高等院校计算机专业及专业基础课系列教材

离散数学教程

耿素云　屈婉玲　王捍贫　编著

北京大学出版社
北　京

内 容 简 介

本书共分五编。第一编为集合论，其中包括集合的基本概念、二元关系、函数、自然数、基数、序数。第二编为图论，其中包括图的基本概念、图的连通性、欧拉图与哈密顿图、树、平面图、图的着色、图的矩阵表示、覆盖集、独立集、匹配、带权图及其应用。第三编为代数结构，其中包括代数系统的基本概念、几个重要的代数系统：半群、群、环、域、格与布尔代数。第四编为组合数学，其中包括组合存在性、组合计数、组合设计与编码以及组合最优化。第五编为数理逻辑，其中包括命题逻辑、一阶谓词逻辑、Herbrand 定理和直觉逻辑。

本书体系严谨、内容丰富、配有大量的例题和习题，并与计算机科学的理论与实践密切结合。

本书不仅适用于计算机及相关专业的本科生或研究生，也可供计算机专业的科技人员使用或参考。

图书在版编目(CIP)数据

离散数学教程/耿素云，屈婉玲，王捍贫编著. —北京：北京大学出版社，2002.6
高等院校计算机专业及专业基础课系列教材
ISBN 7-301-05366-5

Ⅰ. 离… Ⅱ. ① 耿… ② 屈… ③ 王… Ⅲ. 离散数学—高等学校—教材 Ⅳ. 0158

中国版本图书馆 CIP 数据核字(2001)第 087009 号

书　　名：离散数学教程
著作责任者：耿素云　屈婉玲　王捍贫　编著
责 任 编 辑：沈承凤
标 准 书 号：ISBN 7-301-05366-5/TP・0638
出　版　者：北京大学出版社
地　　址：北京市海淀区中关村北京大学校内　100871
网　　址：http://cbs.pku.edu.cn
电　　话：发行部 62752015　编辑部 62752038
排　版　者：兴盛达打字服务社　62549189
电 子 信 箱：zpup@pup.pku.edu.cn
印　刷　者：中国科学院印刷厂
发　行　者：北京大学出版社
经　销　者：新华书店
787 毫米×1092 毫米　16 开本　39.625 印张　981 千字
2002 年 6 月第 1 版　2002 年 6 月第 1 次印刷
定　　价：49.00 元

序

“科教兴国”战略强调教育对国民经济的基础地位，要求高等教育“实施全面素质教育，加强思想品德教育和美育，改革教育内容、课程体系和教学方法……”。为了落实好“科教兴国”这一战略决策，北京大学计算机科学技术系与北京大学出版社合作，编审出版基础主干课和专业主干课系列教材。

目前，伴随着微电子和计算机科学技术渗透到社会的各个领域，人类正跨步迈进知识经济时代。在知识经济时代，具有创新能力的高素质人才是经济持续发展的必备条件。

计算机科学技术包括科学和技术两部分，不仅强调严谨的科学性，同时也注重工程性，是一门科学性和工程性并重的学科。信息科学技术的支柱学科是微电子、计算机、通信和软件，其中微电子是基础，计算机和通信是载体，软件是核心，它们相辅相成，共同培育了知识经济。因而，高素质的信息领域科技人才应该掌握上述学科的基础理论和专业技能。

近年来，北京大学计算机科学技术系通过跟踪、分析国际知名大学的相关课程设置、教学实施情况，借鉴国内兄弟院系的课程体系调整建议，总结北京大学计算机科学技术系集计算机软、硬件技术和微电子学于一体的人才培养经验，对课程体系进行了较大力度的梳理，形成了一系列基础主干课和专业主干课。

这一系列教材正是为配合课程体系的调整而编撰的。所选书稿主要是在我系多年的教学实践中师生反映较好的讲义和教材的基础上修编而成的。我们希望这批教材能够达到“注重基础、淡化专业（或突出交叉）、内容系统、选材先进、利于教学”的要求。

对于教材中的不足之处，欢迎广大读者不吝赐教。

杨芙清

1999 年 9 月

前　　言

离散数学是研究离散量的结构及其相互关系的数学学科，是现代数学的一个重要分支。它在各学科领域，特别在计算机科学与技术领域有着广泛的应用，同时离散数学也是计算机专业的许多专业课程，如程序设计语言、数据结构、操作系统、编译技术、人工智能、数据库、算法设计与分析、理论计算机科学基础等必不可少的先行课程。由于它的基础地位和重要性，国内外许多著名大学的计算机科学技术系都将离散数学作为本专业的一门重要的专业基础课。近年发表的 IEEE 2001 计算机科学与技术专业课程计划在世界引起广泛的反响，这个计划的第一专题就是离散结构。通过离散数学的学习，不但可以使学生掌握处理离散结构的描述工具和方法，为后续课程的学习创造条件，而且可以提高学生的抽象思维和严格的逻辑推理能力，为将来参与创新性的研究和开发工作打下坚实的基础。

这本教材是我们多年从事离散数学教学的结晶。在写作中，我们不仅考虑了理论体系的完整和一致性，同时也注重理论联系实际，多次更新和修订教学内容，以适应计算机科学技术的飞速发展。

本书由五编构成。第一编为集合论，包含集合的基本概念、二元关系、函数、自然数、基数、序数等内容。第二编为图论，包含图的基本概念、欧拉图和哈密顿图、树、图的矩阵表示、平面图、图的着色、覆盖集与独立集、带权图及其应用等内容。第三编为代数结构，包含代数系统、半群与独异点、群、环与域、格与布尔代数等内容。第四编为组合数学，包含组合存在性定理、基本的计算公式、组合计数方法、组合计数定理、组合设计与编码、组合最优化等内容。第五编为数理逻辑，包含命题演算、谓词演算、Herberand 定理、直觉主义逻辑学等内容。

本书内容丰富，并包含了比较多的形式化叙述和证明。据我们的经验完成全部教学需要三个学期，总计 220 学时，一、二编 80 学时，三、四编 80 学时，五编 60 学时。如果没有足够多的学时，也可以根据需要选讲其中的部分章节。本书也可以供普通高校计算机专业的教员、研究生，以及从事计算机软、硬件研究和开发的科技人员使用与参考。

本书第一、二编由耿素云撰写，第三、四编由屈婉玲撰写，第五编由王捍贫撰写。

在编写本书过程中，我们参阅了多种离散数学教材和资料，在此向有关作者表示衷心的感谢。还要特别感谢北京大学出版社的编辑和领导以及校系各级领导多年来对教材出版的大力支持和帮助。

最后，我们诚恳地期待读者对本书提出宝贵意见。

作　　者

2001 年 9 月 于北京大学计算机科学技术系

北京大学计算机科学技术系

专业基础课和专业课教材编审指导小组

组　　长：杨芙清

成　　员：（按姓氏笔画序）

卢晓东　李晓明　许卓群　沈承凤　屈婉玲

张天义　赵宝瑛　袁崇义　董士海　程　旭

北京大学计算机科学技术系专业基础课名称

计算引论
数字逻辑
微机原理
计算机组织与体系结构
离散数学
数据结构
编译原理
操作系统
微电子学概论
集成电路原理与设计

北京大学计算机科学技术系专业课名称

计算机网络概论
数据库概论
软件工程
计算机图形学
面向对象技术引论

目　　录

第一编　集　合　论

第二编　图　　论

第三编　代数结构

第四编　组合数学

第五编 数理逻辑

第一编　集合论

第一章　集　　合

1.1　预 备 知 识

本书将数理逻辑部分作为第五编。由于前 4 编也用到相关的基本知识，所以，本书开头先介绍数理逻辑中最基本的逻辑符号、基本的等值式、重要的推理定律(即重要的重言蕴涵式)，以及一阶谓词逻辑中的个体、谓词、量词等基本概念和几个重要的等值式与推理定律.

一、命题公式(或命题形式)

1. 联结词

用 $p,q,r,\cdots$ 表示原子命题(或称简单命题)，用"1"表示命题的真值为真，用"0"表示命题的真值为假，用 5 种联结词给出最基本的复合命题.

(1) $\neg p$ 是"p 的否定"的符号化形式，称为 p 的**否定式**，"$\neg$"称为否定联结词. $\neg p$ 为真当且仅当 p 为假.

(2) $p\wedge q$ 是"p 与 q"的符号化形式，称为 p 与 q 的**合取式**，"$\wedge$"称为合取联结词. $p\wedge q$ 为真当且仅当 p,q 同时为真.

(3) $p\vee q$ 是"p 或 q"的符号化形式，称为 p 与 q 的**析取式**，"$\vee$"称为析取联结词. $p\vee q$ 为假当且仅当 p,q 同时为假.

(4) $p\rightarrow q$ 是"如果 p，则 q"的符号化形式，称为前件为 p，后件为 q 的**蕴涵式**，"$\rightarrow$"称为蕴涵联结词. $p\rightarrow q$ 为假当且仅当 p 为真而 q 为假.

(5) $p\leftrightarrow q$ 是"p 当且仅当 q"的符号化形式，称为 p 与 q 的**等价式**，"$\leftrightarrow$"称为等价联结词. $p\leftrightarrow q$为真当且仅当 p 与 q 的真值相同(即 p,q 同为真或同为假).

2. 命题公式

$p,q,r,\cdots$既可以表示命题(命题常元)，也可以表示命题变元.

命题公式的形成规则如下：

(1) 单个命题变元(或常元)是命题公式；

(2) 若 A 是命题公式，则$(\neg A)$也是命题公式；

(3) 若 A,B 是命题公式，则$(A\wedge B)$，$(A\vee B)$，$(A\rightarrow B)$，$(A\leftrightarrow B)$也是命题公式；

(4) 只有有限次地应用(1)—(3)形成的符号串才是**命题公式**. 命题公式也称为**命题形式**或简称为**公式**.

设命题公式 A 中含有 n 个命题变元 $p_1,p_2,\cdots,p_n$，给 p_i 指定一个值 α_i(α_i 为 0 或 1，$i=1$，

$2,\cdots,n$)，所得字符串 $\alpha_1\alpha_2\cdots\alpha_n$ 称为 A 的一个**赋值**，A 共有 2^n 个赋值. 若在 $\alpha_1\alpha_2\cdots\alpha_n$ 下 A 的真值为 1，则称它为 A 的**成真赋值**，否则，即 A 的真值为 0，则称它为 A 的**成假赋值**.

若公式 A 没有成假赋值，则称 A 为**重言式**或**永真式**；若 A 没有成真赋值，则称 A 为**矛盾式**或**永假式**；若 A 至少存在一个成真赋值，则称 A 是**可满足式**.

二、等值演算

1. 等值式

若 $A\leftrightarrow B$ 为重言式，则称 A 与 B 是等值的，记为 $A\Leftrightarrow B$，并称 $A\Leftrightarrow B$ 为**等值式**.

2. 基本的等值式

(1) **幂等律**　$A\Leftrightarrow A\vee A$，$A\Leftrightarrow A\wedge A$；

(2) **交换律**　$A\vee B\Leftrightarrow B\vee A$，$A\wedge B\Leftrightarrow B\wedge A$；

(3) **结合律**　$(A\vee B)\vee C\Leftrightarrow A\vee(B\vee C)$，$(A\wedge B)\wedge C\Leftrightarrow A\wedge(B\wedge C)$；

(4) **分配律**　$A\vee(B\wedge C)\Leftrightarrow(A\vee B)\wedge(A\vee C)$，$A\wedge(B\vee C)\Leftrightarrow(A\wedge B)\vee(A\wedge C)$；

(5) **德·摩根律**　$\neg(A\vee B)\Leftrightarrow\neg A\wedge\neg B$，$\neg(A\wedge B)\Leftrightarrow\neg A\vee\neg B$；

(6) **吸收律**　$A\vee(A\wedge B)\Leftrightarrow A$，$A\wedge(A\vee B)\Leftrightarrow A$；

(7) **零律**　$A\vee 1\Leftrightarrow 1$，$A\wedge 0\Leftrightarrow 0$；

(8) **同一律**　$A\vee 0\Leftrightarrow A$，$A\wedge 1\Leftrightarrow A$；

(9) **排中律**　$A\vee\neg A\Leftrightarrow 1$；

(10) **矛盾律**　$A\wedge\neg A\Leftrightarrow 0$；

(11) **双重否定律**　$\neg\neg A\Leftrightarrow A$；

(12) **蕴涵等值式**　$A\rightarrow B\Leftrightarrow\neg A\vee B$；

(13) **等价等值式**　$A\leftrightarrow B\Leftrightarrow(A\rightarrow B)\wedge(B\rightarrow A)$；

(14) **等价否定等值式**　$A\leftrightarrow B\Leftrightarrow\neg A\leftrightarrow\neg B$；

(15) **假言易位**　$A\rightarrow B\Leftrightarrow\neg B\rightarrow\neg A$；

(16) **归谬论**　$(A\rightarrow B)\wedge(A\rightarrow\neg B)\Leftrightarrow\neg A$.

3. 等值演算

(1) **置换规则**　设 $\Phi(A)$ 是含公式 A 的公式，用公式 B 置换 $\Phi(A)$ 中的 A，得公式 $\Phi(B)$，如果 $B\Leftrightarrow A$，则 $\Phi(B)\Leftrightarrow\Phi(A)$.

(2) **等值演算**　由已知的等值式，应用置换规则推演出新的等值式的过程称为等值演算.

等值演算就是应用已知的等值式的置换过程. 下面以证明 $p\rightarrow(q\rightarrow r)$ 与 $(p\wedge q)\rightarrow r$ 等值来说明等值演算的过程.

$p\rightarrow(q\rightarrow r)$

$\Leftrightarrow p\rightarrow(\neg q\vee r)$　　（应用蕴涵等值式和置换规则）

$\Leftrightarrow\neg p\vee(\neg q\vee r)$　　（应用蕴涵等值式和置换规则）

$\Leftrightarrow(\neg p\vee\neg q)\vee r$　　（应用结合律和置换规则）

$\Leftrightarrow\neg(p\wedge q)\vee r$　　（应用德·摩根律和置换规则）

$\Leftrightarrow(p\wedge q)\rightarrow r$　　（应用蕴涵等值式和置换规则）

由以上的演算可知，应用了一些基本的等值式和置换规则，推演出了新的等值式

$$p\rightarrow(q\rightarrow r)\Leftrightarrow(p\wedge q)\rightarrow r.$$

三、命题逻辑推理

1. 推理的形式结构

称蕴涵式

$$(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \to B \tag{*}$$

为**推理的形式结构**，$A_1, A_2, \cdots A_k$ 为推理的**前提**，B 为**结论**. 若推理的形式结构（*）为重言式，则称推理正确，否则称推理不正确.

一般用“$A \Rightarrow B$”表示“$A \to B$”是重言式，所以，当推理正确时，记（*）为

$$(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \Rightarrow B.$$

2. 重要的推理定律

在推理过程中经常使用等值式和下面 8 条推理定律（称重言蕴涵式为推理定律）.

(1) **附加律** $A \Rightarrow (A \vee B)$；

(2) **化简律** $(A \wedge B) \Rightarrow A$，$(A \wedge B) \Rightarrow B$；

(3) **假言推理定律**（简称**假言推理**） $(A \to B) \wedge A \Rightarrow B$；

(4) **拒取式推理定律**（简称**拒取式**） $(A \to B) \wedge \neg B \Rightarrow \neg A$；

(5) **析取三段论推理定律**（简称**析取三段论**） $(A \vee B) \wedge \neg B \Rightarrow A$，$(A \vee B) \wedge \neg A \Rightarrow B$；

(6) **假言三段论推理定律**（简称**假言三段论**） $(A \to B) \wedge (B \to C) \Rightarrow (A \to C)$；

(7) **等价三段论推理定律**（简称**等价三段论**） $(A \leftrightarrow B) \wedge (B \leftrightarrow C) \Rightarrow (A \leftrightarrow C)$；

(8) **构造性二难推理定律**（简称**构造性二难**） $(A \to B) \wedge (C \to D) \wedge (A \vee C) \Rightarrow (B \vee D)$.

3. 判断正确推理的方法

判断推理是否正确，就是判断推理的形式结构

$$(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \to B \tag{*}$$

是否为重言式. 判断一个蕴涵式是否为重言式的方法很多，比如真值表法、等值演算法等都可以证明（*）是否为重言式，但直接证明这个蕴涵式为重言式往往是很麻烦的.

像证 $A \leftrightarrow B$ 为重言式一样，不直接证明 $A \leftrightarrow B \Leftrightarrow \cdots \Leftrightarrow 1$，而是利用基本等值式，从 A 出发证 $A \Leftrightarrow \cdots \Leftrightarrow B$，所以 $A \Leftrightarrow B$（等值关系有传递性）. 在证明（*）为重言式（即推理正确）时，也可以利用基本等值式和重要推理定律，从前提出发证 $A_1 \wedge A_2 \wedge \cdots \wedge A_k \Rightarrow \cdots \Rightarrow B$. 中间有些“$\Rightarrow$”可能是“$\Leftrightarrow$”，这样证明比直接证（*）等值于 1 方便.

例如，证明从前提 $p \to (q \to r)$，p，q，推出结论 r 的推理是正确的.

推理的形式结构为

$$(p \to (q \to r)) \wedge p \wedge q \to r \tag{*}$$

方法一 直接证（*）等值于 1. 演算过程如下：

$(p \to (q \to r)) \wedge p \wedge q \to r$

$\Leftrightarrow (\neg p \vee \neg q \vee r) \wedge p \wedge q \to r$

$\Leftrightarrow ((\neg p \wedge p) \vee (\neg q \vee r) \wedge p) \wedge q \to r$

$\Leftrightarrow (\neg q \vee r) \wedge q \wedge p \to r$

$\Leftrightarrow ((\neg q \wedge q) \vee (r \wedge q)) \wedge p \to r$

$\Leftrightarrow (r \wedge q \wedge p) \to r$

$\Leftrightarrow \neg(r \wedge q \wedge p) \vee r$

$\Leftrightarrow \neg p \vee \neg q \vee (\neg r \vee r)$

$\Leftrightarrow \neg p \vee \neg q \vee 1$

$\Leftrightarrow 1.$

请读者填出以上演算过程中每一步所用的基本等值式.这个演算是相当麻烦的.

方法二 由前提推演出结论.

$(p \to (q \to r)) \wedge p \wedge q$

$\Leftrightarrow ((p \to (q \to r)) \wedge p) \wedge q$ （结合律）

$\Rightarrow (q \to r) \wedge q$ （假言推理）

$\Rightarrow r.$ （假言推理）

显然方法二比方法一简单多了.值得注意的是演算中的每一步所用的是"$\Leftrightarrow$"还是"$\Rightarrow$",特别地,不能将"$\Rightarrow$"当成"$\Leftrightarrow$".

像方法二这样的证明方法在数学中,比如在集合论中是常用的方法.

在数理逻辑中常用的方法是构造证明法,这里就不介绍了.

四、一阶谓词逻辑基本概念与命题符号化

1. 个体、谓词与量词

在一阶谓词逻辑中,将原子命题再细分成主语与谓语,因而引入了个体(或个体词)与谓词的概念.

将可以独立存在的客体(具体事物或抽象概念)称为**个体**或**个体词**,并用 $a,b,c,\cdots$ 表示个体常元,$x,y,z,\cdots$ 表示个体变元.将个体变元的取值范围称为**个体域**,个体域可以是有穷或无穷集合,人们称由宇宙间一切事物组成的个体域为**全总个体域**.

将表示个体性质或彼此之间关系的词称为**谓词**,常用 $F,G,H,\cdots$ 表示谓词常元或变元.用 $F(x)$ 表示 x 具有性质 F.例如,F 表示"…是黑色的",则 $F(x)$ 表示"x 是黑色的",如果取 x 为黑板,并用常元 a 表示黑板,则 $F(a)$ 表示黑板是黑色的.个体变元多于两个的谓词,如 $F(x,y)$ 表示 x 与 y 具有关系 F.例如 $F(x,y)$ 表示"x 大于 y",则 $F(5,2)$ 表示"5 大于 2".

称表示数量的词为**量词**.在数理逻辑中使用的量词有两个:

(1) **全量量词** 全称量词是自然语言中的"所存的"、"一切的"、"任意的"、"每一个"、"都"等的统称,并用符号"$\forall$"表示.而用 $\forall x$ 表示个体域里的所有 x,用 $\forall x F(x)$ 表示个体域里所有 x 都有性质 F.

(2) **存在量词** 存在量词是自然语言中的"有一个"、"至少有一个"、"存在着"、"有的"等的统称,并用"$\exists$"表示.而用 $\exists x$ 表示存在个体域里的 x,用 $\exists x F(x)$ 表示在个体域里存在 x 具有性质 F.

2. 命题符号化

在一阶谓词逻辑中命题符号化应注意以下两个"基本公式".

(1) 个体域中所有有性质 F 的个体都有性质 G,应符号化为

$$\forall x(F(x) \to G(x)).$$

其中,$F(x)$:x 具有性质 F,$G(x)$:x 具有性质 G.

(2) 个体域中存在有性质 F 同时有性质 G 的个体,应符号化为

$$\exists x(F(x) \wedge G(x)).$$

其中，$F(x)$：x 具有性质 F，$G(x)$：x 具有性质 G.

例 将下面命题符号化.

(1) 人都吃饭；

(2) 有人喜欢吃糖；

(3) 男人都比女人跑得快(这是假命题).

这里没有指明个体域，因而使用全总个体域. 用以上两个"基本公式"，容易将这 3 个命题符号化.

(1) 令 $F(x)$：x 为人，$G(x)$：x 吃饭. 命题符号化为 $\forall x(F(x) \rightarrow G(x))$；

(2) 令 $F(x)$：x 为人，$G(x)$：x 喜欢吃糖. 命题符号化为 $\exists x(F(x) \wedge G(x))$；

(3) 令 $F(x)$：x 为男人，$G(y)$：y 为女人，$H(x,y)$：x 比 y 跑得快. 命题符号化为

$$\forall x(F(x) \rightarrow \forall y(G(y) \rightarrow H(x,y))).$$

(3)中公式还有一些等值形式，也可符号化为

$$\forall x \forall y(F(x) \wedge G(y) \rightarrow H(x,y)).$$

五、一阶谓词逻辑公式及其分类

一阶谓词逻辑公式也简称为公式，它的形成规则类似于命题逻辑公式，只需加上一条，即若 A 是公式，则 $\forall xA$ 及 $\exists xA$ 也都是公式.

在公式 $\forall xA$ 和 $\exists xA$ 中，称 x 为**指导变元**，称 A 为相应量词的**辖域**. 在 $\forall x$ 和 $\exists x$ 的辖域中，x 的所有出现都称为**是约束出现的**，A 中不是约束出现的变元称为**自由出现的**. 例如在公式

$$\forall x(F(x) \rightarrow \exists y(G(y) \wedge H(x,y,z)))$$

中，$\forall x$ 的辖域为$(F(x) \rightarrow \exists y(G(y) \wedge H(x,y,z)))$，而 $\exists y$ 的辖域为$(G(y) \wedge H(x,y,z))$. 除 z 是自由出现的变元外，都是约束出现的.

对于给定的公式 A，如果指定 A 的个体域为已知的 D，并用特定的个体常元取代 A 中的个体常元，用特定函数取代 A 中的函数变元，用特定的谓词取代 A 中的谓词变元，则就构成了 A 的一个**解释**.

给定公式 A 为 $\forall x(F(x) \rightarrow G(x))$. 可以给 A 多种解释，例如：

(1) 取个体域 D 为实数集合，$F(x)$：x 是有理数，$G(x)$：x 能表示成分数，则 A 被解释成为"有理数都能表示成分数"，这是真命题.

(2) 取个体域 D 为全总个体域，$F(x)$：x 为人，$G(x)$：x 长着黑头发，则 A 又被解释成"人都长着黑头发"，这是假命题.

一阶谓词逻辑公式也分成 3 类：

(1) 若 A 在任何解释下都为真，则称 A 为**永真式**；

(2) 若 A 在任何解释下均为假，则称 A 为**永假式**；

(3) 若 A 至少存在一个成真的解释，则称 A 为**可满足式**.

六、一阶谓词逻辑等值式与基本等值式

设 A，B 为二公式，若 $A \leftrightarrow B$ 为永真式，则称 A 与 B 等值，记为 $A \Leftrightarrow B$，并称 $A \Leftrightarrow B$ 为等值式.

人们已经证明的基本等值式有以下 4 组:

1. **在有限个体域 $D=\{a_1,a_2,\cdots,a_n\}$ 中消去量词等值式:**

(1) $\forall xA(x) \Leftrightarrow A(a_1) \wedge A(a_2) \wedge \cdots \wedge A(a_n)$;

(2) $\exists xA(x) \Leftrightarrow A(a_1) \vee A(a_2) \vee \cdots \vee A(a_n)$.

2. **量词否定等值式:**

(1) $\neg \forall xA(x) \Leftrightarrow \exists x \neg A(x)$;

(2) $\neg \exists xA(x) \Leftrightarrow \forall x \neg A(x)$.

3. **量词辖域收缩与扩张等值式(B 中不含 x):**

(1) $\forall x(A(x) \vee B) \Leftrightarrow \forall xA(x) \vee B$;　　(2) $\forall x(A(x) \wedge B) \Leftrightarrow \forall xA(x) \wedge B$;

(3) $\forall x(A(x) \rightarrow B) \Leftrightarrow \exists xA(x) \rightarrow B$;　　(4) $\forall x(B \rightarrow A(x)) \Leftrightarrow B \rightarrow \forall xA(x)$;

(5) $\exists x(A(x) \vee B) \Leftrightarrow \exists xA(x) \vee B$;　　(6) $\exists x(A(x) \wedge B) \Leftrightarrow \exists xA(x) \wedge B$;

(7) $\exists x(A(x) \rightarrow B) \Leftrightarrow \forall xA(x) \rightarrow B$;　　(8) $\exists x(B \rightarrow A(x)) \Leftrightarrow B \rightarrow \exists xA(x)$.

以上 8 个公式成立的条件是 B 中不含 x 的出现.

4. **量词分配等值式:**

(1) $\forall x(A(x) \wedge B(x)) \Leftrightarrow \forall xA(x) \wedge \forall xB(x)$;

(2) $\exists x(A(x) \vee B(x)) \Leftrightarrow \exists xA(x) \vee \exists xB(x)$.

(1)说明,全称量词对“$\wedge$”有分配律.注意,全称量词对“$\vee$”不适合分配律.(2)说明,存在量词对“$\vee$”有分配律,而对“$\wedge$”不适合分配律.以上两点说明,在应用中要特别注意.

还应该指出的是,命题逻辑中的基本等值式在一阶谓词逻辑中也均成立,只是其中的公式均为一阶谓词逻辑公式罢了.

七、前束范式

若公式 A 具有如下形式

$$Q_1x_1Q_2x_2\cdots Q_kx_kB,$$

则称 A 为**前束范式**.其中 $Q_i(1 \leqslant i \leqslant k)$ 为$\forall$ 或$\exists$,B 中不含量词.

将公式 A 化成与之等值的前束范式时,除了利用基本的等值式外,有时还用到换名规则.

换名规则　将公式 A 中某量词辖域中出现的某个约束出现的个体变元及相应的指导变元 x_i,都改成公式 A 中没出现过的 x_j,所得公式 $A' \Leftrightarrow A$.

例如,$\forall x(F(x) \rightarrow G(x,y)) \Leftrightarrow \forall z(F(z) \rightarrow G(z,y))$.

下面以求$\forall xF(x) \vee \neg \exists xG(x,y)$的前束范式为例,说明求前束范式的过程.

$\forall xF(x) \vee \neg \exists xG(x,y)$

$\Leftrightarrow \forall xF(x) \vee \forall x \neg G(x,y)$　　(量词否定等值式)

$\Leftrightarrow \forall xF(x) \vee \forall z \neg G(z,y)$　　(换名规则)

$\Leftrightarrow \forall x(F(x) \vee \forall z \neg G(z,y))$　　(辖域扩张等值式)

$\Leftrightarrow \forall x \forall z(F(x) \vee \neg G(z,y))$　　(辖域扩张等值式)

$\Leftrightarrow \forall x \forall z(G(z,y) \rightarrow F(x))$　　(蕴涵等值式)

最后两步都是原公式的前束范式.

八、重要的推理定律

同在命题逻辑中一样,在一阶谓词逻辑中仍称永真的蕴涵式为推理定律.常用的推理定律

有下面 4 条：

(1) $\forall xA(x) \vee \forall xB(x) \Rightarrow \forall x(A(x) \vee B(x))$；

(2) $\exists x(A(x) \wedge B(x)) \Rightarrow \exists xA(x) \wedge \exists xB(x)$；

(3) $\forall x(A(x) \rightarrow B(x)) \Rightarrow \forall xA(x) \rightarrow \forall xB(x)$；

(4) $\forall x(A(x) \rightarrow B(x)) \Rightarrow \exists xA(x) \rightarrow \exists xB(x)$.

在使用以上 4 条推理定律时，千万注意，别将它们当成等值式用，这样会犯错误的.

1.2 集合的概念及集合之间的关系

自从 19 世纪末著名的德国数学家康托(G. Cantor 1845—1918)为集合论做奠基工作以来，集合论在一百多年的时间里，已经成为数学中不可缺少的基本的描述工具，集合已成了数学中最为基本的概念.

集合论分为两种体系，一种是朴素集合论体系，也称为康托集合论体系；另一种是公理集合论体系. 本书不讨论公理集合论体系，在前 6 章介绍的是朴素集合论体系中的主要内容. 在朴素集合论体系中，有些概念，特别是关于集合的概念是不能精确定义的. 我们不给集合下严格定义，这丝毫不会影响对集合的理解.

一般地，人们用大写英文字母 $A,B,C,\cdots$ 表示集合，用小写英文字母 $a,b,c,\cdots$ 表示集合中的元素. 用 $a\in A$ 表示 a 为 A 的元素，读作 a 属于 A，而用 $a\notin A$ 表示 a 不是 A 中的元素，读作 a 不属于 A. 一般用两种方法表示集合.

列举法：列出集合中的全体元素，元素之间用逗号分开，然后用花括号括起来. 设 A 是由 a,b,c,d 为元素的集合，B 是正偶数集合，则 $A=\{a,b,c,d\}$，$B=\{2,4,6,\cdots\}$.

描述法：用谓词 $P(x)$ 表示 x 具有性质 P，用 $\{x\mid P(x)\}$ 表示具有性质 P 的集合，例如，$P_1(x)$：x 是英文字母，$P_2(y)$：y 是十进制数字，则 $C=\{x\mid P_1(x)\}$，$D=\{y\mid P_2(y)\}$ 分别表示 26 个英文字母集合和 10 个十进制数字集合.

对于集合的表示法应该注意以下几点：

(1) 集合中的元素是各不相同的.

(2) 集合中的元素不规定顺序.

(3) 集合的两种表示法有时是可以互相转化的. 例如列举法中的 B 可用描述法表示为 $B=\{x\mid x>0$ 且 x 为偶数$\}$ 或 $\{x\mid x=2(k+1)$，k 为非负整数$\}$.

为方便起见，本书中指定 N,Z,Q,R,C 分别表示自然数集合(含 0)，整数集合，有理数集合，实数集合和复数集合. 有了这个规定之后，列举法中的 B 又可表示为 $\{x\mid x\in N$ 且 x 为非 0 偶数$\}$，或 $\{x\mid x=2(k+1)$ 且 $k\in N\}$. 由此可见，表示一个集合的方法是很灵活多变的，当然要注意准确性和简洁性. 下面讨论集合之间的关系.

定义 1.1 设 A,B 为二集合，若 B 中的每个元素都是 A 中的元素，则称 B 是 A 的**子集**，也称 A 包含 B 或 B 含于 A，记作 $B\subseteq A$. 其符号化形式为 $B\subseteq A \Leftrightarrow \forall x(x\in B \rightarrow x\in A)$.

若 B 不是 A 的子集，则记作 $B\nsubseteq A$，其符号化形式为 $B\nsubseteq A \Leftrightarrow \exists x(x\in B \wedge x\notin A)$.

设 $A=\{a,b,c\}$，$B=\{a,b,c,d\}$，$C=\{a,b\}$，则 $A\subseteq B$，$C\subseteq A$，$C\subseteq B$.

定义 1.2 设 A,B 为二集合，若 A 包含 B 且 B 包含 A，则称 A 与 B **相等**，记作 $A=B$. 即

$$A=B \Leftrightarrow \forall x(x\in A \leftrightarrow x\in B).$$

设 $A=\{2\}$，$B=\{1,4\}$，$C=\{x|x^2-5x+4=0\}$，$D=\{x|x$ 为偶素数$\}$，则 $A=D$ 且 $B=C$.

设 A,B,C 为 3 个集合，容易证明下面 3 个命题为真：

(1) $A\subseteq A$； (2) 若 $A\subseteq B$ 且 $A\neq B$，则 $B\nsubseteq A$； (3) 若 $A\subseteq B$ 且 $B\subseteq C$，则 $A\subseteq C$.

定义 1.3 设 A,B 为二集合，若 A 为 B 的子集，且 $A\neq B$，则称 A 为 B 的**真子集**，或称 B 真包含 A，记作 $A\subset B$. 即 $A\subset B\Leftrightarrow A\subseteq B\wedge A\neq B$.

若 A 不是 B 的真子集，则记作 $A\not\subset B$，其符号化形式为

$$A\not\subset B\Leftrightarrow\exists x(x\in A\wedge x\notin B)\vee(A=B).$$

设 A,B,C 为 3 个集合，从定义不难看出下面 3 个命题为真：

(1) $A\not\subset A$； (2) 若 $A\subset B$，则 $B\not\subset A$； (3) 若 $A\subset B$ 且 $B\subset C$，则 $A\subset C$.

定义 1.4 不拥有任何元素的集合称为**空集合**，简称为**空集**，记作$\varnothing$[①].

$\{x|x^2+1=0\wedge x\in R\}$，$\{(x,y)|x^2+y^2<0\wedge x,y\in R\}$都是空集.

定理 1.1 空集是一切集合的子集.

证明 只要证明，对于任意的集合 A，均有$\varnothing\subseteq A$ 成立，即证明$\forall x(x\in\varnothing\to x\in A)$为真，这是显然的. ▌

推论 空集是惟一的.

证明 设$\varnothing_1$与$\varnothing_2$都是空集，由定理 1.1 可知 $\varnothing_1\subseteq\varnothing_2\wedge\varnothing_2\subseteq\varnothing_1$，所以，$\varnothing_1=\varnothing_2$. ▌

由推论可知，空集无论以什么形式出现，它们都是相等的. 因而

$$\{x|x\neq x\}=\{x|x^2+1=0\wedge x\in R\}=\varnothing.$$

空集是一切集合的子集，从这个意义上看，可以形象地说：$\varnothing$是“最小”的集合. 有无最大的集合呢？回答是否定的，但当讨论某具体问题时，可以定义一个具有相对性的“最大”集合.

定义 1.5 如果限定所讨论的集合都是某一集合的子集，则称该集合为**全集**，常记为 E.

从定义可以看出，全集的概念具有相对性. 例如，当我们讨论区间(a,b)上实数的性质时，可将(a,b)取为全集，当讨论$[0,+\infty)$上实数性质时，可将区间$[0,+\infty)$取成全集. 这说明全集是根据具体情况而决定的，因而具有相对性.

又容易发现，根据某一具体情况定义的全集是不惟一的. 讨论区间(a,b)上实数性质时，当然可以取(a,b)为全集，也可以取区间$[a,b)$，$(a,b]$，$(a,+\infty)$，实数集 R 等为全集. 又如，当讨论的集合都是 $A=\{a,b,c\}$的子集时，可以取 A 为全集，也可以取 $B=\{a,b,c,d\}$为全集，其实，可以取包含 A 的一切集合为全集，而 A 是所要求的全集中“最小”的全集，但找不到所要求的“最大”的全集.

给定若干个集合后，都可以找到包含它们的全集，因而在今后的讨论中，所涉及到的集合都可以看成某个全集 E 的子集.

定义 1.6 设 A 为一个集合，称由 A 的所有子集组成的集合为 A 的**幂集**，记作 $P(A)$[②]. 用描述法表示为 $P(A)=\{x|x\subseteq A\}$.

为方便起见，本书中规定，$\varnothing$为 **0 元集**，含 1 个元素的集合为**单元集**或 **1 元集**，含 2 个元素的集合为 **2 元集**，…，含 n 个元素的集合为 **n 元集**($n\geqslant 1$). 用$|A|$表示 A 中的元素个数，当 A 中

---

① $\varnothing$是丹麦字母，发音为“ugh”.

② 在概率论中，用 $P(A)$表示事件 A 的概率，请读者注意区分. 有的书上用 2^A 表示 A 的幂集.

的元素个数为有限数时，A 为**有穷集**或**有穷集**[1].

为了求出给定集合 A 的幂集，首先求出 A 的由低到高元的所有子集，再将它们组成集合即可. 设 $A=\{a,b,c\}$，求 $P(A)$的步骤如下：

0 元子集为：$\varnothing$；

1 元子集为：$\{a\}$，$\{b\}$，$\{c\}$；

2 元子集为：$\{a,b\}$，$\{a,c\}$，$\{b,c\}$；

3 元子集为：$\{a,b,c\}=A$.

A 的幂集 $P(A)=\{\varnothing,\{a\},\{b\},\{c\},\{a,b\},\{a,c\},\{b,c\},\{a,b,c\}\}$.

从以上的讨论不难证明下面定理.

定理 1.2 设集合 A 的元素个数 $|A|=n$（n 为自然数），则 $|P(A)|=2^n$.

除了 $P(A)$这样由集合构成的集合外，在数学中还会遇到许多其他形式的由集合构成的集合，统称这样的集合为**集族**. 若将集族中的集合都赋予记号，则可得带指标集的集族，见下面定义.

定义 1.7 设 $\mathscr{A}$ 为一个集族，S 为一个集合，若对于任意的 $\alpha\in S$，存在惟一的 $A_\alpha\in\mathscr{A}$ 与之对应，而且 $\mathscr{A}$ 中的任何集合都对应 S 中的某一元素，则称 $\mathscr{A}$ 是以 S 为指标集的**集族**，S 称为 $\mathscr{A}$ 的**指标集**. 常记 $\mathscr{A}=\{A_\alpha|\alpha\in S\}$，或 $\mathscr{A}=\{A_\alpha\}_{\alpha\in S}$.

如果将$\varnothing$看成集族，则称$\varnothing$为**空集族**.

设 $A_1=\{x|x\in N\wedge x$ 为奇数$\}$，$A_2=\{x|x\in N\wedge x$ 为偶数$\}$，则$\{A_1,A_2\}$是以$\{1,2\}$为指标集的集族.

设 p 为一素数，$A_k=\{x|x=k(\mathrm{mod}\ p)\}$，$k=0,1,\cdots,p-1$，则 $\mathscr{A}=\{A_0,A_1,\cdots,A_{p-1}\}$是以$\{0,1,2,\cdots,p-1\}$为指标集的集族，也可以记为 $\mathscr{A}=\{A_k|k\in\{0,1,\cdots,p-1\}\}$，或 $\mathscr{A}=\{A_k\}_{k\in\{0,1,2,\cdots,p-1\}}$.

设 $A_n=\{x|x\in N\wedge x=n\}$，则 $\mathscr{A}=\{A_n|n\in N\}$是以 N 为指标集的集族，集族中的元素为以各自然数为元素的单元集.

令 $N_+=N-\{0\}$，设 $A_n=\{x|0\leqslant x<\frac{1}{n}\wedge n\in N_+\}$，则 $\mathscr{A}=\{A_n|n\in N_+\}$是以 N_+为指标集的集族，其元素为半开半闭区间$\left[0,\frac{1}{n}\right)$，$n=1,2,\cdots$.

在本节结束之前，略谈一下多重集合的概念，前面谈到的集合都是由不同对象（元素）组成的. 某元素在集合中无论重复出现多少次，仍看成是一个元素. 而在实际中，某一元素的重复出现往往表达了某种实际意义. 例如，在某项工程中所需要的工程技术人员的种类可用集合 $A=\{$电机工程师，机械工程师，数学家，制图员，程序员$\}$表示，但从集合 A 看不出所需要人员的数量，于是引出多重集合的概念.

设全集为 E，E 中元素可以不止一次在 A 中出现的集合 A，称为**多重集合**. 若 E 中元素 a 在 A 中出现 $k(k\geqslant 0)$次，则称 a 在 A 中的**重复度**为 k.

设全集 $E=\{a,b,c,d,e\}$. $A=\{a,a,b,b,c\}$为多重集合，其中 a,b 的重复度为 2，C 的重复度为 1，而 d,e 的重复度均为 0.

其实，集合可看成是各元素重复度均小于等于 1 的多重集合.

---

[1] 在本小节所给出的概念，在第五章还要给出严格的定义或表示法.