高等学校计算机专业教材精选·数理基础

离散数学及其应用

周忠荣 主编　林伟初　江定汉　袁 燕　周志轩　编

清华大学出版社

高等学校计算机专业教材精选·数理基础

离散数学及其应用

周忠荣 主编
林伟初 江定汉 袁 燕 周志轩 编

清华大学出版社
北京

内 容 简 介

本书系统阐述了离散数学的经典内容，包括命题逻辑、谓词逻辑、集合、关系、代数系统、图论等方面的基本知识。本书根据计算机科学各专业的需要选择内容、把握尺度，尽可能将离散数学知识和计算机科学中的实际问题相结合。本书编排新颖，每章通过定义、定理、实例、例等形式将内容有机结合、融会贯通，达到学练兼顾的目的。本书加入了机上实现内容，满足了普通高校理工类本科生的实际需求。

本书书末还提供了离散数学常用符号、中英文名词术语对照表、英中文名词术语对照表以及习题答案与提示，能很好地帮助读者理解和学习。

本书既可作为应用型本科和高职高专院校计算机科学各专业的教材，也可作为工程技术人员的参考书。

图书在版编目（CIP）数据

离散数学及其应用 / 周忠荣主编；林伟初等编. —北京：清华大学出版社，2007.12
（高等学校计算机专业教材精选·数理基础）
ISBN 978-7-302-16574-3

Ⅰ. 离… Ⅱ. ①周… ②林… 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(2007)第 185358 号

责任编辑：王听讲　马　珂
责任校对：赵丽敏
责任印制：何　芊

出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
c-service@tup.tsinghua.edu.cn
社 总 机：010-62770175　　**邮购热线**：010-62786544
投稿咨询：010-62772015　　**客户服务**：010-62776969
印 刷 者：北京市清华园胶印厂
装 订 者：三河市李旗庄少明装订厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：18.75　　**字　数**：453 千字
版　　次：2007 年 12 月第 1 版　　**印　次**：2007 年 12 月第 1 次印刷
印　　数：1～6000
定　　价：30.00 元

出版说明

我国高等学校计算机教育近年来迅猛发展，应用计算机知识解决实际问题，已经成为当代大学生的必备能力。

时代的进步与社会的发展对高等学校计算机教育的质量提出了更高、更新的要求。现在，很多高等学校都在积极探索符合自身特点的教学模式，涌现出一大批非常优秀的精品课程。

为了适应社会的需求，满足计算机教育的发展需要，清华大学出版社在进行了大量调查研究的基础上，组织编写了《高等学校计算机专业教材精选》。本套教材从全国各高校的优秀计算机教材中精挑细选了一批很有代表性且特色鲜明的计算机精品教材，把作者们对各自所授计算机课程的独特理解和先进经验推荐给全国师生。

本系列教材特点如下。

(1) 编写目的明确。本套教材主要面向广大高校的计算机专业学生，使学生通过本套教材，学习计算机科学与技术方面的基本理论和基本知识，接受应用计算机解决实际问题的基本训练。

(2) 注重编写理念。本套教材作者群为各校相应课程的主讲，有一定经验积累，且编写思路清晰，有独特的教学思路和指导思想，其教学经验具有推广价值。本套教材中不乏各类精品课配套教材，并力图努力把不同学校的教学特点反映到每本教材中。

(3) 理论知识与实践相结合。本套教材贯彻从实践中来到实践中去的原则，书中的许多必须掌握的理论都将结合实例来讲，同时注重培养学生分析、解决问题的能力，满足社会用人要求。

(4) 易教易用，合理适当。本套教材编写时注意结合教学实际的课时数，把握教材的篇幅。同时，对一些知识点按教育部教学指导委员会的最新精神进行合理取舍与难易控制。

(5) 注重教材的立体化配套。大多数教材都将配套教师用课件、习题及其解答，学生上机实验指导、教学网站等辅助教学资源，方便教学。

随着本套教材陆续出版，相信能够得到广大读者的认可和支持，为我国计算机教材建设及计算机教学水平的提高，为计算机教育事业的发展做出应有的贡献。

清华大学出版社

2006 年 11 月

前　言

离散数学是研究离散量的结构及相互关系的数学科学，是现代数学的一个重要分支。由于计算机只能处理离散的数量关系，所以离散数学是计算机科学各专业最重要的专业基础课之一。随着计算机科学的发展，离散数学作为计算机科学的一种数学工具，其作用日益重要。同时，离散数学还是计算机科学许多专业课程的基础，其基本概念、基本理论和基本方法在数据结构、操作系统、编译原理、软件工程、程序设计语言、算法设计与分析、计算机网络、通信与接口、多媒体技术、数据库管理系统、人工智能、形式语言与自动机、数字电路等课程中有广泛的应用。

应用型本科培养计算机技术方面的应用型高级技术人才。这种类型的人才既需要懂得离散数学的基本概念和基本理论，更需要掌握离散数学的基本方法和实际应用。

由于各院校计算机专业培养目标不同，因而对离散数学知识有不同的要求。已经出版的不同版本的离散数学教材不仅包含的数学分支不完全一样，而且各部分的广度差别较大，难度也显著不同。本教材是在已出版的同类教材的基础上继续探索和创新的结果，相信会满足不同读者的需要。

本教材编者有着长期从事离散数学课程教学的丰富经验，熟悉多门计算机科学专业课程。为了编写出有特色的高质量教材，编者多次向计算机科学方面的专家、学者请教，深入了解计算机科学各专业所需的离散数学知识。在此基础上确定了本教材的下列编写原则：

（1）根据计算机科学各专业对离散数学知识的基本要求确定内容的广度和深度。

本教材包括命题逻辑、谓词逻辑、集合、关系、代数系统、图论 6 个分支，涵盖了离散数学的主要分支。每个分支都包括了基本内容，并严格把握其广度和深度。凡是重要的基本概念、基本方法不惜篇幅讲透彻，例题和习题恰当地控制了难度和深度。

针对应用型本科的培养目标，本教材编写了以下 3 个有特色的内容：①第 1 章介绍了离散数学必需的基础知识；②第 8 章介绍了几个主要算法的伪代码；③附录 A、附录 B、附录 C 收录了离散数学的常用符号及中英文、英中文名词术语对照表。这些内容对应用型本科学生的学习很有帮助。

（2）便于学生阅读理解。

针对应用型本科学生的实际水平和认知能力，本教材在编写方式上采取了以下 3 个措施，期望有助于读者阅读理解：①尽可能先通过实例提出问题，再介绍有关定义、定理和概念，或者随后附加实例对有关概念的各个方面进行补充说明；②对较难理解的概念，充分利用图形、图像和通俗的语言予以说明；③对基本概念、重要定理、重要公式和解题方法，不惜篇幅，叙述清楚。

（3）与专业知识相结合。

各章节都尽可能编写了本部分内容在计算机科学中的实际应用，使离散数学亲近专业。本教材突出培养学生运用离散数学知识解决与计算机科学相关的实际问题的能力。

本教材力求做到：深入浅出、概念准确、知识结构完整。

本教材采用了周忠荣编著、清华大学出版社出版的《计算机数学》中的相关内容，特此说明。

为了便于读者理解和注意，本教材使用了一些特殊的表达方式：

(1) 重要数学名词在第一次出现时以黑体字标出。如：**集合**。

(2) 重要的问题以**【说明】**的方式给出。

(3) 定理、推论、说明和一些重要结论都用楷体字表述。如：一个关系可以既不是对称的，也不是反对称的。

本教材的编写得到了广州大学华软软件学院邹婉玲副院长、徐祥副院长、教务处麦才淞处长、网络技术系黄友谦主任、软件工程系黄思曾主任的全力支持和指导，编者对他们表示感谢。

本教材由周忠荣(第 5,7,8 章和附录)，林伟初(第 2 章)，江定汉(第 6 章)，袁燕(第 1,4 章)，周志轩(第 3 章)编写。周忠荣为全书拟订了详细的编写提纲和要求，并负责统一修改、定稿。江定汉、周志轩审阅了部分章节的初稿，数学教研室的各位教师也给予了积极支持和帮助。

编者期望本教材能得到广大教师和学生的欢迎，能对离散数学课程的改革做些贡献。本教材虽经多次修改，但因编写时间紧迫、编者水平有限，书中疏漏、差错难免，恳请读者批评指正。希望本教材在广大教师和学生的建议和帮助下得到不断的改进和完善。编者的 E-mail 地址是：zzr@tsinghua.org.cn。

编　者

于广州大学华软软件学院

2007 年 8 月

目　录

第1章 基础知识

本章主要介绍以下内容：

(1) 集合、元素的概念。

(2) 整除、素数、合数、带余除法、最大公约数、最小公倍数、模运算、同余等概念。

(3) 数学归纳法、带余除法定理、求最大公约数的辗转相除法、同余的应用等知识。

(4) 序列、典型的整数序列、序列求和等知识。

(5) 排列、组合和二项式定理等基本知识。

(6) 矩阵、矩阵的加法与数乘运算、矩阵的乘法运算、转置矩阵和逆矩阵等基本知识。

1.1 集合的初步知识

什么是集合？像“广州大学华软软件学院的全体学生”、“英文字母表中的26个英文字母”等都是集合。直观地说，把一些确定的、彼此不同的、具有某种共同特性的事物作为一个整体来研究时，这个整体就称为一个**集合**，而组成这个集合的个别事物就称为该集合的**元素**。几乎所有的数学对象，无论它们可能具有哪些特有的性质，它们首先是集合。因此，在某种意义上，集合论成为构建一切数学知识的基础。

实例 1-1 长度为2的二进制串组成一个集合：{00,01,10,11}。

习惯用大写字母 A,B 等表示集合，用小写字母 a,b 等表示元素。

本书最常用的数集符号如下：

N：全体正整数和0组成的集合；

Z：全体整数组成的集合；

$\mathbf{Z}^+$：全体正整数组成的集合；

R：全体实数组成的集合。

如果一个集合中的元素为有限个，则称该集合为**有限集**，否则称它为**无限集**。前面介绍的4个数集都是无限集，而{00,01,10,11}是有限集。

这里只介绍集合的最基本的概念，有关集合的详细内容，将在第4章介绍。

1.2 数学归纳法

数学命题正确性证明有多种方法，本节将介绍一种重要方法：**数学归纳法**。

有这样一种类型的命题：对于大于等于某个正整数 n_0 的所有正整数 n，命题总是成立的。数学归纳法就适用于这类命题的证明。

用数学归纳法证明一个命题需要两个步骤。首先用直接证明法证明命题对正整数 n_0 成立。这一步称为归纳法的**基础步骤**；其次，在假设命题对正整数 $k(k\geqslant n_0)$ 成立的前提下，证明命题对正整数 $k+1$ 也成立。这一步称为归纳法的**归纳步骤**。经过数学归纳法的基础

步骤和归纳步骤就证明了该命题。

对于一些特殊的命题，用数学归纳法证明需要做些改进。例如，基础步骤可能需要用直接证明法证明命题对多个连续正整数（如 n_0 和 n_0+1）同时成立，归纳步骤需要假设命题对多个连续正整数（如 $2,3,\cdots,k$）同时成立（参见后面定理 1-2 的证明）。

例 1-1 用数学归纳法证明：对所有正整数 n，有

$$1+2+3+\cdots+n=\frac{n(n+1)}{2}$$

证明 ① 当 $n=1$ 时，由于 $1=\frac{1\times(1+1)}{2}$，所以命题成立。

② 假设 $n=k$ 时命题成立，即 $1+2+3+\cdots+k=\frac{k(k+1)}{2}$，则有

$$\begin{aligned}1+2+3+\cdots+k+(k+1)&=\frac{k(k+1)}{2}+(k+1)\\&=\frac{k(k+1)+2(k+1)}{2}=\frac{(k+1)[(k+1)+1]}{2}\end{aligned}$$

这表明，当 $n=k+1$ 时命题也成立。

根据①、②两步，命题得证。

例 1-2 用数学归纳法证明：对所有正整数 n，有

$$n<2^n$$

证明 ① 当 $n=1$ 时，由于 $1<2^1$，所以命题成立。

② 假设 $n=k$ 时命题成立，即 $k<2^k$，则有

$$\begin{aligned}k+1&<2^k+1<2^k+2\\&\leqslant 2^k+2^k=2^{k+1}\end{aligned}$$

这表明，当 $n=k+1$ 时命题也成立。

根据①、②两步，命题得证。

1.3 整数的基本性质

人类认识数是从正整数开始的，然后又认识了 0 和负整数。正整数、0 和负整数构成了整数。整数的基本性质非常有用，是研究其他各种类型的数及其性质的基础。

任意两个整数相加、相减或相乘的结果还是整数。但两个整数相除的结果可能是整数，也可能不是整数。因此，整数的性质基本上都是以整数的整除性为基础的。

由于负整数与正整数仅相差一个负号，所以正整数的性质能反映整数的性质。本节的内容基本上是针对正整数的。

1.3.1 整除

定义 1-1 对于任意两个整数 a 和 $b(b\neq 0)$，若存在一个整数 q，使得 $a=qb$，则称 **b 整除 a** 或 **a 能被 b 整除**，记作 $b|a$；否则记作 $b\nmid a$。当 $b|a$ 时称 a 是 b 的**倍数**，b 是 a 的**因数**（或**约数**）；如果还满足 $b\neq\pm a$ 且 $b\neq\pm 1$，则称 b 是 a 的**真因数**。

由整除的定义，很容易证明下面几条简单的性质。

定理 1-1 设 a,b,c 都是整数，且 $a\neq 0$，则有

(1) 若 $a|b,a|c$，则 $a|(b+c)$；

(2) 若 $a|b$，则对任意整数 m 有 $a|mb$；

(3) 若 $a|b,a|c$，则对任意整数 m,n，有 $a|(mb+nc)$；

(4) 若等式

$$b_1+b_2+\cdots+b_n=c_1+c_2+\cdots+c_m$$

中除某一项外，其余各项都是 a 的倍数，则该项也是 a 的倍数；

(5) 若 $a|b,b|c$ $(b\neq 0)$，则 $a|c$；

(6) 若 $a|b,b|a$，则 $b=\pm a$；

(7) 若 $a|b$，则 $|a|\leqslant|b|$，即任一非零整数仅有有限个因数。

证明 (1) 因为 $a|b,a|c$，故有整数 d 和 e，使得 $b=ad$ 和 $c=ae$。由此得

$$b+c=a(d+e)$$

因为 $d+e$ 是整数，所以 $a|(b+c)$。

(4) 在等式 $b_1+b_2+\cdots+b_n=c_1+c_2+\cdots+c_m$ 中，不妨设除 b_1 外的其余各项都是 a 的倍数，从中解出 b_1：$b_1=c_1+c_2+\cdots+c_m-b_2-\cdots-b_n$。

由(1)知，$c_1+c_2+\cdots+c_m-b_2-\cdots-b_n$ 是 a 的倍数，所以，b_1 也是 a 的倍数。

其他性质由读者自己证明。

例 1-3 对于正整数 n，若 $3|n$ 且 $5|n$，则必定 $15|n$。

证明 因为 $3|n$，所以存在正整数 m，使得 $n=3m$，所以 $5|3m$。

又因为 $5|5m$，所以 $5|(2\times 3m-5m)$，即 $5|m$。

从而有 $15|3m$，此即 $15|n$。

1.3.2 素数

有些正整数只能被 1 和它自身整除，而有些正整数可以被 1 和它自身以外的整数整除。据此，可以把正整数进行分类。

定义 1-2 设 a 是大于 1 的正整数，如果 a 只有 1 和 a 两个正因数，则称 a 为**素数或质数**；否则称 a 为**合数**。若合数 a 的某个因数 b 是素数，则称 b 是 a 的**素因数**。

例如，2,3,5,7,11 都是素数，4,6,8,9,10,12 都是合数。12 有两个素因数 2 和 3，8 只有一个素因数 2。

在正整数中，素数占有突出的地位。正如古希腊人所言，素数是认识整数和整数问题的基石。另外，素数本身就有重要的作用。例如，在密码学中，为信息加密的某些方法(如数字盔甲技术)就是以大素数为基础的。

定理 1-2(算术基本定理) 每一个大于 1 的正整数 n 都能惟一地表示为 $p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}$，其中，$2\leqslant p_1<p_2<\cdots<p_s\leqslant n$ 是整数 n 的素因数，$a_i(i=1,2,\cdots,s)$ 是 n 的相应素因数出现的次数。

证明 用数学归纳法。

① 当 $n=2$ 时，由于 2 是素数，所以命题成立。

② 假设 $n=2,3,\cdots,k$ 时命题成立，下面证明在这样的假设下当 $n=k+1$ 时命题也成立。

如果 $k+1$ 是素数，命题已经成立。

如果 $k+1$ 是合数，则必定存在两个数 l 和 m，使得 $k+1=lm$，并且 $2\leqslant l<k+1$ 和 $2\leqslant m<k+1$。

由假设得

$$l=q_1^{b_1}q_2^{b_2}\cdots q_t^{b_t},\quad m=r_1^{c_1}r_2^{c_2}\cdots r_u^{c_u}$$

因而有

$$k+1=lm=q_1^{b_1}q_2^{b_2}\cdots q_t^{b_t}r_1^{c_1}r_2^{c_2}\cdots r_u^{c_u} \tag{a}$$

如果存在某些 $q_v=r_w(v=1,2,\cdots,t;w=1,2,\cdots,u)$，则将它们合并。由于 l 和 m 的因数分解是惟一的，所以，$k+1$ 的因数分解是惟一的，即式(a)可以表示成

$$k+1=p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}$$

这表明，$n=k+1$ 时命题也成立。

根据①、②两步，命题得证。

实例 1-2 (1) $12=2\times2\times3=2^2\times3^1$。

(2) $600=2\times2\times2\times3\times5\times5=2^3\times3^1\times5^2$。

(3) $197=197^1$。

【说明】 根据定义 1-2 和定理 1-2，为了保证素数和合数的整体性质，1 既不能纳入素数也不能纳入合数。所以，正整数可以分为 3 类：①素数；②合数；③1。

如何判断一个正整数是素数还是合数呢？经过长期的研究，数学家们陆续提出了多种方法。下面的定理 1-3 是一种最显见的方法。

定理 1-3 如果 n 是合数，那么 n 必有一个不大于$\sqrt{n}$的素因数。

证明 ① 先证明 n 必有一个大于 1 且不大于$\sqrt{n}$的因子，用反证法。

如果 n 是合数，它必然有一个因子 a，满足 $1<a<n$。于是有 $n=ab$。

由于 $1<a<n$，所以 $1<b<n$。

假设 $a>\sqrt{n}$，且 $b>\sqrt{n}$，则有 $ab>n$。这与 $n=ab$ 矛盾。所以，假设是错误的，因而 a,b 两个数中至少有一个不大于$\sqrt{n}$，不妨设它是 a，即

$$1<a\leqslant\sqrt{n} \tag{a}$$

② 再证明 n 必有不大于$\sqrt{n}$的素因数。

如果 a 是素数，由式(a)知，命题已经得证。

如果 a 不是素数，根据定理 1-2 知，a 至少有一个不大于 a 的素因数 p。当然，p 也是 n 的素因数。再根据式(a)得

$$1<p\leqslant\sqrt{n} \tag{b}$$

命题也得证。

至此，定理证毕。

根据定理 1-3，如果大于 1 的正整数 n 不能被所有小于或等于$\sqrt{n}$的素因数整除，则 n 必然是素数。因此，可以设计一个程序来判断一个正整数是否为素数，参看第 8 章。

1.3.3 带余除法

一个整数并不一定能被另一个整数整除。例如，11 不能整除 30。如果引入商和余数的

知识，11 除 30 可以写成

$$30=2\times11+8$$

其中 2 是商，8 是余数。以上是带余除法定理的一个实例。

定理 1-4(带余除法定理) 设 a 是任意整数，b 是任意正整数，则必然存在惟一的整数 q 和 r，使得

$$a=qb+r \quad (0\leqslant r<b) \tag{1-1}$$

成立。其中，q 和 r 分别称为 b 除 a 的**商**和**余数**。

实例 1-3 (1) 若 $a=16,b=5$，则商 $q=3$，余数 $r=1$，即 $16=3\times5+1$。

(2) 若 $a=17,b=6$，则商 $q=2$，余数 $r=5$，即 $17=2\times6+5$。

(3) 若 $a=3,b=5$，则商 $q=0$，余数 $r=3$，即 $3=0\times5+3$。

(4) 若 $a=-17,b=6$，则商 $q=-3$，余数 $r=1$，即 $-17=(-3)\times6+1$。

【说明】 带余除法中商可以为负数，余数不能为负数。对于实例 1-3 中的(4)，不能说商 $q=-2$，余数 $r=-5$，即等式 $-17=(-2)\times6+(-5)$ 虽然成立，但不是带余除法的正确表示。

计算机科学中经常使用二进制数、八进制数和十六进制数。不同的数制通过下标以示区别。例如，$(73)_8$ 表示八进制数，$(73)_{16}$ 表示十六进制数。对于十进制数，通常将下标连同括号一起省略。将十进制数转换成其他进制的数就是根据带余除法定理进行的。

例 1-4 把十进制数 1249 转换成八进制数。

解 在式(1-1)中令 $b=8$ 就能得到下列 4 个等式

$$1249=156\times8+1$$
$$156=19\times8+4$$
$$19=2\times8+3$$
$$2=0\times8+2$$

由以上 4 个等式可得

$$1249=2\times8^3+3\times8^2+4\times8^1+1\times8^0$$

即

$$1249=(2341)_8$$

用同样的方法可将十进制数 1249 转换成二进制数：$1249=(10011100001)_2$。

推论 设 a 是任意整数，b 是任意正整数，则 $b|a$ 的充分必要条件是式(1-1)中的余数 $r=0$。

由此推论可以看出，带余除法与整除性的关系非常密切。

1.3.4 最大公约数

有一些实际问题需要考虑两个甚至多个整数的公约数，而两个整数的公约数是基础。因此，本书主要介绍两个整数的最大公约数和最小公倍数。

定义 1-3 设 a,b,k 都是正整数，如果 $k|a,k|b$，则称 k 是 a 和 b 的**公约数**；若 d 是 a 和 b 的所有公约数中的最大者，则称 d 是 a 和 b 的**最大公约数**，记为 $d=\gcd(a,b)$。

最大公约数有一些独特的性质：它能写成 a 和 b 的一个线性组合；它不仅比所有其他公约数大，而且也是它们的倍数。这就是下面的定理 1-5。