离散数学基础

洪 帆 编

華中工學院出版社

离散数学基础

洪　帆编

华中工学院出版社

离 散 数 学 基 础
洪 帆 编
责任编辑 韩瑞根
*
华中工学院出版社出版
(武 昌 喻 家 山)
湖北省新华书店发行 各地新华书店经售
湖北省咸宁市印刷厂印刷
*
开本：850×1168 1/32 印张：10.5 字数256,000
印数：12,001—43,000
1983年2月第一版 1984年6月第二次印刷
统一书号：13255—010 定价 1.50元

前　言

由于计算机科学的发展和计算机应用领域的日益广泛，迫切需要用一些适当的数学工具来解决计算机科学各个领域中提出的有关离散量的理论问题。离散数学就是适应这种需要而建立的，它综合了计算机科学中所用到的研究离散量的各个数学课题，并进行系统的、全面的论述，从而为研究计算机科学提供了有力的理论基础和工具。学习和研究离散数学对计算机科学的发展必将起着重要的促进作用。

离散数学是理工科高等院校计算机系重要的专业基础课，它不仅为计算机系有关的专业课，如数据结构、编译原理、操作系统，可计算性理论、人工智能、形式语言与自动机、信息管理与检索以及开关理论等，作了必要的数学准备，而且为学生今后从事计算机科学各方面的工作提供重要的工具。此外，通过离散数学的学习，还可进一步培养学生抽象思维和逻辑推理的能力，因而具有较强的独立学习和工作的能力。

离散数学也是研究自动控制、管理科学、电子工程等的重要工具。因此，它越来越受到各有关方面的科学工作者的重视。

离散数学的内容十分丰富，涉及的面也比较广，凡是以离散量作为其研究对象的数学均属于离散数学。在本书中，不打算论及离散数学的所有内容，而着重讨论集合论、代数结构、图论和数理逻辑这四个方面。因为着眼于为计算机和自动控制等各专业的学生、工作者以及有关工程技术人员提供必备的数学工具，所以对它们的讨论不可能象这些数学分支的有关专著那样深入，只能有选择地对一些在计算机科学中所用到的最基本和最重要的概

念及其性质和方法加以叙述，其目的是使初学者对离散数学的基础知识有一个较全面、系统的了解，为今后在实际工作中应用这些知识或进一步学习有关的内容打下一个良好的基础。

本书是笔者根据华中工学院自动控制与计算机系软件专业学生所用的离散数学讲义修改、补充而成的。在修改过程中，曾参考计算机学会教育专业组1981年8月在大连召开的计算机数学课程教学大纲讨论会所拟定的离散数学（单课型）教学大纲。在内容的安排上，力求做到由直观到抽象，由简单到复杂逐步深入；在叙述上，力求做到对基本概念的阐述通俗易懂，并配有各种例题，便于读者理解和掌握；最后，为了使篇幅不至太长，有些内容安排在练习中，希望读者通过正文的学习自己去完成。本书的绝大部分内容曾在华中工学院软件专业的学生中作过多次讲授。

在本书的编写过程中，经常得到武汉大学数学系主任张远达教授的热情指导，张老师仔细审阅了原稿，提出了许多指导性的意见，使笔者受到不少的启发和教益。集合论部分曾参考武汉大学齐民友教授编写的讲义，齐老师并对笔者原来的讲义提出了一些指导性的改进意见。在此，对两位老师表示深切的谢意。华中工学院自控与计算机系的领导对本书的编写工作给予了许多支持和帮助。计算机软件教研室的有关同志为本书的编写提供了有益的参考资料，在对文稿的抄写和校对上给予了帮助。余洪祖老师对最后一章提出了一些宝贵意见，王广泰老师对讲义的初稿提出了一些意见，最后一章曾参考北京大学陈进媛同志的讲义。韩瑞根同志和华中工学院出版社的有关同志为本书的编辑和出版花了很多工夫。在此，一并表示衷心的感谢。

由于编者水平所限，书中定有许多错误和不妥之处，恳切希望读者批评指正。

洪　帆

1983年2月于华中工学院

目　　录

第一章　集　　合

集合的概念是现代数学中最基本的概念之一，并已深入到各种科学和技术的领域中．对于计算机科学工作者来说，集合的概念是不可缺少的．在开关理论、有限自动机、形式语言等领域中，集合论有着广泛的应用．

这一章我们介绍集合及其子集、幂集、分划等基本概念，集合的并、交、补运算以及这些运算的性质；还介绍文氏图和成员表，它们是对集合进行运算和分析的有用工具；最后介绍集合的标准形式．

§1.1　集　　合

集合是数学中的一个最基本的概念，很难再用别的词来定义它．我们通常只是给予一种描述．

把一些确定的、彼此不同的事物作为一个整体来考虑时，这个整体便称为是一个**集合**．这里所谓“事物”也称“个体”，可以是在极其广泛的意义上使用，甚至包括抽象的事物．例如，全体中国人，一本书中的全部概念，一群羊，所有自然数等等，都分别可以构成集合．

集合里所含有的个体叫做集合的**元素**．例如，全体中国人的集合，它的元素就是每一个中国人；一群羊的集合，它的元素就是该羊群中的每一只羊；所有自然数的集合，它的元素就是每一个自然数．

今后我们用大写拉丁字母表示集合，用小写拉丁字母表示元

素。如果 a 是集合 A 的元素，则记作"$a\in A$"，读作"a 属于集合 A"或"a 在集合 A 中"。如果 a 不是集合 A 的元素，则记作"$a\notin A$"，读作"a 不属于集合 A"或"a 不在集合 A 中"。例如，若用 N 表示自然数的集合，则 $2\in N$，$3\in N$，但 $2.3\notin N$，$-5\notin N$。

关于集合的概念，很重要的一点是当我们给出一个"个体"后，应该能够确定它是否是这个集合的元素。例如，"百货商店里好看的花布"就不成为一个集合，因为对每一种布，没有确定的标准说它是"好看"还是"不好看"。"这个班里的高个子学生"也不构成一个集合。因为在"高个子"与"不是高个子"之间没有明确的界限。但是，如果我们给出一个完全确定的标准（如身高 $h\geqslant 1.7$ 米），合乎这个标准的算是"高个子"，否则不算，那么对于这个班里的每一个学生，总可以明确地断定是否合乎这个标准，不会发生两可的情形，这时"这个班里的高个子学生"就构成一个集合。

下面介绍几个常见的集合的表示符号。

$\boldsymbol{N}$：正整数或自然数集合$(1,2,3,\cdots)$。

$\boldsymbol{Z}$：非负整数集合$(0,1,2,3,\cdots)$。

$\boldsymbol{I}$：整数集合$(0,-1,1,-2,2,\cdots)$。

$\boldsymbol{P}$：素数集合（只能被 1 和它本身整除，不能被其他正整数整除的大于 1 的正整数称作素数）。

$\boldsymbol{Q}$：有理数集合（有理数是可以表示成 i/j 形式的数，这里 i 和 j 都是整数，且 $j\neq 0$）。

$\boldsymbol{R}$：实数集合（包括全部有理数和无理数）。

$\boldsymbol{C}$：复数集合（包括所有形如 $a+ib$ 的数，其中 a、b 是实数，$i=\sqrt{-1}$）。

$\boldsymbol{N}_m(m\geqslant 1)$：介于 1 和 m 之间的正整数集合，计入 1 和 m $(1,2,\cdots,m)$。

$\boldsymbol{Z}_m(m\geqslant 1)$：介于 0 和 $m-1$ 之间的非负整数集合，计入 0 和

$m-1(0,1,2,\cdots,m-1)$。

对于集合，有下面两种常用的表示方法。

把集合的元素按任意顺序逐一写在一个花括弧里，并用逗号分开，这称为**列举法**。例如，设 $a_1, a_2, \cdots, a_n$ 是集合 A 的元素，此外 A 无其它元素，则集合 A 可表示为 $A=\{a_1, a_2, \cdots, a_n\}$。又如，绝对值不超过 3 的所有整数的集合，可记作 $S=\{-3, -2, -1, 0, 1, 2, 3\}$。列举法必须把元素的全体尽列出来，而不能遗漏任何一个，因此，如果一个集合含有许多元素时，用列举法是极其麻烦的。当集合含有无穷多个元素时，列举法更是无能为力。但对这种情形，有时也可列举出集合的一部分元素，而略掉的元素应能由列举出的元素以及它们前后的关系所确定，使得人们一看就明白。例如，$N=\{1,2,3,\cdots\}$，$I=\{\cdots-2,-1,0,1,2\cdots\}$。但这种写法有时是很困难的，可采用另一种表示方法。

集合的另一种表示法称为**描述法**，它是利用详细说明元素 $a\in A$ 的定义条件作出来的。即给定一个条件 $P(x)$，当且仅当 a 使条件 $P(a)$ 成立时，$a\in A$。其一般形式为 $A=\{a|P(a)\}$，读成“A 是使 $P(a)$ 成立的所有元素 a 的集合”。实际上，$P(a)$ 描述了一个规则或公式，它使得我们有可能确定 a 是否在 A 中。例如，绝对值不超过 3 的所有整数的集合用描述法可表示为 $S=\{a|a\in I$ 且 $-3\leqslant a\leqslant 3\}$。又如，$B=\{a|a$ 是中国的省$\}$。

用描述法来表示一个集合，其方式并不是唯一的，因为对一个集合的元素往往可以用多种不同的方式来确定。例如，集合 $\{1,2,3,4\}$ 的元素可定义为不大于 4 的自然数，也可定义为小于 6 而能整除12的自然数；因此集合 $\{1,2,3,4\}$ 可表示为 $\{a|a\in N, a\leqslant 4\}$，也可表示为 $\{a|a\in N, a<6, a|12\}$。

关于集合的概念，还有一点需要提起注意的是，对作为集合的元素的个体，并没有给它们施加什么限制。常常有一些集合其元素本身也是集合。例如，$A=\{5,\{1,2\},d,\{q\}\}$，$B=\{\{1\},\{2,3\},$

$\{1,3\}\}$. 对于这种情形，重要的是把集合 $\{a\}$ 与元素 a 区别开来。例如集合 $\{q\}$ 是集合 A 的元素，$\{q\}\in A$，而 q 是集合 $\{q\}$ 的元素，$q\in\{q\}$，但 q 不是 A 的元素，即 $q\notin A$。

然而，对“包罗一切的集合”或“由一切集合组成的集合”等类似的术语，我们必须避免使用，因为它们会导致集合论中的**悖论**。例如，我们来看著名的罗素悖论。

我们把不包含自身作为元素的集合称为寻常集，而把包含自身作为元素的集合称为不寻常集。于是可知，一个集合或者是寻常集，或者不是寻常集，二者必居其一，且只居其一。今设 T 是由所有寻常集组成的集合，即

$$T=\{A\,|\,A\text{是集合},\ A\notin A\}.$$

现在我们考虑，T 是寻常集还是不寻常集？若 T 是寻常集，则由 T 的定义，T 必包含自身为元素，因此 T 是不寻常集。这与假设矛盾。故 T 不是寻常集，即 T 是不寻常集。然而由不寻常集的定义，就必须有 $T\in T$，因此 T 包含一个不寻常集为元素，这又与 T 的定义矛盾。这就是说，由于假定 T 的存在，无论 T 是寻常集或不寻常集都将引出矛盾。

又如，研究下述情况：某理发师跟且只跟城里所有不能给自己理发的人理发。定义 A 为城里所有由该理发师理发的人的集合，稍加考虑就会明白，A 一定是这样的集合，该理发师 $\in A$，而又有该理发师 $\notin A$。显然这是一个矛盾。因此集合 A 不存在。

定义 1-1 不含有任何元素的集合，称为**空集**，记作 ϕ。

空集看起来很不自然，但却是一个有用的概念。例如，我们说“两条平行线的交点之集是一个空集”即是说“两条平行线没有交点”。又如 $\{x\,|\,x\in I, x^2=8\}=\phi$，即意味着方程 $x^2=8$ 没有整数根。一般说来，如果我们想要证明命题 $P(x)$ 对于一切 x 均不真，则只要证明 $\{x\,|\,P(x)\}=\phi$ 即可。

集合 A 中不同元素的数目，称为集合 A 的**基数**，用 $\#A$ 表示。

当集合A具有有限数目的不同元素，亦即$\#A$为有限时，称A为**有限集**，否则称A为**无限集**。前述的集合N, Z, I, P, Q, R和C都是无限集；集合N_m和Z_m是有限集，因为$\#N_m=\#Z_m=m$。集合的基数后面还要较详细地讨论。

§1.2 集合的包含和相等

集合的包含和相等是集合间的两个基本关系。

定义1.2 设有集合A、B，如果A的每一个元素都是B的元素（即若$a\in A$，必有$a\in B$），则称A是B的**子集**，或说A被包含于B中（或B包含A），记作$A\subseteq B$或$B\supseteq A$。反之，若A不是B的子集，则记作$A\nsubseteq B$或$B\nsupseteq A$。

例1 设$A=\{a,c,d,e\}$，$B=\{a,b,c,x,y\}$，$C=\{a,b\}$，则有$C\subseteq B$，但$C\nsubseteq A$。

注意区别从属关系和包含关系。从属关系$a\in A$是指集合A的元素a与集合A的关系，而包含关系$C\subseteq A$是指集合A与另一个集合C之间的关系。

例2 设$A=\{a,b,c,d\}$，则有$a\in A$，而$\{a\}\subseteq A$。

由从属关系和包含关系的定义可知，并不排斥同时有$A\in B$和$A\subseteq B$的可能性。

例3 设$A=\{a,b,c\}$，$B=\{\{a,b,c\},a,b,c\}$，则显然有$A\in B$同时$A\subseteq B$。

关于集合的包含有如下重要性质：

(1) 对于任意的集合A，有$\phi\subseteq A$；

(2) 对于任意的集合A，有$A\subseteq A$；

(3) 对于任意的集合A、B、C，

若$A\subseteq B$，$B\subseteq C$，则有$A\subseteq C$。

性质(2)和(3)的成立是明显的。我们仅证明性质(1)，用

反证法，设空集ϕ不是某集合A的子集，即$\phi\nsubseteq A$，则必存在元素$x\in\phi$而$x\notin A$，这与空集的定义矛盾，因此，$\phi\subseteq A$。

定义 1-3 设有集合A、B，如果A的每一个元素都是B的元素，B的每一个元素也都是A的元素，则集合A和B称为是**相等**，记作$A=B$。

显然，所谓集合A与集合B相等，即意味着A与B具有完全相同的元素。

由定义1-2和定义1-3可知，当且仅当$A\subseteq B$且$B\subseteq A$时，有$A=B$.

定义 1-3 的实质是一个集合由它的全部元素所确定。

下面给出一些相等集合和不等集合的例子。

例4 $\{1,2,4\}=\{1,2,2,4\}$，

这就是说，在集合的第一种表示法中，某个元素的符号重复出现，不会改变这个集合。然而为了叙述的方便，今后我们不使用这种表示方法，要求列举的元素各不相同。

例5 $\{1,4,2\}=\{1,2,4\}$，

这说明在集合的第一种表示法中，若将元素的次序任意改变，集合不变.

例6 设$P=\{\{1,2\},4\}$，$Q=\{1,2,4\}$，则$P\neq Q$。

又$\{\{1\}\}\neq\{1\}$。

如果$A=\{x|x(x-1)=0\}$，$B=\{0,1\}$，则$A=B$。

定义 1-4 设有集合A、B，若$A\subseteq B$，且$A\neq B$，则称集合A是集合B的**真子集**，用$A\subset B$表示。

例如，集合$\{1,2,3\}$是集合$\{x|x\in I,-3\leqslant x\leqslant 3\}$的真子集。

因为空集是每个集合的子集，所以导出如下定理。

定理 1-1 空集合是唯一的。

证明 假设有两个空集合ϕ_1和ϕ_2，因为空集被包含于每一个集合中，因此有$\phi_1\subseteq\phi_2$，$\phi_2\subseteq\phi_1$，这意味着$\phi_1=\phi_2$。证完。

§1.3 幂　　集

任给一集合A，我们知道空集和集合A都是A的子集。对任何元素$a\in A$，集合$\{a\}$也是A的子集。类似地，我们还可以举出A的其它子集。下面我们来讨论关于集合A的全部子集的集合。

定义 1-5　设有集合A，由A的所有子集组成的集合，称为集合A的**幂集**，记作2^A，即

$$2^A=\{S|S\subseteq A\}.$$

例如，设$A=\{a\}$，则$2^A=\{\phi,\{a\}\}$；

$B=\{a,b\}$，则$2^B=\{\phi,\{a\},\{b\},\{a,b\}\}$；

$C=\{a,b,c\}$，则

$$2^C=\{\phi,\{a\},\{b\},\{c\},\{a,b\},\{a,c\},\{b,c\},\{a,b,c\}\}.$$

空集ϕ的幂集，仅含有元素ϕ，即$2^\phi=\{\phi\}$。

从上述例子可看出，当集合的基数增加时，集合的幂集的基数也随之增加。对于有限集下面的定理给出两者之间的关系。

定理 1-2　设A是具有基数$\#A$的有限集，则$\#(2^A)=2^{\#A}$。

证明　设$\#A=n$，从n个元素中选取i个不同元素的方法共有C_n^i种，这里

$$C_n^i=\frac{n!}{i!(n-i)!}.$$

所以A的不同子集的数目（包括ϕ）为

$$\#(2^A)=C_n^0+C_n^1+C_n^2+\cdots+C_n^n.$$

由二项式定理可知：

$$(x+y)^n=C_n^0x^n+C_n^1x^{n-1}y+C_n^2x^{n-2}y^2+\cdots+C_n^ny^n.$$

令$x=y=1$，便有

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

所以$\#(2^A)=2^n$。因为$\#A=n$，故有$\#(2^A)=2^{\#A}$。证完。

当集合A的元素个数较多时，要毫无遗漏地列出集合A的所有子集是一件相当困难的事情。现在我们引进一种表示法，按照这种表示法，我们能够毫无遗漏地列出一个有限集合的每一个子集。为此，我们对所给集合的元素规定某种次序，使得某个元素可以称为第一个元素，另一个元素为第二个元素，等等（虽然在集合的定义中，并没有这样一种次序），即给每一元素附加一个标号，以便描述这个元素相对于该集合其它元素的位置。例如，在集合$A=\{a,b,c\}$中，我们可以令a是第一个元素，b是第二个元素，c是第三个元素。在A的子集中，常常是有一些元素出现，而其余的元素不出现。我们根据这一情况以及指定给集合中各元素的次序，就用以下方式来表示所有的子集，例如A的各个子集可以表示为

$$B_{000}=\phi,\ B_{001}=\{c\},\ B_{010}=\{b\},\ B_{011}=\{b,c\},\ B_{100}=\{a\},$$
$$B_{101}=\{a,c\},\ B_{110}=\{a,b\},\ B_{111}=\{a,b,c\}.$$

因此 $$2^A=\{B_{000},B_{001},B_{010},B_{011},\cdots,B_{110},B_{111}\}.$$

其中，B的下标是一个三位的二进制数，每一位对应集合A中的一个元素，左边第一位是1还是0表示第一个元素a在子集中出现与否。类似地，第二位和第三位是1还是0分别表示第二个元素b和第三个元素c在子集中出现与否。于是，A的任一子集都可用000—111中的某一下标来表示，反之，若给出这8个（即2^3个）下标中的任何一个，就能够确定出相应的子集。

假设集合$J=\{j|j$是二进制数，$000\leqslant j\leqslant 111\}$，则有

$$2^A=\{B_j|j\in J\}.$$

可以看到，我们只用了下标来确定子集的各元素，而表示这些子集时用到的字母B则是无关紧要的。

上述表示法，可以推广到一般情形，用来表示具有任意n个不同元素的集合的各个子集。用来表示这些子集的下标是十进制数0到2^n-1的二进制表示。为了凑足n个数位，一定要在这些二

进制数的左边插入所需个数的零。我们也可以使用从0到2^n-1的十进制数来作为子集的下标，而只在要确定所对应子集的元素时才转换为二进制数。例如，令$A_6=\{a_1,a_2,\cdots,a_6\}$，显然$A_6$有$2^6=64$个子集，我们可称它们为$B_0,B_1,\cdots,B_{2^6-1}$。下面我们看如何确定$A_6$的任何子集的各元素。

例 $B_7=B_{000111}=\{a_4,a_5,a_6\}$；

$B_{12}=B_{001100}=\{a_3,a_4\}$。

类似于集合的幂集，即所有元素都是集合的这种集合，我们今后还会经常遇到。我们称这种集合为**集合族**。例如，其和为6的不同正整数的集合的集合。

$$\{\{6\},\{1,5\},\{2,4\},\{1,2,3\}\}$$

就是一个集合族。

我们常用记号$\{A_i\}_{i\in K}$来表示所有集合$A_i(i\in K)$所构成的集合族，即

$$\{A_i\}_{i\in K}=\{A_i|i\in K\},$$

这里K是指标集。例如，集合族$\{A_0,A_1,A_2,A_3,A_4\}$可表示为$\{A_i\}_{i\in K}$，这里$K=\{0,1,2,3,4\}$。当$K=\{i|i\in I,\ i_a\leqslant i\leqslant i_b\}$时，又可将集合族$\{A_i\}_{i\in K}$表示为$\{A_i\}_{i=i_a}^{i_b}$。例如上一集合族又可表示为$\{A_i\}_{i=0}^{4}$。

§1.4 集合的运算

我们再引进一个特殊的集合，它包含讨论中的每一个集合。

定义 1-6 如果一个集合包含了某个问题中所讨论的一切集合，则称它为该问题的全域集合，或简称为**全集合**，记作U。

全集合U并非是唯一的，然而一般总是取一个较为方便取用的集合为U。例如，若我们是在实数范围内讨论问题，则可将实数集R取作全集合U；若在正整数范围内讨论问题，则可将正整