dem Buch von Mohar

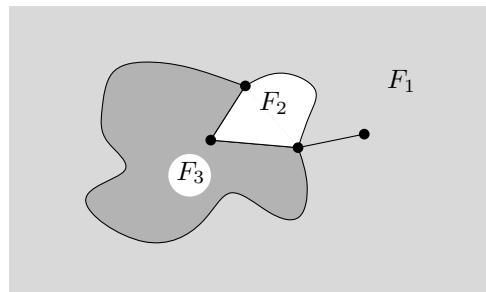
---

<sup>1</sup>Im Englischen bezeichnet man einen ebenen Graph zusammen mit einer Zeichnung in der Ebene auch als *plane Graph*.

und Thomassen [26]. Glücklicherweise führt einen die Intuition auf dem Gebiet der Graphenzeichnungen nur selten in die Irre.

Eine ebene Zeichnung ist eine besonders günstige Form der Visualisierung eines Graphen (Kantenkreuzungen in einer nicht ebenen Zeichnung könnte man fälschlich für Ecken halten), und in einigen Anwendungen, in denen die Zeichnung eine physische Bedeutung hat, können Kantenkreuzungen sogar unzulässig sein (etwa bei Schaltkreisen, die auf eine Seite einer Platine geätzt werden sollen).

**Länder in der Zeichnung eines Graphen.** Sei  $G = (V, E)$  ein topologischer ebener Graph, also ein ebener Graph mit einer gegebenen ebenen Einbettung. Betrachten Sie die Menge aller Punkte in der Ebene, die auf keiner der Kurven liegen. Diese Menge besteht aus endlich vielen zusammenhängenden Gebieten (wir könnten das Papier entlang der gezeichneten Linien in Teile schneiden):



(Wir nennen eine Menge  $A \subseteq \mathbb{R}^2$  *zusammenhängend*, wenn es zu je zwei Punkten  $x, y \in A$  immer eine Kurve  $\alpha \subseteq A$  mit Endpunkten  $x$  und  $y$  gibt. „Zusammenhang“<sup>2</sup> ist ein Beispiel einer topologischen Begriffsbildung.) Diese Gebiete nennen wir die *Länder*<sup>3</sup> unseres topologischen ebenen Graphen. Das nach Außen unbegrenzte Gebiet,

---

<sup>2</sup>Was wir hier eine „zusammenhängende Menge“ nennen, heißt in der Topologie meist eine *wegzusammenhängende Menge*. Eine zusammenhängende Menge wird wie folgt definiert. Eine Menge  $A \subseteq \mathbb{R}^2$  ist zusammenhängend, wenn keine zwei disjunkten offenen Mengen  $A_1, A_2 \subseteq \mathbb{R}^2$  existieren, so dass  $A \subseteq A_1 \cup A_2$  und  $A_1 \cap A \neq \emptyset \neq A_2 \cap A$ . Für die in diesem Kapitel betrachteten Mengen wie die Länder eines Graphen macht es keinen Unterschied, welche der zwei Versionen wir verwenden, und so bleiben wir bei dem kürzeren Namen.

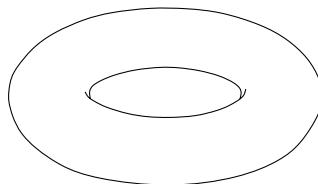
<sup>3</sup>Dieser Name kommt von der Interpretation des gezeichneten Graphen als Landkarte, siehe auch Abschnitt 6.4. Auf englisch heißen die Länder meist *faces*, was mit der Interpretation des Graphen als Gerüst eines geometrischen Körpers zu tun hat (siehe Abschnitt 6.3).

wie  $F_1$  in dem Bild, heißt das *äußere Land* in der Zeichnung, und alle anderen Länder heißen *innere Länder*.

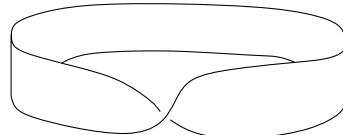
Wir sollten betonen, dass Länder nur *bezüglich einer gegebenen ebenen Zeichnung* definiert sind. Für nicht ebene Zeichnungen sind Länder in der Regel nicht definiert, und wenn man von den Ländern eines ebenen Graphen spricht, sollte klar sein, auf welche Zeichnung man sich bezieht.

**Zeichnungen auf anderen Flächen.** Man kann Graphen auch in andere Flächen als die Ebene einbetten. Wir geben ein paar Beispiele interessanter Flächen.

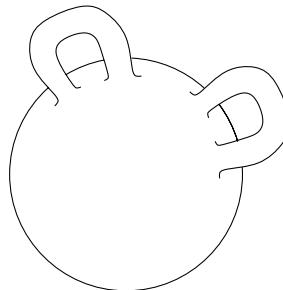
Die Sphäre, also die Oberfläche einer Kugel, ist allgemein bekannt. Die Oberfläche von einem Autoreifen (oder Spritzkuchen) heißt *Torus*:



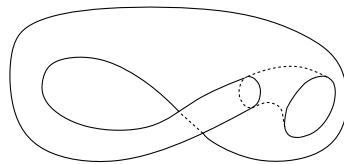
Wenn man bei einem langen Streifen Papier das eine Ende um 180 Grad dreht und dann die beiden Enden aneinanderklebt, dann erhält man eine interessante Fläche, das *Möbiusband*:



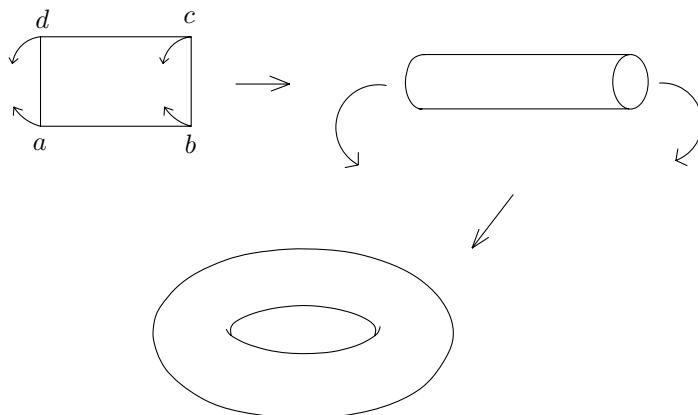
Weitere Beispiele sind eine Sphäre mit zwei „Henkeln“:



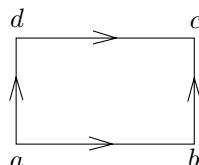
(wenn man sie ein wenig knetet, ohne die Henkel aufzureißen oder neue Löcher hinzuzufügen, kann man sie in die Form einer 8 bringen) sowie die so genannte *Kleinsche Flasche*:



Jede dieser Flächen kann man aus einem ebenen Polygon (d.h. Viereck) durch „Verkleben“ von Außenkanten und einer anschließenden Deformation herstellen. In den obigen Beispielen würden wir außer bei der Sphäre mit zwei Henkeln immer mit einem Rechteck beginnen, dessen Seiten wir auf geeignete Weise verkleben. Das Möbiusband haben wir auf genau diese Art eingeführt, und diese Methode bildet eine mögliche Basis für eine exakte Definition solcher Flächen. Beispielsweise erhält man den Torus so:



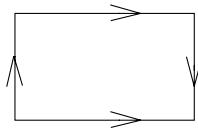
Man identifiziert gegenüberliegende Seiten des Rechtecks  $abcd$  derart, dass die Seite  $ab$  an die Seite  $dc$  kommt und die Seite  $ad$  an die Seite  $bc$ . Die Orientierung, in der die Seiten aneinandergeklebt werden, kennzeichnet man gewöhnlich mit Pfeilen. Die Pfeile in dem folgenden Bild deuten an, dass beim Verkleben der Seiten  $ad$  und  $bc$  der Punkt  $a$  auf den Punkt  $b$  zu liegen kommt und  $d$  auf  $c$ .



Das folgende Bild zeigt noch einmal die „Bastelanleitung“ für das Möbiusband:



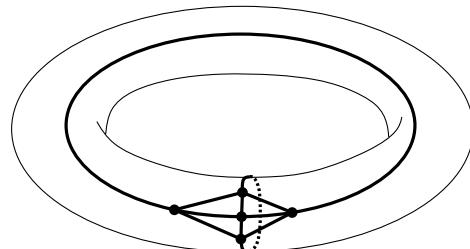
(Wir identifizieren nur die zwei mit Pfeilen gekennzeichneten Seiten derart, dass die Pfeile in die gleiche Richtung zeigen.) Die Kleinsche Flasche wird nach folgendem Muster hergestellt:



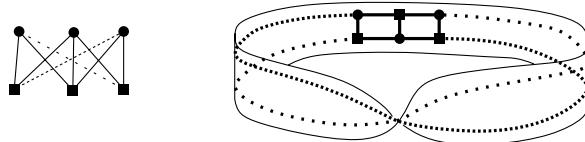
Diese letzte Anleitung dürfen Sie aber nicht zu wörtlich nehmen: Auch wenn Sie dehnbare Stoff benutzen, so werden Sie es doch nicht fertigbringen, eine Kleinsche Flasche zu schneidern, weil die Kleinsche Flasche im dreidimensionalen Euklidischen Raum nicht realisierbar ist (es geht nur, wenn das Rechteck sich selbst durchdringen darf, so wie in dem Bild von der Kleinschen Flasche). Dennoch ist diese Definition der Kleinschen Flasche mathematisch sinnvoll, im  $\mathbb{R}^4$  etwa ist die Konstruktion ohne weiteres durchführbar.

Es gibt einen allgemeinen Satz, dass jede geschlossene Fläche (die keine „Randpunkte“ hat und die in keine Richtung ins Unendliche „wegläuft“; gelehrter klingt der Name „kompakte 2-Mannigfaltigkeit ohne Rand“) durch geeignetes Verkleben und Verformen eines regulären konvexen Polygons aufgebaut werden kann. Wenn die resultierende Fläche zweiseitig ist (das Möbiusband und die Kleinsche Flasche haben nur eine Seite!), dann kann sie stetig in eine Sphäre mit endlich vielen Henkeln deformiert werden. Die Grundlagen dieser Theorie sowie eine Anzahl ähnlicher Themen werden in dem Buch von Stillwell [31] wunderbar erklärt.

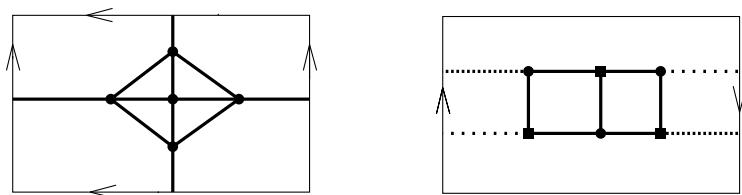
Man kann Graphen danach klassifizieren, auf welche Flächen sie gezeichnet werden können. Wie wir im nächsten Abschnitt zeigen werden, sind der  $K_5$ , der vollständige Graph auf 5 Ecken, und  $K_{3,3}$ , der vollständige bipartite Graph auf 3 + 3 Ecken, beide nicht eben. Aber der  $K_5$  lässt sich unter anderem auf den Torus zeichnen:



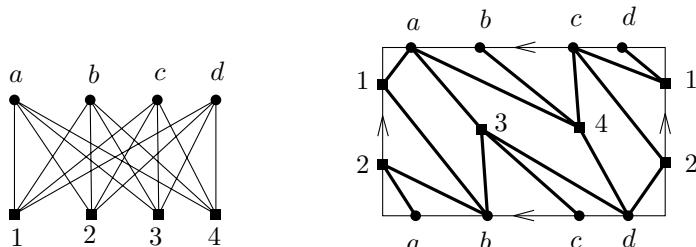
und  $K_{3,3}$  auf das Möbiusband:



Wie oben erklärt, erhält man diese Flächen durch geschicktes Verkleben der Seiten eines Rechtecks. Um unsere räumliche Vorstellung nicht allzu sehr zu strapazieren, können wir die Flächen entlang der Verklebungen wieder aufschneiden und erhalten so eine ebene Zeichnung, in der manche Kanten über die Seiten des Rechtecks „springen“. Für die beiden obigen Zeichnungen sieht das so aus:



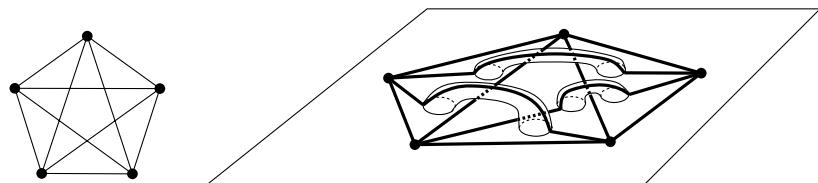
Übrigens kann man sogar den  $K_{4,4}$  auf den Torus zeichnen:



(Auch mit  $K_7$  geht das; siehe Aufgabe 2.) Allgemein gilt

**6.1.2 Hilfssatz.** Jeder Graph kann kreuzungsfrei in eine Sphäre mit genügend vielen Henkeln eingebettet werden.

*Informeller Beweis.* (Für einen formalen Beweis dieses Hilfssatzes fehlt uns die genaue Definition einer Sphäre mit Henkeln.) Wir zeichnen den gegebenen Graphen  $G = (V, E)$  auf die Sphäre, möglicherweise mit kreuzenden Kanten. Seien  $e_1, e_2, \dots, e_n$  alle Kanten, die eine andere kreuzen. Für jede Kante  $e_i$  fügen wir einen Henkel als „Brücke“ hinzu, so dass die Henkel alle disjunkt sind und sich keine Kanten mehr kreuzen:

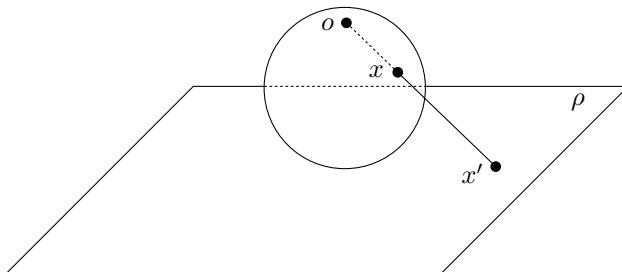


Weil der Graph nur endlich viele Kanten hat, ist es einfach, solche Henkel zu finden.  $\square$

Deshalb ist die folgende Definition sinnvoll.

**6.1.3 Definition.** Die kleinstmögliche Anzahl von Henkeln, deren Aufsetzen auf die Sphäre es ermöglicht, dass ein Graph  $G$  in die so entstandene Fläche kreuzungsfrei eingebettet werden kann, heißt das Geschlecht<sup>4</sup> des Graphen  $G$ .

Zum Abschluss dieses Abschnitts wollen wir noch zeigen, dass die ebenen Graphen genau die Graphen vom Geschlecht 0 sind, also diejenigen, die man auf die Sphäre zeichnen kann. Mit Hilfe der *stereographischen Projektion* ist das sehr leicht einzusehen. Wir legen die Sphäre im dreidimensionalen Raum auf die Zeichenebene  $\rho$ , so dass sich die beiden Flächen in einem Punkt berühren. Mit  $o$  bezeichnen wir den „Nordpol“, den Punkt der Sphäre, der von  $\rho$  den größten Abstand hat:



Die stereographische Projektion ist nun eine bijektive Abbildung zwischen der Sphäre ohne den Nordpol und der Ebene  $\rho$ ; sie bildet einen Punkt  $x \neq o$  der Sphäre auf den Punkt  $x'$  in der Ebene ab, wobei  $x'$  der Schnittpunkt der Gerade  $ox$  mit der Ebene  $\rho$  ist. (Für den Punkt  $o$  ist die Projektion nicht definiert.) Wenn eine kreuzungsfreie Zeichnung eines Graphen  $G$  auf die Sphäre gegeben ist, in der der Punkt  $o$  auf keiner Kante liegt, (das dürfen wir annehmen, weil wir den Nordpol  $o$  willkürlich festlegen können), dann liefert die stereographische Projektion eine ebene Zeichnung von  $G$ . Umgekehrt erhalten wir aus einer

---

<sup>4</sup>Der Begriff Geschlecht wurde ursprünglich für Flächen geprägt. Das Geschlecht einer Sphäre mit Henkeln ist die Anzahl der aufgesetzten Henkel. Interessanterweise wurden zweidimensionale Flächen zuerst in Verbindung mit algebraischen Gleichungen systematisch studiert. Die Menge aller komplexen Lösungen einer Polynomgleichung in zwei Variablen ist typischerweise eine zweidimensionale Fläche, deren Geschlecht verschiedene Eigenschaften der Gleichung bestimmt. Das Gebiet, das sich in diesem Geist mit algebraischen Gleichungen beschäftigt, heißt *algebraische Geometrie* (Cox, Little und O’Shea [19] ist eine hübsche Einführung in das Thema).

ebenen Einbettung durch die inverse Projektion eine Zeichnung auf die Sphäre.

## Aufgaben

1. Finden Sie
  - (a) einen ebenen Graphen, dessen Ecken alle Grad 5 haben,
  - (b) \*zusammenhängende Graphen wie in (a) mit beliebig vielen Ecken.
2. (a) Überprüfen Sie, dass das Bild mit der Zeichnung des  $K_{4,4}$  auf den Torus tatsächlich ein  $K_{4,4}$  ist.  
 (b) Finden Sie eine Zeichnung des  $K_6$  auf den Torus.  
 (c) \*Zeichnen Sie  $K_7$  auf den Torus.
3. \*Sei  $G$  ein ebener Eulerscher Graph. Zeigen Sie: Zu jeder ebenen Zeichnung von  $G$  gibt es eine geschlossene Euler–Tour von  $G$ , die in der betrachteten Zeichnung an keiner Stelle sich selbst kreuzt. (Wenn  $G$  kein Kreis ist, wird es immer Stellen geben, wo sich die Tour selbst trifft, aber sie soll dann nicht kreuzen.)
4. Überlegen Sie, wie eine Definition einer geschlossenen zweidimensionalen Fläche aussehen könnte. Schauen Sie dann in einem Topologiebuch nach, wie die Definition dort steht.

## 6.2 Kreise in ebenen Graphen

In diesem Abschnitt wollen wir kombinatorische Eigenschaften ebenen Graphen untersuchen. Dabei wird sich unter anderem herausstellen, dass man durch rein kombinatorische Betrachtungen, d.h. ohne auf topologische Eigenschaften der Ebene zurückzugreifen oder geometrische Intuition über Graphenzeichnungen zu verwenden, ebene Graphen von nicht ebenen unterscheiden kann. (Man könnte „ebener Graph“ also definieren, ohne zu wissen, was eine Ebene ist!)

Wenn es möglich sein soll, die geometrische Definition ebener Graphen durch eine kombinatorische Definition zu ersetzen, dann muss es eine Eigenschaft der Ebene geben, die Geometrie und Kombinatorik verbindet. Solch eine Eigenschaft drückt sich im Jordanschen Kurvensatz aus. Zuerst eine Definition: Eine *Jordankurve*<sup>5</sup> ist eine geschlossene Kurve ohne Selbstüberschneidungen. Etwas formaler:

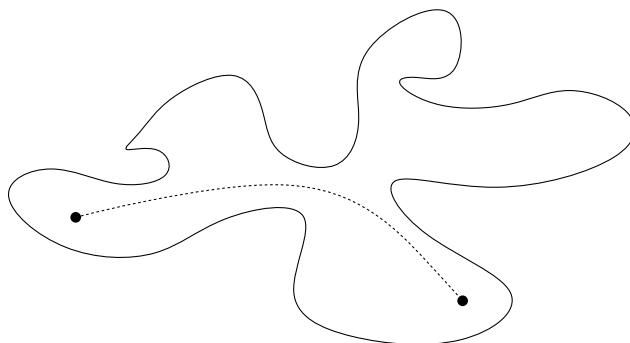
---

<sup>5</sup>Ein anderer gebräuchlicher Name für dieses Objekt ist eine *einfache geschlossene Kurve*.

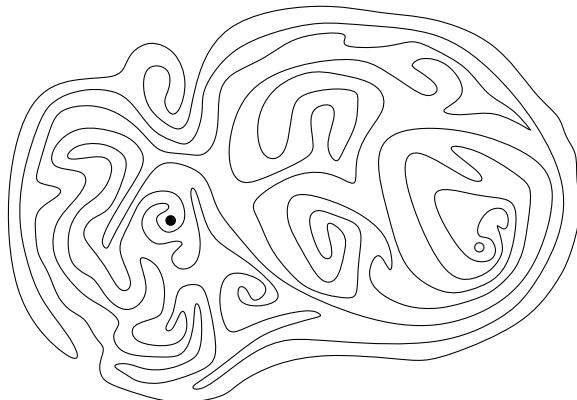
Eine Jordankurve ist eine einfache Kurve, deren Endpunkte zusammenfallen, d.h. ein stetiges Bild des Intervalls  $[0, 1]$  unter einer Abbildung  $f$ , die injektiv ist bis auf  $f(0) = f(1)$ .

**6.2.1 Satz (Jordanscher Kurvensatz).** Eine Jordankurve  $k$  teilt die Ebene in genau zwei zusammenhängende Teile, das „Innere“ und das „Äußere“ von  $k$ , und  $k$  ist der Rand sowohl des Inneren als auch des Äußeren. (Das Innere und das Äußere nennen wir die Gebiete von  $k$ .) Anders ausgedrückt: Wir definieren auf der Menge  $\mathbb{R}^2 \setminus k$  eine Relation  $\approx$ : Es sei genau dann  $x \approx y$ , wenn  $x$  und  $y$  durch eine von  $k$  disjunkte Kurve verbunden werden können. Dann ist  $\approx$  eine Äquivalenzrelation mit zwei Äquivalenzklassen, von denen eine beschränkt ist und die andere unbeschränkt.

Zuerst denkt man, dass dieser Satz intuitiv klar ist; sein Beweis ist aber keineswegs einfach, auch wenn er kürzlich von Thomassen [50] wesentlich vereinfacht wurde. Für einige Jordankurven in der Ebene ist die Behauptung offensichtlich wahr,



doch für andere ist sie schon weniger klar (suchen Sie doch eine Kurve, die die Punkte  $\circ$  und  $\bullet$  miteinander verbindet und die Jordankurve nicht schneidet):



Wenn Sie nun immer noch der Meinung sind, dass der Jordansche Kurvensatz offensichtlich wahr ist, gibt Ihnen vielleicht die Tatsache zu denken, dass sein Analogon auf dem Torus nicht wahr ist. (Überlegen Sie, warum nicht!)

Zur Illustration, dass einen die Intuition auch bei so „offensichtlichen“ Aussagen in die Irre leiten kann, ist auch eine Erweiterung des Jordanschen Kurvensatzes, das *Jordan–Schönflies–Theorem*, geeignet, das aussagt, dass das Innere einer jeden Jordankurve stetig in das Innere des (normalen geometrischen) Kreises verformt werden kann. Genauer: Es existiert eine stetige Abbildung, deren Inverse auch stetig ist, ein so genannter *Homöomorphismus*, zwischen dem (inneren) Gebiet, das eine Jordankurve einschließt, und der gewöhnlichen Kreisscheibe. In Analogie dazu würde man erwarten, wenn man eine „topologische Sphäre“ als das Abbild der gewöhnlichen geometrischen Sphäre unter einer stetigen injektiven Abbildung definiert, dass sich ein von so einem Objekt begrenztes Gebiet stetig in die gewöhnliche Kugel überführen lässt. Aber das stimmt nicht — ein Gegenbeispiel ist als die „Alexandersche gehörnte Sphäre“ bekannt (wie z.B. in dem exzellenten, aber eher fortgeschrittenen Buch von Bredon [18] nachzulesen ist).

Wir möchten noch anmerken, dass die Schwierigkeiten beim Beweis des Jordanschen Kurvensatzes hauptsächlich von der großen Allgemeinheit der Definition für „einfache Kurve“ herrührt: Da ist jede stetige injektive Abbildung aus dem Einheitsintervall zugelassen, und solche Abbildungen können recht „wild“ sein. Eine einfacherer Ansatz, logisch einwandfrei ebene Graphen zu definieren, ist nur solche einfachen Kurven zuzulassen, die aus einer endlichen Anzahl gerader Linien bestehen — nennen wir sie *Polygonzüge*. Wir können dann einen Graphen polygonal eben nennen, wenn er sich mit Polygonzügen kreuzungsfrei zeichnen lässt. Der Jordansche Kurvensatz lässt sich für Polygonzüge relativ einfach beweisen (siehe Aufgabe 7). Es ist auch nicht gar zu schwer

zu beweisen, dass jeder ebene Graph auch polygonal eben ist;<sup>6</sup> dafür benötigt man etwas (aber nicht allzu viel) Topologie. Daher bringt es überhaupt nichts, beim Zeichnen von Graphen nicht polygonale Kurven zuzulassen — außer Problemen mit dem Jordanschen Kurvensatz.

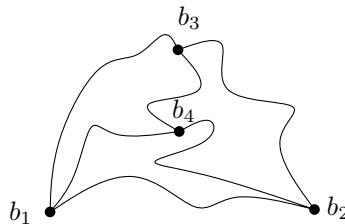
Wie schon angekündigt, ziehen wir es vor, uns an einigen Stellen in den folgenden Ausführungen auf die Intuition zu verlassen. Der Preis für das Ausräumen dieser Unvollkommenheiten wären längere und kompliziertere Beweise; man könnte alle Auslassungen aus dem Jordanschen Kurvensatz und seinen Varianten herleiten.

Beginnen wir mit einem Beweis, dass der Graph  $K_5$  nicht eben ist. Später werden wir das nochmals mit anderen Mitteln nachweisen.

### 6.2.2 Hilfssatz. $K_5$ ist nicht planar.

*Beweis.* Wir führen einen indirekten Beweis. Seien  $b_1, b_2, b_3, b_4, b_5$  die Punkte, die in einer ebenen Zeichnung die Ecken von  $K_5$  repräsentieren. Die Kurve, die die Punkte  $b_i$  und  $b_j$  verbindet, bezeichnen wir mit  $\alpha(i, j)$ .

Weil  $b_1, b_2$  und  $b_3$  Ecken eines Kreises in  $K_5$  sind, bilden die Kurven  $\alpha(1, 2)$ ,  $\alpha(2, 3)$  und  $\alpha(3, 1)$  zusammen eine Jordankurve  $k$ , deshalb liegen die Punkte  $b_4$  und  $b_5$  entweder beide im Inneren oder beide im Äußeren von  $k$ , denn anderenfalls müsste die Kurve  $\alpha(4, 5)$  die Jordankurve  $k$  kreuzen. Nehmen wir zunächst an, dass  $b_4$  wie im folgenden Bild im Inneren von  $k$  liegt:



Dann liegt  $b_5$  im Inneren der Jordankurve, die die Kurven  $\alpha(1, 4)$ ,  $\alpha(2, 4)$  und  $\alpha(1, 2)$  bilden, oder in der Jordankurve  $\alpha(2, 3)$ ,  $\alpha(3, 4)$ ,  $\alpha(2, 4)$ , oder in der Jordankurve  $\alpha(1, 3)$ ,  $\alpha(3, 4)$ ,  $\alpha(1, 4)$ .<sup>7</sup> Im ers-

---

<sup>6</sup>Es gilt sogar die stärkere Aussage, dass sich jeder ebene Graph kreuzungsfrei so zeichnen lässt, dass jede Kante eine gerade Linie ist! Aber das ist nicht so einfach zu beweisen.

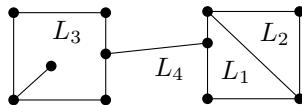
<sup>7</sup>Wir haben nicht gezeigt, dass das Innere dieser drei Jordankurven zusammen das Innere von  $k$  ergibt (außer den Kurven  $\alpha(1, 4)$ ,  $\alpha(2, 4)$  und  $\alpha(3, 4)$ ); das ist einer der Punkte, in denen wir die Intuition beanspruchen.

ten Fall muss die Kurve  $\alpha(3, 5)$  die Jordankurve aus  $\alpha(1, 4)$ ,  $\alpha(2, 4)$ ,  $\alpha(1, 2)$  schneiden, und in den anderen Fällen sieht es ähnlich aus.

Wenn die Punkte  $b_4$  und  $b_5$  beide im Äußeren von  $k$  liegen, geht alles analog.  $\square$

**Länder und Kreise in zweifach zusammenhängenden Graphen.** Sind  $e_1, \dots, e_n$  die Kanten eines Kreises in einem eingebetteten ebenen Graphen  $G$ , dann bilden  $\alpha(e_1), \dots, \alpha(e_n)$  eine Jordankurve. Nach dem Jordanschen Kurvensatz liegt jedes Land von  $G$  entweder im inneren oder im äußeren Gebiet dieser Jordankurve. Der Kürze halber nennen wir auch diese Jordankurve einen *Kreis von  $G$*  (so dass ein Kreis von  $G$  nun ein Kreis im graphentheoretischen Sinne sein kann, d.h. ein Teilgraph von  $G$ , oder die Jordankurve, die in einer Zeichnung von  $G$  eine solchen Kreis repräsentiert).

Bei manchen topologischen ebenen Graphen ist jedes Land das Innere oder Äußere eines Kreises von  $G$ , doch das muss nicht immer so sein. Beispielsweise hat eine ebene Zeichnung eines Baums nur ein einziges Land. Ein anderes Beispiel ist dieses:



Es stellt sich heraus, dass die Gegenbeispiele genau die nicht zweifach zusammenhängenden Graphen sind.

**6.2.3 Hilfssatz.** Sei  $G$  ein zweifach eckenzusammenhängender ebener Graph. Dann ist in jeder ebenen Zeichnung von  $G$  jedes Land das Innere oder Äußere eines Kreises von  $G$ .

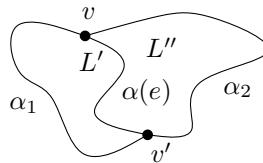
*Beweis.* Wir führen Induktion und verwenden dabei Hilfssatz 4.6.5 (die Charakterisierung 2-zusammenhängender Graphen). Wenn der Graph  $G$  ein Dreieck ist, dann folgt die Aussage des Hilfssatzes aus dem Jordanschen Kurvensatz.

Sei  $G = (V, E)$  ein zusammenhängender topologischer ebener Graph mit mindestens vier Ecken. Nach Hilfssatz 4.6.5 gibt es entweder eine Kante  $e \in E$ , so dass der Graph  $G' = G - e$  2-zusammenhängend ist, oder es gibt einen 2-zusammenhängenden Graphen  $G' = (V', E')$  und eine Kante  $e \in E'$ , so dass  $G = G' \% e$ , wobei  $\%$  die Operation der Kantenunterteilung bezeichnet.

Weil  $G$  ein topologischer ebener Graph ist, ist in beiden Fällen auch  $G'$  ein topologischer ebener Graph. Weil  $G'$  2-zusammenhän-

gend ist, können wir die Induktionsvoraussetzung verwenden. Jedes Land des topologischen Graphen  $G'$  ist also das Innere oder Äußere eines Kreises von  $G'$ .

Betrachten wir als erstes den Fall  $G' = G - e$ ,  $e = \{v, v'\}$ . Die Ecken  $v$  und  $v'$  sind durch die Kurve  $\alpha(e)$  miteinander verbunden, und deshalb liegen sie beide auf dem Rand eines Landes  $L$  von  $G'$ . Sei  $k_L$  der Kreis, der das Land  $L$  berandet. Das folgende Bild zeigt, dass die Kurve  $\alpha(e)$  das Land  $L$  in zwei neue Länder  $F'$  und  $F''$  teilt:



(Dies ist wieder ein Punkt, an dem wir die Anschauung an die Stelle eines Beweises setzen, aber in Aufgabe 7 machen wir das wieder gut.) Die Länder  $L'$  und  $L''$  sind Gebiete der Kreise  $\alpha_1 \cup \alpha(e)$  und  $\alpha_2 \cup \alpha(e)$ , wobei  $\alpha_1$  und  $\alpha_2$  die zwei Kurven sind, die  $v$  und  $v'$  miteinander verbinden und die gemeinsam den Kreis  $k_L$  bilden. Daher werden die Länder von  $G$  wie behauptet alle durch Kreise begrenzt. Dies beendet den Beweis des Induktionsschritts im ersten Fall, in dem  $G = G' + e$ .

Der verbleibende zweite Fall ist einfacher: Ist  $G = G' \% e$  und ist jedes Land von  $G'$  ein Gebiet eines Kreises von  $G'$ , dann folgt direkt aus der Definition des Unterteilens von Kanten, dass  $G$  die gleiche Eigenschaft hat. Damit ist der Beweis des Hilfssatzes beendet.  $\square$

Hilfssatz 6.2.3 zeigt, dass sich 2-zusammenhängende ebene Graphen in gewisser Weise angenehmer verhalten als beliebige ebene Graphen. Weiter stellt sich heraus, dass dreifach eckenzusammenhängende Graphen ein noch viel angenehmeres Verhalten an den Tag legen: Solche Graphen besitzen eine im Wesentlichen eindeutige ebene Zeichnung (genauer: Zwei kreuzungsfreie Zeichnungen auf der Sphäre unterscheiden sich nur durch eine stetige Verformung und eventuell eine Spiegelung), und sind in vieler Hinsicht einfacher zu handhaben (siehe Abschnitt 6.3). Will man Sätze für ebene Graphen beweisen oder Algorithmen entwerfen, dann ist es gewöhnlich ratsam, zuerst 3-zusammenhängende ebene Graphen zu betrachten und den allgemeinen Fall dann durch Zerlegen eines gegebenen Graphen in 3-zusammenhängende Teile zu lösen. Wir werden dieses Thema hier nicht weiter verfolgen.

**Eine kombinatorische Charakterisierung ebener Graphen.**

Die folgende Tatsache ist offensichtlich: *Ein Graph  $G$  ist genau dann eben, wenn jede Unterteilung von  $G$  eben ist.* Diese Eigenschaft kann man für eine kombinatorische Charakterisierung ebener Graphen ausnutzen — eine rein graphentheoretische Charakterisierung, in der keine Geometrie mehr vorkommt. Es geht um das folgende bedeutende Ergebnis:

**6.2.4 Satz (Satz von Kuratowski).** *Ein Graph  $G$  ist genau dann planar, wenn er keinen Teilgraphen besitzt, der zu einer Unterteilung von  $K_{3,3}$  oder zu einer Unterteilung von  $K_5$  isomorph ist.*

Die eine der beiden Implikationen in diesem Satz ist ganz einfach zu beweisen, dass nämlich ein ebener Graph keine Unterteilung eines nicht ebenen Graphen enthalten kann, doch die andere Richtung ist anspruchsvoller; wir werden sie in diesem Buch nicht beweisen.

Dieser Satz zeigt, dass es für die Eigenschaft, nicht eben zu sein, ein Zertifikat gibt, nämlich eine Unterteilung von  $K_{3,3}$  oder  $K_5$ . Wenn man die Planarität von Graphen wirklich mit dem Computer testen möchte und vielleicht sogar eine ebene Zeichnung finden möchte, dann ist diese Methode nicht besonders effizient. Man kennt Algorithmen, die testen, ob ein gegebener Graph eine Unterteilung eines festen (kleinen) Graphen enthält, doch sind sie ziemlich kompliziert und unpraktisch. Zum Testen der Planarität und Finden „netter“ ebener Zeichnungen hat man einige schnelle (allerdings auch komplizierte) Methoden erfunden. Mit solchen Methoden kann man z.B. die Planarität eines Graphen mit  $n$  Ecken in Zeit  $O(n)$  testen. Was „nette“ Zeichnungen betrifft, so weiß man beispielsweise, dass sich jeder ebene Graph auf  $n$  Ecken so zeichnen lässt, dass die Ecken ganzzahlige Koordinaten zwischen 1 und  $n$  haben und die Kanten gerade Linien sind. Neuere Ergebnisse in dieser Richtung sowie weitere Referenzen können Sie in Kant [42] finden. Viele interessante Probleme mit Zeichnungen von Graphen sind noch offen. So ist z.B. zur Zeit nicht bekannt, ob jeder ebene Graph eine ebene Zeichnung zulässt, in der alle Kanten gerade Linien mit ganzzahligem Länge sind. (Dies ist zugleich ein Beispiel dafür, wie leicht man in der diskreten Mathematik Probleme formuliert, die manchmal ganz schön kompliziert sind — ein Tor stellt mehr Fragen, als hundert Weise beantworten können.)

Der Satz von Kuratowski charakterisiert ebene Graphen durch Angabe zweier „Hindernisse“, die der Planarität entgegenstehen, nämlich der Präsenz einer Unterteilung des  $K_5$  oder einer Unterteilung des  $K_{3,3}$ . Kürzlich hat man viele weitere Sätze dieser Art gefunden, die diverse Graphenklassen durch eine endliche Menge von „Hindernissen“ charakterisieren. Die Hindernisse sind meist nicht verbotene Unterteilungen

bestimmter Graphen, sondern so genannte *verbotene Minoren* (siehe Aufgabe 6.4.11). Viele wichtige Probleme der Graphentheorie, einschließlich zahlreicher Fragen zur Effizienz von Algorithmen, konnte man mit diesem Ansatz lösen, und derzeit ist dieses Gebiet (das man als *strukturelle Graphentheorie* bezeichnet) einer der dynamischsten und erfolgreichsten Teile der modernen Graphentheorie. Ein Beispiel für den Fortschritt in diesem Gebiet ist Robertson, Seymour und Thomas [47], wo ein lange Zeit offenes Problem mit ähnlichen Methoden gelöst wurde.

## Aufgaben

1. Zeigen Sie, dass der Graph  $K_{3,3}$  nicht planar ist; sie können sich an dem entsprechenden Beweis für  $K_5$  orientieren.
2. (a) Finden Sie eine Unterteilung entweder von  $K_{3,3}$  oder von  $K_5$  in dem Graphen links in Abb. 4.4.  
 (b) Ist der mittlere Graph in Abb. 4.4 planar?  
 (c) Ist der Graph in Abb. 9.3 planar?
3. Der *vollständige k-partite Graph*  $K_{n_1, n_2, \dots, n_k}$  hat die Eckenmenge  $V = V_1 \dot{\cup} V_2 \dot{\cup} \dots \dot{\cup} V_k$ , wobei die  $V_1, \dots, V_k$  disjunkte Mengen mit  $|V_i| = n_i$  sind. Jede Ecke  $v \in V_i$  ist mit allen Ecken aus  $V \setminus V_i$  verbunden,  $i = 1, 2, \dots, k$ . Beschreiben Sie alle  $k$ -Tupel  $(n_1, n_2, \dots, n_k)$  natürlicher Zahlen,  $k = 1, 2, \dots$ , für die  $K_{n_1, n_2, \dots, n_k}$  ein ebener Graph ist.
4. Im Beweis von Hilfssatz 6.2.3 führen wir Induktion, aber Induktion worüber? (Wir haben keine Zahl explizit als Induktionsparameter angegeben.)
5. Beweisen Sie: Ist jedes Land eines topologischen ebenen Graphen  $G$  das Innere oder Äußere eines Kreises von  $G$ , dann ist  $G$  2-zusammenhängend.
6. \*Betrachten Sie eine beliebige (nicht notwendig ebene) Zeichnung des vollständigen Graphen  $K_n$ . Beweisen Sie, dass sich mindestens  $\frac{1}{5} \binom{n}{4}$  Kantenpaare kreuzen. (Verwenden Sie, dass  $K_5$  nicht eben ist.)
7. Ziel dieser Aufgabe ist, die „Beweislücken“ zu füllen, so dass wir nicht mehr von der geometrischen Anschauung abhängig sind.
  - (a) \*Sei  $k$  eine Jordankurve, die aus endlich vielen geraden Linien besteht (d.h. ein geschlossener Polygonzug). Definieren Sie zwei Punkte aus  $\mathbb{R}^2 \setminus k$  als äquivalent, wenn man sie durch einen Polygonzug, der  $k$  nicht schneidet, miteinander verbinden kann. Beweisen Sie, dass diese Äquivalenzrelation höchstens zwei Äquivalenzklassen hat.

(b) \*Zeigen Sie, dass es in der Situation aus (a) auch mindestens zwei Äquivalenzklassen gibt (also genau zwei). Hinweis: Definieren Sie „innerer Punkt“ als einen Punkt, für den eine vertikale Halbgerade, die von ihm aus nach oben geht,  $k$  ungerade oft schneidet.

(c) Sei  $k$  eine polygonale Jordankurve wie in (a), seien  $p, q$  zwei verschiedene Punkte auf  $k$ , seien  $k_1, k_2$  die zwei Polygonzüge, in die die beiden Punkte  $p$  und  $q$  die Jordankurve  $k$  zerlegen, und seien  $r \in k_1, s \in k_2$  Punkte auf diesen Polygonzügen (verschieden von  $p$  und  $q$ ). Sei  $\ell$  ein Polygonzug, der  $p$  mit  $q$  verbindet und ganz im Inneren von  $k$  liegt (abgesehen von den Endpunkten). Beweisen Sie, dass jeder Polygonzug, der  $r$  mit  $s$  verbindet und (abgesehen von den Endpunkten) ganz im Inneren von  $k$  liegt,  $\ell$  schneiden muss.

## 6.3 Die Euler–Formel

Im Wesentlichen gibt es nur eine einzige quantitative Formel für ebene Graphen. Man kann sagen, dass alle anderen Resultate diese Formel in gewissem Grade benutzen. Zugleich ist sie die älteste graphentheoretische Formel, bereits 1752 war sie Euler bekannt, und manche sagen, dass sogar Descartes sie kannte (1640). Ursprünglich war sie als Aussage über Polytope (geometrische Körper wie der Würfel) formuliert.

**6.3.1 Hilfssatz (Euler–Formel).** *Sei  $G = (V, E)$  ein zusammenhängender ebener Graph, und sei  $f$  die Anzahl der Länder (engl.: faces) in einer ebenen Zeichnung von  $G$ . Dann gilt*

$$|V| - |E| + f = 2.$$

Insbesondere ist die Länderzahl nicht von der konkret gewählten Zeichnung abhängig.

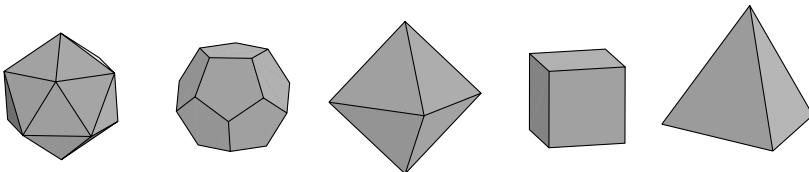
*Beweis.* Wir führen Induktion nach der Kantenzahl von  $G$ . Wenn  $E = \emptyset$  ist, dann ist  $|V| = 1$  und  $f = 1$  und die Formel gilt. Sei also  $|E| \geq 1$ . Wir unterscheiden zwei Fälle:

1. Der Graph  $G$  enthält keinen Kreis. Dann ist  $G$  ein Baum und  $|V| = |E| + 1$ ; und es ist  $f = 1$ , weil eine ebene Zeichnung eines Baumes nur ein (unbegrenztes) Land hat.
2. Es gibt eine Kante  $e \in E$ , die in einem Kreis enthalten ist. In diesem Fall ist der Graph  $G - e$  zusammenhängend und nach Induktionsvoraussetzung gilt für ihn die Euler–Formel (wir betrachten die Zeichnung, die aus der gegebenen Zeichnung von  $G$  durch Entfernen der Kante  $e$  entsteht). Nach dem Jordanschen Kurvensatz grenzt die Kante  $e$  in der betrachteten Zeichnung

von  $G$  an zwei verschiedene Länder  $L$  und  $L'$ . Diese beiden Länder verschmelzen durch das Entfernen von  $e$  zu einem Land. Deshalb erhöhen sich, wenn man die Kante wieder einfügt, die Anzahl der Länder und der Kanten jeweils um 1, während die Eckenanzahl unverändert bleibt. Damit gilt die Euler–Formel auch für  $G$ .

□

**Anwendung: Platonische Körper.** Eine Schule griechischer Philosophen, die sich in die Tradition Platons stellten, maß den besonders regelmäßigen geometrischen Körpern, den so genannten *regulären Polytopen*, eine besondere Bedeutung bei; sie zogen sie sogar zur Erklärung der Struktur des Universums heran. (Übrigens hat sogar noch Kepler es für eine seiner bedeutenden Entdeckungen gehalten, dass — so seine Theorie — die Bahnen der Planeten, und speziell die Abstände, durch die Geometrie der regulären Polytope bestimmt werden.) Ein Polytop ist ein dreidimensionaler konvexer Körper<sup>8</sup> mit endlich vielen Seitenflächen. Bei einem regulären Polytop sind alle Seitenflächen dem gleichen regelmäßigen Vieleck kongruent, und an jedem Eckpunkt des Körpers treffen sich gleich viele dieser Seitenflächen. Einer der Gründe für das schon erwähnte große Interesse an diesen Objekten ist sicher, dass es nur fünf verschiedene Typen gibt: Das Tetraeder, den Würfel, das Oktaeder, das Dodekaeder und das Ikosaeder (in der folgenden Abbildung von rechts nach links):



Diese Tatsache war schon den alten Griechen bekannt. Wenn man die Regularitätsbedingungen ein klein wenig entschärft (wenn man nicht auf Konvexität beharrt, zwei Sorten Seitenflächen erlaubt oder ähnliches) oder wenn man zu höherer Dimension übergeht, trifft man auf viele weitere interessante und schöne geometrische Objekte. Die Forschung auf diesem Gebiet ist noch immer recht aktiv.

Wir werden nun mit Hilfe der Euler–Formel beweisen, dass es keine anderen regulären Körper gibt als die fünf Platonischen Körper. (Dass die Platonischen Körper tatsächlich reguläre Polytope sind, muss man eigentlich auch noch nachweisen; doch dies ist ein geometrisches Problem, das wir hier nicht betrachten.) Der erste Schritt beim Beweis

---

<sup>8</sup>Konvex bedeutet, dass mit je zwei Punkten  $x$  und  $y$  auch die ganze Strecke  $xy$  in dem Körper liegt, d.h. die Fläche hat keine „Dellen“.

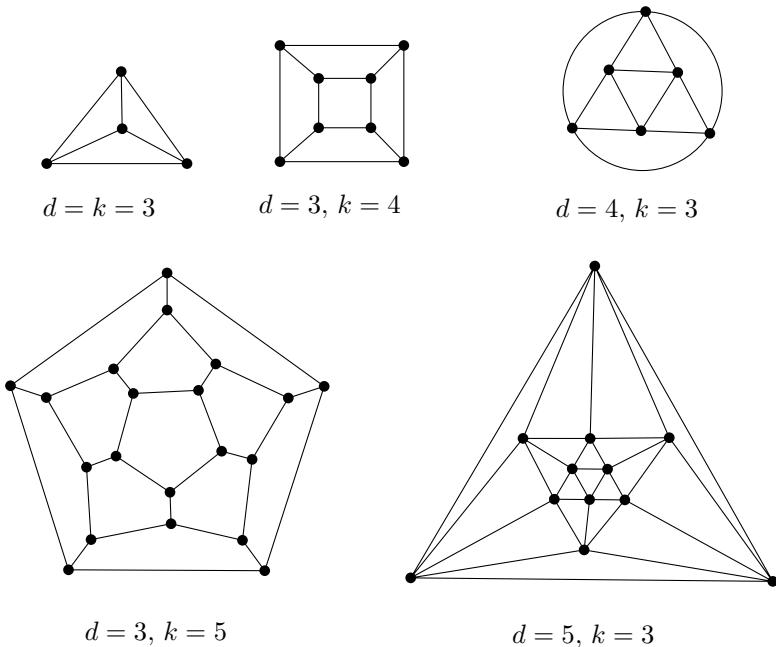


Abb. 6.1 Graphen der Platonischen Körper.

der Nicht-Existenz anderer regulärer Polytope ist, aus einem konvexen Körper einen ebenen Graphen zu gewinnen. Wir platzieren das betrachtete Polytop so in eine Kugel, dass der Mittelpunkt der Kugel innerhalb des Polytops liegt. Dann projizieren wir das Polytop mit dem Kugelmittelpunkt als Projektionszentrum auf die Kugeloberfläche (stellen Sie sich vor, dass das Gerüst des Polytops massiv ist und die Seitenflächen lichtdurchlässig sind und Sie platzieren eine Lampe an den Kugelmittelpunkt). Sie erhalten so einen Graphen, der kreuzungsfrei auf die Sphäre gezeichnet ist, und wir wissen aus Abschnitt 6.1, dass man aus so einer Zeichnung mittels der stereographischen Projektion eine ebene Zeichnung erhält. Die Ecken, Kanten und Seitenflächen des Polytops werden die Ecken, Kanten und Länder dieser ebenen Zeichnung. Daraus kommen auch die Namen „Ecke“ und „Kante“ bei Graphen (und englisch „face“ bei ebenen Graphen). Für die fünf regulären Körper erhalten wir so die Graphen in Abb. 6.1.

Wenn man diese Konstruktion mit einem regulären Polytop beginnt, haben in dem so erhaltenen topologischen ebenen Graphen alle Ecken den gleichen Grad  $d \geq 3$  und bei allen Ländern liegen gleich viele ( $k \geq 3$ ) Ecken auf dem Rand. Die Nicht-Existenz anderer regulärer Polytope folgt deshalb aus dem folgenden Hilfssatz:

**6.3.2 Hilfssatz.** *Sei  $G$  ein topologischer ebener Graph, in dem jede*

Ecke Grad  $d$  hat und auf dem Rand eines jeden Landes  $k$  Ecken liegen (mit irgendwelchen Zahlen  $d \geq 3$  und  $k \geq 3$ ). Dann ist  $G$  isomorph zu einem der Graphen in Abb. 6.1.

*Beweis.* Wir bezeichnen die Eckenzahl in dem betrachteten Graphen  $G = (V, E)$  mit  $n$ , die Kantenzahl mit  $m$  und die Länderzahl mit  $f$ . Zuerst nutzen wir die Gleichung  $\sum_{v \in V} \deg_G(v) = 2|E|$  aus, die sich in unserem Fall auf

$$dn = 2m$$

reduziert. Ganz ähnlich erhält man die Gleichung

$$2m = kf.$$

Wir zählen die geordneten Paare  $(e, F)$ , wobei  $L$  ein Land von  $G$  ist und  $e \in E$  eine Kante, die auf dem Rand von  $L$  liegt. Jede Kante kommt in zwei solchen Paaren vor und jedes Land in  $k$  solchen Paaren.

Als Nächstes drücken wir  $n$  und  $f$  mit Hilfe von  $m$  aus, wozu wir die gerade hergeleiteten Gleichungen verwenden, und setzen die Ergebnisse in die Euler–Formel ein:

$$2 = n - m + f = \frac{2m}{d} - m + \frac{2m}{k}.$$

Nach Addition von  $m$  und Division durch  $2m$  erhalten wir

$$\frac{1}{d} + \frac{1}{k} = \frac{1}{2} + \frac{1}{m}.$$

Sind also  $d$  und  $k$  beide bekannt, dann sind die anderen Parameter  $n$ ,  $m$  und  $f$  schon eindeutig festgelegt. Es ist leicht zu sehen, dass  $\min(d, k) = 3$  ist, denn sonst wäre  $\frac{1}{d} + \frac{1}{k} \leq \frac{1}{2}$ . Für  $d = 3$  erhalten wir  $\frac{1}{k} - \frac{1}{6} = \frac{1}{m} > 0$ , und somit  $k \in \{3, 4, 5\}$ . Analog folgt aus  $k = 3$ , dass  $d \in \{3, 4, 5\}$ . Deshalb muss einer der folgenden Fälle eintreten:

$d$	$k$	$n$	$m$	$f$
3	3	4	6	4
3	4	8	12	6
3	5	20	30	12
4	3	6	12	8
5	3	12	30	20

Nun prüft man leicht nach, dass der Graph in jedem dieser Fälle durch die Werte  $d, k, n, m, f$  eindeutig bestimmt und isomorph zu einem der Graphen in Abb. 6.1 ist.  $\square$

Wir merken an, dass die Verbindung zwischen ebenen Graphen und dreidimensionalen konvexen Polytopen enger ist, als es scheinen mag. Wie wir gesehen haben, erhalten wir aus jedem konvexen Polytop einen

ebenen Graphen (das *Gerüst* des Polytops). Der (schwierigere) Satz von Steinitz garantiert, dass jeder dreifach eckenzusammenhängende ebene Graph der Gerüstgraph eines dreidimensionalen konvexen Polytops ist. Ein wunderbares Buch über die Theorie der konvexen Polytope ist Ziegler [33].

Eine sehr wichtige Eigenschaft ebener Graphen ist, dass sie nur relativ wenige Kanten haben können: Ein ebener Graph auf  $n$  Ecken hat  $O(n)$  Kanten. Der folgende Hilfssatz formuliert diese Eigenschaft präzise:

### 6.3.3 Hilfssatz (Ein ebener Graph hat $O(n)$ Kanten).

- (i) Sei  $G = (V, E)$  ein ebener Graph mit mindestens drei Ecken. Dann ist  $|E| \leq 3|V| - 6$ . Gleichheit gilt im Fall eines maximal ebenen Graphen, d.h. eines ebenen Graphen, den das Hinzufügen einer weiteren Kante (auf der gleichen Eckenmenge) in jedem Fall nicht-planar macht.
- (ii) Enthält der Graph darüber hinaus kein Dreieck (d.h.  $K_3$  als Teilgraph), dann gilt sogar  $|E| \leq 2|V| - 4$ .

(In diesem Hilfssatz lassen wir natürlich keine Graphen mit Mehrfachkanten zu!)

*Beweis von (i).* Wenn der Graph  $G$  nicht maximal eben ist, fügen wir solange Kanten hinzu, bis er maximal eben wird. Teil (i) ist also bewiesen, wenn wir zeigen können, dass für jeden maximal ebenen Graphen mit mindestens drei Ecken  $|E| = 3|V| - 6$  gilt.

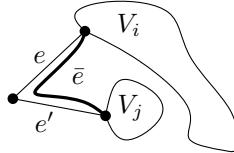
Als erstes wollen wir beweisen, dass jedes Land (einschließlich des äußeren) eines maximal ebenen Graphen auf mindestens drei Ecken ein Dreieck ist,<sup>9</sup> d.h. dass es von einem Kreis der Länge 3 berandet ist.

Ist  $G$  nicht zusammenhängend, dann können wir einfach eine Kante zwischen zwei Ecken aus verschiedenen Komponenten einfügen. Ist  $G$  zusammenhängend, aber nicht 2-zusammenhängend, dann gibt es eine Ecke  $v$ , so dass der Graph  $G - v$  in Komponenten  $V_1, V_2, \dots, V_k$ ,  $k \geq 2$ , zerfällt (an dieser Stelle benötigen wir die Voraussetzung, dass  $G$  mindestens drei Ecken hat). Wir wählen zwei Kanten  $e$  und  $e'$ , die  $v$  mit zwei verschiedenen Komponenten  $V_i$  und  $V_j$  verbinden, und zwar so, dass  $e$  und  $e'$  in der Zeichnung benachbart sind (d.h. dass sie bei  $v$  gemeinsam einen Winkel bilden). Zwischen den beiden anderen

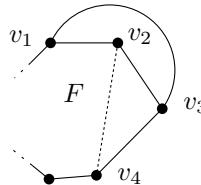
---

<sup>9</sup>Aus diesem Grund nennt man maximal ebene topologische Graphen auch *Triangulierungen*.

Endpunkten kann man eine Kante  $\bar{e}$  einfügen, ohne die Planarität zu zerstören:



Deshalb ist ein maximal ebener Graph mit mindestens drei Ecken notwendig 2-zusammenhängend, und nach Hilfssatz 6.2.3 wird jedes Land von einem Kreis in dem Graphen berandet. Nehmen wir nun an, es gäbe ein Land  $F$ , dessen Grenzkreis die  $t \geq 4$  Ecken  $v_1, \dots, v_t$  enthält. Wenn die Ecke  $v_1$  nicht durch eine Kante mit der Ecke  $v_3$  verbunden ist, dann können wir die Kante  $\{v_1, v_3\}$  in dem Land  $F$  einzeichnen. Wenn aber  $\{v_1, v_3\} \in E(G)$  schon eine Kante von  $G$  ist, dann muss sie außerhalb von  $F$  gezeichnet sein, und deshalb kann nicht auch  $\{v_2, v_4\}$  eine Kante von  $G$  sein, denn sonst müssten sich  $\{v_1, v_3\}$  und  $\{v_2, v_4\}$  kreuzen:



Also können wir die Kante  $\{v_2, v_4\}$  hinzufügen und quer durch das Land  $F$  zeichnen, im Widerspruch zur Annahme, dass  $G$  maximal planar ist.

Jedes Land in einem maximal ebenen Graphen muss also tatsächlich ein Dreieck sein. Daraus folgt, ähnlich wie im Beweis von Hilfssatz 6.3.2, die Gleichung  $3f = 2|E|$ , wobei  $f$  die Länderzahl ist. Wenn wir nun  $f$  mit Hilfe der Euler Formel ausdrücken und in die gerade hergeleitete Gleichung einsetzen, erhalten wir

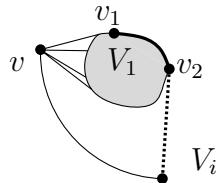
$$|V| - |E| + \frac{2}{3}|E| = 2.$$

Die gewünschte Gleichung  $|E| = 3|V| - 6$  folgt mit einer einfachen Umformung. Damit ist Teil (i) bewiesen.

*Beweis von (ii).* Wir gehen ganz ähnlich vor. Nach eventuellem Hinzufügen von Kanten können wir davon ausgehen, dass der Graph ein maximal dreiecksfreier ebener Graph ist, das soll heißen, dass der

Graph nach Hinzufügen einer neuen Kante ein Dreieck enthält oder nicht mehr planar ist (oder beides). Wieder können wir annehmen, dass der Graph zusammenhängend ist.

Ist  $G$  nicht 2-zusammenhängend, dann gibt es eine Ecke  $v$  deren Entfernen  $G$  in Komponenten  $V_1, \dots, V_k$  zerlegt,  $k \geq 2$ . Sicher können wir eine neue Kante zwischen verschiedenen Komponenten hinzufügen, so dass der Graph eben bleibt, aber dabei könnte durchaus ein Dreieck entstehen (das geschieht genau dann, wenn wir zwei Ecken verbinden, die beide mit  $v$  benachbart sind), deshalb müssen wir etwas vorsichtiger sein. Wenn jede der Komponenten  $V_i$  aus einer einzigen Ecke besteht, dann ist  $G$  ein Baum und die zu beweisende Formel gilt. Nehmen wir also an, dass  $|V_1| \geq 2$ , und betrachten wir ein Land  $F$ , auf dessen Rand sowohl eine Ecke aus  $V_1$  als auch aus einem anderen  $V_i$  liegt, wie im folgenden Bild:



Die Komponente  $V_1$  muss mindestens eine Kante  $\{v_1, v_2\}$  auf dem Rand von  $F$  enthalten, und weil  $G$  dreiecksfrei ist, kann es nicht sein, dass  $v_1$  und  $v_2$  beide mit  $v$  benachbart sind. Deshalb kann man  $v_1$  oder  $v_2$  mit einer Ecke aus  $V_i$  verbinden, ohne ein Dreieck zu erzeugen.

Daher können wir annehmen, dass  $G$  2-zusammenhängend ist. In diesem Fall wird jedes Land in  $G$  durch einen Kreis begrenzt. Jeder solche Kreis hat Länge mindestens 4, und mit doppeltem Abzählen erhalten wir diesmal  $2|E| \geq 4f$ . Mit der Euler–Formel ergibt sich schließlich  $|E| \leq 2|V| - 4$ .  $\square$

**Ein typischer falscher Beweis.** An diesem Satz kann man sehr schön einen häufigen Fehler in Induktionsbeweisen exemplarisch zeigen. Es soll also bewiesen werden, dass jeder topologische ebene Graph mit  $n \geq 3$  Ecken, in dem jedes Land durch ein Dreieck begrenzt wird,  $3n - 6$  Kanten hat. Relativ häufig sieht man (falsche!) Lösungen von etwa der folgenden Art: Ich führe Induktion nach  $n$ . Für  $n = 3$  muss der Graph ein Dreieck sein, muss drei Kanten und drei Ecken haben, und die Behauptung stimmt. Ich nehme nun als Induktionsvoraussetzung an, dass die Behauptung für jeden topologischen ebenen Graphen  $G$  mit  $n$  Ecken gilt. Bei jedem solchen  $G$  darf ich in jedem beliebigen Land eine Ecke

hinzufügen und sie mit allen drei Ecken dieses Landes verbinden, so wie in folgendem Bild:



So erhalte ich einen Graphen  $G'$  mit  $n + 1$  Ecken. Die Kantenzahl von  $G$  ist nach Induktionsvoraussetzung  $3n - 6$ , und wir haben drei neue Kanten hinzugefügt. Also hat  $G'$  Kantenzahl  $3(n + 1) - 6$ , und die Behauptung gilt auch für Graphen mit  $n + 1$  Ecken. Sehen Sie das Problem? Der Beweis funktioniert zwar für alle Graphen, die wir mit der angegebenen Konstruktion aus einem Dreieck erhalten, aber leider lassen sich nicht alle möglichen topologischen ebenen triangulierten Graphen  $G'$  mit  $n+1$  Ecken auf diese Art herstellen. Den Oktaedergraph (siehe Abb.6.1) zum Beispiel bekommen wir so nicht; denn alle seine Ecken haben Grad 4, während jeder so konstruierte Graph mindestens eine Ecke vom Grad 3 hat. (Warum?)

Teil (i) von Hilfssatz 6.3.3 hat eine wichtige und oft gebrauchte Konsequenz, dass nämlich jeder ebene Graph eine Ecke vom Grad höchstens 5 hat. Analog garantiert Teil (ii), dass ein ebener dreiecksfreier Graph eine Ecke vom Grad höchstens 3 enthält.

Aus Teil (i) folgt auch, dass  $K_5$  nicht planar ist, weil er 10 Kanten hat, ein ebener Graph auf 5 Ecken aber höchstens 9 Kanten haben darf. Analog folgt aus (ii), dass  $K_{3,3}$  nicht eben ist, weil ein dreiecksfreier Graph auf 6 Ecken höchstens 8 Kanten hat.

Wir beweisen noch einen weiteren Hilfssatz, der etwas über die möglichen Gradfolgen ebener Graphen aussagt.

**6.3.4 Hilfssatz.** Sei  $G = (V, E)$  ein 2-zusammenhängender ebener Graph mit mindestens drei Ecken. Sei  $n_i$  die Anzahl der Ecken vom Grad  $i$ , und sei  $f_i$  die Anzahl der Länder (in einer festen ebenen Zeichnung), deren berandender Kreis die Länge  $i$  hat. Dann gilt

$$\sum_{i \geq 1} (6 - i)n_i = 12 + 2 \sum_{j \geq 3} (j - 3)f_j,$$

oder anders aufgeschrieben

$$5n_1 + 4n_2 + 3n_3 + 2n_4 + n_5 - n_7 - 2n_8 - \dots = 12 + 2f_4 + 4f_5 + 6f_6 + \dots$$

Daraus folgt, dass  $5n_1 + 4n_2 + 3n_3 + 2n_4 + n_5 \geq 12$  ist, und insbesondere enthält jeder ebene Graph mindestens drei Ecken, deren Grad 5 nicht übersteigt.

*Beweis.* Klar ist  $|V| = \sum_i n_i$  und  $f = \sum_i f_i$ . Wenn wir in der Euler-Formel für  $|V|$  und  $f$  diese Summen einsetzen, erhalten wir

$$2|E| = 2(|V| + f - 2) = \sum_i 2n_i + \sum_j 2f_j - 4. \quad (6.1)$$

Mit doppeltem Abzählen ähnlich wie in den vorangegangenen Beweisen erhalten wir weiter:  $\sum_i i n_i = 2|E| = \sum_j j f_j$ . Darin setzen wir für  $2|E|$  den Wert aus (6.1) ein und erhalten

$$\sum_j (j - 2)f_j + 4 = \sum_i 2n_i \quad \sum_j 2f_j = \sum_i (i - 2)n_i + 4.$$

Wir multiplizieren die erste dieser beiden Gleichungen mit 2 und subtrahieren davon die zweite. Das Ergebnis ist

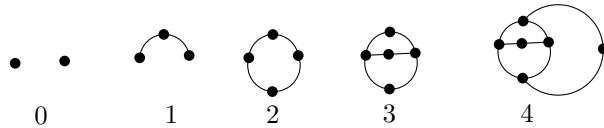
$$\sum_i (6 - i)n_i - 4 = 2 \sum_j (j - 3)f_j + 8.$$

Damit ist der Hilfssatz bewiesen.  $\square$

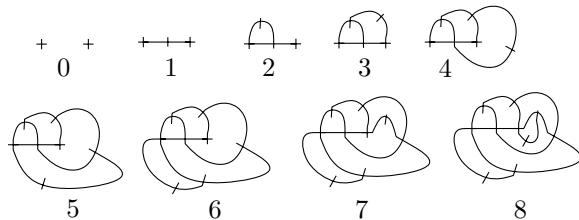
## Aufgaben

1. Beweisen Sie, dass die Schranke  $|E| \leq 2|V| - 4$  für dreiecksfreie ebene Graphen bestmöglich ist. Das heißt: Konstruieren Sie für unendlich viele  $n$  Beispiele dreiecksfreier ebener Graphen mit  $n$  Ecken und  $2n - 4$  Kanten.
2. (a) Zeigen Sie, dass ein topologischer ebener Graph mit  $n \geq 3$  Ecken höchstens  $2n - 4$  Länder hat.  
 (b) Zeigen Sie, dass ein dreiecksfreier topologischer ebener Graph höchstens  $n - 2$  Länder hat.
3. Beweisen Sie, dass ein ebener Graph, in dem jede Ecke Grad mindestens 5 hat, mindestens 12 Ecken hat.
4. Für welche Werte von  $k$  können Sie die folgende Aussage beweisen?  
*Es gibt eine Zahl  $n_0$ , so dass jeder ebene Graph mit mindestens  $n_0$  Ecken wenigstens  $k$  Ecken vom Grad höchstens 5 enthält.* Könnte diese Aussage für alle  $k$  stimmen?
5. \*Betrachten Sie einen maximal dreiecksfreien ebenen Graphen  $G = (V, E)$ , d.h. einen dreiecksfreien ebenen Graphen, so dass jeder Graph der Form  $G + e$ , wobei  $e \in \binom{V}{2} \setminus E$  ist, ein Dreieck enthält oder nicht mehr eben ist. Beweisen Sie, dass jedes Land in jeder Zeichnung eines solchen Graphen ein Viereck oder ein Fünfeck ist.
6. Finden Sie ein weiteres dreidimensionales konvexes Polytop neben den Platonischen Körpern, bei dem alle Seitenflächen kongruente regelmäßige konvexe Vielecke sind. \*Können Sie alle Ausnahmen auflisten?

7. (Das Spiel „Sprouts“<sup>10</sup>) Dieses Spiel haben J. H. Conway und M. S. Paterson erfunden. Am Anfang werden  $n$  Punkte auf ein Blatt Papier gezeichnet (das Spiel ist schon für relativ kleine  $n$  interessant, etwa für  $n = 5$ ). Die Spieler ziehen abwechselnd, und wenn ein Spieler nicht mehr ziehen kann, dann hat er verloren. Ein Zug besteht darin, einen neuen Punkt hinzuzufügen und ihn mit zwei der schon gezeichneten Punkte mit einer Linie zu verbinden. Dabei darf man den neuen Punkt nur mit solchen Punkten verbinden, von denen bisher höchstens zwei Linien ausgehen, und die neue Linie darf keine der alten Linien kreuzen. (In jedem Moment haben wir also eine ebene Zeichnung eines Graphen mit Maximalgrad höchstens 3.) Ein Beispiel:



- (a) Beweisen Sie, dass ein Spiel, das mit  $n$  Punkten beginnt, nicht länger als  $3n - 1$  Züge dauert (unabhängig von der Strategie der Spieler).
- (b) \*Beweisen Sie, dass ein Spiel, das mit  $n$  Punkten beginnt, mindestens  $2n$  Züge dauert (unabhängig von der Strategie der Spieler).
- (c) \*(„Brussels Sprouts“) Wir ändern die Spielregeln ein wenig. Statt Punkten zeichnen wir kleine Kreuze, und in jedem Zug wird ein neu hinzugefügtes Kreuz mit den „Ärmchen“ zweier vorhandenen Kreuze verbunden (d.h. die Ecken haben mit der neuen Regel Maximalgrad 4). Ein Beispiel:



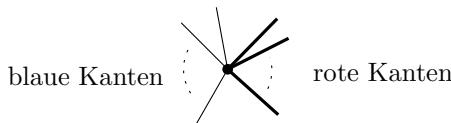
Beweisen Sie, dass dieses Spiel stets genau  $5n - 2$  Züge dauert (so dass von Anfang an klar ist, wer gewinnen wird).

8. Betrachten Sie eine Menge  $G$  mit  $n \geq 2$  Geraden in der Ebene. Keine zwei Geraden seien parallel, aber es kann vorkommen, dass sich mehr als zwei Geraden in einem Punkt schneiden. Wenn man diese Geraden zeichnet, dann entstehen Ecken (Schnittpunkte von Geraden), Kanten

<sup>10</sup>Englisch sprout = Spross, Sprössling.

(Strecken auf den Geraden zwischen zwei Schnittpunkten und Halbgeraden, die sich vom ersten und letzten Schnittpunkt auf jeder Geraden ins Unendliche erstrecken) und Länder (zusammenhängende Gebiete der Ebene nach Entfernen der Geraden).

- (a) \*Drücken Sie die Kantenzahl mittels der Ecken- und Länderzahl aus.
  - (b) Beweisen Sie: Außer wenn sich alle Geraden in einem Punkt schneiden, gibt es höchstens  $n$  Länder, die durch zwei (einseitig unendliche) Kanten begrenzt werden.
  - (c) \*Beweisen Sie: Außer wenn sich alle Geraden in einem Punkt schneiden, gibt es mindestens einen Punkt, in dem sich genau zwei Geraden schneiden. (Dies ist das berühmte *Problem von Sylvester*.)
9. \*\*Betrachten Sie einen beliebigen topologischen ebenen Graphen. Angenommen, jede Kante ist mit einer von zwei Farben (rot oder blau) gefärbt. Zeigen Sie, dass es eine Ecke von folgendem Typ geben muss:



(Wenn man die Ecke zyklisch umläuft, dann bilden die roten Kanten einen Block und ebenso die blauen; einer der beiden Blöcke kann leer sein.)

## 6.4 Das Vier–Farben–Problem

Wir betrachten eine politische Landkarte, in der die Ländergrenzen eingezeichnet sind wie in Abb. 6.2. Wir nehmen an, dass das Staatsgebiet jedes Landes zusammenhängend ist (aus diesem Grund haben wir Inseln wie die Britische, Sizilien, Sardinien oder Korsika in unserer schematischen Darstellung ausgelassen, und wir mussten sogar Russland auslassen — im Jahr 1997 ein nicht zusammenhängender Staat!). Wir sehen zwei Länder als benachbart an, wenn sie ein Stück gemeinsame Grenze haben; dieses gemeinsame Grenzstück darf sehr kurz sein, aber es muss schon eine Grenzlinie sein, ein oder mehrere gemeinsame Grenzpunkte reichen nicht aus (doch diese Situation kommt auf realen Landkarten ohnehin nicht besonders häufig vor). Wir möchten nun jedes Land mit einer Farbe einfärben, und zwar so, dass keine zwei benachbarten Länder die gleiche Farbe erhalten (wie es sich für eine politische Karte gehört). Was ist die minimale



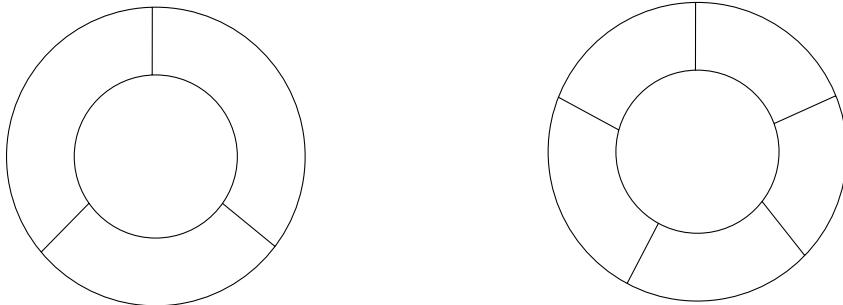
**Abb. 6.2** Eine Beispielkarte für das Vier–Farben–Problem.

Anzahl von Farben, mit der man so eine Färbung vornehmen kann? Bei der in Abb. 6.2 gezeigten Karte kommt man mit vier Farben aus (finden Sie so eine Färbung!).

Dies ist eines der bekanntesten kombinatorischen Probleme:

**6.4.1 Problem (Vier–Farben–Problem).** Kann man jede ebene Landkarte mit vier oder weniger Farben färben?

Mit weniger als vier Farben kommt man im Allgemeinen sicher nicht aus, wie man an obiger Karte sieht (z.B. an Luxemburg oder Österreich) oder an den Beispielen in Abbildung 6.3. Hier beweisen wir, dass man jede Landkarte mit fünf Farben färben kann. Diese Tatsache ist schon seit mehr als hundert Jahren bekannt; im Gegensatz dazu wurde das Vier–Farben–Problem erst Mitte der 1970er Jahre (positiv) beantwortet (man kann also auch vom Vier–Farben–Satz sprechen). Die bisher bekannten Beweise für die Tatsache, dass sich jede ebene Landkarte mit vier Farben färben lässt, sind kompliziert und hängen ganz wesentlich davon ab, eine große Anzahl von



**Abb. 6.3** Zum Färben dieser Landkarten benötigt man mindestens vier Farben.

Fällen mit dem Computer zu analysieren. Bisher hat noch niemand einen computerfreien Beweis geliefert, auch wenn der ursprüngliche Beweis 1995 wesentlich vereinfacht werden konnte (Robertson et al. [46]). Im Jahr 2004 gelang Gonthier [40] ein vollständig vom Computer durchführbarer Beweis. Er übersetzt das Problem in eine geeignete formale Sprache, und in dieser Sprache erzeugt er auch einen Beweis, dessen Korrektheit sich mit Hilfe eines einfachen, relativ allgemeinen Programms vollständig automatisch überprüfen lässt. Allein die Tatsache, dass die formale Aussage wirklich den Vier–Farben–Satz ausdrückt, muss noch vom Menschen überprüft werden.

Einige grundlegende Ideen, auf denen diese schwierigen Beweise beruhen, kommen auch schon im Beweis des „Fünf–Farben–Satzes“ vor.

Das Vier–Farben–Problem sieht nach einer geometrischen Fragestellung aus, doch es kann rein kombinatorisch formuliert werden. Das Färben der Länder einer Landkarte entspricht nämlich dem Färben der Ecken eines ebenen Graphen. Als erstes definieren wir, was wir unter einer Färbung eines beliebigen Graphen verstehen wollen.

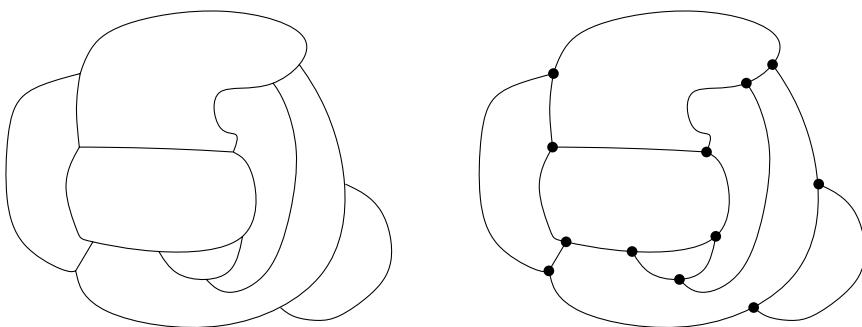
**6.4.2 Definition (Chromatische Zahl).** Sei  $G = (V, E)$  ein Graph und sei  $k$  eine natürliche Zahl. Eine Abbildung  $c: V \rightarrow \{1, 2, \dots, k\}$  heißt eine Färbung<sup>11</sup> des Graphen  $G$ , wenn  $c(x) \neq c(y)$  für jede Kante  $\{x, y\} \in E$  gilt. Die chromatische Zahl von  $G$ , abgekürzt  $\chi(G)$ , ist die kleinste Zahl  $k$ , so dass es eine Färbung  $c: V(G) \rightarrow \{1, 2, \dots, k\}$  gibt.

---

<sup>11</sup> Manchmal sagt man auch *zulässige Färbung* von  $G$ .

Die chromatische Zahl eines Graphen gehört zu den ganz wichtigen kombinatorischen Konzepten. In diesem Buch kommt sie trotzdem nur in diesem Abschnitt vor.

Mathematisch kann man eine Landkarte als Zeichnung eines planaren Graphen auffassen. Die Länder der Landkarte sind die Länder des Graphen, die Ecken des Graphen sind die Punkte, die auf der Grenze von drei oder mehr Ländern liegen, und die Kanten des Graphen sind die Grenzabschnitte zwischen den Ecken:



Sie sehen, dass in solchen Landkarten–Graphen Mehrfachkanten vorkommen können.

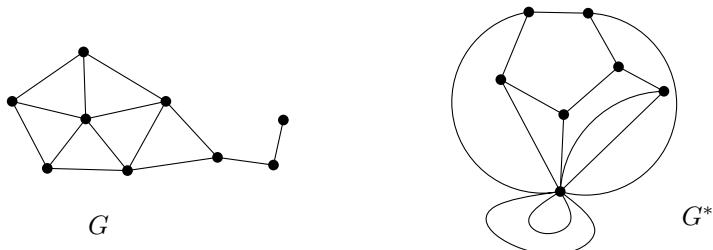
Wir wollen nun das Kartenfärbungsproblem (d.h. Färben der Länder eines topologischen ebenen Graphen) übersetzen in ein Problem, in dem die Ecken eines Graphen (im Sinne der eben gegebenen Definition) zu färben sind. Dazu führen wir den so genannten dualen Graphen ein. Stellen Sie sich vor, dass die Hauptstädte von je zwei Ländern mit einer Autobahn verbunden sind, die nur auf dem Territorium dieser beiden Länder liegt und die gemeinsame Grenze an einer Stelle kreuzt. Wenn wir die Hauptstädte und die verbindenden Autobahnen in die gegebene Landkarte einzeichnen, erhalten wir den dualen Graphen: Die Ecken des dualen Graphen sind die Hauptstädte und die Kanten sind die Autobahnen.

Um den dualen Graphen formal zu definieren, müssen wir Mehrfachkanten und Schlingen zulassen; wir vergegenwärtigen uns deshalb eine Möglichkeit, sie einzuführen. Ein Graph mit Mehrfachkanten und Schlingen kann als ein Tripel  $(V, E, \varepsilon)$  repräsentiert werden, wobei  $V$  und  $E$  disjunkte Mengen sind und  $\varepsilon: E \rightarrow \binom{V}{2} \cup V$  eine Abbildung ist, die jeder Kante ihre zwei Enden und jeder Schlinge ihre Endencke zuordnet (siehe Abschnitt 4.4 für eine detailliertere

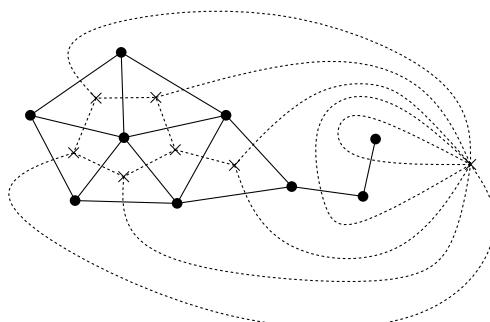
Diskussion). Nun sind wir bereit für eine mathematische Definition des dualen Graphen:

**6.4.3 Definition (Dualer Graph).** Sei  $G$  ein topologischer ebener Graph, d.h. ein ebener Graph  $(V, E)$  mit einer festen ebenen Zeichnung. Mit  $\mathcal{F}$  bezeichnen wir die Menge der Länder von  $G$ . Wir definieren einen Graphen  $(\mathcal{F}, E, \varepsilon)$ , möglicherweise mit Schlingen und Mehrfachkanten, indem wir  $\varepsilon(e) = \{F_i, F_j\}$  setzen, wenn die Kante  $e$  ein gemeinsames Stück Grenze der Länder  $F_i$  und  $F_j$  ist (wir erlauben auch  $F_i = F_j$ , wenn das gleiche Land auf beiden Seiten einer gegebenen Kante liegt). Dieser Graph  $(\mathcal{F}, E, \varepsilon)$  heißt der (geometrische) duale Graph von  $G$  und wird oft  $G^*$  geschrieben.

Ein Beispiel:



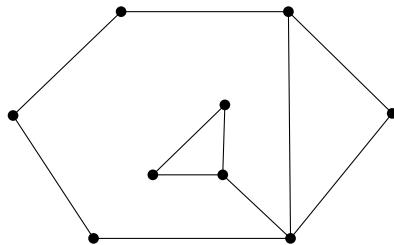
Den dualen Graphen  $G^*$  kann man in die Zeichnung des Graphen  $G$  mit einzeichnen, wie wir es in der anschaulichen Erklärung mit den Hauptstädten und Autobahnen schon vorgeschlagen haben. Wir wählen einen Punkt  $b_F$  in jedem Land  $F$  von  $G$ , und für jede Kante  $e$  von  $G$  zeichnen wir eine Kurve, die  $e$  kreuzt und die Punkte  $b_F$  und  $b_{F'}$  miteinander verbindet, wobei  $F$  und  $F'$  die Länder sind, an die die Kante  $e$  angrenzt. Diese Kurve liegt vollständig in den Ländern  $F$  und  $F'$ . Auf diese Art erhalten wir eine ebene Zeichnung von  $G^*$ :



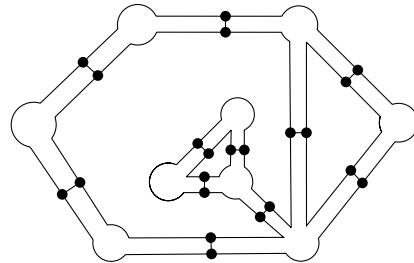
Diese Art der Zeichnung des dualen Graphen macht zugleich seine Planarität offensichtlich. Weitere Beispiele dualer Graphen finden sich in Abb. 6.1. Der Würfelgraph und der Oktaedergraph sind dual zueinander, die Graphen von Dodekaeder und Ikosaeder sind dual zueinander, und schließlich ist der Tetraedergraph (d.h.  $K_4$ ) zu sich selbst dual.

Betrachten Sie eine ebene Landkarte und sehen Sie sie als eine Zeichnung eines ebenen Graphen  $G$  an, wie oben beschrieben. Diese Landkarte lässt sich genau dann mit  $k$  Farben färben, wenn sich die Ecken des dualen Graphen  $G^*$  mit  $k$  Farben färben lassen.

Andererseits erhält man jeden ebenen Graphen als einen Teilgraphen eines geeigneten dualen Graphen. Wir deuten den Beweis nur mit einem Bild an: Z.B. ist der Graph



im dualen Graphen von



enthalten. (Alternativ kann man argumentieren, dass jeder topologische ebene Graph isomorph zum dualen Graphen des dualen Graphen ist.) Deshalb lassen sich Färbungsprobleme von Landkarten umformulieren als Probleme über die (Ecken-) Färbbarkeit ebener Graphen. Insbesondere können wir nun fragen:

**6.4.4 Problem (Nochmals das Vier–Farben–Problem).** Gilt  $\chi(G) \leq 4$  für jeden ebenen Graphen  $G$ ?

Wir beweisen ein schwächeres Resultat:

**6.4.5 Hilfssatz (Fünf–Farben–Satz).** Für jeden ebenen Graphen  $G$  gilt  $\chi(G) \leq 5$ .

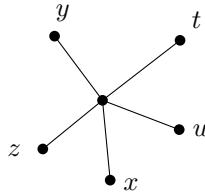
*Erster Beweis.* Wir führen Induktion über die Eckenzahl des Graphen  $G = (V, E)$ . Für  $|V| \leq 5$  ist die Aussage wahr.

Aus Abschnitt 6.3 wissen wir, dass jeder ebene Graph eine Ecke  $v$  vom Grad höchstens 5 hat. Wenn es sogar eine Ecke  $v$  mit  $\deg_G(v) < 5$  gibt, dann betrachten wir den Graphen  $G - v$ , den wir nach Induktionsvoraussetzung mit den Farben  $1, 2, \dots, 5$  färben können. Für die Ecke  $v$  wählen wir eine Farbe  $i \in \{1, 2, \dots, 5\}$ , die unter den (höchstens vier) Farben der Nachbarn von  $v$  nicht vorkommt. So erhalten wir eine Färbung von  $G$  mit (höchstens) fünf Farben.

Mit genau diesem Argument zeigt man, dass die chromatische Zahl jedes ebenen Graphen höchstens 6 ist. Im weiteren Verlauf dieses Beweises arbeiten wir also nur noch an der Verbesserung dieser 6 auf 5.

Es ist auch instruktiv, auf Grundlage dieses Beweises einen Algorithmus zu formulieren, der beliebige ebene Graphen mit höchstens sechs Farben färbt (oder unter Verwendung der noch folgenden Verbesserungen mit höchstens fünf Farben). So ein Algorithmus färbt die anfangs gewählte Ecke  $v$  (von kleinem Grad) ganz zum Schluss, nachdem alle anderen Ecken gefärbt sind.

Es bleibt noch der Fall, dass  $\deg_G(v) = 5$ . Betrachten wir den Graph  $G$  mit einer festen ebenen Zeichnung, und seien  $t, u, x, z, y$  die Nachbarn von  $v$  in zyklischer Reihenfolge in der gewählten Zeichnung (z.B. im Uhrzeigersinn).



Wieder betrachten wir eine Färbung  $c: V(G - v) \rightarrow \{1, 2, \dots, 5\}$  des Graphen  $G - v$  mit fünf Farben, deren Existenz uns die Induktionsvoraussetzung garantiert. Wenn unter den Nachbarn von  $v$  nur vier oder weniger Farben vorkommen, dann ist noch eine Farbe für  $v$  frei, die unter den Nachbarn nicht vorkommt. In diesem Fall wären wir am Ziel; also nehmen wir an, dass die Nachbarn von  $v$  alle verschiedene Farbe haben. Wir betrachten die Ecken  $x$  und  $y$  und definieren  $V_{x,y}$  als die Menge aller Ecken im Graphen  $G - v$ , die mit  $c(x)$  oder mit  $c(y)$  gefärbt sind. Auf jeden Fall sind  $x, y \in V_{x,y}$ . Es

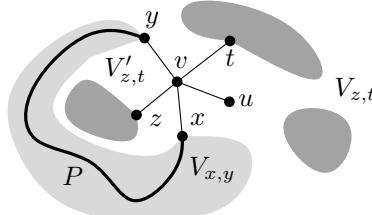
kann nun sein, dass es in  $G - v$  einen Weg von  $x$  nach  $y$  gibt, der nur Ecken aus  $V_{x,y}$  benutzt, es kann aber auch sein, dass nicht. Wir unterscheiden diese zwei Fälle.

1. Es gibt keinen solchen Weg. Sei  $V'_{x,y}$  die Menge aller Ecken  $s \in V(G - v)$ , die von  $x$  aus erreicht werden können über einen Weg, der nur Ecken aus  $V_{x,y}$  verwendet. Insbesondere haben wir  $y \notin V'_{x,y}$ . Wir definieren eine neue Färbung  $c'$  des Graphen  $G - v$ :

$$c'(s) = \begin{cases} c(s) & \text{wenn } s \notin V'_{x,y} \\ c(y) & \text{wenn } s \in V'_{x,y} \text{ und } c(s) = c(x) \\ c(x) & \text{wenn } s \in V'_{x,y} \text{ und } c(s) = c(y) \end{cases}$$

(das bedeutet, dass wir die Farben auf der Menge  $V'_{x,y}$  austauschen). Man sieht leicht, dass  $c'$  wieder eine Färbung von  $G - v$  ist, und weil  $c'(x) = c'(y) = c(y)$  ist, können wir  $c'(v) = c(x)$  setzen, womit wir eine zulässige Färbung von  $G$  mit fünf Farben erhalten.

2. Es gibt einen solchen Weg  $P$  von  $x$  nach  $y$  mit allen Ecken in  $V_{x,y}$ . In diesem Fall betrachten wir die beiden Ecken  $t$  und  $z$  und definieren eine Menge  $V_{t,z}$  als die Menge derjenigen Ecken aus  $G - v$ , die mit den Farben  $c(t)$  und  $c(z)$  gefärbt sind. Die Mengen  $V_{x,y}$  und  $V_{t,z}$  sind disjunkt. In der Zeichnung bildet der Weg  $P$  zusammen mit den Kanten  $\{v, x\}$  und  $\{v, y\}$  einen Kreis:



Einer der Punkte Punkte  $z, t$  liegt im Inneren des Kreises und der andere im Äußeren, deshalb muss jeder Weg von  $z$  nach  $t$  eine Ecke benutzen, die auf dem Kreis liegt. Also kann es keinen Weg von  $z$  nach  $t$  geben, der ausschließlich Ecken aus der Menge  $V_{z,t}$  benutzt; wenn wir mit den Ecken  $z$  und  $t$  in den Rollen von  $x$  und  $y$  in Fall 1 gehen, können wir eine Färbung von  $G$  mit fünf Farben konstruieren.

Damit haben wir den Fünf–Farben–Satz bewiesen.  $\square$

**Kanten kontrahieren.** Wir möchten Ihnen noch einen zweiten Beweis für den Fünf–Farben–Satz zeigen, doch zuvor führen wir eine weitere wichtige Operation auf Graphen ein. Sei  $G = (V, E)$  ein (nicht unbedingt ebener) Graph und sei  $e \in E$  eine seiner Kanten. Die Kante  $e$  zu *kontrahieren* bedeutet, beide Enden von  $e$  miteinander zu identifizieren (so dass sie gemeinsam eine einzige Ecke bilden) und dann die Mehrfachkanten zu entfernen, die dabei möglicherweise entstanden sind. (Man kann sich auch vorstellen, dass die Kante  $e$  aus Gummi ist und sich zusammenzieht, bis beide Enden aufeinanderliegen.) Der so entstandene Graph wird mit  $G.e$  bezeichnet, heißt die *Kontraktion von  $G$  nach  $e$*  und ist formal wie folgt definiert:

$$G.e = (V', E'),$$

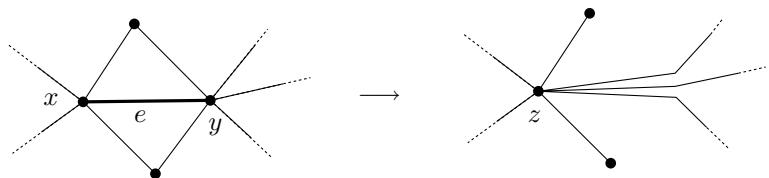
wobei  $e = \{x, y\}$  und

$$\begin{aligned} V' &= (V \setminus \{x, y\}) \cup \{z\} \\ E' &= \{e \in E : e \cap \{x, y\} = \emptyset\} \\ &\quad \cup \{\{z, t\} : t \in V \setminus \{x, y\}, \{t, x\} \in E \text{ oder } \{t, y\} \in E\}; \end{aligned}$$

dabei soll  $z \notin V$  die neue Ecke sein, die die alten Ecken  $x$  und  $y$  ersetzt.

**Lemma.** Ist  $G$  ein ebener Graph und  $e \in E(G)$  eine Kante, dann ist auch der Graph  $G.e$  eben.

„Beweis“. Mit einem Bild:



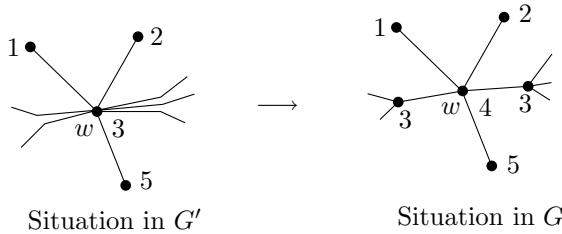
□

*Zweiter Beweis des Fünf–Farben–Satzes 6.4.5.* Wieder gehen wir induktiv (über die Eckenzahl des betrachteten ebenen Graphen  $G = (V, E)$ ) vor. Der Anfang ist wie im ersten Beweis bis zu der Stelle, wo wir einen ebenen Graphen  $G = (V, E)$  mit mindestens sechs Ecken haben, in dem jede Ecke Grad mindestens 5 hat. Wir wählen eine Ecke  $v$  vom Grad 5. Weil  $G$  planar ist, enthält er keinen  $K_5$  als Teilgraph, und deshalb gibt es ein Paar von Nachbarn von  $v$ , die nicht

durch eine Kante verbunden sind. In einem solchen Paar nennen wir die Ecken  $x$  und  $y$ , und die übrigen drei Nachbarn seien  $t, u$  und  $z$ . Wir schauen uns nun den Graphen  $G'$  an, der aus  $G$  durch Kontraktion der Kanten  $\{x, v\}$  und  $\{y, v\}$  entsteht (d.h. das Tripel  $x, y, v$  von Ecken wird durch eine einzige neue Ecke  $w$  ersetzt; Sie können die beiden Kanten nacheinander kontrahieren, Sie können dies aber auch als eine offensichtliche Verallgemeinerung der Definition einer einzelnen Kantenkontraktion ansehen). Dieser Graph ist planar und hat weniger Ecken als  $G$ . Deshalb gibt es nach Induktionsvoraussetzung eine Färbung  $c'$  von  $G'$  mit fünf Farben. In dieser Situation definieren wir eine Färbung  $c$  von  $G$  wie folgt:

$$c(s) = \begin{cases} c'(s) & \text{wenn } s \notin \{x, y, v\} \\ c'(w) & \text{wenn } s \in \{x, y\} \\ i \in \{1, \dots, 5\} \setminus \{c'(w), c'(u), c'(t), c'(z)\} & \text{wenn } s = v. \end{cases}$$

Das Bild unten illustriert diese Definition:



Es ist nicht schwer nachzuprüfen, dass die so definierte Funktion  $c$  wirklich eine zulässige Färbung des Graphen  $G$  ist.  $\square$

Noch ein weiterer Beweis kommt in Aufgabe 13.

Wir möchten noch bemerken, dass man die Frage der Färbbarkeit auch für Graphen untersuchen kann, die sich auf andere Flächen zeichnen lassen. Diese Fragestellung ist vollständig gelöst: die maximal mögliche chromatische Zahl eines Graphen vom Geschlecht  $k$  ist

$$\left\lfloor \frac{7 + \sqrt{1 + 48k}}{2} \right\rfloor.$$

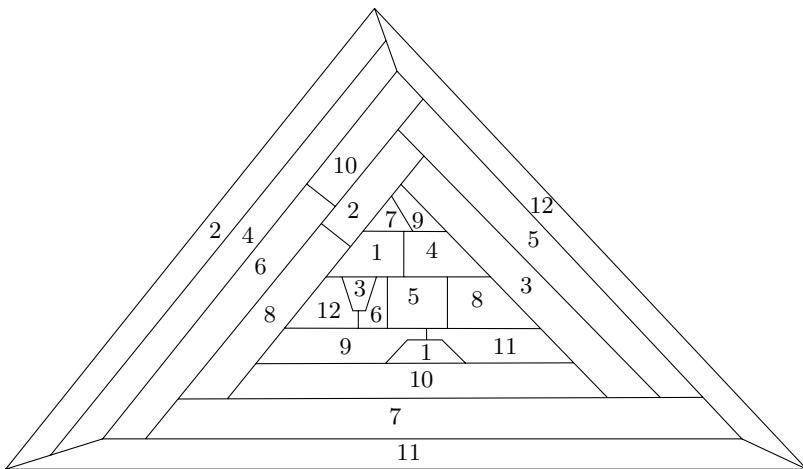
Bemerkenswert ist, dass der Fall des Geschlechts 0, d.h. der Fall ebener Graphen, der bei weitem schwierigste ist. Für  $k > 0$  wurde diese Formel (die Heawood–Formel) schon lange vor dem Vier–Farben–Satz bewiesen.

## Aufgaben

1. Beweisen Sie, dass  $\chi(G) \leq 1 + \max\{\deg_G(x) : x \in V\}$  für jeden (endlichen) Graphen  $G = (V, E)$  gilt.
  2. Für einen Graphen  $G$  ist  $\delta(G) = \min\{\deg_G(v) : v \in V\}$  der *Minimalgrad* von  $G$ . Beweisen Sie, dass  $\chi(G) \leq 1 + \max\{\delta(G') : G' \subseteq G\}$  ist, wobei  $G' \subseteq G$  bedeutet, dass  $G'$  ein Teilgraph von  $G$  ist.
  3. \*Ein Graph  $G$  heißt *außerplanar*, wenn er sich so zeichnen lässt, dass die Grenze eines der Länder (wir dürfen annehmen, dass es das äußere Land ist) alle Ecken von  $G$  enthält. Beweisen Sie, dass die chromatische Zahl eines außerplanaren Graphen höchstens 3 ist.
  4. Sei  $G$  ein dreiecksfreier ebener Graph (d.h. er enthält keinen  $K_3$  als Teilgraph). Beweisen Sie, dass  $\chi(G) \leq 4$ . (Ein schwierigerer Satz von Grötsch sagt, dass sogar  $\chi(G) \leq 3$  ist für alle ebenen dreiecksfreien Graphen.)
  5. *Inf* Entwerfen Sie auf der Grundlage der Beweise des Fünf–Farben–Satzes einen Algorithmus, der einen gegebenen ebenen Graphen mit höchstens fünf Farben färbt. Die Eingabe sei eine ebene Zeichnung des Graphen in der folgenden Form: Für jede Ecke  $v$  in  $G$  ist eine zyklische Liste ihrer Nachbarn gegeben, in der Reihenfolge, in der sie in der Zeichnung vorkommen.
  6. *Inf* (a) Betrachten Sie einen Greedy–Algorithmus zum Färben von Graphen: In jedem Schritt wählt er eine beliebige noch ungefärbte Ecke und färbt sie mit der kleinsten Farbe (die Farben sind ja natürliche Zahlen  $1, 2, \dots$ ), die unter den schon gefärbten Nachbarn dieser Ecke noch nicht vorkommt. Finden Sie zu jeder Zahl  $K$  einen bipartiten Graphen  $G$ , bei dem der Greedy–Algorithmus manchmal  $K$  oder mehr Farben benötigt (obwohl ein bipartiter Graph mit zwei Farben gefärbt werden kann).
    - (b) Finden Sie auch einen planaren Graphen  $G$ , der die in (a) beschriebene schlechte Eigenschaft hat?
    - (c) Man kann den Algorithmus etwas geschickter programmieren: Unter den noch ungefärbten Ecken wird eine mit maximalem Grad gewählt und wie in (a) gefärbt. Zeigen Sie, dass es wie in (a) immer noch Graphen  $G$  gibt, die sich nicht zu benehmen wissen.
    - (d) Sie könnten das als ein Spiel fortsetzen (z.B. für Ihren nächsten Spieletag). Die eine Mannschaft entwickelt Versionen des Greedy–Algorithmus zum Färben von Graphen, die anderen suchen nach Graphen, die sich gegenüber dem vorgeschlagenen Algorithmus renitent verhalten.
- Bemerkung.* Man weiß, dass kein polynomieller Algorithmus besonders sparsam mit der Anzahl der Farben sein kann, indem er z.B. jeden

3-färbaren Graphen mit garantiert weniger als  $K$  Farben färbt ( $K$  eine Konstante), es sei denn es gibt auch polynomiale Algorithmen für optimale Färbungen und viele weitere schwierige Probleme; das wird von den meisten für eher unwahrscheinlich gehalten.

7. Betrachten Sie eine Landkarte  $M$ , in der jeder Staat aus höchstens  $k$  zusammenhängenden Regionen besteht (ein etwas realistischeres Modell der wahren Situation). Zeigen Sie unter Verwendung von Aufgabe 2, dass die chromatische Zahl einer solchen Karte nicht größer als  $6k$  ist (wir bestehen natürlich darauf, dass für jeden Staat alle seine Regionen die gleiche Farbe erhalten).
8. Das folgende Bild ist ein Beispiel einer Landkarte, in der jeder Staat zwei Gebiete hat:



Beweisen Sie, dass die chromatische Zahl dieser Landkarte 12 ist.

9. Beweisen Sie, dass jeder Graph  $G$  mindestens  $(\chi_2^{(G)})$  Kanten hat.
10. (a) \*Betrachten Sie einen ebenen Graphen  $G$ , in dem alle Grade gerade sind. Beweisen Sie, dass man die Länder jeder beliebigen ebenen Zeichnung von  $G$  mit zwei Farben färben kann.  
(b) \*Beweisen mittels (a), dass es keinen topologischen ebenen Graphen gibt, bei dem alle Grade gerade sind, alle inneren Länder Dreiecke und das äußere Land ein Fünfeck.
11. \*Wir nennen einen Graphen  $H$  einen *Minor* eines Graphen  $G$ , wenn man durch wiederholte Anwendung der folgenden Operationen aus  $G$  einen Graphen erhalten kann, der isomorph zu  $H$  ist: Entfernen einer Kante, Entfernen einer isolierten Ecke, Kontrahieren einer Kante. Folgern Sie den folgenden Satz aus dem Satz von Kuratowski: Ein Graph  $G$  ist genau dann planar, wenn weder  $K_5$  noch  $K_{3,3}$  ein Minor von  $G$  ist.

12. (Listenfärbungen) Sei  $G = (V, E)$  ein Graph, und für jede Ecke  $v \in V$  sei eine endliche Liste  $L(v)$  natürlicher Zahlen gegeben. Eine Abbildung  $c: V \rightarrow \mathbb{N}$  heißt eine *Listenfärbung* von  $G$  (bezüglich der gegebenen Listen  $L(v)$ ,  $v \in V$ ), wenn  $c(v) \in L(v)$  ist für alle  $v \in V$  und  $c(v) \neq c(v')$  für alle  $\{v, v'\} \in E$ . Die *listenchromatische Zahl* von  $G$ , geschrieben als  $\chi_\ell(G)$ , ist die kleinste Zahl  $k$ , für die  $G$  eine Listenfärbung besitzt bezüglich aller Listen  $L(v)$ , wenn nur  $|L(v)| \geq k$  gilt.

- (a) Finden Sie ein Beispiel eines Graphen mit  $\chi_\ell(G) > \chi(G)$ .  
 (b) \*Konstruieren Sie für jede natürliche Zahl  $k$  einen bipartiten Graphen  $G$  mit  $\chi_\ell(G) > k$ .

*Bemerkung.* Es gibt einen ebenen Graphen  $G$  mit  $\chi_\ell(G) = 5$ .

13. \*Die Idee der Listenfärbungen aus der vorigen Aufgabe hat Thomasassen zu einem bemerkenswert einfachen Beweis des Fünf–Farben–Satzes 6.4.5 ausgebaut. Vollziehen Sie diesen Beweis nach, indem Sie induktiv (über die Eckenzahl) die folgende Behauptung beweisen:

Sei  $G = (V, E)$  ein topologischer ebener Graph mit Listen  $L(v)$ ,  $v \in V$ , und den folgenden Eigenschaften:

- Die Grenze des unbeschränkten Landes ist ein Kreis  $C$  mit Ecken  $v_1, v_2, \dots, v_k$  (in zyklischer Reihenfolge).
- Alle inneren Länder sind Dreiecke.
- $L(v_1) = \{1\}$ ,  $L(v_2) = \{2\}$ .
- $|L(v_i)| = 3$  für  $i = 3, 4, \dots, k$ .
- $|L(v)| = 5$  für alle Ecken, die von den  $v_i$  verschieden sind (d.h. die nicht auf dem äußeren Kreis  $C$  liegen).

Dann besitzt  $G$  eine Listenfärbung bezüglich der Listen  $L(v)$ .

Dieser Beweis braucht weder die Euler–Formel noch die Existenz einer Ecke kleinen Grades, er ist ein Beispiel einer vollständigen Induktion *par excellence*.



# 7

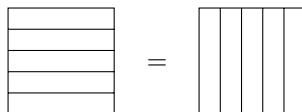
## Die Methode des Doppelten Abzählens

---

Früher, als es noch keine Computer gab, benutzten Rechnungsprüfer doppeltes Abzählen. Beim Addieren der Zahlen in einer Tabelle berechneten Sie erst die Summe der Zeilensummen und dann die Summe der Spaltensummen. Wenn sie sich nicht verrechnet hatten, dann mussten beide Resultate gleich sein. Mathematisch gesprochen, wenn  $A$  eine  $n \times m$  Matrix ist, dann ist

$$\sum_{i=1}^n \sum_{j=1}^m a_{ij} = \sum_{j=1}^m \sum_{i=1}^n a_{ij}.$$

Bildlich geschrieben:



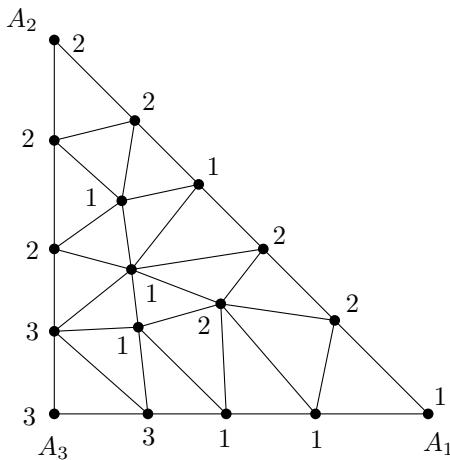
Mit Worten ausgedrückt: Man kann die Reihenfolge der Summanden in so einer doppelten Summe ändern, und das Ergebnis bleibt gleich. Diese einfache Idee liegt vielen mathematischen Tricks und Beweisen zu Grunde; in allen außer den einfachsten Fällen kommen natürlich weitere Ideen dazu. Meist ist die größte Schwierigkeit herauszufinden, was genau man doppelt abzählen sollte.

### 7.1 Paritätsargumente

In Abschnitt 4.3 ist uns das Handshake Lemma begegnet: *Jeder Graph hat eine gerade Anzahl von Ecken ungeraden Grades.* Bewiesen haben wir das mit doppeltem Abzählen (wir haben die „Enden von Kanten“ doppelt abgezählt). Mit diesem Resultat konnten wir einige Zahlentupel als Gradfolgen von Graphen ausschließen — zum

Beispiel das Quintupel  $(3, 3, 3, 3, 3)$ . Es gibt aber noch viele weitere interessante Anwendungen des Handshake Lemmas. So ermöglicht es zum Beispiel manchmal, die Existenz eines bestimmten Objekts zu beweisen. Zu diesem Zweck formulieren wir die Behauptung leicht um: *Wenn wir wissen, dass ein Graph  $G$  mindestens eine Ecke ungeraden Grades hat, dann muss er mindestens zwei solche Ecken haben.* Als Nächstes zeigen wir eine hübsche Anwendung.

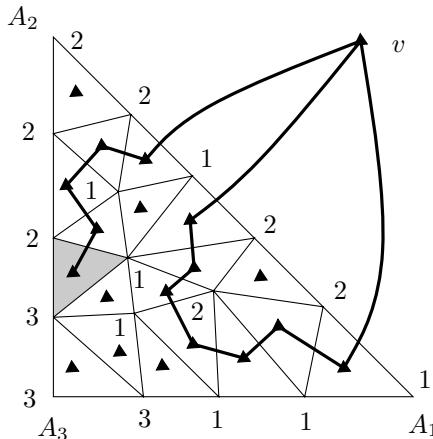
Wir zeichnen ein großes Dreieck mit den Ecken  $A_1, A_2, A_3$  in die Ebene und unterteilen es auf beliebige Weise in endlich viele kleinere Dreiecke, so wie im folgenden Bild:



Keine Ecke eines Dreiecks soll auf einer Kante eines der anderen kleinen Dreiecke liegen, so dass wir das Bild, das auf diese Weise entsteht, als eine Zeichnung eines ebenen Graphen interpretieren können, dessen innere Länder alle den Umfang 3 haben. Wir markieren die Ecken des großen und der kleinen Dreiecke mit den Zahlen 1, 2, 3 und beachten dabei die folgenden Regeln: Die Ecke  $A_i$  erhält die Markierung  $i$ ,  $i = 1, 2, 3$ ; und alle Ecken, die auf der (großen) Dreiecksseite zwischen  $A_i$  und  $A_j$  liegen, erhalten als Markierung entweder  $i$  oder  $j$ . Weitere Bedingungen stellen wir nicht.

**7.1.1 Hilfssatz (Sperner–Lemma — ebene Version).** *In der eben geschilderten Situation gibt es stets ein kleines Dreieck, dessen Ecken alle drei verschiedenen Markierungen 1, 2, 3 tragen.*

*Beweis.* Wir definieren einen Hilfsgraphen  $G$ ; siehe Abb. 7.1. Seine Ecken sind die Länder unserer Triangulierung, d.h. alle kleinen Dreiecke sowie das äußere Land. In der Abbildung sind die Ecken



**Abb. 7.1** Illustration zum Beweis des Sperner-Lemmas.

als kleine schwarze Dreiecke in die zugehörigen Länder eingezeichnet. Die Ecke für das äußere Land nennen wir  $v$ . Zwei Ecken in  $G$  sind durch eine Kante verbunden, wenn die entsprechenden Länder in der ursprünglichen Zeichnung benachbart sind und die Grenzkante zwischen ihnen die Markierungen 1 und 2 trägt. Das betrifft auch die Ecke  $v$  für das äußere Land: Sie ist mit all jenen kleinen Dreiecken benachbart, die mit einer 1-2-markierten Seite an das große Dreieck stoßen.

In diesem Graphen  $G$  kann ein kleines Dreieck nur dann mit einem seiner angrenzenden Dreiecke verbunden sein, wenn eine seiner Seiten die Markierung 1 und eine andere die Markierung 2 trägt. Wenn die dritte Ecke auch mit 1 oder 2 markiert ist, dann ist das kleine Dreieck mit genau zwei der angrenzenden Dreiecke verbunden. Trägt die dritte Ecke die Markierung 3, dann ist das betrachtete Dreieck mit genau einem angrenzenden Dreieck verbunden, und *dies ist der einzige Fall, in dem der Grad eines kleinen Dreiecks im Graphen  $G$  ungerade ist*. Wir zeigen nun, dass die Ecke  $v$  (welche dem Gebiet um das große Dreieck entspricht) in  $G$  ungeraden Grad hat. Dann gibt es nach dem Handshake-Lemma mindestens eine weitere Ecke ungeraden Grades in  $G$ , und dies ist das gesuchte kleine Dreieck mit Markierungen 1, 2, 3.

Die Kanten des Graphen  $G$ , die zu  $v$  inzident sind, können offensichtlich nur die Seite  $A_1A_2$  des großen Dreiecks kreuzen. Nach den Markierungsregeln sind alle Ecken auf dieser Seite mit 1 oder mit 2

markiert. Wenn wir die Folge dieser Markierungen niederschreiben, beginnend bei  $A_1$  und endend bei  $A_2$ , dann hat  $v$  gerade so viele Nachbarn, wie in dieser Folge Wechsel zwischen 1 und 2 vorkommen (d.h. so oft, wie auf einen Block von Einsen ein Block von Zweien folgt oder andersherum). Weil die Folge mit einer 1 beginnt und mit einer 2 endet, muss die Anzahl dieser Wechsel ungerade sein. Also hat  $v$  ungeraden Grad in  $G$ .  $\square$

Das Sperner-Lemma ist mehr als nur eine hübsche Aussage; es ist ein wesentlicher Schritt im Beweis eines berühmten Satzes. Bevor wir diesen Satz formulieren, sehen wir uns zum Aufwärmen ein einfacheres Ergebnis von ähnlicher Art an.

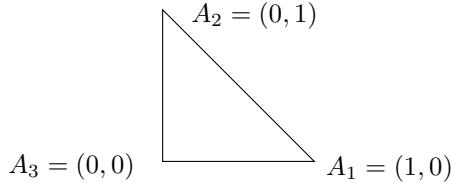
**7.1.2 Hilfssatz (Eindimensionaler Fixpunktsatz).** *Jede stetige Funktion  $f: [0, 1] \rightarrow [0, 1]$  besitzt einen Fixpunkt, das heißt ein  $x \in [0, 1]$  mit der Eigenschaft  $f(x) = x$ .*

Diesen Hilfssatz kann man durch Untersuchung der Funktion  $g(x) = f(x) - x$  beweisen. Die Funktion  $g$  ist stetig mit  $g(0) \geq 0$  und  $g(1) \leq 0$ . Nun ist es intuitiv ziemlich klar, dass der Graph einer solchen stetigen Funktion nicht über die  $x$ -Achse hinüberspringen kann und sie deshalb schneiden muss, also nimmt  $g$  an irgendeiner Stelle in  $[0, 1]$  den Wert 0 an. Die Existenz so einer Stelle streng zu beweisen erfordert doch etwas Arbeit; sie wird uns von der Analysis abgenommen („Nullstellensatz“).

Allgemein heißen solche Sätze Fixpunktsätze, die eine Aussage darüber machen, dass eine Funktion  $f$  unter bestimmten Umständen einen Fixpunkt haben muss, d.h. dass es ein  $x$  gibt mit  $f(x) = x$ . Solche Sätze gehören in vielen Gebieten der Mathematik zu den Schlüsselresultaten. Sie dienen oft zum Beweis der Existenz einer Lösung von Gleichungen verschiedener Typen (Differentialgleichungen, Integralgleichungen, usw.). Sie spielen sogar in der Theorie der Bedeutung von Computerprogrammen, der so genannten Semantik von Programmiersprachen, eine Rolle.

Im Brouwerschen Fixpunktsatz ist das eindimensionale Intervall aus Hilfssatz 7.1.2 durch eine Dreieck in der Ebene ersetzt, oder durch ein Tetraeder im dreidimensionalen Raum, oder durch das Analogon in noch höherer Dimension (ein Simplex). Hier beweisen wir nur die zweidimensionale Version, denn wir haben das Sperner-Lemma nur in zwei Dimensionen bewiesen (siehe aber Aufgabe 5). Auch wenn der Beweis eher in die Analysis gehört, werden wir ihn dennoch präsentieren, und wir werden versuchen, mit einem Minimum an Begriffen und Tatsachen aus der Analysis auszukommen; an die verwendeten Tatsachen werden wir jeweils kurz erinnern.

Sei  $\Delta$  ein Dreieck in der Ebene. Der Einfachheit halber nehmen wir das Dreieck mit den Ecken  $A_1 = (1, 0)$ ,  $A_2 = (0, 1)$  und  $A_3 = (0, 0)$ :



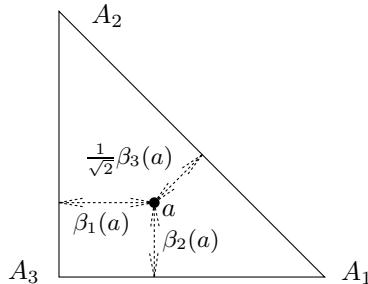
Eine Funktion  $f: \Delta \rightarrow \Delta$  heißt *stetig*, wenn es für jedes  $a \in \Delta$  und für jedes  $\varepsilon > 0$  ein  $\delta > 0$  gibt, so dass jeder Punkt  $b \in \Delta$ , dessen Abstand von  $a$  nicht größer als  $\delta$  ist, auf einen Punkt  $f(b)$  abgebildet wird, dessen Distanz von  $f(a)$  höchstens  $\varepsilon$  ist. Kurz gesagt: Die Bilder nahe beieinander liegender Punkte liegen nahe beieinander.

**7.1.3 Satz (Brouwerscher Fixpunktsatz, ebene Version).** Jede stetige Funktion  $f: \Delta \rightarrow \Delta$  besitzt einen Fixpunkt.

*Beweis.* Wir definieren drei reellwertige Hilfsfunktionen  $\beta_1$ ,  $\beta_2$  und  $\beta_3$  auf dem Dreieck  $\Delta$ . Für einen Punkt  $a \in \Delta$  mit Koordinaten  $(x, y)$  setzen wir

$$\beta_1(a) = x, \quad \beta_2(a) = y, \quad \beta_3(a) = 1 - x - y.$$

Die geometrische Bedeutung der  $\beta_i$  ist in der folgenden Illustration zu sehen:



Die beiden wichtigen Eigenschaften dieser Funktionen sind:  $\beta_i(a) \geq 0$  und  $\beta_1(a) + \beta_2(a) + \beta_3(a) = 1$  für alle  $a \in \Delta$ .

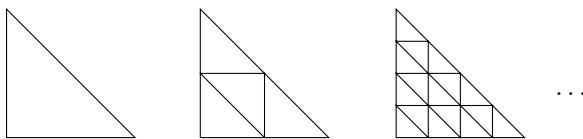
Des Weiteren definieren wir Mengen  $M_1, M_2, M_3 \subseteq \Delta$ :

$$M_i = \{a \in \Delta: \beta_i(a) \geq \beta_i(f(a))\}$$

für  $i = 1, 2, 3$ . Die Menge  $M_i$  besteht aus denjenigen Punkten, die durch die Funktion  $f$  von der Dreiecksseite, die der Ecke  $A_i$  gegenüber liegt, nicht weiter wegbewegt werden.

Jeder Punkt  $p \in M_1 \cap M_2 \cap M_3$  ist ein Fixpunkt der Funktion  $f$ , denn wäre  $p$  nicht fix, dann müsste  $f$  ihn von einer der Seiten wegbewegen. Genauer: Wenn  $p \in M_1 \cap M_2 \cap M_3$  ist, dann gilt  $\beta_i(p) \geq \beta_i(f(p))$  für alle  $i = 1, 2, 3$ , und weil  $\sum_i \beta_i(p) = \sum_i \beta_i(f(p)) = 1$  ist, erhalten wir  $\beta_i(p) = \beta_i(f(p))$  für alle  $i$ , woraus  $p = f(p)$  folgt. Unser Ziel ist nun, einen Punkt in der Schnittmenge  $M_1 \cap M_2 \cap M_3$  zu finden.

Betrachten wir eine Folge von immer feiner werdenden Triangulierungen des Dreiecks  $\Delta$ :



In jeder dieser Triangulierungen markieren wir alle Ecken der Dreiecke mit 1, 2 oder 3. Wir achten darauf, die Regeln aus dem Sperner-Lemma zu befolgen, und außerdem darauf, dass eine Ecke mit Markierung  $i$  zur Menge  $M_i$  gehört. Wir müssen uns nun noch vergewissern, dass das stets möglich ist.

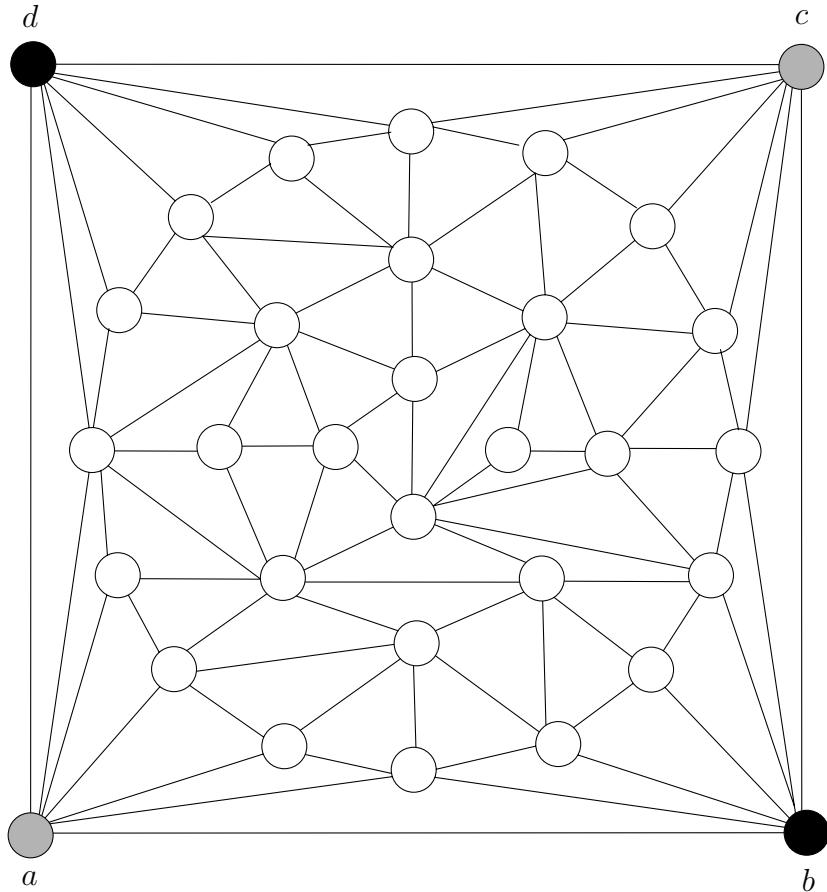
Die Ecke  $A_1$  hat den größtmöglichen Abstand von der ihr gegenüber liegenden Seite; deshalb kann der Abstand durch  $f$  nicht weiter vergrößert werden. Also ist  $A_1 \in M_1$  und wir können  $A_1$  mit 1 markieren; mit dem gleichen Argument können wir  $A_2$  mit 2 und  $A_3$  mit 3 markieren. Ein Punkt  $a$  auf der Seite  $A_1A_2$  erfüllt  $\beta_1(a) + \beta_2(a) = 1$ , woraus folgt, dass  $f(a)$  nicht zugleich  $\beta_1(f(a)) > \beta_1(a)$  und  $\beta_2(f(a)) > \beta_2(a)$  erfüllen kann. Daher ist  $a \in M_1 \cup M_2$ , und wir können alle Ecken auf der Seite  $A_1A_2$  mit 1 oder 2 markieren. Für die anderen Seiten funktioniert das entsprechende Argument. Und schließlich muss jeder Punkt in  $\Delta$  zu mindestens einer der Mengen  $M_i$  gehören, weil er nicht von allen drei Seiten gleichzeitig weiter entfernt werden kann. (Diesmal überlassen wir die Ausarbeitung der Details Ihnen.)

Nun folgt aus dem Sperner-Lemma 7.1.1, dass es in jeder der (immer feiner werdenden) Triangulierungen ein Dreieck mit Markierungen 1, 2, 3 gibt. Wir bezeichnen die Ecken eines solchen Dreiecks in der  $j$ -ten Triangulierung mit  $a_{j,1}, a_{j,2}$  und  $a_{j,3}$ , und zwar so, dass  $a_{j,i}$  jeweils zu  $M_i$  gehört (für  $i = 1, 2, 3$ ).

Wir betrachten die unendliche Folge von Punkten  $(a_{1,1}, a_{2,1}, a_{3,1}, \dots)$  und wählen darin eine unendliche konvergente Teilfolge. Das ist in jedem Falle möglich; es ist sogar so, dass jede unendliche Folge von Punkten in dem Dreieck eine konvergente Teilfolge enthält. (Diese Eigenschaft des Dreiecks nennt man *Kompaktheit* — eine Eigenschaft, die es z.B. mit jeder abgeschlossenen beschränkten Menge teilt.) Nehmen wir also an, wir haben eine konvergente Teilfolge  $(a_{j_1,1}, a_{j_2,1}, a_{j_3,1}, \dots)$  ausgewählt,  $j_1 < j_2 < j_3 < \dots$ , und nennen wir ihren Grenzwert  $p$ .

Wir behaupten, dass  $p \in M_1$  ist. Und wirklich gilt nach Definition von  $M_1$  die Ungleichung  $\beta_1(a_{j_k,1}) \geq \beta_1(f(a_{j_k,1}))$  für alle  $j_k$ , und wenn wir auf beiden Seiten zu einem Grenzwert übergehen, erhalten wir  $\beta_1(p) \geq \beta_1(f(p))$ , denn der Übergang zu einem Grenzwert erhält Ungleichungen zwischen stetigen Funktionen (zwar nicht „ $>$ “, aber „ $\geq$ “).

Weil die Durchmesser der Dreiecke in der Folge der Triangulierungen gegen 0 konvergiert, müssen die Folgen der anderen Ecken, d.h.  $(a_{j_1,2}, a_{j_2,2}, a_{j_3,2}, \dots)$  und  $(a_{j_1,3}, a_{j_2,3}, a_{j_3,3}, \dots)$ , auch gegen den Punkt



**Abb. 7.2** Ein Spielbrett.

$p$  konvergieren. Daraus folgt, dass auch  $p \in M_2$  und  $p \in M_3$  gelten. Somit ist  $p$  der gewünschte Fixpunkt der Funktion  $f$ .  $\square$

Man kennt noch eine Reihe komplizierterer Resultate, die dem Brouwerschen Fixpunktsatz ähneln. Zum Beispiel gibt es bei jeder stetigen Abbildung der Oberfläche einer dreidimensionalen Kugel in die Ebene zwei auf der Kugel gegenüber liegende Punkte, die auf den gleichen Punkt abgebildet werden (dies ist der Satz von Borsuk und Ulam). Solche Sätze beweist man in der *algebraischen Topologie*. Die Beweise verwenden in der Regel ziemlich komplexe Techniken, doch basieren sie im Grunde oft auf Paritätsargumenten wie dem Sperner-Lemma.

Wir wollen uns ein weiteres Beispiel dafür anschauen, wie nützlich das Handshake-Lemma ist. Wir werden ein Spiel analysieren, das

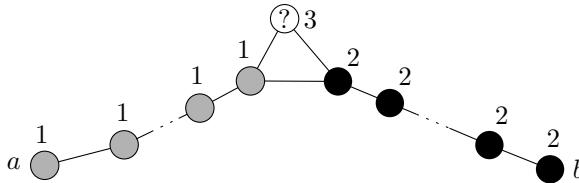
dem Spiel HEX sehr ähnlich ist. Gespielt wird auf einem Brett wie dem in Abb. 7.2 (die Triangulierung innerhalb des großen Quadrats kann auch anders aussehen). Die zwei Spielerinnen ziehen abwechselnd. Ein Zug besteht darin, ein Feld mit einem ihrer Spielsteine zu besetzen — anders ausgedrückt: ein Feld zu färben. Zum Beispiel färbt die erste Spielerin (Alice) Felder grau und die zweite Spielerin (Bettina) schwarz (langweilige Farben, die aber den Vorteil haben in einem schwarz-weißen Buch darstellbar zu sein). Die Felder  $a$  und  $c$  „gehören“ Alice und sind von Anfang an grau, die Felder  $b$  und  $d$  gehören Bettina und sind schwarz. Alice gewinnt, wenn es ihr gelingt, alle Knoten auf einem Weg von  $a$  nach  $c$  zu färben, und Bettina versucht einen schwarzen Weg von  $b$  nach  $d$  zu erzeugen. Wenn alle Felder gefärbt sind, ohne dass es einer Spielerin gelungen ist, ihre beiden Ecken durch so einen Weg zu verbinden, dann endet das Spiel unentschieden.

**7.1.4 Hilfssatz.** *Auf einem Spielbrett der beschriebenen Art (bei dem außen ein Quadrat ist und innen lauter Dreiecke) kann kein Spiel unentschieden enden.*

*Beweis.* Wir führen einen Widerspruchsbeweis: Angenommen, ein Spiel ist unentschieden ausgegangen. Wir nennen die Menge der von Alice gefärbten Felder  $A$ , und die Menge der von Bettina gefärbten Felder nennen wir  $B$ .

Nach den folgenden Regeln bringen wir nun Markierungen 1, 2, 3 an den Feldern an. Ein Feld in  $A$  wird mit 1 markiert, wenn es von ihm aus einen grauen Weg nach  $a$  gibt. Analog werden Felder in  $B$ , die von  $b$  aus mit einem schwarzen Weg erreichbar sind, mit 2 markiert. Alle übrigen Ecken erhalten die Markierung 3. Laut unserer Annahme sind die Ecken  $c$  und  $d$  beide mit 3 markiert, weil sonst eine der beiden Spielerinnen gewonnen hätte.

Wir werden zeigen, dass ein inneres Dreieck  $T$  die Markierungen 1, 2, 3 trägt. Das ist aber ein Widerspruch, weil die mit 3 markierte Ecke von  $T$  (nennen wir das Feld  $x$ ) weder zu  $A$  noch zu  $B$  gehören kann (und also noch ein Zug möglich ist). Würde  $x$  zu  $A$  gehören, dann wäre nämlich  $a$  über einen grauen Weg von  $x$  aus erreichbar, indem man zuerst zu dem mit 1 markierten Nachbarn  $y$  von  $x$  in  $T$  geht; weil  $y$  mit 1 markiert ist, gibt es einen grauen Weg von  $y$  nach  $a$ . Analog kann  $x$  nicht zu  $B$  gehören, ein Widerspruch. Das folgende Bild fasst die Argumentation noch einmal zusammen:



Und wie beweisen wir nun die Existenz eines Dreiecks mit Markierungen 1, 2, 3? Genauso wie das Sperner-Lemma. Dieser Teil sei Ihnen überlassen; ein sehr ähnliches Ergebnis stellen wir in Aufgabe 1 vor.  $\square$

In diesem Beweis haben wir wesentlich benutzt, dass alle inneren Länder Dreiecke sind und das äußere Land nur die vier Ecken  $a, b, c, d$  hat. Wenn beispielsweise auch im Inneren Vierecke zugelassen sind, dann könnte ein Spiel sehr wohl unentschieden enden.

In dem interessanten Buch von Berlekamp, Conway und Guy [15] werden verschiedene Spiele mathematisch analysiert.

## Aufgaben

1. Betrachten Sie eine Zeichnung eines ebenen Graphen, in der alle Länder Dreiecke sind (d.h. drei Ecken haben, auch das äußere). Schreiben Sie an jede Ecke eine der Zahlen 1, 2, 3, ohne sonst irgendwelche Regeln zu beachten. Beweisen Sie, dass es dann eine gerade Anzahl von Ländern gibt, an deren Ecken drei verschiedene Zahlen stehen, egal wie Sie die Zahlen verteilt haben.
2. Ein bekanntes Problem mit einem Bergwanderer geht auch um Fixpunkte. Der Wanderer geht um 6 Uhr in der Frühe los, einen Berg besteigen. Er erreicht den Gipfel um 6 Uhr abends und verbringt die Nacht oben (in einer Hütte). Am nächsten Morgen beginnt er den Abstieg wieder um 6 Uhr, und er nimmt exakt den gleichen Weg wie beim Aufstieg. Unterwegs rastet er oft um die Aussicht zu genießen, so dass er seinen Ausgangspunkt im Tal um 6 Uhr abends erreicht. Beweisen Sie, dass es eine Stelle gibt, an der sich unser Wanderer an beiden Tagen zur gleichen Uhrzeit befand.
3. Ein Bauingenieur steht in einer neu errichteten Wohnung und hält einen Grundriss von eben dieser Wohnung in Händen. Beweisen Sie, dass es einen Punkt auf dem Plan gibt, der genau über dem entsprechenden Punkt in der Wohnung liegt.
4. Entscheiden Sie, für welche der verschiedenen Mengen  $X$  aus der folgenden Liste der analoge Satz zum Brouwerschen Fixpunktsatz 7.1.3 gilt (d.h. jede stetige Funktion  $f: X \rightarrow X$  hat einen Fixpunkt). Wenn

er gilt, dann leiten Sie ihn aus Satz 7.1.3 her, und wenn nicht, dann geben Sie eine Funktion  $f$  als Gegenbeispiel an.

- (a)  $X$  ist ein Kreis in der Ebene (gemeint ist die Kreislinie, nicht die von ihr begrenzte Kreisscheibe);
- (b)  $X$  ist eine Kreisscheibe in der Ebene;
- (c)  $X$  ist ein Dreieck in der Ebene, in dem ein innerer Punkt fehlt;
- (d)  $X$  ist eine Sphäre im dreidimensionalen Raum (die Oberfläche einer Kugel);
- (e)  $X$  ist eine Sphäre im dreidimensionalen Raum, in der ein kleines kreisrundes Loch fehlt;
- (f)  $X$  ist der Torus (siehe Abschnitt 6.1);
- (g)  $X$  ist die Kleinsche Flasche (siehe Abschnitt 6.1).

5. (Sperner-Lemma in 3 Dimensionen)

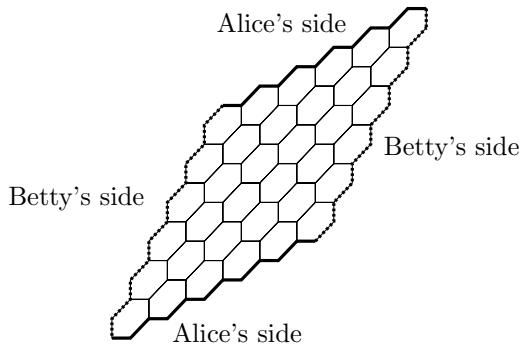
- (a) \*Betrachten Sie ein Tetraeder  $T = A_1A_2A_3A_4$  im dreidimensionalen Raum und eine Unterteilung von  $T$  in kleine Tetraeder, so dass jede Seitenfläche der kleinen Tetraeder entweder in einer der Seitenflächen des großen Tetraeders liegt oder zugleich eine Seitenfläche eines weiteren kleinen Tetraeders ist. Markieren Sie die Ecken der kleinen Tetraeder mit den Zahlen 1, 2, 3, 4, und zwar unter Beachtung der folgenden Regeln: Die Ecke  $A_i$  wird mit der Zahl  $i$  markiert, die Ecken auf der Kante  $A_iA_j$  werden mit  $i$  oder mit  $j$  markiert und die Ecken auf der Fläche  $A_iA_jA_k$  erhalten eine der Markierungen  $i$ ,  $j$  oder  $k$ . Beweisen Sie, dass es ein kleines Tetraeder gibt, dessen Ecken vier verschiedene Markierungen tragen.

- (b) Formulieren und beweisen Sie eine dreidimensionale Version des Brouwerschen Fixpunktsatzes (über stetige Abbildungen eines Tetraeders in sich selbst).

6. Betrachten Sie ein Spiel wie in Hilfssatz 7.1.4.

- (a) Beweisen Sie, dass auf jedem Spielbrett, welches die Bedingungen aus Hilfssatz 7.1.4 erfüllt, entweder Alice oder Bettina eine Gewinnstrategie hat (d.h. wenn sie keinen Fehler macht, gewinnt sie, egal wie die andere spielt).
- (b) Finden Sie ein Beispiel für ein Spielbrett, (das wieder die Bedingungen erfüllt und) auf dem Bettina eine Gewinnstrategie hat.
- (c) \*Zeigen Sie: Wenn das Spielbrett symmetrisch ist bezüglich der Drehung um 90 Grad (d.h. wenn es für beide Spielerinnen gleich aussieht), dann hat Alice immer eine Gewinnstrategie.

7. Vielleicht wissen Sie ja, dass das richtige Spiel HEX von Piet Hein erfunden wurde und auf einem wabenartigen Spielbrett gespielt wird:



Die Spielerinnen besetzen abwechselnd jeweils ein Feld mit einem Stein der eigenen Farbe. Ziel des Spiels ist für beide Spielerinnen, mit den eigenen Steinen ihre beiden Seiten zu verbinden.

- (a) Finden Sie heraus, wie dieses Spiel mit der im Text vorgestellten Version zusammenhängt.
- (b) Weil sie gerade kein HEX-Brett dabei haben, spielen Alice und Bettina HEX auf einem normalen Schachbrett. Alice versucht, zwei gegenüberliegende Seiten zu verbinden, und Bettina versucht es mit den beiden anderen Seiten; dabei gelten zwei Felder als benachbart, wenn sie eine Seite gemeinsam haben. Doch schon finden sie das Spiel ziemlich langweilig. Was meinen Sie, weshalb?

## 7.2 Der Satz von Sperner

Sie haben richtig gelesen: Dies ist das zweite Mal in diesem Kapitel, dass uns der Name Sperner begegnet, doch der Satz von Sperner, mit dem wir uns als nächstes befassen, handelt von etwas ganz anderem als das Sperner-Lemma aus dem vorigen Abschnitt. Es geht dabei um eine  $n$ -Menge  $X$  und ein System  $\mathcal{M}$  von Teilmengen von  $X$ . Wir nennen  $\mathcal{M}$  ein *Unabhängigkeitssystem*, wenn es keine zwei verschiedenen Mengen  $A, B \in \mathcal{M}$  enthält, so dass  $A \subset B$ . Bevor Sie nun weiter lesen, möchten Sie vielleicht einmal versuchen ein möglichst großes Unabhängigkeitssystem auf einer 4-Menge zu finden. Wie viele Mengen „passen“ in so ein System?

**7.2.1 Satz (Satz von Sperner).** Ein Unabhängigkeitssystem auf einer  $n$ -Menge kann höchstens  $\binom{n}{\lfloor n/2 \rfloor}$  Mengen enthalten.

Eigentlich ist dies ein Satz über partiell geordnete Mengen (Posets). Betrachten wir das Mengensystem  $2^X$ , das aus allen Teilmengen der Menge  $X$  besteht. Die Relation  $\subseteq$ , „Teilmenge sein“, ist eine partielle Ordnung auf  $2^X$  (es ist sogar eines der wichtigsten Beispiele

für partielle Ordnungen; siehe Kapitel 2). Ein Unabhängigkeitssystem ist nichts anderes als eine Menge paarweise unvergleichbarer Elemente in dem Poset  $(2^X, \subseteq)$ . Eine Menge paarweise unvergleichbarer Elemente in einem Poset bezeichnet man als *Antikette*; der Satz von Sperner liefert eine obere Schranke für die Größe einer Antikette in  $(2^X, \subseteq)$ .

Bevor wir zum Beweis des Satzes von Sperner kommen, machen wir uns klar, dass die angegebene obere Schranke bestmöglich (d.h. kleinstmöglich) ist, weil das System aller Teilmengen von  $X$  mit der Mächtigkeit  $\lfloor n/2 \rfloor$  ein Unabhängigkeitssystem der Größe  $\binom{n}{\lfloor n/2 \rfloor}$  ist.

*Beweis von Satz 7.2.1.* Zuerst sagen wir, was wir unter einer *Kette* von Teilmengen von  $X$  verstehen wollen: nämlich eine Menge  $\{A_1, A_2, \dots, A_k\}$  von Teilmengen von  $X$ , so dass  $A_1 \subset A_2 \subset \dots \subset A_k$ . In der Sprache der geordneten Mengen ist das einfach eine linear geordnete Teilmenge des Poset  $(2^X, \subseteq)$ .

Der Schlüssel zum Beweis ist die Beobachtung, dass eine Kette und eine Antikette höchstens ein gemeinsames Element haben können. Wenn es uns gelingt zu beweisen, dass das ganze betrachtete Poset als Vereinigung von höchstens  $r$  Ketten dargestellt werden kann, dann enthält automatisch keine Antikette mehr als  $r$  Elemente. In unserem Beweis werden wir diese einfache Beobachtung auf eine noch etwas raffiniertere Weise ausnutzen.

Wir betrachten die *maximalen Ketten* in  $(2^X, \subseteq)$ ; eine maximale Kette ist eine Kette, zu der man keine weitere Menge aus  $2^X$  hinzufügen kann ohne die Ketteneigenschaft zu zerstören. Man macht sich leicht klar, wie die maximalen Ketten aussehen: Sie enthalten für jede der möglichen Mächtigkeiten genau eine Teilmenge von  $X$ ; d.h. sie haben die Form

$$\emptyset \subset \{x_1\} \subset \{x_1, x_2\} \subset \{x_1, x_2, x_3\} \subset \dots \subset \{x_1, x_2, \dots, x_n\}, \quad (7.1)$$

wobei  $x_1, x_2, \dots, x_n$  alle Elemente von  $X$  sind, in einer beliebigen Reihenfolge. Deshalb induziert jede maximale Kette eine lineare Ordnung auf  $X$ , genauso wie andersherum jede lineare Ordnung genau eine maximale Kette ergibt. Folglich gibt es genauso viele maximale Ketten wie Permutationen auf  $X$ , also  $n!$ .

Sei  $\mathcal{M}$  eine Antikette (ein Unabhängigkeitssystem). Wir bilden alle geordneten Paare  $(\mathcal{R}, M)$ , wobei  $M \in \mathcal{M}$  eine Menge ist und  $\mathcal{R}$  eine maximale Kette, die  $M$  enthält. Wir zählen diese Paare auf zwei verschiedene Arten.

Zum einen enthält jede Kette (nach der obigen Beobachtung) höchstens ein  $M \in \mathcal{M}$ , weil  $\mathcal{M}$  eine Antikette ist; die Anzahl der Paare  $(\mathcal{R}, M)$  ist also höchstens gleich der der Anzahl der maximalen Ketten, und die ist  $n!$ .

Andererseits können wir eine Menge  $M \in \mathcal{M}$  nehmen und fragen, wie viele maximale Ketten sie enthalten. Eine maximale Kette der Form (7.1) enthält  $M$  genau dann, wenn  $\{x_1, x_2, \dots, x_k\} = M$ , wo bei  $k = |M|$  ist. Wir fragen also danach, wie viele lineare Ordnungen von  $X$  es gibt, bei denen die ersten  $k$  Elemente genau die Elemente aus  $M$  sind. Die Elemente von  $M$  können wir immer noch auf  $k!$  Arten anordnen, womit wir die ersten  $k$  Mengen der Kette festlegen, und die Elemente außerhalb von  $M$  können wir auf  $(n - k)!$  Arten anordnen, womit wir die restlichen Glieder der Kette bestimmen. Alles in allem ist  $M$  in  $k!(n - k)!$  maximalen Ketten enthalten. Deshalb ist die Anzahl der geordneten Paare  $(\mathcal{R}, M)$  gleich

$$\sum_{M \in \mathcal{M}} |M|!(n - |M|)!,$$

und nach der ersten Überlegung ist dieser Ausdruck höchstens  $n!$ . Nach Division der so erhaltenen Ungleichung durch  $n!$  wissen wir also, dass

$$\sum_{M \in \mathcal{M}} \frac{|M|!(n - |M|)!}{n!} = \sum_{M \in \mathcal{M}} \frac{1}{\binom{n}{|M|}} \leq 1. \quad (7.2)$$

Nun verwenden wir die Tatsache, dass der mittlere Binomialkoeffizient  $\binom{n}{\lfloor n/2 \rfloor}$  mindestens so groß ist wie jeder andere von der Form  $\binom{n}{k}$ ,  $k = 0, 1, \dots, n$ . Damit ergibt sich

$$1 \geq \sum_{M \in \mathcal{M}} \frac{1}{\binom{n}{|M|}} \geq |\mathcal{M}| \frac{1}{\binom{n}{\lfloor n/2 \rfloor}},$$

und damit das gewünschte Ergebnis  $|\mathcal{M}| \leq \binom{n}{\lfloor n/2 \rfloor}$ .  $\square$

Die bemerkenswerte Ungleichung (7.2) heißt die LYM-Ungleichung, nach ihren (voneinander unabhängigen) Entdeckern Lubell, Meshalkin und Yamamoto.

*Ein weiterer Beweis des Satzes von Sperner.* Wie so oft bei wichtigen Sätzen gibt es auch für den Satz von Sperner eine Reihe von Beweisen,

die wesentlich verschieden voneinander sind. An jedem der verschiedenen Beweise gibt es etwas neues zu lernen, oder man genießt einfach die schönen Ideen. Wir werden zwei weitere Beweise vorstellen. Der erste arbeitet mit einer geschickten Überdeckung von  $2^X$  mit Ketten eines speziellen Typs.

Betrachten wir eine Kette in dem Poset  $(2^X, \subseteq)$ , d.h. eine Folge von Mengen, die die jeweils vorangegangenen enthalten:  $M_1 \subset M_2 \subset \dots \subset M_t$ . Eine solche Kette nennen wir *symmetrisch*, wenn sie (für irgend-eine Zahl  $k$ ) genau eine Menge der Mächtigkeit  $k$  enthält, genau eine Menge mit  $k+1$  Elementen, genau eine mit  $k+2, \dots$ , genau eine mit  $n-k$  Elementen, und sonst keine weiteren Mengen. Für  $n=3$  ist beispielsweise die Kette, die aus den Mengen  $\{2\}$  und  $\{2,3\}$  besteht, symmetrisch, ebenso die Kette  $\{\emptyset, \{3\}, \{2,3\}, \{1,2,3\}\}$ , aber die Ketten  $\{\{1\}\}$  und  $\{\emptyset, \{1,2,3\}\}$  sind (in diesem Sinne) nicht symmetrisch. Eine *Partition in symmetrische Ketten* ist eine Methode,  $2^X$  als eine Vereinigung disjunkter symmetrischer Ketten zu schreiben.

Jede Partition in symmetrische Ketten (wenn es überhaupt eine gibt) muss aus genau  $\binom{n}{\lfloor n/2 \rfloor}$  symmetrischen Ketten bestehen, weil jede symmetrische Kette genau eine Menge der Mächtigkeit  $\lfloor n/2 \rfloor$  enthält. Jede Kette hat mit jedem Unabhängigkeitssystem höchstens eine Menge gemeinsam (dies war die wichtige Beobachtung im ersten Beweis des Satzes von Sperner). Daher ist der Satz von Sperner eine Konsequenz aus der folgenden

**Behauptung.** Für jede endliche Menge  $X$  hat das Poset  $2^X$  eine Partition in symmetrische Ketten.

*Beweis der Behauptung.* Ohne Beschränkung der Allgemeinheit können wir annehmen, dass  $X = \{1, 2, \dots, n\}$ . Der Beweis beruht auf der folgenden Konstruktion:

Jeder Menge  $M \subseteq X$  ordnen wir eine Folge „ $m_1 m_2 \dots m_n$ “ aus öffnenden und schließenden Klammern zu, und zwar nach folgender Regel:

$$m_i = \begin{cases} „(“ & \text{wenn } i \in M \\ „)“ & \text{wenn } i \notin M. \end{cases}$$

Z.B. erhalten wir für  $n=7$  und  $M=\{2,6\}$  die Folge „ $m_1 m_2 \dots m_7 = „()())()“$ . Die so erhaltene Klammer-Folge hat keine besonderen Eigenschaften, und ganz offensichtlich braucht sie keine „korrekte“ Beklammerung zu sein, d.h. die öffnenden und schließenden Klammern brauchen nicht ordentlich geschachtelt zu sein. Man kann in ihr jedoch eine „partielle Klammerschachtelung“ finden. Dazu fassen wir zuerst alle Paare „ $()$ “ aufeinanderfolgender Klammern zusammen. Dann beachten wir die schon zusammengefassten Klammern nicht weiter und verfahren mit den übrigen Klammern nach der gleichen Regel. Zwei Beispiele sollen das verdeutlichen:

$$\begin{array}{c}
 ) \underbrace{( \quad ) \quad )} \quad ) \underbrace{( \quad )} \\
 ) \quad ) \quad ( \quad \underbrace{(\quad) \quad (\quad)} \quad ) \quad ) \quad ( \\
 \end{array}$$

Am Ende dieser Prozedur des Zusammenfassens werden im Regelfall noch einige Klammern übrig sein. Die Regel für das Zusammenfassen bewirkt jedoch, dass die Folge der übrig gebliebenen Klammern in drei Teile zerfällt: In einen (möglicherweise leeren) Anfangsteil mit nur schließenden Klammern, einen (möglicherweise leeren) Mittelteil sowie ein (möglicherweise leeres) Ende mit nur öffnenden Klammern.

Wir sagen, dass zwei Folgen von Klammern die *gleiche partielle Schachtelung* haben, wenn die zusammengefassten Klammern in beiden Folgen die gleichen sind (und zwar an der gleichen Position). Dies ist der Fall bei den Folgen, die zu den drei nachstehenden Mengen (als Teilmengen von  $\{1, 2, \dots, 11\}$ ) gehören:

$$\begin{aligned}
 M_1 &= \{4, 5, 6, 8, 11\} \quad \dots \quad ) \quad ) \quad ) \quad ( \quad ( \quad ( \quad ( \quad ) \quad ( \\
 M_2 &= \{5, 6, 8, 11\} \quad \dots \quad ) \quad ) \quad ) \quad ) \quad ( \quad ( \quad ( \quad ( \quad ) \quad ( \\
 M_3 &= \{5, 6, 8\} \quad \dots \quad ) \quad ) \quad ) \quad ) \quad ( \quad ( \quad ( \quad ) \quad )
 \end{aligned}$$

Wenn zwei verschiedene Folgen die gleiche partielle Schachtelung haben, dann muss die eine mehr schließende Klammern im Anfangsteil haben als die andere oder mehr öffnende im Schlussteil. Eine andere Möglichkeit gibt es nicht. Daraus sieht man leicht, dass von zwei Mengen, deren zugehörige Folgen die gleiche partielle Schachtelung aufweisen, die eine eine Teilmenge der anderen sein muss.

Nun definieren wir eine Äquivalenzrelation  $\sim$  auf der Menge  $2^X$ , in der genau dann  $M \sim M'$  gilt, wenn die zu  $M$  und zu  $M'$  gehörenden Klammerfolgen die gleiche partielle Schachtelung haben. Wir behaupten, dass jede der Äquivalenzklassen eine symmetrische Kette ist; dies nachzuprüfen ist eine einfache Aufgabe. So haben wir den Satz von Sperner zum zweiten Mal bewiesen.  $\square$

Zum Abschluss führen wir noch einen weiteren Beweis für den Satz von Sperner vor. Es ist bemerkenswert, wie stark er sich von den beiden vorangegangenen Beweisen unterscheidet, er nutzt die hochgradig symmetrische Struktur des Poset  $(2^X, \subseteq)$  aus.

Wir beginnen mit einer allgemeinen Definition (die schon einmal in Aufgabe 2.1.4 vorgekommen ist). Seien  $(X, \leq)$  und  $(Y, \preceq)$  Posets. Eine Abbildung  $f: X \rightarrow Y$  heißt ein *Poset-Isomorphismus*, wenn  $f$  eine Bijektion ist und für je zwei Elemente  $x, y \in X$  genau dann  $x \leq y$  gilt, wenn  $f(x) \preceq f(y)$ . Ein Isomorphismus eines Poset  $(X, \leq)$  in sich selbst heißt ein *Automorphismus* von  $(X, \leq)$ . Ein Automorphismus erhält alle Eigenschaften, die man mit der Ordnungsrelation  $\leq$  definieren kann.

Z.B. ist  $x$  genau dann das größte Element einer Teilmenge  $A \subseteq X$ , wenn  $f(x)$  das größte Element der Menge  $f(A)$  ist, und so weiter.

*Dritter Beweis des Satzes von Sperner.* Sei  $X$  eine  $n$ -Menge. Jede Permutation  $f: X \rightarrow X$  induziert eine Abbildung  $f^\# : 2^X \rightarrow 2^X$  (die also Teilmengen von  $X$  auf Teilmengen von  $X$  abbildet) durch  $f^\#(A) = \{f(x) : x \in A\}$ . Es ist klar,<sup>1</sup> dass  $f^\#$  eine Bijektion  $2^X \rightarrow 2^X$  ist, sogar ein Automorphismus des Poset  $(2^X, \subseteq)$ .

Betrachten wir nun ein System  $\mathcal{M}$  von Teilmengen der Menge  $X$ . Für jede Permutation  $f$  der Menge  $X$  erhalten wir das Mengensystem  $\{f^\#(M) : M \in \mathcal{M}\}$ ; das ist das System der Bilder der Mengen aus  $\mathcal{M}$  unter der Abbildung  $f^\#$ . Auf diese Weise haben wir eine neue Abbildung

$$f^{\#\#} : 2^{2^X} \rightarrow 2^{2^X}$$

definiert (die Mengensysteme auf Mengensysteme abbildet) und durch die Formel

$$f^{\#\#}(\mathcal{M}) = \{f^\#(M) : M \in \mathcal{M}\}$$

gegeben ist. Die Abbildung  $f^{\#\#}$  ist wieder eine Bijektion.

Wir erklären eine Relation  $\triangleleft$  auf der Menge aller Mengensysteme auf  $X$  (d.h. auf der Menge  $2^{2^X}$ ):

$$\mathcal{M} \triangleleft \mathcal{N} \Leftrightarrow \text{für jedes } M \in \mathcal{M} \text{ gibt es ein } N \in \mathcal{N} \text{ mit } M \subseteq N.$$

Beachten Sie, dass die Relation  $\triangleleft$  etwas anderes ist als die Inklusion zwischen Mengensystemen. Sie ist in der Regel schwächer als die Inklusion (das bedeutet, aus  $\mathcal{M} \subseteq \mathcal{N}$  folgt  $\mathcal{M} \triangleleft \mathcal{N}$ ). Vielleicht möchten Sie jetzt nachweisen, dass die Relation  $\triangleleft$  reflexiv und transitiv ist, aber nicht unbedingt antisymmetrisch (finden Sie ein Beispiel auf einer 3-elementigen Menge  $X$ ).

Der Buchstabe  $\Xi$  (sprich: Ksi) stehe für die Menge aller Unabhängigkeitssysteme auf der Menge  $X$  (also  $\Xi \subset 2^{2^X}$ ). Wir behaupten, dass die Einschränkung der Relation  $\triangleleft$  auf  $\Xi$  schon antisymmetrisch ist, und dass sie folglich eine partielle Ordnung auf  $\Xi$  ist. Sind nämlich  $\mathcal{M}$  und  $\mathcal{N}$  Unabhängigkeitssysteme, für die sowohl  $\mathcal{M} \triangleleft \mathcal{N}$  als auch  $\mathcal{N} \triangleleft \mathcal{M}$  gilt, dann betrachten wir eine beliebige Menge  $M \in \mathcal{M}$ . Das System  $\mathcal{N}$  muss irgendeine Menge  $M' \supseteq M$  enthalten, und dann enthält auch  $\mathcal{M}$  eine Menge  $M'' \supseteq M'$ . Damit haben wir zwei Mengen  $M, M'' \in \mathcal{M}$

<sup>1</sup>In Abschnitt 1.4 haben wir die Konvention eingeführt, das Bild einer Menge unter einer Abbildung genauso zu schreiben wie das Bild eines Elements. In diesem Fall heißt das, dass wir die Menge  $\{f(x) : x \in A\}$  einfach als  $f(A)$  schreiben könnten. In dem nun folgenden Beweis wird es jedoch besser sein, genauer zwischen dem Bild eines Elements und dem Bild einer Menge zu unterscheiden. Aus diesem Grunde haben wir ein neues Symbol, nämlich  $f^\#$ , für die Abbildung auf den Teilmengen eingeführt.

mit  $M \subseteq M''$ , und weil  $\mathcal{M}$  ein Unabhängigkeitssystem ist, folgt, dass  $M = M'' = M'$ , und somit, dass  $M \in \mathcal{N}$ . Dies zeigt, dass  $\mathcal{M} \subseteq \mathcal{N}$  ist, und ganz symmetrisch erhalten wir  $\mathcal{N} \subseteq \mathcal{M}$ , also  $\mathcal{M} = \mathcal{N}$ . Somit ist  $(\Xi, \triangleleft)$  ein Poset.

Des Weiteren behaupten wir, dass für jede Permutation  $f$  die Abbildung  $f^{\# \#}$  ein Automorphismus des Poset  $(\Xi, \triangleleft)$  ist — dies zu verifizieren überlassen wir dem Leser (das ist eine gute Methode um ein wirkliches Verständnis der Objekte  $\Xi$  und  $f^{\# \#}$  zu entwickeln).

Dieser dritte Beweis des Satzes von Sperner beruht nun auf folgendem Lemma:

**Lemma.** *Es bezeichne  $\Xi_0 \subseteq \Xi$  die Menge der Unabhängigkeitssysteme mit der größtmöglichen Anzahl von Mengen. Die Menge  $\Xi_0$  hat ein (bezüglich der Ordnung  $\triangleleft$ ) größtes Element  $\mathcal{N}_0$ . Das bedeutet  $\mathcal{M} \triangleleft \mathcal{N}_0$  für alle  $\mathcal{M} \in \Xi_0$ .*

*Beweis des Lemmas.* Weil es nur endlich viele Mengensysteme auf  $X$  gibt, genügt es zu beweisen, dass es zu je zwei Mengensystemen  $\mathcal{M}, \mathcal{M}' \in \Xi_0$  ein Mengensystem  $\mathcal{N} \in \Xi_0$  gibt, das größer ist als  $\mathcal{M}$  und  $\mathcal{M}'$ , d.h.  $\mathcal{M} \triangleleft \mathcal{N}$  und  $\mathcal{M}' \triangleleft \mathcal{N}$ .

Seien also  $\mathcal{M}, \mathcal{M}' \in \Xi_0$ , dann bilden wir ein neues Mengensystem  $\bar{\mathcal{M}} = \mathcal{M} \cup \mathcal{M}'$ . Weil  $\mathcal{M}$  und  $\mathcal{M}'$  beides Unabhängigkeitssysteme sind, enthält die (bezüglich der Inklusionsordnung von  $\bar{\mathcal{M}}$ ) längste Kette in  $\bar{\mathcal{M}}$  höchstens zwei Mengen. Sei nun  $\bar{\mathcal{M}}_{min}$  das System aller Mengen aus  $\bar{\mathcal{M}}$ , für die  $\bar{\mathcal{M}}$  keine echte Teilmenge enthält, oder anders ausgedrückt das System aller Mengen aus  $\bar{\mathcal{M}}$ , die bezüglich der Inklusion minimal sind. Analog definieren wir das System  $\bar{\mathcal{M}}_{max}$  als das System aller inklusionsmaximalen Mengen aus  $\bar{\mathcal{M}}$ . Wir möchten gerne zeigen, dass das System  $\mathcal{N} = \bar{\mathcal{M}}_{max}$  zu  $\Xi_0$  gehört und sowohl  $\mathcal{M} \triangleleft \bar{\mathcal{M}}_{max}$  als auch  $\mathcal{M}' \triangleleft \bar{\mathcal{M}}_{max}$  erfüllt.

Die Systeme  $\bar{\mathcal{M}}_{min}$  und  $\bar{\mathcal{M}}_{max}$  sind beides Unabhängigkeitssysteme, und es gilt  $\bar{\mathcal{M}} = \bar{\mathcal{M}}_{min} \cup \bar{\mathcal{M}}_{max}$ . Wie man leicht sieht, gilt auch  $\bar{\mathcal{M}}_{max} \triangleright \mathcal{M}$  und  $\bar{\mathcal{M}}_{max} \triangleright \mathcal{M}'$ . Nun bleibt noch zu zeigen, dass  $\bar{\mathcal{M}}_{max}$  die größtmögliche Anzahl von Mengen enthält, d.h.  $|\bar{\mathcal{M}}_{max}| = |\mathcal{M}|$ . Aus der Tatsache, dass  $\mathcal{M}$  und  $\mathcal{M}'$  Unabhängigkeitssysteme sind, erhalten wir  $\mathcal{M} \cap \mathcal{M}' \subseteq \bar{\mathcal{M}}_{min} \cap \bar{\mathcal{M}}_{max}$  (überprüfen Sie das!). Deshalb gilt  $|\bar{\mathcal{M}}_{min}| + |\bar{\mathcal{M}}_{max}| = |\bar{\mathcal{M}}_{min} \cup \bar{\mathcal{M}}_{max}| + |\bar{\mathcal{M}}_{min} \cap \bar{\mathcal{M}}_{max}| \geq |\mathcal{M} \cup \mathcal{M}'| + |\mathcal{M} \cap \mathcal{M}'| = |\mathcal{M}| + |\mathcal{M}'|$ , und wenn  $|\bar{\mathcal{M}}_{max}| < |\mathcal{M}| = |\mathcal{M}'|$  wäre, dann würde  $|\bar{\mathcal{M}}_{min}| > |\mathcal{M}|$  folgen und die Systeme  $\mathcal{M}$  und  $\mathcal{M}'$  hätten nicht die maximal mögliche Größe. Damit ist das Lemma bewiesen.

Wir sind noch im dritten Beweis des Satzes von Sperner. Betrachten wir das größte Element  $\mathcal{N}_0$  der Menge  $(\Xi_0, \triangleleft)$ . Für jede Permutation  $f$  der Menge  $X$  bildet der zugehörige induzierte Automorphismus  $f^{\# \#}$  die Menge  $\Xi_0$  (der Unabhängigkeitssysteme von maximaler Größe) auf sich selbst ab, sein eindeutiges größtes Element  $\mathcal{N}_0$  muss er also auf

sich selbst abbilden:  $f^{\# \#}(\mathcal{N}_0) = \mathcal{N}_0$ . Aber daraus folgt doch, dass  $\mathcal{N}_0$ , wenn es überhaupt eine  $k$ -Menge enthält, schon alle  $k$ -Mengen enthält! Mit anderen Worten,  $\binom{X}{k} \subseteq \mathcal{N}_0$ . Es ist nicht möglich, dem System  $\binom{X}{k}$  irgendeine Menge hinzuzufügen, so dass es unabhängig bleibt, und deshalb muss  $\mathcal{N}_0 = \binom{X}{k}$  sein. Weil die Binomialkoeffizienten  $\binom{n}{\lfloor n/2 \rfloor}$  und  $\binom{n}{\lceil n/2 \rceil}$  die größten sind, folgt  $\mathcal{N}_0 = \binom{X}{\lceil n/2 \rceil}$ .  $\square$

## Aufgaben

1. Wir nennen ein System  $\mathcal{N}$  von Teilmengen von  $X$  ein *Semi-Unabhängigkeitssystem*, wenn es keine drei Mengen  $A, B, C$  mit  $A \subset B \subset C$  enthält.
  - (a) Zeigen Sie mit einer ähnlichen Methode wie im ersten Beweis des Satzes von Sperner, dass  $|\mathcal{N}| \leq 2 \binom{n}{\lfloor n/2 \rfloor}$ , wobei  $n = |X|$ .
  - (b) Zeigen Sie, dass die Abschätzung aus (a) für ungerades  $n$  nicht verbessert werden kann.
2. (a) Bestimmen Sie in der Menge  $\{1, 2, \dots, 10!\}$  die Anzahl maximaler Ketten (mit der Teilbarkeitsrelation als Ordnung).
  - (b) Bestimmen Sie die Anzahl maximaler Antiketten in der Menge  $\{1, 2, \dots, 5!\}$ , geordnet durch die Teilbarkeitsrelation.
3. \*Zeigen Sie, dass die Mengensysteme  $\binom{X}{\lfloor n/2 \rfloor}$  und  $\binom{X}{\lceil n/2 \rceil}$  die einzigen Unabhängigkeitssysteme auf einer  $n$ -Menge  $X$  sind, die die größtmögliche Anzahl von Mengen realisieren.
4. Bestimmen Sie die Anzahl der Automorphismen des Poset  $(2^X, \subseteq)$ .
5. Zeigen Sie durch eine Abwandlung des dritten Beweises vom Satz von Sperner, dass es für jedes endliche Poset  $(P, \leq)$  eine Antikette maximal möglicher Größe gibt, die von allen Automorphismen auf  $(P, \leq)$  auf sich selbst abgebildet wird (d.h. sie ist ein „Fixpunkt“ von allen Automorphismen).
6. Seien  $a_1, a_2, \dots, a_n$  reelle Zahlen mit  $|a_i| \geq 1$ . Sei  $p(a_1, \dots, a_n)$  die Anzahl von Vektoren  $(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n)$ , wobei  $\varepsilon_i = \pm 1$ , für die gilt

$$-1 < \sum_{i=1}^n \varepsilon_i a_i < 1.$$

(a) \*Beweisen Sie, dass für beliebige  $a_1, a_2, \dots, a_n$  die Ungleichung  $p(a_1, \dots, a_n) \leq \binom{n}{\lfloor n/2 \rfloor}$  gilt. (Dies war eine der ersten Anwendungen des Satzes von Sperner — das so genannte Littlewood–Offord–Problem.)

(b) Finden Sie  $a_1, a_2, \dots, a_n$  mit  $p(a_1, \dots, a_n) = \binom{n}{\lfloor n/2 \rfloor}$ .

7. Sei  $n$  eine quadratfreie natürliche Zahl, d.h. sie ist durch keine Quadratzahl größer als 1 teilbar. Bestimmen Sie die maximal mögliche Größe einer Menge von Teilern von  $n$ , in der keine Zahl eine andere teilt (d.h.  $\max|M|$ , wobei  $x \in M \Rightarrow x|n$  und  $x, y \in M, x \neq y \Rightarrow x$  teilt  $y$  nicht).

## 7.3 Ein Problem der extremalen Graphentheorie

In Abschnitt 4.7 haben wir die maximal mögliche Kantenzahl eines Graphen auf  $n$  Ecken untersucht, der kein Dreieck als Teilgraph enthält. Nun wollen wir einer recht ähnlich erscheinenden Frage auf den Grund gehen: Was ist die maximal mögliche Kantenzahl eines Graphen auf  $n$  Ecken, der keinen Teilgraph isomorph zu  $K_{2,2}$  enthält (also keinen Kreis der Länge 4)? ,Teilgraph‘ ist hier nicht im induzierten Sinn gemeint, so dass beispielsweise der vollständige Graph  $K_4$  auf 4 Ecken einen  $K_{2,2}$  enthält.

Man könnte erwarten, dass das  $K_{2,2}$ -Verbot einen ähnlichen Effekt hat wie das  $K_3$ -Verbot, doch überraschenderweise sind die Antworten grundsätzlich verschieden. Ein dreiecksfreier Graph kann bis zu  $\lfloor n^2/4 \rfloor$  Kanten haben, das ist ungefähr die Hälfte von  $\binom{n}{2}$  (der maximalen Kantenzahl eines Graphen auf  $n$  Ecken ohne jede Restriktion). Im Gegensatz dazu sind im  $K_{2,2}$ -freien Graphen deutlich weniger Kanten erlaubt — wie wir sehen werden ist die Größenordnung  $n^{3/2}$ . Für große  $n$  ist diese Zahl im Vergleich zu  $\binom{n}{2}$  (oder auch zu  $\lfloor n^2/4 \rfloor$ ) vernachlässigbar klein.

Diese Probleme gehören beide zur *extremalen Graphentheorie*, in welcher man allgemein die maximal mögliche Kantenzahl eines Graphen auf  $n$  Ecken studiert, wenn ein vorgegebener Graph nicht als Teilgraph vorkommen darf oder, allgemeiner, wenn kein Graph aus einer vorgegebenen Menge verbotener Graphen vorkommen darf. Ein Problem dieser allgemeineren Art ist uns auch schon im Kapitel über Bäume begegnet: Ein Graph auf  $n$  Ecken, der keinen Kreis enthält (ein Wald also) hat höchstens  $n - 1$  Kanten.

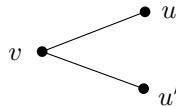
Wir kommen nun zum wesentlichen Resultat dieses Abschnitts.

**7.3.1 Satz.** *Ein Graph  $G$  auf  $n$  Ecken, der keinen Teilgraph isomorph zu  $K_{2,2}$  enthält, hat höchstens  $\frac{1}{2}(n^{3/2} + n)$  Kanten.*

*Bemerkung.* Das bedeutet, dass die mögliche Kantenzahl stark schrumpft, wenn wir  $K_{2,2}$  als Teilgraphen verbieten: Von etwa  $\frac{1}{2}n^2$  Kanten für einen beliebigen Graphen auf ungefähr  $\frac{1}{2}n^{3/2}$  Kanten für einen  $K_{2,2}$ -freien Graphen. Wenn wir im Gegensatz dazu z.B. Dreiecke ( $K_3$ ) verbieten, dann sind immer noch zirka  $n^2/4$  Kanten möglich! (Das belegt der vollständige bipartite Graph  $K_{\lfloor n/2 \rfloor, \lceil n/2 \rceil}$ .)

Wie wir später (in Satz 9.4.1) sehen werden, ist die Schranke aus Satz 7.3.1 für große  $n$  fast bestmöglich.

*Beweis.* Wir schreiben  $V = V(G)$ . Wir werden die Mächtigkeit der Menge  $M$  aller Paare  $(\{u, u'\}, v)$  auf zwei Arten zählen, bei denen  $v \in V$ ,  $\{u, u'\} \in \binom{V}{2}$  und  $v$  mit  $u$  und mit  $u'$  durch eine Kante verbunden ist. Mit anderen Worten: Wir zählen (nicht induzierte) Teilgraphen der Form



Für ein festes Paar  $\{u, u'\}$  kann es nur eine Ecke  $v \in V$  geben, die sowohl mit  $u$  als auch mit  $u'$  verbunden ist. Denn wenn es zwei solche Ecken  $v$  und  $v'$  gäbe, dann würden sie zusammen mit  $u$  und  $u'$  einen Teilgraphen isomorph zu  $K_{2,2}$  bilden. Daher ist  $|M| \leq \binom{n}{2}$ .

Nun überlegen wir uns, wie viele Elemente der Form  $(\{u, u'\}, v)$  eine Ecke  $v \in V$  zur Menge  $M$  beiträgt. Für jedes Paar  $\{u, u'\}$  ihrer Nachbarn trägt  $v$  ein Element zu  $M$  bei; hat  $v$  also Grad  $d$ , dann trägt sie  $\binom{d}{2}$  Elemente bei. Wenn wir die Grade der Ecken aus  $V$  mit  $d_1, d_2, \dots, d_n$  bezeichnen, erhalten wir daher  $|M| = \sum_{i=1}^n \binom{d_i}{2}$ .

Zusammen mit der Abschätzung von eben ergibt sich

$$\sum_{i=1}^n \binom{d_i}{2} \leq \binom{n}{2}. \quad (7.3)$$

Außerdem wissen wir, dass die Kantenzahl des betrachteten Graphen  $\frac{1}{2} \sum_{i=1}^n d_i$  ist. Alles weitere in diesem Beweis sind lediglich Umformungen von Ungleichungen.

Wir zeigen Ihnen hier einen Beweis, ein weiterer ist in Aufgabe 5 skizziert (der zweite ist ein wenig komplizierter, lässt sich jedoch leichter verallgemeinern). Zunächst brauchen wir eine bekannte, allgemein sehr nützliche Ungleichung:

**7.3.2 Hilfssatz (Cauchy–Schwarzsche Ungleichung).** Für beliebige reelle Zahlen  $x_1, x_2, \dots, x_n$  und  $y_1, y_2, \dots, y_n$  gilt

$$\sum_{i=1}^n x_i y_i \leq \sqrt{\sum_{i=1}^n x_i^2} \sqrt{\sum_{i=1}^n y_i^2}.$$

Die Cauchy–Schwarzsche Ungleichung hat eine hübsche geometrische Interpretation. Wenn wir  $x = (x_1, \dots, x_n)$  und  $y = (y_1, \dots, y_n)$

als Vektoren im  $n$ -dimensionalen Euklidischen Raum auffassen, dann steht auf der linken Seite der Ungleichung das *Skalarprodukt* von  $x$  und  $y$ , während auf der rechten Seite das Produkt der Längen der beiden Vektoren steht (machen Sie sich das doch einmal für  $n = 2$ , d.h. für die Ebene, klar — Sie benötigen dazu nur geringe Kenntnisse über Vektoren). Eine der bekannten Formeln über Vektoren besagt, dass der Kosinus des Winkels zwischen zwei Vektoren gleich ihrem Skalarprodukt dividiert durch das Produkt ihrer Längen ist. Die Cauchy–Schwarzsche Ungleichung läuft also darauf hinaus, dass dieser Kosinus nie größer ist als 1.

Die Cauchy–Schwarzsche Ungleichung lernt man normalerweise in der Analysisvorlesung — aber es kann doch nicht schaden, an dieser Stelle zwei elegante Beweise einzufügen, oder?

**Erster Beweis: Mit der Ungleichung vom arithmetischen und geometrischen Mittel.** Der Übersichtlichkeit halber schreiben wir  $X = \sum_{i=1}^n x_i^2$  und  $Y = \sum_{i=1}^n y_i^2$ . Ist  $X = 0$ , so sind alle  $x_i$  gleich 0 und die Ungleichung stimmt, ebenso für  $Y = 0$ . Wir nehmen nun an, dass  $X > 0$  und  $Y > 0$ , und definieren  $a_i = x_i^2/X$ ,  $b_i = y_i^2/Y$ . Die Ungleichung vom arithmetischen und geometrischen Mittel, siehe den Beweis von Satz 3.5.2, sagt uns, dass  $\sqrt{a_i b_i} \leq (a_i + b_i)/2$ . Addition dieser Ungleichungen für  $i = 1, 2, \dots, n$  liefert uns auf der linken Seite

$$\sum_{i=1}^n \sqrt{a_i b_i} = \sum_{i=1}^n \frac{|x_i y_i|}{\sqrt{XY}},$$

und auf der rechten Seite

$$\frac{1}{2} \left( \frac{1}{X} \sum_{i=1}^n x_i^2 + \frac{1}{Y} \sum_{i=1}^n y_i^2 \right) = \frac{1}{2}(1+1) = 1.$$

Also ist  $\sum_{i=1}^n \frac{|x_i y_i|}{\sqrt{XY}} \leq 1$ , und Multiplikation mit  $\sqrt{XY}$  ergibt die Cauchy–Schwarzsche Ungleichung.  $\square$

**Zweiter Beweis: Hexerei mit Diskriminanten.** Für feste Zahlen  $x_i$  und  $y_i$  definieren wir eine Funktion  $p$  in einer neuen Variable  $t$ :

$$p(t) = \sum_{i=1}^n (x_i + t y_i)^2.$$

Wir multiplizieren die Klammern aus, sortieren die Terme nach dem Exponenten in  $t$  und sehen so, dass  $p(t)$  eine quadratische Funktion der Gestalt  $p(t) = at^2 + bt + c$  ist, wobei  $a = \sum_{i=1}^n y_i^2$ ,  $b = 2 \cdot \sum_{i=1}^n x_i y_i$  und  $c = \sum_{i=1}^n x_i^2$ . Andererseits ist  $p(t)$  als eine Summe von Quadraten für alle reellen Zahlen  $t$  nichtnegativ.

Hätte die quadratische Gleichung  $at^2 + bt + c = 0$  eine positive Diskriminante, dann hätte sie zwei reelle Lösungen, und die Funktion  $p(t)$  nähme auf einem Teil der Achse negative Werte an. Folglich ist die Diskriminante nicht positiv, d.h.  $b^2 - 4ac \leq 0$ . Setzen wir nun für  $a, b$  und  $c$  die Terme in  $x_i$  und  $y_i$  ein, erhalten wir genau die Cauchy–Schwarzsche Ungleichung.  $\square$

Dies sind bei weitem nicht alle Beweise der Cauchy–Schwarzschen Ungleichung — einige weitere stecken in Aufgabe 4.

*Fortsetzung des Beweises von Satz 7.3.1.* Offensichtlich können wir annehmen, dass unser Graph keine isolierten Ecken hat, und somit dass  $d_i \geq 1$  ist für alle  $i$ . Dann gilt  $\binom{d_i}{2} \geq \frac{1}{2}(d_i - 1)^2$ , und aus (7.3) erhalten wir, dass

$$\sum_{i=1}^n (d_i - 1)^2 \leq n^2.$$

Nun wenden wir die Cauchy–Schwarzsche Ungleichung an mit  $x_i = d_i - 1$ ,  $y_i = 1$ . Wir erhalten

$$\sum_{i=1}^n (d_i - 1) \leq \sqrt{\sum_{i=1}^n (d_i - 1)^2} \sqrt{n} \leq \sqrt{n^2} \sqrt{n} = n^{3/2},$$

und somit  $|E(G)| = \frac{1}{2} \sum_{i=1}^n d_i \leq \frac{1}{2}(n^{3/2} + n)$ .  $\square$

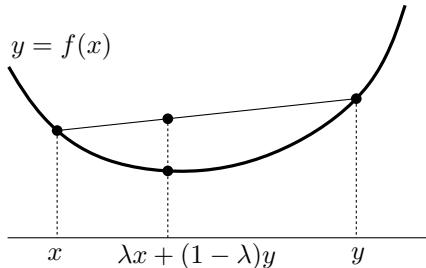
**Die zugehörige Intuition.** In dem Beweis leiten wir zuerst eine obere Schranke für die Summe  $\sum_{i=1}^n \binom{d_i}{2}$  her, und dann fragen wir uns, wie groß die Summe  $\sum_{i=1}^n d_i$  werden kann. Ist  $d_i$  nicht zu klein, so verhält sich  $\binom{d_i}{2}$  ungefähr wie  $\frac{1}{2}d_i^2$ . Vorausgesetzt,  $\sum d_i^2$  ist etwa  $n^2$ , dann wird  $\sum d_i$  dann besonders groß, wenn wir alle  $d_i$  gleich wählen, was in unserem Fall bedeutet, dass jedes etwa  $\sqrt{n}$  sein sollte. Dann ist  $\sum d_i$  ungefähr  $n^{3/2}$ . Dies ist natürlich kein Beweis, doch so eine grobe Rechnung gibt uns oft eine bessere Vorstellung davon, was los ist. Der obige Beweis mit der Cauchy–Schwarzschen Ungleichung ist eine geglättete Version eben dieser Idee.

## Aufgaben

1. Beweisen Sie, dass die Maximalzahl von Kanten eines Graphen auf  $n$  Ecken, der keinen  $K_{2,t}$  als Teilgraphen enthält ( $t \geq 2$ ), ist höchstens

$$\frac{1}{2} \left( \sqrt{t-1} n^{3/2} + n \right).$$

2. Sei  $X$  eine  $n$ -Menge und seien  $S_1, S_2, \dots, S_n$  Teilmengen von  $X$ , für die  $|S_i \cap S_j| \leq 1$  gilt, wenn  $1 \leq i < j \leq n$ . Beweisen Sie, dass mindestens eine der Mengen  $S_i$  eine Mächtigkeit von höchstens  $C\sqrt{n}$  hat, für eine absolute (von  $n$  unabhängige) Konstante  $C$ .
3. Sei  $G$  ein bipartiter Graph, in dem die Eckenklassen die Größen  $n$  und  $m$  haben. Angenommen,  $G$  ist  $K_{2,2}$ -frei. Beweisen Sie, dass  $G$  höchstens  $O(m\sqrt{n} + n)$  Kanten hat. (Wenn  $n$  ausreichend viel größer ist als  $m$ , dann ist dies eine bessere Abschätzung als die Ungleichung aus Satz 7.3.1.)
4. (a) Beweisen Sie die Cauchy–Schwarzsche Ungleichung mit Induktion über  $n$  (quadrieren Sie zunächst beide Seiten).  
 (b) Beweisen Sie die Cauchy–Schwarzsche Ungleichung direkt; starten Sie mit der Ungleichung  $\sum_{i,j=1}^n (x_i y_j - x_j y_i)^2 \geq 0$ .
5. (a) Sei  $f: \mathbb{R} \rightarrow \mathbb{R}$  eine *konvexe Funktion*, d.h. für je zwei Zahlen  $x, y \in \mathbb{R}$  und  $\lambda \in [0, 1]$  gelte  $f(\lambda x + (1 - \lambda)y) \leq \lambda f(x) + (1 - \lambda)f(y)$ . Die geometrische Bedeutung dieser Bedingung ist, dass von den Verbindungslien zwischen je zwei Punkten auf dem Graph von  $f$  nie auch nur ein Stückchen unter dem Graph von  $f$  liegt:



Beweisen Sie (induktiv), dass für konvexe  $f$  die Ungleichung

$$f\left(\frac{1}{n}x_1 + \frac{1}{n}x_2 + \cdots + \frac{1}{n}x_n\right) \leq \frac{1}{n}f(x_1) + \frac{1}{n}f(x_2) + \cdots + \frac{1}{n}f(x_n) \quad (7.4)$$

für beliebige reelle Zahlen  $x_1, x_2, \dots, x_n$  gilt (dies heißt manchmal die *Jensensche Ungleichung*).

(b) Definieren Sie eine Funktion  $f$  durch die Formel

$$f(x) = \begin{cases} 0 & \text{für } x \leq 1 \\ x(x-1)/2 & \text{für } x > 1. \end{cases}$$

Beweisen Sie, dass  $f$  konvex ist.

(c) Beweisen Sie Satz 7.3.1 aus (7.3) unter Verwendung von (a) und (b). Leiten Sie dazu als erstes her, dass  $n \cdot f\left(\frac{m}{2n}\right) \leq \binom{n}{2}$  ist, wobei  $m = |E(G)|$ .

6. \*Leiten Sie mit einer ähnlichen Methode wie in Aufgabe 5 her, dass ein  $K_{3,3}$ -freier Graph mit  $n$  Ecken  $O(n^{5/3})$  Kanten hat.
7. (a) \*Sei  $L$  eine Menge von  $n$  (verschiedenen) Geraden in der Ebene und  $P$  eine Menge von  $n$  (verschiedenen) Punkten in der Ebene. Beweisen Sie, dass die Anzahl der Paare  $(p, \ell)$  mit  $p \in P$ ,  $\ell \in L$ , für die  $p$  auf  $\ell$  liegt, durch  $O(n^{3/2})$  beschränkt ist.

*Bemerkung.* Man weiß, dass die „richtige“ Schranke  $O(n^{4/3})$  ist; siehe Pach und Agarwal [29].

(b) \*Zeigen Sie, dass die Schranke in (a) immer noch gilt, wenn wir die Geraden durch Einheitskreise ersetzen. Verwenden Sie Aufgabe 1.

*Bemerkung.* Auch in diesem Fall ist die beste bekannte obere Schranke  $O(n^{4/3})$ , doch vermutet man, dass die Anzahl der Inzidenzen sogar durch  $O(n^{1+\varepsilon})$  beschränkt ist, und zwar für jede beliebig kleine Konstante  $\varepsilon > 0$  (wobei jedoch die in der  $O(\cdot)$ -Notation versteckte Konstante von  $\varepsilon$  abhängt). Diese Vermutung zu beweisen oder zu widerlegen ist ein sehr anspruchsvolles offenes Problem.

# 8

## Die Anzahl aufspannender Bäume

---

### 8.1 Die Cayley–Formel

Wir bezeichnen die Anzahl der aufspannenden Bäume eines Graphen  $G$  mit  $T(G)$ . Beispielsweise ist  $T(K_3) = 3$ , und in diesem Fall sind alle drei aufspannenden Bäume isomorph. (Wir zählen also wirklich alle aufspannenden Bäume.) In diesem Kapitel sehen wir uns verschiedene Beweise des folgenden Satzes an:

**8.1.1 Satz (Cayley–Formel).** *Für  $n \geq 2$  ist  $T(K_n)$ , die Anzahl der Bäume auf  $n$  Ecken, gleich  $n^{n-2}$ .*

Für diese Formel kennen wir keinen Beweis, der genauso hübsch und einfach ist wie sie selbst. Im Laufe der Zeit hat man viele Beweise gefunden, die auf sehr verschiedenen Ideen beruhen. Jeder davon benutzt einen cleveren Trick oder folgt aus einer nichttrivialen Theorie. In diesem Kapitel stellen wir einige dieser Beweise vor — bei weitem nicht alle! — in erster Linie um die Vielfalt mathematischen Denkens darzustellen.

Der Beweis in Abschnitt 8.2 zählt die Bäume mit gegebener Gradfolge mittels einer pfiffigen Induktion. Summieren über alle möglichen Gradfolgen ergibt die gesuchte Anzahl. In Abschnitt 8.3 konstruieren wir eine Bijektion, und zwar zwischen den aufspannenden Bäumen mit einer Markierung an zwei (möglicherweise gleichen) Ecken — davon gibt es  $n^2 \cdot T(K_n)$  Stück — und allen Abbildungen  $\{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ . Abschnitt 8.4 ist ein Klassiker: Der Prüfer Code codiert Bäume mit Folgen der Länge  $n - 2$ . Die Methode aus Abschnitt 8.5 ist sehr allgemein: Die Anzahl aufspannender Bäume eines beliebigen Graphen kann als eine Determinante ausgedrückt werden. Dieses Verfahren erlaubt vielleicht die tiefsten

Einblicke in die Natur des Problems. Noch ein weiterer Beweis ist in Übung 8.2.2 skizziert.

Wir wollen die Cayley–Formel sicher nicht zu einem der wirklich wichtigen mathematischen Ergebnisse erklären. Doch die Anzahl der aufspannenden Bäume eines Graphen und die zugehörige Theorie haben viele theoretische und auch praktische Anwendungen. Am Anfang stand die Theorie elektrischer Schaltkreise.

Zur Illustration soll uns (ohne Beweis) die „elektrotechnische“ Bedeutung der Anzahl aufspannender Bäume dienen. Wir stellen uns  $G$  als elektrischen Schaltkreis vor, in dem jede Kante ein Stück Draht mit Einheitswiderstand ist und die Ecken einfach die Stellen, an denen die Drähte verbunden sind. Sind  $x$  und  $y$  zwei Ecken, die durch eine Kante verbunden sind, so ist der Widerstand, den wir zwischen  $x$  und  $y$  messen würden, gleich der Anzahl derjenigen aufspannenden Bäume von  $G$ , die die Kante  $\{x, y\}$  enthalten, geteilt durch die Gesamtzahl  $T(G)$  aller aufspannenden Bäume von  $G$ . Zwar ist das Ergebnis in dieser Form nicht besonders nützlich, weil die Widerstände in Anwendungen selten alle gleich sind, aber es gibt eine Verallgemeinerung für Graphen mit Kantengewichten. Mehr zum Thema dieses Kapitels findet sich bei Lovász [9] und Biggs [16].

Für dieses ganze Kapitel soll die Eckenmenge  $V$  des jeweils betrachteten Graphen immer die Menge  $\{1, 2, \dots, n\}$  sein.

## Aufgaben

1. Zeigen Sie, dass es mindestens  $e^{n-1}/n^3$  viele nicht isomorphe Bäume mit  $n$  Ecken gibt (siehe auch Aufgabe 5.2.6!).
2. \*Bestimmen Sie die Anzahl aufspannender Bäume des vollständigen Graphen auf  $n$  Ecken minus eine Kante unter Verwendung der Cayley–Formel 8.1.1.
3. Setze  $T_n = T(K_n)$ . Beweisen Sie die Rekursion

$$(n-1)T_n = \sum_{k=1}^{n-1} k(n-k) \binom{n-1}{k-1} T_k T_{n-k}.$$

*Bemerkung.* Man kann die Cayley–Formel 8.1.1 auch mittels dieser Rekursion beweisen, aber ganz leicht ist es nicht.

4. \*Sei  $G$  ein eben eingebetteter Graph und  $G^*$  der zu  $G$  duale Graph (siehe Definition 6.4.3). Zeigen Sie, dass  $T(G) = T(G^*)$ . Wenn Sie es einfacher finden, können Sie voraussetzen, dass  $G^*$  keine Schlingen und keine Mehrfachkanten enthält.

## 8.2 Ein Beweis mit Gradfolgen

Erst einmal zählen wir die Bäume mit einer gegebenen Gradfolge.

**8.2.1 Hilfssatz.** Seien  $d_1, d_2, \dots, d_n$  positive ganze Zahlen, die die Gleichung  $\sum d_i = 2n - 2$  erfüllen. Die Anzahl der aufspannenden Bäume von  $K_n$ , in denen der Grad jeder Ecke  $i \in V$  gleich  $d_i$  ist, ist

$$\frac{(n-2)!}{(d_1-1)!(d_2-1)!\cdots(d_n-1)!}.$$

*Beweis.* Wir führen Induktion über  $n$ . Für  $n = 1$  und  $2$  ist die Formel richtig (nachrechnen!), das ist der Induktionsanfang. Sei also  $n > 2$ . Weil die Summe der  $d_i$  kleiner als  $2n$  ist, muss ein  $i$  mit  $d_i = 1$  existieren. Wir können annehmen, dass dieses  $i = n$ , also  $d_n = 1$  ist; so ist der Beweis einfacher aufzuschreiben, er geht genauso für jedes andere  $d_i = 1$ . Anders ausgedrückt: Die gesuchte Anzahl hängt sicher nicht davon ab, wie die Ecke vom Grad 1 heißt, ob 1 oder 2 oder  $\dots$  oder  $n$ .

Sei  $\mathcal{T}$  die Menge aller aufspannenden Bäume von  $K_n$  mit der vorgegebenen Gradfolge (d.h. Ecke  $i$  hat Grad  $d_i$ ). Wir klassifizieren alle Bäume in  $\mathcal{T}$  nach dem (einzigsten) Nachbarn der Ecke  $n$ : Für  $1 \leq j \leq n-1$  enthalte  $\mathcal{T}_j$  all jene Bäume aus  $\mathcal{T}$ , in denen die Ecke  $n$  mit der Ecke  $j$  benachbart ist. Wenn wir nun in einem Baum aus  $\mathcal{T}_j$  die Ecke  $n$  und die (einzig) inzidente Kante löschen, dann erhalten wir einen aufspannenden Baum von  $K_{n-1}$ , in dem die Ecke  $i$  den Grad  $d_i$  hat (für  $i \neq j$ ) und Ecke  $j$  Grad  $d_{j-1}$ . Auf diese Art erhalten wir eine Bijektion zwischen  $\mathcal{T}_j$  und der Menge  $\mathcal{T}'_j$  aller aufspannenden Bäume von  $K_{n-1}$  mit Gradfolge  $(d_1, d_2, \dots, d_{j-1}, d_j - 1, d_{j+1}, \dots, d_{n-1})$ ; denn verschiedene Bäume im  $\mathcal{T}_j$  ergeben verschiedene Bäume in  $\mathcal{T}'_j$ , und in einem Baum aus  $\mathcal{T}'_j$  brauchen wir nur die Ecke  $j$  mit der neu hinzugefügten Ecke  $n$  zu verbinden um einen aufspannenden Baum in  $\mathcal{T}_j$  zu erhalten.

Nach Induktionsvoraussetzung ist

$$\begin{aligned} |\mathcal{T}_j| &= |\mathcal{T}'_j| \\ &= \frac{(n-3)!}{(d_1-1)!\cdots(d_{j-1}-1)!(d_j-2)!(d_{j+1}-1)!\cdots(d_{n-1}-1)!} \\ &= \frac{(n-3)!(d_j-1)}{(d_1-1)!(d_2-1)!\cdots(d_{n-1}-1)!}. \end{aligned}$$

Dies stimmt auch noch für  $d_j = 1$ : Dann ist die rechte Seite 0, und tatsächlich gibt es ja keinen aufspannenden Baum mit Grad  $d_j - 1 = 0$  an der Ecke  $j$ .

Also erhalten wir für die Anzahl der aufspannenden Bäume auf  $n$  Ecken mit Gradfolge  $(d_1, d_2, \dots, d_n)$ , wobei wir  $d_n = 1$  annehmen,

$$\begin{aligned} |\mathcal{T}| &= \sum_{j=1}^n |\mathcal{T}_j| = \sum_{j=1}^{n-1} \frac{(n-3)!(d_j-1)}{(d_1-1)!(d_2-1)!\cdots(d_{n-1}-1)!} \\ &= \left( \sum_{j=1}^{n-1} (d_j-1) \right) \frac{(n-3)!}{(d_1-1)!(d_2-1)!\cdots(d_{n-1}-1)!} \\ &= \frac{(n-2)(n-3)!}{(d_1-1)!(d_2-1)!\cdots(d_{n-1}-1)!}. \end{aligned}$$

Weil  $d_n = 1$  ist, können wir den Nenner gefahrlos mit  $(d_n-1)! = 0! = 1$  multiplizieren, und somit ist der Induktionsschritt gezeigt.

□

Nun beweisen wir die Cayley–Formel 8.1.1. Wir summieren einfach über alle möglichen Gradfolgen unter Verwendung des Multinomialssatzes 3.3.5:

$$\begin{aligned} T(K_n) &= \sum_{\substack{d_1, d_2, \dots, d_n \geq 1 \\ d_1 + d_2 + \cdots + d_n = 2n-2}} \frac{(n-2)!}{(d_1-1)!(d_2-1)!\cdots(d_n-1)!} \\ &= \sum_{\substack{k_1+k_2+\cdots+k_n=n-2 \\ k_1, \dots, k_n \geq 0}} \frac{(n-2)!}{k_1!k_2!\cdots k_n!} = (\underbrace{1+1+\cdots+1}_{n \text{ mal}})^{n-2} = n^{n-2}. \end{aligned}$$

□

## Aufgaben

1. (a) \*Bestimmen Sie die Anzahl der Bäume auf der Eckenmenge  $\{1, 2, \dots, n\}$ , in denen alle Eckengrade 1 oder 3 sind.  
 (b) \*Das Gleiche nochmal, aber mit Eckengraden 1, 2 oder 3.
2. (Noch ein Beweis der Cayley–Formel!) Wir bezeichnen die Anzahl der aufspannenden Bäume des  $K_n$ , in denen die Ecke  $n$  den Grad  $k$  hat, mit  $N_k$  ( $k = 1, 2, \dots, n-1$ ).  
 (a) \*Zeigen Sie, dass  $(n-1-k)N_k = k(n-1)N_{k+1}$  gilt,  
 (b) leiten Sie daraus  $N_k = \binom{n-2}{k-1}(n-1)^{n-1-k}$  ab,  
 (c) und beweisen Sie so schließlich die Cayley–Formel 8.1.1.

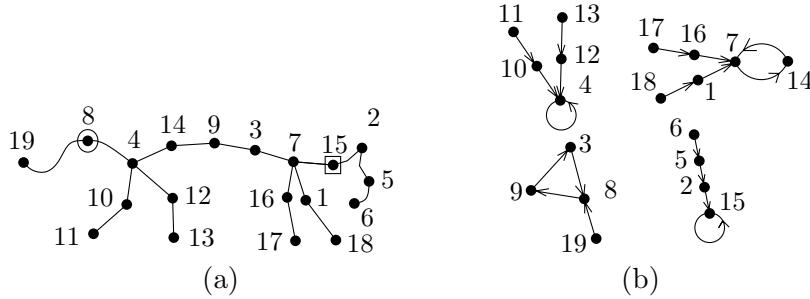


Abb. 8.1 (a) Ein Wirbeltier auf 19 Ecken; (b) die zugehörige Abbildung.

### 8.3 Ein Beweis mit Wirbeltieren

Gegeben sei ein aufspannender Baum des vollständigen Graphen  $K_n$ . Markiere eine seiner Ecken mit einem Kreis und eine — evtl. die gleiche — mit einem Quadrat, wie in Abb. 8.1(a). Diese Bäume mit zwei Markierungen nennen wir *Wirbeltiere* und wir schreiben  $\mathcal{W}$  für die Menge aller Wirbeltiere (für das eingangs gewählte  $n$ ).

Aus jedem aufspannenden Baum des  $K_n$  erhalten wir  $n^2$  Wirbeltiere. Also ist die Anzahl  $T(K_n)$  aller aufspannenden Bäume gleich  $|\mathcal{W}|/n^2$ . Nun bestimmen wir die Anzahl der Wirbeltiere.

**Lemma.** Es gibt eine Bijektion  $F$  zwischen der Menge  $\mathcal{W}$  aller Wirbeltiere und der Menge aller Abbildungen der Eckenmenge  $V$  in sich selbst.

Weil eine  $n$ -Menge  $n^n$  Abbildungen in sich selbst besitzt, gibt es nach dem Lemma ebensoviele Wirbeltiere. Also gibt es  $n^{n-2}$  aufspannende Bäume im  $K_n$ .

*Beweis des Lemmas.* Wir machen uns die Definition der Bijektion  $F$  am Beispiel in Abb. 8.1 klar. Wir beginnen mit dem Wirbeltier aus Abb. 8.1(a). Die markierten Ecken  $\square$  und  $\circlearrowleft$  sind durch einen eindeutigen Weg, die Wirbelsäule, miteinander verbunden. Wir schreiben die Nummern der einzelnen Wirbel hin, zuerst nach Größe geordnet und in die nächste Zeile in der Reihenfolge, in der sie entlang der Wirbelsäule von  $\circlearrowleft$  nach  $\square$  vorkommen:

$$\begin{array}{ccccccc} 3 & 4 & 7 & 8 & 9 & 14 & 15 \\ 8 & 4 & 14 & 9 & 3 & 7 & 15 \end{array}$$

Wir definieren folgenden gerichteten Hilfsgraphen  $H$ : Die Ecken von  $H$  sind die Wirbel, und gerichtete Kanten verlaufen von den Wirbeln aus der ersten Zeile zu den Wirbeln aus der zweiten Zeile. Weil in jede Ecke je eine Kante hinein- und eine hinausführt, ist  $H$  disjunkte Vereinigung gerichteter Kreise (evtl. haben wir isolierte Ecken mit einer gerichteten Schlinge). Anders ausgedrückt: Die Wirbelsäule definiert uns eine Permutation ihrer Wirbel, und  $H$  besteht aus den Zyklen dieser Permutation (siehe Abschnitt 3.2). In unserem Beispiel sind die Zyklen  $(3, 8, 9), (4), (7, 14)$  und  $(15)$ .

Jetzt sehen wir uns wieder das ganze Wirbeltier  $W$  an. Wenn wir die Kanten aus der Wirbelsäule entfernen (sozusagen die Bandscheiben), zerfällt es in Komponenten, die wieder Bäume sind. Wir richten die Kanten in den Komponenten so, dass sie zu dem einen Wirbel in dieser Komponente zeigen. Wir definieren nun einen weiteren gerichteten Hilfsgraphen auf der Eckenmenge  $V$ : Seine Kanten sind alle gerichteten Kanten aus den Komponenten plus die Kanten von  $H$ . Im Bild ist alles klar: Erst zeichnen wir die Zyklen von  $H$ , und dann zeichnen wir an jede Ecke (die ja in  $W$  Wirbel ist) den Baum, der an diesem Wirbel hing; siehe Abb. 8.1(b).

**Behauptung:** Der resultierende gerichtete Graph  $G$  ist der Graph einer Abbildung, d.h. aus jeder Ecke führt genau eine Kante heraus. Für die Wirbel haben wir uns das schon klar gemacht:  $H$  besteht aus gerichteten Zyklen, also hat jede Ecke in  $H$  Aus-Grad=Ein-Grad=1, und im weiteren Verlauf der Konstruktion von  $G$  kommen nur Kanten dazu, die zu den Wirbeln hin gerichtet sind. Für die anderen Ecken stimmt die Behauptung, weil es einen eindeutigen Weg von jeder Ecke von  $W$  zur Wirbelsäule gibt. Der gerichtete Graph  $G$  definiert uns nun eine Abbildung  $f: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ : Für jedes  $i \in V$  setzen wir  $f(i) = j$ , wobei  $j$  diejenige Ecke aus  $G$  ist, in der die eindeutige Kante, die aus  $i$  herausführt, endet. In unserem Beispiel erhalten wir die Abbildung  $1 \mapsto 7, 2 \mapsto 15, 3 \mapsto 8, 4 \mapsto 4, 5 \mapsto 2, 6 \mapsto 5, 7 \mapsto 14, 8 \mapsto 9, 9 \mapsto 3, 10 \mapsto 4, 11 \mapsto 10, 12 \mapsto 4, 13 \mapsto 12, 14 \mapsto 7, 15 \mapsto 15, 16 \mapsto 7, 17 \mapsto 16, 18 \mapsto 1$ , und  $19 \mapsto 8$ . So erhalten wir zu jedem Wirbeltier  $W$  eine Abbildung  $F(W)$ .

Es bleibt zu zeigen, dass diese Abbildung  $F$  eine Bijektion ist. Für die Injektivität muss man zeigen, dass keine zwei Wirbeltiere  $W_1, W_2$  die gleiche Abbildung  $F(W_1) = F(W_2)$  ergeben, dass man also aus  $F(W)$  das Wirbeltier  $W$  konstruieren kann. Dies zu zeigen ist ebenso wie die Surjektivität, dass nämlich jede Abbildung zu einem Wirbeltier gehört, eine Übung.  $\square$

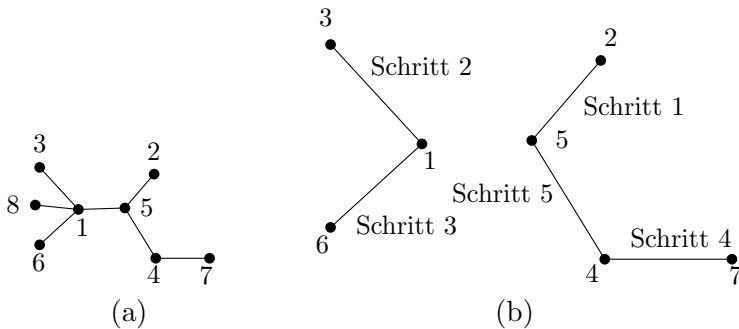
## Aufgaben

1. Zu einer gegebenen Abbildung  $f: V \rightarrow V$  auf einer endlichen Menge  $V$  definieren wir den (gerichteten) *Graphen von  $f$*  als den gerichteten Graphen mit Eckenmenge  $V$  und Kantenmenge  $\{(i, f(i)): i \in V\}$  (wie in dem Beweis oben). Zeigen Sie, dass jede (schwache) Zusammenhangskomponente eines solchen Graphen ein gerichteter Kreis ist, an dessen Ecken möglicherweise Bäume hängen, dessen Kanten zum Kreis zeigen.
2. Gegeben sei eine Abbildung  $f: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$  der Form  $F(W)$  für ein Wirbeltier  $W$ . Beschreiben Sie, wie man das Wirbeltier  $W$  aus der Kenntnis von  $f$  rekonstruieren kann. Zeigen Sie, dass jede Abbildung  $f$  die Form  $F(W)$  hat (benutzen Sie Übung 1).
3. *\*<sup>Inf</sup>* Sei  $f: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$  eine Abbildung. Für jedes  $i \in \{1, 2, \dots, n\}$  wird die Folge  $(i, f(i), f(f(i)), \dots)$  irgendwann periodisch. Entwerfen Sie einen Algorithmus, der für gegebenes  $i$  die (kürzeste) Periode dieser Folge bestimmt. In der Sprache der gerichteten Graphen von Abbildungen möchten wir also im Graphen der Abbildung  $f$  die Länge desjenigen Kreises bestimmen, der  $i$  enthält. Der Speicherbedarf des Algorithmus sollte durch eine Konstante beschränkt sein, also unabhängig von  $n$ . Die Funktion  $f$  steht als „black box“ zur Verfügung.
4. *<sup>Inf</sup>* (a) Entwerfen Sie einen detaillierten Algorithmus, der aus einer Abbildung ein Wirbeltier erzeugt. Wie viele Schritte benötigt er schlimmstenfalls? \*Können Sie ihn so abwandeln, dass er in  $O(n)$  Zeit läuft?  
(b) \*Programmieren Sie den Algorithmus aus (a) und verwenden Sie ihn, um zufällige aufspannende Bäume des vollständigen Graphen aus zufälligen Abbildungen zu erzeugen. Benutzen Sie dieses Programm um den durchschnittlichen (erwarteten) Maximalgrad und Durchmesser eines zufälligen aufspannenden Baumes auf gegebener Eckenanzahl (z.B.  $10^4$ ) experimentell abzuschätzen.

## 8.4 Ein Beweis mit dem Prüfer-Code

Die Anzahl der Folgen der Länge  $k$  über einem Alphabet der Mächtigkeit  $n$  ist  $n^k$ . Wenn wir eine Codierung der aufspannenden Bäume des vollständigen Graphen  $K_n$  durch Folgen der Länge  $n - 2$  über dem Alphabet  $V$  finden, die bijektiv ist, so haben wir einen weiteren Beweis der Cayley–Formel.

Betrachten wir also einen aufspannenden Baum  $T$ , etwa den aus Abbildung 8.2(a). Wir konstruieren nun eine Folge  $P = P(T) = (p_1, p_2, \dots, p_{n-2})$ , den sogenannten Prüfer-Code des Baums  $T$ . Die Grundidee ist, ein Blatt des Baums nach dem anderen abzupflücken,



**Abb. 8.2** (a) Ein aufspannender Baum mit Prüfer-Code  $(5, 1, 1, 4, 5, 1)$ ; (b) Rekonstruktion des Baums aus dem Code.

bis nur noch eine einzelne Kante übrig ist. Wir konstruieren dabei eine Hilfsfolge  $T_0 = T, T_1, T_2, \dots, T_{n-2} \cong K_2$  von Bäumen, und gleichzeitig den Prüfer-Code  $P$ . Angenommen der Baum  $T_{i-1}$  ist schon konstruiert (anfangs ist  $T_0 = T$ , also  $i = 1$ ). Wie jeder Baum mit mindestens 2 Ecken hat  $T_{i-1}$  ein Blatt (d.h. eine Ecke vom Grad 1). Wir suchen uns das kleinste Blatt von  $T_{i-1}$  (die Ecken von  $T$  sind ja die Zahlen von 1 bis  $n$ ), wir entfernen dieses kleinste Blatt zusammen mit der inzidenten Kante aus  $T_{i-1}$  und erhalten  $T_i$ . Gleichzeitig definieren wir das  $i$ -te Glied  $p_i$  für den Prüfer-Code als den *Nachbarn* des gerade gelöschten Blattes. Das ist der ganze Trick: Wir merken uns nicht das Blatt, sondern seinen Nachbarn! Wir führen diese Prozedur sukzessive für  $i = 1, 2, \dots, n - 2$  durch und erhalten so die ganze Folge  $P = P(T)$ .

Jetzt überlegen wir uns, wie wir den ursprünglichen Baum  $T$  aus der Folge  $P = (p_1, p_2, \dots, p_{n-2})$  rekonstruieren können. Wir stellen uns vor, jemand gibt uns eine Folge  $P$ , die er mit der oben beschriebenen Konstruktion aus einem Baum  $T$  erhalten hat, und wir versuchen  $T$  zu rekonstruieren. Das zuerst aus  $T$  entfernte Blatt nennen wir  $b_1$ . Wie können wir  $b_1$  aus der Folge ablesen? Die Ecke  $b_1$  kann sicher nicht in der Folge  $P$  vorkommen, denn man schreibt ja immer nur Ecken auf, die noch vorhanden sind. Andersherum muss aber auch jede Ecke, die in der Menge  $\{p_1, p_2, \dots, p_{n-2}\}$  nicht vorkommt, ein Blatt sein im Baum  $T_0$ ; denn sonst würde man früher oder später von dieser Ecke ein Blatt abpflücken und die Ecke in den Prüfer-Code  $P$  aufnehmen. Das bedeutet, dass  $b_1$  ein Element der Menge  $\{1, 2, \dots, n\} \setminus \{p_1, p_2, \dots, p_{n-2}\}$  ist, und zwar das kleinste.

Wir kennen nun  $b_1$  und wissen, dass diese Ecke im ersten Schritt von der Ecke  $p_1$  abgepfückt wurde, dass also  $b_1$  und  $p_1$  in  $T$  durch eine Kante verbunden sind; wir zeichnen eine Skizze (siehe Abb. 8.2(b)).

Und genauso geht es weiter: Wir haben die Blätter  $b_1, b_2, \dots, b_{i-1}$  gefunden, die in den Schritten 1 bis  $i - 1$  aus  $T$  entfernt wurden, und möchten nun  $b_i$  bestimmen. Es kann keine der Ecken  $p_i, p_{i+1}, \dots, p_{n-2}$  sein, und natürlich auch keine von  $b_1, \dots, b_{i-1}$ ; d.h.  $b_i$  ist das kleinste Element der Menge  $\{1, 2, \dots, n\} \setminus \{p_i, p_{i+1}, \dots, p_{n-2}, b_1, b_2, \dots, b_{i-1}\}$  (die wiederum nicht leer ist). Wir kennen nun auch  $b_i$  und wissen, dass es von  $p_i$  abgepfückt wurde; wir können unsere Zeichnung vervollständigen. In Abb. 8.2(b) sind die ersten 5 Schritte dieser Konstruktion dargestellt. Im sechsten Schritt würden wir die Kante  $\{1, 5\}$  hinzufügen.

Nach  $n - 2$  Schritten kennen wir  $n - 2$  Kanten des aufspannenden Baumes  $T$ , und zwar all die Kanten, die im Laufe der Konstruktion des Prüfer-Codes  $P$  entfernt wurden. Wir brauchen also nur noch die letzte Kante herauszufinden. Ein Ende dieser Kante muss  $p_{n-2}$  sein, der Nachbar der zuletzt entfernten Ecke, und das andere Ende ist die Ecke, die keines der Blätter  $b_1, \dots, b_{n-2}$  ist und auch nicht  $p_{n-2}$ . Im Beispiel in Abb. 8.2 ist es die Kante  $\{1, 8\}$ . Damit haben wir die Beschreibung der Umkehrabbildung abgeschlossen; wir fassen diese Prozedur jedoch noch einmal übersichtlich zusammen, mehr visuell ausgerichtet. Unser hauptsächliches Hilfsmittel ist eine Tabelle mit zwei Zeilen:

$p_1$	$p_2$	$\dots$	$p_{i-1}$	$p_i$	$p_{i+1}$	$\dots$	$p_{n-3}$	$p_{n-2}$	$p_{n-2}$
$e_1$	$e_2$			$e_{i-1}$					
$b_1$	$b_2$	$\dots$	$b_{i-1}$	□					

In der oberen Zeile listen wir alle Zahlen  $p_1, p_2, \dots, p_{n-3}, p_{n-2}, p_{n-2}$  auf (das sind  $n - 1$  Zahlen, denn die Zahl  $p_{n-2}$  wird am Ende noch einmal wiederholt — mit diesem Trick erreichen wir auf elegante Weise, dass der letzte Schritt unserer Prozedur kein Ausnahmefall mehr ist). In die zweite Zeile schreiben wir im Zuge der Konstruktion die Zahlen  $b_1, b_2, \dots, b_{n-1}$ . Wenn wir die Zahlen  $b_1, b_2, \dots, b_{i-1}$  schon hingeschrieben haben, dann ist  $b_i$  die kleinste Zahl, die noch nicht in der unteren Zeile steht und auch nicht in der oberen Zeile darübersteht oder weiter rechts vorkommt. In dem Bild oben schreiben wir dann an die Stelle des Quadrates die kleinste Zahl, die nicht grau hinterlegt ist. Die Kanten  $e_1, e_2, \dots$  des rekonstruierten

aufspannenden Baumes verbinden immer eine Ecke aus der oberen Zeile mit der Ecke, die in der zweiten Zeile unter ihr steht.

Für jede beliebige Folge  $P$  der Länge  $n - 2$  erzeugt dieser Algorithmus einen Graphen  $G$  mit  $n - 1$  Kanten auf der Eckenmenge  $\{1, 2, \dots, n\}$ . Wir wissen auch schon, dass für eine Folge  $P$ , die von einem Baum  $T$  kommt,  $G = T$  ist (so haben wir es gerade eingerichtet). Wir sind aber noch nicht ganz fertig: Wir müssen noch zeigen, dass  $G$  *immer* ein Baum ist, und dass der Prüfer-Code von  $G$  wieder die ursprüngliche Folge  $P$  ist.

Zu diesem Zweck sei  $G_i = (\{1, 2, \dots, n\}, \{e_i, e_{i+1}, \dots, e_{n-1}\})$ . Aus dem Vorgehen bei der Konstruktion der zweiten Zeile sehen wir, dass die Ecke  $b_i$  zur Kante  $e_i$  inzident ist, aber zu keiner der anderen Kanten  $e_{i+1}, \dots, e_{n-1}$ . Daraus folgt, dass  $b_i$  in dem Graphen  $G_i$  den Grad 1 hat. Somit entsteht  $G_i$  aus  $G_{i+1}$  durch Hinzufügen eines Blattes, und aus Hilfssatz 5.1.4 (über das Erzeugen von Bäumen durch Anhängen von Blättern) folgt, dass  $G$  ein Baum ist. Wir sehen sogar genauer, dass eine Komponente des Graphen  $G_i$  ein Baum ist und die restlichen Komponenten  $i - 1$  isolierte Ecken sind.

Wir müssen nun noch prüfen, dass  $b_i$  das kleinste Blatt von  $G_i$  ist. Aus der Definition von  $b_i$  sehen wir, dass ein kleineres Blatt höchstens unter den Ecken  $b_1, b_2, \dots, b_{i-1}$  oder unter  $p_i, \dots, p_{n-2}$  zu finden ist. Der erste Fall ist jedoch unmöglich (weil alle Ecken  $b_1, b_2, \dots, b_{i-1}$  in  $G_i$  den Grad 0 haben). Betrachten wir also für den zweiten Fall eine Ecke  $p_k$  mit  $i < k \leq n - 2$ . Die Ecke  $p_k$  ist in  $G_k$  zu  $b_k$  inzident, und weil  $G_k$  aus isolierten Ecken und einer Baum-Komponente mit mindestens zwei Kanten besteht, ist der Grad der Ecke  $p_k$  in  $G_k$  mindestens 2. Damit folgt, dass die Ecke  $p_k$  auch im Graphen  $G_i$  kein Blatt ist.

Somit ist  $b_i$  das kleinste Blatt im Graphen  $G_i$ , und  $G_{i+1}$  entsteht aus  $G_i$  wirklich nach der oben beschriebenen Prüfer-Codierung für aufspannende Bäume.

Es bleibt noch zu bemerken, dass dieser Algorithmus für jede beliebige Eingabefolge  $P$  funktioniert, weil die Menge, aus der  $b_i$  gewählt wird, nie leer ist, und wir deshalb für jede Eingabefolge  $P$  einen aufspannenden Baum des  $K_n$  erhalten. Wir haben also wirklich eine Bijektion definiert.  $\square$

## Aufgaben

1. Sei  $T$  ein aufspannender Baum des  $K_n$  und  $p = P(T)$  sein Prüfer-Code. Mit  $m_i$  bezeichnen wir die Häufigkeit der Ecke  $i$  in der Folge  $p$ ,  $i = 1, 2, \dots, n$ . Zeigen Sie, dass  $\deg_T(i) = m_i + 1$  für alle  $i$  gilt.
2. <sup>Inf</sup> (a) Entwerfen Sie einen detaillierten Algorithmus, der zu einem Prüfer-Code den zugehörigen aufspannenden Baum von  $K_n$  konstruiert. Wieviele Schritte braucht der Algorithmus im schlimmsten Fall? \*Schaffen Sie es in Zeit  $O(n \log n)$ , oder vielleicht noch schneller?  
(b) \*Programmieren Sie den Algorithmus aus (a). Benutzen Sie ihn wie in Aufgabe 8.3.4(b). Welcher der Algorithmen ist schneller?

## 8.5 Beweise mit Determinanten

Die nun folgenden Beweise der Cayley–Formel beruhen auf linearer Algebra und zeigen uns, dass Determinanten eine kombinatorische Bedeutung haben. (Die Definition der Determinante und die Eigenschaften, die wir benötigen, sind im Anhang zusammengestellt.) Diese Beweise sind ein bisschen schwerer als die vorangegangenen und wir benutzen einige grundlegende Sätze über Determinanten, dafür erhalten wir aber eine Formel für die Anzahl der aufspannenden Bäume eines beliebigen Graphen.

Sei  $G$  ein beliebiger Graph mit Eckenmenge  $V = \{1, 2, \dots, n\}$ ,  $n \geq 2$ , und mit Kantenmenge  $E = \{e_1, e_2, \dots, e_m\}$ . Wir definieren eine  $n \times n$  Matrix  $Q$ , die *Laplace-Matrix* von  $G$ , deren Einträge  $q_{ij}$  wie folgt definiert sind:

$$\begin{aligned} q_{ii} &= \deg_G(i) & i = 1, 2, \dots, n \\ q_{ij} &= \begin{cases} -1 & \text{für } \{i, j\} \in E(G) \\ 0 & \text{sonst} \end{cases} & i, j = 1, 2, \dots, n, i \neq j. \end{aligned}$$

Die Zeilen der Laplace–Matrix summieren sich zum Nullvektor. Diese Beobachtung wird uns gleich von Nutzen sein.

$Q_{ij}$  bezeichne die  $((n-1) \times (n-1))$ -Matrix, die aus  $Q$  durch Streichen der  $i$ -ten Zeile und der  $j$ -ten Spalte entsteht.

Der folgende Satz kann einen schon in Erstaunen versetzen:

**8.5.1 Satz (Matrix-Baum-Satz).** *Für jeden Graphen  $G$  ist die Anzahl aufspannender Bäume  $T(G) = \det Q_{11}$ .*

Übrigens gilt sogar  $T(G) = |\det Q_{ij}|$  für je zwei Indizes  $i, j \in \{1, 2, \dots, n\}$ . Den Beweis dieser Verallgemeinerung stellen wir als Aufgabe 1.

Vor dem Beweis des Matrix-Baum-Satzes wollen wir sehen, dass die Cayley–Formel 8.1.1 aus ihm folgt. Die Laplace–Matrix des vollständigen Graphen  $G = K_n$  hat in der Diagonale lauter Einträge  $n - 1$  und überall sonst  $-1$ . Streichen der ersten Zeile und Spalte ergibt die Matrix

$$\begin{pmatrix} n-1 & -1 & -1 & \dots & -1 \\ -1 & n-1 & -1 & \dots & -1 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ -1 & -1 & -1 & \dots & n-1 \end{pmatrix}.$$

Elementare Zeilen- und Spaltenoperationen lassen die Determinante unverändert. Also los: Erst subtrahieren wir die erste Zeile von jeder anderen, dann ersetzen wir die erste Spalte durch die Summe aller Spalten. Wir erhalten eine Matrix mit  $1, n, n, n, \dots, n$  auf der Diagonalen und unterhalb der Diagonalen nur Nullen. Die Determinante einer Dreiecksmatrix ist das Produkt aller Diagonalelemente, hier also  $n^{n-2}$ .

Wir beweisen Satz 8.5.1 auf zwei Arten. Der erste Beweis ist kürzer und eher graphentheoretisch. Der zweite benutzt mehr lineare Algebra und ist wahrscheinlich die bessere Erklärung, warum der Satz wahr ist.

**Erster Beweis von Satz 8.5.1.** Wir führen einen Induktionsbeweis, und damit dieser funktioniert, verschärfen wir die Induktionsbehauptung und zeigen, dass der Satz auch für Multigraphen gilt, d.h. für Graphen mit Mehrfachkanten. Diese wurden bereits in Abschnitt 4.4 erwähnt: Jedes Paar von Ecken kann durch eine beliebige Anzahl von Kanten verbunden sein (keine, eine oder mehrere). Sind zwei Ecken  $u$  und  $v$  durch mehrere Kanten verbunden, so zählen wir jeden aufspannenden Baum, in dem  $u$  und  $v$  benachbart sind, die entsprechende Anzahl von Malen, mit anderen Worten: wir unterscheiden zwischen aufspannenden Bäumen, die unterschiedliche dieser Kanten verwenden. Der folgende Multigraph hat beispielsweise 6 aufspannende Bäume:



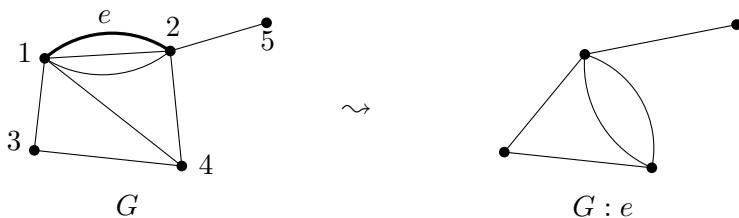
Schlingen lassen wir in unseren Graphen nicht zu, da sie auf die Zahl der aufspannenden Bäume keinen Einfluss haben. Wie sieht die Laplace–Matrix eines Multigraphen aus? Sind zwei Ecken  $u$  und  $v$  durch  $m$  Kanten verbunden, so ist  $q_{uv} = -m$ . Das Diagonalelement

$q_{uu}$  ist der Grad der Ecke  $u$ , wobei Mehrfachkanten entsprechend ihrer Vielfachheit gezählt werden (die mittlere Ecke in der vorangehenden Abbildung ist z.B. vom Grad 5).

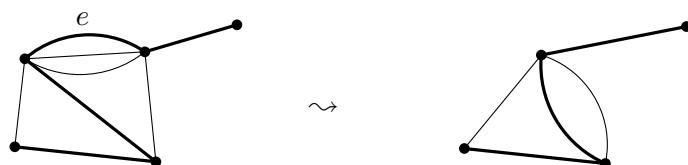
Ferner werden wir die folgende Formel benutzen:

$$T(G) = T(G - e) + T(G : e), \quad (8.1)$$

wobei  $e$  eine beliebige Kante des Graphen  $G$  ist,  $G - e$  den durch Löschen dieser Kante entstehenden Graphen bezeichnet und  $G : e$  den Graphen, den wir durch *Kontraktion* der Kante erhalten. Letzteres bedeutet, dass wir die Kante  $e$  aus  $G$  entfernen und ihre Endencken zu einer verschmelzen. Durch diese Operation können neue Mehrfachkanten entstehen — im Gegensatz zu der in Abschnitt 6.4 eingeführten Art von Kantenkontraktion. Falls allerdings die miteinander verschmolzenen Endencken zuvor noch durch andere Kanten als  $e$  miteinander verbunden waren, so werden diese Kanten gelöscht (stattdessen könnten wir sie zu Schlingen an der durch das Verschmelzen entstandenen Ecke machen, aber Schlingen betrachten wir hier ja nicht). Die folgende Abbildung zeigt ein Beispiel einer Kontraktion:



Um zu sehen, weswegen Gleichung (8.1) gilt, teilen wir die aufspannenden Bäume des Graphen  $G$  in zwei Klassen ein. Aufspannende Bäume der ersten Art sind solche, die die Kante  $e$  nicht enthalten. Das sind aber genau die aufspannenden Bäume des Graphen  $G - e$ , und von diesen gibt es  $T(G - e)$  viele. Aufspannende Bäume der zweiten Art sind solche, die die Kante  $e$  enthalten, und diese entsprechen bijektiv den aufspannenden Bäumen des Graphen  $G : e$ , wie es die folgende Abbildung andeutet



und wovon sich der Leser in Ruhe überzeugen sollte. Somit gibt es  $T(G : e)$  Bäume der zweiten Art.

Nun müssen wir uns noch überlegen, wie sich das Löschen beziehungsweise das Kontrahieren einer Kante auf die Laplace–matrix auswirken. Genauer gesagt: Angenommen, die Kante  $e$  hat die Endecken 1 und 2, wie ändert sich die Matrix  $Q_{11}$ ? Für das Löschen der Kante ist das ganz einfach: Ist  $Q'$  die Laplace–Matrix des Graphen  $G - e$ , so erhalten wir  $Q'_{11}$  aus  $Q_{11}$ , indem wir den Eintrag in der oberen linken Ecke um 1 verringern (das Löschen der Kante beinflusst nur die Elemente der Laplace–Matrix in den Positionen  $(1, 1), (1, 2), (2, 1)$  und  $(2, 2)$ , und wir interessieren uns für die Laplace–Matrix ohne die erste Zeile und die erste Spalte).

Beim Kontrahieren der Kante  $e$  verschwinden die Ecken 1 und 2, und an ihre Stelle tritt eine neue, durch das Verschmelzen entstandene Ecke. Wir nummerieren die Ecken des Graphen  $G : e$  so, dass die neue Ecke die Nummer 1 erhält und eine alte Ecke, wenn sie zuvor die Nummer  $i \geq 3$  hatte, nun die Nummer  $i - 1$ . Es sei  $Q''$  die Laplace–Matrix des Graphen  $G : e$  mit dieser Eckenummerierung. Es ist leicht zu sehen, dass  $Q''_{11} = Q_{11,22}$ , wobei letzteres die Matrix bezeichnet, die wir aus  $Q$  durch Löschen der ersten beiden Zeilen und der ersten beiden Spalten erhalten. Für den Graphen  $G$  aus den beiden obigen Abbildungen gilt zum Beispiel

$$Q_{11} = \begin{pmatrix} 5 & 0 & -1 & -1 \\ 0 & 2 & -1 & 0 \\ -1 & -1 & 3 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}, \quad Q''_{11} = \begin{pmatrix} 2 & -1 & 0 \\ -1 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Jetzt beginnen wir mit dem eigentlichen Induktionsbeweis. Wir zeigen mittels Induktion nach  $m$ , dass für jeden Multigraphen  $G$  mit höchstens  $m$  Kanten gilt, dass  $T(G) = \det Q_{11}$ .

Falls der Knoten Nummer 1 im Multigraphen  $G$  zu keiner Kante inzident ist, so gilt  $T(G) = 0$ . Zugleich ist die erste Zeile der Laplace–Matrix komplett Null, und da sich die Zeilen einer Laplace–Matrix zu Null aufzufaddieren, ist auch die Summe der Zeilen der Matrix  $Q_{11}$  gleich Null. Somit gilt  $\det Q_{11} = 0$  und die zu beweisende Behauptung gilt in diesem Falle. Insbesondere haben wir die Behauptung für den Induktionsanfang  $m = 0$  gezeigt.

Interessanter ist der zweite Fall, dass die Ecke Nummer 1 zu mindestens einer Kante inzident ist. Sei  $e$  eine solche Kante. Wir wählen eine Nummerierung der Ecken, in der die zweite Endecke von  $e$  die

Nummer 2 erhält, und definieren  $Q$ ,  $Q'$  und  $Q''$  wie zuvor als die jeweiligen Laplace-Matrizen von  $G$ ,  $G - e$  und  $G : e$  bezüglich dieser Eckenummerierung. Nach Gleichung (8.1) und nach Induktionsvoraussetzung gilt

$$T(G) = T(G - e) + T(G : e) = \det Q'_{11} + \det Q''_{11} = \det Q'_{11} + \det Q_{11,22}.$$

Bekanntlich ist die Determinante einer Matrix eine lineare Funktion jeder Spalte, und Addition des Vektors  $e_1 = (1, 0, 0, \dots, 0)$  zur ersten Zeile von  $Q'_{11}$  ergibt die Matrix  $Q_{11}$ . Daher gilt  $\det Q_{11} = \det Q'_{11} + \det R$ , wobei die Matrix  $R$  als erste Zeile den Vektor  $e_1$  hat und in den übrigen Zeilen mit  $Q_{11}$  übereinstimmt. Indem wir die Determinante nach der ersten Zeile entwickeln, sehen wir, dass  $\det R = \det Q_{11,22}$  und folglich  $\det Q'_{11} + \det Q_{11,22} = \det Q'_{11} + \det R = \det Q_{11}$ . Dies beendet den Induktionsschritt und somit den ersten Beweis von Satz 8.5.1. Wir merken noch an, dass wir hier nur einen ganz einfachen Spezialfall der Determinantenentwicklungsformel<sup>1</sup> benötigt haben, nämlich den, dass die Zeile, nach der wir entwickeln, eine einzige Eins und ansonsten nur Nullen enthält, und für diesen Spezialfall folgt die Formel unmittelbar aus der Definition der Determinante.  $\square$

**Zweiter Beweis von Satz 8.5.1.** Zunächst einmal wählen wir eine völlig beliebige Orientierung  $\vec{G}$  für den Graphen  $G$ , d.h. wir legen bei jeder Kante  $e_k$  fest, an welcher der beiden Enden  $e_k$  beginnt und an welcher Enden  $e_k$  endet<sup>2</sup> (die Terminologie für gerichtete Graphen wurde in Abschnitt 4.5 eingeführt). Die gerichtete Kante bezeichnen wir mit  $\vec{e}_k$ . Interessanterweise ist das Ergebnis völlig unabhängig von der konkreten Wahl der Orientierung; aber wir brauchen eine für den Beweis. An dieser Stelle definieren wir die Inzidenzmatrix  $D = D_{\vec{G}}$  für die gewählte Orientierung  $\vec{G}$ . Die Inzidenzmatrix hat  $n$  Zeilen, die den Ecken von  $\vec{G}$  entsprechen, und  $m$  Spalten, die den Kanten von  $\vec{G}$  entsprechen. Die Einträge sind

$$d_{ik} = \begin{cases} -1 & \text{wenn } \vec{e}_k \text{ bei } i \text{ beginnt} \\ 1 & \text{wenn } \vec{e}_k \text{ bei } i \text{ endet} \\ 0 & \text{sonst} \end{cases}$$

<sup>1</sup> „Determinantenentwicklungsformel“ ist vermutlich das längste Wort in diesem Buch.

<sup>2</sup>Von den beiden Enden der ungerichteten Kante wird also eine zur „Anfangsseite“.

Die Inzidenzmatrix  $D$  hat in jeder Spalte genau eine 1 und eine  $-1$  und sonst Nullen. Die Summe aller Zeilen ist der Nullvektor.

Mit  $\bar{D}$  bezeichnen wir die Matrix, die aus  $D$  durch Streichen der ersten Zeile entsteht. Die Inzidenz- und die Laplace-Matrix sind beide vom Graphen  $G$  abgeleitet; der Beweis funktioniert nun so, dass wir die Anzahl der aufspannenden Bäume mithilfe der Matrix  $D$  ausdrücken und den folgenden algebraischen Zusammenhang zwischen den beiden Matrizen ausnutzen.

**8.5.2 Lemma.** *Für jede Orientierung  $\vec{G}$  des Graphen  $G$  gelten die Gleichungen  $DD^T = Q$  und  $\bar{D}\bar{D}^T = Q_{11}$ , wobei  $D = D_{\vec{G}}$ .*

*Beweis.* Das Produkt einer  $(n \times m)$ - mit einer  $(m \times n)$ -Matrix ist eine  $(n \times n)$ -Matrix, der  $(i, j)$ -Eintrag von  $DD^T$  ist  $\sum_{k=1}^m d_{ik}d_{jk}$ . Für  $i = j$  ist das Produkt  $d_{ik}d_{jk} = d_{ik}^2$  gleich 1, wenn  $i$  Anfangs- oder Endecke der Kante  $\vec{e}_k$  ist, und 0 sonst; die betrachtete Summe ist also der Grad der Ecke  $i$  in  $G$ . Für  $i \neq j$  ist das Produkt  $d_{ik}d_{jk}$  nur dann von Null verschieden, nämlich  $-1$ , wenn  $\vec{e}_k = (i, j)$  oder  $\vec{e}_k = (j, i)$ . So ist die Laplace-Matrix  $Q$  aber gerade definiert und wir haben  $DD^T = Q$  bewiesen. Für die zweite Gleichung muss man sich nur noch überlegen, wie sich das Streichen der ersten Zeile von  $D$  im Produkt  $DD^T$  auswirkt.  $\square$

Das nächste Lemma beleuchtet den Zusammenhang zwischen Bäumen und Determinanten:

**8.5.3 Lemma.** *T sei ein Graph auf der Eckenmenge  $\{1, 2, \dots, n\}$  mit  $n - 1$  Kanten ( $n \geq 2$ ) und  $\vec{T}$  sei eine Orientierung von T. Weiter sei  $C = D_{\vec{T}}$  die Inzidenzmatrix des gerichteten Graphen  $\vec{T}$  und  $\bar{C}$  die quadratische Matrix, die aus  $C$  durch Löschen der ersten Zeile entsteht. Dann nimmt  $\det \bar{C}$  einen der Werte 0, 1,  $-1$  an und ist genau dann ungleich Null, wenn T ein Baum ist (d.h. wenn T ein aufspannender Baum des vollständigen Graphen auf der Eckenmenge  $\{1, 2, \dots, n\}$  ist).*

*Beweis.* Wir führen Induktion über  $n$ . Der Induktionsanfang ist leicht: Ist  $n = 2$ , so hat  $T$  genau eine Kante, ist also aufspannender Baum, und der Eintrag in der  $(1 \times 1)$ -Matrix  $\bar{C}$  ist entweder  $-1$  oder 1.

Sei nun  $n > 2$ . Wir unterscheiden zwei Fälle, je nachdem ob eine der Ecken  $2, 3, \dots, n$  in  $T$  Grad 1 hat oder nicht.

1. Fall: Eine der Ecken  $2, 3, \dots, n$  hat Grad 1. Ohne Beschränkung der Allgemeinheit können wir annehmen, dass es sich um die Ecke  $n$  handelt (andernfalls nummerieren wir die Ecken einfach um). Die Ecke  $n$  gehört also zu genau einer Kante  $\vec{e}_k$ . Für die Matrix  $\bar{C}$  bedeutet das, dass sie in der letzten Zeile lauter Nullen hat, außer in der  $k$ -ten Spalte, wo eine 1 oder  $-1$  steht.

Wir entwickeln die Determinante von  $\bar{C}$  nach der Zeile, die zur Ecke  $n$  gehört, also nach der  $(n-1)$ -ten:

$$\det \bar{C} = \sum_{j=1}^{n-1} (-1)^{n-1+j} \bar{c}_{n-1,j} \det \bar{C}_{n-1,j},$$

wobei  $\bar{C}_{ij}$  für die Matrix  $\bar{C}$  ohne die  $i$ -te Zeile und  $j$ -te Spalte steht. Weil in der  $(n-1)$ -ten Zeile nur ein Eintrag von Null verschieden ist, nämlich  $\bar{c}_{n-1,k}$ , erhalten wir  $\det \bar{C} = (-1)^{n-1+k} \bar{c}_{n-1,k} \det \bar{C}_{n-1,k}$ , und somit  $|\det \bar{C}| = |\det \bar{C}_{n-1,k}|$ .

Sei  $\vec{T}'$  der gerichtete Graph, der aus  $\vec{T}$  durch Entfernen der Ecke  $n$  und der Kante  $\vec{e}_k$  entsteht. Aus der Inzidenzmatrix  $C' = D_{\vec{T}'}$  von  $\vec{T}'$  erhalten wir durch Streichen der ersten Zeile gerade die Matrix  $\bar{C}' = \bar{C}_{n-1,k}$ . Nach Induktionsvoraussetzung ist deshalb  $|\det \bar{C}'|$  gleich 1 oder 0, je nachdem ob  $T'$  (die ungerichtete Version von  $\vec{T}'$ ) aufspannender Baum auf  $\{1, 2, \dots, n\}$  ist oder nicht. Da wir aus  $T$  eine Ecke vom Grad 1 gelöscht hatten, ist  $T'$  genau dann ein aufspannender Baum, wenn  $T$  einer ist. Damit ist der Fall geklärt, dass es in  $T$  unter  $2, 3, \dots, n$  eine Ecke vom Grad 1 gibt.

2. Fall: Keine der Ecken  $2, 3, \dots, n$  hat Grad 1 in  $T$ . Dann muss  $T$  eine isolierte Ecke haben; denn sonst hätte Ecke 1 mindestens den Grad 1 und alle anderen Ecken hätten mindestens Grad 2, die Gradsumme wäre also größer als  $2|E(T)| = 2(n-1)$  — Widerspruch.

Mit einer isolierten Ecke ist  $T$  sicher kein aufspannender Baum. Wenn wir also zeigen, dass  $\det \bar{C} = 0$ , ist der Beweis geschafft. Wenn eine der Ecken  $2, 3, \dots, n$  isoliert ist, dann hat  $\bar{C}$  eine Nullzeile. Ist die Ecke 1 isoliert, dann ist die Zeilensumme von  $\bar{C}$  der Nullvektor, weil  $D_{\vec{T}}$  Zeilensumme Null hat und die weggelassene Zeile eine Nullzeile ist. In beiden Fällen folgt  $\det \bar{C} = 0$ .  $\square$

Mit diesem Lemma wissen wir nun, dass der Graph  $G$  genauso viele aufspannende Bäume hat wie es  $((n-1) \times (n-1))$ -Untermatrizen mit Determinante 1 oder  $-1$  in  $\bar{D}$  gibt. Der letzte Baustein im

Beweis des Matrix-Baum-Satzes 8.5.1 ist der folgende Satz über Determinanten.

**8.5.4 Satz (Binet–Cauchy).** *A sei eine beliebige Matrix mit n Zeilen und m Spalten. Dann ist*

$$\det(AA^T) = \sum_I \det(A_I)^2,$$

wobei über alle  $n$ -elementigen Teilmengen  $I \in \binom{\{1, 2, \dots, n\}}{n}$  summiert wird und  $A_I$  die Matrix bezeichnet, die aus  $A$  durch Streichen aller Spalten entsteht, deren Indizes nicht in  $I$  enthalten sind.

Der Vollständigkeit halber werden wir auch diesen Satz beweisen, doch erst einmal sehen wir uns an, wie der Matrix-Baum-Satz aus dem Binet–Cauchy–Theorem folgt. Das geht jetzt fix, die Arbeit steckt eben in den beiden Lemmas und dem Binet–Cauchy–Theorem. Aus Lemma 8.5.2 und Satz 8.5.4 erhalten wir

$$\det Q_{11} = \det(\bar{D}\bar{D}^T) = \sum_{I \in \binom{\{1, 2, \dots, n-1\}}{n-1}} \det(\bar{D}_I)^2,$$

und mit Lemma 8.5.3 sehen wir, dass auf der rechten Seite gerade die Anzahl der aufspannenden Bäume von  $G$  steht.  $\square$

*Beweis des Binet–Cauchy–Theorems 8.5.4.* Wir schreiben  $M = AA^T$ . Nach Definition der Determinante ist

$$\det M = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \prod_{i=1}^n m_{i, \pi(i)}.$$

Dabei wird über alle Permutationen  $\pi$  auf der Menge  $\{1, 2, \dots, n\}$  summiert, und  $\operatorname{sgn}(\pi)$  steht für das *Vorzeichen* (oder *Signum*) der Permutation  $\pi$ . Das Vorzeichen ist stets  $+1$  oder  $-1$ . Die genaue Definition des Vorzeichens benötigen wir hier nicht, wir brauchen nur die folgende Eigenschaft:

**8.5.5 Tatsache.** *Ist  $\pi$  eine Permutation auf  $\{1, 2, \dots, n\}$  und sind  $i, j \in \{1, 2, \dots, n\}$ ,  $1 \leq i < j \leq n$ , so bezeichne das Symbol  $\pi_{i \leftrightarrow j}$  die Permutation, die bei  $i$  den Wert  $\pi(j)$  annimmt, bei  $j$  den Wert  $\pi(i)$ , und die überall sonst mit  $\pi$  übereinstimmt. Dann gilt  $\operatorname{sgn}(\pi) = -\operatorname{sgn}(\pi_{i \leftrightarrow j})$ .*

Jetzt setzen wir für die Einträge  $m_{ij}$  der Matrix  $M$  die Werte  $m_{ij} = \sum_{k=1}^m a_{ik}a_{jk}$  in obige Determinantenformel ein und multiplizieren aus. Wir erhalten so

$$\begin{aligned}\det M &= \sum_{\pi} \operatorname{sgn}(\pi) \prod_{i=1}^n \left( \sum_{k=1}^m a_{ik}a_{\pi(i)k} \right) \\ &= \sum_{\pi} \operatorname{sgn}(\pi) \sum_{k_1, k_2, \dots, k_n=1}^m \prod_{i=1}^n a_{i,k_i}a_{\pi(i),k_i}.\end{aligned}$$

Wir führen jetzt etwas praktischere Bezeichnungen ein — eine Methode, die sich oft als hilfreich erweist, auch wenn Bezeichnungen im Grunde natürlich austauschbar sind. Wir können die Wahl des  $n$ -Tupels  $k_1, \dots, k_n$  bei der inneren Summation als Wahl einer Abbildung  $f: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, m\}$  auffassen, definiert durch  $f(i) = k_i$ . Wir schreiben jetzt also

$$\det M = \sum_{\pi} \operatorname{sgn}(\pi) \sum_{f: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, m\}} \prod_{i=1}^n a_{i,f(i)}a_{\pi(i),f(i)}.$$

Wir vertauschen nun die Reihenfolge der Summationen: Zuerst summieren wir über die Permutationen  $\pi$  (innere Summe) und dann über die Funktionen  $f$  (äußere Summe). Außerdem treiben wir das Spiel mit den praktischeren Bezeichnungen weiter und definieren die Symbole

$$P(f, \pi) = \prod_{i=1}^n a_{i,f(i)}a_{\pi(i),f(i)},$$

$$S(f) = \sum_{\pi} \operatorname{sgn}(\pi) P(f, \pi),$$

so dass wir nun

$$\det M = \sum_{f: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, m\}} S(f)$$

schreiben können. Das nun folgende Lemma spielt eine Schlüsselrolle in diesem Beweis:

**8.5.6 Lemma.** *Ist die Funktion  $f: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, m\}$  nicht injektiv, so ist  $S(f) = 0$  (unabhängig von der Matrix  $A$ ).*

*Beweis des Lemmas.* Ist  $f$  nicht injektiv, so existieren Indizes  $i$  und  $j$  mit  $f(i) = f(j)$ . Dann sind die Produkte  $P(f, \pi)$  und  $P(f, \pi_{i \leftrightarrow j})$  für jede Permutation  $\pi$  gleich (zur Bezeichnung  $\pi_{i \leftrightarrow j}$  siehe Tatsache 8.5.5). Läuft  $\pi$  über alle Permutationen, dann läuft auch  $\pi_{i \leftrightarrow j}$  über alle Permutationen (wenn auch in anderer Reihenfolge), und daher ist

$$S(f) = \sum_{\pi} \operatorname{sgn}(\pi_{i \leftrightarrow j}) P(f, \pi_{i \leftrightarrow j}) = \sum_{\pi} -\operatorname{sgn}(\pi) P(f, \pi) = -S(f);$$

also ist wie behauptet  $S(f) = 0$ .

Mit diesem Lemma brauchen wir also nur noch über alle *injektiven* Funktionen  $\{1, 2, \dots, n\} \hookrightarrow \{1, 2, \dots, m\}$  zu summieren:

$$\det(AA^T) = \sum_{f: \{1, 2, \dots, n\} \hookrightarrow \{1, 2, \dots, m\}} S(f),$$

Wir wollen zeigen, dass die rechte Seite in obiger Gleichung gleich  $\sum_I \det(A_I)^2$  ist, wobei über  $I \in \binom{\{1, 2, \dots, m\}}{n}$  summiert wird. Für jedes  $I \in \binom{\{1, 2, \dots, m\}}{n}$  ist

$$\det(A_I)^2 = \det(A_I) \det(A_I^T) = \det(A_I A_I^T).$$

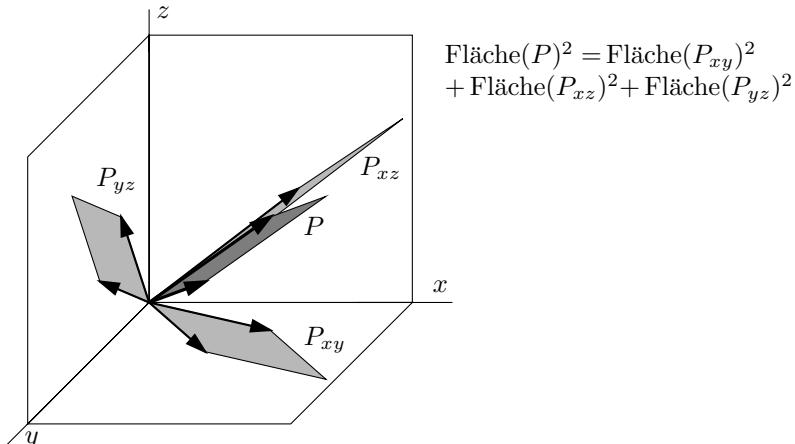
Diese Determinante können wir in genau der gleichen Weise ausdrücken wie die Determinante von  $AA^T$ . Diesmal ergibt sich

$$\det(A_I A_I^T) = \sum_{f: \{1, 2, \dots, n\} \hookrightarrow I} S(f).$$

Damit kommen wir zum Ende:

$$\begin{aligned} \sum_{I \in \binom{\{1, 2, \dots, m\}}{n}} \det(A_I)^2 &= \sum_{I \in \binom{\{1, 2, \dots, m\}}{n}} \sum_{f: \{1, 2, \dots, n\} \hookrightarrow I} S(f) \\ &= \sum_{f: \{1, 2, \dots, n\} \hookrightarrow \{1, 2, \dots, m\}} S(f) = \det(AA^T). \end{aligned}$$

Die zweite Gleichheit gilt deshalb, weil durch eine injektive Funktion  $f: \{1, 2, \dots, n\} \hookrightarrow \{1, 2, \dots, m\}$  ihr ( $n$ -elementiger) Wertebereich eindeutig bestimmt ist. Damit ist das Binet–Cauchy–Theorem 8.5.4 bewiesen.  $\square$

**Abb. 8.3** Die geometrische Bedeutung des Binet–Cauchy–Theorems.

Das Binet–Cauchy-Theorem lässt sich geometrisch als Satz über Volumina interpretieren. Wir verzichten hier auf alle Beweise, denn obwohl elementar, würden sie uns weiter in die Geometrie führen, als wir in diesem Buch gehen wollen. Verstehen wir die  $n$  Zeilen einer  $(n \times m)$ -Matrix als Vektoren  $a_1, a_2, \dots, a_n$  im  $m$ -dimensionalen Raum  $\mathbb{R}^m$ , so spannen diese  $n$  Vektoren ein  $n$ -dimensionales Parallelotop  $P$  in  $\mathbb{R}^m$  auf; Abb. 8.3 illustriert das für den Fall  $m = 3$  und  $n = 2$  (das ist so ziemlich der einzige interessante Fall, den wir zeichnen können). Man kann zeigen, dass  $|\det(AA^T)|$  das Quadrat des  $n$ -dimensionalen Volumens von  $P$  ist (in unserem Beispiel das Quadrat der Fläche von  $P$ ). Die Auswahl einer  $(n \times n)$ -Untermatrix  $B$  entspricht dem Projizieren der Vektoren  $a_1, a_2, \dots, a_n$  auf den  $n$ -dimensionalen Teilraum von  $\mathbb{R}^m$ , der von den entsprechenden  $n$  Koordinatenachsen aufgespannt wird (eine Koordinaten-Hyperebene). In unserem Beispiel gibt es — entsprechend den 3 Koordinatenebenen — 3 mögliche  $(2 \times 2)$ -Untermatrizen.  $|\det(BB^T)|$  ist das Quadrat des Volumens der zugehörigen Projektion von  $P$ , und das Binet–Cauchy–Theorem sagt nun, dass das quadrierte Volumen von  $P$  gleich ist der Summe der quadrierten Volumina aller Projektionen von  $P$  auf Koordinatenhyperebenen. Das zweite interessante Beispiel ist übrigens der Fall  $n = 1$  und  $m = 2$  — der Leser sollte sich die Freude nicht entgehen lassen, selbst herauszubekommen, welcher berühmte Satz in diesem Fall herauskommt.

## Aufgaben

1. In dieser Aufgabe ist  $G$  ein Graph auf  $n$  Ecken,  $Q$  ist seine Laplace-Matrix, und  $Q^*$  ist die Matrix, deren  $(i, j)$ -Eintrag  $(-1)^{i+j} \det Q_{ij}$  ist.

- (a) Zeigen Sie, dass  $\det Q = 0$  ist.
- (b) Beweisen Sie: Wenn  $G$  zusammenhängend ist, dann hat  $Q$  Rang  $n - 1$ .
- (c) \*Beweisen Sie, dass der Rang der Laplace-Matrix eines unzusammenhängenden Graphen höchstens  $n - 2$  ist. Folgern Sie daraus, dass  $Q^*$  die Nullmatrix ist für unzusammenhängendes  $G$ .
- (d) Zeigen Sie: Ist  $G$  zusammenhängend und  $x \in \mathbb{R}^n$  ein beliebiger Vektor, dann gilt  $Qx = 0$  genau dann, wenn  $x$  ein Vielfaches des Vektors  $(1, 1, \dots, 1)$  ist.
- (e) \*Zeigen Sie, dass das Produkt  $QQ^*$  die Nullmatrix ergibt. Folgern Sie mithilfe von (d), dass alle Einträge der Matrix  $Q^*$  gleich sind.
2. Lösen Sie nochmals Aufgabe 8.1.2, diesmal mit dem Matrix-Baum-Satz 8.5.1.
3. \*Bestimmen Sie  $T(K_{n,m})$  (die Anzahl aufspannender Bäume im vollständigen bipartiten Graphen).
4. \*Sei  $G$  ein (ungerichteter) Graph und  $M$  seine Inzidenzmatrix; hat  $G$   $n$  Ecken  $v_1, v_2, \dots, v_n$  und  $m$  Kanten  $e_1, e_2, \dots, e_m$ , dann ist  $M$  eine  $n \times m$  Matrix mit

$$m_{ik} = \begin{cases} 1 & \text{wenn } v_i \in e_k \\ 0 & \text{sonst.} \end{cases}$$

Zeigen Sie, dass die beiden folgenden Bedingungen äquivalent sind:

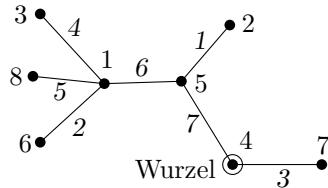
- (i)  $G$  ist bipartit.
- (ii) Jede quadratische Untermatrix von  $M$  (die durch Streichen von Zeilen und Spalten entsteht) hat Determinante 0, 1, oder  $-1$ . Eine Matrix  $M$  mit dieser Eigenschaft heißt *total unimodular*.

## 8.6 Der zurzeit wohl einfachste Beweis

Welcher Beweis ist der einfachste? Das ist natürlich Geschmackssache. Jedenfalls gibt es auch in gut erforschten Bereichen der Mathematik immer wieder die Chance Neues zu entdecken. Ein Beispiel passt in dieses Kapitel. Erst kürzlich hat ein Mathematiker, der Statistiker Jim Pitman von der University of California in Berkeley einen weiteren Beweis der Cayley-Formel gefunden, der auf dem Prinzip des doppelten Abzählens beruht. Diesen einfachen Trick haben wir im vorigen Kapitel mehrfach verwendet. Hier wenden wir ihn wieder an, und zwar auf eine Variante des Ausgangsproblems.

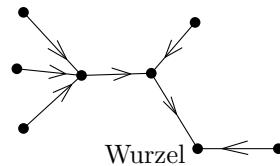
In diesem Beweis zählen wir nicht einfach Bäume, auch nicht Wirbeltiere, nein, wir zählen zweifach SUKOWUBs. Dieses Kunstwort ist eine Abkürzung für SUkzessive KOnstruierte WURzelBäume.

Was ist ein SUKOWUB? Formal ein Tripel  $(T, w, \ell)$ , bestehend aus einem Baum  $T$  auf der Eckenmenge  $V = \{1, 2, \dots, n\}$  (in diesem ganzen Abschnitt ist  $n$  eine feste ganze Zahl), einer Wurzel  $w \in V$  und einer Markierung  $\ell$  der Kanten von  $T$  mit Zahlen  $\{1, 2, \dots, n-1\}$  (d.h.  $\ell$  ist eine Bijektion  $\ell : E(T) \rightarrow \{1, 2, \dots, n-1\}$ ). Das folgende Bild macht die Definition eines SUKOWUB klarer als die formale Definition.



Zugegeben, ein SUKOWUB sieht komplizierter aus als ein Baum (oder ein Wirbeltier). Allerdings gibt es eine einfache alternative Definition. Wir können uns vorstellen, dass wir mit der Eckenmenge  $V$  und einer leeren Kantenmenge beginnen und einen Wurzelbaum konstruieren, indem wir nach und nach einzelne Kanten hinzufügen. Die Markierung  $\ell$  (die Zahlen an den Kanten) codiert die Reihenfolge, in der die Kanten hinzugefügt werden. Weil wir bei jedem Baum  $T$  die Wurzel  $r$  auf  $n$  Arten wählen können und die Markierung  $\ell$  auf  $(n-1)!$  Arten, gibt es insgesamt  $n(n-1)!T(K_n)$  SUKOWUBs.

Nun wollen wir die Anzahl der SUKOWUBs nochmals auf andere Art berechnen. Dazu fassen wir zunächst einmal Wurzelbäume als orientierte Bäume auf, bei denen alle Kanten in Richtung auf die Wurzel hin gerichtet sind:



Die Wurzel ist dann die eindeutige Ecke, aus der keine Kante herausführt (d.h. die einzige Ecke mit Ausgrad 0). Andererseits korrespondiert jede Orientierung eines Baums, in der genau eine Ecke den Ausgrad 0 hat, zu einem eindeutigen Wurzelbaum. Wir bestimmen nun, auf wie viele Arten wir aus dem leeren gerichteten Graph durch schrittweises Hinzufügen gerichteter Kanten in  $(n-1)$  Schritten einen solchen speziell orientierten Baum erzeugen können — und haben damit einen zweiten Ausdruck für die Anzahl aller SUKOWUBs.

Die erste gerichtete Kante muss zwischen zwei verschiedene Ecken verlaufen, die können wir auf  $n(n - 1)$  Arten auswählen. Die zweite Kante muss von der ersten verschieden sein, und sie muss eine weitere Bedingung erfüllen: Weil alle Kanten zur Wurzel hin zeigen, geht von jeder Ecke höchstens eine Kante aus; der Fuß der ersten Kante muss also vom Fuß der zweiten verschieden sein. Für die zweite Kante gibt es  $n(n - 2)$  Möglichkeiten; das direkt herzuleiten ist etwas mühsam und unübersichtlich (bitte versuchen Sie es!), leichter ist es, gleich den allgemeinen Fall zu betrachten.

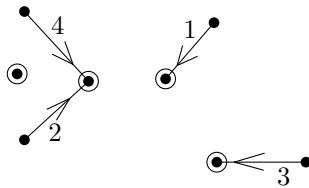
Wie also sieht diese Einschränkung bei der Wahl der nächsten Kante allgemein aus? Wir müssen die folgenden beiden Regeln beachten:

(A) Wir dürfen keinen Kreis erzeugen (in dem zu Grunde liegenden ungerichteten Graphen, in dem wir die Information über die Orientierung der Kanten unbeachtet lassen). Die neu zu wählende Kante muss also zwischen zwei verschiedenen Komponenten des bisher erzeugten Graphen verlaufen (mit Komponenten meinen wir wiederum die Komponenten des zu Grunde liegenden ungerichteten Graphen).

(B) Am Ende muss in jeder Ecke außer der Wurzel eine Kante beginnen. Weil wir nur  $n - 1$  Kanten wählen können, haben wir nichts zu verschenken, in jedem Schritt muss die neu eingefügte Kante in einer Ecke beginnen, von der noch keine zuvor gewählte Kante ausgeht.

Die folgende Beobachtung ist ganz wesentlich: *In jeder Komponente des bisher konstruierten Graphen gibt es genau eine Ecke mit Ausgrad 0.* Das folgt aus der Tatsache, dass jede Komponente mit  $m$  Ecken  $m - 1$  Kanten hat (denn nach (A) ist sie ein Baum) und daraus, dass von jeder Ecke höchstens eine Kante ausgeht (weil wir auch Bedingung (B) in allen vorangegangenen Schritten befolgt haben).

Daraus folgt, dass der Graph zu dem Zeitpunkt, wo wir unter Berücksichtigung der Regeln (A) und (B) schon  $k$  gerichtete Kanten ausgewählt haben,  $n - k$  Komponenten hat (bitte vergewissern Sie sich dessen). Das folgende Bild zeigt die Situation nach der Wahl von vier Kanten (d.h.  $k = 4$ ) im SUKOWUB aus dem ersten Bild:



Die nächste Kante, die mit  $k + 1$  markiert wird, kann in eine beliebige Ecke hineinführen, beginnen muss sie jedoch in der Wurzel einer anderen Komponente. Für diese Kante haben wir dann  $n(n - k - 1)$  Möglichkeiten. Mit diesem Vorgehen konstruieren wir in  $n-1$  Schritten einen SUKOWUB. Wenn sich zwei solche Konstruktionen an irgendeiner Stelle unterscheiden, erhalten wir verschiedene SUKOWUBs (womit der Name gerechtfertigt ist). Die Gesamtzahl aller SUKOWUBs ist also

$$\prod_{k=0}^{n-2} n(n - k - 1) = (n - 1)!n^{n-1}.$$

Aus dem Vergleich dieses Ausdrucks mit dem obigen Ergebnis  $n(n - 1)!T(K_n)$  erhalten wir wieder  $T(K_n) = n^{n-2}$ , die Cayley-Formel.



# 9

# Endliche projektive Ebenen

---

Mathematiker interessieren sich besonders für Objekte, die in einem gewissen Sinn regulär sind. Ein gutes Beispiel sind die platonischen Körper, die wir in Kapitel 6.3 kennen gelernt haben. Es gibt nur wenige, sie sind schön, und sie kommen in Anwendungen vor. Ihre Symmetriegruppen spielen etwa in der Physik eine wichtige Rolle.

In diesem Kapitel werden wir sehr reguläre Familien endlicher Mengen betrachten, die so genannten projektiven Ebenen. Wie der Name vermuten lässt, ist dieser Begriff geometrisch motiviert. Endliche projektive Ebenen sind hochgradig symmetrisch, und auch von ihnen gibt es nicht viele. Will man ihren Nutzen und ihre Schönheit schätzen, muss man zunächst etwas über sie lernen. Übrigens ist das Studium regulärer Konfigurationen von Mengen ähnlich wie bei projektiven Ebenen ein starker Zweig der Kombinatorik (siehe auch Kapitel 13). Empfehlenswerte weiterführende Literatur zu dem vorliegenden Kapitel ist das Buch von Van Lint und Wilson [8].

## 9.1 Definition und grundlegende Eigenschaften

Eine endliche projektive Ebene ist ein System von Teilmengen einer endlichen Menge mit gewissen Eigenschaften.

**9.1.1 Definition (Endliche projektive Ebene).** Sei  $X$  eine endliche Menge, und sei  $\mathcal{L}$  ein System von Teilmengen von  $X$ . Das Paar  $(X, \mathcal{L})$  heißt eine endliche projektive Ebene falls es den folgenden Axiomen genügt:

- (P0) Es gibt eine 4-elementige Menge  $F \subseteq X$ , so dass  $|L \cap F| \leq 2$  für jede Menge  $L \in \mathcal{L}$ .
- (P1) Je zwei verschiedene Mengen  $L_1, L_2 \in \mathcal{L}$  schneiden sich in genau einem Element, das heißt  $|L_1 \cap L_2| = 1$ .
- (P2) Zu je zwei verschiedene Elementen  $x_1, x_2 \in X$  gibt es genau eine Menge  $L \in \mathcal{L}$ , so dass  $x_1 \in L$  und  $x_2 \in L$ .

Ist  $(X, \mathcal{L})$  eine endliche projektive Ebene, so nennen wir die Elemente von  $X$  *Punkte* und die Mengen in  $\mathcal{L}$  *Geraden*. Ist  $x \in X$  ein Punkt,  $L \in \mathcal{L}$  eine Gerade und  $x \in L$ , so sagen wir „der Punkt  $x$  liegt auf der Geraden  $L$ “ oder auch „die Gerade  $L$  geht durch den Punkt  $x$ “.

Übersetzen wir die Axiome (P0)–(P2) in diese neue Sprache, klingen sie schon wie bekannte geometrische Aussagen. Axiom (P1) sagt, dass sich je zwei verschiedene Geraden in genau einem Punkt schneiden (natürlich stimmt das in der gewöhnlichen ebenen Geometrie nicht immer — die Ausnahme sind parallele Geraden!). Axiom (P2) besagt, dass durch zwei verschiedene Punkte genau eine Gerade geht. Axiom (P0) schließlich verlangt die Existenz von vier Punkten, von denen keine drei kollinear sind. Dieses Axiom ist eher behelfsmäßiger Natur und dient nur dazu, einige „degenerierte“ Arten von Mengensystemen auszuschließen, die (P1) und (P2) erfüllen, aber eher uninteressant sind.

Sind  $a, b \in X$  zwei verschiedene Punkte einer endlichen projektiven Ebene, so bezeichnen wir die eindeutig bestimmte Gerade  $L \in \mathcal{L}$ , die durch  $a$  und  $b$  geht, mit dem Symbol  $\overline{ab}$ . Sind  $L, L' \in \mathcal{L}$  zwei verschiedene Geraden, so heißt der eindeutig bestimmte Punkt in  $L_1 \cap L_2$  ihr Schnittpunkt (genau genommen ist der Schnitt von  $L_1$  und  $L_2$  natürlich eine einelementige Menge).

Endliche projektive Ebenen sind das endliche Analogon zu der so genannten projektiven Ebene (genauer der *reellen projektiven Ebene*), die man in der Geometrie studiert. Die oben eingeführte Terminologie („Punkte“, „Geraden“, usw.) folgt dieser Analogie. Wir machen daher einen kleinen Exkurs und erklären die reelle projektive Ebene. Zunächst sollten wir vielleicht bemerken, dass das Adjektiv „reell“ darauf hinweist, dass die reelle projektive Ebene aus der Menge der reellen Zahlen konstruiert wird, und nicht etwa, dass andere projektive Ebenen irgendwie irreal sind.

In der gewöhnlichen (euklidischen) Ebene schneiden sich je zwei Geraden in genau einem Punkt, mit einer Ausnahme: Parallele Geraden schneiden sich überhaupt nicht. In vielen geometrischen Überlegungen sind solche Ausnahmen eher störend, bei Beweisen wie in Rechnungen, weil man mehrere Fälle unterscheiden und getrennt behandeln muss. Die reelle projektive Ebene ist eine Erweiterung der euklidischen Ebene durch eine Menge zusätzlicher Punkte, der so genannten *uneigentlichen Punkte*.

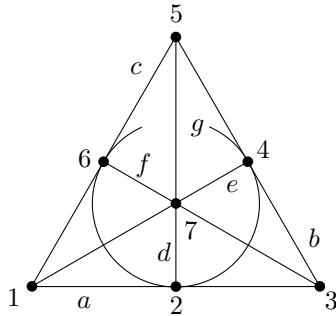
Grob gesagt entspricht jede Richtung von Geraden in der Ebene einem uneigentlichen Punkt, und alle Geraden parallel zu dieser Richtung schneiden sich sich per Definition in diesem Punkt. Alle uneigentlichen

Punkte liegen auf einer einzigen *uneigentlichen Geraden*. Auf diese Art erreicht man, dass sich nun je zwei verschiedene Geraden in genau einem Punkt schneiden (evtl. in einem uneigentlichen). Die Axiome (P1), (P2) und (P0) gelten daher alle in der reellen projektiven Ebene.

Die uneigentlichen Punkte haben nichts Mystisches an sich. Die projektive Ebene ist genau so eine mathematische Konstruktion wie die Entstehung der rationalen Zahlen aus den ganzen Zahlen oder die der reellen Zahlen aus den rationalen, also eine Erweiterung. Falls Sie sich für die Details der Konstruktion der reellen projektiven Ebene interessieren, finden Sie sie in Abschnitt 9.2.

Wir schulden dem Leser noch eine Erklärung des Adjektivs „projektiv“ in dem Ausdruck projektive Ebene. Dafür klären wir zuerst den Begriff der *projektiven Transformation*. Sind zwei Ebenen  $\rho$  und  $\sigma$  im dreidimensionalen Euklidischen Raum gegeben sowie ein Punkt  $c$ , der weder auf  $\rho$  noch auf  $\sigma$  liegt, dann kann man jeden Punkt  $x$  auf  $\rho$  vom Punkt  $c$  aus in die Ebene  $\sigma$  projizieren (indem man eine Gerade durch  $c$  und  $x$  legt und den Schnittpunkt dieser Geraden mit  $\sigma$  als Bildpunkt wählt). Dies definiert uns eine Abbildung, eine so genannte projektive Transformation, von  $\rho$  nach  $\sigma$ . Wirklich? Nun, nicht ganz: Ist  $x \in \rho$  ein Punkt, für den die Gerade durch  $c$  und  $x$  parallel zur Ebene  $\sigma$  ist, so ist in der gewohnten Euklidischen Geometrie das Bild von  $x$  nicht definiert. Wenn wir aber die beiden Ebenen  $\rho$  und  $\sigma$  um eine uneigentliche Gerade zu projektiven Ebenen ergänzen, dann ist diese projektive Transformation eine Bijektion zwischen den beiden projektiven Ebenen. Wenn wir  $\rho$  und  $\sigma$  als zwei Realisierungen der gleichen Ebene auffassen, können wir diese Abbildung als Bijektion der projektiven Ebene auf sich selbst interpretieren. Die projektive Ebene eignet sich also dazu, *projektive Geometrie* in ihr zu treiben; das ist ein Zweig der Geometrie, der sich mit solchen Eigenschaften geometrischer Objekte und Konfigurationen beschäftigt, die unter projektiven Transformationen erhalten bleiben. Zum Beispiel bilden Projektive Transformationen Kegelschnitte (Kreise, Ellipsen, Hyperbeln und Parabeln) auf Kegelschnitte ab, doch eine Ellipse kann in eine Hyperbel transformiert werden (alle anderen denkbaren Verwandlungen sind auch möglich), und eine elegante einheitliche Theorie der Kegelschnitte lässt sich in der projektiven Geometrie formulieren.

Die Analogie zwischen endlichen projektiven Ebenen und der reellen projektiven Ebene ist als Motivation für verschiedene Begriffe nützlich, oft auch für unsere Intuition (wir können geometrische Bilder zeichnen). Geometrische Überlegungen in der reellen projektiven Ebene, die nur die Axiome (P0), (P1) und (P2) benutzen, können auf endliche projektive Ebenen übertragen werden. Vergessen Sie aber nicht, dass trotz allem eine endliche projektive Ebene nur ein System endlicher Mengen mit den Eigenschaften (P0)–(P2) ist und nichts anderes. Andere geometrische Begriffe können daher nicht automatisch übertragen werden.

**Abb. 9.1** Die Fano-Ebene.

Es gibt zum Beispiel keinen vernünftigen Abstandsbegriff in endlichen projektiven Ebenen, es ist daher auch nicht klar, was ein „Kreis“ sein sollte. Ein anderer wichtiger Unterschied ist, dass in der „gewöhnlichen“ geometrischen Ebene die Punkte einer Geraden in natürlicher Weise „entlang“ der Geraden angeordnet sind, sich eine solche Ordnung aber für endliche projektive Ebenen nicht vernünftig definieren lässt.

Wie oben schon bemerkt sind endliche projektive Ebenen eher selten, und es ist gar nicht leicht allein mit der Definition überhaupt ein Beispiel zu finden (versuchen Sie es, wenn Sie es nicht glauben). Schon die kleinste von ihnen ist interessant.

**9.1.2 Beispiel.** Das kleinste Beispiel einer endlichen projektiven Ebene hat 7 Punkte und 7 Geraden, jede enthält 3 Punkte, und heißt die *Fano-Ebene*. Abbildung 9.1 zeigt die Fano-Ebene; die Punkte sind mit 1–7 nummeriert, und die 3 Punkte einer Geraden sind durch eine Strecke verbunden, in einem Fall durch einen Kreis.<sup>1</sup> Diese Geraden sind in der Abbildung mit *a*–*g* bezeichnet.

Obwohl die Fano-Ebene klein ist, ist sie ein nützliches mathematisches Objekt (vgl. Kapitel 9.4 für eine Anwendung), sie taucht auch als Lösung verschiedener Knobelaufgaben auf oder sogar in sehr ernsthaften Problemen wie dem folgenden. Sieben Polizisten werden aus verschiedenen Revieren in den 87-ten Bezirk versetzt. Eine gute Möglichkeit einander kennen zu lernen ist, die Hafenbar in der Bahnhofstraße zu observieren, sonst ein einfacher und irgendwie langweiliger Job, da Kneipenwirte meistens Computerkriminelle, Scheckkartenbetrüger oder ähnliches sind. Für eine Schicht braucht man drei Männer an sieben

---

<sup>1</sup>Man kann zeigen, dass in der euklidischen Ebene 7 Punkte nicht so gezeichnet werden können, dass jedes Tripel, das in der Fano-Ebene einer Geraden entspricht, auf einer euklidischen Geraden liegt — siehe Aufgabe 11.

Einsatzplan für Objekt: Hafenbar			
Mo	Cramer	Hoong	Japp
Di	Cramer	Holcomb	Lestrade
Mi	Holcomb	Hoong	Janvier
Do	Cramer	Janvier	Parker
Fr	Holcomb	Japp	Parker
Sa	Janvier	Japp	Lestrade
So	Hoong	Lestrade	Parker
Unterschrift Kommissar: 			

Abb. 9.2 Einsatzplan für 7 Personen in 7 Schichten zu je 3.

Tagen in der Woche. Wie kann ein Einsatzplan für eine Woche so eingerichtet werden, dass je zwei Polizisten eine gemeinsame Schicht haben? Die Fano-Ebene bietet eine gute Lösung (die Punkte entsprechen den Polizisten und die Schichten den Geraden, angeordnet in irgendeiner Reihenfolge), vgl. Abb. 9.2. Alle müssen gleich viele Schichten machen, niemand muss an mehr als zwei aufeinanderfolgenden Tagen arbeiten, vor allem aber arbeitet in jeder Schicht ein Polizist, der auch schon am Vortag dabei war und weiß, was los war usw.<sup>2</sup> Wir wissen von keinem solchen Schichtplan, der zur Zeit bei der Polizei benutzt wird, aber einige Motorradrennen zum Beispiel werden auf der Basis einer affinen Ebene der Ordnung 4 organisiert (affine Ebenen sind ein mit projektiven Ebenen verwandtes Konzept; vgl. Aufgabe 10 für eine Definition).

Wir beweisen nun einige Hilfssätze, die zeigen, dass wir bei der Konstruktion einer projektiven Ebene viel eingeschränkter sind, als es auf den ersten Blick scheinen mag.

**9.1.3 Hilfssatz.** Sei  $(X, \mathcal{L})$  eine endliche projektive Ebene. Dann enthalten alle Geraden gleich viele Punkte, das heißt:  $|L| = |L'|$  für je zwei Geraden  $L, L' \in \mathcal{L}$ .

*Beweis.* Seien  $L, L' \in \mathcal{L}$  zwei beliebige Geraden. Wir beweisen zunächst folgende Hilfsaussage: Es gibt einen Punkt  $z \in X$ , der

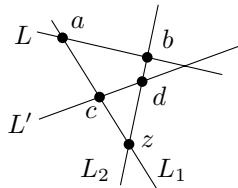
---

<sup>2</sup>Quizfrage für Liebhaber klassischer Krimis: Wissen sie noch, woher die sieben Polizisten in Abb. 9.2 kommen, und kennen Sie die Namen ihrer bekannteren Gegenspieler oder Partner, den Meisterdetektiven?

weder auf  $L$  noch auf  $L'$  liegt.

*Beweis der Hilfsaussage:* Sei  $F \subseteq X$  eine Menge wie in Axiom (P0). Dann ist  $|L \cap F| \leq 2$  und  $|L' \cap F| \leq 2$ . Falls  $F$  nicht in  $L \cup L'$  enthalten ist, sind wir fertig. Es bleibt die Möglichkeit, dass  $L$  mit  $F$  zwei gemeinsame Punkte hat (nennen wir sie  $a, b$ ) und  $L'$  mit  $F$  die verbleibenden beiden Punkte gemeinsam hat (genannt  $c, d$ ). Wir betrachten die Geraden  $L_1 = \overline{ac}$  und  $L_2 = \overline{bd}$ . Sei  $z$  der Schnittpunkt von  $L_1$  und  $L_2$ .

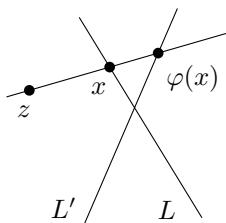
Das folgende Bild illustriert die Situation:



Natürlich müssen wir sehr darauf achten nur die Bedingungen (P0)–(P2) zu benutzen und nicht irgendeine Information aus unserer geometrischen Anschauung. Endliche projektive Ebenen sehen in vielerlei Hinsicht anders aus als die euklidische Ebene.

Wir behaupten, dass  $z \notin L \cup L'$ . Die Geraden  $L$  und  $L_1$  schneiden sich in genau einem Punkt, nämlich  $a$ . Wäre also  $z \in L$ , dann müsste  $z = a$  sein. Das ist aber unmöglich, weil dann die Gerade  $L_2$  die Punkte  $z = a, b$  und  $d$  enthalten würde, also 3 Punkte aus  $F$ . Das widerspricht aber Bedingung (P0). Daher ist  $z \notin L$ , und genauso kann man zeigen, dass  $z \notin L'$ . Damit haben wir die Hilfsaussage bewiesen.

Wir zeigen jetzt, dass die Geraden  $L$  und  $L'$  gleich viele Punkte enthalten. Dazu definieren wir eine Abbildung  $\varphi: L \rightarrow L'$ ; es wird sich zeigen, dass sie eine Bijektion ist. Wir wählen einen festen Punkt  $z \notin L \cup L'$  und definieren das Bild  $\varphi(x)$  von einem Punkt  $x \in L$  als Schnittpunkt der Geraden  $\overline{zx}$  und  $L'$ , wie in dem folgenden Bild:



Nach den Axiomen (P1) und (P2) ist der Punkt  $\varphi(x)$  wohldefiniert. Wir überprüfen nun, ob  $\varphi$  eine Bijektion ist. Für einen beliebigen Punkt  $y \in L'$  betrachten wir die Gerade  $\overline{zy}$ . Sei  $x$  ihr Schnittpunkt mit der Geraden  $L$ . Dann sind die Geraden  $\overline{zy}$  und  $\overline{zx}$  gleich, und daher ist  $y = \varphi(x)$ . Die Abbildung  $\varphi$  ist wie behauptet eine Bijektion und daher  $|L| = |L'|$ .  $\square$

**9.1.4 Definition (Ordnung einer projektiven Ebene).** Die Ordnung einer endlichen projektiven Ebene  $(X, \mathcal{L})$  ist die Zahl  $|L|-1$ , wobei  $L \in \mathcal{L}$  eine Gerade ist (nach dem gerade bewiesenen Hilfssatz hängt die die Ordnung nicht von der Wahl der Geraden  $L$  ab).

Die Fano–Ebene zum Beispiel hat die Ordnung 2 (auf jeder Geraden liegen drei Punkte), und man kann zeigen, dass sie die einzige projektive Ebene der Ordnung 2 ist (bis auf Umbenennung der Punkte, das heißt bis auf Isomorphismen). Es mag seltsam erscheinen, dass wir in der Definition der Ordnung von der Mächtigkeit einer Geraden 1 subtrahieren, aber in anderen Zusammenhängen ist diese Definition sehr natürlich, zum Beispiel in Verbindung mit affinen Ebenen (Aufgabe 10) oder bei lateinischen Quadraten (Abschnitt 9.3).

Wir beweisen weitere Eigenschaften endlicher projektiver Ebenen.

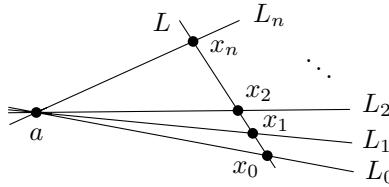
**9.1.5 Hilfssatz.** Sei  $(X, \mathcal{L})$  eine projektive Ebene der Ordnung  $n$ . Dann gilt:

- (i) Durch jeden Punkt von  $X$  gehen genau  $n+1$  Geraden.
- (ii)  $|X| = n^2 + n + 1$ .
- (iii)  $|\mathcal{L}| = n^2 + n + 1$ .

*Beweis von (i).* Wir betrachten einen beliebigen Punkt  $x \in X$ . Zunächst bemerken wir, dass es eine Gerade  $L$  gibt, die  $x$  nicht enthält. Ist  $F$  nämlich die 4-Punkt-Konfiguration wie in (P0) und sind  $a, b, c \in F$  von  $x$  verschiedene Punkte, dann enthält mindestens eine der Geraden  $\overline{ab}$  oder  $\overline{ac}$  den Punkt  $x$  nicht, wie leicht zu überprüfen ist.

Sei also  $L$  eine solche Gerade mit  $x \notin L$ . Zu jedem Punkt  $y \in L$  betrachten wir die Gerade  $\overline{xy}$ ; das sind  $n+1$  Geraden durch  $x$ . Andererseits schneidet jede Gerade durch  $x$  die Gerade  $L$  in einem Punkt  $y \in L$  und wird daher unter den genannten  $n+1$  Geraden mitgezählt. Daher gehen genau  $n+1$  Geraden durch  $x$ .

*Beweis von (ii).* Wir wählen  $L = \{x_0, x_1, x_2, \dots, x_n\} \in \mathcal{L}$  und einen Punkt  $a \notin L$ , wie in dem folgenden Bild:

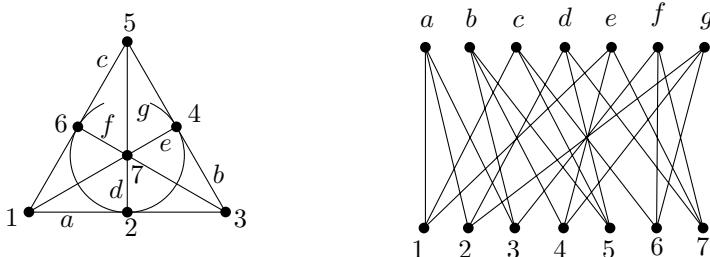


Sei  $L_i$  die Gerade  $\overline{ax_i}$ ,  $i = 0, 1, \dots, n$ . Nach (P1) schneiden sich je zwei dieser Geraden  $L_i$  und  $L_j$  in genau einem Punkt, und zwar ist dieser Punkt  $a$ . Die Geraden  $L_0, L_1, \dots, L_n$  haben außer  $a$  noch  $n$  weitere Punkte und daher zusammen  $(n+1)n+1 = n^2+n+1$  verschiedene Punkte. Es bleibt zu zeigen, dass jeder Punkt  $x \in X \setminus \{a\}$  schon auf einer der Geraden  $L_i$  liegt. Nach (P1) schneidet die Gerade  $\overline{ax}$  die Gerade  $L$  in einem Punkt  $x_i$ , und nach (P2) muss die Gerade  $\overline{ax}$  mit  $L_i$  identisch sein. Damit ist (ii) bewiesen.

Wir verschieben den Beweis zu Teil (iii). Im Folgenden werden wir ein wichtiges Prinzip kennen lernen, aus dem (iii) dann direkt mit dem schon Bewiesenen folgt.  $\square$

**Dualität.** Dualität heißt für projektive Ebenen „die Rollen von Punkten und Geraden vertauschen“. Um das exakter zu formulieren führen wir zunächst den so genannten *Inzidenzgraphen* einer endlichen projektiven Ebene ein. Allgemein kann man den Inzidenzgraphen für ein beliebiges System  $\mathcal{S}$  von Teilmengen einer Menge  $X$  definieren. Der Inzidenzgraph ist ein bipartiter Graph mit der Eckenmenge  $X \cup \mathcal{S}$ , wobei jede Menge  $S \in \mathcal{S}$  mit allen Punkten  $x \in S$  durch eine Kante verbunden wird. Jeder Punkt  $x \in X$  wird daher mit allen Mengen verbunden, in denen er enthalten ist. Kurz gesagt entsprechen die Kanten des Inzidenzgraphen der Relation „ $\in$ “. Abb. 9.3 zeigt den Inzidenzgraphen der Fano-Ebene; die Ecken sind mit den Nummern und Buchstaben der zugehörigen Punkte und Geraden gekennzeichnet. (Nebenbei bemerkt ist der entstandene Graph wichtig und schön, auch wenn die Zeichnung in unserer Abbildung gar nicht hübsch ist, und er hat sogar einen Namen: der *Heawood-Graph*.)

Zu einer gegebenen endlichen projektiven Ebene  $(X, \mathcal{L})$  erhält man das *Duale* von  $(X, \mathcal{L})$ , indem man im Inzidenzgraphen von  $(X, \mathcal{L})$  diejenigen Ecken, die den Punkten zugeordnet waren, nun



**Abb. 9.3** Die Fano–Ebene und ihr Inzidenzgraph.

als Geraden interpretiert und umgekehrt diejenigen Ecken, die ursprünglich zu Geraden gehörten, als Punkte. In Abb. 9.3 können wir einfach oben und unten vertauschen. Aus  $\mathcal{L}$  wird auf die Weise eine Menge von Punkten, und für jeden Punkt  $x \in X$  interpretieren wir die Menge von Geraden  $\{L \in \mathcal{L}: x \in L\}$  als eine Gerade. Im Dualen der Fano–Ebene zum Beispiel sind  $\{a, b, \dots, g\}$  die Punkte, und die Geraden sind  $\{a, c, e\}$  (für den Punkt 1 in der Fano–Ebene),  $\{a, d, g\}$  (für den Punkt 2), und so weiter.

**Hilfssatz.** Das Duale einer endlichen projektiven Ebene ist wieder eine endliche projektive Ebene.

*Beweis.* Sei  $(X, \mathcal{L})$  eine endliche projektive Ebene. Das Duale von  $(X, \mathcal{L})$  ist ein Paar  $(\mathcal{L}, \Lambda)$ , wobei  $\Lambda$  ein System von Teilmengen von  $\mathcal{L}$  ist und jede dieser Teilmengen einem bestimmten Punkt aus  $X$  entspricht. (Beachten Sie, dass verschiedene Punkte immer verschiedenen Mengen in  $\mathcal{L}$  entsprechen, da durch zwei Punkte nur eine Gerade geht.)

Wir müssen die Bedingungen (P0)–(P2) für  $(\mathcal{L}, \Lambda)$  überprüfen. Beginnen wir mit Bedingung (P0). Übersetzt in die Sprache des ursprünglichen Mengensystems  $(X, \mathcal{L})$  bedeutet diese Bedingung, dass wir vier Geraden  $L_1, L_2, L_3, L_4 \in \mathcal{L}$  finden müssen, von denen je drei keinen gemeinsamen Punkt haben. Dazu betrachten wir eine 4-Punkt-Konfiguration  $F = \{a, b, c, d\} \subseteq X$  wie in Bedingung (P0), und wir definieren  $L_1 = \overline{ab}$ ,  $L_2 = \overline{cd}$ ,  $L_3 = \overline{ad}$ ,  $L_4 = \overline{bc}$ . Betrachten wir drei dieser vier Geraden, so enthalten je zwei von ihnen einen Punkt aus  $F$ , und dieser Punkt ist nicht in der dritten Geraden enthalten. Daher haben je drei dieser Geraden  $L_1, \dots, L_4$  einen leeren Schnitt, somit haben wir Bedingung (P0) für das duale Mengensystem bewiesen.

Bedingung (P1) formuliert für das Duale  $(\mathcal{L}, \Lambda)$  verlangt folgendes: Sind  $x, x' \in X$  zwei verschiedene Punkte, dann gibt es genau eine Gerade  $L \in \mathcal{L}$ , die  $x$  und  $x'$  enthält. Das ist aber genau Bedingung (P2) für  $(X, \mathcal{L})$ ! Genauso sieht man, dass (P2) für das Duale der Bedingung (P1) für die ursprüngliche projektive Ebene  $(X, \mathcal{L})$  entspricht.  $\square$

Ab jetzt können wir das Duale einer endlichen projektiven Ebene als die *duale projektive Ebene* bezeichnen. Hilfssatz 9.1.5(i) bedeutet, dass die duale projektive Ebene die gleiche Ordnung wie die ursprüngliche projektive Ebene hat. Man sieht auch, dass die Teile (ii) und (iii) von Hilfssatz 9.1.5 dual zueinander sind, so dass, wenn wir einen von ihnen beweisen, der andere automatisch gelten muss.

Allgemein können wir in einer Aussage über endliche projektive Ebenen der Ordnung  $n$  die Wörter „Punkt“ und „Gerade“ austauschen und erhalten so wieder eine gültige Aussage. Um einen sinnvollen Satz zu erhalten müssen wir natürlich eventuell andere Satzteile auch umformulieren. Übersetzen wir zum Beispiel den Satz „die Geraden  $L_1, L_2$  schneiden sich im Punkt  $x$ “ für das Duale, erhalten wir „die Punkte  $x_1, x_2$  liegen auf der Geraden  $L$ “ usw. Wir haben also ein „Rezept zum Herstellen neuer Sätze“, das uns die Hälfte der Sätze in der projektiven Geometrie gratis liefert! Manchmal wird es das *Dualitätsprinzip* genannt, das den Geometern, die die reelle projektive Ebene studieren, schon lange bekannt ist.

## Aufgaben

1. Zeigen Sie, dass die Fano-Ebene die einzige projektive Ebene der Ordnung 2 ist (d.h. jede projektive Ebene der Ordnung 2 zu ihr isomorph ist — definieren Sie zuerst, was ein Isomorphismus eines Mengensystems ist).
2. \*Konstruieren Sie eine projektive Ebene der Ordnung 3 (bevor Sie den nächsten Abschnitt lesen!).
3. (a) Finden Sie ein Beispiel eines Mengensystems  $(X, \mathcal{L})$  auf einer nicht-leeren endlichen Menge  $X$ , das die Bedingungen (P1) und (P2) erfüllt aber nicht (P0).  
 (b) Finden Sie  $X$  und  $\mathcal{L}$  wie in (a), so dass  $|X| \geq 10$ ,  $|\mathcal{L}| \geq 10$  und so dass jedes  $L \in \mathcal{L}$  mindestens zwei Punkte hat.  
 (c) \*Beschreiben Sie alle Mengensysteme  $(X, \mathcal{L})$  wie in (a).

4. Sei  $X$  eine endliche Menge und  $\mathcal{L}$  ein System von Teilmengen von  $X$ , das den Bedingungen (P1), (P2) und der folgenden Bedingung (P0') genügt:

Es gibt mindestens zwei verschiedene Geraden  $L_1, L_2 \in \mathcal{L}$ , die jede mindestens 3 Punkte haben.

Zeigen Sie, dass  $(X, \mathcal{L})$  eine endliche projektive Ebene ist.

5. Beweisen Sie Teil (iii) von Hilfssatz 9.1.5 direkt ohne die Dualität zu benutzen.
6. Zeigen Sie, dass es in einer Mengenfamilie, die aus 3-elementigen Teilmengen einer 9-elementigen Menge besteht, höchstens 12 Mengen gibt.  
\*Finden Sie ein Beispiel mit 12 Mengen.
7. \* Ist es möglich, 8 Buslinien in einer Stadt so zu legen, dass
  - (i) bei Ausfall jeder beliebigen Linie immer noch jede Haltestelle von jeder anderen Haltestelle mit höchstens einmaligem Umsteigen erreichbar ist;
  - (ii) bei Ausfall zweier beliebiger Linien das Liniennetz unzusammenhängend wird?
8. \*Sei  $X$  eine Menge mit  $n^2 + n + 1$  Elementen,  $n \geq 2$ , und sei  $\mathcal{L}$  eine Familie bestehend aus  $n^2 + n + 1$  Teilmengen von  $X$  der Mächtigkeit  $n + 1$ . Nehmen Sie an, dass je zwei verschiedene Mengen aus  $\mathcal{L}$  sich in höchstens einem Punkt schneiden. Ziel ist zu zeigen, dass  $(X, \mathcal{L})$  eine endliche projektive Ebene der Ordnung  $n$  ist. Die folgenden Hilfsaus sagen sind ein möglicher Weg, den Beweis zu führen.
  - (a) Zeigen Sie mit doppeltem Abzählen, dass jedes Punktpaar aus  $X$  in genau einer Menge aus  $\mathcal{L}$  enthalten ist.
  - (b) Zeigen Sie, dass jeder Punkt in höchstens  $n + 1$  Mengen liegt.
  - (c) Zeigen Sie, dass jeder Punkt in genau  $n + 1$  Mengen liegt.
  - (d) Zeigen Sie, dass sich je zwei Mengen aus  $\mathcal{L}$  schneiden.
  - (e) Überprüfen Sie, dass  $(X, \mathcal{L})$  eine projektive Ebene der Ordnung  $n$  ist.
9. \*Sei  $(X, \mathcal{L})$  eine projektive Ebene der Ordnung  $n$ , und sei  $A \subseteq X$  eine Menge, in der keine drei Punkte auf einer gemeinsamen Geraden liegen. Zeigen Sie, dass  $|A| \leq n + 2$  (für ungerades  $n$  kann man sogar zeigen, dass  $|A| \leq n + 1$ ).
10. (Affine Ebenen) Wir definieren eine *affine Ebene* als ein Paar  $(X, \mathcal{A})$ , wobei  $X$  eine Menge ist und  $\mathcal{A}$  eine Familie von Teilmengen von  $X$  (genannt *Geraden*), die den folgenden Axiomen genügen: Es gibt drei Punkte, die nicht auf einer gemeinsamen Geraden liegen, je zwei Punkte liegen auf genau einer Geraden, und zu jedem Punkt  $p$  und jeder

Geraden  $A \in \mathcal{A}$  mit  $p \notin A$  gibt es genau eine Gerade  $A'$  mit  $A' \cap A = \emptyset$  und  $p \in A'$ .

- (a) Überprüfen Sie, dass diese Axiome in der gewöhnlichen euklidischen Ebene gelten. Finden Sie heraus, wie man aus einer endlichen projektiven Ebene eine endliche affine Ebene konstruieren kann.
  - (b) Wir definieren eine Relation  $\parallel$  auf  $\mathcal{A}$  durch  $A_1 \parallel A_2$  genau dann, wenn  $A_1 \cap A_2 = \emptyset$  oder wenn  $A_1 = A_2$ . Zeigen Sie, dass  $\parallel$  eine Äquivalenzrelation ist.
  - (c) \*Zeigen Sie in Analogie zu den projektiven Ebenen, dass alle Geraden einer affinen Ebene die gleiche Mächtigkeit  $n$  haben und dass eine solche affine Ebene  $n^2 + n$  Geraden und  $n^2$  Punkte hat, wobei durch jeden Punkt  $n + 1$  Geraden gehen.
  - (d) \*Zeigen Sie, dass man aus jeder affinen Ebene der Ordnung  $n$  eine projektive Ebene der Ordnung  $n$  konstruieren kann.
11. Zeigen Sie, dass die Fano-Ebene nicht in die euklidische Ebene eingebettet werden kann. Das heißt, es gibt keine sieben Punkte und sieben Geraden in der euklidischen Ebene, so dass je zwei Punkte auf einer Geraden liegen und je zwei Geraden sich in einem Punkt schneiden. Benutzen Sie Aufgabe 6.3.8.

## 9.2 Existenz endlicher projektiver Ebenen

Projektive Ebenen der Ordnung 2, 3, 4 und 5 existieren. Aber es gibt keine projektive Ebene der Ordnung 6! (Der Beweis ist nicht leicht, Sie finden ihn z.B. in Van Lint und Wilson [8].) Projektive Ebenen der Ordnung 7, 8, 9 existieren wieder, aber keine der Ordnung 10. Gibt es hier eine Gesetzmäßigkeit? Nun, eine projektive Ebene der Ordnung  $n$  existiert immer, wenn es einen Körper mit  $n$  Elementen gibt. Körper ist hier im algebraischen Sinne gemeint, das heißt als eine Menge mit Operationen wie Addition, Subtraktion, Multiplikation und Division, die gewissen Axiomen genügen — im Anhang finden Sie eine Definition. In der Algebra lernt man, dass es genau dann einen Körper mit  $n$  Elementen gibt, wenn  $n$  eine Primzahlpotenz ist. Insbesondere heißt das, dass projektive Ebenen beliebig großer Ordnung existieren.

Ist  $n$  durch mindestens zwei verschiedene Primzahlen teilbar, dann gibt es keinen  $n$ -elementigen Körper; es ist jedoch nicht bekannt, ob es nicht in einigen Fällen dennoch eine projektive Ebene der Ordnung  $n$  gibt. Man kennt einige negative Resultate; lässt zum Beispiel  $n$  bei Division durch 4 den Rest 1 oder 2 und kann  $n$  nicht als Summe zweier ganzzahliger Quadrate dargestellt werden, dann

gibt es keine projektive Ebene der Ordnung  $n$  (der Beweis ist nicht leicht). Dies klärt die Existenz von projektiven Ebenen der Ordnung 6, 14 und vieler anderer Ordnungen, aber längst nicht von allen möglichen Ordnungen. Es sagt zum Beispiel nichts über die Ordnungen  $n = 10$  oder  $12$ .

Die Existenz einer projektiven Ebene der Ordnung 10 wurde ebenfalls ausgeschlossen. Diese Ergebnisse haben eine interessante Geschichte. Für die Ordnung 6 versuchte schon Euler einen Beweis, aber erst Tarry fand um 1900 ein schlüssiges Argument. Für die Ordnung 10 wurde kürzlich ein Beweis gefunden, der einen enormen Rechenaufwand am Computer benötigt. Für die nächsthöhere Ordnung 12 bleibt die Existenz einer projektiven Ebene ein offenes Problem. Natürlich ist dieses Problem im Prinzip durch Überprüfen einer endlichen Zahl von Konfigurationen lösbar, aber die Anzahl der Konfigurationen scheint für die augenblickliche Computertechnik einfach zu gigantisch zu sein.

**Algebraische Konstruktion einer projektiven Ebene.** Für interessierte Leser mit Algebrakenntnissen, erklären wir, wie man eine projektive Ebene aus einem Körper konstruiert. Wir interessieren uns besonders für endliche projektive Ebenen, aber die Konstruktion ist genau die gleiche wie für die reelle projektive Ebene (und allgemein für jeden Körper).

Die formale Konstruktion sieht erst einmal etwas kompliziert aus, denn als Punkte werden wir Äquivalenzklassen auf einer Menge geordneter Tripel ansehen. Doch davon sollte man sich nicht irritieren lassen, die Überprüfung der Axiome ist ganz leicht. Falls es sich bei dem Körper um die reellen Zahlen  $\mathbb{R}$  handelt, hat die Konstruktion eine intuitive geometrische Interpretation, die wir am Schluss zeigen wollen. Manchen Menschen hilft die geometrische Anschauung beim Verständnis der formalen Konstruktion, andere sind vielleicht erst recht verwirrt. Welchen Stellenwert die Anschauung haben soll, kann daher jeder Leser nur für sich entscheiden.

Die Konstruktion beginnt mit einem Körper  $K$ . Für die reelle projektive Ebene (das heißt für die Erweiterung der gewöhnlichen euklidischen Ebene durch uneigentliche Punkte) nehmen wir den Körper  $K$  aller reellen Zahlen  $\mathbb{R}$ . Wählen wir einen  $n$ -elementigen Körper  $K$ , erhalten wir eine endliche projektive Ebene der Ordnung  $n$ . Als Beispiel betrachten wir den 3-elementigen Körper  $K$ , das heißt die Menge  $\{0, 1, 2\}$  mit den arithmetischen Operationen modulo 3.

Wir betrachten zunächst die Menge  $T = K^3 \setminus \{(0, 0, 0)\}$ ; das ist die Menge aller geordneten Tripel  $(x, y, t)$ , wobei  $x, y, t \in K$  und  $x, y, t$  nicht gleichzeitig 0 sind. Auf dieser Menge  $T$  definieren wir eine Äquiva-

lenzrelation  $\approx$  wie folgt: Genau dann sei  $(x_1, y_1, t_1) \approx (x_2, y_2, t_2)$ , wenn ein von Null verschiedenes  $\lambda \in K$  existiert, so dass  $x_2 = \lambda x_1$ ,  $y_2 = \lambda y_1$  und  $t_2 = \lambda t_1$  (es ist nicht schwer zu zeigen, dass dies tatsächlich eine Äquivalenzrelation ist). Punkte in unserer projektiven Ebene sollen die Äquivalenzklassen dieser Relation werden. Die so konstruierte projektive Ebene<sup>3</sup> wird gewöhnlich in der Literatur mit  $PK^2$  bezeichnet, wobei man auch den speziell gewählten Körper statt  $K$  schreiben kann. Die reelle projektive Ebene wird zum Beispiel mit  $P\mathbb{R}^2$  bezeichnet.

Um eine bessere Vorstellung von dieser projektiven Ebene zu bekommen, wählen wir aus jeder Äquivalenzklasse von  $\approx$  ein repräsentatives Tripel aus. Als Repräsentanten wählen wir die Tripel, *deren letzter von Null verschiedener Eintrag 1 ist*. Die Repräsentanten sind dann Tripel vom Typ  $(x, y, 1)$ ,  $(x, 1, 0)$  (für  $x, y \in K$ ) und das Tripel  $(1, 0, 0)$ . Man überzeugt sich leicht, dass jedes andere Tripel zu einem solchen repräsentativen Tripel äquivalent ist und dass keine zwei Repräsentanten äquivalent sind bezüglich  $\approx$ .

Es wäre lästig, die ganze Zeit weiter über Äquivalenzklassen zu sprechen. Im folgenden werden wir daher sagen „ein Punkt  $(x, y, t)$ “ und meinen damit die ganze Äquivalenzklasse, die  $(x, y, t)$  enthält.

Ist  $K$  ein  $n$ -elementiger Körper, können wir nun zählen, wie viele Punkte wir erhalten. Die Anzahl der Punkte der Form  $(x, y, 1)$  ist  $n^2$ , es gibt  $n$  Punkte der Form  $(x, 1, 0)$ , und zusätzlich haben wir den Punkt  $(1, 0, 0)$  — zusammen  $n^2 + n + 1$ , so wie es sein soll. Für  $n = 3$  sind im folgenden Diagramm alle Punkte mit ihren Tripeln gezeichnet; es liegt nahe, die Punkte, deren letzte Koordinate 1 ist, als  $3 \times 3$  Gitter anzurufen.

	•	•	•	•
010	110	210	100	
2	•	•	•	
1	•	•	•	
0	•	•	•	
0	1	2		

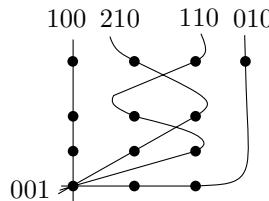
Nun ist es an der Zeit die Geraden zu definieren. Zu jedem Tripel  $(a, b, c) \in K^3 \setminus \{(0, 0, 0)\}$  definieren wir eine Gerade  $L(a, b, c)$  als die Menge aller Punkte  $(x, y, t)$  unserer projektiven Ebene, die die folgende Gleichung erfüllen:

$$ax + by + ct = 0 \quad (9.1)$$

---

<sup>3</sup>Für endliche Körper haben wir noch nicht gezeigt, dass wir endliche projektive Ebenen im Sinne von Definition 9.1.1 erhalten, wir haben noch nicht einmal die Geraden definiert. Genau genommen sollten wir deshalb dieses Objekt, das wir gerade definieren, noch nicht als projektive Ebene bezeichnen. Aber da wir (hoffentlich) unter Freunden sind, gibt es keinen Grund gar so streng zu sein, oder?

Offensichtlich erfüllen zwei äquivalente Tripel  $(x, y, t)$  und  $(\lambda x, \lambda y, \lambda t)$  entweder beide diese Gleichung oder keines von beiden, und wir haben daher tatsächlich eine Punktmenge in der projektiven Ebene definiert. Ebenso sieht man, dass für alle von Null verschiedenen  $\lambda \in K$  die Tripel  $(\lambda a, \lambda b, \lambda c)$  die gleiche Gerade definieren wie das Tripel  $(a, b, c)$ . Wir haben daher auf den Tripeln, die Geraden definieren, die gleiche Äquivalenzrelation wie auf den Tripeln, die Punkte definieren. Wir können dieselben repräsentativen Tripel wie für die Punkte auswählen, das heißt die Tripel, deren letzter von Null verschiedener Eintrag 1 ist. Im folgenden Bild haben wir alle Geraden durch  $(0, 0, 1)$  gezeichnet und mit ihrem repräsentierenden Tripel gekennzeichnet. Wir haben die Tripel zu den meisten Punkten weggelassen (sie sind die gleichen wie im vorangegangenen Diagramm):



Um zu zeigen, dass wir für einen  $n$ -elementigen Körper wirklich eine endliche projektive Ebene der Ordnung  $n$  konstruiert haben, müssen wir die Bedingungen (P0)–(P2) überprüfen. Wir beginnen mit Bedingung (P1) (je zwei Geraden schneiden sich in genau einem Punkt). Seien also  $(a_1, b_1, c_1)$  und  $(a_2, b_2, c_2)$  zwei Tripel, die nicht äquivalent zueinander sind, das heißt keines ist ein Vielfaches des anderen.

Wir könnten jetzt direkt den Schnittpunkt der beiden Geraden berechnen (er ist die Lösung eines kleinen linearen Gleichungssystems) und seine Eindeutigkeit überprüfen. Wir geben einen anderen Beweis, der auf elementaren Ergebnissen der linearen Algebra beruht. Versuchen Sie doch einmal, den Beweis über eine direkte Berechnung zu führen — vielleicht lernen Sie dadurch die lineare Algebra neu schätzen.

Wir betrachten die Tripel  $(a_1, b_1, c_1)$  und  $(a_2, b_2, c_2)$  als dreidimensionale Vektoren über dem Körper  $K$ . Beide sind von Null verschiedene Vektoren, und da keiner ein Vielfaches des anderen ist, sind sie linear unabhängig. Daher hat die Matrix

$$\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{pmatrix}$$

Rang 2 (lineare Unabhängigkeit und der Rang beziehen sich auf den Körper  $K$ ). Wir fassen nun die Spalten dieser Matrix als zweidimensionale Vektoren auf. Wir wissen, dass drei Vektoren in einem zweidimensionalen Raum linear abhängig sind, das heißt, es gibt drei Zahlen  $x, y, t \in K$ , nicht alle gleich Null, so dass

$$x(a_1, a_2) + y(b_1, b_2) + t(c_1, c_2) = (0, 0). \quad (9.2)$$

Betrachten wir diese Gleichung getrennt für jede Koordinate, erhalten wir, dass der Punkt  $(x, y, t)$  auf beiden betrachteten Geraden liegt.

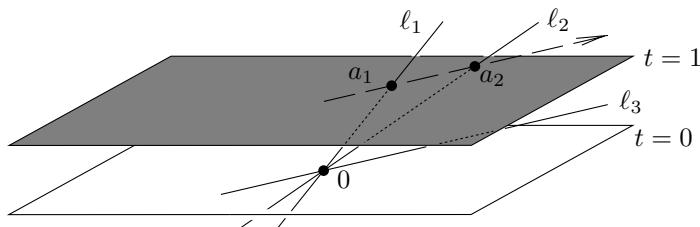
Da der Rang der betrachteten Matrix 2 ist, muss sie zwei linear unabhängige Spalten haben. Als Beispiel nehmen wir an, es sind  $(a_1, a_2)$  und  $(b_1, b_2)$ . Das bedeutet, dass die Gleichung  $x(a_1, a_2) + y(b_1, b_2) = (u, v)$  für jeden Vektor  $(u, v)$  eine eindeutige Lösung hat. Anders gesagt, wenn wir den Wert von  $t$  in Gleichung (9.2) vorgeben, sind die Werte von  $x$  und  $y$  schon eindeutig bestimmt, und alle Lösungen dieser Gleichung sind daher Vielfache dieses einen Vektors. Die beiden betrachteten Geraden schneiden sich also in genau einem Punkt.

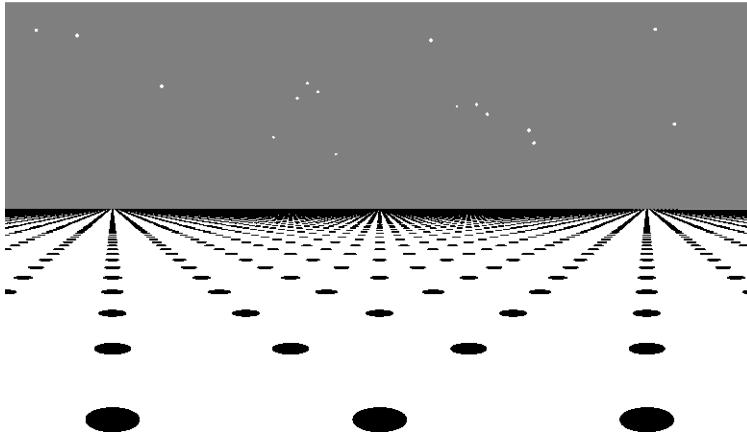
Dieses Argument können wir noch präziser ausdrücken. Die lineare Abbildung, die einen Vektor  $(x, y, t) \in K^3$  auf den Vektor  $x(a_1, a_2) + y(b_1, b_2) + t(c_1, c_2) \in K^2$  abbildet, hat Rang 2, sie ist daher surjektiv und ihr Kern ist eindimensional.

Wir haben (P1) bewiesen. Bedingung (P2) könnte man genauso beweisen, oder wir sagen direkt, dass die Rollen der Tripel  $(a, b, c)$  und  $(x, y, z)$  in Gleichung (9.1) symmetrisch sind, und wir haben daher (wieder) eine Dualität zwischen Geraden und Punkten. Die Überprüfung der Bedingung (P0) schließlich überlassen wir dem Leser.  $\square$

*Geometrische Interpretation.* Zu Beginn des Kapitels haben wir bereits die Grundidee bei der Konstruktion der reellen projektiven Ebene erwähnt, die Euklidische Ebene durch uneigentliche Punkte so zu erweitern, dass es für jede Parallelklasse von Geraden genau einen uneigentlichen Punkt gibt, in dem sich alle Geraden aus dieser Parallelklasse schneiden. Uneigentliche Punkte (im Englischen heißen sie „points at infinity“) kann man sich in einer perspektivischen Zeichnung der Euklidischen Ebene also als „Punkte am Horizont“ vorstellen; siehe dazu Abbildung 9.4, in der die Kreise Punkte mit ganzzahligen Koordinaten repräsentieren.

Um dieses Bild formal zu beschreiben, betrachten wir den dreidimensionalen Raum mit kartesischem Koordinatensystem  $(x, y, t)$ , wobei die  $t$ -Achse die vertikale ist. Unsere Euklidische Ebene legen wir in diesem dreidimensionalen Raum auf  $t = 1$ , grau markiert in der folgenden Zeichnung:





**Abb. 9.4** Die reelle projektive Ebene im Mondschein.

Zu jedem Punkt  $a$  in dieser Ebene gehört eine Gerade  $\ell = \overline{0a}$ , die durch  $a$  und den Ursprung des dreidimensionalen Raums verläuft. In der Zeichnung gehört z.B. zum Punkt  $a_1$  die Gerade  $\ell_1$ . Umgekehrt gehört jede Ursprungsgerade zu genau einem Punkt der grauen Ebene — außer den horizontalen Geraden wie  $\ell_3$ .

Wenn wir nun die Gerade  $\ell_1$  langsam kippen, auf die Position von  $\ell_2$  und weiter in Richtung der horizontalen Position  $\ell_3$ , dann wandert der Punkt in der grauen Ebene auf der gestrichelten Linie langsam in Richtung Unendlichkeit. Es ist also gar nicht so abwegig, sich vorzustellen, dass die horizontalen Geraden wie  $\ell_3$  zu Punkten gehören, die im Unendlichen liegen — uneigentlichen Punkten, wie wir sie zur Euklidischen Ebene hinzufügen möchten. Und nun verwenden wir einen typischen Trick der modernen Mathematik: Statt zu erklären, was uneigentliche Punkte sind und dass sie etwas mit horizontalen Geraden zu tun haben, vergessen wir die Euklidische Ebene und sagen einfach, die Punkte der projektiven Ebene *sind* Ursprungsgeraden im dreidimensionalen Raum. In der oben beschriebenen formalen Konstruktion von  $PK^2$  haben wir es nicht direkt gesagt, aber auch dort war ein Punkt der projektiven Ebene eine Menge der Form  $\{(\lambda x, \lambda y, \lambda t) : \lambda \in K \setminus \{0\}\}$ . Geometrisch entspricht das genau den Ursprungsgeraden in  $K^3$ , nur dass wir den Ursprung weggelassen haben, weil es technisch bequemer ist.

Die Geraden der projektiven Ebene entsprechen im dreidimensionalen Raum den Ebenen, die den Ursprung enthalten; es ist instruktiver, wenn der Leser selbst darüber nachdenkt.

Geraden zu Punkten zu erklären ist zunächst sonderbar. Doch Leser, die schon eine Analysisvorlesung gehört haben, sind wahrscheinlich

1	2	3
2	3	1
3	1	2

1	2	3
3	1	2
2	3	1

**Abb. 9.5** Zwei orthogonale lateinische Quadrate der Ordnung 3.

schon abgebrüht. Sie mussten sich schon sagen lassen, dass eine reelle Zahl in Wirklichkeit eine Menge rationaler Zahlen ist, oder dass eine rationale Zahl in Wirklichkeit eine Äquivalenzklasse auf der Menge aller Paare ganzer Zahlen ist, oder ... Die Vorteile dieser Methode werden z.B. bei Gowers [20] sehr gut erklärt.

*Bemerkung.* Die eben vorgestellte Konstruktion mag den Eindruck vermitteln, dass einige Punkte der projektiven Ebene besondere Punkte sind, verschieden von den anderen. Das ist nicht der Fall, kein Punkt hat eine spezielle Bedeutung; welche Punkte man als die „uneigentlichen“ auffassen will, ist von der Situation abhängig — die projektive Ebene sieht „lokal überall gleich aus“.

Das wird auch aus der geometrischen Interpretation oben klar, wo wir die reelle projektive Ebene mit der Menge aller Ursprungsgeraden im dreidimensionalen Raum identifizieren. Die horizontalen Geraden, die für die uneigentlichen Punkte stehen, sind keine besonderen Geraden.

## Aufgaben

1. *\*\*, Inf* Zeigen Sie, dass es keine projektive Ebene der Ordnung 6 gibt. Schreiben Sie ein Programm, das alle in Frage kommenden Konfigurationen überprüft und ausschließt. Sie müssen schlau sein, denn alle möglichen Familien von 43 7-Tupeln auf 43 Punkten durchzugehen würde zu lange dauern. (Es gibt cleverere Beweise, die keine Fallunterscheidung benötigen, doch die sind nicht leicht zu finden.)

## 9.3 Orthogonale lateinische Quadrate

Ein *lateinisches Quadrat der Ordnung  $n$*  ist eine quadratische Tabelle mit  $n$  Zeilen und  $n$  Spalten. Jeder Eintrag ist eine Zahl aus der Menge  $\{1, 2, \dots, n\}$ , und jede Zahl dieser Menge tritt in genau einer Zeile und in genau einer Spalte auf. Abbildung 9.5 zeigt zwei lateinische Quadrate der Ordnung 3.

Wir erklären jetzt, wann zwei lateinische Quadrate der gleichen Ordnung *orthogonal* heißen. Stellen Sie sich eines der Quadrate auf Transparentpapier geschrieben vor und legen Sie es über das andere Quadrat, so dass die entsprechenden Einträge übereinander liegen. Die Quadrate aus Abb. 9.5 ergeben übereinander gelegt zum Beispiel

1	1	2	2	3	3
2	3	3	1	1	2
3	2	1	3	2	1

Auf diese Weise erhalten wir  $n^2$  geordnete Paare, jedes Paar besteht aus einem Eintrag aus dem Quadrat auf dem Transparentpapier und dem entsprechenden Eintrag des darunter liegenden Quadrats. Die beiden Quadrate heißen orthogonal, wenn kein geordnetes Paar doppelt auftritt. Da es  $n^2$  solcher geordneter Paare mit den Zahlen von 1 bis  $n$  gibt, muss also jedes Paar genau einmal vorkommen.

**9.3.1 Satz.** *Sei  $M$  eine Menge lateinischer Quadrate der Ordnung  $n$ , von denen je zwei orthogonal zueinander sind. Dann ist  $|M| \leq n - 1$ .*

*Beweis.* Wir beginnen mit folgender Beobachtung. Seien  $A$  und  $B$  zwei orthogonale lateinische Quadrate der Ordnung  $n$ , und sei  $\pi$  eine Permutation der Zahlen  $1, 2, \dots, n$ . Wir konstruieren ein neues lateinisches Quadrat  $A'$ , dessen Eintrag an der Stelle  $(i, j)$  die Zahl  $\pi(a_{ij})$  ist, wobei  $a_{ij}$  der Eintrag in dem lateinischen Quadrat  $A$  an der Stelle  $(i, j)$  ist. Es ist nicht schwer mit der Definition zu überprüfen, dass  $A'$  und  $B$  ebenfalls orthogonale lateinische Quadrate sind. Man könnte diese Beobachtung zusammenfassen als „die Orthogonalität lateinischer Quadrate ändert sich nicht, wenn man ihre Symbole umbenennt“.<sup>4</sup>

Nun zum Beweis des Satzes. Stellen wir uns vor, wir haben lateinische Quadrate  $A_1, A_2, \dots, A_t$ , von denen je zwei orthogonal

---

<sup>4</sup>Natürlich gibt es keinen tieferen Grund dafür, ein lateinisches Quadrat unbedingt mit den Zahlen  $1, 2, \dots, n$  auszufüllen. Man kann genauso gut  $n$  verschiedene Buchstaben nehmen oder  $n$  verschiedene Sorten Cognac. Dies ist wohl der rechte Augenblick für die Frage: Warum heißen lateinische Quadrate lateinisch? Anscheinend hat man in einigen alten Problemen als Symbole in den Quadranten lateinische Buchstaben gewählt (während andere Quadrate mit griechischen Buchstaben gefüllt wurden und dementsprechend als griechische Quadrate bezeichnet wurden).

sind. Für jedes  $A_i$  permutieren wir seine Symbole (d.h. die Zahlen  $1, 2, \dots, n$ ) so, dass in dem entstehenden lateinischen Quadrat  $A'_i$  die erste Zeile  $(1, 2, \dots, n)$  ist. Nach obiger Beobachtung sind die lateinischen Quadrate  $A'_1, \dots, A'_t$  immer noch paarweise orthogonal. Betrachten wir in dem Quadrat  $A'_i$  den Eintrag  $(2, 1)$ . Welche Zahlen können dort stehen? Zunächst einmal kann dieser Eintrag nicht 1 sein, denn in der ersten Spalte gibt es schon eine 1 in der ersten Zeile. Dann können keine zwei lateinischen Quadrate  $A'_i$  und  $A'_j$  dieselbe Zahl an der Stelle  $(2, 1)$  haben: Andernfalls könnten wir  $A'_i$  und  $A'_j$  übereinander legen und würden an der Stelle  $(2, 1)$  ein Paar identischer Zahlen erhalten, zum Beispiel  $(k, k)$ . Dieses Paar tritt aber schon als  $k$ -ter Eintrag in der ersten Zeile auf! Deshalb kann jede der Zahlen  $2, 3, \dots, n$  nur in einem der  $A'_i$  an der Stelle  $(2, 1)$  stehen und deshalb ist  $t \leq n - 1$ .  $\square$

Vielleicht wundern Sie sich, warum wir in einem Kapitel über projektive Ebenen plötzlich über lateinische Quadrate sprechen. Der nächste Satz erklärt das.

**9.3.2 Satz.** Zu jedem  $n \geq 2$  gibt es genau dann eine projektive Ebene der Ordnung  $n$ , wenn es  $n - 1$  paarweise orthogonale lateinische Quadrate der Ordnung  $n$  gibt.

*Beweis von Satz 9.3.2.* Wir werden den Beweis nicht im Detail durchführen. Wir beschreiben nur, wie man eine projektive Ebene aus orthogonalen lateinischen Quadrate konstruiert und umgekehrt. Gegeben seien  $n - 1$  orthogonale lateinische Quadrate  $L_1, \dots, L_{n-1}$  der Ordnung  $n$ . Wir konstruieren eine projektive Ebene der Ordnung  $n$ .

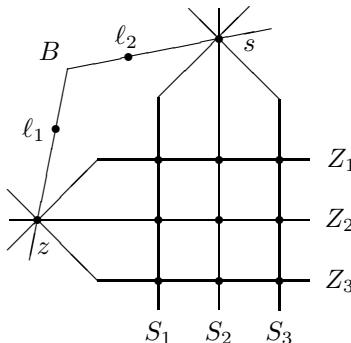
Zuerst definieren wir die Menge  $X$  der Punkte. Sie hat  $n + 1$  un-eigentliche Punkte, die wir mit  $z, s$  und  $\ell_1, \ell_2, \dots, \ell_{n-1}$  bezeichnen, und  $n^2$  Punkte  $(i, j)$ ,  $i, j = 1, 2, \dots, n$ . Jetzt führen wir in mehreren Schritten die Geraden ein. Eine der Geraden  $B = \{z, s, \ell_1, \dots, \ell_{n-1}\}$  besteht aus den uneigentlichen Punkten. Dann gibt es  $n$  Geraden  $Z_1, Z_2, \dots, Z_n$ , wobei

$$Z_i = \{z, (i, 1), (i, 2), \dots, (i, n)\},$$

und schließlich die  $n$  Geraden

$$S_j = \{s, (1, j), (2, j), \dots, (n, j)\}.$$

Das folgenden Bild zeigt alle diese Geraden (für  $n = 3$ ):



Die Punkte und Geraden in der projektiven Ebene, die wir bis jetzt gezeichnet und benannt haben, müssen so in jeder projektiven Ebene der Ordnung  $n$  aussehen (wir haben noch gar keine Information über die  $n - 1$  orthogonalen lateinischen Quadrate benutzt). Die Quadrate benutzen wir jetzt um die Geraden durch die Punkte  $\ell_1, \ell_2, \dots, \ell_{n-1}$  festzulegen (abgesehen von  $B$ ). Wie die Notation nahelegt, bestimmt das lateinische Quadrat  $L_k$  die Gerade durch den Punkt  $\ell_k$ . Ist  $(L_k)_{ij}$  der Eintrag von  $L_k$  in der  $i$ -ten Zeile und  $j$ -ten Spalte, so definieren wir die Geraden

$$G_{km} = \{\ell_k\} \cup \{(i, j) : (L_k)_{ij} = m\}$$

für  $m = 1, 2, \dots, n$  und  $k = 1, 2, \dots, n - 1$ . Ist zum Beispiel  $L_1$  das linke lateinische Quadrat aus Abb. 9.5, so ist die Gerade  $G_{11}$ , die der Zahl 1 in dem Quadrat entspricht,  $G_{11} = \{s_1, (1, 1), (2, 3), (3, 2)\}$ .

Damit haben wir die endliche projektive Ebene, die zu den  $n - 1$  orthogonalen lateinischen Quadrate gehört, beschrieben. Wir müssen jetzt noch die Axiome für projektive Ebenen überprüfen. Es lässt sich leicht ausrechnen, dass die Anzahl der Geraden und der Punkte jeweils  $n^2 + n + 1$  ist. Nach Aufgabe 9.1.8 genügt es nun zu zeigen, dass je zwei Geraden sich in höchstens einem Punkt schneiden. Dazu muss man die beiden Tatsachen benutzen, dass jedes  $L_k$  ein lateinisches Quadrat ist und dass je zwei von ihnen orthogonal sind. Das überlassen wir Ihnen als Übungsaufgabe.

Um die Äquivalenz in Satz 9.3.2 zu zeigen, muss man  $n - 1$  orthogonale lateinische Quadrate aus einer projektiven Ebene der Ordnung  $n$  konstruieren. Diese Konstruktion geht genauso wie die umgekehrte. Wir wählen in der projektiven Ebene zwei beliebige Punkte  $z$  und  $s$  und legen die Bezeichnungen wie in obiger Konstruktion fest. Dann füllen wir das  $k$ -te lateinische Quadrat  $L_k$  entsprechend der Geraden durch den Punkt  $\ell_k$  aus. So viel zum Beweis von Satz 9.3.2. □

*Bemerkung.* Der Beweis wird natürlicher, wenn man endliche affine Ebenen benutzt (vgl. Aufgabe 9.1.10).

## Aufgaben

1. Führen Sie die Konstruktion aus dem Beweis von Satz 9.3.2 für  $n = 2$  durch (es gibt dann bis auf Permutationen der Zahlen nur ein lateinisches Quadrat). Überzeugen Sie sich, dass man auf diese Weise die Fano-Ebene erhält.
2. Zeigen Sie, dass sich in der Konstruktion aus dem Beweis zu Satz 9.3.2 je zwei Geraden in höchstens einem Punkt schneiden (vergessen Sie nicht die Geraden  $Z_i$  und  $S_j$ !). Unterscheiden Sie dabei, ob Sie die Definition eines lateinischen Quadrates benutzen oder die Orthogonalität.
3. Zeigen Sie, dass durch die Konstruktion, die am Ende vom Beweis von Satz 9.3.2 skizziert wird, tatsächlich  $n - 1$  orthogonale lateinische Quadrate entstehen.
4. Wir definieren ein *freies Quadrat* der Ordnung  $n$  als ein  $n \times n$  Quadrat mit Einträgen aus der Menge  $\{1, 2, \dots, n\}$ . Orthogonalität freier Quadrate wird genauso wie für lateinische Quadrate definiert. Betrachten Sie für ein gegebenes  $t$  die beiden folgenden Bedingungen:
  - (i) Es gibt  $t$  paarweise orthogonale lateinische Quadrate der Ordnung  $n$ .
  - (ii) Es gibt  $t + 2$  paarweise orthogonale freie Quadrate der Ordnung  $n$ .
    - (a) Zeigen Sie, dass (ii) aus (i) folgt.
    - (b) \*Zeigen Sie, dass (i) aus (ii) folgt.
5. Sei  $T$  ein endlicher Körper mit  $n$  Elementen. Wir bezeichnen seine Elemente mit  $t_0, t_1, \dots, t_{n-1}$ , wobei  $t_0 = 0$  und  $t_1 = 1$ . Für  $k = 1, 2, \dots, n - 1$  definieren wir  $n \times n$  Matrizen  $S^{(k)}$ , wobei der Eintrag der Matrix  $S^{(k)}$  an der Stelle  $(i, j)$  gleich  $t_i t_k + t_j$  ist (Multiplikation und Addition sind dabei wie im Körper  $T$ ). Zeigen Sie, dass  $S^{(1)}, S^{(2)}, \dots, S^{(n-1)}$  eine Menge von paarweise orthogonalen lateinischen Quadrate der Ordnung  $n$  ist. (Mit Satz 9.3.2 erhalten Sie dann eine neue Konstruktion einer projektiven Ebene der Ordnung  $n$ .)
6. Für natürliche Zahlen  $m \leq n$  definieren wir ein *Lateinisches  $m \times n$  Rechteck* als ein Rechteck mit  $m$  Zeilen und  $n$  Spalten mit Einträgen aus der Menge  $\{1, 2, \dots, n\}$  und zwar so, dass keine Zeile oder Spalte eine Zahl doppelt enthält. Bestimmen Sie die Anzahl aller möglichen  $2 \times n$  Rechtecke.

## 9.4 Kombinatorische Anwendungen

In der Kombinatorik dienen endliche projektive Ebenen häufig als Beispiele für Mengensysteme mit interessanten Eigenschaften. Wenn

man eine Vermutung über endliche Mengensysteme hat und nach einem Gegenbeispiel sucht, oder wenn man ein Mengensystem mit bestimmten Eigenschaften braucht, dann stehen die Chancen nicht schlecht, bei endlichen projektiven Ebenen fündig zu werden.

Versucht man den Nutzen projektiver Ebenen für die Mathematik und ihre Anwendungen darzustellen, dann ist das ungefähr so, als wollte man die Bedeutung von Nudeln für die Küche erklären. Natürlich kann man hervorragend ohne Nudeln kochen. Es gibt auch wunderbare Nudelgerichte, doch ist es eine Sache eines guten Rezepts (und Kochs) sowie der weiteren Zutaten wie Gewürze, ob sie fade oder interessant schmecken. Die Nudel an sich kann wohl nur Spezialisten (und Kinder) begeistern. Wir haben noch nicht genug mathematische Zutaten und Gewürze für ein wirklich raffiniertes Rezept, deshalb servieren wir einfach kombinatorische Hausmannskost.

Just zu der Zeit, als dieser Abschnitt entstand, berichteten Zeitungen über die erste Schweizer Bank, die Online Banking im Internet einföhrte (in den USA gab es das schon seit über einem Jahr). Natürlich ist die Sicherheit der Informationen, die über das Internet ausgetauscht werden, in diesem Fall von höchster Bedeutung. Der Code, der zur Zeit als unknackbar gilt und von dem die Banken sich Sicherheit<sup>5</sup> erhoffen, basiert auf so genannten elliptischen Kurven über endlichen Körpern. Die Theorie elliptischer Kurven wurde seit langem in der Zahlentheorie und algebraischen Geometrie entwickelt, Gebiete, die gewöhnlich als absolut reine Mathematik ohne irgendwelche Anwendungsmöglichkeiten angesehen wurden. Und diese elliptischen Kurven wohnen (als Teilmengen) in endlichen projektiven Ebenen. So kann es kommen.

Das Buch von Koblitz [23] ist sowohl eine Einföhrung in die Zahlentheorie als auch ein Tor zur Welt der mathematischen Kryptographie. Aber kommen wir zurück zu unseren kombinatorischen Anwendungen.

**2-Färbungen von Mengenfamilien.** Sei  $X$  eine endliche Menge und  $\mathcal{M}$  eine Familie von Teilmengen von  $X$ . Wir sagen, dass die Mengenfamilie  $\mathcal{M}$  2-färbbar ist, wenn man jeden Punkt aus  $X$  mit einer von zwei gegebenen Farben, zum Beispiel rot oder weiß, so färben kann, dass jede Menge aus  $M \in \mathcal{M}$  Punkte beider Farben enthält. (2-Färbbarkeit wird in der Literatur oft *Eigenschaft B* genannt.)

Ist zum Beispiel  $X = \{1, 2, 3\}$  und  $\mathcal{M} = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$  dann ist  $\mathcal{M}$  nicht 2-färbbar. Allgemein gilt: Enthält jede Menge aus

---

<sup>5</sup>Softwarereprodukte, die diesen Code benutzen, unterliegen ähnlich strengen US Exportbeschränkungen wie Hightech-Waffen.

$\mathcal{M}$  genau 2 Elemente, dann können wir  $(X, \mathcal{M})$  als Graph auffassen. 2-Färbbarkeit ist dann das Gleiche wie bipartit. Was passiert aber, wenn jede Menge aus  $\mathcal{M}$  mehr als 2 Punkte hat? Was weiß man zum Beispiel, wenn alle Mengen aus  $\mathcal{M}$  genau 3 Punkte haben? Es zeigt sich, dass hier 2-Färbbarkeit sehr viel komplizierter ist als für Graphen. Die Frage etwa, ob ein gegebenes  $\mathcal{M}$  2-färbbar ist oder nicht, ist ein schwieriges algorithmisches Problem.

Betrachten wir die folgende naheliegende Frage: Was ist die kleinste Zahl von Mengen in einer Mengenfamilie  $\mathcal{M}$ , bestehend aus 3-Mengen, die nicht 2-färbbar sind? Es stellt sich heraus, dass die Antwort 7 ist, und die Fano Ebene beantwortet die Frage zur Hälfte: Sie besteht aus sieben Mengen, jede enthält genau drei Punkte, und sie ist nicht 2-färbbar (siehe Aufgabe 1). Tatsächlich ist sie sogar die einzige Mengenfamilie mit sieben 3-Mengen, die nicht 2-färbbar ist! Die zweite Hälfte der Antwort geben wir in Abschnitt 10.1 (Satz 10.1.5), wo wir Methoden einführen, mit denen man zeigen kann, dass alle Mengenfamilien mit sechs oder weniger 3-Mengen 2-färbbar sind.

Man könnte noch viel mehr über 2-Färbbarkeit sagen, ein wichtiges Konzept in der Kombinatorik. Hier wollten wir nur ein kleines Problem aus diesem Gebiet vorstellen, in dem projektive Ebenen überraschend ins Spiel kommen.

**Mehr über  $K_{2,2}$ -freie Graphen mit vielen Kanten.** Nach Satz 7.3.1 hat ein Graph  $G$  mit  $m$  Ecken, der keinen  $K_{2,2}$  als Untergraph enthält, höchstens  $\frac{1}{2}(m^{3/2} + m)$  Kanten. Mit projektiven Ebenen können wir nun zeigen, dass diese Schranke im Allgemeinen fast bestmöglich ist:

**9.4.1 Satz.** Für unendlich viele Werte von  $m$  gibt es  $K_{2,2}$ -freie Graphen auf  $m$  Ecken mit mindestens  $0,35m^{3/2}$  Kanten.

*Beweis.* Wir betrachten eine projektive Ebene der Ordnung  $n$  mit ihrem Inzidenzgraphen (wie in dem Abschnitt über Dualität in 9.1). Die Anzahl der Ecken in dem Graphen ist  $m = 2(n^2 + n + 1)$ . Auf jeder der  $n^2 + n + 1$  Geraden liegen  $n + 1$  Punkte, und das heißt, dass die Anzahl der Kanten insgesamt  $(n^2 + n + 1)(n + 1) \geq (n^2 + n + 1)^{3/2} = (\frac{m}{2})^{3/2} \approx 0,35m^{3/2}$  ist.

Was würde es bedeuten, wenn der Inzidenzgraph einen  $K_{2,2}$  als Untergraph enthalten würde? Nun, in der Sprache projektiver Ebenen würde das heißen, dass es zwei Punkte  $x, x'$  und zwei Geraden

$L, L'$  gibt, so dass  $x \in L, x' \in L, x \in L'$  und  $x' \in L'$ . In einer projektiven Ebene kann das jedoch nicht passieren.  $\square$

*Bemerkung.* Die Konstante 0,35 in Satz 9.4.1 kann noch etwas verbessert werden. Der optimale Wert ist 0,5 (vgl. Aufgabe 2).

## Aufgaben

1. Zeigen Sie, dass die Fano-Ebene nicht 2-färbbar ist.
2. (Bessere  $K_{2,2}$ -freie Graphen) Sei  $n$  eine Primzahlpotenz und sei  $K$  ein  $n$ -elementiger Körper. Wir betrachten die Äquivalenzklassen der Äquivalenzrelation  $\approx$  auf der Menge der Tripel  $K^3 \setminus \{(0, 0, 0)\}$  (wie in Abschnitt 9.2). Diese Klassen sollen die Ecken eines Graphen  $G$  sein, und zwei Ecken  $(a, b, c)$  und  $(x, y, z)$  werden genau dann durch eine Kante verbunden, wenn  $ax + by + cz = 0$ . Zeigen Sie, dass
  - (a) die Kanten wohldefiniert sind,
  - (b) \*der Graph  $G$  keinen  $K_{2,2}$  als Untergraph enthält,
  - (c) jede Ecke mindestens Grad  $n$  hat,
  - (d) wenn  $m = n^2 + n + 1$  die Anzahl der Ecken ist, dann ist die Anzahl der Kanten mindestens  $\frac{1}{2}m^{3/2} - m$ .
3. Sei  $G$  ein bipartiter Graph, dessen Eckenklassen beide  $n$  Ecken enthalten und der keinen  $K_{2,2}$  als Untergraph enthält.
  - (a) \*Zeigen Sie mit der Methode aus Abschnitt 7.3, dass  $G$  höchstens
 
$$\frac{1}{2}n(1 + \sqrt{4n - 3})$$
 Kanten hat.
  - (b) \*Zeigen Sie, dass ein solches  $G$  mit exakt dieser Anzahl von Kanten genau dann existiert, wenn es eine projektive Ebene der Ordnung  $q$  gibt mit  $n = q^2 + q + 1$ .



# 10

## Wahrscheinlichkeit und probabilistische Beweise

---

Wahrscheinlich kennen Sie das eine oder andere Problem, in dem es um die Bestimmung der Wahrscheinlichkeit für das Eintreffen eines Ereignisses geht (mehrere solche Probleme stecken auch in den anderen Kapiteln). In Lehrbüchern finden sich häufig „lebensnahe“ Probleme oder zumindest solche, die lebensnah aussehen. Darin geht es um das Mischen oder Ziehen von Karten, um das Werfen von Münzen oder gar Nadeln, auch um defekte Glühbirnen, unterbrochene Telefonleitungen oder radioaktiven Zerfall — je nach Interessen und Fantasie der Autoren. In diesem Kapitel möchten wir eine bemerkenswerte mathematische Anwendung der Wahrscheinlichkeitstheorie zeigen, wie man nämlich mathematische Aussagen mittels elementarer Wahrscheinlichkeitstheorie beweisen kann, auch wenn sie gar nichts mit Wahrscheinlichkeiten oder Zufall zu tun haben.

Alon und Spencer [13] ist ein hervorragendes Buch zum genaueren Studium probabilistischer<sup>1</sup> Methoden in der Kombinatorik, und als Lehrbuch der Wahrscheinlichkeitstheorie empfehlen wir Grimmett und Stirzaker [21] oder auf Deutsch Krengel [24].

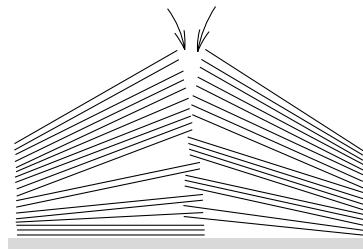
### 10.1 Beweis durch Zählen

In zwei einführenden Beispielen werden wir nicht von Wahrscheinlichkeit sprechen; stattdessen benutzen wir einfache Zählargumente.

**10.1.1 Beispiel.** Wir beginnen mit einem nagelneuen Kartenspiel mit 52 Karten (die Karten liegen noch in der Reihenfolge, wie sie

---

<sup>1</sup>Das Adjektiv „probabilistisch“ bedeutet: „Mit Mitteln der Wahrscheinlichkeitstheorie“. Es ist vom englischen Wort „probability“ für „Wahrscheinlichkeit“ abgeleitet.



**Abb. 10.1** „Professionelles“ Kartenmischen.

aus der Fabrik kommen). Wir mischen die Karten mit der „professionellen“ Methode, bei der man exakt die obere Hälfte der Karten abhebt, und dann die beiden gleich großen Stapel ineinander gleiten lässt; die Ordnung der Karten in jedem Teilstapel bleibt dabei unverändert (siehe Abb. 10.1). Wir beweisen, dass aus höchstens viermaliger Wiederholung dieser Prozedur nicht alle möglichen Anordnungen der Karten hervorgehen können, dass also vier Runden „Profimischen“ sicher keine zufällige Ordnung der Karten ergibt.

*Beweis.* Insgesamt sind  $52!$  Anordnungen der Karten möglich. Wir zählen nun, wie viele verschiedene Anordnungen sich durch oben beschriebene Mischprozedur erzeugen lassen. Auf wie viele Arten kann man die zwei Teilstapel ineinander mischen (zur Unterscheidung nennen wir sie den linken und den rechten Stapel)? Wenn wir die Ordnung der Karten in beiden Stapeln kennen, dann genügt zur Rekonstruktion der Anordnung aller Karten in dem Stapel (nach einmaligem Mischen) die Kenntnis, welche Karten in dem Spiel aus dem linken und welche aus dem rechten Stapel kommen. Nach dem ersten Teilen und ineinander Blättern erhalten wir also eine von  $\binom{52}{26}$  möglichen Ordnungen, durch viermalige Wiederholung erhält man daher höchstens  $\binom{52}{26}^4$  verschiedene Ordnungen. Mit einem Taschenrechner oder mithilfe der Abschätzungen aus Kapitel 3 sehen wir, dass diese Zahl kleiner ist als  $52!$ ; deshalb existiert eine Ordnung, die mit viermaligem Mischen nicht erreichbar ist.  $\square$

Das eben bewiesene Resultat macht keine Aussage darüber, ob wir alle möglichen Ordnungen mit fünfmaligem Mischen erreichen können. Die Frage, wie oft man mischen muss, bis die Reihenfolge der Karten als zufällig bezeichnet werden kann, ist wesentlich schwieriger. Darum geht es im Artikel von Bayer und Diaconis [35].

**Komplizierte Boolesche Funktionen.** Eine Boolesche Funktion in  $n$  Variablen ist eine Abbildung  $f: \{0, 1\}^n \rightarrow \{0, 1\}$ , die jeder möglichen Kombination von  $n$  Nullen und Einsen einen der beiden Werte 0 oder 1 zuweist. (Hier repräsentiert 1 den logischen Wert „wahr“ und 0 den logischen Wert „falsch“.) Eine Boolesche Funktion kann man durch ihre Wertetabelle beschreiben, aber auch auf viele andere Arten. So definiert z.B. ein Computerprogramm, das  $n$  Bit einliest und als Antwort JA oder NEIN ausgibt, eine Boolesche Funktion in  $n$  Variablen. Aber auch ein elektrischer Schaltkreis mit  $n$  Eingabedrähten und einem Ausgabedraht definiert eine Boolesche Funktion in  $n$  Variablen, wobei wir stillschweigend annehmen, dass Ein- und Ausgabe jeweils nur zwei verschiedene Zustände annehmen können.

Wir möchten zeigen, dass es Boolesche Funktionen gibt, die nur sehr lange Beschreibungen haben, d.h. ein sehr langes Programm, einen Schaltkreis mit einer riesigen Anzahl elektrischer Bauteile, etc. Am einfachsten ist dieser Beweis vermutlich mit noch einer anderen Beschreibung Boolescher Funktionen, nämlich durch *logische Formeln*.

Eine *logische Formel in  $n$  Variablen* ist eine Zeichenkette, die aus Symbolen  $x_1, x_2, \dots, x_n$  für die Variablen besteht (jede davon darf auch mehrfach auftreten), aus Klammern und aus den folgenden Symbolen für die logischen Verknüpfungen:  $\wedge$  (die Konjunktion *und*),  $\vee$  (die Disjunktion *oder*),  $\Rightarrow$  (die Implikation *daraus folgt*),  $\Leftrightarrow$  (die Äquivalenz *genau dann, wenn*) und  $\neg$  (die Negation *nicht*). Natürlich ist nicht jede Folge dieser Symbole eine logische Formel; eine Formel muss außerdem einfache syntaktische Regeln wie saubere Klammersetzung befolgen. Die Details dieser Regeln interessieren uns jetzt nicht. Eine korrekte Formel in drei Variablen ist beispielsweise  $(x_1 \wedge x_2) \vee (x_3 \wedge \neg x_1)$ . Jede logische Formel in  $n$  Variablen definiert eine Boolesche Funktion in  $n$  Variablen: Sind Werte für die Variablen  $x_1, x_2, \dots, x_n$  gegeben, dann setzen wir diese Werte in die Formel ein und werten den Wahrheitswert der Formel mithilfe der Regeln für die verschiedenen logischen Verknüpfungen aus. Zum Beispiel ist  $0 \wedge 0 = 0 \wedge 1 = 1 \wedge 0 = 0$  und  $1 \wedge 1 = 1$ , und so weiter. Es ist nicht besonders schwierig zu zeigen, dass sich jede Boolesche Funktion mittels einer Formel ausdrücken lässt. Die Frage ist nun: Wie lang muss so eine Formel sein?

Wir zeigen Folgendes:

**10.1.2 Hilfsatz.** *Es gibt eine Boolesche Funktion in  $n$  Variablen, die nicht durch eine Formel mit weniger als  $2^n / \log_2(n + 8)$  Symbolen beschrieben werden kann. Schon bei 23 Variablen sind demnach für manche Funktionen mehr als eine Million Symbole vonnöten.*

*Beweis.* Die Anzahl aller Booleschen Funktionen in  $n$  Variablen ist  $2^{2^n}$ , während die Anzahl der Formeln in  $n$  Variablen, die man mit höchstens  $m$  Symbolen schreiben kann, nicht größer ist als  $(n + 8)^m$ ; denn auf jeder der  $m$  Positionen in der Formel kann eines der  $n + 7$  erlaubten

Symbole stehen, eventuell auch ein Leerzeichen. Auf diese Weise haben wir auch jede Menge unsinniger Zeichenketten gezählt, doch diese grobe obere Abschätzung genügt völlig. Wenn  $2^{2^n} > (n + 8)^m$ , dann gibt es also eine Boolesche Funktion, die durch eine Formel mit höchstens  $m$  Symbolen nicht ausgedrückt werden kann. Anwendung des Logarithmus auf beide Seiten der Ungleichung ergibt  $m \geq 2^n / \log_2(n + 8)$ .  $\square$

Genauso kann man verfahren, wenn die Booleschen Funktionen als Programme in einer (vorher festgelegten) Programmiersprache gegeben sind, als Schaltkreise aus einer vorgegebenen Palette elektrischer Bauteile, usw. In jedem dieser Fälle zeigt ein Zählargument ähnlich dem eben vorgeführten die Existenz von Funktionen in  $n$  Variablen, die sich nicht mit einem Programm oder Schaltkreis ausdrücken lassen, der kleiner ist als ungefähr  $2^n$ . (Wir haben den Beweis mit logischen Formeln geführt, weil deren Definition und Abzählen besonders leicht ist.)

Diese beiden Beispiele sind nach dem gleichen Muster gestrickt: Wir haben eine Menge von Objekten und möchten zeigen, dass mindestens eines unter ihnen „gut“ ist (d.h. eine gewünschte Eigenschaft aufweist; in Beispiel 10.1.1 sind diejenigen Anordnungen der Karten gut, die mit viermaligem Mischen nicht erreichbar sind). Wir zählen, wie viele Objekte es insgesamt gibt, und bestimmen eine obere Schranke für die Anzahl der „schlechten“ Objekte. Ziel ist auf diese Weise zu zeigen, dass die Anzahl der schlechten Objekte kleiner ist als die Gesamtzahl aller Objekte, denn daraus folgt, dass mindestens eines der Objekte gut sein muss. In vielen Fällen stellt sich auf diese Weise sogar heraus, dass die meisten der Objekte gut sind.

Eine bemerkenswerte Eigenschaft dieser Methode ist, dass wir nicht etwa ein bestimmtes gutes Objekt konstruieren, ja dass wir nicht die leiseste Information erhalten, wie eines aussehen könnte — wir erfahren nur, dass eines existiert. In Beispiel 10.1.1 haben wir gezeigt, dass es eine nicht erreichbare Anordnung der Karten gibt, ohne eine spezielle solche Ordnung anzugeben. Im Beweis von Hilfssatz 10.1.2 finden wir keinen Hinweis, wie eine „komplizierte“ Boolesche Funktion (die keine kurze Formel hat) zu finden ist. Dies ist die typische Situation bei Beweisen dieser Art. Das mag paradox erscheinen, zumal wir in der Regel beweisen können, dass die überwältigende Mehrheit der Objekte gut ist; es ist also wie die Suche nach einem Halm im Strohhaufen (mit nur wenigen Nadeln darin). Doch in vielen Situationen ist es sehr schwierig, sich nicht an den Nadeln zu stechen. Für viele kombinatorische Objekte gibt es relativ einfache Existenzbeweise, jedoch keine oder nur sehr komplizierte explizite Konstruktionen.

Das Argument mit guten und schlechten Objekten lässt sich auch in der Sprache der Wahrscheinlichkeitstheorie formulieren. Stellen wir uns vor, wir wählen ein zufälliges Element aus der Menge der betrachteten Objekte. Wenn wir beweisen, dass dieses Element mit einer von Null verschiedenen Wahrscheinlichkeit gut ist, so folgt daraus, dass es mindestens ein gutes Objekt geben muss. Bei komplizierteren Problemen wird die Formulierung mit Wahrscheinlichkeiten einfacher als das Abzählen der Objekte; außerdem bieten sich dann verschiedene Ergebnisse aus der Wahrscheinlichkeitstheorie an, deren Formulierung ohne Wahrscheinlichkeiten unübersichtlich wird. Das nun folgende Beispiel werden wir in der Sprache der Wahrscheinlichkeitstheorie formulieren — wenn Sie das Gefühl haben, dass Ihnen einige der verwendeten Begriffe fehlen, dann sollten Sie zunächst den folgenden Abschnitt lesen.

**Nochmal 2-Färbungen.** Sei  $X$  eine endliche Menge und  $\mathcal{M}$  ein System von Teilmengen von  $X$ . Wir erinnern uns an die Definition der 2-Färbbarkeit aus Abschnitt 9.4: Wir nennen  $\mathcal{M}$  2-färbbar, wenn sich die Punkte aus  $X$  derart rot oder weiß färben lassen, dass keine Menge aus  $\mathcal{M}$  ausschließlich aus roten oder ausschließlich aus weißen Punkten besteht. Hier geht es um das folgende Problem (von dem wir einen Spezialfall bereits in Abschnitt 9.4 untersucht haben).

**10.1.3 Problem.** Was ist die kleinste Zahl  $m(k)$  von Mengen in einem System  $\mathcal{M}$ , das nicht 2-färbbar ist und in dem jede Menge genau  $k$  Elemente hat?

Einfach ist die Bestimmung von  $m(2) = 3$ , denn ein Graph, der nicht bipartit ist, braucht mindestens drei Kanten. Doch schon für  $k = 3$  ist die Frage sehr viel schwieriger. In Abschnitt 9.4 haben wir ein System mit sieben Tripeln kennen gelernt, das nicht 2-färbbar ist, die Fano-Ebene; also ist  $m(3) \leq 7$ . Tatsächlich ist  $m(3) = 7$ ; um das zu beweisen müssen wir zeigen, dass alle Systeme mit sechs oder weniger Tripeln 2-färbbar sind. Wir beginnen mit einem allgemeinen Satz, aus dem wir im Fall  $k = 3$  eine schwächere Abschätzung erhalten. Mit ein paar Zusatzargumenten verbessern wir diese Abschätzung dann noch auf  $m(3) \geq 7$ .

**10.1.4 Satz.** Es gilt  $m(k) \geq 2^{k-1}$ , d.h. jedes System, das aus weniger als  $2^{k-1}$  Mengen der Größe  $k$  besteht, ist 2-färbbar.

*Beweis.* Sei  $\mathcal{M}$  ein System  $k$ -elementiger Teilmengen einer Menge  $X$  mit  $|\mathcal{M}| = m$ . Jedem Punkt aus  $X$  geben wir nach der folgenden

Regel zufällig eine der Farben Rot oder Weiß. Für jeden Punkt  $x \in X$  werfen wir eine faire Münze. Fällt Kopf, so färben wir  $x$  weiß, fällt Zahl, dann färben wir  $x$  rot.

Sei  $M \in \mathcal{M}$  eines der  $k$ -Tupel in dem betrachteten System. Wie groß ist die Wahrscheinlichkeit, dass alle Punkte aus  $M$  in so einer zufälligen Färbung die gleiche Farbe erhalten? Die Wahrscheinlichkeit dafür, dass alle  $k$  Punkte gleichzeitig weiß sind, ist natürlich  $2^{-k}$ , und die Wahrscheinlichkeit, dass alle Punkte aus  $M$  rot sind, ist ebenso  $2^{-k}$ . Insgesamt ist die Wahrscheinlichkeit dafür, dass  $M$  monochromatisch wird, d.h. dass alle Punkte aus  $M$  die gleiche Farbe erhalten, gleich  $2 \cdot 2^{-k} = 2^{1-k}$ . Deshalb ist die Wahrscheinlichkeit, dass mindestens eine der  $m$  Mengen in  $\mathcal{M}$  monochromatisch ist, höchstens  $m \cdot 2^{1-k}$ . Wenn diese Zahl echt kleiner als 1 ist, d.h. wenn  $m < 2^{k-1}$  ist, dann ist unsere zufällige Färbung mit einer von Null verschiedenen Wahrscheinlichkeit eine 2-Färbung für das System  $\mathcal{M}$ . Das bedeutet, dass es mindestens eine 2-Färbung gibt. Das ist ganz gewiss und sicher und hat nichts mehr mit Wahrscheinlichkeiten zu tun! Wir haben Satz 10.1.4 bewiesen.  $\square$

Wie gut ist die gerade bewiesene Schranke für  $m(k)$ ? Man weiß, dass die Funktion  $m(k)$  für große  $k$  etwa wie  $2^k$  wächst (genauer gesagt, gilt  $m(k) = \Omega(2^k k^{1/3})$  und  $m(k) = O(2^k k^2)$ ; siehe [13]), und so gibt uns der Satz eine recht gute Vorstellung vom Verhalten von  $m(k)$ . Andererseits erhalten wir für  $k = 3$  nur die Abschätzung  $m(k) \geq 4$ , die vom tatsächlichen Wert 7 recht weit entfernt ist. Mit zwei kleinen Tricks überbrücken wir diesen Abstand.

### 10.1.5 Satz. $m(3) \geq 7$ .

Wir müssen zeigen, dass jedes System von 6 Tripeln auf einer endlichen Menge  $X$  2-färbbar ist. Wir unterscheiden zwei Fälle:  $|X| \leq 6$  und  $|X| > 6$ . Nur den ersten Fall werden wir mit einem probabilistischen Argument angehen.

**Lemma.** *Sei  $X$  eine Menge mit höchstens 6 Elementen, und sei  $\mathcal{M}$  ein System von höchstens 6 Tripeln auf  $X$ . Dann ist  $\mathcal{M}$  2-färbbar.*

*Beweis.* Wenn nötig, fügen wir weitere Punkte zur Menge  $X$  hinzu, bis sie genau sechs Punkte hat. Wir wählen drei der sechs Punkte zufällig aus und färben sie weiß, die anderen drei Punkte färben wir rot. So eine Färbung auszuwählen, haben wir  $\binom{6}{3} = 20$  Möglichkeiten. Ist  $M$  ein Tripel aus  $\mathcal{M}$ , dann ist  $M$  nur in zwei der möglichen

Färbungen monochromatisch: Entweder ist  $M$  rot und der Rest weiß, oder  $M$  ist weiß und die restlichen Punkte sind rot. Die Wahrscheinlichkeit, dass  $M$  monochromatisch ist, ist also  $\frac{1}{10}$ . Die Wahrscheinlichkeit, dass eines der sechs Tripel aus  $\mathcal{M}$  monochromatisch ist, ist daher nicht größer als  $\frac{6}{10} < 1$ , also gibt es eine 2-Färbung.  $\square$

Der gleiche Beweis zeigt, dass bis zu neun Tripel auf 6 Punkten 2-färbbar sind.

Für den zweiten Schritt benötigen wir die folgende Definition. Sei  $(X, \mathcal{M})$  ein Mengensystem und  $x, y$  zwei Elemente aus  $X$ . Wir nennen  $x$  und  $y$  *verbunden*, wenn es eine Menge  $M \in \mathcal{M}$  gibt, die  $x$  und  $y$  beide enthält. Sind zwei Punkte  $x$  und  $y$  nicht verbunden, dann definieren wir ein neues Mengensystem  $(X', \mathcal{M}')$ , in dem wir  $x$  und  $y$  „aneinander kleben“: Wir ersetzen die Punkte  $x$  und  $y$  durch einen einzelnen Punkt  $z$ , so dass in allen Mengen, die zuvor  $x$  oder  $y$  enthielten, nun  $z$  enthalten ist. Formal sieht das so aus:  $X' = (X \setminus \{x, y\}) \cup \{z\}$ ,  $\mathcal{M}' = \{M \in \mathcal{M}: M \cap \{x, y\} = \emptyset\} \cup \{(M \setminus \{x, y\}) \cup \{z\}: M \in \mathcal{M}, M \cap \{x, y\} \neq \emptyset\}$ .

Wir stellen fest: Ist  $\mathcal{M}$  ein System von Tripeln und sind zwei Punkte  $x$  und  $y$  nicht verbunden, dann ist  $(X', \mathcal{M}')$  wieder ein System von Tripeln, und die Menge  $X'$  hat einen Punkt weniger als  $X$ . Des Weiteren behaupten wir: Wenn  $(X', \mathcal{M}')$  2-färbbar ist, dann auch  $(X, \mathcal{M})$ . Um das einzusehen betrachten wir eine 2-Färbung der Menge  $X'$  und färben  $X$  genauso, nur dass  $x$  und  $y$  beide die Farbe des Punktes  $z$  erhalten. Auf diese Weise kann natürlich keine monochromatische Menge entstehen. Um den Beweis von Satz 10.1.5 abzuschließen genügt es also, folgendes zu zeigen:

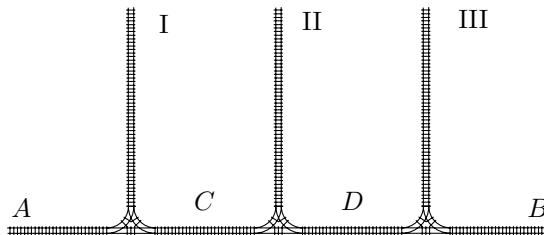
**Lemma.** Sei  $(X, \mathcal{M})$  ein System von sechs Tripeln mit  $|X| \geq 7$ . Dann enthält  $X$  zwei Punkte, die in  $\mathcal{M}$  nicht verbunden sind.

*Beweis.* Ein Tripel  $M \in \mathcal{M}$  bewirkt, dass drei Punktpaare verbunden sind. Durch sechs Tripel können also höchstens  $3 \cdot 6 = 18$  Paare verbunden werden. Die Gesamtzahl an Paaren in einer Menge mit sieben Elementen ist jedoch  $\binom{7}{2} = 21$ , also gibt es ein Paar, das nicht verbunden ist. (Wir können sogar sagen, dass mindestens drei Paare nicht verbunden sind.)  $\square$

Übrigens ist der exakte Wert schon für  $m(4)$  nicht bekannt (genauso wenig für alle größeren  $k$ ). Man sieht ziemlich einfach, dass man auch  $m(4)$  im Prinzip bestimmen kann, indem man endlich viele Konfigurationen (Systeme von Quadrupeln) betrachtet. Doch die Anzahl der zu untersuchenden Konfigurationen übersteigt offenbar die Leistungsfähigkeit auch von Supercomputern, zumindest solange nicht noch ein wirklich guter Einfall die zu leistende Arbeit erheblich reduziert.

## Aufgaben

1. (a) Beweisen Sie, dass jede Boolesche Funktion in  $n$  Variablen durch eine logische Formel ausgedrückt werden kann.  
 (b) Zeigen Sie, dass die Formel in (a) sogar so gewählt werden kann, dass ihre Länge höchstens  $Cn2^n$  ist (mit einer geeigneten Konstante  $C$ ). \*Können Sie die Größenordnung dieser Schranke noch verbessern, vielleicht auf  $O(2^n)$  oder gar noch besser?
2. (a) Beweisen Sie, dass  $m(4) \geq 15$  ist, d.h. dass jedes System von 14 Quadrupeln 2-färbbar ist. Gehen Sie so ähnlich vor wie beim Beweis von Satz 10.1.5, wo wir zwei Fälle nach der Gesamtzahl der Punkte unterschieden haben.  
 (b) \*Finden Sie eine möglichst gute obere Schranke für  $m(4)!$  Kommen Sie unter 50? Unter 30?
3. Gegeben sind 27 echte Münzen und eine gefälschte, die zwar echt aussieht, aber ein wenig schwerer ist. Zeigen Sie, dass man mindestens vier Wägungen braucht um herauszufinden, welche Münze die gefälschte ist. Für die Wägungen steht eine Balkenwaage zur Verfügung, jedoch keine geeichten Gewichte; man kann also nur Information gewinnen, indem man in beide Waagschalen je  $k$  Münzen legt — dann sieht man, ob eine der Seiten schwerer ist, und wenn ja, welche.
4. \*Auf der unten dargestellten Gleisanlage steht ein Zug mit  $n$  Waggons auf Gleis A. Die Wagen sollen auf Gleis B gefahren werden. Dabei darf jeder der Wagen zwischenzeitlich auf den Rangiergleisen I–III abgestellt werden, jedoch auf jedem nur einmal; die Gleisabschnitte C und D soll jeder Wagen nur einmal passieren.



Beweisen Sie, dass es bei genügend großem  $n$  (d.h. bei genügend vielen Waggons) eine Reihenfolge der Wagen gibt, in welcher der Zug nicht auf Gleis B bereitgestellt werden kann.

## 10.2 Endliche Wahrscheinlichkeitsräume

Nun ist es an der Zeit, die grundlegenden Begriffe der Wahrscheinlichkeitstheorie einzuführen. Wir werden uns auf das beschränken,

was wir für unsere Beispiele brauchen. Dieser Abschnitt kann und soll keinesfalls ein gründliches Studium der Wahrscheinlichkeitstheorie ersetzen. Jeder mathematisch oder in theoretischer Informatik gebildete sollte einiges mehr wissen als das hier dargestellte.

Wahrscheinlichkeit ist ein Begriff, der nicht nur innerhalb, sondern auch außerhalb der Mathematik vorkommt: „Im wirklichen Leben“, „in der Praxis“ oder wie auch immer man das nennen mag. „Wirkliche“ Wahrscheinlichkeit zu definieren ist schwierig, ein philosophisches Problem. In der Mathematik wird dieses Problem nicht gelöst, sie gibt uns jedoch ein bestimmtes Modell der „wirklichen“ Wahrscheinlichkeit, und dieses Modell ist ein rein mathematisches Objekt. Als Fundament sind verschiedene einfache Eigenschaften der Wahrscheinlichkeit, die aus unserem Wissen über die „wirkliche Welt“ abgeleitet sind, in Form von Axiomen in das Modell eingebaut, etwa die Tatsache, dass die Wahrscheinlichkeit für das Eintreten eines Ereignisses plus die Wahrscheinlichkeit seines Nicht-Eintretens 1 ergeben. Hat man die Axiome erst einmal akzeptiert, dann arbeitet man mit der mathematischen Wahrscheinlichkeit genauso wie mit jedem anderen mathematischen Objekt, und alle Eigenschaften und Rechenregeln zum Umgang mit Wahrscheinlichkeiten werden aus den Axiomen logisch abgeleitet. Das Modell bewährt sich sehr gut, seine Voraussagen beschreiben das Verhalten der „wirklichen“ Wahrscheinlichkeit sehr gut; dennoch bedeutet das nicht, dass die mathematische und die „wirkliche“ Wahrscheinlichkeit ein und dasselbe sind. Im Folgenden geht es um die Wahrscheinlichkeit im mathematischen Sinne, Beispiele aus dem „wirklichen Leben“ dienen der Motivation der Begriffe und der Axiome.

Ein Grundbegriff in der Wahrscheinlichkeitstheorie ist der *Wahrscheinlichkeitsraum*. Wir beschränken uns hier auf endliche Wahrscheinlichkeitsräume.

**10.2.1 Definition.** Unter einem endlichen Wahrscheinlichkeitsraum verstehen wir ein Paar  $(\Omega, P)$ , wobei  $\Omega$  eine endliche Menge ist  $P: 2^\Omega \rightarrow [0, 1]$  eine Funktion, die jeder Teilmenge von  $\Omega$  eine Zahl aus dem Intervall  $[0, 1]$  zuordnet und die folgenden Eigenschaften hat:

- (i)  $P(\emptyset) = 0$ ,
- (ii)  $P(\Omega) = 1$  und
- (iii)  $P(A \cup B) = P(A) + P(B)$  für je zwei disjunkte Mengen  $A, B \subseteq \Omega$ .

Die Menge  $\Omega$  kann man sich als die Menge aller möglichen Ausgänge eines Zufallsexperiments vorstellen. Ihre Elemente heißen die *Ergebnisse*,  $\Omega$  heißt *Ergebnisraum*. Beim Würfeln zum Beispiel sind die möglichen Ergebnisse „1 ist gefallen“, „2 ist gefallen“, . . . , „6 ist

gefallen“. Wir könnten diese Ergebnisse kürzer als  $\omega_1, \omega_2, \dots, \omega_6$  schreiben. Teilmengen von  $\Omega$  heißen *Ereignisse*. Ein Beispiel für ein Ereignis ist „eine gerade Zahl ist gefallen“, anders geschrieben  $\{\omega_2, \omega_4, \omega_6\}$ . Die einelementigen Ereignisse wie  $\{\omega_2\}$  oder  $\{\omega_5\}$  heißen auch *Elementarereignisse*.

Die Wahrscheinlichkeitstheorie hat ihre eigene Ausdrucksweise für die verschiedenen mengentheoretischen Operationen mit Ereignissen. Zum Beispiel liest man „ $\omega \in A$ “ als „das Ereignis  $A$  ist eingetreten“, „ $\omega \in A \cap B$ “ interpretiert man als „die Ereignisse  $A$  und  $B$  sind beide eingetreten“, „ $A \cap B = \emptyset$ “ liest sich als „die Ereignisse  $A$  und  $B$  können nicht zugleich eintreten“, und so weiter.

Ist  $A \subseteq \Omega$  ein Ereignis, dann heißt die Zahl  $P(A)$  die *Wahrscheinlichkeit des Ereignisses  $A$* . Die Axiome (i)–(iii) beschreiben Eigenschaften, die man von einer Wahrscheinlichkeit erwartet. Aus Bedingung (iii) sieht man leicht, dass es genügt, die Werte der Funktion  $P$  auf den Elementarereignissen (den einelementigen Ereignissen) zu bestimmen, denn die Wahrscheinlichkeit eines Ereignisses ist gleich der Summe der Wahrscheinlichkeiten all seiner Elementarereignisse (diese etwas ungenaue Ausdrucksweise meint: all seiner einelementigen Teilmengen).

Zu Axiom (iii) in der Definition eines endlichen Wahrscheinlichkeitsraums sollten wir noch bemerken, dass für *je zwei Ereignisse  $A, B \subseteq \Omega$* , auch wenn sie nicht disjunkt sind, die Ungleichung  $P(A \cup B) \leq P(A) + P(B)$  gilt (Aufgabe 1).

Der einfachste und wohl auch wichtigste endliche Wahrscheinlichkeitsraum ist der, in dem alle Elementarereignisse die gleiche Wahrscheinlichkeit haben, bei dem also die Funktion  $P$  für alle Ereignisse  $A$  durch

$$P(A) = \frac{|A|}{|\Omega|}$$

gegeben ist.

Der letztgenannte Wahrscheinlichkeitsraum modelliert die so genannte *klassische Definition der Wahrscheinlichkeit*. In dieser von Laplace formulierten Definition geht man davon aus, dass alle möglichen Ausgänge des betrachteten Zufallsexperiments gleich wahrscheinlich sind (eine Annahme, die sich etwa auf Symmetrie oder Homogenität des Experiments stützen kann). Ist die Anzahl aller möglichen Ergebnisse eines Experiments  $n$ , und führen  $m$  unter ihnen zum Eintreffen eines Ereignisses  $A$ , dann ist die Wahrscheinlichkeit des Ereignisses  $A$  als  $m/n$  definiert. Dies drückt man manchmal durch die Merkregel

aus, Wahrscheinlichkeit ist die Anzahl der günstigen Ergebnisse dividiert durch die Anzahl der möglichen Ergebnisse. Zur Klärung, was Wahrscheinlichkeit ist, ist die klassische Definition nicht so recht befriedigend (das Problem liegt in dem Ausdruck „gleich wahrscheinlich“), und außerdem schließt sie unendliche Wahrscheinlichkeitsräume nicht mit ein; in vielen Situationen liefert sie jedoch zumindest eine nützliche Idee zur Berechnung der Wahrscheinlichkeit.

**Unendliche Wahrscheinlichkeitsräume.** Durch die Beschränkung auf endliche Wahrscheinlichkeitsräume haben wir uns die Situation mathematisch wesentlich vereinfacht. (Ein richtiger Wahrscheinlichkeitstheoretiker würde vermutlich auch sagen, dass wir damit alle interessanten Fälle ausgeschlossen haben.) Zur Modellierung vieler interessanter Experimente ist es jedoch natürlicher, mit unendlichen Wahrscheinlichkeitsräumen zu arbeiten, deren Definition technisch etwas komplizierter ist. Wenn wir zum Beispiel fünf zufällige Punkte aus dem Intervall  $[0, 1]$  wählen, wie groß ist die Wahrscheinlichkeit, dass zwei von ihnen einen Abstand höchstens  $\frac{1}{10}$  haben? Wir können zig Fragen von ähnlicher Art stellen. Zuerst müssten wir klären, was unter einem „zufälligen Punkt aus dem Intervall  $[0, 1]$ “ zu verstehen ist. Die Ergebnisse sollten natürlich alle Punkte in  $[0, 1]$  sein. Und die Wahrscheinlichkeit sollte für jeden Punkt die gleiche sein, zumindest wenn wir möchten, dass die Punkte „gleichmäßig verteilt“ sind; weil es unendlich viele Punkte gibt, muss die Wahrscheinlichkeit für jedes Ergebnis 0 sein. Deshalb ist es in diesem Fall nicht möglich, die Wahrscheinlichkeitsfunktion  $P$  allein über die Elementarereignisse zu definieren (wie wir es im endlichen Fall konnten). Die Wahrscheinlichkeit eines Ereignisses  $A$  muss in gewisser Weise ein „Maß“ für  $A$  sein. Das ist ein komplizierterer Begriff, der eng mit Integration und anderen Fragen der Analysis verbunden ist. Andere Beispiele unendlicher Wahrscheinlichkeitsräume werden wir in den Abschnitten 12.5 und 12.6 verwenden, ohne es weiter zu thematisieren.

Als Nächstes listen wir einige wichtige Typen endlicher Wahrscheinlichkeitsräume auf.

**10.2.2 Definition (Eine 0-1-Zufallsfolge der Länge  $n$ ).** Die Ergebnisse in diesem Wahrscheinlichkeitsraum sind alle Folgen der Länge  $n$  aus Nullen und Einsen, d.h. Elemente der Menge  $\{0, 1\}^n$ , und alle Elementarereignisse haben dieselbe Wahrscheinlichkeit. Da es  $2^n$  Elementarereignisse gibt, ist die Wahrscheinlichkeit eines jeden Ereignisses  $A$  gleich  $|A|/2^n$ . Diesen Wahrscheinlichkeitsraum bezeichnen wir mit  $\mathcal{C}_n$ .

Dieser Wahrscheinlichkeitsraum modelliert unter anderem das  $n$ -malige Werfen einer Münze, wenn wir voraussetzen, dass die Münze

„fair“ ist, d.h. dass sie symmetrisch ist und Kopf und Zahl gleich wahrscheinlich sind. Fällt beim  $i$ -ten Wurf Kopf, so schreiben wir eine 1 an die  $i$ -te Stelle der Folge, fällt Zahl, so schreiben wir 0. Ein Beispiel für ein Ereignis ist  $A = \text{„Es fällt genau 10-mal Kopf“}$ , seine Wahrscheinlichkeit ist  $\binom{n}{10}/2^n$ .

**10.2.3 Definition (Eine zufällige Permutation).** Die Ergebnisse in diesem Wahrscheinlichkeitsraum sind alle Permutationen der Menge  $\{1, 2, \dots, n\}$ , und die Wahrscheinlichkeit eines Ereignisses  $A$  ist  $|A|/n!$ . Die Menge aller Permutationen der Menge  $\{1, 2, \dots, n\}$  wird traditionell mit  $S_n$  bezeichnet, und wir nennen den Wahrscheinlichkeitsraum  $\mathcal{S}_n$ .

Dieser Raum ist ein Modell für das Anordnen von  $n$  verschiedenen Elementen in einer zufälligen Reihenfolge, z.B. wenn man ein Kartenspiel gut durchmischt.

**Problem.** Wie groß ist die Wahrscheinlichkeit, dass in einem gut gemischten Bridgespiel das Pik-Ass vor dem Herz-König liegt?

In unserem Modell fragen wir also nach der Wahrscheinlichkeit des Ereignisses  $A = \{\pi \in S_{52} : \pi(1) < \pi(2)\}$ . Natürlich könnten wir hingehen und die Permutationen mit  $\pi(1) < \pi(2)$  zählen, wir können die gesuchte Wahrscheinlichkeit aber auch mit einer einfachen Überlegung herausfinden: Aus Gründen der Symmetrie kann keines der Ereignisse „ $\pi(1) < \pi(2)$ “ und „ $\pi(1) > \pi(2)$ “ wahrscheinlicher sein als das andere, also muss die Wahrscheinlichkeit für beide  $\frac{1}{2}$  sein. Die Wendung „aus Gründen der Symmetrie“ sollten wir aber noch präzisieren: Wir konstruieren eine Bijektion zwischen der Menge  $A$  und der Menge  $A' = \{\pi \in S_{52} : \pi(1) > \pi(2)\}$ , die jeder Permutation  $\pi \in A$  die Permutation  $\pi'$  mit  $\pi'(1) = \pi(2)$ ,  $\pi'(2) = \pi(1)$  und  $\pi'(i) = \pi(i)$  für  $i > 2$  zuordnet. Daher ist  $|A| = |A'|$ , und weil  $A$  und  $A'$  disjunkt sind und zusammen den gesamten Wahrscheinlichkeitsraum überdecken, haben wir  $P(A) = \frac{1}{2}$ .

Das folgende Problem illustriert mit seiner überraschenden Lösung, wie uns die Intuition narren kann.

**Problem.** Wir spielen das folgende Spiel. Unser Gegner hat 100 weiße Karten, und auf jede schreibt er ganz nach seinem Gutdünken eine Zahl. Dann mischt er (oder besser ein unparteiischer Dritter) die Karten und legt den Stapel mit der beschriebenen Seite nach unten auf den Tisch. Nun sind wir an der Reihe. Wir dürfen immer eine Karte von oben wegnehmen und die darauf geschriebene Zahl ansehen, und wir dürfen das Spiel jederzeit beenden. Wir gewinnen, wenn die Zahl auf

der letzten Karte, die wir umgedreht haben, größer ist als die Zahlen auf allen anderen Karten (sowohl den aufgenommenen als auch den noch auf dem Tisch liegenden). Wenn wir gewinnen, bekommen wir 40 Doublezons, verlieren wir, dann zahlen wir 10 Doublezons. Können wir erwarten mit diesem Spiel einen Gewinn zu erzielen?

Auf den ersten Blick scheint dieses Spiel sehr ungünstig für uns zu sein. Dennoch wollen wir einmal die folgende Strategie untersuchen: Wir drehen die ersten 50 Karten um, egal welche Zahlen darauf stehen; wir merken uns die größte Zahl, die wir dabei zu Gesicht bekommen, das sei  $M$ . Dann drehen wir weitere Karten um und stoppen, sobald wir eine Zahl größer oder gleich  $M$  finden. Treffen wir auf keine solche Zahl, dann enden wir mit der letzten Karte.

Wir behaupten, die Wahrscheinlichkeit zu gewinnen ist mit dieser Strategie größer als  $\frac{1}{4}$ . Das bedeutet, wir können erwarten, im Schnitt mindestens eines von vier Spielen zu gewinnen; damit ist unser erwarteter Gewinn in einer genügend langen Serie von Spielen positiv, mindestens etwa  $\frac{1}{4} \cdot 40 - \frac{3}{4} \cdot 10 = 2,50$  Doublezons pro Spiel — zwar kein Vermögen, doch genug für ein Bier. Der Einfachheit halber wollen wir annehmen, dass unser Gegner lauter verschiedene Zahlen auf die Karten schreiben muss (wenn es Sie interessiert, dann können Sie die nötigen Änderungen im Falle beliebiger Zahlen selbst vornehmen). Mit der beschriebenen Strategie gewinnen wir jedenfalls, wenn

- die größte Zahl sich unter den zweiten 50 Karten befindet und
- die zweitgrößte Zahl unter den ersten 50 Karten ist.

Offensichtlich hängt der Ausgang des Spiels mit unserer Strategie allein an der Reihenfolge der Karten und nicht an den konkreten Zahlen, so dass wir uns o.B.d.A. vorstellen dürfen, dass auf den Karten die Zahlen  $1, 2, \dots, 100$  stehen; ihre zufällige Reihenfolge ist damit ein Element aus dem Wahrscheinlichkeitsraum  $S_{100}$ . Uns interessiert das Ereignis  $A = \{\pi \in S_{100}: \pi(100) > 50 \text{ und } \pi(99) \leq 50\}$ . In diesem Zusammenhang ist es geschickt, sich die Permutationen als lineare Ordnungen vorzustellen. Die Position der Zahl 100 kann man auf 50 Arten wählen, die Position der 99 kann unabhängig von der vorigen Wahl auf 50 Arten gewählt werden, die übrigen Zahlen können auf  $98!$  Arten angeordnet werden. Deshalb ist

$$P(A) = \frac{50 \cdot 50 \cdot 98!}{100!} = \frac{50 \cdot 50}{99 \cdot 100} \doteq 0,2525 > \frac{1}{4}.$$

Wir schließen dieses Beispiel mit ein paar Bemerkungen. Das Ereignis  $A$  ist nicht die einzige Situation, in der unsere Strategie erfolgreich ist, deshalb ist die Wahrscheinlichkeit von  $A$  lediglich eine untere Schranke für die Wahrscheinlichkeit zu gewinnen. Die Zahl 50, die unsere Strategie als Schwellenwert einsetzt, maximiert die Wahrscheinlichkeit für das Ereignis  $A$  (nämlich dafür, dass die 99 davor und die 100 danach

kommt). Doch wenn wir weitere Situationen in Betracht ziehen, in denen wir gewinnen, erhalten wir mit einem anderen Schwellenwert eine geringfügig bessere Gewinnerwartung. Das wollen wir nicht weiter im Detail untersuchen; wäre das nicht eine Herausforderung für Sie?

Als Nächstes führen wir das Konzept des „Zufallsgraphen“ ein. Es gibt verschiedene sinnvolle Definitionen, wir wählen hier die einfachste. Ein einfacher, ungerichteter Graph auf der Eckenmenge  $V = \{1, 2, \dots, n\}$  ist eindeutig bestimmt, wenn man für jedes Paar  $\{i, j\} \in \binom{V}{2}$  weiß, ob es eine Kante ist oder nicht. Es gibt deshalb  $2^{\binom{n}{2}}$  Graphen (viele von denen sind natürlich isomorph, doch das soll uns im Moment nicht stören). Einen Zufallsgraphen  $G$  auf der Eckenmenge  $V$  so auszuwählen, dass alle möglichen Graphen die gleiche Wahrscheinlichkeit haben, können wir als das  $\binom{n}{2}$ -malige Werfen einer fairen Münze auffassen: Für jedes Eckpaar werfen wir eine Münze und entscheiden so, ob die beiden Ecken durch eine Kante verbunden sind oder nicht.

**10.2.4 Definition (Ein Zufallsgraph).** Dieser Wahrscheinlichkeitsraum, den wir mit  $\mathcal{G}_n$  bezeichnen, hat als Ergebnismenge  $\Omega$  alle möglichen Graphen auf der Eckenmenge  $\{1, 2, \dots, n\}$ , und zwar alle mit der gleichen Wahrscheinlichkeit  $2^{-\binom{n}{2}}$ .

Interessante Ereignisse im Wahrscheinlichkeitsraum  $\mathcal{G}_n$  sind alle möglichen Grapheneigenschaften wie  $S$  = „der Graph  $G$  ist zusammenhängend“ oder  $B$  = „der Graph  $G$  ist bipartit“. Die exakte Bestimmung solcher Wahrscheinlichkeiten ist oft sehr schwierig, doch in den meisten Fällen wünschen wir nur eine recht grobe Abschätzung. In den beiden genannten Beispielen stellt sich heraus, dass die Wahrscheinlichkeit  $P(S)$  für  $n \rightarrow \infty$  schnell gegen 1 konvergiert, während  $P(B)$  gegen 0 geht. Diese Aussagen fasst man in Worte, indem man sagt, dass „ein Zufallsgraph fast sicher zusammenhängend ist und fast sicher nicht bipartit“. Wir beweisen die zweite dieser Behauptungen; die Vorgehensweise ist typisch für diese Art von Aussagen.

**10.2.5 Hilfssatz.** Ein Zufallsgraph ist fast sicher nicht bipartit, d.h.  $\lim_{n \rightarrow \infty} P(B) = 0$ .

*Beweis.* Wir erinnern uns: Die Eckenmenge  $V$  eines bipartiten Graphen kann derart in zwei Teile  $U$  und  $W$  aufgeteilt werden, dass Kanten ausschließlich zwischen  $U$  und  $W$  verlaufen. Für eine gegebene Teilmenge  $U \subseteq V$  bezeichne  $B_U$  das Ereignis, dass alle Kanten des Zufallsgraphen  $G$  zwischen Ecken aus  $U$  und Ecken aus  $W = V \setminus U$  verlaufen. Ist  $k = |U|$ , dann haben wir  $k(n - k)$  Paare  $\{u, w\}$  mit  $u \in U$  und  $w \in V \setminus U$ , das Ereignis (eine Menge!)  $B_U$  besteht aus  $2^{k(n-k)}$  Gra-

phen. Deshalb ist  $P(B_U) = 2^{k(n-k)-\binom{n}{2}}$ . Es ist nicht schwer zu prüfen, dass die Funktion  $k \mapsto k(n-k)$  ihr Maximum bei  $k = \frac{n}{2}$  annimmt und dass der Wert dieses Maximums  $n^2/4$  ist; daher ist  $k(n-k) \leq n^2/4$  für alle  $k$ . Damit gilt für jedes  $U$ ,

$$P(B_U) \leq 2^{n^2/4 - \binom{n}{2}} = 2^{-n(n-2)/4}.$$

Jeder bipartite Graph gehört zu einem  $B_U$  (bei geeigneter Wahl der Menge  $U$ ). Für verschiedene  $U$  müssen die Ereignisse  $B_U$  nicht disjunkt sein, aber die Wahrscheinlichkeit einer Vereinigung von Ereignissen ist in jedem Fall stets höchstens die Summe der Einzelwahrscheinlichkeiten. Somit ist

$$P(B) \leq \sum_{U \subseteq V} P(B_U) \leq 2^n \cdot 2^{-n(n-2)/4} = 2^{-n(n-6)/4} \rightarrow 0.$$

□

Bei diesem Problem waren wir an einer bestimmten qualitativen Eigenschaft eines „großen“ Zufallsgraphen interessiert. Einer ähnlichen Situation begegnet man in manchen Gebieten der Physik (etwa Thermodynamik oder Festkörperphysik), wo makroskopische Eigenschaften von Objekten studiert werden, die aus unzählig vielen mikroskopischen Teilchen bestehen. Die Theorien fußen auf der Hypothese, dass sich die einzelnen Teilchen in gewissem Sinne zufällig bewegen, und dass die makroskopischen Eigenschaften Resultat ihrer zufälligen Wechselwirkungen sind. Auch bei der Untersuchung des Ferromagnetismus und anderer Eigenschaften von Festkörpern werden Methoden verwendet, die denen für Zufallsgraphen ähneln. Sogar in den Sozialwissenschaften geht man manche Probleme auf analoge Weise an, etwa wenn man die Ausbreitung von Epidemien modelliert.

Definition 10.2.4 ist so formuliert, dass alle Graphen die gleiche Wahrscheinlichkeit haben, indem nämlich die Kantenwahrscheinlichkeit  $\frac{1}{2}$  ist. Für die meisten interessanten Probleme und Anwendungen wählt man die Kantenwahrscheinlichkeit als einen Parameter  $p$ , der im Allgemeinen von  $\frac{1}{2}$  verschieden ist. Konkret bedeutet das, dass ein Zufallsgraph wie bisher durch  $\binom{n}{2}$ -maliges Werfen einer Münze konstruiert wird, ein Wurf für jedes Eckenpaar (bei Kopf Kante, bei Zahl nicht), dass die Münze jedoch nicht „fair“, d.h. nicht symmetrisch ist, sondern mit Wahrscheinlichkeit  $p$  Kopf zeigt und mit Wahrscheinlichkeit  $1-p$  Zahl. Oft untersucht man die Eigenschaften von Zufallsgraphen in Abhängigkeit von der Zahl  $p$ . Ein Beispiel: Wenn wir  $p$  allmählich von 0 auf 1 erhöhen, ab welchem Wert ist der Zufallsgraph typischerweise zusammenhängend? Und wieder ist das Konzept nicht allzu weit von physikalischen Fragen wie dieser entfernt: Bei welcher Temperatur beginnt ein gegebener Kristall zu schmelzen?

**Unabhängige Ereignisse.** Nun fehlt uns nur noch ein weiterer Grundbegriff: Zwei Ereignisse  $A, B$  in einem Wahrscheinlichkeitsraum  $(\Omega, P)$  heißen *unabhängig*, wenn gilt:

$$P(A \cap B) = P(A)P(B).$$

Unabhängigkeit bedeutet: Wenn  $\Omega$  in zwei Teile geteilt wird, in  $A$  und sein Komplement, dann schneidet das Ereignis  $B$  beide Teile im gleichen Verhältnis. Mit anderen Worten, wollte man ein zufälliges Ergebnis  $\omega$  nicht aus ganz  $\Omega$  sondern aus den Ergebnissen in  $A$  ziehen, dann wäre die Wahrscheinlichkeit, dass  $\omega \in B$  ist, genau gleich  $P(B)$  (sofern  $P(A) \neq 0$ ).

Unabhängigkeit bedeutet *nicht*, dass  $A \cap B = \emptyset$  ist, wie man vielleicht denken könnte.

Allermeistens begegnen uns unabhängige Ereignisse, wenn  $\Omega$  die möglichen Ausgänge eines „zusammengesetzten“ Experiments modelliert, das tatsächlich aus zwei Experimenten besteht. Die Elemente aus  $\Omega$ , d.h. die Ergebnisse, können dann als geordnete Paare aufgefasst werden. Nehmen wir an, dass die Durchführung oder der Ausgang des ersten der zwei Experimente in keinem Falle den Ausgang des zweiten Experiments beeinflussen kann, und dass ebenso wenig das zweite Experiment das erste beeinflussen kann (etwa weil die beiden Experimente durch eine dicke Mauer voneinander abgeschottet sind). Ist  $A \subseteq \Omega$  ein Ereignis, das nur vom Ausgang des ersten Experiments abhängt (d.h. wenn wir den Ausgang des ersten Experiments kennen, dann können wir schon entscheiden, ob  $A$  eingetreten ist oder nicht), und ist analog  $B$  ein Ereignis, das nur vom Ausgang des zweiten Experiments abhängt, dann sind die Ereignisse  $A$  und  $B$  unabhängig.

Im Wahrscheinlichkeitsraum  $\mathcal{C}_n$  (zufällige 0-1-Folge der Länge  $n$ ) trifft man häufig auf diese Situation. Hier liegt ja ein zusammengefügtes Experiment vor, das aus  $n$  aufeinander folgenden Münzwürfen besteht, und wir gehen davon aus, dass sie sich gegenseitig in keiner Weise beeinflussen; die Münze verbiegt nicht und wird auch nicht nach dem ersten Wurf gestohlen. Hängt ein Ereignis  $A$  also nur von den ersten fünf Würfen ab (z.B. „bei den ersten fünf Würfen ist mindestens dreimal Kopf gefallen“, und hängt ein Ereignis  $B$  nur vom sechsten und den folgenden Würfen ab (z.B. „bei den Würfen 6 bis 10 ist ungerade oft Kopf gefallen“), so sind diese Ereignisse unabhängig. Entsprechend werden im Wahrscheinlichkeitsraum

$\mathcal{G}_n$  (Zufallsgraph) die Kanten unabhängig voneinander gewählt, also sind beispielsweise die Ereignisse „der Graph  $G$  hat mindestens ein Dreieck auf den Ecken  $1, 2, \dots, 10$ “ und „der Graph  $G$  enthält einen Kreis ungerader Länge, dessen Ecken alle aus  $11, 12, \dots, 20$  sind“ unabhängig.

Nicht immer sind die Verhältnisse so klar. Eine subtilere Situation demonstrieren wir im Wahrscheinlichkeitsraum  $\mathcal{S}_n$  (zufällige Permutation). Die Ereignisse  $A = \{\pi(1) = 1\}$  und  $B = \{\pi(2) = 1\}$  sind offensichtlich *nicht* unabhängig, weil  $P(A) > 0$  und  $P(B) > 0$ , aber  $A \cap B = \emptyset$  und somit  $P(A \cap B) = 0$ . Definieren wir ein weiteres Ereignis  $C = \{\pi(2) = 2\}$ , sieht man ebenso leicht, dass auch  $B$  und  $C$  nicht unabhängig sind. Vielleicht ist es aber nicht mehr so offensichtlich, dass nicht einmal  $A$  und  $C$  unabhängig sind: es ist  $P(A) = P(C) = \frac{1}{n}$ , aber  $P(A \cap C) = \frac{1}{n(n-1)} \neq P(A)P(C)$ . Intuitiv liegt das daran, dass wir einen der  $n$  möglichen Werte für  $\pi(2)$  ausschließen können, wenn wir wissen, dass  $A$  eingetreten ist (d.h.  $\pi(1) = 1$ ), und dass deshalb  $\pi(2) = 2$  eine geringfügig größere Chance hat. Jedoch sind die Ereignisse  $A$  und  $D = \{\pi(2) < \pi(3)\}$  unabhängig, wie man durch Berechnen der entsprechenden Wahrscheinlichkeiten bestätigt. Auf solche Feinheiten sollte man gut Acht geben. Die wohl häufigste Fehlerquelle in probabilistischen Beweisen ist, Ereignisse als unabhängig anzunehmen, die es in Wahrheit nicht sind.

Den Begriff der Unabhängigkeit kann man auf eine größere Anzahl von Ereignissen  $A_1, A_2, \dots, A_n$  erweitern.

**10.2.6 Definition.** Ereignisse  $A_1, A_2, \dots, A_n \subseteq \Omega$  heißen unabhängig, wenn für jede Menge  $I \subseteq \{1, 2, \dots, n\}$  von Indizes gilt, dass

$$P\left(\bigcap_{i \in I} A_i\right) = \prod_{i \in I} P(A_i).$$

Insbesondere verlangt diese Definition, dass je zwei dieser Ereignisse unabhängig sind, aber wir sollten die Warnung aussprechen, dass aus der paarweisen Unabhängigkeit der einzelnen Ereignisse nicht die Unabhängigkeit aller Ereignisse folgt!

In den Wahrscheinlichkeitsräumen  $\mathcal{C}_n$  (zufällige 0-1-Folge) und  $\mathcal{G}_n$  (Zufallsgraph) gibt es typische Situationen mit vielen unabhängigen Ereignissen. Definieren wir Ereignisse  $A_i$  ( $i = 1, \dots, n$ ) im Wahrscheinlichkeitsraum  $\mathcal{C}_n$ , die aus allen Folgen mit einer 1 an der  $i$ -

ten Position bestehen, dann sind die Ereignisse  $A_1, A_2, \dots, A_n$  unabhängig (der Beweis ist nicht schwer).

Sehr oft werden in wahrscheinlichkeitstheoretischen Berechnungen und Beweisen die verwendeten Wahrscheinlichkeitsräume nicht explizit genannt; man arbeitet einfach mit dem passenden, ohne es zu erwähnen. Gerade deshalb ist es wichtig, dass Ihnen die Grundbegriffe klar sind.

Wir schließen diesen Abschnitt mit einem hübschen Beweis ab (einem der ersten Beweise, wo diese Methode verwendet wurde).

Wir betrachten ein Turnier mit  $n$  Spielern, etwa ein Tischtennisturnier, bei dem jeder Spieler gegen jeden anderen antritt; jedes Match hat einen Gewinner. Wenn die Spielstärken der einzelnen Spieler sehr unterschiedlich sind, dann werden wir erwarten, dass der beste Spieler alle anderen schlägt, dass der zweitbeste alle bis auf den besten schlägt, und so weiter, so dass das Turnier die Rangfolge der Spieler unzweideutig widerspiegelt. Ein Turnier, bei dem sich die Spielstärken nicht so stark unterscheiden, wird wahrscheinlich nicht so eindeutig ausgehen. Denn natürlich kann es vorkommen, dass jeder Spieler von einem anderen geschlagen wird. Und was ein richtiger Mathematiker ist, muss zwangsläufig nach der folgenden Verallgemeinerung fragen:

**Problem.** Kann es sein, dass in einem Turnier je zwei Spieler von einem dritten geschlagen werden? Und allgemeiner, für welche Zahlen  $k$  kann es in einem Turnier passieren, dass es zu je  $k$  Spielern einen weiteren gibt, der sie alle schlägt?

Für  $k = 2$  lässt sich ein solches Turnier noch „von Hand“ konstruieren. Doch für größere Werte von  $k$  ist die Konstruktion solcher Turniere schwierig, und man hat lange Zeit vergeblich nach einer Lösung gesucht. Mit Hilfe von Wahrscheinlichkeiten können wir die Existenz eines solchen Turniers (mit vielen Spielern) verhältnismäßig einfach beweisen. Der Einfachheit halber führen wir den Beweis nur für  $k = 3$ , gesucht ist also ein Turnierablauf, bei dem je drei Spieler  $x, y, z$  von einem weiteren Spieler  $w$  geschlagen werden.

Betrachten wir ein zufälliges Turnier, bei dem der Ausgang jedes Spiels durch Los bestimmt wird, etwa durch das Werfen einer fairen Münze. Wir fixieren drei Spieler  $\{x, y, z\}$ . Die Wahrscheinlichkeit, dass ein anderer Spieler  $w$  alle drei besiegt, ist  $2^{-3} = \frac{1}{8}$ . Folglich

ist die Wahrscheinlichkeit, dass  $w$  von mindestens einem der drei besiegt wird, gleich  $\frac{7}{8}$ . Wie groß ist die Wahrscheinlichkeit, dass jeder der  $n - 3$  Spieler, welche die Rolle von  $w$  übernehmen können, gegen mindestens einen von  $x, y, z$  verliert? Für verschiedene Spieler  $w$  sind die Resultate der Spiele gegen  $x, y, z$  paarweise unabhängig voneinander, somit ist die gesuchte Wahrscheinlichkeit  $(\frac{7}{8})^{n-3}$ . Das Tripel  $\{x, y, z\}$  kann auf  $\binom{n}{3}$  Arten gewählt werden, und darum ist die Wahrscheinlichkeit, dass für mindestens eines der Tripel  $\{x, y, z\}$  kein weiterer Spieler sowohl  $x$  als auch  $y$  und  $z$  schlägt, höchstens  $\binom{n}{3}(\frac{7}{8})^{n-3}$ . Mit einem Taschenrechner finden wir heraus, dass diese Wahrscheinlichkeit für  $n \geq 91$  kleiner ist als 1. Deshalb gibt es mindestens einen möglichen Verlauf eines Turniers mit 91 Spielern, bei dem je drei Spieler von einem vierten geschlagen werden. Dies ist die gewünschte Eigenschaft.  $\square$

## Aufgaben

1. Beweisen Sie, dass in einem (endlichen) Wahrscheinlichkeitsraum für je zwei Ereignisse  $A, B$  gilt:  $P(A \cup B) \leq P(A) + P(B)$ . Verallgemeinern Sie das auf den Fall von  $n$  Ereignissen.
2. (Probabilistische Formulierung des Prinzips der Inklusion–Exklusion)
  - (a) Formulieren Sie das Prinzip der Inklusion–Exklusion (Satz 3.7.2) in der Sprache der Wahrscheinlichkeitstheorie: Es seien  $A_1, A_2, \dots, A_n$  Ereignisse in einem endlichen Wahrscheinlichkeitsraum. Nehmen Sie an, dass in diesem Wahrscheinlichkeitsraum alle Elementarereignisse gleich wahrscheinlich sind. Drücken Sie die Wahrscheinlichkeit  $P(A_1 \cup \dots \cup A_n)$  mit den Wahrscheinlichkeiten der verschiedenen Schnitte der  $A_i$  aus.
  - (b) Zeigen Sie, dass die Formel aus (a) für Ereignisse in beliebigen endlichen Wahrscheinlichkeitsräumen gilt. (Nicht einmal die Endlichkeitsbedingung ist wirklich notwendig.)
3. Beweisen Sie, dass ein Zufallsgraph im Sinne von Definition 10.2.4 fast sicher ein Dreieck enthält. (Daraus folgt nochmals Hilfssatz 10.2.5).
4. \*Zeigen Sie, dass ein Zufallsgraph fast sicher zusammenhängend ist.
5. Geben Sie ein Beispiel für drei Ereignisse in einem Wahrscheinlichkeitsraum, von denen je zwei unabhängig sind, die aber nicht alle drei unabhängig sind.
6. Zeigen Sie, dass aus der Unabhängigkeit zweier Ereignisse  $A, B$  die Unabhängigkeit auch ihrer Komplemente  $\Omega \setminus A$  und  $\Omega \setminus B$  folgt.

7. Sei  $(\Omega, P)$  ein endlicher Wahrscheinlichkeitsraum, in dem alle Elementarereignisse die gleiche Wahrscheinlichkeit haben. Zeigen Sie: Ist  $|\Omega|$  eine Primzahl, dann können (außer  $\emptyset$  und  $\Omega$ ) keine zwei Ereignisse unabhängig sein.
8. (a) Zeigen Sie, dass in dem Wahrscheinlichkeitsraum  $\mathcal{C}_n$  die im auf Definition 10.2.6 folgenden Text definierten Ereignisse  $A_1, A_2, \dots, A_n$  tatsächlich unabhängig sind.  
 (b) \*Sei  $(\Omega, P)$  ein endlicher Wahrscheinlichkeitsraum, in dem es  $n$  unabhängige Ereignisse  $A_1, A_2, \dots, A_n \subseteq \Omega$  gibt mit der Eigenschaft  $0 < P(A_i) < 1$  für jedes  $i$ . Zeigen Sie, dass dann  $|\Omega| \geq 2^n$  ist.
9. Nehmen Sie der Einfachheit halber an, dass die Wahrscheinlichkeiten, einen Jungen oder ein Mädchen zu bekommen, gleich sind (auch wenn es nicht ganz stimmt). Wenn Sie von einem Ehepaar wissen, dass sie genau zwei Kinder haben, von denen mindestens einer ein Junge ist, wie groß ist dann die Wahrscheinlichkeit, dass sie zwei Jungen haben?
10. (a) <sup>Inf</sup> Schreiben Sie ein Programm, das einen Zufallsgraphen mit einer vorgegebenen Kantenwahrscheinlichkeit  $p$  erzeugt und seine Zusammenhangskomponenten bestimmt. Wählen Sie eine feste Eckenanzahl  $n$  und bestimmen Sie experimentell, bei welchem Wert für  $p$  der Zufallsgraph zusammenhängend wird und bei welchem Wert für  $p$  er beginnt, eine „riesige Komponente“ zu haben (das könnte man z.B. als eine Komponente mit mindestens  $\frac{n}{2}$  Ecken definieren).  
 (b) \*\*Können Sie Ihre Ergebnisse aus (a) theoretisch erklären? Vielleicht möchten Sie im Buch [13] nachschlagen.

## 10.3 Zufallsvariable und Erwartungswert

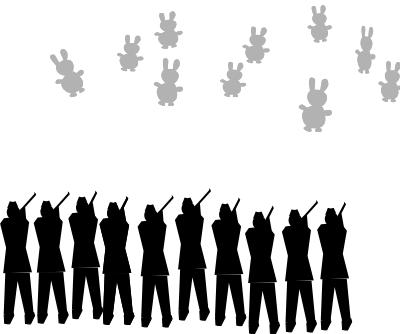
**10.3.1 Definition.** Sei  $(\Omega, P)$  ein endlicher Wahrscheinlichkeitsraum. Eine beliebige Abbildung  $f: \Omega \rightarrow \mathbb{R}$  bezeichnen wir als Zufallsvariable auf  $\Omega$ .

Eine Zufallsvariable  $f$  ordnet also jedem Ergebnis  $\omega \in \Omega$  eine reelle Zahl  $f(\omega)$  zu. Wir sehen uns ein paar Beispiele an.

**10.3.2 Beispiel (Anzahl der Einsen).** Im Wahrscheinlichkeitsraum  $\mathcal{C}_n$  aller 0-1-Folgen der Länge  $n$  können wir eine Zufallsvariable  $f_1$  wie folgt definieren: Für eine Folge  $s$  ist  $f_1(s)$  die Anzahl der Einsen in  $s$ .

**10.3.3 Beispiel (Anzahl der nicht geschossenen Hasen).** Von  $n$  Jägern sucht sich jeder zufällig einen aus einer Gruppe von  $n$  Hasen aus, zielt mit seinem Gewehr auf ihn, und dann drücken alle Jäger gleichzeitig ab. (Das ist kein besonders lustiges Szenario, aber

es kommt zuweilen genau so vor.) Eine Zufallsvariable  $f_2$  ist die Anzahl der Hasen, die nicht geschossen werden (wir nehmen an, dass alle Jäger treffen). Formal ist der Wahrscheinlichkeitsraum hier die Menge aller Abbildungen  $\alpha: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ , die alle die gleiche Wahrscheinlichkeit  $n^{-n}$  haben, und  $f_2(\alpha) = |\{1, 2, \dots, n\} \setminus \alpha(\{1, 2, \dots, n\})|$ .



**10.3.4 Beispiel (Anzahl der Linksmaxima).** Auf dem Wahrscheinlichkeitsraum  $S_n$  aller Permutationen der Menge  $\{1, 2, \dots, n\}$  definieren wir eine Zufallsvariable  $f_3$ :  $f_3(\pi)$  ist die Anzahl der *Linksmaxima* einer Permutation  $\pi$ , d.h. die Anzahl der  $i$ , für die  $\pi(i) > \pi(j)$  für alle  $j < i$ . Es findet ein Wettkampf im Weitsprung statt. Unsere Athleten haben eine sehr stabile Kampfkraft, sie springen die gleiche Weite, und diese Sprungweiten sind für je zwei von ihnen verschieden (diese zugegebenermaßen unrealistischen Annahmen kann man auf ein annehmbares Maß reduzieren). In einer ersten Runde springen  $n$  Wettkämpfer in zufälliger Reihenfolge. Bezeichnen wir mit  $f_3$ , wie oft sich im Verlauf dieser Runde die Bestweite ändert, so ist  $f_3$  eine Zufallsvariable.

**10.3.5 Beispiel (Komplexität eines Sortieralgorithmus).** Diese Zufallsvariable ist etwas komplizierter. Sei  $A$  ein Sortieralgorithmus, der als Eingabe ein  $n$ -Tupel  $(x_1, x_2, \dots, x_n)$  von Zahlen akzeptiert und der als Ausgabe die gleichen Zahlen in aufsteigender Reihenfolge liefert. Angenommen, die Anzahl der Schritte, die  $A$  benötigt, hängt ausschließlich von der Reihenfolge ab, in der die Zahlen eingegeben werden (so dass wir uns die Eingabe als eine Permutation  $\pi$  auf der Menge  $\{1, 2, \dots, n\}$  vorstellen dürfen). Viele

Algorithmen, die zum Sortieren nur paarweise Vergleiche der eingegebenen Zahlen verwenden, erfüllen diese Bedingung; einige davon werden in der Praxis häufig eingesetzt. Wir definieren eine Zufallsvariable  $f_4$  auf dem Wahrscheinlichkeitsraum  $\mathcal{S}_n$ : Sei  $f_4(\pi)$  die Anzahl der Schritte, die Algorithmus  $A$  bei der Eingabefolge  $(\pi(1), \pi(2), \dots, \pi(n))$  benötigt.

**10.3.6 Definition.** Sei  $(\Omega, P)$  ein endlicher Wahrscheinlichkeitsraum und  $f$  eine Zufallsvariable darauf. Der Erwartungswert von  $f$  ist eine reelle Zahl, bezeichnet mit  $\mathbf{E}[f]$  und definiert durch die Formel

$$\mathbf{E}[f] = \sum_{\omega \in \Omega} P(\{\omega\})f(\omega).$$

Haben insbesondere alle Elementarereignisse  $\omega \in \Omega$  die gleiche Wahrscheinlichkeit (was in fast all unseren Beispielen der Fall ist), so ist der Erwartungswert von  $f$  einfach das arithmetische Mittel der Werte, die  $f$  auf den verschiedenen Elementen aus  $\Omega$  annimmt:

$$\mathbf{E}[f] = \frac{1}{|\Omega|} \sum_{\omega \in \Omega} f(\omega).$$

Man kann sich den Erwartungswert so vorstellen: Wenn wir sehr oft ein zufälliges Ergebnis  $\omega$  aus  $\Omega$  ziehen, dann wird der Durchschnitt von  $f$  über die zufällig gewählten  $\omega$  gegen  $\mathbf{E}[f]$  konvergieren.

**Fortsetzung von Beispiel 10.3.2 (Anzahl der Einsen).** Zur Illustration berechnen wir den Erwartungswert der Zufallsvariable  $f_1$ , der Anzahl der Einsen in einer zufälligen 0-1-Folge der Länge  $n$ . Die Zufallsvariable  $f_1$  nimmt den Wert 0 für genau eine Folge aus  $\mathcal{C}_n$  an (alles Nullen), den Wert 1 für  $n$  Folgen,  $\dots$ , den Wert  $k$  für  $\binom{n}{k}$  Folgen. Deshalb ist

$$\begin{aligned} \mathbf{E}[f_1] &= \frac{1}{2^n} \sum_{s \in \{0,1\}^n} f_1(s) \\ &= \frac{1}{2^n} \sum_{k=0}^n \binom{n}{k} k. \end{aligned}$$

In Beispiel 12.1.1 werden wir berechnen, dass die letzte Summe in der Gleichung gleich  $n2^{n-1}$  ist, somit ist  $\mathbf{E}[f_1] = \frac{n}{2}$ . Genau das sagt uns aber auch unsere Intuition: Denn wir erwarten natürlich, dass bei  $n$  Münzwürfen ungefähr  $\frac{n}{2}$  mal Kopf fällt.

Den Wert von  $\mathbf{E}[f_1]$  können wir auch auf einfachere Art bestimmen. Der Trick ist, zu jeder Folge  $s \in \mathcal{C}_n$  die Folge  $\bar{s}$  zu betrachten, die aus  $s$  entsteht, wenn wir alle Nullen durch Einsen ersetzen und alle Einsen durch Nullen. Wir haben dann  $f_1(s) + f_1(\bar{s}) = n$ , also

$$\begin{aligned}\mathbf{E}[f_1] &= \frac{1}{2^n} \sum_{s \in \{0,1\}^n} f_1(s) = \frac{1}{2^n \cdot 2} \sum_{s \in \{0,1\}^n} (f_1(s) + f_1(\bar{s})) \\ &= 2^{-n-1} 2^n n = \frac{n}{2}.\end{aligned}$$

Nun beschreiben wir eine Methode, die uns die Berechnung des Erwartungswertes oft wesentlich vereinfacht (wir haben gesehen, dass die direkte Anwendung der Definition schon in einfachen Fällen ziemlich aufwändig sein kann). Wir benötigen eine Definition und einen einfachen Satz.

**10.3.7 Definition.** Sei  $A \subseteq \Omega$  ein Ereignis in einem Wahrscheinlichkeitsraum  $(\Omega, P)$ . Unter der Indikatorfunktion des Ereignisses  $A$  verstehen wir die Zufallsvariable  $I_A: \Omega \rightarrow \{0, 1\}$ , die wie folgt definiert ist:

$$I_A(\omega) = \begin{cases} 1 & \text{wenn } \omega \in A \\ 0 & \text{wenn } \omega \notin A. \end{cases}$$

(„Indikatorfunktion“ ist also nur ein anderer Name für die charakteristische Funktion von  $A$ .)

**10.3.8 Beobachtung.** Für jedes Ereignis  $A$  ist  $\mathbf{E}[I_A] = P(A)$ .

*Beweis.* Nach der Definition des Erwartungswertes erhalten wir

$$\mathbf{E}[I_A] = \sum_{\omega \in \Omega} I_A(\omega) P(\{\omega\}) = \sum_{\omega \in A} P(\{\omega\}) = P(A).$$

□

Das nun folgende Resultat verdient kaum, ein Satz genannt zu werden, weil sein Beweis (den wir Ihnen überlassen) unmittelbar aus der Definition folgt. Doch im Folgenden wird uns diese Aussage von großem Nutzen sein.

**10.3.9 Satz (Linearität des Erwartungswertes).** Seien  $f, g$  beliebige Zufallsvariablen auf einem endlichen Wahrscheinlichkeitsraum  $(\Omega, P)$ , und sei  $\alpha$  eine reelle Zahl. Dann gelten  $\mathbf{E}[\alpha f] = \alpha \mathbf{E}[f]$  und  $\mathbf{E}[f + g] = \mathbf{E}[f] + \mathbf{E}[g]$ . □

Zu betonen ist, dass  $f$  und  $g$  völlig beliebig sein dürfen, sie brauchen nicht unabhängig zu sein oder irgendwie sonst zusammenzuhängen. Und eine Warnung sollten wir aussprechen: Diese angenehme Eigenschaft des Erwartungswertes gilt *ausschließlich* beim Addieren zweier Zufallsvariablen und bei der Multiplikation mit einer Konstanten. Z.B. gilt im Allgemeinen nicht  $\mathbf{E}[fg] = \mathbf{E}[f]\mathbf{E}[g]$ ! Weiter geht es mit einigen Beispielen, wie nützlich 10.3.7–10.3.9 sind.

**Weitere Fortsetzung von Beispiel 10.3.2 (Anzahl der Einsen).** Wir berechnen  $\mathbf{E}[f_1]$ , die durchschnittliche Anzahl der Einsen, nun auf die vielleicht eleganteste Art. Es sei  $A_i$  das Ereignis „beim  $i$ -ten Wurf fällt Kopf“, also die Menge aller Folgen der Länge  $n$  mit einer 1 an der  $i$ -ten Stelle. Offensichtlich ist  $P(A_i) = \frac{1}{2}$  für alle  $i$ . Für jede Folge  $s \in \{0, 1\}^n$  gilt  $f_1(s) = I_{A_1}(s) + I_{A_2}(s) + \dots + I_{A_n}(s)$  (eine ziemlich komplizierte Art, eine sehr einfache Aussage aufzuschreiben). Aus der Linearität des Erwartungswertes erhalten wir mit Beobachtung 10.3.8

$$\begin{aligned}\mathbf{E}[f_1] &= \mathbf{E}[I_{A_1}] + \mathbf{E}[I_{A_2}] + \dots + \mathbf{E}[I_{A_n}] \\ &= P(A_1) + P(A_2) + \dots + P(A_n) = \frac{n}{2}.\end{aligned}$$

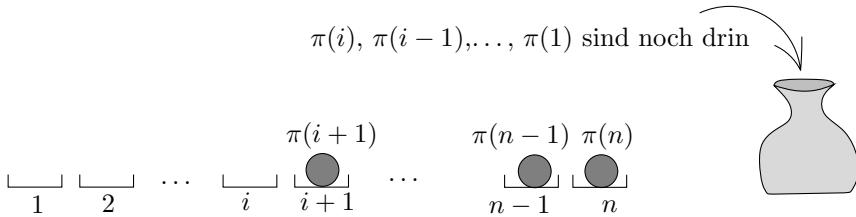
□

**Fortsetzung von Beispiel 10.3.3 (Nicht geschossene Hasen).** Wir wollen  $\mathbf{E}[f_2]$  bestimmen, die erwartete Anzahl der nicht geschossenen Hasen. Diesmal sei  $A_i$  das Ereignis „der  $i$ -te Hase wird nicht geschossen“; formal ist  $A_i$  die Menge aller Abbildungen  $\alpha$ , die kein Element auf  $i$  abbilden. Die Wahrscheinlichkeit, dass der  $j$ -te Jäger den  $i$ -ten Hasen schießt, ist  $\frac{1}{n}$ , und weil die Jäger ihre Hasen unabhängig voneinander wählen, haben wir  $P(A_i) = (1 - 1/n)^n$ . Die weitere Rechnung ist wie im vorigen Beispiel:

$$\mathbf{E}[f_2] = \sum_{i=1}^n \mathbf{E}[I_{A_i}] = \sum_{i=1}^n P(A_i) = \left(1 - \frac{1}{n}\right)^n n \approx \frac{n}{e}$$

(denn  $(1 - 1/n)^n$  konvergiert für  $n \rightarrow \infty$  gegen  $e^{-1}$ ; siehe Aufgabe 3.5.2). Im Schnitt überleben etwa 37% der Hasen. □

**Fortsetzung von Beispiel 10.3.4 (Anzahl der Linksmaxima).** Wir werden nun  $\mathbf{E}[f_3]$  bestimmen, die erwartete Anzahl von Linksmaxima einer zufälligen Permutation. Wir definieren  $A_i$  als das Ereignis „ $i$  ist Linksmaximum von  $\pi$ “, formal:  $A_i = \{\pi \in S_n : \pi(i) >$



**Abb. 10.2** Eine Methode, eine zufällige Permutation zu erzeugen.

$\pi(j)$  für  $j = 1, 2, \dots, i - 1\}$ . Wir behaupten, dass  $P(A_i) = \frac{1}{i}$  ist. Das leitet man wohl am intuitivsten her, indem man sich vorstellt, dass die zufällige Permutation  $\pi$  mit der folgenden Methode erzeugt wird. Wir haben einen Sack, der die Zahlen  $1, 2, \dots, n$  enthält. Wir ziehen daraus zufällig eine Zahl und erklären sie zu  $\pi(n)$ . Dann ziehen wir eine weitere zufällige Zahl, die  $\pi(n-1)$  sein soll, usw., wie in Abb. 10.2 angedeutet. Der Wert von  $\pi(i)$  wird in dem Moment bestimmt, zu dem der Sack genau  $i$  Zahlen enthält. Die Wahrscheinlichkeit, dass wir die größte dieser  $i$  Zahlen zu  $\pi(i)$  machen (das ist gerade das Ereignis  $A_i$ ), ist also  $\frac{1}{i}$ . Das weitere Vorgehen ist wieder das Gleiche wie in den vorangegangenen Beispielen:

$$\mathbf{E}[f_3] = \sum_{i=1}^n \mathbf{E}[I_{A_i}] = \sum_{i=1}^n P(A_i) = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}.$$

Der Wert der Summe auf der rechten Seite ist ungefähr  $\ln n$ ; siehe Abschnitt 3.4.  $\square$

## Aufgaben

1. Zeigen Sie anhand von Beispielen, dass für beliebige Zufallsvariablen  $f$  und  $g$  keine der folgenden Gleichungen erfüllt sein muss:  $\mathbf{E}[fg] = \mathbf{E}[f]\mathbf{E}[g]$ ,  $\mathbf{E}[f^2] = \mathbf{E}[f]^2$ ,  $\mathbf{E}[1/f] = 1/\mathbf{E}[f]$ .
2. Beweisen Sie, dass  $\mathbf{E}[f^2] \geq \mathbf{E}[f]^2$  für jede Zufallsvariable  $f$  gilt.
3. Sei  $f(\pi)$  die Anzahl der Fixpunkte einer Permutation  $\pi$  (siehe Abschnitt 3.8). Berechnen Sie  $\mathbf{E}[f]$  für eine zufällige Permutation  $\pi$  im Raum  $\mathcal{S}_n$ .
4. Sei  $\pi$  eine zufällige Permutation auf der Menge  $\{1, 2, \dots, n\}$ .
  - (a) \*Bestimmen Sie die erwartete Länge desjenigen Zyklus in  $\pi$ , der die Zahl 1 enthält (für die Definition eines Zyklus siehe Abschnitt 3.2).

- (b) \*Bestimmen Sie die erwartete Anzahl der Zyklen von  $\pi$ .
5. An jedem Wochentag nimmt Student X. den Bus zur Universität, sobald er aufgewacht ist; das geschieht zu einer zufälligen Tageszeit (24 Stunden). Nach seinem Tagebuch wartet er durchschnittlich 30 Minuten auf den Bus. Die Busgesellschaft behauptet jedoch, dass der durchschnittliche Abstand zweier Busse über den Tag verteilt (24 Stunden) 15 Minuten beträgt. Können Sie einen Fahrplan konstruieren, so dass beide Aussagen zutreffen?
6. \*Wir werfen  $n$  Mal eine faire Münze. Was ist die erwartete Anzahl von „Serien“? Eine Serie besteht aus aufeinanderfolgenden Würfen mit dem gleichen Ergebnis. Die Wurffolge KKKZZKZK hat zum Beispiel fünf Serien.
7. (Markov–Ungleichung) Sei  $X$  eine Zufallsvariable, die keine negativen Werte annimmt. Sei  $\mu = \mathbf{E}[X]$  ihr Erwartungswert, und sei  $t \geq 1$  eine reelle Zahl. Beweisen Sie, dass die Wahrscheinlichkeit dafür, dass  $X$  einen Wert  $\geq t\mu$  annimmt, höchstens  $\frac{1}{t}$  ist; als Formel:

$$P(\{\omega \in \Omega : X(\omega) \geq t\mu\}) \leq \frac{1}{t}.$$

(Dies ist eine einfache, recht wichtige Ungleichung. Man braucht sie oft um zu zeigen, dass eine betrachtete Größe nur mit vernachlässigbarer Wahrscheinlichkeit sehr groß wird.)

8. (a) Was ist die erwartete Anzahl nicht geschossener Hasen in Beispiel 10.3.3, wenn wir  $m$  Hasen und  $n$  Jäger haben?
- (b) \*Zeigen Sie unter Verwendung von Aufgabe 7 und geeigneter Abschätzungen, dass im Falle  $n > m(\ln m + 5)$  mit Wahrscheinlichkeit mindestens 0,99 kein Hase davonkommt. (Anders ausgedrückt, die meisten Abbildungen aus einer  $n$ -Menge in eine  $m$ -Menge sind surjektiv.)
- (c) \*Lösen Sie Teil (b) noch einmal anders: Erinnern Sie sich, wie wir die Formel für die Anzahl surjektiver Abbildungen mittels Inklusion–Exklusion hergeleitet haben (Aufgabe 3.8.7); verwenden Sie dies und die Bonferroni–Ungleichung (3.18) mit  $q = 1$ .

## 10.4 Einige Anwendungen

In diesem Abschnitt haben wir Beispiele für den Gebrauch der probabilistischen Methode, insbesondere auch der Linearität des Erwartungswertes, zusammengetragen. Es sind keine Standardbeispiele, vielmehr kleine mathematische Schmuckstücke.

**Existenz großer bipartiter Untergraphen.** Gegeben sei ein Graph  $G = (V, E)$ , und wir möchten seine Eckenmenge derart in

zwei Teile partitionieren, dass möglichst viele Kanten zwischen den beiden Teilen verlaufen. Oft wünschen wir darüber hinaus, dass die beiden Teile annähernd gleich groß sind. Der folgende Satz zeigt, dass wir immer erreichen können, dass mindestens die Hälfte der Kanten zwischen den beiden Teilen verläuft, und dass die beiden Teile zudem gleich groß gewählt werden können (wenn die Eckenzahl gerade ist).

**10.4.1 Satz.** *Sei  $G$  ein Graph mit  $2n$ , also gerade vielen, Ecken und mit  $m > 0$  Kanten. Dann lässt sich die Eckenmenge  $V = V(G)$  so in zwei disjunkte  $n$ -Mengen  $A$  und  $B$  aufteilen, dass mehr als  $\frac{m}{2}$  Kanten zwischen  $A$  und  $B$  verlaufen.*

*Beweis.* Wir wählen  $A$  als eine zufällige  $n$ -elementige Teilmenge von  $V$ , alle  $\binom{2n}{n}$  möglichen Teilmengen haben die gleiche Wahrscheinlichkeit, und wir setzen  $B = V \setminus A$ . Mit  $X$  bezeichnen wir die Anzahl der Kanten  $\{a, b\}$  „zwischen“  $A$  und  $B$ , d.h. mit  $a \in A$  und  $b \in B$ . Wir berechnen den Erwartungswert  $\mathbf{E}[X]$  der Zufallsvariable  $X$ . Für jede Kante  $e = \{u, v\} \in E(G)$  definieren wir das Ereignis  $C_e$ , das eintrifft, wenn die Kante  $e$  zwischen  $A$  und  $B$  verläuft:  $C_e = \{A \in \binom{V}{n} : |A \cap e| = 1\}$ . Dann gilt  $X = \sum_{e \in E(G)} I_{C_e}$ , somit ist  $\mathbf{E}[X] = \sum_{e \in E(G)} P(C_e)$ . Wir müssen also noch die Wahrscheinlichkeit  $P(C_e)$  bestimmen.

Insgesamt gibt es  $\binom{2n}{n}$  Wahlmöglichkeiten für  $A$ . Wenn wir verlangen, dass  $u \in A$  und  $v \notin A$ , können wir die verbleibenden  $n - 1$  Elemente für  $A$  auf  $\binom{2n-2}{n-1}$  Arten auswählen. Das Argument funktioniert entsprechend auch für die symmetrische Situation  $u \notin A$ ,  $v \in A$ . Demnach ist

$$P(C_e) = \frac{2 \binom{2n-2}{n-1}}{\binom{2n}{n}} = \frac{n}{2n-1} > \frac{1}{2}.$$

Daraus erhalten wir  $\mathbf{E}[X] = \sum_{e \in E(G)} P(C_e) > \frac{m}{2}$ . Der Erwartungswert von  $X$  ist das arithmetische Mittel der Werte, die  $X$  bei den verschiedenen möglichen Mengen  $A$  annimmt. Ein Mittelwert kann aber nicht größer sein als das Maximum all dieser Werte, folglich kann  $A$  so gewählt werden, dass mehr als die Hälfte der Kanten zwischen  $A$  und  $B$  verläuft.  $\square$

**Unabhängige Mengen.** In Abschnitt 4.7 haben wir die maximal mögliche Kantenzahl eines dreiecksfreien Graphen auf  $n$  Ecken bestimmt. Allgemeiner können wir für vorgegebenes  $k \geq 3$  nach der

maximal möglichen Kantenzahl eines Graphen auf  $n$  Ecken fragen, der keinen zum vollständigen Graph  $K_k$  auf  $k$  Ecken isomorphen Teilgraphen enthält. Diese Frage beantwortet der Satz von Turán, eines der bedeutenden Resultate der extremalen Graphentheorie. Dieser Satz hat verschiedene Formulierungen. In der stärksten Fassung, den wir in Abschnitt 4.7 für  $k = 3$  bewiesen haben (für beliebiges  $k$  siehe Aufgabe 4.7.4), beschreibt er genau, wie ein  $K_k$ -freier Graph mit der größtmöglichen Kantenzahl aussieht. Wir beweisen hier nur die Schranke für die Kantenzahl mit einem wunderbaren probabilistischen Beweis. Wenn man mehr Arbeit investiert, kann man auch die Struktur des Graphen mit maximal vielen Kanten bestimmen, doch diesen Teil lassen wir aus.

Meist wird der Satz von Turán in der „anderen Richtung“ verwendet: *Hat ein Graph auf  $n$  Ecken mehr als soundsoviele Kanten, dann muss er einen  $K_k$  enthalten.* Im Komplement des Graphen  $G$ , d.h. in dem Graphen, der genau dort Kanten hat, wo  $G$  keine hat, sagt der Satz von Turán: *Hat ein Graph auf  $n$  Ecken weniger als soundsoviele Kanten, dann muss er eine unabhängige Menge der Größe mindestens  $k$  enthalten* (eine unabhängige Menge ist eine Menge von Ecken, von denen keine zwei durch eine Kante verbunden sind). Dies ist die vielleicht nützlichste Version für Anwendungen, die wir nun formulieren und beweisen wollen.

**10.4.2 Satz (Satz von Turán).** *Für jeden Graphen  $G$  auf  $n$  Ecken gilt*

$$\alpha(G) \geq \frac{n^2}{2|E(G)| + n};$$

dabei bezeichnet  $\alpha(G)$  die Größe einer größten unabhängigen Eckenmenge im Graphen  $G$ .

Die probabilistische Methode steckt in folgendem Lemma:

**Lemma.** *Für jeden Graphen  $G$  gilt*

$$\alpha(G) \geq \sum_{v \in V(G)} \frac{1}{\deg_G(v) + 1}$$

(wobei  $\deg_G(v)$  für den Grad der Ecke  $v$  in  $G$  steht).

*Beweis.* Angenommen, die Ecken von  $G$  sind von 1 bis  $n$  durchnummierter, und wir wählen eine zufällige Permutation  $\pi$  der Ecken. Wir

definieren eine Menge  $M = M(\pi) \subseteq V(G)$ , die aus all jenen  $v$  bestehen soll, bei denen alle Nachbarn  $u$  die Ungleichung  $\pi(u) > \pi(v)$  erfüllen; d.h. die Ecke  $v$  kommt in der durch die Permutation  $\pi$  gegebenen Ordnung vor all ihren Nachbarn. Weil die Menge  $M(\pi)$  eine unabhängige Menge in  $G$  ist (das sieht man leicht!), gilt  $|M(\pi)| \leq \alpha(G)$  für jede Permutation  $\pi$ . Deshalb ist auch  $\mathbf{E}[|M|] \leq \alpha(G)$ . Nun berechnen wir diesen Erwartungswert.

Zu jeder Ecke  $v$  sei  $A_v$  das Ereignis „ $v \in M(\pi)$ “. Wenn  $N_v$  die Menge aller Nachbarn der Ecke  $v$  bezeichnet, sind alle möglichen Anordnungen der Menge  $N_v \cup \{v\}$  durch die Permutation  $\pi$  gleich wahrscheinlich, also ist die Wahrscheinlichkeit, dass  $v$  das kleinste Element in dieser Menge ist, gleich  $1/(|N_v| + 1) = 1/(\deg_G(v) + 1)$ . Daraus folgt, dass  $P(A_v) = 1/(\deg_G(v) + 1)$  ist, und ähnlich wie schon mehrfach zuvor berechnen wir:

$$\begin{aligned}\alpha(G) &\geq \mathbf{E}[|M|] = \sum_{v \in V(G)} \mathbf{E}[I_{A_v}] \\ &= \sum_{v \in V(G)} P(A_v) = \sum_{v \in V(G)} \frac{1}{\deg_G(v) + 1}.\end{aligned}$$

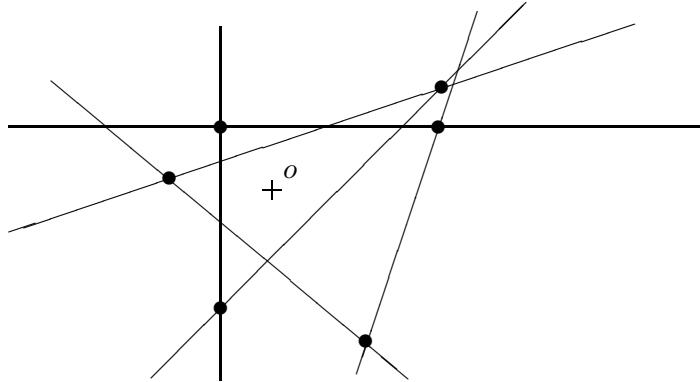
□

*Beweis von Satz 10.4.2.* Wir müssen nur noch ein wenig rechnen. Die Kantenzahl  $e = |E(G)|$  ist die Hälfte der Summe der Eckengrade. Wir haben also folgende Situation: Für nicht negative reelle Zahlen  $d_1, d_2, \dots, d_n$  wissen wir, dass  $\sum_{i=1}^n d_i = 2e$  ist, und wir fragen nach dem kleinstmöglichen Wert der Summe

$$\sum_{i=1}^n \frac{1}{d_i + 1}.$$

Man kann zeigen, dass diese Summe für  $d_1 = d_2 = \dots = d_n = 2e/n$  minimal wird (beweisen dürfen Sie das als Übung), und in diesem Fall hat sie den Wert  $n^2/(2e + n)$ , wie im Satz behauptet. □

**Anzahl der Schnittpunkte  $\leq k$ -ter Ordnung.** Dieses geometrische Problem taucht bei der Analyse gewisser geometrischer Algorithmen auf. Betrachten wir eine Menge  $L$  mit  $n$  Geraden in der Ebene, von denen keine zwei parallel sind und von denen sich keine drei in einem gemeinsamen Punkt schneiden. Ferner sei  $o$  ein Punkt, der auf keiner der Geraden aus  $L$  liegt. Wir werden die



**Abb. 10.3** Schnittpunkte erster Ordnung für eine Geradenmenge.

Schnittpunkte aller Geraden aus  $L$  betrachten. Jedes Geradenpaar hat einen Schnittpunkt, also gibt es insgesamt  $\binom{n}{2}$  Schnittpunkte. Wir wollen sagen, die *Ordnung* eines Schnittpunktes  $v$  sei  $k$ , wenn die Strecke  $ov$  zusätzlich zu den zwei Geraden, die sich in  $v$  schneiden, genau  $k$  weitere Geraden aus  $L$  schneidet (In Abb. 10.3 sind alle Schnittpunkte erster Ordnung eingezeichnet). Was ist bei gegebenem  $n$  und  $k$  die größtmögliche Anzahl Schnittpunkte der Ordnung höchstens  $k$ ? Die Schranke aus dem folgenden Satz ist bis auf den Wert des Proportionalitätsfaktors bestmöglich:

**10.4.3 Satz.** Zu jeder Menge von  $n$  Geraden gibt es nicht mehr als  $3(k+1)n$  Schnittpunkte der Ordnung höchstens  $k$ .

*Beweis.* Zuerst untersuchen wir den speziellen Fall  $k = 0$ . Wir sehen, dass die Geraden aus  $L$  die Ebene in Zellen einteilen und dass die Schnittpunkte nullter Ordnung gerade die Eckpunkte derjenigen Zelle sind, die den Punkt  $o$  enthält. Weil jede Gerade diese Zelle (die ein evtl. offenes Polygon ist) höchstens einmal beranden kann, ist die Anzahl der Seiten höchstens  $n$ , also auch die Anzahl der Schnittpunkte nullter Ordnung. Diese Tatsache werden wir im Beweis für beliebiges  $k$  verwenden, den wir als Nächstes angehen.

Die Zahl  $p$  sei aus dem Intervall  $(0, 1)$  geeignet gewählt, ihren genauen Wert bestimmen wir am Ende des Beweises. Sie beeinflusst die zufällige Wahl einer Teilmenge  $R \subseteq L$ , die wir konstruieren, indem wir jede Gerade  $\ell \in L$  mit Wahrscheinlichkeit  $p$  auswählen

und mit Wahrscheinlichkeit  $1 - p$  nicht auswählen; die Auswahl der verschiedenen Geraden  $\ell$  soll unabhängig voneinander sein.

An dieser Stelle sollten wir wohl ein Wort über den zu Grunde liegenden Wahrscheinlichkeitsraum verlieren. Es handelt sich um eine Verallgemeinerung des Raums  $C_n$  aus Beispiel 10.2.2, der das Werfen einer fairen (symmetrischen) Münze modelliert, bei der Kopf und Zahl gleich wahrscheinlich sind. Im hier betrachteten Fall bräuchten wir eine asymmetrische Münze, bei der Kopf mit Wahrscheinlichkeit  $p$  fällt und Zahl mit Wahrscheinlichkeit  $1 - p$ . Für jede Gerade  $\ell \in L$  werfen wir diese asymmetrische Münze einmal, und wenn Kopf fällt, fügen wir  $\ell$  zu unserer Teilmenge  $R$  hinzu. Formal besteht der Wahrscheinlichkeitsraum aus allen Teilmengen von  $L$ , und die Wahrscheinlichkeit für eine  $r$ -elementige Menge  $R \subseteq L$  ist  $p^r(1-p)^{n-r}$ , wobei  $r = |R|$  (denn um genau die Menge  $R$  durch Münzwürfe zu erhalten, muss bei  $r$  bestimmten Würfen Kopf fallen und bei den anderen  $n - r$  Würfen Zahl). Dies ist einmal ein Beispiel für einen Wahrscheinlichkeitsraum, in dem nicht alle Elementarereignisse die gleiche Wahrscheinlichkeit haben.

Wenden wir uns wieder unserer geometrischen Situation zu. Wir haben also eine zufällige Menge  $R \subseteq L$  von Geraden ausgelost. Wir wollen uns nun vorstellen, dass nur die Geraden aus  $R$  in die Ebene gezeichnet sind. Wir definieren die Zufallsvariable  $f = f(R)$  als die Anzahl der Schnittpunkte, die bezüglich der Geraden aus  $R$  die Ordnung 0 haben; das bedeutet,  $f$  zählt die Schnittpunkte von Geraden aus  $R$ , deren Sicht von  $o$  aus von keiner Geraden aus  $R$  verstellt wird. Wir werden den Erwartungswert  $\mathbf{E}[f]$  auf zwei verschiedene Arten schätzen. Auf der einen Seite haben wir nach der Bemerkung zu Beginn des Beweises  $f(R) \leq |R|$  für jede einzelne Menge  $R$ , und folglich ist  $\mathbf{E}[f] \leq \mathbf{E}[|R|]$ . Wie man unschwer berechnet (z.B. in Aufgabe 8), ist  $\mathbf{E}[|R|] = pn$ .

Nun werden wir  $\mathbf{E}[f]$  auf eine andere Art bestimmen. Für jeden Schnittpunkt  $v$  der Geraden aus  $L$  definieren wir ein Ereignis  $A_v$ , das genau dann eintritt, wenn  $v$  bezüglich der Geraden aus  $R$  einer der Schnittpunkte nullter Ordnung ist, d.h. wenn er 1 zu  $f(R)$  beträgt. Das Ereignis  $A$  tritt genau dann ein, wenn die folgenden zwei Bedingungen erfüllt sind:

- Die beiden Geraden, deren Schnittpunkt  $v$  ist, liegen in  $R$ .
- Keine der Geraden, die die Strecke  $ov$  in einem inneren Punkt schneiden (und so den Blick vom Punkt  $v$  zum Punkt  $o$  verstehen), liegt in  $R$ .

Daraus folgern wir, dass  $P(A_v) = p^2(1-p)^{\ell(v)}$ , wobei  $\ell(v)$  die Ordnung des Schnittpunktes  $v$  bezeichnet.

Sei  $M$  die Menge aller Schnittpunkte von Geraden aus  $L$ , und sei  $M_k \subseteq M$  die Menge der Schnittpunkte höchstens  $k$ -ter Ordnung. Dann ist

$$\begin{aligned}\mathbf{E}[f] &= \sum_{v \in M} \mathbf{E}[I_{A_v}] = \sum_{v \in M} P(A_v) \geq \sum_{v \in M_k} P(A_v) \\ &= \sum_{v \in M_k} p^2(1-p)^{\ell(v)} \geq \sum_{v \in M_k} p^2(1-p)^k = |M_k|p^2(1-p)^k.\end{aligned}$$

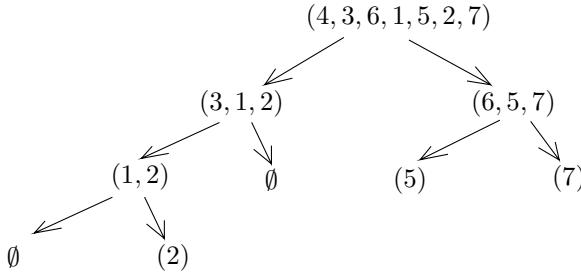
Zusammen ergibt das  $np \geq \mathbf{E}[f] \geq |M_k|p^2(1-p)^k$ , anders ausgedrückt

$$|M_k| \leq \frac{n}{p(1-p)^k}.$$

Schließlich wählen wir die Zahl  $p$  so, dass der Wert auf der rechten Seite der Ungleichung möglichst klein wird. Eine gute Wahl ist beispielsweise  $p = 1/(k+1)$ . Aus Aufgabe 3.5.2 wissen wir, dass  $(1 - \frac{1}{k+1})^k \geq e^{-1} > \frac{1}{3}$  ist für jedes  $k \geq 1$ . Daraus erhalten wir  $|M_k| \leq 3(k+1)n$ , wie behauptet.  $\square$

Die Abschätzung der größtmöglichen Anzahl Schnittpunkte der Ordnung *genau*  $k$  ist übrigens wesentlich komplizierter und noch ungelöst. Das mathematische Teilgebiet, in dem man sich mit Problemen ähnlicher Art beschäftigt, mit kombinatorischen Fragestellungen bei geometrischen Konfigurationen, heißt *kombinatorische Geometrie*. Zu ihrem Studium ist das Buch von Pach und Agarwal [29] höchst empfehlenswert. Etwas spezieller ist das Buch von Sharir und Agarwal [48], in dem es um Probleme geht, die dem hier betrachteten über Schnittpunkte der Ordnung  $k$  sehr ähnlich sind.

**Durchschnittliche Anzahl der Vergleiche in QUICKSORT.**  
Der Algorithmus QUICKSORT erwartet als Eingabe eine Zahlenfolge  $(x_1, x_2, \dots, x_n)$  und geht dann so vor: Die Zahlen  $x_2, x_3, \dots, x_n$  werden mit  $x_1$  verglichen und in zwei Gruppen eingeteilt, in die Zahlen, die kleiner als  $x_1$  sind, und in jene, die mindestens so groß sind wie  $x_1$ . In beiden Gruppen bleibt die Reihenfolge der Zahlen aus der Eingabefolge erhalten. Jede Gruppe wird dann durch einen rekursiven Aufruf von QUICKSORT sortiert. Die Rekursion endet mit trivial kleinen Gruppen (z.B. mit einelementigen). Die Eingabefolge  $(4, 3, 6, 1, 5, 2, 7)$  etwa würde wie folgt sortiert werden:



Dieser Algorithmus kann im schlimmsten Fall etwa  $n^2$  Schritte benötigen (das gemeinste, was man tun kann, ist den Algorithmus mit einer schon sortierten Folge zu konfrontieren). In der Praxis ist QUICKSORT jedoch sehr beliebt und wird als einer der schnellsten Sortieralgorithmen angesehen. Seine Laufzeit ist „im Durchschnitt“ sehr gut. Diese Beobachtung drückt sich zum Teil in dem nun folgenden Satz aus.

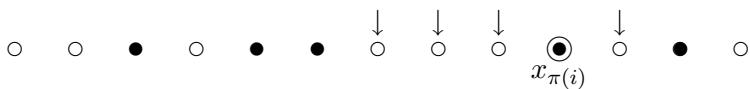
**10.4.4 Satz.** Sei  $x_1 < x_2 < \dots < x_n$  eine Folge reeller Zahlen in aufsteigender Reihenfolge. Sei  $\pi$  eine Permutation der Menge  $\{1, 2, \dots, n\}$ , und sei  $T(\pi)$  die Anzahl der Vergleiche (von jeweils zwei Zahlen), die QUICKSORT bei der Folge  $(x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(n)})$  durchführt. Dann ist der Erwartungswert von  $T(\pi)$  für eine zufällige Permutation  $\pi$  höchstens  $2n \ln n$ .

Jeder Algorithmus, der beliebige  $n$ -Tupel verschiedener reeller Zahlen sortieren kann und dazu nur paarweise Vergleiche dieser Zahlen durchführt, muss im schlimmsten Fall mindestens  $\log_2 n!$  Vergleiche durchführen. Das ist so, weil der Algorithmus aufgrund der Vergleiche eine von  $n!$  möglichen Permutationen herausfinden muss, und  $k$  Vergleiche haben lediglich  $2^k$  verschiedene Ergebnisse. Wie wir aus Abschnitt 3.5 wissen, gilt  $n! \geq \left(\frac{n}{e}\right)^n$ , also ist  $\log_2 n! = (\log_2 e) \ln n! \geq (\log_2 e)(n-1) \ln n \approx 1,443(n-1) \ln n$ . Deshalb ist das durchschnittliche Verhalten von QUICKSORT, das uns Satz 10.4.4 versichert, ziemlich gut.

Der Grund für die durchschnittliche  $O(n \log n)$ -Laufzeit des QUICKSORT Algorithmus ist unschwer zu sehen. Wenn die Elemente in der Eingabefolge in zufälliger Reihenfolge sind, erwarten wir, dass im Regelfall das erste Element die übrigen in zwei Gruppen von vergleichbarer Größe teilt — es ist unwahrscheinlich, dass die eine Gruppe wesentlich kleiner ist als die andere. Wenn dies in den meisten Fällen geschieht, wird die Rekursion des Algorithmus ungefähr  $\log n$  Ebenen haben, und in jeder Ebene der Rekursion benötigen wir insgesamt  $O(n)$  Vergleiche.

Dies mag schon recht überzeugend klingen, ein Beweis ist es aber sicher nicht. Wir geben nun einen richtigen Beweis, der auf einer ganz anderen Idee beruht.

*Beweis von Satz 10.4.4.* Sei  $T_i = T_i(\pi)$  die Anzahl der Elemente, die zu dem Zeitpunkt, wo  $x_{\pi(i)}$  das unterteilende Element ist, mit eben diesem Element  $x_{\pi(i)}$  verglichen werden. Wir haben z.B. stets  $T_1 = n - 1$ , weil  $x_{\pi(1)}$  das erste Element in der Eingabefolge ist und alle anderen Elemente mit ihm verglichen werden. Wenn  $\pi(2) < \pi(1)$  ist, dann ist  $T_2 = \pi(1) - 2$ , und falls  $\pi(2) > \pi(1)$ , ist  $T_2 = n - \pi(1) - 1$ . Allgemein kann man  $T_i$  mittels folgendem Diagramm interpretieren:



Die kleinen Kreise in diesem Diagramm stehen für die Elemente  $x_1, x_2, \dots, x_n$  in aufsteigender Reihenfolge. Die ausgefüllten Kreise sind die Elemente mit Indizes  $\pi(1), \pi(2), \dots, \pi(i - 1)$ , d.h. die ersten  $i - 1$  Elemente der Eingabefolge. Das Element  $x_{\pi(i)}$  ist mit einem Doppelkreis markiert, und die übrigen Elemente haben nicht ausgefüllte Kreise. Es ist nicht schwer zu sehen, dass  $T_i$  genau die Anzahl nicht ausgefüllter Kreise ist, die von dem Element  $x_{\pi(i)}$  aus „sichtbar“ sind, wobei die ausgefüllten Kreise die Sicht blockieren.

Wir werden den Erwartungswert von  $T_i$  untersuchen. Die Hauptidee ist, sich vorzustellen, der Algorithmus laufe rückwärts in der Zeit, wie wenn man einen Film rückwärts ablaufen sieht. Wir betrachten die Indizes  $i$  in umgekehrter Reihenfolge,  $n, n-1, \dots, 1$ , und wir betrachten das zugehörige Bild mit ausgefüllten und nicht ausgefüllten Kreisen. Anfangs sind alle Kreise ausgefüllt. Die zufällige Permutation  $\pi$  ist noch nicht bestimmt, wir erzeugen sie im Laufe der Betrachtungen durch Zufallsentscheidungen. Zuerst wählen wir zufällig einen ausgefüllten Kreis aus und entfernen die Füllung. Der Index dieses Kreises wird  $\pi(n)$ . Dann wählen wir zufällig einen weiteren ausgefüllten Kreis, entfernen die Füllung und haben  $\pi(n-1)$ , und so weiter; dies ist die gleiche Methode, eine zufällige Permutation zu erzeugen, wie in Abb. 10.2. In dem Moment, wo noch  $i$  ausgefüllte Kreise übrig sind, ziehen wir zufällig einen von ihnen, der zu  $x_{\pi(i)}$  korrespondiert. Die Zahl  $T_i$  ist die Anzahl nicht ausgefüllter Kreise, die zu diesem Zeitpunkt von  $x_{\pi(i)}$  sichtbar sind.

Wir bestimmen den Erwartungswert von  $T_i$  mit doppeltem Abzählen. Von jedem der  $n-i$  nicht ausgefüllten Kreise sind höchstens zwei ausgefüllte Kreise sichtbar. Daher ist die Gesamtzahl von Paaren aus einem ausgefüllten und einem nicht ausgefüllten Kreis, die sich gegenseitig sehen können, höchstens  $2(n-i)$ . Im Durchschnitt sieht einer der  $i$  ausgefüllten Kreise höchstens  $\frac{2(n-i)}{i}$  nicht ausgefüllte, also ist  $\mathbf{E}[T_i] \leq \frac{2(n-i)}{i}$ . Weil  $T(\pi) = \sum_{i=1}^n T_i(\pi)$  ist, erhalten wir

$$\mathbf{E}[T] = \sum_{i=1}^n \mathbf{E}[T_i] \leq \sum_{i=1}^n \frac{2(n-i)}{i} = 2n \sum_{i=1}^n \frac{1}{i} - 2n \leq 2n \ln n.$$

□

**Bemerkung.** Man kann zeigen, dass die Wahrscheinlichkeit dafür, dass die Laufzeit von QUICKSORT wesentlich vom Erwartungswert abweicht, recht klein ist (exponentiell klein), d.h. „böse“ Permutationen sind dünn gesät. Das werden wir hier nicht untersuchen.

## Aufgaben

1. Beweisen Sie mit Satz 10.4.2, dass jeder dreiecksfreie Graph auf  $n$  Ecken höchstens  $n^2/4$  Kanten hat; das ergibt noch einen weiteren Beweis von Satz 4.7.1.
2. \*Zeigen Sie, dass für nicht negative reelle Zahlen  $d_1, \dots, d_n$ , die auf 1 summieren, der Ausdruck  $\sum_{i=1}^n 1/(d_i + 1)$  minimal wird für  $d_1 = d_2 = \dots = d_n = 1/n$ .
3. Betrachten Sie folgenden Algorithmus zum Auffinden einer unabhängigen Menge in einem Graphen  $G$ . Entfernen Sie wiederholt eine Ecke maximalen Grades zusammen mit allen inzidenten Kanten aus dem aktuellen Graphen, und zwar solange, bis der aktuelle Graph keine Kanten mehr enthält. Zeigen Sie, dass dieser Algorithmus immer eine unabhängige Menge der Größe mindestens  $F(G) = \sum_{v \in V(G)} 1/(1 + \deg_G(v))$  liefert. Hinweis: Wenn  $H$  aus  $G$  durch Entfernen einer Ecke maximalen Grades entsteht, dann ist  $F(H) \geq F(G)$ .
4. \*Beweisen Sie die folgende Version des Satzes von Turán. Sei  $r \geq 3$  eine ganze Zahl, und  $n$  sei durch  $r-1$  teilbar. Dann hat jeder Graph auf  $n$  Ecken, der keinen  $K_r$  als Teilgraph enthält, höchstens  $\frac{n^2}{2} \left(1 - \frac{1}{r-1}\right)$  Kanten. Führen Sie Induktion über die Zahl  $\frac{n}{r-1}$ .
5. Sei  $G$  ein Graph. Betrachten Sie folgenden Algorithmus. Unterteilen Sie  $V(G)$  in zwei beliebige Teile  $A$  und  $B$ . Solange es eine Ecke gibt, die mehr Nachbarn in dem Teil hat, zu dem sie selbst dazugehört, als

in dem anderen, so nehmen Sie sie aus ihrem Teil hinaus und stecken sie in den anderen (wenn es mehrere solche Ecken gibt, nehmen Sie irgendeine). Zeigen Sie, dass dieser Algorithmus immer zu einem Ende kommt (und geben Sie eine möglichst gute Schranke für die Laufzeit), und dass mindestens die Hälfte der Kanten aus  $G$  zwischen den beiden so konstruierten Teilen  $A, B$  verläuft.

6. (a) Wandeln Sie den oben beschriebenen Algorithmus QUICKSORT wie folgt ab. Die aktuelle Eingabefolge sei  $(x_1, x_2, \dots, x_n)$ . Wählen Sie eine zufällige Zahl  $i$  aus  $1, 2, \dots, n$  (alle Werte mit gleicher Wahrscheinlichkeit  $\frac{1}{n}$ ) und verwenden Sie  $x_i$  als unterteilendes Element. Zeigen Sie, dass für jede feste Eingabe von  $n$  verschiedenen Zahlen  $(x_1, x_2, \dots, x_n)$  die erwartete Anzahl nötiger Vergleiche dieselbe ist, und dass sie wie in Satz 10.4.4 durch  $2n \ln n$  beschränkt ist.  
 (b) \*Betrachten Sie eine andere Modifikation des Algorithmus: Wählen Sie bei gegebener Eingabefolge  $(x_1, x_2, \dots, x_n)$  unabhängig voneinander zwei zufällige Zahlen  $i_1, i_2$  aus  $\{1, 2, \dots, n\}$  und benutzen Sie  $\max(x_{i_1}, x_{i_2})$  als unterteilendes Element. Angenommen,  $x_1, x_2, \dots, x_n$  sind alle verschieden. Zeigen Sie, dass die erwartete Anzahl Vergleiche für eine gegebene Eingabefolge die gleiche ist wie in (a). Die Vergleiche zur Bestimmung von  $\max(x_{i_1}, x_{i_2})$  zählen nicht!
7. \*Betrachten Sie  $n$  (nicht ausgefüllte) Kreise in einer Reihe. Ein Beobachter sitzt in einem der  $n-1$  Zwischenräume. Eine zufällige Teilmenge von  $r$  Kreisen wird schwarz ausgefüllt. Zeigen Sie, dass die erwartete Anzahl weißer (d.h. nicht ausgefüllter) Kreise, die der Beobachter sehen kann, höchstens  $2(n-r)/(r+1)$  ist. (Der Beobachter kann durch weiße Kreise hindurchsehen, nicht jedoch durch schwarze.) Hinweis: Füllen Sie nicht  $r$ , sondern  $r+1$  Kreise schwarz und wählen Sie dann einen zufälligen Kreis, bei dem Sie die Farbe wieder wegwischen.
8. Die Teilmenge  $R \subseteq L$  sei zufällig ausgewählt, wie im Beweis von Satz 10.4.3. Beweisen Sie, dass  $\mathbf{E}[|R|] = pn$ .
- \*Betrachten Sie  $n$  Geraden wie in Satz 10.4.3; als zusätzliche Bedingung verlaufe keine der Geraden vertikal. Wir nennen einen Schnittpunkt  $v$  eine *Spitze*, wenn eine der ihn definierenden Geraden positive Steigung hat und die andere negative Steigung. Beweisen Sie, dass es höchstens  $6(k+1)^2$  Spitzen  $k$ -ter Ordnung gibt.

# 11

## Ramsey–Theorie

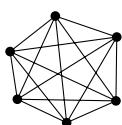
---

Paul Erdős (1913–1996), ein berühmter Mathematiker des 20. Jahrhunderts, einer der Großen der diskreten Mathematik, erzählte gern diese Geschichte. Die Röntgenstrahlen wurden 1895 von Wilhelm Conrad Röntgen entdeckt. Doch bereits früher hatte der Britische Physiker Sir William Crookes einen ähnlichen Effekt beobachtet: Photoplatten wurden auf mysteriöse Weise schwarz, wenn sie in der Nähe einer Schattenkreuzröhre gelagert wurden. Er bemerkte dies und wies seine Assistenten an, die Fotoplatten künftig an einem anderen Ort zu lagern.

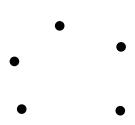
Die Moral dieser Geschichte ist eine zweifache. Erstens, Fortuna begünstigt jene Forscher, die für Entdeckungen bereit sind (Erdős pflegte diesen Aspekt zu betonen). Und zweitens, große Entdeckungen beginnen oft mit einfachen, eher unbedeutenden Beobachtungen. Aus kaum wahrnehmbaren Effekten können bedeutende Theorien erwachsen. Doch wir müssen bereit sein.

Auch in der Mathematik und Informatik gibt es Entdeckungen, die sich anfangs häufig unauffällig äußern, als scheinbar irrelevante Kuriosität. In diesem Kapitel diskutieren wir eine solche kuriose Beobachtung an Graphen mit nicht mehr als 6 Ecken.

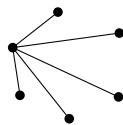
Wir beginnen mit einer populären Form des Resultats. Sechs Leute treffen sich auf einer Party. Einige kennen sich, andere nicht. Die Party könnte schematisch vielleicht nach einem der folgenden Muster dargestellt werden:



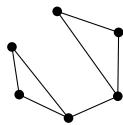
Klassentreffen  
nach 50 Jahren



Dating Party



Fan-Party



Treffen zweier  
Mafia-Bosse

(für die Gäste haben wir Punkte gezeichnet, die im Fall gegenseitiger Bekanntschaft miteinander verbunden sind, und hoppla! wir haben einen Graph auf 6 Ecken). Natürlich gibt es viele weitere Möglichkeiten, die schwerlich alle auf diese Seite passen würden. Doch wie auch immer die Party aussieht, es wird immer drei Gäste geben, die sich gegenseitig kennen, oder drei Gäste, die sich gegenseitig nicht kennen. Wir wissen mit Sicherheit, dass stets eine dieser zwei Möglichkeiten zutreffen wird, auch wenn wir im Voraus nicht wissen, welche.

Diese bescheidene Aussage ist ein winziges Stück einer großen Theorie, der Ramsey–Theorie, von der wir in diesem Kapitel einen kleinen Ausschnitt kennen lernen. Im ersten Abschnitt beweisen wir die Behauptung über Partys mit 6 Gästen (das ist nicht so einfach, wie man denken mag). In Abschnitt 11.2 beweisen wir den Satz von Ramsey für Graphen; damit werden wir die Beschränkung auf 6 Ecken los. Einer weiteren Überraschung, die der Satz von Ramsey bereit hält, begegnen wir in Abschnitt 11.3: Wir können zeigen, dass der Satz von Ramsey wahrhaft riesige Mengen verlangt. Als kombinatorisches Prinzip ist er daher unhandlich und nicht besonders effizient. In diesem Teil kommt die probabilistische Methode aus Kapitel 10 zur Anwendung.

## 11.1 Eine Party zu sechst

Wir zeigen nun die Behauptung für Partys mit 6 Gästen (einschließlich Gastgeber). Die Party stellen wir uns als Graph vor, die Ecken entsprechen den Gästen, die Kanten entsprechen Paaren von Gästen, die sich bereits kennen. Die Bekanntschaftsrelation nehmen wir also stillschweigend als symmetrisch an.

Sei  $G$  ein Graph. Ähnlich wie in Abschnitt 2.4 führen wir folgende Schreibweise ein: Die *Cliquenzahl*  $\omega(G)$  bezeichnet die maximale Eckenzahl eines vollständigen Teilgraphen von  $G$ , und die *Unabhängigkeitsszahl*  $\alpha(G)$  ist die maximale Eckenzahl einer unabhängigen Menge in  $G$ , d.h. einer Menge, in der keine zwei Ecken durch eine Kante verbunden sind.

Wir beweisen folgenden Satz.

**11.1.1 Satz.** *Ist  $G$  ein Graph auf mindestens 6 Ecken, so ist  $\alpha(G) \geq 3$  oder  $\omega(G) \geq 3$ .*

**Beweis.** Wir wählen eine beliebige Ecke  $u$  aus  $G$ . Die übrigen Ecken aus  $V(G) \setminus \{u\}$  teilen wir auf: Die nicht mit  $u$  benachbarten sammeln wir in der Menge  $A = \{v \in V(G) : v \neq u, \{u, v\} \notin E(G)\}$ , die mit  $u$  benachbarten in  $B = V(G) \setminus A \setminus \{u\}$ . Weil  $|V(G)| \geq 6$ , muss eine der Mengen  $A$  und  $B$  mindestens 3 Elemente enthalten. Nun unterscheiden wir zwei Fälle.

1.  $|A| \geq 3$ .  $A$  enthalte die Ecken  $x, y, z$ . Sind je zwei davon in  $G$  benachbart, dann bildet  $\{x, y, z\}$  ein Dreieck  $K_3$  und es ist  $\omega(G) \geq 3$ . Andernfalls, wenn etwa  $\{x, y\} \notin E(G)$ , dann ist  $\{u, x, y\}$  eine unabhängige Menge in  $G$ , also  $\alpha(G) \geq 3$ .
2.  $|B| \geq 3$ . Wir gehen vor wie eben: Entweder ist kein Eckenpaar aus  $B$  eine Kante von  $G$ , dann ist  $\alpha(G) \geq 3$ , oder es gibt zwei Ecken  $x, y \in B$ , die in  $G$  durch eine Kante verbunden sind. In diesem Fall bildet die Menge  $\{u, x, y\}$  einen vollständigen Teilgraphen von  $G$ , und damit ist  $\omega(G) \geq 3$ .  $\square$

Beachten Sie, wie viele Fälle wir zum Beweis dieser Aussage, die sich nur auf Graphen mit 6 Ecken bezieht, unterscheiden mussten. Was für ein Aufwand für ein läppisches Resultat! Doch dies war nur der Auftakt zu allgemeineren Sätzen. Übrigens haben wir beim Beweis von Satz 11.1.1 den Spezialfall  $t = 2$ ,  $n_1 = n_2 = 3$  des folgenden universellen Prinzips verwendet:

**11.1.2 Satz (Schubfachprinzip).**  $n_1, n_2, \dots, n_t$  seien natürliche Zahlen,  $X$  eine Menge mit mindestens  $1 + \sum_{i=1}^t (n_i - 1)$  Elementen, und  $X_1, X_2, \dots, X_t$  seien disjunkte Mengen, die  $X$  überdecken. Dann gibt es ein  $i$ , so dass  $X_i$  mindestens  $n_i$  Elemente hat.

## 11.2 Der Satz von Ramsey für Graphen

Hier ist nun die versprochene Verallgemeinerung von Satz 11.1.1 für „größere Partys“.

**11.2.1 Satz (Satz von Ramsey für Graphen).** Hat ein Graph  $G$  mindestens  $\binom{k+\ell-2}{k-1}$  Ecken, dann ist  $\omega(G) \geq k$  oder  $\alpha(G) \geq \ell$ .

Wir halten fest, dass die Bedingung in dem Satz symmetrisch ist bezüglich  $k$  und  $\ell$ , denn  $\binom{k+\ell-2}{k-1} = \binom{k+\ell-2}{\ell-1}$ .

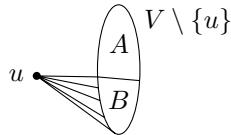
Setzen wir  $k = \ell = 3$ , dann erhalten wir mit dem Satz, dass für jeden Graph  $G$  mit  $\binom{4}{2} = 6$  Ecken  $\omega(G) \geq 3$  oder  $\alpha(G) \geq 3$  ist; das war genau die Aussage von Satz 11.1.1. Dem aufmerksamen Leser

wird nicht entgehen, wie ähnlich der nun folgende Beweis dem von Satz 11.1.1 ist.

**Beweis.** Wir führen Induktion über  $k + \ell$ . Für  $k = 1$  oder  $\ell = 1$  sieht man die Aussage leicht ein. (Man sieht sie auch für  $k = 2$  oder  $\ell = 2$  leicht ein, doch darum brauchen wir uns nicht zu kümmern.)

Nehmen wir also an, dass  $k, \ell \geq 2$  und dass die Aussage für  $k, \ell - 1$  sowie für  $k - 1, \ell$  gilt. Wir setzen  $n = \binom{k+\ell-2}{k-1}$ ,  $n_1 = \binom{k+\ell-3}{k-1}$  und  $n_2 = \binom{k+\ell-3}{k-2}$ . Mit der Pascalschen Formel (3.4) für die Addition von Binomialkoeffizienten haben wir  $n = n_1 + n_2$ ; das schreiben wir in der Form  $n = 1 + ((n_1 - 1) + (n_2 - 1) + 1)$ , womit das Schema des Beweises vorgegeben ist.

Es sei  $G = (V, E)$  ein beliebiger Graph auf  $n$  Ecken. Wir möchten zeigen, dass  $\omega(G) \geq k$  oder  $\alpha(G) \geq \ell$ . Wir wählen eine beliebige Ecke  $u \in V$ . Die übrigen Ecken teilen wir danach, ob sie mit  $u$  verbunden sind oder nicht, in zwei Mengen  $A$  und  $B$  auf; im Bild:



In Formeln,

$$\begin{aligned} A &= \{v \in V \setminus \{u\}: \{u, v\} \notin E\} \\ B &= \{v \in V \setminus \{u\}: \{u, v\} \in E\}. \end{aligned}$$

Nach dem Schubfachprinzip ist  $|A| \geq n_1$  oder  $|B| \geq n_2$ . Wenn  $|A| \geq n_1$ , verwenden wir die Induktionsvoraussetzung für das Paar  $(k, \ell - 1)$ . Laut dieser gilt für den Graphen  $G_A$ , der von der Menge  $A$  induziert ist,  $\omega(G_A) \geq k$  oder  $\alpha(G_A) \geq \ell - 1$ . Im ersten Fall haben wir  $\omega(G) \geq k$ . Im zweiten Fall bildet jede unabhängige Menge  $I \subset A$  zusammen mit der Ecke  $u$  wieder eine unabhängige Menge  $I \cup \{u\}$  in  $G$ , und somit ist  $\alpha(G) \geq \alpha(G_A) + 1 \geq \ell$ .

Der Fall  $|B| \geq n_2$  geht ganz genauso, wieder erhalten wir, dass  $\omega(G) \geq k$  oder  $\alpha(G) \geq \ell$ . Damit ist der Induktionsschritt beendet.  $\square$

Der eben bewiesene Satz erlaubt uns folgende Definition:  $r(k, \ell)$  bezeichne die kleinste natürliche Zahl  $n$ , für die jeder Graph  $G$  auf  $n$  Ecken Cliquenzahl  $\omega(G) \geq k$  oder Unabhängigkeitszahl  $\alpha(G) \geq \ell$  hat. Die Zahlen  $r(k, \ell)$  heißen *Ramsey-Zahlen*. Der Satz von Ramsey

für Graphen sichert die Existenz von  $r(k, \ell)$  für jedes  $k \geq 1$  und jedes  $\ell \geq 1$ .

Die Ramsey–Zahlen, die wir schon bestimmt haben oder die sich leicht bestimmen lassen, sind:

$$\begin{aligned} r(1, \ell) &= 1, & r(k, 1) &= 1 \\ r(2, \ell) &= \ell, & r(k, 2) &= k \\ r(3, 3) &= 6. \end{aligned}$$

Es ist nur eine Handvoll weiterer Werte bekannt. Man weiß z.B., dass  $r(4, 4) = 18$ , doch schon der Wert von  $r(5, 5)$  ist trotz beträchtlichen Anstrengungen bis heute unbekannt.

Im nächsten Abschnitt zeigen wir eine untere Schranke für  $r(k, k)$ .

## Aufgaben

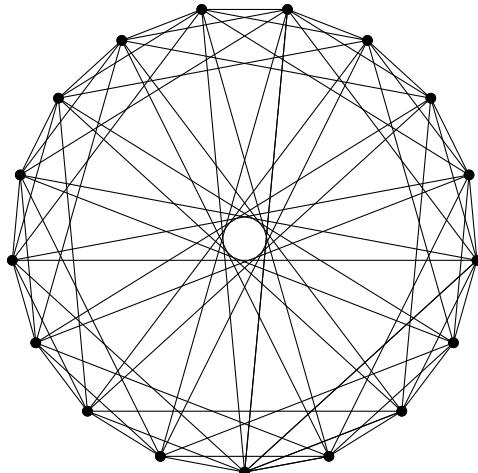
1. (a) Folgern Sie aus Satz 11.2.1, dass es zu jedem  $n$  ein  $N$  mit folgender Eigenschaft gibt: Ist  $X$  eine Menge mit  $N$  Elementen und ist  $\binom{X}{2}$  in zwei Teilmengen  $E_1$  und  $E_2$  partitioniert, dann enthält mindestens einer der Graphen  $(X, E_1)$  und  $(X, E_2)$  einen vollständigen Teilgraphen auf  $n$  Ecken.  
 (b) \*Verallgemeinern Sie die Aussage in (a) auf Partitionen von  $\binom{X}{2}$  in  $r$  Teile und beweisen Sie diese Verallgemeinerung. (Hinweis: Induktion über  $r$ .)
2. Sei  $G$  ein Graph. Wir schreiben  $f(G) = \alpha(G) \cdot \omega(G)$  und definieren  $f(n) = \min f(G)$ , wobei das Minimum über alle Graphen mit  $n$  Ecken genommen wird.
  - (a) Beweisen Sie, dass für  $n \in \{1, 2, 3, 4, 6\}$  gilt:  $f(n) \geq n$ .
  - (b) Beweisen Sie, dass  $f(5) < 5$ .
  - (c)\* Für natürliche Zahlen  $n, k$ ,  $1 < k \leq n/2$ , definieren wir einen Graphen  $C_{n,k}$ : Wir beginnen mit  $C_n$ , dem Kreis der Länge  $n$ , und dann verbinden wir all jene Eckenpaare mit einer Kante, die in  $C_n$  höchstens den Abstand  $k$  haben. Verwenden Sie diese Graphen (wählen Sie  $k$  geschickt!) zum Beweis, dass  $f(n) < n$  für alle  $n \geq 7$ .
3. Zeigen Sie, dass die Funktion  $f(n)$  aus Aufgabe 2 nicht fallend und nach oben unbeschränkt ist.
4. Beweisen Sie, dass aus  $k \leq k'$  und  $\ell \leq \ell'$  folgt, dass  $r(k, \ell) \leq r(k', \ell')$ .
5. \*\*Verstehen und beweisen Sie die folgende Verallgemeinerung des Satzes von Ramsey. *Für je drei natürliche Zahlen  $p, r, n$  gibt es eine Zahl  $N$  mit folgender Eigenschaft: Wenn  $X$  eine beliebige Menge mit mindestens  $N$  Elementen ist und wenn  $\binom{X}{p} = A_1 \cup A_2 \cup \dots \cup A_r$  eine*

beliebige Partition der Menge aller  $p$ -Tupel von Elementen aus  $X$  ist, dann gibt es eine  $n$ -elementige Menge  $Y \subseteq X$ , so dass  $\binom{Y}{p}$  vollständig in einer der Klassen  $A_i$  enthalten ist. (Hinweis: Induktion über  $p$ .)

## 11.3 Eine untere Schranke für die Ramsey-Zahlen

In diesem Abschnitt gelangen wir zu einer der grundlegenden Eigenschaften der Ramsey-Zahlen, die wesentlich ist für ihre Untersuchung und für Anwendungen des Satzes von Ramsey. Wir zeigen, dass die Zahl  $r(k, k)$ , die wir hier mit  $r(k)$  abkürzen, exponentiell wächst. (Wir merken an, dass man bei Verallgemeinerungen, die wir hier aber nicht besprechen wollen, durchaus Funktionen erhält, die noch wesentlich schneller wachsen.) Bevor wir das Resultat formulieren und beweisen, machen wir uns bewusst, was es bedeutet, eine untere Schranke für  $r(k)$  zu beweisen: Wenn wir behaupten, dass  $r(k) > n$ , dann behaupten wir die Existenz eines Graphen  $G$  auf  $n$  Ecken, für den  $\omega(G) < k$  und  $\alpha(G) < k$ . (Insbesondere genügt es nicht zu prüfen, dass  $n < \binom{2k-2}{k-1}$ , denn der Ausdruck  $\binom{2k-2}{k-1}$  aus Satz 11.2.1 ist lediglich eine obere Schranke für  $r(k)$ , der wahre Wert könnte viel kleiner sein!)

Im vorigen Abschnitt haben wir z.B. mit Hilfe des Graphen  $C_5$  gezeigt, dass  $r(3) > 5$ . Wir haben auch erwähnt (aber nicht bewiesen), dass  $r(4) = 18$ . Die Ungleichung  $r(4) > 17$  kann man mittels folgendem Graphen beweisen:



Interessanterweise sind die Graphen für  $r(3) > 5$  und für  $r(4) > 17$  beide (bis auf Isomorphie) eindeutig bestimmt. Dies deutet dar-

auf hin, dass das Problem, die Ramsey–Zahlen nach unten zu beschränken, inhärent schwierig ist.

Hier beweisen wir eine untere Schranke für  $r(k)$  mit der probabilistischen Methode, deren Funktionsweise in Kapitel 10 erklärt ist. Dieser Beweis war einer der ersten kombinatorischen Beweise mit der probabilistischen Methode.

**11.3.1 Satz.** *Es seien  $k$  und  $n$  natürliche Zahlen mit  $\binom{n}{k} \cdot 2^{1-\binom{k}{2}} < 1$ . Dann ist  $r(k) > n$ .*

Welche Zahlen  $k$  und  $n$  erfüllen die Bedingungen des Satzes? Wie bei der probabilistischen Methode üblich, verwenden wir recht grobe, einfache Abschätzungen:

$$\binom{n}{k} \leq \frac{n^k}{k!} < \frac{n^k}{2^{k/2+1}}$$

(die zweite Ungleichung gilt erst ab  $k \geq 3$ ). Wir merken an, dass die Verwendung der genaueren Abschätzungen aus Kapitel 3 nicht viel bringen würde. Der Ausdruck aus Satz 11.3.1 ist also wie folgt beschränkt:

$$\binom{n}{k} \cdot 2^{1-\binom{k}{2}} < \frac{n^k}{2^{k/2+1}} \cdot 2^{1-k(k-1)/2} = \left(\frac{n}{2^{k/2}}\right)^k.$$

Die Bedingung des Satzes ist für  $n = 2^{k/2}$  erfüllt, und wir folgern:

**11.3.2 Folgerung.** *Für alle  $k \geq 3$  gilt  $r(k) > 2^{k/2}$ .*

Diese Ungleichung gilt auch für  $k = 2$ , doch dies folgt nicht aus den obigen Abschätzungen.

**Beweis von Satz 11.3.1.** Wie in Kapitel 10 betrachten wir einen Zufallsgraphen  $G$  auf der Eckenmenge  $V = \{1, \dots, n\}$ , der jede der  $\binom{n}{2}$  potentiellen Kanten mit Wahrscheinlichkeit  $\frac{1}{2}$  enthält, unabhängig von den anderen Kanten.

Sei  $K$  eine beliebige  $k$ -elementige Teilmenge von  $V$ . Mit  $A_K$  bezeichnen wir das Ereignis „die Ecken aus  $K$  induzieren einen vollständigen Teilgraphen  $G$ “. Die Wahrscheinlichkeit  $P(A_K)$  von  $A_K$  ist  $2^{-\binom{k}{2}}$ . Bezeichnen wir analog das Ereignis „die Ecken von  $K$  bilden eine unabhängige Menge in  $G$ “ mit  $B_K$ , dann ist auch  $P(B_K) = 2^{-\binom{k}{2}}$ . Die Wahrscheinlichkeit des Ereignisses  $C_K = A_K \cup B_K$  (d.h.  $K$  induziert entweder einen vollständigen Teilgraph oder eine unabhängige Menge) ist  $2 \cdot 2^{-\binom{k}{2}} = 2^{1-\binom{k}{2}}$ . Die Wahrscheinlichkeit,

dass es eine  $k$ -elementige Teilmenge  $K \subseteq V$  gibt, für die  $C_K$  gilt, nennen wir  $p$ . Diese Wahrscheinlichkeit ist nicht so einfach zu bestimmen, weil die Ereignisse  $C_K$  im Allgemeinen nicht unabhängig sind. Doch für unsere Zwecke genügt es,  $p$  durch die Summe der Wahrscheinlichkeiten aller  $C_K$  nach oben abzuschätzen.

$$p \leq \sum_{K \subseteq V, |K|=k} P(C_K)$$

(die Summe läuft über alle  $k$ -elementigen Teilmengen der  $n$ -elementigen Menge  $V$ ). So erhalten wir  $p \leq \binom{n}{k} \cdot 2^{1-\binom{k}{2}}$ , und somit garantiert die Anahme des Satzes, dass  $p < 1$ . Doch dies bedeutet, dass es *mindestens einen* Graphen auf  $V$  geben muss, für den sowohl  $\alpha$  als auch  $\omega$  kleiner als  $k$  sind.  $\square$

Wir merken an, dass dieser Beweis nicht den geringsten Hinweis darauf gibt, wie man einen Graphen konstruieren könnte, der die Ungleichung  $r(k) > 2^{\frac{k}{2}}$  belegt. Schlimmer noch: Obwohl Erdős diesen berühmten Beweis bereits 1947 entdeckt hat, ist bis zum heutigen Tag keine Konstruktion solcher Graphen bekannt. Diese untere Schranke für Ramsey-Zahlen bleibt ein eindrucksvoller Beleg für die Leistungsfähigkeit der probabilistischen Methode.

## Aufgaben

1. Beweisen Sie, dass  $\sqrt{2} \leq \sqrt[k]{r(k)} \leq 4$  (für alle  $k \geq 2$ ).
2. Konstruieren Sie einen Graphen  $G$ , der belegt, dass  $r(k) \geq (k-1)^2$ .
3. Der Graph oben für  $r(4) > 17$  sieht kompliziert aus, aber eigentlich kann man ihn sich leicht merken. Z.B. kann man sich einfach 17; 1, 2, 4, 8 merken. Oder dies: Quadratische Reste modulo 17. Können Sie diese etwas kryptischen Merkhilfen erklären?
4. Beweisen Sie  $r(4) = 18$ . Betrachten Sie dazu das Beispiel aus dem Text und „verbessern“ Sie den Beweis von Satz 11.2.1.

# 12

# Erzeugende Funktionen

---

In diesem Kapitel stellen wir eine sehr nützliche Technik vor. Die zu Grunde liegende Idee ist erst einmal überraschend: Wollen wir eine unendliche Folge reeller Zahlen untersuchen, dann assoziieren wir mit ihr eine stetige Funktion, die so genannte erzeugende Funktion der Folge. Fragen über unendlich viele Folgenglieder kann man dann anhand eines einzigen Objektes studieren.

In dieser Einführung kommen wir nur zu relativ einfachen Beispielen, von denen man die meisten auch ohne erzeugende Funktionen lösen kann. In einigen Fällen lässt sich das Ziel sogar schneller erreichen, wenn man den richtigen Trick kennt, als mit erzeugenden Funktionen (es ist allerdings nicht immer leicht, diese Tricks zu finden). Diese Tatsache sollte Sie jedoch nicht entmutigen, die Methode der erzeugenden Funktionen zu erlernen, denn mit ihr lassen sich auch schwierigere Probleme lösen, bei denen andere Methoden versagen (oder viel zu kompliziert werden).

Bei einigen Lösungen erwähnen wir alternative Methoden, bei anderen deuten wir sie in den Aufgaben an. Es wird vielleicht auch vorkommen, dass Ihnen eine noch einfachere Lösung in den Sinn kommt.

## 12.1 Polynome

Wie multiplizieren wir die Polynome  $p(x) = x + x^2 + x^3 + x^4$  und  $q(x) = x + x^3 + x^4$ ? Hier ist eine einfache Regel: Multipliziere jeden Term von  $p(x)$  mit jedem Term von  $q(x)$  und addiere alle diese Produkte. Das Addieren dieser Produkte ist einfach, weil alle den Koeffizienten 1 haben. So berechnen wir, dass  $p(x)q(x) = x^8 + 2x^7 + 2x^6 + 3x^5 + 2x^4 + x^3 + x^2$ .

Eine andere Frage: Wir suchen uns eine bestimmte Potenz von  $x$  aus, etwa  $x^5$ , und möchten ihren Koeffizienten in  $p(x)q(x)$  wissen, ohne das ganze Produkt ausrechnen zu müssen. In unserem Beispiel entsteht  $x^5$  durch Multiplikation des Terms  $x$  aus  $p(x)$  mit  $x^4$  aus  $q(x)$ , durch Multiplikation von  $x^2$  aus  $p(x)$  mit  $x^3$  aus  $q(x)$  und

schließlich durch Multiplikation von  $x^4$  aus  $p(x)$  mit  $x$  aus  $q(x)$ . Jede dieser Möglichkeiten trägt 1 zum gesuchten Koeffizienten bei, also ist der Koeffizient von  $x^5$  im Produkt  $p(x)q(x)$  gleich 3.

Die Situation ist die gleiche, als hätten wir vier Silbermünzen zu 1, 2, 3 und 4 Doublezons (dies sind die Exponenten von  $x$  in dem Polynom  $p(x)$ ) und drei Goldmünzen zu 1, 3 und 4 Doublezons (entsprechend den Exponenten von  $x$  in  $q(x)$ ), und wir würden uns fragen, auf wie viele Arten wir fünf Doublezons mit einer Silber- und einer Goldmünze zählen können. Formal ist der Koeffizient von  $x^5$  die Anzahl geordneter Paare  $(i, j)$  mit  $i + j = 5$ ,  $i \in \{1, 2, 3, 4\}$  und  $j \in \{1, 3, 4\}$ .

Wir formulieren die eben für die zwei konkreten Polynome angestellten Betrachtungen nun allgemeiner. Seien  $I$  und  $J$  endliche Mengen natürlicher Zahlen. Wir bilden die Polynome  $p(x) = \sum_{i \in I} x^i$  und  $q(x) = \sum_{j \in J} x^j$  (beachten Sie, dass die Koeffizienten in solchen Polynomen 0 oder 1 sind). Dann ist für jede natürliche Zahl  $r$  die Anzahl der Lösungen  $(i, j)$  der Gleichung

$$i + j = r$$

mit  $i \in I$  und  $j \in J$  gleich dem Koeffizienten von  $x^r$  im Produkt  $p(x)q(x)$ .

Noch interessanter ist die Verallgemeinerung dieser Beobachtung auf Produkte von drei oder mehr Polynomen. Wir wollen das Vorgehen an einem Beispiel illustrieren.

**Problem.** Auf wie viele Arten können wir einen Betrag von 21 Doublezons zählen, wenn wir 6 Ein-Doublezon-Münzen, 5 Zwei-Doublezon-Münzen und 4 Fünf-Doublezon-Münzen haben?

**Lösung.** Die gesuchte Zahl ist gleich der Anzahl der Lösungen der Gleichung

$$i_1 + i_2 + i_3 = 21$$

mit

$$i_1 \in \{0, 1, 2, 3, 4, 5, 6\}, \quad i_2 \in \{0, 2, 4, 6, 8, 10\}, \quad i_3 \in \{0, 5, 10, 15, 20\}.$$

Dabei steht  $i_1$  für den in Ein-Doublezon-Münzen gezahlten Betrag,  $i_2$  für den in Zwei-Doublezon-Münzen gezahlten und  $i_3$  für den in Fünf-Doublezon-Münzen gezahlten.

Wir behaupten, dass die Anzahl der Lösungen dieser Gleichung gerade der Koeffizient von  $x^{21}$  in dem Produkt

$$(1 + x + x^2 + x^3 + \cdots + x^6)(1 + x^2 + x^4 + x^6 + x^8 + x^{10}) \\ \times (1 + x^5 + x^{10} + x^{15} + x^{20})$$

ist (nach Ausmultiplizieren der Klammern und Zusammenfassen der Terme mit gleichen Exponenten). Und wirklich, die Terme mit  $x^{21}$  erhält man, indem man ein  $x^{i_1}$  aus der ersten Klammer nimmt, ein  $x^{i_2}$  aus der zweiten und ein  $x^{i_3}$  aus der dritten, und zwar so, dass  $i_1 + i_2 + i_3 = 21$ . Jede mögliche Kombination von  $i_1$ ,  $i_2$  und  $i_3$  mit dieser Eigenschaft trägt 1 zu dem Koeffizienten von  $x^{21}$  in dem betrachteten Produkt bei.

Wie hilft uns das bei der Lösung unseres Problems? Ganz praktisch:

Das erlaubt uns die Antwort einfach mit einem Computer auszurechnen, wenn wir ein Programm haben, das Polynome multiplizieren kann. Ganz genau so haben die Autoren das Ergebnis bestimmt: Es ist 9. Weil in unserem Beispiel nur relativ wenige Münzen vorkommen, könnten wir die Lösung auch direkt durch Auflisten aller Möglichkeiten bestimmen, doch wie leicht vertut man sich und vergisst eine. Wie dem auch sei, die eben vorgestellte Methode ist nur ein Anfang — man bekommt auf ähnliche Art auch viel kompliziertere Situationen in den Griff.

### Eine kombinatorische Interpretation des Binomialsatzes.

Der Binomialsatz besagt, dass

$$(1 + x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n. \quad (12.1)$$

Auf der linken Seite steht ein Produkt von  $n$  Polynomen, jedes von ihnen ist  $1 + x$ . Genauso wie bei den obigen Betrachtungen mit Münzen ist der Koeffizient von  $x^r$  in dem Ausdruck  $(1 + x)^n$  (nach Ausmultiplizieren der Klammern) gleich der Anzahl Lösungen der Gleichung

$$i_1 + i_2 + \cdots + i_n = r$$

mit  $i_1, i_2, \dots, i_n \in \{0, 1\}$ . Jede Lösung dieser Gleichung entspricht eindeutig einer Auswahl von  $r$  der Variablen  $i_1, i_2, \dots, i_n$ , die den Wert 1 haben — die restlichen  $n - r$  müssen 0 sein. Davon gibt es genauso viele wie  $r$ -elementige Teilmengen in einer  $n$ -Menge, also  $\binom{n}{r}$ . Das bedeutet aber, dass der Koeffizient von  $x^r$  in dem Produkt  $(1 + x)^n$  wie behauptet  $\binom{n}{r}$  ist. Das ist ein kombinatorischer Beweis des Binomialsatzes!

Wenn wir mit Polynomen wie  $(1 + x)^n$  geschickt herumspielen, können wir diverse Identitäten und Formeln mit Binomialkoeffizienten herleiten. Einfache Beispiele haben wir schon in Abschnitt 3.3 gesehen, nämlich die Formeln  $\sum_{k=0}^n \binom{n}{k} = 2^n$  und  $\sum_{k=0}^n (-1)^k \binom{n}{k} = 0$ , die man durch Einsetzen von  $x = 1$  bzw.  $x = -1$  in (12.1) erhält.

Für das nächste Beispiel sollten Sie mit dem Begriff der Ableitung (eines Polynoms) vertraut sein.

**12.1.1 Beispiel.** Für alle  $n \geq 1$  ist

$$\sum_{k=0}^n k \binom{n}{k} = n2^{n-1}.$$

*Beweis.* Diese Gleichung kann man beweisen, indem man beide Seiten von Formel (12.1) differenziert (nach der Variablen  $x$ ). Hinterher muss weiterhin Gleichheit gelten. Differenzieren der linken Seite ergibt  $n(1 + x)^{n-1}$ , Differenzieren der rechten Seite  $\sum_{k=0}^n k \binom{n}{k} x^{k-1}$ . Setzen wir dann  $x = 1$  ein, erhalten wir die behauptete Identität.  $\square$

Ein Beispiel anderen Typs beruht darauf, dass die Koeffizienten in zwei verschiedenen Ausdrücken für ein und dasselbe Polynom die gleichen sein müssen.

*Noch ein Beweis von Hilfssatz 3.3.4.* Wir möchten die Gleichung

$$\sum_{i=0}^n \binom{n}{i}^2 = \binom{2n}{n}$$

beweisen. Dazu betrachten wir die Identität

$$(1 + x)^n (1 + x)^n = (1 + x)^{2n}.$$

Der Koeffizient von  $x^n$  auf der rechten Seite ist nach dem Binomialssatz  $\binom{2n}{n}$ . Auf der linken Seite können wir beide Potenzen  $(1 + x)^n$  mit dem Binomialsatz ausrechnen und dann die Ergebnisse miteinander multiplizieren. Der Koeffizient von  $x^n$  in diesem Produkt lässt sich als  $\binom{n}{0} \binom{n}{n} + \binom{n}{1} \binom{n}{n-1} + \binom{n}{2} \binom{n}{n-2} + \cdots + \binom{n}{n} \binom{n}{0}$  ausdrücken, und das muss die gleiche Zahl sein wie der Koeffizient von  $x^n$  auf der rechten Seite. So erhalten wir

$$\sum_{i=0}^n \binom{n}{i} \binom{n}{n-i} = \binom{2n}{n}.$$

Damit ist Hilfssatz 3.3.4 nochmals auf andere Art bewiesen.  $\square$

Eine Reihe anderer Summen und Formeln bekommt man ähnlich in den Griff. Doch wenn wir kompliziertere Berechnungen versuchen, dann wird die Einschränkung bald störend, dass unsere Polynome nur endlich viele Terme haben können. Es stellt sich heraus, dass das „richtige“ Werkzeug für diese Art Berechnungen verallgemeinerte Polynome sind, in denen unendlich viele Potenzen von  $x$  vorkommen dürfen, so genannte Potenzreihen. Diese sind Thema des nächsten Abschnitts.

## Aufgaben

- Seien  $a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$  und  $b(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$  zwei Polynome. Schreiben Sie eine Formel für den Koeffizienten von  $x^k$  in dem Produkt  $a(x)b(x)$  auf ( $0 \leq k \leq n+m$ ).
- Ein Bäcker verkauft drei Sorten Schnecken — Zuckerschnecken, Mohnschnecken und Streuselschnecken. Wie viele Möglichkeiten gibt es zwölf Schnecken zu kaufen, wenn Sie mindestens zwei von jeder Sorte mitbringen sollen, aber nicht mehr als drei Mohnschnecken? Drücken Sie die gesuchte Anzahl als Koeffizienten einer geeigneten Potenz von  $x$  in einem Produkt von Polynomen aus.
- Auf wieviele Arten kann man 10 identische Bälle an zwei Jungen und zwei Mädchen verschenken, wenn jeder Junge mindestens einen Ball und jedes Mädchen mindestens zwei Bälle erhalten soll? Drücken Sie die Antwort als Koeffizienten einer Potenz von  $x$  in einem geeigneten Produkt von Polynomen aus.
- Beweisen Sie den Multinomialsatz 3.3.5 auf ähnliche Weise, wie wir oben im Text den Binomialsatz bewiesen haben.
- Berechnen Sie die Summe in Beispiel 12.1.1 mit einer geschickten Umformung des Ausdrucks  $k \binom{n}{k}$  und dem Binomialsatz.
- Berechnen Sie die Summe  $\sum_{i=0}^n (-1)^i \binom{n}{i} \binom{n}{n-i}$ .

## 12.2 Potenzreihen

**Eigenschaften von Potenzreihen.** Eine *Potenzreihe* ist eine unendliche Reihe der Form  $a_0 + a_1x + a_2x^2 + \cdots$ , wobei  $a_0, a_1, a_2, \dots$  reelle Zahlen sind und  $x$  eine Variable ist, die als Werte reelle Zahlen annimmt.<sup>1</sup> Diese Potenzreihe bezeichnen wir gewöhnlich mit  $a(x)$ .

---

<sup>1</sup>Es ist oft sehr praktisch, auch komplexe Werte für  $x$  zuzulassen und Methoden der Funktionentheorie anzuwenden. Doch so weit werden wir in dieser Einführung nicht kommen.

Ein einfaches Beispiel für eine Potenzreihe ist

$$1 + x + x^2 + x^3 + \dots \quad (12.2)$$

(alle  $a_i$  sind 1). Ist  $x$  eine reelle Zahl im Intervall  $(-1, 1)$ , dann konvergiert diese Reihe und ihre Summe ist gleich  $\frac{1}{1-x}$  (dies ist die bekannte Formel für die Summe einer unendlichen geometrischen Reihe; ist sie Ihnen nicht vertraut, dann sollten Sie sich auf jeden Fall einmal Aufgabe 1 anschauen). In diesem Sinn bestimmt die Reihe (12.2) die Funktion  $\frac{1}{1-x}$ . Umgekehrt enthält diese Funktion die gesamte Information über die Reihe (12.2). Wenn wir nämlich die Funktion  $k$ -mal ableiten und im Ergebnis  $x = 0$  setzen, dann erhalten wir gerade das  $k$ !-fache des Koeffizienten von  $x^k$ . Mit anderen Worten, die Reihe (12.2) ist die Taylorentwicklung der Funktion  $\frac{1}{1-x}$  bei  $x = 0$ . Insofern kann man die Funktion  $\frac{1}{1-x}$  als Inkarnation der unendlichen Folge  $(1, 1, 1, \dots)$  ansehen und umgekehrt. Diese Verwandlung unendlicher Folgen in Funktionen und wieder zurück ist ein wesentlicher Schritt, wenn man mit erzeugenden Funktionen arbeitet.

Wenn wir im Folgenden erklären, was erzeugende Funktionen sind, müssen wir auf einige elementare Konzepte aus der Analysis zurückgreifen (Konvergenz unendlicher Reihen, Ableitung, Taylorreihe), wie wir es in dem Beispiel eben schon getan haben. Wenn Sie nicht genügend Analysis können um diese Einführung zu verstehen, müssen Sie aber nicht gleich aufgeben, denn bei der Anwendung erzeugender Funktionen braucht man in der Regel fast gar keine Analysis. Sie sollten dann jedoch bereit sein, als gegeben hinzunehmen, dass die unendliche Reihe  $1 + x + x^2 + \dots$  und die Funktion  $\frac{1}{1-x}$  das gleiche Objekt darstellen. Dies können Sie ebenso wie die anderen Tatsachen, die wir hier auflisten, in Ihren Rechnungen verwenden.

Der folgende Hilfssatz sagt uns, dass bei Folgen  $(a_0, a_1, a_2, \dots)$ , deren Glieder nicht allzu schnell wachsen, die zugehörige Potenzreihe  $a(x) = a_0 + a_1x + a_2x^2 + \dots$  wirklich eine Funktion in der reellen Variable  $x$  definiert, zumindest in einer kleinen Umgebung um 0. Und dass man die Folge  $(a_0, a_1, a_2, \dots)$  eindeutig rekonstruieren kann, wenn man weiß, welche Werte diese Funktion annimmt.

**12.2.1 Hilfssatz.** Sei  $(a_0, a_1, a_2, \dots)$  eine Folge reeller Zahlen. Es existiere eine reelle Zahl  $K$ , so dass  $|a_n| \leq K^n$  für alle  $n \geq 1$  gilt. Dann konvergiert die Reihe  $a(x) = \sum_{i=0}^{\infty} a_i x^i$  für jedes  $x \in (-\frac{1}{K}, \frac{1}{K})$  (sogar absolut) und definiert somit eine Funktion in der reellen Variable  $x$  auf diesem Intervall. Diese Funktion werden wir auch mit

$a(x)$  bezeichnen. Die Funktionswerte von  $a(x)$  in einer beliebig kleinen Umgebung der 0 bestimmen eindeutig alle Glieder der Folge  $(a_0, a_1, a_2, \dots)$ . Das bedeutet, die Funktion  $a(x)$  ist in 0 beliebig oft differenzierbar, und für alle  $n = 0, 1, 2, \dots$  ist

$$a_n = \frac{a^{(n)}(0)}{n!}$$

$(a^{(n)}(0)$  steht für die  $n$ -te Ableitung der Funktion  $a(x)$  bei  $x = 0$ .

Dieser Hilfssatz folgt aus elementaren Ergebnissen der Analysis, den Beweis lassen wir weg (ebenso wie die Beweise einiger anderer Resultate in diesem Abschnitt). Elegante Beweise erhält man mit Funktionentheorie (das ist die Theorie der Funktionen in komplexen Variablen), die aber meist nicht Gegenstand der Grundvorlesungen ist. Für unsere Zwecke braucht man allerdings sehr wenig, so dass man die Beweise mit einem gewissen Aufwand auch mit Hilfe elementarer Sätze über Grenzwerte und Ableitungen reeller Funktionen führen kann. In den folgenden Beispielen werden wir nicht explizit überprüfen, ob die jeweilige Potenzreihe wirklich in einer Umgebung der 0 konvergiert (d.h. ob die Voraussetzungen aus Hilfssatz 12.2.1 gegeben sind). Meist ist es leicht, und außerdem lässt es sich in vielen Fällen vermeiden: Denn wenn wir für ein Problem eine korrekte Lösung mittels erzeugenden Funktionen gefunden haben, vielleicht auch mit eher suspekten Methoden, können wir diese Lösung mit anderen Mitteln überprüfen, etwa mit vollständiger Induktion. Und schließlich sollten wir erwähnen, dass es auch eine Theorie der so genannten *formalen Potenzreihen* gibt, die es uns erlaubt, sogar mit Potenzreihen zu arbeiten, die nirgends konvergieren (außer bei 0). Konvergenz ist bei Anwendungen erzeugender Funktionen also fast nie ein Thema.

Nun können wir endlich definieren, was eine erzeugende Funktion sein soll:

**12.2.2 Definition.** Sei  $(a_0, a_1, a_2, \dots)$  eine Folge reeller Zahlen. Unter der erzeugenden Funktion dieser Folge<sup>2</sup> verstehen wir die Potenzreihe  $a(x) = a_0 + a_1x + a_2x^2 + \dots$ .

---

<sup>2</sup>In der Literatur heißt sie oft ausführlicher die *gewöhnliche erzeugende Funktion*. Das lässt darauf schließen, dass es noch andere Typen erzeugender Funktionen gibt. Wir wollen hier nur kurz die so genannte *exponentielle erzeugende Funktion* nennen, die für kombinatorische Anwendungen von besonderer Bedeutung ist. Die exponentielle erzeugende Funktion einer Folge  $(a_0, a_1, a_2, \dots)$  ist die Potenzreihe  $\sum_{i=0}^{\infty} (a_i/i!)x^i$ . Zum Beispiel hat die Folge  $(1, 1, 1, \dots)$  die exponentielle erzeugende Funktion  $e^x$ . Außer in ein paar Aufgaben beschränken wir unsere Darstellung auf gewöhnliche erzeugende Funktionen.

Hat eine Folge  $(a_0, a_1, a_2, \dots)$  nur endlich viele von Null verschiedene Glieder, dann ist ihre erzeugende Funktion ein Polynom. Im vorangegangenen Abschnitt haben wir also erzeugende Funktionen endlicher Folgen benutzt, ohne sie so zu nennen.

**Mit erzeugenden Funktionen umgehen.** In Anwendungen erzeugender Funktionen stoßen wir oft auf Fragen wie: „Was ist die erzeugende Funktion der Folge  $(1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots)$ ?“ Klar, nach Definition ist die erzeugende Funktion  $1 + \frac{1}{2}x + \frac{1}{3}x^2 + \frac{1}{4}x^3 + \dots$ , aber gibt es dafür eine handliche geschlossene Formel? Mit anderen Worten, definiert diese Potenzreihe vielleicht irgendeine Funktion, die wir kennen, z.B. aus der Analysis? (Diese hier ja, nämlich  $-\frac{\ln(1-x)}{x}$ ; siehe unten.) Die Antwort findet man oft mit ein wenig „Basteln“, wie in einer kleinen Werkstatt. Wir haben einen Grundstock an Bauteilen, in unserem Fall sind das Folgen wie  $(1, 1, 1, \dots)$ , deren erzeugende Funktion wir kennen. Und wir haben ein Repertoire einfacher Operationen mit Folgen und den entsprechenden Operationen mit erzeugenden Funktionen. Kennen wir beispielsweise die erzeugende Funktion  $a(x)$  einer Folge  $(a_0, a_1, a_2, \dots)$ , dann ist die erzeugende Funktion der Folge  $(0, a_0, a_1, a_2, \dots)$  gleich  $x a(x)$ . Mit ein wenig Geschick lässt sich die gewünschte Folge meist zurechtzimmern.

Beginnen wir nun, die ersten „Bauteile“ einzukaufen. Zu einer Grundausstattung gehören diverse Beispiele von Taylorreihen (oder Maclaurin-Reihen), die man in der Analysis-Vorlesung kennen lernt. Zum Beispiel haben wir da

$$\frac{x}{1} + \frac{x^2}{2} + \frac{x^3}{3} + \dots = -\ln(1-x) \quad (12.3)$$

(gültig für alle  $x \in (-1, 1)$ ) und

$$1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots = e^x$$

(für alle reellen  $x$ ). Jede Menge weiterer Beispiele findet man in Lehrbüchern der Analysis. Hier folgt nun ein ganz einfaches Resultat, das man besonders häufig braucht:

**12.2.3 Hilfssatz (Verallgemeinerter Binomialsatz).** Für eine beliebige reelle Zahl  $r$  und für jede nicht negative ganze Zahl  $k$  definieren wir den Binomialkoeffizienten  $\binom{r}{k}$  durch die Formel

$$\binom{r}{k} = \frac{r(r-1)(r-2)\dots(r-k+1)}{k!}$$

(insbesondere setzen wir  $\binom{r}{0} = 1$ ). Dann ist die Funktion  $(1+x)^r$  die erzeugende Funktion der Folge  $(\binom{r}{0}, \binom{r}{1}, \binom{r}{2}, \binom{r}{3}, \dots)$ . Die Potenzreihe  $\binom{r}{0} + \binom{r}{1}x + \binom{r}{2}x^2 + \dots$  konvergiert für alle  $|x| < 1$  (unabhängig vom Wert von  $r$ ).

Der Beweis gehört in die Analysis und geht ganz einfach mit der Taylorentwicklung.

Für kombinatorische Anwendungen ist es wichtig zu wissen, dass sich der Binomialkoeffizient  $\binom{r}{k}$  für negatives  $r$  durch einen „gewöhnlichen“ Binomialkoeffizienten (mit ausschließlich nicht negativen Zahlen) ausdrücken lässt:  $\binom{r}{k} = (-1)^k \binom{-r+k-1}{k} = (-1)^k \binom{-r+k-1}{-r-1}$ . Für negative (ganzzahlige) Potenzen von  $1-x$  erhalten wir

$$\frac{1}{(1-x)^n} = \binom{n-1}{n-1} + \binom{n}{n-1}x + \binom{n+1}{n-1}x^2 + \dots + \binom{n+k-1}{n-1}x^k + \dots$$

Dabei ist die Gleichung  $\frac{1}{1-x} = 1 + x + x^2 + \dots$  der Spezialfall  $n = 1$ .

**Operationen mit Folgen und den zugehörigen erzeugenden Funktionen.** Wir richten nun unsere „Werkstatt“ mit den nötigsten Operationen ein, um für das oben beschriebene „Zusammenbasteln“ erzeugender Funktionen gerüstet zu sein. Im Folgenden seien  $(a_0, a_1, a_2, \dots)$  und  $(b_0, b_1, b_2, \dots)$  Folgen und  $a(x)$  und  $b(x)$  die zugehörigen erzeugenden Funktionen.

- A. Addieren wir die Folgen gliedweise, dann ist die entsprechende Operation mit den erzeugenden Funktionen einfach die *Addition*. Die Folge  $(a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots)$  hat also die erzeugende Funktion  $a(x) + b(x)$ .
- B. Eine weitere einfache Operation ist die *Multiplikation mit einer reellen Zahl  $\alpha$* . Die Folge  $(\alpha a_0, \alpha a_1, \alpha a_2, \dots)$  hat die erzeugende Funktion  $\alpha \cdot a(x)$ .
- C. Ist  $n$  eine natürliche Zahl, dann gehört die erzeugende Funktion  $x^n a(x)$  zu der Folge

$$\underbrace{(0, 0, \dots, 0)}_{n \times}, a_0, a_1, a_2, \dots$$

Das ist sehr nützlich, wenn man die Folge um einige Stellen *nach rechts verschieben* möchte.

- D. Was tun, wenn wir die Folge *nach links verschieben* möchten, um also die erzeugende Funktion z.B. für die Folge  $(a_3, a_4, a_5, \dots)$  zu erhalten? Offensichtlich müssen wir durch  $x^3$  dividieren, doch

dürfen wir nicht vergessen zuvor die drei ersten Terme zu subtrahieren. Die korrekte erzeugende Funktion der obigen Folge ist

$$\frac{a(x) - a_0 - a_1x - a_2x^2}{x^3}.$$

- E.** *Substitution von  $\alpha x$  für  $x$ .* Sei  $\alpha$  eine feste reelle Zahl, wir betrachten die Funktion  $c(x) = a(\alpha x)$ . Dann ist  $c(x)$  die erzeugende Funktion der Folge  $(a_0, \alpha a_1, \alpha^2 a_2, \dots)$ . Zum Beispiel wissen wir, dass  $\frac{1}{1-x}$  die erzeugende Funktion der Folge mit lauter Einsen ist, und somit ist nach dieser Regel  $\frac{1}{1-2x}$  die erzeugende Funktion der Folge der Potenzen von 2:  $(1, 2, 4, 8, \dots)$ . Diese Operation verwendet man auch bei folgendem Trick, der alle Terme mit ungeradem Index in der betrachteten Folge durch 0 ersetzt: Wie man leicht sieht, gehört die Funktion  $\frac{1}{2}(a(x) + a(-x))$  zur Folge  $(a_0, 0, a_2, 0, a_4, 0, \dots)$ .
- F.** Eine andere Möglichkeit ist  $x^n$  für  $x$  zu substituieren. Damit erhält man die erzeugende Funktion der Folge, in der beim Index  $nk$  das  $k$ -te Glied der ursprünglichen Folge steht, und deren andere Glieder alle 0 sind. Die Funktion  $a(x^3)$  produziert z.B. die Folge  $(a_0, 0, 0, a_1, 0, 0, a_2, 0, 0, \dots)$ . Eine gemeinsame Verallgemeinerung von E und F ist, für  $x$  gleich eine ganze Potenzreihe einzusetzen. Dafür werden wir nur einige wenige Beispiele in den Übungen sehen.

Probieren wir doch einmal ein paar der zusammengetragenen Operationen aus.

**Problem.** Was ist die erzeugende Funktion der Folge

$$(1, 1, 2, 2, 4, 4, 8, 8, \dots),$$

d.h.  $a_n = 2^{\lfloor n/2 \rfloor}$ ?

**Lösung.** Wie wir in E gesehen haben, hat die Folge  $(1, 2, 4, 8, \dots)$  die erzeugende Funktion  $1/(1-2x)$ . Aus F erhalten wir die erzeugende Funktion  $1/(1-2x^2)$  für die Folge  $(1, 0, 2, 0, 4, 0, \dots)$ , und aus C die erzeugende Funktion  $x/(1-2x^2)$  für die Folge  $(0, 1, 0, 2, 0, \dots)$ . Durch Addition erhalten wir schließlich die erzeugende Funktion für die gegebene Folge; die Antwort ist also  $(1+x)/(1-2x^2)$ .  $\square$

- G.** Die üblichen Operationen aus der Analysis, *Ableiten* und *Integrieren* erzeugender Funktionen, haben natürlich auch eine Bedeutung in der Sprache der Folgen. Die Ableitung  $a'(x)$  der Funktion  $a(x)$  gehört zu der Folge

$$(a_1, 2a_2, 3a_3, \dots).$$

Mit anderen Worten ist das  $k$ -te Glied  $(k+1)a_{k+1}$  (Potenzreihen werden genau wie Polynome Term für Term abgeleitet). Entsprechend liefert die erzeugende Funktion  $\int_0^x a(t)dt$  die Folge  $(0, a_0, \frac{1}{2}a_1, \frac{1}{3}a_2, \frac{1}{4}a_3, \dots)$ ; das heißt, für alle  $k \geq 1$  ist das  $k$ -te Folgenglied gleich  $\frac{1}{k}a_{k-1}$ . So kann man zum Beispiel die Potenzreihe (12.3) für  $\ln(1-x)$  durch Integration der Funktion  $\frac{1}{1-x}$  herleiten.

Hier ein Beispiel, bei dem man mit Ableiten weiterkommt:

**12.2.4 Problem.** Gesucht ist die erzeugende Funktion für die Folge  $(1^2, 2^2, 3^2, \dots)$  der Quadratzahlen, d.h. für die Folge  $(a_0, a_1, a_2, \dots)$  mit  $a_k = (k+1)^2$ .

**Lösung.** Wir beginnen mit der All-1-Folge mit der erzeugenden Funktion  $\frac{1}{1-x}$ . Die erste Ableitung dieser Funktion,  $1/(1-x)^2$ , ergibt wegen G die Folge  $(1, 2, 3, 4, \dots)$ . Die zweite Ableitung ist  $2/(1-x)^3$ , und ihre Folge ist  $(2 \cdot 1, 3 \cdot 2, 4 \cdot 3, \dots)$ , wieder wegen G; das Glied mit Index  $k$  ist  $(k+2)(k+1) = (k+1)^2 + k + 1$ . Doch wir suchen  $a_k = (k+1)^2$ , deshalb subtrahieren wir noch die erzeugende Funktion der Folge  $(1, 2, 3, \dots)$ . So erhalten wir

$$a(x) = \frac{2}{(1-x)^3} - \frac{1}{(1-x)^2}.$$

□

**H.** Die letzte Operation in unserer Sammlung ist wohl die interessanteste: *Multiplikation erzeugender Funktionen*. Das Produkt  $a(x)b(x)$  ist die erzeugende Funktion der Folge  $(c_0, c_1, c_2, \dots)$ , deren Glieder  $c_k$  durch die Gleichungen

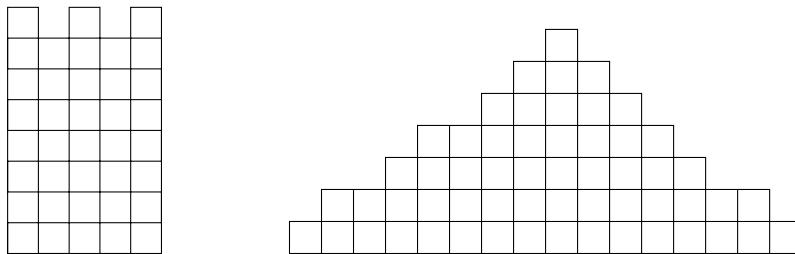
$$\begin{aligned} c_0 &= a_0 b_0 \\ c_1 &= a_0 b_1 + a_1 b_0 \\ c_2 &= a_0 b_2 + a_1 b_1 + a_2 b_0 \\ &\vdots \end{aligned}$$

gegeben sind; allgemein aufgeschrieben:

$$c_k = \sum_{i,j \geq 0: i+j=k} a_i b_j. \quad (12.4)$$

Das merkt sich leicht — die Terme in dem Produkt  $a(x)b(x)$  sind bis zum  $k$ -ten die gleichen wie im Produkt der Polynome  $(a_0 + a_1 x + \dots + a_k x^k)$  und  $(b_0 + b_1 x + \dots + b_k x^k)$ .

Die Multiplikation erzeugender Funktionen besitzt eine kombinatorische Interpretation, die wir fürs Erste anhand eines etwas kindischen Beispiels erklären wollen. Ein vernünftiges Beispiel kommt in Abschnitt 12.4. Angenommen, wir haben eine Kiste voller Bauklötze, alles ununterscheidbare Holzwürfel, und uns ist bekannt, dass es  $a_i$  verschiedene Möglichkeiten gibt einen Turm aus  $i$  Würfeln zu bauen,  $i = 0, 1, 2, \dots$ , und dass es  $b_j$  Möglichkeiten gibt eine Pyramide aus  $j$  Würfeln zu bauen,  $j = 0, 1, 2, \dots$ .



Wenn wir nun aus insgesamt  $k$  Bausteinen gleichzeitig einen Turm und eine Pyramide bauen wollen, dann geht das auf  $c_k = a_0b_k + a_1b_{k-1} + \dots + a_kb_0$  Arten (vorausgesetzt, der Turm und die Pyramide dürfen keine Bausteine gemeinsam benutzen). Kurz gesagt, die erzeugende Funktion für die Anzahl der geordneten Paare (Turm, Pyramide) erhält man als das Produkt der erzeugenden Funktionen für die Anzahl der Türme und für die Anzahl der Pyramiden.

**Bemerkung.** Die oben aufgeführten Operationen sind nicht nur dann nützlich, wenn wir zu einer vorgegebenen Folge die erzeugende Funktion suchen, sondern oft auch für die umgekehrte Aufgabe, zu einer gegebenen erzeugenden Funktion die zugehörige Folge zu finden. Im Prinzip kann man die Folge bestimmen, indem man die Taylorreihe berechnet (das sagt Hilfssatz 12.2.1), d.h. durch wiederholtes Ableiten. In der Praxis ist das jedoch selten eine geschickte Methode.

Wir schließen diesen Abschnitt mit einer Anwendung erzeugender Funktionen. Weitere Beispiele finden Sie in den Aufgaben, einige knifflige Probleme auch in den folgenden Abschnitten.

**Problem.** Eine Kiste enthält 30 rote, 40 blaue und 50 weiße Kugeln; gleichfarbige Kugeln sind nicht zu unterscheiden. Auf wie viele Arten kann man der Kiste 70 Bälle entnehmen?

**Lösung.** Gewappnet mit den Ergebnissen aus Abschnitt 12.1 finden wir, dass die gesuchte Zahl gleich dem Koeffizienten von  $x^{70}$  in dem Produkt

$$(1 + x + x^2 + \cdots + x^{30})(1 + x + x^2 + \cdots + x^{40})(1 + x + x^2 + \cdots + x^{50})$$

ist. Das brauchen wir nicht auszumultiplizieren. Besser ist es, die Faktoren anders zu schreiben:

$$1 + x + x^2 + \cdots + x^{30} = \frac{1 - x^{31}}{1 - x}. \quad (12.5)$$

Das ist die bekannte Formel für die Summe der ersten  $n$  Glieder einer geometrischen Reihe. Wenn Sie sich nicht mehr daran erinnern, können Sie sich wie folgt behelfen. Beginnen Sie mit der erzeugenden Funktion der Folge  $(1, 1, 1, \dots)$ , die ist  $\frac{1}{1-x}$ , und subtrahieren Sie davon die erzeugende Funktion der Folge

$$\underbrace{(0, 0, \dots, 0)}_{31 \times}, 1, 1, \dots,$$

die ist  $x^{31}/(1-x)$ , wie wir oben in Punkt C festgestellt haben. Das Ergebnis ist  $(1 - x^{31})/(1 - x)$ , die erzeugende Funktion der Folge

$$\underbrace{(1, 1, \dots, 1)}_{31 \times}, 0, 0, \dots.$$

So sieht man, dass (12.5) gilt.

Damit können wir nun das ganze Produkt anders schreiben:

$$\frac{1 - x^{31}}{1 - x} \cdot \frac{1 - x^{41}}{1 - x} \cdot \frac{1 - x^{51}}{1 - x} = \frac{1}{(1 - x)^3} (1 - x^{31})(1 - x^{41})(1 - x^{51}).$$

Den Faktor  $(1 - x)^{-3}$  bekommt man mit dem verallgemeinerten Binomialsatz 12.2.3 in den Griff. Im Produkt der übrigen Faktoren  $(1 - x^{31})(1 - x^{41})(1 - x^{51})$  genügt es, die Koeffizienten der Potenzen bis  $x^{70}$  zu bestimmen, was recht einfach ist. Wir erhalten

$$\left( \binom{2}{2} + \binom{3}{2}x + \binom{4}{2}x^2 + \cdots \right) (1 - x^{31} - x^{41} - x^{51} + \cdots),$$

wobei die Pünktchen  $\cdots$  in der zweiten Klammer für Potenzen über  $x^{70}$  stehen. Der Koeffizient von  $x^{70}$  in diesem Produkt ist  $\binom{70+2}{2} - \binom{70+2-31}{2} - \binom{70+2-41}{2} - \binom{70+2-51}{2} = 1061$ .

## Aufgaben

1. (a) Zeigen Sie, dass  $(1-x)(1+x+x^2+\cdots+x^n)$  und  $1-x^{n+1}$  die gleichen Polynome sind und leiten Sie daraus die Formel  $1+x+x^2+\cdots+x^n = (1-x^{n+1})/(1-x)$  her. Für welche Werte von  $x$  ist das korrekt?  
 (b) Zeigen Sie mithilfe der Formel aus (a), dass die unendliche Reihe  $1 + x + x^2 + \cdots$  für alle  $x \in (-1, 1)$  gegen  $\frac{1}{1-x}$  konvergiert und für alle  $x$  außerhalb dieses Intervalls divergiert. (Dafür brauchen Sie ein wenig Analysis.)
2. Bestimmen Sie den Koeffizienten ...  
 (a) von  $x^{15}$  in  $(x^2 + x^3 + x^4 + \cdots)^4$ .  
 (b) von  $x^{50}$  in  $(x^7 + x^8 + x^9 + x^{10} + \cdots)^6$ .  
 (c) von  $x^5$  in  $(1 - 2x)^{-2}$ .  
 (d) von  $x^4$  in  $\sqrt[3]{1+x}$ .  
 (e) von  $x^3$  in  $(2+x)^{3/2}/(1-x)$ .  
 (f) von  $x^4$  in  $(2+3x)^5\sqrt{1-x}$ .  
 (g) von  $x^3$  in  $(1-x+2x^2)^9$ .
3. Finden Sie erzeugende Funktionen für die nachstehenden Folgen (bitte geben Sie sie in geschlossener Form an, nicht als unendliche Reihen!):  
 (a)  $0, 0, 0, 0, -6, 6, -6, 6, -6, \dots$   
 (b)  $1, 0, 1, 0, 1, 0, \dots$   
 (c)  $1, 2, 1, 4, 1, 8, \dots$   
 (d)  $1, 1, 0, 1, 1, 0, 1, 1, 0, \dots$
4. Finden Sie die Wahrscheinlichkeit dafür, mit drei Würfeln genau 12 Augen zu erzielen.
5. Sei  $a_n$  die Anzahl von geordneten Tripeln  $(i, j, k)$  ganzer Zahlen, so dass  $i \geq 0$ ,  $j \geq 1$ ,  $k \geq 1$  und  $i + 3j + 3k = n$ . Finden Sie die erzeugende Funktion der Folge  $(a_0, a_1, a_2, \dots)$  und bestimmen Sie eine Formel für  $a_n$ .
6. Sei  $a_n$  die Anzahl geordneter  $r$ -Tupel  $(i_1, \dots, i_r)$  nicht negativer ganzer Zahlen mit  $i_1 + i_2 + \cdots + i_r = n$ ; hier ist  $r$  eine feste natürliche Zahl.  
 (a) Finden Sie die erzeugende Funktion der Folge  $(a_0, a_1, a_2, \dots)$ .  
 (b) Finden Sie eine Formel für  $a_n$ . (Dieses Problem haben wir in Abschnitt 3.3 mit einer anderen Methode gelöst.)
7. Lösen Sie Problem 12.2.4 ohne Verwendung der Ableitung — wenden Sie stattdessen den verallgemeinerten Binomialsatz an.

8. Sei  $a_n$  die Anzahl der Möglichkeiten, einen Betrag von  $n$  Doublezons mit Münzen zu 1, 2 und 5 Doublezons auszuzahlen.
- Schreiben Sie die erzeugende Funktion für die Folge  $(a_0, a_1, \dots)$  auf.
  - \*Verwenden Sie (a) um eine Formel für  $a_n$  herzuleiten (den nächsten Abschnitt zu lesen könnte hilfreich sein).
9. (a) Sei  $a(x)$  die erzeugende Funktion einer Folge  $(a_0, a_1, a_2, \dots)$ . Zeigen Sie, dass dann  $\frac{1}{1-x}a(x)$  die erzeugende Funktion der Partialsummen  $(a_0, a_0 + a_1, a_0 + a_1 + a_2, \dots)$  ist.
- Berechnen Sie die Summe  $\sum_{k=1}^n k^2$ . Verwenden Sie dabei (a) und die Lösung von Problem 12.2.4.
  - Berechnen Sie auf ähnliche Weise die Summe  $\sum_{k=1}^n k^3$ .
  - Berechnen Sie die Summe  $\sum_{k=0}^m (-1)^k \binom{n}{k}$  für natürliche Zahlen  $n$  und  $m$ .
  - Es sieht nun womöglich so aus, als könnten wir mit dieser Methode jede nur erdenkliche Summe berechnen, doch so einfach ist es nicht. Was passiert, wenn wir versuchen, die Summe  $\sum_{k=1}^n \frac{1}{k}$  auf diese Art zu bestimmen?
10. \*Seien  $n, r$  ganze Zahlen mit  $n \geq r \geq 1$ . Wählen Sie eine zufällige  $r$ -elementige Teilmenge von  $\{1, 2, \dots, n\}$  (jede der  $\binom{n}{r}$  möglichen Teilmengen mit der gleichen Wahrscheinlichkeit) und nennen sie  $R$ . Zeigen Sie, dass der Erwartungswert für die kleinste Zahl in  $R$  gleich  $\frac{n+1}{r+1}$  ist.
11. (Analysiskenntnisse erforderlich) \*Beweisen Sie die Formel für das Produkt zweier Potenzreihen. Das heißt, wenn zwei Potenzreihen  $a(x)$  und  $b(x)$  die Voraussetzungen von Hilfssatz 12.2.1 erfüllen, dann konvergiert die Potenzreihe  $c(x)$ , deren Koeffizienten durch die Formel (12.4) gegeben sind, in einer Umgebung von 0 gegen  $a(x)b(x)$ .
12. (Analysiskenntnisse erforderlich) Sei  $a(x) = a_0 + a_1x + a_2x^2 + \dots$  eine Potenzreihe mit nicht negativen Koeffizienten, d.h. mit  $a_i \geq 0$  für alle  $i$ . Wir definieren ihren *Konvergenzradius*  $\rho$  als

$$\rho = \sup\{x \geq 0 : a(x) \text{ konvergiert}\}.$$

- \*Beweisen Sie, dass  $a(x)$  für jede reelle Zahl  $x \in [0, \rho)$  konvergiert und dass die Funktion  $a(x)$  im Intervall  $[0, \rho)$  stetig ist.
- Finden Sie ein Beispiel einer Folge  $(a_0, a_1, a_2, \dots)$  mit  $\rho = 1$ , so dass die Reihe  $a(\rho)$  divergiert.
- Finden Sie ein Beispiel einer Folge  $(a_0, a_1, a_2, \dots)$  mit  $\rho = 1$ , so dass die Reihe  $a(\rho)$  konvergiert.

13. (Ein warnendes Beispiel; Analysiskenntnisse erforderlich) Definieren Sie eine Funktion  $f$  durch

$$f(x) = \begin{cases} e^{-1/x^2} & \text{für } x \neq 0 \\ 0 & \text{für } x = 0. \end{cases}$$

- (a) \*Zeigen Sie, dass  $f$  an der Stelle 0 beliebig oft differenzierbar ist, und zwar immer mit dem Wert 0.
- (b) Beweisen Sie, dass  $f$  in keiner Umgebung von 0 als Potenzreihe realisiert werden kann.
14. (Exponentielle erzeugende Funktionen) In einer Fußnote haben wir die *exponentielle erzeugende Funktion* einer Folge  $(a_0, a_1, a_2, \dots)$  als die Potenzreihe  $A(x) = \sum_{i=0}^{\infty} (a_i / i!) x^i$  definiert. Hier wollen wir einige kombinatorische Anwendungen skizzieren.

Eine Gruppe von  $n$  Personen kann man auf verschiedene Arten organisieren. Eine Möglichkeit ist zum Beispiel, eine der Personen zum Chef zu erklären und die anderen zu Gefolgsmenschen. Für jede Gruppe mit  $n$  Personen gibt es  $n$  Möglichkeiten diesen Organisationstyp zu realisieren. Andere Beispiele sind: die  $n$  Personen in einer Reihe von links nach rechts aufzustellen ( $n!$  Möglichkeiten), die  $n$  Personen für einen Volkstanz im Kreis aufzustellen (dafür gibt es  $(n - 1)!$  Möglichkeiten), die Leute einfach unorganisiert rumstehen lassen (1 Möglichkeit), sie zu einer Jury küren (12 Möglichkeiten für  $n = 12$ , weil ein Vorsitzender gewählt wird, und 0 Möglichkeiten sonst).

(a) Schreiben Sie für jeden der oben genannten Organisationstypen die exponentielle erzeugende Funktion der zugehörigen Folge auf (d.h. für die Folge  $(a_0, a_1, a_2, \dots)$ , wobei  $a_i$  die Anzahl der Möglichkeiten ist, den betrachteten Organisationstyp mit  $i$  Personen zu realisieren).

(b) Sei  $a_n$  die Anzahl der möglichen Realisierungen eines Organisationstyps A für eine Gruppe von  $n$  Personen, und sei  $b_n$  die Anzahl der möglichen Realisierungen eines Organisationstyps B für eine Gruppe von  $n$  Personen. Ein Arrangement vom Typ C entstehe, indem man die gegebenen  $n$  Personen in zwei Gruppen einteilt, die „erste“ und die „zweite“, und die erste im Typ A organisiert und die zweite im Typ B. Sei  $c_n$  die Anzahl der möglichen Realisierungen vom Organisationstyp C für eine Gruppe von  $n$  Personen. Zeigen Sie: Sind  $A(x)$ ,  $B(x)$  und  $C(x)$  die zugehörigen exponentiellen erzeugenden Funktionen, dann ist  $C(x) = A(x)B(x)$ . Sehen Sie sich auch einige konkrete Beispiele mit den am Anfang dieser Aufgabe beschriebenen Typen an.

(c) \*Sei  $A(x)$  die exponentielle erzeugende Funktion für den Organisationstyp A aus (b), und es sei  $a_0 = 0$  (die „leere Gruppe“ ist nicht zulässig). Ein Arrangement vom Typ D entstehe, indem man die gegebenen  $n$  Personen in  $k$  Gruppen einteilt, die erste, die zweite,  $\dots$ ,

die  $k$ -te Gruppe ( $k = 0, 1, 2, \dots$ ), und jede der Gruppen im Typ A organisiert. Drücken Sie die exponentielle erzeugende Funktion  $D(x)$  mittels  $A(x)$  aus.

- (d) \*Sei  $A(x)$  wie in (c), und ein Arrangement vom Typ E entstehe, indem man die gegebenen  $n$  Personen in einige Gruppen einteilt und jede Gruppe gemäß A organisiert (diesmal kommt es nur auf die Zusammenstellung der Gruppen an, nicht auf ihre Nummerierung). Drücken Sie die exponentielle erzeugende Funktion  $E(x)$  mittels  $A(x)$  aus.
  - (e) Auf wie viele Arten kann man  $n$  Personen in Paaren anordnen (es kommt nur darauf an, wer mit wem ein Paar bildet, die Paare sind nicht nummeriert)? Verwenden Sie (d) zur Lösung.
15. \*Verwenden Sie Teil (d) von Aufgabe 14 zur Bestimmung der exponentiellen erzeugenden Funktion der *Bell-Zahlen*, d.h. die Anzahl der Äquivalenzrelationen auf  $n$  gegebenen Punkten. Berechnen Sie die ersten Terme der Taylorreihe, um das Ergebnis numerisch zu überprüfen (siehe auch Aufgabe 3.8.8).
16. Zwölf Studenten sollen zur Arbeit in fünf verschiedenen Projekten eingeteilt werden. Jeder Student soll an genau einem Projekt teilnehmen; bei jedem Projekt müssen mindestens zwei und höchstens vier Studenten teilnehmen. Auf wie viele Arten ist das möglich? Verwenden Sie die Idee aus Teil (b) von Aufgabe 14.
17. (Nochmal die Garderobenfrau)

(a) \*Verwenden Sie (a) und (d) aus Aufgabe 14, um die exponentielle erzeugende Funktion für die Aufstellungen von  $n$  Personen (zum Tanz) in einen oder mehrere Kreise zu bestimmen (in einem Kreis darf eine beliebige Zahl von Personen stehen, einschließlich 1). Können Sie die Anzahl solcher Aufstellungen auch auf andere Art herausbekommen?

(b) Betrachten Sie Arrangements wie in (a), wobei jedoch jeder Kreis aus mindestens zwei Personen besteht. Geben Sie die exponentielle erzeugende Funktion an.

(c) \*Bestimmen Sie unter Verwendung des Ergebnisses aus (b) die Anzahl der Aufstellungen von  $n$  Personen in Kreise mit jeweils mindestens zwei Personen. Wenn Sie sich nicht verrechnen, das sollte das Ergebnis gleich der Anzahl der fixpunktfreien Permutationen sein (siehe Abschnitt 3.8). Erklären Sie, warum. (Damit erhalten Sie also eine alternative Lösung für das Problem mit der Garderobenfrau, ganz ohne Inklusion–Exklusion!)

## 12.3 Fibonacci-Zahlen und der goldene Schnitt

Wir werden nun die Folge  $(F_0, F_1, F_2, \dots)$  untersuchen, die durch folgende Regeln gegeben ist:

$$F_0 = 0, \quad F_1 = 1, \quad F_{n+2} = F_{n+1} + F_n \quad \text{für } n = 0, 1, 2, \dots$$

Bereits im dreizehnten Jahrhundert hat Leonardo von Pisa, genannt Fibonacci, diese Folge untersucht, deswegen spricht man von den Fibonacci-Zahlen. Ihre ersten Glieder sind

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \dots$$

Fibonacci hat diese Folge als Modell für die Vermehrung von Kaninchen verpackt. Sein Modell war nicht besonders realistisch, aber die Folge hat durchaus eine gewisse Bedeutung in der Biologie (zum Beispiel ist die Anzahl der Blütenblätter bei Blumen sehr oft eine Fibonacci-Zahl; eine mögliche Erklärung versucht Stewart in [49]). In Mathematik und Informatik taucht diese Folge in verschiedenen Zusammenhängen auf, und zwar recht häufig.

Wir werden nun eine Formel für die  $n$ -te Fibonacci-Zahl herleiten und dazu erzeugende Funktionen verwenden. Sei also  $F(x)$  die erzeugende Funktion dieser Folge. Die wesentliche Idee ist, eine Gleichung für die erzeugende Funktion derjenigen Folge aufzuschreiben, deren  $k$ -tes Glied  $F_k - F_{k-1} - F_{k-2}$  ist für alle  $k \geq 2$ . Wegen der Definition der Fibonacci-Zahlen müssen alle Glieder dieser Folge ab dem zweiten 0 sein. Andererseits kann man diese erzeugende Funktion mit den in Abschnitt 12.2 diskutierten Operationen aus  $F(x)$  konstruieren. Auf diese Weise erhalten wir eine Gleichung, aus der wir  $F(x)$  bestimmen können.

Ganz konkret betrachten wir die Funktion  $F(x) - xF(x) - x^2F(x)$ , die zu der Folge

$$\begin{aligned} (F_0, F_1 - F_0, F_2 - F_1 - F_0, F_3 - F_2 - F_1, F_4 - F_3 - F_2, \dots) \\ = (0, 1, 0, 0, 0, \dots) \end{aligned}$$

gehört. In der Sprache der erzeugenden Funktionen bedeutet das  $(1 - x - x^2)F(x) = x$ , oder umgestellt

$$F(x) = \frac{x}{1 - x - x^2}. \quad (12.6)$$

Wenn wir nun versuchen die Taylorreihe dieser Funktion durch Differenzieren zu bestimmen, laufen wir im Kreis: Wir erhalten nur

die definierende Rekursion der Fibonacci-Zahlen). Wir brauchen eine weitere Methode, die bei der Berechnung von Integralen gang und gäbe ist, die *Partialbruchzerlegung*. In unserem Fall garantiert diese Methode, dass die rationale Funktion auf der rechten Seite von (12.6) in der Form

$$\frac{x}{1-x-x^2} = \frac{A}{x-x_1} + \frac{B}{x-x_2}$$

geschrieben werden kann, wobei  $x_1, x_2$  die Nullstellen des quadratischen Polynoms  $1-x-x^2$  sind und  $A$  und  $B$  geeignete Konstanten. Für unsere Zwecke ist eine geringfügig abgewandelte Gestalt dieser Gleichung praktischer, nämlich

$$\frac{x}{1-x-x^2} = \frac{a}{1-\lambda_1 x} + \frac{b}{1-\lambda_2 x}, \quad (12.7)$$

wobei  $\lambda_1 = \frac{1}{x_1}$ ,  $\lambda_2 = \frac{1}{x_2}$ ,  $a = -\frac{A}{x_1}$ , und  $b = -\frac{B}{x_2}$ . Mit (12.7) ist es nicht mehr schwer, eine Formel für  $F_n$  hinzuschreiben: Wir erhalten die Formel  $F_n = a\lambda_1^n + b\lambda_2^n$ . Davon sollten Sie sich nun überzeugen.

Wir überspringen hier ebenso die Berechnung der Nullstellen  $x_1$ ,  $x_2$  der quadratischen Gleichung wie die Bestimmung der Konstanten  $a$  und  $b$  und nennen nur das Ergebnis:

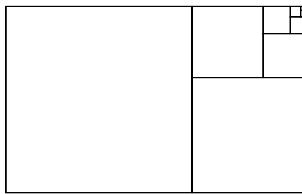
$$F_n = \frac{1}{\sqrt{5}} \left[ \left( \frac{1+\sqrt{5}}{2} \right)^n - \left( \frac{1-\sqrt{5}}{2} \right)^n \right].$$

Ist es nicht erstaunlich, dass diese Formel immer eine ganze Zahl ergibt, für jede natürliche Zahl  $n$ ?

Mit Näherungswerten für die Konstanten sieht die Formel so aus:

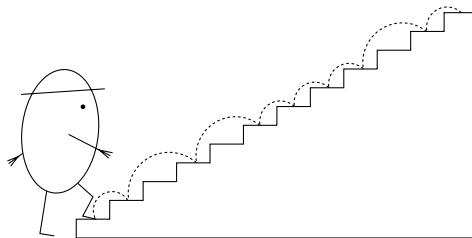
$$F_n = (0.4472135\dots) [(1.6180339\dots)^n - (-0.6180339\dots)^n].$$

Nun sieht man, dass die Zahlen  $F_n$  für große  $n$  etwa  $\frac{1}{\sqrt{5}}\lambda_1^n$  sind (tatsächlich ist  $F_n$  für alle  $n$  gleich diesem Wert, gerundet auf die nächste ganze Zahl), und dass das Verhältnis  $F_n/F_{n+1}$  gegen den Grenzwert  $\frac{1}{\lambda_1} = 0.6180339\dots$  konvergiert. Dieses Verhältnis hielt man im antiken Griechenland für sehr bedeutsam; es hat den Namen *goldener Schnitt*. Ein Rechteck, dessen Seitenlängen im goldenen Schnitt zueinander stehen, wurde als besonders schön angesehen, diese Rechtecke galten als die gefälligsten. (An dem Bild unten können Sie testen, ob Ihre Kriterien für die Ästhetik von Rechtecken die gleichen sind.) Wenn man von einem solchen Rechteck mit Seitenlängen im goldenen Schnitt ein Quadrat abschneidet, dann stehen die Seitenlängen des verbleibenden Rechtecks wieder im goldenen Schnitt:



Ähnlich wie auf die Fibonacci-Zahlen trifft man in der Mathematik erstaunlich häufig auf den goldenen Schnitt. Das Buch von Beutelspacher und Petri [37] zeigt viele seiner Facetten — auf Deutsch!

**Eine andere Herleitung: Treppen steigen.** Betrachten wir eine Treppe mit  $n$  Stufen. Wie viele Arten gibt es die Treppe hochzugehen, wenn wir mit jedem Schritt eine oder zwei Stufen nehmen können?



Mit anderen Worten, auf wie viele Arten kann man die Zahl  $n$  als Summe von Einsen und Zweien schreiben, oder wie viele Lösungen hat die Gleichung

$$s_1 + s_2 + \cdots + s_k = n,$$

mit  $s_i \in \{1, 2\}$ ,  $i = 1, 2, \dots, k$ ,  $k = 0, 1, 2, \dots$ ? Wenn wir die Anzahl der Lösungen  $S_n$  nennen, erhalten wir  $S_1 = 1$ ,  $S_2 = 2$ , und für  $n \geq 1$  ist es nicht schwer zu sehen, dass  $S_{n+2} = S_{n+1} + S_n$  gilt (bitte darüber nachdenken!). Daraus folgt, dass  $S_n$  genau die Fibonacci-Zahl  $F_{n-1}$  ist.

Wir leiten nun die erzeugende Funktion der Folge  $(S_0, S_1, S_2, \dots)$  auf andere Art her. Gemäß dem Rezept aus Abschnitt 12.1 ist bei gegebenem  $k$  die Anzahl der Lösungen der Gleichung  $s_1 + s_2 + \cdots + s_k = n$  mit  $s_i \in \{1, 2\}$  gleich dem Koeffizienten von  $x^n$  in dem Produkt  $(x + x^2)^k$ . Wir können  $k$  jedoch beliebig wählen (es ist ja nicht vorgeschrieben, mit wie vielen Schritten wir die Treppe hochgehen sollen), deshalb ist  $S_n$  der Koeffizient von  $x^n$  in der Summe  $\sum_{k=0}^{\infty} (x + x^2)^k$ . Demnach ist diese Summe die erzeugende Funktion der Folge  $(S_0, S_1, S_2, \dots)$ . Das können wir noch umformen: Die Summe ist eine geometrische Reihe mit dem Wert  $1/(1 - x - x^2)$ . Damit ist die erzeugende Funktion für die Fibonacci-Zahlen  $x/(1 - x - x^2)$ , wie wir vorhin mit dem anderen Ansatz schon gesehen haben.

**Rezepte für Rekursionen.** Mit der in diesem Abschnitt vorgestellten Methode kann man allgemein Rekursionen für eine Folge  $(y_0, y_1, y_2, \dots)$  finden, die für alle  $n = 0, 1, 2, \dots$  die Gleichung

$$y_{n+k} = a_{k-1}y_{n+k-1} + a_{k-2}y_{n+k-2} + \cdots + a_1y_{n+1} + a_0y_n \quad (12.8)$$

erfüllt, wobei  $k$  eine natürliche Zahl ist und  $a_0, a_1, \dots, a_{k-1}$  reelle (oder komplexe) Zahlen sind. Für die Fibonacci-Zahlen sind z.B.  $k = 2$  und  $a_0 = a_1 = 1$ . Wir bezeichnen die Menge aller Folgen  $(y_0, y_1, y_2, \dots)$ , die Gleichung (12.8) genügen, mit dem Symbol  $\mathcal{Y}$  (d.h.  $\mathcal{Y}$  ist von  $k$  und von  $a_0, a_1, \dots, a_{k-1}$  abhängig). Diese Menge enthält im Allgemeinen viele Folgen, weil die ersten  $k$  Glieder der Folge  $(y_0, y_1, y_2, \dots)$  beliebig gewählt werden können (die weiteren Folgenglieder sind dann durch (12.8) festgelegt). Im Folgenden werden wir beschreiben, wie die Folgen in  $\mathcal{Y}$  aussehen, doch zunächst machen wir einen kleinen Ausflug in die Terminologie.

Ein vornehmer Name für Gleichung (12.8) ist *homogene lineare Rekursion k-ten Grades mit konstanten Koeffizienten*. Wir sehen uns einmal die einzelnen Bestandteile dieses komplizierten Namens an.

- Eine *Rekursion* ist der allgemeine Begriff für eine Beziehung (meist eine Formel) zwischen dem  $n$ -ten Glied einer Folge und ein oder mehreren vorangegangenen Folgengliedern.<sup>3</sup>
- *Homogen* steht im Namen, weil mit jeder Folge  $(y_0, y_1, y_2, \dots) \in \mathcal{Y}$  auch die Folge  $(\alpha y_0, \alpha y_1, \alpha y_2, \dots) \in \mathcal{Y}$  ist, und zwar für jede reelle Zahl  $\alpha$ . (In der Mathematik bedeutet „Homogenität“ in der Regel „Invarianz gegen Skalierung“.) Die Rekursion  $y_{n+1} = y_n + 1$  ist im Gegensatz zur hier betrachteten inhomogen.
- Das Wort *linear* bedeutet hier, dass die  $y_j$  in der Rekursion immer nur in der ersten Potenz vorkommen und nie miteinander multipliziert werden. Eine nicht lineare Rekursion ist z.B.  $y_{n+2} = y_{n+1}y_n$ .
- Der Ausdruck *mit konstanten Koeffizienten* schließlich bedeutet, dass  $a_0, a_1, \dots, a_{k-1}$  feste Zahlen sind, die nicht von  $n$  abhängen. Man kann auch Rekursionen wie  $y_{n+1} = (n-1)y_n$  betrachten, wo die Koeffizienten auf der rechten Seite Funktionen von  $n$  sind.

So viel zu dem langen Namen. Wir werden nun ein allgemeines Resultat über die Lösungen einer solchen Rekursion formulieren. Wir definieren das *charakteristische Polynom* der Rekursion (12.8) als das Polynom

$$p(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \cdots - a_1x - a_0.$$

---

<sup>3</sup>Manchmal wird auch der Name *Differenzengleichung* verwendet. Dieser Ausdruck bezieht sich auf die so genannte Differenz einer Funktion, einem Konzept, das in mancher Hinsicht dem Differenzieren ähnelt. Die Theorie der Differenzengleichungen und die Theorie der Differentialgleichungen besitzen viele Analogien.

Beispielsweise ist das charakteristische Polynom der Fibonacci-Rekursion  $x^2 - x - 1$ . Wir erinnern uns, dass jedes Polynom vom Grad  $k$  mit höchstem Koeffizienten 1 in der Form

$$(x - \lambda_1)(x - \lambda_2) \dots (x - \lambda_k)$$

geschrieben werden kann, wobei  $\lambda_1, \dots, \lambda_k$  (im Allgemeinen komplexe) Zahlen sind, die Nullstellen des gegebenen Polynoms.

**12.3.1 Hilfssatz.** Sei  $p(x)$  das charakteristische Polynom der homogenen linearen Rekursion (12.8).

(i) (Einfache Nullstellen) Angenommen,  $p(x)$  hat  $k$  paarweise verschiedene Nullstellen  $\lambda_1, \dots, \lambda_k$ . Dann existieren für jede Folge  $y = (y_0, y_1, \dots) \in \mathcal{Y}$ , die Gleichung (12.8) genügt, komplexe Konstanten  $C_1, C_2, \dots, C_k$ , so dass für alle  $n$  gilt:

$$y_n = C_1 \lambda_1^n + C_2 \lambda_2^n + \dots + C_k \lambda_k^n.$$

(ii) (Allgemeiner Fall) Seien  $\lambda_1, \dots, \lambda_q$  paarweise verschiedene komplexe Zahlen und seien  $k_1, \dots, k_q$  natürliche Zahlen mit  $k_1 + k_2 + \dots + k_q = k$ , so dass

$$p(x) = (x - \lambda_1)^{k_1} (x - \lambda_2)^{k_2} \dots (x - \lambda_q)^{k_q}.$$

Dann existieren für jede Folge  $y = (y_0, y_1, \dots) \in \mathcal{Y}$ , die Gleichung (12.8) genügt, komplexe Konstanten  $C_{ij}$  ( $i = 1, 2, \dots, q$ ,  $j = 0, 1, \dots, k_i - 1$ ), so dass für alle  $n$  gilt:

$$y_n = \sum_{i=1}^q \sum_{j=0}^{k_i-1} C_{ij} \binom{n}{j} \lambda_i^n.$$

Wie löst man nun mit diesem Hilfssatz eine Rekursion der Gestalt (12.8)? Sehen wir uns zwei kurze Beispiele an. Für die Rekursion  $y_{n+2} = 5y_{n+1} - 6y_n$  ist das charakteristische Polynom  $p(x) = x^2 - 5x + 6 = (x - 2)(x - 3)$ . Ihre Nullstellen sind  $\lambda_1 = 2$  und  $\lambda_2 = 3$ , und Hilfssatz 12.3.1 sagt uns, dass wir nach einer Lösung der Form  $C_1 2^n + C_2 3^n$  zu suchen haben. Sind noch Anfangsbedingungen gegeben, z.B.  $y_0 = 2$  und  $y_1 = 5$ , müssen wir Konstanten  $C_1, C_2$  finden, mit denen die Formel diese geforderten Werte für  $n = 0, 1$  annimmt. In unserem Fall ergäbe sich  $C_1 = C_2 = 1$ .

Und nun noch ein (zugegeben eher künstliches) Beispiel mit mehrfachen Nullstellen: Die Gleichung  $y_{n+5} = 8y_{n+4} + 25y_{n+3} - 38y_{n+2} + 28y_{n+1} - 8y_n$  hat das charakteristische Polynom<sup>4</sup>  $p(x) = (x - 1)^2(x - 2)^3$ , somit sagt Hilfssatz 12.3.1, dass die Lösung von der Gestalt  $y_n = C_{10} +$

---

<sup>4</sup>Natürlich haben die Autoren die Koeffizienten so gewählt, dass ein hübsches charakteristisches Polynom herauskommt. Die Anweisungen aus dem Hilfssatz

$C_{11}n + C_{20}2^n + C_{21}n2^n + C_{22}\binom{n}{2}2^n$  sein wird. Die Werte der Konstanten sind wiederum durch die ersten fünf Glieder der Folge  $(y_0, y_1, y_2, \dots)$  bestimmt.

Das hier demonstrierte Vorgehen zum Lösen der Rekursion (12.8) findet man in sehr vielen Lehrbüchern, doch erzeugende Funktionen werden in diesem Zusammenhang selten genannt. Hilfssatz 12.3.1 lässt sich tatsächlich elegant mit linearer Algebra beweisen (siehe Aufgabe 16), und wenn wir erst einmal wissen, dass die Lösung von der genannten Form ist, hat die erzeugende Funktion ihren Zweck erfüllt. Dafür aber brauchen wir sie: Nur mit dieser Methode haben wir im Beispiel oben die korrekte Gestalt für die Fibonacci-Zahlen herausgefunden. Außerdem ist diese hübsche Anwendung erzeugender Funktionen verallgemeinerungsfähig, ein ähnlicher Ansatz führt zuweilen zu Ergebnissen bei Rekursionen anderer Typen, für die keine allgemeine Lösungsstrategie bekannt ist (oder wenn man nicht weiß, wo in der Literatur man sie findet — was so ungefähr auf das Gleiche hinausläuft).

## Aufgaben

1. \*Bestimmen Sie die Anzahl der 0-1-Folgen der Länge  $n$ , die keine zwei aufeinanderfolgenden Nullen enthalten.
2. Beweisen Sie, dass man jede natürliche Zahl  $n \in \mathbb{N}$  als Summe paarweise verschiedener Fibonacci-Zahlen schreiben kann.
3. Finden Sie einen Ausdruck für das  $n$ -te Glied der durch folgende Rekursionen gegebenen Folgen (verwenden Sie die gleiche Methode wie für die Fibonacci-Zahlen oder Hilfssatz 12.3.1).
  - (a)  $a_0 = 2, a_1 = 3, a_{n+2} = 3a_n - 2a_{n+1}$  ( $n = 0, 1, 2, \dots$ ),
  - (b)  $a_0 = 0, a_1 = 1, a_{n+2} = 4a_{n+1} - 4a_n$  ( $n = 0, 1, 2, \dots$ ),
  - (c)  $a_0 = 1, a_{n+1} = 2a_n + 3$  ( $n = 0, 1, 2, \dots$ ).
4. In einer Folge  $(a_0, a_1, a_2, \dots)$  sei jedes Glied außer den beiden ersten das arithmetische Mittel der zwei vorangehenden Glieder, d.h.  $a_{n+2} = (a_{n+1} + a_n)/2$ . Bestimmen Sie den Grenzwert  $\lim_{n \rightarrow \infty} a_n$  (als Funktion von  $a_0, a_1$ ).
5. Lösen Sie die Rekursion  $a_{n+2} = \sqrt{a_{n+1}a_n}$  mit Anfangsbedingungen  $a_0 = 2, a_1 = 8$ , und bestimmen Sie  $\lim_{n \rightarrow \infty} a_n$ .

zur Lösung homogener linearer Rekursionen mit konstanten Koeffizienten klammern (ebenso wie die Methode mit erzeugenden Funktionen) die Frage aus, wie man die Nullstellen des charakteristischen Polynoms finden soll. In den üblichen Lehrbuch-Beispielen haben die Rekursionen deshalb meist Grad 1 oder 2, oder die Koeffizienten sind so gewählt, dass als Nullstellen „vernünftige Zahlen“ herauskommen.

6. (a) Lösen Sie die Rekursion  $a_n = a_{n-1} + a_{n-2} + \cdots + a_1 + a_0$  mit der Anfangsbedingung  $a_0 = 1$ .  
 (b) \*Lösen Sie die Rekursion  $a_n = a_{n-1} + a_{n-3} + a_{n-4} + a_{n-5} + \cdots + a_1 + a_0$  ( $n \geq 3$ ) mit  $a_0 = a_1 = a_2 = 1$ .

7. \*Drücken Sie die Summe

$$S_n = \binom{2n}{0} + 2\binom{2n-1}{1} + 2^2\binom{2n-2}{2} + \cdots + 2^n\binom{n}{n}$$

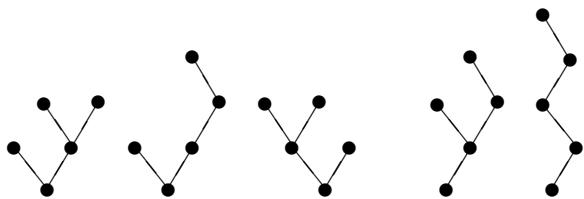
als Koeffizienten von  $x^{2n}$  in einer geeigneten Potenzreihe aus und finden Sie eine einfache Formel für  $S_n$ .

8. Berechnen Sie  $\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n-k}{k} (-4)^{-k}$ .
9. \*Zeigen Sie, dass die Zahl  $\frac{1}{2}[(1+\sqrt{2})^n + (1-\sqrt{2})^n]$  für alle  $n \geq 1$  eine ganze Zahl ist.
10. \*Zeigen Sie, dass die Zahl  $(6+\sqrt{37})^{999}$  nach dem Dezimalkomma mindestens 999 Nullen hat.
11. \*Zeigen Sie, dass die Zahl  $(\sqrt{2}-1)^n$  für jedes  $n \geq 1$  als Differenz der Quadratwurzeln zweier aufeinander folgender Zahlen geschrieben werden kann.
12. \*Bestimmen Sie die Anzahl der Folgen der Länge  $n$ , die aus den Buchstaben  $a$ ,  $b$ ,  $c$  und  $d$  bestehen und bei denen  $a$  nie neben  $b$  steht.
13. („Mini-Tetris“) Auf wie viele Arten kann man ein  $n \times 2$  Rechteck mit den folgenden Steinen lückenlos und ohne Überlappungen belegen? Die Seitenlängen der Steine sind 1 und 2; die Steine können um Vielfache von  $90^\circ$  gedreht werden. In (b) und (c) brauchen Sie nur die erzeugende Funktion zu berechnen oder das Problem auf eine Rekursion der Gestalt (12.8) zu reduzieren; bestimmen Sie auch die Größenordnung des Wachstums (eine asymptotische Näherung für großes  $n$ ).  
 (a)  ,  
 (b) \*  ,  
 (c) \*\*  .
14. *Inf* Diese Aufgabe hängt mit der Theorie formaler Sprachen zusammen. Wir geben die notwendigen Definitionen an, doch um die Aussagen würdigen zu können sollten Sie einmal in ein Buch über Automaten und formale Sprachen schauen.  
 Sei  $\Sigma$  ein endliches Alphabet (etwa  $\Sigma = \{a, b, c\}$ ). Ein *Wort* über  $\Sigma$  ist eine endliche Folge von Buchstaben (wie *babbaacccba*). Das leere Wort mit 0 Buchstaben bezeichnen wir mit  $\varepsilon$ . Eine *Sprache* über  $\Sigma$  ist eine Menge von Wörtern über  $\Sigma$ . Sind  $u$  und  $v$  Wörter, dann ist

$uv$  die Aneinanderreihung von  $u$  und  $v$ , d.h. wir schreiben erst  $u$  und direkt dahinter  $v$ . Die *erzeugende Funktion* einer Sprache  $L$  ist die erzeugende Funktion der Folge  $n_0, n_1, n_2, \dots$ , wobei  $n_i$  die Anzahl der Wörter der Länge  $i$  in  $L$  ist.

Wir nennen eine Sprache  $L$  *sehr regulär*, wenn sie durch endlichmalige Anwendung folgender Regeln erhält:

1. Die Sprachen  $\emptyset$  und  $\{\varepsilon\}$  sind sehr regulär, und die Sprache  $\{\ell\}$  ist sehr regulär für jeden Buchstaben  $\ell \in \Sigma$ .
  2. Sind  $L_1, L_2$  sehr regulär Sprachen, dann ist auch die Sprache  $L_1 \cdot L_2$  sehr regulär, wobei  $L_1 \cdot L_2 = \{uv : u \in L_1, v \in L_2\}$ .
  3. Ist  $L$  eine sehr reguläre Sprache, dann ist auch  $L^*$  sehr regulär, wobei  $L^* = \{\varepsilon\} \cup L \cup L \cdot L \cup L \cdot L \cdot L \cup \dots$
  4. Sind  $L_1, L_2$  sehr reguläre Sprachen mit  $L_1 \cap L_2 = \emptyset$ , dann ist auch  $L_1 \cup L_2$  sehr regulär.
- (a) Zeigen Sie, dass die folgenden Sprachen über  $\Sigma = \{a, b\}$  sehr regulär sind: die Sprache mit allen Wörtern ungerader Länge, die Sprache aller Wörter, die mit  $aab$  anfangen und gerade oft den Buchstaben  $a$  enthalten, und \*die Sprache aller Wörter, in denen nie zwei  $a$  hintereinander stehen.
- (b) \*Zeigen Sie, dass die erzeugende Funktion jeder sehr regulären Sprache eine rationale Funktion ist (ein Quotient zweier Polynome), und beschreiben Sie, wie man sie berechnet.
- (c) \*\*Zeigen Sie, dass die Vereinigung  $L_1 \cup L_2$  zweier sehr regulärer Sprachen  $L_1, L_2$  (die nicht notwendig disjunkt sind) wieder sehr regulär ist. (Deshalb haben reguläre Sprachen rationale erzeugende Funktionen.)
- (d) (Ein Software-Projekt) Suchen Sie Informationen über reguläre Sprachen und ihren Bezug zu endlichen Automaten. Schreiben Sie ein Programm, das als Input eine Spezifikation einer regulären Sprache akzeptiert (als regulären Ausdruck oder als nicht deterministischen endlichen Automaten) und die Formel für die Anzahl der Wörter der Länge  $n$  in der Sprache ausgibt.
15. \*Beweisen Sie Hilfssatz 12.3.1, indem Sie die für die Fibonacci-Zahlen verwendete Methode verallgemeinern (verwenden Sie einen allgemeinen Satz aus der Analysis über die Partialbruchzerlegung einer rationalen Funktion).
16. Beweisen Sie Hilfssatz 12.3.1 direkt, mit linearer Algebra:
  - (a) Zeigen Sie, dass die Menge  $\mathcal{Y}$  ein Vektorraum ist (Folgen werden gliedweise addiert und gliedweise mit komplexen Zahlen multipliziert).
  - (b) Zeigen Sie, dass die Dimension von  $\mathcal{Y}$  gleich  $k$  ist.



**Abb. 12.1** Verschiedene binäre Bäume auf 5 Ecken.

- (c) \*Zeigen Sie, dass in der Situation aus Teil (i) von Hilfssatz 12.3.1 die Folgen  $(\lambda_i^0, \lambda_i^1, \lambda_i^2, \dots)$  zu  $\mathcal{Y}$  gehören (wobei  $i = 1, 2, \dots, k$ ), und dass sie alle linear unabhängig sind in  $\mathcal{Y}$  (somit bilden Sie nach (b) eine Basis des Vektorraums  $\mathcal{Y}$ ). Das beweist Teil (i).
- (d) Zeigen Sie, dass in der Situation aus Teil (ii) von Hilfssatz 12.3.1 jede der Folgen  $((n)_j \lambda_i^n)_{n=0}^\infty$  zur Lösungsmenge  $\mathcal{Y}$  gehört.
- (e) \*\*Beweisen Sie, dass die in (d) betrachteten Folgen in  $\mathcal{Y}$  linear unabhängig sind, d.h. eine Basis bilden.

## 12.4 Binäre Bäume

Wir wollen nun so genannte binäre Bäume betrachten, die oft in Datenstrukturen Verwendung finden. Abbildung 12.1 zeigt einige verschiedene binäre Bäume mit fünf Ecken. Für unsere Zwecke ist die folgende kompakte Definition zweckmäßig: Ein binärer Baum ist entweder leer (hat keine Ecke), oder er besteht aus einer ausgezeichneten Ecke, der *Wurzel*, plus einem geordneten Paar binärer Bäume, dem *linken Teilbaum* und dem *rechten Teilbaum*.<sup>5</sup>

Sei  $b_n$  die Anzahl binärer Bäume mit  $n$  Ecken. Unser Ziel ist, eine Formel für  $b_n$  zu finden. Durch Auflisten aller kleinen binären Bäume finden wir  $b_0 = 1$ ,  $b_1 = 1$ ,  $b_2 = 2$  und  $b_3 = 5$ . Mit diesen Werten können wir nachher prüfen, ob das Ergebnis unserer Betrachtungen richtig ist.

Wie gewöhnlich sei  $b(x) = b_0 + b_1x + b_2x^2 + \dots$  die zugehörige erzeugende Funktion. Für  $n \geq 1$  ist die Anzahl der binären Bäume mit  $n$  Ecken gleich der Anzahl geordneter Paare der Form  $(B, B')$ ,

---

<sup>5</sup>Dies ist eine induktive Definition. Zuerst sagen wir, was ein binärer Baum mit 0 Ecken ist, und dann definieren wir einen binären Baum auf  $n$  Ecken unter Rückgriff auf die schon definierten binären Bäume mit weniger Ecken. Indem wir den leeren binären Baum zulassen, vermeiden wir ein paar Spezialfälle, etwa wenn die Wurzel nur einen linken Teilbaum hat.

wobei  $B$  und  $B'$  binäre Bäume mit zusammen  $n - 1$  Ecken sind. Hat  $B$  also  $k$  Ecken, dann hat  $B'$   $n - k - 1$  Ecken,  $k = 0, 1, \dots, n - 1$ . Deshalb ist die Anzahl solcher geordneten Paare

$$b_n = b_0 b_{n-1} + b_1 b_{n-2} + \cdots + b_{n-1} b_0. \quad (12.9)$$

Vergleichen wir dies mit der Definition der Multiplikation von Potenzreihen, so sehen wir, dass  $b_n$  genau der Koeffizient von  $x^{n-1}$  im Produkt  $b(x) \cdot b(x) = b(x)^2$  ist. (Dies ist das vernünftige Beispiel für die kombinatorische Bedeutung der Multiplikation von erzeugenden Funktionen, die wir in Abschnitt 12.2 angekündigt haben.) Also ist  $b_n$  der Koeffizient von  $x^n$  in der Funktion  $xb(x)^2$ . Somit ist  $xb(x)^2$  die erzeugende Funktion für die gleiche Folge wie  $b(x)$ , außer dass  $b(x)$  den konstanten Term  $b_0 = 1$  hat, während die Potenzreihe  $xb(x)^2$  den konstanten Term 0 hat; das ist so, weil die Formel (12.9) nur für  $n \geq 1$  stimmt. Wir können nun die folgende Gleichung für die erzeugenden Funktionen formulieren:

$$b(x) = 1 + xb(x)^2.$$

Angenommen,  $x$  ist eine reelle Zahl, für welche die Potenzreihe  $b(x)$  konvergiert. Dann ist auch  $b(x)$  eine reelle Zahl, die der quadratischen Gleichung  $b(x) = 1 + xb(x)^2$  genügen muss. Mit der bekannten  $p-q$ -Formel für die Nullstellen einer quadratischen Gleichung berechnen wir, dass  $b(x)$  eine der Zahlen

$$\frac{1 + \sqrt{1 - 4x}}{2x} \quad \text{oder} \quad \frac{1 - \sqrt{1 - 4x}}{2x}$$

sein muss. Das sieht so aus, als gäbe es zwei verschiedene Lösungen. Doch wir wissen, dass die Folge  $(b_0, b_1, b_2, \dots)$  eindeutig bestimmt ist, und also auch ihre erzeugende Funktion. Weil  $b(x)$  stetig ist als Funktion von  $x$  (jedenfalls wo sie konvergiert), müssen wir entweder für alle  $x$  die erste Lösung nehmen (die mit „+“) oder für alle  $x$  die zweite Lösung (die mit „-“). Wenn wir uns die erste Lösung anschauen, sehen wir, dass sie für  $x$  gegen 0 divergent ist, während die erzeugende Funktion  $b(x)$  den Wert  $b_0 = 1$  ergibt. Damit ist klar, dass die erzeugende Funktion  $b(x)$  überall, wo sie konvergiert, gegen die zweite Lösung  $b(x) = (1 - \sqrt{1 - 4x})/2x$  konvergieren muss.

Nun müssen wir noch die Koeffizienten dieser erzeugenden Funktion berechnen. Dabei verwenden wir den verallgemeinerten Binomialsatz 12.2.3. Damit erhalten wir

$$\sqrt{1 - 4x} = \sum_{k=0}^{\infty} (-4)^k \binom{1/2}{k} x^k.$$

Der Koeffizient von  $x^0$  ist 1, also verschwindet der konstante Term der Potenzreihe  $1 - \sqrt{1 - 4x}$ . Deshalb ist die Division durch  $2x$  möglich (alle Koeffizienten um eine Position nach links schieben und halbieren). So erfahren wir, dass für alle  $n \geq 1$

$$b_n = -\frac{1}{2}(-4)^{n+1} \binom{1/2}{n+1}. \quad (12.10)$$

Mit weiteren Umformungen (eine Aufgabe für Sie!) erhält man die ansehnlichere Form

$$b_n = \frac{1}{n+1} \binom{2n}{n}.$$

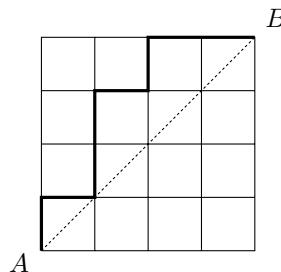
Die so definierten Zahlen  $b_n$  sind unter dem Namen *Catalan-Zahlen* bekannt (ihren Namen tragen sie zu Ehren von Eugène Charles Catalan, nicht wegen Katalonien).

Sie geben nicht nur die Anzahl binärer Bäume an, sie haben viele weitere kombinatorische Interpretationen. Einige davon finden Sie in den Aufgaben.

Mehr über Methoden zum Zählen verschiedener Typen von Graphen, Bäumen, usw. finden Sie beispielsweise im Buch von Harary und Palmer [22]. Software, die viele solche Aufgaben automatisch lösen kann, ist zusammen mit der zu Grunde liegenden Theorie in dem Buch von Flajolet, Salavy und Zimmermann [39] beschrieben.

## Aufgaben

1. Formen Sie den Ausdruck für  $b_n$  aus (12.10) in die „schönere Form“ darunter um.
2. \*Wahrscheinlich ist Ihnen nicht entgangen, dass wir kein Wort über die Konvergenz der Reihe  $b(x)$  verloren haben. Beweisen Sie, dass es eine Zahl  $x \neq 0$  gibt, für die  $b(x)$  konvergiert (verwenden Sie dazu nicht die oben hergeleitete Formel für  $b_n$ , denn die haben wir ja unter der Annahme erhalten, dass  $b(x)$  konvergiert).
3. Betrachten Sie ein  $n \times n$  Schachbrett:



Betrachten Sie die kürzesten Wege aus der Ecke  $A$  in die Ecke  $B$ , die immer entlang der Seiten der quadratischen Felder verlaufen (jeder solche Weg benutzt  $2n$  Seiten).

- (a) Wie viele solche Wege gibt es?
- (b) \*Zeigen Sie, dass die Anzahl der Wege, die nie unter die Diagonale (die Linie  $AB$ ) gehen, genau  $b_n$  ist, d.h. die Catalan-Zahl. Ein solcher Weg ist in der Abbildung eingezeichnet.
- (c) \*\*Geben Sie einen elementaren Beweis für die Formel  $b_n = \frac{1}{n+1} \binom{2n}{n}$ , ohne erzeugende Funktionen.
4. Betrachten Sie ein Produkt von vier Zahlen,  $abcd$ . Es kann auf fünf Arten „beklammert“ werden:  $((ab)c)d$ ,  $(a(bc))d$ ,  $(ab)(cd)$ ,  $a((bc)d)$  und  $a(b(cd))$ . Beweisen Sie, dass die Anzahl solcher Beklammerungen eines Produkts von  $n$  Zahlen die Catalan-Zahl  $b_{n-1}$  ist.
5. Theaterkasse:  $2n$  Personen stehen Schlange nach Eintrittskarten zu je 5 Doublezons. Jeder will ein Ticket kaufen;  $n$  Personen haben eine 5-Doublezon Münze und  $n$  haben einen 10-Doublezon Schein. Der Kassierer hat anfangs kein Geld in der Kasse.
  - (a) Wie viele Anordnungen der Schlange stehenden Menschen gibt es, bei denen der Kassierer jedem, der mit einem 10-Doublezon Schein zahlt, 5 Doublezon Wechselgeld herausgeben kann?
  - (b) Wie groß ist die Wahrscheinlichkeit, dass der Kassierer bei einer zufälligen Reihenfolge der Personen in der Schlange stets genügend Wechselgeld hat?
6. \*Betrachten Sie ein regelmäßiges  $n$ -Eck. Zerteilen Sie es in Dreiecke, indem Sie  $n - 3$  Diagonalen einzeichnen, die sich gegenseitig nicht schneiden (eine Diagonale ist eine Strecke zwischen zwei Ecken). Zeigen Sie, dass die Anzahl solcher Triangulierungen  $b_{n-2}$  ist.
7. Auf einem Kreis sind  $2n$  Punkte markiert. Wir möchten sie zu Paaren zusammenfassen und die Paare mit Strecken verbinden, die sich gegenseitig nicht schneiden. Zeigen Sie, dass dies auf  $b_n$  Arten möglich ist.

8. In dieser und den folgenden Aufgaben kommen *Wurzelbäume* und *gepflanzte Bäume* vor (eingeführt in Abschnitt 5.2, beides sind Bäume mit einer als Wurzel ausgezeichneten Ecke; bei gepflanzten Bäumen ist es ein Unterschied, ob ein Sohn weiter links oder weiter rechts ist als ein anderer, bei Wurzelbäumen nicht).
- Bezeichnen Sie mit  $c_n$  die Anzahl (nicht isomorpher) gepflanzter Bäume mit  $n$  Ecken, in denen jede Ecke, die keine Endecke ist, genau zwei Söhne hat (Beispiele für solche Bäume sind der erste und dritte Baum in Abb. 12.1). Zeigen Sie, dass die zugehörige erzeugende Funktion  $c(x)$  der Gleichung  $c(x) = x + xc(x)^2$  genügt, und finden Sie eine Formel für  $c_n$ .
  - \*Können Sie den Wert von  $c_n$  aus der Kenntnis von  $b_n$  (der Anzahl binärer Bäume) herleiten?
  - Bestimmen Sie  $d_n$ , die Anzahl nicht isomorpher gepflanzter Bäume mit  $n$  Ecken, in denen jede Ecke 0, 1 oder 2 Söhne hat. (Achtung, das ist etwas anderes als binäre Bäume!)
9. Es sei  $t_n$  die Anzahl aller nicht isomorphen gepflanzten Bäume mit  $n$  Ecken.
- Zeigen Sie, dass die zugehörige erzeugende Funktion  $t(x)$  die Gleichung  $t(x) = \frac{x}{1-t(x)}$  erfüllt und berechnen Sie eine Formel für  $t_n$ .
  - \*Können Sie den Wert von  $t_n$  aus der Kenntnis von  $b_n$  herleiten?
10. Wir nennen einen gepflanzten Baum *alt*, wenn er keine *junge Ecke* hat; eine junge Ecke ist ein Blatt, dessen Vater die Wurzel ist. Sei  $s_n$  die Anzahl alter gepflanzter Bäume mit  $n$  Ecken. Drücken Sie die erzeugende Funktion  $s(x)$  mittels  $t(x)$  aus der vorigen Aufgabe aus.
11. \*Betrachten Sie nun Wurzelbäume, in denen jede Ecke, die kein Blatt ist, genau zwei Söhne hat (bei Wurzelbäumen ist die Reihenfolge der Söhne unwesentlich, der erste und der dritte Baum in Abb. 12.1 sind nun also isomorph). Sei  $\bar{b}(x)$  die zugehörige erzeugende Funktion. Zeigen Sie die Gleichung
- $$\bar{b}(x) = 1 + \frac{x}{2} (\bar{b}(x)^2 + \bar{b}(x^2)).$$
12. Betrachten Sie *Alkylradikale*; das sind offenkettige Kohlenwasserstoffe, in denen jedes Kohlenstoffatom vier Einfachbindungen hat, außer einem, das drei Einfachbindungen und eine „freie“ Bindung hat. Solche Moleküle kann man sich als Wurzelbäume vorstellen. Die Ecken sind die Kohlenstoffatome, und jede Ecke hat 0, 1, 2 oder 3 Söhne. Die Anordnung der Söhne einer Ecke ist unwesentlich. Sei  $r_n$  die Anzahl solcher Bäume mit  $n$  Ecken (d.h. von Alkylradikalen mit  $n$  Kohlenstoffatomen), und sei  $r(x)$  die erzeugende Funktion.

(a) \*\*Beweisen Sie die Gleichung

$$r(x) = 1 + \frac{x}{6} (r(x)^3 + 3r(x^2)r(x) + 2r(x^3)).$$

(b) Berechnen Sie mit dieser Gleichung einige Werte  $r_n$  für kleine  $n$ . Vergleichen Sie Ihre Werte mit denen in einem Chemiebuch.

(c) <sup>Inf</sup> Schreiben Sie ein Programm, das die Berechnungen aus (b) durchführt. Ein ehrgeizigeres Projekt wäre ein Programm zu schreiben, das die Koeffizienten von erzeugenden Funktionen berechnet, die durch Gleichungen verschiedener Typen gegeben sein können.

## 12.5 Würfeln

**Problem.** Wir spielen Mensch–Ärgere–Dich–Nicht und wollen loslaufen. Wie oft müssen wir im Schnitt würfeln, bis eine 6 fällt?<sup>6</sup>

Die Wahrscheinlichkeit, gleich in der ersten Runde eine 6 zu würfeln, ist  $p = \frac{1}{6}$ . Die Wahrscheinlichkeit dafür, dass in der ersten Runde keine 6 fällt, aber in der zweiten, ist  $(1-p)p$ ; allgemein ist die Wahrscheinlichkeit, in der  $i$ -ten Runde die erste 6 zu würfeln,  $q_i = (1-p)^{i-1}p$ . Die durchschnittliche Anzahl der Runden (d.h. der Erwartungswert) ist dann

$$S = \sum_{i=0}^{\infty} iq_i = \sum_{i=1}^{\infty} i(1-p)^{i-1}p.$$

Zur Berechnung dieser Reihe führen wir die erzeugende Funktion  $q(x) = q_1x + q_2x^2 + \dots$  ein. Gliedweises Ableiten dieser Reihe ergibt  $q'(x) = 1 \cdot q_1 + 2 \cdot q_2x + 3 \cdot q_3x^2 + \dots$ , also ist das gesuchte  $S$  gerade der Wert von  $q'(1)$ .

Nicht ganz mühefrei berechnen wir unsere erzeugende Funktion als

$$q(x) = \frac{p}{1-p} \cdot \frac{1}{1-(1-p)x} - \frac{p}{1-p}.$$

Eine kleine Übung im Ableiten ergibt  $q'(x) = p/(1-(1-p)x)^2$ , und damit  $S = q'(1) = \frac{1}{p}$ . In unserem Fall, für  $p = \frac{1}{6}$ , ist die durchschnittliche Anzahl der Runden somit 6.

---

<sup>6</sup>Dies ist eine harmlose Formulierung des Problems; eine andere Variante, die sich anbietet, ist Russisches Roulette.

Es gibt auch eine viel kürzere Lösung: Wir würfeln auf jeden Fall mindestens einmal. Mit Wahrscheinlichkeit  $1 - p$  würfeln wir in der ersten Runde keine 6, dann erwarten uns im Schnitt immer noch  $S$  Runden (denn der Würfel hat kein Gedächtnis, die Situation nach einem erfolglosen Versuch ist die gleiche wie ganz am Anfang). Deshalb ist

$$S = 1 + (1 - p)S,$$

und wir bekommen direkt  $S = 1/p$  heraus.

Die in diesem Abschnitt vorgeführte Methode mit erzeugenden Funktionen hat viele Anwendungen in der Wahrscheinlichkeitstheorie. Ist  $X$  eine Zufallsvariable, die den Wert  $i$  mit Wahrscheinlichkeit  $q_i$  annimmt,  $i = 0, 1, 2, \dots$ , und ist  $q(x) = \sum_{i=0}^{\infty} q_i x^i$  die erzeugende Funktion, dann ist der Erwartungswert von  $X$  gleich  $q'(1)$ .

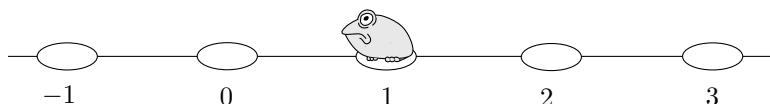
## Aufgaben

1. Verwenden Sie wie oben erzeugende Funktionen zur Berechnung
  - (a) der durchschnittlichen Anzahl der Sechsen, die bei  $n$  Würfen fallen,
  - (b) \*des Erwartungswertes von dem Ausdruck  $(X - 6)^2$ , wobei  $X$  die Anzahl der Würfe mit einem Würfel ist, bis die erste 6 fällt. (Das ist ein Maß für die „typische Abweichung“ von der erwarteten Anzahl der Runden, sie heißt *Varianz*.)
  - (c) Sei  $X$  eine Zufallsvariable, die die Werte  $0, 1, 2, \dots$  annimmt (den Wert  $i$  mit Wahrscheinlichkeit  $q_i$ ), und sei  $q(x)$  die erzeugende Funktion der  $q_i$ . Finden Sie einen Ausdruck für die Varianz von  $X$ , d.h. für die Größe  $\text{Var}[X] = \mathbf{E}[(X - \mathbf{E}[X])^2]$ , der Ableitungen von  $q(x)$  an geeigneten Stellen verwendet.

## 12.6 Zufallswege

Stellen Sie sich die reelle Zahlengerade in die Ebene gezeichnet vor, die ganzen Zahlen mit Kreisen markiert. Ein Frosch hüpfst von Kreis zu Kreis, und zwar nach folgenden Regeln:

- Am Anfang (vor dem ersten Sprung) sitzt der Frosch auf der Zahl 1.



- In jedem Zug hüpfst der Frosch entweder zwei Kreise nach rechts (von  $i$  nach  $i + 2$ ) oder einen Kreis nach links (von  $i$  nach  $i - 1$ ). Er entscheidet sich immer zufällig für eine dieser Möglichkeiten,

die beide die gleiche Wahrscheinlichkeit haben (so als würde er eine faire Münze werfen und seine Entscheidung nach dem Ergebnis Kopf oder Zahl richten).

**Problem.** Wie groß ist die Wahrscheinlichkeit, dass der Frosch irgendwann einmal auf die Zahl 0 kommt?

Zunächst einmal müssen wir klären, was mit so einer Wahrscheinlichkeit gemeint sein soll. Es ist leicht die Wahrscheinlichkeit zu definieren, dass der Frosch die 0 mit einem der ersten sieben Sprünge erreicht (nennen wir diese Wahrscheinlichkeit  $P_7$ ). Für die ersten sieben Sprünge sind  $2^7$  verschiedene Sprungfolgen möglich, denn vor jedem Sprung entscheidet sich der Frosch für eine von zwei Möglichkeiten, und diese Entscheidungen kann er beliebig miteinander kombinieren. Nach den Regeln unseres Spiels haben alle diese Sprungfolgen die gleiche Wahrscheinlichkeit. Die oben definierte Wahrscheinlichkeit  $P_7$  ist gleich der Anzahl der Sprungfolgen, die bei der 0 vorbeikommen (davon gibt es 75), geteilt durch die Gesamtzahl aller Sprungfolgen, also durch  $2^7$ .

Die gesuchte Wahrscheinlichkeit  $P$  kann man als den Grenzwert  $P = \lim_{i \rightarrow \infty} P_i$  definieren, wobei  $P_i$  die oben exemplarisch für  $i = 7$  erklärte Wahrscheinlichkeit ist. Dieser Grenzwert existiert, weil  $P_1 \leq P_2 \leq \dots \leq 1$ .

Sei  $a_i$  die Anzahl der Sprungfolgen der ersten  $i$  Sprünge, bei denen der Frosch die 0 mit dem  $i$ -ten Sprung erreicht, aber nicht vorher. Wir haben also

$$P = \sum_{i=1}^{\infty} \frac{a_i}{2^i}.$$

Wenn wir die erzeugende Funktion  $a(x) = a_1x + a_2x^2 + a_3x^3 + \dots$  einführen, erhalten wir  $P = a(\frac{1}{2})$ .

Zur Lösung des Problem wird es nützlich sein, auch solche Sprungfolgen zu betrachten, die bei einer anderen Zahl starten als bei der 1 (die dann aber nach den gleichen Regeln ablaufen). Was ist zum Beispiel die Anzahl  $b_i$  der Sprungfolgen, die bei der Zahl 2 beginnen und mit dem  $i$ -ten Sprung erstmalig die 0 erreichen? Damit eine solche Sprungfolge zur 0 gelangen kann, muss sie erst 1 erreichen. Sei  $j$  die Nummer des Sprunges, mit dem die 1 erstmalig erreicht wird. Wenn wir  $j$  kennen, dann wissen wir, es gibt  $a_j$  Möglichkeiten, in den Sprüngen  $1, 2, \dots, j-1$  nicht auf die 1 zu treten und genau mit dem  $j$ -ten Sprung auf ihr zu landen. Dann bleiben noch  $i-j$  Sprünge

um von 1 zur 0 zu gelangen, und die Anzahl der Möglichkeiten für diese  $i - j$  Sprünge ist  $a_{i-j}$ . Für gegebenes  $j$  gibt es also  $a_j a_{i-j}$  Möglichkeiten, und insgesamt erhalten wir<sup>7</sup>

$$b_i = \sum_{j=1}^{i-1} a_j a_{i-j}.$$

In der Sprache der erzeugenden Funktionen heißt das  $b(x) = a(x)^2$ .

Entsprechend sei  $c_i$  die Anzahl der Sprungfolgen, die bei der Zahl 3 starten und die 0 erstmals mit dem  $i$ -ten Sprung erreichen. Wie vorhin sehen wir, dass  $c(x) = a(x)b(x) = a(x)^3$ .

Nun betrachten wir Sprungfolgen, die bei 1 beginnen, aus einem anderen Blickwinkel. Mit dem ersten Schritt erreicht der Frosch entweder die 0 direkt (dann ist  $a_1 = 1$ ), oder er springt auf die Zahl 3. Im zweiten Fall hat er  $c_{i-1}$  Möglichkeiten, die 0 erstmals nach weiteren  $i - 1$  Sprüngen zu erreichen. Für  $i > 1$  ist deshalb  $a_i = c_{i-1}$ . Als Beziehung zwischen den erzeugenden Funktionen bedeutet das

$$a(x) = x + xc(x) = x + xa(x)^3. \quad (12.11)$$

Insbesondere erhalten wir für  $x = \frac{1}{2}$  die folgende Gleichung (wenn wir  $P = a(\frac{1}{2})$  schreiben):

$$P = \frac{1}{2} + \frac{1}{2} P^3.$$

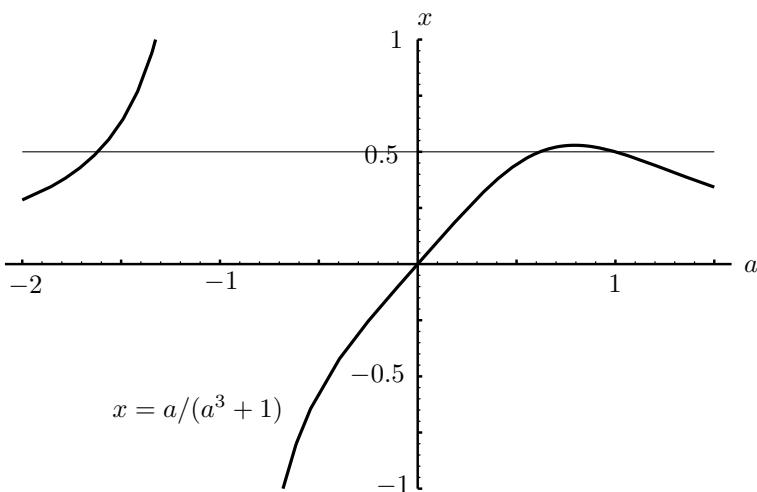
Sie hat drei Lösungen:  $1, \frac{1}{2}(\sqrt{5} - 1)$  und  $-\frac{1}{2}(\sqrt{5} + 1)$ . Die negative Lösung können wir natürlich gleich ausschließen. Der richtige Wert ist der zweite,  $P = \frac{1}{2}(\sqrt{5} - 1) = 0,618033988\dots$  (wieder der goldene Schnitt!).

Warum kann es nicht die 1 sein? Hier ist ein mögliches Argument.

Weil die Reihe  $a(x)$  für  $x = \frac{1}{2}$  konvergiert und weil alle  $a_i$  nicht negativ sind, ist  $a(x)$  eine monoton steigende stetige Funktion in  $x$  auf dem Intervall  $(0, \frac{1}{2}]$ . Außerdem muss  $a(x)$  eine Nullstelle der Gleichung (12.11) sein, mit anderen Worten, für alle solche  $x$  muss  $x = a(x)/(a(x)^3 + 1)$  sein. Wenn wir die Funktion  $a \rightarrow a/(a^3 + 1)$  wie in Abb. 12.2 zeichnen, sehen wir, dass  $a(\frac{1}{2})$  nicht durch den am weitesten rechts liegenden Schnittpunkt der Gerade  $x = \frac{1}{2}$  mit der eingezeichneten Kurve gegeben sein kann, weil dann für alle  $x$ , die auch nur ein wenig kleiner als  $\frac{1}{2}$

---

<sup>7</sup>Hier nutzen wir die Tatsache aus, dass Sprünge nach links immer „kurz“ sind, der Frosch kann nicht von 2 nach 0 gelangen, ohne zuerst auf die 1 zu springen.



**Abb. 12.2** Die Funktion  $x = a/(a^3 + 1)$ .

sind,  $a(x) > 1$  wäre. Diese Überlegung lässt sich zu einem richtigen Beweis ausarbeiten (man muss die Tangente an die Kurve im Punkt  $(1, 1)$  berechnen), wir hoffen aber, das Bild ist überzeugend genug.

Aus Gleichung (12.11) könnten wir im Prinzip die Funktion  $a(x)$  berechnen und dann versuchen die Zahlen  $a_i$  zum Beispiel mit Hilfe der Taylorreihe zu bestimmen (ein ziemlich mühsames Geschäft). Das ist ein sehr angenehmer Effekt der vorgestellten Lösung, dass wir nichts dergleichen zu tun brauchen.

## Aufgaben

- Betrachten Sie einen Zufallsweg: Wir starten bei der Zahl 0 und gehen in jedem Schritt mit gleicher Wahrscheinlichkeit von  $i$  nach  $i + 1$  oder nach  $i - 1$ .
  - \*Beweisen Sie, dass wir mit Wahrscheinlichkeit 1 irgendwann zur 0 zurückkommen.
  - Beweisen Sie, dass mit Wahrscheinlichkeit 1 jede Zahl  $k$  mindestens einmal besucht wird.
- Betrachten Sie einen Zufallsweg wie in der vorangegangenen Aufgabe.
  - \*Sei  $S_n$  die erwartete Anzahl Schritte, bis  $n$  erreicht wird (aus der vorigen Aufgabe wissen wir, dass der Weg mit Wahrscheinlichkeit 1 früher oder später bei  $n$  vorbeikommt). Was ist falsch an der folgenden Argumentation? Wir behaupten,  $S_n = cn$  für eine Konstante  $c$ . Das stimmt für  $n = 0$ , sei also  $n > 0$ . Im Schnitt benötigen wir  $S_1$  Schritte um 1 zu erreichen, und dann  $S_{n-1}$  weitere Schritte um  $n$  von 1 aus zu

erreichen. Deshalb ist  $S_n = S_1 + S_{n-1} = c + c(n-1) = cn$ , wobei  $c = S_1$ .

(b) \*\*Wie viele Schritte muss man im Schnitt gehen, um mindestens  $n$  Schritte von 0 wegzukommen (d.h. um  $n$  oder  $-n$  zu erreichen)?

## 12.7 Zahlpartitionen

Auf wie viele Arten kann man eine natürliche Zahl  $n$  als Summe natürlicher Zahlen schreiben? Die Antwort ist nicht allzu schwierig, wenn wir *geordnete Partitionen* von  $n$  zählen; das heißt, wenn wir die Ausdrücke  $3 = 2 + 1$  und  $3 = 1 + 2$  als zwei verschiedene Arten, 3 als Summe darzustellen, zählen (Aufgabe 1). Das Problem wird sehr viel schwieriger und interessanter, wenn wir Ausdrücke, die sich nur durch die Reihenfolge der Summanden unterscheiden, als identisch ansehen (in diesem Abschnitt sprechen wir dann einfach von *Partitionen von  $n$* ). Für  $n = 5$  zum Beispiel sind die möglichen Partitionen  $5 = 1 + 1 + 1 + 1 + 1$ ,  $5 = 1 + 1 + 1 + 2$ ,  $5 = 1 + 2 + 2$ ,  $5 = 1 + 1 + 3$ ,  $5 = 2 + 3$ ,  $5 = 1 + 4$  und  $5 = 5$ . Sei  $p_n$  die Anzahl der Partitionen von  $n$  in diesem Sinn.

Um die Darstellung der Partitionen eindeutig zu machen, können wir eine „Normalschreibweise“ einführen und z.B. darauf bestehen, dass die Summanden in nicht fallender Reihenfolge geschrieben werden, so wie wir es bei der Auflistung der Partitionen von 5 getan haben. Eine andere Formulierung dieser Frage ist also: Auf wie viele Arten können wir aus  $n$  Ziegeln eine „nicht fallende Mauer“ wie im folgenden Bild bauen (entsprechend den Partitionen  $10 = 1+1+2+2+4$  und  $10 = 1+1+2+6$ )?



(So ein Bild heißt das *Ferrers-Diagramm* der gegebenen Partition.)

Die Definition von  $p_n$  sieht ziemlich einfach aus, und so mag es vielleicht überraschen, dass es keine „einfache“ Formel für  $p_n$  gibt (im Gegensatz etwa zu den Binomialkoeffizienten). Das Problem der Abschätzung von  $p_n$  wurde ursprünglich in der Zahlentheorie betrachtet und 1918 mit unglaublicher Genauigkeit von Hardy und Ramanujan gelöst. (Die Geschichte wird im Buch von Littlewood [25] erzählt, eine sehr empfehlenswerte Lektüre über Mathematik.) Tatsächlich haben Hardy und Ramanujan eine verblüffend exakte (und komplizierte) Formel für  $p_n$  gefunden. Diese genauen Resultate zu beweisen oder auch

nur zu verstehen erfordert Vertrautheit mit einer recht anspruchsvollen Theorie (siehe z.B. Andrews [34]). Hier werden wir dieses Problem nur sehr oberflächlich behandeln; wenn man sich clever anstellt, erhält man nämlich asymptotische Abschätzungen von vernünftiger Qualität für  $p_n$  auf einfache Weise mit erzeugenden Funktionen, und genau das wollen wir tun.

Wir wissen, wie man die Anzahl der Lösungen einer Gleichung der Gestalt

$$i_1 + i_2 + \cdots + i_k = n,$$

wo der Wert eines jeden  $i_j$  in einer vorgegebenen Menge liegt, als Koeffizienten von  $x^n$  in einem geschickt gewählten Polynom ausdrückt. Hier kommt es allerdings auf die Reihenfolge der  $i_j$  an, da ist es nicht so offensichtlich, wie man eine Beziehung zu den (ungeordneten) Partitionen von  $n$  herstellen soll. Der Trick ist,  $i_j$  als *den Beitrag der Summanden mit Wert j* in einer Partition von  $n$  aufzufassen, oder, mit anderen Worten, die Anzahl der Ziegel, die in unserer nicht fällenden Mauer in Stapeln der Höhe genau  $j$  liegen. Dann stehen die Partitionen von  $n$  in Bijektion mit den Lösungen der Gleichung

$$i_1 + i_2 + \cdots + i_n = n$$

mit

$$i_1 \in \{0, 1, 2, 3, \dots\}, \quad i_2 \in \{0, 2, 4, 6, \dots\}, \dots, \quad i_j \in \{0, j, 2j, 3j, \dots\}.$$

Zum Beispiel gehört die Partition  $5 = 1+2+2$  zu der Lösung  $i_1 = 1$ ,  $i_2 = 4$ ,  $i_3 = i_4 = i_5 = 0$ .

Der nächste Schritt ist Routine. Aus der neuen Formulierung erhalten wir sofort, dass  $p_n$  der Koeffizient von  $x^n$  ist in dem Produkt

$$\begin{aligned} P_n(x) &= (1+x+x^2+\cdots)(1+x^2+x^4+x^6+\cdots)\cdots(1+x^n+x^{2n}+\cdots) \\ &= \prod_{k=1}^n \frac{1}{1-x^k}. \end{aligned}$$

Dieses endliche Produkt ist *nicht* die erzeugende Funktion der Folge  $(p_n)_{n=0}^\infty$ . Für die „richtige“ erzeugende Funktion (bei der  $p_n$  der Koeffizient von  $x^n$  für alle  $n$  zugleich ist) müssen wir das unendliche Produkt

$$P(x) = \prod_{k=1}^{\infty} \frac{1}{1-x^k}$$

betrachten. Um aber niemanden mit einem unendlichen Produkt zu erschrecken, bleiben wir für die Abschätzung von  $p_n$  beim endlichen Produkt  $P_n(x)$ .

Wir werden nun eine obere Schranke für  $p_n$  herleiten und verwenden dazu die schon im Beweis von Satz 3.6.1 (Abschätzung des Binomialkoeffizienten) demonstrierte Methode. Für alle Zahlen  $x \in (0, 1)$  ist

$$p_n \leq \frac{1}{x^n} P_n(x) = \frac{1}{x^n} \prod_{k=1}^n \frac{1}{1-x^k}.$$

Wir möchten  $x$  so wählen, dass die rechte Seite möglichst klein wird. Im Umgang mit Produkten ist es oft angebracht zum Logarithmus überzugehen; in diesem Fall erhalten wir

$$\ln p_n \leq \ln \left( \frac{1}{x^n} P_n(x) \right) = -n \ln x - \sum_{k=1}^n \ln(1-x^k).$$

Wir erinnern an die Potenzreihe (12.3) des Logarithmus:

$$-\ln(1-y) = \frac{y}{1} + \frac{y^2}{2} + \frac{y^3}{3} + \frac{y^4}{4} + \dots$$

für alle  $y \in (-1, 1)$ . Deshalb können wir schreiben:

$$\begin{aligned} -\sum_{k=1}^n \ln(1-x^k) &= \sum_{k=1}^n \sum_{j=1}^{\infty} \frac{x^{kj}}{j} = \sum_{j=1}^{\infty} \frac{1}{j} \sum_{k=1}^n x^{jk} \\ &\leq \sum_{j=1}^{\infty} \frac{1}{j} \sum_{k=1}^{\infty} x^{jk} = \sum_{j=1}^{\infty} \frac{1}{j} \frac{x^j}{1-x^j}. \end{aligned}$$

Vielleicht etwas unerwartet wenden wir nun die Formel für geometrische Reihen „rückwärts“ an. Es gilt

$$1-x^j = (1-x)(1+x+x^2+\dots+x^{j-1}) \geq (1-x)jx^{j-1}$$

(weil ja  $0 < x < 1$  ist), somit haben wir

$$\sum_{j=1}^{\infty} \frac{1}{j} \frac{x^j}{1-x^j} \leq \sum_{j=1}^{\infty} \frac{1}{j} \frac{x^j}{(1-x)jx^{j-1}} = \frac{x}{1-x} \sum_{j=1}^{\infty} \frac{1}{j^2}.$$

Als Nächstes machen wir Gebrauch von der folgenden bemerkenswerten

**12.7.1 Tatsache.**  $\sum_{j=1}^{\infty} \frac{1}{j^2} = \frac{\pi^2}{6}$ .

Als mathematische Nachspeise werden wir zum Abschluss dieses Kapitels einen Beweis dafür geben (der auf Euler zurückgeht). Damit können wir unsere Abschätzung von  $\ln p_n$  fortführen und erhalten

$$\ln p_n \leq -n \ln x + \frac{\pi^2}{6} \frac{x}{1-x}.$$

In der jetzt folgenden Rechnung ist es praktisch, eine neue Variable  $u = x/(1-x)$  einzuführen ( $u$  darf eine beliebige Zahl in  $[0, \infty)$  sein, und  $x = u/(1+u)$ ). Mit dieser Substitution und der Ungleichung  $\ln(1 + \frac{1}{u}) \leq \frac{1}{u}$  (die man leicht aus Tatsache 3.5.4 ableitet) erhalten wir

$$\ln p_n < n \ln \left(1 + \frac{1}{u}\right) + \frac{\pi^2}{6} u \leq \frac{n}{u} + \frac{\pi^2}{6} u.$$

Setzen wir  $u = \sqrt{6n}/\pi$  in dem letzten Ausdruck, dann erhalten wir  $\ln p_n \leq \pi \sqrt{\frac{2}{3} n}$ . (Warum ist  $u = \sqrt{6n}/\pi$  die richtige Wahl? Eine kleine Rechnung (Analysis!) zeigt, dass die betrachtete obere Schranke für  $\ln p_n$  als Funktion von  $u$  bei diesem Wert ihr Minimum annimmt.) Wir haben also Folgendes gezeigt:

**12.7.2 Satz.** Für alle  $n \geq 1$  ist

$$p_n < e^{\pi \sqrt{\frac{2}{3} n}} = e^{(2,5650\dots) \sqrt{n}}.$$

**Eine untere Schranke.** Wie gut ist die gerade hergeleitete obere Schranke? Aus den Ergebnissen von Hardy und Ramanujan folgt, dass  $p_n \sim \frac{1}{4\sqrt{3}n} e^{\pi \sqrt{\frac{2}{3} n}}$ , d.h. unsere obere Schranke ist recht gut — die Konstante im Exponenten ist sogar korrekt. Was würden wir aber tun, wenn wir in der Wildnis wären (im weiteren Sinne, soll heißen: weit weg von jeder mathematischen Bibliothek) und wissen wollten, ob die Schranke aus Satz 12.7.2 das richtige Bild vermittelt? Wir leiten schnell eine untere Schranke her, aus der wir zumindest sehen, dass sie nicht unrealistisch hoch ist.

In Aufgabe 1 laden wir Sie ein, die Anzahl geordneter Partitionen von  $n$  in  $k$  Summanden als  $\binom{n-1}{k-1}$  zu bestimmen. Weil zu jeder (ungeordneten) Partition mit  $k$  Summanden höchstens  $k!$  geordnete Partitionen gehören, ist

$$p_n \geq \frac{\binom{n-1}{k-1}}{k!} \geq \frac{(n-1)(n-2)\dots(n-k+1)}{(k!)^2}$$

für jedes  $k \in \{1, 2, \dots, n\}$ . Welches  $k$  ergibt die beste untere Schranke? Wenn wir  $k$  um 1 erhöhen, wird der Nenner mit dem Faktor  $(k+1)^2$

multipliziert und der Zähler mit  $n - k$ . Demzufolge ist  $k + 1$  besser als  $k$ , wann immer  $(k + 1)^2 < n - k$  ist, und für das beste  $k$  sollte  $(k + 1)^2$  ungefähr gleich  $n - k$  sein. Um die Sache nicht zu kompliziert zu machen setzen wir  $k = \lfloor \sqrt{n} \rfloor$ . Die Vorstellung dabei ist, dass sich dann  $(n - 1)(n - 2) \dots (n - k + 1)$  in etwa so verhält wie  $n^{\sqrt{n}}$ . Es folgt eine exakte Berechnung, die diese Vorstellung stützt. Wir haben

$$(n - 1)(n - 2) \dots (n - k + 1) \geq (n - k)^{k-1} = n^{k-1} \left(1 - \frac{k}{n}\right)^{k-1},$$

und weil  $\frac{k}{n} = \lfloor \sqrt{n} \rfloor / n \leq 1 / \lfloor \sqrt{n} \rfloor = \frac{1}{\lfloor \sqrt{n} \rfloor}$  ist und  $(1 - \frac{1}{\lfloor \sqrt{n} \rfloor})^{k-1} > e^{-1}$ , erhalten wir weiter

$$n^{k-1} \left(1 - \frac{k}{n}\right)^{k-1} \geq n^{k-1} \left(1 - \frac{1}{k}\right)^{k-1} \geq \frac{n^k}{e^n}.$$

Nach Satz 3.5.5 haben wir die obere Schranke  $k! \leq ek(k/e)^k$ , womit wir

$$p_n \geq \left(\frac{n}{k^2}\right)^k \frac{e^{2k-3}}{nk^2} \geq \frac{e^{2k-3}}{n^2} \geq \frac{1}{e^5 n^2} e^{2\sqrt{n}}$$

erhalten. Ist  $n$  groß genug, dann ist  $n^2$  viel kleiner als  $e^{\sqrt{n}}$ , folglich ist  $n^{-2}e^{2\sqrt{n}} = \Omega(e^{\sqrt{n}})$ . Wir haben also gezeigt, dass  $p_n$ , wenn  $n$  groß genug ist, zwischen  $e^{c_1\sqrt{n}}$  und  $e^{c_2\sqrt{n}}$  liegt, wobei  $c_2 > c_1 > 0$  geeignete Konstanten sind. Derartige Information über das Wachstum einer Funktion ist oft schon ausreichend.

*Beweis von Tatsache 12.7.1.* Wir beginnen mit der Formel von de Moivre (siehe auch Aufgabe 1.3.4):  $(\cos \alpha + i \sin \alpha)^n = \cos(n\alpha) + i \sin(n\alpha)$ , wobei  $i$  die imaginäre Einheit ist,  $i^2 = -1$ . Wenn wir die linke Seite mit dem Binomialsatz ausrechnen und nur den Imaginärteil auf beiden Seiten betrachten, erhalten wir die Identität

$$\begin{aligned} \binom{n}{1} \sin \alpha \cos^{n-1} \alpha - \binom{n}{3} \sin^3 \alpha \cos^{n-3} \alpha + \binom{n}{5} \sin^5 \alpha \cos^{n-5} \alpha - \dots \\ = \sin(n\alpha). \end{aligned}$$

Mit Hilfe der Funktion  $\cot \alpha = \frac{\cos \alpha}{\sin \alpha}$  können wir die linke Seite auch so schreiben:

$$\sin^n \alpha \left[ \binom{n}{1} \cot^{n-1} \alpha - \binom{n}{3} \cot^{n-3} \alpha + \binom{n}{5} \cot^{n-5} \alpha - \dots \right].$$

Von nun an sei  $n = 2m + 1$  ungerade. Dann kann man den in eckigen Klammern stehenden Ausdruck als  $P(\cot^2 \alpha)$  schreiben, wobei  $P(x)$  das Polynom  $\binom{n}{1}x^m - \binom{n}{3}x^{m-1} + \binom{n}{5}x^{m-2} - \dots$  ist.

Wir behaupten, dass die  $m$  Zahlen  $r_1, r_2, \dots, r_m$  die Nullstellen von  $P(x)$  sind, wobei  $r_k = \cot^2 \frac{k\pi}{n}$ . Und wirklich, für  $\alpha = \frac{k\pi}{n}$  ist  $\sin \alpha \neq 0$ ,

jedoch  $\sin(n\alpha) = 0$ , also muss  $P(\cot^2 \alpha)$  gleich 0 sein. Weil  $r_1, \dots, r_m$  alle verschieden sind und  $P(x)$  Grad  $m$  hat, kann es keine weiteren Nullstellen geben. Daraus folgt

$$P(x) = n(x - r_1)(x - r_2) \dots (x - r_m).$$

Vergleich der Koeffizienten von  $x^{m-1}$  auf beiden Seiten der letzten Gleichung führt zu  $n(r_1 + r_2 + \dots + r_m) = \binom{n}{3}$ . So haben wir die Identität

$$\sum_{k=1}^m \cot^2 \frac{k\pi}{2m+1} = \frac{m(2m-1)}{3} \quad (12.12)$$

hergeleitet. Für  $0 < \alpha < \frac{\pi}{2}$  gilt  $\cot \alpha = 1/\tan \alpha < 1/\alpha$ , und so liefert (12.12) die Ungleichung

$$\sum_{k=1}^m \frac{(2m+1)^2}{\pi^2 k^2} > \frac{m(2m-1)}{3}$$

oder

$$\sum_{k=1}^m \frac{1}{k^2} > \frac{\pi^2}{6} \frac{2m(2m-1)}{(2m+1)^2}.$$

Für  $m \rightarrow \infty$  ergibt das  $\sum_{k=1}^{\infty} 1/k^2 \geq \pi^2/6$ . Die Herleitung der oberen Schranke erfolgt analog. Mit der Identität  $\cot^2 \alpha = \sin^{-2} \alpha - 1$  und der Ungleichung  $\sin \alpha < \alpha$ , die für  $0 < \alpha < \frac{\pi}{2}$  gilt, ergibt (12.12)

$$\frac{m(2m-1)}{3} + m = \sum_{k=1}^m \frac{1}{\sin^2 \frac{k\pi}{2m+1}} > \sum_{k=1}^m \frac{(2m+1)^2}{\pi^2 k^2},$$

was für  $m \rightarrow \infty$  zu  $\sum_{k=1}^{\infty} 1/k^2 \leq \pi^2/6$  führt.  $\square$

## Aufgaben

1. (a) Zeigen Sie, dass die Anzahl der geordneten Partitionen von  $n$  mit  $k$  Summanden, d.h. die Anzahl der Lösungen von  $i_1 + i_2 + \dots + i_k = n$ , bei denen alle  $i_j \geq 1$  sind,  $\binom{n-1}{k-1}$  ist.  
 (b) Berechnen Sie die Anzahl aller geordneten Partitionen von  $n$ . Für  $n = 3$  haben wir z.B. die vier geordneten Partitionen  $3 = 1 + 1 + 1$ ,  $3 = 1+2$ ,  $3 = 2+1$  und  $3 = 3$ . Finden Sie drei Lösungen: eine „direkte“ kombinatorische, eine auf (a) basierende und eine mit erzeugenden Funktionen.
2. (a) *Inf* Schreiben Sie ein Programm, das alle Partitionen von  $n$  aufliest, jede genau einmal. (Das ist eine hübsche Programmierübung.)  
 (b) *Inf* Schreiben Sie ein Programm, das zu gegebenem  $n$  den Wert  $p_n$  berechnet. Zur Genauigkeit: Das Programm sollte zumindest für  $n$

unter 5000 in der Lage sein,  $p_n$  auf 8 Stellen genau zu berechnen (wobei  $p_n$  deutlich kleiner ist als  $10^{100}$ ). Sie können auch einen Wettbewerb organisieren, wer das schnellste korrekte Programm schreibt. (Ein Blick in die Literatur kann ihnen bei einem solchen Wettbewerb einen großen Vorteil verschaffen.)

3. Diesmal betrachten wir die Anzahl  $\bar{p}_n$  der Partitionen von  $n$ , wo *alle Summanden verschieden* sind. Zum Beispiel sind für  $n = 5$  nur die Partitionen  $5 = 1 + 4$  und  $5 = 2 + 3$  zulässig.
  - (a) Drücken Sie  $\bar{p}_n$  als Koeffizienten von  $x^n$  in einem geeigneten Polynom aus.
  - (b) Zeigen Sie mit der Methode aus dem Beweis von Satz 12.7.2, dass  $\bar{p}_n \leq e^{2\sqrt{n}}$  ist.
  - (c) \*Beweisen Sie für alle genügend großen  $n$  eine untere Schranke der Form  $\bar{p}_n \geq e^{c\sqrt{n}}$ , wobei  $c > 0$  eine Konstante ist. Wie groß können Sie  $c$  wählen?
4. (a) Schreiben Sie die erzeugende Funktion für die Zahlen  $\bar{p}_n$  aus Aufgabe 3 auf (die erzeugende Funktion ist ein unendliches Produkt).
  - (b) Bestimmen Sie die erzeugende Funktion für die Anzahl der ungeordneten Partitionen von  $n$  in lauter *ungerade* Summanden (wieder ein unendliches Produkt).
  - (c) \*Überzeugen Sie sich, dass die erzeugenden Funktionen in (a) und (b) die gleichen sind, dass also die Anzahl der Partitionen in verschiedene Summanden gleich der Anzahl der Partitionen in ungerade Summanden ist. \*\*Finden Sie dafür auch ein direktes Argument (eine Bijektion)?
5. Die Königliche Münze von Middle Coinland prägt  $a_1$  verschiedene Typen von 1-Doublezon-Münzen,  $a_2$  Typen von 2-Doublezon-Münzen, usw. Zeigen Sie, dass die Anzahl der Arten, wie man die Summe von  $n$  Doublezons mit solchen Münzen bezahlen kann, gleich dem Koeffizienten von  $x^n$  ist in
 
$$\prod_{i=1}^n \frac{1}{(1-x^i)^{a_i}}.$$
6. (a) Drücken Sie die Anzahl nicht isomorpher Wurzelbäume der Höhe höchstens 2 mit  $m$  Blättern durch die Zahlen  $p_n$  aus. Wurzelbäume und ihre Isomorphismen wurden in Abschnitt 5.2 eingeführt. Die Wurzel zählt nicht als Blatt, und die Höhe eines Wurzelbaums ist der maximale Abstand eines Blattes von der Wurzel.
  - (b) Betrachten Sie diesmal Wurzelbäume der Höhe höchstens 2 mit  $m$  Ecken. Drücken Sie deren Anzahl durch die Zahlen  $p_n$  aus.
  - (c) \*Drücken Sie die Anzahl  $r_n$  der Wurzelbäume mit  $n$  Blättern, die alle Abstand 3 von der Wurzel haben, als Koeffizienten von  $x^n$  in einem

geeigneten Polynom aus (die Zahlen  $p_i$  dürfen darin vorkommen; Sie können sich von Aufgabe 5 inspirieren lassen).

(d) \*\*Zeigen Sie, dass für die Zahlen  $r_n$  aus (c)  $r_n = e^{O(n/\log n)}$  gilt. Verwenden Sie (c) und den Beweis von Satz 12.7.2. (Die Rechnung ist eine kleine Herausforderung.)

(e) \*Zeigen Sie, dass die Abschätzung aus (d) das Wachstum in etwa korrekt wiederspiegelt, d.h. dass  $r_n \geq e^{cn/\log n}$  für eine Konstante  $c > 0$ .



# 13

# Anwendungen der Linearen Algebra

---

Lineare Algebra ist der Teil der Algebra, der von linearen Gleichungssystemen, Matrizen, Determinanten, Vektorräumen und Ähnlichem handelt. In den vorangegangenen Kapiteln haben wir schon in mehreren Beweisen lineare Algebra angewendet, ganz besonders in Abschnitt 8.5. Hier werden wir ein paar weitere Methoden und Anwendungen vorführen. Als Erstes stellen wir zwei Probleme vor, in dem einen geht es um die Existenz so genannter Designs und in dem anderen um die Überdeckung eines vollständigen Graphen mit vollständigen bipartiten Graphen. Unvoreingenommen würde wohl kaum jemand vermuten, dass diese Probleme etwas mit Matrizen zu tun haben, und doch ist der Begriff des Rangs einer Matrix Grundlage einer eleganten Lösung. Interessierte Leser finden jede Menge ähnliches Material in dem sehr anregenden Buch von Babai und Frankl [14]. In den darauf folgenden zwei Abschnitten dieses Kapitels konstruieren wir zu jedem Graphen mehrere Vektorräume; durch sie erhalten wir eine griffige Beschreibung einiger Mengen, die zunächst sehr kompliziert scheinen. In Abschnitt 13.6 werden wir uns schließlich zwei elegante Algorithmen ansehen, in denen neben der linearen Algebra die probabilistische Methode eine Rolle spielt.

In diesem Kapitel setzen wir Grundkenntnisse in linearer Algebra voraus, eine kurze Zusammenfassung finden Sie im Anhang.

## 13.1 Designs

Wir betrachten Systeme endlicher Mengen, die einen hohen Grad an Regularität aufweisen, die so genannten Designs. Endliche projektive Ebenen sind ein Spezialfall dieses Konzepts, doch bei allgemeinen Designs entfällt der geometrische Hintergrund.

Sei  $V$  eine endliche Menge und  $\mathcal{B}$  ein System von Teilmengen der Menge  $V$ . Um zu betonen, dass das Mengensystem  $\mathcal{B}$  auf der Menge  $V$  „lebt“, schreiben wir es als geordnetes Paar  $(V, \mathcal{B})$ . (Ein solches Paar  $(V, \mathcal{B})$  kann man auch als eine Verallgemeinerung von Graphen ansehen, man spricht dann von *Hypergraphen*; die Punkte aus  $V$  heißen dann die *Ecken* und die Mengen in  $\mathcal{B}$  heißen *Hyperkanten*.) Wenn alle Mengen  $B \in \mathcal{B}$  die gleiche Kardinalität  $k$  haben, dann sagen wir,  $(V, \mathcal{B})$  ist *k-uniform*.

Ein wichtiges Beispiel für ein *k-uniformes* Mengensystem haben wir bereits in Kapitel 9 kennen gelernt: Dort haben wir gezeigt, dass die Menge  $V$  der Punkte einer endlichen projektiven Ebene zusammen mit der Menge  $\mathcal{B}$  der Geraden  $(k+1)$ -uniform ist (für eine geeignete Zahl  $k$ ), und dass darüber hinaus  $|V| = |\mathcal{B}| = k^2 + k + 1$  gilt. Dieses Beispiel sollte das Verständnis der folgenden Definition erleichtern, die auf den ersten Blick ziemlich technisch aussieht (die aber mit Beispielen unterfüttert werden wird).

**13.1.1 Definition.** Seien  $v, k, t$  und  $\lambda$  ganze Zahlen mit  $v > k \geq t \geq 1$  und  $\lambda \geq 1$ . Ein  $t$ -Design vom Typ  $(v, k, \lambda)$  (man sagt auch: mit Parametern  $(v, k, \lambda)$ ) ist ein Mengensystem  $(V, \mathcal{B})$ , das die folgenden Bedingungen erfüllt:

- (1)  $V$  hat  $v$  Elemente.
- (2) Jede Menge  $B \in \mathcal{B}$  hat  $k$  Elemente. Die Mengen in  $\mathcal{B}$  heißen die Blöcke.
- (3) Jede  $t$ -elementige Teilmenge der Menge  $V$  ist in genau  $\lambda$  Blöcken aus  $\mathcal{B}$  enthalten.

Zur Illustration dieser Definition folgen einige einfache Beispiele.

**Beispiel.** Sei  $V$  eine endliche Menge und  $k$  eine ganze Zahl. Wir setzen  $\mathcal{B} = \binom{V}{k}$  (in Worten:  $\mathcal{B}$  besteht aus allen  $k$ -elementigen Teilmengen von  $V$ ). Das Paar  $(V, \mathcal{B})$  heißt das *triviale Design*.

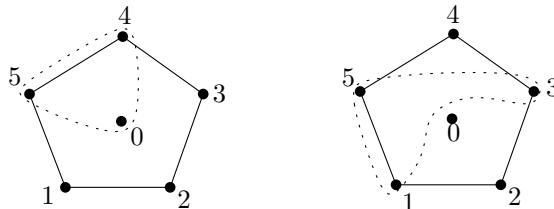
Man prüft leicht nach, dass  $(V, \mathcal{B})$  ein  $t$ -Design vom Typ  $(v, k, \lambda)$  ist, wobei  $t \in \{1, 2, \dots, k\}$  beliebig gewählt werden kann,  $v = |V|$  und  $\lambda = \binom{v-t}{k-t}$ . (Bitte überzeugen Sie sich, dass jede  $t$ -elementige Teilmenge von  $V$  in  $\binom{v-t}{k-t}$  Blöcken  $B \in \mathcal{B}$  enthalten ist.)

**Beispiel.** Sei  $V$  eine  $v$ -Menge, und sei  $k \geq 1$  ein Teiler von  $v$ . Partitionieren Sie die Menge  $V$  in disjunkte  $k$ -elementige Teilmengen  $B_1, B_2, \dots, B_{v/k}$  und setzen Sie  $\mathcal{B} = \{B_1, B_2, \dots, B_{v/k}\}$ . Dann ist  $(V, \mathcal{B})$  ein 1-Design vom Typ  $(v, k, 1)$ .

**Beispiel.** Sei  $V$  die Menge der Punkte einer projektiven Ebene der Ordnung  $n$ , und  $\mathcal{B}$  sei die Menge der Geraden. So ein Paar  $(V, \mathcal{B})$  ist ein 2-Design vom Typ  $(n^2 + n + 1, n + 1, 1)$ . Diese nicht triviale Tatsache haben wir in Abschnitt 9.1 bewiesen. Umgekehrt kann man zeigen, dass jedes 2-Design vom Typ  $(n^2 + n + 1, n + 1, 1)$  mit  $n \geq 2$  eine projektive Ebene der Ordnung  $n$  ist (Aufgabe 1).

**13.1.2 Beispiel.** Sei  $V = \{0, 1, 2, 3, 4, 5\}$ , und  $\mathcal{B}$  bestehe aus den folgenden Tripeln:  $\{0, 1, 2\}, \{0, 2, 3\}, \{0, 3, 4\}, \{0, 4, 5\}, \{0, 1, 5\}, \{1, 2, 4\}, \{2, 3, 5\}, \{1, 3, 4\}, \{2, 4, 5\}, \{1, 3, 5\}$ . Dann ist  $(V, \mathcal{B})$  ein 2-Design vom Typ  $(6, 3, 2)$ . (Das kann man ganz einfach mittels der Definition nachprüfen, man braucht dazu keinen besonderen Einfall.)

Dieses Design lässt sich auch „strukturierter“ definieren. Betrachten Sie einen Kreis mit Ecken  $1, 2, \dots, 5$  und einer zusätzlichen Ecke 0. Das System  $\mathcal{B}$  besteht dann aus allen Eckentripeln, die genau eine Kante aus dem Kreis enthalten, siehe die beiden Beispiele in nachstehendem Diagramm:



Diese Beispiele sollen den (korrekten) Eindruck erwecken, dass Designs eine gewisse Regularität verkörpern. In der Regel ist die Konstruktion von Designs eines vorgegebenen Typs gar nicht leicht, die grundlegende Frage in diesem ganzen Gebiet ist immer die Existenzfrage.

**Grundproblem.** Gegeben Zahlen  $v, k, \lambda, t$ : Entscheiden Sie, ob es ein  $t$ -Design vom Typ  $(v, k, \lambda)$  gibt oder nicht.

Wir werden nun mit algebraischen Mitteln einige notwendige Bedingungen herleiten.

Zum Abschluss dieser kurzen Einführung möchten wir noch erzählen, dass Designs ursprünglich aus der Statistik kommen, aus der Versuchsplanung nämlich. Diese Herkunft hat auch die oben eingeführte Notation beeinflusst.

Stellen Sie sich vor, wir wollten mehrere verschiedene Methoden, eine bestimmte Pflanze zu behandeln, bewerten (z.B. zum Schutz vor Parasiten). Dazu sind  $v$  Behandlungstypen zu vergleichen ( $v$  für „Varianten“). Wir werden die Behandlungen in einer Reihe von Experimenten vergleichen, in denen jeweils  $k$  Behandlungstypen vorkommen können (das ist durch die Versuchsbedingungen vorgegeben). Jedes Experiment wird einen *Block* mit getesteten Behandlungen bilden. Prinzipiell könnten wir alle möglichen  $k$ -Tupel von Behandlungen testen, doch in einer realen Testsituation ist diese triviale Vorgehensweise (vergleiche das „triviale Design“) viel zu aufwändig, und zwar schon für kleine Werte  $k$  und  $v$ . Aus diesem Grunde sind die Statistiker zu Versuchs-Designs übergegangen, so dass sie nicht alle möglichen  $k$ -Tupel testen müssen, sondern nur einige ausgewählte Blöcke. Das kann natürlich zu fehlerhaften Ergebnissen führen, denn die Experimente sind unvollständig: Einige der möglichen Blöcke werden nicht in Betracht gezogen, deshalb bleiben einige der möglichen Wechselwirkungen der Behandlungen unberücksichtigt. Um diese (umgangängliche) Unvollständigkeit der Tests zu kompensieren verlangen wir, dass wenigstens jedes Paar von Behandlungstypen in gleich vielen Versuchsböcken gemeinsam vorkommt. Der Plan einer solchen Versuchsreihe ist gerade ein 2-Design vom Typ  $(v, k, \lambda)$ . Wenn wir fordern, dass jedes Tripel von Behandlungstypen in gleich vielen (nämlich  $\lambda$ ) Versuchstripeln vorkommt, erhalten wir ein 3-Design vom Typ  $(v, k, \lambda)$ , und so weiter.

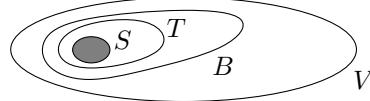
Einige Sorten von Designs laufen in der Literatur unter speziellem Namen: So heißen Designs mit  $\lambda = 1$  *Steiner-Systeme*, 2-Designs bezeichnet man üblicherweise als *Blockpläne*, und *taktische Konfigurationen* sind  $t$ -Designs mit  $t > 2$ .

**Bedingungen an die Parameter.** Es sollte klar sein, dass es ein  $t$ -Design mit Parametern  $(v, k, \lambda)$  nur gibt, wenn die Parameter gewisse Bedingungen erfüllen. Beispielsweise ist ein 1-Design vom Typ  $(v, k, 1)$  eine Partition einer  $v$ -Menge in  $k$ -Mengen, deshalb muss  $v$  durch  $k$  teilbar sein. Ein anderes, weniger triviales Beispiel liefern die projektiven Ebenen, wo  $v$  durch die Größe der Geraden eindeutig bestimmt ist. Der folgende Satz beschreibt die wichtigste Klasse notwendiger Bedingungen für die Existenz eines  $t$ -Designs vom Typ  $(v, k, \lambda)$ .

**13.1.3 Satz.** Angenommen, es gibt ein  $t$ -Design vom Typ  $(v, k, \lambda)$ . Dann müssen die folgenden Brüche in Wirklichkeit ganze Zahlen sein:

$$\lambda \frac{v(v-1)\dots(v-t+1)}{k(k-1)\dots(k-t+1)}, \quad \lambda \frac{(v-1)\dots(v-t+1)}{(k-1)\dots(k-t+1)}, \dots, \quad \lambda \frac{v-t+1}{k-t+1}.$$

*Beweis.* Wir verwenden die Methode des doppelten Abzählens. Sei  $(V, \mathcal{B})$  ein  $t$ -Design vom Typ  $(v, k, \lambda)$ . Wir wählen eine feste ganze Zahl  $s$  mit  $0 \leq s \leq t$  und eine  $s$ -Menge  $S \subseteq V$ . Wir bestimmen nun die Anzahl  $N$  der Paare  $(T, B)$  mit  $S \subseteq T \in \binom{V}{t}$  und  $T \subseteq B \in \mathcal{B}$ :



Einerseits kann man  $T$  auf  $\binom{v-s}{t-s}$  verschiedene Arten aussuchen, und jedes  $T$  ist Teilmenge von genau  $\lambda$  Blöcken  $B \in \mathcal{B}$ ; also ist  $N = \lambda \binom{v-s}{t-s}$ .

Andererseits kann man auch so argumentieren: Sei  $M$  die Anzahl der Blöcke, welche die Menge  $S$  enthalten. Weil jeder Block  $B$ , der  $S$  enthält,  $\binom{k-s}{t-s}$  Mengen  $T$  mit  $t$  Elementen und mit  $S \subseteq T$  enthält, gilt auch  $N = M \binom{k-s}{t-s}$ . Daher ist

$$M = \lambda \frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}} = \lambda \frac{(v-s) \dots (v-t+1)}{(k-s) \dots (k-t+1)},$$

und somit muss der Bruch auf der rechten Seite der Gleichung eine ganze Zahl sein, wie im Satz behauptet.  $\square$

*Bemerkung.* Wenn wir uns obigen Beweis für  $s = 0$  und für  $s = 1$  anschauen, sehen wir, dass  $\lambda \frac{v(v-1)\dots(v-t+1)}{k(k-1)\dots(k-t+1)}$  die Gesamtzahl der Blöcke angibt, und dass  $\lambda \frac{(v-1)\dots(v-t+1)}{(k-1)\dots(k-t+1)}$  die Anzahl jener Blöcke ist, die ein bestimmtes Element  $x \in V$  enthalten, sozusagen der „Grad von  $x$ “. In der oben angesprochenen statistischen Interpretation gibt diese Zahl an, wie oft die Behandlung  $x$  angewendet wurde; meist bezeichnet man sie mit dem Buchstaben  $r$  (für „repetitions“, also Wiederholungen).

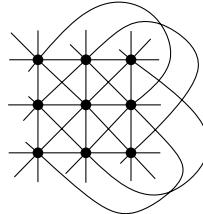
**13.1.4 Beispiel (Steiner–Tripel–Systeme).** Das „erste“ nicht triviale Beispiel für ein  $t$ -Design vom Typ  $(v, k, \lambda)$  erhält man für  $t = 2$ ,  $\lambda = 1$  und  $k = 3$ . Dies ist ein System von Tripeln, in dem jedes Punktpaar in genau einem Tripel enthalten ist. Wir kennen so etwas schon, das ist eine Überdeckung aller Kanten eines vollständigen Graphen mit Dreiecken.

In diesem Fall erfordern die Bedingungen aus Satz 13.1.3, dass

$$\frac{v(v-1)}{6} \quad \text{und} \quad \frac{v-1}{2}$$

ganze Zahlen sind. Daraus folgert man leicht, dass entweder  $v \equiv 1 \pmod{6}$  oder  $v \equiv 3 \pmod{6}$  sein muss. Demnach muss  $v$  eine

der Zahlen  $3, 7, 9, 13, 15, 19, 21, 25, 27, \dots$  sein. Für alle diese Werte von  $v$  existiert ein 2-Design vom Typ  $(v, 3, 1)$ . Solche Designs heißen *Steiner–Tripel–Systeme* (siehe Aufgabe 4). Für  $v = 7$  ist ein Steiner–Tripel–System eine projektive Ebene der Ordnung 2 (die Fano–Ebene). Für  $v = 9$  haben wir das Steiner–System



das man als *affine Ebene* auffassen kann, die man aus einer projektiven Ebene der Ordnung 3 durch Löschen einer Geraden und aller auf ihr liegenden Punkte erhält (siehe Aufgabe 9.1.10).

**Blockpläne.** Für  $t = 2$  (wenn wir also fordern, dass jedes Paar in genau  $\lambda$   $k$ -Tupeln aus  $\mathcal{B}$  enthalten ist) sehen die Bedingungen an die Parameter wie folgt aus:

$$\begin{aligned}\lambda v(v-1) &\equiv 0 \pmod{k(k-1)} \\ \lambda(v-1) &\equiv 0 \pmod{k-1}.\end{aligned}\tag{13.1}$$

Diese Bedingungen garantieren die Existenz eines Blockplans im Allgemeinen nicht mehr. Dann hilft das folgende wichtige (und schwierige) Resultat weiter:

**13.1.5 Satz (Satz von Wilson).** Für jede Wahl von Zahlen  $k \geq 1$  und  $\lambda \geq 1$  gibt es eine Zahl  $v_0(k, \lambda)$ , so dass für alle  $v \geq v_0(k, \lambda)$ , welche die Bedingungen (13.1) erfüllen, ein Blockplan mit Parametern  $(v, k, \lambda)$  existiert.

Das bedeutet, unsere Bedingungen an die Parameter sind auch für  $t = 2$  hinreichend, wenn nur die Grundmenge groß genug ist. Der Satz macht keine Aussage für kleine  $v$ -Werte, etwa über die Existenz von Blockplänen des Typs  $(k^2 + k + 1, k + 1, 1)$ , das sind endliche projektive Ebenen.

Wir haben den Satz hier der Vollständigkeit halber erwähnt, wir werden ihn nicht beweisen. Wenn Sie mögen, finden Sie einen Beweis im Buch von Beth, Jungnickel und Lenz [36].

## Aufgaben

1. (a) Überzeugen Sie sich, dass eine projektive Ebene der Ordnung  $q$  ein Blockplan vom Typ  $(q^2 + q + 1, q + 1, 1)$  ist.

- (b) \*Zeigen Sie nun die Umkehrung, dass nämlich jeder Blockplan vom Typ  $(q^2 + q + 1, q + 1, 1)$  eine projektive Ebene der Ordnung  $q$  ist.
2. \*Zeigen Sie, dass für  $q \geq 2$  jeder Blockplan mit Parametern  $(q^2, q, 1)$  eine affine Ebene der Ordnung  $q$  ist (die Definition finden Sie in Aufgabe 9.1.10).
  3. Konstruieren Sie ein Steiner–Tripel–System mit 15 Elementen.
  4. \*Sei  $m$  eine ungerade natürliche Zahl und  $n = 3m$ . Wir definieren das Mengensystem  $(X, \mathcal{M})$  wie folgt:  $X = \{(x, i) : x = 0, 1, \dots, m-1, i = 1, 2, 3\}$ , und  $\mathcal{M}$  besteht aus allen Tripeln  $\{(x, 1), (x, 2), (x, 3)\}$  sowie allen Tripeln der Form  $\{(x, i), (y, i), (z, i+1)\}$  mit  $x \neq y, x+y \equiv 2z \pmod{m}$  und  $i = 1, 2, 3$ . (Wenn  $i = 3$  ist, dann steht  $i+1$  für 1.) Beweisen Sie, dass  $(X, \mathcal{M})$  ein Steiner–Tripel–System ist.

## 13.2 Die Fisher–Ungleichung

Einer der Begründer der Designtheorie war ein Englischer Statistiker, R. A. Fisher. Obwohl man schon lange Beispiele für Designs kannte (Steiner–Tripel–Systeme schon seit fast 100 Jahren), war Fisher der erste, der eine allgemeine Definition gab und die Bedeutung von Designs im Zusammenhang mit Statistik erkannte. Er fand auch weitere notwendige Bedingungen für die Existenz von Designs.

**13.2.1 Satz (Fisher–Ungleichung).** *Sei  $(V, \mathcal{B})$  ein 2-Design vom Typ  $(v, k, \lambda)$  mit  $v > k$ . Dann ist  $|\mathcal{B}| \geq |V|$ . Folglich erfordert ein Versuchsplan für  $v$  Behandlungen mindestens  $v$  Experimente.*

Es gibt Blockpläne mit  $|\mathcal{B}| = |V|$  (z.B. die endlichen projektiven Ebenen), in diesem Sinne ist die Fisher–Ungleichung optimal. Das folgende Beispiel zeigt, was für überraschende Einsichten sie gestattet.

**Beispiel.** Aus der Fisher–Ungleichung folgt, dass es keinen Blockplan vom Typ  $(16, 6, 1)$  gibt. Denn nach der Bemerkung hinter Satz 13.1.3 müsste ein solcher Blockplan  $\frac{16 \cdot 15}{6 \cdot 5} = 8 < 16$  Blöcke enthalten. Unsere sonstigen Bedingungen sind für diese Parameter jedoch alle erfüllt: Wir haben uns schon überzeugt, dass die Anzahl der Blöcke ganzzahlig ist, auch die Zahl  $r = \frac{15}{5} = 3$  ist eine ganze Zahl. Vielleicht möchten Sie ja analog zeigen, dass die Fisher–Ungleichung auch Blockpläne der Typen  $(21, 6, 1)$  und  $(25, 10, 3)$  ausschließt, obwohl auch diese Parameter alle weiteren Bedingungen erfüllen.

Die Fisher–Ungleichung lässt sich interessanterweise mit elementarer linearer Algebra beweisen, das hat der indische Mathematiker

R. C. Bose herausgefunden. Bevor wir mit dem Beweis beginnen, führen wir die Inzidenzmatrix eines Mengensystems  $(V, \mathcal{B})$  ein; das Konzept ist dem der Inzidenzmatrix eines Graphen analog (das wir für orientierte Graphen in Abschnitt 8.5 eingeführt haben). Wir bezeichnen die Elemente der Menge  $V$  als  $x_1, x_2, \dots, x_v$  und die Mengen aus  $\mathcal{B}$  als  $B_1, B_2, \dots, B_b$ . Wir definieren eine  $v \times b$  Matrix  $A = (a_{ij})$ , deren Zeilen den Punkten in  $V$  entsprechen und deren Spalten den Mengen in  $\mathcal{B}$ , und zwar durch die Formel

$$a_{ij} = \begin{cases} 1 & \text{wenn } x_i \in B_j \\ 0 & \text{sonst.} \end{cases}$$

Die Matrix  $A$  heißt die *Inzidenzmatrix* des Mengensystems  $(V, \mathcal{B})$ .

*Beweis der Fisher–Ungleichung.* Zu einem gegebenen Blockplan  $(V, \mathcal{B})$  betrachten wir die Inzidenzmatrix  $A = (a_{ij})$ . Die zu  $A$  transponierte Matrix  $A^T$  ist eine  $b \times v$  Matrix, demnach ist das Produkt  $AA^T$  eine  $v \times v$  Matrix. Wir zeigen, dass die Matrix  $M = AA^T$  eine sehr einfache Form hat.

Betrachten wir einen Eintrag  $m_{ij}$  von  $M$ . Nach der Definition der Matrixmultiplikation ist

$$m_{ij} = \sum_{k=1}^b a_{ik} a_{jk}$$

(der Eintrag in der  $j$ -ten Spalte und  $k$ -ten Zeile der Matrix  $A^T$  ist  $a_{jk}$ ). Demnach zählt  $m_{ij}$ , wie viele Mengen  $B_k$  sowohl  $x_i$  als auch  $x_j$  enthalten. Nach der Definition eines Blockplans gibt es nur zwei mögliche Werte für  $m_{ij}$ :

$$m_{ij} = \begin{cases} \lambda & \text{für } i \neq j \\ \lambda \frac{v-1}{k-1} & \text{für } i = j. \end{cases}$$

Der Zahl  $\lambda \cdot \frac{v-1}{k-1}$  haben wir weiter oben den Namen  $r$  gegeben, und so können wir die Matrix  $M$  schreiben als

$$\begin{pmatrix} r & \lambda & \dots & \lambda \\ \lambda & r & \dots & \lambda \\ \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \dots & r \end{pmatrix}.$$

Wir möchten zeigen, dass diese Matrix nicht singulär ist, d.h. dass ihre Determinante nicht Null ist. Elementare Zeilenoperationen ergeben

$$\begin{aligned} \det M &= \det \begin{pmatrix} r + (v-1)\lambda & r + (v-1)\lambda & \dots & r + (v-1)\lambda \\ \lambda & r & \dots & \lambda \\ \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \dots & r \end{pmatrix} \\ &= \left( r + (v-1)\lambda \right) \det \begin{pmatrix} 1 & 1 & \dots & 1 \\ \lambda & r & \dots & \lambda \\ \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \dots & r \end{pmatrix} \\ &= \left( r + (v-1)\lambda \right) \det \begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & r-\lambda & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & r-\lambda \end{pmatrix} \\ &= (r + (v-1)\lambda) \cdot (r - \lambda)^{v-1}. \end{aligned}$$

Nun erinnern wir uns, dass  $r = \lambda \cdot \frac{v-1}{k-1}$  ist. Klar ist, dass  $r + (v-1)\lambda \neq 0$ , und weil  $v > k$  ist, gilt auch  $r > \lambda$ ; somit ist  $\det M \neq 0$ . Daher hat die Matrix  $M$  den Rang<sup>1</sup>  $v$ . Wäre aber  $b < v$ , dann hätten die Matrizen  $A$  und  $A^T$  beide einen Rang kleiner als  $v$ , in Konsequenz hätte auch die Matrix  $M = AA^T$  einen Rang  $< v$  (hier verwenden wir eine einfache Eigenschaft des Ranges von Matrizen; siehe Aufgabe 2). Daraus schließen wir  $b \geq v$ . Und die Fisher–Ungleichung ist bewiesen.  $\square$

Diese Anwendung der Rangfunktion war der Startschuss für viele ähnliche (und wichtige) kombinatorische Beweise. Einen weiteren Beweis für die Tatsache, dass  $r(M) = v$  ist, können Sie in Aufgabe 4 führen.

---

<sup>1</sup>Zur Erinnerung: Der *Rang* einer Matrix  $M$ , meist als  $r(M)$  geschrieben, ist die maximale Anzahl linear unabhängiger Zeilen in  $M$ . Die analoge Definition mit Spalten statt Zeilen ergibt stets die gleiche Zahl, das versichert uns ein elementarer Satz aus der linearen Algebra.

## Aufgaben

1. Beweisen Sie die Fisher–Ungleichung für  $\lambda = 1$  direkt (ohne lineare Algebra).
2. Zeigen Sie: Ist  $A$  eine  $n \times k$  Matrix und  $B$  eine  $k \times m$  Matrix, so gilt die Ungleichung  $r(AB) \leq \min(r(A), r(B))$ .
3. \*Sei  $F$  ein Körper und  $G \subseteq F$  ein Unterkörper von  $F$  (vielleicht bevorzugen Sie die konkrete Vorstellung, dass  $F$  der Körper der reellen Zahlen und  $G$  der Körper der rationalen Zahlen ist). Sei  $A$  eine Matrix mit Einträgen aus dem Körper  $G$ . Den Rang von  $A$  kann man über dem Körper  $G$  betrachten (dann sind in Linearkombinationen Koeffizienten in  $G$  erlaubt) oder über dem Körper  $F$  (Linearkombinationen haben Koeffizienten aus  $F$ ). Erklären Sie, warum beide Varianten den gleichen Rang ergeben.
4. Eine reelle quadratische  $n \times n$  Matrix  $M$  heißt *positiv definit*, wenn  $x^T M x > 0$  für jeden von Null verschiedenen (Spalten-) Vektor  $x \in \mathbb{R}^n$  gilt.
  - (a) Warum hat jede positiv definite  $n \times n$  Matrix  $M$  vollen Rang  $n$ ?
  - (b) Zeigen Sie, dass die Matrix  $M$  aus dem Beweis der Fisher–Ungleichung positiv definit ist (und also Rang  $v$  hat, was wir dann ohne Berechnung der Determinante wissen).
5. (a) Seien  $C_1, C_2, \dots, C_m$  Teilmengen einer  $n$ -Menge  $X$ . Angenommen, jedes  $C_i$  enthält ungerade viele Elemente und die Kardinalität aller Schnitte  $C_i \cap C_j$  (für  $i \neq j$ ) ist gerade. Beweisen Sie, dass dann  $m \leq n$  ist. Sehen Sie sich die Matrix  $A^T A$  an, wobei  $A$  die Inzidenzmatrix des betrachteten Mengensystems ist, aber arbeiten Sie über dem Körper mit zwei Elementen (d.h. modulo 2).
  - (b) Betrachten Sie ein ähnliches Problem wie in (a), doch diesmal fordern wir, dass die Größen der Mengen selbst *gerade* sind, während alle  $|C_i \cap C_j|$  (für  $i \neq j$ ) *ungerade* sind. Beweisen Sie, dass wiederum  $m \leq n$  ist.
  - (c) \*Diesmal fordern wir, dass die Mengen  $C_i$  alle verschieden sind und dass ihre Größen und die Größen aller paarweisen Schnitte *gerade* sind. Zeigen Sie, dass man ein solches System mit  $2^{\lfloor n/2 \rfloor}$  Mengen konstruieren kann.
6. (Verallgemeinerte Fisher–Ungleichung) Sei  $X$  eine  $n$ -Menge und  $q$  eine ganze Zahl,  $1 \leq q < n$ . Seien  $C_1, C_2, \dots, C_m$  Teilmengen von  $X$ , so dass alle paarweisen Schnittmengen  $C_i \cap C_j$  (für  $i \neq j$ ) Kardinalität genau  $q$  haben.
  - (a) \*Beweisen Sie mit der Methode aus Aufgabe 4, dass  $m \leq n$  ist. (Behandeln Sie den Fall, dass  $|C_i| = q$  für irgendein  $i$  gilt, getrennt.)

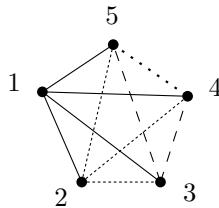
(b) \*Was berechtigt uns dazu, die Behauptung in (a) als „verallgemeinerte Fisher–Ungleichung“ zu bezeichnen? Folgern Sie die Fisher–Ungleichung aus (a)!

### 13.3 Überdeckungen mit bipartiten Graphen

Die folgende Frage ist durch ein Problem aus der Telekommunikation motiviert:

**Problem.** Die Kantenmenge eines vollständigen Graphen  $K_n$  soll als disjunkte Vereinigung der Kantenmengen von  $m$  vollständigen bipartiten Graphen ausgedrückt werden. Was ist der kleinste Wert  $m = m(n)$ , für den das möglich ist?

Eine der Möglichkeiten,  $E(K_n)$  als disjunkte Vereinigung der Kantenmengen von  $n - 1$  vollständigen bipartiten Graphen auszudrücken, ist „Sterne“  $K_{1,n_i}$  zu verwenden. Hier ist solch eine disjunkte Überdeckung für  $n = 5$ :



Zur Konstruktion dieser Art disjunkter Überdeckungen für beliebiges  $n$  gehen wir induktiv vor: Angenommen, wir können  $E(K_{n-1})$  schon mit  $n - 2$  Sternen überdecken. In dem Graphen  $K_n$  werden wir dann eine Ecke  $v$  wählen und alle anstoßenden Kanten mit dem Stern  $K_{1,n-1}$  mit Zentrum  $v$  überdecken; was übrig bleibt, ist ein Graph isomorph zu  $K_{n-1}$ , dessen Kantenmenge wir schon mit  $n - 2$  Sternen überdecken können.

Es ist keineswegs offensichtlich, dass es nicht besser (d.h. mit weniger vollständigen bipartiten Graphen) geht, etwa wenn man vollständige bipartite Graphen verwendet, deren Farbklassen beide groß sind. Doch Graham und Pollak haben mit einer genialen Idee gezeigt, dass es keine bessere disjunkte Überdeckung gibt:

**13.3.1 Satz (Graham–Pollak).** *Es ist  $m(n) \geq n - 1$ .*

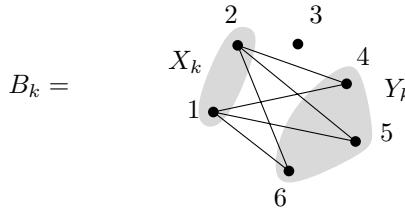
*Beweis.* Nehmen wir an, die vollständigen bipartiten Graphen  $B_1, B_2, \dots, B_m$  bilden eine disjunkte Überdeckung aller Kanten von

$K_n$ , d.h. für alle  $k$  ist  $V(B_k) \subseteq V(K_n) = \{1, 2, \dots, n\}$  und  $E(K_n) = E(B_1) \dot{\cup} E(B_2) \dot{\cup} \dots \dot{\cup} E(B_m)$ . Seien  $X_k$  und  $Y_k$  die Farbklassen von  $B_k$ ; das bedeutet, dass in  $B_k$  alle Kanten zwischen  $X_k$  und  $Y_k$  verlaufen.

Zu jedem Graphen  $B_k$  definieren wir eine  $n \times n$  Matrix  $A_k$ , deren Eintrag in der  $i$ -ten Zeile und  $j$ -ten Spalte

$$a_{ij}^{(k)} = \begin{cases} 1 & \text{wenn } i \in X_k \text{ und } j \in Y_k \\ 0 & \text{sonst} \end{cases}$$

ist. Die Definition von  $A_k$  erinnert an die Adjazenzmatrix des Graphen  $B_k$ , abgesehen davon, dass  $A_k$  nicht symmetrisch ist — jede Kante des Graphen  $B_k$  steuert nur eine 1 bei. Z.B. ist für den Teilgraphen



die Matrix  $A_k$

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Wir behaupten, dass jede der Matrizen  $A_k$  den Rang 1 hat. Das ist so, weil in allen Zeilen von  $A_k$ , die nicht nur Nullen enthalten, der gleiche Vektor steht, nämlich der Vektor, der an den zu  $Y_k$  gehörenden Stellen eine 1 und an allen anderen Stellen eine 0 hat.

Betrachten wir nun die Matrix  $A = A_1 + A_2 + \dots + A_m$ . Jede Kante  $\{i, j\}$  gehört zu genau einem der Graphen  $B_k$ , und deshalb gilt für jedes  $i \neq j$  entweder  $a_{ij} = 1$  und  $a_{ji} = 0$ , oder  $a_{ij} = 0$  und  $a_{ji} = 1$ , wobei  $a_{ij}$  für den Eintrag der Matrix  $A$  an der Stelle  $(i, j)$  steht. Außerdem gilt  $a_{ii} = 0$ . Daraus erhalten wir  $A + A^T = J_n - I_n$ , wobei  $J_n$  die  $n \times n$  Matrix ist, die überall Einsen hat, und  $I_n$  ist die  $n \times n$  Einheitsmatrix mit Einsen auf der Diagonalen und sonst überall Nullen. Wir möchten zeigen, dass der Rang einer solchen Matrix  $A$  mindestens  $n - 1$  ist. Sobald wir das wissen, haben wir  $n - 1 \leq$

$r(A) \leq r(A_1) + \cdots + r(A_m) = m$ , weil für zwei beliebige Matrizen  $M_1$  und  $M_2$  (mit gleicher Größe)  $r(M_1 + M_2) \leq r(M_1) + r(M_2)$  ist; das macht man sich leicht mit der Definition für den Rang einer Matrix klar (Aufgabe 1).

Wir führen die Annahme, dass  $r(A) \leq n - 2$  ist, zum Widerspruch. Fügen wir zu der Matrix  $A$  eine zusätzliche Zeile mit lauter Einsen hinzu, hat die resultierende  $(n + 1) \times n$  Matrix immer noch Rang  $\leq n - 1$ , deshalb lässt sich der Nullvektor als nicht triviale Linearkombination ihrer Spalten ausdrücken. Anders gesagt existiert ein (Spalten-)Vektor  $x \in \mathbb{R}^n$ ,  $x \neq (0, 0, \dots, 0)^T$ , so dass  $Ax = 0$  ist und außerdem  $\sum_{i=1}^n x_i = 0$ .

Aus der letztgenannten Gleichung folgt  $J_n x = 0$ . Wir rechnen:

$$\begin{aligned} x^T (A + A^T)x &= x^T (J_n - I_n)x = x^T (J_n x) - x^T (I_n x) \\ &= 0 - x^T x = - \sum_{i=1}^n x_i^2 < 0. \end{aligned}$$

Andererseits ist aber

$$x^T (A^T + A)x = (x^T A^T)x + x^T (Ax) = 0 \cdot x + x \cdot 0 = 0,$$

ein Widerspruch. Also muss  $r(A) = n - 1$  sein, und Satz 13.3.1 ist bewiesen.  $\square$

## Aufgaben

- Seien  $M_1$  und  $M_2$  zwei  $n \times m$  Matrizen. Zeigen Sie, dass  $r(M_1 + M_2) \leq r(M_1) + r(M_2)$  ist, und finden Sie Beispiele, in denen Gleichheit gilt, sowie Beispiele, in denen die Gleichheit nicht gilt.
- (a) Die Kanten des  $K_n$  sollen mit den Kantenmengen vollständiger bipartiter Teilgraphen überdeckt werden, doch wir bestehen nicht darauf, dass ihre Kantenmengen disjunkt sind (d.h. eine Kante darf mehrfach überdeckt sein). Zeigen Sie, dass es eine Überdeckung mit  $\lceil \log_2 n \rceil$  bipartiten Graphen gibt.  
(b) \*Beweisen Sie, dass eine Überdeckung wie in (a) tatsächlich mindestens  $\lceil \log_2 n \rceil$  bipartite Graphen erfordert.
- \*Diesmal sollen Sie die Kanten des  $K_n$  so mit vollständigen bipartiten Teilgraphen überdecken, dass jede Kante *ungerade oft* überdeckt ist. Beweisen Sie, dass Sie dazu mindestens  $\frac{1}{2}(n-1)$  vollständige bipartite Teilgraphen benötigen. Gehen Sie dabei so ähnlich vor, wie bei dem Beweis im Text, aber arbeiten Sie mit Matrizen über dem Körper mit zwei Elementen. Betrachten Sie an Stelle der Matrix  $A_k$  die Adjazenzmatrix des Graphen  $B_k$ , deren Rang ist 2.

## 13.4 Der Zyklenraum eines Graphen

Sei  $G = (V, E)$  ein ungerichteter Graph. Das Symbol  $\mathcal{K}_G$  bezeichne die Menge aller Kreise im Graphen  $G$  (genauer die Menge aller Teilgraphen, die Kreise sind). Es ist klar, dass dieser Menge so ein besonderer geschwungener Buchstabe zusteht, denn sie ist in der Regel recht groß. Für den vollständigen Graphen  $K_n$  haben wir z.B.

$$|\mathcal{K}_{K_n}| = \sum_{k=3}^n \binom{n}{k} \cdot \frac{(k-1)!}{2}, \quad (13.2)$$

und für den vollständigen bipartiten Graphen  $K_{n,n}$  erhalten wir

$$|\mathcal{K}_{K_{n,n}}| = \sum_{k=2}^n \binom{n}{k}^2 \cdot \frac{k!(k-1)!}{2}. \quad (13.3)$$

Allerdings kann auch  $\mathcal{K}_G = \emptyset$  sein; das ist genau dann der Fall, wenn  $G$  ein Wald ist (eine disjunkte Vereinigung von Bäumen).

Es hat vielleicht den Anschein, dass die Menge  $\mathcal{K}_G$  keine nennenswerte Struktur besitzt. In diesem Abschnitt führen wir eine Verallgemeinerung des Begriffs „Kreis“ ein (sie hat etwas mit dem Stoff aus Abschnitt 4.4 über Eulersche Graphen zu tun), welche die Menge aller Kreise zu einer größeren Menge mit sehr einfacher Struktur ergänzt, zu einem Vektorraum nämlich. Die nun folgenden Ideen kommen ursprünglich aus der Untersuchung elektrischer Schaltkreise.

**13.4.1 Definition (Gerade Kantenmenge).** Sei  $G = (V, E)$  ein (ungerichteter) Graph. Eine Menge  $E' \subseteq E$  heißt gerade, wenn in dem Graphen  $(V, E')$  alle Eckengrade gerade sind.

Beispielsweise sind die leere Menge und die Kantenmenge eines beliebigen Kreises gerade Mengen.

Im Folgenden wird es praktisch sein, Teilgraphen mit ihren Kantenmengen zu identifizieren.

**13.4.2 Lemma.** Eine Kantenmenge  $E'$  ist genau dann gerade, wenn es paarweise disjunkte Kreise  $E_1, E_2, \dots, E_t$  gibt, so dass  $E' = E_1 \dot{\cup} E_2 \dot{\cup} \dots \dot{\cup} E_t$ .

*Beweis.* Ist  $E'$  eine nicht leere gerade Menge, dann ist der Graph  $(V, E')$  kein Wald und enthält einen Kreis  $E_1$ . Die Menge  $E' \setminus E_1$  ist wieder gerade, so dass wir Induktion über die Anzahl der Kanten in  $E'$  führen können.  $\square$

Wir beschreiben nun die Struktur der Familie aller geraden Kantenmengen in einem gegebenen Graphen  $G = (V, E)$  algebraisch. Die

Kanten von  $G$  nennen wir  $e_1, e_2, \dots, e_m$ , und jeder Menge  $A \subseteq E$  ordnen wir ihren *charakteristischen Vektor*  $\mathbf{v}_A = (v_1, v_2, \dots, v_m)$  zu, definiert durch

$$v_i = \begin{cases} 1 & \text{wenn } e_i \in A \\ 0 & \text{sonst.} \end{cases}$$

Die Vektoren werden modulo 2 addiert und multipliziert (das bedeutet  $1 + 1 = 0$ ). Seien  $A, B \subseteq E$  gerade Mengen. Dann ist

$$\mathbf{v}_A + \mathbf{v}_B = \mathbf{v}_C,$$

wobei  $C = (A \cup B) \setminus (A \cap B)$  die *symmetrische Differenz* der Mengen  $A$  und  $B$  ist. Obwohl elementar ist das ein wesentlicher Punkt für das Verständnis des folgenden Stoffs.

Das Symbol  $\mathcal{Z}$  bezeichne die Menge der charakteristischen Vektoren aller geraden Kantenmengen in  $G$ . Man nennt diese Menge den *Zyklenraum* des Graphen  $G$ . Um die Formulierungen einfach zu halten verallgemeinern wir den Begriff des aufspannenden Baums aus Abschnitt 5.3: unter einem *aufspannenden Wald* eines beliebigen Graphen  $G$ , der auch unzusammenhängend sein darf, verstehen wir einen Teilgraphen  $(V(G), \bar{E})$  von  $G$ , der keine Kreise hat und der maximal ist mit dieser Eigenschaft (d.h. das Hinzufügen egal welcher weiteren Kante aus  $G$  erzeugt einen Kreis). Für zusammenhängende Graphen  $G$  sind die aufspannenden Wälder genau die aufspannenden Bäume; für einen nicht zusammenhängenden Graphen besteht ein aufspannender Wald aus aufspannenden Bäumen aller Komponenten.

### 13.4.3 Satz (Zyklenraum–Theorem).

- (1) Für jeden Graphen  $G$  ist die Menge  $\mathcal{Z}$  ein Vektorraum über dem Körper  $GF(2)$  mit 2 Elementen. Die Dimension dieses Vektorraums ist  $|E| - |V| + k$ , wobei  $k$  die Anzahl der Komponenten des Graphen  $G$  ist.
- (2) Wir wählen einen beliebigen aufspannenden Wald  $T = (V, E')$  des Graphen  $G$  und konstruieren zu jeder Kante  $e \in E \setminus E'$  den Kreis  $C_e$  als den (eindeutigen) Kreis, der in dem Graphen  $(V, E' \cup \{e\})$  enthalten ist. Dann bilden die charakteristischen Vektoren der Kreise  $C_e$ ,  $e \in E \setminus E'$ , eine Basis von  $\mathcal{Z}$ .

In diesem Satz steht das Symbol  $GF(2)$  für den 2-elementigen Körper, der aus den Zahlen 0 und 1 besteht und in dem die arithmetischen Operationen modulo 2 ausgeführt werden. Die Buchstaben

$GF$  stehen für „Galois–Feld“, einem traditionellen Namen für endliche Körper; der englische Ausdruck für „Körper“ ist „field“. Die Behauptung,  $\mathcal{Z}$  sei ein Vektorraum über  $GF(2)$ , bedeutet einfach, dass die modulo-2–Summe zweier charakteristischer Vektoren von geraden Mengen wieder ein charakteristischer Vektor einer geraden Menge ist.

Der Kreis  $C_e$  heißt ein *Elementarkreis* (zur Kante  $e$ , bezüglich eines gegebenen aufspannenden Waldes).

*Beweis.* Als erstes zeigen wir, dass  $\mathcal{Z}$  ein Vektorraum ist. Zu diesem Zweck müssen wir nachweisen, dass die Summe zweier Vektoren aus  $\mathcal{Z}$  wieder einen Vektor aus  $\mathcal{Z}$  ergibt, und dass ebenso das Produkt eines Vektors aus  $\mathcal{Z}$  mit einer Zahl aus dem Körper  $GF(2)$  einen Vektor aus  $\mathcal{Z}$  ergibt. Das zweite ist völlig klar, denn wir können ja nur entweder mit 0 multiplizieren ( $0\mathbf{v}_A = \mathbf{v}_\emptyset$ ) oder mit 1 ( $1\mathbf{v}_A = \mathbf{v}_A$ ). Entsprechend der Bemerkung vor dem Satz entspricht das Addieren zweier Vektoren der symmetrischen Differenz der zugehörigen Mengen, deshalb genügt es zu zeigen, dass die symmetrische Differenz zweier gerader Mengen  $A$  und  $B$  wieder eine gerade Menge ist. Wir wählen im Graphen  $G$  eine beliebige Ecke  $v \in V$ . Die Anzahl der zu  $v$  inzidenten Kanten, die zur Menge  $A$  gehören, bezeichnen wir mit  $d_A$ , die zur Menge  $B$  gehören mit  $d_B$  und die sowohl zu  $A$  als auch zu  $B$  gehören mit  $d$ . Die Zahlen  $d_A$  und  $d_B$  sind beide gerade. Die Anzahl der zu  $v$  inzidenten Kanten, die zur symmetrischen Differenz  $(A \cup B) \setminus (A \cap B)$  gehören, ist  $d_A + d_B - 2d$ , deshalb ist der Grad von  $v$  in der symmetrischen Differenz gerade. Die symmetrische Differenz ist also eine gerade Menge, und folglich ist  $\mathcal{Z}$  ein Vektorraum über  $GF(2)$ .

Sei  $(V, E')$  ein aufspannender Wald des Graphen  $G$ . Dann ist  $|E'| = |V| - k$ , wobei  $k$  die Anzahl der Komponenten des Graphen  $G$  ist. Es genügt zu zeigen, dass die charakteristischen Vektoren aller Elementarkreise eine Basis für den Vektorraum  $\mathcal{Z}$  bilden.

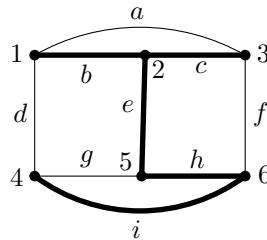
Dazu zeigen wir erst einmal, dass die Elementarkreise linear unabhängig sind. Betrachten wir eine Kante  $e_i \notin E'$ . Der charakteristische Vektor des Elementarkreises  $C_{e_i}$  ist unter den charakteristischen Vektoren aller Elementarkreise der einzige mit einer 1 an der Position  $i$ . Deshalb kann ein charakteristischer Vektor eines Elementarkreises niemals eine Linearkombination anderer solcher Vektoren sein.

Nun wollen wir zeigen, dass die Elementarkreise  $\mathcal{Z}$  erzeugen. Wir wählen eine gerade Menge  $A$  und definieren eine Menge  $B$ , indem wir ihren charakteristischen Vektor angeben:

$$\mathbf{v}_B = \sum_{e \in A \setminus E'} \mathbf{v}_{C_e}.$$

Welche Kanten enthält  $B$ ? Das sind genau die Kanten, die zu ungeraden vielen Elementarkreisen gehören (bezüglich des aufspannenden Waldes  $(V, E')$ ). Auf jeden Fall enthält  $B$  die Menge  $A \setminus E'$ , weil jede ihrer Kanten in einem eindeutigen Elementarkreis liegt. Nun sei  $C$  die symmetrische Differenz der Mengen  $A$  und  $B$ . Das ist eine gerade Menge, und zugleich muss sie in  $E'$  enthalten sein. Weil  $E'$  keine Zyklen hat, muss  $C = \emptyset$  sein, und das bedeutet, dass  $A = B$  ist. Wir haben also die Menge  $A$  als Linearkombination von Elementarkreisen ausgedrückt.  $\square$

**Beispiel.** Betrachten wir den folgenden Graphen  $G = (V, E)$ :



Die Dimension seines Zyklenraums ist  $9 - 6 + 1 = 4$ . Wenn wir den mit dicken Linien eingezeichneten aufspannenden Baum wählen, besteht die zugehörige Basis des Zyklenraums aus den charakteristischen Vektoren der folgenden Elementarkreise:

$$\begin{aligned} C_a &= \{a, b, c\} \\ C_d &= \{b, e, h, i, d\} \\ C_g &= \{g, h, i\} \\ C_f &= \{c, f, h, e\}. \end{aligned}$$

Für den Kreis  $C = \{a, f, i, d\}$  finden wir beispielsweise den Ausdruck  $\mathbf{v}_C = \mathbf{v}_{C_a} + \mathbf{v}_{C_d} + \mathbf{v}_{C_f}$ .

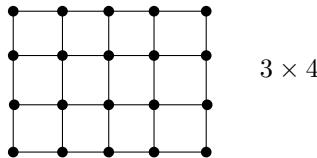
Es folgt eine einfache Konsequenz aus Theorem 13.4.3:

**13.4.4 Folgerung.** Die Anzahl der geraden Mengen in einem Graphen  $G = (V, E)$  mit  $k$  Komponenten ist  $2^{|E|-|V|+k}$ .

Trotz der großen Zahl gerader Mengen ist ihre Struktur einfach, man kann sie alle auf einfache Art aus einer sehr viel kleineren Basis erzeugen. Die Dimension des Zyklenraums, d.h. die Zahl  $|E| - |V| + k$ , heißt die *zyklomatische Zahl* des Graphen  $G = (V, E)$ . (Auch der ältere Name *Betti-Zahl*, der mit einer topologischen Sichtweise zusammenhängt, ist gebräuchlich.)

## Aufgaben

1. Vergewissern Sie sich, dass die Formeln (13.2) und (13.3) stimmen.
2. Beweisen Sie Folgerung 13.4.4.
3. Bestimmen Sie die zyklomatische Zahl eines  $m \times n$  Gittergraphen wie

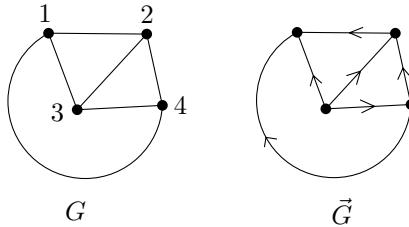


4. Beweisen Sie, dass in jedem topologischen planaren 2-zusammenhängenden Graphen (d.h. ein planarer 2-zusammenhängender Graph mit festgelegter ebener Zeichnung) die Randkreise der inneren Länder eine Basis des Zyklenraums  $\mathcal{Z}$  bilden.

## 13.5 Ströme und Schnitte

In diesem Abschnitt betrachten wir den Stoff aus dem vorangegangenen Abschnitt nochmals aus einem anderen Blickwinkel. Zur Beschreibung werden wir Matrizen verwenden und sowohl auf ungerichtete Graphen als auch ihre Orientierungen Bezug nehmen. In dieser komplizierteren Situation formulieren wir ein Zyklenraum-Theorem analog zu 13.4.3 und lernen neue Zusammenhänge zu sehen.

**Ströme.** Zur Erinnerung wiederholen wir den Begriff der Orientierung aus Abschnitt 8.5. Eine *Orientierung* eines Graphen  $G = (V, E)$  ist ein gerichteter Graph  $\vec{G} = (V, \vec{E})$ , bei dem die Menge  $\vec{E}$  zu jeder Kante  $\{x, y\} \in E$  genau eine der gerichteten Kanten  $(x, y)$  und  $(y, x)$  enthält. Das folgende Bild zeigt einen Graphen und eine seiner möglichen Orientierungen:



(Die Anzahl aller möglichen Orientierungen eines Graphen  $G$  — von denen viele isomorph sein können — ist  $2^{|E|}$ .)

Wir beginnen damit, eine Orientierung  $\vec{G} = (V, \vec{E})$  ein für alle Mal festzulegen. Eine reelle Funktion  $f: \vec{E} \rightarrow \mathbb{R}$  heißt *Strom* (manchmal auch *Fluss*), wenn für jede Ecke  $v$  im Graphen  $G$  gilt:

$$\sum_{x \in V: (v, x) \in \vec{E}} f(v, x) = \sum_{x \in V: (x, v) \in \vec{E}} f(x, v). \quad (13.4)$$

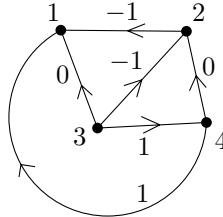
(Ein Strom darf auch negative Werte auf Kanten annehmen.) Die Menge der ungerichteten Kanten  $e$  mit  $f(\vec{e}) \neq 0$ , wobei  $\vec{e}$  die gewählte Orientierung von  $e$  ist, heißt der *Träger* von  $f$ . Man sieht leicht, dass der Träger jedes nicht trivialen Stroms einen Kreis enthält (hier ist es wichtig, mit einer Orientierung eines ungerichteten Graphen zu arbeiten und nicht etwa mit einem gerichteten Graphen, damit die Kanten  $(x, y)$  und  $(y, x)$  nie zugleich auftreten).

Der Begriff des Stroms hat mehrere intuitive Deutungen. Repräsentiert  $\vec{G}$  zum Beispiel einen elektrischen Schaltkreis und ist  $f(e)$  der derzeitige Stromfluss durch eine Kante  $e$ , dann sagt uns Gleichung (13.4), dass an jeder Ecke genauso viel elektrische Ladung hinein- wie hinausfließt. Dies ist das erste Kirchhoff'sche Gesetz. Diese „elektrische“ Interpretation war eine der ursprünglichen Motivationen, die in diesem Abschnitt besprochene Theorie zu entwickeln.

Ein Beispiel für einen Strom erhält man folgendermaßen. Sei  $C = (v_1, v_2, \dots, v_{k+1} = v_1)$  die Folge der Ecken eines (ungerichteten) Kreises im Graphen  $G$ . Wir definieren einen Strom  $f$  in der Orientierung  $\vec{G}$ , indem wir Folgendes festlegen:

$$\begin{aligned} f(v_i, v_{i+1}) &= 1 && \text{wenn } (v_i, v_{i+1}) \in \vec{E} \\ f(v_{i+1}, v_i) &= -1 && \text{wenn } (v_{i+1}, v_i) \in \vec{E} \\ f(x, y) &= 0 && \text{wenn } \{x, y\} \text{ keine Kante von } C \text{ ist.} \end{aligned}$$

Wir sagen, dieser Strom *gehört* zum Kreis  $C$ . (Beachten Sie, dass er vom Umlaufsinn abhängt, in dem die Kanten des ungerichteten Kreises  $C$  aufgelistet sind.) Für den Graphen im Bild oben und für den Kreis mit den Ecken 1, 2, 3, 4 (in dieser Reihenfolge), sieht der Strom so aus:



Man sieht leicht, dass die Summe  $f_1 + f_2$  zweier Ströme  $f_1$  und  $f_2$  wieder ein Strom auf  $\vec{G}$  ist. Für jede reelle Zahl  $c$  ist auch die Funktion  $cf_1$  ein Strom. (In beiden Fällen genügt es, Bedingung (13.4) zu testen.) Die Menge aller Ströme hat also Vektorraumstruktur. Diesmal haben wir einen Vektorraum über den reellen Zahlen. Wir wollen diesen Vektorraum mit  $\mathcal{S}$  bezeichnen und ihn den *Stromraum* von  $G$  nennen.

Man kann zeigen, dass der Stromraum  $\mathcal{S}$  für jeden Graphen  $G$  von solchen Strömen erzeugt wird, die zu Kreisen in  $G$  gehören (siehe Aufgabe 1). Bald werden wir noch genaueres über die Struktur von  $\mathcal{S}$  erfahren.

**Potenzziale und Schnitte.** Sei  $p: V \rightarrow \mathbb{R}$  eine beliebige Funktion ( $p$  für Potential). Wir definieren eine Funktion  $\delta p$  auf der Menge der gerichteten Kanten von  $\vec{G}$  mit der Formel

$$\delta p(x, y) = p(x) - p(y) \quad (13.5)$$

für jede gerichtete Kante  $(x, y) \in \vec{E}$ .

Die Funktion  $\delta p: \vec{E} \rightarrow \mathbb{R}$  heißt eine *Potenzzaldifferenz* oder *Spannung* (wenn Sie noch eine dunkle Ahnung von Physik haben, sehen Sie wahrscheinlich den Zusammenhang zu elektrischen Schaltkreisen). Jede Funktion  $g: \vec{E} \rightarrow \mathbb{R}$ , zu der es ein Potenzial  $p$  gibt, so dass  $g = \delta p$  ist, heißt auch *Potenzzaldifferenz*.

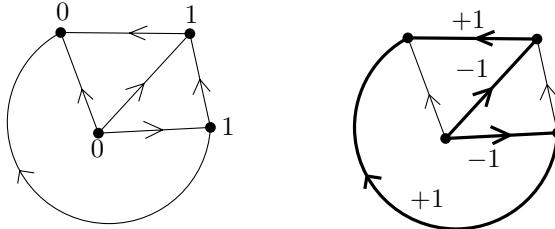
Man macht sich leicht klar, dass die Summe zweier Potenzialdifferenzen wieder eine Potenzialdifferenz ist, ebenso das Produkt einer Potenzialdifferenz mit einer reellen Zahl. Den Vektorraum aller Potenzialdifferenzen bezeichnen wir mit  $\mathcal{R}$  und nennen ihn den *Schnittraum*.

Wieso „Schnittraum“? Betrachten wir einmal folgende Situation: Ein Potenzial  $p$  nehme nur die beiden Werte 0 und 1 an. Wir setzen  $A = \{v \in V: p(v) = 1\}$ ,  $B = V \setminus A$ . Dann ist die Potenzialdifferenz  $g = \delta p$  nur auf den gerichteten Kanten mit einem Ende in  $A$  und dem anderen in  $B$  von Null verschieden:

$$\begin{aligned} g(x, y) &= 1 && \text{für } x \in A, y \in B \\ g(x, y) &= -1 && \text{für } x \in B, y \in A \\ g(x, y) &= 0 && \text{sonst.} \end{aligned}$$

Es ist nahe liegend die Menge aller zwischen  $A$  und  $B$  verlaufenden Kanten einen *Schnitt* zu nennen, weil die Anzahl der Komponenten

bei Entfernung dieser Kanten um 1 erhöht wird (wenn es überhaupt eine Kante zwischen  $A$  und  $B$  gibt). Im folgenden Bild haben wir ein Potenzial  $p$  und seine Potenzialdifferenz eingetragen. Die Kanten des zugehörigen Schnitts sind fett gezeichnet.



Diese ganze Situation beschreiben wir nun mit Hilfe der Inzidenzmatrix. Zu diesem Zweck nummerieren wir die Ecken,  $V = \{v_1, \dots, v_n\}$ , und die Kanten,  $E = \{e_1, \dots, e_m\}$ . Das Symbol  $\vec{e}_i$  bezeichnet die gerichtete Kante in der Orientierung  $\vec{G}$ , die zur Kante  $e_i$  gehört. Wir rufen uns aus Abschnitt 8.5 die *Inzidenzmatrix* der Orientierung  $\vec{G}$  ins Gedächtnis. Diese Matrix  $D$  hat die Maße  $n \times m$ , der Eintrag  $d_{ik}$  ist durch folgende Regel gegeben:

$$d_{ik} = \begin{cases} -1 & \text{wenn } \vec{e}_k \text{ bei } v_i \text{ beginnt} \\ 1 & \text{wenn } \vec{e}_k \text{ bei } v_i \text{ endet} \\ 0 & \text{sonst.} \end{cases}$$

Man kann den Stromraum und den Schnittraum elegant beschreiben:

**13.5.1 Satz.** Der Schnittraum  $\mathcal{R}$  eines jeden Graphen  $G$  wird von den Zeilen der Inzidenzmatrix  $D$  erzeugt. Der Stromraum  $\mathcal{S}$  ist das orthogonale Komplement des Schnittraums  $\mathcal{R}$ , d.h.  $\mathcal{S} = \{x \in \mathbb{R}^m : x^T y = 0 \text{ für alle } y \in \mathcal{R}\}$ .

*Beweis.* Sei  $D = (d_{ij})$  die  $n \times m$  Inzidenzmatrix. Man sieht leicht, dass jede Zeile eine Potenzialdifferenz ist (das zugehörige Potenzial hat eine 1 an der zur Zeile gehörenden Ecke und 0 überall sonst). Betrachten wir nun eine beliebige Potenzialdifferenz  $g = \delta p$ . Für eine gerichtete Kante  $\vec{e}_j = (v_r, v_s)$  gilt  $g(\vec{e}_j) = p(v_r) - p(v_s) = \sum_{i=1}^n d_{ij} p(v_i)$ ; das folgt aus einem Vergleich der Definition der Inzidenzmatrix mit Gleichung (13.5). Wenn wir also die Funktion  $g$  als einen Zeilenvektor auffassen, ist sie eine Linearkombination der Zeilen der Inzidenzmatrix. Demnach erzeugen die Zeilen den Schnittraum  $\mathcal{R}$ .

Wir schreiben nun Bedingung (13.4) an einen Strom  $f$  mittels der Inzidenzmatrix um. Aus der Gleichheit

$$\sum_{x \in V: (x, v) \in \vec{E}} f(x, v) = \sum_{x \in V: (v, x) \in \vec{E}} f(v, x)$$

erhalten wir

$$\sum_{(x,v) \in \vec{E}} f(x,v) - \sum_{(v,x) \in \vec{E}} f(v,x) = 0.$$

Für  $v = v_i$  kann man das auch so schreiben:

$$\sum_{j=1}^m f(\vec{e}_j) d_{ij} = 0.$$

Das Skalarprodukt der Funktion  $f$ , aufgefasst als ein  $m$ -Vektor, mit der  $i$ -ten Zeile der Matrix  $D$  ist also 0. Das bedeutet, dass  $f$  zu jeder Zeile von  $D$  orthogonal ist; wir sehen sogar, dass  $f$  genau dann zu allen Zeilen von  $D$  orthogonal ist, wenn  $f$  ein Strom ist. Somit sind die Vektorräume  $\mathcal{S}$  und  $\mathcal{R}$  (aufgefasst als Unterräume des Vektorraums  $\mathbb{R}^m$ ) orthogonale Komplemente voneinander.  $\square$

Was ist die Dimension des Schnittraums  $\mathcal{R}$ ? Nach obigem Satz ist sie die Dimension des von den Zeilen der Inzidenzmatrix  $D$  erzeugten Vektorraums. Ein einfaches Resultat aus der linearen Algebra, das wir schon mehrfach angewendet haben, sagt uns, dass das gleich der Dimension des von den Spaltenvektoren von  $D$  erzeugten Vektorraums ist, und diese werden wir nun bestimmen.

Für die  $j$ -te Spalte von  $D$  schreiben wir  $d_j$  (das entspricht der gerichteten Kante  $\vec{e}_j$ ).

Wir betrachten eine Menge  $J \subseteq \{1, 2, \dots, m\}$  von Spaltenindizes und fragen uns, wann die Menge der Spalten  $\{d_j : j \in J\}$  linear abhängig ist. Lineare Abhängigkeit bedeutet, dass es Zahlen  $c_j$ ,  $j \in J$ , gibt, die nicht alle Null sind und für die  $\sum_{j \in J} c_j d_j$  der Nullvektor ist. Nun haben wir ein lineares Gleichungssystem, wir schreiben die einzelnen Gleichungen separat auf. Die  $i$ -te Gleichung, die zur Ecke  $v_i$  gehört, lautet

$$\sum_{j \in J} c_j d_{ij} = 0.$$

Wenn wir  $c_t = 0$  für  $t \notin J$  setzen, erhalten wir die Bedingung (13.4) aus der Definition eines Stroms, somit ist  $c = (c_1, c_2, \dots, c_m)$  ein von Null verschiedener Strom. Also enthält der Träger von  $c$  einen Kreis (siehe Aufgabe 2).

Außerdem wissen wir schon, dass es zu jedem Kreis  $C$  einen von Null verschiedenen Strom mit Träger  $C$  gibt. Insgesamt erhalten wir, dass die Spaltenmenge  $\{d_j : j \in J\}$  genau dann linear unabhängig ist, wenn die Kantenmenge  $\{e_j : j \in J\}$  keinen Kreis enthält. Also ist der Rang der Matrix  $D$  gleich  $n - k$ , wobei  $k$  die Komponentenzahl des Graphen  $G$  ist. Wir haben bewiesen:

**13.5.2 Satz.** Der Schnittraum  $\mathcal{R}$  eines Graphen  $G$  mit  $n$  Ecken,  $m$  Kanten und  $k$  Komponenten hat Dimension  $n - k$  und der Stromraum  $\mathcal{S}$  hat Dimension  $m - n + k$ .

Dieses Ergebnis kann man als eine raffiniertere Version von Satz 13.4.3 (über den reellen Zahlen) auffassen.

Die Beziehung zwischen geraden Kantenmengen und Schnitten oder zwischen Strömen und Potenzialdifferenzen ist eine Dualität. Die oben angestellten Betrachtungen lassen sich auf weiter gehende kombinatorische Objekte als Graphen ausdehnen. Das tut man in der so genannten *Matroidtheorie* (siehe z.B. Oxley [28]).

## Aufgaben

1. Definieren Sie einen „Elementarstrom bezüglich eines gegebenen aufspannenden Waldes“. Zeigen Sie, dass der Stromraum von solchen Elementarströmen erzeugt wird.
2. (a) Sei  $f: \vec{E} \rightarrow \mathbb{R}$  ein von Null verschiedener Strom einer Orientierung  $\vec{G}$  eines ungerichteten Graphen  $G$ . Beweisen Sie, dass der Träger von  $f$  einen Kreis enthält.  
 (b) Wahr oder falsch? Der Träger eines jeden Stroms ist eine gerade Menge.

## 13.6 Probabilistisches Testen

**Matrixmultiplikation testen.** Zwei quadratische Matrizen zu multiplizieren ist für viele Anwendungen eine sehr wichtige Operation. Ein Algorithmus zur Multiplikation zweier  $n \times n$  Matrizen, der die Definition eins zu eins umsetzt, benötigt ungefähr  $n^3$  arithmetische Operationen. Doch überraschenderweise hat man geschickte Algorithmen erfunden, die ein solches Produkt asymptotisch schneller berechnen können. Derartige Algorithmen finden Sie zum Beispiel in Aho, Hopcroft und Ullman [12]. Der aktuelle Rekord ist ein Algorithmus, der nur  $O(n^{2,376})$  Operationen benötigt. Weil jedoch die in der  $O()$  Notation versteckte Konstante riesig groß ist, ist dieser Algorithmus nur von theoretischem Interesse.

Doch was heute noch graue Theorie ist, mag schon morgen kommerziell genutzt werden, und so könnte man sich vorstellen, dass eine Software-Firma ein Programm Namens MATRIX WIZARD verkauft, das laut Angaben der Firma quadratische Matrizen mit unglaublicher Geschwindigkeit multiplizieren kann. Weil Ihre Anwendung der Matrixmultiplikation jedoch kritisch ist und ein falsches Ergebnis schwer wiegende Folgen haben könnte, würden Sie gerne sicherstellen, dass MATRIX WIZARD Matrizen nicht nur schnell

multipliziert, sondern auch korrekt. Sie können es mit vielen Beispielen testen, doch egal wie viele Tests das Programm besteht, heißt das nicht unbedingt, dass es *immer* richtig rechnet. Wirklich zufrieden wären Sie, wenn Ihnen ein einfaches *Testprogramm* zur Verfügung stünde, das Sie einfach an MATRIX WIZARD anhängen könnten und das immer überprüfen würde, ob das behauptete Ergebnis, die Matrix  $C$ , wirklich das Produkt der Eingabematrizen  $A$  und  $B$  ist. Ein Testprogramm, das einfach  $A$  und  $B$  multipliziert und das Ergebnis mit  $C$  vergleicht, wäre natürlich wenig sinnvoll; da Sie Matrizen nicht so schnell multiplizieren können wie MATRIX WIZARD, wären alle Vorteile des teuren Multiplikationsalgorithmus für die Katz. Doch es stellt sich heraus, dass es tatsächlich einen sehr einfachen, effizienten Test für Matrixmultiplikation gibt, wenn wir nicht absolute Gewissheit verlangen, sondern dem Test eine geringe Fehlerwahrscheinlichkeit zugestehen. Der Einfachheit halber nehmen wir an, dass die betrachteten Matrizen rationale Zahlen enthalten; es funktioniert aber alles ganz genauso auch bei Matrizen über jedem anderen Körper.

**13.6.1 Satz (Matrixmultiplikations–Test nach Freivalds).** Es gibt einen randomisierten Algorithmus, der für je drei  $n \times n$  Eingabematrizen  $A, B, C$  mit rationalen Einträgen  $O(n^2)$  arithmetische Operationen ausführt und dann entweder KORREKT oder INKORREKT antwortet. Wenn  $A, B, C$  die Gleichung  $AB = C$  erfüllen, dann sagt der Algorithmus auf jeden Fall KORREKT. Wenn aber  $AB \neq C$ , dann antwortet der Algorithmus INKORREKT mit mindestens der Wahrscheinlichkeit  $\frac{1}{2}$ .

Mit „randomisierter Algorithmus“ meinen wir einen Algorithmus, der einige Entscheidungen zufällig treffen kann. Wir dürfen uns das so vorstellen, dass er einige Male „eine Münze wirft“ und je nach Ergebnis (Kopf/Zahl) auf eine von zwei möglichen Arten fortfährt.

In richtigen Computern sitzt natürlich kein Zwerg, der bei Bedarf Münzen wirft, denn ein Zwerg würde (wie jede andere bekannte physikalische Realisierung eines Zufallsexperiments) die Berechnungen beträchtlich verlangsamen, von den anderen technischen Problemen ganz zu schweigen. Zufall wird durch komplizierte, nicht zufällige Berechnungen simuliert; wenn das „gut“ gelingen soll, ist das eine sehr anspruchsvolle Herausforderung. Doch in den meisten Programmiersprachen ist ein mehr oder weniger befriedigender Zufallszahlengenerator eingebaut,

und so werden wir dieses Problem nicht weiter verfolgen und annehmen, dass uns echte Zufallszahlen zur Verfügung stehen. Mehr über randomisierte Algorithmen, insbesondere im Zusammenhang mit dem Freivalds–Test, finden Sie im Buch von Motwani und Raghavan [27]. Die Lektüre dieses Buchs ist ein Genuss für jeden, der an Kombinatorik und theoretischer Informatik interessiert ist.

In unserem Fall heißt das, dass der Algorithmus aus dem Satz für feste Matrizen  $A, B, C$  mit  $AB \neq C$  manchmal INKORREKT und manchmal KORREKT antworten kann, je nach dem Ausgang der internen Zufallsentscheidungen. Der Satz behauptet, dass die Wahrscheinlichkeit für die (falsche) Antwort KORREKT nicht größer ist als  $\frac{1}{2}$ .

Halt, werden Sie vielleicht rufen, soll das heißen, dass im Falle eines Rechenfehlers von MATRIX WIZARD der Test das Ergebnis mit Wahrscheinlichkeit  $\frac{1}{2}$  für richtig hält? Das ist doch, bitteschön, noch schlechter als beim Wetterbericht! Nun gut, es gibt da aber einen subtilen Unterschied: Den Testalgorithmus können wir mehrere Male für die gleichen Matrizen  $A, B, C$  starten, und wenn die Antwort nur ein einziges Mal INKORREKT ist, genügt das um  $AB \neq C$  zu erkennen. Wenn wir  $k$ -mal die gleichen  $A, B, C$  mit  $AB \neq C$  testen, dann ist die Wahrscheinlichkeit dafür, jedes Mal die falsche Antwort KORREKT zu erhalten und so den Rechenfehler durchgehen zu lassen, höchstens  $(\frac{1}{2})^k$ , weil die Antworten der einzelnen Testläufe unabhängig voneinander sind. Für  $k = 50$  etwa liegt diese Wahrscheinlichkeit unter  $10^{-15}$ , womit dies vermutlich sehr viel unwahrscheinlicher ist, als dass der Computer, auf dem der Algorithmus läuft, nächsten Freitag von Ameisen oder einer Atombombe zerstört wird. (Den Wetterbericht 50 Mal hintereinander zu hören liefert hingegen nicht annähernd diese fast absolute Sicherheit über das morgige Wetter.) Und so können wir die Folgerung aus dem Satz auch anders formulieren: In  $O(n^2 \log \frac{1}{\delta})$  Laufzeit kann man die Wahrscheinlichkeit, dass die Antwort falsch ist, unter  $\delta$  drücken, und zwar für jede Zahl  $\delta > 0$ , die man sich vorgibt.

*Beweis von Satz 13.6.1.* Der Algorithmus ist tatsächlich sehr einfach. Wir wählen einen zufälligen Vektor  $x \in \{0, 1\}^n$ , alle  $2^n$  möglichen Vektoren sollen gleich wahrscheinlich sein (der zu Grunde liegende Wahrscheinlichkeitsraum ist also  $\mathcal{S}_n$  aus Definition 10.2.2). Wir berechnen den Vektor  $y = ABx - Cx$ , wobei wir  $x$  und  $y$  als  $n \times 1$  Matrizen auffassen. Ist  $y = 0$ , so geben wir KORREKT aus, sonst INKORREKT.

Einen Vektor und eine  $n \times n$  Matrix kann man mit  $O(n^2)$  Operationen multiplizieren. Die richtige Methode, das Produkt  $ABx$  auszurechnen, ist  $A(Bx)$  zu klammern, wofür wir zwei Matrix–Vektor Multiplikationen ausführen müssen. So erhalten wir  $y$  in  $O(n^2)$  Schritten. Nun ist noch die Behauptung über die Wahrscheinlichkeit zu beweisen. Wenn  $AB = C$  ist, dann ist offensichtlich  $y = ABx - Cx = (AB - C)x = 0$ ; in diesem Fall sagt der Algorithmus also stets KORREKT. Wir nehmen an, dass  $AB \neq C$  ist, und schreiben  $D = AB - C$ . Es genügt folgendes zu zeigen:

**Lemma.** *Sei  $D$  eine rationale  $n \times n$  Matrix mit mindestens einem von Null verschiedenen Eintrag. Dann ist die Wahrscheinlichkeit dafür, dass  $y = Dx$  der Nullvektor ist, für einen zufälligen Vektor  $x \in \{0,1\}^n$  höchstens  $\frac{1}{2}$ .*

*Beweis des Lemmas.* Angenommen,  $d_{ij} \neq 0$  ist ein Eintrag der Matrix  $D$ . Wir zeigen, dass in diesem Fall  $y_i = 0$  mit Wahrscheinlichkeit höchstens  $\frac{1}{2}$  gilt. Es ist

$$y_i = d_{i1}x_1 + d_{i2}x_2 + \cdots + d_{in}x_n = d_{ij}x_j + S,$$

wobei

$$S = \sum_{\substack{k=1,2,\dots,n \\ k \neq j}} d_{ik}x_k.$$

Wir stellen uns vor, dass wir die Werte für die Einträge von  $x$  mit  $n$  Münzwürfen festlegen und dass derjenige Münzwurf, mit dem wir den Wert von  $x_j$  bestimmen, als letztes erfolgt (weil die Münzwürfe unabhängig sind, kommt es ja nicht darauf an). Vor diesem letzten Wurf ist die Zahl  $S$  schon festgelegt, denn sie ist von  $x_j$  unabhängig. Nach dem letzten Wurf ist entweder  $y_i = S$  (wenn  $x_j = 0$ ) oder  $y_i \neq S$  (wenn  $x_j = 1$ ). In mindestens einem dieser Fälle ist  $y_i \neq 0$ , folglich ist die Wahrscheinlichkeit, dass  $y_i = 0$ , höchstens  $\frac{1}{2}$ . Damit ist das Lemma bewiesen, und auch der Beweis von Satz 13.6.1 ist abgeschlossen.  $\square$

Es ist eine wohl bekannte Tatsache, dass es fast unmöglich ist, kompliziertere Software fehlerfrei zu programmieren. Das ist beunruhigend, denn uns umgeben mehr und mehr computergesteuerte Maschinen, und die Möglichkeit, dass etwas nicht funktioniert, ist sehr real (spektakuläre Beispiele waren die Probleme bei den Apollo und Space Shuttle Projekten, doch man muss nicht unbedingt in den Weltraum gehen, um Softwarefehler zu finden). Es ist ein bestechender Gedanke, die Ergebnisse

komplizierter Berechnungen einem unabhängigen Test zu unterwerfen. Neuere Forschungen haben ergeben, dass praktisch jede Berechnung einer probabilistischen Überprüfung zugänglich ist. Im Prinzip kann man die Ergebnisse eines sehr schnellen Computers sehr zuverlässig (im Sinne der Wahrscheinlichkeitstheorie) von einem sehr viel langsameren Computer testen lassen. Auch wenn sich diese Vorgehensweise noch nicht wirklich durchgesetzt hat, eröffnet sie doch interessante Möglichkeiten.

Darüber hinaus hat diese Richtung der Informatik gemeinsam mit Ideen aus anderen Bereichen zu einigen sehr tiefen und unerwarteten Resultaten geführt. So konnte man beweisen, dass gewisse algorithmische Probleme „schwer approximierbar“ sind. Man weiß z.B. schon lange, dass die Aufgabe, in einem gegebenen Graphen einen größtmöglichen vollständigen Teilgraphen zu finden, zu einer gewissen Klasse schwieriger Probleme gehört, die man „NP-vollständig“ nennt. Die neuen Resultate sagen nun, wenn es einen effizienten Algorithmus zur Approximation der Größe eines größten vollständigen Teilgraphen mit irgend-einem vernünftigen vorgegebenen Fehler gäbe, dann gäbe es auch einen effizienten Algorithmus, der diese Größe exakt bestimmt. Auch wenn es etwas mysteriös scheint, dass der Beweis eines solchen Resultats etwas mit probabilistischen Tests zu tun haben soll: es ist so. Mehr zu diesen neuen Entwicklungen und noch einiges andere findet man bei Arora und Barak [11].

**Probabilistischer Assoziativitätstest.** Sei  $S$  eine Menge und sei  $\circ$  eine *binäre Operation* auf  $S$ . Das heißt, dass je zwei Elementen  $a, b \in S$  ein Element  $c \in S$  zugeordnet wird, und dieses  $c$  wird mit  $a \circ b$  bezeichnet. Formal ist  $\circ$  also eine Abbildung  $S \times S \rightarrow S$ . Sie kennen schon viele binäre Operationen mit Zahlen. Zum Beispiel ist „+“ (die Addition) eine binäre Operation auf der Menge aller natürlichen Zahlen, und „–“ (die Subtraktion) ist eine binäre Operation auf der Menge aller ganzen Zahlen. Andererseits ist „–“ keine binäre Operation auf  $\mathbb{N}$  und „/“ (die Division) ist keine binäre Operation auf der Menge aller reellen Zahlen im Sinne unserer Definition. All diese uns so vertrauten Operationen gehorchen verschiedenen Gesetzen wie Kommutativität ( $a + b = b + a$ ) oder Assoziativität ( $(a + b) + c = a + (b + c)$ ). Hier werden wir eine wirklich beliebige Operation  $\circ$  betrachten, sie darf völlig regellos und anarchistisch sein; wir machen keine Annahmen wie Kommutativität, Assoziativität oder dergleichen.

In der Algebra heißt eine Menge  $S$  mit einer beliebigen binären Operation ein *Gruppoid*.

Vielleicht ist es erhellend, die Definition einer binären Operation auf

$S$  mit der Definition einer binären Relation auf  $S$  zu vergleichen: Eine Relation ordnet jedem Paar  $(a, b) \in S \times S$  eine Antwort JA oder NEIN zu (die Elemente stehen entweder in Relation zueinander oder nicht), während eine Operation dem Paar  $(a, b)$  ein „Ergebnis“ zuordnet, das wiederum in  $S$  liegt. Im Gegensatz zur großen Zahl nicht mathematischer Beispiele für Relationen scheint es, als gäbe es Operationen im hier betrachteten Sinne ausschließlich in der Mathematik; zumindest wir sehen kein einziges überzeugendes, nicht triviales Beispiel außerhalb der Mathematik. Natürlich gibt es viele Situationen, in denen aus zwei Objekten ein drittes Objekt von gleicher Art entsteht, aber von einer binären Operation erwarten wir, dass je zwei Objekte so kombiniert werden können und dass das Ergebnis auch wieder von der gleichen Art ist.

Wir interessieren uns für den Fall, dass  $S$  eine endliche Menge ist; die Operation  $\circ$  sei durch eine Wertetabelle gegeben, wie die folgende im Fall  $S = \{A, B, \Gamma, \Delta\}$ :

$\circ$	$A$	$B$	$\Gamma$	$\Delta$
$A$	$A$	$A$	$A$	$A$
$B$	$A$	$B$	$\Gamma$	$\Delta$
$\Gamma$	$A$	$\Gamma$	$A$	$\Gamma$
$\Delta$	$A$	$\Delta$	$A$	$B$

Wir würden gerne prüfen, ob die gegebene Operation  $\circ$  assoziativ ist oder nicht. Wir nennen ein Tripel  $(a, b, c) \in S^3$  ein *assoziatives Tripel*, wenn  $(a \circ b) \circ c = a \circ (b \circ c)$  gilt, ansonsten ein *nicht assoziatives Tripel*. Eine offensichtliche Methode ist, alle Tripel  $(a, b, c) \in S^3$  durchzugehen und auf Assoziativität zu testen. Für jedes Tripel  $(a, b, c)$  müssen wir zweimal in der Tabelle nachsehen um  $(a \circ b) \circ c$  zu bestimmen, und zwei weitere Male um  $a \circ (b \circ c)$  zu berechnen. Ist also  $|S| = n$ , so benötigt dieser munter drauflos rechnende Assoziativitätstest großenordnungsmäßig  $n^3$  Operationen.

Wir stellen nun einen genialen Algorithmus von Rajagopalan und Schulman vor, der Assoziativität mit  $O(n^2)$  Operationen testet. Wieder ist es ein randomisierter Algorithmus, dessen Antwort nicht mit 100%-iger Sicherheit richtig ist.

**13.6.2 Satz.** *Es gibt einen randomisierten Algorithmus mit den folgenden Eigenschaften. Er akzeptiert als Eingabe eine mittels Wertetabelle definierte binäre Operation  $\circ$  auf einer gegebenen  $n$ -Menge. Die Ausgabe ist eine der Antworten ASSOZIATIV oder NICHTASSOZIATIV und die Laufzeit ist  $O(n^2)$ . Im Fall, dass  $\circ$  assoziativ ist, gibt der Algorithmus stets die korrekte Antwort ASSOZIATIV,*

und im Fall, dass  $\circ$  nicht assoziativ ist, entdeckt er die Nichtassoziativität mit Wahrscheinlichkeit mindestens  $\frac{1}{8}$  (bei jeder beliebigen Operation  $\circ$ ).

Die Wahrscheinlichkeit einer falschen Antwort kann man beliebig klein machen, indem man den Algorithmus oft genug wiederholt, ähnlich wie bei Satz 13.6.1. Das heißt, wenn wir den Algorithmus für eine nicht assoziative Operation  $k$ -mal wiederholen, wird er mit Wahrscheinlichkeit mindestens  $1 - \left(\frac{7}{8}\right)^k$  mindestens einmal die Antwort NICHTASSOZIATIV geben.

Ein randomisierter Algorithmus für den Test auf Assoziativität, der einem spontan einfällt, wäre wiederholt ein zufälliges Tripel  $(a, b, c) \in S^3$  zu wählen und auf Assoziativität zu testen. Doch der springende Punkt ist, dass sich Nicht-Assoziativität nicht in vielen Tripeln zu manifestieren braucht. Die Operation aus der obigen Wertetabelle hat z.B. nur zwei nicht assoziative Tripel, nämlich  $(\Delta, \Delta, \Gamma)$  und  $(\Delta, \Gamma, \Delta)$ , während es insgesamt  $4^3 = 64$  Tripel gibt. Tatsächlich gibt es für jedes  $n \geq 3$  ein Beispiel für eine Operation auf einer  $n$ -Menge mit genau einem nicht assoziativen Tripel (Aufgabe 4). Deshalb ist unsere Chance, die Nicht-Assoziativität zu bemerken, selbst wenn wir  $n^2$  zufällige Tripel testen, nur  $\frac{1}{n}$ , und nicht eine Konstante wie beim Algorithmus in Satz 13.6.2.

*Beweis von Satz 13.6.2.* Sei  $S$  die gegebene  $n$ -Menge. Zunächst definieren wir zu  $S$  einen Vektorraum über  $GF(2)$ . Das erinnert stark an die Definitionen für den Zyklenraum eines Graphen in Abschnitt 13.4.

Mit  $V$  bezeichnen wir die Menge aller  $n$ -Tupel aus Nullen und Einsen, deren Glieder mit den Elementen aus  $S$  nummeriert sind. Für  $a \in S$  und  $v \in V$  bezeichne  $(v)_a \in \{0, 1\}$  denjenigen Eintrag von  $v$ , der mit dem Element  $a$  nummeriert ist. Weiter sei  $\mathbf{v}_a$  für ein Element  $a \in S$  der charakteristische Vektor der Menge  $\{a\}$ , d.h. der Vektor, bei dem der zu  $a$  gehörende Eintrag 1 ist und alle anderen Einträge 0.

Man kann die Menge  $V$  als einen Vektorraum über dem 2-elementigen Körper  $GF(2)$  auffassen, was an die im Zusammenhang mit dem Zyklenraum eines Graphen angestellten Überlegungen erinnert. Man addiert Vektoren komponentenweise, ebenso multipliziert man einen Vektor mit einem Element aus  $GF(2)$  komponentenweise.

Weil wir es mit mehreren verschiedenen Arten von Objekten zu tun haben, wollen wir uns zur besseren Unterscheidung an folgen-

de Notation halten: Die Buchstaben  $u, v, w$  stehen für Elemente aus  $V$ , d.h.  $n$ -Tupel von Nullen und Einsen, die griechischen Buchstaben  $\alpha, \beta, \gamma$  bezeichnen Elemente aus  $GF(2)$ , d.h. 0 oder 1, und  $a, b, c, p, q, r$  sind Elemente aus  $S$ .

Als Nächstes definieren wir auf Grundlage der Operation  $\circ$  auf  $S$  eine binäre Operation auf  $v$ , die wir auch  $\circ$  schreiben. Für  $u, v \in S$  setzen wir

$$u \circ v = \sum_{a,b \in S} (u)_a (v)_b \mathbf{v}_{a \circ b}.$$

Die Multiplikation  $(u)_a (v)_b$  auf der rechten Seite ist die in  $GF(2)$ , mit dem Ergebnis wird der Vektor  $\mathbf{v}_{a \circ b}$  multipliziert, und das Summenzeichen addiert Vektoren aus  $V$ . Das wird anschaulicher, wenn wir für den Moment  $S = \{p, q, r\}$  annehmen und  $u = \alpha_p \mathbf{v}_p + \alpha_q \mathbf{v}_q + \alpha_r \mathbf{v}_r$ ,  $v = \beta_p \mathbf{v}_p + \beta_q \mathbf{v}_q + \beta_r \mathbf{v}_r$  schreiben. Natürlich sind  $\alpha_p, \alpha_q, \alpha_r \in \{0, 1\}$  einfach die Einträge von  $u$ , und bei  $v$  sieht es analog aus. Um den Vektor  $u \circ v$  zu finden, multiplizieren wir als erstes die Klammern aus:

$$\begin{aligned} & (\alpha_p \mathbf{v}_p + \alpha_q \mathbf{v}_q + \alpha_r \mathbf{v}_r) \circ (\beta_p \mathbf{v}_p + \beta_q \mathbf{v}_q + \beta_r \mathbf{v}_r) \\ &= \alpha_p \beta_p (\mathbf{v}_p \circ \mathbf{v}_p) + \alpha_p \beta_q (\mathbf{v}_p \circ \mathbf{v}_q) + \cdots + \alpha_r \beta_r (\mathbf{v}_r \circ \mathbf{v}_r). \end{aligned}$$

Dann „vereinfachen“ wir diesen Ausdruck mit Hilfe der Definition  $\mathbf{v}_a \circ \mathbf{v}_b = \mathbf{v}_{a \circ b}$  für alle  $a, b \in S$ .

Wir behaupten, dass die Operation  $\circ$  auf  $V$  genau dann assoziativ ist, wenn schon  $\circ$  auf  $S$  assoziativ war. Natürlich, wenn  $(a, b, c)$  ein nicht assoziatives Tripel in  $S$  ist, mit  $(a \circ b) \circ c = p \neq q = a \circ (b \circ c)$ , dann haben wir  $(\mathbf{v}_a \circ \mathbf{v}_b) \circ \mathbf{v}_c = \mathbf{v}_p \neq \mathbf{v}_q = \mathbf{v}_a \circ (\mathbf{v}_b \circ \mathbf{v}_c)$ . Der Nachweis der Assoziativität von  $\circ$  auf  $V$  bei assoziativem  $\circ$  auf  $S$  ist eine leichte Übung (Aufgabe 5).

Für den Algorithmus, der die Assoziativität testen soll, definieren wir eine Funktion  $g: V^3 \rightarrow V$  durch

$$g(u, v, w) = [(u \circ v) \circ w] - [u \circ (v \circ w)].$$

Nach der obigen Diskussion wissen wir, dass  $g$  genau dann die Nullfunktion ist, wenn  $\circ$  assoziativ ist (auf  $V$  und somit auch auf  $S$ ). Sind Vektoren  $u, v \in V$  gegeben, dann kann man  $u \circ v$  mit der Wertetabelle für  $\circ$  auf  $S$  in  $O(n^2)$  Operationen berechnen. Deshalb lässt sich auch  $g(u, v, w)$  in Zeit  $O(n^2)$  auswerten.

Nun sind wir soweit, den Algorithmus zu Satz 13.6.2 zu formulieren.

**13.6.3 Algorithmus.** Wähle zufällig und unabhängig voneinander drei Vektoren  $u, v, w \in V$  (jeder der  $2^n$  Vektoren aus  $V$  wird mit gleicher Wahrscheinlichkeit  $u$ , usw.). Berechne  $g(u, v, w)$  und antworte ASSOZIATIV, wenn  $g(u, v, w) = 0$  ist, sonst NICHT ASSOZIATIV.

Es bleibt zu zeigen, dass für eine nicht assoziative Operation  $\circ$  die Antwort NICHT ASSOZIATIV mit Wahrscheinlichkeit mindestens  $\frac{1}{8}$  herauskommt. Das heißt, dass mindestens  $\frac{1}{8}$  der möglichen Tripel  $(u, v, w) \in V^3$  nicht assoziativ sind. Dazu fixieren wir irgendein nicht assoziatives Tripel  $(a, b, c) \in S^3$ . Wir nennen zwei Tripel  $(u_1, v_1, w_1)$  und  $(u_2, v_2, w_2)$  äquivalent, wenn  $u_1$  und  $u_2$  in allen Komponenten übereinstimmen, außer eventuell in dem zu  $a$  gehörenden Eintrag (d.h.  $u_1 - u_2 = \alpha \mathbf{v}_a$ ,  $\alpha \in GF(2)$ ),  $v_1$  und  $v_2$  in allen Komponenten außer möglicherweise der zu  $b$  gehörenden übereinstimmen, und  $w_1$  und  $w_2$  sich wenn überhaupt nur in dem zu  $c$  gehörenden Eintrag unterscheiden. Jede Äquivalenzklasse hat genau acht Elemente. Wir zeigen, dass jede Äquivalenzklasse mindestens ein nicht assoziatives Tripel enthält:

**Lemma.** Sei  $(a, b, c)$  ein nicht assoziatives Tripel. Für alle  $u, v, w \in V$  gibt es  $\alpha, \beta, \gamma \in GF(2)$ , so dass

$$g(u + \alpha \mathbf{v}_a, v + \beta \mathbf{v}_b, w + \gamma \mathbf{v}_c) \neq 0.$$

*Beweis des Lemmas.* Was wir tatsächlich zeigen ist, dass die Summe

$$\sigma = \sum_{\alpha, \beta, \gamma \in GF(2)} g(u + \alpha \mathbf{v}_a, v + \beta \mathbf{v}_b, w + \gamma \mathbf{v}_c)$$

nicht Null ist. Aus der Definition der Operation  $\circ$  auf  $V$  erhalten wir für alle  $u, v, w \in V$

$$g(u, v, w) = \sum_{p, q, r \in S} (u)_p (v)_q (w)_r \mathbf{v}_{g(p, q, r)}.$$

Wenn wir dies in die Summe  $\sigma$  einsetzen und die Reihenfolge der Summation vertauschen, erhalten wir

$$\sigma = \sum_{p, q, r \in S} \left[ \sum_{\alpha, \beta, \gamma \in GF(2)} (u + \alpha \mathbf{v}_a)_p (v + \beta \mathbf{v}_b)_q (w + \gamma \mathbf{v}_c)_r \right] \mathbf{v}_{g(p, q, r)}.$$

Die Summe in den Klammern kann man unter Ausnutzen der Distributivität in  $GF(2)$  auch wie folgt schreiben:

$$\begin{aligned} & \sum_{\alpha, \beta, \gamma \in GF(2)} (u + \alpha \mathbf{v}_a)_p (v + \beta \mathbf{v}_b)_q (w + \gamma \mathbf{v}_c)_r \\ &= [(u)_p + (u + \mathbf{v}_a)_p] [(v)_q + (v + \mathbf{v}_b)_q] [(w)_r + (w + \mathbf{v}_c)_r] \\ &= (2u + \mathbf{v}_a)_p (2v + \mathbf{v}_b)_q (2w + \mathbf{v}_c)_r = (\mathbf{v}_a)_p (\mathbf{v}_b)_q (\mathbf{v}_c)_r \end{aligned}$$

weil  $2 = 1+1 = 0$  in  $GF(2)$ . Folglich ist genau einer der Summanden von  $\sigma$  ungleich Null, nämlich der mit  $p = a$ ,  $q = b$  und  $r = c$ , somit ist  $\sigma = \mathbf{v}_{g(a,b,c)} \neq 0$ . Dies beweist das Lemma und schließt damit den Beweis von Satz 13.6.2 ab.  $\square$

*Bemerkungen.* Den Algorithmus und seine Analyse könnte man auch formulieren, ohne den Vektorraum  $V$  einzuführen. Wir könnten einfach über zufällige Teilmengen von  $S$  reden usw., aber das scheint das Ganze nicht klarer zu machen, sondern eher zu verschleiern. Man kann diesen Ansatz auch verallgemeinern und so andere Identitäten für eine oder mehrere binäre oder  $k$ -näre Operationen auf einer gegebenen endlichen Menge testen; einige interessante Probleme sind aber weiterhin ungelöst. Mehr Details finden Sie in dem Originalartikel von Rajagopalan und Schulman [45].

## Aufgaben

1. Angenommen, wir wählen die Komponenten des Vektors  $x$  zufällig aus der Menge  $\{0, 1, \dots, m\}$  statt aus  $\{0, 1\}$  im Freivalds–Test (Satz 13.6.1). Zeigen Sie, dass die Wahrscheinlichkeit für eine falsche Antwort in diesem Fall höchstens  $\frac{1}{m}$  ist.
2. \*Angenommen, wir haben ein sehr schnelles Programm zur Multiplikation zweier Polynome  $p(x)$  und  $q(x)$  mit ganzzahligen Koeffizienten. Entwickeln Sie einen schnellen probabilistischen Test für die Korrektheit des Ergebnisses, analog zum Freivalds–Test für die Matrixmultiplikation. Wenn drei Polynome  $p(x)$ ,  $q(x)$  und  $r(x)$  gegeben sind, sollte der Algorithmus testen, ob  $r(x) = p(x)q(x)$ . Benutzen Sie die Tatsache, dass ein nicht triviales Polynom vom Grad  $d$  höchstens  $d$  Nullstellen hat.
3. Wie viele binäre Operationen gibt es auf einer  $n$ -Menge  $S$ ?
4. \*Finden Sie für jedes  $n \geq 3$  ein Beispiel für eine  $n$ -Menge  $S$  und auf ihr eine nicht assoziative binäre Operation, die nur ein nicht assoziatives Tripel besitzt.
5. Es sei  $\circ$  eine assoziative Operation auf  $S$ . Beweisen Sie, dass dann auch die im Beweis von Satz 13.6.2 definierte Operation  $\circ$  auf  $V$  assoziativ ist.

6. *Inf* Implementieren Sie den randomisierten Algorithmus zum Test auf Assoziativität. Vergleichen Sie seine Geschwindigkeit bei verschiedenen Eingaben mit der des simplen  $O(n^3)$ -Algorithmus.
7. Sei  $S$  eine endliche Menge mit einer binären Operation  $\circ$ . Für  $G \subseteq S$  sei  $G^{(1)} = G$  und  $G^{(k+1)} = G^{(k)} \cup \{a \circ b : a, b \in G^{(k)}\}$ ; des Weiteren sei  $\langle G \rangle = \bigcup_{k=1}^{\infty} G^{(k)}$ . Von einer Menge  $G \subseteq S$  sagt man, sie *erzeugt*  $S$ , wenn  $\langle G \rangle = S$ .
  - (a) Zeigen Sie: Wenn  $S$  von  $G$  erzeugt wird und  $(a \circ g) \circ c = a \circ (g \circ c)$  für alle  $a, b \in S$  und  $g \in G$  gilt, dann muss  $\circ$  assoziativ sein.
  - (b) \*Die Menge  $S$  zusammen mit der Operation  $\circ$  heißt eine *Quasigruppe*, wenn es für alle  $a, b \in S$  ein eindeutiges  $x \in S$  gibt mit  $a \circ x = b$  und ein eindeutiges  $y \in S$  mit  $y \circ a = b$ . Beweisen Sie: Ist  $S$  mit  $\circ$  eine Quasigruppe,  $A \subset S$  eine nicht leere Menge und  $b \in S \setminus \langle A \rangle$ , dann ist  $|\langle A \cup \{b\} \rangle| \geq 2|\langle A \rangle|$ .
  - (c) Sei  $S$  mit  $\circ$  eine Quasigruppe und  $|S| = n$ . Beweisen Sie unter Verwendung von (b), dass es eine Menge mit höchstens  $\log_2 n + 1$  Elementen gibt, die  $S$  erzeugt, und *Inf,\** die man in Zeit  $O(n^2 \log n)$  finden kann.

Für eine Quasigruppenoperation  $\circ$  ergeben (a) und (c) zusammen einen Assoziativitätstest, der völlig ohne Zufall funktioniert und Laufzeit  $O(n^2 \log n)$  hat.
8. (Abschlussaufgabe) (a) Können Sie nun, nachdem Sie das Buch durchgearbeitet haben, alle Probleme aus Abschnitt 1.1 lösen?  
 (b) Erklären Sie mindestens eines der Probleme einschließlich einer Lösung einem gebildeten Menschen, der jedoch kein Spezialist sein sollte (z.B. jemandem, der in der Schule nicht schlecht war in Mathe, sich aber seit dem Abitur nicht mehr damit beschäftigt hat)! Diese Übung ist für Ihr Fortkommen möglicherweise die allerwichtigste aus diesem Buch.



# Anhang: Grundlagen aus der Algebra

---

Dies ist ein Crashkurs über Matrizen, Vektorräume, Körper und andere Begriffe aus der Algebra, die an einigen Stellen in diesem Buch verwendet werden. Im Gegensatz zu den anderen Kapiteln ist dieser Teil aber nicht als eine Einführung in das Gebiet gedacht. Er richtet sich hauptsächlich an solche Leser, die schon Kenntnisse auf dem Gebiet haben, die aber die genauen Definitionen nicht mehr präsent haben oder sie in einer etwas anderen Form kennen.

**Matrizen.** Eine Matrix ist ein rechteckiges Zahlenschema. Die Einträge können reelle oder komplexe Zahlen sein, aber auch Elemente anderer algebraischer Strukturen. Eine  $m \times n$  Matrix hat  $m$  Zeilen und  $n$  Spalten. In einer Matrix  $A$  nennt man den Eintrag in der  $i$ -ten Zeile und der  $j$ -ten Spalte gewöhnlich  $a_{ij}$ . Eine  $3 \times 4$  Matrix  $A$  hat also im Allgemeinen die Form

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{pmatrix}.$$

Eine Matrix ist dadurch gekennzeichnet, dass die Tabelle der Einträge von großen Klammern begrenzt ist.

Eine Matrix wird mit einer Zahl  $\alpha$  multipliziert, indem jeder Eintrag mit  $\alpha$  multipliziert wird. Zwei  $m \times n$  Matrizen  $A$  und  $B$  werden addiert, indem man die entsprechenden Einträge addiert. Das heißt, mit  $C = A + B$  haben wir  $c_{ij} = a_{ij} + b_{ij}$  für  $i = 1, 2, \dots, m$  und  $j = 1, 2, \dots, n$ .

Die *Multiplikation von Matrizen* ist komplizierter. Das Produkt  $AB$  zweier Matrizen  $A$  und  $B$  ist nur definiert, wenn die Anzahl der Spalten von  $A$  gleich der Anzahl der Zeilen von  $B$  ist. Wenn  $A$  eine  $m \times n$  Matrix ist und  $B$  eine  $n \times p$  Matrix, dann ist das Produkt  $C = AB$  eine  $m \times p$  Matrix mit

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}.$$

Bildlich geschrieben:

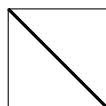
$$\begin{array}{c}
 \begin{array}{c} n \\ \text{Zeile } i \\ m \end{array} \\
 \boxed{\phantom{000}} \\
 A
 \end{array}
 \cdot
 \begin{array}{c} p \\ \text{Spalte } j \\ n \end{array}
 = 
 \begin{array}{c} p \\ \bullet c_{ij} \\ m \end{array}
 \boxed{\phantom{000}} \\
 C
 \end{array}$$

Wenn  $A$  eine  $m \times n$  Matrix ist und  $x = (x_1, x_2, \dots, x_n)$  ein Vektor, dann können wir  $x$  als eine  $n \times 1$  Matrix auffassen (wir stellen uns den Vektor in Spaltenform geschrieben vor) und interpretieren das Produkt  $Ax$  als ein Produkt von zwei Matrizen.

Wenn  $A$  eine  $m \times n$  Matrix ist, dann bezeichnet  $A^T$  die  $n \times m$  Matrix mit dem Element  $a_{ji}$  in der  $i$ -ten Zeile und  $j$ -ten Spalte. Die Matrix  $A^T$  heißt die zu  $A$  *transponierte* Matrix. Wenn wir zum Beispiel  $x = (x_1, x_2, \dots, x_n)$  als einen Spaltenvektor auffassen, das heißt als eine  $n \times 1$  Matrix, dann ist  $x^T$  eine  $1 \times n$  Matrix oder ein Zeilenvektor. (In der Literatur werden Vektoren manchmal sogar ohne das Transpositionszeichen als Zeilenvektoren aufgefasst.) Wenn  $x$  und  $y$  (Spalten-)Vektoren mit  $n$  Einträgen sind, ist das Produkt  $x^T y$  eine  $1 \times 1$  Matrix, das heißt eine einzige Zahl, genannt das *Skalarprodukt* von  $x$  und  $y$ . Ausgeschrieben heißt das  $x^T y = \sum_{i=1}^n x_i y_i$ . Die Vektoren  $x$  und  $y$  heißen *orthogonal*, wenn  $x^T y = 0$ .

Um ein Matrixprodukt zu transponieren haben wir die Formel  $(AB)^T = B^T A^T$ .

Hier noch einige Bezeichnungen für Matrizen: Eine *quadratische Matrix* ist eine  $n \times n$  Matrix, das heißt eine Matrix mit genauso vielen Zeilen wie Spalten. Die (*Haupt-*)*Diagonale* einer  $n \times n$  Matrix  $A$  besteht aus den Elementen  $a_{11}, a_{22}, a_{33}, \dots, a_{nn}$ ; schematisch:



Eine *obere Dreiecksmatrix* hat unterhalb der Diagonalen nur Nullen, das heißt  $a_{ij} = 0$  für  $i > j$ . Eine *Diagonalmatrix* darf nur auf der Diagonalen von Null verschiedene Einträge haben, das heißt  $a_{ij} = 0$  für  $i \neq j$ . Die  $n \times n$  *Einheitsmatrix*  $I_n$  hat Einsen auf der Diagonalen und sonst überall Nullen.

**Determinanten.** Jeder quadratischen Matrix  $A$  wird eine Zahl  $\det(A)$  zugeordnet, genannt die *Determinante* von  $A$ . Die Determinante von  $A$  wird durch die Formel

$$\det(A) = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \prod_{i=1}^n a_{i,\pi(i)}$$

definiert, wobei die Summe über alle Permutationen  $\pi$  der Menge  $\{1, 2, \dots, n\}$  läuft und  $\operatorname{sgn}(\pi)$  das *Signum* der Permutation  $\pi$  bezeichnet. Das Signum einer Permutation ist entweder  $+1$  oder  $-1$ , und es kann kurz definiert werden als das Vorzeichen des folgenden Ausdrucks:

$$\prod_{1 \leq i < j \leq n} (\pi(j) - \pi(i)).$$

Die Determinante einer  $2 \times 2$  Matrix  $A$  ist zum Beispiel  $a_{11}a_{22} - a_{12}a_{21}$ . Dies ist fast der einzige Fall, bei dem man die Determinante mit Hilfe der Definition berechnet. Für größere Matrizen stehen verschiedene andere Methoden zur Berechnung der Determinante zur Verfügung. Solche Methoden basieren meist auf den folgenden Rechenregeln für Determinanten:

1. Die Determinante einer oberen Dreiecksmatrix (insbesondere einer Diagonalmatrix) ist gleich dem Produkt ihrer Einträge auf der Diagonalen.
2. („Elementare Zeilenoperationen I“) Multipliziert man in einer Matrix  $A$  alle Einträge einer Zeile mit einer Zahl  $\alpha$ , dann wird die Determinante mit  $\alpha$  multipliziert. Insbesondere wird  $\det(A) = 0$ , wenn  $A$  eine Zeile mit Nulleinträgen hat. Analoges gilt für die Spalten.
3. („Elementare Zeilenoperationen II“) Die Determinante ändert sich nicht, wenn man das Vielfache einer Zeile zu einer anderen Zeile addiert. Das heißt wenn  $i \neq k$  Zeilenindizes sind und wenn der Eintrag  $a_{ij}$  ersetzt wird durch  $a_{ij} + \alpha a_{kj}$  für  $j = 1, 2, \dots, n$ , wobei  $\alpha$  eine feste Zahl ist, dann bleibt die Determinante gleich. Analoges gilt für die Spalten.
4. Für zwei  $n \times n$  Matrizen  $A, B$  ist  $\det(AB) = \det(A)\det(B)$ .
5. („Entwickeln einer Determinante nach einer Zeile“) Für einen Zeilenindex  $i$  haben wir die Formel

$$\det(A) = \sum_{j=1}^n (-1)^{i+j} a_{ij} \det(A_{ij}),$$

wobei  $A_{ij}$  die Matrix bezeichnet, die aus  $A$  durch Streichen der  $i$ -ten Zeile und der  $j$ -ten Spalte entsteht.

Eine quadratische Matrix  $A$  heißt *nicht singulär*, wenn  $\det(A) \neq 0$  ist. Eine *Untermatrix* einer Matrix  $A$  ist eine Matrix, die aus  $A$  durch Streichen von Zeilen und/oder Spalten entsteht. Der *Rang* einer Matrix  $A$ , bezeichnet mit  $r(A)$ , ist die größte Zahl  $k$ , so dass  $A$  eine nicht singuläre  $k \times k$  Untermatrix besitzt (später geben wir eine alternative Definition des Rangs). Für Produkt und Summe von Matrizen gibt es die Ungleichungen  $r(AB) \leq \min(r(A), r(B))$  und  $r(A + B) \leq r(A) + r(B)$ .

**Gruppen und Körper.** Sei  $X$  eine Menge. Eine *binäre Operation* auf  $X$  ist eine Abbildung von  $X \times X$  nach  $X$ ; das heißt, je zwei Elementen  $a, b \in X$  wird ein Element aus  $X$  zugeordnet (siehe auch Abschnitt 13.6). Addition und Multiplikation auf der Menge der natürlichen Zahlen sind zum Beispiel binäre Operationen (die Subtraktion hingegen nicht). Binäre Operationen werden gewöhnlich mit Symbolen wie  $*$ ,  $\circ$ ,  $+$ ,  $\cdot$  geschrieben. Ist zum Beispiel  $*$  eine binäre Operation, so schreiben wir  $a * b$  für dasjenige Element, welches durch  $*$  dem Paar  $(a, b)$  zugeordnet wird.

Eine binäre Operation  $*$  heißt *assoziativ*, falls  $a * (b * c) = (a * b) * c$  für alle  $a, b, c \in X$ . Eine binäre Operation  $*$  heißt *kommutativ*, falls  $a * b = b * a$  für alle  $a, b \in X$ . Praktisch alle binären Operationen, denen man in der Mathematik begegnet, sind assoziativ, aber es gibt wichtige Operationen, die nicht kommutativ sind, wie die Multiplikation von  $n \times n$  Matrizen oder die Komposition von Abbildungen auf einer Menge.

Eine *Gruppe* ist eine Menge  $G$  zusammen mit einer assoziativen binären Operation  $*$ , die den folgenden Axiomen genügt (es gibt viele äquivalente Versionen der Axiome):

- (i) Es gibt ein Element  $e \in G$ , genannt *neutrales Element*, so dass  $a * e = e * a = a$  für alle  $a \in G$ .
- (ii) Für jedes  $a \in G$  gibt es ein Element  $b \in G$  mit  $a * b = b * a = e$ , wobei  $e$  das neutrale Element ist. Ein solches  $b$  wird das *Inverse* von  $a$  genannt und gewöhnlich mit  $a^{-1}$  bezeichnet.

Einige wichtige Beispiele für Gruppen sind die ganzen Zahlen mit der Addition als Operation, die Menge aller positiven reellen Zahlen mit der Multiplikation, die Menge aller nicht singulären reellen  $n \times n$  Matrizen mit der Multiplikation, die Menge aller Permutationen

nen einer gegebenen Menge  $X$  mit der Komposition oder die Menge aller Drehungen um den Ursprung im dreidimensionalen Raum mit der Komposition (also der Hintereinanderausführung der Drehungen). Die natürlichen Zahlen mit der Addition sind hingegen keine Gruppe, genausowenig wie die reellen Zahlen mit der Multiplikation.

Ein *Körper* ist eine Menge  $K$  mit zwei binären Operationen  $+$  und  $\cdot$  (diese Symbole bezeichnen hier nicht unbedingt die gewöhnlichen Operationen mit Zahlen), so dass gilt:

1. Die Menge  $K$  mit der Operation  $+$  ist eine kommutative Gruppe mit neutralem Element 0.
2. Die Menge  $K \setminus \{0\}$  mit der Operation  $\cdot$  ist eine kommutative Gruppe mit neutralem Element 1.
3. Es gilt das *Distributivgesetz*:  $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$  für alle  $a, b, c \in K$ .

Die Multiplikation  $a \cdot b$  wird oft nur als  $ab$  geschrieben. Wichtige Körper sind die rationalen Zahlen, die reellen Zahlen und die komplexen Zahlen (mit der Addition und Multiplikation als Operationen). Die ganzen Zahlen mit der Addition und Multiplikation bilden hingegen keinen Körper.

Wenn  $K$  ein Körper ist und  $L$  eine Teilmenge von  $K$ , die 0 und 1 aus  $K$  enthält, unter den Operationen aus  $K$  abgeschlossen ist (das heißt  $a + b \in L$  und  $a \cdot b \in L$  für alle  $a, b \in L$ ) und mit diesen Operationen ein Körper ist, dann heißt  $L$  ein *Unterkörper* von  $K$ . Der Körper der rationalen Zahlen ist zum Beispiel ein Unterkörper der reellen Zahlen.

In der Kombinatorik benötigen wir oft endliche Körper. Ein endlicher Körper mit  $q$  Elementen wird, falls er existiert, meistens mit  $GF(q)$  bezeichnet. Der einfachste endliche Körper ist  $GF(2)$ . Er besteht nur aus der Menge  $\{0, 1\}$  mit der gewöhnlichen Multiplikation der ganzen Zahlen und mit folgender Addition:  $0 + 0 = 1 + 1 = 0$ ,  $0 + 1 = 1 + 0 = 1$ . Ein endlicher Körper  $GF(q)$  existiert genau dann, wenn  $q$  eine Primzahlpotenz ist. Falls  $q$  eine Primzahl ist, kann  $GF(q)$  leicht dargestellt werden: Es ist die Menge  $\{0, 1, 2, \dots, q-1\}$ , wobei die Addition und Multiplikation zunächst wie bei den ganzen Zahlen berechnet werden, aber nachdem wir zwei Zahlen addiert oder multipliziert haben, dividieren wir durch  $q$  und behalten nur den Rest (man nennt das *Arithmetik modulo q*). Die obige Definition von  $GF(2)$  ist ein Spezialfall dieser Konstruktion. Ist hingegen  $q = p^k$  eine Primzahlpotenz mit einer Primzahl  $p$  und mit  $k > 1$ ,

dann ist die Menge  $\{0, 1, \dots, q - 1\}$  mit der Arithmetik modulo  $q$  *kein Körper*. Die Konstruktion von  $GF(q)$  geht dann anders und ist komplizierter.

**Vektorräume.** Sei  $K$  ein Körper (meistens darf man sich die reellen Zahlen vorstellen). Ein *Vektorraum* über  $K$  ist eine kommutative Gruppe  $V$  mit einer Operation  $+$  und neutralem Element  $0$  zusammen mit einer Abbildung (einer Operation), die jedem Paar  $(\alpha, v)$  mit  $\alpha \in K$  und  $v \in V$  ein Element aus  $V$  zuordnet. Das bedeutet, dass jedes Element aus  $V$  mit jedem Element aus  $K$  „multipliziert“ werden kann. Diese Multiplikation wird meistens ohne Malzeichen geschrieben, wir schreiben einfach  $\alpha v$ , wenn wir  $v$  mit  $\alpha$  multiplizieren wollen. Folgende Bedingungen müssen für alle  $u, v \in V$  und  $\alpha, \beta \in K$  erfüllt sein:  $\alpha(u + v) = \alpha u + \alpha v$ ,  $(\alpha + \beta)v = \alpha v + \beta v$  (es gibt also zwei verschiedene Distributivgesetze),  $\alpha(\beta v) = (\alpha\beta)v$  (so etwas wie Assoziativität) und  $1v = v$ . Damit kann man viele andere Eigenschaften beweisen, zum Beispiel  $0v = 0$  (die linke 0 ist aus dem Körper  $K$  und die rechte 0 im Vektorraum  $V$ ). Die Elemente aus  $V$  heißen *Vektoren*.

Das häufigste und wichtigste Beispiel eines Vektorraums ist das folgende: Wir betrachten alle  $n$ -Tupel reeller Zahlen (für eine gegebene natürliche Zahl  $n$ ) zusammen mit der komponentenweisen Addition und Multiplikation mit einer reellen Zahl. Dies ist ein Vektorraum über dem Körper der reellen Zahlen, aber analog kann man den Vektorraum aller  $n$ -Tupel mit Elementen aus jedem anderen Körper  $K$  betrachten und erhält so einen Vektorraum über  $K$ . Dieser Vektorraum wird gewöhnlich mit  $K^n$  bezeichnet.

Eine Menge  $A \subset V$  heißt *linear abhängig*, wenn es Vektoren  $v_1, v_2, \dots, v_n \in A$ ,  $n \geq 1$ , und Zahlen  $\alpha_1, \alpha_2, \dots, \alpha_n \in K$  gibt, nicht alle  $\alpha_i = 0$ , mit  $\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_n v_n = 0$ . Ist  $A$  nicht linear abhängig, so heißt  $A$  *linear unabhängig*.

Die größtmögliche Mächtigkeit einer linear unabhängigen Menge in  $V$  heißt *Dimension* von  $V$ , und jede linear unabhängige Teilmenge dieser Mächtigkeit von  $V$  heißt *Basis* von  $V$ . Der Vektorraum  $K^n$  hat, wie nicht anders zu erwarten, die Dimension  $n$ .

Jeder Vektorraum hat eine Basis und jede (bezüglich der Inklusion) maximal linear unabhängige Menge ist eine Basis. In der Kombinatorik haben wir es meistens mit Vektorräumen endlicher Dimension zu tun. Falls  $(e_1, e_2, \dots, e_n)$  eine Basis eines  $n$ -dimensionalen Vektorraumes  $V$  ist, kann jeder Vektor  $v \in V$  eindeutig als  $\sum_{i=1}^n \alpha_i e_i$

mit  $\alpha_1, \alpha_2, \dots, \alpha_n \in K$  dargestellt werden. Die Zahlen  $\alpha_1, \dots, \alpha_n$  heißen dann die *Koordinaten* von  $v$  bezüglich der Basis  $(e_1, \dots, e_n)$ . Jedem Vektor  $v \in V$  wird auf diese Weise ein Vektor aus  $K^n$  zugeordnet, nämlich das  $n$ -Tupel seiner Koordinaten. So erhalten wir eine Bijektion zwischen  $V$  und dem Vektorraum  $K^n$  (es gibt viele solcher Bijektionen, abhängig jeweils von der Wahl der Basis). Alle  $n$ -dimensionalen Vektorräume über einem gegebenen Körper sind im Wesentlichen „gleich“, das heißt sie sind isomorph in einem geeigneten definierten Sinn. Daher kann man  $K^n$  als den  $n$ -dimensionalen Vektorraum über  $K$  ansehen, und Vektoren kann man sich gewöhnlich als  $n$ -Tupel von Zahlen vorstellen. Manchmal ist es aber auch praktischer mit anderen Modellen von  $n$ -dimensionalen Vektorräumen über  $K$  zu arbeiten.

Ein *Unterraum* eines Vektorraums  $V$  ist eine Teilmenge  $W \subseteq V$ , die abgeschlossen ist bezüglich der Addition und der Multiplikation mit Elementen aus  $K$ , das heißt  $u + v \in W$  und  $\alpha u \in W$  für alle  $\alpha \in K$  und  $u, v \in W$ . Ist  $X \subseteq V$  eine Menge von Vektoren, dann ist das *Erzeugnis* von  $X$  oder die *lineare Hülle* von  $X$  der kleinste Unterraum von  $V$ , der  $X$  enthält. Explizit aufgeschrieben ist er die Menge  $\{\sum_{i=1}^n \alpha_i v_i : n \in \mathbb{N}, \alpha_1, \dots, \alpha_n \in K, v_1, \dots, v_n \in X\}$ .

Der Rang einer  $m \times n$  Matrix  $A$  mit Einträgen aus einem Körper  $K$  ist gleich der Dimension des von den Zeilen von  $A$  (aufgefasst als  $n$ -elementige Vektoren) erzeugten Unterraums im Raum  $K^n$ . Er ist auch gleich der Dimension des von den Spaltenvektoren von  $A$  erzeugten Unterraums in  $K^m$ . Diese Definition des Rangs ist in gewisser Weise „elementarer“ als die obige Definition über Determinanten.

Für zwei Vektorräume  $V$  und  $W$  über einem Körper  $K$  definieren wir eine *lineare Abbildung* von  $V$  nach  $W$  als eine Abbildung  $f: V \rightarrow W$  mit  $f(\alpha u) = \alpha f(u)$  und  $f(u + v) = f(u) + f(v)$  für alle  $\alpha \in K$  und  $u, v \in V$ . Der *Kern* von  $f$  ist die Menge  $\ker(f) = \{v \in V: f(v) = 0\}$ . Der Kern von  $f$  ist ein Unterraum von  $V$  und die Menge  $f(V)$  ist ein Unterraum von  $W$ . Die Dimension von  $f(V)$  heißt der *Rang* von  $f$ . Für jede lineare Abbildung  $f: V \rightarrow W$  gilt  $\dim \ker(f) + \dim f(V) = \dim V$ .

Sei  $(e_1, e_2, \dots, e_n)$  eine Basis von  $V$  und  $(f_1, f_2, \dots, f_m)$  eine Basis von  $W$ . Dann gibt es eine Bijektion zwischen den linearen Abbildungen  $f: V \rightarrow W$  und den  $m \times n$  Matrizen mit Einträgen aus  $K$ . Wie wir wissen, kann man jeden Vektor  $v \in V$  eindeutig als  $v = \sum_{i=1}^n \alpha_i e_i$

darstellen. Jede lineare Abbildung  $f: V \rightarrow W$  lässt sich wie folgt ausdrücken:

$$f(v) = f\left(\sum_{i=1}^n \alpha_i e_i\right) = \sum_{j=1}^m \left(\sum_{i=1}^n a_{ji} \alpha_i\right) f_j,$$

wobei die  $a_{ij}$  die Elemente aus der  $m \times n$ -Matrix  $A$  sind, die zu  $f$  korrespondiert. Mit anderen Worten: Ist  $\alpha$  der Spaltenvektor mit den Koordinaten von  $v$  bezüglich der Basis  $(e_1, \dots, e_n)$  und  $\beta$  der Spaltenvektor mit den Koordinaten von  $f(v)$  bezüglich der Basis  $(f_1, \dots, f_m)$ , so gilt  $\beta = A\alpha$ .

Lineare Abbildungen können also als abstrakte Version von Matrizen angesehen werden. Die Multiplikation von Matrizen entspricht der Komposition von linearen Abbildungen. Der Rang einer linearen Abbildung entspricht dem Rang der zugehörigen Matrix (unabhängig von der Wahl der Basis).

**Geometrische Deutung.** Oft ist es nützlich, Objekte der linearen Algebra geometrisch zu deuten. Das vertieft nicht nur das Verständnis, sondern hilft auch beim Entwickeln der Intuition. (Abgesehen davon visualisieren die meisten Mathematiker ohnehin gern abstrakte Sachverhalte, malen Bildchen und Diagramme.) Und wie unsere Leserinnen und Leser vermutlich wissen (jedenfalls nach Durcharbeiten des Buches), ist die lineare Algebra ein nützliches Hilfsmittel bei der Arbeit mit geometrischen Objekten. Eine allgemeine Regel für gute geometrische Interpretationen gibt es nicht. Doch einige Interpretationen für Begriffe aus der linearen Algebra sind Standard, wir zeigen hier einige einfache Möglichkeiten. Wir werden uns auf den dreidimensionalen Vektorraum  $\mathbb{R}^3$  beschränken. Doch mit ein wenig Erfahrung können geometrische Skizzen auch in höheren Dimensionen helfen (Mathematiker skizzieren besonders gern Dinge, die „in Wirklichkeit“ nicht zu existieren scheinen).

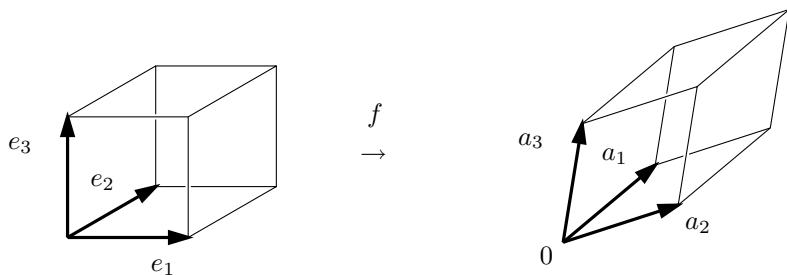
Die Unterräume des Vektorraums  $\mathbb{R}^3$  lassen sich leicht geometrisch beschreiben: der Punkt 0 (der *Ursprung*), alle Geraden und Ebenen, die den Ursprung enthalten, sowie der gesamte Raum  $\mathbb{R}^3$ . Lineare Abhängigkeit dreier Vektoren  $a_1, a_2, a_3 \in \mathbb{R}^3$  bedeutet einfach, dass die Punkte  $a_1, a_2$  und  $a_3$  in einer Ebene liegen, die auch den Ursprung enthält.

Eine Ebene, die den Ursprung nicht enthält, ist kein Unterraum. Eine solche Ebene können wir jedoch als einen in Richtung eines geeigneten Vektors verschobenen Unterraum beschreiben (so eine Ver-

schiebung heißt *Translation*). Alternativ können wir eine Ebene als Lösungsmenge eines linearen Gleichungssystems beschreiben, d.h. als die Menge aller Vektoren  $x = (x_1, x_2, x_3) \in \mathbb{R}^3$ , die eine Gleichung der Form  $a^T x = a_1 x_1 + a_2 x_2 + a_3 x_3 = b_0$  erfüllen, mit einem geeignet gewählten  $b_0 \in \mathbb{R}$  und einem Punkt  $a \in \mathbb{R}^3$ , der nicht der Ursprung ist.

Wenn wir eine  $m \times 3$  Matrix  $A$  gegeben haben und einen Spaltenvektor  $b \in \mathbb{R}^m$  mit  $m$  Koordinaten, dann repräsentiert die Matrixgleichung  $Ax = b$  einfach ein System  $m$  linearer Gleichungen, für die der Vektor  $x$  eine Lösung ist. Jede Zeile von  $A$  ergibt eine der Gleichungen. Mit Ausnahme des singulären Falls, dass eine Zeile nur aus Nullen besteht, legt jede solche Gleichung eine eindeutige Ebene fest. Daraus folgt, dass die Lösungsmenge der Gleichung  $Ax = b$  gerade die Schnittmenge von  $m$  Ebenen ist (falls nicht eine der Zeilen von  $A$  aus lauter Nullen besteht). Für  $m = 2$  können diese beiden Ebenen gleich sein (dann besteht die Lösungsmenge aus allen Punkten dieser Ebene), sie können parallel sein (dann gibt es keine Lösung), oder sie sind verschieden und schneiden sich (und zwar in einer Geraden, die Lösungsmenge besteht dann aus allen Punkten dieser Schnittgeraden). Welche dieser Möglichkeiten zutrifft, lässt sich am Rang der Matrix  $A$  ablesen: In den ersten beiden Fällen hat  $A$  den Rang 1, im dritten Fall ist der Rang 2. Im Fall  $m = 3$  sieht es ähnlich aus: Eine Matrix  $A$  vom Rang 3 gehört zu drei Ebenen, deren Durchschnitt ein einzelner Punkt ist. Bei kleinerem Rang liegt eine von mehreren möglichen „degenerierten“ Situationen vor (wo zwei der Ebenen gleich oder parallel sind oder der Schnitt zweier Ebenen parallel zur dritten Ebene ist).

Sei  $e_1 = (1, 0, 0)$ ,  $e_2 = (0, 1, 0)$ ,  $e_3 = (0, 0, 1)$  die Standardbasis des Vektorraums  $\mathbb{R}^3$ . Eine lineare Abbildung  $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$  ist durch die Bilder  $a_i = f(e_i)$  der Basisvektoren eindeutig bestimmt. Jedem Vektor  $x \in \mathbb{R}^3$  wird der Vektor  $f(x) = Ax \in \mathbb{R}^3$  zugeordnet, wobei  $A$  eine  $3 \times 3$  Matrix mit Spalten  $a_1, a_2, a_3$  ist. (Genauer und mit der üblichen Terminologie ausgedrückt gehört die Matrix  $A$  zu der linearen Abbildung  $f$  bezüglich der Basen  $(e_1, e_2, e_3)$  und  $(e_1, e_2, e_3)$ .) Die Abbildung  $f$  überführt dann den Einheitswürfel in das Parallelepiped, das von den Vektoren  $a_1, a_2, a_3$  erzeugt wird:



Der Wert der Determinante  $\det A$  ist dem Betrage nach genau das Volumen dieses Parallelepipeds. Ein Spezialfall ist, dass für  $\det A = 0$ , also wenn  $A$  Rang  $r(A) \leq 2$  hat, alle Vektoren  $a_1, a_2, a_3$  in einer gemeinsamen Ebene liegen. In diesem Fall erhalten wir also (an Stelle eines „richtigen“ Parallelepipeds) ein „flach gedrücktes“ mit Volumen 0. Allgemeiner: Ist  $K \subset \mathbb{R}^3$  eine Menge vom Volumen  $v$ , dann hat die Menge  $f(K)$  das Volumen  $v|\det A|$ . In höheren Dimensionen hat der Betrag der Determinante analoge Bedeutung. Sogar das Vorzeichen der Determinante besitzt eine natürliche geometrische Bedeutung: Für ein Tripel  $a_1, a_2, a_3$  zeigt es die „Orientierung“ des Tripels an. Ein Beispiel für ein Tripel mit positiver Orientierung ist  $(e_1, e_2, e_3)$ , während das Tripel  $(e_1, e_2, -e_3)$  negativ orientiert ist.

# Literatur

---

## Deutsche Lehrbücher

- [1] M. Aigner: *Diskrete Mathematik*, Vieweg Verlag, Braunschweig etc., 1993.
- [2] R. Diestel: *Graphentheorie*, 3. Auflage, Graduate Texts in Mathematics 173, Springer-Verlag, Berlin etc., 2006.

## Englische Lehrbücher

- [3] N. Biggs: *Discrete Mathematics*, Revised edition, Clarendon Press, Oxford, 1989.
- [4] B. Bollobás: *Graph Theory. An Introductory Course*, corrected 3rd printing, Graduate Texts in Mathematics 63, Springer-Verlag, Berlin etc., 1990.
- [5] P. Cameron: *Combinatorics: Topics, Techniques, Algorithms*, Cambridge University Press, Cambridge, 1994.
- [6] P. Flajolet, R. Sedgewick: *Analytic Combinatorics*, to appear; a preliminary version was available on the web page of P. Flajolet in summer 2006.
- [7] R. Graham, D. Knuth und O. Patashnik: *Concrete Mathematics: A Foundation for Computer Science*, Addison-Wesley, Reading, Massachusetts, 1989.
- [8] J. H. van Lint und R. M. Wilson: *A Course in Combinatorics*, Cambridge University Press, Cambridge, 1992.
- [9] L. Lovász: *Combinatorial Problems and Exercises*, 2. Auflage, Akadémiai Kiadó, Budapest und North-Holland, Amsterdam, 1993.
- [10] I. Stewart and D. Tall: *The Foundations of Mathematics*, Oxford University Press, Oxford, 1977.

## Weiterführende Literatur

- [11] S. Arora und B. Barak: *Complexity Theory: A Modern Approach*, Vorabversion im Web (September 2006), soll 2007 erscheinen.

- [12] A. Aho, J. Hopcroft und J. Ullman: *The Design and Analysis of Computer Algorithms*, Addison-Wesley, Reading, Massachusetts, 1983.
- [13] N. Alon und J. Spencer: *The Probabilistic Method*, 2. Auflage, John Wiley, New York, 2000.
- [14] L. Babai und P. Frankl: *Linear algebra methods in combinatorics* (Preliminary version 2), Department of Computer Science, The University of Chicago, 1992.
- [15] E. R. Berlekamp, J. H. Conway und R. K. Guy: *Winning Ways for Your Mathematical Plays*. Vol. 1: Games in general. Vol. 2: Games in particular. Academic Press, London, 1982. Deutsche Übersetzung *Gewinnen*, 4 Bände. Vieweg Verlag, Braunschweig etc., 1985/86.
- [16] N. Biggs: *Algebraic Graph Theory*, 2nd edition, Cambridge University Press, Cambridge, 1993.
- [17] J. M. Borwein und P. B. Borwein: *Pi and the AGM*, John Wiley, New York, 1987.
- [18] G. Bredon: *Topology and Geometry*, Graduate Texts in Mathematics 139, Springer-Verlag, Berlin etc., 1993.
- [19] D. Cox, J. Little und D. O'Shea: *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*, 2nd edition, Springer-Verlag, Berlin etc., 1996.
- [20] T. Gowers: Mathematics. A Very Short Introduction, Oxford University Press, Oxford 2002.
- [21] G. R. Grimmett und D. R. Stirzaker: *Probability and Random Processes*, 2nd edition, Oxford University Press, Oxford, 1992.
- [22] F. Harary und E. M. Palmer: *Graphical Enumeration*, Academic Press, New York und London, 1973.
- [23] N. Koblitz: *A Course in Number Theory and Cryptography*, 2nd edition, Graduate Texts in Mathematics 114, Springer-Verlag, Berlin etc., 1994.
- [24] Krengel: *Einführung in die Wahrscheinlichkeitstheorie und Statistik*, Vieweg Verlag, Braunschweig etc., 1988.
- [25] J. Littlewood: *A Mathematician's Miscellany*, London, Methuen, 1953.
- [26] B. Mohar und C. Thomassen: *Graphs on Surfaces*, Johns Hopkins University Press, Baltimore, Maryland, 1997.

- [27] R. Motwani und P. Raghavan: *Randomized Algorithms*, Cambridge University Press, New York, 1995.
- [28] J. G. Oxley: *Matroid Theory*, Oxford University Press, Oxford, 1992.
- [29] J. Pach und P. K. Agarwal: *Combinatorial Geometry*, John Wiley, New York, 1995.
- [30] A. de Saint-Exupéry: *Le petit prince*, Deutsche Übersetzung *Der kleine Prinz*, Rauch Verlag, Düsseldorf, 2000.
- [31] J. Stillwell: *Classical Topology and Combinatorial Group Theory*, Graduate Texts in Mathematics 72, Springer-Verlag, Berlin etc., 1980.
- [32] W. T. Trotter: *Combinatorics and Partially Ordered Sets: Dimension Theory*, Johns Hopkins Series in the Mathematical Sciences, Johns Hopkins University Press, Baltimore, Maryland, 1992.
- [33] G. Ziegler: *Lectures on Polytopes*, Revised ed., Graduate Texts in Mathematics 152, Springer-Verlag, Berlin etc., 1998.

## Weitere Referenzen

- [34] G. E. Andrews: *The Theory of Partitions* (Encyclopedia of mathematics and its applications, vol. 2), Addison-Wesley, Reading, Massachusetts, 1976.
- [35] D. Bayer und P. Diaconis: Trailing the dovetail shuffle to its lair, *Annals of Applied Probability* 2(1992), No. 2, 294–313.
- [36] Th. Beth, D. Jungnickel und H. Lenz: *Design Theory*, B.I. Wissenschaft Verlag, Mannheim, Wien, Zürich, 1985.
- [37] A. Beutelspacher, B. Petri: *Der goldene Schnitt*, BI Wissenschaftsverlag, Mannheim etc., 1989.
- [38] K. Chandrasekhar: *Introduction to Analytic Number Theory*, Springer-Verlag, Berlin etc., 1968.
- [39] P. Flajolet, B. Salvy und P. Zimmerman: Automatic average-case analysis of algorithms, *Theoretical Computer Science* 79(1991), 37–109.
- [40] G. Gonthier: A computer-checked proof of the Four Color Theorem, Technical Report, Microsoft Research, Cambridge, United Kingdom.
- [41] R. L. Graham, M. Grötschel und L. Lovász (editors): *Handbook of Combinatorics*, Vol. 1–2, North-Holland, Amsterdam, 1995.

- [42] G. Kant: Drawing planar graphs using the canonical ordering, *Algorithmica* 16(1996), 4–32.
- [43] D. Karger, P. Klein und R. Tarjan: A randomized linear-time algorithm to find minimum spanning trees, *Journal of the ACM* 42(1995) 321–328.
- [44] D. Knuth: *The Art of Computer Programming*, Vol. I: Fundamental Algorithms, Addison-Wesley, Reading, Massachusetts, 1968.
- [45] S. Rajagopalan and L. J. Schulman: Verification of identities, *SIAM J. Computing* 29,4(2000) 1155–1163.
- [46] N. Robertson, D. P. Sanders, P. D. Seymour und R. Thomas: The Four Color Theorem, *Journal of Combinatorial Theory Ser. B* 70(1997), 2–44.
- [47] N. Robertson, P. D. Seymour und R. Thomas: Permanents, Pfaffian orientations, and even directed circuits, *Ann. Math.* 150(1999), 929–975.
- [48] M. Sharir und P. K. Agarwal: *Davenport-Schinzel Sequences and Their Geometric Applications*, Cambridge University Press, Cambridge, 1995.
- [49] I. Stewart: Mathematical recreations, *Scientific American* 272(1995), No. 1, 76–79.
- [50] C. Thomassen: The Jordan-Schoenflies theorem and the classification of surfaces, *American Mathematical Monthly* 99(1992), No. 2, 116–130.



“Modul X” (drawing by Jiří Načeradský and Jaroslav Nešetřil).

# Hinweise zu ausgewählten Übungen

---

**1.2.2.** Nennen wir die rechte Seite  $m$ . Dann ist  $m$  die eindeutige Zahl mit  $m^2 \leq \lfloor x \rfloor < (m+1)^2$ . Das ist aber gleichbedeutend mit  $m^2 \leq x < (m+1)^2$ , und daher ist  $m = \lfloor \sqrt{x} \rfloor$ .

**1.2.3(d).** Siehe Abschnitt 12.4, Übung 4.

**1.2.7.** Schreiben Sie alle Zahlen in der Form  $2^k(2m+1)$ , mit ganzen Zahlen  $k, m \geq 0$ . Weil  $m$  höchstens 500 verschiedene Werte annehmen kann, muss die betrachtete Menge zwei Zahlen der Form  $2^k(2m+1)$  und  $2^{k'}(2m+1)$ ,  $k < k'$ , enthalten.

**1.3.3(a).** Fügt man zu  $n$  schon gezeichneten eine weitere hinzu, so zerteilt diese genau  $n+1$  der schon vorhandenen Regionen.

**1.3.3(b).** Benutzen Sie (a) im Induktionsschritt. Das Ergebnis ist  $(n^3 + 5n + 6)/6$ .

**1.3.5.** Zeigen Sie, dass der Zähler in jedem Schritt kleiner wird.

**1.3.6.** Zerteilen Sie das Schachbrett in vier  $2^{n-1} \times 2^{n-1}$ -Teile und platzieren Sie einen Stein so, dass er auf allen Teilen liegt, nur nicht auf dem mit dem fehlenden Feld.

**1.3.7(b).** Die Strategie ist, immer den letzten Zug des ersten Spielers umgekehrt nachzumachen. Dass diese Strategie funktioniert, lässt sich indirekt (mit Widerspruch) beweisen (wenn sich ein  $n$ -Block durch einen Zug des zweiten Spielers wiederholt, dann finden Sie eine frühere Wiederholung eines anderen  $n$ -Blockes).

**1.3.8.** Induktion nach  $n$ . Sei  $S$  die am weitesten links gelegene Spalte, die anfangs ein schwarzes Kästchen enthält, und  $Z$  die unterste solche Zeile. Nach Induktionsvoraussetzung sind nach dem Zeitpunkt  $n-1$  alle Kästchen oberhalb von  $Z$  und rechts von  $S$  weiß. Es kann höchstens noch das eine Kästchen, das in Zeile  $Z$  und Spalte  $S$  liegt, schwarz sein, doch das wird im nächsten Schritt weiß.

**1.3.9.** Die Antwort ist 4. Beschreiben Sie mit Induktion über  $m$  die Verteilung der Teilchen zum Zeitpunkt  $2^m - 1$ . (Das Minus ist kein Druckfehler!)

**1.3.10.** Definieren Sie  $x_1 = \min(M)$ ,  $x_{i+1} = \min(M \setminus \{x_1, \dots, x_i\})$ . Wäre  $M$  unendlich, dann hätte die Menge  $\{x_1, x_2, \dots\}$  kein größtes Element.

**1.3.12.** Nehmen Sie an, die  $n_i$  sind der Größe nach geordnet:  $1 < n_i \leq n_j$ . Dann könnten Sie damit beginnen zu zeigen, dass die Summe der Quadrate auf keinen Fall kleiner wird, wenn Sie  $n_i$  durch  $n_i - 1$  und  $n_j$  durch  $n_j + 1$  ersetzen. Zeigen Sie dann, dass Sie jede beliebige Ausgangssituation auf die in dem unvollständigen Beweis beschriebene Extremsituation zurückführen können.

**1.3.13.** Eine Möglichkeit ist, Induktion nach  $n$  zu führen. Nehmen Sie an, die Behauptung ist richtig für alle  $n < n_0$  und betrachten Sie ein  $M$  zu  $n = n_0$ . Betrachten Sie  $M' = M \setminus \{[1, n]\}$  (wenn  $[1, n]$  nicht in  $M$  enthalten ist, ist  $M = M'$ ). Nun sind zwei Fälle zu unterscheiden: Wenn kein Intervall von  $M'$  die 1 enthält, dann ist nach Induktionsvoraussetzung  $|M'| \leq n - 2$ . Andernfalls sei  $q < n_0$  die größte Zahl, so dass  $[1, q] \in M'$  ist. Wenden Sie nun die Induktionsvoraussetzung auf  $M_1 = \{I \in M': I \subseteq [1, q]\}$  und  $M_2 = M' \setminus M_1$  an.

**1.3.14.**  $k\lfloor n/2 \rfloor$ . Benutzen Sie im Beweis, dass  $m \leq k\lfloor n/2 \rfloor$  ist, die Tatsache, dass jedes  $I_j$  mindestens eine gerade Zahl enthält.

**1.4.7(c).** Es genügt zu zeigen, dass es keine Bijektion von der Menge  $\{1, 2, \dots, n\}$  in eine echte Teilmenge  $A \subset \{1, 2, \dots, n\}$  gibt. Führen Sie Induktion nach  $n$ . Der Induktionsanfang ( $n = 1$ ) ist klar. Nehmen Sie an, es gäbe so eine Bijektion  $f: \{1, 2, \dots, n\} \rightarrow A$ ,  $n > 1$ . Wenn  $f(n) = n$  ist oder  $n \notin A$ , dann ist die Einschränkung von  $f$  auf  $\{1, 2, \dots, n-1\}$  eine Bijektion von  $\{1, 2, \dots, n-1\}$  in eine echte Teilmenge. Wenn  $f(n) = i \neq n$  ist, dann gibt es ein  $j < n$  mit  $f(j) = n$ ; definieren Sie  $g(j) = i$ ,  $g(k) = f(k)$  für  $k \neq j, n$ . Diese Funktion  $g$  ist eine Bijektion von  $\{1, 2, \dots, n-1\}$  in eine echte Teilmenge.

**1.5.3(a).** Es gibt nur endlich viele Relationen auf  $X$ .

**1.5.3(c).** Versuchen Sie es mit  $(\mathbb{N}, <)$ .

**1.5.4(b).** Die Paare, die bezüglich  $R \circ S$  in Relation stehen, entsprechen denjenigen Einträgen in der Matrix  $A_R A_S$ , die nicht Null sind.

**1.6.9(b).** Wenn die Kongruenzrelation  $\sim$  nicht die Gleichheitsrelation ist, setzen Sie  $q = \min\{|x - y|: x \neq y, x \sim y\}$ . Beweisen Sie, dass  $\equiv_q$  und  $\sim$  die gleichen Relationen sind.

**1.6.9(c).** Ja für (a), nein für (b) (Sehen Sie einfach alle geraden Zahlen als äquivalent an, während die ungeraden Zahlen immer nur zu sich selbst äquivalent sind, dann haben Sie ein Gegenbeispiel).

**2.1.2.** Definieren Sie die Relation  $S = \{(x, x): x \in X\} \cup R \cup R \circ R \cup R \circ R \circ R \cup \dots$  und zeigen Sie, dass diese eine Ordnung ist.

**2.1.3.** Auf der Menge aller rationalen Zahlen mit der gewohnten Ordnung ist die Relation „unmittelbarer Vorgänger“ leer.

**2.1.4(b).** Eine endliche linear geordnete Menge hat ein (einziges) größtes Element. Wenn es einen Isomorphismus gibt, muss er das größte Element der einen Menge auf das der anderen abbilden. Und nun Induktion!

**2.1.4(c).** Z.B. die gewohnte Ordnung und die umgekehrte Ordnung ( $1 \succ 2 \succ 3 \succ \dots$ ).

**2.1.4(d).** Überabzählbar viele: Partitionieren Sie  $\mathbb{N}$  in unendliche Teilmengen  $S_1, S_2, \dots$  und hängen Sie alle diese Mengen aneinander (so dass alle Elemente aus  $S_1$  kleiner sind als alle aus  $S_2$ , die wiederum kleiner sind als alle aus  $S_3, \dots$ ); jedes  $S_i$  kann wie die natürliche Ordnung von  $\mathbb{N}$  geordnet werden oder wie die umgekehrte (oder auch noch ganz anders).

**2.2.9(d).** Zeigen Sie, dass für jedes  $A \subseteq X$  gilt:  $\inf A = \sup\{x \in X : x \leq a \text{ for all } a \in A\}$ .

**2.4.7.** Induktion nach  $|X|$ . Sei  $x$  ein minimales Element, und sei  $y$  minimal unter den Elementen, für die  $x \prec y$  (wenn es kein solches  $y$  gibt, dann ist  $X$  eine Antikette). Sei  $A$  eine maximal große Antikette in  $X \setminus \{x, y\}$ . Ist  $|A| < \alpha$ , verwenden wir die Induktionsannahme. Andernfalls zerlegen wir die Mengen  $\{t \in X : \exists a \in A t \leq a\}$  und  $\{t \in X : \exists a \in A t \geq a\}$  jeweils in  $\alpha$  Ketten, die wir bei den Elementen aus  $A$  zusammenfügen.

**3.1.2.** Codieren Sie ein Paar  $(A, B)$  als eine Abbildung  $f : \{1, 2, \dots, n\} \rightarrow \{0, 1, 2\}$ : ein Element  $x \in A$  erhält den Funktionswert 2,  $x \in B \setminus A$  den Wert 1 und  $x \notin B$  den Wert 0.

**3.1.5(b).** Wählen Sie als erste Spalte irgendeinen Vektor aus dem Körper mit  $q$  Elementen (außer dem Nullvektor). Die zweite Spalte darf kein Vielfaches der ersten sein, damit sind  $q$  Vektoren verboten. Die dritte Spalte darf keine Linearkombination der beiden ersten sein, damit sind  $q^2$  Vektoren verboten (keine zwei verschiedenen Linearkombinationen der beiden ersten Spalten ergeben den gleichen Vektor — prüfen Sie es nach!). Allgemein gibt es  $q^n - q^i$  Möglichkeiten für die  $i$ -te Spalte.

**3.1.6.** Bilden Sie aus allen Teilern Paare, zu  $d$  gehört  $n/d$ . Wenn  $n$  keine Quadratzahl ist, dann „geht es auf“.

**3.2.1.**  $(n - 1)!$ .

**3.2.3(b).** Was ist die Ordnung einer Permutation mit einem einzigen Zyklus der Länge  $k$ ? Wie sieht es aus, wenn die Permutation zwei Zyklen der Längen  $k_1$  und  $k_2$  hat?

**3.2.5(a).** Schreibt man eine Permutation mit  $k$  aufsteigenden Segmenten rückwärts, dann erhält man eine Permutation mit  $n + 1 - k$  aufsteigenden Segmenten.

**3.2.5(b).** Betrachten Sie eine Permutation der Menge  $\{1, 2, \dots, n - 1\}$ , die (in einzeiliger Schreibweise)  $k$  Segmente hat, und fügen Sie die Zahl  $n$  an einer der  $n + 1$  möglichen Positionen ein. Für wie viele der Positionen hat die daraus resultierende Permutation  $k + 1$  Segmente, und für wie viele Positionen hat sie  $k$  Segmente?

**3.2.5(c).** Euler hat die Formel  $f(n, k) = \sum_{j=0}^k (-1)^j \cdot (k - j)^n \binom{n+1}{j}$  hergeleitet.

**3.2.5(d).** Teilen Sie die Permutationen in Klassen ein, und zwar nach der Menge  $\{\pi(1), \pi(2), \dots, \pi(k + 1)\}$  der Zahlen, die auf den ersten  $k + 1$

Positionen stehen. Alle Ordnungen dieser  $k + 1$  Zahlen haben die gleiche Wahrscheinlichkeit. Für wie viele der  $(k + 1)!$  möglichen Ordnungen der ersten  $k + 1$  Zahlen hat das erste aufsteigende Segment die Länge  $k$ ? Es ergibt sich die Wahrscheinlichkeit  $k/(k + 1)!$ .

**3.2.6(c).** Stellen Sie sich die Zahlen zu jedem Zeitpunkt gemäß einer Permutation  $\pi$  angeordnet vor; der Austausch zweier benachbarter Zahlen vermindert die Anzahl der Inversionen höchstens um 1.

**3.2.7(b).** Wie viele der Zahlen  $1, 2, \dots, n$  sind durch  $p^j$  teilbar ( $j = 1, 2, \dots$ )? Die gesuchte Formel ist  $\lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \dots$ .

**3.3.3(b).** Auf der rechten Seite steht die Anzahl der  $(r + 2)$ -Tupel nicht negativer ganzer Zahlen mit  $X_1 + X_2 + \dots + X_{r+2} = n - r$ . Teilen Sie diese  $(r + 2)$ -Tupel in  $n - r + 1$  Gruppen ein, und zwar abhängig vom Wert von  $X_{r+2}$ , und berechnen Sie die Anzahl der Lösungen für jede der Gruppen einzeln. Sie erhalten so die linke Seite.

**3.3.4.** Schreiben Sie den  $k$ -ten Term als  $\binom{n}{m} \binom{n-m}{n-k}$  und klammern Sie  $\binom{n}{m}$  aus der Summe aus. Das Ergebnis ist  $\binom{n}{m} 2^{n-m}$ .

**3.3.5(a).** Verwenden Sie  $\frac{1}{k} \binom{k}{m} = \frac{1}{m} \binom{k-1}{m-1}$  und Formel (3.7).

**3.3.5(b).**  $k \binom{k}{m} = (k + 1) \binom{k}{m} - \binom{k}{m} = (m + 1) \binom{k+1}{m+1} - \binom{k}{m}$ .

**3.3.6.** Sei  $M$  eine  $m$ -Menge und  $N$  eine  $n$ -Menge. Beide Seiten zählen die geordneten Paare  $(X, Y)$  mit  $X \subseteq M$ ,  $Y \subseteq N \cup X$  und  $|Y| = m$ : Auf der linken Seite wählen wir zuerst  $X$  und dann  $Y$ , auf der rechten Seite wählen wir erst  $Y \cap N$ , dann  $Y \cap M$ , und schließlich  $X$ .

**3.3.7.** Setzen Sie  $k_i = f(i + 1) - f(i)$ ,  $k_0 = f(1) - 1$ ,  $k_n = n - f(n)$ . Die gesuchte Zahl ist die Anzahl nicht negativer ganzzahliger Lösungen der Gleichung  $k_0 + k_1 + \dots + k_n = n$ .

**3.3.9.** Sei  $\{a_1, \dots, a_k\}$  so eine Teilmenge,  $a_1 < a_2 < \dots < a_k$ . Ordnen Sie dieser Teilmenge das  $k$ -Tupel  $\{a_1, a_2 - 1, a_3 - 2, \dots, a_k - k + 1\}$  zu. Dies ist eine Bijektion zwischen den beschriebenen Teilmengen und  $\binom{\{1, 2, \dots, n-k+1\}}{k}$ .

**3.3.10(b).** Das Ergebnis ist  $\binom{n+1}{2}^2$ .

**3.3.10(c).** Berechnen Sie den Flächeninhalt des großen Quadrats auf zwei Arten. Die Seitenlänge ist  $2(1 + 2 + 3 + \dots + n)$ , die  $k$ -te „Schicht“ (von der Mitte aus gezählt) enthält  $4k$  Quadrate der Größe  $k \times k$ .

**3.3.15(b).** In Formel (3.1) für den Binomialkoeffizienten ist genau einer der Faktoren im Zähler durch  $p$  teilbar. Also ist  $\binom{n}{p}$  genau dann durch  $p$  teilbar, wenn dieser Faktor auch durch  $p^2$  teilbar ist.

**3.3.16(a).** Setzen Sie die folgenden Werte in den Binomialsatz ein:  $x = 1$ ,  $x = -1$ ,  $x = i$ , und  $x = -i$  ( $i = \sqrt{-1}$  steht für die imaginäre Einheit). Addieren Sie die so erhaltenen Gleichungen. Schreiben Sie die  $n$ -ten Potenzen auf der rechten Seite mit Hilfe der Formel von de Moivre um. Die gesuchte Zahl ist durch den Ausdruck  $2^{n-2} + 2^{n/2-1} \cos \frac{\pi n}{4}$  gegeben. Überzeugen Sie sich von der Korrektheit, indem Sie ein paar kleine Werte für  $n$  einsetzen.

**3.3.16(b).** Gehen Sie vor wie in (a), aber setzen Sie diesmal die drei (komplexen) Nullstellen der Gleichung  $x^3 = 1$  für  $x$  ein.

**3.3.19.** Wenn sich zuerst die Elfen in eine Reihe stellen, dann gibt es acht mögliche Positionen für die Kobolde. Wählen Sie fünf davon aus und platzieren Sie die Kobolde.

**3.3.23.** Die mit  $A_1: \binom{n-k-1}{k-1}$ . Alle: diese Zahl mal  $\frac{n}{k}$ .

**3.3.24(b).** Zeigen Sie, dass es immer genau zwei Dreiecke gibt, die zwei Seiten mit dem  $n$ -Eck gemein haben. Wenn wir von einem Dreieck  $T_0$  ausgehen, das zwei Seiten mit dem  $n$ -Eck gemeinsam hat, können wir ein angrenzendes Dreieck  $T_1$  wählen, dann ein Dreieck  $T_2$ , das an  $T_1$  grenzt, usw. Für  $T_0$  haben wir  $n$  Möglichkeiten und in jedem der folgenden Schritte gibt es zwei Möglichkeiten. Jede Triangulierung kann man mit diesem Prozess auf zwei verschiedene Arten finden, weil es zwei Dreiecke gibt, die als  $t_0$  in Frage kommen. Das Ergebnis ist  $n2^{n-5}$ .

**3.3.26(a).** Die linke Seite zählt die verschiedenen Anordnungen von  $n$  Objekten, wenn es  $k_i$  Objekte der  $i$ -ten Sorte gibt. Auf der rechten Seite wählen Sie zuerst die Sorte Objekt für die erste Position und dann arranieren Sie die übrigen Objekte.

**3.3.27(a).**  $\binom{r_1+r_2+\dots+r_k}{r_1, r_2, \dots, r_k}$ .

**3.3.27(b).**  $(n-1)!/\prod_{i=1}^k (r_i + 1)$ , wobei  $n = |X| = 1 + \sum_{i=1}^k (r_i + 1)$ .

**3.4.2.** Zum Beispiel  $f(n) = n^{\lfloor n/2 \rfloor}$ ,  $g(n) = n^{\lfloor (n+1)/2 \rfloor - 1/2}$ .

**3.4.4.**  $|f|$  ist durch eine Konstante beschränkt,  $|g|$  ist nach unten durch eine Konstante beschränkt,  $|h|$  ist durch eine Polynomfunktion beschränkt.

**3.4.5.** Bringen Sie zuerst alle Funktionen in die Gestalt  $e^{f(n)}$ .

**3.5.2(b).** Ansatz:  $1 + \frac{1}{n} = \frac{n+1}{n} = 1/(1 - \frac{1}{n+1}) \geq 1/e^{-1/(n+1)}$ .

**3.5.3.** Die Gerade  $y = x + 1$  ist Tangente am Funktionsgraphen von  $e^x$  im Punkt  $(0, 1)$ . Die Funktion  $e^x$  ist konvex (die zweite Ableitung ist nirgends negativ), und deshalb kann sie keine Tangente ein zweites Mal treffen.

**3.5.7(b).** Setzen Sie  $A = (x_1 + x_2 + \dots + x_{n-1})/(n-1)$ . Wenn Sie  $AG(n)$  auf die Zahlen  $x_1, \dots, x_{n-1}$  und  $A$  anwenden, erhalten Sie  $A^n = ((x_1 + x_2 + \dots + x_{n-1} + A)/n)^n \geq x_1 x_2 \dots x_{n-1} A$  und daraus  $A \geq (x_1 \dots x_{n-1})^{1/(n-1)}$ .

**3.5.10.** Die Funktion  $\ln x$  ist konkav, und deshalb liegt jedes Dreieck mit Eckpunkten  $(i, \ln i)$ ,  $(i+1, \ln i)$ , und  $(i+1, \ln(i+1))$  vollständig unter dem Funktionsgraphen (Sie sollten sich eine Skizze zeichnen). Der Flächeninhalt eines solchen Dreiecks ist  $\frac{1}{2}(\ln(i+1) - \ln i)$ . Also ist  $\ln n! \leq \ln n + \int_1^n \ln x \, dx - \frac{1}{2} \sum_{i=1}^{n-1} (\ln(i+1) - \ln i)$ . Noch eine weitere Umformung, und Sie sind fertig.

**3.5.11.** Induktion über  $n$ .

**3.5.12.** Untere Schranke: Induktion; zeigen Sie  $2(\sqrt{n+1} - \sqrt{n}) \leq 1/\sqrt{n}$ , indem Sie die linke Seite in einen Bruch mit Nenner  $\sqrt{n+1} + \sqrt{n}$  umformen. Die obere Schranke können Sie ähnlich herleiten.

**3.6.2(a).** Alle diese Primzahlen teilen  $\binom{2m}{m}$ .

**3.6.2(b).** Wenn  $P$  das Produkt der Primzahlen aus (a) ist, dann ist  $\log_2 P \leq 2m$ , und andererseits ist  $P \geq m^{\pi(2m) - \pi(m)}$ . Daraus folgt  $\pi(2m) \leq \pi(m) + O(m/\ln m)$ .

**3.6.2(c).** Die größte Potenz von  $p$ , die  $n!$  teilt, hat den Exponenten  $\lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \dots$ . Gehen Sie von der Gleichung  $\binom{2m}{m} = (2m)!/(m!)^2$  aus und finden Sie einen Ausdruck für die Differenz der höchsten Potenzen von  $p$  in Zähler und Nenner.

**3.6.2(d).** Aus (c) folgt  $2^{2n}/(n+1) \leq \binom{2n}{n} \leq (2n)^{\pi(2n)}$ .

**3.7.2.** Man kann z.B. so vorgehen, wie im zweiten Beweis des Prinzips der Inklusion–Exklusion, nämlich den Beitrag eines Elements  $x$  auf beiden Seiten untersuchen.

**3.8.2(b).** Wählen Sie zuerst die  $k$  Fixpunkte aus. Der Rest ist eine Permutation ohne Fixpunkte, wie in dem Garderobenproblem.

**3.8.4.** Klassifizieren Sie alle Permutationen nach der Anzahl ihrer Fixpunkte. Drücken Sie die Anzahl der Permutationen eines Typs mit Hilfe der Funktion  $D(k)$  aus.

**3.8.5(a).** Betrachten Sie eine fixpunktfreie Verteilung der Hüte auf die  $n$  Herren. Herr Nr. 1 tauscht den Hut, den er fälschlicherweise bekommen hat, gegen seinen eigenen, sagen wir mit Herrn Nr.  $i$ . Dann geht er. Wenn Herr Nr.  $i$  nach diesem Tausch auch seinen eigenen Hut hat, dann geht er auch und wir haben eine Situation mit  $n-2$  Herren. Sonst sind noch  $n-1$  Herren da.

**3.8.7(c).** Angenommen, die Abbildung geht in die Menge  $\{1, 2, \dots, m\}$ . Sei  $A_i$  die Menge der Abbildungen, die kein Element auf  $i$  abbilden. Bestimmen Sie mit Inklusion–Exklusion  $|A_1 \cup \dots \cup A_m|$ , die Anzahl der „bösen“ Abbildungen. Für  $m = n$  muss  $n!$  herauskommen.

**3.8.7(d).** Eine surjektive Abbildung  $f: N \rightarrow M$  (mit  $|M| = m$ ) definiert eine Äquivalenzrelation mit  $m$  Äquivalenzklassen auf  $N$ . Zeigen Sie, dass jede Äquivalenzrelation auf  $N$  mit  $m$  Klassen zu genau  $m!$  surjektiven Abbildungen korrespondiert.

**3.8.8(a).** Sie können den Hinweis zu (d) und das Ergebnis aus (c) in der vorigen Aufgabe verwenden.

**3.8.8(b).** Addieren Sie das Ergebnis aus (a) über alle  $k$ . Sie erhalten das folgende Ergebnis:  $\sum_{k=0}^n \frac{1}{k!} \sum_{j=0}^k (-1)^j \binom{k}{j} (k-j)^n$ .

**3.8.8(c).** Schreiben Sie  $i$  für  $k-j$  im Ergebnis aus (b), lassen Sie  $k$  formal bis  $\infty$  laufen (das ist zulässig, weil die innere Summe, die die Anzahl der Äquivalenzrelationen mit  $k$  Klassen auf einer  $n$ -Menge ausdrückt, 0 ist für  $k > n$ ) und sortieren Sie die Summanden um.

**3.8.11(b).** Schreiben Sie jeden Faktor in dem Produkt in der Form  $1 + p_i + p_i^2 + \cdots + p_i^{\alpha_i}$ .

**3.8.11(c).** Sei  $n = 2^q \prod_{i=1}^r p_i^{\alpha_i}$ , die  $p_i$  ungerade Primzahlen. Nach (b) muss  $2n = t \prod (p_i^{\alpha_i} + p_i^{\alpha_i-1} + \cdots + 1)$  sein,  $t = 2^{q+1} - 1$ . Wenn Sie diesen Ausdruck durch  $t \prod p_i^{\alpha_i}$  teilen, erhalten Sie  $1 + 1/t = \prod (1 + 1/p_i + \cdots + 1/p_i^{\alpha_i})$ . Nun wird  $t$  aber von einem  $p_i$  geteilt. Damit die rechte Seite der Gleichung nicht größer wird als die linke, muss  $r = 1$  sein und  $t = p_1$ .

**3.8.12.** Für jede Primzahl  $p_i \leq N$  sei  $A_i$  die Menge der Paare  $(m, n)$ , so dass  $p_i | n$  und  $p_i | m$ . Mit Inklusion–Exklusion können Sie nun die Anzahl „böser“ Paare bestimmen.

**3.8.13(a).** Definieren Sie  $A_i$  als die Menge aller Graphen, in denen Ecke  $i$  Grad 0 hat, und berechnen Sie  $|A_1 \cup \cdots \cup A_n|$ .

**3.8.14.** Definieren Sie  $A_i$  als die Menge aller Anordnungen, in denen Paar  $i$  nebeneinander sitzt.

**4.1.5(b).** Ein einfaches Gegenbeispiel ist das folgende: Nehmen Sie zwei Dreiecke mit Eckenmengen  $\{1, 2, 3\}$  und  $\{4, 5, 6\}$  und fügen Sie die Kanten  $\{1, 4\}$ ,  $\{2, 5\}$  und  $\{3, 6\}$  hinzu.

**4.1.6.**  $(2n - 1)(2n - 3)(2n - 5) \cdots \cdot 5 \cdot 3$ .

**4.1.8.** Hier ist eine Methode,  $2^{n^2/2 - O(n \log n)}$  nicht isomorphe Graphen zu konstruieren (das sind beinahe so viele, wie wir mit dem Zählarumentum im Text gefunden haben). Sei  $n$  groß genug und sei  $m$  die kleinste ganze Zahl mit  $2^m \geq n$ . Wir bezeichnen die  $n$  Ecken mit  $a, b, c, d, u_0, u_1, \dots, u_{m-1}$  und  $v_0, v_1, \dots, v_{n-m-5}$ ; wir schreiben  $U = \{u_0, \dots, u_{m-1}\}$ ,  $V = \{v_0, \dots, v_{n-m-5}\}$ . Verbinden Sie  $a$  mit  $b$ ,  $b$  mit  $c$ , mit  $d$  und mit allen Ecken aus  $U$ . Wählen Sie einen asymmetrischen Graphen auf  $U$ , etwa den Weg  $u_0, u_1, \dots, u_{m-1}$  plus die Kante  $\{u_1, u_3\}$ . Verbinden Sie die Ecken  $c$  und  $d$  mit jeder Ecke aus  $V$  (so dass  $a$  die einzige Ecke vom Grad 1 ist). Wählen Sie einen beliebigen Graph auf  $V$ . Verbinden Sie schließlich jede Ecke  $v_i \in V$  mit den Ecken  $u_{j_1}, \dots, u_{j_k}$ , wobei  $0 \leq u_1 < u_2 < \cdots < u_k \leq m-1$  die (einzig bestimmen) Zahlen mit  $2^{j_1} + 2^{j_2} + \cdots + 2^{j_k} = i$  sind (dies entspricht der Binärschreibweise von  $i$ ). Es ist nicht schwer zu prüfen, dass man für verschiedene Graphen auf  $V$  nicht isomorphe Graphen auf  $n$  Ecken erhält. Damit haben wir mindestens  $2^{\binom{n-m-5}{2}}$  nicht isomorphe Graphen auf  $n$  Ecken.

**4.2.2.** In einem Graphen mit maximal vielen Kanten sind natürlich alle Komponenten vollständige Graphen. Sind die Eckenzahlen in den Komponenten  $n_1, \dots, n_k$ ,  $\sum n_i = k$ , dann haben wir  $\binom{n_1}{2} + \cdots + \binom{n_k}{2}$  Kanten, und wir wollen diesen Ausdruck als eine Funktion von  $n_1, \dots, n_k$  maximieren. Das geht am einfachsten mit folgendem Trick: Wenn  $n_1 \geq n_2 > 1$ , dann wird der Wert des Ausdrucks jedenfalls nicht kleiner, wenn wir  $n_1$  um 1 erhöhen und  $n_2$  um 1 erniedrigen. Das Maximum wird also angenommen, wenn  $n_1 = n - k + 1$  und  $n_i = 1$  für  $i = 2, 3, \dots, n$ .

**4.2.4.** Wenn  $G$  keinen ungeraden Kreis enthält, dann zeigen Sie, dass jede Komponente bipartit ist. Sie können also annehmen, dass  $G$  zusammenhängend ist. Weisen Sie den Ecken Werte  $+1$  und  $-1$  nach folgender Regel zu: Schreiben Sie an eine beliebige Ecke die Zahl  $+1$ , und immer, wenn eine Ecke  $v$  an eine Ecke anstößt, neben der die Zahl  $x$  steht, schreiben Sie an  $v$  die Zahl  $-x$ . Zeigen Sie, dass Sie auf diese Weise jeder Ecke des Graphen  $+1$  oder  $-1$  zuweisen und dass keine zwei Ecken mit dem selben Wert adjazent sind.

**4.2.5.** Ist  $v$  eine Ecke mit mindestens 2 Nachbarn, dann muss sie mit allen Ecken in ihrer Komponente verbunden sein. Jede Komponente muss  $K_3$  oder  $K_{1,n}$  sein.

**4.2.6.** Die Komponenten sind: beliebige zusammenhängende Graphen auf  $\leq 4$  Ecken, Sterne  $K_{1,n}$ , Sterne  $K_{1,n}$  mit einer extra Kante (die ein Dreieck erzeugt) oder zwei Sterne  $K_{1,n}$  und  $K_{1,m}$ , deren Zentren durch eine Kante verbunden sind. (Mit dem Zentrum eines Sterns meinen wir die Ecke, die mit allen anderen verbunden ist.)

**4.2.8.** Gewöhnlich definiert man den Durchmesser eines Graphen als  $\max\{d_G(u,v) : u, v \in V(G)\}$  und den Radius als  $\min_{v \in V(G)} \max_{u \in V(G)} d_G(u,v)$ .

**4.2.11.** Für eine gegebene Ecke  $v_i$  zählt der  $(i,i)$ -Diagonaleintrag in  $A_G^4$  die Spaziergänge der Länge 4, die in  $v_i$  beginnen und auch enden. Jeder 4-Kreis in  $G$  trägt acht solche Spaziergänge bei. Aber so ein Spaziergang kann auch viermal die gleiche Kante entlangführen (jede Kante trägt zwei solche Spaziergänge bei), oder zwei Kanten mit einer gemeinsamen Ecke zweimal (jedes Paar von Kanten mit einer gemeinsamen Ecke liefert Beitrag 4).

**4.3.1.** Eine Möglichkeit ist diese: Der erste Graph hat keinen Kreis der Länge 4, der zweite hat zwei solche Kreise und der dritte 5.

**4.3.8(a).** Das geht nicht. Die Gradfolge müsste  $(0, 1, \dots, n-1)$  sein, aber wenn es eine Ecke gibt, die zu allen anderen Ecken adjazent ist, dann kann keine Ecke Grad 0 haben.

**4.3.8(b).** Für alle  $n \geq 2$ . Konstruieren Sie induktiv Graphen  $G_n$ , deren Gradfolge die Zahlen  $0, 1, \dots, n-2$  enthält (mit  $\lfloor (n-1)/2 \rfloor$  wiederholt).  $G_2$  sind zwei isolierte Ecken,  $G_{n+1}$  entsteht aus dem Komplement von  $G_n$  durch Hinzufügen einer isolierten Ecke (das *Komplement* eines Graphen  $G = (V, E)$  ist der Graph  $(V, \binom{V}{2} \setminus E)$ ).

**4.3.10.** Betrachten Sie die Färbung mit der geringstmöglichen Anzahl “monochromatischer” Kanten (bei denen beide Enden die gleiche Farbe haben). Gäbe es einen monochromatischen Weg der Länge 2, dann könnte man die Farbe der mittleren Ecke wechseln.

**4.3.11.** Betrachten Sie in  $G$  einen Weg maximaler Länge. Eine Endstelle dieses Weges ist mit mindestens zwei anderen Ecken auf diesem Weg verbunden; so erhalten Sie den gewünschten Kreis.

**4.3.12.** Natürlich muss  $k \leq n - 1$  sein, und  $kn$  muss gerade sein. Diese Bedingung ist auch hinreichend; setzen Sie z.B.  $V = \{0, \dots, n - 1\}$ ,  $E = \{\{i, j\} : (i - j) \bmod n \in S\}$ , wobei  $S = \{1, -1, 2, -2, \dots, \frac{k}{2}, -\frac{k}{2}\}$  für gerades  $k$  und  $S = \{1, -1, \dots, \frac{k-1}{2}, -\frac{k-1}{2}, \frac{n}{2}\}$  für  $k$  ungerade und  $n$  gerade.

**4.3.16.** Es genügt zu zeigen, dass wenn  $\{u, v\} \in E(G)$ , dann  $\deg_G(u) = \deg_G(v)$ . Sei  $U$  die Menge aller Nachbarn von  $u$  außer  $v$ , und sei  $V$  die Menge aller Nachbarn von  $v$  außer  $u$ . Jede Ecke in  $U$  hat vier Nachbarn in  $V$ , und analog hat jede Ecke in  $V$  vier Nachbarn in  $U$ . Also ist  $|U| = |V|$  (Beweis mit doppeltem Abzählen der Kanten zwischen  $U$  und  $V$ ).

**4.3.17.** Beweis mit Widerspruch: Nehmen Sie an, dass je zwei Ecken eine ungerade Anzahl gemeinsamer Nachbarn besitzen. Schauen Sie sich für eine beliebige Ecke  $v$  den durch die Nachbarn von  $v$  induzierten Teilgraph an. Alle Grade in diesem Teilgraphen sind ungerade, und deshalb ist der Grad von  $v$  gerade. Zählen wir nun Spaziergänge der Länge 2, die bei  $v$  beginnen. Ihre Gesamtzahl ist gerade (weil alle Ecken geraden Grad haben). Eine ungerade Anzahl dieser Spaziergänge kommt zu  $v$  zurück, aber bei jeder anderen Ecke kommen ungerade viele Spaziergänge an, und deshalb muss die Anzahl der Ecken außer  $v$  gerade sein — ein Widerspruch.

**4.4.6.** Die Anzahl ungerader Folgenglieder muss gerade sein.

**4.4.9(a).** Betrachten Sie den längsten Weg in  $G$  und die Mengen der Nachbarn seiner beiden Enden.

**4.4.9(b).** Im Allgemeinen nein: Ein geeigneter vollständiger bipartiter Graph ist ein Gegenbeispiel.

**4.5.7.** Entfernen Sie alle Ritter, zu deren rechten ein Verbündeter sitzt. Die restlichen Ritter sind immer abwechselnd aus den beiden Burgen, also ist ihre Anzahl gerade; die Anzahl der entfernten Ritter ist die gleiche.

**4.5.8.** Induktion über die Anzahl der Ecken. Für eine beliebige Ecke  $v$  sei  $T_1$  das durch die Ecken mit Kopf  $v$  induzierte Turnier und  $T_2$  das durch die Ecken mit Fuß  $v$  induzierte Turnier. Beginnen Sie den Weg in  $T_1$ , setzen Sie ihn in  $T_2$  fort, und setzen Sie beide Teile in  $v$  zusammen.

**4.5.9.** Induktion über die Eckenzahl  $n$ . Ist  $T$  ein Turnier auf  $n$  Ecken, dann löschen Sie ein Ecke  $u$ , und  $v$  sei eine Ecke der gewünschten Art in dem kleineren Problem. Wenn in  $T$  die Ecke  $v$  nicht in ein oder zwei Schritten von  $u$  erreicht werden kann, dann ist  $(v, u) \in E(T)$ ; auch aus allen Ecken, von denen aus die Kante in  $v$  hineinführt, geht die Kante in  $u$  hinein, und deshalb kann  $u$  in höchstens zwei Schritten von jeder Ecke aus erreicht werden.

**4.6.2(b).** Unterteilen Sie jede Kante in  $K_{n+1}$ .

**4.6.2(c).** Sei  $T$  ein Baum (siehe Kapitel 5), in dem alle Ecken außer den Blättern Grad  $n$  haben, und der eine Ecke mit Abstand  $n$  von allen Blättern

hat (ein vollständiger  $n$ -ärer Baum). Machen Sie eine Kopie  $T'$  von  $T$  und identifizieren Sie jedes Blatt von  $T'$  mit seinem Urbild in  $T$ .

**4.6.3(a).** Ja.

**4.6.3(b).** Ja.

**4.6.4.** Es geht z.B. mit Induktion, wenn man auf eine „Ohrenzerlegung“ (siehe vorige Aufgabe) zurückgreift.

**4.6.5.** Es ist  $k$ . Zeigen Sie, dass je zwei Ecken des Würfels durch  $k$  eckendisjunkte Wege verbunden werden können.

**4.6.6.** Sei  $A$  eine Menge von  $k$  Ecken. Zählen Sie die Kanten, die  $A$  mit den anderen Ecken verbinden, auf zwei Arten, unter der Annahme, dass  $G - A$  mehr als  $k$  Komponenten hat.

**4.6.7.** Für  $n = 2k - 1$  muss  $G$  ein  $K_{2k-1}$  sein. Für  $n \geq 2k$ : Wenn es eine Ecke vom Grad  $\leq 2k - 3$  gibt, entfernen Sie sie und führen Sie Induktion. Ansonsten nehmen Sie an, dass  $G$ , wenn man  $\leq k - 1$  Ecken entfernt, in zwei nicht leere Teile  $G_1$  und  $G_2$  aufgeteilt werden kann, die durch keine Kanten verbunden sind. Zeigen Sie, dass die Induktionsvoraussetzung für  $G_1$  oder für  $G_2$  gelten muss, weil  $G$  sonst zu wenige Kanten hätte.

**5.1.6.** Es ist doch  $2n - 2 = 2|E(T)| = \sum_{v \in V(T)} \deg_T(v) = \sum_{i=1}^{n-1} ip_i$ . Die gewünschte Ungleichung ergibt sich durch eine einfache Umformung.

**5.1.8(c).** Induktion nach  $n$ . Sei  $n \geq 3$ , und  $(d_1, \dots, d_n)$  erfülle die Bedingung (ii). Dann gibt es ein  $d_i = 1$  und ebenso ein  $d_j > 1$  (nehmen Sie der Einfachheit halber an, dass  $d_n = 1$ ,  $d_{n-1} > 1$ ). Nach Induktionsvoraussetzung können Sie einen Baum mit Gradfolge  $(d_1, \dots, d_{n-2}, d_{n-1} - 1)$  konstruieren; hängen Sie ein neues Blatt an die Ecke Nummer  $n - 1$  an.

**5.2.5.** Teilen Sie die Folgen in zwei Gruppen ein, die mit 0 beginnen und die mit 1 beginnen, und sortieren Sie beide Gruppen getrennt. Wenn man den Algorithmus wirklich implementiert, dann werden gar nicht die Folgen selbst verschoben (bzw. sortiert), sondern man arbeitet mit Zeigern auf sie.

**5.2.6.** Der Code eines Baums auf  $n$  Ecken hat Länge  $2n$ . Also kann es höchstens  $4^n$  verschiedene Codes geben.

**5.3.1.** Beweisen Sie, dass sich die Markierung jeder einzelnen Ecke höchstens  $(\log_2 n)$  Mal ändert.

**5.3.2.** Der Graph  $G$  sei gegeben durch Listen  $S_v$  von Kanten, die jede Ecke  $v \in V(G)$  enthalten. Speichern Sie in einer doppelt verketteten Liste  $N$  alle Kanten, die zwischen der Menge  $V_i$  und ihrem Komplement verlaufen, und merken Sie sich darüber hinaus für jede Kante, die zu  $N$  gehört, einen Zeiger auf die Stelle, wo sie in  $N$  vorkommt. Wenn die neu hinzugefügte Ecke  $y_i$  Grad  $d$  hat, dann können alle Listen und Zeiger in Zeit  $O(d)$  aktualisiert werden.

**5.3.3(a).** Induktion über die Eckenzahl. Zeigen Sie, dass es für jede Kante  $\{v, v'\} \in E(T)$  eine Ordnung  $v_1, v_2, \dots, v_n$  der Ecken gibt, so dass  $v_1 = v$ ,

$v_n = v'$  und der Abstand zwischen  $v_i$  und  $v_{i+1}$  höchstens 3 ist,  $i = 1, 2, \dots, n - 1$ .

**5.4.1.** Wenden Sie Kruskals Algorithmus mit der Gewichtsfunktion  $-w$  an.

**5.4.4.** Der Ablauf des Greedy–Algorithmus ist eindeutig festgelegt und liefert einen minimal aufspannenden Baum. Der Korrektheitsbeweis zeigt, dass jeder andere aufspannende Baum ein größeres Gewicht haben muss.

**5.4.5.** In jeder Menge von Kanten gleichen Gewichts nehmen Sie die Kanten von  $T$  nach vorn. Sei  $T'$  der vom Greedy–Algorithmus berechnete Baum,  $e'_1, \dots, e'_{n-1}$  seine Kanten in der Reihenfolge ihrer Auswahl und  $e_1, \dots, e_{n-1}$  die Kanten von  $T$  nummeriert nach der gewählten Ordnung. Sei  $k$  der kleinste Index mit  $e_k \neq e'_k$ . Leiten Sie aus der Existenz von  $k$  einen Widerspruch her: Es ist  $w(e'_k) < w(e_k)$ , aber aus dem Beweis im Text wissen wir, dass  $w(e'_i) \leq w(e_i)$  für alle  $i$ , und also ist  $T$  nicht minimal.

**5.4.6.** Folgt aus Aufgabe 5.

**5.4.8(a).** Wenn  $v$  Grad  $\geq 7$  hat, dann gibt es Kanten  $\{v, u_1\}$  und  $\{v, u_2\}$  mit Winkel  $< 60$  Grad. Zeigen Sie, dass eine davon durch die Kante  $\{u_1, u_2\}$  ersetzt werden kann.

**5.4.8(b).** Beweisen und verwenden Sie die Tatsache, dass für ein konvexes Viereck  $ABCD$  die Ungleichungen  $|AB| + |CD| \leq |AC| + |BD|$  und  $|BC| + |AD| \leq |AC| + |BD|$  gelten. Zeigen Sie, dass man zwei kreuzende Kanten durch zwei nicht kreuzende ersetzen kann.

**5.4.9.** Bedecken Sie das Einheitsquadrat mit einem  $\sqrt{n} \times \sqrt{n}$  Schachbrett. Ordnen Sie die Felder des Schachbretts so in einer Folge  $s_1, s_2, \dots, s_n$  an, dass aufeinanderfolgende Felder benachbart sind. Konstruieren Sie einen Weg auf den gegebenen Punkten, der zuerst durch alle Punkte in  $s_1$  geht, dann durch alle Punkte in  $s_2$ , usw.

**5.4.10(a).** Sei  $E_M$  ein maximum Matching (d.h. eines mit größtmöglicher Kantenzahl) und  $E_G$  das Matching, das der Greedy–Algorithmus konstruiert hat. Ordnen Sie jeder Kante  $e \in E_M$  die erste Kante aus  $E_G$  zu, die sie schneidet. Jede Kante  $\check{e} \in E_G$  wird auf diese Weise höchstens zwei Kanten  $e_1, e_2 \in E_M$  mit  $w(e_1), w(e_2) \leq w(\check{e})$  zugeordnet.

**5.4.11(b).** Seien  $e_1, \dots, e_k$  die von dem Greedy–Algorithmus ausgewählten Kanten und  $\check{e}_1, \dots, \check{e}_t$  die Kanten einer minimalen Kantenbedeckung. Sei  $k_1 = |\{i: e_i \cap (e_1 \cup \dots \cup e_{i-1}) = \emptyset\}|$ , und analog  $t_1 = |\{i: \check{e}_i \cap (\check{e}_1 \cup \dots \cup \check{e}_{i-1}) = \emptyset\}|$ . Dann gilt  $|V| = k + k_1 = t + t_1$ . Beobachtung: In den Schritten für  $i > k_1$  muss mindestens eine Endecke jeder Kante  $\check{e}_j$ , die zu  $t_1$  beiträgt, bedeckt worden sein, und deshalb  $k_1 \geq \frac{1}{2}t_1$ . Daraus erhalten wir  $k = t + t_1 - k_1 \leq t + \frac{1}{2}t_1 \leq \frac{3}{2}t$ .

**5.4.12.** Sei  $V = \{1, 2, \dots, 2^{k+2} - 2\} \cup \{a_1, a_2, b_1, b_2, \dots, b_k\}$ . Die Ecke  $a_1$  ist mit  $1, 3, 5, \dots$  verbunden;  $a_2$  mit  $2, 4, 6, \dots$ ;  $b_i$  mit  $2^i - 1, 2^i, \dots, 2^{i+1} -$

2; darüber hinaus sind  $a_1, a_2$  mit allen  $b_i$  verbunden. Der Greedy-Algorithmus wählt alle  $b_i$ , während die optimale dominierende Menge  $\{a_1, a_2\}$  ist.

**5.5.5(a).** Beweisen Sie, dass nach der  $i$ -ten Phase jede Komponente mindestens  $2^i$  Ecken hat.

**5.5.5(b).** Halten Sie für jede Komponente eine Liste der ausgehenden Kanten. In jeder Phase kann man jede Liste durchgehen und die Kante minimalen Gewichts darin finden.

**6.1.1(a).** Abb. 6.1.

**6.1.1(b).** Man kann Graphen  $G_1, G_2$  aus (a) zusammenkleben. Zum Beispiel entfernt man eine Kante  $\{a, b\}$ , die ans äußere Land von  $G_1$  grenzt, und eine Kante  $\{c, d\}$ , die ans äußere Land von  $G_2$  grenzt, und fügt die Kanten  $\{a, c\}$  und  $\{b, d\}$  hinzu.

**6.1.3.** Induktion über die Kantenzahl. Betrachten Sie eine Ecke  $v$  vom Grad mindestens 4 und wählen Sie zwei Kanten, die an  $v$  stoßen und die (in der zyklischen Reihenfolge um  $v$ ) benachbart sind. Wenn möglich sollten diese beiden Kanten in verschiedene Komponenten von  $G - v$  führen. Ersetzen Sie diese zwei Kanten durch eine, die die beiden anderen Enden verbindet. (Vielleicht ist es günstig, Mehrfachkanten zuzulassen?)

**6.2.6.** Auf jedem 5-Tupel von Ecken haben wir eine Kopie des  $K_5$ , in dem sich irgendein Paar von Kanten kreuzt. Wir erhalten daher mindestens  $\binom{n}{5}$  Paare kreuzender Kanten. Jede Kreuzung wird in dieser Rechnung in  $n - 4$  Kopien von  $K_5$  gezählt.

**6.2.7(a).** Wählen Sie eine Kreisscheibe  $D$ , für die  $k \cap D$  eine gerade Linie ist. Von jedem Punkt in  $\mathbb{R}^2 \setminus k$  aus kann man  $D$  mit einem Polygonzug erreichen (einfach indem man  $k$  entlangläuft). Aber  $D \setminus k$  hat höchstens zwei Äquivalenzklassen, weil je zwei Punkte auf der gleichen Seite mit einer Linie verbunden werden können.

**6.3.5.** Behandeln Sie zuerst den Fall, dass  $G$  nicht 2-zusammenhängend ist. Beweisen Sie, dass man bei einem 2-zusammenhängenden Graphen  $G$  in jedes Land, das durch 6 oder mehr Kanten berandet ist, eine Diagonale einfügen kann. Man muss sich dabei sehr vorsehen, kein Dreieck zu erzeugen! Vielleicht müssen Sie mehrere Fälle unterscheiden.

**6.3.7(a).** Wenn von einem Punkt  $k \leq 3$  Kanten ausgehen, dann sagen Sie, dass er  $3 - k$  Freiheitsgrade hat. Die Summe aller Freiheitsgrade ist anfangs  $3n$ ; spätestens wenn sie den Wert 2 unterschreitet, ist kein Zug mehr möglich; und jeder Zug verringert die Freiheitsgrade um 1.

**6.3.7(c).** Zeigen Sie, dass in der Schlussstellung in jedes Land genau ein „unbenutzter“ Arm hineinragt. Die Gesamtzahl unbenutzter Arme bleibt während des gesamten Spiels konstant, und so muss es am Ende  $4n$  Länder geben. Mit jedem Zug verringert sich entweder die Anzahl der Komponenten um 1 oder die Zahl der Länder erhöht sich um 1.

**6.3.8(a).** Beweisen Sie mit Induktion über  $n$ , dass  $e = v + f - 1$ ; unterscheiden Sie beim Hinzufügen einer Gerade zwischen entstehenden und vorhandenen Schnittpunkten.

**6.3.8(c).** Folgern Sie  $e \geq 3f - n$  aus (b). Wenn  $d_i$  die Anzahl der Geraden ist, die durch den  $i$ -ten Schnittpunkt gehen, gilt  $\sum d_i = e - n$  (weil jede Kante zwei Enden hat, außer den  $2n$  Halbgeraden). Setzen Sie  $f$  aus (a) ein, dann erhalten Sie  $\sum d_i \leq 3v - 3$ .

**6.3.9.** Sie können annehmen, dass der Graph zusammenhängend ist. Ein rot–blauer Winkel sei ein Paar  $(f, v)$  von einem Land  $f$  und einer Ecke  $v$  auf dem Rand von  $f$  mit folgender Eigenschaft: Geht man die Grenze von  $f$  im Uhrzeigersinn entlang (gegen den Uhrzeigersinn beim äußeren Land), dann gelangt man über eine rote Kante zu  $v$  und geht über eine blaue Kante weiter. Zeigen Sie mit doppeltem Abzählen und der Euler–Formel, dass es eine Ecke mit höchstens einem rot–blauen Winkel gibt.

**6.4.2.** Führen Sie Induktion über die Eckenzahl. Entfernen Sie aus einem gegebenen Graphen eine Ecke kleinsten Grades, färben Sie den Rest und fügen Sie die Ecke wieder ein.

**6.4.3.** Ein Teilgraph eines außerplanaren Graphen ist außerplanar. Deshalb genügt es nach Aufgabe 2 zu zeigen, dass ein außerplanarer Graph stets eine Ecke vom Grad  $\leq 2$  hat. Das kann man aus der Euler–Formel folgern, wenn man ausnutzt, dass es ein Land gibt, das an mindestens  $n$  Kanten grenzt.

**6.4.4.** Zeigen Sie, dass  $\delta(G) \leq 3$  ist, und verwenden Sie Aufgabe 2.

**6.4.6(b).** Sie finden sogar einen Baum!

**6.4.6(c).** Fügen Sie genügend viele neue Blätter hinzu um die Grade anzupassen.

**6.4.10(a).** Induktion über die Kantenzahl. Betrachten Sie ein Land  $F$  und die Menge jener Kanten  $E_F$ , die auf seiner Grenze liegen. Zeigen Sie, dass alle Eckengrade in dem Graphen  $(V, E_F)$  gerade sind. Entfernen Sie aus  $G$  die Kanten in  $E_F$ , färben Sie den Rest nach Induktionsvoraussetzung, fügen Sie die Kanten aus  $E_F$  wieder ein und geben Sie dem Land  $F$  die andere Farbe.

**6.4.10(b).** Färben Sie die Länder mit zwei Farben. Die Kantenzahl können Sie als die Summe des Umfangs aller Länder mit der einen von den zwei Farben ausdrücken, aber auch als die Summe des Umfangs aller Länder mit der anderen Farbe. Doch der eine Ausdruck ist durch 3 teilbar, der andere nicht.

**6.4.12(b).** Auf die eine Seite setzen Sie  $k$  Ecken  $v_1, \dots, v_k$  und weisen der Ecke  $v_i$  die Liste  $L(v_i) = \{k(i-1)+1, k(i-1)+2, \dots, ki\}$  zu. Für jede Menge  $S$ , die aus jeder der Mengen  $L(v_i)$  genau ein Element enthält, geben Sie eine Ecke  $v_S$  mit der Liste  $L(v_S) = S$  auf die andere Seite.

**6.4.13.** Unterscheiden Sie im Induktionsschritt zwei Fälle. Wenn es eine Kante  $\{v_i, v_j\}$  gibt, bei der die beiden Enden  $v_i$  und  $v_j$  auf dem Kreis  $C$

liegen, aber nicht aufeinander folgen, dann zerlegen Sie  $G$  entlang dieser Kante. Andernfalls entfernen Sie die Ecke  $v_k$  und passen die Listen ihrer Nachbarn der neuen Situation an.

**7.1.1.** Definieren Sie einen Hilfsgraphen genau wie im Beweis des Sperner-Lemmas.

**7.1.2.** Stellen Sie sich zwei Wanderer am gleichen Tag vor, den einen beim Aufstieg, den anderen beim Abstieg.

**7.1.4.** Ja nur für (b) und (e). In (a) ist eine Drehung um den Mittelpunkt ein Gegenbeispiel; in (d) sei  $f(x)$  der Punkt, der  $x$  auf der Sphäre gegenüberliegt (der zu  $x$  „antipodale“ Punkt).

**7.1.5(a).** Machen Sie den Beweis der ebenen Version nach. Verbinden Sie solche Tetraeder durch eine Kante, die eine mit 1, 2, 3 markierte Seitenfläche gemeinsam haben, und verwenden Sie die ebene Version um zu zeigen, dass der Grad des äußeren „Landes“ ungerade ist.

**7.1.6(b).** Stellen Sie sicher, dass  $a$  viel weiter von  $c$  entfernt ist als  $b$  von  $d$ .

**7.1.6(c).** Mit Widerspruch. Hätte Bettina eine Gewinnstrategie, dann könnte Alice ihren ersten Zug beliebig setzen und befände sich danach im Wesentlichen in Bettinas Situation (ein besetztes Feld mehr aus dem ersten Zug kann nur von Vorteil sein). Sie könnte also Bettinas Gewinnstrategie benutzen.

**7.1.7(b).** Zeigen Sie, dass Bettina eine sehr einfache Strategie hat, ein Unentschieden zu erreichen.

**7.2.3.** Ein Unabhängigkeitssystem  $\mathcal{M}$  erfüllt  $\sum_{M \in \mathcal{M}} \binom{n}{|M|}^{-1} \leq 1$ , und im System  $\binom{X}{\lfloor n/2 \rfloor}$  gilt die Gleichheit. Deshalb haben alle Mengen in einem Unabhängigkeitssystem  $\mathcal{M}$  von größter Größe die Mächtigkeit  $\lfloor n/2 \rfloor$  oder  $\lceil n/2 \rceil$  (für gerades  $n$  sind Sie also fertig). Zeigen Sie: Wenn es  $t$  Mengen der Mächtigkeit  $\lfloor n/2 \rfloor$  gibt in  $\mathcal{M}$  und  $0 < t < \binom{n}{\lfloor n/2 \rfloor}$ , dann gibt es  $< \binom{n}{\lfloor n/2 \rfloor} - t$  Mengen in  $\mathcal{M}$  mit der Mächtigkeit  $\lceil n/2 \rceil$ .

**7.2.4.** Definieren Sie zu einem Automorphismus  $h$  eine Abbildung  $f: X \rightarrow X$ , wobei  $f(x)$  dasjenige  $y$  ist, für das  $h(\{x\}) = \{y\}$ . Zeigen Sie, dass  $h = f^\#$  ist (dass also alle Automorphismen von Permutationen kommen und es  $n!$  von ihnen gibt).

**7.2.6(a).** Wenden Sie den Satz von Sperner auf das Mengensystem  $\{\{i: \varepsilon_i = 1\}: \sum \varepsilon_i a_i \in (-1, 1)\}$  an.

**7.2.7.** Sei  $n = p_1 p_2 \dots p_n$  die Primfaktorzerlegung von  $n$ . Ordnen Sie jedem Teiler  $d = p_{i_1} p_{i_2} \dots p_{i_k}$  die Menge  $M_d = \{i_1, \dots, i_k\} \subseteq \{1, 2, \dots, n\}$  zu; dann gilt  $d_1 | d_2 \Leftrightarrow M_{d_1} \subseteq M_{d_2}$ . Verwenden Sie nun den Satz von Sperner.

**7.3.1.** Machen Sie den Beweis für  $K_{2,2}$  nach, mit dem einzigen Unterschied, dass eine Ecke  $v$  höchstens  $t - 1$  Elemente zu  $M$  beiträgt.

**7.3.6.** Untersuchen Sie nicht  $f(x) = x(x - 1)/2$ , sondern die Funktion  $f(x)$ , die für  $x \leq 2$  den Wert 0 annimmt und für  $x > 2$  den Wert  $x(x - 1)(x - 2)/6$ . Zeigen Sie, dass  $f$  konkav ist, und verwenden Sie dies ähnlich wie bei verbotenem  $K_{2,2}$ .

**7.3.7(a).** Der Graph mit Eckenmenge  $P \cup L$ , dessen Kanten den Paaren entsprechen, die zu zählen sind, enthält keinen  $K_{2,2}$ .

**7.3.7(b).** Diesmal enthält der Graph keinen  $K_{2,3}$ .

**8.1.1.** In Abschnitt 4.1 haben wir eine Schranke für die Anzahl nicht isomorpher Graphen hergeleitet. Gehen Sie entsprechend vor und benutzen Sie die Cayley–Formel 8.1.1 sowie die Abschätzung 3.5.5 für  $n!$ .

**8.1.2.** Zählen Sie die Bäume, die eine feste Kante des  $K_n$  enthalten. Wegen der Symmetrie ist diese Zahl unabhängig von der konkret gewählten Kante. Benutzen Sie die Cayley–Formel 8.1.1.

**8.1.3.** Zählen Sie die aufspannenden Wälder mit genau zwei Komponenten, bei denen in jeder Komponente eine Ecke markiert ist. Einerseits können wir aus jedem aufspannenden Baum des  $K_n$  auf  $n - 1$  Arten eine Kante löschen. Andererseits können wir auf  $k(n - k)$  Arten Ecken markieren, wenn ein Baum auf einer  $k$ -elementigen Teilmenge der Ecken und einer auf den restlichen  $n - k$  Ecken gegeben sind.

**8.1.4.** Betrachten Sie zu gegebenem aufspannenden Baum  $T$  in  $G$  den Teilgraphen von  $G^*$ , der all die Kanten enthält, die nicht von Kanten aus  $T$  gekreuzt werden. Zeigen Sie, dass dieser Teilgraph ein aufspannender Baum von  $G^*$  ist. Wir verweisen auf Lovász [9] für die Details.

**8.2.1(a).** Die Anzahl ist 0, wenn  $n$  ungerade ist. Für gerades  $n$  gibt es  $\frac{n}{2} + 1$  Blätter und  $\frac{n}{2} - 1$  Ecken vom Grad 3 (Induktion). Wir summieren also den Ausdruck  $(n - 2)!/2^{n/2-1}$  über alle möglichen Vektoren  $(d_1, \dots, d_n)$  mit  $d_i \in \{1, 3\}$  und  $\sum d_i = 2n - 2$ . Die Substitution  $k_i = \frac{1}{2}(d_i - 1)$  zeigt, dass die Anzahl der Summanden gleich der Anzahl  $(\frac{n}{2} - 1)$ -elementiger Teilmengen einer  $n$ -Menge ist. Das Ergebnis ist  $(n - 2)! \binom{n}{n/2-1} 2^{-n/2+1}$ .

**8.2.1(b).** Besonders leicht geht es mit erzeugenden Funktionen. Die gesuchte Zahl ist der Koeffizient von  $x^{2n-2}$  in dem Ausdruck  $(n - 2)!(x + x^2 + \frac{1}{2}x^3)^n$ , den man mit Hilfe des Multinomialssatzes erhält. (Teil (a) kann auch so gelöst werden.)

**8.2.2(a).** Beide Seiten der Gleichung zählen die Paare  $(T, T^*)$  aufspannender Bäume mit  $\deg_T(n) = k$ ,  $\deg_{T^*}(n) = k + 1$ , und  $T^*$  erhält man aus  $T$  durch folgende Operation: Wähle eine Kante  $\{i, j\} \in E(T)$  mit  $i \neq n \neq j$ , lösche sie, und füge von den beiden Kanten  $\{i, n\}$  und  $\{j, n\}$  diejenige ein, die die beiden Komponenten von  $T - \{i, j\}$  verbindet. Aus einem Baum  $T$  erhalten wir  $n - 1 - k$  verschiedene  $T^*$ , und jeder  $T^*$  kann von  $k(n - 1)$  verschiedenen  $T$  kommen.

**8.2.2(c).**  $\sum_k N_k$  ist nach dem Binomialssatz das Gleiche wie  $((n - 1) + 1)^{n-2}$ .

**8.3.3.** Stellen Sie sich vor, zwei Fußgänger starten im gerichteten Graphen von  $f$  von der Ecke  $i$  aus. Einer der beiden durchläuft eine Kante pro Minute, der andere eine Kante alle zwei Minuten. Wann treffen sich die beiden Fußgänger wieder in einer Ecke?

**8.4.1.** Die Ungleichung  $\deg_T(i) \geq m_i + 1$  sieht man leicht ein. Zugleich ist  $\sum_i m_i = n - 2$  und  $\sum_i (\deg_T(i) - 1) = 2(n - 1) - n = n - 2$ , also muss für alle  $i$  Gleichheit gelten.

**8.5.1(a).** Die Zeilensumme von  $Q$  ist 0.

**8.5.1(b).** Wenn  $T(G) > 0$ , dann ist  $\det Q_{11} \neq 0$  nach Satz 8.5.1.

**8.5.1(c).** Die Summe aller Zeilen, die zu einer bestimmten Komponente von  $G$  gehören, ist 0, d.h. für jede Komponente wird eine Zeile von anderen Zeilen erzeugt. Hat  $G$  mindestens zwei Komponenten, so hat der von den Zeilen von  $Q$  erzeugte Vektorraum also Dimension  $< n - 1$ .

**8.5.1(d).** Der Kern der linearen Abbildung  $x \mapsto Qx$  enthält  $(1, 1, \dots, 1)$ , weil die Zeilensumme 0 ist, und nach (b) ist er eindimensional.

**8.5.1(e).** Das Produkt der  $i$ -ten Zeile von  $Q$  und der  $i$ -ten Spalte von  $Q^*$  ist  $\det Q$ , entwickelt nach der  $i$ -ten Zeile. Sie wissen, dass  $\det Q = 0$ . Die anderen Einträge im Produkt  $QQ^*$  sind die Determinanten von anderen Matrizen, in denen allerdings eine Zeile mehrfach vorkommt, und also auch 0.

**8.5.3.** Das Ergebnis ist  $n^{m-1}m^{n-1}$ .

**8.5.4.** Für die eine Richtung: Berechnen Sie die Determinante der Incidenzmatrix eines ungeraden Kreises. Für die andere Richtung: Führen Sie Induktion ähnlich wie in Lemma 8.5.3.

**9.1.3(c).** Möglichkeiten:  $\mathcal{L} = \{X\}$ ,  $\mathcal{L} = \{X, \{a\}\}$  für ein  $a \in X$  und  $\mathcal{L} = \{X \setminus \{a\}\} \cup \{\{a, x\}: x \in X \setminus \{a\}\}$  für ein  $a \in X$ . Beim Beweis kann Übung 4 hilfreich sein.

**9.1.4.** Zeigen Sie, dass zwei Punkte von  $L_1 \setminus L_2$  und zwei Punkte von  $L_2 \setminus L_1$  zusammen eine Konfiguration  $F$  wie in Axiom (P0) bilden.

**9.1.6.** Höchstens 4 Mengen können einen beliebigen gegebenen Punkt enthalten.

**9.1.7.** Ja. Zeichnen Sie 8 Geraden in der Ebene in allgemeiner Lage (je zwei sind nicht parallel, je drei Geraden schneiden sich nicht in einem gemeinsamen Punkt). Die Schnittpunkte repräsentieren die Haltestellen und die Geraden die Buslinien.

**9.1.8(a).** Jedes Paar liegt in höchstens einer Menge. Jede Menge bedeckt  $\binom{n+1}{2}$  Paare. Es zeigt sich, dass die Anzahl der bedeckten Paare gleich der Anzahl aller Paare ist und daher alle Paare bedeckt sein müssen.

**9.1.8(b).** Gäbe es mehr solcher Mengen, hätten sie zusammen mehr als  $n^2 + n + 1$  Punkte.

**9.1.8(c).** Zählen Sie die Paare  $(x, L)$ ,  $x \in L$  doppelt ab und benutzen Sie (b).

**9.1.8(d).** Es gibt  $n^2 + n + 1$  verschiedene Geraden, die eine gegebene Gerade schneiden.

**9.1.9.** Betrachten Sie einen Punkt  $a \in A$ . Die  $n + 1$  Geraden, die den Punkt enthalten, bedecken alle Punkte aus  $X$ , und jede von ihnen enthält außer  $a$  höchstens einen Punkt aus  $A$ .

**9.1.10(a).** Entfernen Sie die Punkte einer beliebigen Geraden.

**9.1.10(b).** Transitivität: Angenommen  $A_1 \parallel A_2$ ,  $A_2 \parallel A_3$  und  $x \in A_1 \cap A_3$ . Dann sind  $A_1$  und  $A_3$  zwei Geraden durch  $x$  und parallel zu  $A_2$ , im Widerspruch zum dritten Axiom.

**9.1.10(c).** Um zu zeigen, dass je zwei Geraden  $A, A'$  die gleiche Mächtigkeit haben, konstruieren Sie eine Bijektion, die Parallelen zu einer Geraden  $\overline{xy}$  mit  $x \in A$  und  $y \in A'$  benutzt.

**9.1.10(d).** Fügen Sie für jede Äquivalenzklasse von  $\parallel$  einen neuen „uneigentlichen“ Punkt hinzu, fügen Sie ihn zu den Geraden der Äquivalenzklasse hinzu und bilden Sie aus allen uneigentlichen Punkten eine Gerade. Überprüfen Sie die Axiome.

**9.3.4(a).** Fügen Sie zu den  $t$  gegebenen orthogonalen lateinischen Quadraten ein Quadrat hinzu, dessen Einträge in der  $i$ -ten Zeile alle gleich  $i$ ,  $i = 1, 2, \dots, n$  sind, und ein Quadrat, dessen Einträge in der  $j$ -ten Spalte alle gleich  $j$  sind  $j = 1, 2, \dots, n$ .

**9.3.4(b).** Damit ein freies Quadrat orthogonal zu einem anderen sein kann, muss es jedes  $i \in \{1, 2, \dots, n\}$  genau  $n$ -mal enthalten. Permutieren Sie die Einträge in den gegebenen  $t + 2$  orthogonalen freien Quadraten so, dass in dem ersten Quadrat die Zahlen  $i$  alle in der  $i$ -ten Zeile stehen  $i = 1, \dots, n$  (alle Quadrate werden mit der gleichen Permutation permutiert). Permutieren Sie dann die Einträge innerhalb jeder Zeile (wieder die gleiche Permutation für alle Quadrate) so, dass in dem zweiten Quadrat in der  $j$ -ten Spalte alle Einträge  $j$  sind. Überprüfen Sie, dass die verbleibenden  $t$  Quadrate alle lateinische Quadrate sind.

**9.3.6.**  $n! \times$  (die Anzahl der Permutationen ohne Fixpunkte).

**9.4.3(a).** Die beiden Eckenmengen seien  $A$  und  $B$ ; doppeltes Abzählen liefert  $\sum \binom{d_i}{2} = \binom{n}{2}$ , wobei die  $d_i$  die Grade der Ecken in  $A$  sind, und wir haben  $m = |E(G)| = \sum_i d_i$ . Diesmal müssen wir genau rechnen: Nach Cauchy–Schwarz ist  $m^2 \leq n \sum d_i^2 = 2n \sum \binom{d_i}{2} + nm \leq n^2(n - 1) + nm$ . Lösen Sie die entstehende quadratische Ungleichung nach  $m$  auf.

**10.1.1(a).** Eine Funktion in  $n$  Variablen definiert zwei Funktionen in  $n - 1$  Variablen, eine für  $x_n = 0$  und eine für  $x_n = 1$ . Sie können also Induktion über  $n$  führen.

**10.1.3.** Jede Wägung hat drei mögliche Ausgänge, deshalb kann man mit drei Wägungen nur eine von  $3^3$  Möglichkeiten herausfinden.

**10.1.4.** Codieren Sie alle möglichen Rangiervorgänge auf den gegebenen Gleisen, z.B. „ein Wagen von Gleis A auf Gleis I, einer von A nach C, einer

von I nach C, einer von C nach II, ...“. Zeigen Sie, dass es höchstens  $K^n$  viele verschiedene Codes gibt (für eine Konstante  $K$ ); es gibt dann auch höchstens so viele realisierbare Anordnungen der Wagen auf Gleis B, und diese Zahl ist für große  $n$  kleiner als  $n!$ .

**10.2.2(a).**  $P(A_1 \cup \dots \cup A_n) = \sum_{\emptyset \neq I \subseteq \{1, \dots, n\}} (-1)^{|I|-1} P(\bigcap_{i \in I} A_i)$ .

**10.2.2(b).** Alle drei Beweise des Prinzips der Inklusion–Exklusion aus Kapitel 3 lassen sich mühelos verallgemeinern.

**10.2.4.** Bei einem unzusammenhängenden Graphen gibt es eine echte nicht leere Teilmenge  $A$  der Eckenmenge, so dass zwischen  $A$  und dem Komplement von  $A$  keine Kanten verlaufen. Berechnen Sie die Wahrscheinlichkeit dieses Ereignisses für ein festes  $A$  und summieren Sie dann über alle möglichen  $A$ .

**10.2.8.** Wenn Sie einige der  $A_i$  durch ihre Komplemente ersetzen, haben Sie immer noch lauter unabhängige Ereignisse, und der Schnitt aller dieser Ereignisse hat immer noch eine positive Wahrscheinlichkeit. Auf diese Weise können Sie  $2^n$  disjunkte Ereignisse mit positiver Wahrscheinlichkeit erzeugen.

**10.2.9.** Die Antwort ist  $\frac{1}{3}$ . (Nennen Sie die Kinder A und B. Dann gibt es drei gleichermaßen wahrscheinliche Szenarien: A=Junge, B=Junge; A=Junge, B=Mädchen; A=Mädchen, B=Junge.)

**10.3.2.** Zeigen Sie  $0 \leq \mathbf{E}[(f - \mathbf{E}[f])^2] = \mathbf{E}[f^2] - \mathbf{E}[f]^2$ .

**10.3.3.** Benutzen Sie Indikatorfunktionen. Sei  $A_i$  das Ereignis „ $\pi(i) = i$ “. Das Ergebnis ist  $\mathbf{E}[f] = 1$ .

**10.3.4(a).** Sei  $A_i$  das Ereignis „1 ist in einem Zyklus der Länge  $i$  enthalten“. Zeigen Sie, dass  $P(A_i) = \frac{1}{n}$  ist, und schreiben Sie den gesuchten Erwartungswert als  $\sum_{i=1}^n i \cdot \mathbf{E}[I_{A_i}]$ .

**10.3.4(b).** Sei  $A_{ij}$  das Ereignis „ $j$  liegt in einem Zyklus der Länge  $i$ “. Aus Teil (a) wissen wir, dass  $P(A_{ij}) = \frac{1}{n}$ . Zeigen Sie, dass sich der gesuchte Erwartungswert als  $\sum_{i,j=1}^n \frac{1}{i} \mathbf{E}[I_{A_{ij}}]$  ausdrücken lässt.

**10.3.6.** Besser zählt man die Grenzen zwischen Serien. Die Wahrscheinlichkeit, dass an einer gegebenen Position zwischen zwei Würfen eine Serie endet und die nächste beginnt, ist  $\frac{1}{2}$ .

**10.3.7.** Es gilt  $\mu = \sum_{\omega \in \Omega} P(\{\omega\})X(\omega) \geq \sum_{\omega \in \Omega: X(\omega) \geq t\mu} P(\{\omega\})t\mu = t\mu P(\{\omega \in \Omega: X(\omega) \geq t\mu\})$ .

**10.4.4.** Ein  $K_r$ -freier Graph mit mindestens  $r-1$  Ecken und mit maximal vielen Kanten muss einen  $K_{r-1}$  enthalten. Reißen Sie einen  $K_{r-1}$  heraus und bestimmen Sie die Anzahl gelöschter Kanten.

**10.4.6(b).** Sei  $L$  die Menge der Zahlen, die kleiner als das unterteilende Element sind, und  $R$  die Menge der größeren Zahlen. Zeigen Sie, dass die Zahl  $\min(|L|, |R|)$  in den beiden betrachteten Varianten des Algorithmus die gleiche Wahrscheinlichkeitsverteilung aufweist. Diese Zahl bestimmt die Größen der zwei Teilstufen für die Rekursion völlig.

**10.4.7.** In  $R$  seien die  $r$  Kreise, die schwarz bleiben,  $c$  sei der Kreis, der kurzzeitig schwarz war und nun wieder weiß, und  $S(R)$  sei die Menge derjenigen weißen Kreise, die der Beobachter (bei gegebenem  $R$ ) sehen kann. Sei  $p$  die Wahrscheinlichkeit, dass  $c \in S(R)$  ist. Weil  $c$  ein zufälliges Element aus  $R \cup \{c\}$  ist, erhalten wir  $p \leq 2/(r+1)$ . Weil wir aber zuerst  $R$  wählen könnten und dann aus den  $n-r$  weißen Kreisen  $c$ , ist  $p$  der durchschnittliche Wert von  $|S(R)|/(n-r)$ . Also ist  $p = \mathbf{E}[|S(R)|]/(n-r)$ .

**10.4.9.** Es gibt höchstens zwei Spitzen nullter Ordnung. Bestimmen Sie auf zwei Arten die erwartete Anzahl Spitzen nullter Ordnung für eine zufällige Teilmenge  $R$  der Geraden, so wie im Beweis im Text.

**12.1.4.** Um bei der Multiplikation von  $n$  Klammern den Term  $x_1^{k_1} \dots x_m^{k_m}$  zu erhalten, müssen wir  $k_1$  Klammern wählen, aus denen wir  $x_1$  nehmen,  $\dots$ ,  $k_m$  Klammern, aus denen wir  $x_m$  wählen. Die Anzahl der Wahlmöglichkeiten ist gerade der Multinomialkoeffizient.

**12.1.6.** Beginnen Sie mit der Gleichung  $(1-x)^n(1+x)^n = (1-x^2)^n$ .

**12.2.5.**  $a(x) = (1-x)^{-1}x^6(1-x^3)^{-2} = x^6(1+x+x^2)/(1-x^3)^3$ . Verwenden Sie den verallgemeinerten Binomialsatz.

**12.2.8(a).** Die erzeugende Funktion ist  $1/((1-x)(1-x^2)(1-x^5))$ .

**12.2.9(d).** Ergebnis:  $(-1)^m \binom{n-1}{m}$ .

**12.2.10.** Für  $1 \leq k \leq n-r+1$  gibt es  $\binom{n-k}{r-1}$  Teilmengen mit kleinstem Element  $k$ , wir müssen also  $\sum_k k \binom{n-k}{r-1}$  berechnen. Das geht z.B., indem man die Gleichung  $[x^{r-1}/(1-x)^r][x/(1-x)^2] = x^r/(1-x)^{r+2}$  betrachtet und die Koeffizienten von  $x^n$  vergleicht. Oder wir bezeichnen den Erwartungswert mit  $f(n, r)$  und haben dann die Rekursion  $f(n, r) = p + (1-p)(1+f(n-1, r))$  mit  $p = \frac{r}{n}$  (weil entweder die 1 in  $R$  enthalten ist, das geschieht mit Wahrscheinlichkeit  $p$ , oder  $R$  als  $r$ -elementige Teilmenge von  $\{2, 3, \dots, n\}$  aufgefasst werden kann). Dann folgt  $f(n, r) = \frac{n+1}{r+1}$  mit vollständiger Induktion.

**12.2.12(a).** Für die Stetigkeit müssen Sie beweisen, dass für  $x_0 \in [0, \rho)$  gilt:  $\lim_{x \rightarrow x_0} |a(x) - a(x_0)| = 0$ . Verwenden Sie die Abschätzung  $|x_0^i - x^i| \leq |x_0 - x|(x_0^{i-1} + x_0^{i-2}x + \dots + x^{i-1}) \leq |x - x_0|im^{i-1}$ , wobei  $m = \max(x, x_0)$ .

**12.2.12(c).** Zum Beispiel  $a_i = 1/i^2$ .

**12.2.13(a).** Zeigen Sie zunächst (mit Induktion), dass jede Ableitung der Funktion  $f$  an einer Stelle  $x \neq 0$  die Gestalt  $R(x)e^{-1/x^2}$  hat, wobei  $R(x)$  ein Quotient zweier Polynome ist. Beweisen Sie dann, dass alle Ableitungen bei 0 gleich 0 sind.

**12.2.13(b).** Wäre  $f$  eine Potenzreihe, dann könnte man die Koeffizienten mithilfe der Ableitungen ausdrücken — sie müssten alle 0 sein.

**12.2.14(a).** Für die kreisförmige Aufstellung:  $-\ln(1-x)$ .

**12.2.14(c).**  $D(x) = 1/(1 - A(x))$ .

**12.2.14(d).**  $E(x) = e^{A(x)}$ .

**12.2.14(e).** Die exponentielle erzeugende Funktion ist  $e^{x^2/2}$ .

**12.2.15.** Verwenden Sie Teil (d) und organisieren Sie die Teilgruppen in unstrukturierte Versammlungen mit mindestens einem Teilnehmer, d.h.  $A(x) = e^x - 1$ . Das Ergebnis ist  $e^{e^x-1}$ .

**12.2.16.** Die exponentielle erzeugende Funktion ist  $(x^2/2! + x^3/3! + x^4/4!)^5$ . Die Antwort ist  $12!$  mal der Koeffizient von  $x^{12}$ .

**12.2.17(a).** Solche Aufstellungen korrespondieren bijektiv mit Permutationen, weil sie die Zyklen der Permutation codieren.

**12.2.17(b).** Das Ergebnis ist  $e^{-\ln(1-x)-x} = (1+x+x^2+\dots)(1-x/1!+x^2/2!-x^3/3!+\dots)$ .

**12.3.1.** Sei  $a_n$  (bzw.  $b_n$ ) die Anzahl solcher Folgen, die auf 0 (bzw. 1) enden. Leiten Sie Rekursionen für  $a_n$  und für  $b_n$  her. Das Ergebnis sind die Fibonacci-Zahlen.

**12.3.2.** Induktion nach  $n$ . Nennen Sie eine Darstellung von  $n$  als Summe verschiedener Fibonacci-Zahlen *reduziert*, wenn in ihr keine zwei aufeinander folgenden Fibonacci-Zahlen vorkommen. Jede Darstellung lässt sich in eine reduzierte umwandeln, indem man wiederholt die zwei größten aufeinander folgenden Fibonacci-Zahlen durch ihre Summe ersetzt. Betrachten Sie für den Schritt von  $n$  nach  $n+1$  eine reduzierte Darstellung von  $n$ , addieren Sie 1, und reduzieren Sie sie wieder. Übrigens ist die reduzierte Darstellung eindeutig.

**12.3.5.** Betrachten Sie die Folge  $b_n = \log_2 a_n$ .

**12.3.7.** Ein geeigneter Ausdruck ist  $\sum_{k=0}^{\infty} x^k (1+2x)^k = 1/(1-x-2x^2) = \frac{1}{3}[1/(1+x) + 2/(1-2x)]$ , die Formel ist  $\frac{2}{3}4^n + \frac{1}{3}$ .

**12.3.8.**  $(n+1)/2^n$ .

**12.3.9.** Sie genügt der Rekursion  $a_{n+2} = 2a_{n+1} + a_n$  mit  $a_0 = a_1 = 1$ .

**12.3.10.** Zeigen Sie, dass  $x_n = (6 + \sqrt{37})^n - (6 - \sqrt{37})^n$  die Gleichung  $x_{n+2} = 12x_{n+1} + x_n$  mit Anfangsbedingungen  $x_0 = 2$ ,  $x_1 = 12$  erfüllt und daher für alle  $n$  eine ganze Zahl ergibt. Machen Sie dann Gebrauch von der Tatsache, dass  $\sqrt{37} - 6 < 0,1$  ist.

**12.3.11.** Die Gleichung  $\sqrt{x+1} - \sqrt{x} = y$  hat die Lösung  $x = ((1-y^2)/2y)^2$  ( $0 < y < 1$ ). Daher genügt es zu zeigen, dass dieses  $x$  ganzzahlig ist für  $y = (\sqrt{2}-1)^n$ . Wir erhalten  $x = a_n^2$ , wobei  $a_n = \frac{1}{2}[(\sqrt{2}+1)^n - (\sqrt{2}-1)^n]$  ist. Finden Sie eine Rekursion für  $a_n$  und zeigen Sie mittels vollständiger Induktion, dass  $a_n$  für gerades  $n$  ganzzahlig ist und für ungerades  $n$  ein ganzzahliges Vielfaches von  $\sqrt{2}$ .

**12.3.12.** Bezeichnen Sie mit  $u_n$  die Anzahl solcher Folgen, die mit  $a$  oder  $b$  beginnen, und bezeichnen Sie mit  $v_n$  die Anzahl solcher Folgen, die mit  $c$  oder  $d$  beginnen. Sie erhalten die Rekursionen  $u_n = u_{n-1} + 2v_{n-1}$  und

$v_n = 2u_{n-1} + 2v_{n-1}$ . Schreiben Sie die zugehörigen Gleichungen für die erzeugenden Funktionen  $u(x)$  und  $v(x)$  nieder, lösen Sie sie, und berechnen Sie die Koeffizienten. Das Ergebnis ist  $u_n + v_n = \frac{\sqrt{17}+1}{4\sqrt{17}} (\frac{1}{2}(3+\sqrt{17}))^{n+1} + \frac{\sqrt{17}-1}{4\sqrt{17}} (\frac{1}{2}(3-\sqrt{17}))^{n+1}$ .

**12.3.13(a).** Die Zahl ist  $F_{n+1}$ .

**12.3.13(b).** Rekursion:  $a_{n+3} = a_{n+2} + 4a_{n+1} + 2a_n$ ,  $a_0 = 1$ ,  $a_1 = 1$ ,  $a_2 = 5$ ;  $a_n \sim \frac{1}{\sqrt{3}}(1 + \sqrt{3})^n$ .

**12.3.13(c).** Sei  $a_n$  die gesuchte Zahl und  $b_n$  die Anzahl der Möglichkeiten, ein  $n \times 2$  Rechteck ohne die linke obere Ecke zu belegen (wir halten es für einfacher, sich die längere Seite vertikal vorzustellen). Rekursionen:  $a_n = a_{n-1} + 2b_{n-1} + a_{n-2}$ ,  $b_n = a_{n-2} + b_{n-1}$ ,  $a_0 = a_1 = 1$ ,  $b_0 = b_1 = 0$ . Gleichungen für die erzeugenden Funktionen:  $b(x) = xb(x) + x^2a(x)$ ,  $a(x) = 1 + x(a(x) + 2b(x)) + x^2a(x)$ . Daraus erhalten Sie  $a(x) = (1-x)/(1-2x-x^3)$  und  $a_n \sim (0,4607\dots)(2,0556\dots)^n$ .

**12.3.14(a).** Für die Sprache ohne aufeinanderfolgende  $a$ : Setzen Sie  $A = \{a\}$ ,  $B = \{b\}$ . Dann erhält man die betrachtete Sprache als  $B^*.(A.B.B^*)^* \cup B^*.(A.B.B^*)^*.A$ , womit sie sehr regulär ist.

**12.3.14(b).** Ist  $a(x)$  die erzeugende Funktion von  $L_1$  und  $b(x)$  von  $L_2$ , dann ist  $a(x)b(x)$  die erzeugende Funktion von  $L_1.L_2$ ,  $1/(1-a(x))$  ist die erzeugende Funktion von  $L_1^*$ , und  $a(x) + b(x)$  ist die erzeugende Funktion von  $L_1 \cup L_2$  (vorausgesetzt  $L_1 \cap L_2 = \emptyset$ ).

**12.3.14(c).** Man kann diese Aufgabe mit deterministischen endlichen Automaten lösen; schauen Sie in ein Buch über Automaten und formale Grammatik.

**12.3.16(b).** Zeigen Sie, dass die Folgen, bei denen das  $j$ -te Glied 1 ist und die Glieder  $y_0, \dots, y_{k-1}$  sind 0 (für  $j = 0, 1, \dots, k-1$ ), eine Basis bilden.

**12.3.16(c).** Um die lineare Unabhängigkeit zu zeigen, genügt es zu überprüfen, dass die Vektoren mit den ersten  $k$  Gliedern der betrachteten Folgen linear unabhängig sind. Dazu können Sie das Determinantenkriterium für lineare Unabhängigkeit benutzen. Hoffentlich erinnern Sie sich noch an die Vandermonde–Determinante (die Sie wahrscheinlich aus der Vorlesung Lineare Algebra kennen).

**12.3.16(e).** Die vielleicht einfachste Methode ist, das Wachstumsverhalten der Folgen zu betrachten. Wären die Folgen linear abhängig, könnte eine schneller wachsende Folge als Linearkombination von langsamer wachsenden ausgedrückt werden, was offensichtlich unmöglich ist. Ein Problem hat man bei diesem Ansatz nur dann, wenn es mehrere komplexe Nullstellen mit gleichem Betrag gibt. Diesen Fall muss man separat behandeln, zum Beispiel mit der Vandermonde–Determinante wie im Hinweis zu (c). Eine Alternative ist, die Determinante für die ersten  $k$  Glieder wie in (c) zu betrachten und zu beweisen, dass sie nicht 0 ist.

**12.4.2.** Codieren Sie einen binären Baum mit  $n$  Ecken durch eine Folge mit  $O(n)$  Buchstaben und/oder Ziffern, und zeigen Sie so, dass  $b_n \leq C^n$  für eine geeignete Konstante  $C$ .

**12.4.3(a).**  $\binom{2n}{n}$ .

**12.4.3(b).** Ein Weg, der nie unter die Diagonale geht, codiert einen binären Baum: Teilen Sie den Weg in zwei Teile, und zwar an der Stelle, wo er zum ersten Mal die Diagonale trifft (der zweite Teil kann leer sein). Entfernen Sie die erste und die letzte Kante aus dem ersten Teil und lassen Sie den zweiten Teil, wie er ist. Die beiden Teile codieren dann rekursiv den linken und rechten Teilbaum (ein leerer Weg codiert den leeren Baum).

**12.4.3(c).** Zur Beschreibung der Lösung führen wir Koordinaten ein:  $A$  ist  $(0, 0)$ ,  $B$  ist  $(n, n)$ . Vergrößern Sie das Schachbrett um eine Spalte auf der rechten Seite. Zeigen Sie, dass die Wege, welche doch unter die Diagonale gehen, bijektiv auf die kürzesten Wege von  $A$  nach  $B_1 = (n+1, n-1)$  abgebildet werden können: Folgen Sie dem gegebenen Weg von  $A$  nach  $B$  bis zum Ende der ersten Kante, die unter der Diagonale liegt, und spiegeln Sie ab diesem Punkt den Rest des Weges an der Geraden  $y = x - 1$ . Das ergibt einen Weg von  $A$  nach  $B_1$ . Prüfen Sie, dass das eine Bijektion ergibt.

**12.4.4.** Finden Sie eine Bijektion mit den Wegen auf dem Schachbrett aus der vorigen Übung, die nicht unter die Diagonale gehen.

**12.4.8(b).**  $c_{2n+1} = b_n$ . Man erhält eine Bijektion zwischen den gepflanzten Bäumen in der Aufgabe und den binären Bäumen aus dem Text, indem man von dem gegebenen gepflanzten Baum alle Blätter abpflückt.

**12.4.9(a).** Ergebnis:  $t_n = b_{n-1}$ .

**12.4.10.** Ein alter Baum ist entweder allein die Wurzel, oder er entsteht durch Anhängen  $k$  gepflanzter Bäume mit jeweils mindestens zwei Ecken an die Wurzel, deshalb ist  $s(x) = x + x/(1 - t(x) + x)$ .

**12.6.1(a).** Sei  $a_i$  die Anzahl der Sprungfolgen, die bei 1 beginnen und nach  $i$  Schritten erstmals zur 0 zurückkehren. Die gesuchte Wahrscheinlichkeit ist  $a(\frac{1}{2})$ . Leiten Sie die Beziehung  $a(x) = x + xa(x)^2$  her. Den Wert von  $a_i$  kann man auch explizit berechnen, zum Beispiel mit den Catalan-Zahlen.

**12.6.2(b).** Das Problem ist, dass  $S_1$  unendlich ist (obwohl 1 fast sicher schließlich erreicht wird, ist die erwartete Zeit dafür unendlich!).

**12.7.1(a).** So eine geordnete Partition kann man codieren, indem man die Zahlen  $1, 2, \dots, n$  in  $k$  Segmente aufeinander folgender Zahlen einteilt. Betrachten Sie die  $(k-1)$ -elementige Teilmenge von  $\{1, 2, \dots, n-1\}$ , in der die letzten Zahlen aus allen Segmenten (außer dem letzten) enthalten sind.

**12.7.1(b).** Eine direkte Lösung geht wie in (a) (Betrachten Sie alle Teilmengen von  $\{1, 2, \dots, n-1\}$ ). Die erzeugende Funktion für (a) ist  $x^k/(1-x)^k$ , und die Summe über alle  $k \geq 1$  ist  $x/(1-2x)$ .

**12.7.3(a).**  $(1+x)(1+x^2)\dots(1+x^n)$ .

**12.7.3(c).** Finden Sie eine Bijektion zwischen allen Partitionen von  $n$  mit  $k$  verschiedenen Summanden und allen Partitionen von  $n - \binom{k}{2}$  mit  $k$  (nicht notwendig verschiedenen) Summanden. Wenden Sie dann die im Text demonstrierte Methode an, um die untere Schranke zu erhalten.

**12.7.4(c).** Die erzeugenden Funktionen sind  $(1+x)(1+x^2)(1+x^3)\dots$  und  $1/((1-x)(1-x^3)(1-x^5)\dots)$ . Multiplizieren Sie Zähler und Nenner des ersten Ausdrucks mit  $(1-x)(1-x^2)(1-x^3)\dots$ . Das führt zu  $((1-x^2)(1-x^4)(1-x^6)\dots)/((1-x)(1-x^2)(1-x^3)\dots)$ , und die Faktoren mit geraden Potenzen in  $x$  kürzen sich weg. Die Bijektion finden Sie z.B. bei Van Lint und Wilson [8].

**12.7.6(a).**  $p_0 + p_1 + \dots + p_m$ .

**12.7.6(b).** Es gibt eine bijektive Abbildung dieser Bäume auf die Partitionen von  $m - 1$ : Die Größen der Komponenten nach Entfernen der Wurzel bestimmen die Partition von  $m - 1$ .

**12.7.6(c).**  $\prod_{i=1}^m 1/(1-x^i)^{p_i}$ .

**12.7.6(d).** Wenn man wie im Beweis von Satz 12.7.2 vorgeht, erhält man  $\ln r_n \leq -n \ln x + \sum_{j=1}^{\infty} (P_n(x^j) - 1)/j$ . Im Text wurde gezeigt, dass  $\ln P_n(x) \leq Cx/(1-x)$ . Setzen Sie  $x = 1 - \frac{c}{\ln n}$ , und wählen Sie  $c > 0$  klein genug. Dann ist  $-n \ln x$  ungefähr  $\frac{n}{c \ln n}$ , und dann ist immer noch ein gewisses Geschick nötig um zu zeigen, dass die Summe  $\sum_{j=1}^{\infty} (e^{Cx^j/(1-x^j)} - 1)/j$  von ungefähr der gleichen Größenordnung ist wie ihr erster Summand (also etwa  $n^{c \cdot C}$ ).

**12.7.6(e).** Betrachten Sie Bäume von besonderer Gestalt, an deren Wurzel  $k$  Teilbäume mit jeweils  $q$  Blättern hängen. Deren Anzahl ist mindestens  $p_q^k/k!$ . Verwenden Sie aus dem Text die Abschätzung für  $p_n$  und wählen Sie  $k$  und  $q$  passend.

**13.1.1(b).** Dieses Problem ist im Wesentlichen dual zu Aufgabe 9.1.8.

**13.2.2.** Jede Zeile der Matrix  $AB$  ist eine Linearkombination der Zeilen der Matrix  $B$  (mit Koeffizienten, die durch die entsprechende Zeile von  $A$  gegeben sind), deshalb ist  $r(AB) \leq r(B)$ .

**13.2.3.** Dass eine quadratische Matrix nicht singulär ist, ist äquivalent dazu, dass ihre Determinante nicht Null ist, und die Definition der Determinante ist vom zu Grunde liegenden Körper unabhängig. Den Rang einer nicht quadratischen Matrix kann man als die Größe der größten nicht singulären quadratischen Untermatrix beschreiben.

**13.2.4(a).** Hätte sie Rang  $< n$ , dann besäße das lineare Gleichungssystem  $Mx = 0$  eine nicht triviale Lösung, und so eine Lösung erfüllt  $x^T Mx = 0$ .

**13.2.4(b).**  $M$  ist Summe einer Diagonalmatrix  $D$  mit lauter positiven Einträgen auf der Diagonalen und einer Matrix  $L$ , deren Einträge alle  $\lambda > 0$  sind. Für jedes von Null verschiedene  $x \in \mathbb{R}^v$  haben wir  $x^T Dx > 0$  und  $x^T Lx \geq 0$ .

**13.2.6(a).** Wenn  $A$  die Inzidenzmatrix des Mengensystems ist, dann ist  $A^T A$  Summe einer Matrix  $Q$ , deren Einträge alle  $q$  sind, und einer Diagonalmatrix  $D$ , deren Diagonaleinträge  $|C_i| - q > 0$  sind (wenn  $|C_i| > q$ ). Deshalb ist  $A^T A$  positiv definit und also nicht singulär.

**13.2.6(b).** Betrachten Sie in der Situation der Fisher–Ungleichung das zu  $(V, \mathcal{B})$  duale Mengensystem und wenden Sie (a) an.

**13.3.2(b).** Beweisen Sie mittels Induktion über  $k$ : Wenn  $E$  eine Vereinigung der Kantenmengen von  $k$  bipartiten Graphen auf der Eckenmenge  $\{1, 2, \dots, n\}$  ist, dann gibt es eine Menge mit mindestens  $\lceil n/2^k \rceil$  Ecken, zwischen denen keine Kante aus  $E$  verläuft.

**13.5.2(b).** Falsch.

**13.6.2.** Ein Vorschlag: Wenn  $r(x)$  Grad  $d$  hat, berechnen Sie  $r(z) - p(z)q(z)$  für eine zufällig gewählte Zahl  $z$  aus der Menge  $\{1, 2, \dots, 2d\}$ . Ist das Ergebnis 0, dann ist  $r(x) - p(x)q(x)$  mit Wahrscheinlichkeit mindestens  $\frac{1}{2}$  das Nullpolynom.

**13.6.4.** Angenommen,  $0 \in S$ . Setzen Sie  $a \circ b = 0$  für alle  $a, b \in S$ , mit einer einzigen Ausnahme:  $x \circ y = x$  für irgendwelche  $x, y \in S \setminus \{0\}$ .

**13.6.7(a).** Wenn alle Tripel  $(a, b, c)$  mit  $b \in G^{(k)}$  assoziativ sind, dann sind auch alle Tripel mit  $b \in G^{(k+1)}$  assoziativ.

**13.6.7(c).** Starten Sie mit  $G_1 = \{g_1\}$  für ein beliebiges  $g_1 \in S$ , führen Sie Buch über  $\langle G_k \rangle$ , und setzen Sie  $G_{k+1} = G_k \cup \{g_{k+1}\}$  für irgendein  $g_{k+1} \in S \setminus \langle G_k \rangle$ . Nach (b) verdoppelt sich die Größe von  $\langle G_k \rangle$  in jedem Schritt. Der Beweis, dass  $\langle G_k \rangle$  in der gewünschten Zeit gehandhabt werden kann, braucht dann noch eine gute Idee.

# Stichwortverzeichnis

---

$\binom{V}{2}$ , 120	$A^T$ , 436
$\binom{X}{k}$ , 74(3.3.1)	$G + \bar{e}$ , 158(4.6.2)
$\binom{n}{k}$ , 73	$G\%e$ , 158(4.6.2)
$\binom{n}{k_1, \dots, k_m}$ , 79	$G - e$ , 157(4.6.2)
$\prec$ , 48	$G - v$ , 158(4.6.2)
$\preceq$ , 47	$G.e$ , 235(4.6.2)
$\sum$ , 9, 13	$G \cong H$ , 124(4.1.2)
$\prod$ , 9	$\overline{ab}$ , 290
$a   b$ , 49(2.1.2)	$\Delta_X$ , 42
$(a, b)$ , 8	$\Omega(\cdot)$ , 91
$[a, b]$ , 8	$\Theta(\cdot)$ , 91
$\lfloor x \rfloor$ , 8	$\alpha(n)$ , 186
$\lceil x \rceil$ , 9	$\alpha(G)$ , 341(10.4.2)
$\{x, y\}$ , 11	$\alpha(P)$ , 60
$(x, y)$ , 11	$\chi(\cdot)$ , 229(6.4.2)
$\emptyset$ , 12	$\delta p$ , 420
$2^X$ , 13	$\delta(\cdot)$ , 237(Aufg. 2)
$\subseteq$ , 14	$\omega(G)$ , 351
$\subset$ , 14	$\omega(P)$ , 60
$ X $ , 13, 35(Aufg. 7)	$\pi$ , 99
$X^2$ , 16	Berechnung, 100(Aufg. 8)
$X \dot{\cup} Y$ , 14	$\pi(n)$ , 105(3.6.3)
$X \times Y$ , 16	
$\{\dots\}$ , 10	$A_G$ , 132(4.2.3)
$R[x]$ , 44	Abbildung, siehe Funktion
$R^{-1}$ , 42	Abschluss, transitiver,
$R \circ S$ , 38	45(Aufg. 4)
$xRy$ , 36	Abstand (in Graphen), 132
$f(X)$ , 30	adjazente Ecken, 121
$f(x)$ , 29	Adjazenzmatrix, 37, 132(4.2.3)
$f^{-1}$ , 34	Äquivalenzrelation, 42(1.6.2)
$f: X \rightarrow Y$ , 29	Anzahl, 117(Aufg. 8)
$f: X \hookrightarrow Y$ , 32	Datenstruktur, 186(5.3.4),
$f: x \mapsto y$ , 29	187(Aufg. 1)
$f \sim g$ , 91	äußerer Land, 204

- affine Ebene, 299(Aufg. 10), 406, 407(Aufg. 2)
- Algebra, lineare (Anwendung), 274–284, 301–304, 382(Aufg. 16), 401–433
- Algorithmus
  - Borůvka, 197(5.5.3)
  - Greedy, 190(5.4.2), 192, 194(Aufg. 10), 194(Aufg. 11), 194(Aufg. 12)
  - Jarník, 195(5.5.1)
  - Kruskal, 190(5.4.2)
  - Prim, siehe
    - Jarník–Algorithmus
  - QUICKSORT, 345–348
  - randomisierter, 424
  - Sortier-, 73(Aufg. 6), 345–348
- Antikette, 60, 251, 257(Aufg. 5)
- antisymmetrische Relation, 41(1.6.1)
- Anzahl
  - Abbildungen, 65(3.1.1)
  - Äquivalenzrelationen, 117(Aufg. 8)
  - Alkyradikale, 387(Aufg. 12)
  - Anordnungen, 79
  - aufspannende Bäume, siehe Anzahl Bäume
    - für beliebige Graphen, 274(8.5.1)
  - Bäume, 264–288
    - mit gegebener Gradfolge, 266(8.2.1)
    - nicht isomorphe, 182(Aufg. 6), 265(Aufg. 1), 399(Aufg. 6)
  - binäre Bäume, 383–385
  - binäre Wurzelbäume, 387(Aufg. 11)
  - geordnete  $k$ -Tupel, 82(Aufg. 17)
- gepflanzte Bäume, 387(Aufg. 8), 387(Aufg. 9)
- gerade Mengen, 417(13.4.4)
- Graphen, 118(Aufg. 13), 125
  - nicht isomorphe, 126, 128(Aufg. 8)
- injektive Abbildungen, 68(3.1.4)
- Kanten eines ebenen Graphen, 221(6.3.3)
- Kugelverteilungen, 75, 83(Aufg. 18)
- Lösungen, 75, 359
- lateinische Rechtecke, 310(Aufg. 6)
- monotone Funktionen, 81(Aufg. 7)
- Partitionen von  $n$ , 393–400
- surjektive Abbildungen, 116(Aufg. 7)
- Teiler, 117(Aufg. 11)
- Teilmengen, 66(3.1.2), 74(3.3.2), 82(Aufg. 16)
  - ungerade, 67(3.1.3), 78
- Triangulierungen (eines Vielecks), 84(Aufg. 24), 386(Aufg. 6)
- ungeordnete  $k$ -Tupel, 82(Aufg. 17)
- arithmetisches Mittelwert, 95
- assoziativ (Operation), 14, 438
- asymmetrisch
  - Baum, 181(Aufg. 1)
  - Graph, 127(Aufg. 3)
- asymptotische Analyse, 88
- aufspannender Baum, 182–188
  - Algorithmus, 183(5.3.2), 187(5.3.5)
  - maximal, 193(Aufg. 1)
  - minimal, 188–200
- aufspannender Wald, 415
- aufsteigendes Segment einer Permutation, 72(Aufg. 5)

- Ausgrad, 152  
 außerplanarer Graph,  
     237(Aufg. 3)  
 Automorphismus  
     eines Graphen, 127(Aufg. 3)  
     eines Poset, 254, 257(Aufg. 5)  
 azyklische Relation, 52(Aufg. 2)
- $\mathcal{B}_n$ , 59
- Bäume, Anzahl, 182(Aufg. 6),  
     264–288, 383–385,  
     387(Aufg. 8),  
     387(Aufg. 9),  
     387(Aufg. 11),  
     399(Aufg. 6)
- Basis, 440
- Baum, 169(5.1.1)  
     asymmetrischer, 181(Aufg. 1)  
     aufspannender, 182–188  
         Algorithmus, 183(5.3.2)  
         minimal, 188–200  
     binärer, 383–385  
     Code, 176  
     gepflanzter, 176  
     Steiner, 189  
     Wurzel-, 176
- Bedeckung, Kanten-,  
     194(Aufg. 11)
- Bedingungen an Parameter,  
     404(13.1.3)
- Bell-Zahl, 117(Aufg. 8),  
     374(Aufg. 15)
- Bernoulli-Ungleichung, 101
- Bertrandsches Postulat, 106
- Betti-Zahl, siehe zyklomatische Zahl
- Bijektion, 31(1.4.3)
- Bild, 29
- binäre Operation, 427, 438
- binärer Baum, 383–385
- Binet–Cauchy, Satz, 281(8.5.4)
- Binomialkoeffizient, 73–84,  
     360–361, 362(Aufg. 6)
- Näherung, 101–106
- verallgemeinerter, 365(12.2.3)
- Binomialsatz, 77(3.3.3)  
     kombinatorische Bedeutung,  
     360
- verallgemeinerter, 365(12.2.3),  
     384
- bipartiter Graph, 123,  
     135(Aufg. 4),  
     285(Aufg. 4)  
     vollständiger, 122
- Blatt, 171
- Blockplan, 404, 406
- Bonferroni–Ungleichung, 111
- Boolesche Funktion, 316,  
     321(Aufg. 1)
- Borsuk–Ulam, Satz, 246
- Borůvka, Algorithmus,  
     197(5.5.3)
- Breitensuche, 132
- Brouwerscher Fixpunktsatz,  
     244(7.1.3), 249(Aufg. 5)
- $C(G)$ , 180
- $C_n$ , 122
- $C_n$ , 324(10.2.2)
- Catalan-Zahl, 385–386
- Cauchy–Schwarzsche Ungleichung,  
     259(7.3.2), 262(Aufg. 4)
- Cayley–Formel, 264(8.1.1)
- charakteristische Funktion, 67
- charakteristisches Polynom, 378
- chromatische Zahl, 229(6.4.2),  
     237(Aufg. 2)  
     listen-, 239(Aufg. 12)
- Code  
     eines Baums, 176  
     Prüfer, 270
- $d_G(\cdot, \cdot)$ , 132
- Datenstruktur für Äquivalenzrelationen,  
     186(5.3.4), 187(Aufg. 1)
- de Bruijn Graph, 155
- de Moivre, Satz, 397
- de Morgansche Gesetze, 15

- $\deg_G(\cdot)$ , 136
- $\deg_G^+(\cdot)$ , 152
- $\deg_G^-(\cdot)$ , 152
- Dérangement, 113
- Design, 401–409
- Determinante, 437
  - entwickeln, 437
- Diagonale, 42, 436
- Diagonalmatrix, 436
- Diagramm
  - Ferrers, 393
  - Hasse, 51
  - Pfeil-, 28
- Differenz, symmetrische, 415
- Digraph, siehe gerichteter Graph
- Dilworth, Satz, 63(Aufg. 7)
- Dimension, 440
- distributiv (Operation), 15, 439
- dominierende Menge, 194(Aufg. 12)
- doppeltes Abzählen, 74, 240–263, 299(Aufg. 8), 405
- dreiecksfreier Graph, 163–167, 341
- Dreiecksmatrix, 436
- dual
  - Graph, 231(6.4.3)
  - aufspannende Bäume, 265(Aufg. 4)
  - projektive Ebene, 296
- Dualität, 296, 304
- Durchmesser, 135(Aufg. 8)
  
- E**, 335(10.3.6)
- $e$ , 96
- $E(G)$ , 120
- Ebene
  - affine, 299(Aufg. 10), 406, 407(Aufg. 2)
  - Fano, 292
  - projektive, siehe projektive Ebene
- ebene Zeichnung, 202(6.1.1)
- ebener Graph, 201–239
  
- Gradfolge, 224(6.3.4)
- Kantenzahl, 221(6.3.3)
- maximal, 221(6.3.3)
- Ecke, 119(4.1.1)
  - Zusammenhangszahl, 157
- Eigenschaft B, 311
- Einbettung
  - eines Graphen, 202(6.1.1)
  - geordneter Mengen, 57(2.3.1)
- Eingrad, 152
- Einheitsmatrix, 436
- Element
  - größtes, 55(2.2.4)
  - kleinstes, 55(2.2.4)
  - maximales, 53(2.2.2)
  - Maximum, 55
  - minimales, 53(2.2.2)
  - Minimum, 55
- elementare Zeilenoperation, 437
- Elementarkreis, 416
- endliche projektive Ebene, 289–313
  - Definition, 289(9.1.1), 298(Aufg. 4), 299(Aufg. 8), 406(Aufg. 1)
  - Existenz, 300–301
  - Ordnung, 295(9.1.4)
- endlicher Wahrscheinlichkeitsraum, 322(10.2.1)
- Entwickeln (Determinante), 437
- Erdős–Szekeres–Lemma, 61(2.4.6)
- Erdős, Paul, 350
- Ereignis, 323
- Ereignisse, unabhängige, 329–331
- Ergebnis, 322
- Erwartungswert, 333–349, 388
  - Definition, 335(10.3.6)
  - Linearität, 336(10.3.9)
- Erweiterung, lineare, 53
- erzeugende Funktion, 358–400
  - exponentielle, 373(Aufg. 14)
  - Operationen, 366–369

- zu einer Folge, 364(12.2.2)
- Euler
  - Formel, 217(6.3.1)
    - für Bäume, 170(5.1.2)
  - Funktion, 114–116,
    - 117(Aufg. 9)
  - Tour, 143
  - Zahl, 96
- Eulerscher Graph, 142–156,
  - 209(Aufg. 3)
- $\text{ex}_G(\cdot)$ , 180
- exponentielle erzeugende Funktion, 373(Aufg. 14)
- extremale Graphentheorie, 166, 258, 341
- Exzentrizität, 180
- Färbung
  - einer Landkarte, 227–239
  - eines Graphen, 229(6.4.2)
  - Listen-, 239(Aufg. 12)
- Fakultät, 71
  - Näherung, 93–99, 100(Aufg. 9)
  - Teilbarkeit, 73(Aufg. 7)
- Fano–Ebene, 292, 310(Aufg. 1)
- Ferrers–Diagramm, 393
- Fibonacci–Zahl, 375–377
- Fisher–Ungleichung, 407(13.2.1), 410(Aufg. 6)
- Fixpunkt, 113, 338(Aufg. 3)
  - satz, 243(7.1.2), 244(7.1.3)
- Flasche, Kleinsche, 204
- Folge, monotone, 62
- Formel
  - Cayley, 264(8.1.1)
  - de Moivre, 25(Aufg. 4)
  - Euler, 217(6.3.1)
    - für Bäume, 170(5.1.2)
  - Heawood, 236
  - Leibniz, 82(Aufg. 13)
  - logische, 316, 321(Aufg. 1)
  - Stirling, 99
- Fortsetzung, lineare, 84(Aufg. 27)
- Freivalds–Test, 424(13.6.1)
- Funktion, 28(1.4.1)
  - Anzahl, 65(3.1.1)
  - bijektive, 31(1.4.3)
  - Boolesche, 316, 321(Aufg. 1)
  - charakteristische, 67
  - erzeugende, 358–400
    - exponentielle, 373(Aufg. 14)
  - Operationen, 366–369
  - zu einer Folge, 364(12.2.2)
- Euler, 114–116, 117(Aufg. 9)
- Graph, 269, 270(Aufg. 1), 270(Aufg. 3)
- Identität, 34(Aufg. 4)
- injektive, 31(1.4.3)
  - Anzahl, 68(3.1.4)
- konvexe, 262(Aufg. 5)
- lineare, 441
- monotone, 81(Aufg. 7)
- Periode, 270(Aufg. 3)
- surjektive, 31(1.4.3)
  - Anzahl, 116(Aufg. 7)
- $GF(q)$ , 439
- $GF(2)$ , 415
- $\mathcal{G}_n$ , 327(10.2.4)
- ganze Zahlen, 8
- Garderobenfrau–Problem, 112(3.8.1), 374(Aufg. 17)
- Rekursion, 116(Aufg. 4), 116(Aufg. 5)
- Gebiet, siehe Land
  - Jordankurve, 210(6.2.1)
- geometrischer Mittelwert, 95
- geordnet
  - Menge, 47–63
  - Paar, 11
- gepflanzter Baum, 176
- Gerüst (eines Polytops), 221
- Gerade
  - einer projektiven Ebene, 290(9.1.1)
  - uneigentliche, 291
- gerade Menge, 414(13.4.1)
  - Anzahl, 417(13.4.4)

- gerichtet  
 Graph, 151(4.5.1)  
 Kante, 151(4.5.1)  
 Kreis, 152  
 Tour, 152  
 Geschlecht, 208(6.1.3)  
 $ggT(m, n)$ , 114  
 goldener Schnitt, 376, 391  
 größtes Element, 55(2.2.4)  
 Grad (einer Ecke), 136  
 Gradfolge, 136  
   eines Baumes, 174(Aufg. 8)  
   eines ebenen Graphen,  
     224(6.3.4)  
   eines Graphen, 136–141  
 Graham–Pollak, Satz,  
     411(13.3.1)  
 Graph, 119(4.1.1)  
   Anzahl, 118(Aufg. 13), 125  
   nicht isomorphe,  
     128(Aufg. 8)  
   asymmetrischer, 127(Aufg. 3)  
   außerplanarer, 237(Aufg. 3)  
   bipartiter, 123, 135(Aufg. 4),  
     285(Aufg. 4)  
   vollständiger, 122  
   chromatische Zahl, 229(6.4.2),  
     237(Aufg. 2)  
 de Bruijn, 155  
 dreiecksfreier, 163–167,  
     348(Aufg. 1)  
 dualer, 231(6.4.3)  
   aufspannende Bäume,  
     265(Aufg. 4)  
 Durchmesser, 135(Aufg. 8)  
 ebener, 201–239  
   Gradfolge, 224(6.3.4)  
   Kantenzahl, 221(6.3.3)  
   maximal, 221(6.3.3)  
 $k$ -eckenzusammenhängender,  
     156  
 Einbettung, 202(6.1.1)  
 einer Abbildung, 269,  
   270(Aufg. 1),  
   270(Aufg. 3)  
 Eulerscher, 142–156,  
     209(Aufg. 3)  
 Färbung, 229(6.4.2)  
 gerichteter, 151(4.5.1)  
 Heawood, 142(Aufg. 15), 296  
 Inzidenz-, 296, 312  
 Isomorphismus, 123(4.1.2)  
 Kanten-, 150(Aufg. 8)  
 $k$ -kantenzusammenhängender,  
     156  
 Kneser, 126, 127(Aufg. 1)  
 listenchromatische Zahl,  
     239(Aufg. 12)  
 Metrik, 132  
   mit Mehrfachkanten, 147  
   mit Schlingen, 148  
   ohne  $K_k$ , 341  
   ohne  $K_{2,2}$ , 258, 312  
   ohne  $K_{2,t}$ , 261(Aufg. 1)  
   ohne  $K_{3,3}$ , 263(Aufg. 6)  
   orientierter, 151  
   Orientierung, 278  
 Petersen, 126, 127(Aufg. 1)  
 Radius, 135(Aufg. 8)  
 regulärer, 142(Aufg. 12)  
 schwach zusammenhängender,  
     153(4.5.2)  
 stark zusammenhängender,  
     153(4.5.2)  
 topologischer, 202(6.1.1)  
 tough, 163(Aufg. 6)  
 vollständiger, 122  
 vollständiger  $k$ -partiter,  
     167(Aufg. 3)  
 Zeichnung, 121, 202(6.1.1)  
 zufällig Eulersch,  
     150(Aufg. 10)  
 Zufalls-, 327(10.2.4),  
     332(Aufg. 4),  
     332(Aufg. 3)  
 zusammenhängender, 130  
 2-zusammenhängender,  
     157–163  
 kritisch, 162(Aufg. 2)

- Greedy–Algorithmus, 190(5.4.2),  
   192, 194(Aufg. 10),  
   194(Aufg. 11),  
   194(Aufg. 12)  
 Grötsch, Satz, 237(Aufg. 4)  
 Gruppe, 438
- Halbordnung, 48  
 Hamiltonsch  
   Kreis, 149(Aufg. 7),  
     188(Aufg. 3)  
   Weg, 156(Aufg. 8)  
 Handshake Lemma, 138  
   Anwendungen, 240–248  
 harmonisch  
   Mittelwert, 100(Aufg. 6)  
   Zahl, 86(3.4.1), 101(Aufg. 13)  
 Hasse–Diagramm, 51  
 Hauptdiagonale, 436  
 Heawood  
   Formel, 236  
   Graph, 142(Aufg. 15), 296  
 Hintereinanderausführung  
   von Funktionen, 30  
 Hülle, lineare, 441  
 Hypergraph, 402
- $I_n$ , 436  
 Identität, 34(Aufg. 4)  
 Indikatorfunktion, 336(10.3.7)  
 Induktion, 18  
 induzierter Teilgraph, 129(4.2.1)  
 $\inf A$ , 56(Aufg. 9)  
 Infimum, 56(Aufg. 9)  
 injektive Abbildung, 31(1.4.3)  
   Anzahl, 68(3.1.4)  
 Inklusion–Exklusion, 106–112,  
   332(Aufg. 2)  
   Anwendungen, 112–118  
 innere Länder, 204  
 inverse Relation, 42  
 Inversion (einer Permutation),  
   73(Aufg. 6)  
 Inzidenzgraph, 296, 312
- Inzidenzmatrix, 278,  
   285(Aufg. 4), 408, 421  
 Isomorphismus  
   von Bäumen, 175–181  
   von Graphen, 123(4.1.2)  
   von Posets, 52(Aufg. 4), 254
- $J_n$ , 412  
 Jarník, Algorithmus, 195(5.5.1)  
 Jensensche Ungleichung,  
   262(Aufg. 5)  
 Jordan–Schönflies–Theorem, 211  
 Jordankurve, 209  
 Jordanscher Kurvensatz,  
   210(6.2.1)
- $K_G$ , 414  
 $K_n$ , 122  
 $K_{n,m}$ , 122  
 Kante, 119(4.1.1)  
   Bedeckung, 194(Aufg. 11)  
   gerichtete, 151(4.5.1)  
   Gewicht, 189  
   Kontraktion, 235  
   Mehrfach-, 147  
   Unterteilung, 158(4.6.2)  
   Zusammenhang, 156  
 Kantengraph, 150(Aufg. 8)  
 kartesisches Produkt, 16  
 Kern, 441  
 Kette, 55(Aufg. 2), 60(2.4.4), 251  
   symmetrische, 253  
 Kleinsche Flasche, 204  
 kleinstes Element, 55(2.2.4)  
 Kneser–Graph, 126, 127(Aufg. 1)  
 Knoten (in einem Graphen),  
   siehe Ecke  
 Koeffizient  
   Binomial-, 73–84, 360–361,  
     362(Aufg. 6)  
   verallgemeinerter,  
     365(12.2.3)  
   Multinomial-, 80  
 Körper, 439  
   Platonischer, 218

- Kohlenwasserstoffe, Anzahl, 387(Aufg. 12)
- kommutativ (Operation), 15, 438
- Kompaktheit, 245
- Komplement, 135(Aufg. 1)
- Komplexität (eines Algorithmus), 184
- Komponente, 131
- Komposition
  - von Funktionen, 30
  - von Relationen, 38
- Konfiguration, taktische, 404
- Kontraktion, 235
- konvex
  - Funktion, 262(Aufg. 5)
  - Körper, 218
- Kreis, 122
  - Elementar-, 416
  - Hamiltonscher, 149(Aufg. 7), 188(Aufg. 3)
  - in einem Graphen, 130
- kritisch 2-zusammenhängender Graph, 162(Aufg. 2)
- Kruskal, Algorithmus, 190(5.4.2)
- Kuratowski, Satz, 215(6.2.4)
- Kurve, 201
  - Jordan-, 209
- Land (eines ebenen Graphen), 203
- Landkarte (Färbung), 227–239
- Laplace-Matrix, 274, 284(Aufg. 1)
- lateinisch
  - Quadrat, 306–310
  - Quadrate, orthogonale, 307
  - Rechteck, 310(Aufg. 6)
- leer
  - Menge, 12
  - Produkt, 13
  - Summe, 13
- Leibniz-Formel, 82(Aufg. 13)
- Lemma
  - Erdős-Szekeres, 61(2.4.6)
- Sperner, 241(7.1.1), 249(Aufg. 5)
- lexikographische Ordnung, 48, 179
- linear
  - Abbildung, 441
  - abhängig (Menge), 440
  - Algebra (Anwendung), 274–284, 301–304, 382(Aufg. 16), 401–433
  - Erweiterung, 53
  - Fortsetzung, 84(Aufg. 27)
  - Hülle, 441
  - Ordnung, 42(1.6.2)
  - unabhängig, 440
- Linearität des Erwartungswertes, 336(10.3.9)
- Linksmaximum, 334(10.3.4), 337
- listenchromatische Zahl, 239(Aufg. 12)
- Listenfärbung, 239(Aufg. 12)
- Littlewood–Offord–Problem, 257(Aufg. 6)
- logische Formel, 316, 321(Aufg. 1)
- LYM-Ungleichung, 252
- Mader, Satz, 163(Aufg. 7)
- Markov–Ungleichung, 339(Aufg. 7)
- Matching, 194(Aufg. 10)
- Matrix, 435
  - Diagonal-, 436
  - Einheits-, 436
  - Inzidenz-, 278, 285(Aufg. 4), 408, 421
  - Laplace, 274, 284(Aufg. 1)
  - Multiplikation, 133(4.2.4), 435
    - Test, 424(13.6.1)
  - nicht singuläre, 438
  - Permutations-, 136(Aufg. 12)
  - positiv definite, 410(Aufg. 4)
  - Rang, 409, 438
  - total unimodulare, 285(Aufg. 4)

- transponierte, 436
- Matroid, 193, 423
- maximal aufspannender Baum, 193(Aufg. 1)
- maximales Element, 53(2.2.2)
- Maximum, 55
- Mehrfachkanten, 147
- Menge
  - dominierende, 194(Aufg. 12)
  - geordnete, 47–63
  - leere, 12
  - partiell geordnete, 48
  - unabhängige, 60(2.4.1), 341, 351
  - zusammenhängende, 203
- $n$ -Menge, 65
- Mengenfamilie, 12
- Mengensystem, 12
  - 2-färbbares, 311, 318–320, 321(Aufg. 2)
- Menger, Satz, 159
- Metrik, 132, 135(Aufg. 7)
- metrischer Raum, 132
- minimal aufspannender Baum, 188–200
- minimales Element, 53(2.2.2)
- Minimum, 55
- Minor, 216, 238(Aufg. 11)
- Mittelwert
  - arithmetisches, 95
  - geometrisches, 95
  - harmonisches, 100(Aufg. 6)
- Möbiusband, 204
- monochromatisch, 319
- monotone Folge, 62
- monotone Funktion (Anzahl), 81(Aufg. 7)
- Multigraph, 147
- Multinomialkoeffizient, 80
- Multinomialsatz, 80(3.3.5), 267, 362(Aufg. 4)
- $\mathbb{N}$ , 8
- Nachbar, 121
- Näherung
- Binomialkoeffizient, 101–106
- Fakultät, 93–99, 100(Aufg. 9)
- natürliche Zahlen, 8
- Netzwerk, 189
- nichtsinguläre Matrix, 438
- $O(\cdot)$ , 89(3.4.2)
- $o(\cdot)$ , 91
- Ohrenzerlegung, 161
- Operation, binäre, 427, 438
- Ordnung, 42(1.6.2)
  - einer Permutation, 72(Aufg. 3)
  - einer projektiven Ebene, 295(9.1.4)
  - eines Lateinischen Quadrats, 306
  - lexikographische, 48, 179
  - lineare, 42(1.6.2)
  - partielle, 48
  - totale, 42(1.6.2)
- orientierter Graph, 151
- Orientierung, 155(Aufg. 4), 278
- orthogonal
  - lateinische Quadrate, 307
  - Vektoren, 436
- $P(\cdot)$ , 322(10.2.1)
- $p_n$ , 393
- $P_n$ , 122
- $\mathcal{P}(X)$ , 13
- Paar
  - geordnetes, 11
  - ungeordnetes, 11
- Parameter
  - Bedingungen, 404(13.1.3)
  - eines Designs, 402
- Partialbruchzerlegung, 376
- partielle Ordnung, 48
- Partition
  - von  $n$ , 393–400
  - geordnete, 393, 398(Aufg. 1)
- Pascalsches Dreieck, 77
- perfekte Zahl, 117(Aufg. 11)
- Periode einer Funktion, 270(Aufg. 3)

- Permutation, 70–73
  - aufsteigendes Segment, 72(Aufg. 5)
- Fixpunkt, 113, 338(Aufg. 3), 374(Aufg. 17)
- Inversion, 73(Aufg. 6)
- Linksmaximum, 334(10.3.4), 337
- Matrix, 136(Aufg. 12)
- Ordnung, 72(Aufg. 3)
- Signum, 437
- zufällige, 73, 113, 325(10.2.3), 330, 338, 341
- Zyklus, 71, 338
- Petersen–Graph, 126, 127(Aufg. 1)
- Pfeildiagramm, 28
- Platonische Körper, 218
- Polynom, charakteristisches, 378
- Polytop, reguläres, 218
- Poset, 48, 250
  - Automorphismus, 254, 257(Aufg. 5)
  - Isomorphismus, 52(Aufg. 4), 254
- positiv definite Matrix, 410(Aufg. 4)
- Postulat von Bertrand, 106
- Potenzial, 156(Aufg. 5), 420
- Potenzialdifferenz, 420
- Potenzmenge, 13
- Potenzreihe, 362–364, 373(Aufg. 13)
- Prim, Algorithmus, siehe Jarník–Algorithmus
- Primzahlsatz, 105(3.6.3)
- Prinzip
  - Inklusion–Exklusion, 106–112, 332(Aufg. 2)
    - Anwendungen, 112–118
  - Schubfach, 352(11.1.2)
- probabilistische Beweise, 314–349
- Problem
- Garderobenfrau, 112(3.8.1), 374(Aufg. 17)
- Rekursion, 116(Aufg. 4), 116(Aufg. 5)
- Littlewood–Offord, 257(Aufg. 6)
- maximal aufspannender Baum, 193(Aufg. 1)
- minimal aufspannender Baum, 190(5.4.1)
- Sylvester, 226(Aufg. 8)
- Vier–Farben, 228
- Produkt, 9
  - kartesisches, 16
  - leeres, 13
  - Skalar-, 436
- Projektion, stereographische, 208
- projektive Ebene
  - Dualität, 296, 304
  - endliche, 289–313
    - Definition, 289(9.1.1), 298(Aufg. 4), 299(Aufg. 8), 406(Aufg. 1)
    - Existenz, 300–301
    - Ordnung, 295(9.1.4)
  - Konstruktion, 301–304, 308–309
    - reelle, 290, 301
  - Prüfer Code, 270
- Punkt
  - einer projektiven Ebene, 290(9.1.1)
  - uneigentlicher, 290
- Quadrat, lateinisches, 306–310
- quadratische Matrix, 436
- QUICKSORT, 345–348
- $\mathbb{R}$ , 8
- $\mathcal{R}$ , 420
- $r(A)$ , 438
- $r(k, \ell)$ , 353
- Radius, 135(Aufg. 8)
- Ramsey, Satz, 352(11.2.1)

- für  $p$ -Tupel, 354(Aufg. 5)
- Ramsey-Zahl, 353
- randomisierter Algorithmus, 424
- Rang (einer Matrix), 409, 438
- rationale Zahlen, 8
- Raum
  - metrischer, 132
  - Schnitt-, 420
  - Strom-, 420
  - Wahrscheinlichkeits-
    - endlicher, 322(10.2.1)
    - unendlicher, 324
  - Zyklen-, 415(13.4.3)
- Rechteck, lateinisches, 310(Aufg. 6)
- reelle projektive Ebene, 290, 301
- reelle Zahlen, 8
- reflexive Relation, 41(1.6.1)
- regulär
  - Graph, 142(Aufg. 12)
  - Polytop, 218
- Reihe, Potenz-, 362–364, 373(Aufg. 13)
- Rekursion, 377–380
- Relation, 36(1.5.1)
  - Äquivalenz-, 42(1.6.2)
  - antisymmetrische, 41(1.6.1)
  - azyklische, 52(Aufg. 2)
  - inverse, 42
  - reflexive, 41(1.6.1)
  - symmetrische, 41(1.6.1)
  - transitive, 41(1.6.1), 73(Aufg. 6)
- Verknüpfung, 38
- $\mathcal{S}$ , 420
- $S_n$ , 113
- $\mathcal{S}_n$ , 325(10.2.3)
- Satz
  - Binet–Cauchy, 281(8.5.4)
  - Binomial-
    - kombinatorische Bedeutung, 360
    - verallgemeinerter, 365(12.2.3), 384
- Borsuk–Ulam, 246
- Brouwer, 244(7.1.3), 249(Aufg. 5)
- de Moivre, 25(Aufg. 4), 397
- Dilworth, 63(Aufg. 7)
- Fixpunkt-, 243(7.1.2), 244(7.1.3)
- Gradfolgen, 138(4.3.3)
- Graham–Pollak, 411(13.3.1)
- Grötsch, 237(Aufg. 4)
- Jordan–Schönflies, 211
- Jordanscher Kurven-, 210(6.2.1)
- Kuratowski, 215(6.2.4)
- Mader, 163(Aufg. 7)
- Menger, 159
- Multinomial-, 80(3.3.5), 267, 362(Aufg. 4)
- Primzahl-, 105(3.6.3)
- Ramsey, 352(11.2.1)
  - für  $p$ -Tupel, 354(Aufg. 5)
- Sperner, 250(7.2.1)
- Steinitz, 221
- Turán, 167(Aufg. 4), 341(10.4.2), 348(Aufg. 4)
- Wilson, 406(13.1.5)
- Schlinge, 148
- Schnitt, 420
  - goldener, 376, 391
- Schnittpunkt  $k$ -ter Ordnung, 342–345, 349(Aufg. 9)
- Schnittraum, 420
- Schubfachprinzip, 352(11.1.2)
- schwach zusammenhängender Graph, 153(4.5.2)
- Seitenfläche (eines Polytops), 219
- $\text{sgn}(\pi)$ , 437
- Signum einer Permutation, 437
- Skalarprodukt, 436
- Sohn (in Wurzelbaum), 176
- Sortieralgorithmus, 73(Aufg. 6), 345–348
- Sortierung, topologische, 54

- Spannung, 420
- Spaziergang, 131
- Sperner, Satz, 250(7.2.1)
- Sperner–Lemma, 241(7.1.1),  
249(Aufg. 5)
- Sphäre mit Henkeln, 204
- stark zusammenhängender  
Graph, 153(4.5.2)
- Steiner–Baum, 189
- Steiner–System, 403(13.1.2),  
404, 405(13.1.4),  
407(Aufg. 4)
- Steinitz, Satz, 221
- stereographische Projektion, 208
- Stirling–Formel, 99
- Strom, 419
- Stromraum, 420
- Summe, 9, 13
  - leere, 13
- sup  $A$ , 56(Aufg. 9)
- Supremum, 56(Aufg. 9)
- surjektive Abbildung, 31(1.4.3)
- Sylvester, Problem, 226(Aufg. 8)
- symmetrische
  - Differenz, 415
  - Kette, 253
  - Relation, 41(1.6.1)
- $T(\cdot)$ , 264
- taktische Konfiguration, 404
- Teilfolge, 62
- Teilgraph, 129(4.2.1)
  - induziert, 129(4.2.1)
- Teilmengen
  - Anzahl, 66(3.1.2), 74(3.3.2),  
82(Aufg. 16)
- Tiefensuche, 132
- topologische Sortierung, 54
- topologischer Graph, 202(6.1.1)
- Torus, 204
- total unimodulare Matrix,  
285(Aufg. 4)
- totale Ordnung, 42(1.6.2)
- tough (Graph), 163(Aufg. 6)
- Tour, 144
- Eulersche, 143
- gerichtete, 152
- Träger, 419
- transitiv
  - Abschluss, 45(Aufg. 4)
  - Relation, 41(1.6.1),  
73(Aufg. 6)
- transponierte Matrix, 436
- Triangulierung, 221(6.3.3)
  - eines Vielecks, 84(Aufg. 24),  
386(Aufg. 6)
- Turán, Satz, 167(Aufg. 4),  
341(10.4.2),  
348(Aufg. 4)
- Turnier, 156(Aufg. 8), 331
- unabhängig
  - Ereignisse, 329–331
  - Menge, 60(2.4.1), 341, 351
- Unabhängigkeitssystem, 250
- ungeordnetes Paar, 11
- Ungleichung
  - Bernoulli, 101
  - Bonferroni, 111
  - Cauchy–Schwarz, 259(7.3.2),  
262(Aufg. 4)
  - Fisher, 407(13.2.1),  
410(Aufg. 6)
  - Jensen, 262(Aufg. 5)
  - LYM, 252
  - Markov, 339(Aufg. 7)
- uniformes (Mengensystem), 402
- UNION–FIND, 186(5.3.4),  
187(Aufg. 1)
- Unterkörper, 439
- Untermatrix, 438
- Unterraum, 441
- Unterteilung (eines Graphen),  
158(4.6.2)
- $V(G)$ , 120
- Varianz, 389(Aufg. 1)
- Variation, 69
- Vater (in Wurzelbaum), 176
- Vektoren, orthogonale, 436

- Vektorraum, 440
- verallgemeinerter Binomialsatz, 365(12.2.3), 384
- Verknüpfung
  - von Funktionen, 30
  - von Relationen, 38
- Vier-Farben-Problem, 228
- vollständig
  - bipartiter Graph, 122
  - Graph, 122
  - Induktion, 18
  - $k$ -partiter Graph, 167(Aufg. 3)
- Wahrscheinlichkeit, 73(Aufg. 5), 94, 113, 118(Aufg. 12), 314–349, 356–357, 388–393
- Wahrscheinlichkeitsraum
  - endlicher, 322(10.2.1)
  - unendlicher, 324
- Wald, 183
  - aufspannender, 415
- Weg, 122, 130
  - eindeutiger, 170(5.1.2)
  - Hamiltonscher, 156(Aufg. 8)
  - Zufalls-, 389–393
- wegzusammenhängende Menge, 203
- Wilson, Satz, 406(13.1.5)
- Wohlordnung, 19
- Würfel (Graph), 155
- Wurzelbaum, 176
- $\mathbb{Z}$ , 8
- $\mathcal{Z}$ , 415
- Zahl
  - Bell, 117(Aufg. 8), 374(Aufg. 15)
  - Betti, siehe zyklomatische Zahl
  - Catalan, 385–386
  - chromatische, 229(6.4.2) listen-, 239(Aufg. 12)
- Eulersche, 96
- Fibonacci, 375–377
- ganze, 8
- harmonische, 86(3.4.1), 101(Aufg. 13)
- natürliche, 8
- perfekte, 117(Aufg. 11)
- Ramsey, 353
- rationale, 8
- reelle, 8
- zyklomatische, 418
- Zeichnung eines Graphen, 202(6.1.1)
- Zeilenoperation, elementare, 437
- Zeitkomplexität, 184
- Zentroid, 182(Aufg. 7)
- Zentrum eines Graphen, 180
- zufällig Eulerscher Graph, 150(Aufg. 10)
- zufällige Permutation, 73, 113, 325(10.2.3), 330, 338, 341
- Zufallsgraph, 327(10.2.4), 332(Aufg. 4), 332(Aufg. 3)
- Zufallsvariable, 333(10.3.1)
- Zufallsweg, 389–393
- zusammenhängend
  - Graph, 130
  - Menge, 203
- Zusammenhang
  - schwacher, 153(4.5.2)
  - starker, 153(4.5.2)
- Zusammenhangszahl, 157
- 2-Färbung, 311, 318–320, 321(Aufg. 2)
- 2-zusammenhängender Graph, 157–163
  - kritisch, 162(Aufg. 2)
- Zyklenraum, 415(13.4.3)
- zyklomatische Zahl, 418
- Zyklus
  - einer Permutation, 71, 338