离散数学笔记

1.基础知识

1.1 集合与序列

1.1.1集合概念

组成一个集合的条件是能够明确地判断任意一个对象是或者不是该 集合的元素
集合中的元素没有次序，一个集合中也没有相同的元素，如果一个 集合中出现若干个相同的元素，则将它们作为一个元素 即一个集合由它的元素所决定，与描述它时列举其元素的特定顺序无关

1.1.2集合形式化表示

外延表示法（列举法）& 内涵表示法（描述法）

1.1.3幂集

假设 A 是集合，A 的所有子集所组成的集合称作A的幂 集（power set），记作P (A)，即 P (A) = { x | x 包含于A }

如：A ={a，c} P(A) = {φ，{a}，{c}，{a，c}}

1.1.4基数或势

一个集合A 所包含的元素数目称为该集合的基数或势 （cardinality），记作 |A| 或 #A 或 card(A)

1.1.5集合的运算

1） 并运算：$A \cup B = \{x | x \in A \vee x \in B\}$

2） 交运算：$A \cap B = \{x | x \in A \wedge x \in B\}$

3） 差运算：$A - B = \{x | x \in A \wedge x \notin B\}$

4） 对称差：$A \oplus B = (A - B) \cup (B - A) = (A \cup B) - (A \cap B)$

5） A的绝对补集$\sim A$定义如下：

$$\sim A = E - A = \{x | x \in E \wedge x \notin A\}$$

幂等律	$A\cup A=A$
	$A\cap A=A$
结合律	$(A\cup B)\cup C=A\cup(B\cup C)$
	$(A\cap B)\cap C=A\cap(B\cap C)$
交换律	$A\cup B=B\cup A$
	$A\cap B=B\cap A$

分配律	$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$
	$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$
同一律	$A\cup\varnothing=A$
	$A\cap E=A$
零　律	$A\cup E=E$
	$A\cap\varnothing=\varnothing$
排中律	$A\cup\sim A=E$
矛盾律	$A\cap\sim A=\varnothing$
吸收律	$A\cup(A\cap B)=A$
	$A\cap(A\cup B)=A$
德摩根律	$A-(B\cup C)=(A-B)\cap(A-C)$
	$A-(B\cap C)=(A-B)\cup(A-C)$
	$\sim(B\cup C)=\sim B\cap\sim C$
	$\sim(B\cap C)=\sim B\cup\sim C$
	$\sim\varnothing=E$
	$\sim E=\varnothing$

1.2数论基础

1.2.1整数的整除性

若余数 r =0，则称 m 能被 n 整除（m is dividable by n）， 或 n 整除 m（n divides m），记作 n|m。若 n|m，则存在整数 q 使得 m=q*n，且有 n≤|m|

假设 a, b, c 是整数，a≠0，则
(a) 若 a|b 且 a|c，则对于任意的整数 x, y，有 a|(xb+yc);
(b) 若 b≠0，a|b 且 b|c，则 a|c;
(c) 若 b≠0，a|b 且 b|a，则 a=±b。

1.2.2欧几里得算法与裴蜀等式

定理 设 a=qb+r，其中 a, b, q, r 都是整数，则 GCD(a, b) = GCD(b, r)

- 欧几里得算法（辗转相除法） **GCD (a, b)**
- 输入：整数 a, b ，满足 $a \ge b \ge 0$ ，且 a, b 不全为0
- 输出：GCD(a, b)

Step1 If $b = 0$ then return a

Step2 Else return GCD(b, a mod b)

其中，若 $a=q \cdot b+r$ 且 $0 \le r < b$

则定义 $a \bmod b = r$

- 对于不全为0的整数 a, b 和 d ，方程 $sa+tb=d$ 存在整数解 s 和 t 当且仅当 GCD(a, b)|d 。
- 方程 $sa+tb=d$ 称作**裴蜀（Bezout）等式**或**贝祖等式**。

1.2.3同余

- 设 n 是正整数，a 和 b 是整数，如果$n|(a-b)$，则称 a **模 n 同余于 b**，或 **a 与 b 模 n 同余（congruent）**，记作 $a \equiv b \pmod{n}$，n 称为**模（modulus）**
- 例
  - $70 \equiv 5 \pmod{13}$
  - $-19 \equiv 6 \pmod{25}$

1.3布尔矩阵及其运算

是一个元素为0或1的矩阵

定义其补 （complement）为 A = [~aij] = [1-aij]

定义A 和B的并（join）为A∨B = C = [cij],其中 $c_{ij} = \begin{cases} 1 & 若\ a_{ij}=1\ 或\ b_{ij}=1 \\ 0 & 若\ a_{ij}=0\ 且\ b_{ij}=0 \end{cases}$

则定义A 和B的交（meet）为A∧B = D = [dij]，其中 $d_{ij} = \begin{cases} 1 & 若\ a_{ij}=1\ 且\ b_{ij}=1 \\ 0 & 若\ a_{ij}=0\ 或\ b_{ij}=0 \end{cases}$

设 A=[aij] 是 m·n 的布尔矩阵， B=[bij] 是 n·r 的布尔矩 阵，则定义 A 和 B 的 布尔积（Boolean product）为 A⊙B = C = [cij]，其中

$$c_{ij}=\begin{cases}1 & 若存在k，\ 1\le k\le n，\\ & 使得\ a_{ik}=1\ 且\ b_{kj}=1\\ 0 & 否则\end{cases}$$

1.4计数基础

1.3.1 鸽巢原理

若有 n 个鸽巢，n+1 个鸽子，则至少有一个巢内有至 少两个鸽子。

1.3.2容斥原理

- 定理

  设 A、B 为两个有限集，则

  $$|A\cup B|=|A|+|B|-|A\cap B|。$$

- 容斥原理可以推广到三个有限集元素的计数问题：
- 定理

  设 A, B, C 是有限集合，则

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

2.命题逻辑

2.1命题

1) 命题：能判断其真值的陈述句.
2) 真值：真、假.　　（1、0）
3) 真命题：真值为真的命题.
4) 假命题：真值为假的命题.
5) 原子命题（简单命题）：不能再被分解成更简单的命题.
6) 复合命题：由简单命题通过联结词联结而成的命题.

2.2命题联结词

<table>
<tr><th>联结词</th><th>符号化</th><th>真值表</th></tr>
<tr><td>否定</td><td>$\neg$</td><td><table><tr><td>p</td><td>$\neg p$</td></tr><tr><td>0</td><td>1</td></tr><tr><td>1</td><td>0</td></tr></table></td></tr>
<tr><td>合取</td><td>$\wedge$</td><td><table><tr><td>p</td><td>q</td><td>$p\wedge q$</td></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>0</td></tr><tr><td>1</td><td>0</td><td>0</td></tr><tr><td>1</td><td>1</td><td>1</td></tr></table></td></tr>
<tr><td>析取</td><td>$\vee$</td><td><table><tr><td>p</td><td>q</td><td>$p\vee q$</td></tr><tr><td>0</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td></tr><tr><td>1</td><td>1</td><td>1</td></tr></table></td></tr>
<tr><td>蕴涵</td><td>$\rightarrow$</td><td><table><tr><td>p</td><td>q</td><td>$p\rightarrow q$</td></tr><tr><td>0</td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>0</td></tr><tr><td>1</td><td>1</td><td>1</td></tr></table></td></tr>
<tr><td>等价</td><td>$\leftrightarrow$</td><td><table><tr><td>p</td><td>q</td><td>$p\leftrightarrow q$</td></tr><tr><td>0</td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>0</td></tr><tr><td>1</td><td>0</td><td>0</td></tr><tr><td>1</td><td>1</td><td>1</td></tr></table></td></tr>
</table>

2.3命题公式及其赋值

1） 命题变元：取值 1（真）或 0（假）的变元.

2） 合式公式：将命题变元用联结词或圆括号按一定逻辑关系联结起来的符号串.

3） 设 $p_1,p_2,\ldots,p_n$ 是出现在公式 A 中的全部命题变元，给 $p_1,p_2,\ldots,p_n$ 各指定一个真值，称为对 A 的一个赋值，若指定的一组值使 A 为 1，则称这组值为 A 的成真赋值；若使 A 为 0，则称这组值的成假赋值.

设 A 为任一命题公式

1） 若 A 在它的各种赋值下取值均为真，则称 A 为重言式或永真式.

2） 若 A 在它的各种赋值下取值均为假，则称 A 为矛盾式或永假式.

3） 若 A 不是矛盾式，则称 A 为可满足式.

2.4等值式

常见等值式：

1) 双重否定律 $A \Leftrightarrow \neg\neg A$

2) 幂等律 $A \Leftrightarrow A \vee A$, $A \Leftrightarrow A \wedge A$

3) 交换律 $A \vee B \Leftrightarrow B \vee A$, $A \wedge B \Leftrightarrow B \wedge A$

4) 结合律 $(A \vee B) \vee C \Leftrightarrow A \vee (B \vee C)$

$(A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C)$

5) 分配律 $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$ （$\vee$对$\wedge$的分配律）

$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$ （$\wedge$对$\vee$的分配律）

6) 德摩根律 $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$, $\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$

7) 吸收律 $A \vee (A \wedge B) \Leftrightarrow A$, $A \wedge (A \vee B) \Leftrightarrow A$

8) 零律 $A \vee 1 \Leftrightarrow 1$, $A \wedge 0 \Leftrightarrow 0$

9) 同一律 $A \vee 0 \Leftrightarrow A$, $A \wedge 1 \Leftrightarrow A$

10) 排中律 $A \vee \neg A \Leftrightarrow 1$

11) 矛盾律 $A \wedge \neg A \Leftrightarrow 0$

12) 蕴涵等值式 $A \rightarrow B \Leftrightarrow \neg A \vee B$

13) 等价等值式 $A \leftrightarrow B \Leftrightarrow (A \rightarrow B) \wedge (B \rightarrow A)$

14) 假言易位 $A \rightarrow B \Leftrightarrow \neg B \rightarrow \neg A$

15) 等价否定等值式 $A \leftrightarrow B \Leftrightarrow \neg A \leftrightarrow \neg B$

16) 归谬论 $(A \rightarrow B) \wedge (A \rightarrow \neg B) \Leftrightarrow \neg A$

2.5析取范式和合取范式

1) 文字：命题变元及其否定.

2) 简单析取式：仅由有限个文字构成的析取式.

3) 简单合取式：仅由有限个文字构成的合取式.

4) 析取范式：由有限个简单合取式的析取构成的命题式. $A_1 \vee A_2 \vee \ldots \vee A_s$，其中 $A_i (i=1,2,\ldots,s)$ 是简单合取式.

5) 合取范式：由有限个简单析取式的合取构成的命题式. $B_1 \wedge B_2 \wedge \ldots \wedge B_t$，其中 $B_j (j=1,2,\ldots,t)$ 是简单析取式.

2.6主析取范式和主合取范式

在含有n个命题变元的简单合取式（简单析取式）中，若每个命题变元和它的否定式恰好出现一个且仅出现一次，而且命题变元或它的否定式按照下标从小到大顺序排列，称这样的简单合取式（简单析取式）为极小项（极大项）.

表 1　含 p,q 的极小项与极大项

极小项			极大项		
公式	成真赋值	名称	公式	成假赋值	名称
$\neg p \wedge \neg q$	0 0	m_0	$p \vee q$	0 0	M_0
$\neg p \wedge q$	0 1	m_1	$p \vee \neg q$	0 1	M_1
$p \wedge \neg q$	1 0	m_2	$\neg p \vee q$	1 0	M_2
$p \wedge q$	1 1	m_3	$\neg p \vee \neg q$	1 1	M_3

2.7命题逻辑的推理

- **推理**是从前提推出结论的思维过程
- **前提(premise)**，或称**假设(hypothesis)**，是指已知的命题公式 $A_1, A_2 \ldots A_n$
- **结论(conclusion)**是从前提出发应用推理规则推出的命题公式 B
- **正确的推理**或**有效的推理**即是指 $A_1 \wedge A_2 \wedge \ldots \wedge A_n \Rightarrow B$ 是重言式

- 定理（**基本推理公式**）以下蕴涵式皆为重言式：

(a) 附加律　$A \Rightarrow (A \vee B)$

(b) 化简律　$(A \wedge B) \Rightarrow A$

(c) 假言推理/分离式　$(A \Rightarrow B) \wedge A \Rightarrow B$

(d) 析取三段论　$(A \vee B) \wedge \sim B \Rightarrow A$

(e) 拒取式　$(A \Rightarrow B) \wedge \sim B \Rightarrow \sim A$

(f) 假言三段论　$(A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow (A \Rightarrow C)$

□主要的推理规则：

(a) 前提引入规则

在证明的任何步骤上，都可引入前提。

(b) 结论引入规则

在证明的任何步骤上，所证明的结论都可以作为后续证明的前提。

(c) 代入规则 $(A \Rightarrow B) \wedge ((B \wedge C) \Rightarrow r) \Rightarrow ((A \wedge C) \Rightarrow r)$ 是重言式

与命题逻辑等值演算中的代入规则相同。

(d) 置换规则

在证明的任何步骤上，命题公式中的任何子命题公式都可以用与之等值的命题公式置换

附加前提

欲证明	等价地证明
前提: $p_1, p_2, \ldots, p_k$	前提: $p_1, p_2, \ldots, p_k, r$
结论: $r \Rightarrow q$	结论: q

反证法

□欲证明：

- 前提：A_1，A_2，…，A_n
- 结论：B

□可以等价地证明：

- 前提：A_1，A_2，…，A_n，$\sim B$
- 结论：矛盾

3.谓词逻辑

3.1谓词与量词

□个体词（**individual**）是一个命题里表示思维对象的词，表示独立存在的具体或抽象的客体

□具体的、确定的个体词称为个体常项，一般用 a, b, c 表示

□抽象的、不确定的个体词称为个体变项，一般用 x, y, z 表示

□个体变项的取值范围称作个体域或论域（**domain of the discourse**）

□宇宙间一切事物组成的个体域称作全总个体域（**universal domain of individuals**）

- 表示个体词性质或相互之间关系的词称作**谓词（predicate）**。
- 如果命题里只有一个个体词，这时表示该个体词性质或属性的词便称为谓词。这是**一元（目）谓词**，以 $P(x)$, $Q(x)$, …表示。

- 如果在命题里的个体词多于一个，那么表示这几个个体词间的关系的词称作谓词。这是多元（目）谓词，有 n 个个体的谓词 $P(x_1, \ldots, x_n)$ 称 **n 元（目）谓词**，以 $P(x, y)$, $Q(x, y)$, $R(x, y, z)$, …表示。
- **全称量词(universal quantification)** "$\forall$"
  - 读作"所有的x"、"任意x"或"一切x"
  - 含意相当于自然语言中的"任意的"、"所有的"、"一切的"、"每一个"、"凡"等
  - $(\forall x)P(x)$ 意指对论域 D 中的所有个体都具有性质 P
  - 命题 $(\forall x)P(x)$ 当且仅当对论域中的所有 x 来说，$P(x)$ 均为真时方为真。

- **存在量词(existential quantification)** "$\exists$"
  - 读作"存在x"
  - 含意相当于自然语言中的"某个"、"存在"、"有的"、"至少有一个"、"有些"等
  - $(\exists x)P(x)$ 意指对论域 D 中至少有一个个体具有性质 P

3.2谓词公式及分类

- 谓词逻辑中的**谓词公式(well formed formula，简记为wff)**递归地定义为：
  - (1) 命题常项、命题变项和原子谓词公式（不含联结词的谓词）是谓词公式；
  - (2) 如果 A 是谓词公式，则 $\sim A$ 也是谓词公式；
  - (3) 如果 A 和 B 是谓词公式，则由逻辑联结词联结 A 和 B 的符号串也是谓词公式，
  - (4) 若 A 是谓词公式，且 A 中无 $\forall x$ 及 $\exists x$ 出现，则 $(\forall x)A(x)$, $(\exists x)A(x)$ 也是谓词公式；
  - (5) 只有有限次地应用(1)-(4)构成的符号串才是谓词公式。
- 谓词公式也称为**合式公式**，简称**公式**。

- 类似于命题逻辑中对命题公式进行的真值指派，可以对谓词逻辑公式赋予不同的解释
- 谓词公式的一个**解释（interpretation）**由下面4部分组成：
  - (1) 非空的论域 D；
  - (2) D 中一部分特定元素；
  - (3) D 上一些特定的函数；
  - (4) D 上一些特定的谓词。
- 例 谓词公式 $(\exists x)\, P(f(x), 2)$

①D ②

$F(x) \Rightarrow G(x+y,2)$

④ ③

1.逻辑有效式

设 A 为一个谓词公式，若 A 在任何解释下真值均为真

2.矛盾式

设 A 为一个谓词公式，若 A 在任何解释下真值均为假

3.可满足式

设 A 为一个谓词公式，若至少存在一个解释使 A 为真（逻辑有效式一定是可满足式；反之不然）

4.代换实例

- 设命题公式 A_0 含命题变项 $p_1, p_2, \ldots, p_n$，用 n 个谓词公式 $A_1, A_2, \ldots, A_n$ 分别处处代换 $p_1, p_2, \ldots, p_n$，所得公式 A 称为 A_0 的**代换实例**。
- 例
  - $p \Rightarrow q$
  - $P(y) \Rightarrow Q(z)$
  - $(\forall x)P(x) \Rightarrow (\exists x)Q(x)$

- 定理

命题公式中的重言式的代换实例都是逻辑有效式，在谓词公式中可仍称为**重言式**；命题公式中的矛盾式的代换实例都是矛盾式。

- 例
  - (1) $\forall x\, P(x) \Rightarrow (\forall x \exists y\, Q(x,y) \Rightarrow \forall x\, P(x))$

    $p \Rightarrow (q \Rightarrow p)$
  - (2) $\forall x\, P(x) \Rightarrow (\forall x\, P(x) \vee \exists y\, G(y))$

    $p \Rightarrow (p \vee q)$

5.谓词公式的各部分名称

- 设 A 为谓词公式，B 为 A 中的一个连续的符号串，且 B 为谓词公式，则称 B 为 A 的**子公式（sub formula）**
- 设 A 为谓词公式，$(\forall x)P(x)$ 或 $(\exists x)P(x)$ 为公式 A 的子公式
  - 紧跟在 ∀、∃ 之后的 x 称为量词的**指导变项**或**作用变项**，$P(x)$ 称为相应量词的**作用域**或**辖域（scope）**
  - 在辖域中 x 的一切出现均称为**约束出现**，受指导变项所约束
  - 所有约束出现的变项称为**约束变项（bounded variable）**
  - 在 A 中除了约束变项外出现的变项均称为**自由变项（free variable）**，不受指导变项的约束

3.3自然语句形式化

- 基本方法是：
  - **1.** 首先要将问题分解成一些原子命题和逻辑联结符
  - **2.** 之后分解出各个原子命题的个体词、谓词和量词
  - **3.** 按照合式公式的表示规则翻译出自然语句

3.4谓词逻辑的等值演算

- 谓词逻辑中的基本等值式主要分两类：
  - 其一是从命题公式移植来的等值式，即命题逻辑中基本等值式的代换实例
    - 如$(\forall x)F(x)\Rightarrow(\exists y)G(y) \equiv \sim(\forall x)F(x)\vee(\exists y)G(y)$
  - 另一类是谓词逻辑所特有的等值式，与量词有关

- **（量词否定等值式/德 摩根律）**
  - 设 $A(x)$ 是含 x 自由出现的公式，则

$$\sim(\forall x)A(x)\equiv(\exists x)\sim A(x)$$

$$\sim(\exists x)A(x)\equiv(\forall x)\sim A(x)$$

□（量词辖域收缩与扩张等值式）

设 $A(x)$ 是含 x 自由出现的公式，谓词公式 B 中不含 x 的出现，则有

$$\forall x(A(x)\vee B) \equiv \forall xA(x)\vee B$$
$$\forall x(A(x)\wedge B) \equiv \forall xA(x)\wedge B$$
$$\exists x(A(x)\vee B) \equiv \exists xA(x)\vee B$$
$$\exists x(A(x)\wedge B) \equiv \exists xA(x)\wedge B$$

□（量词分配等值式）

设 $A(x)$, $B(x)$ 是含 x 自由出现的谓词公式，则有

$$\forall x(A(x)\wedge B(x)) \equiv \forall xA(x)\wedge \forall xB(x)$$
$$\exists x(A(x)\vee B(x)) \equiv \exists xA(x)\vee \exists xB(x)$$

□注意：$\forall$对$\vee$不满足分配律，$\exists$对$\wedge$不满足分配律

当 $D = \{a_1, a_2, \ldots, a_m\}$ 时

$\forall x\, A(x) \equiv A(a_1)\wedge A(a_2)\wedge\ldots\wedge A(a_m)$,

$\exists x\, A(x) \equiv A(a_1)\vee A(a_2)\vee\ldots\vee A(a_m)$

□设 $A(x, y)$ 是含 x, y 自由出现的谓词公式，则有

$$\forall x\forall y\, A(x, y) \equiv \forall y\forall x\, A(x, y)$$
$$\exists x\exists y\, A(x, y) \equiv \exists y\exists x\, A(x, y)$$

□这组等值式表明相同量词与排列的次序无关，但是对于不同量词，不能随意更换次序，即 $(\forall x)(\exists y)A(x, y)$ 与 $(\exists y)(\forall x)A(x, y)$ 不等值

1.三条等值演算规则

□谓词逻辑包括以下三条等值演算规则：

- 置换规则
  - □设 $\Phi(A)$ 是含谓词公式 A 的公式，$\Phi(B)$ 是用谓词公式 B 取代 $\Phi(A)$ 中的 A（不一定是每一处）之后得到的谓词公式，若 $A\equiv B$，则 $\Phi(A)\equiv\Phi(B)$。
- 代替规则
- 换名规则

- $\forall x\,(P(x,z) \Rightarrow \exists y\, Q(x,y)) \wedge \forall x\, R(x,y)$
- 同一个个体变项符号既有约束出现又有自由出现，容易引起概念上的混淆。
- 为避免这种情况，引入了下面的代替规则和换名规则，使得
  - 同一个个体变项符号在一个公式中只呈现一种形式，要么为约束出现，要么为自由出现
  - 同时使不同的量词所约束的个体变项不同名，便于计算机处理
- **（代替规则）**将谓词公式 A 中某个自由出现的个体变项的**所有**自由出现改成 A 中未曾出现的某个个体变项符号，其余部分不变，记所得谓词公式为 A'，则 $A \equiv A'$
- **（换名规则）**将谓词公式 A 中某量词的指导变项及其在辖域内的所有约束出现改成该量词辖域内未曾出现的某个个体变项符号，其余部分不变，记所得谓词公式为 A'，则 $A \equiv A'$

2.证明假命题

- 证明 $\forall x\,(P(x) \Rightarrow Q(x))$ 是假命题的方法——
- 由
  $\sim(\forall x(P(x) \Rightarrow Q(x))) \equiv (\exists x)(P(x) \wedge \sim Q(x)))$
- 则只需要找到论域 D 中一个个体 x_0 使得 $P(x_0)$ 同时 $Q(x_0)$ 为假
- 这个过程称作反驳（ **disproof** ）
- x_0 称作反例（ **counterexample** ）

3.5前束范式

- 设 A 为一谓词公式，如果满足
  (1) 所有量词都位于该公式的最左边；
  (2) 所有量词前都不含否定词；
  (3) 量词的辖域都延伸到整个公式的末端，
- 则称 A 为**前束范式（prenex formal form）**

- 前束范式的一般形式为：

$$\underline{Q_1 x_1 Q_2 x_2 \ldots Q_n x_n}\ \underline{M(x_1, x_2, \ldots, x_n)}$$

- 其中 $Q_i (1 \le i \le n)$ 为 $\forall$ 或 $\exists$
- $Q_1 x_1 Q_2 x_2 \ldots Q_n x_n$ 称为**前束**
- M 为不含量词的公式，称作公式的**基式**或**母式**

- 化前束范式的基本方法：

步骤1. 消去谓词公式中的联结词⇒，⇔；

步骤2. 将谓词公式中的否定词 ~ 右移

步骤3. 将谓词公式中的量词左移（使用量词分配等值式、量词辖域收缩与扩张等值式），必要时将变项改名

3.6谓词逻辑的推理

- （**基本推理公式**）以下蕴含式都是普遍有效公式
  - $(\forall x)P(x)\lor(\forall x)Q(x)\Rightarrow(\forall x)(P(x)\lor Q(x))$
  - $(\exists x)(P(x)\land Q(x))\Rightarrow(\exists x)P(x)\land(\exists x)Q(x)$
  - $(\forall x)(P(x)\Rightarrow Q(x))\Rightarrow((\forall x)P(x)\Rightarrow(\forall x)Q(x))$
  - $(\forall x)(P(x)\Rightarrow Q(x))\Rightarrow((\exists x)P(x)\Rightarrow(\exists x)Q(x))$
  - $(\forall x)(\forall y)P(x, y)\Rightarrow(\exists x)(\forall y)P(x, y)$
  - $(\exists x)(\forall y)P(x, y)\Rightarrow(\forall y)(\exists x)P(x, y)$
  - $(\forall x)(\exists y)P(x, y)\Rightarrow(\exists x)(\exists y)P(x, y)$

- 而所使用的推理规则除**命题逻辑**的推理演算中用到的几条**基本推理规则**外，还包括四条有关量词的消去和引入规则：
  - 全称推广规则/全称量词引入规则(UG)
  - 全称举例规则/全称量词消去规则(US)
  - 存在推广规则/存在量词引入规则(EG)
  - 存在举例规则/存在量词消去规则(ES)

□全称量词消去规则：

$$\forall x\ P(x) \Rightarrow P(y) \text{ 或 } \forall x\ P(x) \Rightarrow P(a)$$

其中 y 是论域中一个体

□意指如果所有的 $x \in D$ 都具有性质 P，那么 D 中任一个体 y 必具有性质 P

□该规则使用的条件是：

- ■(1) 第一式中，取代 x 的 y 应为任意的不在 $P(x)$中约束出现的个体变项
- ■(2) 第二式中，a 为任意个体常项
- ■(3) 用 y 或 a 去取代 $P(x)$ 中自由出现的 x 时，必须在 x 自由出现的一切地方进行取代

□全称量词引入规则：

$$P(y) \Rightarrow (\forall x)P(x),$$

□其中 y 是论域中任一个体。意指如果任一个个体 $y \in D$ 都具有性质 P，那么 D 中所有个体 x 都具有性质 P。

□该规则使用的条件是：

- ■(1) 无论 $P(y)$ 中自由出现的个体变项 y 取何值，$P(y)$ 应该均为真。
- ■(2) 取代自由出现的 y 的 x 不能在 $P(y)$ 中约束出现。

□存在量词引入规则：

$$P(a) \Rightarrow (\exists x)P(x),$$

□其中 a 是论域中一个体常项。意指如果有个体常项 a 具有性质 P，那么 $(\exists x)P(x)$ 必真。

□该规则使用的条件是：

- ■(1) a 是特定的个体常项
- ■(2) 取代 a 的 x 不在 $P(a)$ 中出现过

□存在量词消去规则：

$$(\exists x)P(x) \Rightarrow P(a),$$

□其中 ***a*** 是论域中的一个个体常项。意指如果论域 ***D*** 中存在某个体具有性质 ***P***，那么必有特定个体 ***a*** 具有该性质 ***P***。

□该规则使用的条件是：

- (1) ***a*** 是使 ***P*** 为真的特定的个体常项
- (2) ***a*** 不在 ***P*(*x*)** 中出现
- (3) ***P*(*x*)** 中没有其它自由出现的个体变项
- (4) ***a*** 是在推导中未曾使用过的

先消去存在量词，再消去全称量词

□使用推理规则的推理演算过程是：

- **步骤1.** 首先将以自然语句表示的推理问题形式化，转换为谓词公式
- **步骤2.** 若不能直接使用基本的推理公式则消去量词
- **步骤3.** 在无量词下使用规则和公式进行推理
- **步骤4.** 最后再引入量词，得到相应结论

□特别注意如下两点：

(1) 在既需要消去存在量词又需要消去全称量词时，一般要先使用存在量词消去规则，再使用全称量词消去规则。

(2) 使用US，UG，ES，EG规则时，量词的辖域都必须延伸到整个公式的末端。

换言之，在含有多个量词的谓词推理中，使用消去规则应该按照从左到右的顺序，而引入规则的使用应该按照从右到左的顺序。

4.二元关系

4.1关系及其表示

1.有序对与笛卡儿积

有序对定义

□由两个对象 ***a*, *b*** 按照一定次序组成的二元组称为一个**有序对**或**序偶（ordered pair）**，记作 **(*a*, *b*)**，其中 ***a*** 是它的**第一元素**或**第一座标**，***b*** 是它的**第二元素**或**第二座标**。

- $(a, b) = (c, d)$ 当且仅当 $a = c$ 且 $b = d$

笛卡尔积定义

□设 A、B 为两个集合，定义它们的**笛卡尔积（Cartesian product）**$A\times B$ 为

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

□它也称作**直积（direct product）**。

■$A\times\varnothing = \varnothing\times B = \varnothing$

■一般来讲 $A\times B \neq B\times A$

2.二元关系

二元关系定义

□假设 A、B 是集合，$A\times B$ 的子集 R 称为**A到B的一个二元关系**，简称为**关系（relation）**。

□若 $R\subseteq A\times B$，当 $(a, b)\in R$ 时，称 **a与b具有关系R（a is related to b by R）**，记为aRb；

□若 $(a, b)\notin R$，则称 **a, b** 不具有关系 **R**，记为 **$a\not{R}b$**。

□如果 $A=B$ 则称 R 为 **A上的一个二元关系**。

恒等关系

□假设 A 是任一个集合，则可定义 A 上的**恒等关系（equality relation）**为：$I_A = \{ (a, a) \mid a\in A \}$。

□即 $(a, b)\in I_A$ 当且仅当 $a = b$。

定义域与值域

□假设 A、B 是集合，$R\subseteq A\times B$ 是 A 到 B 的一个二元关系，

□R 的**定义域（domain）**为集合

$$\text{Dom}(R) = \{ a \mid a\in A,\ \text{存在 } b\in B \text{ 使得 } (a, b)\in R \},$$

即R中所有有序对的第一元素构成的集合；

□R 的**值域（range）**为集合

$$\text{Ran}(R) = \{ b \mid b\in B,\ \text{存在 } a\in A \text{ 使得 } (a, b)\in R \},$$

即R中所有有序对的第二元素构成的集合。

像集

- 假设 A、B 是集合，$R \subseteq A \times B$ 是 A 到 B 的一个二元关系，
- 对于 A 中任一元素 x，可定义 x 的**像集(image)**为

  $R(x) = \{ y \in B \mid xRy \}$；
- 对于A的任一子集A_1，可定义A_1的**像集**为

  $R(A_1) = \{ y \in B \mid xRy$ 对某 $x \in A_1$ 成立$\}$，

且定义 $R(\varnothing)=\varnothing$。

3.二元关系的表示形式

- 二元关系主要具有以下三种表示方法
  - 笛卡尔积的子集
    - 有序对的集合
  - 关系矩阵
  - 有向图表示

关系矩阵

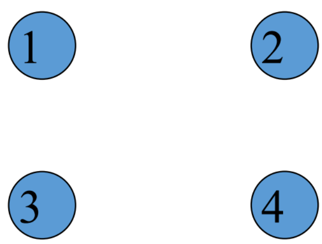
- 设 $A = \{a_1, a_2, \ldots, a_m\}$，$B = \{b_1, b_2, \ldots, b_n\}$，$R$ 是从 A 到 B 的关系，
- 定义 R 的关系矩阵为一个 $m \times n$ 的布尔矩阵 $\mathbf{M}_R = [r_{ij}]_{m \times n}$，其中

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

关系图

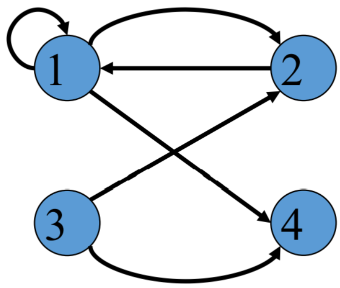
- 对 A 中每个元素，画一个圆形，并在圆形之中标明该元素。
- 此称之为关系图的**顶点（vertice）**

- $A=\{ 1, 2, 3, 4 \}$
- $R=\{ (1,1), (1,2), (1,4), (2,1), (3,2), (3,4) \}$



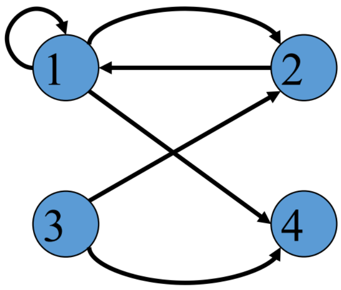
□若 $(a_i, a_j)\in R$，则从顶点 a_i 向顶点 a_j 画一个箭头，称为**有向边**或简称**边（edge）**，若 $a_i=a_j$ 则称这条边为**自环（cycle）**。

- $A=\{1,2,3,4\}$
- $R=\{$ (1,1), (1,2), (1,4), (2,1), (3,2), (3,4) $\}$



□得到的图表示称作关系 R 的**关系图（directed graph，**或**digraph）**。

- $A=\{1,2,3,4\}$
- $R=\{$ (1,1), (1,2), (1,4), (2,1), (3,2), (3,4) $\}$



4.2关系的运算

1.关系的基本运算

交，并，补

□R 与 S 的**交（intersection）**关系 $R\cap S$ 定义为:

$(a, b)\in R\cap S$ 当且仅当 $(a, b)\in R$ 且 $(a, b)\in S$;

□R 与 S 的**并（union）关系** $R\cup S$ 定义为:

$(a, b)\in R\cup S$ 当且仅当 $(a, b)\in R$ 或 $(a, b)\in S$;

□R 的**补（complement）**关系 R 定义为；

$a\overline{R}b$ 当且仅当 $a\not{R}b$

逆

□假设 A、B 是两个集合，R 为 A 到 B 的关系，则 R 的**逆（inverse）关系** 定义为

$$R^{-1}=\{(b, a)|b\in B, a\in A , (a, b)\in R\}\subseteq B\times A。$$

□简言之，R 的逆关系是由将 R 中每个有序对的元素顺序交换构成的。

左复合

□假设 A、B、C 是集合，R 为 A 到 B 的关系，S 为 B 到 C 的关系，则 $S\circ R$ 表示 A 到 C 的一个关系

$$S\circ R =\{(a, c) \mid a\in A, c\in C, \text{存在 } b\in B \text{ 使得 } (a, b)\in R \text{ 且 } (b, c)\in S \},$$

称为 R 和 S 的**复合（composition）关系**或**合成关系**。

关系运算的性质（7个定理）

定理1

□定理1

假设 A、B 是集合，R、S 为 A 到 B 的关系，则：

■$\mathrm{Dom}(R^{-1}) = \mathrm{Ran}(R)$，$\mathrm{Dom}(R) = \mathrm{Ran}(R^{-1})$；

■$\overline{\overline{R}} = R$;

■$(R^{-1})^{-1} = R$；

■$\overline{R^{-1}} = (\overline{R})^{-1}$;

■$(R\cap S)^{-1} = R^{-1}\cap S^{-1}$ 且 $(R\cup S)^{-1} = R^{-1}\cup S^{-1}$。

■$\overline{R\cap S} = \overline{R}\cup\overline{S}$ 且 $\overline{R\cup S} = \overline{R}\cap\overline{S}$。

定理2

□定理2

假设 A、B、C、D 均为非空集合，R 为 A 到 B 的关系，S 为 B 到 C 的关系，T 为 C 到 D 的关系，则

$$T\circ(S\circ R) = (T\circ S)\circ R$$

定理3

□定理3

假设 A、B、C 为非空集合，R 为 A 到 B 的关系，S 为 B 到 C 的关系，则

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

定理4

□定理4

假设 A、B、C 是集合，R、S 为 A 到 B 的关系，

- 若 $R\subseteq S$，则 $R^{-1}\subseteq S^{-1}$；
- 若 $R\subseteq S$，则 $\overline{S}\subseteq\overline{R}$。

定理5

□定理5

假设 A、B、C 为集合，R_1、R_2 为 A 到 B 的关系，S_1、S_2 为 B 到 C 的关系，$R_1\subseteq R_2$，$S_1\subseteq S_2$，则 $S_1\circ R_1\subseteq S_2\circ R_2$。

定理6

□定理6

假设 A、B、C、D 为集合，R 为 A 到 B 的关系，S_1、S_2 为 B 到 C 的关系，T 为 C 到 D 的关系，则：

- $(S_1\cup S_2)\circ R = (S_1\circ R)\cup(S_2\circ R)$
- $(S_1\cap S_2)\circ R \subseteq (S_1\circ R)\cap(S_2\circ R)$
- $T\circ(S_1\cup S_2) = (T\circ S_1)\cup(T\circ S_2)$
- $T\circ(S_1\cap S_2) \subseteq (T\circ S_1)\cap(T\circ S_2)$

定理7

□定理7

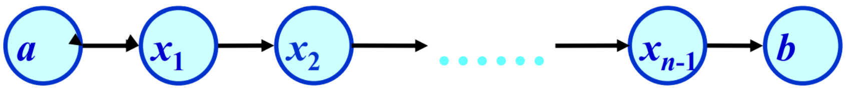
假设 A、B、C 为集合，R 为 A 到 B 的关系，S 为 B 到 C 的关系，则对于 A 的任意子集 A_1 有：

$$(S\circ R)(A_1) = S(R(A_1))\ 。$$

2.关系的幂和道路

道路

- 假设 A 为集合，$a, b \in A$，集合 A 上关系 R 中从 a 到 b **长为 n 的道路（path）**是指 A 上有限序列 $\pi: a, x_1, x_2, \ldots x_{n-1}, b$，满足：
  - $a\ R\ x_1$
  - $x_i\ R\ x_{i+1}$，$1 \le i \le n-2$
  - $x_{n-1}\ R\ b$
- 注：长度为n的道路包含n+1个顶点（允许重复）。



- 假设 A 为集合，$a, b \in A$，集合 A 上关系 R 中从 a 到 b 的一条**道路（path）**是指 A 上有限序列 $\pi: a, x_1, x_2, \ldots x_{n-1}, b$，
- 其中 $n>0$ 称为该道路的**长度（length）**，
- a 称作道路的**起点**，b 称作道路的**终点**。

- 设 R 为集合 A 上的关系
- 定义 A 上的关系 R^n 为：
  - $a, b \in A$，则 $a\ R^n\ b$ 当且仅当存在 R 中从 a 到 b 长为 n 的道路
- 定义 A 上的关系 R^∞ 为：
  - $a, b \in A$，则 $a\ R^\infty\ b$ 当且仅当存在 R 中从 a 到 b 的道路

- 设 R 为集合 A 上的关系，n 为自然数
- 则 R 的 **n 次幂（power）**R^n 可递归地定义为
  - $R^0 = I_A$
  - $R^n = R^{n-1} \circ R$，n=1, 2, 3, ...
- 与之前的定义**等价**

- 设 R 为有限集合 A 上的关系，n 为自然数，则
  - $M_{R^2} = M_R \odot M_R$
  - $M_{R^n} = M_R \odot M_R \ldots \odot M_R$ (n个R的复合)

    也记作 $(M_R)_\odot{}^n$

□定理：

设 R 为集合 A 上的关系，则

$$R^{\infty} = R \cup R^2 \cup R^3 \cup \ldots\ldots,$$

即

$$\mathbf{M}_{R^{\infty}} = \mathbf{M}_R \vee \mathbf{M}_{R^2} \vee \mathbf{M}_{R^3} \vee \ldots$$
$$= \mathbf{M}_R \vee (\mathbf{M}_R)_{\odot}^{2} \vee (\mathbf{M}_R)_{\odot}^{3} \ldots$$

4.3关系的性质

1.关系性质的定义和判断

自反

□① 假设 R 为集合 A 上的关系，

- ■如果 $(a, a) \in R$ 对于所有 $a \in A$ 成立，则称 R 是自反的（reflexive），或称 R 满足自反性；
- ■如果 $(a, a) \notin R$ 对于所有 $a \in A$ 成立，则称 R 是非自反的（irreflexive），或称 R 满足非自反性。

	关系矩阵的特点	关系图的特点
自反关系 $\forall a\ (a, a) \in R$	主对角线元素全是1，即对于所有 i，$\mathbf{M}_R(i, i) = 1$	每个顶点都有自环
非自反关系 $\forall a\ (a, a) \notin R$	主对角线元素全是0，即对于所有 i，$\mathbf{M}_R(i, i) = 0$	每个顶点都无自环

对称

□② 假设 R 为集合 A 上的关系，

- ■如果对于任意 $a, b \in A$，若 $(a, b) \in R$ 必然有 $(b, a) \in R$，则称 R 是对称的（symmetric），或称 R 满足对称性；
- ■如果对于任意 $a, b \in A$，若 $(a, b) \in R$ 必然有 $(b, a) \notin R$，则称 R 是非对称的（asymmetric），或称 R 满足非对称性；
- ■如果对于任意 $a, b \in A$，若 $(a, b) \in R$ 且 $(b, a) \in R$ 必然有 $a = b$，则称 R 是反对称的（antisymmetric），或称 R 满足反对称性。

	关系矩阵的特点	关系图的特点
对称关系	矩阵是对称矩阵，即 对于所有i, j，$\mathbf{M}_R(i, j)=\mathbf{M}_R(j, i)$	如果两个顶点之间有边， 一定是一对方向相反的边
非对称关系	对于所有i, j， 若$\mathbf{M}_R(i, j)=1$则 $\mathbf{M}_R(j, i)=0$	两顶点之间至多存在一条 有向边，每个顶点都无自环
反对称关系	对于所有i, j， 若$i\neq j$且$\mathbf{M}_R(i, j)=1$则$\mathbf{M}_R(j, i)=0$	两互异顶点之间至多存在 一条有向边，允许存在自环

传递

- ③ 假设 R 为集合 A 上的关系，
  - 如果对于任意 $a, b, c\in A$，若 $(a, b)\in R$ 且 $(b, c)\in R$ 必然有 $(a, c)\in R$，则称 R 是**传递的（transitive）**，或称 R 满足传递性。

- 保留对称关系的有向图中的顶点，且将所有有向边改作无向边，其结果称作该关系的**图（graph）**。

	关系矩阵的特点	关系图的特点
传递关系	对于所有 i, j, 若$(\mathbf{M}_R \odot \mathbf{M}_R)(i, j) = 1$ 则 $\mathbf{M}_R(i, j) = 0$	如果存在有向边 (i, j) 和 (j, k)，则存在 有向边 (i, k)

关系判断

- 定理 设 R 为集合 A 上的关系，则
  - R 具有对称性当且仅当 $R = R^{-1}$
  - R 具有非对称性当且仅当 $R\cap R^{-1} = \varnothing$
  - R 具有反对称性当且仅当 $R\cap R^{-1} \subseteq I_A$
- 定理 设 R 为集合 A 上的关系，则
  - R 具有自反性当且仅当 $I_A\subseteq R$
  - R 具有非自反性当且仅当 $R\cap I_A = \varnothing$

- 定理 设 R 为集合 A 上的关系，则
  - R 具有传递性当且仅当 $R^2 \subseteq R$
  - R 具有传递性当且仅当对于所有 $n \geq 1$，$R^n \subseteq R$ 成立。
    - （充分性——令 $n=2$）
    - （必要性——对 n 进行归纳即可证明）

自反关系	$I_A \subseteq R$
非自反关系	$R \cap I_A = \varnothing$
对称关系	$R = R^{-1}$
非对称关系	$R \cap R^{-1} = \varnothing$
反对称关系	$R \cap R^{-1} \subseteq I_A$
传递关系	$R^2 \subseteq R$；或者 $R^n \subseteq R$ 对所有 $n \geq 1$成立

2.关系运算对性质的保持

- 定理1

设 R 和 S 为集合 A 上的关系，则

(a) 若 R 是自反的，那么 R^{-1} 也是自反的；

(b) 若 R 和 S 都是自反的，那么 $R \cap S$，$R \cup S$ 及 $S \circ R$ 都是自反的；

(c) R 是自反的当且仅当 $\overline{R}$ 是非自反的。

- 定理2

设 R 和 S 为集合 A 上的关系，则

(a) 若 R 是对称的，那么 R^{-1} 和 R 也是对称的

(b) 若 R 是对称的，那么 R^n 也是对称的

(c) 若 R 和 S 都是对称的，那么 $R \cap S$ 和 $R \cup S$ 也是对称的。

- 定理3

设 R 和 S 为集合 A 上的关系，则

(a) $(R \cap S)^2 \subseteq R^2 \cap S^2$

(b) 若 R 是传递的，那么 R^{-1} 也是传递的

(c) 若 R 和 S 都是传递的，那么 $R \cap S$ 也是传递的

如果 R 和 S 具有如下性质	那么				
	$\overline{R}$	R^{-1}	$R\cap S$	$R\cup S$	$S\circ R$
自反性	具有非自反性	✓	✓	✓	✓
非自反性	具有自反性	✓	✓	✓	?
对称性	✓	✓	✓	✓	?
反对称性	?	✓	✓	?	?
传递性	?	✓	✓	?	?

4.4关系的闭包

- R_1 称作 R 的关于某特定性质的**闭包**，如果
  - ① R_1 包含 R；
  - ② R_1 具有所希望的性质；且
  - ③ R_1 是 A 上满足①和②的最小关系。
    - 若 A 上的关系 S 也满足①和②则必然有 $R_1\subseteq S$。

- 一般将关系 R 的
  - **自反闭包**记作 $r(R)$
  - **对称闭包**记作 $s(R)$
  - **传递闭包**记作 $t(R)$

1.自反闭包

- 设 R 是集合 A 上的一个关系，则
- R 的自反闭包是 $R\cup I_A$。

① $R\subseteq R\cup I_A$。

② $R\cup I_A$ 具有自反性——由于 $I_A\subseteq R\cup I_A$。

③ 若 $R\subseteq S$ 且 S 是自反的，

则 $I_A\subseteq S$

于是 $R\cup I_A\subseteq S$。

2.对称闭包

- 设 R 是集合 A 上的一个关系，则
- R 的对称闭包是 $R\cup R^{-1}$。
  - ① $R\subseteq R\cup R^{-1}$
  - ② $(R\cup R^{-1})^{-1}=(R)^{-1}\cup(R^{-1})^{-1}=R^{-1}\cup R$
    $=R\cup R^{-1}$。
  - ③ 若 S 具有对称性，且 $R\subseteq S$，则
    - 由 S 是对称的，有 $S=S^{-1}$。
    - 由 $R\subseteq S$，得到 $R^{-1}\subseteq S^{-1}$。

  因此 $R\cup R^{-1}\subseteq S\cup S^{-1}=S$

  $R\cup R^{-1}\subseteq S$。

3.传递闭包

- 定理

设 R 为集合 A 上的任意二元关系，则 R^{∞} 是 R 的传递闭包。

4.沃舍尔算法

```
C ← M_R
for k = 1 to n
  for i = 1 to n
    for j = 1 to n
      C[i, j] ← C[i, j]∨(C[i, k]∧C[k, j] )
```

$2\times n^3$

新知识：Warshall算法纸上作业法

- 第k次
  - 第k行为1元素所在列画纵向直线，
  - 第k列为1元素所在行画横向直线，
  - 直线相交位置如果为0，则改为1。

5.关系闭包运算的性质

- 定理1

假设 R 是集合 A 上的关系，则
  - R 是自反的当且仅当 $r(R)=R$
  - R 是对称的当且仅当 $s(R)=R$
  - R 是传递的当且仅当 $t(R)=R$

□定理2

假设 R, S 是集合 A 上的关系且 $R \subseteq S$，则

(a) $r(R) \subseteq r(S)$

(b) $s(R) \subseteq s(S)$

(c) $t(R) \subseteq t(S)$

□定理3

假设 R 是集合 A 上的关系，则

(a) 如果 R 是自反的，那么 $s(R)$ 和 $t(R)$ 都是自反的

(b) 如果 R 是对称的，那么 $r(R)$ 和 $t(R)$ 都是对称的

(c) 如果 R 是传递的，那么 $r(R)$ 是传递的。

□定理4

设 R 是集合 A 上任一二元关系，则

(a) $r(s(R)) = s(r(R))$

(b) $r(t(R)) = t(r(R))$

(c) $t(s(R)) \supseteq s(t(R))$

4.5等价关系和集合的划分

1.等价关系、等价类和商集

等价关系

□假设 R 是非空集合 A 上的关系，如果 R 是自反的、对称的和传递的，则称 R 是 A 上的**等价关系（equivalence relation）**。

等价类和商集

□假设 R 是非空集合 A 上的等价关系，元素 $a \in A$，集合 $R(a)$ 称为 a 所在的**等价类（equivalence class）**，也记作 $[a]_R$ 或 $[a]$。

□集合 $\{R(a) | a \in A\}$ 称作 A 关于 R 的**商集（quotient sets）**，记作 A/R；a 称作 $R(a)$ 的**代表元**。

□定理

设 R 是 A 上的一个等价关系，$a, b \in A$，则 aRb 当且仅当 $R(a)=R(b)$。

□定理

假设 A两个集合，R、S 为集合 A 上的两个等价关系，则 $R\cap S$ 也是等价关系。

（为什么？）

□但一般来讲 $R\cup S$ 不一定也是等价关系。

（为什么？）

□定理

假设 R、S 为集合 A 上的等价关系，则包含 $R\cup S$ 的最小等价关系为 $(R\cup S)^{\infty}$

2.集合的划分

□集合 A 的非空子集的集合 $\mathscr{P}$称作 A 的一个划分或者商集，如果

- ■1. A 中的每一个元素都包含于 $\mathscr{P}$中的一个元素；
- ■2. 若 A_1 和 A_2 是 $\mathscr{P}$中的相异元素，则必然有 $A_1\cap A_2=\varnothing$。

□ $\mathscr{P}$ 中的元素称作这个划分的划分块。

- 假设 A 是整数集的任一子集，n 是一个大于1的正整数
- 则可以根据模 n 的余数对 A 进行划分

3.等价关系与划分的一一对应

由划分构造等价关系

□定理

设 $\mathscr{P}$ 是集合 A 的一个划分，定义 A 上的关系 R 为：

aRb 当且仅当 a 和 b 属于同一个划分块。

则 R 是 A 上的一个等价关系。

□定理

设 R 是 A 上的一个等价关系，则

$\mathscr{P} = A/R = \{ R(a) \mid a\in A \}$ 是 A 的一个划分，

而且 R 就恰是由 $\mathscr{P}$ 决定的等价关系。

- 定理的证明：

  而且由引理知，aRb 当且仅当 a, b 属于 $\mathscr{P} = A/R = \{ R(a) \mid a \in A \}$ 的同一个划分块，因此 $\mathscr{P}$ 决定的等价关系就是 R 。

- 由划分与等价关系的一一对应，可得：
- 定理

  设 R_1 和 R_2 为非空集合 A 上的等价关系，则 $R_1 = R_2$ 当且仅当 $A/R_1 = A/R_2$ 。

5.函数

5.1函数的定义

函数

- A 和 B 为非空集合
- 设 f 为 A 到 B 的二元关系，若对于任意$x \in \mathrm{Dom}(f)$ 都存在唯一的 $y \in \mathrm{Ran}(f)$ 使得 $(x, y) \in f$ 成立，则称 f 为**函数 (function)**。
- 函数也称作**映射（mapping）**或**变换（transformation）**

- 假设A 到 B 的二元关系 f 为函数
- 如果 $a \notin \mathrm{Dom}(f)$，那么 $f(a) = \varnothing$
- 如果 $f(a) = \{b\}$，习惯上使用元素 b 来表示集合 $\{b\}$ 并且写作 $f(a) = b$
- f可以被描述为有序对的集合 $\{(a, f(a)) \mid a \in \mathrm{Dom}(f)\}$

- 假设A 到 B 的二元关系 f 为函数
- $y = f(x)$ 中，x 称为**自变量（argument）**，y 为 **f 在 x 的值（value）**或 **x 在 f 作用下的像（image）**。

- 设 A、B 是非空集合，f 是 A 到 B 的一个关系，如果对每个 $x \in A$，存在唯一的 $y \in B$，使得 $(x, y) \in f$，则称 f 为**A到B的函数**，记作 $f: A \to B$。
- 对于 A 到 B 的函数 f，

  $\mathrm{Dom}(f) = A$，$\mathrm{Ran}(f) \subseteq B$。

- 例 　　　　A到B的函数？
  - $A=B=\mathbb{R}$
  - $f(x)=x+1$ ✓
  - $f(x)=\sqrt{x}$ ✗
  - $f(x)=\dfrac{1}{x}$ ✗

定义域与值域要相同

□设 A 是一个任意非空集合. A 上的恒等函数表示为1_A，其定义为 $1_A(a)=a$

5.2函数的性质

□设函数 $f: A\to B$，

- ■若 $\mathrm{Ran}(f)=B$，则称 f 是满射 （**surjection**）或映上的（**onto**）；
- ■若任意 $y\in\mathrm{Ran}(f)$ 都存在唯一的 $x\in A$ 使得 $f(x)=y$，则称 $f: A\to B$ 是单射 （**injection**）或一一的（**one-to-one**）；
- ■若 f 既是满射又是单射，则称 f 是双射（**bijection**）或一一对应（**one-to-one correspondence**）。

□f 是满射意味着：对于任意 $y\in B$，都存在 $x\in A$ 使得 $f(x)=y$

□f 是单射另有如下两个等价定义：

- ■对于任意 $a, b\in A$ 满足 $a\neq b$ ，均有$f(a)\neq f(b)$
- ■如果 $a, b\in A$ 满足 $f(a)=f(b)$，则 $a=b$

□定理

假设 A 和 B 是两个有限集合且满足 $|A|=|B|$，则函数 $f: A\to B$ 是单射当且仅当 f 是满射。

□定理

假设 A 和 B 都是有限集合，则：

(a) 若 $|A|<|B|$，则必然存在从 A 到 B 的单射函数、必然不存在从 A 到 B 的满射函数；

(b) 若 $|A|>|B|$，则必然存在从 A 到 B 的满射函数、必然不存在从 A 到 B 的单射函数；

(c) 若 $|A|=|B|$，则必然存在从 A 到 B 的双射函数。

□推论

假设 A 是有限集合，B 是无限集合，则：

- (a) 必然不存在从 A 到 B 的满射函数
- (b) 必然不存在从 B 到 A 的单射函数

5.3函数的复合

□定理1

设 A, B, C 是集合，f 是 A 到 B 的关系，g 是 B 到 C 的关系。若 f, g 是函数，则：

- $g \circ f$ 也是函数，且满足
- $\mathrm{Dom}(g \circ f) = \{ x \mid x \in \mathrm{Dom}(f)$ 且 $f(x) \in \mathrm{Dom}(g) \}$
- 对于任意 $x \in \mathrm{Dom}(g \circ f)$ 有 $g \circ f(x) = g(f(x))$

□定理2

假设 A、B、C 为非空集合，函数 $f: A \rightarrow B, g: B \rightarrow C$，则

(a)如果 g 和 f 都是满射，则 $g \circ f$ 也是满射

(b)如果 g 和 f 都是单射，则 $g \circ f$ 也是单射

(c)如果 g 和 f 都是双射，则 $g \circ f$ 也是双射

□定理3

假设 A、B、C 为非空集合，函数 $f: A \rightarrow B, g: B \rightarrow C$，则

(a)若 $g \circ f$ 是单射，则 f 是单射

(b)若 $g \circ f$ 是满射，则 g 是满射

(c)若 $g \circ f$ 是双射，则 f 是单射，g 是满射

□定理4

假设 A、B 为集合，函数 $f: A\to B$，则 $f = f\circ 1_A = 1_B\circ f$。

5.4逆函数

逆函数

□假设 A、B 为集合，如果函数 $f: A\to B$ 作为关系的逆关系 f^{-1} 是 B 到 A 的函数，则称之为**可逆的（invertible）**，此时称 f^{-1} 为 f 的**反函数**或**逆函数（inverse function）**。

□定理

假设 A、B 为集合，设 $f: A\to B$，若函数 f^{-1} 存在则；

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

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

□下面一个定理给出了逆函数存在的充要条件：

□定理

假设 A、B 为非空集合，函数 $f: A\to B$，则

(a) f 可逆当且仅当 f 是双射

(b) f 的逆函数若存在则也是双射

□定理3

若函数 $f: A\to B$ 和 $g: B\to A$ 满足 $g\circ f=1_A$ 和 $f\circ g=1_B$，则 f 是一个 A 到 B 的双射，g 是一个 B 到 A 的双射，而且 f 和 g 互为逆函数。

5.5计算机科学中的常用函数

特征函数

□设 U 为全集，对于任意集合 $A\subseteq U$，可定义 A 的**特征函数（characteristic function）** $\chi_A: U\to\{0,1\}$ 为

$$\chi_A(x)=\begin{cases} 1 & \text{If } x\in A \\ 0 & \text{If } x\notin A. \end{cases}$$

地板函数和天花板函数

- 定义在ℝ上的**地板函数（floor function）**，也称作**下取整函数**或者**高斯函数**，其值是不超过自变量 x 的最大整数，记作 floor(x) 或 $\lfloor x \rfloor$
- 定义在ℝ上的**天花板函数（ceiling function）**，也称作**上取整函数**，其值是不小于 x 的最小整数，记做 ceiling(x) 或 $\lceil x \rceil$

6.偏序关系

6.1 偏序关系和偏序集

1.偏序关系和偏序集的定义与性质

假设 R 是集合 A 上的关系，如果R是自反的、反对称的 和传递的，则称 R 是 A 上的一个偏序（partial order） 或半序（semi order）关系，一般简记作"≤"或"≥"。
集合 A 和偏序关系 R 构成的有序二元组 (A, R)称作偏序 集（partially ordered set，简记为poset）或半序集 （semi ordered set)

- 假设 (A, R) 为偏序集，$a, b \in A$，如果有 $a \leq b$ 或 $b \leq a$ 成立，则称 a, b 是**可比的（comparable）**，否则称 a, b 是**不可比的（incomparable）**。

- 假设 (A, R) 为偏序集，如果对于任意 $a, b \in A$，a, b 都是可比的，则
  - 称 R 为**线序（linear order）**或**全序（total order）**，
  - (A, R) 称作**线序集（linearly ordered set）**或**全序集（totally ordered set）**，也称为**链（chain）**。

- 那么 R^{-1} 也是 A 上的偏序关系，称之为 R 的**对偶（dual）**。
- 偏序集 (A, R^{-1}) 称做偏序集 (A, R) 的**对偶**。

拟序

拟序关系

- 假设 R 是集合 A 上的关系，如果 R 是非自反的和传递的，则称 R 是 A 上的一个**拟序（quasiorder）**关系，一般简记作"<"或">"。

□定理

假设 R 是集合 A 上的关系，如果R 是非自反和传递的，则 R 一定是非对称的。

□定理

假设 R 是集合 A 上的关系，

(a) 如果 R 是一拟序关系，那么 $r(R) = R \cup I_A$ 是一偏序关系；

(b) 如果 R 是一偏序关系，那么 $R - I_A$ 是一拟序关系。

2.积偏序和字典序

□定理

假设 $(A, \leq_1)$ 和 $(B, \leq_2)$ 是两个偏序集，则可以定义在 $A \times B$ 上的偏序关系 $\leq$ 为：

$$(a, b) \leq (a', b') \text{ 当且仅当 } a \leq_1 a' \text{ 且 } b \leq_2 b',$$

称之为**积偏序（product partial order）**。

□假设 $(A, \leq_1)$ 和 $(B, \leq_2)$ 是两个偏序集，则可以在 $A \times B$ 上定义偏序关系 $\prec$为：

$$(a, b) \prec (a', b')$$

$$\text{当且仅当 } a <_1 a'，\text{或者 } a = a' \text{ 且 } b \leq_2 b',$$

称之为**词典序（lexicographic order）**或**字典序（dictionary order）**。

3.哈斯图

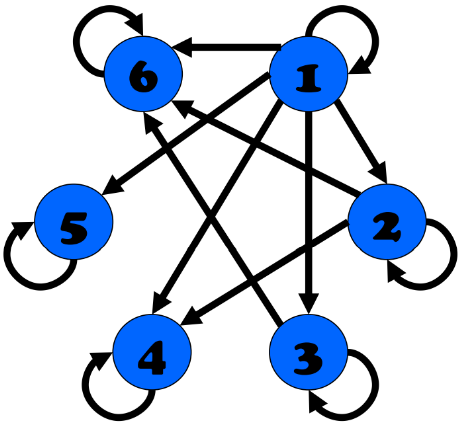
□定理：

■假设 $(A, \leq)$ 是偏序集，则在拟序集 $(A, <)$ 中不存在长度大于1的圈。

哈斯图画法

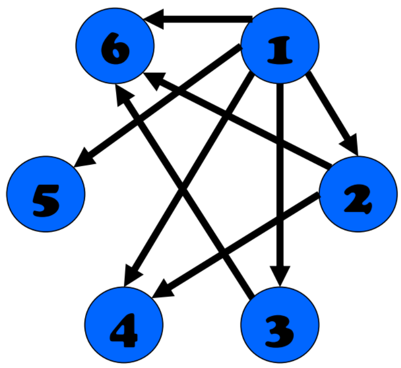
哈斯图画法

- 第1步： 删除自环
  - 由于一定具有自反性



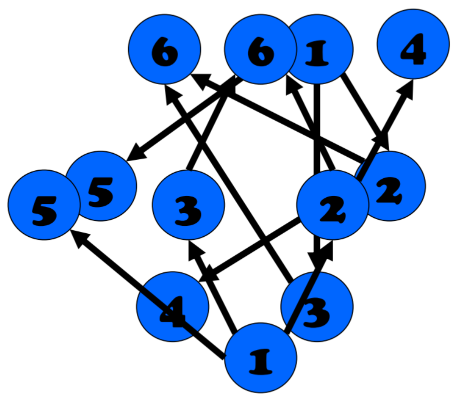
哈斯图画法

- 第2步：若 ***aDb*** 且不存在 ***c*** 使得 ***aDc*** 且***cDb***，则保留有向边 **(*a*, *b*)**
  - 由于一定具有传递性



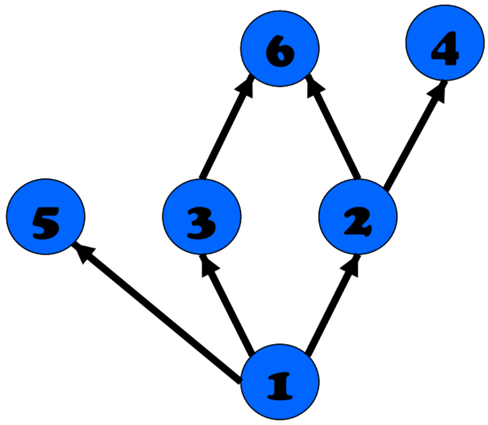
哈斯图画法

- 第 3 步: 重新组织各个顶点的位置，使得各个有向边的方向都朝向上方或斜上方
  - 由定理，不存在长度大于**1**的回路



◻哈斯图画法

- 第 4 步： 忽略“箭头”



◻哈斯图画法

- 第 5 步: 把所有的顶点替换成点