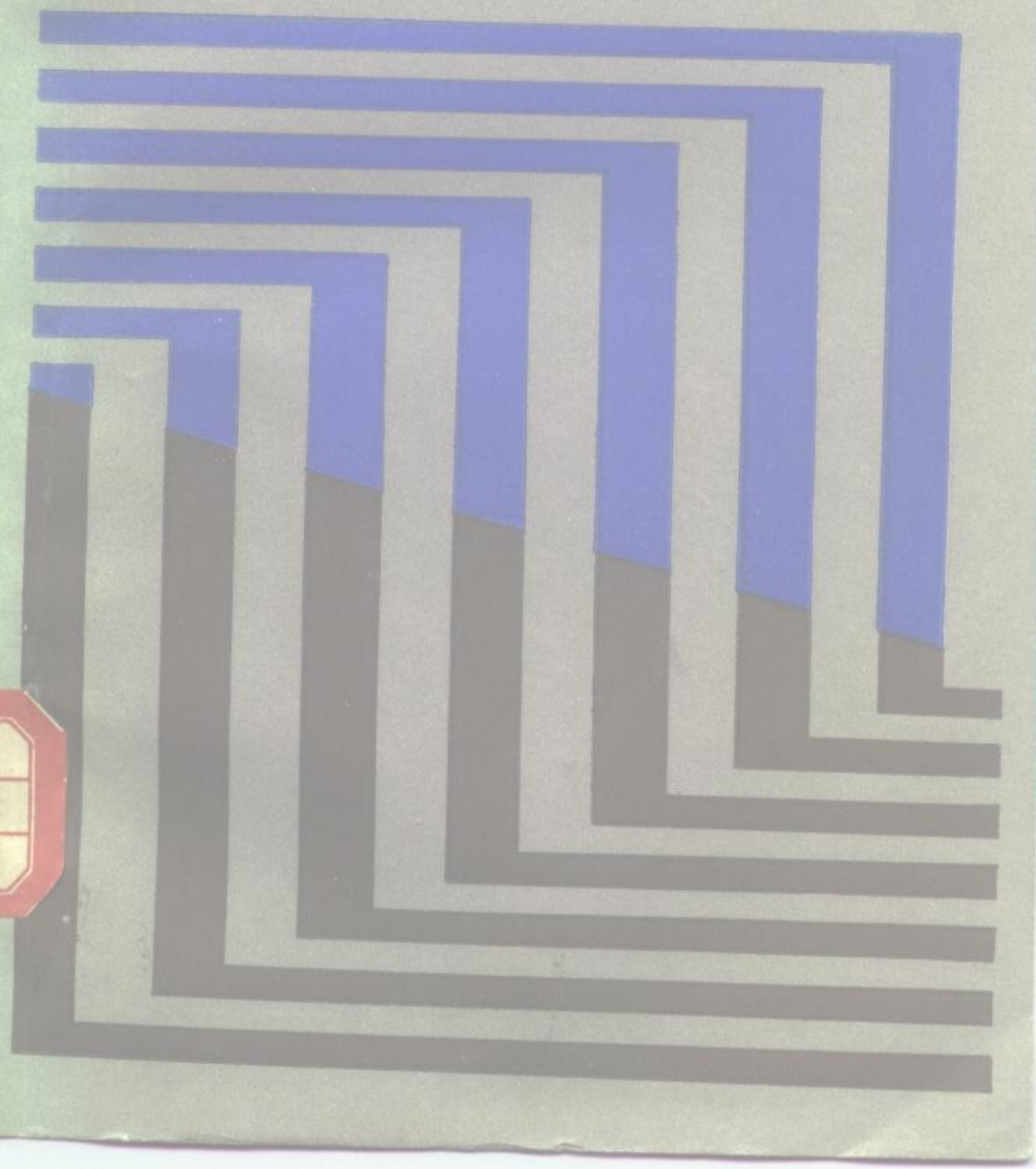
离散数学及其在计算机中的应用

徐洁磐
惠永涛 编著



离散数学及其在计算机中的应用

徐洁磐　惠永涛　编著

人民邮电出版社

内 容 提 要

离散数学和计算机科学关系密切。本书介绍离散数学的各个分支是联系到在计算机中的应用来叙述的，并阐明了各分支之间的关系，使读者能有一个较全面的概念。全书共九章：集合论，映射与无限集，近世代数，图论，谓词逻辑，递归函数论，离散数学在计算机科学中的应用。章末附有习题。可供从事计算机和数学方面的科技工作者、教师和学生学习、参考。

离散数学及其在计算机中的应用

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
河北省邮电印刷厂印刷
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　　1985年7月第一版
印张：12 12/23 页数：198　1985年7月河北第一次印刷
字数：284 千字　　印数：1—15,000册

统一书号：15045·总3051-有5418

定价：2.05元

序　言

离散数学是计算机科学的理论基础之一，它所研究的对象是各种各样的离散量，以及离散量之间的关系。由于计算机科学中出现的基本量大多是离散型的，因此，学习离散数学若能联系计算机中的应用，将会有更明确的目的，更能使理论与实际密切结合，本书致力于达到这个目标，而且在最后一章将专门介绍几个应用实例。

离散数学现由多门数学分支组成，各分支从不同角度研究各种离散量之间数与形的关系。这些分支并非互相独立，它们之间有着密切联系。阐明各分支的特点及分支之间的关系也是本书的目标之一。通过本书的学习，读者对离散数学能有一个全面的概念。

本书力图叙述清楚，立论精确，尽可能做到通达易懂，深入浅出。文中引入例题较多，便于自学。本书章节较多，读者可以根据自己的需要自行取舍。要提请注意的是，各章所用的数学符号以各章的约定为准。

本书适合从事计算机和数学方面的科技工作者，教师和学生学习。

华东工程学院朱宗正副教授和刘凤玉同志详细审阅了全书，并提供了宝贵意见，在此表示衷心的感谢。

由于作者水平有限，本书中的错误和不妥之处，恳请读者和专家们批评指正。

作者

1985　于南京

目　录

第一章　集合论……1

§ 1　集合和元素的概念 ……1

§ 2　集合的子集 ……3

§ 3　全集和空集 ……4

§ 4　集合的运算，文氏图 ……5

§ 5　有限集合中的元素数目 ……14

习题一……18

第二章　关系……20

§ 1　关系的基本概念 ……20

§ 2　关系的性质 ……23

§ 3　关系的运算 ……25

§ 4　关系的闭包运算 ……31

§ 5　具有特定性质的关系 ……35

习题二……40

第三章　映射与无限集……43

§ 1　映射 ……43

§ 2　无限集 ……49

习题三……58

第四章　近世代数……60

§ 1　代数运算 ……60

§ 2　代数系统 ……65

§ 3　同态和同构 ……67

§ 4 半群和单元半群 ……70
§ 5 群论 ……73
§ 6 环，理想，整环和域 ……99
§ 7 偏序集和格……109
习题四 ……122
第五章 图论 ……126
§ 1 图的基本概念……126
§ 2 连通性……130
§ 3 图的矩阵表示……139
§ 4 权图，最小权通路和最小权回路……142
§ 5 二分图……154
§ 6 平面图……159
§ 7 四色图……165
§ 8 树……170
§ 9 有向图……188
习题五 ……196
第六章 命题逻辑 ……201
§ 1 命题与命题联结词……201
§ 2 命题公式……211
§ 3 重言式……227
§ 4 范式……234
习题六 ……247
第七章 谓词逻辑 ……250
§ 1 谓词逻辑的基本概念……251
§ 2 谓词逻辑公式及其基本永真公式……259
§ 3 谓词逻辑与其它离散结构间的关系……266
习题七 ……270

第八章　递归函数论 ……273
§ 1　递归函数的研究特点……273
§ 2　递归函数的构造方法……275
§ 3　原始递归函数……292
§ 4　一般递归函数及部分递归函数……312
§ 5　判定问题……326
习题八 ……328
第九章　离散数学在计算机科学中的应用 ……329
§ 1　离散数学在关系数据库中的应用……330
§ 2　离散数学与纠错码……351
§ 3　谓词逻辑在程序正确性证明中的应用……372

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：正整数集合，即自然数集合

Z：非负整数集合

I：整数集合

Q：有理数集合

R：实数集合

C：复数集合

$N_m(m \geqslant 1)$：1 到 m 之间的正整数集合

$Z_m(m\geqslant 0)$：1 到 $m-1$ 之间的非负整数集合。

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$\}$

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

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 $a_0=1$，$a_1=1$，$a_{i+1}=a_i+a_{i-1}$，$i\geqslant 1$，于是

$S=\{a_0, a_1, \cdots, a_i, a_{i+1}=a_i+a_{i-1}, \cdots, |i\geqslant 1\}$

$=\{a_k\,|\,k\geqslant 0\}$。

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$S_1\subseteq S_3$，$S_2\subseteq S_3$。

§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$\{1, 2, 3, \cdots, 7\}$，$\{x \mid x\in N$ 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 $\phi \subseteq S$ 而且 $\phi \in S$；如果 $S=\{\{\phi\}\}$，则 $\phi \subseteq S$ 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	
$A\cup\phi=A$	$A\cap U=A$
$A\cup U=U$	$A\cap\phi=\phi$

双重补
$\overline{\overline{A}}=A$

取补律	
$A\cup\overline{A}=U$	$A\cap\overline{A}=\phi$
$\overline{U}=\phi$	$\overline{\phi}=U$

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，如果 $x\in A$，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) 如果 $A\subseteq B$，则有 $(A\cap B)=A$，$(A\cup B)=B$。

证明：假定 $A\subseteq B$，令 $x\in A$，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 $(A\cap B)=A$。

令 $x\in(A\cup B)$，于是 $x\in A$ 或 $x\in B$，如果 $x\in A$，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：$A-B=A\cap\bar{B}\subseteq A$ (由 (2))

例 1-7 求证 $A-(A-B)=A\cap B$

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

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

$=A\cap B$

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

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

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

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

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

由于 $A\cap B\cap C$，$A\cap\bar{B}\cap C$，$A\cap\bar{B}\cap\bar{C}$ 是两两分离的 (为什

么?)，故 $(A\cap B\cap C)\cup A\cap\bar{B}\cap C=\phi$，但是 $(A\cap B\cap C)\cup(A\cap\bar{B}\cap C)=A\cap C$，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) $A\oplus U=\bar{A}$ （其中 U 是全集）

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

(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：

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

$$=A\cap(B\cap\bar{C}\cup\bar{B}\cap C)$$
$$=A\cap((B-C)\cup(C-B))$$
$$=A\cap(B\oplus C)$$

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

$x\in A\Rightarrow x\in A\cap B$

$\Rightarrow x\notin A\oplus B$(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）

$\Rightarrow x\in C$

(2) 任取$x\in B$，此时若$x\notin A$，则

$x\notin A\Rightarrow x\notin A\cap B$

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

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

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

$\Rightarrow x\in\bar{A}\cap C$（$x\in A\cap\bar{C}$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

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