“十二五”普通高等教育本科国家级规划教材　计算机系列教材

离散数学（第3版）

邓辉文　编著

清华大学出版社

“十二五”普通高等教育本科国家级规划教材

邓辉文 编著

离散数学（第3版）

清华大学出版社
北京

内容简介

本书根据 IEEE-CS/ACM Computing Curricula 2005 系统地阐述离散数学的经典内容，渗透初等数论知识. 全书共分 8 章，分别介绍集合、映射与运算，关系，命题逻辑，谓词逻辑，代数结构，图论，几类特殊的图以及组合计数. 本书以集合、映射、运算和关系为主线，使全书内容联系紧密，具有较强的逻辑性. 每节都有精选习题，书后有习题答案及提示. 所用符号尽可能与其他专业课程一致，专业术语均有对应的英文.

本书叙述详尽、通俗易懂、结构严谨、逻辑清晰、便于自学，适合于计算机及相关专业作为一个学期教材(48/72/90 学时)，也可供考研学生及相关专业技术人员参考.

本书配套的《离散数学习题解答(第 3 版)》(ISBN 978-7-302-33113-1)同时由清华大学出版社出版，在出版社网站有本书配套的电子教案 PPT 可供下载. 目前，已编写完成 14 套考试题.

图书在版编目(CIP)数据

离散数学/邓辉文编著. --3 版. --北京：清华大学出版社，2013
计算机系列教材
ISBN 978-7-302-32827-8

Ⅰ. ①离…　Ⅱ. ①邓…　Ⅲ. ①离散数学—高等学校—教材　Ⅳ. O158

中国版本图书馆 CIP 数据核字(2013)第 136644 号

责任编辑：汪汉友
封面设计：常雪影
责任校对：白　蕾
责任印制：刘海龙

出版发行：清华大学出版社
　　网　　址：http://www.tup.com.cn，http://www.wqbook.com
　　地　　址：北京清华大学学研大厦 A 座　　**邮　　编：**100084
　　社 总 机：010-62770175　　**邮　　购：**010-62786544
　　投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
　　质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张：**17.75　　**字　　数：**432 千字
版　　次：2006 年 10 月第 1 版　2014 年 1 月第 3 版　　**印　　次：**2014 年 1 月第 1 次印刷
印　　数：1～2000
定　　价：29.50 元

产品编号：053595-01

前　言

离散数学是研究离散量的结构及其相互之间关系的学科，它与当今计算机所处理的对象相一致．离散数学是教育部2009年“高等学校计算机科学与技术专业核心课程教学实施方案”中8门核心课程之一，在专业教学体系中起着重要的基础理论支撑作用．

本教材自出版以来被多所高校选用，已连续多次印刷，2012年荣幸评为首批“十二五”普通高等教育本科国家级规划教材．根据教育部通知要求，入选教材应继续修订完善，及时补充反映最新知识、技术和成果的内容，与时俱进，在原书的基础之上将初等数论知识融入在第1章和第2章，加强了内容的历史发展和进一步待思考问题的概要说明，并做了如下改动．

（1）在第1章中加入了数论中的基本内容，如素数、素因数分解、模运算、最大公因数、最小公倍数和欧拉函数等．同时还给出了常见的证明方法：直接法、举反例法、数学归纳法和反证法等．

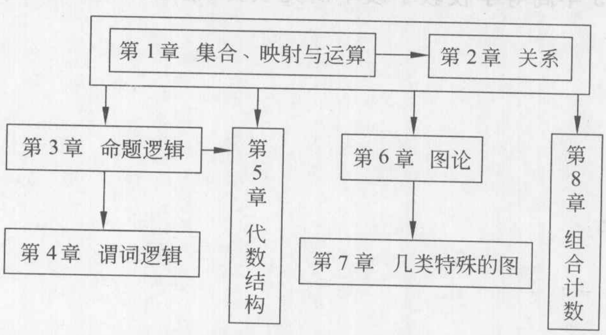
（2）在第2章中，将整数集合 **Z** 上的整除、模同余关系作为 **Z** 上的关系很自然地引入，同时还介绍线性同余方程或线性同余方程组．

（3）由于教学时数和多数学校的教学现状，精简了代数结构内容．

（4）由于组合计数在算法分析和设计中的重要性，组合计数是离散数学课程实施方案中的核心知识单元，属于必学内容，增加“组合计数”一章．

（5）新增每章小结内容．

本着离散数学为计算机其他专业课程，如数据结构、操作系统、计算机组成原理、数据库原理、算法设计与分析、编译原理、软件工程、计算机网络及人工智能等的学习提供必要数学基础的原则，同时考虑到大多数高校教学学时数的安排，本书共分8章，分别介绍集合、映射与运算，关系，命题逻辑，谓词逻辑，代数结构，图论以及几类特殊的图和组合计数．全书以集合、映射、运算和关系为主线，使全书内容联系紧密，具有较强的逻辑性．每节都有精选习题，书后有习题答案及提示．各章之间的联系如下图所示：



通过这些内容的学习，以培养学生抽象思维能力（包括符号抽象和计算抽象）、严密的逻辑思维能力以及计算思维（computational thinking）能力，能够将计算机作为认知工具，按计

算机方式求解问题.

本书讲授约需 72 课时(见下表),根据教学课时以及学生具体情况,对于第 4 章、第 5 章和第 8 章内容可适当删减(第 1 章最后两节、第 2 章最后两节也可考虑适当删减),可讲授 50 学时左右. 适当增加部分内容或加强习题训练,可作为 90 学时教材使用. 在学习过程中,若能结合本书配套的《离散数学习题解答(第 3 版)》学习,则能起到举一反三、加深课本内容学习和理解的作用.

学时数安排表

章	节的学时数
1	2+2+2+1+1+1=9
2	2+2+2+1+1+1+2=11
3	1+2+2+2+2+1+1=11
4	2+1+1+1+1+1=7
5	2+2+2+2=8
6	2+1+1+1+3+1+1=10
7	1+1+2+2+1+1+1+1=10
8	2+2+2=6

在学习过程中,请查阅有关网络教学资源:

(1) Kenneth H. Rosen website: http://www.mhhe.com/rosen.

(2) ArsDigita University: http://aduni.org/courses/discrete/index.php? view=cw.

(3) Harver Mudd College:

http://www.infocobuild.com/education/learn-through-videos/mathematics/discrete-mathematics.html.

(4) MIT(Massachusetts Institute of Technology):

http://ocw.mit.edu/OcwWeb/Electrical-Engineering-and-Computer-Science/6-042JFall-2005/CourseHome/index.htm.

教材建设是一项长期的艰苦过程,由于编者水平有限,缺点和疏漏在所难免,恳请大家不吝指正并提出宝贵修改意见,以便不断改进和完善,作者万分感激. 欢迎索取教学用 PPT 素材和考试用 14 套考试用套题(huiwend@swu.edu.cn).

感谢重庆市 2013 年高等学校教学改革研究项目(编号: 133013)资助.

编 者

2013 年 10 月

目 录

第 1 章　集合、映射与运算

集合是现代数学的最基本概念，映射是现代数学的基本概念，运算本质上就是映射，其基本内容在中学已出现．由于信息科学很多理论研究和应用研究都与集合、映射和运算有关，需要进一步较系统、深入地学习集合、映射和运算的有关内容．

集合、映射、运算和关系是贯穿于本书的一条主线，它们可使离散数学内容不"离散"．

1.1　集合的有关概念

1.1.1　集合

现代数学均建立在集合基础之上，集合已渗透到自然科学以及社会科学的各个研究领域．在非数值信息的表示及处理中，可以借助于集合去实现数据的表示、删除、插入、排序以及描述数据间的关系，在程序设计、数据结构、数据库和软件工程等课程中会经常用到．

众所周知，集合论创始人德国数学家 G. Cantor(1845—1918)在讨论函数项级数的收敛点问题时定义了集合．根据 G. Cantor 的朴素集合论观点，**集合**(set)是具有某种特定性质的对象汇集成的一个整体，其中的每一个对象都称为该集合的**元素**(element)，如班上的所有男生就组成一个集合．我们把一些特定对象看作一个整体就是一个集合，尽管这种理解存在不足之处．

数学上常用一对大括号{ }表示一个整体．

在讨论集合时，应该先指定所讨论的范围，这是避免在集合论中出现某些悖论的最好方法．所指定的范围本身就是一个集合，称为**全集**(universal set)，有时候称为论域，用 U 表示．在画文氏(John Venn，1834—1923)图时，用一个矩形框表示，如图 1-1 所示．

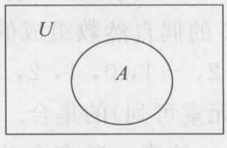


图　1-1

集合通常用大写字母 A,B,C,D 等表示．

给定一个集合，比如 A，对于全集中的任意元素 x，有且只有下述两种情形出现：

(1) 若 x 是 A 中的元素，则称 x **属于** A，记为 $x\in A$；

(2) 若 x 不是 A 中的元素，则称 x **不属于** A，记为 $x\notin A$．

显然，这样的集合 A 有一个明确的边界．

思考　班上的所有高个子同学看作一个整体时是一个**模糊集合**(fuzzy set)[1]，你能想出描述它的方法吗？

常见的数的集合(用正黑体字母表示)有：$\mathbf{N}$ 是自然数集合，包括数 0；正整数集合 $\mathbf{N}^+$；$\mathbf{Z}$ 是整数集合(正整数集合也可以记为 $\mathbf{Z}^+$)；$\mathbf{Q}$ 是有理数集合；$\mathbf{R}$ 是实数集合；$\mathbf{C}$ 是复数集合；$\mathbf{Z}_m=\{0, 1, 2, \cdots, m-1\}$．

下面介绍素数集合 $\mathbf{P}$．

对于任意整数 m 和 n，若存在整数 q，使得 $n=qm$，则称 m 为 n 的**因数**(divisor)，又称 m

整除(divides)n 或 n 被 m 整除，记为 $m|n$(与中学要求 $m\neq 0$ 不同)．于是，6 和 -6 的因数有 $1,-1,2,-2,3,-3,6,-6$，特别地，$2|6$，$-2|6$，$2|-6$，$-2|-6$．任意整数都是 0 的因数，即对于任意 $m\in\mathbf{Z}$，有 $m|0$．对于任意正整数 n，用 D_n 表示 n 的所有正因数组成的集合，于是 $D_{12}=\{1,2,3,4,6,12\}$．

对于大于 1 的正整数 p，若 $D_p=\{1,p\}$，即 p 的正因数只有 1 和 p，则称 p 为**素数**(prime)，否则称 p 为**合数**(composite number)．素数又称为质数．1 既不是素数也不是合数．最前面的10个素数为 2，3，5，7，11，13，17，19，23，29．

检查一个大于 1 的正整数是否为素数称为素数测试．素数测试不仅具有重要的理论意义，而且在计算机密码学中具有十分重要的应用价值．若 n 是合数，则存在 a 和 b 使得 $n=bc$，$1<a<n$，$1<b<n$．于是 a 和 b 中必有一个小于等于$\sqrt{n}$．因此，要检查 n 是否为素数，只需要检查 n 是否有一个小于等于$\sqrt{n}$的大于 1 的因数即可．根据此结论，可以编写一个程序以检验给定的正整数是否为素数．

当 n 为合数时，即 $n=ab$，$1<a<n$，$1<b<n$，有 $1<2^a-1<2^n-1$ 且 $2^n-1=(2^a)^b-1$．容易验证 $x^m-y^m=(x-y)(x^{m-1}+x^{m-2}y+\cdots+y^{m-1})$，进而 $2^a-1|2^n-1$，因此 2^n-1 是合数．当 n 为素数时，$2^2-1=3$，$2^3-1=7$，$2^5-1=31$，$2^7-1=127$ 都是素数，$2^{11}-1=2047=23\times 89$ 是合数．对于素数 p，2^p-1 称为 Mersenne 数．到 2005 年为止，一位德国数学爱好者、眼科医生马丁·诺瓦克博士使用 GIMPS(Greatest Internet Prime Mesen Search)系统找到的最大 Mersenne 素数是 $2^{25964951}-1$，这个数的十进位数有 7816230 位．读者也可以加入到 Mersenne 素数寻找的行列中(www. mersenne. org/prime. htm)，也许你会在 15 分钟内成为名人．

表示集合的常用方法有下面几种：

(1) **列举法** 将集合中的元素按一定规律列举出来，元素之间用逗号隔开，如小于10 的偶自然数组成的集合为$\{0,2,4,6,8\}$，自然数集合 $\mathbf{N}=\{0,1,2,3,\cdots\}$，$\mathbf{Z}=\{\cdots,-3,-2,-1,0,1,2,3,\cdots\}$．这种表示方法适用于元素个数有限或元素出现的规律性很强(元素可列)的集合．

注意 所有素数组成的集合 $\mathbf{P}$ 在理论上可用列举法表示(见第 1.6.4 节可数集合)，但由于素数有无限多个且尚未找到其出现规律，用列举法表示在实际操作时存在一定困难．

(2) **描述法** 这种方法用得最多，它只需把集合中元素满足的条件描述出来即可，一般形式是$\{x|x$ 满足的条件$\}$．例如，小于 10 的偶自然数组成的集合可表示为$\{x|x$ 是自然数且 x 是偶数且 x 小于 $10\}$．

鉴于递归(recursive)法在本书后面章节的讨论中要用到，如合式公式(WFF)的定义，更主要的是这种定义方法在研究递归函数、程序设计中函数的递归调用以及算法的递归实现等内容时的重要作用，下面简单介绍递归法，又称为归纳(inductive)法[2]．

大家知道，许多现象的变化呈现出前因后果联系，即现象的变化结果与其前面的一个或几个结果密切相关．常说的“知道他的过去，就知道他的现在；知道他的过去和现在，就知道他的将来”，体现的正是递归的思想．

一般来说，如果一个问题可以归结到其前面一个问题或前面一些问题，这就是递归问题，递归(recurrence)又称为递推．

可以用递归法定义集合.

(3) **递归法** 首先给出这个集合的初始元素；然后给出由集合中已知元素构造其他元素的方法；最后强调，有限次使用前面的步骤得到的元素是集合中仅有的元素.

【例 1-1】 自然数集合 **N** 可以递归定义如下：

首先，$0\in\mathbf{N}$；

其次，若 $n\in\mathbf{N}$，则 n 的后继 $n+1\in\mathbf{N}$；

最后，有限次使用前面的步骤得到的元素是集合 **N** 中仅有的元素.

集合的递归定义中，最后步骤很重要，它强调除有限次使用前面的步骤得到的元素是集合中元素外，不含有别的元素. 不过，请大家注意递归或递推和迭代的区别及联系[3].

在计算机科学中，还可以用别的方法定义集合，例如定义一种程序设计语言的语法时常采用的 BNF 范式法等(参见编译原理课程).

若集合 A 是有限集合，则用 $|A|$ 表示集合 A 中的元素个数，它与函数项级数收敛点的多少密切相关. 在中学使用的记号是 card(A).

需要注意的是，集合中的元素可以是任意对象，如元素本身又可以是集合等. 例如 $A=\{a,\{a,b\},b,c\}$，这时 $|A|=4$，即 A 中有 4 个元素，分别是 $a,\{a,b\},b,c$.

思考 所有不以自身为元素的集合能构成集合吗？

这是一个著名的罗素(B. A. M. Russell)悖论. 所谓悖论，就是逻辑上不一致. 假设存在这样的集合 $A=\{X\mid X\notin X\}$，则无论 $A\in A$ 或 $A\notin A$ 都是矛盾的. 避免这种悖论的方法是指定全集[4]，这就是强调全集的重要性. 而信息科学中出现的集合不会有悖论，因此本书不讨论公理化集合论.

在没有特别说明的情况下，集合之间的元素是没有次序的，前面的集合 A 也可以记为 $A=\{a,b,c,\{a,b\}\}$等. 同时，若没有特别说明，所讨论的集合不是多重集，即集合中的元素原则上不重复，所以集合$\{a,\{a,b\},b,b,c\}$就是集合 A.

若集合 A 中有两个 a 元素，五个 b 元素，无限多个 c 元素，则 A 是可重集，这时 A 可以表示为 $A=\{2\cdot a,5\cdot b,\infty\cdot c\}$. 可重集在讨论组合计数时经常用到.

把不含有任何元素的集合称为**空集**(empty set)，记为$\varnothing$或$\{\}$.

1.1.2 子集

一般来说，集合的子集比其本身要“小”一些.

【定义 1-1】 给定两个集合 A 和 B，若 A 中的任意元素都属于 B，则称 A 是 B 的**子集**(subset)，或称 A 包含在 B，或称 B 包含 A，记为 $A\subseteq B$，如图 1-2 所示.

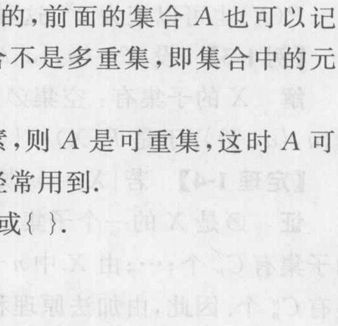


图 1-2

若 A 不是 B 的子集，这时集合 A 中至少有一个元素不属于 B.

显然有下面的定理.

【定理 1-1】 对于任意的集合 A，有$\varnothing\subseteq A$.

若两个集合 A,B 有完全相同的元素，则称这两个集合**相等**，记为 $A=B$.

我们有下述结论.

【定理 1-2】 设 A,B,C 是任意集合，下列结论成立.

(1) $A\subseteq A$;

(2) 若 $A\subseteq B$ 且 $B\subseteq A$，则 $A=B$;

(3) 若 $A\subseteq B$ 且 $B\subseteq C$，则 $A\subseteq C$.

我们知道，上述定理中结论(2)的逆也成立，这就是定理 1-3.

【定理 1-3】 $A=B$ 的充要条件是 $A\subseteq B$ 且 $B\subseteq A$.

该定理是证明两个集合相等的基本方法.

【定义 1-2】 若 $A\subseteq B$ 且 $A\neq B$，则称 A 是 B 的**真子集**(proper subset)，记为 $A\subset B$.

需要注意"$\in$"与"$\subseteq$"的区别，前者讨论的是元素与集合的关系，后者讨论的是集合与集合的关系，参见下面的例子.

【例 1-2】 设 A,B,C 是任意集合，若 $A\subseteq B$，$B\in C$，是否必有 $A\subseteq C$?

解 不成立. 例如，$A=\{a,b\}$，$B=\{a,b,c\}$，$C=\{a,\{a,b,c\}\}$，这时有 $A\subseteq B$，$B\in C$，而因为 $b\notin C$，所以结论不成立.

注意 在很多情况下，可以直接根据已知条件得出结论，但对于有些问题的讨论，举反例是一种最具说服力的方法.

1.1.3 幂集

【定义 1-3】 给定集合 X，由 X 的所有子集组成的集合称为 X 的**幂集**(power set)，记为 $P(X)$，即

$$P(X)=\{A\mid A\subseteq X\}$$

$P(X)$ 也可以记为 2^X，这种记法与下面的定理 1-4 有一定的关系.

【例 1-3】 设 $X=\{a,\{a,b\}\}$，计算 $P(X)$.

解 X 的子集有：空集 $\varnothing$；由一个元素构成的子集 $\{a\}$，$\{\{a,b\}\}$；由两个元素构成的子集 $\{a,\{a,b\}\}$. 于是 $P(X)=\{\varnothing,\{a\},\{\{a,b\}\},\{a,\{a,b\}\}\}$.

【定理 1-4】 若 $|X|=n$，则 $|P(X)|=2^n$.

证 $\varnothing$ 是 X 的一个子集；由 X 中一个元素构成的子集有 C_n^1 个；由 X 中两个元素构成的子集有 C_n^2 个；…；由 X 中 $n-1$ 个元素构成的子集有 C_n^{n-1} 个；由 X 中 n 个元素构成的子集有 C_n^n 个. 因此，由加法原理和二项式定理知 X 的子集合共有

$$1+C_n^1+C_n^2+\cdots+C_n^{n-1}+C_n^n=(1+1)^n=2^n(\text{个})$$

上述定理也可以用乘法原理很方便证得，见习题 1.1.

1.1.4 n 元组

下面用最简洁方式介绍 n 元组.

【定义 1-4】 论域 U 中选取的 n 个元素 $x_1,x_2,\cdots,x_n$ 按照一定顺序排列，就得到一个 n 元有序组，简称 **n 元组**(ordered n-tuple)，记为 $(x_1,x_2,\cdots,x_n)$ 或 $\langle x_1,x_2,\cdots,x_n\rangle$.

在不强调排列的元素个数时，可以简称**元组**.

线性代数中的 n 维向量是 n 元组，有 n 个元素的字符串是 n 元组. n 元组 $(x_1,x_2,\cdots,x_n)$ 中，x_i 称为第 i 分量或第 i 位置元素 $(1\leqslant i\leqslant n)$，它本身又可以是集合.

平面直角坐标系中任意一个点用 2 元组表示；空间直角坐标系中任意一个点用 3 元组