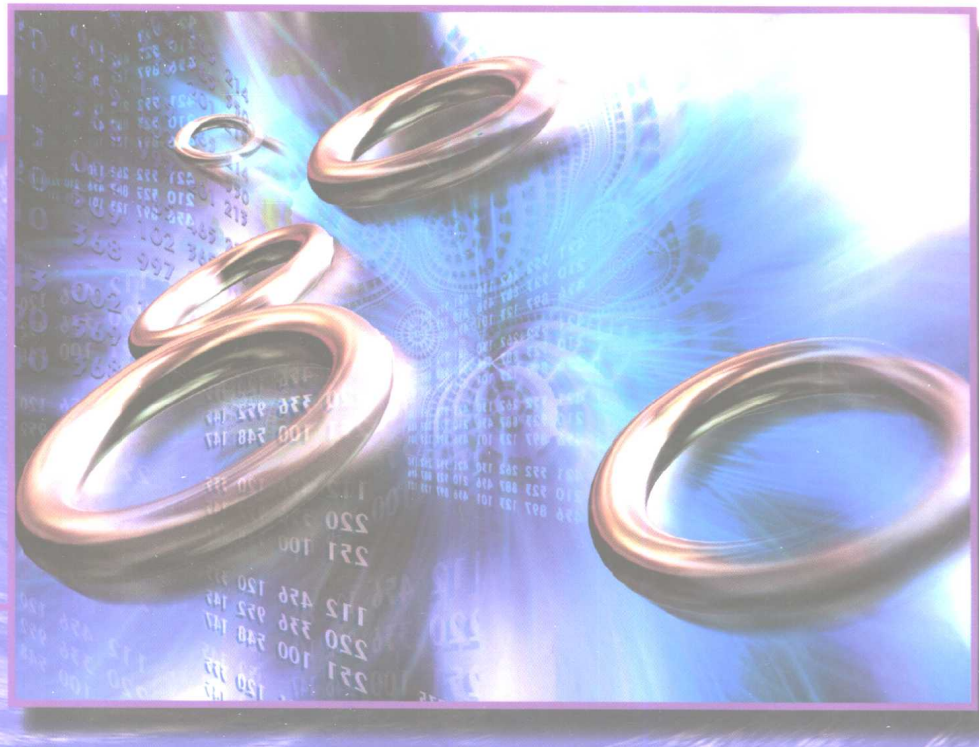
21世纪高等院校计算机专业基础课程教学辅导丛书

离散数学



钟国亮　编著

中国水利水电出版社
www.waterpub.com.cn
全華

21世纪高等院校计算机专业基础课程教学辅导丛书

离散数学

钟国亮　编著

中国水利水电出版社

内 容 提 要

本书采用 Q&A 对话方式，将书中的内容按由浅入深的顺序，以循序渐进的方式予以介绍。内容包括：集合、关系、近似表示法与应用，逻辑、布尔代数与应用，递推方程、生成函数与算法分析，图论、图论算法与应用，机器模型、NP 完备与估计算法，数论、密码学与应用，概率、近世代数与应用。

本书可以作为高等院校离散数学课程授课教师的教学参考用书，也可以作为学生自学的参考资料。

图书在版编目（CIP）数据

离散数学 / 钟国亮编著. —北京：中国水利水电出版社，2004.3
（21 世纪高等院校计算机专业基础课程教学辅导丛书）
ISBN 7-5084-2020-9

Ⅰ. 离… Ⅱ. 钟… Ⅲ. 离散数学—高等学校—教学参考资料 Ⅳ. O158

中国版本图书馆 CIP 数据核字（2004）第 009884 号

书　　名	**离散数学**
作　　者	钟国亮　编著
出版　发行	中国水利水电出版社（北京市三里河路 6 号　100044） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）63202266（总机）　68331835（营销中心）　82562819（万水）
经　　售	全国各地新华书店和相关出版物销售网点
排　　版	北京万水电子信息有限公司
印　　刷	北京蓝空印刷厂
规　　格	787mm×1092mm　16 开本　17 印张　385 千字
版　　次	2004 年 3 月第 1 版　2004 年 3 月第 1 次印刷
印　　数	0001—5000 册
定　　价	24.00 元

序

多年来，我在台湾科技大学教授离散数学的课程。本书主要依照上课的讲义结合国内外相关的学术材料以 Q&A 的方式写作而成。相关的文献索引在书中都会详列出来。我在构想本书的时候，采用很自然的 Q&A 对话方式，将书中七章的内容按由浅入深和循序渐进的方式予以介绍。希望此书除了能够被当成一本不错的教科书外，也能够成为想了解这个领域的同学的优秀参考书。依照本书的内容，它除了适合于离散数学的课程外，也很适合当作算法课程的辅助教材。

本书的三大特点为：

- 采用很自然的 Q&A 方式将每一个典型的问题与解答或是一个重要的定理与证明交待出来。一个 Q&A 和下一个 Q&A 之间尽可能保持很自然的联系以保证内容的流畅。
- 在适当的地方，会交待出该章中相关问题与别的章节的关联性。另外，每章所附的作业均附有解答以方便读者核对答案，从而加深学习的效果。
- 书中包括了不少较新且很重要的题材，例如：消息理论、编码论和密码学的重要概念与核心方法。希望这些材料的加入对读者将来在学习相关课程时会有帮助。这些题材在当今的通讯、压缩、图像多媒体和信息安全等领域都有很大的应用。

本书共分七章。第一章介绍集合的概念及容斥原理的应用。基于集合的概念，在本章中引入复杂度的符号定义、关系、函数、部分有序集、近似表示法和组合计数的应用等重要内容。在第二章中，首先介绍最基本的命题逻辑，再来介绍逻辑推论。接下来讲解带有量词的谓词逻辑以及如何将逻辑式转换成范式。随后介绍了布尔代数及其在电路设计中的应用。最后，介绍了 Davis 和 Putnam 程序在加快演绎过程中的作用。第三章先介绍递推方程、生成函数、递推方程求解和生成函数在组合计数中的应用。然后，介绍 6 个著名排序法的复杂度分析。另外还会详细讨论快速傅利叶变换、快速多项式相乘和两个计算几何的应用问题。第四章介绍图论常用的符号和许多基本性质及定理。还介绍了一些著名的图论算法，例如：最短路径算法、最小生成树算法、最大流算法和二部图的最大匹配。在这一章的最后介绍了警卫配置和图的着色这两大应用。第五章介绍有关机器模型、形式语言、NP 完备和估计算法的重要概念和定理。第六章主要介绍数论、密码学和应用，其中所牵涉到的数学背景都会详细介绍。第七章主要介绍基于概率背景的消息理论。另外，我们也会介绍近世代数和编码论的许多重要定义和定理。最后，介绍贝氏法则和熵编码的应用。

本书内容为本人亲自撰写，限于本人的水平与经验，书中缺点与错误在所难免，还望读者不吝指正。本书得以出版，由衷感谢全华科技图书的大力协助。在此，非常感谢曾经选修过我的课的同学们，谢谢你们在学习时给予我的意见与指正。另一方面，非常感谢陈品瑾、赖振洋、沈骏吉、林志贤、游士纬、黄咏淮、郑又方、黄佩玲、黄翊伦和吴世通等

同学在读完我的手稿后，给我提出的宝贵建议。也谢谢项洁教授和李家同教授的鼓励。谨以此书献给我的母亲和家人。

钟国亮　台湾科技大学
http://www.cs.ntust.edu.tw/~klchung
2003 年 6 月

目　　录

第一章　集合、关系、近似表示法与应用

1.1　前言

在本书的第一章，我们从最基本的集合（Set）谈起。介绍完集合的定义、性质和运算后，我们利用集合的计数（Counting）概念，推出容斥原理（Inclusion-Exclusion Principle）。另外，通过多集合中集合之间的属性关系（Attribute Relation），定义出关系，并且讨论什么是部分有序集（Partial Order Set）。最后，介绍两个相关的应用：卡特兰数目（Catalan Number）计算，和城堡多项式（Rook Polynomial）的计算。这两个应用都会充分使用到容斥原理的技巧。前者在组合计数中是很古典的著名范例，而后者可让读者领略分进合击（Divide and Conquer）的美妙概念。

1.2　单一集合的定义、可数性与复杂度符号

此节为本书的正式起头。先讨论集合是很恰当的，尤其像离散数学的讨论题材，常用到集合的符号和相关的定义。从本节起一直到本书的结束，我们都是采用 Q&A（Question & Answer）的方式将例题、定理和证明介绍出来。

Q1 是否可以举个单一集合的例子，并以不同方式表示？

Ans 假设有四个元素（Element），2、4、6 和 8，这四个元素形成一个集合 S，集合 S 至少有下列三种表示方式：

（1）　$S=\{2,4,6,8\}$

（2）　$S=\{x \mid x\text{为小于10的正偶数}\}$

（3）　$S=\{2k \mid 1\le k\le 4,\ k\text{为整数}\}$

集合 S 内的元素 2 属于 S，可写成 $2\in S$。

EOA

在上面的 Q&A 中，符号 Q 代表问题（Question）；符号 Ans（Answer）代表答案，而 EOA（End of Answer）代表解答或证明结束了。通常，我们用大写字母表示集合，而用小写字母表示元素。

Q2 什么叫空集合（Empty Set）和幂集合（Power Set）？

Ans 如果一个集合里不包含任何元素，那么这个集合就叫空集合。空集合可写成{ }或 ϕ。有一个集合，它内含空集合则写成{{ }}或{ϕ}。前面 Q1 所述的集合 S，我们用 $|S|$ 代表其元素的个数（Cardinality）。我们在一些组合（Combinatorics）的问题中，有时会用到一个集合的幂集合概念。简单地讲，幂集合就是该集合内所有子集合形成的集合。以 Q1 中的 S 为例，S 的幂集合可写成
$P(S)=\{\phi,\{2\},\{4\},\{6\},\{8\},\{2,4\},...,\{2,4,6,8\}\}$ 且 $|P(S)|=2^4=16$。

EOA

在 S 中，{2,4} 为 S 的子集合，我们用 $\{2,4\}\subset S$ 来表示 {2,4} 包含于 S。

Q3 假设一集合 S，其元素个数为 $|S|=n$，则 S 的幂集合的元素个数有多少？

Ans S 内的所有子集依其元素个数分类，则有内含零个元素的，内含 1 个元素的，内含 2 个元素的，一直到内含 n 个元素的子集。把这些子集加起来，总共有 $|P(S)|=\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+...+\binom{n}{n}$ 个不同的子集。如何得到 $|P(S)|$ 的封闭型式（Closed Form）呢？我们来看一个二项式展开式（Binomial Expansion）

$$(x+y)^n=\sum_{i=0}^{n}\binom{n}{i}x^i y^{n-i}$$

将 $x=1$ 和 $y=1$ 代入上述二项式展开式，可得到

$$2^n=\sum_{i=0}^{n}\binom{n}{i}=|P(S)|$$

所以 S 的幂集合的元素个数为 2^n。

EOA

在 Q3 中，幂集合的元素个数计算可通过二项式展开来求得，除了这个方式，有没有别的方式也可求得 $|P(S)|=2^n$？请看 Q4 的证明。

Q4 关于 $|P(S)|=2^n$ 的证明，有没有更简单的证明？

Ans 另一个更简单的证明是这样的。在形成 S 的集合时，集合 S 内的任一元素可被挑到或没有被挑到，也就是任一元素有两种选择法。因为 $|S|=n$，所以共有 2^n 种挑法，也就是共形成 2^n 个不同的子集，即 $|P(S)|=2^n$。

EOA

Q4 的方法虽简单，然而 Q3 的证法中有组合等式的技巧在内，也有其另一层的意义。Q1 举的例子为一有限集(Finite Set)且 $|S|=4$。但是有些集合的元素个数是无限的(Infinite)。

例如，质数的个数是无限的，证明请参见第六章。若一个集合内的元素个数为无限，则该集合称作无限集。

Q5 什么叫无限集的可数（Countable）性或不可数（Uncountable）性？

Ans 这个概念源自于数学家康托（Cantor）的想法。一个无限集若为可数，则集合内的元素和自然数集 N 的元素之间有一对一的对应关系，否则该无限集为不可数。

EOA

Q6 整数集 $Z=\{...-2,-1,0,1,2...\}$ 是无限集，但它是可数还是不可数呢？

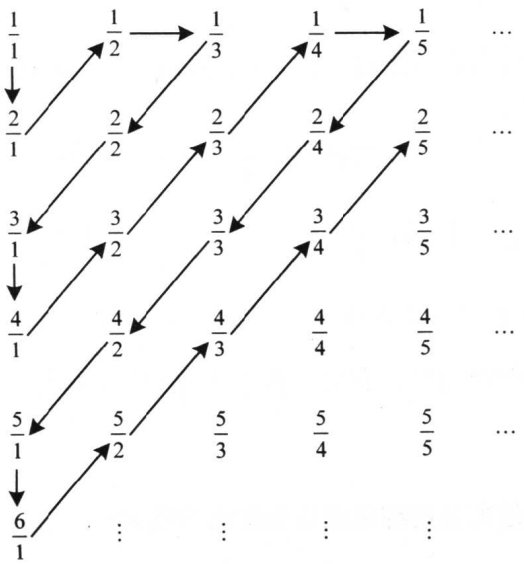
Ans 首先将 Z 调整成 $Z=\{0,1,-1,2,-2,3,-3...\}$，则在此调整后的 Z 中，其内的元素很自然地和 N 有一对一的对应关系。所以 Z 为可数的无限集。

EOA

介绍完整数集 Z，很自然地会想到有理数集。由于有理数 $\frac{q_1}{p_1}$ 和有理数 $\frac{q_2}{p_2}$ 的中间有 $\frac{q_1p_2+p_1q_2}{2(p_1p_2)}$ 个有理数，所以由集合的稠密性很容易知道有理数集是无限集。

Q7 正有理数集 $Q^+=\left\{\frac{q}{p}\middle| p,q\in Z^+\right\}$ 是否为不可数的无限集？

Ans 我们先将 Q^+ 内的元素依下列扫描次序排列如下：



在上图中，任一正有理数$\frac{q}{p}$均可算出其在图中的次序。例如，$\frac{1}{1}$的次序为1，$\frac{1}{3}$的次序为4。若$p+q$为偶数，则$\frac{q}{p}$的次序为$\left(\sum_{i=1}^{p+q-2} i\right)+q=\frac{(p+q-2)(p+q-1)}{2}+q$。例如，$\frac{1}{5}$的次序为$\left(\sum_{i=1}^{4} i\right)+1=11$。若$p+q$为奇数，则$\frac{q}{p}$的次序为$\left(\sum_{i=1}^{p+q-2} i\right)+p$。例如，$\frac{4}{3}$的次序为$\left(\sum_{i=1}^{5} i\right)+3=\frac{5\times 6}{2}+3=18$。讨论完$\frac{q}{p}$的次序计算，算出来的次序就是对应到自然数集的数。所以Q^+为可数的无限集。

EOA

上面叙述的Q^+的扫描次序和DCT（Discrete Cosine Transform）进行量化后扫描的次序有些类似[4]，在量化后的DCT系数矩阵中，依上述扫描次序，DCT系数大致上会有递减的现象。

Q8 有了Q7的证明后，如何证明有理数集$Q=\left\{\frac{q}{p}\middle| p,q\in Z\right\}$为可数的无限集？

Ans 首先，我们将Z调整成$Z=\{0,1,-1,2,-2,3,-3...\}$，则很容易找出$Z$和$N$之间一对一的对应关系。来看一个较复杂的有理数集$Q$的例子，回顾Q7证明中$Q^+$所对应的图，$Q$可写成有次序的集合$Q=\left\langle 0,1,-1,2,-2,\frac{1}{2},-\frac{1}{2},...\right\rangle$。再回到重新安排后的集合$Q=\left\langle 0,\frac{1}{1},-\frac{1}{1},\frac{2}{1},-\frac{2}{1},\frac{1}{2},-\frac{1}{2},\frac{1}{3},...\right\rangle$，依据上述的分析，当$p+q$为正偶数时，可得$Q$中的正有理数$\frac{q}{p}$对应于$N$中的$1+2\left[\left(\sum_{i=1}^{p+q-2} i\right)+q-1\right]+1$
$=2\left[\frac{(p+q-2)\times(p+q-1)}{2}+q-1\right]+2=(p+q-2)\times(p+q-1)+2(q-1)+2$。例如在$Q$中的$\frac{1}{1}$对应于$N$中的2；在$Q$中的$\frac{1}{3}$对应于$N$中的$2\times 3+2=8$。当$p+q$为正奇数时，在$Q$中的$\frac{q}{p}$对应于$N$中的$1+2\left[\left(\sum_{i=1}^{p+q-2} i\right)+p-1\right]+1=$
$(p+q-2)\times(p+q-1)+2(p-1)+2$。例如，$Q$中的$\frac{4}{1}$对应于$N$中的$3\times 4+2=14$。综合以上两种情形的分析，我们证得$Q$为可数的无限集。

EOA

Q9 是否可以把上一题的证明综合成较系统化的形式？

Ans 在 Q8 的证明中，已得知无限集 Q 为可数的，因为无限集 $Q=\left\langle 0,\frac{1}{1},-\frac{1}{1},\frac{2}{1},-\frac{2}{1},\frac{1}{2},-\frac{1}{2},\frac{1}{3},...\right\rangle$ 和 N 有一对一对应。Q 中的 $\frac{q}{p}$ 若为正偶数时，对应于 N 中的 $(p+q-2)\times(p+q-1)+2(q-1)+2$；若 $\frac{q}{p}$ 为负偶数时，对应于 N 中的 $(p+q-2)\times(p+q-1)+2(q-1)+3$。$Q$ 中的 $\frac{q}{p}$ 若为正奇数时，对应于 N 中的 $(p+q-2)\times(p+q-1)+2(p-1)+2$；若 $\frac{q}{p}$ 为负奇数时，对应于 N 中的 $(p+q-2)\times(p+q-1)+2(p-1)+3$。

EOA

有理数集具有稠密性，同理，实数集 R 亦具有稠密性，所以 R 也是无限集。

Q10 实数集 R 是否为不可数的？

Ans 实数集为有理数集和无理数集的联集。为方便讨论，在 R 的集合中，我们只考虑 $T=(1,2]$ 这个半开区间即可，原因是在这个半开区间内的集合已知是无限集，若能证明出它是不可数的，就能够说明无限集 R 是不可数的。要直接证明 T 为不可数，不是一件容易的事，我们改和间接的证法。所谓的间接证法就是反证法，这种间接式的证法在本书的很多地方都可见到，我们在第二章时会用逻辑的方式再论述这种证法。令 T 为可数的，则表示 T 中的元素和 N 有一对一的对应关系。我们假设 T 的元素和 N 的对应中，可定出一有序集 $\overline{T}=\langle t_1,t_2,...\rangle$，这里 $t_i=1.t_{i1}t_{i2}...$ 且 $t_{ij}\in\{0,1,2,...,9\}$。换言之，$\overline{T}$ 中的第 i 个元素对应于 N 中的 i。令 $\bar{t}=1.\bar{t}_1\bar{t}_2\bar{t}_3...$，且 $\bar{t}_i=0$ 若 $t_{ii}=9$；$\bar{t}_i=9-t_{ii}$，若 $t_{ii}\in\{0,1,2,...,8\}$。很明显，因为 $\bar{t}=1.\bar{t}_1\bar{t}_2\bar{t}_3...$，所以 $\bar{t}\in\overline{T}$，也就是 $\bar{t}$ 是 $\overline{T}$ 中的一个元素，但根据 $\bar{t}$ 的建构法及对角排除的原因，我们却无法在 $\overline{T}$ 中找到其所在的地方，也就无法在 N 中找到一个元素与其对应，这是矛盾的。以上的证明就是有名的康托对角化证明法（Diagonalization Method）。

EOA

到此为止，我们大致对单一集合的定义、符号使用、幂集合和无限集的可数性等部问题做了一番介绍。

Q11 在数据结构课程里曾讲过 θ、O 和 Ω 三种符号，它们是否为三种集合的符号？

Ans 这三种符号的确可视为集合的符号。θ 念作 Theta，O 念作 Big-O，而 Ω 念作 Omega。它们在算法（Algorithm）的复杂度分析（Complexity Analysis）上常用来

表示时间或内存的花费。它们可说是很重要的复杂度符号。

EOA

Q 12 是否要以先定义θ这个复杂度的数学表示方式？

Ans 假设有一算法所花的时间复杂度为$\frac{1}{2}n^2$，此处n为问题输入的大小（Input Size）。令函数$f(n)=\frac{1}{2}n^2$，只要我们可找到三个常数c_1、c_2和n_0，使得对任意的$n\geq n_0$均满足$0\leq c_1g(n)\leq f(n)\leq c_2g(n)$，则$f(n)$可写成$\theta(g(n))$。以$f(n)=\frac{1}{2}n^2$为例，的确可找到$c_1=\frac{1}{3}$、$c_2=\frac{3}{4}$和$n_0=1$，使得对任意$n\geq 1$均满足$0\leq\frac{1}{3}n^2\leq\frac{1}{2}n^2\leq\frac{3}{4}n^2=\theta(n^2)$。很明显，$\theta$符号的确是一个很简洁的表示符号，省掉了很多不同系数的困扰。简单地讲，当$f(n)$用$f(n)$中最高次的$g(n)$以$\theta(g(n))$的方式表示时，表示可找到$c_1g(n)$和$c_2g(n)$两个函数，当$n\geq n_0$时，$c_1g(n)\leq f(n)\leq c_2g(n)$成立。此时$\theta(g(n))$不失为$f(n)$的一个简洁有力的表示方式。

EOA

根据上述对θ的定义，可视$\theta(n^2)$为一无限且不可数集。除了θ的表示法外，我们设计算法，其复杂度分析的上限（Upper Bound）也常以O表示，而下限（Lower Bound）以Ω表示。

Q 13 是否可以定义O和Ω表示法？

Ans 假设一算法的复杂度仍为$f(n)=\frac{1}{2}n^2$，因为可找到常数$c=\frac{3}{4}$，使得$f(n)\leq c\times g(n)$，此处$g(n)=n^2$且$n\geq n_0=1$。所以我们表示$f(n)$为$O(n^2)$。口语地说，就是$f(n)$可用$f(n)$中最高次的$g(n)$以$O(g(n))$来表示时，代表我们可找到常数c和n_0，使得当$n\geq n_0$时，$0\leq f(n)\leq c\times g(n)$成立。同理，$O(n^2)$也是一无限且不可数集。符号$\theta$和O常被用来表示复杂度的上限，然而第三个符号$\Omega$用来表示一个问题的复杂度下限。$\Omega$的定义和O刚好相反，一个函数$f(n)$可表示成$\Omega(g(n))$时，可找到常数$c$和$n$。使得当$n\geq n_0$时，$f(n)\geq c\times g(n)\geq 0$成立。很明显，$\Omega(n)$也是一无限且不可数集。

EOA

Q 14 $O(g(n))$和$\Omega(g(n))$有什么不同的意义？

Ans 针对同一个问题，例如排序（Sorting）的问题，利用冒泡法（Bubble Sort），排序的问题可在$O(n^2)$的时间内解决，$O(n^2)$可说是一个上限。排序问题的下限为

$\Omega(n\log n)$，关于排序的相关上限和下限证明留到第三章再来细谈。我们以排序为例来画一个图（见图 1.2.1）以解释上限和下限两者的关系。

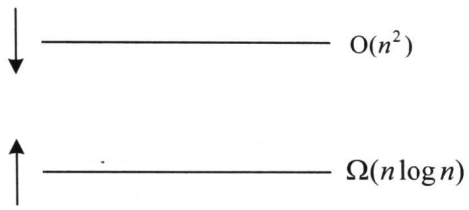


图 1.2.1　上限与下限的关系图

图 1.2.1 中的箭头↓表示排序的上限仍有向下修正的空间，而箭头↑表示排序的下限仍有向上修正的空间。上限的向下修正需要提出更好的排序算法，而下限的向上修正靠的是更严谨的理论证明。就排序而言，快速排序法（Quicksort）的时间复杂度为 $O(n\log n)$，其与下限 $\Omega(n\log n)$ 正好相遇，我们也称快速排序法为最佳排序法（Optimal Sorter）（见第三章的讨论）。

EOA

在这一节的集合讨论中，我们加入了 θ、O 和 Ω 三个复杂度的符号，可以说是一种比较新的安排。

1.3　多集合的运算与容斥原理

在上一节中，我们主要针对单集合的相关问题来阐述，在这一节中，我们将介绍多集合的相关问题。

Q1　集合之间常用到的运算有哪些？

Ans　令集合 $A=\{x,y,z\}$ 和集合 $B=\{x,y\}$，B 中的元素均属于 A，因为 B 为 A 的子集，我们称 B 包含于 A，可写成 $B\subset A$，也可以写成 $B\subseteq A$。两个集合之间常用的运算有交集 $\cap$（Intersection）、并集 $\cup$（Union）和差集 $-$（Difference）。先假设 U 为全集（Universal Set）且 $U=\{a,b,x,y,z\}$。则很容易验证 $A\cup\{a,b\}=U$、$A\cap B=B$、$A-B=\{z\}$ 和 $U-A=\{a,b\}$。单一集合 A 的补集（Complement）表示成 $\overline{A}=U-A$。例如 $\overline{B}=\{a,b,z\}$。另一种较特殊的运算为对称差集（Symmetric Difference），表示为 $A\oplus B=(A-B)\cup(B-A)=\{z\}$。

EOA

假设集合 A、集合 B 和全集 U 的关系如图 1.3.1 所示。

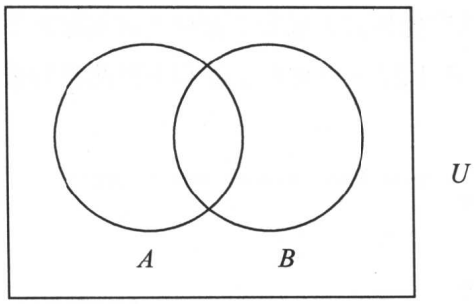
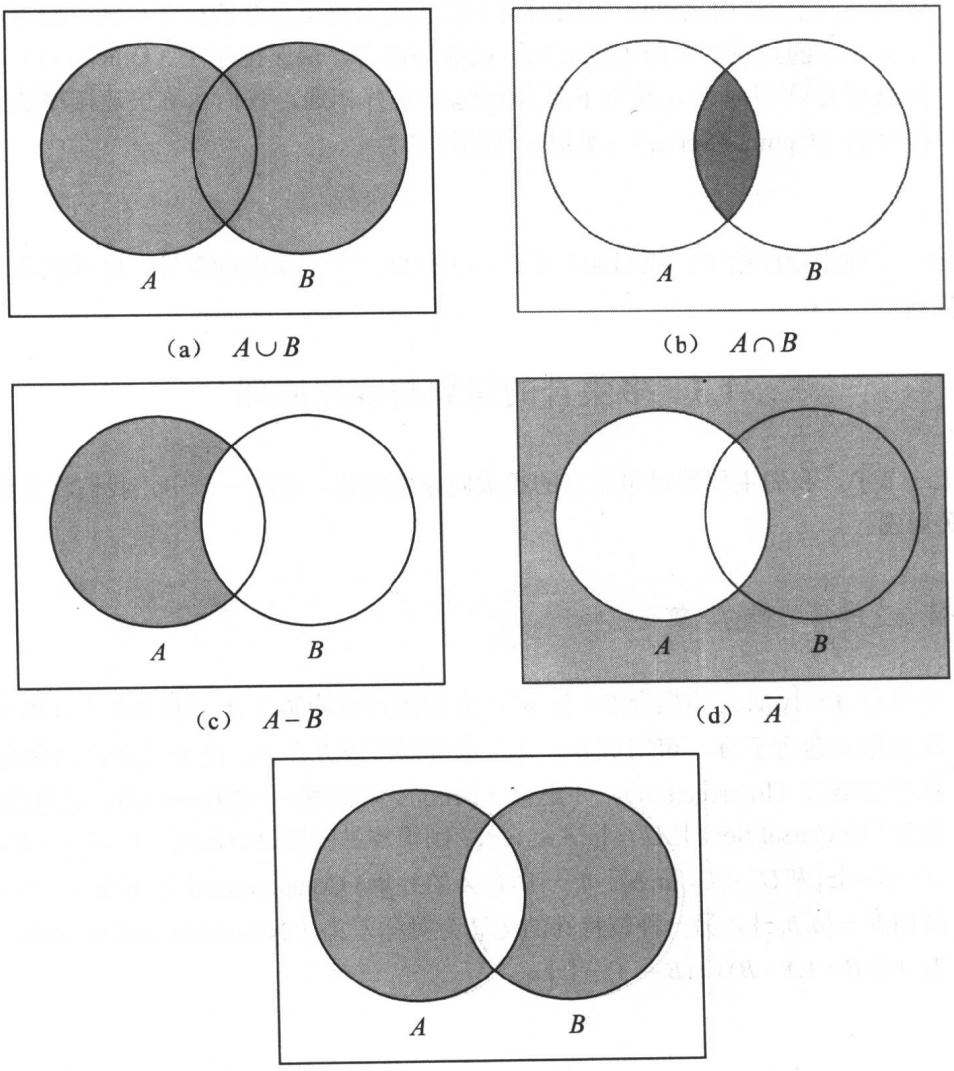


图 1.3.1 一个例子

上述的五个集合运算 $A\cup B$、$A\cap B$、$A-B$、$\overline{A}$ 和 $A\oplus B$ 的结果可用图 1.3.2（a）、（b）、（c）、（d）和（e）的阴影区域表示。



（a） $A\cup B$　　（b） $A\cap B$

（c） $A-B$　　（d） $\overline{A}$

（e） $A\oplus B$

图 1.3.2 五种集合运算

Q2 可否用较系统化的方法来证明多集合搭配运算的等式？

Ans 利用真值表（True Table）法来证明集合的等式是很系统化的方法。基本上，所谓的真值指的是集合中的某元素，若该元素在某集合S内，则S设定为 1 否则设定为 0。真值表示法用来证明集合等式是很简洁有力的。例如：要证明$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$这个等式。等式中并集对交集的分配律所对应的真值表如图 1.3.3 所示。由图中的第 4 列和第 6 列的相等性来看，确实上述的集合等式是成立的。

ABC	$A\cup B$	$A\cup C$	$(A\cup B)\cap(A\cup C)$	$B\cap C$	$A\cup(B\cap C)$
000	0	0	0	0	0
001	0	1	0	0	0
010	1	0	0	0	0
011	1	1	1	1	1
100	1	1	1	0	1
101	1	1	1	0	1
110	1	1	1	0	1
111	1	1	1	1	1

图 1.3.3　并集对交集分配律的真值表证法

EOA

其实，真值表法的证明方法也多少带有穷举的组合验证味道。利用上面的证法，很容易证得$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$（见习题 1.3.1）。

Q3 可否再利用真值表法证明另一个集合等式？

Ans 证明$\overline{A\cup B}=\overline{A}\cap\overline{B}$仿照上题的证法，我们可得图 1.3.4 的真值表：

A B	$A\cup B$	$\overline{A\cup B}$	$\overline{A}$ $\overline{B}$	$\overline{A}\cap\overline{B}$
0 0	0	1	1 1	1
0 1	1	0	1 0	0
1 0	1	0	0 1	0
1 1	1	0	0 0	0

图 1.3.4　$\overline{A\cup B}=\overline{A}\cap\overline{B}$ 的真值表证法

比较上面真值表中的第三列和第五列，可证得$\overline{A\cup B}=\overline{A}\cap\overline{B}$。

EOA