Chapter 1

集合论

Discrete Mathematics

January 3, 2015

黄正华, 数学与统计学院, 武汉大学

1.1

Contents

1.2

"离散" 的含义?

离散数学 数学的几个分支的总称, 以研究离散量的结构和相互间的关系为主要目标, 其研究对象一般地是有限个或可数无穷个元素. 比如, 集合论、组合学、数论等等.

离散量 与连续量相对, 离散量是指分散开来的、不存在中间值的量. 比如, 开关 *v.s.* 音量旋钮.

1.3

离散数学的内容

- 集合论 (Set Theory)
- 线性代数 (Linear Algebra)
- 图论 (Graph Theory)
- 数理逻辑 (Mathematical Logic)

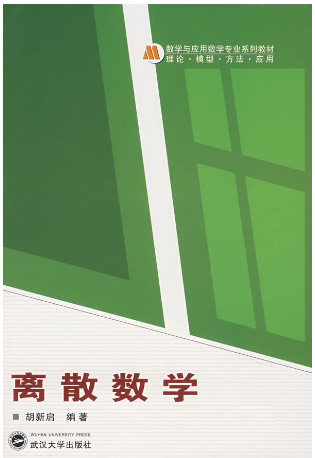
- 数论 (Number Theory)
- 组合论 (Combinatorics)
- 概率论 (Probability Theory)

1.4

课程教材

References

[1] 胡新启 离散数学 武汉大学出版社, 2007.

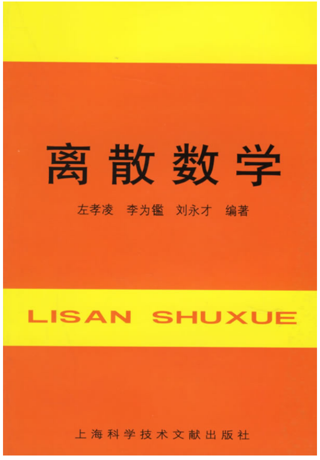


1.5

参考书籍

References

[1] 左孝凌, 李为鑑, 刘永才 离散数学 上海科学技术文献出版社, 1982.

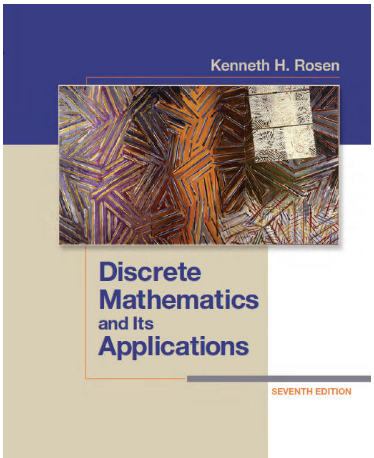


1.6

参考书籍

References

[1] Kenneth H. Rosen Discrete Mathematics and Its Application. (Seventh Edition) McGraw-Hill, 2012.

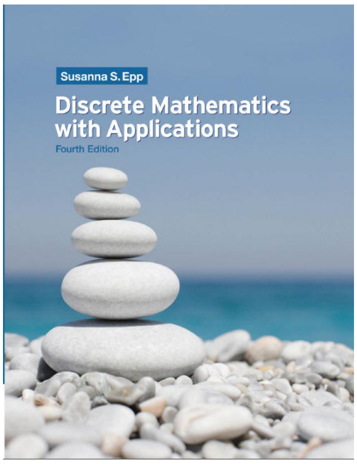


1.7

参考书籍

References

[1] Susanna S. Epp Discrete Mathematics with Applications. (4th Edition) Brooks/Cole, 2011.



1.8

1 集合的基本概念

集合的定义

- 集合是一个不能精确定义的基本概念.
- 直观地说, 集合是具有某种属性的事物的全体, 或是一些确定对象的汇合. 而这些事物就是这个集合的元素 (element) 或成员 (member).

- 一个集合把世间万物分成两类, 一些对象属于该集合, 是组成这个集合的成员, 另一些对象不属于该集合.
- 由于一个集合的存在, 世上的对象可分成两类, 任一对象或属于该集合或不属于该集合, 二者必居其一也只居其一.

1.9

集合的记法

- 集合, 通常用大写的英文字母来标记, 如 A, B, C, $\ldots$;
- 元素, 通常用小写字母来表示, 如 a, b, c, $\ldots$.
- 若 a 是集合 A 中的元素, 则称 a 属于集合 A, 记作 $a \in A$.
- 用 $x \notin X$ 表示元素 x 不属于集合 X.

1.10

集合的表示

1. *列举法:* 列出集合的所有元素.
   例如 $A = \{a, b, c, \ldots, z\}$.
2. *描述法:* 用语言概括出集合中元素的特性, 以确定集合的元素.
   例如
   $$B = \{x \mid x \in \mathbb{R} \ \wedge \ x^2 - 1 = 0\}$$
   表示方程 $x^2 - 1 = 0$ 的实数解集.

有的集合可以用两种方法来表示, 如 B 也可以写成 $\{-1, 1\}$. 但是有些集合不能用列举法表示, 如实数集合.

1.11

常见的数集

常见的数的集合, 有约定的记号来表示.

- $\mathbb{N}$ —— 自然数集合 (the set of **natural numbers**. 一般约定 0 是自然数).
  $$\mathbb{N} = \{0, 1, 2, 3, \ldots\}.$$
- $\mathbb{Z}$ —— 整数集合 (the set of **integers**. Zahl /tsa:l/ *n.*【德】数).
  $$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}.$$
- $\mathbb{Q}$ —— 有理数集合 (the set of **rational numbers**. Quotient, 商).
  $$\mathbb{Q} = \{p/q \mid p \in \mathbb{Z},\ q \in \mathbb{Z},\ \text{and } q \neq 0\}.$$
- $\mathbb{R}$ —— 实数集合 (the set of **real numbers**).
- $\mathbb{C}$ —— 复数集合 (the set of **complex numbers**).
- $\mathbb{Z}^+$ —— 正整数集合.
  $$\mathbb{Z}^+ = \{1, 2, 3, \ldots\}.$$

1.12

集合的性质

集合的基本特性:

- 确定性. 任一元素或属于该集合或不属于该集合, 两者必居其一.
- 无重复性. 集合的元素是彼此不同的. 如果同一个元素在集合中多次出现, 应该认为是一个元素. 如
$$\{1, 1, 2, 2, 3\} = \{1, 2, 3\}.$$
- 无序性. 集合的元素是无序的. 如
$$\{1, 2, 3\} = \{3, 1, 2\}.$$
- 抽象性. 集合中的元素是抽象的, 甚至可以是集合. 例如,
$$S = \Big\{a,\ \{b,\ c\},\ \{\{d\}\}\Big\},$$
其中 a, $\{b, c\}$, $\{\{d\}\}$ 是集合 S 的元素. 注意 $b \in \{b,\ c\}$, 但 $b \notin S$, 即 b 并不是集合 S 的元素. 1.13

空集与全集

Definition 1 (空集)**.** 不包含任何元素的集合, 称为空集 (empty set), 记作 $\varnothing$.

例如, $A = \{x \mid x \in \mathbb{R} \wedge x^2 + 1 = 0\}$ 是空集, 式中 $\mathbb{R}$ 表示实数集合.

Definition 2 (全集)**.** 在一定范围内, 如果所有涉及的集合都是某一集合的子集, 则称该集合为全集或论域 (Universe), 一般记作 U 或者 E. 1.14

有限集与无限集

- 只含有有限多个元素的集合称为有限集 (finite sets), 否则称为无限集 (infinite sets).
- 有限集合中元素的个数称为集合的基数 (cardinality).
- 集合 A 的基数表示为 $|A|$, 或者 $\mathrm{card}(A)$. 例如,
$$|\varnothing| = 0.$$
1.15

2 子集与集合的相等

集合间的关系

Theorem 3. *两个集合 A 和 B 相等, 当且仅当它们包含的元素相同.*

集合 A 与 B 相等, 记作 $A = B$. 若 A 与 B 不相等, 则记作 $A \neq B$.

Definition 4 (子集 & 真子集)**.** 如果 A 中每个元素都是 B 中的元素, 则称 A 为 B 的子集 (subset), 记作 $A \subseteq B$ 或 $B \supseteq A$. 如果 $A \subseteq B$ 且 $A \neq B$, 则称 A 为 B 的真子集 (proper subset), 记作 $A \subset B$.

$$A \subseteq B \Leftrightarrow (\forall x)(x \in A \to x \in B), \tag{1}$$
$$A \subset B \Leftrightarrow (\forall x)(x \in A \to x \in B) \wedge (\exists x)(x \in B \wedge x \notin A). \tag{2}$$
1.16

集合间的关系

Theorem 5. 设 A, B 为两个集合. $A = B$ 当且仅当 $A \subseteq B$ 且 $B \subseteq A$. 即

$$A = B \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A). \tag{3}$$

Theorem 6. 对于任意集合 A, $\varnothing \subseteq A$. 即空集是一切集合的子集.

平凡子集 (trivial subset)

任意非空集合 A 至少有两个子集: A 和 $\varnothing$. 称 A 和 $\varnothing$ 是 A 的 平凡子集.

1.17

集合间的关系

Theorem 7. 空集是惟一的.

证: 假设存在空集 $\varnothing_1$ 和 $\varnothing_2$, 由前述定理有

$$\varnothing_1 \subseteq \varnothing_2, \qquad \varnothing_2 \subseteq \varnothing_1.$$

根据集合相等的充要条件, 有

$$\varnothing_1 = \varnothing_2.$$

1.18

Example 8. 判断下列命题是否正确:

1. $\varnothing \subseteq \varnothing$;
2. $\varnothing \in \varnothing$;
3. $\varnothing \subseteq \{\varnothing\}$;
4. $\varnothing \in \{\varnothing\}$.

解:

- 因为空集是任何集合的子集, 所以 (1)、(3) 为真.
- (2) 为假. (因为空集不含任何元素.)
- 这里 $\varnothing$ 是集合 $\{\varnothing\}$ 的元素, 所以 (4) 为真.

1.19

注意事项

- 区分 $\in$ 和 $\subseteq$;
- $\{\varnothing\}$ 是一元集, 而不是空集;

$$\begin{aligned} \operatorname{card}\big(\{\varnothing\}\big) &= 1; \\ \operatorname{card}(\varnothing) &= 0. \\ \{\varnothing\} &\neq \varnothing; \\ \varnothing &\in \{\varnothing\}. \end{aligned}$$

1.20

罗素悖论 (Russell's paradox, 1901)

设论域是所有集合的集合, 并定义集合

$$S = \{A \mid A \notin A\}.$$

这样, S 是不以自身为元素的全体集合的集合.

那么 "S" 是不是它自己的元素呢?

- 假设 S 不是自己的元素, 那么 S 满足条件 $A \notin A$, 而该条件定义了集合 S, 所以 $S \in S$.
- 另一方面, 如果 $S \in S$, 那么 S 必须满足定义 S 的条件, 所以 $S \notin S$.

1.21

罗素悖论 (1901)

罗素曾经用*理发师悖论* (Barber paradox) 来解释他的悖论:

某镇上一位理发师宣布, 他只给那些不给自己刮脸的人刮脸.

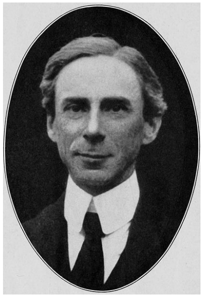
那么问题是: *理发师的脸, 谁来刮?!*

罗素悖论起因于集合可以是自己的元素的概念.

康托之后所创立的许多公理化集合论, 都直接或间接地限制集合成为它自己的元素, 从而避免了罗素悖论.

1.22

伯特兰・罗素

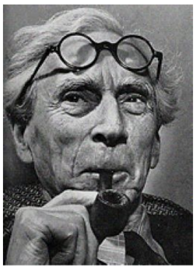


Bertrand Russell (1872 - 1970) was a British philosopher, logician, mathematician, historian, and social critic. He was born in Wales, into one of the most prominent aristocratic families in Britain. He became an orphan at an early age and was placed in the care of his father's parents, who had him educated at home. He entered Trinity College, Cambridge, in 1890, where he excelled in mathematics and in moral science.

He won a fellowship on the basis of his work on the foundations of geometry. In 1910 Trinity College appointed him to a lectureship in logic and the philosophy of mathematics.

Russell fought for progressive causes throughout his life. He held strong pacifist views, and his protests against World War I led to dismissal from his position at Trinity College.

1.23

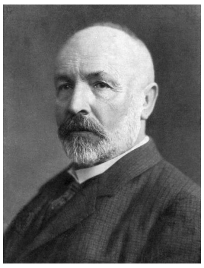


伯特兰・罗素

He was imprisoned for 6 months in 1918 because of an article he wrote that was branded as seditious. Russell fought for women's suffrage in Great Britain. In 1961, at the age of 89, he was imprisoned for the second time for his protests advocating nuclear disarmament.

Russell's greatest work was in his development of principles that could be used as a foundation for all of mathematics. His most famous work is *Principia Mathematica*, written with Alfred North Whitehead, which attempts to deduce all of mathematics using a set of primitive axioms. He wrote many books on philosophy, physics, and his political ideas. Russell won the Nobel Prize for literature in 1950. 1.24

集合论创立者: 康托



Georg Cantor(1845-1918) was born in St. Petersburg, Russia, where his father was a successful merchant. Cantor developed his interest in mathematics in his teens. He began his university studies in Zurich in 1862, but when his father died he left Zurich. He continued his university studies at the University of Berlin in 1863, where he studied under the eminent mathematicians Weierstrass, Kummer, and Kronecker.

He received his doctor's degree in 1867, after having written a dissertation on number theory. Cantor assumed a position at the University of Halle in 1869, where he continued working until his death. Cantor is considered the founder of set theory. His contributions in this area include the discovery that the set of real numbers is uncountable. He is also noted for his many important contributions to analysis. 1.25

集合论创立者: 康托

Cantor also was interested in philosophy and wrote papers relating his theory of sets with metaphysics. Cantor married in 1874 and had five children. His melancholy temperament was balanced by his wife's happy disposition. Although he received a large inheritance from his father, he was poorly paid as a professor. To mitigate this, he tried

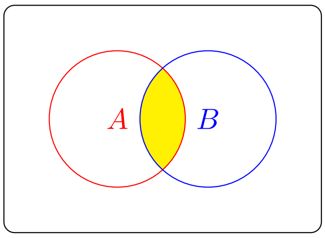


Figure 1: 交集 $A \cap B$.

to obtain a better-paying position at the University of Berlin. His appointment there was blocked by Kronecker, who did not agree with Cantor's views on set theory.

Cantor suffered from mental illness throughout the later years of his life. He died in 1918 in a psychiatric clinic. 1.26

3 集合的运算及其性质

集合的运算

Definition 9 (交集 (intersection of sets))**.** 集合 A 和 B 的交集记为 $A \cap B$, 定义为:

$$A \cap B = \{x \mid x \in A \wedge x \in B\}.$$

例如, $A = \{1, 2, 3\}$, $B = \{1, 3, 5\}$, 则 $A \cap B = \{1, 3\}$. 进一步有 1.27

$$A_1 \cap A_2 \cap \cdots \cap A_n \triangleq \bigcap_{i=1}^{n} A_i; \tag{4}$$

$$A_1 \cap A_2 \cap \cdots \cap A_n \cap \cdots \triangleq \bigcap_{i=1}^{\infty} A_i. \tag{5}$$

1.28

Definition 10 (并集 (union of sets))**.** 集合 A 和 B 的并集记为 $A \cup B$, 定义为:

$$A \cup B = \{x \mid x \in A \vee x \in B\}.$$

例如, $A = \{1, 2, 3\}$, $B = \{1, 3, 5\}$. 则 $A \cup B = \{1, 2, 3, 5\}$.
类似地有, $\bigcup_{i=1}^{n} A_i$, $\bigcup_{i=1}^{\infty} A_i$. 1.29

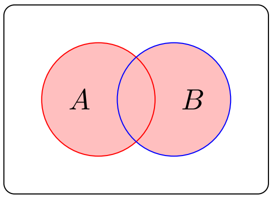


Figure 2: 并集 $A \cup B$.

Definition 11 (差集 (difference set)). 集合 A 和 B 的差集 (相对补) 记为 $A - B$(或记为 $A \backslash B$), 定义为:

$$A - B = \{x \mid x \in A \wedge x \notin B\}.$$

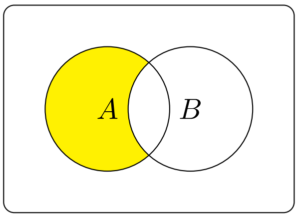


Figure 3: 差集 $A - B$.

例如 $A = \{1, 2, 3\}$, $B = \{1, 3, 5\}$. 则 $A - B = \{2\}$. 1.30

Definition 12 (补集 (complement, complementation)). 集合 A 的补集 (绝对补) 记为 $\sim A$, 定义为

$$\sim A = E - A = \left\{x \mid x \in E \wedge x \notin A\right\}.$$

常见的记法还有: $\overline{A}$, A^{c}, A'.

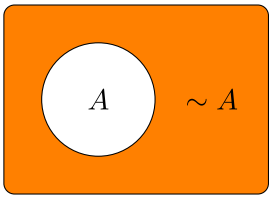


Figure 4: 补集 $\sim A$.

形式上有: $E = \sim A \cup A, \qquad \sim A \cap A = \varnothing.$ 1.31

集合的对称差

Definition 13 (对称差 (symmetric difference)). 集合 A 和 B 的对称差 (环和), 记为 $A \oplus B$. 定义为

$$A \oplus B = (A - B) \cup (B - A) = \left\{x \mid x \in A \bar{\vee} x \in B\right\}. \tag{6}$$

或记为 $A + B$. 1.32

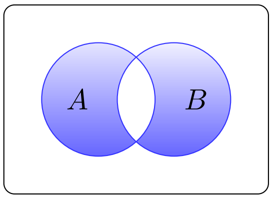


Figure 5: 对称差 $A \oplus B$.

对称差的性质

1. $A \oplus B = (A \cup B) - (A \cap B)$;
2. $B \oplus A = A \oplus B$;
3. $A \oplus A = \varnothing$;
4. $A \oplus \varnothing = A$;
5. $(A \oplus B) \oplus C = A \oplus (B \oplus C)$.

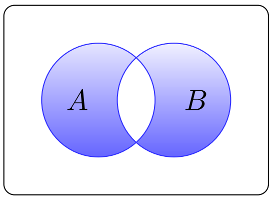
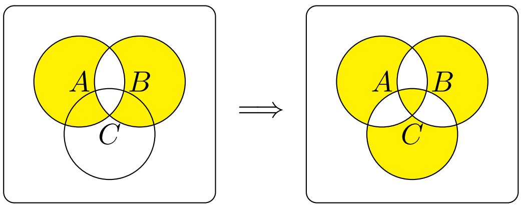


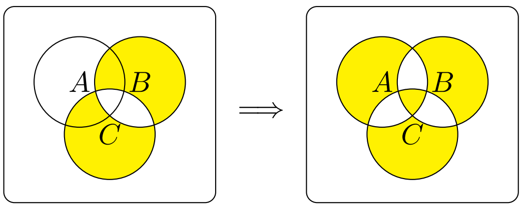
Figure 6: 对称差 $A \oplus B$.

1.33

结合律 $(A \oplus B) \oplus C = A \oplus (B \oplus C)$



(a) $(A \oplus B) \oplus C$



(b) $A \oplus (B \oplus C)$

1.34

基本性质

Name	*Identity*
幂等律 (Idempotent laws)	$A \cup A = A, \qquad A \cap A = A$
结合律 (Associative laws)	$(A \cup B) \cup C = A \cup (B \cup C)$, $(A \cap B) \cap C = A \cap (B \cap C)$
交换律 (Commutative laws)	$A \cup B = B \cup A, \qquad A \cap B = B \cap A$
分配律 (Distributive laws)	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
同一律 (Identity laws)	$A \cup \varnothing = A, \qquad A \cap U = A$
零律 (Domination laws)	$A \cup U = U, \qquad A \cap \varnothing = \varnothing$
双补律 (Complement laws)	$A \cup \overline{A} = U, \qquad A \cap \overline{A} = \varnothing$
德・摩根律 (De Morgan's laws)	$\overline{A \cup B} = \overline{A} \cap \overline{B}$, $\overline{A \cap B} = \overline{A} \cup \overline{B}$
吸收律 (Absorption laws)	$A \cup (A \cap B) = A, \qquad A \cap (A \cup B) = A$
对合律 (Complementation law)	$\overline{(\overline{A})} = A$

1.35

Example 14. 确定下列各式:

1. $\varnothing \cap \{\varnothing\}$,
2. $\{\varnothing\} \cap \{\varnothing\}$,
3. $\{\varnothing, \{\varnothing\}\} - \varnothing$,
4. $\{\varnothing, \{\varnothing\}\} - \{\varnothing\}$,
5. $\{\varnothing, \{\varnothing\}\} - \{\{\varnothing\}\}$.

1. $\varnothing \cap \{\varnothing\} = \varnothing$,
2. $\{\varnothing\} \cap \{\varnothing\} = \{\varnothing\}$,
3. $\{\varnothing, \{\varnothing\}\} - \varnothing = \{\varnothing, \{\varnothing\}\}$,
4. $\{\varnothing, \{\varnothing\}\} - \{\varnothing\} = \{\{\varnothing\}\}$,
5. $\{\varnothing, \{\varnothing\}\} - \{\{\varnothing\}\} = \{\varnothing\}$.

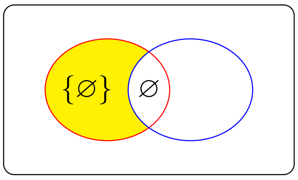


Figure 7: $\{\varnothing, \{\varnothing\}\} - \{\varnothing\}$

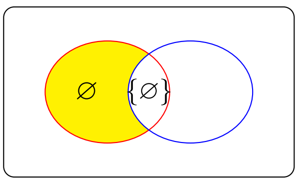


Figure 8: $\{\varnothing, \{\varnothing\}\} - \{\{\varnothing\}\}$

1.36

4 幂集

幂集

Definition 15 (幂集)**.** 给定集合 A, 以 A 的全体子集为元素构成的集合, 称为 A 的幂集 (power set). 记为 $\mathscr{P}(A)$ (或 2^A). 即

$$\mathscr{P}(A) = \{X \mid X \subseteq A\}. \tag{7}$$

Example 16. $A = \{1, 2, 3\}$, 将 A 的子集分类:

- 0 元子集, 也就是空集, 只有一个: $\varnothing$;
- 1 元子集, 即单元集: $\{1\}$, $\{2\}$, $\{3\}$;
- 2 元子集: $\{1, 2\}$, $\{1, 3\}$, $\{2, 3\}$;
- 3 元子集: $\{1, 2, 3\}$, 即 A 自身.

则 A 的幂集为 $\mathscr{P}(A) = \big\{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\big\}$. 1.37

幂集

Theorem 17. *设 A 为一有限集合, 且 $\operatorname{card}(A) = n$, 那么 $\operatorname{card}\big(\mathscr{P}(A)\big) = 2^n$. 或记为*

$$|\mathscr{P}(A)| = 2^{|A|}.$$

证: 注意到 A 的 0 元子集有 C_n^0 个, A 的 1 元子集有 C_n^1 个, $\cdots$, A 的 k 元子集有 C_n^k 个.

A 的全部子集构成了幂集 $\mathscr{P}(A)$, 所以

$$\begin{aligned} \operatorname{card}\big(\mathscr{P}(A)\big) &= C_n^0 + C_n^1 + \cdots + C_n^k + \cdots + C_n^n \\ &= (1+1)^n \\ &= 2^n. \end{aligned}$$

□ 1.38

幂集

Example 18. 确定下列集合的幂集:

1. $A = \big\{a, \{a\}\big\}$;
2. $\mathscr{P}(\varnothing)$;
3. $\mathscr{P}\big(\mathscr{P}(\varnothing)\big)$.

解: ① $\mathscr{P}(A) = \Big\{\varnothing, \{a\}, \{\{a\}\}, \{a, \{a\}\}\Big\}$.

② 因为 $\mathscr{P}(\varnothing) = \{\varnothing\}$, 所以

$$\mathscr{P}\big(\mathscr{P}(\varnothing)\big) = \{\varnothing, \{\varnothing\}\}.$$

③ $\mathscr{P}\Big(\mathscr{P}\big(\mathscr{P}(\varnothing)\big)\Big) = \Big\{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\Big\}$.

(☞ 注意检验 $\operatorname{card}\big(\mathscr{P}(A)\big) = 2^n$.) 1.39

5 序偶与笛卡儿积

序偶

Definition 19 (序偶)**.** 两个元素 x, y 构成的有序二元组 $\langle x, y\rangle$, 叫序偶 (ordered pairs) 或有序对. 通常把 $\langle x, y\rangle$ 定义为

$$\langle x, y\rangle \triangleq \{\{x\}, \{x, y\}\}.$$

称 x 为 $\langle x, y\rangle$ 的第一元素 (或第一分量、坐标), 称 y 为第二元素 (或第二分量、坐标).

☞ 在集合中 $\{a, b\} = \{b, a\}$, 它们是无序偶; 但对于序偶 $\langle a, b\rangle \neq \langle b, a\rangle$. 1.40

序偶

Definition 20 (序偶的相等)**.** 对任意序偶 $\langle a, b\rangle$, $\langle c, d\rangle$,

$$\langle a, b\rangle = \langle c, d\rangle, \quad \text{当且仅当 } a = c, b = d.$$

1.41

三元序组 (三元组)

Definition 21 (三元序组)**.** 三元序组是一个序偶, 其第一个元素本身也是一个序偶, 可形式化表示为

$$\big\langle\langle x, y\rangle, z\big\rangle \tag{8}$$

约定三元序组可以记作: $\langle x, y, z\rangle$.

☞

$$\big\langle\langle x, y\rangle, z\big\rangle \neq \big\langle x, \langle y, z\rangle\big\rangle.$$

因为 $\big\langle x, \langle y, z\rangle\big\rangle$ 不是三元序组. 1.42

n 元序组 (ordered n-tuples)

Definition 22 (n 元序组)**.** 递归地定义 n 元序组 $\langle a_1, \cdots, a_n\rangle$:

$$\begin{aligned}
\langle a_1, a_2\rangle &\triangleq \big\{\{a_1\}, \{a_1, a_2\}\big\} \\
\langle a_1, a_2, a_3\rangle &\triangleq \big\langle\langle a_1, a_2\rangle, a_3\big\rangle \\
&\cdots \\
\langle a_1, \cdots, a_n\rangle &\triangleq \big\langle\langle a_1, \cdots, a_{n-1}\rangle, a_n\big\rangle
\end{aligned}$$

第 i 个元素 x_i 称作 n 元序组的第 i 个坐标.

☞ 注意: n 元序组是一个二元组, 其中第一个分量是 $n-1$ 元序组. 1.43

n 元序组

Theorem 23. 两个 n 元序组相等

$$\begin{aligned} &\langle a_1, a_2, \cdots, a_n\rangle = \langle b_1, b_2, \cdots, b_n\rangle \\ \Leftrightarrow\ &(a_1 = b_1) \wedge (a_2 = b_2) \wedge \cdots \wedge (a_n = b_n). \end{aligned}$$

1.44

笛卡尔积 (Cartesian product)

Definition 24 (笛卡尔积)**.** 对任意集合 $A_1, A_2, \cdots, A_n$,

1. $A_1 \times A_2$ 称为集合 A_1, A_2 的笛卡尔积或直积, 定义为 $A_1 \times A_2 = \big\{\langle u, v\rangle \mid u \in A_1 \wedge v \in A_2\big\}$.
2. 递归地定义 $A_1 \times A_2 \times \cdots \times A_n$: $A_1 \times A_2 \times \cdots \times A_n = (A_1 \times A_2 \times \cdots \times A_{n-1}) \times A_n$.
3. $A \times A \times \cdots \times A$ 简记为 A^n.

例如, $A = \{1, 2\}$, $B = \{\alpha, \beta, \gamma\}$, 则

$$A \times B = \big\{\langle 1,\alpha\rangle, \langle 1,\beta\rangle, \langle 1,\gamma\rangle, \langle 2,\alpha\rangle, \langle 2,\beta\rangle, \langle 2,\gamma\rangle\big\}.$$

☞ 若 $A = \varnothing$ 或 $B = \varnothing$, 则

$$A \times B = \varnothing.$$

常见的笛卡尔集:

- 二维平面 $\mathbb{R} \times \mathbb{R}$,
- n 维实数空间 $\mathbb{R}^n$ 等.

1.45

笛卡尔积 (Cartesian product)

The adjective *Cartesian* refers to the French mathematician and philosopher René Descartes (who used the name *Renatus Cartesius* in Latin).

René Descartes (1596 – 1650) has been dubbed the “Father of Modern Philosophy”. Descartes’ influence in mathematics is equally apparent; the Cartesian coordinate system was named after him. He is credited as the father of analytical geometry, the bridge between algebra and geometry, crucial to the discovery of infinitesimal calculus and analysis.

He is perhaps best known for the philosophical statement “Cogito ergo sum” (French: *Je pense, donc je suis*; English: *I think, therefore I am*; or *I am thinking, therefore I exist* or *I do think, therefore I do exist*; Chinese: 我思故我在). 1.46

笛卡尔积 (Cartesian product)

Example 25. 设 $A = \{\text{Ace, King, Queen, Jack}, 10, 9, 8, 7, 6, 5, 4, 3, 2\}$, $B = \{\spadesuit, \heartsuit, \clubsuit, \diamondsuit\}$.
则笛卡尔集 $A \times B$ 是

$$\begin{aligned}
\{ &\langle \text{Ace}, \spadesuit\rangle, \langle \text{King}, \spadesuit\rangle, \langle \text{Queen}, \spadesuit\rangle, \cdots, \langle 3, \spadesuit\rangle, \langle 2, \spadesuit\rangle, \\
&\langle \text{Ace}, \heartsuit\rangle, \langle \text{King}, \heartsuit\rangle, \langle \text{Queen}, \heartsuit\rangle, \cdots, \langle 3, \heartsuit\rangle, \langle 2, \heartsuit\rangle, \\
&\langle \text{Ace}, \clubsuit\rangle, \langle \text{King}, \clubsuit\rangle, \langle \text{Queen}, \clubsuit\rangle, \cdots, \langle 3, \clubsuit\rangle, \langle 2, \clubsuit\rangle, \\
&\langle \text{Ace}, \diamondsuit\rangle, \langle \text{King}, \diamondsuit\rangle, \langle \text{Queen}, \diamondsuit\rangle, \cdots, \langle 3, \diamondsuit\rangle, \langle 2, \diamondsuit\rangle, \}.
\end{aligned}$$

1.47

笛卡尔积不满足交换律

- $A \times B \neq B \times A$, 当 $A \neq \varnothing \wedge B \neq \varnothing \wedge A \neq B$ 时.

事实上, 因为

$$A \times B = \big\{\langle a, b\rangle \;\big|\; a \in A \wedge b \in B\big\}, \tag{9}$$
$$B \times A = \big\{\langle b, a\rangle \;\big|\; b \in B \wedge a \in A\big\}. \tag{10}$$

而序偶 $\langle a, b\rangle \neq \langle b, a\rangle$, 当 $a \neq b$ 时.

Example 26. 例如 $A = \{1, 2\}$, $B = \{\alpha, \beta\}$, 则

$$\begin{aligned}
A \times B &= \big\{\langle 1, \alpha\rangle, \langle 1, \beta\rangle, \langle 2, \alpha\rangle, \langle 2, \beta\rangle\big\}, \\
B \times A &= \big\{\langle \alpha, 1\rangle, \langle \beta, 1\rangle, \langle \alpha, 2\rangle, \langle \beta, 2\rangle\big\}.
\end{aligned}$$

显然 $A \times B \neq B \times A$.

1.48

笛卡尔积不满足结合律

- $(A \times B) \times C \neq A \times (B \times C)$, 当 $A \neq \varnothing \wedge B \neq \varnothing \wedge C \neq \varnothing$ 时

事实上, 因为

$$\begin{aligned}
(A \times B) \times C &= \Big\{\big\langle\langle a, b\rangle, c\big\rangle \;\big|\; \langle a, b\rangle \in A \times B \wedge c \in C\Big\} \qquad (11)\\
&= \Big\{\langle a, b, c\rangle \;\big|\; a \in A \wedge b \in B \wedge c \in C\Big\}, \\
A \times (B \times C) &= \Big\{\big\langle a, \langle b, c\rangle\big\rangle \;\big|\; a \in A \wedge \langle b, c\rangle \in B \times C\Big\}. \qquad (12)
\end{aligned}$$

而 $\big\langle a, \langle b, c\rangle\big\rangle$ 不是三元组, 所以

$$(A \times B) \times C \neq A \times (B \times C).$$

1.49

笛卡儿积的性质

Theorem 27. *设 A, B, C 为任意集合, $*$ 表示 $\cup, \cap$ 或 $-$ 运算, 那么有如下结论:*

1. *笛卡尔积对于并、交、差运算可左分配. 即:*

$$A \times (B * C) = (A \times B) * (A \times C). \tag{13}$$

2. *笛卡尔积对于并、交、差运算可右分配. 即:*

$$(B * C) \times A = (B \times A) * (C \times A). \tag{14}$$

比如我们来证明

$$(B \cap C) \times A = (B \times A) \cap (C \times A), \tag{15}$$

$$(A - B) \times C = (A \times C) - (B \times C). \tag{16}$$

1.50

Example 28. 证明 $(B \cap C) \times A = (B \times A) \cap (C \times A)$.

证: 在集合 $(B \cap C) \times A$ 中任取 $\langle x, y \rangle$, 那么

$$\begin{aligned}
& \langle x, y \rangle \in (B \cap C) \times A \\
\Leftrightarrow\ & x \in (B \cap C) \wedge y \in A \\
\Leftrightarrow\ & (x \in B \wedge x \in C) \wedge y \in A \\
\Leftrightarrow\ & x \in B \wedge y \in A \wedge x \in C \wedge y \in A \\
\Leftrightarrow\ & (x \in B \wedge y \in A) \wedge (x \in C \wedge y \in A) \\
\Leftrightarrow\ & \langle x, y \rangle \in (B \times A) \wedge \langle x, y \rangle \in (C \times A) \\
\Leftrightarrow\ & \langle x, y \rangle \in (B \times A) \cap (C \times A).
\end{aligned}$$

所以 $(B \cap C) \times A = (B \times A) \cap (C \times A)$. □ 1.51

Example 29. 证明 $(A - B) \times C = (A \times C) - (B \times C)$.

证: 在集合 $(A \times C) - (B \times C)$ 中任取 $\langle x, y \rangle$, 那么

$$\begin{aligned}
& \langle x, y \rangle \in (A \times C) - (B \times C) \\
\Leftrightarrow\ & \langle x, y \rangle \in A \times C \wedge \neg \langle x, y \rangle \in B \times C \\
\Leftrightarrow\ & (x \in A \wedge y \in C) \wedge \neg (x \in B \wedge y \in C) \\
\Leftrightarrow\ & (x \in A \wedge y \in C) \wedge (\neg x \in B \vee \neg y \in C) \\
\Leftrightarrow\ & (x \in A \wedge y \in C) \wedge (x \notin B \vee y \notin C) \\
\Leftrightarrow\ & (x \in A \wedge y \in C \wedge x \notin B) \vee (x \in A \wedge y \in C \wedge y \notin C) \\
\Leftrightarrow\ & (x \in A \wedge y \in C \wedge x \notin B) \vee \mathbf{F} \\
\Leftrightarrow\ & x \in A \wedge x \notin B \wedge y \in C \\
\Leftrightarrow\ & x \in (A - B) \wedge y \in C \\
\Leftrightarrow\ & \langle x, y \rangle \in (A - B) \times C.
\end{aligned}$$

所以 $(A - B) \times C = (A \times C) - (B \times C)$. □ 1.52

Theorem 30. 若 $C \neq \varnothing$, 则

$$A \subseteq B \Leftrightarrow A \times C \subseteq B \times C \Leftrightarrow C \times A \subseteq C \times B.$$

证: 若 $A \subseteq B$, 任取 $\langle x, y\rangle \in A \times C$, 有

$$\begin{aligned}\langle x, y\rangle \in A \times C &\Rightarrow x \in A \wedge y \in C \\ &\Rightarrow x \in B \wedge y \in C \Rightarrow \langle x, y\rangle \in B \times C.\end{aligned}$$

因此, $A \times C \subseteq B \times C$.

反之, 若 $A \times C \subseteq B \times C$. 取 $y \in C$, 则有

$$\begin{aligned}x \in A &\Rightarrow x \in A \wedge y \in C \Leftrightarrow \langle x, y\rangle \in A \times C \\ &\Rightarrow \langle x, y\rangle \in B \times C \Leftrightarrow x \in B \wedge y \in C \\ &\Leftrightarrow x \in B.\end{aligned}$$

因此, $A \subseteq B$. 类似可证: $A \subseteq B \Leftrightarrow (C \times A \subseteq C \times B)$. □ 1.53

Theorem 31. 设 A, B, C, D 为四个非空集合, 则

$$A \times B \subseteq C \times D \Leftrightarrow A \subseteq C, B \subseteq D.$$

证: 若 $A \times B \subseteq C \times D$, 对任意 $x \in A$ 和 $y \in B$ 有

$$\begin{aligned}(x \in A) \wedge (y \in B) &\Rightarrow \langle x, y\rangle \in A \times B \\ &\Rightarrow \langle x, y\rangle \in C \times D \\ &\Rightarrow (x \in C) \wedge (y \in D).\end{aligned}$$

即 $A \subseteq C$ 且 $B \subseteq D$.

反之, 若 $A \subseteq C$ 且 $B \subseteq D$, 对任意 $x \in A$ 和 $y \in B$ 有

$$\begin{aligned}\langle x, y\rangle \in A \times B &\Leftrightarrow (x \in A) \wedge (y \in B) \\ &\Rightarrow (x \in C) \wedge (y \in D) \\ &\Leftrightarrow \langle x, y\rangle \in C \times D.\end{aligned}$$

因此 $A \times B \subseteq C \times D$. □ 1.54

练习

习题

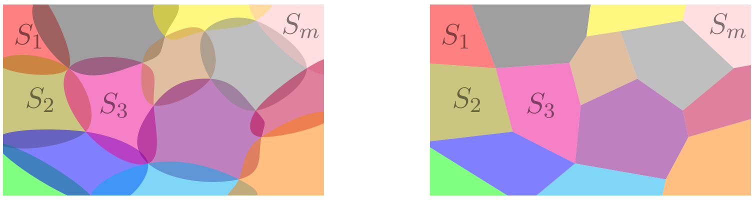
设 $A = \{0, 1\}$, $B = \{1, 2\}$, 确定下面的集合.

1. $A \times \{1\} \times B$;
2. $A^2 \times B$.

解: ① $A \times \{1\} \times B = \{\langle 0, 1, 1\rangle, \langle 0, 1, 2\rangle, \langle 1, 1, 1\rangle, \langle 1, 1, 2\rangle\}$.

② $A^2 \times B = A \times A \times B = \{\langle 0, 0, 1\rangle, \langle 0, 1, 1\rangle, \langle 0, 0, 2\rangle, \langle 0, 1, 2\rangle, \langle 1, 0, 1\rangle, \langle 1, 0, 2\rangle, \langle 1, 1, 1\rangle, \langle 1, 1, 2\rangle\}$.

1.55



(a) 集合的覆盖　　(b) 集合的划分

练习

习题

设 $A = \{a, b\}$, 构成集合 $\mathscr{P}(A) \times A$.

解: 由 $\mathscr{P}(A) = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$, 所以

$$\begin{aligned}\mathscr{P}(A) \times A = \{&\langle\varnothing, a\rangle, \langle\varnothing, b\rangle, \langle\{a\}, a\rangle, \langle\{a\}, b\rangle, \\ &\langle\{b\}, a\rangle, \langle\{b\}, b\rangle, \langle\{a, b\}, a\rangle, \langle\{a, b\}, b\rangle\}.\end{aligned}$$

1.56

6 集合的覆盖与划分

集合的划分与覆盖

Definition 32 (集合的覆盖 & 划分)**.** 设 A 为非空集合, $S = \{S_1, S_2, \cdots, S_m\}$, 其中 $S_i \subseteq A$, $S_i \neq \varnothing$, $i = 1, 2, \cdots, m$.

- 若 $\bigcup\limits_{i=1}^{m} S_i = A$, 则集合 S 称作集合 A 的覆盖 (covering).
- 若 $\bigcup\limits_{i=1}^{m} S_i = A$, 且 $S_i \cap S_j = \varnothing$ $(i \neq j)$, 则称 S 是 A 的划分 (partition).

1.57

Definition 33 (交叉划分)**.** 若 $\{A_1, A_2, \cdots, A_r\}$ 与 $\{B_1, B_2, \cdots, B_s\}$ 是同一个集合 A 的两种划分, 则其中所有 $A_i \cap B_j \neq \varnothing$ 组成的集合, 称为是原来两种划分的交叉划分.

Example 34. 给定一个玩具积木的集合

$$A = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8\}.$$

按颜色划分: $\{\{x_1, x_3, x_4, x_7\}, \{x_2, x_5, x_6, x_8\}\}$.

按形状划分: $\{\{x_1, x_2, x_5, x_6\}, \{x_3, x_4, x_7, x_8\}\}$.

同时考虑颜色和形状, 得交叉划分:

$$\{\{x_1\}, \{x_2, x_5, x_6\}, \{x_3, x_4, x_7\}, \{x_8\}.\}.$$

1.58

Theorem 35. 设 $\{A_1, A_2, \cdots, A_r\}$ 与 $\{B_1, B_2, \cdots, B_s\}$ 是同一个集合 X 的两种划分, 则其交叉划分亦是原集合的一种划分.

证: 设 $\{A_1, A_2, \cdots, A_r\}$ 与 $\{B_1, B_2, \cdots, B_s\}$ 交叉划分为

$$T = \left\{A_i \cap B_j \,\middle|\, 1 \leqslant i \leqslant r,\, 1 \leqslant j \leqslant s\right\}.$$

首先, 在 T 中任取两个元素 $A_i \cap B_h$, $A_j \cap B_k$, 证明它们的交集为空:

1. 当 $i \neq j$, 且 $h = k$ 时,
$$(A_i \cap B_h) \cap (A_j \cap B_k) = (A_i \cap A_j) \cap (B_h \cap B_k) = \varnothing \cap B_h = \varnothing.$$
2. 当 $i \neq j$, 且 $h \neq k$ 时,
$$(A_i \cap B_h) \cap (A_j \cap B_k) = (A_i \cap A_j) \cap (B_h \cap B_k) = \varnothing \cap \varnothing = \varnothing.$$
3. 当 $i = j$, 且 $h \neq k$ 时, 与 ① 类同.

其次, 证明 T 中所有元素的并集等于 X:

$$\begin{aligned}
\bigcup_{i=1}^{r} \bigcup_{h=1}^{s} (A_i \cap B_h) &= \bigcup_{i=1}^{r} (A_i \cap B_1) \cup (A_i \cap B_2) \cup \cdots \cup (A_i \cap B_s) \\
&= \bigcup_{i=1}^{r} \left(A_i \cap (B_1 \cup B_2 \cup \cdots \cup B_s)\right) \\
&= \bigcup_{i=1}^{r} (A_i \cap X) \\
&= \left(\bigcup_{i=1}^{r} A_i\right) \cap X \\
&= X \cap X = X.
\end{aligned}$$

□ 1.59

Definition 36 (划分的加细)**.** 给定 X 的任意两个划分 $\{A_1, A_2, \cdots, A_r\}$ 和 $\{B_1, B_2, \cdots, B_s\}$, 若对于每一个 A_j 均有 B_k 使 $A_j \subseteq B_k$, 则 $\{A_1, A_2, \cdots, A_r\}$ 称为是 $\{B_1, B_2, \cdots, B_s\}$ 的加细.

Theorem 37. 任何两种划分的交叉划分, 都是原来各划分的一种加细.

证: 设 $\{A_1, A_2, \cdots, A_r\}$ 与 $\{B_1, B_2, \cdots, B_s\}$ 交叉划分为

$$T = \left\{A_i \cap B_j \,\middle|\, 1 \leqslant i \leqslant r,\, 1 \leqslant j \leqslant s\right\}.$$

则对 T 中任意元素 $A_i \cap B_j$, 均有

$$A_i \cap B_j \subseteq A_i, \quad A_i \cap B_j \subseteq B_j.$$

故 T 是原划分的加细. □ 1.60

Example 38. 给定一个玩具积木的集合

$$A=\{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8\}.$$

按颜色划分: $\{\{x_1, x_3, x_4, x_7\}, \{x_2, x_5, x_6, x_8\}\}.$

按形状划分: $\{\{x_1, x_2, x_5, x_6\}, \{x_3, x_4, x_7, x_8\}\}.$

同时考虑颜色和形状, 得交叉划分:

$$\{\{x_1\}, \{x_2, x_5, x_6\}, \{x_3, x_4, x_7\}, \{x_8\}\}.$$

从这个例子容易看到:

1. 交叉划分也是原集合的一种划分;
2. 交叉划分是原来各划分的加细. 1.61

7 基本计数原理

鸽巢原理 (pigeonhole principle)

Figure 9: 将 10 只鸽子放进 9 个鸽笼, 那么一定有一个鸽笼放进了至少 2 只鸽子.

Theorem 39 (鸽巢原理)**.** *若有 n 个笼子和 $n+1$ 只鸽子, 所有的鸽子都被关在鸽笼里, 那么至少有一个笼子里有至少 2 只鸽子.* 1.62

鸽巢原理 (pigeonhole principle)

鸽巢原理 (或鸽笼原理), 又名抽屉原理, 最早是由狄利克雷在 1834 年给出的, 常常称为狄利克雷抽屉原理 (Dirichlet's drawer principle), 或简称狄利克雷原理.

鸽巢原理的一个一般表述:

Theorem 40 (鸽巢原理)**.** *将 n 个物体放入 m 个盒子里, 若 $n>m$, 则至少有一个盒子里有两个或两个以上的物体.* 1.63

G. Lejeune Dirichlet

G. Lejeune Dirichlet (1805-1859) was a German mathematician credited with the modern formal definition of a function. He was born into a French family living near Cologne, Germany. He studied at the University of Paris and held positions at the University of Breslau and the University of Berlin. In 1855 he was chosen to succeed Gauss at the University of Göttingen.

Dirichlet made many important discoveries in number theory, including the theorem that there are infinitely many primes in arithmetical progressions $an+b$ when a and b are relatively prime. He proved the $n = 5$ case of Fermat's Last Theorem, that there are no nontrivial solutions in integers to $x^5 + y^5 = z^5$. Dirichlet also made many contributions to analysis. 1.64

鸽巢原理举例

Example 41. 武汉市至少有两个人头发数一样多.

证: 人的头发数一般在 15 万根左右, 可以假定没有人有超过 100 万根头发, 但武汉人口数量为约 700 万.

如果我们让每一个鸽巢对应一个头发数字, 鸽子对应于人, 那就变成了有大于 100 万只鸽子要进到至多 100 万个巢中.

所以. 可以得到 "武汉市至少有两个人头发数一样多" 的结论. 1.65

鸽巢原理举例

Example 42. 有 n 个人互相握手 (不重复握手), 必有两人握手次数相同.

证: 鸽巢对应于握手次数, 鸽子对应于人, 每个人都可以握 $[0, n-1]$ 次.

但 0 和 $n-1$ 不能同时存在. 因为如果一个人不和任何人握手, 那就不会存在一个和所有其他人都握过手的人.

所以鸽巢是 $n-1$ 个, 但有 n 个人 (n 只鸽子), 故得证. 1.66

鸽巢原理推广

Theorem 43 (The Generalized Pigeonhole Principle)**.** *把 n 个物体放入 m 个盒子里, 则至少有一个盒子里至少有 $\lceil n/m \rceil$ 个物体.*

☞ 其中 $\lceil x \rceil$ 称为 取顶函数 (ceiling function).

x	$\lfloor x \rfloor$	$\lceil x \rceil$
2.4	2	3
-2.4	-3	-2
-2	-2	-2

与之相对的是 取整函数 (floor function), 记为 $\lfloor x \rfloor$ 或者 $[x]$.

$$\begin{aligned}\lceil x \rceil &= \min\{n \in \mathbb{Z} \mid n \geqslant x\},\\ \lfloor x \rfloor &= \max\{m \in \mathbb{Z} \mid m \leqslant x\}.\end{aligned}$$

例如,

证: 反证法. 设所有的盒子里的物体数都不超过 $\lceil n/m \rceil - 1$, 则物体总数至多为

$$\begin{aligned}& m\left(\left\lceil \frac{n}{m} \right\rceil - 1\right)\\ <\ & m\left(\left(\frac{n}{m} + 1\right) - 1\right) \qquad (\text{因为 } \lceil \tfrac{n}{m} \rceil < \tfrac{n}{m} + 1)\\ =\ & n.\end{aligned}$$

这与物体总数为 n 矛盾. □

Example 44. 在 100 个人中, 至少有 $\lceil 100/12 \rceil = 9$ 个人的生日, 是在同一个月份. 1.67

鸽巢原理推广

Example 45. 在任意 6 个人中, 或者有 3 个人相互认识, 或者有 3 个人相互陌生.

证: 记这 6 人分别为 A, B, C, D, E, F. 以 A 为例, 把余下 5 人分入 2 个盒子, 其中一个盒子表示和 A 认识, 另一个表示和 A 陌生.

则至少有一个盒子里有至少 $\lceil 5/2 \rceil = 3$ 个人, 即以下情形必居其一:

1. 至少有 3 个人和 A 认识;
2. 至少有 3 个人和 A 陌生.

考虑情形 1. 不妨设 B, C, D 都和 A 认识, 则有以下两种可能:

(i) 若在 B, C, D 这 3 人中, 至少有 2 人相互认识, 则此 6 人中已经有 3 人相互认识.

(ii) 否则 B, C, D 这 3 人相互陌生, 亦有命题成立.

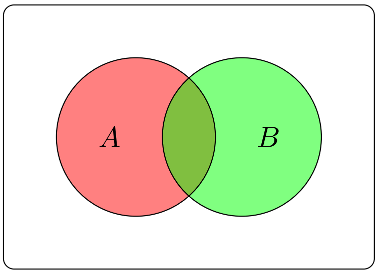
对情形 2 有类似的推理. □ 1.68

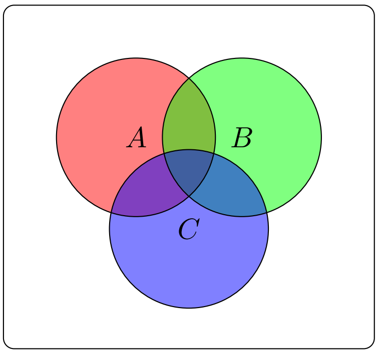
容斥原理 (Inclusion–exclusion principle)

Theorem 46 (容斥原理)**.** *设 A, B 均为有限集, 则有*

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

1.69





容斥原理

Theorem 47 (容斥原理)**.** 设 A, B, C 均为有限集, 则有

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

1.70

容斥原理

一般形式:

Theorem 48. 设 A_1, A_2, $\ldots$, A_n $(n \geqslant 2)$ 均为有限集, 则有

$$\begin{aligned}\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{1 \leqslant i < j \leqslant n} |A_i \cap A_j| + \sum_{1 \leqslant i < j < k \leqslant n} |A_i \cap A_j \cap A_k| \\ - \cdots + (-1)^{n-1} |A_1 \cap A_2 \cap \cdots \cap A_n|\end{aligned}$$

1.71

概率论中的容斥原理

☞容斥原理在概率论中也有相同的形式:

$$\mathbb{P}(A_1 \cup A_2) = \mathbb{P}(A_1) + \mathbb{P}(A_2) - \mathbb{P}(A_1 \cap A_2),$$

当 $n = 3$ 时, 公式为:

$$\begin{aligned}\mathbb{P}(A_1 \cup A_2 \cup A_3) = \mathbb{P}(A_1) + \mathbb{P}(A_2) + \mathbb{P}(A_3) \\ - \mathbb{P}(A_1 \cap A_2) - \mathbb{P}(A_1 \cap A_3) - \mathbb{P}(A_2 \cap A_3) \\ + \mathbb{P}(A_1 \cap A_2 \cap A_3).\end{aligned}$$

一般地:

$$\mathbb{P}\Big(\bigcup_{i=1}^{n} A_i\Big) = \sum_{i=1}^{n}\mathbb{P}(A_i) - \sum_{i,j\,:\,i<j}\mathbb{P}(A_i\cap A_j) + \sum_{i,j,k\,:\,i<j<k}\mathbb{P}(A_i\cap A_j\cap A_k) - \cdots + (-1)^{n-1}\,\mathbb{P}\Big(\bigcap_{i=1}^{n} A_i\Big).$$

1.72

Example 49. A computer company receives 350 applications from computer graduates for a job planning a line of new Web servers. Suppose that 220 of these people majored in computer science, 147 majored in business, and 51 majored both in computer science and in business. How many of these applicants majored neither in computer science nor in business?

Solution: Let A_1 be the set of students who majored in computer science and A_2 the set of students who majored in business. Then $A_1 \cup A_2$ is the set of students who majored in computer science or business (or both), and $A_1 \cap A_2$ is the set of students who majored both in computer science and in business. By the principle of inclusion-exclusion, the number of students who majored either in computer science or in business (or both) equals

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2| = 220 + 147 - 51 = 316.$$

We conclude that $350 - 316 = 34$ of the applicants majored neither in computer science nor in business. □ 1.73

Example 50. A total of 1232 students have taken a course in Spanish, 879 have taken a course in French, and 114 have taken a course in Russian. Further, 103 have taken courses in both Spanish and French, 23 have taken courses in both Spanish and Russian, and 14 have taken courses in both French and Russian. If 2092 students have taken at least one of Spanish, French, and Russian, how many students have taken a course in all three languages?

Solution: Let S be the set of students who have taken a course in Spanish, F the set of students who have taken a course in French, and R the set of students who have taken a course in Russian. Then

$$|S| = 1232, \quad |F| = 879, \quad |R| = 114,$$
$$|S\cap F| = 103, \quad |S\cap R| = 23, \quad |F\cap R| = 14,$$

and

$$|S\cup F\cup R| = 2092.$$

When we insert these quantities into the equation

$$|S\cup F\cup R| = |S| + |F| + |R| - |S\cap F| - |S\cap R| - |F\cap R| + |S\cap F\cap R|,$$

we obtain

$$2092 = 1232 + 879 + 114 - 103 - 23 - 14 + |S \cap F \cap R|.$$

We now solve for $|S \cap F \cap R|$. We find that $|S \cap F \cap R| = 7$. Therefore, there are seven students who have taken courses in all three languages. $\square$ 1.74

Chapter 2

二元关系

Discrete Mathematics

January 3, 2015

黄正华, 数学与统计学院, 武汉大学

2.1

1 关系的定义及表示

关系的概念

事物之间存在着各式各样的关系. 例如,

- 人际关系 (老乡关系, 同学关系, 朋友关系等);
- 数之间的大于关系, 整除关系等.

Example 1. 三名学生 A, B, C 选修 α, β, γ, δ 四门课, 设 A 选 α 和 δ, B 选 γ, C 选 α 和 β, 那么, 学生选课的对应关系可记为:

$$R = \big\{\langle A, \alpha\rangle, \langle A, \delta\rangle, \langle B, \gamma\rangle, \langle C, \alpha\rangle, \langle C, \beta\rangle\big\} \tag{1}$$

集合 R 反映了学生集合 $S = \{A, B, C\}$ 与课程集合 $T = \{\alpha, \beta, \gamma, \delta\}$ 之间的某种关系.

☞ 集合 R 是直积 $A \times B$ 的子集. 2.2

关系的概念

Definition 2 (关系 (relation))**.** 令 A 和 B 是任意两个集合, 直积 $A \times B$ 的子集 R 称为 A 到 B 的二元关系.

1. R 中的任一序偶 $\langle x, y\rangle$ 可记为 $\langle x, y\rangle \in R$, 或 xRy.
2. 不在 R 中的序偶 $\langle x, y\rangle$ 记为 $\langle x, y\rangle \notin R$, 或 $x \not R y$.

特别地, 若 $R \subseteq A \times A$, 称 R 为 A 上的二元关系.

几个特殊的二元关系

1. $\varnothing \subseteq A \times B$, 称 $\varnothing$ 为 A 到 B 的空关系.
2. $A \times B \subseteq A \times B$, 称 $A \times B$ 为 A 到 B 的全关系或全域关系.
3. $I_A = \big\{\langle x, x\rangle \big| x \in A\big\}$, 称为 A 上的恒等关系.

2.3

集合 A 上的二元关系

集合 A 上的二元关系, 很常见.

Example 3. 设 $A = \{1, 2, 3, 4\}$, 求 A 上的 "小于等于" 关系 L_A.

解:

$$\begin{aligned} L_A &= \big\{\langle x, y\rangle \bigm| x \in A \wedge y \in A \wedge x \leqslant y\big\} \\ &= \big\{\langle 1,1\rangle, \langle 1,2\rangle, \langle 1,3\rangle, \langle 1,4\rangle, \langle 2,2\rangle, \langle 2,3\rangle, \langle 2,4\rangle, \langle 3,3\rangle, \langle 3,4\rangle, \langle 4,4\rangle\big\}. \end{aligned}$$

Example 4. Let A be the set $\{1, 2, 3, 4\}$. Which ordered pairs are in the relation $R = \{\langle a, b\rangle \mid a \text{ divides } b\}$?

Solution: Because $\langle a, b\rangle$ is in R if and only if a and b are positive integers not exceeding 4 such that a divides b, we see that

$$R = \big\{\langle 1,1\rangle, \langle 1,2\rangle, \langle 1,3\rangle, \langle 1,4\rangle, \langle 2,2\rangle, \langle 2,4\rangle, \langle 3,3\rangle, \langle 4,4\rangle\big\}. \quad \square$$

2.4

Definition 5 (定义域, 值域)**.** 设 R 为一个二元关系,

- 由 $\langle x, y\rangle \in R$ 的所有 x 组成的集合 $\operatorname{dom} R$ 称为 R 的定义域 (domain), 即

$$\operatorname{dom} R = \big\{x \bigm| (\exists y)(\langle x, y\rangle \in R)\big\} \tag{2}$$

- 由 $\langle x, y\rangle \in R$ 的所有 y 组成的集合 $\operatorname{ran} R$ 称为 R 的值域 (range), 即

$$\operatorname{ran} R = \big\{y \bigm| (\exists x)(\langle x, y\rangle \in R)\big\} \tag{3}$$

显然地,

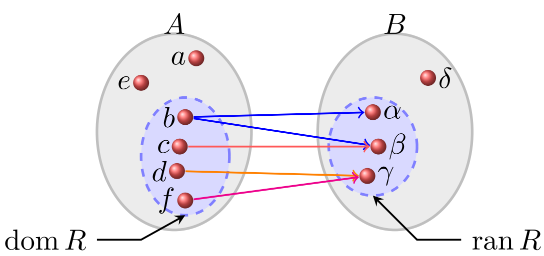
- $\operatorname{dom} R \subseteq A$,
- $\operatorname{ran} R \subseteq B$,
- $R \subseteq \operatorname{dom} R \times \operatorname{ran} R \subseteq A \times B$.

2.5

Example 6. 设 $A = \{a, b, c, d, e, f\}$, $B = \{\alpha, \beta, \gamma, \delta\}$. 记关系 R 为

$$R = \{\langle b, \alpha\rangle, \langle b, \beta\rangle, \langle c, \beta\rangle, \langle d, \gamma\rangle, \langle f, \gamma\rangle\}$$

那么如图所示:



$$\operatorname{dom} R = \{b, c, d, f\}, \qquad \operatorname{ran} R = \{\alpha, \beta, \gamma\}.$$

☞ 强调: 关系 R 是直积 $A \times B$ 的子集. R 也是 $\operatorname{dom} R \times \operatorname{ran} R$ 的子集.

2.6

Example 7. 在一个有 n 个元素的集合 A 上, 可以有多少种不同的关系?

解: 集合 A 上的二元关系的个数与 $A\times A$ 的子集个数相同. 若 $\mathrm{card}(A)=n$, 则

$$\mathrm{card}(A\times A)=n^2, \tag{4}$$

所以, $A\times A$ 的子集个数就有 2^{n^2} 个, 即 A 上不同的二元关系有 2^{n^2} 个. □

例如, 在集合 $\{a,b,c,d\}$ 上有 $2^{4^2}=2^{16}=65536$ 个不同的二元关系.

在集合 $\{a,b,c,d,e\}$ 上有 $2^{5^2}=2^{25}=33554432$ 个不同的二元关系.

在集合 $\{a,b,c,d,e,f\}$ 上有 $2^{6^2}=2^{36}=68719476736$ 个不同的二元关系.

☞ 若 $\mathrm{card}(A)=m$, $\mathrm{card}(B)=n$. 问 A 到 B 可以有多少个不同的二元关系?(答案: 2^{mn} 个.) 2.7

二元关系的表示

一个二元关系可用 ① 集合(序偶的集合), ② 关系矩阵, ③ 关系图表示. 下面来看关系矩阵和关系图.

关系矩阵

给定两个有限集合 $X=\{x_1,\,x_2,\,\cdots,x_m\}$, $Y=\{y_1,\,y_2,\,\cdots,\,y_n\}$. 设 R 为从 X 到 Y 的一个二元关系. 则对应于关系 R 的关系矩阵为矩阵 $M_R=(r_{ij})_{m\times n}$, 其中

$$r_{ij}=\begin{cases}1, & \langle x_i,\,y_j\rangle\in R,\\ 0, & \langle x_i,\,y_j\rangle\notin R.\end{cases}\qquad (i=1,\,2,\,\cdots,\,m;\ j=1,\,2,\,\cdots,\,n.)$$

2.8

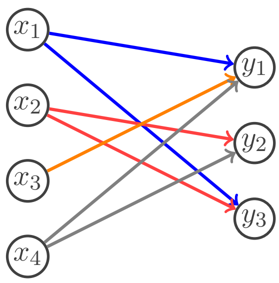
Example 8. 设集合 $X=\{x_1,\,x_2,\,x_3,\,x_4\}$, $Y=\{y_1,\,y_2,\,y_3\}$. X 到 Y 上的关系 R 为

$$R=\big\{\langle x_1,\,y_1\rangle,\,\langle x_1,\,y_3\rangle,\,\langle x_2,\,y_2\rangle,\,\langle x_2,\,y_3\rangle,\,\langle x_3,\,y_1\rangle,\,\langle x_4,\,y_1\rangle,\,\langle x_4,\,y_2\rangle\big\}.$$

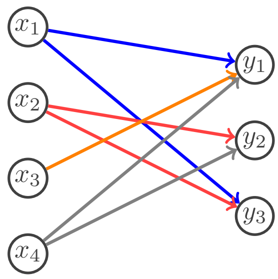
试写出关系矩阵 M_R.

解: 关系矩阵为 也可以用图形来表示关系 R: 2.9

$$M_R=\begin{array}{c} \\ x_1\\ x_2\\ x_3\\ x_4\end{array}\begin{array}{c}\begin{array}{ccc} y_1 & y_2 & y_3\end{array}\\ \begin{pmatrix}1&0&1\\0&1&1\\1&0&0\\1&1&0\end{pmatrix}\end{array}.$$



关系图



- 关系图中表示元素的小圆圈, 称为结点 (node);
- 表示元素间具有 R 关系的有向线段或有向弧, 称为有向边 (direct edge);
- 起点和终点重合的有向边, 称为环 (loop) 或自回路.
- 关系 R 的关系图记为 G_R.

2.10

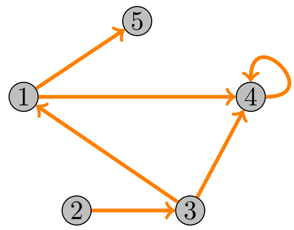
关系图

Example 9. 设 $A = \{1, 2, 3, 4, 5\}$, 在 A 上的二元关系 R 定义为:

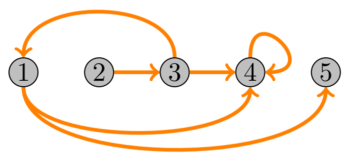
$$R = \big\{\langle 1, 5\rangle, \langle 1, 4\rangle, \langle 2, 3\rangle, \langle 3, 1\rangle, \langle 3, 4\rangle, \langle 4, 4\rangle\big\}$$

画出 R 的关系图.

解: 因为 R 是 A 上的关系, 故只需画出 A 中的每个元素即可.



或者



2.11

习题

对 $P = \{0,1,2,3,4,5,6\}$ 上的二元关系, $R = \big\{\langle x, y\rangle \bigm| x < y \vee x \text{ 是质数}\big\}$, 写出关系矩阵.

解: 因为 P 中的元素为质数的有: 2, 3, 5. 又注意到联接词为 $\vee$, 得关系矩阵为:

$$M_R = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

2.12

习题

对 $P = \{0,1,2,3,4,5,6\}$ 上的二元关系, $R = \{\langle x, y\rangle \mid x < y \vee x \text{ 是质数}\}$, 写出关系矩阵.

若设 $R_1 = \{\langle x, y\rangle \mid x < y\}$, $R_2 = \{\langle x, y\rangle \mid x \text{ 是质数}\}$. 则

$$M_{R_1} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad M_{R_2} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

从中不难发现 $M_{R_1} \vee M_{R_2} = M_R$ 的规律:

矩阵对应位置的元素作 “$\vee$” 运算: $0 \vee 0 = 0$, $0 \vee 1 = 1 \vee 0 = 1$, $1 \vee 1 = 1$.

☞ 若关系为 $R = \{\langle x, y\rangle \mid x < y \wedge x \text{ 是质数}\}$ 呢?

2.13

2 关系的运算

关系的运算

Theorem 10. *若 Z 和 S 是从集合 X 到集合 Y 的两个关系, 则 Z, S 的并、交、补、差, 仍是 X 到 Y 的关系.*

证明思路: 根据 “关系是直积的子集” 可证.

证: 因为 $Z \subseteq X \times Y$, $S \subseteq X \times Y$, 故

$$Z \cup S \subseteq X \times Y, \tag{5}$$

$$Z \cap S \subseteq X \times Y, \tag{6}$$

$$\sim S = (X \times Y - S) \subseteq X \times Y, \tag{7}$$

$$Z - S = Z \cap \sim S \subseteq X \times Y. \tag{8}$$

□

2.14

Example 11. Let R_1 be the “less than” relation on the set of real numbers and let R_2 be the “greater than” relation on the set of real numbers, that is, $R_1 = \{\langle x, y\rangle \mid x < y\}$ and $R_2 = \{\langle x, y\rangle \mid x > y\}$. What are $R_1 \cup R_2$, $R_1 \cap R_2$, $R_1 - R_2$, $R_2 - R_1$, and $R_1 \oplus R_2$?

Solution: We note that $\langle x, y\rangle \in R_1 \cup R_2$ if and only if $\langle x, y\rangle \in R_1$ or $\langle x, y\rangle \in R_2$. Hence, $\langle x, y\rangle \in R_1 \cup R_2$ if and only if $x < y$ or $x > y$. Because the condition $x < y$ or $x > y$ is the same as the condition $x \neq y$, it follows that $R_1 \cup R_2 = \{\langle x, y\rangle \mid x \neq y\}$. In other words, the union of the "less than" relation and the "greater than" relation is the "not equals" relation.

Next, note that it is impossible for a pair $\langle x, y\rangle$ to belong to both R_1 and R_2 because it is impossible for $x < y$ and $x > y$. It follows that $R_1 \cap R_2 = \varnothing$.

We also see that $R_1 - R_2 = R_1$, $R_2 - R_1 = R_2$, and $R_1 \oplus R_2 = R_1 \cup R_2 - R_1 \cap R_2 = \{\langle x, y\rangle \mid x \neq y\}$. □ 2.15

逆关系

Definition 12 (逆关系)**.** 设 R 是从 A 到 B 的二元关系, 关系 R 的逆 (R 的逆关系) 记为 R^{c} 或 $\widetilde{R}$, 定义如下:

$$R^{\mathrm{c}} = \big\{\langle b,\, a\rangle \mid \langle a,\, b\rangle \in R\big\}.$$

Example 13. 例如, 对关系 $R = \{\langle 1,\, a\rangle, \langle 2,\, b\rangle, \langle 3,\, c\rangle\}$, 其逆关系为

$$R^{\mathrm{c}} = \big\{\langle a,\, 1\rangle, \langle b,\, 2\rangle, \langle c,\, 3\rangle\big\}.$$

☞ 注意一个常用的表达:

$$\langle a,\, b\rangle \in R \Leftrightarrow \langle b,\, a\rangle \in R^{\mathrm{c}}.$$

2.16

- 恒等关系的逆, 是恒等关系;
- 空关系的逆, 是空关系;
- 全域关系的逆, 是全域关系.

2.17

逆关系的求法

1. 列举法: 把 R 中每一序偶的元素顺序互换, 可得到逆关系 R^{c} 的所有元素.
2. 关系矩阵: 将矩阵 M_R 转置, 得 R^{c} 的关系矩阵 $M_{R^{\mathrm{c}}}$. 即

$$M_{R^{\mathrm{c}}} = M_R^{\mathrm{T}}.$$

3. 关系图: 在 R 的关系图中, 颠倒每条弧 (有向边) 的箭头方向, 得到 R^{c} 的关系图.

2.18

逆关系的性质

Theorem 14. 设 R, R_1, R_2 是 A 到 B 的二元关系, 则

1. $(R^{\mathrm{c}})^{\mathrm{c}} = R$;

2. $(R_1 \cup R_2)^{\mathrm{c}} = R_1^{\mathrm{c}} \cup R_2^{\mathrm{c}}$;

3. $(R_1 \cap R_2)^c = R_1^c \cap R_2^c$;

4. $(R_1 - R_2)^c = R_1^c - R_2^c$;

5. $(\overline{R})^c = \overline{R^c}$, (这里 $\overline{R} = A \times B - R$).

☞ 其中 $\overline{R} = A \times B - R$ 是 $A \times B$ 中不属于 R 的序偶所成的集合, 称为 R 的关系补 (complement of a relation). 或说, $\overline{R}$ 是 R 关于 $A \times B$ 的补集. 有常用关系式:

$$\langle a, b\rangle \in R \Leftrightarrow \langle a, b\rangle \notin \overline{R}, \quad \text{或} \quad \langle a, b\rangle \notin R \Leftrightarrow \langle a, b\rangle \in \overline{R}.$$

下面来证明 ⑤ . 2.19

Example 15. 设 R 是 A 到 B 的二元关系, 则 $(\overline{R})^c = \overline{R^c}$.

比如,

$$M_R = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix},$$

$$M_{\overline{R}} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \quad M_{(\overline{R})^c} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix};$$

$$M_{R^c} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad M_{\overline{R^c}} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}.$$

证: 注意到关系式

$$\langle a, b\rangle \in R \Leftrightarrow \langle b, a\rangle \in R^c,$$
$$\langle a, b\rangle \notin R \Leftrightarrow \langle a, b\rangle \in \overline{R}.$$

对任意的 $\langle a, b\rangle \in (\overline{R})^c$, 有

$$\begin{aligned} \langle a, b\rangle \in (\overline{R})^c &\Leftrightarrow \langle b, a\rangle \in \overline{R} \\ &\Leftrightarrow \langle b, a\rangle \notin R \\ &\Leftrightarrow \langle a, b\rangle \notin R^c \\ &\Leftrightarrow \langle a, b\rangle \in \overline{R^c}. \end{aligned}$$

所以

$$(\overline{R})^c = \overline{R^c}.$$

2.20

复合关系

Definition 16 (复合关系)**.** 设 R_1 是从 A 到 B 的关系, R_2 是从 B 到 C 的关系, 则 R_1 与 R_2 的复合关系为从 A 到 C 的关系, 记为 $R_1 \circ R_2$, 定义为

$$R_1 \circ R_2 = \{\langle a, c\rangle \mid a \in A \wedge c \in C \wedge (\exists b)(b \in B \wedge \langle a, b\rangle \in R_1 \wedge \langle b, c\rangle \in R_2)\}.$$

其中 $\circ$ 表示关系的合成运算. 2.21

关系合成运算的性质

- 设 R 是从 A 到 B 的关系, I_A, I_B 分别是 A, B 上的恒等关系, 则 $I_A \circ R = R \circ I_B = R$;
- 如果关系 R_1 的值域与 R_2 的定义域的交集为空集, 则合成关系 $R_1 \circ R_2$ 是空关系;
- 关系的合成满足结合律:
  设 R_1, R_2, R_3 分别是从 A 到 B, B 到 C, C 到 D 的关系, 则

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

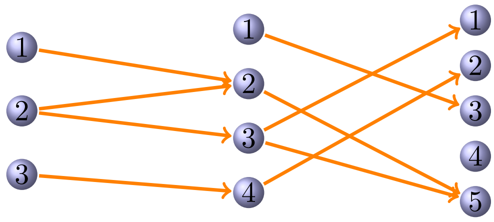
2.22

Example 17. 设关系 $R = \{\langle 1,2\rangle, \langle 2,3\rangle, \langle 3,4\rangle, \langle 2,2\rangle\}$, $S = \{\langle 4,2\rangle, \langle 2,5\rangle, \langle 3,1\rangle, \langle 1,3\rangle, \langle 3,5\rangle\}$. 求复合关系 $R \circ S$, $S \circ R$, $R \circ R$, $R \circ R \circ R$.

解:

$$\begin{aligned}
R \circ S &= \{\langle 1,5\rangle, \langle 2,1\rangle, \langle 3,2\rangle, \langle 2,5\rangle\}, \\
S \circ R &= \{\langle 4,2\rangle, \langle 4,3\rangle, \langle 3,2\rangle, \langle 1,4\rangle\}, \\
R \circ R &= \{\langle 1,2\rangle, \langle 1,3\rangle, \langle 2,2\rangle, \langle 2,3\rangle, \langle 2,4\rangle\}, \\
R \circ R \circ R = (R \circ R) \circ R &= \{\langle 1,2\rangle, \langle 1,3\rangle, \langle 1,4\rangle, \langle 2,2\rangle, \langle 2,3\rangle, \langle 2,4\rangle\}.
\end{aligned}$$

用关系图来反映关系的复合, 更为直观、可靠. 比如 $R \circ S$:



2.23

用关系矩阵求复合关系

设 $A \circ B = C$, 关系矩阵为 $M_A = (a_{ij})_{n\times n}$, $M_B = (b_{ij})_{n\times n}$, $M_C = (c_{ij})_{n\times n}$. 则

$$c_{ij} = \bigvee_{k=1}^{n} (a_{ik} \wedge b_{kj}). \tag{9}$$

上式中 $\vee$ 代表逻辑加, 满足 $0 \vee 0 = 0$, $0 \vee 1 = 1$, $1 \vee 0 = 1$, $1 \vee 1 = 1$. $\wedge$ 代表逻辑乘, 满足 $0 \wedge 0 = 0$, $0 \wedge 1 = 0$, $1 \wedge 0 = 0$, $1 \wedge 1 = 1$.

如何理解?

- 公式 (9) 的理解: 要想 "i" 与 "j" 建立关系, 则至少存在一个 "k", 使 "i" 与 "k" 有关系, 且 "k" 与 "j" 有关系. (公式 (9) 中的 $\bigvee$ 和 $\wedge$ 分别体现的就是 "至少存在一个" 和 "且".)

- 逻辑加和逻辑乘的理解: 关系矩阵中的元素 1 和 0, 表达的是关系的 “有” 和 “无”, 即 **T** 和 **F**. (把运算规则中的 1 和 0 分别换成 **T** 和 **F**, 易见等式成立.) 2.24

Example 18. 设 $A = \{1, 2, 3, 4\}$, $B = \{2, 3, 4\}$, $C = \{1, 2, 3\}$, R_1 是从 A 到 B 的关系, R_2 是从 B 到 C 的关系:

$$R_1 = \big\{\langle x, y\rangle \bigm| x + y = 6\big\} = \big\{\langle 2, 4\rangle, \langle 3, 3\rangle, \langle 4, 2\rangle\big\}, \tag{10}$$

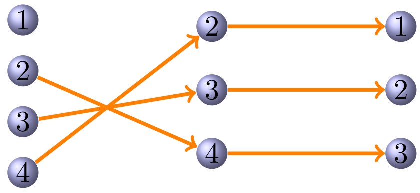
$$R_2 = \big\{\langle y, z\rangle \bigm| y - z = 1\big\} = \big\{\langle 2, 1\rangle, \langle 3, 2\rangle, \langle 4, 3\rangle\big\}. \tag{11}$$

分别用列举法、图示法、关系矩阵法表示关系的合成 $R_1 \circ R_2$.

解: ① (列举法)

$$R_1 \circ R_2 = \big\{\langle 2, 3\rangle,\ \langle 3, 2\rangle,\ \langle 4, 1\rangle\big\}.$$

② (图示法)



解: ③ (关系矩阵法)

$$M_{R_1 \circ R_2} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array}\!\!\begin{array}{c} \begin{array}{ccc} 2 & 3 & 4 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \end{array} \circ \begin{array}{c} \\ 2 \\ 3 \\ 4 \end{array}\!\!\begin{array}{c} \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{array} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array}\!\!\begin{array}{c} \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \end{array}.$$

2.25

关系的幂

Definition 19 (关系的幂)**.** 设 R 是集合 A 上的二元关系, $n \in \mathbb{N}$ 为任一自然数, 则 R 的 n 次幂记为 R^n, 定义为:

1. R^0 为 A 上的恒等关系,

$$R^0 = \big\{\langle x,\ x\rangle \bigm| x \in A\big\}.$$

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

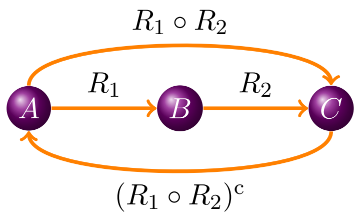
2.26

Theorem 20. 设 R_1 是从 A 到 B 的关系, R_2 是从 B 到 C 的关系, 则

$$(R_1 \circ R_2)^{\mathrm{c}} = R_2^{\mathrm{c}} \circ R_1^{\mathrm{c}} \tag{12}$$

证:

$$\begin{aligned}
&\langle c,\, a\rangle \in (R_1 \circ R_2)^{\mathrm{c}} \\
\Leftrightarrow\ &\langle a,\, c\rangle \in R_1 \circ R_2 \\
\Leftrightarrow\ &(\exists b)\big(b \in B \wedge \langle a,\, b\rangle \in R_1 \wedge \langle b,\, c\rangle \in R_2\big) \\
\Leftrightarrow\ &(\exists b)\big(b \in B \wedge \langle b,\, a\rangle \in R_1^{\mathrm{c}} \wedge \langle c,\, b\rangle \in R_2^{\mathrm{c}}\big) \\
\Leftrightarrow\ &\langle c,\, a\rangle \in R_2^{\mathrm{c}} \circ R_1^{\mathrm{c}}.
\end{aligned}$$



2.27

3 关系的基本类型

关系的基本类型

以下设 R 是集合 A 上的一个二元关系, 讨论 R 的几个基本类型:

1. 自反;
2. 对称;
3. 传递;
4. 反自反;
5. 反对称. 2.28

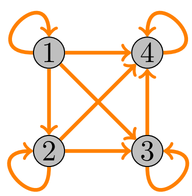
自反 (reflexive)

Definition 21. 若对 A 中的每一 x, 有 xRx, 则称 R 是自反的;

$$\begin{aligned}
R\text{ 是自反的} &\Leftrightarrow (\forall x)(x \in A \to xRx) \\
&\Leftrightarrow M_R\text{ 主对角元全为 }1 \\
&\Leftrightarrow G_R\text{ 每一结点有自回路.}
\end{aligned}$$

例如, 设 $A = \{1, 2, 3, 4\}$, R 为 “$\leqslant$”. 则

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



☞ “$=$”, “$\leqslant$”

都是具有自反性关系的例子. 又如平面上三角形的全等关系是自反的. 2.29

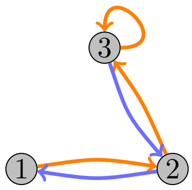
对称 (symmetric)

Definition 22. 若对每一 $x, y \in A$, xRy 蕴含着 yRx, 则称 R 是对称的;

$$\begin{aligned} R \text{ 是对称的} &\Leftrightarrow (\forall x)(\forall y)(x \in A \wedge y \in A \wedge xRy \to yRx) \\ &\Leftrightarrow M_R \text{ 是对称矩阵} \\ &\Leftrightarrow G_R \text{ 有向边成对出现 (若有 } a \text{ 到 } b \text{ 的弧, 则必有 } b \text{ 到 } a \text{ 的弧).} \end{aligned}$$

例如,

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



相等、等势[1]7>

如果在两个集合 A, B 之间存在一个一一对应, 则称 A, B 是等势的.、同余等都是具有对称性的关系的例子. 2.30

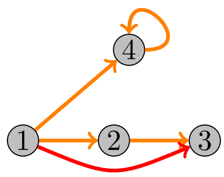
传递 (transitive)

Definition 23. 对每一 $x, y, z \in A$, 若 xRy, yRz 蕴含着 xRz, 则称 R 是传递的.

$$\begin{aligned} R \text{ 是传递的} &\Leftrightarrow (\forall x)(\forall y)(\forall z)(x \in A \wedge y \in A \wedge z \in A \wedge xRy \wedge yRz \to xRz) \\ &\Leftrightarrow G_R \text{ 中若从 } a \text{ 到 } b \text{ 有一条路径, 则从 } a \text{ 到 } b \text{ 有一条弧.} \end{aligned}$$

例如,

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



☞ “$=$”, “$<$”, “$\leqslant$”, “$\subset$”, “$\subseteq$”, 整除, 等势, 同余等都是具有传递性关系的例子. 2.31

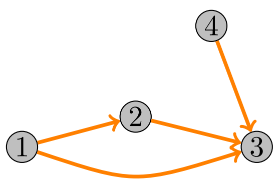
反自反 (irreflexive)

Definition 24. 对 A 中的每一 x, 若 $x \not R x$, 则称 R 是反自反的;

$$\begin{aligned} R \text{ 是反自反的} &\Leftrightarrow (\forall x)(x \in A \to x \not R x) \\ &\Leftrightarrow M_R \text{ 主对角元全为 } 0 \\ &\Leftrightarrow G_R \text{ 每一结点无自回路.} \end{aligned}$$

例如,

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



☞ “$<$”, “$>$” 是具有反自反性质的两个重要关系. 2.32

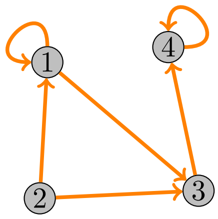
[1] <

反自反 (irreflexive)

注意: 一个不是自反的关系, 不一定就是反自反的.

例如,

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



- 关系矩阵的主对角元素不是全为 1, 所以不是 “自反” 的;
- 关系矩阵的主对角元素不是全为 0, 所以不是 “反自反” 的.

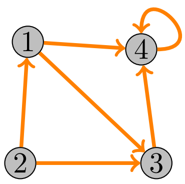
☞ “自反” 的否定不是 “反自反”. 2.33

反对称 (antisymmetric)

Definition 25. 对每一 x, $y \in A$, 若 xRy, yRx 蕴含着 $x = y$, 则称 R 是反对称的;

$$\begin{aligned} R \text{ 是反对称的} &\Leftrightarrow (\forall x)(\forall y)(x \in A \land y \in A \land xRy \land yRx \to x = y) \\ &\Leftrightarrow (\forall i)(\forall j)\big(i, j \in \{1, 2, \dots, n\} \land i \neq j \land (a_{ij} = 1) \to (a_{ji} = 0)\big); \\ &\Leftrightarrow G_R \text{ 中若有 } a \text{ 到 } b \text{ 的弧, 则必没有 } b \text{ 到 } a \text{ 的弧;} \end{aligned}$$

例如, $M_R = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ 2.34

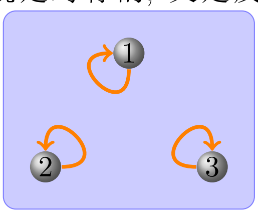


反对称 (antisymmetric)

例如, 实数集合中 “$\leqslant$” 是反对称的; 集合的 “$\subseteq$” 关系是反对称的.

注意: 可能有某种关系, 既是对称的, 又是反对称的. 例如, [1em]

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



☞ “对称” 的否定不是 “反对称”.

(不具备对称性的关系称为非对称关系 (asymmetric). 例如 “$<$” 和 “$\subset$”.) 2.35

Theorem 26. 设 R 为 A 上的关系, 证明

1. R 在 A 上自反, 当且仅当 $I_A \subseteq R$.
2. R 在 A 上反自反, 当且仅当 $R \cap I_A = \varnothing$.
3. R 在 A 上传递, 当且仅当 $R \circ R \subseteq R$.

证: ① 必要性. 任取 $\langle x, x\rangle \in I_A$, 如果 R 在 A 上自反, 必有

$$\langle x, x\rangle \in I_A \Rightarrow x \in A \Rightarrow \langle x, x\rangle \in R,$$

从而 $I_A \subseteq R$.

充分性. 当 $I_A \subseteq R$ 时, 任取 $x \in A$, 有

$$x \in A \Rightarrow \langle x, x\rangle \in I_A \Rightarrow \langle x, x\rangle \in R,$$

因此 R 在 A 上是自反的.

☞ 直观地看, R 是自反的, 则 M_R 的主对角线元素全为 1. 所以 $I_A \subseteq R$.

② $\boxed{R \text{ 是反自反的 } \Leftrightarrow (\forall x)(x \in A \to \langle x, x\rangle \notin R) \Leftrightarrow M_R \text{ 主对角元全为 } 0.}$

必要性 (反证法). 设 R 在 A 上反自反, 但 $R \cap I_A \neq \varnothing$, 必存在 $\langle x, y\rangle \in R \cap I_A$, 则

$$\begin{aligned}\langle x, y\rangle \in R \cap I_A &\Rightarrow \langle x, y\rangle \in R \wedge \langle x, y\rangle \in I_A\\ &\Rightarrow \langle x, y\rangle \in R \wedge (x = y)\\ &\Rightarrow \langle x, x\rangle \in R.\end{aligned}$$

这与 R 是反自反的相矛盾.

充分性. 设 $R \cap I_A = \varnothing$, 任取 $x \in A$, 则

$$x \in A \Rightarrow \langle x, x\rangle \in I_A \Rightarrow \langle x, x\rangle \notin R.$$

所以 R 在 A 上是反自反的.

③ (必要性) 设 R 在 A 上是传递的. 任取 $\langle x, y\rangle \in R \circ R$, 有

$$\begin{aligned}\langle x, y\rangle \in R \circ R &\Rightarrow (\exists t)(\langle x, t\rangle \in R \wedge \langle t, y\rangle \in R)\\ &\Rightarrow \langle x, y\rangle \in R. \qquad \text{(由传递性)}\end{aligned}$$

所以 $R \circ R \subseteq R$.

(充分性) 设 $R \circ R \subseteq R$. 任取 $\langle x, y\rangle \in R$, $\langle y, z\rangle \in R$, 则

$$\begin{aligned}\langle x, y\rangle \in R \wedge \langle y, z\rangle \in R &\Rightarrow \langle x, z\rangle \in R \circ R\\ &\Rightarrow \langle x, z\rangle \in R.\end{aligned}$$

所以 R 是传递的. □

2.36

Theorem 27. 设 R 是集合 A 上的二元关系, 则

1. R 是对称的, 当且仅当 $R^c = R$.
2. R 是反对称的, 当且仅当 $R \cap R^c \subseteq I_A$.

只证 ② .
例如,

$$M_R = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \qquad M_{R^c} = M_R^{\mathrm{T}} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix},$$

$$M_{R \cap R^c} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

证: 设 R 是反对称的. 假定 $\langle a, b\rangle \in R \cap R^c$, 则

$$\begin{aligned} &\langle a, b\rangle \in R \wedge \langle a, b\rangle \in R^c \\ \Rightarrow &\langle a, b\rangle \in R \wedge \langle b, a\rangle \in R \end{aligned}$$

而 R 是反对称的, 故 $a = b$. 所以

$$\langle a, b\rangle = \langle b, a\rangle \in I_A.$$

即 $R \cap R^c \subseteq I_A$. 证: 反之, 设 $R \cap R^c \subseteq I_A$. 对 $\langle a, b\rangle \in R$ 和 $\langle b, a\rangle \in R$, 则

$$\begin{aligned} &\langle a, b\rangle \in R \wedge \langle b, a\rangle \in R \\ \Leftrightarrow &\langle a, b\rangle \in R \wedge \langle a, b\rangle \in R^c \\ \Leftrightarrow &\langle a, b\rangle \in R \cap R^c \\ \Rightarrow &\langle a, b\rangle \in I_A \\ \Rightarrow &a = b. \end{aligned}$$

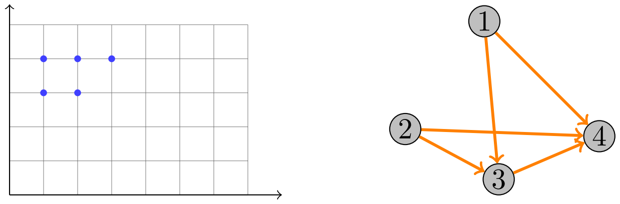
故 R 是反对称的. □

2.37

设 R 是集合 A 上的二元关系, 则

1. R 是对称的, 当且仅当 $R^c = R$.
2. R 是反对称的, 当且仅当 $R \cap R^c \subseteq I_A$.

也可以用关系矩阵直观地加以解释.
记 $M_R = (u_{ij})$, $M_{R^c} = (v_{ij})$, $M_{R \circ R^c} = (w_{ij})$.
由 $M_{R^c} = M_R^{\mathrm{T}}$, 知 $v_{ij} = u_{ji}$.
又 R 是反对称的, 知 $u_{ij} \neq u_{ji}$ $(i \neq j)$.



(a) 坐标图　　(b) 关系图

则 $i \neq j$ 时,

$$
\begin{aligned}
w_{ij} &= u_{ij} \wedge v_{ij} \\
&= u_{ij} \wedge u_{ji} \\
&= 0.
\end{aligned}
$$

故 $R \cap R^{\mathrm{c}} \subseteq I_A$.　　例如,

$$
M_R = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix},
$$

$$
M_{R^{\mathrm{c}}} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix},
$$

$$
M_{R \cap R^{\mathrm{c}}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.
$$

2.38

给定 $A = \{1, 2, 3, 4\}$, 考虑 A 上的关系 R, 若

$$
R = \big\{\langle 1, 3\rangle, \langle 1, 4\rangle, \langle 2, 3\rangle, \langle 2, 4\rangle, \langle 3, 4\rangle\big\},
$$

1. 在 $A \times A$ 的坐标图中标出 R, 并绘出它的关系图;
2. R 是 i) 自反的, ii) 对称的, iii) 传递的, iv) 反对称的吗?

解: ① 见下图.

② R 是传递的和反对称的; 不是自反或对称的. $\square$ 2.39

4　关系的闭包

关系的闭包运算

问题: 关系可以具有自反、对称、传递等性质. 但是, 不是所有的关系都具有这些性质.

解决: 可以通过对给定的关系添加新的元素 (序偶), 使所得的新关系具有这些性质.

要求: 与此同时, 又不添加过多的元素, 做到恰到好处, 即添加的元素要最少.

对给定的关系, 用扩充一些序偶的办法, 得到具有某些性质的新关系, 这就是闭包运算. 2.40

关系的闭包运算

Definition 28. 设 R 是 A 上的二元关系, 关系 R' 是 R 的自反闭包 (对称闭包, 传递闭包), 如果

1. R' 是自反的 (对称的, 传递的);
2. $R \subseteq R'$;
3. 对任何自反的 (对称的, 传递的) 关系 R'', 如果 $R \subseteq R''$, 那么 $R' \subseteq R''$.

R 的自反、对称和传递闭包分别记为

$$r(R), \quad s(R), \quad t(R).$$

☞ R 的自反 (对称、传递) 闭包, 是包含 R 的最小自反 (对称、传递) 关系. 2.41

闭包的性质

从闭包的定义知, R 的自反闭包 (对称闭包, 传递闭包) 是包含 R 且具有自反 (对称, 传递) 性质的 “最小” 关系.

如果 R 已经具备这些性质, 那么 R 自身就是具备这些性质且包含 R 的 “最小” 关系.

于是, 有下面的定理:

Theorem 29. *设 R 是集合 A 上的关系, 那么*

1. *R 是自反的, 当且仅当 $r(R) = R$.*
2. *R 是对称的, 当且仅当 $s(R) = R$.*
3. *R 是传递的, 当且仅当 $t(R) = R$.*

下证 ② . 其他证明类似. 2.42

闭包的性质

Theorem

设 R 是集合 A 上的二元关系, 则 R 是对称的, 当且仅当 $s(R) = R$.

证: 设 R 是对称的. 则 R 满足对称闭包的定义:

1. R 是对称的;
2. $R \subseteq R$;
3. 对任何对称关系 R', 如果 $R \subseteq R'$, 那么 $R \subseteq R'$.

反之, 若 $s(R) = R$, 由对称闭包定义知 R 是对称的. □ 2.43

构造闭包的方法

设 R 是集合 A 上的二元关系, 则

1. 自反闭包 $r(R) = R \cup I_A$;
2. 对称闭包 $s(R) = R \cup R^c$;
3. 传递闭包 $t(R) = \bigcup_{i=1}^{\infty} R^i = R \cup R^2 \cup R^3 \cup \cdots (\triangleq R^+)$.

☞ 前两个用关系矩阵很容易解释. 下面作为三个定理来逐一证明. 2.44

Theorem 30. 设 R 是集合 A 上的二元关系, 则自反闭包 $r(R) = R \cup I_A$.

分析 注意结论: S 是集合 A 上的自反关系, 当且仅当 $I_A \subseteq S$. (或见 P.119 习题 (2).)

证: 设 $R' = R \cup I_A$. 下面验证 R' 满足 "自反闭包" 的定义:

1. "R' 是自反的": 因为 $I_A \subseteq R'$.
2. "$R \subseteq R'$": 由 $R' = R \cup I_A$.
3. "对任何自反关系 R'', 如果 $R \subseteq R''$, 那么 $R' \subseteq R''$":
   设 R'' 是自反的, 则 $I_A \subseteq R''$. 如果 $R \subseteq R''$, 则
   $$R' = R \cup I_A \subseteq R''.$$

综上得证

$$r(R) = R \cup I_A.$$

□ 2.45

Theorem 31. 设 R 是集合 A 上的二元关系, 则对称闭包 $s(R) = R \cup R^c$.

证: 设 $R' = R \cup R^c$. 下面验证 R' 满足 "对称闭包" 定义:

1. "R' 是对称的":
$$\begin{aligned}\langle x, y\rangle \in R' &\Leftrightarrow \langle x, y\rangle \in R \vee \langle x, y\rangle \in R^c \\ &\Leftrightarrow \langle y, x\rangle \in R^c \vee \langle y, x\rangle \in R \\ &\Leftrightarrow \langle y, x\rangle \in R'.\end{aligned}$$
2. "$R \subseteq R'$": 由 $R' = R \cup R^c$.
3. "对任何对称关系 R'', 如果 $R \subseteq R''$, 那么 $R' \subseteq R''$": 下证任意 $\langle x, y\rangle \in R'$, 有 $\langle x, y\rangle \in R''$:
$$\langle x, y\rangle \in R' \Rightarrow \langle x, y\rangle \in R \vee \langle x, y\rangle \in R^c,$$
   (i) $\langle x, y\rangle \in R \Rightarrow \langle x, y\rangle \in R''$ (由 $R \subseteq R''$);
   (ii) $\langle x, y\rangle \in R^c \Rightarrow \langle y, x\rangle \in R \subseteq R'' \Rightarrow \langle x, y\rangle \in R''$ (由 R'' 是对称的).

综上得证 $s(R) = R \cup R^c$. □ 2.46

Theorem 32. 设 R 是集合 A 上的二元关系, 则 $t(R)=\bigcup\limits_{i=1}^{\infty} R^i = R\cup R^2\cup R^3\cup \cdots (\triangleq R^+)$.

分析: $t(R)=\bigcup\limits_{i=1}^{\infty} R^i \Leftrightarrow \Big(\bigcup\limits_{i=1}^{\infty} R^i \subseteq t(R)\Big) \wedge \Big(t(R)\subseteq \bigcup\limits_{i=1}^{\infty} R^i\Big)$.

证: ① 先证 $\bigcup\limits_{i=1}^{\infty} R^i \subseteq t(R)$, 用归纳法.

1. 由传递闭包定义知 $R\subseteq t(R)$;
2. 假定 $n\geqslant 1$ 时, $R^n\subseteq t(R)$. 设 $\langle x,\, y\rangle\in R^{n+1}$.

$$
\begin{aligned}
R^{n+1}=R^n\circ R &\Leftrightarrow (\exists c)(c\in A\wedge\langle x,\, c\rangle\in R^n\wedge\langle c,\, y\rangle\in R)\\
&\Rightarrow (\exists c)\big(c\in A\wedge\langle x,\, c\rangle\in t(R)\wedge\langle c,\, y\rangle\in t(R)\big)\\
&\Rightarrow \langle x,\, y\rangle\in t(R)\\
&\Rightarrow R^{n+1}\subseteq t(R).
\end{aligned}
$$

所以 $\bigcup\limits_{i=1}^{\infty} R^i\subseteq t(R)$. ② 再证 $t(R)\subseteq\bigcup\limits_{i=1}^{\infty} R^i$. 由传递闭包 $t(R)$ 是包含 R 的最小传递关系, 往下只需要证明 $\bigcup\limits_{i=1}^{\infty} R^i$ 是传递的.

$$
\begin{aligned}
&\langle x,\, y\rangle\in\bigcup_{i=1}^{\infty} R^i\wedge\langle y,\, z\rangle\in\bigcup_{i=1}^{\infty} R^i\\
\Leftrightarrow\ &(\exists s)(\exists t)(s\in\mathbb{N}\wedge t\in\mathbb{N}\wedge\langle x,\, y\rangle\in R^s\wedge\langle y,\, z\rangle\in R^t)\\
\Leftrightarrow\ &\langle x,\, z\rangle\in R^s\circ R^t=R^{s+t}\\
\Rightarrow\ &\langle x,\, z\rangle\in\bigcup_{i=1}^{\infty} R^i.
\end{aligned}
$$

得 $\bigcup\limits_{i=1}^{\infty} R^i$ 是传递的. 由于包含 R 的传递关系都包含 $t(R)$, 故 $t(R)\subseteq\bigcup\limits_{i=1}^{\infty} R^i$. $\square$ 2.47

Example

设 $A=\{a,\, b,\, c\}$, R 是 A 上的二元关系, $R=\big\{\langle a,\, b\rangle,\, \langle b,\, c\rangle,\, \langle c,\, a\rangle\big\}$. 求 $r(R)$, $s(R)$, $t(R)$.

解: 自反闭包:

$$
\begin{aligned}
r(R)&=R\cup I_A\\
&=\big\{\langle a,\, b\rangle,\, \langle b,\, c\rangle,\, \langle c,\, a\rangle,\, \langle a,\, a\rangle,\, \langle b,\, b\rangle,\, \langle c,\, c\rangle\big\}.
\end{aligned}
$$

对称闭包:

$$
\begin{aligned}
s(R)&=R\cup R^c\\
&=\big\{\langle a,\, b\rangle,\, \langle b,\, c\rangle,\, \langle c,\, a\rangle,\, \langle b,\, a\rangle,\, \langle c,\, b\rangle,\, \langle a,\, c\rangle\big\}.
\end{aligned}
$$

下面求传递闭包 $t(R)$. 这里

$$M_R = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

2.48

Example

设 $A = \{a,\, b,\, c\}$, R 是 A 上的二元关系, $R = \big\{\langle a,\, b\rangle,\, \langle b,\, c\rangle,\, \langle c,\, a\rangle\big\}$. 求 $r(R)$, $s(R)$, $t(R)$.

$$M_{R^2} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \circ \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

$$M_{R^3} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \circ \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$M_{R^4} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \circ \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

注意到 $M_R = M_{R^4}$, 即 $R = R^4$. 2.49

Example

设 $A = \{a,\, b,\, c\}$, R 是 A 上的二元关系, $R = \big\{\langle a,\, b\rangle,\, \langle b,\, c\rangle,\, \langle c,\, a\rangle\big\}$. 求 $r(R)$, $s(R)$, $t(R)$.

由 $R = R^4$ 有:

$$\begin{aligned} R &= R^4 = \cdots = R^{3n+1}, \\ R^2 &= R^5 = \cdots = R^{3n+2}, \\ R^3 &= R^6 = \cdots = R^{3n+3}. \quad (n = 1,\, 2,\, 3,\, \cdots) \end{aligned}$$

故

$$\begin{aligned} t(R) &= \bigcup_{i=1}^{\infty} R^i = R \cup R^2 \cup R^3 \cup \cdots = R \cup R^2 \cup R^3 \\ &= \{\langle a,a\rangle, \langle b,b\rangle, \langle c,c\rangle, \langle a,b\rangle, \langle b,c\rangle, \langle c,a\rangle, \langle b,a\rangle, \langle c,b\rangle, \langle a,c\rangle\}. \end{aligned}$$

这里

$$M_{t(R)} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

2.50

Theorem 33. 设 R 是有限集合 X 上的二元关系, $\mathrm{card}(X)=n$, 则存在正整数 $k \leqslant n$, 使得

$$t(R)=R\cup R^2\cup\cdots\cup R^k.$$

证: 设有 $x, y \in X$. 记 $t(R)=R^+$.

$$\begin{aligned}
&\langle x, y\rangle \in R^+ = R\cup R^2\cup R^3\cup\cdots && (13)\\
\Rightarrow\ &(\exists R^p)\big(\langle x, y\rangle \in R^p\big) && (14)\\
\Leftrightarrow\ &(\exists x_{i_1})(\exists x_{i_2})\cdots(\exists x_{i_{p-1}})\big(xRx_{i_1}\wedge x_{i_1}Rx_{i_2}\wedge\cdots x_{i_{p-1}}Ry\big) && (15)
\end{aligned}$$

假设满足上述条件的最小 p 大于 n. 则在 $x_{i_1}, x_{i_2}, \cdots, x_{i_{p-1}}$ 当中必存在相同的元素. 即存在 $0\leqslant t<q\leqslant p$, 使 $x_{i_t}=x_{i_q}$. 则 x 到 y 的 "复合路径"

$$xRx_{i_1},\ x_{i_1}Rx_{i_2},\ \cdots,\ x_{i_{t-1}}Rx_{i_t},\ x_{i_t}Rx_{i_{t+1}},\ \cdots,\ x_{i_q}Rx_{i_{q+1}},\ \cdots,\ x_{i_{p-1}}Ry \qquad (16)$$

可简化为

$$xRx_{i_1},\ x_{i_1}Rx_{i_2},\ \cdots,\ x_{i_{t-1}}Rx_{i_t},\ x_{i_q}Rx_{i_{q+1}},\ \cdots,\ x_{i_{p-1}}Ry \qquad (17)$$

这与 p 是最小的假设矛盾, 故 $p>n$ 不成立. □ 2.51

Theorem

设 R 是有限集合 X 上的二元关系, $\mathrm{card}(X)=n$, 则存在正整数 $k\leqslant n$, 使得

$$t(R)=R\cup R^2\cup\cdots\cup R^k.$$

☞ 从本定理可以知道, 在 n 个元素的有限集上关系 R 的传递闭包可以改写为

$$t(R)=R\cup R^2\cup\cdots\cup R^n, \qquad (18)$$

而不必再使用

$$t(R)=\bigcup_{i=1}^{\infty}R^i=R\cup R^2\cup R^3\cup\cdots. \qquad (19)$$

2.52

利用关系矩阵求闭包

Theorem 34. 设关系 R, $r(R)$, $s(R)$, $t(R)$ 的关系矩阵分别为 M, M_r, M_s, M_t, 则

1. $M_r = M + I$;
2. $M_s = M + M^{\mathrm{T}}$;
3. $M_t = M + M^2 + M^3 + \cdots$;

2.53

Warshall 算法 (1962)

Warshall 提出了求 R^+ 的一个有效算法:[2]

Step 1 置新矩阵 $A := M$;

Step 2 置 $i := 1$;

Step 3 对所有 j, 如果 $A[j,\,i] = 1$, 则对 $k = 1,\,2,\,\cdots,\,n$,

$$A[j,\,k] := A[j,\,k] + A[i,\,k] \tag{20}$$

Step 4 $i := i + 1$;

Step 5 如果 $i \leqslant n$, 则转到 **Step 3**; 否则停止.

这里, $A[j,\,i]$ 表示矩阵中第 j 行, 第 i 列的元素. 加法是逻辑加. 2.54

如何理解?

Step 3 对所有 j, 如果 $A[j,\,i] = 1$, 则对 $k = 1,\,2,\,\cdots,\,n$,

$$A[j,\,k] := A[j,\,k] + A[i,\,k]$$

若 $A[j,\,i] = 1$, 即已有 x_j 到 x_i 的关系. 接下来的问题:

x_j 是否存在到 x_k 的关系呢?

1. 如果 x_j 到 x_k 已经存在关系, 则 $A[j,\,k] = 1$, 赋值 $A[j,\,k] := A[j,\,k]+A[i,\,k]$ 不会改变 $A[j,\,k]$ 的值.
2. 如果 x_j 到 x_k 没有关系, 由已有的 x_j 到 x_i 的关系, 现在看是否有 x_j 通过 x_i 再到 x_k 的 (复合) 关系.
    - 如果 $A[i,\,k] = 1$, 则 $A[j,\,k]$ 获得新值 1. 即通过关系的复合运算, 可以建立 x_j 到 x_k 的关系;
    - 而若 $A[i,\,k] = 0$, 则 $A[j,\,k]$ 仍为 0.

总之, 赋值 $A[j,\,k] := A[j,\,k] + A[i,\,k]$ 就是为了建立 x_j 到 x_k 的可能关系. 2.55

如何理解?

Step 3 对所有 j, 如果 $A[j,\,i] = 1$, 则对 $k = 1,\,2,\,\cdots,\,n$,

$$A[j,\,k] := A[j,\,k] + A[i,\,k]$$

若 $A[j,\,i] = 1$, 即已有 x_j 到 x_i 的关系. 接下来的问题:

x_j 是否存在到 x_k 的关系呢?

$$\begin{array}{cc}
 & \begin{array}{cccccc} & & & i & & \end{array} \\
\begin{array}{c} \\ i \\ \\ j \\ \\ \end{array} &
\begin{pmatrix}
\vdots & \vdots & \cdots & \vdots & \cdots & \vdots \\
A[i,\,1] & A[i,\,2] & & A[i,\,i] & \cdots & A[i,\,n] \\
\vdots & \vdots & & \vdots & & \vdots \\
A[j,\,1] & A[j,\,2] & \cdots & 1 & \cdots & A[j,\,n] \\
\vdots & \vdots & & \vdots & & \vdots
\end{pmatrix}
\end{array}$$

[2] Stephen Warshall. A theorem on Boolean matrices. *Journal of the ACM*, 9(1):11-12, January 1962.

直观地看, 就是把第 i 行的值, "叠加" 到第 j 行的对应位置.

比如, 若 $A[i,\,1]=1$, $A[j,\,1]=0$. 可以得到新值 $A[j,\,1]=1$. 2.56

如何理解?

Step 3 对所有 j, 如果 $A[j,\,i]=1$, 则对 $k=1,\,2,\,\cdots,\,n$,

$$A[j,\,k]:=A[j,\,k]+A[i,\,k]$$

若 $A[j,\,i]=1$, 即已有 x_j 到 x_i 的关系. 接下来的问题:

x_j 是否存在到 x_k 的关系呢?

$$\begin{array}{c}
\begin{array}{cccccc} & & & i & & \end{array} \\
\begin{array}{c} \\ i \\ \\ j \\ \\ \end{array}
\begin{pmatrix}
\vdots & \vdots & \cdots & \vdots & \cdots & \vdots \\
A[i,\,1] & A[i,\,2] & & A[i,\,i] & \cdots & A[i,\,n] \\
\vdots & \vdots & & \vdots & & \vdots \\
A[j,\,1] & A[j,\,2] & \cdots & \boxed{1} & \cdots & A[j,\,n] \\
\vdots & \vdots & & \vdots & & \vdots
\end{pmatrix}
\end{array}$$

注意循环是从 i 开始, 即逐列进行的. 实际操作:

逐列进行. 在第 i 列中若有 $A[j,\,i]=1$, 则把第 i 行叠加到第 j 行. 2.57

Example 35. 设 $A=\{a,b,c,d\}$, $R=\big\{\langle a,b\rangle,\langle b,a\rangle,\langle b,c\rangle,\langle c,d\rangle\big\}$, 用 Warshall 算法求 $t(R)$.

解: 对关系矩阵逐列使用 Warshall 算法:

$$A:=M_R=\begin{pmatrix}0&1&0&0\\1&0&1&0\\0&0&0&1\\0&0&0&0\end{pmatrix}
\xlongequal[r_2+r_1]{A[2,1]=1}\begin{pmatrix}0&1&0&0\\1&1&1&0\\0&0&0&1\\0&0&0&0\end{pmatrix}
\xlongequal[r_1+r_2]{A[1,2]=1}\begin{pmatrix}1&1&1&0\\1&1&1&0\\0&0&0&1\\0&0&0&0\end{pmatrix}$$

$$\xlongequal[r_2+r_2]{A[2,2]=1}\begin{pmatrix}1&1&1&0\\1&1&1&0\\0&0&0&1\\0&0&0&0\end{pmatrix}
\xlongequal[r_1+r_3]{A[1,3]=1}\begin{pmatrix}1&1&1&1\\1&1&1&0\\0&0&0&1\\0&0&0&0\end{pmatrix}
\xlongequal[r_2+r_3]{A[2,3]=1}\begin{pmatrix}1&1&1&1\\1&1&1&1\\0&0&0&1\\0&0&0&0\end{pmatrix}$$

$$\xlongequal[r_1+r_4]{A[1,4]=1}\begin{pmatrix}1&1&1&1\\1&1&1&1\\0&0&0&1\\0&0&0&0\end{pmatrix}
\xlongequal[r_2+r_4]{A[2,4]=1}\begin{pmatrix}1&1&1&1\\1&1&1&1\\0&0&0&1\\0&0&0&0\end{pmatrix}
\xlongequal[r_3+r_4]{A[3,4]=1}\begin{pmatrix}1&1&1&1\\1&1&1&1\\0&0&0&1\\0&0&0&0\end{pmatrix}.$$

从解题中, 我们容易发现一点规律:

1. 主对角线上的元, 可以不用理会.
2. 若 $A[j,i]=1$, 而第 i 行的元素全为零, 也可以跳过此处. 2.58

利用关系图求闭包

记 R, $r(R)$, $s(R)$, $t(R)$ 的关系图分别为 G, G_r, G_s, G_t.

- 考察 G 的每个结点, 如果没有环就加上一个环, 最终得到的是 G_r;
- 考察 G 的每一条边, 如果 x_i 到 x_j 有一条单向边, 则增加一条反方向边, 最终得到 G_s;
- 考察 G 的每个顶点,
  - 若 x_i 有到 x_j 的 "间接路径", 就添加从 x_i 到 x_j 的直接连线.
  - 若从 x_i 出发, 能回到 x_i, 则在 x_i 应有一个环.

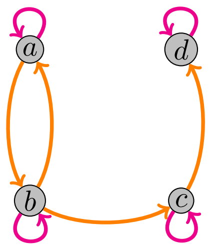
  最终得到 G_t.

2.59

Example 36. 设 $A = \{a, b, c, d\}$, $R = \{\langle a, b\rangle, \langle b, a\rangle, \langle b, c\rangle, \langle c, d\rangle\}$, 求 $r(R)$, $s(R)$, $t(R)$.

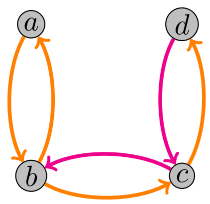
解: $r(R)$, $s(R)$, $t(R)$ 的关系图和关系矩阵如下.

① G_r 和 $M_{r(R)}$:



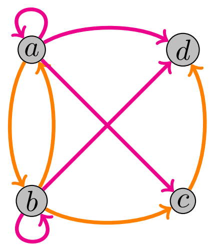
$$M_{r(R)} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

② G_s 和 $M_{s(R)}$:



$$M_{s(R)} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

③ G_t 和 $M_{t(R)}$:



$$M_{t(R)} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

2.60

Theorem 37. *设 R 是 X 上的二元关系, 则*

1. $rs(R) = sr(R)$;
2. $rt(R) = tr(R)$;
3. $st(R) \subseteq ts(R)$;

证: ① 令 I_X 表示 X 上的恒等关系,

$$
\begin{aligned}
sr(R) &= s\big(I_X \cup R\big) && (r(R) = I_X \cup R)\\
&= \big(I_X \cup R\big) \cup \big(I_X \cup R\big)^{\mathrm{c}} && (s(R) = R \cup R^{\mathrm{c}})\\
&= \big(I_X \cup R\big) \cup \big(I_X^{\mathrm{c}} \cup R^{\mathrm{c}}\big) &&\\
&= I_X \cup R \cup R^{\mathrm{c}} && (I_X^{\mathrm{c}} = I_X)\\
&= I_X \cup s(R) && (R \cup R^{\mathrm{c}} = s(R))\\
&= rs(R) && (I_X \cup R = r(R))
\end{aligned}
$$

证: ②

$$
\begin{aligned}
tr(R) = t(R \cup I_X) &= \bigcup_{i=1}^{\infty} (R \cup I_X)^i\\
&= \bigcup_{i=1}^{\infty} (I_X \cup \bigcup_{j=1}^{i} R^j)\\
&= I_X \cup \bigcup_{i=1}^{\infty} R^i\\
&= I_X \cup t(R) = rt(R).
\end{aligned}
$$

注意等式: $(R \cup I_X)^i = I_X \cup R \cup R^2 \cup R^3 \cup \cdots \cup R^i$. 2.61

证明:

$$
(R \cup I_X)^i = I_X \cup R \cup R^2 \cup R^3 \cup \cdots \cup R^i. \tag{21}
$$

证: 用归纳法证明.

当 $i = 1$ 时, (21) 式显然成立.

当 $i = 2$ 时, 注意到 $I_X \circ R = R = R \circ I_X$,

$$
\begin{aligned}
(R \cup I_X)^2 &= (R \cup I_X) \circ (R \cup I_X) = (R \cup I_X) \circ R \cup (R \cup I_X) \circ I_X\\
&= (R \circ R \cup R) \cup (R \cup I_X) = R^2 \cup R \cup I_X.
\end{aligned}
$$

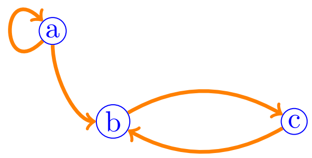
假设当 $i = k$ 时成立. 当 $i = k + 1$ 时,

$$
\begin{aligned}
(R \cup I_X)^{k+1} &= (R \cup I_X)^k \circ (R \cup I_X)\\
&= (R^k \cup \cdots \cup R^2 \cup R \cup I_X) \circ (R \cup I_X)\\
&= \big((R^k \cup \cdots \cup R^2 \cup R \cup I_X) \circ R\big) \cup \big((R^k \cup \cdots \cup R^2 \cup R \cup I_X) \circ I_X\big)\\
&= (R^{k+1} \cup R^k \cup \cdots \cup R^2 \cup R) \cup (R^k \cup \cdots \cup R^2 \cup R \cup I_X)\\
&= R^{k+1} \cup R^k \cup \cdots \cup R^2 \cup R \cup I_X.
\end{aligned}
$$

所以当 $i = k + 1$ 时 (21) 式成立. □ 2.62

习题

根据图中的有向图, 写出邻接矩阵和关系 R, 并求出 R 的自反闭包和对称闭包.



解:

$$M_R = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

$$\begin{aligned} R &= \{\langle a,a\rangle, \langle a,b\rangle, \langle b,c\rangle, \langle c,b\rangle\}, \\ r(R) &= \{\langle a,a\rangle, \langle b,b\rangle, \langle c,c\rangle, \langle a,b\rangle, \langle b,c\rangle, \langle c,b\rangle\}, \\ s(R) &= \{\langle a,a\rangle, \langle a,b\rangle, \langle b,a\rangle, \langle b,c\rangle, \langle c,b\rangle\}. \end{aligned}$$

2.63

习题

设 R_1, R_2 为非空集合 A 上的关系, 且 $R_1 \supseteq R_2$, 则

1. $r(R_1) \supseteq r(R_2)$;
2. $s(R_1) \supseteq s(R_2)$;
3. $t(R_1) \supseteq t(R_2)$.

证: ① 因 $R_1 \supseteq R_2$, 故 $R_1 \cup I_A \supseteq R_2 \cup I_A$, 即

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

② 由 $s(R_1) \supseteq R_1$, 又 $R_1 \supseteq R_2$, 所以 $s(R_1) \supseteq R_2$. 又 $s(R_1)$ 是对称的, 而 $s(R_2)$ 是包含 R_2 的最小对称关系, 所以

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

③ 由 $t(R_1) \supseteq R_1$, 又 $R_1 \supseteq R_2$, 所以 $t(R_1) \supseteq R_2$. 又 $t(R_1)$ 是传递的, 而 $t(R_2)$ 是包含 R_2 的最小传递关系, 所以 $t(R_1) \supseteq t(R_2)$. □ 2.64

5 等价关系与等价类

等价关系 (equivalence relation)

等价关系是一类重要的二元关系.

Definition 38 (等价关系)**.** 设 R 为非空集合 A 上的二元关系, 称 R 为 A 上的等价关系, 如果 R 是

1. 自反的,
2. 对称的,
3. 传递的.

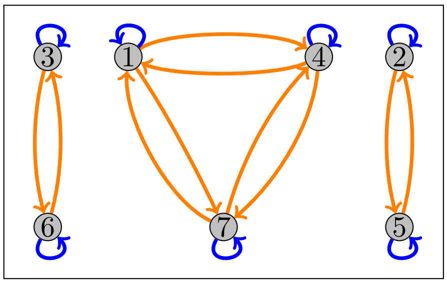
例如, 三角形的全等关系、相似关系, 数的相等关系, 命题逻辑中等价关系都是等价关系. 2.65

Example 39. 设 $A = \{1,2,3,4,5,6,7\}$, $\mathbb{Z}$ 为整数集合, A 上的关系 R 定义为:

$$R = \big\{\langle x,\, y\rangle \,\big|\, x, y \in A \wedge (x-y)/3 \in \mathbb{Z}\big\}.$$

说明 R 是等价关系.

解: $R = \{\langle 1,1\rangle, \langle 2,2\rangle, \langle 3,3\rangle, \langle 4,4\rangle, \langle 5,5\rangle, \langle 6,6\rangle, \langle 7,7\rangle, \langle 1,4\rangle, \langle 4,1\rangle, \langle 1,7\rangle, \langle 7,1\rangle, \langle 2,5\rangle, \langle 5,2\rangle, \langle 3,6\rangle, \langle 6,3\rangle, \langle 4,7\rangle, \langle 7,4\rangle\}$, 显然 R 是自反的, 对称的和传递的, 因此 R 是等价关系. R 的关系图如下:



2.66

Example 40. 设 R 为整数集合 $\mathbb{Z}$ 上的关系, k 为正整数, 令

$$R = \big\{\langle x,\, y\rangle \,\big|\, x, y \in \mathbb{Z} \wedge x \equiv y \pmod{k}\big\}.$$

称 R 为模 k 同余关系, 并称 x 与 y 模 k 相等. 证明 R 是等价关系.

证: 设任意 $a, b, c \in \mathbb{Z}$,

1. 因 $(a-a)/k = 0$, 故 $\langle a, a\rangle \in R$, 即 R 是自反的.
2. 若 $\langle a, b\rangle \in R$, 可令 $a - b = kt$ (t 为整数), 则 $b - a = -kt$, 所以
$$b \equiv a \pmod{k}.$$
3. 若 $\langle a, b\rangle \in R$, $\langle b, c\rangle \in R$, 可令 $a - b = kt$, $b - c = ks$ (其中 t, s 为整数), 那么 $a - c = (a-b) + (b-c) = k(t+s)$, 即
$$a \equiv c \pmod{k}.$$
故 $\langle a, c\rangle \in R$.

综上所述, R 是等价关系. □ 2.67

等价类 (equivalence class)

Definition 41 (等价类)**.** 设 R 为非空集合 A 上的等价关系, $\forall a \in A$, 令

$$[a]_R = \big\{x \mid x \in A \wedge aRx\big\}. \tag{22}$$

称 $[a]_R$ 为 a 关于 R 的等价类. 简称为 a 的等价类, 简记为 $[a]$.

2.68

Example 42. 设 $A = \{a, b, c\}$, 求等价关系

$$R = \{\langle a,a\rangle, \langle b,b\rangle, \langle c,c\rangle, \langle b,c\rangle, \langle c,b\rangle\}$$

的所有等价类.

解:

$$[a] = \{a\},$$
$$[b] = [c] = \{b, c\}.$$

2.69

Theorem 43. 设 R 为非空集合 A 上的等价关系, $\forall a, b \in A$,

$$aRb \Leftrightarrow [a]_R = [b]_R. \tag{23}$$

证: ① 若 aRb, 任取 $c \in [a]_R$,

$$c \in [a]_R \Rightarrow aRc \Rightarrow cRa \Rightarrow cRb \Rightarrow bRc \Rightarrow c \in [b]_R,$$

故

$$[a]_R \subseteq [b]_R.$$

同理可证 $[b]_R \subseteq [a]_R$. 故 $[a]_R = [b]_R$.

② 反之, 若 $[a]_R = [b]_R$, 则

$$a \in [a]_R \Rightarrow a \in [b]_R \Rightarrow bRa \Rightarrow aRb.$$

□

2.70

商集

集合 A 上的等价关系 R 将 A 划分为等价类, 以等价类作元素, 得到新的集合, 称为 A 关于 R 的商集.

Definition 44. 设 R 为非空集合 A 上的等价关系, 集合 $\big\{[a]_R \mid a \in A\big\}$ 称为 A 关于 R 的商集 (quotient set), 记作 A/R.

2.71

Example 45. 设 $A = \{a, b, c\}$, R 为等价关系:

$$R = \big\{\langle a, a\rangle, \langle b, b\rangle, \langle c, c\rangle, \langle b, c\rangle, \langle c, b\rangle\big\},$$

则 A 关于 R 的商集为:

$$\begin{aligned} A/R &= \{[a], [b], [c]\} \\ &= \big\{\{a\}, \{b, c\}\big\}. \end{aligned}$$

2.72

Theorem 46. 集合 A 上的等价关系 R, 决定了 A 的一个划分, 该划分就是商集 A/R.

证:

1. $A/R = \big\{[a]_R \mid a \in A\big\}$, 显然

$$\bigcup_{a \in A} [a]_R = A.$$

2. 对 $\forall a \in A$, 有 $a \in [a]_R$, 所以 A 中的每个元素都属于某个分块.
3. 下面证明 A 中的任一个元素仅属于某一个分块.
   设 $\forall a \in A$, $a \in [b]_R$ 且 $a \in [c]_R$, 那么

$$bRa, \quad cRa.$$

   因 R 对称, 所以 aRc. 又因 R 是传递的, 所以 bRc. 从而

$$[b]_R = [c]_R.$$

综上所述, A/R 是 A 关于 R 的一个划分. □ 2.73

Theorem 47. 集合 A 的一个划分确定 A 的元素间的一个等价关系.

证: 设集合 A 有一个划分 $\{A_1, A_2, \cdots, A_k\}$, 定义关系 R 为

$$R = \big\{\langle x, y\rangle \mid x, y \text{ 在同一分块中}\big\}.$$

1. 任意 $a \in A$, 由 a 与 a 属于同一分块, 得 $\langle a, a\rangle \in R$, 故 R 是自反的.
2. 若 $\langle a, b\rangle \in R$, 则 a 与 b 属于同一分块, 当然 b 与 a 也属于同一分块, 所以 $\langle b, a\rangle \in R$. 即 R 是对称的.
3. 若 $\langle a, b\rangle \in R$, $\langle b, c\rangle \in R$, 设 a, b 同属于分块 A_i, b, c 同属于分块 A_j. 由划分的定义, 当 $i \neq j$ 时,

$$A_i \cap A_j = \varnothing,$$

   但 b 只能属于一个分块, 所以 $A_i = A_j$. 于是 a, c 属于同一分块, 即 $\langle a, c\rangle \in R$, 故 R 是传递的.

综上, R 是 A 上的等价关系. □ 2.74

Example 48. 设 $A=\{a,b,c,d,e\}$, A 有一个划分 $S=\{\{a,b\},\{c\},\{d,e\}\}$, 试写出划分 S 所确定的 A 上的等价关系.

解: 令关系 R 为:

$$\begin{aligned} R &= \{\langle x,\, y\rangle \mid x, y \text{ 在同一分块中}\} \\ &= A_1 \times A_1 \cup A_2 \times A_2 \cup \cdots \cup A_k \times A_k. \end{aligned}$$

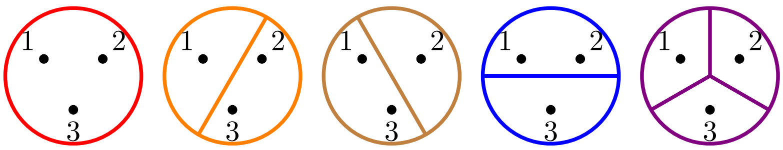
则 R 为 A 上的等价关系. 所以有如下的等价关系:

$$\begin{aligned} R_1 &= \{a,b\}\times\{a,b\} = \{\langle a,a\rangle,\langle a,b\rangle,\langle b,a\rangle,\langle b,b\rangle\}, \\ R_2 &= \{c\}\times\{c\} = \{\langle c,c\rangle\}, \\ R_3 &= \{d,e\}\times\{d,e\} = \{\langle d,d\rangle,\langle d,e\rangle,\langle e,d\rangle,\langle e,e\rangle\}, \\ R &= R_1\cup R_2\cup R_3 \\ &= \{\langle a,a\rangle,\langle b,b\rangle,\langle c,c\rangle,\langle d,d\rangle,\langle e,e\rangle,\langle a,b\rangle,\langle b,a\rangle,\langle d,e\rangle,\langle e,d\rangle\}. \end{aligned}$$

2.75

Example 49. 求出集合 $A=\{1,2,3\}$ 上的所有等价关系.

解: 因 A 的所有划分如下图所示:



A 上的所有等价关系就是上述 5 种划分对应的等价关系, 它们依次为 E_A, R_2, R_3, R_4, I_A, 其中

$$\begin{aligned} E_A &= A\times A, && \text{(全域关系)} \\ I_A &= \{\langle 1,1\rangle,\langle 2,2\rangle,\langle 3,3\rangle\}, && \text{(恒等关系)} \\ R_2 &= \{\langle 2,3\rangle,\langle 3,2\rangle\}\cup I_A, \\ R_3 &= \{\langle 1,3\rangle,\langle 3,1\rangle\}\cup I_A, \\ R_4 &= \{\langle 2,1\rangle,\langle 1,2\rangle\}\cup I_A. \end{aligned}$$

2.76

Theorem 50. 设 R_1 和 R_2 是非空集合 A 上的两个等价关系, $R_1=R_2$ 当且仅当 $A/R_1=A/R_2$.

证: ① 若 $R_1 = R_2$, 因 $A/R_1 = \{[a]_{R_1} \mid a \in A\}$, $A/R_2 = \{[a]_{R_2} \mid a \in A\}$. 对任意 $a \in A$,

$$[a]_{R_1} = \{x \mid x \in A, aR_1x\} = \{x \mid x \in A, aR_2x\} = [a]_{R_2}.$$

所以 A/R_1 和 A/R_2 中的元素相同, 即 $A/R_1 = A/R_2$.

② 反之, 若 $A/R_1 = A/R_2$, 则对任意 $[a]_{R_1} \in A/R_1$, 必有 $[c]_{R_2} \in A/R_2$, 使得 $[a]_{R_1} = [c]_{R_2}$. 所以, 对任意 $\langle a, b\rangle \in R_1$, 有

$$\begin{aligned}\langle a, b\rangle \in R_1 &\Leftrightarrow a \in [a]_{R_1} \wedge b \in [a]_{R_1}\\ &\Leftrightarrow a \in [c]_{R_2} \wedge b \in [c]_{R_2}\\ &\Rightarrow \langle a, b\rangle \in R_2.\end{aligned}$$

得 $R_1 \subseteq R_2$. 同理可证 $R_2 \subseteq R_1$. 所以 $R_1 = R_2$. □ 2.77

6 相容关系

相容关系

Definition 51 (相容关系)**.** 集合 A 上的二元关系 r 称为相容关系, 如果 r 是

1. 自反的,
2. 对称的.

相容关系也可能满足传递性. 或者说, 等价关系也是相容关系.

相容关系也常称为相似关系 (similarity relation). 2.78

Example 52. 设集合 $A = \{\text{cat, teacher, cold, desk, knife, by}\}$, 定义关系:

$$r = \{\langle x, y\rangle \mid x, y \in A \text{ 且 } x \text{ 和 } y \text{ 有相同的字母}\}.$$

显然 r 是一个相容关系.

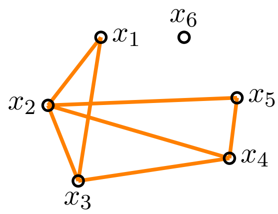
令 $x_1 = \text{cat}$, $x_2 = \text{teacher}$, $x_3 = \text{clod}$, $x_4 = \text{desk}$, $x_5 = \text{knife}$, $x_6 = \text{by}$. 则 r 的关系矩阵为

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

$$M_r: \begin{array}{c|ccccc} x_2 & 1 & & & & \\ x_3 & 1 & 1 & & & \\ x_4 & 0 & 1 & 1 & & \\ x_5 & 0 & 1 & 0 & 1 & \\ x_6 & 0 & 0 & 0 & 0 & 0 \\ \hline & x_1 & x_2 & x_3 & x_4 & x_5 \end{array}$$

注意到相容关系矩阵的对称性和对角线元素都是 1, 可将矩阵用梯形表示.

关系图也可以得到相应的简化:

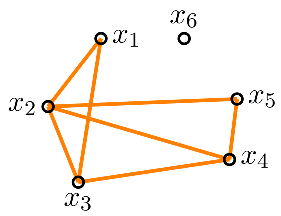


2.79

相容类

Definition 53 (相容类)**.** 设 r 是集合 A 上的相容关系, C 是 A 的子集. 如果对于 C 中任意两个元素 a_1, a_2 有 $a_1 r a_2$, 则称 C 是由相容关系 r 产生的相容类.

Example 54.



如图的相容关系 r 可产生相容类 $\{x_1, x_2\}$, $\{x_1, x_3\}$, $\{x_2, x_3\}$, $\{x_6\}$, $\{x_2, x_4, x_5\}$ 等等.

对于前三个相容类, 都能加进新的元素组成新的相容类, 而后两个相容类, 加入任一新元素, 就不再组成相容类, 我们称它为最大相容类.

2.80

最大相容类

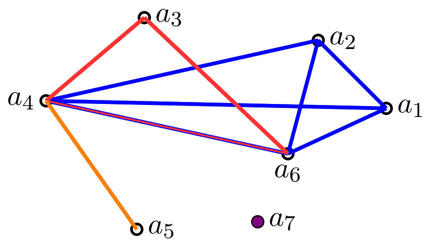
Definition 55 (最大相容类)**.** 设 r 是集合 A 上的相容关系, 不能真包含在任何其它相容类中的相容类, 称作最大相容类. 记作 C_r.

Remark

1. $\forall x \in C_r \Rightarrow (\exists y \in C_r)(x C_r y)$; $\forall x \in C_r \Rightarrow \neg(\exists z \in A - C_r)(x C_r z)$.
2. 在相容关系图中, 最大完全多边形的顶点集合, 就是最大相容类.
3. 在相容关系图中, 孤立结点, 以及不是完全多边形的两个结点的连线, 也是最大相容类.

2.81

Example 56. 设给定相容关系如图所示, 写出最大相容类.



解: 最大相容类为:

$$\{a_1, a_2, a_4, a_6\}, \quad \{a_3, a_4, a_6\}, \quad \{a_4, a_5\}, \quad \{a_7\}.$$

2.82

Theorem 57. 设 r 是有限集 A 上的相容关系, C 是一个相容类, 那么必存在一个最大相容类 C_r, 使得 $C \subseteq C_r$.

证: 设 $A=\{a_1,a_2,\cdots,a_n\}$, 构造相容类序列

$$C_0\subset C_1\subset C_2\subset\cdots,\quad 其中\ C_0=C.$$

且 $C_{i+1}=C_i\cup\{a_j\}$, 这里 j 是满足 $a_j\notin C_i$ 而 a_j 与 C_i 中各元素都有相容关系的最小足标.

由于 A 的元素个数 $\mathrm{card}(A)=n$, 所以至多经过 $n-\mathrm{card}(C)$ 步, 就使这个过程终止, 而此序列的最后一个相容类, 就是所要找的最大相容类. □ 2.83

完全覆盖

☞ $\forall a\in A$ 可以组成相容类 $\{a\}$, 由前述定理可知, $\{a\}$ 必包含在一个最大相容类 C_r 中,

因此, 若由所有最大相容类作出一个集合, 则 A 中每一元素至少属于该集合的一个成员之中, 所以最大相容类集合必覆盖集合 A.

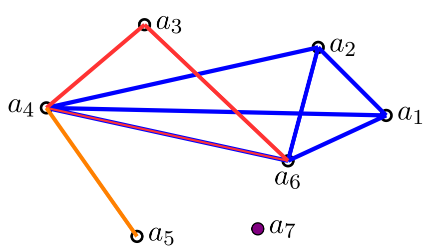
Definition 58. 在集合 A 上给定相容关系 r, 其最大相容类的集合, 称作集合 A 的*完全覆盖*, 记作 $C_r(A)$.

2.84

完全覆盖

1. 集合 A 的覆盖不是惟一的, 因此给定相容关系 r, 可以作成不同的相容类的集合, 它们都是 A 的覆盖.
2. 但给定相容关系 r, 只能对应惟一的完全覆盖. 例如图中的相容关系 r 有惟一的完全覆盖:

$$\big\{\{a_1,\,a_2,\,a_4,\,a_6\},\,\{a_3,\,a_4,\,a_6\},\,\{a_4,\,a_5\},\,\{a_7\}\big\}.$$



2.85

Theorem 59. *给定集合 A 的覆盖 $\{A_1,A_2,\cdots,A_n\}$, 由它确定的关系*

$$r=A_1\times A_1\cup A_2\times A_2\cup\cdots\cup A_n\times A_n$$

是相容关系.

证: 因为 $A = \bigcup_{i=1}^{n} A_i$, $\forall x \in A$, $\exists j > 0$ 使得 $x \in A_j$, 则 $\langle x, x\rangle \in A_j \times A_j$. 又 $r = \bigcup_{i=k}^{n} A_k \times A_k$, 所以

$$\langle x, x\rangle \in r.$$

即 r 是自反的.

其次, $\forall x, y \in A$ 且 $\langle x, y\rangle \in r$, $\exists h > 0$ 使 $\langle x, y\rangle \in A_h \times A_h$, 故必有

$$\langle y, x\rangle \in A_h \times A_h,$$

即 $\langle y, x\rangle \in r$, 所以 r 是对称的.

得证 r 是 A 上的相容关系. □

2.86

Theorem

给定集合 A 的覆盖 $\{A_1, A_2, \cdots, A_n\}$, 由它确定的关系

$$r = A_1 \times A_1 \cup A_2 \times A_2 \cup \cdots \cup A_n \times A_n$$

是相容关系.

☞ 给定集合 A 上的任意一个覆盖, 必可在 A 上构造对应于此覆盖的一个相容关系. 但是不同的覆盖却能构造相同的相容关系.

Example 60. 设 $A = \{1, 2, 3, 4\}$, 集合 $\big\{\{1, 2, 3\}, \{3, 4\}\big\}$ 和 $\big\{\{1, 2\}, \{2, 3\}, \{1, 3\}, \{3, 4\}, \big\}$ 都是 A 的覆盖, 但它们可以产生相同的相容关系:

$$\begin{aligned} r = \big\{&\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 2, 1\rangle, \langle 2, 2\rangle, \langle 2, 3\rangle, \langle 3, 2\rangle, \\ &\langle 1, 3\rangle, \langle 3, 1\rangle, \langle 3, 3\rangle, \langle 4, 4\rangle, \langle 3, 4\rangle, \langle 4, 3\rangle\big\}. \end{aligned}$$

2.87

7 序关系

序

序 (order), 指一类定义在非空集 A 上, 以满足传递性为基本条件的二元关系, 它是通常的实数之间大小次序概念的推广.

在实数系中, 两个实数之间的 “小于或等于” 关系 (记为 $\leqslant$) 是一种序, 它满足:

1. 自反性: $a \leqslant a$;
2. 反对称性: 若 $a \leqslant b$ 且 $b \leqslant a$, 则 $a = b$.
3. 传递性: 若 $a \leqslant b$, $b \leqslant c$, 则 $a \leqslant c$.
4. 强连结性: 任给 a, b, 则 $a \leqslant b$ 和 $b \leqslant a$ 中至少有一个成立.

☞ 一般说来, 如果任何集合 A 上存在二元关系 (记为 $\preccurlyeq$),

- 能满足上述 ① ∼ ④ , 则称 A 上有一全序关系 $\preccurlyeq$, A 为全序集;
- 只满足 ① , ② , ③ 的, 称为偏序.

2.88

偏序 (partial-ordering)

Definition 61. 如果集合 A 上的二元关系 R 是自反的、反对称的和传递的, 那么称 R 为 A 上的偏序关系 (或偏序). 称序偶 $\langle A,\ R\rangle$ 为偏序集 (partially ordered set, 或 poset).

- 偏序, 又称半序 (semi-ordering).
- 如果 R 是偏序关系, $\langle A,\ R\rangle$ 常记为 $\langle A,\ \preccurlyeq\rangle$. "$\preccurlyeq$" 是序关系符号, 读作 "小于或者等于".
- R 是偏序时, aRb 就记为 $a \preccurlyeq b$.

Example 62. • 在任意实数集 A 中, 以大小关系 $\leqslant$ 为序, 即 $\langle A, \leqslant\rangle$ 是偏序集;

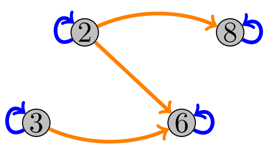
- 集合 A 的幂集 $\mathscr{P}(A)$ 中, 以包含关系"$\subseteq$" 为序, 即 $\langle \mathscr{P}(A),\ \subseteq\rangle$ 是偏序集;
- 在正整数集中, 以整除为序, 得到一个偏序集. 2.89

Example 63. 给定集合 $A = \{2, 3, 6, 8\}$, 令 "$\preccurlyeq$"$= \big\{\langle x,\ y\rangle \mid x$ 整除 $y\big\}$. 验证 "$\preccurlyeq$" 是偏序关系.

解: 集合 $A = \{2, 3, 6, 8\}$ 上的整除关系为

$$\preccurlyeq = \big\{\langle 2,\ 2\rangle,\ \langle 2,\ 6\rangle,\ \langle 2,\ 8\rangle,\ \langle 3,\ 3\rangle,\ \langle 3,\ 6\rangle,\ \langle 6,\ 6\rangle,\ \langle 8,\ 8\rangle\big\}.$$

关系矩阵和关系图如下:[2ex] $M_{\preccurlyeq} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$



从关系矩阵和关系图可以看出 "$\preccurlyeq$" 是自反、反对称和传递的, 所以是偏序关系.

注意: 偏序集中的任意两个元素之间, 并不一定都具有偏序关系. 例如 2 不整除 3, 此时称 2 和 3 不可比. 2.90

也可以一般地证明这个问题:

Example 64. 令 $A \subseteq \mathbb{N}^+$, 对任意 $m, n \in A$, $m\big|n$ 表示 m 整除 n 的关系 (即 n 为 m 的整数倍: 存在整数 k 满足 $n = km$), 试证 $\langle A,\ \big|\rangle$ 是偏序集.

证: 即要证整除关系具有自反性, 反对称性, 传递性.

1. 自反性: $(\forall m)(m \in A \to m\big|m)$;
2. 反对称性: $(\forall m)(\forall n)\big((m\big|n) \wedge (n\big|m) \to (m = n)\big)$;
3. 传递性:

$$(\forall m)(\forall n)(\forall k)\Big((m\big|n) \wedge (n\big|k) \to (\exists u)(\exists v)\big((k = un) \wedge (n = vm)\big)\Big)$$

$$\Rightarrow (\forall m)(\forall n)(\forall k)\big((m\big|n) \wedge (n\big|k) \to (m\big|k)\big)$$

$\square$ 2.91

顶点的“盖住”关系

利用偏序关系的自反性、反对称性和传递性, 可以简化一个偏序关系的关系图, 得到偏序集的哈斯图.

为了说明哈斯图的画法, 首先定义偏序集中顶点的盖住关系.

Definition 65. 设 $\langle A, \preccurlyeq\rangle$ 为偏序集, $\forall x, y \in A$, 如果 $x \preccurlyeq y$, $x \neq y$, 且不存在 $z \in A$ 使得 $x \preccurlyeq z \preccurlyeq y$, 则称 y 盖住 x. 并且记

$$\mathrm{COV}A = \big\{\langle x, y\rangle \bigm| x, y \in A;\ y \text{ 盖住 } x\big\}. \tag{24}$$

☞ 通俗地讲, 序关系 “$\preccurlyeq$” 是指集合中元素之间的顺序性.

- “$x \preccurlyeq y$” 的含义是: 依照这个顺序, “x 排在 y 的前面” 或 “x 就是 y, 是同一个元素”.
- 而所谓 “y 盖住 x”, 是指 “x 紧排在 y 的前面”. (还有别的元素也能紧排在 y 的前面吗?) 2.92

顶点的“盖住”关系

Example 66. 对集合 $A = \{1, 2, 4, 6\}$ 上的整除关系, 有

- 2 盖住 1;
- 4 和 6 都盖住 2;
- 但 4 不盖住 1, 因为有 $1 \preccurlyeq 2 \preccurlyeq 4$;
- 6 也不盖住 4, 因为 $4 \preccurlyeq 6$ 不成立.

则

$$\mathrm{COV}A = \big\{\langle 1, 2\rangle, \langle 2, 4\rangle, \langle 2, 6\rangle\big\}.$$

☞ 可见, 在偏序关系中, 把 “盖住” 仅仅理解为 “紧排在前面”, 是不全面的.

哈斯图是把元素按 “层” 来排列, 紧排在 2 后面的 4 和 6 就处在同一层. 2.93

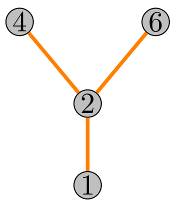
偏序集合的哈斯 (Hasse [3]) 图表示

哈斯图的作法

设有偏序集 $\langle A, \preccurlyeq\rangle$, $\forall x, y \in A$ $(x \neq y)$, 适当排列结点的顺序使得:

1. 若 $x \preccurlyeq y$, 则将 x 画在 y 的下方.
2. 如果 y 盖住 x, 则用一条直线连接 x 和 y.

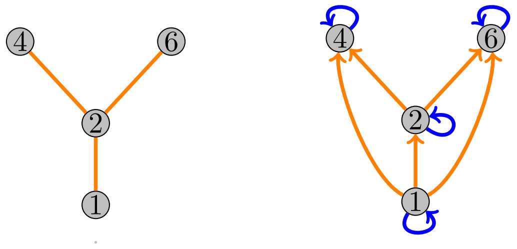
对集合 $A = \{1, 2, 4, 6\}$ 上的整除关系, 有哈斯图



2.94

注意哈斯图与关系图的不同. 哈斯图表达的是 “盖住” 关系, 即 $\mathrm{COV}A$.

[3] Helmut Hasse, 1898 — 1979, 德国数学家.



(a) 哈斯图　　(b) 关系图

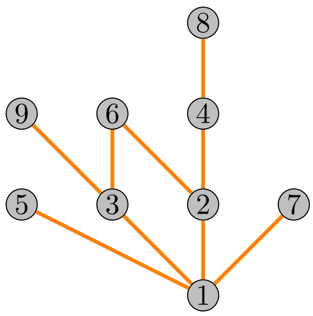
Example 67. 对集合 $A = \{1, 2, 4, 6\}$ 上的整除关系, 哈斯图表示的是

$$\mathrm{COV}A = \big\{\langle 1,\ 2\rangle,\ \langle 2,\ 4\rangle,\ \langle 2,\ 6\rangle\big\}.$$

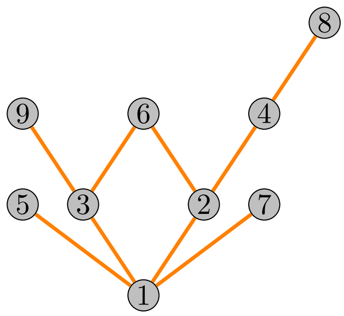
哈斯图中: 无环, 无 “第三边”, 不使用箭头, 更无双边 (与关系图的区别); 无水平边 (同层次元素不可比). 2.95

Example 68. 画出偏序集 $\big\langle\{1, 2, 3, 4, 5, 6, 7, 8, 9\}, R_{整除}\big\rangle$ 的哈斯图.

解: 其哈斯图如下:

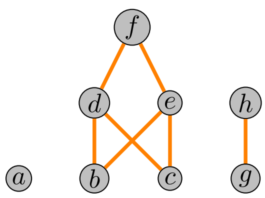


或者



2.96

Example 69. 已知偏序集 $\langle A,\ R\rangle$ 的哈斯图如下图所示, 试求出集合 A 和关系 R 的表达式.



解: 集合 A 为

$$A = \{a,\ b,\ c,\ d,\ e,\ f,\ g,\ h\}.$$

注意到哈斯图中有 7 条边, 又注意到偏序关系的传递性, 得

$$R = \big\{\langle b, d\rangle, \langle b, e\rangle, \langle b, f\rangle, \langle c, d\rangle, \langle c, e\rangle, \langle c, f\rangle, \langle d, f\rangle, \langle e, f\rangle, \langle g, h\rangle\big\}. \tag{25}$$

☞ 这里 (25) 式是正确解答吗? 注意不要遗漏了偏序关系的自反性, 正解:

$$R = \{\langle b,d\rangle, \langle b,e\rangle, \langle b,f\rangle, \langle c,d\rangle, \langle c,e\rangle, \langle c,f\rangle, \langle d,f\rangle, \langle e,f\rangle, \langle g,h\rangle\} \cup I_A. \tag{26}$$

如果问题是要我们由哈斯图求关系图, 也要注意同样的问题. □ 2.97

链

Definition 70. 设 $\langle A, \preccurlyeq\rangle$ 为偏序集,

1. 在 A 的一个子集中, 如果每两个元素都是有关系的, 则称这个子集为链 (chain).
2. 在 A 的一个子集中, 如果每两个元素都是无关的, 则称这个子集为反链.

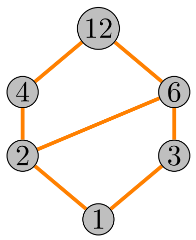
☞ 通俗地讲, 链中的每两个元素都是可比的; 反链中的每两个元素都是不可比的.
约定: 若 A 的子集只有单个元素, 则这个子集既是链又是反链. 2.98

链

Example 71. 设 A 是正整数 $m = 12$ 的因子的集合, 并设 $\preccurlyeq$ 为整除关系. 求 $\mathrm{COV}A$.

解: 集合 $A = \{1, 2, 3, 4, 6, 12\}$, 且

$$\mathrm{COV}A = \{\langle 1,2\rangle, \langle 1,3\rangle, \langle 2,4\rangle, \langle 2,6\rangle, \langle 3,6\rangle, \langle 4,12\rangle, \langle 6,12\rangle\}.$$



- 子集 $\{1,2,4,12\}$, $\{1,3,6,12\}$, $\{1,2,6,12\}$, $\{1,2,4\}$, $\{2,6\}$ 都是链;
- 子集 $\{2,3\}$, $\{3,4\}$ 都是反链;
- 子集 $\{1,2,3,6\}$ 既不是链, 也不是反链.

☞ 在哈斯图上, 链中的元素分布在沿盖住方向的一条线上. 2.99

全序集合

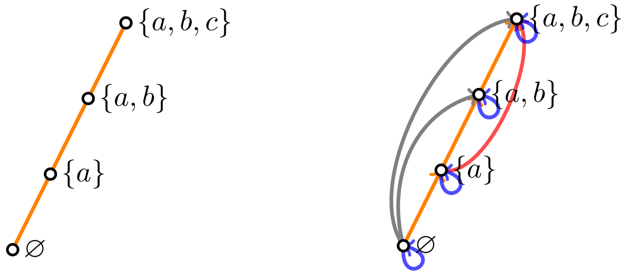
Definition 72. 在偏序集 $\langle A, \preccurlyeq\rangle$ 中, 如果 A 是一个链, 则

- 称 $\langle A, \preccurlyeq\rangle$ 为全序集合 (totally ordered set) 或线序集合 (linearly ordered set);
- 二元关系 $\preccurlyeq$ 称为 A 上的全序关系 (或线序关系).

☞ 所谓 “全序”, 就是在自反、反对称、传递的基础上, 添加了可比性 (强连结性), 即

$$(\forall a)(\forall b)\big((a,\, b \in A) \to (a \preccurlyeq b) \vee (b \preccurlyeq a)\big).$$

自然数集 $\mathbb{N}$, 整数集 $\mathbb{Z}$, 有理数集 $\mathbb{Q}$, 实数集 $\mathbb{R}$ 上的 $\leqslant$ 关系, 就是全序概念的起源. 2.100



(a) 哈斯图　　　(b) 关系图

Example 73. 给定 $A = \big\{\varnothing, \{a\}, \{a,b\}, \{a,b,c\}\big\}$ 上的包含关系 $\subseteq$, 证明 $\langle A, \subseteq\rangle$ 是全序集合.

解: 包含关系 $\subseteq$ 显然是自反的, 反对称和传递的, 所以 $\langle A, \subseteq\rangle$ 是偏序集. 而且 A 中任意两个元素都可比:

$$\varnothing \subseteq \{a\} \subseteq \{a,b\} \subseteq \{a,b,c\}.$$

所以 $\langle A, \subseteq\rangle$ 是全序集合. 2.101

极大、极小元; 最大、最小元

Definition 74. 设 $\langle A, \preccurlyeq\rangle$ 为偏序集, $B \subseteq A$, 对 $b \in B$,

1. 如果 B 中没有任何元素 x, 满足 $b \neq x$ 且 $b \preccurlyeq x$, 则称 b 为 B 的极大元 (maximal element);
2. 如果 B 中没有任何元素 x, 满足 $b \neq x$ 且 $x \preccurlyeq b$, 则称 b 为 B 的极小元 (minimal element).

☞ b 为 B 的极小元: 如果 B 中不存在任何小于 b 的元素, 即 b 小于 B 中任何异于 b 且与 b 可比较的元素. 用符号表达如下:

$$(\forall x \in B)\big(x \preccurlyeq b \to x = b\big).$$

b 为 B 的极大元, 用符号表达如下:

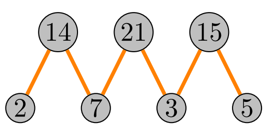
$$(\forall x \in B)\big(b \preccurlyeq x \to x = b\big).$$

2.102

极大、极小元; 最大、最小元

Example 75. 设 $A = \{2, 3, 5, 7, 14, 15, 21\}$. 偏序集为 $\langle A, \mid\rangle$. 求 $B = \{2, 3, 7, 14, 21\}$ 的极大元和极小元.

解: $\langle A, \mid\rangle$ 的哈斯图如下:



B 的极小元集合是 $\{2, 7, 3\}$, B 的极大元集合是 $\{14, 21\}$. □

- 极大元是哈斯图中最末端的元素;
- 极小元是哈斯图中最底层的元素;
- 不同的极小元 (极大元) 之间是无关的, 是不可比的. 2.103

极大、极小元; 最大、最小元

Definition 76. 设 $\langle A, \preccurlyeq \rangle$ 为偏序集, $B \subseteq A$, 对 $b \in B$,

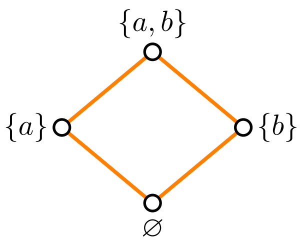
1. 对于 B 中每一个元素 x 有 $x \preccurlyeq b$, 则称 b 为 B 的最大元 (largest element, greatest element);
2. 对于 B 中每一个元素 x 有 $b \preccurlyeq x$, 则称 b 为 B 的最小元 (least element, smallest element).

或用符号表达如下:

1. 若 $(\forall x)(x \in B \to x \preccurlyeq b)$ 成立, 则称 b 为 B 的最大元;
2. 若 $(\forall x)(x \in B \to b \preccurlyeq x)$ 成立, 则称 b 为 B 的最小元; 2.104

极大、极小元; 最大、最小元

Example 77. 考虑偏序集 $\langle \mathscr{P}(\{a, b\}), \subseteq \rangle$, 其哈斯图为:



1. 若 $B = \{\{a\}, \varnothing\}$, 则 $\{a\}$ 是 B 的最大元; $\varnothing$ 是 B 的最小元.
2. 若 $B = \{\{a\}, \{b\}\}$, 则 B 没有最大元和最小元, 因为 $\{a\}$ 和 $\{b\}$ 是不可比较的. 2.105

极大、极小元; 最大、最小元

Theorem 78. *设 $\langle A, \preccurlyeq \rangle$ 为偏序集且 $B \subseteq A$, 若 B 有最大 (最小) 元, 则必是惟一的.*

证: 假定 a 和 b 两者都是 B 的最大元素, 则 $a \preccurlyeq b$ 和 $b \preccurlyeq a$, 从 $\preccurlyeq$ 的反对称性, 得到 $a = b$.

B 的最小元情况与此类似. □

一个偏序集的子集, 甚至是全序子集都未必有最小元或最大元.

例如, 在实数集合 $\mathbb{R}$ 中, 以通常的大小关系为序, 则 {所有的整数}, {所有的正有理数}, $(0, 1)$ 等子集都没有最小元.

当然, 最大元的情形类似. 2.106

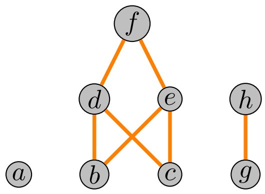
极大、极小元; 最大、最小元

注: 最小元与极小元的不同

- 最小元是 B 中最小的元素, 它与 B 中其它元素都可比; 而极小元不一定与 B 中所有元素都可比, 只要没有比它小的元素, 它就是极小元.
- 对于有穷集 B, 极小元一定存在, 但最小元不一定存在. 最小元如果存在, 一定是惟一的, 但极小元可能有多个.
- 如果 B 中只有一个极小元, 则它一定是 B 的最小元; 如果 B 中有最小元, 则它一定是 B 的惟一的极小元.

类似的, 极大元与最大元也有这种区别和联系. 2.107

Example 79. 考虑如图所示的偏序集 $\langle A, \preccurlyeq\rangle$, 求 A 的极小元、最小元、极大元、最大元.



解: 由该偏序集的哈斯图可知:

- 极小元: a, b, c, g;
- 极大元: a, f, h;
- 没有最小元与最大元. □

☞ 由这个例子可以知道, 哈斯图中的孤立顶点既是极小元也是极大元. 2.108

偏序集的子集的上界、下界

Definition 80. 设 $\langle A, \preccurlyeq\rangle$ 为偏序集, $B \subseteq A$, $a \in A$:

1. 若 $(\forall x)(x \in B \to x \preccurlyeq a)$ 成立, 则称 a 为 B 的上界 (upper bound);
2. 若 $(\forall x)(x \in B \to a \preccurlyeq x)$ 成立, 则称 a 为 B 的下界 (lower bound);

☞ 注意这里 $a \in A$. 即 B 的上界、下界不一定是 B 中的元素. 2.109

偏序集的子集的上界、下界

Definition 81. 设 $\langle A, \preccurlyeq\rangle$ 为偏序集, $B \subseteq A$,

1. 设 a 是 B 的一个上界, 若对 B 的所有上界 y 均有 $a \preccurlyeq y$, 则称 a 为 B 的最小上界 (least upper bound) 或上确界 (supremum), 记为 $\mathrm{LUB}B$ 或 $\sup B$;
2. 设 b 是 B 的一个下界, 若对 B 的所有下界 z 均有 $z \preccurlyeq b$, 则称 b 为 B 的最大下界 (greatest lower bound) 或下确界 (infimum), 记为 $\mathrm{GLB}B$ 或 $\inf B$.

☞ 或者:

1. 令 $C = \{a \mid a \text{ 为 } B \text{ 的上界}\}$, 则称 C 的最小元为 B 的 最小上界;
2. 令 $D = \{b \mid b \text{ 为 } B \text{ 的下界}\}$, 则称 D 的最大元为 B 的 最大下界. 2.110

偏序集的子集的上界、下界

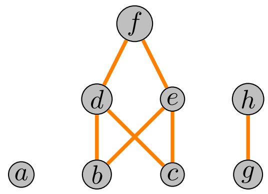
注

- B 的最小元一定是 B 的下界, 同时也是 B 的最大下界. 但反过来不一定正确, B 的下界不一定是 B 的最小元, 因为它可能不是 B 中的元素.
- 同样的, B 的最大元一定是 B 的上界, 同时也是 B 的最小上界. B 的上界也不一定是 B 的最大元.
- B 的上界、下界、最小上界、最大下界都可能不存在. 如果存在, 最小上界与最大下界是惟一的.

2.111

☞ B 的上界、下界、最小上界、最大下界都可能不存在? 看一个例子.

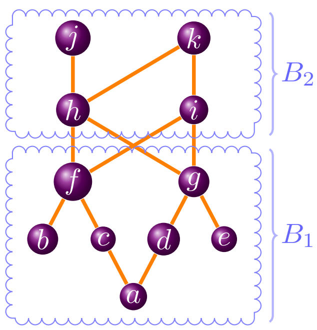
Example 82. 考虑如下哈斯图所示的偏序集.



令 $B = \{b, c, d\}$, 则 B 的下界和最大下界都不存在, 上界有 d 和 f, 最小上界为 d.

2.112

Example 83. 给定偏序集 $\langle A, \preccurlyeq \rangle$ 的哈斯图, 求 $B_1 = \{a, b, c, d, e, f, g\}$, $B_2 = \{h, i, j, k\}$, $B_3 = \{f, h, j, i, g\}$ 的上界, 下界, 上确界, 下确界.



子集	上界	下界	上确界	下确界
$\{a, b, c, d, e, f, g\}$	h, i, j, k	无	无	无
$\{h, i, j, k\}$	无	a, b, c, d, e, f, g	无	无
$\{f, h, j, i, g\}$	无	a	无	a

2.113

Example 84. 对 $\langle \mathbb{R}, \leqslant \rangle$ 的子集 $B_1 = \{x \mid 0 < x < 1\}$; $B_2 = \{x \mid 0 \leqslant x < +\infty\}$.

1. 关于 B_1, 有
   - 0 为 B_1 的最大下界; 1 为 B_1 的最小上界;
   - B_1 有无穷多个上界 $\big((\forall x)(x \geqslant 1 \to x$ 为 B_1 的上界$)\big)$;
   - B_1 有无穷多下界 $\big((\forall x)(x \leqslant 0 \to x$ 为 B_1 的下界$)\big)$;
   - 但 0, 1 不属于 B_1, 故不是 B_1 的最小 (大) 元素.
2. 关于 B_2, 有
   - 0 为 B_2 的最小元素, 故也是最大下界;
   - B_2 有无穷多下界 $\big((\forall x)(x \leqslant 0 \to x$ 为 B_2 的下界$)\big)$;
   - 但 B_2 没有上界, 更没有最小上界.

2.114

良序集合

Definition 85. 设 $\langle A, \preccurlyeq \rangle$ 为偏序集, 如果 A 的每一非空子集总含有最小元, 那么 $\preccurlyeq$ 称为 A 上的良序 (well-ordering), 序偶 $\langle A, \preccurlyeq \rangle$ 叫做良序集合.

Example 86. 例如, $I_n = \{1, 2, \cdots, n\}$ 及 $\mathbb{N}^+ = \{1, 2, 3, \cdots\}$, 对于 $\leqslant$ 关系来说是良序集合, 即 $\langle I_n, \leqslant \rangle$, $\langle \mathbb{N}, \leqslant \rangle$ 是良序集合.

2.115

良序集合

Theorem 87. *每一良序集合, 一定是全序集合.*

证: 设 $\langle A, \preccurlyeq \rangle$ 为良序集合. 则 $\langle A, \preccurlyeq \rangle$ 已经是偏序集.

要进一步证 $\langle A, \preccurlyeq \rangle$ 为全序集, 只需要证

$$(\forall a)(\forall b)\big((a, b \in A) \to (a \preccurlyeq b) \vee (b \preccurlyeq a)\big)$$

成立.

对 $\forall a, b \in A$, 可构成子集 $\{a, b\}$. 由 $\langle A, \preccurlyeq \rangle$ 为良序集合, 则 $\{a, b\}$ 必存在最小元素: a 或 b.

所以

$$(a \preccurlyeq b) \vee (b \preccurlyeq a).$$

□

2.116

良序集合

Theorem 88. *每一有限的全序集合, 一定是良序集合.*

证: 设 $A=\{a_1, a_2, \cdots, a_n\}$, 令 $\langle A, \preccurlyeq\rangle$ 是全序集.

假设 $\langle A, \preccurlyeq\rangle$ 不是良序集, 则必存在非空子集 $B \subseteq A$, 在 B 中不存在最小元.

由于 B 是一个有限集合, 故一定可以找出两个元素 x 与 y 是无关的.

由于 $\langle A, \preccurlyeq\rangle$ 是全序集, $x, y \in A$, 所以 x 与 y 必有关系, 得出矛盾.

故 $\langle A, \preccurlyeq\rangle$ 必是良序集. □

上述结论对于无限的全序集合不一定成立. 例如 $\langle (0,1), \leqslant \rangle$ 是一个全序集合, 但不是良序集合, 因为集合本身就不存在最小元素. 2.117

良序集合

Example 89. 1. 实数集 $\mathbb{R}$ 上的 "$\leqslant$" 关系是全序关系, 因为任何两个数总是可比大小的; 但它不是良序关系, 例如其子集 $A=(0,1]$ 无最小元素;

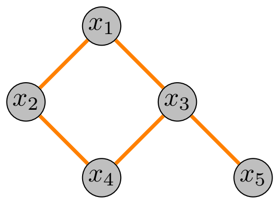
2. 正整数集合 $\mathbb{N}^+$ 上的整除关系一般来说不是全序关系, 如集合 $\{1,2,3\}$ 上的整除关系就不是全序关系, 因为 2 和 3 不可比;
3. 全序集合 $\langle \mathbb{Z}, \leqslant\rangle$ 不是良序集合, 因为 $\mathbb{Z}$ 的某些子集 (例如 $\mathbb{Z}$ 本身) 不包含最小元素.

☞ 总的来说, 偏序、全序、良序, 依次加强. 2.118

Example 90. 设集合 $P=\{x_1, x_2, x_3, x_4, x_5\}$ 上的偏序关系如图所示.

① 找出 P 的最大元, 最小元, 极大元, 极小元.

② 找出子集 $\{x_2, x_3, x_4\}$, $\{x_3, x_4, x_5\}$, $\{x_1, x_2, x_3\}$ 的上界, 下界, 上确界, 下确界.



解: ① P 的最大元是 x_1, 无最小元. 极大元是 x_1, 极小元是 x_4, x_5.

② 如下表:

子集	上界	下界	上确界	下确界
$\{x_2, x_3, x_4\}$	x_1	x_4	x_1	x_4
$\{x_3, x_4, x_5\}$	x_1, x_3	无	x_3	无
$\{x_1, x_2, x_3\}$	x_1	x_4	x_1	x_4

2.119

Chapter 4

代数系统

Discrete Mathematics

October 8, 2012

黄正华, 数学与统计学院, 武汉大学 4.1

教学内容

代数系统的引入，运算及其性质，半群，群与子群，阿贝尔群和循环群，陪集与拉格朗日定理，同态与同构，环与域. 4.2

教学目的

(1) 掌握运算及其性质；
(2) 理解半群、群、阿贝尔群、循环群的概念、性质；
(3) 知道陪集的概念，掌握拉格朗日定理；
(4) 知道同态、同构的概念；
(5) 理解环、域的概念. 4.3

Contents

1 代数系统的引入

运算 & 封闭

Definition 1. 对集合 A，一个从 A^n 到 B 的映射, 称为集合 A 上的一个 n 元运算 (n-nary operation). 如果 $B \subseteq A$, 则称该运算是封闭的.

Example 2.
- 例如 $f: \mathbb{N} \times \mathbb{N} \to \mathbb{N}, f(\langle x, y\rangle) = x + y$ (这里 $+$ 表示普通的加法运算) 就是自然数集合 $\mathbb{N}$ 上封闭的二元运算.
- 而普通的减法不是自然数集合 $\mathbb{N}$ 上封闭的二元运算. 因为两个自然数相减
4.5 可能得负数, 而负数不是自然数. 这时称集合 $\mathbb{N}$ 对减法运算不封闭.

代数系统

Definition 3. 一个非空集合 A 及定义在 A 上的 k 个运算 $f_1, f_2, \cdots, f_k$ 所组成的系统, 称为一个代数系统 (algebraic system), 记作 $\langle A, f_1, f_2, \cdots, f_k\rangle$.

☞ 代数系统也可以用 $\langle A, +, -, *, \cdots\rangle$ 表示, 其中 $+, -, *, \cdots$ 表示 A 的各个
4.6 代数运算.

Example 4. 设 $S = \{1, 2, 3, 4\}$, 定义 S 上的二元运算 $\circ$ 如下:

$$x \circ y = (xy) \pmod 5, \quad \forall x, y \in S \tag{1}$$

则 $\langle S, \circ\rangle$ 构成一个代数系统.

这里, 运算 $\circ$ 还可用表格的形式来定义, 称为运算表:

$\circ$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

4.7 从表中可以看出, 运算 $\circ$ 在 S 上是封闭的.

代数系统

Example 5. 有类似的封闭性质的代数系统, 还有如
- $\langle \mathbb{Z}, +\rangle$, $+$ 表示通常的加法运算.
- $\langle \mathbb{Z}, *\rangle$, $*$ 表示通常的乘法运算.
- $\langle \mathscr{P}(S), \cup, \cap, \sim\rangle$ 等,

4.8 这里 $\mathbb{Z}$ 表示整数集合, $\mathscr{P}(S)$ 表示集合 S 的幂集.

2 运算及其性质

封闭

Definition 6. 设 $*$ 是定义在集合 A 上的二元运算, 如果对任意 $x, y \in A$, 都有 $x * y \in A$, 则称运算 $*$ 在 A 上封闭.

☞ 通俗地讲, 封闭就是和谐、不自相矛盾.

4.9 理论、系统都具有这个特点: 基本要求是能自成一体.

可交换

Definition 7. 设 $*$ 为 A 上的二元运算, 如果对任意 $x, y \in A$, 都有

$$x * y = y * x$$

则称二元运算 $*$ 在 A 上是可交换的.

Example 8. 例如,

- 实数集合上的加法和乘法是可交换的, 但减法不可交换.
- 幂集 $\mathscr{P}(A)$ 上的 $\cup$, $\cap$, $\oplus$ (对称差) 都是可交换的, 但是相对补运算 (差运算) 不可交换.

4.10

可交换

Example 9. 设 $A = \{a, b, c, d\}$, 由表

$*$	a	b	c	d
a	a	b	c	d
b	b	d	a	c
c	c	a	b	dd
d	d	c	aa	b

所给的代数运算是否满足交换律?

解: 注意到 $d * c = a$, 而 $c * d = d$, 所以该运算不满足交换律.

☞ 可见满足交换律的运算, 其运算表是对称的.

4.11

可结合

Definition 10. 设 $*$ 为 A 上的二元运算, 如果对于任意的 $x, y, z \in A$ 都有

$$(x * y) * z = x * (y * z),$$

则称运算 $*$ 在 A 上是可结合的.

Example 11. 例如普通的加法和乘法, 在自然数集 $\mathbb{N}$, 整数集 $\mathbb{Z}$, 有理数集 $\mathbb{Q}$, 实数集 $\mathbb{R}$ 和复数集 $\mathbb{C}$ 上都是可结合的. 减法就不满足结合律:

$$(a - b) - c \neq a - (b - c), \quad 除非\ c = 0.$$

4.12

可分配

Definition 12. 设 $\circ$ 和 $*$ 是集合 A 上的两个二元运算, 如果对任意的 $x, y, z \in A$, 有

$$x * (y \circ z) = (x * y) \circ (x * z), \tag{2}$$

$$(y \circ z) * x = (y * x) \circ (z * x), \tag{3}$$

则称运算 $*$ 对 $\circ$ 是可分配的.

Example 13. 例如,

- 实数集 $\mathbb{R}$ 上的乘法对加法是可分配的;
- 在幂集 $\mathscr{P}(S)$ 上 $\cup$ 和 $\cap$ 是互相可分配的.

4.13

吸收律

Definition 14. 设 $\circ$ 和 $*$ 是 A 上两个可交换的二元运算, 如果对于任意的 $x, y \in A$ 都有

$$x * (x \circ y) = x, \tag{4}$$

$$x \circ (x * y) = x, \tag{5}$$

则称 $\circ$ 和 $*$ 满足*吸收律*.

Example 15. 例如幂集 $\mathscr{P}(S)$ 上的 $\cup$ 和 $\cap$ 运算满足吸收律: 任意 $A, B \in \mathscr{P}(S)$, 有

$$A \cup (A \cap B) = A, \tag{6}$$

$$A \cap (A \cup B) = A. \tag{7}$$

4.14

等幂律

Definition 16. 设 $\circ$ 为 A 上的二元运算, 如果对于任意的 $x \in A$ 都有 $x \circ x = x$, 则称运算 $\circ$ 是*等幂的*, 或称该运算适合*等幂律*.

Example 17. 例如幂集 $\mathscr{P}(S)$ 上的 $\cup$ 和 $\cap$ 运算满足等幂律: 任意 $A \in \mathscr{P}(S)$, 有

$$A \cup A = A, \quad A \cap A = A.$$

4.15

左幺元, 右幺元, 幺元

Definition 18. 设 $\circ$ 为 A 上的二元运算,

- 如果存在 $e_l \in A$, 使得对任意 $x \in A$ 都有
  $$e_l \circ x = x \tag{8}$$
  则称 e_l 是 A 中关于 $\circ$ 运算的一个*左幺元*.
- 如果存在 $e_r \in A$, 使得对任意 $x \in A$ 都有
  $$x \circ e_r = x \tag{9}$$
  则称 e_r 是 A 中关于 $\circ$ 运算的一个*右幺元*.
- 若 $e \in A$ 关于 $\circ$ 运算既是*左幺元*又是*右幺元*, 则称 e 为 A 上关于 $\circ$ 运算的*幺元*.

4.16

左幺元, 右幺元, 幺元

Example 19. 在自然数集 $\mathbb{N}$ 上, 0 是加法的幺元, 1 是乘法的幺元.

Example 20. 指出幂集 $\mathscr{P}(S)$ 上, $\cup$ 运算和 $\cap$ 运算的幺元.

4.17 解: $\cup$ 运算的幺元是 $\varnothing$, $\cap$ 运算的幺元是 S.

Theorem 21. *设 $\circ$ 为 A 上的二元运算, e_l, e_r 分别为 $\circ$ 运算的左幺元和右幺元, 则 $e_l = e_r = e$, 且 e 为 A 上关于 $\circ$ 运算的惟一的幺元.*

证: ① 因

$$e_l = e_l \circ e_r \qquad (e_r\ \text{为右幺元})$$

$$e_l \circ e_r = e_r \qquad (e_l\ \text{为左幺元})$$

所以 $e_l = e_r$.

令 $e_l = e_r = e$, 则 e 是 A 中的幺元.

② 假设 e' 是 A 中的另一个幺元, 则有

$$e' = e \circ e' = e.$$

所以 e 是 A 中关于 $\circ$ 运算的惟一的幺元. □ 4.18

Example 22. 设 $S = \{\alpha, \beta, \gamma, \delta\}$, $*$ 运算由下表定义, 指出 $*$ 运算是否有左幺元, 右幺元?

$*$	α	β	δ	γ
α	δ	α	β	γ
β	α	β	δ	γ
δ	α	β	δ	γ
γ	δ	γ	α	β

解: β 和 δ 都是 S 中关于 $*$ 运算的左幺元; $*$ 运算没有右幺元. 4.19

左零元, 右零元, 零元

Definition 23. 设 $\circ$ 为 A 上的二元运算,

- 若存在元素 $\theta_l \in A$ 使得对于任意 $x \in A$ 有
$$\theta_l \circ x = \theta_l \tag{10}$$
则称 θ_l 是 A 上关于 $\circ$ 运算的*左零元*.
- 若存在元素 $\theta_r \in A$ 使得对于任意 $x \in A$ 有
$$x \circ \theta_r = \theta_r \tag{11}$$
则称 θ_r 是 A 上关于 $\circ$ 运算的*右零元*.
- 若 $\theta \in A$ 关于 $\circ$ 运算既是*左零元*又是*右零元*, 则称 θ 为 S 上关于 $\circ$ 运算的*零元*.

4.20

左零元, 右零元, 零元

Example 24. 例如自然数集合上 0 是普通乘法的零元, 而加法没有零元.

Example 25. 指出幂集 $\mathscr{P}(S)$ 上, $\cup$ 运算和 $\cap$ 运算的零元.

解: $\cup$ 运算的零元是 S, $\cap$ 运算的零元是 $\varnothing$.

注意

通俗地讲,

- 幺元是运算中影响最小的元: 运算的结果还是对方;
- 零元是运算中影响最大的元: 运算的结果总是自己.

4.21

Theorem 26. 设 $\circ$ 为 A 上的二元运算, θ_l 和 θ_r 分别为 $\circ$ 运算的左零元和右零元, 则有 $\theta_l = \theta_r = \theta$, 且 θ 是 A 上关于 $\circ$ 运算的惟一零元.

证: 设 θ_l 和 θ_r 分别为 $\circ$ 运算的左零元和右零元, 所以

$$\theta_l = \theta_l \circ \theta_r = \theta_r \tag{12}$$

令 $\theta_l = \theta_r = \theta$, 则 θ 是 A 上关于 $\circ$ 运算的零元.

假设 θ' 也是 A 中的零元, 则有

$$\theta' = \theta \circ \theta' = \theta,$$

4.22 所以 θ 是 A 中关于 $\circ$ 运算的惟一的零元. □

Theorem 27. 设 $\circ$ 为 A 上的二元运算, e 和 θ 分别为 $\circ$ 运算的幺元和零元, 如果 A 至少有两个元素, 则 $e \neq \theta$.

证: 用反证法. 假设 $e = \theta$, 则对 $\forall x \in A$ 有

$$\begin{aligned} x &= x \circ e && (e \text{ 是幺元}) \\ &= x \circ \theta && (e = \theta) \\ &= \theta && (\theta \text{ 是零元}) \end{aligned}$$

4.23 此式说明 A 中只有惟一的元素 θ, 与 A 中至少含有两个元素矛盾. □

左逆元, 右逆元, 逆元

Definition 28. 设 $\circ$ 为 A 上的二元运算, $e \in A$ 为 $\circ$ 运算的幺元, 对于 $x \in A$,

- 如果存在 y_l 使得 $y_l \circ x = e$, 则称 y_l 是 x 的左逆元.
- 如果存在 y_r 使得 $x \circ y_r = e$, 则称 y_r 是 x 的右逆元.
- 若 $y \in S$ 既是 x 的左逆元又是 x 的右逆元, 则称 y 是 x 的逆元 (inverse elements).
  - 如果 x 的逆元存在, 则称 x 是可逆的.
  - 一个元素 x 的逆元通常记为 x^{-1}.
  - 当运算被称为 "加法运算" 时 (记为 $+$), x 的逆元可记为 $-x$.

4.24

Example 29. 例如, 在整数集合 $\mathbb{Z}$ 上, 加法的幺元是 0. 对任何整数, 它的加法逆元都存在, 即它的相反数 $-x$.

注意

对于给定的集合和二元运算来说,

- 如果幺元或零元存在, 一定是惟一的.
- 而逆元能否存在, 与元素有关. 有的元素有逆元, 有的元素没有逆元, 不同的元素对应着不同的逆元.
  - 一个元素的左逆元不一定等于它的右逆元.
  - 一个元素可以有左逆元不一定有右逆元.
  - 甚至一个元素的左 (右) 逆元不一定是惟一的.

Theorem 30. 设 $\circ$ 为 A 上可结合的二元运算, e 为幺元. 对 $x \in A$, 若存在左逆元 y_l 和右逆元 y_r, 则有 $y_l = y_r = y$, 且 y 是 x 的惟一的逆元.

证: ① 对于 $x \in A$, 注意到 y_l 和 y_r 是 x 的左、右逆元, 有 $y_l \circ x = e$ 和 $x \circ y_r = e$, 得

$$\begin{aligned} y_l &= y_l \circ e && (e \text{ 是幺元}) \\ &= y_l \circ (x \circ y_r) && (y_r \text{ 是 } x \text{ 的右逆元}) \\ &= (y_l \circ x) \circ y_r && (\circ \text{ 为可结合的}) \\ &= e \circ y_r && (y_l \text{ 是 } x \text{ 的左逆元}) \\ &= y_r && (e \text{ 是幺元}) \end{aligned}$$

令 $y_l = y_r = y$, 则 y 是 x 的逆元.

证: ② 下面证明逆元的惟一性.

假若 $y' \in A$ 也是 x 的逆元, 则

$$\begin{aligned} y' &= y' \circ e && (e \text{ 是幺元}) \\ &= y' \circ (x \circ y) && (y \text{ 是 } x \text{ 的逆元}) \\ &= (y' \circ x) \circ y && (\circ \text{ 为可结合的}) \\ &= e \circ y && (y' \text{ 是 } x \text{ 的逆元}) \\ &= y. && (e \text{ 是幺元}) \end{aligned}$$

所以 y 是 x 惟一的逆元. □ 4.26

Example 31. 设代数系统 $\langle A, * \rangle$, 其中 $A = \{a, b, c\}$, A 上的二元运算 $*$ 定义如表: 试分析 $*$ 运算的封闭性, 交换性, 等幂性. A 中关于 $*$ 是否有幺元和零元? 如有幺元, 每个元素是否有逆元? 如有, 求出逆元.

$*$	a	b	c
a	a	b	c
b	b	a	c
c	c	c	c

解: 这些运算性质可直接从运算表看出:

- $*$ 运算是封闭的, 因为表中每个元素都属于 A.
- $*$ 运算可交换, 因运算表关于主对角线对称.
- $*$ 运算不等幂, 因运算表主对角线有的元素与所在行列表头元素不同.
- $*$ 运算有零元 c, 因为 c 所在行列中的元素都是与它相同.
- $*$ 运算有幺元 a, 因为 a 所在行列中的元素依次与表头行列一致.
- a 和 b 均以自身为逆元, 因为 a, b 所在行和列交汇处的元素为幺元. 4.27

Example 32. 设 $\mathbb{N}_k = \{0, 1, 2, \cdots, k-1\}$, 在 $\mathbb{N}_k$ 定义运算 $+_k$ 如下: 对任意 $x, y \in \mathbb{N}_k$

$$x +_k y = \begin{cases} x + y, & x + y < k \\ x + y - k, & x + y \geqslant k \end{cases}$$

试分析 $\mathbb{N}_k$ 中的每个元素是否有逆元? 如有, 求出逆元.

解: 因为对任意 $x \in \mathbb{N}_k$, $x+0=x<k$, 所以

$$x +_k 0 = 0 +_k x = x + 0 = x,$$

故 0 是幺元.

对任意 $x \in \mathbb{N}_k$, 令 $x +_k y = 0$, 分两种情况讨论:

(1) 如果 $x+y<k$, 按运算 $+_k$ 的定义, 有 $x +_k y = x+y = 0$, 因 $x, y \in \mathbb{N}_k$, 可知 $x=y=0$, 因此 0 以自身为逆元;

(2) 如果 $x+y \geqslant k$, 则有 $x +_k y = x+y-k=0$, 解出 $y=k-x$. 即每个非 0 元
4.28 素 x 都有逆元 $k-x$. □

从运算表看运算的性质

对代数系统 $\langle A, *\rangle$, 其二元运算 $*$ 的性质可以根据运算表表现出来:

- *运算 $*$ 具有封闭性, 当且仅当运算表中的每个元素都属于 A.*
- *运算 $*$ 具有可交换性, 当且仅当运算表关于主对角线是对称的.*
- *运算 $*$ 具有等幂性, 当且仅当运算表的主对角线上的每一元素与它所在行 (列) 的表头元素相同.*
- *A 中关于运算 $*$ 具有零元, 当且仅当该元素所对应的行和列中的元素都与该元素相同.*
- *A 中关于运算 $*$ 具有幺元, 当且仅当该元素所对应的行和列依次与运算表的行和列相一致.*
- *设 A 中关于运算 $*$ 具有幺元, a 和 b 互逆, 当且仅当位于 a 所在行和 b 所*
4.29 *在列的元素及 b 所在行和 a 所在列的元素都是幺元.*

3 半群

广群 & 半群

Definition 33. 如果集合 S 上的二元运算 $*$ 是封闭的, 则称代数系统 $\langle S, *\rangle$ 为*广群* (groupoid). 也称为*群坯*.

Definition 34. 如果集合 S 上的二元运算 $*$ 是封闭的, 并且满足结合律, 则称代
4.30 数系统 $\langle S, *\rangle$ 为*半群* (semigroup).

Example 35. 设 $S=\{a, b, c\}$, 定义 S 上的运算 $*$ 如表所示, 验证 $\langle S, *\rangle$ 是否为半群.

$*$	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

解: 从运算可看出运算 $*$ 是封闭的.

另外 a, b, c 皆为左幺元, 所以, 对任意 $x, y, z \in S$, 均有

$$x*(y*z) = y*z = (x*y)*z$$

4.31 所以 $*$ 运算是可结合的. 从而 $\langle S, *\rangle$ 是半群. □

☞ 代数系统 $\langle \mathbb{N}^+, -\rangle$ 和 $\langle \mathbb{R}, /\rangle$ 是半群吗? 这里 $\mathbb{N}^+$ 为正整数集, $\mathbb{R}$ 为实数
4.32 集, $-$ 和 $/$ 是普通的减法和除法.

子半群

Theorem 36. 设 $\langle S, *\rangle$ 为一半群, $B \subseteq S$ 且 $*$ 在 B 上封闭, 那么 $\langle B, *\rangle$ 也是一个半群. 通常称 $\langle B, *\rangle$ 为 $\langle S, *\rangle$ 的子半群.

证明思路: 结合律在 B 上仍成立.

Example 37. 普通乘法运算在某些集合上构成 $\langle \mathbb{R}, \times\rangle$ 的子半群. 例如:

- $\langle [0, 1], \times\rangle$;
- $\langle [0, 1), \times\rangle$;
- $\langle \mathbb{Z}, \times\rangle$. 4.33

Theorem 38. 设 $\langle S, *\rangle$ 为一个半群, 如果 S 是一个有限集合, 则必有 $a \in S$, 使得 $a * a = a$.

证: 因 $\langle S, *\rangle$ 是半群, $\forall b \in S$, 由 $*$ 的封闭性可知

$$b * b \in S, \text{ 记 } b^2 = b * b$$

$$b^2 * b = b * b^2 \in S, \text{ 记 } b^3 = b^2 * b = b * b^2$$

$$\vdots$$

因 S 是一个有限集合, 所以 $\exists j > i$, 使

$$b^i = b^j$$

令 $p = j - i$, 即 $j = p + i$, 代入上式得 $b^i = b^p * b^i$

所以, $b^q = b^p * b^q$, $q \geqslant i$.

因为 $p \geqslant 1$, 所以 $\exists k \geqslant 1$, 使得

$$kp \geqslant i$$

对于 $b^{kp} \in S$, 有

$$\begin{aligned} b^{kp} &= b^p * b^{kp} \\ &= b^p * (b^p * b^{kp}) \\ &= b^{2p} * b^{kp} \\ &= b^{2p} * (b^p * b^{kp}) \\ &= \cdots \\ &= b^{kp} * b^{kp} \end{aligned}$$ 4.34

所以, 存在 $a = b^{kp}$, 使 $a * a = a$.

Definition 39. 含有幺元的半群, 称为独异点 (monoid), 或亚群, 含幺半群. 4.35

Theorem 40. 设 $\langle S, *\rangle$ 是一个独异点, 则在关于运算 $*$ 的运算表中任何两行或两列都是不相同的.

证: 设 S 中关于 $*$ 运算的幺元是 e. 4.36

$*$	$\cdots$	a	$\cdots$	b	$\cdots$
$\vdots$	$\cdots$	$\vdots$	$\cdots$	$\vdots$	$\cdots$
e	$\cdots$	a	$\cdots$	b	$\cdots$
$\vdots$	$\cdots$	$\vdots$	$\cdots$	$\vdots$	$\cdots$

$*$	$\cdots$	e	$\cdots$
$\vdots$	$\cdots$	$\vdots$	$\cdots$
a	$\cdots$	a	$\cdots$
$\vdots$	$\cdots$	$\vdots$	$\cdots$
b	$\cdots$	b	$\cdots$
$\vdots$	$\cdots$	$\vdots$	$\cdots$

$\forall a, b \in S$, 且 $a \neq b$ 时, 有

$$e * a = a \neq b = e * b, \tag{13}$$

$$a * e = a \neq b = b * e. \tag{14}$$

所以, 在 $*$ 的运算表中不可能有两行或两列是相同的. □

Example 41. 设 $\mathbb{Z}$ 是整数集合, m 是任意正整数, Z_m 是由模 m 的同余类组成的同余类集, 在 Z_m 上定义两个二元运算 $+_m$ 和 $\times_m$ 分别如下:

对于任意的 $[i], [j] \in Z_m$

$$[i] +_m [j] = \big[(i + j) \pmod m\big] \tag{15}$$

$$[i] \times_m [j] = \big[(i \times j) \pmod m\big] \tag{16}$$

试证明在这两个二元运算的运算表中任何两行或两列都是不相同的.

证: 考察代数系统 $\langle Z_m, +_m\rangle$ 和 $\langle Z_m, \times_m\rangle$, 先分三步证明 $\langle Z_m, +_m\rangle$ 是独异点, 再利用定理的结论:

(1) 证明两个运算在 Z_m 上封闭;
(2) 证明两个运算满足结合律;
(3) 证明 $[0]$ 是 $\langle Z_m, +_m\rangle$ 的幺元, $[1]$ 是 $\langle Z_m, \times_m\rangle$ 的幺元.

4.37 本例题的实例见表 5-3.2 和表 5-3.3.

Theorem 42. *设 $\langle S, *\rangle$ 是一个独异点, 对于任意 $a, b \in S$, 若 a, b 均有逆元, 则*

(1) $(a^{-1})^{-1} = a$;
(2) $a * b$ 有逆元, 且 $(a * b)^{-1} = b^{-1} * a^{-1}$.

证: ① 因 a^{-1} 和 a 为互为逆元, 直接得到结论.

② 必须证明两种情况:

$$(a * b) * (b^{-1} * a^{-1}) = e$$

和

$$(b^{-1} * a^{-1}) * (a * b) = e$$

4.38 利用结合律容易得出.

4 群与子群

群

Definition 43. 称代数系统 $\langle G, *\rangle$ 为群 (group), 如果

(1) 运算 $*$ 是封闭的.
(2) 运算 $*$ 是可结合的.
(3) 存在幺元 e.
(4) 每一元素 x 都有逆元 x^{-1}.

4.39 上述四个条件, 依次得到概念: 广群 $\longrightarrow$ 半群 $\longrightarrow$ 独异点 $\longrightarrow$ 群.

Example 44. 例如,

- $\langle \mathbb{Z}, +\rangle$, $\langle \mathbb{Q}^+, *\rangle$, $\langle \mathbb{R} - \{0\}, *\rangle$ 都是群, 这里, $+$ 和 $*$ 表示数的加法和乘法, $\mathbb{Z}$ 表示整数集, $\mathbb{Q}^+$ 表示正有理数集, $\mathbb{R}$ 表示实数集.
  - $\langle \mathbb{Z}, +\rangle$ 的幺元为 0, 逆元 $x^{-1} = -x$.
  - $\langle \mathbb{Q}^+, *\rangle$ 的幺元为 1, 逆元 $x^{-1} = 1/x$.

- $\langle R-\{0\},*\rangle$ 的幺元为 1, 逆元 $x^{-1}=1/x$.

- $\langle \mathbb{N},+\rangle$, $\langle \mathbb{R},*\rangle$ 不是群.
  - $\mathbb{N}$ 中除幺元 0 外, 其余元素无逆元.
  - $\mathbb{R}$ 中 0 无逆元.

4.40

Example 45. $R=\{0°,60°,120°,180°,240°,300°\}$, $\star$ 是 R 上的二元运算, $a\star b$ 表示先旋转 a 再旋转 b 的角度, 并规定旋转 360° 等于原来的状态. 验证 $\langle R,\star\rangle$ 是一个群.

$\star$	0°	60°	120°	180°	240°	300°
0°	0°	60°	120°	180°	240°	300°
60°	60°	120°	180°	240°	300°	0°
120°	120°	180°	240°	300°	0°	60°
180°	180°	240°	300°	0°	60°	120°
240°	240°	300°	0°	60°	120°	180°
300°	300°	0°	60°	120°	180°	240°

解: 验证 $\langle R,\star\rangle$ 满足

(1) 运算 $\star$ 封闭;
(2) 满足结合律: $(a\star b)\star c$ 和 $a\star(b\star c)$ 的旋转角度为 $a+b+c \pmod{360°}$.
(3) 有幺元 0°;
(4) 元素都有逆元: 60°, 120°, 180° 分别与 300°, 240°, 180° 互逆. □

4.41

有限群, 有限群的阶数, 无限群

Definition 46. 设 $\langle G,*\rangle$ 是一个群.

- 若 G 为有限集, 则称 $\langle G,*\rangle$ 为*有限群* (finite group); 此时 G 的元素个数称为该有限群的*阶数* (order), 记为 $|G|$.
- 若 G 为无限集, 称 $\langle G,*\rangle$ 为*无限群* (infinite group).

4.42

Theorem 47. *群中不可能有零元.*

证: 设 $\langle G,*\rangle$ 为群.
① 当群的阶为 1 时, 它的惟一元素视作幺元 e.
② 设 $|G|>1$ 且群有零元 θ. 那么群中任何元素 $x\in G$, 都有

$$x*\theta=\theta*x=\theta\neq e.$$

所以, 零元 θ 就不存在逆元, 与 $\langle G,*\rangle$ 是群的假设矛盾. □

4.43

Theorem 48. *设 $\langle G,*\rangle$ 为群, 对于 $a,b\in G$, 必存在 $x\in G$, 使得关于 x 的方程 $a*x=b$, $x*a=b$ 都有惟一解.*

证: ① 先证解的存在性.
设 a 的逆元 a^{-1}, 令

$$x=a^{-1}*b, \qquad \text{(构造一个解)}$$

则

$$\begin{aligned} a*x &= a*(a^{-1}*b) \\ &= (a*a^{-1})*b \\ &= e*b \\ &= b. \end{aligned}$$

证: ② 再证解惟一性.

若另有解 x_1 满足 $a*x_1=b$, 则

$$a^{-1}*(a*x_1)=a^{-1}*b$$

即

$$x_1=a^{-1}*b. \qquad \square$$

4.44

Theorem 49. *设 $\langle G,*\rangle$ 为群, 那么, 对任意 $a,\ x,\ y\in G$,*

$$a*x=a*y\Rightarrow x=y \tag{17}$$

$$x*a=y*a\Rightarrow x=y \tag{18}$$

因此, 群中消去律成立.

证: 设 $a*x=a*y$, 且 a 的逆元是 a^{-1}, 则有

$$\begin{aligned} a^{-1}*(a*x) &= a^{-1}*(a*y) \\ (a^{-1}*a)*x &= (a^{-1}*a)*y \qquad \text{(结合律)} \\ e*x &= e*y \\ x &= y. \end{aligned}$$

4.45 同理可证 (18) 式. $\square$

置换

Definition 50. 设 S 是一个非空集合, 从集合 S 到 S 的一个双射称为 S 的一个*置换*.

Example 51. 设 $S=\{a,\ b,\ c,\ d\}$. $f:S\longmapsto S$, $f(a)=b$; $f(b)=d$; $f(c)=a$; $f(d)=c$. 这个置换可以表示成如下形式:

$$\begin{pmatrix} a & b & c & d \\ b & d & a & c \end{pmatrix}$$

4.46

Theorem 52. *设 $\langle G,*\rangle$ 为群, 那么, 运算表中的每一行或每一列都是群 G 的元素的置换.*

证: 先证运算表中的任一行或任一列所含 G 中的一个元素不可能多于一次.

用反证法: 设 $a\in G$ 对应的行有两个元素都是 c, 即

$$a*b_1=a*b_2=c,\quad 且\ b_1\neq b_2.$$

$*$	$\cdots$	b_1	$\cdots$	b_2	$\cdots$
$\vdots$	$\cdots$	$\vdots$	$\cdots$	$\vdots$	$\cdots$
a	$\cdots$	c	$\cdots$	c	$\cdots$
$\vdots$	$\cdots$	$\vdots$	$\cdots$	$\vdots$	$\cdots$

由消去律得 $b_1 = b_2$. 这与 $b_1 \neq b_2$ 矛盾.

再证 G 中每一个元素必出现一次.

证: 考察对应于元素 $a \in G$ 的那一行, 设 b 是 G 中的任意一个元素, 则 $a^{-1} * b \in G$, 它必出现在运算表的顶行.

$*$	$\cdots$	$a^{-1} * b$	$\cdots$
$\vdots$	$\cdots$	$\vdots$	$\cdots$
a	$\cdots$	b	$\cdots$
$\vdots$	$\cdots$	$\vdots$	$\cdots$

由于

$$b = a * (a^{-1} * b),$$

所以 b 必定出现在运算表中对应于 a 的那一行.

综上得出: $\langle G, * \rangle$ 的运算表中每一行都是 G 的元素的一个置换, 且每一行都是不同的. 对于列的证明类似. □ 4.47

等幂元

Definition 53. 代数系统 $\langle G, * \rangle$ 中, 如果存在 $a \in G$, 有 $a * a = a$, 则称 a 为运算 $*$ 的等幂元.

4.48

等幂元

Theorem 54. *在群 $\langle G, * \rangle$ 中, 除幺元 e 之外, 不可能有任何别的等幂元.*

证: 因为 $e * e = e$, 所以 e 是等幂元.

现设 $a \in G$, $a \neq e$ 且 $a * a = a$, 则有

$$\begin{aligned} a &= e * a \\ &= (a^{-1} * a) * a \\ &= a^{-1} * (a * a) \\ &= a^{-1} * a && (\text{已假设 } a * a = a) \\ &= e. \end{aligned}$$

与假设 $a \neq e$ 相矛盾. □ 4.49

子群

Definition 55. 设 $\langle G, *\rangle$ 是群, $S \subseteq G$, S 非空. 如果 $\langle S, *\rangle$ 也是群, 则称 $\langle S, *\rangle$ 为 $\langle G, *\rangle$ 的*子群* (subgroup).

Definition 56. 设 $\langle G, *\rangle$ 为群, $\langle S, *\rangle$ 为 G 的子群, 如果 $S = \{e\}$ 或 $S = G$, 那么称 $\langle S, *\rangle$ 为 $\langle G, *\rangle$ 的*平凡子群*.

☞ 简言之, $\langle \{e\}, *\rangle$ 和 $\langle G, *\rangle$ 是群 $\langle G, *\rangle$ 的两个平凡子群.

G 还可能有其它的子群, 称为 G 的真子群. 例如, 偶数全体构成整数加群的
4.50 一个真子群.

Example 57. $\langle \mathbb{Z}, +\rangle$ 是一个群, 设 $\mathbb{Z}_E = \{x \mid x = 2n, n \in \mathbb{Z}\}$, 证明 $\langle \mathbb{Z}_E, +\rangle$ 是 $\langle \mathbb{Z}, +\rangle$ 的一个子群.

证: 本题的实质是要证明 $\langle \mathbb{Z}_E, +\rangle$ 是群. 按群的定义证明如下:

(1) 证明 $+$ 运算在 $\mathbb{Z}_E$ 上封闭: 任取 $x, y \in \mathbb{Z}_E$, 可设 $x = 2n_1$, $y = 2n_2$, 其中 $n_1, n_2 \in \mathbb{Z}$. 那么 $x + y = 2(n_1 + n_2) \in \mathbb{Z}_E$, 故运算封闭.

(2) 因 $+$ 运算在 $\mathbb{Z}$ 上可结合, 而 $+$ 运算在 $\mathbb{Z}_E$ 上封闭, 所以, $+$ 运算在 $\mathbb{Z}_E$ 上可结合.

(3) 因 $\langle \mathbb{Z}, +\rangle$ 的幺元 0 在 $\mathbb{Z}_E$ 中, 所以 $\langle \mathbb{Z}_E, +\rangle$ 有幺元 0.

(4) 对任意 $x = 2n \in \mathbb{Z}_E$, 有 $2n + 2(-n) = 0$, 而 $-n \in \mathbb{Z}$, 即 $2(-n) \in \mathbb{Z}_E$. 这说明 $\mathbb{Z}_E$ 中的任意元素有逆元.

4.51 所以 $\langle \mathbb{Z}_E, +\rangle$ 是群, 又因 $\mathbb{Z}_E \subseteq \mathbb{Z}$, 所以 $\langle \mathbb{Z}_E, +\rangle$ 是群 $\langle \mathbb{Z}, +\rangle$ 的子群. □

Theorem 58. *设 $\langle G, *\rangle$ 为群, $\langle S, *\rangle$ 为 $\langle G, *\rangle$ 的子群, 那么, $\langle G, *\rangle$ 中的幺元 e 必定也是 $\langle S, *\rangle$ 中的幺元.*

证: 已知 $\langle G, *\rangle$ 中的幺元 e, 设 $\langle S, *\rangle$ 中的幺元为 e_1.

对于任意一个元素 $x \in S \subseteq G$, 必有

$$e_1 * x = x = e * x.$$

则由消去律有,

$$e_1 = e.$$

□

4.52

Theorem 59. *设 $\langle G, *\rangle$ 为群, S 为 G 的非空子集, 如果对于任意元素 $a, b \in S$, 有 $a * b^{-1} \in S$, 则 $\langle S, *\rangle$ 必定是 $\langle G, *\rangle$ 的子群.*

证: 分四步证明:

(1) 先证 G 中的幺元 e 也是 S 中的幺元:

对任意元素 $a \in S \subseteq G$, $e = a * a^{-1} \in S$ 且 $a * e = e * a = a$, 即 e 也是 S 中的幺元.

(2) 其次证 S 中的每一个元素都有逆元:

对任意元素 $a \in S$ 中, 因为 $e \in S$, 所以 $e * a^{-1} \in S$, 即 $a^{-1} \in S$.

(3) 然后证明 $*$ 在 S 中是封闭的:

对任意元素 $a, b \in S$, $b^{-1} \in S$, 而 $b = (b^{-1})^{-1}$. 所以

$$a * b = a * (b^{-1})^{-1} \in S. \tag{19}$$

(4) 结合律是保持的.

因此, $\langle S, * \rangle$ 是 $\langle G, * \rangle$ 的子群. □ 4.53

Theorem 60. *设 $\langle G, * \rangle$ 为群, B 为 G 的非空子集, 如果 B 是一个有限集, 那么, 只要运算 $*$ 在 B 上封闭, $\langle B, * \rangle$ 必定是 $\langle G, * \rangle$ 的子群.*

证: 先证幺元的存在性.

设任意元素 $b \in B$, 若 $*$ 在 B 上封闭, 则元素 $b^2 = b*b$, $b^3 = b^2*b$, $b^4 = b^3*b$, $\cdots$, 都在 B 中.

由于是有限集, 所以必存在正整数 i 和 j $(i < j)$, 使得

$$b^i = b^j, \quad 即\ b^i = b^i * b^{j-i}. \tag{20}$$

可见 $e = b^{j-i}$ 是 $\langle G, * \rangle$ 中的幺元, 且该幺元也在子集 B 中.

再证任意 $b \in B$ 存在逆元.

如果 $j - i > 1$, 则由 $e = b^{j-i} = b * b^{j-i-1}$, 可知 b^{j-i-1} 是 b 的逆元, 且 $b^{j-i-1} \in B$;

如果 $j - i = 1$, 则 (20) 式为 $b^i = b^i * b$, 可知 b 是幺元, 而幺元是以自身为逆元的.

综上, $\langle B, * \rangle$ 是 $\langle G, * \rangle$ 的一个子群. □ 4.54

5 阿贝尔群和循环群

阿贝尔群

Definition 61. 如果群 $\langle G, * \rangle$ 中的二元运算 $*$ 是可交换的, 则称该群为*阿贝尔群* (Abelian group), 也叫*交换群* (commutative group).

4.55

Example 62. 证明 1, 2, 3, 4 阶群都是交换群.

解: 群 $\langle G, * \rangle$ 的运算表中的每行 (列) 都是 G 中元素的一个置换. 因此很容易得出 1, 2, 3, 4 阶群的运算表, 不论其元素是什么, 只要它们构成群, 其群表的形式是固定不变的.

$*$	1
1	1

$*$	1	2
1	1	2
2	2	1

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

由群表可知, 1, 2, 3, 4 阶群都是交换群. 4.56

四阶群 $\langle \{1, 2, 3, 4\}, * \rangle$ 的群表有四种形式:

*	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

*	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

*	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	2	1
4	4	3	1	2

*	1	2	3	4
1	1	2	3	4
2	2	3	4	1
3	3	4	1	2
4	4	1	2	3

4.57

Theorem 63. *群 $\langle G, *\rangle$ 是阿贝尔群的充分必要条件是: 对任意 $a, b \in G$, 有*

$$(a*b)*(a*b) = (a*a)*(b*b). \tag{21}$$

证: 充分性. 对任意 $a, b \in G$, 如果 $(a*b)*(a*b) = (a*a)*(b*b)$, 那么,

$$a^{-1}*(a*b)*(a*b)*b^{-1} = a^{-1}*(a*a)*(b*b)*b^{-1},$$

$$(a^{-1}*a)*(b*a)*(b*b^{-1}) = (a^{-1}*a)*(a*b)*(b*b^{-1}), \qquad \text{(结合律)}$$

$$b*a = a*b.$$

这说明 $*$ 运算是可交换的.

必要性. 若群 $\langle G, *\rangle$ 是交换群, 则对任意 $a, b \in G$, 有

$$\begin{aligned}(a*b)*(a*b) &= a*(b*a)*b \\ &= a*(a*b)*b \\ &= (a*a)*(b*b).\end{aligned}$$

□

4.58

幂 (乘方)

- 在一个群 $\langle G, *\rangle$ 里, 结合律是成立的. 所以
$$a_1 * a_2 * \cdots * a_n$$
有意义, 是 G 的某一个元.
- $a*a*\cdots*a$ 当然也是 G 的一个元, 记为
$$\underbrace{a*a*\cdots*a}_{n\text{个}} = a^n, \quad n \text{ 是正整数}.$$
叫做 a 的 n 次幂 (或 n 次方). 并且规定
$$a^0 = e, \tag{22}$$
$$a^{-n} = (a^{-1})^n, \quad (n \text{ 是正整数}). \tag{23}$$
- 对任意的整数 n, m 容易算出
$$a^n * a^m = a^{n+m}, \tag{24}$$
$$(a^n)^m = a^{nm}. \tag{25}$$

4.59

循环群

Definition 64. 如果群 $\langle G, * \rangle$ 有元素 a, 使得 G 中任意元素都可表示成 a 的幂, 即

$$G = \{a^k \mid k \text{ 为任意整数}\}. \tag{26}$$

则称该群为循环群 (cyclic group). a 称为循环群 G 的 生成元.

Example 65. 所有复数

$$e^{\frac{2k\pi i}{n}} = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, \quad (k = 0, 1, 2, \ldots, n-1) \tag{27}$$

作为一个 n 阶有限循环群, $e^{\frac{2\pi i}{n}}$ 是它的一个生成元. 4.60

Example 66. 全体整数的集合 $\mathbb{Z}$ 关于普通加法构成一个群, 我们把它称为整数加群. 试说明整数加群 $\langle \mathbb{Z}, + \rangle$ 是循环群.

解: 群 $\langle \mathbb{Z}, + \rangle$ 的幺元是 0. 任意 $a \in \mathbb{Z}$, 其逆元为 $-a$.

这个群的全体的元都是 1 的乘方. (假如把 $\mathbb{Z}$ 的代数运算不用 $+$ 而用 $*$ 来表示, 就很容易明白了.)

假定 m 是任意正整数, 则

$$m = \underbrace{1 + 1 + \cdots + 1}_{m} = \underbrace{1 * 1 * \cdots * 1}_{m} = 1^m$$

所以, 对任意 $m \in \mathbb{Z}$, 有

$$m = \begin{cases} \underbrace{1 + 1 + \cdots + 1}_{m} = 1^m, & m > 0, \\ 0 = 1^0, & m = 0, \\ \underbrace{(-1) + (-1) + \cdots + (-1)}_{|m|} = (-1)^{|m|} = (1^{-1})^{|m|} = 1^m, & m < 0. \end{cases} \quad \square$$

4.61

Example 67. 设 $G = \{\alpha, \beta, \gamma, \delta\}$, 定义 G 上的运算 $*$ 如下表, 说明 $\langle G, * \rangle$ 是循环群.

$*$	α	β	δ	γ
α	α	β	δ	γ
β	β	α	γ	δ
δ	δ	γ	β	α
γ	γ	δ	α	β

(1) 由运算表可知运算封闭;
(2) 可验证运算 $*$ 是可结合的;
(3) α 是幺元;
(4) β, γ, δ 的逆元分别是 β, δ, γ.

所以, $\langle G, * \rangle$ 是群.

γ, δ 都是生成元:

$$\begin{aligned}
&\gamma^1 = \gamma, \quad \gamma^2 = \beta,\\
&\gamma^3 = \beta * \gamma = \delta,\\
&\gamma^4 = \delta * \gamma = \alpha;\\
&\delta^1 = \delta, \quad \delta^2 = \beta,\\
&\delta^3 = \beta * \delta = \gamma,\\
&\delta^4 = \gamma * \delta = \alpha.
\end{aligned}$$

β 不是生成元:

$$\begin{aligned}
&\beta^1 = \beta, \quad \beta^2 = \alpha,\\
&\beta^3 = \alpha * \beta = \beta,\\
&\beta^4 = \beta * \beta = \beta^2 = \alpha.
\end{aligned}$$

□

4.62

Theorem 68. *循环群是阿贝尔群.*

证: 设 $\langle G, *\rangle$ 是循环群, 生成元是 a.

对任意 $x, y \in G$, 可令 $x = a^r$, $y = a^s$. r, s 为整数. 那么

$$\begin{aligned}
x * y &= a^r * a^s\\
&= a^{r+s}\\
&= a^{s+r}\\
&= a^s * a^r\\
&= y * x.
\end{aligned}$$

4.63 交换律满足, 这就证明了循环群 $\langle G, *\rangle$ 是阿贝尔群. □

Theorem 69. *设 a 是 n 阶有限循环群 $\langle G, *\rangle$ 的生成元, 则 $a^n = e$, 且*

$$G = \{a, a^2, a^3, \cdots, a^{n-1}, a^n = e\}$$

其中, e 是幺元, n 是使 $a^n = e$ 的最小正整数. (称 n 为元素 a 的阶.)

证: (用反证法) 假定 $a^m = e$, m 是正整数, 且 $m < n$.

按所设, G 中任一元素皆可表示成 a^k, 令 $k = mg + r$, 其中 g 是整数, $0 \leqslant r < m$. 于是

$$a^k = a^{mg+r} = (a^m)^g * a^r = a^r$$

这说明 G 中任一元素皆可表示成 a^r, 从而 G 中至多只有 m 个不同的元素, 与 $|G| = n(> m)$ 矛盾.

剩下的问题是要证明 $a, a^2, a^3, \cdots, a^{n-1}, a^n$ 是不同的元素.

假设 $a^i = a^j$, $1 \leqslant i < j \leqslant n$, 那么

$$e = a^i * a^{-i} = a^j * a^{-i} = a^{j-i}, 1 \leqslant j - i < n.$$

4.64 按假设, n 是使 $a^n = e$ 的最小正整数, 所以 $a^i = a^j$ 不可能. □

有限循环群的典型例子

整数集合 $\mathbb{Z}$ 按同余关系 $R = \{\langle a, b\rangle \mid a \equiv b \pmod{n}\}$, 划分为 n 个等价类 (模 n 的**剩余类**):

$$[0] = \{\cdots, -2n, -n, \boxed{0}, n, 2n, \cdots\}; \tag{28}$$

$$[1] = \{\cdots, -2n+1, -n+1, \boxed{1}, n+1, 2n+1, \cdots\}; \tag{29}$$

$$\cdots\cdots$$

$$[n-1] = \{\cdots, -n-1, -1, \boxed{n-1}, 2n-1, 3n-1, \cdots\}. \tag{30}$$

令 $G = \{[0], [1], [2], \cdots, [n-1]\}$, 规定 "加法" 运算:

$$[a] \oplus [b] = [a+b] \tag{31}$$

则 $\langle G, \oplus\rangle$ 是一个群 (**模 n 的剩余类加群**). 4.65

有限循环群的典型例子

$\oplus$	$[0]$	$[1]$	$\cdots$	$[n-2]$	$[n-1]$
$[0]$	$[0]$	$[1]$	$\cdots$	$[n-2]$	$[n-1]$
$[1]$	$[1]$	$[2]$	$\cdots$	$[n-1]$	$[0]$
$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$
$[n-1]$	$[n-1]$	$[0]$	$\cdots$	$[n-3]$	$[n-2]$

易见 G 的幺元 $e = [0]$, 且 $[1]$ 是 G 的一个生成元.

任意 $[i] \in G$, 有

$$[i] = \underbrace{[1] \oplus [1] \oplus \cdots \oplus [1]}_{i} \triangleq [1]^i,$$

显然,

$$\boxed{G = \{[1], [1]^2, [1]^3, \cdots, [1]^{n-1}, [1]^n = [0] = e\}.}$$

4.66

Example 70. 设 G 刚好包含 $x^3 = 1$ 的三个根:

$$1, \qquad \varepsilon_1 = \frac{-1+\sqrt{-3}}{2}, \qquad \varepsilon_2 = \frac{-1-\sqrt{-3}}{2}.$$

对于普通乘法来说, G 构成一个群. 为什么? 是循环群吗?

解: ① $\langle G, \times\rangle$ 是一个群:

(1) 运算封闭. 注意, 其中

$$\varepsilon_1^2 = \frac{1+(-3)-2\sqrt{-3}}{4} = \frac{-1-\sqrt{-3}}{2} = \varepsilon_2, \quad \varepsilon_2^2 = \varepsilon_1.$$

(2) 满足结合律.

(3) 幺元是 1.

(4) 逆元存在: ε_1 与 ε_2 互逆; 幺元 1 的逆元是自己.

② 是循环群: ε_1 与 ε_2 都是生成元. □

可见, 循环群的生成元可以是不惟一的. 4.67

7 陪集和拉格朗日定理

培集与拉格朗日定理

这一节的主要内容是利用群 G 的一个子群 H 来作一个分类, 并得到相应的定理.

4.68

相关的定义和结论, 都可以用 “整数的模 n 剩余类加群” 作为原型来理解.

培集

Definition 71. 设 $\langle H, *\rangle$ 为 $\langle G, *\rangle$ 的子群, $a \in G$. 集合

$$aH \triangleq \{a * h \mid h \in H\}, \tag{32}$$

$$Ha \triangleq \{h * a \mid h \in H\}, \tag{33}$$

分别称为由 a 确定的 H 在 G 中的*左陪集*和*右陪集*.

a 称为代表元素.

注

- 群的每个子集不见得都是群. 子群的陪集是群论中的一个重要内容, 由这一概念可以引导出一个重要结果, 即拉格朗日定理. 它指出群与其子群之间存在的一个重要关系.
- 这里只就左陪集进行讨论, 右陪集也有类似的结论.

4.69

Theorem 72 (拉格朗日定理)**.** *设 $\langle H, *\rangle$ 为 $\langle G, *\rangle$ 的子群, $a, b \in G$, 那么*

(1) $R = \{\langle a, b\rangle \mid a \in G, b \in G$ 且 $a^{-1} * b \in H\}$ 是 G 中的一个等价关系. 对于 $a \in G$, 若记 $[a]_R = \{x \mid x \in G$ 且 $\langle a, x\rangle \in R\}$, 则

$$[a]_R = aH \tag{34}$$

(2) 如果 $\langle G, *\rangle$ 为有限群, $|G| = n$, $|H| = m$, 那么 $m|n$ (即 H 的阶整除 G 的阶).

证: ① 先证关系 R 是等价关系.

- 关系 R 是自反的:

  对于任意 $a \in G$, 必有 $a^{-1} \in G$, 使

  $$a^{-1} * a = e \in H.$$

  所以 $\langle a, a\rangle \in R$.

4.70

$R = \{\langle a, b\rangle \mid a \in G, b \in G$ 且 $a^{-1} * b \in H\}$

- 关系 R 是对称的:

  若 $\langle a, b\rangle \in R$. 则 $a^{-1} * b \in H$, 因为 H 是 G 的子群, 故

  $$(a^{-1} * b)^{-1} = b^{-1} * a \in H$$

  所以, $\langle b, a\rangle \in R$.

- 关系 R 是传递的:

  若 $\langle a, b\rangle \in R$, $\langle b, c\rangle \in R$. 则 $a^{-1} * b \in H$, $b^{-1} * c \in H$, 所以

  $$a^{-1} * b * b^{-1} * c = a^{-1} * c \in H$$

  则 $\langle a, c\rangle \in R$.

对于 $a \in G$, 有 $b \in [a]_R \Leftrightarrow \langle a, b\rangle \in R \Leftrightarrow a^{-1} * b \in H \Leftrightarrow b \in aH$. 因此

$$[a]_R = aH.$$

4.71

拉格朗日定理

② 由于 R 是 G 中的一个等价关系, 所以必定将 G 划分成不同的等价类 $[a_1]_R$, $[a_2]_R$, $\cdots$, $[a_k]_R$, 使得

$$G = \bigcup_{i=1}^{k} [a_i]_R = \bigcup_{i=1}^{k} a_i H \qquad (a_i \in G)$$

若 $h_1, h_2 \in H$, 且 $h_1 \neq h_2$, $a \in G$, 那么 $a * h_1 \neq a * h_2$. 所以

$$|a_i H| = |H| = m, \quad i = 1, 2, \cdots, k.$$

因此

$$n = |G| = \left| \bigcup_{i=1}^{k} a_i H \right| = \sum_{i=1}^{k} |a_i H| = k \cdot m.$$

所以 H 阶的整除 G 的阶, 即 $m|n$. □ 4.72

拉格朗日定理的推论

推论 1

任何质数阶[1]的群不可能有非平凡子群.

证: (反证法) 假设质数阶群 $\langle G, * \rangle$ 有非平凡子群 $\langle H, * \rangle$.

根据拉格朗日定理, 则 $|H|(1 < |H| < |G|)$ 是 $|G|$ 的因子, 与 $|G|$ 为质数矛盾. □ 4.73

推论 2

设 $\langle G, * \rangle$ 为 n 阶有限群, e 是群 $\langle G, * \rangle$ 的幺元. 那么

(1) 对于任意 $a \in G$, a 的阶[2] 必是 n 的因子, 且必有 $a^n = e$;

(2) 如果 n 为质数, 则 $\langle G, * \rangle$ 必是循环群.

证: ① 若 $a \in G$, a 的阶数为 m, 则循环群 $\langle \{a, a^2, \cdots, a^m\}, * \rangle$ 是 G 的子群.

根据拉格朗日定理, $m|n$. 令 $n = mk$, 则

$$a^n = a^{mk} = (a^m)^k = e^k = e.$$

② 令 $\langle G', * \rangle = \langle \{a, a^2, \cdots, a^m\}, * \rangle$, 则 G' 是 G 的循环子群.

如前述, m 是 n 的一个因子, 已知 n 为质数, 故 $n = m$, 或 $m = 1$.

- 若 $n = m$, 则 $G = G'$. G' 是循环群, 所以 G 是循环群.
- 若 $m = 1$, 则 $a = e$, 而 a 是 G 中的任意一个元素, 所以 $G = \{e\}$, 是循环群. □ 4.74

Example 73. 在 $X = \mathbb{R} - \{0, 1\}$ 定义 6 个函数:

$$f_1(x) = x; \qquad f_2(x) = x^{-1}; \qquad f_3(x) = 1 - x;$$
$$f_4(x) = (1-x)^{-1}; \quad f_5(x) = (x-1)x^{-1}; \quad f_6(x) = x(x-1)^{-1}.$$

则 $\langle F, \circ \rangle$ 是群, 这里 $F = \{f_1, f_2, f_3, f_4, f_5, f_6\}$, “ $\circ$” 是函数的复合运算. 试求 $\langle F, \circ \rangle$ 的所有子群.

解: 先写出运算表.

[1]质数, 即素数: 大于 1 而无真因数的自然数.

[2]元素 a 的阶, 是满足 $a^t = e$ 的最小正整数 t.

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_4	f_3	f_6	f_5
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_2	f_5	f_1	f_3
f_5	f_5	f_3	f_6	f_1	f_4	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

比如,

$$\begin{aligned} f_2\big(f_3(x)\big) &= \big(f_3(x)\big)^{-1} \\ &= (1-x)^{-1} \\ &= f_4(x), \end{aligned}$$

所以 $f_2 \circ f_3 = f_4$. 再如,

$$\begin{aligned} f_3\big(f_2(x)\big) &= 1 - f_2(x) \\ &= 1 - x^{-1} \\ &= (x-1)x^{-1} \\ &= f_5(x), \end{aligned}$$

所以 $f_3 \circ f_2 = f_5$. 因 $|F| = 6$, $\langle F, \circ \rangle$ 的子群只能是 $1, 2, 3, 6$ 阶群.

- 平凡子群: $\langle \{f_1\}, \circ \rangle$, $\langle F, \circ \rangle$.
- 2 阶子群: $\langle \{f_1, f_2\}, \circ \rangle$, $\langle \{f_1, f_3\}, \circ \rangle$, $\langle \{f_1, f_6\}, \circ \rangle$.
- 3 阶子群:$\langle \{f_1, f_4, f_5\}, \circ \rangle$.

注意这里

- f_1 是幺元;
- f_2, f_3, f_6 的阶为 2;
- f_4, f_5 的阶为 3. □

4.75

Example 74. (续前例) 令 $H = \{f_1, f_4, f_5\}$, $\langle H, \circ \rangle$ 是 $\langle F, \circ \rangle$ 的子群. 求 $F = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ 中的各元素所确定的 H 在 F 中的所有左陪集.

$$\begin{aligned} f_1H &= \{f_1, f_4, f_5\}, & f_2H &= \{f_2, f_3, f_6\}, \\ f_3H &= \{f_2, f_3, f_6\} = f_2H, & f_4H &= \{f_1, f_4, f_5\} = f_1H, \\ f_5H &= \{f_1, f_4, f_5\} = f_1H, & f_6H &= \{f_2, f_3, f_6\} = f_2H. \end{aligned}$$

从此例看到,

- 由群 $\langle F, \circ \rangle$ 的子群 $\langle H, \circ \rangle$ 所确定的所有不同左陪集 $(\{f_1, f_4, f_5\}, \{f_2, f_3, f_6\})$ 中只有一个是子群;
- 任意两个左陪集要么相等, 要么相交为空. □

4.76

8 同态与同构

Example 75. 设 α, β, γ 是带正电荷的粒子, δ, ε 是中性粒子, ζ 是带负电荷的粒子, 下表描述了这些粒子间相互作用的结果:

$\otimes$	α	β	γ	δ	ε	ζ
α	α	β	α	α	γ	δ
β	β	α	γ	β	γ	ε
γ	α	γ	α	β	γ	ε
δ	α	β	β	δ	ε	ζ
ε	γ	γ	γ	ε	ε	ζ
ζ	δ	ε	ε	ζ	ζ	ζ

令 $A = \{\alpha, \beta, \gamma, \delta, \varepsilon, \zeta\}$, 则 $\langle A, \otimes\rangle$ 是一个代数系统.

$*$	1	0	-1
1	1	1	0
0	1	0	-1
-1	0	-1	-1

如果只考虑带电粒子的正负特性, 则这些粒子相互作用的结果可用另一个系统 $\langle B, *\rangle$ ($B = \{1, 0, -1\}$) 概括地描述. 建立从 A 到 B 的映射 f,

$$f(x) = \begin{cases} 1, & x \in \{\alpha, \beta, \gamma\}, \\ 0, & x \in \{\delta, \varepsilon\}, \\ -1, & x \in \{\zeta\}. \end{cases}$$

对任意 $a_1, a_2 \in A$, 有

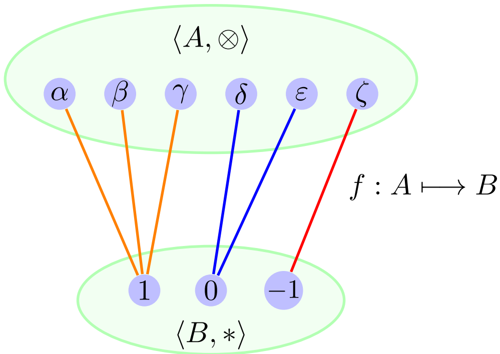
$$f(a_1 \otimes a_2) = f(a_1) * f(a_2)$$

例如, $f(\beta \otimes \zeta) = f(\varepsilon) = 0$, $f(\beta) * f(\zeta) = 1 * (-1) = 0$. 所以,

$$f(\beta \otimes \zeta) = f(\beta) * f(\zeta).$$

这时, 称 f 为代数系统 $\langle A, \otimes\rangle$ 到 $\langle B, *\rangle$ 的一个同态. 4.77

$f(\alpha) = f(\beta) = f(\gamma) = 1$, $f(\delta) = f(\varepsilon) = 0$, $f(\zeta) = -1$:



例如,

$$\beta \otimes \zeta = \varepsilon, \quad 1 * (-1) = 0;$$

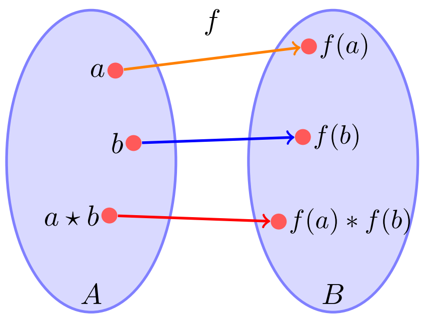
$$f(\beta \otimes \zeta) = f(\varepsilon) = 0 = 1 * (-1) = f(\beta) * f(\zeta).$$

4.78

同态

Definition 76. 设 $\langle A, \star \rangle$ 和 $\langle B, * \rangle$ 是两个代数系统, $\star$ 和 $*$ 分别是 A 和 B 上的二元运算. 如果存在映射 $f : A \longmapsto B$, 对任意 $a_1, a_2 \in A$, 有

$$f(a_1 \star a_2) = f(a_1) * f(a_2) \tag{35}$$



(1) 称 f 是 $\langle A, \star \rangle$ 到 $\langle B, * \rangle$ 的一个同态映射 (homomorphism), 简称同态;
(2) 称 $\langle A, \star \rangle$ 同态于 $\langle B, * \rangle$, 记作 $A \sim B$;
(3) 称 $\langle f(A), * \rangle$ 为 $\langle A, \star \rangle$ 的一个同态象 (image under homomorphism). 其中

$$f(A) = \{x \mid x = f(a), \, a \in A\} \subseteq B. \tag{36}$$

4.79

同态

<u>注</u>

- 普通的映射讨论的是两个集合 A 和 B 的关系;
- 同态讨论的是与代数运算也发生关系的映射. 即两个代数系统之间的联系.
- 若 f 是 $\langle A, \star \rangle$ 到 $\langle B, * \rangle$ 的一个同态映射, 则任意 $a_1, a_2 \in A$, 只要

$$a_1 \longrightarrow b_1, \qquad a_2 \longrightarrow b_2, \tag{37}$$

  就有

$$a_1 \star a_2 \longrightarrow b_1 * b_2. \tag{38}$$

4.80

Example 77. 记 $B = \{1, -1\}$. 对代数系统 $\langle \mathbb{Z}, + \rangle$ 和 $\langle B, \times \rangle$ (普通的加法和乘法),

(1) f_1: $\quad a \longrightarrow 1, \quad (a$ 是 $\mathbb{Z}$ 的任一元)

是一个 $\mathbb{Z}$ 到 B 的同态映射. 因为任意 $a_1, a_2 \in \mathbb{Z}$, 有

$$a_1 \longrightarrow 1, \qquad a_2 \longrightarrow 1,$$
$$a_1 + a_2 \longrightarrow 1 = 1 \times 1.$$

(2) f_2: $\quad a \longrightarrow +1, \quad$ (若 a 是偶数)
$\quad a \longrightarrow -1, \quad$ (若 a 是奇数)

则 f_2 是一个 $\mathbb{Z}$ 到 B 的 (满射的) 同态映射. 例如, 若 a_1 奇, a_2 偶, 则

$$a_1 \longrightarrow -1, \qquad a_2 \longrightarrow +1,$$
$$a_1 + a_2 \longrightarrow -1 = (-1) \times (+1).$$

4.81 ☞ 同态映射可能不惟一.

(a) $\langle A, \star \rangle$

$\star$	a	b
a	a	b
b	b	a

(b) $\langle B, \oplus \rangle$

$\oplus$	偶	奇
偶	偶	奇
奇	奇	偶

(c) $\langle C, * \rangle$

$*$	0°	180°
0°	0°	180°
180°	180°	0°

同构

Definition 78. 设 f 是 $\langle A, \star \rangle$ 到 $\langle B, * \rangle$ 一个同态,

(1) 如果 f 是 A 到 B 的满射, 则称 f 是 $\langle A, \star \rangle$ 到 $\langle B, * \rangle$ 满同态 (或同态满射).

(2) 如果 f 是 A 到 B 的入射 (即单射), 则称 f 是 $\langle A, \star \rangle$ 到 $\langle B, * \rangle$ 单一同态.

(3) 如果 f 是 A 到 B 的双射 (即一一映射), 则称 f 为同构映射, 并称 $\langle A, \star \rangle$ 与 $\langle B, * \rangle$ 同构 (isomorphism), 记作 $A \cong B$. 4.82

Example 79. 设 $A = \{1, 2, 3\}$, $\overline{A} = \{4, 5, 6\}$. A 与 $\overline{A}$ 的代数运算 $\star$ 与 $*$ 分别为

$\star$	1	2	3
1	3	3	3
2	3	3	3
3	3	3	3

$*$	4	5	6
4	6	6	6
5	6	6	6
6	6	6	6

那么
$$1 \longrightarrow 4, \quad 2 \longrightarrow 5, \quad 3 \longrightarrow 6$$
是一个 A 与 $\overline{A}$ 间的同构映射. 因为
$$a \star b = 3 \longrightarrow 6 = \overline{a} * \overline{b}.$$

☞ A 同 $\overline{A}$ 没有什么本质上的区别, 惟一的区别只是命名的不同而已. 4.83

Example 80. 代数系统 $\langle B, \oplus \rangle$, 和 $\langle C, * \rangle$ 都是与 $\langle A, \star \rangle$ 同构的:

研究同构的意义

假定对于代数运算 $\circ$ 与 $\bar{\circ}$ 来说, A 与 $\overline{A}$ 同构. 那么

- 对于代数运算 $\circ$ 与 $\bar{\circ}$ 来说, A 与 $\overline{A}$ 这两个集合, 抽象地来看, 没有什么区别 (只有命名上的不同).
- 若一个集合有一个只与这个集合的代数运算有关的性质, 那么另一个集合有一个完全相同的性质. (比如结合律, 交换律等.) 4.84

Example 81. 设 $\mathbb{R}$ 是实数集, $\mathbb{R}_+$ 为正实数集合, 说明代数系统 $\langle \mathbb{R}_+, \cdot \rangle$ 与 $\langle \mathbb{R}, + \rangle$ 是同构的. ($+, \cdot$ 是普通的加法, 乘法.)

解: 为说明 $\langle \mathbb{R}_+, \cdot \rangle$ 与 $\langle \mathbb{R}, + \rangle$ 是同构的, 必须建立 $\mathbb{R}_+$ 到 $\mathbb{R}$ 的双射 f, 并且对任意 $x_1, x_2 \in \mathbb{R}_+$, 有
$$f(x_1 \cdot x_2) = f(x_1) + f(x_2). \tag{39}$$
可令 $f : \mathbb{R}_+ \longmapsto \mathbb{R}$, $f(x) = \ln x$, 则 f 是 $\mathbb{R}_+$ 到 $\mathbb{R}$ 的双射, 且
$$\begin{aligned} f(x_1 \cdot x_2) &= \ln(x_1 \cdot x_2) \\ &= \ln x_1 + \ln x_2 \\ &= f(x_1) + f(x_2). \end{aligned}$$
所以, 代数系统 $\langle \mathbb{R}_+, \cdot \rangle$ 与 $\langle \mathbb{R}, + \rangle$ 是同构的. □

$$\boxed{\text{先算后映} = \text{先映后算}}$$ 4.85

自同态 & 自同构

Definition 82. 设 $\langle A, *\rangle$ 是代数系统,

(1) 如果 f 是 $\langle A, *\rangle$ 到 $\langle A, *\rangle$ 的一个同态, 则称 f 为自同态.
(2) 如果 g 是 $\langle A, *\rangle$ 到 $\langle A, *\rangle$ 的一个同构, 则称 g 为自同构.

4.86

Example 83. 设 $A = \{1, 2, 3\}$, 代数运算 $\star$ 由下表给定.

$\star$	1	2	3
1	3	3	3
2	3	3	3
3	3	3	3

那么

$$f : 1 \longrightarrow 2,\ 2 \longrightarrow 1,\ 3 \longrightarrow 3 \tag{40}$$

是一个对于 $\star$ 来说的 A 的自同构.

4.87

Theorem 84. *设 G 是代数系统的集合, 则 G 中代数系统间的同构关系是等价关系.*

证: ① 设任意 $\langle A, *\rangle \in G$, 令 $f : A \longmapsto A$, $f(a) = a$, $a \in A$. 从而

$$\langle A, *\rangle \cong \langle A, *\rangle.$$

即同构关系是自反的.

② 设 $\langle A, *\rangle \cong \langle B, \star\rangle$, 那么存在双射 $f : A \longmapsto B$, 故 $f^{-1} : B \longmapsto A$ 也是双射, 所以

$$\langle B, \star\rangle \cong \langle A, *\rangle.$$

因而该关系是对称的.

③ 设 $\langle A, *\rangle \cong \langle B, \star\rangle$, $\langle B, \star\rangle \cong \langle C, \oplus\rangle$, 则存在双射 $f : A \longmapsto B$ 和 $g : B \longmapsto C$, 那么 $g \circ f : A \longmapsto C$ 也是双射, 所以

$$\langle A, *\rangle \cong \langle C, \oplus\rangle.$$

因而该关系是传递的.

4.88 因此, 同构关系是等价关系. □

Theorem 85. *设 f 是代数系统 $\langle A, \star\rangle$ 到 $\langle B, *\rangle$ 的同态映射, 如果 $\langle A, \star\rangle$ 是半群 (独异点, 群), 则同态象 $\langle f(A), *\rangle$ 也是半群 (独异点, 群).*

证: 以群为例进行证明.

① $*$ 运算在 $f(A)$ 上封闭.

因 f 是同态, 所以 $f(A) \subseteq B$. 对任意 $b_1, b_2 \in f(A)$, 有 $a_1, a_2 \in A$, 使得 $f(a_1) = b_1$, $f(a_2) = b_2$, 那么

$$b_1 * b_2 = f(a_1) * f(a_2) = f(a_1 \star a_2) \in f(A),$$

② $*$ 运算在 $f(A)$ 上可结合.

对任意 $b_1, b_2, b_3 \in f(A)$, 有 $a_1, a_2, a_3 \in A$, 使得 $f(a_1) = b_1$, $f(a_2) = b_2$, $f(a_3) = b_3$, 那么

$$\begin{aligned}
b_1 * (b_2 * b_3) &= f(a_1) * \big(f(a_2) * f(a_3)\big) \\
&= f(a_1) * f(a_2 \star a_3) \\
&= f\big(a_1 \star (a_2 \star a_3)\big) \\
&= f\big((a_1 \star a_2) \star a_3\big) \\
&= f(a_1 \star a_2) * f(a_3) \\
&= \big(f(a_1) * f(a_2)\big) * f(a_3) \\
&= (b_1 * b_2) * b_3.
\end{aligned}$$

③ 存在幺元.

设 e 是 $\langle A, \star\rangle$ 的幺元, 对任意 $b \in f(A)$, 有 $a \in A$, 使得 $f(a) = b$, 那么

$$b * f(e) = f(a) * f(e) = f(a \star e) = f(a) = b.$$

同时,

$$b * f(e) = f(a \star e) = f(e \star a) = f(e) * f(a) = f(e) * b.$$

所以, $f(e)$ 是 $\langle f(A), *\rangle$ 的幺元.

④ 任意元素有逆元.

对任意 $b \in f(A)$, 有 $a \in A$, 使得 $f(a) = b$, 因 $\langle A, \star\rangle$ 是群, 则 a 有逆元 a^{-1}, 且 $f(a^{-1}) \in f(A)$, 那么

$$f(a) * f(a^{-1}) = f(a \star a^{-1}) = f(e)$$
$$f(e) = f(a^{-1} \star a) = f(a^{-1}) * f(a).$$

因 $f(e)$ 是 $\langle f(A), *\rangle$ 的幺元, 所以 $f(a^{-1})$ 是 $f(a)$ 的逆元.

所以任意 $b = f(a) \in f(A)$ 有逆元, 即 $f(a)^{-1} = f(a^{-1})$.

由上述, $\langle f(A), *\rangle$ 是群. $\square$ 4.89

<u>注</u>

从前述的证明中, 我们可以看到:

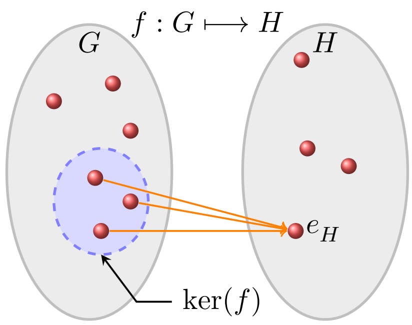
- 若 e 是 A 的幺元, 则 $f(e)$ 是 $f(A)$ 的幺元; (A 是独异点, 或群.)
- 若 x^{-1} 是 x 的逆元, 则 $f(x^{-1})$ 是 $f(x)$ 的逆元. (A 是群.)

4.90

Definition 86. 设 f 是群 $\langle G, \star\rangle$ 到群 $\langle H, *\rangle$ 的一个同态映射, e_H 是 $\langle H, *\rangle$ 的幺元, 令

$$\ker(f) = \{x \mid x \in G \text{ 且 } f(x) = e_H\}$$

称 $\ker(f)$ 是同态映射 f 的核, 简称同态核 (kernel of homomorphism).



Theorem 87. *设 f 是群 $\langle G, \star\rangle$ 到群 $\langle H, *\rangle$ 的一个同态映射，则 f 的同态核 K 是 G 的子群. (即 $\langle K, \star\rangle$ 是 $\langle G, \star\rangle$ 的子群)*

证: ① 对任意 $k_1, k_2 \in K$, 有

$$f(k_1 \star k_2) = f(k_1) * f(k_2) = e_H * e_H = e_H. \tag{41}$$

所以 $k_1 \star k_2 \in K$, 所以 $\star$ 运算在 K 上封闭.

② 进而可知 $\star$ 运算在 K 上可结合.

③ 又因 f 是群 $\langle G, \star\rangle$ 到群 $\langle H, *\rangle$ 的同态映射, 根据前述定理,

$$e_H = f(e). \tag{42}$$

这说明 $e \in K$, e 也是 K 的幺元.

④ 对任意 $k \in K$, $f(k) = e_H$.

$$f(k^{-1}) = \big(f(k)\big)^{-1} = (e_H)^{-1} = e_H. \tag{43}$$

4.92 所以 $k^{-1} \in K$, 即 K 中任意元素有逆元. 从而 K 是 G 的子群.

同余关系 & 同余类

Definition 88. 设 $\langle A, *\rangle$ 是一个代数系统, R 是 A 上的等价关系. 如果 $\langle a_1, a_2\rangle, \langle b_1, b_2\rangle \in R$ 时, 有

$$\langle a_1 * b_1,\ a_2 * b_2\rangle \in R, \tag{44}$$

则称 R 为 A 上关于运算 $*$ 的同余关系.

由该同余关系将 A 划分成的等价类叫做同余类.

4.93

Example 89. 给定代数系统 $\langle \mathbb{Z}, +\rangle$ 和 $\mathbb{Z}$ 上的模 k 等价关系 R, 证明 R 是 $\mathbb{Z}$ 上关于运算 $+$ 的同余关系.

证: 设 $\langle a, b\rangle, \langle c, d\rangle \in R$, 那么可令:

$$a - b = kn_1,\ c - d = kn_2, \quad n_1, n_2 \in \mathbb{Z}, \tag{45}$$

所以,

$$\begin{aligned} &(a-b) + (c-d) = k(n_1+n_2), \quad n_1+n_2 \in \mathbb{Z} \\ \Leftrightarrow\ &(a+c) - (b+d) = k(n_1+n_2) \\ \Leftrightarrow\ &\langle a+c,\ b+d\rangle \in R. \end{aligned}$$

4.94 按定义, R 是 $\mathbb{Z}$ 上关于运算 $+$ 的同余关系. □

Example 90. 给定代数系统 $\langle A, *\rangle$, $A = \{a, b, c, d\}$, 运算 $*$ 定义如下表, 给定 A 上的等价关系 $R = \{\langle a,a\rangle, \langle b,b\rangle, \langle c,c\rangle, \langle d,d\rangle, \langle a,b\rangle, \langle b,a\rangle, \langle c,d\rangle, \langle d,c\rangle\}$, 分析 R 是否为 A 上关于运算 $*$ 的同余关系.

*	a	b	c	d
a	a	a	d	c
b	b	a	d	a
c	c	b	a	b
d	c	d	b	a

证: $\langle a, b\rangle, \langle c, d\rangle \in R$, 但

$\langle a * c,\ b * d\rangle = \langle d, a\rangle \notin R$,

按定义, R 不是同余关系.

□

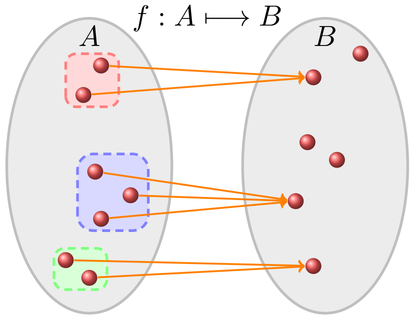


Figure 1: 同余关系 —— 特殊的等价关系

- 从同余关系的定义可知, 同余关系首先是等价关系.
- 同余关系与代数系统上的运算有关, 所以等价关系不一定是同余关系.

Theorem 91. 设 $\langle A, \star \rangle$ 是一个代数系统, R 是 A 上的同余关系. $B = \{A_1, A_2, \cdots, A_r\}$ 是由 R 诱导的 A 的一个划分, 那么必存在新的代数系统 $\langle B, * \rangle$, 它是 $\langle A, \star \rangle$ 的同态象.

本定理证明线索:

(1) 在 B 上建立运算 $*$;

(2) 证 $\langle A, \star \rangle$ 与 $\langle B, * \rangle$ 满同态, 即要构造一个满射 $f : A \longmapsto B$, 使

$$f(x \star y) = f(x) * f(y).$$

证: 在 B 上定义二元运算 $*$: 对任意 $A_i, A_j \in B$, 任取 $a_1 \in A_i$, $a_2 \in A_j$, 如果 $a_1 \star a_2 \in A_k$, 则定义 $A_i * A_j = A_k$.

因 R 是 A 上的同余关系, 所以上述定义的 $A_i * A_j = A_k$ 是惟一的.

其次, 作映射 $f : A \longmapsto B$, $f(a) = A_i$, $a \in A_i$. 显然 f 是满射.

对任意 $x, y \in A$, 则 x, y 应属于某一分块, 可设 $x \in A_i$, $y \in A_j$, 这里 $1 < i, j < r$; 同时, $x \star y$ 必属于 B 中的某个同余类, 不妨设 $x \star y \in A_k$. 于是

$$f(x \star y) = A_k = A_i * A_j = f(x) * f(y).$$

因此, f 是由 $\langle A, \star \rangle$ 到 $\langle B, * \rangle$ 的满同态, 即 $\langle B, * \rangle$ 是 $\langle A, \star \rangle$ 的同态象. □ 4.96

Theorem 92. 设 f 是 $\langle A, \star \rangle$ 到 $\langle B, * \rangle$ 的同态映射, 定义 A 上的二元关系 R:

$$\langle a, b \rangle \in R \quad \text{当且仅当} \quad f(a) = f(b).$$

则 R 是 A 上的同余关系.

证: 先证 R 是 A 上的等价关系:

- 对任意 $a \in A$, 因 $f(a) = f(a)$, 所以 $\langle a, a \rangle \in R$;
- 若 $\langle a, b \rangle \in R$, 则 $f(a) = f(b)$, 亦有 $f(b) = f(a)$, 所以 $\langle b, a \rangle \in R$;
- 若 $\langle a, b \rangle \in R$, $\langle b, c \rangle \in R$, 则 $f(a) = f(b)$, $f(b) = f(c)$, 于是 $f(a) = f(c)$, 所以 $\langle a, c \rangle \in R$.

其次, 若 $\langle a, b \rangle \in R$, $\langle c, d \rangle \in R$, 则

$$f(a * c) = f(a) \star f(c) = f(b) \star f(d) = f(b * d).$$

所以, $\langle a * c, b * d \rangle \in R$. 故 R 是 A 上的同余关系. □ 4.97

9 环与域

环与域

本节讨论具有两个运算的代数系统 $\langle A, \oplus, *\rangle$. 它可视为 $\langle A, \oplus\rangle$ 和 $\langle A, *\rangle$ 组合而成的代数系统. 我们把第一个运算 $\oplus$ 称为 "加法"; 把第二个运算 $*$ 称为 "乘法".

4.98

例如实数集上具有加和乘运算的代数系统 $\langle \mathbb{R}, +, \cdot\rangle$.

环

Definition 93. 设 $\langle A, \oplus, *\rangle$ 是代数系统, 如果

(1) $\langle A, \oplus\rangle$ 是阿贝尔群;

(2) $\langle A, *\rangle$ 是半群.

(3) 运算 $*$ 对 $\oplus$ 是可分配的. 即对任意 $a, b, c \in A$, 有

$$a * (b \oplus c) = (a * b) \oplus (a * c), \tag{46}$$

$$(b \oplus c) * a = (b * a) \oplus (c * a). \tag{47}$$

则称 $\langle A, \oplus, *\rangle$ 是环 (ring).

4.99

注

- 为了方便, 常称环 $\langle A, \oplus, *\rangle$ 的第一个运算 $\oplus$ 为 "加法", 并记为 $+$;
- 用 θ 表示加法幺元, 用 $-a$ 表示 a 的加法逆元, 将 $a + (-b)$ 记为 $a - b$;
- 称第二个运算 $*$ 为 "乘法", 并记为 $\circ$.

4.100

Theorem 94. *设 $\langle A, +, \circ\rangle$ 是环, 用 θ 表示加法幺元, 用 $-a$ 表示 a 的加法逆元, 将 $a + (-b)$ 记为 $a - b$. 则对任意 $a, b, c \in A$, 有*

(1) $a \circ \theta = \theta \circ a = \theta$, (加法幺元是乘法零元)

(2) $a \circ (-b) = (-a) \circ b = -(a \circ b)$,

(3) $(-a) \circ (-b) = a \circ b$,

(4) $a \circ (b - c) = a \circ b - a \circ c$,

(5) $(b - c) \circ a = b \circ a - c \circ a$.

4.101

(以下依次来证明...)

① $$a \circ \theta = \theta \circ a = \theta.$$

证: 因为 θ 是加法幺元, $\forall x \in A$, 有 $\theta + x = x$. 所以

$$\begin{aligned} a \circ \theta &= a \circ (\theta + \theta), && (\theta \text{ 是加法幺元}) \\ &= a \circ \theta + a \circ \theta. && (\text{分配律}) \end{aligned}$$

上式等价于

$$a \circ \theta + \theta = a \circ \theta + a \circ \theta.$$

由消去律, 得

$$\theta = a \circ \theta.$$

同理可证 $\theta \circ a = \theta$.

② $$a \circ (-b) = (-a) \circ b = -(a \circ b).$$

证: $a \circ (-b) = -(a \circ b)$ 可理解为 $a \circ b$ 的加法逆元是 $a \circ (-b)$. 证明如下:

$$\begin{aligned}
a \circ b + a \circ (-b) &= a \circ \big(b + (-b)\big) && \text{(分配律)}\\
&= a \circ \theta \\
&= \theta. && \text{(结论 ①)}
\end{aligned}$$

所以

$$a \circ (-b) = -(a \circ b).$$

同理可证 $a \circ (-b) = -(a \circ b)$. 4.103

③ $$(-a) \circ (-b) = a \circ b$$

证: 由结论 ② , 及: $(a^{-1})^{-1} = a$, 得

$$\begin{aligned}
(-a) \circ (-b) &= -\big(a \circ (-b)\big) && \text{(结论 ②)}\\
&= -\big(-(a \circ b)\big) && \text{(结论 ②)}\\
&= a \circ b. && \big((a^{-1})^{-1} = a\big)
\end{aligned}$$

4.104

④ $$a \circ (b - c) = a \circ b - a \circ c.$$

证:

$$\begin{aligned}
a \circ (b - c) &= a \circ \big(b + (-c)\big)\\
&= a \circ b + a \circ (-c) && \text{(分配律)}\\
&= a \circ b + \big(-(a \circ c)\big) && \text{(结论 ②)}\\
&= a \circ b - a \circ c.
\end{aligned}$$

结论 ⑤ 同理. □ 4.105

交换环 & 含幺环

Definition 95. 设 $\langle A, +, \circ\rangle$ 是环,

(1) 如果 $\langle A, \circ\rangle$ 是可交换的, 则称 $\langle A, +, \circ\rangle$ 是交换环 (commutative ring).
(2) 如果 $\langle A, \circ\rangle$ 含有幺元, 则称 $\langle A, +, \circ\rangle$ 是含幺环 (ring with unity).

注

- 以上定义针对的是乘法 $\circ$;
- 对含幺环, $\langle A, \circ\rangle$ 是独异点;
- 一般, 一个环未必有一个乘法幺元. 例如 $\mathbb{Z}_E = \{$所有偶数$\}$, 对普通加法和乘法构成一个环, 但是没有乘法幺元.

4.106

零因子

Definition 96. 设 $\langle A, +, \circ\rangle$ 是环, 如果存在 $a, b \in A$, 且 $a \neq \theta$, $b \neq \theta$, 使得 $a \circ b = \theta$, 则称 $\langle A, +, \circ\rangle$ 是含零因子环. a 和 b 称为零因子.

注

- 零因子: “两个非零的数相乘等于零”;
- 强调这个概念, 是因为
$$a \circ b = 0 \Rightarrow a = 0 \text{ 或 } b = 0 \tag{48}$$
这一条普通的计算规则, 在一般的环里并不一定成立;
- 一个环当然可以没有零因子, 比如整数环;
- 4.107 显然, 在而且只在一个没有零因子的环里, (48) 式才会成立.

Theorem 97. 一个环 $\langle A, +, \circ\rangle$ 没有零因子, 当且仅当乘法满足消去律, 即
$$c \neq \theta,\ c \circ a = c \circ b \Rightarrow a = b.$$
$$c \neq \theta,\ a \circ c = b \circ c \Rightarrow a = b.$$

证: 设 $c \circ a = c \circ b$ 且 $c \neq \theta$, 则
$$\begin{aligned} c \circ (a - b) &= c \circ a - c \circ b = c \circ a + (-c \circ b) \\ &= c \circ a + (-c \circ a) \\ &= \theta. \end{aligned}$$
若环 $\langle A, +, \circ\rangle$ 无零因子, 由上式及 $c \neq \theta$, 得
$$a - b = \theta,$$
两边加 b, 得 $a = b$. 另一式类似可证. 即证消去律成立.

反之, 设 $a \neq \theta$, $a \circ b = \theta$, 因 $a \circ \theta = \theta$, 得
$$a \circ b = a \circ \theta,$$
4.108 若消去律成立, 得 $b = \theta$. 这说明 $\langle A, +, \circ\rangle$ 无零因子. □

零因子

Example 98. 一个数域 F 上的一切 $n \times n$ 矩阵对于矩阵的加法和乘法来说, 构成一个环. 这个环有幺元, 即单位矩阵. 当 $n \geqslant 2$ 时, 这个环是非交换环, 有零因子 (或者说, 不满足消去律).

以上我们认识了一个环可能满足的三种附加条件: (1) 乘法满足交换律, (2) 存在幺元, (3) 零因子不存在 (满足消去律). 一个环当然可以满足其中的一个或多个附加条件. 同时满足以上三个条件的环, 称为整环.
4.109

整环

Definition 99. 设 $\langle A, +, \circ\rangle$ 是环, 如果

(1) $\langle A, \circ\rangle$ 是可交换的;

(2) $\langle A, \circ\rangle$ 含有幺元;

(3) $\langle A, \circ\rangle$ 无零因子 (或满足消去律):
$$a \circ b = \theta \Rightarrow a = \theta \text{ 或 } b = \theta. \tag{49}$$
则称 $\langle A, +, \circ\rangle$ 是整环.

☞ 环 + 乘法幺元 + 乘法可交换 + 乘法消去律 = 整环
4.110

整环

Example 100. 整数环 $\langle\mathbb{Z}, +, \cdot\rangle$ 是整环, 因 $\langle\mathbb{Z}, \cdot\rangle$ 可交换, 有幺元 1, 且无零因子 (即不可能有两个非零的数相乘等于零).

4.111

域

上面我们提到了三个附加条件:

(1) 乘法满足交换律,

(2) 存在幺元,

(3) 零因子不存在 (满足消去律).

还有一个附加条件没有提到, 即逆元的存在性.

注意到零元 θ 是没有逆元的, 即不存在元素 a 使得 $\theta \circ a = a \circ \theta = e$. 我们看这个新的附加条件:

(4) 每一个不等于零元的元有一个逆元.

4.112

域

注意附加条件 (4) 成立必有附加条件 (3) 成立, 即, 若环中每一个不等于零元的元有一个逆元, 则零因子不存在 (满足消去律). 因为

$$a \neq \theta, a \circ b = \theta \Rightarrow a^{-1} \circ a \circ b = b = \theta.$$

一个环如果满足附加条件 (1), (2), (4), 则称为域.

4.113

域

Definition 101. 设 $\langle A, +, \circ\rangle$ 是代数系统, 如果

(1) $\langle A, +\rangle$ 是阿贝尔群;

(2) $\langle A - \{\theta\}, \circ\rangle$ 是阿贝尔群;

(3) 运算 $\circ$ 对 $+$ 是可分配的,

则称 $\langle A, +, \circ\rangle$ 是域 (field).

Example 102.
- $\langle\mathbb{R}, +, \circ\rangle$, $\langle\mathbb{Q}, +, \circ\rangle$, $\langle\mathbb{C}, +, \circ\rangle$ 都是域.
- 但 $\langle\mathbb{Z}, +, \circ\rangle$ 是整环而不是域,
  因 $\langle\mathbb{Z} - \{0\}, \circ\rangle$ 不是群: 整数除 ± 1 之外, 均无乘法逆元.
- 此例说明整环不一定是域.

4.114

域 V.S. 整环

两者的定义区别在于

整环	$\langle A, \circ\rangle$ 是可交换含幺半群, 且无零因子;
域	$\langle A - \{\theta\}, \circ\rangle$ 是阿贝尔群.

事实上, 域的概念是在整环中增加了 “除了零元外, 每个元都有逆元” 这个条件.

Theorem 103. *域一定是整环.*

4.115

Theorem 104. 有限整环一定是域.

证: 设 $\langle A, +, \circ\rangle$ 是有限整环, 则 $\langle A, \circ\rangle$ 是可交换的含幺半群, 要证 $\langle A, +, \circ\rangle$ 是域, 只须证任意非零元 c, 都有乘法逆元.

事实上, 若 $a, b \in A$, 且 $a \neq b$, 则 $a \circ c \neq b \circ c$ (否则, 因 $\langle A, \circ\rangle$ 无零因子, 由消去律而导致 $a = b$).

又因运算 $\circ$ 封闭, 从而有 $A \circ c = A$.

用 e 表示乘法幺元. 由 $A \circ c = A$, 则存在 $d \in A$, 使得 $d \circ c = e$.

4.116 故 d 是 c 的乘法逆元, 这说明 $\langle A - \{\theta\}, \circ\rangle$ 是阿贝尔群. □

同态映射

可以将同态概念推广到具有两个运算的代数系统.

Definition 105. 设 $\langle A, +, \circ\rangle$ 和 $\langle B, \oplus, \odot\rangle$ 是两个代数系统, 对任意 $a, b \in A$, 如果映射 $f : A \longmapsto B$ 满足

(1) $f(a + b) = f(a) \oplus f(b)$,

(2) $f(a \circ b) = f(a) \odot f(b)$,

则称 f 是 $\langle A, +, \circ\rangle$ 到 $\langle B, \oplus, \odot\rangle$ 的一个同态映射.

称 $\big\langle f(A), \oplus, \odot\big\rangle$ 是 $\langle A, +, \circ\rangle$ 的同态象.

4.117

Example 106. 设 $\langle \mathbb{N}, +, \cdot\rangle$ 是一个代数系统, $\mathbb{N}$ 是自然数集, $+$ 和 $\cdot$ 是普通的加法和乘法运算, 并设代数系统 $\big\langle\{$偶, 奇$\}, \oplus, \odot\big\rangle$, 其运算表如下:

$\oplus$	偶	奇
偶	偶	奇
奇	奇	偶

$\odot$	偶	奇
偶	偶	偶
奇	偶	奇

容易验证映射

$$f(n) = \begin{cases} \text{偶}, & \text{若 } n = 2k, k = 0, 1, 2, \cdots \\ \text{奇}, & \text{若 } n = 2k + 1, k = 0, 1, 2, \cdots \end{cases}$$

是由 $\langle \mathbb{N}, +, \cdot\rangle$ 到 $\big\langle\{$偶, 奇$\}, \oplus, \odot\big\rangle$ 的同态映射.

4.118

Theorem 107. 任一环的同态象是一个环.

证: 设 $\langle A, +, \circ\rangle$ 是一个环, 且 $\langle B, \oplus, \odot\rangle$ 是关于同态映射 f 的同态象.

由 $\langle A, +,\rangle$ 是阿贝尔群, 则同态象 $\langle B, \oplus\rangle$ 是群; 容易验证 $\oplus$ 也满足交换律, 所以 $\langle B, \oplus\rangle$ 是阿贝尔群.

由 $\langle A, \circ\rangle$ 是半群, 则同态象 $\langle B, \odot\rangle$ 也是半群.

证: 对于任意的 $b_1, b_2, b_3 \in B$, 必有相应的 a_1, a_2, a_3, 使得

$$f(a_i) = b_i, \qquad (i = 1, 2, 3)$$

于是

$$
\begin{aligned}
b_1 \odot (b_2 \oplus b_3) &= f(a_1) \odot \big(f(a_2) \oplus f(a_3)\big) \\
&= f(a_1) \odot f(a_2 + a_3) \\
&= f\big(a_1 \cdot (a_2 + a_3)\big) \\
&= f\big((a_1 \cdot a_2) + (a_1 \cdot a_3)\big) \\
&= f(a_1 \cdot a_2) \oplus f(a_1 \cdot a_3) \\
&= \big(f(a_1) \odot f(a_2)\big) \oplus \big(f(a_1) \odot f(a_3)\big) \\
&= (b_1 \odot b_2) \oplus (b_1 \odot b_3).
\end{aligned}
$$

同理可证 $(b_2 \oplus b_3) \odot b_1 = (b_1 \odot b_2) \oplus (b_1 \odot b_3)$.

因此, $\langle B, \oplus, \odot \rangle$ 是一个环. □ 4.119

练习

已知一个环 $\langle \{a, b, c, d\}, +, \cdot \rangle$, 它的运算由下表给出:

$+$	a	b	c	d
a	aa	b	c	d
b	b	c	d	aa
c	c	d	aa	b
d	d	aa	b	c

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	c	a	c
c	a	a	a	a
d	a	c	a	c

它是一个交换环吗? 它有乘法幺元吗? 这个环中的零元是什么? 并求出每个元素的加法逆元.

解:

(1) 因为 $\cdot$ 的运算表是对称的, 所以环 $\langle \{a, b, c, d\}, +, \cdot \rangle$ 是交换环;

(2) 没有乘法幺元;

(3) 环中的零元是 a;

(4) 由 $+$ 运算表可见: a 和 c 以自身为加法逆元; b 和 d 互为加法逆元. □ 4.120

阿贝尔 & 世界知名数学大奖

阿贝尔 —— 天才与贫困

阿贝尔 (Niels Henrik Abel, 1802–1829), 挪威数学家.

1821 年入 Christiania 大学 (今挪威 Oslo 大学).

1824 年, 他解决了用根式求解五次方程的不可能性问题, 由此引入可交换群 (也称阿贝尔群) 的概念.

为了能有更多的读者, 他的论文以法文写成 (也送给了 C. F. 高斯), 但是在外国数学家中没有引起反响. 4.121

阿贝尔 —— 天才与贫困

1825 年, 他去柏林, 结识了 A. L. 克雷尔 (August Leopold Crelle, 1780–1856), 并成为好友.

1826 年, 他鼓励克雷尔创办了数学刊物《纯数学与应用数学杂志》, 这个杂志是世界上第一个专门从事数学研究的定期刊物. 该杂志的前三卷刊登了阿贝尔 22 篇论文, 使欧洲数学家开始注意他的工作.

1826 年阿贝尔到巴黎, 遇见了 A. M. 勒让德和 A. L. 柯西等著名数学家. 他写了一篇关于椭圆积分的论文, 提交给法国科学院, 不幸未得到重视, 他只好又回到柏林.

克雷尔为他谋求教授职位, 没有成功. 1827 年阿贝尔贫病交迫地回到了挪威, 靠做家庭教师维生.

4.122 1829 年 4 月 6 日, 阿贝尔因肺结核去世, 在世二十六年零八个月.

阿贝尔 —— 天才与贫困

阿贝尔去世后两天, 克雷尔来信说, 阿贝尔将被任命为柏林大学的数学教授.

他与 Évariste Galois (1811–1832) 的英才早逝, 是数学史上的悲剧. 此后荣誉和褒奖接踵而至.

阿贝尔在数学方面的成就是多方面的. 和雅可比同时奠定了椭圆函数论的基础, 得出了阿贝尔定理. 还有阿贝尔积分, 阿贝尔函数以及关于

4.123 正项级数收敛的阿贝尔判别法等研究成果.

阿贝尔奖 The Abel Prize[3]

挪威政府捐出二亿挪威克朗 (约三千二百万美元) 的基金, 于 2002 年 (阿贝尔诞辰 200 周年) 设立了 “阿贝尔奖”.

该奖每年颁发一次, 奖金为 600 万挪威克朗 (约 95 万美元). 这是一个专门针对数学专业的奖项, 是目前国际上专业数学奖中奖金额最大的奖项之一.

- 2003: **Jean-Pierre Serre**,[4] Collège de France.
- 2004: **Sir Michael Francis Atiyah**, University of Edinburgh; **Isadore M. Singer**, Massachusetts Institute of Technology.
- 2005: **Peter D. Lax**, Courant Institute of Mathematical Sciences, New York University.

[3]阿贝尔奖官方网址: `http://www.abelprisen.no/en/`.

[4]Jean-Pierre Serre, 1926 年生于法国, 1954 年获菲尔兹奖, 2000 年获沃尔夫奖.

- 2006: **Lennart Carleson**,[5] Royal Institute of Technology, Sweden.
- 2007: **Srinivasa S. R. Varadhan**, Courant Institute of Mathematical Sciences, New York University. 4.124

世界知名数学大奖

奖项	首颁时间	颁发频度	所在国家或组织	奖金额
菲尔兹奖	1932 年	4 年	IMU	15000 加元
沃尔夫奖	1978 年	1 年	以色列	10 万美元
克拉福德奖[6]	1982 年	1 年	瑞典	50 万美元
阿贝尔奖	2003 年	1 年	挪威	600 万挪威克朗
邵逸夫奖	2004 年	1 年	中国	100 万美元

4.125

菲尔兹 Fields Prize[7]

1924 年, 在多伦多举行的国际数学家大会 (International Congress of Mathematicians, ICM) 上, 提议创设一项数学奖, 这次会议余下的钱用来建立这个奖的基金.

菲尔兹奖在每 4 年一届的 ICM 上颁发, 奖品包含一枚金质奖章和 15,000 加元 (约 13,000 美元[8]). 奖项的名称是纪念 J. C. Fields 教授, 他是位加拿大数学家, 曾任 1924 年数学家大会秘书长.

菲尔兹奖有一项特别的规定: 受奖者年龄必须不超过 40 岁.

华裔菲尔兹奖得主:

- 1982: Shing-Tung Yau (丘成桐).
- 2006: Terence Tao (陶哲轩). 4.126

沃尔夫奖 The Wolf Prizes[9]

沃尔夫奖是世界上具有较高学术声望的多学科国际奖.

1976 年由以色列议会设立, 1978 年首次颁奖. 沃尔夫科学基金会是在 Ricardo Wolf 及其夫人 Francisca Subirana Wolf 的倡导下设立的, 基金来自 Ricardo Wolf 及其家族一千万美元的捐赠.

沃尔夫基金会设有：数学、物理、化学、医学、农业五个奖（1981 年增设艺术奖）. 通常每年颁发一次, 每个奖的奖金数额为 10 万美元.

华裔沃尔夫奖得主:

- 1978, 物理: 吴健雄 (1912–1997, 生于江苏, 哥伦比亚大学教授.)
- 1983, 数学: 陈省身 (1911–2004, 生于浙江, 加州大学伯克利分校教授.)

[5] Lennart Carleson, 1992 年获沃尔夫奖. 1978–1982 年 IMU 主席.

[6] 克拉福德奖主要分三个部分: Astronomy and Mathematics, Geosciences, Biosciences. 依次每年颁发其中之一, 所以, 事实上数学奖要约 6 年颁发一次.

[7] 菲尔兹奖官方网址: `http://www.mathunion.org/Prizes/Fields/index.html`.

[8] 美元兑加拿大元的比价约为 $1:1.13$ (2006/11/29).

[9] 沃尔夫奖官方网址: `http://www.wolffund.org.il/wolfpriz.html`.

- 1991, 农业: 杨祥发 (1932 年生于台湾, 加州大学戴维斯分校教授.)
- 2004, 农业: 袁隆平 (1930 年生于北京, 中国工程院院士.)
- 2004, 医学: 钱永健 (1952 年生于纽约, 加州大学圣地亚哥分校教授.)

4.127

克拉福德奖 The Crafoord Prize

The Crafoord Prize in astronomy and mathematics, biosciences, geosciences or polyarthritis research is awarded by the Royal Swedish Academy of Sciences annually according to a rotating scheme. The prize sum of USD 500,000 makes the Crafoord one of the world's largest scientific prizes.

Anna-Greta and Holger Crafoord's Fund was established in 1980 and the first prize was awarded in 1982. The prize is intended to promote international basic research in the disciplines:

- Astronomy and Mathematics,
- Geosciences,
- Biosciences, with particular emphasis on ecology and
- Polyarthritis (rheumatoid arthritis).

4.128

克拉福德奖 The Crafoord Prize

These disciplines are chosen so as to complement those for which the Nobel Prizes are awarded. The recipients are worthy scientists who receive the prize in accordance with a set scheme:

- Year 1 Astronomy and Mathematics
- Year 2 Geosciences
- Year 3 Biosciences
- Year 4 Astronomy and Mathematics

The prize in polyarthritis is awarded only when a special committee has shown that scientific progress in this field has been such that an award is justified.

The laureates are announced in mid-January each year, and the prize is presented in April on “Crafoord Day”. It is received from the hand of His Majesty the King of Sweden.

4.129

克拉福德奖 The Crafoord Prize[10]

数学奖得奖者:

- 1982: Vladimir, Igorevich Arnold, Louis Nirenberg.
- 1988: Pierre Deligne, Alexander Grothendieck.
- 1994: Simon Donaldson, Shing-Tung Yau (丘成桐).
- 2001: Alain Connes.

4.130

[10] 克拉福德奖官方网址: http://www.crafoordprize.se/.

邵逸夫奖 The Shaw Prize[11]

邵逸夫奖是由香港著名的电影制作人邵逸夫先生于 2002 年 11 月创立. 首届的颁奖礼在 2004 年 9 月 7 日在香港举行.

邵逸夫奖设有数学奖、天文学奖、生命科学与医学奖, 共三个奖项, 每个奖项一百万美元奖金; 它是个国际性奖项, 由邵逸夫奖基金会有限公司管理.

数学奖得奖者:

- 2004 年: 陈省身.
- 2005 年: Andrew J. Wiles.
- 2006 年: 吴文俊, David Mumford.
- 2007 年: Robert Langlands and Richard Taylor.
- 2008 年: Vladimir Arnold and Ludwig Faddeev.
- 2009 年: Simon K Donaldson and Clifford H Taubles.
- 2010 年: Jean Bourgain. 4.131

[11]邵逸夫奖官方网址: `http://www.shawprize.org/en/index.html`.

Chapter 5

格

Discrete Mathematics

December 27, 2012

黄正华, 数学与统计学院, 武汉大学

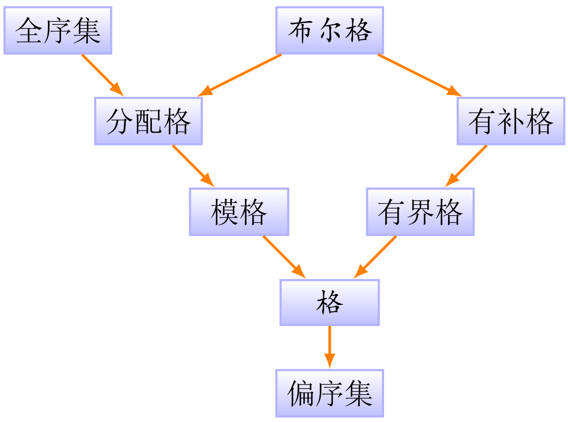
5.1

主要内容

- 格 (Lattice): 一个偏序集, 其任意两个元素都有最小上界和最大下界.
- 特殊的格: 分配格, 有补格.
- 布尔代数: 有补分配格.

5.2

本章概念关系图



5.3

Contents

 5.4

1 格的定义

本节主要内容:

1. 格的两种定义;
2. 格的基本性质;
3. 格与代数系统间的关系. 5.5

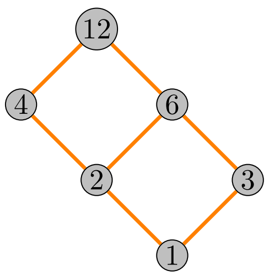
回顾:

Definition 1 (偏序)**.** 如果集合 A 上的关系 $\preccurlyeq$ 具有

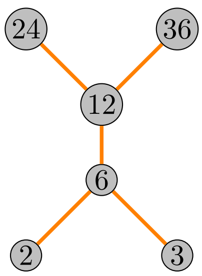
1. 自反性,
2. 反对称性,
3. 传递性.

则称关系 $\preccurlyeq$ 为 A 上偏序关系. $\langle A, \preccurlyeq\rangle$ 称为偏序集. 5.6

Example 2. 设 $X = \{1, 2, 3, 4, 6, 12\}$, $Y = \{2, 3, 6, 12, 24, 36\}$. 集合 X 和 Y 关于整除关系 "$\mid$" 构成两个偏序集: $\langle X, \mid\rangle$, $\langle Y, \mid\rangle$. 它们的哈斯图如下:



(a) $\langle X, \mid\rangle$



(b) $\langle Y, \mid\rangle$

虽然都是偏序集, 但是它们有一个重要的差别:

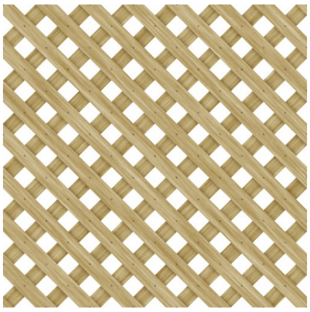
- $\langle X, \mid\rangle$ 中 "每两个元素构成的集合" 都有最大下界和最小上界.
- $\langle Y, \mid\rangle$ 无此特点. 5.7

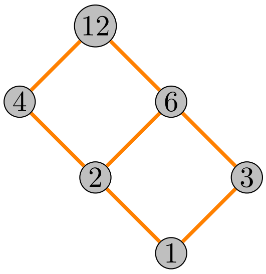
格的定义

Definition 3 (格)**.** 如果偏序集 $\langle A, \preccurlyeq\rangle$ 中任意两个元素都有最小上界和最大下界, 则称 $\langle A, \preccurlyeq\rangle$ 是格 (lattice).

lattice: 木格, 窗格. a 和 b 的最小上界: $\mathrm{lub}\{a, b\}$. (least upper bound)

a 和 b 的最大下界: $\mathrm{glb}\{a, b\}$. (greatest lower bound) 5.8





格的典型例子

Example 4. 偏序集 $\langle \mathscr{P}(S), \subseteq \rangle$ 是格:

任意 $S_1, S_2 \in \mathscr{P}(S)$, 它们的最大下界为 $S_1 \cap S_2$; 最小上界为 $S_1 \cup S_2$.

☞ 这是格的一个典型例子. 关于格的很多性质, 都可以借助这个例子理解.

Example 5. 偏序集 $\langle \mathbb{Z}^+, | \rangle$ 是格:

$\mathbb{Z}^+$ 中任意两个元素的最小公倍数、最大公约数就是这两个元素的最小上界和最大下界. 5.9

格的等价定义

为什么格的定义中是要求 "两个元素"? 事实上, 多个元素也可以. 因为, "任意两个元素有上下确界" 当且仅当 "任意有限个元素有上下确界". 从而, 格有如下的等价定义.

Definition 6. 偏序集 $\langle A, \preccurlyeq \rangle$ 是一个格, 当且仅当 A 中任意非空有限子集 S 有最小上界、最大下界.

其中要求子集元素个数 "有限" 是重要的, 不能是 "任意的非空子集". 比如 $\langle \mathbb{N}, \leqslant \rangle$ 是一个格, 但不是任意的非空子集都有最小上界、最大下界 —— $\mathbb{N}$ 就是它自己的一个子集, 它没有最小上界. 5.10

Definition 7. 设 $\langle A, \preccurlyeq \rangle$ 是格, 在 A 上定义两个二元运算 $\vee$ 和 $\wedge$: 对任意 $a, b \in A$,

$$a \vee b \triangleq \mathrm{lub}\{a, b\}, \tag{1}$$

$$a \wedge b \triangleq \mathrm{glb}\{a, b\}. \tag{2}$$

则二元运算 $\vee$ 和 $\wedge$ 分别称为并运算和交运算; 称 $\langle A, \vee, \wedge \rangle$ 是格 $\langle A, \preccurlyeq \rangle$ 所诱导的代数系统.

Example 8. 在格 $\langle \mathscr{P}(S), \subseteq \rangle$ 诱导的代数系统中, 运算 $\vee$ 和 $\wedge$ 就是普通的并、交运算: 任意 $S_1, S_2 \in \mathscr{P}(S)$, 有

$$S_1 \vee S_2 = S_1 \cup S_2, \quad S_1 \wedge S_2 = S_1 \cap S_2.$$

Example 9. 在格 $\langle \mathbb{Z}, \leqslant \rangle$ 或 $\langle \mathbb{N}, \leqslant \rangle$ 诱导的代数系统中, 运算 $\vee$ 和 $\wedge$ 就是普通的取大、取小运算. 比如, 任意的 $a, b \in \mathbb{N}$, 有

$$a \vee b = \max\{a, b\}, \quad a \wedge b = \min\{a, b\}.$$

Example 10. 对于格 $\langle \mathbb{Z}^+, | \rangle$ 来说, 其诱导的代数系统 $\langle \mathbb{Z}^+, \vee, \wedge \rangle$ 中的二元运算 $\vee$ 和 $\wedge$ 分别为: 对任意的 $a, b \in \mathbb{Z}^+$ 有

$$a \vee b = \mathrm{LCM}(a, b), \qquad \text{(least common mutiple, 最小公倍数)}$$

$$a \wedge b = \mathrm{GCD}(a, b). \qquad \text{(greatest common divisor, 最大公约数)}$$

这个定义表明, 从格出发, 可以构造一个代数系统. 这也说明了格这类特殊偏序集的重要性. 5.11

格的对偶原理

设 $\langle A, \preccurlyeq \rangle$ 是偏序集, 用 $\succcurlyeq$ 表示偏序关系 $\preccurlyeq$ 的逆关系, 则

- $\langle A, \succcurlyeq \rangle$ 也是偏序集.
- $\langle A, \preccurlyeq \rangle$ 与 $\langle A, \succcurlyeq \rangle$ 的哈斯图是互为颠倒的.
- 称 $\langle A, \preccurlyeq \rangle$, $\langle A, \succcurlyeq \rangle$ 为彼此对偶的偏序集.
- 如果其中一个是格, 则另一个也是格.
- 由格 $\langle A, \preccurlyeq \rangle$ 诱导的代数系统的并 (交) 运算, 正好是由格 $\langle A, \succcurlyeq \rangle$ 诱导的代数系统的交 (并) 运算.

Theorem 11 (对偶原理)**.** *设 P 是对任意格都为真的命题, 将 P 中的 $\preccurlyeq, \vee, \wedge$ 分别换成 $\succcurlyeq, \wedge, \vee$ 得命题 Q, 则 Q 对任意格也是真的命题. (Q 称为 P 的对偶命题.)*

5.12

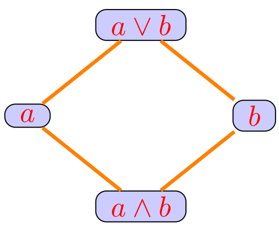
格的基本性质

Theorem 12. *设 $\langle A, \preccurlyeq \rangle$ 是格, 对任意 $a, b \in A$, 有*

$$a \preccurlyeq a \vee b, \qquad b \preccurlyeq a \vee b,$$

$$a \wedge b \preccurlyeq a, \qquad a \wedge b \preccurlyeq b.$$

分析 由 $\vee, \wedge$ 的定义即得上述结论. 如图:



证 因为 $a \vee b$ 是 a 和 b 的 (最小) 上界, 所以

$$a \preccurlyeq a \vee b, \qquad b \preccurlyeq a \vee b.$$

由对偶原理, 即得

$$a \wedge b \preccurlyeq a, \qquad a \wedge b \preccurlyeq b. \qquad \square$$

5.13

Theorem 13. 设 $\langle A, \preccurlyeq\rangle$ 是格, $a, b, c, d \in A$, 若 $a \preccurlyeq b$, $c \preccurlyeq d$, 则

$$a \vee c \preccurlyeq b \vee d, \tag{3}$$

$$a \wedge c \preccurlyeq b \wedge d. \tag{4}$$

证　已知 $a \preccurlyeq b$, $c \preccurlyeq d$, 又

$$b \preccurlyeq b \vee d, \quad d \preccurlyeq b \vee d,$$

由传递性可得

$$a \preccurlyeq b \vee d, \quad c \preccurlyeq b \vee d.$$

这说明 $b \vee d$ 是 a 和 c 的一个上界, 但 $a \vee c$ 是 a 和 c 的最小上界, 所以

$$a \vee c \preccurlyeq b \vee d.$$

类似地可以证明

$$a \wedge c \preccurlyeq b \wedge d. \qquad \square$$

5.14

推论
设 $\langle A, \preccurlyeq\rangle$ 是格, $a, b, c \in A$, 若 $b \preccurlyeq c$, 则

$$a \vee b \preccurlyeq a \vee c, \qquad a \wedge b \preccurlyeq a \wedge c.$$

这个性质称为格的保序性.

证　已知 $b \preccurlyeq c$, 又 $a \preccurlyeq a$, 所以

$$a \vee b \preccurlyeq a \vee c.$$

同理有

$$a \wedge b \preccurlyeq a \wedge c. \qquad \square$$

5.15

Theorem 14. 设 $\langle A, \preccurlyeq\rangle$ 是一个格, 那么, 对于任意的 $a, b \in A$, 有

$$a \preccurlyeq b \iff a \wedge b = a \iff a \vee b = b.$$

证 先证明 $a \preccurlyeq b \iff a \wedge b = a$.

设 $a \preccurlyeq b$. 又 $a \preccurlyeq a$, 则 a 是 a 和 b 的下界, 而 $a \wedge b$ 是最大下界, 得

$$a \preccurlyeq a \wedge b.$$

又

$$a \wedge b \preccurlyeq a,$$

所以

$$a \wedge b = a. \qquad \text{(反对称性)}$$

反之, 假定 $a \wedge b = a$, 又 $a \wedge b \preccurlyeq b$, 所以

$$a \preccurlyeq b.$$

因此, $a \preccurlyeq b \iff a \wedge b$. 其他的证明类似. □ 5.16

Theorem 15. 设 $\langle A, \preccurlyeq\rangle$ 是一个格, 那么, 对于任意的 $a, b \in A$, 有

$$a \preccurlyeq b \iff a \wedge b = a \iff a \vee b = b.$$

此时的哈斯图为:

“小 ∧ 大 = 小”, “小 ∨ 大 = 大”

5.17

格的基本性质

Theorem 16. 设 $\langle A, \preccurlyeq\rangle$ 是格, 由格 $\langle A, \preccurlyeq\rangle$ 所诱导的代数系统为 $\langle A, \vee, \wedge\rangle$, 则对任意的 $a, b, c, d \in A$, 有 *[1ex]*

① $\left.\begin{aligned} a \vee b = b \vee a, \\ a \wedge b = b \wedge a. \end{aligned}\right\}$ *(交换律)*

② $\left.\begin{aligned} a \vee (b \vee c) = (a \vee b) \vee c, \\ a \wedge (b \wedge c) = (a \wedge b) \wedge c. \end{aligned}\right\}$ *(结合律)*

③ $\left.\begin{aligned} a \vee a = a, \\ a \wedge a = a. \end{aligned}\right\}$ *(幂等律)*

④ $\left.\begin{aligned} a \vee (a \wedge b) = a, \\ a \wedge (a \vee b) = a. \end{aligned}\right\}$ *(吸收律)*

5.18

下证结合律: $a \vee (b \vee c) = (a \vee b) \vee c$.

分析 由偏序的反对称性, 可证下列两式同时成立:

$$(a \vee b) \vee c \preccurlyeq a \vee (b \vee c), \tag{5}$$

$$a \vee (b \vee c) \preccurlyeq (a \vee b) \vee c. \tag{6}$$

证 因为 $b \preccurlyeq b \vee c$, 由保序性得

$$a \vee b \preccurlyeq a \vee (b \vee c).$$

反复使用结论 “$x \preccurlyeq x \vee y$, $y \preccurlyeq x \vee y$”, 有

$$c \preccurlyeq b \vee c \preccurlyeq a \vee (b \vee c).$$

这说明 $a \vee (b \vee c)$ 是 $a \vee b$ 和 c 的一个上界. 但 $(a \vee b) \vee c$ 是 $a \vee b$ 和 c 的最小上界, 所以

$$(a \vee b) \vee c \preccurlyeq a \vee (b \vee c).$$

类似可证

$$a \vee (b \vee c) \preccurlyeq (a \vee b) \vee c.$$

因而 $$a \vee (b \vee c) = (a \vee b) \vee c.$$ □ 5.19

证明吸收律: $a \vee (a \wedge b) = a$.

证 因为

$$a \wedge b \preccurlyeq a,$$

所以

$$a \vee (a \wedge b) = a. \tag{7}$$

这里 (7) 式成立的理由是 “大 $\vee$ 小 $=$ 大”. □ 5.20

引理

设 $\langle A, \vee, \wedge \rangle$ 是一个代数系统, 其中 $\vee$, $\wedge$ 都是二元运算且满足吸收律, 那么 $\vee$, $\wedge$ 必满足幂等律.

证 对任意 $a, b \in A$, 因 $\vee$, $\wedge$ 满足吸收律, 所以

$$a \vee (a \wedge b) = a, \tag{8}$$

$$a \wedge (a \vee b) = a. \tag{9}$$

由 b 的任意性, 在 (8) 式中用 $a \vee b$ 取代 b 仍然成立, 可得

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

$$a \vee \big(a \wedge (a \vee b)\big) = a.$$

$$a \vee \big(\underbrace{a \wedge (a \vee b)}_{a}\big) = a.$$

再由 (9) 式得:

$$a \vee a = a.$$

同理可证 $$a \wedge a = a.$$ □ 5.21

格与代数系统之间的关系

Theorem 17. 设 $\langle A, \vee, \wedge \rangle$ 是一个代数系统, 其中 $\vee, \wedge$ 都是二元运算, 且满足交换律、结合律和吸收律, 则 A 上存在偏序关系 $\preccurlyeq$, 使 $\langle A, \preccurlyeq \rangle$ 是一个格.

分析 证明思路:

1. 在 A 上构造偏序关系 $\preccurlyeq$;
2. 证明 $\langle A, \preccurlyeq \rangle$ 中任意两个元素有最小上界和最大下界.

证 在 A 上定义二元关系 $\preccurlyeq$: 对任意 $a, b \in A$,

$$a \preccurlyeq b \iff a \wedge b = a.$$

先证 $\preccurlyeq$ 是偏序. 5.22

- 运算 $\wedge$ 满足吸收律, 由引理知满足幂等律: 对任意 $a \in A$, $a \wedge a = a$. 所以

$$a \preccurlyeq a.$$

  从而 $\preccurlyeq$ 是自反的.
- 设 $a \preccurlyeq b$, 则 $a \wedge b = a$. 如果同时有 $b \preccurlyeq a$, 则 $b \wedge a = b$. 而运算 $\wedge$ 满足交换律, 所以

$$a \wedge b = b \wedge a.$$

  故 $a = b$. 从而 $\preccurlyeq$ 是反对称的.
- 设 $a \preccurlyeq b$, $b \preccurlyeq c$, 则 $a \wedge b = a$, $b \wedge c = b$. 那么

$$\begin{aligned} a \wedge c &= (a \wedge b) \wedge c && (a \wedge b = a) \\ &= a \wedge (b \wedge c) && (\text{结合律}) \\ &= a \wedge b && (b \wedge c = b) \\ &= a. && (a \wedge b = a) \end{aligned}$$

  所以 $a \preccurlyeq c$, 说明 $\preccurlyeq$ 是传递的.

5.23

其次, 证明 $a \wedge b$ 是 a, b 的最大下界. 因

$$
\begin{aligned}
(a \wedge b) \wedge a &= a \wedge (b \wedge a) && \text{(结合律)} \\
&= a \wedge (a \wedge b) && \text{(交换律)} \\
&= (a \wedge a) \wedge b && \text{(结合律)} \\
&= a \wedge b. && \text{(幂等律)}
\end{aligned}
$$

$$(a \wedge b) \wedge b = a \wedge (b \wedge b) = a \wedge b.$$

又由 $\preccurlyeq$ 的定义, 可得 $a \wedge b \preccurlyeq a$, $a \wedge b \preccurlyeq b$. 说明 $a \wedge b$ 是 a, b 的下界.

设 c 是 a, b 的任一下界, 则 $c \preccurlyeq a$, $c \preccurlyeq b$. 按 $\preccurlyeq$ 的定义有

$$c \wedge a = c, \qquad c \wedge b = c.$$

进而有

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

按 $\preccurlyeq$ 的定义有 $c \preccurlyeq a \wedge b$. 故 $a \wedge b$ 是 a, b 的最大下界. 5.24

第三, 证明 $a \vee b$ 是 a, b 的最小上界.

先证 $a \wedge b = a$ 与 $a \vee b = b$ 等价.

若 $a \wedge b = a$, 则

$$
\begin{aligned}
a \vee b &= (a \wedge b) \vee b && (a \wedge b = a) \\
&= b \vee (a \wedge b) && \text{(交换律)} \\
&= b \vee (b \wedge a) && \text{(交换律)} \\
&= b. && \text{(吸收律)}
\end{aligned}
$$

于是 $a \vee b = b$.

反之, 若 $a \vee b = b$, 则

$$
\begin{aligned}
a \wedge b &= a \wedge (a \vee b) && (a \vee b = b) \\
&= a. && \text{(吸收律)}
\end{aligned}
$$

亦即 $a \wedge b = a$.

由此可见, 偏序关系 $\preccurlyeq$ 的等价定义为: “$a \preccurlyeq b \iff a \vee b = b$. ” 5.25

可以用证明 “ $a \wedge b$ 是 a, b 的最大下界” 类似的方法证明 “ $a \vee b$ 是 a, b 的最小上界”.

综上所述, $\langle A, \preccurlyeq \rangle$ 是格. □

☞ 事实上, 这个定理给出的是格的另一个定义方式.

Definition 18. 设 $\langle A, \vee, \wedge\rangle$ 是一个代数系统, 其中 $\vee$, $\wedge$ 都是二元运算, 且满足交换律、结合律和吸收律, 定义 A 上的偏序关系 $\preccurlyeq$: 对任意 $a, b \in A$,

$$a \preccurlyeq b \iff a \wedge b = a. \quad (\text{或 } a \preccurlyeq b \iff a \vee b = b.)$$

则 $\langle A, \preccurlyeq\rangle$ 是一个格.

由格 $\langle A, \preccurlyeq\rangle$ 可以构造代数系统 $\langle A, \vee, \wedge\rangle$, 反过来, 由代数系统 $\langle A, \vee, \wedge\rangle$ 出发也可以返回到格 $\langle A, \preccurlyeq\rangle$. 5.26

Theorem 19 (弱分配律)**.** *在一个格 $\langle A, \preccurlyeq\rangle$ 中, 对任意的 $a, b, c \in A$, 都有*

$$a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge (a \vee c), \tag{10}$$
$$(a \wedge b) \vee (a \wedge c) \preccurlyeq a \wedge (b \vee c). \tag{11}$$

分析

- 比较: 集合的并、交运算的分配律

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C), \tag{12}$$
$$(A \cap B) \cup (A \cap C) = A \cap (B \cup C). \tag{13}$$

- 谓之 "分配不等式", 或弱分配律, 次分配律;
- 这里, (10) 式与 (11) 式是互为对偶的.

下证 (10) 式成立, (11) 式由对偶原理可得. 5.27

证 要证 $a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge (a \vee c)$, 可以先分别证明

$$a \preccurlyeq (a \vee b) \wedge (a \vee c), \tag{14}$$
$$b \wedge c \preccurlyeq (a \vee b) \wedge (a \vee c). \tag{15}$$

- (14) 式成立, 因为

$$\begin{aligned} a &= a \wedge a && (\text{幂等性}) \\ &\preccurlyeq (a \vee b) \wedge (a \vee c). && \big(a \preccurlyeq (a \vee b),\ a \preccurlyeq (a \vee c)\big) \end{aligned}$$

- (15) 式成立, 因为

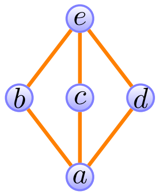
$$b \wedge c \preccurlyeq b \preccurlyeq a \vee b,$$
$$b \wedge c \preccurlyeq c \preccurlyeq a \vee c,$$

所以

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

5.28

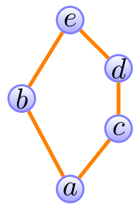
Example 20. 分配不等式实例:



$$b \wedge (c \vee d) = b \wedge e = b, \quad (b \wedge c) \vee (b \wedge d) = a \vee a = a.$$

☞ 称为钻石格 (diamond lattice). 5.29

Example 21. 分配不等式实例:



$$d \wedge (b \vee c) = d \wedge e = d, \quad (d \wedge b) \vee (d \wedge c) = a \vee c = c.$$

☞ 称为五角格 (pentagon lattice). 5.30

推论

设 $\langle A, \preccurlyeq \rangle$ 是一个格, 对于任意的 $a, b, c \in A$, 必有

$$(a \wedge b) \vee (a \wedge c) \preccurlyeq a \wedge \big(b \vee (a \wedge c)\big), \tag{16}$$

$$a \vee \big(b \wedge (a \vee c)\big) \preccurlyeq (a \vee b) \wedge (a \vee c). \tag{17}$$

证 注意到前述定理的结论:

$$a \preccurlyeq c \iff a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge c, \tag{18}$$

而 $a \preccurlyeq a \vee c$ 恒成立, 将 (18) 式中的 c 换成 $a \vee c$, 即得

$$a \preccurlyeq c \iff a \vee \big(b \wedge c\big) \preccurlyeq (a \vee b) \wedge c.$$

$$a \preccurlyeq a \vee c \iff a \vee \big(b \wedge (a \vee c)\big) \preccurlyeq (a \vee b) \wedge (a \vee c).$$

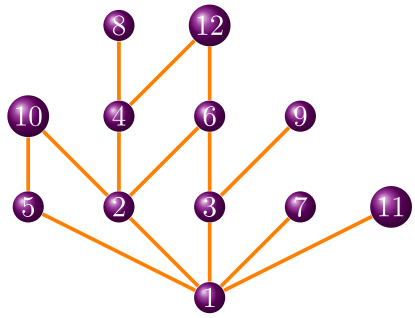
而上式左边恒成立, 则右边也恒成立. 即证 (17) 成立.

又 (16) 式与 (17) 式是互为对偶的, 所以 (16) 式成立. □ 5.31

练习

设 $L = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$, $\langle L, \preccurlyeq \rangle$ 是偏序集, $\preccurlyeq$ 定义为: 对于 $n_1, n_2 \in L$, $n_1 \preccurlyeq n_2$ 当且仅当 n_1 是 n_2 的因子. 问 $\langle L, \preccurlyeq \rangle$ 是否为格?

解 不是格. 哈斯图为:



例如, “9 和 10” 没有最小上界. □ 5.32

2 子格与格同态

Definition 22 (子格)**.** 设 $\langle A, \preccurlyeq \rangle$ 是格, $\langle A, \vee, \wedge \rangle$ 是 $\langle A, \preccurlyeq \rangle$ 诱导的代数系统. 设 B 是 A 的非空子集. 如果运算 $\vee$ 和 $\wedge$ 在 B 中封闭, 则称 $\langle B, \preccurlyeq \rangle$ 是 $\langle A, \preccurlyeq \rangle$ 的子格.

可以证明, 子格也是格.

Example 23. 设 E^+ 是正偶数的全体, 易知 $\langle E^+, | \rangle$ 是 $\langle \mathbb{Z}^+, | \rangle$ 的子格:

任何两个偶数的最大公约数和最小公倍数都是偶数, 运算 $\vee$ 和 $\wedge$ 关于 E^+ 是封闭的. 5.33

Example 24. 设 $\langle S, \preccurlyeq \rangle$ 是一个格, 任取 $a \in S$, 构造 S 的子集为:

$$T = \left\{ x \;\middle|\; x \in S \text{ 且 } x \preccurlyeq a \right\},$$

则 $\langle T, \preccurlyeq \rangle$ 是 $\langle S, \preccurlyeq \rangle$ 的一个子格.

证 对任意的 $x, y \in T$, 必有 $x \preccurlyeq a$ 和 $y \preccurlyeq a$, 所以

$$x \vee y \preccurlyeq a, \qquad (a \text{ 是 } x, y \text{ 的上界})$$
$$x \wedge y \preccurlyeq a, \qquad (x \wedge y \preccurlyeq x \vee y)$$

故

$$x \vee y \in T, \qquad x \wedge y \in T.$$

运算 $\vee$ 和 $\wedge$ 关于 T 是封闭的, 因此, $\langle T, \preccurlyeq \rangle$ 是 $\langle S, \preccurlyeq \rangle$ 的一个子格. □ 5.34

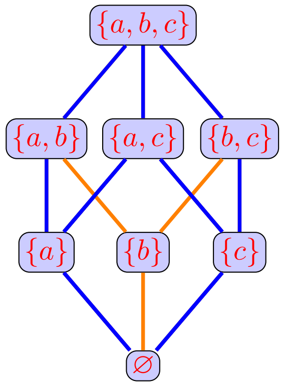
注意

若 $\langle A, \preccurlyeq \rangle$ 是格, $B \subseteq A$ 且 $B \neq \varnothing$, 则 $\langle B, \preccurlyeq \rangle$ 仍然是偏序集,

- 但 $\langle B, \preccurlyeq\rangle$ 不一定是格.
- 即使是格, 也不一定是 $\langle A, \preccurlyeq\rangle$ 的子格.

5.35

Example 25. 设 $S = \{a, b, c\}$, 则 $\langle \mathscr{P}(S), \subseteq\rangle$ 是格, 其哈斯图如下.[1em]



取
$A = \big\{\varnothing, \{a\}, \{c\}, \{a, c\}\big\}$,
$B = \big\{\varnothing, \{a\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\big\}$.
则

- $\langle A, \subseteq\rangle$ 是 $\langle \mathscr{P}(S), \subseteq\rangle$ 的子格;
- $\langle B, \subseteq\rangle$ 是格, 但不是 $\langle \mathscr{P}(S), \subseteq\rangle$ 的子格. 这是因为

$$\{a, b\} \cap \{b, c\} = \{b\} \notin B.$$

5.36

格同态

格 $\langle A, \preccurlyeq\rangle$ 可视为具有两个二元运算的代数系统 $\langle A, \vee, \wedge\rangle$, 其中运算满足交换律、结合律、吸收律和幂等律.

因此, 对格可引入代数系统中同态的概念.

5.37

格同态

Definition 26. 设 $\langle A_1, \preccurlyeq_1\rangle, \langle A_2, \preccurlyeq_2\rangle$ 是格, 它们所诱导的代数系统分别是 $\langle A_1, \vee_1, \wedge_1\rangle$, $\langle A_2, \vee_2, \wedge_2\rangle$. 如果存在映射 $f : A_1 \to A_2$, 使对任意 $a, b \in A_1$, 有

$$f(a \vee_1 b) = f(a) \vee_2 f(b), \qquad f(a \wedge_1 b) = f(a) \wedge_2 f(b).$$

- 则称 f 是从 $\langle A_1, \vee_1, \wedge_1\rangle$ 到 $\langle A_2, \vee_2, \wedge_2\rangle$ 的格同态.
- 称 $\langle f(A_1), \preccurlyeq_2\rangle$ 是 $\langle A_1, \preccurlyeq_1\rangle$ 的格同态象.
- 如果 f 是双射, 则称 f 是从 $\langle A_1, \vee_1, \wedge_1\rangle$ 到 $\langle A_2, \vee_2, \wedge_2\rangle$ 的格同构. 也称格 $\langle A_1, \preccurlyeq_1\rangle, \langle A_2, \preccurlyeq_2\rangle$ 同构.

5.38

Theorem 27. 设 f 是格 $\langle A_1, \preccurlyeq_1\rangle$ 到 $\langle A_2, \preccurlyeq_2\rangle$ 的格同态. 对任意 $x, y \in A_1$, 如果 $x \preccurlyeq_1 y$, 则 $f(x) \preccurlyeq_2 f(y)$.

证　已知 $x \preccurlyeq_1 y$, 因 $x \preccurlyeq_1 y \iff x \wedge_1 y = x$, 则

$$x \wedge_1 y = x.$$

所以

$$\begin{aligned} f(x) &= f(x \wedge_1 y) && (x \wedge_1 y = x) \\ &= f(x) \wedge_2 f(y). && (f \text{ 是格同态}) \end{aligned}$$

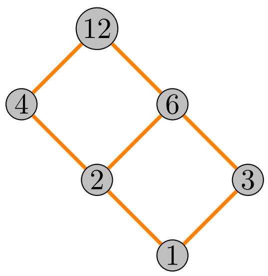
而 $f(x) \wedge_2 f(y) = f(x) \iff f(x) \preccurlyeq_2 f(y)$, 所以

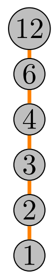
$$f(x) \preccurlyeq_2 f(y). \qquad \square$$

注:
此定理说明, 格同态是保序的. 但, 其逆不真.

5.39

Example 28. 设 $A = \{1, 2, 3, 4, 6, 12\}$, $\langle A, | \rangle$ 和 $\langle A, \preccurlyeq \rangle$ 都是格, 其中 " | " 表示整除关系, "$\preccurlyeq$" 表示数的 "小于等于" 关系.





作映射 $f: A \to A$, $f(x) = x$. 显然, 若 $x|y$, 则 $f(x) \preccurlyeq f(y)$, 因而 f 是保序的.

　但 f 不是格同态. 例如:

$$\underbrace{f(4 \wedge_1 6)}_{=2} \neq \underbrace{f(4) \wedge_2 f(6)}_{=4}.$$

5.40

Theorem 29. 设两个格为 $\langle A_1, \preccurlyeq_1 \rangle$ 和 $\langle A_2, \preccurlyeq_2 \rangle$, f 是 A_1 到 A_2 的双射. 则 f 是格 $\langle A_1, \preccurlyeq_1 \rangle$ 到 $\langle A_2, \preccurlyeq_2 \rangle$ 的格同构, 当且仅当

$$\forall\, a, b \in A_1, \quad a \preccurlyeq_1 b \iff f(a) \preccurlyeq_2 f(b). \tag{19}$$

证　(1) 设 f 是格 $\langle A_1, \preccurlyeq_1 \rangle$ 到 $\langle A_2, \preccurlyeq_2 \rangle$ 的格同构. 下证 (19) 式成立.

i) 对任意 $a, b \in A_1$, 如果 $a \preccurlyeq_1 b$, 由保序性, 则 $f(a) \preccurlyeq_2 f(b)$.

ii) 若 $f(a) \preccurlyeq_2 f(b)$, 则

$$\begin{aligned} f(a) &= f(a) \wedge_2 f(b) \\ &= f(a \wedge_1 b). && (f \text{ 是同构}) \end{aligned}$$

而 f 是双射, 则

$$
\begin{aligned}
f(a\wedge_1 b)=f(a) &\iff a\wedge_1 b=a\\
&\iff a\preccurlyeq_1 b.
\end{aligned}
$$

5.41

续证: (2) 假设对任意 $a,b\in A_1$, $a\preccurlyeq_1 b \iff f(a)\preccurlyeq_2 f(b)$. 即映射 f 是保序的.

要证 f 是 $\langle A_1,\preccurlyeq_1\rangle$ 到 $\langle A_2,\preccurlyeq_2\rangle$ 的格同构, 即要证

$$f(a\wedge_1 b)=f(a)\wedge_2 f(b), \tag{20}$$

$$f(a\vee_1 b)=f(a)\vee_2 f(b). \tag{21}$$

要证 (20) 式成立, 即要证

$$f(a\wedge_1 b)\preccurlyeq_2 f(a)\wedge_2 f(b), \qquad f(a)\wedge_2 f(b)\preccurlyeq_2 f(a\wedge_1 b)$$

同时成立.

因为 $a\wedge_1 b\preccurlyeq_1 a$, $a\wedge_1 b\preccurlyeq_1 b$, 由 f 的保序性, 得

$$f(a\wedge_1 b)\preccurlyeq_2 f(a), \qquad f(a\wedge_1 b)\preccurlyeq_2 f(b).$$

所以

$$f(a\wedge_1 b)\preccurlyeq_2 f(a)\wedge_2 f(b).$$

5.42

续证: 记 $f(a)\wedge_2 f(b)\triangleq f(d)$, 则 $f(d)\preccurlyeq_2 f(a)$, $f(d)\preccurlyeq_2 f(b)$. 由 f 的保序性, 得

$$d\preccurlyeq_1 a, \qquad d\preccurlyeq_1 b.$$

所以, $d\preccurlyeq_1 a\wedge_1 b$. 再由保序性, 得 $f(d)\preccurlyeq_2 f(a\wedge_1 b)$, 即

$$f(a)\wedge_2 f(b)\preccurlyeq_2 f(a\wedge_1 b).$$

类似可证 $f(a\vee_1 b)=f(a)\vee_2 f(b)$ 成立.

故 f 是 $\langle A_1,\preccurlyeq_1\rangle$ 到 $\langle A_2,\preccurlyeq_2\rangle$ 的格同构. □ 5.43

练习

设 $\langle A,\preccurlyeq\rangle$ 是一个格, 任取 a, b 且 $a\prec b$ (意指 $a\preccurlyeq b$ 且 $a\neq b$). 构造集合

$$B=\left\{\,x \;\middle|\; x\in A \text{ 且 } a\preccurlyeq x\preccurlyeq b\,\right\}$$

则 $\langle B,\preccurlyeq\rangle$ 也是一个格,

证 可证 $\langle B,\preccurlyeq\rangle$ 是 $\langle A,\preccurlyeq\rangle$ 的子格. 下证“集合 B 关于运算是封闭的” 即可.

任意 $x, y \in B \subseteq A$, 有

$$a \preccurlyeq x \preccurlyeq b, \quad a \preccurlyeq y \preccurlyeq b.$$

所以由 $a \preccurlyeq x$, 和 $a \preccurlyeq y$, 可得

$$a \preccurlyeq x \vee y.$$

由 $x \preccurlyeq b$, 和 $y \preccurlyeq b$, 可得

$$x \vee y \preccurlyeq b.$$

所以 $a \preccurlyeq x \vee y \preccurlyeq b$, 即 $x \vee y \in B$. 同理可证 $x \wedge y \in B$. □ 5.44

3 几种特殊的格

本节介绍几种特殊的格：

- 分配格；
- 有补格；
- 模格. 5.45

分配格

格中任意三个元素 a, b, c 满足分配不等式:

$$a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge (a \vee c) \tag{22}$$

$$a \wedge (b \vee c) \succcurlyeq (a \wedge b) \vee (a \wedge c) \tag{23}$$

是否存在格使上述两式等号成立呢?

回答是肯定的. 比如格的典型例子 $\langle \mathscr{P}(S), \subseteq \rangle$, 其分配律是成立的. 5.46

分配格

Definition 30. 设 $\langle A, \vee, \wedge \rangle$ 是由格 $\langle A, \preccurlyeq \rangle$ 诱导的代数系统. 如果对任意 a, b, $c \in A$, 满足

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c), \qquad \text{(并对交可分配)}$$

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c). \qquad \text{(交对并可分配)}$$

则称 $\langle A, \preccurlyeq \rangle$ 是分配格.

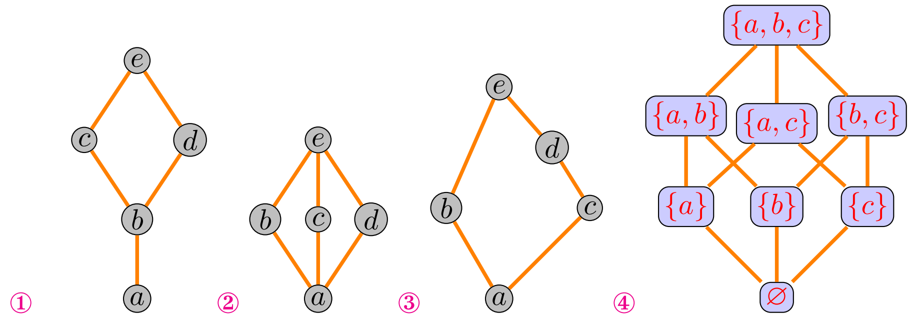
☞ 这和我们熟知的集合运算的分配律, 有完全相同的形式:

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

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

可见 $\langle \mathscr{P}(S), \subseteq \rangle$ 也是分配格的典型例子. 5.47

Example 31. 判断下列各图是否为分配格?



解　(1), (4) 是分配格. (2), (3) 不是分配格. 在 (2) 中,

$$b \wedge (c \vee d) = b \wedge e = b, \quad (b \wedge c) \vee (b \wedge d) = a \vee a = a,$$

在 (3) 中,

$$d \wedge (b \vee c) = d \wedge e = d, \quad (d \wedge b) \vee (d \wedge c) = a \vee c = c. \qquad \square$$

(2), (3) 这两个具有五个元素的格是很重要的, 分别称为钻石格 (diamond lattice) 和五角格 (pentagon lattice), 分别记为 M_3 和 N_5. 5.48

有一个如下的重要结论 (证明略去).

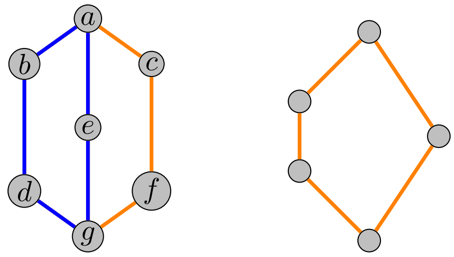
Theorem 32. 一个格是分配格的充要条件是, 在该格中没有任何子格与 M_3 和 N_5 中的任一个同构.

(a) 钻石格 M_3　　(b) 五角格 N_5

5.49

Example 33. 如图 (a) 所示的格中, $\langle \{a, b, d, g, e\}, \preccurlyeq \rangle$ 是格 $\langle \{a, b, c, d, e, f, g\}, \preccurlyeq \rangle$ 的子格,

而这个子格与图 (b) 是同构的, 所以, 图 (a) 所示的格不是分配格. 5.50



(a) (b)

Theorem 34. 如果格中运算 $\wedge$ 对运算 $\vee$ 可分配, 则运算 $\vee$ 对运算 $\wedge$ 可分配. 反之亦然.

证 设 a, b, c 是格中任意元素, 如果

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \tag{24}$$

则

$$\begin{aligned}
& (a \vee b) \wedge (a \vee c) \\
= & \big((a \vee b) \wedge a\big) \vee \big((a \vee b) \wedge c\big) && (\wedge \text{ 对 } \vee \text{ 可分配}) \\
= & a \vee \big((a \vee b) \wedge c\big) && \big((a \vee b) \wedge a = a\big) \\
= & a \vee \big((a \wedge c) \vee (b \wedge c)\big) && (\wedge \text{ 对 } \vee \text{ 可分配}) \\
= & \big(a \vee (a \wedge c)\big) \vee (b \wedge c) && (\text{结合律}) \\
= & a \vee (b \wedge c).
\end{aligned}$$

类似可证 $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \Rightarrow a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$. □ 5.51

Theorem 35. 链是分配格.

证 设 $\langle A, \preccurlyeq \rangle$ 是链, 则 $\langle A, \preccurlyeq \rangle$ 是格. (链中的任意两个元都是可比的. 比如 $a \preccurlyeq b$, 则 $a \wedge b = a$, $a \vee b = b$. 任意两个元素都有最小上界和最大下界, 所以是格.)

对任意 $a, b, c \in A$, 可分两种情况讨论:

1. $a \preccurlyeq b$ 或 $a \preccurlyeq c$.
2. $b \preccurlyeq a$ 且 $c \preccurlyeq a$.

① $a \preccurlyeq b$ 或 $a \preccurlyeq c$.

$$a \wedge (b \vee c) = \begin{cases} a \wedge c = a, & b \preccurlyeq c, \\ a \wedge b = a, & c \preccurlyeq b. \end{cases}$$

$$(a \wedge b) \vee (a \wedge c) = \begin{cases} a \vee (a \wedge c) = a, & a \preccurlyeq b, \\ (a \wedge b) \vee a = a, & a \preccurlyeq c. \end{cases}$$

所以, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$. 5.52

续证: ② $b \preccurlyeq a$ 且 $c \preccurlyeq a$.

这时必有 $b \vee c \preccurlyeq a$ (上界). 进而有

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

另一方面, 由 $b \preccurlyeq a$ 且 $c \preccurlyeq a$ 可得:

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

所以,

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

得证: 链是分配格. □ 5.53

Theorem 36. 设 $\langle A, \preccurlyeq\rangle$ 是分配格, 则对任意 $a, b, c \in A$, 如果

$$a \wedge b = a \wedge c \quad \text{且} \quad a \vee b = a \vee c$$

则必有

$$b = c.$$

证

$$\begin{aligned}
(a \wedge b) \vee c &= (a \wedge c) \vee c && (a \wedge b = a \wedge c)\\
&= c && (\text{吸收律})\\
(a \wedge b) \vee c &= (a \vee c) \wedge (b \vee c) && (\text{分配律})\\
&= (a \vee b) \wedge (b \vee c) && (a \vee b = a \vee c)\\
&= (b \vee a) \wedge (b \vee c) && (\text{交换律})\\
&= b \vee (a \wedge c) && (\text{分配律})\\
&= b \vee (a \wedge b) && (a \wedge b = a \wedge c)\\
&= b. && (\text{吸收律})
\end{aligned}$$

所以 $b = c$. □ 5.54

模格

Theorem 37. 设 $\langle A, \preccurlyeq\rangle$ 是一个格, 则对于任意的 $a, b, c \in A$, 有

$$a \preccurlyeq c \iff a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge c.$$

证 ① 设 $a \preccurlyeq c$. 由 $a \preccurlyeq c \iff (a \vee c) = c$, 得

$$\begin{aligned}
a \vee (b \wedge c) &\preccurlyeq (a \vee b) \wedge (a \vee c) && (\text{分配不等式})\\
&= (a \vee b) \wedge c. && ((a \vee c) = c)
\end{aligned}$$

② 若 $a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge c$, 则由

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

所以, $a \preccurlyeq c$. □ 5.55

Definition 38. 设 $\langle A, \vee, \wedge \rangle$ 是由格 $\langle A, \preccurlyeq \rangle$ 诱导的代数系统. 如果对任意 a, b, $c \in A$, 只要 $a \preccurlyeq c$, 就有

$$a \vee (b \wedge c) = (a \vee b) \wedge c, \tag{25}$$

则称 $\langle A, \preccurlyeq \rangle$ 是模格 (modular lattice).

☞ 对照前述结论:

设 $\langle A, \preccurlyeq \rangle$ 是一个格, 则对于任意的 a, b, $c \in A$, 有

$$a \preccurlyeq c \iff a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge c. \tag{26}$$

☞ 把 (25) 式与 "分配等式" 相比较:

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c), \tag{27}$$

知分配格必定是模格. 5.56

Theorem 39. 分配格必定是模格.

证 设 $\langle A, \preccurlyeq \rangle$ 是分配格, 任意的 a, b, $c \in A$, 若 $a \preccurlyeq c$, 则

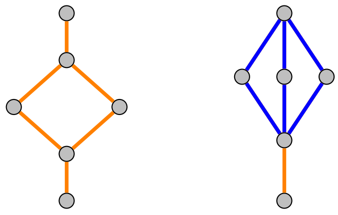
$$a \vee c = c.$$

故

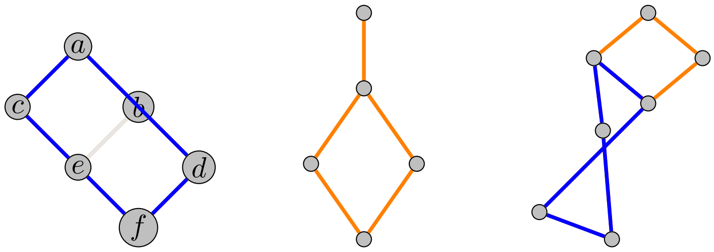
$$\begin{aligned} a \vee (b \wedge c) &= (a \vee b) \wedge (a \vee c) && \text{(分配律)} \\ &= (a \vee b) \wedge c. \end{aligned}$$

即证 $\langle A, \preccurlyeq \rangle$ 是模格. □ 5.57

模格不一定是分配格

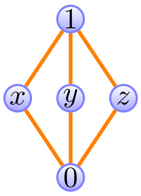


(a) (b)



(a) (b) (c)

Example 40.



钻石格 M_3 不是分配格, 但它是模格.

对于任意的 $a, b, c \in \{0, 1, x, y, z\}$, 若有 $a \preccurlyeq c$, 则必有 $a = 0$ 或者 $c = 1$.

若 $a = 0$, 则

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

若 $c = 1$, 则

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

所以它是模格. □

5.58

练习

试举两个含有 6 个元素的格, 一个是分配格, 另一个不是分配格.

解 分配格如图 (a) 所示, 不是分配格如图 (b) 所示.

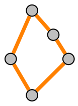
图 (b) 中有子格与钻石格同构, 所以图 (b) 不是分配格. □

当然, 分配格的最直接例子是链. 非分配格还有很多, 比如六个元素组成的一个环形结构, 此时在其中任取 5 点都是和五角格 N_5 同构的. 5.59

练习

在下图中给出的几个格, 哪个是分配格?

解 图 (b) 是分配格.

图 (a), (c) 中都有子格与  同构, 所以图 (a), (c) 不是分配格. □ 5.60

格的全下界、全上界

Definition 41. 设 $\langle A, \preccurlyeq \rangle$ 是格, 如果存在元素 $a \in A$, 对任意 $x \in A$, 都有

$$a \preccurlyeq x,$$

则称 a 为格 $\langle A, \preccurlyeq \rangle$ 的全下界. 格的全下界记为 0.

Definition 42. 设 $\langle A, \preccurlyeq \rangle$ 是格, 如果存在元素 $a \in A$, 对任意 $x \in A$, 都有

$$x \preccurlyeq a,$$

则称 a 为格 $\langle A, \preccurlyeq \rangle$ 的全上界. 格的全上界记为 1. 5.61

格的全下界、全上界

Theorem 43. *格的全下界 (全上界) 如果存在, 则必惟一.*

证 假设格 $\langle A, \preccurlyeq \rangle$ 有两个全下界 a 和 b. 那么按全下界的定义, 应有

$$a \preccurlyeq b \quad 和 \quad b \preccurlyeq a$$

同时成立, 从而

$$a = b.$$

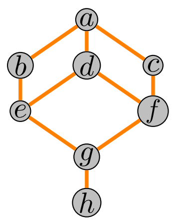
□ 5.62

有界格

Definition 44. 具有全下界和全上界的格称为有界格.

Example 45. 设 S 是有限集合, 那么格 $\langle \mathscr{P}(S), \subseteq \rangle$ 是有界格, 其全下界是 $\varnothing$, 全上界是 S.

Example 46. 如图所示的格中, h 是全下界, a 是全上界. 该格是有界格.



5.63

Theorem 47. *设 $\langle A, \preccurlyeq \rangle$ 是有界格, 则对任意 $a \in A$, 必有*

$$a \vee 1 = 1, \qquad a \wedge 1 = a; \tag{28}$$

$$a \vee 0 = a, \qquad a \wedge 0 = 0. \tag{29}$$

证　因 $\langle A, \preccurlyeq \rangle$ 是有界格, 对任意 $a \in A$, 应有 $0 \preccurlyeq a \preccurlyeq 1$. 再由格的性质, 即可得:

$$a \vee 1 = 1, \qquad a \wedge 1 = a;$$
$$a \vee 0 = a, \qquad a \wedge 0 = 0. \qquad \square$$

注

- 运算 $\vee$ 的零元和幺元分别为 1 和 0.
  - $a \vee 1 = 1 \vee a = 1 \Rightarrow$ 1 是 $\vee$ 的零元;
  - $a \vee 0 = 0 \vee a = a \Rightarrow$ 0 是 $\vee$ 的幺元.
- 运算 $\wedge$ 的零元和幺元分别为 0 和 1.
  - $a \wedge 0 = 0 \wedge a = 0 \Rightarrow$ 0 是 $\wedge$ 的零元;
  - $a \wedge 1 = 1 \wedge a = a \Rightarrow$ 1 是 $\wedge$ 的幺元.

5.64

补元

Definition 48. 设 $\langle A, \preccurlyeq \rangle$ 是有界格, 对 $a \in A$, 若存在 $b \in A$, 使

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

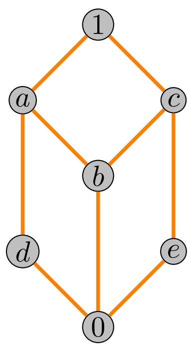
则称 b 是 a 的补元.

Example 49. 设 S 是有限集合, 对有界格 $\langle \mathscr{P}(S), \subseteq \rangle$, 其全下界是 $\varnothing$, 全上界是 S. 任意 $A \in \mathscr{P}(S)$, A 的补元是 $S - A$.

5.65

补元

Example 50.



如图所示有界格中,

- d 和 c, d 和 e, a 和 e, 0 和 1 互为补元, 即 $a, c, d, e, 0, 1$ 都有补元.
- 但 b 没有补元.
- 一个元的补元可以有多个: 例如, d, e 有两个补元;
- 0 是 1 惟一的补元; 1 是 0 惟一的补元.

对于元素 $a \in A$, 可以存在多个补元, 也可以不存在补元.

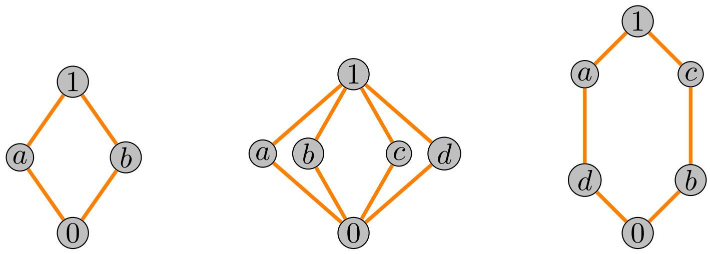
5.66

有补格

Definition 51. 在一个有界格中, 如果每个元素至少有一个补元, 则称此格为有补格.

Example 52. 如下是一些有补格的例子.

5.67



(a)　　(b)　　(c)

Theorem 53. 在有界分配格中, 若某元素有补元, 则必惟一.

证　设 a 有补元 b, c, 则有

$$a \vee b = 1, \qquad a \wedge b = 0; \tag{30}$$

$$a \vee c = 1, \qquad a \wedge c = 0. \tag{31}$$

那么,

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

由分配格的性质得

$$b = c.$$

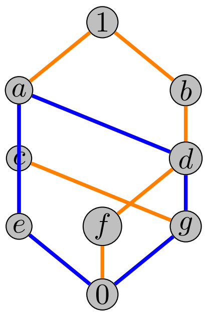
□

注

- 当补元惟一时, 我们通常用 x', $\overline{x}$ 或 $\neg x$ 表示 x 的补元.
- 注意到有补格是有界格, 故有补分配格中, 每个元素必有惟一的补元.

5.68

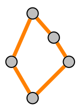
练习



试根据如图所示有界格, 回答以下问题.

- a 和 f 的补元素分别是哪些元素?
- 该有界格是分配格吗?
- 该有界格是有补格吗?

解

- a 和 f 都没有补元;
- 该有界格不是是分配格: 有子格与  同构;
- 该有界格不是有补格. □

5.69

4 布尔代数

主要内容

布尔代数 (或布尔格) 是抽象了集合运算和逻辑运算二者的根本性质的一个代数结构.

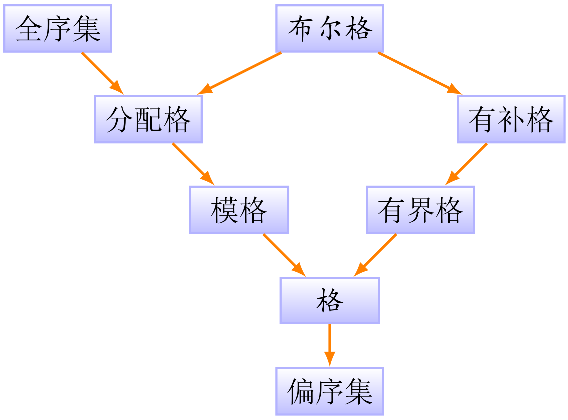
在这一节中将证明:

任何一个有限布尔代数必定与格 $\langle \mathscr{P}(S), \subseteq \rangle$ 所诱导的代数系统同构.

Definition 54. 一个有补分配格称为布尔格 (**Boolean lattice**).

5.70

概念之间的关系



5.71

布尔代数

注意到有补分配格 (布尔格) 的每个元素有补元, 且惟一.

在布尔格 $\langle A, \preccurlyeq \rangle$ 上可以确定一个一元运算, 记为 "$^-$", 使得 $\bar{a}$ 为 a 的补元. 这个一元运算称为补运算.

Definition 55. 由布尔格 $\langle A, \preccurlyeq \rangle$, 可以诱导一个代数系统 $\langle A, \vee, \wedge, ^- \rangle$, 这个代数系统称为布尔代数 (**Boolean lattice**).

☞ 为了强调布尔代数中的最小元 0 和最大元 1, 也记布尔代数为 $\langle A, \vee, \wedge, ^-, 0, 1 \rangle$.

Example 56. 设 S 是非空有限集合, 则 $\langle \mathscr{P}(S), \subseteq \rangle$ 是一个布尔格. 而由这个布尔格所诱导的代数系统 $\langle \mathscr{P}(S), \cup, \cap, \ \sim \rangle$ 是一个布尔代数.

5.72

布尔代数的等价定义

Definition 57. 布尔代数是一个集合 A, 提供了两个二元运算 $\wedge$, $\vee$, 一个一元运算 $\neg$ 和两个元素 0 和 1, 对于集合 A 的任意元素 a, b 和 c, 满足

1. 结合律: $a \vee (b \vee c) = (a \vee b) \vee c$, $a \wedge (b \wedge c) = (a \wedge b) \wedge c$;
2. 交换律: $a \vee b = b \vee a$, $a \wedge b = b \wedge a$;
3. 吸收律: $a \vee (a \wedge b) = a$, $a \wedge (a \vee b) = a$;
4. 分配律: $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$;

5. 互补律: $a \vee \neg a = 1$, $a \wedge \neg a = 0$.

☞ 前三条就是格的定义; 加上后面两条, 说明布尔代数是有补分配格. 5.73

Example 58. 最简单的布尔代数只有两个元素 0 和 1, 其运算表为:

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

a	$\neg a$
0	1
1	0

☞ 应用于逻辑和电路设计. 5.74

Theorem 59. 设 a, b 是布尔代数中任意两个元素, 则

$$\overline{(\overline{a})} = a; \tag{32}$$

$$\overline{a \vee b} = \overline{a} \wedge \overline{b}; \tag{33}$$

$$\overline{a \wedge b} = \overline{a} \vee \overline{b}. \tag{34}$$

证 ① 按定义, a 与 $\overline{a}$ 互补, 所以 $\overline{a}$ 的补元是 a, 即

$$\overline{(\overline{a})} = a. \tag{35}$$

② 可直接验证 $a \vee b$ 的补元是 $(\overline{a} \wedge \overline{b})$:

$$\begin{aligned}
(a \vee b) \vee (\overline{a} \wedge \overline{b}) &= (a \vee b \vee \overline{a}) \wedge (a \vee b \vee \overline{b}) && (\text{分配律})\\
&= (1 \vee b) \wedge (a \vee 1)\\
&= 1 \wedge 1 = 1,\\
(a \vee b) \wedge (\overline{a} \wedge \overline{b}) &= (a \wedge \overline{a} \wedge \overline{b}) \vee (b \wedge \overline{a} \wedge \overline{b})\\
&= (0 \wedge \overline{b}) \vee (\overline{a} \wedge 0)\\
&= 0 \vee 0 = 0.
\end{aligned}$$

所以 $\overline{a \vee b} = \overline{a} \wedge \overline{b}$. 同理可证 (34) 式. □ 5.75

布尔代数的同构

Definition 60. 设 $\langle A, \vee, \wedge, ^- \rangle$ 和 $\langle B, \vee, \wedge, ^- \rangle$ 是两个布尔代数, 如果存在双射 $f : A \to B$, 对任意 a, $b \in A$, 有

$$f(a \vee b) = f(a) \vee f(b) \tag{36}$$

$$f(a \wedge b) = f(a) \wedge f(b) \tag{37}$$

$$f(\overline{a}) = \overline{f(a)} \tag{38}$$

则称 $\langle A, \vee, \wedge, ^- \rangle$ 和 $\langle B, \vee, \wedge, ^- \rangle$ 同构.

5.76

5 有限布尔代数的表示定理

有限布尔代数

Definition 61. 具有有限个元素的布尔代数叫有限布尔代数.

<u>注</u>

关于有限布尔代数有如下重要结论:

- 对任一正整数 n, 必存在含有 2^n 个元素的布尔代数.
- 任一有限布尔代数的元素的个数必为 2^n, n 为正整数.
- 元素个数相同的布尔代数, 都是同构的.

为了证明上述关于有限布尔代数的结论, 先引入原子的概念. 5.77

原子

Definition 62. 设格 $\langle A, \preccurlyeq \rangle$ 具有全下界 0, 如果有元素 a 盖住[1] 0, 则称元素 a 为原子.

<u>注</u>

如果 a, b 皆为原子, $a \neq b$, 则 $a \wedge b = 0$.

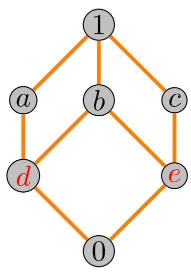
因为, 若 $a \wedge b \neq 0$, 则

$$0 \preccurlyeq a \wedge b \preccurlyeq a \ (\text{或 } b),$$

则 a 和 b 没有盖住 0, 导致 " a 和 b 不是原子" 的矛盾. 5.78

原子

Example 63. 例如, 如图所示格中, 元素 d, e 是原子.



☞ 可见

- 原子不是惟一的.
- 一个元素可以盖住多个元素. 例如, 1 盖住 a, b, c; b 盖住 d, e. 5.79

---

[1]在偏序集 $\langle A, \preccurlyeq \rangle$ 中, $\forall x, y \in A$, 如果 $x \preccurlyeq y$, $x \neq y$, 且不存在 $z \in A$ 使得 $x \preccurlyeq z \preccurlyeq y$, 则称 y 盖住 x. (见第二章)

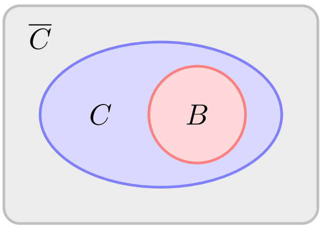


Figure 1: $B \cap \overline{C} = \varnothing$ 当且仅当 $B \subseteq C$.

Theorem 64. *设 $\langle A, \preccurlyeq \rangle$ 是一个具有全下界 0 的有限格. 若 $b \neq 0$, 则至少存在一个原子 a, 使得 $a \preccurlyeq b$.*

证　如果 b 本身为原子, 因 $b \preccurlyeq b$, 命题得证.

如果 b 不是原子, 按盖住的定义, 必存在 $b_1 \in A$, 使得

$$0 \prec b_1 \prec b.$$

若 b_1 为原子, 命题得证. 否则, 必存在 $b_2 \in A$, 使

$$0 \prec b_2 \prec b_1 \prec b.$$

因为 A 是有限集合, 经过上述有限的步骤之后, 必可找到一个原子 b_i, 使

$$0 \prec b_i \prec \cdots \prec b_2 \prec b_1 \prec b,$$

它是 $\langle A, \preccurlyeq \rangle$ 中的一条链, 其中 b_i 是原子, 且 $b_i \preccurlyeq b$. □ 5.80

引理 1
在布尔格中, $b \wedge \overline{c} = 0$ 当且仅当 $b \preccurlyeq c$.

用集合的情形, 很容易理解这个结论:

证　如果 $b \wedge \overline{c} = 0$, 则

$$\begin{aligned}
& (b \wedge \overline{c}) \vee c = 0 \vee c = c, \\
\text{又}\quad & (b \wedge \overline{c}) \vee c = (b \vee c) \wedge (\overline{c} \vee c) && \text{(分配律)} \\
& \qquad = (b \vee c) \wedge 1 \\
& \qquad = b \vee c. \\
\Rightarrow\quad & b \vee c = c \\
\Longleftrightarrow\quad & b \preccurlyeq c.
\end{aligned}$$

反之, 如果 $b \preccurlyeq c$, 则

$$\begin{aligned}
& b \wedge \overline{c} \preccurlyeq c \wedge \overline{c} && \text{(格的保序性)} \\
\Rightarrow\quad & b \wedge \overline{c} \preccurlyeq 0 \\
\Rightarrow\quad & b \wedge \overline{c} = 0.
\end{aligned}$$

□ 5.81

引理 2

设 $\langle A, \vee, \wedge, {}^{-}\rangle$ 是一个有限布尔代数, 若 $b \in A$, 且 $b \neq 0$, 又设 $a_1, a_2, \cdots, a_k$ 是 A 中满足 $a_j \preccurlyeq b$ $(j = 1, 2, \cdots, k)$ 的所有原子, 则

$$b = a_1 \vee a_2 \vee \cdots \vee a_k.$$

证　令 $c = a_1 \vee a_2 \vee \cdots \vee a_k$, 因 $a_j \preccurlyeq b$ $(0 \leqslant j \leqslant k)$, 所以 $c \preccurlyeq b$. 下面证明 $b \preccurlyeq c$.

根据引理 1, 只须证 $b \wedge \bar{c} = 0$. 用反证法.

假设 $b \wedge \bar{c} \neq 0$. 则存在原子 a, 使

$$a \preccurlyeq b \wedge \bar{c}.$$

又 $b \wedge \bar{c} \preccurlyeq b$, $b \wedge \bar{c} \preccurlyeq \bar{c}$, 由传递性得:

$$a \preccurlyeq b, \qquad a \preccurlyeq \bar{c}.$$

因 a 是原子, 且 $a \preccurlyeq b$, 所以

$$a \in \{a_1, a_2, \cdots, a_k\},$$

故 $a \preccurlyeq c$.

由 $a \preccurlyeq \bar{c}$ 和 $a \preccurlyeq c$ 可得 $a \preccurlyeq \bar{c} \wedge c$, 从而 $a \preccurlyeq 0$, 与 a 是原子矛盾.

假设不成立. 得证 $b \preccurlyeq c$. □ 5.82

引理 3

设 $\langle A, \vee, \wedge, {}^{-}\rangle$ 是一个有限布尔代数, 若 $b \in A$, 且 $b \neq 0$, 又设 $a_1, a_2, \cdots, a_k$ 是 A 中满足 $a_j \preccurlyeq b$ $(j = 1, 2, \cdots, k)$ 的所有原子, 则 $b = a_1 \vee a_2 \vee \cdots \vee a_k$ 是将 b 表示为原子的并的惟一形式.

证　设 b 有另一表达式: $b = a_{j_1} \vee a_{j_2} \vee \cdots \vee a_{j_t}$, 其中 a_{j_r} $(0 \leqslant r \leqslant t)$ 是原子. 于是有 $a_{j_r} \preccurlyeq b$ $(0 \leqslant r \leqslant t)$.

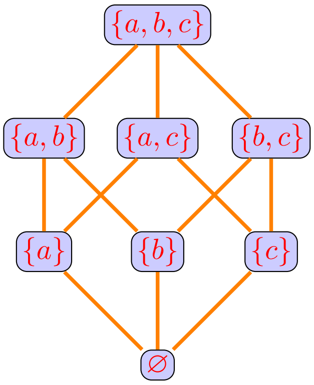
因为已设 $a_1, a_2, \cdots, a_k$ 是 A 中所有满足 $a_i \preccurlyeq b$ 的不同原子, 所以 $t \leqslant k$. 问题转化为证明 $t = k$.

假设 $t < k$, 则 $\exists\, a_{j_0} \in \{a_1, a_2, \cdots, a_k\}$, 使得 $a_{j_0} \notin \{a_{j_1}, a_{j_2}, \cdots, a_{j_t}\}$. 因

$$\begin{aligned}
& a_{j_0} \wedge (a_{j_1} \vee a_{j_2} \vee \cdots \vee a_{j_t}) = a_{j_0} \wedge (a_1 \vee a_2 \vee \cdots \vee a_{j_0} \vee \cdots \vee a_k) \\
\Longleftrightarrow\ & (a_{j_0} \wedge a_{j_1}) \vee (a_{j_0} \wedge a_{j_2}) \vee \cdots \vee (a_{j_0} \wedge a_{j_t}) \\
& \qquad = (a_{j_0} \wedge a_1) \vee (a_{j_0} \wedge a_2) \vee \cdots \vee (a_{j_0} \wedge a_{j_0}) \vee \cdots \vee (a_{j_0} \wedge a_k) \\
\Longleftrightarrow\ & 0 \vee 0 \vee \cdots \vee 0 = 0 \vee 0 \vee \cdots \vee a_{j_0} \vee 0 \vee \cdots \vee 0 \\
\Longleftrightarrow\ & a_{j_0} = 0.
\end{aligned}$$

与 a_{j_0} 是原子相矛盾, 故必有 $t = k$. □ 5.83

Example 65.



比如布尔代数 $\langle \mathscr{P}(S), \cup, \cap, \sim\rangle$, 其中

$$S = \{a, b, c\}.$$

对 $\mathscr{P}(S)$ 中的元素 $\{a, b\}$ 来说, $\{a\}$, $\{b\}$ 是满足 "$\preccurlyeq \{a, b\}$" 的所有原子, 有

$$\{a, b\} = \{a\} \cup \{b\}.$$

类似地,

$$\{a, c\} = \{a\} \cup \{c\},$$
$$\{b, c\} = \{b\} \cup \{c\},$$
$$\{a, b, c\} = \{a\} \cup \{b\} \cup \{c\}.$$

这些表示为原子的并的形式当然是惟一的.

5.84

引理 4

设 $\langle A, \preccurlyeq\rangle$ 是布尔格, a 为任意一个原子, $b \neq 0$, 则

$$a \preccurlyeq b \ \ 和 \ \ a \preccurlyeq \overline{b}$$

两式中, 有且仅有一个成立.

分析 这从含义上是不难理解的. b 的 "原子表达式"

$$b = a_1 \vee a_2 \vee \cdots \vee a_k$$

是惟一的.

对任意的原子 a, 它要么是 $a_1, a_2, \cdots, a_k$ 其中之一, 要么不在其中.

易知,

$$a \preccurlyeq b \text{ 和 } a \preccurlyeq \overline{b}$$

两式中有且仅有一个成立. **证** 因 $a \wedge b \preccurlyeq a$, 而 a 为原子, 则只可能有

$$a \wedge b = 0 \ \ 或者 \ \ a \wedge b = a.$$

1. 若 $a \wedge b = 0$, 即 $a \wedge \overline{(\overline{b})} = 0$, 根据引理 1,

$$a \wedge \overline{(\overline{b})} = 0 \Longleftrightarrow a \preccurlyeq \overline{b}$$

2. 若 $a \wedge b = a$, 由格的性质有

$$a \wedge b = a \Longleftrightarrow a \preccurlyeq b.$$

下面证明两式仅有一个成立.

假设 $a \preccurlyeq b$ 和 $a \preccurlyeq \overline{b}$ 同时成立，则

$$a \preccurlyeq b \wedge \overline{b},$$

即 $a = 0$, 这与 a 是原子矛盾. $\square$ 5.85

Theorem 66 (Stone 表示定理)**.** 设 $\langle A, \vee, \wedge, ^{-} \rangle$ 是由有限布尔格 $\langle A, \preccurlyeq \rangle$ 所诱导的有限布尔代数, S 是布尔格 $\langle A, \preccurlyeq \rangle$ 中所有原子的集合, 则

$$\langle A, \vee, \wedge, ^{-} \rangle \text{ 和 } \langle \mathscr{P}(S), \cup, \cap, \sim \rangle \text{ 同构.}$$

证明的主要思路 (具体证明略):

1. 作映射 $f : A \to \mathscr{P}(S)$,
   - 当 $a = 0$ 时, $f(a) = \varnothing$;
   - 当 $a \neq 0$ 时, $f(a) = S_i$, S_i 表示所有满足 $x \preccurlyeq a$ 的原子 x 的集合. 然后证明 f 是双射.
2. 证明 f 是同构映射:

$$\begin{aligned} f(a \vee b) &= f(a) \cup f(b), \\ f(a \wedge b) &= f(a) \cap f(b), \\ f(\overline{a}) &= \overline{f(a)}. \end{aligned}$$

5.86

Stone 表示定理

推论 1

有限布尔格的元素的个数必等于 2^n, 其中 n 是布尔格中所有原子的个数.

推论 2

元素的个数相同的有限布尔代数是同构的. 5.87

Example 67. 设 $\langle S, \vee, \wedge, ^{-} \rangle$ 是布尔代数, x, $y \in S$. 证明 $x \preccurlyeq y$ 当且仅当 $\overline{y} \preccurlyeq \overline{x}$.

解 由引理 1,

$$\begin{aligned} \overline{y} \preccurlyeq \overline{x} &\iff \overline{y} \wedge \overline{(\overline{x})} = 0 \\ &\iff \overline{y} \wedge x = 0 \\ &\iff x \wedge \overline{y} = 0 \\ &\iff x \preccurlyeq y. \end{aligned}$$

故在任何布尔代数中, $x \preccurlyeq y$ 当且仅当 $\overline{y} \preccurlyeq \overline{x}$. $\square$ 5.88

布尔表达式

Definition 68. 设 $\langle A, \vee, \wedge, {}^{-} \rangle$ 是布尔代数, 称 A 中的元素为*布尔常元*. 以 A 为取值范围的变元叫*布尔变元*.

Definition 69. 设 $\langle A, \vee, \wedge, {}^{-} \rangle$ 是布尔代数, 在其上的*布尔表达式* (Boolean expressions) 定义为:

1. A 中任何元素 (即*布尔常元*) 是布尔表达式;
2. 任何布尔变元是一个布尔表达式;
3. 若 e_1, e_2 是布尔表达式, 则 $\overline{e_1}$, $e_1 \vee e_2$, $e_1 \wedge e_2$ 也都是布尔表达式;
4. 只有通过有限次运用规则 (2), (3) 所构造的符号串是布尔表达式.

☞ *我们见过类似的定义方式: 命题演算的合式公式; 谓词演算的合式公式.* 5.89

Example 70. 设 $\langle \{0, a, b, 1\}, \vee, \wedge, {}^{-} \rangle$ 是布尔代数, 则

$$a, \tag{39}$$

$$1 \vee x_1, \tag{40}$$

$$(1 \vee x_1) \wedge x_2, \tag{41}$$

$$(a \wedge x_2) \vee (b \wedge x_1) \vee (x_2 \wedge x_3), \tag{42}$$

都是布尔表达式, 这里 x_1, x_2, x_3 是布尔变元.

并且 (40), (41), (42) 式分别称为

- 含有单个变元 x_1 的布尔表达式;
- 含有两个变元 x_1, x_2 的布尔表达式;
- 含有三个变元 x_1, x_2, x_3 的布尔表达式. 5.90

n 元布尔表达式

Definition 71. 一个含 n 个相异变元的布尔表达式, 称为 *n 元布尔表达式*, 记作

$$E(x_1, x_2, \cdots, x_n),$$

其中 $x_1, x_2, \cdots, x_n$ 为变元.

Definition 72 (布尔表达式的值)**.** 设 $\langle A, \vee, \wedge, {}^{-} \rangle$ 是布尔代数. n 元布尔表达式 $E(x_1, x_2, \cdots, x_n)$ 的值是指: 将 A 中的布尔常元作为变元 x_i 的值来代替表达式中相应的变元 (*即对变元赋值*), 从而计算得出的表达式的值. 5.91

n 元布尔表达式

Example 73. 设布尔代数 $\langle\{0,\,1\},\vee,\wedge,^{-}\rangle$ 上的一个 3 元布尔表达式为

$$E(x_1,x_2,x_3)=(x_1\vee x_2)\wedge(\overline{x_1}\vee\overline{x_2})\wedge(\overline{x_2\vee x_3}).$$

当赋值为 $x_1=1$, $x_2=0$, $x_3=1$ 时, 其值为:

$$\begin{aligned}E(1,0,\,1)&=(1\vee 0)\wedge(\overline{1}\vee\overline{0})\wedge\overline{(0\vee 1)}\\&=1\wedge 1\wedge 0\\&=0.\end{aligned}$$

5.92

布尔表达式的等价

Definition 74. 设 $E_1(x_1,x_2,\cdots,x_n)$ 和 $E_2(x_1,x_2,\cdots,x_n)$ 是布尔代数 $\langle A,\vee,\wedge,^{-}\rangle$ 上的两个 n 元布尔表达式, 如果对 n 个变元的任意赋值均相等, 即对任意赋值 $x_i=\widetilde{x_i}$, $\widetilde{x_i}\in A$ 均有

$$E_1(\widetilde{x_1},\,\widetilde{x_2},\,\cdots,\,\widetilde{x_n})=E_2(\widetilde{x_1},\,\widetilde{x_2},\,\cdots,\,\widetilde{x_n}),\tag{43}$$

则称布尔表达式 E_1, E_2 是等价的. 记作:

$$E_1(x_1,\,x_2,\,\cdots,\,x_n)=E_2(x_1,\,x_2,\,\cdots,\,x_n).\tag{44}$$

☞ 这类似于定义 "命题公式的等价"、"谓词公式的等价". 5.93

Example 75. 在布尔代数 $\langle\{0,\,1\},\vee,\wedge,^{-}\rangle$ 上的两个布尔表达式

$$E_1(x_1,x_2,x_3)=(x_1\wedge x_2)\vee(x_1\wedge\overline{x_3}),\tag{45}$$

$$E_2(x_1,x_2,x_3)=x_1\wedge(x_2\vee\overline{x_3}),\tag{46}$$

容易验证, 它们是等价的. 比如

$$\begin{aligned}E_1(0,1,1)&=(0\wedge 1)\vee(0\wedge\overline{1})=0\wedge 0=0,\\E_2(0,1,1)&=0\wedge(1\vee\overline{1})=0,\end{aligned}$$

等等.

或者直接由运算规律验证:

$$\begin{aligned}E_2(x_1,x_2,x_3)&=x_1\wedge(x_2\vee\overline{x_3})\\&=(x_1\wedge x_2)\vee(x_1\wedge\overline{x_3})&&\text{(分配律)}\\&=E_1(x_1,x_2,x_3).\end{aligned}$$

5.94

布尔函数

设 $E(x_1, x_2, \cdots, x_n)$ 是布尔代数 $\langle A, \vee, \wedge, ^- \rangle$ 上的一个 n 元布尔表达式, 因为运算 $\vee$, $\wedge$, $^-$ 在 A 上封闭, 任意有序 n 元组 $\langle a_1, a_2, \cdots, a_n \rangle$ $(a_i \in A)$, 可以对应着布尔表达式 $E(x_1, x_2, \cdots, x_n)$ 的一个值, 这个值必属于 A.

因此, $E(x_1, x_2, \cdots, x_n)$ 确定了一个由 A^n 到 A 的函数.

Definition 76. 设 $\langle A, \vee, \wedge, ^- \rangle$ 是布尔代数, 一个由 A^n 到 A 的函数如果能用 $\langle A, \vee, \wedge, ^- \rangle$ 上的一个 n 元布尔表达式来表示, 则称该函数为布尔函数.

一个由 A^n 到 A 的函数并不是一定能用 $\langle A, \vee, \wedge, ^- \rangle$ 上的一个布尔表达式表示. 5.95

Example 77. 设 $A = \{0, 1\}$, 下面的表格表示了一个从 A^3 到 A 的函数 f.

	f
$\langle 0, 0, 0 \rangle$	0
$\langle 0, 0, 1 \rangle$	0
$\langle 0, 1, 0 \rangle$	1
$\langle 0, 1, 1 \rangle$	0
$\langle 1, 0, 0 \rangle$	1
$\langle 1, 0, 1 \rangle$	1
$\langle 1, 1, 0 \rangle$	0
$\langle 1, 1, 1 \rangle$	1

容易验证其布尔函数表达式为:

$$E(x_1, x_2, x_3) = (\overline{x_1} \wedge x_2 \wedge \overline{x_3}) \vee (x_1 \wedge \overline{x_2}) \vee (x_1 \wedge x_3).$$

5.96

小项 & 大项

在给出下一个定理之前, 我们先给出小项、大项、析取范式、合取范式的概念.

Definition 78. 一个含有 n 个变元 x_1, x_2, $\cdots$, x_n 的布尔表达式, 如果它有形式

$$\widetilde{x_1} \wedge \widetilde{x_2} \wedge \cdots \wedge \widetilde{x_n} \tag{47}$$

其中 $\widetilde{x_i}$ 是 x_i 或 $\overline{x_i}$ 中的任一个, 则我们称这个布尔表达式为小项.

如果它有形式

$$\widetilde{x_1} \vee \widetilde{x_2} \vee \cdots \vee \widetilde{x_n} \tag{48}$$

则我们称这个布尔表达式为大项.

每个位置 x_i 或 $\overline{x_i}$ 必出现且仅出现一次. 和命题逻辑里的定义完全一样, 后面的很多概念均是如此. 5.97

小项 & 大项

- 两个布尔变元 x_1, x_2 可构成 2^2 个小项和 2^2 个大项;

小项	二进制下标	十进制下标	大项	二进制下标	十进制下标
$\overline{x_1} \wedge \overline{x_2}$	m_{00}	m_0	$x_1 \vee x_2$	M_{00}	M_0
$\overline{x_1} \wedge x_2$	m_{01}	m_1	$x_1 \vee \overline{x_2}$	M_{01}	M_1
$x_1 \wedge \overline{x_2}$	m_{10}	m_2	$\overline{x_1} \vee x_2$	M_{10}	M_2
$x_1 \wedge x_2$	m_{11}	m_3	$\overline{x_1} \vee \overline{x_2}$	M_{11}	M_3

- n 个布尔变元 $x_1, x_2, \cdots, x_n$, 可构成 2^n 个小 (大) 项.

5.98

析取范式 & 合取范式

Definition 79. 形如

$$m_0 \vee m_1 \vee \cdots \vee m_t \tag{49}$$

的布尔表达式称为析取范式;

形如

$$M_0 \wedge M_1 \wedge \cdots \wedge M_t \tag{50}$$

的布尔表达式称为合取范式.

其中 m_i 表示小项, M_i 表示大项, $i = 1, 2, \cdots, t$.

☞ 简言之,

- 析取范式: 小项之并;
- 合取范式: 大项之交.

5.99

Theorem 80. 对于两个元素的布尔代数 $\langle\{0, 1\}, \vee, \wedge, ^{-}\rangle$, 任意一个从 $\{0, 1\}^n$ 到 $\{0, 1\}$ 的函数都是布尔函数.

证 对于一个从 $\{0, 1\}^n$ 到 $\{0, 1\}$ 的函数, 先用那些使函数值为 1 的有序 n 元组分别构造小项

$$\widetilde{x_1} \wedge \widetilde{x_2} \wedge \cdots \wedge \widetilde{x_n}, \tag{51}$$

其中

$$\widetilde{x_i} = \begin{cases} x_i, & \text{如果有序 } n \text{ 元组中的第 } i \text{ 个分量为 } 1, \\ \overline{x_i} & \text{如果有序 } n \text{ 元组中的第 } i \text{ 个分量为 } 0. \end{cases}$$

然后, 再由这些小项所构成的析取范式, 它就是给定函数对应的布尔表达式, 从而该函数是布尔函数. □ ☞ 注: 当然, 也可用那些使函数值为 0 的有序 n 元组分别构造大项

$$\widetilde{x_1} \vee \widetilde{x_2} \vee \cdots \vee \widetilde{x_n}, \tag{52}$$

其中

$$\widetilde{x_i} = \begin{cases} x_i, & \text{如果有序 } n \text{ 元组中的第 } i \text{ 个分量为 } 0, \\ \overline{x_i} & \text{如果有序 } n \text{ 元组中的第 } i \text{ 个分量为 } 1. \end{cases}$$

由这些大项所构成的合取范式, 也是给定函数对应的布尔表达式. □ 5.100

Example 81. 求由下表所给定的函数 $f(x_1, x_2, x_3)$ 的析取范式、合取范式.

	f	构造小项	构造大项
$\langle 0, 0, 0\rangle$	1	$\overline{x_1} \wedge \overline{x_2} \wedge \overline{x_3}$	
$\langle 0, 0, 1\rangle$	0		$x_1 \vee x_2 \vee \overline{x_3}$
$\langle 0, 1, 0\rangle$	1	$\overline{x_1} \wedge x_2 \wedge \overline{x_3}$	
$\langle 0, 1, 1\rangle$	0		$x_1 \vee \overline{x_2} \vee \overline{x_3}$
$\langle 1, 0, 0\rangle$	0		$\overline{x_1} \vee x_2 \vee x_3$
$\langle 1, 0, 1\rangle$	0		$\overline{x_1} \vee x_2 \vee \overline{x_3}$
$\langle 1, 1, 0\rangle$	0		$\overline{x_1} \vee \overline{x_2} \vee x_3$
$\langle 1, 1, 1\rangle$	1	$x_1 \wedge x_2 \wedge x_3$	

解 函数 $f(x_1, x_2, x_3)$ 的析取范式:

$$f(x_1, x_2, x_3) = (\overline{x_1} \wedge \overline{x_2} \wedge \overline{x_3}) \vee (\overline{x_1} \wedge x_2 \wedge \overline{x_3}) \vee (x_1 \wedge x_2 \wedge x_3).$$

解 合取范式:

$$\begin{aligned} f(x_1, x_2, x_3) = (x_1 \vee x_2 \vee \overline{x_3}) \wedge (x_1 \vee \overline{x_2} \vee \overline{x_3}) \wedge (\overline{x_1} \vee x_2 \vee x_3) \\ \wedge (\overline{x_1} \vee x_2 \vee \overline{x_3}) \wedge (\overline{x_1} \vee \overline{x_2} \vee x_3). \end{aligned}$$

□ 5.101

一般布尔代数上的析 (合) 取范式

布尔代数 $\langle\{0, 1\}, \vee, \wedge, ^{-}\rangle$ 上的布尔表达式的析取范式、合取范式可以扩充到一般的布尔代数上.

Definition 82. 设 $E(x_1, x_2, \cdots, x_n)$ 是布尔代数 $\langle A, \vee, \wedge, ^{-}\rangle$ 上任一布尔表达式.

- 若 $E(x_1, x_2, \cdots, x_n)$ 能表示成

$$(a_0 \wedge m_0) \vee (a_1 \wedge m_1) \vee \cdots \vee (a_t \wedge m_t), \tag{53}$$

  则称形如 (53) 式的布尔表达式为析取范式;

- 若 $E(x_1, x_2, \cdots, x_n)$ 能表示成

$$(a_0 \vee M_0) \wedge (a_1 \vee M_1) \wedge \cdots \wedge (a_t \vee M_t), \tag{54}$$

  则称形如 (54) 式的布尔表达式为合取范式.

其中 a_i 表示布尔常元, m_i 表示小项, M_i 表示大项, $i = 1, 2, \cdots, t$. 5.102

Theorem 83. *设 $E(x_1, x_2, \cdots, x_n)$ 是布尔代数 $\langle A, \vee, \wedge, ^{-}\rangle$ 上任一布尔表达式, 则它一定可化为析 (合) 取范式.*

(证明略.)

☞ 作为布尔代数的直接应用, 命题逻辑可用布尔代数

$$\langle\{\mathbf{F}, \mathbf{T}\}, \vee, \wedge, ^{-}\rangle$$

来描述.

一个原子命题可视为一个布尔变元, 其值非 **T** 即 **F**. 因此, 任一复合命题都能用布尔代数

$$\langle\{\mathbf{F}, \mathbf{T}\}, \vee, \wedge, ^{-}\rangle$$

中的一个布尔函数来表示. 5.103

练习

将布尔代数 $\langle\{0, 1\}, \vee, \wedge, ^{-}\rangle$ 上的布尔表达式

$$E(x_1, x_2, x_3) = (x_1 \wedge x_2) \vee x_3 \tag{55}$$

化为合取范式.

解

$$\begin{aligned}
E(x_1, x_2, x_3) &= (x_1 \wedge x_2) \vee x_3 \\
&= (x_1 \vee x_3) \wedge (x_2 \vee x_3) \\
&= (x_1 \vee (x_2 \wedge \overline{x_2}) \vee x_3) \vee ((x_1 \wedge \overline{x_1}) \vee x_2 \vee x_3) \\
&= (x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee \overline{x_2} \vee x_3) \wedge (\overline{x_1} \vee x_2 \vee x_3) \\
&= M_0 \wedge M_2 \wedge M_4.
\end{aligned}$$

或者用列表的方式确定大项. **解**

	$E(x_1, x_2, x_3)$	构造大项
$\langle 0, 0, 0\rangle$	0	$x_1 \vee x_2 \vee x_3$
$\langle 0, 0, 1\rangle$	1	
$\langle 0, 1, 0\rangle$	0	$x_1 \vee \overline{x_2} \vee x_3$
$\langle 0, 1, 1\rangle$	1	
$\langle 1, 0, 0\rangle$	0	$\overline{x_1} \vee x_2 \vee x_3$
$\langle 1, 0, 1\rangle$	1	
$\langle 1, 1, 0\rangle$	1	
$\langle 1, 1, 1\rangle$	1	

得 $E(x_1, x_2, x_3) = (x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee \overline{x_2} \vee x_3) \wedge (\overline{x_1} \vee x_2 \vee x_3)$. □ 5.104

习题

设 $E(x_1, x_2, x_3) = (x_1 \wedge x_2) \vee (x_2 \wedge x_3) \vee (\overline{x_2} \wedge x_3)$ 是布尔代数 $\langle \{0, 1\}, \vee, \wedge, ^{-} \rangle$ 上的一个布尔表达式. 试写出 $E(x_1, x_2, x_3)$ 的析取范式和合取范式.

解 对 $E(x_1, x_2, x_3)$ 写出其对应的函数表, 然后构造小项、大项:

	$E(x_1, x_2, x_3)$	构造小项	构造大项
$\langle 0, 0, 0 \rangle$	0		$x_1 \vee x_2 \vee x_3$
$\langle 0, 0, 1 \rangle$	1	$\overline{x_1} \wedge \overline{x_2} \wedge x_3$	
$\langle 0, 1, 0 \rangle$	0		$x_1 \vee \overline{x_2} \vee x_3$
$\langle 0, 1, 1 \rangle$	1	$\overline{x_1} \wedge x_2 \wedge x_3$	
$\langle 1, 0, 0 \rangle$	0		$\overline{x_1} \vee x_2 \vee x_3$
$\langle 1, 0, 1 \rangle$	1	$x_1 \wedge \overline{x_2} \wedge x_3$	
$\langle 1, 1, 0 \rangle$	1	$x_1 \wedge x_2 \wedge \overline{x_3}$	
$\langle 1, 1, 1 \rangle$	1	$x_1 \wedge x_2 \wedge x_3$	

解 $E(x_1, x_2, x_3)$ 的析取范式:

$$\begin{aligned} E(x_1, x_2, x_3) = & \left(\overline{x_1} \wedge \overline{x_2} \wedge x_3\right) \vee \left(\overline{x_1} \wedge x_2 \wedge x_3\right) \vee \left(x_1 \wedge \overline{x_2} \wedge x_3\right) \\ & \vee \left(x_1 \wedge x_2 \wedge \overline{x_3}\right) \vee \left(x_1 \wedge x_2 \wedge x_3\right). \end{aligned}$$

$E(x_1, x_2, x_3)$ 的合取范式:

$$E(x_1, x_2, x_3) = \left(x_1 \vee x_2 \vee x_3\right) \wedge \left(x_1 \vee \overline{x_2} \vee x_3\right) \wedge \left(\overline{x_1} \vee x_2 \vee x_3\right). \qquad \square$$

5.105

Chapter 6

图

Discrete Mathematics

November 29, 2011

黄正华, 数学与统计学院, 武汉大学

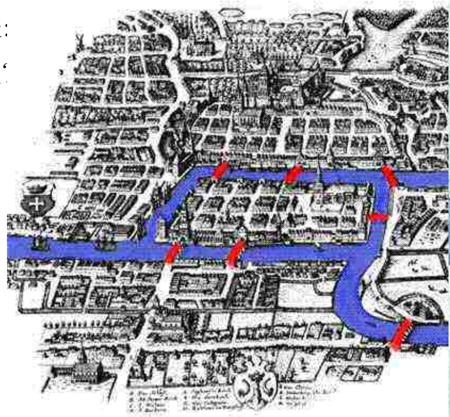
6.1

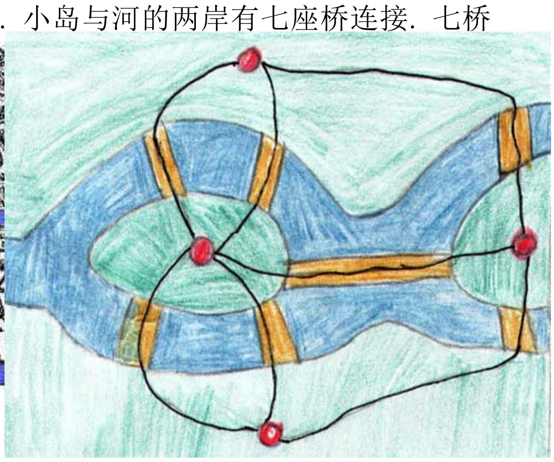
Contents

图论起源

图论的最早论文是欧拉 (Leonhard Euler) 在 1736 年发表的. 文章讨论了哥尼斯堡七桥问题. 当时哥尼斯堡 (Königsberg, 今俄罗斯加里宁格勒) 市区跨普雷格尔河 (Pregel) 两岸, 河中心有两个小岛. 小岛与河的两岸有七座桥连接. 七桥问题是:

到原地





Leonhard Euler 6.3

参考书籍

References

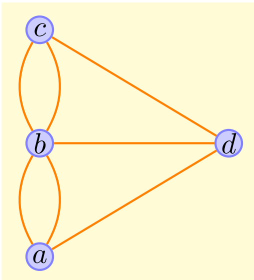
[1] J. A. Bondy and U. S. R. Murty. Graph Theory with Applications. The Macmillan Press Ltd., 1976

[2] J. A. 邦迪 U. S. R. 默蒂 著 吴望名, 李念祖, 吴兰芳, 谢伟如, 梁文沛 译 图论及其应用. 科学出版社, 1984.

6.4

1 图的基本概念

图的定义



七桥问题可以简洁地由左图表示.

这类图示包含三个组成部分: 结点、边、结点与边的对应关系. 抽象其特点, 我们得到图 (Graph) 的定义.

Definition 1. 一个图 G 是一个三元序组 $\langle V(G), E(G), \varphi_G \rangle$, 其中

- $V(G)$ 是一个非空的结点集合 (vertex set),
- $E(G)$ 是边集合 (edge set),
- φ_G 是从边集合 $E(G)$ 到结点无序偶 (有序偶) 集合上的函数.

6.5

Example 2. 设 $G = \langle V(G), E(G), \varphi_G \rangle$, 其中 $V(G) = \{a, b, c, d\}$, $E(G) = \{e_1, e_2, e_3, e_4, e_5, e_6\}$, 而 φ_G 定义为

$$\varphi_G(e_1) = (a, b), \quad \varphi_G(e_2) = (a, c),$$
$$\varphi_G(e_3) = (b, d), \quad \varphi_G(e_4) = (b, c),$$
$$\varphi_G(e_5) = (d, c), \quad \varphi_G(e_6) = (a, d).$$

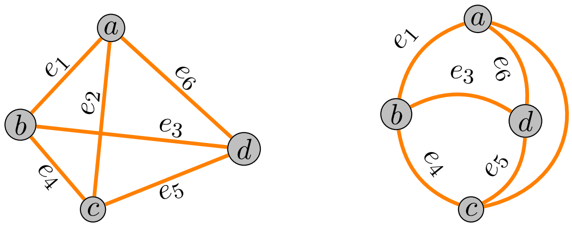
图 G 可用图形表示为如下的图 (a) 或 (b):

6.6

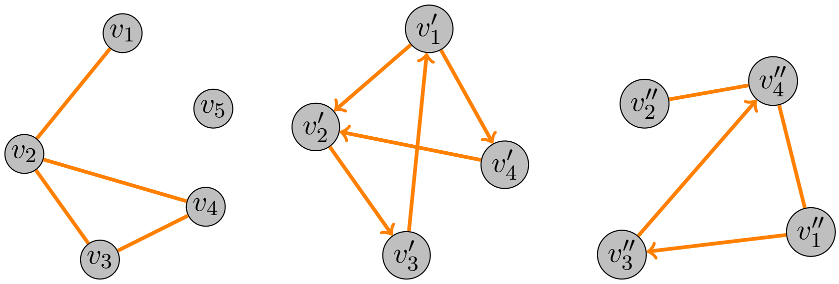
与图相关的概念和约定

- 每条边都是无向边的图叫无向图;
- 每条边都是有向边的图叫有向图;
- 既有无向边又有有向边的图叫混合图.

6.7



(a) (b)



(a) 无向图 (b) 有向图 (c) 混合图

与图相关的概念和约定

这些图可分别表示为:

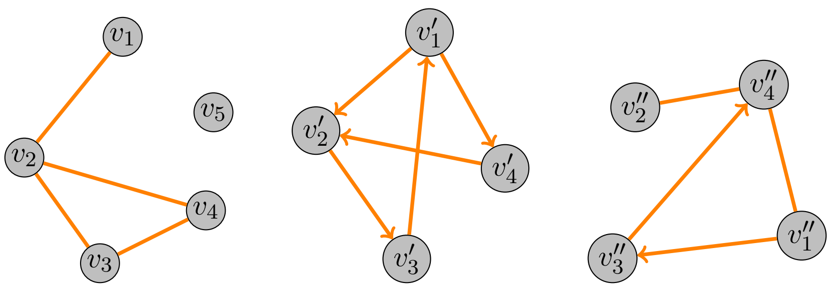
$$
\begin{aligned}
G &= \langle V,\, E\rangle = \Big\langle \{v_1, v_2, v_3, v_4, v_5\},\, \{(v_1, v_2),\, (v_2, v_3),\, (v_3, v_4),\, (v_2, v_4)\} \Big\rangle \\
G' &= \langle V',\, E'\rangle = \Big\langle \{v_1', v_2', v_3', v_4'\},\, \{\langle v_1', v_2'\rangle,\, \langle v_2', v_3'\rangle,\, \langle v_3', v_1'\rangle,\, \langle v_1', v_4'\rangle,\, \langle v_4', v_2'\rangle\} \Big\rangle \\
G'' &= \langle V'',\, E''\rangle = \Big\langle \{v_1'', v_2'', v_3'', v_4''\},\, \{(v_1'', v_4''),\, (v_2'', v_4''),\, \langle v_1'', v_3''\rangle,\, \langle v_3'', v_4''\rangle\} \Big\rangle
\end{aligned}
$$

6.8

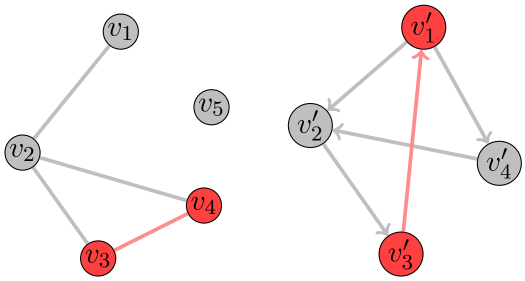
与图相关的概念和约定

- 若两个结点与同一条边相关联, 则称两个结点是邻接点.
- 关联于同一结点的两条边叫邻接边.

6.9

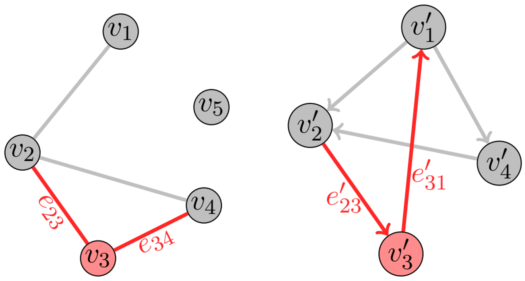


(a) G (无向图) (b) G' (有向图) (c) G'' (混合图)



(d) G (e) G'

Figure 1: 例如, “v_3 与 v_4”, “v'_1 与 v'_3” 是邻接点

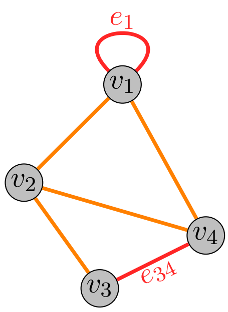


(a) G (b) G'

Figure 2: 例如, “e_{23} 与 e_{34}”, “e'_{31} 与 e'_{23}” 是邻接边

与图相关的概念和约定

- 设图 $G = \langle V, E\rangle$, $e_k = (v_i, v_j)$, 则 v_i, v_j 叫 e_k 的端点; 并称 e_k 与 v_i, v_j 相关联.
- 关联于同一结点的一条边, 称为自回路或环.
- 环的方向没有意义: 它即可作为有向边, 也可作无向边.

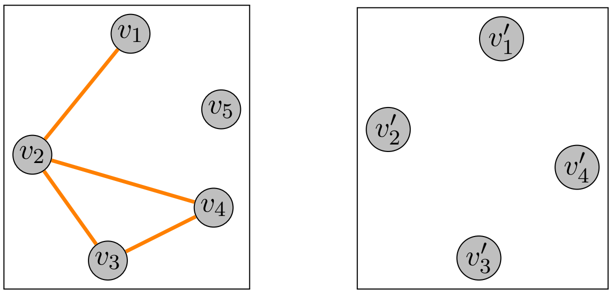


6.10

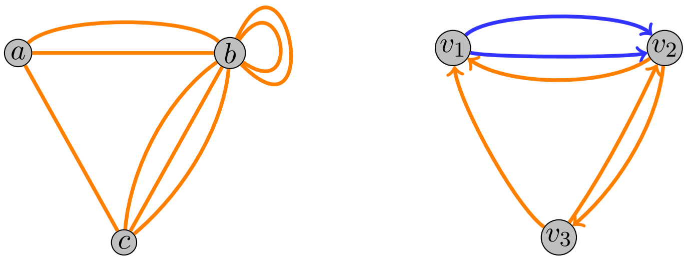
与图相关的概念和约定

- 不与任何结点相邻接的结点, 称为孤立点.
- 仅由孤立结点组成的图叫零图; 由一个孤立结点构成的图叫平凡图.

6.11



(a) 孤立点: v_5　　(b) 零图



(a)　　(b)

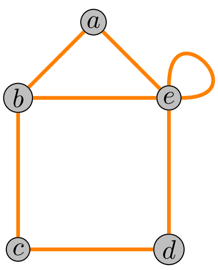
与图相关的概念和约定

- 关联于同一对结点的多条边 (有向边应同向), 叫平行边.
- 包含平行边的图, 叫多重图.
- 不含平行边和环的图, 叫简单图.

6.12

Definition 3. 在图 $G = \langle V, E\rangle$ 中, 与结点 v 相关联的边数, 叫该结点的度数, 记作 $\deg(v)$.

- 称 $\Delta(G) = \max\{\deg(v) \mid v \in V(G)\}$ 为图 G 的最大度;
- 称 $\delta(G) = \min\{\deg(v) \mid v \in V(G)\}$ 为图 G 的最小度.
- 约定: 每个环在其对应的结点上, 度数增加 2.



例如左图 G 中, 各结点度数为:

$$\deg(a) = 2; \qquad \deg(b) = 3;$$
$$\deg(c) = 2; \qquad \deg(d) = 2;$$
$$\deg(e) = 5.$$

最大度和最小度为:

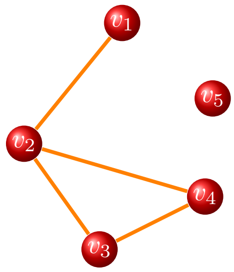
$$\Delta(G) = 5; \qquad \delta(G) = 2.$$

6.13

Theorem 4. *每个图中, 结点度数的总和等于边数的 2 倍.*

$$\sum_{v \in V} \deg(v) = 2|E|.$$

证: 因为每条边关联两个结点, 且一条边给予关联的每个结点的度数为 1,



从而一条边产生且仅产生两度, 故结点度数的总和是边数的 2 倍. □

☞ 一个图的结点度数是偶数.

6.14

Example 5. 设一个图具有 10 个结点, 而且每个结点的度数都为 6. 问此图有多少条边?

解: 结点度数的总和为

$$\sum_{v\in V}\deg(v)=10\times 6=60.$$

所以 $2|E|=60$. 得 $|E|=30$, 即此图有 30 条边. □

6.15

Theorem 6. *任何图中, 度数为奇数的结点必为偶数个.*

证: 设 V_1 和 V_2 分别是图 G 中奇数度数和偶数度数结点集. 则

$$\sum_{v\in V_1}\deg(v)+\sum_{v\in V_2}\deg(v)=\sum_{v\in V}\deg(v)=2|E|$$

上式中 $\sum\limits_{v\in V_2}\deg(v)$ 为偶数, $2|E|$ 也是偶数.

故 $\sum\limits_{v\in V_1}\deg(v)$ 必为偶数, 即 $|V_1|$ 是偶数. □

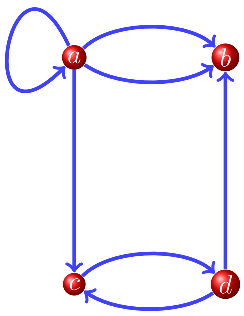
6.16

Definition 7. 在有向图 G 中,

1. 射入一个结点的边数, 称为该结点的入度, 记为 $\deg^-(v)$;
2. 由一个结点射出的边数, 称为该结点的出度, 记为 $\deg^+(v)$;
3. 结点入度与出度之和, 称为该结点的度数, 即 $\deg(v)=\deg^-(v)+\deg^+(v)$.

6.17

Example 8.



左图中,

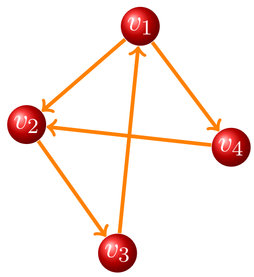
- 结点 a 的出度为 4, 入度为 1, 结点 a 的度数为 5.
- 其余各结点的度数皆为 3:
  - 结点 b 的出度为 0, 入度为 3;
  - 结点 c 的出度为 1, 入度为 2;
  - 结点 d 的出度为 2, 入度为 1.

6.18

Theorem 9. *在有向图中, 所有结点出度之和等于所有结点入度之和. 即*

$$\sum_{v \in V} \deg^-(v) = \sum_{v \in V} \deg^+(v) = |E|.$$

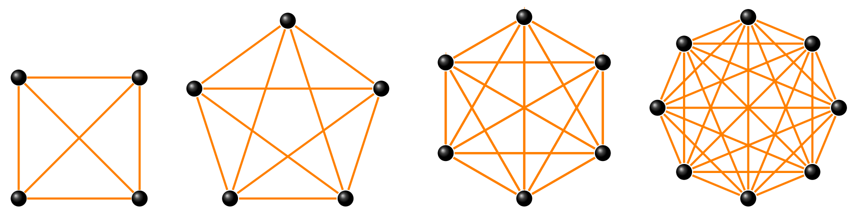
证: 因每条有向边恰好产生一个出度和一个入度,



从而出度和入度是成对出现的, 所以出度之和等于入度之和. □ 6.19

完全图

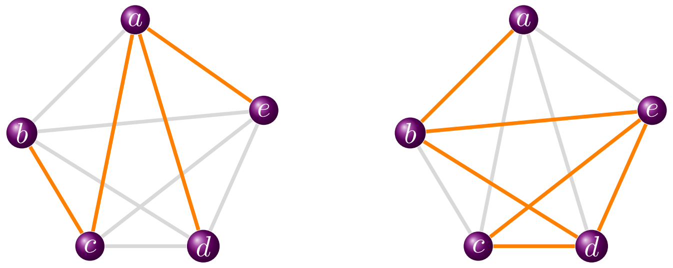
Definition 10.
- 简单图 $G = \langle V, E \rangle$ 中, 若每对结点之间均有边相连, 则称该图为完全图.
- 有 n 个结点的无向完全图记作 K_n.



(a) K_4 (b) K_5 (c) K_6 (d) K_8

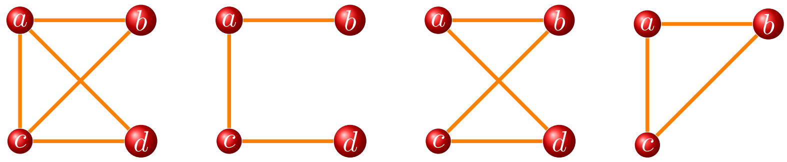
6.20

Theorem 11. *无向完全图 K_n 的边数为 $\frac{1}{2}n(n-1)$.*



(a) G (b) $\overline{G}$

Figure 3: G 与 $\overline{G}$ 互为补图.



(a) G (b) G_1 (c) G_2 (d) G_3

证: K_n 中任意两个结点有且仅有一条边相连, 那么 n 个结点中任取两个结点的组合数为

$$\binom{n}{2} = \frac{1}{2}n(n-1).$$

即 K_n 的边数为

$$|E| = \frac{1}{2}n(n-1). \qquad \square$$

<u>注意</u>

完全图, 首先是简单图 (不含有平行边和环).

6.21

Definition 12. 由图 G 的所有结点和所有能使图 G 成为完全图的添加边组成的图, 称为图 G 相对于完全图的补图, 或简称为 G 的补图, 记作 $\overline{G}$.

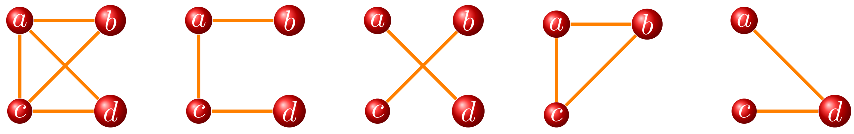
6.22

Definition 13. 给定图 $G = \langle V, E \rangle$ 和 $G_1 = \langle V_1, E_1 \rangle$,

- 如果 $E_1 \subseteq E$, $V_1 \subseteq V$, 则称 G_1 为 G 的子图.
- 如果 $V_1 = V$, 即 G_1 包含 G 的所有结点, 则称 G_1 为 G 的生成子图.

Example 14. 如图, G_1, G_2 是 G 的子图, 也是 G 的生成子图. G_3 仅为 G 的子图.

6.23



(a) G　(b) G_1　(c) G_2　(d) G_3　(e) G_4

Definition 15. 设图 $G_1 = \langle V_1, E_1 \rangle$ 是 $G = \langle V, E \rangle$ 的子图. 令 $G_2 = \langle V_2, E_2 \rangle$, 如果

- $E_2 = E - E_1$,
- 且 V_2 中仅包含 E_2 中的边所关联的结点,

则称 G_2 为子图 G_1 相对于图 G 的补图.

Example 16. 图中 G_1 相对于 G 的补图是 G_2;

而 G_3 相对于 G 的补图是 G_4. **问**: G_1 **的补图是**? 6.24

图的同构

Definition 17. 给定图 $G = \langle V, E \rangle$ 和 $G' = \langle V', E' \rangle$, 如果存在双射 $g : V \to V'$, 且 $e = (v_i, v_j)$ 是 G 的一条边当且仅当 $e' = \big(g(v_i), g(v_j)\big)$ 是 G' 的一条边, 则称 G' 与 G 同构. 记作 $G \simeq G'$.

从定义可得两图同构的几个必要条件:

1. 结点数相同;
2. 边数相同;
3. 对应结点的度数相等.

<u>注</u>

简言之, 同构的两个图的顶点之间, 具有保持相邻关系的一一对应. 6.25

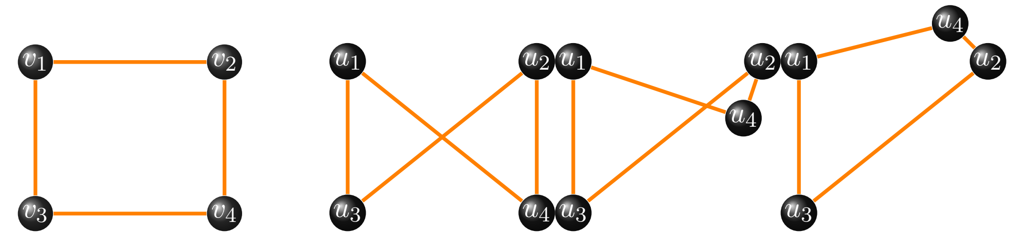
Example 18. 判断下列图是否同构:

☞ $v_1 \to u_1$, $v_3 \to u_3$, $v_4 \to u_2$, $v_2 \to u_4$, 容易判断是同构的.

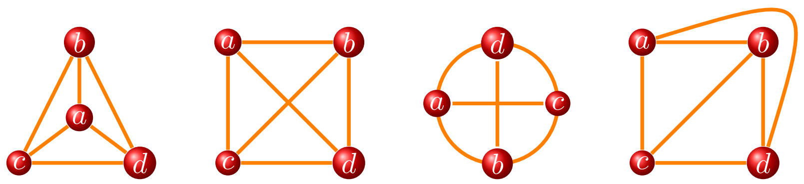
(把图 G_2 中的 u_4 上移就看得更清楚了.) 6.26

Example 19. 图中 G_1, G_2, G_3, G_4 是彼此同构的.

☞ 事实上, 它们都是完全图 K_4. 6.27



(a) G_1 (b) G_2



(a) G_1 (b) G_2 (c) G_3 (d) G_4

Example 20. 下面的三个图是同构的: 6.28

Example 21. 图中 G_1, G_2 是彼此不同构的.

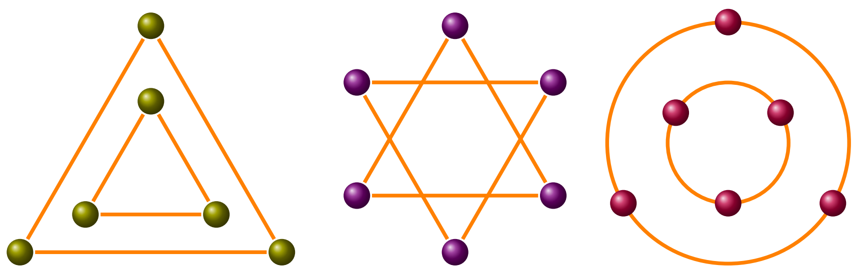
如果两图同构, 则对应结点的度数应相同.

- 度数为 3 的两个结点 v_1 与 u_1 相对应.
- 但是, 与分别 v_1 和 u_1 相邻接的各三个结点, 度数不一致:
  - v_1 的三个邻接点中, 度数为 2 的有一个, 度数为 1 的有两个;
  - u_1 的三个邻接点中, 度数为 2 的有两个, 度数为 1 的有一个. 6.29

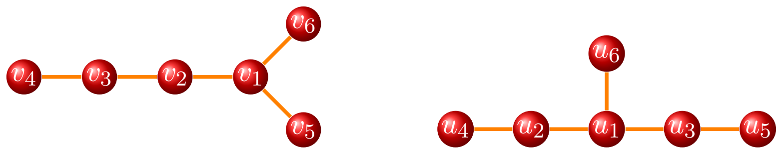
Example 22. 判断下列图是否同构:

注意 G_1 中有两个度数为 3 的结点 v_3, v_2; G_2 中度数为 3 的结点是 u_5, u_3. 容易看到图形是同构的.

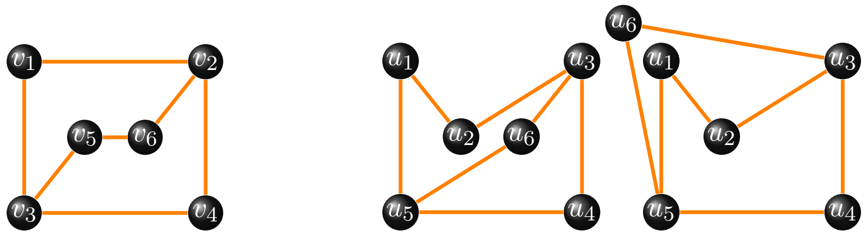
把 u_6 上移可以看得更清楚. 6.30



(a) (b) (c)



(a) G_1 (b) G_2



(a) G_1 (b) G_2

练习 P.279 (4)

下面两个图是同构的.[1]

根据点与边的关联关系, 在两图编号相同的结点间建立双射, 便可知这两个图同构. 6.31

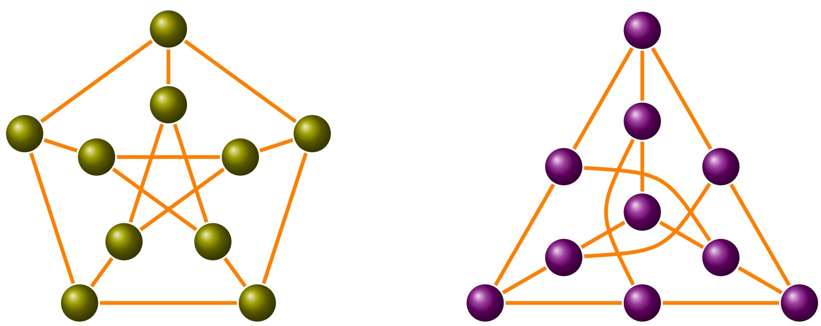
判断下列图形是否同构 6.32

判断下列图形是否同构 6.33

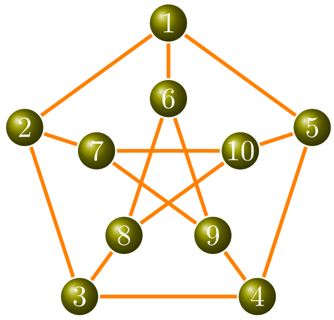
判断下列图形是否同构 6.34

判断下列图形是否同构 6.35

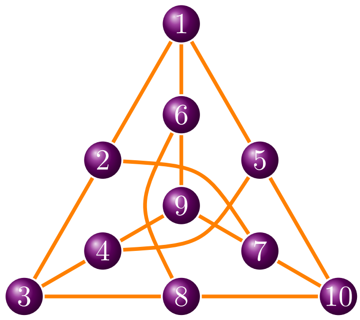
[1]彼得森图. 彼得森 (Julius Peter Christian Peterson, 1839 – 1910) 丹麦人.



(a) G_1 (b) G_2



(a) G_1



(b) G_2

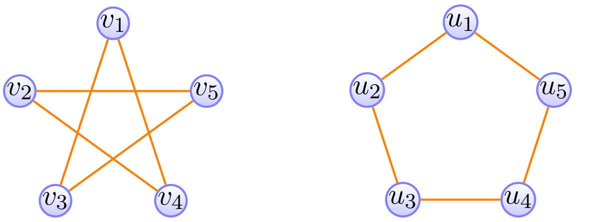


Figure 4: 判断同构性

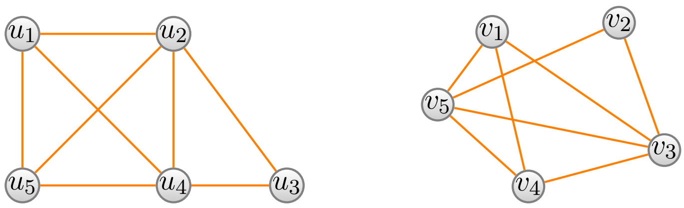


Figure 5: 判断同构性

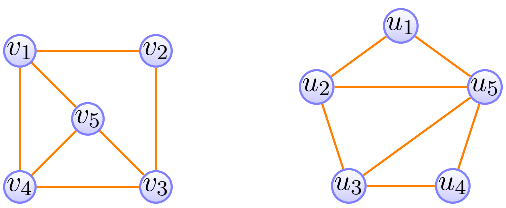


Figure 6: 判断同构性

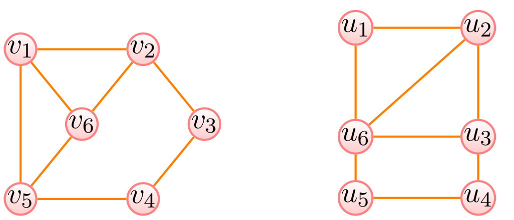


Figure 7: 判断同构性

2 路与回路

路与回路

本节主要内容:

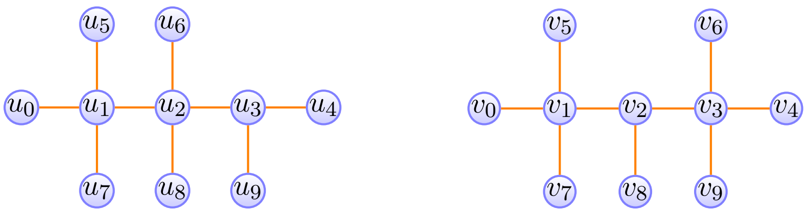


Figure 8: 判断同构性

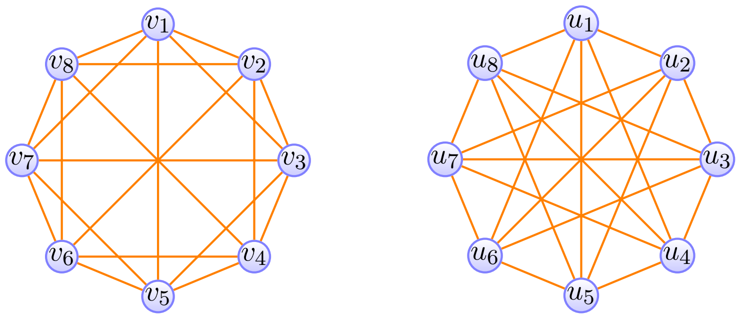


Figure 9: 判断同构性

1. 路
2. 连通的概念
3. 删除结点和边与图的连通性
4. 有向图的可达性
5. 有向图的连通性

6.36

路

图论中的一个常见问题是从给定的结点出发, 沿着边移动, 到达另一指定结点. 所经过的点边序列就形成了路的概念.

Definition 23. 给定图 $G = \langle V, E\rangle$, 设 $v_0, v_1, v_2, \cdots, v_n \in V$, $e_1, e_2, \cdots, e_n \in E$, 其中 e_i 是关联结点 v_{i-1}, v_i 的边, 点边交替序列

$$v_0 e_1 v_1 e_2 v_2 \cdots e_n v_n$$

称为联结 v_0 到 v_n 的路.

- v_0 和 v_n 分别称为该路的起点和终点.
- 如果 $v_0 = v_n$, 称该路为回路.

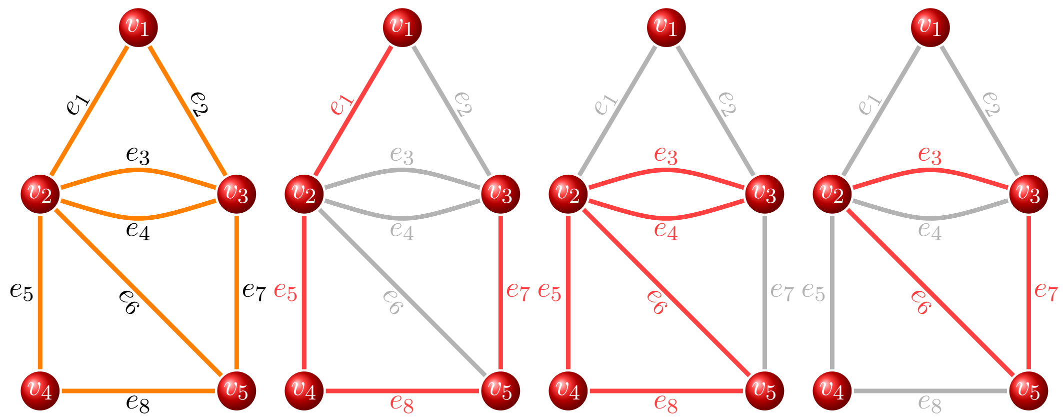
6.37

路

1. 若路中各边均不相同, 则称为迹;
2. 若路中各结点均不相同, 则称为通路;
3. 若闭合通路中各结点均不相同, 则称为圈.

6.38

例如下图中:



- $v_1e_1v_2e_5v_4e_8v_5e_7v_3$ 是迹 (无重复的边), 也是通路 (无重复结点);
- $v_2e_3v_3e_4v_2e_6v_5e_8v_4e_5v_2$ 是回路 (起点与终点重合), 但不是圈;
- $v_2e_3v_3e_7v_5e_6v_2$ 是圈 (是回路, 但没有重复的结点). 6.39

Theorem 24. *在具有 n 个结点的图中, 如果从结点 v_j 到 v_k 存在一条路, 则从结点 v_j 到 v_k 必存在一条不多于 $n-1$ 边的路.*

证: 设从结点 v_j 到 v_k 存在一路, 该路的结点序列为

$$v_j \cdots v_i \cdots v_k.$$

如果该路有 m 条边, 则该路的结点序列中有 $m+1$ 个结点.

若 $m > n-1$, 则必存在结点 v_s, 它在该路中不止出现一次, 可设该路的结点序列为

$$v_j \cdots v_s \cdots v_s \cdots v_k.$$

去掉 v_s 到 v_s 之间这段路:

$$v_j \cdots \underbrace{v_s \cdots v_s} \cdots v_k \Rightarrow v_j \cdots v_s \cdots v_k.$$

则 $v_j \cdots v_s \cdots v_k$ 仍然是 v_j 到 v_k 的路, 但此时路中边数已减少.

如果所得的这条路中的边仍然大于 $n-1$, 重复上述步骤, 最终可得一条 v_j 到 v_k 且路中边数不多于 $n-1$ 条边的路. □ 6.40

例如下图有 5 个结点, $v_1e_1v_2e_3v_3e_4v_2e_6v_5e_8v_4$ 是图中从 v_1 到 v_4 路, 它有 5 条边.

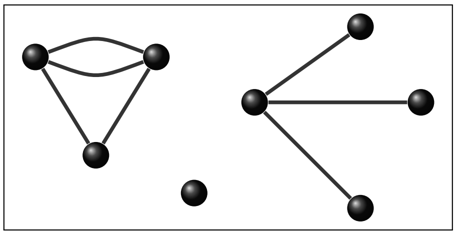
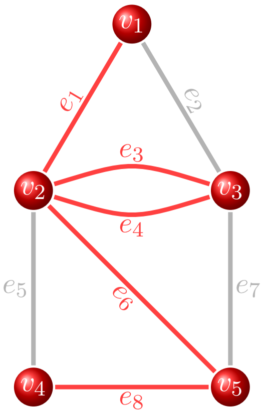


Figure 10: 非连通图 G.



去掉 v_2 到 v_2 之间的路 $e_3v_3e_4v_2$, 所得的路 $v_1e_1v_2e_6v_5e_8v_4$ 仍然是从 v_1 到 v_4 路, 其边数小于 $5-1$. 6.41

连通

Definition 25. 在无向图 G 中, 如果从结点 u 到 v 存在一条路, 则称结点 u 和结点 v 是连通的.

Definition 26. 对无向图 $G = \langle V, E\rangle$ 而言, 结点集合 V 上的连通关系是等价关系. 该连通关系将结点集合作出一个划分, 每个划分块连同它们所关联的边称为图 G 的一个连通分支. 把图 G 的连通分支数记为 $W(G)$. 6.42

Example 27. 如图, 图 G 是具有三个连通分支的非连通图.

G 的连通分支数为

$$W(G) = 3.$$

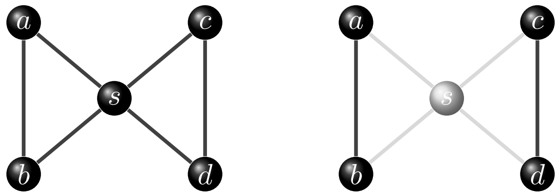
Definition 28. 若图 G 只有一个连通分支, 则称图 G 是连通图. 6.43

连通性 & 结点和边的删除

连通图中, 删除某些点或者边, 将使图变得不连通.

结点和边的删除:

- 在图中删除结点 v, 就是将结点 v 及 v 所关联的边都删除.
- 在图中删除某边, 则只须删除该边, 而保留边所关联的结点. 6.44



(a) (b)

Definition 29. 设无向图 $G = \langle V, E\rangle$ 中, 若有结点集 $V_1 \subset V$, 使图 G 删除了 V_1 的所有结点后所得的子图是不连通的, 而删除了 V_1 的任一真子集后所得的子图仍是连通的, 则称 V_1 是图 G 的*点割集*.

如果某一个结点构成一个点割集, 则称该结点为*割点*.

Example 30. 如图, (a) 中删除割点 s, 成为有两个连通分支的非连通图 (b).

6.45

Definition 31. 非完全图 G 的*点连通度* (简称*连通度*) 定义为:

$$k(G) = \min\left\{ |V_i| \,\middle|\, V_i \text{ 是点割集 } \right\}$$

由定义可知, 连通度是为了产生一个不连通图所要删除结点的最少数目. 那么,

- 非连通图的连通度为 0;
- 存在割点的连通图的连通度为 1;
- 完全图 K_n 删除 $m\,(m < n-1)$ 个结点后仍是连通的, 删除 $n-1$ 个结点后成为仅有一个孤立结点的平凡图, 故定义
$$k(K_n) = n - 1.$$

6.46

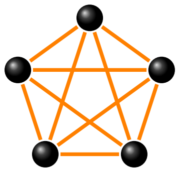
Example 32. 例如, 完全图 K_5 的删除:

所以, $k(K_5) = 4$.

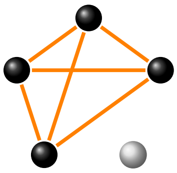
6.47

Definition 33. 设无向图 $G = \langle V, E\rangle$ 为连通图, 若有边集 $E_1 \subset E$, 使图 G 删除了 E_1 中的所有边后所得的子图是不连通的, 而删除了 E_1 的任一真子集后所得的子图仍是连通的, 则称 E_1 是图 G 的*边割集*. 如果某一条边构成一个边割集, 则称该边为*割边* (或*桥*).

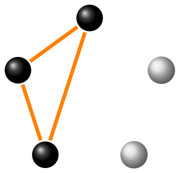
Example 34. 求下图所示的图 G 的割点和割边.



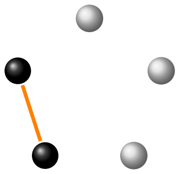
(a)



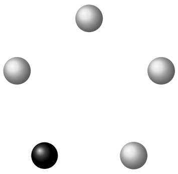
(b)



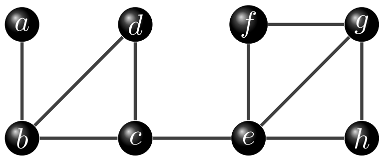
(c)



(d)



(e)



割点: b, c, e.

割边: e_{ab}, e_{ce} 6.48

Definition 35. 非平凡图 G 的边连通度定义为:

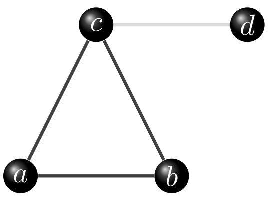
$$\lambda(G) = \min\{\, |E_1| \mid E_1 \text{ 是边割集}\}.$$

由定义可知, 边连通度是为了产生一个不连通图所要删除边的最少数目.

- 若 G 为平凡图[2], 定义 $\lambda(G) = 0$;
- G 为非连通图时 $\lambda(G)$ 亦为 0.

6.49

Example 36. 求下图所示的图 G 的边连通度.



删除边 e_{cd} 就会产生不连通图, 所以

$$\lambda(G) = 1.$$

6.50

[2]平凡图: 由一个孤立结点构成的图.

Theorem 37. 设 G 为无向图, 则

$$k(G) \leqslant \lambda(G) \leqslant \delta(G).$$

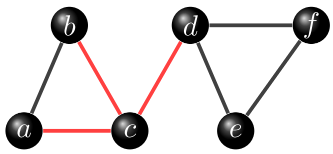
分析: $k(G)$ 是点连通度; $\lambda(G)$ 是边连通度; $\delta(G)$ 是图 G 的最小度.

证: 若 G 不连通, 则 $k(G) = \lambda(G) = 0$, 而 $\delta(G) \geqslant 0$, 故上式成立.

若 G 连通, 分两部分证明.

① 证明 $\lambda(G) \leqslant \delta(G)$.

- 如果 G 是平凡图 (只有一个孤立点构成的图), 则 $\lambda(G) = 0 \leqslant \delta(G)$.
- 如果 G 不是平凡图, 则因每一个结点所有关联的边必含有一个边割集, 故 $\lambda(G) \leqslant \delta(G)$. (因删去某结点关联的所有边, 该结点将成为孤立结点, 使原图变成不连通, 故被删去的边中必含有边割集.)



续证: 若 G 连通,

② 证 $k(G) \leqslant \lambda(G)$.

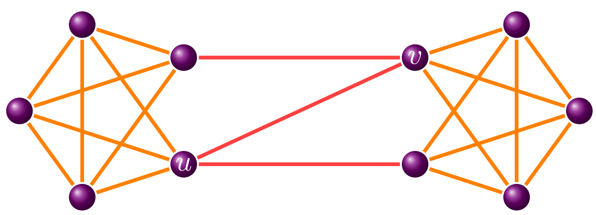
- 若 $\lambda(G) = 1$, 则 G 有一条割边, 从而 $k(G) = 1$.
- 若 $\lambda(G) \geqslant 2$, 因删去 $\lambda(G)$ 条边可使 G 不连通, 但删去 $\lambda(G) - 1$ 条边 G 仍是连通的, 且此时出现有一条桥 $e = (u, v)$.
  - 对这 $\lambda(G) - 1$ 条边中的每条边, 都选一个与 u 或 v 不同的端点, 删去这些端点, 则至少删去 $\lambda(G) - 1$ 条边.
  - 如果这时产生的图是不连通的, 则 $k(G) \leqslant \lambda(G) - 1 < \lambda(G)$;
  - 如果这时产生的图是连通的, 则 e 仍是桥, 此时再删去 u 或 v, 必产生一个非连通图, 故 $k(G) \leqslant \lambda(G)$.

由上述, 定理得证. □ 这个定理的证明可以用下图的例子予以说明. 这里

$$k(G) = 2,$$

$$\lambda(G) = 3,$$

$$\delta(G) = 4.$$



6.51

Theorem 38. 一个连通无向图 G 中的结点 v 是割点的充分必要条件是, 存在两个结点 u 和 w, 使连接结点 u 和 w 的 $[\triangle]$ 每一条路都通过 v.

证: ① 若结点 v 是连通无向图 $G = \langle V, E\rangle$ 的割点, 删去 v 得子图 G', 则 G' 至少包含两个连通分支:

$$G_1 = \langle V_1, E_1\rangle, \qquad G_2 = \langle V_2, E_2\rangle$$

取 $u \in V_1$, $w \in V_2$, 因 G 连通, 故 G 必有一条连结 u 和 w 的路 c. 但 u 和 w 在 G' 不连通, 因此路 c 必须经过点 v, 这说明连接结点 u 和 w 的每条路都通过 v.

② 反之, 若连接任意结点 v_i 和 v_j 的每条路都通过 v, 删去 v 得子图 G'', 则在 G'' 中, 此二结点必不连通的, 故 v 是图 G 的割点.

定理得证. □

6.52

有向图的连通性

- 无向图的连通概念不能直接推广到有向图.
- 在有向图 $G = \langle V, E\rangle$ 中, 如果从结点 u 到 v 有一条路, 则称从 u 可达 v.
- 如果 u 可达 v, 则 u, v 之间的最短路的长度, 称为结点 u, v 之间的距离, 记作 $d\langle u, v\rangle$, 它满足性质:

$$d\langle u, v\rangle \geqslant 0 \tag{1}$$

$$d\langle u, u\rangle = 0 \tag{2}$$

$$d\langle u, v\rangle + d\langle v, w\rangle \geqslant d\langle u, w\rangle \tag{3}$$

6.53

有向图的连通性

- 如果从 u 到 v 不可达, 则记 $d\langle u, v\rangle = \infty$.
- 距离的概念也适用于无向图.
- 注意, 对有向图, $d\langle u, v\rangle$ 一般不等于 $d\langle v, u\rangle$.
- 将 $D = \max\left\{ d\langle u, v\rangle \;\middle|\; u, v \in V \right\}$ 称为图 G 的直径.
- 可达性是有向图结点集上的二元关系, 它是自反的和传递的, 但一般不是对称的. 所以可达性不是等价关系.

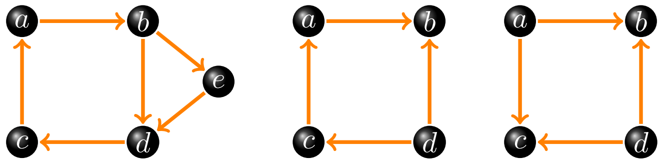
6.54

有向图的连通性

Definition 39. 在简单有向图 G 中,

- 任何一对结点间, 如果至少从一个结点到另一个结点可达, 则称该图是单侧连通的.
- 如果图 G 中任何一对结点之间相互可达, 则称图 G 是强连通的.
- 如果在图 G 中略去边的方向, 视为无向图是连通的, 则称图 G 是弱连通的.

6.55



(a) G_1 (b) G_2 (c) G_3

Example 40. 下列各有向图的连通性:

- G_1 是强连通的 (任何一对结点之间相互可达);
- G_2 是单侧连通的 (任何一对结点间, 至少从一个结点到另一个结点可达);
- G_3 是弱连通的 (略去边的方向, 视为无向图是连通的).

6.56

Theorem 41. *一个有向图是强连通的, 当且仅当 G 中有一个回路, 它至少包含每个结点一次.*

证: 充分性. 如果图 G 中有一个回路, 它至少包含每个结点一次, 则 G 中任何两个结点相互可达, 故图 G 是强连通的.

必要性. 如果有向图 G 是强连通的, 则 G 中任何两个结点相互可达, 故可从图中任一结点 v 出发, 经由图中所有的结点, 再返回 v, 从而形成一个回路. □

6.57

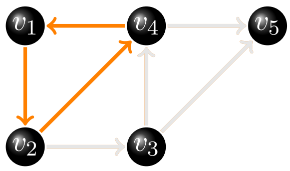
Definition 42. 在简单有向图 G 中,

- 具有强连通性的极大子图, 称为强分图. (或者说, 一个子图 G' 是**强分图**, 如果 G' 具备强连通性, 且任何包含 G' 的子图都不再具备强连通性.)
- 具有单侧连通性的极大子图, 称为单侧分图.
- 具有弱连通性的极大子图, 称为弱分图.

6.58

Example 43. 例如下图中,

- 包含结点 $\{v_1, v_2, v_3, v_4\}$ 的子图是强分图 (因为它具备强连通性, 而且再添加结点就不再具备强连通性).
- 仅包含一个孤立结点 v_5 的子图也是强分图 (再添加任意结点都不再具备强连通性).
- 包含结点 $\{v_1, v_2, v_4\}$ 的子图是强连通图, 但不是强分图 (因为添加结点 v_3 可以得到更大的强连通图).



6.59

Theorem 44. 在有向图 $G = \langle V, E\rangle$ 中, 它的每一个结点位于且只位于一个强分图中.

证: ① 设任意 $v \in V$, 令 S 是图 G 中所有与 v 相互可达的结点集合, 当然 $v \in S$. 则 S 是 G 的一个强分图. 因此, G 的每个结点必位于一个强分图中.

② 假设 v 位于两个强分图 S_1 和 S_2 中, 因 S_1 中每个结点与 v 相互可达, 而 v 与 S_2 中每个结点也相互可达, 故 S_1 和 S_2 中任何一对结点通过 v 都是相互可达的.

这与 S_1 和 S_2 为强分图矛盾. 故 G 的每个结点位于且只位于一个强分图中. □ 6.60

练习

若无向图 G 中恰有两个奇数度结点 u 和 v, 则 u, v 之间必有一条路.

解: 由结论 "任何图中奇数度结点为偶数个", 所以 u, v 必位于 G 的同一连通分支中.

则 u, v 之间必有一条路. □ 6.61

3 图的矩阵表示

图的矩阵表示

本节主要内容:

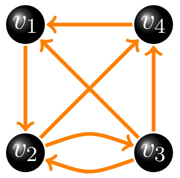
1. 邻接矩阵
2. 可达性矩阵和连通矩阵
3. 关联矩阵 6.62

邻接矩阵

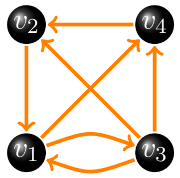
Definition 45. 设 $G = \langle V, E\rangle$ 是一个简单图, 它有 n 个结点 $V = \{v_1, v_2, \cdots v_n\}$, 则 n 阶方阵 $A(G) = (a_{ij})$ 称为 G 的邻接矩阵, 其中

$$a_{ij} = \begin{cases} 1, & v_i \text{ 与 } v_j \text{ 相邻接;} \\ 0, & \text{其它.} \end{cases}$$

6.63

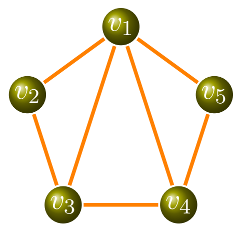


(a) G



(b) G'

Example 46.

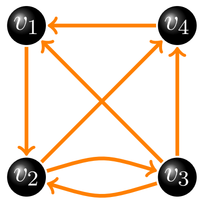


左图的邻接矩阵为:

$$A\left(G\right)=\begin{pmatrix}0&1&1&1&1\\1&0&1&0&0\\1&1&0&1&0\\1&0&1&0&1\\1&0&0&1&0\end{pmatrix}.$$

- 当给定的简单图是无向图时, 邻接矩阵是对称的;
- 当给定的图是有向图时, 邻接矩阵并不一定对称. 6.64

Example 47. 例如,



上图的邻接矩阵列为:

$$A(G)=\begin{array}{c}\\ v_1\\ v_2\\ v_3\\ v_4\end{array}\begin{array}{c}\begin{matrix}v_1&v_2&v_3&v_4\end{matrix}\\ \begin{pmatrix}0&1&0&0\\0&0&1&1\\1&1&0&1\\1&0&0&0\end{pmatrix}\end{array}.$$

有 v_i 到 v_j 的有向连线, 则 $a_{ij}=1$; 否则, $a_{ij}=0$. 6.65

图的邻接矩阵显然与 n 个结点的标定次序有关, 因而同一个图可得出不同的邻接矩阵.

例如, 在下图 G 中将结点 v_1 与 v_2 的次序交换, 得到 G':

上两图的邻接矩阵分别为:

$$A(G)=\begin{pmatrix}0&1&0&0\\0&0&1&1\\1&1&0&1\\1&0&0&0\end{pmatrix},\quad A(G')=\begin{pmatrix}0&0&1&1\\1&0&0&0\\1&1&0&1\\0&1&0&0\end{pmatrix}.$$

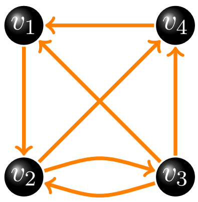
注意到, 矩阵 $A(G)$ 和 $A(G')$ 可以通过交换行和列而相互得出. 6.66

置换等价

- 一般地, 如果两个矩阵可以通过交换行和列而相互得出, 则称它们置换等价.

- 置换等价是 n 阶布尔矩阵集合上的一个等价关系.
- 忽略这种元素次序的任意性, 可取图 G 的任一邻接矩阵视为该图的邻接矩阵.

6.67

Example 48. 

例如, 上图的两个置换等价邻接矩阵:

$$A(G)=\begin{pmatrix}0&1&0&0\\0&0&1&1\\1&1&0&1\\1&0&0&0\end{pmatrix},\qquad A(G)=\begin{array}{c}\\ v_2\\ v_3\\ v_1\\ v_4\end{array}\!\!\begin{array}{c}\begin{array}{cccc}v_2&v_3&v_1&v_4\end{array}\\ \begin{pmatrix}0&1&0&1\\1&0&1&1\\1&0&0&0\\0&0&1&0\end{pmatrix}\end{array}.$$

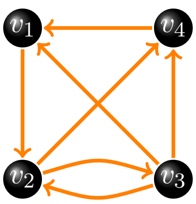
6.68

简单有向图 G 的邻接矩阵 $A(G)=\left(a_{ij}\right)_{n\times n}$ 中,

1. 第 i 行元素之和等于 v_i 的出度.
2. 第 j 列元素之和等于 v_j 的入度.

例如, 如图有向图中,

- v_3 的出度 $=1+1+0+1=3$,
- v_3 的入度 $=0+1+0+0=1$.

Example 49. 

$$A(G)=\begin{array}{c}\\ v_1\\ v_2\\ v_3\\ v_4\end{array}\!\!\begin{array}{c}\begin{array}{cccc}v_1&v_2&v_3&v_4\end{array}\\ \begin{pmatrix}0&1&0&0\\0&0&1&1\\1&1&0&1\\1&0&0&0\end{pmatrix}\end{array}.$$

6.69

邻接矩阵的应用

问题: 设图 $G=\langle V,E\rangle$ 的邻接矩阵为 $A(G)$, $V=\{v_1,v_2,\cdots,v_n\}$. 如何计算连结 v_i 与 v_j 长度为 2 的路的数目?

分析: 注意从 v_i 到 v_j 长度为 2 的路中间必经由某个结点 v_k, 即 $v_i\to v_k\to v_j$, 而且 $a_{ik}=a_{kj}=1$, 那么 $a_{ik}\cdot a_{kj}=1$.

反之, 如果不存在路径 $v_iv_kv_j$, 则 $a_{ik}=0$ 或 $a_{kj}=0$, 从而 $a_{ik}\cdot a_{kj}=0$.

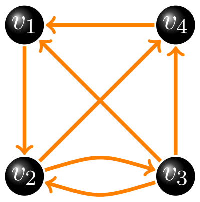
所以从 v_i 到 v_j 长度为 2 的路径的数目等于

$$\underbrace{a_{i1}\cdot a_{1j}}_{v_iv_1v_j}+\underbrace{a_{i2}\cdot a_{2j}}_{v_iv_2v_j}+\cdots+\underbrace{a_{in}\cdot a_{nj}}_{v_iv_nv_j}=\sum_{k=1}^{n}\underbrace{a_{ik}\cdot a_{kj}}_{v_iv_kv_j}$$

按矩阵的乘法法则, 此和式恰好是 $\left(A(G)\right)^2$ 中第 i 行第 j 列元素 $a_{ij}^{(2)}$.

$$\left(a_{ij}^{(2)}\right)_{n\times n}=\left(A\left(G\right)\right)^2=\begin{pmatrix}a_{11}&a_{12}&\cdots&a_{1n}\\a_{21}&a_{22}&\cdots&a_{2n}\\\vdots&\vdots&&\vdots\\a_{n1}&a_{n2}&\cdots&a_{nn}\end{pmatrix}\cdot\begin{pmatrix}a_{11}&a_{12}&\cdots&a_{1n}\\a_{21}&a_{22}&\cdots&a_{2n}\\\vdots&\vdots&&\vdots\\a_{n1}&a_{n2}&\cdots&a_{nn}\end{pmatrix}.$$

6.70



Example 50.

$$A(G)=\begin{pmatrix}0&1&0&0\\0&0&1&1\\1&1&0&1\\1&0&0&0\end{pmatrix}$$

$$\left(A(G)\right)^2=\begin{pmatrix}0&0&1&1\\2&1&0&1\\1&1&1&1\\0&1&0&0\end{pmatrix}$$

例如, 如左有向图, $\left(A(G)\right)^2$ 中的第 2 行第 1 列元素等于 2, 说明连结 v_2 与 v_1 长度为 2 的路的有两条: $v_2v_4v_1$, $v_2v_3v_1$.

分析*:*

$$\begin{aligned}a_{21}^{(2)}&=a_{21}a_{11}+a_{22}a_{21}+a_{23}a_{31}+a_{24}a_{41}\\&=0\cdot0+0\cdot0+1\cdot1+1\cdot1=2.\end{aligned}$$

注意从 v_2 到 v_1 长度为 2 的路中间必经由一个结点 v_k, 即 $v_2\to v_k\to v_1$.

比如, $k=3$ 时, $a_{23}a_{31}=1\cdot1$ 表示从 v_2 到 v_3, 再 v_3 到 v_1 有路.

6.71

☞ 还可以进一步计算从 v_i 到 v_j 长度为 3 的路的数目.

注意从 v_i 到 v_j 长度为 3 的路径可视为从 v_i 到中间结点 v_k 长度为 1 的路径, 再连接从 v_k 到 v_j 长度为 2 的路径.

所以从 v_i 到 v_j 长度为 3 的路径的数目等于

$$a_{ij}^{(3)}=\sum_{k=1}^{n}a_{ik}\cdot a_{kj}^{(2)},$$

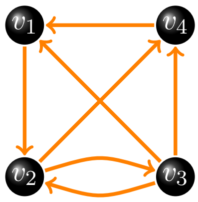
即

$$\left(a_{ij}^{(3)}\right)_{n\times n}=\left(A(G)\right)^3=\left(A(G)\right)\cdot\left(A(G)\right)^2.$$

一般地有:

$$\left(a_{ij}^{(l)}\right)_{n\times n}=\left(A\left(G\right)\right)^l=\underbrace{\begin{pmatrix}a_{11}&\cdots&a_{1n}\\\vdots&\ddots&\vdots\\a_{n1}&\cdots&a_{nn}\end{pmatrix}\cdots\begin{pmatrix}a_{11}&\cdots&a_{1n}\\\vdots&\ddots&\vdots\\a_{n1}&\cdots&a_{nn}\end{pmatrix}}_{l}.$$

$a_{ij}^{(l)}$ 表示从 v_i 到 v_j 长度为 l 的路的数目. 6.72



Example 51.
$$A(G)=\begin{pmatrix}0&1&0&0\\0&0&1&1\\1&1&0&1\\1&0&0&0\end{pmatrix}$$

$$\left(A(G)\right)^2=\begin{pmatrix}0&0&1&1\\2&1&0&1\\1&1&1&1\\0&1&0&0\end{pmatrix}$$

$$\left(A(G)\right)^3=A(G)\cdot\left(A(G)\right)^2=\begin{pmatrix}2&1&0&1\\1&2&1&1\\2&2&1&2\\0&0&1&1\end{pmatrix}$$

比如, $\left(A(G)\right)^3$ 中的第 2 行第 1 列元素等于 1, 说明连结 v_2 与 v_1 长度为 3 的路的有一条 (即 $v_2v_3v_4v_1$).

6.73

前述的结论对无向图也是成立的.

Theorem 52. 设图 $G=\langle V,E\rangle$ 的邻接矩阵为 $A(G)$, 则矩阵 $\left(A(G)\right)^l$ 中的第 i 行第 j 列元素等于 G 中连结 v_i 与 v_j 长度为 l 的路的数目.

证: 对 l 用数学归纳法.

当 $l=2$ 时, 由前述讨论可知成立.

设命题对 l 成立, 由
$$\left(A(G)\right)^{l+1}=A(G)\cdot\left(A(G)\right)^l,$$
故
$$a_{ij}^{(l+1)}=\sum_{k=1}^{n}a_{ik}\cdot a_{kj}^{(l)},$$
上式右边的每一项表示由 v_i 经过一条边到 v_k, 再由 v_k 经过一条长度为 l 的路到 v_j 的总长度为 $l+1$ 的路的数目.

对所有 k 求和, 即得 $a_{ij}^{(l+1)}$ 是所有从 v_i 到 v_j 的长度为 $l+1$ 的路的数目, 故命题对 $l+1$ 成立. □ 6.74

可达性矩阵

对一个有 n 个结点的有向图, 要判断一个结点 v_i 到 v_j 是否存在路, 可以计算 $A,A^2,A^3,\cdots,A^n$. 当有某个 A^l 的 $a_{ij}^{(l)}\geqslant 1$, 就表明结点 v_i 到 v_j 可达.

(这里最多计算到 A^n 就可以了: 具有 n 个结点的有向图, 若结点 v_i 到 v_j 有一条路, 则必然有一条长度不超过 n 的通路.)

有向图 G 中从 v_i 到 v_j 是否有路可达, 可用矩阵表达.

Definition 53. 设 $G=\langle V,E\rangle$ 为简单有向图, $V=\{v_1,v_2,\cdots v_n\}$, 定义一个 $n\times n$ 矩阵 $P=(p_{ij})$, 其中
$$p_{ij}=\begin{cases}1, & \text{从 } v_i \text{ 到 } v_j \text{ 至少存在一条路},\\ 0, & \text{从 } v_i \text{ 到 } v_j \text{ 不存在路}.\end{cases}$$

称 P 为图 G 的可达性矩阵.

6.75

邻接矩阵 & 可达性矩阵

☞ 由图 G 的邻接矩阵 A, 可以得到可达性矩阵 P:
令

$$B_n = A + A^2 + \cdots + A^n,$$

将 B_n 中不为零的元素全部换成 1, 而等于零的元素不变, 即得可达性矩阵 P. 6.76

Example 54. 设图 G 的邻接矩阵为 $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$, 求可达性矩阵.

解:

$$A^2 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 2 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad A^3 = \begin{pmatrix} 2 & 1 & 0 & 1 \\ 1 & 2 & 1 & 1 \\ 2 & 2 & 1 & 2 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad A^4 = \begin{pmatrix} 1 & 2 & 1 & 1 \\ 2 & 2 & 2 & 3 \\ 3 & 3 & 2 & 3 \\ 2 & 1 & 0 & 1 \end{pmatrix},$$

$$B_4 = A + A^2 + A^3 + A^4 = \begin{pmatrix} 3 & 4 & 2 & 3 \\ 5 & 5 & 4 & 6 \\ 7 & 7 & 4 & 7 \\ 3 & 2 & 1 & 2 \end{pmatrix}, \quad P = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

☞ 我们只关心矩阵里的元是否非零, 所以可以进行矩阵的布尔运算. 6.77

布尔矩阵的和、积

设 $A = (a_{ij})_{n\times n}$, $B = (b_{ij})_{n\times n}$ 是布尔矩阵,

1. 令 $C = A \vee B = (c_{ij})_{n\times n}$, 称为布尔矩阵求 "和", 其中
$$c_{ij} = a_{ij} \vee b_{ij}.$$
2. 令 $D = A \circ B = (d_{ij})_{n\times n}$, 称为布尔矩阵求 "积", 其中
$$d_{ij} = \bigvee_{k=1}^{n} (a_{ik} \wedge b_{kj}).$$

Example 55.

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \vee \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

6.78

可达性矩阵的计算

求可达性矩阵可简化为:

1. 由图 G 的邻接矩阵 A 求可达性矩阵 P:
$$P = A^{(1)} \vee A^{(2)} \vee \cdots \vee A^{(n)},$$
其中的元素 $A^{(i)}$ 表示 A^i 对应的布尔矩阵.

2. 用 Warshall 算法计算:

- 因为有向简单图的邻接矩阵 A 可视为: 具有 n 个结点的集合 V 上的邻接关系 R 的关系矩阵;
- 而可达性矩阵可视为: 邻接关系 R 的传递闭包所对应的矩阵.

6.79

计算可达性矩阵举例

$$A=\begin{pmatrix}0&1&0&0\\0&0&1&1\\1&1&0&1\\1&0&0&0\end{pmatrix} A^2=\begin{pmatrix}0&0&1&1\\2&1&0&1\\1&1&1&1\\0&1&0&0\end{pmatrix} A^3=\begin{pmatrix}2&1&0&1\\1&2&1&1\\2&2&1&2\\0&0&1&1\end{pmatrix} A^4=\begin{pmatrix}1&2&1&1\\2&2&2&3\\3&3&2&3\\2&1&0&1\end{pmatrix}$$

方法 1. 先由邻接矩阵 A 求 B_4,

$$B_4 = A + A^2 + A^3 + A^4,$$

然后写出可达性矩阵 P.

$$B_4 = \begin{pmatrix}3&4&2&3\\5&5&4&6\\7&7&4&7\\3&2&1&2\end{pmatrix}, \quad P = \begin{pmatrix}1&1&1&1\\1&1&1&1\\1&1&1&1\\1&1&1&1\end{pmatrix}.$$

6.80

计算可达性矩阵举例

方法 2. 将 A, A^2, A^3, A^4 转换为布尔矩阵 $A^{(1)}$, $A^{(2)}$, $A^{(3)}$, $A^{(4)}$, 则

$$P = A^{(1)} \vee A^{(2)} \vee A^{(3)} \vee A^{(4)}.$$

$$P = \begin{pmatrix}0&1&0&1\\0&0&1&1\\1&1&0&1\\1&0&0&0\end{pmatrix} \vee \begin{pmatrix}0&0&1&1\\1&1&0&1\\0&1&1&1\\0&1&0&0\end{pmatrix} \vee \begin{pmatrix}1&1&0&1\\1&1&1&1\\1&1&1&1\\0&0&1&1\end{pmatrix} \vee \begin{pmatrix}1&1&1&1\\1&1&1&1\\1&1&1&1\\1&1&0&1\end{pmatrix}$$

$$= \begin{pmatrix}1&1&1&1\\1&1&1&1\\1&1&1&1\\1&1&1&1\end{pmatrix}.$$

6.81

计算可达性矩阵举例

方法 3. 用 Warshall 算法计算, 逐列进行: 在第 i 列中若有 $a_{ji} = 1$, 则把第 i 行叠加到第 j 行.

$$M := \underbrace{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}}_{i=1} := \underbrace{\begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}}_{i=2}$$

$$:= \underbrace{\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}}_{i=3} := \underbrace{\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}}_{i=4} = P.$$

6.82

关联矩阵

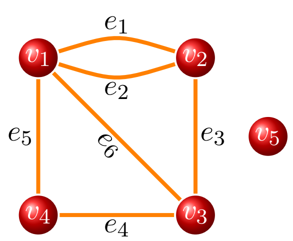
Definition 56. 设 $G = \langle V, E \rangle$ 为无向图, $V = \{v_1, v_2, \cdots v_p\}$, $E = \{e_1, e_2, \cdots e_q\}$, 定义矩阵 $M(G) = \left(m_{ij}\right)_{p \times q}$, 其中

$$m_{ij} = \begin{cases} 1, & \text{若 } v_i \text{ 关联 } e_j, \\ 0, & \text{若 } v_i \text{ 不关联 } e_j. \end{cases}$$

称 $M(G)$ 为图 G 的完全关联矩阵.

6.83

Example 57. 例如, 写出下图的关联矩阵.



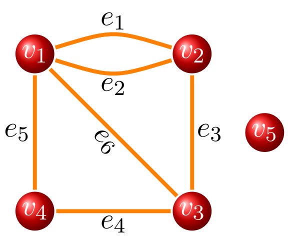
$$M(G) = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{cccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}.$$

6.84

从完全关联矩阵可得出图的有关信息:

1. 因每边只关联两个结点, 故每列有且只有两个 1, 其余为 0.
2. 每行各元素之和即相应结点的度数.
3. 若某行各元素皆为 0, 则相应结点为孤立结点.
4. 平行边所对应的列完全相同.

5. 同一个图当结点或边的编序不同时，其对应的关联矩阵仅有行序和列序的差异.



$$M(G) = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{cccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}.$$

6.85

完全关联矩阵

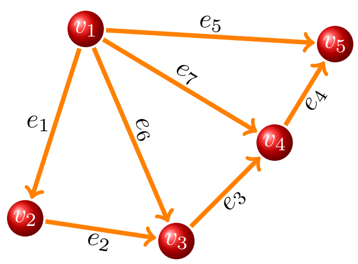
Definition 58. 设 $G = \langle V, E\rangle$ 为简单有向图, $V = \{v_1, v_2, \cdots v_p\}$, $E = \{e_1, e_2, \cdots e_q\}$, 定义矩阵 $M(G) = \left(m_{ij}\right)_{p\times q}$, 其中

$$m_{ij} = \begin{cases} 1, & \text{若在 } G \text{ 中 } v_i \text{ 是 } e_j \text{ 的起点,} \\ -1, & \text{若在 } G \text{ 中 } v_i \text{ 是 } e_j \text{ 的终点,} \\ 0, & \text{若 } v_i \text{ 与 } e_j \text{ 不关联.} \end{cases}$$

$M(G)$ 称为有向图 G 的完全关联矩阵.

6.86

Example 59. 例如, 写出如下简单有向图的关联矩阵.

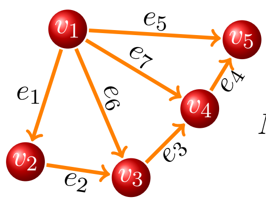


$$M(G) = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{ccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & -1 & -1 & 0 & 0 \end{pmatrix} \end{array}.$$

6.87

从有向图的完全关联矩阵可得出图的有关信息:

1. 每边关联一个始点, 一个终点. 故每列只有一个元素为 1, 一个元素为 -1, 其余为 0.
2. 每行的 1 之和即相应结点的出度, -1 之和即相应结点的入度.
3. 若某行各元素皆为 0, 则相应结点为孤立结点.
4. 平行边所对应的列完全相同.



$$M(G) = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{ccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 & -1 & 0 & 0 \end{pmatrix} \end{array}$$

.

6.88

结点的合并

在关联矩阵里, 记 v_i 对应的行为 $\vec{v_i}$, 规定运算:

$$\vec{v_i} \oplus \vec{v_j}$$

其中

1. 对有向图, $\oplus$ 是普通的加法;
2. 对无向图, $\oplus$ 是对应分量的模 2 加法运算.

运算的目的是把 v_i 与 v_j 合并, 而且要达到一个要求: 合并若得到了自回路, 要删去.

6.89

Example 60. 合并图中结点 v_4 与 v_5, 反映在矩阵 $M(G)$ 上 $v_4 \oplus v_5$.

$$M(G) = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{ccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

$$M(G') = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_{4,5} \end{array} \begin{array}{c} \begin{array}{ccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

6.90

两个关于关联矩阵的秩的结论:

Theorem 61. 设连通图 G 有 r 个结点, 则其完全关联矩阵的秩为 $r-1$. 即

$$\operatorname{rank} M(G) = r - 1$$

(证明略)

推论

设图 G 有 r 个结点, w 个最大连通子图, 则图 G 的完全关联矩阵的秩为 $r-w$.

6.91

小结

图的矩阵表示所用到的几种不同的矩阵

1. 邻接矩阵: 点与点之间的邻接关系.

   A^l 的作用?

2. 可达性矩阵 (和连通矩阵): 路的存在性.

   可达性矩阵的三种求法?

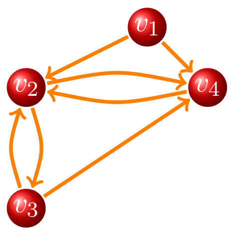
3. 完全关联矩阵: 结点与边的关系.

   运算 $\vec{v_i} \oplus \vec{v_j}$ 的作用?

6.92

练习

求如下有向图的邻接矩阵 A, 指出从 v_1 到 v_4 且长度为 2 和 4 的路. 并计算 A^2, A^4 来验证.



解: 从 v_1 到 v_4 长度为 2 的路有 1 条: $v_1v_2v_4$.

从 v_1 到 v_4 长度为 4 的路有 3 条: $v_1v_2v_4v_2v_4$, $v_1v_2v_3v_2v_4$, $v_1v_4v_2v_3v_4$.

$$A = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}, A^2 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix},$$

$$A^3 = \begin{pmatrix} 0 & 2 & 1 & 2 \\ 0 & 1 & 2 & 2 \\ 0 & 2 & 1 & 2 \\ 0 & 2 & 0 & 1 \end{pmatrix}, A^4 = \begin{pmatrix} 0 & 3 & 2 & 3 \\ 0 & 4 & 1 & 3 \\ 0 & 3 & 2 & 3 \\ 0 & 1 & 2 & 2 \end{pmatrix}.$$

6.93

4 欧拉图与汉密尔顿图

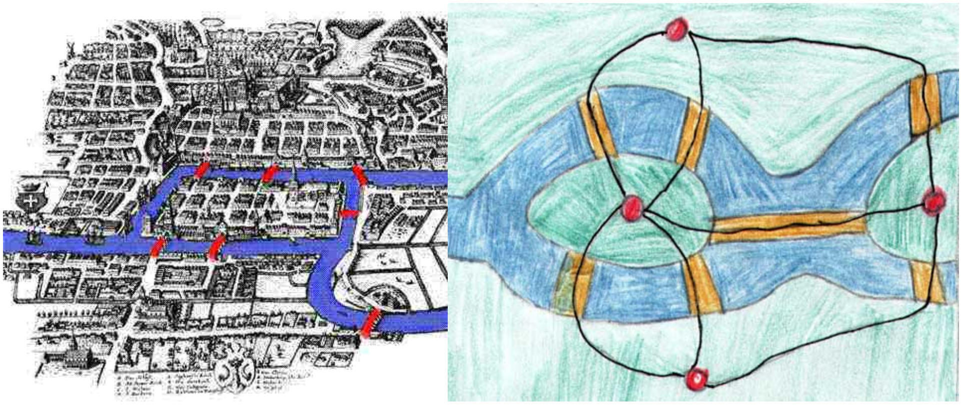
欧拉图与汉密尔顿图

本节主要内容:

1. 欧拉图
2. 有向图中的欧拉路
3. 周游世界问题
4. 汉密尔顿图
5. 标识法

6.94

欧拉图



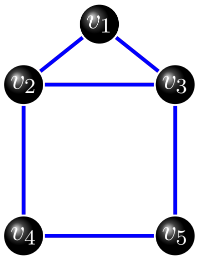
Definition 62. 设图 G 无孤立结点.

- 若存在一条路, 经过图中每边一次且仅一次, 称该路为欧拉路.
- 若存在一条回路, 经过图中每边一次且仅一次, 则称该回路为欧拉回路.

具有欧拉回路的图叫欧拉图.

6.95

Example 63. 例如, 下图具有欧拉路, 而没有欧拉回路.



从图中 v_2 出发, 经过图中每边一次且仅一次到 v_3, 可得欧拉路:

$$v_2 v_1 v_3 v_5 v_4 v_2 v_3.$$

但此图不可能有欧拉回路, 因而不是欧拉图.

6.96

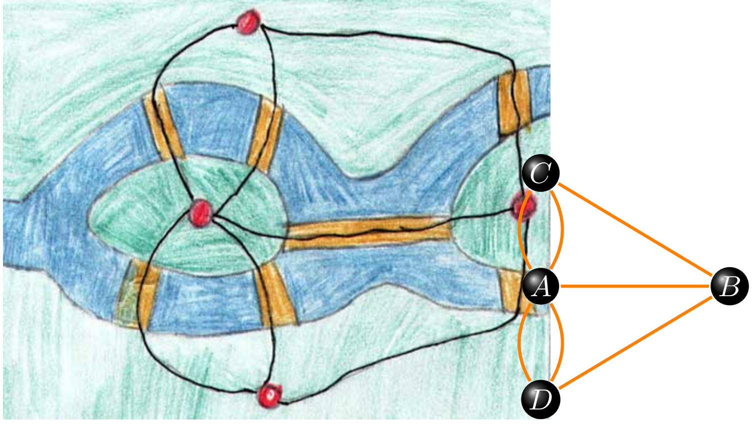
Theorem 64. *无向图 G 有一条欧拉路, 当且仅当 G 连通, 且有零个或两个奇数度结点.*

证: 必要性. 设图 G 有欧拉路

$$v_0 e_1 v_1 e_2 v_2 \cdots e_i v_i e_{i+1} \cdots e_k v_k,$$

其中结点可重复出现, 但边不重复, 且每条边都经历一次, 因此, 欧拉路遍历 G 中所有结点, 所以 G 是连通的.

- 若 v_i 不是端点, 则 $\deg(v_i)$ 必为偶数; (因 v_i 在欧拉路中每出现一次必关联两条边.)
- 而对端点 v_0 和 v_k,
  - 如果 $v_0 = v_k$, 则 $\deg(v_0)$ 为偶数, 即 G 中无奇数度结点;



– 如果 $v_0 \neq v_k$, 则 $\deg(v_0)$ 和 $\deg(v_k)$ 必为奇数, 故 G 中有两个奇数度结点.

证: 充分性. 当 G 连通, 且有零个或两个奇数度结点. 可按如下方法构造一条欧拉路.

(1) 若 G 有两个奇数度结点 v_0 和 v_k, 因 G 连通, 可构造一条迹 (无重复边的路) L_1: $v_0e_1v_1e_2\cdots v_k$; 若 G 无奇数度结点, 则可从任何结点 v_i 出发构造一条闭迹 L_1: $v_ie_1v_1e_2\cdots v_i$.

(2) 如果 L_1 遍历 G 的所有边, 则 L_1 就是一条欧拉路.

(3) 如果 L_1 未遍历 G 的所有边, 则删除 L_1 后得子图 G', G' 中每个结点的度数 为偶数. 因 G 连通, 所以 L_1 与 G' 至少有一个结点 v_j 重合, 在 G' 中从结点 v_j 出发可构造闭迹 L_2.

(4) 如果 L_1 和 L_2 组合在一起恰为 G, 则得一条欧拉路, 否则重复第 3 步, 如此下去, 必可得到一条经过图 G 所有边的欧拉路. □ 6.97

推论

无向图 G 具有一条欧拉回路, 当且仅当 G 连通, 且所有结点度数皆为偶数.

由推论可知, 七桥问题无解:

$$\deg(A) = 5, \quad \deg(B) = \deg(C) = \deg(D) = 3.$$

故欧拉回路必不存在. □ 6.98

一笔画问题

Example 65. "一笔画问题" 即欧拉路的存在性问题. 例如下图中

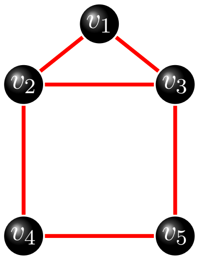
$$\deg(v_2) = \deg(v_3) = 3,$$

$$\deg(v_1) = \deg(v_4) = \deg(v_5) = 2.$$

故必有从 v_2 到 v_3 的一笔画. (或 v_3 到 v_2) 6.99

欧拉路可推广到有向图.

Definition 66. 经过有向图中每边一次且仅一次的单向路 (回路), 称为单向欧拉路 (回路).



Theorem 67. 有向图 G 具有一条单向欧拉回路，当且仅当 G 连通，且每个结点的入度等于出度. 有向图 G 具有一条单向欧拉路，当且仅当 G 连通，且除两个结点之外，每个结点的入度等于出度. 而这两个结点，一个结点的入度比出度大 1，另一个结点的入度比出度小 1.

(证明与前述定理类似.) 6.100

William Rowan Hamilton[3]

哈密顿 (William Rowan Hamilton, 1805 — 1865), 爱尔兰数学家、物理学家.

- 1823 年到爱尔兰的三一学院学习.
- 1827 年获爱尔兰皇家天文学家的称号.
- 1835 年获封为爵士. 6.101
- 1837 年当选爱尔兰皇家科学院院长.

哈密顿在数学上的最主要贡献是发现了“四元数”(quaternions), 建立了向量代数和向量分析的基础.

William Rowan Hamilton[4]

On October 6, 1843, while out walking in Dublin, Hamilton formed a new set of numbers called the quaternions in which there are four key ingredient numbers, namely 1, i, j, and k, satisfying the following multipicative rules:

$$i^2 = j^2 = k^2 = -1,$$
$$ij = k, \quad jk = i, \quad ki = j,$$
$$ji = -k, \quad kj = -i, \quad ik = -j.$$

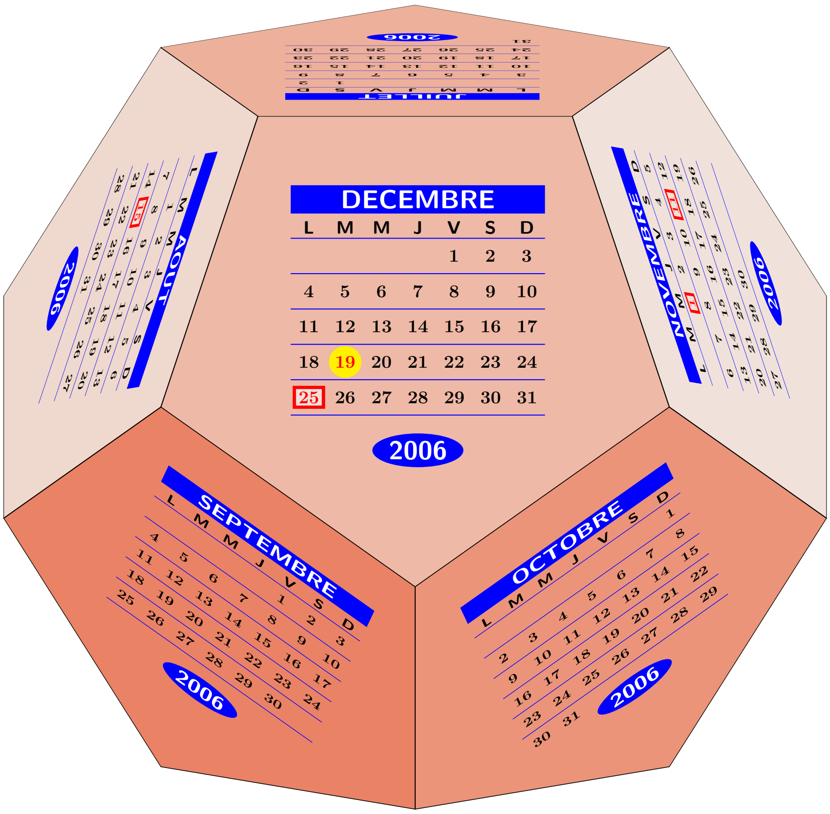
Hamilton was so pleased with his discovery that he stopped on his walk to carve these equations with a knife into the sandstone of Brougham Bridge (see Irish stamp above).

6.102

周游世界问题

[3]Available at www.hkame.org.hk/bookmark2005

[4]Available at http://www.maths.otago.ac.nz/



十二面体的 20 个顶点用不同的城市作标记. 智力题的目标是在一个城市开始, 延十二面体的边旅行, 访问其他 19 个城市每个恰好一次, 回到第一个城市结束.

(旅行经过的回路可以用钉子和细线来标记.) 6.103

正十二面体 6.104

一个展开了的正十二面体 6.105

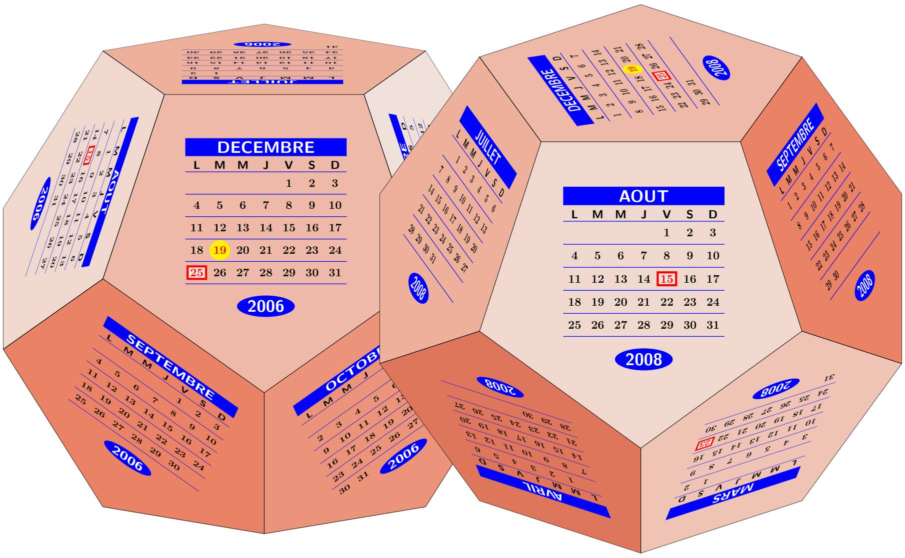
汉密尔顿图

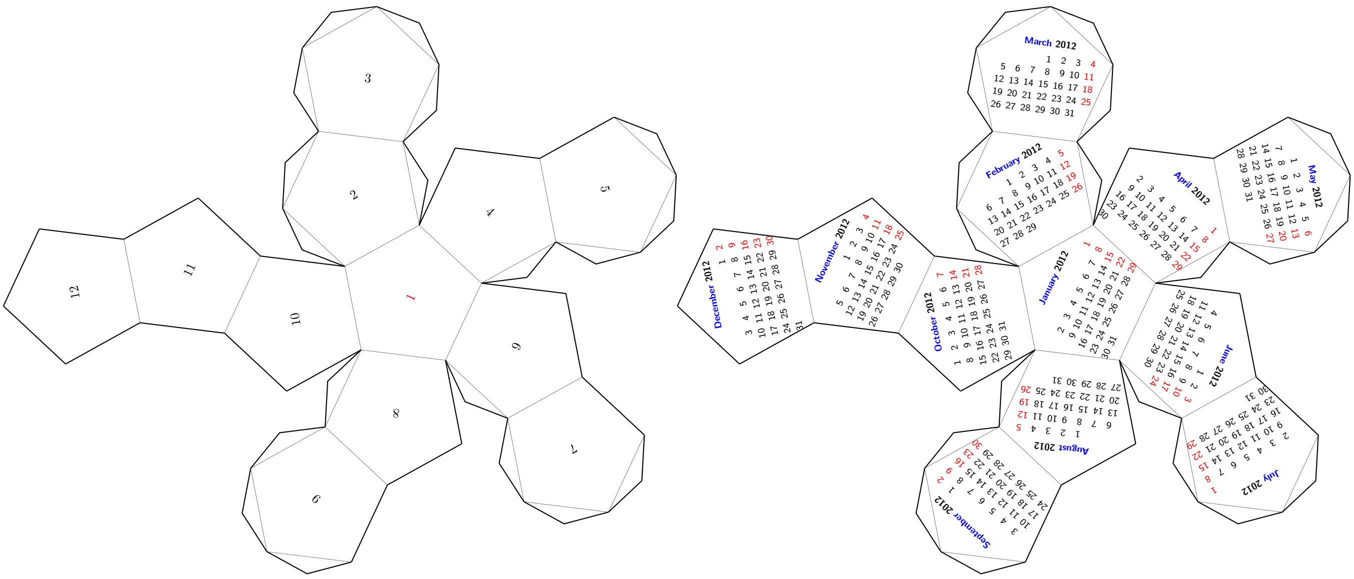
Definition 68. 给定图 G,

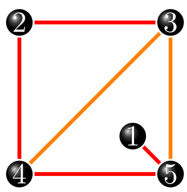
- 经过图中每个结点一次且仅一次的路, 称为汉密尔顿路.
- 经过图中每个结点一次且仅一次的回路, 称为汉密尔顿回路.
- 具有汉密尔顿回路的图, 叫汉密尔顿图. 6.106

Example 69. 例如, 判断下面各图是否为汉密尔顿图.

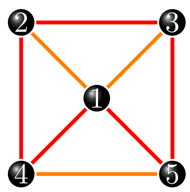
- 图 (a) 中有汉密尔顿路, 但不存在汉密尔顿回路, 所以它不是汉密尔顿图;
- 图 (b) 中有汉密尔顿回路, 它是汉密尔顿图;
- 图 (c) 中既无汉密尔顿回路, 也不存在汉密尔顿路. 6.107


DECEMBRE
L M M J V S D
2006
AOUT
L M M J V S D
2008
SEPTEMBRE
JUILLET
AVRIL
MARS

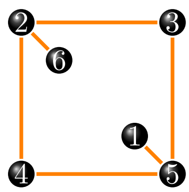

1
2
3
4
5
6
7
8
9
10
11
12
January 2012
February 2012
March 2012
April 2012
May 2012
June 2012
July 2012
August 2012
September 2012
October 2012
November 2012
December 2012



(a)



(b)



(c)

Theorem 70. 若无向图 $G=\langle V,E\rangle$ 是汉密尔顿图, 任意 $S\subseteq V$, 则
$$W(G-S)\leqslant |S|,$$
其中 $W(G-S)$ 表示 G 中删除 S 后所得子图 $G-S$ 的连通分支数.

证: 设 C 是 G 中的一条汉密尔顿回路.

1. 如果 S 中的结点在 C 上两两相邻, 则 $W(C-S)=1\leqslant|S|$.
2. 如果 S 中的结点在 C 上存在 r ($2\leqslant r\leqslant|S|$) 个互不相邻的部分, 则 $W(C-S)=r\leqslant|S|$.

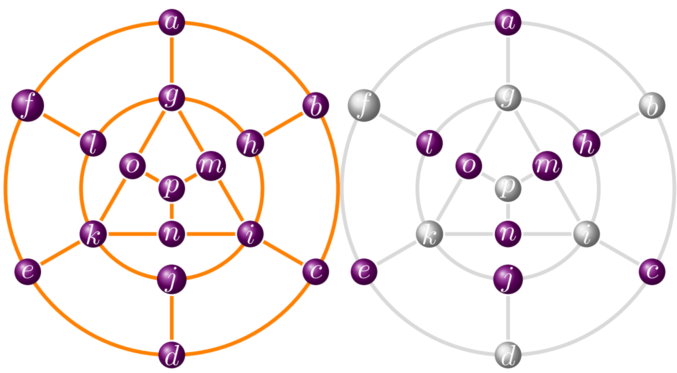
一般说来, S 中的结点在 C 上既有相邻的, 又有不相邻的, 所以总有 $W(C-S)\leqslant|S|$.

注意到 $C-S$ 是 $G-S$ 的生成子图, 故
$$W(G-S)\leqslant W(C-S)\leqslant|S|.$$
□

定理只是汉密尔顿图的必要条件.

如果图 G 不满足这个条件, 则 G 肯定不是汉密尔顿图.

☞ 定理的用途: 判断一个图不是汉密尔顿图. 6.108



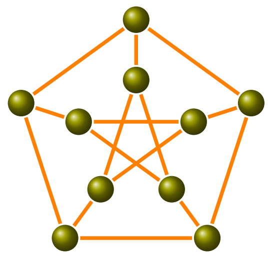
Example 71.

因为
$$W\big(G-\{a,b,c,d,e,f,g\}\big)=9$$
$$\nleqslant\big|\{a,b,c,d,e,f,g\}\big|=7.$$
所以图 G 不是汉密尔顿图. □ 6.109

即使图 G 满足定理的条件, 也不能肯定 G 是汉密尔顿图.

如彼得森图, 它满足定理的条件, 但它不是汉密尔顿图.

1. 删除 1 个或 2 个结点仍是连通图.
2. 删除 3 个结点, 最多得 2 个连通分支的子图.
3. 删除 4 个结点, 最多得 3 个连通分支的子图.
4. 删除 5 个或 5 个结点, 则所得子图的结点数已不大于 5, 从而排除了出现 5 个以上连通分支的可能性.



所以该图满足 $W(G-S) \leqslant |S|$, 但可以证明它是非汉密尔顿图.

到目前为止, 判断一个图是否为汉密尔顿图还只能依据定义. 只有部分满足特定条件的图才能用判别法 (充分条件). 6.110

Theorem 72. 设 G 是具有 n 个结点的简单图, 如果图中每对结点度数之和大于或等于 $n-1$, 则 G 中存在一条汉密尔顿路.

证: ① **先证 G 连通, 用反证法.**

假设 G 不连通, 则至少有两个连通分支 G_1 和 G_2. 又设 G_1 有 n_1 个结点, G_2 有 n_2 个结点. 任取 $v_1 \in G_1$, $v_2 \in G_2$, 则

$$\deg(v_1) \leqslant n_1 - 1, \qquad \deg(v_2) \leqslant n_2 - 1$$

(因图 G 是简单图). 从而有

$$\deg(v_1) + \deg(v_2) \leqslant n_1 + n_2 - 2 < n - 1$$

与题设矛盾.

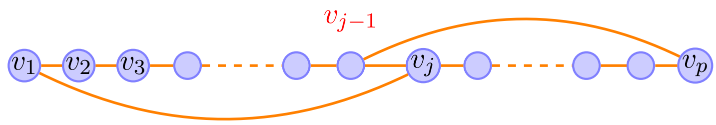
② **在 G 中构造一条汉密尔顿回路.**

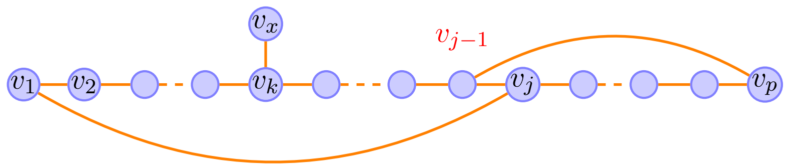
设 G 中有 $p-1$ 条边的路 $v_1v_2\cdots v_p$ $(p<n)$, 且路中各结点均不同. 6.111

证明 (续):

设 G 中有 $p-1$ 条边的路 $v_1v_2\cdots v_p$, 且路中各结点均不同.

- 若 v_1 或 v_p 有邻接于不在该路上的结点, 则可将该路扩展为包含该邻接结点的有 p 条边的路.
- 反之, 若 v_1 或 v_p 与该路外的结点都不邻接, 则存在包含结点序列 $v_1v_2\cdots v_p$ 的回路. 事实上
  1. 若 v_1 邻接 v_p, 则 $v_1v_2\cdots v_pv_1$ 即是所求的回路;
  2. 若 v_1 与 v_p 不邻接, 假设 v_1 与路内的 k 个结点 $v_s, v_m, \cdots, v_j, \cdots, v_t$ 相邻接, $2 \leqslant s, m, \cdots, j, \cdots, t \leqslant p-1$.
     - 如果 v_p 与 $v_{s-1}, v_{m-1}, \cdots, v_{j-1}, \cdots, v_{t-1}$ 中之一邻接, 比如说 v_{j-1}, 则 $v_1v_2\cdots v_{j-1}v_pv_{p-1}\cdots v_jv_1$ 即是所求的回路 (如图); 6.112





证明 (续):

- 如果 v_p 与 $v_{s-1}, v_{m-1}, \cdots, v_{j-1}, \cdots, v_{t-1}$ (共 k 个) 都不邻接, 则 v_p 至多邻接于 $p-k-1$ 个结点 (路 $v_1v_2\cdots v_p$ 内除 v_p 外共 $p-1$ 个结点). 从而

$$\deg(v_p) \leqslant p-k-1$$

又 $\deg(v_1)=k$, 故 $\deg(v_p)+\deg(v_1) \leqslant p-1 < n-1$. 这与题设矛盾.

以上已经证明, 存在包含所有结点 $v_1, v_2 \cdots, v_p$ 的回路. 6.113

证明 (续):

因 G 连通, 故 G 中必有不属于该回路的结点 v_x, 它与 $v_1, v_2, \cdots, v_p$ 中的某结点 v_k 邻接, 这样就得出包含 p 条边的路:

$$v_xv_k\cdots v_{j-1}v_p\cdots v_jv_1v_2\cdots v_{k-1}$$

对得到的 p 条边的路重复前述方法, 可得 $p+1$ 条边的路.

如此继续, 可得有 $n-1$ 条边的路, 它是汉密顿路. □ 6.114

Theorem 73 (Ore 定理)**.** *设 G 是具有 n 个结点的无向简单图, $n \geqslant 3$. 如果 G 中任一对结点度数之和都大于等于 n, 则在 G 中存在一条汉密尔顿回路. (即 G 是汉密尔顿图.)*

证: 由前述的定理知, 在 G 中存在一条汉密尔顿路, 设为 $v_1v_2\cdots v_n$.

1. 若 v_1 与 v_n 邻接, 则得到一条汉密尔顿回路. 定理得证.
2. 若 v_1 与 v_n 不邻接, 假设 v_1 邻接于 $v_{i_1}, v_{i_2}, \cdots, v_{i_k}$, $(2 \leqslant i_j \leqslant n-1)$. 可以证明 " v_n 邻接于 $v_{i_1-1}, v_{i_2-1}, \cdots, v_{i_k-1}$ 中之一".

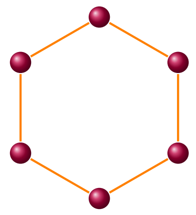
   如果 v_n 不邻接于 $v_{i_1-1}, v_{i_2-1}, \cdots, v_{i_k-1}$ 中任一结点, 则 v_n 至多邻接于 $n-k-1$ 个结点. 从而

$$\deg(v_n) \leqslant n-k-1$$

   又 $\deg(v_1)=k$, 故 $\deg(v_n)+\deg(v_1) \leqslant n-k-1+k = n-1$. 这与题设矛盾. 所以必有汉密尔顿回路 $v_1v_2\cdots v_{j-1}v_nv_{n-1}\cdots v_jv_1$. □

注意:

本定理只不过是充分条件, 而非必要条件. 不满足定理中条件的图, 也可能是汉密尔顿图.

Example 74.  例如, 左图是具有 6 个结点的无向简单图, 它显然是汉密尔顿图, 但该图中任一对结点度数之和等于 4, 并不大于等于图中结点总数 6.

6.115

标识法

判断图 G 中是否存在汉密尔顿路或汉密尔顿回路, 除按定义来判断之外, 没有一个充分必要条件可以作为判断方法.

下面的标识法是一个可作参照的方法. (但这不是一个 "充要条件".)

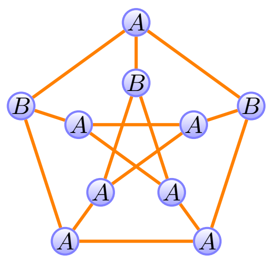
标识法的步骤如下:

1. 先用字母 A 标识图中任一结点, 接着用 B 标识图中与 A 邻接的结点. 然后再用字母 A 标识图中与 B 邻接的结点, 如此下去, 直到图中所有结点标识完毕.
2. 在标识过程中, 遇到相邻结点出现相同标记时, 可在此边上增加一个结点, 并标上相异标识.
3. 标识完毕后, 如果若 A, B 数目差一个以上, 则该图不存在汉密尔顿回路.

6.116

标识法

用标识法说明彼得森图不是汉密尔顿图.



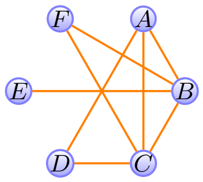
- 先用字母 A 标识图中任一结点;
- 接着用 B 标识图中与 A 邻接的结点;
- 然后再用字母 A 标识图中与 B 邻接的结点.

A, B 数目差一个以上, 所以彼得森图不存在汉密尔顿回路. □

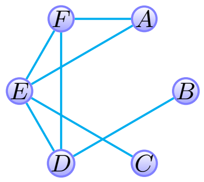
6.117

Example 75. 本学期某个班的学生共计选修了 A, B, C, D, E, F 六门课. 其中一部分人同时选修 A, C, D, 一部分选修 B, C, F, 一部分选修 B, E, 还有一部分选修 A, B. 期末考试要求每天考一门课, 六天内考完. 为了减轻学生负担, 要求每个人都不会连续参加考试. 试设计一个考试日程表.

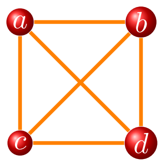
解: 以每门课为一个结点, 共同选修的课程之间用边相连, 得到图 (a). 由题意, 相邻结点对应的课程不能连续考试, 而不相邻的结点所对应的课程允许连续考试. 因此作图 (a) 的补图 (b).



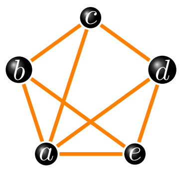
(a)



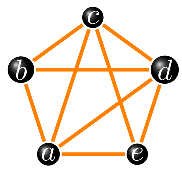
(b)



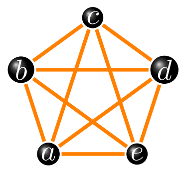
(a) G_1



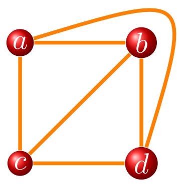
(b) G_2



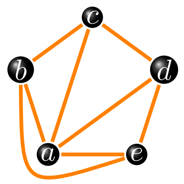
(c) G_3



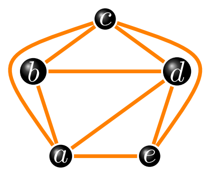
(d) G_4



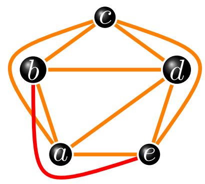
(a) G_1'



(b) G_2'



(c) G_3'



(d) G_4'

问题归结为在图 (b) 中找一条哈密尔顿路. 如依次按顺序 C, E, A, F, D, B 进行考试, 就是一个符合要求的考试安排. □ 6.118

5 平面图

平面图

本节主要内容:

1. 平面图的概念
2. 欧拉公式
3. 库拉托夫斯基定理 6.119

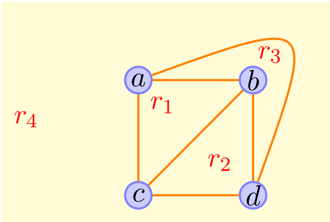
平面图的概念

Definition 76. 能画在一个平面上且任何两边除端点外互不相交的图, 称为平面图.

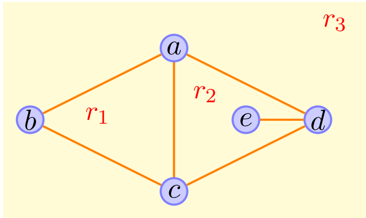
☞ 这里说的是 “能画在”, 有些图形从表面看有几条边是相交的, 但是不能就此肯定它不是平面图. 6.120

Example 77. 判断下面各图是否为平面图.

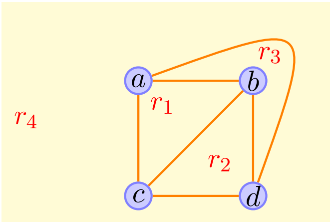
G_1, G_2, G_3 是平面图, G_4 不是平面图. 6.121



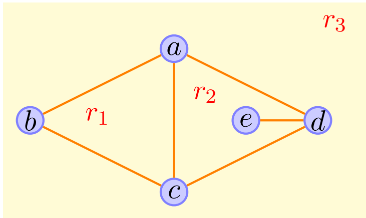
(a)



(b)



(a)



(b)

将平面图 G 的每个边不交叉的图画在一个平面上, 称为图 G 的一个平面表示.

Definition 78. 平面图 G 的某个平面表示, 将 G 所在的平面划分成若干区域, 每个区域叫图 G 的一个面; 包围每个面的边, 称为该面的边界; 边界上边的条数, 叫该面的次数, 面 r 的次数记作 $\deg(r)$.

Example 79. 图 (a) 有 4 个面; 图 (b) 有 3 个面. 图 (b) 中: $\deg(r_1) = 3, \quad \deg(r_2) = 5, \quad \deg(r_3) = 4.$

6.122

Theorem 80. *一个有限平面图, 面的次数之和等于其边数的两倍.*

证: 因一条边或是两个面的公共边, 或在一个面中作为该面的边界被计算过两次, 所以各面次数之和等于边数的两倍. □

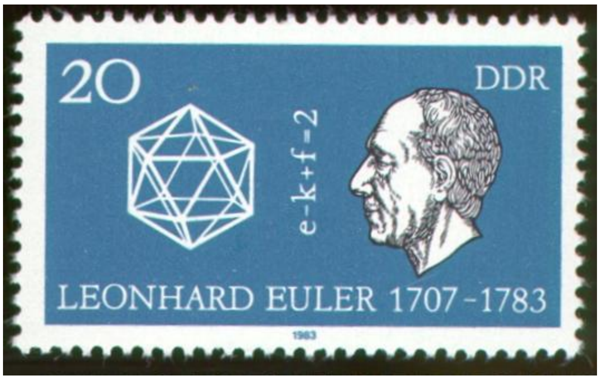
Example 81.

- 图 (a) 有 6 条边; 4 个面, 每面次数皆为 3.
- 图 (b) 中 $\deg(r_1) = 3, \quad \deg(r_2) = 5, \quad \deg(r_3) = 4.$
  图 (b) 有 6 条边; 有 3 个面, 各面次数之和为 12.

6.123

Theorem 82 (欧拉公式)**.** *设 G 是连通平面图, 有 v 个结点, e 条边, r 个面, 则*

$$v - e + r = 2.$$



证: 对边数用归纳法证明.

- 若 G 为平凡图 (孤立结点), 则 $v=1$, $e=0$, $r=1$ 公式成立.
- 若 G 仅有一条边, 则 $v=2$, $e=1$, $r=1$ 公式成立; 或 $v=1$, $e=1$, $r=2$ 公式仍然成立.
- 设 G 有 k 条边时, 欧拉公式成立. 当 G 有 $k+1$ 条边时, 设其结点数为 v, 面数为 r, 可分两种情况讨论:
  - 如 G 中有度数为 1 的结点, 删除该结点及其关联的一条边得图 G'. 显然, G' 也是连通平面图, 设 G' 的结点数, 边数和面数依次为 v', $e'=k$, r', 按归纳假设应满足欧拉公式, 即 $v'-e'+r'=2$, 亦即 $(v-1)-(e-1)+r=2$, 从而有 $v-e+r=2$.
  - 如 G 中没有度数为 1 的结点, 则在有限面的边界中删除一条边得图 G'. G' 也是连通平面图且边数等于 k, 按归纳假设应满足欧拉公式, 即 $v'-e'+r'=2$, 亦即 $v-(e-1)+(r-1)=2$, 从而有 $v-e+r=2$.

  综上所述, 当边数为 $k+1$ 时公式成立. 定理得证. □

6.124

Theorem 83. 设 G 是有 v 个结点, e 条边的连通简单平面图, 且 $v\geqslant 3$, 则

$$e\leqslant 3v-6.$$

证: 设 G 的面数为 r, 当 $v=3$, $e=2$ 时, 公式成立.

当 $e\geqslant 3$ 时, 因 G 为简单图, 每面的次数不小于 3(否则意味着有平行边或环, 就不是简单图了).

又由各面次数之和为 $2e$, 因此

$$2e\geqslant 3r,$$

再由欧拉公式 $v-e+r=2$, 有 $r=2+e-v$, 带入上式得:

$$2e\geqslant 3(2+e-v),$$

即

$$e\leqslant 3v-6.$$ □

6.125

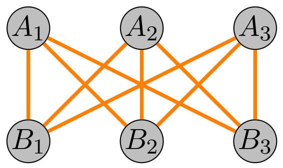
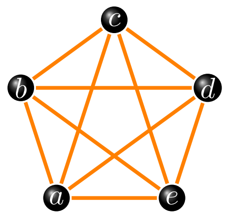


Figure 11: $K_{3,3}$

☞ 定理给出了结点数大于等于 3的连通简单平面图应满足的必要条件, 可用来判断某些图不是平面图.

Example 84. 例如, 应用定理可知 K_5 不是平面图.



因 K_5 是连通简单图,

$$v = 5, \quad 3v - 6 = 9, \quad \text{而 } e = 10,$$

不满足定理给出的条件 $e \leqslant 3v - 6$. □ 6.126

推论

设 G 是 v 个结点, e 条边的连通平面图, 且 G 的各面的次数大于等于 4, 则 $e \leqslant 2v - 4$.

证: 由所设, G 的各面次数之和大于等于 $4r$, 这里 r 为 G 的面数. 所以

$$2e \geqslant 4r, \qquad \text{即 } e \geqslant 2r.$$

再由欧拉公式 $v - e + r = 2$, 有 $r = 2 + e - v$, 带入上式得:

$$e \geqslant 2(2 + e - v),$$

得

$$e \leqslant 2v - 4. \qquad \square$$

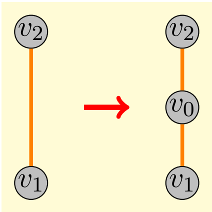
☞ 推论给出了各面次数大于等于 4 的连通平面图应满足的必要条件, 所以可用来判断某些图不是平面图. 6.127

Example 85. 例如, 应用推论可知 $K_{3,3}$ 不是平面图.

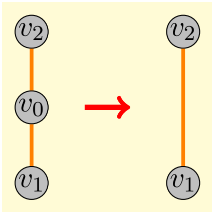
如果 $K_{3,3}$ 是连通平面图, 由每个面的次数都不小于 4 (因为在 $K_{3,3}$ 中任取三个结点, 其中必有两个结点不相邻). 又

$$v = 6, \quad 2v - 4 = 8, \quad \text{且 } e = 9,$$

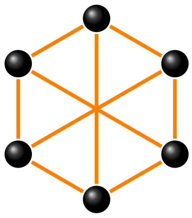
不满足推论给出的条件 $e \leqslant 2v - 4$. □ 6.128



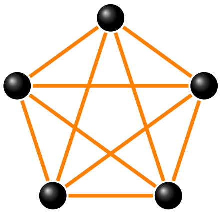
(a) 插入结点



(b) 删除结点



(a) $K_{3,3}$



(b) K_5

Kuratowski 定理

欧拉公式可用来判断某些图不是平面图. 但不能用来判断某图是平面图.

Kuratowski [5]2> 库拉托夫斯基 (Kazimierz Kuratowski, 1896 – 1980) 波兰人, 华沙大学教授. 给出了一个判断平面图的充分必要条件. 为此, 先介绍 "在二度结点内同构" 的定义. 6.129

Kuratowski 定理

Definition 86. 给定图 G_1, G_2, 如果它们同构, 或通过反复插入或删除度数为 2 的结点之后它们同构, 则称 G_1 与 G_2 在二度结点内同构.

插入或删除 2 度结点示意图:

6.130

Kuratowski 定理

Theorem 87. *一个图是平面图, 当且仅当它不包含与 $K_{3,3}$ 或 K_5 在二度结点内同构的子图.*

($K_{3,3}$ 和 K_5 常称为库拉托夫斯基图.)

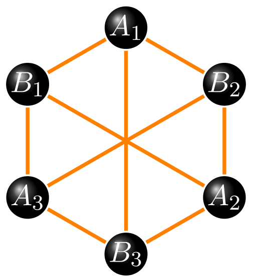
(证明略.) 6.131

Kuratowski 定理

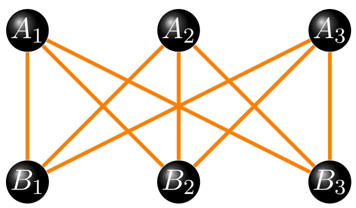
注意 $K_{3,3}$ 的不同表示, 下面两个图都是 $K_{3,3}$:

6.132

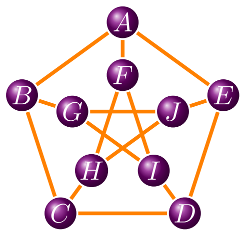
[5]<



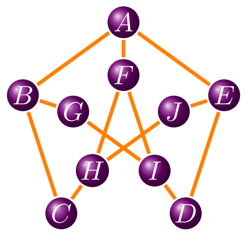
(a) $K_{3,3}$



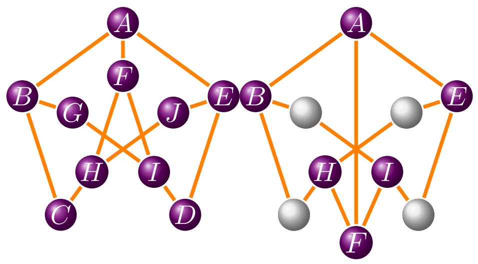
(b) $K_{3,3}$



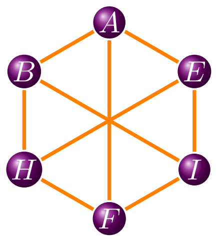
(a) Petersen 图



(b) 取 Petersen 图子图



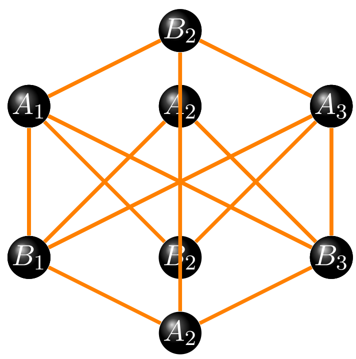
(c) 子图的变形



(d) 删 除 二 度 结 点 C, D, G, J 得 $K_{3,3}$

Kuratowski 定理

注意 $K_{3,3}$ 的不同表示, 下面两个图都是 $K_{3,3}$:



6.133

证明 Petersen 图不是平面图.

6.134

练习

假定连通平面性简单图有 20 个结点, 每个结点的度数都是 3. 这个平面图有多少个区域?

解: 由题知, $v = 20$. 则所有结点的度数之和为 $20 \times 3 = 60$. 而

$$\sum_{v \in V} \deg(v) = 2e,$$

所以 $e = 30$. 由欧拉公式得

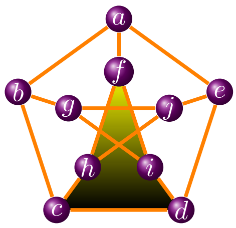
$$\begin{aligned} r &= e - v + 2 \\ &= 30 - 20 + 2 \\ &= 12. \end{aligned}$$

□

6.135

练习

应用欧拉公式证明 Petersen 图不是平面图.



证: Petersen 图中, $v = 10$, $e = 15$, 从图上可以看出, 每个面由 5 条边围成. 根据定理 7-5.1, 如果 Petersen 图是平面图, 则 $2e = 5r$. 所以

$$r = \frac{2}{5}e = 6$$

$$\Rightarrow v - e + r = 10 - 15 + 6 = 1 \neq 2$$

这说明 Petersen 图不满足欧拉公式, 故它不是平面图. □

6.136

6 对偶图与着色

对偶图与着色

本节主要内容:

1. 着色问题
2. 对偶图的概念
3. 正常着色
4. Welch Powell 着色法
5. 四色定理 (The Four-Color Theorem)

6.137

Four Color Conjecture [6]

The concept of the Four Coloring Theorem was born in 1852 when Francis Guthrie noticed that he only needed four different colors to color in a map of England.

Through his brother, Frederick, Francis communicated his discovery to De Morgan. Francis wondered if De Morgan would be able to tell him if it was true or not. De Morgan was unsure, so he asked the same question to Hamilton 6.138
in Dublin. Hamilton was unable to help, so De Morgan continued to ask other prominent mathematicians.

Four Color Conjecture

In the US, Charles Peirce attempted to prove the Four Color Conjecture in the 1860's and continued to for the remainder of his life.

In 1879, Cayley wrote a paper to the Royal Geographical Society explaining the difficulties in attempting to prove the Conjecture.

On July 17, 1879, a mathematician by the name of Kempe announced a proof for the Four Color Conjecture. However, eleven years later Heawood, a lecturer at Durham England, pointed out that Kempe's proof was incorrect. Along with proving Kempe wrong, Heawood was able to prove that every planar map is five colorable. In 1898, Heawood also proved that if the number of edges around a region is divisible by three then the region is four colorable. 6.139

Four Color Conjecture

In 1880 a man by the name of Tait came up with his own proof for the Four Color Conjecture. Once again the proof was proved false, this time by Petersen in 1891.

In the midst of these two failed attempts at finding a proof for the Four Color Conjecture, Kempe and Tait both made other major contributions to the world of mathematics. Kempe discovered what would later become known as Kempe chains and Tait devised a equivalent form of the Four Color Theorem for three-edge-coloring.

The next major contribution was the concept of reducibility by Birkoff. Using Birkoff's work, Franklin proved that any map with up to 25 regions can be four colorable in 1922. 6.140

Four Color Conjecture

In 1926 Reynolds increased the number of regions to 27. Winn increased it to 35 in 1940, Ore and Stemple to 39 in 1970, and Mayer to 95 in 1976. Heesch

[6]Available at: `http://www.facstaff.bucknell.edu/udaepp/090/w3/ryanp.htm`

later developed the two main concepts that eventually led to the final proof. They were reducibility and discharging.

Finally, in 1976, Kenneth Appel and Wolfgang Haken at the University of Illinois with the aid of a computer program that was thousands of lines long and took over 1200 hours to run, basing their methods on reducibility using Kempe chains.

The Four Color Theorem was the first major theorem to be proved using a computer. 6.141

对偶图的概念

Definition 88. 给定平面图 $G = \langle V, E\rangle$, 设它有 n 个面 $F_1, F_2, \cdots, F_n$. 若图 $G^\star = \langle V^\star, E^\star\rangle$ 满足下列条件:

1. 对图 G 的任意一个面 F_i, 其内部有且仅有一个结点 $v_i^\star$ 属于 $V^\star$;
2. 对图 G 的任意两个面 F_i, F_j 的公共边界 e_k 有且仅有一条边 $e_k^\star$ 属于 $E^\star$, 使 $e_k^\star = (v_i^\star, v_j^\star)$, 且 $e_k^\star$ 与 e_k 相交;
3. 当且仅当 e_k 只是一个面 F_i 的边界时, $v_i^\star$ 有一个环 $e_k^\star$ 与 e_k 相交.

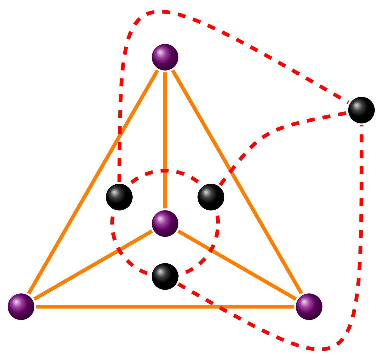
则称图 $G^\star$ 是图 G 的对偶图.

☞ 对偶图显然是相互的. $G^\star$ 是 G 的对偶图, 则 $G^\star$ 也是 G 的对偶图. 特别是连通平面图的对偶图也是平面图. 6.142

Definition 89. 图 G 的对偶图 $G^\star$ 同构于 G, 则称图 G 是自对偶图.

Example 90. 自对偶图的例子:

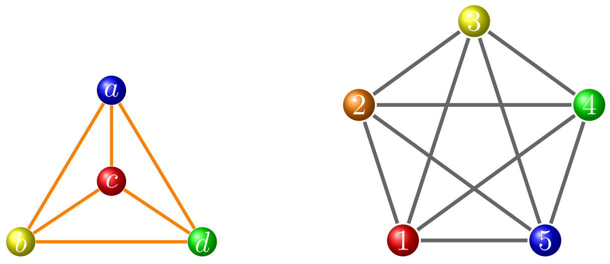
- “面” 演化为 “点”;
- “面的公共边界” 演化为 “点的邻接边”.



6.143

正常着色

- 由对偶图的概念, 可以将 “地图的着色” 转化为对 “平面图结点的着色”.
- 因而四色问题归结为: 证明对任何一个平面图, 可用四种颜色对其结点实施着色, 使邻接的结点有不同的颜色.



(a) (b)

着色

图 G 的正常着色 (简称 "着色") 指对 G 的每个结点指定一种颜色, 使邻接的结点具有不同的颜色.

- 如果图 G 着色用了 n 种颜色, 则称图 G 是 n-色的.
- 图 G 着色所需的最少颜色数称为 G 的着色数, 记作 $\chi(G)$.

6.144

正常着色

Example 91. 下图中,

- 图 (a) 着色所需的最少颜色数为 4, 因此它是 4-色的.
- 图 (b) 着色所需的最少颜色数为 5, 因此它是 5-色的.

6.145

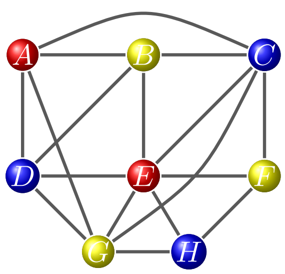
Welch Powell 着色法

用 Welch Powell 方法对图 G 实施着色, 可以确定某个图 G 是否是 n-色的. 步骤如下:

1. 将图 G 的所有结点按度数递减的次序排列 (度数相同的结点次序随意);
2. 用第一种颜色对度数最大的结点着色, 并按排列次序, 依次对与前面已着色点不相邻的结点着上同样的颜色;
3. 用第二种颜色对未着色结点按步骤 (2) 着色; 用第三种颜色继续如法着色, $\cdots$, 直到所有结点全部着色为止.

6.146

Example 92. 对下图着色.



解: 各结点度数为: E 度数为 6; C, G 度数为 5; A, B, D 度数为 4; F, H 度数为 3. 结点递减排序: E, C, G, A, B, D, F, H.

- 用红色对 E 及不相邻的结点 A 着色;
- 用蓝色对 C 及不相邻的结点 D, H 着色;
- 用黄色对 G 及不相邻的结点 B, F 着色.

6.147

四色定理

Theorem 93. *$\chi(K_n) = n$, K_n 是有 n 个结点的完全图.*

证: 因完全图 K_n 的每个结点与其它的 $n-1$ 个结点都邻接, 所以每个结点必须着不同的颜色, 才能使邻接结点有不同的颜色, 故 K_n 的着色数不少于 n.

又因 n 个结点的着色数至多为 n, 因而 $\chi(K_n) = n$. □

Theorem 94 (四色定理)**.** *任意平面图最多是 4-色的.*

(证明略) 6.148

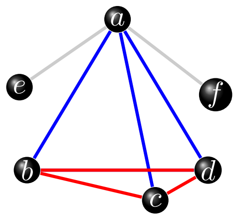
练习

六人在一起, 或者三人互相认识, 或者三人彼此不认识.

解: 将 6 个人分别用平面上 a, b, c, d, e, f 六点表示. 从任一人出发, 该人与其它五人或认识, 或不认识.

如两人认识, 则相应两点用红线相连, 否则, 用蓝线相连.

不失一般性, 考虑从 a 开始, 与其它五点可以有五条线相连. 那么五条线中必有 3 条会着上相同的颜色. [1ex]



假定 ab, ac, ad 为蓝色,

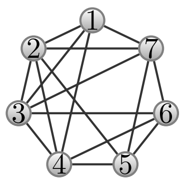
1. 如果此时 bc, cd, bd 中有一条边为蓝色 (比如 bd 边为蓝色), 则可构成一个蓝色三角形, 因而六人中有三人不认识; 6.149
2. 如果此时 bc, cd, bd 全为红色, 则 b, c, d 彼此认识, 因而六人中有三人认识. □

Example 95. 如何安排大学的期末考试, 使得没有学生在同一时间有两门考试?

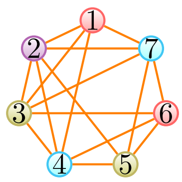
解: 用结点表示课程, 若在两个结点所表示的课程里有公共的学生, 则在这两个结点之间有边. 用不同颜色来表示期末考试的不同时间段. 考试的安排就对应于所关联的图的着色.

例如, 假定要安排七门课的期末考试, 这七门课程的编号为 1 到 7. 不妨设下列成对的课程有公共的学生: 1 和 2, 1 和 3, 1 和 4, 1 和 7, 2 和 3, 2 和 4, 2 和 5, 2 和 7, 3 和 4, 3 和 6, 3 和 7, 4 和 5, 4 和 6, 5 和 6, 5 和 7, 以及 6 和 7.

因为这个图的色数为 4, 所以需要 4 个时间段. □ 6.150



(a)



(b)

Chapter 7

树

Discrete Mathematics

November 29, 2011

黄正华, 数学与统计学院, 武汉大学

7.1

Contents

7.2

1 树与生成树

树与生成树

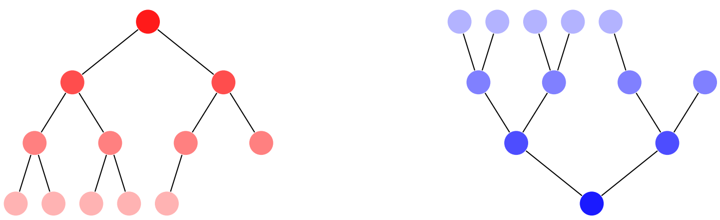
1. 树的定义
2. 生成树
3. 最小生成树
4. Kruskal 算法

树是图论中重要的概念之一, 在计算机科学中有广泛的运用. 7.3

树的定义

Definition 1. 一个连通且无回路的无向图称为树 (tree).

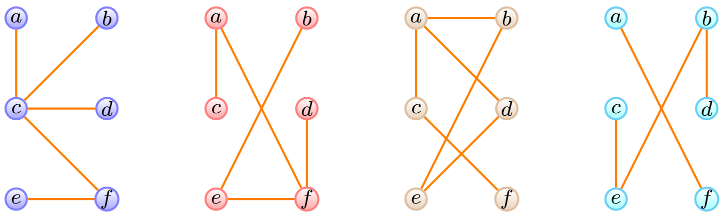
- 树中度数为 1 的结点叫树叶 (leave);
- 度数大于 1 的结点叫分枝点 (branched node) 或内点.
- 如果一个无向图的每个连通分支是树, 则称为森林 (forest).



7.4

树的定义

如图,



(a) G_1　(b) G_2　(c) G_3　(d) G_4

- G_1 和 G_2 是树, 它们都是没有回路的简单图.
- G_3 不是树, 因为结点 a, b, e, d 构成回路.
- G_4 不是树, 因为它不连通. 7.5

Theorem 2. *给定图 T, 下列关于树的定义是等价的:*

1. *无回路的连通图.*
2. *无回路且 $e = v - 1$. (其中 e 为边数, v 为结点数.)*
3. *连通且 $e = v - 1$.*
4. *无回路, 但增加一条边, 得到且仅得到一个回路.*
5. *连通, 但删除一条边则不连通.*
6. *每对结点间有且仅有一条路.* 7.6

给定图 T, 下列关于树的定义是等价的:

1. 无回路的连通图.
2. 无回路且 $e = v - 1$. (其中 e 为边数, v 为结点数.)

证: 由 (1) 证 (2). 归纳法证明.

当 $v = 2$ 时, 因 T 无回路且连通, 则 $e = 1$, 所以 $e = v - 1$ 成立.

设 $v = k - 1$ 时命题成立. 当 $v = k$ 时, 因 T 无回路且连通, 因而至少有一个度数为 1 的结点.

否则, 因各点皆连通且度数大于等于 2. 从某结点 v_i 出发, 可达另一个结点 v_j, 再继续, 可经由一些结点后返回某结点 v_i. 这样就产生了回路. 与假设矛盾. 故至少有一个度数为 1 的结点.

删除该结点及其关联的一条边得 $k - 1$ 个结点的子图 T', 它仍是连通的, 且 $e' = v' - 1$, 即 $e - 1 = (v - 1) - 1$, 整理得 $e = v - 1$. □ 7.7

给定图 T, 下列关于树的定义是等价的:

1. 无回路的连通图.
2. 无回路且 $e = v - 1$. (其中 e 为边数, v 为结点数.)
3. 连通且 $e = v - 1$.
4. 无回路, 但增加一条边, 得到且仅得到一个回路.
5. 连通, 但删除一条边则不连通.
6. 每对结点间有且仅有一条路.

证: 由 (6) 证 (1). 每对结点间有路, 则 T 连通.

因每对结点间仅有一条路, 则 T 无回路. 否则, 回路上的两点之间至少有两条道路, 与所设矛盾.

故 T 是无回路的连通图. □ 7.8

树的概念是亚瑟 · 凯莱 [1] 提出的.

饱和碳氢化合物与树

英国数学家亚瑟 · 凯莱在 1857 年发明了树, 当时他试图列举饱和碳氢化合物 $\mathbf{C}_n\mathbf{H}_{2n+2}$ 的同分异构体.

左图为什么是树?

结点数:

$$v = n + (2n + 2) = 3n + 2$$

结点度数之和:

$$4 \times n + 1 \times (2n + 2) = 6n + 2$$

则边数 $e = 3n + 1$. 因是连通图, 且 $e = v - 1$, 所以是树. 7.9

Theorem 3. *任一棵树中至少有两片树叶.*

证: 设树 $T = \langle V, E\rangle$, $|V| = v$. 因 T 连通, 对任意 $v_i \in V$, 有 $\deg(v_i) \geqslant 1$, 而

$$\sum \deg(v_i) = 2e = 2(v - 1) \tag{1}$$

- 如果 T 的每个结点的度数皆大于 2, 则 $\sum \deg(v_i) \geqslant 2v$, 与 (1) 式矛盾.
- 如果 T 只有一个结点的度数等于 1, 则 $\sum \deg(v_i) \geqslant 2(v - 1) + 1$, 即 $\sum \deg(v_i) \geqslant 2v - 1$, 也与 (1) 式矛盾.

故 T 中至少有两个结点的度数等于 1, 即有两片树叶. □ 7.10

[1] Arthur Cayley (1821–1895) 17 岁进入剑桥三一学院学习, 1849 年获律师资格, 在其律师生涯中写下了超过 300 篇的数学论文. 1863 年返回剑桥任教职.

生成树

Definition 4. 若图 G 的生成子图 T 是树, 则称 T 为 G 的生成树.

- T 中的边叫做树枝 (branch);
- G 中不属于 T 的边叫做弦 (chord);
- 所有弦的集合称为 T 的补.

7.11

Example 5. 如图,

- T_1 是 G 的一棵生成树,
- e_1, e_3, e_5, e_7, e_8 是 T_1 的树枝;
- e_2, e_4, e_6 是 T_1 的弦;
- $\{e_2, e_4, e_6\}$ 是 T_1 的补.
- T_2, T_3 也是 G 的生成树.

7.12

Theorem 6. 连通图至少有一棵生成树.

证: 如果图 G 连通且无回路, 则 G 就是一棵生成树.

如果图 G 连通且有一个回路, 则删去回路上的一条边得图 G_1, 显然 G_1 也是连通的.

- 如果 G_1 无回路, 则 G_1 是生成树.
- 如果 G_1 仍有回路, 则重复上述步骤, 直到无回路为止, 可得一个与 G 有相同结点且无回路的连通图, 它是 G 的一棵生成树. □

7.13

连通图的秩

连通图的秩

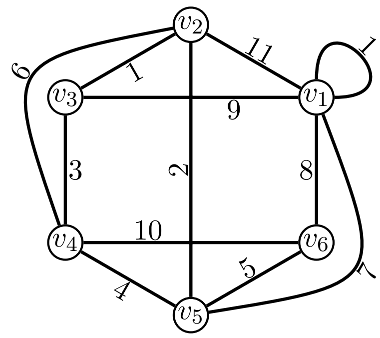
设 $G = \langle V, E \rangle$ 是一个连通图, $|V| = n$, $|E| = m$, 则 G 的生成树有 $n-1$ 条边. 因此, 为得出 G 的一棵生成树应删去 $m-(n-1)$ 条边. 数 $m-(n-1)$ 称为 G 的秩.

简言之: 连通图 G 的秩是指产生 G 的一棵生成树应删去的边数.

7.14

最小生成树问题

设有 6 个村庄 v_i, $i = 1, 2, \cdots, 6$, 欲修建道路使村村可通. 现已有修建方案如下带权无向图所示, 其中边表示道路, 边上的数字表示修建该道路所需费用, 问应选择修建哪些道路可使得任意两个村庄之间是可达的, 且总的修建费用最低?



7.15

最小生成树

Definition 7. 设图 $G = \langle V, E\rangle$, 对应于 G 的每一条边 e, 指定一个正数 $C(e)$, 称为边 e 的权.

- 设 T 是 G 的生成树, T 的各边权数之和
$$\sum C(e_i)$$
称为树 T 的树权, 记作 $C(T)$.
- G 的所有生成树中树权最小者, 叫最小生成树.

最小生成树在许多实际问题中, 如交通运输, 管道铺设等, 有广泛的应用. 7.16

Kruskal 算法 [2]

Theorem 8. *设图 G 有 n 个结点, 以下算法产生一棵最小生成树:*

1. *取最小权边 e_1, 令 $i := 1$;*
2. *若 $i = n - 1$, 则结束. 否则转 ③ ;*
3. *设已选中的边为 $e_1, e_2, \cdots, e_i$. 在 G 中选不同于 $e_1, e_2, \cdots, e_i$ 的边 e_{i+1}, 使 $\{e_1, e_2, \cdots, e_i, e_{i+1}\}$ 中无回路, 且 e_{i+1} 是满足此条件的最小权边;*
4. *$i := i + 1$, 转 ② .*

7.17

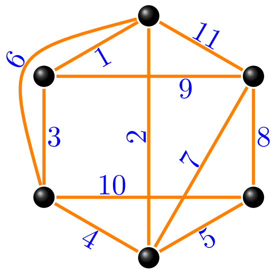
Kruskal 算法

注

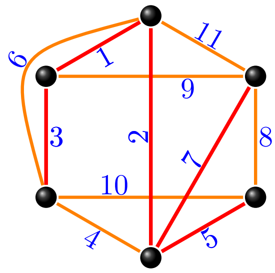
Kruskal 算法实际求解时的两种方式:

1. 逐步选取边权最小的边, 但始终保持已选取的边不构成回路, 直到边数达到 $n - 1$ 条为止.
2. 不断删除边权最大的边而保持图的连通性且无回路. 直到边数剩 $n - 1$ 条时停止.

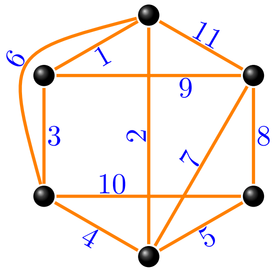
7.18



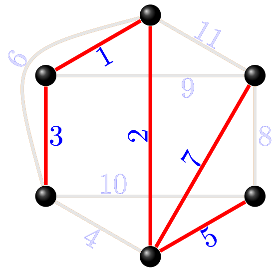
(a)



(b)



(a)



(b)

Example 9 (Kruskal 算法举例). 在下图中求最小生成树 (方法 1).

图中有 6 个结点, 所以要选取 5 条边.

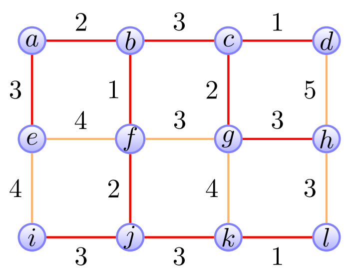
(注意: 边权为 1, 2, 3 的边选取了之后, 边权为 6, 4 的边就不能选了. 否则构成回路.) 7.19

Kruskal 算法举例

Example 10. 在下图中求最小生成树 (方法 2). 7.20

Kruskal 算法举例

Example 11. 用 Kruskal 算法给出最小生成树.



---

[2]Joseph Bernard Kruskal (b. 1929 in New York) is an American mathematician, statistician, and psychometrician.

解: 选择的步骤如下表.

步骤	边	权
1	$\{c,d\}$	1
2	$\{k,l\}$	1
3	$\{b,f\}$	1
4	$\{c,g\}$	2
5	$\{a,b\}$	2
6	$\{f,j\}$	2
7	$\{b,c\}$	3
8	$\{j,k\}$	3
9	$\{g,h\}$	3
10	$\{i,j\}$	3
11	$\{a,e\}$	3
		总计: 24

当然, 最小生成树不是惟一的, 除非图 G 中所有边的权值都不相同. 7.21

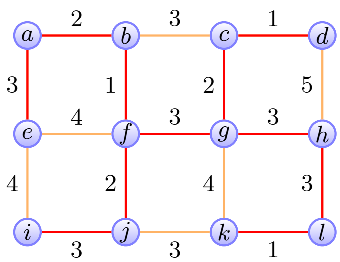
Prim 算法

另一种寻找最小生成树的算法叫做 Prim 算法, 该算法由一个权最小的边开始, 在所有相邻接的边中选择一个权值最小的边, 且不形成回路, 直到形成一个最小生成树.

注意 Prim 算法和 Kruskal 算法的区别. Prim 算法是在与已经选择的树相邻接的边中, 寻找最小权的边, 并且不构成回路. Kruskal 算法不要求下一个找到的边和已经找到的边相邻接, 只要求权最小而且不构成回路. 7.22

Prim 算法举例

Example 12. 用 Prim 算法给出其最小生成树.



解: 选择的步骤如下表.

步骤	边	权
1	$\{b, f\}$	1
2	$\{a, b\}$	2
3	$\{f, j\}$	2
4	$\{a, e\}$	3
5	$\{i, j\}$	3
6	$\{f, g\}$	3
7	$\{c, g\}$	2
8	$\{c, d\}$	1
9	$\{g, h\}$	3
10	$\{h, l\}$	3
11	$\{k, l\}$	1
		总计: 24

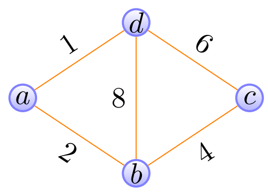
同样, 此问题答案不是惟一的. 7.23

Prim 算法和 Kruskal 算法

Prim 算法和 Kruskal 算法都是一种贪婪算法.

所谓贪婪算法 (greedy algorithm), 是指一类采用 "局部最优" 方式的说法, 它在每次循环时都只考虑如何使本次选择做到最优, 而暂不考虑总体是否达到最优.

但是, 每一步最优并不一定能保证全局最优, 例如, 如果采用贪婪算法在下图中求解由 a 到 c 的最短路径, 若在每一步都选择到已选顶点最小权值的边, 将得到路径 (a, d, c), 但这并不是从 a 到 c 的最短路径.



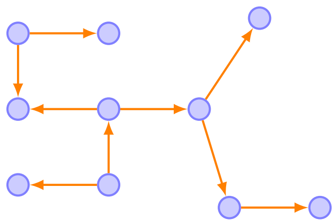
Prim 算法和 Kruskal 算法这两个贪婪算法, 对最小生成树的结果都是最优的. 7.24

2 根树及其应用

根树及其应用

1. 有向树
2. m 叉树
3. 有序树
4. 最优树
5. 前缀码

7.25



有向树

Definition 13. 如果一个有向图在不考虑边的方向时是一棵树, 则这个有向图称为有向树.

Example 14. 如图为一棵有向树: 7.26

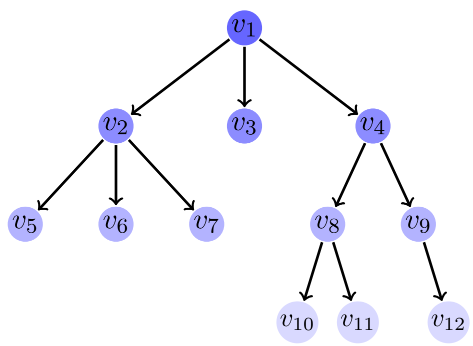
有向树

Definition 15. 一棵有向树, 如果恰有一个结点的入度为 0, 其余所有结点的入度都为 1, 则称为根树 (rooted tree).

1. 入度为 0 的结点称为根;
2. 出度为 0 的结点称为叶;
3. 出度不为 0 的结点称为分枝点或内点.

7.27

Example 16. 如图为一棵根树:



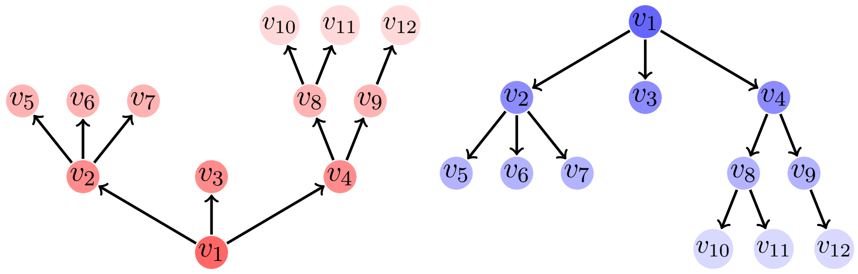
其中, v_1 为根, v_1, v_2, v_4, v_8, v_9 为分枝点, 其余结点为叶. 7.28

有向树

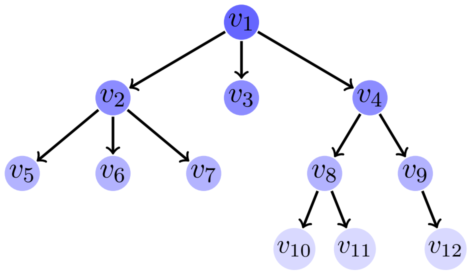
结点的层次

在一棵根树中, 从根到某个结点的单向通路的长度 (即边数) 是固定的, 它叫做该结点的层次.

Example 17. 如图, 结点 v_2, v_3, v_4 的层次为 1. 结点 v_{10}, v_{11}, v_{12} 的层次为 3.

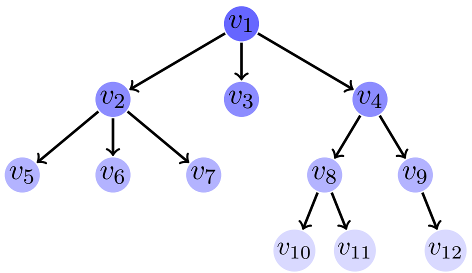


(a) (b)



7.29

根树的递归定义



根树中每一个结点都可以看作是原来树中某一棵子树的根. 从而, 根树可递归定义为:

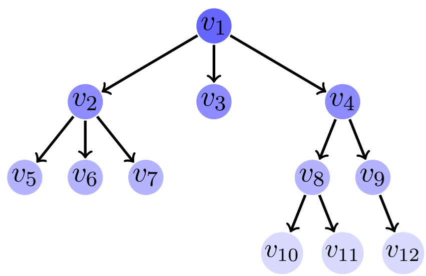
Definition 18. 根树包含一个或多个结点, 这些结点中某一个称为根, 其他所有结点被分成有限个子根树. 7.30

根树的两种画法

根树可以有树根在上或树根在下两种画法, 它们是同构的.

Example 19.

图 (a) 是根树的自然表示法. 7.31



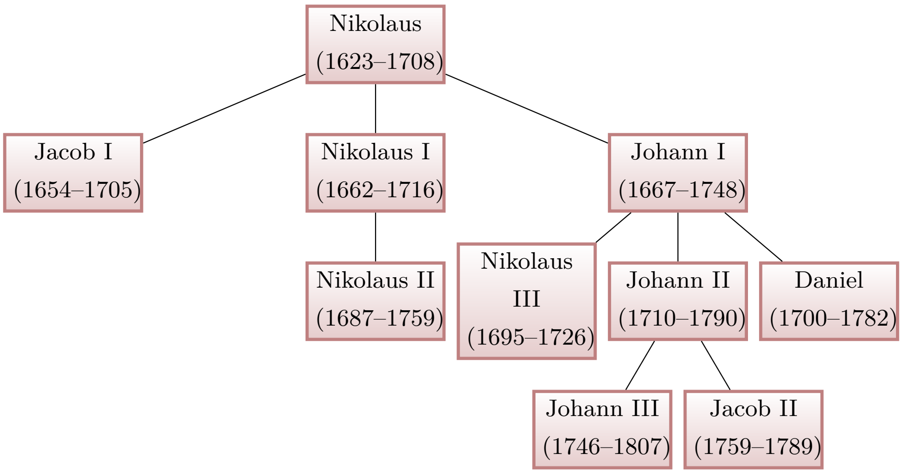
Example 20.

图中,

- v_2 称为 v_1 的儿子, v_1 称为 v_2 的父亲;
- v_1 称为 v_5 的祖先, v_5 称为 v_1 的后裔;
- v_{10}, v_{11}, v_{12} 称为兄弟.

对其它的结点有类似的说法. 树的术语起源于植物学和族谱学. 7.32

伯努利家族[3]的族谱图



7.33

m 叉树

Definition 21. 1. 在根树中, 若每个结点的出度小于等于 m, 则称该树为 m 叉树.

2. 如果每个结点的出度恰好等于 m 或 0, 则称该树为完全 m 叉树.
3. 如果完全 m 叉树所有树叶的层次都相同, 则称为正则 m 叉树.

7.34

Example 22. 7.35

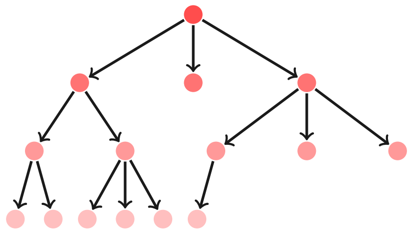
用 m 叉树表示实际问题

Example 23. M 和 E 两人进行网球比赛, 如果一人连胜两局或一共胜三局, 则比赛结束, 试用二叉树表示比赛可能发生的各种情况.

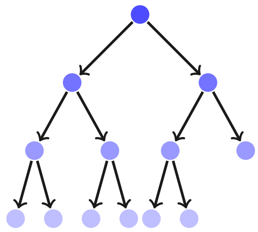
解: 用二叉树的分枝点表示每局赛事, 每局比赛的胜负标在其两个儿子结点的旁边. 从树根到树叶的每一条路对应比赛可能发生的一种情况: 7.36

- EE, MM ; EMM , MEE ;
- $EMEE$, $MEMM$;
- $EMEME$, $EMEMM$, $MEMEE$, $MEMEM$.

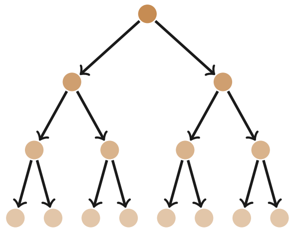
[3]著名的瑞士数学家家族. 见: E.T. 贝尔《数学精英》P.152, 商务印书馆.



(a) 三叉树



(b) 完全二叉树



(c) 正则二叉树

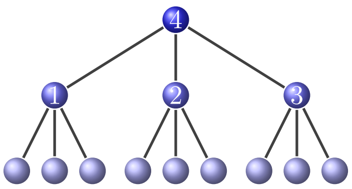
Theorem 24. 设有完全 m 叉树, 其树叶数为 l, 分枝点数为 i, 则

$$(m-1)i = l-1$$

证: 可将完全 m 叉树视为每局有 m 位选手参加比赛的单淘汰赛计划表.

树叶数 l 表示参加比赛的选手数, 分枝点表示比赛的局数. 因每局比赛将淘汰 $(m-1)$ 位选手, 故比赛结果共要淘汰 $(m-1)i$ 位选手, 最后得出一位冠军.

因此 $(m-1)i+1=l$, 即 $(m-1)i=l-1$. □



例如左图所示为 9 位选手参加比赛的情况: 7.37

$$l=9, \quad i=4, \quad m=3.$$

完全 m 叉树的性质

事实上, 这个定理还有一个简单的证明.

对完全 m 叉树, 设其树叶数为 l, 分枝点数为 i, 则结点总数 n 为

$$n=l+i, \qquad \text{或} \qquad n=mi+1.$$

所以 $l+i=mi+1$, 即 $(m-1)i=l-1$.

其中 $n=mi+1$ 是因为每个分枝点都有 m 个儿子, 且全部结点中只有树根不是某个结点的儿子. 这个结论可以作为一个定理.

Theorem 25. 对完全 m 叉树, 若分枝点数为 i, 则结点总数为 $n=mi+1$. 7.38

完全 m 叉树的性质

从上面的讨论中, 我们还可以看到, 对完全 m 叉树, 知道 l, i, n 这三个中的一个, 则其它两个必定可求.

Theorem 26. *对完全 m 叉树,*

1. *若结点总数 n 为已知, 则分枝点数为 $i = (n-1)/m$, 树叶数为 $l = n - i = n - (n-1)/m$.*
2. *若分支点数 i 为已知, 则结点总数为 $n = mi + 1$, 树叶数为 $l = n - i = (m-1)i + 1$.*
3. *若树叶数 l 为已知, 则结点总数为 $n = (ml-1)/(m-1)$, 分枝点数为 $i = (l-1)/(m-1)$.*

7.39

Example 27. 假定我们开始一个发送手机短信的游戏, 要求每个收到短信的人把短信再转发给另外某 4 个人, 每人只能收到一次短信. 有些人收到短信后这样做了, 但是有些人收到短信后没有转发. 如果某个时刻已经有 100 人收到了短信而没有转发, 问有多少人发出过短信?

解: 可以用一个完全 4 叉树表示这个过程. 每个人是一个结点, 收到了短信而没有转发的人是树叶, 转发了短信的人是分枝点, 则树叶总数是 $l = 100$.

分枝点数为

$$i = \frac{l-1}{m-1} = \frac{100-1}{4-1} = 33,$$

所以一共有 33 人发出了短信. □

7.40

有序树

在根树中, 一般将树根放在最上面, 但分枝点关联的各分枝的左中右按顺序却有种种不同的摆法. 所以, 标定根树中结点和边的次序在应用中是必要的.

- 标定了结点和边的次序的根树叫*有序树*.
- 任一有序树都可用二叉树来表示.

7.41

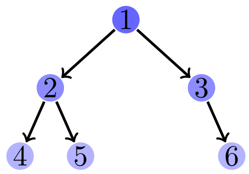
有序树写为对应的二叉树

任何一棵有序树都可以改写为一棵对应的二叉树, 方法如下:

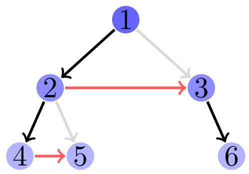
1. 删除始于每个结点除最左边的一个分枝外的其余分枝; 在同一层次中的兄弟结点之间用自左到右的有向边连接.
2. 对某个结点, 直接位于该结点下面的结点作为*左儿子*. 位于同一水平线上与该结点右邻的结点作为*右儿子*.
3. 改写之后的树根仅有一个儿子, 规定是左儿子.

下页是一个例子... 7.42

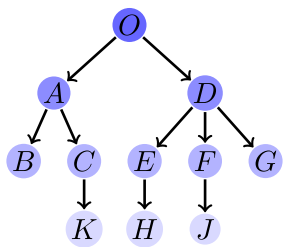
7.43



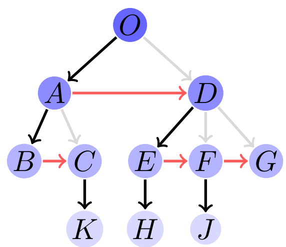
(a)



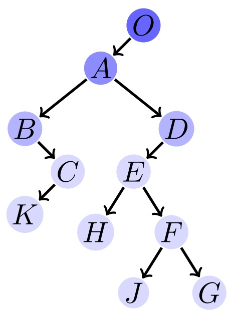
(b)



(a)



(b)

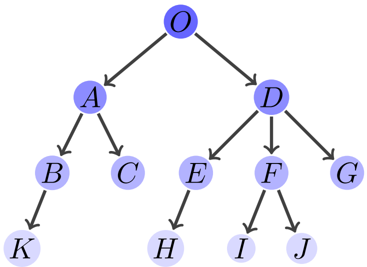


(c)

通路长度

Definition 28. 1. 在根树中, 从树根到某结点的通路的边数叫该结点的通路长度.

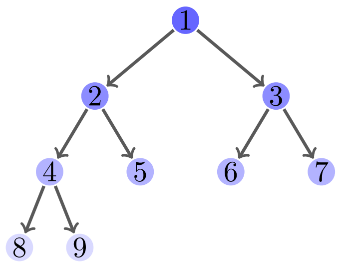
2. 将分枝点的通路长度称为内部通路长度;
3. 树叶的通路长度叫外部通路长度.



例如, 图中结点 K 的通路长度为 3; 结点 F 的通路长 7.44
度为 2;

Theorem 29. *设完全二叉树有 n 个分枝点 (含根结点), 且内部通路长度的总和为 I, 外部通路长度的总和为 E, 则 $E = I + 2n$.*

例如



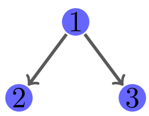
上图为一棵完全二叉树, 其中有 9 个结点, 分枝点 (即内点) 有 4 个,

$$I = 1 + 1 + 2 = 4,$$

$$E = 3 + 3 + 2 + 2 + 2 = 12.$$

证: 对分枝点数 n 进行归纳证明.

当 $n = 1$ 时, $E = 2$, $I = 0$, 故公式成立.



续证: 假设 $n = k - 1$ 时成立.

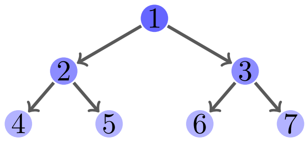
当 $n = k$ 时, 若删去一个分枝点 v (即删除该分枝点的儿子).

设该分枝点的通路长度为 l, 且 v 的两个儿子是树叶, 得出的新树为 T'.

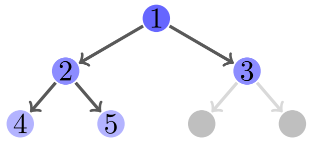
与原树相比, T' 减少了两片通路长度为 $l + 1$ 的树叶和一个通路长度为 l 的分枝点, 所以, $E' = E - 2(l + 1) + l$, 且 $I' = I - l$.

又 T' 有 $k - 1$ 个分枝点, 所以 $E' = I' + 2(k - 1)$.

代入前两式并整理得 $E = I + 2k$. □ 7.45



(a) T



(b) T'

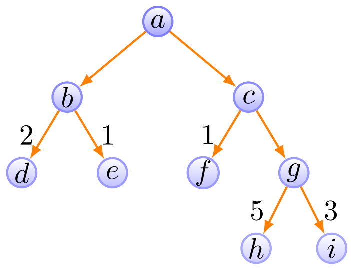


Figure 1: 带权二叉树 T

最优树

Definition 30. • 设二叉树有 t 片树叶, 各片树叶分别带有权数 $w_1, w_2, \cdots, w_t$, 则该二叉树称为带权二叉树.

- 设带权二叉树中权为 w_i 的树叶的通路长度为 $L(w_i)$, 将

$$w(T) = \sum_{i=1}^{t} w_i L(w_i)$$

称为带权二叉树的权.

- 在所有带权 $w_1, w_2, \cdots, w_t$ 的二叉树中, $w(T)$ 最小的树称为最优树.

7.46

Example 31.

$$\begin{aligned} w(T) &= \sum_{i=1}^{t} w_i L(w_i) \\ &= 2 \times 2 + 1 \times 2 + 1 \times 2 + 5 \times 3 + 3 \times 3 \\ &= 32 \end{aligned}$$

7.47

Theorem 32. 设 T 为带权 $w_1 \leqslant w_2 \leqslant \cdots \leqslant w_t$ 的最优树, 则

① 带权 w_1, w_2 的树叶 v_{w_1}, v_{w_2} 是兄弟.

② 以树叶 v_{w_1}, v_{w_2} 为儿子的分枝点的通路最长.

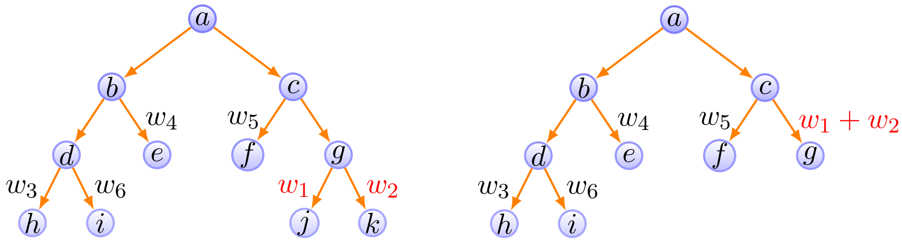
简而言之: 最优树中具有最小权的两片树叶是兄弟, 且其通路长度最大.

证: 设带权 $w_1, w_2, \cdots, w_t$ 的最优树中, v 是通路最长的分枝点. v 的两个儿子分别带权 w_x, w_y. 那么

$$L(w_x) \geqslant L(w_1), \qquad L(w_y) \geqslant L(w_2)$$

若 $L(w_x) > L(w_1)$, 将 w_x 与 w_1 对调得到新树 T', 则

$$\begin{aligned} w(T') - w(T) &= \big(L(w_x)w_1 + L(w_1)w_x\big) - \big(L(w_x)w_x + L(w_1)w_1\big) \\ &= L(w_x)(w_1 - w_x) + L(w_1)(w_x - w_1) \\ &= (w_x - w_1)\big(L(w_1) - L(w_x)\big) < 0 \end{aligned}$$



(a) T (b) T'

所以 $w(T') < w(T)$, 与 T 是最优树的假设矛盾, 故 $L(w_x) = L(w_1)$.

同理可证 $L(w_x) = L(w_2)$. 所以 $L(w_1) = L(w_2) = L(w_x) = L(w_y)$.

分别将 w_1, w_2 与 w_x, w_y 对调, 得出最优树, 带权 w_1, w_2 的树叶是兄弟. □ 7.48

Theorem 33. 设 T 为带权 $w_1 \leqslant w_2 \leqslant \cdots \leqslant w_t$ 的最优树, 若将以带权 w_1, w_2 的树叶为儿子的分枝点改为带权 $w_1 + w_2$ 的树叶, 得到一棵新树 T', 则 T' 也是最优树.

注意:

$$w(T) = w(T') + w_1 + w_2$$

简而言之: 求带 t 个权的最优树, 可简化为求带 $t-1$ 个权的最优树. 证: 由题设可知:

$$w(T) = w(T') + w_1 + w_2 \tag{2}$$

若 T' 不是最优树, 则必有另一棵带权 $w_1 + w_2, w_3, \cdots, w_t$ 的最优树 T''. 将 T'' 中带权 $w_1 + w_2$ 的树叶 $v_{w_1+w_2}$ 生成两个儿子 (带权 w_1, w_2 的树叶), 得到新树 $\widehat{T}$, 则

$$w(\widehat{T}) = w(T'') + w_1 + w_2 \tag{3}$$

由假设, $w(T'') \leqslant w(T')$. 如果 $w(T'') < w(T')$, 比较 (2), (3) 式可知 $w(\widehat{T}) < w(T)$, 与 T 是带权 $w_1, w_2, \cdots, w_t$ 的最优树相矛盾.

因此, $w(T'') = w(T')$. 即 T' 是带权 $w_1 + w_2, w_3, \cdots, w_t$ 的最优树. □ 7.49

前缀码

Definition 34. 给定一个序列的集合, 如果不存在一个序列是另一个序列的前缀, 则该序列的集合称为前缀码.

例如,

- $\{100, 101, 00, 01, 11\}$ 是前缀码,
- 而 $\{001, 010, 00, 01, 10\}$ 就不是前缀码.

7.50

Theorem 35. 任意一棵二叉树对应一个前缀码.

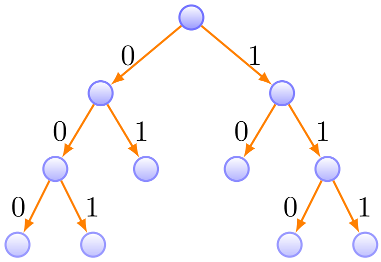


Figure 2: 带权二叉树 T

证: 给定一棵二叉树, 从每个分枝点出发, 将左枝标为 0, 右枝标为 1, 则每片树叶对应一个 0 和 1 组成的序列, 该序列是从树根到该树叶的通路上各边标号组成的.

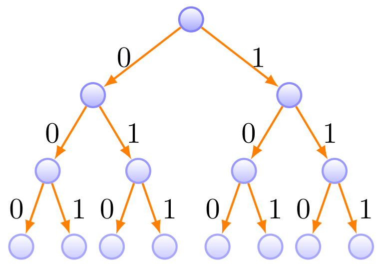
显然, 没有一片树叶对应的序列, 是另一片树叶对应序列的前缀. 所以任意一棵二叉树对应一个前缀码.

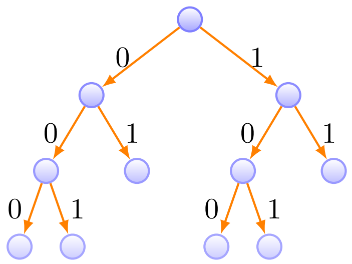
7.51

Theorem 36. 任意一个前缀码对应一棵二叉树.

证: 设 h 是某个前缀码中最长序列的长度. 作一棵高为 h 的正则二叉树, 将每个分枝点的左、右枝分别标以 0 和 1, 则每片树叶对应一个 0 和 1 组成的序列, 该序列是从树根到该树叶的通路上各边标号组成的. 因此, 长度不超过 h 的每个 0 和 1 组成的序列必对应一个结点.

将对应于前缀码中的每个序列的结点给予一个标记, 并删去标记结点的后裔及由它们射出的边. 再删去未加标记的树叶, 得到一棵新的二叉树, 其树叶就对应给定的前缀码.



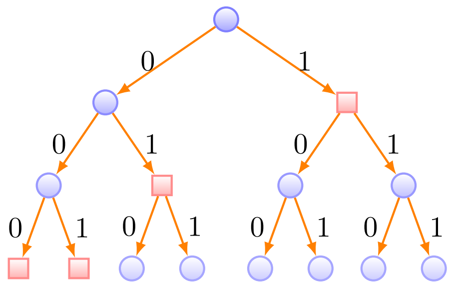


7.52

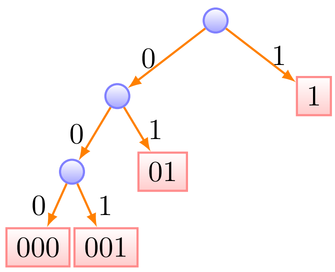
Example 37. 给定前缀码 $\{000, 001, 01, 1\}$, 求对应的二叉树.

解: 作一棵高为 3 的正则二叉树; 标记对应前缀码的结点, 并删去标记结点的后裔.

7.53



(a) T



(b) T'

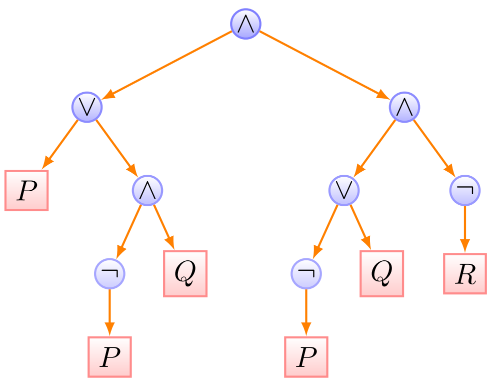
- 由前缀码和二叉树的对应关系可知, 如果给定的前缀码对应的二叉树是完全二叉树, 则根据此前缀码可对任意二进制序列译码.
  例如, 由前例中的前缀码 $\{000, 001, 01, 1\}$ 可对任意二进制序列译码. 随意写一个由 0 和 1 组成的字符串, 例如:
  $$00010011011101001$$
  它可译为且只能译为:
  $$000, 1, 001, 1, 01, 1, 1, 01, 001$$
- 如果被译的序列的最后部分不能构成前缀码中的序列, 可约定添加 0 或 1, 直到能译出为止.
- 如果前缀码对应的二叉树不是完全二叉树, 例如 $\{000, 001, 1\}$ 也是前缀码, 但它不能对任意二进制序列译码. 上述二进制序列, 用这组编码就无法译出.

7.54

练习

用根树表示 $(P \vee (\neg P \wedge Q)) \wedge ((\neg P \vee Q) \wedge \neg R)$.

解:



7.55

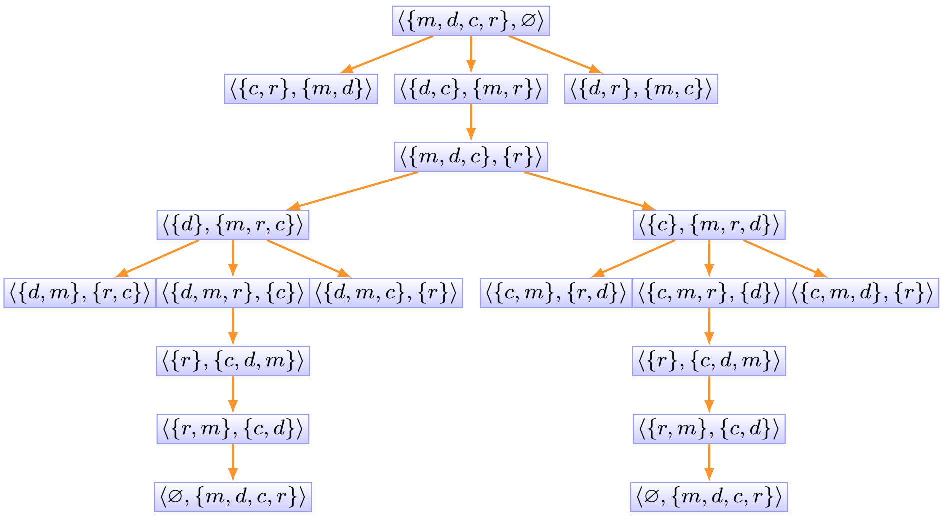
Example 38. 试用有向图描述下列问题的解:

某人 m 带一条狗 d, 一只猫 c 和一只兔子 r 过河. m 每次游过河时只能带一只动物, 而没人管理时, 狗与兔子不能共处, 猫和兔子也不能共处. 问 m 怎样把三个动物带过河去?

分析：用结点代表状态，状态用序偶 $\langle S_1, S_2\rangle$ 来表示，这里 S_1，S_2 分别是左岸、右岸的人和动物的集合. 例如初始状态为 $\langle\{m,d,c,r\}, \varnothing\rangle$，最终的目的即是 $\langle\varnothing, \{m,d,c,r\}\rangle$.

注意不能出现集合 $\{d, r\}$，$\{c, r\}$. 当出现集合 $\{d, r\}$ 或 $\{c, r\}$ 时，方案终止. 如果出现之前已有的状态，方案也终止，如下一页图中第 4 层出现的 $\langle\{d,m,c\}, \{r\}\rangle$ 和 $\langle\{c,m,d\}, \{r\}\rangle$，都是返回到了第 2 层的状态 $\langle\{m,d,c\}, \{r\}\rangle$，从而方案终止. 7.56

解: 注意到不能出现集合 $\{d, r\}$ 或 $\{c, r\}$，描述上述问题的有向图如下.



7.57

Chapter 8

命题逻辑

Discrete Mathematics

November 24, 2011

黄正华, 数学与统计学院, 武汉大学

8.1

Contents

8.2

数理逻辑简介

- 研究人的思维形式和规律的科学称为逻辑学. 由于研究的对象和方法各有侧重而又分为
  - 形式逻辑
  - 辨证逻辑
  - 数理逻辑
- 数理逻辑是运用数学方法研究推理的科学.

  - 数理逻辑又叫符号逻辑, 因为它的主要工具是符号体系.
  - 数理逻辑的核心是把逻辑推理符号化, 即变成象数学演算一样的逻辑演算.

- 在本课程中主要介绍命题逻辑和谓词逻辑. 8.3

关于逻辑的故事

一人在寻找真理, 别人问他: “你真的不知道真理是什么吗? ” 那个人说: “当然! ”

别人又问: “你既然不知道真理是什么, 当你找到真理的时候, 你又如何辨别出来呢? 如果你辨别得出真理与否, 那说明你已经知道了真理是什么, 又何来寻找呢? ” 8.4

关于逻辑的故事

上帝真的是万能的吗?[1]

让我们来提出一个问题: 上帝是否能创造出一块连自己都举不起来的石头?

如果上帝创造出了一块连他自己都举不起来的石头, 那么上帝就不是万能的, 因为有一块石头他举不起来.

如果上帝不能创造出一块连他自己都举不起来的石头, 那么上帝也不是万能的, 因为有一块石头他创造不出来.

所以无论上帝是否能创造出这么一块石头, 他都不是万能的. 8.5

关于逻辑的故事

据传, 古希腊有一个叫欧提勒士的年轻人, 向当时著名的智者普罗达哥拉斯学习法律. 双方签了一个合同, 结束学业之后, 学生付给老师一半学费, 另一半学费则要等到学生第一次出庭打赢官司, 再支付.

可是学生一直没有打赢官司, 剩下的一半学费老师迟迟没有拿到. 老师终于等不及了, 就向法庭起诉, 要学生支付另一半学费.

老师说: “如果你打赢这场官司, 依照合同, 你得把另一半学费付给我; 如果你打输这场官司, 那么根据法庭判决, 你也得把另一半学费付给我. 所以, 不管你这场官司是赢是输, 你都要把学费给我.”

学生反驳道: “如果我打输这场官司, 依照合同, 我不需要把另一半学费付给你; 如果我打赢这场官司, 那么根据法庭判决, 我也不需要把另一半学费付给你. 所以, 不管我这场官司是赢是输, 我都不需要把学费给你.” 8.6

关于逻辑的故事

逻辑推理俱乐部门口贴着一张布告:“欢迎你加入推理俱乐部! 只要你通过推理取得一张申请表, 就可以获得会员资格了!”

只见桌子上摆着两个盒子: 一个圆盒子, 一个方盒子.

[1]此问题与宗教或信仰无关. 这里我们只谈及逻辑.

圆盒子上写着一句话:“申请表不在此盒中”. 方盒子上写着一句话:“这两句话中只有一句是真话”.

那么申请表在哪个盒子里呢?

- 设方盒子上写的话 (“这两句话中只有一句是真话”) 是真的, 推出圆盒子上的话 (“申请表不在此盒中”) 是假的. 推出申请表在圆盒子中.
- 设方盒子上的话 (“这两句话中只有一句是真话”) 是假的, 推出圆盒子上的话也是假的. 推出申请表在圆盒子中.
- 或者方盒子上的话是真的, 或者方盒子上的话是假的. 总之, 申请表在圆盒子中. 8.7

数理逻辑的简单历史 —— 三个阶段

0. Aristotle: 形式逻辑 (古典逻辑).
1. 初始阶段: (1660s — 19 世纪末) 将数学应用于逻辑 (Leibniz, George Boole, De Morgan). Leibniz
2. 过度阶段: (19 世纪末 — 1940 前后) 逻辑应用于数学.
3. 成熟阶段: (1930s — 1970s) 成为数学的独立分支. 8.8

1 命题及其符号化

1.1 命题与命题变元

命题 (propositions *or* statements)

- 命题是非真即假的陈述句.
  - 首先判定它是否为陈述句;
  - 其次判断它是否有惟一的真值.
- 真值只有两个: 真或假[2]3> 只有说法 “真值为真” 或 “真值为假” —— 没有 “假值” 一说.. 记作 True 和 False. 分别用符号 **T** 和 **F** 表示. (也经常分别用 1 和 0 表示.) 8.9

Example 1. 判断下列句子是否为命题.

1. 4 是素数. ✔
2. $\sqrt{2}$ 是无理数. ✔
3. x 大于 y. ✗
4. 外太空有生命. ✔

[2] <

5. 明年元旦武汉是晴天. ✔
6. π 大于 $\sqrt{2}$ 吗? ✗
7. 请不要吸烟! ✗
8. 我正在说假话. (悖论) ✗

8.10

简单命题 & 复合命题

根据命题的构成形式, 可以将命题分为:

- 简单命题: 只由一个主语和一个谓语构成的最简单的陈述句, 称为简单命题, 或原子命题或原子 (atoms).
- 复合命题: 由原子命题和命题联结词构成. 也称为分子命题.

Example 2. <2>

- “明天下雪”、“4 是素数” 都是原子命题.
- “明天下雪或明天下雨” 是复合命题.

8.11

命题的符号化

- 可以用以下两种形式将命题符号化:
  - 用大写字母; 例如, P: 今天天气晴好.
  - 用数字. 例如, [17]: 今天天气晴好.
- 上述的 P 和 [17] 称为命题标识符.

8.12

命题常量, 命题变元, 指派

- 命题常量 *(proposition constants)* —— 表示具体命题的命题标识符. 例如, P: 今天天气晴好. 则 P 是命题常量.
- 命题变元 *(proposition variable)* —— 未指定具体命题、可以代表任意命题的命题标识符. 比如讨论运算规律时使用的命题标识符. 命题变元不是命题.
- 指派 *(assignments)* —— 命题变元用一个特定命题取代, 从而成为一个命题, 这个过程称为对命题变元进行指派. 集合 $\{\mathbf{T}, \mathbf{F}\}$ 是命题变元的值域.

8.13

1.2 命题联结词

联结词

$$\boxed{\text{原子命题} + \text{联结词} = \text{复合命题}}$$

联结词是复合命题的重要组成部分, 又称为逻辑运算符. 常用的有五种:

- 否定 $\neg$
- 合取 $\wedge$
- 析取 $\vee$
- 蕴含 $\rightarrow$
- 等价 $\leftrightarrow$

8.14

否定 ¬

Definition 3 (否定 (negation)). • 设 P 为命题, 则 P 的否定是一个新的命题, 记为 $\neg P$, 读做 "非 P".

• 若 P 为 **T**, 则 $\neg P$ 为 **F**; 若 P 为 **F**, 则 $\neg P$ 为 **T**.

P	$\neg P$
T	**F**
F	**T**

8.15

合取 ∧

Definition 4 (合取 (conjunction)). • 如果 P 和 Q 是命题, 那么 "P 并且 Q" 也是命题, 记为 $P \wedge Q$, 或 $P \times Q$ 称为 P 与 Q 的合取, 读做 "P 与 Q" 或 "P 并且 Q".

• $P \wedge Q$ 真值为 **T**, 当且仅当 P 和 Q 真值都为 **T**.

P	Q	$P \wedge Q$
T	**T**	**T**
T	**F**	**F**
F	**T**	**F**
F	**F**	**F**

8.16

Example 5. 设 P: 这些都是男生; 则 $\neg P$: 这些不都是男生. (不能写成 "这些都不是男生". Why?)

Example 6. <3> P: 2 是素数, Q: 2 是偶数; 则 $P \wedge Q$: 2 是素数, 并且是偶数. 8.17

析取 ∨

Definition 7 (析取 (disjunction)). • 如果 P 和 Q 是命题, 那么 "P 或 Q" 也是命题, 记为 $P \vee Q$, 或 $P + Q$ 称为 P 与 Q 的析取, 读做 "P 或 Q".

• $P \vee Q$ 真值为 **T**, 当且仅当 P 或 Q 至少有一个真值为 **T**.

P	Q	$P \vee Q$
T	**T**	**T**
T	**F**	**T**
F	**T**	**T**
F	**F**	**F**

☞"或" 的语意: "可兼或", "排斥或"(也称异或, 不可兼或), 表示大概、大约. 8.18

"可兼或"(inclusive-or) 和 "排斥或"(exclusive-or)

Example 8. 将下列命题符号化:

1. 张三爱唱歌或爱听音乐;
2. 张三在 202 房间或 203 房间.

解: (1) 设 P: 张三爱唱歌, Q: 张三爱听音乐; 这里的 "或" 是 "可兼或", 也称为 "相容或", 即两者可以同时为真, 因此可以符号化为 $P \vee Q$. 解: (2) 设 U: 张三在 202 房间, V: 张三在 203 房间. 如果也符号化为 $U \vee V$, 张三就同时在两个房间, 这违背题意. 这里的 "或" 是 "排斥或". 要达到只能在一个房间的要求, 可用多个联结词符号化为

$$(U \wedge \neg V) \vee (\neg U \wedge V)$$

return ☞ 析取指的是 "可兼或".

8.19

Example 9. 将下列命题符号化:

1. 小王是跳远冠军或百米赛跑冠军.
2. 小王在宿舍或在图书馆.
3. 选小王或小李中的一人当班长.

解:

1. $P \vee Q$. (可兼或) 其中 P: 小王是跳远冠军. Q: 小王是百米赛跑冠军.
2. $(P \wedge \neg Q) \vee (\neg P \wedge Q)$. (排斥或) 其中 P: 小王在宿舍. Q: 小王在图书馆.
3. $(P \wedge \neg Q) \vee (\neg P \wedge Q)$. (排斥或) 其中 P: 选小王为班长. Q: 选小李当班长.

8.20

蕴含 $\rightarrow$

Definition 10 (蕴含 (implication)).
- 给定两个命题 P 和 Q, 其蕴含命题是一个复合命题, 记作 $P \rightarrow Q$, 读作 "P 蕴含 Q" 或 "如果 P, 那么 Q" 或 "若 P, 则 Q".
- 当且仅当 P 的真值为 **T**, Q 的真值为 **F** 时, $P \rightarrow Q$ 的真值为 **F**.
- 称 P 为前件 (或前题), Q 为后件 (或结论).

P	Q	$P \rightarrow Q$
T	**T**	**T**
T	**F**	**F**
F	**T**	**T**
F	**F**	**T**

8.21

关于 $P \to Q$ 真值表的注解

- 在自然语言中, "如果 P, 那么 Q" 中的前件 P 与后件 Q 往往具有某种内在联系. 而在数理逻辑中, P 与 Q 可以无任何内在联系. 例如: ☞ 如果雪是黑的, 那么太阳从西方出来.
- 在数学或其它自然科学中, "如果 P, 那么 Q" 往往表达的是前件 P 为真, 后件 Q 也为真的推理关系. 但在数理逻辑中, 作为一种 "善意推定" 的规定, 当 P 为假时, 无论 Q 是真是假, $P \to Q$ 均为真. 也就是说, 只有 P 为 **T** 并且 Q 为 **F** 这一种情况, 才能使得复合命题 $P \to Q$ 为 **F**.

☞ 什么是 "善意的推定"?

8.22

善意的推定

Example 11. 张三对李四说: "若我去图书馆, 我一定帮你借那本书". 可以将这句话表示为命题 $P \to Q$ (P: 张三去图书馆, Q: 张三借那本书). 后来张三因有事未去图书馆, 即 P 为 **F**, 此时按规定 $P \to Q$ 为 **T**. 我们可理解为张三讲了真话, 即他要是去图书馆, 我们相信他一定会为李四借书. 这就是所谓 "善意的推定".

8.23

Example 12. 将下列命题符号化:

1. 只要天不下雨, 我就骑自行车上班.
2. 只有天不下雨, 我才骑自行车上班.

解: 设 P: 天下雨, Q: 我骑自行车上班.

1. $\neg P \to Q$. (天不下雨是骑车上班的充分条件.)
2. $Q \to \neg P$, 或 $P \to \neg Q$. (如果骑自行车上班, 一定是天不下雨.)

8.24

Example 13. 将下列命题符号化:

1. 除非今天天气好, 否则我不会去公园.
2. 我将去镇上, 仅当我有时间.

解: ① 含义: 我去公园必定是天气好, 至于天气好是否去公园, 在命题中没有涉及.

设 P: 今天天气好. Q: 我去公园.

$$Q \to P.$$

② 设 P: 我将去镇上. Q: 我有时间.

$$P \to Q.$$

8.25

注

以下句式均可符号化为 $P \to Q$:

- "如 P, 则 Q",
- "因为 P, 所以 Q",
- "只要 P, 就 Q",
- "P, 仅当 Q", (我将去镇上, 仅当我有时间时.)
- "只有 Q, 才 P", (只有天不下雨, 我才骑自行车上班.)
- "除非 Q, 才 P",
- "除非 Q, 否则非 P". (除非天气好, 否则我不会去公园的.)

8.26

等价 $\leftrightarrow$

Definition 14 (等价 (two-way-implication)).

- 给定两个命题 P 和 Q, 其复合命题 $P \leftrightarrow Q$ 称作等价命题, 读作 "P 当且仅当 Q".
- $P \leftrightarrow Q$ 为 **T**, 当且仅当 P 和 Q 同时为 **T**, 或同时为 **F**.
- 等价联结词 "$\leftrightarrow$" 也可以记作 "$\rightleftarrows$" 或 "iff".

P	Q	$P \leftrightarrow Q$
T	**T**	**T**
T	**F**	**F**
F	**T**	**F**
F	**F**	**T**

8.27

Example 15. 分析下列各命题的真值:

1. $2+2=4$, 当且仅当 3 是奇数.
2. $2+2=4$, 当且仅当 3 不是奇数.
3. $2+2\neq 4$, 当且仅当 3 是奇数.
4. $2+2\neq 4$, 当且仅当 3 不是奇数.

解: 设 P: $2+2=4$. Q: 3 是奇数.

1. $P \leftrightarrow Q$, 真值为 **T**. (因 P, Q 皆为真);
2. $P \leftrightarrow \neg Q$, 真值为 **F**. (因 P 为真, $\neg Q$ 为假);
3. $\neg P \leftrightarrow Q$, 真值为 **F**. (因 $\neg P$ 为假, Q 为真);
4. $\neg P \leftrightarrow \neg Q$, 真值为 **T**. (因 $\neg P$, $\neg Q$ 皆为假).

8.28

Example 16. 设 P: 天下雨, Q: 草木枯黄. 则

$\neg P$**:** 天不下雨;
$\neg P \wedge Q$**:** 天不下雨并且草木枯黄;
$\neg P \vee Q$**:** 天不下雨或草木枯黄;
$\neg P \rightarrow Q$**:** 如果天不下雨, 那么草木枯黄;
$\neg P \leftrightarrow Q$**:** 天不下雨当且仅当草木枯黄.

8.29

小结

1. 命题是客观上能判明真假的陈述句. 当命题为真时, 称命题的真值为 “真”; 否则, 说命题的真值为 “假”.
2. 析取联结词 $\vee$ 指的是 “可兼或”; 而汉语中的 “或”, 既可以用于 “可兼或”, 也可用于 “排斥或”.
3. 复合命题 $P \rightarrow Q$ 表示的逻辑关系是: Q 是 P 的必要条件, P 是 Q 的充分条件.
   - 在数学中, “如 P, 则 Q” 往往要求前件为真, 后者为真的推理关系.
   - 但在数理逻辑中规定: 当前件为假, 不论后件为真为假, 均有 $P \rightarrow Q$ 为真.

8.30

练习 (答案: ① A. ② A, D. ③ A, D.)

多项选择:

1. 设 P: 天热. Q: 我去游泳. R: 我在家读书. 则命题 “如天热, 我去游泳, 否则在家读书.” 的符号化结果是 ( ). (A) $(P \rightarrow Q) \vee (\neg P \rightarrow R)$; (B) $(P \rightarrow Q) \wedge (\neg P \rightarrow R)$; (C) $(P \wedge Q) \vee (\neg P \wedge R)$; (D) $(P \wedge Q) \wedge (\neg P \wedge R)$.
2. 设 P: 我上街. Q: 我有空闲时间. 则命题 “我上街, 仅当我有空闲时间.” 的符号化结果是 ( ). (A) $P \rightarrow Q$; (B) $Q \rightarrow P$; (C) $\neg P \rightarrow \neg Q$; (D) $\neg Q \rightarrow \neg P$.
3. 设 P: 我上街. Q: 我有空闲时间. 则命题 “除非我有空闲时间, 否则我不上街.” 的符号化结果是 ( ). (A) $P \rightarrow Q$; (B) $Q \rightarrow P$; (C) $\neg P \rightarrow \neg Q$; (D) $\neg Q \rightarrow \neg P$.

8.31

2 命题公式

2.1 命题公式及其真值

命题公式

Definition 17 (命题公式 (合式公式))**.** 以下条款规定了命题公式 (proposition formula) 的含义:

(1) 真值 0, 1 是命题公式;

(2) 命题常元、命题变元是命题公式;

(3) 如果 A 是命题公式, 那么 $\neg A$ 也是命题公式;

(4) 如果 A 和 B 是命题公式, 那么 $(A \wedge B)$, $(A \vee B)$, $(A \to B)$, $(A \leftrightarrow B)$ 都是命题公式;

(5) 只有有限次地应用 (1)~(4) 构成的符号串, 才是命题公式.

命题公式又称为*合式公式* (Wff, Well formed formula). 8.32

Example 18.
- 下列公式都是命题公式:

$$\neg(P \wedge Q)$$
$$\neg(P \to Q)$$
$$\big(P \to (P \vee \neg Q)\big)$$
$$\Big(\big((P \to Q) \wedge (Q \to R)\big) \leftrightarrow (S \leftrightarrow T)\Big)$$

- 下列都不是命题公式:

$$(P \to Q) \to (\wedge Q)$$
$$\big(P \to Q, (P \wedge Q) \to Q\big)$$

约定: 最外层的圆括号可以省略. 8.33

联结词运算的秩序

- 运算符结合力的强弱顺序约定为: $\neg$, $\wedge$, $\vee$, $\to$, $\leftrightarrow$.
  - 没有括号时按强弱先后顺序执行.
  - 相同运算符按从左至右顺序执行, 括号可省去. 例如, $A \vee (B \vee C)$ 与 $A \vee B \vee C$ 运算顺序一样.
  - 最外层的括号总可以省去. 例如, $(A \wedge B)$ 常写为 $A \wedge B$.
- 要养成"先 $\wedge$ 后 $\vee$" 的习惯.

Example 19. <2> 例如, 下列两式的运算顺序完全一样:

$$\big((\neg P \vee \neg S) \vee (\neg Q \wedge R)\big) \to \big((R \vee P) \vee Q\big) \tag{1}$$
$$\neg P \vee \neg S \vee \neg Q \wedge R \to R \vee P \vee Q \tag{2}$$

8.34

命题的翻译

命题符号化应注意以下几点:

- 确定句子是否为命题;
- 正确表示原子命题和选择命题联结词;
- 要按逻辑关系翻译而不能凭字面翻译. 例如翻译:
  - Tom 和 Jerry 是好朋友.
  - 蓝色和黄色可以调配成绿色. 8.35

命题的翻译

Example 20. 符号化下列命题:

1. 张三不是不聪明, 而是不用功.
2. 李文与李武是兄弟.
3. 除非你努力, 否则你将失败.
4. 如果我上街, 我就去书店看看, 除非我很累.

解: ① $\neg P \wedge Q$, 其中 P: 张三不聪明. Q: 张三不用功. 解: ② P,P: 李文与李武是兄弟. (原子命题.) 解: ③ $\neg P \to Q$, 其中 P: 你努力. Q: 你将失败. 解: ④ $Q \to (\neg P \to R)$. 或者 $\neg P \to (Q \to R)$; 或者 $(\neg P \wedge Q) \to R$ 其中 P: 我很累. Q: 我上街. R: 我去书店看看. 8.36

真值表的构造

Example 21. 构造 $\neg P \vee Q$ 的真值表.

解:

P	Q	$\neg P$	$\neg P \vee Q$
T	**T**	**F**	**T**
T	**F**	**F**	**F**
F	**T**	**T**	**T**
F	**F**	**T**	**T**

8.37

真值表的构造

Example 22. 构造 $\neg(P \wedge Q) \leftrightarrow (\neg P \vee \neg Q)$ 的真值表.

P	Q	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P$	$\neg Q$	$\neg P \vee \neg Q$	$\neg(P \wedge Q) \leftrightarrow (\neg P \vee \neg Q)$
T	**T**	**T**	**F**	**F**	**F**	**F**	**T**
T	**F**	**F**	**T**	**F**	**T**	**T**	**T**
F	**T**	**F**	**T**	**T**	**F**	**T**	**T**
F	**F**	**F**	**T**	**T**	**T**	**T**	**T**

- $\neg(P \wedge Q) \leftrightarrow (\neg P \vee \neg Q)$ 的真值全为真, 这类公式为永真公式, 记为 **T**. (另有永假公式, 记为 **F**.)
- $\neg(P \wedge Q)$ 与 $(\neg P \vee \neg Q)$ 的所有真值相同, 称二者是等价的. 8.38

2.2 命题公式的等值式

公式的等价

Definition 23 (公式的等价)**.** 若命题公式 A 和 B 的所有真值全都相同, 则称 A 和 B 等值或逻辑等价. 记作 $A \Leftrightarrow B$.

注: $A \Leftrightarrow B$, 当且仅当 $A \leftrightarrow B$ 为永真公式.

如: $\neg(P \wedge Q) \leftrightarrow (\neg P \vee \neg Q)$ 的真值全为真, 则

$$\neg(P \wedge Q) \quad 与 \quad (\neg P \vee \neg Q)$$

是等价的或逻辑相等. 反之亦然.

8.39

用真值表证明公式等价

Example 24. 试证 $\neg P \vee Q \Leftrightarrow P \to Q$.

证: 列出真值表

P	Q	$\neg P$	$\neg P \vee Q$	$P \to Q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

可知 $\neg P \vee Q$ 与 $P \to Q$ 真值相同, 所以 $\neg P \vee Q \Leftrightarrow P \to Q$.

☞ 牢记本题结论: $P \to Q \Leftrightarrow \neg P \vee Q$.

8.40

Example 25. 证明 $P \leftrightarrow Q \Leftrightarrow (P \to Q) \wedge (Q \to P)$.

证: 列出真值表:

P	Q	$P \leftrightarrow Q$	$P \to Q$	$Q \to P$	$(P \to Q) \wedge (Q \to P)$
T	T	T	T	T	T
T	F	F	F	T	F
F	T	F	T	F	F
F	F	T	T	T	T

$P \leftrightarrow Q$ 与 $(P \to Q) \wedge (Q \to P)$ 真值相同, 得证二者等价.

☞ 记住这个简单的结论. 8.41

Example 26. 证明 $P \leftrightarrow Q \Leftrightarrow (P \wedge Q) \vee (\neg P \wedge \neg Q)$.

证: 列出真值表:

P	Q	$P \leftrightarrow Q$	$(P \wedge Q) \vee (\neg P \wedge \neg Q)$
T	T	T	T
T	F	F	F
F	T	F	F
F	F	T	T

$P \leftrightarrow Q$ 与 $(P \wedge Q) \vee (\neg P \wedge \neg Q)$ 真值相同, 得证二者等价.

☞ 建议记住这个结论: 这是 $\leftrightarrow$ 向 $\vee, \wedge$ 的转化式. 8.42

常用的等价公式:

对合律	$\neg\neg P \Leftrightarrow P$	1
幂等律	$P \vee P \Leftrightarrow P,\ P \wedge P \Leftrightarrow P$	2
结合律	$(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$ $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$	3
交换律	$P \vee Q \Leftrightarrow Q \vee P,\quad P \wedge Q \Leftrightarrow Q \wedge P$	4
分配律	$P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$ $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$	5
吸收律	$P \vee (P \wedge Q) \Leftrightarrow P,\quad P \wedge (P \vee Q) \Leftrightarrow P$	6
德 · 摩根律	$\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$ $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$	7
同一律	$P \vee \mathbf{F} \Leftrightarrow P,\ P \wedge \mathbf{T} \Leftrightarrow P$	8
零律	$P \vee \mathbf{T} \Leftrightarrow \mathbf{T},\ P \wedge \mathbf{F} \Leftrightarrow \mathbf{F}$	9
否定律	$P \vee \neg P \Leftrightarrow \mathbf{T},\ P \wedge \neg P \Leftrightarrow \mathbf{F}$	10

8.43

常用等价公式的记忆

- 从含义上理解记忆.
- 对比集合的运算律记忆.

分配律	$P\vee(Q \wedge R) \Leftrightarrow (P \vee Q)\wedge(P \vee R)$ $P\wedge(Q \vee R) \Leftrightarrow (P \wedge Q)\vee(P \wedge R)$	$P\cup(Q \cap R) = (P \cup Q)\cap(P \cup R)$ $P\cap(Q \cup R) = (P \cap Q)\cup(P \cap R)$
吸收律	$P \vee (P \wedge Q) \Leftrightarrow P$ $P \wedge (P \vee Q) \Leftrightarrow P$	$P \cup (P \cap Q) = P$ $P \cap (P \cup Q) = P$
德 · 摩根律	$\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$ $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$	$\sim(P \cup Q) = \sim P \cap \sim Q$ $\sim(P \cap Q) = \sim P \cup \sim Q$

- 同一律、零律、否定律中的 **F**, **T** 可分别对比集合中的空集 $\varnothing$, 全集.

8.44

Example 27. 证明 $(P \to Q) \wedge (Q \to P) \Leftrightarrow (P \wedge Q) \vee (\neg P \wedge \neg Q)$. (不使用真值表.)

证:

$$
\begin{aligned}
& (P \to Q) \wedge (Q \to P) \\
\Leftrightarrow\ & (\neg P \vee Q) \wedge (\neg Q \vee P) \\
\Leftrightarrow\ & \big((\neg P \vee Q) \wedge \neg Q\big) \vee \big((\neg P \vee Q) \wedge P\big) \\
\Leftrightarrow\ & \big((\neg P \wedge \neg Q) \vee (Q \wedge \neg Q)\big) \vee \big((\neg P \wedge P) \vee (Q \wedge P)\big) \\
\Leftrightarrow\ & (\neg P \wedge \neg Q) \vee \mathbf{F} \vee \mathbf{F} \vee (Q \wedge P) \\
\Leftrightarrow\ & (\neg P \wedge \neg Q) \vee (Q \wedge P)
\end{aligned}
$$

8.45

置换

Definition 28. <1-> 如果 X 是合式公式 A 的一部分, 且 X 本身也是一个合式公式, 则称 X 为公式 A 的子公式.

Theorem 29 (置换规则 Rule of Replacement)**.** *<2-> 设 X 是合式公式 A 的子公式, 且 $X \Leftrightarrow Y$. 将 A 中的 X 用 Y 来置换, 得到新的公式 B. 则 $A \Leftrightarrow B$.*

即, 如果

$$\underbrace{X \wedge P \vee Q \cdots}_{A} \xrightarrow{X \Leftrightarrow Y} \underbrace{Y \wedge P \vee Q \cdots}_{B}$$

则 $A \Leftrightarrow B$. 8.46

例如

- 在 $P \vee Q \Leftrightarrow Q \vee P$ 中以 $A \wedge B$ 代 P 得
$$(A \wedge B) \vee Q \Leftrightarrow Q \vee (A \wedge B)$$
- 或以 $\neg C$ 代 P, 同时, 以 $\neg A \wedge B$ 代 Q 得
$$\neg C \vee (\neg A \wedge B) \Leftrightarrow (\neg A \wedge B) \vee \neg C$$

8.47

2.3 命题公式的逻辑蕴含式

重言式 (tautology)

Definition 30 (重言式 (tautology))**.** 重言式即永真公式: 无论对分量作怎样的指派, 其对应的真值永为 **T**.

例如, $\neg(P \wedge Q) \leftrightarrow (\neg P \vee \neg Q)$ 是重言式.

注

- 任何两个重言式的合取或析取, 仍然是一个重言式. (A 为 **T**, B 为 **T**, A 与 B 析取 (或合取) 仍为 **T**.)
- 一个重言式, 对同一分量都用任何 Wff 置换, 其结果仍为一重言式. (因为重言式的真值与分量的指派无关.)

8.48

矛盾式 (contradiction *or* absurdity)

- 矛盾式即永假公式, 记为 **F**.
  - 任何两个矛盾式的合取或析取, 仍然是一个矛盾式.
  - 一个矛盾式, 对同一分量都用任何 Wff 置换, 其结果仍为一矛盾式.

8.49

重言式 v.s 等价

P	Q	$P\wedge Q$	$\neg(P\wedge Q)$	$\neg P$	$\neg Q$	$\neg P\vee\neg Q$	$\neg(P\wedge Q)\leftrightarrow(\neg P\vee\neg Q)$
T	**T**	**T**	**F**	**F**	**F**	**F**	**T**
T	**F**	**F**	**T**	**F**	**T**	**T**	**T**
F	**T**	**F**	**T**	**T**	**F**	**T**	**T**
F	**F**	**F**	**T**	**T**	**T**	**T**	**T**

- $\neg(P\wedge Q)\Leftrightarrow(\neg P\vee\neg Q)$.
- $\neg(P\wedge Q)\leftrightarrow(\neg P\vee\neg Q)$ 是重言式.

Theorem 31. *<2> 设 A, B 是两个 Wff. $A\Leftrightarrow B$ 当且仅当 $A\leftrightarrow B$ 为一个重言式.*

8.50

蕴含式

Definition 32. 当且仅当命题公式 $P\to Q$ 为重言式时, 称 " P 蕴含 Q", 记为 $P\Rightarrow Q$, 它又称为逻辑蕴含式 (logically implication).

蕴含式的理解

符号 $\Rightarrow$ 不是联结词, 它表示公式间的 "永真蕴含" 关系, 也可以看成是 "推导" 关系.

即 $P\Rightarrow Q$ 可以理解成: 由 P 可推出 Q. (即由 P 为真, 可以推出 Q 也为真.)

> 当 $P\to Q$ 为永真时, 则认为 "由 P 可推出 Q", 即 "P 蕴含 Q".

8.51

证明蕴含式 $P\Rightarrow Q$ 的方法

方法 1. 列真值表, 证明 $P\to Q$ 为永真式 (略).

下面讨论另外两种方法.

先看 $P\to Q$ 的真值表: 如果 $P\to Q$ 为永真式, 则下述真值表的第二组指派不会出现.

P	Q	$P\to Q$
T	**T**	**T**
T	**F**	**F**
F	**T**	**T**
F	**F**	**T**

于是有下面两种证明方法.

方法 2. 假设前件 P 为 **T**, 推出后件 Q 也为 **T**.

方法 3. 假设后件 Q 为 **F**, 推出前件 P 也为 **F**. 8.52

证明 $\neg P\wedge(P\vee Q)\Rightarrow Q$.

证: 设 $\neg P \wedge (P \vee Q)$ 为真, 则 $\neg P$ 和 $P \vee Q$ 都为真. 那么 P 为假, 再由 $P \vee Q$ 为真, 得知 Q 为真.

证明 $(P \to Q) \wedge (Q \to R) \Rightarrow P \to R$.

证: 设 $P \to R$ 为假, 则 P 为真, 且 R 为假.

- 若 Q 为真, 则 $Q \to R$ 为假;
- 若 Q 为假, 则 $P \to Q$ 为假.

故 $(P \to Q) \wedge (Q \to R)$ 为假. 8.53

方法 2. 假设前件为 $\mathbf{T}$, 推出后件也为 $\mathbf{T}$.

Example 33. 求证: $\big((A \wedge B) \to C\big) \wedge \neg D \wedge (\neg C \vee D) \Rightarrow \neg A \vee \neg B$.

证: 设前件 $\big((A \wedge B) \to C\big) \wedge \neg D \wedge (\neg C \vee D)$ 为 $\mathbf{T}$. 则

$$\big((A \wedge B) \to C\big), \quad \neg D, \quad (\neg C \vee D)$$

均为 $\mathbf{T}$.

由 $\neg D$ 为 $\mathbf{T}$, 则 D 为 $\mathbf{F}$.

又 $\neg C \vee D$ 为 $\mathbf{T}$, 得 $\neg C$ 为 $\mathbf{T}$, 即 C 为 $\mathbf{F}$.

又 $\big((A \wedge B) \to C\big)$ 为 $\mathbf{T}$, 得 $A \wedge B$ 为 $\mathbf{F}$.

而 $\neg A \vee \neg B \Leftrightarrow \neg(A \wedge B)$, 所以 $\neg A \vee \neg B$ 为 $\mathbf{T}$. 得证. 8.54

方法 3. 假设后件为 $\mathbf{F}$, 推出前件也为 $\mathbf{F}$.

Example 34. 求证: $\big((A \wedge B) \to C\big) \wedge \neg D \wedge (\neg C \vee D) \Rightarrow \neg A \vee \neg B$.

证: 假设后件 $\neg A \vee \neg B$ 为 $\mathbf{F}$, 即 $\neg(A \wedge B)$ 为 $\mathbf{F}$, 亦即则 $A \wedge B$ 为 $\mathbf{T}$.

1. 如 C 为 $\mathbf{F}$, 则 $\big((A \wedge B) \to C\big)$ 为 $\mathbf{F}$, 所以前件 $\big((A \wedge B) \to C\big) \wedge \neg D \wedge (\neg C \vee D)$ 为 $\mathbf{F}$.
2. 如 C 为 $\mathbf{T}$, 则
   (a) 若 D 为 $\mathbf{T}$, 则 $\neg D$ 为 $\mathbf{F}$, 所以前件 $\big((A \wedge B) \to C\big) \wedge \neg D \wedge (\neg C \vee D)$ 为 $\mathbf{F}$.
   (b) 若 D 为 $\mathbf{F}$, 则 $\neg C \vee D$ 为 $\mathbf{F}$, 所以前件 $\big((A \wedge B) \to C\big) \wedge \neg D \wedge (\neg C \vee D)$ 为 $\mathbf{F}$.

   综上得证.

(或者先讨论 D 的真值, 也可以证明.) 8.55

常用逻辑蕴含式

$P \wedge Q \Rightarrow P$	1
$P \wedge Q \Rightarrow Q$	2
$P \Rightarrow P \vee Q$	3
$\neg P \Rightarrow P \to Q$	4
$Q \Rightarrow P \to Q$	5
$\neg(P \to Q) \Rightarrow P$	6
$\neg(P \to Q) \Rightarrow \neg Q$	7
$P \wedge (P \to Q) \Rightarrow Q$	8
$\neg Q \wedge (P \to Q) \Rightarrow \neg P$	9
$\neg P \wedge (P \vee Q) \Rightarrow Q$	10
$(P \to Q) \wedge (Q \to R) \Rightarrow P \to R$	11
$(P \vee Q) \wedge (P \to R) \wedge (Q \to R) \Rightarrow R$	12
$(P \to Q) \wedge (R \to S) \Rightarrow (P \wedge R) \to (Q \wedge S)$	13
$(P \leftrightarrow Q) \wedge (Q \leftrightarrow R) \Rightarrow P \leftrightarrow R$	14

8.56

Theorem 35. 设 P, Q 为任意两个命题公式, $P \Leftrightarrow Q$ 的充分必要条件是

$$P \Rightarrow Q \text{ 且 } Q \Rightarrow P.$$

证: 若 $P \Leftrightarrow Q$, 则 $P \leftrightarrow Q$ 为重言式. 因为

$$P \leftrightarrow Q \Leftrightarrow (P \to Q) \wedge (Q \to P),$$

故 $P \to Q$ 和 $Q \to P$ 皆为 **T**, 即

$$P \Rightarrow Q \text{ 且 } Q \Rightarrow P.$$

反之, 若 $P \Rightarrow Q$ 且 $Q \Rightarrow P$, 则 $P \to Q$ 和 $Q \to P$ 皆为 **T**, 从而 $P \leftrightarrow Q$ 为 **T**, 即 $P \leftrightarrow Q$ 为重言式, 亦即 $P \Leftrightarrow Q$. 8.57

蕴含式的性质

(1) 若 $A \Rightarrow B$ 且 A 是重言式, 则 B 必为重言式.

证: 因为 $A \to B$ 为永真式, 所以, 当 A 为永真时, B 必为永真 (否则与 $A \to B$ 为永真相矛盾).

(2) 若 $A \Rightarrow B$, $B \Rightarrow C$, 则 $A \Rightarrow C$.

证: 由 $A \Rightarrow B$, $B \Rightarrow C$, 则 $A \to B$, $B \to C$ 为永真式, 从而 $(A \to B) \wedge (B \to C)$ 亦为永真式.

由常用蕴含式 $(A \to B) \wedge (B \to C) \Rightarrow (A \to C)$, 及性质 (1), 得 $A \to C$ 是永真式, 亦即 $A \Rightarrow C$. 8.58

(3) 若 $A \Rightarrow B$ 且 $A \Rightarrow C$, 则 $A \Rightarrow B \wedge C$.

证: 设 A 的真值为 **T**, 由于 $A \Rightarrow B$, $A \Rightarrow C$, 则 B, C 为 **T**, 从而 $B \wedge C$ 为 **T**, 故 $A \to B \wedge C$ 为 **T**, 从而 $A \Rightarrow B \wedge C$.

(4) 若 $A \Rightarrow B$ 且 $C \Rightarrow B$, 则 $A \vee C \Rightarrow B$.

证: 因 $A \to B$ 和 $C \to B$ 为 **T**, 那么 $(A \to B) \wedge (C \to B)$ 为 **T**. 而

$$\begin{aligned}(A \to B) \wedge (C \to B) &\Leftrightarrow (\neg A \vee B) \wedge (\neg C \vee B) \\ &\Leftrightarrow (\neg A \wedge \neg C) \vee B \\ &\Leftrightarrow \neg(A \vee C) \vee B \\ &\Leftrightarrow (A \vee C) \to B.\end{aligned}$$

故 $A \vee C \to B$ 为永真, 从而 $A \vee C \Rightarrow B$. 8.59

证明 $\neg A \to (B \vee C)$, $D \vee E$, $(D \vee E) \to \neg A \Rightarrow B \vee C$.

证: 由 $D \vee E, (D \vee E) \to \neg A$ 均为 **T**, 用 I_8 得 $\neg A$ 为 **T**,
又由 $\neg A \to (B \vee C)$ 为 **T**, 得 $B \vee C$ 为 **T**.
得证 $\neg A \to (B \vee C)$, $D \vee E$, $(D \vee E) \to \neg A \Rightarrow B \vee C$.

反证: 设后件 $B \vee C$ 为 **F**.
又 $\neg A \to (B \vee C)$ 为 **T**, 得 $\neg A$ 为 **F**.
而 $(D \vee E) \to \neg A$ 为 **T**, 则 $D \vee E$ 为 **F**.
这与 $D \vee E$ 为 **T** 矛盾. 假设不成立. 得证. 8.60

2.4 全功能联结词集合

最小联结词组: $\{\neg, \vee\}$; $\{\neg, \wedge\}$;

由 "$\neg$", "$\wedge$", "$\vee$", "$\to$", "$\leftrightarrow$" 组成的命题公式, 必可以由仅包含 $\{\neg, \vee\}$ 或 $\{\neg, \wedge\}$ 的命题公式替代.

$\leftrightarrow$	$P \leftrightarrow Q \Leftrightarrow (P \to Q) \wedge (Q \to P)$
$\to$	$P \to Q \Leftrightarrow \neg P \vee Q$
$\vee$	$P \wedge Q \Leftrightarrow \neg(\neg P \vee \neg Q)$

8.61

3 范式及其应用

3.1 析取范式与合取范式

对偶式

Definition 36 (对偶式)**.** 设给定的命题公式 A 仅含联结词 $\neg, \wedge, \vee$. A^* 为将 A 中符号 $\wedge$, $\vee$, **T**, **F** 分别改换为 $\vee$, $\wedge$, **F**, **T** 后所得的公式. 那么称 A^* 为 A 的对偶式 (dual).

比如, $A = (\neg P \vee Q) \wedge R$ 的对偶式为

$$A^* = (\neg P \wedge Q) \vee R.$$

8.62

Theorem 37. 设公式 A 和 A^* 中仅含命题变元 $P_1, \cdots, P_n$, 及联结词 $\neg, \wedge, \vee$; 则

$$\neg A(P_1, P_2, \cdots, P_n) \Leftrightarrow A^*(\neg P_1, \neg P_2, \cdots, \neg P_n) \tag{3}$$

$$A(\neg P_1, \neg P_2, \cdots, \neg P_n) \Leftrightarrow \neg A^*(P_1, P_2, \cdots, P_n) \tag{4}$$

此定理是德 · 摩根律的推广.

比如设 $A(P, Q) = P \vee Q$, 则 $A^*(P, Q) \Leftrightarrow P \wedge Q$. 而

$$\neg A(P, Q) \Leftrightarrow \neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q, \tag{5}$$

$$A^*(\neg P, \neg Q) \Leftrightarrow \neg P \wedge \neg Q, \tag{6}$$

所以

$$\neg A(P, Q) \Leftrightarrow A^*(\neg P, \neg Q).$$

8.63

Theorem 38 (对偶原理)**.** 设 A^*, B^* 分别是命题公式 A, B 的对偶式. 如果 $A \Leftrightarrow B$, 则 $A^* \Leftrightarrow B^*$.

比如分配律:

$$\underbrace{P \vee (Q \wedge R)}_{A} \Leftrightarrow \underbrace{(P \vee Q) \wedge (P \vee R)}_{B}$$

$$\underbrace{P \wedge (Q \vee R)}_{A^*} \Leftrightarrow \underbrace{(P \wedge Q) \vee (P \wedge R)}_{B^*}$$

证: 设 $A(P_1, P_2, \cdots, P_n) \Leftrightarrow B(P_1, P_2, \cdots, P_n)$, 按等价定义可知

$$A(P_1, P_2, \cdots, P_n) \leftrightarrow B(P_1, P_2, \cdots, P_n) \tag{7}$$

是永真式. 那么

$$A(\neg P_1, \neg P_2, \cdots, \neg P_n) \leftrightarrow B(\neg P_1, \neg P_2, \cdots, \neg P_n) \tag{8}$$

也为永真式. 所以

$$A(\neg P_1, \neg P_2, \cdots, \neg P_n) \Leftrightarrow B(\neg P_1, \neg P_2, \cdots, \neg P_n). \tag{9}$$

根据前一定理中 (2) 式, 得

$$\neg A^*(P_1, P_2, \cdots, P_n) \Leftrightarrow \neg B^*(P_1, P_2, \cdots, P_n). \tag{10}$$

故 $A^* \Leftrightarrow B^*$. ($\neg A \Leftrightarrow \neg B$ 当且仅当 $A \Leftrightarrow B$.) □ 8.64

合取范式

Definition 39 (合取范式)**.** 一个命题公式称为合取范式 (conjunctive normal form), 当且仅当它具有形式:

$$A_1 \wedge A_2 \wedge \cdots \wedge A_n, \quad (n \geqslant 1) \tag{11}$$

其中 A_1, A_2, $\cdots$, A_n 都是由命题变元或其否定构成的析取式.

例如

$$(P \vee \neg Q \vee R) \wedge (\neg P \vee Q) \wedge \neg Q \tag{12}$$

是合取范式 (整体是合取式, 各部分是析取式.). 8.65

析取范式

Definition 40 (析取范式)**.** 一个命题公式称为析取范式 (conjunctive normal form), 当且仅当它具有形式:

$$A_1 \vee A_2 \vee \cdots \vee A_n, \quad (n \geqslant 1) \tag{13}$$

其中 $A_1, A_2, \cdots, A_n$ 都是由命题变元或其否定构成的合取式.

例如

$$\neg P \vee (P \wedge Q) \vee (P \wedge \neg Q \wedge R) \tag{14}$$

是析取范式 (整体是析取式, 各部分是合取式.). 8.66

Example 41. 求 $(P \to Q) \to P$ 的析取范式和合取范式.

解: 析取范式:

$$\begin{aligned} (P \to Q) \to P &\Leftrightarrow (\neg P \vee Q) \to P && (\text{去} \to) \\ &\Leftrightarrow \neg(\neg P \vee Q) \vee P \\ &\Leftrightarrow (P \wedge \neg Q) \vee P. \end{aligned}$$

合取范式:

$$\begin{aligned} (P \to Q) \to P &\Leftrightarrow (P \wedge \neg Q) \vee P \\ &\Leftrightarrow (P \vee P) \wedge (\neg Q \vee P) && (\text{分配律}) \\ &\Leftrightarrow P \wedge (\neg Q \vee P). \end{aligned}$$

8.67

求析取范式或合取范式的步骤:

1. 将命题公式中的联结词全部化为 $\neg, \wedge, \vee$;
2. 利用德 · 摩根律, 将否定符号 $\neg$ 直接移到各命题变元之前;
3. 利用分配律、结合律将命题公式化为析取范式或合取范式. 8.68

练习

求下列命题的析取范式和合取范式:

$$Q \wedge \big((P \vee \neg Q) \to R\big). \tag{15}$$

解: 求析取范式:

$$\begin{aligned} & Q \wedge \big((P \vee \neg Q) \to R\big) \\ \Leftrightarrow\ & Q \wedge (\neg(P \vee \neg Q) \vee R) && (\text{消去} \to) \\ \Leftrightarrow\ & Q \wedge \big((\neg P \wedge Q) \vee R\big) && (\text{内移} \neg) \\ \Leftrightarrow\ & \big(Q \wedge (\neg P \wedge Q)\big) \vee (Q \wedge R) && (\text{分配律}) \\ \Leftrightarrow\ & (\neg P \wedge Q) \vee (Q \wedge R). \end{aligned}$$

解: 求合取范式:

$$
\begin{aligned}
& Q \wedge \big((P \vee \neg Q) \to R\big) \\
\Leftrightarrow\ & Q \wedge \big((\neg P \wedge Q) \vee R\big) && (\text{消去 } \to) \\
\Leftrightarrow\ & Q \wedge \big((\neg P \vee R) \wedge (Q \vee R)\big) && (\text{分配律}) \\
\Leftrightarrow\ & Q \wedge (\neg P \vee R) \wedge (Q \vee R).
\end{aligned}
$$

8.69

3.2 主范式

为什么要讨论 “主范式”?

下面将讨论 “主范式”(主析取范式, 主合取范式), 这是因为一个命题的析取范式或合取范式并不是惟一的.

例如 $P \vee (Q \wedge R)$ 是一个析取范式, 但它也可以写成

$$P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R).$$

主范式的研究, 使得命题公式可以转化为一个标准形式, 从而易于判断命题公式的性质特征.

在引入主范式的讨论时, 还要涉及小项、大项的概念. 8.70

布尔合取 *or* 小项

Definition 42. n 个命题变元 $P_1, P_2, \cdots, P_n$ 的合取式, 称作布尔合取或小项, 在任一小项中

(i) 每个变元 P_i 与它的否定 $\neg P_i$ 不能同时出现,

(ii) 但 P_i 与 $\neg P_i$ 必须出现且仅出现一次.

Example 43. 例如, 两个变元 P 和 Q 的所有小项为:

$$P \wedge Q,\ P \wedge \neg Q,\ \neg P \wedge Q,\ \neg P \wedge \neg Q.$$

一般地, n 个命题变元共有 2^n 个小项.

Example 44. n 个变元 $P_1, P_2, \cdots, P_n$ 的小项形如:

$$\underbrace{(\quad) \wedge (\quad) \wedge \cdots \wedge (\quad)}_{n},$$

其中的第 i 个括号内, 只能填上 P_i 和 $\neg P_i$ 之中的一个, 所有不同的填法共有 2^n 个.

所以, n 个命题变元共有 2^n 个小项. 8.71

小项的真值

P	Q	$P \wedge Q$	$P \wedge \neg Q$	$\neg P \wedge Q$	$\neg P \wedge \neg Q$
T	**T**	**T**	**F**	**F**	**F**
T	**F**	**F**	**T**	**F**	**F**
F	**T**	**F**	**F**	**T**	**F**
F	**F**	**F**	**F**	**F**	**T**

- 没有两个小项是等价的;
- 每个小项都只有一个真值为 **T**. (这是合取式本身的特点.) 8.72

P	0	0	0	0	1	1	1	1	
Q	0	0	1	1	0	0	1	1	
R	0	1	0	1	0	1	0	1	
$\neg P \wedge \neg Q \wedge \neg R$	1	0	0	0	0	0	0	0	$m_{000} = \neg P \wedge \neg Q \wedge \neg R$
$\neg P \wedge \neg Q \wedge R$	0	1	0	0	0	0	0	0	$m_{001} = \neg P \wedge \neg Q \wedge R$
$\neg P \wedge Q \wedge \neg R$	0	0	1	0	0	0	0	0	$m_{010} = \neg P \wedge Q \wedge \neg R$
$\neg P \wedge Q \wedge R$	0	0	0	1	0	0	0	0	$m_{011} = \neg P \wedge Q \wedge R$
$P \wedge \neg Q \wedge \neg R$	0	0	0	0	1	0	0	0	$m_{100} = P \wedge \neg Q \wedge \neg R$
$P \wedge \neg Q \wedge R$	0	0	0	0	0	1	0	0	$m_{101} = P \wedge \neg Q \wedge R$
$P \wedge Q \wedge \neg R$	0	0	0	0	0	0	1	0	$m_{110} = P \wedge Q \wedge \neg R$
$P \wedge Q \wedge R$	0	0	0	0	0	0	0	1	$m_{111} = P \wedge Q \wedge R$

小项 & 编码: 小项真值为 1 时, 对应的一组真值指派.

- 表中的 0, 1 分别代表真值 **F**, **T**.
- 二进制编码也可以转为十进制, 如 $m_{001} \triangleq m_1$, $m_{010} \triangleq m_2$, $m_{011} \triangleq m_3$.

8.73

小项的性质

1. 当真值指派与编码相同时[3], 小项真值为 **T**, 在其余均为 **F**. 例如:
$$m_{001} = \neg P \wedge \neg Q \wedge R,$$
$$m_{010} = \neg P \wedge Q \wedge \neg R.$$
2. 任意两个不同小项的合取式为永假[4]2-> 任意两个不同小项中至少出现一对 P_i, $\neg P_i$..
3. 全体小项的析取式为永真[5]3-> 对任意一组真值指派, 都有 (且仅有) 一个小项真值为 **T**., 记为:
$$\sum_{i=0}^{2^n-1} m_i = m_0 \vee m_1 \vee \cdots \vee m_{2^n-1} \Leftrightarrow \mathbf{T}$$

8.74

主析取范式

Definition 45. 对于给定的命题公式 A, 如果存在公式 A' 满足

1) $A' \Leftrightarrow A$;

2) A' 仅由小项的析取所组成.

则称 A' 为 A 的主析取范式 (major disjunctive normal form).

- 例如
$$P \to Q \Leftrightarrow (P \wedge Q) \vee (\neg P \wedge Q) \vee (\neg P \wedge \neg Q),$$
这里 $(P \wedge Q) \vee (\neg P \wedge Q) \vee (\neg P \wedge \neg Q)$ 就是 $P \to Q$ 的主析取范式.

8.75

[3] 真值 **T** 和 **F** 分别记为 1 和 0.

[4] <

[5] <

主析取范式

Theorem 46. 在真值表中，一个公式的真值为 **T** 的指派所对应的小项的析取，即为此公式的主析取范式.

Example 47.

P	Q	$P\wedge Q$	$P\wedge\neg Q$	$\neg P\wedge Q$	$\neg P\wedge\neg Q$	$P\to Q$
T	**T**	**T**	**F**	**F**	**F**	**T**
T	**F**	**F**	**T**	**F**	**F**	**F**
F	**T**	**F**	**F**	**T**	**F**	**T**
F	**F**	**F**	**F**	**F**	**T**	**T**

$$P\to Q\Leftrightarrow(P\wedge Q)\vee(\neg P\wedge Q)\vee(\neg P\wedge\neg Q).$$

证: 记 B 为 "公式 A 真值为 **T** 的指派所对应的小项的析取", 下证 $A\Leftrightarrow B$:

- 若 A 在某一指派下, 真值为 **T**, 则必有 B 中的某个小项真值为 **T**, 所以此时 B 真值为 **T**.
- 对 A 为 **F** 的某一指派, 其对应的小项不包含在 B 中, 故此时 B 真值为 **F**. 8.76

☞ 实际使用真值表求主析取范式时, 并不需要列出所有的小项.

如使用下表可求得 $P\to Q\Leftrightarrow(P\wedge Q)\vee(\neg P\wedge Q)\vee(\neg P\wedge\neg Q)$.

P	Q	$P\wedge Q$	$P\wedge\neg Q$	$\neg P\wedge Q$	$\neg P\wedge\neg Q$	$P\to Q$
T	**T**	**T**	**F**	**F**	**F**	**T**
T	**F**	**F**	**T**	**F**	**F**	**F**
F	**T**	**F**	**F**	**T**	**F**	**T**
F	**F**	**F**	**F**	**F**	**T**	**T**

也可以简化为:

P	Q	$P\to Q$	
T	**T**	**T**	➠ $P\wedge Q$
T	**F**	**F**	
F	**T**	**T**	➠ $\neg P\wedge Q$
F	**F**	**T**	➠ $\neg P\wedge\neg Q$

8.77

Example 48. 求 $P\vee Q$, $\neg(P\wedge Q)$ 的主析取范式. 解: 由真值表

P	Q	$P\vee Q$	$\neg(P\wedge Q)$
T	**T**	**T**	**F**
T	**F**	**T**	**T**
F	**T**	**T**	**T**
F	**F**	**F**	**T**

得

$$P \vee Q \Leftrightarrow (P \wedge Q) \vee (P \wedge \neg Q) \vee (\neg P \wedge Q),$$
$$\neg(P \wedge Q) \Leftrightarrow (P \wedge \neg Q) \vee (\neg P \wedge Q) \vee (\neg P \wedge \neg Q).$$

return 8.78

Example 49. 设公式 A 的真值如下表所示, 求 A 的主析取范式.

P	Q	R	A
T	**T**	**T**	**T**
T	**T**	**F**	**F**
T	**F**	**T**	**F**
T	**F**	**F**	**T**
F	**T**	**T**	**F**
F	**T**	**F**	**F**
F	**F**	**T**	**F**
F	**F**	**F**	**T**

解: 公式 A 的主析取范式为

$$A \Leftrightarrow (P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge \neg R)$$

☞ 注意这也是研究主范式的一个用途: 已知公式为真和为假的赋值, 写出该公式的表达式. 8.79

用等价公式构成主析取范式

Example 50. 求 $(P \wedge Q) \vee (\neg P \wedge R) \vee (Q \wedge R)$ 的主析取范式.

解:

$$
\begin{aligned}
& (P \wedge Q) \vee (\neg P \wedge R) \vee (Q \wedge R) \\
\Leftrightarrow\ & \big(P \wedge Q \wedge (R \vee \neg R)\big) \vee \big(\neg P \wedge R \wedge (Q \vee \neg Q)\big) \vee \big(Q \wedge R \wedge (P \vee \neg P)\big) \\
\Leftrightarrow\ & (P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (\neg P \wedge R \wedge Q) \vee (\neg P \wedge R \wedge \neg Q).
\end{aligned}
$$

8.80

求 $P \to \big((P \to Q) \wedge \neg(\neg Q \vee \neg P)\big)$ 的主析取范式.

解:

$$
\begin{aligned}
& P \to \big((P \to Q) \wedge \neg(\neg Q \vee \neg P)\big) \\
\Leftrightarrow\ & \neg P \vee \big((\neg P \vee Q) \wedge (Q \wedge P)\big) && (去 \to) \\
\Leftrightarrow\ & \neg P \vee \big((\neg P \wedge Q \wedge P) \vee (Q \wedge Q \wedge P)\big) && (分配律) \\
\Leftrightarrow\ & \neg P \vee (\neg P \wedge P \wedge Q) \vee (Q \wedge P) \\
\Leftrightarrow\ & \neg P \vee (\mathbf{F} \wedge Q) \vee (P \wedge Q) && (否定律) \\
\Leftrightarrow\ & \neg P \vee \mathbf{F} \vee (P \wedge Q) && (零律) \\
\Leftrightarrow\ & \neg P \vee (P \wedge Q) && (同一律) \\
\Leftrightarrow\ & \big(\neg P \wedge (Q \vee \neg Q)\big) \vee (P \wedge Q) && (添加项) \\
\Leftrightarrow\ & (\neg P \wedge Q) \vee (\neg P \wedge \neg Q) \vee (P \wedge Q).
\end{aligned}
$$

8.81

求 $P \to \big((P \to Q) \wedge \neg(\neg Q \vee \neg P)\big)$ 的主析取范式.

另解:
$$
\begin{aligned}
& P \to \big((P \to Q) \wedge \neg(\neg Q \vee \neg P)\big) \\
\Leftrightarrow\ & \neg P \vee ((\neg P \vee Q) \wedge (Q \wedge P)) && (\text{去} \to) \\
\Leftrightarrow\ & \big(\neg P \vee (\neg P \vee Q)\big) \wedge \big(\neg P \vee (Q \wedge P)\big) && (\text{分配律}) \\
\Leftrightarrow\ & (\neg P \vee \neg P \vee Q) \wedge \big((\neg P \vee Q) \wedge (\neg P \vee P)\big) \\
\Leftrightarrow\ & \neg P \vee Q \\
\Leftrightarrow\ & \big(\neg P \wedge (Q \vee \neg Q)\big) \vee ((P \vee \neg P) \wedge Q) && (\text{添加项}) \\
\Leftrightarrow\ & (\neg P \wedge Q) \vee (\neg P \wedge \neg Q) \vee (\neg P \wedge Q) \vee (P \wedge Q) \\
\Leftrightarrow\ & (\neg P \wedge Q) \vee (\neg P \wedge \neg Q) \vee (P \wedge Q)\,.
\end{aligned}
$$

☞ 重要的步骤在于: 去 $\to$, 添加项. 8.82

利用等价公式求主析取范式的步骤:

1. 化归为析取范式 (总的方向);
2. 除去析取范式中所有永假的析取式 (同一律);
3. 将析取式中重复出现的合取项和相同的变元合并 (幂等律);
4. 对合取项补入没有出现的命题变元 (如添加 $(P \vee \neg P)$ 式), 再用分配律展开. 8.83

布尔析取 *or* 大项

Definition 51. n 个命题变元 $P_1, P_2, \cdots, P_n$ 的析取式, 称作布尔析取或大项, 其中

(i) 每个变元 P_i 与它的否定 $\neg P_i$ 不能同时出现,

(ii) 但 P_i 与 $\neg P_i$ 必须出现, 且仅出现一次.

Example 52. <2> 例如, 两个变元 P 和 Q 的大项为:

$$P \vee Q,\ P \vee \neg Q,\ \neg P \vee Q,\ \neg P \vee \neg Q.$$

一般地, n 个命题变元共有 2^n 个大项. 8.84

大项 & 编码

- 表...编...的 0, 使得该大项真值为 **F**, ...0 的一组指派.
- 二进制编码也可以转为十进制, 如 $M_{000} \triangleq M_0$, $M_{101} \triangleq M_5$, $M_{111} \triangleq M_7$. 8.85

大项的性质

(i) 当真值指派与编码相同时[6], 大项真值为 **F**, 在其余均为 **T**. 例如:

$$M_{001} = P \vee Q \vee \neg R, \tag{16}$$

$$M_{010} = P \vee \neg Q \vee R. \tag{17}$$

[6] 真值 **T** 和 **F** 分别记为 1 和 0.

P	0	0	0	0	1	1	1	1	
Q	0	0	1	1	0	0	1	1	
R	0	1	0	1	0	1	0	1	
$P\vee Q\vee R$	0	1	1	1	1	1	1	1	$M_{000}=P\vee Q\vee R$
$P\vee Q\vee\neg R$	1	0	1	1	1	1	1	1	$M_{001}=P\vee Q\vee\neg R$
$P\vee\neg Q\vee R$	1	1	0	1	1	1	1	1	$M_{010}=P\vee\neg Q\vee R$
$P\vee\neg Q\vee\neg R$	1	1	1	0	1	1	1	1	$M_{011}=P\vee\neg Q\vee\neg R$
$\neg P\vee Q\vee R$	1	1	1	1	0	1	1	1	$M_{100}=\neg P\vee Q\vee R$
$\neg P\vee Q\vee\neg R$	1	1	1	1	1	0	1	1	$M_{101}=\neg P\vee Q\vee\neg R$
$\neg P\vee\neg Q\vee R$	1	1	1	1	1	1	0	1	$M_{110}=\neg P\vee\neg Q\vee R$
$\neg P\vee\neg Q\vee\neg R$	1	1	1	1	1	1	1	0	$M_{111}=\neg P\vee\neg Q\vee\neg R$

(ii) 任意两个不同大项的析取式为永真[7].

(iii) 全体大项的合取式为永假, 记为:

$$\prod_{i=0}^{2^n-1} M_i = M_0\wedge M_1\wedge\cdots\wedge M_{2^n-1}\Leftrightarrow \mathbf{F}$$

8.86

主合取范式

Definition 53 (主合取范式)**.** 对于给定的命题公式 A, 如果存在公式 A' 满足

1) $A'\Leftrightarrow A$;
2) A' 仅由大项的合取所组成.

则称 A' 为 A 的主合取范式 (major conjunctive normal form).

8.87

主合取范式

Theorem 54. 在真值表中, 一个公式的真值为 **F** 的指派所对应的大项的合取, 即为此公式的主合取范式.

Example 55.

P	Q	$P\vee Q$	$P\vee\neg Q$	$\neg P\vee Q$	$\neg P\vee\neg Q$	$P\leftrightarrow Q$
T	**T**	**T**	**T**	**T**	**F**	**T**
T	**F**	**T**	**T**	**F**	**T**	**F**
F	**T**	**T**	**F**	**T**	**T**	**F**
F	**F**	**F**	**T**	**T**	**T**	**T**

$$P\leftrightarrow Q\Leftrightarrow(\neg P\vee Q)\wedge(P\vee\neg Q).$$

8.88

利用真值表求 $(P\wedge Q)\vee(\neg P\wedge R)$ 的主析取范式与主合取范式.

解

[7] 对任意一组真值指派, 有且仅有一个大项真值为 **F**.

P	Q	R	$(P \wedge Q) \vee (\neg P \wedge R)$
T	**T**	**T**	**T**
T	**T**	**F**	**T**
T	**F**	**T**	**F**
T	**F**	**F**	**F**
F	**T**	**T**	**T**
F	**T**	**F**	**F**
F	**F**	**T**	**T**
F	**F**	**F**	**F**

主析取范式: $(P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (\neg P \wedge Q \wedge R) \vee (\neg P \wedge \neg Q \wedge R)$ $= m_{111} \vee m_{110} \vee m_{011} \vee m_{001} \triangleq m_7 \vee m_6 \vee m_3 \vee m_1 \triangleq \sum_{1,3,6,7}$.[1ex] 主合取范式: $(\neg P \vee Q \vee \neg R) \wedge (\neg P \vee Q \vee R) \wedge (P \vee \neg Q \vee R) \wedge (P \vee Q \vee R)$ $= M_{101} \wedge M_{100} \wedge M_{010} \wedge M_{000} \triangleq M_5 \wedge M_4 \wedge M_2 \wedge M_0 \triangleq \prod_{0,2,4,5}$.

☞ 主析取范式与主合取范式的简记式中的下标是“互补”的. *Why?* 8.89

为什么编码是“互补”的?

命题公式的真值只有 **T** 和 **F**. 与 **T** 对应的真值指派做了小项的编码, 剩下的是 **F** 对应的真值指派, 作为大项的编码, 这两部分是“互补”的. (合起来就是全部的真值指派.)

$(P \wedge Q) \vee (\neg P \wedge R) \Leftrightarrow \sum_{1,3,6,7} \Leftrightarrow \prod_{0,2,4,5}$.

P	Q	R	$(P \wedge Q) \vee (\neg P \wedge R)$		
T	**T**	**T**	**T**	$(P \wedge Q \wedge R)$	$m_{111} = m_7$
T	**T**	**F**	**T**	$(P \wedge Q \wedge \neg R)$	$m_{110} = m_6$
T	**F**	**T**	**F**	$(\neg P \vee Q \vee \neg R)$	$M_{101} = M_5$
T	**F**	**F**	**F**	$(\neg P \vee Q \vee R)$	$M_{100} = M_4$
F	**T**	**T**	**T**	$(\neg P \wedge Q \wedge R)$	$m_{011} = m_3$
F	**T**	**F**	**F**	$(P \vee \neg Q \vee R)$	$M_{010} = M_2$
F	**F**	**T**	**T**	$(\neg P \wedge \neg Q \wedge R)$	$m_{001} = m_1$
F	**F**	**F**	**F**	$(P \vee Q \vee R)$	$M_{000} = M_0$

☞ 发现规律了没有? 由真值表, 如果只需要写出主析取范式或主合取范式的简记式, 那就太简单了! 8.90

知道主析取范式, 直接写出主合取范式?

如果已经得到了主析取范式, 可以直接写出主合取范式: 对主析取范式中没有出现的小项组合, 将 $\wedge$ 换为 $\vee$, P_i 换为 $\neg P_i$, 而 $\neg P_j$ 换为 P_j, 即得到构成主合取范式的所有大项.

$(P \wedge Q) \vee (\neg P \wedge R) \Leftrightarrow \sum_{1,3,6,7} \Leftrightarrow \prod_{0,2,4,5}$.

P	Q	R	$(P\wedge Q)\vee(\neg P\wedge R)$	小项与大项	没有出现的小项
T	**T**	**T**	**T**	$(P\wedge Q\wedge R)$	
T	**T**	**F**	**T**	$(P\wedge Q\wedge \neg R)$	
T	**F**	**T**	**F**	$(\neg P\vee Q\vee \neg R)$	$P\wedge\neg Q\wedge R$
T	**F**	**F**	**F**	$(\neg P\vee Q\vee R)$	$P\wedge\neg Q\wedge\neg R$
F	**T**	**T**	**T**	$(\neg P\wedge Q\wedge R)$	
F	**T**	**F**	**F**	$(P\vee\neg Q\vee R)$	$\neg P\wedge Q\wedge\neg R$
F	**F**	**T**	**T**	$(\neg P\wedge\neg Q\wedge R)$	
F	**F**	**F**	**F**	$(P\vee Q\vee R)$	$\neg P\wedge\neg Q\wedge\neg R$

理论支持? $\neg A(P_1,P_2,\cdots,P_n)\Leftrightarrow A^*(\neg P_1,\neg P_2,\cdots,\neg P_n)$. 怎么理解? 8.91

验证 $\neg A(P_1,P_2,\cdots,P_n)\Leftrightarrow A^*(\neg P_1,\neg P_2,\cdots,\neg P_n)$.

记 $(P\wedge Q)\vee(\neg P\wedge R)$ 为 $A(P,Q,R)$.

P	Q	R	$A(P,Q,R)$	小项与大项	A 中没有出现的小项	$\neg A(P,Q,R)$
T	**T**	**T**	**T**	$(P\wedge Q\wedge R)$		**F**
T	**T**	**F**	**T**	$(P\wedge Q\wedge \neg R)$		**F**
T	**F**	**T**	**F**	$(\neg P\vee Q\vee \neg R)$	$P\wedge\neg Q\wedge R$	**T**
T	**F**	**F**	**F**	$(\neg P\vee Q\vee R)$	$P\wedge\neg Q\wedge\neg R$	**T**
F	**T**	**T**	**T**	$(\neg P\wedge Q\wedge R)$		**F**
F	**T**	**F**	**F**	$(P\vee\neg Q\vee R)$	$\neg P\wedge Q\wedge\neg R$	**T**
F	**F**	**T**	**T**	$(\neg P\wedge\neg Q\wedge R)$		**F**
F	**F**	**F**	**F**	$(P\vee Q\vee R)$	$\neg P\wedge\neg Q\wedge\neg R$	**T**

可见 A 中没有出现的小项, 构成 $\neg A(P,Q,R)$ 的小项.

$$\begin{aligned}
A(P,Q,R)&\Leftrightarrow(P\wedge Q\wedge R)\vee(P\wedge Q\wedge\neg R)\vee(\neg P\wedge Q\wedge R)\vee(\neg P\wedge\neg Q\wedge R)\,,\\
\neg A(P,Q,R)&\Leftrightarrow(P\wedge\neg Q\wedge R)\vee(P\wedge\neg Q\wedge\neg R)\vee(\neg P\wedge Q\wedge\neg R)\vee(\neg P\wedge\neg Q\wedge\neg R)\,,\\
A^*(P,Q,R)&\Leftrightarrow(P\vee Q\vee R)\wedge(P\vee Q\vee\neg R)\wedge(\neg P\vee Q\vee R)\wedge(\neg P\vee\neg Q\vee R)\,,\\
A^*(\neg P,\neg Q,\neg R)&\Leftrightarrow(\neg P\vee\neg Q\vee\neg R)\wedge(\neg P\vee\neg Q\vee R)\wedge(P\vee\neg Q\vee\neg R)\wedge(P\vee Q\vee\neg R)\,.
\end{aligned}$$

8.92

Example 56. 求 $(P\to Q)\wedge Q$ 的主析取范式与主合取范式.

解: 主析取范式为:

$$\begin{aligned}
&(P\to Q)\wedge Q\\
\Leftrightarrow&(\neg P\vee Q)\wedge Q\\
\Leftrightarrow&(\neg P\wedge Q)\vee(Q\wedge Q)\\
\Leftrightarrow&(\neg P\wedge Q)\vee(Q\wedge(P\vee\neg P))\\
\Leftrightarrow&(\neg P\wedge Q)\vee(Q\wedge P)\vee(Q\wedge\neg P)\\
\Leftrightarrow&(\neg P\wedge Q)\vee(P\wedge Q)\\
\Leftrightarrow&m_{01}\vee m_{11}=\sum\nolimits_{1,3}.
\end{aligned}$$

主合取范式为:

$$\begin{aligned}
&(P\to Q)\wedge Q\\
\Leftrightarrow&(\neg P\vee Q)\wedge Q\\
\Leftrightarrow&(\neg P\vee Q)\wedge((P\wedge\neg P)\vee Q)\\
\Leftrightarrow&(P\vee Q)\wedge(\neg P\vee Q)\\
\Leftrightarrow&M_{00}\wedge M_{10}\\
=&\prod\nolimits_{0,2}.
\end{aligned}$$

由于主析取范式与主合取范式的简记式中的下标是“互补”的, 因此也可由其中一个直接求另一个. 8.93

练习

利用编码的互补性, 求 $P \leftrightarrow Q$ 的主析取范式与主合取范式.

解:

$$\begin{aligned} P \leftrightarrow Q &\Leftrightarrow (P \to Q) \wedge (Q \to P) \\ &\Leftrightarrow (\neg P \vee Q) \wedge (\neg Q \vee P) \\ &\Leftrightarrow (\neg P \vee Q) \wedge (P \vee \neg Q) && \text{(主合取范式)} \\ &= M_{10} \wedge M_{01} \\ &= \prod\nolimits_{1,2} \\ &\Leftrightarrow \sum\nolimits_{0,3} \\ &= m_{00} \vee m_{11} \\ &= (\neg P \wedge \neg Q) \vee (P \wedge Q). && \text{(主析取范式)} \end{aligned}$$

8.94

3.3 范式的应用

范式的应用

(1) 判定二命题公式是否等值. $P \Leftrightarrow Q$ 当且仅当 P 与 Q 有相同的主析 (合) 取范式.

(2) 判定命题公式的类型. 设 P 是含有 n 个变元的命题公式:

  (a) P 为重言式, 当且仅当 P 的主析取范式中含有 2^n 个小项.

  (b) P 为永假式, 当且仅当 P 的主合取范式中含有 2^n 个大项.

(3) 求命题公式的成真和成假赋值.

8.95

用将合式公式化为范式的方法证明下列两式是等价的:

$$(A \to B) \wedge (A \to C), \quad A \to (B \wedge C).$$

解: 由

$$\begin{aligned} (A \to B) \wedge (A \to C) &\Leftrightarrow (\neg A \vee B) \wedge (\neg A \vee C), \\ A \to (B \wedge C) &\Leftrightarrow \neg A \vee (B \wedge C) \\ &\Leftrightarrow (\neg A \vee B) \wedge (\neg A \vee C), \end{aligned}$$

得

$$(A \to B) \wedge (A \to C) \Leftrightarrow A \to (B \wedge C).$$

8.96

求下列各式的主析取范式及主合取范式, 并指出哪些是重言式.

(a) $(\neg P \vee \neg Q) \to (P \leftrightarrow \neg Q)$;

解: (a)

$$\begin{aligned}
& (\neg P \vee \neg Q) \to (P \leftrightarrow \neg Q) \\
\Leftrightarrow\ & \neg(\neg P \vee \neg Q) \vee (P \leftrightarrow \neg Q) \\
\Leftrightarrow\ & (P \wedge Q) \vee \overbrace{(P \wedge \neg Q) \vee (\neg P \wedge Q)}^{8} && \text{(主析取范式)} \\
=\ & \sum\nolimits_{1,2,3} \\
\Leftrightarrow\ & \prod\nolimits_{0} \\
=\ & P \vee Q.^{9} && \text{(主合取范式 (只含一个大项!))}
\end{aligned}$$

8.97

求下列各式的主析取范式及主合取范式, 并指出哪些是重言式.

(e) $P \to \big(P \wedge (Q \to P)\big)$.

解: (e)

$$\begin{aligned}
& P \to \big(P \wedge (Q \to P)\big) \\
\Leftrightarrow\ & \neg P \vee \big(P \wedge (\neg Q \vee P)\big) \\
\Leftrightarrow\ & (\neg P \vee P) \wedge (\neg P \vee (\neg Q \vee P)) \\
\Leftrightarrow\ & \mathbf{T} \wedge (\mathbf{T} \vee \neg Q) \\
\Leftrightarrow\ & \mathbf{T} && \text{(重言式)} \\
\Leftrightarrow\ & \sum\nolimits_{0,1,2,3} \\
=\ & (P \wedge Q) \vee (P \wedge \neg Q) \vee (\neg P \wedge Q) \vee (\neg P \wedge \neg Q) && \text{(主析取范式)}
\end{aligned}$$

可见 $P \to \big(P \wedge (Q \to P)\big)$ 是重言式. (没有主合取范式.)

8.98

Example 57. A, B, C, D 四个人中要派两个人出差, 按下述三个条件有几种派法? 如何派?

1. 若 A 去则 C 和 D 中要去一人;
2. B 和 C 不能都去;
3. C 去则 D 要留下.

[1]注意到 $P \leftrightarrow Q \Leftrightarrow (P \wedge Q) \vee (\neg P \wedge \neg Q)$.

[2]前面有例子证明过 $P \vee Q \Leftrightarrow (P \wedge Q) \vee (P \wedge \neg Q) \vee (\neg P \wedge Q)$. 见前例.

解: 设 A: A 派出. 其他类似设定. 则派出的三个条件为

$$A \to (C \bar{\vee} D), \quad \neg(B \wedge C), \quad C \to \neg D.$$

往下求使命题

$$\big(A \to (C \bar{\vee} D)\big) \wedge \big(\neg(B \wedge C)\big) \wedge (C \to \neg D) \tag{18}$$

为 **T** 的真值指派.

可以通过主析取范式求解, 也可以借助真值表求解. (见下一页) 8.99

注意到 "四个人中要派两个人", 所以真值表中只列出真值指派有 2 个为真的情形:

A	B	C	D	$\big(A \to (C \bar{\vee} D)\big) \wedge \big(\neg(B \wedge C)\big) \wedge (C \to \neg D)$
1	1	0	0	0
1	0	1	0	1
1	0	0	1	1
0	1	1	0	0
0	1	0	1	1
0	0	1	1	0

注意到表中公式真值为 1 所对应的真值指派, 得派出方式有三种:

$$A \wedge C, \qquad A \wedge D, \qquad B \wedge D.$$

8.100

4 命题演算的推理理论

有效结论

在逻辑学中把从所谓前提的一些命题出发, 依据公认的推理规则, 推导出所谓结论的一个命题的过程称为有效推理或形式证明, 所得结论叫做有效结论.

Definition 58 (有效结论)**.** 设 A 和 C 是两个命题公式. 当且仅当

$$A \to C \text{ 为一重言式, 即 } A \Rightarrow C,$$

称 "C 是 A 的有效结论". 或 "C 可由 A 逻辑地推出".

注意: 不是正确结论. 比如

如果猪会飞, 那么太阳从西边出来.

是重言式. 而命题 "太阳从西边出来" 的真值为 **F**. 8.101

Definition 59 (推广到有 n 个前提的情形)**.** 设 $H_1, H_2, \cdots, H_n$ 和 C 是命题公式, 当且仅当

$$H_1 \wedge H_2 \wedge \cdots \wedge H_n \Rightarrow C$$

称 C 是 "一组前提 $H_1, H_2, \cdots, H_n$ 的有效结论".

注

- 在形式证明中重要的是推理的有效性, 而不在于结论是否真实;
- 所谓 "推理有效" 是指, 结论是前提的合乎逻辑的结果.

8.102

论证方法

判别有效结论的过程就是论证过程. 论证方法有

1. 真值表法;
2. 直接证法;
3. 间接证法:
   - 反证法;
   - CP 规则.

8.103

真值表法

要证明 $H_1 \wedge H_2 \wedge \cdots \wedge H_m \Rightarrow C$ 是否成立, 使用真值表有两个方法:

1. 对于每一个 $H_1, H_2, \cdots, H_m$ 真值均为 **T** 的行, C 也有真值 **T**. (前件为真, 后件也为真.)
2. 对于每一个 C 的真值为 **F** 的行, $H_1, H_2, \cdots, H_m$ 的真值中至少有一个为 **F**. (后件为假, 前件也为假.)

8.104

Example 60. 一份统计表格的错误或者是由于材料不可靠, 或者是由于计算有错误; 这份统计表格的错误不是由于材料不可靠, 所以这份统计表格是由于计算有错误.

解: 设 P: 统计表格的错误是由于材料不可靠; Q: 统计表格的错误是由于计算有错误. 则有

$$\neg P \wedge (P \vee Q) \Rightarrow Q.$$

P	Q	$\neg P$	$P \vee Q$	$\neg P \wedge (P \vee Q)$
T	**T**	**F**	**T**	**F**
T	**F**	**F**	**T**	**F**
F	**T**	**T**	**T**	**T**
F	**F**	**T**	**F**	**F**

从真值表看到: 当 $\neg P$ 和 $P \vee Q$ 的真值都为 **T** 时 (在第三行), Q 也为 **T**. 所以 $\neg P \wedge (P \vee Q) \Rightarrow Q$.

或者由: 当 Q 的真值为 **F** 时, $\neg P$ 和 $P \vee Q$ 的至少有一个为 **F**.

☞本题证明的是一个常用蕴含式, 本质上就是我们常用的排除法. 8.105

Example 61. 如果张老师来了, 这个问题可以得到解答; 如果李老师来了, 这个问题也可以得到解答. 总之张老师或李老师来了, 这个问题就可以得到解答.

解: 设 P: 张老师来了; Q: 李老师来了; R: 这个问题可以得到解答. 则有

$$(P \to R) \wedge (Q \to R) \wedge (P \vee Q) \Rightarrow R.$$

P	Q	R	$P \to R$	$Q \to R$	$P \vee Q$
T	**T**	**T**	**T**	**T**	**T**
T	**T**	**F**	**F**	**F**	**T**
T	**F**	**T**	**T**	**T**	**T**
T	**F**	**F**	**F**	**T**	**T**
F	**T**	**T**	**T**	**T**	**T**
F	**T**	**F**	**T**	**F**	**T**
F	**F**	**T**	**T**	**T**	**F**
F	**F**	**F**	**T**	**F**	**F**

从真值表看到: 当 $P \to R$, $Q \to R$ 和 $P \vee Q$ 的真值都为 **T** 时 (在第一、三、五行), R 也为 **T**. 所以 $(P \to R) \wedge (Q \to R) \wedge (P \vee Q) \Rightarrow R$. (☞ 二段推论) 8.106

直接证明法

直接证明法就是由一组前提, 利用一些公认的推理规则, 根据已知的等价公式或蕴含公式, 推演得到有效的结论.

- P 规则 (前提引入): 前提在推导过程中的任何时候都可以引入.
- T 规则 (结论引用): 在推导中, 如果有一个或多个公式重言蕴涵着公式 S (结论), 则公式 S 可以引入推导之中.

常用的蕴含公式和等价公式, 是推理证明的基础. 8.107

常用蕴含式

1. $P \wedge Q \Rightarrow P$ 若 $P \wedge Q$ 为真, 则 P 为真.
2. $P \wedge Q \Rightarrow Q$
3. $P \Rightarrow P \vee Q$
4. $Q \Rightarrow P \vee Q$
5. $\neg P \Rightarrow P \to Q$ 若 $\neg P$ 为真, 即 P 为假, 则 $P \to Q$ 为真.
6. $Q \Rightarrow P \to Q$

8.108

常用蕴含式

7. $\neg(P \to Q) \Rightarrow P$
8. $\neg(P \to Q) \Rightarrow \neg Q$
9. $P, Q \Rightarrow P \wedge Q$
10. $\neg P, P \vee Q \Rightarrow Q$
11. $P, P \to Q \Rightarrow Q$
12. $\neg Q, P \to Q \Rightarrow \neg P$

(7) $P \to Q$ 为假, 只能是 P 为真, Q 为假. (7) 或者

$$\begin{aligned}\neg(P \to Q) &\Leftrightarrow \neg(\neg P \vee Q) \\ &\Leftrightarrow P \wedge \neg Q \\ &\Rightarrow P \quad (\text{或} \Rightarrow \neg Q).\end{aligned}$$

(9) 合取引入. (10) 析取三段论, 或 "选言推理", "排除法". (11) 假言推理, 最常用的推理规则. (12) 设 $\neg Q$ 为真, 即 Q 为假; 要 $P \to Q$ 为真, 则 P 必须为假. 得 $\neg P$ 为真. 此为 "拒取式", 即 "反证法". 8.109

常用蕴含式

13. $P \to Q, Q \to R \Rightarrow P \to R$
14. $P \vee Q, P \to R, Q \to R \Rightarrow R$
15. $A \to B \Rightarrow (A \vee C) \to (B \vee C)$
16. $A \to B \Rightarrow (A \wedge C) \to (B \wedge C)$

(13) 假言三段论. 表明推理的传递性. (14) 假设 $P \vee Q$, $P \to R$, $Q \to R$ 为真.

- 若 P 为真, 要 $P \to R$ 为真, 必 R 为真.
- 若 P 为假, 则 Q 为真. 要 $Q \to R$ 为真, 必 R 为真.

(15)

$$\begin{aligned}&(A \vee C) \to (B \vee C) \\ \Leftrightarrow\ &\neg(A \vee C) \vee (B \vee C) \\ \Leftrightarrow\ &(\neg A \wedge \neg C) \vee (B \vee C) \\ \Leftrightarrow\ &(\neg A \vee B \vee C) \wedge (\neg C \vee B \vee C) \\ \Leftrightarrow\ &(\neg A \vee B \vee C) \\ \Leftrightarrow\ &(A \to B) \vee C\end{aligned}$$

由 I_3, 知

$$(A \to B) \Rightarrow (A \to B) \vee C$$

8.110

常用等价式

1. $\neg\neg P \Leftrightarrow P$ 对合律
2. $P \vee Q \Leftrightarrow Q \vee P$ 交换律
3. $P \wedge Q \Leftrightarrow Q \wedge P$
4. $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$ 结合律
5. $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$
6. $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$ 分配律
7. $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$

8.111

常用等价式

8. $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$ 德 · 摩根律
9. $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$
10. $P \vee P \Leftrightarrow P$ 幂等律
11. $P \wedge P \Leftrightarrow P$
12. $R \vee (P \wedge \neg P) \Leftrightarrow R$ 同一律
13. $R \wedge (P \vee \neg P) \Leftrightarrow R$
14. $R \vee (P \vee \neg P) \Leftrightarrow \mathbf{T}$ 零律
15. $R \wedge (P \wedge \neg P) \Leftrightarrow \mathbf{F}$

8.112

常用等价式

16. $P \to Q \Leftrightarrow \neg P \vee Q$
17. $\neg(P \to Q) \Leftrightarrow P \wedge \neg Q$
18. $P \to Q \Leftrightarrow \neg Q \to \neg P$
19. $P \to (Q \to R) \Leftrightarrow (P \wedge Q) \to R$
20. $P \leftrightarrow Q \Leftrightarrow (P \to Q) \wedge (Q \to P)$
21. $P \leftrightarrow Q \Leftrightarrow (P \wedge Q) \vee (\neg P \wedge \neg Q)$
22. $\neg(P \leftrightarrow Q) \Leftrightarrow P \leftrightarrow \neg Q$

☞下证 E_{19} 和 E_{22}. 8.113

证明 E_{19}: $P \to (Q \to R) \Leftrightarrow (P \wedge Q) \to R$.

证:

$$\begin{aligned}
P \to (Q \to R) &\Leftrightarrow \neg P \vee (Q \to R) && (E_{16})\\
&\Leftrightarrow \neg P \vee (\neg Q \vee R) && (E_{16})\\
&\Leftrightarrow (\neg P \vee \neg Q) \vee R && (\text{结合律})\\
&\Leftrightarrow \neg(P \wedge Q) \vee R && (\text{德 · 摩根律})\\
&\Leftrightarrow (P \wedge Q) \to R && (E_{16})
\end{aligned}$$

$P \to (Q \to R) \not\Leftrightarrow (P \to Q) \to R.$ 8.114

证明 E_{22}: $\neg(P \leftrightarrow Q) \Leftrightarrow P \leftrightarrow \neg Q$.

证: 注意到 $P \leftrightarrow Q \Leftrightarrow (P \wedge Q) \vee (\neg P \wedge \neg Q)$, 有

$$P \leftrightarrow \neg Q \Leftrightarrow (P \wedge \neg Q) \vee (\neg P \wedge Q). \qquad (19)$$

又

$$\neg(P \leftrightarrow Q) \Leftrightarrow P \,\bar{\vee}\, Q \Leftrightarrow (P \wedge \neg Q) \vee (\neg P \wedge Q). \qquad (20)$$

由 (19) 式和 (20) 式知

$$\neg(P \leftrightarrow Q) \Leftrightarrow P \leftrightarrow \neg Q.$$

(☞ 或用真值表, 也很简捷.) 8.115

形式推理的表上作业

形式推理的具体操作可在包含 3 列的一张表上进行:

- 第一列是序号, 将各次操作按先后排序;
- 第二列是断言或命题公式, 内容可以是前提, 中间结论或最终结论;
- 第三列是注释或根据, 表明所引用的推理规则及与之有关的行的编号.

证明 $\neg(P \wedge \neg Q), \neg Q \vee R, \neg R \Rightarrow \neg P$.

(1)	$\neg R$	P
(2)	$\neg Q \vee R$	P
(3)	$\neg Q$	T(1),(2) I
(4)	$\neg(P \wedge \neg Q)$	P
(5)	$\neg P \vee Q$	T(4) E
(6)	$\neg P$	T(3),(5) I

8.116

形式推理的表上作业

为什么可以这样表示?

- 蕴含式 $P \Rightarrow Q$ 的证明方法之一就是: 假设前件 P 为 **T**, 能够推得后件 Q 也为 **T**.
- 第二列所列命题公式, 均是真值为 **T** 的. (只是省略, 不言自明而已.)

证明 $\neg(P \wedge \neg Q), \neg Q \vee R, \neg R \Rightarrow \neg P$.

(1)	$\neg R$	P
(2)	$\neg Q \vee R$	P
(3)	$\neg Q$	T(1),(2) I
(4)	$\neg(P \wedge \neg Q)$	P
(5)	$\neg P \vee Q$	T(4) E
(6)	$\neg P$	T(3),(5) I

8.117

Example 62. 证明 $(P \vee Q) \wedge (P \rightarrow R) \wedge (Q \rightarrow S) \Rightarrow S \vee R$.

证:

(1)	$P \vee Q$	P
(2)	$\neg P \rightarrow Q$	T(1) E
(3)	$Q \rightarrow S$	P
(4)	$\neg P \rightarrow S$	T(2),(3) I
(5)	$\neg S \rightarrow P$	T(4) E
(6)	$P \rightarrow R$	P
(7)	$\neg S \rightarrow R$	T(5),(6) I
(8)	$S \vee R$	T(7) E

8.118

Example

证明 $(W \vee R) \rightarrow V, V \rightarrow C \vee S, S \rightarrow U, \neg C \wedge \neg U \Rightarrow \neg W$.

证:

(1)	$\neg C \wedge \neg U$	P
(2)	$\neg U$	T(1) I
(3)	$S \to U$	P
(4)	$\neg S$	T(2),(3) I
(5)	$\neg C$	T(1) I
(6)	$\neg C \wedge \neg S$	T(4),(5) E
(7)	$\neg(C \vee S)$	T(6) E
(8)	$(W \vee R) \to V$	P
(9)	$V \to C \vee S$	P
(10)	$(W \vee R) \to (C \vee S)$	T(8),(9) I
(11)	$\neg(W \vee R)$	T(7),(10) I
(12)	$\neg W \wedge \neg R$	T(11) E
(13)	$\neg W$	T(12) I

8.119

Example

证明 $(W \vee R) \to V,\ V \to C \vee S,\ S \to U,\ \neg C \wedge \neg U \Rightarrow \neg W$.

另证:

(1)	$\neg C \wedge \neg U$	P
(2)	$\neg U$	T(1) I
(3)	$S \to U$	P
(4)	$\neg S$	T(2),(3) I
(5)	$\neg C$	T(1) I
(6)	$\neg C \wedge \neg S$	T(4),(5) I(I_9)
(7)	$\neg(C \vee S)$	T(6) E
(8)	$V \to C \vee S$	P
(9)	$\neg V$	T(7),(8) I
(10)	$(W \vee R) \to V$	P
(11)	$\neg(W \vee R)$	T(9),(10) I
(12)	$\neg W \wedge \neg R$	T(11) E
(13)	$\neg W$	T(12) I

8.120

Example

证明 $(W \vee R) \to V,\ V \to C \vee S,\ S \to U,\ \neg C \wedge \neg U \Rightarrow \neg W$.

注意: 在上述证明中, 反复用到了 I_{12}:

$$\neg Q,\ P \to Q \Rightarrow \neg P$$

8.121

相容 & 不相容

"相容" 与 "不相容"

设 $P_1, P_2, \cdots, P_n$ 是出现于前提 $H_1, H_2, \cdots, H_m$ 中的全部命题变元.

- 对于 $P_1, P_2, \cdots, P_n$ 的一些真值指派, 如果能使 $H_1 \wedge H_2 \wedge \cdots \wedge H_m$ 的真值为 **T** , 则称公式 $H_1, H_2, \cdots, H_m$ 是相容的.
- 如果对于 $P_1, P_2, \cdots, P_n$ 的每一组真值指派, 使得 $H_1 \wedge H_2 \wedge \cdots \wedge H_m$ 的真值均为 **F**, 则称公式 $H_1, H_2, \cdots, H_m$ 是不相容的.

8.122

间接证明法之一: 反证法

要证

$$H_1 \wedge H_2 \wedge \cdots \wedge H_m \Rightarrow C,$$

记作

$$S \Rightarrow C,$$

即

$$S \to C,\ \text{或}\ \neg S \vee C$$

为 **T**, 故 $S \wedge \neg C$ 为 **F**. 即 S 与 $\neg C$ 不相容.

因此要证 $H_1 \wedge H_2 \wedge \cdots \wedge H_m \Rightarrow C$, 只要证 $H_1, H_2, \cdots, H_m$ 与 $\neg C$ 是不相容的.

☞ 这其实就是我们经常使用的反证法. 8.123

间接证明法之一: 反证法

Example 63. 证明 $A \to B, \neg(B \vee C)$ 可逻辑推出 $\neg A$.

证: 使用反证法, 下证 $A \to B, \neg(B \vee C)$ 与 $\neg(\neg A)$ 不相容.

(1)	A	P(附加前提)
(2)	$A \to B$	P
(3)	B	T(1),(2) I
(4)	$\neg(B \vee C)$	P
(5)	$\neg B \wedge \neg C$	T(4) E
(6)	$\neg B$	T(5) I
(7)	$B \wedge \neg B$ (矛盾)	T(3),(6) I

8.124

Example

用反证法再次证明 $(W \vee R) \to V, V \to C \vee S, S \to U, \neg C \wedge \neg U \Rightarrow \neg W$.

证:

(1)	W	P(附加前提)
(2)	$W \vee R$	T(1) I
(3)	$(W \vee R) \to V$	P
(4)	$V \to C \vee S$	P
(5)	$(W \vee R) \to (C \vee S)$	T(3),(4) I
(6)	$C \vee S$	T(2),(5) I
(7)	$\neg C \wedge \neg U$	P
(8)	$\neg C$	T(7) I
(9)	S	T(6),(8) I
(10)	$S \to U$	P
(11)	U	T(10) I
(12)	$\neg U$	T(7) I
(13)	$U \wedge \neg U$(矛盾)	T(11),(12) E

8.125

间接证明法的另一种情形: CP 规则

若要证明

$$H_1 \wedge H_2 \wedge \cdots \wedge H_m \Rightarrow (R \to C), \tag{21}$$

将 $H_1 \wedge H_2 \wedge \cdots \wedge H_m$ 记作 S, 即要证

$$S \Rightarrow (R \to C), \tag{22}$$

即 $S \to (R \to C)$ 为 **T**.

由 E_{19}: $P \to (Q \to R) \Leftrightarrow (P \wedge Q) \to R$, 知

$$S \to (R \to C) \Leftrightarrow (S \wedge R) \to C. \tag{23}$$

从而, 要证明 $S \Rightarrow (R \to C)$, 转化为证明

$$(S \wedge R) \Rightarrow C. \tag{24}$$

这就是 CP 规则 (Conditional Proof).

这里, 将 R 称为附加前提. 8.126

间接证明法另一种情形: CP 规则

Example 64. 证明 $A \to (B \to C), \neg D \vee A, B$ 重言蕴含 $D \to C$.

证:

(1)	D	P (附加前提)
(2)	$\neg D \vee A$	P
(3)	A	T(1),(2) I
(4)	$A \to (B \to C)$	P
(5)	$(B \to C)$	T(3),(4) I
(6)	B	P
(7)	C	T(5),(6) I
(8)	$D \to C$	CP

8.127

对下面的论述构造一个证明:

如果李明来武汉大学, 若王军不生病, 则王军一定去看望李明. 如果李明出差到武汉, 那么李明一定来武汉大学. 王军没有生病. 所以, 如果李明出差到武汉, 王军一定去看望李明.

证: 设 P: 李明出差到武汉; Q: 李明来武汉大学; R: 王军生病; S: 王军去看望李明. 则问题归结为证:

$$Q \to (\neg R \to S),\ P \to Q,\ \neg R \Rightarrow P \to S.$$

列表证明如下:

(1)	P	P (附加前提)
(2)	$P \to Q$	P
(3)	Q	T(1),(2) I
(4)	$Q \to (\neg R \to S)$	P
(5)	$\neg R \to S$	T(3),(4) I
(6)	$\neg R$	P
(7)	S	T(5),(6) I
(8)	$P \to S$	CP

Example 65. 在某研讨会的休息时间, 3 名与会者根据王教授的口音对他是哪个省市的人进行了判断:

- 甲说王教授不是南京人, 是上海人;
- 乙说王教授不是上海人, 是南京人;
- 丙说王教授既不是上海人, 也不是杭州人.

听完以上 3 人的判断后, 王教授笑着说, 他们 3 人中有一人说的全对, 有一人说对了一半, 另一人说的全不对. 试分析王教授是哪里人?

解: 设 N: 王教授是南京人, S: 王教授是上海人, H: 王教授是杭州人; 且

- 甲的判断为 $\neg N \wedge S$,
- 乙的判断为 $N \wedge \neg S$,
- 丙的判断为 $\neg S \wedge \neg H$.

进一步设

- 甲的判断全对 $B_1 = \neg N \wedge S$,
- 甲的判断对一半 $B_2 = (\neg N \wedge \neg S) \vee (N \wedge S)$,
- 甲的判断全错 $B_3 = N \wedge \neg S$,
- 乙的判断全对 $C_1 = N \wedge \neg S$,
- 乙的判断对一半 $C_2 = (N \wedge S) \vee (\neg N \wedge \neg S)$,
- 乙的判断全错 $C_3 = \neg N \wedge S$,
- 丙的判断全对 $D_1 = \neg S \wedge \neg H$,
- 丙的判断对一半 $D_2 = (\neg S \wedge H) \vee (S \wedge \neg H)$,
- 丙的判断全错 $D_3 = S \wedge H$.

由王教授所说

$$\begin{aligned} E = &(B_1 \wedge C_2 \wedge D_3) \vee (B_1 \wedge C_3 \wedge D_2) \vee (B_2 \wedge C_1 \wedge D_3) \\ &\vee (B_2 \wedge C_3 \wedge D_1) \vee (B_3 \wedge C_1 \wedge D_2) \vee (B_3 \wedge C_2 \wedge D_1) \end{aligned} \tag{25}$$

为真命题.

而

$$\begin{aligned} (B_1 \wedge C_2 \wedge D_3) &= (\neg N \wedge S) \wedge \big((N \wedge S) \vee (\neg N \wedge \neg S)\big) \wedge (S \wedge H) \\ &\Leftrightarrow \big((\neg N \wedge S \wedge N \wedge S) \vee (\neg N \wedge S \wedge \neg N \wedge \neg S)\big) \wedge (S \wedge H) \\ &\Leftrightarrow (\mathbf{F} \vee \mathbf{F}) \wedge (S \wedge H) \\ &\Leftrightarrow \mathbf{F} \end{aligned} \tag{26}$$

$$\begin{aligned} B_1 \wedge C_3 \wedge D_2 &= (\neg N \wedge S) \wedge (\neg N \wedge S) \wedge \big((\neg S \wedge H) \vee (S \wedge \neg H)\big) \\ &\Leftrightarrow (\neg N \wedge S \wedge \neg S \wedge H) \vee (\neg N \wedge S \wedge S \wedge \neg H) \\ &\Leftrightarrow \mathbf{F} \vee (\neg N \wedge S \wedge \neg H) \\ &\Leftrightarrow \neg N \wedge S \wedge \neg H \end{aligned} \tag{27}$$

$$
\begin{aligned}
(B_3 \wedge C_1 \wedge D_2) = (N \wedge \neg S) \wedge (N \wedge \neg S) \wedge \big((\neg S \wedge H) \vee (S \wedge \neg H)\big) \\
\Leftrightarrow (N \wedge \neg S \wedge \neg S \wedge H) \vee (N \wedge \neg S \wedge S \wedge \neg H) \\
\Leftrightarrow (N \wedge \neg S \wedge H) \vee \mathbf{F} \\
\Leftrightarrow (N \wedge \neg S \wedge H)
\end{aligned} \tag{28}
$$

类似可得 8.129

$$(B_2 \wedge C_1 \wedge D_3) \Leftrightarrow \mathbf{F} \tag{29}$$

$$(B_2 \wedge C_3 \wedge D_1) \Leftrightarrow \mathbf{F} \tag{30}$$

$$(B_3 \wedge C_2 \wedge D_1) \Leftrightarrow \mathbf{F} \tag{31}$$

于是, 由同一律可知

$$E \Leftrightarrow (\neg N \wedge S \wedge \neg H) \vee (N \wedge \neg S \wedge H) \tag{32}$$

因为王教授不能既是上海人, 又是杭州人, 因而 $(N \wedge \neg S \wedge H) \Leftrightarrow \mathbf{F}$.
于是只有 $(\neg N \wedge S \wedge \neg H)$ 为真命题, 即王教授是上海人.
甲说的全对, 丙说对了一半, 而乙全说错了.

这一类的推理在报纸、杂志的智力游戏里经常可以看到. 平时我们处理这类推理时并没有这么复杂. 比如: 假设 “甲说的全对”, 由乙与甲所说相反, 则乙说的全错, 同时丙说对了一半. 这个假设与王教授所说不矛盾, 所以假设成立, 问题解决. 或者: 王教授不可能同时是两个城市的人, 则丙至少说对了一半, 从而全错只可能是甲乙之一, 然后再来作判断. 这个例子放在这里只是为了说明一种方法. 8.130

莱布尼茨 —— “样样皆通的大师”

Gottfried Wilhelm von Leibniz (Leipzig July 1, 1646 – November 14, 1716 in Hannover), a philosopher, scientist, mathematician, diplomat, librarian, and lawyer.

- 政治家成为数学家 [1666 年法学博士学位 美因茨选侯 腓特烈公爵]
- 普遍符号语言 [“$\cup$, $\cap$; $\sim$; $\cong$, $\frac{a}{b}$”]
- 26 岁学数学 [惠更斯 计算机器 $\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \cdots$]
- 创立微积分 [1677 年 $\int$ Summa dx 牛莱之争]
- 与中国的联系 [康熙 (1654–1722) 科学院 二进制 八卦 《中国近事》(1697)]
- 没有结婚, 没有在大学当教授
- 孤寂地离世 return 8.131

Chapter 9

谓词逻辑

Discrete Mathematics

December 30, 2011

黄正华, 数学与统计学院, 武汉大学

9.1

Contents

9.2

1 谓词逻辑命题的符号化

1.1 个体与谓词

个体 & 谓词

命题作为反映判断的句子, 由主语和谓语两部分组成, 这里分别称为个体和谓词:

- 在原子命题中所描述的对象称为个体 (常用小写字母 a, b, c 表示);
- 用以描述个体性质或个体间关系的部分称为谓词 (常用大写字母 A, B 表示).

例如, 若 A 表示 "是个大学生", c 表示 "张三", e 表示 "李四", 则

- $A(c)$ 表示 "张三是个大学生";
- $A(e)$ 表示 "李四是个大学生".

☞ 这一讨论问题的方式类似于 "函数" 概念.

9.3

用谓词表达命题

- 一般来说, "x 是 A" 类型的命题可以用 $A(x)$ 表达.
- 对于 "x 大于 y" 这种两个个体之间关系的命题, 可表达为 $B(x, y)$, 这里 B 表示谓词 "$\cdots$ 大于 $\cdots$".
- 我们把 $A(x)$ 称为一元谓词, $B(x, y)$ 称为二元谓词, $M(a, b, c)$ 称为三元谓词, 依次类推.
- 通常把二元以上谓词称作*多元谓词*.

9.4

谓词 & 谓词填式

- 单独一个谓词不是完整的命题.
- 谓词字母后填以个体所得的式子, 称为*谓词填式*.
- 如果 A 为 n 元谓词, $a_1, a_2, \cdots, a_n$ 是个体名称, 则 $A(a_1, a_2, \cdots, a_n)$ 就成为一个命题.

9.5

1.2 量词

Example 1.

- 命题 "x 是素数" 中, x 是个体, 谓词是 "是素数", 记为 P, 则此谓词表达式可写为 $P(x)$.
- 特别, $P(5)$ 是命题: "5 是素数".
- 此例中 x 表示不确定的个体, 称为*个体变元*; 5 是*个体常元*.

这里, $P(x)$ 的真值随 x 而变, 它对某些 x 可能为真, 对某些 x 可能为假. 所以, $P(x)$ 是*命题函数*, 而不是命题.

9.6

简单命题函数

Definition 2. 由① 一个谓词, ② 一些个体变元, 组成的表达式称为*简单命题函数*.

由定义可见

- n 元谓词, 就是 "有 n 个个体变元" 的命题;
- 当 $n = 0$ 时, 称为 *0 元谓词*. 0 元谓词本身就是一个命题 (类似常数函数).
- 故命题是 n 元谓词的一个特殊情况.

9.7

复合命题函数

Definition 3. 由一个或 n 个简单命题函数, 以及逻辑联结词 (如 $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrows$ 等) 组合而成的表达式, 称为*复合命题函数*.

- 逻辑联结词 $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrows$ 的意义, 与命题演算中的解释相同.

- 命题函数不是命题. 只有个体变元取特定的名称时, 才能成为一个命题. 例如 $Q(x,y)$ 表示 "x 比 y 重", 当 x, y 指人或物时, 它是一个命题; 但若 x, y 指实数时, 就不是一个命题.
- 个体变元的取值范围, 对命题的真值有影响. 例如 $R(x)$ 表示 "x 是大学生". 当 x 的讨论范围是某大学的一个班级时, $R(x)$ 为永真; 当 x 的讨论范围是某中学的一个班级时, $R(x)$ 为永假; 当 x 的讨论范围是一个剧场中的观众时, $R(x)$ 有真有假.

9.8

个体域

- 在命题函数中, 个体变元的论述范围, 称为个体域.
- 个体域可以是有限的, 也可以是无限的.
- 把各种个体域综合在一起作为论述范围的域, 称全总个体域.

☞ 个体域之于命题函数, 类似定义域之于函数. 9.9

量词

- 全称量词: $\forall$, 表达 "对所有的", "每一个", "对任一个".
- 存在量词: $\exists$, 表达 "存在一些", "至少有一个", "对于一些".
- $\forall$ 是 Any 的第一个字母的倒写.
- $\exists$ 是 Exist 的第一个字母的反写.

9.10

Example 4. 符号化下列命题:

1. 没有不犯错误的人.
2. 发光的不都是金子.

解: ① 设 $M(x)$: x 是人. $Q(x)$: x 犯错误. 则命题符号化为

$$(\forall x)\big(M(x) \to Q(x)\big).$$

或者

$$\neg(\exists x)\big(M(x) \wedge \neg Q(x)\big).$$

② 设 $L(x)$: x 是发光的东西. $G(x)$: x 是金子. 则命题符号化为

$$(\exists x)\big(L(x) \wedge \neg G(x)\big).$$

或者

$$\neg(\forall x)\big(L(x) \to G(x)\big).$$

9.11

Example 5. 用谓词表达式写出下列命题:

1. 小张不是工人.
2. 小莉是非常聪明和美丽的.
3. 每一个有理数是实数.
4. 某些实数是有理数.

5. 直线 a 与直线 b 平行当且仅当直线 a 与 b 不相交.

解: ① 设 $W(x)$: x 是工人. c: 小张. 得

$$\neg W(c).$$

② 设 $C(x)$: x 是聪明的. $B(x)$: x 是美丽的. l: 小莉. 得

$$C(l) \wedge B(l).$$

③ 设 $Q(x)$: x 是有理数. $R(x)$: x 是实数. 则

$$(\forall x)\big(Q(x) \rightarrow R(x)\big).$$

④ 设 $R(x)$: x 是实数. $Q(x)$: x 是有理数. 则

$$(\exists x)\big(R(x) \wedge Q(x)\big).$$

⑤ 设 $P(x, y)$: 直线 x 平行于直线 y. $Q(x, y)$: 直线 x 与直线 y 相交. 则

$$P(a, b) \rightleftarrows \neg Q(a, b).$$

9.12

练习

找出下列句子所对应的谓词表达式:

1. 所有教练员是运动员 $(J(x), L(x))$;
2. 某些运动员是大学生 $(S(x))$;
3. 某些教练是年老的, 但是健壮的 $(O(x), V(x))$;
4. 金教练既不老但也不是健壮的 (j);
5. 某些大学生运动员是国家选手 $(C(x))$.

解: ① 设 $J(x)$: x 是教练员; $L(x)$: x 是运动员. 则

$$(\forall x)\big(J(x) \rightarrow L(x)\big).$$

② 设 $S(x)$: x 是大学生; $L(x)$: x 是运动员. 则

$$(\exists x)\big(S(x) \wedge L(x)\big).$$

③ 设 $J(x)$: x 是教练员; $O(x)$: x 是年老的; $V(x)$: x 是健壮的. 则

$$(\exists x)\big(J(x) \wedge O(x) \wedge V(x)\big).$$

④ 设 $O(x)$: x 是年老的; $V(x)$: x 是健壮的; j: 金教练. 则

$$\neg O(j) \wedge \neg V(j).$$

⑤ 设 $S(x)$: x 是大学生; $L(x)$: x 是运动员; $C(x)$: x 是国家选手. 则

$$(\exists x)\big(S(x) \wedge L(x) \wedge C(x)\big).$$

9.13

2 谓词公式及其真值

谓词公式

Definition 6. • 不出现命题联结词和量词的谓词填式称为*谓词演算的原子公式*. 简称*原子谓词公式*. 例如 $A(x_1, x_2, \cdots, x_n)$.

- 由下列递归规则生成的公式称为*谓词演算的合式公式* (简称*谓词公式*):
  1. 原子谓词公式是合式公式;
  2. 若 A 和 B 是合式公式, 则 $\neg A$, $A \wedge B$, $A \vee B$, $A \rightarrow B$, $A \rightleftarrows B$, $(\forall x)A$, $(\exists x)A$ 是合式公式;
  3. 只有有限步应用 (1) 和 (2) 生成的公式才是合式公式.

☞ *定义方式与命题演算的合式公式相同.*

9.14

括号的问题

谓词合式公式表达中括号的使用:

- 与第一章中讨论命题公式时的约定相同: 最外层的括号可以省略.
- 量词后面接原子公式, 括号省略. 例如, $(\forall x)\big(P(x)\big)$ 总是写为 $(\forall x)P(x)$.
- 量词后面接非原子公式, 则括号不能省略. 例如, $(\forall x)\big(P(x) \vee Q(x)\big)$ 不能写成 $(\forall x)P(x) \vee Q(x)$.

9.15

Example 7. 尽管有人聪明, 但未必一切人都聪明. $\big(P(x),\ M(x)\big)$

解: $\exists x\big(M(x) \wedge P(x)\big) \wedge \neg\Big(\forall x\big(M(x) \rightarrow P(x)\big)\Big)$

Example 8. 极限的定义: 任给小正数 ε, 则存在一个正数 δ, 使得当 $0 < |x-a| < \delta$ 时有 $|f(x)-b| < \varepsilon$. 此时即称 $\lim_{x \to a} f(x) = b$.

解: 设 $P(x, y)$ 表示 "x 大于 y", $Q(x, y)$ 表示 "x 小于 y". 则 $\lim_{x \to a} f(x) = b$ 可表示为:

$$(\forall \varepsilon)(\exists \delta)(\forall x)\Big(\Big(\big(P(\varepsilon, 0) \rightarrow P(\delta, 0)\big) \wedge P(|x-a|, 0) \wedge Q(|x-a|, \delta)\Big) \rightarrow Q(|f(x)-b|, \varepsilon)\Big)$$

9.16

Example 9. 设 $P(x)$, $L(x)$, $R(x, y, z)$ 和 $E(x, y)$ 分别表示 "x 是一个点", "x 是一条直线", "z 通过 x 和 y", "$x = y$". 符号化下面的句子: 对每两个点, 有且仅有一条直线通过该两点.

解:

$$\begin{aligned}(\forall x)(\forall y)\Big(&\big(P(x) \wedge P(y) \wedge \neg E(x, y)\big) \\ &\rightarrow (\exists! z)\big(L(z) \wedge R(x, y, z)\big)\Big)\end{aligned}$$

注: 符号 " $\exists!$ " 表示 "有且仅有一个".
$(\exists! x)P(x)$ 表示: "存在惟一的 x 使 $P(x)$ 为真".

9.17

3 谓词公式的前束范式

指导变元 & 作用域

- 指导变元 —— 把 $\forall x$ 或 $\exists x$ 中的变元 x 叫做相应量词的指导变元 (或作用变元).
- 作用域 —— 把紧跟在 $\forall x$ 或 $\exists x$ 后面并用圆括号括起来的公式, 或者没有圆括号括着的原子公式, 称为相应量词的作用域 (或辖域). 比如,

$$(\forall x)\big(P(x) \vee Q(x)\big)$$

  指导变元 x 的作用域是 $P(x) \vee Q(x)$.

9.18

自由变元 & 约束变元

- 约束变元 —— 在量词作用域中出现的、与指导变元相同的变元, 称为约束变元. 相应变元的出现, 称为约束出现.
- 自由变元 —— 除约束变元外的一切变元, 称为自由变元. 相应变元的出现称为自由出现. 比如,

$$(\forall x)P(x) \vee Q(x)$$

其中 $P(x)$ 内的 x 是约束变元, 而 $Q(x)$ 内的 x 是自由变元.

9.19

约束变元换名规则

- 换名的原因: 为了避免一个变元既是自由变元又是约束变元可能引起的混淆. 比如:

$$(\forall x)P(x) \vee Q(x)$$

容易在含义上误会为

$$(\forall x)\big(P(x) \vee Q(x)\big)$$

- 换名规则: 一个公式中的约束变元可以更改如下:
    1. 若要换名, 则该变元在量词及其作用域中的所有出现均需一起改变, 其余部分不变.
    2. 换名时所选用的符号必须是量词作用域内未出现的符号, 最好是公式中未出现的符号.

9.20

换名规则

Example 10.

$$(\forall x)P(x) \vee Q(x) \Leftrightarrow (\forall y)P(y) \vee Q(x); \tag{1}$$

$$(\forall x)\big(P(x) \vee Q(x,y)\big) \wedge R(x) \vee S(z) \Leftrightarrow (\forall w)\big(P(w) \vee Q(w,y)\big) \wedge R(x) \vee S(z). \tag{2}$$

但注意:

$$(\forall x)\big(P(x) \vee Q(x,y)\big) \wedge R(x) \vee S(z) \not\Leftrightarrow (\forall y)\big(P(y) \vee Q(y,y)\big) \wedge R(x) \vee S(z). \tag{3}$$

9.21

自由变元代入规则

- 自由变元的代入, 即自由变元的改名.
- 自由变元代入规则:
    1. 对于谓词公式中的自由变元可以代入, 代入时需要对公式中出现该自由变元的每一处进行代入.
    2. 用以代入的变元与原公式中所有变元的名称不能相同.

9.22

习题

对下列谓词公式中的自由变元进行代入.

a) $\big(\exists y\, A(x,\, y) \to \forall x\, B(x,\, z)\big) \land \exists x\, \forall z\, C(x,\, y,\, z)$.

b) $\big(\forall y\, P(x,\, y) \land \exists z\, Q(x,\, z)\big) \lor \forall x\, R(x,\, y)$.

解: a) $\big(\exists y\, A(u,\, y) \to \forall x\, B(x,\, v)\big) \land \exists x\, \forall z\, C(x,\, w,\, z)$.

b) $\big(\forall y\, P(u,\, y) \land \exists z\, Q(v,\, z)\big) \lor \forall x\, R(x,\, w)$.

9.23

- 设论域为 $\{a_1,\, a_2,\, \cdots,\, a_n\}$, 则

$$(\forall x)A(x) \Leftrightarrow A(a_1) \land A(a_2) \land \cdots \land A(a_n) \tag{4}$$

$$(\exists x)A(x) \Leftrightarrow A(a_1) \lor A(a_2) \lor \cdots \lor A(a_n) \tag{5}$$

- 量词对变元的约束, 往往与量词的出现顺序有关, 约定 “量词按从左到右的顺序读出”.

9.24

Example 11. 如果论域是集合 $\{a,\, b,\, c\}$, 试消去下面公式中的量词:

1. $(\forall x)P(x)$;
2. $(\forall x)R(x) \land (\forall x)S(x)$;
3. $(\forall x)R(x) \land (\exists x)S(x)$.

解: ① $(\forall x)P(x) \Leftrightarrow P(a) \land P(b) \land P(c)$.

② $(\forall x)R(x) \land (\forall x)S(x) \Leftrightarrow R(a) \land R(b) \land R(c) \land S(a) \land S(b) \land S(c)$.

③ $(\forall x)R(x) \land (\exists x)S(x) \Leftrightarrow \big(R(a) \land R(b) \land R(c)\big) \land \big(S(a) \lor S(b) \lor S(c)\big)$

9.25

习题. 寻求下列公式的真值:

1. $(\forall x)\big(P(x) \lor Q(x)\big)$, 其中 $P(x): x = 1$; $Q(x): x = 2$; 论域是 $\{1,\, 2\}$.
2. $(\forall x)\big(P \to Q(x)\big) \lor R(a)$, 其中 $P: 2 > 1$; $Q(x): x \leqslant 3$; $R(x): x > 5$ 而 $a: 5$; 论域是 $\{-2,\, 3,\, 6\}$.

解: ① $(\forall x)\big(P(x) \lor Q(x)\big) \Leftrightarrow \big(P(1) \lor Q(1)\big) \land \big(P(2) \lor Q(2)\big)$,

而 $P(1)$ 为 $\mathbf{T}$, $P(2)$ 为 $\mathbf{F}$; $Q(1)$ 为 $\mathbf{F}$, $Q(2)$ 为 $\mathbf{T}$. 所以

$$(\forall x)\big(P(x) \lor Q(x)\big) \Leftrightarrow (\mathbf{T} \lor \mathbf{F}) \land (\mathbf{F} \lor \mathbf{T}) \Leftrightarrow \mathbf{T}.$$

② $(\forall x)\big(P \to Q(x)\big) \Leftrightarrow \big(P \to Q(-2)\big) \land \big(P \to Q(3)\big) \land \big(P \to Q(6)\big)$,

其中 P 为 $\mathbf{T}$, $Q(-2)$ 为 $\mathbf{T}$; $Q(3)$ 为 $\mathbf{T}$, $Q(6)$ 为 $\mathbf{F}$. 所以

$$(\forall x)\big(P \to Q(x)\big) \Leftrightarrow (\mathbf{T} \to \mathbf{T}) \land (\mathbf{T} \to \mathbf{T}) \land (\mathbf{T} \to \mathbf{F}) \Leftrightarrow \mathbf{T} \land \mathbf{T} \land \mathbf{F} \Leftrightarrow \mathbf{F}$$

又 $R(a)$ 为 $\mathbf{F}$, 所以

$$(\forall x)\big(P \to Q(x)\big) \lor R(a) \Leftrightarrow \mathbf{F} \lor \mathbf{F} \Leftrightarrow \mathbf{F}.$$

9.26

前束范式

Definition 12. 一个公式, 如果量词均在全式的开头, 它们的作用域延伸到整个公式的末尾, 则该公式叫做前束范式.

前束范式可记为下述形式:

$$(\Box v_1)(\Box v_2)\cdots(\Box v_n)A \tag{6}$$

其中 $\Box$ 是量词 $\forall$ 或 $\exists$; v_i 是个体变元; A 是没有量词的谓词公式. 9.27

Example 13. 例如

$$(\forall x)(\forall y)\big(F(x)\wedge G(y)\to H(x,y)\big), \tag{7}$$

$$(\forall x)(\forall y)(\exists z)\big(F(x)\wedge G(y)\wedge H(z)\to L(x,y,z)\big) \tag{8}$$

等公式都是前束范式.

而

$$(\forall x)\Big(F(x)\to(\exists y)\big(G(y)\wedge H(x,y)\big)\Big), \tag{9}$$

$$(\exists x)\Big(F(x)\wedge(\forall y)\big(G(y)\to H(x,y)\big)\Big) \tag{10}$$

等都不是前束范式. 9.28

Theorem 14. *任意一个谓词公式, 均和一个前束范式等价.* 9.29

Example 15. 求下面公式的前束范式:

1. $(\forall x)F(x)\wedge\neg(\exists x)G(x)$;
2. $(\forall x)F(x)\vee\neg(\exists x)G(x)$.

解: ①

$$\begin{aligned}
(\forall x)F(x)\wedge\neg(\exists x)G(x) &\Leftrightarrow (\forall x)F(x)\wedge\neg(\exists y)G(y) && \text{(换名)}\\
&\Leftrightarrow (\forall x)F(x)\wedge(\forall y)\neg G(y) && \text{(量词转化)}\\
&\Leftrightarrow (\forall x)\big(F(x)\wedge(\forall y)\neg G(y)\big) && \text{(扩张作用域)}\\
&\Leftrightarrow (\forall x)(\forall y)\big(F(x)\wedge\neg G(y)\big) && \text{(扩张作用域)}
\end{aligned}$$

或者

$$\begin{aligned}
(\forall x)F(x)\wedge\neg(\exists x)G(x) &\Leftrightarrow (\forall x)F(x)\wedge(\forall x)\neg G(x) && \text{(量词转化)}\\
&\Leftrightarrow (\forall x)\big(F(x)\wedge\neg G(x)\big) && (E_{24})
\end{aligned}$$

9.30

②

$$
\begin{aligned}
(\forall x)F(x) \vee \neg(\exists x)G(x) &\Leftrightarrow (\forall x)F(x) \vee (\forall x)\neg G(x) && \text{(量词转化)} \\
&\Leftrightarrow (\forall x)F(x) \vee (\forall y)\neg G(y) && \text{(换名)} \\
&\Leftrightarrow (\forall x)\big(F(x) \vee (\forall y)\neg G(y)\big) && \text{(扩张作用域)} \\
&\Leftrightarrow (\forall x)(\forall y)\big(F(x) \vee \neg G(y)\big) && \text{(扩张作用域)}
\end{aligned}
$$

问: ② 的下述求法是否正确?

$$
\begin{aligned}
(\forall x)F(x) \vee \neg(\exists x)G(x) &\Leftrightarrow (\forall x)F(x) \vee (\forall x)\neg G(x) && (11) \\
&\Leftrightarrow (\forall x)\big(F(x) \vee \neg G(x)\big). && (12)
\end{aligned}
$$

9.31

4 重言蕴含式与推理规则

4.1 重言蕴含式

谓词公式的等价

谓词公式的赋值

谓词公式常由命题变元和个体变元组成.[1] 当个体变元由确定的个体所取代, 命题变元由确定的命题所取代时, 就称作对谓词公式赋值.

Definition 16. 给定任何两个谓词公式 Wff A 和 Wff B, 设它们有共同的个体域 E, 若对 A 和 B 的任一组变元进行赋值, 所得命题的真值都相同, 则称谓词公式 A 和 B 在 E 上是等价的, 并记作: $A \Leftrightarrow B$.

9.32

有效, 不可满足, 可满足

Definition 17. 给定任意谓词公式 A, 其个体域为 E, 如果对于 A 的所有赋值,

1. A 都为真, 则称 A 有效或永真;
2. A 在所有赋值下都为假, 则称 A 永假或不可满足;
3. A 至少在一种赋值下为真, 则称 A 可满足;

9.33

命题公式的推广

命题演算中的等价公式表和蕴含公式表都可以推广到谓词演算中使用. 例如:

$$(\forall x)\big(P(x) \to Q(x)\big) \Leftrightarrow (\forall x)\big(\neg P(x) \vee Q(x)\big) \tag{13}$$

$$(\forall x)P(x) \vee (\exists y)R(x, y) \Leftrightarrow \neg\big(\neg(\forall x)P(x) \wedge \neg(\exists y)R(x, y)\big) \tag{14}$$

$$(\exists x)H(x, y) \wedge \neg(\exists x)H(x, y) \Leftrightarrow \mathbf{F} \tag{15}$$

9.34

[1] 例如谓词公式 $(\forall x)\big(A(x) \vee B\big)$, 包含命题变元和个体变元.

量词与联结词 ¬ 之间的关系

量词转化律:

$$\neg(\forall x)P(x) \Leftrightarrow (\exists x)\neg P(x) \tag{16}$$

$$\neg(\exists x)P(x) \Leftrightarrow (\forall x)\neg P(x) \tag{17}$$

即, 出现在量词之前的否定, 不是否定该量词, 而是否定被量化了的整个命题.

例如, “*这个班所有的同学都参加这次活动*”, 要否定这个命题, 只需要说明 “*存在一个同学没有参加活动*” 就可以了, 而不是 “*所有的同学都没有参加这次活动*”. 即

$$\neg(\forall x)P(x) \ \not\Leftrightarrow \ (\forall x)\neg P(x).$$

9.35

量词与联结词 ¬ 之间的关系

再比如, “任意的 $x \in E$, x 是实数”, 其否定为

“存在 $x \in E$, x 不是实数”.

而不是

“任意的 $x \in E$, x 不是实数”.

量词的转化律, 可以在有限个体域上证明.

设个体域中的个体变元为 $a_1, a_2, \cdots, a_n$, 则

$$\begin{aligned}\neg(\forall x)A(x) &\Leftrightarrow \neg\big(A(a_1) \wedge A(a_2) \wedge \cdots \wedge A(a_n)\big) &(18)\\ &\Leftrightarrow \neg A(a_1) \vee \neg A(a_2) \vee \cdots \vee \neg A(a_n) &(19)\\ &\Leftrightarrow (\exists x)\neg A(x) &(20)\end{aligned}$$

9.36

量词作用域的扩张与收缩

量词的作用域中, 常有合取或析取项, 如果其中一个为命题, 则可以将该命题移至量词作用域之外. 如

$$(\forall x)\big(A(x) \vee B\big) \Leftrightarrow (\forall x)A(x) \vee B, \tag{21}$$

$$(\forall x)\big(A(x) \wedge B\big) \Leftrightarrow (\forall x)A(x) \wedge B, \tag{22}$$

$$(\exists x)\big(A(x) \vee B\big) \Leftrightarrow (\exists x)A(x) \vee B, \tag{23}$$

$$(\exists x)\big(A(x) \wedge B\big) \Leftrightarrow (\exists x)A(x) \wedge B. \tag{24}$$

或者, 量词的作用域中有自由变元时, 也有类似的扩张或收缩. 例如:

$$(\forall x)\big(A(x) \vee B(y)\big) \Leftrightarrow (\forall x)A(x) \vee B(y).$$

9.37

Theorem 18. 下列等价式成立:

$$(\forall x)A(x) \to B \Leftrightarrow (\exists x)\big(A(x) \to B\big) \tag{25}$$

$$(\exists x)A(x) \to B \Leftrightarrow (\forall x)\big(A(x) \to B\big) \tag{26}$$

$$B \to (\forall x)A(x) \Leftrightarrow (\forall x)\big(B \to A(x)\big) \tag{27}$$

$$B \to (\exists x)A(x) \Leftrightarrow (\exists x)\big(B \to A(x)\big) \tag{28}$$

9.38

Example 19. 证明 $(\forall x)A(x) \to B \Leftrightarrow (\exists x)\big(A(x) \to B\big)$

证:

$$\begin{aligned}
(\forall x)A(x) \to B &\Leftrightarrow \neg(\forall x)A(x) \vee B && (E_{16}) \\
&\Leftrightarrow (\exists x)\big(\neg A(x)\big) \vee B && (\text{量词转化律}) \\
&\Leftrightarrow (\exists x)\big(\neg A(x) \vee B\big) && (\text{作用域的扩张}) \\
&\Leftrightarrow (\exists x)\big(A(x) \to B\big) && (E_{16})
\end{aligned}$$

9.39

Example 20. 证明 $B \to (\forall x)A(x) \Leftrightarrow (\forall x)\big(B \to A(x)\big)$

证:

$$\begin{aligned}
B \to (\forall x)A(x) &\Leftrightarrow \neg B \vee (\forall x)A(x) && (E_{16}) \\
&\Leftrightarrow (\forall x)\big(\neg B \vee A(x)\big) && (\text{作用域的扩张}) \\
&\Leftrightarrow (\forall x)\big(B \to A(x)\big) && (E_{16})
\end{aligned}$$

9.40

量词与命题联结词之间的一些等价式

量词分配等价式:

$$(\forall x)\big(A(x) \wedge B(x)\big) \Leftrightarrow (\forall x)A(x) \wedge (\forall x)B(x) \tag{29}$$

$$(\exists x)\big(A(x) \vee B(x)\big) \Leftrightarrow (\exists x)A(x) \vee (\exists x)B(x) \tag{30}$$

注意:

$$(\forall x)\big(A(x) \vee B(x)\big) \not\Leftrightarrow (\forall x)A(x) \vee (\forall x)B(x) \tag{31}$$

$$(\exists x)\big(A(x) \wedge B(x)\big) \not\Leftrightarrow (\exists x)A(x) \wedge (\exists x)B(x) \tag{32}$$

9.41

量词与命题联结词之间的一些蕴含式

$$(\forall x)A(x) \lor (\forall x)B(x) \Rightarrow (\forall x)\big(A(x) \lor B(x)\big) \tag{33}$$

$$(\exists x)\big(A(x) \land B(x)\big) \Rightarrow (\exists x)A(x) \land (\exists x)B(x) \tag{34}$$

Example 21. 设个体域为自然数集合, $A(x)$: x 为奇数; $B(x)$: x 为偶数.

- 则 $(\exists x)A(x)$ 为真, $(\exists x)B(x)$ 为真, 故 $(\exists x)A(x) \land (\exists x)B(x)$ 为真; 但 $(\exists x)\big(A(x) \land B(x)\big)$ 为假. 所以 (34) 式反过来不成立.
- 类似地, $(\forall x)A(x)$ 为假, 且 $(\forall x)B(x)$ 为假, 故 $(\forall x)A(x) \lor (\forall x)B(x)$ 为假; 但 $(\forall x)(A(x) \lor B(x))$ 为真, 所以 (33) 式反过来也不成立.

9.42

量词与命题联结词之间的一些蕴含式

类似还有

$$(\forall x)\big(A(x) \to B(x)\big) \Rightarrow (\forall x)A(x) \to (\forall x)B(x) \tag{35}$$

$$(\forall x)\big(A(x) \rightleftarrows B(x)\big) \Rightarrow (\forall x)A(x) \rightleftarrows (\forall x)B(x) \tag{36}$$

后面我们会给出 (35) 式的证明.

9.43

Example 22. 证明 $E_{29}:\ (\exists x)\big(A(x) \to B(x)\big) \Leftrightarrow (\forall x)A(x) \to (\exists x)B(x)$.

证:

$$\begin{aligned}
(\exists x)\big(A(x) \to B(x)\big) &\Leftrightarrow (\exists x)\big(\neg A(x) \lor B(x)\big) && (E_{16})\\
&\Leftrightarrow (\exists x)\neg A(x) \lor (\exists x)B(x) && (\text{量词的分配})\\
&\Leftrightarrow \neg(\forall x)A(x) \lor (\exists x)B(x) && (\text{量词的转化律})\\
&\Leftrightarrow (\forall x)A(x) \to (\exists x)B(x) && (E_{16})
\end{aligned}$$

9.44

Example 23. 证明 $I_{19}:\ (\exists x)A(x) \to (\forall x)B(x) \Rightarrow (\forall x)\big(A(x) \to B(x)\big)$.

证:

$$\begin{aligned}
(\exists x)A(x) \to (\forall x)B(x) &\Leftrightarrow \neg\big((\exists x)A(x)\big) \lor (\forall x)B(x) && (E_{16})\\
&\Leftrightarrow (\forall x)\neg A(x) \lor (\forall x)B(x) && (\text{量词转化律})\\
&\Rightarrow (\forall x)(\neg A(x) \lor B(x)) && (I_{17})\\
&\Leftrightarrow (\forall x)\big(A(x) \to B(x)\big) && (E_{16})
\end{aligned}$$

9.45

多个量词的使用

等价式:

$$(\forall x)(\forall y)P(x,y) \Leftrightarrow (\forall y)(\forall x)P(x,y) \tag{37}$$

$$(\exists x)(\exists y)P(x,y) \Leftrightarrow (\exists y)(\exists x)P(x,y) \tag{38}$$

蕴含式:

$$(\forall x)(\forall y)P(x,y) \Rightarrow (\exists y)(\forall x)P(x,y) \tag{39}$$

$$(\exists y)(\forall x)P(x,y) \Rightarrow (\forall x)(\exists y)P(x,y) \tag{40}$$

$$(\forall x)(\exists y)P(x,y) \Rightarrow (\exists y)(\exists x)P(x,y) \tag{41}$$

Example 24. 设个体域为实数集合, $P(x,\ y) : x - y = 1$, 则 $(\forall x)(\exists y)P(x,y)$ 为真, 而 $(\exists y)(\forall x)P(x,y)$ 为假, 所以 (40) 反过来不成立.

9.46

4.2 推理规则

谓词演算的推理规则

- 全称指定规则 (US, Universal Specification):

$$\frac{(\forall x)P(x)}{\therefore \quad P(c)} \tag{42}$$

- 全称推广规则 (UG, Universal Generalization):

$$\frac{P(x)}{\therefore \quad (\forall x)P(x)} \tag{43}$$

9.47

谓词演算的推理规则

- 存在指定规则 (ES, Existential Specification):

$$\frac{(\exists x)P(x)}{\therefore \quad P(c)} \tag{44}$$

- 存在推广规则 (EG, Existential Generalization):

$$\frac{P(c)}{\therefore \quad (\exists x)P(x)} \tag{45}$$

9.48

关于 US, ES, EG, UG 的注解

- US, ES 又叫*删除量词规则*, 其作用是在推导中删除量词. 一旦删除了量词, 就可用命题演算的各种规则与方法进行推导.
- UG, EG 的作用则是在推导过程中*添加量词*, 使结论呈量化形式.
- 全称量词与存在量词的基本差别也突出地体现在删除和添加量词规则使用中. 例如, ES 中 $P(c)$ 的 c 取特定值, 而 US 中 $P(c)$ 的 c 可取任意值. 在 UG 规则使用中更要注意这方面的分析才不会引出错误的结论.

9.49

Example 25. 证明 $(\forall x)\big(H(x) \to M(x)\big) \wedge H(s) \Rightarrow M(s)$. 其中

$H(x)$**:** x 是一个人.
$M(x)$**:** x 是要死的.
s**:** 苏格拉底.

证:

(1)	$(\forall x)\big(H(x) \to M(x)\big)$	P
(2)	$H(s) \to M(s)$	US(1)
(3)	$H(s)$	P
(4)	$M(s)$	T(2),(3) I

9.50

Example 26. 构造下面推理的证明: 任何自然数都是整数; 存在着自然数. 所以存在着整数. 个体域为实数集合 R.

证: 先将原子命题符号化: 设 $F(x)$: x 为自然数; $G(x)$: x 为整数. 则前提: $(\forall x)(F(x) \to G(x))$, $(\exists x)F(x)$; 结论: $(\exists x)G(x)$.

(1)	$(\exists x)F(x)$	P
(2)	$F(c)$	ES(1)
(3)	$(\forall x)(F(x) \to G(x))$	P
(4)	$F(c) \to G(c)$	US(3)
(5)	$G(c)$	T(2),(4) I
(6)	$(\exists x)G(x)$	EG(5)

9.51

注意:

- 当既有含存在量词, 又有含全称量词的前提时, 在证明中先引入带存在量词的前提.
- 当有多个含存在量词的前提时, 对每个前提使用 ES 规则所引入的变元应与以前不同.

比如, 如果证明如下进行:

(1)	$(\forall x)(F(x) \to G(x))$	P
(2)	$F(c) \to G(c)$	US(1)
(3)	$(\exists x)F(x)$	P
(4)	$F(c)$	ES(3)
(5)	$G(c)$	T(2),(4) I
(6)	$(\exists x)G(x)$	EG(5)

在 (2) 中取 $c = \sqrt{2}$, 则 $F(\sqrt{2}) \to G(\sqrt{2})$ 为真 (前件假), 而 (4) 中 $F(\sqrt{2})$ 为假,
这样从真的前件推出了假的中间结果. 9.52

Example 27. 构造下面推理的证明:

前提: $(\forall x)(F(x) \to G(x))$, $(\exists x)(F(x) \wedge H(x))$; 结论: $(\exists x)(G(x) \wedge H(x))$

证: (注意, 在证明序列中先引入带存在量词的前提.)

(1)	$(\exists x)(F(x) \wedge H(x))$	P
(2)	$(F(c) \wedge H(c))$	ES(1)
(3)	$(\forall x)(F(x) \to G(x))$	P
(4)	$F(c) \to G(c)$	US(3)
(5)	$F(c)$	T(2) I
(6)	$G(c)$	T(4),(5) I
(7)	$H(c)$	T(2) I
(8)	$G(c) \wedge H(c)$	T(6),(7)
(9)	$(\exists x)(G(x) \wedge H(x))$	EG(8)

9.53

Example 28. 构造下面推理的证明: (个体域为实数集合).

不存在能表示成分数的无理数; 有理数都能表示成分数. 因此, 有理数都不是无理数.

证: 设 $F(x)$: x 为无理数; $G(x)$: x 为有理数, $H(x)$: x 能表示成分数.

前提: $\neg(\exists x)(F(x) \wedge H(x))$, $(\forall x)(G(x) \to H(x))$; 结论: $(\forall x)(G(x) \to \neg F(x))$.

(1)	$\neg(\exists x)(F(x) \wedge H(x))$	P
(2)	$(\forall x)(\neg F(x) \vee \neg H(x))$	T(1) E
(3)	$(\forall x)(H(x) \to \neg F(x))$	T(2) E
(4)	$H(y) \to \neg F(y)$	US(3)
(5)	$(\forall x)(G(x) \to H(x))$	P
(6)	$G(y) \to H(y)$	US(5)
(7)	$G(y) \to \neg F(y)$	T(6),(4) I
(8)	$(\forall x)(G(x) \to \neg F(x))$	UG(7)

注意: 不能对直接对 $\neg(\exists x)(F(x) \wedge H(x))$ 使用 ES 规则. 9.54

Example 29. 证明$(\forall x)\big(C(x) \to W(x) \wedge R(x)\big) \wedge (\exists x)\big(C(x) \wedge Q(x)\big) \Rightarrow (\exists x)\big(Q(x) \wedge R(x)\big)$.

证:

(1)	$(\exists x)\big(C(x) \wedge Q(x)\big)$	P
(2)	$C(a) \wedge Q(a)$	ES(2)
(3)	$(\forall x)\big(C(x) \to W(x) \wedge R(x)\big)$	P
(4)	$C(a) \to W(a) \wedge R(a)$	US(3)
(5)	$C(a)$	T(2) I
(6)	$W(a) \wedge R(a)$	T(4),(5) I
(7)	$Q(a)$	T(2) I
(8)	$R(a)$	T(6) I
(9)	$Q(a) \wedge R(a)$	T(7),(8) I
(10)	$(\exists x)\big(Q(x) \wedge R(x)\big)$	EG

9.55

Example 30. 证明 $(\forall x)\big(P(x) \vee Q(x)\big) \Rightarrow (\forall x)P(x) \vee (\exists x)Q(x)$.

证: 注意到 $(\forall x)P(x) \vee (\exists x)Q(x) \Leftrightarrow \neg(\forall x)P(x) \rightarrow (\exists x)Q(x)$, 下面使用 CP 规则来证明.

(1)	$\neg(\forall x)P(x)$	P(附加前提)
(2)	$(\exists x)\neg P(x)$	T(1) E
(3)	$\neg P(c)$	ES(2)
(4)	$(\forall x)\big(P(x) \vee Q(x)\big)$	P
(5)	$P(c) \vee Q(c)$	US(4)
(6)	$Q(c)$	T(3),(5) I
(7)	$(\exists x)Q(x)$	EG(6)
(8)	$\neg(\forall x)P(x) \rightarrow (\exists x)Q(x)$	CP

9.56

Example 31 (练习). 证明 $(\forall x)\big(A(x) \rightarrow B(x)\big) \Rightarrow (\forall x)A(x) \rightarrow (\forall x)B(x)$.

证: 使用 CP 规则:

(1)	$(\forall x)A(x)$	P(附加前提)
(2)	$A(y)$	US(1)
(3)	$(\forall x)\big(A(x) \rightarrow B(x)\big)$	P
(4)	$A(y) \rightarrow B(y)$	US(3)
(5)	$B(y)$	T(2),(4)
(6)	$(\forall x)B(x)$	UG(5)
(7)	$(\forall x)A(x) \rightarrow (\forall x)B(x)$	CP

9.57