



21 世纪大学本科
计算机专业系列教材

屈婉玲 耿素云 张立昂 编著

离散数学

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

- 根据教育部高教司主持评审的《中国计算机科学与技术学科教程 2002》组织编写
- 与美国 ACM 和 IEEE/CS *Computing Curricula 2004* 同步



清华大学出版社

21世纪大学本科计算机专业系列教材

离散数学

屈婉玲 耿素云 张立昂 编著



清华大学出版社

北京

内 容 简 介

本教材是根据 ACM 和 IEEE/CS 最新推出的 *Computing Curricula 2004*, 以及教育部高等教育司组织评审通过的《中国计算机科学与技术学科教程 2002》中制定的关于“离散数学”的知识结构和体系撰写的。全书共 14 章, 主要包含证明技巧、数理逻辑、集合与关系、函数、图和树、组合计数、初等数论、离散概率和代数系统等内容。本书体系严谨, 选材精炼, 讲解翔实, 例题丰富, 注重与计算机科学技术的实际问题相结合, 并选配了大量难度适当的习题, 适合教学。另外, 本书有配套习题解答与学习指导等辅导用书, 以满足教学需要。

本书适合作为计算机和相关专业本科生“离散数学”的教学用书, 也可以作为对离散数学感兴趣的人的参考书。

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

本书封面贴有清华大学出版社防伪标签, 无标签者不得销售。

本书防伪标签采用特殊防伪技术, 用户可通过在图案表面涂抹清水, 图案消失, 水干后图案复现; 或将表面膜揭下, 放在白纸上用彩笔涂抹, 图案在白纸上再现的方法识别真伪。

图书在版编目(CIP)数据

离散数学/屈婉玲, 耿素云, 张立昂编著. —北京: 清华大学出版社, 2005. 6

(21 世纪大学本科计算机专业系列教材)

ISBN 7-302-10757-2

I. 离… II. ①屈… ②耿… ③张… III. 离散数学—高等学校—教材 IV. O158

中国版本图书馆 CIP 数据核字(2005)第 028041 号

出 版 者: 清华大学出版社

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

社 总 机: 010-62770175

地 址: 北京清华大学学研大厦

邮 编: 100084

客 户 服 务: 010-62776969

责任编辑: 张瑞庆

封面设计: 孟繁聪

印 刷 者: 北京嘉实印刷有限公司

装 订 者: 三河市春园印刷有限公司

发 行 者: 新华书店总店北京发行所

开 本: 185×230 印 张: 25.5 字 数: 535 千字

版 次: 2005 年 6 月第 1 版 2005 年 6 月第 1 次印刷

书 号: ISBN 7-302-10757-2/TP·7161

印 数: 1~5000

定 价: 32.00 元

21 世纪大学本科计算机专业系列教材编委会

名誉主任：陈火旺

主任：李晓明

副主任：钱德沛 焦金生

委员：(按姓氏笔画为序)

马殿富 王志英 王晓东 宁洪 刘辰

孙茂松 李大友 李仲麟 吴朝晖 何炎祥

宋方敏 张大方 张长海 周兴社 侯文永

袁开榜 钱乐秋 黄国兴 蒋宗礼 曾明

廖明宏 樊孝忠

秘书：张瑞庆

本书责任编辑：李晓明

序 言

PREFACE

21 世纪是知识经济的时代,是人才竞争的时代.随着 21 世纪的到来,人类已步入信息社会,信息产业正成为全球经济的主导产业.计算机科学与技术信息产业中占据了最重要的地位,这就对培养 21 世纪高素质创新型计算机专业人才提出了迫切的要求.

为了培养高素质创新型人才,必须建立高水平的教学计划和课程体系.在 20 多年跟踪分析 ACM 和 IEEE 计算机课程体系的基础上,紧跟计算机科学与技术的发展潮流,及时制定并修正教学计划和课程体系是尤其重要的.计算机科学与技术的发展对高水平人才的要求,需要我们从总体上优化课程结构,精炼教学内容,拓宽专业基础,加强教学实践,特别注重综合素质的培养,形成“基础课程精深,专业课程宽新”的格局.

为了适应计算机科学与技术学科发展和计算机教学计划的需要,要采取多种措施鼓励长期从事计算机教学和科技前沿研究的专家教授积极参与计算机专业教材的编著和更新,在教材中及时反映学科前沿的研究成果与发展趋势,以高水平的科研促进教材建设.同时适当引进国外先进的原版教材.

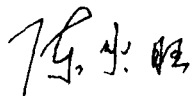
为了提高教学质量,需要不断改革教学方法与手段,倡导因材施教,强调知识的总结、梳理、推演和挖掘,通过加快教案的不断更新,使学生掌握教材中未及时反映的学科发展新动向,进一步拓宽视野.教学与科研相结合是培养学生实践能力的有效途径.高水平的科研可以为教学提供最先进的高新技术平台和创造性的工作环境,使学生得以接触最先进的计算机理论、技术和环境.高水平的科研还可以为高水平人才的素质教育提供良好的物质基础.学生在课题研究中不但能了解科学研究的艰辛和科研工作者的奉献精神,而且能熏陶和培养良好的科研作风,锻炼和培养攻关能力和协作精神.

进入 21 世纪,我国高等教育进入了前所未有的大发展时期,时代的进步与发展对高等教育质量提出了更高、更新的要求.2001 年 8 月,教育部颁发了《关于加强高等学校本科教学工作,提高教学质量的若干意见》.文件指出,本科教育是高等教育的主体和基础,抓好本科教学是提高整个高等教育质量的重点和关键.随着高等教育的普及和高等学校的扩招,在校大学本科计算机专业学生的数量将大量上升,对适合 21 世纪大学本科计算机科学与技术学科课程体系要求的,并且适合中国学生学习的计算机专业教材的需求量

也将急剧增加.为此,中国计算机学会和清华大学出版社共同规划了面向全国高等院校计算机专业本科生的“21世纪大学本科计算机专业系列教材”.本系列教材借鉴美国ACM和IEEE/CS最新制定的*Computing Curricula 2001*(简称CC2001)课程体系,反映当代计算机科学与技术学科水平和计算机科学技术的新发展、新技术,并且结合中国计算机教育改革成果和中国国情.

中国计算机学会教育专业委员会和全国高等学校计算机教育研究会,在清华大学出版社的大力支持下,跟踪分析CC2001,并结合中国计算机科学与技术学科的发展现状和计算机教育的改革成果,研究出了《中国计算机科学与技术学科教程2002》(China Computing Curricula 2002,简称CCC2002),该项研究成果对中国高等学校计算机科学与技术学科教育的改革和发展具有重要的参考价值和积极的推动作用.

“21世纪大学本科计算机专业系列教材”正是借鉴美国ACM和IEEE/CS CC2001课程体系,依据CCC2002基本要求组织编写的计算机专业教材.相信通过这套教材的编写和出版,能够在内容和形式上显著地提高我国计算机专业教材的整体水平,继而提高我国大学本科计算机专业的教学质量,培养出符合时代发展要求的具有较强国际竞争力的高素质创新型计算机人才.



中国工程院院士

国防科学技术大学教授

21世纪大学本科计算机专业系列教材编委会名誉主任

2002年7月

前 言

FOREWORD

科学技术的发展离不开基础研究和创新. 19—20 世纪是人类科学技术飞速发展的时代, 其中作为数学基础的微积分为促进物理学和其他工程学科的发展起到至关重要的作用. 21 世纪是信息时代, 作为信息科学和计算机科学的数学基础, 离散数学受到越来越多的关注. 在美国 ACM 和 IEEE/CS 最新推出的 *Computing Curricula 2004* 课程体系和我国教育部高等教育司组织评审通过的《中国计算机科学与技术学科教程 2002》(CCC2002) 中, 离散数学都被列入核心课程.

离散数学研究各种离散形式的对象, 研究它们的结构及其关系, 在数据结构、算法设计与分析、操作系统、编译系统、人工智能、软件工程、网络与分布式计算、计算机图形学、人机交互、数据库以及计算机体系结构等领域都得到了广泛的应用. 除了计算机科学以外, 在自动化、化学工程、生物学、经济学等各个学科领域中, 都广泛使用数学建模, 而离散数学是数学建模的重要工具之一. 离散数学已经成为计算机科学技术和相关专业的必修课程.

除了作为多门课程必需的数学基础之外, 离散数学中所体现的现代数学思想对于加强学生的素质教育, 培养学生的抽象思维和逻辑表达能力, 提高发现问题、分析问题、解决问题的能力也有着不可替代的作用.

国内外现已出版了各种版本的《离散数学》教材, 取材差异很大, 深浅不一, 风格各异. 本教材是以《中国计算机科学与技术学科教程 2002》中制定的关于离散数学的知识结构和体系为依据撰写的, 主要内容包含证明技巧、数理逻辑、集合与关系、函数、图和树、组合计数、初等数论、离散概率和代数系统等. 在教材编写过程中, 作者力求体系严谨、选材适当、适于教学, 同时在素材组织上更加注重在计算机科学技术中的应用.

全书共分 14 章. 第 1 章介绍全书使用的数学语言(主要是命题逻辑符号和集合运算)与证明方法. 第 2 章和第 3 章分别介绍命题逻辑和一阶逻辑的基本概念、等值演算和推理理论. 第 4 章和第 5 章介绍离散结构的集合表示——关系和函数, 讨论关系和函数的各种运算、性质、表示方法以及应用. 第 6 章和第 7 章介绍离散结构的图形表示——图和树, 包括图的基本概念、图的矩阵表示、特殊图、无向树和有向树及其应用. 第 8 章到第 10 章介

绍组合计数技术及其在计算机科学技术中的应用. 第 11 章到第 13 章介绍初等数论和离散概率及其在密码学和算法分析中的应用. 第 14 章简要介绍离散系统的代数模型. 每章除了阐述相关的概念和定理之外, 还配有典型的例题, 并且选用或编写了数十道难度适当的习题供课后练习使用.

为了更好地为使用本教材的读者服务, 作者还撰写和开发了与本教材配套的教学辅助用书和电子教案.

本书的第 1 章至第 3 章和第 6 章、第 7 章由耿素云编写; 第 4 章、第 5 章、第 8 章至第 10 章和第 14 章由屈婉玲编写; 第 11 章至第 13 章由张立昂编写.

在编写过程中, 作者参考了国内外多种版本的《离散数学》教材和相关的文献资料, 从中吸取了许多好的思想, 摘取了不少有用的素材, 在此一并向有关作者致谢. 感谢“21 世纪大学本科计算机专业系列教材”编委会和清华大学出版社对本书出版的大力支持, 特别要感谢李晓明教授, 他在百忙之中认真地审阅了全稿, 并提出了宝贵的修改意见, 使作者受益匪浅. 我们更期待着广大读者, 特别是用本书作教材的老师 and 学生, 对本书的批评、指正、建议和评论.

作 者

2005 年 2 月于北京大学

目 录

CONTENTS

第 1 章 数学语言与证明方法	1
1.1 常用的数学符号	1
1.1.1 集合符号	1
1.1.2 运算符号	2
1.1.3 逻辑符号	3
1.2 集合及其运算	5
1.2.1 集合及其表示法	5
1.2.2 集合之间的包含与相等	6
1.2.3 集合的幂集	8
1.2.4 集合的运算	8
1.2.5 基本集合恒等式及其应用	11
1.3 证明方法概述	16
1.3.1 逻辑推理的形式结构	16
1.3.2 公理、定理与证明	17
1.3.3 证明方法	19
1.3.4 数学归纳法	24
习题	30
第 2 章 命题逻辑	35
2.1 命题逻辑基本概念	35
2.1.1 命题与联结词	35
2.1.2 命题公式及其分类	42
2.2 命题逻辑等值演算	48
2.2.1 等值式与等值演算	48
2.2.2 联结词完备集	53

2.3	范式	55
2.3.1	析取范式与合取范式	55
2.3.2	主析取范式与主合取范式	58
2.4	命题逻辑推理理论	66
2.4.1	推理的形式结构	66
2.4.2	自然推理系统 P	69
2.4.3	归结证明法	75
	习题	78
第3章	一阶逻辑	84
3.1	一阶逻辑基本概念	84
3.1.1	命题逻辑的局限性	84
3.1.2	个体词、谓词与量词	84
3.1.3	一阶逻辑命题符号化	86
3.1.4	一阶逻辑公式与分类	90
3.2	一阶逻辑等值演算	95
3.2.1	一阶逻辑等值式与置换规则	95
3.2.2	一阶逻辑前束范式	99
3.3	一阶逻辑推理理论	102
3.3.1	一阶逻辑中推理的形式结构	102
3.3.2	量词消去与引入规则	102
3.3.3	自然推理系统 F	104
	习题	107
第4章	关系	113
4.1	关系的定义及其表示	113
4.1.1	有序对与笛卡儿积	113
4.1.2	二元关系的定义	114
4.1.3	二元关系的表示	116
4.2	关系的运算	117
4.2.1	关系的基本运算	117
4.2.2	关系的幂运算	121
4.3	关系的性质	124
4.3.1	关系性质的定义和判别	124

4.3.2	关系的闭包	128
4.4	等价关系与偏序关系	133
4.4.1	等价关系	133
4.4.2	等价类和商集	134
4.4.3	集合的划分	135
4.4.4	偏序关系	137
4.4.5	偏序集与哈斯图	138
	习题	143
第5章	函数	148
5.1	函数的定义及其性质	148
5.1.1	函数的定义	148
5.1.2	函数的像与完全原像	151
5.1.3	函数的性质	151
5.2	函数的复合与反函数	155
5.2.1	函数的复合	155
5.2.2	反函数	157
	习题	158
第6章	图	162
6.1	图的基本概念	162
6.1.1	无向图与有向图	162
6.1.2	顶点的度数与握手定理	164
6.1.3	简单图、完全图、正则图、圈图、轮图、方体图	167
6.1.4	子图、补图	169
6.1.5	图的同构	170
6.2	图的连通性	172
6.2.1	通路和回路	172
6.2.2	无向图的连通性与连通度	173
6.2.3	有向图的连通性及其分类	176
6.3	图的矩阵表示	176
6.3.1	无向图的关联矩阵	177
6.3.2	有向无环图的关联矩阵	177
6.3.3	有向图的邻接矩阵	178

6.3.4	有向图的可达矩阵	180
6.4	几种特殊的图	181
6.4.1	二部图	181
6.4.2	欧拉图	184
6.4.3	哈密顿图	186
6.4.4	平面图	191
	习题	200
第7章	树及其应用	205
7.1	无向树	205
7.1.1	无向树的定义及其性质	205
7.1.2	生成树与基本回路和基本割集	208
7.1.3	最小生成树	211
7.2	根树及其应用	212
7.2.1	根树及其分类	212
7.2.2	最优树与哈夫曼算法	213
7.2.3	最佳前缀码	214
7.2.4	根树的周游及其应用	216
	习题	218
第8章	组合计数基础	222
8.1	基本计数规则	223
8.1.1	加法法则	223
8.1.2	乘法法则	224
8.1.3	分类处理与分步处理	224
8.2	排列与组合	225
8.2.1	集合的排列与组合	225
8.2.2	多重集的排列与组合	229
8.3	二项式定理与组合恒等式	232
8.3.1	二项式定理	232
8.3.2	组合恒等式	233
8.3.3	非降路径问题	237
8.4	多项式定理与多项式系数	240
8.4.1	多项式定理	240

8.4.2 多项式系数	241
习题	242
第9章 容斥原理	245
9.1 容斥原理及其应用	245
9.1.1 容斥原理的基本形式	245
9.1.2 容斥原理的应用	246
9.2 对称筛公式及其应用	250
9.2.1 对称筛公式	250
9.2.2 棋盘多项式与有限制条件的排列	252
习题	256
第10章 递推方程与生成函数	257
10.1 递推方程及其应用	257
10.1.1 递推方程的定义及实例	257
10.1.2 常系数线性齐次递推方程的求解	260
10.1.3 常系数线性非齐次递推方程的求解	263
10.1.4 递推方程的其他解法	265
10.1.5 递推方程与递归算法	270
10.2 生成函数及其应用	272
10.2.1 牛顿二项式定理与牛顿二项式系数	272
10.2.2 生成函数的定义及其性质	273
10.2.3 生成函数的应用	276
10.3 指数生成函数及其应用	281
10.4 Catalan 数与 Stirling 数	284
习题	289
第11章 初等数论	292
11.1 素数	292
11.2 最大公约数与最小公倍数	296
11.3 同余	298
11.4 一次同余方程与中国剩余定理	301
11.4.1 一次同余方程	301
11.4.2 中国剩余定理	303

11.4.3	大整数算术运算	304
11.5	欧拉定理和费马小定理	306
	习题	307
第 12 章	离散概率	312
12.1	随机事件与概率、事件的运算	312
12.1.1	随机事件与概率	312
12.1.2	事件的运算	314
12.2	条件概率与独立性	315
12.2.1	条件概率	315
12.2.2	独立性	317
12.2.3	伯努利概型与二项概率公式	318
12.3	离散型随机变量	319
12.3.1	离散型随机变量及其分布律	319
12.3.2	常用分布	321
12.3.3	数学期望	322
12.3.4	方差	324
12.4	概率母函数	326
	习题	329
第 13 章	初等数论和离散概率的应用	333
13.1	密码学	333
13.1.1	恺撒密码	333
13.1.2	RSA 公钥密码	334
13.2	产生伪随机数的方法	337
13.2.1	产生均匀伪随机数的方法	337
13.2.2	产生离散型伪随机数的方法	338
13.3	算法的平均复杂度分析	340
13.3.1	排序算法	340
13.3.2	散列表的检索和插入	344
13.4	随机算法	348
13.4.1	随机快速排序算法	348
13.4.2	多项式恒零测试	349
13.4.3	素数测试	351

13.4.4 蒙特卡罗法和拉斯维加斯法	352
习题	353
第 14 章 代数系统	356
14.1 二元运算及其性质	356
14.1.1 二元运算与一元运算的定义	356
14.1.2 二元运算的性质	358
14.2 代数系统	362
14.2.1 代数系统的定义与实例	362
14.2.2 代数系统的分类	363
14.2.3 子代数系统与积代数系统	364
14.2.4 代数系统的同态与同构	365
14.3 几个典型的代数系统	367
14.3.1 半群与独异点	367
14.3.2 群	368
14.3.3 环与域	376
14.3.4 格与布尔代数	379
习题	385

第 1 章

数学语言与证明方法

1.1 常用的数学符号

1.1.1 集合符号

$x \in A$ —— x 是 A 的元素.

$x \notin A$ —— x 不是 A 的元素.

$A \subseteq B$ —— A 是 B 的子集, 或 A 包含于 B (B 包含 A).

$A \not\subseteq B$ —— A 不是 B 的子集, 或 B 不包含 A .

$A \subset B$ —— A 是 B 的真子集.

$A = B$ —— A 与 B 有相同的元素.

$A \cup B$ —— A 并 B .

$\bigcup_{i=1}^n A_i$ —— A_1, A_2, \dots, A_n 之并.

$A \cap B$ —— A 交 B .

$\bigcap_{i=1}^n A_i$ —— A_1, A_2, \dots, A_n 之交.

$A - B$ —— B 对 A 的相对补.

$A \oplus B$ —— A 与 B 的对称差.

$P(A)$ —— A 的幂集.

\emptyset —— 空集.

\mathbf{N} —— 自然数集 (含 0).

\mathbf{N}^+ —— 非 0 自然数集.

\mathbf{Z} —— 整数集.

\mathbf{Z}^+ —— 正整数集.

\mathbf{Q} —— 有理数集.

Q^* —— 非零有理数集, 即 $Q - \{0\}$.

R —— 实数集.

R^* —— 非零实数集, 即 $R - \{0\}$.

C —— 复数集.

1.1.2 运算符号

$\sum_{i=1}^n a_i$ —— a_1, a_2, \dots, a_n 之和, 即 $a_1 + a_2 + \dots + a_n$.

$\sum_{i=1}^{\infty} a_i$ —— a_1, a_2, \dots 之和, 即 $a_1 + a_2 + \dots$.

$\prod_{i=1}^n a_i$ —— a_1, a_2, \dots, a_n 之积, 即 $a_1 \cdot a_2 \cdot \dots \cdot a_n$.

$\sum_{i=1}^{\infty} a_i$ —— a_1, a_2, \dots 之积, 即 $a_1 \cdot a_2 \cdot \dots$.

$a \mid b$ —— a 整除 b . 例如, $3 \mid 9, 2 \mid 8, \dots$.

$a \nmid b$ —— a 不能整除 b . 例如, $3 \nmid 8, 2 \nmid 9, \dots$.

$a \equiv b \pmod{n}$ —— a 与 b 被 n 除余数相同. 例如, $4 \equiv 7 \pmod{3}, 1 \equiv 3 \pmod{2}$, 等等.

$(a - b) \equiv 0 \pmod{n}$ —— $n \mid (a - b)$. 例如, $(4 - 7) \equiv 0 \pmod{3}, (5 - 3) \equiv 0 \pmod{2}$, 等等.

其实, $a \equiv b \pmod{n}$ 与 $(a - b) \equiv 0 \pmod{n}$ 意义相同.

$\max(a, b)$ (或 $\max\{a, b\}$) —— 为 a, b 中的大者. 例如, $\max(5, 7) = 7, \max(-5, 8) = 8$, 等等.

$\min(a, b)$ (或 $\min\{a, b\}$) —— 为 a, b 中的小者. 例如, $\min(-2, 5) = -2, \min(5, 7) = 5$, 等等.

$\gcd(a, b)$ —— a 与 b 的最大公约数. 例如, $\gcd(5, 7) = 1, \gcd(3, 27) = 3, \gcd(6, 8, 10) = 2$, 等等.

$\text{lcm}(a, b)$ —— a 与 b 的最小公倍数. 例如, $\text{lcm}(5, 7) = 35, \text{lcm}(2, 4, 8) = 8, \text{lcm}(3, 4, 27) = 108$, 等等.

$|x|$ —— x 的绝对值 (x 为任意实数), 即

$$|x| = \begin{cases} x & \text{当 } x \geq 0 \text{ 时} \\ -x & \text{当 } x < 0 \text{ 时} \end{cases}$$

例如, $|-2.5| = 2.5, |3.3| = 3.3, |0| = 0$.

$[x]$ —— 大于等于 x 的最小整数. 例如, $[-2.2] = -2, [-2] = -2, [-1.5] = -1$,