

Springer 大学数学图书——影印版

DISCRETE MATHEMATICS

Elementary and Beyond

离散数学

基础与提高

L. Lovász J. Pelikán K. Vesztergombi 著



TSINGHUA
UNIVERSITY PRESS



Springer

Springer 大学数学图书——影印版

DISCRETE MATHEMATICS
Elementary and Beyond

离散数学

基础与提高

L. Lovász J. Pelikán K. Vesztergombi 著



TSINGHUA
UNIVERSITY PRESS

北京



Springer

内 容 提 要

本书包括组合、图论及它们在优化和编码等领域的应用。全书只有约 300 页,但涵盖了信息领域一些广泛而有趣的应用,及离散数学领域新颖而前沿的研究课题。

本书非常适合计算机科学、信息与计算科学等专业作为“离散数学”引论课程的教材或参考书。

L. Lovász, J. Pelikán, K. Vesztergombi
Discrete Mathematics: Elementary and Beyond
EISBN: 0-387-95584-4

Copyright © 2003 by Springer-Verlag New York, Inc.

Original Language published by Springer-Verlag. All Rights Reserved.

本书原版由 Springer-Verlag 出版。版权所有,盗印必究。

Tsinghua University Press is authorized by Springer-Verlag to publish and distribute exclusively this English language reprint edition. This edition is authorized for sale in the People's Republic of China only (excluding Hong Kong, Macao SAR and Taiwan). Unauthorized export of this edition is a violation of the Copyright Act. No part of this publication may be reproduced or distributed by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.

本英文影印版由 Springer-Verlag 授权清华大学出版社独家出版发行。此版本仅限在中华人民共和国境内(不包括中国香港、澳门特别行政区及中国台湾地区)销售。未经授权的本书出口将被视为违反版权法的行为。未经出版者预先书面许可,不得以任何方式复制或发行本书的任何部分。

北京市版权局著作权合同登记号 图字:01-2006-5263

版权所有,翻印必究。举报电话:010-62782989 13501256678 13801310933

图书在版编目(CIP)数据

离散数学:基础与提高=Discrete Mathematics: Elementary and Beyond/罗瓦茨(Lovász, L.), 培理肯(Pelikán, J.), 维斯特冈比(Vesztergombi, K.)著. —影印本. —北京:清华大学出版社, 2006.9

(Springer 大学数学图书)

ISBN 7-302-13826-5

I. 离… II. ①罗… ②培… ③维… III. 离散数学-英文 IV. O158

中国版本图书馆 CIP 数据核字(2006)第 109953 号

出 版 者:清华大学出版社

<http://www.tup.com.cn>

社总机:010-6277 0175

地 址:北京清华大学学研大厦

邮 编:100084

客户服务:010-6277 6969

责任编辑:陈朝晖

印 装 者:清华大学印刷厂

发 行 者:新华书店总店北京发行所

开 本:155×235 印张:19.25

版 次:2006 年 9 月第 1 版 2006 年 9 月第 1 次印刷

书 号:ISBN 7-302-13826-5/O · 574

印 数:1~5000

定 价:39.00 元

Springer 大学数学图书——翻译版

- 信息和编码理论 (Information and Coding Theory)
Jones, Gareth A., Jones, J. Mary
- 对称 (Symmetries)
Johnson, D. L.
- 矩阵群 (Matrix Groups)
Baker, Andrew
- 生物数学引论 (Essential Mathematical Biology)
Britton, Nicholas F.
- 狭义相对论 (Special Relativity)
Woodhouse, N.M.J.
- 高等微积分 (Second Year Calculus)
Bressoud, David M.
- 线性泛函分析 (Linear Functional Analysis)
Rynne, Bryan P., Youngson, Martin A.
- 离散数学引论 (A First Course in Discrete Mathematics)
Anderson, Ian
- 离散数学 (Discrete Mathematics)
Lovász, L., Pelikán, J., Vesztegombi, K.
- 数学的读写和证明 (Reading, Writing, and Proving)
Daepp, Ulrich, Gorkin, Pamela
- 随机过程基础 (Basic Stochastic Processes)
Brzezniak, Zdzislaw, Zastawniak, Tomasz
- 代数基本定理 (The Fundamental Theorem of Algebra)
Fine, Benjamin, Rosenberger, Gerhard

注：前有“○”者为将要出版的图书，前有“●”者为已经出版的图书。

Springer 大学数学图书——影印版

- Information and Coding Theory (信息和编码理论)
Jones, Gareth A., Jones, J. Mary
- Symmetries (对称)
Johnson, D. L.
- Matrix Groups (矩阵群)
Baker, Andrew
- Essential Mathematical Biology (生物数学引论)
Britton, Nicholas F.
- Special Relativity (狭义相对论)
Woodhouse, N.M.J.
- Second Year Calculus (高等微积分)
Bressoud, David M.
- Linear Functional Analysis (线性泛函分析)
Rynne, Bryan P., Youngson, Martin A.
- A First Course in Discrete Mathematics (离散数学引论)
Anderson, Ian
- **Discrete Mathematics (离散数学)**
Lovász, L., Pelikán, J., Vesztegombi, K.
- Reading, Writing, and Proving (数学的读写和证明)
Daepp, Ulrich, Gorkin, Pamela
- Basic Stochastic Processes (随机过程基础)
Brzezniak, Zdzisław, Zastawniak, Tomasz
- The Fundamental Theorem of Algebra (代数基本定理)
Fine, Benjamin, Rosenberger, Gerhard

注：前有“○”者为将要出版的图书，前有“●”者为已经出版的图书。

序 言

在学校教书多年，当学生（特别是本科生）问有什么好的参考书时，我们所能推荐的似乎除了教材还是教材，而且不同教材之间的差别并不明显，特色也不鲜明。所以多年前我们就开始酝酿，希望为本科学生引进一些好的参考书，为此清华大学数学科学系的许多教授与清华大学出版社共同付出了很多心血。

这里首批推出的十余本图书，是从 Springer 出版社的多个系列丛中精心挑选出来的。在丛书的筹划过程中，我们挑选图书最重要的标准并不是完美，而是有特色并包容各个学派（有些书甚至有争议，比如从数学上看也许不够严格），其出发点是希望我们的学生能够吸纳百家之长；同时，在价格方面，我们也做了很多工作，以使得本系列丛书的价格能让更多学校和学生接受，使得更多学生能够从中受益。

本系列的图书按其定位，大体有如下四种类型（一本书可以属于多类，但这里限于篇幅不能一一介绍）。

一、适用面比较广、有特色并可以用作教材或参考书的图书。例如：

● Lovász et al.: Discrete Mathematics. 2003

该书是离散数学的入门类型教材。与现有的教材（包括国外的教材）相比，它涵盖了离散数学新颖而又前沿的研究课题，同时还涉及信息科学方面既基本又有趣的应用；在着力打好数学基础的同时，也强调了数学与信息科学的关联。姚期智先生倡导和主持的清华大学计算机科学试验班，已经选择该书作为离散数学课程的教材。

二、在目前国内的数学教育中，课程主要以学科的纵向发展为主线，而对数学不同学科之间的联系讨论很少，学生缺乏把不同学科视为一个数学整体的训练，这方面的读物尤其欠缺。这是本丛书一个重要的着力点。最典型的是：

● Fine/Rosenberger: The Fundamental Theorem of Algebra. 1997

该书对数学中最重要的定理——代数基本定理给出了六种证明，方法涉及到分析、代数与拓扑；附录中还给出了 Gauss 的证明和 Cauchy 的证明。全书以一个数学问题为主线展开，纵横数学的核心领域；结构严谨、文笔流畅、浅显易懂、引人

入胜，是一本少见的能够让读者入迷的好读物，用它来引导学生欣赏和领会“数学的美”绝对不会落于空谈。该书适于自学、讨论，也是极好的短学期课程教材。

● **Baker: Matrix Groups. 2001**

就内容而言，本书并不超出我国大学线性代数、抽象代数和一般拓扑学课程的内容，但是本书所讲的是李群和李代数的基础理论——这是现代数学和物理学非常重要的工具。各种矩阵群和矩阵代数是李群和李代数最典型和最重要的例子，同时也能帮助学生建立数学不同学科的联系。从矩阵出发，既能把握李群和李代数的实质，又能学会计算和运用，所以这是一本不可多得的好书。

三、科学与技术的发展不断为数学提出新的研究课题，因此在数学学科的发展过程中，来自其他学科的推动力是不能忽视的。本系列中第三种类型的读物就是强调数学与其他学科的联系。例如：

● **Woodhouse: Special Relativity. 2003**

该书将物理与数学有机结合，体现了物理学家伽利略的名言：“大自然是一部用数学语言写成的巨著。”不仅如此，本书作者还通过对线性代数、微积分、场论等数学的运用进一步强调并贯穿这样的观点：数学的真谛和发展存在并产生于物理或自然规律及其发现中。精读此书有助于理解物理学和数学的整体关系。

● **Britton: Essential Mathematical Biology. 2003**

生命科学在本世纪一定会有很大发展，其对数学的需求和推动是可以预见的。因此生物数学在应用数学中占有日益重要的地位，数学系培养的学生至少一部分人应当对这个领域有所了解。随着生命科学的迅速发展，生物数学也发展很快。本书由浅入深，从经典的问题入手，最后走向学科前沿和近年的热点问题。该书至少可以消除学生对生物学的神秘感。

四、最后一类是适合本科学生的课外读物。这类图书对激发和引导学生学习数学的兴趣会非常有帮助，而且目前国内也急需这样的图书。例如：

● **Daepf/Gorkin: Reading, Writing and Proving. 2003**

该书对初学高等数学的读者来说特别有意义。它的基本出

发点是引导读者以研究的心态去学习,让读者养成独立思考的习惯,并进而成为研究型的学习者。该书将一个学习数学的过程在某种意义下程序化,努力让学习者养成一个好的学习习惯,以及学会如何应对问题。这里的程序化并不是机械,目的是在于培养习惯。该书特色鲜明,类似的图书确实很少。

● **Brzezniak/Zastawniak: Basic Stochastic Processes. 1999**

随机过程在数学、科学和工程中有越来越广泛的应用,本书适合国内的需要。其主要特点是:习题是巩固和延伸学习内容的基本手段,而且有十分完整的解答,非常适合自学和作为教学参考书。这是一本难得的好书,它 1999 年出版,到 2000 年已经是第 3 次印刷,到 2003 年则第 6 次重印。

本系列丛书中的大部分图书还将翻译为中文出版,以适应更多读者的需要。丛书筹划过程中,冯克勤、郑志勇、卢旭光、郑建华、王殿军、杨利军、叶俊、扈志明等很多清华大学的教授都投入了大量精力,他们之中很多人也将是后面中文版的译者。此外,我们今后还将不断努力丰富引进丛书的种类,同时也会将选书的范围在可能情况下进一步扩大到其他高水平的出版机构。

教育是科学和技术发展的基石,数学教育更是基石的基础。因为是基础所以它重要;也因为基础所以它显示度不高,容易不被重视。只有将人才培养放到更高的地位上,中国成为创新型国家的目标才会成为可能。

本系列丛书的正式推出,圆了一个我们多年的梦,但这无疑仅仅是开始。

白峰杉

2006 年 6 月于清华园

L. Lovász
J. Pelikán
K. Vesztergombi

Discrete Mathematics

Elementary and Beyond

With 95 Illustrations



Springer

Undergraduate Texts in Mathematics

Editors

S. Axler

F.W. Gehring

K.A. Ribet

Springer

New York

Berlin

Heidelberg

Hong Kong

London

Milan

Paris

Tokyo

Preface

For most students, the first and often only course in college mathematics is calculus. It is true that calculus is the single most important field of mathematics, whose emergence in the seventeenth century signaled the birth of modern mathematics and was the key to the successful applications of mathematics in the sciences and engineering.

But calculus (or analysis) is also very technical. It takes a lot of work even to introduce its fundamental notions like continuity and the derivative (after all, it took two centuries just to develop the proper definition of these notions). To get a feeling for the power of its methods, say by describing one of its important applications in detail, takes years of study.

If you want to become a mathematician, computer scientist, or engineer, this investment is necessary. But if your goal is to develop a feeling for what mathematics is all about, where mathematical methods can be helpful, and what kinds of questions do mathematicians work on, you may want to look for the answer in some other fields of mathematics.

There are many success stories of applied mathematics outside calculus. A recent hot topic is mathematical cryptography, which is based on number theory (the study of the positive integers $1, 2, 3, \dots$), and is widely applied, for example, in computer security and electronic banking. Other important areas in applied mathematics are linear programming, coding theory, and the theory of computing. The mathematical content in these applications is collectively called *discrete mathematics*. (The word “discrete” is used in the sense of “separated from each other,” the opposite of “continuous;” it is also often used in the more restrictive sense of “finite.” The more everyday version of this word, meaning “circumspect,” is spelled “discreet.”)

The aim of this book is not to cover “discrete mathematics” in depth (it should be clear from the description above that such a task would be ill-defined and impossible anyway). Rather, we discuss a number of selected results and methods, mostly from the areas of combinatorics and graph theory, with a little elementary number theory, probability, and combinatorial geometry.

It is important to realize that there is no mathematics without *proofs*. Merely stating the facts, without saying something about why these facts are valid, would be terribly far from the spirit of mathematics and would make it impossible to give any idea about how it works. Thus, wherever possible, we will give the proofs of the theorems we state. Sometimes this is not possible: quite simple, elementary facts can be extremely difficult to prove, and some such proofs may take advanced courses to go through. In these cases, we will at least state that the proof is highly technical and goes beyond the scope of this book.

Another important ingredient of mathematics is *problem solving*. You won’t be able to learn any mathematics without dirtying your hands and trying out the ideas you learn about in the solution of problems. To some, this may sound frightening, but in fact, most people pursue this type of activity almost every day: Everybody who plays a game of chess or solves a puzzle is solving discrete mathematical problems. The reader is strongly advised to answer the questions posed in the text and to go through the problems at the end of each chapter of this book. Treat it as puzzle solving, and if you find that some idea that you came up with in the solution plays some role later, be satisfied that you are beginning to get the essence of how mathematics develops.

We hope that we can illustrate that mathematics is a building, where results are built on earlier results, often going back to the great Greek mathematicians: that mathematics is alive, with more new ideas and more pressing unsolved problems than ever: and that mathematics is also an art, where the beauty of ideas and methods is as important as their difficulty or applicability.

László Lovász

József Pelikán

Katalin Vesztergombi

Contents

Preface	xiii
1 Let's Count!	1
1.1 A Party	1
1.2 Sets and the Like	4
1.3 The Number of Subsets	9
1.4 The Approximate Number of Subsets	14
1.5 Sequences	15
1.6 Permutations	17
1.7 The Number of Ordered Subsets	19
1.8 The Number of Subsets of a Given Size	20
2 Combinatorial Tools	25
2.1 Induction	25
2.2 Comparing and Estimating Numbers	30
2.3 Inclusion-Exclusion	32
2.4 Pigeonholes	34
2.5 The Twin Paradox and the Good Old Logarithm	37
3 Binomial Coefficients and Pascal's Triangle	43
3.1 The Binomial Theorem	43
3.2 Distributing Presents	45
3.3 Anagrams	46
3.4 Distributing Money	48

3.5	Pascal's Triangle	49
3.6	Identities in Pascal's Triangle	50
3.7	A Bird's-Eye View of Pascal's Triangle	54
3.8	An Eagle's-Eye View: Fine Details	57
4	Fibonacci Numbers	65
4.1	Fibonacci's Exercise	65
4.2	Lots of Identities	68
4.3	A Formula for the Fibonacci Numbers	71
5	Combinatorial Probability	77
5.1	Events and Probabilities	77
5.2	Independent Repetition of an Experiment	79
5.3	The Law of Large Numbers	80
5.4	The Law of Small Numbers and the Law of Very Large Numbers	83
6	Integers, Divisors, and Primes	87
6.1	Divisibility of Integers	87
6.2	Primes and Their History	88
6.3	Factorization into Primes	90
6.4	On the Set of Primes	93
6.5	Fermat's "Little" Theorem	97
6.6	The Euclidean Algorithm	99
6.7	Congruences	105
6.8	Strange Numbers	107
6.9	Number Theory and Combinatorics	114
6.10	How to Test Whether a Number is a Prime?	117
7	Graphs	125
7.1	Even and Odd Degrees	125
7.2	Paths, Cycles, and Connectivity	130
7.3	Eulerian Walks and Hamiltonian Cycles	135
8	Trees	141
8.1	How to Define Trees	141
8.2	How to Grow Trees	143
8.3	How to Count Trees?	146
8.4	How to Store Trees	148
8.5	The Number of Unlabeled Trees	153
9	Finding the Optimum	157
9.1	Finding the Best Tree	157
9.2	The Traveling Salesman Problem	161
10	Matchings in Graphs	165

10.1 A Dancing Problem	165
10.2 Another matching problem	167
10.3 The Main Theorem	169
10.4 How to Find a Perfect Matching	171
11 Combinatorics in Geometry	179
11.1 Intersections of Diagonals	179
11.2 Counting regions	181
11.3 Convex Polygons	184
12 Euler's Formula	189
12.1 A Planet Under Attack	189
12.2 Planar Graphs	192
12.3 Euler's Formula for Polyhedra	194
13 Coloring Maps and Graphs	197
13.1 Coloring Regions with Two Colors	197
13.2 Coloring Graphs with Two Colors	199
13.3 Coloring graphs with many colors	202
13.4 Map Coloring and the Four Color Theorem	204
14 Finite Geometries, Codes, Latin Squares, and Other Pretty Creatures	211
14.1 Small Exotic Worlds	211
14.2 Finite Affine and Projective Planes	217
14.3 Block Designs	220
14.4 Steiner Systems	224
14.5 Latin Squares	229
14.6 Codes	232
15 A Glimpse of Complexity and Cryptography	239
15.1 A Connecticut Class in King Arthur's Court	239
15.2 Classical Cryptography	242
15.3 How to Save the Last Move in Chess	244
15.4 How to Verify a Password—Without Learning it	246
15.5 How to Find These Primes	246
15.6 Public Key Cryptography	247
16 Answers to Exercises	251
Index	287

1

Let's Count!

1.1 A Party

Alice invites six guests to her birthday party: Bob, Carl, Diane, Eve, Frank, and George. When they arrive, they shake hands with each other (strange European custom). This group is strange anyway, because one of them asks, "How many handshakes does this mean?"

"I shook 6 hands altogether," says Bob, "and I guess, so did everybody else."

"Since there are seven of us, this should mean $7 \cdot 6 = 42$ handshakes," ventures Carl.

"This seems too many" says Diane. "The same logic gives 2 handshakes if two persons meet, which is clearly wrong."

"This is exactly the point: Every handshake was counted twice. We have to divide 42 by 2 to get the right number: 21," with which Eve settles the issue.

When they go to the table, they have a difference of opinion about who should sit where. To resolve this issue, Alice suggests, "Let's change the seating every half hour, until we get every seating."

"But you stay at the head of the table," says George, "since it is your birthday."

How long is this party going to last? How many different seatings are there (with Alice's place fixed)?

Let us fill the seats one by one, starting with the chair on Alice's right. Here we can put any of the 6 guests. Now look at the second chair. If Bob

sits in the first chair, we can put any of the remaining 5 guests in the second chair; if Carl sits in the first chair, we again have 5 choices for the second chair, etc. Each of the six choices for the first chair gives us five choices for the second chair, so the number of ways to fill the first two chairs is $5 + 5 + 5 + 5 + 5 + 5 = 6 \cdot 5 = 30$. Similarly, no matter how we fill the first two chairs, we have 4 choices for the third chair, which gives $6 \cdot 5 \cdot 4$ ways to fill the first three chairs. Proceeding similarly, we find that the number of ways to seat the guests is $6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$.

If they change seats every half hour, it will take 360 hours, that is, 15 days, to go through all the seating arrangements. Quite a party, at least as far as the duration goes!

1.1.1 How many ways can these people be seated at the table if Alice, too, can sit anywhere?

After the cake, the crowd wants to dance (boys with girls, remember, this is a conservative European party). How many possible pairs can be formed?

OK, this is easy: there are 3 girls, and each can choose one of 4 boys, this makes $3 \cdot 4 = 12$ possible pairs.

After ten days have passed, our friends really need some new ideas to keep the party going. Frank has one: "Let's pool our resources and win the lottery! All we have to do is to buy enough tickets so that no matter what they draw, we will have a ticket with the winning numbers. How many tickets do we need for this?"

(In the lottery they are talking about, 5 numbers are selected out of 90.)

"This is like the seating," says George. "Suppose we fill out the tickets so that Alice marks a number, then she passes the ticket to Bob, who marks a number and passes it to Carl, and so on. Alice has 90 choices, and no matter what she chooses, Bob has 89 choices, so there are $90 \cdot 89$ choices for the first two numbers, and going on similarly, we get $90 \cdot 89 \cdot 88 \cdot 87 \cdot 86$ possible choices for the five numbers."

"Actually, I think this is more like the handshake question," says Alice. "If we fill out the tickets the way you suggested, we get the same ticket more than once. For example, there will be a ticket where I mark 7 and Bob marks 23, and another one where I mark 23 and Bob marks 7."

Carl jumps up: "Well, let's imagine a ticket, say, with numbers 7, 23, 31, 34, and 55. How many ways do we get it? Alice could have marked any of them: no matter which one it was that she marked, Bob could have marked any of the remaining four. Now this is really like the seating problem. We get every ticket $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$ times."

"So," concludes Diane, "if we fill out the tickets the way George proposed, then among the $90 \cdot 89 \cdot 88 \cdot 87 \cdot 86$ tickets we get, every 5-tuple occurs not