

山东省强化建设重点学科

“聊城大学课程与教学论”基金项目

现代数学课程研究

宋宝和 主编
房元霞 副主编

现代数学课程 的学科基础

房元霞 于兴江 宗培磊 著



山东大学出版社

责任编辑
孙秀英

封面设计
午云



ISBN 7-5607-3244-5



9 787560 732442 >

定价(全三册) : 48.00元

山东省强化建设重点学科

“聊城大学课程与教学论”基金项目

现代数学课程研究

宋宝和 主编
房元霞 副主编

现代数学课程 的学科基础

房元霞 于兴江 宗培磊 著



山东大学出版社

图书在版编目(CIP)数据

现代数学课程的学科基础/宋宝和主编. —济南:
山东大学出版社, 2006. 8
(现代数学课程研究)
ISBN 7-5607-3244-5

I. 现...

II. 宋...

III. 数学教学-教学研究-高等学校

IV. 01-4

中国版本图书馆 CIP 数据核字(2006)第 099270 号

山东大学出版社出版发行

(山东省济南市山大南路 27 号 邮政编码:250100)

山东省新华书店经销

济南景升印业有限公司印刷

850×1168 毫米 1/32 21 印张 528 千字

2006 年 8 月第 1 版 2006 年 8 月第 1 次印刷

定价(全三册): 48.00 元

版权所有,盗印必究

凡购本书,如有缺页、倒页、脱页,由本社营销部负责调换



主编简介

宋宝和，博士，聊城大学教授、研究生导师，山东省新课程高考改革研究项目“语文、数学、外语”课题组组长，山东省强化重点建设学科“数学课程与教学论方向”学科带头人，全国合作教学研究中心副主任，《数学教育学报》编委，教育部山东师范大学教育课程研究中心兼职研究员，长期从事数学及数学教育研究，主持多项国家及省级研究课题，已出版专著四部、教材一部，在《课程 教材 教法》、《中国教育学刊》、《数学教育学报》等学术期刊发表论文40余篇。

目 录

第一章 开关电路与布尔代数	(1)
第一节 布尔代数的一般理论	(2)
第二节 开关电路与布尔代数	(5)
第三节 布尔代数的运算法则、布尔函数和基本定理	(10)
第四节 布尔函数的两种标准形	(13)
第五节 布尔函数的简化	(17)
第六节 布尔函数的电路实现	(24)
第二章 差分方程	(28)
第一节 基本概念 线性差分方程解的基本定理	(28)
第二节 一阶常系数线性差分方程	(32)
第三节 二阶常系数线性差分方程	(38)
第四节 差分方程的简单经济应用	(43)
第三章 优选法	(46)
第一节 什么是优选法	(46)
第二节 单因素优选法	(47)
第三节 双因素优选法	(67)
第四章 球面几何初步	(76)
第一节 球面及球面上的圆	(76)
第二节 球面上的几何图形及坐标系	(82)

第三节	球面三角形的性质	(86)
第四节	球面三角形的计算公式	(93)
第五章	图论初步	(98)
第一节	图的基本概念	(98)
第二节	路与连通性	(104)
第三节	欧拉图与哈密顿图	(108)
第四节	树	(115)
第五节	最短路问题	(121)
第六章	欧拉公式与闭曲面分类	(127)
第一节	拓扑变换与拓扑不变量	(127)
第二节	欧拉公式的发现	(130)
第三节	欧拉公式的证明	(137)
第四节	正多面体只有五种的证明和拓扑思想的应用	(141)
第五节	曲面	(148)
第六节	曲面的欧拉示性数	(153)
第七章	信息安全与密码	(160)
第一节	信息安全与密码学简介	(160)
第二节	密码学与信息安全的基本概念	(163)
第三节	流密码	(167)
第四节	公钥体制以及基于大数分解的 RSA 方案	(170)
第五节	基于离散对数的 Diffie-Hellman 方案 和 ELGamal 方案	(174)
第六节	秘密分割 Shamir 门限方案	(178)
附录	王小云教授成功破译 MD5, SHA-1	(181)
参考文献		(186)
后记		(188)

第一章

开关电路与布尔代数

高度的抽象性及其带来的符号化、形式化是数学的基本特征之一。不同的实际问题经抽象、概括后,可以得到相同的数学概念、运算法则,乃至同一数学理论。反之,同一数学概念、运算法则和数学理论可应用到表面看来完全不同的实际问题中。

布尔代数最初是作为对逻辑思维法则的研究出现的。英国哲学家布尔(George Boole, 1815~1864)于 1847 年的论文《逻辑的数学分析》及《思维法则的研究》中引入了布尔代数。20 世纪 30 年代,信息论科学的创始人美国的申农(C. E. Shannon, 1916~2001)发表了《继电器和开关电路的符号分析》一文,为布尔代数在工艺技术中的应用开创了道路。20 世纪 50 年代苏联科学家把布尔代数发展成为接点网络实用中的通用理论,又使布尔代数又成了计算机科学重要的基础理论。

从逻辑上讲,布尔代数是一个命题演算系统。

从抽象代数的观点讲,布尔代数是一个代数系统。

从集合的观点讲,它是一个集合代数。

从工程技术的观点讲,布尔代数是电路代数,数字电路的设计离不开它。

你可能了解数理逻辑、集合论和抽象代数的有关知识(不了解的读者不妨从第二节开始阅读),所以在本章中,我们不再重复这些内容,而是先回顾布尔代数的抽象定义,再结合开关电路来体会布尔先生创造的这种崭新的代数系统,把逻辑思维的规律,归结为代数演算的过程,并初步认识布尔代数在数字电路设计中的应用价值。

第一节 布尔代数的一般理论

设 $(S, \leq)$ 是偏序集,如果 $\forall a, b \in S, \{a, b\}$ 都有最小上界和最大下界,则称 S 关于偏序关系 $\leq$ 作成一个格。

由于最小上界和最大下界的唯一性,可以把求 $\{a, b\}$ 的最小上界和最大下界看成 a 与 b 的二元运算“ $\wedge$ ”与“ $\vee$ ”,即 $a \vee b$ 和 $a \wedge b$ 分别表示 a 与 b 的最小上界和最大下界。这里出现的 $\vee$ 与 $\wedge$ 不再代表逻辑上的析取与合取运算,而是格中的运算符。

偏序集 $(P(A), \subseteq)$ 是格。因为 $\forall x, y \in P(A), x \vee y$ 就是 $x \cup y, x \wedge y$ 就是 $x \cap y$ 。由于 $\cup$ 和 $\cap$ 运算在 $P(A)$ 上是封闭的,所以 $x \cup y, x \cap y \in P(A)$ 。我们称 $(P(A), \subseteq)$ 为 A 的幂集格。偏序集 $(Z, \leq)$ 也是格。因为 $\forall a, b \in Z, a \vee b = \max\{a, b\}, a \wedge b = \min\{a, b\}$,它们都是整数。这样 $\vee$ 与 $\wedge$ 分别是偏序集 $(Z, \leq)$ 上的“取大”和“取小”运算。任一全序集都是格。这是因为如果 a 与 b 是全序集的两个元素,我们有 $a \leq b$ 或 $b \leq a$,在前一种情况下, $a \vee b = b, a \wedge b = a$,而在后一种情况下, $a \vee b = a, a \wedge b = b$ 。

在一个偏序集中,如果它的每一个子集(有限集或无限集)都有一个最小上界和最大下界,就称这种格为完全格。对于任一完全格 L, L 本身作为一个子集它的最小上界就是整个格的最大元素, L 的最大下界就是整个格的最小元素,分别记为 1 和 0 。这样一个完全格中,对于任一元素 a ,有 $0 \leq a$ 和 $a \leq 1$ 。

A 的幂集格 $P(A)$ 是一个完全格, 格中的最大元素为 $1=A$ (全集), 最小元素为 $0=\emptyset$ (空集)。集合 $B=\{1, 2, 3, 6\}$, 取偏序关系为整除关系, 这时 $a \vee b = [a, b]$ (a 与 b 的最小公倍数), $a \wedge b = (a, b)$ (a 与 b 的最大公约数)。显而易见 B 是一个完全格, 最大元是 6, 最小元是 1。

在一个格 L 中, $a \wedge b$ 与 $a \vee b$ 可视为格上的两种运算, 可以证明这两种运算适合交换律、结合律、幂等律和吸收律, 这样格就是具有两个二元运算的代数系统 $(L, \wedge, \vee)$ 。

一般说来, 格中运算 $\vee$ 与 $\wedge$ 不一定满足分配律, 满足分配律的格成为分配格。

设 $(L, \vee, \wedge)$ 是格, 若 $\forall a, b, c \in L$, 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 L 为分配格。

前述两个完全格都是分配格。

具有最大元素与最小元素的格称为有界格。在有界格中同一律和零律成立。

在一个有界格 L 中, 如果对于 L 的元素 a , 存在元素 $\bar{a} \in L$, 使得 $a \vee \bar{a} = 1$, 同时 $a \wedge \bar{a} = 0$, 就称 $\bar{a}$ 为 a 的补元 (余元)。如果 L 中的每一个元素都有补元, 就称 L 为有补格。

定理 1 设 $(L, \wedge, \vee, 0, 1)$ 是有界分配格。若 $a \in L$, 且对于 a 存在补元 b , 则 b 是 a 的唯一补元。

证明 假设 $c \in L$ 也是 a 的补元, 则有

$$a \vee c = 1, \quad a \wedge c = 0$$

又知 b 是 a 的补元, 故

$$a \vee b = 1, \quad a \wedge b = 0$$

从而得到

$$a \vee c = a \vee b, \quad a \wedge c = a \wedge b$$

由于 L 是分配格

$$\begin{aligned} c &= c \vee (a \wedge c) = c \vee (a \wedge b) = (c \vee a) \wedge (c \vee b) \\ &= (b \vee a) \wedge (c \vee b) = (b \vee a) \wedge (b \vee c) \\ &= b \vee (a \wedge c) = b \vee (a \wedge b) = b \end{aligned}$$

定义 1 一个有补、分配格称为一个布尔代数。

布尔代数的一个重要的例子就是 A 的幂集 $P(A)$ 所成的格, 我们称其为集合代数。在布尔代数中, 每个元素都存在着唯一的补元, 可以把求补元的运算看作是布尔代数中的一元运算。从而可以把一个布尔代数标记为 $(B, \wedge, \vee, -, 0, 1)$, 其中“ $-$ ”为求补运算。由此可以看出, 下文我们所说的布尔代数, 实际上仅是一个除空集外最简单的布尔代数。

定理 2 设 $(B, \wedge, \vee, -, 0, 1)$ 是布尔代数, 则

(1) 双重否定律 $\forall a \in B, \bar{\bar{a}} = a$

(2) 德摩根律 $\forall a, b \in B, \overline{a \wedge b} = \bar{a} \vee \bar{b}, \overline{a \vee b} = \bar{a} \wedge \bar{b}$

证明 (1) $\bar{a}$ 是 a 的补元, a 也是 $\bar{a}$ 的补元, 由补元的唯一性得 $\overline{(\bar{a})} = \bar{\bar{a}} = a$ 。

(2) 对于 $\forall a, b \in B$ 有

$$\begin{aligned} (a \wedge b) \vee (\bar{a} \vee \bar{b}) &= (a \vee \bar{a} \vee \bar{b}) \wedge (b \vee \bar{a} \vee \bar{b}) \\ &= (1 \vee \bar{b}) \wedge (\bar{a} \vee 1) = 1 \wedge 1 = 1 \end{aligned}$$

$$\begin{aligned} (a \wedge b) \wedge (\bar{a} \vee \bar{b}) &= (a \wedge b \wedge \bar{a}) \vee (a \wedge b \wedge \bar{b}) \\ &= (0 \wedge b) \vee (a \wedge 0) = 0 \vee 0 = 0 \end{aligned}$$

所以 $\bar{a} \vee \bar{b}$ 是 $a \wedge b$ 的补元, 根据补元的唯一性有 $\overline{a \wedge b} = \bar{a} \vee \bar{b}$ 。同理可证 $\overline{a \vee b} = \bar{a} \wedge \bar{b}$ 。

当我们验证一个代数系统是布尔代数时, 根据定义, 必须验证交换律、结合律、吸收律、分配律成立, 还必须验证每个元素都存在着补元, 实际上可以简单一些。

定义 2 设 $(B, *, \circ)$ 是代数系统, $*$ 和 $\circ$ 是二元运算。若 $*$ 和 $\circ$ 满足:

(1) 交换律, 即 $\forall a, b \in B$ 有

$$a * b = b * a, \quad a \circ b = b \circ a$$

(2) 分配律, 即 $\forall a, b, c \in B$ 有

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

(3) 同一律, 即存在 $0, 1 \in B$, 使得 $\forall a \in B$ 有

$$a * 1 = a \quad a \circ 0 = a$$

(4) 互补律(矛盾律和排中律), 即 $\forall a \in B$, 存在 $\bar{a} \in B$ 使得

$$a * \bar{a} = 0, \quad a \circ \bar{a} = 1$$

则称 $(B, *, \circ)$ 是一个布尔代数。

以上定义中的同一律是说 1 是 $*$ 运算的单位元, 0 是 $\circ$ 运算的单位元, 可以证明 1 和 0 分别也是 $\circ$ 和 $*$ 运算的零元。为了证明 $(B, *, \circ)$ 是布尔代数, 只须证明它是一个格, 即证明 $*$ 和 $\circ$ 运算满足结合律和吸收律, 我们在此略去证明, 有兴趣的读者可以作为练习。

第二节 开关电路与布尔代数

我们以开关电路为背景引出布尔代数。

电子数字计算机、电子交换机等数字系统虽然十分复杂, 但是它们主要都是用开关元件构成的。所谓开关元件, 指的是这类元件本身具有或者表现出两种截然不同的状态。例如, 一般的电键或开关具有闭合与断开两种状态; 电磁继电器有动作或释放两种状态; 晶体二极管或三极管的截止及导通; 晶体管电路输出电位的高低; 脉冲电路输出脉冲的有无, 等等。

用开关元件构成的电路叫做开关电路, 而用电子开关元件构成的电路则通常称为数字电路(这里仅研究数字电路的逻辑功能方面)。

由于开关元件具有相同的共性, 所以我们仅以开关控制的电路为例说明。每一开关有两种状态: 通和不通; 每一电路也有两种

状态:通和不通。我们用小写英文字母表示开关,大写英文字母表示电路。图 1-2-1 是由一个开关控制的电路,图 1-2-2 表示开关 a 和开关 b 串联得到的电路,只有当两个开关同时闭合时,指示灯才会亮;图 1-2-3 表示开关 a 和开关 b 并联得到的电路,只要任何一个开关闭合,指示灯都会亮;而在图 1-2-4 中,开关断开时灯亮,开关闭合时灯反而不亮。

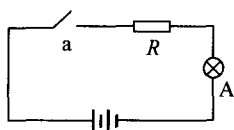


图 1-2-1

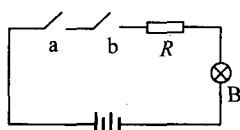


图 1-2-2

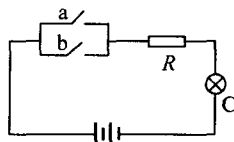


图 1-2-3

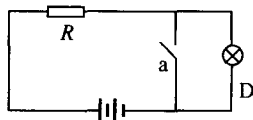


图 1-2-4

一般地,对任意电路 A, B 也可经过串联、并联或反演得到新的电路,它们顺序记作“ A 串联 B ”、“ A 并联 B ”、“ A 的反演”。 A, B 原来的状态与新的电路的状态之间的关系如表 1-2-1~1-2-3 所示。

表 1-2-1

电路 A	电路 B	A 串联 B
不通	不通	不通
不通	通	不通
通	不通	不通
通	通	通

表 1-2-2

电路 A	电路 B	A 串联 B
不通	不通	不通
不通	通	通
通	不通	通
通	通	通

表 1-2-3

电路 A	A 的反演
不通	通
通	不通

我们已经习惯于数学的符号化方法。只要把上面各表中的状态“通”、“不通”用简单符号表示,就能大大简化。我们用数字“1”表示“通”,用数字“0”表示“不通”。在其他开关元件中用“1”表示电位信号中的高电位,脉冲信号中的有脉冲,或继电器电路中的继电器开关或接点的动作状态;反之,用“0”表示低电位,无脉冲信号或者继电器开关或接点的静止状态。当然在这里“1”与“0”已失去原来的数字意义,只是代表两种截然不同的电路的状态或命题的真值。再进一步符号化,而用“ $\cdot$ ”表示“串联”,“ $+$ ”表示“并联”,用“ $-$ ”表示“反演”,这样“ $A \cdot B$ ”就是“A 串联 B”,“ $A+B$ ”就是“A 并联 B”,“ $\bar{A}$ ”就是“A 的反演”,这些关系可用表 1-2-4~1-2-6 表示。

表 1-2-4

A	B	$A \cdot B$
0	0	0
0	1	0
1	0	0
1	1	1

表 1-2-5

A	B	$A + B$
0	0	0
0	1	1
1	0	1
1	1	1

表 1-2-6

A	$\bar{A}$
0	1
1	0

现在来看看,经过符号化后,我们得到了什么。

(1)一个集合 $B = \{0, 1\}$ 和在集合 B 上规定的三种运算,分别记作“ $\cdot$ ”(乘),“ $+$ ”(加),“ $-$ ”(补或非)如下:

$$\begin{array}{lll}
 \text{“} \cdot \text{”}: 0 \cdot 0 = 0 & \text{“} + \text{”}: 0 + 0 = 0 & \text{“} - \text{”}: \bar{0} = 1 \\
 0 \cdot 1 = 0 & 0 + 1 = 1 & \bar{1} = 0 \\
 1 \cdot 0 = 0 & 1 + 0 = 1 & \\
 1 \cdot 1 = 1 & 1 + 1 = 1 &
 \end{array}$$

三种运算的顺序是先“—”，后“ $\cdot$ ”和“+”，“ $\cdot$ ”可省略不写，有括号的先算括号里面的。不难证明， $\{B=\{0,1\}; \cdot, +, 1\}$ 为一个布尔代数。

(2)任何电路可以表示成一个布尔代数式。例如，电路图 1-2-5 可表示成： $((a \cdot b) + (c \cdot d)) \cdot \bar{e}$ 。欲知电路的效应，例如当 $a=1, b=0, c=1, d=1, e=0$ 时，按照前面提供的规则进行计算得：

$$((1 \cdot 0) + (1 \cdot 1)) \cdot \bar{0} = (0 + 1) \cdot 1 = 1 \cdot 1 = 1$$

即此时的状态是“通”。

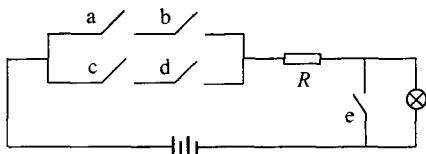


图 1-2-5

当然，每一个类似上面这样有一些小写字母（表示开关）经“+”，“ $\cdot$ ”，“—”运算及适当的括号连接起来的布尔代数式也给出一个电路来。

在本节最后，我们提出下面一个具体问题：设计一个三人表决的电路，当多数人赞同时，表决通过。即实现表 1-2-7 效应的电路。

表 1-2-7

a	b	c	$f(a, b, c)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1

1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

事实上,这个电路所要求效应,就不是前述简单的电键开关电路所容易实现的,还需要我们展开对布尔代数的进一步讨论。

第三节 布尔代数的运算法则、布尔函数和基本定理

一、布尔代数的运算法则

设 a, b, c 为布尔代数中的任意变量。

(1) 双重否定律 $\bar{\bar{a}} = a$

(2) 幂等律 $a \cdot a = a, a + a = a$

(3) 交换律 $a \cdot b = b \cdot a, a + b = b + a$

(4) 结合律 $(a \cdot b) \cdot c = a \cdot (b \cdot c), (a + b) + c = a + (b + c)$

(5) 分配律 $a \cdot (b + c) = a \cdot b + a \cdot c, a + b \cdot c = (a + b) \cdot (a + c)$

(6) 德摩根律 $\overline{a \cdot b} = \bar{a} + \bar{b}, \overline{a + b} = \bar{a} \cdot \bar{b}$

(7) 吸收律 $a \cdot (a + b) = a, a + a \cdot b = a$

(8) 零律 $a \cdot 0 = 0, a + 1 = 1$

(9) 同一律 $a \cdot 1 = a, a + 0 = a$

(10) 排中律 $a + \bar{a} = 1$

(11) 矛盾律 $a \cdot \bar{a} = 0$

这些定律你可能比较熟悉,因为它们在集合论、概率论、命题逻辑中都成立。把布尔代数与开关电路相联系,物理也会给出我们一些启示。例如,设 a 表示开关 a ,两个开关 a 串联和由一个开关 a 组成的电路是等效的,所以 $a \cdot a = a$ 在布尔代数 B 中也应该