高等学校试用教材

离散数学

王湘浩　管纪文　刘叙华

高等教育出版社

高等学校试用教材

离散数学

王湘浩　管纪文　刘叙华

高等教育出版社

内 容 提 要

本书是以吉林大学计算机科学系离散数学讲义为基础，经过修改补充编写而成的。全书着重介绍了离散数学各分支的一些基本内容，主要包括：集合、关系与映射、图论基础、数理逻辑、整数理论以及代数结构等。本书可作为高等学校计算机有关专业离散数学课程的试用教材或参考书，也可供从事计算机工作的有关人员参考。

责任编辑：鲍 涌

高等学校试用教材

离 散 数 学

王湘浩 管纪文 刘叙华

*

高等教育出版社出版

新华书店北京发行所发行

北京印刷三厂印装

*

开本 850×1168 1/32 印张 7.5 字数 181,000

1983年5月第1版 1983年10月第1次印刷

印数 00,001—20,500

书号13010·0866 定价 0.86 元

序

这本教材是以吉林大学计算机科学系离散数学的讲义为基础，经过修改补充而定稿的．鉴于学生学习本课时，是初次接触较抽象的数学，因此这次修改力求做到容易懂和少而精，避免内容庞杂和名词罗列．我们认为，本课除了使学生获得必要的知识，还应培养学生的数学能力，以便日后有所需要时，学生能够自己阅读进一步的材料．而那些庞杂的内容和纷繁的名词只能起到干扰作用，无助于数学能力的提高，即使当时能够记住，过些时候也就忘了．当然，少而精和容易懂都不是很容易做到的，希望使用这本教材的老师和同学，多向我们提出宝贵意见，以便我们进一步修改。

第一章介绍集合，包括映射和关系等基础知识．

第二章和第三章属于数理逻辑部分，这两章主要介绍命题逻辑和一阶逻辑的基本知识，我们的注意力不在于数理逻辑这门科学本身所着重的问题，而在于将数理逻辑做为一种数学工具，应用在计算机科学上所应掌握的必备知识．

第四章介绍图论方面的基本知识。

第五章介绍整数的理论．

第六章、第七章属于近世代数的群环域部分，这两章主要是利用吉林大学从一九五三年到现在数学系和计算机科学系讲授近世代数的材料编写的．一般离散数学书多侧重群论，环和域的内容很少．我们认为，环的有些内容和群是平行的，讲了群以后，再讲环的这些内容可以只用很少的时间，或主要让学生自学．第七章的多项式部分可能要和高等代数的内容有重复，如果在那里已经

学了这些内容，这里当然就可以略去不讲．因此，和一般离散数学相比较，这本书实际上只是多一点数论和有限域．我们觉得，至少对于软件专业的学生来说，这些是完全必要的．单位根和有限域我们尝试用一种新的讲法，以便学生易于接受．

第八章介绍布氏代数和格论方面基础知识，特别，讨论了有限布尔代数的性质和布尔表达式的化简问题．

作者对王钲旋，谷新英两位同志表示感谢，他们在校对原稿时提出了宝贵意见，付出了辛勤的劳动．

作者

1983 年 3 月 1 日于长春吉林大学

目　录

第一章 集 合

§1 基本概念

集合是数学中最基本的概念. 当我们讨论某一类对象的时候, 就把这一类对象的整体称为集合. 而集合中的对象就称为该集合中的元素.

设 A 是一个集合, a 是集合 A 中的元素, 今后将这一事实记以 $a\in A$, 读做 a 属于 A; 若 a 不是集合 A 中的元素, 则记以 $a\notin A$, 读做 a 不属于 A.

例如, 这间课堂里所有桌子的整体就做成一个桌子集合. 每一个桌子都属于这个集合, 每一个椅子都不属于这个集合.

又如, 世界上所有哺乳动物的整体做成一个哺乳动物集合. 每一条狗都属于这个集合, 每一只青蛙都不属于这个集合.

又如, 平面上的所有点的整体做成平面点集; 所有连续函数的整体做成连续函数集, 等等.

有限个元素 $a_1, \cdots, a_n$ 做成的集合, 称为有穷集, 记以 $\{a_1, \cdots, a_n\}$; 无限个元素做成的集合, 称为无穷集.

特别, 不含元素的集合称为空集, 记以 ϕ. 一个元素 a 做成的集合, 记为 $\{a\}$.

定义 1 当 A, B 两个集合的元素完全一样, 即 A, B 两个集合实际上是同一集合时, 则称集合 A, B 相等, 记以 $A=B$.

定义 2 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, 记以 $A\subseteq B$. 若 $A\subseteq B$, 且 $A\neq B$, 则称 A 是 B 的真子集, 记以 $A\subset B$.

当我们所讨论的集合都是某一集合的子集时，这一集合就称为全集，记为 E.

由定义，下面的结论是显然的：对于任意两个集合 A, B, $A=B$ 的充要条件是 $A\subseteq B$ 且 $B\subseteq A$.

定义 3 设 A 是集合，A 的所有子集做成的集合称为 A 的幂集，记为 $\rho(A)$ 或 2^A.

显然，若 A 为有穷集，元素数为 n，则 2^A 的元素数为

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

定义 4 设 A, B 是两个集合. 属于集合 A 而不属于集合 B 的所有元素组成的集合，称为 A 与 B 的差集，记为 $A-B$.

例如，令 $A=\{a, b, c, d\}$, $B=\{b, c, f, g\}$，于是 $A-B=\{a, d\}$.

又如，令 $A=\{a, b, c, d\}$, $B=\{e, f, g\}$，于是 $A-B=\{a, b, c, d\}$.

定义 5 设 A, B 为两个集合，所有序偶 (x, y) 做成的集合（其中 $x\in A, y\in B$），称为 A, B 的直乘积，记为 $A\times B$.

例如，令 A 是直角坐标系中 x 轴上的点集，B 是 y 轴上的点集，于是，$A\times B$ 就和平面点集一一对应.

定义 6 设 A, B 是两个集合. 所有属于 A 或者属于 B 的元素做成的集合，称为 A 和 B 的并集，记为 $A\cup B$.

例如，令 $A=\{a, b, c, d\}$, $B=\{c, d, e\}$，于是 $A\cup B=\{a, b, c, d, e\}$.

定义 7 设 A, B 是两个集合. 由既属于 A 又属于 B 的元素做成的集合，称为 A 和 B 的交集，记为 $A\cap B$.

例如，令 $A=\{a, b, c, d\}$, $B=\{a, c, e, f\}$，于是 $A\cap B=\{a, c\}$.

定义 8 设 A 是一个集合，全集 E 与 A 的差集称为 A 的余集，记为 $\bar{A}$.

例如，令 $E=\{a,b,c,d,e\}$，$A=\{a,b\}$，于是 $\bar{A}=\{c,d,e\}$.

又如，令 E 是全体人类做成的集合，A 是所有身高小于 1.60米的人做成的集合，于是，$\bar{A}$ 是所有身高大于或等于 1.60 米的人做成的集合.

不难证明，对于任意集合 A,B,C 有如下算律：

1. $A\cap A=A, A\cup A=A$.
2. $A\cap B=B\cap A, A\cup B=B\cup A$. （交换律）
3. $(A\cap B)\cap C=A\cap(B\cap C)$,
   $(A\cup B)\cup C=A\cup(B\cup C)$. （结合律）
4. $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$,
   $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$. （分配律）
5. $A\cap(A\cup B)=A, A\cup(A\cap B)=A$. （吸收律）
6. $A\cap\bar{A}=\phi$, $A\cup\bar{A}=E$.
7. $\overline{(A\cap B)}=\bar{A}\cup\bar{B}$,
   $\overline{(A\cup B)}=\bar{A}\cap\bar{B}$. （De Morgan 律）
8. $E\cap A=A, E\cup A=E$.
9. $\phi\cap A=\phi, \phi\cup A=A$.

例如，我们来证明：$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$.

任取 $a\in A\cap(B\cup C)$，即 $a\in A$ 且 $a\in B\cup C$. 亦即 $a\in A$ 且 $a\in B$ 或 $a\in C$. 于是 $a\in A\cap B$ 或者 $a\in A\cap C$，故 $a\in(A\cap B)\cup(A\cap C)$. 即证得

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

任取 $a'\in(A\cap B)\cup(A\cap C)$，即 $a'\in A\cap B$ 或者 $a'\in A\cap C$，亦即 $a'\in A$ 且 $a'\in B$，或者 $a'\in A$ 且 $a'\in C$. 总之，$a'\in A$，且 $a'\in B$ 或者 $a'\in C$，即 $a'\in A$ 且 $a'\in B\cup C$，故 $a'\in A\cap(B\cup C)$. 即证得

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

总之，我们证明了：

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

一个集合 S 实际上就确定了一个性质 P，例如，规定性质 P 如下：若 $x\in S$，则称 x 有性质 P；否则，x 无性质 P.

一个性质 P 实际上也确定了一个集合 S. 例如，我们令集合 S 由所有具有性质 P 的元素做成.

因此，集合 S 可以用如下方式表示：

$$S=\{x\mid x\text{ 具有性质 }P\}$$

例如，在直角坐标系中，以坐标原点为心的单位圆圆周上所有点做成的集合 S 可表示如下：

$$S=\{(x,y)\mid x^2+y^2=1\}$$

又如，设 A,B 是两个集合，A 和 B 的交集可表示如下：

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

习　题

1. 设 $S=\{2,a,\{3\},4\}$，$R=\{\{a\},3,4,1\}$ 指出下面的写法哪些是对的，哪些是错的：

$\{a\}\in S$，$\{a\}\in R$，$\{a,4,\{3\}\}\subseteq S$，$\{\{a\},1,3,4\}\subset R$，$R=S$，$\{a\}\subseteq S$，$\{a\}\subseteq R$，$\phi\subseteq R$，$\phi\subseteq\{\{a\}\}\subseteq R\subseteq E$，$\{\phi\}\subseteq S$，$\phi\in R$，$\phi\subseteq\{\{3\},4\}$.

2. 写出下面集合的幂集合

$\{a,\{b\}\}$，$\{1,\phi\}$，$\{X,Y,Z\}$.

3. 对任意集合 A，B，证明：

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

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

举例说明：$\rho(A)\cup\rho(B)\neq\rho(A\cup B)$.

§2 关　系

在日常生活中，象在数学中一样，关系的概念是一个基本概

念. 例如, 在人群中有朋友关系, 父子关系, 同学关系等等; 在数学中有相等关系, 整除关系, 小于关系, 大于关系等等.

不难看到, 每一种关系都描述了在某一集合中两个元素之间的一种特征. 而这种特征也可以用一个集合描述出来.

定义 1 设 A 是一个集合, 由 A 中元素做成的一些有序对的集合 R, 亦即集合 $A\times A$ 中的一个子集 R, 称为集合 A 上的一个二元关系, 简称为关系. 对于 $x\in A, y\in A$, 若 $(x,y)\in R$, 则称 x, y 有关系 R, 记以 xRy; 若 $(x,y)\notin R$, 则称 x, y 没有关系 R, 记以 $x\not{R}y$.

例如:

自然数之间的大于关系 $=\{(x,y)\mid x, y$ 是自然数并且 $x>y\}$

人群中的父子关系 $=\{(x,y)\mid x, y$ 是人并且 x 是 y 的父亲$\}$

若 R, S 是集合 A 上的两个关系, 并且 $R\subseteq S$, 则称 R 为 S 的子关系.

即然关系是集合, 那么自然在关系之间也有象集合之间那样的交, 并, 余等运算.

例如: 设 R, S 是集合 A 上的两个关系, 于是对 $x\in A, y\in A$, 有

$x(R\cup S)y\Longleftrightarrow xRy$ 或者 xSy.

$x(R\cap S)y\Longleftrightarrow xRy$ 并且 xSy.

$x\bar{R}y\Longleftrightarrow x\not{R}y$.

定义 2 集合 A 上的关系 R 称为有反身性, 如果对每个 $x\in A$, 都有 xRx.

定义 3 集合 A 上的关系 R 称为有对称性, 如果 xRy, 则 yRx. 其中 $x\in A, y\in A$.

定义 4 集合 A 上的关系 R 称为有反对称性, 如果 xRy, yRx, 则必有 $x=y$. 其中 $x\in A, y\in A$.

定义 5 集合 A 上的关系 R 称为有传递性，如果 xRy, yRz，则 xRz. 其中 $x\in A, y\in A, z\in A$.

例如，数之间的相等关系，具有反身性，对称性，传递性，反对称性. 小于关系和大于关系没有反身性，没有对称性，但是有反对称性和传递性. 父子关系既无反身性，也无对称性又无传递性，但是具有反对称性.

定义 6 设 R 是集合 A 上的一个关系，令

$$R^{-1}=\{(y,x)\mid x\in A, y\in A, \text{并且有 } xRy\}$$

则称关系 R^{-1} 为关系 R 的逆.

例如，小于关系的逆关系是大于关系，大于关系的逆关系是小于关系，相等关系的逆关系仍是相等关系.

显然，对任意关系 R，$R=R^{-1}$ 的充要条件是 R 具有对称性.

定义 7 设 R, S 是集合 A 上的两个关系，令

$R\cdot S=\{(x,y)\mid x\in A, y\in A \text{ 并且有一个 } z\in A \text{ 使得 } xRz, zSy\}$.

称关系 $R\cdot S$ 为关系 R 和 S 的乘积.

不难证明，关系的乘法满足结合律，但是不满足交换律.

定理 1 集合 A 上的关系 R 具有传递性的充要条件是 $R\cdot R\subseteq R$（$R\cdot R$ 可简记为 R^2）.

证明：必要性. 若 R 具有传递性，任取 $(x,y)\in R^2$，于是存在 $z\in A$，使得

$$xRz,\quad zRy$$

因为 R 是传递的，所以有 xRy，即 $(x,y)\in R$.

故 $R^2\subseteq R$.

充分性. 若 $R^2\subseteq R$，如果 xRy, yRz，则 xR^2z. 故 xRz. 所以 R 是传递性的.

在日常生活中和在数学中，我们常常碰到对一些对象进行分类的问题. 例如，对一些几何图形，我们可以使用面积之间的相等

关系将这些几何图形分类，即面积相等的几何图形算做一类，这种分类使得每个几何图形都必定属于某类，并且不同类之间没有公共元素．又如，在人群中，我们可以用同性关系将人群分类，即同性别的人算做一类．这种分类也使得每一个人都必定属于某类，并且不同类之间没有公共元素．

因此，任意一个分类法总是在某一观点下把一些元素看做是同样的，并且希望每一个元素在这种分类法下都必定属于而且仅仅属于某一类．具有这种功能的分类法，在数学上就叫做一个等价关系，其严格定义如下：

定义 8 设A是一个非空集合，$\cong$是A上的一个关系．如果$\cong$具有反身性，对称性，传递性，则称$\cong$是一个等价关系．

例如，上面提到的几何图形的面积之间的相等关系，人群中的同性关系都是等价关系．

定义 9 设A是一个非空集合，$\cong$是A上的等价关系．A的一个非空子集M叫做一个等价类，如果

1）若$a\in M, b\in M$，则$a\cong b$．

2）若$a\in M, b\notin M$，则$a\ncong b$；或者

若$a\in M, a\cong b$，则$b\in M$．

换句话说，如果M中任意两个元素等价，而M中任意元素与M外任意元素不等价，则M就是一个等价类．

例如，上面提到的，所有面积相等的几何图形就组成一个等价类（在面积相等关系下），所有男人就组成一个等价类（在同性关系下）．

定理 2 设$\cong$是集合A上的等价关系，于是等价类是存在的．

证明： 任取$a\in A$，令

$$M=\{x\mid x\in A \text{ 并且 } x\cong a\}$$

显然，M非空．

任取 $x_1 \in M, x_2 \in M$, 由于 $x_1 \cong a, x_2 \cong a$, 而$\cong$具有对称性, 传递性, 所以 $x_1 \cong x_2$.

任取 $x_1 \in M$, 若 $x_1 \cong y$, 则由于 $x_1 \cong a$, 所以 $y \cong a$, 故 $y \in M$.

因此, M是一个等价类.

定理 3 设$\cong$是集合 A 上的等价关系, $M_1, M_2, \cdots$, 是 A 中所有等价类. 于是

$$A = M_1 \cup M_2 \cup \cdots$$

并且 $M_i \cap M_j = \phi (i \neq j)$. 亦即, 集合 A 上的等价关系把 A 分成了互不相交的等价类.

证明: 任取 $M_i, M_j, i \neq j$. 若有 $x \in M_i \cap M_j$, 则任取 $a \in M_i$, $b \in M_j$, 都有 $a \cong x, b \cong x$, 故 $a \cong b$, 故 $M_i = M_j$, 矛盾.

任取 $a \in A$, 令

$$M = \{x \mid x \in A \text{ 并且 } x \cong a\}$$

由定理 2 知, M是等价类, 故有 k, 使得 $M = M_k$. 因为 $a \in M$, 所以 $a \in M_1 \cup M_2 \cup \cdots \cup M_k \cup \cdots$. 故 $A \subseteq M_1 \cup M_2 \cup \cdots$.

显然有 $M_1 \cup M_2 \cup \cdots \subseteq A$.

故 $A = M_1 \cup M_2 \cup \cdots$.

下面我们讨论另一种重要的关系——部分序关系.

定义 10 设R是集合 A 上的一个关系. 如果R具有反身性, 反对称性, 传递性, 则称 R 为一个部分序关系(或称半序关系). 集合 A 在部分序关系R下做成一个部分序集.

显然, 一个部分序集的子集仍为部分序集.

例如, 集合中的包含关系就是一个部分序关系, 由一些集合做为元素而做成的集合, 在集合的包含关系下是一个部分序集.

通常, 将部分序关系R写做$\leqslant$, 读做"小于或等于"

定义 11 一个部分序集 A(其部分序关系为$\leqslant$)说是一个序集,如果对 A 中任意两个元素 a, b,必有 $a\leqslant b$ 或者 $b\leqslant a$. 序集有时也称为链.

显然,序集的子集仍为序集.

例如,数的集合在数的大小关系下做成一个序集.

设 A 是一个部分序集,其部分序关系为$\leqslant$. 如果 A 中有一个元素 a,对于所有的 $x\in A$,都有 $x\leqslant a(a\leqslant x)$,则称 a 为集合 A 的最大(最小)元素.

A 中元素 a 说是一个极大(极小)元素,如果除 a 之外,A 中没有元素 x,使得 $a\leqslant x(x\leqslant a)$.

对于 A 中的子集 M,A 中元素 a 称为子集 M 的一个上界(下界),如果对 M 中任意元素 m,都有 $m\leqslant a(a\leqslant m)$. M 的上界(下界)未必在 M 中,甚至 M 未必有上界(下界).

对于 A 的子集 M,A 中元素 a 称为 M 的最小上界(或称上确界),如果 a 是 M 的一个上界,并且对 M 的任意一个上界 x,都有 $a\leqslant x$.

同理,可定义 M 的最大下界(或称下确界).

一个部分序集,可以用所谓 Hasse 图直观地表示出来. Hasse 图的画法如下:以平面上的点代表部分序集中的元素.

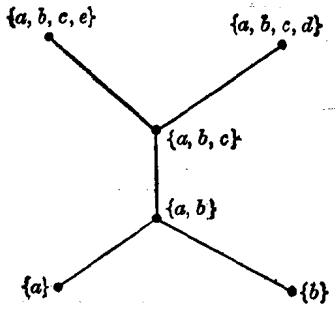
1) 若 $x\leqslant y$,且 $x\neq y$,则将 x 画在 y 的下面.

2) 若 $x\leqslant y, x\neq y$,并且没有不同于 x, y 的 z,使得 $x\leqslant z\leqslant y$,则在 x, y 之间用直线连结.

例如,令

$$A=\{\{a\},\{b\},\{a,b\},\{a,b,c\},\{a,b,c,d\},\{a,b,c,e\}\}$$

显然,A 在集合的包含关系下是一个部分序集. A 的 Hasse 图如下:



此部分序集中无最大，最小元素．但是有极大，极小元素．$\{a, b, c, d\}$和$\{a, b, c, e\}$是极大元素，$\{a\}$，$\{b\}$是极小元素．

对于子集$\{\{a\}, \{b\}\}$，$\{a, b\}$是其最小上界，但是，此子集无下界，当然更没有最大下界．

习　题

1. 设 R, S 是集合 A 上的两个关系．试证明下列等式：

$$(R \cdot S)^{-1} = S^{-1} \cdot R^{-1}$$

$$(R^{-1})^{-1} = R$$

$$(R \cup S)^{-1} = R^{-1} \cup S^{-1}$$

$$(R \cap S)^{-1} = R^{-1} \cap S^{-1}$$

2. 设 R 是集合 A 上的关系．令

$$R^{+} = \{(x, y) \mid x \in A, y \in A \text{ 并且存在 } n > 0, \text{使得 } xR^{n}y\}$$

称 R^{+} 是 R 的**传递闭包**．证明：R^{+}是包含 R 的最小具有传递性的关系．

3. 若关系 R 是不反身的，是对称的，试证明 R 不是传递的．

4. 若集合 A 上的关系是对称的，反对称的，试指明关系 R 的结构．

5. 若集合 A 上的关系 R 具有传递性，则 $R^{+} = R$．

6. 设 R 是集合 A 上的关系．如果

1) 对任意 $a \in A$，都有 aRa．

2) 若 aRb, aRc，则 bRc．

证明：R 是等价关系．

7. 有人说："等价关系中的反身性可以不要，因为反身性可以从对称性