内容提要

离散数学和计算机科学关系密切。本书系统介绍了离散数学的基础理论，阐述了各个分支之间的联系，还说明了它在计算机中的应用。全书共九章：集合论、关系、映射和无限集、近世代数、图论、命题逻辑、谓词逻辑、命题逻辑和谓词逻辑的公理化理论、离散数学在计算机中的应用。章末附有习题。适合于作为计算机专业的学生和自学考试者的教材，也可供从事计算机和数学方面的科技工作者和教师学习、参考。

离散数学及其在计算机中的应用

（修订版）

徐洁磐　惠永涛　编著

责任编辑：林秉方

人民邮电出版社出版

北京东长安街27号

河南邮电印刷厂印刷

新华书店北京发行所发行

各地新华书店经售

开本：787×1092 1/32　　1988年 10 月　　第二版

印张：11 12/32　页数：182　　1988年 10 月　第一次印刷

字数：260 千字　　印数：1—8 000 册

ISBN 7-115—03616—0/TP·001

定价：4.10 元

再版前言

离散数学是计算机科学的一门重要的基础课程，它是由多个数学分支组成的，包括数理逻辑、集合论、关系、映射、图论和近世代数。此外组合理论、可计算性理论、形式语言和自动机等，均是它的研究范畴，但限于篇幅，本书只介绍前者。

离散数学的各个分支，它们从不同的角度研究各种离散量的结构和相互关系。这些分支既是独立的又是相互有联系的，阐明各个分支的特点及它们之间的关系是本书的目标之一。

通过系统地学习本书，培养读者的抽象思维能力和逻辑推理能力，为掌握计算机的其它学科，为从事计算机的科学研究、生产和应用开发，奠定良好的数学基础。

本书同第一版相比，主要作了下面几方面修改：

1. 在第七章中，增加了前束范式和斯科林范式。

2. 将第一版第八章的“递归函数论”全部删除，改为“命题逻辑和谓词逻辑的公理化理论”，这是因为目前本科和专科的离散数学的教学大纲中没有列入递归函数论，它是高年级学生或研究生的选修课。经调整之后，进一步加强了数理逻辑的基础理论。

3. 将第一版第九章第3节的“谓词逻辑在程序正确性证明中的应用”改为“谓词逻辑与逻辑程序设计语言”，现在，基于谓词逻辑理论的逻辑程序设计语言应用十分广泛，两者比较，后者比前者更有实用价值。

4. 对其它章节的内容，作了少量的修改和调整，增加了

一些习题。

5. 为了适应不同程度的读者的要求及教学时数之差异，将全书内容按难度分了层次，在书中有关章节的标题之前及少量习题的题号之前冠以“*”，说明它不作基本要求，读者可以根据实际情况取舍。另外图论中的一些算法亦可跳过，均不会影响内容的完整性。

本书力图叙述清楚，取材适宜，立论精确，通达易懂，深入浅出。文中引入较多例题，便于自学。适合于计算机专业的学生及自学考试者作教材，也可供从事计算机和数学方面的科技工作者和教师学习、参考。

本书承南京工学院杨祥金副教授和华东工程学院刘凤玉副教授主审，他们在百忙之中详细审阅了全书并提供了十分宝贵的修订意见，在此表示衷心感谢。

在修订过程中，还得到南京大学吕义忠副教授，孙慧澄副教授和沈忠洪老师的热情支持，他们从各自研究的业务领域提供了十分有益的意见，在此向他们表示诚挚的谢意。

由于作者水平有限，书中错误和不妥之处难免，恳请读者和专家们批评指正。

作者　　1987年4月

目　录

第一章 集合论

§1 集合和元素的概念

集合的理论在现代数学中起了十分重要的作用，许多数学工作者认为集合论的语言是各门数学的基础。对计算机科学工作者来说，集合的概念也是必不可少的。

首先我们对集合及其元素的概念作一初步说明。一般地说，一个**集合**是指所研究对象的全体，其中每个对象是该集合中的一个**元素**（也叫成员）。对任意一个集合 S 和一个元素 x，若 x 是 S 中的一个元素，记以 $x\in S$，读作“x 属于 S”，若 x 不是 S 中的一个元素，记作 $x\notin S$，读作“x 不属于 S”。显然，任意一个元素要么属于某一个集合，要么不属于某一个集合，二者必居其一。

本书中，除非特别声明，下面几个符号是常用来表示特定集合的。

N：自然数集合 $\{0, 1, 2, \cdots\}$*；

I：整数集合

Q：有理数集合

* 在本书中，自然数集合包括零。

R：实数集合

$N_m(m\geq 1)$：集合$\{0, 1, 2, \cdots, m-1\}$

表示一个集合中的元素通常有三种方法：

第一，列举已知集合中的元素，如$A=\{1,2,3,4\}$，$B=\{1, 2, \cdots, 100\}$，$C=\{2, 4, 6, \cdots\}$。

第二，当一个集合A中的元素很多或者无穷时，则用元素特性刻划的方法来表示。如用P表示某种特性，$P(a)$表示元素a满足特性P，则

$$A=\{a|P(a)\}$$

表示A是所有使$P(a)$成立的元素a构成的集合。P可以是某项规定或某个公式，例如：

$A=\{x|x\in I$并且$x<0\}$

$B=\{x|x=y^2$并且y是正整数$\}$

$C=\{x|x$是有效的FORTRAN标识符$\}$

$D=\{x|x$是开始为c，结束为t的三个字母的字$\}$

$=\{\text{cat}, \text{cot}, \cdots, \text{cut}\}$

第三，可以通过计算规则定义集合中的元素，这种情况下的集合有的称为递归指定集合。

例 1-1 设$a_0=1$，$a_1=1$，$a_{i+1}=a_i+a_{i-1}$，$i\geq 1$，于是$S=\{a_k|k\geq 0\}=\{1,1,2,3,5,8,\cdots\}$。

如果一个集合的元素是有限的，称它为有限集，反之是无限集。我们最常见的自然数集合是无限集，无限集将在第三章专门讨论。

设A是有限集，则A中元素的数目用$n(A)$或$|A|$表示。关于集合中的元素及计算方法，后面要作专门研究。

§2 集合的子集

定义 1-1 设 A 和 B 是两个集合，如果 A 中的每个元素也是 B 中的一个元素，则称 A 是 B 的一个**子集**，记作 $A\subseteq B$。A 是 B 的子集也叫 A 被 B 包含，或叫 B 包含 A。

如果 A 不是 B 的一个子集，即 A 中至少有一个元素不属于 B，记作 $A\nsubseteq B$ 或 $B\nsupseteq A$。

定义 1-2 设 A 和 B 是两个集合，如果 A 中的每个元素是 B 中的一个元素，同时 B 中的每个元素也是 A 中的一个元素，则称 A 和 B **相等**，记作 $A=B$。

如果 A 中至少有一个元素不在 B 中或者 B 中至少有一个元素不在 A 中，则称 A 和 B **不等**，记作 $A\neq B$。

集合间的包含和相等是两个极其重要的概念，它们之间的关系可归结为下述定理。

定理 1-1 设 A 和 B 是两个集合，则 $A=B$ 当且仅当 $A\subseteq B$ 且 $B\subseteq A$。

证明：假定 $A=B$，由相等的定义，A 中每个元素在 B 中，所以 $A\subseteq B$，同样 B 中每个元素在 A 中，所以 $B\subseteq A$；

反之，若 $A\neq B$，故 A 中至少有一个元素不在 B 中，这与 $A\subseteq B$ 矛盾，或者 B 中至少有一个元素不在 A 中，这与 $B\subseteq A$ 矛盾，所以 $A\neq B$ 是不可能的；

故 $A=B$。

定义 1-3 设 A 和 B 是两个集合，如果 $A\subseteq B$ 并且 $A\neq B$，则称 A 是 B 的**真子集**（或叫**真包含**），记以 $A\subset B$。

例 1-2 设集合 $A=\{1, 3, 4, 5, 8, 9\}$，$B=\{1, 2,$

3，5，7}，$C=\{1, 5\}$，则有$A\supset C$，$B\supset C$。这是因为C中的每个元素在B和A中。然而$B\not\subset A$。因为$2, 7\in B$，但是$2, 7\notin A$。

例 1-3 设$S_1=\{a\}$，$S_2=\{\{a\}\}$，则$S_1\neq S_2$。S_1和S_2无公共元素，每个集合仅有一个元素。再令$S_3=\{a, \{a\}\}$，则S_3有两个元素。这三个集合的关系是：$S_1\neq S_3$；$S_2\neq S_3$，然而$S_1\subset S_3$，$S_2\subset S_3$。

§3 全集和空集

在这一节，我们将介绍两个特殊的集合——全集和空集。

定义 1-4 如果一个集合包含了我们所考虑的每一个集合，则称该集合为**全集**。除非特别声明，本书用U表示全集。

例 1-4 设有一个方程

$$(x+1)(2x-3)(3x+4)(x^2-2)(x^2+1)=0$$

对于这个方程，如果U是全体复数的集合，则其解集（即该方程根的集合）是

$$S=\{-1, 3/2, -4/3, \sqrt{2}, -\sqrt{2}, i, -i\}$$

如果U是全体实数集合，则其解集是

$$A=\{-1, 3/2, -4/3, \sqrt{2}, -\sqrt{2}\}$$

自然，当U是全体整数集合，自然数集合时，读者不难求出其相应的解集。

相反，如果仅仅给出某些集合，譬如说$A=\{1, 2, 3\}$，$B=\{4, 5, 6, 7\}$，那么我们难以知道其全集是什么，因为U可以是$\{1, 2, 3, \cdots, 7\}$，$\{x|x\in N且x<100\}$，N，$I\cdots$。不过今后在集合的应用中，我们研究集合时，总认为它包含在固定大的集合之中，一般不再声明其全集是哪一个。因为读者完

全可从研究的具体问题而知道其全集，例如，在平面几何中，全集是平面上的所有的点。

与全集相反的概念是空集。

定义 1-5 没有元素的集合称为**空集**，记以ϕ。

定理 1-2 设A是任意一个集合，则有$\phi\subseteq A$。

证明：用反证法。若$\phi\nsubseteq A$，由定义，ϕ中至少有一个元素不属于A，这与空集ϕ的定义发生矛盾，故有$\phi\subseteq A$。

对任意一个集合A，总有$\phi\subseteq A\subseteq U$。

定理 1-3 空集ϕ是唯一的。

证明：用反证法。设ϕ_1和ϕ_2是两个空集，则由于ϕ_1是空集，根据定理1—2有$\phi_1\subseteq\phi_2$；由于ϕ_2是空集，根据定理1—2有$\phi_2\subseteq\phi_1$；因此$\phi_1=\phi_2$。

注意，ϕ和$\{\phi\}$是不同的，前者是没有元素的一个集合，后者是以空集ϕ作为其元素的一个集合。如果$S=\{\phi\}$，则$\phi\subset S$而且$\phi\in S$；如果$S=\{\{\phi\}\}$，则$\phi\subset S$但是$\phi\notin S$。

§4 集合的运算，文氏图

定义 1-6 设A和B是两个集合，则

（1）A和B的并，记为$A\cup B$，是由A和B中的所有元素构成的集合，即

$$A\cup B=\{x\mid x\in A\text{或}x\in B\}$$

（2）A和B的交，记为$A\cap B$，是由A和B中的所有公共元素构成的集合，即

$$A\cap B=\{x\mid x\in A\text{并且}x\in B\}$$

特殊情况：如果A和B无公共元素，此时$A\cap B=\phi$，称A和

B 是分离的。

（3）A和B的差，记为$A-B$，是由属于A而不属于B的元素构成的集合，即

$$A-B=\{x \mid x\in A \text{并且} x\notin B\}$$

定义 1-7 一个集合A的补，记为$\overline{A}$，是由属于全集U但不属于A的所有元素构成的集合，即

$$\overline{A}=\{x \mid x\in U \text{并且} x\notin A\}$$

所以$\overline{A}$是全集U和A的差集。

对任意两个集合A和B，有$A-B=A\cap\overline{B}$。

例 1-5 设$A=\{1, 2, 3, 5\}$，$B=\{1, 2, 4, 6\}$，$U=N$（N为自然数集），求A和B的并集，交集，差集和$\overline{A}$，$\overline{B}$

解： $A\cup B=\{1, 2, 3, 4, 5, 6\}$

$A\cap B=\{1, 2\}$

$A-B=\{3, 5\}$

$B-A=\{4, 6\}$

$\overline{A}=\{0, 4, 6, 7, \cdots\}$

$\overline{B}=\{0, 3, 5, 7, 8, \cdots\}$

集合的运算满足一些基本定律，为便于比较，列表如下：

等幂律	
$A\cup A=A$	$A\cap A=A$
结合律	
$(A\cup B)\cup C=A\cup(B\cup C)$	$(A\cap B)\cap C=A\cap(B\cap C)$
交换律	
$A\cup B=B\cup A$	$A\cap B=B\cap A$
分配律	
$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$	$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$

恒　等　律
$A\cup\phi=A\qquad A\cap U=A$
$A\cup U=U\qquad A\cap\phi=\phi$
吸　收　律
$A\cup(A\cap B)=A\qquad A\cap(A\cup B)=A$
双　重　补
$\overline{\overline{A}}=A$
取　补　律
$A\cup\overline{A}=U\qquad A\cap\overline{A}=\phi$
$\overline{U}=\phi\qquad\overline{\phi}=U$
德·摩根定律
$\overline{(A\cup B)}=\overline{A}\cap\overline{B}\qquad\overline{(A\cap B)}=\overline{A}\cup\overline{B}$

如果在一个表达式中同时具有取补，交和并的运算，其运算的优先次序是先作取补运算，再作交的运算，最后作并的运算，若表达式中有括号，则先作内层括号中的运算。利用补、交及并的优先次序，可减少表达式中括号的层数。

下面我们利用前述的一些定义及基本定律来证明一些常用的关系式，通过这些证明，读者将会掌握基本的解题方法。

例 1-6

(1) 求证　如果 $A\subseteq B$，$C\subseteq D$，则有

$$(A\cup C)\subseteq(B\cup D)，(A\cap C)\subseteq(B\cap D)。$$

证明：任取 $x\in(A\cup C)$，于是$x\in A$或$x\in C$，由于 $A\subseteq B$，$C\subseteq D$，故$x\in B$或 $x\in D$，从而有 $x\in(B\cup D)$，所以 $(A\cup C)\subseteq(B\cup D)$。

同理可证明　$(A\cap C)\subseteq(B\cap D)$。

(2) 求证　$(A\cap B)\subseteq A\subseteq(A\cup B)$

$$(A\cap B)\subseteq B\subseteq(A\cup B)。$$

证明：任取$x\in(A\cap B)$，则$x\in A$成立，因此$(A\cap B)\subseteq A$；另一方面，任取$x\in A$，则$x\in(A\cup B)$肯定成立，因此

$A\subseteq(A\cup B)$，故有

$$(A\cap B)\subseteq A\subseteq(A\cup B)$$

同样可证明$(A\cap B)\subseteq B\subseteq(A\cup B)$。

(3) 求证如果$A\subseteq B$，则有$(A\cap B)=A$，$(A\cup B)=B$。

证明： 假定$A\subseteq B$，任取$x\in A$，于是$x\in B$，因此$x\in(A\cap B)$，得到$A\subseteq(A\cap B)$；另一方面，$(A\cap B)\subseteq A$。所以$(A\cap B)=A$。

任取$x\in(A\cup B)$，于是$x\in A$或$x\in B$，如果$x\in A$，由于$A\subseteq B$则有$x\in B$，所以$(A\cup B)\subseteq B$；另一方面$(A\cup B)\supseteq B$，故$(A\cup B)=B$。

(4) 求证 $(A-B)\subseteq A$。

证明： $A-B=A\cap\overline{B}\subseteq A$(由(2))

例 1-7 求证 $A-(A-B)=A\cap B$

证明： $A-(A-B)=A-(A\cap\overline{B})=A\cap\overline{(A\cap\overline{B})}$

$=A\cap(\overline{A}\cup\overline{\overline{B}})=(A\cap\overline{A})\cup(A\cap B)=\phi\cup(A\cap B)$

$=A\cap B$

例 1-8 求证 $(A\cap B)\cup C=A\cap(B\cup C)$当且仅当$C\subseteq A$。

证明： 设$(A\cap B)\cup C=A\cap(B\cup C)$，由于$C\subseteq(A\cap B)\cup C$，$A\cap(B\cup C)\subseteq A$，故$C\subseteq A$；

反之，如果$C\subseteq A$，则$A\cup C=A$，故$(A\cap B)\cup C=(A\cup C)\cap(B\cup C)=A\cap(B\cup C)$。

例 1-9 求证 $A-(B-C)=(A-B)-C$当且仅当$A\cap C=\phi$。

证明： 先设$A-(B-C)=(A-B)-C$，于是

$$A-(B-C)=A-(B\cap\overline{C})=A\cap\overline{(B\cap\overline{C})}$$

$$=A\cap(\overline{B}\cup C)=(A\cap\overline{B})\cup(A\cap C)$$

$$=A\cap\overline{B}\cap(C\cup\overline{C})\cup A\cap(B\cup\overline{B})\cap C$$

$$=(A\cap B\cap C)\cup(A\cap\overline{B}\cap C)\cup(A\cap\overline{B}\cap\overline{C})$$

$= (A - B) - C = A \cap \overline{B} \cap \overline{C}$ （右端）

由于$A \cap B \cap C$，$A \cap \overline{B} \cap C$，$A \cap \overline{B} \cap \overline{C}$是两两分离的（为什么?)，故$(A \cap B \cap C) \cup (A \cap \overline{B} \cap C) = \phi$，但是$(A \cap B \cap C) \cup (A \cap \overline{B} \cap C) = A \cap C$，所以$A \cap C = \phi$。

充分性的证明从略。

两个集合A和B之差是不满足结合律和交换律的，我们引进另外一种运算称为对称差。

定义 1-8 集合A和B的**对称差**，记以$A \oplus B$，是：

$$A \oplus B = (A - B) \cup (B - A)$$

即

$$A \oplus B = \{x \mid x \in A \text{且} x \notin B \text{或} x \in B \text{且} x \notin A\}$$

对称差的元素属于A或B，但不能同时属于A和B。

定理 1-4

(1) $A \oplus (B \oplus C) = (A \oplus B) \oplus C$

(2) $A \oplus B = B \oplus A$

(3) $A \oplus \phi = A$

(4) $A \oplus A = \phi$

(5) $A \oplus U = \overline{A}$（其中$U$是全集）

(6) $A \oplus \overline{A} = U$

(7) $A \oplus B = (A \cup B) - (A \cap B)$

(8) $A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$

证明： 对(8)我们可以证明如下：

$(A \cap B) \oplus (A \cap C)$

$= ((A \cap B) - (A \cap C)) \cup ((A \cap C) - (A \cap B))$

$= (A \cap B) \cap (\overline{A \cap C}) \cup (\overline{A \cap B}) \cap (A \cap C)$

$= A \cap B \cap \overline{A} \cup A \cap B \cap \overline{C} \cup \overline{A} \cap A \cap C \cup A \cap \overline{B} \cap C$

$= (A\cap\overline{A})\cap B\cup A\cap B\cap\overline{C}\cup A\cap\overline{B}\cap C$

$= \phi\cap B\cup A\cap B\cap\overline{C}\cup A\cap\overline{B}\cap C$

$= A\cap B\cap\overline{C}\cup A\cap\overline{B}\cap C$

$= A\cap(B\cap\overline{C}\cup\overline{B}\cap C)$

$= A\cap((B-C)\cup(C-B))$

$= A\cap(B\oplus C)$

下面为叙述简单，有时用记号“甲⇒乙”表示由甲能推出乙。

例 1-10 假定$A\oplus B=A\oplus C$，则有$B=C$。

证明： 欲证$B=C$，只须证$B\subseteq C$且$B\supseteq C$。

(1) 任取$x\in B$，此时若$x\in A$，则

$x\in A\cap B$

$\Rightarrow x\notin A\oplus B$（由对称差定义导出）

$\Rightarrow x\notin A\oplus C$（由$A\ominus B=A\oplus C$）

$\Rightarrow x\in A\cap C$（由对称差定义导出）

$\Rightarrow x\in C$

任取$x\in B$，此时若$x\notin A$，则

$x\notin A\cap B$

$\Rightarrow x\in A\oplus B$（由对称差定义导出）

$\Rightarrow x\in A\oplus C$（由$A\oplus B=A\oplus C$）

$\Rightarrow x\in A\cap\overline{C}$或$x\in\overline{A}\cap C$

$\Rightarrow x\in\overline{A}\cap C$（$x\in A\cap\overline{C}$不成立）

$\Rightarrow x\in C$

所以，对任意$x\in B$，不管x是否属于A，总有$x\in C$，故$B\subseteq C$。

(2) 任取$x\in C$，按同样的方法，可证明

$B\supseteq C$，所以$B=C$。

集合的幂集是一个很重要的概念。

定义 1-9 设 S 是一个有限集合，则 S 的所有子集所组成的集合称为 S 的**幂集**，用 $\rho(S)$ 或 2^S 表示，即

$$\rho(S)=\{X \mid X\subseteq S\}$$

例 1-11 设 $S=\{1, 2, 3\}$，则

$$\rho(S)=\{\phi, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, S\}$$

对于空集 ϕ，其幂集为：$\rho(\phi)=\{\phi\}$

还有：$\rho(\rho(\phi))=\{\phi, \{\phi\}\}$

$$\rho(\rho(\rho(\phi)))=\{\phi, \{\phi\}, \{\{\phi\}\}, \{\phi, \{\phi\}\}\}$$

以后将会证明如果 S 有 k 个元素，则 $\rho(S)$ 有 2^k 个元素。

例 1-12 设 A 和 B 是两个集合，则

(1) $\rho(A)\cup\rho(B)\subseteq\rho(A\cup B)$

(2) $\rho(A)\cap\rho(B)=\rho(A\cap B)$

证明：(1) 任取 $X\in(\rho(A)\cup\rho(B))$

$$\Rightarrow X\in\rho(A) \text{或} X\in\rho(B)$$
$$\Rightarrow X\subseteq A \text{或} X\subseteq B$$
$$\Rightarrow X\subseteq(A\cup B)$$
$$\Rightarrow X\in\rho(A\cup B)$$

故 $\rho(A)\cup\rho(B)\subseteq\rho(A\cup B)$

(2) 任取 $X\in\rho(A)\cap\rho(B)$

$$\Rightarrow X\in\rho(A) \text{且} X\in\rho(B)$$
$$\Rightarrow X\subseteq A \text{且} X\subseteq B$$
$$\Rightarrow X\subseteq(A\cap B)$$
$$\Rightarrow X\in\rho(A\cap B)$$

故 $\rho(A)\cap\rho(B)\subseteq\rho(A\cap B)$

反之，任取 $X\in\rho(A\cap B)$