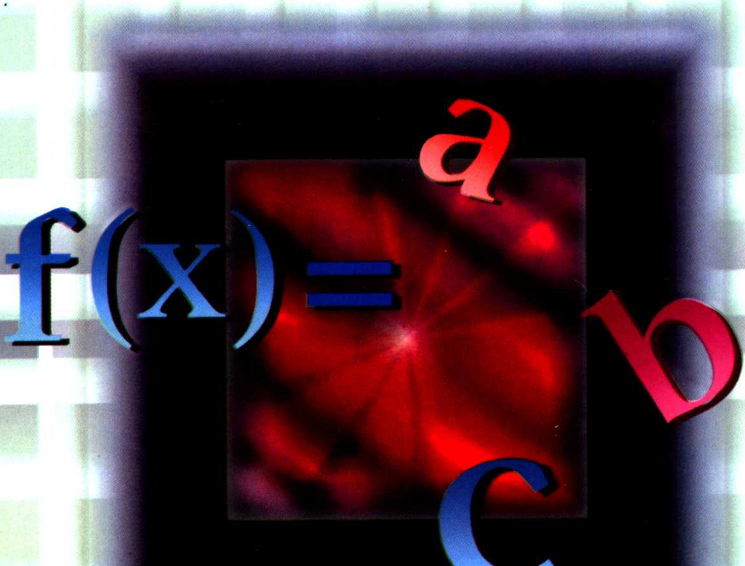
离散数学
及其在计算机中的应用

（第三次修订）

徐洁磐　朱怀宏　宋方敏　编著



人民邮电出版社
POSTS & TELECOM PRESS

离散数学及其在计算机中的应用

（第三次修订）

徐洁磐　朱怀宏　宋方敏　编著

人民邮电出版社

图书在版编目(CIP)数据

离散数学及其在计算机中的应用/徐洁磐,朱怀宏,宋方敏编著.
—3版(修订本). —北京:人民邮电出版社,2005.4
ISBN 7-115-13237-2

Ⅰ.离... Ⅱ.①徐...②朱...③宋... Ⅲ.①离散数学—数学理论②离散数学—计算机应用 Ⅳ.0158②TP3

中国版本图书馆CIP数据核字(2005)第024501号

离散数学及其在计算机中的应用(第三次修订)

◆ 编　　著　徐洁磐　朱怀宏　宋方敏
责任编辑　梁　凝

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街14号
邮编　100061　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
读者热线　010-67129258
北京隆昌伟业印刷有限公司印刷
新华书店总店北京发行所经销

◆ 开本:850×1168　1/32
印张:13.5
字数:357千字　　2005年4月第3版
印数:27 631-31 630册　　2005年4月北京第9次印刷

ISBN 7-115-13237-2/TN·2441

定价:22.00元

本书如有印装质量问题,请与本社联系 电话:(010)67129223

第四版序言

本书自 1985 年出版至今已 20 年并经历了三个版本的修改，目前，这次已是第四版了。本书以简单、明了、讲解清楚为其特色，同时将离散数学与计算机科学紧密结合构成了本书的另一个特色。在这一版中将继续保持本书原有特色，同时也对其做了一些必要的修改与调整，主要目的是使读者能对所学内容更进一步了解与掌握。本版调整的内容是：

（1）为便于读者复习，在本版的每章中均增加有复习提纲，该提纲为复习该章提供帮助。

（2）为帮助读者加深对内容的理解，在本版中增添了若干习题，特别是增添了一些带有全局性与理解性的习题。

（3）在本版中的所有习题均附有答案，这主要是为方便读者解题。

（4）对第三版中所出现的一些错误做了订正。

本书非常适合作为计算相关专业（特别是应用类专业）的大学本科、专科的教材，它还适合作为职业技术教学、自学考试的教材以及参考资料。本书还可作为从事计算机及相关应用的科技人员学习、参考之用。

本书的复习提纲编写由徐洁磐完成，习题增补及全部解答由朱怀宏完成，全书错误订正由徐洁磐完成。

在本书出版 20 年的过程中，作者不断得到广大读者的支持和帮助，希望在今后还能继续得到广大读者的支持和帮助，在这里谨向广大读者表示诚挚的感谢。

作　者

2004 年 11 月 20 日于南京

内 容 提 要

离散数学和计算机科学关系密切。本书系统地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。主要内容包括：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。章末附有复习提纲及习题，书末附有各章习题解答。

本书适合作为计算机及相关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研究的科技工作者和教师学习参考。

目　　录

第一章 集 合 论

1.1 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，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。

$\boldsymbol{N}$：自然数集合$\{0,1,2,\cdots\}$ *

$\boldsymbol{I}$：整数集合

$\boldsymbol{Q}$：有理数集合

$\boldsymbol{R}$：实数集合

$\boldsymbol{N}_m(m \geqslant 1)$：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 $A=\{1,2,3,4\}$，$B=\{1,2,\cdots,100\}$，$C=\{2,4,6,\cdots\}$。

---

* 在本书中，自然数集合的元素包括零。

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

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

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：

$A=\{x \mid x \in \boldsymbol{I}$ 并且 $x<0\}$

$B=\{x \mid x=y^2$ 并且 y 是正整数$\}$

$C=\{x \mid x$ 是有效的 FORTRAN 标识符$\}$

$D=\{x \mid x$ 是开始为 c，结束为 t 的三个字母的字$\}$

$\quad=\{\mathrm{cat},\mathrm{cot},\cdots,\mathrm{cut}\}$

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

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。

1.2 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**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 中的每个元素都在 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，且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 $S_1\subset S_3$，$S_2\subset S_3$。

1.3 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元素的集合，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：

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

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是全体整数集合或自然数集合时，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$\{1,2,3,\cdots,7\}$，$\{x|x\in \boldsymbol{N}$ 且 $x<100\}$，$\boldsymbol{N}$，$\boldsymbol{I}$，…。不过今后在集合的应用中，我们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$\varnothing$。

定理 1-2 设A是任意一个集合，则有$\varnothing\subseteq A$。

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

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

定理 1-3 空集$\varnothing$是惟一的。

证明：用反证法。设$\varnothing_1$和$\varnothing_2$是两个空集，则由于$\varnothing_1$是空集，根据定理 1-2 有$\varnothing_1\subseteq\varnothing_2$；由于$\varnothing_2$是空集，根据定理 1-2 有$\varnothing_2\subseteq\varnothing_1$；因此$\varnothing_1=\varnothing_2$。

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

1.4 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 $A\cap B=\varnothing$，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 $\overline{A}$，它是由属于全集 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	
$A\cup\varnothing=A$	$A\cap U=A$
$A\cup U=U$	$A\cap\varnothing=\varnothing$
吸 收 律	
$A\cup(A\cap B)=A$	$A\cap(A\cup B)=A$
双 重 补	
$\overline{\overline{A}}=A$	
取 补 律	
$A\cup\overline{A}=U$	$A\cap\overline{A}=\varnothing$
$\overline{U}=\varnothing$	$\overline{\varnothing}=U$
德·摩根定律	
$\overline{(A\cup B)}=\overline{A}\cap\overline{B}$	$\overline{(A\cap B)}=\overline{A}\cup\overline{B}$

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) 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　$(A\cap C)\subseteq(B\cap D)$。

(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：

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

同理可证 $(A\cap B)\subseteq B\subseteq(A\cup B)$。

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

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

$=A\cap B$

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 $A\cap C=\varnothing$。

证明：先设 $A-(B-C)=(A-B)-C$，于是有：

$$\begin{aligned}
&A-(B-C)=A-(B\cap\overline{C})=A\cap\overline{(B\cap\overline{C})}\\
&=A\cap(\overline{B}\cup C)=(A\cap\overline{B})\cup(A\cap C)\\
&=A\cap\overline{B}\cap(C\cup\overline{C})\cup A\cap(B\cup\overline{B})\cap C\\
&=(A\cap B\cap C)\cup(A\cap\overline{B}\cap C)\cup(A\cap\overline{B}\cap\overline{C})\\
&=(A-B)-C=A\cap\overline{B}\cap\overline{C}\quad\text{（右端）}
\end{aligned}$$

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

C,所以 $A \cap C = \varnothing$。

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 下面的等式是成立的:

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

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

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

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

(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:我们仅对(8)作证明如下:

$$\begin{aligned}
&(A \cap B) \oplus (A \cap C) \\
&= ((A \cap B) - (A \cap C)) \cup ((A \cap C) - (A \cap B)) \\
&= (A \cap B) \cap \overline{(A \cap C)} \cup \overline{(A \cap B)} \cap (A \cap C) \\
&= A \cap B \cap \overline{A} \cup A \cap B \cap \overline{C} \cup \overline{A} \cap A \cap C \cup A \cap \overline{B} \cap C \\
&= (A \cap \overline{A}) \cap B \cup A \cap B \cap \overline{C} \cup A \cap \overline{B} \cap C \\
&= \varnothing \cap B \cup A \cap B \cap \overline{C} \cup A \cap \overline{B} \cap C \\
&= A \cap B \cap \overline{C} \cup A \cap \overline{B} \cap C \\
&= A \cap (B \cap \overline{C} \cup \overline{B} \cap C) \\
&= A \cap ((B - C) \cup (C - B)) \\
&= A \cap (B \oplus C)
\end{aligned}$$

下面为叙述简单，有时用记号“甲$\Rightarrow$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 $A \oplus B = A \oplus C$）

$\Rightarrow x \in A \cap C$（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：

$$B \supseteq C\text{，所以 } B = C\text{。}$$

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：

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

对于空集$\varnothing$，其幂集为：$\rho(\varnothing) = \{\varnothing\}$

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

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

可以很容易证明，如果 S 有 k 个元素，则 $\rho(S)$ 有 2^k 个元素。