计算机科学组合学丛书

组合数学

（第3版）

卢开澄　卢华明

清华大学出版社

计算机科学组合学丛书

组 合 数 学

（第3版）

卢开澄　卢华明

清华大学出版社

内 容 简 介

本书是《组合数学》(第二版)的修订版。全书共有6章,分别是:排列与组合,母函数与递推关系,容斥原理与鸽巢原理,贝恩塞特引理与波利亚定理,区组设计与编码,组合算法与复杂性分析。本书内容取舍得当,理论联系实际。

本书是计算机系本科生和研究生的教学用书,也可作为数学专业师生的教学参考书。

图书在版编目(CIP)数据

组合数学/卢开澄等著. —3版. —北京:清华大学出版社,2002
(计算机科学组合学丛书)
ISBN 7-302-04581-X

Ⅰ. 组… Ⅱ. 卢… Ⅲ. 组合数学 Ⅳ. 0157

中国版本图书馆CIP数据核字(2002)第045422号

出版者:清华大学出版社(北京清华大学学研大厦,邮编 100084)
http://www.tup.tsinghua.edu.cn
印刷者:北京四季青印刷厂
发行者:新华书店总店北京发行所
开 本:850×1168 1/32 **印张**:15.75 **字数**:392千字
版 次:2002年7月第3版
书 号:ISBN 7-302-04581-X/TP·2714
印 数:12001~17000
定 价:19.80元

计算机科学组合学丛书

前　言

电子计算机的出现是20世纪的大事，它改变了我们这个世界的面貌。可以毫不夸张地说，它的影响遍及所有的角落，几乎无处不感觉到它的存在。数学更不例外。严格地说，电子计算机本身就是近代数学的辉煌成就。将计算机与数学割裂开来，既不合理也不可能。组合学也就是在计算机科学蓬勃发展的刺激下崛起的，从而成为近若干年来最活跃的数学分支。它研究的问题有的可追溯到欧拉和哈密尔顿等18世纪的数学家，但它成为一个新的分支还是近若干年的事。它从与计算机科学相结合中获得了广阔的发展空间，从而也为计算机科学奠定了理论基础。

什么是计算机科学呢？有的学者将它定义为研究算法的一门学科。研究算法无疑是计算机科学的重要领域，也是本丛书的核心内容，贯穿始终。组合学家在20世纪70年代初建立的算法复杂性"NP理论"，至今仍然令无数计算机科学工作者与数学工作者为之折腰。

计算机科学里的组合学内容十分广泛。本丛书涉及组合分析、图论、组合算法、近代密码学、编码理论及算法复杂性等7部分。

组合分析是算法的理论基础。组合分析之于组合算法犹如数学分析于与计算数学，众所周知，前者是后者的理论根基。

图论原来是组合数学这个"家族"的主要成员，只因它已成长壮大，故自立门户独立出去。

算法复杂性的NP理论是近30年的一大成就。研究表明，对

于一类叫做 NPC 类的困难问题，至今都不存在有效算法，但它们难度相当，只要其中任何一个找到多项式解法，则全体都获得解决；或证明它们根本不存在有效办法。不论是前者还是后者都还看不见露到海平面上的桅杆塔，它吸引了众多的有志之士。密码学是其中十分引人入胜的分支。如若设计好的密码，对它的破译等价于某一 NPC 类困难问题，无疑这样的密码将是牢不可破的。

在计算机网络深入普及的信息时代，信息本身就是时间，就是财富。信息传输通过的是脆弱的公共信道，信息储存于“不设防”的计算机系统中，如何保护信息的安全使之不被窃取乃至于不被篡改或破坏，已成为当今普遍关注的重大问题。密码是有效而且可行的办法。在计算机网络的刺激下，近代密码学便在算法复杂性理论的基础上建立起来了。密码作为一种技术，自从人类有了战争，不久便有了它。但作为一门学科则是近 20 多年的事。甚至于它已成为其他学科的基础。密码也从此走出“军营”，进入百姓家。

实际中的“优化”问题是大量的，半个多世纪以来它曾经几度辉煌。近来在计算机科学的影响下，又出现了若干闪光点，十分耀眼，引人注目。

实际上密码也是一种编码。如果说密码学研究的编码是保证通信的保密与安全，则编码理论研究的是通信中如何纠错与检错。计算机纠错码是既实用、理论上又饶有趣味的分支。

本丛书是作者在清华大学计算机科学与技术系长期工作的总结。它不是一部长篇记述，而是互相关联又彼此相对独立，因此难免有少量交叉。它们涉及的面如此之广，囿于作者的水平，缺点和错误在所难免，敬请读者不吝指正。谢谢。

第3版序言

第3版与第2版不同之点在于将原来第6章的线性规划，换成现在与算法复杂性分析有关的内容，还增加了一些应用实例，删去线性规划是为了给新增加内容让出空间，新增加的部分无疑更贴近计算机科学。

本书各章基本上是互相独立的，比如讲了第1、第2两章后，再讲第5章，也是一种可以采用的方案。

第2章和第6章是由卢华明执笔的。

写在“再版”前的话

转眼间《组合数学(算法与分析)》一书(上、下册)出版已快十年了。一本好的科技书总是要通过使用、修改、再使用、再修改几个反复才能臻于完善。出版社和作者都有出修订版的愿望。正好在此期间,原书上册被选作全国计算机专业的教材,这样两者便结合起来进行。本书问世之日,也是再版修订完成之时。读者不难发现“再版”中有相当数量的新增内容,有的虽材料依旧,但已是重新改写过的。

“组合数学”研究的问题源远流长,有的甚至于可追溯到欧拉等著名数学家。然而它之所以成为最活跃的一个数学分支,则是近年来受计算机科学蓬勃发展的刺激和影响。它从计算机的科学研究中获取了广阔的发展空间。本书是原书上册的再版,所以它仅仅是基础理论部分。基础是重要的,但毕竟不是全体。在它的出版后松一口气之余,余下部分的改写便自然而然地提到日程上来了。我计划在新的一册《算法与复杂性分析:组合算法》一书中继续完成它。

作　者

1991.1.20

引　言

在现代数学的各个分支中，发展最快的当推组合学了。其原因在于它在计算机科学、通信、实验设计、优化等领域有着广泛的应用。应特别指出的是受计算机科学蓬勃发展刺激的结果。

快速电子计算机的出现是20世纪最有影响的一件大事，它改变了这个世界的面貌，以至于无处不感到它的存在。许多过去被认为难以解决的难题，在计算机的支持下迎刃而解，同时又提出更多富有发展前景的新课题。组合数学在这个过程中获得了自己的发展空间。

组合数学所讨论的问题来源于实际，因此从内容来看确实丰富多彩，以至于很难用一句话来概括什么叫“组合数学”。本书只能就它所研究的若干问题进行介绍。大致包括如下几个方面：

1. 计数和枚举。计数是组合数学中主要的内容之一。很多场合需要它，比如计算概率。不仅如此，计算机科学中的算法分析，即对算法的时间、空间进行复杂性分析时，组合数学更是不可或缺的。有的人将组合数学看做是算法分析的理论基础，这是不无道理的。

2. 图论。图论是组合数学中比较成熟的一个分支。成长壮大了以至于可以独立出去。图论研究的问题有的可以追溯到欧拉、哈密尔顿等18世纪的数学家，它成为一个数学分支则是近卅余年的事。图论在网络流理论、电路网络以及计算机科学的研究中担当了十分重要的角色，其中如流动推销员问题等已是著名的组合数学困难问题。

3. 容斥原理与鸽巢原理以及反演公式等。

4. 组合设计，包含实验设计与计算机编码理论等。

5. 组合优化问题。

组合的问题灵活多样。经常听到读者问："学好这门数学有没有什么窍门？"依我的经验，它来源于实际，可先从规模小的模型着手，从实际出发分析它，从中找到规律性的东西，再推及一般，读者不妨一试。

本书各章相对独立，读者学习时可以跳过已经熟悉的内容。

目　录

第1章　排列与组合

1.1　基本计数法则

组合数学在研究计数时经常要用到最基本的两个法则，一个是加法法则，另一个是乘法法则. 以后没有特别说明都假定事件 A 和 B 是无关的两类.

1.1.1　加法法则、乘法法则及排列与组合

1. 加法法则

若具有性质 A 的事件有 m 个，具有性质 B 的事件有 n 个，则具有性质 A 或性质 B 的事件有 $m+n$ 个.

最简单的例子是事件 A 为大于 0 小于 10 的偶数，即 $A=\{2,4,6,8\}$；事件 B 是大于 0 而小于 10 的奇数，而 $B=\{1,3,5,7,9\}$，则大于 0 而小于 10 的整数 $C=\{1,2,3,4,5,6,7,8,9\}$ 共 9 个，大于 0 而小于 10 的整数或为偶数(属于 A)，或为奇数(属于 B)，根据加法法则共有 $4+5=9$ 个.

2. 乘法法则

若具有性质 A 的事件有 m 个，具有性质 B 的事件有 n 个，则具有性质 A 与性质 B 的事件有 mn 个.

例 1.1　设一标识符由两个字符组成：第 1 个字符由 a,b,c,d,e 组成，第 2 个字符由 1,2,3 组成. 依据乘法法则共有 $5\times3=15$ 种产生方式，即

$$a1,a2,a3;b1,b2,b3;c1,c2,c3;d1,d2,d3;e1,e2,e3$$

例 1.2　设 A 到 B 有 3 条不同的路径，B 到 C 也有 3 条不同的