离散数学

大连理工大学软件学院

陈志奎 博士、教授、博士生导师

办公室： 综合楼405，Tel： 62274392

实验室：综合楼一楼

Mobile: 13478461921

Email: zkchen@dlut.edu.cn

zkchen00@hotmail.com

QQ： 1062258606

第八章　格与布尔代数

回 顾

- 半群和独异点的定义及性质
- 半群和独异点的同态与同构
- 积半群
- 群的基本定义与性质
- 置换群和对称群
- 子群与陪集
- 群的同态与同构
- 环与域

回 顾

- 群的定义
- 群的性质
  - 群的基本性质
  - 幂运算规则
  - 方程存在唯一解
  - 消去律
  - 元素的阶
  - 群的阶
  - Abel群
- 子群的定义
- 子群的判定定理
- 子群的性质
  - 生成子群
  - 中心C
  - 子群的交
  - 子群格
- 子群的陪集定义与性质
- 拉格朗日定理

回　顾

- 循环群定义及性质
  - 生成元、n阶循环群、无限循环群
- 置换群定义及性质
- 群的同态与同构
  - 群同态映射：单一同态、满同态、群同构映射
- 环的概念与性质
- 域的概念
- 应用：群与网络安全

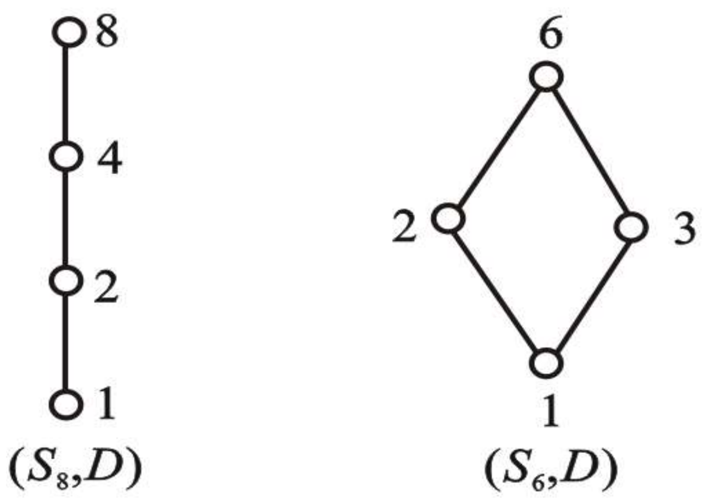
主要内容

- 格的定义及性质
- 格的对偶原理
- 子格
- 分配格、有补格
- 布尔代数

8.1 格的定义与性质

定义8.1.1 设$\langle L, \preccurlyeq \rangle$是偏序集，如果$\forall a, b \in L$，$\{a, b\}$都有最小上界和最大下界，则称$L$关于偏序$\preccurlyeq$构成格，称$\langle L, \preccurlyeq \rangle$是格.

例 8.1.1 设n是正整数，S_n是n的正因子的集合. D为整除关系，则偏序集$\langle S_n, D \rangle$构成格. $\forall x, y \in S_n$，$x \vee y$是$lcm(x, y)$，即x与y的最小公倍数。 $x \wedge y$是$\gcd(x, y)$，即x与y的最大公约数.



对偶原理

设 f 是含有格中元素以及符号 $=, \preccurlyeq, \succcurlyeq, \vee$ 和 $\wedge$ 的命题。令 f^* 是将 f 中的 $\preccurlyeq$ 替换成 $\succcurlyeq$，$\succcurlyeq$ 替换成 $\preccurlyeq$，$\vee$ 替换成 $\wedge$，$\wedge$ 替换成 $\vee$ 所得到的命题. 称 f^* 为 f 的对偶命题。

例如, 在格中令 f 是 $(a \vee b) \wedge c \preccurlyeq c$, f^* 是 $(a \wedge b) \vee c \succcurlyeq c$.

格的对偶原理

设 f 是含有格中元素以及符号 $=$，$\preccurlyeq$，$\succcurlyeq$，$\vee$ 和 $\wedge$ 等的命题。若 f 对一切格为真，则 f 的对偶命题 f^* 也对一切格为真。

例如, 如果对一切格 L 都有 $\forall a, b \in L, a \wedge b \preccurlyeq a$，那么对一切格 L 都有 $\forall a, b \in L, a \vee b \succcurlyeq a$。

- 注意：对偶是相互的，即 $(f^*)^* = f$

8.1 格的定义与性质

定理8.1.1 设 $\langle L, \preccurlyeq \rangle$ 是格, 则运算$\vee$和$\wedge$适合交换律、结合律、幂等律和吸收律, 即

(1) $\forall a, b \in L$, 有

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

(2) $\forall a, b, c \in L$, 有

$$(a \vee b) \vee c = a \vee (b \vee c), (a \wedge b) \wedge c = a \wedge (b \wedge c)$$

(3) $\forall a \in L$, 有

$$a \vee a = a, a \wedge a = a$$

(4) $\forall a, b \in L$, 有

$$a \vee (a \wedge b) = a, a \wedge (a \vee b) = a$$

8.1 格的定义与性质

➢ 格中满足四条运算定律，但等幂律可由吸收律推出，故上述定义只需满足三条运算定律即可。

定义8.1.2 设$\langle S, *, \circ\rangle$是含有两个二元运算$*$和$\circ$的代数系统。如果$*$和$\circ$满足交换律、结合律、吸收律，则$\langle S, *, \circ\rangle$构成一个格。

8.1 格的定义与性质

定理8.1.2 设$\langle S,*,\circ\rangle$是具有两个二元运算的代数系统，并且$*$和$\circ$运算满足交换律、结合律、等幂律和吸收率。则可以适当的定义S中的偏序关系$\preccurlyeq$，使得$\langle S,\preccurlyeq\rangle$构成一个格，且$\forall a,b\in S$，有

$$a\wedge b=a*b, a\vee b=a\circ b.$$

8.1 格的定义与性质

定理8.1.3 设$\boldsymbol{L}$是格, 则$\forall \boldsymbol{a}, \boldsymbol{b} \in \boldsymbol{L}$有

$$\boldsymbol{a} \preccurlyeq \boldsymbol{b} \Leftrightarrow \boldsymbol{a} \wedge \boldsymbol{b} = \boldsymbol{a} \Leftrightarrow \boldsymbol{a} \vee \boldsymbol{b} = \boldsymbol{b}$$

证明（了解）： (1) 先证 $a \preccurlyeq b \Rightarrow a \wedge b = a$

由 $a \preccurlyeq a$ 和 $a \preccurlyeq b$ 可知 a 是$\{a, b\}$的下界, $a \preccurlyeq a \wedge b$。

显然有$a \wedge b \preccurlyeq a$. 由反对称性得 $a \wedge b = a$。

(2) 再证 $a \wedge b = a \Rightarrow a \vee b = b$

根据吸收律有 $b = b \vee (b \wedge a)$。

由 $a \wedge b = a$ 和上面的等式得 $b = b \vee a$, 即 $a \vee b = b$。

(3) 最后证 $a \vee b = b \Rightarrow a \preccurlyeq b$

由 $a \preccurlyeq a \vee b$得 $a \preccurlyeq a \vee b = b$

8.1 格的定义与性质

定义8.1.3 设$\langle S, \wedge, \vee\rangle$是格，L是S的非空子集，如果L关于格中的运算$\wedge$和$\vee$仍构成格，那么L是S的子格。

定义8.1.4 格的一些基本概念：

完全格：若格的每个非空子集均有上下确界，则称其为完全格。

有界格：若格$\langle L, \leq\rangle$有最小元 0 和最大元 1 ，则称此格为有界格。并且记作$\langle L, \leq, 0, 1\rangle$, 显然完全格必然有最小元和最大元。但反之不一定成立。

补元：在有界格$\langle L, \leq, 0, 1\rangle$中，对任意元素$a \in L$，若存在$b \in L$,并且$\boldsymbol{a * b = 0}$, $\boldsymbol{a \oplus b = 1}$,则称$b$是$a$的补元，补元是相互的，但补元不唯一。

8.1 格的定义与性质

例8.1.2 设**L**是格，$\forall \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in \boldsymbol{L}$有

$$\boldsymbol{a} \vee (\boldsymbol{b} \wedge \boldsymbol{c}) \leq (\boldsymbol{a} \vee \boldsymbol{b}) \wedge (\boldsymbol{a} \vee \boldsymbol{c})$$

证明： 由$a \leq a$， $b \wedge c \leq b$得

$$a \vee (b \wedge c) \leq a \vee b$$

$$a \vee (b \wedge c) \leq a \vee c$$

从而有

$$a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$$

8.2 分配格、有补格与布尔代数

定义8.2.1 设$\langle L, *, \oplus\rangle$是格，若$\forall a, b, c \in L$,有

$$(\forall a)(\forall b)(\forall c)\big(a, b, c \in L \to a * (b \oplus c) = (a * b) \oplus (a * c)\big)$$

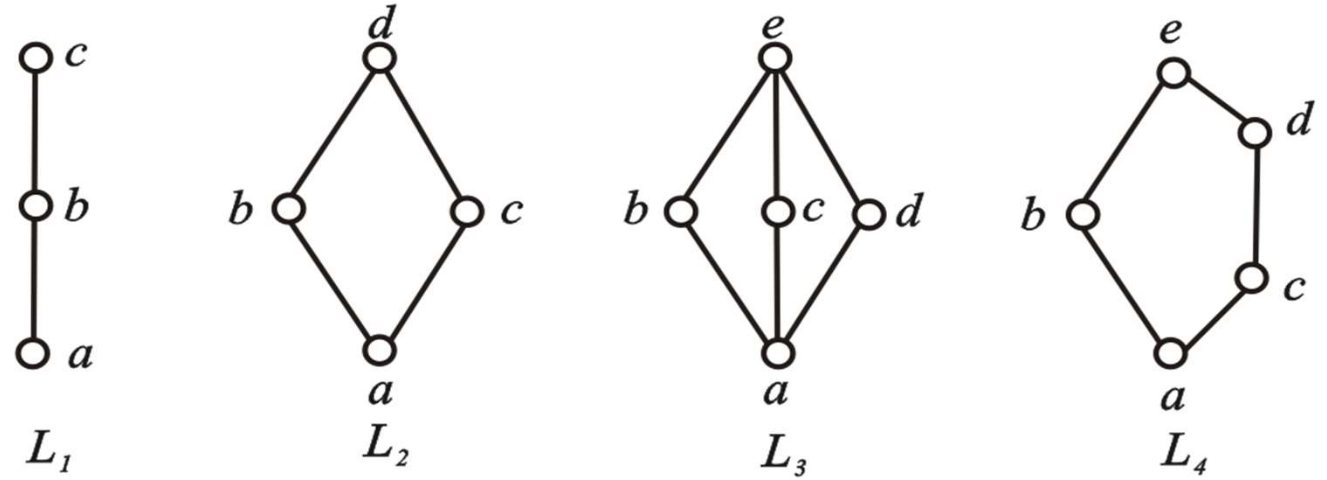
$$(\forall a)(\forall b)(\forall c)\big(a, b, c \in L \to a \oplus (b * c) = (a \oplus b) * (a \oplus c)\big)$$

则称L为分配格。

- 注意：可以证明以上两个条件互为充分必要条件。

8.2 分配格、有补格与布尔代数

例8.2.1 图中哪些是分配格，哪些不是分配格？



L_1 和 L_2 是分配格，L_3 和 L_4不是分配格。

称 L_3为钻石格，L_4为五角格。

在L_3中，$b \wedge (c \vee d) = b \wedge e = b$

$(b \wedge c) \vee (b \wedge d) = a \vee a = a$

同时在L_4中，$c \vee (b \wedge d) = c \vee a = c$

$(c \vee b) \wedge (c \vee d) = e \wedge d = d$

8.2 分配格、有补格与布尔代数

定义8.2.2 若有界格L中，每一个元素都有补元，则称L为有补格。

定义8.2.3 如果一个格是有补分配格，那么称它为布尔格或布尔代数。

定义8.2.5 设L是格，$\mathbf{0} \in \boldsymbol{L}, \boldsymbol{a} \in \boldsymbol{L}$, 若 $\forall \boldsymbol{b} \in \boldsymbol{L}$ 有

$$\mathbf{0} < \boldsymbol{b} \leq \boldsymbol{a} \Leftrightarrow \boldsymbol{b} = \boldsymbol{a}$$

则称$\boldsymbol{a}$是L中的原子。

8.2 分配格、有补格与布尔代数

定义8.2.4 设$\langle S,*,\circ\rangle$是含有两个二元运算的代数系统，若$*$和$\circ$满足：

（1）交换律：$\forall a,b\in S$ 有

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

（2）分配律： $\forall a,b,c\in S$ 有

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

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

（3）同一律：$\exists 0,1\in S$，使得$\forall a\in S$ 有

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

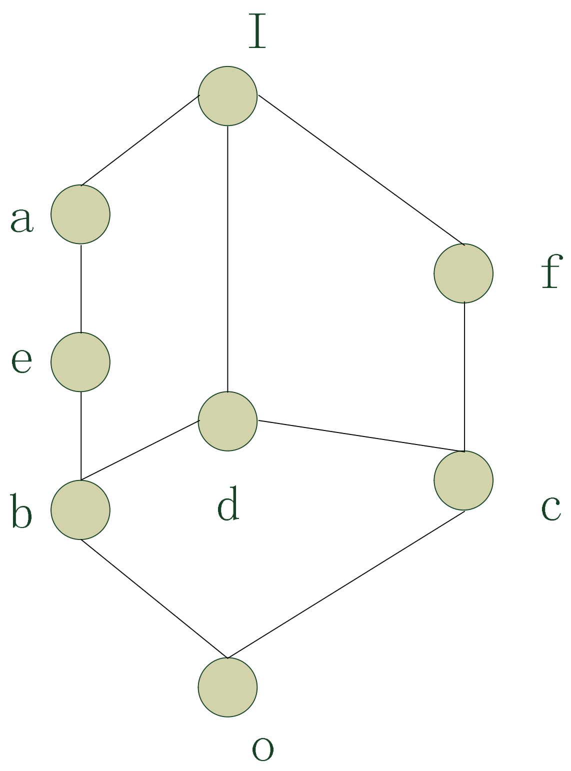
（4）补元律： $\forall a\in S$， $\exists a'\in S$ 使得

$$a*a'=0,a\circ a'=1$$

则称$\langle S,*,\circ\rangle$是一个布尔代数。

8.2 分配格、有补格与布尔代数

例8.2.2 证明如左图所示的哈塞尔图的格不是一个布尔代数。



证明： 元素a和e都是c的补，即他们两个元素c都满足

$$x \vee x' = I, x \wedge x' = 0$$

但是要求这样的性质要求这样的元素在布尔代数中是唯一的。因此，所给出的格不可能是一个布尔代数。

8.3 应用

布尔代数在数字电路设计中有重要的应用。在抽象代数中，布尔代数是捕获了集合运算和逻辑运算二者的根本性质的一个代数结构（就是说一组元素和服从定义的公理的在这些元素上运算）。特别是，它处理集合运算交集、并集、补集；和逻辑运算与、或、非。

因为真值可以在逻辑电路中表示为二进制数或电平，这种相似性同样扩展到它们，所以布尔代数在电子工程和计算机科学中同在数理逻辑中一样有很多实践应用。在电子工程领域专门化了的布尔代数也叫做逻辑代数，在计算机科学领域专门化了布尔代数也叫做布尔逻辑。

8.3 应用

布尔代数也叫做布尔格。关联于格（特殊的偏序集合）是在集合包含 $A \subseteq B$ 和次序 $a \leq b$ 之间的相似所预示的。

考虑$\{x, y, z\}$的所有子集按照包含排序的格。这个布尔格是偏序集合，在其中$\{x\} \leq \{x, y\}$。任何两个格的元素，比如$p = \{x, y\}$和$q = \{y, z\}$，都有一个最小上界，这里是$\{x, y, z\}$，和一个最大下界，这里是$\{y\}$。这预示了最小上界（并或上确界）被表示为同逻辑OR一样的符号$p \vee q$；而最大下界（交或下确界）被表示为同逻辑AND一样的符号$p \wedge q$。

8.3 应用

在数字电路中的布尔代数是一个集合A，提供了两个二元运算 (逻辑与)、 (逻辑或)，一个一元运算(逻辑非)和两个元素0（逻辑假）和1（逻辑真），此外，对于集合A的所有元素a, b和c，下列公理成立：

$a \vee (b \vee c) = (a \vee b) \vee c$　　$a \wedge (b \wedge c) = (a \wedge c) \wedge b$　　结合律

$a \vee b = b \vee a$　　$a \wedge b = b \wedge a$　　交换律

$a \vee 0 = a$　　$a \wedge 1 = a$　　吸收律

$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$　　分配律

$a \vee \neg a = 1$　　$a \wedge \neg a = 0$　　互补律

以上公式中的前三条结合律、交换律、吸收率说明布尔代数也可以定义为有补分配格。并且格中的最小元素为0，最大元素为1，任何元素a的补¬a都是唯一确定的。

总　结

- 格的定义及性质
- 格的对偶原理
- 子格
- 分配格、有补格
- 布尔代数

作 业

P181: 2,4,12