离散数学基础

柏元淮 冼其尤 编著

暨南大学出版社

离散数学基础

柏元淮　冼其尤　编著

暨南大学出版社

图书在版编目(CIP)数据

离散数学基础/柏元准　冼其尤编著.—广州:暨南大学出版社,1996.3
ISBN7—81029—462—8

Ⅰ.离
Ⅱ.柏
Ⅲ.离散数学
Ⅳ.O158

暨南大学出版社出版
(广州·石牌·510632)
新华书店经销
华夏激光照排中心
暨南大学印刷厂印刷
开本:850×1168　1/32
印张:7.625 印张　16.5 万字
版次:1995 年 12 月第 1 版
1996 年 1 月第 1 次印刷
印数:1—3000 册
定价:12.00 元

序

本教材是我们的离散数学讲义的重新编写本。离散数学是计算机科学的基础理论之一，它的每一个论题都是可以单独成书的。为了适应离散数学这门课程80个学时的教学需要，我们对材料进行了适当的取舍，力求贯彻少而精的原则。总的思想是，努力体现离散数学的主要内容和方法，避免内容庞杂，面面俱到。第一章是基础知识，介绍了集合、关系和映射。第二章、第三章是数理逻辑的内容，简要介绍了命题演算、谓词演算的思想和方法。第四章是图的理论。第五章和第六章属于代数结构方面的内容，初步介绍了格、布尔代数、群环域等结构。为了使学生更好地理解课程的内容和掌握必须的方法，我们在教材中没有减少例子的篇幅和习题的数量。从我们编写离散数学讲义，到现在出版这本离散数学基础，期间已数易其稿。尽管这样，由于作者水平有限，缺点错误在所难免，恳请读者不吝赐教。

作者感谢几何代数教研室的同志们对本书编写所给予的帮助，感谢多年来使用离散数学讲义的同志们所提出的宝贵意见。作者还感谢钱志大同志，他仔细阅读了本书的初稿，并提出了很多改进的意见。最后，作者感谢暨南大学出版社的同志们在印行本书过程中提供的有效和愉快的合作。

作者

1996年1月于

暨南大学

目 录

第一章
集合，关系和映射

§1.1 集合

我们采用朴素的观点来描述集合，那就是在一定范围内的讨论对象组成的整体称为集合.集合中的对象称为该集合的元素.

上面描述的并不是集合的定义.因为集合是最基本的概念，我们只能用“集合”这个词的某些同义词，例如“整体”来描述它，而不能用比“集合”更简单的概念来定义.下面的几个例子有助于理解集合这个术语的直观意义.

例 1 某校数学系一年级全体同学的集合.

例 2 三本不同的书 a, b, c 组成的集合 $\{a, b, c\}$.

例 3 所有自然数(即正整数)的集合 **N**;所有整数(即正整数、零、负整数)的集合 **Z**;所有有理数的集合 **Q**;所有实数的集合 **R**;所有复数的集合 **C**.

例 3 中给出的那些特殊集合的符号将在全书中自始至终使用.

通常以大写字母 $A, B, \cdots$ 代表集合. 集合 A 中的对象称为 A 的元, 或元素, 它们可以是具体的东西, 也可以是抽象的概念. 我们用小写字母 $a, b, \cdots$ 代表元素. 若 a 是集合 A 的元素, 则记 $a \in A$, 读作"a 是 A 的一个元素", 或者"a 属于 A"; 若 a 不是 A 的元素, 则记 $a \overline{\in} A$, 读作"a 不是 A 的元素", 或者"a 不属于 A".

设 n 是非负整数, 若集合 A 含有 n 个元素, 则称集合 A 的基数是 n, 记为 $|A| = n$. 如果集合 A 的基数是非负整数, 则称 A 是有限集合, 否则称 A 是无限集合. 例如上面例 1 和例 2 的集合都是有限集合, 而例 3 中的每个集合都是无限集合. 一个元素 a 作成的集合记为 $\{a\}$, 不含元素的集合称为空集. 空集记为 $\varnothing$. 空集 $\varnothing$ 的基数为 0, 即 $|\varnothing| = 0$. 请读者注意 $\varnothing$ 和 $\{\varnothing\}$ 的区别.

定义 1.1.1 设 A, B 是两个集合, 若 A 的元素都是 B 的元素, 则称 B 包含 A, 或称 A 是 B 的子集, 记为 $A \subseteq B$. 若 $A \subseteq B$, 但存在 $b \in B$, 使得 $b \overline{\in} A$, 则称 A 是 B 的真子集. 有时为了强调 A 是 B 的真子集, 此时也记为 $A \subset B$.

例如, 例 3 的集合之间有 $\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$.

易验证, 任意集合 A 均以空集 $\varnothing$ 为其一个子集合. 事实上, 若 $\varnothing$ 不是 A 的子集合, 则有 $x \in \varnothing$, 使 $x \overline{\in} A$. 但这是不可能的, 因为空集 $\varnothing$ 不包含任何元素. 故由子集的定义, $\varnothing \subseteq A$.

定义 1.1.2 若 A, B 两个集合的元素完全一样, 则称集合 A 等于集合 B, 记为 $A = B$.

$A = B$ 当且仅当 $A \subseteq B$ 且 $B \subseteq A$.

由旧的集合形成新集合有许多方法, 下面三种运算是基本的.

定义 1.1.3 A, B 是两个集合，所有属于 A 或者属于 B 的元素组成的集合，称为 A, B 的并集，记为 $A \cup B$.

定义 1.1.4 A, B 是两个集合，既属于 A 又属于 B 的元素组成的集合，称为 A, B 的交集，记为 $A \cap B$.

定义 1.1.5 A, B 是两个集合，属于 A 但不属于 B 的元素组成的集合，称为 A 与 B 的差集，记为 $A-B$.

定义 1.1.3、1.1.4 和 1.1.5 可以分别用符号表示为

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

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

$$A - B = \{x \mid x \in A \text{ 且 } x \overline{\in} B\}.$$

当我们讨论的集合都是某一集合的子集时，这一集合就称为全集. 全集常记为 E.

定义 1.1.6 设 A 是集合，全集 E 和 A 的差集称为 A 的余集，记为 $\overline{A}(=E-A)$.

定理 1.1.7 对任意集合 A, B, C，下面的法则成立：

(1)交换律：$A \cap B = B \cap A, A \cup B = B \cup A$.

(2)结合律：$(A \cap B) \cap C = A \cap (B \cap C)$,

$$(A \cup B) \cup C = A \cup (B \cup C).$$

(3)分配律：$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,

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

(4)吸收律：$A \cap (A \cup B) = A, A \cup (A \cap B) = A$.

(5)莫根律：$\overline{A \cap B} = \overline{A} \cup \overline{B}, \overline{A \cup B} = \overline{A} \cap \overline{B}$.

(6)幂等律：$A \cap A = A, A \cup A = A$.

(7)同一律：$A \cap E = A, A \cup \varnothing = A$.

(8)零　律：$A \cap \varnothing = \varnothing, A \cup E = E$.

(9)排中律：$A \cup \overline{A} = E$.

(10)矛盾律：$A \cap \overline{A} = \varnothing$.

(11)双重否定律：$A=A$.

利用定义1.1.2来证明这些法则是简单的：要证 $A=B$，即是去证 $A\subseteq B$ 且 $B\subseteq A$. 下面以证明莫根律的第一式为例来说明这一思想.

任取 $a\in\overline{A\cap B}\Rightarrow a\in E-(A\cap B)\Rightarrow a\in E$ 且 $a\overline{\in}A\cap B\Rightarrow a\in E$ 且 $a\overline{\in}A$ 或 $a\overline{\in}B\Rightarrow a\in\overline{A}$ 或 $a\in\overline{B}\Rightarrow a\in\overline{A}\cup\overline{B}$，即有 $\overline{A\cap B}\subseteq\overline{A}\cup\overline{B}$.

任取 $a\in\overline{A}\cup\overline{B}\Rightarrow a\in\overline{A}$ 或 $a\in\overline{B}\Rightarrow a\in E$ 和 $a\overline{\in}A\cap B\Rightarrow a\in\overline{A\cap B}$，故又有 $\overline{A}\cup\overline{B}\subseteq\overline{A\cap B}$.

综合得 $\overline{A\cap B}=\overline{A}\cup\overline{B}$.

以上介绍了集合间的三种基本运算并、交、差. 下面再介绍两种由旧的集合组成新集合的方法，它们在以后常要遇到.

定义1.1.8 设 A 是集合. A 的所有子集构成的集合称为 A 的幂集合，记为 $\rho(A)$（或 2^A）.

幂集合 $\rho(A)$ 可用符号表示为

$$\rho(A)=\{x\mid x\subseteq A\}.$$

若有限集合 A 的基数是 n，则 $\rho(A)$ 有

$$C_n^0+C_n^1+C_n^2+\cdots+C_n^n=2^n$$

个元素，即 $|\rho(A)|=2^{|A|}$. 例如 $A=\{1,2,3\}$，则

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

定义1.1.9 设 A,B 是集合. 所有序偶 $(x,y)(x\in A,y\in B)$ 组成的集合称为 A,B 的直乘积（或加氏积），记为 $A\times B$. 当 A,B 至少有一个为空集 $\varnothing$ 时，规定 $A\times B=\varnothing$.

A,B 的直乘积 $A\times B$ 可用符号表示为

$$A\times B=\{(x,y)\mid x\in A,y\in B\}.$$

直乘积 $A\times B$ 里的元素 (x,y) 和 (x',y') 称为相等，当且仅当 $x=x',y=y'$. 当 A,B 均为有限集合时，$A\times B$ 也是有限集

合，且$|A\times B|=|A|\cdot|B|$.

例如$A=\{1,2\}$，$B=\{3,4\}$，则

$$A\times B=\{(1,3),(1,4),(2,3),(2,4)\}.$$

确定一个集合就是确定它的元素.换句话说，集合 A 被确定，当且仅当我们能够断定任何给定的对象 x 是否属于 A.通常，集合 A 的元素通过它们所具有的一些公共性质被确定.因此，一个集合 A 实际上就确定了一个性质 P.例如，对于集合 A，我们可以规定性质 P 如下：若 $x\in A$，则 x 具性质 P；$x\overline{\in}A$，则 x 无性质 P.反之，一个性质 P 实际上也确定了一个集合 A.事实上，我们可以令集合 A 为由所有具有性质 P 的元素组成.于是，集合 A 可以由如下方式表示：

$$A=\{x\mid x\text{ 具性质 }P\}.$$

例如，前面关于集合的并、交、差、幂集合和直乘积的符号表示就是这样的表示法.又如，非负整数集合，平面上单位圆圆周上点的集合可分别表示为：

$$\mathbf{Z}^{+}=\{x\mid x\in\mathbf{Z},x\geqslant 0\},$$

$$\mathbf{B}=\{(x,y)\mid x^2+y^2=1,(x,y)\in\mathbf{R}\times\mathbf{R}\},$$

等等.

习题

(1)设 $A=\{2,a,\{3\},4\}$，$B=\{\{a\},3,4,1\}$.指出下面哪些写法是对的，哪些是错的.

$\{a\}\in A$，$\{a\}\subset A$，$\{a,4,\{3\}\}\subseteq A$，$A=B$，$\{a\}\in B$，

$\{a\}\subset B, \varnothing\subset\{\{a\}\}\subset A\subseteq E, \{\varnothing\}\subseteq A, \varnothing\subseteq B, \varnothing\subseteq\varnothing, \varnothing\in\varnothing, \varnothing\subseteq\{\varnothing\}, \varnothing\in\{\varnothing\}$.

(2)设 A, B 如第(1)题,写出 $A\times B, \rho(A)\cap\rho(B)$.

(3)证明:关于任意集合 A, B,下面三个论断等价:

(ⅰ)$A\subseteq B$.

(ⅱ)$A\cup B=B$.

(ⅲ)$A\cap B=A$.

(4)对于任意集合 A, B,证明 $A-B=A\cap\overline{B}$.由此并利用法则 1.1.7 证明:

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

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

(5)令

$A=\{(a,b)\mid a\in\mathbf{R}, b\in\mathbf{R}, a\geqslant b\}$,

$B=\{(a,b)\mid a\in\mathbf{R}, b\in\mathbf{R}, a\leqslant b\}$.

求 $\overline{A}, \overline{B}, A\cap B, A\cup B, A-B$.

(6)对任意集合 A, B,证明:

(ⅰ)$\rho(A)\cup\rho(B)\subseteq\rho(A\cup B)$,举例说明等号可以不成立.

(ⅱ)$\rho(A)\cap\rho(B)=\rho(A\cap B)$.

(7)对任意集合 A, B, C,证明:

(ⅰ)$A\times(B\cup C)=(A\times B)\cup(A\times C)$.

(ⅱ)$(A\cap B)\times C=(A\times C)\cap(B\times C)$.

§1.2 关系

"关系"是日常生活中的一个基本概念.事物之间不是存在着这种关系,就是存在着那种关系.如人群中有朋友关系、同学

关系、师生关系等等."关系"也是数学上的一个基本概念.例如实数的相等关系、大于关系、小于关系;三角形的全等关系、相似关系等等.本节中,我们在集合中引进关系这一概念.集合中给出的一个关系,实际上描述了这个集合中有关系的两个元素之间的一种特征,而这种特征也可以借用一个集合来刻画.换言之,我们可以用集合来定义关系.

定义 1.2.1 设 A, B 是集合.直乘积 $A \times B$ 的一个子集 R,称为 A 到 B 的一个二元关系.特别,当 $A = B$ 时,$A \times A$ 的一个子集 R 称为 A 上的一个二元关系,简称 A 上的一个关系.

若 $(x, y) \in R$,则称 x, y 有关系 R,记为 xRy.若 $(x, y) \overline{\in} R$,则称 x, y 没有关系 R,记为 $x \overline{R} y$.

例 1 令 $A = \{1, 2, 3\}$, $B = \{a, b, c\}$.则

$$R = \{(1, a), (1, c), (2, b)\}$$

就是 A 到 B 的一个二元关系.令

$$P = \{(x, y) \mid x \in \mathbf{N}, y \in \mathbf{N}, x = y\},$$

则 P 是自然数集合 $\mathbf{N}$ 上通常的数的相等关系.

例 2 对于任意集合 A, A 上如下三种特殊的关系在以后都要遇到.

(1)空关系 $\varnothing$,即 $A \times A$ 的空子集 $\varnothing$.

(2)全域关系 E_A: $E_A = A \times A$.

(3)恒等关系 I_A: $I_A = \{(x, x) \mid x \in A\}$.

定义 1.2.1 实际上是用集合来表示关系.有限集合上的关系还可以用矩阵表示或用图表示.

设 A 是基数为 n 的非空有限集,给定 A 的元素的一个顺序 $v_1, v_2, \cdots v_n$. R 是 A 上的一个关系.定义 $M(R) = (a_{ij})_{n \times n}$,式中

$$a_{ij}=\begin{cases}1, \text{若 } v_iRv_i;\\ 0, \text{若 } v_i\overline{R}v_j.\end{cases}$$

矩阵 $M(R)$称为 R 的关系矩阵.

仍设 A 是基数为 n 的非空有限集,给定 A 的元素的一个顺序 $v_1, v_2, \cdots, v_n$. R 是 A 上的一个关系.构作一个图 D 如下.以 $v_1, v_2, \cdots, v_n$ 作为顶点集合,若$(v_i, v_j)\in R$,则从 v_i 到 v_j 连一条有向弧(箭头指向 v_j).这样得到的(有向)图 D 称为 R 的关系图.

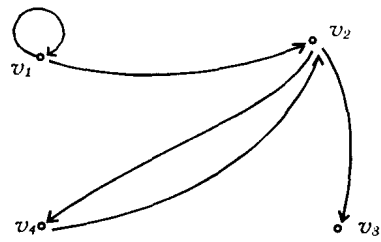
例 3 设 $A=\{v_1, v_2, v_3, v_4\}$, A 上的关系

$R=\{(v_1, v_1), (v_1, v_2), (v_2, v_3), (v_2, v_4), (v_4, v_2)\}$,

R 的关系矩阵

$$M(R)=\begin{pmatrix}1&1&0&0\\0&0&1&1\\0&0&0&0\\0&1&0&0\end{pmatrix}.$$

R 的关系图 D 为



定义 1.2.2 设 P, R 是集合 A 上的两个关系.

(1)称关系 R 包含关系 P,如果

$$aPb\Rightarrow aRb.$$

此时记 $P\subseteq R$.

(2)称关系 R 是关系 P 的转置,如果

$$aPb\Leftrightarrow bRa.$$

此时记 $P=R^T$.

(3)P 和 R 的积 $P\cdot R$(或 PR)是如下定义的 A 上的关系:

$aPRb\Leftrightarrow$存在 $c\in A$ 使 aPc 且 cRb.

(4)P 与 R 的和 $P+R$ 是如下定义的 A 上的关系:

$a(P+R)b\Leftrightarrow aPb$ 或 aRb.

易知,若关系 P 是关系 R 的转置,则关系 R 也是关系 P 的转置,由此便有 $(R^T)^T=R$. 又当 $P=R$ 时,R 和 R 的积记为 R^2. 规定 $R^0=I_A$,则对任意非负整数 n,可归纳定义 n 个 R 的积 R^n. 最后,看 $P,R,P+R$ 为 $A\times A$ 的子集,显然有 $P+R=P\cup R$.

不难验证,对有限集合 A 上的关系 P,R 有

$$M(R^T)=M(R)^T;$$

$$M(PR)=M(P)M(R);$$

$$M(P+R)=M(P)+M(R),$$

式中矩阵元素乘法是布尔积,矩阵元素加法是布尔和:

·	0	1
0	0	0
1	0	1

+	0	1
0	0	1
1	1	1

例4 $A=\{a,b,c\}$. $R=\{(a,b),(a,c),(b,c)\}$, $P=\{(a,b),(b,a),(c,a)\}$. 则

$$R^T=\{(b,a),(c,a),(c,b)\},$$

$$PR=\{(a,c),(b,b),(b,c),(c,b),(c,c)\},$$

$$RP=\{(a,a),(b,a)\},$$

$$P+R=\{(a,b),(a,c),(b,a),(b,c),(c,a)\}.$$

$$R^2=\{(a,c)\},R^3=\varnothing.$$

$$P^2=\{(a,a),(b,b),(c,b)\},P^3=P.$$

定义 1.2.3 设 R 是 A 上的关系. R 的传递闭包 R^+ 是如下定义的 A 上的关系:

$$aR^+b\Leftrightarrow\text{存在 } n>0 \text{ 使 } aR^nb.$$

由定义易知

$$R^+=R^1+R^2+R^3+\cdots+R^n+\cdots,$$

当 A 是有限集合时,

$$M(R^+)=M(R)+M(R)^2+M(R)^3+\cdots+M(R)^n+\cdots.$$

例 5 设 R 是 A 上的关系. R 的关系矩阵

$$M(R)=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix},$$

则 $M(R^+)=M(R)$, 即有 $R^+=R$. 又设 P 是 B 上的关系. P 的关系矩阵

$$M(P)=\begin{pmatrix}1&1&0&1\\0&1&1&0\\0&1&0&1\\1&1&0&0\end{pmatrix},$$

则 $M(P^+)=\begin{pmatrix}1&1&1&1\\1&1&1&1\\1&1&1&1\\1&1&1&1\end{pmatrix}$, 即 $P^+=E_B$.

定义 1.2.4 集合 A 上的关系 R 称为有反身性, 如果对任意 $x\in A$, 都有 xRx.

集合 A 上的关系 R 称为有对称性，如果 xRy，则有 yRx，其中 $x\in A, y\in A$.

集合 A 上的关系 R 称为有传递性，如果 xRy，yRz，则有 xRz，其中 $x\in A, y\in A, z\in A$.

集合 A 上的关系 R 称为有反对称性，如果 xRy，yRx，则有 $x=y$，其中 $x\in A, y\in A$.

例 6 **R** 上的关系

$$R=\{(x,y)\mid x=y\}$$

具有反身、对称、传递和反对称性质. **R** 上的关系

$$P=\{(x,y)\mid x\geqslant y\}$$

具有反身性、传递性和反对称性，但无对称性.

令 $A=\{1,2,3,4\}$. $R=\{(1,2),(2,1),(2,3)\}$ 是 A 上的关系. 易知，R 没有反身性，没有对称性，没有传递性，也没有反对称性.

设 R 是有限集合 A 上的关系. R 是反身的当且仅当 R 的关系图的每个顶点都有一条以该顶点为起点和终点的弧(这样的弧称为环)，当且仅当 R 的关系矩阵 $M(R)$ 的主对角线元素全不为零. 关系 R 是对称的当且仅当 R 的关系图中，对任意两个不同的顶点 u，v，若有从 u 到 v 的弧，则也有从 v 到 u 的弧，当且仅当 R 的关系矩阵 $M(R)$ 是对称矩阵. 关系 R 是传递的当且仅当 $R^2\subseteq R$，当且仅当 $R^+=R$.

从上面的例 6 可以看出，在一个集合上可以给出不同的关系. 对于集合的某个关系，它可能具有定义 1.2.4 中的某一个或某几个性质，也可能不具有定义 1.2.4 中的任何一个性质. 下面我们介绍集合的两种重要关系：等价关系和半序关系.

定义 1.2.5 设 A 是非空集合，R 是 A 上的一个关系. 如果 R 具有反身性、对称性和传递性，则称 R 是 A 上的一个等价