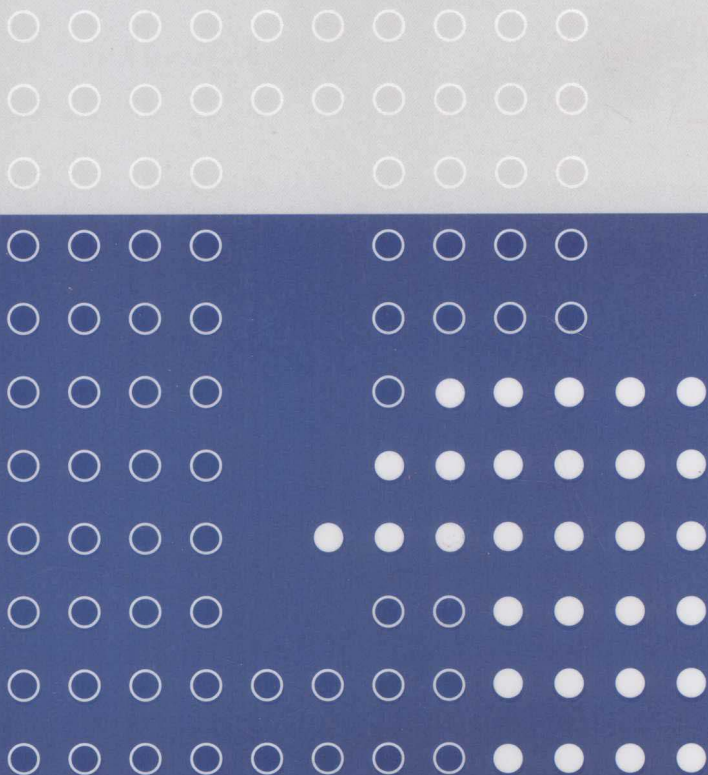




普通高等教育“十一五”国家级规划教材 计算机系列教材

# 离散数学 (第2版)



邓辉文 编著



清华大学出版社



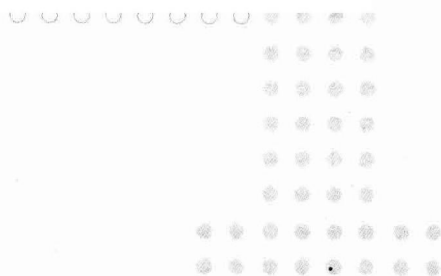
普通高等教育“十一五”国家级规划

0158  
D287=2

材

邓辉文 编著

# 离散数学(第2版)



清华大学出版社  
北京

## 内 容 简 介

本书根据 IEEE-CS/ACM Computing Curricula 2005 系统地阐述了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 2 版)》(ISBN 978-7-302-21229-4)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 10 套考试题.

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。

版权所有, 侵权必究. 侵权举报电话: 010-62782989 13701121933

## 图书在版编目(CIP)数据

离散数学/邓辉文编著.—2 版.—北京: 清华大学出版社, 2010. 3

(计算机系列教材)

ISBN 978-7-302-21193-8

I. 离… II. 邓… 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(2009)第 191715 号

责任编辑: 汪汉友

责任校对: 时翠兰

责任印制: 王秀菊

出版发行: 清华大学出版社

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

社 总 机: 010-62770175

投稿与读者服务: 010-62776969, [c-service@tup.tsinghua.edu.cn](mailto:c-service@tup.tsinghua.edu.cn)

质 量 反 馈: 010-62772015, [zhiliang@tup.tsinghua.edu.cn](mailto:zhiliang@tup.tsinghua.edu.cn)

印 装 者: 清华大学印刷厂

经 销: 全国新华书店

开 本: 185×260

印 张: 17.25

字 数: 414 千字

版 次: 2010 年 3 月第 2 版

印 次: 2010 年 3 月第 1 次印刷

印 数: 1~4000

定 价: 26.00 元

---

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题, 请与清华大学出版社出版部联系调换。  
联系电话: 010-62770177 转 3103 产品编号: 035297-01

# 前 言

离散数学的研究对象是离散量,它是计算机科学与技术专业(计算机专业、计算机工程专业、软件专业和信息技术专业)的核心课程,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到重要的基础理论支撑作用。

本书第 1 版在三年时间内连续多次印刷,根据 IEEE-CS/ACM Computing Curricula 2005 年和 2009 年 8 月在青岛召开的“全国高等学校离散数学暑期师资培训与教学研讨会”的会议精神,在原书的基础之上将初等数论知识融入第 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。

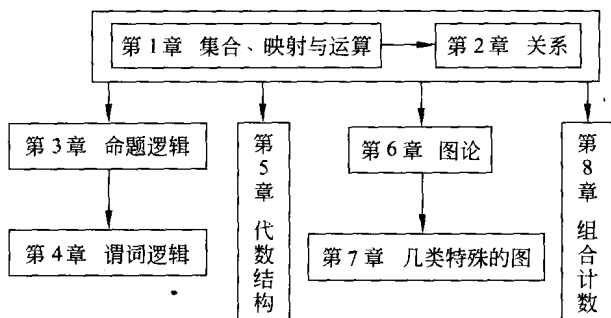
(1) 在第 1 章中加入了数论中的基本内容,如素数、素因数分解、模运算、最大公因数、最小公倍数、Euler 函数等。同时还给出了常见的证明方法:直接法、举反例法、数学归纳法和反证法等。

(2) 在第 2 章,将整数集合  $\mathbf{Z}$  上的整除、模同余作为  $\mathbf{Z}$  上的关系很自然地引入,同时还介绍了线性同余方程或线性同余方程组。

(3) 由于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,因此新增加“组合计数”的章节。

本着离散数学为数据结构、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计算机其他专业课程的学习提供必要的数学基础的原则,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,也可作为专科学生、网络学院学生、成教学生作为教材使用. 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 2 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,请查阅下列教学资源网站:

- 哈佛大学 <http://lib.harvard.edu/e-resources/details/d/descmath.html>.
- 普林斯顿大学 <http://www.math.princeton.edu/~bsudakov/seminar.html>.
- 伯克利大学 <http://www-inst.eecs.berkeley.edu/~cs70/>.
- 肯塔基大学 <http://www.ms.uky.edu/~math/Research/Margot/DM/Discrete-Math.html>.
- 离散数学论坛网址 <http://mathforum.org/discrete>.
- 布朗大学 <http://www.cs.brown.edu/courses/cs022/>.
- 科罗拉多大学 <http://www.colorado.edu/education/DMP/>.
- 数学世界网址 <http://mathworld.wolfram.com/topics/DiscreteMathematics.html>.

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,肯请大家不吝指正并提出宝贵修改意见以不断改进和完善(huiwend@swu.edu.cn),作者万分感激. 欢迎索取教学用 PPT 素材和 10 套考试题.

编 者

2009 年 10 月

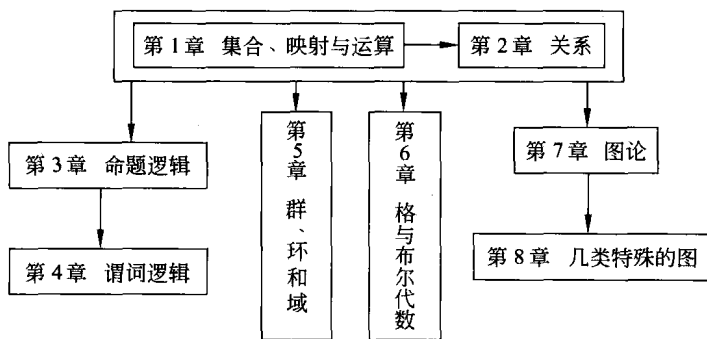
# 第 1 版前言

离散数学是研究离散量的结构及其相互之间的关系的一门学科,它与当今计算机所处理的对象相一致.

离散数学是计算机及相关专业的一门核心课程,它不是一门纯数学课程,而是计算机学科的专业基础课程.一方面,离散数学为后继课程如数据结构、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、计算机网络及人工智能等的学习提供必要的数学基础;另一方面,通过离散数学的学习,培养学生抽象思维能力和严密的逻辑推理能力,为进一步学习打下坚实的基础.

本书是根据作者多年的教学经验编写的,同时也参考了国内、外的离散数学教材.所选内容经典,适合普通高等院校本科生作为教学用书,也可作为考研学生和计算机工作者的参考书.

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,群、环和域,格与布尔代数,图论以及几类特殊的图.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.



本书讲授约需 80 课时,根据教学课时以及学生具体情况,对于第 4 章和第 5 章内容可适当删减,并可作为专科学生、网络学院学生及成人教育学生的教材.在学习过程中,若能结合本书的习题解答学习,则能举一反三、加深对课本内容的学习和理解.

由于编者水平有限,缺点和疏漏在所难免,肯请大家不吝指正,万分感激.

编者

2006 年 8 月

# 目 录

第 1 章 集合、映射与运算 .....	1
1.1 集合的有关概念 .....	1
1.1.1 集合 .....	1
1.1.2 子集 .....	3
1.1.3 幂集 .....	4
1.1.4 $n$ 元组 .....	5
1.1.5 笛卡儿积 .....	6
习题 1.1 .....	6
1.2 映射的有关概念 .....	7
1.2.1 映射的定义 .....	7
1.2.2 映射的性质 .....	9
1.2.3 逆映射 .....	10
1.2.4 复合映射 .....	11
习题 1.2 .....	13
1.3 运算的定义及性质 .....	14
1.3.1 运算的定义 .....	14
1.3.2 运算的性质 .....	17
习题 1.3 .....	21
1.4 集合的运算 .....	22
1.4.1 并运算 .....	22
1.4.2 交运算 .....	23
1.4.3 补运算 .....	24
1.4.4 差运算 .....	26
1.4.5 对称差运算 .....	27
习题 1.4 .....	28
1.5 集合的划分与覆盖 .....	29
1.5.1 集合的划分 .....	29
1.5.2 集合的覆盖 .....	32
习题 1.5 .....	32
1.6 集合的对等 .....	32
1.6.1 集合对等的定义 .....	33
1.6.2 无限集合 .....	33
1.6.3 集合的基数 .....	34
1.6.4 可数集合 .....	34

1.6.5	不可数集合 .....	35
1.6.6	基数的比较 .....	35
习题 1.6	.....	36
<b>第 2 章 关系</b>	.....	<b>37</b>
2.1 关系的概念	.....	37
2.1.1	$n$ 元关系的定义 .....	37
2.1.2	2 元关系 .....	38
2.1.3	关系的定义域和值域 .....	41
2.1.4	关系的表示 .....	42
2.1.5	函数的关系定义 .....	43
习题 2.1	.....	44
2.2 关系的运算	.....	46
2.2.1	关系的集合运算 .....	46
2.2.2	关系的逆运算 .....	46
2.2.3	关系的复合运算 .....	47
2.2.4	关系的其他运算 .....	51
习题 2.2	.....	51
2.3 关系的性质	.....	52
2.3.1	自反性 .....	52
2.3.2	反自反性 .....	53
2.3.3	对称性 .....	54
2.3.4	反对称性 .....	55
2.3.5	传递性 .....	56
习题 2.3	.....	58
2.4 关系的闭包	.....	59
2.4.1	自反闭包 $r(R)$ .....	59
2.4.2	对称闭包 $s(R)$ .....	60
2.4.3	传递闭包 $t(R)$ .....	61
习题 2.4	.....	64
2.5 等价关系	.....	65
2.5.1	等价关系的定义 .....	65
2.5.2	等价类 .....	66
习题 2.5	.....	68
2.6 相容关系	.....	69
2.6.1	相容关系的定义 .....	69
2.6.2	相容类 .....	70
习题 2.6	.....	71
2.7 偏序关系	.....	71



2.7.1	偏序关系的定义 .....	71
2.7.2	偏序集的哈斯图 .....	73
2.7.3	偏序集中的特殊元素 .....	74
习题 2.7	.....	76
<b>第 3 章</b>	<b>命题逻辑</b> .....	<b>78</b>
3.1	命题的有关概念 .....	78
习题 3.1	.....	80
3.2	逻辑联结词 .....	80
3.2.1	否定联结词 $\neg p$ .....	81
3.2.2	合取联结词 $p \wedge q$ .....	81
3.2.3	析取联结词 $p \vee q$ .....	81
3.2.4	异或联结词 $p \oplus q$ .....	82
3.2.5	条件联结词 $p \rightarrow q$ .....	82
3.2.6	双条件联结词 $p \leftrightarrow q$ .....	83
3.2.7	与非联结词 $p \uparrow q$ .....	83
3.2.8	或非联结词 $p \downarrow q$ .....	84
3.2.9	条件否定联结词 $p \overset{n}{\rightarrow} q$ .....	84
习题 3.2	.....	84
3.3	命题公式及其真值表 .....	85
3.3.1	命题公式的定义 .....	85
3.3.2	命题的符号化 .....	86
3.3.3	命题公式的真值表 .....	86
3.3.4	命题公式的类型 .....	87
习题 3.3	.....	88
3.4	逻辑等值的命题公式 .....	89
3.4.1	逻辑等值的定义 .....	90
3.4.2	基本等值式 .....	91
3.4.3	等值演算法 .....	92
3.4.4	对偶原理 .....	93
习题 3.4	.....	93
3.5	命题公式的范式 .....	95
3.5.1	命题公式的析取范式及合取范式 .....	95
3.5.2	命题公式的主析取范式及主合取范式 .....	98
习题 3.5	.....	103
3.6	联结词集合的功能完备性 .....	104
3.6.1	联结词的个数 .....	104
3.6.2	功能完备联结词集 .....	105
习题 3.6	.....	107

3.7	命题逻辑中的推理 .....	108
3.7.1	推理形式有效性的定义 .....	108
3.7.2	基本推理规则 .....	109
3.7.3	命题逻辑的自然推理系统 .....	110
习题 3.7	.....	114
<b>第 4 章</b>	<b>谓词逻辑</b> .....	<b>116</b>
4.1	个体、谓词、量词和函词 .....	116
4.1.1	个体 .....	116
4.1.2	谓词 .....	117
4.1.3	量词 .....	117
4.1.4	函词 .....	119
习题 4.1	.....	119
4.2	谓词公式及命题的符号化 .....	120
4.2.1	谓词公式 .....	120
4.2.2	命题的符号化 .....	120
习题 4.2	.....	122
4.3	谓词公式的解释及类型 .....	124
4.3.1	谓词公式的解释 .....	124
4.3.2	谓词公式的类型 .....	125
习题 4.3	.....	125
4.4	逻辑等值的谓词公式 .....	127
4.4.1	谓词公式等值的定义 .....	127
4.4.2	基本等值式 .....	127
习题 4.4	.....	129
4.5	谓词公式的前束范式 .....	129
4.5.1	谓词公式的前束范式的定义 .....	129
4.5.2	谓词公式的前束范式的计算 .....	130
习题 4.5	.....	130
4.6	谓词逻辑中的推理 .....	131
4.6.1	逻辑蕴涵式 .....	131
4.6.2	基本推理规则 .....	131
4.6.3	谓词逻辑的自然推理系统 .....	132
习题 4.6	.....	134
<b>第 5 章</b>	<b>代数结构</b> .....	<b>136</b>
5.1	代数结构简介 .....	136
5.1.1	代数结构的定义 .....	136
5.1.2	两种最简单的代数结构: 半群及独异点 .....	137

5.1.3	子代数	138
5.1.4	代数结构的同态与同构	138
习题 5.1		140
5.2	群的定义及性质	141
5.2.1	群的有关概念	141
5.2.2	子群	143
5.2.3	群的同态	144
习题 5.2		144
5.3	环和域	145
5.3.1	环的定义	145
5.3.2	几种特殊的环	146
5.3.3	域的定义	147
5.3.4	有限域	148
习题 5.3		149
5.4	格与布尔代数	150
5.4.1	格的定义和性质	150
5.4.2	分配格	153
5.4.3	有补格	154
5.4.4	布尔代数	155
习题 5.4		157
<b>第 6 章</b>	<b>图论</b>	<b>159</b>
6.1	图的基本概念	159
6.1.1	图的定义	159
6.1.2	邻接	161
6.1.3	关联	161
6.1.4	简单图	161
习题 6.1		162
6.2	节点的度数	163
习题 6.2		165
6.3	子图、图的运算和图同构	165
6.3.1	子图	165
6.3.2	图的运算	166
6.3.3	图同构	167
习题 6.3		168
6.4	路与回路	168
6.4.1	路	169
6.4.2	回路	169
习题 6.4		170

6.5	图的连通性 .....	171
6.5.1	无向图的连通性 .....	171
6.5.2	无向连通图的点连通度与边连通度 .....	172
6.5.3	有向图的连通性 .....	173
习题 6.5	.....	175
6.6	图的矩阵表示 .....	176
6.6.1	图的邻接矩阵 .....	176
6.6.2	图的可达矩阵 .....	177
6.6.3	图的关联矩阵 .....	178
习题 6.6	.....	179
6.7	赋权图及最短路径 .....	180
6.7.1	赋权图 .....	180
6.7.2	最短路径 .....	180
习题 6.7	.....	182
<b>第 7 章</b>	<b>几类特殊的图 .....</b>	<b>183</b>
7.1	欧拉图 .....	183
7.1.1	欧拉图的有关概念 .....	183
7.1.2	欧拉定理 .....	183
7.1.3	中国邮递员问题 .....	184
习题 7.1	.....	185
7.2	哈密尔顿图 .....	186
7.2.1	哈密尔顿图的有关概念 .....	186
7.2.2	哈密尔顿图的必要条件 .....	187
7.2.3	哈密尔顿图的充分条件 .....	187
7.2.4	旅行商问题 .....	189
习题 7.2	.....	189
7.3	无向树 .....	190
7.3.1	无向树的定义 .....	190
7.3.2	无向树的性质 .....	191
7.3.3	生成树 .....	192
7.3.4	最小生成树 .....	193
习题 7.3	.....	194
7.4	有向树 .....	195
7.4.1	有向树的定义 .....	195
7.4.2	根树 .....	195
7.4.3	$m$ 叉树 .....	196
7.4.4	有序树 .....	199
7.4.5	定位二叉树 .....	199

习题 7.4 .....	201
7.5 平面图 .....	202
7.5.1 平面图的有关概念 .....	203
7.5.2 欧拉公式 .....	204
7.5.3 库拉托夫斯基定理 .....	205
7.5.4 平面图的对偶图 .....	205
习题 7.5 .....	206
7.6 平面图的面着色 .....	207
7.6.1 平面图的面着色定义 .....	208
7.6.2 图的节点着色 .....	208
7.6.3 任意图的边着色 .....	209
习题 7.6 .....	210
7.7 二部图及其匹配 .....	210
7.7.1 二部图 .....	211
7.7.2 匹配 .....	211
习题 7.7 .....	212
<b>第 8 章 组合计数</b> .....	<b>214</b>
8.1 排列组合与二项式定理 .....	214
8.1.1 排列 .....	214
8.1.2 组合 .....	215
8.1.3 二项式定理 .....	216
习题 8.1 .....	217
8.2 生成函数 .....	217
8.2.1 组合计数生成函数 .....	217
8.2.2 排列计数生成函数 .....	219
习题 8.2 .....	221
8.3 递归关系 .....	221
8.3.1 递归关系的概念 .....	221
8.3.2 常用的递归关系求解方法 .....	223
习题 8.3 .....	227
<b>附录 A 符号索引</b> .....	<b>228</b>
<b>附录 B 中英文名词索引</b> .....	<b>231</b>
<b>附录 C 习题答案及提示</b> .....	<b>236</b>
<b>参考文献</b> .....	<b>259</b>

# 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,它们可使得离散数学内容不“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,见图 1-1 所示.

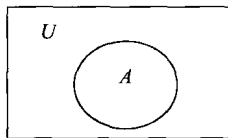


图 1-1

集合通常用大写字母 $A, B, C, D$ 等表示.

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

- (a) 若 $x$ 是 $A$ 中的元素,则称 $x$ 属于 $A$ ,记为 $x \in A$ ;
- (b) 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)<sup>[1]</sup>,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; $\mathbf{Z}_m = \{0, 1, 2, \dots, m-1\}$ .

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既不是素数又不是合数.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 $x^m - y^m = (x - y)(x^{m-1} + x^{m-2}y + \dots + y^{m-1})$ ,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.你也可以加入到Mersenne素数寻找的行列中([www.mersenne.org/prime.htm](http://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 $\mathbf{N} = \{0, 1, 2, 3, \dots\}$ , $\mathbf{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ .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1.5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 $\{x | x \text{ 满足的条件}\}$ .例如小于10的偶自然数组成的集合可表示为 $\{x | x \text{ 是自然数且 } x \text{ 是偶数且 } x \text{ 小于 } 10\}$ .

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<sup>[2]</sup>.

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  $\mathbf{N}$  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  $\mathbf{N}$  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,请大家注意递归与递推与迭代的区别及联系<sup>[3]</sup>.

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  $\text{card}(A)$ .

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  $A = \{X | X \notin X\}$ ,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<sup>[4]</sup>,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  $\emptyset$  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  $A \subseteq B$ .

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  $\emptyset \subseteq A$ .

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  $A \subseteq B, B \in C$ , 但因为  $b \notin C$ ,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  $\emptyset$ ;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  $P(X) = \{\emptyset, \{a\}, \{\{a, b\}\}, \{a, \{a, b\}\}\}$ .

组合计数,简称计数(counting)就是计算满足一定条件的离散对象的安置方式的数目.计算机科学是研究算法的一门科学,组合计数是算法分析与设计的基础,它对于分析算法的时间复杂度和空间复杂度是至关重要的.从儿时的数“数”也略知组合计数的重要性.

计数的基本原理有加法原理和乘法原理,它们是研究计数的基础.

**加法原理**(addition principle) 若事件  $A_1$  有  $m_1$  种不同选取方式,事件  $A_2$  有  $m_2$  种不同选取方式, ..., 事件  $A_k$  有  $m_k$  种不同选取方式,在这  $k$  个事件之间没有共同的选取方式时,则这  $k$  个事件之一发生有  $m_1 + m_2 + \dots + m_k$  种不同选取方式.

例如,假设一个班有  $m_1$  个男生,有  $m_2$  个女生,根据加法原理知,该班有  $m_1 + m_2$  个同学.若将计数的元素划分成若干个不同的类,先分类计数,再相加,这种方法称为分类处理,见图 1-2(a).

**乘法原理**(multiplication principle) 若事件  $A_1$  有  $m_1$  种不同选取方式,事件  $A_2$  有  $m_2$  种不同选取方式, ..., 事件  $A_k$  有  $m_k$  种不同选取方式,则这  $k$  个事件依次发生有  $m_1 m_2 \dots m_k$  种不同选取方式.

例如,假设从  $A$  到  $B$  有  $m_1$  条线路,从  $B$  到  $C$  有  $m_2$  条线路,那么根据乘法原理知,从  $A$  先到  $B$  紧接着再从  $B$  到  $C$  就有  $m_1 m_2$  条线路.若计数时需要分成独立的几步才能完成,先分别计算每一步的选取方式,再相乘,这种方法称为分步处理,见图 1-2(b).

在计数过程中,分类处理和分步处理可能会嵌套使用.

从  $n$  个不同的元素中,取  $r$  个出来按顺序排列,就是  $n$  个元素的  $r$ -排列(permutation),其排列个数记为  $P_n^r$  或  $P(n, r)$ .