



华南理工大学
South China University of Technology

离散数学

作者：夏同

学院：计算机科学与工程学院

班级：1 班

学号：202530451676

日期：2025 年 12 月 3 日

厚德尚学 自强不息
务实创新 追求卓越

目录

第一章 命题逻辑	1
1.1 命题与命题公式	1
1.2 命题演算的关系式	4
1.3 析取范式, 合取范式	7
第二章 谓词逻辑	9
2.1 谓词逻辑基本概念	9
2.2 换名, 前束范式	11
2.3 谓词公式的等价和蕴含关系式	13
第三章 集合与关系	16
3.1 集合	16
3.2 集合的笛卡尔积	22
3.3 关系	24
3.4 自反, 对称, 传递关系, 闭包	30
3.5 Warshell 算法	34
3.6 等价关系, 等价类, 覆盖和划分	37
3.7 偏序关系, 全序关系, 良序关系	40
第四章 函数	44
4.1 函数(映射)的定义与表示	44
4.2 单/满/双射, 反函数, 复合	47
4.3 自然数	50
4.4 集合的基数, 等势	51
第五章 图论	56
5.1 图的基本概念	56
5.2 特殊图	62
5.3 树	62

第一章 命题逻辑

1.1 命题与命题公式

定义 1.1.1 命题

命题是用陈述句表示的一个为真或者为假，但不能同时为真又为假的判断语句

一个语句是命题，关键在于它是否在“逻辑上”具有一个确定的真值（即要么为真，要么为假），而不取决于我们是否知道或能够验证这个真值。只要一个陈述句在原则上可能为真或为假，即使我们目前无法判断（例如由于科学限制或信息不足），它仍然是一个命题。

比如“除了地球以外的其他星球有生物”，好像我们还不知道真假，但是我们知道，它有一个潜在的真值：要么其他星球上存在生物（真），要么不存在（假）。尽管我们目前无法证实或证伪这个陈述，但它的真值是客观存在的，不会同时为真又为假。

而语句“ $2 + x = 5$ ”，我们从逻辑上无法认为它一定为真，或者一定为假，因为 x 是变元，有时这个式子成立，有时不成立，因此这个语句不是命题。

除此以外，问句，感叹句，祈使句表示的语义不具备真值，不是命题。比如“多漂亮的花啊！”这句话，有的人觉得好看，有的人觉得不好看，所以它没有确定的真值，不是命题。

定义 1.1.2 悖论

悖论是用陈述句表示的一个如果为真则推出为假、如果为假则推出为真，从而无法一致地分配真值的判断语句。

比如著名的理发师悖论等

定义 1.1.3 原子命题（简单命题）

原子命题是不能被分解为更简单命题的命题，它不包含任何逻辑联结词，是构成复合命题的基本单位。

原子命题（简单命题）的特点是它的真值是内在的、最基本的，不依赖于其他命题。例如：“今天是星期五。”和“雪是白的。”

定义 1.1.4 复合命题

复合命题是由一个或一个以上的原子命题（简单句）通过逻辑联结词（如“并非”、“并且”、“或者”、“如果…那么…”、“当且仅当”等连词）组合而成的命题。

复合命题的真值则完全由其包含的原子命题的真值以及所使用的逻辑联结词的规则共同决定。例如：“今天是星期五并且天气很好。”这个复合命题的真假，取决于“今天是星期五”和“天气很好”这两个原子命题的真假以及“并且”这个词的逻辑含义。

定义 1.1.5 逻辑联结词

逻辑联结词是用来连接一个或多个命题，从而构成更复杂的复合命题的逻辑运算符。它们定义了原子命题之间的逻辑关系，并决定了复合命题的真值。

1. **否定联结词** (\neg , 读作“非”): 表示对原命题的否定。命题 $\neg P$ 为真，当且仅当命题 P 为假。
2. **合取联结词** (\wedge , 读作“且”或“与”): 表示两个命题同时成立。命题 $P \wedge Q$ 为真，当且仅当 P 和 Q 同时为真。
3. **析取联结词** (\vee , 读作“或”): 表示两个命题至少有一个成立。命题 $P \vee Q$ 为真，当且仅当 P 和 Q 至少有一个为真（此为“相容或”，即允许两者同时为真）。
4. **蕴涵联结词** (\rightarrow 或 \supset , 读作“如果…那么…”): 表示前一个命题是后一个命题的充分条件。命题 $P \rightarrow Q$ 为假，当且仅当 P 为真而 Q 为假；其余情况均为真。
5. **等价联结词** (\leftrightarrow , 读作“当且仅当”): 表示两个命题互为充分必要条件。命题 $P \leftrightarrow Q$ 为真，当且仅当 P 和 Q 的真值相同（即同真或同假）。
6. **与非联结词** (\uparrow , 读作“与非”): 表示合取的否定。命题 $P \uparrow Q$ 为真，当且仅当 P 和 Q 不同时为真。其真值等价于 $\neg(P \wedge Q)$ 。
7. **或非联结词** (\downarrow , 读作“或非”): 表示析取的否定。命题 $P \downarrow Q$ 为真，当且仅当 P 和 Q 同时为假。其真值等价于 $\neg(P \vee Q)$ 。
8. **异或联结词** (\oplus , 读作“异或”): 表示不相容的析取。命题 $P \oplus Q$ 为真，当且仅当 P 和 Q 的真值不同（即一真一假）。其真值等价于 $(P \wedge \neg Q) \vee (\neg P \wedge Q)$ 。

比如“登录服务器必须输入一个有效的口令”，符号化后就是：令 P : 登录服务器， Q : 输入一个有效的口令，符号化： $P \rightarrow Q$ ，需要注意后者是必要不充分条件，因为输入口令后，可能还需要其它步骤才能登陆服务器。

有的人不理解的可能是因为蕴含前件为假时，蕴含式总为真。这个定义源于我们对“承诺”或“规则”是否被违反的判断。逻辑学中的蕴涵式 $P \rightarrow Q$ 可以看作一个“承诺”：如果 P 成立，则我保证 Q 也成立。这个承诺的真假，取决于在 P 成立的情况下，我是否履行了承诺。如果 P 是假的，那么前提条件就没有被满足，这个规则或承诺就自动进入“不适用”或“未被激活”的状态。既然承诺没有被激活，那么我们自然不能说它被违反了。在逻辑上，我们便将“未被违反”的状态定义为“真”。

定义 1.1.6 逻辑联结词的运算优先级

$\neg > \wedge > \vee > \rightarrow > \leftrightarrow$ ，合取优先级大于析取优先级。

给定一个含有 n 个命题变元的命题公式，易得这 n 个命题变元共有 2^n 种不同的赋值，将命题

公式在所有赋值下的真值列成一个表，成为该命题的真值表，所以真值表有 2^n 行，真值表实际上定义了一个函数，从 2^n 种赋值映射到一个真值（真或假）。对于每种赋值，函数的输出可以是真或假两种选择。因此，所有可能的函数数量是 2^{2^n} 个。这意味着，对于 n 个命题变元，存在 2^{2^n} 个不同的真值表。

定义 1.1.7（最小）全功能联结词集

在命题逻辑中，一个联结词集合被称为全功能联结词集，当且仅当该集合中的联结词足以表达所有可能的真值函数。换句话说，使用该集合中的联结词可以构造出任意的命题公式，并能够表示所有可能的 2^{2^n} 个不同的真值表（其中 n 为命题变元的个数）。如果从一个全功能联结词集中移除任何一个联结词后，剩下的联结词集合不再是全功能的，则称该集合为最小全功能联结词集。

列举所有的最小全功能联结词集： $\{\neg, \wedge\}$, $\{\neg, \vee\}$, $\{\neg, \rightarrow\}$, $\{\uparrow\}$ （与非集）, $\{\downarrow\}$ （或非集）。考试一般考选择题，归纳出特点就是：一定要出现否定（或者包含有），析取、合取、蕴含这三个出现一个就行，不出现时必然是单一的 $\{\uparrow\}$ （与非集）, $\{\downarrow\}$ （或非集）。

特别的，异或 $\{\oplus\}$ 不是最小全功能联结词集，甚至不是全功能联结词集。事实上，命题的真值只有 0 和 1，而恰好异或运算有一个重要特性：当输入的真值变化时，输出总是以“可预测的线性方式”变化。具体来说，如果我们只使用异或运算，无论怎么组合，得到的结果都只能表达“奇偶校验”类型的关系——即计算输入中 1 的个数是奇数还是偶数。这种运算无法表达更复杂的逻辑关系，比如“两个输入必须同时为 1”（与运算）或“至少一个输入为 1”（或运算）。

为什么与运算和或运算更强大呢？因为它们能表达“非线性”的关系。与运算 $P \wedge Q$ 要求两个输入必须同时满足条件，这不是简单的奇偶关系。同样，或运算 $P \vee Q$ 允许至少一个条件满足，这也超出了异或的能力范围。

而与非运算 \uparrow 和或非运算 \downarrow 之所以强大，是因为它们内在包含了“否定”的能力。例如，单用与非运算就能表示否定： $\neg P = P \uparrow P$ 。一旦能够表示否定，再加上它们原有的组合能力，就可以构造出所有其他逻辑运算，包括与、或、蕴含等。

例题 1.1.1

证明 $\{\uparrow\}$ （与非集）, $\{\downarrow\}$ （或非集）是最小全功能联结词集

解 1.1.1.

$$\neg P \Leftrightarrow P \uparrow P$$

$$P \wedge Q \Leftrightarrow (P \uparrow Q) \uparrow (P \uparrow Q)$$

$$P \vee Q \Leftrightarrow (P \uparrow P) \uparrow (Q \uparrow Q)$$

$$P \rightarrow Q \Leftrightarrow P \uparrow (Q \uparrow Q)$$

$$P \leftrightarrow Q \Leftrightarrow (P \uparrow (Q \uparrow Q)) \uparrow ((Q \uparrow (P \uparrow P)) \uparrow (Q \uparrow (P \uparrow P)))$$

类似地：

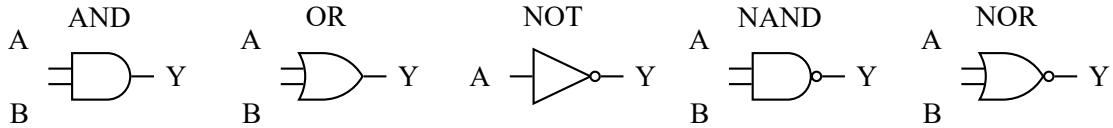
$$\neg P \Leftrightarrow P \downarrow P$$

$$P \vee Q \Leftrightarrow (P \downarrow Q) \downarrow (P \downarrow Q)$$

$$P \wedge Q \Leftrightarrow (P \downarrow P) \downarrow (Q \downarrow Q)$$

$$P \rightarrow Q \Leftrightarrow (P \downarrow P) \downarrow Q$$

$$P \Leftrightarrow Q \Leftrightarrow ((P \downarrow P) \downarrow Q) \downarrow ((Q \downarrow Q) \downarrow P)$$



1.2 命题演算的关系式

$P \Leftrightarrow Q$ (逻辑等价) 的定义是: $P \Leftrightarrow Q$ 为永真式/重言式; $P \Rightarrow Q$ (逻辑蕴含) 的定义是: $P \rightarrow Q$ 为永真式;

证明两个命题公式等价, 方法是: 1. 比较真值表; 2. 等价运算 (使用等价符号 \Leftrightarrow)

置换规则: 它允许在逻辑公式中, 用逻辑等价的子公式替换另一个子公式, 而不改变原公式的真值。

定义 1.2.1 对偶式

在命题逻辑中, 设 A 是一个仅包含联结词 \neg (否定)、 \wedge (合取) 和 \vee (析取) 的命题公式。 A 的对偶式是通过将 A 中所有的 \wedge 替换为 \vee , 所有的 \vee 替换为 \wedge , 同时将所有的 1 (真) 替换为 0 (假), 所有的 0 (假) 替换为 1 (真) 而得到的新公式, 记作 A^*

定理 1.2.1 对偶式的性质

设 A 和 B 是仅包含联结词 \neg 、 \wedge 和 \vee 的命题公式, A^* 和 B^* 分别是它们的对偶式

1. 对偶原理: 若 $A \Leftrightarrow B$, 则 $A^* \Leftrightarrow B^*$ 。逻辑等价关系在对偶变换下保持不变。
2. 否定与对偶的关系: $A \Leftrightarrow (A^*)^*$, 即 A 的对偶式的对偶式等于 A 本身。
3. 永真式与永假式的对偶: 若 A 永真, 则 A^* 永假; 若 A 永假, 则 A^* 永真。
4. 对偶式的否定: $\neg A \Leftrightarrow (\neg A^*)^*$, 其中 $\neg A^*$ 表示先将 A 中的原子命题取否定, 再求对偶式。
5. 对偶式的运算: $(A \wedge B)^* = A^* \vee B^*$, $(A \vee B)^* = A^* \wedge B^*$, $(\neg A)^* = \neg(A^*)$
6. $A \Rightarrow B$ 的充分必要条件是 $B^* \Rightarrow A^*$

性质 5 是由定义导出的, 性质 4 是因为否定运算在对偶变换下保持不变, 对偶式定义只涉及交换 \wedge 和 \vee , 性质 3 更显然, 因为永真式为 1, 永假式为 0, 对偶变换后显然颠倒。

下面证明性质 6, 第一步: 证明如果 $A \Rightarrow B$, 则 $B^* \Rightarrow A^*$, 由于 $A \Rightarrow B$, 所以 $A \rightarrow B$ 是永真式。根据对偶式的性质, 永真式的对偶是永假式, 因此 $(A \rightarrow B)^*$ 是永假式, 将蕴含式转换为基本联结词: $A \rightarrow B \Leftrightarrow \neg A \vee B$, 所以 $(\neg A \vee B)^*$ 是永假式, 根据对偶式的定义: $(\neg A \vee B)^* = (\neg A)^* \wedge B^* = \neg A^* \wedge B^*$, 因此 $\neg A^* \wedge B^*$ 是永假式, 这意味着对于所有赋值, $\neg A^* \wedge B^*$ 都为假。两边同时取否定得到 $\neg A^* \rightarrow \neg B^*$ 为真, 即 $B^* \rightarrow A^*$ 为永真式, 所以 $B^* \Rightarrow A^*$ 。第二步: 证明如果 $B^* \Rightarrow A^*$, 则 $A \Rightarrow B$ 由于 $B^* \Rightarrow A^*$, 根据第一步的结论 (将 A 替换为 B^* , B 替换为 A^*), 我们有: $(A^*)^* \Rightarrow (B^*)^*$, 根据对偶式的性质, $(A^*)^* = A$, $(B^*)^* = B$, 所以 $A \Rightarrow B$ 。综上, $A \Rightarrow B$ 当且仅当 $B^* \Rightarrow A^*$ 。

定理 1.2.2 重要等价关系

1. 基本等价关系

双重否定律: $\neg\neg P \Leftrightarrow P$

等幂律 (幂等律): $P \vee P \Leftrightarrow P, P \wedge P \Leftrightarrow P$

交换律: $P \vee Q \Leftrightarrow Q \vee P, P \wedge Q \Leftrightarrow Q \wedge P$

结合律: $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R), (P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$

分配律: $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R), P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$

吸收律: $P \vee (P \wedge Q) \Leftrightarrow P, P \wedge (P \vee Q) \Leftrightarrow P$

德摩根律: $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q, \neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$

2. 常元相关等价关系

零元律: $P \vee 1 \Leftrightarrow 1, P \wedge 0 \Leftrightarrow 0$ 同一律: $P \vee 0 \Leftrightarrow P, P \wedge 1 \Leftrightarrow P$

排中律: $P \vee \neg P \Leftrightarrow 1$ 矛盾律: $P \wedge \neg P \Leftrightarrow 0$

3. 蕴含与等价关系

蕴含等值式: $P \rightarrow Q \Leftrightarrow \neg P \vee Q$ (“ P 发生且 Q 不发生”是不可能的)

逆否等值式: $P \rightarrow Q \Leftrightarrow \neg Q \rightarrow \neg P$

等价等值式: $P \leftrightarrow Q \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$

等价否定等值式: $P \leftrightarrow Q \Leftrightarrow \neg P \leftrightarrow \neg Q$

归谬论: $(P \rightarrow Q) \wedge (P \rightarrow \neg Q) \Leftrightarrow \neg P$ (不可能同时蕴含正反面)

4. 其他重要等价关系

输出律: $(P \wedge Q) \rightarrow R \Leftrightarrow P \rightarrow (Q \rightarrow R)$

应该注意, 形如 $A \Leftrightarrow B, A \Rightarrow B$ 不是命题公式, 而是命题关系式。而应用这些等价关系式可以证明公式互相等价, 或者求主析取范式, 主合取范式。解题过程中应该利用等价符号。

但是当题目要证明“若 p 则 q ”这样的蕴含关系, 就可以出新的考题。我们可以将要证明的蕴含关系利用蕴含式写出来, 再证明其永真 (解题过程中应该利用等价符号), 这就需要用到等价关系式 (或者真值表)。

但是, 当转化出来的命题公式的蕴含前件或者后件中含有较多的命题变元, 就需要使用推理定律, 并使用编号 1234 一步步写出推理过程, 而不是这里的等价关系式, 解题过程中也不应该出现等价符号。考试一般考“利用构造法验证推理是否有效”(指的是构造定理证明系统)。

上面提到的输出律, 即 **CP 规则**:

定理 1.2.3 CP 规则 (附加前提规则)

对于任意公式 $A_1, A_2, \dots, A_n, B, C$, 如果 A_1, A_2, \dots, A_n, B 可以推出 C , 则 A_1, A_2, \dots, A_n 可以推出 $B \rightarrow C$ 。

这意味着, 如果我们能从前提集合和临时假设 B 推导出 C , 那么我们就能从原前提集合推导出条件语句 $B \rightarrow C$, 而不再依赖假设 B 。

除了这个规则外，还有若干规则需要遵循：

1. 前提引入规则：在证明的任何步骤中，可以随时引入已知的前提条件。在证明过程中，并不需要用完所有给定的前提。关键是选择能够有效推导出结论的前提组合。当前提自身存在矛盾时，并不影响这个规则的合理性，因为矛盾本身已经足以推出任何结论。
2. 结论引入规则：从已知条件出发，通过有效的推理规则推导出新的结论。
3. 置换规则：在证明过程中，可以用逻辑等价的公式替换原公式，而不改变推理的有效性。最后的置换规则恰恰给出了推理中“不允许使用等价符号”的替代方案。

定理 1.2.4 蕴含关系式

1. 化简律： $P \wedge Q \Rightarrow P$ （或 $P \wedge Q \Rightarrow Q$ ），（抓住重点，忽略次要）
2. 附加律： $P \Rightarrow P \vee Q$ ，（有真则真，多说不妨）
3. 假言推理（分离规则）： $(P \rightarrow Q) \wedge P \Rightarrow Q$ （有条件就执行）
4. 拒取式： $(P \rightarrow Q) \wedge \neg Q \Rightarrow \neg P$ （结果不成立，前提必为假）
5. 假言三段论： $(P \rightarrow Q) \wedge (Q \rightarrow R) \Rightarrow (P \rightarrow R)$ （环环相扣）
6. 析取三段论： $(P \vee Q) \wedge \neg P \Rightarrow Q$ （非此即彼）
7. 构造性二难： $(P \rightarrow Q) \wedge (R \rightarrow S), P \vee R \Rightarrow Q \vee S$ （分兵二路，两路夹击）
8. 破坏性二难： $(P \rightarrow Q) \wedge (R \rightarrow S), \neg Q \vee \neg S \Rightarrow \neg P \vee \neg R$
9. 等价三段论： $(P \leftrightarrow Q) \wedge (Q \leftrightarrow R) \Rightarrow (P \leftrightarrow R)$ （两头落空，源头有错）
10. 归结式： $(P \vee Q) \wedge (\neg P \vee R) \Rightarrow (Q \vee R)$ （两头下注，必中一个）

归结证明是一种基于归结原理的自动定理证明方法，基础是“归结式”：对于两个子句 $C_1 = P \vee A$ 和 $C_2 = \neg P \vee B$ ，可以通过消去互补文字 P 和 $\neg P$ ，得到归结式 $A \vee B$ 。解题过程是：先将待证明的公式转化为合取范式，得到子句集合，然后通过反复应用归结规则，从子句集中推导新的子句，如果能够推导出空子句（矛盾），则证明原公式是不可满足的，否则直到推导出结果为止。

除了利用这些推理规则并使用演绎法进行推理，也可以先附加前提（CP），再直接证明。或者先附加结论的否定（归谬法）再进行间接推演。

定义 1.2.2 相容

如果存在一个真值赋值使得所有公式 A_1, A_2, \dots, A_n 同时为真，则称它们是相容的（一致的）；否则称它们是不相容的（矛盾的），即这些命题公式的合取式为矛盾式。

有了这个思路，我们可以将结论取否定加入到前提条件集合中，证明前提条件不相容，也就是说“题目出错了”，从而证明原来的结论是正确的。

1.3 析取范式, 合取范式

定义 1.3.1 析取范式和合取范式, 极小项极大项, 主析取, 主合取范式

析取范式是若干个简单合取式(文字的合取)的析取, 形如: $(P \wedge \neg Q) \vee (R \wedge S) \vee \dots$

合取范式是若干个简单析取式(文字的析取)的合取, 形如: $(P \vee \neg Q) \wedge (R \vee S) \wedge \dots$

任何命题公式都存在等价的析取范式和合取范式, 可通过蕴含等价、内移否定、分配律得。

极小项是包含所有命题变元或其否定的简单合取式, 每个变元恰好出现一次。例如, 对于变元 P, Q , 极小项有: $P \wedge Q$, $P \wedge \neg Q$, $\neg P \wedge Q$, $\neg P \wedge \neg Q$ 。

极大项是包含所有命题变元或其否定的简单析取式, 每个变元恰好出现一次。例如, 对于变元 P, Q , 极大项有: $P \vee Q$, $P \vee \neg Q$, $\neg P \vee Q$, $\neg P \vee \neg Q$ 。

主析取范式是由极小项组成的析取范式, 每个极小项对应公式的一个成真赋值。

主合取范式是由极大项组成的合取范式, 每个极大项对应公式的一个成假赋值。

任何命题公式都存在等价的唯一主析取范式和主合取范式。永真的主合取范式为空(无极大项), 永假式的主析取范式为空(无极小项)。

所以由上述定义得知, 主析取范式或主合取范式中不一定有极小项或者极大项。极小项一般用小写 m_i 表示, 极大项一般用大写 M_i 表示。

关于成真赋值和成假赋值与谁对应, 这里提供理解和记忆的方式:

由于析取范式由若干个简单合取式(极小项)通过析取联结词连接而成, 而析取运算具有“一真即真”的特性, 这类似于逻辑代数中的“或”运算: 0(假)参与运算不改变结果(相当于没有贡献), 而每个1(真)项(对应极小项为真)都会使结果为真。因此, 为了和原命题保持等价关系, 主析取范式的每一个极小项都要对应着公式的一个成真赋值, 不然就不可以代表(或者等价于)原命题公式。

进而, 将真值表中每个成真赋值对应的二进制数转化为十进制, 即可得到该极小项的下标(如赋值 $P = 1, Q = 0, R = 1$ 对应 m_5)。主析取范式就是所有这些极小项(如 m_2, m_5, m_7)用逻辑加连接起来的形式: $\sum(2, 5, 7)$ 。

由于合取范式由若干个简单析取式(极大项)通过合取联结词连接而成, 而合取运算具有“一假即假”的特性, 这类似于逻辑代数中的“与”运算: 1(真)参与运算不改变结果(相当于没有贡献), 而每个0(假)项(对应极大项为假)都会使结果为假。因此, 为了和原命题保持等价关系, 主合取范式的每一个极大项都要对应着公式的一个成假赋值, 不然就不可以代表(或者等价于)原命题公式。

进而, 将真值表中每个成假赋值对应的二进制数转化为十进制, 即可得到该极大项的下标(如赋值 $P = 1, Q = 0, R = 1$ 对应 M_5)。主合取范式就是所有这些极大项(如 M_2, M_5, M_7)用逻辑乘连接起来的形式 $\prod(2, 5, 7)$

对主析取范式(主合取范式)使用分配律(可以理解为多项式乘法)可以得到等价的主合取范式(主析取范式)。

$$(P \wedge Q) \vee (\neg P \wedge \neg Q) = (P \vee \neg P) \wedge (P \vee \neg Q) \wedge (Q \vee \neg P) \wedge (Q \vee \neg Q) = (P \vee \neg Q) \wedge (Q \vee \neg P)$$

例题 1.3.1 2023 年真题

用等值演算法求取下列公式: $(\neg P \rightarrow Q) \rightarrow (P \vee \neg Q)$ 的合取范式

$$\begin{aligned}
 (\neg P \rightarrow Q) \rightarrow (P \vee \neg Q) &\Leftrightarrow \neg(\neg P \rightarrow Q) \vee (P \vee \neg Q) \quad (\text{蕴含等值式}) \\
 &\Leftrightarrow \neg(P \vee Q) \vee (P \vee \neg Q) \quad (\text{蕴含等值式}) \\
 &\Leftrightarrow (\neg P \wedge \neg Q) \vee (P \vee \neg Q) \quad (\text{德摩根定律}) \\
 &\Leftrightarrow [\neg P \vee (P \vee \neg Q)] \wedge [\neg Q \vee (P \vee \neg Q)] \quad (\text{分配律}) \\
 &\Leftrightarrow [(\neg P \vee P) \vee \neg Q] \wedge [P \vee (\neg Q \vee \neg Q)] \quad (\text{结合律}) \\
 &\Leftrightarrow P \vee \neg Q
 \end{aligned}$$

例题 1.3.2 2023 年真题

构造下面推理的证明。前提: $p \vee q, p \rightarrow \neg r, s \rightarrow t, \neg s \rightarrow r, \neg t$, 结论: q

1	$s \rightarrow t$	前提引入
2	$\neg s \vee t$	蕴含等值式 (从 1)
3	$\neg t$	前提引入
4	$\neg s$	析取三段论 (从 2,3)
5	$\neg s \rightarrow r$	前提引入
6	r	假言推理 (从 4,5)
7	$p \rightarrow \neg r$	前提引入
8	$\neg p$	拒取式 (从 6,7)
9	$p \vee q$	前提引入
10	q	析取三段论 (从 8,9)

第二章 谓词逻辑

2.1 谓词逻辑基本概念

定义 2.1.1 个体词 谓词 n 元谓词 个体常元变元 谓词常项变项

在谓词逻辑中，命题被分解为个体词和谓词两部分。

个体词是命题中表示具体或抽象对象的词，包括表示特定个体的个体常元（如 a, b, c ）和表示不确定个体的个体变元（如 x, y, z ）。

谓词是用来说明个体性质或个体间关系的词，包括表示特定性质或关系的谓词常项（如 P, Q, R ）和表示不确定性质或关系的谓词变项（如 F, G, H ）。 n 元谓词是涉及 n 个个体的谓词，表示 n 元关系，如一元谓词 $P(x)$ 描述个体性质，二元谓词 $R(x, y)$ 描述两个体间关系， n 元谓词 $F(x_1, x_2, \dots, x_n)$ 描述 n 个个体的关系。

定义 2.1.2 谓词表达式，命题函数，个体域，论述域

在谓词逻辑中，谓词表达式是由谓词和个体词组成的符号串，用于表示个体的性质或个体间的关系，例如 $P(x)$ 、 $R(a, b)$ 等。

命题函数是以个体变元（其取值范围就是个体域，也称作论述域）为自变量的函数，其取值是一个命题，当个体变元被特定个体常元替换时，命题函数转化为一个具体的命题。例如， $P(x)$ 是一个命题函数，当 x 取值为 a 时， $P(a)$ 成为一个命题。命题函数的真值取决于个体变元的取值和谓词的含义。

可以看出，谓词表达式可以判断真值，命题函数不可以。个体域可以是无限或者有限的，没有特别说明时，个体变元的论述域指的是把整个宇宙中一切事物都作为对象的集合，所以当大题没有说个体域是什么时，最好不要想当然的自我设想个体域，比如说有的题目说“所以人都是学生”，那么最好还是设置命题函数“ $M(x) : x$ 是人”，或者声明个体域 x 是人，不要直接不管了。

定义 2.1.3 量词

量词是用于表示个体变元在个体域中取值范围的逻辑符号。

全称量词 (\forall): 表示“对所有”或“任意”，如 $\forall x P(x)$ 表示“对所有 x , $P(x)$ 成立”。

存在量词 (\exists): 表示“存在”或“至少有一个”，如 $\exists x P(x)$ 表示“存在 x 使得 $P(x)$ 成立”。

除了这两种基本量词外，还有一些扩展的量词表示法：

唯一存在量词 ($\exists!$): 表示“存在唯一的”，如 $\exists! x P(x)$ 表示“存在唯一的 x 使得 $P(x)$ 成立”

计数量词: 如 $\exists_n x P(x)$ 表示“恰好有 n 个 x 满足 $P(x)$ ”

注意，在使用全称量词时，表示个体范围的特性谓词和表示个体性质的谓词构成条件关系式： $\forall x(P(x) \rightarrow Q(x))$ ；使用存在量词时，表示个体范围的特性谓词和表示个体性质的谓词构成合取关系式： $\exists x(P(x) \wedge Q(x))$ 。

考虑命题“所有大学生都年轻”。如果我们错误地用合取式： $\forall x(Student(x) \wedge Young(x))$ 这表示“每个个体都是大学生并且年轻”——要求宇宙中所有个体都必须是大学生！这显然过强了。正确的条件式： $\forall x(Student(x) \rightarrow Young(x))$ 只对“是大学生”的那些个体施加“年轻”的要求，对非大学生个体没有要求，这才是符合题意的。

考虑命题“有大学生聪明”。如果我们错误地用条件式： $\exists x(Student(x) \rightarrow Smart(x))$ 这个公式在逻辑上等价于 $\exists x(\neg Student(x) \vee Smart(x))$ ，只要存在任意一个非大学生，这个公式就为真，完全偏离原意。而 $\exists x(Student(x) \wedge Smart(x))$ 表达了“存在一个个体既是大学生又聪明”的含义。

实际上，两种表达在特定条件下可以转换： $\forall x(P(x) \rightarrow Q(x)) \Leftrightarrow \neg \exists x(P(x) \wedge \neg Q(x))$

定义 2.1.4 谓词演算的合式公式，简称谓词合式公式

合式公式是谓词逻辑中形式推理和语义解释的基本单位，其递归定义如下：

1. 原子公式是合式公式：如果 P 是 n 元谓词， t_1, t_2, \dots, t_n 是项（个体常元、个体变元或函数），则 $P(t_1, t_2, \dots, t_n)$ 是合式公式
2. 逻辑联结词组合：如果 A 和 B 是合式公式，则 $(\neg A)$ 、 $(A \wedge B)$ 、 $(A \vee B)$ 、 $(A \rightarrow B)$ 、 $(A \leftrightarrow B)$ 也是合式公式
3. 量词组合：如果 A 是合式公式， x 是个体变元，则 $(\forall x A)$ 和 $(\exists x A)$ 也是合式公式
4. 只有有限次应用上述规则构成的表达式才是合式公式

定义 2.1.5 指导变元，辖域，约束变元，约束出现，自由变元，自由出现，闭式

在谓词逻辑中，量词和变元的使用涉及以下重要概念：

指导变元：紧跟在量词后面的个体变元称为指导变元，如 $\forall x$ 中的 x 和 $\exists y$ 中的 y 。

辖域：量词所作用的公式范围称为该量词的辖域。如 $\forall x(P(x) \rightarrow Q(x))$ 中， $(P(x) \rightarrow Q(x))$ 是 $\forall x$ 的辖域。

约束变元：在量词辖域内出现且与该量词指导变元相同的个体变元称为约束变元。

约束出现：个体变元在公式中的某次出现如果处于某个量词的辖域内，且与该量词的指导变元相同，则称为约束出现。

自由变元：在公式中不被任何量词约束的个体变元称为自由变元。

自由出现：个体变元在公式中的某次出现如果不是约束出现，则称为自由出现。

闭式：不包含任何自由出现的个体变元的谓词公式称为闭式。闭式中所有个体变元都是约束出现的，这样的公式具有确定的真值。

例如，在公式 $\forall x(P(x, y) \rightarrow \exists z Q(x, z))$ 中： x 和 z 是指导变元， $(P(x, y) \rightarrow \exists z Q(x, z))$ 是 $\forall x$ 的辖域， $Q(x, z)$ 是 $\exists z$ 的辖域，第一个 x 和第二个 x 是约束出现（被 $\forall x$ 约束）， y 是自由出现（自由变元）， z 是约束出现（被 $\exists z$ 约束），该公式不是闭式，因为包含自由变元 y 。

定义 2.1.6 谓词公式的解释和分类

谓词公式的解释是指为公式中的符号赋予具体含义的过程, 包括以下四个组成部分:

1. **个体域 D :** 一个非空集合, 规定个体变元的取值范围
2. **个体常元的指定:** 为每个个体常元指定 D 中的一个特定元素
3. **函数符号的指定:** 为每个 n 元函数符号指定 D^n 到 D 的映射
4. **谓词符号的指定:** 为每个 n 元谓词符号指定 D^n 到 {真, 假} 的映射

给定解释 I 和公式 A , 可以通过递归方式计算 A 在 I 下的真值。闭式在任意解释下的真值是确定的, 而包含自由变元的公式真值取决于自由变元的取值。公式 A 是永真式当且仅当 A 在所有解释下为真; A 是可满足式当且仅当存在解释使 A 为真; A 是永假式当且仅当 A 在所有解释下为假。

谓词公式判断类型是比较困难的, 为了判断一些简单的情形, 可以定义代换实例:

定义 2.1.7 谓词公式的代换实例

谓词公式的代换实例, 是指通过将命题逻辑中的命题公式中的命题变元替换为谓词公式而得到的谓词公式。具体来说, 设 A 是一个命题公式, 其中包含命题变元 P_1, P_2, \dots, P_n 。如果用一个谓词公式 B_i ($i = 1, 2, \dots, n$) 替换 A 中的每个命题变元 P_i , 则得到的新公式 A' 称为 A 的一个代换实例。

代换实例保持了原命题公式的逻辑结构, 只是将原子命题替换为谓词公式。如果原命题公式是永真式(矛盾式), 则其所有代换实例也是永真式(矛盾式)。

例如, 命题公式 $P \rightarrow (Q \wedge P)$ 的一个代换实例可以是: $\forall xP(x) \rightarrow (\exists yQ(y) \wedge \forall xP(x))$ 。而在代换实例的视角来看, 有些谓词公式可以通过像命题公式那样进行等价变换, 从而证明一些命题公式之间有等价关系或者蕴含关系。这就需要用到之前的推理定律。详见 2.3

2.2 换名, 前束范式

换名的动机是让谓词公式中尽量不要出现同样的变元, 以便于区分和进行逻辑推理。

约束变元换名规则允许在公式中更改约束变元的名称, 而不改变公式的逻辑含义。比如将 $\forall x(P(x) \rightarrow \exists yQ(x, y))$ 中的 x 换为 z , 得到 $\forall z(P(z) \rightarrow \exists yQ(z, y))$, 要求如下:

1. 只能更改约束变元的名称, 不能更改自由变元;
2. 换名必须在整个量词的辖域内一致进行
3. 新变元名称不能与公式中已有的自由变元同名
4. 多个量词约束的同名变元必须同时换名

自由变元代入规则允许用项替换公式中的自由变元。例如将 $\forall xP(x, y)$ 中的自由变元 y 用常元 a 代入, 得到 $\forall xP(x, a)$, 要求如下:

1. 代入必须对自由变元的所有自由出现同时进行

2. 代入项中不能含有在公式中受约束的变元

3. 代入后原公式的逻辑含义保持不变

注意, 约束变元换名, 改变的是变元符号, 不改变变元的性质(仍是约束变元), 自由变元代入是用具体的项(常元、函数或其他变元)替换自由变元换名规则保持公式的逻辑等价性。

举一个例子, 比如谓词公式: $\forall x(P(x, y) \rightarrow \exists y Q(x, y))$, 这个公式存在两个问题: 一是自由变元 y 与约束变元 y 同名, 容易引起混淆, 二是量词 $\forall x$ 和 $\exists y$ 的约束变元 x 和 y 在公式中混合使用, 不利于逻辑推理。下面换名:

第一步: 自由变元代入: 将自由变元 y 用常元 a 代入: $\forall x(P(x, a) \rightarrow \exists y Q(x, y))$

第二步: 约束变元换名: 将存在量词 $\exists y$ 的约束变元 y 换名为 z : $\forall x(P(x, a) \rightarrow \exists z Q(x, z))$ 。经过两个规则的应用, 我们得到的新公式: 自由变元 y 已被具体化为常元 a , 约束变元 y 被换名为 z , 避免了名称冲突, 现在公式中每个变元的角色清晰: x 是 \forall 的约束变元, z 是 \exists 的约束变元, a 是常元, 新公式与原公式逻辑等价, 但更便于进行逻辑推理。

常常利用换名将谓词公式化为与其自身等价的规范形式, 成为前束范式:

定义 2.2.1 前束范式, 首标, 母式

前束范式是谓词逻辑中的一种标准形式, 其中所有量词都出现在公式的最前端, 且其辖域延伸到公式的末尾。形式化地, 一个公式是前束范式当且仅当它具有以下形式:

$Q_1 x_1 Q_2 x_2 \cdots Q_n x_n M$, 其中 $Q_1 x_1 Q_2 x_2$ 为首标, M 为母式

其中: $Q_i (i = 1, 2, \dots, n)$ 是量词符号 (\forall 或 \exists), $x_i (i = 1, 2, \dots, n)$ 是个体变元。

将任意谓词公式化为前束范式的步骤通常包括: 消去蕴含联结词 \rightarrow 和等价联结词 \leftrightarrow , 将否定符号 \neg 内移, 使其只作用于原子公式, 将量词向左移动, 并适当换名避免变元冲突。

例如谓词公式 $\forall x \forall y (\exists z (P(x, z) \wedge P(y, z)) \rightarrow \exists u Q(x, y, u))$ 化为前束范式的过程是:

$$\begin{aligned} & \forall x \forall y (\exists z (P(x, z) \wedge P(y, z)) \rightarrow \exists u Q(x, y, u)) \\ & \Leftrightarrow \forall x \forall y (\neg \exists z (P(x, z) \wedge P(y, z)) \vee \exists u Q(x, y, u)) && \text{置换规则} \\ & \Leftrightarrow \forall x \forall y (\forall z (\neg P(x, z) \vee \neg P(y, z)) \vee \exists u Q(x, y, u)) && \text{置换规则} \\ & \Leftrightarrow \forall x \forall y \forall z \exists u (\neg P(x, z) \vee \neg P(y, z) \vee Q(x, y, u)) && \text{量词辖域扩张} \end{aligned}$$

由于上面的 x, y 的辖域覆盖到公式末尾, 而且 z 和 u 的虽然辖域不同, 但名称不同, 无需换名, 下面再看一个需要换名的例子。求下列谓词公式的前束范式: $\neg \exists x A(x) \rightarrow \forall y B(x, y)$

$$\begin{aligned} & \neg \exists x A(x) \rightarrow \forall y B(x, y) \\ & \Leftrightarrow \forall x \neg A(x) \rightarrow \forall y B(x, y) && \text{否定等价转换} \\ & \Leftrightarrow \forall z \neg A(z) \rightarrow \forall y B(x, y) && \text{换名} \\ & \Leftrightarrow \forall z \forall y (\neg A(z) \rightarrow B(x, y)) && \text{量词辖域扩张} \\ & \Leftrightarrow \forall z \forall y (A(z) \vee B(x, y)) && \text{置换规则} \end{aligned}$$

2.3 谓词公式的等价和蕴含关系式

与上一章类似，当两个谓词公式 A 和 B 满足 $A \leftrightarrow B$ 为永真式时，我们说 A 和 B 是等价的，等价关系式的形式为： $A \Leftrightarrow B$ ；当两个谓词公式 A 和 B 满足 $A \rightarrow B$ 为永真式时，我们说 A 蕴含 B ，蕴含关系式的形式为： $A \Rightarrow B$ 。

定理 2.3.1 常见的等价关系式

1. 去括号 (B 含 x)： $\exists x(A(x) \rightarrow B(x)) \Leftrightarrow \forall xA(x) \rightarrow \exists xB(x)$
2. 去括号 (B 含 x)： $\forall y(A(y) \rightarrow B(x)) \Leftrightarrow \exists xA(x) \rightarrow B(x)$
3. 去括号 (B 不含 x)： $\forall x(\exists x)(B(\wedge, \vee, \rightarrow)A(x)) \Leftrightarrow \forall x(\exists x)B(\wedge, \vee, \rightarrow)A(x)$
4. 去括号 (B 不含 x)： $\forall x(A(x) \rightarrow B) \Leftrightarrow \exists xA(x) \rightarrow B \quad \exists x(A(x) \rightarrow B) \Leftrightarrow \forall xA(x) \rightarrow B$
5. 分配律： $\forall x(A(x) \wedge B(x)) \Leftrightarrow \forall xA(x) \wedge \forall xB(x) \quad \exists x(A(x) \vee B(x)) \Leftrightarrow \exists xA(x) \vee \exists xB(x)$
6. 交换律： $\forall x\forall yA(x, y) \Leftrightarrow \forall y\forall xA(x, y) \quad \exists x\exists yA(x, y) \Leftrightarrow \exists y\exists xA(x, y)$

3 和 4 即书上给出的量词辖域扩张与收缩律，2 虽然说 B 含 x ，但是由于此时蕴含前件不含 x ，而是含有 y ，且指导变元是 y ，所以此时和 4 一样。上面的公式利用等价变形都可以解决，下面给出理解和记忆的方式。

1. 左边说“至少有一个 x ，能够确保：如果它满足 A ，那么它也满足 B ”。右边说“如果所有的 x 都满足 A ，那么至少有一个 x 满足 B ”。例如：“假设你是老师，你承诺说你会找一些幸运儿学生，如果他们来上课就能及格”，这等价于“如果所有学生都来上课，那么有学生能及格”，因为你总要挑选学生给到及格。

2. 需要注意在这个公式中， $B(x)$ 中的变元是自由变元（没有被任何量词约束），因此两边都表示关于某个特定个体 x 的陈述。左边说“对任何一个 y ，如果 y 具有性质 A ，那么 x 具有性质 B ”；右边说“如果存在某个个体具有性质 A ，那么 x 具有性质 B ”。例如，“如果任何人都都是医生，那么张三健康”等价于“如果有医生存在，那么张三健康”。由于 x 是自由变元，两边讨论的都是同一个特定的 x （这里也可以视作存在量词引入）， $B(x)$ 描述的是这个特定个体的性质，不受量词影响。

3. 当 B 是与 x 无关的事实陈述时，可以把 B 从量词中“提出来”。例如，“对所有学生，今天下雨且他们要考试”等价于“今天下雨且所有学生都要考试”。

4. 左边说“每个 A 都导致 B ”；右边说“只要有 A 存在就会导致 B ”。例如，“如果每个学生作弊，就取消考试”等价于“只要有学生作弊，就取消考试”。

5. “每个人都既聪明又勤奋”等价于“每个人都聪明且每个人都勤奋”。“有人会唱歌或跳舞”等价于“有人会唱歌或者有人会跳舞”。

6. “任何两个人都是朋友”等价于“对任何人来说，与任何人都是朋友”，量词顺序不影响含义。“存在两个人是朋友”等价于“存在这样的两个人，他们是朋友”，存在量词的顺序也不影响含义。

定理 2.3.2 常见的蕴含关系式（结论的弱化）

1. $\exists x A(x) \rightarrow \exists x B(x) \Rightarrow \exists x(A(x) \rightarrow B(x))$
2. $\forall x A(x) \rightarrow \exists x B(x) \Rightarrow \exists x(A(x) \rightarrow B(x))$
3. $\forall x A(x) \vee \forall x B(x) \Rightarrow \forall x(A(x) \vee B(x)) \Rightarrow \neg \forall x A(x) \rightarrow \exists x B(x)$
4. $\exists x(A(x) \wedge B(x)) \Rightarrow \exists x A(x) \wedge \exists x B(x)$
5. $\forall x(A(x) \rightarrow B(x)) \Rightarrow \forall x A(x) \rightarrow \forall x B(x)$
6. $\exists x(A(x) \rightarrow B(x)) \Rightarrow \exists x A(x) \rightarrow \exists x B(x)$
7. $\forall x \forall y A(x, y) \Rightarrow \forall x A(x, x)$
8. $\exists x A(x, x) \Rightarrow \exists x \exists y A(x, y)$
9. $\forall x \forall y A(x, y) \Rightarrow \exists y \forall x A(x, y) \Rightarrow \forall x \exists y A(x, y) \Rightarrow \exists x \exists y A(x, y)$

1. 如果存在某个 x 满足 $A(x)$, 那么存在某个 x 满足 $B(x)$ 。注意, 这里的两个 x 可能不是同一个个体, 也可能是同一个个体, 当为后一种情况, 就得到了蕴含后件。所以蕴含关系 $\exists x A(x) \rightarrow \exists x B(x) \Rightarrow \exists x(A(x) \rightarrow B(x))$ 成立。

2. 如果所有 x 满足 $A(x)$, 那么存在某个 x 满足 $B(x)$ 。单独考虑这个对 $B(x)$ 量身定制的 x 也会满足 $A(x)$, 此时 $A(x) \rightarrow B(x)$ 成立, 蕴含关系 $\forall x A(x) \rightarrow \exists x B(x) \Rightarrow \exists x(A(x) \rightarrow B(x))$ 成立。

3. 左边是一个强条件: 要么所有个体都满足 A , 要么所有个体都满足 B 。右边是一个弱条件: 每个个体至少满足 A 或 B 之一。显然, 如果左边成立, 那么右边必须成立, 因为如果所有个体都满足 A , 那么每个个体都满足 A , 所以满足 A 或 B ; 类似如果所有个体都满足 B , 也一样。但反过来不一定成立: 可能有些个体满足 A 但不满足 B , 有些满足 B 但不满足 A , 所以右边真但左边假, 因此蕴含关系 $\forall x A(x) \vee \forall x B(x) \Rightarrow \forall x(A(x) \vee B(x))$ 成立。而另一个蕴含关系式作为例题安排在后面了。

4. 如果存在一个个体同时满足 A 和 B , 那么当然存在满足 A 的个体 (就是这个个体) 和存在满足 B 的个体 (也是这个个体), 但是右边的两个 x 可能一样也可能不一样, 蕴含关系 $\exists x(A(x) \wedge B(x)) \Rightarrow \exists x A(x) \wedge \exists x B(x)$ 显然成立。

5. 每一个满足 A 的 x 都同时满足 B , 那当 x 恒满足 A 时就会恒满足 B , 但当存在不满足 A 的个体时, 前提不施加任何约束, 因此可能存在某些个体满足 A 但不满足 B , 只要不是所有个体都满足 A , 前提仍然为真。蕴含关系 $\forall x(A(x) \rightarrow B(x)) \Rightarrow \forall x A(x) \rightarrow \forall x B(x)$ 显然成立。

6. 对于某特定的 x , 如果 $A(x)$ 成立, 那么 $B(x)$ 也成立。但是右边的两个 x 可能一样也可能不一样, 蕴含关系 $\exists x(A(x) \rightarrow B(x)) \Rightarrow \exists x A(x) \rightarrow \exists x B(x)$ 显然成立。

7. 左边说 A 关系对所有个体对都成立。右边说 A 关系对所有自对 (即个体与自身) 都成立。如果左边成立, 特别地, 当 $y = x$ 时, $A(x, x)$ 成立, 因此蕴含关系 $\forall x \forall y A(x, y) \Rightarrow \forall x A(x, x)$ 成立。

8. 如果存在一个个体与自身满足 A , 那么取个体 x 和 y (取 $y = x$) 满足 A 。所以左边蕴含右边, 即 $\exists x A(x, x) \Rightarrow \exists x \exists y A(x, y)$ 。但可能 $A(x, y)$ 成立对于 x 和 y 不同, $A(x, x)$ 不成立。

9. 从“全局 A ”到“存在万能 y ”(万能钥匙) 到“每个 x 有对应 y ”(专用钥匙) 到“存在一对”(碰运气), 强度递减, 蕴含关系成立。

上面的叙述其实已经用到了四大谓词逻辑推理规则：

定理 2.3.3 四大谓词逻辑推理规则

1. 全称实例化 (Universal Instantiation, UI): 从全称命题推出特定实例。

$$\forall x P(x) \Rightarrow P(c), \text{ 其中 } c \text{ 是个体域中的任意个体}$$

使用要求与注意事项： c 必须属于个体域中的个体，且 c 不能在 $A(x)$ 中约束出现，可以对同一个全称命题进行多次实例化，得到不同的实例，实例化时保持变元的一致性。例如，从“所有人都会死”推出“苏格拉底会死”。

2. 存在实例化 (Existential Instantiation, EI) 从存在命题推出特定实例。

$$\exists x P(x) \Rightarrow P(c), \text{ 其中 } c \text{ 是个体域中的某个特定个体}$$

使用要求与注意事项：除了 x 以外， $A(x)$ 不能出现其它自由出现的个体变元，同时 c 必须是新引入的常元，不能和公式或推理证明过程中的其它常元或变元相同； c 不能出现在结论中（因为不知道具体是哪个个体）；只能对同一个存在量词使用一次 EI。例如，从“有人迟到了”推出“令小王是那个迟到的人”

3. 全称泛化 (Universal Generalization, UG) 从特定实例推出全称命题。

$$P(c) \Rightarrow \forall x P(x), \text{ 其中 } c \text{ 是个体域中的任意个体}$$

使用要求与注意事项： c 必须是自由出现的个体变元，不能有特殊性质，且 c 不能在 $A(x)$ 中约束出现，必须确保对个体域中所有个体都成立。示例：通过证明任意一个三角形的内角和为 180 度，推出所有三角形的内角和为 180 度。

4. 存在泛化 (Existential Generalization, EG): 从特定实例推出存在命题。

$$P(c) \Rightarrow \exists x P(x), \text{ 其中 } c \text{ 是个体域中的某个特定个体}$$

使用要求与注意事项： c 可以是任意已知个体，但是取代 c 的 x 不可以在 $A(c)$ 中出现过，即不能和已有的量词绑定。示例：从“苏格拉底是哲学家”推出“存在哲学家”。

5. 易错点：在使用 EI 引入新常元后，不能再对该常元使用 UG

例题：证明 $\forall x(A(x) \vee B(x)) \Rightarrow \neg \forall x A(x) \rightarrow \exists x B(x)$

(1)	$\forall x(A(x) \vee B(x))$	前提
(2)	$\neg \forall x A(x)$	附加前提
(3)	$\exists x \neg A(x)$	由 (2) 量词否定转换
(4)	$\neg A(c)$	由 (3) 存在实例化 (EI)， c 为新常量
(5)	$A(c) \vee B(c)$	由 (1) 全称实例化 (UI)
(6)	$B(c)$	由 (4)(5) 析取三段论
(7)	$\exists x B(x)$	由 (6) 存在泛化 (EG)
(8)	$\neg \forall x A(x) \rightarrow \exists x B(x)$	由 (2)(7) 条件证明 (CP)

第三章 集合与关系

3.1 集合

定义 3.1.1 空集，全集，有限集，无限集，元素个数

空集：不含任何元素的集合，记作 \emptyset 或 $\{x|x \neq x\}$ 。空集是任何集合的子集。空集是唯一的。

全集：特定讨论中包含所有对象的集合，记作 U 。全集是相对的，取决于讨论的上下文。

有限集：元素个数有限的集合。如果集合 A 有 n 个元素，其中 n 是非负整数，则 A 是有限集。

无限集：不是有限集的集合，即元素个数无限多的集合。如自然数集 \mathbb{N} 、实数集 \mathbb{R} 等。

元素个数：有限集 A 中元素的数目，记作 $|A|$ 或 $card(A)$ 。无限集的元素个数用基数概念描述，如可数无限集、不可数无限集等。

定义 3.1.2 集合的包含关系

子集：如果集合 A 中的每个元素都是集合 B 中的元素，则称 A 是 B 的子集，记作 $A \subseteq B$ 。

空集是空集的子集

真子集：如果 $A \subseteq B$ 且 $A \neq B$ ，则称 A 是 B 的真子集，记作 $A \subset B$ 。即

$$\forall x(A(x) \rightarrow B(x)) \wedge \exists x(B(x) \wedge \neg A(x))$$

定义 3.1.3 集合的基本运算

交集：集合 A 和 B 的交集是由所有既属于 A 又属于 B 的元素组成的集合，记作 $A \cap B$ 。

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

并集：集合 A 和 B 的并集是由所有属于 A 或属于 B 的元素组成的集合，记作 $A \cup B$ 。

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

补集：集合 A 的补集是由全集中所有不属于 A 的元素组成的集合，记作 $\sim A$ 。

$$\sim A = \{x \in U \mid x \notin A\}$$

差集：集合 A 与 B 的差集是由所有属于 A 但不属于 B 的元素组成的集合：

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

对称差： A 和 B 的对称差是由所有属于 A 或属于 B 但不同时属于两者的元素组成的集合

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

幂集：集合 A 的幂集是由 A 的所有子集构成的集合，记作 $P(A)$ ：

$$P(A) = \{X \mid X \subseteq A\}$$

定理 3.1.1 容斥原理

对于有限集合 A_1, A_2, \dots, A_n , 有:

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

然后主要写一些差集, 对称差, 幂集的性质。

定理 3.1.2 差集的性质

分配律: $A - (B \cup C) = (A - B) \cap (A - C) = (A - B) - C$ $A - (B \cap C) = (A - B) \cup (A - C)$

分配律: $(A \cup B) - C = (A - C) \cup (B - C)$ $(A \cap B) - C = (A - C) \cap (B - C)$

去括号: $A - (B - C) = (A - B) \cup (A \cap C)$

传递性: 如果 $A \subseteq B$, 则 $A - C \subseteq B - C$

第二条恒等变形就可以了比较简单, 第四条也好理解, $x \in A \wedge x \notin C$ 显然蕴含 $x \in B \wedge x \notin C$
第一条和第三条有点难, 一个很霸道的方式是, 对于全集 U 内的元素 x , 考虑真值表

$x \in A$	$x \in B$	$x \in C$	$x \in (B \cup C)$	$x \in (B - C)$	$x \in A - B$	$x \in A - C$	$x \in A \cap C$
0	0	0	0	0	0	0	0
0	0	1	1	0	0	0	0
0	1	0	1	1	0	0	0
0	1	1	1	0	0	0	0
1	0	0	0	0	1	1	0
1	0	1	1	0	1	0	1
1	1	0	1	1	0	1	0
1	1	1	1	0	0	0	1

然后, 目标表达式比较

$x \in A$	$x \in B$	$x \in C$	$x \in A - (B \cup C)$	$x \in (A - B) \cap (A - C)$	$x \in (A - B) - C$
0	0	0	0	0	0
0	0	1	0	0	0
0	1	0	0	0	0
0	1	1	0	0	0
1	0	0	1	1	1
1	0	1	0	0	0
1	1	0	0	0	0
1	1	1	0	0	0

从表 2 可以看出第 4,5,6 列的真值完全相同，因此： $A - (B \cup C) = (A - B) \cap (A - C) = (A - B) - C$

$x \in A$	$x \in B$	$x \in C$	$x \in A - (B - C)$	$x \in (A - B) \cup (A \cap C)$
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	0	0
1	0	0	1	1
1	0	1	1	1
1	1	0	0	0
1	1	1	1	1

从表 3 可以看出，第 4 列和第 5 列的真值完全相同，因此 $A - (B - C) = (A - B) \cup (A \cap C)$

定理 3.1.3 对称差的性质

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

分配律： $A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$

差形式： $A \oplus B = (A \cup B) - (A \cap B)$

取补集： $\sim (A \oplus B) = (\sim A \oplus B) = (A \oplus \sim B)$

常见等价关系： $A \oplus B = \emptyset$ 当且仅当 $A = B$ ， $A \oplus B = A \oplus C$ 当且仅当 $B = C$

消去律： $(A \oplus B) \oplus (B \oplus C) = A \oplus C$ （可以推广）

证明： $(A \oplus B) \oplus C = A \oplus (B \oplus C)$

A	B	C	$A \oplus B$	$(A \oplus B) \oplus C$	$B \oplus C$	$A \oplus (B \oplus C)$	是否相等
0	0	0	0	0	0	0	是
0	0	1	0	1	1	1	是
0	1	0	1	1	1	1	是
0	1	1	1	0	0	0	是
1	0	0	1	1	0	1	是
1	0	1	1	0	1	0	是
1	1	0	0	0	1	0	是
1	1	1	0	1	0	1	是

如果要求必须使用等价变形，我们依然可以使用真值表写出两者的主析取范式，然后比较。两者的主析取范式完全相同，因此： $(A \oplus B) \oplus C = A \oplus (B \oplus C)$ ，具体的解答过程则是先将左右两边化为交并补运算，真值表可以起到检查是否正确的作用。

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

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

证明: $A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$

A	B	C	$B \oplus C$	$A \cap (B \oplus C)$	$A \cap B$	$A \cap C$	$(A \cap B) \oplus (A \cap C)$	相等
0	0	0	0	0	0	0	0	是
0	0	1	1	0	0	0	0	是
0	1	0	1	0	0	0	0	是
0	1	1	0	0	0	0	0	是
1	0	0	0	0	0	0	0	是
1	0	1	1	1	0	1	1	是
1	1	0	1	1	1	0	1	是
1	1	1	0	0	1	1	0	是

证明: $(A \cup B) \oplus (A \cup C) \subseteq A \cup (B \oplus C)$

A	B	C	$B \oplus C$	$A \cup (B \oplus C)$	$A \cup B$	$A \cup C$	$(A \cup B) \oplus (A \cup C)$	蕴含关系
0	0	0	0	0	0	0	0	相等
0	0	1	1	1	0	1	1	相等
0	1	0	1	1	1	0	1	相等
0	1	1	0	0	1	1	0	相等
1	0	0	0	1	1	1	0	左真右假
1	0	1	1	1	1	1	0	左真右假
1	1	0	1	1	1	1	0	左真右假
1	1	1	0	1	1	1	0	左真右假

可以发现, 当全集内的某个元素 x 满足 $x \in (A \cup B) \oplus (A \cup C)$ 时, x 必然满足 $x \in A \cup (B \oplus C)$

证明: $(A \oplus B) \oplus (B \oplus C) = A \oplus C$

A	B	C	$A \oplus B$	$B \oplus C$	$(A \oplus B) \oplus (B \oplus C)$	$A \oplus C$	是否相等
0	0	0	0	0	0	0	是
0	0	1	0	1	1	1	是
0	1	0	1	1	0	0	是
0	1	1	1	0	1	1	是
1	0	0	1	0	1	1	是
1	0	1	1	1	0	0	是
1	1	0	0	1	1	1	是
1	1	1	0	0	0	0	是

然而, 此题用真值表, 是杀鸡用牛刀, 其实最简单的方法是利用结合律:

$$(A_1 \oplus A_2) \oplus (A_2 \oplus A_3) = A_1 \oplus (A_2 \oplus A_2) \oplus A_3 = A_1 \oplus \emptyset \oplus A_3 = A_1 \oplus A_3$$

定理 3.1.4 对称差的代数结构

对于任意集合序列 A_1, A_2, \dots, A_n , 有

$$(A_1 \oplus A_2) \oplus (A_2 \oplus A_3) \oplus \cdots \oplus (A_{n-1} \oplus A_n) = A_1 \oplus A_n$$

对于任意形式的对称差链, 只要每个中间项出现偶数次, 就会相互抵消。例如:

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

因为通过结合律和交换律, B 和 C 实际上各出现两次, 因此抵消。

证明: $\sim(A \oplus B) = (\sim A \oplus B)$

$$\begin{aligned}\sim(A \oplus B) &= \sim((A \cap \sim B) \cup (\sim A \cap B)) = (\sim A \cup B) \cap (A \cup \sim B) \\ &= (\sim A \cap A) \cup (\sim A \cap \sim B) \cup (A \cap B) \cup (B \cap \sim B) \\ &= (\sim A \cap \sim B) \cup (A \cap B) = (\sim A \oplus B)\end{aligned}$$

定理 3.1.5 幂集的性质

设 X 是一个集合, $P(X)$ 表示 X 的幂集 (即 X 的所有子集构成的集合)。幂集具有以下性质:

1. 如果 $|X| = n$ (有限), 则 $|P(X)| = 2^n$, $P(\emptyset) = \{\emptyset\}$, 有 $1 = 2^0$ 个元素
2. 单调性: 如果 $A \subseteq B$, 则 $P(A) \subseteq P(B)$
3. $P(A) \cup P(B) \subseteq P(A \cup B)$, 当且仅当 $A \subseteq B$ 或 $B \subseteq A$ 取等
4. $P(A) \cap P(B) = P(A \cap B)$
5. $P(A - B) \subseteq (P(A) - P(B)) \cup \{\emptyset\}$

性质 3 的证明比较简单:

$$P(A) \cup P(B) \subseteq P(A \cup B) \cup P(A \cup B) = P(A \cup B)$$

分别放缩左右两侧即可, 而且这样的操作还有一个好处, 就是可以看清蕴含关系变成等价关系时的特殊条件 (当且仅当 $A \subseteq B$ 或 $B \subseteq A$ 取等)。我们不妨再看一个例子:

证明或证伪: $A \subset B \wedge C \subset D \Rightarrow (A \cup C) \subset (B \cup D)$

解: 考虑 $B = A \cup C, D = A \cup C$, 则

$$A \subset (A \cup C), C \subset (A \cup C) \Rightarrow (A \cup C) = (B \cup D)$$

显然该命题错误, 改成 $A \subset B \wedge C \subset D \Rightarrow (A \cup C) \subseteq (B \cup D)$ 即可。

证明或证伪: $A \subset B \wedge C \subset D \Rightarrow (A \cap C) \subset (B \cap D)$

解: 同样错误, 考虑 $A \cap C \subset A, C - A \neq \emptyset, B \cap D \subset B, D - B \neq \emptyset$, 则转化为

$$(A \cap C) \cap (B \cap D) = (A \cap B) \cap (C \cap D) \subset A \cap B$$

显然, 这里 $(A \cap B) = (C \cap D)$ 完全是可能的, 所以仍然需要改成 \subseteq

性质 4 显然, 一个集合既是 A 的子集, 又是 B 的子集, 那么其元素都在 A, B 中, 即在 $A \cap B$ 中, 反过来, 一个集合的元素在 $A \cap B$ 中, 那么也在 A, B 中, 故既是 A 的子集又是 B 的子集。

下面证明性质 5: $P(A - B) \subseteq (P(A) - P(B)) \cup \{\emptyset\}$

$$\begin{aligned} P(A - B) &= \{x \mid x \subseteq (A \cap \sim B)\} = \{x \mid x \subseteq A \wedge x \subseteq \sim B\} \\ &\subseteq \{x \mid x \subseteq A \wedge x \not\subseteq B\} = (P(A) - P(B)) \cup \{\emptyset\} \end{aligned}$$

需要说明的是, 涉及到幂集的性质的有关证明不可以使用真值表, 或者说用真值表比较麻烦, 因为我们考虑集合之间的关系的时候, 由于集合可能有不止一个元素, 所以 x 中的元素全在 A 中的反面, 不是“ x 中的元素全不在 A 中”, 而是“ x 中的元素不全在 A 中”。这就导致了

$$x \not\subseteq A \wedge x \not\subseteq B \Leftarrow x \not\subseteq A \cup B$$

和之前的情形大不相同, 此时要分多种情形讨论, 复杂度明显升高。但是, 真值表还是可以帮助我们进行集合的等价运算, 如:

例题 3.1.1

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

解 3.1.1. 设全集为 U , 观察到三个并集中都有 B , 所以合并:

$$\begin{aligned} &(A \cap B \cap C) \cup (\sim A \cap B \cap C) \cup (A \cap B \cap \sim C) \\ &= [B \cap (A \cap C)] \cup [B \cap (\sim A \cap C)] \cup [B \cap (A \cap \sim C)] \quad (\text{结合律}) \\ &= B \cap [(A \cap C) \cup (\sim A \cap C) \cup (A \cap \sim C)] \quad (\text{分配律}) \\ &= B \cap \{[(A \cup \sim A) \cap C] \cup (A \cap \sim C)\} \quad (\text{分配律}) \\ &= B \cap [(U \cap C) \cup (A \cap \sim C)] \quad (\text{补集律: } A \cup \sim A = U) \\ &= B \cap [C \cup (A \cap \sim C)] \quad (\text{同一律: } U \cap C = C) \\ &= B \cap [(C \cup A) \cap (C \cup \sim C)] \quad (\text{分配律}) \\ &= B \cap [(A \cup C) \cap U] \quad (\text{交换律和补集律}) \\ &= B \cap (A \cup C) \quad (\text{同一律}) \end{aligned}$$

另一种方式就是使用真值表: 我们通过分析元素 x 的属于关系来简化该表达式。定义真值表, 其中 1 表示 x 属于集合, 0 表示 x 不属于集合:

$x \in A$	$x \in B$	$x \in C$	$x \in A \cap B \cap C$	$x \in \sim A \cap B \cap C$	$x \in A \cap B \cap \sim C$	$x \in$ 整体表达式
0	0	0	0	0	0	0
0	0	1	0	0	0	0
0	1	0	0	0	0	0
0	1	1	0	1	0	1
1	0	0	0	0	0	0
1	0	1	0	0	0	0
1	1	0	0	0	1	1
1	1	1	1	0	0	1

从真值表可知, x 属于整体表达式当且仅当满足以下条件: $x \in B$ 为真, 同时 $x \in A$ 或 $x \in C$ 为真, 这等价于 $x \in B \cap (A \cup C)$ 。

伪装的方式是:

设 x 是全集中的任意元素, 我们分析 x 属于该并集的条件。

若 $x \in A \cap B \cap C$, 则 $x \in A$, $x \in B$, $x \in C$

若 $x \in \sim A \cap B \cap C$, 则 $x \notin A$, $x \in B$, $x \in C$

若 $x \in A \cap B \cap \sim C$, 则 $x \in A$, $x \in B$, $x \notin C$

综合三种情况, x 属于该并集当且仅当同时满足: $x \in B$, $x \in A$ 或 $x \in C$ (即 $x \in A \cup C$), 因此, x 属于该并集当且仅当 $x \in B \cap (A \cup C)$

这种等价变形的题目比较简单, 首先化成交并补, 然后只需要观察重复出现的结构 (有的时候还需要进行适当的换元) 接着等价运算。题目一难或者看不出来了, 就利用真值表来证明。

3.2 集合的笛卡尔积

定义 3.2.1 集合的笛卡尔积

设 A 和 B 是两个集合, A 与 B 的 **笛卡尔积** (或称直积) 定义为所有有序对 (a, b) 组成的集合, 其中 $a \in A$, $b \in B$, 记作 $A \times B$:

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

推广到 n 个集合: 对于 n 个集合 A_1, A_2, \dots, A_n , 它们的笛卡尔积定义为所有 n 元有序组 (a_1, a_2, \dots, a_n) 组成的集合, 其中 $a_i \in A_i$:

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

当 $A = B$ 时, $A \times A$ 可简写为 A^2 , n 个相同集合 A 的笛卡尔积可简写为 A^n

空集与任何集合的笛卡尔积为空集: $\emptyset \times A = A \times \emptyset = \emptyset$

定理 3.2.1 笛卡尔积的性质

不交换: $(A \times B = B \times A) \Leftrightarrow (A = \emptyset) \vee (B = \emptyset) \vee (A = B)$

分配律: $A \times (B \cup C) = (A \times B) \cup (A \times C)$ $(A \cup B) \times C = (A \times C) \cup (B \times C)$

分配律: $A \times (B \cap C) = (A \times B) \cap (A \times C)$ $(A \cap B) \times C = (A \times C) \cap (B \times C)$

分配律: $A \times (B - C) = (A \times B) - (A \times C)$ $(A - B) \times C = (A \times C) - (B \times C)$

分配律: $(A \oplus B) \times C = (A \times C) \oplus (B \times C)$ $A \times (B \oplus C) = (A \times B) \oplus (A \times C)$

积的交等于交的积: $(A \times C) \cap (B \times D) = (A \cap B) \times (C \cap D)$

积的并蕴含并的积: $(A \times C) \cup (B \times D) \subseteq (A \cup B) \times (C \cup D)$

差的积蕴含积的差: $(A - B) \times (C - D) \subseteq (A \times C) - (B \times D)$ (后者元素数量更多, 基数更大)

存在一个单射: $P(A) \times P(B) \rightarrow P(A \times B)$

单调性: $A \subseteq C \wedge B \subseteq D \Rightarrow A \times B \subseteq C \times D$

注意到性质 4 可以分解为性质 2 和 3, 性质 5 可以分解为性质 234, 下面给出证明:

$$\begin{aligned}
 (x, y) \in A \times (B \cup C) &\Leftrightarrow x \in A \wedge y \in (B \cup C) \Leftrightarrow x \in A \wedge (y \in B \vee y \in C) \\
 &\Leftrightarrow (x \in A \wedge y \in B) \vee (x \in A \wedge y \in C) \\
 &\Leftrightarrow (x, y) \in A \times B \cup A \times C \\
 (x, y) \in A \times (B \cap C) &\Leftrightarrow x \in A \wedge y \in (B \cap C) \Leftrightarrow x \in A \wedge (y \in B \wedge y \in C) \\
 &\Leftrightarrow (x \in A \wedge y \in B \wedge y \in C) \\
 &\Leftrightarrow (x, y) \in A \times B \cap A \times C \\
 (x, y) \in A \times (B - C) &\Leftrightarrow x \in A \wedge y \in (B - C) \Leftrightarrow x \in A \wedge (y \in B \wedge y \notin C) \\
 &\Leftrightarrow (x \in A \wedge y \in B \wedge y \notin C) \\
 &\Leftrightarrow (x, y) \in A \times B - (A \times C) \\
 (x, y) \in (A \oplus B) \times C &\Leftrightarrow x \in (A \oplus B) \wedge y \in C \\
 &\Leftrightarrow (x \in A \wedge x \notin B \wedge y \in C) \vee (x \in B \wedge x \notin A \wedge y \in C) \\
 &\Leftrightarrow (x, y) \in (A \times C) \oplus (B \times C) \\
 (x, y) \in (A \times C) \cap (B \times D) &\Leftrightarrow (x, y) \in A \times C \wedge (x, y) \in B \times D \\
 &\Leftrightarrow (x \in A \wedge y \in C) \wedge (x \in B \wedge y \in D) \\
 &\Leftrightarrow (x \in A \wedge x \in B) \wedge (y \in C \wedge y \in D) \\
 &\Leftrightarrow x \in A \cap B \wedge y \in C \cap D \\
 &\Leftrightarrow (x, y) \in (A \cap B) \times (C \cap D) \\
 (x, y) \in (A \times C) \cup (B \times D) &\Leftrightarrow (x, y) \in A \times C \vee (x, y) \in B \times D \\
 &\Leftrightarrow (x \in A \wedge y \in C) \vee (x \in B \wedge y \in D) \\
 &\Leftrightarrow (x \in A \vee x \in B) \wedge (x \in A \vee y \in D) \\
 &\quad \wedge (y \in C \vee x \in B) \wedge (y \in C \vee y \in D) \\
 &\Rightarrow (x \in A \vee x \in B) \wedge (y \in C \vee y \in D) \\
 &\Leftrightarrow x \in A \cup B \wedge y \in C \cup D \\
 &\Leftrightarrow (x, y) \in (A \cup B) \times (C \cup D) \\
 (x, y) \in (A - B) \times (C - D) &\Leftrightarrow x \in A - B \wedge y \in C - D \\
 &\Leftrightarrow (x \in A \wedge x \notin B) \wedge (y \in C \wedge y \notin D) \\
 &\Leftrightarrow (x \in A \wedge y \in C) \wedge (x \notin B \wedge y \notin D) \\
 &\Rightarrow (x, y) \in A \times C \wedge (x, y) \notin B \times D \\
 &\Leftrightarrow (x, y) \in (A \times C) - (B \times D)
 \end{aligned}$$

最后一个蕴含符号是因为 $(x \notin B \wedge y \notin D) \vee (x \in B \wedge y \notin D) \vee (x \notin B \wedge y \in D) \Leftrightarrow (x, y) \notin B \times D$
 最后一个性质当且仅当 $A = B = \emptyset$ 或 $A, B \neq \emptyset$ 时, 等号成立。

3.3 关系

定义 3.3.1 关系

在集合论中，一个**二元关系**是指元素都是有序对的非空集合，或者空集。二元关系也可以简称为关系。对于二元关系 R ，如果 $(x, y) \in R$ ，则称 x, y 有 R 关系，反之，则称 x, y 没有 R 关系，写作 $x \not\sim y$ ，其中 $A = \text{dom } R, B = \text{ran } R$ ，分别称作**定义域**和**值域**。

全域关系：从 A 到 B 的**全域关系**是完整的笛卡尔积 $A \times B$ ，即包含所有可能有序对的关系。

恒等关系：在集合 A 上的**恒等关系**（或称对角线关系）是所有形如 (a, a) 的有序对组成的集合，其中 $a \in A$

空关系：从 A 到 B 的**空关系**是空集 \emptyset ，即不包含任何有序对的关系。记作 $R = \emptyset$

一个 n 元关系是 n 个集合 A_1, A_2, \dots, A_n 的笛卡尔积的一个子集，即 $R \subseteq A_1 \times A_2 \times \dots \times A_n$ 。

集合 A, B ，如果 $|A| = n, |B| = m$ ，则 $|A \times B| = nm$ ，子集有 2^{mn} 个，所以从 A 到 B 的关系个数为 2^{mn} 。 A 上有 2^{n^2} 个不同的二元关系。比如整除关系， $(2, 6)$ 就属于自然数集上的整数关系。

可以用列举法，描述法来写出集合表示二元关系，如 $>= \{(x, y) | x, y \in \mathbb{R} \wedge x > y\}$

定义 3.3.2 关系图

设 A 是一个有限集合， R 是 A 上的二元关系（即 $R \subseteq A \times A$ ）。 R 的**关系图**是一个有向图：

顶点集：集合 A 中的每个元素对应图中的一个顶点

边集：对于每个有序对 $(a, b) \in R$ ，在图中添加一条从 a 指向 b 的有向边

自环：如果 $(a, a) \in R$ ，则在顶点 a 处添加一个自环

关系图的性质

如果 R 是自反关系，则每个顶点都有自环

如果 R 是对称关系，则任意两个顶点之间要么没有边，要么有双向边

如果 R 是反对称关系，则任意两个不同顶点之间最多只有一条有向边

如果 R 是传递关系，则图中任意两条连续的有向边 $a \rightarrow b$ 和 $b \rightarrow c$ 都对应一条边 $a \rightarrow c$

定义 3.3.3 二元关系的邻接矩阵

设 $A = \{a_1, a_2, \dots, a_m\}$ 和 $B = \{b_1, b_2, \dots, b_n\}$ 是有限集合， $R \subseteq A \times B$ 是一个从 A 到 B 的二元关系。 R 的**邻接矩阵**是一个 $m \times n$ 的矩阵 $M_R = [m_{ij}]$ ，其中元素定义为：

$$m_{ij} = \begin{cases} 1, & \text{如果 } (a_i, b_j) \in R \\ 0, & \text{如果 } (a_i, b_j) \notin R \end{cases}$$

特殊情况：当 $A = B$ 时，邻接矩阵是方阵，当 R 是空关系时，邻接矩阵是全零矩阵

当 R 是全域关系时，邻接矩阵是全一矩阵，当 R 是恒等关系 I_A 时，邻接矩阵是单位矩阵

性质：关系的并、交、补运算对应矩阵的布尔运算，关系的复合运算对应矩阵的布尔乘法，关系的逆对应矩阵的转置

定义 3.3.4 关系的逆运算

设 R 是一个从集合 A 到集合 B 的二元关系，即 $R \subseteq A \times B$ 。关系 R 的逆运算定义为一个新关系 R^{-1} ，它是从 B 到 A 的关系，用集合描述法表示为：

$$R^{-1} = \{(b, a) \mid (a, b) \in R\}$$

其中， $R^{-1} \subseteq B \times A$ 。逆运算将原关系中的每个有序对的顺序反转。

由于逆运算只是反转了有序对的顺序，所以有以下性质成立：

定理 3.3.1 关系的逆运算的性质

设 R 和 S 是从集合 A 到集合 B 的二元关系， Q 是从 B 到集合 C 的二元关系：

1. 双重逆定理： $(R^{-1})^{-1} = R$
2. 并集的逆： $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$
3. 交集的逆： $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$
4. 差集的逆： $(R - S)^{-1} = R^{-1} - S^{-1}$
5. 补集的逆： $(\sim R)^{-1} = \sim (R^{-1})$ ，其中 $\sim R = (A \times B) - R$ 是 R 的补集
6. 复合关系的逆： $(Q \circ R)^{-1} = R^{-1} \circ Q^{-1}$ ，其中 $Q \circ R$ 是关系复合运算
7. 包含关系的逆：如果 $R \subseteq S$ ，则 $R^{-1} \subseteq S^{-1}$
8. 域和值域的关系： $\text{dom}(R^{-1}) = \text{ran}(R)$, $\text{ran}(R^{-1}) = \text{dom}(R)$

定义 3.3.5 关系的复合运算

设 R 是从集合 A 到集合 B 的二元关系， S 是从集合 B 到集合 C 的二元关系，即 $R \subseteq A \times B$, $S \subseteq B \times C$ 。 R 与 S 的复合关系（或称合成关系）是一个从 A 到 C 的二元关系，记作 $S \circ R$

$$S \circ R = \{(a, c) \in A \times C \mid \exists b \in B : (a, b) \in R \wedge (b, c) \in S\}$$

如果使用关系图表示关系的复合运算，就是将两张关系图“合并”，**步骤 1：绘制原始关系图**，绘制 R 的关系图： A 中元素指向 B 中元素的有向边，绘制 S 的关系图： B 中元素指向 C 中元素的有向边。**步骤 2：寻找连接路径**：对于每个 $a \in A$ 和 $c \in C$ ，检查是否存在中间元素 $b \in B$ ，如果存在路径 $a \rightarrow b$ （属于 R ）和 $b \rightarrow c$ （属于 S ），则在复合关系图中添加边 $a \rightarrow c$ 。**步骤 3：构建复合关系图**：复合关系图包含顶点集 $A \cup C$ （中间集合 B 的顶点不出现），边集由所有满足条件的 $a \rightarrow c$ 组成，这相当于在原始图中寻找长度为 2 的路径并直接连接起点和终点。

定理 3.3.2 关系的复合运算的性质

$$(S \cup P) \circ R = (S \circ R) \cup (P \circ R) \quad R \circ (S \cup P) = (R \circ S) \cup (R \circ P)$$

$$(S \cap P) \circ R \subseteq (S \circ R) \cap (P \circ R) \quad R \circ (S \cap P) \subseteq (R \circ S) \cap (R \circ P)$$

$$(Q \circ R)^{-1} = R^{-1} \circ Q^{-1}$$

为什么一个相等，另一个只有包含关系？其实，是因为把复合运算用谓词逻辑表达后，量词是存在量词，辖域为整个公式，所以如果括号内部是析取，就可以直接等价（分配律），如果括号内部是合取，则需要弱化： $\exists x(P(x) \wedge Q(x)) \Rightarrow \exists xP(x) \wedge \exists xQ(x)$ ，下面给出证明：

$$\begin{aligned}
\forall(x, y) \in (S \cup P) \circ R &\Leftrightarrow \exists z((x, z) \in R \wedge (z, y) \in S \cup P) \\
&\Leftrightarrow \exists z((x, z) \in R \wedge ((z, y) \in S \vee (z, y) \in P)) \\
&\Leftrightarrow \exists z(((x, z) \in R \wedge (z, y) \in S) \vee ((x, z) \in R \wedge (z, y) \in P)) \\
&\Leftrightarrow \exists z((x, z) \in R \wedge (z, y) \in S) \vee \exists z((x, z) \in R \wedge (z, y) \in P) \\
&\Leftrightarrow (x, y) \in S \circ R \vee (x, y) \in P \circ R \\
&\Leftrightarrow (x, y) \in (S \circ R) \cup (P \circ R) \\
\\
\forall(x, y) \in R \circ (S \cup P) &\Leftrightarrow \exists z((x, z) \in S \cup P \wedge (z, y) \in R) \\
&\Leftrightarrow \exists z(((x, z) \in S \vee (x, z) \in P) \wedge (z, y) \in R) \\
&\Leftrightarrow \exists z(((x, z) \in S \wedge (z, y) \in R) \vee ((x, z) \in P \wedge (z, y) \in R)) \\
&\Leftrightarrow \exists z((x, z) \in S \wedge (z, y) \in R) \vee \exists z((x, z) \in P \wedge (z, y) \in R) \\
&\Leftrightarrow (x, y) \in R \circ S \vee (x, y) \in R \circ P \\
&\Leftrightarrow (x, y) \in (R \circ S) \cup (R \circ P) \\
\\
\forall(x, y) \in (S \cap P) \circ R &\Leftrightarrow \exists z((x, z) \in R \wedge (z, y) \in S \cap P) \\
&\Leftrightarrow \exists z((x, z) \in R \wedge ((z, y) \in S \wedge (z, y) \in P)) \\
&\Rightarrow \exists z((x, z) \in R \wedge (z, y) \in S) \wedge \exists z((x, z) \in R \wedge (z, y) \in P) \\
&\Leftrightarrow (x, y) \in S \circ R \wedge (x, y) \in P \circ R \\
&\Leftrightarrow (x, y) \in (S \circ R) \cap (P \circ R) \\
\\
\forall(x, y) \in R \circ (S \cap P) &\Leftrightarrow \exists z((x, z) \in S \cap P \wedge (z, y) \in R) \\
&\Leftrightarrow \exists z(((x, z) \in S \wedge (x, z) \in P) \wedge (z, y) \in R) \\
&\Rightarrow \exists z((x, z) \in S \wedge (z, y) \in R) \wedge \exists z((x, z) \in P \wedge (z, y) \in R) \\
&\Leftrightarrow (x, y) \in R \circ S \wedge (x, y) \in R \circ P \\
&\Leftrightarrow (x, y) \in (R \circ S) \cap (R \circ P)
\end{aligned}$$

设 $R \subseteq A \times B$ 和 $Q \subseteq B \times C$ 是二元关系。证明 $(Q \circ R)^{-1} = R^{-1} \circ Q^{-1}$ ，对于任意有序对 (c, a) ，有：

$$\begin{aligned}
(c, a) \in (Q \circ R)^{-1} &\Leftrightarrow (a, c) \in Q \circ R \\
&\Leftrightarrow \exists b \in B((a, b) \in R \wedge (b, c) \in Q) \\
&\Leftrightarrow \exists b \in B((b, a) \in R^{-1} \wedge (c, b) \in Q^{-1}) \\
&\Leftrightarrow (c, a) \in R^{-1} \circ Q^{-1}
\end{aligned}$$

因此， $(Q \circ R)^{-1} = R^{-1} \circ Q^{-1}$ 成立。

证明：设 A 是 R 上的关系，则 $R \circ I_A = I_A \circ R = R$

$$\begin{aligned} (x, y) \in R \circ I_A &\Leftrightarrow \exists z \in A, ((x, z) \in I_A \wedge (z, y) \in R) \\ &\Leftrightarrow \exists z (z \in A \wedge x = z \wedge (z, y) \in R) \\ &\Rightarrow (x, y) \in R \quad \text{存在量词的合取性质} \\ (x, y) \in R &\Rightarrow (x, x) \in I_A \wedge (x, y) \in R \\ &\Rightarrow (x, y) \in R \end{aligned}$$

定义 3.3.6 关系的幂

设 R 是集合 A 上的二元关系（即 $R \subseteq A \times A$ ）。关系 R 的幂 R^n （其中 n 是非负整数）递归定义如下，其中 $I_A = \{(a, a) \mid a \in A\}$ 是 A 上的恒等关系， \circ 表示关系的复合运算。关系幂的性质包括： $R^m \circ R^n = R^{m+n}$, $(R^m)^n = R^{mn}$:

$$R^0 = I_A \quad (\text{恒等关系})$$

$$R^n = R \circ R^{n-1} \quad \text{对于 } n \geq 1$$

性质 1: $R^m \circ R^n = R^{m+n}$, 对 n 进行数学归纳法。

基础步骤: 当 $n = 0$ 时, $R^m \circ R^0 = R^m \circ I_A = R^m = R^{m+0}$

归纳假设: 假设对于 $n = k$ 有 $R^m \circ R^k = R^{m+k}$, 当 $n = k + 1$ 时

$$\begin{aligned} R^m \circ R^{k+1} &= R^m \circ (R \circ R^k) \\ &= (R^m \circ R) \circ R^k \quad (\text{复合运算结合律}) \\ &= R^{m+1} \circ R^k \\ &= R^{(m+1)+k} \quad (\text{归纳假设}) \\ &= R^{m+(k+1)} \end{aligned}$$

因此, 由数学归纳法, 性质 1 成立。

性质 2: $(R^m)^n = R^{mn}$ 对 n 进行数学归纳法。

基础步骤: 当 $n = 0$, $(R^m)^0 = I_A = R^0 = R^{m \cdot 0}$

归纳假设: 假设对于 $n = k$ 有 $(R^m)^k = R^{mk}$, 当 $n = k + 1$ 时

$$\begin{aligned} (R^m)^{k+1} &= (R^m)^k \circ R^m \\ &= R^{mk} \circ R^m \quad (\text{归纳假设}) \\ &= R^{mk+m} \quad (\text{性质 1}) \\ &= R^{m(k+1)} \end{aligned}$$

因此, 由数学归纳法, 性质 2 成立。

定理 3.3.3 关系的幂的性质

设 R_1, R_2, R_3 是集合 A 上的二元关系, 如果 $R_1 \subseteq R_2$ 那么:

- (1) $R_1 \circ R_3 \subseteq R_2 \circ R_3$
- (2) $R_3 \circ R_1 \subseteq R_3 \circ R_2$

证明(1): 设 $(x, z) \in R_1 \circ R_3$, 则存在 $y \in A$ 使得 $(x, y) \in R_1$ 且 $(y, z) \in R_3$ 。由于 $R_1 \subseteq R_2$, 有 $(x, y) \in R_2$, 因此 $(x, z) \in R_2 \circ R_3$ 。故 $R_1 \circ R_3 \subseteq R_2 \circ R_3$ 。

证明(2): 设 $(x, z) \in R_3 \circ R_1$, 则存在 $y \in A$ 使得 $(x, y) \in R_3$ 且 $(y, z) \in R_1$ 。由于 $R_1 \subseteq R_2$, 有 $(y, z) \in R_2$, 因此 $(x, z) \in R_3 \circ R_2$ 。故 $R_3 \circ R_1 \subseteq R_3 \circ R_2$ 。

定理 3.3.4 关系的幂的性质

设 R 是集合 A 上的二元关系 (即 $R \subseteq A \times A$), 且 $|A| = n$, 则存在自然数 s, t , 使得

- (1) $R^s = R^t, 0 \leq s < t \leq 2^{n^2}$
- (2) 对任意 $k \in \mathbb{N}, R^{s+k} = R^{t+k}$

设 $|A| = n$, 则 $A \times A$ 的子集个数为 2^{n^2} , 即不同的二元关系最多有 2^{n^2} 个。

考虑序列 $R^0, R^1, R^2, \dots, R^{2^{n^2}}$, 共 $2^{n^2} + 1$ 个关系。由鸽巢原理, 必存在 $0 \leq s < t \leq 2^{n^2}$ 使得 $R^s = R^t$, 这就证明了性质(1)。对于性质(2), 对任意 $k \in \mathbb{N}$, 有:

$$\begin{aligned} R^{s+k} &= R^s \circ R^k \quad (\text{幂的定义}) \\ &= R^t \circ R^k \quad (\text{由 } R^s = R^t) \\ &= R^{t+k} \quad (\text{幂的定义}) \end{aligned}$$

因此, $R^{s+k} = R^{t+k}$ 对任意 $k \in \mathbb{N}$ 成立。

定义 3.3.7 布尔加和布尔乘，用矩阵表示关系的复合

布尔加（逻辑或运算）：定义两个布尔值 a 和 b 的布尔加为：

$$a \vee b = \begin{cases} 1, & \text{如果 } a = 1 \text{ 或 } b = 1 \\ 0, & \text{否则} \end{cases}$$

布尔加对应逻辑或运算，满足交换律、结合律和幂等律。

布尔乘（逻辑与运算）：定义两个布尔值 a 和 b 的布尔乘为：

$$a \wedge b = \begin{cases} 1, & \text{如果 } a = 1 \text{ 且 } b = 1 \\ 0, & \text{否则} \end{cases}$$

布尔乘对应逻辑与运算，满足交换律、结合律和分配律。

邻接矩阵布尔乘法：设 A 和 B 是两个布尔矩阵，其乘积 $C = A \cdot B$ 通过布尔运算定义：

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

其中： \wedge 表示布尔乘（逻辑与），用于计算对应元素的乘积， \vee 表示布尔加（逻辑或），用于累积部分结果，运算结果 $c_{ij} = 1$ 当且仅当存在 k 使得 $a_{ik} = 1$ 且 $b_{kj} = 1$ ，这种布尔矩阵乘法正好对应关系复合的邻接矩阵计算： $M_{S \circ R} = M_R \cdot M_S$ 。

翻译成人话，就是：确定 A, B 相乘之后的矩阵 C 的位于某一行某一列的元素，就需要把 A 的对应的行向量和 B 的对应的列向量（先转置，变成横的）抽出来做布尔点积（当我们定义了布尔加和布尔乘，布尔点积就被定义了）。考虑以下示例中使用的矩阵：

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad AB = \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}$$

3.4 自反, 对称, 传递关系, 闭包

定义 3.4.1 自反, 对称, 传递关系

设 R 是集合 A 上的二元关系 (即 $R \subseteq A \times A$)。

自反关系: R 是自反的当且仅当对于所有 $a \in A$, 都有 $(a, a) \in R$ 。即: $\forall a \in A, (a, a) \in R$

对称关系: R 是对称的当且仅当对于所有 $a, b \in A$, 如果 $(a, b) \in R$, 则 $(b, a) \in R$ 。即:

$$\forall a, b \in A, (a, b) \in R \Rightarrow (b, a) \in R$$

传递关系: R 是传递的当且仅当对于所有 $a, b, c \in A$, 如果 $(a, b) \in R$ 且 $(b, c) \in R$, 则 $(a, c) \in R$ 。

即: $\forall a, b, c \in A, [(a, b) \in R \wedge (b, c) \in R] \Rightarrow (a, c) \in R$

反自反关系: R 是反自反的当且仅当对于所有 $a \in A$, 都有 $(a, a) \notin R$ 。即: $\forall a \in A, (a, a) \notin R$

反对称关系: R 是反对称的当且仅当对于所有 $a, b \in A$, 如果 $(a, b) \in R$ 且 $(b, a) \in R$, 则 $a = b$ 。即: $\forall a, b \in A, [(a, b) \in R \wedge (b, a) \in R] \Rightarrow a = b$

引入关系图, 那么自反关系当且仅当每一个结点都有环, 反自反关系当且仅当每一个结点都没有环, 对称关系当且仅当每两个结点之间要么有 2 条反向的有向边 (可以视作无向边), 要么没有边; 反对称关系当且仅当每两个结点之间要么没有边, 要么只可以有一条有向边。传递关系当且仅当在关系图中若存在结点 a 到 b 的有向边和结点 b 到 c 的有向边, 则有结点 a 到 c 的有向边。

如果引入邻接矩阵的话, 自反关系对应矩阵的对角线元素全为 1, 反自反关系对应矩阵的对角线元素全为 0, 对称关系对应矩阵是对称矩阵, 反对称关系对应矩阵是反对称矩阵, 传递关系满足其矩阵的 2 次幂所对应的关系包含于 1 次幂所对应的关系。

但是要注意: 一个关系不可能同时是自反或者反自反关系, 但是也可能既不是自反的, 也不是反自反的。一个矩阵可以同时是对称的和反对称的 (如空关系), 但是也可能既不是对称的, 也不是反对称的。

空关系和单元素关系 (只包含零个, 一个有序对的关系) 总是传递的, 因为当一个命题的前提为假的时候, 结论总为真。

定理 3.4.1 自反对称传递关系的性质

- (1) R 是自反的当且仅当 $I_A \subseteq R$, R 是反自反的当且仅当 $R - I_A = R$
- (2) R 是对称的当且仅当 $R = R^T$, R 是反对称的当且仅当 $R \cap R^T \subseteq I_A$
- (3) R 是传递的当且仅当 $R^2 \subseteq R$

定理 3.4.2 关系运算对关系属性的保持性

设 R_1, R_2 是集合 A 上的二元关系。各种关系运算对关系属性的保持性如下：

运算	自反性	反自反性	对称性	反对称性	传递性	等价性
逆运算 R^{-1}	保持	保持	保持	保持	保持	保持
交集 $R_1 \cap R_2$	保持	保持	保持	保持	保持	保持
并集 $R_1 \cup R_2$	保持	保持	保持	不一定	不一定	不一定
差集 $R_1 - R_2$	不一定	保持	保持	保持	保持	不一定
对称差 $R_1 \oplus R_2$	不一定	保持	保持	不一定	不一定	不一定
复合 $R_1 \circ R_2$	保持	不一定	不一定	不一定	不一定	不一定
幂运算 R^n	保持	保持	不一定	不一定	保持	不一定

详细说明与反例：

自反性：自反关系是否能维持，取决于每一个结点的自环有没有受到影响，显然，并集、交集、逆、复合、幂运算保持自反性，差集不一定保持（注意不是一定不保持，因为我们可以让邻接矩阵的大小不同，做差后主对角线上还会有 1）

反自反性：和自反关系类似的是，并集、交集、逆、幂运算保持反自反性，但是，差集、对称差、也会保持，这是因为两个集合中都没有形如 (x, x) 的有序对，所以不管怎么交怎么并怎么做差，都不会影响到反自反性。但是，复合不一定保持：如 $R_1 = \{(1, 2)\}$, $R_2 = \{(2, 1)\}$, 则 $R_1 \circ R_2 = \{(1, 1)\}$ 不是反自反的

对称性：并集、交集、逆、差集（显然，如果做差会消去元素的话，那一定是成对地消去有序对）、对称差（差集和并集保持，那么对称差保持）保持对称性，复合、幂运算不一定保持：如 $A = \{1, 2, 3\}$, $R = \{(1, 2), (2, 1), (2, 3)\}$ 对称，但 $R^2 = \{(1, 1), (1, 3), (2, 2)\}$ 不对称

反对称性：交集、差集保持反对称性；并集、对称差、复合、幂运算不一定保持：如 $A = \{1, 2\}$, $R_1 = \{(1, 2)\}$, $R_2 = \{(2, 1)\}$ 都反对称，但 $R_1 \cup R_2$ 不反对称，并集的情况很好理解，因为 R_1, R_2 两个矩阵合在一起，明显可能会导致有元素关于对角线对称。由此，对称差因为含有并集运算，所以也显然不一定维持，幂运算可能会出现 $R_1 = \{(1, 2), (3, 2)\}$, $R_2 = \{(2, 3), (2, 1)\}$, 则 $R_1 \circ R_2 = \{(1, 1), (1, 3), (3, 3), (3, 1)\}$, 不是反对称的

传递性：交集、幂运算保持传递性，并集、对称差、复合不一定保持：如 $A = \{1, 2\}$, $R_1 = \{(1, 2)\}$, $R_2 = \{(2, 1)\}$ 都传递，但 $R_1 \cup R_2$ 不传递，进而对称差也不一定维持，考虑集合 $A = \{1, 2, 3, 4\}$ ，定义两个关系： $R = \{(1, 2), (3, 4)\}$ $S = \{(2, 3), (4, 1)\}$ ，计算复合关系 $R \circ S$: $R \circ S = \{(1, 3), (3, 1)\}$ ，因此， $R \circ S$ 不满足传递性。此反例证明传递关系的复合不一定传递。

定义 3.4.2 等价关系

设 R 是集合 A 上的二元关系（即 $R \subseteq A \times A$ ）。如果 R 同时满足是自反的，对称的，传递的，则称 R 为等价关系。若 (x, y) 属于此集合中，记作 $x \sim y$

定义 3.4.3 自反/对称/传递闭包

设 R 是集合 A 上的二元关系。若 R' 满足 $R' \subseteq R$ 且 R' 是自反/对称/传递的, 且对 A 上任何包含 R 的关系 R'' , 都有 $R' \subseteq R''$, 则称 R' 是 R 的自反/对称/传递闭包。

自反闭包: R 的自反闭包是包含 R 的最小自反关系, 记作 $r(R)$, 定义为:

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

其中 $I_A = \{(a, a) \mid a \in A\}$ 是 A 上的恒等关系。

对称闭包: R 的对称闭包是包含 R 的最小对称关系, 记作 $s(R)$, 定义为:

$$s(R) = R \cup R^{-1}$$

其中 $R^{-1} = \{(b, a) \mid (a, b) \in R\}$ 是 R 的逆关系。

传递闭包: R 的传递闭包是包含 R 的最小传递关系, 记作 $t(R)$, 定义为:

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

其中 R^n 表示关系 R 的 n 次幂 (关系的复合)。对于元素个数为 n 的集合 A 来说, A 上的关系 R 的传递闭包又可以写作:

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

R 的自反对称传递闭包写作 $tsr(R) = t(s(r(R)))$.

要证明 $\bigcup_{n=1}^{\infty} R^n = R \cup R^2 \cup R^3 \cup \dots$ 是 R 的传递闭包, 需要证明 3 个性质:

1. 包含性: $R \subseteq \bigcup_{n=1}^{\infty} R^n$, 显然当 $n = 1$ 时, $R^1 = R$, 所以 $R \subseteq \bigcup_{n=1}^{\infty} R^n$ 。

2. 传递性: $\bigcup_{n=1}^{\infty} R^n$ 是传递的, 设 $(a, b) \in \bigcup_{n=1}^{\infty} R^n$ 且 $(b, c) \in \bigcup_{n=1}^{\infty} R^n$, 则存在 $m, n \geq 1$ 使得: $(a, b) \in R^m, (b, c) \in R^n$, 由关系幂的性质, $(a, c) \in R^m \circ R^n = R^{m+n}$, 而 $R^{m+n} \subseteq \bigcup_{n=1}^{\infty} R^n$, 所以 $(a, c) \in \bigcup_{n=1}^{\infty} R^n$ 。

3. 最小性: $\bigcup_{n=1}^{\infty} R^n$ 是最小的传递关系

用数学归纳法证明: 设 T 是任意包含 R 的传递关系, 则对任意 $n \geq 1$, $R^n \subseteq T$ 。

基础情况: $n = 1$ 时, $R^1 = R \subseteq T$ 。

归纳假设: 假设 $R^k \subseteq T$ 对某个 $k \geq 1$ 成立。

归纳步骤: 对于 $R^{k+1} = R^k \circ R$,

$$\begin{aligned} (a, b) \in R^{k+1} &\Rightarrow \exists c \text{ 使得 } (a, c) \in R^k \text{ 且 } (c, b) \in R \\ &\Rightarrow (a, c) \in T \text{ 且 } (c, b) \in T \quad (\text{归纳假设和 } R \subseteq T) \\ &\Rightarrow (a, b) \in T \quad (\text{因为 } T \text{ 是传递的}) \end{aligned}$$

所以 $R^{k+1} \subseteq T$ 。

由数学归纳法, 对所有 $n \geq 1$, $R^n \subseteq T$, 因此 $\bigcup_{n=1}^{\infty} R^n \subseteq T$ 。

结论: $\bigcup_{n=1}^{\infty} R^n$ 是包含 R 的最小传递关系, 即传递闭包。

定理 3.4.3 闭包的性质

设 R_1, R_2 是集合 A 上的二元关系, 则:

- (1) $R_1 \subseteq R_2 \Rightarrow r(R_1) \subseteq r(R_2)$
- (2) $R_1 \subseteq R_2 \Rightarrow s(R_1) \subseteq s(R_2)$
- (3) $R_1 \subseteq R_2 \Rightarrow t(R_1) \subseteq t(R_2)$
- (4) $r(R_1) \cup r(R_2) = r(R_1 \cup R_2) \quad r(R_1) \cap r(R_2) = r(R_1 \cap R_2)$
- (5) $s(R_1) \cup s(R_2) = s(R_1 \cup R_2) \quad s(R_1 \cap R_2) \subseteq s(R_1) \cap s(R_2)$
- (6) $t(R_1) \cup t(R_2) \subseteq t(R_1 \cup R_2) \quad t(R_1 \cap R_2) \subseteq t(R_1) \cap t(R_2)$

性质 1: 由于 $R_1 \subseteq R_2$, 且 $I_A \subseteq I_A$, 故 $r(R_1) = R_1 \cup I_A \subseteq R_2 \cup I_A = r(R_2)$ 。

性质 2: 由于 $R_1 \subseteq R_2$, 则 $R_1^{-1} \subseteq R_2^{-1}$, 故 $s(R_1) = R_1 \cup R_1^{-1} \subseteq R_2 \cup R_2^{-1} = s(R_2)$ 。

性质 3: 由于 $R_1 \subseteq R_2$, 则对任意 $n \geq 1$ 有 $R_1^n \subseteq R_2^n$, 故 $t(R_1) = \bigcup_{n=1}^{\infty} R_1^n \subseteq \bigcup_{n=1}^{\infty} R_2^n = t(R_2)$ 。

性质 4:

$$\begin{aligned} r(R_1) \cup r(R_2) &= (R_1 \cup I_A) \cup (R_2 \cup I_A) = (R_1 \cup R_2) \cup I_A = r(R_1 \cup R_2) \\ r(R_1) \cap r(R_2) &= (R_1 \cup I_A) \cap (R_2 \cup I_A) = (R_1 \cap R_2) \cup I_A = r(R_1 \cap R_2) \end{aligned}$$

性质 5: 由于 $R_1 \cap R_2 \subseteq R_1$ 且 $R_1 \cap R_2 \subseteq R_2$, 由单调性得 $s(R_1 \cap R_2) \subseteq s(R_1) \cap s(R_2)$ 。另外:

$$\begin{aligned} s(R_1) \cup s(R_2) &= (R_1 \cup R_1^{-1}) \cup (R_2 \cup R_2^{-1}) \\ &= (R_1 \cup R_2) \cup (R_1^{-1} \cup R_2^{-1}) \\ &= (R_1 \cup R_2) \cup (R_1 \cup R_2)^{-1} = s(R_1 \cup R_2) \end{aligned}$$

性质 6: 由单调性, $t(R_1) \subseteq t(R_1 \cup R_2)$ 且 $t(R_2) \subseteq t(R_1 \cup R_2)$, 故并集包含于右边。同理, 由 $R_1 \cap R_2 \subseteq R_1$ 和 $R_1 \cap R_2 \subseteq R_2$, 得 $t(R_1 \cap R_2) \subseteq t(R_1) \cap t(R_2)$ 。

定理 3.4.4 闭包运算的复合

- (1) $s(r(R)) = r(s(R))$
- (2) $r(t(R)) = t(r(R))$
- (3) $s(t(R)) \subseteq t(s(R))$

(1) 性质 1 证明如下:

$$\begin{aligned} s(r(R)) &= s(R \cup I_A) = (R \cup I_A) \cup (R \cup I_A)^{-1} \quad (\text{对称闭包定义}) \\ &= R \cup I_A \cup R^{-1} \cup I_A^{-1} \quad (\text{逆运算分配律}) = R \cup R^{-1} \cup I_A \quad (\text{因为 } I_A^{-1} = I_A) \\ r(s(R)) &= r(R \cup R^{-1}) = (R \cup R^{-1}) \cup I_A \quad (\text{自反闭包定义}) = R \cup R^{-1} \cup I_A \end{aligned}$$

(2) 性质 2 证明如下:

$$r(t(R)) = t(R) \cup I_A \quad t(r(R)) = t(R \cup I_A)$$

由于 $R \cup I_A \subseteq t(R) \cup I_A$, 且 $t(R) \cup I_A$ 是传递的, 所以 $t(R \cup I_A) \subseteq t(R) \cup I_A$ 。由于 $R \subseteq R \cup I_A \subseteq t(R \cup I_A)$ 且 $I_A \subseteq t(R \cup I_A)$, 所以 $t(R) \subseteq t(R \cup I_A)$, 故 $t(R) \cup I_A \subseteq t(R \cup I_A)$

(3) 性质 3 证明如下：

$$s(t(R)) = t(R) \cup t(R)^{-1} \quad t(s(R)) = t(R \cup R^{-1})$$

由于 $t(R) \subseteq t(R \cup R^{-1}) = t(s(R))$, 且 $t(R)^{-1} = t(R^{-1}) \subseteq t(R^{-1} \cup R) = t(s(R))$ (因为 $R^{-1} \subseteq s(R)$), 所以：

$$s(t(R)) = t(R) \cup t(R)^{-1} \subseteq t(s(R)) \cup t(s(R)) = t(s(R))$$

因此, $s(t(R)) \subseteq t(s(R))$ 。这个结论告诉我们; 传递关系的对称闭包可能会丢失传递性, 但是对称关系的传递闭包不会丢失对称性。比如关系 $R = \{(1, 2), (3, 2)\}$ 是传递的, 但是其对称闭包 $s(R) = \{(1, 2), (2, 1), (2, 3), (3, 2)\}$ 并不是传递的.

定理 3.4.5 自反传递对称闭包

R 是非空集合上的二元关系, 则 $tsr(R) = t(s(r(R)))$ 是包含 R 的最小等价关系。

设 $E = t(s(r(R)))$ 。需要证明以下三点:

1. 包含性: 由于 $r(R) \supseteq R$, $s(r(R)) \supseteq r(R) \supseteq R$, 且 $t(s(r(R))) \supseteq s(r(R)) \supseteq R$, 故 $E \supseteq R$ 。

2. E 是等价关系:

自反性: $r(R)$ 是自反的, $s(r(R))$ 保持自反性 (对称闭包不破坏自反性), $t(s(r(R)))$ 也保持自反性 (传递闭包不破坏自反性), 故 E 是自反的。

对称性: $s(r(R))$ 是对称的 (因为对称闭包)。若 S 是对称关系, 则 $t(S)$ 也是对称的 (因为若 $(x, y) \in t(S)$, 则存在路径 $x = x_0, x_1, \dots, x_n = y$ 使得 $(x_i, x_{i+1}) \in S$; 由对称性, 路径反向 $y = x_n, x_{n-1}, \dots, x_0 = x$ 也在 S 中, 故 $(y, x) \in t(S)$)。因此 E 是对称的。

传递性: 由传递闭包的定义, E 是传递的。

3. 最小性: 设 E' 是任意包含 R 的等价关系。由于 E' 是自反的, $E' \supseteq r(R)$; 由于 E' 是对称的, $E' \supseteq s(r(R))$; 由于 E' 是传递的, $E' \supseteq t(s(r(R))) = E$ 。故 E 是包含 R 的最小等价关系。

3.5 Warshell 算法

设 $A = \{1, 2, 3, 4, 5\}$, 关系 R 的邻接矩阵为:

$$M = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

这个关系表示一个有向环: $1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 1$ 。

应用 Warshall 算法:

迭代 1 ($k = 1$): 先关注第一列，因为我们需要关注是否存在某个有序对的后一个数是 1，然后，再关注是否存在某个有序对前一个数是 1，显然此时就要看第一行了。循环往复这个过程知道遍历完成。

$$\begin{aligned} M^*[5, 1] \wedge M^*[1, 2] &= 1 \wedge 1 = 1 \Rightarrow M^*[5, 2] = 0 \vee 1 = 1 \\ M^*[5, 1] \wedge M^*[1, 3] &= 1 \wedge 0 = 0 \Rightarrow M^*[5, 3] = 0 \\ M^*[5, 1] \wedge M^*[1, 4] &= 1 \wedge 0 = 0 \Rightarrow M^*[5, 4] = 0 \\ M^*[5, 1] \wedge M^*[1, 5] &= 1 \wedge 0 = 0 \Rightarrow M^*[5, 5] = 0 \end{aligned}$$

更新后矩阵：

$$M^* = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

迭代 2 ($k = 2$): 先关注第二列，因为我们需要关注是否存在某个有序对的后一个数是 2，然后，再关注是否存在某个有序对前一个数是 2，显然此时就要看第二行了。循环往复这个过程知道遍历完成。

$$\begin{aligned} M^*[1, 2] \wedge M^*[2, 3] &= 1 \wedge 1 = 1 \Rightarrow M^*[1, 3] = 0 \vee 1 = 1 \\ M^*[5, 2] \wedge M^*[2, 3] &= 1 \wedge 1 = 1 \Rightarrow M^*[5, 3] = 0 \vee 1 = 1 \\ M^*[1, 2] \wedge M^*[2, 4] &= 1 \wedge 0 = 0 \Rightarrow M^*[1, 4] = 0 \\ M^*[1, 2] \wedge M^*[2, 5] &= 1 \wedge 0 = 0 \Rightarrow M^*[1, 5] = 0 \end{aligned}$$

更新后矩阵：

$$M^* = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

迭代 3 ($k = 3$): 先关注第三列，因为我们需要关注是否存在某个有序对的后一个数是 3，然后，再关注是否存在某个有序对前一个数是 3，显然此时就要看第三行了。循环往复这个过程知道遍历完成。

$$\begin{aligned} M^*[1, 3] \wedge M^*[3, 4] &= 1 \wedge 1 = 1 \Rightarrow M^*[1, 4] = 0 \vee 1 = 1 \\ M^*[2, 3] \wedge M^*[3, 4] &= 1 \wedge 1 = 1 \Rightarrow M^*[2, 4] = 0 \vee 1 = 1 \\ M^*[5, 3] \wedge M^*[3, 4] &= 1 \wedge 1 = 1 \Rightarrow M^*[5, 4] = 0 \vee 1 = 1 \end{aligned}$$

更新后矩阵:

$$M^* = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

迭代 4 ($k = 4$): 先关注第四列, 因为我们需要关注是否存在某个有序对的后一个数是 4, 然后, 再关注是否存在某个有序对前一个数是 4, 显然此时就要看第四行了。循环往复这个过程知道遍历完成。

$$M^*[1, 4] \wedge M^*[4, 5] = 1 \wedge 1 = 1 \Rightarrow M^*[1, 5] = 0 \vee 1 = 1$$

$$M^*[2, 4] \wedge M^*[4, 5] = 1 \wedge 1 = 1 \Rightarrow M^*[2, 5] = 0 \vee 1 = 1$$

$$M^*[3, 4] \wedge M^*[4, 5] = 1 \wedge 1 = 1 \Rightarrow M^*[3, 5] = 0 \vee 1 = 1$$

$$M^*[5, 4] \wedge M^*[4, 5] = 1 \wedge 1 = 1 \Rightarrow M^*[5, 5] = 0 \vee 1 = 1$$

更新后矩阵:

$$M^* = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

迭代 5 ($k = 5$): 先关注第五列, 因为我们需要关注是否存在某个有序对的后一个数是 5, 然后, 再关注是否存在某个有序对前一个数是 5, 显然此时就要看第五行了。循环往复这个过程知道遍历完成。**迭代 5 ($k = 5$):**

$$M^*[1, 5] \wedge M^*[5, 1] = 1 \wedge 1 = 1 \Rightarrow M^*[1, 1] = 0 \vee 1 = 1$$

$$M^*[2, 5] \wedge M^*[5, 2] = 1 \wedge 1 = 1 \Rightarrow M^*[2, 2] = 0 \vee 1 = 1$$

$$M^*[3, 5] \wedge M^*[5, 3] = 1 \wedge 1 = 1 \Rightarrow M^*[3, 3] = 0 \vee 1 = 1$$

$$M^*[4, 5] \wedge M^*[5, 4] = 1 \wedge 1 = 1 \Rightarrow M^*[4, 4] = 0 \vee 1 = 1$$

最终传递闭包矩阵:

$$M^* = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

结果分析: 由于原关系构成一个有向环, 传递闭包是全关系, 即任意两个顶点之间都存在路径。这个例子展示了 Warshall 算法如何处理复杂的有向图结构。

3.6 等价关系, 等价类, 覆盖和划分

定义 3.6.1 等价类, 商集, 覆盖, 划分, 类, 块

设 R 是集合 A 上的一个等价关系 (即 R 满足自反性、对称性和传递性)。对于任意元素 $a \in A$, a 的等价类定义为:

$$[a]_R = \{x \in A \mid (a, x) \in R\}$$

商集: 所有等价类构成的集合称为 A 关于 R 的商集, 记作:

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

设 A 是一个非空集合, $\mathcal{C} = \{A_1, A_2, \dots, A_n\}$ 是 A 的一族非空子集。

覆盖: 如果 \mathcal{C} 满足 $\bigcup_{i=1}^n A_i = A$, 则称 \mathcal{C} 是 A 的一个覆盖。

划分: 如果 \mathcal{C} 满足以下两个条件: $\bigcup_{i=1}^n A_i = A$ (覆盖性), 对任意 $i \neq j$, 有 $A_i \cap A_j = \emptyset$ (互不相交性), 则称 \mathcal{C} 是 A 的一个划分。此时 $\mathcal{C} = \{A_1, A_2, \dots, A_n\}$ 中的任意一个元素为 A 的一个类或划分的一个块。

设集合 $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$, 定义等价关系 R 为模三同余关系, 即对于任意 $a, b \in A$, $a R b$ 当且仅当 $a \equiv b \pmod{3}$ 。则 A 的等价类如下: 余数为 0 的等价类: $[3] = \{3, 6\}$, 余数为 1 的等价类: $[1] = \{1, 4, 7\}$, 余数为 2 的等价类: $[2] = \{2, 5, 8\}$ 。注意: 等价类的代表元选择不唯一, 例如 $[3] = [6]$, $[1] = [4] = [7]$, $[2] = [5] = [8]$ 。

商集为:

$$A/R = \{[1], [2], [3]\} = \{\{1, 4, 7\}, \{2, 5, 8\}, \{3, 6\}\}$$

商集 A/R 是 A 的一个划分, 第一点是因为覆盖性: $[1] \cup [2] \cup [3] = \{1, 4, 7\} \cup \{2, 5, 8\} \cup \{3, 6\} = A$; 第二点是因为互不相交性: $[1] \cap [2] = \emptyset$, $[1] \cap [3] = \emptyset$, $[2] \cap [3] = \emptyset$ 。

覆盖但不构成划分的例子: 考虑 $\mathcal{C} = \{\{1, 2, 3\}, \{3, 4, 5\}, \{5, 6, 7\}, \{7, 8, 1\}\}$

先看覆盖性: $\{1, 2, 3\} \cup \{3, 4, 5\} \cup \{5, 6, 7\} \cup \{7, 8, 1\} = A$, 是覆盖

但不构成划分, 因为 $\{1, 2, 3\} \cap \{3, 4, 5\} = \{3\} \neq \emptyset$

定理 3.6.1 等价类的性质

- (1) $\forall x \in A, [x]_R \neq \emptyset$, 且 $[x]_R \subseteq A$ 。
- (2) $\forall x, y \in A, (x, y) \in R \Rightarrow [x]_R = [y]_R$ 。
- (3) $\forall x, y \in A, (x, y) \notin R \Rightarrow [x]_R \cap [y]_R = \emptyset$ 。
- (4) $\bigcup_{x \in A} [x]_R = A$ 。

证明(1): 由于 R 是自反的, 对任意 $x \in A$, 有 $(x, x) \in R$, 所以 $x \in [x]_R$, 故 $[x]_R \neq \emptyset$ 。由等价类的定义 $[x]_R = \{y \in A \mid (x, y) \in R\}$, 显然 $[x]_R \subseteq A$ 。

证明(2): 设 $(x, y) \in R$ 。要证 $[x]_R = [y]_R$ 。

先证 $[x]_R \subseteq [y]_R$: 对任意 $z \in [x]_R$, 有 $(x, z) \in R$ 。由对称性, $(y, x) \in R$, 再由传递性, $(y, z) \in R$ 且 $(x, z) \in R$ 推出 $(y, z) \in R$, 所以 $z \in [y]_R$ 。

再证 $[y]_R \subseteq [x]_R$: 对任意 $z \in [y]_R$, 有 $(y, z) \in R$ 。由对称性, $(x, y) \in R$, 再由传递性, $(x, z) \in R$ 且 $(y, z) \in R$ 推出 $(x, z) \in R$, 所以 $z \in [x]_R$ 。因此 $[x]_R = [y]_R$ 。

证明(3): 用反证法。假设存在 $x, y \in A$ 满足 $(x, y) \notin R$, 但 $[x]_R \cap [y]_R \neq \emptyset$, 则存在 $z \in [x]_R \cap [y]_R$, 即 $(x, z) \in R$ 且 $(y, z) \in R$ 。由对称性, $(z, y) \in R$, 再由传递性, $(x, z) \in R$ 且 $(z, y) \in R$ 推出 $(x, y) \in R$, 与假设矛盾。故 $[x]_R \cap [y]_R = \emptyset$ 。

证明(4): 显然 $\bigcup_{x \in A} [x]_R \subseteq A$ 。另一方面, 对任意 $a \in A$, 有 $a \in [a]_R \subseteq \bigcup_{x \in A} [x]_R$, 所以 $A \subseteq \bigcup_{x \in A} [x]_R$ 。因此 $\bigcup_{x \in A} [x]_R = A$ 。

定理 3.6.2 划分是等价关系的另一种描述

假设 $\{A_1, A_2, \dots, A_n\}$ 是 A 的一个划分, 则 R 是 A 上的关系, $R = \{(x, y) \mid x, y \in A_i, i = 1, 2, \dots, n\}$, 则 R 是等价关系。

要证明 R 是等价关系, 需验证自反性、对称性和传递性。

1. 自反性: 对于任意 $x \in A$, 由于 $\{A_1, A_2, \dots, A_n\}$ 是 A 的划分, 存在 i 使得 $x \in A_i$ 。由 R 的定义, $(x, x) \in R$, 故 R 是自反的。

2. 对称性: 对于任意 $x, y \in A$, 若 $(x, y) \in R$, 则存在 i 使得 $x, y \in A_i$ 。因此 $y, x \in A_i$, 故 $(y, x) \in R$, R 是对称的。

3. 传递性: 对于任意 $x, y, z \in A$, 若 $(x, y) \in R$ 且 $(y, z) \in R$, 则存在 i, j 使得 $x, y \in A_i$ 且 $y, z \in A_j$ 。由于 $y \in A_i \cap A_j$, 且划分中的集合互不相交, 故 $A_i = A_j$ 。因此 $x, z \in A_i$, 从而 $(x, z) \in R$, R 是传递的。

综上, R 是等价关系。

定理 3.6.3 等价关系与划分的一一对应

设 A 是一个非空集合, $\{A_1, A_2, \dots, A_m\}$ 是 A 的一个划分。则:

划分的每一个划分块 A_i ($i = 1, 2, \dots, m$) 中的任意两个元素都有关系 R , 因此每一个划分块都是 R 的一个等价类。

由此可见, 集合 A 上的等价关系是对集合 A 中的元素做划分, 使得同一划分块中的元素之间有等价关系。

反之, 由一个划分可以确定唯一的一个等价关系, 这个等价关系的等价类就是划分的划分块。也就是说, 集合 A 上的等价关系与集合 A 的划分是一一对应的。

在非空集合 A 上给定一个划分, 可以找出由该划分所唯一确定的 A 上的等价关系, 方法如下: 把 A 的划分 $\{A_1, A_2, \dots, A_m\}$ 的每一个划分块 A_i , 求笛卡儿积 $A_i \times A_i$, 然后求这些笛卡儿积的并集:

$$R = (A_1 \times A_1) \cup (A_2 \times A_2) \cup \dots \cup (A_m \times A_m)$$

这个并集 R 即为所求的等价关系。

给定一个等价关系 R , 它的等价类构成 A 的一个划分, 给定 A 的一个划分, 通过上述方法构

造的关系 R 是一个等价关系, 这两种构造是互逆的, 建立了等价关系与划分之间的一一对应。

设集合 $A = \{1, 2, 3, 4, 5\}$, 考虑 A 的一个划分:

$$\mathcal{P} = \{\{1, 2, 3\}, \{4, 5\}\}$$

按照定理中的方法, 我们构造等价关系 R :

$$\begin{aligned} R &= (A_1 \times A_1) \cup (A_2 \times A_2) \\ &= (\{1, 2, 3\} \times \{1, 2, 3\}) \cup (\{4, 5\} \times \{4, 5\}) \\ &= \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\} \\ &\quad \cup \{(4, 4), (4, 5), (5, 4), (5, 5)\} \end{aligned}$$

如果从等价关系 R 出发, 可以得到划分 A/R , 这个划分恰好就是原来的划分 \mathcal{P} 。

例题 3.6.1 写出一个集合所有的等价关系

求集合 $A = \{1, 2, 3\}$ 的所有的等价关系及其对应的商集

集合 A 的等价关系与 A 的划分一一对应。 A 的划分共有 5 种, 如下所示:

1. 划分: $\{\{1, 2, 3\}\}$

等价关系: $R_1 = A \times A = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$

商集: $A/R_1 = \{\{1, 2, 3\}\}$

2. 划分: $\{\{1, 2\}, \{3\}\}$

等价关系: $R_2 = (\{1, 2\} \times \{1, 2\}) \cup (\{3\} \times \{3\}) = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$

商集: $A/R_2 = \{\{1, 2\}, \{3\}\}$

3. 划分: $\{\{1, 3\}, \{2\}\}$

等价关系: $R_3 = (\{1, 3\} \times \{1, 3\}) \cup (\{2\} \times \{2\}) = \{(1, 1), (1, 3), (3, 1), (3, 3), (2, 2)\}$

商集: $A/R_3 = \{\{1, 3\}, \{2\}\}$

4. 划分: $\{\{2, 3\}, \{1\}\}$

等价关系: $R_4 = (\{2, 3\} \times \{2, 3\}) \cup (\{1\} \times \{1\}) = \{(2, 2), (2, 3), (3, 2), (3, 3), (1, 1)\}$

商集: $A/R_4 = \{\{2, 3\}, \{1\}\}$

5. 划分: $\{\{1\}, \{2\}, \{3\}\}$

等价关系: $R_5 = (\{1\} \times \{1\}) \cup (\{2\} \times \{2\}) \cup (\{3\} \times \{3\}) = \{(1, 1), (2, 2), (3, 3)\}$

商集: $A/R_5 = \{\{1\}, \{2\}, \{3\}\}$

因此, 集合 A 共有 5 个不同的等价关系, 分别对应 5 种划分。

定理 3.6.4 等价关系之间的关系等价于划分之间的关系

设 R_1 和 R_2 是集合 A 上的两个等价关系, 则以下两个条件等价:

- (1) $R_1 \subseteq R_2$
- (2) R_1 的划分 C_1 的每一个等价类都是 R_2 的划分 C_2 的一个等价类

(1) \Rightarrow (2): 假设 $R_1 \subseteq R_2$ 。设 $[x]_{R_1}$ 是 R_1 的任意一个等价类。对任意 $y \in [x]_{R_1}$, 有 $(x, y) \in R_1$ 。由于 $R_1 \subseteq R_2$, 所以 $(x, y) \in R_2$, 即 $y \in [x]_{R_2}$ 。因此 $[x]_{R_1} \subseteq [x]_{R_2}$, 即 R_1 的每个等价类都包含在 R_2 的某个等价类中。

(2) \Rightarrow (1): 假设 R_1 的每个等价类都是 R_2 的某个等价类的子集。设 $(x, y) \in R_1$, 则 x 和 y 属于 R_1 的同一个等价类 $[x]_{R_1}$ 。由假设, 存在 R_2 的等价类 C 使得 $[x]_{R_1} \subseteq C$, 所以 $x, y \in C$, 即 $(x, y) \in R_2$ 。因此 $R_1 \subseteq R_2$ 。

综上, 两个条件等价。

3.7 偏序关系, 全序关系, 良序关系

定义 3.7.1 偏序关系, 可比, 覆盖, 全序关系

设 R 是集合 A 上的二元关系。

偏序关系: 如果 R 满足自反性, 反对称性, 传递性, 则称 R 为 A 上的偏序关系, 通常用符号“ \preceq ”表示偏序关系, 记作 (A, \preceq) 。若 $(x, y) \in R$, 记作 $x \preceq y$

可比: 设 (A, \preceq) 是偏序集, $x, y \in A$ 。如果 $x \preceq y$ 或 $y \preceq x$, 则称 x 和 y 是可比的; 否则称 x 和 y 是不可比的。

覆盖: 设 (A, \preceq) 是偏序集, $x, y \in A$ 且 $x \neq y$ 。如果 $x \preceq y$, $x \neq y$ (即 $x < y$) 且不存在 $z \in A$ 使得 $x < z < y$, 则称 y 覆盖 x (或称 x 是 y 的直接前驱, y 是 x 的直接后继)。

全序关系: 设 (A, \preceq) 是偏序集。如果对于任意 $x, y \in A$, x 和 y 都是可比的, 即 $\forall x, y \in A, x \preceq y$ 或 $y \preceq x$, 则称 \preceq 是 A 上的全序关系 (或称线序关系), 此时 (A, \preceq) 称为全序集。

考虑集合 $A = \{1, 2, 3, 4, 5, 6\}$, 定义整除关系 \preceq 为: $x \preceq y$ 当且仅当 $x | y$ (即 x 整除 y), 则 (A, \preceq) 构成一个偏序集, 因为整除关系满足:

自反性: $\forall x \in A, x | x$

反对称性: 若 $x | y$ 且 $y | x$, 则 $x = y$

传递性: 若 $x | y$ 且 $y | z$, 则 $x | z$

覆盖关系分析: 在偏序集中, y 覆盖 x 当且仅当 $x < y$, 且不存在 $z \in A$ ($z \neq x, z \neq y$) 使得 $x < z < y$, 考虑元素 1 和 4: $1 \preceq 4$ 成立, 因为 $1 | 4$, 但存在 $z = 2$, 使得 $1 \preceq 2 \preceq 4$ (即 $1 | 2$ 且 $2 | 4$), 因此, 4 不覆盖 1, 类似地, 4 覆盖 2, 因为 $2 | 4$ 且不存在 z 满足 $2 < z < 4$

在判断偏序关系时, 自反性是容易被忽视的, 比如小于和小于等于。

定义 3.7.2 哈斯图

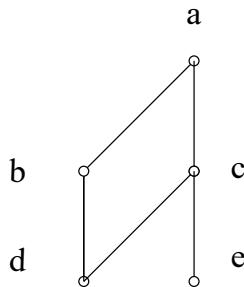
哈斯图 (Hasse diagram) 是有限偏序集的一种直观图示方法

顶点表示: 用平面上的点表示偏序集中的每个元素

位置安排: 如果 $x \preceq y$, 则将 x 放在 y 的下方 (保持偏序的方向性)

边的关系: 仅当 y 覆盖 x (即 y 是 x 的直接后继) 时, 才在 x 和 y 之间画一条线段

省略规则: 省略自反关系 (不画自环), 省略传递关系 (如果 $x \preceq y$ 且 $y \preceq z$, 但不画 x 到 z 的边), 尽量避免边的交叉, 保持图的清晰性

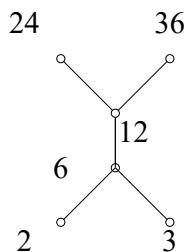


如上图, 集合 $A = \{1, 2, 3, 4, 5\}$, 集合 A 上的偏序关系

$$(A, \preceq) = \{(d, b), (d, c), (d, a), (e, c), (e, a), (b, a), (c, a), (a, a), (b, b), (c, c), (d, d), (e, e)\}$$

窍门是从下往上一个个地遍历所有结点, 这样能保证不重不漏。

以下给出 $\{2, 3, 6, 12, 24, 36\}$ 的整除关系的哈斯图:



$$R = \left\{ \begin{array}{l} (2, 2), (3, 3), (6, 6), (12, 12), (24, 24), (36, 36), \\ (2, 6), (2, 12), (2, 24), (2, 36), \\ (3, 6), (3, 12), (3, 24), (3, 36), \\ (6, 12), (6, 24), (6, 36), \\ (12, 24), (12, 36) \end{array} \right\}$$

定义 3.7.3 偏序集中的特殊元素

设 (S, \preceq) 是一个偏序集, $A \subseteq S$ 是一个非空子集。

最小元: 元素 $a_0 \in A$ 称为 A 的最小元, 如果对于所有 $a \in A$, 有 $a_0 \preceq a$ 。

最大元: 元素 $a_1 \in A$ 称为 A 的最大元, 如果对于所有 $a \in A$, 有 $a \preceq a_1$ 。

极小元: 元素 $a_m \in A$ 称为 A 的极小元, 如果不存在 $a \in A$ 使得 $a \prec a_m$ (即不存在 $a \in A$ 满足 $a \preceq a_m$ 且 $a \neq a_m$)。

极大元: 元素 $a_M \in A$ 称为 A 的极大元, 如果不存在 $a \in A$ 使得 $a_M \prec a$ (即不存在 $a \in A$ 满足 $a_M \preceq a$ 且 $a_M \neq a$)。

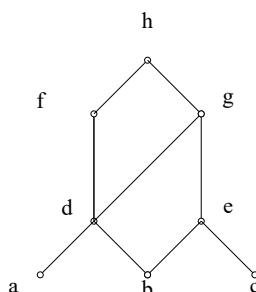
上界: 元素 $s \in S$ 称为 A 的上界, 如果对于所有 $a \in A$, 有 $a \preceq s$ 。

下界: 元素 $s \in S$ 称为 A 的下界, 如果对于所有 $a \in A$, 有 $s \preceq a$ 。

最小上界 (上确界): A 的最小上界是 A 的所有上界中的最小元, 记作 $\sup A$ 或 $\bigvee A$ 。

最大下界 (下确界): A 的最大下界是 A 的所有下界中的最大元, 记作 $\inf A$ 或 $\bigwedge A$ 。

最小元和最大元如果存在则唯一, 但极小元和极大元可以有多个, 上界和下界不一定属于 A , 它们可以是 S 中的任意元素, 最小上界和最大下界如果存在则唯一, 符号 \prec 表示严格偏序: $x \prec y \Leftrightarrow (x \preceq y \wedge x \neq y)$, 如下图是偏序关系 (A, R) 的哈斯图: 子集 $\{a, b, c\}$ 的上界是 g, h , 最小上界



是 g , 无下界和最大下界。子集 $\{f, g, h\}$ 的上界是 h , 最小上界是 h , 下界是 a, b, d , 最大下界是 d 。子集 $\{e, g\}$ 的上界是 g, h , 最小上界是 g , 下界是 b, c, e , 最大下界是 e 。偏序集

$$\begin{aligned}
 R = & (a, a), (b, b), (c, c), (d, d), (e, e), (f, f), (g, g), (h, h), \\
 & (a, d), (a, f), (a, g), (a, h), \\
 & (b, d), (b, e), (b, f), (b, g), (b, h), \\
 & (c, e), (c, g), (c, h), \\
 & (d, f), (d, g), (d, h), \\
 & (e, g), (e, h), \\
 & (f, h), \\
 & (g, h)
 \end{aligned}$$

定义 3.7.4 良序集

设 (S, \preccurlyeq) 是一个全序集 (即 \preccurlyeq 是 S 上的全序关系)。如果 S 的每个非空子集都有最小元, 则称 (S, \preccurlyeq) 为良序集, \preccurlyeq 称为 S 上的良序关系。

(S, \preccurlyeq) 是良序集当且仅当: \preccurlyeq 是 S 上的全序关系; 对 S 的任意非空子集 $A \subseteq S$, 存在 $a_0 \in A$ 使得对所有的 $a \in A$, 有 $a_0 \preccurlyeq a$ 。

良序集一定是全序集, 但全序集不一定是良序集, **有限全序集一定是良序集**, 自然数集 (\mathbb{N}, \leq) 是良序集 (良序原理), 整数集 (\mathbb{Z}, \leq) 是全序集但不是良序集 (因为负整数子集没有最小元), 实数上的小于等于关系 (\mathbb{R}, \leq) 是全序集但不是良序集 (因为开区间 $(0, 1)$ 没有最小元)。

定义 3.7.5 严格偏序关系

反自反, 反对称和传递关系, 称作严格偏序关系。严格偏序关系和偏序关系有密切联系, 区别仅在于 (x, x) 是否属于这个关系。

比如实数集上的小于关系不是偏序关系, 因为其不满足自反性, 但是却是严格偏序关系。

第四章 函数

4.1 函数（映射）的定义与表示

定义 4.1.1 函数，定义域，值域，陪域，像，原像

函数：设 A 和 B 是两个集合。一个从 A 到 B 的函数 f 是一个特殊的二元关系，它对 A 中的每个元素 x 指定 B 中唯一的一个元素，记为 $f(x)$ 。记作 $f : A \rightarrow B$ 。

定义域：函数 $f : A \rightarrow B$ 的定义域是集合 A ，即函数输入的全体。

陪域：函数 $f : A \rightarrow B$ 的陪域是集合 B ，即函数输出的可能取值范围。

值域：函数 $f : A \rightarrow B$ 的值域是 f 在 A 上所有取值的集合，即 $\{f(x) | x \in A\}$ ，陪域的子集。

像：对于子集 $S \subseteq A$ ， S 在 f 下的像是集合 $f(S) = \{f(x) | x \in S\}$ 。

原像：对于子集 $T \subseteq B$ ， T 在 f 下的原像是集合 $f^{-1}(T) = \{x \in A | f(x) \in T\}$ 。

注：函数也称为映射。函数必须满足单值性：对每个 $x \in A$ ，有且仅有一个 $f(x) \in B$ 与之对应。而且定义域中的每个元素都必须有对应的值。做题时关注定义域，如果有些定义域的元素没有对应的值，则该关系不是函数。

如： $\{(x_1, x_2) | x_1, x_2 \in \mathbb{N}, x_1 + x_2 = 10\}$ 就不是函数

定义 4.1.2 计算机科学中的特殊函数类型

设 A 和 B 是集合，定义以下特殊函数类型：

常函数：函数 $f : A \rightarrow B$ 称为常函数，如果存在 $b \in B$ 使得对所有 $a \in A$ ，有 $f(a) = b$ 。即函数值不随自变量变化。

恒等函数：函数 $f_A : A \rightarrow A$ ，如果对于所有 $x \in A$ 都有 $f(x) = x$ ，则称为恒等函数。

特征函数：设 $S \subseteq A$ ， S 的特征函数 $f_S : A \rightarrow \{0, 1\}$ 定义为：

$$f_S(a) = \begin{cases} 1 & \text{如果 } a \in S \\ 0 & \text{如果 } a \notin S \end{cases}$$

自然映射：设 \sim 是 A 上的等价关系， A/\sim 是商集。自然映射 $\pi : A \rightarrow A/\sim$ 定义为 $\pi(a) = [a]$ ，其中 $[a]$ 是 a 的等价类。

上取整函数：函数 $\lceil \cdot \rceil : \mathbb{R} \rightarrow \mathbb{Z}$ 定义为 $\lceil x \rceil = \min\{n \in \mathbb{Z} | n \geq x\}$ ，即不小于 x 的最小整数。

下取整函数：函数 $\lfloor \cdot \rfloor : \mathbb{R} \rightarrow \mathbb{Z}$ 定义为 $\lfloor x \rfloor = \max\{n \in \mathbb{Z} | n \leq x\}$ ，即不大于 x 的最大整数。

定理 4.1.1 函数经过集合运算后的函数性

设 $f, g : A \rightarrow B$ 是两个函数。将 f 和 g 视为 $A \times B$ 的子集(即它们的图像)。那么:

$f \cap g$ 是从 A 到 B 的函数当且仅当 $f = g$ 。

$f \cup g$ 是从 A 到 B 的函数当且仅当 $f = g$ 。

$\sim f = A \times B - f$ 不是从 A 到 B 的函数,除非 $A = \emptyset$ 。

$f - g$ 是从 A 到 B 的函数当且仅当对于所有 $a \in A$, 有 $f(a) \neq g(a)$ 。

$f \oplus g$ 是从 A 到 B 的函数当且仅当 $A = \emptyset$ 。

对于 $f \cap g$: 如果 $f = g$, 则 $f \cap g = f$, 是从 A 到 B 的函数。反之, 如果 $f \cap g$ 是从 A 到 B 的函数, 则对任意 $a \in A$, 存在唯一的 $b \in B$ 使得 $(a, b) \in f \cap g$, 故 $(a, b) \in f$ 且 $(a, b) \in g$, 即 $f(a) = b$ 且 $g(a) = b$, 所以 $f(a) = g(a)$ 对所有 $a \in A$ 成立, 即 $f = g$ 。

对于 $f \cup g$: 如果 $f = g$, 则 $f \cup g = f$, 是从 A 到 B 的函数。反之, 如果 $f \cup g$ 是从 A 到 B 的函数, 则对任意 $a \in A$, 存在唯一的 $b \in B$ 使得 $(a, b) \in f \cup g$ 。如果存在 $a \in A$ 使得 $f(a) \neq g(a)$, 则 $(a, f(a)) \in f$ 和 $(a, g(a)) \in g$ 都在 $f \cup g$ 中, 但 $f(a) \neq g(a)$, 违反函数的单值性, 矛盾。故对所有 $a \in A$, 有 $f(a) = g(a)$, 即 $f = g$ 。

对于 $\sim f$: 如果 $A \neq \emptyset$, 取 $a \in A$, 则存在 $b = f(a)$ 使得 $(a, b) \in f$, 故 $(a, b) \notin \sim f$ 。但对 $b' \neq b$, 有 $(a, b') \in \sim f$, 且 b' 有多个选择(因为 B 至少有两个元素, 或如果 $|B| = 1$ 则 b' 唯一, 但通常 B 非空), 但 $\sim f$ 中包含所有 (a, b') 对于 $b' \neq b$, 所以对同一个 a , 有多个 b' 对应, 违反单值性。如果 $A = \emptyset$, 则 f 是空函数, $\sim f = \emptyset$, 也是空函数(从空集到 B 的函数)。

对于 $f - g$: 如果对于所有 $a \in A$, 有 $f(a) \neq g(a)$, 则对每个 $a \in A$, 有 $(a, f(a)) \in f$ 但 $(a, f(a)) \notin g$, 故 $(a, f(a)) \in f - g$, 且唯一, 所以 $f - g = f$, 是从 A 到 B 的函数。反之, 如果 $f - g$ 是从 A 到 B 的函数, 则对每个 $a \in A$, 存在唯一的 $b \in B$ 使得 $(a, b) \in f - g$, 故 $(a, b) \in f$ 且 $(a, b) \notin g$, 所以 $b = f(a)$ 且 $b \neq g(a)$, 即 $f(a) \neq g(a)$ 。

对于 $f \oplus g$: 如果 $A = \emptyset$, 则 f 和 g 都是空函数, $f \oplus g = \emptyset$, 是从空集到 B 的函数。如果 $A \neq \emptyset$, 假设 $f \oplus g$ 是从 A 到 B 的函数。则对任意 $a \in A$, 存在唯一的 $b \in B$ 使得 $(a, b) \in f \oplus g$ 。但由对称差定义, $(a, b) \in f \oplus g$ 当且仅当 (a, b) 在 f 或 g 中但不同时在两者中。如果 $f(a) = g(a)$, 则 $(a, f(a))$ 不在 $f \oplus g$ 中, 矛盾于存在性。如果 $f(a) \neq g(a)$, 则 $(a, f(a))$ 和 $(a, g(a))$ 都在 $f \oplus g$ 中, 违反唯一性。故当 $A \neq \emptyset$ 时, $f \oplus g$ 不是函数。

定理 4.1.2 函数关系的性质

设 A 和 B 是两个集合。所有从 A 到 B 的函数的集合记为 B^A , 即:

$$B^A = \{f \mid f : A \rightarrow B\}$$

如果 A 和 B 都是有限集, 且 $|A| = m$, $|B| = n$, 则 $|B^A| = n^m$ 。

如果 $A = \emptyset$, 则 $B^A = \{\emptyset\}$ (空函数)。如果 $B = \emptyset$ 且 $A \neq \emptyset$, 则 $B^A = \emptyset$ 。

特别地, 2^A 表示 A 的幂集 $\mathcal{P}(A)$, 因为 2^A 与 A 的特征函数集合 $\{f : A \rightarrow \{0, 1\}\}$ 一一对应。

定理 4.1.3 函数定义域的性质

设 $f : A \rightarrow B$ 是一个函数, $S, T \subseteq A$, 则:

$$(1) \text{ 若 } S \subseteq T, \text{ 则 } f(S) \subseteq f(T) \quad (2) f(S \cap T) \subseteq f(S) \cap f(T)$$

$$(3) f(S) - f(T) \subseteq f(S - T) \quad (4) f(S) \oplus f(T) \subseteq f(S \oplus T)$$

(1) 设 $y \in f(S)$, 即存在 $x \in S$ 使得 $f(x) = y$ 。那么由于 $S \subseteq T$, 所以 $x \in T$, 因此 $y = f(x) \in f(T)$ 。故 $f(S) \subseteq f(T)$ 。

(2) 设 $y \in f(S \cap T)$, 则存在 $x \in S \cap T$ 使得 $f(x) = y$ 。由于 $x \in S$ 且 $x \in T$, 所以 $y \in f(S)$ 且 $y \in f(T)$, 即 $y \in f(S) \cap f(T)$ 。故 $f(S \cap T) \subseteq f(S) \cap f(T)$ 。

(3) 设 $y \in f(S) - f(T)$, 则 $y \in f(S)$ 且 $y \notin f(T)$ 。由 $y \in f(S)$, 存在 $x \in S$ 使得 $f(x) = y$ 。假设 $x \in T$, 则 $y = f(x) \in f(T)$, 矛盾。故 $x \notin T$, 即 $x \in S - T$, 所以 $y \in f(S - T)$ 。

(4) 由对称差的定义和(3)的结果:

$$f(S) \oplus f(T) = (f(S) - f(T)) \cup (f(T) - f(S)) \subseteq f(S - T) \cup f(T - S)$$

由于 $f(S - T) \cup f(T - S) = f((S - T) \cup (T - S)) = f(S \oplus T)$, 所以 $f(S) \oplus f(T) \subseteq f(S \oplus T)$ 。

定理 4.1.4 等号成立的条件

设 $f : A \rightarrow B$ 是一个函数, $S, T \subseteq A$, 则:

(1) $f(S \cap T) = f(S) \cap f(T)$ 当且仅当对于任意 $s \in S$ 和 $t \in T$, 如果 $f(s) = f(t)$, 则存在 $x \in S \cap T$ 使得 $f(x) = f(s)$ (等于没说)。特别的, 如果 f 是单射, 就满足此条件。

(2) $f(S) - f(T) = f(S - T)$ 当且仅当 f 是单射。

(3) $f(S) \oplus f(T) = f(S \oplus T)$ 当且仅当 f 是单射。

(1) 我们已经知道 $f(S \cap T) \subseteq f(S) \cap f(T)$ 总是成立。要证明反向包含, 设 $y \in f(S) \cap f(T)$, 则存在 $s \in S$ 和 $t \in T$ 使得 $f(s) = y$ 且 $f(t) = y$ 。如果 f 是单射, 则 $s = t \in S \cap T$, 所以 $y \in f(S \cap T)$ 。更一般地, 如果存在 $x \in S \cap T$ 使得 $f(x) = f(s) = y$, 则 $y \in f(S \cap T)$ 。

(2) 我们已经知道 $f(S) - f(T) \subseteq f(S - T)$ 总是成立。要证明反向包含, 设 $y \in f(S - T)$, 则存在 $x \in S - T$ 使得 $f(x) = y$ 。由于 $x \in S$, 所以 $y \in f(S)$ 。如果 f 是单射, 则 $y \notin f(T)$ (否则存在 $z \in T$ 使得 $f(z) = y$, 由单射性 $x = z \in T$, 矛盾), 所以 $y \in f(S) - f(T)$ 。

(3) 由对称差的定义和(1)(2)的结果, 当 f 是单射时, 有:

$f(S) \oplus f(T) = (f(S) - f(T)) \cup (f(T) - f(S)) = f(S - T) \cup f(T - S) = f((S - T) \cup (T - S)) = f(S \oplus T)$
反之, 如果 f 不是单射, 等号可能不成立。

注 4.1.1. 当 f 不是单射时, 等号可能不成立。例如, 考虑函数 $f : \{1, 2\} \rightarrow \{1\}$, $f(1) = f(2) = 1$, 取 $S = \{1\}$, $T = \{2\}$:

$$f(S \cap T) = f(\emptyset) = \emptyset, \text{ 但 } f(S) \cap f(T) = \{1\} \cap \{1\} = \{1\}$$

$$f(S) - f(T) = \{1\} - \{1\} = \emptyset, \text{ 但 } f(S - T) = f(\{1\}) = \{1\}$$

$$f(S) \oplus f(T) = \{1\} \oplus \{1\} = \emptyset, \text{ 但 } f(S \oplus T) = f(\{1, 2\}) = \{1\}$$

4.2 单/满/双射, 反函数, 复合

定义 4.2.1 单射、满射、双射

设 $f : A \rightarrow B$ 是一个函数。

单射 (injection): f 是单射当且仅当对于任意 $x_1, x_2 \in A$, 如果 $f(x_1) = f(x_2)$, 则 $x_1 = x_2$ 。即不同的输入对应不同的输出。

满射 (surjection): f 是满射当且仅当对于任意 $b \in B$, 存在 $a \in A$ 使得 $f(a) = b$ 。即函数的值域等于陪域 B 。

双射 (bijection): f 是双射当且仅当它既是单射又是满射。即存在一一对应关系。

等价定义:

f 是单射 $\Leftrightarrow f$ 有左逆 (存在 $g : B \rightarrow A$ 使得 $g \circ f = \text{id}_A$)

f 是满射 $\Leftrightarrow f$ 有右逆 (存在 $h : B \rightarrow A$ 使得 $f \circ h = \text{id}_B$)

f 是双射 $\Leftrightarrow f$ 有逆函数 (存在 $f^{-1} : B \rightarrow A$ 使得 $f^{-1} \circ f = \text{id}_A$ 且 $f \circ f^{-1} = \text{id}_B$)

定义 4.2.2 反函数

设函数 $f : A \rightarrow B$ 是一个从定义域 A 到值域 B 的双射函数。 f 的反函数, 记作 $f^{-1} : B \rightarrow A$, 定义为满足以下条件的函数:

$$f^{-1}(b) = a \quad \text{当且仅当} \quad f(a) = b$$

其中 $b \in B$, $a \in A$ 。

定义 4.2.3 函数的复合

设 $f : A \rightarrow B$ 和 $g : B \rightarrow C$ 是两个函数。函数 f 和 g 的复合函数 $g \circ f : A \rightarrow C$ 定义为

$$(g \circ f)(x) = \{(x, z) | x \in A \wedge z \in C \wedge \exists y(y \in B \wedge (x, y) \in f \wedge (y, z) \in g)\}$$

注意如果 f 的值域不是 g 的定义域的子集, 则复合函数 $g \circ f$ 无法定义。下面证明: 若 $f : A \rightarrow B$ 和 $g : B \rightarrow C$ 是两个函数, 则 $g \circ f$ 是 $A \rightarrow C$ 的函数

1. 存在性: 对于任意 $x \in A$, 存在 $z \in C$ 使得 $(x, z) \in g \circ f$ 。

由于 $f : A \rightarrow B$ 是函数, 对于任意 $x \in A$, 存在唯一的 $y \in B$ 使得 $(x, y) \in f$ 。由于 $g : B \rightarrow C$ 是函数, 对于这个 $y \in B$, 存在唯一的 $z \in C$ 使得 $(y, z) \in g$ 。因此, 存在 $z \in C$ 使得 $\exists y(y \in B \wedge (x, y) \in f \wedge (y, z) \in g)$, 即 $(x, z) \in g \circ f$ 。

2. 唯一性: 对于任意 $x \in A$, 如果 $(x, z_1) \in g \circ f$ 且 $(x, z_2) \in g \circ f$, 则 $z_1 = z_2$ 。

假设 $(x, z_1) \in g \circ f$ 且 $(x, z_2) \in g \circ f$ 。

则存在 $y_1, y_2 \in B$ 使得: $(x, y_1) \in f$ 且 $(y_1, z_1) \in g$, $(x, y_2) \in f$ 且 $(y_2, z_2) \in g$ 。

由于 f 是函数, 对于给定的 x , 有唯一的 y 使得 $(x, y) \in f$, 所以 $y_1 = y_2$ 。

令 $y = y_1 = y_2$ 。由于 g 是函数, 对于给定的 y , 有唯一的 z 使得 $(y, z) \in g$, 所以 $z_1 = z_2$ 。

综上, $g \circ f$ 满足函数的定义, 因此是 $A \rightarrow C$ 的函数。

定理 4.2.1 函数复合的性质

设 $f : A \rightarrow B$, $g : B \rightarrow C$ 和 $h : C \rightarrow D$ 是函数。

(1) 结合律: $(h \circ g) \circ f = h \circ (g \circ f)$

(2) 单射、满射、双射的传递性:

如果 f 和 g 都是单/满/双射, 则 $g \circ f$ 是单/满/双射。

(3) 通过复合函数确定原函数的性质:

如果 $g \circ f$ 是单射, 则 f 是单射。如果 $g \circ f$ 是满射, 则 g 是满射。

如果 $g \circ f$ 是双射, 则 f 是单射且 g 是满射。

(4) 衍生结论:

如果 $g \circ f$ 是满射, 且 g 是单射, 则 f 是满射。

如果 $g \circ f$ 是单射, 且 f 是满射, 则 g 是单射。

(1) 对任意 $x \in A$, 有:

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

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

所以 $(h \circ g) \circ f = h \circ (g \circ f)$ 。

(2) 首先证明单射的传递性: 设 $x_1, x_2 \in A$, 若 $(g \circ f)(x_1) = (g \circ f)(x_2)$, 即 $g(f(x_1)) = g(f(x_2))$ 。由于 g 是单射, 有 $f(x_1) = f(x_2)$, 又因 f 是单射, 有 $x_1 = x_2$ 。故 $g \circ f$ 是单射。

其次证明满射的传递性: 对任意 $c \in C$, 由于 g 是满射, 存在 $b \in B$ 使得 $g(b) = c$ 。又因 f 是满射, 存在 $a \in A$ 使得 $f(a) = b$ 。于是 $(g \circ f)(a) = g(f(a)) = g(b) = c$ 。故 $g \circ f$ 是满射。

双射的传递性由前两个结果直接可得。

(3) 首先证明: 如果 $g \circ f$ 是单射, 则 f 是单射。设 $x_1, x_2 \in A$, 若 $f(x_1) = f(x_2)$, 则 $g(f(x_1)) = g(f(x_2))$, 即 $(g \circ f)(x_1) = (g \circ f)(x_2)$ 。由于 $g \circ f$ 是单射, 有 $x_1 = x_2$ 。故 f 是单射。

其次证明: 如果 $g \circ f$ 是满射, 则 g 是满射。对任意 $c \in C$, 由于 $g \circ f$ 是满射, 存在 $a \in A$ 使得 $(g \circ f)(a) = c$, 即 $g(f(a)) = c$ 。令 $b = f(a) \in B$, 则 $g(b) = c$ 。故 g 是满射。

最后, 如果 $g \circ f$ 是双射, 则它既是单射又是满射, 由前两个结果可知 f 是单射且 g 是满射。

(4)(1) 假设 $g \circ f$ 是满射, 且 g 是单射。要证明 f 是满射, 即对任意 $b \in B$, 存在 $a \in A$ 使得 $f(a) = b$ 。由于 $g \circ f$ 是满射, 对于任意 $b \in B$, 令 $c = g(b)$, 则存在 $a \in A$ 使得 $(g \circ f)(a) = g(f(a)) = c = g(b)$ 。由于 g 是单射, 由 $g(f(a)) = g(b)$ 可得 $f(a) = b$ 。因此对任意 $b \in B$, 存在 $a \in A$ 使得 $f(a) = b$, 即 f 是满射。

(4)(2) 假设 $g \circ f$ 是单射, 且 f 是满射。要证明 g 是单射, 即对任意 $b_1, b_2 \in B$, 如果 $g(b_1) = g(b_2)$, 则 $b_1 = b_2$ 。由于 f 是满射, 存在 $a_1, a_2 \in A$ 使得 $f(a_1) = b_1$ 和 $f(a_2) = b_2$ 。由 $g(b_1) = g(b_2)$ 得 $g(f(a_1)) = g(f(a_2))$, 即 $(g \circ f)(a_1) = (g \circ f)(a_2)$ 。由于 $g \circ f$ 是单射, 有 $a_1 = a_2$, 从而 $b_1 = f(a_1) = f(a_2) = b_2$ 。因此 g 是单射。

考虑一个快递运输的比喻来解释函数复合的性质:

设 $A = \text{寄件人集合}$, $B = \text{中转站集合}$, $C = \text{收件人集合}$ 。

函数 $f : A \rightarrow B$ 表示从寄件人到中转站的运输过程。函数 $g : B \rightarrow C$ 表示从中转站到收件人的运输过程。复合函数 $g \circ f : A \rightarrow C$ 表示从寄件人到收件人的完整运输过程。

结合律: 如果还有第四个地点 D (例如国际转运中心) 和函数 $h : C \rightarrow D$, 那么无论是先组合 g 和 h 再与 f 组合, 还是先组合 f 和 g 再与 h 组合, 最终结果都是将快递从 A 经 B 和 C 运送到 D 。运输路径是确定的, 与组合方式无关。

单射、满射、双射的传递性: 如果从寄件人到中转站 (f) 和中转站到收件人 (g) 都是“一对一”运输 (单射), 那么整个运输过程 ($g \circ f$) 也是“一对一”的。每个寄件人的快递最终会送到不同的收件人手中。如果两个阶段都能覆盖所有可能的地址 (满射), 那么整个运输过程也能覆盖所有收件人。如果两个阶段都是完美的“一对且全覆盖” (双射), 那么整个运输过程也是完美的。

通过复合函数确定原函数的性质: 如果整个运输过程 ($g \circ f$) 是“一对一”的 (单射), 那么第一阶段 (f) 必须是“一对一”的。因为如果两个寄件人的快递在中转站就混在一起了, 那么最终不可能送到不同的收件人手中。如果整个运输过程能覆盖所有收件人 (满射), 那么第二阶段 (g) 必须能覆盖所有收件人。因为如果中转站有些地址无法送达最终收件人, 那么这些收件人就收不到快递。如果整个运输过程完美无缺 (双射), 那么第一阶段必须保证不混件 (单射), 第二阶段必须保证全覆盖 (满射)。

定理 4.2.2 复合函数的反函数

设 $f : B \rightarrow C$ 和 $g : A \rightarrow B$ 都是双射函数, 则复合函数 $f \circ g : A \rightarrow C$ 也是双射函数

$$(f \circ g)^{-1} = g^{-1} \circ f^{-1}$$

要证明 $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$, 需要验证两个条件 $f \circ f^{-1} = f^{-1} \circ f$ 均为恒等函数; 设定义在集合 A 上的恒等函数为 id_A :

1. 左复合等于恒等映射:

$$(f \circ g) \circ (g^{-1} \circ f^{-1}) = f \circ (g \circ g^{-1}) \circ f^{-1} = f \circ \text{id}_B \circ f^{-1} = f \circ f^{-1} = \text{id}_C$$

2. 右复合等于恒等映射:

$$(g^{-1} \circ f^{-1}) \circ (f \circ g) = g^{-1} \circ (f^{-1} \circ f) \circ g = g^{-1} \circ \text{id}_B \circ g = g^{-1} \circ g = \text{id}_A$$

因此, $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$ 。

例题 4.2.1

设 $f : A \rightarrow B$ 和 $g : B \rightarrow P(A)$, 其中 $P(A)$ 表示 A 的幂集, 且对于任意 $b \in B$ 有 $g(b) = \{x | (x \in A) \wedge (f(x) = b)\}$ 。证明: 若 f 是满射, 则 g 是单射

要证明 g 是单射, 即对于任意 $b_1, b_2 \in B$, 如果 $g(b_1) = g(b_2)$, 则 $b_1 = b_2$ 。由于 f 是满射, 对于任意 $b \in B$, 存在至少一个 $x \in A$ 使得 $f(x) = b$, 现在假设 $g(b_1) = g(b_2)$ 。由于 $g(b_1)$ 非空, 存在 $x \in g(b_1)$ 。因为 $g(b_1) = g(b_2)$, 所以 $x \in g(b_2)$ 。

根据 g 的定义: $x \in g(b_1)$ 意味着 $f(x) = b_1$, $x \in g(b_2)$ 意味着 $f(x) = b_2$, 因此, $b_1 = f(x) = b_2$, 即 $b_1 = b_2$ 。故 g 是单射。

4.3 自然数

定义 4.3.1 后继集与自然数集的定义

后继集: 设 A 是一个集合, A 的后继集定义为 $A^+ = A \cup \{A\}$ 。

自然数集的递归定义 (冯·诺依曼定义):

1. **基础:** $0 = \emptyset$

2. **递归步骤:** $n + 1 = n^+ = n \cup \{n\}$

3. **极限情况:** 自然数集 \mathbb{N} 是包含 0 且在后继运算下封闭的最小集合

按照这个定义, 自然数可以具体构造为:

$$0 = \emptyset$$

$$1 = 0^+ = \emptyset \cup \{\emptyset\} = \{\emptyset\}$$

$$2 = 1^+ = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}$$

$$3 = 2^+ = \{\emptyset, \{\emptyset\}\} \cup \{\{\emptyset, \{\emptyset\}\}\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$$

⋮

性质: 每个自然数都是它前面所有自然数的集合; $n = \{0, 1, 2, \dots, n - 1\}$; 这种定义方式使得 $m < n$ 当且仅当 $m \in n$; 自然数集 \mathbb{N} 是一个归纳集

定义 4.3.2 第一数学归纳法

设 $P(n)$ 是一个与自然数 n 相关的命题。如果满足:

基础步骤: $P(0)$ 成立 (即 $P(\emptyset)$ 成立)

归纳步骤: 对于任意自然数 n , 如果 $P(n)$ 成立, 则 $P(n^+)$ 也成立

其中 $n^+ = n \cup \{n\}$ 是 n 的后继集, 那么, 对于所有自然数 n , $P(n)$ 都成立。即

$$P(0) \wedge \forall n \in \mathbb{N}(P(n) \rightarrow P(n^+)) \rightarrow \forall n \in \mathbb{N}, P(n)$$

原理的集合论基础: 数学归纳法原理等价于自然数集的良序原理

证明: 任何自然数都不是自己的元素。

使用数学归纳法证明。**基础步骤:** 考虑 $n = 0$ 。根据定义, $0 = \emptyset$, 即空集。空集不包含任何元素, 因此显然 $0 \notin 0$ 。**归纳步骤:** 假设对于某个自然数 n , 有 $n \notin n$ (归纳假设)。我们需要证明 $n + 1 \notin n + 1$ 。根据自然数的定义, $n + 1 = n \cup \{n\}$, 因此 $n + 1$ 的元素是 n 的所有元素以及 n 本身。

反设 $n + 1 \in n + 1$ 。那么由于 $n + 1 = n \cup \{n\}$, 我们有两种可能: $n + 1 \in n$, 或者 $n + 1 = n$ 。考虑第一种情况: 如果 $n + 1 \in n$, 那么根据引理 1 (自然数的传递性), 由于 n 是自然数, 它是传递的, 所以 $n + 1 \subset n$ 。但 $n \in n + 1$ (由定义), 因此 $n \in n$, 这与归纳假设 $n \notin n$ 矛盾。考虑第二

种情况：如果 $n + 1 = n$ ，那么这意味着 $n \cup \{n\} = n$ ，从而 $\{n\} \subseteq n$ ，即 $n \in n$ 。但这与归纳假设 $n \notin n$ 矛盾。

两种情况均导致矛盾。因此，原假设 $n + 1 \in n + 1$ 不成立，故 $n + 1 \notin n + 1$ 。

定义 4.3.3 集合的特征函数

设 A 是全集 E 的子集， A 的特征函数 f_A 定义为：

$$f_A : E \rightarrow \{0, 1\}, f_A(x) = \begin{cases} 1 & \text{如果 } x \in A \\ 0 & \text{如果 } x \notin A \end{cases}$$

特征函数完全确定了集合 A ，因为 $A = \{x \mid f_A(x) = 1\}$ 。

定理 4.3.1 特征函数与集合运算

设 A 和 B 是集合，它们的特征函数分别为 f_A 和 f_B ，则有以下关系：

$$\begin{aligned} f_{A \cup B}(x) &= \max(f_A(x), f_B(x)) = f_A(x) + f_B(x) - f_A(x)f_B(x) \\ f_{A \cap B}(x) &= \min(f_A(x), f_B(x)) = f_A(x)f_B(x) \\ f_{A^c}(x) &= 1 - f_A(x) \\ f_{A-B}(x) &= f_A(x)(1 - f_B(x)) \\ f_{A \oplus B}(x) &= |f_A(x) - f_B(x)| = f_A(x) + f_B(x) - 2f_A(x)f_B(x) \end{aligned}$$

4.4 集合的基数，等势

定义 4.4.1 基数，比较两个集合的基数，等势

集合 A 的基数（或称势）是衡量集合大小的概念，记为 $|A|$ 。对于有限集，基数就是集合中元素的个数。无限集的基数概念更为复杂，需要用到选择公理等相关理论。

A 和 B 称为等势（记作 $|A| = |B|, A \sim B$ ），即存在一个从 A 到 B 的双射（一一对应）。

$|A| \leq |B|$ 表示存在从 A 到 B 的单射

$|A| < |B|$ 表示 $|A| \leq |B|$ 但 $|A| \neq |B|$

$|A| \geq |B|$ 表示存在从 A 到 B 的满射

定理 4.4.1 基数的性质

设 M 是一个集合， $P(M)$ 是其幂集， $P(M)$ 的基数记为 $|P(M)|$ 。则： $|P(M)| > |M|$

假设存在双射 $f : M \rightarrow P(M)$ 。这个双射将集合 M 中的每个元素和 M 的每一个子集建立了一一对应关系，再定义集合 $A = \{x \in M \mid x \notin f(x)\}$ ，意思是找出来所有这样的元素，满足它们分别所对应的那一个子集中不含有它自身。由于 $A \subseteq M$ ，有 $A \in P(M)$ ，即它是幂集中的一个元素，

所以根据假设， A 理应和 M 中的某一个元素对应，设这个元素为 a ，即 $f(a) = A$ 。如果 $a \in A$ ，那么根据 A 的定义， $a \notin f(a)$ ，而 $f(a) = A$ ，所以 $a \notin A$ ，矛盾。如果 $a \notin A$ ，即 $a \notin f(a)$ ，那么根据 A 的定义， a 满足 A 的条件，所以 $a \in A$ ，矛盾。

这个构造的核心思想是自指悖论，类似于“理发师悖论”：理发师宣称：我给所有不给自己理发的人理发。那么理发师给自己理发吗？在我们的证明中：集合 A 被定义为“所有不包含在自己的像中的元素”所形成的集合，那么它是否包含在它自己的像中？

定义 4.4.2 有限集与无限集

有限集：一个集合 A 称为有限集，如果存在某个自然数 n 和双射 $f : A \rightarrow \{0, 1, 2, \dots, n-1\}$ ，即 A 与某个自然数等势。此时 $|A| = n$ 。

无限集：不是有限集的一个集合 A 称为无限集。即不存在任何自然数 n 使得 A 与某自然数等势。

可数无限集：与自然数集 \mathbb{N} 等势的集合，即存在从 \mathbb{N} 到 A 的双射。例如 \mathbb{Z}, \mathbb{Q} 。

不可数无限集：无限但不可数的集合，即其基数严格大于可数无限集的基数。例如：实数集 \mathbb{R} 、复数集 \mathbb{C} 。

注：可数无限集的基数记为 \aleph_0 （阿列夫零），实数集的基数记为 \aleph （连续统基数）。

定理 4.4.2 有限集和无限集的基数

有限集不和其任何一个子集等势

一个集合是无限集当且仅当它与它自己的某一个真子集等势

设 S 是一个有限集，假设存在 S 的一个真子集 $T \subset S$ 使得 $|T| = |S|$ 。但由于 T 是 S 的真子集， $|T| < |S|$ ，矛盾。因此有限集不能与它的任何真子集等势。

设 S 是无限集。我们可以构造一个单射但不是满射的函数 $f : S \rightarrow S$ ，例如通过选择可数无限子集并建立双射。这样 $f(S)$ 就是 S 的一个真子集，且与 S 等势。反过来，如果 S 与它的某个真子集等势，假设 S 是有限集，则与第一部分矛盾。因此 S 必须是无限集。

定理 4.4.3 无限集必然含有可数的子集

任意一个无限集必然含有可数的子集。

这个证明使用了选择公理（通过递归选择元素）：

设 X 是一个无限集。我们需要证明 X 包含一个可数无限子集。由于 X 是无限的，它非空，因此我们可以选择一个元素 $a_1 \in X$ 。考虑集合 $X - \{a_1\}$ ，由于 X 是无限的， $X - \{a_1\}$ 仍是非空的（否则 X 将是有限的），所以我们可以选择一个元素 $a_2 \in X - \{a_1\}$ 。类似地，假设我们已经选择了互不相同的元素 $a_1, a_2, \dots, a_n \in X$ ，由于 X 是无限的， $X - \{a_1, a_2, \dots, a_n\}$ 非空，因此我们可以选择 $a_{n+1} \in X - \{a_1, a_2, \dots, a_n\}$ 。通过数学归纳法，我们构造了一个序列 $\{a_n\}_{n=1}^{\infty}$ ，其中所有 a_n 互不相同。则集合 $\{a_n \mid n \in \mathbb{N}\}$ 是 X 的一个可数无限子集。

定理 4.4.4 自然数集与有理数集等势

- (1) 自然数集与有理数集等势
- (2) 证明存在双射 $g : \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$

证明 $\mathbb{N} \times \mathbb{N}$ 与 \mathbb{N} 等势。

定义函数 $g : \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$ 如下：我们使用对角线枚举法。将 $\mathbb{N} \times \mathbb{N}$ 中的元素排列成一个二维网格，按照对角线顺序枚举：

$$\begin{aligned} & (0, 0), \\ & (0, 1), (1, 0), \\ & (0, 2), (1, 1), (2, 0), \\ & (0, 3), (1, 2), (2, 1), (3, 0), \\ & \vdots \end{aligned}$$

更形式化地，我们可以定义配对函数（这里和书上略有不同，因为这里是从 $(0, 0)$ 开始的）：

$$g(n) = (i, j) \quad \text{其中 } n = \frac{(i+j)(i+j+1)}{2} + j$$

这个函数是双射，因为不同的 n 对应不同的对 (i, j) ，而且每个对 $(i, j) \in \mathbb{N} \times \mathbb{N}$ 都有对应的 $n \in \mathbb{N}$ ，因此， $\mathbb{N} \times \mathbb{N}$ 与 \mathbb{N} 等势。

第二步：证明 \mathbb{Q} 与 \mathbb{N} 等势。

考虑有理数集 \mathbb{Q} ，每个有理数可以唯一表示为既约分数 $\frac{p}{q}$ ，其中 $p \in \mathbb{Z}, q \in \mathbb{N}^+$ ，且 $\gcd(p, q) = 1$ 。

定义函数 $h : \mathbb{Q} \rightarrow \mathbb{Z} \times \mathbb{N}^+$ 为 $h\left(\frac{p}{q}\right) = (p, q)$ ，其中 $\frac{p}{q}$ 是既约分数。

由于 \mathbb{Z} 与 \mathbb{N} 等势（可以通过交错排列正负整数来构造双射），且 \mathbb{N}^+ 与 \mathbb{N} 等势，所以 $\mathbb{Z} \times \mathbb{N}^+$ 与 $\mathbb{N} \times \mathbb{N}$ 等势。

结合第一步的结果， $\mathbb{Z} \times \mathbb{N}^+$ 与 \mathbb{N} 等势，因此 \mathbb{Q} 与 \mathbb{N} 等势。

综上，自然数集 \mathbb{N} 与有理数集 \mathbb{Q} 等势。

定理 4.4.5

可数个可数集合的并集仍然是可数集合。

设有一族可数集合 $\{A_n\}_{n=1}^{\infty}$ ，其中每个 A_n 是可数集合（即至多可数）。考虑并集 $S = \bigcup_{n=1}^{\infty} A_n$ 。需要证明 S 是可数集合。

由于每个 A_n 是可数的，存在满射 $f_n : \mathbb{N} \rightarrow A_n$ （如果 A_n 有限，则通过重复元素构造满射；如果 A_n 可数无限，则存在双射）。

现在，考虑笛卡尔积 $\mathbb{N} \times \mathbb{N}$ 。由于 $\mathbb{N} \times \mathbb{N}$ 是可数集合（存在双射 $g : \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$ ），定义映射 $f : \mathbb{N} \times \mathbb{N} \rightarrow S$ 为：

$$f(n, m) = f_n(m).$$

由于每个 f_n 是满射, f 是满射从 $\mathbb{N} \times \mathbb{N}$ 到 S 。又因为存在满射 $g : \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$, 复合映射 $f \circ g : \mathbb{N} \rightarrow S$ 是满射。因此, 存在满射从 \mathbb{N} 到 S , 这意味着 S 至多可数。

如果至少有一个 A_n 是无限集合, 则 S 是无限集合, 因此 S 是可数无限集合; 否则, 如果所有 A_n 有限, 则 S 可能有限或无限, 但至多可数。综上, S 是可数集合。

定理 4.4.6

开区间 $(0, 1)$ 是不可列的

使用康托尔对角线法证明。假设 $(0, 1)$ 是可数集合, 则存在双射 $f : \mathbb{N} \rightarrow (0, 1)$ 。我们可以将 $(0, 1)$ 中的所有实数枚举为:

$$x_1, x_2, x_3, \dots$$

每个 x_n 可以写成十进制小数形式 (为避免表示不唯一, 约定不使用无限连续的 9 的表示):

$$x_1 = 0.a_{11}a_{12}a_{13}\dots$$

$$x_2 = 0.a_{21}a_{22}a_{23}\dots$$

$$x_3 = 0.a_{31}a_{32}a_{33}\dots$$

⋮

其中每个 $a_{ij} \in \{0, 1, \dots, 9\}$ 。现在构造实数 $y = 0.b_1b_2b_3\dots \in (0, 1)$, 其中:

$$b_n = \begin{cases} 1 & \text{如果 } a_{nn} \neq 1 \\ 2 & \text{如果 } a_{nn} = 1 \end{cases}$$

这样确保 $b_n \neq a_{nn}$ 且 $b_n \neq 9$ (避免表示歧义)。

则 y 与每个 x_n 都不同, 因为 y 的第 n 位小数 b_n 与 x_n 的第 n 位小数 a_{nn} 不同。因此 y 不在枚举中, 与 f 是满射矛盾。假设错误, $(0, 1)$ 是不可数集合。

定理 4.4.7

实数集是不可列的

本题只需构造一个一一对应映射将 \mathbb{R} 映射到 $(0, 1)$ 上即可。或者构造一个一一对应映射将 $(0, 1)$ 映射到 \mathbb{R} 上即可。比如 $f : (0, 1) \rightarrow \mathbb{R}$ 可以定义为: $f(x) = \tan\left(\pi x - \frac{\pi}{2}\right)$

定理 4.4.8 \mathbb{R} 和 $\mathbb{R} \times \mathbb{R}$ 等势

实数集 \mathbb{R} 与其笛卡尔积 $\mathbb{R} \times \mathbb{R}$ 等势, 即存在从 \mathbb{R} 到 $\mathbb{R} \times \mathbb{R}$ 的双射。

我们可以通过构造显式的双射来证明。已知 $|\mathbb{R}| = \mathfrak{c}$, 且:

$$|\mathbb{R} \times \mathbb{R}| = \mathfrak{c} \times \mathfrak{c} = \max(\mathfrak{c}, \mathfrak{c}) = \mathfrak{c}$$

具体构造双射 $f : \mathbb{R} \rightarrow \mathbb{R} \times \mathbb{R}$ 的一种方法是通过交错小数展开:

对任意 $x \in \mathbb{R}$, 考虑其十进制展开 (为避免表示不唯一, 约定不使用无限连续的 9 的表示)。将 x 的小数部分按奇偶位分开:

$$x = a_0.a_1a_2a_3a_4\dots$$

定义:

$$f(x) = (0.a_1a_3a_5\dots, 0.a_2a_4a_6\dots)$$

即用奇数位小数构造第一个坐标, 偶数位小数构造第二个坐标。

可以验证这是一个双射, 因此 \mathbb{R} 和 $\mathbb{R} \times \mathbb{R}$ 等势。

第五章 图论

5.1 图的基本概念

定义 5.1.1 有向图, 无向图, 平行边, 邻接, 环, 孤立点, 简单图

1. 一个无向图可以被表示为 $G = (V, E)$, 其中 V 是一个非空集合 (有限), 称为顶点集, 其元素称为顶点或节点, E 是 V 中元素的无序对构成的集合, 称为边集, 即 $E \subseteq \{\{u, v\} \mid u, v \in V, u \neq v\}$
2. 一个有向图可以被表示为 $G = (V, E)$, 其中 V 是一个非空集合 (有限), 称为顶点集, 其元素称为顶点或节点, E 是 V 中元素的有序对构成的集合, 称为边集, 即 $E \subseteq \{(u, v) \mid u, v \in V, u \neq v\}$
3. 平行边: 在无向图中, 连接同一对顶点的多条边称为平行边, 在有向图中, 同一方向连接同一对顶点的多条弧称为平行边。
4. 邻接: 在无向图中, 如果存在边 $e = \{u, v\}$, 则称顶点 u 和 v 是邻接的 (相邻的)
5. 环: 如果一条边的两个端点关联于同一个结点, 称为环。
6. 孤立点: 在无向图中, 如果一个顶点不与任何其他顶点相邻, 则称它为孤立点。

不管是无向图还是有向图, 边集允许重复的元素多次出现, 即在一对结点之间存在多条边。如果关联一对结点的有向边的方向相同且有多个, 则称为平行边。

定义 5.1.2 度的概念

度数 (无向图): 顶点 v 的度数 (简称度) $\deg(v)$ 是与该顶点相关联的边的数量, 自环通常算作 2 度 (因为连接同一顶点的两个端点)

入度和出度 (有向图): 顶点 v 的入度 $\deg^-(v)$ 是以 v 为弧头的弧的数量, 顶点 v 的出度 $\deg^+(v)$ 是以 v 为弧尾的弧的数量, 顶点 v 的总度数 $\deg(v) = \deg^-(v) + \deg^+(v)$

悬挂结点: 度数为 1 的顶点称为悬挂结点, 在有向图中, 通常指总度数为 1 的顶点

悬挂边: 与悬挂结点相关联的边称为悬挂边。

最大度和最小度: 图 G 的最大度 $\Delta(G) = \max\{\deg(v) \mid v \in V(G)\}$, 图 G 的最小度 $\delta(G) = \min\{\deg(v) \mid v \in V(G)\}$

最大入度和最小入度 (有向图): 图 D 的最大入度 $\Delta^-(D) = \max\{\deg^-(v) \mid v \in V(D)\}$, 图 D 的最小入度 $\delta^-(D) = \min\{\deg^-(v) \mid v \in V(D)\}$

最大出度和最小出度 (有向图): 图 D 的最大出度 $\Delta^+(D) = \max\{\deg^+(v) \mid v \in V(D)\}$, 图 D 的最小出度 $\delta^+(D) = \min\{\deg^+(v) \mid v \in V(D)\}$

定义 5.1.3 图的基本分类

带权图: 每个结点或者每条边都带有数值的图称为带权图。

简单图: 如果一个图不存在平行边也不存在环，则称它为简单图。

多重图: 如果一个图存在平行边，则称它为多重图。

n 阶图: 具有 n 个顶点的图称为 n 阶图。

零图: 边集为空（没有边，只有结点）的图称为零图，即所有顶点都是孤立点。

平凡图: 只有一个顶点且没有边的图称为平凡图，是最简单的非空图（一阶零图）。

空图: 顶点集为空的图称为空图（通常不考虑）。

完全图: 任意两不同顶点之间都恰有一条边的简单图称为完全图。 n 阶完全图记作 K_n 。

二分图: 顶点集 V 可以划分为两个不相交子集 V_1 和 V_2 ，使得每条边的一个端点在 V_1 中，另一个端点在 V_2 中，称为二分图。

完全二分图: 顶点集 V 可以划分为两个不相交子集 V_1 和 V_2 ，使得每条边的一个端点在 V_1 中，另一个端点在 V_2 中，且 V_1 中的每个顶点都与 V_2 中的每个顶点相连，且图中没有其他边，则称 G 为完全二分图，记作 $K_{m,n}$ ，其中 $m = |X|$, $n = |Y|$

正则图: 所有顶点度数都相同的图称为正则图。若每个顶点的度数均为 k ，称为 k -正则图。

环图: n 个顶点 v_1, v_2, \dots, v_n 依次连接形成的环状图称为环图，记作 C_n 。

轮图: 在环图 C_{n-1} 中添加一个顶点，并将该顶点与环图中所有顶点相连，称为轮图 W_n 。

n 方体图: 用 n 维超立方体的顶点和边构成的图称为 n 方体图，记作 Q_n 。顶点集为所有长度为 n 的二进制串，两个顶点相邻当且仅当它们的二进制表示恰好有一位不同。

定理 5.1.1 图的基本定理

握手定理: 设 $G = (V, E)$ 是一个无向图，则所有顶点的度数之和满足 $\sum_{v \in V} \deg(v) = 2|E|$

证明: 由于每条边连接两个顶点，每条边在度数求和中被计算了两次（一次为每个端点）。因此，总度数之和等于边数的两倍。具体地，对于每条边 $e = \{u, v\} \in E$ ，它贡献 1 到 $\deg(u)$ 和 1 到 $\deg(v)$ ，所以在求和 $\sum_{v \in V} \deg(v)$ 中，每条边恰好被计算两次。故

$$\sum_{v \in V} \deg(v) = 2|E|$$

定理 5.1.2 有向图握手定理

设 $D = (V, A)$ 是有向图，则所有顶点的入度之和等于所有顶点的出度之和，且都等于边数：

$$\sum_{v \in V} \deg^-(v) = \sum_{v \in V} \deg^+(v) = |A|$$

证明: 每条有向边有一个起点和一个终点，为起点的出度贡献 1，为终点的入度贡献 1。因此，总入度之和等于总出度之和，都等于边数。

定理 5.1.3 握手定理推论

任意图中，度数为奇数的顶点个数为偶数。

设 G 是 n 阶无向图，则 G 中最大度数满足 $\Delta(G) \leq n - 1$ 。

在任意无向图中，所有顶点的平均度数为 $\frac{2|E|}{|V|}$ 。

如果无向图 G 是 k -正则图（每个顶点度数均为 k ），则 $k|V| = 2|E|$

设 V_1 为度数为奇数的顶点集合， V_2 为度数为偶数的顶点集合。由握手定理，总度数和为偶数。 V_2 中顶点度数之和为偶数，故 V_1 中顶点度数之和也必为偶数，因此 $|V_1|$ 必为偶数。

定理 5.1.4 可简单图化的判定定理（Havel-Hakimi 算法）

一个非负整数序列 $d = (d_1, d_2, \dots, d_n)$ （其中 $d_1 \geq d_2 \geq \dots \geq d_n$ ，和为偶数）是可简单图化的，当且仅当可以通过 **Havel-Hakimi 算法** 判定：

1. 将序列按非递增顺序排序
2. 如果序列全为零，则是可简单图化的
3. 如果序列中有负数，或最大度数 $d_1 \geq n$ ，则不可简单图化
4. 否则，删除第一个元素 d_1 ，然后将接下来的 d_1 个元素每个减 1
5. 返回步骤 1，重复上述过程

如果序列可简单图化，那么存在一个简单图以该序列为度序列，如果在某一步出现负数，说明无法构造满足条件的简单图，如果算法最终得到全零序列，则原序列是可简单图化的

示例：判定序列 $(3, 3, 2, 2, 2)$ 是否可简单图化：

```
(3, 3, 2, 2, 2)  删除 3, 后面 3 个数各减 1
→(2, 1, 1, 2)  重新排序为(2, 2, 1, 1)
→(2, 2, 1, 1)  删除 2, 后面 2 个数各减 1
→(1, 0, 1)  重新排序为(1, 1, 0)
→(1, 1, 0)  删除 1, 后面 1 个数减 1
→(0, 0)  全为零, 可简单图化
```

定义 5.1.4 补图

设 $G = (V, E)$ 是一个简单无向图（无自环和无重边），其顶点集 V 有 n 个顶点。令 K_n 表示完全图，其顶点集为 V ，边集为 $E(K_n)$ （即所有可能的无序顶点对）。则图 G 的补图记为 $\sim G$ ：

$$\sim G = (V, E(K_n) - E)$$

换句话说， $\sim G$ 的边集由 K_n 中所有不在 G 中的边组成。

定义 5.1.5 图的基本运算

1. 删除边运算设 $G = (V, E)$ 是一个图, $e \in E$ 是 G 的一条边。从 G 中删除边 e 得到的图记为 $G - e$, 定义为:

$$G - e = (V, E - \{e\})$$

即顶点集不变, 仅从边集中移除边 e 。

2. 删除边集运算设 $G = (V, E)$ 是一个图, $F \subseteq E$ 是 G 的一个边子集。从 G 中删除边集 F 得到的图记为 $G - F$, 定义为:

$$G - F = (V, E - F)$$

即顶点集不变, 从边集中移除所有属于 F 的边。

3. 删除结点运算设 $G = (V, E)$ 是一个图, $v \in V$ 是 G 的一个顶点。从 G 中删除顶点 v 得到的图记为 $G - v$, 定义为:

$$G - v = (V - \{v\}, E - \{e \in E \mid v \in e\})$$

即从顶点集中移除 v , 同时移除所有与 v 相关联的边。

4. 删除结点集运算设 $G = (V, E)$ 是一个图, $U \subseteq V$ 是 G 的一个顶点子集。从 G 中删除顶点集 U 得到的图记为 $G - U$, 定义为:

$$G - U = (V - U, E - \{e \in E \mid e \cap U \neq \emptyset\})$$

即从顶点集中移除所有属于 U 的顶点, 同时移除所有与 U 中顶点相关联的边。

5. 边的收缩运算设 $G = (V, E)$ 是一个图, $e = uv \in E$ 是 G 的一条边。收缩边 e 得到的图记为 G/e , 定义为: 将顶点 u 和 v 合并为一个新顶点 w , 所有与 u 或 v 相关联的边(除 e 外)改为与 w 相关联, 删去边 e , 如果合并后产生重边, 通常保留一条(简单图)或全部保留(多重图)。形式化地, $G/e = (V', E')$, 其中:

$$V' = (V - \{u, v\}) \cup \{w\}, \quad E' = E - \{e\}$$

6. 加新边运算设 $G = (V, E)$ 是一个图, $e = (u, v)$ 是连接 G 中两个顶点 $u, v \in V$ 但 $e \notin E$ 的边。向 G 中添加新边 e 得到的图记为 $G + e$, 定义为:

$$G + e = (V, E \cup \{e\})$$

即顶点集不变, 向边集中添加新边 e 。

注意, 删去边通常会保留结点, 但是删去结点通常不会保留边, 加新边不会引入新的结点, 边的收缩会影响结点的数量。

定义 5.1.6 子图及相关概念

1. **子图**设图 $G = (V, E)$ 和图 $H = (V', E')$ 。如果 $V' \subseteq V$ 且 $E' \subseteq E$, 并且 H 中每条边的端点都在 V' 中, 则称 H 是 G 的子图, 记作 $H \subseteq G$ 。
2. **母图**如果 H 是 G 的子图, 则称 G 是 H 的母图。
3. **真子图**如果 H 是 G 的子图, 且 $H \neq G$ (即 $V' \subset V$ 或 $E' \subset E$), 则称 H 是 G 的真子图。
4. **生成子图**如果 H 是 G 的子图, 且 $V' = V$ (即顶点集相同), 则称 H 是 G 的生成子图。
5. **导出的子图**记作导出子图分为两类:

结点集导出子图: 对于 G 的顶点子集 $V_1 \subseteq V$, 由 S 导出的子图记作 $G(V_1)$, 其顶点集为 S , 边集为 G 中所有端点都在 S 中的边, 即 $E(G(V_1)) = \{e \in E \mid e \subseteq S\}$ 。

边集导出子图: 对于 G 的边子集 $F \subseteq E$, 由 F 导出的子图记作 $G[F]$, 其顶点集为 F 中所有边的端点的并集, 边集为 F 。

注意, 生成子图保留了全部的结点, 以及某些边 (可选)。但是结点集导出子图仅保留部分的结点, 而其边集则是由其保留的结点来确定。边集导出子图仅保留部分的边, 而其顶点集则是由其保留的边来确定。

再加上上面介绍的删除结点, 删除边等运算, 下面讨论它们的区别和联系。

$G(V - V_1)$ 是由结点集 $V - V_1$ 导出的子图, 也就是在图 G 中删除结点集 V_1 以及所有它们关联的边所得到的子图。所以可以将 $G(V - V_1)$ 视作 $G - V_1$ 。而 $G(E - E_1)$ 是由边集 $E - E_1$ 导出的子图, 也就是在图 G 中删除边集 E_1 以及里面的所有边所导出的子图, 反观 $G - E_1$, 由于删除边集时要保留结点不可以删除, 所以删除边集运算不会改变结点数量, 而删除边集导出的子图会改变结点数量, 因为导出过程关注边 (及其关联的结点) 而非可能存在的孤立结点, 所以要注意区别 $G(E - E_1)$ 和 $G - E_1$ 。

定义 5.1.7 图的同构, 自互补图

设 $G = (V, E)$ 和 $H = (U, F)$ 是两个简单图 (无向图或有向图)。如果存在一个双射函数 $f : V \rightarrow U$, 使得对于 G 中的任意两个顶点 $u, v \in V$:

$$(u, v) \in E(G) \iff (f(u), f(v)) \in E(H)$$

则称图 G 和图 H 是同构的, 记作 $G \cong H$, 并称 f 是 G 到 H 的一个同构映射。

自互补图: 如果一个图与自身的补图同构, 则称该图为自互补图。

定理 5.1.5 同构的不变量

如果两个图同构, 则它们必须共享以下性质 (同构不变量):

顶点数相同, 边数相同, 结点度数序列相同 (不计顺序), 连通分支数和每个分支的大小相同, 围长 (最短环长度) 相同, 直径相同, 色数相同, 特征多项式相同 (邻接矩阵的特征多项式)

注意: 同构关系是等价关系 (自反、对称、传递)

定理 5.1.6 自互补图的性质

设 G 是一个 n 阶自互补图（即 $G \cong \sim G$ ），则以下性质成立：

自互补图对应的完全图边数为偶数

顶点数性质： $n \equiv 0 \pmod{4}$ 或 $n \equiv 1 \pmod{4}$

边数性质： G 的边数为 $\frac{n(n-1)}{4}$

正则性：如果 d 是 G 中某个顶点的度数，则 $n-1-d$ 也必须是 G 中某个顶点的度数

直径性质：自互补图的直径最大为 3（直径的定义后文会给出）

连通性：所有自互补图都是连通的

边数性质：由于 G 和 $\sim G$ 同构，它们边数相等，所以自互补图对应的完全图边数为偶数。完全图 K_n 有 $\frac{n(n-1)}{2}$ 条边，这些边被平分给 G 和 $\sim G$ ，所以 G 的边数为 $\frac{n(n-1)}{4}$ ，这必须是整数，故 $n(n-1)$ 必须被 4 整除。

在同构映射下，度数为 d 的顶点映射到度数为 $n-1-d$ 的顶点。如果直径大于 3，则存在距离为 4 的顶点对，在补图中距离为 1，矛盾。如果不连通，则补图连通，但自互补图必须与补图有相同的连通性。

例题 5.1.1

证明：6 个人聚在一起，必然有 3 个人互相认识彼此（双向认识），或者至少有 3 个人互相都不认识彼此（双向不认识）。

将 6 个人视为 6 个顶点，构建一个完全图 K_6 。定义图 G ：顶点表示人，边表示两人互相认识。则补图 $\sim G$ 表示两人互相不认识。问题转化为证明：要么 G 包含一个三角形（即 3 个顶点两两相连），要么 $\sim G$ 包含一个三角形。

考虑任意顶点 v 。在完全图 K_6 中， v 与其他 5 个顶点相连。由于边要么在 G 中，要么在 $\sim G$ 中，有：

$$\deg_G(v) + \deg_{\sim G}(v) = 5$$

因此， $\deg_G(v)$ 和 $\deg_{\sim G}(v)$ 中至少有一个大于等于 3。不妨设 $\deg_G(v) \geq 3$ （如果 $\deg_{\sim G}(v) \geq 3$ ，证明类似，只需交换 G 和 $\sim G$ 的角色）。

设 v 在 G 中的三个邻居为 a, b, c 。现在考虑 a, b, c 之间的边：

如果 a, b, c 中有一对在 G 中相连，比如 $ab \in E(G)$ ，则 v, a, b 构成一个三角形在 G 中（即三人互相认识）。

如果 a, b, c 中没有任何一对在 G 中相连，则 a, b, c 之间的所有边都在 $\sim G$ 中，即 $ab, ac, bc \in E(\sim G)$ ，所以 a, b, c 构成一个三角形在 $\sim G$ 中（即三人互相不认识）。

因此，无论哪种情况，都存在一个三角形在 G 或 $\sim G$ 中，即必有 3 个人互相认识或 3 个人互相不认识。证毕。

5.2 特殊图**5.3 树**