高等学校试用教材

离散数学导论

徐洁磐 编

高等教育出版社

高等学校试用教材

离散数学导论

徐洁磐　编

高等教育出版社

内 容 提 要

本书比较系统地介绍了离散数学领域中各分支的基本内容，它主要有：集合论、关系、图论、代数结构、数理逻辑、有限自动机及图灵机等．它可作为高等院校计算机有关专业“离散数学”课程的教材或参考书，也可供从事计算机工作的科研人员、工程技术人员以及其他有关人员参考。

本书原由人民教育出版社出版。1983 年 3 月 9 日，上级同意恢复“高等教育出版社”；本书今后改用高等教育出版社名义继续印行。

高等学校试用教材

离散数学导论

徐洁磐　编

*

高等教育出版社出版

新华书店北京发行所发行

河北省〇五印刷厂印装

*

开本 850×1168 1/32　印张 11　字数 260,000

1982 年 5 月第 1 版　1984年 7 月第 3 次印刷

印数 28,001—36,200

书号13010·0742　　定价 1.05 元

序

离散数学导论一书是作者近年来在南京大学计算机科学系讲授此课程的讲义的基础上整理而成的. 它可以作为理工科院校计算机有关专业学生的教材，也可作为从事计算机工作的有关人员的参考书.

本书内容比较广泛，它不仅包括目前一般离散数学的基本内容，如：集合论、图论、关系与映射，代数系统及数理逻辑等，它还包括目前应用得比较广泛的一些内容，如有限自动机理论、图灵机器等.

作者力图将离散数学中的各部分内容能有机的联系起来，同时也尽量充分地将各部分内容的特色表达清楚.

由于离散数学是一门数学，因此作者力求叙述严格，证明与推导逻辑性强、思路清楚，使学生通过此课程学习后能得到严格的逻辑推理与抽象思维能力的训练. 但是，考虑到此课程是为计算机有关专业学生而开设的，因此在编写过程中作者力求做到能密切结合计算机的实际，能将理论与实际紧密地结合起来，使读者能知道如何利用离散数学的理论去解决计算机中的实际问题.

作者在编写过程中尽量做到内容深入浅出，文字浅显易懂，因此，本书非常适合于读者自学.

一般讲，只要具有初等数学知识的人即可看懂此书. 但是，希望读者能具有一定的逻辑思维能力，这样，可以较为容易地掌握本书的实质.

在编写过程中曾得到惠永涛、汪承藻两位老师的协助，在此表示感谢。

作　　者

1982.4.南京

目　录

第一章 绪 言

1 计算机科学与离散数学

由于计算技术的日益发展、计算机应用的日益拓广、计算机软件的日益丰富、计算机理论研究的日趋完善，从而产生了计算机科学．在计算机科学的研究中需要借助于一些工具与方法，而离散数学正是研究计算机科学之有力工具．

离散数学作为有力的数学工具，对计算机的发展、计算机科学的研究起着重大的作用．远在计算机产生之前，图灵(Turing)在研究可计算性问题时建立了著名的图灵机．图灵机的基本结构思想为1946年计算机的问世在理论上奠定了基础．在计算机发展的初期，利用布尔代数理论研究开关电路从而建立了一门完整的数字逻辑理论，对计算机的逻辑设计起了很大的作用．在近期，利用自动机理论研究形式语言；利用谓词演算研究程序正确性问题；利用代数结构研究编码理论；利用能行性理论研究计算机中的可计算性问题等等．目前，离散数学在计算机研究中的作用越来越大．计算机科学中普遍地采用离散数学中的一些基本概念、基本思想、基本方法，使得计算机科学越趋完善与成熟．

所有这些，使得离散数学成为了解和学习计算机科学、掌握和研究计算机科学之必需的理论工具．在现代计算机科学中，如果不了解离散数学的基本内容则已经到了寸步难行的地步．

2 离散数学之特征

离散数学是数学中的一个分支，它以离散量作为其研究之主

要对象，如自然数、真假值、字母表等．这使它与数学中的数学分析在研究对象上形成了鲜明的差别．数学分析是以连续量作为其研究对象的．由于这两种数学在研究对象上的本质区别，使数学分成为连续数学与离散数学两大类．

在离散数学中非常重视“能行性”问题的研究．要解决一个问题，首先要证明此问题解的存在性．但是，光解决存在性问题是不够的，还需要找出得到此问题解的步骤来，而且其步骤必须是有限的、有规则的．这就是所谓“能行性”问题的研究．

离散数学之上述特性使得它成为研究计算机科学之基本数学工具．由于计算机(不管是硬件还是软件)是一个离散的结构，故计算机科学的研究对象大都呈离散形式．在计算机中任何一个问题(不管是硬件还是软件)不仅需要解的存在性，而且更需要解的能行性．因此，离散数学成了研究计算机科学之最合适的工具．

3 离散数学的内容

由于离散数学是以离散量作为其研究对象，故一切以离散现象作为其研究对象或作为其研究对象之一的数学均可属于离散数学．它们可以是：代数结构、数理逻辑、图论、自动机理论、递归函数等等．它还包括诸如组合数学、数论、离散概率等方面．

离散数学各分支间虽然其研究对象一致，但其研究方法各异、研究的侧重点也有所不同，故各具特色，它们互相补充、互相促进、互相渗透，逐渐形成了一门具有一定共性之学科．

第二章　集合论

集合的概念是一般数学及离散数学中的基本概念，亦是计算机科学中经常应用的基本概念．集合论还能直接应用到计算机科学的各个部分中去，如程序语言中、数据结构的研究中等等。

§1　集合论基础

1.1　关于集合的概念

由于集合的概念是数学中之基本概念，故无法对集合确定一个确切的定义，正象在几何中无法定义点、直线一样．由此，我们只能对它进行一些说明.

我们说一些不同的确定的对象的全体称为集合．而这些对象称为集合的元素．由此可见，集合是由元素组成．元素与集合一样，也是无法定义的，它可以理解为存在于世上的客观物体，当然啰，这些物体可以是具体的也可以是抽象的，如人、书、桌子、花、太阳、地球、原子、自然数、实数、字母、点、三角形等等.

对于集合我们可以举一些例子：

地球上全体人类构成一个集合，而每个人则是此集合之元素.

一计算机之内存全体单元构成一个集合，而其每个单元为此集合之元素.

全体自然数构成一个集合，而每个自然数是这个集合的元素.

我们一般用带标号或不带标号之大写字母表示集合，如 A, M, X_1、B_i 等．我们一般用带标号或不带标号之小写字母表示集合的元素，如 a_1, b_2, x, y 等．为了表示一个集合由哪些元素组成，

我们一般将集合的元素全部列出(元素间以逗点隔开)并左右用花括号括起,以表示由这些元素组成之集合. 例如集合 A 由元素 a、b、c、d 组成则可写成

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

对于集合必须注意几点:

(1) 集合中的元素是确定的,也就是说,对集合 A,任一元素 a 或属于此集合或不属于此集合, 两者必居其一. 若一元素 a 属于集合 A,则用 $a\in A$ 表之,若不属于 A,则用 $a\notin A$ 表之.

(2) 集合中之每个元素均不相同, 亦即集合 $\{a, b, b, c, d\}$ 与 $\{a, b, c, d\}$ 是一样的.

除此之外,我们对集合不作任何其他限制,使它具有最广泛之含义.

对集合的元素我们也不作任何限制, 它具有一切我们能找得到的客观事物. 甚至某一集合可以作为另一集合之元素, 如 $A=\{1, 2, \{a, b\}\}$,其中集合 $\{a, b\}$ 是集合 A 之元素.

对于应由哪些元素构成一集合,从理论上讲也不作任何限制. 当然,在实际应用时,它往往具有明确的范围. 即是说, 一集合之元素往往具有一共同之性质.

对于集合元素之个数我们也不作任何限制, 它可是有限个也可是无限个. 一集合如由有限个元素组成,则叫有限集;一集合如由无限个元素组成,则叫无限集. 如自然数集即为无限集,地球上人的集合即是有限集. 特别,对元素个数为零的集合叫做空集,记以 ϕ. 如"缺席今天会议的人"构成集合 A, 则今天全体出席会议表示 $A=\phi$.

与空集相对应的是全集,一个集合,如果它能包括我们所考虑的目标之内的所有元素,则此集合叫做全集,记以 E. 如我们讨论存贮器, 则存贮器之全体存贮单元构成一个全集 E. 如我们讨论

人的问题时则全体人类构成一个全集 E.

集合的表示法前面已经提到，即集合 A 由元素 a, b, c, d 组成可写为 $A=\{a, b, c, d\}$. 这种表示法叫“枚举法”，也就是将集合所有元素一一列出，但有时也可只列出一部分元素，而其余部分可从前后关系中很明显的知道，如

$$A=\{1, 2, 3, 4, \cdots\}$$

表示全体自然数集合. 又如

$$A=\{1, 2, 3, \cdots, 100\}$$

表示从 1 到 100 之 100 个自然数所构成之集合.

集合尚可用另一种方法表示之，这个方法是用一集合之元素所具有之共同性质来刻划这个集合. 如正偶数组成之集合 A 可写成

$$A=\{x \mid x \text{ 是正偶数}\}$$

对一般集合可用下面方式表之

$$A=\{x \mid P(x)\}$$

其中 P 表示某性质，这个集合 A 表示由满足性质 P 的元素 x 所组成.

1.2 集合间的关系

集合间一般可有两种关系：相等关系与包含关系.

定义 1 如果集合 A 与集合 B 有相同之元素，则称这两个集合是相等的，记以 $A=B$，否则称这两个集合不相等，记以 $A \neq B$.

定义 2 集合 A、B，如果当 $a \in A$ 必有 $a \in B$，则称 B 包含 A，或称 A 是 B 的子集，记以 $B \supseteq A$ 或 $A \subseteq B$. 如果 $B \supseteq A$ 且存在 b，使得 $b \in B$ 但 $b \notin A$ 则称 A 是 B 的真子集，记以 $B \supset A$ 或 $A \subset B$. 若集合 A, B 间不满足 $A \subseteq B$ 则称 B 不包含 A，记以 $A \nsubseteq B$.

对于集合的相等与包含关系，可用一种图——叫文氏图 (Venn Diagram) 表示之.

文氏图在表示集合中的关系时较为直观、形象，故目前被广泛应用于集合论中．在文氏图中用一个平面中的区域表示一个全集，而对包含于全集内之集合用平面区域内之圆表示之．这样，全集内之集合间关系就可用平面区域内圆之间的关系表示之．对于相等、包含等关系可以很形象地用文氏图表示(见图 1)．

图 1　相等与包含关系之文氏图

例 1：设 $N=\{0,1,2,\cdots\}$，$A=\{1,2,3,\cdots,100\}$则我们有 $A\subseteq N$，并且有 $A\subset N$．

例 2：设 $A=\{1,2,3,3\}$，$B=\{1,2,3\}$则我们有 $A=B$．

例 3　设 $A=\{i\mid i$ 为正整数$\}B=\{j\mid j$ 为正偶数$\}$则有 $B\subseteq A$，且 $B\subset A$．

对于相等与包含关系我们有下面的一些定理：

定理 1　对任一集合 A，必有 $\phi\subseteq A$．

[**证**]　假设 $\phi\subsetneq A$，则必至少存在一个 x，有$x\in\phi$ 但 $x\notin A$，但是 ϕ 中无元素，故 $x\notin\phi$．由此与假设矛盾，从而得证．

定理 2　对任一集合 A，必有 $E\supseteq A$．

此定理证明较为简单故从略．

由上面两个定理我们可以得到

定理 3　对任一集合 A，必有 $\phi\subseteq A\subseteq E$．

定理 4　有集合 A 与 B，则 $A=B$ 之充分必要条件是 $A\supseteq B$ 且 $B\supseteq A$．

[证] 充分性: 设 $A\supseteq B$ 且 $B\supseteq A$, 且假设 $A\neq B$, 则根据定义必至少存在一个元素属于一集合而不属于另一集合, 令此元素为 x, 且令 $x\in A, x\notin B$, 但根据 $A\subseteq B$ 之定义, $x\in A$ 则必有 $x\in B$. 由此产生矛盾, 从而得证. 用类似方法对于 $x\in B$ 且 $x\notin A$ 亦可得到矛盾. 由此定理充分性得证.

必要性: 设 $A=B$, 且假设 $A\supseteq B$, $A\subseteq B$ 中至少有一个不保持, 设 $A\subseteq B$ 不保持, 此表示必至少存在一个 $x\in A$ 但 $x\notin B$, 但这与 $A=B$ 矛盾. 类似的对 $A\supseteq B$ 不保持也得到与 $A=B$ 矛盾, 由此定理必要性得证.

这个定理建立了集合之相等与包含间的关系.

1.3 集合代数

在这里我们用代数的方法讨论集合. 即建立一些集合的运算以及这些运算间的基本关系式.

首先我们建立一些集合的运算:

定义 3 由集合 A、B 之所有元素合并组成之集合, 叫集合 A 与 B 的并集, 记以 $A\cup B$.

例 4: $A=\{1,2,3,4\}, B=\{3,4,5,6\}$则

$$A\cup B=\{1,2,3,4,5,6\}$$

定义 4 由集合 A、B 所有的公共元素所组成之集合叫集合 A 与 B 的交集, 记以 $A\cap B$.

例 5: $A=\{1,3,5,7,9\}, B=\{1,3,8,10\}$则

$$A\cap B=\{1,3\}$$

定义 5 集合 A、B 若满足: $A\cap B=\phi$ 则称 A 与 B 是分离的.

定义 6 由集合 A、B 中所有属于集合 A 而不属于集合 B 之元素所组成的集合叫集合 A 对集合 B 的差集, 记以 $A-B$.

例 6: $A=\{a,b,c,d,e,f\}, B=\{d,e,f,g,h\}$则

$$A-B=\{a,b,c\}$$

由差集可直接定义补集.

定义7 集合 A 之补集 $\sim A$ 可定义为

$$\sim A = E - A$$

例 7: 设 $E=\{0, 1, 2, 3, \cdots\}$, $A=\{0, 2, 4, 6, \cdots\}$ 则

$$\sim A = E - A = \{1, 3, 5, 7, \cdots\}$$

我们还可以由差集定义对称差:

定义8 集合 A、B 之对称差(或叫布尔和) $A+B$ 可定义为

$$A+B=(A-B)\cup(B-A)$$

例 8: 设 $A=\{1, 2, 3, 4\}$, $B=\{3, 4, 5, 6\}$ 则

$$A+B=\{1, 2, 5, 6\}$$

由例中可以看出 $A+B$ 即为 A、B 之所有的非公共元素所组成之集合.

到此为止, 我们定义了四个二元运算即并运算、交运算、差运算及对称差运算, 以及一个一元运算: 补运算. 这五个运算可用文氏图表示, 如图 2.

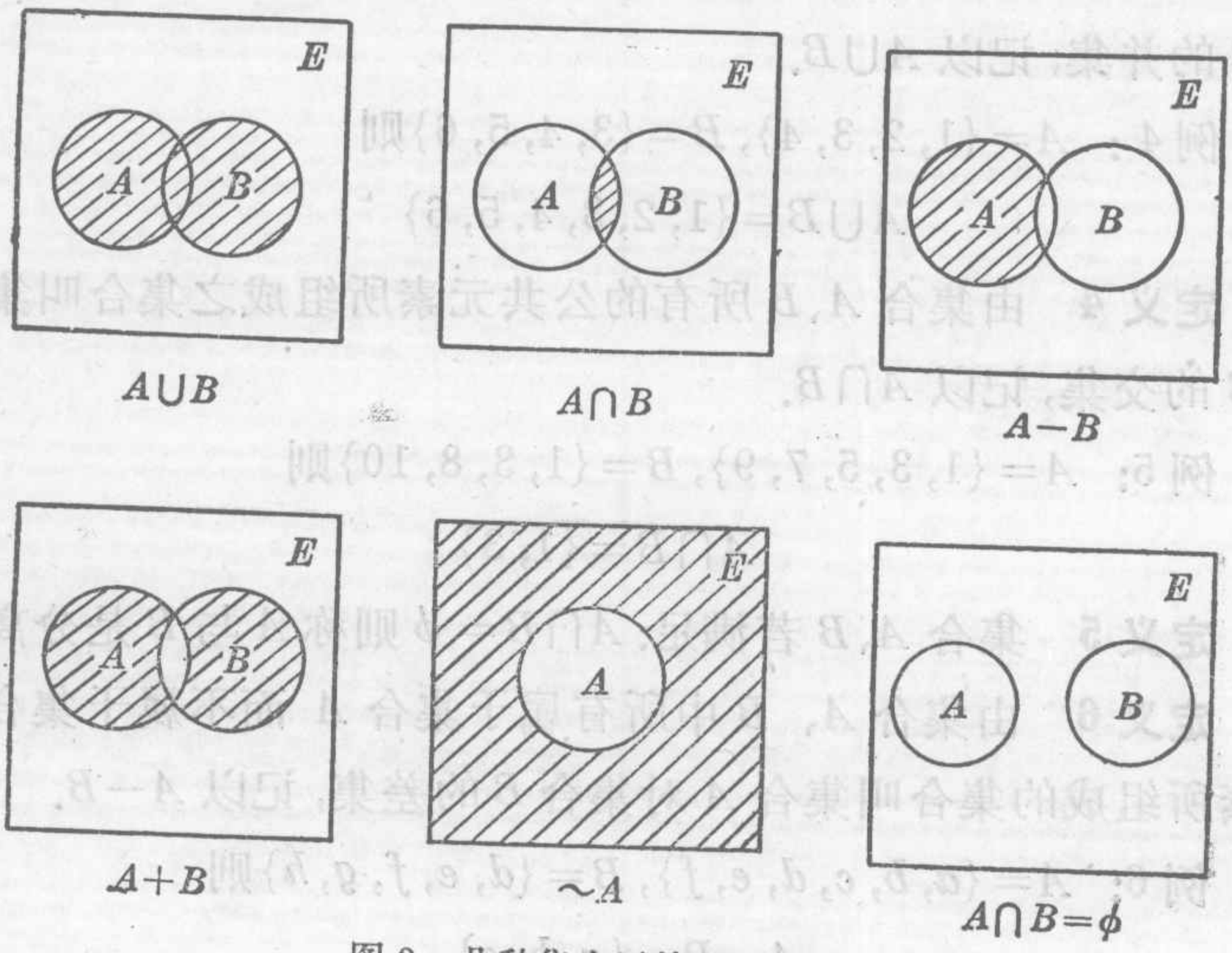

图 2 几种集合运算的文氏图

在这五种运算中，我们下面着重讨论并、交、补三种运算之基本公式.

由定义，我们可知并、交运算满足交换律，即：

$$A \cup B = B \cup A \tag{2-1}$$

$$A \cap B = B \cap A \tag{2-2}$$

由定义，我们可知并、交运算满足结合律，即：

$$A \cup (B \cup C) = (A \cup B) \cup C \tag{2-3}$$

$$A \cap (B \cap C) = (A \cap B) \cap C \tag{2-4}$$

由定义还可知，并、交运算还满足分配律，即：

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \tag{2-5}$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \tag{2-6}$$

由定义我们还可以得到有关空集、全集及补集的几个公式：

$$A \cup \phi = A \tag{2-7}$$

$$A \cap E = A \tag{2-8}$$

$$A \cup \sim A = E \tag{2-9}$$

$$A \cap \sim A = \phi \tag{2-10}$$

我们可以证明：

$$A \cup E = E \tag{2-11}$$

$$A \cap \phi = \phi \tag{2-12}$$

对(2-11)我们有

$$\begin{aligned} A \cup E &= (A \cup E) \cap E && \text{由(2-8)} \\ &= E \cap (A \cup E) && \text{由(2-2)} \\ &= (A \cup \sim A) \cap (A \cup E) && \text{由(2-9)} \\ &= A \cup (\sim A \cap E) && \text{由(2-5)} \\ &= A \cup \sim A && \text{由(2-8)} \\ &= E && \text{由(2-9)} \end{aligned}$$

对(2-12)我们有

$$A\cap\phi=(A\cap\phi)\cup\phi \qquad \text{由(2-7)}$$
$$=\phi\cup(A\cap\phi) \qquad \text{由(2-1)}$$
$$=(A\cap\sim A)\cup(A\cap\phi) \qquad \text{由(2-10)}$$
$$=A\cap(\sim A\cup\phi) \qquad \text{由(2-6)}$$
$$=A\cap\sim A \qquad \text{由(2-7)}$$
$$=\phi \qquad \text{由(2-10)}$$

我们还可以证明等幂律:

$$A\cup A=A \qquad (2\text{-}13)$$
$$A\cap A=A \qquad (2\text{-}14)$$

对于(2-13)我们有

$$A=A\cup\phi \qquad \text{由(2-7)}$$
$$=A\cup(A\cap\sim A) \qquad \text{由(2-10)}$$
$$=(A\cup A)\cap(A\cup\sim A) \qquad \text{由(2-5)}$$
$$=(A\cup A)\cap E \qquad \text{由(2-9)}$$
$$=A\cup A \qquad \text{由(2-8)}$$

对于(2-14)我们有

$$A=A\cap E \qquad \text{由(2-8)}$$
$$=A\cap(A\cup\sim A) \qquad \text{由(2-9)}$$
$$=(A\cap A)\cup(A\cap\sim A) \qquad \text{由(2-6)}$$
$$=(A\cap A)\cup\phi \qquad \text{由(2-10)}$$
$$=A\cap A \qquad \text{由(2-7)}$$

此外还有两个吸收律:

$$A\cup(A\cap B)=A \qquad (2\text{-}15)$$
$$A\cap(A\cup B)=A \qquad (2\text{-}16)$$

对于(2-15)我们有

$$A\cup(A\cap B)=(A\cap E)\cup(A\cap B) \qquad \text{由(2-8)}$$
$$=A\cap(E\cup B) \qquad \text{由(2-6)}$$

$$= A \cap E \qquad \text{由(2-11)}$$

$$= A \qquad \text{由(2-8)}$$

类似地，对于(2-16)我们有

$$A \cap (A \cup B) = (A \cup \phi) \cap (A \cup B) \qquad \text{由(2-7)}$$

$$= A \cup (\phi \cap B) \qquad \text{由(2-5)}$$

$$= A \cup \phi \qquad \text{由(2-12)}$$

$$= A \qquad \text{由(2-7)}$$

我们可以证明，只有ϕ及E才能分别满足(2-7)及(2-8)(此叫做ϕ及E之唯一性)，即

假设除ϕ外尚有X满足(2-7)，则此时我们有$A \cup \phi = A$及$A \cup X = A$

将X及ϕ分别代入上面第一式、第二式之A内得到

$$X \cup \phi = X$$

$$\phi \cup X = \phi$$

由(2-1)可得

$$\phi = \phi \cup X = X \cup \phi = X$$

由此得到$\phi = X$.

用类似的方法可证得只有E满足(2-8).

我们还可以证明，只有$\sim A$才能同时满足(2-9)及(2-10)(此叫做$\sim A$之唯一性)，即：

假设除$\sim A$外尚有A^*满足(2-9)及(2-10)，则有

$$A^* = A^* \cup \phi \qquad \text{由(2-7)}$$

$$= A^* \cup (A \cap \sim A) \qquad \text{由(2-10)}$$

$$= (A^* \cup A) \cap (A^* \cup \sim A) \qquad \text{由(2-5)}$$

$$= (A \cup A^*) \cap (A^* \cup \sim A) \qquad \text{由(2-1)}$$

$$= E \cap (A^* \cup \sim A) \qquad \text{由假设 } A^* \text{ 满足(2-9)}$$

$$= (A^* \cup \sim A) \cap E \qquad \text{由(2-2)}$$