

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。

版权所有,翻印必究。

本书封面贴有清华大学出版社激光防伪标签,无标签者不得销售。

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

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之于计算数学,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版不同之处在于将原来第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

引言	XV
第 1 章 排列与组合	1
1.1 基本计数法则	1
1.1.1 加法法则、乘法法则及排列与组合	1
1.1.2 应用举例	2
1.2 一一对应	5
1.3 排列	11
1.4 圆周排列	15
1.5 组合	16
1.6 排列的生成算法	23
1.6.1 序数法	23
1.6.2 字典序法	26
1.6.3 换位法	28
1.7 组合的生成	30
1.8 允许重复的组合与不相邻的组合	31
1.8.1 允许重复的组合	31
1.8.2 不相邻的组合	33
1.9 组合意义的解释	34
1.10 应用举例	46
1.11 司特林(Stirling)公式	58
1.11.1 瓦利斯(Wallis)公式	58
1.11.2 司特林公式的证明	60

习题	63
第 2 章 母函数与递推关系	68
2.1 母函数的引入	68
2.2 母函数的性质	73
2.2.1 若干基本的母函数	74
2.2.2 基本公式	75
2.3 整数的拆分	80
2.4 费勒斯(Ferrers)图像	85
2.5 关于拆分数 $p(n)$ 的讨论	88
2.5.1 欧拉公式	88
2.5.2 拆分数估计式	94
2.6 指数型母函数	97
2.6.1 问题的提出	97
2.6.2 指数型母函数的引入	99
2.7 递推关系举例	104
2.8 Fibonacci(费卜拉契)数列	115
2.8.1 问题的提出	115
2.8.2 问题的解	116
2.8.3 若干等式	119
2.8.4 优选法	121
2.9 解线性常系数递推关系特征根法	126
2.9.1 二阶线性常系数齐次递推关系	126
2.9.2 一阶、二阶线性常系数非齐次递推关系	133
2.9.3 叠加原理	136
2.10 任意阶齐次递推关系	137
2.11 一般线性常系数非齐次递推关系	145
2.12 应用举例	151
2.13 非线性递推关系举例	176

2.13.1	司特林(Stirling)数	176
2.13.2	卡特朗(Catalan)数	184
2.13.3	举例	189
2.14	递推关系解法的补充	195
	习题	198
第3章	容斥原理与鸽巢原理	207
3.1	容斥原理	207
3.1.1	引论	207
3.1.2	容斥原理的两个基本公式	208
3.1.3	例子	212
3.2	棋盘多项式和有限制条件的排列	219
3.2.1	有限制的排列	219
3.2.2	棋盘多项式	219
3.2.3	有禁区的排列问题	223
3.3	广义的容斥原理	228
3.3.1	问题的引入	228
3.3.2	特殊情况	229
3.3.3	一般公式	231
* 3.3.4	广义容斥原理的证明	235
3.4	广义容斥原理的若干应用	238
* 3.5	第二类司特林数展开式	242
* 3.6	错排问题的推广	244
* 3.7	容斥原理在数论上的应用	246
3.7.1	埃拉托逊斯(Eratosthenes)筛法	246
3.7.2	欧拉函数 $\phi(n)$	248
* 3.8	n 对夫妻问题	249
* 3.9	反演公式	252
3.9.1	反演定理	252

3.9.2 若干应用	256
3.10 鸽巢原理	259
3.10.1 问题的引入	259
3.10.2 一般的鸽巢原理	260
3.11 鸽巢原理的推广	265
3.11.1 推广形式之一	265
3.11.2 例	265
3.11.3 推广形式之二	274
3.12 拉蒙赛(Ramsey)数	275
3.12.1 拉蒙赛问题	275
3.12.2 拉蒙赛数	281
习题	285
第4章 贝恩塞特(Burnside)引理与波利亚(Pólya)定理	294
4.1 群的概念	294
4.1.1 定义	294
4.1.2 群的基本性质	297
4.2 置换群	299
4.3 循环、奇循环与偶循环	305
4.4 贝恩塞特(Burnside)引理	312
4.4.1 若干概念	312
4.4.2 重要定理	315
4.4.3 例	320
4.5 波利亚(Pólya)定理	324
4.6 举例	327
4.7 母函数形式的波利亚定理	336
4.8 图的计数	342
4.9 波利亚定理的若干推广	348
习题	354

第 5 章 区组设计与编码	357
5.1 问题的提出	357
5.2 拉丁方与正交的拉丁方	359
5.2.1 问题的引入.....	359
5.2.2 正交拉丁方及其性质.....	361
5.3 域的概念	363
5.4 Galois 域 $GF(p^n)$	365
5.5 正交拉丁方的构造	368
5.6 正交拉丁方应用举例	372
5.7 均衡不完全的区组设计(BIBD)	374
5.7.1 基本概念.....	374
5.7.2 (b, v, r, k, t) -设计	374
5.8 区组设计的构成方法	380
5.9 斯梯纳三元系	383
5.10 科克曼女生问题.....	386
5.11 有限射影空间.....	387
5.11.1 二维的射影几何.....	387
5.11.2 有限域上的射影空间.....	391
5.12 阿达玛(Hadamard)矩阵	392
5.13 编码理论的基本概念.....	398
5.14 对称二元信道.....	402
5.15 纠错码.....	404
5.15.1 最近邻法则.....	404
5.15.2 汉明不等式.....	405
5.16 若干简单的编码.....	406
5.16.1 重复码.....	406
5.16.2 奇偶校验码.....	407
5.17 线性码.....	408

5.17.1	生成矩阵与校验矩阵·····	408
5.17.2	关于生成矩阵和校验矩阵的定理·····	412
5.17.3	译码步骤·····	413
5.18	汉明码·····	413
5.19	陪集译码法·····	416
5.20	BCH 码 ·····	420
5.21	其他编码技术简介·····	423
5.21.1	利用区组设计纠错码·····	423
5.21.2	利用阿达玛矩阵进行编码·····	424
	习题·····	426
第 6 章	组合算法与复杂性分析·····	432
6.1	归并排序算法 ·····	432
6.1.1	归并排序·····	432
6.1.2	举例·····	433
6.1.3	复杂性分析·····	434
6.2	快速排序 ·····	435
6.2.1	算法的描述·····	435
6.2.2	复杂性分析·····	438
6.3	Ford-Johnson 排序法 ·····	440
6.4	求第 k 个元素 ·····	444
6.5	排序网络 ·····	446
6.5.1	0-1 原理 ·····	447
6.5.2	B_n 网络 ·····	448
6.5.3	复杂性估计·····	449
6.5.4	Batcher 奇偶归并网络 ·····	451
6.6	快速傅里叶变换(FFT) ·····	453
6.6.1	问题的提出·····	453
6.6.2	预备定理·····	454

6.6.3	快速算法·····	455
6.6.4	复杂性分析·····	459
6.7	DFS 算法 ·····	460
6.7.1	算法的引入·····	460
6.8	判决树 ·····	465
6.8.1	银币问题·····	465
6.8.2	举例·····	468
6.9	渡河问题 ·····	472
6.10	TSM 问题与分支定界法 ·····	473
6.11	多段判决·····	478
6.11.1	问题的提出·····	478
6.11.2	最佳原理·····	481
6.11.3	矩阵链积问题·····	481
6.12	NPC 问题 ·····	483

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 $5 \times 3 = 15$ 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