

离散数学 及其在计算机中的应用

(第三次修订)

徐洁磐 朱怀宏 宋方敏 编著

人民邮电出版社

内 容 提 要

离散数学和计算机科学关系密切。本书系统地介绍了离散数学的基础理论,阐述了各个分支之间的联系,还说明了它在计算机中的应用。主要包括:集合论、关系、映射和无限集、近世代数、图论、命题逻辑、谓词逻辑、命题逻辑和谓词逻辑的公理化理论、离散数学在计算机中的应用。章末附有复习提纲及习题,书末附有各章习题解答。

本书适合作为计算机及相关专业的学生和自学考试者的教材,也可供从事计算机和数学方面研究的科技工作者和教师学习参考。

图书在版编目(CIP)数据

离散数学及其在计算机中的应用/徐洁磐,朱怀宏,宋方敏编著.

—3 版(修订本). —北京:人民邮电出版社,2005.4

ISBN 7-115-13237-2

I. 离... II. ①徐... ②朱... ③宋... III. ①离散数学—数学理论
②离散数学—计算机应用 IV. 0158②TP3

中国版本图书馆 CIP 数据核字(2005)第 024501 号

离散数学及其在计算机中的应用(第三次修订)

◆ 编 著 徐洁磐 朱怀宏 宋方敏
责任编辑 梁 凝

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 <http://www.ptpress.com.cn>
读者热线 010-67129258
北京隆昌伟业印刷有限公司印刷
新华书店总店北京发行所经销

◆ 开本:850×1168 1/32
印张:13.5
字数:357 千字 2005 年 4 月第 3 版
印数:27 631-31 630 册 2005 年 4 月北京第 9 次印刷

ISBN 7-115-13237-2/TN · 2441

定价:22.00 元

本书如有印装质量问题,请与本社联系 电话:(010)67129223

第四版序言

本书自 1985 年出版至今已 20 年并经历了三个版本的修改,目前,这次已是第四版了。本书以简单、明了、讲解清楚为其特色,同时将离散数学与计算机科学紧密结合构成了本书的另一个特色。在这一版中将继续保持本书原有特色,同时也对其做了一些必要的修改与调整,主要目的是使读者能对所学内容更进一步了解与掌握。本版调整的内容是:

(1) 为便于读者复习,在本版的每章中均增加有复习提纲,该提纲为复习该章提供帮助。

(2) 为帮助读者加深对内容的理解,在本版中增添了若干习题,特别是增添了一些带有全局性与理解性的习题。

(3) 在本版中的所有习题均附有答案,这主要是为方便读者解题。

(4) 对第三版中所出现的一些错误做了订正。

本书非常适合作为计算相关专业(特别是应用类专业)的大学本科、专科的教材,它还适合作为职业技术教学、自学考试教材以及参考资料。本书还可作为从事计算机及相关应用的科技人员学习、参考之用。

本书的复习提纲编写由徐洁磐完成,习题增补及全部解答由朱怀宏完成,全书错误订正由徐洁磐完成。

在本书出版 20 年的过程中,作者不断得到广大读者的支持和帮助,希望在今后还能继续得到广大读者的支持和帮助,在这里谨向广大读者表示诚挚的感谢。

作 者

2004 年 11 月 20 日于南京

目 录

第一章 集合论.....	1
1.1 集合和元素的概念	1
1.2 集合的子集	2
1.3 全集和空集	3
1.4 集合的运算、文氏图.....	5
1.5 有限集中的元素数目	13
习题一	16
第二章 关系	22
2.1 关系的基本概念.....	22
2.2 关系的性质.....	25
2.3 关系的运算.....	26
2.4 关系的闭包运算.....	31
2.5 具有特定性质的关系.....	35
习题二	39
第三章 映射与无限集	45
3.1 映射.....	45
3.2 无限集.....	51
习题三	58
第四章 近世代数	63
4.1 代数运算.....	63
4.2 代数系统.....	68

4.3	同态和同构.....	69
4.4	半群和单元半群.....	72
4.5	群论.....	74
4.6	环、理想、整环和域.....	96
4.7	偏序集和格	105
	习题四.....	115
第五章 图论.....		130
5.1	图的基本概念	130
5.2	连通性	133
5.3	图的矩阵表示	141
5.4	权图、最小权通路和最小权回路.....	145
5.5	二分图	157
5.6	平面图	162
5.7	四色图	167
5.8	树	172
5.9	有向图	188
	习题五.....	196
第六章 命题逻辑.....		213
6.1	命题与命题联结词	213
6.2	命题公式	221
6.3	重言式	237
6.4	范式	243
	习题六.....	251
第七章 谓词逻辑.....		260
7.1	谓词逻辑的基本概念	260
7.2	谓词逻辑公式及其基本永真公式	267

7.3	前束范式与斯科林范式	274
7.4	函数	276
	习题七.....	277
第八章	命题逻辑与谓词逻辑的公理化理论.....	283
8.1	公理化理论的基本思想	283
8.2	命题逻辑的公理系统	284
8.3	谓词逻辑的公理系统	289
	习题八.....	294
第九章	离散数学在计算机科学中的应用.....	298
9.1	离散数学在关系数据库中的应用	298
9.2	离散数学与纠错码	324
9.3	谓词逻辑与逻辑程序设计语言	342
	习题九.....	356
	习题解答.....	358
	习题一解答.....	358
	习题二解答.....	365
	习题三解答.....	373
	习题四解答.....	376
	习题五解答.....	387
	习题六解答.....	400
	习题七解答.....	415
	习题八解答.....	419
	习题九解答.....	421
	参考文献.....	423

第一章 集合论

1.1 集合和元素的概念

集合的理论在现代数学中起了十分重要的作用,集合论的语言是各门数学的基础。对计算机科学工作者来说,集合的概念也是必不可少的。

首先我们对集合及其元素的概念作一初步说明。一般地说,一个集合是指所研究对象的全体,其中每个对象是该集合中的一个元素(也叫成员)。对任意一个集合 S 和一个元素 x ,若 x 是 S 中的一个元素,记以 $x \in S$,读作“ x 属于 S ”,若 x 不是 S 中的一个元素,记作 $x \notin S$,读作“ x 不属于 S ”。显然,任意一个元素要么属于某一个集合,要么不属于某一个集合,二者必居其一。

本书中,除非特别声明,下面几个符号是常用来表示特定集合的。

N : 自然数集合 $\{0, 1, 2, \dots\}^*$

I : 整数集合

Q : 有理数集合

R : 实数集合

$N_m (m \geq 1)$: 集合 $\{0, 1, 2, \dots, m-1\}$

表示一个集合中的元素通常有三种方法:

第一,列举已知集合中的元素,如 $A = \{1, 2, 3, 4\}$, $B = \{1, 2, \dots, 100\}$, $C = \{2, 4, 6, \dots\}$ 。

* 在本书中,自然数集合的元素包括零。

第二, 当一个集合 A 中的元素很多或者无穷时, 则用元素特性刻划的方法来表示。如用 P 表示某种特性, $P(a)$ 表示元素 a 满足特性 P , 则

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

表示 A 是所有使 $P(a)$ 成立的元素 a 构成的集合。 P 可以是某项规定或某个公式, 例如:

$$A = \{x \mid x \in \mathbf{I} \text{ 并且 } x < 0\}$$

$$B = \{x \mid x = y^2 \text{ 并且 } y \text{ 是正整数}\}$$

$$C = \{x \mid x \text{ 是有效的 FORTRAN 标识符}\}$$

$$D = \{x \mid x \text{ 是开始为 } c, \text{ 结束为 } t \text{ 的三个字母的字}\}$$

$$= \{\text{cat}, \text{cot}, \cdots, \text{cut}\}$$

第三, 可以通过计算规则定义集合中的元素, 这种情况下的集合有的称为递归指定集合。

例 1-1 设 $a_0 = 1, a_1 = 1, a_{i+1} = a_i + a_{i-1}, i \geq 1$, 于是 $S = \{a_k \mid k \geq 0\} = \{1, 1, 2, 3, 5, 8, \cdots\}$ 。

如果一个集合的元素是有限的, 称它为有限集, 反之是无限集。我们最常见的自然数集合是无限集, 无限集将在第三章专门讨论。

设 A 是有限集, 则 A 中元素的数目用 $n(A)$ 或 $|A|$ 表示。关于集合中的元素及计算方法, 后面要作专门研究。

1.2 集合的子集

定义 1-1 设 A 和 B 是两个集合, 如果 A 中的每个元素也是 B 中的一个元素, 则称 A 是 B 的子集, 记作 $A \subseteq B$ 。 A 是 B 的子集也叫 A 被 B 包含, 或叫 B 包含 A 。

如果 A 不是 B 的子集, 即 A 中至少有一个元素不属于 B , 记作 $A \not\subseteq B$ 或 $B \not\supseteq A$ 。

定义 1-2 设 A 和 B 是两个集合, 如果 A 中的每个元素是 B 中

的一个元素,同时 B 中的每个元素也是 A 中的一个元素,则称 A 和 B 相等,记作 $A=B$ 。

如果 A 中至少有一个元素不在 B 中或者 B 中至少有一个元素不在 A 中,则称 A 和 B 不等,记作 $A \neq B$ 。

集合间的包含和相等是两个极其重要的概念,它们之间的关系可归结为下述定理。

定理 1-1 设 A 和 B 是两个集合,则 $A=B$ 当且仅当 $A \subseteq B$ 且 $B \subseteq A$ 。

证明: 假定 $A=B$,由相等的定义, A 中每个元素在 B 中,所以 $A \subseteq B$,同样 B 中每个元素在 A 中,所以 $B \subseteq A$;

反之,若 $A \neq B$,故 A 中至少有一个元素不在 B 中,这与 $A \subseteq B$ 矛盾,或者 B 中至少有一个元素不在 A 中,这与 $B \subseteq A$ 矛盾,所以 $A \neq B$ 是不可能的;

故 $A=B$ 。

定义 1-3 设 A 和 B 是两个集合,如果 $A \subseteq B$ 并且 $A \neq B$,则称 A 是 B 的真子集(或叫真包含),记以 $A \subset B$ 。

例 1-2 设集合 $A=\{1,3,4,5,8,9\}$, $B=\{1,2,3,5,7\}$, $C=\{1,5\}$,则有 $A \supset C$, $B \supset C$ 。这是因为 C 中的每个元素都在 B 和 A 中,然而 $B \not\subset A$,因为 $2,7 \in B$,但是 $2,7 \notin A$ 。

例 1-3 设 $S_1=\{a\}$, $S_2=\{\{a\}\}$,则 $S_1 \neq S_2$ 。 S_1 和 S_2 无公共元素,且每个集合仅有一个元素。再令 $S_3=\{a,\{a\}\}$,则 S_3 有两个元素。这三个集合的关系是: $S_1 \neq S_3$, $S_2 \neq S_3$,然而 $S_1 \subset S_3$, $S_2 \subset S_3$ 。

1.3 全集和空集

在这一节,我们将介绍两个特殊的集合——全集和空集。

定义 1-4 如果一个集合包含了我们所考虑的每一个元素的集合,则称该集合为全集。除非特别声明,本书用 U 表示全集。

例 1-4 设有一个方程:

$$(x+1)(2x-3)(3x+4)(x^2-2)(x^2+1)=0$$

对于这个方程,如果 U 是全体复数的集合,则其解集(即该方程根的集合)是:

$$S = \{-1, 3/2, -4/3, \sqrt{2}, -\sqrt{2}, i, -i\}$$

如果 U 是全体实数集合,则其解集是:

$$A = \{-1, 3/2, -4/3, \sqrt{2}, -\sqrt{2}\}$$

自然,当 U 是全体整数集合或自然数集合时,读者不难求出其相应的解集。

相反,如果仅仅给出某些集合,譬如说 $A = \{1, 2, 3\}$, $B = \{4, 5, 6, 7\}$, 那么我们难以知道其全集是什么,因为 U 可以是 $\{1, 2, 3, \dots, 7\}$, $\{x | x \in \mathbf{N} \text{ 且 } x < 100\}$, $\mathbf{N}$, $\mathbf{I}$, $\dots$ 。不过今后在集合的应用中,我们总认为它包含在固定大的集合之中,一般不再声明其全集是哪一个。因为读者完全可从研究的具体问题而知道其全集,例如,在平面几何中,全集是平面上的所有的点。

与全集相反的概念是空集。

定义 1-5 没有元素的集合称为空集,记以 $\emptyset$ 。

定理 1-2 设 A 是任意一个集合,则有 $\emptyset \subseteq A$ 。

证明: 用反证法。若 $\emptyset \not\subseteq A$, 由定义, $\emptyset$ 中至少有一个元素不属于 A , 这与空集 $\emptyset$ 的定义发生矛盾, 故有 $\emptyset \subseteq A$ 。

对任意一个集合 A , 总有 $\emptyset \subseteq A \subseteq U$ 。

定理 1-3 空集 $\emptyset$ 是惟一的。

证明: 用反证法。设 $\emptyset_1$ 和 $\emptyset_2$ 是两个空集, 则由于 $\emptyset_1$ 是空集, 根据定理 1-2 有 $\emptyset_1 \subseteq \emptyset_2$; 由于 $\emptyset_2$ 是空集, 根据定理 1-2 有 $\emptyset_2 \subseteq \emptyset_1$; 因此 $\emptyset_1 = \emptyset_2$ 。

注意, $\emptyset$ 和 $\{\emptyset\}$ 是不同的, 前者是没有元素的一个集合, 后者是以空集 $\emptyset$ 作为其元素的一个集合。如果 $S = \{\emptyset\}$, 则 $\emptyset \subset S$ 而且 $\emptyset \in S$; 如果 $S = \{\{\emptyset\}\}$, 则 $\emptyset \subset S$ 但是 $\emptyset \notin S$ 。

1.4 集合的运算、文氏图

定义 1-6 设 A 和 B 是两个集合,则:

(1) A 和 B 的并,记为 $A \cup B$,是由 A 和 B 中的所有元素构成的集合,即:

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

(2) A 和 B 的交,记为 $A \cap B$,是由 A 和 B 中的所有公共元素构成的集合,即:

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

特殊情况:如果 A 和 B 无公共元素,此时 $A \cap B = \emptyset$,称 A 和 B 是分离的。

(3) A 和 B 的差,记为 $A - B$,是由属于 A 而不属于 B 的元素构成的集合,即:

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

定义 1-7 一个集合 A 的补,记为 $\bar{A}$,它是由属于全集 U 但不属于 A 的所有元素构成的集合,即:

$$\bar{A} = \{x \mid x \in U \text{ 并且 } x \notin A\}$$

所以 $\bar{A}$ 是全集 U 和 A 的差集。

对任意两个集合 A 和 B ,有 $A - B = A \cap \bar{B}$ 。

例 1-5 设 $A = \{1, 2, 3, 5\}$, $B = \{1, 2, 4, 6\}$, $U = N$ (N 为自然数集),求 A 和 B 的并集、交集、差集和 $\bar{A}$ 、 $\bar{B}$ 。

解: $A \cup B = \{1, 2, 3, 4, 5, 6\}$

$$A \cap B = \{1, 2\}$$

$$A - B = \{3, 5\}$$

$$B - A = \{4, 6\}$$

$$\bar{A} = \{0, 4, 6, 7, \dots\}$$

$$\bar{B} = \{0, 3, 5, 7, 8, \dots\}$$

集合的运算满足一些基本定律,为便于比较,列表如下:

等 幂 律	
$A \cup A = A$	$A \cap A = A$
结 合 律	
$(A \cup B) \cup C = A \cup (B \cup C)$	$(A \cap B) \cap C = A \cap (B \cap C)$
交 换 律	
$A \cup B = B \cup A$	$A \cap B = B \cap A$
分 配 律	
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
恒 等 律	
$A \cup \emptyset = A$	$A \cap U = A$
$A \cup U = U$	$A \cap \emptyset = \emptyset$
吸 收 律	
$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
双 重 补	
$\overline{\overline{A}} = A$	
取 补 律	
$A \cup \overline{A} = U$	$A \cap \overline{A} = \emptyset$
$\overline{\overline{U}} = \emptyset$	$\overline{\emptyset} = U$
德 • 摩根定律	
$\overline{(A \cup B)} = \overline{A} \cap \overline{B}$	$\overline{(A \cap B)} = \overline{A} \cup \overline{B}$

如果在一个表达式中同时具有取补、交和并的运算,其运算的优先次序是先作取补运算,再作交的运算,最后作并的运算,若表达式中有括号,则先作内层括号中的运算。利用补、交及并的优先次序,可减少表达式中括号的层数。

下面我们利用前述的一些定义及基本定律来证明一些常用的关系式,通过这些证明,读者将会掌握基本的解题方法。

例 1-6

(1) 如果 $A \subseteq B, C \subseteq D$,则有:

$$(A \cup C) \subseteq (B \cup D), (A \cap C) \subseteq (B \cap D)。$$

证明: 任取 $x \in (A \cup C)$, 于是 $x \in A$ 或 $x \in C$, 由于 $A \subseteq B, C \subseteq D$, 故 $x \in B$ 或 $x \in D$, 从而有 $x \in (B \cup D)$, 所以 $(A \cup C) \subseteq (B \cup D)$ 。

同理可证 $(A \cap C) \subseteq (B \cap D)$ 。

(2) 求证 $(A \cap B) \subseteq A \subseteq (A \cup B)$
 $(A \cap B) \subseteq B \subseteq (A \cup B)。$

证明：任取 $x \in (A \cap B)$ ，则 $x \in A$ 成立，因此 $(A \cap B) \subseteq A$ ；另一方面，任取 $x \in A$ ，则 $x \in (A \cup B)$ 肯定成立，因此 $A \subseteq (A \cup B)$ ，故有：

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

同理可证 $(A \cap B) \subseteq B \subseteq (A \cup B)$ 。

(3) 如果 $A \subseteq B$ ，则有 $(A \cap B) = A$ ， $(A \cup B) = B$ 。

证明：假定 $A \subseteq B$ ，任取 $x \in A$ ，于是 $x \in B$ ，因此 $x \in (A \cap B)$ ，得到 $A \subseteq (A \cap B)$ ；另一方面， $(A \cap B) \subseteq A$ 。所以 $(A \cap B) = A$ 。

任取 $x \in (A \cup B)$ ，于是 $x \in A$ 或 $x \in B$ ，如果 $x \in A$ ，由于 $A \subseteq B$ ，则有 $x \in B$ ，所以 $(A \cup B) \subseteq B$ ；另一方面 $(A \cup B) \supseteq B$ ，故 $(A \cup B) = B$ 。

(4) 求证 $(A - B) \subseteq A$ 。

证明： $A - B = A \cap \bar{B} \subseteq A$ (由(2))

例 1-7 求证 $A - (A - B) = A \cap B$

证明： $A - (A - B) = A - (A \cap \bar{B}) = A \cap \overline{(A \cap \bar{B})}$
 $= A \cap (\bar{A} \cup \bar{\bar{B}}) = (A \cap \bar{A}) \cup (A \cap B) = \emptyset \cup (A \cap B)$
 $= A \cap B$

例 1-8 求证 $(A \cap B) \cup C = A \cap (B \cup C)$ 当且仅当 $C \subseteq A$ 。

证明：设 $(A \cap B) \cup C = A \cap (B \cup C)$ ，由于 $C \subseteq (A \cap B) \cup C$ ， $A \cap (B \cup C) \subseteq A$ ，故 $C \subseteq A$ ；

反之，如果 $C \subseteq A$ ，则 $A \cup C = A$ ，故 $(A \cap B) \cup C = (A \cup C) \cap (B \cup C) = A \cap (B \cup C)$ 。

例 1-9 求证 $A - (B - C) = (A - B) - C$ 当且仅当 $A \cap C = \emptyset$ 。

证明：先设 $A - (B - C) = (A - B) - C$ ，于是有：

$$\begin{aligned} A - (B - C) &= A - (B \cap \bar{C}) = A \cap \overline{(B \cap \bar{C})} \\ &= A \cap (\bar{B} \cup C) = (A \cap \bar{B}) \cup (A \cap C) \\ &= A \cap \bar{B} \cap (C \cup \bar{C}) \cup A \cap (B \cup \bar{B}) \cap C \\ &= (A \cap B \cap C) \cup (A \cap \bar{B} \cap C) \cup (A \cap \bar{B} \cap \bar{C}) \\ &= (A - B) - C = A \cap \bar{B} \cap \bar{C} \quad (\text{右端}) \end{aligned}$$

由于 $A \cap B \cap C$ 、 $A \cap \bar{B} \cap C$ 、 $A \cap \bar{B} \cap \bar{C}$ 是两两分离的(为什么?)，故 $(A \cap B \cap C) \cup (A \cap \bar{B} \cap C) = \emptyset$ ，但是 $(A \cap B \cap C) \cup (A \cap \bar{B} \cap C) = A \cap$

C , 所以 $A \cap C = \emptyset$ 。

充分性的证明从略。

两个集合 A 和 B 之差是不满足结合律和交换律的, 我们引进另外一种运算称为对称差。

定义 1-8 集合 A 和 B 的对称差, 记以 $A \oplus B$, 是:

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

即:

$$A \oplus B = \{x \mid x \in A \text{ 且 } x \notin B \text{ 或 } x \in B \text{ 且 } x \notin A\}$$

对称差的元素属于 A 或 B , 但不能同时属于 A 和 B 。

定理 1-4 下面的等式是成立的:

- (1) $A \oplus (B \oplus C) = (A \oplus B) \oplus C$
- (2) $A \oplus B = B \oplus A$
- (3) $A \oplus \emptyset = A$
- (4) $A \oplus A = \emptyset$
- (5) $A \oplus U = \bar{A}$ (其中 U 是全集)
- (6) $A \oplus \bar{A} = U$
- (7) $A \oplus B = (A \cup B) - (A \cap B)$
- (8) $A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$

证明: 我们仅对(8)作证明如下:

$$\begin{aligned} & (A \cap B) \oplus (A \cap C) \\ &= ((A \cap B) - (A \cap C)) \cup ((A \cap C) - (A \cap B)) \\ &= (A \cap B) \cap \overline{(A \cap C)} \cup \overline{(A \cap B)} \cap (A \cap C) \\ &= A \cap B \cap \bar{A} \cup A \cap B \cap \bar{C} \cup \bar{A} \cap A \cap C \cup A \cap \bar{B} \cap C \\ &= (A \cap \bar{A}) \cap B \cup A \cap B \cap \bar{C} \cup A \cap \bar{B} \cap C \\ &= \emptyset \cap B \cup A \cap B \cap \bar{C} \cup A \cap \bar{B} \cap C \\ &= A \cap B \cap \bar{C} \cup A \cap \bar{B} \cap C \\ &= A \cap (B \cap \bar{C} \cup \bar{B} \cap C) \\ &= A \cap ((B - C) \cup (C - B)) \\ &= A \cap (B \oplus C) \end{aligned}$$

下面为叙述简单,有时用记号“甲 $\Rightarrow$ 乙”表示由甲能推出乙。

例 1-10 假定 $A \oplus B = A \oplus C$, 则有 $B = C$ 。

证明: 欲证 $B = C$, 只须证 $B \subseteq C$ 且 $B \supseteq C$ 。

(1) 任取 $x \in B$, 此时若 $x \in A$, 则:

$$\begin{aligned} & x \in A \cap B \\ & \Rightarrow x \notin A \oplus B \text{ (由对称差定义导出)} \\ & \Rightarrow x \notin A \oplus C \text{ (由 } A \oplus B = A \oplus C \text{)} \\ & \Rightarrow x \in A \cap C \text{ (由对称差定义导出)} \\ & \Rightarrow x \in C \end{aligned}$$

任取 $x \in B$, 此时若 $x \notin A$, 则:

$$\begin{aligned} & x \notin A \cap B \\ & \Rightarrow x \in A \oplus B \text{ (由对称差定义导出)} \\ & \Rightarrow x \in A \oplus C \text{ (由 } A \oplus B = A \oplus C \text{)} \\ & \Rightarrow x \in A \cap \bar{C} \text{ 或 } x \in \bar{A} \cap C \\ & \Rightarrow x \in \bar{A} \cap C \text{ (} x \in A \cap \bar{C} \text{ 不成立)} \\ & \Rightarrow x \in C \end{aligned}$$

所以, 对任意 $x \in B$, 不管 x 是否属于 A , 总有 $x \in C$, 故 $B \subseteq C$ 。

(2) 任取 $x \in C$, 按同样的方法, 可证明:

$$B \supseteq C, \text{ 所以 } B = C.$$

集合的幂集是一个很重要的概念。

定义 1-9 设 S 是一个有限集合, 则 S 的所有子集所组成的集合称为 S 的幂集, 用 $\rho(S)$ 或 2^S 表示, 即:

$$\rho(S) = \{X \mid X \subseteq S\}$$

例 1-11 设 $S = \{1, 2, 3\}$, 则:

$$\rho(S) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, S\}$$

对于空集 $\emptyset$, 其幂集为: $\rho(\emptyset) = \{\emptyset\}$

还有: $\rho(\rho(\emptyset)) = \{\emptyset, \{\emptyset\}\}$

$$\rho(\rho(\rho(\emptyset))) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$$

可以很容易证明, 如果 S 有 k 个元素, 则 $\rho(S)$ 有 2^k 个元素。

例 1-12 设 A 和 B 是两个集合, 则:

$$(1) \rho(A) \cup \rho(B) \subseteq \rho(A \cup B)$$

$$(2) \rho(A) \cap \rho(B) = \rho(A \cap B)$$

证明: (1) 任取 $X \in (\rho(A) \cup \rho(B))$

$$\Rightarrow X \in \rho(A) \text{ 或 } X \in \rho(B)$$

$$\Rightarrow X \subseteq A \text{ 或 } X \subseteq B$$

$$\Rightarrow X \subseteq (A \cup B)$$

$$\Rightarrow X \in \rho(A \cup B)$$

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

(2) 任取 $X \in \rho(A) \cap \rho(B)$

$$\Rightarrow X \in \rho(A) \text{ 且 } X \in \rho(B)$$

$$\Rightarrow X \subseteq A \text{ 且 } X \subseteq B$$

$$\Rightarrow X \subseteq (A \cap B)$$

$$\Rightarrow X \in \rho(A \cap B)$$

故: $\rho(A) \cap \rho(B) \subseteq \rho(A \cap B)$

反之, 任取 $X \in \rho(A \cap B) \Rightarrow X \subseteq (A \cap B)$

$$\Rightarrow X \subseteq A \text{ 且 } X \subseteq B$$

$$\Rightarrow X \in \rho(A) \text{ 且 } X \in \rho(B)$$

$$\Rightarrow X \in (\rho(A) \cap \rho(B))$$

故: $\rho(A) \cap \rho(B) \supseteq \rho(A \cap B)$

所以: $\rho(A) \cap \rho(B) = \rho(A \cap B)$

一般情况下, $\rho(A) \cup \rho(B) \neq \rho(A \cup B)$, 我们举例说明如下:

$$A = \{a\}, B = \{b\}, A \cup B = \{a, b\}$$

$$\rho(A) \cup \rho(B) = \{\emptyset, \{a\}, \{b\}\}$$

$$\rho(A \cup B) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$$

故: $\rho(A) \cup \rho(B) \neq \rho(A \cup B)$

研究集合运算时, 文氏图是一种有用的直观形象工具。文氏图是集合的一种图形表示, 在平面上用矩形表示全集 U , 矩形内的一个圆表示某一个集合, 属于某集合的元素在圆内, 不属于的在圆外。对

于一个集合、两个集合和三个集合的文氏图分别表示在图 1-1 中。

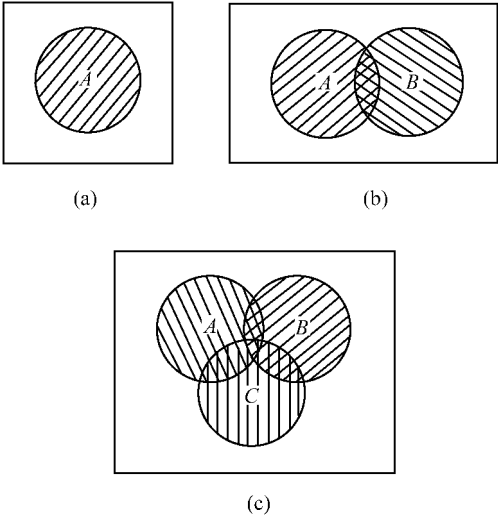


图 1-1 文氏图实例之一

于是 $(A \cup B)$ 、 $(A \cap B)$ 、 $(A - B)$ 、 $\overline{A}$ 、 $(A \oplus B)$ 、 $(A \cap B) = \emptyset$ 的文氏图见图 1-2。

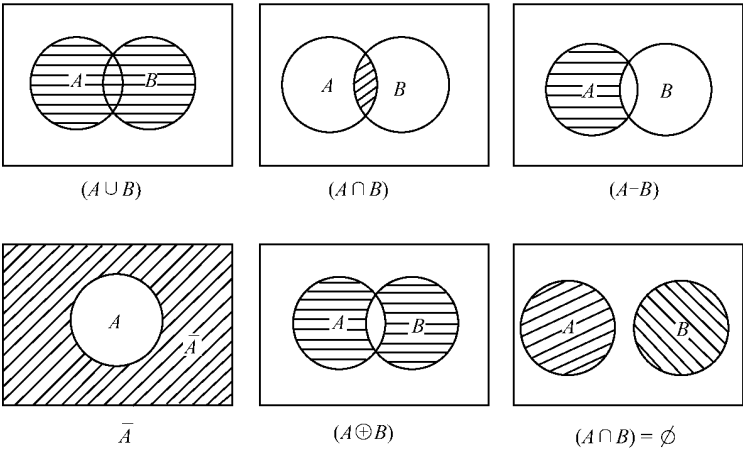


图 1-2 文氏图实例之二

例 1-13 若 $A \cup B = A \cup C$, 是否必有 $B = C$? 若 $A \cap B = A \cap C$, 是否必有 $B = C$?

解: 均不一定, 可用文氏图说明如下, 见图 1-3。

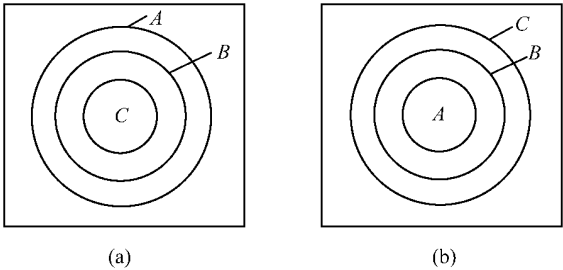


图 1-3 例 1-13 文氏图说明

由图 1-3(a), $A \cup B = A \cup C$, 但 $B \neq C$;
 由图 1-3(b), $A \cap B = A \cap C$, 但 $B \neq C$ 。
 利用文氏图的方法也可证明一些较复杂的关系式。

例 1-14 求证 $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

证明: 比较图 1-4(c) 和 (f), 发现其阴影部分完全相同, 所以有:

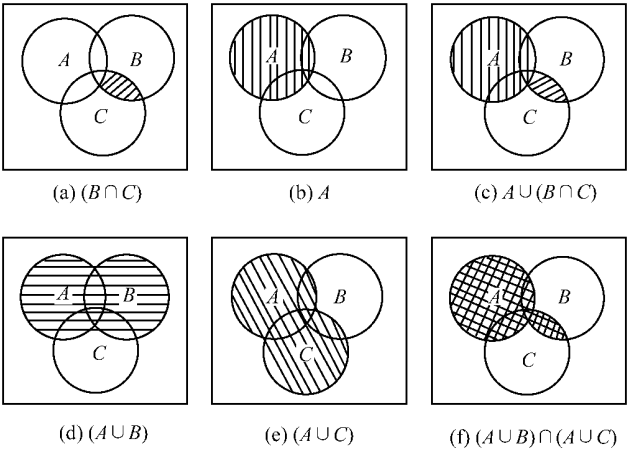


图 1-4 例 1-14 文氏图说明

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

用同样的方法,可以证明:

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

1.5 有限集合中的元素数目

在本章 1.4 中,我们已经知道,如果集合 S 有 2 个元素或 3 个元素,则其幂集的元素有 $2^2=4$ 和 $2^3=8$ 个,一般有如下结论:

定理 1-5 如果集合 S 具有 n 个元素,则 $\rho(S)$ 有 2^n 个元素,即 $|\rho(S)|=2^n$ 。

证明: 因为 $|S|=n$,由组合理论,从 n 个元素选取 i 个不同元素的组合数是

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

由 1 个元素构成的 S 的子集有 C_n^1 个,

由 2 个元素构成的 S 的子集有 C_n^2 个,

.....

由 n 个元素构成的 S 的子集有 C_n^n 个。

此外还有一个空集 $\emptyset$,故 S 的全体子集数是:

$$|\rho(S)| = 1 + C_n^1 + C_n^2 + \cdots + C_n^n$$

由二项式定理:

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

令 $x=y=1$,所以有:

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

因此:

$$|\rho(S)| = 2^n$$

由于 $2^n > n$ (当 $n > 0$),所以我们马上得出结论:任何一个有限集,其幂集的元素总比该集合的元素多,或者说一个集合的幂集总比该集合大,即 $|\rho(S)| > |S|$ 。

例 1-15 设 $n=0$, 则 $S=\emptyset, \rho(S)=\{\emptyset\}$,

$$|\rho(S)|=2^0-1;$$

若 $n=1, S=\{a\}$, 则 $\rho(S)=\{\emptyset, \{a\}\}$,

$$|\rho(S)|=2^1=2$$

下面, 我们讨论并集中的元素数目的计算规则。

定理 1-6 如果 A 和 B 是分离的有限集合, 则有:

$$|A \cup B| = |A| + |B|$$

其中“+”是普通的算术加。

证明: 在计算 $(A \cup B)$ 中元素时, 先计算 A 中的元素, 计有 $|A|$ 个。再计算 $(A \cup B)$ 中的其余元素。不在 A 中的其余元素在 B 中, 而且由于 A 和 B 是分离的, B 中也没有元素在 A 中, 所以有 $|B|$ 个不在 A 中的元素在 B 中; 因此

$$|A \cup B| = |A| + |B|$$

当 A 和 B 不分离时, $|A \cup B|$ 的公式如下:

定理 1-7 如果 A 和 B 是有限集合, 则有:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

其中“-”是普通的算术减。

证明: 当 A 和 B 是有限集合时, 显然 $(A \cup B)$ 和 $(A \cap B)$ 是有限的。 $A \cup B = B - (A - B)$, 而 B 和 $(A - B)$ 是分离的, 据定理 1-6, 有

$$|A \cup B| = |B| + |A - B|$$

另一方面, $A = (A - B) \cup (A \cap B)$ 且 $(A - B)$ 和 $(A \cap B)$ 是分离的, 据定理 1-6, 有

$$|A| = |A - B| + |A \cap B|$$

故有

$$|A \cup B| = |A| + |B| - |A \cap B|$$

这一定理的证明, 如果直接采用文氏图的知识来推导, 就显得很简单, 见图 1-5。由图 1-5 可得

$$|A \cup B| = |S_1| + |S_2| + |S_3|$$

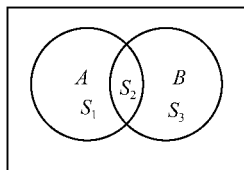


图 1-5 定理 1-5 文氏图说明

$$= (|S_1| + |S_2|) + (|S_2| + |S_3|) - |S_2|$$

$$= |A| + |B| - |A \cap B|$$

通过对定理 1-7 的两种证明方法进行比较,读者可发现:当集合数目较少时充分利用文氏图这种直观概念来研究问题有时会带来一定的方便。

定理 1-8 对任意三个有限集合 A, B, C 有:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B|$$

$$- |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

证明: 因为 $A \cup B \cup C = (A \cup B) \cup C$, 由前述定理:

$$|A \cup B \cup C| = |A \cup B| + |C| - |(A \cup B) \cap C|$$

$$= |A| + |B| - |A \cap B| + |C| - |(A \cap C) \cup (B \cap C)|$$

$$= |A| + |B| + |C| - |A \cap B| - |A \cap C|$$

$$- |B \cap C| + |(A \cap C) \cap (B \cap C)|$$

$$= |A| + |B| + |C| - |A \cap B| - |A \cap C|$$

$$- |B \cap C| + |A \cap B \cap C|$$

最后一步利用了公式 $(A \cap B) \cap (B \cap C) = A \cap B \cap C$ 。

例 1-16 假定有 120 个学生,其中 100 个学生至少要学法、德、英三种语言的一种;还假定 65 人学法语,45 人学德语,42 人学英语;20 人学法语和德语,25 人学法语和英语,15 人学德语和英语。问同时学三种语言的有多少人?仅学一种语言的各有多少人?

解: 令 A, B, C 分别表示学法语、德语和英语的学生的集合,于是:

$$|A \cup B \cup C| = |A| + |B| + |C|$$

$$- |A \cap B| - |A \cap C|$$

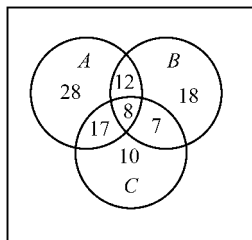
$$- |B \cap C| + |A \cap B \cap C|$$

$$100 = 65 + 45 + 42 - 20 - 25 - 15$$

$$+ |A \cap B \cap C|$$

$$|A \cap B \cap C| = 8$$

即有 8 人学三种语言。



把这结果填在文氏图 1-6 上。由图

图 1-6 例 1-16 文氏图说明

1-6 可直接得到:28 人仅学法语,18 人仅学德语,10 人仅学英语,12 人仅学法语和德语而不学英语,17 人仅学法语和英语而不学德语,7 人仅学德语和英语而不学法语。

习 题 一

1.1 列出下列集合的元素:

- (1) $\{q | q \in Q, q^2 - 1 = 15 \text{ 而且 } q^3 = 60\}$
 (2) $\{r | r \in R, r^2 + r - 6 = 0\}$
 (3) $\{i | i \in I, i^2 - 10i - 24 < 0 \text{ 且 } 5 \leq i \leq 15\}$

1.2 求下列集合的幂集:

- (1) $\{\emptyset, a, \{a\}\}$ (2) $A = \{1, 2, 3, 4\}$

1.3 判定下列各题是否成立?

- (1) $\{a\} \in \{\{a\}\}$ (2) $\{a\} \subseteq \{\{a\}\}$
 (3) $\{a\} \in \{\{a\}, a\}$ (4) $\{a\} \subseteq \{\{a\}, a\}$

1.4 证明下面集合是存在的:

- (1) $A = \{S | S \text{ 是一个集合}\}$
 (2) $A = \{S | S \text{ 是一个集合并且 } S \notin S\}$

1.5 证明定理 1-4 的其余部分。

1.6 设 A, B, C 是任意集合,问:

- (1) 如果 $A \in B, B \in C$, 则 $A \in C$ 吗? 试举例说明。
 (2) 如果 $A \in B, B \subseteq C$, 则 $A \in C$ 吗? 试证明之。
 (3) 如果 $A \in B, B \subseteq C$, 则 $A \subseteq C$ 吗?
 (4) 如果 $A \subseteq B, B \subseteq C$, 则 $A \in C$ 吗? $A \subseteq C$ 吗?
 (5) 若 $A \cap B = A \cap C, \bar{A} \cap B = \bar{A} \cap C$, 证明 $B = C$ 。
 (6) 若 $A \cap C \subseteq B \cap C, A \cap \bar{C} \subseteq B \cap \bar{C}$, 证明 $A \subseteq B$ 。
 (7) $A \subseteq B$ 和 $A \in B$ 是否会同时成立?

1.7 设 A, B, C 是任意集合,问下列等式成立的条件是什么?

- (1) $(A - B) \cup (A - C) = A$

$$(2) (A-B) \cup (A-C) = \emptyset$$

$$(3) (A-B) \cap (A-C) = \emptyset$$

$$(4) (A-B) \oplus (A-C) = \emptyset$$

1.8 设 I 的子集如下:

$$A = \{1, 2, 7, 8\}, B = \{i \mid i^2 \leq 50\}$$

$$C = \{i \mid i \text{ 整除 } 30\}, D = \{i \mid i = 2^k, k \in I, 0 \leq k \leq 6\}$$

求下列集合:

$$(1) A \cup (B \cup (C \cup D))$$

$$(2) A \cap (B \cap (C \cap D))$$

$$(3) B - (A \cup C)$$

$$(4) (\bar{A} \cap B) \cup D$$

1.9 已知 N 的子集如下:

$$A = \{n \mid n < 12\} \quad B = \{n \mid n \leq 8\}$$

$$C = \{n \mid n = 2k, k \in N\} \quad D = \{n \mid n = 3k, k \in N\}$$

$$E = \{n \mid n = 2k - 1, k \in N\}$$

用 A, B, C, D, E 表示下列集合:

$$(1) \{2, 4, 6, 8\}$$

$$(2) \{3, 6, 9\}$$

$$(3) \{10\}$$

$$(4) \{n \mid n \text{ 为偶数}, n > 10\}$$

$$(5) \{n \mid n = 3 \text{ 或 } n = 6 \text{ 或 } n = 9\}$$

$$(6) \{n \mid n \text{ 是偶数且 } n \leq 10, \text{ 或 } n \text{ 是奇数且 } n > 9\}$$

1.10 设 A, B, C 是 U 的子集, 利用文氏图证明下列等式:

$$(1) \overline{(A \cup B)} \cup C = \bar{A} \cap \bar{B} \cup C$$

$$(2) A - (B \cup C) = (A - B) \cap (A - C)$$

1.11 在 60 个人的调查中, 有 25 人读《人民日报》, 26 人读《体育报》, 26 人读《光明日报》, 9 人同时读《人民日报》和《光明日报》, 11 人同时读《人民日报》和《体育报》, 8 人同时读《体育报》和《光明日报》, 8 人不读任何报纸。求:

(1) 同时读三种报纸的人数。

(2) 恰好只读一种报纸的人数。

1.12 下列哪一条可称为集合? ()

A. 某本书中第 a 页上汉字的全体

B. 很大数的全体

C. 高个子全体

D. 接近于 0 的数的全体

1.13 下列四式中,错误的是()

A. $\emptyset \subseteq \emptyset$ B. $\emptyset \neq 0$ C. $\emptyset \subseteq \{0\}$ D. $\emptyset \in \emptyset$

1.14 列举集合的元素 $A = \{x | x^2 < 50, x \text{ 为正奇数}\} =$ _____;

$B = \{x | x = p/q, p+q=5, p, q \in \text{自然数}\} =$ _____。

1.15 集体 A 和 B 的对称差记为 $A \oplus B, A \oplus B =$ _____;
 $A \oplus \emptyset$ _____。

1.16 对集合 A, B 若 $A \subseteq B$, 则有 $(A \cap B) = A, (A \cup B) = B$ 。
试证明之。

1.17 指出下列错误的等式()

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

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

1.18 N_1 为偶数集合, N_2 为奇数集合, N_3 为质数集合, 则有
 $N_1 \cap N_2 =$ _____; $N_1 \cap N_3 =$ _____。

1.19 化简 $(A - B - C) \cup ((A - B) \cap C) \cup (A \cap B - C) \cup (A \cap B \cap C)$

1.20 指出下列错误的式子()

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

C. $A \oplus A = \emptyset$ D. $A \cap (B \oplus C) \neq (A \cap B) \oplus (A \cap C)$

1.21 设 E 为全集, A, B 为非空集且 $B \subset A$, 则空集为()

A. $A \cap B$ B. $\bar{A} \cap \bar{B}$ C. $\bar{A} \cap B$ D. $A \cap \bar{B}$

1.22 求证 $A - (A - B) = A \cap B$ 。

1.23 $A = \{1, 2, 3, \{1, 2\}, \{3\}\}, B = \{2, \{2, 3\}, \{1\}\}$, 则 $A - B =$ _____; $B - A =$ _____。

1.24 $A = \{2, 3\}, B = \{1, 4, 7\}, C = \{3, 5\}$ $A \cup (B \oplus C) =$ _____;
 $(A \cup B) \oplus (A \cup C) =$ _____。

1.25 已知 $A \subseteq B$ 且 $A \in B$, 下列结论哪个对?()

- A. 是不可能的 B. 是可能的
C. A 必须是空集 D. B 必须是全集

1.26 集合 $\{0\}$ 的所有子集是()

- A. $\emptyset$ B. $\emptyset, \{0\}$ C. $\{\emptyset\}$ D. $\{\emptyset, \{0\}\}$

1.27 用列举法表示以下集合的元素:

$$A = \{x \mid 3 < x < 4, x \in I\} = \underline{\hspace{2cm}}; (I \text{ 为整数集})$$

$$B = \{x \mid x^2 = 1, x \in I\} = \underline{\hspace{2cm}}.$$

1.28 请用 $\in, \subset, \subseteq$ 填下列空格:

$$\{a\} \underline{\hspace{1cm}} \{\{a\}, 3, 4, 1\};$$

$$\{a, 4, \{3\}\} \underline{\hspace{1cm}} \{2, a, \{3\}, 4\};$$

$$\{\{a\}\} \underline{\hspace{1cm}} \{\{a\}, 3, 4, 1\}.$$

1.29 化简 $((A \cup B \cup C) \cap (A \cup B)) - ((A \cup (B - C)) \cap A)$ 。

“集合论”复习提纲

1. 主要内容

- 集合的基本概念。
- 集合运算。
- 有限集及其元素计数。

2. 复习重点

- 了解集合论的基本思想与基本运算规则。
- 了解各种不同集合:如空集 $\emptyset$ 、全集 U 、幂集 $\rho(A)$ 等。

3. 集合的基本概念

- 集合:是一些研究对象的全体。
- 元素:组成集合的对象。
- 集合与元素间的关系: $a \in S, a \notin S$ 。

——集合的三种表示方法：列举法、特性刻画法及递归表示法。

——集合的子集：集合 A 中的元素都是集合 B 中的元素则称 A 是 B 的子集，记以 $A \subseteq B$ 。

——三种不同的子集：子集： $A \subseteq B$ ；真子集： $A \subset B$ 及集合相等： $A = B$ 。

——空集：没有元素的集合，记以 $\emptyset$ 。

——全集：包含所有考虑元素的集合，记以 U 。

——幂集：集合 A 的所有子集的集合，记以 $\rho(A)$ 。

4. 集合运算

——集合的五种运算

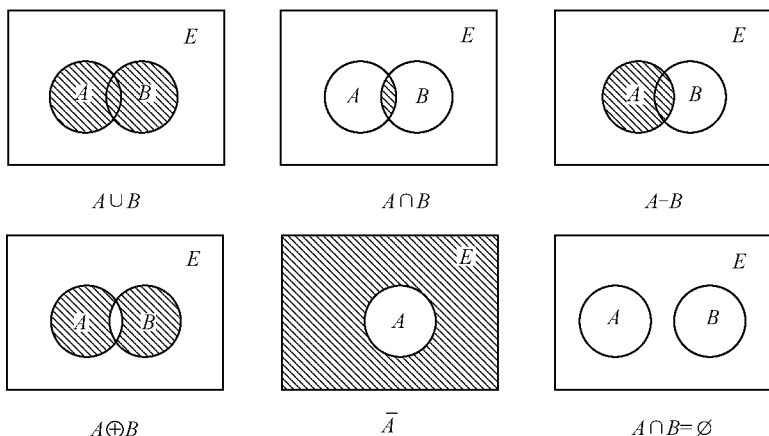
- 集合并运算： $A \cup B$ 。
- 集合交运算： $A \cap B$ 。
- 集合差运算： $A - B$ 。
- 集合对称差运算： $A \oplus B$ 。
- 集合补运算： $\bar{A}$ 。

——集合并、交、补的 21 个运算公式：

- 等幂律： $A \cup A = A$
 $A \cap A = A$
- 结合律： $(A \cup B) \cup C = A \cup (B \cup C)$
 $(A \cap B) \cap C = A \cap (B \cap C)$
- 交换律： $A \cup B = B \cup A$
 $A \cap B = B \cap A$
- 分配律： $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- 恒等律： $A \cup \emptyset = A$ $A \cap U = A$
 $A \cup U = U$ $A \cap \emptyset = \emptyset$
- 吸收律： $A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$
- 双重补： $\bar{\bar{A}} = A$

- 取补律: $A \cup \bar{A} = U$ $A \cap \bar{A} = \emptyset$ $\bar{\bar{U}} = \emptyset$ $\overline{\emptyset} = U$
- 德·摩根定律: $\overline{(A \cup B)} = \bar{A} \cap \bar{B}$ $\overline{(A \cap B)} = \bar{A} \cup \bar{B}$

——集合运算的文氏图表示:



5. 有限集及其元素计数

——有限集: 集合元素个数为有限。

——无限集: 集合元素个数为无限。

——集合基数: 集合元素个数称集合基数(或势)记以 $|A|$ 。

——有限集元素计数的三种方法:

- 如 A 与 B 分离, 则有: $|A \cup B| = |A| + |B|$ 。
- $|A \cup B| = |A| + |B| - |A \cap B|$ 。
- $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |A \cap B \cap C|$ 。

第二章 关 系

2.1 关系的基本概念

我们首先引入元素的有序偶 (a, b) 概念,其中 a 是第一个元素, b 是第二个元素,通常 $(a, b) \neq (b, a)$,除非 $a = b$ 。下面给出它的定义。

定义 2-1 两个元素 a 和 b 的有序偶是两个元素的序列,用 (a, b) 表示。其中 a 称为有序偶的第一分量, b 称为第二分量。两个有序偶 (a, b) 、 (c, d) 相等即 $(a, b) = (c, d)$ 当且仅当它们的对应分量分别相等即 $a = c$ 且 $b = d$ 。

定义 2-2 设 A 和 B 是两个集合, A 到 B 的笛卡尔乘积 $A \times B$ 是

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

即 A 到 B 的笛卡尔乘积是所有有序偶的集合,其中有序偶的第一个分量属于 A ,第二个分量属于 B 。

例 2-1 令 $A = \{1, 2\}$, $B = \{p, q\}$, $C = \{a, b, c\}$, $D = \emptyset$, 则:

$$A \times B = \{(1, p), (1, q), (2, p), (2, q)\};$$

$$A \times C = \{(1, a), (2, a), (1, b), (2, b), (1, c), (2, c)\};$$

$$A \times D = \emptyset。$$

有了有序偶和笛卡尔乘积的概念,我们可以讨论关系了。

定义 2-3 设 A 和 B 是两个集合,从 A 到 B 的一个二元关系 R 就是 $A \times B$ 的一个子集,即:

$$R \subseteq A \times B$$

如果 $R = A \times B$,称 R 是 A 到 B 的全关系,如果 $R = \emptyset$,称 R 是空关系。如果 $A = B$,便说 R 是 A (或 B)上的关系,自然, $R = A \times A$ 称为 A 上的全关系。为方便起见, $A \times A$ 有时记为 A^2 。

通常,如果两个元素的有序偶 $(x,y)\in R$,便称 x 与 y 具有关系 R ,亦可用 xRy 表示,反之如果 $(x,y)\notin R$,便称 x 与 y 不具有关系 R ,亦可用 $x\not Ry$ 表示。

一个二元关系 R 的定义域是 R 中有序偶的第一个元素构成的集合,用 $D(R)$ 表示;值域是 R 中有序偶的第二个元素构成的集合,用 $V(R)$ 表示。 A 称为 R 的前域, B 称为 R 的陪域。一般情况 $D(R)\subseteq A,V(R)\subseteq B$ 。

图 2-1 是从 A 到 B 的一个关系 R 的图形表示,从 $a_i\in A$ 到 $b_i\in B$ 存在一个箭头当且仅当 $(a_i,b_j)\in R$ 。

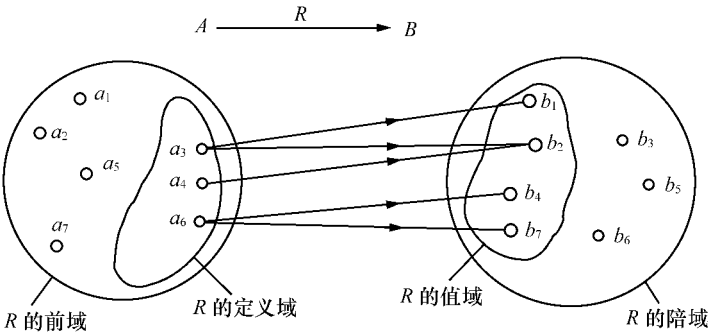


图 2-1 从 A 到 B 的关系 R 图示

$$\begin{aligned}
 R &= \{(a_3,b_1),(a_3,b_2),(a_4,b_2),(a_6,b_4), \\
 &\quad (a_6,b_7)\} \subset A \times B \\
 D(R) &= \{a_3,a_4,a_6\} \\
 V(R) &= \{b_1,b_2,b_4,b_7\}
 \end{aligned}$$

例 2-2 令 $A=\{1,2,3\},R=\{(1,2),(1,3),(3,2)\}$,则 R 是 A 上的一个关系,因为 $R\subseteq A\times A$ 。对这种关系, $1R2,1R3,3R2,1R1,2R1,2R2,2R3,3R1,3R3$ 。

R 的定义域是 $\{1,3\}$,值域是 $\{2,3\}$ 。

例 2-3 整数集 I 上的“ m 整除 n ”是一个关系,习惯写成 $m|n$,例如 $6|30$ 。

设集合 A 上的关系满足：

$$E = \{(a_i, a_i) \mid a_i \in A\}$$

则称 E 是 A 上的恒等关系。如 $A = \{0, 1, 2\}$ ，则：

$$E = \{(0, 0), (1, 1), (2, 2)\}$$

如果把有序偶 (a, b) 推广到 n 元有序组 $(a_1, a_2, \dots, a_n) (n > 2)$ ，其中 a_i 称 n 元有序组的第 i 个元素，就可以定义 n 个集合的笛卡尔乘积和 n 元关系。

定义 2-4 设 $A_1, A_2, \dots, A_n$ 是 n 个集合，则 $A_1, A_2, \dots, A_n$ 的笛卡尔乘积（记以 $A_1 \times A_2 \times \dots \times A_n$ ）是：

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_i \in A_i, \\ i = 1, 2, \dots, n\}$$

若 R 是 $A_1 \times A_2 \times \dots \times A_n$ 的任意一个子集，即：

$$R \subseteq A_1 \times A_2 \times \dots \times A_n$$

则称 R 是 $A_1, A_2, \dots, A_n$ 的一个 n 元关系。

为方便起见， $A_1 \times A_2 \times \dots \times A_n$ 可简记为 $\prod_{i=1}^n A_i$ ，当各个 A 都为同一集合 A 时，简记为 A^n 。

我们经常要用到 n 元关系，如在数据库的关系模型中，常用它来描述数据间的关系。

例 2-4 课程表关系 R_1 如表 2-1 所示：

表 2-1 课程表关系 R_1

课 程 号	节 数	教 师	课 程 名 称
CS105	10	A	计算机科学
CS105	20	B	计算机科学
CS105	30	C	计算机科学
CS170	10	D	数 学
CS170	20	E	数 学
CS240	10	F	离 散 结 构
CS240	20	G	离 散 结 构

其中每一行是这关系 R_1 中的一个元素,行的次序是不重要的。

注意,用表格方法来表示关系也是经常采用的。在数据库、数据结构等学科中常用此法定义一个关系。这在第九章中要进一步介绍。

2.2 关系的性质

二元关系的性质在以下各节中起特别重要的作用,现在定义如下:

- 定义 2-5 设 R 是 A 上的一个关系,即 $R \subseteq A \times A$,于是,若:
- (1) 对每个 $x \in A$,有 $(x, x) \in R$,则称 R 是 A 上的自反关系。
 - (2) 对每个 $x \in A$,有 $(x, x) \notin R$,则称 R 是 A 上的非自反关系。
 - (3) 对每个 $x, y \in A$,如果 $(x, y) \in R$,便有 $(y, x) \in R(x \neq y)$,则称 R 是 A 上的对称关系。
 - (4) 对每个 $x, y \in A$,如果 $(x, y) \in R$ 并且 $(y, x) \in R$,便有 $x = y$,则称 R 是 A 上的反对称关系。
 - (5) 对每个 $x, y, z \in A$,如果 $(x, y) \in R$ 并且 $(y, z) \in R$,便有 $(x, z) \in R$,则称 R 是 A 上的传递关系;否则称非传递关系。

例 2-5 设有整数集合 I ,问 I 上的空关系(用 $\emptyset$ 表示)、全关系、 $=$ 、 $<$ 、 $\leq$ 及整除关系(用 D 表示)是否满足自反性、非自反性、对称性、反对称性和传递性?

解: 为清楚起见,将它们列为表 2-2。

表 2-2 关系 5 种性质表

	$\emptyset$	$I \times I$	$=$	$<$	$\leq$	D
自反性	否	是	是	否	是	否
非自反性	是	否	否	是	否	否
对称性	是	是	是	否	否	否
反对称性	是	否	是	是	是	否
传递性	是	是	是	是	是	是

我们知道,关系也是一个集合,设集合 A 上有两个关系 R_1 和 R_2 ,它们具有相同的性质,那么对它们作并、交、差等运算后的结果是否保持原来的性质呢?这里情况较复杂,为使读者清晰起见,列为表 2-3。

表 2-3 关系 5 种性质的运算表				
	$R_1 \cup R_2$	$R_1 \cap R_2$	$R_1 - R_2$	$(A \times A) - R_1$
自反性	是	是	否	否
非自反性	是	是	是	否
对称性	是	是	是	是
反对称性	否	是	是	否
传递性	否	是	否	否

例 2-6 设 $S = \{1, 2, 3\}$,
 $R_1 = \{(1, 1), (1, 2), (2, 2), (2, 3)\}$
 $R_2 = \{(1, 2), (2, 3), (1, 3)\}$
 $R_3 = \{(1, 1), (2, 2), (2, 3), (3, 2), (3, 3)\}$
 其中 R_1 既不是自反的,也不是非自反的, R_3 是自反的, R_1 和 R_2 是反对称的, R_3 是对称的; R_2 和 R_3 是传递的,但 R_1 不是传递的,因为 $(1, 2) \in R$ 并且 $(2, 3) \in R$ 但 $(1, 3) \notin R$ 。

上述关系中,自反性、对称性和传递性尤其重要,以后会经常遇到。

2.3 关系的运算

关系也是集合,因此集合论中的并、交、差等运算也完全适合关系,不再赘述。我们在这一节要定义另外一些运算,通过这些运算可以由一些已知关系产生新的关系。

1. 补运算

定义 2-6 设 $R \subseteq A \times B$,则 R 关于 $A \times B$ 的补(简称 R 的补)是

集合 $\bar{R} = (A \times B) - R$ 。

例如, $R \subseteq \{1, 2, 3\} \times \{1, 2, 3, 4\}$, $R = \{(1, 2), (2, 3), (1, 3)\}$, 则 $\bar{R} = \{(1, 1), (1, 4), (2, 1), (2, 2), (2, 4), (3, 1), (3, 2), (3, 3), (3, 4)\}$ 。

2. 复合运算

定义 2-7 设 $R_1 \subseteq A \times B$, $R_2 \subseteq B \times C$, 则 R_1 和 R_2 的复合是 $R_1 \circ R_2 = \{(a, c) \mid a \in A, c \in C, \text{且存在 } b \in B \text{ 使得 } (a, b) \in R_1 \text{ 以及 } (b, c) \in R_2\}$ 。

这意味着 $R_1 \circ R_2$ 是 A 到 C 的关系, 即 $R_1 \circ R_2 \subseteq A \times C$ 。复合关系的示意图见图 2-2。图中:

$$R_1 = \{(a_1, b_1), (a_2, b_3), (a_1, b_2)\}$$

$$R_2 = \{(b_4, c_1), (b_2, c_2), (b_3, c_3)\}$$

$$R_1 \circ R_2 = \{(a_1, c_2), (a_2, c_3)\}$$

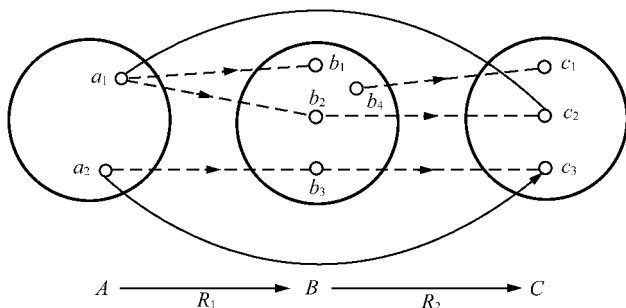


图 2-2 复合关系图示

若(1) R_1 是父子关系, 则 $R_1 \circ R_1$ 是祖孙关系。

(2) R_1 是兄弟关系, R_2 是父子关系, 则 $R_1 \circ R_2$ 是叔侄关系。

定理 2-1 设 $R_1 \subseteq A \times B$, $R_2 \subseteq B \times C$ 及 $R_3 \subseteq C \times D$, 则 $R_1 \circ (R_2 \circ R_3) = (R_1 \circ R_2) \circ R_3$ 。

证明: 先证 $(R_1 \circ R_2) \circ R_3 \subseteq R_1 \circ (R_2 \circ R_3)$ 。令 $(a, d) \in (R_1 \circ R_2) \circ R_3$ 。

R_3 , 则至少存在一个 $c \in C$, 使得 $(a, c) \in (R_1 \circ R_2)$ 并且 $(c, d) \in R_3$; 又至少存在一个 $b \in B$, 使得 $(a, b) \in R_1$ 并且 $(b, c) \in R_2, (c, d) \in R_3$; 由于 $(b, c) \in R_2$ 且 $(c, d) \in R_3$, 故得 $(b, d) \in (R_2 \circ R_3)$, 因此 $(a, d) \in R_1 \circ (R_2 \circ R_3)$ 。反之亦可证明 $R_1 \circ (R_2 \circ R_3) \subseteq (R_1 \circ R_2) \circ R_3$ 。故定理成立。

这条定理说明复合关系满足结合律。

复合关系进一步推广:

定义 2-8 设 $R \subseteq A \times A, n \in N$, 则 R 的第 n 次幂 (用 R^n 表示) 是:

$$(1) R^0 = \{(x, x) \mid x \in A\} = E$$

$$(2) R^{n+1} = R^n \circ R$$

对于 R 的 n 次幂还有下面定理:

定理 2-2 设 $R \subseteq A \times A, m, n \in N$, 则:

$$(1) R^m \circ R^n = R^{m+n}$$

$$(2) (R^m)^n = R^{mn}$$

通常复合运算对并运算满足分配律, 即若 $R_1 \subseteq A \times B, R_2 \subseteq B \times C, R_3 \subseteq B \times C$, 则有:

$$R_1 \circ (R_2 \cup R_3) = (R_1 \circ R_2) \cup (R_1 \circ R_3)$$

$$\text{而 } R_1 \circ (R_2 \cap R_3) \subseteq (R_1 \circ R_2) \cap (R_1 \circ R_3)。$$

但是一般情况下 $S \circ R \neq R \circ S$ 。

例 2-7 试证 $(R \cup E)^n = E \cup \bigcup_{i=1}^n R^i$

其中 $\bigcup_{i=1}^n R^i = R^1 \cup R^2 \cup \dots \cup R^n, E$ 为恒等关系。

证明: 用数学归纳法。

(1) 当 $n=1$ 时, 显然成立;

(2) 设 $n=k$ 时成立, 即有 $(R \cup E)^k = \bigcup_{i=1}^k R^i \cup E$, 现证 $n=k+1$ 时也成立:

$$(R \cup E)^{k+1} = (R \circ E)^k \circ (R \cup E) = (E \cup \bigcup_{i=1}^k R^i) \circ (R \cup E)$$

$$= E \circ R \cup \bigcup_{i=2}^{k+1} R^i \cup E \circ E \cup \left(\bigcup_{i=1}^k R^i \right) \circ E$$

$$= R \cup \bigcup_{i=2}^{k+1} R^i \cup E \cup \bigcup_{i=1}^k R^i = \bigcup_{i=1}^{k+1} R^i \cup E$$

例 2-8 设 $A = \{a, b, c, d\}$, A 上的一个关系 $R = \{(a, b), (b, a), (b, c), (c, d)\}$, 于是:

$$R^0 = \{(a, a), (b, b), (c, c), (d, d)\}$$

$$R^1 = R^0 \circ R = R$$

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

$$R^3 = R^2 \circ R = \{(a, b), (b, a), (b, c), (a, d)\}$$

$$R^4 = R^3 \circ R = \{(a, a), (b, b), (a, c), (b, d)\}$$

我们发现 $R^4 = R^2$, 因此 $R^4 \circ R = R^2 \circ R$, 即:

$$R^5 = R^3, \text{ 类似有 } R^6 = R^4 = R^2, \text{ 可以用归纳法得出 } R^{2n+1} = R^3,$$

$$R^{2n} = R^2, (n \geq 1).$$

这例说明有限集上的关系 R , 不是所有的幂都是互异的, 下面的定理刻画了这一性质。

定理 2-3 设 $R \subseteq A \times A$, $|A| = n$, $(n \in N)$, 则存在 s 和 t , 使得 $R^s = R^t$. 其中 $0 \leq s < t \leq 2^{n^2}$.

证明: A 上的每个二元关系是 $A \times A$ 的一个子集, 因为 $A \times A$ 有 n^2 个元素, 因此 $\rho(A \times A)$ 有 2^{n^2} 个元素, 说明 A 上有 2^{n^2} 个不同关系, R 的不同幂不会超过 2^{n^2} 个, 但在序列 $R^0, R^1, R^2, \dots, R^{2^{n^2}}$ 中, 有 $2^{n^2} + 1$ 项, 因此至少有两项相等。

如果 R 是无限集上的关系, 则不具备上述性质。例如, 若 $A = N$, 而且 $(x, y) \in R \Leftrightarrow y = x + 1$, 则 $(x, z) \in R^s \Leftrightarrow z = x + s$ (其中 $\Leftrightarrow$ 表示当且仅当), 在这种情况下, A 上 R 的所有幂都不相同。

定理 2-4 设 R 是集合 A 上的二元关系, 假定存在 s 和 t , 且 $s < t$, 使 $R^s = R^t$, 则:

$$(1) \text{ 对所有 } k \geq 0, R^{s+k} = R^{t+k}.$$

$$(2) \text{ 对所有 } k, i \geq 0, R^{s+i+kp} = R^{s+i}, \text{ 其中 } p = t - s.$$

(3) 令 $S = \{R^0, R^1, R^2, \dots, R^{i-1}\}$, 则对所有 $q \in N$, 有 $R^q \in S$ 。

证明: (1)和(2)用归纳法证明, 留作练习。现在证明(3), 令 $q \in N$, 若 $q < t$, 则由定义, $R^q \in S$; 假定 $q \geq t$, 则 q 可表示成 $s + kp + i$, 其中 $i < p$, 由(2)得到 $R^q = R^{s+i}$, 由于 $s + i < t$, 所以 $R^q \in S$ 。

3. 逆运算

通过关系的逆运算可由已知关系产生逆关系。

定义 2-9 设 $R \subseteq A \times B$, 则关系 R 的逆关系(用 $\tilde{R}$ 表示)是 $\tilde{R} = \{(y, x) \mid (x, y) \in R\}$

例如, 设 $R = \{(1, 2), (2, 3), (1, 3)\}$, 则:

$$\tilde{R} = \{(2, 1), (3, 2), (3, 1)\}$$

定理 2-5 设有三个关系 $R \subseteq A \times B$, $R_1 \subseteq A \times B$ 和 $R_2 \subseteq A \times B$, 则有下面的等式:

$$(1) \quad \tilde{\tilde{R}} = R$$

$$(2) \quad \widetilde{R_1 \cup R_2} = \tilde{R}_1 \cup \tilde{R}_2$$

$$(3) \quad \widetilde{(R_1 \cap R_2)} = \tilde{R}_1 \cap \tilde{R}_2$$

$$(4) \quad \widetilde{A \times B} = B \times A$$

$$(5) \quad \widetilde{\emptyset} = \emptyset$$

$$(6) \quad \tilde{\tilde{R}} = \bar{\bar{R}}$$

$$(7) \quad \widetilde{R_1 - R_2} = \tilde{R}_1 - \tilde{R}_2$$

$$(8) \quad \text{如果 } R_1 \subseteq R_2, \text{ 则 } \tilde{R}_1 \subseteq \tilde{R}_2$$

证明: (仅证明其中的(1), (3), (6), (7))

$$\begin{aligned} (1) \quad R &= \{(a, b) \mid (a, b) \in R\} \\ &= \{(a, b) \mid (b, a) \in \tilde{R}\} \\ &= \{(a, b) \mid (a, b) \in \tilde{\tilde{R}}\} \\ &= \{\tilde{\tilde{R}}\} \end{aligned}$$

$$\begin{aligned} (3) \quad \text{令 } (a, b) &\in \widetilde{R_1 \cap R_2} \\ \Rightarrow (b, a) &\in (R_1 \cap R_2) \end{aligned}$$

$$\Rightarrow (b, a) \in R_1 \text{ 且 } (b, a) \in R_2$$

$$\Rightarrow (a, b) \in \tilde{R}_1 \text{ 且 } (a, b) \in \tilde{R}_2$$

$$\Rightarrow (a, b) \in \tilde{R}_1 \cap \tilde{R}_2$$

所以 $\widetilde{R_1 \cap R_2} \subseteq \tilde{R}_1 \cap \tilde{R}_2$

反之, 令 $(a, b) \in \tilde{R}_1 \cap \tilde{R}_2$

$$\Rightarrow (a, b) \in \tilde{R}_1 \text{ 且 } (a, b) \in \tilde{R}_2$$

$$\Rightarrow (b, a) \in R_1 \text{ 且 } (b, a) \in R_2$$

$$\Rightarrow (b, a) \in R_1 \cap R_2$$

$$\Rightarrow (a, b) \in \widetilde{R_1 \cap R_2}$$

故 $\tilde{R}_1 \cap \tilde{R}_2 \subseteq \widetilde{R_1 \cap R_2}$

所以 $R_1 \cap R_2 = \widetilde{\tilde{R}_1 \cap \tilde{R}_2}$

(6) 令 $(a, b) \in \tilde{\tilde{R}}$

$$\Rightarrow (b, a) \in \tilde{R}$$

$$\Rightarrow (b, a) \notin R \quad (\text{由补的定义导出})$$

$$\Rightarrow (a, b) \notin \tilde{R}$$

$$\Rightarrow (a, b) \in \tilde{\tilde{R}}$$

故, $\tilde{\tilde{R}} \subseteq \tilde{R}$, 同理可以证明 $\tilde{R} \subseteq \tilde{\tilde{R}}$, 所以原等式成立。

(7) 由于 $R_1 - R_2 = R_1 \cap \bar{R}_2$, 故

$$\begin{aligned} \widetilde{(R_1 - R_2)} &= \widetilde{R_1 \cap \bar{R}_2} = \tilde{R}_1 \cap \tilde{\bar{R}_2} = \tilde{R}_1 \cap \bar{\tilde{R}_2} \\ &= \tilde{R}_1 - \tilde{R}_2 \end{aligned}$$

其余各题留给读者证明。

2.4 关系的闭包运算

假定 P 是关系的任何一性质。一个关系 R 的 P 闭包是最小关系 R' , 使得 $R \subseteq R'$ 且 R' 具有性质 P 。但是我们常用的是三个闭包, 现具体定义如下:

定义 2-10 设 $R \subseteq A \times A$, 则 R 的自反(对称, 传递)闭包是 R' , 它满足下面三个条件:

- (1) R' 是自反的(对称的, 传递的)
- (2) $R \subseteq R'$
- (3) 对任一自反(对称, 传递)关系 R'' , 如果 $R \subseteq R''$, 则 $R' \subseteq R''$ 。

我们用 $r(R)$ 、 $s(R)$ 、 $t(R)$ 分别表示 R 的自反闭包、对称闭包和传递闭包。

例 2-9

(1) $<$ 的自反闭包是 $\leq$ 。

(2) 令 $R \subseteq \{1, 2, 3\} \times \{1, 2, 3\}$, 而且 $R = \{(1, 2), (1, 3)\}$, 则

$$r(R) = \{(1, 1), (2, 2), (3, 3), (1, 2), (1, 3)\}$$

$$s(R) = \{(1, 2), (2, 1), (1, 3), (3, 1)\}$$

$$t(R) = R$$

由定义仔细推敲, 可以知道: 如果 R 已是自反的, 则 $r(R) = R$; 如果 R 已是对称的, 则 $s(R) = R$; 如 R 已是传递的, 则 $t(R) = R$ 。通常怎么来构造 R 的自反(对称, 传递)闭包呢? 下面分别介绍这方面的内容。

定理 2-6 设 $R \subseteq A \times A$, 则 $r(R) = R \cup E$, 其中 $E = \{(x, x) \mid x \in A\}$ ——恒等关系。

证明: 令 $R' = R \cup E$, 我们来证明它满足自反闭包之定义。由于 $R' = R \cup E$, 故它是自反的而且 $R \subseteq R'$; 又假定还有 $R'' \subseteq A \times A$ 是自反的而且 $R \subseteq R''$ 。任取 $(a, b) \in R'$, 则 $(a, b) \in R$ 或者 $(a, b) \in E$, 如果 $(a, b) \in R$, 则 $(a, b) \in R''$, 因为 $R \subseteq R''$ 。如果 $(a, b) \in E$, 则 $a = b$, 故 $(a, b) \in R''$, 因为 R'' 是自反的。从而得 $R' \subseteq R''$ 。所以有 $R' = r(R)$ 。

定理 2-7 设 $R \subseteq A \times A$, 则 $s(R) = R \cup \tilde{R}$ 。

证明: 令 $R' = R \cup \tilde{R}$, 显然 $R \subseteq R'$, 由于 $(\widehat{R \cup \tilde{R}}) = (\tilde{R} \cup \tilde{\tilde{R}}) = R \cup \tilde{R}$, 所以 R' 是对称的。若还有 $R'' \subseteq A \times A$ 是对称的而且 $R \subseteq R''$, 下面证明 $R' \subseteq R''$ 。任取 $(a, b) \in R'$, 故 $(a, b) \in R$ 或者 $(a, b) \in \tilde{R}$ 。如果 $(a, b) \in R$, 由假设 $(a, b) \in R''$; 如果 $(a, b) \in \tilde{R}$, 则 $(b, a) \in R$, 因此 $(b,$

$a) \in R''$, 但 R'' 是对称的, 所以 $(a, b) \in R''$ 。得出 $R' \subseteq R''$ 。所以有 $s(R) = R \cup \tilde{R}$ 。

例 2-10

- (1) I 上 $\neq$ 的自反闭包是全关系 $I \times I$;
- (2) $R = \emptyset$ 的自反闭包是恒等关系 E ;
- (3) $< \subseteq I \times I$ 的对称闭包是 $\neq$;
- (4) $\leq \subseteq I \times I$ 的对称闭包是全关系 $I \times I$;
- (5) 恒等关系 E 的对称闭包是 E , $\neq$ 的对称闭包是 $\neq$ 。

定理 2-8 设 $R \subseteq A \times A$, 则:

$$t(R) = \bigcup_{i=1}^{\infty} R^i = R \cup R^2 \cup R^3 \cup \dots$$

证明: 分两部分:

- (1) 证 $\bigcup_{i=1}^{\infty} R^i \subseteq t(R)$, 用归纳法证 $R^n \subseteq t(R)$ 对一切 n 都成立。

(a) 奠基: 由传递闭包定义立即得到 $R \subseteq t(R)$;

(b) 归纳: 假设 $R^n \subseteq t(R)$ 对 $n \geq 1$ 成立, 令 $(a, b) \in R^{n+1}$, 因为 $R^{n+1} = R^n \circ R$, 所以存在 $c \in A$, 使得 $(a, c) \in R^n$, 并且 $(c, b) \in R$, 由归纳假设和奠基, $(a, c) \in t(R)$ 并且 $(c, b) \in t(R)$, 由于 $t(R)$ 是传递的, 所以 $(a, b) \in t(R)$, 即 $R^{n+1} \subseteq t(R)$, 由于 $R^n \subseteq t(R)$ 对所有 $n \geq 1$ 都成立, 所以 $\bigcup_{i=1}^{\infty} R^i \subseteq t(R)$ 。

- (2) 证 $t(R) \subseteq \bigcup_{i=1}^{\infty} R^i$ 。先证 $\bigcup_{i=1}^{\infty} R^i$ 是传递的, 令 (a, b) 和 (b, c) 是

$\bigcup_{i=1}^{\infty} R^i$ 中的任意元素, 于是存在一些整数 $s \geq 1, t \geq 1$ 使 $(a, b) \in R^s, (b, c) \in R^t$, 于是 $(a, c) \in R^s \circ R^t$, 即 $(a, c) \in R^{s+t}$, 所以 $(a, c) \in \bigcup_{i=1}^{\infty} R^i$, 因此

$\bigcup_{i=1}^{\infty} R^i$ 是传递的。由于 $t(R)$ 是最小的传递关系, 所以 $t(R) \subseteq \bigcup_{i=1}^{\infty} R^i$ 。

当 $R \subseteq A \times A, (a, b) \in t(R)$ 意指 A 中存在一系列元素 $x_0, x_1, \dots, x_n$, (其中 $n \geq 1, x_0 = a, x_n = b$), 而且 $0 \leq i < n$, 使 $(x_i, x_{i+1}) \in R$, 反之亦然。

由定理 2-3 和定理 2-4, 可以得出具有 n 个元素的有限集合上的关系 R 的传递闭包是:

$$t(R) = \bigcup_{i=1}^{2^{n^2}} R^i$$

这个结论可以进一步改善如下:

定理 2-9 设 $R \subseteq A \times A, |A| = n$, 则 $t(R) = \bigcup_{i=1}^n R^i$ 。

例 2-11

(1) 设 $R = \{(a, b), (b, c), (c, d)\}$, 则:

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

$$R^3 = \{(a, d)\}, R^4 = \emptyset$$

所以 $t(R) = \{(a, b), (b, c), (c, d), (a, c), (b, d), (a, d)\}$

(2) 设 $R \subseteq I \times I$, 使得 aRb 当且仅当 $b = a + 1$, 则 $t(R) = <$ 。

例 2-12 设 $R \subseteq A \times A$, 试证:

$$(1) rs(R) = sr(R)$$

$$(2) rt(R) = tr(R)$$

$$(3) st(R) \subseteq ts(R)$$

(其中 $rs(R)$ 表示 R 的对称闭包的自反闭包, $sr(R)$ 表示 R 的自反闭包的对称闭包, $rt(R)$ 、 $st(R)$ 都用类似方法理解)。

$$\begin{aligned} \text{证明: } (1) \quad sr(R) &= s(R \cup E) = (R \cup E) \cup \widetilde{R \cup E} \\ &= R \cup E \cup \tilde{R} \cup \tilde{E} \\ &= R \cup \tilde{R} \cup E = s(R) \cup E \\ &= r(s(R)) = rs(R) \end{aligned}$$

$$(2) \quad rt(R) = t(R) \cup E$$

$$\begin{aligned} tr(R) &= t(R \cup E) = \bigcup_{i=1}^{\infty} (R \cup E)^i \\ &= (R \cup E) \cup (R \cup E)^2 \cup (R \cup E)^3 \cup \cdots \\ &= R \cup E \cup R^2 \cup R^3 \cup \cdots \\ &= t(R) \cup E = r(t(R)) \\ &= rt(R) \end{aligned}$$

(3) 由于 $s(R) = R \cup \tilde{R} \supseteq R$, 故 $ts(R) \supseteq t(R)$

$sts(R) \supseteq st(R)$, 而 $ts(R)$ 是对称的,

所以 $ts(R) \supseteq st(R)$ 。

2.5 具有特定性质的关系

通常我们总是按照关系的性质处理集合中的元素的。按照关系的性质可把关系分成各种类型, 其中等价关系尤为重要, 它在分析离散结构中起特别重要的作用。

1. 等价关系和划分

这两个概念是密切相联的, 我们先给出它们的定义, 然后找到它们之间的联系。

定义 2-11 一个非空集合 S 的一个划分 P 是 S 的 n 个非空子集的集合, 它满足下面两个条件:

(1) 对所有 $A_i, A_j \in P$ 且 $i \leq n, j \leq n$, 如果 $A_i \neq A_j$, 则有 $A_i \cap A_j = \emptyset$;

(2) $\bigcup_{i=1}^n A_i = S$ 。

其中每个 A_i 称为划分 P 的块。

由定义可知, 划分中的每个块是两两互不相交的, S 中任一元素必属于某一块, 图 2-3 是五个块的划分示意图。

例 2-13 设 $S = \{1, 2, \dots, 8, 9\}$, 其子集的集合有:

(1) $\{\{1, 3, 5\}, \{2, 4, 6, 8\}, \{5, 7, 9\}\}$

(2) $\{\{1, 3, 5\}, \{2, 6\}, \{4, 8, 9\}\}$

(3) $\{\{1, 3, 5\}, \{2, 4, 6, 8\}, \{7, 9\}\}$

显然(2)不是 S 的划分, 因为三个块中都不含有 7, (1)也不是 S 的划分, 因为 $\{1, 3, 5\} \cap \{5, 7, 9\} \neq \emptyset$, (3)是 S 的一个划分。

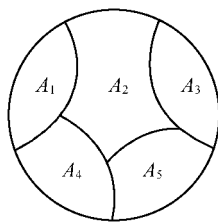


图 2-3 五个块的划分示意图

又如 $\{1, 2, 3\}$ 的划分是 $\{\{1\}, \{2\}, \{3\}\}, \{\{1, 2, 3\}\}, \{\{1\}, \{2, 3\}\}, \{\{2\}, \{1, 3\}\}, \{\{3\}, \{1, 2\}\}$ 。

定义 2-12 设 $R \subseteq A \times A$, 如果 R 满足自反性、对称性和传递性, 则称 R 是一个等价关系。

例 2-14 设有整数集合 I , 对整数 $m > 1$ 及两个整数 x 和 y , 如果 $(x-y)$ 能被 m 整除, 则称 x 和 y 是按模 m 同余的, 记作:

$$x \equiv y \pmod{m}$$

例如, $m=4$, 则 $11 \equiv 3 \pmod{4}$, 因为 4 能整除 $(11-3)$ 。

定理 2-10 按模 m 同余是一个等价关系。

证明: (下面用 $(x-y) \mid m$ 表示 $(x-y)$ 被 m 整除)。

(1) 自反性: 对每个 $x \in I$, $(x-x) \mid m$, 所以

$$x \equiv x \pmod{m};$$

(2) 对称性: 假定 $x \equiv y \pmod{m}$, 所以 $(x-y) \mid m$, $y-x = -(x-y)$, 所以 $(y-x) \mid m$, 即 $y \equiv x \pmod{m}$;

(3) 传递性: 假定 $x \equiv y \pmod{m}$ 并且 $y \equiv z \pmod{m}$, 所以 $(x-y) \mid m$ 并且 $(y-z) \mid m$, 而 $x-z = (x-y) + (y-z)$ 。故 $(x-z) \mid m$, 即 $x \equiv z \pmod{m}$ 。

例 2-15 设 $R_1 \subseteq A \times A, R_2 \subseteq A \times A$ 是两个等价关系, 试证 $R_1 \cap R_2$ 也是一个等价关系。

证明: (1) 自反性: 对任意 $x \in A$, 有 $(x, x) \in R_1$ 并且 $(x, x) \in R_2$, 故 $(x, x) \in R_1 \cap R_2$;

(2) 对称性: 对任意 $x, y \in A$, 如果 $(x, y) \in R_1$, 则有 $(y, x) \in R_1$, 即 $(x, y) \in R_1 \Rightarrow (y, x) \in R_1$, 同理 $(x, y) \in R_2 \Rightarrow (y, x) \in R_2$, 所以 $(x, y) \in R_1$ 且 $(x, y) \in R_2 \Rightarrow (y, x) \in R_1$ 且 $(y, x) \in R_2$, 即 $(x, y) \in R_1 \cap R_2 \Rightarrow (y, x) \in R_1 \cap R_2$;

(3) 传递性: 对任意 $x, y, z \in A$, 因 $(x, y) \in R_1$ 且 $(y, z) \in R_1 \Rightarrow (x, z) \in R_1$; $(x, y) \in R_2$ 且 $(y, z) \in R_2 \Rightarrow (x, z) \in R_2$, 所以 $(x, y) \in R_1$ 且 $(y, z) \in R_1$ 且 $(x, y) \in R_2$ 且 $(y, z) \in R_2 \Rightarrow (x, z) \in R_1$ 且 $(x, z) \in R_2$, 即: $(x, y) \in R_1 \cap R_2$ 且 $(y, z) \in R_1 \cap R_2 \Rightarrow (x, z) \in R_1 \cap R_2$ 。

下面我们把集合中的元素按等价关系分类。

定义 2-13 设 $R \subseteq A \times A$ 是一个等价关系,对每个元素 $a \in A$, a 关于 R 的等价类是 A 的一个子集 $\{x \mid xRa\}$, 用 $[a]_R$ 表示, 即:

$$[a]_R = \{x \mid xRa\}$$

集合 A 关于 R 的等价类的全体称为 A 关于 R 的商集, 用 A/R 表示, 即:

$$A/R = \{[a]_R \mid a \in A\}$$

在不会发生概念含糊的情况下, 常把 $[a]_R$ 简写为 $[a]$, 现在进一步研究集合 A 的等价类具有什么性质, 下面的定理刻划了这一点。

定理 2-11 设 $R \subseteq A \times A$ 是一个等价关系, 则:

- (1) 对每个元素 $a \in A$, 有 $a \in [a]$;
- (2) $[a] = [b]$ 当且仅当 $(a, b) \in R$;
- (3) 如果 $[a] \neq [b]$, 则 $[a] \cap [b] = \emptyset$ 。

证明: (1) 因为 R 是自反的, 对每个 $a \in A$ 有 $(a, a) \in R$, 所以 $a \in [a]$ 。

(2) 假定 $(a, b) \in R$, 我们希望证到 $[a] = [b]$ 。令 $x \in [b]$, 于是 $(b, x) \in R$, 由 R 的传递性, 得 $(a, x) \in R$, 即 $x \in [a]$, 从而 $[b] \subseteq [a]$; 又因为 R 是对称的, 所以 $(b, a) \in R$, 令 $x \in [a]$, 于是 $(a, x) \in R$, 所以 $(b, x) \in R$, 即 $x \in [b]$, 从而 $[a] \subseteq [b]$ 。因此 $[a] = [b]$ 。

另一方面, 如果 $[a] = [b]$, 由 (1), $b \in [b] = [a]$, 所以 $(a, b) \in R$ 。

(3) 为了证明 (3), 我们证明等价的矛盾命题: 如果 $[a] \cap [b] \neq \emptyset$, 则 $[a] = [b]$ 。

如果 $[a] \cap [b] \neq \emptyset$, 则必有 $x \in [a] \cap [b]$, 因此 $(a, x) \in R$ 并且 $(b, x) \in R$, 由 R 的对称性, 得 $(x, b) \in R$, 再由 R 的传递性, 得 $(a, b) \in R$, 再由 (2) 得 $[a] = [b]$ 。

这条定理说明每个元素 x , 均属于它自己的类; 具有相同关系的元素在同一类; 不同的等价类是两两分离的。这条定理已包含了商集的基本性质, 而且有下面等式:

$$\bigcup_{x \in A} [x] = A$$

对此式可以证明如下：

假定 $c \in \bigcup_{x \in A} [x]^*$ ，因此 c 必在某一个等价类中，譬如说在 $[a]$ 中，即 $c \in [a]$ ，因为 $[a] \subseteq A$ ，故 $c \in A$ ，从而得到 $\bigcup_{x \in A} [x] \subseteq A$ 。

又假定 $c \in A$ ，因此 $c \in [c] \subseteq \bigcup_{x \in A} [x]$ ，从而有 $A \subseteq \bigcup_{x \in A} [x]$ 。
所以： $\bigcup_{x \in A} [x] = A$ 。

这就找到了集合 A 上的等价关系 R 的商集 A/R 与 A 的划分的关系，即商集是一个划分。

例 2-16 令 $S = \{1, 2, 3, 4\}$ ， $R = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 3), (2, 4), (3, 1), (4, 2)\}$ 是 S 上的一个等价关系，其等价类是： $[1] = \{1, 3\}$ ， $[2] = \{2, 4\}$ ， $[3] = \{3, 1\}$ ， $[4] = \{4, 2\}$ ，其中 $[1] = [3]$ ， $[2] = [4]$ ，所以 $\{[1], [2]\}$ 是 S 的一个划分。

2. 相容关系

定义 2-14 设 $R \subseteq A \times A$ ，如果 R 是自反的和对称的，则称 R 是 A 上的相容关系。

例 2-17 设 $R \subseteq \{1, 2, 3, 4\} \times \{1, 2, 3, 4\}$ ， $R = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (2, 4), (3, 1), (3, 2), (3, 3), (3, 4), (4, 2), (4, 3), (4, 4)\}$

从相容关系的定义可知等价关系必是相容关系，但反之不然。

定义 2-15 设 $R \subseteq A \times A$ 是一个相容关系， A 的子集 B 称为相容关系 R 的最大相容类的条件是：

- (1) 任一 $x \in B$ ，都与 B 中所有其他的元素有相容关系。
- (2) $A - B$ 中没有有一个元素能与 B 中的所有元素都有相容关系。

例 2-17 中的最大相容类是 $\{1, 2, 3\}$ ， $\{2, 3, 4\}$ 。现在以子集 $\{1, 2, 3\} \subseteq \{1, 2, 3, 4\}$ 予以说明。首先 $(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (1, 3), (2, 3), (3, 1), (3, 2)$ 均在 R 之中，其次， $\{1, 2, 3, 4\} - \{1, 2,$

* $\bigcup_{x \in A} [x]$ 表示 A 的各个等价类的集合。

$3\} = \{4\}$, 而 4 不能与 $\{1, 2, 3\}$ 中的每个元素有相容关系。因为 $(1, 4) \notin R, (4, 1) \notin R$ 。

定义 2-16 设 R 是 A 上的一个相容关系, 其最大相容类的集合称为 A 的完全覆盖。

对于例 2-17, 我们求得它的完全覆盖是:

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

容易看出, 如果 R 是 A 上的一个等价关系, 则 A 的完全覆盖是关于 R 的划分。

定理 2-12 每个相容关系 R , 惟一地定义一个完全覆盖。

此外还有一个十分重要的偏序关系, 将在第四章介绍。

习 题 二

2.1 设 $A = \{0, 1\}, B = \{1, 2\}$, 求笛卡尔乘积:

(1) $A \times B$ (2) $A^2 \times B$

(3) $B \times A$ (4) $B^2 \times A$

(5) $(A \times B)^2$

2.2 在具有 X 轴和 Y 轴的平面直角坐标系统中, 对 $X \times Y$ 作几何解释, 其中:

$$X = \{x \mid x \in R, -3 \leq x \leq 2\}$$

$$Y = \{y \mid y \in R, -2 \leq y \leq 0\}$$

2.3 对任意集合 A, B, C , 证明:

(1) $A \times (B \cup C) = (A \times B) \cup (A \times C)$

(2) $A \times (B \cap C) = (A \times B) \cap (A \times C)$

(3) $A \times B = B \times A$ 当且仅当 $A = \emptyset$ 或 $B = \emptyset$ 或 $A = B$

2.4 设 $A = \{0, 1, 2, 3\}$, A 上的两个关系为:

$$R_1 = \{(i, j) \mid j = i + 1 \text{ 或 } j = i/2\}$$

$$R_2 = \{(i, j) \mid i = j + 2\}$$

求复合关系:

$$(1) R_1 \circ R_2 \qquad (2) R_2 \circ R_1 \qquad (3) R_1 \circ R_2 \circ R_1$$

2.5 设 R_1, R_2 和 R_3 都是集合 A 上的关系, 证明:

(1) 如果 $R_1 \subseteq R_2$, 则 $R_1 \circ R_3 \subseteq R_2 \circ R_3$;

(2) 如果 $R_1 \subseteq R_2$, 则 $R_3 \circ R_1 \subseteq R_3 \circ R_2$ 。

2.6 证明定理 2-5 的其余部分。

2.7 有人说, 假定集合 A 上的一个关系 R 满足对称性和传递性, 那么 R 也满足自反性, 他的推论方法是: 因为 R 是对称的, 所以:

$$aRb \Rightarrow bRa$$

因为 R 是传递的, 所以:

$$aRb \text{ 且 } bRa \Rightarrow aRa$$

问这个推理方法有什么错误?

2.8 设 R_1 和 R_2 是 A 上的对称关系, 证明:

如果 $R_1 \circ R_2 \subseteq R_2 \circ R_1$, 则 $R_1 \circ R_2 = R_2 \circ R_1$

2.9 如果 A 上的关系 R 和 S 是自反的, 证明 $R \circ S$ 和 $R \cap S$ 也是自反的。

2.10 设 R 是集合 X 上的关系, E 是 X 上的恒等关系, 试证:

(1) R 是自反的当且仅当 $E \subseteq R$;

(2) R 是非自反的当且仅当 $E \cap R = \emptyset$;

(3) R 是对称的当且仅当 $R = \tilde{R}$;

(4) R 是反对称的当且仅当 $R \cap \tilde{R} \subseteq E$;

(5) R 是传递的当且仅当 $(R \circ R) \subseteq R$ 。

2.11 设 $S = \{a, b, c\}$, 其中关系为:

(1) $R_1 = \{(a, b), (a, c)(c, b)\}$

(2) $R_2 = \{(a, b), (b, c)(c, c)\}$

(3) $R_3 = \{(a, b), (b, a)(c, c)\}$

(4) $R_4 = \{(a, b), (b, c)(c, a)\}$

求它们的传递闭包 $t(R_1), t(R_2), t(R_3), t(R_4)$ 。

2.12 设 R_1 和 R_2 是集合 A 上的两个关系, 而且 $R_1 \supseteq R_2$, 证明:

$$(1) r(R_1) \supseteq r(R_2)$$

$$(2) s(R_1) \supseteq s(R_2)$$

$$(3) t(R_1) \supseteq t(R_2)$$

2.13 设 R_1 和 R_2 是集合 A 上的两个关系,证明:

$$(1) r(R_1 \cup R_2) = r(R_1) \cup r(R_2)$$

$$(2) s(R_1 \cup R_2) = s(R_1) \cup s(R_2)$$

(3) $t(R_1 \cup R_2) \supseteq t(R_1) \cup t(R_2)$, 并举一个反例说明一般情况下 $t(R_1 \cup R_2) \neq t(R_1) \cup t(R_2)$

2.14 证明定理 2-4 的其余部分。

2.15 如果 R 是集合 A 上的等价关系,则 R 的逆关系也是 A 上的等价关系。

2.16 设 $N = \{1, 2, 3, \dots\}$, 并设 $\sim$ 是 $N \times N$ 上的关系,其定义为:若 $ad = bc$, 则 $(a, b) \sim (c, d)$, 证明 $\sim$ 是一个等价关系。

2.17 设 R 是集合 $A = \{1, 2, \dots, 6\}$ 上的等价关系,

$R = \{(1, 1), (1, 5), (2, 2), (2, 3), (2, 6), (3, 2), (3, 3), (3, 6), (4, 4), (5, 1), (5, 5), (6, 2), (6, 3), (6, 6)\}$ 求 R 的等价类。

2.18 证明定理 2-12。

2.19 $P = \{a, b, c, d\}$ 的最大划分是 _____; 最小划分 _____。

2.20 集合 $A = \{1, 2, \dots, 10\}$ 上的关系 $R = \{(x, y) | x + y = 10 \text{ 且 } x, y \in A\}$, 则 R 的性质为()。

A. 自反的

B. 对称的

C. 传递的, 对称的

D. 非自反的, 传递的

2.21 $A = \{1, 2, 3, 4\}$ 上的关系 $R_1 = \{(1, 2), (2, 3), (3, 4)\}$ 可用矩阵 M_{R_1} 表示如下:

$$M_{R_1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

若表示关系 R 的矩阵具有主对角线全为 1, 按主对角对称, 那么该关系应具备_____性和_____性。

2.22 $A = \{a, b, c\}, R = \{(a, a), (a, b)\}$ 则 $s(R) =$ _____; $t(R) =$ _____。

2.23 设 R 是 $A = \{a, b, c, d\}$ 上的二元关系, $R = \{(b, a), (a, b), (c, c), (d, d)\}$, 求最小的正整数 $m, n, m < n$, 使得 $R^m = R^n$

2.24 $A = \{a, b, c\}, A_1 = \{\{a\}, \{b, c\}, \{c\}\}, A_2 = \{\{a, b, c\}\}, A_3 = \{\{a\}, \{b\}, \{c\}\}, A$ 的划分为 _____, A 的完全覆盖为 _____。

2.25 R, Q 都是 A 上的等价关系, 则 $s(R \cap Q) =$ _____; $t(R \cap Q) =$ _____。

“关系”复习提纲

1. 主要内容

- 关系基本概念。
- 关系运算。
- 关系性质。
- 闭包。
- 关系等价性与相容性。

2. 复习重点

- 了解关系基本思想、运算及性质。
- 了解几种特殊的关系。

3. 关系的基本概念

——有序偶: 两个具有固定次序的元素 x, y 所构成的序列称为有序偶, 记以 (x, y) 。

——笛卡尔乘积： $A \times B = \{(a, b) \mid a \in A, b \in B\}$ 。

——二元关系： $A \times B$ 的子集。

—— n 元有序组： $(x_1, x_2, \dots, x_n)$ 。

——笛卡尔乘积： $A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_i \in A_i \in i=1, 2, \dots, n\}$ 。

—— n 元关系： $A_1 \times A_2 \times \dots \times A_n$ 的子集。

——几种特殊关系：

- 空关系： $\emptyset$
- 全关系： $A \times B$
- 恒等关系： $E_A = \{(x, x) \mid x \in A\}$

4. 关系运算

——关系补运算 $\bar{R}$ ：设 $R \subseteq A \times B$ ，则有 $\bar{R} = (A \times B) - R$ 。

——关系复合运算 $R_1 \circ R_2$ ：设 $R_1 \subseteq A \times B, R_2 \subseteq B \times C$ ，则 $R = R_1 \circ R_2 = \{(a, c) \mid a \in A, c \in C, \text{存在 } b \in B \text{ 使得 } (a, b) \in R_1, (b, c) \in R_2\}$ 。

——关系逆运算 $\tilde{R}$ ：设有 $R \subseteq A \times B$ ，则 $\tilde{R} = \{(y, x) \mid (x, y) \in R\}$ 。

5. 关系的 5 个性质

——关系自反性： $R \subseteq A \times A$ ，若 $x \in A$ ，有 $(x, x) \in R$ 则称 R 满足自反性。

——关系非自反性： $R \subseteq A \times A$ ，若 $x \in A$ ，有 $(x, x) \notin R$ 则称 R 满足非自反性。

——关系对称性： $R \subseteq A \times A$ ，若 $x, y \in A$ ，便有 $(y, x) \in R$ ，则称 R 满足对称性。

——关系反对称性： $R \subseteq A \times A$ ，若 $x, y \in A$ ，便有 $(y, x) \notin R$ ，则称 R 满足反对称性。

——关系传递性： $R \subseteq A \times A$ ，若 $x, y, z \in A$ ，有 $(x, y) \in R, (y, z) \in R$ ，便有 $(x, z) \in R$ ，则称 R 满足传递性。

6. 闭包

——闭包定义, $R \subseteq A \times A$, 如有 R 满足:

- R' 是自反的(对称、传递);
- $R \subseteq R'$;
- 对任一自反(对称、传递)关系 R'' , 如有 $R \subseteq R''$, 则 $R' \subseteq R''$, 则

称 R' 是 R 的自反(对称、传递)闭包, 记以 $r(R)$ 、 $s(R)$ 及 $t(R)$ 。

——闭包性质:

- $r(R) = R \cup E$ 。
- $s(R) = R \cup \tilde{R}$ 。
- $t(R) = \bigcup_{i=1}^{\infty} R^i = R^1 \cup R^2 \cup R^3 \cup \dots$ 。
- 设 $|A| = n$, 则有 $t(R) = \bigcup_{i=1}^n R^i$ 。

7. 等价关系

——划分: 集合 S 及 P , P 是 S 的 n 个非空子集 $A_1, A_2, \dots, A_n$ 的集

合, 且有 $A_i \neq A_j$ 则 $A_i \cap A_j = \emptyset$ 及 $\bigcup_{i=1}^n A_i = S$, 则称 P 为 S 的一个划分。

——等价关系: 满足自反性、对称性与传递性的关系。

——等价类: 等价关系 $R \subseteq A \times A$, $a \in A$, a 关于 R 的等价类为

$$[a]_R = \{x \mid xRa\}。$$

——商集: A 关于 R 等价类全体, 记以 A/R , $A/R = \{[a]_R \mid a \in A\}$ 。

8. 相容关系

——相容关系: 满足自反性、对称性的关系。

——最大相容类: 关系 $R \subseteq A \times A$ 是相容的, $B(\subseteq A)$ 满足:

- $x \in B$ 都与 B 中其他元素相容;
- $A - B$ 中无元素与 B 中所有元素相容。

——完全覆盖: $R \subseteq A \times A$ 是相容的, 其最大相容类集合称完全覆盖。

第三章 映射与无限集

映射、函数等术语都是同义词,选用哪一个术语决定于数学的传统习惯,数学的背景和场合。本章扼要地介绍映射的基本概念和性质,然后用映射的方法讨论无限集及代数系统。

3.1 映 射

1. 映射的概念

定义 3-1 设有集合 A 和 B ,假定有一个法则,譬如 f ,对 A 中的每个元素 a 都能在 B 中找到一个惟一的元素 b 与之对应,那么这个法则称为从 A 到 B 的一个映射,记以:

$$f: A \rightarrow B \text{ 或 } f(a) = b$$

上面 $a \in A$ 亦称为象源, $b \in B$ 称为 a 在映射 f 之下的象(或值), A 称为 f 的定义域, B 称为 f 的陪域,在 f 的作用下, A 中所有元素的象构成的象集(或值域)用 $f(A)$ 表示,即:

$$f(A) = \{b \mid b = f(a), a \in A, b \in B\}$$

下面图 3-1 是一个映射的图形表示,它解释了上面提到的概念。

从 A 到 B 的一个映射也是从 A 到 B 的一个关系,但是它具有特别的性质,主要表现在两个方面:

(1) A 中的每个元素均出现在关系中,并作为关系有序偶的第一个分量;

(2) 如果 $f(a) = b$ 而且 $f(a) = c$,则 $b = c$,即 A 中的每个元素,在 f 作用下的值是惟一的。

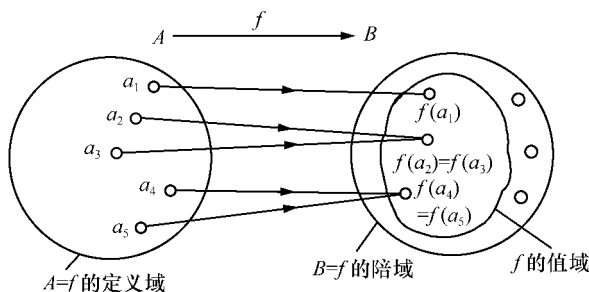


图 3-1 映射图

2. 几种特殊的映射

定义 3-2 设 $f:A \rightarrow B$ 是一个映射,

(1) 如果 $f(a_i) = f(a_j)$, 可推出 $a_i = a_j$, 则 $f:A \rightarrow B$ 称为一对一映射(或入射)。否则叫多对一映射。

(2) 如果 $f(A) = B$, 则称 $f:A \rightarrow B$ 是满射。若 $f(A) \subset B$, 则称 $f:A \rightarrow B$ 是内射。

(3) 如果 $f:A \rightarrow B$ 既是一对一映射又是满射, 则称 $f:A \rightarrow B$ 是一一对应映射(或双射)。

其图形表示见图 3-2。

例 3-1 设从实数集 R 到 R 的四个映射如下:

$$f_1(x) = x^2, f_2(x) = 2^x,$$

$$f_3(x) = x^3 - 2x^2 - 5x + 6, f_4(x) = x^3$$

这些映射的图形如图 3-3: 其中 f_1 既不是一对一的映射, 也不是满射, 它是多对一映射; f_2 是一对一映射, 但不是满射; f_3 是满射, 但不是一对一的映射; f_4 是一一对应的映射。

例如, $f:I \rightarrow I_m$, 其中 $f(i) = i \pmod{m}$, 它是从整数集到 $\{0, 1, 2, \dots, m-1\}$ 的映射, 但不是一对一映射。

$f:2^U \rightarrow 2^U$, 其中 $f(S) = S$, 它是 U 的幂集上的一一对应映射。

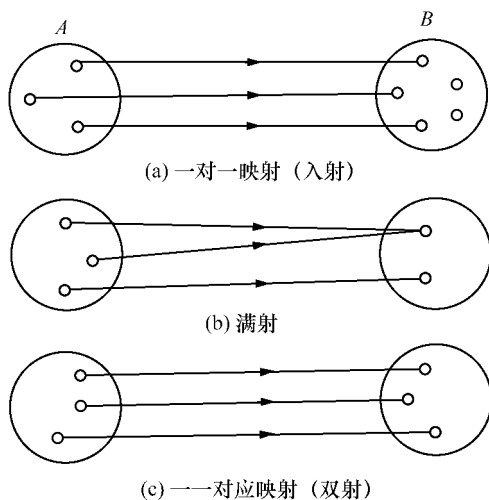


图 3-2 三种映射图

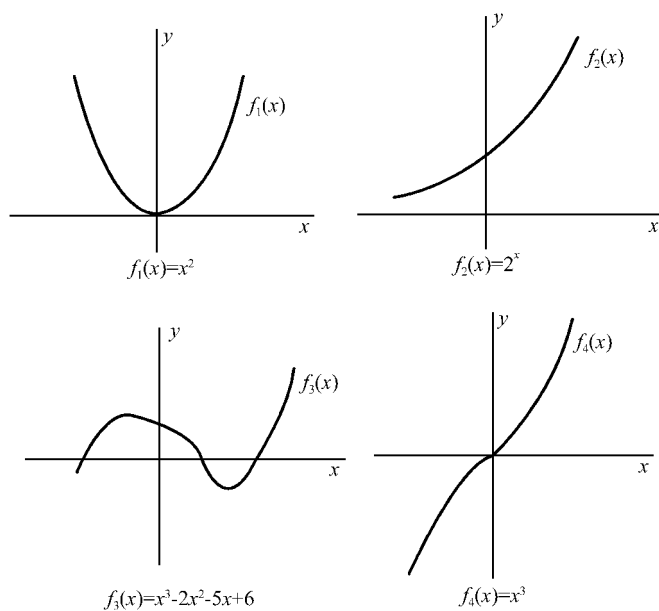


图 3-3 例 3.1 中四个映射

3. 映射的复合

定义 3-3 设有两个映射:

$$f:A \rightarrow B, g:B \rightarrow C$$

则 f 和 g 的复合, 记以 $f \circ g$, 是一个映射:

$$f \circ g:A \rightarrow C$$

其中 $f \circ g(a) = g(f(a))$ 。

因此, 如果 $b \in B$ 是 $a \in A$ 在 f 之下的象, $c \in C$ 是 b 在 g 之下的象, 则 c 是 a 在 $f \circ g$ 之下的象。 f 和 g 之复合的示意图见图 3-4。

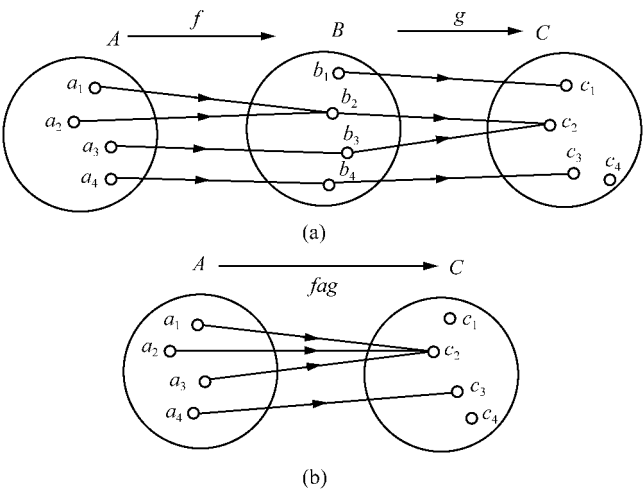


图 3-4 复合映射图

例 3-2 设有映射 $f:\rho(A) \rightarrow \mathbf{I}$, 其中 A 是有限集, $f(S) = |S|$, $S \in \rho(A)$ 。另外有一个映射 $g:\mathbf{I} \rightarrow \mathbf{R}$, 其中 $g(i) = (i - 5)/2$ 。于是 f 和 g 的复合映射是 $f \circ g:\rho(A) \rightarrow \mathbf{R}$ 。其中:

$$f \circ g(S) = g(f(S)) = g(|S|) = (|S| - 5)/2$$

对于多于两个映射的复合方法, 可依此类推。设有 r 个映射如下:

$$f_1:A_1 \rightarrow A_2, f_2:A_2 \rightarrow A_3, \dots, f_r:A_r \rightarrow A_{r+1},$$

则 $f_1 \circ f_2 \circ \dots \circ f_r$ 表示从 A_1 到 A_{r+1} 的映射。

当 $A_1 = A_2 = \dots = A_{r+1} = A, f_1 = f_2 = \dots = f_r = f$ 时, 则 $f_1 \circ f_2 \circ \dots \circ f_r$ 简记为 f^r 。

例 3-3 设有映射 $f:I \rightarrow I$, 其中 $f(i) = 2i + 1$, 那么 $f^3:I \rightarrow I$ 表示三次复合映射。

$$\begin{aligned} f^3(i) &= f(f(f(i))) = f(f(2i + 1)) \\ &= f(4i + 3) = 8i + 7 \end{aligned}$$

定理 3-1 设 $f \circ g$ 是复合映射:

- (1) 如果 f 和 g 都是满射, 则 $f \circ g$ 也是满射。
- (2) 如果 f 和 g 都是一对一映射, 则 $f \circ g$ 也是一对一映射。
- (3) 如果 f 和 g 都是一一对应映射, 则 $f \circ g$ 也是一一对应映射。

证明: 令 $f:A \rightarrow B, g:B \rightarrow C$ 是两个映射:

(1) 令 $c \in C$, 因为 g 是满射, 所以必有某个元素 $b \in B$, 使得 $g(b) = c$; 又因为 f 是满射, 所以必有某个元素 $a \in A$, 使得 $f(a) = b$, 于是:

$$f \circ g(a) = g(f(a)) = g(b) = c$$

由于 c 是 C 中任意的元素, 故 $f \circ g$ 是从 A 到 C 的满射。

(2) 令 a_1 和 a_2 是 A 中任意两个元素, 假定 $a_1 \neq a_2$, 因为 f 是一对的, 所以 $f(a_1) \neq f(a_2)$, 又因为 g 是一对一的, 所以 $g(f(a_1)) \neq g(f(a_2))$, 即:

$$f \circ g(a_1) \neq f \circ g(a_2)$$

故 $f \circ g$ 是从 A 到 C 的一对一映射。

(3) (证略)

4. 逆映射

定义 3-4 设有一个映射 $f:A \rightarrow B$, 如果它的逆关系 $\tilde{f}:B \rightarrow A$ 也是一个映射, 则称 $\tilde{f}$ 是 f 的一个逆映射。

一般说来, 一个关系的逆关系总是存在的, 但是一个映射的逆映

射未必总是存在的,下面的定理告诉我们一个映射存在逆映射的充分必要条件。

定理 3-2 一个映射 $f:A \rightarrow B$ 有逆映射当且仅当 f 是一一对应的映射。

证明: 设 $f:A \rightarrow B$ 是一一对应的。令:

$$f = \{(a, b) \mid a \in A, b \in B, f(a) = b\}$$

$$\tilde{f} = \{(b, a) \mid (a, b) \in f\}$$

因为 f 是满射,所以对每个 $b \in B$,有 $a \in A$,使得 $(a, b) \in f$,因此必有 $(b, a) \in \tilde{f}$,即 $\tilde{f}$ 的定义域是 B 。又因为 f 是一对一的,故对每个 $b \in B$,有惟一的 $a \in A$,使得 $(a, b) \in f$,亦即仅有一个 $a \in A$,使 $(b, a) \in \tilde{f}$ 。所以 $\tilde{f}$ 是一个映射,由于 $\tilde{f}$ 是 f 的一个逆关系而且 $\tilde{f}$ 也是一个映射,据定义 $\tilde{f}:B \rightarrow A$ 是 $f:A \rightarrow B$ 的逆映射。(请读者进一步证明, $\tilde{f}$ 还是一一对应的。)

必要性的证明从略。

定义 3-5 设有映射 $f:A \rightarrow A$,若对每个元素 $a \in A$,有 $f(a) = a$,则称 f 是 A 上的恒等映射,并用 E_A 表示。

显然恒等映射必是一一对应的。

定理 3-3 对任意一个映射 $f:A \rightarrow B$,有:

$$E_A \circ f = f \circ E_B = f$$

证明: 因为 $f:A \rightarrow B$ 是映射,所以任取 $a \in A$,必有 $b \in B$,使 $f(a) = b$ 。

$$\text{而} \quad E_A \circ f(a) = f(E_A(a)) = f(a) = b$$

$$f \circ E_B(a) = E_B(f(a)) = E_B(b) = b$$

故: $E_A \circ f = f \circ E_B = f$

定理 3-4 如果映射 $f:A \rightarrow B$ 有逆映射 $\tilde{f}:B \rightarrow A$,则:

$$(1) f \circ \tilde{f} = E_B$$

$$(2) \tilde{f} \circ f = E_A$$

$$(3) \tilde{\tilde{f}} = f$$

证明: (留给读者练习)

例 3-4 设映射 $f: \mathbf{R} \rightarrow \mathbf{R}$ 为 $f(x) = 2x - 3$ 。显然这个 f 是一一对应的, 所以有其逆映射 $\tilde{f}$ 存在。试求 $\tilde{f}$ 的公式。

解: 令 y 是在 f 之下 x 的象:

$$y = f(x) = 2x - 3$$

反之, x 亦是 y 在 $\tilde{f}$ 之下的象, 解得:

$$x = (y + 3)/2$$

于是: $\tilde{f}(y) = (y + 3)/2$ 。

3.2 无 限 集

1. 一般概念

有了映射的理论, 我们就可以进一步研究集合特别是无限集的问题, 我们经常要回答一个集合有多大, 两个集合哪个大哪个小的问题, 为此要引进基数的概念, 基数是用来度量一个集合“大小”的数。

根据基数的观点, 利用映射的方法, 我们来精确地给出有限集和无限集的定义。

定义 3-6 一个集合 A 与集合 $N_n = \{0, 1, 2, \dots, n-1\}$, 如果存在一一对应的映射 $f: N_n \rightarrow A$, 则称 A 是有限集, 其基数是 $n \in \mathbf{N}$; 如果 A 不是有限的, 它就是无限集。

一个集合有 n 个不同元素, 它就是基数为 n 的有限集。人们最熟悉的自然数集 $\mathbf{N}$ 是无限的。我们可以作理论上证明。

定理 3-5 自然数集 $\mathbf{N}$ 是无限的。

证明: 要证明 $\mathbf{N}$ 不是有限的, 就是要证明不存在 $n \in \mathbf{N}$, 使得从 N_n 到 $\mathbf{N}$ 存在一一对应的映射。令 g 是从 N_n 到 $\mathbf{N}$ 的任一映射, $n \in \mathbf{N}$ 。设:

$$K = 1 + \max\{g(0), g(1), \dots, g(n-1)\}$$

于是 $K \in \mathbf{N}$, 但是对每个 $x \in \{0, 1, 2, \dots, n-1\}$, 有 $g(x) \neq K$, 因此 g 不可能是一一对应的映射, 由于 n 和 g 是任意的, 从而得出结论: $\mathbf{N}$

是无限的。

如果采用另一种定义,也许会对证明问题带来方便。

定义 3-7 如果存在一对一映射 $f:A \rightarrow A$,使得 $f(A) \subset A$ (即 $f(A)$ 是 A 的真子集),则集合 A 是无限的。若 A 不是无限的,它就是有限的。

例 3-5 (1) 自然数集 N 是无限的。(2) 实数集 R 是无限的。

证明: (1) 设映射 $f:N \rightarrow N$ 定义为 $f(x) = 2x$,显然 f 是一一对一映射,而且 $f(N) \subset N$,所以 N 是无限的。

(2) 令映射 $f:R \rightarrow R$,其中:

$$f(x) = x + 1 \quad \text{当 } x \geq 0$$

$$f(x) = x \quad \text{当 } x < 0$$

这个 f 是一一对映射,而且 $f(R) = \{x | x \in R \text{ 且 } x \notin (0, 1)\}$,显然 $f(R) \subset R$ 。

对于有限集,基数就是它的元素个数;对无限集,规定自然集 N 的基数是 $\aleph_0$ (念作阿列夫零)*。

定义 3-8 如果存在一一对应的映射 $f:N \rightarrow A$,则称 A 的基数是 $\aleph_0$,即:

$$|A| = \aleph_0$$

凡是具有基数 $\aleph_0$ 的任意集合,称为可数无限集。

例 3-6 设 I 是正整数集合,则 $|I| = \aleph_0$ 。因为 $f:N \rightarrow I_+$ 可定义为 $f(x) = x + 1$,此时 f 是一一对应的映射。另外 $|I| = \aleph_0$ 因为 $f:N \rightarrow I$ 定义为:

$$f(x) = \begin{cases} \frac{x}{2} & \text{当 } x \text{ 为偶数} \\ -\frac{x+1}{2} & \text{当 } x \text{ 为奇数} \end{cases}$$

此时 f 是一一对应的映射。

* $\aleph_0$ 为希伯来文第一个字母,此符号为数学家 Cantor 所引用。

我们把有限集或具有基数 $\aleph_0$ 的无限集统称为可数的,否则称为不可数的,可数的基本意思是:对于有限集,其中元素与 $\{0,1,\cdots,n-1\}$ 中元素可依次建立一一对应关系;对无限集,其中元素与 $\{0,1,2,\cdots\}$ 中元素可依次建立一一对应关系。

上面的例子是直接给出函数的解析式方法,亦可用枚举的方法找出集合 A 与 $N_n=\{0,1,2,\cdots,n-1\}$ 或 N 的一一对应关系。

例 3-7 字母集 $\{a,b,c,\cdots,z\}$ 有基数 26,因为我们可以建立从 $\{a,b,c,\cdots,z\}$ 到 N_{26} 的一一对应映射如下:

$$\begin{array}{ccccccc} a, & b, & c, & \cdots, & z \\ \uparrow & \uparrow & \uparrow & & \uparrow \\ 0, & 1, & 2, & \cdots, & 25 \end{array}$$

例 3-8 证明 $N\times N$ 是可数的。

证明: 我们先把 $N\times N$ 中的元素按一定规则排出来,见图 3-5,其中水平线上方及垂直线左方的是自然数。

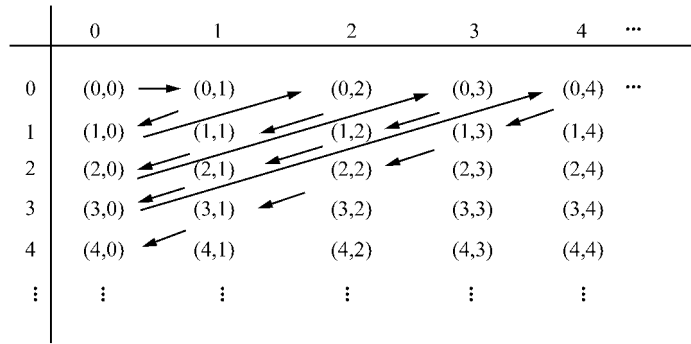


图 3-5 $N\times N$ 的排列图

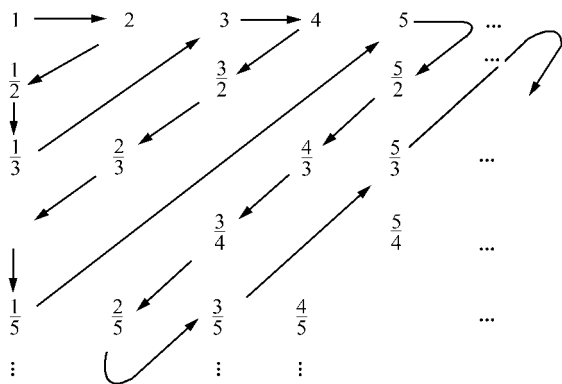
按箭头所指方向排列,就可以把任意 $(x,y)\in N\times N$ 与一个自然数建立对应关系,而且有函数关系如下:

$$f(m,n)=(m+n+1)(m+n)/2+m$$

例 3-9 有理数 Q 是可数的,为了证明这个结论,按下述方法列

1	2	3	4	5...
$\frac{1}{2}$	$\frac{2}{2}$	$\frac{3}{2}$	$\frac{4}{2}$	$\frac{5}{2}$...
$\frac{1}{3}$	$\frac{2}{3}$	$\frac{3}{3}$	$\frac{4}{3}$	$\frac{5}{3}$...
$\frac{1}{4}$	$\frac{2}{4}$	$\frac{3}{4}$	$\frac{4}{4}$	$\frac{5}{4}$...
$\frac{1}{5}$	$\frac{2}{5}$	$\frac{3}{5}$	$\frac{4}{5}$	$\frac{5}{5}$...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$...

然后按下面箭头路线表示出来,见图 3-6。



于是,得到正有理数序列如下:

$$1, 2, \frac{1}{2}, \frac{1}{3}, 3, 4, \frac{3}{2}, \frac{2}{3}, \frac{1}{4}, \frac{1}{5}, 5, \dots$$

• 54 •

0 1, -1, 2, -2, $\frac{1}{2}$, $-\frac{1}{2}$, $\frac{1}{3}$, $-\frac{1}{3}$, 3, -3, 4, -4 ...

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

0 1 2 3 4 5 6 7 8 9 10 11 12 ...

对于任意两个集合,特别是无限集,如何来比较它们的基数呢?
为此我们要引进两个集合基数的 size 问题。

定义 3-9 设 A 和 B 是两个任意集合:

(1) 若它们之间存在一一对应映射 $f: A \rightarrow B$, 则称 A 和 B 的基数“相同”,或者说它们属于同一个基数类,记以 $|A| = |B|$ 。

(2) 若从 A 到 B 存在一对一映射 $f: A \rightarrow B$, 则称 A 的基数“小于或等于” B 的基数,记以 $|A| \leq |B|$ 。

(3) 若 $|A| \leq |B|$ 且 $|A| \neq |B|$, 则称 A 的基数“小于” B 的基数,记以 $|A| < |B|$ 。

下面两条定理,刻划了两个任意集合的基数之间的关系,它非常重要,但不作证明。

定理 3-6 设 A 和 B 是两个集合,则 $|A|$ 和 $|B|$ 必定满足下述三条中的一条:

(1) $|A| < |B|$

(2) $|B| < |A|$

(3) $|A| = |B|$

定理 3-7 设 A 和 B 是集合,若 $|A| \leq |B|$ 而且 $|B| \leq |A|$, 则 $|A| = |B|$ 。

因此,若要证明两个集合有相同基数,只要找到两个一对一映射: $f: A \rightarrow B, g: B \rightarrow A$ 。我们知道找一对一映射要比找一一对应映射容易,这就给证明问题带来了方便。

由第一章,我们已经知道,对任何一个有限集合 A , 其基数小于其幂集的基数,即若 $|A| = m$ 有 $|\rho(A)| = 2^m > m$, 即 $|A| < |\rho(A)|$ 。

下面的问题是如果 A 是无限集,是否能得出同样的结论?事实上对无限集 A , $|A| < |\rho(A)|$ 也成立。详细证明留给读者自证。

因此对任意一个无限集 A , 至少存在一个集合 (譬如就是 $\rho(A)$), 其基数比 A 的基数大, 特别是总存在一个集合, 它的基数比自然数集 N 的基数大, 因此总存在一些集合是不可数的。

定理 3-8 集合 $\tilde{R} = \{r | r \in R, 0 < r < 1\}$ 是不可数的。

证明: $\tilde{R}$ 的每个元素可以写成一个十进制小数 $s_i = 0. r_{i1} r_{i2} r_{i3} \dots$ 。其中 $r_{ij} \in \{0, 1, \dots, 9\}, i, j \in N$, 假定 $\tilde{R}$ (它是无限的) 是可数的, 所以存在一一对应的映射, $f: \tilde{R} \rightarrow N$, 对每个 $n \geq 0$, 令实数 $s_n = 0. r_{n1} r_{n2} r_{n3} \dots$ 的象是 n , 因此这个 f 是由下面定义的:

$$\begin{array}{ccc} s_0 & s_1 & s_2 \dots \\ \downarrow & \downarrow & \downarrow \\ 0 & 1 & 2 \dots \end{array}$$

下面考虑另一个实数 $\bar{s} = 0. \bar{r}_{11} \bar{r}_{22} \bar{r}_{33} \dots$, 其中 $\bar{r}_{ii}$ 是任意一个不同于 r_{ij} 的十进制数, 如可取 $\bar{r}_{ii} = 9 - r_{ii}$, 因此 $\bar{s}$ 不同于任意一个 s_i , 不可能成为 f 的定义域中的元素, 所以从 $\tilde{R}$ 到 N 的一一对应映射不可能存在。

因此 $\tilde{R}$ 是不可数的, 并且定义其基数是 C 。

我们怎样从 $\tilde{R}$ 的不可数推广到实数集 R 也不可数呢? 事实上

$$f(x) = \begin{cases} \frac{1}{2x} - 1 & \text{当 } 0 < x \leq \frac{1}{2} \\ \frac{1}{2(x-1)} + 1 & \frac{1}{2} \leq x < 1 \end{cases}$$

是从 $\tilde{R}$ 到 R 的一一对应映射。所以 $\tilde{R}$ 和 R 是基数相同的, 即 R 的基数也是 C , 说明实数集 R 是不可数的。需说明的是 $\rho(N)$ 的基数也是 C 。

因此 C 是比 $\aleph_0$ 更高一级的基数。人们自然会想起, 是否会在不同于基数 $\aleph_0$ 和 C 的其他无限集, 使得它们的基数能排成一定的次序呢? 关于这一点的讨论已经超出本书的范围, 在此不作深入的讨论。

2. 计算机中空间与时间的无限性

计算机能存储数据, 它有存储数据的存储单元。这些存储单元包括内存、外存以及寄存器等所有一切存储实体。我们称它们为计

算机的存储空间。计算机的存储空间有一定的特性：

(1) 计算机的存储空间是有基本单位的。在计算机中存储数据的最基本单位是一个二进位数据,这种单位叫“位”或叫“比特(bit)”。没有比这更小的单位了,因此,它是最基本的单位。由于在计算机中它的对外界面是字(word)。一般,一个字可由若干个比特组成,它们可以是八个、十六个、二十四个、三十二个等。因此,有时也可用字作为存储空间的基本单位。此外还有用字节(byte)(一个字取4、8、16或32个比特)作为基本单位的。

存储空间存在基本单位这个事实告诉我们,在计算机中存储空间是离散的、可数的。

(2) 计算机存储空间的大小。计算机的存储空间到底有多大?是有限还是无限(可数无限)?这个问题我们得从存储器谈起。我们知道,计算机的内存、寄存器等等一般都是有相对固定数量的,因此,它们都是有限的。计算机的外存则情况就有点不同了,我们可以将它们分成为两部分来讨论:

① 对于固定的磁盘盘片,它们的容量也是有限的。

② 对于磁带、活动的磁盘盘片,则情况就有所不同了。因为虽然对于每盘磁带或每片盘片的存储空间都是固定的,但是,由于它们都是活动的,一台磁带机可以在一盘磁带存储满后再换上一盘空磁带继续存储,这样,一台磁带机的可存储容量就不再是固定的了。从理论上讲,它可以存储任意多的数据量,因此,它的存储容量是可数无限。当然,在实际上人类也无法搜集可数无限多个数据,当今世界也没有可数无限多盘磁带,我们也没有这么无限多的时间去存储这么多的数据,因此,一般这种可数无限我们称为潜在的可数无限。即指,它是在理论上的可数无限,而实际上并没有实现,但它的确可以存储任意多的数据量。对可装活动盘片的磁盘也有类似的情况。

因此,总的来说,计算机的存储空间是可数无限。

其次,我们讨论计算机中的时间概念。计算机中的时间也有一定特性:

(3) 计算机中的时间是有基本单位的,它的基本单位是主频的一个周期。因此,计算机中的时间概念与一般的所谓时间概念不同,计算机中的时间是离散的、可数的。在计算机的时间概念中可以存在一个起始时间,这个起始时间一般可用 $t=0$ 表示。

(4) 计算机中时间的长短。从理论上讲,任一台计算机它可以计算任意大、任意复杂的算题,即它可以计算在时间上任意长的算题,这就是说,计算机的时间可以是可数无限的。当然,世界上现存的计算机,哪怕速度相当快,譬如说每秒钟可以运行上亿次、几十亿次的计算机,实际上由于各种物理上的原因,它们也远远无法计算任意长的时间。而且即使它们确能计算时间上任意长的算题,但可能哪一代人也都无法亲眼目睹其全过程。因此,这种时间上的可数无限也是潜在的可数无限。

计算机中空间和时间的可数无限性是计算机理论的一个极其重要基础。它告诉我们计算机所能处理的信息以及时间的幅度的范围是可数集,即有限集或可数无限集。

习 题 三

3.1 下面的关系哪一个构成函数?

$$(1) \{(n_1, n_2) \mid n_1, n_2 \in \mathbf{N}, n_1 + n_2 < 10\}$$

$$(2) \{(r_1, r_2) \mid r_1, r_2 \in \mathbf{R}, r_2 = r_1^2\}$$

$$(3) \{(r_1, r_2) \mid r_1, r_2 \in \mathbf{R}, r_2^2 = r_1\}$$

$$(4) \{(n_1, n_2) \mid n_1, n_2 \in \mathbf{N}, n_2 \text{ 为小于 } n_1 \text{ 的素数的数目}\}$$

3.2 设映射

$$f: 2^U \times 2^U \rightarrow 2^U$$

其中 $f(S_1, S_2) = S_1 \cap S_2, S_1, S_2 \in 2^U$,

证明: f 的陪域和值域相等。

3.3 下面哪一个是一一对映射、满射或一一对应映射?

$$(1) f: \mathbf{N} \rightarrow \mathbf{R}, \text{ 其中 } f(n) = \log_{10} n + 1$$

- (2) $f: \mathbf{N} \rightarrow \mathbf{R}$, 其中 $f(n) = \sqrt{n}$
 (3) $f: \mathbf{R} \rightarrow \mathbf{R}$, 其中 $f(r) = 2r - 15$
 (4) $f: \mathbf{R} \rightarrow \mathbf{R}$, 其中 $f(r) = r^2 + 2r - 15$
 (5) $f: \mathbf{N} \rightarrow \mathbf{N}$, 其中 $f(n_1, n_2) = n_1 n_2$
 (6) $f: 2^U \times 2^U \rightarrow 2^U \times 2^U$,

其中 $f(S_1, S_2) = (S_1 \cup S_2, S_1 \cap S_2)$

3.4 A 和 B 是有限集合, 问有多少个不同的一对一映射 $f: A \rightarrow B$? 有多少个一一对应的映射?

3.5 设有映射 $f: A \rightarrow B, g: B \rightarrow C$, 证明:

- (1) 如果 $f \circ g$ 是一对一映射, 则 f 是一对一映射。
 (2) 如果 $f \circ g$ 是满射, 则 g 是满射。
 (3) 如果 $f \circ g$ 是一一对应映射, 则 f 是一对一映射, g 是满射。

3.6 证明定理 3-4。

3.7 如果 $f: A \rightarrow B, g: B \rightarrow C$ 都是一一对应映射,

证明: $(f \circ g) = \widetilde{g} \circ \widetilde{f}$

3.8 设 $A = \{a | a \in \mathbf{R}, a \geq 0\}, B = \{b | b \in \mathbf{R}, 0 \leq b \leq 1\}$, 试找一个 A 到 B 的满射。

3.9 设 $\varnothing$ 是 A 与 B 间的一一对应映射, 若 a 是 A 中的一个元素, 问:

$$\widetilde{\varnothing}[\varnothing(a)] = ? \quad \varnothing[\widetilde{\varnothing}(a)] = ?$$

若 $\varnothing$ 是 A 上的一一对应映射, 结论又是什么?

3.10 证明两个无限集合之交不一定是无限集合。

3.11 设 A 和 B 是无限集合, $B \subseteq A$, 问 $A - B$ 是否一定无限? 是否一定有限?

3.12 设 N 为自然数集, 证明 $|\rho(N)| = 2^{\aleph_0}$

3.13 设函数 f 和 g 分别为 $f(x) = 2x + 1, g(x) = x^2 - 2$, 试找出定义复合函数 $f \circ g$ 的数学公式。

3.14 设有三个映射如下:

- (1) $f: \mathbf{R} \rightarrow \mathbf{R}, f(x) = x$

$$(2) f: I \rightarrow N, f(x) = |x|$$

其中 $|x|$ 表示 x 的绝对值

$$(3) f: R \rightarrow R_+, f(x) = 2^x$$

问:

(1) 上述映射的象集是什么?

(2) 哪个映射有逆映射? 若有, 其表达式是什么?

3.15 实数集 R 上的函数是“……是取……的平方”, 这是 $R \rightarrow R$ 的()

- A. 映射 B. 一对一映射(入射)
C. 满射 D. 一一对应映射(双射)

3.16 举例说明, 并不是每个集合到自身的单射(一对一的映射)都是一一对应的(双射)。

3.17 $f: A \rightarrow A$ 为双射, $f^{-1}: A \rightarrow A$ 是 $f: A \rightarrow A$ 的逆映射, $a \in A, f(a) = b$, 下面不成立的式子为()

- A. $f^{-1}(f(a)) = a$ B. $f(f^{-1}(b)) = b$
C. $f(f^{-1}(a)) = f^{-1}(f(a))$ D. $f(f^{-1}(a)) \neq f^{-1}(f(a))$

3.18 集合 A 和 B 之间存在一一对应映射 $f: A \rightarrow B$, 则下面关于基数的式子成立的是()

- A. $|A| = |B|$ B. $|A| > |B|$ C. $|A| < |B|$ D. $|A| \neq |B|$

3.19 $f: A \rightarrow B, g: B \rightarrow C$ 是两个一对一映射, 复合映射 $f \circ g: A \rightarrow C$ 满足()

- A. $f \circ g$ 是满射 B. $f \circ g$ 是一一对应映射
C. $f \circ g$ 是一一对一映射 D. $f \circ g$ 不一定是 A 或 B 或 C

“映射与无限集”复习提纲

1. 主要内容

——映射基本概念。

- 映射的运算。
- 映射的性质。
- 无限集基本概念。
- 几种常用的无限集。

2. 复习重点

- 映射的基本概念。
- 无限集的分级。

3. 映射基本概念及其运算

——映射:映射 $f:A \rightarrow B$ 表示对 A 中每个元素 a 都能在 B 中找到惟一元素与之对应,也可记为 $f(a)=b$ 。

——关系与映射:映射 $f:A \rightarrow B$ 是一种特殊关系,它满足:

• A 中每个元素均出现在关系中(作为关系有序偶的第一个分量)。

- 如果 $f(a)=b, f(a)=c$ 则 $b=c$ 。

——三种映射:

- 一对一映射: $f(ai)=f(aj)$ 则 $ai=aj$ 。
- 满射: $f(A)=B$ 。
- 一一对应映射:一对一映射又是满射。

——映射的两种运算:

- 映射的复合运算: $f:A \rightarrow B, g:B \rightarrow C$ 则复合运算: $f \circ g:A \rightarrow C$, 其中 $f \circ g(a)=g(f(a))$ 。
- 映射的逆运算: $f:A \rightarrow B$ 则逆运算: $\tilde{f}:B \rightarrow A$ 。

——映射的两个性质:

• $f \circ g$ 是映射的复合,如 f, g 满射(一对一,一一对应)则 $f \circ g$ 也是满射(一对一,一一对应)。

- $f:A \rightarrow B$ 有逆映射 $\Leftrightarrow f$ 是一一对应的。

4. 无限集

——无限集的两个定义：

- $f: N_n \rightarrow A$ 一一对应则 A 为有限集；否则是无限集。
- $f: A \rightarrow A$ 使得 $f(A) \subset A$, 则 A 为无限集；否则是有限集。

——可数无限集：

- 自然数集 N 是无限的。

$: N \rightarrow A$ 是一一对应, A 也是无限的, 且称为可数无限, 其基数为 $\aleph_0$ 。

- Q 是可数无限。

——不可数无限集: R 是不可数无限集, 其基数为 C 。

——无限集的基数：

- 基数相等: $f: A \rightarrow B$ 一一对应, 则称 $|A| = |B|$ 。
- 基数不等: $f: A \rightarrow B$ 一对一, 则称 $|A| \leq |B|$ 。
: $|A| \leq |B|$ 且 $|A| \neq |B|$ 则称 $|A| < |B|$ 。
- $|A| < |\rho(A)|$ 。

——无限集分级(按基数分级)

- 可数无限集 $\aleph_0$ 。
- 实数集 C 。
- 更大基数的集: $\rho(A)$ 。

第四章 近世代数

4.1 代数运算

代数是一门研究运算的科学,在代数中其运算对象是集合中的元素,图 4-1(a)和(b)的运算可以看作两只“黑盒子”,它具有各种输入和一个输出。

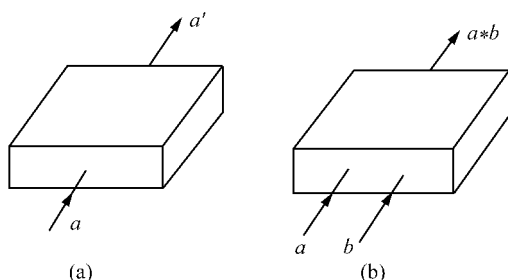


图 4-1 代数运算

其中(a)有一个输入 a ,产生一个输出 a' ,我们称它为一元运算,(b)有两个输入 a 和 b ,产生一个输出 $a*b$,我们称它为二元运算。一般而言:

集合 S 上的一元运算实际上是从 S 到 S 的一个特殊映射,如集合论中的取补运算,命题演算中的非运算,数字逻辑电路中的延迟元件都是一元运算的例子。

集合 S 上的二元运算实际上是从 $S \times S$ 到 S 的一个特殊映射,如实数集合上的加法和乘法分别是两个二元运算。

推而广之,集合 S 上的 m 元运算实际上是从 S^m 到 S 的一个特殊映射,显然 $m=1$ 或 2 分别是上述的一元、二元运算。

我们主要研究的是二元运算,也会遇到一元运算,并用 $a * b$ 表示在映射下有序偶 (a, b) 的象, $*$ 、 $\circ$ 、 $+$ 、 $\times$ 等等是常用的二元运算符号。

例如, $N = \{0, 1, 2 \cdots\}$ 是自然数集合,在 N 上的普通 $+$ 和 $\times$ 是二元运算,因为对任意 $a, b \in N, a + b \in N, a \times b \in N$,但是减法则不是 N 上的二元运算,因为 $1 - 2 \notin N$,在实数集 R 上的普通 $+$ 、 $\times$ 和 $-$ 均是 R 上二元运算,但是除则不是,因为除数为零无定义。

对于一个有限集上的运算可用表格定义,如 $A = \{1, 2, 3\}$,则下表定义了一个二元运算 $*$,其 $x * y$ 是指位于 x 行、 y 列的元素,如 $2 * 3 = 2, 3 * 2 = 1$ 。

$*$	1	2	3
1	2	1	1
2	3	1	2
3	3	1	2

接着我们要定义一元运算和二元运算的封闭性。
定义 4-1 设 Δ 和 $*$ 是分别定义在 A 上的一元运算和二元运算。若 S 是 A 的子集,并且有:

- (1) 如果 $a \in S$,有 $\Delta a \in S$,则称 S 关于 Δ 运算是封闭的。
- (2) 如果 $a, b \in S$,有 $a * b \in S$,则称 S 关于 $*$ 运算是封闭的。

例如 I 是整数集合, I_+ 是正整数集合,显然 $I_+ \subset I$,则 I_+ 在加法运算和乘法运算之下是封闭的,在 I_+ 上的减法运算是不封闭的。

根据运算的定义,我们可以得到结论:定义在某个集合上的运算对它自身集合总是封闭的。

封闭性的定义可推广到 m 元运算。
 二元运算可有下面的一个或若干个性质。在以下各节中,除非特别说明,我们所讲的运算均指二元运算。

1. 结合律

定义 4-2 设 $*$ 是集合 S 上的运算, 如果对每个 $a, b, c \in S$, 有:

$$a * (b * c) = (a * b) * c$$

则称 $*$ 满足结合律。

2. 交换律

定义 4-3 设 $*$ 是集合 S 上的运算, 如果对每个 $a, b \in S$, 有:

$$a * b = b * a$$

则称 $*$ 满足交换律。

3. 单位元素

定义 4-4 设 $*$ 是集合 S 上的运算, 如果有 $e \in S$, 而且对每个 $x \in S$ 有:

$$e * x = x * e = x$$

则称 e 是关于运算 $*$ 的单位元素(或叫恒等元素)。

4. 零元素

定义 4-5 设 $*$ 是集合 S 上的运算, 如果有 $\theta \in S$, 而且对每个 $x \in S$, 有:

$$\theta * x = x * \theta = \theta$$

则称 θ 是关于运算 $*$ 的零元素。

有时我们把单位元素分成左单位元素和右单位元素, 把零元素分成左零元素和右零元素, 为此我们给出如下定义。

定义 4-6 设 $*$ 是集合 S 上的运算, 如有 $e_l \in S$, 而且对每个 $x \in S$, 有:

$$e_l * x = x$$

则称 e_l 是关于运算 $*$ 的左单位元素。

如有 $e_r \in S$, 而且对每个 $x \in S$, 有:

$$x * e_r = x$$

则称 e_r 是关于运算 $*$ 的右单位元素。

如果有 $\theta_l \in S$, 而且对每个 $x \in S$ 有:

$$\theta_l * x = \theta$$

则称 θ_l 是关于 $*$ 的左零元素。

如有 $\theta_r \in S$, 而且对每个 $x \in S$ 有:

$$x * \theta_r = \theta_r$$

则称 θ_r 是关于运算 $*$ 的右零元素。

有时左右单位元素可不同时存在, 但当同时存在时, 则有 $e_l = e_r$ 。

左右零元素也可不同时存在, 但当同时存在时, 则有 $\theta_l = \theta_r$ 。这一重要性质可用下面的定理来刻画。

定理 4-1 设 $*$ 是集合 S 上的一个运算, 具有左、右单位元素, 则:

$$e_l = e_r$$

证明: 因为 e_l 和 e_r 分别是左、右单位元素, 所以:

$$e_r = e_l * e_r = e_l$$

定理 4-2 设 $*$ 是集合 S 上的运算, 具有左零元素和右零元素, 则:

$$\theta_l = \theta_r$$

证明: 因为 θ_l 和 θ_r 分别是左右零元素, 所以:

$$\theta_r = \theta_l * \theta_r = \theta_l$$

注意, 单位元素和零元素在代数系统中占十分重要的地位, 必须对它的性质透彻了解。除非特别说明, 下面所讲单位元素, 均指左右单位元素都存在的情况, 即 $e_l = e_r = e$, 所讲零元素是指左右零元素都存在的情况, 即 $\theta_l = \theta_r = \theta$ 。

定理 4-3 对运算 $*$, 如果单位元素存在, 则是惟一的, 如果零

元素存在,则是惟一的。

证明: 反证法,如果有两个单位元素,不妨设 e 和 e' , 因为 e 是单位元素, 所以有 $e * e' = e' * e = e'$, 又因为 e' 是单位元素, 所以也有 $e * e' = e' * e = e$, 所以 $e = e'$ 。

对零元素的惟一性证明可用类似的方法。留给读者自己证明。

5. 逆元素

定义 4-7 设 $*$ 是集合 S 上的一个运算, 且有单位元素 $e \in S$, 如果对每个 $x \in S$, 存在 $y \in S$, 使:

$$x * y = y * x = e$$

则称 y 是 x 的逆元素, 记以 x^{-1} 。

逆元素是相互的, 即 x 是 y 的逆元素, y 也是 x 的逆元素。

读者可以证明, 任一元素 a 之逆元素若存在则是惟一的。

6. 分配律

定义 4-8 如果 $*$ 和 $\circ$ 是集合 S 上的两个运算, 如果对任意 $a, b, c \in S$, 有:

$$a \circ (b * c) = (a \circ b) * (a \circ c)$$

$$(b * c) \circ a = (b \circ a) * (c \circ a)$$

则称 $\circ$ 对 $*$ 满足分配律。

例 4-1 例如 $\circ$ 和 $*$ 是集合 A 上的两个运算, 并且 $*$ 满足结合律, $\circ$ 对 $*$ 满足分配律, 则:

$$\begin{aligned} & (a_1 \circ b_1) * (a_1 \circ b_2) * (a_2 \circ b_1) * (a_2 \circ b_2) \\ &= (a_1 \circ b_1) * (a_2 \circ b_1) * (a_1 \circ b_2) * (a_2 \circ b_2) \end{aligned}$$

证明:

$$\begin{aligned} & (a_1 \circ b_1) * (a_1 \circ b_2) * (a_2 \circ b_1) * (a_2 \circ b_2) \\ &= (a_1 \circ (b_1 * b_2)) * (a_2 \circ (b_1 * b_2)) = (a_1 * a_2) \circ (b_1 * b_2) \\ &= ((a_1 * a_2) \circ b_1) * ((a_1 * a_2) \circ b_2) \\ &= (a_1 \circ b_1) * (a_2 \circ b_1) * (a_1 \circ b_2) * (a_2 \circ b_2) \end{aligned}$$

4.2 代数系统

代数中的运算对象是集合中的元素,在早先的代数中,这些元素一般都是数字,它可以是整数、实数和复数,历史上称为古典代数。后来,数学工作者逐渐认识到,元素不仅可以是数字,事实上还可以是很多其他东西。这些东西可以是抽象的,也可以是具体的。因此出现了近世代数,亦叫抽象代数、代数结构或代数系统的概念。

简单地说,一个集合及定义在这个集合上的一个或多个(封闭)运算(主要讨论一元和二元的)一起称为一个代数系统。设集合 S 及其运算 $*$, $\circ$, $\dots$, 于是我们用记号 $(S, *, \circ, \dots)$ 表示一个代数系统。例如,整数集 I 上定义了通常加(+),乘($\times$)和减($-$),则 $(I, +)$, $(I, -)$, $(I, \times)$, $(I, +, -)$, $(I, +, \times)$, $(I, -, \times)$, $(I, +, -, \times)$ 均是代数系统,而 $(I, \div)$ 不是代数系统,因为除($\div$)不是 I 上的二元运算,若 R 是除了零的实数集,那么 $(R, \div)$ 是一个代数系统,因为 $\div$ 是 R 上的一个二元运算。

设 $(A, *, \circ, \dots)$ 是代数系统,若 A 的基数是有限的,则称它是有限代数系统,反之是无限代数系统。

为了研究一个代数系统,有时要求考察其子代数系统,我们就 $(S, *, \triangle)$ 及 $(S', *', \triangle')$ 形式的两个代数系统给出其定义。

定义 4-9 设 $(S, *, \triangle)$ 和 $(S', *', \triangle')$ 是两个代数系统, $*$ 和 $*'$ 均是二元运算, $\triangle$ 和 $\triangle'$ 均是一元运算,若:

(1) $S' \subseteq S$,

(2) 对任意 $a, b \in S'$, 有 $a * b = a *' b \in S'$, $\triangle a = \triangle' a \in S'$ 则称 $(S', *', \triangle')$ 是 $(S, *, \triangle)$ 的子代数系统。

对于 S 和 S' 上运算符号少于二个或多于二个的情况,可用类似上面方法给出相应的子代数系统的定义。

在本章中,我们将研究若干种特定的代数系统,主要是半群、单元半群、群、环和域,它们具有图 4-2 的层次关系。

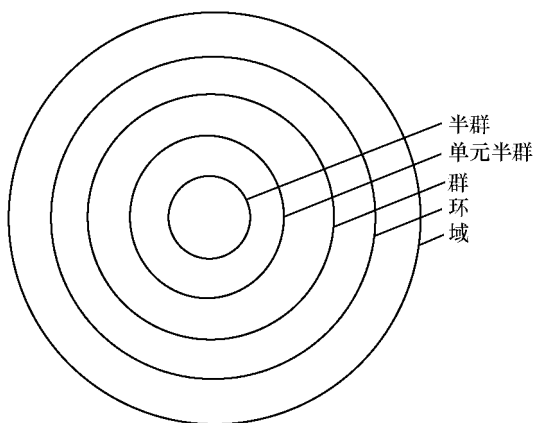


图 4-2 各种代数系统的层次图

4.3 同态和同构

为了对代数系统进行比较,研究它们之间的关系要利用同态和同构作为工具,在下面考虑各种具体的代数系统时,经常会用到它,因此先引进这预备概念。为简单起见,我们先考虑仅具有一个二元运算符的代数系统的情况。

定义 4-10 设 $(S, \circ)$ 和 $(T, *)$ 是两个代数系统,如果存在一个映射(即函数) $f: S \rightarrow T$,使得对每个 $a, b \in S$,有:

$$f(a \circ b) = f(a) * f(b)$$

则称 f 是从 $(S, \circ)$ 到 $(T, *)$ 的同态映射,简称同态,此时亦称 $(S, \circ)$ 和 $(T, *)$ 是同态的。

由于 f 可以是 S 到 T 的内射,亦可以是 S 到 T 的满射,亦可以是 S 到 T 的一一对应映射(即双射),因此我们可进一步规定:

设 $(S, \circ)$ 和 $(T, *)$ 是两个代数系统,如果存在一个从 S 到 T 的满射 f ,使得对任意 $a, b \in S$,有:

$$f(a \circ b) = f(a) * f(b)$$

则称 f 是从 $(S, \circ)$ 到 $(T, *)$ 的满同态, 此时亦称 $(S, \circ)$ 和 $(T, *)$ 是满同态的。

定义 4-11 设 $(S, \circ)$ 和 $(T, *)$ 是两个代数系统, 如果存在一一对应的映射 $f: S \rightarrow T$, 使得对任意 $a, b \in S$, 有:

$$f(a \circ b) = f(a) * f(b)$$

则称 f 是从 $(S, \circ)$ 到 $(T, *)$ 的同构映射, 简称同构, 此时亦称 $(S, \circ)$ 和 $(T, *)$ 是同构的, 并记以 $(S, \circ) \cong (T, *)$ 。

特殊情况, 如果 $S = T$, 且 f 是同构的, 则称 f 是自同构。

从上面定义可看出, 同构的条件最强, 其次是满同态, 再其次是同态。它们三者之间关系可用图 4-3 刻划。

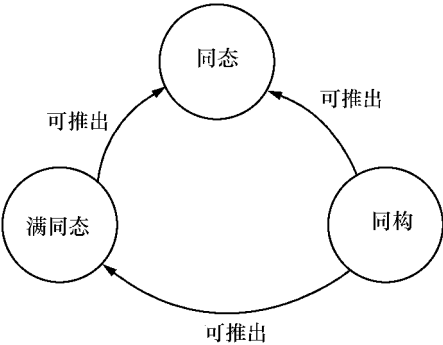


图 4-3 同构、满同态与同态间的关系图

推而广之, 若两个代数系统包含有限多个运算, 比如说都是 k 个, 即 $(S, \circ_1, \circ_2, \dots, \circ_k)$ 和 $(T, *_1, *_2, \dots, *_k)$, 则要对每个运算均满足以下条件:

$$\begin{aligned} f(a \circ_1 b) &= f(a) *_1 f(b) \\ f(a \circ_2 b) &= f(a) *_2 f(b) \\ &\vdots \\ f(a \circ_k b) &= f(a) *_k f(b) \end{aligned}$$

此时才称 f 是同态或同构。

例 4-2 设 R 和 R_+ 分别是实数和正实数的集合, 于是 $(R, +)$ 和 $(R_+, \cdot)$ 是两个代数系统, 其中 $+$ 和 $\cdot$ 分别是普通的加和乘运算, 证明 $(R, +)$ 和 $(R_+, \cdot)$ 是同构的。

证明: 令 $f: R \rightarrow R_+, f(x) = e^x$

(1) $f: R \rightarrow R_+$ 是一一对应的映射。因为对任何 $x_1, x_2 \in R$, 如果 $x_1 \neq x_2$, 则有 $e^{x_1}, e^{x_2} \in R_+$ 且 $e^{x_1} \neq e^{x_2}$, 所以 $f(x_1) \neq f(x_2)$, 又对每个 $x \in R_+$, 有 $\ln x \in R$ 。

(2) $f(x_1 + x_2) = e^{x_1 + x_2} = e^{x_1} \cdot e^{x_2} = f(x_1) \cdot f(x_2)$, 故 f 是从 $(R, +)$ 到 $(R_+, \cdot)$ 的同构, 即 $(R, +) \cong (R_+, \cdot)$ 。

例 4-3 设 R 是有理数集, R 上的运算是普通加法, S 是不等于零的有理数集, S 上的运算是普通乘法, 所以 $(R, +)$ 和 $(S, \cdot)$ 是两个代数系统, 问 $(R, +)$ 和 $(S, \cdot)$ 之间有无同构映射。

解: 设有同构映射 $\varphi: R \rightarrow S$, 因为 $\varphi(0) = \varphi(0 + 0) = \varphi(0) \cdot \varphi(0)$ 且 $\varphi(0) \neq 0$ 。故 $\varphi(0) = 1$ 。设 $\varphi(a) = -1$, $\varphi(a + a) = (-1) \cdot (-1) = 1$ 故 $a + a = 0, a = 0$, 从而 $\varphi(0) = -1$, 矛盾。所以从 $(R, +)$ 到 $(S, \cdot)$ 无同构映射存在。

例 4-4 设 R 是实数集合, S 是 R 的子集, R 上的运算是普通乘法, 问以下的映射 f 是否为从 $(R, \cdot)$ 到 $(S, \cdot)$ 的同态? 若是同态是否为满同态?

(1) $x \rightarrow 2x$

解: 不是同态。因为有 $x_1, x_2 \in R$, 且有:

$$f(x_1 \cdot x_2) = 2(x_1 \cdot x_2) \neq f(x_1) \cdot f(x_2)$$

(2) $x \rightarrow x^2$ (注: $x^2 = x \cdot x$)

解: 是同态。 $S = \{y | y \geq 0 \text{ 的实数} \}$ 。映射 $f: R \rightarrow S, f(x) = x^2$ 。对每个 $x_1, x_2 \in R$, 有:

$$\begin{aligned} f(x_1 \cdot x_2) &= (x_1 \cdot x_2)^2 = (x_1 \cdot x_2) \cdot (x_1 \cdot x_2) \\ &= (x_1 \cdot x_1) \cdot (x_2 \cdot x_2) = f(x_1) \cdot f(x_2) \end{aligned}$$

又对每个 $y \in S$, 有 $x \in R$, 使得:

$$f(x) = x^2 = y$$

所以是满同态的。

$$(3) x \rightarrow -x$$

解: $f(x) = -x$, 但:

$$f(x_1 \circ x_2) = -(x_1 \circ x_2) \neq f(x_1) \circ f(x_2)$$

所以 $f: R \rightarrow S$ 不是同态映射。

在同态和同构的定义中,把“代数系统”四个字换成“半群”或“单元半群”或“群”,就分别得出半群同态和同构,单元半群同态和同构,群同态和同构的概念。这些概念特别是群同态和同构在下面各节中常会遇到。

下面讨论各种具体的代数结构。

4.4 半群和单元半群

在数学或自动机理论中,在语言和程序设计的数学研究中,有时只要求代数系统具有结合律的运算,或具有结合律及单位元素的运算。

定义 4-12 设 $(A, \circ)$ 是一个代数系统,如对任意 $a, b, c \in A$, 有 $a \circ (b \circ c) = (a \circ b) \circ c$, 则称 $(A, \circ)$ 是半群。

半群的条件最弱,它只要求满足结合律。

定义 4-13 设 $(M, \circ)$ 是一个代数系统,如果:

(1) 对每个 $a, b, c \in M$, 有 $a \circ (b \circ c) = (a \circ b) \circ c$ (结合律)。

(2) 存在一个单位元素 $e \in M$, 即对每个 $a \in M$, 有 $a \circ e = e \circ a = a$ 。

则称 $(M, \circ)$ 是一个单元半群。

如果单元半群 $(M, \circ)$ 的运算 $\circ$ 也满足交换性质,即对每个 $a, b \in M$, 有 $a \circ b = b \circ a$, 则又称 $(M, \circ)$ 是交换单元半群。

例如,设 N, I, Q 分别代表自然数、整数和有理数集, $+$ 和 $*$ 代表普通加法和乘法, 则 $(N, +)$ 、 $(N, *)$ 、 $(I, +)$ 、 $(I, *)$ 、 $(Q, +)$ 、 $(Q, *)$ 均是交换单元半群, 但是 $(I, -)$ 不是半群, 因为 $a - (b - c) \neq (a - b) - c$ 。

我们把从一个集合到它自身集合上的一个映射称为一个变换。

定理 4-4 设 A 是任一集合, 令 $A^A = \{f \mid f: A \rightarrow A\}$ 是从 A 到 A 的所有变换的集合, 则 $(A^A, \circ)$ 是一个单元半群, 称为 A 的变换单元半群, 这里 $\circ$ 为复合运算。

证明 如 $f, g \in A^A$, 则复合 $f \circ g \in A^A$ 。又映射之复合总是满足结合律的, 因为如果 $f, g, h \in A^A$, 则对每个 x , 有:

$$f \circ (g \circ h)(x) = h(g(f(x)))$$

而: $(f \circ g) \circ h(x) = h(f \circ g(x)) = h(g(f(x)))$

其单位元素是映射 E_A 。

所以 $(A^A, \circ)$ 是一个单元半群。

例 4-5 如果 $A = \{0, 1\}$, 写出 A 的变换单元半群 $(A^A, \circ)$ 的表。

解: 变换集合有 4 个元素, e, f, g, h , 定义如下:

$$e(0) = 0 \quad f(0) = 0 \quad g(0) = 1 \quad h(0) = 1$$

$$e(1) = 1 \quad f(1) = 0 \quad g(1) = 0 \quad h(1) = 1$$

其表如下:

$*$	e	f	g	h
e	e	f	g	h
f	f	f	h	h
g	g	f	e	h
h	h	f	f	h

在任何一个具有单位元素 e 的单元半群 $(M, \circ)$ 中, 任一元素 $a \in M$ 的幂定义如下:

$$(1) a^0 = e$$

$$(2) a^{i+1} = a^i \circ a (i=0, 1, 2, \dots)$$

对任何两个非负整数 i 和 j , 有:

$$(1) a^i \circ a^j = a^{i+j}$$

$$(2) (a^i)^j = a^{i \times j}$$

在单元半群 $(M, \circ)$ 中任何一元素 $a \in M$, 如果 $a \circ a = a$, 称 a 是等

幂元素,由此可方便地扩充,对任何一个 $r \geq 2, a^r = a$ 。显然每个单元半群至少包含一个等幂元素——单位元素。

定义 4-14 一个单元半群 $(M, \circ)$, 如果包含一个元素 g , 使得对每个元素 $a \in M$, 可表示成:

$$a = g^r (r \geq 0)$$

则称 $(M, \circ)$ 是循环单元半群, 其中 g 是 $(M, \circ)$ 的生成元素。

定理 4-5 每个循环单元半群是可交换的单元半群。

证明: 令 $(M, \circ)$ 是循环单元半群, 其生成元素是 g , 如 $a, b \in M$, 则 a, b 可以写作 $a = g^i, b = g^j$
故 $a \circ b = g^i \circ g^j = g^{i+j} = g^{j+i} = g^j \circ g^i = b \circ a$

4.5 群 论

1. 群的概念

定义 4-15 一个代数系统 $(G, *)$, 如果:

(1) 运算 $*$ 满足结合律, 即对每个 $a, b, c \in G$, 有:

$$(a * b) * c = a * (b * c)$$

(2) 存在单位元素 $e \in G$, 即对每个 $a \in G$, 有:

$$e * a = a * e = a$$

(3) 每个元素 $a \in G$, 有其逆元素 $a^{-1} \in G$, 即 $a * a^{-1} = a^{-1} * a = e$ 则称代数系统 $(G, *)$ 是一个群。可简称为 G 是一个群。

如果运算 $*$ 还满足交换律, 即对每个 $a, b \in G$, 有 $a * b = b * a$, 则群 $(G, *)$ 称为交换群, 或阿贝尔群。

最熟悉的例子是 $(I, +)$ 、 $(R, +)$ 、 $(C, +)$ 都是在加法运算下的阿贝尔群, 又设 R^* 、 C^* 是除掉零的实数和复数集合, 那么 $(R^*, *)$ 和 $(C^*, *)$ 都是乘法意义下的阿贝尔群。

又如, $G = \{1, -1, i, -i\}$ 是复数集合, $*$ 是复数乘法, 则 $(G, *)$ 是阿贝尔群。结合律容易验证是成立的, 1 是单位元素, $1^{-1} = 1$,

$$(-1)^{-1} = -1, i^{-1} = -i, (-i)^{-1} = i.$$

例 4-6 设群 $(G, *)$ 对任意 $x \in G$, 有 $x * x = e$ (简记 $x^2 = e$), 则 $(G, *)$ 一定是阿贝尔群。

证明: 对任意 $a, b \in G, a * b = e * a * b * e$

$$\begin{aligned} &= b^2 * a * b * a^2 \\ &= b * (b * a) * (b * a) * a \\ &= b * (b * a)^2 * a \\ &= b * e * a \\ &= b * a \end{aligned}$$

故 $(G, *)$ 是阿贝尔群。

例 4-7 设 S 是所有 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 形式的矩阵 (即 2×2) 的集合, 其中

a, b, c, d 是有理数, 其运算是矩阵乘 $*$, 那么 $(S, *)$ 不是一个群, 因为 S 中任一元素的逆元素并不总存在, 但考虑 G 是具有非零行列式的 2×2 矩阵的集合, 则 $(G, *)$ 是一个群, 其单位元素是:

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

任一矩阵 $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 的逆矩阵是 $A^{-1} = \begin{pmatrix} d/|A| & -b/|A| \\ -c/|A| & a/|A| \end{pmatrix}$ (此处 $|A| = ad - bc$ 是行列式)。但 $(G, *)$ 不是阿贝尔群, 因为矩阵乘法不满足交换律。这是遇到的第一个非阿贝尔群的例子。

定义 4-16 在群 $(G, *)$ 中元素的数目 $|G|$, 称为群的阶, 如果 $|G|$ 有限, 称 $(G, *)$ 是有限群, 否则称为无限群。

我们知道, 两个代数系统同态或同构是一种映射, 这种映射保持它们的运算, 在群里, 它显得特别重要。

设 $(G, \circ)$ 和 $(H, *)$ 是两个群, $f: G \rightarrow H$ 是一个映射, 如果对每个 $a, b \in G$, 有:

$$f(a \circ b) = f(a) * f(b)$$

则称 f 是一个群同态映射, 简称群同态。

若上述的映射 $f: G \rightarrow H$ 是一一对应的映射, 而且对任意 $a, b \in G$, 有:

$$f(a \circ b) = f(a) * f(b)$$

则称 f 是一个群同构映射, 简称群同构, 此时亦称 $(G, \circ)$ 和 $(H, *)$ 同构, 记作:

$$(G, \circ) \cong (H, *)$$

如果两个群是相同的运算符号, 如 $(G, \circ)$ 和 $(H, \circ)$, 则条件改为:

$$f(a \circ b) = f(a) \circ f(b)$$

两个群同构实际上具有完全相同的性质。同态没有这个结论, 但是单位元素和逆元素在同态情况下也保持的。

定理 4-6 如果 $f: G \rightarrow H$ 是群同态, 则:

(1) $f(e_G) = e_H$, 其中 $e_G \in G, e_H \in H$, 这是两个单位元素。

(2) $f(a^{-1}) = f(a)^{-1}$, 其中 $a, a^{-1} \in G$ 。

(注: $f(a)^{-1}$ 意指 $[f(a)]^{-1}$)

证明:

$$(1) f(e_G) = f(e_G \circ e_G) = f(e_G) \circ f(e_G),$$

$$\text{所以: } f(e_G)^{-1} \circ f(e_G) = f(e_G)^{-1} \circ f(e_G) \circ f(e_G)$$

$$\text{即: } f(e_G) = e_H$$

$$(2) \text{ 对任意 } a \in G, a \circ a^{-1} = a^{-1} \circ a = e_G$$

$$e_H = f(e_G) = f(a \circ a^{-1}) = f(a) \circ f(a^{-1})$$

$$e_H = f(e_G) = f(a^{-1} \circ a) = f(a^{-1}) \circ f(a)$$

因此 $f(a^{-1})$ 是 $f(a)$ 的逆元素, 即 $f(a^{-1}) = f(a)^{-1}$

2. 群的性质

在这里, 我们将根据群的定义, 推出一般群所具有的基本性质。

定理 4-7 如果 $(G, *)$ 是一个群, 则对每个 $a, b \in G$, 有:

(1) 存在一个惟一的元素 $x \in G$, 使得 $a * x = b$ 。

(2) 存在一个惟一的元素 $y \in G$, 使得 $y * a = b$ 。

证明:

(1) 取 $x = a^{-1} * b$, 有

$$a * x = a * (a^{-1} * b) = (a * a^{-1}) * b = b$$

所以这样的 x 是存在的。

若还有 $x_1 \in G$, 满足 $a * x_1 = b$, 所以:

$$a * x = a * x_1$$

$$a^{-1} * (a * x) = a^{-1} * (a * x_1)$$

$$(a^{-1} * a) * x = (a^{-1} * a) * x_1$$

$$x = x_1$$

因此 $x = a^{-1} * b$ 是满足 $a * x = b$ 的惟一元素。

(2) 我们可用类似的方法证明。

这一性质, 反应在运算的定义表上, 在每一行上, G 中的每个元素只出现一次, 在每一列上, G 中的元素只出现一次。

例如: $S = \{\alpha, \beta, \gamma, \delta\}$, $*$ 和 $\circ$ 的定义分别如下:

$*$	α	β	γ	δ	$\circ$	α	β	γ	δ
α	β	δ	α	γ	α	α	β	γ	δ
β	δ	γ	β	α	β	β	α	δ	γ
γ	α	β	γ	δ	γ	γ	δ	α	α
δ	γ	α	δ	β	δ	δ	γ	β	β

显然 $(S, *)$ 是一个群, 而 $(S, \circ)$ 则不是一个群, $\circ$ 的定义表上 γ 行的 α, δ 行的 β 均出现两次。

定理 4-8 如果 $(G, *)$ 是一个群, 则对每个 $a, b, c \in G$, 有:

$$(1) a * b = a * c \Rightarrow b = c$$

$$(2) b * a = c * a \Rightarrow b = c$$

这条定理称为消去律, 它是定理 4-7 的直接推论。

定理 4-9 如果 $(G, *)$ 是一个群, 则对每个 $a, b \in G$, 有:

$$(a * b)^{-1} = b^{-1} * a^{-1}。$$

证明: 因为 $(a * b) * (a * b)^{-1} = e$ 而:

$$\begin{aligned}(a * b) * (b^{-1} * a^{-1}) &= a * (b * b^{-1}) * a^{-1} \\ &= a * e * a^{-1} = a * a^{-1} = e\end{aligned}$$

所以 $(a * b) * (a * b)^{-1} = (a * b) * (b^{-1} * a^{-1})$ 由消去律得 $(a * b)^{-1} = b^{-1} * a^{-1}$

推论: 设 $(G, *)$ 是一个群, 则对每个 $a_1, a_2, \dots, a_n \in G$, 有:

$$(a_1 * a_2 * \dots * a_n)^{-1} = a_n^{-1} * a_{n-1}^{-1} * \dots * a_2^{-1} * a_1^{-1}$$

其中 a 与 a^{-1} 互为逆元素。

此推论可用数学归纳法证明。消去律在证明时常用到。

例 4-8 令 $(G, \circ)$ 是一个群, $g \in G$, 设有一个映射 $f: G \rightarrow G$, 其中 $f(x) = g \circ x \circ g^{-1}$, 证明 f 是一个 G 到 G 的同构。

证明:

(1) 对每个 $x, y \in G$, 有:

$$\begin{aligned}f(x \circ y) &= g \circ (x \circ y) \circ g^{-1} = g \circ x \circ g^{-1} \circ g \circ y \circ g^{-1} \\ &= (g \circ x \circ g^{-1}) \circ (g \circ y \circ g^{-1}) \\ &= f(x) \circ f(y)\end{aligned}$$

所以 f 是 G 到 G 的同态映射。

(2) 对 $x, y \in G$, 假定 $f(x) = f(y)$, 则:

$$g \circ x \circ g^{-1} = g \circ y \circ g^{-1}$$

所以 $x = y$ (由消去律)

故 f 是 G 到 G 的一对一映射。

(3) 对每个 $x \in G$, 于是有:

$$f(g^{-1} \circ x \circ g) = g \circ g^{-1} \circ x \circ g \circ g^{-1} = x$$

因此 f 是 G 到 G 上的满射。

由上面三点, 所以 f 是 G 到 G 的一个同构映射。

关于群中元素的阶(也称周期)是常用到的一个重要概念。

设 a 是群 $(G, *)$ 中的一个元素, 如果存在一个最小的正整数 r , 使得 $a^r = e$, 则 r 称为元素 a 的阶。如果不存在这种正整数 r , 则称 a 之阶无限。显然单位元素的阶总是 1。

注意一个群的阶和群中一个元素的阶是不同的概念。

定理 4-10 如果群 $(G, *)$ 的一个元素 a 具有阶 r , 则 $a^k = e$ 当且仅当 k 是 r 的倍数。

证明:

(1) 若 k 是 r 的倍数, 即 $k = tr$, 其中 t 是正整数, 于是 $a^k = a^{tr} = (a^r)^t = e^t = e$ 。

(2) 若 $a^k = e$, 而 k 不是 r 的倍数, 即 $k = tr + q$ ($0 \leq q < r$), 则 $a^q = a^{k-tr} = a^k * a^{-tr} = e * e^{-t} = e * e = e$, 但是 r 是使得 $a^r = e$ 的最小正整数, 故 $q = 0$, 即 $k = tr$ 。

因此, 如果 $a^r = e$, 但 r 无因子 d ($0 < d < r$), 使 $a^d = e$, 则肯定 r 就是 a 之阶。如 $a^{12} = e$, 但 $a^2 \neq e, a^3 \neq e, a^4 \neq e, a^6 \neq e$, 则肯定 12 就是 a 之阶。

例 4-9 设群 $(G, *)$ 的元素 a 的阶是 n , 则 a^r 的阶是 $\frac{n}{d}$, 其中 $d = (r, n)$ 是 r 和 n 的最大公因子。

证明: 因为 $d = (r, n)$, 所以 $r = r_1 d, n = n_1 d$, 而 $(r_1, n_1) = 1$ (即互质)。

$$(a^r)^{\frac{n}{d}} = a^{\frac{rn}{d}} = (a^n)^{\frac{r}{d}} = e_1^r = e$$

再证 $\frac{n}{d}$ 是使 $(a^r)^{\frac{n}{d}} = e$ 的最小正整数。

设还有正整数 P 使 $(a^r)^P = e$, 即 $a^{rP} = e$, 而 n 是 a 之阶, 由定理 4-10, n 整除 rP , $\frac{rP}{n} = \frac{r_1 d P}{n_1 d} = \frac{r_1 P}{n_1}$ 。因为 $(r_1, n_1) = 1$, 故 n_1 整除 P ,

即 $\frac{n}{d}$ 整除 P , 所以 $\frac{n}{d}$ 是最小的正整数。

定理 4-11 设 $(G, *)$ 是一个群, a 是 G 的任意一个元素, 则 a 的阶与 a 的逆元素 a^{-1} 的阶相同。

证明: 设 a 有有限阶 r , 即 $a^r = e$, 因此:

$$(a^{-1})^r = (a^r)^{-1} = e^{-1} = e$$

因此如果 t 是 a^{-1} 之阶, 有 $t \leq r$ 。而:

$$a^t = ((a^{-1})^t)^{-1} = e^{-1} = e$$

因此 $r \leq t$ 。最后有 $r = t$ 。

例 4-10 在一个有限群里,阶大于 2 的元素的数目必定是偶数。

证明: 设 $(G, *)$ 是具有阶为 n 的有限群,即 $|G| = n$,任取 $a \in G$,
 $a^m = e (m > 2)$, a 的逆元素, $a^{-1} \in G$, 故 $(a^{-1})^m = (a^m)^{-1} = e^{-1} = e$, 由
前面定理, m 亦是 a^{-1} 的阶, 则必定 $a \neq a^{-1}$ 。

反证法, 若 $a = a^{-1}$, 则 $a^2 = e$, 所以 a 之阶不大于 2, 这与 $m > 2$
矛盾, 所以 $a \neq a^{-1}$, 即当 a 之阶大于 2 时, a 与它的逆元素总是成对
出现的, 所以是偶数。

进一步我们可以证明, 若 G 是一个阶为偶数的有限群, 则在 G
里阶为 2 的元素的数目必定是奇数。设 $|G| = 2n$, 所以 G 中的每个
元的阶是有限的, 阶为 1 的元素是单位元素, 是惟一的。设阶为 2 的
元素个数为 m_2 , 阶大于 2 的元素个数必定是偶数, 设 $2m_3$, 故:

$$2n = 1 + m_2 + 2m_3$$

所以 m_2 必为奇数。

定理 4-12 设 $(G, *)$ 是阿贝尔群, 设 a, b 是 G 的两个元素, 其
阶分别是 r 和 s , 如果 r 和 s 互为素数, 即 $(r, s) = 1$, 则 $a * b$ 之阶
是 rs 。

证明: 因为 $(G, *)$ 是阿贝尔群, 所以:

$$(a * b)^{rs} = (a^r)^s * (b^s)^r = e * e = e$$

假定有另一 p , 使得 $(a * b)^p = e$, 所以:

$$\begin{aligned} e &= (a * b)^p = ((a * b)^p)^r = (a * b)^{pr} \\ &= (a^r)^p * (b)^{pr} = e * (b)^{pr} \end{aligned}$$

由定理 4-10, s 整除 pr , 而 $(r, s) = 1$, 所以 s 整除 p 。同理 r 亦整除 p ,
从而 rs 能整除 p , 所以 rs 是 $(a * b)$ 的阶。

推论: 设 $(G, *)$ 是阿贝尔群, 令元素 $a_1, a_2, \dots, a_n$ 的阶分别是
 $r_1, r_2, \dots, r_n$, 如果 $(r_i, r_j) = 1, (i \neq j)$ 则 $a_1 * a_2 * \dots * a_n$ 之阶是 $r_1 r_2$
 $\dots r_n$ 。

可以用数学归纳法证明这个推论, 不再赘述。

定理 4-13 在一个有限群 $(G, *)$ 里, 每个元素的阶有限而且每

个元素的阶至多为 $|G|$ 。

证明：令 a 是 G 中任一元素，在序列：

$$a, a^2, a^3, \dots, a^{|G|+1}$$

中，至少有两个元素相等，譬如说 $a^r = a^p$ ，其中 $1 \leq p < r \leq |G| + 1$ ，现有：

$$e = a^0 = a^{-r} = a^r * a^{-r} = a^r * a^{-p} = a^{-p}$$

因此， a 具有的阶至多 $r - p \leq |G|$ 。

定理 4-14 设 $(G, *)$ 和 $(H, *)$ 是同构的两个群，则 G 和 H 中对应的元素有相同的阶。

证明：令 $f: G \rightarrow H$ 是一个群同构，令 $f(y) = h$ ，假定 y 和 h 的阶分别是 m 和 n 。当 m 有限时，则 $h^m = f(y)^m = f(y^m) = f(e) = e$ ，所以 h 的阶 n 也有限的， $n \leq m$ 。

假定 n 是有限的， $f(y^n) = f(y)^n = h^n = e = f(e)$ ，由于 f 是一一对应的映射， $y^n = e$ ，因此 m 是有限的，而且 $m \leq n$ 。因此 m 和 n 都有限时， $m = n$ ，或 m 和 n 都无限。

3. 子群

常会出现这种情况，一个群的某些子集，在同样运算下也能构成一个群，我们称这样的群为一个子群，如 $(\mathbf{R}, +)$ 是一个群，而 $(\mathbf{I}, +)$ 也是一个群，但 $\mathbf{I} \subseteq \mathbf{R}$ ，所以 $(\mathbf{I}, +)$ 是 $(\mathbf{R}, +)$ 的一个子群。现在给出它的确切定义。

定义 4-17 设 $(G, *)$ 是一个群， H 是 G 的一个非空子集，如果：

- (1) 满足封闭性，即对每个 $a, b \in H$ ，有 $a * b \in H$ ；
- (2) 存在逆元素，即对每个 $a \in H$ ，有 $a^{-1} \in H$ 。

则称 $(H, *)$ 是 $(G, *)$ 的一个子群。

条件(1)和(2)等价于对每个 $a, b \in H$ ，有 $a * b^{-1} \in H$ 。

如果 $G = H$ 或 $H = \{e\}$ ，(此处 e 是 G 的一个单位元素)，则称 $(H, *)$ 是 $(G, *)$ 的一个平凡子群。如果 $H \subset G$ ，则称 $(H, *)$ 是 $(G, *)$ 的一个真子群，如果 $(H, *)$ 是 $(G, *)$ 的真子群而且无真子群

$(H, *)$ 存在,使得 $H \subset H$,那么称 $(H, *)$ 是 $(G, *)$ 的极大子群。例如所有 4 的倍数的集合在加法运算下,构成的一个群是 $(I, +)$ 的真子群,但不是极大的。因为所有 2 的倍数的集合在加法运算下也构成一个 $(I, +)$ 的真子群。

例 4-11 群 $(G, *)$ 和它的子群 $(H, *)$ 的单位元素相同。

证明: 任取 $x \in H$,有 $x^{-1} \in H$,且 $x * x^{-1} = e' \in H$ 。另一方面,因为 $H \subseteq G$,所以 $x, x^{-1} \in G$,且 $x * x^{-1} = e \in G$,故 $e = e' = x * x^{-1}$ 。我们还可以证明,在 H 中的元素 a 的逆元素和它在 G 中的逆元素也是相同的,设 a 在 G 和 H 中逆元素分别是 b 和 b' ,所以有 $a * b = a * b' = e = e'$,由消去律得 $b = b'$ 。

定理 4-15 如果 $(H, *)$ 是 $(G, *)$ 的一个子代数(系统),则 $(H, *)$ 也是一个群。

证明: 我们要证明 $(H, *)$ 满足群的三个条件。由于在运算 $*$ 下, H 是封闭的,如果对任意 $a, b, c \in H$,则 $a * (b * c) = (a * b) * c$ 在 $(G, *)$ 中成立,因此在 $(H, *)$ 中也成立。由于 $H \neq \emptyset$,它至少包含一个元素,譬如说 $a \in H$,而 $a^{-1} \in H$,故 $a * a^{-1}$ 就是 H 的单位元素,至于逆元素由子群定义自然满足。因此 $(H, *)$ 是一个群。

定理 4-16 设 $(G, *)$ 是一个群,且 H 是 G 的有限的非空子集,而且对每个 $a, b \in H$,有 $a * b \in H$,则 $(H, *)$ 是 $(G, *)$ 的一个子群。

证明: 根据子群的定义,我们必须证明对每个元素 $a \in H$,其逆元素 $a^{-1} \in H$ 。由封闭性, $a \in H, a^2 \in H, a^3 \in H, \dots$ 。因为 H 是有限的,因此总是会存在 $1 \leq i < j$,使得 $a^i = a^j$ 。由消去律可得到 $a^{j-i} = e, (j-i > 0)$,因此 $e \in H$ 。再把 $a^{j-i} = e$ 写成 $e = a * a^{j-i-1} = a^{j-i-1} * a$,因此 $a^{-1} = a^{j-i-1} \in H$,这是因为 $j-i-1 \geq 0$ 。

例 4-12 设 f 和 g 是从群 $(G, *)$ 到 $(H, \circ)$ 的同态映射,求证: $(C, *)$ 是 $(G, *)$ 的一个子群。其中 $C = \{x | x \in G \text{ 且 } f(x) = g(x)\}$ 。

证明: 首先 $C \subseteq G$ 。又对任意 $a, b \in C$,有 $f(a) = g(a), f(b) = g(b)$,另一方面,有 $a * b \in G$ 。因为 f 和 g 都是从 G 到 H 的同态映射,故 $f(a * b) = f(a) \circ f(b), g(a * b) = g(a) \circ g(b) = f(a) \circ f(b)$,所

以 $f(a * b) = g(a * b)$, 故 $a * b \in C$ 。其次, 设 $a \in C$, 则 $f(a) = g(a)$, 而 $e = f(a * a^{-1}) = f(a) \circ f(a^{-1})$, 故 $f(a)^{-1} = f(a^{-1})$, 同理 $g(a)^{-1} = g(a^{-1})$ 。因为 $f(a) = g(a)$, 得到 $f(a)^{-1} = g(a)^{-1}$, 故 $f(a^{-1}) = g(a^{-1})$, 所以 $a^{-1} \in C$ 。

由子群定义可知 $(C, *)$, 是 $(G, *)$ 的子群。

例 4-13 设 $(H_1, *)$ 和 $(H_2, *)$ 是群 $(G, *)$ 的两个子群, 证明: $(H_1 \cap H_2, *)$ 亦是 $(G, *)$ 的子群。

证明: 因为 $H_1 \subseteq G, H_2 \subseteq G$, 故 $H_1 \cap H_2 \subseteq G$, 现在任取 $a, b \in H_1 \cap H_2$, 于是 $a, b \in H_1$, 并且 $a, b \in H_2$, 于是 $a * b^{-1} \in H_1$, 并且 $a * b^{-1} \in H_2$, 故 $a * b^{-1} \in H_1 \cap H_2$ 。

由子群的定义, 得 $(H_1 \cap H_2, *)$ 亦是群 $(G, *)$ 的子群。

4. 循环群

我们来研究这样一类群, 它的每个元素都可写成某个元素的幂, 这样的群称之循环群。

定义 4-18 设 $(G, *)$ 是一个群, 如果存在一个元素 $g \in G$, 使得 $G = \{g^n \mid g \in G \text{ 且 } n \in \mathbf{I}\}$, 则称 $(G, *)$ 是一个循环群, 元素 $g \in G$ 称为这循环群的生成元素。

由此定义可知, 每个循环群必定是阿贝尔群, 因为 $a = q^r, b = q^s$, $a * b = q^r * q^s = q^{r+s} = q^s * q^r = b * a$ 。

又如, $(\{1, -1, i, -i, *\})$ 是一个循环群, 因为 $i^0 = 1, i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1, i^5 = i, \dots$ 。群的阶是 4, 单位元素 $e = 1$ 的阶是 1, -1 的阶是 2, i 和 $-i$ 的阶是 4。

令 $Q^* = Q - \{0\}$ 是非零有理数的集合, 则在乘法运算下 $(Q^*, *)$ 是一个群, 单位元素是 $e = 1$, -1 的阶是 2, 每个其他元素的阶是无限的, 群的阶也是无限的, 然而它不是一个循环群, 因为没有有一个有理数 r , 可以使得其他每个非零有理数用 r^n 表示。

对于群 $(G, *)$ 中的一个元素, 可生成群 G 的子群。

定理 4-17 如果 g 是群 $(G, *)$ 中的一个元素, g 的阶是 m , 令

$H = \{gr \mid r \in I\}$, 则 $(H, *)$ 是 $(G, *)$ 的一个 m 阶子群。它称为由 g 生成的循环子群。(其中 I 代表整数集)

证明: 首先 $(H, *)$ 是 $(G, *)$ 的一个子群。这是因为对所有 $r, s \in I$, 有:

$$(1) \text{ 对每个 } g^r, g^s \in H, g^r * g^s = g^{r+s} \in H$$

$$(2) \text{ 设 } g^r \in H, \text{ 有 } (g^r)^{-1} = g^{-r} \in H$$

其次证明它是 m 阶子群。

如果元素 g 的阶是无限的, 我们证明 g^r 都是互不相同的。假定 $g^r = g^s$, 不妨设 $r > s$, 于是 $g^{r-s} = e$, 于是 g 的阶 $\leq r-s$, 这与 g 的阶无限发生矛盾。在 g 的阶无限的情况下, $|H|$ 也是无限的。

如果元素 g 的阶是有限正整数 m , 我们证明 $H = \{g^0 = e, g^1, g^2, \dots, g^{m-1}\}$ 。假定 $g^r = g^s$, 其中 $0 \leq s < r \leq m-1$, 于是 $g^{r-s} = e$, 其中 $0 < r-s < m$, 这与 g 的阶是 m 发生矛盾, 因此 H 中的元素是互不相同的。对任何其他元素 g^t , t 总能写成 $t = km + r$, 其中 $0 \leq r < m$, 于是:

$$g^t = g^{km+r} = g^{km} * g^r = (g^m)^k * g^r = e^k * g^r = g^r$$

因此 $H = \{g^0, g^1, \dots, g^{m-1}\}$ 。

在这种情况下, $|H| = m$ 。

定理 4-18 如果有限群 $(G, *)$ 具有阶 n , 若有一个元素 $g \in G$ 的阶也是 n , 则 $(G, *)$ 是由 g 生成的循环群。

证明: 由定理 4-17 我们已经知道 $(H, *)$ 是由 g 生成的 $(G, *)$ 的循环子群。它有阶 n , 因此 H 是 G 的有限子集, 与 G 有同样多的元素, 因此 $G = H$, 所以 $(G, *)$ 是由 g 生成的循环群。

定理 4-19 阶相同的循环群是同构的。

证明: 令 $(G, *)$ 是由 g 生成的循环群, $(H, *)$ 是由 h 生成的循环群。

(1) 如果 G 和 H 的阶为无限。定义映射如下:

$$f: G \rightarrow H, f(g^r) = h^r, r \in I.$$

于是 f 是 G 和 H 间的一一对应的映射:

$$\begin{aligned} f(g^r * g^s) &= f(g^{r+s}) = h^{r+s} = h^r * h^s \\ &= f(g^r) * f(g^s) \end{aligned}$$

所以 f 是一个群同构映射。

(2) 如果 G 和 H 有有限阶 n , $G = \{e, g, g^2, \dots, g^{n-1}\}$, $H = \{e, h, h^2, \dots, h^{n-1}\}$, 我们定义映射如下:

$f: G \rightarrow H, f(g^r) = h^r, r = 0, 1, \dots, n-1$, 那么 f 是一一对应的。如果 $0 \leq r, s \leq n-1$, 令 $r+s = kn+l$, 其中 $0 \leq l \leq n-1$, 于是:

$$\begin{aligned} f(g^r * g^s) &= f(g^{r+s}) = f(g^{kn+l}) \\ &= f((g^n)^k * g^l) = f(e^k * g^l) \\ &= f(g^l) = h^l \\ f(g^r) * f(g^s) &= h^r * h^s = h^{r+s} \\ &= h^{kn+l} = (h^n)^k * h^l = e^k * h^l = h^l \end{aligned}$$

故: $f(g^r * g^s) = f(g^r) * f(g^s)$

所以 f 是一个群同构映射。

由于 $(I, +)$ 是一个阶无限的循环群, $(I_n, +)$ 是一个阶有限的循环群。根据上述定理, 每个循环群或者与 $(I, +)$ 同构, 或者与 $(I_n, +)$ 同构, 二者必居其一。 $(I, +)$ 称整数加群。其中 $I_n = \{0, 1, 2, \dots, n-1\}$ 。

例 4-14 证明: 一个循环群的每个子群也是循环群。

证明: 设 $(G, *)$ 是循环群, 生成元素是 a , $(H, *)$ 是它的子群。

(1) 若 $H = \{e\}$, 显然成立。

(2) 若 $a \in H$, 则对任意 $x \in H$, 有 $x = a^m$, 所以 $(H, *)$ 是 $(G, *)$ 的循环子群。

(3) 若 $a \in G$ 且 $a \notin H$, 因为 G 中每个元素能表示成 a^r 形式, 故 H 中元素也呈 a^r 形式, 我们取 H 中幂指数最小的正整数的元素 (不妨设为 a^r), 可断言 a^r 就是 H 的生成元素。证明如下:

令 x 是 H 中的任一其他元素, 由于 $x \in G$, 所以 $x = a^p$, 由于 r 最小, 用 r 除 p , 得商 q , 余数 t , 即:

$$p = qr + t$$

其中, $0 \leq t < r$ 于是:

$$a^p = a^{qr+t} = a^{qr} * a^t = (a^r)^q * a$$

因为 $a^p \in H, (a^r)^q \in H$, 所以 $a^t \in H$, 我们已假定 r 是最小幂指数, 故得 $t=0$ 。

于是任意 $x \in H$, 有 $x = (a^r)^q$, 即 a^r 是 H 的生成元素。

例 4-15 假定 $(G, *)$ 是循环群, $(G, *)$ 和 $(\bar{G}, *)$ 满同态, 证明 $(\bar{G}, *)$ 也是循环群。

证明: 因为 $(G, *)$ 和 $(\bar{G}, *)$ 满同态, 所以 $\bar{G}$ 是群, 设 f 是 G 到 $\bar{G}$ 的满同态映射, 又设 $G = \{a^n \mid n \in I\}$, 由于 f 是满同态, 所以 $\bar{G} = \{f(a^n) \mid n \in I\} = \{(f(a))^n \mid n \in I\}$ 为循环群。

5. 置换群

我们先引进置换的含义。一个有限集合上的 n 个元素的一个置换是到它自身集合上的一个一对一映射。如 $P = \{a, b, c\}$, 则有:

$$e = \pi_0: a \rightarrow a, b \rightarrow b, c \rightarrow c$$

$$\pi_1: a \rightarrow a, b \rightarrow c, c \rightarrow b$$

$$\pi_2: a \rightarrow b, b \rightarrow a, c \rightarrow c$$

$$\pi_3: a \rightarrow b, b \rightarrow c, c \rightarrow a$$

$$\pi_4: a \rightarrow c, b \rightarrow a, c \rightarrow b$$

$$\pi_5: a \rightarrow c, b \rightarrow b, c \rightarrow a$$

所以上述的 $\epsilon, \pi_1, \pi_2, \dots, \pi_5$, 均是 P 上的六个置换, 对置换习惯上还用下述记号表示:

$$\epsilon = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} \quad \pi_1 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$$

$$\pi_2 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \quad \pi_3 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$$

$$\pi_4 = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} \quad \pi_5 = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}$$

设集合 P 有 n 个元素, P 上的所有置换之集合用 P_n 表示, 则有

下面定理。

定理 4-20 $|P_n|=n!$

证明：不妨设 $P=\{1,2,\cdots,n\}$ ，由于 $|P_n|$ 是从 P 到 P 的所有一对一映射的数目，据排列理论，在一对一情况下，元素 1 的象有 n 种可能，在 1 的象选定的情况下，2 的象有 $(n-1)$ 种可能，同理 3 的象有 $(n-2)$ 种可能，依此类推，得：

$$|P_n|=n(n-1)(n-2)\cdots 2\times 1=n!$$

所以上例 $P_3=\{\epsilon,\pi_1,\pi_2,\pi_3,\pi_4,\pi_5\}$ 。

我们仍以 P_3 为例，在 P_3 上定义复合运算 $*$ ，问：它是否能构成群？答案是肯定的，我们发现它首先是封闭的，如：

$$\begin{aligned}\pi_1*\pi_2 &= \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}*\begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \\ &= \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}=\pi_3\in P_3\end{aligned}$$

同理可验证对任意 π_i,π_j ，有 $\pi_i*\pi_j\in P_3$ ，其中 $0\leq i,j\leq 5$ ，并列表如下：

$*$	ϵ	π_1	π_2	π_3	π_4	π_5
ϵ	ϵ	π_1	π_2	π_3	π_4	π_5
π_1	π_1	ϵ	π_3	π_2	π_5	π_4
π_2	π_2	π_4	ϵ	π_5	π_1	π_3
π_3	π_3	π_5	π_1	π_4	ϵ	π_2
π_4	π_4	π_2	π_5	ϵ	π_3	π_1
π_5	π_5	π_3	π_4	π_1	π_2	ϵ

显然单位元是 ϵ ，其结合律也成立。如：

$$\begin{aligned}\pi_1*(\pi_4*\pi_5) &= \pi_1*\pi_1=\epsilon \\ (\pi_1*\pi_4)*\pi_5 &= \pi_5*\pi_5=\epsilon\end{aligned}$$

另外每个元素的逆元素也存在，如 $\epsilon^{-1}=\epsilon,\pi_1^{-1}=\pi_1,\pi_2^{-1}=\pi_2,\pi_3^{-1}=\pi_4,\pi_4^{-1}=\pi_3,\pi_5^{-1}=\pi_5$ ，所以 $(P_3,*)$ 是一个群，由于 P_3 的每个

元素是置换,我们称它为置换群。即一个群的元素是置换而其运算是复合运算,那么称它为置换群。

我们已经知道,有限集合 P 上的 n 个元素的置换有 $n!$ 个,但置换群并没有要求 P 上的所有置换($n!$ 个),它仅说明集合 P 上的一些置换及复合运算若能构成群,便是置换群。

n 个元素的集合 P 上的所有置换及其复合运算肯定构成一个群,我们称它为 n 次对称群,用符号 $(P_n, *)$ 表示,故 $(P_3, *)$ 是对称群。显然对称群是置换群的特例。由上表可看到 $(\{\epsilon, \pi_1\}, *)$, $(\{\epsilon, \pi_5\}, *)$, $(\{\epsilon, \pi_2\}, *)$, $(\{\epsilon, \pi_3, \pi_4\}, *)$ 都是置换群。

6. 陪集,商群

(1) 子群的陪集和拉格朗日(Lagrange)定理

我们知道,当且仅当 $(a-b)$ 被 n 整除,在整数集 I 上的两个整数 a 和 b 为模 n 同余关系,记以 $a \equiv b \pmod{n}$ 。在此基础上我们进一步定义任何一个群对它的子群取模的概念。

定义 4-19 设 $(G, *)$ 是群,其子群是 $(H, *)$,对任意 $a, b \in G$,当且仅当 $a * b^{-1} \in H$,称 a 和 b 为模 H 同余关系,记作 $a \equiv b \pmod{H}$ 。

定理 4-21 关系 $a \equiv b \pmod{H}$ 是 G 上的等价关系。

证明: 对任意 $a, b, c \in G$,有:

(1) $a * a^{-1} = e \in H$,因此关系是自反的。

(2) $a \equiv b \pmod{H} \Rightarrow a * b^{-1} \in H$
 $\Rightarrow (a * b^{-1})^{-1} = b * a^{-1} \in H$
 $\Rightarrow b \equiv a \pmod{H}$

故这关系是对称的。

(3) $a \equiv b \pmod{H}$ 且 $b \equiv c \pmod{H}$
 $\Rightarrow a * b^{-1} \in H$ 且 $b * c^{-1} \in H$
 $\Rightarrow (a * b^{-1}) * (b * c^{-1}) \in H$
 $\Rightarrow a * c^{-1} \in H$
 $\Rightarrow a \equiv c \pmod{H}$

故这关系是传递的。

综上所述, $a \equiv b \pmod{H}$ 是一个等价关系。下面按等价关系分类。包含 a 的等价类是:

$$\begin{aligned} [a] &= \{x \in G \mid x \equiv a \pmod{H}\} \\ &= \{x \in G \mid x * a^{-1} \in H\} \\ &= \{x \in G \mid x = h * a\} \\ &= \{h * a \mid h \in H\} \end{aligned}$$

可见,以 a 为代表的等价类实质上是 a 从右边乘 H 中的每个元素所得到的集合,记以 Ha ,即:

$$Ha = \{h * a \mid h \in H\}$$

称为 H 在 $(G, *)$ 中的一个右陪集。

同理可定义左陪集如下:

$$aH = \{a * h \mid h \in H\}$$

例 4-16 仍然以 3 次对称群为例, $P_3 = \{\epsilon, \pi_1, \pi_2, \dots, \pi_5\}$, $(\{\epsilon, \pi_1\}, *)$, $(\{\epsilon, \pi_2\}, *)$, $(\{\epsilon, \pi_5\}, *)$, $(\{\epsilon, \pi_3, \pi_4\}, *)$ 都是置换群,当然它们都是 $(P_3, *)$ 的子群,我们看 $\{\epsilon, \pi_1\}$ 的右陪集:

$$\begin{aligned} \{\epsilon, \pi_1\}\epsilon &= \{\epsilon * \epsilon, \pi_1 * \epsilon\} = \{\epsilon, \pi_1\} \\ \{\epsilon, \pi_1\}\pi_1 &= \{\epsilon * \pi_1, \pi_1 * \pi_1\} = \{\pi_1, \epsilon\} \\ \{\epsilon, \pi_1\}\pi_2 &= \{\epsilon * \pi_2, \pi_1 * \pi_2\} = \{\pi_2, \pi_3\} \\ \{\epsilon, \pi_1\}\pi_3 &= \{\epsilon * \pi_3, \pi_1 * \pi_3\} = \{\pi_3, \pi_2\} \\ \{\epsilon, \pi_1\}\pi_4 &= \{\epsilon * \pi_4, \pi_1 * \pi_4\} = \{\pi_4, \pi_5\} \\ \{\epsilon, \pi_1\}\pi_5 &= \{\epsilon * \pi_5, \pi_1 * \pi_5\} = \{\pi_5, \pi_4\} \end{aligned}$$

上述的右陪集只有三个是互不相同的,即:

$$\{\epsilon, \pi_1\}, \{\pi_2, \pi_3\}, \{\pi_4, \pi_5\}$$

再看 $\{\epsilon, \pi_1\}$ 的左陪集:

$$\begin{aligned} \epsilon\{\epsilon, \pi_1\} &= \{\epsilon * \epsilon, \epsilon * \pi_1\} = \{\epsilon, \pi_1\} \\ \pi_1\{\epsilon, \pi_1\} &= \{\pi_1 * \epsilon, \pi_1 * \pi_1\} = \{\pi_1, \epsilon\} \\ \pi_2\{\epsilon, \pi_1\} &= \{\pi_2 * \epsilon, \pi_2 * \pi_1\} = \{\pi_2, \pi_4\} \\ \pi_3\{\epsilon, \pi_1\} &= \{\pi_3 * \epsilon, \pi_3 * \pi_1\} = \{\pi_3, \pi_5\} \end{aligned}$$

$$\pi_4 \{ \epsilon, \pi_1 \} = \{ \pi_4 * \epsilon, \pi_4 * \pi_1 \} = \{ \pi_4, \pi_2 \}$$

$$\pi_5 \{ \epsilon, \pi_1 \} = \{ \pi_5 * \epsilon, \pi_5 * \pi_1 \} = \{ \pi_5, \pi_3 \}$$

因此 $\{ \epsilon, \pi_1 \}$ 有三个互不相同的左陪集, 即:

$$\{ \epsilon, \pi_1 \}, \{ \pi_2, \pi_4 \}, \{ \pi_3, \pi_5 \}$$

我们还发现 $\{ \epsilon, \pi_1 \}$ 的左右陪集不都相等。

我们再考察子群 $\{ \epsilon, \pi_3, \pi_4 \}$ 的右陪集:

$$\{ \epsilon, \pi_3, \pi_4 \} \epsilon = \{ \epsilon * \epsilon, \pi_3 * \epsilon, \pi_4 * \epsilon \}$$

$$= \{ \epsilon, \pi_3, \pi_4 \}$$

$$\{ \epsilon, \pi_3, \pi_4 \} \pi_1 = \{ \epsilon * \pi_1, \pi_3 * \pi_1, \pi_4 * \pi_1 \}$$

$$= \{ \pi_1, \pi_2, \pi_5 \}$$

$$\{ \epsilon, \pi_3, \pi_4 \} \pi_2 = \{ \epsilon * \pi_2, \pi_3 * \pi_2, \pi_4 * \pi_2 \}$$

$$= \{ \pi_2, \pi_5, \pi_1 \}$$

$$\{ \epsilon, \pi_3, \pi_4 \} \pi_3 = \{ \epsilon * \pi_3, \pi_3 * \pi_3, \pi_4 * \pi_3 \}$$

$$= \{ \pi_3, \pi_4, \epsilon \}$$

$$\{ \epsilon, \pi_3, \pi_4 \} \pi_4 = \{ \epsilon * \pi_4, \pi_3 * \pi_4, \pi_4 * \pi_4 \}$$

$$= \{ \pi_4, \epsilon, \pi_3 \}$$

$$\{ \epsilon, \pi_3, \pi_4 \} \pi_5 = \{ \epsilon * \pi_5, \pi_3 * \pi_5, \pi_4 * \pi_5 \}$$

$$= \{ \pi_5, \pi_1, \pi_2 \}$$

因此, $\{ \epsilon, \pi_3, \pi_4 \}$ 有二个不同的右陪集, 即:

$$\{ \epsilon, \pi_3, \pi_4 \}, \{ \pi_1, \pi_2, \pi_5 \}$$

再看 $\{ \epsilon, \pi_3, \pi_4 \}$ 的左陪集:

$$\epsilon \{ \epsilon, \pi_3, \pi_4 \} = \{ \epsilon, \pi_3, \pi_4 \}$$

$$\pi_1 \{ \epsilon, \pi_3, \pi_4 \} = \{ \pi_1, \pi_2, \pi_5 \}$$

$$\pi_2 \{ \epsilon, \pi_3, \pi_4 \} = \{ \pi_2, \pi_5, \pi_1 \}$$

$$\pi_3 \{ \epsilon, \pi_3, \pi_4 \} = \{ \pi_3, \pi_4, \epsilon \}$$

$$\pi_4 \{ \epsilon, \pi_3, \pi_4 \} = \{ \pi_4, \epsilon, \pi_3 \}$$

$$\pi_5 \{ \epsilon, \pi_3, \pi_4 \} = \{ \pi_5, \pi_1, \pi_2 \}$$

因此, $\{ \epsilon, \pi_2, \pi_4 \}$ 的左陪集有两个, 即:

$$\{ \epsilon, \pi_3, \pi_4 \}, \{ \pi_1, \pi_2, \pi_5 \}$$

我们发现子群 $\{\epsilon, \pi_3, \pi_4\}$ 的左右陪集是相等的。这种子群称为正规子群。

定理 4-22 设 $(H, *)$ 是群 $(G, *)$ 的一个子群, 则:

(1) $b \in Ha$ 当且仅当 $b * a^{-1} \in H$;

(2) $b \in aH$ 当且仅当 $a^{-1} * b \in H$ 。

证明:

(1) $b \in Ha$ 当且仅当存在 $h \in H$, 使得 $b = h * a$, 因此, 当且仅当 $b * a^{-1} = h$, 因此当且仅当 $b * a^{-1} \in H$ 。

(2) 证明方法与(1)类似。从略。

定理 4-23 设 $(H, *)$ 是 $(G, *)$ 的子群, 而且 a, b 是 G 中任意元素, 则:

(1) 或者 $aH = bH$, 或者 $(aH) \cap (bH) = \emptyset$,

(2) 或者 $Ha = Hb$, 或者 $(Ha) \cap (Hb) = \emptyset$ 。

证明:

(1) 如果 $(aH) \cap (bH) \neq \emptyset$, 令任意元素 $h \in (aH) \cap (bH)$, 于是存在 $h_1, h_2 \in H$, 使得 $h = a * h_1 = b * h_2$, 立即得 $a = b * h_2 * h_1^{-1}$ 。现在任取 $a' \in aH$, 于是有 $h' \in H$, 使得 $a' = a * h' = b * h_2 * h_1^{-1} * h'$ 。由于 $h_1, h_2, h' \in H$, 故 $h_2 * h_1^{-1} * h' \in H$, 得到 $a' = b * (h_2 * h_1^{-1} * h') \in bH$ 。反之任意取 $b' \in bH$, 同样可证明 $b' \in aH$, 所以有:

$$aH = bH$$

用类似的方法可以证明(2)。

例 4-17 设 $(H, *)$ 是 $(G, *)$ 的子群, 则:

(1) 如果 $b \in aH$, 则 $bH = aH$,

(2) 如果 $b \in Ha$, 则 $Hb = Ha$ 。

证明:

(1) 因为 bH 一定包含 $b * e = b$, 所以 $(bH) \cap (aH) \neq \emptyset$, 由上述定理得:

$$bH = aH$$

(2) 的证明从略。

例 4-18 群 $(G, *)$ 中的子群 $(H, *)$ 的任意两个右(左)陪集均存在一一对应的映射。

证明: 令 Ha 是 G 中 H 的一个右陪集, 我们证明 Ha 和 H 之间存在一一对应的映射, 从而得出任何两个右陪集之间存在一一对应的映射。

用 $\varnothing(h) = h * a$ 来定义 $\varnothing: H \rightarrow Ha$, 于是 $\varnothing$ 是从 H 到 Ha 上的满射。假定 $\varnothing(h_1) = \varnothing(h_2)$, 所以 $h_1 * a = h_2 * a$, 从而求得 $h_1 = h_2$, 因此 $\varnothing$ 是一一对应的映射。

由定理 4-23, H 的不同右陪集是分离的, 而且每个元素 $a \in G$, 总属于它的右陪集 Ha , 对于 H 的左陪集, 也有这个结论。为此有下述定理。

定理 4-24 令 $(H, *)$ 是 $(G, *)$ 的子群, 则:

- (1) H 的所有不同的右陪集是 G 的一个划分;
- (2) H 的所有不同的左陪集是 G 的一个划分。

例 4-19 我们继续考察 $(\{\epsilon, \pi_1, \pi_2, \dots, \pi_5\}, *)$ $\{\epsilon, \pi_1\}$ 的右陪集形成的划分是:

$$\{\{\epsilon, \pi_1\}, \{\pi_2, \pi_3\}, \{\pi_4, \pi_5\}\}$$

$\{\epsilon, \pi_1\}$ 的左陪集形成的划分是:

$$\{\{\epsilon, \pi_1\}, \{\pi_2, \pi_4\}, \{\pi_3, \pi_5\}\}$$

$\{\epsilon, \pi_3, \pi_4\}$ 的右(或左)陪集形成的划分是:

$$\{\{\epsilon, \pi_3, \pi_4\}, \{\pi_1, \pi_2, \pi_5\}\}。$$

这里定义的划分称为关于 H 在 G 中的右(或左)陪集划分。

同一子群的所有左(或右)陪集的元素数目相同的, 而且在有限群情况下, 左陪集的数目与右陪集的数目相同。群 $(G, *)$ 的一个子群 $(H, *)$ 的左(或右)陪集的数目称为 H 在 G 中的指数 K , 因此前面例中 $\{\epsilon, \pi_1\}$ 在 $\{\epsilon, \pi_1, \pi_2, \dots, \pi_5\}$ 中的指数是 3, $\{\epsilon, \pi_3, \pi_4\}$ 在 $\{\epsilon, \pi_1, \dots, \pi_5\}$ 中的指数是 2, 这里有一条著名的 Lagrange 定理:

定理 4-25 设 $(G, *)$ 是一个有限群, $(H, *)$ 是它的一个子群, 则:

$$|G|/|H|=K(\text{指数})$$

这条定理说明群的子群的阶必定是群的阶的一个因子。显然若群的阶是素数,它必定无真子群存在。

例 4-20 设 $(G, \circ)$ 是有限群, a 是 G 中任意元素, 则 a 的阶是 $|G|$ 的一个因子。

证明: 设 $a \in G$ 的阶为 r , 它可形成一个群的子群是:

$$(\{e, a, a^2, \dots, a^{r-1}\}, \circ)$$

由 Lagrange 定理, r 是 $|G|$ 的因子。

例 4-21 设 a 是有限群 $(G, *)$ 的一个元素, 则有 $a^{|G|} = e$ 。

证明: 不妨设 a 的阶是 m , 则 $|G| = mr$ (r 是正整数), 因此 $a^{|G|} = a^{mr} = (a^m)^r = e^r = e$ 。

例 4-22 设群 $(G, *)$ 的阶是素数, 则 $(G, *)$ 必是循环群。

证明: 令 $|G| = P$, 若 $P=1, G=\{e\}$, 显然是循环群; 若 $P \geq 2$, 所有其他元素有阶 P 而且至少有一个。由定理 4-18, G 是循环群。

上述例子均是由 Lagrange 定理推出的。要注意的是 Lagrange 定理的逆定理不一定成立, 即如果 K 是 $(G, *)$ 阶的一个因子, 不一定得出 $(G, *)$ 有阶 K 的一个子群。

(2) 正规子群和商群

我们考察一个群的子群的左右陪集相等的情况。

定义 4-20 设群 $(G, *)$ 的子群是 $(N, *)$, 如果对每个 $a \in G, n \in N$ 有 $a^{-1} * n * a \in N$, 则称 $(N, *)$ 是 $(G, *)$ 的一个正规子群。

例 4-23 证明对每个 $a \in G, Na = aN$ 当且仅当 $(N, *)$ 是 $(G, *)$ 的一个正规子群。

证明: 设 $Na = aN$, 则对每个 $n \in N, n * a \in Na = aN$, 因此 $n * a = a * n_1$, 其中 $n_1 \in N$, 故 $a^{-1} * n * a = n_1 \in N$, 因此 $(N, *)$ 是一个正规子群。

充分性的证明留给读者练习。

因此, 有些书是用 $Na = aN$ 定义正规子群 N 的。

定理 4-26 如果 $(N, *)$ 是群 $(G, *)$ 的正规子群, 则 $(G/N, *)$

是一个群。其中 $G/N = \{Na \mid a \in G\}$, 运算 $*$ 定义为 $(Na_1) * (Na_2) = N(a_1 * a_2)$

证明: 先证明按照这种方法定义的运算是合适的, 即两个陪集 Na_1 和 Na_2 的运算(乘积)与代表元 a_1 和 a_2 的选择无关。设 h_1 和 a_1 在同一陪集, 从而有 $h_1 \equiv a_1 \pmod{N}$, 设 h_2 和 a_2 在同一陪集, 从而有 $h_2 \equiv a_2 \pmod{N}$ 。现在证明 $Nh_1 * h_2 = Na_1 * a_2$ 。我们有 $h_1 * a_1^{-1} = n_1 \in N, h_2 * a_2^{-1} = n_2 \in N$, 所以 $h_1 * h_2 * (a_1 * a_2)^{-1} = h_1 * h_2 * a_2^{-1} * a_1^{-1} = n_1 * a_1 * n_2 * a_2 * a_2^{-1} * a_1^{-1} = n_1 * a_1 * n_2 * a_1^{-1}$, 因为 $(N, *)$ 是正规子群, 故 $a_1 * n_2 * a_1^{-1} \in N, n_1 * a_1 * n_2 * a_1^{-1} \in N$ 。因此 $h_1 * h_2 \equiv a_1 * a_2 \pmod{N}$, $Nh_1 * h_2 = Na_1 * a_2$, 因此定义的运算是合适的。

运算也满足结合律, 因为 $(Na_1 * Na_2) * Na_3 = N(a_1 * a_2) * Na_3 = N((a_1 * a_2) * a_3) = N(a_1 * (a_2 * a_3)) = Na_1 * (Na_2 * Na_3)$ 。

又因为 $Na * Ne = Na * e = Na, Ne * Na = Ne * a = Na$, 所以单位元素是 $Ne = N$ 。

又因为 $Na * Na^{-1} = Na * a^{-1} = Ne = N$, 同理 $Na^{-1} * Na = N$, 故 Na 和 Na^{-1} 互逆。

因此 $(G/N, *)$ 是一个群, 称为 $(G, *)$ 关于 $(N, *)$ 的商群。

例 4-24 $(I_n, +)$ 是 $(I, +)$ 关于子群 $(nI, +)$ 的商群。其中 $I_n = \{0, 1, 2, \dots, n-1\}, nI = \{n * i \mid i \in I\}$ 。

证明: $(I, +)$ 是阿贝尔群, 它的每个子群是正规的, 而 $(nI, +)$ 是子群, 关系 $a \equiv b \pmod{nI}$ 等价于 $(a-b) \in nI$, 亦等价于 $n \mid (a-b)$, 因此 $a \equiv b \pmod{nI}$ 与 $a \equiv b \pmod{n}$ 完全相同, 因此 $(I_n, +)$ 就是 $(I/nI, +)$ 。其中 $+$ 定义为 $[a] + [b] = [a+b]$ 。

(3) 同态定理

同态定理是群论中一条很重要的定理, 它阐明了同态、正规子群和商群之间的关系。

定义 4-21 设 $f: G \rightarrow H$ 是群同态, 则:

$$K = \{a \mid a \in G \text{ 且 } f(a) = e_H\}$$

称为 f 的同态核。另一方面, $f(G) = \{f(a) \mid a \in G\}$, 称为 f 的象集, 它们的示意图见图 4-4。

定理 4-27 设 $f: G \rightarrow H$ 是群同态, 则:

- (1) $(K, *)$ 是 $(G, *)$ 的正规子群。
- (2) f 是一一对映射当且仅当 $K = \{e_G\}$ 。

证明: (1) 令 $a, b \in K$, 故 $f(a) = f(b) = e_H$, 于是:

$$f(a * b) = f(a) * f(b) = e_H * e_H$$

故:

$$a * b \in K$$

又:

$$f(a^{-1}) = f(a)^{-1} = e_H^{-1} = e_H$$

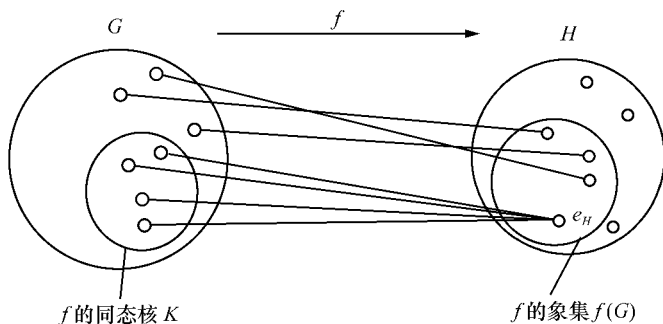


图 4-4 同态核及其象集示意图

故:

$$a^{-1} \in K,$$

所以 $(K, *)$ 是 $(G, *)$ 的一个子群。

令 $a \in K, b \in G$, 于是:

$$\begin{aligned} f(b^{-1} * a * b) &= f(b^{-1}) * f(a) * f(b) \\ &= f(b)^{-1} * e_H * f(b) = f(b)^{-1} * f(b) = e_H \end{aligned}$$

因此 $b^{-1} * a * b \in K$ 。因此 $(K, *)$ 是 $(G, *)$ 的正规子群。

(2) 如果 f 是一对一的, 仅有一个元素映射到 e_H , 因此 $K = \{e_G\}$ 。反之, 如果 $K = \{e_G\}$, 假定 $f(a_1) = f(a_2)$, 于是 $f(a_1 * a_2^{-1}) = f(a_1) * f(a_2)^{-1} = e_H$, 故 $a_1 * a_2^{-1} \in K = \{e_G\}$, 因此有 $a_1 = a_2$ 。

定理 4-28 对每个群同态 $f: G \rightarrow H$, f 的象集是 $(H, *)$ 的一个

子群。

证明：设 f 的象集是 $f(G)$ ，令 $f(a_1), f(a_2) \in f(G)$ ，则 $f(a_1) * f(a_2) = f(a_1 * a_2) \in f(G)$ ， $f(a_1)^{-1} = f(a_1^{-1}) \in f(G)$ ，所以 $f(G)$ 是 H 的一个子群。

定理 4-29 设 $f: G \rightarrow H$ 是群同态， K 是 f 的同态核，则 G/K 与 f 的象 $f(G)$ 同构。

证明：令 $\varphi: G/K \rightarrow f(G)$ ，定义如下：

$$\varphi(Ka) = f(a)$$

我们先证明 φ 的定义是合适的，即：如果 $Ka = Kb$ ，则 $\varphi(Ka) = \varphi(Kb)$ 。假定 $Ka = Kb$ ，则 $a \cdot b^{-1} \in K$ ，于是 $f(a \cdot b^{-1}) = e_H$ ，又 $f(a) \cdot f(b)^{-1} = f(a) \cdot f(b^{-1}) = f(a \cdot b^{-1}) = e_H$ ，故 $f(a) = f(b)$ ，即 $\varphi(Ka) = \varphi(Kb)$ 。

其次证明 φ 是同态。设 $Ka, Kb \in G/K$ ，于是：

$$\begin{aligned}\varphi(KaKb) &= \varphi(Ka \cdot b) = f(a \cdot b) \\ &= f(a) \cdot f(b) = \varphi(Ka) \cdot \varphi(Kb)\end{aligned}$$

因此 φ 是一个同态。

下面再证 φ 是一一对应的，若 $\varphi(Ka) = \varphi(Kb)$ ，于是：

$$f(a) = f(b)$$

故： $f(a) \cdot f(b)^{-1} = f(a) \cdot f(b^{-1}) = f(a \cdot b^{-1}) = e_H$

所以 $a \cdot b^{-1} \in K$ ，得 $Ka = Kb$ ，另一方面，令 $h \in f(G)$ ，所以存在 $a \in G$ ，使得 $f(a) = h$ ，即 $\varphi(Ka) = f(a) = h$ ，因此 φ 是一一对应的映射。亦即：

$$(G/K, *) \cong (f(G), \cdot)$$

4.6 环、理想、整环和域

在这节，我们将研究比前面更复杂的代数系统，它具有两个运算，习惯上用 $+$ 和 $\circ$ 表示，注意， $+$ 和 $\circ$ 仅表示两种不同的二元运算符而已，不一定是普通的加和乘运算。

犹如群论的研究一样,环、理想和整环等理论知识,可以用于研究误差检测和校正码及它们的物理实现上,而这些都是计算机科学工作者所感兴趣的问题。

1. 环

定义 4-22 设代数系统 $(R, +, \circ)$ 如果对任意 $a, b, c \in R$, 它满足下列条件:

(1) 加结合律, 即:

$$(a + b) + c = a + (b + c)$$

(2) 加交换律, 即:

$$a + b = b + a$$

(3) 存在加单位元素 $0 \in R$, 使得 $a + 0 = 0 + a = a$

(4) 存在加逆元素, 即对每个 $a \in R$, 有一个 $-a \in R$, 使得 $a + (-a) = 0$

(5) 乘结合律, 即:

$$a \circ (b \circ c) = (a \circ b) \circ c$$

(6) 乘对加分配律, 即:

$$a \circ (b + c) = a \circ b + a \circ c \quad (\text{左分配律})$$

$$(b + c) \circ a = b \circ a + c \circ a \quad (\text{右分配律})$$

则称 $(R, +, \circ)$ 是一个环。通常将加单位元素 0 叫环的零元素。

从上述定义可知, (1)~(4) 是 $(R, +, \circ)$ 关于 $+$ 的阿贝尔群, 即它等价于说 $(R, +)$ 是阿贝尔群。

我们可以用 $a + (-b)$ 来定义 $a - b$, 即 $a - b \equiv a + (-b)$ 。

定义 4-23 若 $(R, +, \circ)$ 是一个环, 而且它关于 $\circ$ 满足交换律, 即对每个 $a, b \in R$, 有 $a \circ b = b \circ a$, 则称 $(R, +, \circ)$ 是个交换环。

并不是每个环均满足乘的交换律的。

对环 $(R, +, \circ)$, 若存在一个元素 $e \in R$, 使得对每个 $a \in R$, 有:

$$e \circ a = a \circ e = a$$

则称 e 是 R 的乘单位元素, 常把 e 写成 1 ; 若 $a \neq 0$, 而且对每个 $b, c \in$

R , 有:

$$a \circ b = a \circ c \Rightarrow b = c$$

$$b \circ a = c \circ a \Rightarrow b = c$$

则称 $(R, +, \circ)$ 满足乘消去律。

例如, $(\{1, 0\}, +, \circ)$ 是个交换环, 其中 $+$ 和 $\circ$ 的定义如下:

$+$	0	1	$\circ$	0	1
0	0	1	0	0	0
1	1	0	1	0	1

例 4-25 证明 $(\mathbb{Z}_n, +, \circ)$ 是个交换环, 其中 $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$, $+$ 和 $\circ$ 分别是按模 n 同余类的乘和加, 即:

$$[x] + [y] = [x + y]$$

$$[x] \circ [y] = [x \circ y]$$

证明: 可以逐条验证如下:

(1) $(\mathbb{Z}_n, +)$ 是阿贝尔群(略!)

(2) $([x] \circ [y]) \circ [z] = [x \circ y \circ z] = [x] \circ ([y] \circ [z])$

(3) $[x] \circ ([y] + [z]) = [x] \circ [y + z]$

$$= [x \circ (y + z)] = [x \circ y + x \circ z]$$

$$= [x \circ y] + [x \circ z] = [x] \circ [y] + [x] \circ [z]$$

(4) 同理可证 $([y] + [z]) \circ [x] = [y] \circ [x] + [z] \circ [x]$

故 $(\mathbb{Z}_n, +, \circ)$ 是个交换环。

另外我们最熟悉的代数系统 $(I, +, \circ)$ 是具有乘单位元素的交换环, 它满足消去律。

定理 4-30 设 $(R, +, \circ)$ 是一个环, 对每个 $a, b \in R$, 有:

$$(1) a \circ 0 = 0 \circ a = 0$$

$$(2) a \circ (-b) = (-a) \circ b = -(a \circ b)$$

$$(3) (-a) \circ (-b) = a \circ b$$

证明:

(1) $a \circ 0 = a \circ (0 + 0) = a \circ 0 + a \circ 0$, 两边加 $-(a \circ 0)$, 得 $0 = a \circ 0$, 即 $a \circ 0 = 0$ 。同理可证 $0 \circ a = 0$ 。

$$\begin{aligned}
(2) \quad (-a) \circ b &= a \circ b + (-a) \circ b - (a \circ b) \\
&= (a - a) \circ b - (a \circ b) \\
&= 0 \circ b - (a \circ b) \\
&= 0 - (a \circ b) = -(a \circ b)
\end{aligned}$$

同理可证 $a \circ (-b) = -(a \circ b)$ 。

$$(3) \quad (-a) \circ (-b) = -(a \circ (-b)) = -(-(a \circ b)) = a \circ b$$

如果环 $(R, +, \circ)$ 有非零元素 $a, b \in R$, 使得 $a \circ b = 0$, 则称 $(R, +, \circ)$ 有零因子, 此时若 a 是非零因子, 则 b 必是 $(R, +, \circ)$ 的一个零因子。反之亦然, 甚至 a 和 b 都可以是 $(R, +, \circ)$ 的零因子。

例如 $(\mathbb{Z}_4, +, \circ)$ 中有零因子, 因为 $[2] \circ [2] = [0]$ 。注意 $[0]$ 是零元素。

定理 4-31 一个环 $(R, +, \circ)$ 无零因子当且仅当环 $(R, +, \circ)$ 满足消去律。

证明: 假定 R 无零因子, 令 $a, b, c \in R$ 是满足 $a \circ b = a \circ c$ 的, (其中 $a \neq 0$), 因此 $a \circ b - a \circ c = 0$, 即 $a \circ (b - c) = 0$, 所以 $b - c = 0$, 即 $b = c$, 因此 $(R, +, \circ)$ 满足消去律。

另一方面, 用反证法: 设 R 有零因子, 令 $a, b \in R$, 使得 $a \circ b = 0$, 假定 $a \neq 0$, 有 $a \circ b - a \circ 0 = 0$, 即 $a \circ b = a \circ 0$, 由消去律得 $b = 0$, 类似地, 如果 $b \neq 0$, 则可证到 $a = 0$ 。这都与 R 有零因子相矛盾。

下面给出一个环的子环的条件。

定义 4-24 设 $(R, +, \circ)$ 是一个环, S 是 R 的非空子集, 若对每个 $a, b \in S$, 有:

- (1) $a + b \in S$
- (2) $-a \in S$
- (3) $a \cdot b \in S$

则称 $(S, +, \cdot)$ 是 $(R, +, \cdot)$ 的子环。

由于我们在 R 中可以用 $a - b \equiv a + (-b)$ 来定义减, 则条件(1)和(2)可用 $a - b$ 来代替, 而(1)和(2)蕴含着 $(S, +)$ 是 $(R, +)$ 的子群。

例 4-26 证明 $(Q(\sqrt{2}), +, \cdot)$ 是环 $(R, +, \cdot)$ 的一个子环, 其中 R 是实数集, Q 是有理数集, 而且 $Q(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in Q\}$ 。

证明: 令 $x_1 = a + b\sqrt{2}, x_2 = c + d\sqrt{2}$, 于是:

$$(1) x_1 - x_2 = (a - c) + (b - d)\sqrt{2} \in Q(\sqrt{2})$$

$$(2) x_1 \cdot x_2 = (a \cdot c + b \cdot d) + (a \cdot d + b \cdot c)\sqrt{2} \in Q(\sqrt{2})$$

所以 $(Q(\sqrt{2}), +, \cdot)$ 是 $(R, +, \cdot)$ 的一个子环。

下面给出两个环的同态和同构的定义。

定义 4-25 设 $(R, +, \cdot)$ 和 $(S, +, \cdot)$ 是两个环, $f: R \rightarrow S$ 是一个映射, 如果对所有 $a, b \in R$, 有:

$$(1) f(a + b) = f(a) + f(b);$$

$$(2) f(a \cdot b) = f(a) \cdot f(b)。$$

则称 f 是一个环同态。

如果两个环用的是不同的运算符, 例如, $(R, +, \cdot)$ 和 $(S, \oplus, \circ)$, 则 $f: R \rightarrow S$ 是环同态的条件是:

$$(1) f(a + b) = f(a) \oplus f(b)$$

$$(2) f(a \cdot b) = f(a) \circ f(b)$$

上述的 $f: R \rightarrow S$ 如果是一一对应映射, 而且又满足上述 (1)、(2) 的条件, 则 f 称为环同构映射, 亦是说环 $(R, +, \cdot)$ 和 $(S, \oplus, \circ)$ 同构, 记以 $(R, +, \cdot) \cong (S, \oplus, \circ)$, 简记为 $R \cong S$ 。

2. 理想

理想是具有特殊性质的子环, 它在环中起的作用犹如正规子群在群中的作用。

定义 4-26 设 $(R, +, \cdot)$ 是一个环, $(D, +, \cdot)$ 是它的子环, 若对每个 $a \in R, d \in D$, 有 $a \cdot d \in D, d \cdot a \in D$, 则称 $(D, +, \cdot)$ 是 $(R, +, \cdot)$ 的理想子环, 简称理想。

如果 $D = R$, 或者 $D = \{0\}$, 则称 $(D, +, \cdot)$ 是 $(R, +, \cdot)$ 的平凡理想; 否则, 便称 $(D, +, \cdot)$ 是 $(R, +, \cdot)$ 的真理想; 若 $(D, +, \cdot)$ 是

$(R, +, \cdot)$ 的真理想, 但不存在 $D' \supset D$, 使得 $(D' +, \cdot)$ 亦是 $(R, +, \cdot)$ 的真理想, 则称 $(D, +, \cdot)$ 是 $(R, +, \cdot)$ 的极大理想。

如果 $(D, +, \cdot)$ 是 $(R, +, \cdot)$ 的理想, 对某个 $g \in D$, 有 $D = \{r \cdot g \mid r \in R\}$, 则称 $(D, +, \cdot)$ 为主理想, 显然 g 是 $(D, +, \cdot)$ 的生成元素。若一个环的每个理想皆是主理想, 则该环 $(R, +, \cdot)$ 为主理想环。

例 4-27 设环 $\bar{I} = (I, +, \cdot)$ 的子环是:

$$(\{m \cdot i \mid i \in I\}, +, \cdot)$$

其中 m 是某个非负整数, 显然它是 $\bar{I}$ 的一个理想, 它还是一个主理想, 事实上, $(I, +, \cdot)$ 的每个理想都是主理想, 这点可以证明如下:

令 m 是 D 中最小的非负整数, 对任意 $n \in D$, $n = m \cdot i + r$, 其中 $0 \leq r < m$, 因为 $m \cdot i \in D$, 所以 $n - m \cdot i = r \in D$, 由假设 m 是最小的正整数, 故 $r = 0$, 即 $n = m \cdot i$ 。因此 $D = \{m \cdot i \mid i \in I\}$, 从而得出结论: $(I, +, \cdot)$ 是主理想环。

例 4-28 设 $(D_1, +, \cdot)$ 和 $(D_2, +, \cdot)$ 是环 $(R, +, \cdot)$ 的两个理想, 试证: $(D_1 \cap D_2, +, \cdot)$ 亦是 $(R, +, \cdot)$ 的一个理想。

证明: 因为 $(D_1, +, \cdot)$ 和 $(D_2, +, \cdot)$ 都是理想, 现在令 $a, b \in D_1 \cap D_2$, $r \in R$, 于是 $a, b \in D_1$, $a, b \in D_2$, 从而有:

$$a - b, r \cdot a, a \cdot r \in D_1$$

$$\text{及 } a - b, r \cdot a, a \cdot r \in D_2,$$

因此 $a - b, r \cdot a, a \cdot r \in D_1 \cap D_2$, 故 $(D_1 \cap D_2, +, \cdot)$ 是一个理想。

可利用理想推出商环。这和正规子群可推出商群相似。

定理 4-32 设 $(D, +, \cdot)$ 是 $(R, +, \cdot)$ 中的理想, D 的陪集的集合 $\{D + a \mid a \in R\}$ 形成一个环。其中运算定义如下:

$$(D + a) + (D + b) = D + (a + b)$$

$$(D + a) \cdot (D + b) = D + a \cdot b$$

这种环称为商环, 用 $(R/D, +, \cdot)$ 表示。其证明略。

3. 整环

定义 4-27 设 $(R, +, \cdot)$ 是一个具有乘单位元素的交换环, 如果

它无零因子,则称 $(R, +, \circ)$ 是一个整环。

例 4-29 设 I, Q, R 分别代表整数集、有理数集和实数集, $Z_4 = \{[0], [1], [2], [3]\}$, 则 $(I, +, \circ), (Q, +, \circ), (R, +, \circ)$ 是整环, 但是 $(Z_4, +, \circ)$ 不是整环, 因为 $[2] \circ [2] = [0]$, 所以 $[2]$ 是一个零因子。

定理 4-33 如果 a 是整环 $(D, +, \circ)$ 的一个非零元素, 且 $a \circ b = a \circ c$, 则有 $b = c$ 。

证明: 如果 $a \circ b = a \circ c$, 则 $a \circ (b - c) = 0$, 因为 D 是整环, 所以无零因子, 又 $a \neq 0$, 所以应 $b - c = 0$, 即 $b = c$ 。

环 $(Z_m, +, \circ)$ 是常遇到的, 它是否会构成一个整环呢? 下面的定理给出了它能构成整环的充要条件。

定理 4-34 环 $(Z_m, +, \circ)$ 是一个整环当且仅当 m 是一个素数。

其证明从略。

一般说来, 在环中可以加上、减去或乘以环中的元素, 但是除以环中的元素并不总是可行的, 即使在整环上, 其中元素能满足消去律, 也并不总可以用非零元素除的, 譬如说, $x, y \in I$, 则 $a \circ x = a \circ y \Rightarrow x = y$, 但不是 I 中每个元素都能用 a 除的。

最有用的数字系统是用非零元素除的那些数字系统, 这种系统称为域, 所以接着我们要介绍域的基本概念。

4. 域

定义 4-28 设代数系统 $(F, +, \circ)$ 是个交换环, 如果它:

- (1) 存在单位元素 $e \in F$, 使得对所有 $a \in F$, 有 $e \circ a = a \circ e = a$;
- (2) 对每个非零元素 $a \in F$, 存在一个元素 $a^{-1} \in F$, 使得 $a^{-1} \circ a = a \circ a^{-1} = e$ 。

则称 $(F, +, \circ)$ 是一个域。

注意, a^{-1} 是在乘意义下 a 之逆元素, $-a$ 是在加意义下 a 之逆元素。由于域 F 的加和乘的逆元素是不同的, 所以一个域 F 之基数至少是 2。

例 4-30 设 R, Q 分别是实数和有理数的集合, 则 $(R, +, \circ), (Q, +, \circ)$ 是域。

又如 $(\mathbb{Z}_3, +, \circ)$ 中 $+$, $\circ$ 定义如下:

$+$	$[0]$	$[1]$	$[2]$	$\circ$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[1]$	$[2]$	$[0]$	$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[2]$	$[0]$	$[1]$	$[2]$	$[0]$	$[2]$	$[1]$

显然 $(\mathbb{Z}_3, +, \circ)$ 是环。又因为它交换律成立,有乘单位元素 $[1]$,每个非零元素 a 有乘逆元素 a^{-1} ,即 $[1]^{-1}=[1]$, $[2]^{-1}=[2]$ 。所以 $(\mathbb{Z}_3, +, \circ)$ 是域。

定理 4-35 每个域均满足消去律(因此无零因子)。

证明: 令 $(F, +, \circ)$ 是域, 令 $a \neq 0, b$ 和 c 是 F 中元素, 如果 $a \circ b = a \circ c$, 则 $a^{-1} \circ a \circ b = a^{-1} \circ a \circ c$, 因此 $b=c$ 。

由此我们立即得到:

定理 4-36 每个域是一整环。

这条定理的逆定理一般不成立。例如 $(I, +, \circ)$ 不是域, 因为乘逆元素不存在。但当有限整环时, 其逆定理成立。

定理 4-37 每个有限整环是一个域。

证明: 令 $(D, +, \circ)$ 是一个有限整环, 设 $a, b \in D$, 而且 $a \neq b$, 于是对每个非零元素 $c \in D$, 由消去律(整环满足消去律), $a \circ c \neq b \circ c$, 因此 $D \circ c = D$, 存在 $d \in D$, 使得 $d \circ c = e$, 因此每个非零元素 c , 有乘逆元素 $c^{-1} = d \in D$, 故 $(D, +, \circ)$ 是域。

采用另一种证明方法是: 设 $D = \{a_1, a_2, \dots, a_n\}$, 令非零元素 $a \in D$, 考虑:

$$D' = aD = \{a \circ a_1, a \circ a_2, \dots, a \circ a_n\}$$

因为 a 是非零元素, 由消去律, 得:

$$a \circ a_i = a \circ a_j \Rightarrow a_i = a_j$$

因此 D' 中元素是互不相同的。它是 D 中元素的重新排列, 即 $D = D'$ 。 D' 中必有一元素(譬如说 $a \circ a_k$)等于 D 中单位元素 e , 即 $a \circ a_k = e$, 因此 a_k 是 a 的逆元素, 由于 a 是 D 中任意一个非零元素, 所以

$(D, +, \circ)$ 是一个域。

例 4-31 问 $(Q(\sqrt{2}), +, \circ)$ 是否为整环？是否为域？

解：我们已经知道， $(Q(\sqrt{2}), +, \circ)$ 是一个交换环，如果 $a + b\sqrt{2}$ 是非零元素，所以 a 和 b 至少有一个不是零，它的逆元素是：

$$\frac{1}{a + b\sqrt{2}} = \frac{a}{a^2 - 2b^2} - \frac{b\sqrt{2}}{a^2 - 2b^2}$$

这个逆元素是 $Q(\sqrt{2})$ 中的一个元素，所以 $(Q(\sqrt{2}), +, \circ)$ 是一个域，也是一个整环。

例 4-32 如 p 是素数，则 Z_p 是一个域。

解： $Z_p = \{[0], [1], \dots, [p-1]\}$ ，我们来证明 Z_p 无零因子，设任取 $[a], [b] \in Z_p$ ，假定 $[a] * [b] = [0]$ ，即 $a * b \equiv 0 \pmod{p}$ ，于是 p 整除 $a * b$ ，因为 p 是素数，所以 p 整除 a 或 b ，这样 $a \equiv 0 \pmod{p}$ ，或 $b \equiv 0 \pmod{p}$ ，即 $[a] = [0]$ 或 $[b] = [0]$ ，因此 Z_p 无零因子，它是一个整环，由于 Z_p 是有限整环，所以它是域。

例 4-33 考虑整数模 10 的 $(Z_{10}, +, \circ)$ 环，求：

(1) $-[3]$ ， $-[8]$ ，和 $[3]^{-1}$ ，

(2) 令 $f(x) = 2x^2 + 4x + 4$ ，求 $f(x)$ 在 Z_{10} 上的根。

解：(1) 由于 $-a$ 在环中，意味着 $a + (-a) = (-a) + a = 0$ ，因此 $-[3] = [7]$ ，因为 $[3] + [7] = [7] + [3] = [0]$ ；同样道理， $-[8] = [2]$ ；由于 a^{-1} 在环中，意味着 $a \circ a^{-1} = a^{-1} \circ a = e$ ，因此， $[3]^{-1} = [7]$ ，因为 $[3] \circ [7] = [7] \circ [3] = [1]$ 。

(2) 用 Z_{10} 中元素代入 x 中，看哪一个元素产生 $[0]$ 。

$$f([0]) = [4], f([1]) = [0],$$

$$f([2]) = [0], f([3]) = [4],$$

$$f([4]) = [2], f([5]) = [4],$$

$$f([6]) = [0], f([7]) = [0],$$

$$f([8]) = [4], f([9]) = [2]。$$

这根是 $[1]$ ， $[2]$ ， $[6]$ 和 $[7]$ 。这例子说明一个 n 次多项式在某一

环上可以有多个根,如果在域上则不可能出现这种情况。

4.7 偏序集和格

1. 偏序集

定义 4-29 如果 $R \subseteq A \times A$ 是自反的、反对称的和传递的,则称 R 是 A 上的一个偏序关系,集合 A 是关于 R 的偏序集,用 (A, R) 表示。

对于偏序关系 R ,通常用 $\leq$ 表示(此符号在这里并不表示小于或等于),若 $a \leq b$,可读作“ a 在 b 前”,此外还有附加的表示: $a < b$ 意指 $a \leq b$ 且 $a \neq b$,对于 $\geq, >$ 有类似的解释。

例 4-34 自然数集 N 是关于 $\leq$ 的偏序集。可以验证如下:

- (1) 自反的。对每个 $a \in N$,有 $a \leq a$;
- (2) 反对称的。对每个 $a, b \in N$,如 $a \leq b$ 且 $b \leq a$,则必有 $a = b$;
- (3) 传递的。对每个 $a, b, c \in N$,如 $a \leq b$ 且 $b \leq c$,则有 $a \leq c$ 。

例 4-35 设有两个序列 $(a_1, a_2, \dots, a_r), (b_1, b_2, \dots, b_s)$,其中 $r \leq s$,如果 $a_1 = b_1, a_2 = b_2, \dots, a_r = b_r$,则称序列 $(a_1, a_2, \dots, a_r)$ 是 $(b_1, b_2, \dots, b_s)$ 的一个前缀,这是一个关系,称为前缀关系。现在证明,集合 A 上的序列的集合 S 对前缀关系 R 是偏序的,即 (S, R) 是偏序集。

证明:

- (1) 自反的:对任意序列 $s \in S$, s 是 s 的前缀;
- (2) 反对称性:对任意序列 $s_1, s_2 \in S$,如果 s_1 是 s_2 的前缀且 s_2 是 s_1 的前缀,则 s_1 和 s_2 必有同样的元素而且逐项相等。因此 $s_1 = s_2$;

- (3) 传递性:如果 a 是 b 的前缀, b 是 c 的前缀,则 a 是 c 的前缀。

令 A 是 $\{a, b, c\}$ 上的序列的集合, P 是前缀关系,于是:

$$(a, b)P(a, b, c)$$

$$(a, b)P(a, b, a)。$$

设偏序集 $(A, \leq)$, 对任意元素 $a, b \in A$, 如果:

$$a \leq b \text{ 或 } b \leq a$$

则称 A 中的两个元素 a, b 是可比较的, 否则称 a, b 不可比较的。另一方面, 如果偏序集 A 中的每对元素均可比较, 即如对每个 $a, b \in A$, 有 $a \leq b$ 或 $b \leq a$, 则称 A 为线性次序的或全序的。如 $(\mathbb{N}, \leq)$ 就是线性次序集。

线性次序的一个重要实例是字典次序。

定义 4-30 设 Σ 是一个线性次序的有限字母表, Σ^* 是字集, 假定 $s = s_0 s_1 \cdots s_m$ 和 $t = t_0 t_1 \cdots t_n$, 其中 $s, t \in \Sigma^*$, 于是我们定义 $\leq$ 如下:

(1) s 是 t 的一个前缀, 或者

(2) 若存在 $r \leq m$ 使 $s_i = t_i (i=0, \cdots, r-1)$ 且 $s_r < t_r$, 则 $s \leq t$ 。

这就是字的次序关系的定义。比如, 字“apple”, “apply”和“application”具有通常的字母次序, 由 $(R, \leq)$ 之定义, 可以看出

$$\text{apple} < \text{application} < \text{apply}$$

再如: “add”、“addition”、“address”, 由定义(1)、(2)得出

$$\text{add} < \text{addition} < \text{address}$$

为了直观形象起见, 有限偏序集也可用图形表示, 这种图形又称哈斯(Hasse)图, 画法如下:

设有偏序集 $(A, \leq)$:

(1) A 中每个元素用小圆圈表示;

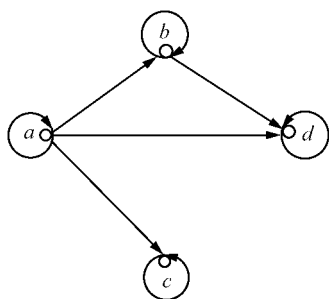
(2) 自反性不在图上表示出来;

(3) 对 $x, y \in A$, 如果 $y \leq x$ 且不存在 $z \in A$, 使得 $y \leq z$ 且 $z \leq x$, 则 x 和 y 用一条直线连接, 而且 x 画在 y 的上方;

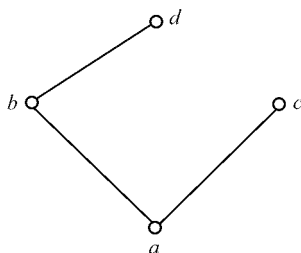
(4) 所有直线不画箭头。

例 4-36 设 $S = \{a, b, c, d\}$, 其上 $R = \{(a, a), (b, b), (c, c), (d, d), (a, b), (a, c), (a, d), (b, d)\}$, 则 (S, R) 的关系图和哈斯图如图 4-5 所示。

例 4-37 令 $A = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24\}$, 其上的关系是“ x 整除 y ”, 则其哈斯图如图 4-6 所示。



(a) (S, R) 之关系图



(b) (S, R) 之哈斯图

图 4-5 例 4-36 哈斯图

在研究格之前,先介绍最大下界和最小上界的概念。

定义 4-31 设 x 和 y 是 $(P, \leq)$ 中的任意两个元素, 对一个元素 $a \in P$, 如果 $a \leq x, a \leq y$, 而且对任何 $a' \in P$, 有 $(a' \leq x \text{ 且 } a' \leq y) \Rightarrow a' \leq a$ 。则称 a 是 x 和 y 的最大下界, 记以 $\text{glb}(x, y) = a$ 。

设 x 和 y 是 $(P, \leq)$ 中的任意两个元素, 对一个元素 $b \in P$, 如果 $x \leq b, y \leq b$, 而且对任何 $b' \in P$, 有 $(x \leq b' \text{ 且 } y \leq b') \Rightarrow b \leq b'$, 则称 b 是 x 和 y 的最小上界, 记以 $\text{lub}(x, y) = b$ 。

定理 4-38 设 x 和 y 是偏序集 $(P, \leq)$ 中的两个元素, 如果 x 和 y 有一个最大下界 glb , 则这个 glb 是惟一的, 如果 x 和 y 有一个最小上界 lub , 则这个 lub 是惟一的。

证明: 设 x 和 y 有两个最大下界 a_1, a_2 , 即 $\text{glb}(x, y) = a_1$, $\text{glb}(x, y) = a_2$, 由定义:

$$a_1 \leq x, a_1 \leq y; a_2 \leq x, a_2 \leq y,$$

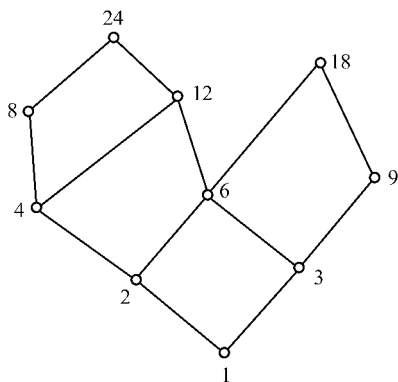


图 4-6 例 4-37 哈斯图

$$a_1 \leq a_2, a_2 \leq a_1$$

因此由反对称性,得 $a_1 = a_2$ 。

对最小上界的惟一性,用类似的方法证明。

例 4-38 对于任何一个正整数 m ,我们用 D_m 表示能整除 m 的所有因子的集合,若 $m=36$,则:

$$D_{36} = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$$

其上的关系是整除关系 $\leq$,则 $(D_{36}, \leq)$ 是偏序集。其哈斯图如图 4-7 所示。

显然图 4-7 任意两个元素 a, b 有最小上界和最大下界而且:

$$\text{glb}(a, b) = \text{gcd}(a, b)$$

其中 $\text{gcd}(a, b)$ 表示 a, b 之最大公约数:

$$\text{lub}(a, b) = \text{lcm}(a, b)$$

其中 $\text{lcm}(a, b)$ 表示 a, b 之最小公倍数。

但并不是任何情况下任意两个元素有最小上界和最大下界的,如图 4-8 表示的偏序集 $(P, \leq)$,其中 $\text{lub}(b, c) = a, \text{glb}(d, e) = f$,但是 $\text{glb}(b, c)$ 不存在, $\text{lub}(d, e)$ 不存在。

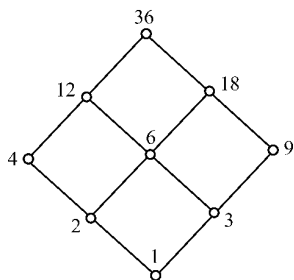


图 4-7 例 4-38 哈斯图

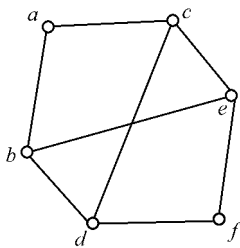


图 4-8 不存在最小上界与最大下界的偏序集

2. 格

在定义格之前,先作符号上的约定,对偏序集 $(P, \leq)$ 中的任意两个元素 x 和 y ,如果有最小上界和最大下界,用下述记号表示:

$$x \vee y = \text{lub}(x, y)$$

$$x \wedge y = \text{glb}(x, y)$$

其中“ $\vee$ ”和“ $\wedge$ ”分别称为“保联”和“保交”运算。

定义 4-32 一个格,记以 $(P, \wedge, \vee)$,是一个偏序集,其中任意两个元素 x 和 y ,有最小上界和最大下界,即:

$$x \vee y = \text{lub}(x, y)$$

$$x \wedge y = \text{glb}(x, y)$$

在不特别强调运算符的情况下, $(P, \wedge, \vee)$ 简记为 P ,格实质上是一个代数系统。

若格 P 中元素有限,则 P 是有限格。

例 4-39 幂集 $P(U)$ 上的包含关系 $\subseteq$ 定义了一个偏序集, $P(U)$ 中任意两个元素, s_1, s_2 ,有一个 lub 和一个 glb ,即:

$$\text{lub}(s_1, s_2) = s_1 \cup s_2$$

$$\text{glb}(s_1, s_2) = s_1 \cap s_2$$

因此 $(P(U), \cup, \cap)$ 是一个格。

注意,不是每个偏序集都是格,如:

$$A = \{2, 3, 4, 6, 8, 12, 36, 60\}$$

A 上的整除关系是 $\leq$,则 $(A, \leq)$ 是偏序集,但不是格。因为它不是任意两个元素有最小上界和最大下界的。如 $\text{glb}(2, 3)$ 不存在, $\text{lub}(12, 8)$ 不存在。

设 $(P, \wedge, \vee)$ 是一个格, M 是 P 的非空子集,若 $(M, \wedge, \vee)$ 也构成一个格,则称 $(M, \wedge, \vee)$ 是 $(P, \wedge, \vee)$ 的子格。我们不难得出结论: $(M, \wedge, \vee)$ 是 $(P, \wedge, \vee)$ 的子格当且仅当 M 关于 $\wedge$ 和 $\vee$ 的运算是封闭的。

定义 4-33 设 $(P, \wedge, \vee)$ 和 $(L, \wedge, \vee)$ 是两个格,若存在一一对应的映射 $f: P \rightarrow L$,使得对任意元素 $a, b \in P$,有:

$$f(a \wedge b) = f(a) \wedge f(b)$$

$$f(a \vee b) = f(a) \vee f(b)$$

则称 $(P, \wedge, \vee)$ 和 $(L, \wedge, \vee)$ 是同构的。

根据 $\vee$ 和 $\wedge$ 的定义、 glb 和 lub 的概念,我们可得出下面的关

系式：

定理 4-39 设 P 是格, 则对任意 $a, b, c \in P$, 有：

$$\text{或} \quad \left. \begin{array}{l} a \leq a \vee b, b \leq a \vee b \\ a \vee b \geq a, a \vee b \geq b \end{array} \right\} \text{(I)}$$

$$\text{或} \quad \left. \begin{array}{l} a \leq c \text{ 且 } b \leq c \Rightarrow a \vee b \leq c \\ c \geq a \text{ 且 } c \geq b \Rightarrow c \geq a \vee b \end{array} \right\} \text{(II)}$$

$$\text{或} \quad \left. \begin{array}{l} a \wedge b \leq a, a \wedge b \leq b \\ a \geq a \wedge b, b \geq a \wedge b \end{array} \right\} \text{(III)}$$

$$\text{或} \quad \left. \begin{array}{l} c \leq a \text{ 且 } c \leq b \Rightarrow c \leq a \wedge b \\ a \geq c \text{ 且 } b \geq c \Rightarrow a \wedge b \geq c \end{array} \right\} \text{(IV)}$$

这些关系式可作为证明其他关系的公理。

例 4-40 设 P 是格, 如果 $a \leq c, b \leq d$, 则有 $a \vee b \leq c \vee d$, 反之, 若 $c \leq a, d \leq b$, 则有 $c \wedge d \leq a \wedge b$ 。

证明：先证 $a \vee b \leq c \vee d$ 。由于 $c \leq c \vee d, d \leq c \vee d$, 由 $\leq$ 的传递性, $a \leq c \vee d, b \leq c \vee d$, 而 $a \vee b$ 是 a 和 b 的最小上界, 故 $a \vee b \leq c \vee d$ 。

下面再证 $c \wedge d \leq a \wedge b$ 。由于 $c \wedge d \leq c, c \wedge d \leq d$, 由 $\leq$ 的传递性, $c \wedge d \leq a, c \wedge d \leq b$, 而 $a \wedge b$ 是 a 和 b 的最大下界, 故 $c \wedge d \leq a \wedge b$ 。

上面介绍的性质, 是我们下面进一步研究格的基本出发点。

3. 格的基本定律

为证明方便起见, 介绍格中任一命题的对偶式这一概念。在格 $(P, \wedge, \vee)$ 中的一个命题的符号 $\leq, \geq, \wedge, \vee$ 依次用 $\geq, \leq, \vee, \wedge$ 替换, 就得到另一个新命题, 这个新命题是原命题的对偶式; 反之原命题也是新命题的对偶式。因此对偶式是相互的, 即甲命题是乙命题的对偶式, 乙命题也是甲命题的对偶式。如：

甲命题	乙命题
$a \leq a \vee b$	$a \geq a \wedge b$
$a \wedge (b \vee a) = a \vee a$	$a \vee (b \wedge a) = a \wedge b$

均互为对偶式。

下面是一条对偶定律。

对偶定律：在格 $(P, \wedge, \vee)$ 中,任何一条定理的对偶式是一条定理。

现在我们证明格中一些重要的基本定理。

定理 4-40 设 P 是格,对每个 $a \in P$,有:

$$(1) a \vee a = a \quad (2) a \wedge a = a$$

证明：先证明(1)。因为 $a \leq a \vee a$,由 $\leq$ 的自反性, $a \geq a$,由(II)
 $a \geq a \vee a$,由 $\leq$ 的反对称性,得:

$$a \vee a = a$$

由对偶定律,

$$a \wedge a = a$$

这条定理称为等幂律。

定理 4-41 设 P 是格,对每个 $a, b \in P$,有:

$$(1) a \vee b = b \vee a \quad (2) a \wedge b = b \wedge a$$

证明：先证明(1)。因为 $a \vee b \geq b$, $a \vee b \geq a$,由(II) $a \vee b \geq b \vee a$,
另一方面 $b \vee a \geq a$, $b \vee a \geq b$,由(II), $b \vee a \geq a \vee b$,由 $\leq$ 的反对称性,得:

$$a \vee b = b \vee a$$

由对偶定律, $a \wedge b = b \wedge a$ 亦成立。

所以 $\vee$ 和 $\wedge$ 运算都满足交换律。

定理 4-42 设 P 是格,则对每个 $a, b, c \in P$,有:

$$(1) a \vee (b \vee c) = (a \vee b) \vee c$$

$$(2) a \wedge (b \wedge c) = (a \wedge b) \wedge c$$

证明：先证明(1)。令 $x = a \vee (b \vee c)$, $y = (a \vee b) \vee c$,由(I), $x \geq a$
而且 $x \geq b \vee c$,由(I)及传递性, $x \geq b$ 而且 $x \geq c$ 。现在由 $x \geq a$, $x \geq b$ 得
 $x \geq (a \vee b)$,再由 $x \geq (a \vee b)$ 及 $x \geq c$ 得 $x \geq (a \vee b) \vee c$,故 $x \geq y$ 。

同理可证明 $x \leq y$,由反对称性得 $x = y$,即 $a \vee (b \vee c) = (a \vee b) \vee c$ 。

由对偶定律得: $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ 。

所以 $\vee$ 和 $\wedge$ 运算满足结合律。

定理 4-43 设 P 是格, 对每个 $a, b \in P$, 有:

$$(1) a \vee (a \wedge b) = a$$

$$(2) a \wedge (a \vee b) = a$$

证明: 先证明(1)因为 $a \leq a \vee (a \wedge b)$, 由 $\leq$ 的自反性, 有 $a \geq a$, 由(Ⅲ) $a \geq a \wedge b$, 再由(Ⅱ) $a \geq a \vee (a \wedge b)$, 由反对称性, 得:

$$a \vee (a \wedge b) = a$$

根据对偶定律, 立即得到:

$$a \wedge (a \vee b) = a$$

所以 $\vee$ 和 $\wedge$ 运算满足吸收律。

定理 4-44 设 P 是格, 则对每个 $a, b \in P$, 有:

$$a \wedge b = a, \text{ 当且仅当 } a \vee b = b$$

证明: 假定 $a \wedge b = a$, 利用吸收律, 有:

$$\begin{aligned} b &= b \vee (b \wedge a) = b \vee (a \wedge b) \\ &= b \vee a = a \vee b \end{aligned}$$

反之, 假定 $a \vee b = b$, 由吸收律, 有:

$$a = a \wedge (a \vee b) = a \wedge b$$

因此 $a \wedge b = a$ 当且仅当 $a \vee b = b$

下面我们讨论几种特殊的格。

4. 分配格

定义 4-34 如果格 P 满足分配律, 即对任意 $a, b, c \in P$, 有:

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

则称格 P 是一个分配格。

例 4-41 图 4-9 表示的三个格, 哪个是分配格? 哪个不是分配格?

解: (a)不是分配格, 因为:

$$b \wedge (c \vee d) = b \wedge a = b \quad \text{而:}$$

$$(b \wedge c) \vee (b \wedge d) = e \vee e = e$$

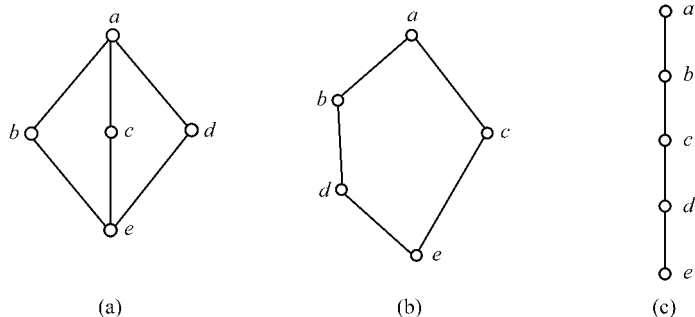


图 4-9 例 4-41 示例图

同理, (b) 也不是分配格, 但 (c) 是分配格。所以不是所有的格都是分配格。

5. 有界格

首先, 我们引进偏序集 $(P, \leq)$ 的上界和下界的概念。

定义 4-35 设 a 是偏序集 $(P, \leq)$ 的一个元素, 并且:

(1) 如果对每个 $x \in P$, 有 $a \leq x$, 则称 a 是 $(P, \leq)$ 的下界。

(2) 如果对每个 $x \in P$, 有 $x \leq a$, 则称 a 是 $(P, \leq)$ 的上界。

下界和上界亦称最小元素和最大元素。在例 4-38 中, 上界是 36, 下界是 1, 在图 4-8 中, 上界是 a , 下界是 f 。

定理 4-45 如果偏序集 $(P, \leq)$ 有下界, 则这个下界是惟一的, 如果有上界, 则这个上界是惟一的。

证明: 用反证法。设有两个下界 $a_1, a_2 \in P$, 因为 a_1 是 $(P, \leq)$ 的下界, 故 $a_1 \leq a_2$, 又因为 a_2 是 $(P, \leq)$ 的下界, 故 $a_2 \leq a_1$, 由此得出 $a_1 = a_2$ 。

对上界惟一性的证明从略。

例如, 非负整数集有通常的次序:

$$0 < 1 < 2 < 3 < \dots$$

显然 0 是下界, 但是它无上界。

有限集合 S , 其幂集是 $\rho(S)$, 则 $(\rho(S), \subseteq)$ 是个偏序集, 空集 $\emptyset$ 是其下界, S 是其上界。

定义 4-36 如果一个格既有下界(记以 0)又有上界(记以 1), 则称这格为有界格。

例 4-42 设 P 是一个有界格, 则对任意元素, $a \in P$, 有:

$$\begin{aligned} a \vee 1 &= 1 & a \vee 0 &= a \\ a \wedge 1 &= a & a \wedge 0 &= 0 \end{aligned}$$

证明: $a \vee 1 = 1$ 。因为 $a \vee 1 \in P$, 而且 1 是 $(P, \leq)$ 的上界, 故 $a \vee 1 \leq 1$; 另一方面 $1 \leq a \vee 1$, 由反对称性, $a \vee 1 = 1$ 。

对其余三个等式的证明从略。由此可知, 1 是 $(P, \wedge, \vee)$ 关于 $\wedge$ 的恒等元素, 0 是 $(P, \wedge, \vee)$ 关于 $\vee$ 的恒等元素, 由于格若有界, 则 1 和 0 是惟一的, 所以从偏序图上看 1 是在偏序图的最上层, 0 是在最下层。

假定 $P = \{a_1, a_2, \dots, a_n\}$, P 是一个有限格, 则 $a_1 \vee a_2 \vee \dots \vee a_n$ 是它的上界, $a_1 \wedge a_2 \wedge \dots \wedge a_n$ 是它的下界。因此对每个有限格, 它的上界和下界总是存在的。

6. 有补格

定义 4-37 设 P 是一个有界格, 如果对每个元素 $a \in P$, 有一个元素 $\bar{a} \in P$, 使得:

$$a \vee \bar{a} = 1 \quad a \wedge \bar{a} = 0$$

则称格 P 是一个有补格。其中 $\bar{a}$ 是 a 的补元。

显然 $\bar{0} = 1, \bar{1} = 0$

一个格如果它既是有补格, 又是分配格, 则称这种格是有补分配格。有补分配格又称布尔代数。对有补分配格, 有下述定理:

定理 4-46 在一个有补分配格 P 中, 任何一个元素 $a \in P$ 的补元是惟一的。

证明: 反证法。对元素 $a \in P$, 假定有两个补元 $a_1, a_2 \in P$,

使得:

$$a \vee a_1 = 1, a \wedge a_1 = 0$$

$$a \vee a_2 = 1, a \wedge a_2 = 0$$

因此: $a_1 = a_1 \wedge 1 = a_1 \wedge (a \vee a_2)$

$$= (a_1 \wedge a) \vee (a_1 \wedge a_2)$$

$$= 0 \vee (a_1 \wedge a_2)$$

$$= (a_2 \wedge a) \vee (a_2 \wedge a_1)$$

$$= a_2 \wedge (a \vee a_1)$$

$$= a_2 \wedge 1 = a_2$$

定理 4-47 (德·摩根定理)

设 P 是有补分配格, 则对每个 $a_1, a_2 \in P$, 有:

$$(1) \overline{a_1 \vee a_2} = \bar{a}_1 \wedge \bar{a}_2$$

$$(2) \overline{a_1 \wedge a_2} = \bar{a}_1 \vee \bar{a}_2$$

证明: 先证明(1)。利用分配律:

$$(a_1 \vee a_2) \wedge (\bar{a}_1 \wedge \bar{a}_2)$$

$$= (a_1 \wedge \bar{a}_1 \wedge \bar{a}_2) \vee (a_2 \wedge \bar{a}_2 \wedge \bar{a}_1)$$

$$= 0 \vee (a_2 \wedge \bar{a}_2 \wedge \bar{a}_1) = 0$$

$$(a_1 \vee a_2) \vee (\bar{a}_1 \wedge \bar{a}_2)$$

$$= (a_1 \vee a_2 \vee \bar{a}_1) \wedge (a_1 \vee a_2 \vee \bar{a}_2)$$

$$= 1 \wedge 1 = 1$$

因此(1)成立。根据对偶原理,(2)亦成立。

习 题 四

4.1 设在实数集 R 上的 $*$ 运算定义如下:

$$a * b = a + b + 2ab$$

(1) 求 $2 * 3, 3 * (-5), 7 * \frac{1}{2}$;

(2) $(R, *)$ 是否半群? 是否交换半群?

- (3) 求单位元素；
- (4) 哪些元素有逆元素？逆元素是什么？

4.2 下面一张表,其中最左边的表示各个集合,顶上一行表示各种运算,问它们是否为封闭的?填上“是”或“否”。

集 合 \ 运 算	+	×	-	$ x-y $	max	min
I						
N						
$\{x 0 \leq x \leq 10\}$						
$\{x -10 \leq x \leq 0\}$						
$\{2x x \in I\}$						

4.3 下表的各运算都是定义在实数集上的,问各种性质是否成立?填上“是”或“否”。

性 质 \ 运 算	+	-	×	÷	max	min	$ x-y $
结 合 律							
交 换 律							
单位元素							
逆 元 素							

4.4 设 N_k 是开始 k 个自然数(包括零)之集合,即 $N_k = \{0, 1, \dots, k-1\}$, N_k 上的运算 f_k 定义如下:

$$xf_ky = \begin{cases} x+y & \text{当 } x+y < k \text{ 时} \\ x+y-k & \text{当 } x+y \geq k \text{ 时} \end{cases}$$

问: f_k 是否满足结合律? 单位元素是什么? 每个元素的逆元素是什么?

4.5 设 A 是一个非空集合, A 上的运算定义如下: $a * b = a$, 假定 A 的元素数目大于 1,

- 问(1) $(A, *)$ 是半群吗?
- (2) $(A, *)$ 是交换半群吗?

(3) $(A, *)$ 有单位元素吗?

4.6 证明如果 $(G, *)$ 是阿贝尔群, 则对任意 $a, b \in G$, 有

$$(a * b)^n = a^n * b^n$$

4.7 设 R 是实数集合, 证明 R 的可以写成 $f(x) = ax + b$ (a, b 是实数, $a \neq 0$) 形式的所有变换构成一个群 (称为变换群), 它是否为阿贝尔群?

4.8 证明一个变换群的单位元素一定是恒等映射。

4.9 设 G 是阶为 6 的群, 证明 G 至多有一个阶为 3 的子群。

4.10 证明如果群 $(G, *)$ 中每个元素的逆元是它自己, 则该群必定是阿贝尔群。

4.11 证明阶是素数的群必定是循环群。

4.12 设 H 是 G 的子群, 具有性质: H 的任意两个左陪集的乘积仍是一个左陪集, 则 H 是 G 的一个正规子群。

4.13 找出 $(\mathbb{Z}_{12}, +_{12})$ 的所有子群。

4.14 求 $(\mathbb{Z}_6, +_6)$ 中子群 $H = \{[0], [3]\}$ 的左陪集和右陪集, 问左右陪集是否相等。

注: $+_{12}$ 表示模 12 相加, $+_6$ 表示模 6 相加。

4.15 设 $(H, *)$ 是 $(G, *)$ 的子群, 证明: $H = Ha$ 当且仅当 $a \in H$

4.16 假定 H 和 N 是 G 的子群, 且 N 是 G 的正规子群, 证明 $H \cap N$ 是 H 的正规子群。

4.17 假定 J 和 K 是环 R 的理想子环, 证明 $J \cap K$ 也是 R 的理想子环。

4.18 设 $(R, +, \cdot)$ 是一个环, a, b, c 是 R 中任意元素, 证明

(1) 如果 $a \cdot b = b \cdot a$, 则

$$a \cdot (-b) = (-b) \cdot a \text{ 及 } a \cdot (b^{-1}) = (b^{-1}) \cdot a$$

(2) 如果 $a \cdot b = b \cdot a$ 并且 $a \cdot c = c \cdot a$, 则

$$a \cdot (b + c) = (b + c) \cdot a \text{ 及 } a \cdot (b \cdot c) = (b \cdot c) \cdot a$$

4.19 设 $(R, +, \cdot)$ 是一个环, R 的子群 G 定义如下:

$$G = \{a \mid a^{-1} \in R\}$$

证明 $(G, \cdot)$ 是一个群

4.20 设 $(R, +, \cdot)$ 是一个环, 其中对每个 $a \in R$, 有 $a^2 = a$, (这种环称为布尔环),

(1) 证明 R 一定满足交换律。

(2) 证明对所有 $a \in R, a + a = 0$ 。

(3) 如果 $|R| > 2$, 则 $(R, +, \cdot)$ 不可能是整环。

4.21 构造具有三个元素的一个域。

4.22 代数系统 $(F, +, \cdot)$ 定义如下:

+	a	b	c	d	•	a	b	c	d
a	a	b	c	d	a	a	a	a	a
b	b	a	d	c	b	a	b	c	d
c	c	d	a	b	c	a	c	d	b
d	d	c	b	a	d	a	d	b	c

(1) 证明 $(F, +, \cdot)$ 是一个域。

(2) 在 $(F, +, \cdot)$ 中解下面方程组:

$$\begin{cases} x + cy = a \\ cx + y = b \end{cases}$$

4.23 设 $(F, +, \cdot)$ 是一个域, $(R, +, \cdot)$ 是 $(F, +, \cdot)$ 的子环, 证明 $(R, +, \cdot)$ 是否一定为一个整环。

4.24 图 4-10 是四个偏序集的图形, 这些偏序集能构成格吗?

4.25 证明: 如果 $(L, \vee, \wedge)$ 是一个有限格, 那么 L 一定既有最大元素, 又有最小元素。

4.26 在格 $(\rho(A), \vee, \wedge)$ 中, $A = \{a, b, c, d, e, f, g, h, i\}$, 计算 $\pi_1 \vee \pi_2, \pi_1 \wedge \pi_2$, 其中:

$$\pi_1 = \{\{a, d\}, \{b, c\}, \{e, g, i\}, \{f\}, \{h\}\}$$

$$\pi_2 = \{\{a, f\}, \{b, c\}, \{d\}, \{e, h\}, \{g, i\}\}$$

4.27 图 4-9 表示的次序图哪些格是有补格?

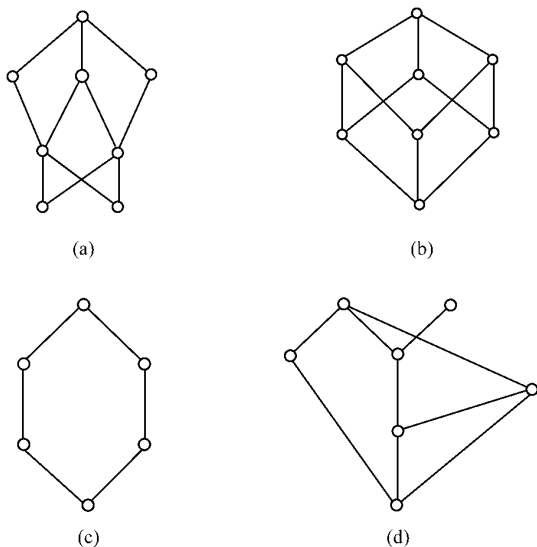


图 4-10

4.28 用一个例子说明不是每个有补格都是分配格,也不是每个分配格都是有补格。

4.29 图 4-11 表示一个有补格 $(L, \vee, \wedge)$ 的次序图,决定 L 中每个元素的补元。

4.30 下列运算中,哪些运算关于整数集不能构成半群? ()

A. $a \circ b = \max(a, b)$

B. $a \circ b = b$

C. $a \circ b = 2ab$

D. $a \circ b = |a - b|$

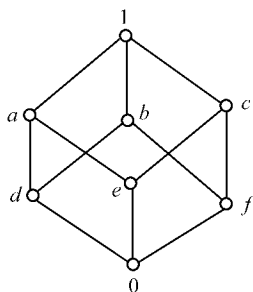


图 4-11

4.31 设 $(H, 0)$ 和 $(K, 0)$ 是 $(G, 0)$ 的子群, 下面哪个代数系统仍是 $(G, 0)$ 的子群? ()

A. $(HK, 0)$

B. $(H \cap K, 0)$

C. $(H - K, 0)$

D. $(K - H, 0)$

4.32 在代数系统中,整环和域的关系为()

- A. 整环一定是域 B. 域不一定是整环
C. 域一定是整环 D. 域一定不是整环

4.33 下面哪个偏序集构成有界格?()

- A. $(N, \leq)$ $N = \{0, 1, 2, \dots\}$
B. $(I, \geq)$ I 为整数集合
C. $(\{2, 3, 4, 6, 12\}, |)$ $|$ 表示整除关系
D. $(\rho(A), \subseteq)$ $A = \{a, b, c\}$

4.34 设 $(\{a, b, c, d\}, *)$ 是四阶群, e 为单位元素, 当四阶群含有 _____ 元素时, 这个群称为循环群; 阶相同的循环群是 _____。

4.35 一个格, 可以记为 $(P, \wedge, \vee)$ 是一个偏序集, 其中任意两个元素, x, y , 有 _____ 和 _____; 即 $x \vee y =$ _____, $x \wedge y =$ _____。

4.36 $f: G \rightarrow H, (G, \circ)$ 和 $(H, *)$ 是群同态, e_G 和 e_H 分别是单位元素, $x_1, x_2 \in G, y_1, y_2 \in H, f(x_1) = y_1, f(x_2) = y_2$ 下面不成立的结论是()

- A. $f(y_1 * y_2) = x_1 \circ x_2$ B. $f(e_G) = e_H$
C. $f(x_1^{-1}) = y_1^{-1}$ D. $f(x_1 \circ x_2) = y_1 * y_2$

4.37 I 是整数集合, $I_n = \{0, 1, 2, \dots, n-1\}$ $(G, *)$ 是一个循环群, 下列结论成立的是()

- A. $(G, *)$ 与 $(I, +)$ 或 $(I_n, +_n)$ 同构, 二者必有一个成立 ($+_n$ 是模 n 的加法)
B. $(G, *)$ 为无限循环群时, 不可能与 $(I, +)$ 同构
C. $(G, *)$ 为 n 阶循环群时, 不可能与 $(I_n, +_n)$ 同构
D. $(I, +), (I_n, +_n)$ 本身都不是循环群

4.38 S 是所有 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 形式的 2×2 矩阵的集合, 其中 a, b, c, d 是有理数, $*$ 是矩阵乘法, 代数系统 $(S, *)$ 中的单位元素是 _____;

零元素是_____。

4.39 设 $(A, |)$ 为偏序关系,其中 $|$ 为整除关系,即 $a|b$,当且仅当 a 整除 b

$$A = \{1, 2, 3, 5, 6, 15, 30\}$$

试画出这个偏序关系的哈斯图,并判定是否为格。

4.40 $(G, *)$ 是群,下列性质不成立的是()

A. 对任何 $a, b \in G$,存在惟一的 x 满足 $a * x = b$

B. 对任何 $a, b \in G$,存在惟一的 y 满足 $y * a = b$

C. A, B 中的 $x = y$

D. $c, a, b \in G$,若 $a * c = a * b$,则 $b = c$

4.41 $(G, *)$ 是阿贝尔群, $a, b \in G$, a 的阶为7, b 的阶为5,则 $a * b$ 的阶为()

A. 7

B. 35

C. 12

D. 5

4.42 $(F, +, \circ)$ 是域,下述条件可以不成立的是()

A. $(F, +)$ 和 $(F, \circ)$ 都有单位元素

B. $(F, +)$ 和 $(F, \circ)$ 都有逆元素

C. $+$ 对 $\circ$ 有分配律, $\circ$ 对 $+$ 也有分配律

D. $(F, +)$ 和 $(F, \circ)$ 都满足交换律

4.43 每个循环单元半群都是_____交换的,可交换的单元半群_____生成元素。

4.44 若同构的群认为是相同的,那么3阶群有_____个,4阶群_____个。

4.45 如果一个代数系统 $(S, *)$ 有单位元素,那么在什么条件下,可以保证一个元素的左逆元素等于右逆元素,且一个元素的逆元素是惟一的。

4.46 $(G, *)$ 是群, $a \in G$,其阶为12, $b = (a^{-1})^8$,则 b 的阶为()

A. 3

B. 8

C. 12

D. 24

4.47 $(G, *)$ 是有限群,下列结论是错误的为()

A. 每个元素的阶都是有限的

- B. 阶大于 2 的元素数目是偶数
 C. 阶大于 2 的元素数目是奇数
 D. 若 $|G|=2n$, 则阶为 2 的元素数目是奇数

4.48 代数系统 $(A, +, \circ)$ 是交换环, 下述可以不满足的条件是()

- A. $(A, +)$ 和 $(A, \circ)$ 都满足结合律
 B. $(A, +)$ 和 $(A, \circ)$ 都满足交换律
 C. 乘 $(\circ)$ 对加 $(+)$ 满足分配律
 D. 加 $(+)$ 对乘 $(\circ)$ 也满足分配律

4.49 若 A 是关于 R 的偏序集, 下述结论可以不成立的是()

- A. R 满足自反性
 B. A 中任意两个元素 a, b 都是可比较的, 即有 $(a, b) \in R$ 或 $(b, a) \in R$
 C. R 满足传递性
 D. R 满足反对称性

4.50 代数系统 $(I, *)$, 对 $a, b \in I, a * b = a + b - ab$, 因为对任何 $a, b, c \in I$ 有 $(a * b) * c = a + b - ab + c - (a + b - ab)c = a + b + c - ab - ac - bc + abc = a * (b * c)$, 又因为存在 _____ 是 _____, 所以 $(I, *)$ 是单元半群。

4.51 代数系统 $(\rho(A), \cup)$ 中单位元素为 _____; 零元素为 _____。

4.52 已知 $A = \{a, b, c\}$, 代数系统 $(A, *)$ 的运算表为

$*$	a	b	c
a	a	b	c
b	b	a	c
c	c	c	c

试讨论 $(A, *)$ 的有关特征。

4.53 设 $(H, *)$ 是 $(G, *)$ 的子群, $a, b \in G$, 下列结论成立的是()

A. $aH=bH$

B. $Ha=Hb$

C. $aH=bH$ 或者 $(aH) \cap (bH) = \emptyset$

D. $(aH) \cap (bH) = \emptyset$

4.54 代数系统 $(A, +, \circ)$ 是环, 下述可以不满足的条件是 ()

A. $(A, +)$ 和 $(A, \circ)$ 都有单位元素

B. $(A, +)$ 和 $(A, \circ)$ 都满足结合律

C. $(A, +)$ 满足交换律

D. 乘 $(\circ)$ 对加 $(+)$ 满足分配律

4.55 群 $(I, +)$, I 是整数集合, 是一个循环群, 其生成元是 _____ 和 _____。 _____ 则称 $(A, \circ)$ 和 $(B, *)$ 同构。

4.56 给定环 $(\{5x | x \in I\}, +, \cdot)$, 其中 I 是整数集, $+$ 和 $\cdot$ 是普通的加法和乘法, 它 _____ 整环, 因为 _____。

4.57 R 和 R^+ 分别是实数和正实数集, $+$, $*$ 表示通常的加法和乘法, 试证明 $(R, +)$ 和 $(R^+, *)$ 同构。

“近世代数”复习提纲

1. 主要内容

——代数系统一般性介绍。

——群论。

——其他代数系统。

2. 复习重点

——代数系统的一般知识及全貌。

——群论。

3. 代数系统

——代数系统: 集合上具有封闭性的运算所构成的系统

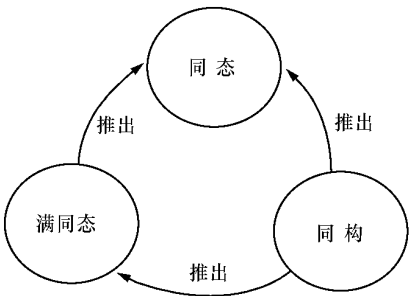
$(S, \circ)$ 。

- 运算:是一种特殊的映射。
- 运算分类:一元运算、二元运算、 n 元运算。
- 运算封闭性: $a, b \in A$, 则 $a \circ b \in A$ 。
- 代数子系统(或称子代数): $(S, \circ)$ 中如有 $S' \subseteq S, a, b \in S'$ 有: $a * b = a \circ b$ 则称 $(S', *)$ 为 $(S, \circ)$ 的子系统。
- 代数系统六个性质

- 结合律: $(a \circ b) \circ c = a \circ (b \circ c)$ 。
- 交换律: $a \circ b = b \circ a$ 。
- 分配律: $a \circ (b * c) = (a \circ b) * (a \circ c)$ 。
- 单位元: $a \circ e = a$ 。
- 逆元: $a \circ a^{-1} = e$ 。
- 零元: $a \circ 0 = 0$ 。

——代数系统的同构与同态

- 同态: $(x, \circ)$ 与 $(y, *)$ 存在 $g: X \rightarrow Y$ 使得如 $x_1, x_2 \in X$, 则有:
 $g(x_1 \circ x_2) = g(x_1) * g(x_2)$ 。
- 满同态: $(x, \circ)$ 与 $(y, *)$ 存在一一对应 $g: x \rightarrow y$, 使得如 $x_1, x_2 \in X$, 则有:
 $g(x_1 \circ x_2) = g(x_1) * g(x_2)$ 。
- 同构: $(x, \circ)$ 与 $(y, *)$ 存在一一对应 $g: x \rightarrow y$, 使得如 $x_1, x_2 \in X$, 则有:
 $g(x_1 \circ x_2) = g(x_1) * g(x_2)$ 。
- 同态、满同态及同构间的关系如下图所示:



4. 半群与群

——半群与单元半群

- 半群:代数系统满足结合律。
- 单元半群:具单位元的半群。
- 交换单元半群:具交换律的单元半群。
- 循环单元半群:含有生成元的单元半群。

——群的基本概念

- 群:代数系统满足结合律并有单位元。
- 交换群:满足交换律的群。
- 有限群与无限群:群 $(G, *)$ 中 $|G|$ 有限则称有限群; $|G|$ 无限

则称无限群。

- 子群: G 上的子集所构成的群。
- 群同态:群 $(G, \circ)$ 与 $(H, *)$ 有 $f:G \rightarrow H, a, b \in G$, 有: $f(a \circ b)$
 $= f(a) * f(b)$ 。

• 群同构:群 $(G, \circ)$ 与 $(H, *)$ 有 $f:G \rightarrow H$ 一一对应, $a, b \in G$,
有: $f(a \circ b) = f(a) * f(b)$ 。

——群的性质

- 群 $(G, *)$ 的方程式 $a * x = b, y * a = b$ 存在惟一解;
- 群 $(G, *)$ 满足消去律:由 $a * b = a * c$ 可得: $b = c$;由 $b * a =$
 $c * a$ 可得 $b = c$;

- 群 $(G, *)$ 中元素 a 的阶为 r 则 $a^k = e \Leftrightarrow k$ 是 r 倍数;
- 群 $(G, *)$ 中元素有 a 的阶与 a^{-1} 的阶相等;
- 可换群 $(G, *)$ 中元素 a, b 的阶分别为 r, s , 如有 $(r, s) = 1$ 则

$a * b$ 之阶为 rs ;

- 有限群 $(G, *)$ 中元素的阶为有限且最多不超过 $|G|$;
- 同构两个群间对应元素有相同阶。

——子群性质

- 群与其子群的单位元相同;

- 群的一个子代数亦必为群；
- 两个子群的交亦必为子群。

——循环群

• 群 $(G, *)$ 中存在 $g \in G$ 有 $G = \{g^n \mid g \in G, n \in I\}$ 则称它是循环群, g 称生成元素。

• 群 $(G, *)$ 中 g 的阶为 m 则 $(H, *)$ (中 $H = \{gr \mid r \in I\}$)是 G 的 m 阶子群也是循环群。

• 有限群 $(G, *)$ 有阶 n , 若 g 的阶也为 n , 则该群是由 g 生成的循环群。

- 一个循环群的子群也是循环群。
- 一个循环群的满同态群也是循环群。

——置换群

• 集合 P 置换所构成的集合 $E(P)$ 与置换的复合运算 $*$ 所构成的群 $(E(P), *)$ 称为置换群。

• 集合 $P(|P|=n)$ 上所有置换所构成的集合与置换复合运算 $*$ 必构成群, 称 n 次对称群。

- n 次对称群 $(G, *)$ 中 $|P|=n!$ 。

——陪集与 Lagrange 定理

• 陪集: H 是 G 的子群, $Ha = \{ha \mid h \in H\}$, $aH = \{ah \mid h \in H\}$ 分别称 H 在 G 中的右陪集、左陪集。

• Lagrange 定理: 有限群 $(G, *)$ 及其子群 $(H, *)$, 则必有 $|G|/|H|=k$ 。

——正规子群、商群与同态群

• 正规子群: 群 $(G, *)$ 子群 $(H, *)$ 如有: $a \in G$ 则 $aH = Ha$ 则称 H 是 G 的正规子群。

• 商群: H 是 G 的正规子群, 对 $Ha, Hb \in G/H$, 二元运算 $Ha * Hb = Hab$ 构成群, 则称 H 是 G 的商群, 记以 $(G/H, *)$ 。

• f 的同态核: f 是 $(G, \circ)$ 到 $(G' \otimes)$ 的群同态, 则 G 的子集 $K = \{k \mid k \in G, f(k) = e_{G'}\}$ 称 f 的同态核。

• 同态定理, f 是群 $(G, \circ)$ 与 $(G' \otimes)$ 的满同态, K 是 f 的同态核, 则必有: $(G/K, *)$ 与 $(G' \otimes)$ 同构。

5. 其他代数系统

——环

• $(R, +, \circ)$ 对 $(R, +)$ 可换群; $(R, \circ)$ 半群; 运算 $\circ$ 对 $+$ 满足分配律。

• 交换环: 环 $(R, +, \circ)$ 满足对 $\circ$ 的交换律。

• 环的运算

$$a \circ 0 = 0 \circ a = 0;$$

$$a \circ (-b) = (-a) \circ b = -(a \circ b);$$

$$(-a) \circ (-b) = a \circ b.$$

• 环中无零因子 $\Leftrightarrow$ 环满足消去律。

• 子环: 环 $(R, +, \circ)$ 如有 $S \subseteq R$, $(S, +, \circ)$ 也是环, 则称 S 是 R 子环。

• 环 $(R, +, \circ)$ 如有 $S \subseteq R$ 且 $a + b \in S$, $-a \in S$, $a \circ b \in S$ 则 S 是 R 子环。

——理想

• 理想: 环 $(R, +, \circ)$ 有子环 $(D, +, \circ)$, 如 $a \in R, d \in D$, 有 $a \circ d \in D, d \circ a \in D$ 则称 $(D, +, \circ)$ 是 R 理想(子环)。

• D_1 与 D_2 是环 $(R, +, \circ)$ 理想, 必有 $D_1 \cap D_2$ 是 R 理想。

• 商环: 环 $(R, +, \circ)$ 的理想 D , 其中 $(D, +)$ 的陪集集合 $\{D + a \mid a \in R\}$ 形成环, 其运算为: $(D + a) \oplus (D + b) = D + (a + b)$, $(D + a) \circ (D + b) = D + (a \circ b)$, 该环 $(R/D, \oplus, \circ)$ 称 R 关于 D 的商环。

——整环

• 整环: $(R, +, \circ)$ 是具有单位元交换环, 如无零因子则称其为整环。

• 整环: $(R, +, \circ) a \neq 0$, 如有 $a \circ b = a \circ c$ 则必有 $b = c$ 。

• 环: $(Em, +, \circ)$ 是整环 $\Leftrightarrow m$ 为素数。

——域

• 环: $(R, +, \circ)$ 中运算 $\circ$ 满足交换律, 有单位元、逆元。

- 域满足消去律。
- 域是整环。
- 有限整环是域。

——偏序集

- 偏序集: $R \subseteq A \times A$ 满足自反、反对称及传递。
- 线性次序: (R, A) 上 $a, b \in A$ 有 ab 或 $b \leq a$ 则称 A 为线性次序。

字典次序: 线性次序一种特例。

——格

- 格 $(P, \wedge, \vee)$ 是偏序集, 且有 $x \vee y = \text{lub}(x, y), x \wedge y = \text{glb}(x, y)$ 。
- 格的运算性质:

$$\left. \begin{array}{l} a \leq a \vee b, b \leq a \vee b \\ a \vee b \geq a, a \vee b \geq b \end{array} \right\} \text{I}$$

$$\left. \begin{array}{l} a \leq c \text{ 且 } b \leq c \Rightarrow a \vee b \leq c \\ c \geq a \text{ 且 } c \geq b \Rightarrow c \geq a \vee b \end{array} \right\} \text{II}$$

$$\left. \begin{array}{l} a \wedge b \leq a, a \wedge b \leq b \\ a \geq a \wedge b, b \geq a \wedge b \end{array} \right\} \text{III}$$

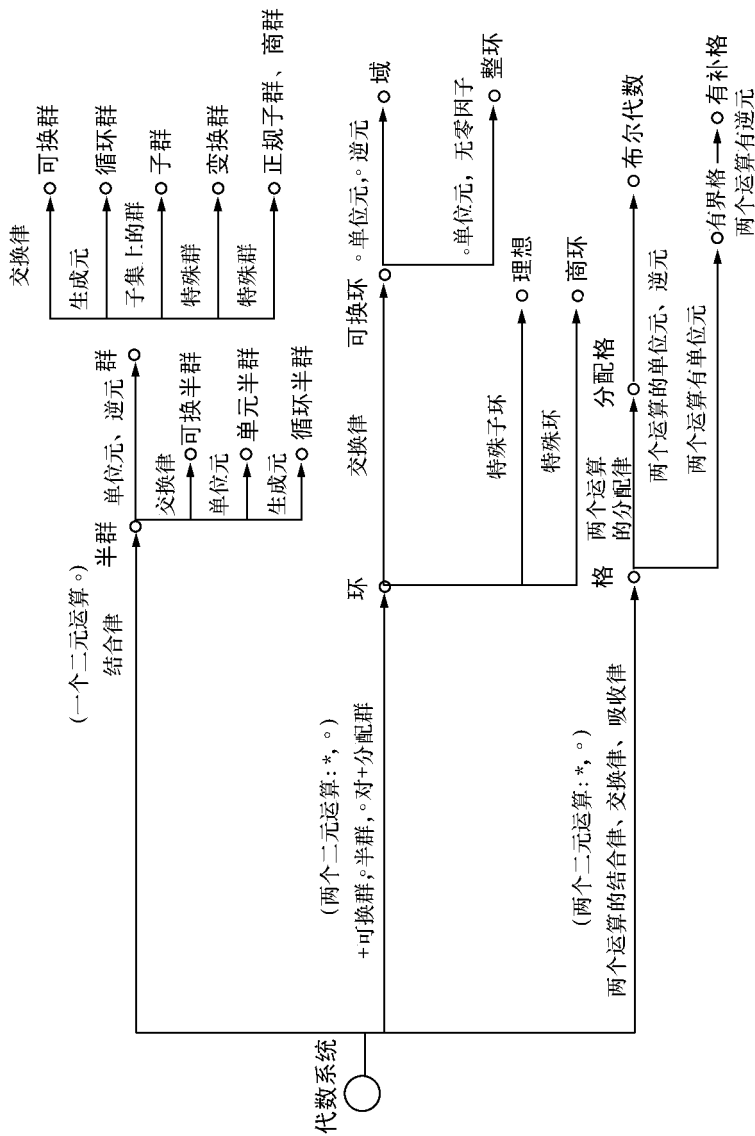
$$\left. \begin{array}{l} c \leq a \text{ 且 } c \leq b \Rightarrow c \leq a \wedge b \\ a \geq c \text{ 且 } b \geq c \Rightarrow a \wedge b \geq c \end{array} \right\} \text{IV}$$

- 格 $(P, \wedge, \vee)$ 中的任一定理的对偶式也是定理。
- 格满足结合律、交换律、等幂律、吸收律。
- 分配格: 满足分配律的格。
- 有界格: 格的两个运算 $\wedge, \vee$ 有单位元 $0, 1$ 。
- 补格: 格的两个运算 $\wedge, \vee$ 有逆元。

——布尔代数

- 布尔代数: 有补分配格是布尔代数。
- 布尔代数满足结合律、分配律、吸收律、等幂律、交换律、另一律、同一律、互补律、双补律及德摩根定律。

6. 代数系统结构图



第五章 图 论

术语“图”在数学上的表示有不同的意义,我们在讨论关系和函数时,已经谈到了关系和函数图的表示。这章我们将要扩充图的讨论,在研究图的一般概念、连通性之后,介绍几类很有用的图,即:树、二分图、平面图及有向图等等。

5.1 图的基本概念

一个图 G 定义为 $G=(V,E)$, 其中:

(1) $V=\{v_1, v_2, \dots, v_n\}$ 是有限的非空结点集合, v_i 称为结点, 简称点。

(2) E 是结点的无序偶的集合, 这些无序偶称为 G 的边, 所以 E 是 G 的边集, 其中边具有 (v_i, v_j) 之形式, 也可用 e_k 表示 (v_i, v_j) 。

这里讲的结点对是 unordered 偶, 若用图形表示即为每条边, 是不带方向的, 因而也称 G 是无向图; 若每条边都是有序偶 (从而每条边都带方向), 则称 G 是有向图。我们首先研究无向图, 然后研究有向图。因此在介绍有向图之前, 除非特别声明, 我们所讲的图均指无向图。另外, 图 G 的点集可拓广到无限集, 但本书仅研究有限集。

例 5-1 设有无向图 $G=(V,E)$, 见图 5-1(a), 其中 $V=\{v_1, v_2, \dots, v_5\}$, $E=\{(v_1, v_2), (v_1, v_3), (v_2, v_4), (v_3, v_5), (v_4, v_5), (v_1, v_1), (v_1, v_5), (v_2, v_3)\}$ 。

我们把连接同一条边的两个点称为相邻点, 连接同一个点的边称为相邻边, 或称点关联的边, 连接同一点的一条边称为环, 如图 5-1(a) 所示, 边 $e_1=(v_1, v_2)$ 的相邻点是 v_1, v_2 ; v_2 的相邻边是 e_1, e_6 和 e_2 ; e_8 是环。若一图中两个结点间有一条以上的边, 图论中称它

们为平行边,具有平行边的图称为重图,如图 5-1(b)的 e_3 和 e_4 是平行边,该图是重图。注意,此处的平行边的概念与平面几何的平行边的概念是截然不同的。本书主要研究既不具有平行边也不具有环的无向图称简单图。

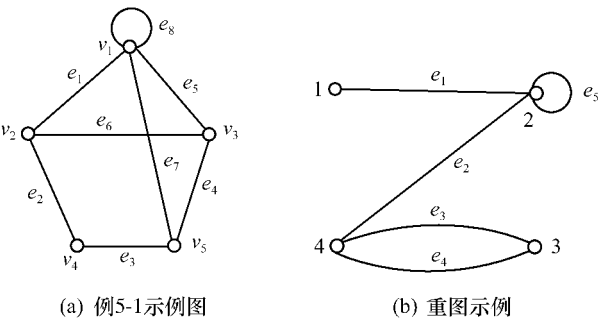


图 5-1 两个图例

也可用图的结点数和边数来命名图,我们把具有 n 个结点、 m 条边的图称为 (n, m) 图,通常把 $(1, 0)$ 图叫作平凡图。

我们把结点 v 的相邻边的数目称为 v 的次数,用 $\deg(v)$ 表示,由于计算图的各个结点次数时,每条边计算 2 次,因此有下面一条简单的然而重要的定理。

定理 5-1 设 G 是一个 (n, m) 图,具有结点集合 $V = \{v_1, v_2, \dots, v_n\}$, 则:

$$\sum_{i=1}^n \deg(v_i) = 2m$$

在图 5-1(b)中, $\deg(1)=1, \deg(2)=4, \deg(3)=2, \deg(4)=3$ 。

$$\sum_{i=1}^4 \deg(v_i) = 10 = 2 \times 5$$

图中结点次数为零的结点称为孤立点。

一个 (n, m) 图, $n \geq 2$, 它的每个结点与其余的 $n-1$ 个结点有边相连, 那么这个 (n, m) 图称为完全图, 因此一个完全图具有的边

数是：

$$m = C_n^2 = n(n-1)/2$$

如图 5-2(a)是有 5 个结点的完全图。

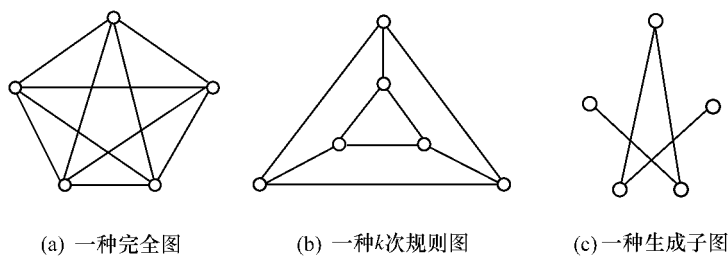


图 5-2 三个图例

如果一个图的每个结点的次数都是 k , 则该图称为 k 次规则图, 如图 5-2(b)是 3 次规则图。

设 $G=(V, E), \tilde{G}=(\tilde{V}, \tilde{E})$, 若 $\tilde{V} \subseteq V, \tilde{E} \subseteq E$, 则称 $\tilde{G}$ 是 G 的子图, 若 $\tilde{E} \subset E, \tilde{V} \subseteq V$, 则称 $\tilde{G}$ 是 G 的真子图。若 $\tilde{V}=V, \tilde{E} \subset E$, 则称 $\tilde{G}$ 是 G 的生成子图。图 5-2(c)是 5-2(a)的生成子图。

我们已经讲了一个结点的次数是该结点关联的边数, 若结点次数是奇数, 称它为奇次结点, 简称奇结点, 反之称它为偶次结点, 简称偶结点, 它们之间有下列关系。

定理 5-2 任何一个图 G , 奇结点的数目一定是偶数。

证明： 设 V_1 和 V_2 分别是 G 的奇次结点集合和偶次结点集合。所以有：

$$\sum_{x \in v_1} \deg(x) + \sum_{x \in v_2} \deg(x) = \sum_{x \in v} \deg(x) = 2m \quad (m \text{ 是边数})$$

因为 $\sum_{x \in v_2} \deg(x)$ 是偶数, 所以 $\sum_{x \in v_1} \deg(x)$ 也是偶数, 所以 v_1 中结点数一定是偶数。

令 $G=(V, E)$ 和 $\overline{G}=(\overline{V}, \overline{E})$ 是两个简单图, 如果存在一一对应的映射 $h: V \rightarrow \overline{V}$, 使得 $(v_i, v_j) \in E$ 当且仅当 $(h(v_i), h(v_j)) \in \overline{E}$, 则称

G 和 $\overline{G}$ 是同构的图。

例 5-2 下面两个图(如图 5-3 所示) $G=(V,E)$ 和 $G'=(V',E')$ 是同构的。

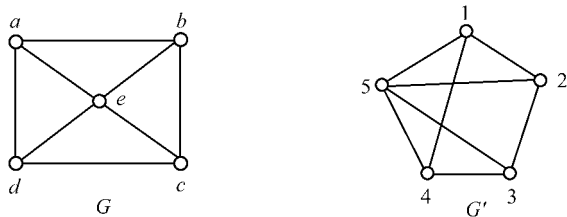


图 5-3 两个同构图

解：可以建立其一一对应的映射如下：

$$h(a)=1, h(b)=2, h(c)=3$$

$$h(d)=4, h(e)=5$$

且有： $(a,b) \in E$ 当且仅当 $(1,2) \in E'$

$(b,c) \in E$ 当且仅当 $(2,3) \in E'$

$(c,d) \in E$ 当且仅当 $(3,4) \in E'$

$(a,d) \in E$ 当且仅当 $(1,4) \in E'$

$(a,e) \in E$ 当且仅当 $(1,5) \in E'$

$(b,e) \in E$ 当且仅当 $(2,5) \in E'$

$(c,e) \in E$ 当且仅当 $(3,5) \in E'$

$(d,e) \in E$ 当且仅当 $(4,5) \in E'$

所以 G 和 G' 是同构的。

5.2 连通性

在图 G 中,任意一条边的序列 $(v_{i_0}, v_{i_1}), (v_{i_1}, v_{i_2}), \dots, (v_{i_{l-1}}, v_{i_l})$, 称为 v_{i_0} 和 v_{i_l} 间的长度是 l 的通路。为简便起见,可写作 $P = (e_{i_1}, e_{i_2}, \dots, e_{i_l})$, 其中, $e_{i_k} = (v_{i_{k-1}}, v_{i_k}), 1 \leq k \leq l$; 也可写作 $P: (v_{i_0},$

$v_{i_1}, \dots, v_{i_l}$)。在图论中,一条通路的长度是指该通路的边数,与通常意义下的长度是截然不同的概念。我们以例来说明这点。在体育比赛中,男子 $4 \times 400\text{m}$ 接力赛中,若把 400m 作一条边,则其全程长度是 4,因为它有 4 条边,女子 $4 \times 100\text{m}$ 接力赛,若把 100m 作一条边,则其全程长度也是 4。

通路中的 v_{i_0} 和 v_{i_l} 可以有两种情况,一是 $v_{i_0} = v_{i_l}$,称这样的通路为闭通路,我们约定把闭通路叫做回路;二是 $v_{i_0} \neq v_{i_l}$,称这样的通路是开通路,我们约定今后开通路简称为通路。

在一条通路中,若每条边只经过一次,则称该通路是简单通路。同理,在一条回路中,若每条边只出现一次,则称该回路是简单回路。

在一条通路中,若每个结点只经过一次,则称该通路是基本通路。同理,在一条回路中,除首尾两结点外,每个结点只出现一次,则该回路是基本回路。

显然,基本回路必是简单回路,基本通路必是简单通路,但反之却未必成立。

例 5-3 设 $G=(V,E)$ 如图 5-4 所示,则 $P_1=(4,1,2,5,1,2,3,6)$ 是从 4 到 6 长度为 7 的一条通路,但不是简单通路,因为边 $(1,2)$ 在序列中出现两次。

$P_2=(4,1,5,2,3,5,6)$ 是从 4 到 6 长度为 6 的一条通路,而且是简单通路,但不是基本通路,因为结点 5 在序列中出现两次。

$P_3=(4,1,5,3,6)$ 是从 4 到 6 长度为 4 的简单通路和基本通路。

$C_1=(1,4,5,6,3,5,1)$ 是一条简单回路,但不是基本回路。

$C_2=(1,2,3,6,5,1)$ 是一条简单回路,也是基本回路。

$C_3=(1,5,3,6,5,1)$ 是一条回路,它既不是简单的,也不是基本的。

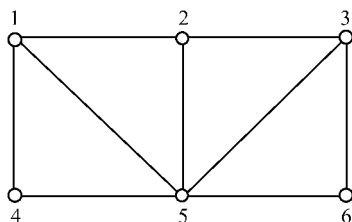


图 5-4 图的通路示例

对一条通路, 消去一些不必要的边, 总可以找到一条基本通路。
 我们把这个结论归结为如下一条定理。

定理 5-3 图 G 中结点 u 到结点 v 存在一条通路当且仅当从 u 到 v 存在一条基本通路。

通路、回路、简单通路(回路)、基本通路(回路)是十分重要的概念。

定义 5-1 图 G 中两个结点 v_i 和 v_j , 如果 v_i 和 v_j 间存在一条通路, 则称两个结点 v_i 和 v_j 是连通的, 若图 G 中任意两个结点均连通, 则称 G 是连通图, 否则是 非连通图。

例 5-4 设有两个图如图 5-5 所示。

其中图 5-5(a)是非连通图, 5-5(b)是连通图。

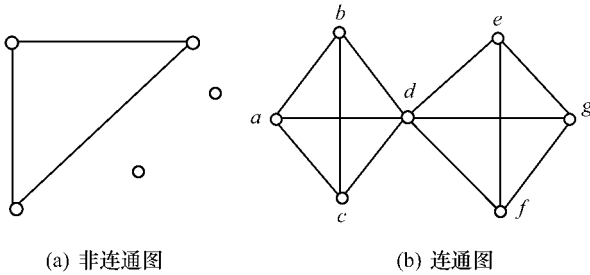


图 5-5 图连通性示例

当一个图 G 有 n 个子图, 每个子图均是连通的, 于是图 G 就有 n 个连通子图, 若 G 中任意一个连通子图不与别的连通子图连通, 那么这种连通子图是图 G 的一个独立子图, 如图 5-6 是具有 10 个结点的图, 它有 4 个独立子图, 即 G_1 、 G_2 、 G_3 和 G_4 。

例 5-5 设在一次国际会议上有 7 个人, 各懂的语言如下:

- a. 会讲英语;
- b. 会讲英语和西班牙语;
- c. 会讲英语、汉语和俄语;
- d. 会讲日语和西班牙语;

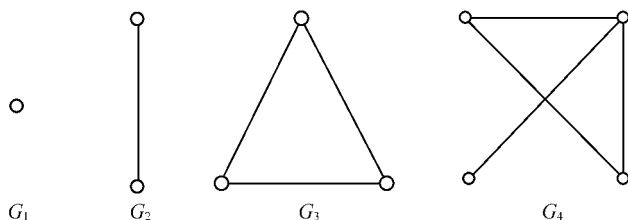


图 5-6 独立子图

- e. 会讲德语和汉语；
- f. 会讲法语、日语和俄语；
- g. 会讲法语和德语。

问：他们中间是否任何两个人可对话（必要时通过别人作翻译）？

解：利用图 5-7，我们把 7 个人及 7 种语种都用结点表示，人和所懂语言的关系用边表示，问题变成任何两人之间是否存在一条通路。我们可以看出，这是一个连通图，所以每两个人均可对话。

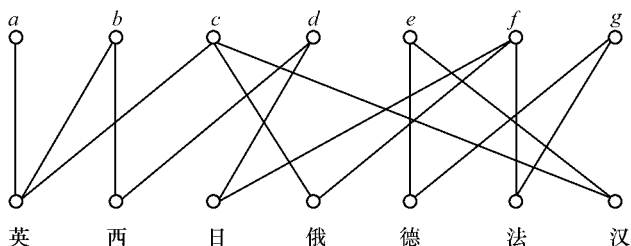


图 5-7 例 5-5 示例图

我们来进一步讨论最短通路的问题。设结点 v_i 和 v_j 间是连通的，它们之间存在一条或两条以上的通路，我们把其中长度最短的通路称为 v_i 和 v_j 的短程线，短程线的长度称为 v_i 和 v_j 的距离，用 $d(v_i, v_j)$ 表示。如图 5-5(b) 中， $d(a, f) = 2$ ， $d(a, g) = 2$ ， $d(a, d) = 1$ ，等等。

对于图 G 的简单通路和短程线及其长度有一个简单的关系，用下述定理刻画它。

定理 5-4 设图 $G=(V, E)$, $V=\{v_1, v_2, \dots, v_n\}$, 于是对任意的连通结点 $v_i, v_j \in V (v_i \neq v_j)$, 其短程线是长度最多为 $n-1$ 的一条简单通路。

证明：考察任意一条通路：

$$P_1 = (v_{i_0}, v_{i_1}, \dots, v_{i_{l-1}}, v_{i_l})$$

其中 $v_{i_0} \neq v_{i_l}$, 若 P_1 有任意重复的结点, 譬如说, $v_{i_j} = v_{i_k}$, 那么删除 v_{i_j} 与 v_{i_k} 间部分通路 $(v_{i_{j+1}}, \dots, v_{i_{k-1}})$ 得到一条长度较小的通路：

$$P_2 = (v_{i_0}, v_{i_1}, \dots, v_{i_j}, v_{i_k}, \dots, v_{i_l})$$

如果 P_2 有任意重复的结点, 可以再删除有关的一部分通路, 又得到一条长度较小的通路 P_3 , 依此进行, 直到求到一条简单通路为止, 它连接 v_{i_0} 及 v_{i_l} , 但比 v_{i_0} 与 v_{i_l} 间任意一条非简单通路的长度小。现在, 在任意一条长度为 l 的简单通路 $(v_{i_0}, v_{i_1}, \dots, v_{i_l})$ 中, 各结点一定是不同的, 这蕴含 $l+1 \leq n$, 因此 $l \leq n-1$ 。

在图论应用方面的一个很普遍的问题是：设有一个连通图 G , 是否可以找到一个回路, 这个回路包括 G 的每条边一次而且仅仅一次。这个问题最早来源于历史上著名的哥尼斯堡(königsberg)桥问题。18 世纪, 哥尼斯堡城位于普雷格尔(Pregel)河畔, 河中有两个小岛, 岛与岛之间, 岛与河岸之间共架有 7 座桥, 如图 5-8(a) 所示。

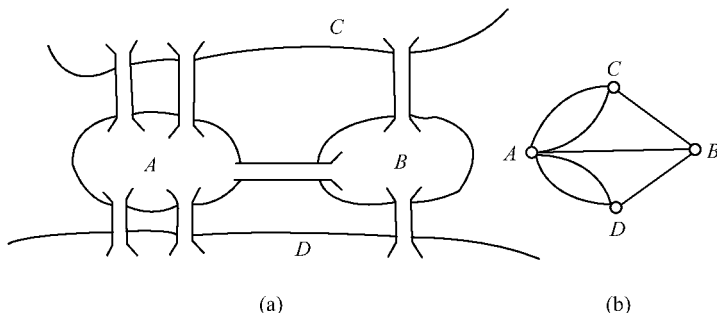


图 5-8 欧拉图原型

那里的人们提出：是否能从 A, B, C, D 任意一处出发, 经过每座

桥一次而且仅仅一次再返回到原处？(用图论的说法就是那条简单回路是否存在。)

问题看起来似乎很简单,但是那儿的人们谁都无法解决这个问题,于是哥尼斯堡的人们写信给当时著名的瑞士数学家欧拉(L·Euler),欧拉把这个具体问题抽象为图 5-8(b),其中 A、B、C、D 分别代表两个岛和河的两岸,边代表桥,1736 年,他证明并宣布人们提出的问题是无解的,从而解决了这个难题。下面我们介绍他的论点。为此我们先引进欧拉回路和欧拉图的概念。

定义 5-2 经连通图 G 的每条边一次而且仅仅一次的回路称为 G 的欧拉回路;具有欧拉回路的图称为欧拉图。

欧拉回路简称 E 回路,欧拉图简称 E 图。

定理 5-5 一个连通图 G 是欧拉图当且仅当 G 的每个结点次数是偶数。

证明: 假设 G 是欧拉图,令 a 是 G 的欧拉回路,对 G 中每个结点 v ,回路 a 每次经过一个结点 v 时,该结点的次数加 2(进入 v 和离开 v 各一次),由于在 a 中每条边仅出现一次,所以每个结点的次数一定是 2 的倍数。

反之,假定 G 的每个结点是偶次。若 G 是平凡图,则定理平凡真。否则,由于 G 的每个结点是偶次,所以 G 一定至少存在一条基本回路,譬如说 σ_1 ,从 G 中去掉 σ_1 的边后,得到 G 的生成子图 G_1 , G_1 的每个结点仍然是偶次,如果 G_1 至少还有一条边,则 G_1 一定至少存在一条基本回路,譬如说 σ_2 ,再从 G_1 中除去 σ_2 的边,得到生成子图 G_2 , G_2 的每个结点仍然是偶次,这过程经有限步重复之后, G 的所有边均已除去了。

现在将除去的边集划分成有限条基本回路,它构成基本回路集 S 。显然, S 中至少有一个基本回路。

(1) 设 $\sigma_i \in S$,如果 σ_i 是这个划分中惟一的基本回路,显然 σ_i 就是欧拉回路。

(2) 否则,一定还有另外的基本回路,譬如说 $\sigma_i \in S$,由 G 的连通

性, σ_i 和 σ_j 必有一个公共结点 v , 如果 σ_i 和 σ_j 是这个划分中仅有的两条基本回路, 那么欧拉回路是开始于结点 v , 绕 σ_i , 再绕 σ_j , 最后结束于 v 。

(3) 否则, 一定还有第三条基本回路, 譬如说 $\sigma_k \in S$, 由 G 的连通性, σ_k 和 σ_i 或和 σ_j 必有一个公共结点 v' , 不妨说与 σ_j 有 v' 。如果 σ_i 、 σ_j 和 σ_k 是这个划分中仅有的三条基本回路, 那么欧拉回路可这样选定: 开始于 v , 绕 σ_i 的回路, 沿 σ_j 到 v' , 再绕 σ_k , 经 σ_i 返回到 v 。

这个过程可以一直进行下去, 由于 S 中的基本回路是有限的, 故经过有限步总可找到欧拉回路。

因此 G 是欧拉图。

这个定理提供了判别欧拉图的十分简单的方法。因此哥尼斯堡桥不具有欧拉回路, 因为它的结点是奇次结点。

例如, 图 5-9 是欧拉图, 因为它的每个结点均是偶结点, 它的十条边可以划分成为三条回路:

$$\sigma_1 = (v_1, v_2, v_3, v_1)$$

$$\sigma_2 = (v_3, v_4, v_5, v_3)$$

$$\sigma_3 = (v_5, v_6, v_7, v_8, v_5)$$

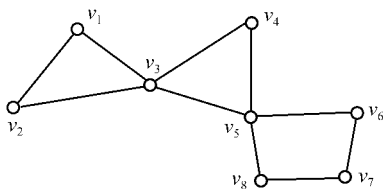


图 5-9 欧拉图示例

因此 v_3 是 σ_1 和 σ_2 的公共结点, v_5 是 σ_2 和 σ_5 的公共结点, 这个图的一条欧拉回路是:

$$E = (v_2, v_1, v_3, v_4, v_5, v_6, v_7, v_8, v_5, v_3, v_2)$$

定义 5-3 经过连通图 G 的每条边一次而且仅仅一次的通路称为欧拉通路。

同样我们可以找到图 G 是否存在欧拉通路的简单判别方法。

定理 5-6 一个连通图 $G = (V, E)$, v_i 和 v_j 之间存在欧拉通路当且仅当 G 中只有 v_i 和 v_j 是奇结点。

证明: 我们在 G 中人为地加上一条边 (v_i, v_j) 得到图 G' , 这时 G 有欧拉通路当且仅当 G' 有欧拉回路, 而 G' 有欧拉回路当且仅当 G' 的所有结点均是偶结点。所以 G' 中的 v_i 和 v_j 是偶结点, 最后去掉

加上的边 (v_i, v_j) , 则 G' 还原成 G , 可见 G 中的 v_i 和 v_j 是奇结点。

根据上述概念, 我们分析下面两个图的情况:

图 5-10(a) 是一个欧拉图, 它的一条可能的欧拉回路是:

$$(e_1, e_2, e_4, e_{10}, e_{11}, e_{14}, e_{15}, e_{16}, e_{19}, e_{17}, e_{18}, \\ e_{20}, e_{13}, e_9, e_{12}, e_5, e_6, e_8, e_7, e_3)$$

图 5-10(b) 存在欧拉通路, 它的一条可能的欧拉通路是:

$$(1, 2, 3, 4, 6, 3, 5, 6, 7, 2, 8, 7, 1, 8)$$

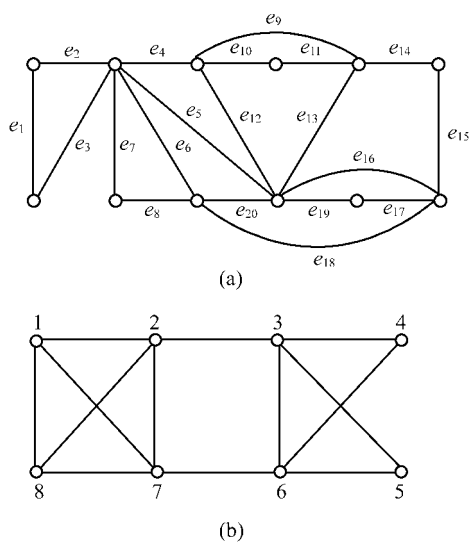


图 5-10 两种欧拉图

图论中另外一个广泛应用的问题是: 已知一个图, 是否存在一条回路, 它经过 G 中每个结点一次而且仅仅一次。为此, 我们引进哈密顿 (Hamilton) 回路和哈密顿图的概念。

定义 5-4 经过图 G 的每个结点一次而且仅仅一次的回路称为哈密顿回路; 具有哈密顿回路的图称为哈密顿图。

哈密顿回路简称 **H 回路**, 哈密顿图简称 **H 图**。

我们已经学过, 对一个图 G 是否是 **E 图** 有一种简单的判别法,

遗憾的是,至今还没有找到判别图 G 是否是 H 图的充分必要条件,不少数学家正在兴致勃勃地研究这个问题,因为解决这个问题对理论方面和应用方面都具有重大意义。

哈密顿图和欧拉图有明显区别,但也有联系。为了弄清其区别,可看图 5-11 的四个图,显然其中(a)是欧拉图也是哈密顿图,(b)是欧拉图但不是哈密顿图,(c)是哈密顿图但不是欧拉图,(d)既不是欧拉图也不是哈密顿图。

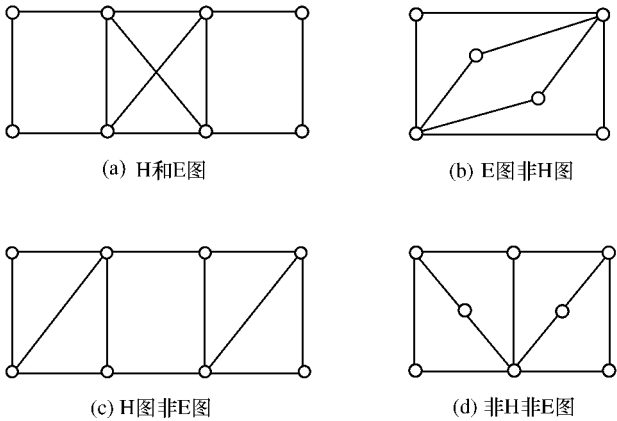


图 5-11 四种不同图

5.3 图的矩阵表示

图形表示是图的一种表示方法,它的优点是形象直观,但有时为便于计算,图常用矩阵表示。对于简单图,习惯上有两类矩阵。

定义 5-5 设图 $G=(V,E)$, 令 $M=[m_{ij}]$ 是 $m \times n$ 阶矩阵, m_{ij} 定义如下:

$$m_{ij} = \begin{cases} 1, & \text{如果结点 } v_i \text{ 与边 } e_j \text{ 关联} \\ 0, & \text{其他情况} \end{cases}$$

则称 $M=[m_{ij}]$ 是 G 的关联矩阵。

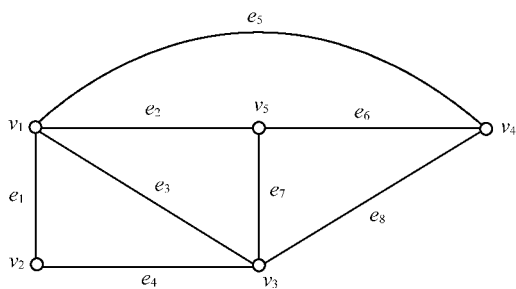


图 5-12 例 5-6 所示的图

例 5-6 图 5-12 及相应的关联矩阵如下：

$$\begin{matrix}
 & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 \\
 \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{matrix} & \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}
 \end{matrix}$$

定义 5-6 设图 $G=(V,E)$, 令 $A=[a_{ij}]$ 是 $m\times m$ 阶矩阵, 其中 a_{ij} 定义如下：

$$a_{ij} = \begin{cases} 1, & \text{当 } (v_i, v_j) \in E \\ 0, & \text{当 } (v_i, v_j) \notin E \end{cases}$$

则称 $A=[a_{ij}]$ 是 G 的相邻矩阵, 也可称邻接矩阵。

例如, 图 5-12 的相邻矩阵是：

$$\begin{matrix}
 & v_1 & v_2 & v_3 & v_4 & v_5 \\
 \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{matrix} & \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}
 \end{matrix}$$

相邻矩阵在判定 G 的连通性方面有很大用处。通过矩阵乘法运算之后得到 A^l 。 A^l 中每个元素有什么图论意义呢？下面的定理说明矩阵 A^l 中各元素的意义。

定理 5-7 设 G 是具有结点集 $V = \{v_1, v_2, \dots, v_n\}$ 的图, 其相邻矩阵是 A , 则 $A^l (l=1, 2, \dots, n)$ 的第 (i, j) 个元素是由 v_i 到 v_j 的长度等于 l 的通路数目。

证明: 对 l 归纳

(1) 奠基: 当 $l=1$ 时, $A^l = A$, 由 A 的定义, 断言是成立的。

(2) 归纳: 设 $l=k$ 时, A^k 的第 (i, j) 个元素是 $a_{ij}^{(k)}$, 假定断言成立, 下面证明 $l=k+1$ 时, 断言亦成立。

因为 $A^{k+1} = A^k \cdot A$, 所以 $a_{ij}^{(k+1)} = \sum_{h=1}^n a_{ih}^{(k)} \cdot a_{hj}$, 但是 $a_{ih}^{(k)} \cdot a_{hj}$ 是由 v_i 到 v_j 长度为 $k+1$ 的一条通路, 因此 $a_{ij}^{(k+1)}$ 是由 v_i 到 v_j 长度为 $k+1$ 的通路的总数, 而 $a_{ij}^{(k+1)}$ 是矩阵 A^{k+1} 的第 (i, j) 个元素, 故定理成立。

由这条定理还可以得出几个结论:

(1) $d(v_i, v_j)$ 是使得 A^l 的第 (i, j) 个元素为非零的最小整数 l (其中 $v_i \neq v_j$)。

(2) $a_{ii}^{(l)}$ 表示开始并结束于 v_i 长度为 l 的回路数目。

(3) $a_{ij}^{(l)} = 0 (i \neq j)$ 表示由 v_i 到 v_j 无长度为 l 的通路存在。

对具有 m 个结点的图 G , 由 v_i 到 v_j 的任意一条基本通路的长度小于或等于 $m-1$, 因此矩阵:

$$A + A^2 + \dots + A^{m-1} = \tilde{A}$$

如果没有从 v_i 到 v_j 的基本通路, 则 $\tilde{A}$ 的第 (i, j) 个元素是零。此时, v_i 和 v_j 属于不同的独立子图, 所以是连通图当且仅当 $\tilde{A}$ 除对角线外全是非零元素。

例 5-7 图 $G=(V, E)$ 的图形表示如图 5-13 所示, 它的相邻矩阵如下:

$$\mathbf{A} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

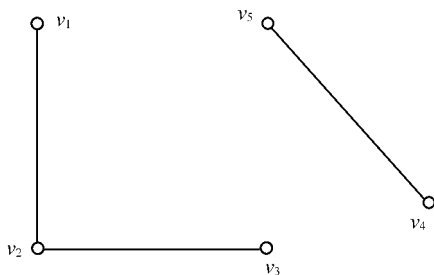


图 5-13 例 5-7 示例图

于是：

$$\mathbf{A}^2 = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\mathbf{A}^3 = \begin{bmatrix} 0 & 2 & 0 & 0 & 0 \\ 2 & 0 & 2 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \quad \mathbf{A}^4 = \begin{bmatrix} 2 & 0 & 2 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 \\ 2 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

结合图形,我们分析矩阵元素的图论意义。由矩阵可以得出：

(1) v_1 和 v_2 是连通的,长度为 1 的通路是 (v_1, v_2) 。长度为 3

的通路有 2 条: $((v_1, v_2), (v_2, v_1), (v_1, v_2))$ 及 $((v_1, v_2), (v_2, v_3), (v_3, v_2))$ 。

(2) 无长度为 3 的回路, 长度为 2 的回路各结点都有, 如 v_1 的回路是 (v_1, v_2, v_1) , v_2 的回路是 (v_2, v_1, v_2) 及 (v_2, v_3, v_2) , 等等。对于长度是 4 的各结点的回路同样可以找到。

(3) 结点 v_1 和 v_3 之间长度为 4 的通路有 2 条, 即 $(v_1, v_2, v_1, v_2, v_3)$ 及 $(v_1, v_2, v_3, v_2, v_3)$ 。

(4) 结点 v_3 和 v_4 之间无通路存在, 所以 v_3 和 v_4 属于不同的独立子图。

(5) v_1 和 v_3 间的距离是 2, 即 $d(v_1, v_3) = 2$, 因为 A^2 使得第 (1, 3) 个元素成为不等于零的最小数是 1, 而 A^4 虽然也能使第 (1, 3) 个元素不等于零, 但它的值是 2。

对于矩阵上其余各元素值的图论意义, 均可按照定理作类似的解释。所以用矩阵方法表示图, 可帮助我们z从理论上深入研究图论。

5.4 权图、最小权通路和最小权回路

在具体应用中, 权图是一种极其重要的图, 本节介绍权图的基本知识。

定义 5-7 设图 $G = (V, E)$, 对 G 中的每条边 e_i , 相应地赋予一个非负数据 $w(e_i)$, 称 $w(e_i)$ 为边 e_i 的权, 每条边带有权的图称为带权图, 简称权图。

我们还要规定什么是一条通路 P 的权, 什么是一条回路 C 的权。

通路 P 的权是指该通路中各条边的权之和, 设 $P = (e_1, e_2, \dots, e_n)$, e_i 之权是 $w(e_i)$, 则通路 P 的权是:

$$w(P) = \sum_{e_i \in P} w(e_i)$$

G 中一条回路 C 的权是该回路中各条边的权之和, 故:

$$w(C) = \sum_{e_i \in C} w(e_i)$$

一般说来,从 v_i 到 v_j 的通路有若干条,构成了一个从 v_i 到 v_j 的通路集合,我们感兴趣的是其中权最小的那条通路,称为最小权通路,同理, v_i 的回路一般也有若干条,我们所关心的是其中权最小的那条回路,称为最小权回路。

需要特别指出的是,这里所说的“权”具有十分广泛的意义,以图 5-14 来说明,设它是一个传输网络,若“权”代表通常意义下的距离,则 v_i 到 v_j 通路之“权”代表该通路的距离,最小权通路是使运输距离最小的那条通路;若“权”代表传输时间,则最小权通路代表传输时间最短的通路;若“权”代表费用,则最小权通路就是运输费用最省的通路。对于最小权回路,也有类似的解释。

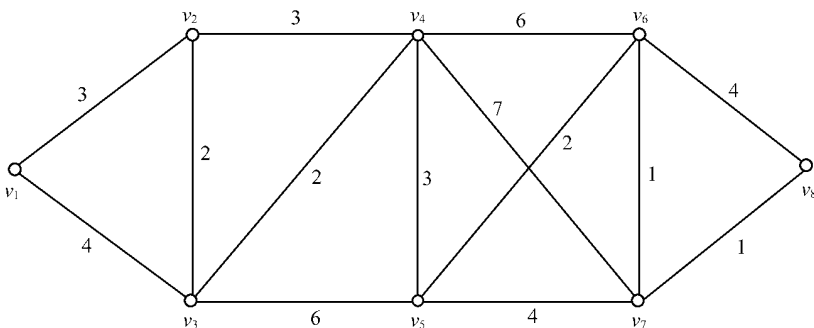


图 5-14 权图

进一步要问,如何求一个权图的最小权通路 P 的问题,我们介绍一种算法,这算法用以求权图的任意两结点间的最小权通路。在介绍这算法之前,先定义带权图的矩阵表示方法。

设权图 $G=(V, E)$, G 的矩阵 $D=[d_{ij}]$, 其中

$$d_{ij} = \begin{cases} w(v_i, v_j) & \text{当 } (v_i, v_j) \in E \\ \infty & \text{当 } (v_i, v_j) \notin E \\ 0 & \text{当 } v_i = v_j \end{cases}$$

图 5-14 的矩阵是：

$$D = \begin{matrix} & \begin{matrix} v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 & v_8 \end{matrix} \\ \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6 \\ v_7 \\ v_8 \end{matrix} & \begin{bmatrix} 0 & 3 & 4 & \infty & \infty & \infty & \infty & \infty \\ 3 & 0 & 2 & 3 & \infty & \infty & \infty & \infty \\ 4 & 2 & 0 & 2 & 6 & \infty & \infty & \infty \\ \infty & 3 & 2 & 0 & 3 & 6 & 7 & \infty \\ \infty & \infty & 6 & 3 & 0 & 2 & 4 & \infty \\ \infty & \infty & \infty & 6 & 2 & 0 & 1 & 4 \\ \infty & \infty & \infty & 7 & 4 & 1 & 0 & 2 \\ \infty & \infty & \infty & \infty & \infty & 4 & 2 & 0 \end{bmatrix} \end{matrix}$$

下面介绍求图中任意两个结点间最小权通路的算法：

设 $G=(V,E)$, V 具有 n 个结点：

(1) 决定权图矩阵 $D^{(0)}=[d_{ij}]=[d_{ij}^{(0)}]$, 因此 $D^{(0)}=D$ 。

(2) 从 $D^{(0)}$ 出发构造矩阵 $D^{(1)}, D^{(2)}, \dots, D^{(n)}$ 。

已知 $D^{(k-1)}=[d_{ij}^{(k-1)}]$, 则第 k 个矩阵 $D^{(k)}=[d_{ij}^{(k)}]$ 的定义如下：

$$d_{ij}^{(k)} = \min\{d_{ij}^{(k-1)}, d_{ik}^{(k-1)} + d_{kj}^{(k-1)}\} \quad (k \neq i, j)$$

它表示从 v_i 到 v_j 而中间结点仅属于 v_i 到 v_k 的 k 个结点的所有通路中的最小权通路之权。

计算时从 $k=1$ 开始, 让 i 和 j 分别取遍从 1 到 n 的值, 然后 k 增加 1, 反复进行, 直到 $k=n$ 为止。

(3) 最后求得的 $D^{(n)}=[d_{ij}^{(n)}]$ 中的元素 $d_{ij}^{(n)}$ 就是从 v_i 到 v_j 的通路的最小权。

上述算法可用图 5-15 的程序流程图来描述。

若一个图的结点和边较多, 根据上述算法用手工方法来构造 $D^{(1)}, D^{(2)}, \dots, D^{(n)}$ 是相当麻烦的, 我们可借助计算机来完成。以图 5-14 为例, 由计算机求得任意两点间的最小权通路如下: ($D^{(0)}$ 矩阵如前一个矩阵所示)

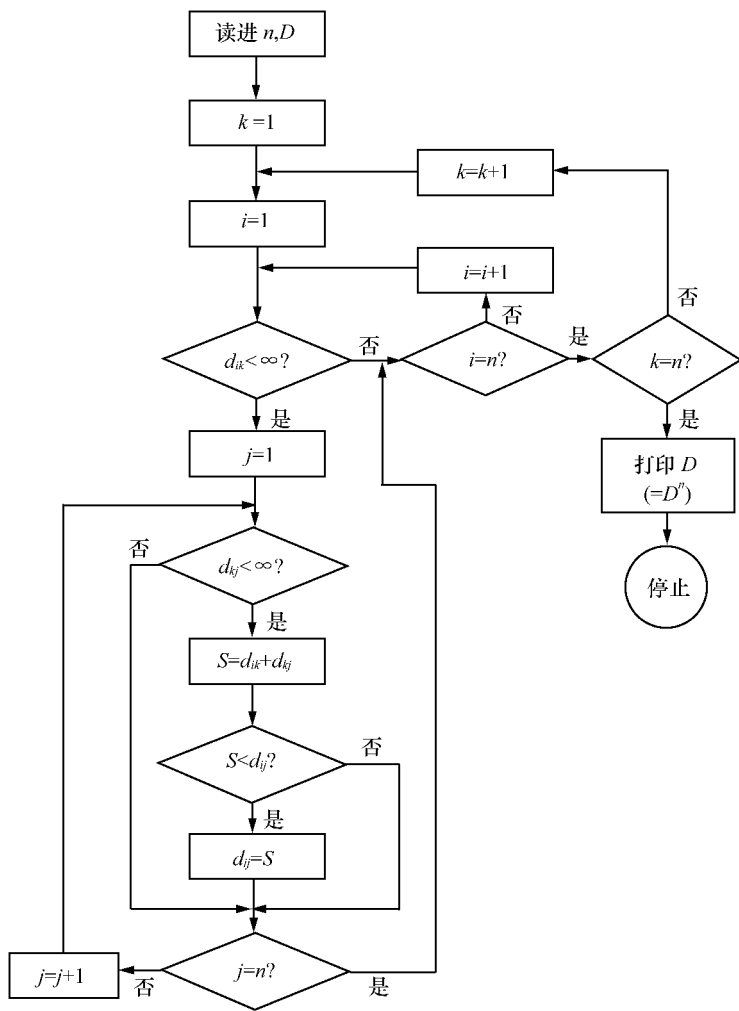


图 5-15 最小权通路算法流程图

$$\mathbf{D}^1 = \begin{bmatrix} 0 & 3 & 4 & \infty & \infty & \infty & \infty & \infty \\ 3 & 0 & 2 & 3 & \infty & \infty & \infty & \infty \\ 4 & 2 & 0 & 2 & 6 & \infty & \infty & \infty \\ \infty & 3 & 2 & 0 & 3 & 6 & 7 & \infty \\ \infty & \infty & 6 & 3 & 0 & 2 & 4 & \infty \\ \infty & \infty & \infty & 6 & 2 & 0 & 1 & 4 \\ \infty & \infty & \infty & 7 & 4 & 1 & 0 & 2 \\ \infty & \infty & \infty & \infty & \infty & 4 & 2 & 0 \end{bmatrix}$$

$$\mathbf{D}^2 = \begin{bmatrix} 0 & 3 & 4 & 6 & \infty & \infty & \infty & \infty \\ 3 & 0 & 2 & 3 & \infty & \infty & \infty & \infty \\ 4 & 2 & 0 & 2 & 6 & \infty & \infty & \infty \\ 6 & 3 & 2 & 0 & 3 & 6 & 7 & \infty \\ \infty & \infty & 6 & 3 & 0 & 2 & 4 & \infty \\ \infty & \infty & \infty & 6 & 2 & 0 & 1 & 4 \\ \infty & \infty & \infty & 7 & 4 & 1 & 0 & 2 \\ \infty & \infty & \infty & \infty & \infty & 4 & 2 & 0 \end{bmatrix}$$

$$\mathbf{D}^3 = \begin{bmatrix} 0 & 3 & 4 & 6 & 10 & \infty & \infty & \infty \\ 3 & 0 & 2 & 3 & 8 & \infty & \infty & \infty \\ 4 & 2 & 0 & 2 & 6 & \infty & \infty & \infty \\ 6 & 3 & 2 & 0 & 3 & 6 & 7 & \infty \\ 10 & 8 & 6 & 3 & 0 & 2 & 4 & \infty \\ \infty & \infty & \infty & 6 & 2 & 0 & 1 & 4 \\ \infty & \infty & \infty & 7 & 4 & 1 & 0 & 2 \\ \infty & \infty & \infty & \infty & \infty & 4 & 2 & 0 \end{bmatrix}$$

$$\mathbf{D}^4 = \begin{bmatrix} 0 & 3 & 4 & 6 & 9 & 12 & 13 & \infty \\ 3 & 2 & 0 & 3 & 6 & 9 & 10 & \infty \\ 4 & 2 & 0 & 2 & 5 & 8 & 9 & \infty \\ 6 & 3 & 2 & 0 & 3 & 6 & 7 & \infty \\ 9 & 6 & 5 & 3 & 0 & 2 & 4 & \infty \\ 12 & 9 & 8 & 6 & 2 & 0 & 1 & 4 \\ 13 & 10 & 9 & 7 & 4 & 1 & 0 & 2 \\ \infty & \infty & \infty & \infty & \infty & 4 & 2 & 0 \end{bmatrix}$$

$$\mathbf{D}^5 = \begin{bmatrix} 0 & 3 & 4 & 6 & 9 & 11 & 13 & \infty \\ 3 & 0 & 2 & 3 & 6 & 8 & 10 & \infty \\ 4 & 2 & 0 & 2 & 5 & 7 & 9 & \infty \\ 6 & 3 & 2 & 0 & 3 & 5 & 7 & \infty \\ 9 & 6 & 5 & 3 & 0 & 2 & 4 & \infty \\ 11 & 8 & 7 & 5 & 2 & 0 & 1 & 4 \\ 13 & 10 & 9 & 7 & 4 & 1 & 0 & 2 \\ \infty & \infty & \infty & \infty & \infty & 4 & 2 & 0 \end{bmatrix}$$

$$\mathbf{D}^6 = \begin{bmatrix} 0 & 3 & 4 & 6 & 9 & 11 & 12 & 15 \\ 3 & 0 & 2 & 3 & 6 & 8 & 9 & 12 \\ 4 & 2 & 0 & 2 & 5 & 7 & 8 & 11 \\ 6 & 3 & 2 & 0 & 3 & 5 & 6 & 9 \\ 9 & 6 & 5 & 3 & 0 & 2 & 3 & 6 \\ 11 & 8 & 7 & 5 & 2 & 0 & 1 & 4 \\ 12 & 9 & 8 & 6 & 3 & 1 & 0 & 2 \\ 15 & 12 & 11 & 9 & 6 & 4 & 2 & 0 \end{bmatrix}$$

$$\mathbf{D}^7 = \begin{bmatrix} 0 & 3 & 4 & 6 & 9 & 11 & 12 & 14 \\ 3 & 0 & 2 & 3 & 6 & 8 & 9 & 11 \\ 4 & 2 & 0 & 2 & 5 & 7 & 8 & 10 \\ 6 & 3 & 2 & 0 & 3 & 5 & 6 & 8 \\ 9 & 6 & 5 & 3 & 0 & 2 & 3 & 5 \\ 11 & 8 & 7 & 5 & 2 & 0 & 1 & 3 \\ 12 & 9 & 8 & 6 & 3 & 1 & 0 & 2 \\ 14 & 11 & 10 & 8 & 5 & 3 & 2 & 0 \end{bmatrix}$$

$$\mathbf{D}^8 = \begin{bmatrix} 0 & 3 & 4 & 6 & 9 & 11 & 12 & 14 \\ 3 & 0 & 2 & 3 & 6 & 8 & 9 & 11 \\ 4 & 2 & 0 & 2 & 5 & 7 & 8 & 10 \\ 6 & 3 & 2 & 0 & 3 & 5 & 6 & 8 \\ 9 & 6 & 5 & 3 & 0 & 2 & 3 & 5 \\ 11 & 8 & 7 & 5 & 2 & 0 & 1 & 3 \\ 12 & 9 & 8 & 6 & 3 & 1 & 0 & 2 \\ 14 & 11 & 10 & 8 & 5 & 3 & 2 & 0 \end{bmatrix}$$

上述矩阵 $\mathbf{D}^1$ 到 $\mathbf{D}^8$ 是在计算机上用 FORTRAN 程序设计语言求得的, 其中 $\mathbf{D}^1$ 到 $\mathbf{D}^7$ 是中间结果, $\mathbf{D}^8$ 是要求的最终结果, 对照图 5-14 所示的例子, 完全符合事实, 相应的程序如下:

```
MASTER PROGRAM
INTEGER D
DIMENSION(8,8)
READ(1,5)D
WRITE(3,10)D
5  FORMAT(8I3)
10 FORMAT(/5X,8I5)
```

```

DO 18 K=1,8
CALL SUB(D,8,K,500)
WRITE(3,15)D
15  FORMAT(1H0,5X,8I10)
18  CONTINUE
STOP
END
SUBROUTINE SUB(D,N,K,M)
INTEGER D(N,N),S
DO 12 I=1,N
IF(D(I,K) • EQ • M)GO TO 12
DO 12 J=1,N
IF(D(K,J) • EQ • M)GO TO 12
S=D(I,K)+D(K,J)
IF(S • LT • D(I,J))D(I,J)=S
12  CONTINUE
RETURN
END

```

其中 M 代表 ∞ , 根据具体问题的要求取一个足够大的数字。

下面我们来研究关于最小权 H 回路及其近似解法。

作为哈密顿回路的一个推广是推销员问题, 亦称货郎担问题。

设有一个推销员从他所在的城市出发去访问 $n-1$ 个城市, 要求每个城市经过一次而且仅仅一次, 然后返回原地, 问他的旅行路线应作怎样的安排才能最经济? 用图论观点来说, 就是要找一条权最小的哈密顿回路, 即所谓最小权 H 回路。显然, 研究这类问题是非常有趣而且很有实用价值的, 但是很可惜, 至今还没有找到好的解决办法, 我们在这里介绍一种“近邻法”。要注意, 按此方法求得的 H 回路未必就是最小权 H 回路, 但很接近最小权 H 回路。

近邻法的步骤如下:

设 $G=(V,E)$ 是具有 n 个结点的带权的完全图, 其中 $w(e_i)$ 是边 e_i 的权, 从中找一条较好的 H 回路的步骤是:

(1) 任取一个结点为始点, 找出最靠近始点的一个结点(最靠近是指两点间权最小), 这样便构成了具有一条边的初始通路。

(2) 设 x 是刚加在这条通路上的一个结点, 在所有不在这条通路上的结点中, 选一个最靠近 x 的结点, 并将 x 与这个结点连接起来的边加到这条通路上, 从而得到一条较前次更长的通路, 重复这个步骤, 直到 G 中的每个结点均出现在这条通路上为止。

(3) 将始点和最后加到这条通路上的结点用边连结, 便得到一条 H 回路。

例 5-8 设有一个货郎住在市镇 a , 为推销货物, 他要访问市镇 b, c 和 d , 这四个市镇间的实际距离(通常意义下的)如图 5-16(a)所示, 问他应该怎样安排旅行路线, 才能使他所走的路程较短?

解: 按照“近邻法”的步骤, 我们求得子图(b)、(c)、(d)和(e), 其中(e)是最后结果, 得到总距离是 48, 但是最近的一条 H 回路总距离是 47, 所以由“近邻法”求得的 H 回路未必是最小 H 回路, 但是它很接近最小权 H 回路。

例 5-9 设图 5-17 是一个带权的图, 用“近邻法”求 H 回路。

解: 求解的过程如图 5-17(b)到(f)所示, 其中(f)是最后结果, 由(f)发现, 这条 H 回路之权是 40, 但最小权 H 回路之权是 37, 如图 5-17(g)所示。因此求得的 H 回路的权很接近 40。

欧拉图的应用及其推广的例子是邮路问题。设一个邮递员从邮局出发沿着他所管辖的街道送信, 然后返回到邮局, 他应选择怎样的路线, 才能使得所走的实际路程最短呢? 我们知道, 如果他管辖的街道恰好成为欧拉图, 就不存在最短路程的问题, 因为不论他怎样安排行走路线, 所走路程总是一定的。但实际问题中一般不会恰巧就是欧拉图, 必然某些街道要重复经过, 因此邮路问题是一个既与欧拉图又与最小权通路有关的问题。

我们把邮路问题用图论的概念描述如下: 在一个网络(即权图)

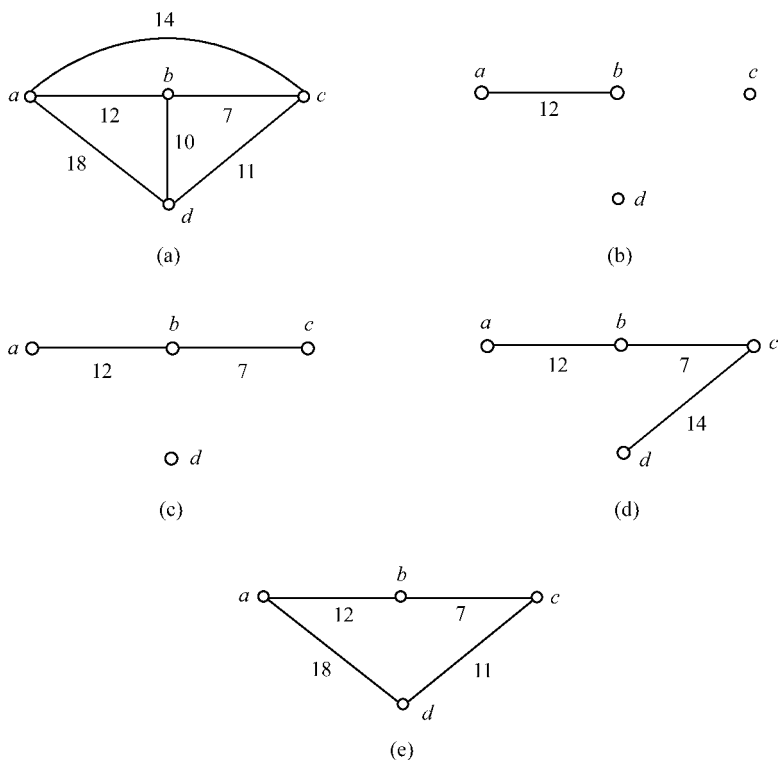


图 5-16 货郎担问题求解过程

N 中,怎样找到一条回路 C ,使得 C 包含 N 中的每条边至少一次,而且回路 C 具有最小权 $w(C)$ 。

这条回路 C 分两种情况:

(1) 如果 N 是欧拉图,必定有欧拉回路, C 即找到。

(2) 如果 N 是具有从 v_i 到 v_j 的欧拉通路的连通图, C 的构造如下:

找从 v_i 到 v_j 的欧拉通路及 v_i 到 v_j 的最小权通路。这两条通路合并在一起就是最小权回路。

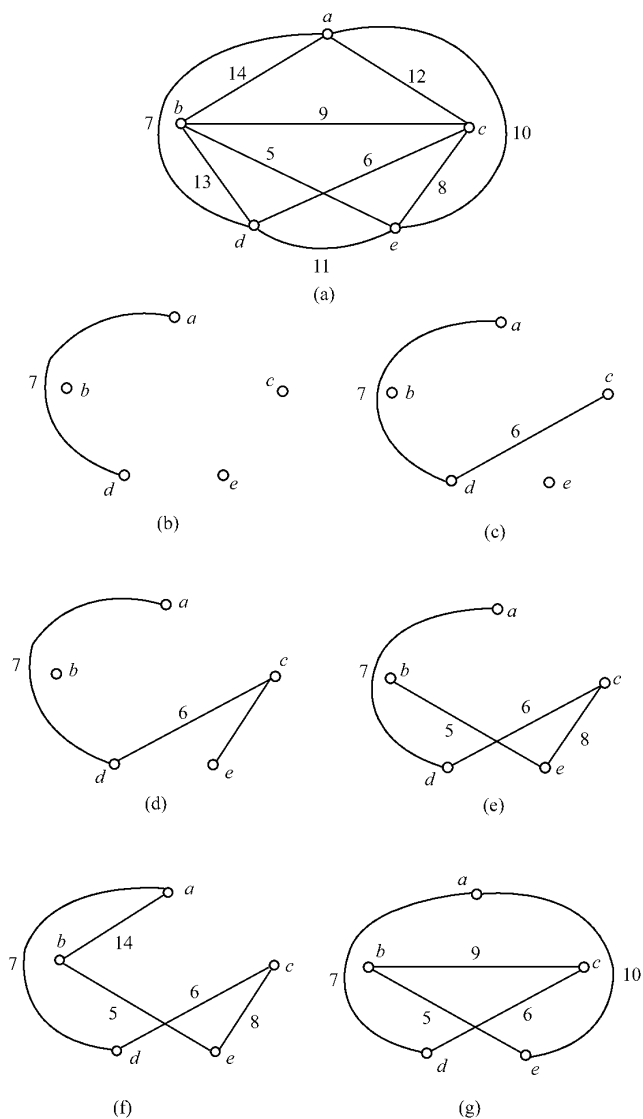


图 5-17 邮路问题求解过程

例 5-10 图 5-18 是非欧拉图,它有欧拉通路如下:

$$(v_1, v_2, v_3, v_5, v_4, v_3, v_1, v_4, v_6, v_5, v_2, v_6)$$

v_1 和 v_6 的最小权通路如下:

$$(v_1, v_4, v_5, v_2, v_6)$$

上述两条通路合并得:

$$(v_1, v_2, v_3, v_5, v_4, v_3, v_1, v_4, v_6, v_5, v_2, v_6, v_2, v_5, v_4, v_1)$$

这就是具有最小权的一条邮路。

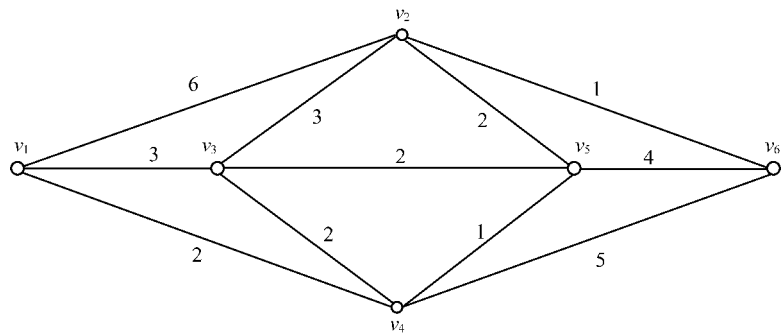


图 5-18 例 5-10 的示例图

一般说来,网络中包括各条边之回路,其重复的边数与奇结点数有关,若奇结点多于 2,则回路中会出现更多的重复的边,问题是怎样使重复边的权总和最小,对此数学家已作了理论上的证明,得出结论如下:

设 C 是网络 N 中一条包含 N 的所有边的回路,则 C 具有最小权当且仅当:

- (1) 每条边最多重复一次。
- (2) 在 N 的每个回路上,有重复边的权之和小于回路权的一半。

下面我们将要介绍几种特殊类型的图。

5.5 二 分 图

定义 5-8 如果图 $G=(V,E)$ 的结点能分成两个子集 $\hat{V}_1 \subset V$ 和 $\hat{V}_2 \subset V$, 使得同一个子集中的任意两个结点无边相连, 则称 G 是二分图。 $\hat{V}_1$ 和 $\hat{V}_2$ 称为 G 的互补结点子集。

把图的结点分成两个集合 $\hat{V}_1$ 和 $\hat{V}_2$, 而且 $\hat{V}_1$ 和 $\hat{V}_2$ 互不相交, 这称为图的二划分。一个完全二分图是一个具有二划分的简单二分图, 其中 $\hat{V}_1$ 的每个结点与 $\hat{V}_2$ 的每个结点相连。若 $|\hat{V}_1|=m, |\hat{V}_2|=n$, 则这样的图(即完全二分图)记为 $K_{m,n}$ 。

例 5-11 两个完全二分图如图 5-19(a)和(b)所示, 一般的二分图如图 5-19(c)。

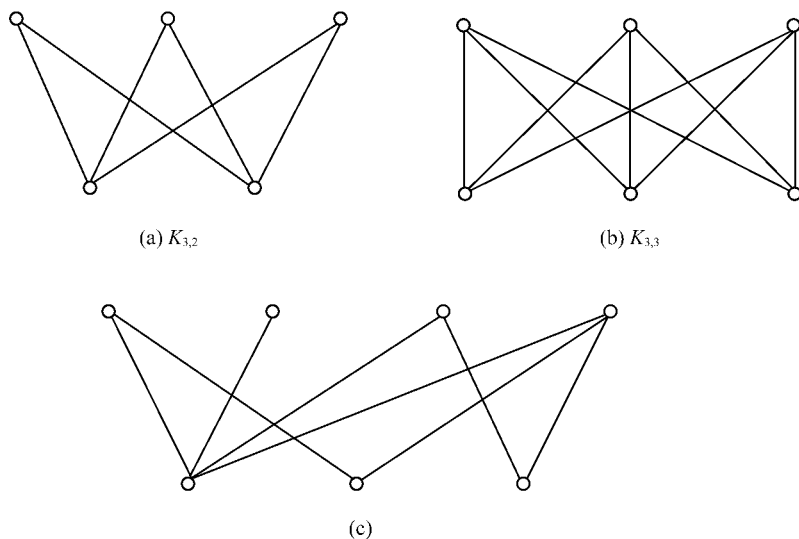


图 5-19 三个二分图

定理 5-8 一个图 G 是二分图当且仅当它的所有回路的长度是偶数。

证明：如果 G 是二分图，则 V 可分成 $\tilde{V}_1$ 和 $\tilde{V}_2$ 两个子集。而且对于 $(v_i, v_j) \in E$ ，有 $v_i \in \tilde{V}_1, v_j \in \tilde{V}_2$ 。令 $(v_{i0}, v_{i1}, \dots, v_{i{l-1}}, v_{il}) = C_i$ 是 G 中长度为 l 的回路。不失一般性，我们可以假定 $v_{i0} \in \tilde{V}_1$ ，因此 $v_{i2}, v_{i4}, \dots, v_{il} \in \tilde{V}_1$ ，而 $v_{i1}, v_{i3}, \dots, v_{i{l-1}} \in \tilde{V}_2$ 。因此 $l-1$ 必定是奇数，故 l 是偶数。

反之，假定 G 中每个回路的长度是偶数，若 G 是连通图。定义 V 的两个子集如下：

$$\tilde{V}_1 = \{v_i \mid v_i \text{ 与一个固定结点 } x \text{ 的距离是偶数}\}$$

$$\tilde{V}_2 = V - \tilde{V}_1$$

假定存在一条边 $(v_i, v_j) \in E$ ，使得 $v_i, v_j \in \tilde{V}_1$ ，于是由结点 x 到 v_i 的短程线长度是偶数，边 (v_i, v_j) 及由 x 到 v_i 的短程线（长度是偶数）一起构成一条回路，这条回路的长度必定是奇数，这与已知条件矛盾。因此 G 中无 $(v_i, v_j) \in E$ ，使得 $v_i \in \tilde{V}_1, v_j \in \tilde{V}_1$ 。同理，若有边 $(v_i, v_j) \in E$ ，而且 $v_i \in \tilde{V}_2, v_j \in \tilde{V}_2$ ，也会与已知条件发生矛盾。从而得出结论，若有边 $(v_i, v_j) \in E$ ，必定 $v_i \in \tilde{V}_1, v_j \in \tilde{V}_2$ 。因此 G 是一具有 $\tilde{V}_1$ 和 $\tilde{V}_2$ 互补结点子集的二分图。

如果 G 的每个回路的长度是偶数，但是 G 不是连通图，那么 G 必由独立连通子图组成，此时上述定理对每个独立子图也是成立的。也就是说，一个图 G 的独立子图是二分图当且仅当该独立子图的回路长度是偶数。

例 5-12 设我边防军民捕获六名不同国籍的间谍 a, b, c, d, e, f ，他们各自懂下列语言：

a ：会讲汉语、法语和日语；

b ：会讲德语、日语和俄语；

c ：会讲英语和法语；

d ：会讲汉语和西班牙语；

e ：会讲英语和德语；

f ：会讲俄语和西班牙语。

问是否可将这六人锁在两个房间内，使得每个房间的人不能直

接对话？

解：把六个人和七种语言分别用图的结点表示，边代表人与语言的关系，于是得到图 5-20。

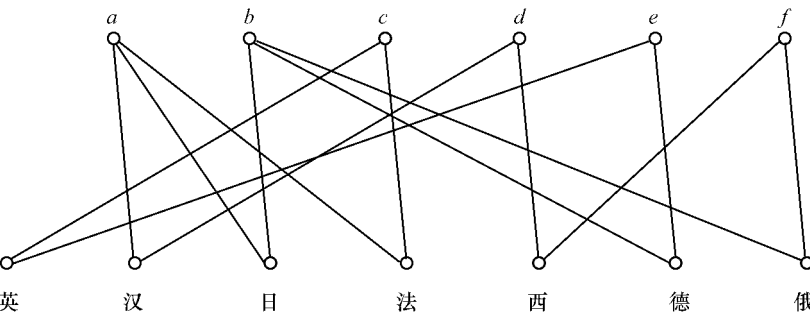


图 5-20 例 5-12 图示

这是一个二分图，由图可看出，若如下分配：

$$\text{房间 1} = \{a, e, f\}$$

$$\text{房间 2} = \{b, c, d\}$$

则每个房间内的人不可能直接对话。

例 5-13 一教研室有四名教师(王、李、张、陈)，他们能教四门课程：数学(M)、FORTRAN 语言(F)、操作系统(OS)、C 语言(C)，其中王能教操作系统和数学，李能教 FORTRAN、操作系统和 C，张能教 C，陈能教数学和 FORTRAN。问怎样分配才能使每个教师不教自己不熟悉的课程？

解：这个问题先用二分图表示出课程与教师之间的关系如图 5-21所示。

显然，张教 C，其余三人的一种可能的分配办法是王教数学，陈教 FORTRAN，李教操作系统。

匹配(或叫相配)的问题与二分图密切相关。

令 G 是一个二分图，具有互补结点子集 $\tilde{V}_1$ 和 $\tilde{V}_2$ ，其 $\tilde{V}_1 = \{v_1, v_2, \dots, v_r\}$ ，从 $\tilde{V}_1$ 到 $\tilde{V}_2$ 的一个匹配是 G 的一个子图，这个子图具有

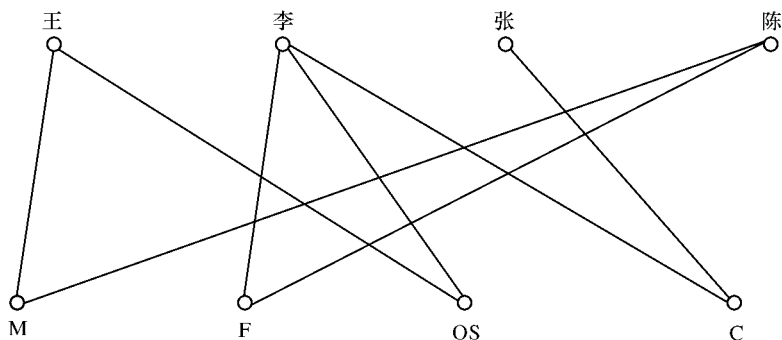


图 5-21 例 5-13 图示

如下形式的 r 条边,即:

$$(v_1, v'_1), (v_2, v'_2), \dots, (v_r, v'_r)$$

其中 $v'_1, v'_2, \dots, v'_r \in \tilde{V}_2$, 而且 $v'_i \neq v'_j$ 。

例 5-14 图 5-22(a) 表示具有互补结点集合 $\tilde{V}_1$ 和 $\tilde{V}_2$ 的二分图, (b) 是 (a) 的一种 $\tilde{V}_1$ 到 $\tilde{V}_2$ 的可能匹配。

显然, 图 5-22(b) 是 (a) 的一个子集而且满足匹配定义。值得注意的是, 并不是所有的二分图都存在一种匹配, 如图 5-23 就不存在 $\tilde{V}_1$ 到 $\tilde{V}_2$ 的匹配。

那么, 一个二分图总存在匹配的条件是什么呢?

定理 5-9 设 G 是具有互补结点子集 $\tilde{V}_1$ 和 $\tilde{V}_2$ 的二分图, 则 G 有一个从 $\tilde{V}_1$ 到 $\tilde{V}_2$ 的匹配当且仅当 $\tilde{V}_1$ 中每 k 个结点 ($k=1, 2, \dots, |\tilde{V}_1|$) 至少要与 $\tilde{V}_2$ 中 k 个结点连通(这条件称为相异条件)。

这定理的充分性证明较难, 此处从略。

定理 5-10 设 G 是具有互补结点子集 $\tilde{V}_1$ 和 $\tilde{V}_2$ 的二分图, 那么 G 有 $\tilde{V}_1$ 到 $\tilde{V}_2$ 的匹配的条件是: 存在整数 $t > 0$,

- (1) $\tilde{V}_1$ 中的每个结点, 至少存在 t 条相邻边。
- (2) $\tilde{V}_2$ 中的每个结点, 至多存在 t 条相邻边。

我们把这两个条件简称“ t 条件”。

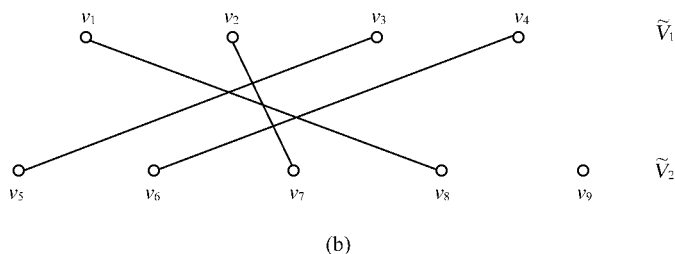
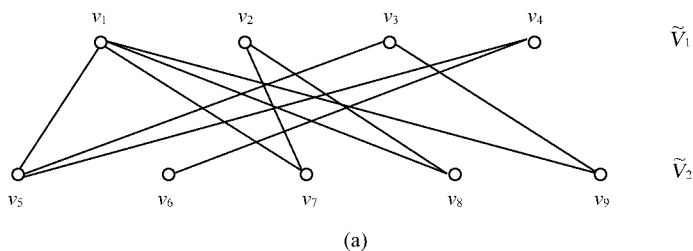


图 5-22 例 5-14 图示之一

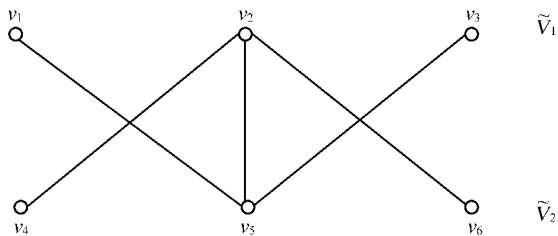


图 5-23 例 5-14 图示之二

证明:

如果(1)成立, 设 $\tilde{V}_1$ 中的任一子集 V'_1 有 k 个结点 ($k=1, 2, \dots, |\tilde{V}_1|$), 则与 V'_1 中 k 个结点相邻的边的总数至少为 kt 。由(2), $\tilde{V}_2$ 中至少要有 k 个结点成为这些边的端点。因此 $\tilde{V}_1$ 中的每 k 个结点 ($k=1, 2, \dots, |\tilde{V}_1|$) 至少与 $\tilde{V}_2$ 中 k 个结点连通。由前条定理, G 有一个 $\tilde{V}_1$ 到 $\tilde{V}_2$ 的匹配。

例 5-15 设有二分图如图 5-24 所示,问它是否存在从 $\tilde{V}_1$ 到 $\tilde{V}_2$ 的匹配。

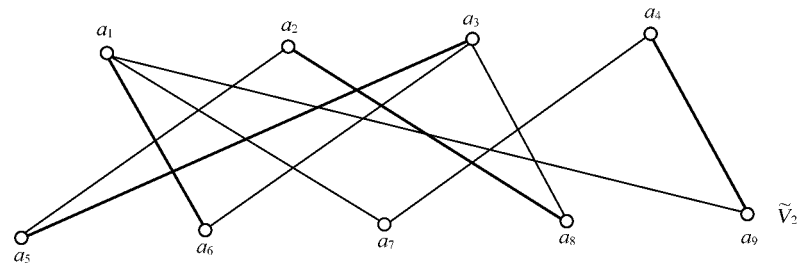


图 5-24 例 5-15 图示

- 解: (1) 显然,“ t 条件”是满足的($t=2$)。
- (2) 相异条件也是满足的,因为每 k 个结点,譬如说 $k=2$, $\tilde{V}_1$ 中的 a_1 和 a_2 与 $\tilde{V}_2$ 中有 5 个结点连通, a_2 和 a_4 与 $\tilde{V}_2$ 中 4 个结点连通(其他情况可以一一验证),所以相异条件满足。
- (3) $\tilde{V}_1$ 到 $\tilde{V}_2$ 的一种可能匹配如图上粗线所示。

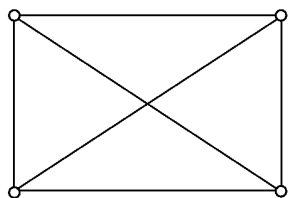
5.6 平面图

研究平面图是很有实用价值的。如大家熟悉的印刷电路,除结点外,它的导线是不能交叉的,这就是平面图的例子。

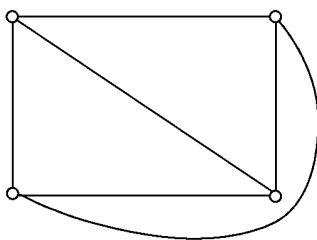
定义 5-9 一个图 G 如能画在平面上,除结点外,它的边都不相交,这种图称为平面图,反之称为非平面图。

注意,有许多图表面上是相交的,但如能移动其边,使它不相交,这图仍然是平面图,试分析图 5-25 中的各图。

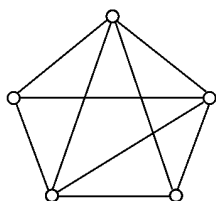
在图 5-25 中,(a)与(b)是同一个图,它是平面图;(c)与(d)是同一个图,它也是平面图。但(e)是非平面图,因为不管你如何移动,它总会有两条线交叉,如(f)所示;对于(g)也是如此,它的一种可能的移动见(h)。



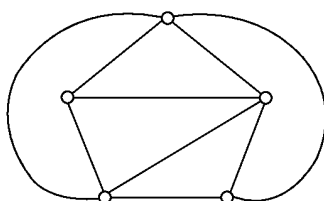
(a)



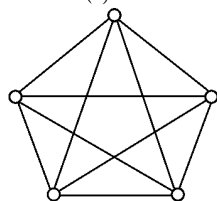
(b)



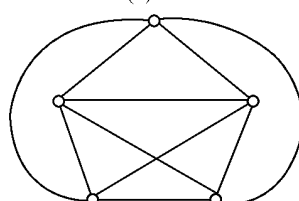
(c)



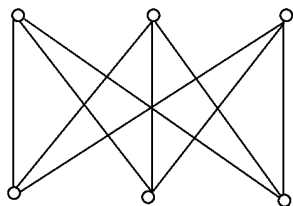
(d)



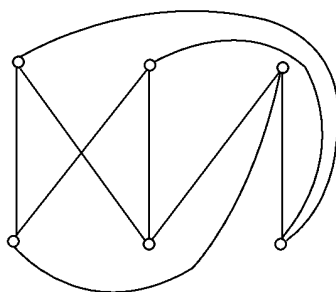
(e)



(f)



(g)



(h)

图 5-25 平面图与非平面图示例

假定把一个平面图画在纸上,然后用剪刀沿各条边剪下,于是这平面将分成若干块纸片,每块纸片称为平面的区域,即一个平面图形的区域是由边围成的,而且它不可以再分成更小的子区域。如果区域的面积是有限的,称它为有限区域,如果区域的面积是无限的,称它为无限区域。如图 5-26 所示,整个平面图围成五个区域, r_1 和 r_2 分别由三条边围成, r_3 由三条边围成, r_4 由四条边围成,它们均是有限区域, r_5 是由三条边围成的无限区域。

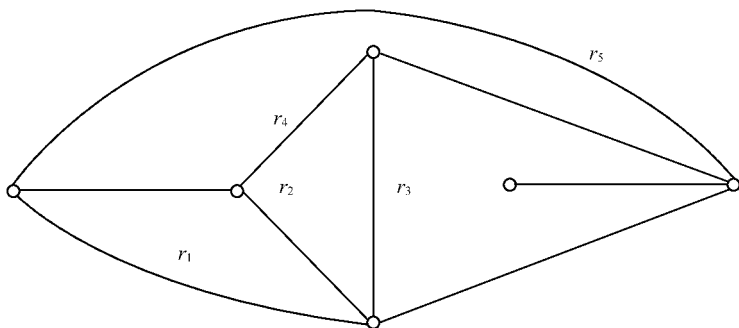


图 5-26 平面图示例之一

显然,任何一个有限区域至少由三条边围成,任何一个平面图有而且仅有一个无限区域。下面我们研究一个平面图应该满足的条件。

定理 5-11 对于任何一个连通平面图 G , 有:

$$v - e + r = 2$$

其中 v 代表 G 的结点数目, e 代表 G 的边数, r 代表 G 的区域数。

这个公式称为平面图的欧拉公式。

证明: 对边作归纳。

(1) 当 G 是单个结点时, 可能有两种情况。一是仅仅一个孤立点, 见图 5-27(a), 此时, $e=0$, 显然公式是成立的; 另一种是带有一个环, 见图 5-27(b), 此时, $v=1, e=1, r=2$, 所以公式仍然成立。

(2) 假定对 $e=k$ 时成立, 即:

$$v' - k + r' = 2$$

在 G 上加一条边, 即 $e=k+1$, 此时有两种情况。一是增加一条边同时加了一个结点, 如图 5-27(c) 所示, 即 $v=v'+1, e=k+1, r=r'$, 故 $(v'+1)-(k+1)+r'=v'-k+r'=2$; 二是增加的一条边不增加结点, 而是连接 G 中的两个结点, 如图 5-27(d) 所示, 此时 $v=v', e=k+1, r=r'+1$, 于是:

$$v' - (k+1) + (r'+1) = v' - k + r' = 2$$

所以定理成立。

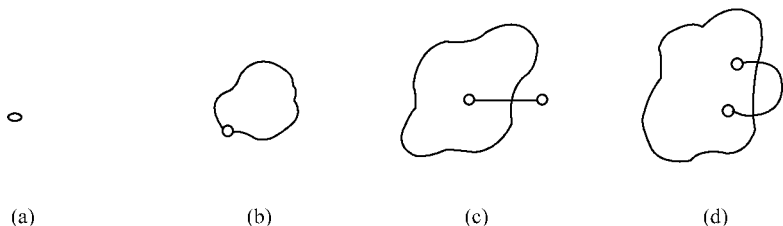


图 5-27 平面图示例之二

必须强调指出, 欧拉公式只适用于连通平面图的情况, 即任何一个连通平面图毫无例外地满足欧拉公式, 不满足欧拉公式的则不是平面图。但要注意, 直接使用欧拉公式是很困难的, 因为其区域数 r 是不容易从图上看出的。所以我们应用欧拉公式来找出一个平面图应该满足的不等式。

定理 5-12 任何一个连通无环的平面图 G , 如果每个区域由三条及三条以上的边组成, 则有:

$$e \leqslant 3v - 6 \quad (1)$$

证明: 由于 G 是平面图, 每个区域由三条及三条以上的边组成, 所以围区域所用总的边数 $\geqslant 3r$; 另一方面, 图中每条边最多为两个区域的边界, 因此总的边数小于或等于 $2e$, 从而有:

$$3r \leqslant \text{总的边数} \leqslant 2e$$

即:

$$r \leqslant \frac{2}{3}e$$

以 $r \leq \frac{2}{3}e$ 代入欧拉公式,从而消去区域数 r ,得到相应的不等式是:

$$2 \leq v - e + \frac{2}{3}e$$

即:
$$e \leq 3v - 6$$

所以每个区域由三条及三条以上的边围成的平面图要满足相应的不等式,不满足相应不等式的肯定不是平面图。例如图 5-25(c), $v=5, e=9$, 显然满足不等式(1), 但图 5-25(e), $v=5, e=10$, 显然不满足不等式(1), 所以不是平面图。

我们再看图 5-25(g), $v=6, e=9$, 满足 $9 \leq 18 - 6$, 但事实上它并不是一个平面图, 这是为什么呢? 原来图 5-25(g) 的每个区域至少由四条边构成, 所以判别它不能用不等式(1)。对于至少由四条边围成区域的情况, 必须另外建立其不等式。

定理 5-13 任何一个无环的连通平面图 G , 如果每个区域由四条及四条以上的边围成, 则有相应不等式:

$$e \leq 2v - 4 \quad (2)$$

证明方法与上一定理类似, 此处不再赘述。对于图 5-25(g), $v=6, e=9$, 用不等式(2)判别, 发现 $9 \leq 12 - 4$ 不成立, 故它不是平面图。

由此我们得到找平面图所满足不等式的一般方法:

若平面图的每个区域至少有五条边围成, 则相应的不等式是:

$$3e \leq 5v - 10$$

若平面图的每个区域至少有六条边围成, 则相应的不等式是:

$$2e \leq 3v - 6$$

依此类推。判别平面图的不等式, 要随着平面图围成区域的最少边数的改变而改变, 若不根据情况而套用某一个不等式, 会导致错误的结论。

我们的结论是: 凡是平面图一定满足相应的不等式, 不满足相应不等式的肯定不是平面图, 但是满足某一个不等式的未必都是平

面图。

凡是不超过四个结点的图不可能存在非平面图,五个结点和六个结点的非平面图就是图 5-25(e)和(g),分别叫 K_5 图和 $K_{3,3}$ 图,它们是非平面图的两个最小模型。1930 年,波兰数学家 K. Kuratowski 找到了判别非平面图的充要条件,叙述这条定理之前,先说明图的一个性质。如果在图的一条边上插入一个新的 2 次结点(即该结点次数为 2),使一条边变成两条边,或者对于两条关联于一个 2 次结点的边,去掉这个结点,使两条边合成一条边,则图的平面性不受影响。确切地说,如果两个图 G_1 和 G_2 是同构的或者通过反复插入和(或)除去 2 次结点,它们能变成同构的图,则称它们是在 2 次结点内同构的。

定理 5-14 (Kuratowski 定理)一个图是平面图,当且仅当它不包含与 $K_{3,3}$ 或 K_5 在 2 次结点内同构的子图。

定理 5-15 设 $G=(V,E)$ 是一个连通平面图,且它至少有 3 个结点,则 G 中至少有一个结点(譬如说 v),使得 $\deg(v)\leq 5$ 。

证明: 设 p 是 G 的结点数, q 是 G 的边数。用反证法,假如 G 的每个结点 v_i ,有 $\deg(v_i)\geq 6$,由定理 5-1 可知:

$$\sum_{i=1}^p \deg(v_i) = 2q$$

于是:

$$2q \geq 6p, \text{ 即 } q \geq 3p > 3p - 6$$

但我们已经证明(见定理 5-12)一个连通平面图,当结点 $p \geq 3$ 时, p 和 q 的关系是:

$$q \leq 3p - 6$$

显然发生矛盾。因此至少有一个 $v \in V$, 满足 $\deg(v) \leq 5$ 。

在证明一个图是五色图时要用到这定理。

5.7 四 色 图

当你打开一张中华人民共和国地图的时候,呈现在你眼前的是

光彩夺目的颜色,尽管她的幅源是如此辽阔,但各省的形状、大小及位置都能用不同的颜色分得清清楚楚,这是与地图着色理论分不开的。我们下面要研究的四色图理论,就是来源于地图的着色。

下面我们在平面图的基础上,利用图论方法简单地介绍四色图问题。

1. 平面图区域的四色问题

定义 5-10 设平面图 G 的任意两个区域有一条公共边,则称这两个区域是相邻区域。

例 5-16 设有一个平面图如图 5-28 所示, r_2 和 r_3 、 r_2 和 r_5 、 r_5 和 r_6 等均是相邻区域,而 r_1 和 r_4 、 r_1 和 r_2 等均不是相邻区域。

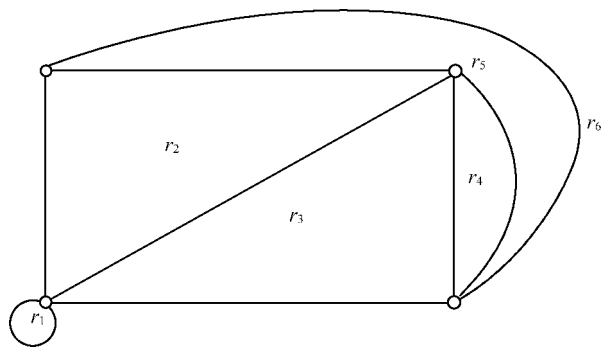


图 5-28 一种三色图

定义 5-11 一个平面图 G 的着色法是对 G 的颜色设计,使得任何相邻两个区域有不同的颜色。

如果存在一种着色法,用了 n 种颜色,则称图 G 是 n 色图。记以 $X(G)=n$ 。

图 5-28 只要三种颜色,所以 G 是三色图。一种可能的着色法如下:

- r_1 区域着红色;
- r_2 区域着黄色;

r_3 区域着红色;

r_4 区域着黄色;

r_5 区域着红色;

r_6 区域着绿色。

对于任何一个连通平面图,要在相邻区域上着不同的颜色,至少要用几种呢?早先,数学家曾经证明并得出如下的结论:

定理 5-16 任何一个连通平面图是五色图。

但后来在平面图上经多次试验,没有找到一种平面图一定要用五种颜色的。在 100 多年前,有人猜测只要用四种颜色就够了,这就是世界上著名的四色猜测问题。这个猜测一经提出,迷住了许多数学家,但是谁都无法用数学的方法证明它。直到 1976 年,Appel 和 Haken 两人宣布了四色理论的证明方法。他们用大型电子计算机分析了 2000 多种图包括几百万种情况,花了大量的机器时间,终于证明了这个问题,从而解决了 100 多年来引人注目的难题。

这条定理是这样叙述的。

定理 5-17(四色定理) 如果对一个连通平面图的各个区域着色,使得相邻的区域有不同的颜色,那么所用的颜色可以不多于四种。

简单地说,每个平面图区域是四色的。

2. 平面图结点的四色问题

与平面图区域四色理论相类似的是平面结点的着色问题。

一个平面图 G 的结点着色法是对 G 的结点的颜色的一种设计,使得相邻两个结点有不同的颜色。如果一个图存在一种着色法,它用了 n 种颜色,则称 G 是 n 色图。亦用 $X(G)=n$ 表示。

读者自然会联想到这样一个十分重要的问题,对于任何一个连通平面图,欲使相邻结点(即关联同一条边的两个结点)着不同的颜色,是否也只要四种就够了?答案是肯定的。为了讨论这个问题,先介绍平面图 G 的对偶图 G^* 的概念。

图的对偶概念叙述如下：

已知一个连通平面图 G ，具有区域 $F_1, F_2, \dots, F_n$ (包括一个无限区域)。在每个区域 F_i 内取一个结点 f_i ，把具有公共边的两个相邻区域都用一条曲线连结其结点。显然，每条曲线跨过两个区域的公共边，而且可以使这些曲线互不相交，这样我们求得一个新的图 G^* ，从而 G^* 的每个结点只对应 G 的一个区域；反之， G^* 的每个区域只对应 G 的一个结点， G^* 的每条边只与 G 的一条边相交，反之亦然。则 G^* 称为 G 的一个对偶图。

例 5-17 图 5-29 上的实线为图 G ，它的对偶图 G^* 用虚线表示。

对于 G 的对偶图 G^* ， G 中每个区域的着色对应 G^* 中一个结点着色，反之亦然，因此得到下面的定理：

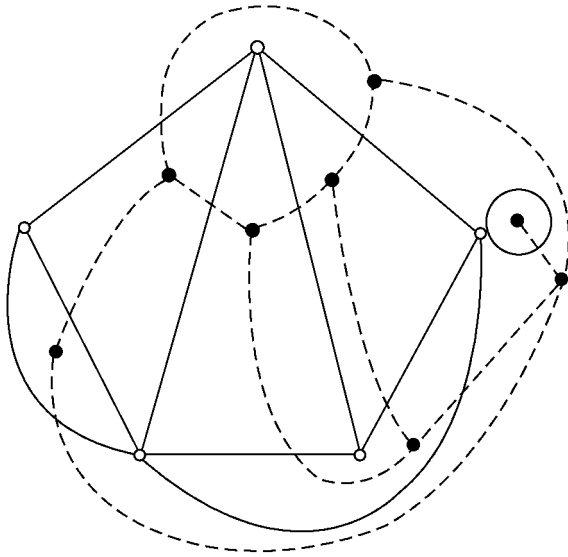


图 5-29 例 5-17 图示

定理 5-18 G 的区域是 n 色当且仅当 G^* 的结点是 n 色。

由于平面图区域的四色定理已经在 1976 年证明了，所以平面图结点四色定理也成立。即：每个平面图的结点是 4 色的。

对平面图结点着色法有一个简单算法：

(1) 首先将 G 的结点按次数递减次序方式排序(由于有相同次数的结点,所以排序不是惟一的)。

(2) 用一种颜色先着在序列的第一个结点上,然后将这种颜色依次着在这序列的与此结点不相邻的后继结点上。

(3) 余下未着色的结点构成一个子序列,换一种颜色按与第(2)步相似的方法在这子序列上着色。如此进行,直到各个结点都已着色为止。

例 5-18 设有一个平面图如图 5-30 所示,试给这图 G 着色。

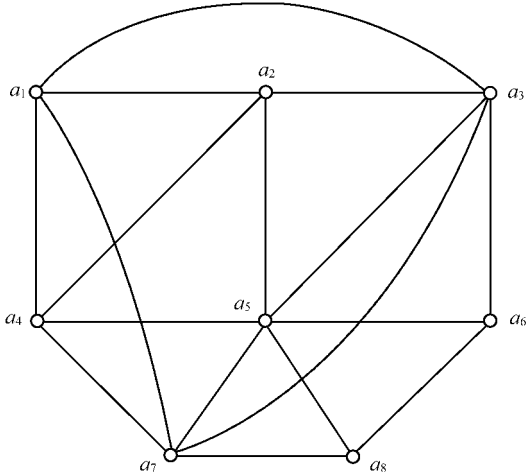


图 5-30 例 5-18 图示

算法如下：

(1) 将结点按次数递减次序排序,得到排序如下：

$$a_5, a_3, a_7, a_1, a_2, a_4, a_6, a_8$$

用第一种颜色着在 a_5, a_1 上,得到序列是：

$$\boxed{a_5}, a_3, a_7, \boxed{a_1}, a_2, a_4, a_6, a_8$$

(2) 用第二种颜色着在余下的空白子序列的 a_3, a_4, a_8 上,用 $\triangle$

表示某结点着了第二种颜色,得到序列如下:

$$\boxed{a_5}, \triangle a_3, a_7, \boxed{a_1}, a_2, \triangle a_4, a_6, \triangle a_8$$

(3) 用第三种颜色着在余下的空白子序列的 a_7 、 a_2 和 a_6 上,故每个相邻结点着了不同的颜色,这个结点序列只要用三种颜色就够了,因此 G 是 3 色图,即:

$$X(G) = 3$$

定理 5-19 对于连通平面图 G , G 是 2 色图当且仅当 G 的每个回路的长度是偶数。

证明: 假定 G 是 2 色图,令 M 是着第一种颜色的结点集合, N 是着第二种颜色的结点集合,由于 M 中的结点着相同颜色,所以 M 中结点互相不相邻,即没有连接 M 中每两个结点的边。同理, N 中结点也互相不相邻,所以 M 和 N 构成一个二分图。即 G 是一个二分图。由定理 5-8 可得出 G 的每个回路的长度是偶数。

最后,假定 G 的每个回路是偶数,我们来证明它能推出 G 是 2 色图。

我们取一个结点,着上第一种颜色,譬如说是红色。其他结点颜色着法如下:如果一个结点着了红色,则该点各相邻点着第二种颜色,譬如说白色;如果一个结点着了白色,则该点的各相邻点着红色,由于每个回路长度是偶数,所以没有相邻结点着同样的颜色,因此 G 是 2 色图,即 $X(G)=2$ 。

5.8 树

1. 树的概念

树是一种特殊的平面图,它是一种非线性结构,在计算机的算法分析、数据结构等方面有着广泛的应用。

定义 5-12 一棵树 T 是不包含任何回路的连通图。

例如图 5-31 中的各图均符合树的定义,所以它们都是树。

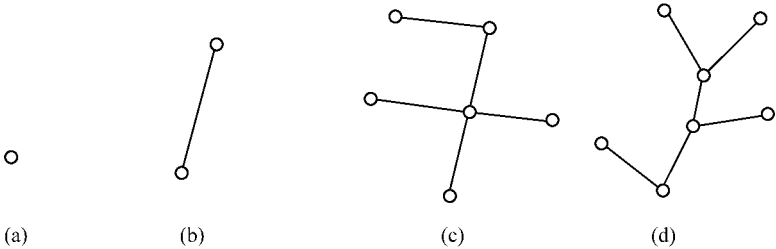


图 5-31 四种树

把树 T 的图形画出来,很像自然界的树,故取名于它,而且其他的术语也取名于自然界树上的有关术语。

根树是十分重要的概念,我们从树出发,对根树加以递归定义如下:

具有结点集合 V 的根树 T 是一棵树,使得:

- (1) T 有专门指定的结点譬如说 $v_1 \in V$,称为树的根。
- (2) 除掉 v_1 后 T 的子图可分成 $T_1, T_2, \dots, T_r$, 每个 T_i 又是一棵树($i=1, \dots, r$)。

按这定义,每个 T_i 是 v_1 的一棵子树,子树的根又称为 v_1 的儿子。

除根之外,次数 ≥ 2 的结点又称为树的分支结点,简称结点,次数 $=1$ 的结点又称为树的叶。从一个结点到某片叶的通路是一个分叉,从根到某一结点 v 的通路长度是 v 的级。习惯上把树根画在上方,叶画在下方,当然,不受这限制也是完全可以的。

例 5-19 有一棵树如图 5-32 所示。

这棵树 T 是一棵根树, a 是 T 的根, a 有三棵子树,这三棵子树的结点集合是 $V_1 = \{b, e, i, f\}, V_2 = \{c, g\}, V_3 = \{d, h, j, k\}$ 。其中每棵子树也是根树,它们的根分别是 b, c, d 。进一步可再分。

在这棵树 T 中, b, c, d, e, h 是 T 的分支结点, i, f, g, j, k 是 T

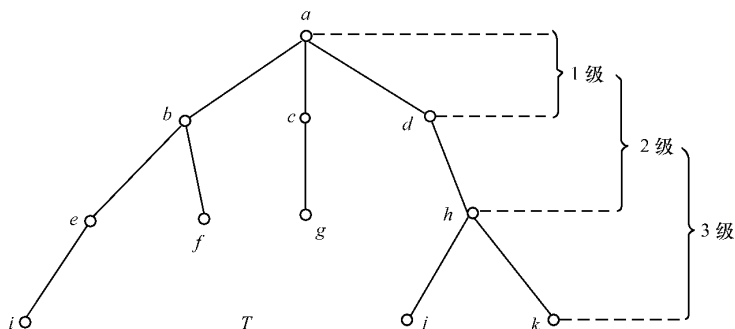


图 5-32 例 5-19 图示

的叶。 b, c, d 的级都是 1; e, f, g, h 的级都是 2; i, j, k 的级都是 3。

关于树的术语,采用家族的一套说法也是司空见惯的,树的每一个根是它的子树的那些根的父亲,这些根互相称为兄弟,而且都是它们父亲的孩子。显然,一棵树总有一个根(主根)是没有父亲的,叶是没有儿子的。

例如图 5-32, a 有三个儿子 b, c, d 。 a 是 b, c, d 的父亲, b 是 e 和 f 的父亲, b 有两个儿子 e 和 f , 当然 b, c, d 是兄弟, e 和 f 也是兄弟, 推广这方面的概念是很自然的, a 是 e 的祖父, 是 i 的曾祖父, b 是 g 的伯父, c 是 e 的叔父, e, f, g, h 是同一代堂兄弟, 等等。

欲排出一系列事件的逻辑位置, 那么用根树结构是一种好的方法, 譬如李(Li)和王(Wang)两人进行乒乓球冠军赛, 规定谁连续胜两场或总数先胜三场, 谁就获冠军, 那么这次冠军赛可能的比赛场次用根树表示就一目了然(见图 5-33)。图上标有 L 表示该场李获胜, 标 W 表示该场王获胜。

这是李、王两位运动员争夺冠军赛可能出现的比赛场次, 最多进行 5 场。

还可以用若干种与实际树很不相似的方式表示树结构。图 5-34(a) 的树可用 (b)、(c)、(d) 表示。其中 (b) 称为包含法, (c) 称为圆括号法, (d) 称为图表法。

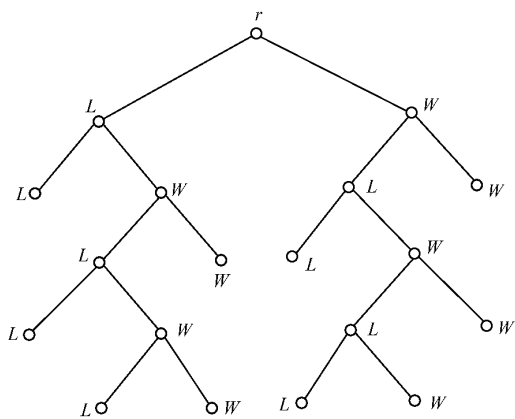
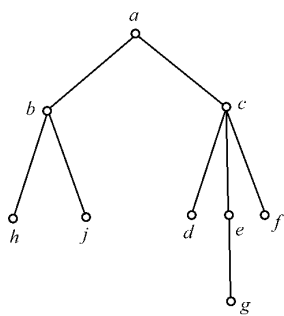
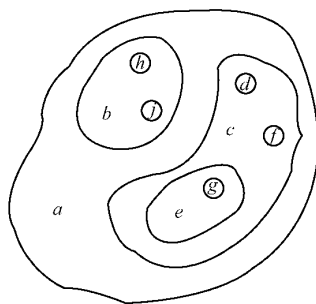


图 5-33 树的图示



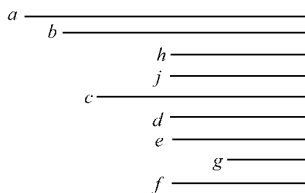
(a)



(b) 包含法

$(a(b(h)(j))(c(d)(e(g))(f)))$

(c) 圆括号法



(d) 图表法

图 5-34 四种不同的树结构表示法

大量实际问题均可用树结构表示。

例 5-20 多数国家实行邮政编码, 邮件的分类是一种树结构。下面的图 5-35 是按照 ZIP 码(一种 5 位十进制代码)分类的流程图, 当当地的所有信件到达邮局 N 后, 在邮局 N 读 ZIP 码的最高位, 于是把信件分到 10 个下属邮局 $N_1, N_2, \dots, N_9, N_0$, 每个邮局 N_i 再把该局的信件读 ZIP 码的第二位, 又把邮局 N_i 的信件分到它的下属邮局, 如此进行, 直到分到最下层的邮局为止, 总共有 10^5 种可能性。按照这种编码的树分成五级。

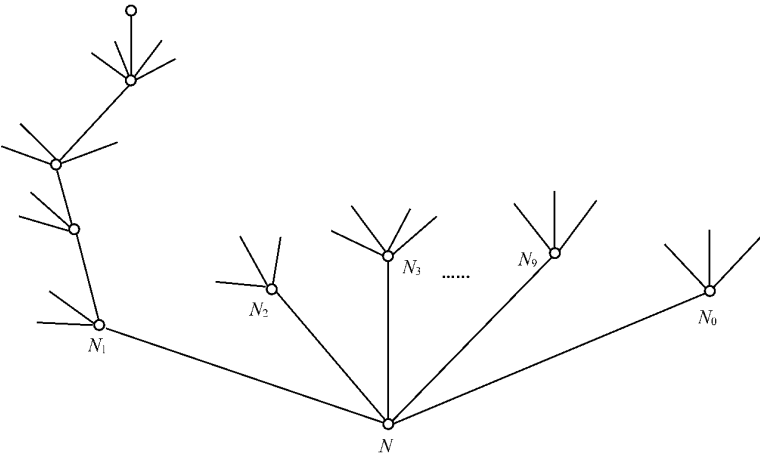


图 5-35 例 5-20 树结构表示

例 5-21 给定一个整数序列, 其中没有两个整数是相同的, 求它的最大的单调递增子序列。

这个问题可用树结构表示。设给定的整数序列是 4, 1, 13, 7, 0, 2, 8, 11, 3, 树的结点(除根之外)表示一个整数, 从根到某个给定结点 v 的通路描述了结束于 v 的单调递增子序列, 见图 5-36。从这棵树可以看出, 它有四个单调递增子序列, 它们是 (4, 7, 8, 11), (1, 7, 8, 11), (1, 2, 8, 11) 和 (0, 2, 8, 11)。每条通路之长度是 4, 由于这种树是表示数据的, 因此计算机科学工作者把它称为数据树。

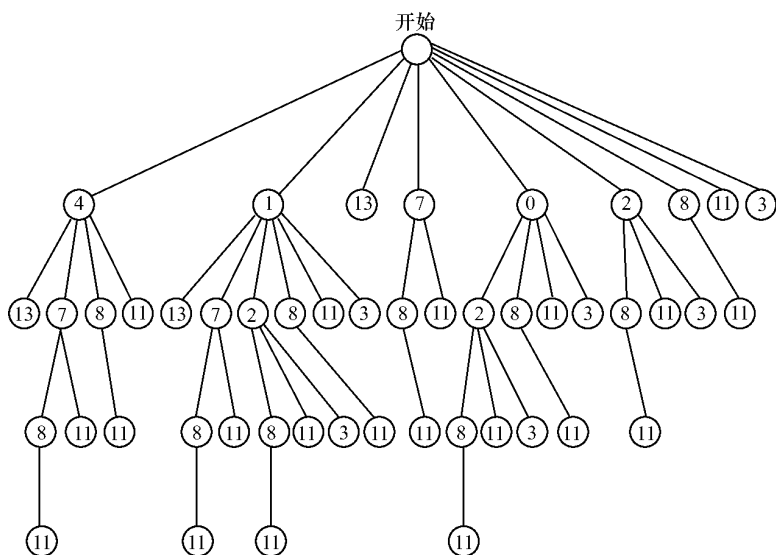


图 5-36 数据树

例 5-22 一个代数表达式的操作呈树结构,如 $(a \div b) + (c * d * e)$ 之树,见图 5-37。

例 5-23 一个句子“这小孩吃一只大苹果”的语法结构可用树结构表示,见图 5-38。

树的基本性质:

定理 5-20 设 T 是树, v_i 和 v_j 是任意两个不同的结点,那么 v_i 和 v_j 间存在惟一的通路。如果再加上一条边 (v_i, v_j) ,则构成一条惟一的简单回路。

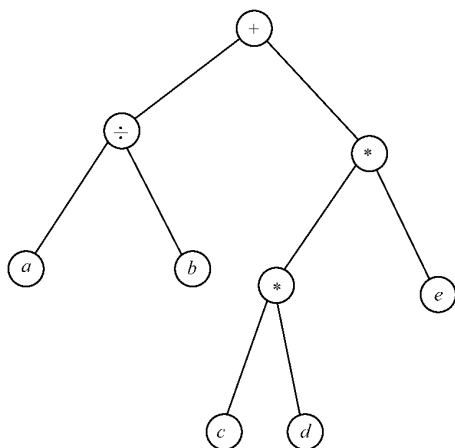


图 5-37 例 5-22 图示

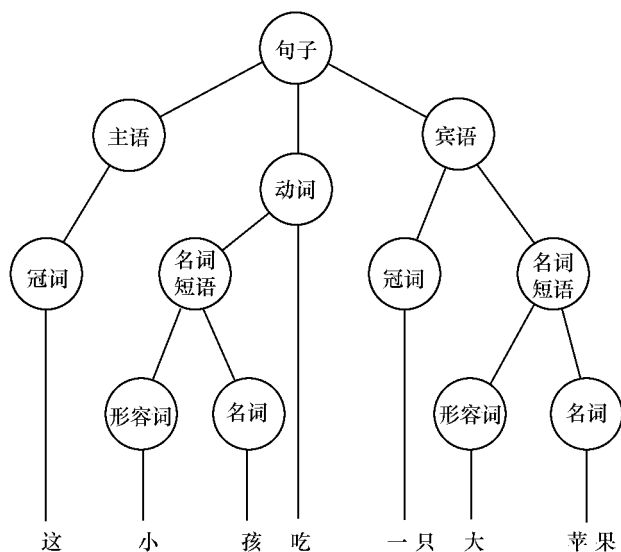


图 5-38 例 5-23 图示

证明：由于 T 是连通的，于是一定存在一条通路，因此有连接 v_i 和 v_j 的简单通路，令 P_1 是这条简单通路。如果 P_2 是连接 v_i 和 v_j 的另一条简单通路，那么 $P_1 P_2$ 包含一条回路，这与树的定义矛盾。因此 P_1 是连接 v_i 和 v_j 的惟一简单通路。

如果边 (v_i, v_j) 加到树 T 上，则 $(P_1, (v_i, v_j))$ 便构成一个回路，我们已经知道，除掉 P_1 通路外， v_i 和 v_j 间不存在另外的简单通路，所以边 (v_i, v_j) 与任何其他简单通路不能构成回路，所以只存在一条回路。

定理 5-21 对于一棵 (n, m) 树，边和结点有下述关系：

$$m = n - 1$$

其中 m 是树的边数， n 是树的结点数。

证明：用数学归纳法（对结点数 n 归纳）

(1) 验证。当 $n=1$ 或 2 时， (n, m) 树只可能有如图 5-39 所示的两种情形，等式显然成立。

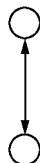
(2) 归纳。假定对所有 $i < n$, 定理成立, 即有 $m = i - 1$ 。对 (n, m) 树, 除去其中一条边, 于是得到两棵子树, 记以 (n_1, m_1) 和 (n_2, m_2) , 显然, $n_1 < n, n_2 < n$ 。由归纳假设, 有:

$$m_1 = n_1 - 1$$

(a)

$$m_2 = n_2 - 1$$

图 5-39 定理 5-21 说明图



(b)

因为 $n = n_1 + n_2, m = m_1 + m_2 + 1$, 所以有:

$$m = n_1 + n_2 - 2 + 1 = n - 1$$

定义 5-13 $t(t > 0)$ 棵树的集合称为森林。

如图 5-31 中有四棵树, 这四棵树组成了森林。如果把由四棵独立的树组成的森林加上一个结点, 并把这四棵树作为此结点的子树, 那么该森林便成为一棵树了, 所以我们亦把四棵独立的树看作是森林的子树。同样, 我们亦可用结点和边数来命名森林, 若一个森林具有 n 个结点 m 条边, 就称它为 (n, m) 森林。

推论: 如果树 T 是 (n, m) 森林, 具有 t 棵子树, 则:

$$m = n - t$$

我们上面介绍的树的基本性质是十分重要的, 它可以作为树的等价定义。即:

定义 5-14 (1) 任何两个结点间存在惟一通路的图是树。

(2) 一个连通图, 若它的边和结点满足 $m = n - 1$, 则这个连通图是树。

(3) 边和结点满足 $m = n - 1$ 而且无回路的图是树。

树有各种应用, 而最大的应用莫过于二叉树, 因此, 我们将重点讨论二叉树。

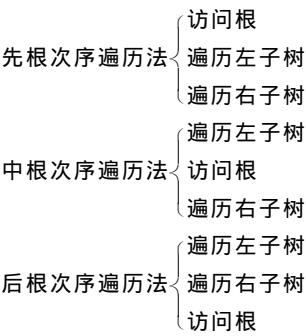
2. 二叉树

定义 5-15 一棵树 T , 如果每个结点 v 最多有两棵子树, 则称树

T 为二叉树。如果两棵子树全出现,则左边的一棵称为 v 的左子树,右边的一棵称为 v 的右子树。若仅出现一棵子树,则或者指定它为右子树,或者指定它为左子树。一棵树的每个结点有两棵子树或者说每个父亲有两个儿子,则称该树为完全二叉树。

如图 5-33 所示为 19 个结点的二叉树,而且是完全二叉树。

对于二叉树,一个十分重要的问题是要找到一些方法,能系统地访问树的结点,使得每个结点恰好访问一次。我们在这里介绍“遍历”二叉树的方法,主要有三种:



例 5-24 图 5-40 是一棵二叉树 T 。

在先根次序下, T 上的结点被访问的先后关系是:

$$\rightarrow a b d c e g f h i$$

在中根次序下, T 上的结点被访问的先后关系是:

$$\rightarrow d b a e g c h f i$$

在后根次序下, T 上的结点被访问的先后关系是:

$$\rightarrow d b g e h i f c a$$

顺便说一下,先根次序是由来已久的有趣的概念,在封建社会里,皇帝的位置传给他的长子,长子死后又传给他的长子。如果这一分支的人全部死去,再按同样的方式传给这个家族的其他子孙们。所以在理论上,可以提供所有皇帝的家谱,以先根次序写出其结点,然后,如果仅仅考虑今天还活着的人,就能得到皇位的承袭次序。

上述概念应用到实际问题中去,我们可以举一个代数操作的例子。

例 5-25 代数表达式 $y = 3 * \ln(x+1) + a/x^2$ 。其树结构表示如图 5-41 所示。

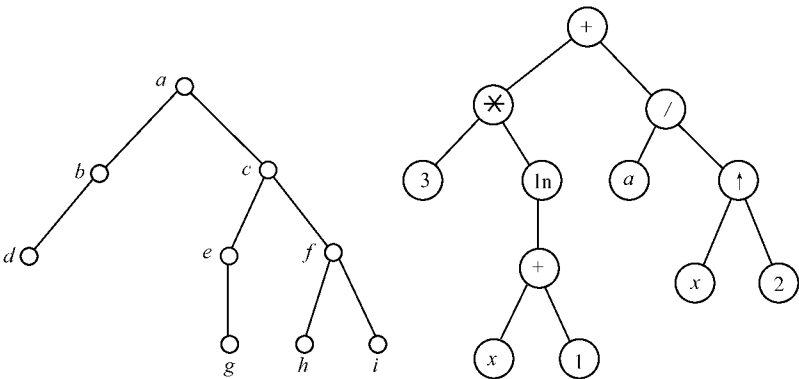


图 5-40 一棵二叉树

图 5-41 代数表达式的树结构

在先根次序下,得到表达式:

$$+ * 3 \ln + x 1 / a \uparrow x 2$$

这就是表达式的前缀表示,或称“波兰记号”,顺便说一下,波兰记号是波兰数学家 Lukasiewicz 引进的,虽然这里未详细介绍,但这是十分有用的记号。

在中根次序下,得到表达式:

$$3 * \ln x + 1 + a / x \uparrow 2$$

这就是表达式的中缀表示,基本上与原来的表达式顺序一样,但无括号,这时表达式的运算优先级有时是不明确的。

在后根次序下,得到表达式:

$$3 x 1 + \ln * a x 2 \uparrow / +$$

这就是表达式的后缀表示,或称“逆波兰记号”,这种表示给表达式的编译带来方便。

现在,我们要介绍怎样用相应的二叉树来表示任何一棵根树,首先,我们要弄懂为什么要将一般树化成二叉树? 由于树在计算机内存中可通过多重链表来表示,每个链结点所占内存单元的个数依赖

于该结点的儿子个数,一个结点生 n 个儿子,一般要用 $(n+1)$ 个单元表示该结点,其中 n 个单元用来指出该结点的各儿子的位置,结点一般表示为:

数据	儿子 ₁	儿子 ₂	...	儿子 _n
----	-----------------	-----------------	-----	-----------------

通常树的结点生的儿子数不同,这样就给表示上带来问题。如果各结点在内存中用定长来表示,就得以儿子数最多的结点所占内存单元数作为标准,这样对算法是简单的,但会浪费很多内存单元,极不经济。如果以各个结点实际占用内存数来表示树(即用不定长方法),这样内存是省了,但是算法很复杂。

所以树的存储表示大都先转化成二叉树。在数据结构和算法分析中,读者将会看到它的优越性。下面我们介绍将任意树化为二叉树的一般步骤:

- (1) 从根开始,保留每个双亲同其最左边的儿女的连线,撤销与别的儿女的连线。
- (2) 兄弟间加线连接。
- (3) 以树的主根为圆心,将整棵树顺时针转 45° 。

例 5-26 图 5-42(a)按上述三个步骤变换后,得到二叉树,如图 5-42(c)所示。

这是树与二叉树的自然对应。对于森林,也可以用二叉树表示,其步骤是:

- (1) 把每棵树的根加线连接。
- (2) 再把每棵树化为二叉树。
- (3) 顺时针旋转 45° 。

如图 5-43 是具有两棵子树的森林,执行上述(1)和(2)两步后,得到图 5-44,执行第(3)步后,得到图 5-45。这就是森林和二叉树之间的自然对应。

遍历森林的方法也可以导出,将森林用二叉树表示后,就可以定义遍历森林的先根次序和后根次序。方法如下:

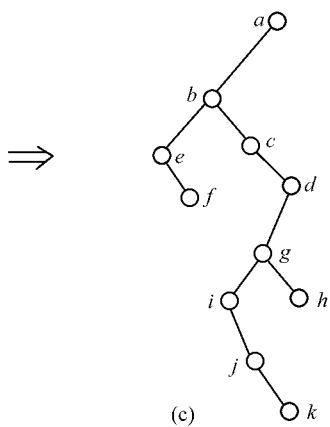
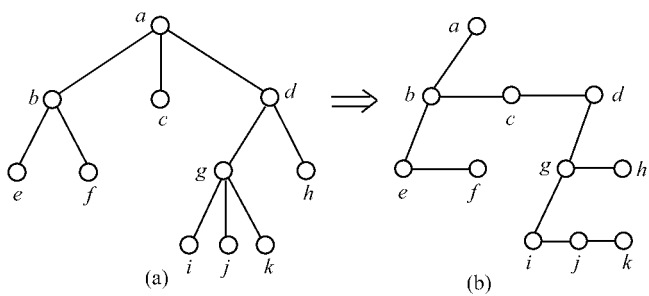


图 5-42 例 5-26 图示

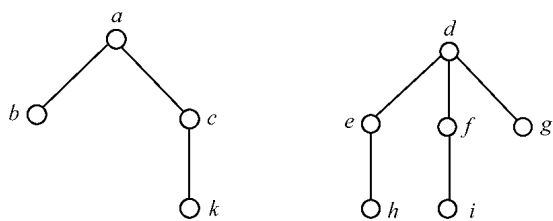


图 5-43 例 5-27 图示之一

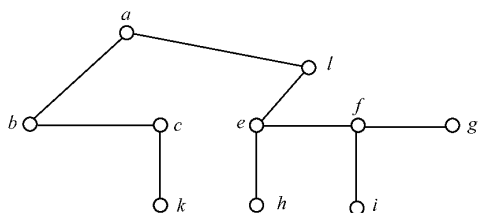


图 5-44 例 5-27 图示之二

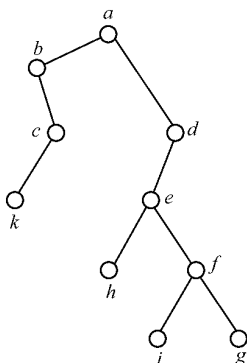


图 5-45 例 5-27 图示之三

- | | |
|------|---|
| | { 访问头一棵树的根
遍历头一棵树的子树(按先根次序法)
遍历剩下的树(按先根次序法) |
| 先根次序 | |
| | |
| | { 遍历头一棵树的子树(按后根次序法)
访问头一棵树的根
遍历剩下的树(按后根次序法) |
| 后根次序 | |
| | |

先根次序和后根次序的定义十分精确地刻划了树与二叉树的自然对应,我们把这些定义和遍历二叉树的定义作比较就会发现,在先根次序下遍历一个森林,恰好等同于在先根次序下遍历相应的二叉树,在后根次序下遍历一个森林,恰好等同于在中根次序下遍历相应的二叉树。尤其幸运的是,树的后根次序对应二叉树的中根次序,而不是后根次序,这就避免了后根次序遍历二叉树的方法,而后者是比较麻烦的。

例 5-27 图 5-43 在先根次序下得到:

→ *abckdehfig*

而图 5-45 在先根次序下得到:

→ *abckdehfig*

所以两个序列完全相同。

另一方面,图 5-43 在后根次序下得到:

$\rightarrow bkcaheifgd$

而图 5-45 在中根次序下得到:

$\rightarrow bkcaheifgd$

这说明按后根次序遍历树及按中根次序遍历二叉树,其效果完全一样。

这从一个方面说明了树可用二叉树表示的理由,因为人们可以找到它们的自然对应。

3. 生成树和最小生成树

定义 5-16 设 G 是一个连通图, G 的一棵生成树 T_G 是包含 G 的所有结点的示图的树。

给出一个连通图 G ,怎样求它的生成树呢?可以按下面的算法进行:

- (1) 令 G 是 G_1 ,置 $i=1$;
- (2) 若 G_i 无回路,则 $T_G=G_i$,生成树已找到;
- (3) 否则,在 G_i 中消去回路 C_i 的一条边,得到图 G_{i+1} ,因为 C_i 是 G_i 中的一条回路,所以 G_{i+1} 包含了 G_i 的所有结点, G_i 是连通的,故 G_{i+1} 也是连通的;
- (4) $i=i+1$ (即 i 增加 1),然后返回到(2)。

其流程图如图 5-46 所示。

例 5-28 设有一个图 G ,如图 5-47(a)所示,求它的生成树。

图中 G_2 、 G_3 、 G_4 是求 G 的生成树的中间过程, $G_5=T_G$ 就是所求的生成树。

由于每次迭代过程中, G_i 中的 C_i 及相应的边 e_i 取法不是惟一的,所以最后求得的生成树 T_G 一般说来也不是惟一的,但对于一个 (n, m) 连通图来说,消去的边数是恒定

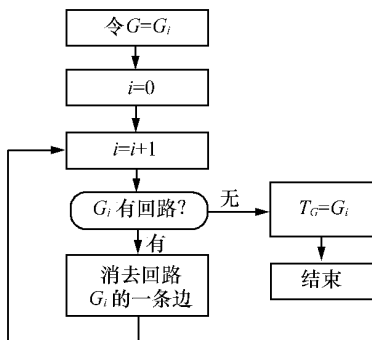


图 5-46 生成树求找的算法流程图

的,由于得到的 T_G 是 $(n, n-1)$ 图,因此消去的边数是 $m - (n-1)$ 条。
 $m - (n-1)$ 这个数称为 (n, m) 图的秩。除去的每条边称为 G 的弦。譬如说,上面介绍过的图 5-47 是 $(6, 9)$ 图,因此除去的边是 $9 - (6-1) = 4$ 。

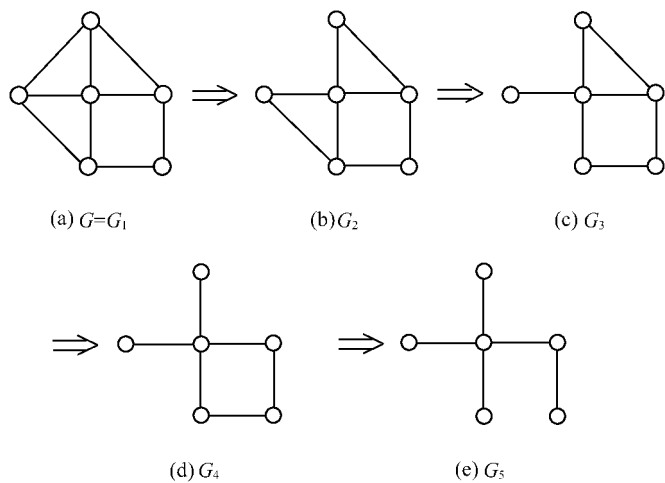


图 5-47 一个求解生成树的图示

对于带权的图,不仅要求出其生成树,而且求出的生成树各条边权之和为最小,这就是所谓的最小生成树的概念。

定义 5-17 设 G 是带权的连通图, G 的最小生成树是 G 的一棵生成树,而且它的边的权之和比 G 的所有别的生成树的边的权之和都小。

只要在前述算法基础上稍加改动,就可以找到求最小生成树的算法。即每次迭代时,在上述算法的第(3)步消去 C_i 中权最大的边。

例 5-29 设连通图 G 各条边的权如图 5-48(a) 所示,其最小生成树如图 5-48(b) 所示,权之和是 39。

下面再介绍求最小生成树的另外一种算法。

设 $G=(V, E)$ 是一个具有 n 个 $(n \geq 2)$ 结点的完全图,由 $G_i=(V, E_i)$ 构造 G 的最小生成树 T_G 的步骤如下:

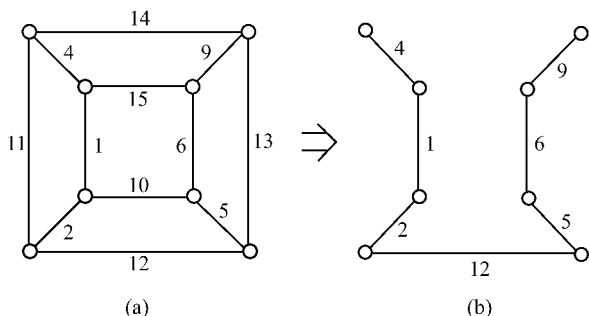


图 5-48 例 5-29 图示

(1) 置 $i=1$, 令 G_i 的边取的是 G 中权最小的边, 譬如说这边是 e_i

(2) 若 G_i 已是 G 的生成树, 则令 $T_G=G_i$ 。

(3) 否则, 在 $E-E_i$ 中找一条最小权的边, 加到 G_i 中, 且不形成回路, 得到 $G_{i+1}=(V, E_{i+1})$ 图。

(4) $i=i+1$, 然后返回到 (2)。

当 G_i 变成一个 G 的生成树时, 这个算法一定在 $i=n-1$ 时执行完毕。因此由这个算法生成的生成树一定是 G_{n-1} 图, 而且可以证明 G_{n-1} 就是要求的 G 的最小生成树, 其证明过程从略。

求一个图 G 的最小生成树是很有实用价值的。

例 5-30 假设我们想要修筑五个城市连接的铁路网, 使其造价尽可能小。又设任意两个城市之间铁路造价如下 (以亿元为单位):

$$w(v_1, v_2) = 4, w(v_1, v_3) = 7$$

$$w(v_1, v_4) = 16, w(v_1, v_5) = 10$$

$$w(v_2, v_3) = 13, w(v_2, v_4) = 8$$

$$w(v_2, v_5) = 7, w(v_3, v_4) = 3$$

$$w(v_3, v_5) = 10, w(v_4, v_5) = 12$$

按照上述造价, 先构造一个完全图 G , 如图 5-49(a) 所示, 因此要修筑使造价最小的铁路网, 便变成求 G 的最小生成树 T_G , 按上述

方法,我们求图 5-49 中 G 的生成树。

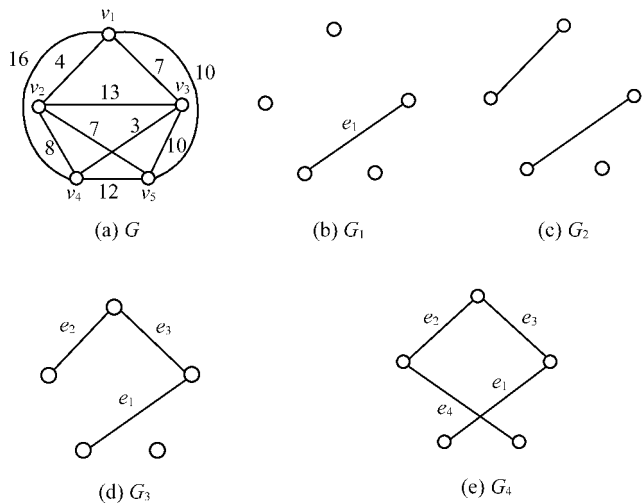


图 5-49 例 5-30 图示

上图 G_1 、 G_2 和 G_3 是求 G 的最小生成树的中间过程。 $G_4 = T_G$ 是最后求得的生成树,其中 e_1 、 e_2 、 e_3 、 e_4 表示按照算法添边的次序。最小生成树 T_G 之权是 21(单位:亿元)。

5.9 有 向 图

有向图在计算机中有着广泛的应用,大家最熟悉的例子是程序流程图,它是一种有向图。由于我们已较详细地研究了无向图,它的不少概念可以引伸到有向图,所以这里主要介绍它的一些基本性质。

1. 基本概念

定义 5-18 一个有向图 D 由结点集合 $V = \{v_1, v_2, \dots, v_n\}$ 和边集 $E \subseteq V \times V$ 所组成。

如果要强调点集和边集两部分,写成 $D = (V, E)$ 。需要特别指

出的是,有向图的边是由结点的有序偶组成的, E 中的边具有方向性。为了与无向图中的无向边区别起见,我们在此节用 $\langle a, b \rangle$ 表示有序偶,即有向边。并称 a 为 $\langle a, b \rangle$ 的始点, b 为 $\langle a, b \rangle$ 的终点。有向边画在平面上时,它的方向用箭头标出。

例 5-31 一个具有四个结点八条边的有向图如图 5-50 所示。

其中 e_3 称为环。 e_2 和 e_3 是连接 v_1 和 v_3 的同方向的两条边,称为平行边,显然它与平面几何上的平行边是完全不同的概念。但 e_5 和 e_6 是两条不同的边,所以是非平行边。具有平行边的图称为重图,无环非重图的有向图称为简单有向图。下面主要研究简单有向图。

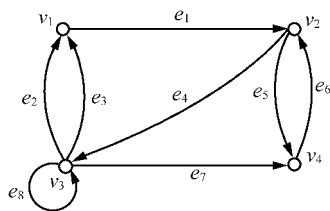


图 5-50 一个有向图

对图中的结点 v ,以 v 为始点的边数称为 v 的引出次数,以 v 为终点的边数称为 v 的引入次数, v 的引入、引出次数之和称为 v 的全次数,图的各结点的引入次数之和恰好等于各结点的引出次数之和,并且恰好等于图的边数。

关于有向图的子图、真子图和生成子图的术语与无向图的子图、真子图和生成子图有同样的含义。

这里,必须对有向通路的概念给予定义。

我们把有向图中有向边的序列:

$$\langle v_{i_0}, v_{i_1} \rangle, \langle v_{i_1}, v_{i_2} \rangle, \dots, \langle v_{i_{n-1}}, v_{i_n} \rangle$$

称为从 v_{i_0} 到 v_{i_n} 长度为 n 的有向通路,记以:

$$P = (\langle v_{i_0}, v_{i_1} \rangle, \langle v_{i_1}, v_{i_2} \rangle, \dots, \langle v_{i_{n-1}}, v_{i_n} \rangle)$$

在上下文不会引起混淆的情况下,为了书写方便,有时可简写为:

$$P = (v_{i_0}, v_{i_1}, \dots, v_{i_n})$$

或:

$$P = v_{i_0} v_{i_1} \dots v_{i_n}$$

或:

$$P = (e_{i_1}, e_{i_2}, \dots, e_{i_n})$$

注意 P 中的边(或点)均可出现多次。

有了有向通路的概念,那么无向图中的简单通路和简单回路、基本通路和基本回路、短程线和距离等定义均可以引伸到有向图中,但要把上述定义中的无向通路转换成有向通路,读者可以给出它们相应的定义。

定理 5-22 具有 n 个结点的简单有向图,任一条基本通路的长度小于 n 。

其证明方法与无向图中的定理 5-4 相似。

关于连通图的概念,在有向图中更为复杂一些。我们先给出两个结点的连通性的概念。

若在有向图 D 中存在从 v_i 到 v_j 的有向通路,则称 v_i 到 v_j 是连通的。

例如图 5-51 的四个图(a)、(b)、(c)和(d),它们各有其特点,根据其不同的特点,我们引出关于图连通性的有关术语。

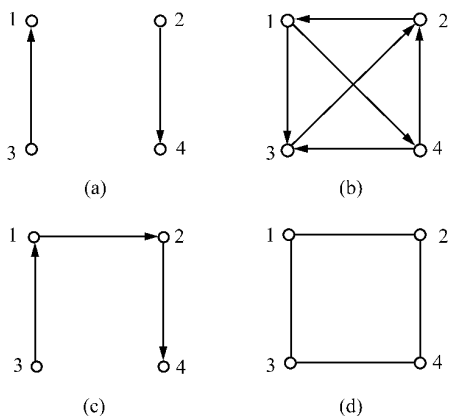


图 5-51 四种图的连通性

其中(a)是非连通图;(b)的每对结点均互相连通,称(b)为强连通图;(c)不是每对结点均互相连通,如从 2 到 1 就不连通,但从单方向看是连通的,这类图称为单向连通图;(d)中 2 和 3、1 和 4 都不存在通路,但去掉边的方向后从无向图观点看是连通图,这类图称为弱连通图。这些概念十分重要,现给出它们的确切定义:

定义 5-19 设有向图 D , 如果每对结点都是互相连通的, 则 D 是强连通图; 如图中每对结点至少有一个方向是连通的, 则称 D 是单向连通图; 如果 D 中至少有一对结点不满足单向连通, 但去掉边的方向后从无向图观点看是连通图, 则 D 是弱连通图。

显然, 它们三者具有如图 5-52 所示的关系。

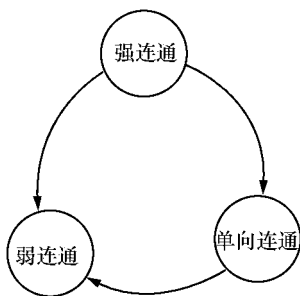


图 5-52 三种连通间关系

有向图与关系是密切联系在一起的, 令 $D=(V, E)$, 是简单有向图, 则 $E \subseteq V \times V$, 因此 E 是 V 上的二元关系; 反之, 如果 R 是 V 上的一个关系, 则 $D=(V, R)$ 是简单有向图。因此, 在一个集合上的关系和图的含义是相同的。

2. 有向图的矩阵

和无向图相似, 对于任何一个有向图, 我们可以用矩阵来表示其关系, 一个图的关系矩阵也称相邻矩阵。

设有向图 $G=(V, E)$, $V=\{v_1, v_2, \dots, v_n\}$, 则 G 的相邻矩阵 $M=[a_{ij}]_{n \times n}$, 其中

$$a_{ij} = \begin{cases} 1 & \text{如果 } \langle v_i, v_j \rangle \in E \\ 0 & \text{如果 } \langle v_i, v_j \rangle \notin E \end{cases}$$

例 5-32 图 5-53 及其关系矩阵如下:

$$\begin{matrix} & \begin{matrix} a & b & c & d \end{matrix} \\ \begin{matrix} a \\ b \\ c \\ d \end{matrix} & \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} \end{matrix}$$

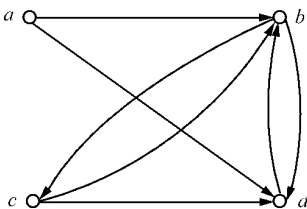


图 5-53 例 5-32 图示

图的矩阵运算常用来判定图的连通性, 这主要利用下述定理。

定理 5-23 设具有 n 个结点的有向图 D 的矩阵是 M , 则 $M^n = [a_{ij}]$ 中的 a_{ij} 表示从结点 v_i 到 v_j 长度是 n 的通路数目。

其证明与无向图中的定理 5-7 相似, 读者自己给予证明。

我们仍以例 5-32 来说明此定理。我们要求从 a 到 d 长度分别为 2、3 和 4 的通路数目, 于是求 M^2 、 M^3 和 M^4 。先求 M^2 :

$$M^2 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

所以从 a 到 d 长度为 2 的通路有 1 条, 这条通路是 $(\langle a, b \rangle, \langle b, d \rangle)$ 。

再求 M^3 :

$$M^3 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 2 & 1 & 2 \\ 0 & 1 & 2 & 2 \\ 0 & 2 & 1 & 2 \\ 0 & 2 & 0 & 1 \end{bmatrix}$$

所以从 a 到 d 长度为 3 的通路有 2 条, 这两条通路是:

$(\langle a, b \rangle, \langle b, c \rangle, \langle c, d \rangle)$

$(\langle a, d \rangle, \langle d, b \rangle, \langle b, d \rangle)$

再求 M^4 :

$$M^4 = \begin{bmatrix} 0 & 2 & 1 & 2 \\ 0 & 1 & 2 & 2 \\ 0 & 2 & 1 & 2 \\ 0 & 2 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} =$$

$$\begin{bmatrix} 0 & 3 & 2 & 3 \\ 0 & 4 & 1 & 3 \\ 0 & 3 & 2 & 3 \\ 0 & 1 & 2 & 2 \end{bmatrix}$$

所以从 a 到 d 长度为 4 的通路有 3 条,这 3 条通路是:

$(\langle a, b \rangle, \langle b, c \rangle, \langle c, b \rangle, \langle b, d \rangle)$

$(\langle a, d \rangle, \langle d, b \rangle, \langle b, c \rangle, \langle c, d \rangle)$

$(\langle a, b \rangle, \langle b, d \rangle, \langle d, b \rangle, \langle b, d \rangle)$

读者可以进一步分析 M^2 、 M^3 、 M^4 上各元素的意义。

定理 5-24 设 M 是 D 的矩阵,结点有 n 个,令:

$$C = M + M^2 + \cdots + M^{n-1}$$

则 D 是强连通当且仅当 C 除主对角线外无元素等于零。

证明: C 的 (i, j) 元素是零当且仅当 $M, M^2, \cdots, M^{n-1}$ 的 (i, j) 记录都是零。这意味着不存在从 v_i 到 v_j 长度小于或等于 $n-1$ 的通路,因此不存在从 v_i 到 v_j 的简单通路。因此 D 是强连通当且仅当 C 的 (i, j) 记录是非零 ($i \neq j$)。

3. 无向图化为有向图的方法

我们知道,一个连通有向图转变为无向图很简单,只要将每条有向边用无向边代替即可,而且有向图转换成的无向图是惟一的。我们感兴趣的而且很有实用价值的是如何将一个连通无向图转变成有向图,一般说来这是比较复杂的。为了保证转变成的有向图是连通图,就不是简单地用有向边代替无向边,而且转变成的有向图不一定是惟一的。

下面我们介绍将无向图转变成有向图的一种算法。

$v_n\}$ 。把 G 转变为连通有向图的步骤如下:

(1) 令 $V_1 = \{v_1\}, i=1, G=G_i$ 。

(2) $V=V_i$ 吗？

如果 $V=V_i$, 则将 G_i 中剩下的所有无向边任意加上箭头即可, G_i 就是要求的有向图。

如果 $V \neq V_i$, 则:

(3) 在 G_i 中任意取一条边 (v_{i_0}, v_{i_1}) , 使得 $v_{i_0} \in V_i, v_{i_1} \in V - V_i$ 。由于 G 是连通图, 这边必定存在。找一条基本回路或基本通路。

$$a_i = (v_{i_0}, v_{i_1}, \dots, v_{i_{l-1}}, v_{i_l})$$

其中 $v_{i_l} \in V_i$, $\{v_{i_1}, v_{i_2}, \dots, v_{i_{l-1}}\} = \widehat{V}_i \subset V - V_i$, 将 a_i 的每条边上加箭头, 使它成为一条有向通路, 即 $(\langle v_{i_0}, v_{i_1} \rangle, \langle v_{i_1}, v_{i_2} \rangle, \dots, \langle v_{i_{l-1}}, v_{i_l} \rangle)$, 然后把 G_i 和加了箭头的通路 a_i 一起用 G_{i+1} 表示, 令 $V_{i+1} = V_i \cup \widehat{V}_i$. 由于属于 V_i 的每对结点用有向通路表示

了($V_1 = \{v_1\}$ 自然是真的)。因此每个 $v \in V_i$ 和 G_{i+1} 中的 $\tilde{v} \in \tilde{V}_i$, 存在有向通路:

$v, \dots, v_{i_0}, \dots, \tilde{v}$ 和 $\tilde{v}, \dots, v_{i_l}, \dots, v$ 这样属于 V_{i+1} 中的每对结点连成一条有向通路。

(4) $i=i+1$ (即 i 增中 1), 返回到(2)。

例 5-33 设某一个城市的街道如图 5-54 所示,该城市街道狭窄,车辆甚多,为保证行车安

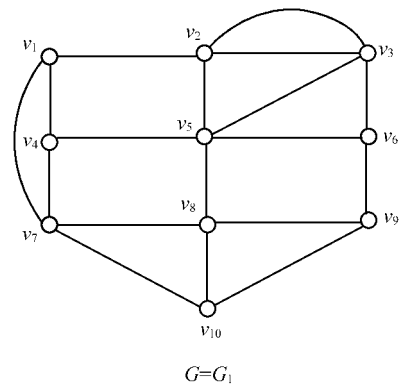
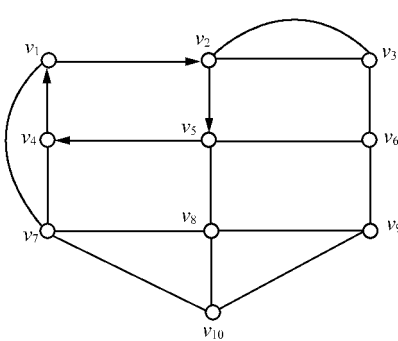


图 5-54 例 5-33 图示之一

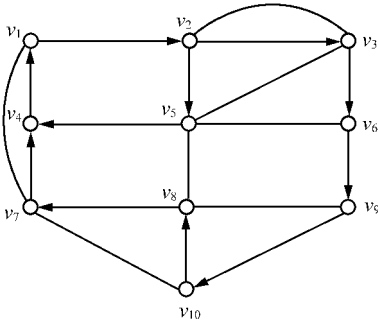
全和提高行驶速度,该市政府规定车辆只准单向行驶,问怎样规定方向,才能保证车辆从某一地点开到该城市任意其他地点?这个问题实际上是要把图 5-54 改变成一个连通有向图。我们按照上述算法给它规定方向,其中图 5-55、图 5-56 是中间过程,图 5-57 就是最后

求得的有向图。



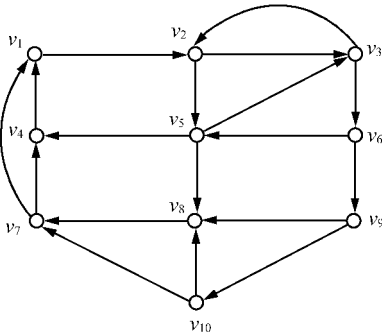
$V_1 = \{v_1\}$
 $a_1 = v_1 v_2 v_5 v_4 v_1$ (有向)
 $V_1 = \{v_2, v_5, v_4\}$
此时 $G = G_2$
但是 $V_2 = V_1 \cup V_1 \neq V$

图 5-55 例 5-33 图示之二



$V_2 = V_1 \cup \tilde{V}_1 = \{v_1, v_2, v_5, v_4\}$
 $a_2 = v_2 v_3 v_6 v_9 v_{10} v_8 v_7 v_4$ (有向)
 $\tilde{V}_2 = \{v_3, v_6, v_7, v_8, v_9, v_{10}\}$
此时 $G = G_8$
而 $V_3 = V_2 \cup \tilde{V}_2 = V$

图 5-56 例 5-33 图示之三



由于 $V = V_3$ ，所以将余下的无向边全部改变成有向边，其方向此时可任意指定。此图就是要求的有向图

图 5-57 例 5-33 图示之四

习 题 五

无向图部分

5.1 设 $V = \{u, v, w, x, y\}$, 画出图 $G = (V, E)$

其中:

$$(1) E = \{(u, v), (u, x), (v, w), (v, y), (x, y)\}$$

$$(2) E = \{(u, v), (v, w), (w, x), (w, y), (x, y)\}$$

再求各个结点的次数

5.2 设有一个无向图 G 如图 5-58 所示, 问它是否与图 5-25(g) 同构?

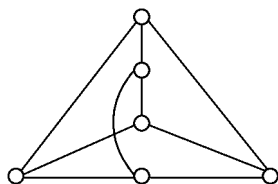


图 5-58

5.3 设 G 是具有 4 个结点的完全图。

(1) 写出 G 的所有子图。

(2) 写出 G 的所有生成子图。

(3) G 的所有互不同构的子图有多少?

5.4 画出具有 8 个结点的两个 3 次规则图。

5.5 分别画出 $K_{2,6}$ 和 $K_{3,4}$ 图。

5.6 画出一个重图 G , 使它的相邻矩阵为

$$A = \begin{bmatrix} 1 & 3 & 0 & 0 \\ 3 & 0 & 1 & 1 \\ 0 & 1 & 2 & 2 \\ 0 & 1 & 2 & 0 \end{bmatrix}$$

5.7 有一个图如图 5-59 所示。

(1) 从 a 到 h 的所有基本通路。

(2) 从 a 到 h 的所有简单通路。

(3) 从 a 到 h 的距离。

5.8 图 5-60 中哪个有欧拉通路,哪个有欧拉回路,哪个有哈密顿通路,哪个有哈密顿回路。

5.9 证明定理 5-3。

5.10 设图 G_1 和 G_2 的相邻矩阵分别为 A_1 和 A_2 。

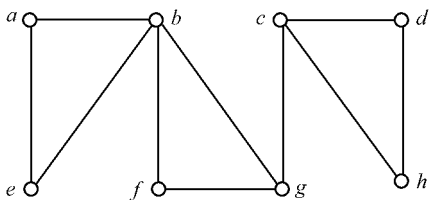


图 5-59

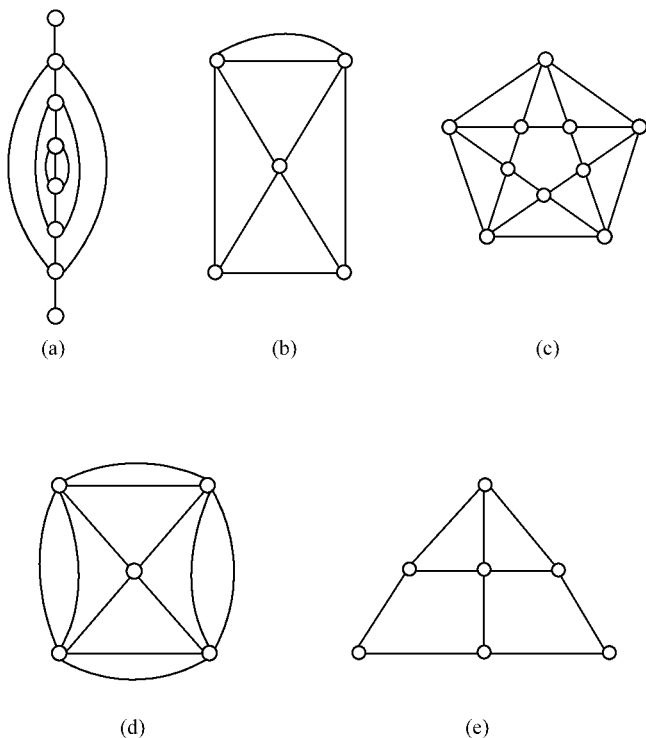


图 5-60

(1) 求 A_1^l ($l=1,2,\dots,6$) 及 A_2^l ($l=1,2,\dots,7$)。

(2) 在 G_1 内列出每两个结点之间的距离。

(3) 列出 G_1 和 G_2 中的所有基本回路。

$$\mathbf{A}_1 = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix} \quad \mathbf{A}_2 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

5.11 假定一个图 G 是二分图,试说明可以规定 G 的结点的一种次序,使它的相邻矩阵 A 具有下面的形式:

$$\mathbf{A} = \begin{bmatrix} 0 & \mathbf{B} \\ \mathbf{C} & 0 \end{bmatrix}$$

5.12 利用四种颜色,对图 5-61 着色,使得相邻区域的颜色均不同。

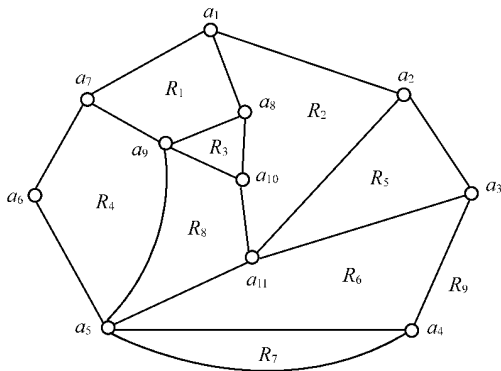


图 5-61

5.13 构造图 5-61 的对偶图。

5.14 设有一棵树,

(1) 有两个结点其次数为 2,一个结点其次数为 3,三个结点其次数为 4。问它有几个次数为 1 的结点?

(2) 又如果有 n_2 个结点其次数为 2, n_3 个结点其次数为 3, $\dots$, n_k 个结点其次数为 k 。问它有几个结点其次数为 1?

5.15 尽可能多地画出具有 5 个结点的树, 而且均不互相同构。

5.16 对于图 5-62, 求它的最小生成树。

5.17 证明下面三个命题是等价的:

(1) G 是 2 色图。

(2) G 是二分图。

(3) G 的每个基本回路的长度是偶数。

5.18 设有一个代数表达式如下:

$$\frac{(3x - 5y)^4}{a(2b + c^2)}$$

(1) 画出这个代数表达式相应的根树。用“ $\uparrow$ ”表示乘方, “ $*$ ”表示乘, “ $/$ ”表示除。

(2) 分别用先根次序法、中根次序法和后根次序法重写其代数表达式。

有向图部分

5.19 设有向图 D 如图 5-63 所示,

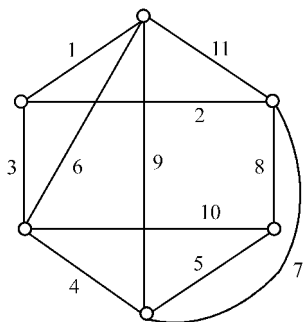


图 5-62

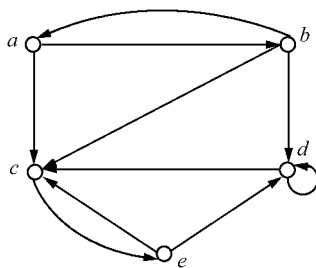


图 5-63

(1) 求每个结点的引入次数和引出次数。

(2) 求从 a 到 d 的所有基本通路。

- (3) 求它的相邻矩阵 M_D 。
- (4) 求从 a 到 c 长度小于或等于 3 的通路数。
- (5) D 是强连通、弱连通还是单向连通的？

5.20 令 D 是具有结点 v_1, v_2, v_3, v_4 的有向图, 它有矩阵表示如下:

$$M = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

- (1) 画出这矩阵表示的有向图 D 。
- (2) 求从 v_1 到 v_1 长度是 3 的回路数以及从 v_1 到 v_2 、从 v_1 到 v_3 、从 v_1 到 v_4 长度是 3 的通路数。
- (3) D 是单向连通的还是强连通的？

5.21 设有一个城市的街道图如图 5-64 所示, 在每条街道上规定一个方向, 使它成为一个有向连通图。

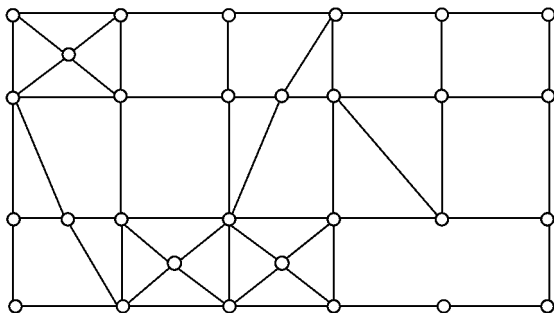
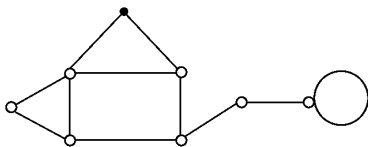


图 5-64

- 5.22 图 $G(V, E)$ 是简单有向图, 邻接矩阵刻画下列哪种关系?
() (邻接矩阵也称相邻矩阵)
- A. 点与点 B. 点与边 C. 边与点 D. 边与边
- 5.23 给定平面图 G 如下, 平面图的面数是()

- A. 6
B. 5
C. 8
D. 9



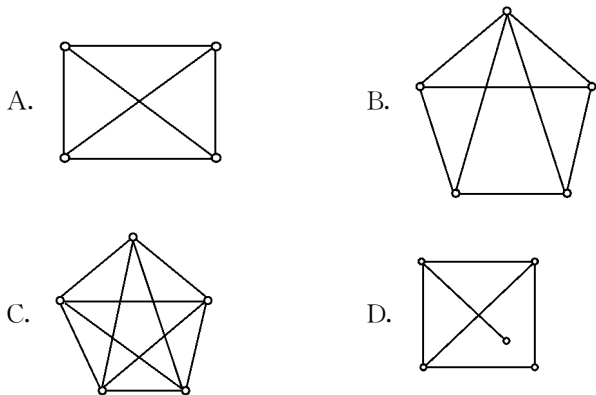
5.24 一棵树有 2 个 4 度结点, 3 个 3 度结点, 其余结点都是叶子, 则叶子结点的数目为()

- A. 9 B. 8 C. 7 D. 10

5.25 G 为 (n, m) 图, 其中有 n_k 个结点的度为 k , 其余结点的度均为 $k+1$, 试证明 $n_k = (k+1)n - 2m$ (其中 n 为图 G 的结点数目, m 为边数)。

5.26 试画出 K_4 (4 阶无向简单完全图) 的所有非同构的生成子图。

5.27 下列图中不是平面图的是()



5.28 对树 T , 下列正确的结论为()

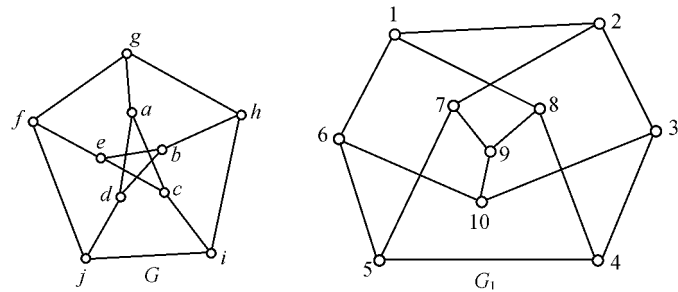
- A. 树不是连通图 B. 存在回路
C. 是没有回路的连通图 D. 结点数和边数相等

5.29 具有 4 个结点非同构的有根树有: _____

5.30 G 是 n 个结点、 m 条边的无向简单图, v 是度为 k 的结

点,则 $G-v$ (G 中去掉 v 结点的图) 中有 _____ 个结点, _____ 条边。

5.31 证明下面图 G 和 G_1 同构。



5.32 $(d_1, d_2, \dots, d_n)$ 表示 n 个结点的图的各结点的度, 即 $\deg(V_i) = d_i$ 若有简单图与之对应, 则称其为可解的。

试说明如下数据是否可解, 并图示之。

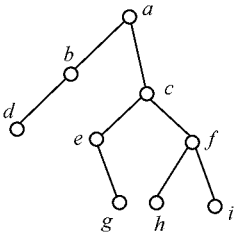
- (1) $(1, 1, 1, 2, 3)$
- (2) $(3, 3, 3, 3)$
- (3) $(2, 3, 3, 4, 5, 6)$

5.33 对于一个连通的平面图 G , 设 V 代表结点数目, e 代表边数, r 代表平面图的区域数目, 下面成立的结论是 ()

- A. $v + r = e + 2$
- B. $v - e + r = 3$
- C. $e = v + r$
- D. $v - e + r = 5$

5.34 已知二叉树先根遍历的结果是 ()

- A. $abdcegfhi$
- B. $abcdefghi$
- C. $dbaegchfi$
- D. $dbagehifca$



5.35 有 33 个电灯, 拟公用一个电源, 至少需 5 插头的接线板个数为 ()

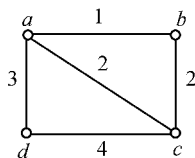
A. 7 B. 8 C. 9 D. 14

5.36 G 为 n 个结点的连通图, G 的生成树 T 的权为 _____; 若 T 为 _____, 则称 T 为最小生成树。

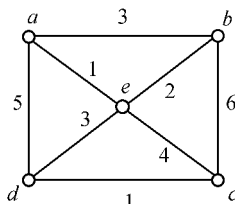
5.37 5 个结点可以构成无向树。—。 —。 —。 —, 与它非同构的无向树有 _____ 和 _____。

5.38 图 G 有 9 个结点, 度不是 5 就是 6, 试证 G 中至少有 5 个 6 度结点或 6 个 5 度结点。

5.39 求下面带权图的最小生成树。



(1)



(2)

5.40 如果对一个连通平面图各个区域着色, 使得相邻的区域有不同的颜色, 那么所用颜色的种数可以不多于()

A. 2 种 B. 3 种 C. 4 种 D. 5 种

5.41 有 $n(n \geq 3)$ 个结点, m 条边的连通简单图是平面图的必要条件是()

A. $m \leq 3n + 6$ B. $m \geq 3n - 6$
C. $n \leq 3m - 6$ D. $m \leq 3n - 6$

5.42 具有 4 个结点的非同构的无向树的数目为()

A. 2 个 B. 3 个 C. 4 个 D. 5 个

5.43 由一个孤立点构成的图称为 _____; 简单图中不包含 _____。

5.44 设 $G=(V, E)$ 是 n 个结点、 m 条边的连通图, 要确定 G 的一棵生成树, 必须删去 G 中的边数为()

A. $n-m-1$ B. $n-m+1$

C. $m-n+1$ D. $m-n-1$

5.45 设图 G 是有 n 个结点、 m 条边的欧拉图, n, m 有关系 ()

A. $n=m$

B. n, m 的奇偶性必相同

C. n, m 的奇偶性必相反

D. n, m 的奇偶性可以相同也可以相反

5.46 $G=(V, E)$ 是无向连通图, 若 $|V|=100, |E|=100$, 则从 G 中能找到 _____ 条回路。

5.47 如果一个图的每个结点的次数(度)都是 k , 则称该图为 k 次正则图(k 次正则图)。

试证明 3 次正, 则图必有偶数个结点。

5.48 无向图 $G=(V, E), V=\{v_1, v_2, \dots, v_6\}$

$E=\{(v_1, v_2), (v_2, v_2), (v_2, v_4), (v_4, v_5), (v_3, v_4), (v_1, v_3), (v_3, v_1)\}$

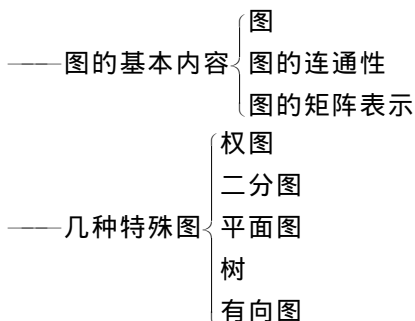
(1) 图示 G ;

(2) 判定 G 是否为简单图;

(3) 求出图中各结点的度。

“图论”复习提纲

1. 主要内容



2. 复习重点

——图的基本概念与图的连通性。

——树的基本概念、树的性质、二叉树及生成树。

3. 图的基本概念

——图:图由结点及边所组成,记以 $G=\langle V, E \rangle$ 。

——结点与结点集:结点是图的基本概念,而图由若干结点构成的集合 $V=\{v_1, v_2, \dots, v_n\}$ 所组成。

——边与边集:边是图中结点的无序偶,而图由若干边构成的集合 $E=\{e_1, e_2, \dots, e_m\}$ 所组成。

——有向图与无向图:边带方向的图称有向图;边不带方向的图称无向图。

——相邻点与相邻边:连接同一边的两个结点称相邻点;连接同一个点的两个边称相邻边。

——环:连接同一点的边称环。

——平行边与重图:两个结点间有一条以上边称平行边,具有平行边的图称重图。

——简单图:无环无平行边的图。

——结点次数与孤立点:结点相邻边数称次数,记以 $\deg(v)$;次数为 0 的结点称孤立点。

—— K 次数规则图:图中每个结点次数均为 K 。

——奇次结点与偶次结点:结点次数为奇数与偶数。

——次数性质: (n, m) 图有 $\sum_{i=1}^n \deg(v_i) = 2m$ 。

—— (n, m) 图:具有 n 个结点 m 条边的图。

——平凡图: $(1, 0)$ 图。

——完全图:图中每两个结点间均有边相连,此时, (n, m) 图中 $m = C_n^2$ 。

——子图: $G=(V,E)$ 与 $G'=(V',E')$,若 $V'\subseteq V, E'\subseteq E$,则称 G' 是 G 的子图。

——真子图: $G=(V,E)$ 与 $G'=(V',E')$,若 $V'\subset V, E'\subset E$,则称 G' 是 G 的真子图。

——生成子图: $G=(V,E)$ 与 $G'=(V',E')$,若 $V'=V, E'\subset E$,则称 G' 是 G 的生成子图。

4. 图的连通性

——通路:两结点间有边的序列相连。

——通路长度:通路中边数。

——回路:通路中两结点(起点和终点)相同。

——简单通路:通路中每条边只经过一次。

——简单回路:回路中每条边只经过一次。

——基本通路:通路中每个点只经过一次。

——基本回路:回路中每个点只经过一次。

——结点连通:两结点间有通路。

——连通图:图中任两结点间均有通路。

——连通子图:图中子图是连通的。

——独立子图:图中任一连通子图,它与图中其他连通子图不相连。

——短程线:两结点间长度最短之通路。

——距离:两结点间短程线长度,记以 $d(v_i, v_j)$ 。

——短程线性质: $d(v_i, v_j) \leq n-1$ 。

——欧拉回路:经过连通图每条边一次的回路并记以 E 回路。

——欧拉通路:经过连通图每条边一次的通路并记以 E 通路。

——欧拉图:具有 E 回路的图,记以 E 图。

——欧拉图性质: G 是 E 图 $\Leftrightarrow$ 每个结点次数为偶数。

——哈密尔顿回路:经过图每个结点一次的回路并记以 H 回路。

——哈密尔顿通路: 经过图每个结点一次的通路并记以 H 通路。

——哈密尔顿图: 具有 H 回路的图并记以 H 图。

5. 图的矩阵表示

——相邻矩阵: $G=(V, E)$ 的相邻矩阵 $A=[a_{ij}]$ 是 $m \times m$ 阶矩阵:

$$a_{ij} = \begin{cases} 1, & \text{当 } (v_i, v_j) \in E \\ 0, & \text{当 } (v_i, v_j) \notin E \end{cases}$$

——相邻矩阵性质: G 的相邻矩阵 A 有:

• $A^l (l=1, 2, \dots, n)$ 的第 (i, j) 个元素是由 V_i 到 V_j 的长度等于 l 的通路数。

- $d(v_i, v_j)$ 是使得 A^l 的第 (i, j) 个元素为非零的最小整数 l 。
- $a_{ij}^{(l)}$ 表示开始并结束于 v_i 长度为 l 的回路数。
- $a_{ij}^{(l)}=0$ 表示由 v_i 到 v_j 无长度为 l 的通路存在。
- 对 $A+A^2+\dots+A^{m-1}=\tilde{A}$, 连通图 $\Leftrightarrow \tilde{A}$ 除对角线外全是非零元素。

6. 权图、最小权通路与最小权回路

——权图基本概念。

- 权图: 图中边赋予有关非负数据 ω 的图。
- 通路的权: 通路 P 中各边权之和 $\omega(P) = \sum_{i \in P} \omega(e_i)$ 。
- 回路的权: 回路 C 中各边权之和 $\omega C = \sum_{i \in C} \omega(e_i)$ 。
- 最小权通路: 从 v_i 到 v_j 中权为最小的通路。
- 最小权回路: v_i 的权为最小的回路。
- 权图矩阵表示: 权图 G 的矩阵 $D=[d_{ij}]$:

$$d_{ij} = \begin{cases} \omega(v_i, v_j), & (v_i, v_j) \in E \\ \infty, & (v_i, v_j) \notin E \\ 0, & v_i = v_j \end{cases}$$

——求解最小权通路算法：

(1) $D^{(0)} = D$ 。

(2) 从 $D^{(0)}$ 起构造 $D^{(1)}, D^{(2)}, \dots, D^{(n)}$ ：

可由 $D^{(K-1)}$ 构造 $D^{(K)}$ 如下：

$$d_{ij}^{(k)} = \min\{d_{ij}^{(k-1)}, d_{ik}^{(k-1)} + d_{kj}^{(k-1)}\} \quad (k \neq i, j)$$

计算从 $k=1$ 起, i, j 从 1 到 n , 然后 $k+1$, 反复进行, 直到 $k=n$ 为止。

(3) $D^{(n)}$ 中 $d_{i,j}^{(n)}$ 即为从 v_i 到 v_j 的通路最小权。

——最小权 H 回路与 E 回路

- 货郎担问题: 最小权 H 回路。
- 货郎担问题解: 仅存在一种相似解。
- 邮路问题: 最小权 E 回路。
- 邮路问题求解: 邮路 C 为最小权 $\Leftrightarrow$ 每边最多重复一次, 且在图中每回路上重复边的权之和小于回路权的一半。

7. 二分图

——二分图基本概念

- 二分图: $G=(V, E)$ 中两子集 $\tilde{V}_1 \subset V, \tilde{V}_2 \subset V$, 有 $\tilde{V}_1$ 与 $\tilde{V}_2$ 间无边相连。
- 二划分: G 中无孤立点且连通, $\tilde{V}_1 \cup \tilde{V}_2 = V, \tilde{V}_1 \cap \tilde{V}_2 = \emptyset$, 此种二分图称为二划分。
- 完全二分图: $\tilde{V}_1$ 与 $\tilde{V}_2$ 间都有边相连的二分图。
- 二分图性质: 二分图 $\Leftrightarrow$ 所有回路长度为偶数。

——二分图的匹配

- 匹配: 二分图 G 的 $\tilde{V}_1$ 与 $\tilde{V}_2$, 有 $\tilde{V}_1 = \{v_1, v_2, \dots, v_r\}$, 则 $\tilde{V}_1$ 到 $\tilde{V}_2$ 的匹配是 G 的子图, 它有 r 条边: $(v_1, v'_1), (v_2, v'_2), \dots, (v_r, v'_r), (v'_1, v'_2, \dots, v'_r \in \tilde{V}_2, \text{且 } v_i \neq v_j)$ 。
- 匹配的性质之一——相异条件: 二分图 G 从 $\tilde{V}_1$ 到 $\tilde{V}_2$ 的匹配 $\Leftrightarrow \tilde{V}_1$ 中每 k 个结点至少要与 $\tilde{V}_2$ 中 k 个结点连通。

• 匹配的性质之二—— t 条件:二分图 G 从 $\tilde{V}_1$ 到 $\tilde{V}_2$ 的匹配条件是,存在 $t > 0$ 。

(1) $\tilde{V}_1$ 中每个结点至少存在 t 条相邻边。

(2) $\tilde{V}_2$ 中每个结点至多存在 t 条相邻边。

8. 平面图

——平面图基本概念

- 平面图:平面上的图除结点外,其边均不相交。
- 平面图的区域:平面图可沿边划分成独立的区域。

——平面图性质

• 欧拉公式:连通平面图有: $v - e + r = 2$ (v 为结点数, e 为边数, r 为区域数)。

• 连通无环平面图有: $e \leq 3v - 6$ (每个区域由三条及以上边围成)。

• 连通无环平面图有: $e \leq 2v - 4$ (每个区域由四条及以上边围成)。

• Kuratowski 定理:平面图 $\Leftrightarrow$ 它不包含与 $K_{3,3}$, K_5 在二次结点内同构的子图。

• 至少有三个结点的连通平面图,则至少有一个结点 v 满足 $\deg(v) \leq 5$ 。

9. 树

——树的基本概念

- 树:不含回路的连通图。
- 子树:树的子图。
- 根:树中某特定结点。
- 分支结点:除根外次数 ≥ 2 的结点。
- 叶:次数为 1 的结点。
- 结节点:从根到结点的通路长度。

• 结点的双亲、子女、兄弟、子树:结点与其上一级结点所构成的子树的根称双亲,而结点间称兄弟,结点称根的子树。

- 森林:树的集合。

——树的基本性质

- (n, m) 树有: $m = n - 1$ 。
- 树 $\Leftrightarrow$ 连通图且 $m = n - 1$ 。
- 树 $\Leftrightarrow (n, m)$ 图, $m = n - 1$ 且无回路。
- 树 $\Leftrightarrow$ 图中两结点间存在惟一简单通路。

——二叉树

- 二叉树: 结点次数 ≤ 2 。
- 左(右)子树: 二叉树中左(右)边子树。
- 完全二叉树: 所有结点次数为 2。
- 遍历: 搜索二叉树结点的过程使每个结点恰好访问一遍。
- 遍历的三种方法: 先根次序遍历法、中根次序遍历法及后根次序遍历法。

- 树转化为二叉树的方法:

(1) 从树的根开始保留双亲同其最左边子女的连线, 撤销与别的子女的连线;

(2) 兄弟间加线连接;

(3) 以树的主根为圆心, 将树顺时针转 45° 。

——生成树

- 生成树: 连通图中包含所有结点的子图为树。
- 生成树的秩与弦: (n, m) 连通图的生成树所去掉的边称弦,

所去掉的边数为 $m - n + 1$, 称为秩。

- 最小生成树: 连通权图中权之和最小的生成树。
- 生成树的生成算法:

(1) 令 G 是 G_1 , 置 $i = 1$;

(2) 若 G_i 无回路, C_i 为生成树, 生成树找到;

(3) 否则, G_i 消去回路 C_i 中的一条边得 G_{i+1} , G_{i+1} 是连通的;

(4) $i = i + 1$, 返回(2)。

- 最小生成树生成算法之一: 在上面算法中(3)处消去 G_i 中权

最大的边。

- 最小生成树生成算法之二：

- (1) $i=1, G_i$ 的边取 G 中权最小者；

- (2) 若 G_i 已是生成树, 则算法结束；

- (3) 否则, 在 $E-E_i$ 中找一条最小权的边加入 G_i 且不形成回路, 得到 G_{i+1} ；

- (4) $i=i+1$, 返回(2)。

10. 有向图

——有向图基本概念

- 有向图: 图 $G=(V, E)$ 中 E 是 V 的有偶序集合。

- 有向边: 有向图中有偶序称有向边, 其第一个元素称起点, 第二个元素称终点。

- 有向图的环: 有向图中特殊的有向边: (v_i, v_i) 。

- 有向图的平行边: 有向图中连接 v_i, v_j , 且同方向的两条边。

- 有向图的重图: 有平行边的有向图。

- 简单有向图: 无环无平行边的有向图。

- 有向图结点的引出次数、引入次数与全次数: 图中结点 v , 以 v 为起点的边数称 v 的引出次数, 记以 $\overrightarrow{\deg}(v)$; 以 v 为终点的边数称 v 的引入次数, 记以 $\overleftarrow{\deg}(v)$, v 的引入、引出次数之和称全次数, 记以 $\deg(v)$ 。

- 有向图中的通路: 有向图中两结点 v_i 到 v_j 有有向边序列相连。

- 有向图中通路性质: n 个结点简单有向图中基本通路长度小于 n 。

- 有向图连通性。

- (1) 强连通: 图中每对结点均连通；

- (2) 单向连通: 图中每对结点至少有一个方向连通；

- (3) 弱连通: 图中每条边去掉方向后是无向连通。

——有向图矩阵表示:有向图 G 的相邻矩阵 $M=[a_{ij}]_{n \times n}$:

$$a_{ij} = \begin{cases} 1, & \text{若 } \langle v_i, v_j \rangle \in E \\ 0, & \text{若 } \langle v_i, v_j \rangle \notin E \end{cases}$$

——有向图 D 有 n 个结点,其矩阵为 M ,则 $M^n=[a_{ij}^n]$ 中 a_{ij}^n 表示从结点 v_i 到 v_j 长度为 n 的通路数。

——有向图 D 有 n 个结点,其矩阵为 M , $C=M+M^2+\cdots+M^{n-1}$,则 D 是强连通 $\Leftrightarrow C$ 中除对角线外无元素为零。

第六章 命题逻辑

6.1 命题与命题联结词

1. 命题

我们知道,世界上存在着很多仅与两值有关的事物,如一个普通开关,它可有两个状态:一为“闭合”状态,一为“断开”状态。一个灯泡也有两个状态,一为“亮”状态,一为“熄”状态。又如继电器接点也有“吸合”与“释放”两个状态。在计算机的逻辑电路中有“高电位”与“低电位”两个不同状态。在程序设计中的逻辑条件判断中有“满足条件”与“不满足条件”这两种状态。在日常逻辑判断中对语句有“真”与“假”两种状态。所有这些例子都说明,存在着很多以两值为对象的事物。这些事物我们称为命题,而命题的两个值可以用 0 与 1 来表示。

命题可分为命题常量与命题变量。所谓命题常量指的是这个命题的值是固定不变的。所谓命题变量指的是这个命题的值是可变的。

在命题中,有些命题是基本的、原始的,它不能再被分割成为更小的命题,这些命题称为原子命题。如下列命题均为原子命题:

- 一个继电器的接点
- 一个灯泡
- 一个简单句

当然,也有些命题并不是最基本的,它们还可以被分解成更小的命题,或者说,它们可以由更小的命题组合而成,这些命题称为复合

命题。如下面的命题均为复合命题：

由若干个继电器所组成的一个开关电路

由若干个简单句组成的复合句

命题这个词来源于形式逻辑，而且在形式逻辑中应用得很普遍。

因此，我们在这里要特别提一下命题在形式逻辑这个范畴内的含义。在形式逻辑中，命题表示一个能判别真假的语句。其中真的用 1 表示，假的用 0 表示。但并不是所有语句都能判别真假的。一般讲，只有陈述句才能判别真假。因此，一般讲，也只有陈述句才可能是命题。前面所提到的原子命题与复合命题的例子中的简单句与复合句，严格地讲，应是简单陈述句与复合陈述句。

下面我们举一些这方面的例子。下列语句为命题：

人总是要死的

中华人民共和国的首都是北京

$2+2=5$

菊花总是在春天开放

在这四个语句中，它们均为陈述句，都能判别真假，其中前两个语句为真，后两个语句为假。因此，它们都是命题。

下列语句均不为命题：

我要三个苹果

对不起，请你让一下

祝你一路顺风

这三个语句都不是陈述句，都不能判别其真假，故它们都不是命题。

2. 命题联结词

在实际生活中，命题与命题间是可以通过某种方式联结起来的。例如若干个开关可以按串联、并联或桥联方式联结成一个开关电路，若干个命题语句可通过某些联结词构成一个复合语句，若干个逻辑判别条件可通过不同联接方式构成一个程序框图。所有这些联接方

式我们称为命题联结词或命题运算符。

一般常用的命题联结词有下面三个：

(1) 否定

在开关中开的否定是关；关的否定是开。在逻辑电路中高电位的否定是低电位；低电位的否定是高电位；在语句中，真的否定是假，假的否定是真。所有这些，抽象成命题后即表示：取值为 0 的命题的否定是 1；取值为 1 的命题的否定是 0。一般一个命题 P 的否定可记为 $\neg P$ ，念作非 P 。一个命题的否定与此命题间值的关系可用表 6-1 表之。这种表叫否定联结词的真值表。

表 6-1 否定联结词的真值表

P	$\neg P$
0	1
1	0

在语句中一个命题 P 的否定 $\neg P$ 也是一个命题，它的含义与原命题 P 相反。如命题 P 为“今天下雪”，则命题 $\neg P$ 为“今天不下雪”；命题 Q 为“6 是素数”，则命题 $\neg Q$ 为“6 不是素数”。在逻辑电路中某电位 P 可通过反相器而得另一电位，这个电位与原电位相反即为 $\neg P$ 。在开关中，开关的一个状态为断开时，则另一个状态为闭合；反之亦然。因此，若一个状态是 P 时，则另一个状态为 $\neg P$ 。条件语句

if P then A else B

表示若为 P 时转向 A ；若为 $\neg P$ 时转向 B 。它可用图 6-1 表示之。

(2) 合取

开关电路中，两个开关按串联方式联结后只有当它们均为闭合时，联接在电路上的灯泡才亮，见图 6-2(a)，逻辑电路中 与门的两个输入端只有当它们都是高电位时其输出端才是高电位，见图 6-2(b)。在语句中当两个命题用“并且”联结词联结后构成一个复合语句，只有当两个命题均为“真”时，这个复合语句才为真。所有这些表明：两个命题在按照前面所述的方式联结后，联结所得的复合命题只

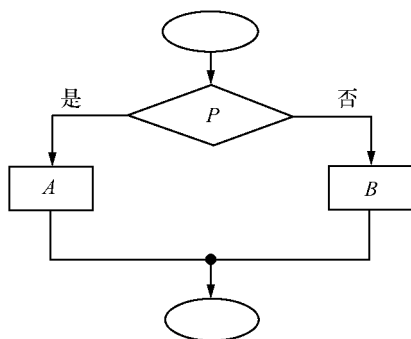


图 6-1 一个电路图

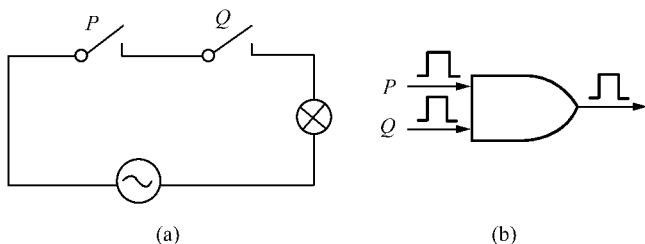


图 6-2 两种开关电路之一——逻辑：“与”

有当两个命题均为“1”时才为 1。

两个命题间的这种联结方式称为两个命题的合取。命题 P 与 Q 的合取可记为 $P \wedge Q$ 或 $P \times Q$ 。合取可以念作 P 乘 Q 或 P 并且 Q 。命题 P 与 Q 的合取以及命题 P, Q 间值的关系可用表 6-2 表示之。 $P \wedge Q$ 也可叫 P 与 Q 的合取式,而 P, Q 叫做这个合取式的合取项。

表 6-2 P 与 Q 的合取真值表

P	Q	$P \wedge Q$
0	0	0
0	1	0
1	0	0
1	1	1

合取这个联结词在语句中表示“并且”的含义；在逻辑电路中表示“与门”；在开关电路中表示“串联”联接方式。

以语句为例，设命题 P 为“我将去广州”，命题 Q 为“你将去上海”，则命题“我将去广州并且你将去上海”可写成 $P \wedge Q$ 。

设命题 P 为“今天下雨”，命题 Q 为“今天下雪”，则命题“今天下雨又下雪”可写成 $P \wedge Q$ 。

注意，这个命题中的“又”实质上是“并且”的同义词。因此，凡是与“并且”有相同含义的联结词，即这些联结词与其命题间满足表 6-2 真值表的关系，均是合取联结词。

(3) 析取

在开关电路中，两个开关按并联方式联结后只要当它们中有一个为闭合时，联接在电路上的灯泡就亮，见图 6-3(a)。在逻辑电路中或门的两个输入端只要它们中有一个是高电位时，其输出端即为高电位，可见图 6-3(b)。在语句中当两个命题用“或者”联结词联结后构成一个复合语句，此时只要两个命题中有一个为“真”时，这个复合语句一定也为“真”。所有这些表示，两个命题按照前面所述方式联结后，只要两个命题中有一个为“1”它也一定为“1”。

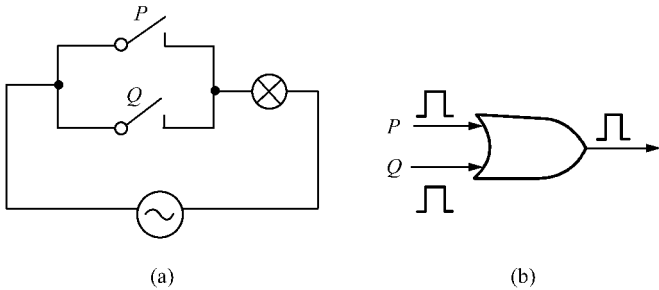


图 6-3 两种开关电路之二——逻辑：“或”

两个命题间的这种联结方式称为两个命题的析取。命题 P 与 Q 的析取可记为 $P \vee Q$ 或 $P + Q$ 。析取可念作 P 或者 Q 、 P 加 Q 。命题 P 与 Q 的析取以及命题 P 、 Q 间值的关系可用表 6-3 表示之。

$P \vee Q$ 也可叫 P 与 Q 的析取式,而 P 和 Q 叫做这个析取式的析取项。

表 6-3 P 与 Q 的析取真值表

P	Q	$P \vee Q$
0	0	0
0	1	1
1	0	1
1	1	1

析取这个联结词在语句中表示“或者”的含义。在逻辑电路中表示“或门”,在开关电路中表示“并联”联接方式。

以语句为例,设命题 P 为“明天中央歌舞团将有演出”,命题 Q 为“明天东方歌舞团将有演出”,则命题“明天中央歌舞团将有演出或者明天东方歌舞团将有演出”可写成 $P \vee Q$ 。

注意,根据析取真值表, P 与 Q 中只要有一个为“1”,则 $P \vee Q$ 即为“1”;不但如此, P 与 Q 同时为“1”时,则 $P \vee Q$ 亦为“1”。在这个例子中,中央歌舞团与东方歌舞团中只要有一个明天有演出,则 $P \vee Q$ 即为真。而且,中央歌舞团与东方歌舞团明天一起都演出,则 $P \vee Q$ 亦为真。我们再看一个例子,在这个例子中我们将会看到有不同的情况出现。设命题 P 为“李教授明天将出国访问”,命题 Q 为“李教授明天将去北京肿瘤医院住院开刀”;则命题“李教授明天将出国访问或住院开刀”是否可以写成 $P \vee Q$ 呢?回答是否定的。为什么呢?从表面上看,似乎这是可以的,因为两个命题间用“或者”相联,是符合前面的解释的。但是仔细研究可以发现,前一例中的“或者”与这一例中的“或者”有着稍为不同的含义。其主要差别在于在这个例中, P 与 Q 不可能同时为 1,即李教授不可能既出国访问又住院开刀。但前一例中,中央歌舞团与东方歌舞团是可以在明天一起都有演出的。虽然在两个命题间都用或者相联,但前一个或者是“可兼的或”,而后一个是“不可兼的或”。根据析取的真值表,“不可兼的或”不满足析取真值表的要求。

在命题逻辑中有了上面所讲的三个联结词就足够了。但是,为了方便起见,还可以引入若干个命题联结词。它们在某些场合特别有用。

(4) 蕴含

表 6-4 蘊含真值表

P	Q	$P \rightarrow Q$
0	0	1
0	1	1
1	0	0
1	1	1

设命题 P 为“明天下雪”，命题 Q 为“明天我穿棉衣”，则命题“如果明天下雪则我穿棉衣”可写成 $P \rightarrow Q$ 。

(5) 等价

• 219 •

在日常语言中, $P \leftrightarrow Q$ 相当于“ P 等价 Q ”、“ P 当且仅当 Q ”、以及“ P 与 Q 互为充要条件”等。它表示 P 与 Q 有相同的逻辑含义。如: 设命题 P 为“ $2+3=5$ ”, 命题 Q 为“ $5-3=2$ ”则命题“ $2+3=5$ 等价于 $5-3=2$ ”, 可写为 $P \leftrightarrow Q$ 。

P	Q	$P \leftrightarrow Q$
0	0	1
0	1	0
1	0	0
1	1	1

P	Q	$P \uparrow Q$
0	0	1
0	1	1
1	0	1
1	1	0

(7) 魏伯联结词

魏伯联结词又可叫或非联结词,它可记为 $P \downarrow Q$, 它的逻辑含义可由表 6-7 确定。

表 6-7 “魏伯”真值表

P	Q	$P \downarrow Q$
0	0	1
0	1	0
1	0	0
1	1	0

魏伯联结词在逻辑电路中相当于或非门。

(8) 异或

异或联结词记为 $P \oplus Q$ 或 $P \bar{\vee} Q$ 。它的逻辑含义可由表 6-8 确定。

在日常语言中,异或即表示不可兼的或。由此,我们说,日常生活中的“或者”由于存在着“可兼的”和“不可兼的”两种不同的逻辑含义,因而可分别用析取及异或两个命题联结词来表示。

表 6-8 “异或”真值表

P	Q	$P \oplus Q$
0	0	0
0	1	1
1	0	1
1	1	0

6.2 命题公式

1. 复合命题

一些原子命题经过一定数量的命题联结词联结后可以构成一个

新命题,这个新命题叫复合命题。复合命题的值可由原子命题的值经命题联结词真值表而得之。

下面我们举一些关于复合命题的实例。

例 6-1 试将下面语句写成复合命题形式:

天黑了,前面山中有狼,因此他决定留下来不走了。

我们可以令 P 为“天黑了”, Q 为“前面山中有狼”, R 为“他决定要走”。由此可将上面的语句写成为:

$$(P \wedge Q) \rightarrow \neg R$$

例 6-2 试将下面的语句写成复合命题形式:

如果没有老王和老李帮助我,我是完不成这个任务的。

我们可以令 P 为“老王帮助我”, Q 为“老李帮助我”, R 是“我完成这个任务”。由此,上面的语句可以写成:

$$\neg (P \wedge Q) \rightarrow \neg R$$

例 6-3 对于语句“居里夫人是波兰人,她是一个伟大的科学家,由于她对科学事业作出了巨大的贡献,因此,她被授予诺贝尔奖金”。我们可以令 P 为“居里夫人是波兰人”, Q 为“居里夫人是个伟大的科学家”, R 为“居里夫人对科学事业作出了巨大贡献”,令 S 为“居里夫人被授予诺贝尔奖金”。由此上述语句可写成:

$$(P \wedge Q \wedge (R \rightarrow S))$$

这段语句是真的,因为根据历史事实有:

$$P=1$$

$$Q=1$$

$$R=1$$

$$S=1$$

因此根据“ $\wedge$ ”与“ $\rightarrow$ ”的真值表有

$$1 \wedge 1 \wedge (1 \rightarrow 1) = 1 \wedge 1 = 1$$

注意,在复合语句中有时要引入括号。我们对命题联结词规定了一个结合力强弱的先后次序,它们是:

$$(1) \neg$$

(2) $\wedge, \vee, \oplus, \uparrow, \downarrow$

(3) $\rightarrow$

(4) $\leftrightarrow$

其中(2)的五个命题联结词具有相同的结合能力。凡符合上述结合力次序者括号可以省略。否则则要加括号。

2. 命题变元与命题公式

为了对命题逻辑作形式化研究,今后我们对命题只注意其值而不注意其内在含义;对命题联结词我们也只承认它由真值表定义,而并不理会它的实际含义。这样,我们就可以在此基础上对命题逻辑作形式的研究。

一个特定的命题是一个常值命题,它不是具有值 1 就是具有值 0。一个任意的命题是一个变量命题,在公式中的变量命题称为命题变元,它的变域是 0 与 1 所组成的集合。常用 P, Q, R 表示命题变元。

用命题变元及命题联结词可以构成命题公式。

定义 6-1 命题公式,简称公式,按下列法则生成:

(1) 命题变元是公式。

(2) 如果 P 是公式,则 $\neg P$ 是公式。

(3) 如果 P, Q 是公式,则 $(P \wedge Q), (P \vee Q), (P \rightarrow Q)$ 以及 $(P \leftrightarrow Q)$ 是公式。

(4) 公式只能由上述法则经有限步骤生成。

由此可以看出,命题公式由命题变元、命题联结词及圆括号构成,而其中之圆括号进行适当的省略。特别是一个公式最外层的括号常有省略。

按照上述定义,下面所表示的均为公式:

$$\begin{array}{c} P \rightarrow Q \\ P \\ (P \vee Q) \rightarrow Q \end{array}$$

$$\neg(P \rightarrow Q) \leftrightarrow (P \vee Q)$$

而下面所表示的都不是公式：

$$P \vee$$

$$\neg(\vee Q \vee P) \rightarrow PP$$

一个公式的真假可由公式的真值表决定，而公式的真值表由命题变元通过命题联结词真值表构成。

例 6-4 设有命题公式：

$$\neg(P \vee Q) \rightarrow (P \wedge R)$$

它的真值表中有变元 P, Q, R ，它的值可这样求得：

- (1) 按照析取真值表求得 $P \vee Q$ 的真值表；
- (2) 按照否定真值表求得 $\neg(P \vee Q)$ 的真值表；
- (3) 按照合取真值表求得 $P \wedge R$ 的真值表；
- (4) 按照蕴含真值表最后求得 $\neg(P \vee Q) \rightarrow (P \wedge R)$ 之真值表。

其过程可见表 6-9：

表 6-9 求 $\neg(P \vee Q) \rightarrow (P \wedge R)$ 真值表之过程

P	Q	R	$P \vee Q$	$\neg(P \vee Q)$	$P \wedge R$	$\neg(P \vee Q) \rightarrow (P \wedge R)$
0	0	0	0	1	0	0
0	0	1	0	1	0	0
0	1	0	1	0	0	1
0	1	1	1	0	0	1
1	0	0	1	0	0	1
1	0	1	1	0	1	1
1	1	0	1	0	0	1
1	1	1	1	0	1	1

而此公式之真值表可见表 6-10。

表 6-10 公式 $\neg(P \vee Q) \rightarrow (P \wedge R)$ 真值表

P	Q	R	$\neg(P \vee Q) \rightarrow (P \wedge R)$
0	0	0	0
0	0	1	0

续表

P	Q	R	$\neg(P \vee Q) \rightarrow (P \wedge R)$
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	1

一个命题公式的真值表刻画了这个公式的逻辑含义。因此，两个公式如果它们的真值表相同，我们就说它们是相等的。如公式：

$$\neg(P \wedge Q), \neg P \vee \neg Q$$

有相同真值表，见表 6-11 和 6-12。

表 6-11 $\neg(P \wedge Q)$ 的真值表

P	Q	$P \wedge Q$	$\neg(P \wedge Q)$	P	Q	$\neg(P \wedge Q)$
0	0	0	1	0	0	1
0	1	0	1	0	1	1
1	0	0	1	1	0	1
1	1	1	0	1	1	0

(a)

(b)

表 6-12 $\neg P \vee \neg Q$ 的真值表

P	Q	$\neg P$	$\neg Q$	$\neg P \vee \neg Q$	P	Q	$\neg P \vee \neg Q$
0	0	1	1	1	0	0	1
0	1	1	0	1	0	1	1
1	0	0	1	1	1	0	1
1	1	0	0	0	1	1	0

(a)

(b)

我们可以从表 6-9 中看出：公式 $\neg(P \vee Q) \rightarrow (P \wedge R)$ 与 $P \vee Q$ 有相同的值，就是说它们的真值表是相同的。因此我们说这两个公式

是相等的,即有:

$$\neg(P \vee Q) \rightarrow (P \wedge R) = P \vee Q$$

3. 命题公式的基本等式

研究命题公式的相等性问题是命题演算的重要研究课题之一,但是,用何种方法研究较为合适呢?当然,根据相等性定义,可用真值表的方法去研究公式间的相等性问题,但这不是一个好办法,因为:

(1) 真值表的方法是一个很麻烦的方法,特别是当命题变元较多时,真值表的计算是很花时间的,所花时间的程度甚至可能连现代最快速的计算机也无法计算。这样说也许不少读者可能会不相信,但是只要仔细推算就会发现事情要比想像的复杂得多。我们知道,有 n 个变元的公式,它们必具有 2^{2^n} 个不同的真值表,而每个真值表都有 2^n 行。若 $n=6$,则 $2^{2^6} = 2^{64} \approx 2 \times 10^{19}$;若 $n=9$ 时,真值表的数目就达到 $2^{2^9} = 2^{512} \approx 10^{154}$ 。

(2) 真值表的方法也是一个乏味的方法,它对于培养逻辑思维与推理能力帮助甚少。

因此,我们一般采用另外一种办法。这种办法是:首先,用真值表的方法得到一些数目不多的基本等式;其次,利用基本等式推导而求得为数众多的等式。这种方法基本上是利用推导而求得等式的方法,因此也可称推导法。

下面我们给出一些基本等式。为易于了解起见,我们将基本等式分成三类予以介绍。

4. 关于否定、析取、合取联结词的基本等式

本节中介绍的第一类基本上是关于否定、析取、合取联结词的等式,它们有下面几组:

第一组:等幂律

$$(1) P \vee P = P$$

$$(2) P \wedge P = P$$

第二组:交换律

$$(3) P \vee Q = Q \vee P$$

$$(4) P \wedge Q = Q \wedge P$$

第三组:结合律

$$(5) (P \vee Q) \vee R = P \vee (Q \vee R)$$

$$(6) (P \wedge Q) \wedge R = P \wedge (Q \wedge R)$$

第四组:分配律

$$(7) P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$$

$$(8) P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R)$$

第五组:否定律

$$(9) \neg \neg P = P \text{ (双否定律)}$$

$$(10) \neg (P \vee Q) = \neg P \wedge \neg Q \text{ (德·摩根定律)}$$

$$(11) \neg (P \wedge Q) = \neg P \vee \neg Q \text{ (德·摩根定律)}$$

第六组:常元律

$$(12) P \vee \neg P = 1$$

$$(13) P \wedge \neg P = 0$$

$$(14) 1 \vee P = 1$$

$$(15) 0 \wedge P = 0$$

$$(16) 0 \vee P = P$$

$$(17) 1 \wedge P = P$$

由上面六组 17 个等式可以推出很多其他的等式。

例 6-5 试证明:

$$P \vee (P \wedge Q) = P \quad (18)$$

$$\text{证明: } P \vee (P \wedge Q) = (P \wedge (Q \vee \neg Q)) \vee (P \wedge Q)$$

由(12) 及(17)

$$= (P \wedge Q) \vee (P \wedge \neg Q) \vee (P \wedge Q) \quad \text{由(7)}$$

$$= (P \wedge Q) \vee (P \wedge \neg Q) \quad \text{由(1)(3)}$$

$$= P \wedge (Q \vee \neg Q) \quad \text{由(7)}$$

$$= P \quad \text{由(12) 及(17)、(3)}$$

例 6-6 试证明:

$$P \wedge (P \vee Q) = P \quad (19)$$

$$\text{证明: } P \wedge (P \vee Q) = (P \wedge P) \vee (P \wedge Q) \quad \text{由(7)}$$

$$= P \vee (P \wedge Q) \quad \text{由(2)}$$

$$= P \quad \text{由(18)}$$

在等式(19)的证明中,我们除了应用(1)—(17)的 17 个基本等式外,还可以应用已推导出来的等式(18)。

等式(18)与(19)是很有用的等式,它们叫做吸收律。

例 6-7 试化简公式:

$$(\neg P \vee \neg Q) \vee (\neg \neg P \vee Q)$$

$$\text{证明: } (\neg P \vee \neg Q) \vee (\neg \neg P \vee Q)$$

$$= (\neg P \vee \neg Q) \vee (P \vee Q) \quad \text{由(9)}$$

$$= (\neg P \vee P) \vee (\neg Q \vee Q) \quad \text{由(3) 及(5)}$$

$$= 1 \vee 1 \quad \text{由(12)(14)}$$

$$= 1 \quad \text{由(1)}$$

公式的相等性在实际中有很多用处,它可以优化一个电路,简化一个程序,它还可以简化混乱的逻辑思维使它们表达清晰,条理清楚。下面我们以几例说明之。

例 6-8 请将下面的语句表达得更清楚一些,或将它的确切含义表达出来。

(1) 老王没有上火车站去接他是不对的。而他没有在火车站等老王也是不对的;

(2) 你去与不去都没有关系;

(3) 兰花香茉莉花香,兰花与茉莉花都香,没有不香的兰花也没有不香的茉莉花。

解: (1) 设 P 为“老王上火车站去接他”, Q 为“他在火车站等老王”,则上述语句可写为:

$$\neg(\neg P) \wedge \neg(\neg Q)$$

我们可以用基本公式将这个公式化简成：

$$\neg(\neg P) \wedge \neg(\neg Q) = P \wedge Q \quad \text{由(9)}$$

因此,这个句子确切的逻辑含义是:老王应到火车站去接他,而他也应在火车站等老王。

(2) 设 P 为“你去”,则上述语句可写为:

$$P \vee \neg P$$

我们可以将这个公式化简成:

$$P \vee \neg P = 1 \quad \text{由(12)}$$

它表示这个语句永远是真的。

(3) 设 P 为“兰花香”, Q 为“茉莉花香”,则上述语句可写为:

$$P \wedge Q \wedge (P \wedge Q) \wedge \neg(\neg P) \wedge \neg(\neg Q)$$

我们可以将这个公式化简成:

$$\begin{aligned} & P \wedge Q \wedge (P \wedge Q) \wedge \neg(\neg P) \wedge \neg(\neg Q) \\ &= P \wedge Q \wedge (P \wedge Q) \wedge P \wedge Q \quad \text{由(9)} \end{aligned}$$

$$= (P \wedge Q) \wedge (P \wedge Q) \wedge (P \wedge Q) \quad \text{由(6)}$$

$$= P \wedge Q \quad \text{由(2)}$$

所以这个语句的明确含义是:兰花香,茉莉花香。

例 6-9 试用较少的开关设计一个与图 6-4 有相同功能的电路:

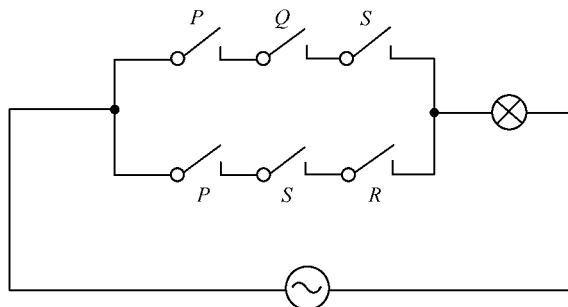


图 6-4 例 6-9 中的开关电路

解：我们可以将图 6-4 所示之开关电路写成为：

$$(P \wedge Q \wedge S) \vee (P \wedge R \wedge S)$$

利用基本等式可以将此公式化简成：

$$\begin{aligned} & (P \wedge Q \wedge S) \vee (P \wedge R \wedge S) \\ &= (P \wedge S \wedge Q) \vee (P \wedge S \wedge R) \end{aligned} \quad \text{由(4)}$$

$$= (P \wedge S) \wedge (Q \vee R) \quad \text{由(7)}$$

因此我们可以将这个开关电路化简成图 6-5 所示的开关电路,这个电路的功能与上一个一样,但它更简单,所需开关数更少。

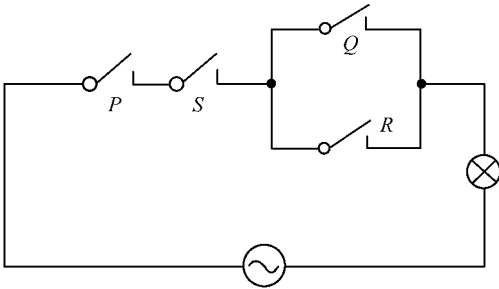


图 6-5 例 6-9 中之化简后的开关电路

例 6-10 将下面用程序设计语言写成的一段程序化简：

if A then if B then X else Y elseif B then X else Y

解：我们可将这段程序用图 6-6 的程序流程图表示。这段程序中执行 X 的条件为：

$$(A \wedge B) \vee (\neg A \wedge B)$$

执行 Y 的条件为：

$$(A \wedge \neg B) \vee (\neg A \wedge \neg B)$$

它们分别化简为：

$$(A \wedge B) \vee (\neg A \wedge B) = (B \wedge A) \vee (B \wedge \neg A) \quad \text{由(4)}$$

$$= B \wedge (A \vee \neg A) \quad \text{由(7)}$$

$$= B \wedge 1 \quad \text{由(12)}$$

$$= B \quad \text{由(17)}$$

$$(A \wedge \neg B) \vee (\neg A \wedge \neg B) = (\neg B \wedge A) \vee (\neg B \wedge \neg A)$$

$$= \neg B \wedge (A \vee \neg A)$$

$$= \neg B \wedge 1$$

$$= \neg B$$

由(4)

由(7)

由(12)

由(17)

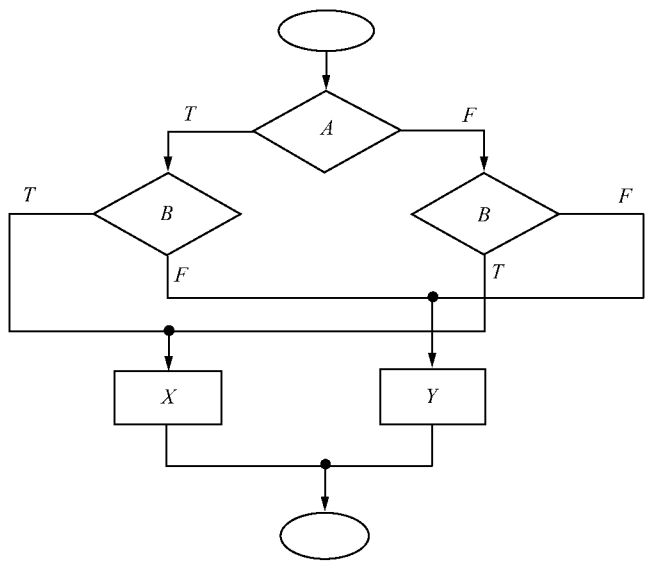


图 6-6 例 6-10 中之程序流程图

故这段程序可化简成

if B then X else Y

其流程图为图 6-7 所示。

例 6-11 试将图 6-8 所示之逻辑电路化简。

解：我们可以将图 6-8 所示的电路写成：

$((P \wedge Q) \vee (P \wedge R)) \wedge (Q \vee R)$

然后化简这个公式：

$((P \wedge Q) \vee (P \wedge R)) \wedge (Q \vee R)$

$$= (P \wedge (Q \vee R)) \wedge (Q \vee R)$$

由(7)

$$= P \wedge ((Q \vee R) \wedge (Q \vee R))$$

由(6)

$$= P \wedge (Q \vee R)$$

由(2)

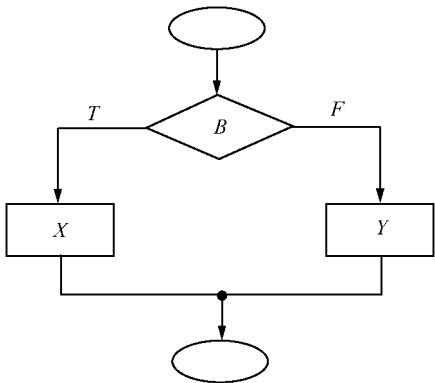


图 6-7 例 6-10 中之化简后的程序流程图

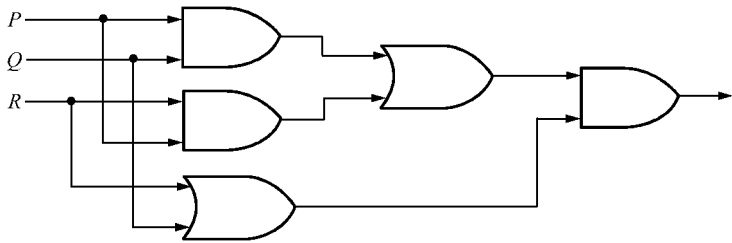


图 6-8 例 6-11 中之逻辑电路图

故此电路可以化简成图 6-9 所示电路。

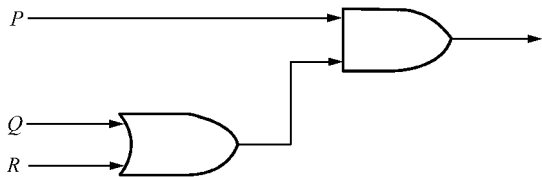


图 6-9 例 6-11 中之化简后的逻辑电路图

5. 关于蕴涵和等价联结词的基本等式

在前面与否定、析取、合取联结词有关的十七个基本等式以及二个非基本等式基础上,这里介绍与蕴涵及等价联结词有关的第二类基本等式,它们可以分为四组:

第七组:关于蕴涵的等式

$$(20) P \rightarrow (Q \rightarrow R) = (P \rightarrow Q) \rightarrow (P \rightarrow R)$$

$$(21) P \rightarrow Q = \neg Q \rightarrow \neg P$$

$$(22) \neg P \rightarrow P = P$$

第八组:关于等价的等式

$$(23) P \leftrightarrow Q = Q \leftrightarrow P$$

$$(24) (P \leftrightarrow Q) \leftrightarrow R = P \leftrightarrow (Q \leftrightarrow R)$$

$$(25) \neg P \leftrightarrow Q = P \leftrightarrow \neg Q$$

第九组:常元与变元的关系

$$(26) P \rightarrow P = 1$$

$$(27) P \leftrightarrow P = 1$$

$$(28) P \leftrightarrow \neg P = \neg P \leftrightarrow P = 0$$

$$(29) 1 \rightarrow P = P$$

$$(30) 0 \rightarrow P = 1$$

$$(31) P \rightarrow 1 = 1$$

$$(32) P \rightarrow 0 = \neg P$$

$$(33) 1 \leftrightarrow P = P$$

$$(34) 0 \leftrightarrow P = \neg P$$

第十组:联结词化归

$$(35) P \rightarrow Q = \neg P \vee Q$$

$$\begin{aligned}(36) P \leftrightarrow Q &= (P \rightarrow Q) \wedge (Q \rightarrow P) \\ &= (\neg P \vee Q) \wedge (\neg Q \vee P) \\ &= (P \wedge Q) \vee (\neg P \wedge \neg Q)\end{aligned}$$

我们也可由上面的 36 个基本公式推出其他一些等式来。

例 6-12 我们可以推得等式：

$$P \vee Q = \neg P \rightarrow Q$$

解： $P \vee Q = \neg(\neg P) \vee Q$ 由(9)

$$= \neg P \rightarrow Q \quad \text{由(35)}$$

例 6-13 我们可以推得等式：

$$P \wedge Q = \neg(P \rightarrow \neg Q)$$

解： $P \wedge Q = \neg(\neg P \vee \neg Q)$ 由(10) 及(9)

$$= \neg(P \rightarrow \neg Q) \quad \text{由(35)}$$

我们可以对一些实际的例子利用这 36 个等式进行化简。

例 6-14 将语句“如果张医生不负责任,那病人可能不得不重新开刀”用另一个语句表示。

解：令 P 为“张医生负责任”, Q 为“病人重新开刀”,则上述语句可以写成为：

$$\neg P \rightarrow \neg \neg Q$$

利用基本等式化简成为：

$$\neg P \rightarrow \neg \neg Q = \neg Q \rightarrow P \quad \text{由(21)}$$

所以上述语句相当于：如果病人不重新开刀,说明张医生负责任。

例 6-15 试述语句“不会休息的人不会工作,没有丰富知识的人也不会工作”与语句“工作得好的人一定会休息并且有丰富的知识”具有相同的含义。

解：设 P 为“某人工作得好”, Q 为“某人会休息”, R 为“某人有丰富的知识”。此时第一个语句可写为：

$$(\neg Q \rightarrow \neg P) \wedge (\neg R \rightarrow \neg P)$$

第二个语句可写为：

$$P \rightarrow Q \wedge R$$

利用基本等式我们有：

$$\begin{aligned} & (\neg Q \rightarrow \neg P) \wedge (\neg R \rightarrow \neg P) \\ &= (P \rightarrow Q) \wedge (P \rightarrow R) \end{aligned} \quad \text{由(21)}$$

$$= (\neg P \vee Q) \wedge (\neg P \vee R) \quad \text{由(35)}$$

$$= \neg P \vee (Q \wedge R) \quad \text{由(18)}$$

$$= P \rightarrow Q \wedge R \quad \text{由(35)}$$

由此我们证得了两个语句具有相同的含义。

6. 关于异或、谢佛、魏伯联结词的基本等式

在上面基本等式的基础上我们再介绍异或、谢佛、魏伯这几个联结词及与这些联结词有关的第三类基本等式。它们可分成四组：

第十一组：关于异或的等式

$$(37) P \oplus Q = Q \oplus P$$

$$(38) P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$$

$$(39) \neg (P \oplus Q) = \neg P \oplus Q = P \oplus \neg Q$$

第十二组：关于谢佛、魏伯的等式

$$(40) P \uparrow Q = Q \uparrow P$$

$$(41) P \uparrow P = \neg P$$

$$(42) P \downarrow Q = Q \downarrow P$$

$$(43) P \downarrow P = \neg P$$

第十三组：常元与变元的关系

$$(44) P \oplus P = 0$$

$$(45) 1 \oplus P = \neg P$$

$$(46) 0 \oplus P = P$$

$$(47) 1 \uparrow P = \neg P$$

$$(48) 0 \uparrow P = 1$$

$$(49) 1 \downarrow P = 0$$

$$(50) 0 \downarrow P = \neg P$$

第十四组：化归

$$(51) P \oplus Q = \neg (P \leftrightarrow Q)$$

$$(52) P \uparrow Q = \neg (P \wedge Q)$$

$$(53) P \downarrow Q = \neg (P \vee Q)$$

我们可以用上面 53 个等式推出很多其他等式来。

例 6-16 试证仅用谢佛一个联结词即可表示所有联结词。

证明：由(41)可知： $\neg P = P \uparrow P$

可以证得：

$$\begin{aligned} P \vee Q &= (P \uparrow P) \uparrow (Q \uparrow Q) \\ P \vee Q &= \neg(\neg P \wedge \neg Q) && \text{由(10) 及(9)} \\ &= (\neg P) \uparrow (\neg Q) && \text{由(52)} \\ &= (P \uparrow P) \uparrow (Q \uparrow Q) && \text{由(41)} \end{aligned}$$

还可以证得：

$$\begin{aligned} P \wedge Q &= (P \uparrow Q) \uparrow (P \uparrow Q) \\ P \wedge Q &= \neg(\neg(P \wedge Q)) && \text{由(9)} \\ &= \neg(P \uparrow Q) && \text{由(53)} \\ &= (P \uparrow Q) \uparrow (P \uparrow Q) && \text{由(41)} \end{aligned}$$

又由(35)、(36)及(51)可知蕴含、等价、异或均可由否定、析取、合取表示。故此例得证。

例 6-17 试证仅用魏伯一个联结词即能表示所有联结词。

证明：由(53)知： $\neg P = P \downarrow P$

可以证得：

$$\begin{aligned} P \wedge Q &= (P \downarrow P) \downarrow (Q \downarrow Q) \\ P \wedge Q &= \neg(\neg P \vee \neg Q) && \text{由(11) 及(9)} \\ &= (\neg P) \downarrow (\neg Q) && \text{由(53)} \\ &= (P \downarrow P) \downarrow (Q \downarrow Q) && \text{由(43)} \end{aligned}$$

还可以证得：

$$\begin{aligned} P \vee Q &= (P \downarrow Q) \downarrow (P \downarrow Q) \\ P \vee Q &= \neg(\neg(P \vee Q)) && \text{由(11) 及(9)} \\ &= \neg(P \downarrow Q) && \text{由(53)} \\ &= (P \downarrow Q) \downarrow (P \downarrow Q) && \text{由(43)} \end{aligned}$$

这两个例的证明从理论上回答了为什么在逻辑电路中只要有一种与非门或只要有一种或非门就足够了的原因。

异或、谢佛及魏伯这三个联结词在计算机中用处很大，在计算机

的电路中只要有一种与非门——即谢佛联结词即可以构造所有逻辑电路。同理,只要有一种或非门——即魏伯联结词也可以构造所有逻辑电路。

6.3 重 言 式

1. 关于重言式的基本概念

在命题公式中有一种类型的公式引起了我们特别的注意,它有一种奇特的特性——即不管公式中的命题变元如何变化,这个公式的值永远为真。这种公式我们叫做重言式或叫永真公式。

下面我们举个关于重言式的例子。

例 6-18 下面的公式均为重言式:

$$(1) (P \wedge Q) \rightarrow P$$

$$(2) P \rightarrow (P \vee Q)$$

$$(3) (P \wedge P) \leftrightarrow P$$

(1)—(3)可以很容易用真值表的方法或基本公式推导的方法来证明,因此留给读者作为习题。

例 6-19 下面的公式均不是重言式:

$$(1) (P \vee Q) \rightarrow (P \wedge Q)$$

$$(2) (P \wedge Q) \leftrightarrow P$$

$$(3) (\neg P \vee P) \rightarrow (\neg P \wedge P)$$

其证明的方法也很容易,请读者自己证明。

例 6-19 中(1)—(3)虽都不为重言式,但是在这三个公式中的(3)特别引起我们的注意。这主要是由于(3)具有一个与重言式截然相反的特性,即不管命题变元如何变化,公式(3)永远为假。这种具有不管公式中的命题变元如何变化,公式永远为假的特性的公式,称为矛盾式或永假公式。

重言式与矛盾式是性质截然相反的两种特定的公式。但是,它

们之间是可以互相转化的,即重言式的否定是矛盾式;矛盾式的否定是重言式。因此我们只要研究其中的一个即可。一般均着重研究重言式。

在重言式的研究中,我们特别感兴趣的是蕴含重言式与等价重言式。如果蕴含式 $P \rightarrow Q$ 永为真,则称为蕴含重言式,并记为:

$$P \Rightarrow Q$$

如例 6-18 中之(1)、(2)均为蕴含重言式,因此它们可以分别记为:

$$(P \wedge Q) \Rightarrow P$$

及:

$$P \Rightarrow (P \vee Q)$$

如果等价式 $P \leftrightarrow Q$ 为永真,则称为等价重言式,并记为:

$$P \Leftrightarrow Q$$

如例 6-18 中之(3)即为等价重言式,可记为

$$(P \wedge P) \Leftrightarrow P$$

比较等价重言式与相等性概念后会发现,它们是两个相同的概念。亦即,如某两公式相等,则它们间可构成一个等价重言式。如等式:

$$\neg(P \wedge Q) = \neg P \vee \neg Q$$

可构成重言式: $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$

如重言式:

$$\neg \neg P \Leftrightarrow P$$

可导出等式:

$$\neg \neg P = P$$

由于命题公式的等式问题已在上一节中作过介绍,因此,关于等价重言式不再作详细介绍。我们将重点介绍蕴含重言式。

2. 蕴含重言式

首先介绍几个较为重要的蕴含重言式:

$$I_1 \quad P \wedge Q \Rightarrow P$$

$$\begin{array}{ll}
I_2 & P \wedge Q \Rightarrow Q \\
I_3 & P \Rightarrow P \vee Q \\
I_4 & Q \Rightarrow P \vee Q \\
I_5 & \neg P \Rightarrow P \rightarrow Q \\
I_6 & Q \Rightarrow P \rightarrow Q \\
I_7 & \neg (P \rightarrow Q) \Rightarrow P \\
I_8 & \neg (P \rightarrow Q) \Rightarrow \neg Q \\
I_9 & \neg P \wedge (P \vee Q) \Rightarrow Q \\
I_{10} & \neg Q \wedge (P \vee Q) \Rightarrow P \\
I_{11} & P \wedge (P \rightarrow Q) \Rightarrow Q \\
I_{12} & \neg Q \wedge (P \rightarrow Q) \Rightarrow \neg P \\
I_{13} & (P \rightarrow Q) \wedge (Q \rightarrow R) \Rightarrow P \rightarrow R \\
I_{14} & (P \rightarrow Q) \wedge (R \rightarrow S) \Rightarrow P \wedge R \rightarrow Q \wedge S \\
I_{15} & (P \vee Q) \wedge (P \rightarrow R) \wedge (Q \rightarrow R) \Rightarrow R
\end{array}$$

上面这些蕴含重言式的正确性可以通过真值表得到证明,也可以通过基本等式加以证明。我们不想对它们中的每一个进行证明,这里证明其中的两个,其余的请读者自行去证。

我们先证明 I_7 的正确性:

$$\begin{aligned}
\neg (P \rightarrow Q) \rightarrow P &= \neg (\neg P \vee Q) \rightarrow P && \text{由(35)} \\
&= (P \wedge \neg Q) \rightarrow P && \text{由(10)} \\
&= \neg (P \wedge \neg Q) \vee P && \text{由(35)} \\
&= \neg P \vee Q \vee P && \text{由(11)} \\
&= 1 && \text{由(12)}
\end{aligned}$$

再证明 I_{12} 的正确性:

$$\begin{aligned}
&(\neg Q \wedge (P \rightarrow Q)) \rightarrow \neg P \\
&= (\neg Q \wedge (\neg P \vee Q)) \rightarrow \neg P && \text{由(35)} \\
&= \neg (\neg Q \wedge (\neg P \vee Q)) \vee \neg P && \text{由(35)} \\
&= (Q \vee \neg P) \vee (P \wedge \neg Q) && \text{由(10)、(11) 及(3)} \\
&= (Q \vee \neg P \vee P) \wedge (Q \vee \neg P \vee \neg Q) && \text{由(8)}
\end{aligned}$$

$$= 1 \wedge 1$$

由(12)、(14)及(3)

$$= 1$$

由真值表

除了上述蕴含重言式外,等价重言式也可作为蕴含重言式。因为我们有:

$$P \leftrightarrow Q \Rightarrow P \rightarrow Q$$

$$P \leftrightarrow Q \Rightarrow Q \rightarrow P$$

这表示 P 、 Q 等价可以有 P 蕴含 Q 及 Q 蕴含 P 。所以,如果有 $P \Leftrightarrow Q$ 就表示有 $P \Rightarrow Q$ 及 $Q \Rightarrow P$ 。6.2 中的全部基本等式可以作为蕴含重言式。而且一个等式可以作为两个蕴含重言式。如等式(7)可以拆成下面两个蕴含重言式:

$$P \wedge (Q \vee R) \Rightarrow (P \wedge Q) \vee (P \wedge R)$$

和:

$$(P \wedge Q) \vee (P \wedge R) \Rightarrow P \wedge (Q \vee R)$$

这样一来,蕴含重言式就很多了。

等价重言式表示了两个公式间的双向推导性;而蕴含重言式则表示了两公式间的单向推导性。

3. 蕴含重言式与推理规则

蕴含重言式反映了人类思维的一些推理方法与规则。我们知道,在人类思维活动中,需要进行大量的逻辑推理,如数学定理的证明,科学规则的探索,社会现象的分析等。这些推理一般是由一些已知条件出发推得一些未知结果,也就是由一些前题推得一些结论,它们可以表示为:

$$P_1, P_2, \dots, P_n \vdash Q_1, Q_2, \dots, Q_m$$

其中 P_i 、 Q_j 分别表示前提与结论,而符号“ $\vdash$ ”表示“推导出”的意思。

蕴含重言式 $P \Rightarrow Q$ 表示“如 P 为真则 Q 亦为真”。亦即是说:假设已知 P 为真,则可推得 Q 亦为真。因此可以认为 P 为前题, Q 为结论。所以蕴含重言式 $P \Rightarrow Q$ 相当于下面的推理:

$$P \vdash Q$$

成立。

推理 $P \vdash Q$ 也可表示为：

$$\frac{P}{Q}$$

如我们有 $P \wedge Q \Rightarrow R$, 它相当于下面的推理,

$$P, Q \vdash R$$

成立。

它也可以表示成为：

$$\frac{P}{\frac{Q}{R}}$$

因此, 根据上面的蕴含重言式我们可以得到很多的推理规则, 现将一些重要的列出如下:

R_1	$P \wedge Q \vdash P$	(简化式)
R_2	$P \wedge Q \vdash Q$	
R_3	$P \vdash P \vee Q$	(附加式)
R_4	$Q \vdash P \vee Q$	
R_5	$\neg P \vdash P \rightarrow Q$	
R_6	$Q \vdash P \rightarrow Q$	
R_7	$\neg(P \rightarrow Q) \vdash P$	
R_8	$\neg(P \rightarrow Q) \vdash \neg Q$	
R_9	$P, Q \vdash P \wedge Q$	
R_{10}	$\neg P, P \vee Q \vdash Q$	(析取三段论)
R_{11}	$P, P \rightarrow Q \vdash Q$	(假言推论)
R_{12}	$\neg Q, P \rightarrow Q \vdash \neg P$	(拒取式)
R_{13}	$P \rightarrow Q, Q \rightarrow R \vdash P \rightarrow R$	(假言三段论)
R_{14}	$P \rightarrow Q, R \rightarrow S \vdash P \wedge R \rightarrow Q \wedge S$	
R_{15}	$P \vee Q, P \rightarrow R, Q \rightarrow R \vdash R$	(二段推论)

上面这些推理规则有的是形式逻辑中很重要的推理规则,有的是日常生活中经常用到的一些推理规则。

如 R_{13} 在形式逻辑中称为假言三段论,在数学中称为传递规则。这个规则在日常生活中用得很多。我们可以举几个例子:

例 6-20 如果下列前提是真的:

如果你吸烟,则你会吸入大量尼古丁;

如果你吸入大量尼古丁,那么你将会得很多病;

如果你得了病,那就会影响你的寿命。

那么,根据这些前提,两次应用传递规则可得到结论:

如果你吸烟,那就会影响你的寿命。

又如推理规则 R_{10} 又称析取三段论,它在日常生活中也应用得很多。如在侦察某一案件后,已确定作案者必为甲、乙两人中的一个。此时,我们要获得最后结论的办法之一是,只要能排除其中一人的作案可能性则作案者必为另一人。

再如推理规则 R_{12} 又称拒取式,它也在日常生活中用得很多,可以用两个例子来作说明。

例 6-21 如果我们有两个前提:

只要老李在南京,他一定会去火车站接老王;

老李没有上火车站接老王。

则根据这些前提由 R_{12} 可得出结论:

老李不在南京。

例 6-22 某女子在某日晚归家途中被杀害,据多方调查确证凶手为王某或陈某,但是,后又经查证,作案之晚王某在工厂值夜班,没有外出。根据上述案情我们可得前提:

(1) 凶手为王某或陈某;

(2) 如果某某为凶手,则他在作案当晚必外出;

(3) 王某案发之晚并未外出;

此时由(2)、(3)利用 R_{12} 得出结论:

(4) 王某不是凶手;

又由 1、4 利用 R_{10} 得出结论:

(5) 陈某是凶手。

6.4 范 式

命题公式的形式是多样的,这对我们研究命题带来了不便。为此,我们将研究命题公式的标准形式问题——这就是范式。范式的研究对命题逻辑的发展起了极重大的作用。

1. 析取范式与特异析取范式

我们首先研究一种范式叫析取范式。析取范式有如下的形式特点:

- (1) 析取范式是一个析取式。
- (2) 析取范式中的每个析取项是一个合取式。
- (3) 这个合取式只包含命题变元及其否定。

下面的一些公式都是析取范式:

$$\begin{aligned} & (\neg P \wedge \neg P) \vee (P \wedge Q) \\ & (\neg P \wedge P \wedge P) \vee (Q \wedge Q \wedge P) \\ & \neg P \vee (P \wedge Q) \vee (P \wedge R) \end{aligned}$$

析取范式为命题公式提供了一种标准的形式。但是,这种标准形式有一个缺点,即是它的形式不是惟一的。如命题公式 $(P \vee Q) \wedge (P \vee R)$ 的析取范式至少有下列两个:

$$\begin{aligned} & P \vee (Q \wedge R) \\ & (P \wedge P) \vee (P \wedge Q) \vee (P \wedge R) \vee (Q \wedge R) \end{aligned}$$

这种标准式的不惟一性给研究问题带来不少困难,因此,我们需要对析取范式作进一步的要求,从而得到一个比析取范式条件更为严格的范式,这种范式叫特异析取范式。

特异析取范式需具有下列的形式特点:

- (1) 特异析取范式是一个析取范式。

(2) 在特异析取范式的每个析取项中,该公式的所有命题变元均须出现,它或以命题变元或以命题变元的否定形式出现,且仅出现一次。

例如公式:

$$P \vee Q$$

它的特异析取范式为:

$$(P \wedge Q) \vee (P \wedge \neg Q) \vee (\neg P \wedge Q)$$

又如公式:

$$P \vee (Q \wedge R)$$

它的特异析取范式为:

$$(P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (P \wedge \neg Q \wedge R) \vee (P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge Q \wedge R)$$

一个命题公式化归成特异析取范式的过程是:

(1) 利用等式(35)、(36)、(51)、(52)及(53)将公式中出现的联结词 $\rightarrow$ 及 $\leftrightarrow$ 、 $\oplus$ 、 $\uparrow$ 、 $\downarrow$ 之处化归成仅出现联结词 $\neg$ 、 $\wedge$ 及 $\vee$ 。

(2) 利用等式(10)、(11)将否定符号深入至命题变元,并利用(9)减少否定符号,使命题变元前的否定符号最多为一个。

(3) 利用分配律将公式化归成析取范式。

(4) 除去析取范式中所有为永假析取的项,即出现有 $\neg P \wedge P$ 形式的项。

(5) 若析取项中同一命题变元出现多次,则用等式(2)将其简化成只出现一次。

(6) 若析取项中不是公式中的所有命题变元均出现,则用 $P = P \wedge (Q \vee \neg Q)$ 在析取项中将变元 Q 补充进去,且利用分配律将它展开成几个析取项,并除去相同之析取项。

例 6-23 试求公式 $(P \wedge (P \rightarrow Q)) \vee Q$ 之特异析取范式。

解: 按上述之化归过程有:

$$(1) (P \wedge (P \rightarrow Q)) \vee Q = (P \wedge (\neg P \vee Q)) \vee Q$$

$$(2) (P \wedge (\neg P \vee Q)) \vee Q = (P \wedge \neg P) \vee (P \wedge Q) \vee Q$$

$$(3) (P \wedge \neg P) \vee (P \wedge Q) \vee Q = (P \wedge Q) \vee Q$$

$$\begin{aligned}(4) (P \wedge Q) \vee Q &= ((P \wedge Q) \vee Q) \wedge (P \vee \neg P) \\ &= (P \wedge Q) \vee (P \wedge Q) \vee (\neg P \wedge Q) \\ &= (\neg P \wedge Q) \vee (P \wedge Q)\end{aligned}$$

由此得到特异析取范式。

特异析取范式的析取项叫最小项, n 个命题变元可以有 2^n 个最小项。一个 n 个命题变元所构成的公式总可以用若干个最小项的析取组成。因此, 最小项是构成公式的基本细胞。

对 n 个变元的任一最小项必存在也只存在一组值使其为真, 这组值的选择可按下列规则:

- (1) 对最小项中出现的命题变元取值为 1。
- (2) 对最小项中出现的命题变元的否定取值为 0。

在变元的排列次序固定下, 每个最小项的对应值的二进编码称作这个最小项的序号。

例如对三个命题变元, 它一共可有 $2^3 = 8$ 个最小项, 它所对应的取值及序号可以表示如下:

最小项	对应的取值	序号
$\neg P \wedge \neg Q \wedge \neg R$	(0, 0, 0)	0
$\neg P \wedge \neg Q \wedge R$	(0, 0, 1)	1
$\neg P \wedge Q \wedge \neg R$	(0, 1, 0)	2
$\neg P \wedge Q \wedge R$	(0, 1, 1)	3
$P \wedge \neg Q \wedge \neg R$	(1, 0, 0)	4
$P \wedge \neg Q \wedge R$	(1, 0, 1)	5
$P \wedge Q \wedge \neg R$	(1, 1, 0)	6
$P \wedge Q \wedge R$	(1, 1, 1)	7

任一个公式如果其变元按固定次序排列, 且其最小项按其序号的递增(或递减)次序排列时, 所得的特异析取范式是惟一的。

由此可见, 特异析取范式是一种较为理想的标准形式。

一命题公式除了用上述化归的办法可以建立特异析取范式外, 还可以用真值表的方法建立特异析取范式。其过程如下:

- (1) 对一公式 A 构造其真值表。
- (2) 从真值表中取得最小项,即从真值表中取使公式 A 为 1 的那些项的取值,而每个取值均可对应一个最小项。
- (3) 将所得之最小项按序号递升次序排列而得到特异析取范式。

例 6-24 设一公式 A 的真值表如表 6-13 所示,求其特异析取范式。

解: 它的最小项是取值为 $(0,0,0)$ 、 $(1,0,0)$ 及 $(1,1,1)$ 的对应项,它们是: $\neg P \wedge \neg Q \wedge \neg R$ 、 $P \wedge \neg Q \wedge \neg R$ 、 $P \wedge Q \wedge R$ 。

因此这个公式的特异析取范式是:

表 6-13 公式 A 的真值表

P	Q	R	A
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

$A = (\neg P \wedge \neg Q \wedge \neg R) \vee (P \wedge \neg Q \wedge \neg R) \vee (P \wedge Q \wedge R)$ 利用这个方法还可以将一个实际问题很快地表示成命题公式。

例 6-25 一种简单的表决机器,表决者每人座位旁有一个按钮,当表决时若表示同意则按按钮,否则不按按钮。表决结果当超过半数时会场主席台上的红灯就亮,不超过半数则亮绿灯。为简单起见设表决者仅三人。试设计满足上述条件的表决机器。

解: 设三个表决者的按钮分别为 P 、 Q 、 R ,并设表决机器中红灯亮为 A ,绿灯亮为 B 。根据题意可以将其真值表列出(见表 6-14)。

根据真值表我们可以很快写出 A 与 B 的特异析取范式:

$$A = (\neg P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge R) \vee (P \wedge Q \wedge \neg R)$$

$$\begin{aligned}
 & (P \wedge Q \wedge \neg R) \vee (P \wedge Q \wedge R) \\
 B = & (\neg P \wedge \neg Q \wedge \neg R) \vee (\neg P \vee \neg Q \wedge R) \\
 & \vee (\neg P \wedge Q \wedge \neg R) \vee (P \wedge \neg Q \wedge \neg R)
 \end{aligned}$$

再将 A 与 B 分别化简后得：

$$\begin{aligned}
 A = & (P \wedge (Q \vee R)) \vee (Q \wedge R) \\
 B = & (\neg P \wedge (\neg Q \vee \neg R)) \vee (\neg Q \wedge \neg R)
 \end{aligned}$$

表 6-14 表决器的真值表

P	Q	R	A	B
0	0	0	0	1
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	0

其电路图如图 6-10 所示。

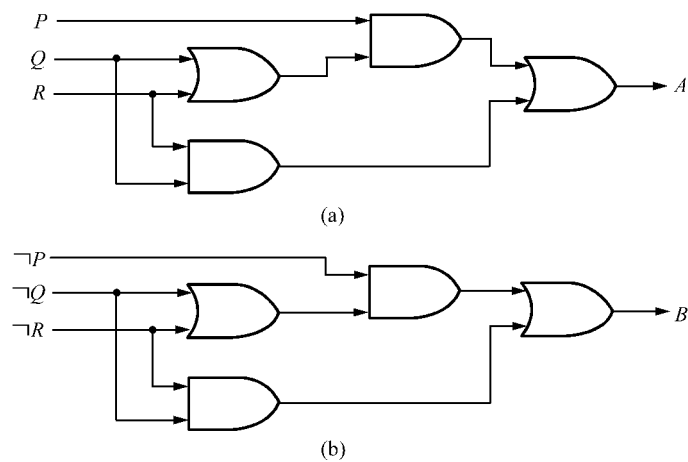


图 6-10 例 6-25 的逻辑电路图

2. 合取范式与特异合取范式

合取范式有如下的形式特点：

- (1) 合取范式是一个合取式。
- (2) 合取范式中的每个合取项是一个析取式。
- (3) 这个析取式只包括命题变元及其否定。

下面的一些公式都是合取范式：

$$\begin{aligned} & (\neg P \vee \neg P) \wedge (P \vee Q) \\ & (\neg P \vee \neg P) \wedge (Q \vee Q \vee P) \\ & \neg P \wedge (P \vee Q) \wedge (P \vee R) \end{aligned}$$

合取范式也有一个缺点，即它的表示形式不是惟一的。为此，我们引入特异合取范式。特异合取范式需具有下列之形式特点：

- (1) 特异合取范式是合取范式。
- (2) 在特异合取范式的每个合取项中，该公式中的所有变元均出现，它或以命题变元或以命题变元之否定形式出现且仅出现一次。

例如公式：

$$P \wedge Q$$

它的特异合取范式为：

$$(P \vee Q) \wedge (P \vee \neg Q) \wedge (\neg P \vee Q)$$

又如公式：

$$(Q \vee P) \wedge (Q \vee R)$$

它的特异合取范式为：

$$(P \vee Q \vee \neg R) \wedge (P \vee Q \vee R) \wedge (\neg P \vee Q \vee R)$$

一命题公式化归成特异合取范式的过程是：

- (1) — (3) 与特异析取范式方法相同。
- (4) 除去式中所有为永真的合取项，即出现有 $P \vee \neg P$ 形式之项。
- (5) 若合取项中同一命题变元出现多次，则可用公式 $P \vee P = P$ 将其化简成只出现一次。

(6) 合取项中若尚有命题变元不出现, 设它为 Q , 则用公式 $P = P \vee (Q \wedge \neg Q)$ 在合取项中将 Q 补入, 并用分配律将其展开成几个合取项并消除相同的合取项。

例 6-26 试求公式 $(\neg P \rightarrow R \vee P) \wedge (Q \leftrightarrow P)$ 之特异合取范式。

解: 按上述化归过程有:

$$\begin{aligned}
 (1) & (\neg P \rightarrow R \vee P) \wedge (Q \leftrightarrow P) \\
 &= (\neg \neg P \vee R \vee P) \wedge ((\neg Q \vee P) \wedge (\neg P \vee Q)) \\
 (2) & (\neg \neg P \vee R \vee P) \wedge ((\neg Q \vee P) \wedge (\neg P \vee Q)) \\
 &= (P \vee R \vee P) \wedge ((\neg Q \vee P) \wedge (\neg P \vee Q)) \\
 (3) & (P \vee R \vee P) \wedge ((\neg Q \vee P) \wedge (\neg P \vee Q)) \\
 &= (P \vee R \vee P) \wedge (\neg Q \vee P) \wedge (\neg P \vee Q) \\
 (4) & (P \vee R \vee P) \wedge (\neg Q \vee P) \wedge (\neg P \vee Q) \\
 &= (P \vee R) \wedge (P \vee \neg Q) \wedge (\neg P \vee Q) \\
 (5) & (P \vee R) \wedge (P \vee \neg Q) \wedge (\neg P \vee Q) \\
 &= (P \vee Q \vee R) \wedge (P \vee \neg Q \vee R) \wedge (P \vee \neg Q \vee \neg R) \\
 &\quad \wedge (\neg P \vee Q \vee \neg R) \wedge (\neg P \vee Q \vee R)
 \end{aligned}$$

由此得到特异合取范式。

特异合取范式的合取项叫最大项, n 个命题变元可以有 2^n 个最大项。一个由 n 个命题变元所构成的公式总可以用若干个最大项的合取组成。因此, 最大项也是构成公式的基本细胞。

对 n 个变元的任一最大项, 必存在也只存在一组值使其为假。这组值的选择可按下列规则:

- (1) 对最大项中出现的命题变元取值为 0。
- (2) 对最大项中出现的命题变元的否定取值为 1。

在变元排列次序固定下, 每个最大项的对应值的二进编码可叫做这个最大项的序号。

例如对三个命题变元, 它一共可有 $2^3 = 8$ 个最大项, 它们所对应的取值及序号可以表示如下:

最大项	对应的取值	序号
$\neg P \vee \neg Q \vee \neg R$	(1,1,1)	7
$\neg P \vee \neg Q \vee R$	(1,1,0)	6
$\neg P \vee Q \vee \neg R$	(1,0,1)	5
$\neg P \vee Q \vee R$	(1,0,0)	4
$P \vee \neg Q \vee \neg R$	(0,1,1)	3
$P \vee \neg Q \vee R$	(0,1,0)	2
$P \vee Q \vee \neg R$	(0,0,1)	1
$P \vee Q \vee R$	(0,0,0)	0

任一公式如其变元按固定次序排列且其最大项按序号的递增(或递减)次序排列时,一公式的特异合取范式是惟一的。

由此可见,特异合取范式也是一种较为理想的标准形式。

除了用上述化归办法建立特异合取范式外,还可用真值表的方法建立特异合取范式。其过程如下:

- (1) 对一公式 A 构造其真值表。
- (2) 从真值表中取得其最大项,即从真值表中取使公式 A 为 0 的那些项的取值,而每个取值均可对应一个最大项。
- (3) 将所得之最大项按序号递增次序排列而得到特异合取范式。

例 6-27 设公式 A 的真值表如表 6-15 所示。试求其特异合取范式。

表 6-15

公式 A 的真值表

P	Q	A
0	0	0
0	1	0
1	0	1
1	1	0

解: 它的最大项是取值为 (0,0)、(0,1)、(1,1) 的对应项,它们是:

$$\neg P \vee \neg Q, \neg P \vee Q \text{ 及 } P \vee Q$$

因此,这个公式 A 的特异合取范式是:

$$A = (P \vee Q) \wedge (\neg P \vee Q) \wedge (\neg P \vee \neg Q)$$

与特异析取范式类似,利用这个方法还可以将一个实际问题很快地表示成命题公式。

习 题 六

6.1 设 P 表示“他讲法语”, Q 表示“他讲英语”,将下列各公式翻译成自然语言:

- | | |
|--|------------------------------|
| (1) $(P \vee Q)$ | (2) $(P \wedge Q)$ |
| (3) $(P \wedge \neg Q)$ | (4) $(\neg P \vee \neg Q)$ |
| (5) $\neg(\neg P)$ | (6) $\neg(\neg P \wedge Q)$ |
| (7) $(P \leftrightarrow Q)$ | (8) $(\neg P \rightarrow Q)$ |
| (9) $\neg(\neg P \vee Q) \vee (P \wedge \neg Q)$ | |

6.2 将下列各命题翻译成符号公式:

- (1) 她的身材很高,也很温雅。
- (2) 说她长得高而且很温雅是不对的。
- (3) 她既不高也不温雅。
- (4) 李明读新民晚报或新华日报,但不读人民日报。
- (5) 如果高俊在屋里,则他在做功课或看电视。
- (6) 如果高俊不在屋里或者在做功课,那么他不在看电视。
- (7) 两个三角形全等当且仅当它们的三条边对应相等。

6.3 构造下列各题的真值表:

- (1) $(p \wedge (\neg q \rightarrow p)) \wedge \neg((p \leftrightarrow \neg q) \rightarrow (q \vee \neg p))$
- (2) $(q \leftrightarrow (r \rightarrow \neg p)) \vee ((\neg q \rightarrow p) \leftrightarrow r)$
- (3) $(p \rightarrow (q \rightarrow r)) \rightarrow ((p \rightarrow q) \rightarrow (p \rightarrow r))$
- (4) $(\neg q \rightarrow \neg p) \rightarrow (p \rightarrow q)$

6.4 证明:

$$(1) p \vee (p \wedge q) = p$$

$$(2) \neg(p \vee q) \vee (\neg p \wedge q) = \neg p$$

6.5 证明:(不用真值表法)

$$(1) (p \wedge q) \vee \neg p = \neg p \vee q$$

$$(2) (p \wedge q) \rightarrow r = (p \rightarrow r) \vee (q \rightarrow r)$$

$$(3) p \rightarrow (q \rightarrow r) = (p \wedge \neg r) \rightarrow \neg q$$

6.6 用真值表法验证 6.3 第 2 节中的 I_1 到 I_{15} 是重言式。

6.7 先将下面各题翻译成符号公式,然后检验其论证是否正确。

(1) 如果 6 是偶数,则 2 不能整除 7。

或者 5 不是素数,或者 2 整除 7。

5 是素数。

因此 6 是奇数。

(2) 在我夫人的生日那天,我送给她一束花。

或者这是我夫人的生日,或者我工作迟了。

今天我未送花给我夫人。

因此我今天工作迟了。

(3) 如果我工作,那我不能学习。

或者我工作,或者我考数学。

我通过了数学考试。

因此我学习过了。

(4) 如果我工作,那我不能学习。

或者我工作,或者我考数学。

我工作过了。

因此我参加了数学考试。

(5) 如果我学习,那我考试不会失败。

如果我不踢足球,那我将学习。

我考试失败了。

因此我踢了足球。

6.8 在一次演讲会上,有位政治家说:“如果国家税收增加,那么通货膨胀率将下降,只要而且仅仅只要美元不贬值”。在一次发表电视讲话时又说:“如果通货膨胀率下降,或者美元不贬值,则国家税收将不会增加”。在一次出国访问时又说:“或者国家税收必须增加,或者美元将贬值而且通货膨胀率将下降”,因此他的结论是国家税收将要提高,通货膨胀率将会下降,美元将不贬值。

问这位政治家的论证是否正确?(提示:仿照第7题的做法)

6.9 求下列各公式的析取范式和特异析取范式、合取范式和特异合取范式:

$$(1) (\neg p \vee \neg q) \rightarrow (p \leftrightarrow \neg q)$$

$$(2) q \wedge (p \vee \neg q)$$

$$(3) p \vee (\neg p \rightarrow (q \vee (\neg q \rightarrow r)))$$

$$(4) p \rightarrow (q \wedge r) \wedge (\neg p \rightarrow (\neg q \wedge \neg r))$$

$$(5) p \rightarrow (p \wedge (q \rightarrow p))$$

6.10 证明下列各公式是重言式。

$$(1) (p \wedge q) \vee (\neg p \wedge q) \vee (p \wedge \neg q) \vee (\neg p \wedge \neg q)$$

$$(2) (p \vee q) \wedge (\neg p \vee q) \vee (p \vee \neg q) \wedge (\neg p \vee \neg q)$$

$$(3) \neg(p \vee q) \vee (\neg p \wedge q) \vee p$$

$$(4) ((p \rightarrow q) \wedge p) \rightarrow q$$

$$(5) ((p \rightarrow q) \rightarrow (\neg q \rightarrow \neg p)) \rightarrow ((\neg q \rightarrow \neg p) \rightarrow (p \rightarrow q))$$

$$(6) (p \leftrightarrow q) \leftrightarrow ((p \wedge q) \vee (\neg p \wedge \neg q))$$

$$(7) (p \leftrightarrow q) \leftrightarrow ((r \wedge p) \leftrightarrow (r \wedge q)) \wedge ((r \vee p) \leftrightarrow (r \vee q))$$

6.11 重言式的否定式是()

- A. 重言式 B. 矛盾式
C. 可满足式(偶然式) D. 蕴含式

6.12 在命题公式中 $P \rightarrow Q$ 和 $\neg Q \rightarrow \neg P$ 是_____； $\neg P \rightarrow P$ 和_____是等价的。

6.13 证明 $P \wedge (P \rightarrow Q) \rightarrow Q$ 是重言式。

6.14 将下面的命题公式化为析取范式和合取范式。

$$\neg (P \rightarrow Q) \wedge Q \wedge R$$

6.15 下面哪个命题公式是重言式()

A. $(P \rightarrow Q) \wedge (Q \rightarrow P)$

B. $(P \wedge Q) \rightarrow P$

C. $(\neg P \vee Q) \wedge \neg (\neg P \wedge \neg Q)$

D. $\neg (P \vee Q)$

6.16 证明 $\neg (\neg P \rightarrow \neg Q) = Q \wedge \neg P$

6.17 化简下列公式,并判定公式是否为重言式、矛盾式或偶然式:

$$((p \rightarrow q) \rightarrow p) \leftrightarrow p$$

6.18 下面哪个命题公式不是重言式()

A. $Q \rightarrow (P \vee Q)$

B. $(P \wedge Q) \rightarrow P$

C. $\neg (P \wedge \neg Q) \wedge (\neg P \vee Q)$

D. $(P \rightarrow Q) \leftrightarrow (\neg P \vee Q)$

6.19 试在空格中写出等值演算的依据:

$$P \rightarrow (Q \vee R)$$

$$= \neg P \vee (Q \vee R) \quad \underline{\hspace{2cm}}$$

$$= \neg P \vee \neg P \vee Q \vee R \quad \underline{\hspace{2cm}}$$

$$= (\neg P \vee Q) \vee (\neg P \vee R) \quad \underline{\hspace{2cm}}$$

$$= (P \rightarrow Q) \vee (P \rightarrow R) \quad \underline{\hspace{2cm}}$$

6.20 证明 $P \wedge \neg Q \vee Q = P \vee Q$

6.21 化简公式并判定是否为重言式、矛盾式或偶然式: $(\neg p \rightarrow q) \rightarrow (\neg q \vee p)$

6.22 下面命题公式为重言式的是()

A. $P \rightarrow (Q \vee R)$

B. $(P \rightarrow (Q \rightarrow R)) \rightarrow ((P \rightarrow Q) \rightarrow (P \rightarrow R))$

C. $(P \vee R) \vee (P \rightarrow Q)$

D. $(P \vee Q) \leftrightarrow (Q \vee R)$

6.23 两个重言式的析取是_____；一个重言式和矛盾式的
的_____是矛盾式。

6.24 证明 $(P \rightarrow Q) \rightarrow (Q \vee R) = P \vee Q \vee R$

6.25 求下式的析取范式和合取范式

$$p \wedge (p \rightarrow q)$$

6.26 下面哪一组公式不等价？()

A. $\neg(A \rightarrow B); A \wedge \neg B$

B. $\neg(A \leftrightarrow B); (A \wedge \neg B) \vee (\neg A \wedge B)$

C. $A \rightarrow (B \vee C); \neg A \wedge (B \vee C)$

D. $A \rightarrow (B \vee C); (A \wedge \neg B) \rightarrow C$

6.27 证明 $A \rightarrow (B \rightarrow C), B \rightarrow (C \rightarrow D)$, 则 $A \rightarrow (B \rightarrow D)$ 。

6.28 求 $\neg(p \vee q) \leftrightarrow (p \wedge q)$ 的析取范式和合取范式。

“命题逻辑”复习提纲

1. 主要内容

- 命题逻辑基本概念。
- 命题逻辑基本等式。
- 命题逻辑推理规则。
- 命题逻辑的范式。

2. 复习重点

- 命题逻辑基本等式。
- 命题逻辑推理规则及应用。

3. 命题与命题联结词

- 命题：能判断真假的陈述句。

——原子命题:最简单的不可再分的命题。

——真值:命题的值称真值,真值有 0,1 两种。

——命题联结词:

- 否定: $\neg P$ 。
- 或者: $P \wedge Q$ 。
- 并且: $P \vee Q$ 。
- 蕴含: $P \rightarrow Q$ 。
- 等价: $P \leftrightarrow Q$ 。
- 谢佛: $P \uparrow Q$ 。
- 魏泊: $P \downarrow Q$ 。
- 异或: $P \oplus Q$ 。

4. 命题公式

——复合命题:原子命题与命题联结词结合构成新的命题。

——真值表:复合命题的值可用以真值为值的表表示称真值表。

——命题公式:命题公式简称公式:

- (1) 命题变元是公式;
- (2) P 是公式则 $\neg P$ 也是公式;
- (3) P, Q 是公式则 $P \vee Q, P \wedge Q, P \rightarrow Q, P \leftrightarrow Q$ 也是公式;
- (4) 公式由且仅由经(1)–(3)有限步内生成。

——有关否定、分析、合取的基本等式:

- 等幂律: $P \vee P = P, P \wedge P = P$ 。
- 交换律: $P \vee Q = Q \vee P, P \wedge Q = Q \wedge P$ 。
- 结合律: $(P \vee Q) \vee R = P \vee (Q \vee R), (P \wedge Q) \wedge R = P \wedge (Q \wedge R)$ 。
- 分配律: $P \wedge (P \vee Q) = (P \wedge Q) \vee (P \wedge R), P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R)$ 。
- 否定律: $\neg \neg P = P, \neg (P \vee Q) = \neg P \wedge \neg Q, \neg (P \wedge Q) = \neg P \vee \neg Q$ 。
- 常元律: $P \vee \neg P = 1, P \wedge \neg P = 0, 1 \vee P = 1, 0 \wedge P = 0, 0 \vee P$

$$=1, 1 \wedge P = P。$$

——有关蕴含与等价基本等式：

- $P \rightarrow (Q \rightarrow R) = (P \rightarrow Q) \rightarrow (P \rightarrow R)。$
- $P \rightarrow Q = \neg Q \rightarrow \neg P。$
- $\neg P \rightarrow P = P。$
- $P \leftrightarrow Q = Q \leftrightarrow P。$
- $(P \leftrightarrow Q) \leftrightarrow R = P \leftrightarrow (Q \leftrightarrow R)。$
- $\neg P \leftrightarrow Q = P \leftrightarrow \neg Q。$
- $P \rightarrow P = 1。$
- $P \leftrightarrow P = 1。$
- $P \leftrightarrow \neg P = \neg P \leftrightarrow P = 0。$
- $1 \rightarrow P = P。$
- $0 \rightarrow P = 1。$
- $P \rightarrow 1 = 1。$
- $P \rightarrow 0 = \neg P。$
- $1 \rightarrow P = P。$
- $0 \leftrightarrow P = \neg P。$

——有关异或、谢佛及魏泊基本等式：

- 关于异或等式： $P \oplus Q = Q \oplus P, P \oplus (Q \oplus R) = (P \oplus Q) \oplus R,$
 $\neg (P \oplus Q) = \neg P \oplus Q = P \oplus \neg Q。$
- 关于谢佛及魏泊等式： $P \uparrow Q = Q \uparrow P, P \uparrow P = P, P \downarrow Q = Q \downarrow$
 $P, P \downarrow P = \neg P。$
- 常元律： $P \oplus Q = 0, 1 \oplus P = \neg P, 0 \oplus P = P, 1 \uparrow P = \neg P, 0 \uparrow P$
 $= 1, 1 \downarrow P = 0, 0 \downarrow P = \neg P。$
- 化归律： $P \oplus Q = \neg (P \leftrightarrow Q), P \uparrow Q = \neg (P \wedge Q), P \downarrow Q$
 $= \neg (P \vee Q)。$

5. 重言式

——永真式：所有指派均为真的公式，又称重言式。

——永假式:所有指派均为假的公式,又称矛盾式。

——可满足式:至少存在一个指派使公式为真。

——蕴含重言式 $P \Rightarrow Q: P \rightarrow Q$ 永真。

——等价重言式 $P \Leftrightarrow Q: P \leftrightarrow Q$ 为真。

——15 个蕴含重言式:

$$I_1: P \wedge Q \Rightarrow P。$$

$$I_2: P \wedge Q \Rightarrow Q。$$

$$I_3: P \Rightarrow P \vee Q。$$

$$I_4: Q \Rightarrow P \vee Q。$$

$$I_5: \neg P \Rightarrow P \rightarrow Q。$$

$$I_6: Q \Rightarrow P \rightarrow Q。$$

$$I_7: \neg (P \rightarrow Q) \Rightarrow P。$$

$$I_8: \neg (P \rightarrow Q) \Rightarrow \neg Q。$$

$$I_9: \neg P \wedge (P \vee Q) \Rightarrow Q。$$

$$I_{10}: \neg Q \wedge (P \vee Q) \Rightarrow P。$$

$$I_{11}: P \wedge (P \rightarrow Q) \Rightarrow Q。$$

$$I_{12}: \neg Q \wedge (P \rightarrow Q) \Rightarrow \neg P。$$

$$I_{13}: (P \rightarrow Q) \wedge (Q \rightarrow R) \Rightarrow P \rightarrow R。$$

$$I_{14}: (P \rightarrow Q) \wedge (R \rightarrow S) \Rightarrow (P \wedge R) \rightarrow (Q \wedge S)。$$

$$I_{15}: (P \vee Q) \wedge (P \rightarrow R) \wedge (Q \rightarrow R) \Rightarrow R。$$

6. 推理规则

$$R_1: P \wedge Q \vdash P。$$

$$R_2: P \wedge Q \vdash Q。$$

$$R_3: P \vdash P \vee Q。$$

$$R_4: Q \vdash P \vee Q。$$

$$R_5: \neg P \vdash P \rightarrow Q。$$

$$R_6: \neg Q \vdash P \rightarrow Q。$$

$$R_7: \neg (P \rightarrow Q) \vdash P。$$

$$R_8 : \neg (P \rightarrow Q) \vdash \neg Q。$$

$$R_9 : P, Q \vdash P \wedge Q。$$

$$R_{10} : \neg P, P \vee Q \vdash Q。$$

$$R_{11} : P, P \rightarrow Q \vdash Q。$$

$$R_{12} : \neg Q, P \rightarrow Q \vdash \neg P。$$

$$R_{13} : P \rightarrow Q, Q \rightarrow R \vdash P \rightarrow R。$$

$$R_{14} : P \rightarrow Q, R \rightarrow S \vdash P \wedge R \rightarrow Q \wedge S。$$

$$R_{15} : P \vee Q, P \rightarrow R, Q \rightarrow R \vdash R。$$

7. 范式

——析取范式:是一个析取式,每个析取项是一个合取式,每个合取式仅含命题变元或其否定。

——特异析取范式:析取范式中每个析取项所有命题均以变元或其否定形式出现一次。

——合取范式:是一个合取式,每个合取项是一个析取式,每个析取式仅含命题变元及其否定。

——特异合取范式:合取范式中每个合取项所有命题均以变元或其否定形式出现一次。

——最大项与最小项:

- 最小项:特异析取范式的析取项。
- 最大项:特异合取范式的合取项。
- 重言式的充要条件:特异析取范式包含所有最小项。
- 矛盾式的充要条件:特异合取范式包含所有最大项。

第七章 谓词逻辑

谓词逻辑是命题逻辑的进一步扩充与延伸。我们知道在命题逻辑中基本的研究对象是命题,一个原子命题是不能再分割的。两个命题之间没有任何内在的联系。这种研究方法显然是不足以刻画世界上事物间千变万化的逻辑联系,就连最古老最简单的亚里斯多德三段论也无法从命题逻辑中推出。所谓亚里斯多德三段论方法即是由一个大前提、一个小前提可以推出一个结论。现举例如下:

大前提:凡人必死;

小前提:张三是人;

结论:张三必死。

这三段论中的三段之每一段均为一个命题。设大前提、小前提及结论的命题分别为 P 、 Q 、 R ,则此三段论可写为:

$$P \wedge Q \rightarrow R$$

而在命题逻辑中是无法推出这个公式为真。这是由于在这三段论中 P 、 Q 、 R 之间有着内在的逻辑联系。而这种联系在命题逻辑中是无法刻画出来的。

从这个例子可以看出命题逻辑是很不够的,因而有必要在命题逻辑的基础上进一步进行扩充与延伸——这就是我们要研究的谓词逻辑。

7.1 谓词逻辑的基本概念

1. 谓词与个体

在谓词逻辑中为了研究命题间的内在联系,有必要对命题作进

一步的分解。例如有命题“沈阳是城市”，我们可以将它分解成两部分。一部分是“是城市”，它可叫做谓词；另一部分是“沈阳”，它可叫做个体。当将个体与谓词结合在一起时就成为一个明确的命题。

仅仅谓词或仅仅个体是无法构成一个完整的逻辑含义的。只有将它们结合后才能构成一个完整、独立的逻辑断言。一般我们用大写拉丁字母表示谓词，用小写字母表示个体。例如设 F 为“是城市”， a 为“沈阳”。当将谓词与个体联合构成命题时，用括号将个体括住并直接安放在谓词后面。如“沈阳是城市”可写为 $F(a)$ 。

有时，在命题中出现的个体可能是变量，如命题“ $x^2 > 0$ ”中个体即为变量 x ，而若令谓词为 P ，则此命题可写为 $P(x)$ 。一般为便于讨论，我们常将分解成谓词和个体的命题简单地就叫做谓词。

在谓词 $F(x)$ 中一般变化的仅是个体 x ，我们在这里并不考虑 F 变化的情况，因此这种谓词 F 可称为常值谓词，而个体 x 可称为个体变元。如在个体变元中代入一确定常量，则这个常量就叫个体或叫个体常量。

下面的断言均可写成谓词：

我是中国人。

x 是素数。

林强住在农村。

若令 F 为“是中国人”， a 为“我”，则“我是中国人”可写成 $F(a)$ ；令 P 为“是素数”，个体变元是 x ，则“ x 是素数”可写成 $P(x)$ ；令 R 为“住在农村”， a 为“林强”，则“林强住在农村”可写成 $R(a)$ 。

上面叙述的谓词都仅仅只有一个个体（变元），但有时可能会出现两个个体（变元）。如：“王华与汪玲是夫妻”，它的谓词是“…与…是夫妻”，其中两个个体是“王华”及“汪玲”，如设谓词为 F ，王华、汪玲分别为 a, b ，则此断言可以写成为 $F(a, b)$ 。又如“ $y = x^2 + 2x + 1$ ”，它的两个个体变元是 x, y ，设谓词为 P ，则可写成为 $P(x, y)$ 。这种谓词通常叫二元谓词。类似，有时可能会出现有三个或更多的个体（变

元),如“上海位于杭州与南京之间”,“江苏省东临黄海、南接浙江、北靠山东、西连安徽”,都有三个或三个以上的个体(变元)。凡个体变元超过一个者都叫做多元谓词。

一元谓词刻划了个体的性质,多元谓词刻划了个体间的关系。多元谓词中个体在谓词中的次序有时是至关重要的。如“上海位于杭州与南京之间”这个命题是真的,其中“上海”、“南京”、“杭州”三个个体间次序不能随便颠倒,否则有可能成为假命题。例如将个体次序颠倒写成“杭州位于南京与上海之间”,就成为假命题了。

一个谓词中个体变元是有一定变化范围的,如谓词“ $x \leq 100$ ”中的个体变元 x 的变化范围是实数。又如谓词“ x 嫁给 y ”中个体变元 x 的变化范围是女人,而 y 的变化范围是男人。每个个体的变化范围构成了此个体的个体域。一般要求个体域中至少有一个元素。

有了谓词概念后,我们就可以将一些思想更深刻地刻划出来。下面我们举几个例子来说明。

例 7-1 爸爸是老师,妈妈是老师,我和弟弟是学生。

解: 令 $F(x)$ 表示“ x 是老师”, $P(x)$ 表示“ x 是学生”,并令爸爸为 a , 妈妈为 b , 我是 c , 弟弟是 d , 则上述语句可写为式子:

$$F(a) \wedge F(b) \wedge P(c) \wedge P(d)$$

例 7-2 请你把那个高个子戴眼镜的人喊来。

解: 令 $F(x, y)$ 表示“请 x 把 y 喊来”, $G(x)$ 表示“ x 是高个子”, $H(x)$ 表示“ x 戴眼镜”, $R(x)$ 表示“ x 是人”, a 表示“你”, b 表示“那个”。这样,此一语句可写为式子:

$$F(a, b) \wedge G(b) \wedge H(b) \wedge R(b)$$

例 7-3 那个小青年正在逗这只大黑狗熊。

解: 令 $F(x, y)$ 表示“ x 正在逗 y ”, $G(x)$ 表示“ x 是小的”, $H(x)$ 表示“ x 是大的”, $P(x)$ 表示“ x 是青年”, $R(x)$ 表示“ x 是黑的”, $S(x)$ 表示“ x 是狗熊”, a 表示“那个”, b 表示“这个”。这样,此一语句可写为式子:

$$F(a, b) \wedge G(a) \wedge H(b) \wedge P(a) \wedge R(b) \wedge S(b)$$

一般讲,对日常的语言,我们可以给出一个大体的准则,根据这些准则可写出其逻辑表达式来。

名 词:专用名词(如上海,林强等)为个体。

通用名词(如狗熊、人等)一般是谓词。

代名词:人称代词(如你、我、他)是个体。

指示代词(如这个、那个)是个体。

不定代词(如任何、每个、有些)是量词(见后)。

形容词:一般是谓词。

数 词:一般是量词(见后)。

动 词:一般是谓词。

副 词:一般与所修饰的动词合并为谓词,不再分解。

前置词:与别的有关字合并为一,本身不独立表示。

连接词:一般是命题联结词。

以上准则只供参考,在具体应用时常有许多例外。

2. 量词

一个带有个体变元的谓词的值是不确定的。这种谓词可以看成是一个函数,它以个体域为定义域,以 0、1 为值域。这个函数我们可以叫做命题函数。如设 $P(x, y)$ 表示“ $x < y$ ”, x, y 的定义域为实数集 R ,此时, $P(x, y)$ 的值是不确定的,它是 x, y 的函数,当 x, y 的值确定后它的值随之也跟着确定。如令 $x = 2, y = 3$,此时有 $P(2, 3) = 1$;如令 $x = 7, y = 4$,此时有 $P(7, 4) = 0$,这种确定的谓词是一个命题,所以叫命题函数。

因此,确定谓词的真假的办法是在其个体变元中代入一个属于该个体域的一个值。此后,这个谓词的真假也就确定了。

在谓词逻辑中谓词与其个体变元的个体域的值间存在着一定关系,个体域的不同值对应谓词的不同真假值,特别值得注意的是个体变元的个体域作为整体与谓词的关系,一般讲它们可以有下面四种关系:

- (1) 个体域的所有值均使谓词为真。
- (2) 个体域的所有值均使谓词为假。
- (3) 个体域的有些值使谓词为真。
- (4) 个体域的有些值使谓词为假。

为表示这四种关系我们引入了计量个体域的值与谓词关系的符号叫量词。量词有两种,一种叫全称量词,另一种叫存在量词,全称量词反映了个体域的所有值与谓词的关系,存在量词反映了个体域的有些值与谓词的关系。

对个体变元 x 以及它的域值与谓词 $F(x)$ 的“所有”关系可用如下的形式表示:

$$\forall_x(F(x))$$

其中“ $\forall$ ”为全称量词记号,它可表示为“所有”。而上面所述的关系(1)、(2)则可用如下形式表示:

$$\forall_x(F(x)) = 1$$

$$\forall_x(F(x)) = 0$$

$\forall_x(F(x))$ 有一个确定的值,它不是 0 就是 1,因此整个式子是确定的。这里面的变元 x 与一般变元有着明显区别,我们称这种变元为约束变元。

对个体变元 x 以及它的域值与谓词 $F(x)$ 的“有些”关系可用如下的形式表示:

$$\exists_x(F(x))$$

其中“ $\exists$ ”为存在量词记号,它可表示为“有些”。而上面所述的关系(3)、(4)则可用如下形式表示:

$$\exists_x(F(x)) = 1$$

$$\exists_x(F(x)) = 0$$

同样 $\exists_x(F(x))$ 有一个确定的值,它不是 0 就是 1,因此整个式子是确定的。与全称量词一样,存在量词中的变元 x 也是约束变元。

全称量词与存在量词都叫量词,紧跟量词后括号内的式子叫该

量词的辖域。量词反映了个体域整体与谓词间的真假关系,刻划了个体域整体与谓词间真假的数量关系。从这里也可以看出,在谓词逻辑中个体的个体域是很重要的。因此,每个谓词中的个体的个体域必须是确定的。但是,对于不同的谓词,不同的个体的个体域也是千变万化各不相同的,这对我们研究谓词逻辑带来很多不便。为了方便起见,有时我们干脆将所有个体域统一成一个个体域,这个个体域我们叫全总个体域。所谓全总个体域即是所有个体组成的个体域。这样一来,谓词中所有个体的个体域就全部统一了。因此,我们在谓词逻辑的研究中可以完全不必考虑个体域的大小与差异。但是,此时必须用特定的谓词对个体所变化的范围特性作出明确的刻划,这种谓词我们叫做特性谓词。对于受全称量词所束缚的个体变元(是约束变元),它的特性谓词可加在全称量词辖域内,与原式构成一个蕴含式,并以此特性谓词作为蕴含前件而原式为后件。对于受存在量词所束缚的个体变元(也是约束变元),它的特性谓词可加在存在量词辖域内,与原式构成一个合取式。对于不受量词约束的个体变元,可在整个公式中作为合取式中的合取项加入之。

由于在谓词逻辑中引入了个体、谓词以及量词概念,使得谓词逻辑的表达能力更加广泛和深刻。下面我们举几个有关例子。

例 7-4 对任一实数都满足:

$$(x+1)^2 = x^2 + 2x + 1$$

解: $R(x)$ 表示“ x 是实数”,则上述思想可写成:

$$\forall x(R(x) \rightarrow ((x+1)^2 = x^2 + 2x + 1))$$

例 7-5 凡人都要睡觉和吃饭。

解: 令 $M(x)$ 表示“ x 是人”, $A(x)$ 表示“ x 睡觉”, $E(x)$ 表示“ x 吃饭”。则上述思想可写成为:

$$\forall x(M(x) \rightarrow A(x) \wedge E(x))$$

例 7-6 世界上有好人也有坏人。

解: 令 $M(x)$ 表示“ x 是人”, $G(x)$ 表示“ x 是好的”, $B(x)$ 表示“ x 是坏的”。则上述思想可写成为:

$$\exists x(M(x) \wedge G(x)) \wedge \exists x(M(x) \wedge B(x))$$

例 7-7 二次方程式 $ax^2 + bx + c = 0$ 不一定存在实数解。

解：令 $R(x)$ 表示“ x 是实数”，则上述思想可写成：

$$\neg \exists x(R(x) \wedge (ax^2 + bx + c = 0))$$

例 7-8 在程序设计语言中一维整数数组：

$$\text{Array } A[1:50]$$

其中之每一项不为 0。

解：令 $I(x)$ 表示“ x 是整数”，令 $\leq (x, y)$ 表示“ $x \leq y$ ”， $\neq (x, y)$ 表示“ $x \neq y$ ”。则上述思想可写成为：

$$\forall x(I(x) \wedge \leq(1, x) \wedge \leq(x, 50) \rightarrow \neq(A(x), 0))$$

例 7-9 计算机中的设备只有登记入册(设备登记表)后才能供用户使用,请用谓词逻辑分别写出：

(1) 相对号为 03 的设备可提供用户使用；

(2) 相对号为 03 的设备不能提供用户使用。

解：设 $T(x)$ 表示可以与计算机相联的设备相对号, $P(x)$ 表示设备登记表中的相对号。此时,上述思想可写成为：

$$(1) \exists x(T(x) \wedge (P(x) \rightarrow = (3, x)))$$

$$(2) \forall x(T(x) \rightarrow (P(x) \rightarrow \neq (3, x)))$$

例 7-10 对于所有自然数 x, y 均有：

$$x + y \geq x$$

解：令 $N(x)$ 表示“ x 是自然数”，此时,上述思想可写成为：

$$\forall x \forall y (N(x) \wedge N(y) \rightarrow (x + y \geq x))$$

例 7-11 如果实数 x 大于实数 y , 而实数 y 大于实数 z , 则有实数 x 大于实数 z 。

解：令 $R(x)$ 表“ x 是实数”，则此时上述思想可写为：

$$\forall x \forall y \forall z (R(x) \wedge R(y) \wedge R(z) \rightarrow (<(y, x) \wedge <(z, y) \rightarrow <(z, x)))$$

例 7-12 每个实数必存在比它大的另外的实数。

解：令 $R(x)$ 表“ x 是实数”，此时,上述思想可写成为：

$$\forall x(R(x) \rightarrow (\exists y(R(y) \wedge \langle x, y \rangle)))$$

例 7-13 每个自然数都有惟一的一个后继数。

解：令 $N(x)$ 表示“ x 是自然数”， $B(x, y)$ 表示“ y 是 x 的后继数”，此时，上述思想可写成为：

$$\forall x(N(x) \rightarrow (\exists y(N(y) \wedge B(x, y))) \wedge \forall x \forall y \forall z (N(x) \wedge N(y) \wedge N(z) \rightarrow (B(x, y) \wedge B(x, z) \rightarrow \neg (y, z))))$$

例 7-14 某些计算机与某些外部设备之间不能相联。

解：令 $C(x)$ 表示“ x 是计算机”， $D(x)$ 表示“ x 是外部设备”， $P(x, y)$ 表示“ x 能与 y 相联”，此时，上述思想可写成为：

$$\exists x \exists y (C(x) \wedge D(y) \wedge \neg P(x, y))$$

例 7-15 有些人喜欢吃所有的食物。

解：令 $M(x)$ 表示“ x 是人”， $E(x)$ 表示“ x 是食物”， $L(x, y)$ 表示“ x 喜欢吃 y ”，此时，上述思想可写成为：

$$\exists x (M(x) \wedge \forall y (E(y) \rightarrow L(x, y)))$$

例 7-16 将高等数学中极限的定义：

$$\lim_{x \rightarrow c} f(x) = K$$

用谓词逻辑中的表达式刻划之。

解：我们知道上述之极限定义是：任给 $\epsilon > 0$ ，必存在一个 $\delta > 0$ ，对所有 x ，如果：

$$|x - c| < \delta, \text{ 则必有 } |f(x) - K| < \epsilon$$

我们令 $R(x)$ 表示“ R 是实数”，则极限之定义可写为：

$$\forall \epsilon ((R(\epsilon) \wedge \epsilon > 0) \rightarrow \exists \delta ((R(\delta) \wedge \delta > 0) \wedge \forall x (R(x) \rightarrow (|x - c| < \delta \rightarrow |f(x) - K| < \epsilon))))$$

7.2 谓词逻辑公式及其基本永真公式

1. 谓词逻辑公式

在命题逻辑的基础上将命题分解成谓词与个体，并引入了量

词等概念后构成了谓词逻辑的公式。在谓词逻辑公式中,命题、谓词、量词、联结词等按命题逻辑及谓词逻辑的要求构成了谓词逻辑公式。

在谓词逻辑中有一些最基本的公式,它们称为原子公式,由 n 元谓词 F 以及 n 个个体变元 $x_1, x_2, \dots, x_n$ 所构成的 $F(x_1, x_2, \dots, x_n)$ 是一个原子公式

由原子公式出发,我们可以定义谓词逻辑公式。

谓词逻辑公式又称公式可定义如下:

定义 7-1 (1)原子公式是公式。

(2) 若 A 是公式,则 $(\neg A)$ 也是公式。

(3) 若 A, B 是公式,则 $(A \wedge B)$ 、 $(A \vee B)$ 、 $(A \leftrightarrow B)$ 、 $(A \rightarrow B)$ 也是公式。

(4) 若 A 是公式, x 是个体变元,则 $\forall x(A)$ 、 $\exists x(A)$ 也是公式。

(5) 公式只能由上面规则经有限步骤生成。

在公式中,量词及联结词结合力强弱的先后顺序是:

(1) $\exists, \forall$

(2) $\neg$

(3) $\wedge, \vee$

(4) $\rightarrow$

(5) $\leftrightarrow$

按照上述规定,可减少公式中的括号层数。

命题逻辑公式是谓词逻辑公式的一个特例。在谓词逻辑公式中,有两种类型变元,一种是命题变元,一种是个体变元。但是要注意,我们前面已讲过约束变元,实际上受约束变元束缚的公式是确定的,故约束变元不是真的变元。真正变化的个体变元是不受约束的变元,这种变元称为自由变元。因此,我们可以归纳如下:谓词逻辑公式中出现的变元是命题变元与自由个体变元。

在谓词逻辑公式中,只要对所出现的命题变元与自由变元赋予确定的值后,谓词逻辑公式的值也就相应地确定。此时,公式的值不

是 0 就是 1。

下面的公式都是谓词逻辑公式：

$$P(x, y) \wedge P(y, x) \rightarrow F(x, x) \wedge F(y, y)$$

$$\forall x(P(x, y) \rightarrow R(x))$$

$$\exists x \forall y(E(x, y) \wedge E(y, z))$$

$$P \wedge F(x) \rightarrow \neg Q \vee P(y)$$

$$P \wedge Q \rightarrow Q \wedge P$$

与命题逻辑公式一样, 有的谓词逻辑公式不管对命题变元或自由变元赋予什么值它永为真, 这种公式我们称为谓词逻辑的永真公式或简称为永真公式。同样, 若不管对命题变元或自由变元赋予什么值它永为假, 这种公式我们称为谓词逻辑的永假公式或简称为永假公式。由于永假公式之否定即为永真公式, 故我们一般只要研究永真公式就够了。

我们感兴趣的是等价永真公式与蕴含永真公式。亦即是具有下列形式的永真公式：

$$F \Leftrightarrow F'$$

$$F \Rightarrow F'$$

而等价永真式 $F \Leftrightarrow F'$, 我们又可写成：

$$F = F'$$

称做 F 与 F' 相等。

2. 谓词逻辑的基本永真公式

我们可以给出一些基本的永真公式, 其他的永真公式可由这些基本永真公式推出。这些基本永真公式的正确性我们不准备都证明, 有时我们仅用几个例子加以说明。

(1) 命题永真公式的推广

在命题逻辑中的永真公式(或叫重言式)也是谓词逻辑永真公式, 特别是在命题永真公式中的命题用谓词逻辑公式代入后所得的公式亦为永真公式。

例 7-17 在命题逻辑中我们有： $P \rightarrow Q = \neg P \vee Q$ ，则我们在这里可以将：

$$\forall x(P(x)) \rightarrow \exists y(E(y))$$

化归为：

$$\forall x(P(x)) \rightarrow \exists y(E(y)) = \neg \forall x(P(x)) \vee \exists y(E(y))$$

例 7-18 我们有：

$$\forall x(P(x) \rightarrow Q(x)) = \forall x(\neg P(x) \vee Q(x))$$

因为在命题逻辑中我们有 $P \rightarrow Q = \neg P \vee Q$ 。

(2) 全称量词与存在量词间的关系

全称量词与存在量词间是有一定内在逻辑联系的，为说明此问题我们举几个例子。

例 7-19 我们知道“有些人今天没有到校上课”与“不是所有人今天都到校上课”具有相同的含义。设 $P(x)$ 表示“ x 今天到校上课”，则上述思想可表示成：

$$\exists x(\neg P(x)) = \neg \forall x(P(x))$$

例 7-20 我们知道，“所有的人都不吃狐狸肉”与“不存在吃狐狸肉的人”具有相同的含义。设 $P(x)$ 表示“ x 吃狐狸肉”，则上述思想可表示成：

$$\forall x(\neg P(x)) = \neg(\exists x(P(x)))$$

从这两个例中，我们可以看出全称量词与存在量词相互间是能转化的，我们可以得到其转换公式如下：

$$\exists x(\neg P(x)) = \neg(\forall x(P(x))) \quad (1)'$$

$$\forall x(\neg P(x)) = \neg(\exists x(P(x))) \quad (2)'$$

这两个永真公式告诉我们：

① 在谓词运算中只要有一个量词就足够了。因为由(1)'、(2)'可推得：

$$\forall x(P(x)) = \neg(\exists x(\neg P(x)))$$

$$\exists x(P(x)) = \neg(\forall x(\neg P(x)))$$

② 量词外面的否定符号可深入至量词辖域内，反之亦然。

(3) 量词辖域的扩张与收缩

在量词辖域内存在着一些与量词所约束的变元无关的公式,在某些情况下,这些公式可以自辖域内移出。反之亦可移入。这些永真公式是:

$$\forall x(P(x) \vee Q) = \forall x(P(x)) \vee Q \quad (3)'$$

$$\forall x(P(x) \wedge Q) = \forall x(P(x)) \wedge Q \quad (4)'$$

$$\exists x(P(x) \vee Q) = \exists x(P(x)) \vee Q \quad (5)'$$

$$\exists x(P(x) \wedge Q) = \exists x(P(x)) \wedge Q \quad (6)'$$

其中 Q 内不出现 x 。

我们可以证明(3)'的正确性。因此,(3)'中之 Q 或为 0 或为 1,当它为 0 时(3)'成立;当它为 1 时,(3)'亦成立。故(3)'成立。

(4)'、(5)'、(6)'之证明与(3)'类似。

由上述几个式子还可以推得下面几个永真公式:

$$\forall x(P(x)) \rightarrow Q = \exists x(P(x) \rightarrow Q) \quad (7)'$$

$$\exists x(P(x)) \rightarrow Q = \forall x(P(x) \rightarrow Q) \quad (8)'$$

$$Q \rightarrow \forall x(P(x)) = \forall x(Q \rightarrow P(x)) \quad (9)'$$

$$Q \rightarrow \exists x(P(x)) = \exists x(Q \rightarrow P(x)) \quad (10)'$$

我们先证明(7)'的正确性:

$$\begin{aligned} \forall x(P(x)) \rightarrow Q &= \neg(\forall x(P(x))) \vee Q && \text{由(35)'} \\ &= \exists x(\neg(P(x))) \vee Q && \text{由(1)'} \\ &= \exists x(\neg(P(x)) \vee Q) && \text{由(5)'} \\ &= \exists x(P(x) \rightarrow Q) && \text{由(35)} \end{aligned}$$

我们可以用类似的方法去证明(8)'、(9)'、(10)'的正确性。

(4) 量词与命题联结词间的关系

量词与命题联结词间也有几个永真公式:

$$\forall x(P(x) \wedge Q(x)) = \forall x(P(x)) \wedge \forall x(Q(x)) \quad (11)'$$

$$\exists x(P(x) \vee Q(x)) = \exists x(P(x)) \vee \exists x(Q(x)) \quad (12)'$$

对这两个永真公式的正确性我们可用几个例子来说明。

例 7-21 “所有学生都参加了考试并且都取得了较好成绩”与

“所有学生都参加了考试并且所有学生都取得了较好的成绩”这两句话有相同的意义。

例 7-22 “有人抽烟或有人喝酒”与“有人抽烟或喝酒”这两句话有相同的意义。

这两个永真公式告诉我们量词可以深入到某些命题公式内。

关于量词与命题联结词间还可有下面两个永真公式：

$$\forall x(P(x)) \vee \forall x(Q(x)) \Rightarrow \forall x(P(x) \vee Q(x)) \quad (13)'$$

$$\exists x(P(x) \wedge Q(x)) \Rightarrow \exists x(P(x)) \wedge \exists x(Q(x)) \quad (14)'$$

要注意的是这二个永真公式是蕴含永真公式。

这两个蕴含永真公式的正确性我们也可用几个例子来说明。

例 7-23 我们知道,由“今天所有人都唱歌或今天所有人都跳舞”可以推得“今天所有人都唱歌或跳舞”。

例 7-24 我们知道,由“有人既喜欢下棋又喜欢打牌”可以推得“有人喜欢下棋并且有人喜欢打牌”。

但要注意的是, $(13)'$ 、 $(14)'$ 之逆不一定成立。即 $\forall x(P(x) \vee Q(x)) \rightarrow \forall x(P(x)) \vee \forall x(Q(x))$ 与 $\exists x(P(x)) \wedge \exists x(Q(x)) \rightarrow \exists x(P(x) \wedge Q(x))$ 不一定为永真。我们可以由上两个例中看出“今天所有的人都唱歌或跳舞”并不能推得“今天所有的人都唱歌或今天所有的人都跳舞”,因为可能一部分人唱歌而另一部分人跳舞。同样,也不一定能由“有些人喜欢下棋并且有些人喜欢打牌”推得“有些人既喜欢下棋又喜欢打牌”。因为可能一部分人喜欢下棋而并不喜欢打牌,而另一部分人喜欢打牌却并不喜欢下棋。

关于量词与命题联结词间还可有下面的两个蕴含永真公式：

$$\forall x(P(x) \rightarrow Q(x)) \Rightarrow \forall x(P(x)) \rightarrow \forall x(Q(x)) \quad (15)'$$

$$\forall x(P(x) \rightarrow Q(x)) \Rightarrow \exists x(P(x)) \rightarrow \exists x(Q(x)) \quad (16)'$$

我们可以用几个例子作说明。

例 7-25 “每个数如它大于零则它的三次方亦必大于零”可推出“如果所有数都大于零则所有它的三次方亦必大于零。”

例 7-26 “每个数如它大于零则它的三次方亦必大于零”可推

出“如存在一些数大于零则必存在一些数的三次方亦大于零。”

同样, (15)'、(16)'之逆不一定成立。亦即是说 $(\forall x(P(x)) \rightarrow \forall x(Q(x))) \rightarrow \forall x(P(x) \rightarrow Q(x))$, 与 $(\exists x(P(x)) \rightarrow \exists x(Q(x))) \rightarrow \forall x(P(x) \rightarrow Q(x))$ 不一定成立。例如“如果有些车没有汽油则一定存在一些车无法开动”, 不一定能推出“对所有的车如果它没有汽油则它一定无法开动”。因为车子的种类很多, 有些车需要汽油才能开动, 如汽车; 但有些车不一定需要汽油也能开动, 如电车、马车、自行车等。

公式(15)'、(16)'表示量词可深入至蕴含式内部。

(5) 公式中量词的添加与除去

公式中量词的添加与除去可有下面一些永真公式:

$$\forall x(P(x)) \Rightarrow P(x) \quad (17)'$$

$$P(x) \Rightarrow \exists x(P(x)) \quad (18)'$$

这两个公式的正确性也是不言而喻的。因为如 $\forall x(P(x))$ 为真, 则公式 $P(x)$ 必为永真。同样, 如 $P(x)$ 为永真, 即是说, 对任一个个体变元 x , $P(x)$ 为真, 则 $\exists x(P(x))$ 也一定为真。

例 7-27 “所有的人都需要空气”必可推出“人需要空气”。

例 7-28 “人需要空气”必可以推出“有人需要空气”。

同样, (17)'、(18)'之逆不成立。

公式(17)'、(18)'给出了量词添加与除去的基本规则, 而且也给出了自由变元与约束变元间转换关系的一个准则。

(6) 多个量词间的次序排列

多个全称量词或多个存在量词间它们的次序是可以任意排列的, 对此有下列之永真公式:

$$\forall x \forall y(P(x, y)) = \forall y \forall x(P(x, y)) \quad (19)'$$

$$\exists x \exists y(P(x, y)) = \exists y \exists x(P(x, y)) \quad (20)'$$

(19)'、(20)'的正确性是比较容易理解的。我们仅举一个例子作说明。

例 7-29 “所有王庄的人和所有李庄的人都参加了群众大会”与“所

有李庄的人和所有王庄的人都参加了群众大会”这两句话是相同的。

多个量词间的次序排列关系尚有下面的永真公式,这个公式是蕴含永真公式:

$$\exists x \forall y (P(x, y)) \Rightarrow \forall x \exists y (P(x, y)) \quad (21)'$$

我们可以用例子说明这个公式的正确性。

例 7-30 我们可由“有些人看过所有数理逻辑的书”推出“所有数理逻辑的书都有人看过”。

但要注意,此公式之逆不一定成立。如上例中,“所有数理逻辑的书都有人看过”并不一定能推出“有人看过所有数理逻辑的书”。因为可能几个人分别看过部分数理逻辑的书,而他们全体则可能将所有数理逻辑的书都看过了。

除此之外,我们还可以有:

$$\forall x (P(x)) \Rightarrow \exists x (P(x)) \quad (22)'$$

这个公式的永真性也是显而易见的。

例 7-31 “所有猫都会捉老鼠”可以推出“有些猫会捉老鼠”。

同样,这个公式之逆不一定能成立。因为由“有些猫会捉老鼠”不一定能推出“所有猫都会捉老鼠”。

到此为止,我们给出了 22 个谓词逻辑永真公式,可以由这些永真公式推导出其他的永真公式来。但一般讲,这 22 个基本公式在大多数场合下也已经够用。

7.3 前束范式与斯科林范式

在谓词逻辑中,一般有两种范式,一种叫前束范式,一种叫斯科林范式。我们先讨论前束范式。

一个公式如果它的所有量词均出现在公式的最前面,它们的辖域一直延伸到公式末,且公式中不出现联结词 $\rightarrow$ 及 $\leftrightarrow$,则这种形式的公式称为前束范式。如下面的公式是前束范式:

$$\forall x \forall y \forall z (P(x) \vee Q(x, y) \vee R(y, z))$$

可以把前束范式分成两部分,一是公式的量词部分,称之为首标;二是命题逻辑公式部分。由于这种公式将量词集中在首标,因此公式比较有规则。

任何一个公式可表示成前束范式,其化归过程如下:

(1) 将公式中的联结词 $\rightarrow$ 和 $\leftrightarrow$ 换成 $\neg$ 、 $\vee$ 、 $\wedge$ 等联结词。

(2) 利用命题逻辑中的等式(9)、(10)、(11)及谓词逻辑中的等式(1)'和(2)',将公式中的否定符号深入到谓词变元之前。

(3) 为防止混淆,公式中的所有约束变元及自由变元均应不同,若有相同应更改之。

(4) 利用公式(3)'—(6)',扩大量词的辖域至整个公式。

例 7-32 将公式:

$$(\forall xP(x) \vee \exists yR(y)) \rightarrow \forall xF(x)$$

化归成前束范式。

解: (1) 除去联结词 $\rightarrow$

$$\begin{aligned} & (\forall xP(x) \vee \exists yR(y)) \rightarrow \forall xF(x) \\ &= \neg(\forall xP(x) \vee \exists yR(y)) \vee \forall xF(x) \end{aligned}$$

(2) 将否定符号深入到谓词变元之前

$$\begin{aligned} & \neg(\forall xP(x) \vee \exists yR(y)) \vee \forall xF(x) \\ &= (\exists x\neg P(x) \wedge \forall y\neg R(y)) \vee \forall xF(x) \end{aligned}$$

(3) 更改变元符号

$$\begin{aligned} & (\exists x\neg P(x) \wedge \forall y\neg R(y)) \vee \forall xF(x) \\ &= (\exists x\neg P(x) \wedge \forall y\neg R(y)) \vee \forall zF(z) \end{aligned}$$

(4) 将量词辖域扩大到整个公式

$$\begin{aligned} & (\exists x\neg P(x) \wedge \forall y\neg R(y)) \vee \forall zF(z) \\ &= \exists x\forall y\forall z(\neg P(x) \wedge \neg R(y) \vee F(z)) \end{aligned}$$

前束范式虽有优点,但也有缺点,主要是其首标比较混乱,全称量词与存在量词排列无一定规则。

1920年斯科林(Skolem)对它进行改造,使首标中所有量词具有一定规则,让存在量词均出现在全称量词之前,即首标部分由两部分

组成,前面部分是存在量词,后面部分是全称量词,如:

$$\exists x \exists y \forall z \forall t (P(x, y) \wedge Q(y, z) \wedge R(z, t))$$

是斯科林范式。

斯科林范式是比较理想的范式,它将一个公式顺序地分成三部分:公式的所有存在量词,公式的所有全称量词,命题逻辑公式。这给谓词逻辑的研究带来方便。

任何一个公式均可化归成斯科林范式,其化归过程比较复杂,这里不作介绍。

7.4 函 数

在谓词逻辑中除了引入谓词概念以外,还需引入“函数”概念。函数建立了个体变量间的转换关系。函数有一元函数与多元函数之分,一元函数有如下之形式:

$$y = f(x)$$

其中 f 为函数符, x, y 为个体变量。多元函数有如下之形式:

$$y = f(x_1, x_2, \dots, x_n)$$

其中 f 为函数符, $x_1, x_2, \dots, x_n, y$ 为个体变量。此种多元函数称为 n 元函数。

在函数中,个体经函数作用后所得的仍是个体,所以函数是个体到个体的映射。

例 7-33 王强的爸爸去南京了。

解: 设 $F(x, y)$ 为“某人 x 到 y 地方去了”, $f(x)$ 为“ x 的爸爸”。并设 a 为王强, b 为南京,此时上面的语句可写为:

$$F(f(a), b)$$

例 7-34 徐飞龙和他父亲、祖父三人一起去看演出。

解: 设 $F(x, y, z)$ 为“某人 x 、某人 y 与某人 z 一起看演出”, 设 $f(x)$ 为“ x 的父亲”, 又设 a 为徐飞龙, 此时上述语句可写为:

$$F(a, f(a), f(f(a)))$$

在谓词逻辑中加入函数后,谓词逻辑公式中增加了一个“项”的概念。

项:

(1) 个体常量是项;

(2) 个体变量是项;

(3) 设 f 为 n 元函数符, $t_1, t_2, \dots, t_n$ 为项, 则 $f(t_1, t_2, \dots, t_n)$ 是项;

(4) 项由且仅由有限次使用(1)、(2)、(3)所得。

有了项以后,原有的原子公式可作适当修改如下:

原子公式:

设 p 是 n 元谓词符, $t_1, t_2, \dots, t_n$ 为项, 则 $p(t_1, t_2, \dots, t_n)$ 是原子公式。

原子公式经修改后有关谓词逻辑公式的定义就不必修改了。

习 题 七

7.1 用谓词写出下列各断言:

(1) 长江比黄河长,金陵饭店比北京饭店高。

(2) 高斯是伟大的数学家但不是文学家。

(3) 南京位于武汉和上海之间。

(4) 他和她是兄妹。

(5) 没有不犯错误的人。

(6) 对一切实数, $x^2 > 0$ 或 $x^2 = 0$ 。

(7) 凡有生命之物必会死。

(8) 所有四边形内角之和都是 360° 。

(9) 不是所有的男人都比女人高。

(10) 凡是对顶角必相等;但相等未必是对顶角。

(11) 有而且仅有一个素数是偶数。

(12) 凡是资本家都会剥削人,但剥削人者未必都是资本家。

7.2 下面哪些是命题？

- (1) $\forall x(P(x) \rightarrow Q(x) \wedge R)$
- (2) $\forall x(P(x) \rightarrow \neg Q(x) \vee S(x) \wedge R)$
- (3) $\forall x \exists y(\neg P(x) \rightarrow Q(x) \wedge S(y))$

7.3 指出下面各式的自由变元和约束变元,并决定量词的辖域。

- (1) $\exists x((P(x) \vee R(x)) \wedge S(x)) \rightarrow \forall x(P(x) \wedge Q(x))$
- (2) $\forall x(P(x) \leftrightarrow Q(x)) \wedge \exists xR(x) \vee S(x)$
- (3) $\forall x(P(x) \wedge \exists yR(x, y))$

7.4 如果个体域是 $\{0, 1, 2, 3\}$, 消去以下各式的量词。

- (1) $\exists xR(x) \wedge \forall xS(x)$
- (2) $\forall xA(x) \wedge \forall (x)B(x)$
- (3) $\forall x\neg A(x) \vee \forall xB(x)$

7.5 若个体域是整数集, 决定下面哪些公式是真的。

- (1) $\forall x \exists y(x + y = 0)$
- (2) $\exists x \forall y(x + y = 0)$
- (3) $\exists x \forall y(x^2 + 3x - 5 > 0)$
- (4) $\forall x \exists y(x^2 - 5 = y^2)$

7.6 求下列各公式的真值(其中(3)——(11)各小题的个体域均是整数集 I)。

- (1) $\forall x(x = 1 \vee x = 2)$, 个体域是 $\{1, 2\}$
- (2) $\forall x(3 > 2 \rightarrow x \leq 3) \vee 3 > 5$, 个体域是 $\{-2, 3, 5, 6\}$
- (3) $\exists x(x > 1 \rightarrow x = 1)$
- (4) $\forall x(x^2 - 1 \geq 0)$
- (5) $\forall x(x^2 - x - 1 \neq 0)$
- (6) $\exists x(2x^2 - 3x + 1 = 0)$
- (7) $\exists x(x^2 - 3 = 0)$
- (8) $\forall x \exists y(x^2 = y)$
- (9) $\exists x \forall y(x^2 = y)$

$$(10) \forall x \exists y (y^2 = x)$$

$$(11) \exists x \forall y (y^2 = x)$$

7.7 求下面各式的前束范式:

$$(1) \neg (\forall x \exists y P(x, y) \leftrightarrow \exists x \forall y (\neg P(x, y)))$$

$$(2) \neg (\exists x \forall y P(x, y) \leftrightarrow \forall x \exists y (\neg P(x, y)))$$

$$(3) \exists x (\neg \exists y P(x, y)) \rightarrow (\exists z Q(z) \rightarrow R(x))$$

7.8 证明

$$(1) \forall x (P(x) \vee Q(x)) \Rightarrow \forall x P(x) \vee \exists x Q(x)$$

$$(2) \forall x (P(x) \rightarrow Q(x) \wedge R(x)) \wedge \exists x (P(x) \wedge Q(x)) \Rightarrow \exists x (Q(x) \wedge$$

$R(x))$

7.9 谓词公式 $(\forall x)(p(x) \vee (\exists y)R(y)) \rightarrow Q(x)$ 中变元 x 是

()

A. 自由变元

B. 约束变元

C. 既不是自由变元也不是约束变元

D. 既是自由变元也是约束变元

7.10 公式 $(\forall x)(\forall y)(P(x, y) \wedge Q(x, y)) \wedge (\exists x)P(x, y)$

中 $(\forall x)$ 的辖域是_____ ; $(\exists x)$ 的辖域是_____。

7.11 设 $C(x)$: x 是国家选手, $G(x)$: x 是健壮的, 命题“没有一个国家选手不是健壮的”, 可符号化为()

$$A. \neg (\forall x)(C(x) \wedge \neg G(x)) \quad B. \neg (\exists x)(C(x) \rightarrow \neg G(x))$$

$$C. \neg (\exists x)(C(x) \wedge \neg G(x)) \quad D. \neg (\forall x)(C(x) \rightarrow \neg G(x))$$

7.12 试将下列各式译成汉语, $p(x)$: x 是质数; $E(x)$: x 是偶数; $D(x, y)$: x 除尽 y ;

$$P(5) \underline{\hspace{2cm}}$$

$$E(2) \wedge P(2) \underline{\hspace{2cm}}$$

$$(\forall x)(D(2, x) \rightarrow E(x))$$

$$(\exists x)(E(x) \wedge D(x, 6))$$

7.13 设 $L(x)$: x 是演员; $J(x)$: x 是老师; $A(x, y)$: x 钦佩 y ;

命题“所有演员都钦佩某些老师”可符号化为()

- A. $(\forall x)L(x) \rightarrow A(x, y)$
B. $(\forall x)(L(x) \rightarrow (\exists y)(J(y) \wedge A(x, y)))$
C. $(\forall x)(\exists y)(L(x) \wedge J(y) \wedge A(x, y))$
D. $(\forall x)(\exists y)(L(x) \wedge J(y) \rightarrow A(x, y))$

7.14 $A(x)$: x 是人, $B(x)$: x 犯错误; 命题“没有不犯错误的人”可以形式化为()

- A. $(\forall x)(A(x) \wedge B(x))$ B. $\neg(\exists x)(A(x) \rightarrow \neg B(x))$
C. $\neg(\exists x)(A(x) \wedge B(x))$ D. $\neg(\exists x)(A(x) \wedge \neg B(x))$

7.15 在谓词演算中, 下列各式中正确的是()

- A. $(\exists x)(\forall y)A(x, y) \Leftrightarrow (\forall y)(\exists x)A(x, y)$
B. $(\exists x)(\exists y)A(x, y) \Leftrightarrow (\exists y)(\exists x)A(x, y)$
C. $(\exists x)(\forall y)A(x, y) \Leftrightarrow (\forall x)(\exists y)A(x, y)$
D. $(\forall x)(\forall y)A(x, y) \Leftrightarrow (\forall y)(\forall x)B(x, y)$

7.16 $\forall x(P(x)) \vee \forall x(Q(x))$ _____ $\forall x(P(x) \vee Q(x))$
 $\exists x(P(x) \vee Q(x))$ _____ $\exists x(P(x)) \vee \exists x(Q(x))$

“谓词逻辑”复习提纲

1. 主要内容

- 谓词逻辑基本概念。
- 谓词逻辑基本公式。
- 谓词逻辑的范式。

2. 复习重点

- 谓词逻辑基本公式。

3. 谓词逻辑基本概念

- 个体: 客体。

——谓词:刻划个体性质与关系。

——个体域:个体变化范围。

——全总个体域:所有考虑的个体作为论述范围。

——量词:刻划个体数量,有存在量词 $\exists$ 及全称量词之分,表示‘有一些’及‘所有’。

——约束变元与自由变元:受量词约束的个体变元称约束变元,不受量词约束的个体变元称自由变元。

——谓词逻辑公式的原子公式: $P(x_1, x_2, \dots, x_n)$ 。

——谓词逻辑公式:

(1) 原子公式是公式;

(2) $\neg A$ 是公式;

(3) $A \vee B, A \wedge B, A \rightarrow B, A \leftrightarrow B$ 是公式;

(4) $\forall x(A), \exists x(A)$ 是公式;

(5) 公式仅由(1)——(4)经有限步构成。

——函数 $y = f(x)$:个体间的转换关系

4. 谓词逻辑基本公式

- $\exists x(\neg P(x)) = \neg(\forall x P(x))$
- $\forall x(\neg P(x)) = \neg(\exists x P(x))$
- $\forall x(P(x) \vee Q) = \forall x P(x) \vee Q$
- $\forall x(P(x) \wedge Q) = \forall x P(x) \wedge Q$
- $\exists x(P(x) \vee Q) = \exists x P(x) \vee Q$
- $\exists x(P(x) \wedge Q) = \exists x P(x) \wedge Q$
- $\forall x P(x) \rightarrow Q = \exists x(P(x) \rightarrow Q)$
- $\exists x P(x) \rightarrow Q = \forall x(P(x) \rightarrow Q)$
- $Q \rightarrow \forall x P(x) = \forall x(Q \rightarrow P(x))$
- $Q \rightarrow \exists x P(x) = \exists x(Q \rightarrow P(x))$
- $\forall x(P(x) \wedge Q(x)) = \forall x(P(x) \wedge \forall x Q(x))$
- $\exists x P(x) \vee Q(x) = \exists x(P(x) \vee \exists x Q(x))$

- $\forall x P(x) \vee \forall x Q(x) \Rightarrow \forall x P(x) \vee Q(x)$
- $\exists x (P(x) \wedge \exists x Q(x)) \Rightarrow \exists x (P(x) \wedge \exists x Q(x))$
- $\forall x (P(x) \rightarrow Q(x)) \Rightarrow \forall x P(x) \rightarrow \forall x Q(x)$
- $\forall x (P(x) \rightarrow Q(x)) \Rightarrow \exists x P(x) \rightarrow \exists x Q(x)$
- $\forall x P(x) \Rightarrow P(x)$
- $P(x) \Rightarrow \exists x P(x)$
- $\forall x \forall y P(x, y) = \forall y \forall x P(x, y)$
- $\exists x \exists y P(x, y) = \exists y \exists x P(x, y)$

5. 谓词逻辑范式

——前束范式: 一个公式仅出现 $\neg$, $\vee$ 与 $\wedge$ 并且所有量均出现在最前面其辖域一直延伸止末尾。

——斯科林范式: 前束范式中量词的出现分为两部分, 首先出现存在量词, 其次出现全称量词。

第八章 命题逻辑与谓词逻辑的 公理化理论

公理化理论是数学中的基本理论,近来它在计算机科学中用处很大。我们通过本章命题逻辑与谓词逻辑公理化理论的介绍,使读者对公理化理论有一个初步的了解。

8.1 公理化理论的基本思想

自然科学中的一些理论性学科有很多规则和定理,但这些规则中有些是最基本的,使得某学科领域内的所有其他的规则和定理均可由这些最基本的规则推出,这些最基本的规则称为公理。公理可视为一门学科的基础,它的正确性是公认的,因此不需要证明。而学科领域中的其他规则和定理均可从公理出发加以证明。

更进一步,我们可以脱离具体的学科而将公理化理论作进一步抽象。也就是说我们可以定义一些脱离具体语义解释而只有语法含义的定理和规则,以此作为公理,建立起一个公理系统。这种公理系统具有广泛的抽象性。如果对公理系统中的抽象符号给予某学科领域中的具体含义后,其公理在该学科中是正确的话,则说公理系统在该学科中有一个解释。一个公理系统往往可以有多种解释,这说明一个抽象的公理系统可以作为专门学科的基础。这种抽象的公理系统我们称之为形式化公理系统,简称形式系统。

在公理系统中,一般需讨论三个问题:

1. 不矛盾性

在公理系统中要求所有的公理是互相不矛盾的。相互矛盾的公

理在表面上有时不一定能看得出来,但往往会在定理中表示出来,即可从公理系统中推出两个截然相反的定理来。不矛盾性是对一个公理系统的基本要求。

2. 完备性

公理系统的完备性可有两种含义:

(1) 相对完备性。一个公理系统如果是为某学科建立的,该学科中所有定理和规则均能在该系统中推出,则说此系统相对于该学科来说是完备的。

(2) 绝对完备性。在一个公理系统中如果将任何一个非定理的公式作为公理加入到系统后,所得的系统均为矛盾的系统,则说该系统是绝对完备的。

一个系统最好具有完备性,至少是相对完备的,但也允许不是完备的。当然不完备的公理系统不是一个好的公理系统。

3. 独立性

公理系统中的每条公理应该独立,即每条公理不可能由其他公理推出。

一个公理系统最好具有独立性,但有时为了某种方便起见,不独立的公理系统也是可以的。

8.2 命题逻辑的公理系统

现在我们讨论命题逻辑中的公理系统。它称为命题逻辑永真公式的公理系统,简称公理系统。一个完整的公理系统由两部分组成,它们是系统的组成部分和推理部分。组成部分给出了系统的基本符号和公式;推理部分给出了系统的公理、基本规则以及定理的含义。

一、系统的组成部分

基本符号：

命题： $P, Q, R, \dots$

联结词： $\neg, \vee, \wedge, \rightarrow, \leftrightarrow$

括号： $(,)$

公式：

见定义 6-1

二、推理部分

1. 公理

- (1) $P \rightarrow P$
- (2) $(P \rightarrow (Q \rightarrow R)) \rightarrow (Q \rightarrow (P \rightarrow R))$
- (3) $(P \rightarrow Q) \rightarrow ((Q \rightarrow R) \rightarrow (P \rightarrow R))$
- (4) $(P \rightarrow (P \rightarrow Q)) \rightarrow (P \rightarrow Q)$
- (5) $(P \leftrightarrow Q) \rightarrow (P \rightarrow Q)$
- (6) $(P \leftrightarrow Q) \rightarrow (Q \rightarrow P)$
- (7) $(P \rightarrow Q) \rightarrow ((Q \rightarrow P) \rightarrow (P \leftrightarrow Q))$
- (8) $P \wedge Q \rightarrow Q$
- (9) $P \wedge Q \rightarrow P$
- (10) $P \rightarrow (Q \rightarrow P \wedge Q)$
- (11) $P \rightarrow P \vee Q$
- (12) $Q \rightarrow P \vee Q$
- (13) $(Q \rightarrow P) \rightarrow ((R \rightarrow P) \rightarrow (Q \vee R \rightarrow P))$
- (14) $(P \rightarrow \neg Q) \rightarrow (Q \rightarrow \neg P)$
- (15) $\neg \neg P \rightarrow P$

2. 推理规则

分离规则： $P \rightarrow Q, P \vdash Q$ (读作对 $P \rightarrow Q, P$ 施行分离规则而得 Q)。

3. 定理

(1) 公理是定理；

(2) 如果 $P \rightarrow Q$, P 是定理, 则对它们施行分离规则所得 Q 也是定理；

(3) 定理仅限于此。

由公理系统证明一个公式 Q 是定理必须给出其证明过程。证明过程是一公式序列: $P_1, P_2, P_3, \dots, P_n$, 其中每个 $P_i (i = 1, 2, \dots, n)$ 必须满足下面条件:

(1) P_i 或者是公理之一；

(2) P_i 或是前面的 $P_k, P_r (k, r < i)$ 施行分离规则而得；

(3) 最后 P_n 即为定理 Q 。

我们便说 $P_1, P_2, \dots, P_n$ 为定理 Q 的永真证明过程。

下面我们利用公理系统证明定理, 即命题逻辑中的永真公式。

例 8-1 试证 $P \vee Q \rightarrow Q \vee P$ 为永真公式。

证明:

(1) $Q \rightarrow Q \vee P$ 公(12)

(2) $P \rightarrow Q \vee P$ 公(11)

(3) $(P \rightarrow Q \vee P) \rightarrow ((Q \rightarrow Q \vee P) \rightarrow (P \vee Q \rightarrow Q \vee P))$
公(13)

(4) $((Q \rightarrow Q \vee P) \rightarrow (P \vee Q \rightarrow Q \vee P))$ 分(3), (2)

(5) $P \vee Q \rightarrow Q \vee P$ 分(4), (1)

定理得证。

注意在定理证明中, 每个步骤后面都附有说明, 它叫证明根据, 用以说明每一步骤所用的公理或规则。其中“公”表示公理, “分”表示分离规则。

例 8-2 试证 $P \vee P \rightarrow P$ 为永真公式。

证明:

(1) $P \rightarrow P$ 公(1)

$$(2) (P \rightarrow P) \rightarrow ((P \rightarrow P) \rightarrow (P \vee P \rightarrow P)) \quad \text{公(13)}$$

$$(3) (P \rightarrow P) \rightarrow (P \vee P \rightarrow P) \quad \text{分(2), (1)}$$

$$(4) P \vee P \rightarrow P \quad \text{分(3), (1)}$$

例 8-3 试证 $P \rightarrow \neg \neg P$ 为永真公式。

证明:

$$(1) \neg P \rightarrow \neg P \quad \text{公(1)}$$

$$(2) (\neg P \rightarrow \neg P) \rightarrow (P \rightarrow \neg \neg P) \quad \text{公(14)}$$

$$(3) P \rightarrow \neg \neg P \quad \text{分(2), (1)}$$

我们现在再讨论公理系统中的推理规则。在本公理系统中只有一条分离规则,它的用处很大,由它能得到很多别的推理规则,其方法是:对于每个形如 $A(P_1, P_2, \dots, P_n) \rightarrow B(P_1, P_2, \dots, P_n)$ 的永真公式均对应一个推理规则:

$$A(P_1, P_2, \dots, P_n) \vdash B(P_1, P_2, \dots, P_n)$$

即对每个永真公式 $A(P_1, P_2, \dots, P_n) \rightarrow B(P_1, P_2, \dots, P_n)$, 如果有 $A(P_1, P_2, \dots, P_n)$ 为永真公式,则由分离规则可得 $B(P_1, P_2, \dots, P_n)$ 为永真公式,因此可由 $A(P_1, P_2, \dots, P_n)$ 推出 $B(P_1, P_2, \dots, P_n)$,记以:

$$A(P_1, P_2, \dots, P_n) \vdash B(P_1, P_2, \dots, P_n)$$

只要在公理系统中有一条蕴含型的永真公式,就可同时得到一个推理规则,由这种方法所推得的规则叫导出规则。

我们利用导出规则可以从公理系统中的 15 条公理而推得 15 条导出规则,它们是:

$$\text{规则 1} \quad P \vdash P$$

$$\text{规则 2} \quad P \rightarrow (Q \rightarrow R) \vdash Q \rightarrow (P \rightarrow R)$$

$$\text{规则 3} \quad P \rightarrow Q, Q \rightarrow R \vdash P \rightarrow R$$

$$\text{规则 4} \quad P \rightarrow (P \rightarrow Q) \vdash P \rightarrow Q$$

$$\text{规则 5} \quad P \leftrightarrow Q \vdash P \rightarrow Q$$

$$\text{规则 6} \quad P \leftrightarrow Q \vdash Q \rightarrow P$$

$$\text{规则 7} \quad P \rightarrow Q, Q \rightarrow P \vdash P \leftrightarrow Q$$

规则 8 $P \wedge Q \vdash Q$

规则 9 $P \wedge Q \vdash P$

规则 10 $P, Q \vdash P \wedge Q$

规则 11 $P \vdash P \vee Q$

规则 12 $Q \vdash P \vee Q$

规则 13 $Q \rightarrow P, R \rightarrow P \vdash Q \vee R \rightarrow P$

规则 14 $P \rightarrow \neg Q, Q \vdash \neg P$

规则 15 $\neg \neg P \vdash P$

利用导出规则还可以得到其他的所有推理规则。

到此为止,我们已知道利用此公理系统可以证明命题逻辑中的永真公式(以及推理规则),这种证明方法叫永真推理方法。这种证明方法的最大缺点是证明比较烦琐,比较难。为此要设法予以改造,其改造的方法称为假设推理法,在说明假设推理法之前,我们先引进一条推理定理。

推理定理: 设有 $A_1, A_2, \dots, A_n \vdash B$, 则必有 $A_1, A_2, \dots, A_{n-1} \vdash A_n \rightarrow B$ 。

推论: 设有 $A_1, A_2, \dots, A_n \vdash B$, 则必有:

$\vdash A_1 \rightarrow (A_2 \rightarrow (A_3 \rightarrow (\dots (A_n \rightarrow B) \dots)))$

即: $A_1 \rightarrow (A_2 \rightarrow (A_3 \rightarrow (\dots (A_n \rightarrow B) \dots)))$ 为永真。

关于这条定理的证明,已超出本书范围。

推理定理告诉我们,为了证明一个带蕴含符的复杂公式是永真的,只要证明它的最后一个后件为永真,而其所有前件(假设前提)均可作为已知条件(永真公式)使用。此种证明方法由于减少了待证成分而增加了永真成分,从而使证明变得较容易、方便,证明过程从本质上得到简化。目前我们一般采用假设推理方法。

例 8-4 试证 $(P \rightarrow (Q \rightarrow R)) \rightarrow (Q \rightarrow (P \rightarrow R))$ 为永真公式。

证明: 由推理定理可知,只要证:

$$P \rightarrow (Q \rightarrow R), Q, P \vdash R$$

(1) P

假设前提

(2) $P \rightarrow (Q \rightarrow R)$ 假设前提

(3) $Q \rightarrow R$ 分(2), (1)

(4) Q 假设前提

(5) R 分(3), (4)

定理得证。

例 8-5 试证 $(P \rightarrow Q) \rightarrow ((P \rightarrow R) \rightarrow (P \rightarrow Q \wedge R))$ 为定理。

证明：由推理定理可知,只要证：

$$P \rightarrow Q, P \rightarrow R, P \vdash Q \wedge R$$

(1) $P \rightarrow Q$ 假设前提

(2) $P \rightarrow R$ 假设前提

(3) P 假设前提

(4) Q 分(1), (3)

(5) R 分(2), (3)

(6) $Q \wedge R$ 规则 10

从上面两个例子可以看出,利用假设推理可使证明过程大大简化。

对于这个公理系统还有两点要说明。首先,可以证明这个公理系统是不矛盾的、完备的(相对完备与绝对完备),但它不是独立的。关于这点,由于证明复杂,本书不作介绍。其次我们称这个公理系统是命题逻辑公理系统,这主要是因为命题逻辑可看成此公理系统的一种语义解释。公理系统中的系统构成与命题逻辑公式构成一致,公理系统中的公理均为命题逻辑中的永真公式,因而公理系统中的定理亦为命题逻辑中的永真公式。

8.3 谓词逻辑的公理系统

本节我们讨论谓词逻辑中的公理系统,它称为谓词逻辑永真公式的公理系统,简称为公理系统。

一、系统组成部分

基本符号：

命题： $P, Q, R, \dots$

个体： $x, y, z, \dots$

谓词： F, G, H

联结词： $\neg, \vee, \wedge, \rightarrow, \leftrightarrow$

量词： $\exists, \forall$

括号： $(,)$

公式：

见定义 7-1

二、推理部分

1. 公理

- (1) $P \rightarrow P$
- (2) $(P \rightarrow (Q \rightarrow R)) \rightarrow (Q \rightarrow (P \rightarrow R))$
- (3) $(P \rightarrow Q) \rightarrow ((Q \rightarrow R) \rightarrow (P \rightarrow R))$
- (4) $(P \rightarrow (P \rightarrow Q)) \rightarrow (P \rightarrow Q)$
- (5) $(P \leftrightarrow Q) \rightarrow (P \rightarrow Q)$
- (6) $(P \leftrightarrow Q) \rightarrow (Q \rightarrow P)$
- (7) $(P \rightarrow Q) \rightarrow ((Q \rightarrow P) \rightarrow (P \leftrightarrow Q))$
- (8) $P \wedge Q \rightarrow Q$
- (9) $P \wedge Q \rightarrow P$
- (10) $P \rightarrow (Q \rightarrow P \wedge Q)$
- (11) $P \rightarrow P \vee Q$
- (12) $Q \rightarrow P \vee Q$
- (13) $(Q \rightarrow P) \rightarrow ((R \rightarrow P) \rightarrow (Q \vee R \rightarrow P))$
- (14) $(P \rightarrow \neg Q) \rightarrow (Q \rightarrow \neg P)$

$$(15) \neg \neg P \rightarrow P$$

$$(16) \forall x P(x) \rightarrow P(x)$$

$$(17) P(x) \rightarrow \exists x P(x)$$

这 17 个公理中,前 15 个与命题逻辑中的公理是相同的,公理 16 和 17 中的 $P(x)$,表示公式 P 中含有变元 x 。

2. 推理规则

$$(1) ' \text{分离规则}: P \rightarrow Q, P \vdash Q$$

$$(2) ' \text{全称规则}: Q \rightarrow P(x) \vdash Q \rightarrow \forall x P(x) \quad (\text{简称全})$$

$$(3) ' \text{存在规则}: P(x) \rightarrow Q \vdash \exists x P(x) \rightarrow Q \quad (\text{简称存})$$

3. 定理

(1) 公理是定理;

(2) 如果 $P \rightarrow Q$, P 是定理,则 Q 也是定理;

(3) 如果 $Q \rightarrow P(x)$ 是定理,则 $Q \rightarrow \forall x P(x)$ 也是定理;

(4) 如果 $P(x) \rightarrow Q$ 是定理,则 $\exists x P(x) \rightarrow Q$ 也是定理;

(5) 定理仅限于此。

由公理系统证明一个公式 Q 是定理必须给出其证明过程。证明过程是一公式序列: $P_1, P_2, \dots, P_n$, 其中每个 $P_i (i = 1, 2, \dots, n)$ 必须满足下面条件:

(1) P_i 或是诸公理之一;

(2) P_i 或是前面的 $P_k, P_r (k, r < i)$ 施行分离规则而得;

(3) P_i 或是前面的 $P_k (k < i)$ 施行全称规则而得;

(4) P_i 或是前面的 $P_k (k < i)$ 施行存在规则而得;

(5) 最后 P_n 即为定理 Q 。

我们便说 $P_1, P_2, \dots, P_n$ 为定理 Q 的永真证明过程。

下面我们利用此公理系统证明谓词逻辑中的永真公式。

例 8-6 试证 $\exists x \forall y P(x, y) \rightarrow \forall y \exists x P(x, y)$ 为定理。

证明:

- $$\begin{aligned}
(1) & (\forall y P(x, y) \rightarrow P(x, y)) \rightarrow ((P(x, y) \rightarrow \exists x P(x, y)) \\
& \rightarrow (\forall y P(x, y) \rightarrow \exists x P(x, y))) \quad \text{公(3)} \\
(2) & \forall y P(x, y) \rightarrow P(x, y) \quad \text{公(16)} \\
(3) & (P(x, y) \rightarrow \exists x P(x, y)) \rightarrow (\forall y P(x, y) \rightarrow \exists x P(x, y)) \\
& \quad \text{分(1), (2)} \\
(4) & P(x, y) \rightarrow \exists x P(x, y) \quad \text{公(17)} \\
(5) & \forall y P(x, y) \rightarrow \exists x P(x, y) \quad \text{分(4), (3)} \\
(6) & \forall y P(x, y) \rightarrow \forall y \exists x P(x, y) \quad \text{全(5)} \\
(7) & \exists x \forall y P(x, y) \rightarrow \forall y \exists x P(x, y) \quad \text{存(6)}
\end{aligned}$$

定理得证。

本公理系统共有三条推理规则,其中全称规则还可以以另外的形式出现,即

- $$(4)' P(x) \rightarrow \forall x P(x) \quad (\text{全称推广规则,简称 UG})$$

我们只要在全称规则中将 Q 用 $x \vee \neg x$ 代入即可得到。由公理 16 和公理 17 可得到两条导出规则,即:

- $$\text{规则 16: } \forall x P(x) \vdash P(x) \quad (\text{全称指定规则,简称 US})$$

- $$\text{规则 17: } P(x) \vdash \exists x P(x) \quad (\text{存在推广规则,简称 EG})$$

在这公理系统中也存在推理定理。

推理定理: 设有 $R_1, R_2, \dots, R_n \vdash Q$, 且推理过程中对 R_i 不作代入, 各 R_i 至少被使用一次且在施行全称规则与存在规则时绝不对各 R_i 中的自由变元进行, 则必有:

$$R_1, R_2, \dots, R_{n-1} \vdash R_n \rightarrow Q$$

推论: 设有 $R_1, R_2, \dots, R_n \vdash Q$, 且在推理过程中对 R_i 不作代入, 各 R_i 至少被使用一次且在施行全称规则与存在规则时绝不对各 R_i 中的自由变元进行, 则必有:

$$\vdash R_1 \rightarrow (R_2 \rightarrow (R_3 \rightarrow (\dots (R_n \rightarrow Q) \dots)))$$

即:

$$R_1 \rightarrow (R_2 \rightarrow (R_3 \rightarrow (\dots (R_n \rightarrow Q) \dots)))$$

为永真公式。

关于这条定理的证明,本书从略。

由推理定理可以得出下面的规则:

规则 18: $\exists xP(x) \vdash P(e)$ (存在指定规则简称 ES)

这条规则中, $P(e)$ 中的 e 叫额外变元,它是一种额外假设的自由变元,它的变化范围是使 $\exists xP(x)$ 成立的 x ,因而与一般自由变元不同,各个不同额外变元的变化范围亦不同。

利用推理定理可以引入假设推理法,在这个公理系统中,充分利用 UG、US、EG、ES 规则可使推理过程变得简单,但使用 UG 及 ES 规则时有一些限制条件,现叙述如下。

使用全称推广规则 UG 时必须遵守:

- (1) 对假设前提中所出现的自由变元不能使用此规则;
- (2) 对额外变元不能使用此规则;
- (3) 一个公式中若含有额外变元,则对这公式中的自由变元亦不能使用此规则。

因为不同的额外变元变化的范围是不同的,因此使用存在指定规则 ES 时要注意的:不同的额外变元需用不同的符号表示,以示区别,而且不能相互作代入。

在推理时可利用 US 和 ES 将一个公式中的量词全部除去,从而得到一个命题逻辑公式,然后利用命题逻辑中的方法推理,最后在得到结论前利用 UG 与 EG 重新加入量词,使它恢复成谓词逻辑公式。要注意的是在使用规则时要严格遵守某些限制。

例 8-7 试证明下面公式是永真公式:

$$\forall x(P(x) \rightarrow Q(x)) \rightarrow (\forall xP(x) \rightarrow \forall xQ(x))$$

证明: 用假设推理只要证明:

$$\forall x(P(x) \rightarrow Q(x)), \forall xP(x) \vdash \forall xQ(x)$$

- | | |
|--|---------|
| (1) $\forall x(P(x) \rightarrow Q(x))$ | 假设前提 |
| (2) $P(x) \rightarrow Q(x)$ | US: (1) |
| (3) $\forall xP(x)$ | 假设前提 |
| (4) $P(x)$ | US: (3) |

(5) $Q(x)$ 分(2), (4)

(6) $\forall xQ(x)$ UG: (5)

定理得证。

例 8-8 试证下面公式是永真公式:

$$\exists x \forall y A(x, y) \rightarrow \forall y \exists x A(x, y)$$

证明: 用假设推理只要证明:

$$\exists x \forall y A(x, y) \vdash \forall y \exists x A(x, y)$$

(1) $\exists x \forall y A(x, y)$ 假设前提

(2) $\forall y A(e, y)$ ES: (1)

(3) $A(e, y)$ US: (2)

(4) $\exists x A(x, y)$ EG: (3)

(5) $\forall y \exists x A(x, y)$ UG: (4)

对这个公理系统还要说明两点: 首先, 可以证明这个系统是不矛盾的, 它是相对完备的, 但不是绝对完备的, 也不是独立的。其次, 我们称这系统为谓词逻辑公理系统, 这主要是因为谓词逻辑可看成这个公理系统的一种语义解释。公理系统中的系统构成与谓词逻辑构成一致。公理系统中的公理是谓词逻辑中的永真公式, 因而公理系统中的定理也是谓词逻辑中的永真公式。

习 题 八

8.1 试述公理化的特点。

8.2 试证命题逻辑永真公式公理系统中公理 1 不是独立的。

8.3 试用假设推理方法证明下面的定理:

$$(1) (R \rightarrow P) \rightarrow ((R \rightarrow Q) \rightarrow (R \rightarrow P \wedge Q))$$

$$(2) (P \wedge Q \rightarrow R) \rightarrow (P \rightarrow (Q \rightarrow R))$$

8.4 指出下面证明过程的错误之处:

$\exists x P(x) \wedge \exists x Q(x) \rightarrow \exists x (P(x) \wedge Q(x))$ 的“证明”如下:

$$(1) \exists x P(x) \wedge \exists x Q(x)$$

(2) $\exists xP(x)$

(3) $\exists xQ(x)$

(4) $P(e)$

(5) $Q(e)$

(6) $P(e) \wedge Q(e)$

(7) $\exists x(P(x) \wedge Q(x))$

8.5 试述假设推理法之特点及优越性。

8.6 试用假设推理证明下面的定理：

(1) $\forall x(P(x) \rightarrow Q(x)) \rightarrow (\exists xP(x) \rightarrow \exists xQ(x))$

(2) $\forall x \forall y P(x, y) \rightarrow \forall y \forall x P(x, y)$

“命题逻辑与谓词逻辑公理化理论”复习提纲

1. 主要内容

——公理系统的基本概念。

——公理系统的结构。

——永真推理、假设推理。

——命题逻辑公理系统。

——谓词逻辑公理系统。

2. 复习重点

——公理系统的结构。

——命题逻辑公理系统。

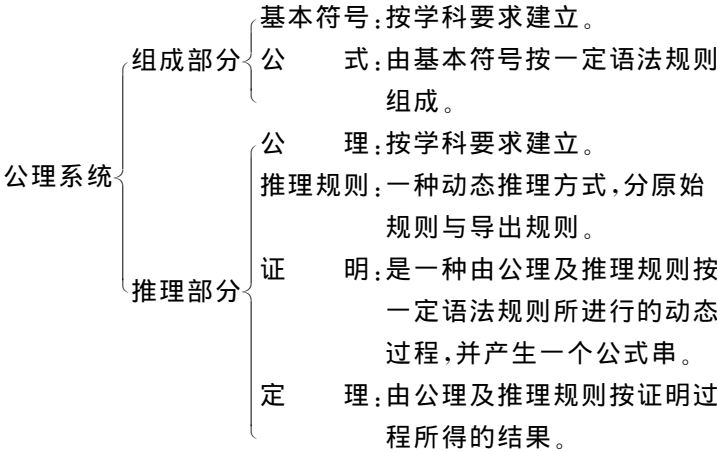
3. 基本概念

——公理：学科领域中最基本的原理与规则。

——公理系统：以公理为基础所建立的基于一定语法规范的形式系统。

——公理系统的三大性质:不矛盾、完备性与独立性。

——公理系统的结构:



——假设推理:设有 $A_1, A_2, \dots, A_n \vdash B$ 则必有: $A_1 \rightarrow (A_2 \rightarrow (\dots (A_n \rightarrow B) \dots))$ 。

4. 命题逻辑公理系统

——基本符号:命题、联结词及括号。

——公式:(略)。

——公理:

- $P \rightarrow P$ 。
- $P \rightarrow (Q \rightarrow R) \rightarrow (Q \rightarrow (P \rightarrow R))$ 。
- $(P \rightarrow Q) \rightarrow ((Q \rightarrow R) \rightarrow (P \rightarrow R))$ 。
- $(P \rightarrow (P \rightarrow Q)) \rightarrow (P \rightarrow Q)$ 。
- $(P \leftrightarrow Q) \rightarrow (P \rightarrow Q)$ 。
- $(P \leftrightarrow Q) \rightarrow (Q \rightarrow P)$ 。
- $(P \rightarrow Q) \rightarrow ((Q \rightarrow P) \rightarrow (P \leftrightarrow Q))$ 。
- $(P \wedge Q) \rightarrow Q$ 。
- $(P \wedge Q) \rightarrow P$ 。

- $P \rightarrow (Q \rightarrow P \wedge Q)$ 。
- $P \rightarrow P \vee Q$ 。
- $Q \rightarrow P \vee Q$ 。
- $(P \rightarrow Q) \rightarrow ((R \rightarrow P) \rightarrow (Q \vee R \rightarrow P))$ 。
- $(P \rightarrow \neg Q) \rightarrow (Q \rightarrow \neg P)$ 。
- $\neg \neg P \rightarrow P$ 。

——推理规则：

- 分离规则： $P \rightarrow Q, P \vdash Q$ 。
- 导出规则：公理系统中每条蕴含永真式。

5. 谓词逻辑公理系统

——基本符号：命题、个体、谓词、联结词、量词及括号。

——公式：(略)。

——公理：命题逻辑公式的 15 条公理加： $\forall x P(x) \rightarrow P(x)$ 及 $P(x) \rightarrow \exists x P(x)$ 。

——推理规则：分离规则、全称推广规则 UG、全称指定规则 US、存在推广规则 EG、存在指定规则 ES 及导出规则。

第九章 离散数学在计算机科学中的应用

任何一门学科在其研究过程中常常需要借助一些工具和方法。计算机科学在其研究过程中也需要借助数学工具,这个数学工具即是离散数学。离散数学对计算机发展和计算机科学的研究起着重要的作用。远在计算机产生之前,即 1936 年,图灵(A. M. Turing)在研究能行性理论过程中建立了有名的图灵机理论,图灵机的出现为计算机的诞生从理论上奠定了基础。在计算机发展初期,利用命题逻辑、布尔代数理论研究开关电路,从而建立起一门完整的数字逻辑理论,对计算机的逻辑设计起了很大作用。在近期,利用代数结构研究编码理论,利用谓词逻辑研究程序正确性问题,利用能行性理论(如递归函数论)研究计算机中的可计算性理论。最近几年研究范围越来越深入,如用图论研究数据结构、操作系统的结构与死锁问题,用关系代数、谓词逻辑研究数据库等。为了了解离散数学与计算机科学的关系,我们在这章准备介绍离散数学的几个应用,它们是:离散数学在关系数据库中的应用,谓词逻辑在逻辑程序设计中的应用及代数结构在编码理论中的应用。从中可以看到离散数学在这些领域中是如何发挥作用的,也可以看到如何将一个实际问题抽象为一个数学问题,经过数学研究后又应用到实际中去的全过程。

9.1 离散数学在关系数据库中的应用

1. 关系数据库简介

数据库是计算机管理数据的一种机构,一般来讲,它由两部分组成,一个是供存放数据用的大量存储空间,它们可以是磁盘、光盘、磁

带等外存空间,另一个是管理数据库中数据的一组程序,这组程序叫数据库管理系统简称 DBMS,用户可以通过数据库管理系统所提供的语言使用数据库中的数据,这种使用包括下列几个方面:

- (1) 数据的检索:从数据库中取出满足一定条件要求的数据。
- (2) 数据的插入:将一些数据存储到数据库中供以后使用。
- (3) 数据的修改:修改数据库中指定的数据。
- (4) 数据的删除:删除数据库内指定的数据。

供用户使用数据库的语言有的从终端装置打入,这种语言一般叫终端查询语言,简称为 SQL;有的可附属于某些宿主语言,如可附属于 FORTRAN、COBOL 等语言作为这些语言的扩充成分。

数据库内的数据一般都按一定格式组织与存放,数据库内数据的基本组织格式如下:

(1) 实体:实体是数据库中数据的基本存放单位,如职工的简历、工资单、课程概貌、合同执行情况、物资供销情况等均是实体,数据库内实体是一个整体,它内部的数据相互间是有逻辑联系的。

(2) 属性:实体都有一些性质,这些性质叫此实体的属性,如职工简历这个实体就有姓名、性别、年龄等属性,所有实体的属性就组成了这个实体,如职工简历这个实体实际上就由姓名、性别、年龄等属性组成。

(3) 属性域:实体的每个属性的表现形式都是统一的,如姓名是由 n 个字母所组成的字,性别为 $\{M, F\}$ 中之一(M 代表男性, F 代表女性),年龄由两个数字所组成,对每个属性它有一个表示范围,如姓名这个属性的表示范围是 n 个由 26 个字母所组成的集合中的字母,而性别的表示范围是集合 $\{M, F\}$,年龄的表示范围是从 18 到 65 间的 48 个数字(这里假定职工参加工作年龄是 18 周岁,退休年龄最晚是 65 岁),这种属性的表示范围就是属性域,每个属性都有一个属性域。

(4) 实体集:凡具有相同结构形式(即属性与属性域)的实体

集合。

(5) 联系：在数据库中实体是基本的数据单位，但是各实体间是有一定联系的，如实体集学生与课程之间有联系，这个联系是学生修读课程，教师也是实体，而教师与学生、课程也有联系。在数据库中存储数据时不仅要存放实体的数据，而且要存放联系的数据，如上例中，不仅要存放有关教师、学生、课程的实体，而且还要存放学生修读何种课程的情况及教师教授何种课程的情况，只有这样数据库中的这个数据信息才是完整的。

数据库目前可以有三种结构模型，它们分别叫层次模型、网络模型和关系模型。用关系模型作为结构模型的数据库叫关系式数据库。我们在这里只讨论关系式数据库，其他的两种结构模型就不再作介绍了。

在关系数据库中数据按二维表的形式存放，这种二维表就叫关系，数据库中的实体与联系均按这种二维表的形式存放。

二维表的形式如表 9-1 所示，它包括有行和列。一张二维表可有 m 行 n 列，二维表的每一行叫元组，它代表一个完整的数据。一个元组有 n 个分量，因此这个元组又叫 n 元元组。二维表的每一列表示数据的分量。这种二维表叫 n 元关系。

表 9-1

二维表的形式

n 列					
					
					
					

m 行

设一个实体 A 有 n 个属性，分别为 $A_1, A_2, A_3, \cdots, A_n$ ，它可表示如下：

$$A(A_1, A_2, \dots, A_{n-1}, A_n)$$

这个实体可以允许存放 m 个数据,此时这个实体集可用一个关系表示之,亦即可用一张二维表表示之,这张二维表的每一列是一个属性,二维表的每一行可存放实体集中的一个实体,这个表示实集的二维表见表 9-2。

表 9-2 实体集 A 的关系

A_1	A_2	A_3		A_{n-1}	A_n	} m 行

现在我们举几个例子,设有实体集 S 表示学生概况,它有四个属性:学号、姓名、年龄、所属系名,分别可用 $S^\#$ 、 SN 、 SA 及 SD 表示,这个实体集存放 10 个学生的概况,它们可用下列关系(表 9-3)表示。

表 9-3 实体集 S 的关系

$S^\#$	SN	SA	SD
01	AB	20	CS
02	AC	21	MA
03	AD	22	MA
04	AE	21	CS
05	AF	20	CS
06	AG	20	CS
07	AH	22	MA
08	AI	23	MA
09	AJ	21	CS
10	AK	19	MA

又设有实体集课程的概况 C ,它有三个属性:课程号、课程名、先

修课号,它们分别用 $C^\#$ 、 CN 、 $PC^\#$ 表示之,(我们假定每门课的先修课有且只有一门),这个实体集存放六门课的概况,它们可用下列关系(表 9-4)表示。

表 9-4 实体集 C 的关系

$C^\#$	CN	$PC^\#$
01	OS	02
02	PL	05
03	DB	06
04	ML	05
05	MC	06
06	DS	04

实体集与实体集间的联系也可用关系表示,如学生修读课程的情况可用学号与课程号构成一个新关系 SC ,它刻划学生修课情况,这个关系可用二维表 9-5 表示。

表 9-5 联系 SC 的关系

$S^\#$	$C^\#$
01	01
01	02
02	01
02	02
02	03
03	05
04	04
04	05
04	06
05	01
05	05
06	01
07	01

续表

S [#]	C [#]
07	02
08	04
08	06
09	01
09	03
09	05
10	04
10	06

有时,在关系所表示的联系中还可以附加一些数据,如关系 SC 中还可以加入学生修读课程的成绩 CG,这时可在原关系中增加一个属性 CG 表示之,这个修改后的关系还可叫 SC,以后我们常用这种修改后的 SC,这种修改后的关系 SC 可用二维表 9-6 表示。

表 9-6 修改后的关系 SC

S [#]	C [#]	CG
01	01	90
01	02	80
02	01	90
02	02	80
02	03	87
03	05	74
04	04	98
04	05	94
04	06	92
05	01	60
05	05	55
06	01	88

续表

S [#]	C [#]	CG
07	01	77
07	02	67
08	04	98
08	06	97
09	01	87
09	03	85
09	05	81
10	04	73
10	06	79

从上面表示可以看出,数据实体集与联系均可用二维表表示,在数据库中,用这种二维表构造数据的模型就叫关系式数据库。

用户使用关系式数据库就是对一些二维表进行检索、插入、修改和删除等操作,关系式数据库中的数据库管理系统必须向用户提供使用数据库的语言,一般称为数据子语言,这种语言目前是以关系代数或谓词逻辑中的方法表示的,说得确切一些就是这种语言以关系代数或谓词逻辑作为它的数学基础。由于用这种数学的方法去表示,使得对这些语言的研究成为对关系代数或谓词逻辑的研究,优化语言的表示变成为对关系代数与谓词逻辑的化简问题。由于引入了数学表示方法,使得关系数据库具有比其他几种数据库较为优越的条件,正因为如此,关系数据库近几年来发展迅速,目前已成为占领市场的主流产品。

2. 关系代数与数据子语言

由前面我们知道,关系数据库的数据子语言,它的基本操作对象是二维表,它的基本操作是插入、检索、修改与删除,为了用数学的方法表示语言,有必要对其操作对象与基本操作加以研究,并将其抽象成数学符号与运算。

(1) 二维表与 n 元有序组的集合

二维表是数据子语言的操作对象,一张二维表可看成是若干元组的集合,而 n 元元组可视为一个 n 元有序组,因此一张二维表可看成是 n 元有序组的集合,故我们说,数据子语言的操作对象是 n 元有序组的集合。

(2) 基本操作与集合运算

数据子语言的操作对象是集合,而对其对象操作可视为对集合的运算,下面对几种基本操作分别加以研究。

① 检索与集合运算

我们先考虑对一张二维表的检索,对它的检索不外乎选择表中满足某些条件的一些行和列,例如对表 9-3 表示的二维表 S ,要求年龄大于 21 岁的学生的学号与姓名,这是一种检索操作,它要求选择满足 $SA>21$ 的那些行,再由这些行中选出属性学号与学生,这种检索操作的结果还是一张二维表,这张二维表有两个属性以及一些满足 $SA>21$ 的行,可用表 9-7 表示。

表 9-7 满足 $SA>21$ 的关系

$S^{\#}$	SN
03	AD
07	AH
08	AI

由此可见检索是由一张表到另一张表的操作,从数学观点看,检索是一种一元运算,即一个集合通过此运算而得到另一个集合,因此我们定义两种一元检索运算,一个叫选择,另一个叫投影。

定义 9-1 设有关系 R ,它由 m 个 n 元元组组成,则 $\Pi_{a_{i1},a_{i2},\dots,a_{in}}(R)$ 也是一个关系,它由 m 个 i_n 元元组组成,而每个元组由属性 $a_{i1}, a_{i2}, \dots, a_{in}$ 组成,这个运算叫做 R 在属性 $a_{i1}, a_{i2}, \dots, a_{in}$ 上的投影($a_{i1}, a_{i2}, \dots, a_{in}$ 均是 R 的属性)。

所以投影运算是从二维表选择一些指定的列而组成的新表,下

面我们看二个例。

例 9-1 打印全体学生名单。

解：我们可将这要求写为：

$$\Pi_{SN}(S)$$

例 9-2 打印所有课程号和课程名。

解：我们可将此要求写为：

$$\Pi_{c^{\#},CN}(C)$$

按这二个例所得的公式,我们可以从表 S 、 C 分别得到两张新表 (表 9-8 和表 9-9),详细写出如下：

表 9-8	$\Pi_{SN}(S)$	表 9-9	$\Pi_{C,CN}(C)$
	$S^{\#}$	$C^{\#}$	CN
	01	01	OS
	02		
	03	02	PL
	04		
	05	03	DB
	06	04	ML
	07		
	08	05	MC
	09		
	10	06	DS

定义 9-2 设有关系 R ,则 $\sigma_F(R)$ 也是关系,它由 R 中满足条件 F 的元组所组成, F 为逻辑条件,它是一个命题公式,它按下列方法组成：

- (1) 它的基本操作数是常量或元组分量(即属性)。
- (2) 由基本操作数通过比较运算($<$, $=$, $>$, $\leq$, $\geq$)而构成命题。
- (3) 由命题通过命题联结词($\neg$, $\vee$, $\wedge$)构成命题公式。

这种运算叫 R 的选择运算。

所以选择运算是从二维表中选出那些满足 F 的元组而组成新

表,下面我们看两个例子。

例 9-3 取出年龄大于 21 岁的数学系学生的概况。

解:我们可以将此要求写为:

$$\sigma_{SA>21 \wedge SD=MA}(S)$$

例 9-4 取出先行课程号为 02 的课程概况。

解:此要求可写为:

$$\sigma_{PC^{\#}=02}(C)$$

将运算 Π 与 σ_F 联合应用于关系就可以从关系中检索出所要求的任意行与列的内容,现举两例。

例 9-5 取出学号为 04 的学生所有修读课程号以及其分数。

解:我们可以将此要求写为:

$$\Pi_{c^{\#},CG}\sigma_{S^{\#}=04}(SC)$$

例 9-6 打印所有计算机系学生的名单。

解:我们可以将此要求写为

$$\Pi_{SN}\sigma_{S^{\#}=CS}(S)$$

这样我们可以用两个一元运算 Π 及 σ_F 检索一张二维表的内容,但是我们已经讲过,各实体间是有联系的,亦即各表之间是有联系的,因此我们可以检索与几张表有关的内容。如我们要检索学生名为 AI 所修读课程的课程号,这种检索就要牵涉到两张表,一张是 S 另一张是 SC。对于这种检索,上述的两个一元运算显然已经不够,因此我们需要引入另外的新的运算,即笛卡尔乘积。

定义 9-3 设关系 R、S 分别为 n 及 m 元,则 $R \times S$ 也是一个关系,它有 $n+m$ 元,它的元组的前 n 个分量取自 R 中的元组,而其后 m 个分量取自 S 中的元组,因此,它共有 $n \times m$ 个元组,这种二元运算 $R \times S$ 叫 R 和 S 的笛卡尔乘积。

下面我们举一个关于笛卡尔乘积的例。

例 9-7 设有关系 R 和 S(见表 9-10(a)和(b)),求 R 和 S 的笛卡尔乘积。

解：两个关系 R 与 S 的笛卡尔乘积见表 9-10(c)。

表 9-10 $R \times S$

(a) R			(b) S			(c) $R \times S$					
A	B	C	D	E	F	A	B	C	D	E	F
a	b	c	b	g	a	a	b	c	b	g	a
d	a	f	d	a	f	a	b	c	d	a	f
c	b	d				d	a	f	b	g	a
						d	a	f	d	a	f
						c	b	d	b	g	a
						c	b	d	d	a	f

从笛卡尔乘积的定义可以看出,这种运算是将两张表联成一张表的运算,如果我们所要检索的内容牵涉到两张表,此时只要先用这个运算将两张表统一成一张表,然后再用投影和选择就会找出所需检索的内容。

但是在大多数情况下两张相联表之间均有一定关系,亦即两张表中均有相同的分量,如表 S 与 SC 间有相同的分量 $S^\#$,表 C 与 SC 间有相同的分量 $C^\#$,而我们需要相联后的表是由那些在公共分量处有相等内容的元组构成。因此我们在笛卡尔乘积基础上再引入一个二元运算叫自然联接。

定义 9-4 设有 n 元关系 R 和 m 元关系 S , R 有属性 $r_1, r_2, \dots, r_n$, S 有属性 $s_1, s_2, \dots, s_m$, 其中属性 $s_1, s_2, \dots, s_p$ 分别与属性 $r_{n-p}, r_{n-p+1}, \dots, r_n$ 相同,此时可定义 R 与 S 的自然联接 $R \bowtie S$ 如下:

$$R \bowtie S = \Pi_{r_1, r_2, \dots, r_n, s_{p+1}, s_{p+2}, \dots, s_m, \sigma_{s_1=r_{n-p} \wedge \dots \wedge s_p=r_n}}(R \times S)$$

现在举几个自然联接的例子。

例 9-8 设 R 与 S 均为三元关系,其二维表见表 9-11(a)和(b),求 $R \bowtie S$ 。

解: 关系 R 与 S 的自然联接 $R \bowtie S$ 为五元关系,其二维表见(c)。

表 9-11

$R \bowtie S$

(a)R			(b)S			(c) $R \bowtie S$				
A	B	C	C	D	E	A	B	C	D	E
1	2	3	6	5	1	1	2	3	5	4
2	1	6	4	1	3	2	1	6	5	1
3	6	4	3	5	4	3	6	4	1	3

例 9-9 找出学生的姓名为 AI 所修读课程的课程号。

解：这个检索与表 S 及 SC 有关,故首先用自然联接将 S 与 SC 联成一张表,然后再在联接后的表中用 Π 与 σ_F 找出所需内容,故可写成为：

$$\Pi_{c^{\#}} \sigma_{SN=AI} (S \bowtie SC)$$

例 9-10 找出学生的学号为 03 所修读课程的课程名。

解：这个检索与表 SC 与 C 有关,因此先用自然联接将 SC 与 C 联成一张表,然后再在联接后的表中用 Π 与 σ_F 找出所需内容,故可写为：

$$\Pi_{CN \sigma_{s^{\#}} = 03} (SC \bowtie C)$$

同样的道理,如果一个检索涉及到三张表,则可用两次自然联接将三张表联成一张表,然后再对这一张表用两个一元运算 Π 与 σ_F ,最后可求得检索所要求的内容。下面举一例。

例 9-11 打印学生姓名为 AI 所修读课程的课程名。

解：这个检索牵涉到三张表,因此有：

$$\Pi_{CN \sigma_{SN}} = AI (S \bowtie SC \bowtie C)$$

到此为止,我们介绍了有关检索的几个例子,其中二个一元运算二个二元运算,这四个运算实际上只要三个就够了,因为自然联接可用其余三个运算表示之,有了这几个运算后,对二维表的检索就完成了。

② 插入、修改和删除操作与集合运算

所谓插入操作就是在关系中增加一些元组,为完成这种操作我

们可以引入另一个集合运算。从集合论中我们已经知道,这种操作相当于集合的并运算。

例 9-12 设有关系 R 如表 9-12 所示,现在在 R 中增加关系 S 中的所有元组, S 如下表,试求增加后的关系。

解: 关系 R 增加 S 的元组后所得的关系为 $R \cup S$,见下表。

表 9-12			$R \cup S$		
关系 R			关系 S		
A	B	C	A	B	C
1	2	5	4	3	1
2	1	3			
5	4	3	2	4	1

关系 $R \cup S$		
A	B	C
1	2	5
2	1	3
5	4	3
4	3	1
2	4	1

例 9-13 设某系开设课程之概况由关系 C 表示之(见表 9-4),现增设两门课为

$C^\#$	CN	$PC^\#$
07	PP	05
08	RP	07

请将此两门课之概况插入关系 C 中。

解: 我们构造一个新关系 C' 如表 9-13 所示:

表 9-13		关系 C'	
$C^\#$	CN	$PC^\#$	
07	PP	05	
08	RP	07	

此时关系 C 经插入关系 C' 后所构成的关系为 $C \cup C'$,其表读者不难作出,留作练习。

所谓删除操作是在关系中除去一些元组,为完成此操作我们也

要引入一个集合运算,这种操作相当于集合的差运算。

例 9-14 设有关系 R 如下表所示,现在在 R 中除去关系 S 中所出现的元组,关系 S 见下表,试求除去后的关系。

表 9-14

关系 R

A	B	C
1	2	4
2	1	5
3	7	1

R-S

关系 S

A	B	C
1	2	4
3	7	1

关系 $R-S$

A	B	C
2	1	5

解: 关系 R 中除去 S 中所出现的元组后所得的关系为 $R-S$ (见表 9-14)。

例 9-15 设某校学生概貌由关系 S 表示,现有两个学生因病退学,因此需要从 S 中除去,设这两学生之学号为 03、05,求除名后之学生概貌。

解: 我们先求病退学生概况表,它们是:

$$\sigma_{S^{\#}=03 \wedge S^{\#}=05}(S)$$

其次求除名后之学生概貌表,它们是:

$$S - \sigma_{S^{\#}=03 \wedge S^{\#}=05}(S)$$

最后谈所谓修改操作。它是将 R 中某些元组的内容作适当修改。例如学生 AD 由数学系转入计算机系,实际上是将表 9-3 中的关系 S 中 AD 的元组中的系名属性 SD 由 MA 修改成 CS 。

完成修改操作不需要引入新的集合运算。我们知道修改操作相当于对须修改的元组进行删除操作,然后将修改好的新元组作插入操作。因此相应的集合运算是先进行差运算再作并运算。

例 9-16 设有关系 R ,现欲将其分量 A 为 04 的元组修改成关系 S 所示的状态。求修改后的关系。其中 R 、 S 见下表 9-15(a)、(b)。

表 9-15

(a) 关系 R

A	B	C
01	ROM	381
02	RAM	467
03	PAM	541
04	UAM	446

例 9-16 之关系表

(b) 关系 S

A	B	C
04	UAM	441

(c) 关系 $(R - \sigma_{A=04}(R)) \cup S$

A	B	C
01	ROM	381
02	RAM	467
03	PAM	541
04	UAM	441

解：对关系 R 修改后的关系为：

$$(R - \sigma_{A=04}(R)) \cup S$$

它可用表 9-15(c)表示之。

(3) 数据子语言与关系代数

综上所述我们可以知道，在关系数据库中需要向用户提供使用数据库的数据子语言。这个数据子语言可以允许用户对数据库进行检索、插入、修改及删除操作。这种数据子语言相当于一种代数结构，而这个代数结构的研究对象是 n 元有序组的集合，对它一共有五种基本操作，其中两个是一元运算三个是二元运算，它们是：

投影运算： $\Pi(R)$ 。

选择运算： $\sigma_F(R)$ 。

笛卡尔乘积： $R \times S$ 。

并运算： $R \cup S$ 。

差运算： $R - S$ 。

这些运算都是封闭的。因此它们构成了一个代数系统，称为关系代数。

由此可见，对关系式数据库中的数据子语言的研究可归结为对关系代数的研究，这样就建立了关系代数与数据子语言间的联系。

要注意的是，在上面的运算中自然联接并不出现，这是因为自然联接并不是基本运算符，它可以由其他运算符生成。

(4) 数据子语言的优化与关系代数

在关系数据库中，用户用数据子语言使用数据库，相同的要求有

例如,设一用户希望了解学生 AC 修读课程 PL 的成绩,对它有几种不同的写法:

这三种写法表示了相同的检索要求,但是具有极不相同的效率,其中①的效率最低,关键是它所执行的自然联接运算所花的时间较长。③的效率最高,主要是由于它所执行的自然联接运算所花时间最短,这是因为执行自然联接的关系 $\Pi_{S^{\#}} \sigma_{SN=AC}(S)$ 、 SC 、与 $\Pi_{C^{\#}} \sigma_{CN=PL}(C)$ 的元组数与元数远远少于关系 S 、 SC 及 C 。我们从表 9-16(a)和(b)中可以看出这三个关系中有二个很简单,其中(a)是关系 $\Pi_{S^{\#}} \sigma_{SN=AC}(S)$, (b)是关系 $\Pi_{C^{\#}} \sigma_{CN=PL}(C)$ 。对它们执行自然联接所需时间远远少于对 S 、 SC 及 C 所执行自然联接的时间。②的效率比①高得多,但比③低,它介于①与③之间。

(a)

$S^\#$

02

(b)

$C^\#$

02

• 313 •

① 笛卡尔乘积的结合律：

$$(R_1 \times R_2) \times R_3 = R_1 \times (R_2 \times R_3)$$

② 投影的串接：

$$\Pi_{A_1, A_2, \dots, A_n} (\Pi_{B_1, B_2, \dots, B_m} (R)) = \Pi_{A_1, A_2, \dots, A_n} (R)$$

其中 $A_i \in \{B_1, B_2, \dots, B_m\}$

③ 选择的串接：

$$\sigma_{F_1 \wedge F_2} (R) = \sigma_{F_1} (\sigma_{F_2} (R))$$

④ 选择与投影的交换：

$$\begin{aligned} \sigma_F (\Pi_{A_1, A_2, \dots, A_n} (R)) &= \Pi_{A_1, A_2, \dots, A_n} (\sigma_F (R)), \\ \Pi_{A_1, A_2, \dots, A_n} (\sigma_F (R)) \\ &= \Pi_{A_1, A_2, \dots, A_n} (\sigma_F (\Pi_{A_1, A_2, \dots, A_n, B_1, B_2, \dots, B_n} (R))) \end{aligned}$$

⑤ 选择与笛卡尔乘积：

若 F 只涉及 R_1 , 则 $\sigma_F (R_1 \times R_2) = \sigma_F (R_1) \times R_2$

若 F 只涉及 R_2 , 则 $\sigma_F (R_1 \times R_2) = R_1 \times \sigma_F (R_2)$

若 $F = F_1 \wedge F_2$, 而 F_1 只涉及 R_1 , F_2 只涉及 R_2 , 则：

$$\sigma_F (R_1 \times R_2) = \sigma_{F_1} (R_1) \times \sigma_{F_2} (R_2)$$

若 $F = F_1 \wedge F_2$, 而 F_1 只涉及 R_1 , 则：

$$\sigma_F (R_1 \times R_2) = \sigma_{F_2} (\sigma_{F_1} (R_1) \times R_2)$$

⑥ 投影与笛卡尔乘积：

$$\Pi_{A_1, \dots, A_n} (R_1 \times R_2) = \Pi_{B_1, \dots, B_m} (R_1) \times \Pi_{C_1, \dots, C_k} (R_2)$$

这里 A_i 中 B_j 仅与 R_1 有关, C_r 仅与 R_2 有关。

我们可以用上述六组等式通过等式转换实现数据语言的优化。

例 9-17 $\Pi_{SN} \sigma_{SA > 21} (S \times SC)$

$$\begin{aligned} &= \Pi_{SN} (\sigma_{SA > 21} (S) \times SC) \\ &= \Pi_{SN} (\sigma_{SA > 21} (S)) \times \Pi_0 (SC) \\ &= \Pi_{SN} (\sigma_{SA > 21} (S)) \times \emptyset \\ &= \Pi_{SN} (\sigma_{SA > 21} (S)) \end{aligned}$$

其中: Π_0 表示在空属性上的投影。

例 9-18 $\Pi_{S^\#} . CN \sigma_{SD = MA \wedge C^\# = 05} (S \times C)$

$$= \Pi_{S^{\#}, CN} ((\sigma_{SD=MA}(S)) \times (\sigma_{C^{\#}=05}(SC)))$$

$$= \Pi_{S^{\#}} (\sigma_{SD=MA}(S)) \times \Pi_{CN} (\sigma_{C^{\#}=05}(C))$$

例 9-19

$$\begin{aligned} & \Pi_{S^{\#}, C^{\#}} (\sigma_{SD=MA \wedge PC^{\#}=05} (\Pi_{SD, S^{\#}}(S)) \times (\Pi_{C^{\#}, PC^{\#}}(C))) \\ &= \Pi_{S^{\#}, C^{\#}} ((\sigma_{SD=MA} (\Pi_{SD, S^{\#}}(S))) \times \bar{v} (\sigma_{PC^{\#}=05} (\Pi_{C^{\#}, PC^{\#}}(C)))) \\ &= \Pi_{S^{\#}} (\sigma_{SD=MA} (\Pi_{SD, S^{\#}}(S))) \times \Pi_{C^{\#}} \\ & \quad (\sigma_{PC^{\#}=05} (\Pi_{C^{\#}, PC^{\#}}(C))) \\ &= \Pi_{S^{\#}} (\Pi_{SD, S^{\#}} (\sigma_{SD=MA}(S))) \times \Pi_{C^{\#}} \\ & \quad (\Pi_{C^{\#}, PC^{\#}} (\sigma_{PC^{\#}=05}(C))) \\ &= \Pi_{S^{\#}} (\sigma_{SD=MA}(S)) \times \Pi_{C^{\#}} (\sigma_{PC^{\#}=05}(C)) \end{aligned}$$

从上面三个例子可以看出,在数据子语言中,可以用关系代数的等式转换以简化表示,达到提高效率的目的。

由上面所述,我们也可以看出如何将关系数据库的数据子语言抽象成关系代数,又如何用关系代数的方法优化数据子语言的全过程。

3. 谓词逻辑与数据子语言

关系数据库中数据子语言除了可以用关系代数表示外,还可以用谓词逻辑表示,叫关系演算。

(1) 集合论与谓词逻辑

关系代数是基于集合论的,而关系演算是基于谓词逻辑的,要建立关系代数与关系演算间的联系,其首要的理论基础是要建立集合论与谓词逻辑间的联系,下面将讨论此问题。

首先,我们知道,任一个集合必有一个谓词(或谓词逻辑公式)与之对应,如自然数集合 N 必有一个自然数谓词 $N(x)$ 与之对应,使之当 x 为自然数时 $N(x)$ 为真, x 为非自然数时 $N(x)$ 为假,即:

$$N(x) = \begin{cases} 1 & \text{当 } x \text{ 为自然数} \\ 0 & \text{当 } x \text{ 为非自然数} \end{cases}$$

故我们可用谓词逻辑公式去表示与刻划集合,这个公式可叫集

合的特性谓词(或特性公式)。集合 A 与其特性公式 $P(x)$ 间可有如下之关系：

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

这样,我们就可以建立集合与公式间的一一对应关系如下：

集合	谓词逻辑公式
A	$P(x)$
$x \in A$	$P(x) = 1$
$x \notin A$	$P(x) = 0$

设有集合 A 与 B , 它们的特性谓词分别为 $P(x)$ 和 $Q(x)$, 则此两集合可分别写为：

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

$$B = \{x \mid Q(x)\}$$

并且有：

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

$$A \cup B = \{x \mid P(x) \vee Q(x)\}$$

$$A \cap B = \{x \mid P(x) \wedge Q(x)\}$$

$$A - B = \{x \mid P(x) \wedge \neg Q(x)\}$$

$$A + B = \{x \mid P(x) \oplus Q(x)\}$$

这样,我们就建立了集合论与谓词逻辑公式间的如下一一对应关系：

集合论	谓词逻辑公式
A	$P(x)$
B	$Q(x)$
$\bar{A}$	$\neg P(x)$
$A \cup B$	$P(x) \vee Q(x)$
$A \cap B$	$P(x) \wedge Q(x)$
$A - B$	$P(x) \wedge \neg Q(x)$
$A + B$	$P(x) \oplus Q(x)$

此外,还可以有：

集合论

谓词逻辑公式

全集 $\cup$

永真公式 $P(x) \vee \neg P(x)$

空集 $\emptyset$

永假公式 $P(x) \wedge \neg P(x)$

$A=B$

$P(x)=Q(x)$

$A \neq B$

$P(x) \neq Q(x)$

$A \supseteq B$

$P(x) \Rightarrow Q(x)$

(2) 二维表与谓词逻辑

从关系代数看,关系数据库中的基本数据结构二维表是一个 n 元有序组的集合。在谓词逻辑中,这个集合可以用一个谓词,逻辑特性公式表示,下面我们用两个例子来加以说明。

例 9-20 表 9-17 所列之二维表可用谓词 $F(x, y) = (x = y) \wedge N(x)$ 表示。其中 $N(x)$ 表示 x 为自然数。

例 9-21 表 9-18 所列之二维表可用谓词 $F(x, y) = (x = y + 1) \wedge \left(\frac{y}{2} = \left\lfloor \frac{y}{2} \right\rfloor \right) \wedge N(y)$ 表示。

表 9-17 例 9-20 之关系表

x	y
1	1
2	2
3	3
4	4
5	5
$\vdots$	$\vdots$

表 9-18 例 9-21 之关系表

x	y
3	2
5	4
7	6
9	8
11	10
$\vdots$	$\vdots$

(3) 基本操作与谓词逻辑

数据子语言的操作对象二维表可用谓词公式表示,而对其对象的操作也可用谓词公式表示,但这种谓词公式与传统谓词公式略有不同。

基本符号:

个体变量:如 $x, y, z, \dots$ (相当于二维表中属性变量)。

个体常量:如 $a, b, c, \dots$ (相当于二维表中数据)。

谓词符:如 $P, Q, R, \dots$ (相当于二维表名)。

函数符:如 $f, g, h, \dots$ (相当于数据库中的公式)。

联结符: $\wedge, \vee, \neg, \rightarrow$ 。

量词: $\exists, \forall$ 。

括号: $(,)$ 。

项:

① 个体变量是项;

② 个体常量是项;

③ 设 $t_1, t_2, \dots, t_n$ 是项, f 是函数符, 则 $f(t_1, t_2, \dots, t_n)$ 是函数,

函数是项;

④ 项由且仅由上述①~③经有限步骤生成。

原子公式:

① 刻划二维表的谓词 $R(x_1, x_2, \dots, x_n)$ 是原子公式, 其中 x_i 为二维表中的属性变量。

② $x_i \theta x_j$ 是原子公式, x_i, x_j 为个体变量, θ 为比较符 ($<, >, =, \leq, \geq$)。

③ $x_i \theta a, a \theta x_i$ 是原子公式, 其中 x_i 为个体变量, a 为个体常量。

④ 原子公式由且仅由上面三种形式组成。

下面我们定义谓词公式:

定义 9-5 一个谓词公式(可简称公式)可定义如下:

① 原子公式是公式;

② R, S 是公式, 则 $(\neg R), (R \wedge S), (R \vee S)$ 及 $(R \rightarrow S)$ 是公式;

③ R 是公式, 则 $\exists x R(x), \forall x R(x)$ 是公式;

④ 公式由且仅由上述①~③经有限步骤构成。

下面我们利用谓词公式刻划基本操作。我们先讨论插入、删除和修改。在关系代数中我们知道可以用并运算与差运算分别表示插入与删除, 而在谓词逻辑中我们知道并运算相当于联结词“或

者”，而差运算相当于联结词“并且”再在第二项中加以否定。这样我们设：

$$R = \{ (x_1, x_2, \cdots, x_n) \mid P(x_1, x_2, \cdots, x_n) \}$$

$$S = \{ (x_1, x_2, \cdots, x_n) \mid Q(x_1, x_2, \cdots, x_n) \}$$

则有：

基本操作	关系代数	逻辑公式
插入	$R \cup S$	$\{ (x_1, x_2, \cdots, x_n) \mid P(x_1, x_2, \cdots, x_n) \vee Q(x_1, x_2, \cdots, x_n) \}$
删除	$R - S$	$\{ (x_1, x_2, \cdots, x_n) \mid P(x_1, x_2, \cdots, x_n) \wedge \neg Q(x_1, x_2, \cdots, x_n) \}$

而修改操作是由删除和插入两个操作组合而成的，因此删除、插入既然可由谓词刻划，修改也可由谓词刻划。

接着我们要讨论检索。用上面类似的办法，投影、选择、笛卡尔乘积也可用谓词公式来表示，设有 $R = \{ (x_1, x_2, \cdots, x_n) \mid P(x_1, x_2, \cdots, x_n) \}$ ， $S = \{ (y_1, y_2, \cdots, y_m) \mid Q(y_1, y_2, \cdots, y_m) \}$ ，则有：

基本操作	关系代数	谓词逻辑
投影	$\Pi_{x_{i_1}, x_{i_2}, \cdots, x_{i_k}}(R)$	$\{ (x_{i_1}, x_{i_2}, \cdots, x_{i_k}) \mid \exists x_{i_1} \exists x_{i_2} \cdots \exists x_{i_n} P_{(x_1, x_2, \cdots, x_n)} \}$
选择	$\sigma_F(R)$	$\{ (x_1, x_2, \cdots, x_n) \mid P(x_1, x_2, \cdots, x_n) \wedge F \}$
笛卡尔乘积	$R \times S$	$\{ (x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_m) \mid P(x_1, x_2, \cdots, x_n) \wedge Q(y_1, y_2, \cdots, y_m) \}$

这样，我们把关系数据库中的数据子语言变成谓词逻辑中的谓词公式，因而可以用谓词公式研究数据子语言。

利用上面所定义的谓词公式对关系数据库的研究所形成的理论叫关系演算。可以证明，关系代数与关系演算在理论上是等价的。

* 中 $\{x_{i_1}, x_{i_2}, \cdots, x_{i_k}, x_{j_1}, x_{j_2}, \cdots, x_{j_r}\} = \{x_1, x_2, \cdots, x_n\}$ ，而 x_{i_p} 与 x_{j_q} 间均各不相同。

利用关系演算可进一步研究基于关系数据库的演绎数据库、知识库以及智能数据库理论等。

(4) 关系演算的若干例子

我们可以用关系演算中的公式表示关系数据库中的数据操作，在实际应用中它可以很方便地对数据作检索及增、删、改操作，下面我们举几个例子。

我们以表 9-3、9-4 及 9-6 所定义的二维表 S 、 C 及 SC 作为操作对象，并定义它们的谓词分别为： $S(S^\#, SN, SA, SD)$ ， $C(C^\#, CN, PC^\#)$ 以及 $SC(S^\#, C^\#, CG)$

例 9-22 打印全体学生名单。

解：我们可将这个要求写为：

$$\exists S^\# \exists SA \exists SD S(S^\#, SN, SA, SD)$$

例 9-23 打印所有课程号和课程名。

解：我们可将此要求写为：

$$\exists PC^\# C(C^\#, CN, PC^\#)$$

例 9-24 取出年龄大于 21 岁的数学系学生概况。

解：我们可将此要求写为：

$$S(S^\#, SN, SA, SD) \wedge SA > 21$$

例 9-25 取出先行课程号为 02 的课程情况。

解：我们可将此要求写为：

$$C(C^\#, CN, PC^\#) \wedge PC^\# = 02$$

例 9-26 取出学号为 04 的学生所修读课程号及其分数。

解：我们可将此要求写为：

$$\exists S^\# SC(S^\#, C^\#, CG) \wedge S^\# = 04$$

例 9-27 打印所有计算机系学生的名单。

解：我们可将此要求写为：

$$\exists S^\# \exists SA \exists SD S(S^\#, SN, SA, SD) \wedge SD = CS$$

例 9-28 找出学生姓名为 AI 所修读课程的课程号。

解：我们可将此要求写为：

$$\exists S^\# \exists SN \exists SA \exists SD \exists CG (S(S^\#, SN, SA, SD) \\ \wedge SC(S^\#, C^\#, CG) \wedge SN = AI)$$

例 9-29 找出学生学号为 03 所修读课程的课程名。

解：我们可将此要求写为：

$$\exists S^\# \exists CG \exists C^\# \exists PC^\# (SC(S^\#, C^\#, CG) \\ \wedge C(C^\#, CN, PC^\#) \wedge S^\# = 03)$$

例 9-30 打印学生姓名为 AI 所修读课程的课程名。

解：我们可将此要求写为：

$$\exists S^\# \exists SN \exists SA \exists SD \exists C^\# \exists CG \exists PC^\# (S(S^\#, SN, SA, CD) \\ \wedge SC(S^\#, C^\#, CG) \wedge C(C^\#, CN, PC^\#) \wedge SN = AI)$$

例 9-31 在学生中插入如下之元组：

(030,王家松,27,CS)

解：我们令能插入之元组的谓词为 S' ，此时有：

$$S(S^\#, SN, SA, SD) \vee S'(S^\#, SN, SA, SD)$$

例 9-32 在课程中删除课程号为 07 的课程。

解：我们可将此要求写为：

$$C(C^\#, CN, PC^\#) \wedge \neg (C(C^\#, CN, PC^\#) \wedge C^\# = 07)$$

(5) 关系演算的公理系统

近年来对基于关系演算的关系式数据库的理论研究有了进一步发展，这就是关系演算的公理系统，该公理系统由三部分（三组公理）组成，即特殊化公理、事实性公理、演绎性公理。

① 特殊化公理

特殊化公理给出了关系数据库满足的条件或假设的参考环境，它们共 4 条。

公理 9.1.1 完全性公理

设关系数据库有二维表 R ，它有元组：

$$(e_{1,1}, e_{1,2}, \dots, e_{1,n}) \\ (e_{2,1}, e_{2,2}, \dots, e_{2,n}) \\ \dots\dots\dots$$

$$(e_{m,1}, e_{m,2}, \dots, e_{m,n})$$

此时必有：

$$\begin{aligned} & \forall_{x_1} \forall_{x_2} \cdots \forall_{x_u} (R(x_1, x_2, \dots, x_u) \rightarrow \\ & (x_1 = e_{1,1} \wedge x_2 = e_{1,2} \wedge \cdots \wedge x_n = e_{1,n}) \\ & \vee (x_1 = e_{2,1} \wedge x_2 = e_{2,2} \wedge \cdots \wedge x_n = e_{2,n}) \vee \cdots \\ & \vee (x_1 = e_{m,1} \wedge x_2 = e_{m,2} \wedge \cdots \wedge x_n = e_{m,n})) \end{aligned}$$

完全性公理给出了关系数据库中一个二维表有且仅有的元组。

关系数据库中每个二维表均有这样一个公理。

公理 9.1.2 惟一性公理

设关系数据库中有几个个体 $e_1, e_2, \dots, e_n$ ，此时惟一性公理可写为：

$$\begin{aligned} & (e_1 \neq e_2) \\ & (e_1 \neq e_3) \\ & \dots\dots \\ & (e_1 \neq e_n) \\ & (e_2 \neq e_3) \\ & \vdots \\ & \vdots \\ & (e_2 \neq e_n) \\ & \vdots \\ & \vdots \\ & \vdots \\ & (e_{n-1} \neq e_n) \end{aligned}$$

惟一性公理表示关系数据库中每个个体必惟一。

公理 9.1.3 域封闭公理

域封闭公理可表示如下：

$$\forall_x (x = e_1 \vee x = e_2 \vee \cdots \vee x = e_n)$$

此公理给出了关系数据库中个体变量的变化范围。此公理告诉我们，个体变量的变域必须在惟一性公理所规定的个体之内。

以上三个公理给出了关系数据库中个体常量、个体变量及二维表的限制条件。

最后一条是相等性公理,这主要是因为在前面三条公理中都用到到了相等性概念,相等性是一个谓词可叫相等谓词,因此需对其作定义,相等性公理即是对相等谓词作定义的公理。

公理 9.1.4 相等性公理

自反性: $\forall_x (x = x)$

对称性: $\forall_x \forall_y (x = y \rightarrow y = x)$

传递性: $\forall_x \forall_y \forall_z (x = y \wedge x = z \rightarrow y = z)$

等项替代原理: $\forall_{x_1} \forall_{x_2} \cdots \forall_{x_n} \forall_{y_1} \forall_{y_2} \cdots \forall_{y_m} (P(x_1, x_2, \cdots, x_n)$

$\wedge x_1 = y_1 \wedge x_2 = y_2 \wedge \cdots \wedge x_n = y_n \rightarrow P(y_1, y_2, \cdots, y_n))$

以上四个公理构成了关系数据库的特殊化公理。

② 事实性公理

关系数据库中所有数据都以二维表的元组形式出现,所有这些元组都作为事实性公理。

公理 9.2 事实性公理

设关系数据库有元组 $(e_1, e_2, \cdots, e_n)$, 如有:

$$(e_1, e_2, \cdots, e_n) \in R$$

则必有:

$$R(e_1, e_2, \cdots, e_n)$$

③ 演绎性公理

演绎性公理给出了关系数据库中的演绎性规则。在关系数据库中,模式定义、窗口等均由演绎性规则形式,它们可用演绎性公理给出。

演绎性公理一般以蕴含式形式表示。

关系演算公理系统所采用的推理方法、定理及证明过程与谓词逻辑一样。谓词逻辑中的公理由于是永真,因此在关系演算中也可认为是公理。关系数据库中的操作如检索等即是公理系统中的定理。而增、删、改操作则是对公理系统的重整。

9.2 离散数学与纠错码

1. 纠错码简单介绍

我们知道,在计算机和数据通信中,经常需要将二进制数字信号进行传递,这种传递的距离近则数米、数十米,远则超过数千公里。在传递信息过程中,由于存在着各种干扰,可能会使二进信号产生失真现象。即在传递过程中二进信号 0 可能会变成 1,而 1 可能会变成 0。图 9-1 是一个二进制信号传递的简单模型,它有一个发送端和一个接收端,二进信号串 $X = x_1x_2 \cdots x_n$ 从发送端发出经传递介质而至接收端。由于存在着各种干扰对传递介质的影响,因而接收端收到的二进信号串 $X' = x'_1x'_2 \cdots x'_n$ 中的 x_i 可能不一定就与 x'_i 相等,从而产生了二进制信号的传递错误。

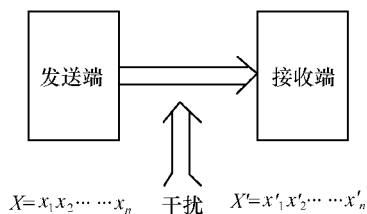


图 9-1 数据通信中信号干扰图示

由于计算机中和数据通信系统中的信号传递是如此的频繁与广泛,因此,如何防止传输错误就变得相当重要了,当然,要解决这个问题可有不同的途径。人们所想到的第一个途径是提高设备的抗干扰能力和信号的抗干扰能力。但是,大家都知道,这种从物理角度去提高抗干扰能力并不能完全消除错误的出现。第二个途径就是这一节所要讲的采用纠错码的方法,以提高抗干扰能力。这种纠错码的方法是从编码上下功夫,使得二进数码在传递过程中一旦出错,在接收端的纠错码装置就能立刻发现错误,并将其纠正。由于这种方法简单易行,因此目前在计算机中和数据通信系统中被广泛地采用。采用这种方法后,二进制信号传递模型就可以变成如图 9-2 所示的模型了。

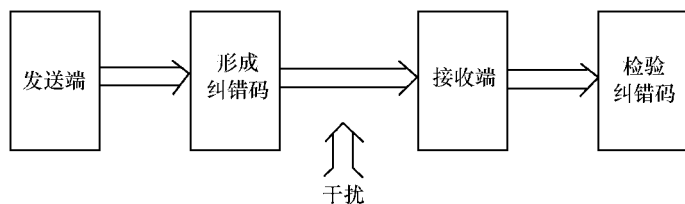


图 9-2 数据通信中纠错码的应用图示

从这个模型可以看到,当二进制信号串从发送端发送时,需按规定转换成具有抗干扰能力的纠错码,然后才发送出去。在接收端,当收到二进制信号串后即对收到的纠错码进行检验,查对在途中是否失真,如失真即负责纠正。

这个模型的一个典型实现,就是在远程数据传输系统中具纠错能力的数据传输装置,如图 9-3 所示。

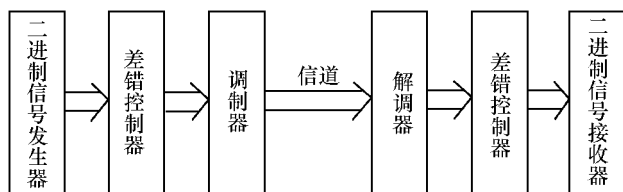


图 9-3 有纠错能力的数据传输装置

从图中可以看出,二进制信号发生器发出信号(二进制信号发生器可以是计算机,或者是由人控制的某些装置如终端),经差错控制器形成纠错码,然后经调制器使二进制信号变成为适宜于信道传播的电信号,这种信号通过信道传输至接收端首先通过解调器将其还原成原来的二进制信号,再经差错控制器检验经信道传输后是否产生失真,并采取措施进行纠正。经纠正后的二进制信号送入二进制信号接收器,从而完成整个传输过程。二进制信号接收器可以是计算机或其他接收装置如终端等。

但是,为什么纠错码具有发现错误、纠正错误的能力呢?纠错码

又是按什么样的原则去编的呢？为了说明这些问题，我们首先要介绍一些基本概念。

首先我们说由 0、1 所组成的串称为字，一些字的集合称为码。码中的字称为码字，不在码中的字称为废码。码中的每个二进制信号 0 或 1 称为码元。

我们下面举出几个关于纠错码的例子。

设有长度为 2 的字，它们一共可有 $2^2=4$ 个，它们所组成的字集 $S_2=\{00,01,10,11\}$ 。当我们选取编码为 S_2 时，这种编码不具有抗干扰能力。因为当 S_2 中的一个字如 10 在传递过程中其第一个码元 1 变成 0，因而整个字成为 00 时，由于 00 亦为 S_2 中的字，故我们并不能发现传递中是否出错。但是，当我们如选取 S_2 的一个子集 $C_2=\{00,11\}$ 作为编码时就会发生另一种完全不同的情况。因为此时，01、10 均为废码，而当 11 在传递过程中第一个由 1 变成 0，即整个字成为 01 时，由于 01 是废码，因而我们发现传递过程中出现了错误。对 00 也有同样的情况。但是，这种编码有一个缺点，即它只能发现错误而不能纠正错误，因此我们还需要选择另一种能纠错的编码。现在我们考虑长度为 3 的字，它们一共可有 $2^3=8$ 个，在它们所组成的字集 $S_3=\{000,001,010,011,100,101,110,111\}$ 中我们选取编码 $C_3=\{001,110\}$ 。利用此种编码我们不但能发现错误而且能纠正错误。因为码字 001 出现错误后将变为：000、011、101，而码字 110 出现错误后将变为 111、100、010。故如码字 001 在传递过程中任何一个码元出现了错误（例如第一个码元由 0 变成 1），整个码字就会变成 101、011 或 000，但是都可知其原正确码为 001。对于原来正确的码字 110 也有类似的情况。故对编码 C_3 ，我们不但能发现错误还能纠正错误。当然，上述之编码尚有一个缺点，它只能发现并纠正单个错误。当错误超过两个码元时它就既无力发现，更无法纠正了。

2. 纠错码的纠错能力

我们前面已看出按 C_2 编码仅能发现单个错误，按 C_3 编码可发

现单个错误并纠正单个错误,可以看出,不同的编码具有不同的纠错能力。可是,编码方式与纠错能力间到底有什么必然的联系呢?为此,我们需对其作较为详细的研究。

我们先定义一个代数系统。

设 S_n 是长度为 n 的字位串集,即:

$$S_n = \{x_1 x_2 \cdots x_n \mid x_i = 0 \vee x_i = 1\}$$

在 S_n 上定义一个运算 $\oplus$, 设 $X = x_1 x_2 \cdots x_n, Y = y_1 y_2 \cdots y_n$, 则有:

$$Z = x \oplus y = z_1 z_2 \cdots z_n$$

其中 $z_i = x_i \oplus y_i (i=1, 2, \cdots, n)$, 而运算符 $\oplus$ 为按位加。

S_n 中的任两个元素作运算 $\oplus$ 后仍在 S_n 内, 故它是封闭的。因此 $(S_n, \oplus)$ 是一个代数系统。

定理 9-1 代数系统 $(S_n, \oplus)$ 是群。

证明: $(S_n, \oplus)$ 满足结合律。它的单位元素是 $\overbrace{000 \cdots 0}^n$, S_n 的逆元素是它自己。因此, $(S_n, \oplus)$ 是群。

定义 9-6 S_n 的任一子集 C , 如果 $(C, \oplus)$ 是群, 则称码 C 是群码。

定义 9-7 S_n 中的两个元素, $X = x_1 x_2 \cdots x_n, Y = y_1 y_2 \cdots y_n$, 我们令:

$$H(X, Y) = \sum_{i=1}^n (x_i \oplus y_i)$$

我们称 $H(X, Y)$ 为 X 与 Y 的汉明距离。

从定义可以看出, X 和 Y 的汉明距离是 X 和 Y 中对应位码元不同的个数。设 S_3 中两个码字为 000 和 011, 这两个码字的汉明距离为 2。而 000 与 111 的汉明距离为 3。

定理 9-2 设 $X, Y, Z \in S_n$, 则我们有:

$$(1) H(X, X) = 0$$

$$(2) H(X, Y) = H(Y, X)$$

$$(3) H(X, Y) + H(Y, Z) \geq H(X, Z)$$

证明：(1)、(2)是显然的。对(3)我们有：

$$\begin{aligned} H(X,Y) + H(Y,Z) &= \sum_{i=1}^n (x_i \oplus y_i) + \sum_{i=1}^n (y_i \oplus z_i) \\ &= \sum_{i=1}^n ((x_i \oplus y_i) + (y_i \oplus z_i)) \\ &\geq \sum_{i=1}^n (x_i \oplus z_i) = H(X,Z) \end{aligned}$$

定义 9-8 一个码 C 中所有不同码字的汉明距离的极小值称为码 C 的最小距离,记为 $d_{\min}(C)$ 。亦即有：

$$d_{\min}(C) = \min_{\substack{X,Y \in C \\ X \neq Y}} (H(X,Y))$$

例如

$$\begin{aligned} d_{\min}(S_2) &= d_{\min}(S_3) = 1 \\ d_{\min}(C_2) &= 2 \\ d_{\min}(C_3) &= 3 \end{aligned}$$

下面我们给出两个定理,它们刻划了编码方式与纠错能力间的关系。

定理 9-3 一个码 C 能检查出不超过 k 个错误的充分必要条件是：

$$d_{\min}(C) \geq k+1$$

证明：充分性。设有： $d_{\min}(C) \geq k+1$ 。又设 C 中码字 X 经传递后变成 X' 。如传递过程中产生错误且错误位数 $r \leq k$,则有 $H(X, X') = r \leq k$ 且 $X \neq X'$ 。又对 C 中任一不为 X 之码字 Y ,我们有：

$$H(X,Y) \geq d_{\min}(C) \geq k+1 > H(X,X')$$

故可知 $X' \notin C$,所以可知 X' 是废码。充分性得证。

必要性。设码 C 能检查出不超过 k 个错误,这表示与一码字的汉明距离不超过 k (且 >0)的所有字都是废码。故可知码 C 中任两码字的汉明距离至少为 $k+1$ 。故有：

$$d_{\min}(C) \geq k+1$$

定理 9-4 码 C 能纠正 k 个错误的充分必要条件是：

$$d_{\min}(C) \geq 2k + 1$$

证明：充分性。设 $d_{\min}(C) \geq 2k + 1$ ，又设 $X \in C$ 经传送后变成 X' 。 $H(X, X') = k$ ，对任一 $Y \in C$ 且 $Y \neq X$ ，因为：

$$H(X', Y) \geq d_{\min}(C) \geq 2k + 1$$

所以有：

$$H(X', Y) \geq H(X, Y) - H(X, X') \geq (2k + 1) - k = k + 1$$

根据最小距离译码原则*， X' 可纠正成 X 。充分性得证。

必要性。设码 C 能纠正 k 个错。我们用反证法，如 $d_{\min}(C) \leq 2k$ ，则存在 $X, Y \in C$ ， $H(X, Y) \leq 2k$ 。由定理可知 $H(X, Y) \geq k + 1$ ， X 与 Y 中至少 $k + 1$ 位不同，设发送字 X 经传递后变成 X' ，而 X' 与 X 中有 k 位不同，且这 k 位刚好是 X 与 Y 不同位的一部分。又因为 $H(X, Y) \leq 2k$ ，所以有 X' 与 Y 的不同位数 $\leq k$ ，即 $H(X', Y) \leq k$ 。根据最小距离译码原则，如果 $H(X', Y) < k$ ，则 X' 可错误地纠正成 Y 。如 $H(X', Y) = k$ ，则 X' 可纠正为 X 或 Y 。故此时不能纠正 k 个错误，与假设矛盾。由此必要性得证。

上述两个是很重要的定理。它给出了编码最小距离的大小与检错、纠错能力的关系。下面我们用这两个定理看几个例子。

例 9-33 我们前面讲过 $C_2 = \{00, 11\}$ 能检出单个错误。因 $d_{\min}(C_2) = 2 = 1 + 1$ ，故可以查出一个错。

例 9-34 我们前面讲过 $C_3 = \{000, 111\}$ 能纠正单个错误，因 $d_{\min}(C_3) = 3 = 2 \times 1 + 1$ ，故可以纠正单个错误。

例 9-35 我们前面讲过的编码 S_2, S_3 分别包括了长度为 2、3 的所有的码，因而：

$$d_{\min}(S_2) = d_{\min}(S_3) = 1$$

可知 S_2, S_3 既不能查错又不能纠错。从这个例子中也可看出，一个编码中如包含了某长度的所有码，则此种编码一定无抗干扰能力。

* 所谓最小距离译码原则，即是给定码 C ，设接收字为 X' ，而 X' 为废码时，我们总可以在 C 中找出一个码字 X ，使得有 $H(X, X') = \min_{Y \in C} H(Y, X')$ ，此时可将 X' 译为 X 。

例 9-36 我们来考察一种叫奇偶校验码的编码。我们知道编码 $S_2 = \{00, 01, 10, 11\}$ 没有抗干扰能力。但我们可以在 S_2 的每个码字后增加一位(叫奇偶校验位), 这一位的设置是这样安排的, 它使每个码字所含 1 的个数为偶数个。按这种方法编码后 S_2 就变成为:

$$S'_2 = \{000, 011, 101, 110\}$$

而它的最小距离 $d_{\min}(S') = 2$, 故由定理 9-3 可知, 它可以检出单个错误。而事实也是如此, 当传递过程中发生了单个错误则码字就变成含有奇数个 1 的废码。

类似地, 增加奇偶校验位使码字所含 1 的个数为奇数个时也可得到相同的结果。

可以将这个结果推广到 S_n 中去, 不管 n 多大, 只要增加一奇偶校验位总可能查出一个错误。这种奇偶校验码在计算机中是使用得很普遍的一种纠错码, 它的优点是所付的代价较小(只要增加一位附加的奇偶校错位), 而且这种码的生成与检查也很简单, 它的缺点是不能纠正错误。

3. 纠错码的选择

我们知道 S_2 无纠错能力, 但在 S_2 中选取 C_2 后, C_2 具有发现单错之能力。同样, S_3 无纠错之能力。从这里可以看出, 如何从一些编码中选取一些码字组成新码, 使其具有一定的纠错能力, 是一个很重要的课题。在这节中我们将讨论这个问题。

我们先从一个例子开始讲起。在计算机中经常使用一种编码叫汉明码, 它是 1950 年由汉明提出的, 这种编码能发现并纠正一个错误。

先讲汉明码的一个特例, 设有编码 S_4 , S_4 中每个码字为 $a_1 a_2 a_3 a_4$, 若增加三位校验位 a_5, a_6, a_7 , 从而使它成为长度为 7 的码字 $a_1 a_2 a_3 a_4 a_5 a_6 a_7$ 。其中校验位 a_5, a_6, a_7 应满足下列方程:

$$a_1 \oplus a_2 \oplus a_3 \oplus a_5 = 0 \quad (1)$$

$$a_1 \oplus a_2 \oplus a_4 \oplus a_6 = 0 \quad (2)$$

其次,它能纠正一个错误。因为当 C 中码字发生单错后,不同的字位错误可使方程中不同的等式不成立。如当 a_3 发生错误时则必有方程(1)、(3)不成立,而当 a_2 发生错误时则必有方程(1)、(2)不成立。方程中 3 个等式的八种组合可对应 $a_1 - a_7$ 的 7 个码元中每个码的错误以及一个正确无错的码字。为讨论方便起见,我们建立 3 个谓词:

$$P_1(a_1, a_2 \cdots a_7): a_1 \oplus a_2 \oplus a_3 \oplus a_5 = 0$$

$$P_2(a_1, a_2 \cdots a_7): a_1 \oplus a_2 \oplus a_4 \oplus a_6 = 0$$

$$P_3(a_1, a_2 \cdots a_7): a_1 \oplus a_3 \oplus a_4 \oplus a_7 = 0$$

这 3 个谓词的真假与对应等式是否成立相一致。

我们建立 3 个集合 S_1, S_2, S_3 分别对应 P_1, P_2, P_3 。我们令:

$$S_1 = \{a_1, a_2, a_3, a_5\}$$

$$S_2 = \{a_1, a_2, a_4, a_6\}$$

$$S_3 = \{a_1, a_3, a_4, a_7\}$$

显然, S_i 是使 P_i 为假的所有可能出错字位的集合。我们可构成下面 7 个非空集合:

$$S_1 \cap S_2 \cap S_3 = \{a_1\}$$

$$S_1 \cap S_2 \cap \bar{S}_3 = \{a_2\}$$

$$S_1 \cap \bar{S}_2 \cap S_3 = \{a_3\}$$

$$S_1 \cap S_2 \cap \bar{S}_3 = \{a_5\}$$

$$\bar{S}_1 \cap S_2 \cap S_3 = \{a_4\}$$

$$\bar{S}_1 \cap S_2 \cap \bar{S}_3 = \{a_6\}$$

$$\bar{S}_1 \cap \bar{S}_2 \cap S_3 = \{a_7\}$$

从这 7 个集合我们可以决定出错位。例如 $\bar{S}_1 \cap S_2 \cap S_3 = \{a_4\}$, 即表示 $a_4 \notin S_1, a_4 \in S_2, a_4 \in S_3$ 。所以如 a_4 出错, 则必有 P_1 为真, P_2, P_3 为假。反之亦然。照此类推, 我们可以得到表 9-20。这样, 我们就看出这种编码 C 能纠正一个错误。

我们可以将这个例子予以适当抽象提高。首先, 方程(1)、(2)、(3)可用矩阵的形式表示:

$$\vec{X} \cdot \mathbf{H}^T = \mathbf{0}'$$

表 9-20

纠错对照表

P_1	P_2	P_3	出 错 字 母
1	1	1	无
1	1	0	a_7
1	0	1	a_6
1	0	0	a_4
0	1	1	a_5
0	1	0	a_3
0	0	1	a_2
0	0	0	a_1

其中 $\vec{X} = (a_1, a_2, \dots, a_7)$, 而 $\mathbf{H}$ 为:

$$\mathbf{H} = \begin{Bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{Bmatrix}$$

$\mathbf{H}^T$ 则是 $\mathbf{H}$ 的转置矩阵。

从这里可以看出, 一个编码可由矩阵 $\mathbf{H}$ 确定, 而它的纠错能力可由 $\mathbf{H}$ 的特性决定之。下面我们讨论矩阵 $\mathbf{H}$ 。

定义 9-9 一个码字 X 所含 1 的个数叫此码字的重量, 并记为: $W(X)$ 。

如码字 0001001 的重量为 2, 码字 1000000 的重量为 1。码字 00...0 的重量为 0, 我们可以将 00...0 记为 $0'$ 。

定理 9-5 设有码 C , 对任一 $X, Y \in C$, 有

$$H(X, Y) = H(X \oplus Y, 0') = W(X \oplus Y)$$

证明: 设 $X = x_1 x_2 \dots x_n, Y = y_1 y_2 \dots y_n, Z = X \oplus Y = z_1 z_2 \dots z_n$, 其中 $z_i = x_i \oplus y_i$ ($i = 1, 2, \dots, n$), 此时我们有:

$$\begin{aligned} H(X, Y) &= \sum_{i=1}^n (x_i \oplus y_i) = \sum_{i=1}^n z_i = \\ &= \sum_{i=1}^n (z_i \oplus 0) = H(X \oplus y, 0') \end{aligned}$$

又因为 $\sum_{i=1}^n z_i = W(Z)$, 所以有:

$$H(X, Y) = H(X \oplus Y, 0') = \sum_{i=1}^n z_i = W(z) = W(X \oplus Y)$$

定理 9-6 群码 C 中非零码字的最小重量等于此群码的最小距离。亦即有:

$$\min_{\substack{Z \in C \\ Z \neq 0}} W(Z) = d_{\min}(C)$$

证明: 因 $(C, \oplus)$ 是群, 它的单位元是 $0'$ 。对任一非零码字 Z , 有:

$$\begin{aligned} W(Z) &= W(Z \oplus 0') = H(Z, 0') \\ &\geq \min_{\substack{X, Y \in C \\ X \neq Y}} H(X, Y) = d_{\min}(C) \end{aligned}$$

所以有:

$$\min_{\substack{Z \in C \\ Z \neq 0}} W(Z) \geq d_{\min}(C)$$

另外, 设有 $X, Y \in C$ 且 $X \neq Y$, 此时我们有 $X \oplus Y \in C$ 且 $X \oplus Y \neq 0$ 。

并有
$$H(X, Y) = W(X \oplus Y) \geq \min_{\substack{Z \in C \\ Z \neq 0}} W(Z)$$

故有:
$$d_{\min}(C) = \min_{\substack{X, Y \in C \\ X \neq Y}} H(X, Y) \geq \min_{\substack{Z \in C \\ Z \neq 0}} W(Z)$$

最后得到:

$$\min_{\substack{Z \in C \\ Z \neq 0}} W(Z) = d_{\min}(C)$$

这个定理给出了群码 C 的最小距离与最小重量的关系。

定理 9-7 设 H 是 k 行 n 列矩阵, $X = x_1, x_2, \dots, x_n$, 并设集合 G :

$$G = \{X \mid \vec{X} \cdot H^T = 0'\}$$

则 $(G, \oplus)$ 是群, 即 G 是群码。

证明: $(S_n, \oplus)$ 是群且是有限群。 $G \subseteq S_n$ 。根据有限群子群判别条件, 只要证明 G 是封闭的就行了。即若 $X, Y \in G$, 只要证得 $X \oplus Y \in G$ 就行了。因为 $X \in G$, 所以有:

$$\vec{X} \cdot H^T = 0$$

又因为 $Y \in G$, 所以有:

$$\vec{Y} \cdot H^T = 0$$

而此时我们有:

$$\overrightarrow{(X \oplus Y)} \cdot H^T = (\vec{X} \cdot H^T) \oplus (\vec{Y} \cdot H^T) = 0' \oplus 0' = 0'$$

所以有:

$$X \oplus Y \in G$$

由此定理得证。

由此例可知汉明码是群码。

定义 9-10 群码 $G = \{X \mid \vec{X} \cdot H^T = 0\}$ 称为由 H 生成的群码, 而 G 中每一码字, 称为由 H 生成的码字, 矩阵 H 称为一致校验矩阵。

现在我们介绍矩阵列向量的概念。设矩阵 H 为:

$$H = \begin{pmatrix} h_{11} & h_{12} & h_{13} & \cdots & h_{1n} \\ h_{21} & h_{22} & h_{23} & \cdots & h_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ h_{k1} & h_{k2} & h_{k3} & \cdots & h_{kn} \end{pmatrix}$$

我们令:

$$h_i = \begin{pmatrix} h_{1i} \\ h_{2i} \\ \vdots \\ h_{ki} \end{pmatrix} \quad \text{其中 } i = 1, 2, \cdots, n$$

此时 H 可记为:

$$H = (h_1 \quad h_2 \quad h_3 \cdots h_n)$$

而 h_i 叫矩阵 H 的第 i 个列向量。

如有 H 的列向量 h_i, h_j , 则我们说 $h_i \oplus h_j$ 为:

$$h_i \oplus h_j = \begin{pmatrix} h_{1i} + h_{1j} \\ h_{2i} + h_{2j} \\ \vdots \\ h_{ki} + h_{kj} \end{pmatrix}$$

我们用下面的定理将列向量间建立联系。

定理 9-8 一致校验矩阵 H 生成一个重量为 p 的码字的充分必要条件是 H 中存在 p 个列向量, 它们的按位加为 $0'$ 。

证明: 充分性。若 H 中有 p 个列向量 $h_{i1}, h_{i2}, \dots, h_{ip}$ 满足:

$$h_{i1} \oplus h_{i2} \oplus \dots \oplus h_{ip} = 0$$

此时我们可按下列规则构成一个字 $X = x_1 x_2 \dots x_n$:

(1) $x_{i1}, x_{i2}, x_{i3}, \dots, x_{ip}$ 均为 1。

(2) 其余均为 0。

显然, 此 X 满足:

$$\vec{X} \cdot H^T = (h_{i1} \oplus h_{i2} \oplus \dots \oplus h_{ip})^T = 0'$$

故此 X 即为由 H 生成的重量为 p 的码字。

必要性。若 H 生成重量为 p 的码字 X , 而 $X = x_1 x_2 \dots x_n$, 其中有: $x_{i1} = x_{i2} = x_{i3} = \dots = x_{in} = 1$, 其余均为 0, 且由 $\vec{X} \cdot H^T = 0'$, 可得:

$$h_{i1} \oplus h_{i2} \oplus \dots \oplus h_{in} = 0'$$

故 p 个列向量的按位加为 $0'$ 。

由上面几个定理我们可以得到一个极为重要的定理:

定理 9-9 由 H 生成的群码的最小距离等于 H 中列向量按位加为 0 的最小列向量数。

这个定理建立了最小距离与列向量数间的联系。我们从前面的定理已经知道, 一个码的纠错能力由其最小距离决定。故这个定理也告诉了我们一个群码的纠错能力可由其一致校验矩阵 H 中列向量按位加为 0 的最小列向量数决定。故只要选取适当的 H 就可使其生成的码达到预定的纠错能力。

由此例也可以看出, 前面所述之汉明码, 它的矩阵 H 中没有零列向量, 且各列向量间均互不相同, 但它的第二、三、四列向量之和为 $0'$, 按定理我们可知这个码的最小距离是 3, 而且可知此群码必能纠正单个错误。

将上述之汉明码推广到一般的情况, 码 C 之每一码字 X 由信息位 $x_1 x_2 \dots x_n$ 及附加校验位 $x_{m+1} \cdot x_{m+2} \dots x_{m+k}$ 组成, 其形式为:

$$X = x_1 x_2 \cdots x_m x_{m+1} \cdots x_{m+k}$$

X 中其信息位与校验位间有下面的关系:

$$x_{m+i} = q_{i1}x_1 + q_{i2}x_2 + \cdots + q_{im}x_m \quad (i = 1, 2, \cdots, k)$$

而 $q_{ij} \in \{0, 1\}$ $(j = 1, 2, \cdots, m)$

作矩阵 H :

$$H = (\underbrace{Q}_{k \times m} \underbrace{I}_{k \times h})$$

其中:

$$Q = \begin{pmatrix} q_{11} & q_{12} & \cdots & q_{1m} \\ q_{21} & q_{22} & \cdots & q_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ q_{k1} & q_{k2} & \cdots & q_{km} \end{pmatrix}, \quad I = \begin{pmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}_{h \times k}$$

码 C 中任一码字满足方程:

$$\vec{X} \cdot H^T = 0'$$

令 $n = m + k$, 而这种码我们就称为 (n, m) 码。

要使码 C 能纠正单个错误, 由前面定理可知, 只要对 H 作适当的赋值使得 H 的列向量均不相同且无零列向量, 这样可保证 C 的最小距离 > 2 , 即要求 H 中的 Q 的列向量均不为 $0'$ 且不出现 I_k 中的所有 k 个列向量。

Q 的列向量是 k 维的, 故可有 2^k 个不同列向量, 而供 Q 选择的列向量是这 2^k 个列向量中除去 I_k 中 k 个列向量及零列向量以外的所有 $2^k - k - 1$ 个列向量。故我们可在这 $2^k - k - 1$ 个列向量中任选 m 个列向量组成 Q 。故 m 与 k 之间必须满足:

$$m \leq 2^k - k - 1$$

$$\text{或: } 2^k \geq (m + k) + 1 = n + 1$$

$$\text{或: } k \geq \log_2(n + 1)$$

因此, 只要码 C 中校验位位数 k 满足:

$$k \geq \log_2(n + 1)$$

总可以在 $2^k - k - 1$ 个列向量中任选 m 个组成 Q , 而使 C 具有纠正单

个错误的能力。

从这里我们也可以看出如何组织具有一定要求的纠错能力的纠错码。

例 9-37 设 $n=9, k \geq \log_2(n+1) = \log_2(9+1) = \log_2 10 > 3, \therefore k \geq 3$, 如取 $k=4$, 则 $m=9-4=5$, 所以一致校验矩阵 H 中 Q 应有 5 个向量, 而 $2^k - k - 1 = 2^4 - 4 - 1 = 11$ 。所以 Q 可以有 $C_{11}^5 = 462$ 个组成方法。故下列的 H 所生成的群码均至少可以纠正单个错误:

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$H = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

由此可知一码字长为五位可附加四位校验位, 而校验位的值可按上述给定的 H 生成, 从而构成一长为九位的纠错码, 而这个纠错码至少可以纠正单个错误。

例 9-38 设 $n=7$, 则 $k \geq \log_2(7+1) = \log_2 8 = 3$, 我们取 $k=3$, 则 $m=4$, 所以一致校验矩阵 H 中 Q 应有四个列向量。而 $2^k - k - 1 = 2^3 - 3 - 1 = 4$, 故 Q 可由四个列向量惟一决定, 它们是:

$$\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

因而 H 是:

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

此 H 即为上面所述之汉明码的 H 。

4. 群码的校正

从上面我们知道了如何设计一个纠错码以及如何发现错误,并指出错误码元的确切位置,而在这节我们主要研究一个简便的方法去纠正错误。这个方法叫做查表译码法。为介绍这种方法需要应用商群中的一些理论,如左(右)陪集的概念和拉格朗日定理等。

设有一汉明码 C , 它的字长为 n , 其信息位长为 m , 校验位长为 k 。我们已知 $(S_n, \oplus)$ 是群而 $(C, \oplus)$ 是它的子群。设有 $X \in C$, X 在传递过程中第 i 位发生了错误而变成 X' 。设重量为 1 的所有码字为 $e_1 = 100 \cdots 0, e_2 = 010 \cdots 0, \dots, e_n = 00 \cdots 01$, 而此时有 $X' \oplus e_i = X$, 或 $X \oplus e_i = X'$ 。如何由 X' 恢复成 X 的一个办法是首先列出所有的 X 所可能出现单错的码字, 即对所有 $X \in C$, 所有 $e_i (i=1, 2, \dots, n)$ 列出:

$$X' \oplus e_i = X$$

将它们组成一张表。

其次, 当出现单错时 X 变成 X' , 此时用 X' 查上述之表, 查到 X' 后再用公式:

$$X' \oplus e_i = X$$

将其恢复成 X 。从而完成纠正单错的功能。

上述纠正单错的思想在具体实现时是这样安排的:

(1) 我们知道 $e_i \in S_n$ 但 $e_i \notin C$, 这是因为 $W(e_i) = 1$, 而 C 可纠正单错, 故对任一 $X \in C$ 有 $W(X) \geq 3$, 故有 $e_i \notin C$ 。

(2) 因 $e_i \notin C$, 故我们可以构造群 $(S_n, \oplus)$ 中的子群 $(C, \oplus)$ 关于 e_i 的左陪集 $e_i \oplus C$, 这种左陪集可有 n 个, 它们是:

$$e_1 \oplus C$$

$$e_2 \oplus C$$

...

$$e_n \oplus C$$

(3) 我们有 $C \subset S_n$, 故在 S_n 内还可以构作集合 C 。

(4) 由拉格朗日定理可知 C 在 S_n 中的左陪集个数有 $|S_n| /$

(7) 我们可按译码表校正单错。设有 $X \in C$ 经传递后出现单错变成 X' , 经查表, X' 在表中第 i 行第 j 列。此时可将 X' 校正为 c_j ——表第 j 列之首行。而 X' 之错码位为 i , 其中 e_i 为第 i 行之首位; $e_i \oplus c_1 = e_i$ (因 c_1 为零码字), 这就是查表译码法。

例 9-39 设 $n=6, m=3$, 一致校验矩阵是:

$$\boldsymbol{H} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

其校验位可从下列方程获得:

$$\begin{aligned} a_4 &= a_1 \oplus a_2 \\ a_5 &= a_1 \oplus a_3 \\ a_6 &= a_1 \oplus a_2 \oplus a_3 \end{aligned}$$

$\boldsymbol{H}$ 的列向量中无零向量且各不相同, 且 $h_1 \oplus h_2 \oplus h_5 = 0'$ 。故 $\boldsymbol{H}$ 所生成的群码 C 可以纠正单错。生成的 C 为:

$$C = \{000000, 001011, 010101, 011110, 100111, 101100, 110010, 111001\}$$

它的译码表由表 9-22 给出。

表 9-22 **C 的译码表**

C	000000	001011	010101	011110	100111	101100	110010	111001
$e_1 \oplus C$	100000	101011	110101	111110	000111	001100	010010	011001
$e_2 \oplus C$	010000	011011	000101	001110	110111	111100	100010	101001
$e_3 \oplus C$	001000	000011	011101	010110	101111	100100	111010	110001
$e_4 \oplus C$	000100	001111	010001	011010	100011	101000	110110	111101
$e_5 \oplus C$	000010	001001	010111	011100	100101	101110	110000	111011
$e_6 \oplus C$	000001	001010	010100	011111	100110	101101	110011	111000
$z \oplus C$	000110	001101	010011	011000	100001	101010	110100	111111

设有某一 $X' = 100110$, 我们可在译码表中找到这个码字, 它在第六行第五列, 它的正确码字在第五列的 C 行, 即为: 100111。而它的出错位为第六位, 其 e_6 在第六行的首列, 即为: 000001。

9.3 谓词逻辑与逻辑程序设计语言

在公理化理论一章中我们已经看到,由于引入了假设推理,使得由公理系统中的公理和推理规则出发而求得定理的过程变得十分简单。于是人们就进一步猜想,是否有一种固定的算法,按照这种算法,可以证明谓词逻辑中的任何公理系统的任何定理的正确性;如果真存在这种算法的话,将这种算法用计算机实现后,则谓词演算中的定理就可以用计算机证明,从而实现了定理的自动证明。这种想法1965年由美国数理逻辑学家罗宾逊(Robinson)得到了证明,罗宾逊证明了谓词逻辑的“半可判定性”,即在谓词演算中存在一种算法,只要公式是永真的,就能用此算法推出,他所使用的算法叫消解原理(resolution principle)。

自1965年以来,对这种算法的研究达到了高潮,其目的是为了使用此算法在计算机中实现更为方便与有效,其中较为知名的是线性消解法。

1972年法国马赛大学的 Colmerauer 在上述研究成果基础上设计了一种逻辑程序设计语言,称为 PROLOG(programming in logic)语言,不久,便在计算机上实现。

这样,现实世界中的问题只要能使用谓词逻辑公理系统方式表示出来,就可以将它写成 PROLOG 程序,然后用计算机实现,其过程见图 9-4。因此通过此种方式可以用计算机解决现实世界中很多逻辑问题。

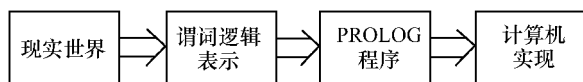


图 9-4 PROLOG 程序实现流程

在这一节我们介绍消解原理及 PROLOG 语言。对此了解后就能对计算机实现与解决逻辑问题的全过程充分认识。

1. 子句与子句集

为了便于推理,对谓词逻辑中的永真公式需进一步规范化。这可在斯科林范式基础上进行,其过程如下:

(1) 利用 US、ES 将公式中的量词除去。

例 9-40 试将 $\exists x \forall y (\neg A(x, y) \vee (B_1(x, y) \wedge B_2(x, y)))$ 进一步规范化。

解: 首先由 $\exists x \forall y (\neg A(x, y) \vee (B_1(x, y) \wedge B_2(x, y)))$ 可以推出 $\neg A(e, y) \vee (B_1(e, y) \wedge B_2(e, y))$

(2) 除去量词后的公式就是一个命题演算公式,此时可将公式化归成合取范式。

在上例中可有:

$$\begin{aligned} & \neg A(e, y) \vee (B_1(e, y) \wedge B_2(e, y)) \\ &= (\neg A(e, y) \vee B_1(e, y)) \wedge (\neg A(e, y) \vee B_2(e, y)) \end{aligned}$$

(3) 将每个合取项用蕴含式表示,这种蕴含式称为子句 (clause)。

上例中可以化为:

$$\begin{aligned} & (\neg A(e, y) \vee B_1(e, y)) \wedge (\neg A(e, y) \vee B_2(e, y)) \\ &= (A(e, y) \rightarrow B_1(e, y)) \wedge (A(e, y) \rightarrow B_2(e, y)) \end{aligned}$$

(4) 最后一个公式可用一个子句集表示,一个公式是永真的与一个子句集永真(子句集中每个子句为永真)相一致。

于是 $(A(e, y) \rightarrow B_1(e, y)) \wedge (A(e, y) \rightarrow B_2(e, y))$ 可用下面的子句集表示:

$$\{A(e, y) \rightarrow B_1(e, y), A(e, y) \rightarrow B_2(e, y)\}$$

这样一个公式总可以用一组子句表示,每个子句具有单一的蕴含形式。这种蕴含式既简单又便于推理。

下面我们进一步讨论子句的形式。对任何一个合取项,设它有 k 个带否定符的命题以及 $n-k$ 个不带否定符的命题:

$$\neg A_1 \vee \neg A_2 \vee \cdots \vee \neg A_k \vee A_{k+1} \vee A_{k+2} \cdots \vee A_n$$

对这个合取项总可以将其转换成蕴含式,使得蕴含式中无否定符出现。化归的方式如下:

$$\begin{aligned} & \neg A_1 \vee \neg A_2 \vee \cdots \vee \neg A_k \vee A_{k+1} \vee \cdots \vee A_n \\ &= \neg (A_1 \wedge A_2 \wedge \cdots \wedge A_k) \vee (A_{k+1} \vee \cdots \vee A_n) \\ &= (A_1 \wedge A_2 \wedge \cdots \wedge A_k) \rightarrow (A_{k+1} \vee \cdots \vee A_n) \end{aligned}$$

为推理方便,一般将它写成:

$$A_{k+1} \vee A_{k+2} \vee \cdots \vee A_n \leftarrow A_1 \wedge A_2 \wedge \cdots \wedge A_k$$

或写成:

$$A_{k+1}, A_{k+2}, \cdots, A_n \leftarrow A_1, A_2, \cdots, A_k$$

这个公式给出了子句的标准形式。

有一种特殊类型的子句需要讨论,它称为 **Horn** 子句。当子句中 $k=n-1$ 时,则称此子句为 Horn 子句。这子句具有下面形式:

$$A_n \leftarrow A_1, A_2, \cdots, A_{n-1}$$

在 Horn 子句中当 $n=1$ 时,称为断言,断言具有下面形式:

$$A_n \leftarrow$$

在 Horn 子句中,当 $k=n$ 时称为假设,它具有下面的形式:

$$\leftarrow A_1, A_2, \cdots, A_{n-1}$$

在 Horn 子句中,当 $n=0$ 时称为空子句,空子句可写成:

$$\{\rightarrow\} \text{ 或 } \square$$

由于推理中可由 Horn 子句得出惟一的结论,因此 Horn 子句的作用很大。

下面我们举几个例子。

例 9-41 试将“每个人都犯错误”用子句形式表示。

我们可以将这语句写成如下形式:

$$\forall x \exists y (Human(x) \rightarrow Mistake(y) \wedge Does(x, y))$$

利用 US、ES 后,可得到:

$$H(x) \rightarrow M(e) \wedge D(x, e)$$

(为书写方便,我们分别用 H 、 M 、 D 表示 Human、Mistake 和 Does),将所得公式化归成特异合取范式:

$$\begin{aligned}
& H(x) \rightarrow M(e) \wedge D(x, e) \\
& = \neg H(x) \vee (M(e) \wedge D(x, e)) \\
& = (\neg H(x) \vee M(e)) \wedge (\neg H(x) \vee D(x, e)) \\
& = (H(x) \rightarrow M(e)) \wedge (H(x) \rightarrow D(x, e))
\end{aligned}$$

最后得到子句集 $\{H(x) \rightarrow M(e), H(x) \rightarrow D(x, e)\}$

例 9-42 试将祖先关系“父母是祖先,祖先的祖先是祖先”用子句集表示。

我们可以将这语句用下面的形式表示:

$$\begin{aligned}
& \forall x \forall y (\text{parent}(x, y) \vee \exists z (\text{Ancestor}(x, z) \\
& \wedge \text{Ancestor}(z, y))) \rightarrow \text{Ancestor}(x, y)
\end{aligned}$$

利用 US、ES 后,可得到

$$(P(x, y) \vee (A(x, e) \wedge A(e, y))) \rightarrow A(x, y)$$

此处 P 、 A 是 Parent、Ancestor 之简写,将上式化为特异合取范式:

$$\begin{aligned}
& (P(x, y) \vee (A(x, e) \wedge A(e, y))) \rightarrow A(x, y) \\
& = (\neg P(x, y) \vee A(x, y)) \wedge \neg A(x, e) \\
& \vee \neg A(e, y) \vee A(x, y)
\end{aligned}$$

最后得到子句集

$$\{A(x, y) \leftarrow P(x, y), A(x, y) \leftarrow A(x, e), A(e, y)\}$$

2. 消解原理

我们知道,在公理系统中,有公理和定理两部分,公理是已知的永真公式,定理是要求证的永真公式,公理可用子句集表示,设子句集为 S ,则:

$$S = \{E_1, E_2, \dots, E_n\}$$

其中 $E_i (i=1, \dots, n)$ 表示子句。

设定理用 E 表示,下面分几个步骤讨论。

(1) 子句集的相容性

一个子句集如存在语义解释,则称它是相容的,否则称为不相容

的。如 $\{\leftarrow P, P\leftarrow\}$ 是不相容的子句集,而 $\{P\leftarrow Q, Q\leftarrow R\}, \{x\leftarrow, y\leftarrow\}$ 都是相容的,因为在现实世界中总可以找到一种语义解释使每个子句为永真。

相容性是一个公理系统的必备条件,一个不相容的公理系统在现实世界中是不存在的,因而没有讨论的必要。

由相容子句集 S 可推得结论 E 相当于 $S \cup \{\neg E\}$ 是不相容的。

例如我们可以由:

$$\{A \leftarrow B, B\}$$

可得出 A , 它相当于:

$$\{A \leftarrow B, B, \neg A\}$$

是不相容的。

因此要证明由 S 可推得定理 E 相当于证明 $S \cup \{\neg E\}$ 是不相容的。

(2) 不相容性的证明方法

我们讨论子句集不相容性的证明方法。

定理 9-10 设有永真公式:

$$A_{k+1} \vee A_{k+2} \vee \cdots \vee A_n \leftarrow A_1 \wedge A_2 \wedge \cdots \wedge A_k$$

$$B_{h+1} \vee B_{h+2} \vee \cdots \vee B_m \leftarrow B_1 \wedge B_2 \wedge \cdots \wedge B_h$$

(其中 $A_i = B_j, i \leq k, j \geq h$), 则必有永真公式:

$$A_{k+1} \vee A_{k+2} \vee \cdots \vee A_n \vee B_{h+1} \vee \cdots \vee B_{j-1} \vee B_{j+1} \vee \cdots \vee B_m \leftarrow A_1 \wedge A_2 \wedge \cdots \wedge A_{i-1} \wedge A_{i+1} \wedge \cdots \wedge A_k \wedge B_1 \wedge B_2 \wedge \cdots \wedge B_h$$

证明: 已知:

$$A_1 \wedge A_2 \cdots \wedge A_{i-1} \wedge A_i \wedge A_{i+1} \wedge \cdots \vee A_k \rightarrow A_{k+1} \vee A_{k+2} \vee \cdots \vee A_n \quad (1)$$

$$B_1 \wedge B_2 \cdots B_h \rightarrow B_{h+1} \vee B_{h+2} \vee \cdots \vee B_{j-1} \vee B_j \vee B_{j+1} \vee \cdots \vee B_m \quad (2)$$

由(1), (2)得:

$$\neg A_1 \vee \neg A_2 \vee \cdots \vee \neg A_{i-1} \vee \neg A_i \vee \neg A_{i+1} \vee \cdots \vee \neg A_k \vee A_{k+1} \vee \cdots \vee A_n \quad (3)$$

$$\neg B_1 \vee \neg B_2 \vee \cdots \vee \neg B_h \vee B_{h+1} \vee B_{h+2} \vee \cdots \vee B_{j-1} \vee B_j \vee B_{j+1} \vee \cdots \vee B_m \quad (4)$$

将(3)和(4)合并得:

$$\neg A_1 \vee \neg A_2 \vee \cdots \vee \neg A_{i-1} \vee \neg A_{i+1} \vee \cdots \vee \neg A_k \vee \neg B_1 \vee \neg B_2 \vee \neg B_3 \vee \cdots$$

$$\vee \neg B_h \vee A_{k+1} \vee A_{k+2} \vee \cdots \vee A_n \vee B_{h+1} \vee B_{h+2} \vee \cdots \vee B_{j-1} \vee B_{j+1} \vee \cdots \vee B_m$$

由此得到：

$$A_1 \wedge A_2 \wedge \cdots \wedge A_{i-1} \wedge A_{i+1} \wedge \cdots \wedge A_k \wedge B_1 \wedge B_2 \wedge \cdots \wedge B_h \rightarrow A_{k+1} \vee A_{k+2} \vee \cdots \vee A_n \vee B_{h+1} \vee \cdots \vee B_{j-1} \vee B_{j+1} \vee \cdots \vee B_m$$

证毕。

推论 1 设有永真公式：

$$A_{k+1} \vee A_{k+2} \vee \cdots \vee A_n \leftarrow A_1 \wedge A_2 \wedge \cdots \wedge A_k$$

$$B_{h+1} \vee B_{h+2} \vee \cdots \vee B_m \leftarrow B_1 \wedge B_2 \wedge \cdots \wedge B_h$$

(其中 $A_i = B_j, i \leq k, j \geq h$)，则必有永真公式：

$$B_{h+1} \vee \cdots \vee B_{i-1} \vee B_{j+1} \vee \cdots \vee B_m \vee A_{k+1} \vee A_{k+2} \vee \cdots \vee A_n \leftarrow A_1 \wedge A_2 \wedge \cdots \wedge A_{i-1} \wedge A_{i+1} \wedge \cdots \wedge A_k \wedge B_1 \wedge \cdots \wedge B_h$$

推论 2 设有永真公式：

$$A_n \leftarrow A_1, A_2, \cdots, A_{n-1}$$

$$B_m \leftarrow B_1, B_2, \cdots, B_{m-1}$$

(其中 $A_n = B_i, i < m$)，则必有永真公式：

$$B_m \leftarrow A_1, A_2, \cdots, A_{n-1}, B_1, B_2, \cdots, B_{i-1}, B_{i+1}, \cdots, B_{m-1}$$

推论 3 由 $\{P \leftarrow, \leftarrow P\}$ 可得到 $\square$ (空子句)。

证明：由 $\{P \leftarrow, \leftarrow P\}$ ，用推论 2 可得出 $\{\leftarrow\}$ ，即为 $\square$ 。

这个定理说明两点。

① 两个子句其不同的两边如有相同命题可消去，这是消解原理的基本思想，此方法叫反驳法。

② 由推论 3 还可以知道，由不相容的子句集可得空子句。

这样我们可以得到一种新的证明方法，即由 S 为公理系统证明 E 为定理的过程可以改为：

① 作 $S' = S \cup \{\neg E\} = \{E_1, E_2, \cdots, E_n, \neg E\}$ ——公理系统，

② 从 $\neg E$ 开始在 S' 内不断用反驳法，

③ 最后如出现空子句则结束。

这种定理的证明方法所使用的仅是反驳法，其基本过程为：

① 寻找两个子句不同端间相同的命题，这过程称匹配或合一。

② 找到后进行消去并将两子句合并。

这样在谓词逻辑中任何公理系统下的证明过程都变得十分简单, 这为计算机证明定理从理论上作好了准备。

下面我们举几个简单例子。

例 9-43 试证由 $(\neg S \vee R) \wedge (\neg Q \vee \neg R \vee P)$ 可推出 $(\neg S \vee \neg Q) \wedge P$ 。

证明: 由 $(\neg S \vee R) \wedge (\neg Q \vee \neg R \vee P)$ 可得出子句集:

$$S = \{S \rightarrow R, Q \wedge R \rightarrow P\}$$

即: $S = \{R \leftarrow S, P \leftarrow Q, R\}$

而: $(\neg S \vee \neg Q) \wedge P$ 的否定可表示成

$$S, Q \leftarrow P$$

构造一个新集合 S' :

$$S' = \{R \leftarrow S, P \leftarrow Q, R, S, Q \leftarrow P\}$$

从 $S, Q \leftarrow P$ 开始用反驳法。

$$\text{由 } \begin{cases} S, Q \leftarrow P \\ P \leftarrow Q, R \end{cases} \quad \text{可得出 } S \leftarrow R$$

$$\text{由 } \begin{cases} S \leftarrow R \\ R \leftarrow S \end{cases} \quad \text{可得出 } \square$$

定理得证。

例 9-44 试证由 $R \wedge Q \wedge (P \vee \neg Q \vee \neg R)$ 可推出 P ,

证明: 由 $R \wedge Q \wedge (P \vee \neg Q \vee \neg R)$ 可得子句集:

$$S = \{P \leftarrow Q, R, R \leftarrow, Q \leftarrow\}$$

构造新句子集:

$$S' = \{P \leftarrow Q, R, R \leftarrow, Q \leftarrow, \leftarrow P\}$$

由 $\leftarrow P$ 开始用反驳法:

$$\text{由 } \begin{cases} \leftarrow P \\ P \leftarrow Q, R \end{cases} \quad \text{可得出 } \leftarrow Q, R$$

$$\text{由 } \begin{cases} \leftarrow Q, R \\ Q \leftarrow \end{cases} \quad \text{可得出 } \leftarrow R$$

由 $\begin{cases} \leftarrow R \\ R \leftarrow \end{cases}$ 可得出 $\square$

定理得证。

(3) 代换合一与匹配

我们已经介绍了消解原理的基本思想,它的关键步骤是合一或匹配,现在我们较详细地讨论这个问题。

要在两子句中不同端寻找相同的命题这件事,乍一看似乎不复杂,但要深入研究就会发现并非那么容易。首先,因为我们讨论的是谓词逻辑,所以命题一般以谓词形式出现,具有:

$$P(x_1, x_2, \dots, x_n)$$

之形式。

两个谓词相同的含义有下面几种情况:

① 两个谓词符相同。

② 个体变元的数目相同。

③ 对应个体变元相同。这又可分为三种情形:

(a) 两者均为变量,此时需对变量作代换使之相同;

(b) 一个为变量另一个为常量,此时必须对变量作代换使之与常量一致;

(c) 两者均为常量,此时两常量应相等。

因此,在比较两个谓词是否相同不仅要逐条比较还要进行代换,不同的代换可得到不同的结果。

现在我们介绍代换。

对一组变元 $x_1, x_2, \dots, x_n$, 它可分别用 t_1 替换 x_1 , t_2 替换 x_2 , $\dots, t_n$ 替换 x_n , 从而得到另一组变元 $t_1, t_2, \dots, t_n$, 这种替换过程叫代换, 它可写成:

$$\theta = \{t_1/x_1, t_2/x_2, \dots, t_n/x_n\}$$

例 9-45 设有公式 $E = F(x, y)$, 代换 $\theta = \{a/x, b/y\}$, 则有 $E\theta = F(a, b)$ 。

复合代换也是一种代换。设有:

$$\theta = \{t_1/x_1, t_2/x_2, \dots, t_n/x_n\}$$

$$\lambda = \{\mu_1/y_1, \mu_2/y_2, \dots, \mu_m/y_m\}$$

则称 $\theta \circ \lambda = \{t_1 \circ \lambda/x_1, t_2 \circ \lambda/x_2, \dots, t_n \circ \lambda/x_n, \mu_1/y_1, \mu_2/y_2, \dots, \mu_m/y_m\}$ 为 θ 与 λ 的复合代换。

例 9-46 设公式 $E = F(x, y)$, 代换 $\theta = \{t_1/x, t_2/y\}$, $\lambda = \{a/t_1, b/t_2\}$, 则有:

$$E\theta \circ \lambda = F(t_1, t_2)\lambda = F(a, b)$$

有了代换概念后就可用它进行消解, 下面用一例说明之。

例 9-47 设有子句集 $\{P(y) \leftarrow Q(z), Q(y) \leftarrow P(f(x))\}$, 试用反驳法消解之。

证明: 作代换 $\theta = \{x/x, f(x)/y, f(x)/z\}$ 之后得到:

$$(P(y) \leftarrow Q(z))\theta = P(f(x)) \leftarrow Q(f(x))$$

$$(Q(y) \leftarrow P(f(x)))\theta = Q(f(x)) \leftarrow P(f(x))$$

对这两子句进行消解得到空子句 $\square$ 。

也可作另一代换: $\lambda = \{a/x, f(a)/y, f(a)/z\}$ 后得到:

$$(P(y) \leftarrow Q(z))\lambda = P(f(a)) \leftarrow Q(f(a))$$

$$(Q(y) \leftarrow P(f(x)))\lambda = Q(f(a)) \leftarrow P(f(a))$$

此两子句进行消解后也可得到空子句。

从上例可以看出, 通过代换可使两公式相同, 这种代换称为合一。即对 $\{E_1, E_2, \dots, E_n\}$, 如果存在一种代换 λ , 使得:

$$E_1\lambda = E_2\lambda = \dots = E_n\lambda$$

则称此代换为合一。

从上例中可看出, 合一不是惟一的, 它可以有多个, 其中最一般性的合一称为匹配, 即对 $\{E_1, E_2, \dots, E_n\}$, 如存在一个合一 σ , 使得对其他任一个合一 θ_i , 均存在代换 λ_i , 满足:

$$\theta_i = \sigma \circ \lambda_i$$

则称 σ 为 $\{E_1, E_2, \dots, E_n\}$ 的匹配。

例 9-48 设有 $\{P(\mu, y, g(y)), P(x, f(\mu), z)\}$, 试给出其匹配。

解: 作 $\sigma = \{\mu/x, f(\mu)/y, g(f(\mu))/z\}$, 它是一个合一, 因为有:

$$P(\mu, y, g(y))\sigma = P(\mu, f(\mu), g(f(\mu)))$$

$$P(x, f(\mu), z)\sigma = P(\mu, f(\mu), g(f(\mu)))$$

同时它也是一个匹配, 因为对任一合一 θ_i , 均有 $\lambda_i = \{a/\mu\}$, 使得:

$$\theta_i = \sigma \circ \lambda$$

如有合一:

$$\theta = \{a/\mu, a/x, f(a)/y, g(f(a))/z\}$$

$$P(\mu, y, g(y))\theta = P(a, f(a), g(f(a)))$$

$$P(x, f(\mu), z)\theta = P(a, f(a), g(f(a)))$$

而 $\theta = \sigma \circ \lambda$, 即有:

$$\begin{aligned} P(\mu, y, g(y))\sigma \circ \lambda &= P(\mu, f(\mu), g(f(\mu)))\lambda \\ &= P(a, f(a), g(f(a))) \end{aligned}$$

$$\begin{aligned} P(x, f(\mu), z)\sigma \circ \lambda &= P(\mu, f(\mu), g(f(\mu)))\lambda \\ &= P(a, f(a), g(f(a))) \end{aligned}$$

为了进行消解, 我们引入了代换, 能使若干个公式相同的代换称为合一, 最一般的合一称为匹配, 在消解过程中, 我们一般使用合一与匹配, 它是消解过程的关键。

(4) 几个实例

例 9-49 设有一组关于父母和祖父母的客观事实, 要求某些祖孙关系:

$$S \left\{ \begin{array}{ll} \text{Father(John, Ares)} \leftarrow & E_1 \\ \text{Father(Ares, Bob)} \leftarrow & E_2 \\ \text{Mother(Mary, Ares)} \leftarrow & E_3 \\ \text{Mother(Ann, Bob)} \leftarrow & E_4 \\ \text{Parent}(x, y) \leftarrow \text{Father}(x, y) & E_5 \\ \text{Parent}(x, y) \leftarrow \text{Mother}(x, y) & E_6 \\ \text{Grandparent}(x, y) \leftarrow \text{Parent}(x, z), & \\ \text{Parent}(z, y) & E_7 \end{array} \right.$$

要求证: $\text{Grandparent(John, Bob)} \leftarrow$

证明：用消解法：

$$\begin{aligned} &\leftarrow G(J,B) \\ &\quad | E_7 \\ &\leftarrow P(J,z),P(z,B) \\ &\quad | E_5 \\ &\leftarrow F(J,z),P(z,B) \\ &\quad | E_5 \\ &\leftarrow F(J,z),F(z,B) \\ &\quad | E_1 \\ &\leftarrow F(A,B) \\ &\quad | E_2 \\ &\quad \square \end{aligned}$$

例 9-50 试证明下列的智力测验题目(水容器问题)。设有两个分别能盛 7 升与 5 升的水容器,开始时两个容器均空,允许对容器做三种操作:

- ① 容器倒满水;
- ② 将容器中的水倒光;
- ③ 从一个容器倒水至另一个容器,使一个容器倒光而另一个容器倒满。

最后要求能使大容器(能盛 7 升的容器)中有 4 升水,并求其操作过程。

具体要求见图 9-5。

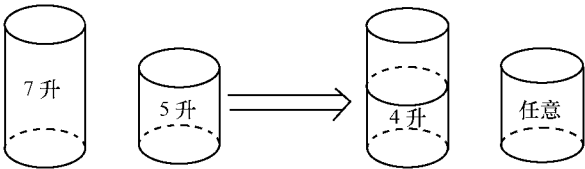


图 9-5 水容器图示

证明：用消解法：

① 作一个谓词 $\text{State}(u, v)$ 表示两个容器盛水之状态，如 $\text{State}(3, 1)$ 表示大容器盛 3 升，小容器盛 1 升。

② 在这个问题中的公理系统为：

开始时两容器为空，

允许做三种操作。

要求得到的定理为：大容器装 4 升水，小容器不限。

③ 将上述问题用子句形式表示为

$W_1 \text{state}(0, 0) \leftarrow$ 两容器均为容

$W_2 \text{state}(7, v) \leftarrow \text{state}(u, v)$ 将大容器倒满水

$W_3 \text{state}(u, 5) \leftarrow \text{state}(u, v)$ 将小容器倒满水

$W_4 \text{state}(0, v) \leftarrow \text{state}(u, v)$ 将大容器的水倒光

$W_5 \text{state}(u, 0) \leftarrow \text{state}(u, v)$ 将小容器的水倒光

$W_6 \text{state}(0, y) \leftarrow \text{state}(u, v), u + v = y, y \leq 5$
从容器 u 将水倒至 v ，使 u 空

$W_7 \text{state}(x, 0) \leftarrow \text{state}(u, v), u + v = x, x \leq 7$
从容器 v 倒水至 u ，使 v 空

$W_8 \text{state}(7, y) \leftarrow \text{state}(u, v), u + v = 7 + y$
从容器 v 将水倒至 u ，使 u 满

$W_9 \text{state}(x, 5) \leftarrow \text{state}(u, v), u + v = x + 5$
从容器 u 将水倒至 v ，使 v 满

这个问题的子句集为：

$$S = \{W_1, W_2, W_3, W_4, W_5, W_6, W_7, W_8, W_9\}$$

所求的定理可写成：

$$\text{state}(4, v) \leftarrow$$

它的否定为：

$$W_0: \leftarrow \text{state}(4, v)$$

故：

$$S' = \{W_0, W_1, W_2, W_3, W_4, W_5, W_6, W_7, W_8, W_9\}$$

其消解过程如图 9-6 所示。
定理证毕。

3. PROLOG 语言简介

PROLOG 语言是以谓词逻辑为其表现形式，以消解原理为其实现基础而研制成的一种逻辑程序设计语言。这种语言用 Horn 子句作为基本表示语句，一共有三个语句，具体要求见表 9-23，其中 P_i 为谓词。

除了三个语句外，PROLOG 语言还设置一些固定的常谓词，称为内部谓词，内部谓词用于实现一些非逻辑功能，如基本算术运算，组织输出格式及控制搜索路径等。

整个 PROLOG 程序由两部分组成，它们分别称为数据库与提问。数据库由事实与规则组成，它相当于公理系统，提问用询问语句表示，它相当于对应公理系统的定理。

例 9-51 一个数据库例子：

- | | |
|----------------------------------|----|
| (1) likes(john,food) | 事实 |
| (2) likes(john,wine) | 事实 |
| (3) likes(marry,wine) | 事实 |
| (4) likes(marry,food) | 事实 |
| (5) likes(john,x):-likes(x,wine) | 规则 |

表 9-23

语句名	事实(fact)	规则(rule)	询问(query)
形式	P_i	$P_1:-P_2,P_3,\cdots,P_n$	$?-P_1,P_2,\cdots,P_n$
逻辑含义	$P_i \leftarrow$ (断言)	$P_1, \leftarrow P_2, \cdots, P_n$ (Horn 子句)	$\leftarrow P_1, P_2, \cdots, P_n$ (假设)
语义	P_i 为真	若 $P_2, P_3, \cdots, P_n$ 为真, 则 P_1 为真	$P_1 \wedge P_2 \wedge \cdots \wedge P_n$ 为真吗?

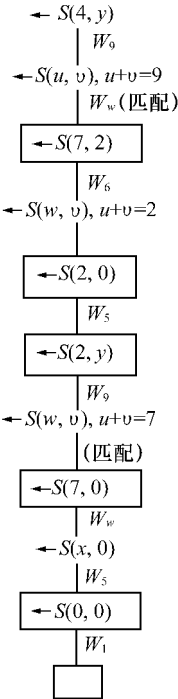


图 9-6 水容器问题消解过程图

对这个数据库可以提问。提问有两种形式。一种叫 yes/no 形式,对于所提问的语句,系统只要回答是或否,也就是说,回答是否是公理系统下的定理。例如对上述数据库作如下提问时:

? -likes(john,wine)

系统回答:yes

? -likes(john,marry)

系统回答:yes

而对

? -likes(marry,john)

系统回答:no

另一种提问是根据提问要求给出满足条件的答案,如:

? -like(john,x)

系统首先给出一个答案:

x=food

如用户尚需继续得到答案,只要打个逗号,系统又给出一个答案,这样直到所有答案均给出后,系统给出 NO。下面给出上例的全部过程。

? -likes(john,x)

x=food;

x=wine;

x=marry;

no

下面是一个完整的 PROLOG 程序:

例 9-52 图 9-7 的连通性
可用 PROLOG 程序表示:

connected(a,b)

connected(a,c)

connected(d,e)

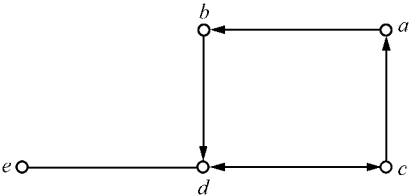


图 9-7 连通性的图示

```

connected( $b, d$ )
connected( $c, d$ )
connected( $c, a$ )
connected( $e, d$ )
path( $x, y$ ):¬connected( $x, y$ )
path( $x, y$ ):¬connected( $x, z$ ), path( $z, y$ )

```

可以对它提问：

```

? ¬path( $a, b$ )
    yes
? ¬path( $a, d$ )
    yes
? ¬path( $a, x$ ), path( $e, x$ )
     $x = d$ ;
    no
? ¬path( $a, x$ ), path( $x, e$ )
     $x = c$ ;
     $x = b$ ;
     $x = d$ ;
    no

```

习 题 九

9.1 根据本书所述试举两个离散数学在计算机中的应用实例。

9.2 选择一个计算应用领域并用离散数学知识以解决该领域中的理论与实际问题的例子。

“离散数学在计算机科学中的应用”复习提纲

1. 主要内容

——在关系数据库中应用。

- 在纠错码中应用。
- 在计算机软件中应用。

2. 复习重点

- 离散数学如何与应用建立联系以及如何指导应用。
- 离散数学在关系数据库中应用。

3. 离散数学应用

- 在关系数据库中应用
 - 关系代数—近世代数应用。
 - 关系演算—谓词逻辑及公理化理论应用。
- 在纠错码中应用
 - 集合论及近世代数的应用。
- 逻辑程序设计语言
 - 用谓词逻辑方法构作程序设计语言,建立起谓词逻辑在计算机软件中的应用。

习 题 解 答

习题一解答

1.1 (1) 答: $\emptyset$

(2) 答: $\{-3, 2\}$

(3) 答: $\{5, 6, 7, 8, 9, 10, 11\}$

1.2 (1) 答: $\{\emptyset, \{\emptyset\}, \{a\}, \{\{a\}\}, \{\emptyset, a\}, \{\emptyset, \{a\}\}, \{a\}, \{a\}\}, \{\emptyset, a, \{a\}\}$

(2) 答: $\rho(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}\}$

1.3 (1) 答: 成立, $\{a\}$ 是 $\{\{a\}\}$ 的元素。

(2) 答: 不成立, a 和 $\{a\}$ 是不同的元素。

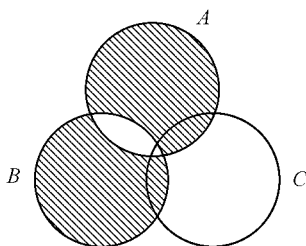
(3) 答: 成立, 同(1)。

(4) 答: 成立, $\{a\}$ 中的元素 a 在 $\{\{a\}, a\}$ 中可以找到。

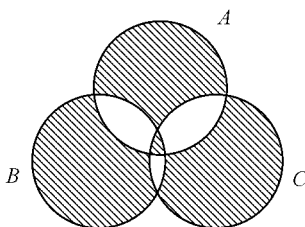
1.4 证明(1) $\{S\}$ 中 S 是集合, 而 $\{S\}$ 中 S 是 $\{S\}$ 的元素。(即 $S \in \{S\}$), 按元素的定义, 集合 S 也可作为元素, 故 $\{S\}$ 是有一个元素 S 的集合。

(2) $\{S\}$ 中 S 是集合并满足 $S \in S$, 由于 S 也可作为元素, 且由于 S 中不包含 S 作为元素, 故 $S \in S$ 成立, 因此 $\{S | S \text{ 是一个集合}\} = \{S | S \text{ 是一个集合并且 } S \in S\}$, 因此 $\{S | S \text{ 是一个集合并且 } S \in S\}$ 是集合。

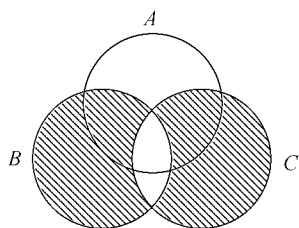
1.5 (1) 证明: 用文氏图证:



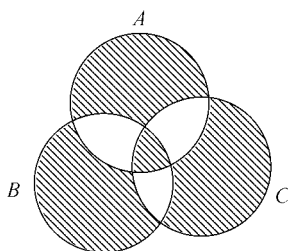
$A \oplus B$



$(A \oplus B) \oplus C$



$B \oplus C$



$A \oplus (B \oplus C)$

根据上述文氏图, 可知 $A \oplus (B \oplus C) = (A \oplus B) \oplus C$

(2) 证明: $A \oplus B = (A - B) \cup (B - A)$

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

(3) 证明: $A \oplus \emptyset = (A - \emptyset) \cup (\emptyset - A) = A \cup \emptyset = A$

(4) 证明: $A \oplus A = (A - A) \cup (A - A) = \emptyset \cup \emptyset = \emptyset$

(5) 证明: $A \oplus U = (A - U) \cup (U - A) = \emptyset \cup \bar{A} = \bar{A}$

(6) 证明: $A \oplus \bar{A} = (A - \bar{A}) \cup (\bar{A} - A) = A \cup \bar{A} = U$

(7) 证明:

$$\begin{aligned} \text{右边} &= (A \cup B) \cap (\overline{A \cap B}) = (A \cup B) \cap (\bar{A} \cup \bar{B}) \\ &= ((A \cup B) \cap \bar{A}) \cup ((A \cup B) \cap \bar{B}) \\ &= ((A \cap \bar{A}) \cup (B \cap \bar{A})) \cup ((A \cap \bar{B}) \cup (B \cap \bar{B})) \\ &= (B \cap \bar{A}) \cup (A \cap \bar{B}) \\ &= (B - A) \cup (A - B) \end{aligned}$$

$$=B\oplus A$$

$$=A\oplus B=\text{左边}$$

1.6 (1) 答:① 令 $A=\emptyset, B=\{\emptyset\}, C=\{\emptyset, \{\emptyset\}\}$ 则有 $A\in B$, $B\in C$, 且 $A\in C$, 成立。

② 令 $A=\{a\}, B=\{\emptyset, \{a\}\}, C=\{\emptyset, a, \{\emptyset, \{a\}\}\}$ 则有 $A\in B$, $B\in C$, 但 $A\notin C$ (因为 $\{a\}$ 不是 C 的元素) 不成立。

故若 $A\in B, B\in C$, 但 $A\in C$ 不一定成立。

(2) 证明: $\because B\subseteq C$, 故 B 中的每一个元素都是 C 中的元素; 又 $\because A\in B$, 故 A 是 B 中的一个元素, $\therefore A$ 是 C 中的一个元素, 即 $A\in C$ 。

(3) ① 令 $A=\emptyset, B=C=\{\emptyset\}$,

于是 $A\in B, B\subseteq C$ 且 $A\subseteq C$, 成立。

② 令 $A=\{a\}, B=\{\{a\}\}, C=\{\{a\}, b\}$

于是 $A\in B, B\subseteq C$, 但 $A\nsubseteq C$, 不成立。

故若 $A\in B, B\subseteq C$, 但 $A\subseteq C$ 不一定成立。

(4) ① 令 $A=\emptyset, B=C=\{\emptyset\}$,

则 $A\subseteq B, B\subseteq C$, 且 $A\in C$, 成立。

② 令 $A=\{1\}, B=\{1, 2\}, C=\{1, 2, 3\}$,

则 $A\subseteq B, B\subseteq C$, 但 $A\notin C$, 不成立。

故若 $A\subseteq B, B\subseteq C$, 则 $A\in C$ 不一定成立。

证明: $\because$ 对任意的 $a\in A$, 有 $A\subseteq B$ 则 $a\in B$,

又 $\because B\subseteq C$, 则 $a\in C$,

$\therefore A\subseteq C$ 。

(5) 证明: $\because A\cap B=A\cap C, \bar{A}\cap B=\bar{A}\cap C$,

$\therefore B=U\cap B=(A\cup\bar{A})\cap B=(A\cap B)\cup(\bar{A}\cap B)$

$= (A\cap C)\cup(\bar{A}\cap C)=(A\cup\bar{A})\cap C=U\cap C=C$ 。

(6) 证明: $\because A\cap C\subseteq B\cap C, A\cap\bar{C}\subseteq B\cap\bar{C}$, 由书中例 1-6 得:

$(A\cap C)\cup(A\cap\bar{C})\subseteq(B\cap C)\cup(B\cap\bar{C})$ 。

$\therefore A\cap(C\cup\bar{C})\subseteq B\cap(C\cup\bar{C})$ 。 $\therefore A\subseteq B$ 。

(7) 答:① 令 $A=\emptyset, B=\{\emptyset\}$, 则 $A\subseteq B$ 且 $A\in B$ 。

② 令 $A=\{a\}, B=\{\{a\}\}$, 则 $A\subseteq B$, 但 $A\notin B$ 。

③ 令 $A=\{a\}, B=\{a, b\}$, 则 $A\subseteq B$, 但 $A\notin B$ 。

故 $A\subseteq B$ 和 $A\in B$ 不一定同时成立。

$$1.7 \quad (1) \text{ 解: } \because (A-B)\cup(A-C)=A \Leftrightarrow (A\cap\bar{B})\cup(A\cap\bar{C})=A \\ \Leftrightarrow A\cap(\bar{B}\cup\bar{C})=A \Leftrightarrow A\cap(\overline{B\cap C})=A \Leftrightarrow A\subseteq\overline{B\cap C}$$

$\therefore (A-B)\cup(A-C)=A$ 成立的条件是 $A\subseteq\overline{B\cap C}$

$$(2) \text{ 解: } \because (A-B)\cup(A-C)=\emptyset \xLeftrightarrow[\text{由7-(1)}] A\cap(\overline{B\cap C})=\emptyset,$$

$\therefore (A-B)\cup(A-C)=\emptyset$ 成立的条件是 $A\subseteq B\cap C$ 。

$$(3) \text{ 解: } \because (A-B)\cap(A-C)=\emptyset \Leftrightarrow (A\cap\bar{B})\cap(A\cap\bar{C})=\emptyset, \\ \Leftrightarrow A\cap(\overline{B\cup C})=\emptyset.$$

$\therefore (A-B)\cap(A-C)=\emptyset$ 成立的条件是 $A\subseteq(B\cup C)$ 。

$$(4) \text{ 解: } \because (A-B)\oplus(A-C)=\emptyset \Leftrightarrow ((A-B)\cup(A-C))-(A \\ -B)\cap(A-C)=\emptyset \xLeftrightarrow[\text{由7-(1),(3)}] (A\cap(\overline{B\cap C}))-(A\cap(\overline{B\cup C}))=\emptyset \Leftrightarrow \\ A\cap((\overline{B\cap C})-(\overline{B\cup C}))=\emptyset \Leftrightarrow A\cap((\overline{B\cap C})\cap(B\cup C))=\emptyset \Leftrightarrow A\cap \\ ((B\cup C)\cap(\overline{B\cap C}))=\emptyset \Leftrightarrow A\cap((B\cup C)-(B\cap C))=\emptyset \Leftrightarrow A\cap(B \\ \oplus C)=\emptyset$$

$\therefore (A-B)\oplus(A-C)=\emptyset$ 成立的条件是 $A\subseteq\overline{B\oplus C}$ 。

$$1.8 \quad (1) \text{ 解: } A\cup(B\cup(C\cup D))=\{-30, -15, -7, -6, -5, \\ -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 15, 16, 30, 32, 64\}$$

$$(2) \text{ 解: } A\cap(B\cap(C\cap D))=\{1, 2\}$$

$$(3) \text{ 解: } B-(A\cup C)=\{-7, -4, 0, 4\}$$

$$(4) \text{ 解: } (\bar{A}\cap B)\cup D=\{-7, -6, -5, -4, -3, -2, -1, 0, 1, 2, \\ 3, 4, 5, 6, 8, 16, 32, 64\}$$

$$1.9 \quad (1) \text{ 解: } B\cap C=\{2, 4, 6, 8\}$$

(2) 解: $A \cap D = \{3, 6, 9\}$

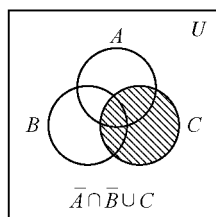
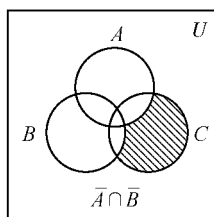
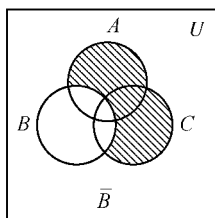
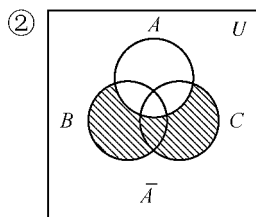
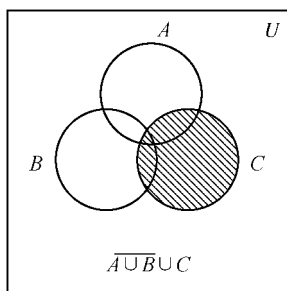
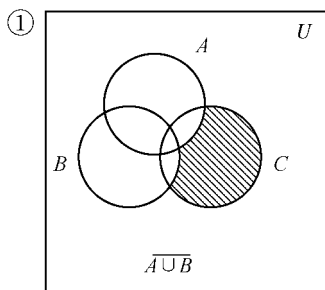
(3) 解: $(A - B) \cap C = \{10\}$

(4) 解: $C - A = \{n | n \text{ 为偶数}, n > 10\}$

(5) 解: $A \cap D = \{n | n = 3 \text{ 或 } n = 6 \text{ 或 } n = 9\}$

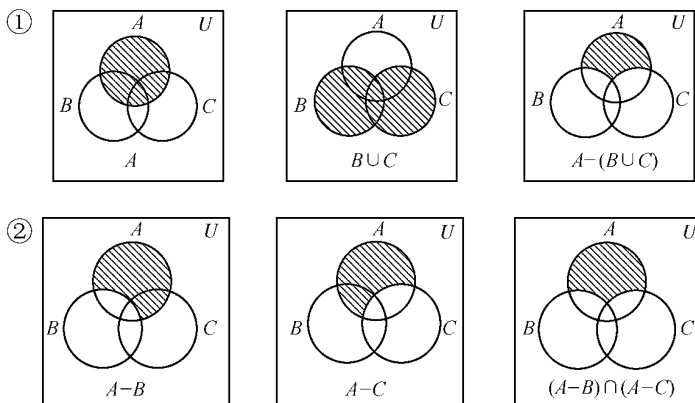
(6) 解: $(A \cap C) \cup (A - (B \cup C \cup D)) \cup E - A$ 。

1.10 (1) 解:



故有: $(\bar{A} \cup \bar{B}) \cup C = \bar{A} \cap \bar{B} \cup C$

(2) 解:



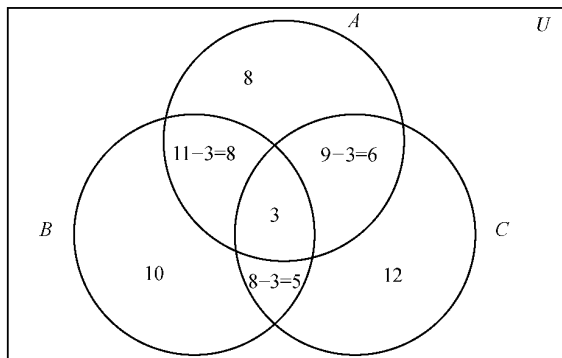
故有 $A - (B \cup C) = (A - B) \cap (A - C)$ 。

1.11 解:令 A, B, C 分别表示阅读《人民日报》、《体育报》、《光明日报》的人的集合,于是:

$$\begin{aligned}
 |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - \\
 &\quad |B \cap C| + |A \cap B \cap C| \\
 60 - 8 &= 25 + 26 + 26 - 11 - 9 - 8 + |A \cap B \cap C| \\
 |A \cap B \cap C| &= 3
 \end{aligned}$$

即有 3 人同时读三种报纸。

借用文氏图表示各种人数的关系



即恰好只读《人民日报》的人有 8 人;只读《体育报》的人有 10 人,只读《光明日报》的人有 12 人。

1.12 答: A (元素的定义要具体)

1.13 答: D (空集中不应含元素)

1.14 解: $A = \{1, 3, 5, 7\}; B = \left\{\frac{1}{4}, \frac{4}{1}, \frac{2}{3}, \frac{3}{2}\right\}$

1.15 解: $(A - B) \cup (B - A); A$

1.16 证明:① $\because (A \cap B) \subseteq A,$

又 $\because A \subseteq B,$ 任取 $x \in A \Rightarrow x \in B \Rightarrow x \in A \cap B$

$\therefore A \subseteq (A \cap B), \quad \therefore (A \cap B) = A。$

② $\because (A \cup B) \supseteq B,$

又 $\because$ 任取 $x \in (A \cup B) \Rightarrow x \in A$ 或 $x \in B,$

$\because A \subseteq B, \quad \therefore$ 若 $x \in A \Rightarrow x \in B$

$\therefore (A \cup B) \subseteq B, \quad \therefore (A \cup B) = B。$

1.17 答: C (应该是: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$)

1.18 答: $\emptyset; \{2\}$

1.19 解:原式 $= (A \cap \bar{B} \cap \bar{C}) \cup (A \cap \bar{B} \cap C) \cup (A \cap B \cap \bar{C}) \cup$
 $(A \cap B \cap C)$
 $= ((A \cap \bar{B}) \cap (\bar{C} \cup C)) \cup ((A \cap B) \cap (\bar{C} \cup C))$
 $= (A \cap \bar{B}) \cup (A \cap B) = A \cap (\bar{B} \cup B) = A$

1.20 答:D

1.21 答:C

1.22 证明:左边 $= A - (A \cap \bar{B}) = A \cap \overline{(A \cap \bar{B})} = A \cap (\bar{A} \cup B)$
 $= (A \cap \bar{A}) \cup (A \cap B) = A \cap B$

1.23 解: $A - B = \{1, 3, \{1, 2\}, \{3\}\}$
 $B - A = \{\{2, 3\}, \{1\}\}$

1.24 解: $A \cup (B \oplus C) = \{2, 3\} \cup \{1, 3, 4, 5, 7\}$
 $= \{1, 2, 3, 4, 5, 7\}$
 $(A \cup B) \oplus (B \cup C) = \{1, 2, 3, 4, 7\} \oplus \{2, 3, 5\}$
 $= \{1, 4, 7\} \cup \{5\} = \{1, 4, 5, 7\}$

1.25 答:B

1.26 答:B

1.27 解: $A = \emptyset$; $B = \{-1, 1\}$

1.28 解: $\in$; $\subset$; $\subset$

1.29 解:原式 $= (A \cup B) - A = (A \cup B) \cap \bar{A}$
 $= (A \cap \bar{A}) \cup (B \cap \bar{A})$
 $= B \cap \bar{A} = B - A$

习题二解答

2.1 (1) 解: $A \times B = \{(0, 1), (0, 2), (1, 1), (1, 2)\}$

(2) 解: $A^2 \times B = A \times A \times B = \{(0,0,1), (0,0,2), (0,1,1), (0,1,2), (1,0,1), (1,0,2), (1,1,1), (1,1,2)\}$

(3) 解: $B \times A = \{(1,0), (1,1), (2,0), (2,1)\}$

(4) 解: $B^2 \times A = \{(1,1,0), (1,1,1), (1,2,0), (1,2,1), (2,1,0), (2,1,1), (2,2,0), (2,2,1)\}$

(5) 解: $(A \times B)^2 = (A \times B) \times (A \times B) = \{((0,1), (0,1)), ((0,1), (0,2)), ((0,1), (1,1)), ((0,1), (1,2)), ((0,2), (0,1)), ((0,2), (0,2)), ((0,2), (1,1)), ((0,2), (1,2)), ((1,1), (0,1)), ((1,1), (0,2)), ((1,1), (1,1)), ((1,1), (1,2)), ((1,2), (0,1)), ((1,2), (0,2)), ((1,2), (1,1)), ((1,2), (1,2))\}$

2.2 解: $X \times Y$ 是以 $x = -3, x = 2, y = -2, y = 0$ 为边的一个矩形面区域

2.3 (1) 证明:

$$\begin{aligned} A \times (B \cup C) &= \{(x, y) \mid x \in A \text{ 且 } y \in B \cup C\} \\ &= \{(x, y) \mid x \in A \text{ 且 } y \in B \text{ 或 } x \in A \text{ 且 } y \in C\} \\ &= \{(x, y) \mid (x, y) \in A \times B \text{ 或 } (x, y) \in A \times C\} \\ &= \{(x, y) \mid (x, y) \in A \times B \cup A \times C\} \\ &= (A \times B) \cup (A \times C) \end{aligned}$$

(2) 证明:

$$\begin{aligned} A \times (B \cap C) &= \{(x, y) \mid x \in A \text{ 且 } y \in B \cap C\} \\ &= \{(x, y) \mid x \in A \text{ 且 } y \in B \text{ 且 } x \in A \text{ 且 } y \in C\} \\ &= \{(x, y) \mid (x, y) \in A \times B \text{ 且 } (x, y) \in A \times C\} \\ &= \{(x, y) \mid (x, y) \in (A \times B) \cap (A \times C)\} \\ &= (A \times B) \cap (A \times C) \end{aligned}$$

(3) 证明: “ $\Rightarrow$ ”:

设 $A \times B = B \times A$, 则 $A = \emptyset$ 或 $B = \emptyset$;

或当 $A \neq \emptyset$ 且 $B \neq \emptyset$ 时,

对任意的 $a \in A$, 任意的 $b \in B$, 则有 $(a, b) \in A \times B$,

由于 $A \times B = B \times A$, 故有 $(a, b) \in B \times A$, 从而 $a \in B, b \in A$, 得到 $A \subseteq B$ 且 $B \subseteq A$, 所以 $A = B$

“ $\Leftarrow$ ”:

当 $A = \emptyset$ 时, $A \times B = \emptyset \times B = \emptyset = B \times \emptyset = B \times A$

当 $B = \emptyset$ 时, $A \times B = A \times \emptyset = \emptyset = \emptyset \times A = B \times A$

当 $A = B$ 时, $A \times B = A \times A = B \times A$

2.4 解: 先求 $R_1 = \{(0, 1), (1, 2), (2, 3), (0, 0), (2, 1)\}$, $R_2 = \{(2, 0), (3, 1)\}$, 则有: (1) $R_1 \circ R_2 = \{(1, 0), (2, 1)\}$

(2) $R_2 \circ R_1 = \{(2, 1), (2, 0), (3, 2)\}$

(3) $R_1 \circ R_2 \circ R_1 = \{(1, 1), (1, 0), (2, 2)\}$

2.5 (1) 证明: 对任意 $(a, c) \in R_1 \circ R_3$, 则存在 $b \in A$ 使得 $(a, b) \in R_1$ 且 $(b, c) \in R_3$, 由于 $R_1 \subseteq R_2$, 所以存在 $b \in A$ 使得 $(a, b) \in R_2$ 且 $(b, c) \in R_3$, 于是 $(a, c) \in R_2 \circ R_3$ 因而得 $R_1 \circ R_3 \subseteq R_2 \circ R_3$

(2) 证明: 对任意 $(a, c) \in R_3 \circ R_1$, 则存在 $b \in A$ 使得 $(a, b) \in R_3$ 且 $(b, c) \in R_1$, 由于 $R_1 \subseteq R_2$, 所以存在 $b \in A$ 使得 $(a, b) \in R_3$ 且 $(b, c) \in R_2$, 于是 $(a, c) \in R_3 \circ R_2$ 因而得 $R_3 \circ R_1 \subseteq R_3 \circ R_2$

2.6 证明定理 2-5 的其余部分.

(2) 证明: $\widehat{R_1 \cup R_2} = \{(x, y) \mid (y, x) \in R_1 \cup R_2\}$
 $= \{(x, y) \mid (y, x) \in R_1 \text{ 或 } (y, x) \in R_2\} = \{(x, y) \mid (x, y) \in \tilde{R}_1 \text{ 或 } (x, y) \in \tilde{R}_2\} = \{(x, y) \mid (x, y) \in \tilde{R}_1 \cup \tilde{R}_2\} = \tilde{R}_1 \cup \tilde{R}_2$

(4) 证明: $\widehat{A \times B} = \{(a, b) \mid (b, a) \in A \times B\}$
 $= \{(a, b) \mid (a, b) \in B \times A\} = B \times A$

(5) 证明: $\because \emptyset$ 不含有序偶; $\therefore \widetilde{\emptyset}$ 也不含有序偶, 即 $\widetilde{\emptyset}$ 是空集,
 $\therefore \widetilde{\emptyset} = \emptyset$

(8) 证明: 对任意的 $(x, y) \in \tilde{R}_1$, 则 $(y, x) \in R_1$, 由于 $R_1 \subseteq R_2$, 所

以 $(y, x) \in R_2$, 从而 $(x, y) \in \tilde{R}_2$, 于是 $\tilde{R}_1 \subseteq \tilde{R}_2$ 。

2.7 解: 错误是此人所推出的 aRa 中的 a 不代表 A 中的任意元素, 而是受到对称性限制的 (对称性未必涉及到 A 中的所有元素), 即仅适合 aRb 的那些 a , 而自反性则要求对 A 中的任意一个元素 a 均有 aRa 。

2.8 证明: 只需证明 $R_2 \circ R_1 \subseteq R_1 \circ R_2$

对任意的 $(a, c) \in R_2 \circ R_1$, 则存在 $b \in A$, 使 $(a, b) \in R_2$ 且 $(b, c) \in R_1$, 由于 R_1 和 R_2 都是对称的, 所以有: $(c, b) \in R_1$ 且 $(b, a) \in R_2$, 从而 $(c, a) \in R_1 \circ R_2$, 由条件知 $R_1 \circ R_2 \subseteq R_2 \circ R_1$ 成立, 所以 $(c, a) \in R_2 \circ R_1$ 。

因此存在 $d \in A$, 使 $(c, d) \in R_2$ 且 $(d, a) \in R_1$ 。

根据 R_1, R_2 的对称性, 有: $(a, d) \in R_1$ 且 $(d, c) \in R_2$, 故 $(a, c) \in R_1 \circ R_2$, 因此 $R_2 \circ R_1 \subseteq R_1 \circ R_2$ 。

所以有 $R_1 \circ R_2 = R_2 \circ R_1$ 。

2.9 证明: 对任意的 $a \in A$, $\because R$ 是自反的, $\therefore (a, a) \in R$, 又 $\because S$ 是自反的, $\therefore (a, a) \in S$ 。

根据复合运算和交运算的定义分别有 $(a, a) \in R \circ S$ 和 $(a, a) \in R \cap S$. $\therefore R \circ S$ 和 $R \cap S$ 都是自反的。

2.10 (1) 证明: “ $\Rightarrow$ ”: 对任意的 $(x, x) \in E$, $\because E$ 是恒等关系, $\therefore x$ 是 A 的任意元素, 由于 R 是自反的, 即 $(x, x) \in R$, 故 $E \subseteq R$ 。

“ $\Leftarrow$ ”对任意 $x \in A$, 则 $(x, x) \in E$, $\because E \subseteq R$, $\therefore (x, x) \in R$, 故 R 是自反的。

(2) 证明: “ $\Rightarrow$ ”假定 $E \cap R \neq \emptyset$, 则存在 $a \in A$, 使 $(a, a) \in E \cap R$. 即有 $(a, a) \in R$, 其中 $a \in A$, 因而 R 不是非自反的, 这与条件 R 是非自反的相矛盾, 故 $E \cap R = \emptyset$ 。

“ $\Leftarrow$ ”假定 R 不是非自反的,则存在 $(a,a) \in R$, 其中 $a \in A$, 由于 E 是 A 上的恒等关系, 对任意的 $a \in A$, 均有 $(a,a) \in E$, 因此存在 $(a,a) \in E \cap R$, 其中 $a \in A$, 这与条件 $E \cap R = \emptyset$ 相矛盾, 所以 R 是非自反的。

(3) 证明: “ $\Rightarrow$ ” $R = \{(x,y) \mid (x,y) \in R\} \xrightarrow{\text{对称}} \{(x,y) \mid (y,x) \in R\} = \{(x,y) \mid (x,y) \in \tilde{R}\} = \tilde{R}$ 。

“ $\Leftarrow$ ”对任意 $x, y \in A$, 若 $(x,y) \in R$, 由于 $R = \tilde{R}$, 故 $(x,y) \in \tilde{R}$, 从而 $(y,x) \in R$, 因此 R 是对称的。

(4) 证明: “ $\Rightarrow$ ”对任意的 $(x,y) \in R \cap \tilde{R} \neq \emptyset$, 则 $(x,y) \in R$ 且 $(x,y) \in \tilde{R}$, 即 $(x,y) \in R$ 且 $(y,x) \in R$, 因为 R 是反对称的, 所以 $x = y$, 即 $(x,y) = (x,x) \in E$, 故 $R \cap \tilde{R} \subseteq E$, 当 $R \cap \tilde{R} = \emptyset$ 时, 因为 $\emptyset$ 是任何集合的子集, 故亦有 $R \cap \tilde{R} = \emptyset \subseteq E$. “ $\Leftarrow$ ”对任意 $x, y \in A$, 若 $(x,y) \in R$ 且 $(y,x) \in R$, 则 $(x,y) \in R$ 且 $(x,y) \in \tilde{R}$, 于是 $(x,y) \in R \cap \tilde{R}$, 因为 $R \cap \tilde{R} \subseteq E$, 所以 $(x,y) \in E$, 从而 $x = y$, 故 R 是反对称的。

(5) 证明: “ $\Rightarrow$ ”对任意的 $(x,z) \in R \circ R$, 则存在 $y \in A$, 使 $(x,y) \in R$ 且 $(y,z) \in R$, 因为 R 是传递的, 所以 $(x,z) \in R$, 故有 $R \circ R \subseteq R$ 。

“ $\Leftarrow$ ”对任意的 $x, y, z \in A$, 如果 $(x,y) \in R$ 且 $(y,z) \in R$, 则 $(x,z) \in R \circ R$, 因为 $R \circ R \subseteq R$, 所以 $(x,z) \in R$, 故 R 是传递的。

2.11 (1) 解: $t(R_1) = \{(a,b), (a,c), (c,b)\}$

(2) 解: $t(R_2) = \{(a,b), (b,c), (c,c), (a,c)\}$

(3) 解: $t(R_3) = \{(a,b), (b,a), (c,c), (a,a), (b,b)\}$

(4) 解: $t(R_4) = R_4 \cup R_4^2 \cup R_4^3 = \{(a,b), (b,c), (c,a)\} \cup \{(a,c), (b,a), (c,b)\} \cup \{(a,a), (b,b), (c,c)\} = \{(a,a), (b,b), (c,c), (a,b), (a,c), (b,a), (b,c), (c,a), (c,b)\}$

2.12 (1) 证明: $\because R_1 \supseteq R_2, \therefore R_1 \cup E \supseteq R_2 \cup E$,

即 $r(R_1) \supseteq r(R_2)$ 。

(2) 证明: $\because R_1 \supseteq R_2$, 由定理 2-5(8) 知, $\widetilde{R_1} \supseteq \widetilde{R_2}$

$\therefore R_1 \cup \widetilde{R_1} \supseteq R_2 \cup \widetilde{R_2}$, 即 $S(R_1) \supseteq S(R_2)$

(3) 证明: 对任意的 $n \in N$, 根据数学归纳法可知: $R_1 \supseteq R_2 \Rightarrow R_1^n \supseteq R_2^n$ 。

对任意的 $(x, y) \in t(R_2) = R_2 \cup R_2^2 \cup R_2^3 \cup \dots$

则存在 $m \in N$, 使 $(x, y) \in R_2^m$, 有 $R_1^m \supseteq R_2^m$,

故 $(x, y) \in R_1^m$, 因此有 $(x, y) \in R_1 \cup R_1^2 \cup R_1^3 \dots = t(R_1)$, 所以有 $t(R_1) \supseteq t(R_2)$ 。

2.13 (1) 证明: $r(R_1 \cup R_2) = (R_1 \cup R_2) \cup E = (R_1 \cup E) \cup$

$(R_2 \cup E) = r(R_1) \cup r(R_2)$

(2) 证明: $S(R_1 \cup R_2) = (R_1 \cup R_2) \cup (\widetilde{R_1 \cup R_2})$

$= (R_1 \cup \widetilde{R_1}) \cup (R_2 \cup \widetilde{R_2})$

$= S(R_1) \cup S(R_2)$

(3) 证明: 对任意的 $n \in N$, 当 $n=2$ 时, $(R_1 \cup R_2)^2 = R_1^2 \cup (R_1 \circ R_2) \cup (R_2 \circ R_1) \cup R_2^2 \supseteq R_1^2 \cup R_2^2$

假定 $n=k$ 时有 $(R_1 \cup R_2)^k \supseteq R_1^k \cup R_2^k$, 则 $(R_1 \cup R_2)^{k+1} = (R_1 \cup R_2)^k \circ (R_1 \cup R_2) \supseteq (R_1^k \cup R_2^k) \circ (R_1 \cup R_2) = R_1^{k+1} \cup (R_1^k \circ R_2) \cup (R_2^k \circ R_1) \cup R_2^{k+1} \supseteq R_1^{k+1} \cup R_2^{k+1}$

于是 $(R_1 \cup R_2)^n \supseteq R_1^n \cup R_2^n$, 对任意的 n 均成立。

$t(R_1 \cup R_2) = (R_1 \cup R_2) \cup (R_1 \cup R_2)^2 \cup (R_1 \cup R_2)^3 \dots = \bigcup_{n=1}^{\infty} (R_1 \cup$

$R_2)^n \supseteq \bigcup_{n=1}^{\infty} (R_1^n \cup R_2^n) = (\bigcup_{n=1}^{\infty} R_1^n) \cup (\bigcup_{n=1}^{\infty} R_2^n) = t(R_1) \cup t(R_2)$

2.14 (1) 证明: 用归纳法。

当 $k=1$ 时, $R^{s+1} = R^s \circ R = R^t \circ R = R^{t+1}$

假设当 $k=n$ 时成立, 即 $R^{s+n} = R^{t+n}$,

对 $k=n+1$ 时,

$R^{s+n+1} = R^{s+n} \circ R = R^{t+n} \circ R = R^{t+n+1}$,

故 $R^{s+k} = R^{t+k}$ 。

(2) 证明:用归纳法。

当 $k=1$ 时, $R^{s+i+p} = R^{s+i+t-s} = R^{t+i} = R^{s+i}$ (由(1)得)

假设当 $k=n$ 时成立,即 $R^{s+i+n(t-s)} = R^{s+i}$,

对 $k=n+1$ 时有:

$$\begin{aligned} R^{s+i+(n+1)(t-s)} &= R^{s+i+n(t-s)+(t-s)} = R^{s+i+(t-s)} \\ &= R^{t+i} = R^{s+i} \text{ (由(1)得)。} \end{aligned}$$

2.15 证明: $\because R$ 是集合 A 上的等价关系,则

(1) $\because R$ 是自反的,即对任意 $x \in A$,有 $(x, x) \in R$,

$\therefore (x, x) \in \tilde{R}$. $\therefore \tilde{R}$ 是自反的。

(2) $\because R$ 是对称的,对任意 $(x, y) \in R$,有 $(y, x) \in R$,

$\therefore$ 有 $(y, x) \in \tilde{R}, (x, y) \in \tilde{R}$. $\therefore \tilde{R}$ 是对称的。

(3) $\because R$ 是传递的. 即如果有 $(x, y) \in R, (y, z) \in R$ 有 $(x, z) \in R$, $\therefore$ 对应有如果 $(y, x) \in \tilde{R}, (z, y) \in \tilde{R}, (z, x) \in \tilde{R}$, $\therefore \tilde{R}$ 满足传递性。

由(1)~(3)知 R 的逆关系 $\tilde{R}$ 也是 A 上的等价关系。

2.16 证明:根据条件若 $ad=bc$,则 $(a, b) \sim (c, d)$

(1) $\because ab=ba \therefore (a, b) \sim (a, b)$ 是自反的。

(2) $\because$ 若有 $(a, b) \sim (c, d), \therefore ad=bc, \therefore cb=da$

$\therefore (c, d) \sim (a, b)$, 满足对称性。

(3) $\because$ 若有 $(a, b) \sim (c, d), (c, d) \sim (e, f),$

$$\therefore ad=bc, cf=de, \text{可得 } c=\frac{ad}{b}, c=\frac{de}{f},$$

$$\frac{ad}{b}=\frac{de}{f} \therefore af=be, \therefore \text{有 } (a, b) \sim (e, f) \text{ 满足传递性}$$

故由(1)~(3)可知 $\sim$ 是一个等价关系。

2.17 解:等价类是: $[1]=\{1,5\}, [2]=\{2,3,6\}$
 $[3]=\{3,2,6\}, [4]=\{4\}, [5]=\{5,1\}, [6]=\{6,2,3\}$ 。

2.18 证明:如果 R 是集合 A 上的相容关系,对于 A 中的任意元素 a ,集合 $\{a\}$ 是一个相容类,且可对此集合不断地添加新的元素,直到使它成为最大相容类,因而 A 中的每个元素都将是某一个最大相容类中的元素,所以相容关系 R 产生的所有最大相容类构成的集合是 A 的一个覆盖;又由最大相容类的定义可知,一个最大相容类不可能是另一个最大相容类的子集,故由此最大相类构成的集合是 A 的惟一的完全覆盖。

2.19 解: $\{\{a,b,c,d\}\}; \{\{a\}, \{b\}, \{c\}, \{d\}\}$ 。

2.20 答:B

2.21 答:自反;对称。

2.22 解: $S(R)=\{(a,a), (a,b), (b,a)\}$ 。
 $t(R)=R \cup R^2 \cup R^3=\{(a,a), (a,b)\}$ 。

2.23 解: $R^2=R \circ R=\{(b,b), (a,a), (c,c), (d,d)\}$
 $R^3=R^2 \circ R=\{(b,a), (a,b), (c,c), (d,d)\}$ 。

2.24 解: $A_3; A_3$ 。

2.25 解: $S(R \cap Q)=R \cap Q; t(R \cap Q)=R \cap Q$ 。

习题三解答

3.1 (1) 解:不能构成函数。

(2) 解:可以构成函数,实际上对应每个实数 r_1 ,只有惟一的实数 r_1^2 ,即 r_2 。

(3) 解:不能构成函数,比如 $r_1 = 9$,在本法则对应下,有 $r_2 = 3$ 及 $r_2 = -3$ 两个象了。

(4) 解:可以构成函数,建下表说明:

n_1	1	2	3	4	5	6	7	8	9	10	11	12	13	14...
n_2	0	0	1	2	2	3	3	4	4	4	4	5	5	6...

对应于每个 n_1 ,有且只有一个“小于 n_1 的素数的数目”,表中加 □者为素数。

3.2 证明: $\because$ 对任意的 $S \in 2^u$,则存在 $(S_1, S_2) \in 2^u \times 2^u$,

使 $f(S_1, S_2) = S$ (事实上,令 $S_1 = S, S_2 = u$),

则 $f(S_1, S_2) = f(S, u) = S \cap u = S$ 。

$\therefore f$ 是从 $2^u \times 2^u$ 到 2^u 的满射,从而 f 的陪域和值域都是 2^u 。

3.3 解:其中(4)、(6)是普通的映射;(1)、(2)是一一对映射;
(3)、(5)是满射;(3)又是一一对应映射。

3.4 解:设 A 和 B 是有限集合, $|A| = m, |B| = n$,要使映射为一对一映射,必须有 $|A| \leq |B|$,即 $m \leq n$ 。在 B 中任意选出 m 个元素的任一全排列,都能形成 $A \rightarrow B$ 的一个不同的一对一映射,故 $f: A \rightarrow B$ 的不同的一对一映射有: $C_n^m \cdot m!$ 个。

如果又要使 $f: A \rightarrow B$ 为双射,必须有 $|A| = |B|$,

设 $A = \{a_1, a_2, \dots, a_m\}, B = \{b_1, b_2, \dots, b_m\}$,

则对 a_1 的对应的元素共有 m 种取法, a_2 的对应元素在 a_1 取定后

共有 $m-1$ 种取法, a_3 的对应元素在 a_1 和 a_2 取定后共有 $m-2$ 种取法, 以此类推, a_m 对应元素有 $m-(m-1)$ 种取法。故 $f:A \rightarrow B$ 的不同的一一对应映射共有: $m(m-1)(m-2)\cdots(m-m+1)=m!$ 个。

3.5 证明:

(1) $\because f \circ g$ 是一一对映射,

$\therefore$ 如果 f 不是一一对映射, 则必存在 $a_1 \neq a_2$ 时,

有 $f(a_1) = f(a_2) = b \in B$,

由于 $f \circ g(a_1) = g(f(a_1)) = g(f(a_2)) = f \circ g(a_2)$ 得出 $f \circ g$ 不是一对一的, 与题设矛盾。

(2) 设任意的 $c \in C$, 因为 $f \circ g$ 是满射, 故必有 $a \in A$, 使得 $f \circ g(x) = c$, 因为 $f \circ g(a) = g(f(a))$, 此处 $f(a) = b \in B$, 由 g 是函数, 故每个 $b \in B$, 必有 $c \in C$, 使 $c = g(b)$, 但每个 c 在 g 作用下都是 B 中元素的一个象, 由 c 的任意性, 可知 g 是满射的。

(3) 因为 $f \circ g$ 是一一对应的映射, 故 $f \circ g$ 是满射和一对一映射, 由上述(1)和(2)可知 f 是一一对映射, g 是满射。

3.6 证明: (1) $\because f:A \rightarrow B$ 有逆映射 $\tilde{f}:B \rightarrow A$,

$\therefore$ 任取 $(a, b) \in f$, 有 $(b, a) \in \tilde{f} \Rightarrow (a, a) \in f \circ \tilde{f} \Rightarrow f \circ \tilde{f} = E_A$ 。

证明: (2) $\because f:A \rightarrow B$ 有逆映射 $\tilde{f}:B \rightarrow A$,

$\therefore$ 任取 $(b, a) \in \tilde{f}$, 有 $(a, b) \in f$,

$\Rightarrow (b, b) \in \tilde{f} \circ f \Rightarrow \tilde{f} \circ f = E_B$ 。

证明: (3) $\because f:A \rightarrow B$ 有逆映射 $\tilde{f}:B \rightarrow A$,

$\therefore$ 任取 $(a, b) \in f$, 有 $(b, a) \in \tilde{f} \Rightarrow (a, b) \in \tilde{\tilde{f}} \Rightarrow \tilde{\tilde{f}} = f$ 。

3.7 证明: $\because f:A \rightarrow B, g:B \rightarrow C$ 均为双射, $\therefore f \circ g$ 是从 A 到 C 的双射, 故 $\widetilde{f \circ g}$ 是 C 到 A 的双射, 又 $\tilde{g} \circ \tilde{f}$ 是 C 到 A 的双射, 所以 $\widetilde{f \circ g}$ 和 $\tilde{g} \circ \tilde{f}$ 有相同的定义域 C , 有相同的陪域 A 。

对任意的 $c \in C$, 则存在 $a \in A$ 使 $\widetilde{f \circ g}(c) = a$, 于是 $f \circ g(a) = c$, 即

$g(f(a))=c$, 由于 g^{-1} 是 C 到 B 的双射, 所以 $f(a)=g^{-1}(c)$, 又由于 $\tilde{f}$ 是 B 到 A 的双射, 所以 $a=\tilde{f}(\tilde{g}(c))$, 即 $a=\tilde{g}\circ\tilde{f}(c)$, 从而对任意的 $c\in C$, $\widetilde{f\circ g}(c)=\tilde{g}\circ\tilde{f}(c)$, 可见 $\widetilde{f\circ g}=\tilde{g}\circ\tilde{f}$.

3.8 解: 本题 A 到 B 的一种满射 f 的定义域对任意的 $x\in A$,

$$f(x)=\begin{cases} x & \text{当 } 0\leq x\leq 1, \\ \frac{1}{x} & \text{当 } 1\leq x<+\infty \end{cases} \quad x\in R$$

注: 本题的 f 不惟一。

3.9 解: $\because \varnothing$ 是 A 到 B 的双射, $\therefore a\in A$, 则 $\widetilde{\varnothing}(\varnothing(a))=\widetilde{\varnothing}(b)=a$. 而 $\varnothing(\widetilde{\varnothing}(a))$ 不存在。

但如果 $\varnothing$ 是 A 上的双射, 即 $\varnothing:A\rightarrow A$, 有 $a\in A$, 则 $\widetilde{\varnothing}(\varnothing(a))=a$, $\varnothing(\widetilde{\varnothing}(a))=a$.

3.10 解: 可举例说明之, 设 $A=\{a\mid a\in R, 0\leq a\leq 1\}$, $B=\{\dots, -2, -1, 0, 1, 2, \dots\}$ 都是无限集, 但是 $A\cap B=\{0, 1\}$ 是有限集, 故两个无限集之交不一定是无限集。

3.11 解: 不一定, 可举例说明之, 设 $A=\{0, 1, 2, \dots\}$, $B=\{1, 2, \dots\}$ 都是无限集且 $B\subseteq A$, 而 $A-B=\{0\}$ 是有限集, 故当 A, B 都是无限集时, $A-B$ 不一定无限。又如 $A=\{\dots, -1, 0, 1, \dots\}$, $B=\{1, 2, \dots\}$ 都是无限集且 $B\subseteq A$, 而 $A-B=\{\dots, -1, 0\}$ 是无限集, 故当 A, B 都是无限集时, $A-B$ 不一定有限。

3.12 证明: 根据集合及其幂集中元素之间个数的关系, 有:

$$\begin{array}{ccc} |\rho(1)| & |\rho(2)| \cdots & |\rho(k)| \cdots \\ \downarrow & \downarrow \cdots & \downarrow \cdots \\ 2^1 & 2^2 & 2^k \cdots \end{array}$$

利用数学归纳法,在 $N=1$ 时, $|\rho(1)|=2^1$,

假设当 $N=k$ 时成立,即 $|\rho(k)|=2^k$ 。

当 $N=k+1$ 时,相邻项的个数关系为 2 倍的关系,

即 $|\rho(k+1)|=|\rho(k)|\times 2=2^k\times 2=2^{k+1}$ 。

根据一一对应关系有 $|\rho(N)|=2^{|N|}$,而 N 的基数为 $\aleph_0$,故有 $|\rho(N)|=2^{\aleph_0}$ 。

3.13 解: $\because f(x)=2x+1, g(x)=x^2-2$,

$$\begin{aligned}\therefore f\circ g &= g(f(x)) = g(2x+1) = (2x+1)^2 - 2 \\ &= 4x^2 + 4x + 1 - 2 = 4x^2 + 4x - 1.\end{aligned}$$

3.14 解:(1) $\because f$ 是实数集 R 到实数集 R 的映射, $f(x)=x$ 是一一对应映射,它的象集为 R ,有逆映射 $\tilde{f}(x)=x$ 。

(2) 象集是 N ,无逆映射。

(3) 象集是 R_+ ,无逆映射。

3.15 答:A

3.16 解:例: $f:N\rightarrow N, f(n)=n+2, N=\{0,1,2,\cdots\}$, f 是一对一映射,但 $0,1\notin f(N)$,因此 f 不是满射,所以不是一一对应的。

3.17 答:D

3.18 答:A

3.19 答:C

习题四解答

4.1 解:(1) $2*3=17$; $3*(-5)=-32$;

$$7 * \frac{1}{2} = \frac{29}{2}.$$

(2) 是半群, 是交换半群。

(3) 单位元素是 0。

(4) $a \in R - \{-\frac{1}{2}\}$, 即实数集 R 中除去 $-\frac{1}{2}$ 后的元素都有逆元

素, 逆元素为: $a^{-1} = -\frac{a}{1+2a}$ 。

4.2 解:

运 算 集 合	+	×	—	$ x-y $	$\max(x,y)$	$\min(x,y)$
I	是	是	是	是	是	是
N	是	是	否	是	是	是
$\{x 0 \leq x \leq 10\}$	否	否	否	是	是	是
$\{x -10 \leq x \leq 0\}$	否	否	否	否	是	是
$\{2x x \in I\}$	是	是	是	是	是	是

4.3 解: $a \in R, b \in R - \{0\}$

运 算 性 质	+	—	×	÷	max	min	$ x-y $
结合律	是	否	是	否	是	是	否
交换律	是	否	是	否	是	是	是
单位元	0	无	1	无	无	无	无
逆 元	$-a$	无	$\frac{1}{b}$	无	无	无	无

4.4 对任意的 $x, y, z \in N_k, \therefore (x f_k y) f_k z = x f_k (y f_k z)$

$$= \begin{cases} x+y+z & \text{当 } x+y+z < k \\ x+y+z-k & \text{当 } k \leq x+y+z < 2k \\ x+y+z-2k & \text{当 } x+y+z \geq 2k \end{cases}$$

$\therefore f_k$ 满足结合律。

$\because 0 \in N_k$ 且对任意 $x \in N_k$ 有 $xf_k 0 = 0f_k x = x + 0 = x$ 。

$\therefore 0$ 是单位元素。

又对任意 $x \in N_k - \{0\}$ $\because xf_k(k-x) = (k-x)f_k x$

$= (x + (k-x)) - k = 0 \quad \therefore$ 非 0 的 x 的逆元素是 $k-x$, 另外, 0 的逆元是 0 自己。

4.5 解: (1) $\because$ 对任意的 $a, b, c \in A, (a * b) * c = a * c = a, a * (b * c) = a * b = a. \quad \therefore (a * b) * c = a * (b * c)$

$\therefore$ 是半群。

解: (2) $\because$ 对任意的 $a, b \in A, a * b = a$, 而 $b * a = b$ 。

$\therefore a * b \neq b * a$, 故不是交换半群。

解: (3) 无单位元素。

4.6 证明: $(a * b)^n = (a * b) * (a * b) * \cdots * (a * b)$

* 可结合 $a * (b * a) * (b * a) * \cdots * (b * a) * b$

* 可交换 $(a * a \cdots * a) * (b * b \cdots * b) = a^n * b^n$ 。

4.7 证明: 令 $G = \{f \mid \forall x \in R, f(x) = ax + b, a \neq 0, a, b \in R\}$

(1) 对任意 $x \in R, E_R(x) = x = 1 \times x + 0$, 故 $E_R \in G$, 从而 $G \neq \emptyset$ 。

(2) 对任意的 $f, g \in G$, 则存在 $a, b, c, d \in R, a \neq 0, c \neq 0$, 使 $f(x) = ax + b, g(x) = cx + d$, 于是 $f \circ g(x) = g(f(x)) = g(ax + b) = c(ax + b) + d = acx + (bc + d)$, 由于 $ac, bc + d \in R$ 且 $ac \neq 0$,

故 $f \circ g \in G$, 知复合运算 $\circ$ 是 G 上封闭的二元运算。

(3) $\circ$ 满足结合律。

(4) $(G, \circ)$ 的单位元素是 E_R 。

(5) 对任意的 $f \in G$, 任意的 $x \in R$, 有 $f(x) = ax + b$, 其中 $a, b \in R, a \neq 0$, 由于 $g(x) = \frac{1}{a}x + \frac{-b}{a}$ 所定义的 $g \in G$, 具有 $f \circ g(x) =$

$$g(f(x)) = \frac{1}{a}(ax+b) + \frac{-b}{a} = x = E_R(x)$$

$$g \circ f(x) = f(g(x)) = a \cdot \left(\frac{1}{a}x + \frac{-b}{a}\right) + b = x = E_R(x)。$$

故 $f \circ g = g \circ f = E_R$, 所以 g 是 f 的逆元素。

由(1)~(5)知 $(G, \circ)$ 是一个群。

设 $f_1, f_2 \in G$, 对任意的 $x \in R$, $f_1(x) = 2x + 5$, $f_2(x) = 3x + 7$,

则 $f_1 \circ f_2(x) = f_2(2x + 5) = 3 \times (2x + 5) + 7 = 6x + 22$

$$f_2 \circ f_1(x) = f_1(3x + 7) = 2 \times (3x + 7) + 5 = 6x + 19,$$

可见 $f_1 \circ f_2 \neq f_2 \circ f_1$, 因此 $(G, \circ)$ 不是阿贝尔群。

4.8 证明: 设 $(G, \circ)$ 是某个集合 A 的一些变换构成的变换群, 设 ϵ 是 $(G, \circ)$ 的单位元素, 对任意的 $f \in G$, 若 g 是 f 的逆元, 那么 $f \circ g = g \circ f = \epsilon$, 于是对任意的 $x \in A$,

$\epsilon(x) = g \circ f(x) = f \circ g(x) = x$, 然而当 E_A 为 A 的恒等映射时, $E_A(x) = x$; 由此可见 $\epsilon = E_A$, 所以 $(G, \circ)$ 的单位元素必是恒等映射。

4.9 证明: 见书中例 4-9, 知 6 的最大公因子是 3。

4.10 证明: 对任意的 $a, b \in G$, 有 $a * b \in G$,

$\because$ 一个元素的逆元素是它自己, 于是 $a * b = (a * b)^{-1} = b^{-1} * a^{-1} = b * a$,

$\therefore (G, *)$ 是阿贝尔群。

4.11 证明: 设群的阶 $|G| = P$ 是素数, a 不是 G 的单位元素, 若 a 的阶是 m , 则 $m \neq 1$, 由定理 4-17 可知,

$H = \{a^r | r \in I\}$ 关于 $*$ 是一个 m 阶循环子群, 又由定理 4-25 可知, m 是 P 的因数, 但素数 P 只有因数 P 和 1, m 又不等于 1, 故 $m = P$, 由定理 4-18 可知, $(G, *)$ 是一个循环群。

4.12 证明: 设有子群 H 的任意两个左陪集 aH, bH , 其乘积为: $aH * bH = (a * b)H$ 对 $h_1, h_2, h_3 \in H$, 有 $a * h_1 = n_1 \in aH, b * h_2 = n_2 \in bH, n_1 * n_2 = (a * b) * h_3 \in (a * b)H$,

$$h_3 = (a * b)^{-1} * n_1 * n_2 = b^{-1} * a^{-1} * a * h_1 * b * h_2 = b^{-1} * h_1 * b * h_2 \in H$$

由定理 4-7 得: $b^{-1} * h_1 * b \in H$;

同理对 $bH * aH = (b * a)H$, 有 $h_4 \in H$,

$$n_2 * n_1 = (b * a) * h_4 \in (b * a)H$$

$$h_4 = (b * a)^{-1} * n_2 * n_1 = a^{-1} * b^{-1} * b * h_2 * a * h_1 = a^{-1} * h_2 * a * h_1 \in H$$

得: $a^{-1} * h_2 * a \in H$ 。

故 H 是正规子群。

4.13 解: (1) 1 阶子群 ($\{[0]\}, +_{12}$)。

(2) 2 阶子群 ($\{[0], [6]\}, +_{12}$)。

(3) 3 阶子群 ($\{[0], [4], [8]\}, +_{12}$)。

(4) 4 阶子群 ($\{[0], [3], [6], [9]\}, +_{12}$)。

(5) 6 阶子群 ($\{[0], [2], [4], [6], [8], [10]\}, +_{12}$)。

(6) 12 阶子群 ($Z_{12}, +_{12}$)。

4.14 解: ($Z_6, +_6$) 是交换群, 左右陪集相等, 都是 $\{[0], [3]\}, \{[1], [4]\}$ 和 $\{[2], [5]\}$ 。

4.15 证明: “ $\Rightarrow$ ” 设 $a \in G$, 因为 $\{h | h \in H\} = H = Ha = \{h * a | h \in H\}$, 故有 $h_1 \in H$ 使 $h_1 = h * a$,

于是 $a = h^{-1} * h_1$, 因为 $(H, *)$ 是 $(G, *)$ 的子群, 所以 $h^{-1} * h_1 \in H$, 即 $a \in H$ 。

“ $\Leftarrow$ ” 因为 $a \in H$, 所以对任意的 $x \in H$, 则 $a^{-1} \in H$, 因而 $x * a^{-1} \in H$, 于是存在 $h_1 \in H$, 使 $h_1 = x * a^{-1}$, 即 $x = h_1 * a \in Ha$, 所以 $H \subseteq$

Ha , 另外, 对任意的 $y \in Ha$, 则存在 $h_2 \in H$, 使 $y = h_2 * a$, 因为 $a \in H$, 所以 $y \in H$, 故 $Ha \subseteq H$, 从而有 $H = Ha$ 。

4.16 证明: $H \cap N$ 是 H 的非空子集, N 是 G 的正规子群。

对于任意的 $x, y \in H \cap N$, 有 $x, y \in H$ 且 $x, y \in N$, 从而有 $x * y \in H$ 且 $x * y \in N$, 于是 $x * y \in H \cap N$, 又有对任意的 $x \in H \cap N$, 有 $x \in H$ 且 $x \in N$, 从而有 $x^{-1} \in H$ 且 $x^{-1} \in N$, 于是 $x^{-1} \in H \cap N$, 因此, $H \cap N$ 是 H 的子群;

另有对任意的 $x \in H \cap N, h \in H$ 有 $h^{-1} * x * h \in H$ 且 $h^{-1} * x * h \in N$, 于是 $h^{-1} * x * h \in H \cap N$, 所以 $H \cap N$ 是 H 的正规子群。

4.17 证明: 设有环 $(R, +, \cdot), (J, +, \cdot), (K, +, \cdot)$ 是 R 的理想子环,

$\because$ 对任意的 $a, b \in J \cap K$, 有 $a, b \in J$ 且 $a, b \in K, a \cdot b \in J$ 且 $a + b \in J$ 且 $a \cdot b \in K$ 且 $a + b \in K$ 且 $-a \in J$ 且 $-a \in K$,

$\therefore a \cdot b \in J \cap K, a + b \in J \cap K, -a \in J \cap K, \therefore (J \cap K, +, \cdot)$ 是子环, 又 $\because$ 对任意的 $a \in J \cap K$, 有 $a \in J$ 且 $a \in K$, 对任意的 $x \in R$, 有 $ax \in J$ 且 $ax \in K$ 且 $x \cdot a \in J$ 且 $x \cdot a \in K, \therefore a \cdot x \in J \cap K, x \cdot a \in J \cap K, \therefore (J \cap K, +, \cdot)$ 是理想子环。

4.18 证明:

(1) $\because a \cdot b = b \cdot a \quad \therefore a \cdot (-b) = -(a \cdot b) = -(b \cdot a) = (-b) \cdot a$

又 $\because$ 根据所需证明的 $a \cdot b^{-1} = b^{-1} \cdot a$, 可知元素 b 存在乘法逆元素, 且乘法单位元素 1 也存在。

$$\begin{aligned} \therefore a \cdot (b^{-1}) &= 1 \cdot (a \cdot b^{-1}) = (b^{-1} \cdot b) \cdot (a \cdot b^{-1}) \\ &= b^{-1} \cdot (b \cdot a) \cdot b^{-1} = b^{-1} \cdot (a \cdot b) \cdot b^{-1} \\ &= (b^{-1} \cdot a) \cdot (b \cdot b^{-1}) = (b^{-1}) \cdot a. \end{aligned}$$

(2) $\because a \cdot b = b \cdot a$ 且 $a \cdot c = c \cdot a$,

$$\therefore a \cdot (b+c) = a \cdot b + a \cdot c = b \cdot a + c \cdot a = (b+c) \cdot a$$

$$\begin{aligned} \therefore a \cdot (b \cdot c) &= (a \cdot b) \cdot c = (b \cdot a) \cdot c = b \cdot (a \cdot c) = b \cdot (c \cdot a) \\ &= (b \cdot c) \cdot a. \end{aligned}$$

4.19 证明:

(1) $\because 1^{-1} = 1 \in R, \therefore 1 \in G$, 且 G 非空,

对于任意的 $a, b \in G$, 必有 $a^{-1} \in R$ 且 $b^{-1} \in R$, 故 $b^{-1} \cdot a^{-1} \in R$, 并且 $(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = (a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = 1$, 因此 $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1} \in R$, 于是 $a \cdot b \in G$, 故 $(G, \cdot)$ 是封闭的。

(2) $\because G$ 是 R 的子集, $\therefore \cdot$ 在 G 上是可结合的。

(3) $\because$ 对于任意的 $a \in G$, 必有 $a^{-1} \in R$, 由于 a 与 a^{-1} 互为逆元素

$$\therefore (a^{-1})^{-1} = a \in R, \therefore a^{-1} \in G.$$

(4) $\cdot$ 运算的单位元素 $1 \in G$ 。

$\therefore$ 由 (1)~(4) 可知 $(G, \cdot)$ 是一个群。

4.20 证明:

(1) $\because$ 对于任意的 $a, b \in R$, 都有 $a+b \in R, a^2 = a$

$$\begin{aligned} \therefore (a+b) \cdot (a+b) &= a+b \Rightarrow a \cdot a + a \cdot b + b \cdot a + b \cdot b = a+b \Rightarrow \\ a+a \cdot b+b \cdot a+b &= a+b, \end{aligned}$$

$$\therefore \text{其中 } a \cdot b + b \cdot a = 0, \text{ 即 } a \cdot b = -b \cdot a.$$

$$\begin{aligned} (2) \because \text{对任意的 } a \in R, \text{ 均有 } a+a \in R, a^2 = a, \therefore (a+a) \cdot (a+a) &= a+a \Rightarrow a \cdot a + a \cdot a + a \cdot a + a \cdot a = a+a \Rightarrow a+a+a+a, \therefore a+a \\ &= 0. \end{aligned}$$

由此 (2) 的结论可知 $b \cdot a = -ba$, 再与上述 (1) 的结论 $a \cdot b = -b \cdot a$ 相比较, 可知 $a \cdot b = b \cdot a$, $\therefore R$ 满足交换律。

(3) 用反证法, 如果 $(R, +, \cdot)$ 是一个整环, 且有三个或三个以上的元素, 则存在 $a \in R, a \neq 0, a \neq 1$ 且 $a \cdot a = a$,

$$\text{即有: } a \neq 0, a-1 \neq 0 \text{ 且 } a \cdot (a-1) = a \cdot a - a = a - a = 0,$$

这与整环中的无零因子条件相矛盾。所以 $(R, +, \cdot)$ 不可能是

一个整环。

4.21 解: $(Z_3, +_3, \cdot_3)$ 是一个具有 3 个元素的域。

其中 $+_3$ 为模 3 加法, $\cdot_3$ 为模 3 乘法。 $Z_3 = \{0, 1, 2\}$ 。

4.22 (1) 证明: 由运算表知 $(F, +)$ 对运算 $+$ 是可结合和可交换的, a 是 $+$ 运算的单位元素, 任一元素均有逆元素, $-a = a, -b = b, -c = c, -d = d$, 故 $(F, +)$ 是阿贝尔群, 除了零元素 a 以外, $(F - \{a\}, \cdot)$ 也是一个阿贝尔群, 且 $\cdot$ 对 $+$ 运算满足分配律, 乘单位元素为 b , 所以 $(F, +, \cdot)$ 是域

$$(2) \text{ 对方程组: } \begin{cases} x + c \cdot y = a & (1) \\ c \cdot x + y = b & (2) \end{cases}$$

$$(2) \cdot (-c) + (1) \text{ 得: } x - c^2 \cdot x = a - b \cdot c,$$

$$(b - d) \cdot x = a - c, c \cdot x = c, x = b,$$

$$\text{将 } x = b \text{ 代入 (2) 得: } y = b - c \cdot b = b - c = d,$$

$$\text{故方程组的解为: } \begin{cases} x = b \\ y = d \end{cases}.$$

4.23 解: 此时 $(R, +, \cdot)$ 不一定是整环, 可举一例来说明, 例如令 $(F, +, \cdot)$ 为 $(Q, +, \cdot)$, 有理数上的普通加法和乘法, 是一个域, 令 $(R, +, \cdot)$ 为 $(\{2x | x \in I\}, +, \cdot)$, 偶整数集合上的普通加法和乘法, 则此时 $(R, +, \cdot)$ 为 $(F, +, \cdot)$ 的子环, 但它不含乘单位元素, 不是整环。

4.24 解: 图(a)不是格; 图(b)是格; 图(c)是格; 图(d)不是格。

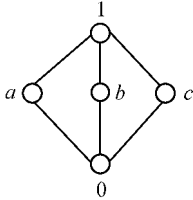
4.25 证明: 令 $L = \{a_1, a_2, \dots, a_n\}$, 则 $a_1 \vee a_2 \vee \dots \vee a_n$ 是 L 的上界, 即最大元素,

$a_1 \wedge a_2 \wedge \dots \wedge a_n$ 是 L 的下界, 即最小元素。

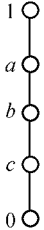
4.26 解: $\Pi_1 \vee \Pi_2 = \Pi_1 \cup \Pi_2 = \{\{a, d\}, \{b, c\}, \{e, g, i\}, \{f\}, \{h\}, \{a, f\}, \{d\}, \{e, h\}, \{g, i\}\}.$
 $\Pi_1 \wedge \Pi_2 = \Pi_1 \cap \Pi_2 = \{\{b, c\}\}.$

4.27 答: (a)是有补格, (b)是有补格, (c)不是有补格。

4.28 解:



是有补格
不是分配格;



是分配格
不是有补格。

4.29 解: $\bar{1}=0, \quad \bar{a}=f, \quad \bar{b}=e, \quad \bar{c}=d.$
 $\bar{0}=1, \quad \bar{f}=a, \quad \bar{e}=b, \quad \bar{d}=c.$

4.30 答:D。

4.31 答:B。

4.32 答:C。

4.33 答:D。

4.34 答:四阶元素时;同构的。

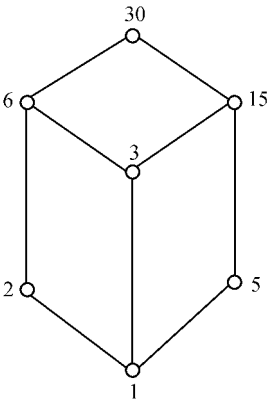
4.35 答:最小上界和最大下界; $x \vee y = lub(x, y); x \wedge y = glb(x, y).$

4.36 答:A。

4.37 答:A。

4.38 答: $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

4.39 解:



∵其中任意两个元素都有最大下界和最小上界存在。
∴是格。

4.40 答:C。

4.41 答:B。

4.42 答:C。

4.43 答:可;不一定有。

4.44 答:1;2。

4.45 解:在单位元素唯一的条件下,有 $a * a_{\text{右}}^{-1} = a_{\text{左}}^{-1} * a = e$
 $\Rightarrow a * a_{\text{右}}^{-1} * a_{\text{右}}^{-1} = a_{\text{左}}^{-1} * a * a_{\text{右}}^{-1} \Rightarrow e * a_{\text{右}}^{-1} = a_{\text{左}}^{-1} * e \Rightarrow a_{\text{右}}^{-1} = a_{\text{左}}^{-1}$ 。

反证法:若有 2 个右逆元: $a_{\text{右}}^{-1}, a_{\text{右}'}^{-1}$, 则: $a * a_{\text{右}}^{-1} = a * a_{\text{右}'}^{-1} = e$
 $\Rightarrow a_{\text{左}}^{-1} * a * a_{\text{右}}^{-1} = a_{\text{左}}^{-1} * a * a_{\text{右}'}^{-1} \Rightarrow e * a_{\text{右}}^{-1} = e * a_{\text{右}'}^{-1} \Rightarrow a_{\text{右}}^{-1} = a_{\text{右}'}^{-1}$ 。

同理有 $a_{\text{左}}^{-1} = a_{\text{左}'}^{-1}$, 故结论成立。

4.46 答:A。

4.47 答:C。

4.48 答:D。

4.49 答:B。

4.50 0;单位元素。

4.51 $\emptyset$;A。

4.52 解:根据运算表有:

① 满足封闭性;② 满足结合律;③ 满足交换律;④ 不满足等幂律;⑤ 有单位元素 a ;⑥ a 和 b 有逆元素: $a^{-1} = a, b^{-1} = b, c$ 无逆元素;⑦ 有零元素为 c 。

4.53 答:C。

4.54 答:A。

4.55 答:1 和 -1。

4.56 答:不是;没有乘单位元素。

4.57 证明:令 $f:R \rightarrow R^+, f(x)=e^x$ 为双射。

对任意 $a, b \in R, f(a)=e^a, f(b)=e^b$

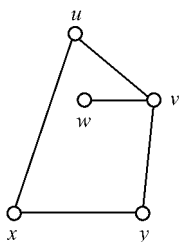
$$\because f(a+b)=e^{a+b}=e^a * e^b = f(a) * f(b)$$

$$\therefore (R, +) \cong (R^+, *).$$

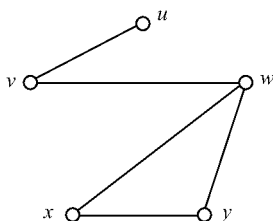
习题五解答

5.1 解:

(1)



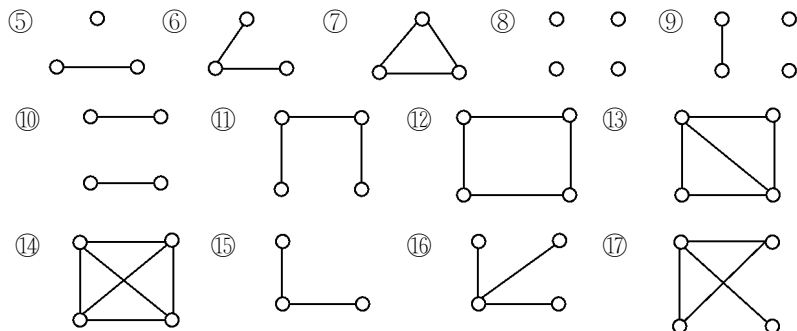
(2)

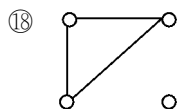


5.2 解:同构的,可找出各自图中两组各 3 个结点的对应关系。

5.3 解:

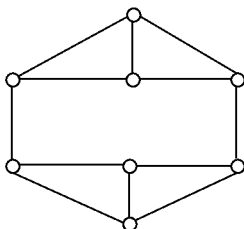
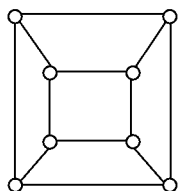
① ○ ② ○ ○ ③ ○—○ ④ ○



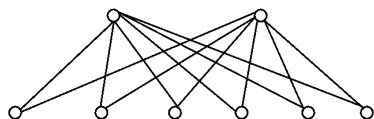


以上①~⑮为 18 个互不同构的子图;其中⑧~⑮是其 11 个生成子图。

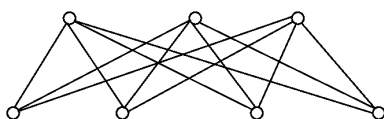
5.4 解:



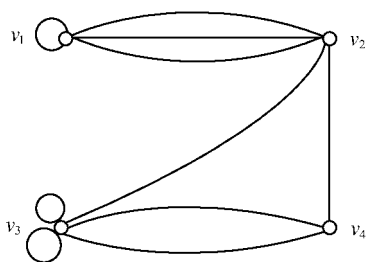
5.5 解: $K_{2,6}$ 图为:



$K_{3,4}$ 图为:



5.6 解: 重图 G 为:



5.7 解:(1) 基本通路为: (a,b,g,c,h) 、 (a,b,g,c,d,h) 、 (a,b,f,g,c,h) 、 (a,b,f,g,c,d,h) 、 (a,e,b,g,c,h) 、 (a,e,b,g,c,d,h) 、 (a,e,b,f,g,c,h) 、 (a,e,b,f,g,c,d,h) 。

(2) 简单通路同(1)。

(3) a 到 h 的距离为 4, 即 (a,b,g,c,h) 。

5.8 解:图(a)有欧拉通路、哈密顿通路;

图(b)有欧拉通路、哈密顿通路、哈密顿回路;

图(c)有欧拉回路、哈密顿通路、哈密顿回路;

图(d)有哈密顿通路、哈密顿回路;

图(e)有哈密顿通路、哈密顿回路。

5.9 证明:“ $\Rightarrow$ ”设从 u 到 v 存在一条通路,若其中有相同结点 w ,例如 $u, \cdots w, \cdots w, v$,则删去 w 到 w 的那些边,它仍是 u 到 v 的通路,如此反复进行,直到没有重复结点为止,此时所得通路就是 u 到 v 的基本通路。

“ $\Leftarrow$ ”设 u 到 v 存在一条基本通路,根据基本通路的定义,知 u 到 v 是连通的,故 u 到 v 之间必有通路存在。

5.10 解:

$$(1) A_1^1 = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$A_1^2 = \begin{bmatrix} 3 & 1 & 1 & 2 & 1 & 1 \\ 1 & 2 & 0 & 1 & 1 & 1 \\ 1 & 0 & 2 & 1 & 2 & 0 \\ 2 & 1 & 1 & 3 & 1 & 1 \\ 1 & 1 & 2 & 1 & 4 & 1 \\ 1 & 1 & 0 & 1 & 1 & 2 \end{bmatrix}$$

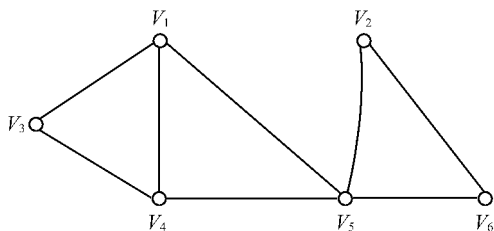
$$A_1^3 = \begin{bmatrix} 4 & 2 & 5 & 5 & 7 & 2 \\ 2 & 2 & 2 & 2 & 5 & 3 \\ 5 & 2 & 2 & 5 & 2 & 2 \\ 5 & 2 & 5 & 4 & 7 & 2 \\ 7 & 5 & 2 & 7 & 4 & 5 \\ 2 & 3 & 2 & 2 & 5 & 2 \end{bmatrix}$$

$$A_1^4 = \begin{bmatrix} 17 & 9 & 9 & 16 & 13 & 9 \\ 9 & 8 & 4 & 9 & 9 & 7 \\ 9 & 4 & 10 & 9 & 14 & 4 \\ 16 & 9 & 9 & 17 & 13 & 9 \\ 13 & 9 & 14 & 13 & 24 & 9 \\ 9 & 7 & 4 & 9 & 9 & 7 \end{bmatrix}$$

$$A_1^5 = \begin{bmatrix} 38 & 22 & 33 & 39 & 51 & 22 \\ 22 & 16 & 18 & 22 & 33 & 17 \\ 33 & 18 & 18 & 33 & 26 & 18 \\ 39 & 22 & 33 & 38 & 51 & 22 \\ 51 & 33 & 26 & 51 & 44 & 33 \\ 22 & 16 & 18 & 22 & 32 & 16 \end{bmatrix}$$

$$A_1^6 = \begin{bmatrix} 123 & 73 & 77 & 122 & 121 & 73 \\ 73 & 50 & 44 & 73 & 77 & 49 \\ 77 & 44 & 66 & 77 & 102 & 44 \\ 122 & 73 & 77 & 123 & 121 & 73 \\ 121 & 77 & 102 & 121 & 168 & 77 \\ 72 & 48 & 44 & 72 & 76 & 48 \end{bmatrix}$$

(2) 作出图 G_1 如下:



各结点间的距离为:

$$d(V_1, V_2) = 2,$$

$$d(V_1, V_3) = 1,$$

$$d(V_1, V_4) = 1,$$

$$d(V_1, V_5) = 1,$$

$$d(V_1, V_6) = 2,$$

$$d(V_2, V_3) = 3, \quad d(V_2, V_4) = 2, \quad d(V_2, V_5) = 1,$$

$$d(V_2, V_6) = 1, \quad d(V_3, V_4) = 1, \quad d(V_3, V_5) = 2,$$

$$d(V_3, V_6) = 3, \quad d(V_4, V_5) = 1, \quad d(V_4, V_6) = 2,$$

$$d(V_5, V_6) = 1.$$

(3) 根据(2)中 G_1 图得到如下基本回路:

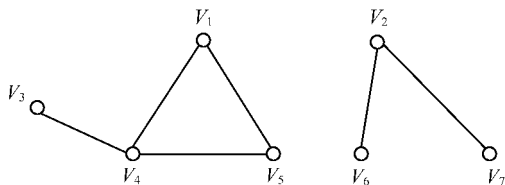
$$(V_1 V_3 V_4 V_1), (V_1 V_4 V_5 V_1), (V_1 V_3 V_4 V_5 V_1), (V_2 V_5 V_6 V_2),$$

$$(V_3 V_1 V_4 V_3), (V_3 V_1 V_5 V_4 V_3), (V_4 V_1 V_3 V_4), (V_4 V_5 V_1 V_4),$$

$$(V_4 V_3 V_1 V_5 V_4), (V_5 V_2 V_6 V_5), (V_5 V_1 V_4 V_5), (V_5 V_1 V_3 V_4 V_5),$$

$$(V_6 V_2 V_5 V_6).$$

作出 G_2 图如下:



根据图找出如下基本回路：
 $(V_1V_4V_5V_1)$ 、 $(V_4V_1V_5V_4)$ 、 $(V_5V_1V_4V_5)$ 。

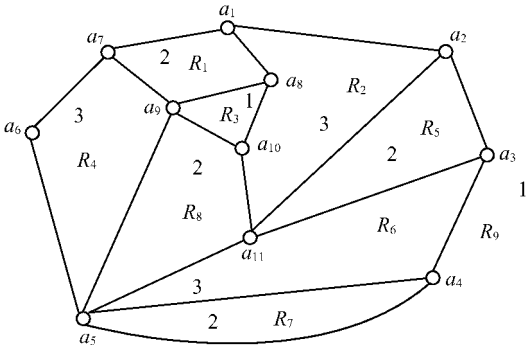
5.11 解:根据二分图的性质,它有两个互补结点子集 V_1 和 V_2 ,假定各自集合中的结点为:

$$V_1=\{V_{11},V_{12},\cdots,V_{1i}\},V_2=\{V_{21},V_{22},\cdots,V_{2j}\}$$

可按次序 $V_{11},V_{12},\cdots,V_{1i},V_{21},V_{22},\cdots,V_{2j}$ 来排列,即 V_{11} 排第 1, V_{12} 排第 2、……、 V_{1i} 排第 i 、 V_{21} 排第 $i+1$ 、… V_{2j} 排第 $i+j$ 位,(也就是将某结点子集排序在前,另一互补结点子集跟在后面排)。

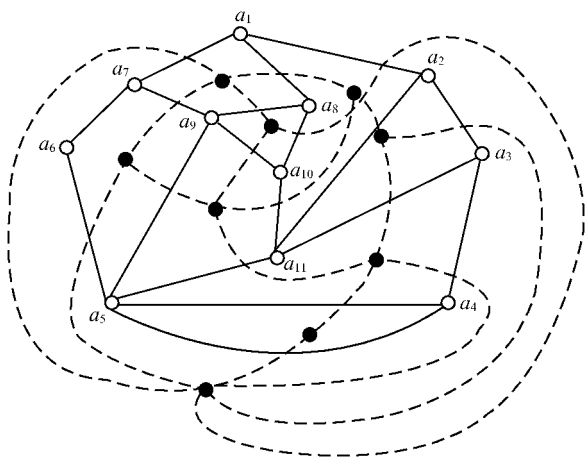
如此可得相邻矩阵 $A=\begin{bmatrix} 0 & B \\ C & 0 \end{bmatrix}$ 的形式。

5.12 解:用数字表示不同的颜色标在图中各区域内:



5.13 解:构造相应的对偶图 G^* 见下图的实心点和虚线所示部分:

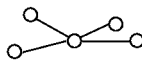
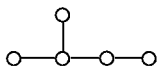
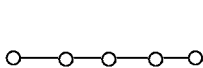
5.14 (1) 解:设有 x 个次数为 1 的结点,则该树的结点总数为: $n=2+1+3+x=6+x$,边数 $m=n-1=5+x$,因为 $\sum \deg(V_i)=2m$,故 $2\times(5+x)=2\times2+1\times3+3\times4+x\times1$,得 $x=9$,所以共有 9



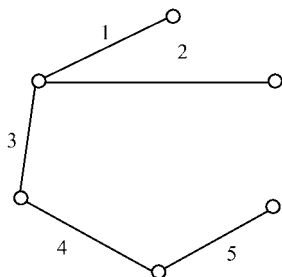
个次数为 1 的结点。

(2) 解: 设有 n_1 个次数为 1 的结点, 则树的结点总数为: $n = n_1 + n_2 + n_3 + \cdots + n_k$, 边数 $m = n - 1$, 由 $\sum \deg(V_i) = 2m$ 得: $n_1 + 2n_2 + 3n_3 + \cdots + kn_k = 2(n_1 + n_2 + n_3 + \cdots + n_k) - 2$, 故解出 $n_1 = n_3 + 2n_4 + \cdots + (k - 2)n_k + 2$ 。

5.15 解:



5.16 解:



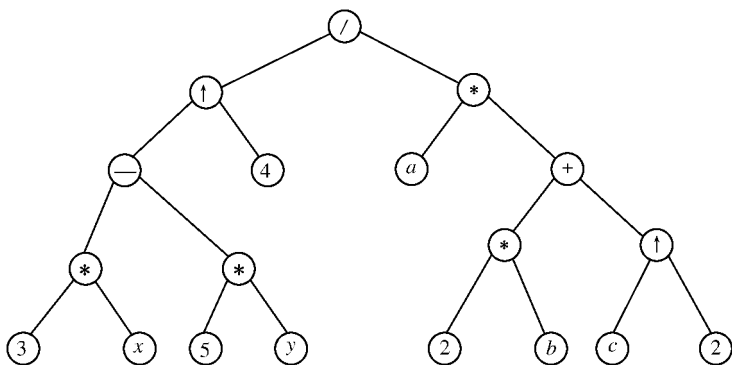
5.17 证明:先证(1)、(2)等价,即 G 是 2-色图 $\Leftrightarrow G$ 是二分图,
 “ $\Rightarrow$ ”设 G 可用两种颜色 x 和 y 正常着色,标上 x 和 y 颜色的结点集
 分别为 V_1 和 V_2 ,显然 V_1 中的结点互不相邻接, V_2 中的结点也互相
 不相邻接,即 G 中每一边 e 的一个端点在 V_1 中,另一个端点在 V_2 中,
 所以 G 是二分图。

“ $\Leftarrow$ ”设 G 是二分图,其互补结点子集为 V_1, V_2 ,给 V_1 和 V_2 中
 的结点分别着上 x 和 y 两种不同的颜色,这显然是正常着色的
 2-色图。

故(1) $\Leftrightarrow$ (2);另证(2) $\Leftrightarrow$ (3)见定理 5.8 的证明;上述又可推得
 (1) $\Leftrightarrow$ (3)。

所以(1)、(2)、(3)三个命题是等价的。

5.18 解:(1) 相应根树如下:



(2) 先根次序代数表达式:

$$/\uparrow - * 3x * 5y 4 * a + * 2b \uparrow c 2$$

中根次序代数表达式:

$$3 * x - 5 * y \uparrow 4 / a * 2 * b + c \uparrow 2$$

后根次序代数表达式:

$$3x * 5y * - 4 \uparrow a 2b * c 2 \uparrow + * /$$

5.19 解:(1)

	a	b	c	d	e
引入次数	1	2	4	3	1
引出次数	2	2	1	2	2

(2) 有三条: $(a b d)$ 、 $(a b c e d)$ 、 $(a c e d)$ 。

(3) 相邻矩阵如下:

$$M_D = \begin{matrix} & \begin{matrix} a & b & c & d & e \end{matrix} \\ \begin{matrix} a \\ b \\ c \\ d \\ e \end{matrix} & \begin{bmatrix} 0 & 1 & \boxed{1} & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix} \end{matrix}$$

(4) 作出相应的矩阵来判定通路数目:

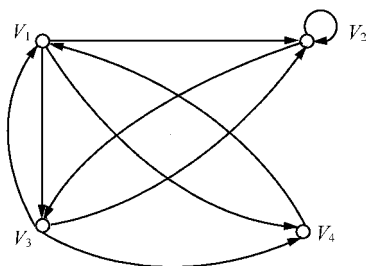
$$M_D^2 = \begin{bmatrix} 1 & 0 & \boxed{1} & 1 & 1 \\ 0 & 1 & 2 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \quad M_D^3 = \begin{bmatrix} 0 & 1 & \boxed{3} & 2 & 1 \\ 1 & 0 & 3 & 3 & 2 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 2 & 1 \\ 0 & 0 & 2 & 2 & 1 \end{bmatrix}$$

可根据上述矩阵中虚线所框的数字来判定,即

从 a 到 c 长度为 1 的通路有 1 条、长度为 2 的通路为 1 条、长度为 3 的通路有 3 条,故有:小于或等于 3 的通路数有: $1+1+3=5$ (条)。

(5) D 是单向连通的。

5.20 解:(1)其有向图如下:



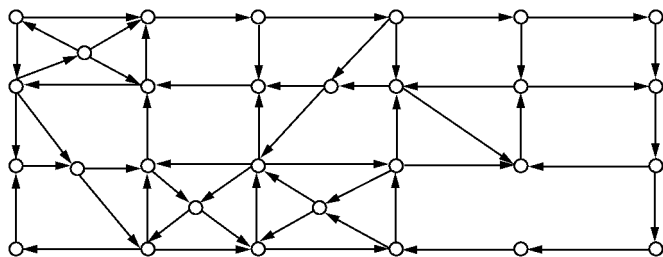
(2) 先求出相应矩阵:

$$M^2 = \begin{bmatrix} 2 & 2 & 1 & 1 \\ 1 & 2 & 1 & 1 \\ 1 & 2 & 2 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \quad M^3 = \begin{bmatrix} 2 & 5 & 4 & 3 \\ 2 & 4 & 3 & 2 \\ 3 & 5 & 3 & 3 \\ 2 & 2 & 1 & 1 \end{bmatrix}$$

V_1 到 V_1 长度是 3 的回路有 2 条, V_1 到 V_2 长度是 3 的通路有 5 条, V_1 到 V_3 长度是 3 的通路有 4 条, V_1 到 V_4 长度是 3 的通路有 3 条。

(3) 图 D 是强连通的。

5.21 解:可根据书上 P. 182 无向图变为有向图的算法来标方向。



5.22 答:A。

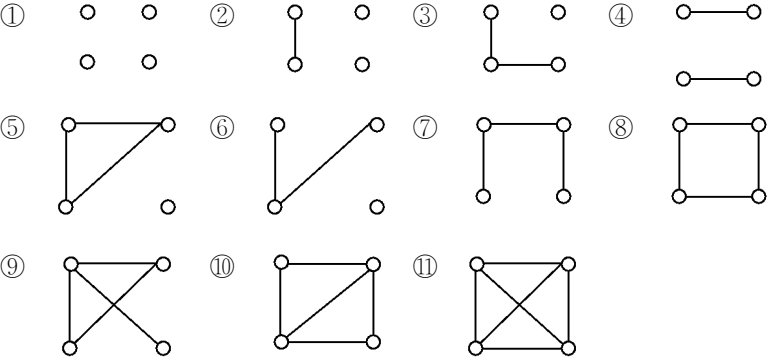
5.23 答:B。

5.24 答:A。

5.25 证明: $\because \sum_{i=1}^n \deg(V_i)=2m$

$$\begin{aligned} n_k \cdot k+(n-n_k) \cdot(k+1) &=n_k \cdot k+n \cdot k-n_k \cdot k+n-n_k \\ &=n \cdot(k+1)-n_k=2 m \\ \therefore n_k &=(k+1) \cdot n-2 m 。 \end{aligned}$$

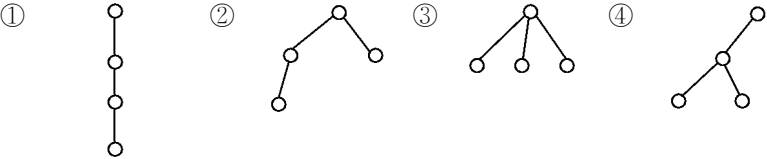
5.26 解:



5.27 答:C。

5.28 答:C。

5.29 解:



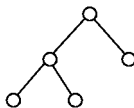
5.30 答: $n-1$; $m-k$ 。

5.31 证明: 找出两图中结点的对应关系:

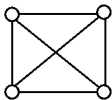
$h(a)=8,$ $h(b)=3,$ $h(c)=9,$ $h(d)=4,$
 $h(e)=10$ $h(f)=6,$ $h(g)=1,$ $h(h)=2,$
 $h(i)=7,$ $h(j)=5。$

相应的边也将一一对应, 所以图 G 和 G_1 同构。

5.32 解: (1) 可解的, 如图示



(2) 可解的, 如图示



(3) 不可解的, 因为奇数度结点数不可能为奇数个。

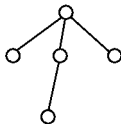
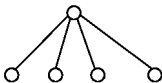
5.33 答: A。

5.34 答: A。

5.35 答: B。

5.36 答: $n-1$; 权是最小的树。

5.37 答:

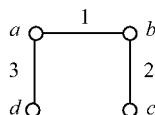
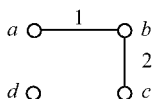
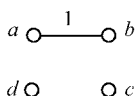


5.38 证明: $\because$ 图 G 有 9 个结点, 根据定理任何图中奇结点个数为偶数(个), 因此 5 度结点的个数只能是 0, 2, 4, 6, 8, 此时分别对应 6 度个数的结点的个数为 9, 7, 5, 3, 1。

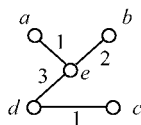
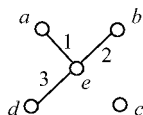
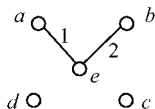
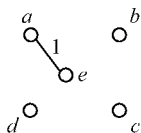
$\therefore$ 对上述五种情况都满足至少有 5 个 6 度或 6 个 5 度结点。

5.39 解:

(1)



(2)



5.40 答:C。

5.41 答:D。

5.42 答:A。

5.43 答:平凡图;平行边。

5.44 答:C。

5.45 答:D。

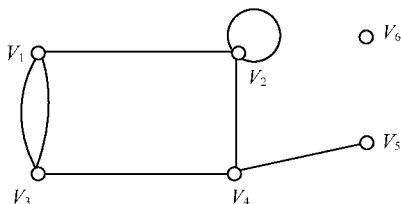
5.46 答:1。

5.47 证明:设3次正则图共有 n 个结点 $V_1, V_2, \dots, V_n$ 。

则 $\sum_{i=1}^n \deg(V_i) = 2m = 3n$, 此时 $3n$ 必为偶数,

若 n 为奇数时, $3n$ 也应为奇数, 此处不可能成立, 故 n 必为偶数, 因此3次正则图必有偶数个结点。

5.48 解:(1)



(2) 因为有平行边, 故不是简单图。

(3) $d(V_1) = 3, \quad d(V_2) = 4, \quad d(V_3) = 3, \quad d(V_4) = 3,$
 $d(V_5) = 1, \quad d(V_6) = 0。$

习题六解答

6.1 解:(1) 他讲法语或英语。

(2) 他讲法语并且讲英语。

(3) 他会讲法语而不讲英语。

(4) 他不讲法语或不讲英语。

(5) 他不是不讲法语。

(6) 他不是不讲法语讲英语。

(7) 他讲法语等同于他讲英语。

(8) 他如果不讲法语就讲英语。

(9) 他只讲法语或英语其中之一。

6.2 解(1) 设 P : 她身材高, Q : 她很温雅。

$P \wedge Q$ 。

(2) 设 P 、 Q 同(1)。

$\neg (P \wedge Q)$ 。

(3) 设 P 、 Q 同(1)。

$\neg P \wedge \neg Q$ 。

(4) 设 P : 李明读新民晚报, Q : 李明读新华日报, R : 李明读人民日报。

$(P \vee Q) \wedge \neg R$ 。

(5) 设 P : 高俊在屋里, Q : 高俊在做功课, R : 高俊在看电视。

$P \rightarrow (Q \oplus R)$ 。

(6) 设 P 、 Q 、 R 同(6)

$(\neg P \vee Q) \rightarrow \neg R$ 。

(7) 设 P : 两个三角形全等, Q : 两个三角形的三条边对应相等。

$P \leftrightarrow Q$ 。

6.3 (1) 解:

p	q	$(p \wedge (\neg q \rightarrow p)) \wedge \neg ((p \leftrightarrow \neg q) \rightarrow (q \vee \neg p))$
0	0	0
0	1	0
1	0	1
1	1	0

(2) 解:

p	q	r	$(q \leftrightarrow (r \rightarrow \neg p)) \vee ((\neg q \rightarrow p) \leftrightarrow r)$
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	1

续表

p	q	r	$(q \leftrightarrow (r \rightarrow \neg p)) \vee ((\neg q \rightarrow p) \leftrightarrow r)$
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

(3) 解:

p	q	r	$(p \rightarrow (q \rightarrow r)) \rightarrow ((p \rightarrow q) \rightarrow (p \rightarrow r))$
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	1

(4) 解:

p	q	$(\neg q \rightarrow \neg p) \rightarrow (p \rightarrow q)$
0	0	1
0	1	1
1	0	1
1	1	1

6.4 (1) 证明:用真值表法

p	q	$p \vee (p \wedge q)$	p
0	0	0	0

续表

p	q	$p \vee (p \wedge q)$	p
0	1	0	0
1	0	1	1
1	1	1	1

表中反映等式两边 0、1 的结果值相同。

(2) 证明:用真值表法

p	q	$\neg (p \vee q) \vee (\neg p \wedge q)$	$\neg p$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	0	0

6.5 (1) 证明: $(p \vee q) \vee \neg p = (p \vee \neg p) \wedge (q \vee \neg p)$
 $= 1 \wedge (q \vee \neg p) = \neg p \vee q。$

(2) 证明: $(p \wedge q) \rightarrow r = \neg (p \wedge q) \vee r = (\neg p \vee \neg q) \vee r$
 $= \neg p \vee r \vee \neg q \vee r = (p \rightarrow r) \vee (q \rightarrow r)。$

(3) 证明: $p \rightarrow (q \rightarrow r) = \neg p \vee (\neg q \vee r) = \neg p \vee r \vee \neg q$
 $= \neg (p \wedge \neg r) \vee \neg q = (p \wedge \neg r) \rightarrow \neg q。$

6.6 解:列出 $I_1 \sim I_{15}$ 的真值表:

I_1 :

P	Q	$(P \wedge Q) \rightarrow P$
0	0	1
0	1	1
1	0	1
1	1	1

表中结果永为真

$I_2 :$

P	Q	$(P \wedge Q) \rightarrow Q$
0	0	1
0	1	1
1	0	1
1	1	1

$I_3 :$

P	Q	$P \rightarrow (P \vee Q)$
0	0	1
0	1	1
1	0	1
1	1	1

$I_4 :$

P	Q	$Q \rightarrow (P \vee Q)$
0	0	1
0	1	1
1	0	1
1	1	1

$I_5 :$

P	Q	$\neg P$	$P \rightarrow Q$	$\neg P \rightarrow (P \rightarrow Q)$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	1
1	1	0	1	1

$I_6 :$

P	Q	$P \rightarrow Q$	$Q \rightarrow (P \rightarrow Q)$
0	0	1	1
0	1	1	1
1	0	0	1
1	1	1	1

$I_7 :$

P	Q	$P \rightarrow Q$	$\neg (P \rightarrow Q)$	$\neg (P \rightarrow Q) \rightarrow P$
0	0	1	0	1
0	1	1	0	1
1	0	0	1	1
1	1	1	0	1

$I_8 :$

P	Q	$P \rightarrow Q$	$\neg (P \rightarrow Q)$	$\neg Q$	$\neg (P \rightarrow Q) \rightarrow \neg Q$
0	0	1	0	1	1
0	1	1	0	0	1
1	0	0	1	1	1
1	1	1	0	0	1

$I_9 :$

P	Q	$\neg P$	$P \vee Q$	$\neg P \wedge (P \vee Q)$	$\neg P \wedge (P \vee Q) \rightarrow Q$
0	0	1	0	0	1
0	1	1	1	1	1
1	0	0	1	0	1
1	1	0	1	0	1

$I_{10} :$

P	Q	$\neg Q$	$P \vee Q$	$\neg Q \wedge (P \vee Q)$	$\neg Q \wedge (P \vee Q) \rightarrow P$
0	0	1	0	0	1
0	1	0	1	0	1
1	0	1	1	1	1
1	1	0	1	0	1

$I_{11} :$

P	Q	$P \rightarrow Q$	$P \wedge (P \rightarrow Q)$	$P \wedge (P \rightarrow Q) \rightarrow Q$
0	0	1	0	1
0	1	1	0	1
1	0	0	0	1
1	1	1	1	1

$I_{12} :$

P	Q	$\neg Q$	$P \rightarrow Q$	$\neg P$	$\neg Q \wedge (P \rightarrow Q)$	$\neg Q \wedge (P \rightarrow Q) \rightarrow \neg P$
0	0	1	1	1	1	1
0	1	0	1	1	0	1
1	0	1	0	0	0	1
1	1	0	1	0	0	1

$I_{13} :$

P	Q	R	$P \rightarrow Q$	$Q \rightarrow R$	$P \rightarrow R$	$(P \rightarrow Q) \wedge (Q \rightarrow R)$	$(P \rightarrow Q) \wedge (Q \rightarrow R) \rightarrow (P \rightarrow R)$
0	0	0	1	1	1	1	1
0	0	1	1	1	1	1	1
0	1	0	1	0	1	0	1
0	1	1	1	1	1	1	1
1	0	0	0	1	0	0	1

续表

PQR	$P \rightarrow Q$	$Q \rightarrow R$	$P \rightarrow R$	$(P \rightarrow Q) \wedge (Q \rightarrow R)$	$(P \rightarrow Q) \wedge (Q \rightarrow R) \rightarrow (P \rightarrow R)$
1 0 1	0	1	1	0	1
1 1 0	1	0	0	0	1
1 1 1	1	1	1	1	1

I_{14} :

$PQRS$	$P \rightarrow Q$	$R \rightarrow S$	$P \wedge R$	$Q \wedge S$	$(P \rightarrow Q) \wedge (R \rightarrow S)$	$(P \wedge R) \rightarrow (Q \wedge S)$	$(P \rightarrow Q) \wedge (R \rightarrow S) \rightarrow (P \wedge R) \rightarrow (Q \wedge S)$
0 0 0 0	1	1	0	0	1	1	1
0 0 0 1	1	1	0	0	1	1	1
0 0 1 0	1	0	0	0	0	1	1
0 0 1 1	1	1	0	0	1	1	1
0 1 0 0	1	1	0	0	1	1	1
0 1 0 1	1	1	0	1	1	1	1
0 1 1 0	1	0	0	0	0	1	1
0 1 1 1	1	1	0	1	1	1	1
1 0 0 0	0	1	0	0	0	1	1
1 0 0 1	0	1	0	0	0	1	1
1 0 1 0	0	0	1	0	0	0	1
1 0 1 1	0	1	1	0	0	0	1
1 1 0 0	1	1	0	0	1	1	1
1 1 0 1	1	1	0	1	1	1	1
1 1 1 0	1	0	1	0	0	0	1
1 1 1 1	1	1	1	1	1	1	1

I_{15} :

PQR	$P \vee Q$	$P \rightarrow R$	$Q \rightarrow R$	$(P \vee Q) \wedge (P \rightarrow R)$	$(P \vee Q) \wedge (P \rightarrow R) \wedge (Q \rightarrow R)$	$(P \vee Q) \wedge (P \rightarrow R) \wedge (Q \rightarrow R) \rightarrow R$
000	0	1	1	0	0	1
001	0	1	1	0	0	1
010	1	1	0	1	0	1
011	1	1	1	1	1	1
100	1	0	1	0	0	1
101	1	1	1	1	1	1
110	1	0	0	0	0	1
111	1	1	1	1	1	1

6.7 (1) 解: 设 P : 6 是偶数, Q : 2 能整除 7, R : 5 是素数。

则有: $P \rightarrow \neg Q, \neg R \vee Q, R$ 作为条件来推理。

① $\neg R \vee Q, R \vdash Q$, ② $P \rightarrow \neg Q, Q \vdash \neg P$ ($\neg P$ 为结论)

$\neg P$ 表示 6 不是偶数, 是奇数, 此论证不对, 因为所给条件中 $\neg R \vee Q$ 是错误的。

(2) 解: 设 P : 这天我夫人生日, Q : 我送我夫人一束花, R : 我工作迟了。

则有 $P \rightarrow Q, P \vee R, \neg Q$ 作为条件来推理:

① $\neg Q, P \rightarrow Q \vdash \neg P$, ② $P \vee R, \neg P \vdash R$ (R 为结论)

本题结论正确。

(3) 解: 设 P : 我工作, Q : 我学习, R : 我考了数学。

则有: $P \rightarrow \neg Q, P \vee R, R$ 作为条件来推理:

① $\because P \rightarrow \neg Q = Q \rightarrow \neg P, P \vee R = \neg P \rightarrow R$,

$\therefore Q \rightarrow \neg P, \neg P \rightarrow R \vdash Q \rightarrow R$

② 由 $Q \rightarrow R$ 和 R 为真无法推出 Q 为真或假, 故本题结论推理错误。

(4) 解: 设 P : 我工作, Q : 我学习, R : 我考数学。

则有: $P \rightarrow \neg Q, P \vee R, P$ 作为条件来推理:

(1) $P, P \rightarrow \neg Q \vdash \neg Q$,

(2) $\neg Q, P \vee R$, 无法推出本题结论。

(5) 解: 设 P : 我学习, Q : 我考试失败, R : 我踢足球。

则有: $P \rightarrow \neg Q, \neg R \rightarrow P, Q$ 作为条件来推理:

① $Q, P \rightarrow \neg Q \vdash \neg P$,

② $\neg R \rightarrow P = R \vee P$,

$\neg P, R \vee P \vdash R$ (R 为结论),

本题推理过程正确。

6.8 解: 设 P : 国家增加税收, Q : 通货膨胀率下降, R : 美元贬值。

用符号公式表示此政治家的三次讲话及所得结论如下:

(1) $(P \rightarrow Q) \wedge \neg R$ 即: $P \rightarrow Q, \neg R$;

(2) $(Q \vee \neg R) \rightarrow \neg P$ 即: $(R \rightarrow Q) \rightarrow \neg P$;

(3) $(P \vee (R \wedge Q)) = (P \vee R) \wedge (P \vee Q)$ 即: $\neg P \rightarrow R, \neg P \rightarrow Q$ 。

结论: $P \wedge Q \wedge \neg R$ 。

用(1)~(3)作为条件来推理如下:

$(R \rightarrow Q) \rightarrow \neg P, \neg P \rightarrow Q \vdash (R \rightarrow Q) \rightarrow Q = (\neg Q \wedge R) \vee Q = R \vee Q, R \vee Q, \neg R \vdash Q$ ①

$\neg R, \neg P \rightarrow R \vdash P$ ②, 另有条件中 $\neg R$ ③。

由①、②、③知此政治家的条件和结论的论证推理正确。

6.9 (1) 解: 析取范式、特异析取范式:

$(\neg p \vee \neg q) \rightarrow (p \leftrightarrow \neg q) = \neg(\neg p \vee \neg q) \vee ((\neg p \vee \neg q) \wedge (p \vee q))$

$= (p \wedge q) \vee (\neg p \wedge q) \vee (p \wedge \neg q)$

合取范式、特异合取范式:

$(\neg p \vee \neg q) \rightarrow (p \leftrightarrow \neg q) = p \vee q$ 。

(2) 解:析取范式: $(p \wedge q) \vee (q \wedge \neg q)$,

特异析取范式: $p \wedge q$ 。

合取范式: $q \wedge (p \vee \neg q)$

特异合取范式: $(q \vee (p \wedge \neg p)) \wedge (p \vee \neg q) = (p \vee q) \wedge (\neg p \vee q) \wedge (p \vee \neg q)$ 。

(3) 解:原式 $= p \vee (p \vee (q \vee (q \vee r))) = p \vee q \vee r$ 。

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

析取范式为 $p \vee q \vee r$ 。

特异析取范式为:

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

合取范式及特异合取范式为: $p \vee q \vee r$ 。

(4) 解:原式 $= p \rightarrow (q \wedge r) \wedge (p \vee (\neg q \wedge \neg r))$

$= p \rightarrow ((q \wedge r) \wedge (p \vee \neg q) \wedge (p \vee \neg r))$

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

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

$= (\neg p \vee q) \wedge (\neg p \vee r)$ 。

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

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

$= (\neg p \vee q \vee r) \wedge (\neg p \vee q \vee \neg r) \wedge (\neg p \vee \neg q \vee r)$ 。

$(\neg p \vee q) \wedge (\neg p \vee r) = (\neg p \wedge \neg p) \vee (\neg p \wedge q) \vee (\neg p \wedge r)$
 $\vee (q \wedge r)$ 。

真值表：

p	q	r	原式
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

析取范式：

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

特异析取范式：(从真值表得出)

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

合取范式： $(\neg p \vee q) \wedge (\neg p \vee r)$

$$\text{特异合取范式：} (\neg p \vee q \vee r) \wedge (\neg p \\ \vee q \vee \neg r) \wedge (\neg p \vee \neg q \vee r)$$

$$(5) \text{ 解：原式} = \neg p \vee (p \wedge (\neg q \vee p)) = \neg p \vee ((p \wedge \neg q) \vee (p \wedge p)) \\ = \neg p \vee (p \wedge \neg q) \vee p = 1 (\text{重言式})$$

真值表：

p	q	原式
0	0	1
0	1	1
1	0	1
1	1	1

析取范式： $\neg p \vee (p \wedge \neg q) \vee p$ 。

特异析取范式：

$$(\neg p \wedge \neg q) \vee (\neg p \wedge q) \vee (p \wedge \neg q) \\ \vee (p \wedge q)。$$

合取范式： $\neg p \vee (p \wedge \neg q) \vee p = (\neg p$

$$\vee p \vee p) \wedge (\neg p \vee p \vee \neg q) \\ = (\neg p \vee p) \wedge (\neg p \vee p \vee \neg q)。$$

6.10 (1) 解：本公式是所有最小项均出现的特异析取范式，故它是重言式。

$$(2) \text{ 解：原式} = (p \wedge \neg p) \vee q \vee (p \wedge \neg p) \vee \neg q = q \vee \neg q = 1。$$

$$(3) \text{ 解：原式} = (\neg p \wedge \neg q) \vee ((\neg p \vee p) \wedge (p \vee q)) \\ = (\neg p \wedge \neg q) \vee p \vee q = ((\neg p \vee p) \wedge (\neg q \vee p)) \vee q \\ = \neg q \vee p \vee q = 1 \vee p = 1。$$

$$(4) \text{ 解：原式} = ((\neg p \vee q) \wedge p) \rightarrow q = \neg ((\neg p \vee q) \wedge p) \vee q \\ = \neg ((\neg p \wedge p) \vee (p \wedge q)) \vee q = \neg (p \wedge q) \vee q$$

$$= \neg p \vee \neg q \vee q = \neg p \vee 1 = 1。$$

$$\begin{aligned} (5) \text{ 解:原式} &= ((\neg p \vee q) \rightarrow (q \vee \neg p)) \rightarrow ((q \vee \neg p) \rightarrow (\neg p \vee q)) \\ &= (\neg(\neg p \vee q) \vee (q \vee \neg p)) \rightarrow (\neg(q \vee \neg p) \vee (\neg p \vee q)) \\ &= \neg((p \wedge \neg q) \vee (q \vee \neg p)) \vee ((\neg q \wedge p) \vee (\neg p \vee q)) \\ &= (\neg(p \wedge \neg q) \wedge \neg(q \vee \neg p)) \vee ((\neg q \vee \neg p) \wedge (p \vee \neg p) \vee q) \\ &= ((\neg p \vee q) \wedge (\neg q \wedge p)) \vee (\neg q \vee \neg p \vee q) \\ &= ((\neg p \vee q) \wedge (\neg q \wedge p)) \vee (\neg p \vee 1) \\ &= 1。 \end{aligned}$$

$$\begin{aligned} (6) \text{ 解:原式} &= (p \leftrightarrow q) \leftrightarrow ((p \wedge q) \vee \neg p) \wedge ((p \wedge q) \vee \neg q) \\ &= (p \leftrightarrow q) \leftrightarrow ((p \vee \neg p) \wedge (q \vee \neg p)) \wedge ((p \vee \neg q) \wedge (q \vee \neg q)) \\ &= (p \leftrightarrow q) \leftrightarrow ((p \rightarrow q) \wedge (q \rightarrow p)) \\ &= (p \leftrightarrow q) \leftrightarrow (p \leftrightarrow q) = 1。 \end{aligned}$$

(7) 解:非重言式,可用真值表法或公式法验证。

6.11 答:B。

6.12 答:等价的; P

$$\begin{aligned} 6.13 \text{ 证明:原式} &= P \wedge (\neg P \vee Q) \rightarrow Q = (P \wedge \neg P) \vee (P \wedge Q) \rightarrow Q \\ &= (P \wedge Q) \rightarrow Q = \neg(P \wedge Q) \vee Q = \neg P \vee \neg Q \vee Q = \neg P \vee 1 = 1 \\ &\text{故为重言式。} \end{aligned}$$

$$\begin{aligned} 6.14 \text{ 解:原式} &= \neg(\neg P \vee Q) \wedge Q \wedge R = (P \wedge \neg Q) \wedge Q \wedge R \\ &= P \wedge \neg Q \wedge Q \wedge R = 0。 \end{aligned}$$

既是析取范式又是合取范式(是一个矛盾式)。

6.15 答:B。

$$6.16 \text{ 证明:原式左边} = \neg(P \vee \neg Q) = \neg P \wedge Q = Q \wedge \neg P。$$

故左边 = 右边。

$$\begin{aligned} 6.17 \quad \text{解: 原式} &= (\neg(\neg p \vee q) \vee p) \leftrightarrow p \\ &= ((\neg(\neg p \vee q) \vee p) \wedge (p \rightarrow (\neg(\neg p \vee q) \vee p))) \\ &= (((\neg p \vee q) \wedge \neg p) \vee p) \wedge (\neg p \vee (\neg(\neg p \vee q) \vee p)) \\ &= ((\neg p \wedge \neg p) \vee (q \wedge \neg p) \vee p) \wedge (\neg p \vee (p \wedge \neg q) \vee p) \\ &= (\neg p \vee (q \wedge \neg p) \vee p) \wedge (\neg p \vee (p \wedge \neg q) \vee p) \\ &= (\neg p \vee p \vee (q \wedge \neg p)) \wedge (\neg p \vee p \vee (p \wedge \neg q)) \\ &= 1 \wedge 1 = 1 \end{aligned}$$

故本公式为重言式。

6.18 答: C。

6.19 解: ① 利用联结词化归公式 $P \rightarrow Q = \neg P \vee Q$ 。

② 等幂律 $P \vee P = P$ 。

③ 交换律 $P \vee Q = Q \vee P$ 。

④ 化归公式 $\neg P \vee Q = P \rightarrow Q$ 。

$$\begin{aligned} 6.20 \quad \text{证明: } P \wedge \neg Q \vee Q &= (P \wedge \neg Q) \vee Q = (P \vee Q) \wedge (\neg Q \vee \\ Q) &= (P \vee Q) \wedge 1 = P \vee Q. \end{aligned}$$

故左边 = 右边。

$$\begin{aligned} 6.21 \quad \text{解: 原式} &= (p \vee q) \rightarrow (\neg q \vee p) = \neg(p \vee q) \vee (\neg q \vee p) \\ &= (\neg p \wedge \neg q) \vee (\neg q \vee p) = (\neg p \vee \neg q \vee p) \wedge (\neg q \vee \neg q \vee p) \\ &= 1 \wedge (\neg q \vee p) = p \vee \neg q \end{aligned}$$

是偶然式。

6.22 答: C。

6.23 答: 重言式; 合取。

$$\begin{aligned}
6.24 \quad & \text{证明: 左边} = \neg(P \rightarrow Q) \vee (Q \vee R) \\
& = \neg(\neg P \vee Q) \vee (Q \vee R) \\
& = (P \wedge \neg Q) \vee (Q \vee R) = (P \vee (Q \vee R)) \wedge ((Q \vee R) \vee \neg Q) \\
& = (P \vee Q \vee R) \wedge (Q \vee \neg Q \vee R) = (P \vee Q \vee R) \wedge (1 \vee R) \\
& = P \vee Q \vee R = \text{右边}。
\end{aligned}$$

$$\begin{aligned}
6.25 \quad & \text{解: } p \wedge (p \rightarrow q) = p \wedge (\neg p \vee q) = (p \wedge \neg p) \vee (p \wedge q)。 \\
& \text{析取范式为: } (p \wedge \neg p) \vee (p \wedge q)。 \\
& \text{合取范式为: } p \wedge (\neg p \vee q)。
\end{aligned}$$

6.26 答: C。

6.27 证明: ① A	附加前提, cp 规则。
② $A \rightarrow (B \rightarrow C)$	前提。
③ $B \rightarrow C$	由①、②。
④ B	附加前提。
⑤ $B \rightarrow (C \rightarrow D)$	前提。
⑥ $C \rightarrow D$	由④、⑤。
⑦ $B \rightarrow D$	由③、⑥。
⑧ $A \rightarrow (B \rightarrow D)$	由①、⑦。

$$\begin{aligned}
6.28 \quad & \text{解: 原式} = (\neg(p \vee q) \rightarrow (p \wedge q)) \wedge ((p \wedge q) \rightarrow \neg(p \vee q)) \\
& = ((p \vee q) \vee (p \wedge q)) \wedge (\neg(p \wedge q) \vee \neg(p \vee q)) \\
& = ((p \vee q) \vee p) \wedge ((p \vee q) \vee q) \wedge ((\neg p \vee \neg q) \vee (\neg p \wedge \neg q)) \\
& = (p \vee q) \wedge (p \vee q) \wedge (\neg p \vee \neg q \vee \neg p) \wedge (\neg p \vee \neg q \vee \neg q) \\
& = (p \vee q) \wedge (\neg p \vee \neg q) \\
& \text{为合取范式。}
\end{aligned}$$

$$\begin{aligned}
& (p \vee q) \wedge (\neg p \vee \neg q) = ((p \vee q) \wedge \neg p) \vee ((p \vee q) \wedge \neg q) \\
& = ((p \wedge \neg p) \vee (q \wedge \neg p)) \vee ((p \wedge \neg q) \vee (q \wedge \neg q))
\end{aligned}$$

$$=(q \wedge \neg p) \vee (p \wedge \neg q)$$

$$=(p \wedge \neg q) \vee (\neg p \wedge q)$$

为析取范式。

习题七解答

7.1 (1) 解: 令 $P(x, y): x$ 比 y 长, $Q(x, y): x$ 比 y 高, 长江为 a , 黄河为 b , 金陵饭店为 c , 北京饭店为 d 。

则语句为: $P(a, b) \wedge Q(c, d)$ 。

(2) 解: 令 $P(x): x$ 是数学家, $Q(x): x$ 是伟大的, $R(x): x$ 是文学家, a 表示高斯。

则语句为: $P(a) \wedge Q(a) \wedge (\neg R(a))$ 。

(3) 解: 令 $P(x, y, z): x$ 位于 y 和 z 之间, a 表示南京, b 表示武汉, c 表示上海。

则语句为: $P(a, b, c)$ 。

(4) 解: 令 $P(x, y): x$ 和 y 是兄妹, a 表示他, b 表示她。

则语句为: $P(a, b)$ 。

(5) 解: 令 $P(x): x$ 是人, $Q(x): x$ 犯错误

则语句为: $\neg (P(x) \wedge (\neg Q(x)))$ 。

(6) 解: 令 $R(x): x$ 是实数。

则语句为: $\forall x (R(x) \rightarrow (x^2 > 0 \vee x^2 = 0))$ 。

(7) 解: 令 $P(x): x$ 是有生命之物, $Q(x): x$ 必会死。

则语句为: $\forall x (P(x) \rightarrow Q(x))$ 。

(8) 解: 令 $P(x): x$ 是四边形, $Q(x): x$ 内角之和是 360° 。

则语句为: $\forall x (P(x) \rightarrow Q(x))$ 。

(9) 解: 令 $P(x, y): x$ 比 y 高, $M(x): x$ 是男人, $W(y): y$ 是女人。

则语句为: $\neg (\forall x \forall y (P(x, y) \wedge M(x) \wedge W(y)))$ 。

(10) 解: 令 $P(x, y): x, y$ 互为对顶角, $E(x, y): x$ 等于 y 。

则语句为: $\forall x \forall y (P(x, y) \rightarrow E(x, y)) \wedge \neg \forall x \forall y (E(x, y) \rightarrow P(x, y))$ 。

(11) 解: 令 $P(x):x$ 是素数, $Q(x):x$ 是偶数。

则语句为: $\exists x(P(x) \wedge Q(x) \wedge \forall y(P(y) \wedge Q(y) \rightarrow x=y))$ 。

(12) 解: 令 $P(x):x$ 是资本家, $Q(x):x$ 会剥削人。

则语句为: $\forall x(P(x) \rightarrow Q(x)) \wedge \neg \forall x(Q(x) \rightarrow P(x))$ 。

7.2 (1) 解: 不是; (2) 解: 不是; (3) 解: 是。

7.3 (1) 解: $\exists x$ 中的 x 是约束变元, 其中 $\exists$ 的辖域为 $((P(x) \vee R(x)) \wedge S(x))$; $\forall x$ 中的 x 是约束变元, 其中 $\forall$ 的辖域为 $(P(x) \wedge Q(x))$ 。

(2) 解: $\forall x$ 中的 x 是约束变元, 其中 $\forall$ 的辖域为 $(P(x) \leftrightarrow Q(x))$; $\exists x$ 中的 x 是约束变元, 其中 $\exists$ 的辖域为 $R(x)$; $S(x)$ 中的 x 为自由变元。

(3) 解: $\forall x$ 中的 x 是约束变元, 其中 $\forall$ 的辖域为 $(P(x) \wedge \exists yR(x, y))$, $\exists y$ 中的 y 是约束变元, 其中 $\exists$ 的辖域为 $R(x, y)$ 。

7.4 (1) 解: $(R(0) \vee R(1) \vee R(2) \vee R(3)) \wedge (S(0) \wedge S(1) \wedge S(2) \wedge S(3))$ 。

(2) 解: $(A(0) \wedge A(1) \wedge A(2) \wedge A(3)) \wedge (B(0) \wedge B(1) \wedge B(2) \wedge B(3))$ 。

(3) 解: $\neg (A(0) \vee A(1) \vee A(2) \vee A(3)) \vee (B(0) \wedge B(1) \wedge B(2) \wedge B(3))$ 。

7.5 (1) 解: 真; (2) 解: 假; (3) 解: 真; (4) 解: 假。

7.6 (1) 解: 真。

(2) 解: 将个体域中的个体分别代入公式, 然后合取, 当用 $x=5$ 代入时: $(3 > 2 \rightarrow 5 \leq 3) \vee 3 > 5 = (1 \rightarrow 0) \vee 0 = 0$

即其中此合取式里有一项为 0, 故公式的真值为假。

(3) 解: 当 x 取值 1 时有: $(1 > 1 \rightarrow 1 = 1) = 0 \rightarrow 1 = 1$ 故为真。

(4) 解: 当 x 取值 0 时有: $(0 - 1 \geq 0)$ 为假, 故公式的真值为假。

(5) 解: 不论 x 取何整数值时, 均为真, 故公式的真值为真。

(6) 解: 当 x 取值 1 时有: $2 \times 1^2 - 3 \times 1 + 1 = 0$, 故公式的真值为真。

(7) 解: 不论 x 取何整数值时 $x^2 - 3$ 不可能为 0, 故公式的真假为假。

(8) 解: 公式的真值为真。

(9) 解: 公式的真值为假。

(10) 解: 公式的真值为假。

(11) 解: 公式的真值为假。

7.7 (1) 解: 原式 $= \neg ((\forall x \exists y P(x, y) \rightarrow \exists x \forall y (\neg P(x, y))) \wedge (\exists x \forall y (\neg P(x, y)) \rightarrow (\forall x \exists y P(x, y)))$

$= \neg ((\neg \forall x \exists y P(x, y) \vee \exists x \forall y (\neg P(x, y))) \wedge (\neg \exists x \forall y (\neg P(x, y)) \vee \forall x \exists y P(x, y)))$

$= \neg ((\exists x \forall y \neg P(x, y) \vee \exists x \forall y (\neg P(x, y))) \wedge (\forall x \exists y P(x, y) \vee \forall x \exists y P(x, y)))$

$= \neg (\exists x \forall y \neg P(x, y) \vee \exists x \forall y (\neg P(x, y))) \vee \neg (\forall x \exists y P(x, y) \vee \forall x \exists y P(x, y))$

$= \forall x \exists y P(x, y) \vee \exists x \forall y (\neg P(x, y))$

$= \forall x \exists y P(x, y) \vee \exists u \forall w (\neg P(u, w))$

$= \forall x \exists y \exists u \forall w (P(x, y) \vee \neg P(u, w))。$

(2) 解: 原式 $= \neg ((\exists x \forall y P(x, y) \rightarrow \forall x \exists y (\neg P(x, y))) \wedge (\forall x \exists y (\neg P(x, y)) \rightarrow \exists x \forall y P(x, y)))$

$= \neg ((\neg \exists x \forall y P(x, y) \vee \forall x \exists y (\neg P(x, y))) \wedge (\neg \forall x \exists y (\neg P(x, y)) \vee \exists x \forall y P(x, y)))$

$= \neg (\forall x \exists y (\neg P(x, y)) \wedge (\exists x \forall y P(x, y)))$

$= \neg \forall x \exists y (\neg P(x, y)) \vee \neg \exists x \forall y P(x, y)$

$$= \exists x \forall y P(x, y) \vee \forall x \exists y (\neg P(x, y))$$

$$= \exists x \forall y \forall u \exists w (P(x, y) \vee \neg P(u, w))。$$

(3) 解: 原式 $= \neg \exists x (\neg \exists y P(x, y)) \vee (\neg \exists z Q(z) \vee R(x))$

$$= \forall x \exists y P(x, y) \vee (\forall z \neg Q(z) \vee R(x))$$

$$= \forall x \exists y P(x, y) \vee (\forall z \neg Q(z) \vee R(u))$$

$$= \forall x \exists y \forall z (P(x, y) \vee \neg Q(z) \vee R(u))。$$

7.8 (1) 证明: 原式

$$= \neg \exists x (\neg P(x) \wedge \neg Q(x)) \Rightarrow \neg (\exists x (\neg P(x)) \wedge \exists x (\neg Q(x)))$$

$$= \forall x P(x) \vee \forall x Q(x) \Rightarrow \forall x P(x) \vee \exists x Q(x)$$

(2) 证明: 原式 $= \forall x (\neg P(x) \vee (Q(x) \wedge R(x))) \wedge \exists x (P(x) \wedge Q(x))$

$$= \forall x ((\neg P(x) \vee Q(x)) \wedge \forall x (\neg P(x) \vee R(x))) \wedge \exists x (P(x) \wedge Q(x))$$

$$= \forall x (\neg P(x) \vee Q(x)) \wedge \forall x (\neg P(x) \vee R(x)) \wedge \exists x (P(x) \wedge Q(x))$$

$$= \neg \exists x (P(x) \wedge \neg Q(x)) \wedge \neg \exists x (P(x) \wedge \neg R(x)) \wedge \exists x (P(x) \wedge Q(x))$$

$$\Rightarrow \neg (\exists x P(x) \wedge \exists x \neg Q(x)) \wedge \neg (\exists x P(x) \wedge \exists x \neg R(x)) \wedge \exists x P(x) \wedge \exists x Q(x)$$

$$= (\neg \exists x P(x) \vee \neg \exists x \neg Q(x)) \wedge (\neg \exists x P(x) \vee \neg \exists x \neg R(x)) \wedge \exists x P(x) \wedge \exists x Q(x)$$

$$= ((\neg \exists x P(x) \wedge \exists x P(x)) \vee (\neg \exists x \neg Q(x) \wedge \exists x P(x))) \wedge (\neg \exists x P(x) \vee \neg \exists x \neg R(x)) \wedge \exists x Q(x)$$

$$= \forall x Q(x) \wedge \exists x Q(x) \wedge ((\exists x P(x) \wedge \neg \exists x P(x)) \vee (\exists x P(x) \wedge \forall x R(x)))$$

$$= \forall x Q(x) \wedge \exists x Q(x) \wedge \exists x P(x) \wedge \forall x R(x)$$

$$\Rightarrow \forall x Q(x) \wedge \forall x R(x) \wedge \exists x P(x)$$

$$= \forall x (Q(x) \wedge R(x)) \wedge \exists x P(x)$$

$$\Rightarrow \exists x(Q(x) \wedge R(x)) \wedge \exists xP(x)$$

$$\Rightarrow \exists x(Q(x) \wedge R(x))。$$

7.9 答:D。

7.10 答: $(P(x, y) \wedge Q(x, y)); P(x, y)。$

7.11 答:C。

7.12 解:5 是质数;2 是偶数并且 2 是质数;对于所有 x ,若 x 能被 2 除尽,则 x 是偶数;某些偶数能除尽 6。

7.13 答:B。

7.14 答:D。

7.15 答:B。

7.16 答: $\Rightarrow$; $=。$

习题八解答

8.1 答:各领域中都有一些最基本的规则称为公理,可由公理来推出其他的规则和定理,公理的正确性是公认的,可以脱离具体的领域将公理抽象化(只有语法含义)构成形式系统,主要涉及三方面:

1. 不矛盾性。公理系统中所有公理互不矛盾的。

2. 完备性。对于一个赋予具体含义的公理系统,对于其所表示的领域中的所有定理、规则均可在系统中推出,则称其具有相对完备性;如果将另一非定理的公式加入公理系统后,会使系统成为矛盾的系统,则称其具有绝对完备性。

3. 独立性。系统中的每条公理不可能由其他公理推出。

8.2 解:实际上令公理(2)中 P, Q 均取 R 时,有:

$(R \rightarrow (R \rightarrow R)) \rightarrow (R \rightarrow (R \rightarrow R))$ 。

令 $(R \rightarrow (R \rightarrow R))$ 为 P , 则有 $P \rightarrow P$ 形式。

8.3 (1) 证明:由推理定理可知,只要证明:

$R \rightarrow P, R \rightarrow Q, R \vdash P \wedge Q$

- | | |
|---------------------|-------------|
| ① R | 假设前提。 |
| ② $R \rightarrow P$ | 假设前提。 |
| ③ P | 分②、①。 |
| ④ $R \rightarrow Q$ | 假设前提。 |
| ⑤ Q | 分④、①。 |
| ⑥ $P \wedge Q$ | 规则 10. ③、⑤。 |

(2) 证明:由推理定理可知,只要证明: $P \wedge Q \rightarrow R, P, Q \vdash R$

- | | |
|------------------------------|-------------|
| ① P | 假设前提。 |
| ② Q | 假设前提。 |
| ③ $P \wedge Q$ | 规则 10. ①、②。 |
| ④ $P \wedge Q \rightarrow R$ | 假设前提。 |
| ⑤ R | 分④、③。 |

8.4 解:错在:由(4)、(5)中的 e 对有些 $P(e)$ 成立、 e 对有些 $Q(e)$ 成立,得到(6)的 $P(e)、Q(e)$ 一定同时成立,即不应得出 $P(e) \wedge Q(e)$ 。

8.5 答:假设推理法利用推理定理,对于证明一个带蕴含符的复杂公式为永真的,只要证明它的最后一个后件为永真,而其所有前件(假设前提),均可作为已知条件(永真公式)使用。此种方法由于减少了待证成分而增加了永真成分,从而使证明变得相对容易、方

便,证明过程从本质上得到简化。

8.6 (1) 证明:只要证 $\forall x(P(x) \rightarrow Q(x)), \exists xP(x) \vdash \exists xQ(x)$ 。

① $\forall x(P(x) \rightarrow Q(x))$ 假设前提。

② $P(e) \rightarrow Q(e)$ $US①$ 。

③ $\exists xP(x)$ 假设前提。

④ $P(e)$ $ES③$ 。

⑤ $Q(e)$ 分②、④。

⑥ $\exists xQ(x)$ $EG⑤$ 。

(2) 证明:只要证 $\forall x \forall y P(x, y) \vdash \forall y \forall x P(x, y)$

① $\forall x \forall y P(x, y)$ 假设前提。

② $\forall y P(x, y)$ $US①$ 。

③ $P(x, y)$ $US②$ 。

④ $\forall x P(x, y)$ $UG③$ 。

⑤ $\forall y \forall x P(x, y)$ $UG④$ 。

习题九解答

9.1 可以从第九章的3个应用中选择2个,它们是:

(1) 离散数学在关系数据库中的应用。

主要应用近世代数建立关系代数理论,应用数理逻辑建立关系演算理论,用这些理论可以建立关系数据库模型。

(2) 离散数学在纠错码中的应用。

主要应用近世代数建立纠错码理论,用于数据通信的数码纠错。

(3) 离散数学在逻辑程序设计语言中的应用。

主要应用谓词逻辑理论建立逻辑程序设计语言,并用该语言以求解实际应用中的问题。

9.2 解题者可根据自己熟悉的应用领域自由回答,在解题中应注意:

(1) 选择的应用要适当。

(2) 选用的工具(如集合论、图论、近世代数及数理逻辑)在应用时要作适当之调整。

(3) 用离散数学的目的是为解决应用中的问题,因此在选用工具时要注意最终能用该工具解决应用中的具体问题。

参 考 文 献

- 1 Kleene S C 著 . 莫绍揆译 . 元数学导论 . 北京:科学出版社,1984
- 2 王兵山等 . 离散数学 . 长沙:国防科大出版社,1985
- 3 王元元等 . 离散数学 . 北京:科学出版社,1994
- 4 左孝凌 . 离散数学 . 上海:上海科技文献出版社,1996
- 5 耿素云等 . 离散数学基础 . 北京:北京大学出版社,1997
- 6 徐洁磐 . 离散数学导论 . 北京:高等教育出版社,1990
- 7 张效祥,徐家福 . 计算机科学技术百科全书 . 北京:清华大学出版社,1998
- 8 任现森等 . 计算机数学基础——离散数学 . 北京:中央广播电视大学出版社,2000
- 9 Enderton H B. Element of set Theory. New York:Academic press, 1977
- 10 Burris S. A Course in Universal Algebra. New York:Springer-Verlag,1981
- 11 Matt J L, Kandel A, Baker T P. Discrete Mathematics for Computer Scientists. Prentice Hall Company, 1983