数理逻辑课程整理

吕铭 Lyu Ming

2015 年 12 月 31 日

目录

1 命题逻辑

1.1 命题逻辑的基本定义

1. 术语: 简单命题, 复合命题, 命题变项
   - 合式公式 (Wff, 命题): 有限次递归定义
   - 解释 I: 对于命题的各命题变项指定真值
   - 文字: 命题变项 P 及其否定式 $\neg P$
   - 互补对: P 与 $\neg P$
   - 合 (析) 取式: 一些文字的合 (析) 取组成的公式
2. 逻辑联结词:

联结词	符号	优先级
否定词 (negation)	$\neg$	0
合取词 (conjunction)	$\wedge$	1
析取词 (disjunction)	$\vee$	2
蕴涵词 (implication)	$\rightarrow$	3
双条件词 (biconditional)	$\leftrightarrow$	4
异或	$\bar{\vee}$, $\oplus$	
与非	$\uparrow$	
或非	$\downarrow$	

3. 重言式 (Tautology), 矛盾式, 可满足式 (含重言式)
4. 代入规则: 一个重言式, 对其中所有相同的 命题变项 P 都用一合式公式 X 代换, 其结果仍为一重言式. 记作 $\frac{P}{X}$

1.2 波兰表达式

- 波兰表达式: 所有符号使用前置式
- 逆波兰表达式: 所有符号使用后置式

1.3 命题逻辑的等值性

1. 等值: 若在其中的任一解释下, 公式 A 和 B 的真值都相同. 记作 $A = B$ 或 $A \Leftrightarrow B$
   - 充要条件: $A \leftrightarrow B$ 是重言式
2. 逆命题, 否命题, 逆否命题
   - 一个命题与它的逆否命题等值
   - 一个命题的逆命题与它的否命题等值

1.4 等值公式

1. 基本等值公式 (命题定律):
   - 双重否定率: $\neg\neg P = P$
   - 结合律, 交换律: $\vee, \wedge, \leftrightarrow$
   - 分配率: $\vee$ 对 $\wedge$; $\wedge$ 对 $\vee$, $\rightarrow$ 对 $\rightarrow$
   - 等幂律 (恒等率)
     $P \vee P = P \wedge P = P$
     $P \rightarrow P = P \leftrightarrow P = T$
   - 吸收率
     $P \vee (P \wedge Q) = P$
     $P \wedge (P \vee Q) = P$
   - 摩根率
     $\neg(P \vee Q) = \neg P \wedge \neg Q$
     $\neg(P \wedge Q) = \neg P \vee \neg Q$
     $\neg(P \rightarrow Q) = P \wedge \neg Q$
     $\neg(P \leftrightarrow Q) = \neg P \leftrightarrow Q = P \leftrightarrow \neg Q = (\neg P \wedge Q) \vee (P \wedge \neg Q)$
   - 同一律
     $P \vee F = P \wedge T = T \rightarrow P = T \leftrightarrow P = P$
     $P \rightarrow F = F \leftrightarrow P = \neg P$
   - 零率
     $P \vee T = T; \quad P \wedge F = F$
     $P \rightarrow T = T; \quad F \leftrightarrow P = T$
   - 补余率
     $P \vee \neg P = T; \quad P \wedge \neg P = F$
     $P \rightarrow \neg P = \neg P; \quad \neg P \rightarrow P = P; \quad P \leftrightarrow \neg P = F$
2. 其他常用公式
   $P \rightarrow Q = \neg P \vee Q$
   $P \leftrightarrow Q = (P \rightarrow Q) \wedge (Q \rightarrow P)$
   $P \leftrightarrow Q = (P \wedge Q) \vee (\neg P \wedge \neg Q)$
   $P \leftrightarrow Q = (\neg P \vee Q) \wedge (P \vee \neg Q)$
   $P \rightarrow (Q \rightarrow R) = (P \wedge Q) \rightarrow R$
   $P \rightarrow (Q \rightarrow R) = Q \rightarrow (P \rightarrow R)$
   $(P \rightarrow R) \wedge (Q \rightarrow R) = (P \vee Q) \rightarrow R$

1.5 置换规则

- 子公式: X 是合式公式 A 的一部分, 且 X 本身也是一个合式公式
- 置换: 设 X 为公式 A 的子公式, 用与 X 等值的公式 Y 将 A 中的 X 代替
- 置换规则: 置换前后公式等值

1.6 命题公式与真值表

如何从真值表获得逻辑表达式

- 从 T 来列写, 用 $\vee$ 连接
  $(\bullet \wedge \bullet) \vee (\bullet \wedge \bullet) \vee (\bullet \wedge \bullet)$
- 从 F 来列写, 用 $\wedge$ 连接
  $(\bullet \vee \bullet) \wedge (\bullet \vee \bullet) \wedge (\bullet \vee \bullet)$

1.7 联结词的完备性

1. 真值函项: 所有合式公式关于等值性的等价类
2. 联结词的完备集: 设 C 是一个联结词的集合, 如果任何 n 元 $(n \geq 1)$ 真值函项都可以由仅含 C 中的联结词构成的公式表示, 则称 C 是完备的联结词集合, 或说 C 是联结词的完备集
3. $\{\neg, \vee, \wedge\}, \{\neg, \wedge\}, \{\neg, \vee\}, \{\neg, \rightarrow\}, \{\uparrow\}, \{\downarrow\}$ 是联结词完备集

1.8 对偶式

对于仅使用联结词 $\neg, \vee, \wedge$ 的命题公式,

1. A 作替换 $(\vee, \wedge, T, F) \rightarrow (\wedge, \vee, F, T)$ 得 A^*, A 和 A^* 互为对偶式
2. 对于 $A = A(P_1, \cdots, P_n)$, 记 $A^- = A(\neg P_1, \cdots, \neg P_n)$

3. $\neg(A^*) = (\neg A)^*$, $\neg(A^-) = (\neg A)^-$

4. $(A^*)^* = A$, $(A^-)^- = A$

5. $\neg A = A^{*-}$ (本质是摩根率)

6. $A = B$ 则 $A^* = B^*$

7. $A \to B$ 永真则 $B^* \to A^*$ 永真

8. A 与 A^-; $\neg A$ 与 A^* 同永真, 同可满足

1.9 范式

1. 析取范式: 形如 $A_1 \vee A_2 \vee \cdots \vee A_n$, 其中 A_i 是合取式

2. 合取范式: 形如 $A_1 \wedge A_2 \wedge \cdots \wedge A_n$, 其中 A_i 是析取式

3. 范式定理: 任何一命题公式都存在与之等值的合取范式和析取范式

4. 极小项: n 个命题变项 P_i 组成 $Q_1 \wedge \cdots \wedge Q_n$ 其中 $Q_i = P_i$ 或 $\neg P_i$, 记为 m_k $(0 \le k \le 2^n - 1)$

   - 每个极小项仅在一个解释下为真
   - 极小项两两不等值, 且 $m_i \wedge m_j = F$ $(i \neq j)$
   - $\bigvee_k m_k = T$

5. 极大项: n 个命题变项 P_i 组成 $Q_1 \vee \cdots \vee Q_n$ 其中 $Q_i = P_i$ 或 $\neg P_i$, 记为 M_k $(0 \le k \le 2^n - 1)$

   - 每个极大项仅在一个解释下为假
   - 极小项两两不等值, 且 $m_i \vee m_j = T$ $(i \neq j)$
   - $\bigwedge_k m_k = F$

6. 主析 (合) 取范式: 仅由极小 (大) 项的析 (合) 取构成的析 (合) 取范式称为主析 (合) 取范式

7. 主析 (合) 取范式定理: 任一含有 n 个命题变项的公式, 都存在唯一的与之等值的且恰仅含这 n 个命题变项的主析 (合) 取范式

8. 主范式的转换: 对于各项取极大 (小) 项全集的补集并取非.

9. 空公式:

   - 永真式的主合取范式为空公式
   - 矛盾式的主析取范式为空公式

1.10 推理形式

以符号 (合式公式) 表示的推理关系. 正确的推理形式要求前提真则结论必真.

- 重言蕴含 $\Rightarrow$: 前提 $\Rightarrow$ 结论, 表示公式间的真值关系

- $A \Rightarrow B$ 的充要条件是 $A \to B$ 是永真式 / $A \wedge \neg B$ 是矛盾式

- 基本推理公式

  1. $P \wedge Q \Rightarrow P$
  2. $\neg(P \to Q) \Rightarrow P$: 1 的推论
  3. $\neg(P \to Q) \Rightarrow \neg Q$: 1 的推论
  4. $P \Rightarrow P \vee Q$
  5. $\neg P \Rightarrow P \to Q$ 2 的逆否
  6. $Q \Rightarrow P \to Q$ 3 的逆否
  7. $\neg P \wedge (P \vee Q) \Rightarrow Q$
  8. $P \wedge (P \to Q) \Rightarrow Q$: 假言推理, 分离规则, 7 的变形
  9. $\neg Q \wedge (P \to Q) \Rightarrow \neg P$ 7 的变形
  10. $(P \to Q) \wedge (Q \to R) \Rightarrow P \to R$: 三段论
  11. $(Q \to R) \Rightarrow ((P \vee Q) \to (P \vee R))$
  12. $(Q \to R) \Rightarrow ((P \to Q) \to (P \to R))$
  13. ......

1.11 推理演算

应用如下规则证明推理形式

1. 前提引入规则: 推理过程中可随时引入前提

2. 结论引入规则: 中间结论可作为后续推理的前提

3. 代入规则: 仅限于重言式中的命题变项

4. 置换规则: 利用等值公式对部分公式进行置换

5. 分离规则: 由 A 及 $A \to B$ 成立,, 可将 B 分离出来

6. 条件证明规则: $A_1 \wedge A_2 \Rightarrow B$ 与 $A_1 \Rightarrow A_2 \to B$ 等价

1.12 归结法

仅有一条归结推理规则的机械推理法, 基于 $A \Rightarrow$ 成立等价于 $A \wedge \neg B$ 是矛盾式. 具体步骤:

1. $A \wedge \neg B$ 出发

2. 建立子句集 S: 取合取范式 $A \wedge \neg B = \bigwedge_i C_i$, $S = \{C_i\}$

3. 对于 S 中的子句作归结 (消去互补对), 归结结果放入 S. 重复此步骤

4. 直至归结出矛盾式

其中归结式定义: $C_1 = L \vee C_1'$, $C_2 = \neg L \vee C_2'$ 则归结式 $R(C_1, C_2) = C_1' \vee C_2'$

1.13 命题逻辑的公理化 *

略...

1. 公理系统的结构

    - 初始符号: 公理系统内允许出现的全体符号的集合
    - 形成规则: 公理系统内允许出现的合法符号序列的形成方法与规则
    - 公理: 精选的最基本的重言式, 作为推演其它所有重言式的依据
    - 变形规则: 公理系统所规定的推理规则
    - 建立定理: 公理系统所作演算的主要内容, 包括所有的重言式和对它们的证明

2. 具有代表性的命题逻辑的公理系统

系统名称	年代	公理总条数 *
Russell	1910	5 (4)
Frege	1879	6 (3)
Hilbert—Bernays	1934	15
王浩算法	1959	1**
自然演绎系统		0***

* 括号内是彼此独立的条数;
** 10 条变形规则;
*** 5 条变形规则

3. 完备性: 是否所有的重言式或所有成立的定理都可由所建立的公理系统推导出来

4. 可靠性: 非重言式或者不成立的定理是否也可由所建立的公理系统推导出来

5. 语义完备性, 语义无矛盾性, 命题演算的可判定性

6. 非标准逻辑: 如多值逻辑, 模态逻辑

2 谓词逻辑

1. 个体词: 个体词是指所研究对象中可以独立存在的具体的或抽象的客体.

    - 个体常项 $a, b, c, \cdots$
    - 个体变项 $x, y, z, \cdots$
    - 个体域/论域 D

2. 谓词: 用来刻划个体词的性质或多个个体词间关系的词. 又可看作是由给定的个体域到集合 $\{T, F\}$ 上的一个映射, $P, Q, R, \cdots$

    - 谓词常项, 谓词变项
    - 一元谓词 $P(x)$, 多元谓词 $P(x, y, \cdots)$
    - 命题逻辑中为一个命题是没有个体变项的零元谓词. 谓词逻辑符号中命题变项 $p, q, r, \cdots$

3. 函数: 某一个体域到另一个体域的映射. 谓词逻辑中的函数一般不单独使用, 而是嵌入在谓词中. $P(f(x), g(x))$

4. 量词: 表示个体常项或变项之间数量关系的词

    - 全称量词 (Universal quantifier) $\forall$
    - 存在量词 (xistential quantifier) $\exists$
    - 量词的辖域: 量词所约束的范围称
    - 约束出现: $(\forall x)$ 和 $(\exists x)$ 辖域中, x 的所有出现

- 约束变元: 所有约束出现的变元
- 自由变元: 不是约束出现的其它变元

5. 一阶谓词逻辑: 在所讨论的谓词逻辑中, 限定量词仅作用于个体变项, 不允许量词作用于命题变项和谓词变项, 也不讨论谓词的谓词

6. 合式公式 (谓词公式): 递归定义, 相比命题逻辑特别的 A 是合式公式则, x 是自由变元, 则 $(\forall x)A$, $(\exists x)A$ 也是合式公式

7. 自然语句的形式化

   - 唯一性:
     $(\exists x)(P(x) \wedge (\forall y)(P(y) \rightarrow (x = y)))$
   - 多次量化: 从右至左依次量化

2.1 普遍有效性和判定问题

1. 普遍有效公式: 任何解释下均为真的谓词公式

2. 不可满足公式: 任何解释下均为假的谓词公式

3. 可满足公式: 至少存在一个解释使之为真的谓词公式

4. 普遍有效性的判定:

   - 有限域总能转化为命题逻辑. 普遍有效性依赖于个体域的元素数量.
     - 在 $|D| = k$ 上普遍有效, 则在 $|D'| \leq k$ 上普遍有效
     - 在 $|D| = k$ 上可满足, 则在 $|D'| \geq k$ 上可满足
   - 一阶谓词逻辑不可判定: 对任一谓词公式而言, 没有一个能行的方法判明它是否是普遍有效的. [1]

5. 可判定的一阶逻辑子类包括

   - 仅含一元谓词变项的公式
   - 所有变项都被公式最前置的量词约束, 且仅含一种量词的公式
   - 个体域有穷

[1] 1936 年 Turing 和 Church 分别独立地证明: 一阶谓词逻辑的普遍有效性是半可判定的, 即如果公式本身是普遍有效 (或不可满足) 的, 则存在有限的判定算法, 否则不存在有限的判定算法

2.2 等值性

1. 等值定义: $A \leftrightarrow B$ 是普遍有效的. 记为 $A = B$ 或 $A \Leftrightarrow B$

2. 命题公式替换可以得到一类等值公式

3. 否定型等值公式
   $\neg(\forall x)P(x) = (\exists x)\neg P(x)$
   $\neg(\exists x)P(x) = (\forall x)\neg P(x)$

4. 量词对 $\vee, \wedge, \rightarrow$ 在其中之一是不含个体变元的命题变项 (q) 时满足分配率, 如
   $(\forall x)(P(x) \vee q) = (\forall x)P(x) \vee q$
   $(\exists x)(P(x) \vee q) = (\exists x)P(x) \vee q$

5. $\forall$ 对 $\wedge$, $\exists$ 对 $\vee$ 的分配率
   $(\forall x)(P(x) \wedge Q(x)) = (\forall x)P(x) \wedge (\forall x)Q(x)$
   $(\exists x)(P(x) \vee Q(x)) = (\exists x)P(x) \vee (\exists x)Q(x)$
   弱化的版本
   $(\forall x)(P(x) \vee Q(x)) \Rightarrow (\forall x)P(x) \vee (\forall x)Q(x)$
   $(\exists x)(P(x) \wedge Q(x)) \Rightarrow (\exists x)P(x) \wedge (\exists x)Q(x)$

6. 变元易名的分配率
   $(\forall x)(\forall y)(P(x) \vee Q(y)) = (\forall x)P(x) \vee (\forall x)Q(x)$
   $(\exists x)(\exists y)(P(x) \wedge Q(y)) = (\exists x)P(x) \wedge (\exists x)Q(x)$

2.3 范式

1. 前束范式, 形如:
   $A = (Q_1 x_1) \cdots (Q_n x_n) M(x_1, \cdots, x_n)$
   其中 $Q_i \in \{\forall, \exists\}$; M 不含量词, 称为 A 的基式或母式

2. 前束范式存在定理: 一阶谓词逻辑的任一公式存在与之等值的前束范式 (不唯一)

3. Skolem 标准型, 形如:
   $A = (\exists x_1) \cdots (\exists x_i)(\forall x_{i+1}) \cdots (\forall x_n) M(x_1, \cdots, x_n)$

   - $i \geq 1$: $\exists$ 前束范式: 逻辑完备性的证明
   - $i = 0$: $\forall$ 前束范式 (Skolem 标准型): 归结法的定理证明

4. 存在定理:

   - 一阶谓词逻辑的任一公式 A 都可转化为 $\exists$ 前束范式, 使 A 是普遍有效的当且仅当其 $\exists$ 前束范式是普遍有效的

- 一阶谓词逻辑的任一公式 A 都可转化为 $\forall$ 前束范式, 使 A 是不可满足的当且仅当其 $\forall$ 前束范式是不可满足的

5. 转换为范式的方法:

$$(\exists x)(\forall y)P(x,y) \stackrel{*}{\longleftrightarrow}$$
$$(\exists x)\big((\exists y)(P(x,y)\wedge\neg S(x,y))\vee(\forall z)S(x,z)\big)$$
$$(\exists x)P(x) \stackrel{**}{\longleftrightarrow} P(a)$$
$$(\forall x)(\exists y)P(x,y) \stackrel{**}{\longleftrightarrow} (\forall)P(x,f(x))$$

*: 普遍有效意义下的, 用于 $\exists$ 前束范式
**: 不可满足意义下的, 用于 $\forall$ 前束范式

2.4 推理演算与归结法

1. 全称量词消去和引入 $(\forall x)P(x) \Leftrightarrow P(y)$
2. 存在量词消去和引入 $(\exists x)P(x) \Leftrightarrow P(c)$
3. 归结法:
   (a) $A \to B \Leftrightarrow A \wedge \neg B$
   (b) 由 Skolem 标准型建立子句集 S
   (c) 对 S 进行归结直到出现空子句

3 集合论

1. 集合间关系的形式表示:
   (a) $A = B \Leftrightarrow (\forall x)(x \in A \leftrightarrow x \in B)$
   (b) $A \neq B \Leftrightarrow (\exists x)\neg(x \in A \leftrightarrow x \in B)$
   (c) $A \subseteq B \Leftrightarrow (\forall x)(x \in A \to x \in B)$
   (d) $A \subset B \Leftrightarrow (A \subseteq B \wedge A \neq B)$
2. 集合的运算
   (a) $A \cap B = \{x | x \in A \wedge x \in B\}$
   (b) $A \cup B = \{x | x \in A \vee x \in B\}$
   (c) $A - B = \{x | x \in A \wedge x \notin B\}$
   (d) $-A = E - A = \{x | x \notin A\}$
   (e) $A \oplus B = (A - B) \cup (B - A)$
3. 广义交和广义并
   (a) $\bigcup A = \{x | (\exists z)(z \in A \wedge x \in z)\}$
   (b) $\bigcap A = \{x | (\forall z)(z \in A \to x \in z)\}$
   (c) 定义 $\bigcup\varnothing = \varnothing$, $\bigcap\varnothing$ 无意义
4. 幂集 $P(A) = \{x | x \subseteq A\}$
5. 有序对: $\langle x, y\rangle = \{\{x\}, \{x, y\}\}$
6. 推广 n 元组:
   $\langle x_1, \cdots, x_n\rangle = \langle\langle x_1, \cdots, x_{n-1}\rangle, x_n\rangle$ $(n \neq 2)$
7. 笛卡尔积 $A \times B = \{\langle x, y\rangle | x \in A \wedge y \in B\}$
8. 推广 n 阶笛卡尔积
   $A_1 \times \cdots \times A_n = \{\langle x_1, \cdots, x_n\rangle | x_1 \in A_1 \wedge \cdots \wedge x_n \in A_n\}$
9. 符号优先级依次为
   (a) 一元运算符 $(-A, P(A), \bigcap A, \bigcup A)$
   (b) 二元运算符 $(-, \cap, \cup, \oplus, \times)$
   (c) 集合关系符 $(=, \subseteq, \subset, \in)$
   (d) 一元联结词 $(\neg)$
   (e) 二元联结词 $(\wedge, \vee, \to, \leftrightarrow)$
   (f) 逻辑关系符 $(\Leftrightarrow, \Leftarrow)$
10. 图示法: 文氏图; 幂集图示法; 笛卡尔积图示法

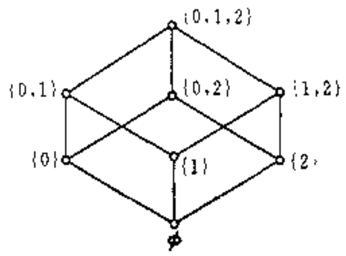

图 1: 幂集图示法

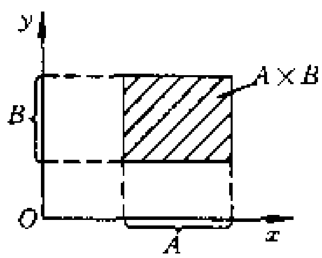

图 2: 笛卡尔积图示法

3.1 集合的运算性质

1. 交换律与结合律 $\cap, \cup$
2. 分配率 $\cap$ 与 $\cup$ 互相
3. 幂等律 $A \cup A = A \cap A = A$
4. 吸收率 $A \cup (A \cap B) = A \cap (A \cup B) = A$
5. 摩根率
   $A - (B \cup C) = (A - B) \cap (A - C)$
   $A - (B \cap C) = (A - B) \cup (A - C)$
6. 同一律 $A \cup \varnothing = A \cap E = A$
7. 零律 $A \cup E = E$, $A \cap \varnothing = \varnothing$
8. 补余率 $A \cup -A = E$, $A \cap -A = \varnothing$
9. 双补律 $-(-A) = A$
10. 差集的性质
    - $A - B = A - (A \cap B)$
    - $A - B = A \cap -B$
    - $A \cup (B - A) = A \cup A$
    - $A \cap (B - C) = (A \cap B) - C$
11. 对称差的性质
    - $A \oplus B = B \oplus A$
    - $(A \oplus B) \oplus C = A \oplus (B \oplus C)$
    - $A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$
    - $A \oplus \varnothing = A$, $A \oplus A = \varnothing$
    - $A \oplus (A \oplus B) = B$

3.2 集合的关系性质

1. 任意集合

$$A \subseteq B \Rightarrow (A \cup C) \subseteq (B \cup C)$$
$$A \subseteq B \Rightarrow (A \cap C) \subseteq (B \cap C)$$
$$(A \subseteq B) \wedge (C \subseteq D) \Rightarrow (A \cup C) \subseteq (B \cup D)$$
$$(A \subseteq B) \wedge (C \subseteq D) \Rightarrow (A \cap C) \subseteq (B \cap D)$$
$$(A \subseteq B) \wedge (C \subseteq D) \Rightarrow (A - C) \subseteq (B - D)$$
$$C \subseteq D \Rightarrow (A - D) \subseteq (A - C)$$

2. 幂集的性质

$$A \subseteq B \Leftrightarrow P(A) \subseteq P(B)$$
$$A = B \Leftrightarrow P(A) = P(B)$$
$$P(A) \in P(B) \Leftrightarrow A \in B$$
$$P(A) \cap P(B) = P(A \cap B)$$
$$P(A) \cup P(B) \subseteq P(A \cup B)$$
$$P(A - B) \subseteq (P(A) - P(B)) \cup \{\varnothing\}$$

3. 广义交和广义并

$$A \subseteq B \Rightarrow \bigcup A \subseteq \bigcup B$$
$$A \subseteq B \Rightarrow \bigcap B \subseteq \bigcap A$$
$$\bigcup (A \cup B) = (\bigcup A) \cup (\bigcup B)$$
$$\bigcup (A \cup B) = (\bigcup A) \cap (\bigcup B)$$
$$\bigcup (P(A)) = A$$

4. 传递集合 $(\forall x)(\forall y)((x \in y \wedge y \in A) \to x \in A)$
   $\Leftrightarrow A \subseteq P(A) \Leftrightarrow P(A)$ 是传递集合
   $\Rightarrow \bigcup A$ 是传递集合 $\Leftarrow A$ 的元素都是传递集合
   $\Rightarrow A \neq \varnothing \to \bigcap A = \varnothing$ (由正则公理导出)
   A 的元素都是传递集合, 则 $\cap A$ 是传递集合
5. 笛卡尔积一般不满足交换律和结合律. $(A \times \varnothing = \varnothing \times A = \varnothing)$
6. $x, y \in A \Rightarrow \langle x, y \rangle \in PP(A) \equiv P(P(A))$
7. 笛卡尔积的性质

$$A \times (B \cup C) = (A \times B) \cup (A \times C)$$
$$A \times (B \cap C) = (A \times B) \cap (A \times C)$$
$$(B \cup C) \times A = (B \times A) \cup (C \times A)$$
$$(B \cap C) \times A = (B \times A) \cap (C \times A)$$
$$A \subseteq B \Leftrightarrow A \times C \subseteq B \times C \Leftrightarrow C \times A \subseteq C \times B$$
$$A \times B \subseteq C \times D \Leftrightarrow A \subseteq C \wedge B \subseteq D$$

3.3 有限集合的基数

1. 有限集合基数 (cardinal number, potency) 记作 $|A| = n$ 或 $\mathrm{card}(A) = n$. $|\varnothing| = 0$
2. $|P(A)| = 2^{|A|}$, $|A \times B| = |A| \cdot |B|$

3. 对于集合 A, B

$$|A \cup B| = |A| + |B| - |A \cap B| \leq |A| + |B|$$
$$|A \cap B| \leq \min(|A|, |B|)$$
$$|A - B| \geq |A| - |B|$$
$$|A \oplus B| = |A| + |B| - 2|A \cap B|$$

3.4 集合公理系统

任一集合的所有元素都是集合, 其他对象用集合定义. 集合论公理系统的目的:

- 判定集合的存在性
- 构造所有合法集合 (合法性)

ZF (Zermelo-Frankel) 集合论公理系统: [2]

1. 外延公理: 集合相等的条件
   $(\forall x)(\forall y)(x = y \leftrightarrow (\forall z)(z \in x \leftrightarrow z \in y)$
2. 空集存在公理: 定义空集
   $(\exists x)(\forall y)(y \notin x)$
   且由外延公理, 空集是唯一的, 记为 $y = \varnothing$
3. 无序对集合存在公理 *:
   $(\forall x)(\forall y)(\exists z)(\forall u)(u \in z \leftrightarrow (u = x \vee u = y))$
4. 并集合存在公理: 集合的广义并的存在性
   $(\forall x)(\exists y)(\forall z)(z \in y \leftrightarrow (\exists u)(z \in u \wedge u \in x))$
5. 子集公理模式 (分离公理模式)*:
   $(\forall x)(\exists y)(\forall z)(z \in y \leftrightarrow (z \in x \wedge P(z)))$
   谓词公式 $P(z)$ 任取 (公理模式), 交集, 差集, 广义交和笛卡儿积 [3] 的存在性
   - 不存在一切集合的集合:
     若存在这样的 A, 由子集公理, 令 $A_0 = \{x | x \in A \wedge x \notin x\}$, 即 $x \in A \Leftrightarrow x \in A \wedge x \neq x$. 令 $x = A_0$ 可得矛盾. ($\bigcap \varnothing$ 不存在)
6. 幂集合公理: 定义幂集 $y = P(x)$
   $(\forall x)(\exists y)(\forall z)(z \in y \leftrightarrow (\forall u)(u \in z \rightarrow u \in x))$
7. 正则公理: (排除奇异集合)
   $(\forall x)(x \neq \varnothing \rightarrow (\exists y)(y \in x \wedge (x \cap y = \varnothing)))$
   称 y 为 x 的极小元
   - $(\forall A)(A \neq A)$
   - $(\forall A_1)(\forall A_2)\neg(A_1 \in A_2 \wedge A_2 \in A_1)$
   - 奇异集合 A 定义:
     存在集合序列 $A_i (i \in \mathbb{N})$, 使得 $A_i \in A \wedge A_{i+1} \in A_i$
   - 满足正则公理等价于不是奇异集合
   - $(\forall A)$ $A \neq \varnothing$ 是传递集合 $\rightarrow \varnothing \in A$
8. 无穷公理: 定义自然数集合 $x = \mathbb{N}$
   $(\exists x)(\varnothing \in x \wedge (\forall y)(y \in x \rightarrow (y \cup \{y\}) \in x))$
   - 这个定义下 $m < n \Leftrightarrow m \subset n$
   - 集合的三歧性: $(\forall x)(\forall y)((x \in A \wedge y \in A) \rightarrow (x \in y \vee x = y \vee y \in x))$. 自然数集合 $\mathbb{N}$ 与每个自然数 $n \in \mathbb{N}$ 都有三歧性
9. 替换公理模式: 子集公理模式的二元推广
   $(\forall x)(\exists! y)P(x, y) \rightarrow (\forall t)(\exists s)\tilde{P}(s, t)$
   其中 $(\exists! y)P(x, y)$ 表示
   $(\exists y)(P(x, y) \wedge (\forall z)(P(x, z) \rightarrow z = y))$
   $\tilde{P}(s, t)$ 表示
   $(\forall u)(u \in s \leftrightarrow (\exists z)(z \in t \wedge P(z, u))$
   - 根据空集定理和幂集定理, $PP(\varnothing)$ 是集合. 令 $P(\varnothing, x) = P(\{\varnothing\}, y) = T$ 得到 (3) 无序对集合存在
   - 令 $P(x, y) = p(x) \wedge (x = y)$ 即为 (5) 子集公理模式
10. 选择公理:
    $(\forall x)(R(x) \rightarrow (\exists u)S(x, u))$
    其中 $R(x)$ 表示
    $(\forall y)\big((y \in x \rightarrow y \neq \varnothing) \wedge (\forall y)(\forall z)((y \in x \wedge z \in x \wedge y \neq z) \rightarrow (y \cap z = \varnothing))\big)$
    $S(x, u)$ 表示
    $(\forall y)(y \in x \rightarrow (\exists! t)(t \in y \wedge t \in u)$.
    - 等价于: 对于任意关系存在子集为函数, 且定义域相等

[2] 其他还有 GB (Godel & Bernays) 公理系统等.

[3] $x \in A \wedge y \in B \Rightarrow \langle x, y \rangle \in PP(A \cup B)$

* 其中 (3) 无序对集合存在与 (5) 子集公理模式可由其他公理导出

3.5 关系的定义

1. 二元关系: 有序对的集合或者空集, 记作 R. $\langle x,y\rangle \in R$ 记作 xRy
2. $A\times B$ 的子集定义 A 到 B 的二元关系; 特别的 $A\times A$ 的子集定义 A 上的二元关系
3. n 元关系: $A_1\times\cdots\times A_n$ 的子集
4. 特殊的二元关系:
   - 恒等关系
$I_A=\{\langle x,x\rangle|x\in A\}$
   - 全关系/全域关系
$E_A=\{\langle x,y\rangle|x\in A\wedge y\in A\}$
   - 空关系 $\varnothing$
5. 定义域 (dom), 值域 (ran) 和域 (fld):
   - $\mathrm{dom}(R)=\{x|(\exists y)(\langle x,y\rangle\in R)\}$
   - $\mathrm{ran}(R)=\{y|(\exists x)(\langle x,y\rangle\in R)\}$
   - $\mathrm{fld}(R)=\mathrm{dom}(R)\cup\mathrm{ran}(R)=(\bigcup\bigcup R)$
6. 关系的逆 R^{-1}
$R^{-1}=\{\langle x,y\rangle|\langle y,x\rangle\in R\}$
7. 关系的合成 $S\circ R$
$S\circ R=\{\langle x,z\rangle|(\exists y)(\langle x,y\rangle\in R\wedge\langle y,z\rangle\in S)\}$
   - $R_1\circ(R_2\cup R_3)=R_1\circ R_2\cup R_1\circ R_3$
   - $R_1\circ(R_2\cap R_3)\subseteq R_1\circ R_2\cap R_1\circ R_3$
   - $(R_1\cup R_2)\circ R_3=R_1\circ R_3\cup R_2\circ R_3$
   - $(R_1\cap R_2)\circ R_3\subseteq R_1\circ R_3\cap R_2\circ R_3$
8. 关系在集合上的限制 $R\upharpoonright A$
$R\upharpoonright A=\{\langle x,y\rangle|\langle x,y\rangle\in R\wedge x\in A\}$
9. 集合在关系下的象 $R[A]$
$R[A]=\{y|(\exists x)(x\in A\wedge\langle x,y\rangle\in R\}$
   - $R[\bigcup A]=\bigcup\{R[B]|B\in A\}$
   - $R[\bigcap A]\subseteq\bigcap\{R[B]|B\in A\}$
   - $R[A]-R[B]\subseteq R[A-B]$
10. 关系矩阵 $\boldsymbol{M}(R)$: 对于 $R\subseteq X\times Y$, $\boldsymbol{M}(R)=(r_{ij})_{|X|\times|Y|}$, 其中
$$r_{ij}=\begin{cases}1, & \langle x_i,y_j\rangle\in R\\ 0, & \langle x_i,y_j\rangle\notin R\end{cases}$$
    - 布尔数域上 $\boldsymbol{M}(S\circ R)=\boldsymbol{M}(R)\boldsymbol{M}(S)$
11. 关系图 $G(R)=\langle V,E\rangle$ (有向图): 对于 $R\subseteq X\times Y$, $V=X\cup Y$, $E=\{e_{ij}|\langle x_i,y_j\rangle\in R\}$

3.6 关系的性质

R 在 A 上:

1. 自反: $(\forall x)(x\in A\to xRx)$
   - R_1,R_2 是自反的, 则 $R_1^{-1},R_1\cap R_2,R_1\cup R_2$ 也是自反的
2. 非自反: $(\forall x)(x\in A\to x\not R x)$
3. 对称: $(\forall x)(\forall y)((x\in A\wedge y\in A\wedge xRy)\to yRx)$
   - R_1,R_2 是对称的, 则 $R_1^{-1},R_1\cap R_2,R_1\cup R_2$ 也是对称的
   - R 是对称的, 则 $R^{-1}=R$
4. 反对称: $(\forall x)(\forall y)((x\in A\wedge y\in A\wedge xRy\wedge yRx)\to x=y)$
   - R_1,R_2 是反对称的, 则 $R_1^{-1},R_1\cap R_2$ 也是反对称的
   - R 是反对称的, 则 $R\cap R^{-1}=I_A$
5. 传递: $(\forall x)(\forall y)(\forall z)((x\in A\wedge y\in A\wedge z\in A\wedge xRy\wedge yRz)\to xRz)$
   - R_1,R_2 是传递的, 则 $R_1^{-1},R_1\cap R_2$ 也是传递的

3.7 关系的闭包

1. 递归推广关系合成到 R^n
2. 定理:
   - 有限集合 A 上的关系 R, 存在自然数 $s\neq t$ 使 $R^s=R^t$ (鸽巢原理)

表 1: 关系的特征

	自反 Reflexive (10.4.1)	非自反 Irreflexive (10.4.1)	对称 Symmetric (10.4.2)	反对称 Antisymmetric (10.4.2)	传递 Transitive (10.4.3)
定义要点	$x \in A \to xRx$	$x \in A \to x \not R x$ $\langle x, x\rangle \notin R$	$xRy \to yRx$ $\langle x, y\rangle \in R \to \langle y, x\rangle \in R$	$xRy \wedge x \neq y \to y \not R x$ $xRy \wedge yRx \to x = y$	$xRy \wedge yRz \to xRz$ $\langle x, y\rangle \in R \wedge \langle y, z\rangle \in R \to \langle x, z\rangle \in R$
关系矩阵的特点	$r_{ii} = 1$ 主对角元均为1	$r_{ii} = 0$ 主对角元均为0	对称矩阵 $r_{ij} = r_{ji}$	若 $r_{ij} = 1 \wedge i \neq j \to r_{ji} = 0$	无直观特点或难以直接判断
关系图的特点	每个结点都有自圈	每个结点都没有自圈	若两个结点之间有边，一定是一对方向相反的边	若两个结点之间有边，一定是一条有向边	若从结点x_i到x_j有边，x_j到x_k有边，则从x_i到x_k一定有边

关系 \ 性质	自反性	非自反性	对称性	反对称性	传递性
恒等关系 I_A	√	×	√	√	√
全域关系 E_A	√	×	√	×	√
A上的空关系 Φ	×	√	√	√	√
N上的整除关系	√	×	×	√	√
包含关系 $\subseteq$	√	×	×	√	√
真包含关系 $\subset$	×	√	×	√	√

表 2: 关系的运算特征

运算 \ 性质	自反性	非自反性	对称性	反对称性	传递性
R^{-1}	√	√	√	√	√
$R_1 \cap R_2$	√	√	√	√	√
$R_1 \cup R_2$	√	√	√	×	×
$R_1 - R_2$	√	√	√	√	×
$R_1 \circ R_2$	√	×	×	×	×

- $p = |s - t|$, $B = \{R^0 = I_A, R^1, \cdots, R^{t-1}\}$, 则 $(\forall q)(q \in \mathbb{N} \to R^q \in B)$

3. 闭包: 对于 $A \neq \varnothing$ 上的关系 R, 若 R' 满足

   (a) R' 是自反的 (对称的, 传递的)

   (b) $R \subseteq R'$

   (c) $(\forall R'')$ R'' 是 A 上自反的 (对称的, 传递的) 关系, $R \subseteq R'' \to R' \subseteq R''$

   则称 R' 为关系 R 的自反 (对称, 传递) 闭包, 记作 $r(R)$ ($s(R)$, $t(R)$)

4. 闭包的性质

   - R 是自反的 (对称的, 传递的) 等价于其闭包是自身
   - $R_1 \subseteq R_2 \to x(R_1) \subseteq x(R_x)$. $(x = r, s, t)$
   - $r(R_1) \cup r(R_2) = r(R_1 \cup R_2)$
   - $s(R_1) \cup s(R_2) = s(R_1 \cup R_2)$
   - $t(R_1) \cup t(R_2) \subseteq t(R_1 \cup R_2)$
   - R 是自反的, 则 $s(R)$ 和 $t(R)$ 是自反的
   - R 是对称的, 则 $r(R)$ 和 $t(R)$ 是对称的
   - R 是传递的, 则 $r(R)$ 是传递的
   - $rs(R) = sr(R)$
   - $rt(R) = tr(R)$
   - $st(R) \subseteq ts(R)$

5. 闭包的构造

   - $r(R) = R \cup R^0$
   - $s(R) = R \cup R^{-1}$
   - $t(R) = R \cup R^2 \cup R^3 \cup \cdots$

   特别的, 存在 $k \leq n$ 使 $t(R) = R \cup \cdots \cup R^k$

6. 传递闭包构造的 Warshall 算法

Listing 1: Warshall 算法

```
for i=1 to n, j=1 to n, k=1 to n
        r_jk = r_jk ∨ (r_ji ∧ r_ik)
```

3.8 等价关系和划分

1. 等价关系: 自反, 对称和传递的关系
2. 等价类 $[x]_R = \{y | y \in A \wedge xRy\}$, 或记作 $[x], \overline{x}$
3. 全部等价类的集合: 商集, 记作 A/R
4. 划分 π (不多, 非空, 不漏, 不重):
   (a) $(\forall x)(x \in \pi \to x \subseteq A)$
   (b) $\varnothing \notin \pi$
   (c) $\bigcup \pi = A$
   (d) $(\forall x)(\forall y)((x \in \pi \wedge y \in \pi \wedge x \neq y) \to x \cap y - \varnothing)$
5. 等价类是一个划分
6. 等价关系诱导划分 π_R; 划分诱导等价关系 R_π.
7. $\pi = \pi_R \leftrightarrow R = R_\pi$

3.9 相容关系和覆盖

1. 相容关系: 自反和对称的关系
2. 相容类 $C = \{x | x \in A \wedge (\forall y)(y \in C \to xRy)\}$
3. 最大相容类 C_R 不是任何相容类的真子集
   $(\forall x)(x \in A - C_R \to (\exists y)(y \in C_R \wedge x \not R y))$
4. 非空有限集合上的任何相容类存在最大相容类超集
5. 覆盖 Ω (不多, 非空, 不漏):
   (a) $(\forall x)(x \in \Omega \to x \subseteq A)$
   (b) $\varnothing \notin \Omega$
   (c) $\bigcup \Omega = A$
6. 完全覆盖: 最大相容类的集合 $C_R(A)$. 完全覆盖是唯一的

3.10 偏序关系与上下界

1. 偏序关系: 自反, 反对称, 传递的关系, 记作 $\leq$
2. 拟序关系: 非自反, 传递的关系, 记作 $<$
   - 拟序关系是反对称的
3. 对于拟序关系 R, $R \cup R^0$ 是偏序关系
4. 对于偏序关系 R, $R - R^0$ 是拟序关系
5. A 和 A 上关系 R 称为结构 $\langle A, R \rangle$. 偏序结构或称偏序集
6. 盖住: 对于偏序集 $\langle A, \leq \rangle$, 对于 $x, y \in A$ 且 $x \leq y \wedge x \neq y$, 如果 $\neg(\exists z)(x \leq z \leq y)$, 则称 y 盖住 x
7. A 上的盖住关系 $\mathrm{cov}A = \{\langle x, y \rangle$ 是唯一的
8. 哈斯 (Hasse) 图
   (a) 每个顶点代表一个元素
   (b) $x \leq y$ 且 $x \neq y$ 则 y 在 x 的上方
   (c) $\langle x, y \rangle \in \mathrm{cov}A$ 则连无向边
9. 对于偏序关系 $\langle A, \leq \rangle$, 且 $B \subseteq A$
   (a) $(\exists y)(y \in B \wedge (\forall x)(x \in B \to y \leq x))$: y 为 B 的最小元
   (b) $(\exists y)(y \in B \wedge (\forall x)(x \in B \to x \leq y))$: y 为 B 的最大元
   (c) $(\exists y)(y \in B \wedge (\forall x)((x \in B \wedge x \leq y) \to x = y))$: y 为 B 的极小元
   (d) $(\exists y)(y \in B \wedge (\forall x)((x \in B \wedge y \leq x) \to x = y))$: y 为 B 的极大元
   (e) 最小 (大) 元不一定存在, 存在必定唯一; 极小 (大) 元一定存在, 不一定唯一
   (f) $(\exists y)(y \in A \wedge (\forall x)(x \in B \to x \leq y))$: y 为 B 的上界
   (g) 上确界 (最小上界): 上界集合的最小元
   (h) $(\exists y)(y \in A \wedge (\forall x)(x \in B \to y \leq x))$: y 为 B 的下界
   (i) 下确界 (最小下界): 下界集合的最大元
   (j) 上下界不一定存在, 不一定唯一; 上下确界不一定存在, 存在一定唯一

3.10.1 全系关系

1. 可比的: $x \leq y \vee y \leq x$

2. 全序关系 (线序关系): 任意两个元素可比. 全序集

3. 对于偏序关系 $\langle A, \leq \rangle$, 且 $B \subseteq A$

   (a) 链 B: 元素都可比. 链的长度

   (b) 反链 B: 元素都不可比. 反链的长度

4. $\langle A, \leq \rangle$ 中最长链的长度 n, 则将元素分成不相交的反链, 反链的个数至少是 n.
   极大元的集合是一条反链. 据此做数学归纳可证明

3.10.2 良序关系

1. 良序关系: 任何非空子集都有最小元. 良序集

2. 良序集一定是全序集. 取二元子集可证

3. 有限全序集一定是良序集

4. 良序化: 定义良序关系

5. 任意集合都可以良序化 (由选择公理证明)