离散数学复习

郝杰

haojie@bupt.edu.cn

北京邮电大学信息安全中心

考试内容

第一部分 数理逻辑

第一章 命题逻辑（1.6节不考）

第二章 一阶逻辑

第二部分 集合论

第三章 集合的基本概念和运算

第四章 二元关系和函数

第三部分 图论

第五章 图的基本概念

第六章 特殊的图（不考）

第三部分 代数系统（不考）

第1章 命题逻辑

1.1 命题符号化及联结词

1.2 命题公式及分类

1.3 等值演算

1.4 范式

1.5 联结词全功能集

1.7 推理理论

命题逻辑

命题(Proposition): 判断结果惟一的陈述句。

命题的真值： 命题的判断结果--真或假(1或0)

- 简单命题：简单陈述句构成的，不能再被继续分割的命题（不含任何联结词）.
- 复合命题：由一个或几个简单命题通过联结词(connectives)按一定规则复合而成的新的命题。

用已有命题产生新命题

- 5个常用联结词:
  - 否定联结词（非， ¬ ）
  - 合取联结词（与， ∧ ）
  - 析取联结词（或， ∨ ）
  - 蕴涵联结词（如果…，则… ， → ）
  - 等价联结词（当且仅当，↔ ）

- 命题符号化

- 五种最基本、最常用的联结词组成的集合

  $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$，

  称为一个联结词集。其中 $\neg$ 为一元联结词，其余的都是二元联结词。

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$
0	0	1	0	0	1	1
0	1	1	0	1	1	0
1	0	0	0	1	0	0
1	1	0	1	1	1	1

命题公式

定义 命题公式

(1) 单个命题常项或变项 $p, q, r, \ldots, p_i, q_i, r_i, \ldots, 0, 1$是命题公式；

(2) 若 A 是命题公式，则 $(\neg A)$ 也是命题公式；

(3) 若 A, B是命题公式，则 $(A\wedge B), (A\vee B), (A\to B), (A\leftrightarrow B)$也是命题公式；

(4) 只有有限次地应用(1)~(3)形成的符号串才是命题公式。

定义 赋值或解释

- 设 A 为一命题公式， $p_1, p_2, \ldots, p_n$是出现在 A 中的所有命题变项。给 $p_1, p_2, \ldots, p_n$各指定一个真值，称为对A 的一个赋值或解释。
- 若指定的一组值使 A 的真值为 1，则称这组值为 A 的成真赋值；若使 A 的真值为0，则称这组值为 A 的成假赋值。

真值表

定义 真值表

- 将命题公式 A 在所有赋值下的取值情况列成的表，称为 A 的真值表。

例：公式 $A=(q\to p)\wedge q\to p$ 的真值表

p q	$q\to p$	$(q\to p)\wedge q$	$(q\to p)\wedge q\to p$
0 0	1	0	1
0 1	0	0	1
1 0	1	0	1
1 1	1	1	1

命题公式的类型

北京邮电大学 Beijing University of Posts and Telecommunications

定义 重言式 矛盾式 可满足式

设A为一个命题公式

(1) 若A无成假赋值，则称A为重言式(也称永真式，tautology).

(2) 若A无成真赋值，则称A为矛盾式(也称永假式，contradiction).

(3) 若A不是矛盾式，则称A为可满足式(contingency).

注意：重言式是可满足式，但反之不真。

2元真值函数对应的真值表

例如：$p\to q$, $\neg p\vee q$, $(\neg p\vee q)\vee(\neg(p\to q)\wedge q)$ 等都对应表中的 $F_{13}^{(2)}$

p	q	$F_0^{(2)}$	$F_1^{(2)}$	$F_2^{(2)}$	$F_3^{(2)}$	$F_4^{(2)}$	$F_5^{(2)}$	$F_6^{(2)}$	$F_7^{(2)}$
0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1
p	q	$F_8^{(2)}$	$F_9^{(2)}$	$F_{10}^{(2)}$	$F_{11}^{(2)}$	$F_{12}^{(2)}$	$F_{13}^{(2)}$	$F_{14}^{(2)}$	$F_{15}^{(2)}$
0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1

等值

定义

- 给定两个命题公式 A和 B，设 $p_1, p_2, \ldots, p_n$为出现于 A 和 B 中的所有命题变项，则公式 A 和 B 都有 2^n 个赋值，若在任一赋值之下，公式 A 和 B 的真值都相同，则称 A 和 B 是等值的，记作 $A \Leftrightarrow B$.

定义

- 设 A, B 为两个命题公式，若等价式 $A \leftrightarrow B$ 为一个重言式，则称 A 和 B 是等值的，记作 $A \Leftrightarrow B$.

等值演算

等值演算:

由已知的等值式推演出新的等值式的过程

等值演算的基础:

(1) 等值关系的性质：自反、对称、传递

(2) 基本的等值式

(3) 置换规则

基本等值式

双重否定律: $\neg\neg A \Leftrightarrow A$

等幂律: $A\vee A \Leftrightarrow A$, $A\wedge A \Leftrightarrow A$

交换律: $A\vee B \Leftrightarrow B\vee A$, $A\wedge B \Leftrightarrow B\wedge A$

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

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

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

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

德·摩根律: $\neg(A\vee B) \Leftrightarrow \neg A\wedge\neg B$

$\neg(A\wedge B) \Leftrightarrow \neg A\vee\neg B$

吸收律: $A\vee(A\wedge B) \Leftrightarrow A$

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

零律: $A\vee 1 \Leftrightarrow 1$, $A\wedge 0 \Leftrightarrow 0$

同一律: $A\vee 0 \Leftrightarrow A$, $A\wedge 1 \Leftrightarrow A$

排中律: $A\vee\neg A \Leftrightarrow 1$

矛盾律: $A\wedge\neg A \Leftrightarrow 0$

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

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

假言易位: $A\rightarrow B \Leftrightarrow \neg B\rightarrow\neg A$

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

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

应用举例——证明两个公式等值

例1 证明 $p\rightarrow(q\rightarrow r) \Leftrightarrow (p\wedge q)\rightarrow r$

证 $p\rightarrow(q\rightarrow r)$

$\Leftrightarrow\neg p\vee(\neg q\vee r)$ （蕴涵等值式，置换规则）

$\Leftrightarrow(\neg p\vee\neg q)\vee r$ （结合律，置换规则）

$\Leftrightarrow\neg(p\wedge q)\vee r$ （德·摩根律，置换规则）

$\Leftrightarrow(p\wedge q) \rightarrow r$ （蕴涵等值式，置换规则）

说明:也可以从右边开始演算.

因为每一步都用置换规则，故可不写出.

熟练后，基本等值式也可以不写出.

应用举例——证明两个公式不等值

例2 证明: $p \to (q \to r) \not\Leftrightarrow (p \to q) \to r$

用等值演算不能直接证明两个公式不等值,证明两个公式不等值的基本思想是找到一个赋值使一个成真,另一个成假.

- 方法一 真值表法.
- 方法二 观察赋值法. 容易看出000, 010等是左边的成真赋值，是右边的成假赋值.
- 方法三 用等值演算先化简两个公式，再观察.

应用举例——判断公式类型

例3 用等值演算法判断下列公式的类型

(1) $q \wedge \neg(p \to q)$

解 $q \wedge \neg(p \to q)$

$\Leftrightarrow q \wedge \neg(\neg p \vee q)$ （蕴涵等值式）

$\Leftrightarrow q \wedge (p \wedge \neg q)$ （德·摩根律）

$\Leftrightarrow p \wedge (q \wedge \neg q)$ （交换律，结合律）

$\Leftrightarrow p \wedge 0$ （矛盾律）

$\Leftrightarrow 0$ （零律）

由最后一步可知，该式为矛盾式.

应用举例

例4 **简化下面一段程序**

```
If A ∧ B then
   If B ∨ C then
      X
   Else
      Y
   End
Else
   If A ∧ C then
      Y
   Else
      X
   End
End
```

执行程序段 X 的条件为

$((A \wedge B) \wedge (B \vee C)) \vee (\neg(A \wedge B) \wedge \neg(A \wedge C))$

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

执行程序段 Y 的条件为

$((A \wedge B) \wedge \neg(B \vee C)) \vee (\neg(A \wedge B) \wedge (A \wedge C))$

$\Leftrightarrow A \wedge \neg B \wedge C$

```
If A∧ ¬B∧C then
      Y
Else
      X
End
```

范式

范式:命题公式在等值意义下的一种标准形式.

定义

- 仅由有限个简单合取式组成的析取式 $A_1 \vee A_2 \vee \ldots \vee A_r$ 称为**析取范式**，其中$A_1, A_2, \ldots, A_r$是简单合取式.
- 仅由有限个简单析取式组成的合取式 $A_1 \wedge A_2 \wedge \ldots \wedge A_r$ 称为**合取范式**，其中$A_1, A_2, \ldots, A_r$是简单析取式.

例:

$\neg p \vee q \vee \neg r$, $(p \wedge \neg q) \vee (q \wedge r)$ —— 析取范式

$\neg p \vee q \vee \neg r$, $(p \vee \neg q) \wedge (q \vee r)$ —— 合取范式

范式存在定理

定理 范式存在定理

- 任何命题公式都存在着与之等值的析取范式与合取范式.

求公式A的范式的步骤：

(1) 消去A中的$\rightarrow$, $\leftrightarrow$（若存在）

$$A\rightarrow B\Leftrightarrow\neg A\vee B$$

$$A\leftrightarrow B\Leftrightarrow(\neg A\vee B)\wedge(A\vee\neg B)$$

(2) 否定联结词$\neg$的内移或消去

$$\neg\neg A\Leftrightarrow A$$

$$\neg(A\vee B)\Leftrightarrow\neg A\wedge\neg B$$

$$\neg(A\wedge B)\Leftrightarrow\neg A\vee\neg B$$

范式存在定理

(3) 使用分配律

$A\vee(B\wedge C) \Leftrightarrow (A\vee B)\wedge(A\vee C)$　　求合取范式

$A\wedge(B\vee C) \Leftrightarrow (A\wedge B)\vee(A\wedge C)$　　求析取范式

例：求$\neg(p\to q)\vee\neg r$ 的析取范式与合取范式

解 $\neg(p\to q)\vee\neg r$

$\Leftrightarrow \neg(\neg p\vee q)\vee\neg r$

$\Leftrightarrow (p\wedge\neg q)\vee\neg r$　　析取范式

$\Leftrightarrow (p\vee\neg r)\wedge(\neg q\vee\neg r)$　　合取范式

注意: 公式的析取范式与合取范式不惟一.

主范式

定义 极小项

- 在含有n个命题变项的简单合取式中，若每个命题变项与其否定有且仅有一个出现一次，则称这样的简单合取式为极小项.

定义 极大项

- 在含有n个命题变项的简单析取式中，若每个命题变项与其否定有且仅有一个出现一次，则称这样的简单析取式为极大项.

例：n=2, 命题变项为 p, q 时，

- 极小项：$\neg p \wedge \neg q$, $p \wedge \neg q$, …
- 极大项：$\neg p \vee q$, $\neg p \vee \neg q$, …

3个命题构成的极小项与极大项

极小项			极大项		
公式	成真赋值	名称	公式	成假赋值	名称
$\neg p \wedge \neg q \wedge \neg r$	0 0 0	m_0	$p \vee q \vee r$	0 0 0	M_0
$\neg p \wedge \neg q \wedge r$	0 0 1	m_1	$p \vee q \vee \neg r$	0 0 1	M_1
$\neg p \wedge q \wedge \neg r$	0 1 0	m_2	$p \vee \neg q \vee r$	0 1 0	M_2
$\neg p \wedge q \wedge r$	0 1 1	m_3	$p \vee \neg q \vee \neg r$	0 1 1	M_3
$p \wedge \neg q \wedge \neg r$	1 0 0	m_4	$\neg p \vee q \vee r$	1 0 0	M_4
$p \wedge \neg q \wedge r$	1 0 1	m_5	$\neg p \vee q \vee \neg r$	1 0 1	M_5
$p \wedge q \wedge \neg r$	1 1 0	m_6	$\neg p \vee \neg q \vee r$	1 1 0	M_6
$p \wedge q \wedge r$	1 1 1	m_7	$\neg p \vee \neg q \vee \neg r$	1 1 1	M_7

主范式

定义

- 如果公式 A 的析取范式中的简单合取式全是极小项，则称该析取范式为**主析取范式**.
- 如果公式 A 的合取范式中的简单析取式全是极大项，则称该合取范式为**主合取范式**.

定理

- 任何命题公式都存在着与之等值的主析取范式和主合取范式, 并且是**唯一**的.

例： n=3, 命题变项为 p, q, r 时，

$(\neg p\wedge\neg q\wedge r)\vee(\neg p\wedge q\wedge r) \Leftrightarrow m_1\vee m_3$ 是主析取范式

$(p\vee q\vee\neg r)\wedge(\neg p\vee q\vee\neg r) \Leftrightarrow M_1\wedge M_5$ 是主合取范式

求主析取范式的步骤

设公式 A 含命题变项 $p_1, p_2, \ldots, p_n$

(1) 求 A 的析取范式 $A' = B_1 \vee B_2 \vee \ldots \vee B_s$, 其中$B_j$是简单合取式, j=1,2, … ,s

(2) 若某个B_j既不含p_i, 又不含$\neg p_i$, 则将B_j展开成

$$B_j \Leftrightarrow B_j \wedge (p_i \vee \neg p_i) \Leftrightarrow (B_j \wedge p_i) \vee (B_j \wedge \neg p_i)$$

重复这个过程, 直到所有简单合取式都是长度为n的极小项为止

(3) 消去重复出现的极小项, 即用m_i代替$m_i \vee m_i$

(4) 将极小项按下标从小到大排列

例： 求$\neg(p\to q)\vee\neg r$ 的主析取范式

解 (1) $\neg(p\to q)\vee\neg r \Leftrightarrow (p\wedge\neg q)\vee\neg r$

$p\wedge\neg q \Leftrightarrow (p\wedge\neg q)\wedge 1$ 同一律

$\Leftrightarrow (p\wedge\neg q)\wedge(\neg r\vee r)$ 排中律

$\Leftrightarrow (p\wedge\neg q\wedge\neg r)\vee(p\wedge\neg q\wedge r)$ 分配律

$\Leftrightarrow m_4\vee m_5$

$\neg r \Leftrightarrow (\neg p\vee p)\wedge(\neg q\vee q)\wedge\neg r$ 同一律, 排中律

$\Leftrightarrow (\neg p\wedge\neg q\wedge\neg r)\vee(\neg p\wedge q\wedge\neg r)\vee(p\wedge\neg q\wedge\neg r)\vee(p\wedge q\wedge\neg r)$

$\Leftrightarrow m_0\vee m_2\vee m_4\vee m_6$ 分配律

得 $\neg(p\to q)\vee\neg r \Leftrightarrow m_0\vee m_2\vee m_4\vee m_5\vee m_6$

求主合取范式的步骤

设公式 A 含命题变项 $p_1, p_2, \ldots, p_n$

(1) 求A的合取范式$A'=B_1\wedge B_2\wedge \ldots \wedge B_s$, 其中$B_j$是简单析取式, $j=1,2, \ldots ,s$

(2) 若某个B_j既不含p_i, 又不含$\neg p_i$, 则将B_j展开成

$$B_j \Leftrightarrow B_j\vee(p_i\wedge\neg p_i) \Leftrightarrow (B_j\vee p_i)\wedge(B_j\vee\neg p_i)$$

重复这个过程，直到所有简单析取式都是长度为n的极大项为止

(3) 消去重复出现的极大项, 即用M_i代替$M_i\wedge M_i$

(4) 将极大项按下标从小到大排列

例： 求$\neg(p\to q)\lor\neg r$ 的主合取范式

解 $\neg(p\to q)\lor\neg r \Leftrightarrow (p\lor\neg r)\land(\neg q\lor\neg r)$

$p\lor\neg r \Leftrightarrow p\lor 0\lor\neg r$ 同一律

$\Leftrightarrow p\lor(q\land\neg q)\lor\neg r$ 矛盾律

$\Leftrightarrow (p\lor q\lor\neg r)\land(p\lor\neg q\lor\neg r)$ 分配律

$\Leftrightarrow M_1\land M_3$

$\neg q\lor\neg r \Leftrightarrow (p\land\neg p)\lor\neg q\lor\neg r$ 同一律, 矛盾律

$\Leftrightarrow (p\lor\neg q\lor\neg r)\land(\neg p\lor\neg q\lor\neg r)$ 分配律

$\Leftrightarrow M_3\land M_7$

得 $\neg(p\to q)\lor\neg r \Leftrightarrow M_1\land M_3\land M_7$

主范式的用途

(1) 求公式的成真赋值和成假赋值

(2) 判断公式的类型

- A为重言式⇔A的主析取范式含2^n个极小项

  ⇔A的主合取范式为1.
- A为矛盾式⇔ A的主析取范式为0

  ⇔ A的主合取范式含2^n个极大项
- A为非重言式的可满足式

  ⇔A的主析取范式中至少含一个且不含全部极小项

  ⇔A的主合取范式中至少含一个且不含全部极大项

(3) 判断两个公式是否等值

定理

- 设 m_i 与 M_i 是由同一组命题变项形成的极小项和极大项, 则$\neg m_i \Leftrightarrow M_i$,$\neg M_i \Leftrightarrow m_i$.

例:

- $\neg m_0 \Leftrightarrow M_0$

  $\neg(\neg p \wedge \neg q \wedge \neg r) \Leftrightarrow p \vee q \vee r$

- $m_0 \Leftrightarrow \neg M_0$

  $\neg p \wedge \neg q \wedge \neg r \Leftrightarrow \neg (p \vee q \vee r)$

由主析取范式求主合取范式

设 $A \Leftrightarrow m_{i_1} \vee m_{i_2} \vee \cdots \vee m_{i_s}$

没有出现的极小项是 $m_{j_1}, m_{j_2}, \cdots, m_{j_t}$，其中 $t = 2^n\text{-}s$,

于是 $\neg A \Leftrightarrow m_{j_1} \vee m_{j_2} \vee \cdots \vee m_{j_t}$

$$A \Leftrightarrow \neg(m_{j_1} \vee m_{j_2} \vee \cdots \vee m_{j_t})$$

$$\Leftrightarrow \neg m_{j_1} \wedge \neg m_{j_2} \wedge \cdots \wedge \neg m_{j_t}$$

$$\Leftrightarrow M_{j_1} \wedge M_{j_2} \wedge \cdots \wedge M_{j_t}$$

例 求$A=(\neg p\wedge\neg q\wedge r)\vee(\neg p\wedge q\wedge r)\vee(p\wedge q\wedge r)$的主合取范式

解 $A \Leftrightarrow m_1\vee m_3\vee m_7$

$$\Leftrightarrow M_0\wedge M_2\wedge M_4\wedge M_5\wedge M_6$$

推理理论

❑ 推理的形式结构

- ➢ $A_1 \wedge A_2 \wedge \dots \wedge A_k \rightarrow B$
- ➢ 前提： $A_1, A_2, \dots, A_k$

结论： B

定义 推理正确

❑ 若对于任意赋值，如果 $A_1 \wedge A_2 \wedge \dots \wedge A_k$ 为真时， B 也为真，则称由前提 $A_1, A_2, \dots, A_k$ 推出结论 B 的**推理正确**，并称B是 $A_1 \wedge A_2 \wedge \dots \wedge A_k$ 的**逻辑结论**或**有效结论**.

构造证明法

构造证明法，建立在推理定律（重言蕴含式）的基础之上

$A \Rightarrow (A \vee B)$	附加律
$(A \wedge B) \Rightarrow A$	化简律
$(A \to B) \wedge A \Rightarrow B$	假言推理
$(A \to B) \wedge \neg B \Rightarrow \neg A$	拒取式
$(A \vee B) \wedge \neg B \Rightarrow A$	析取三段论
$(A \to B) \wedge (B \to C) \Rightarrow (A \to C)$	假言三段论
$(A \leftrightarrow B) \wedge (B \leftrightarrow C) \Rightarrow (A \leftrightarrow C)$	等价三段论
$(A \to B) \wedge (C \to D) \wedge (A \vee C) \Rightarrow (B \vee D)$	构造性二难
$(A \to B) \wedge (\neg A \to B) \Rightarrow B$	构造性二难(特殊形式)
$(A \to B) \wedge (C \to D) \wedge (\neg B \vee \neg D) \Rightarrow (\neg A \vee \neg C)$	破坏性二难

证明中常用推理规则

(1) 前提引入规则：在证明的任一步，都可引入前提

(2) 结论引入规则：中间结论可作为后续推理的前提

(3) 置换规则：利用等值公式对部分公式进行置换

(4) 假言推理规则

$$\frac{\begin{array}{c}A\rightarrow B\\ A\end{array}}{\therefore B}$$

(5) 附加规则

$$\frac{A}{\therefore A\vee B}$$

(6) 化简规则

$$\frac{A\wedge B}{\therefore A}$$

证明中常用推理规则

北京邮电大学 Beijing University of Posts and Telecommunications

(7) 拒取式规则

$$\begin{array}{l} A\to B \\ \neg B \\ \hline \therefore \neg A \end{array}$$

(8) 假言三段论规则

$$\begin{array}{l} A\to B \\ B\to C \\ \hline \therefore A\to C \end{array}$$

(9) 析取三段论规则

$$\begin{array}{l} A\vee B \\ \neg B \\ \hline \therefore A \end{array}$$

(10)构造性二难推理规则

$$\begin{array}{l} A\to B \\ C\to D \\ A\vee C \\ \hline \therefore B\vee D \end{array}$$

(11) 合取引入规则

$$\begin{array}{l} A \\ B \\ \hline \therefore A\wedge B \end{array}$$

构造证明之一 ：直接证明法

前提：$(p\vee q)\rightarrow r$，$r\rightarrow s$，$\neg s$　结论：$\neg p\wedge\neg q$

证明：

① $r\rightarrow s$　　前提引入

② $\neg s$　　前提引入

③ $\neg r$　　①②拒取式

④ $(p\vee q)\rightarrow r$　　前提引入

⑤ $\neg(p\vee q)$　　③④拒取式

⑥ $\neg p\wedge\neg q$　　⑤置换

构造证明之二 ：附加前提证明法

- 欲证明
  - 前提：$A_1, A_2, \ldots, A_k$
  - 结论：$B \to C$
- 等价地证明
  - 前提：$A_1, A_2, \ldots, A_k, B$
  - 结论：C
- 原因：$(A_1 \wedge A_2 \wedge \ldots \wedge A_k) \to (B \to C)$

$$\Leftrightarrow \neg(A_1 \wedge A_2 \wedge \ldots \wedge A_k) \vee (\neg B \vee C)$$

$$\Leftrightarrow \neg(A_1 \wedge A_2 \wedge \ldots \wedge A_k) \vee (\neg B) \vee C$$

$$\Leftrightarrow \neg(A_1 \wedge A_2 \wedge \ldots \wedge A_k \wedge B) \vee C$$

$$\Leftrightarrow (A_1 \wedge A_2 \wedge \ldots \wedge A_k \wedge B) \to C$$

构造证明之二 ：附加前提证明法

例: 前提：$p \lor q$，$p \to r$，$r \to \neg s$　结论：$s \to q$

解　前提：$p \lor q$，$p \to r$，$r \to \neg s$，s　结论：q

① s	附加前提引入
② $p \to r$	前提引入
③ $r \to \neg s$	前提引入
④ $p \to \neg s$	②③假言三段论
⑤ $\neg p$	①④拒取式
⑥ $p \lor q$	前提引入
⑦ q	⑤⑥析取三段论

构造证明之三 ：归谬法 (反证法)

- 欲证明　前提：$A_1, A_2, \ldots, A_k$，结论：B.
- 将$\neg B$加入前提，若推出矛盾，则得证推理正确.

定理

- $(A_1 \wedge A_2 \wedge \ldots \wedge A_k) \Rightarrow B$ 推理正确，当且仅当 $A_1 \wedge A_2 \wedge \ldots \wedge A_k \wedge \neg B$ 为矛盾式.

原因:

$$A_1 \wedge A_2 \wedge \ldots \wedge A_k \rightarrow B$$

$$\Leftrightarrow \neg(A_1 \wedge A_2 \wedge \ldots \wedge A_k) \vee B$$

$$\Leftrightarrow \neg(A_1 \wedge A_2 \wedge \ldots \wedge A_k \wedge \neg B)$$

构造证明之三 ： 归谬法 (反证法)

例 构造下面推理的证明

前提：$\neg(p\wedge q)\vee r$，$r\rightarrow s$，$\neg s$，p

结论：$\neg q$

证明：用归缪法，证明 $\neg(p\wedge q)\vee r) \wedge (r\rightarrow s) \wedge \neg s \wedge p \wedge q$ 为矛盾式

① q	结论否定引入
② $r\rightarrow s$	前提引入
③ $\neg s$	前提引入
④ $\neg r$	②③拒取式
⑤ $\neg(p\wedge q)\vee r$	前提引入
⑥ $\neg(p\wedge q)$	④⑤析取三段论
⑦ $\neg p\vee\neg q$	⑥置换
⑧ $\neg p$	①⑦析取三段论
⑨ p	前提引入
⑩ $\neg p\wedge p$	⑧⑨合取

离散数学复习

郝杰

haojie@bupt.edu.cn

北京邮电大学信息安全中心

北京邮电大学 Beijing University of Posts and Telecommunications

命题逻辑的局限性

- 命题逻辑不能表达所有正确的推理. 例:

  所有实数的平方都是非负的.

  π是一个实数.

  π的平方是非负的.

- 在命题逻辑中，符号化为：$(p \wedge q) \to r$

  ——推理不正确（非重言式）

一阶逻辑（谓词逻辑）

- 谓词逻辑：
  - 区分主语、谓语，
  - 引入个体词，谓词、量词

- 可将谓词逻辑理解为

  命题逻辑 + {个体词，谓词，量词，函数}

基本概念——量词

量词(Quantifier)

- 表示个体常项或变项之间数量关系的词称为量词。
- 一般将量词分为全称量词和存在量词两种。

基本概念——量词

	何时为真	何时为假
$\forall x F(x)$	对个体域中的每个x，$F(x)$都为真	至少存在一个x，使$F(x)$为假
$\exists x F(x)$	个体域中至少有一个x，使$F(x)$为真	对个体域中的每个x，$F(x)$都为假

一阶逻辑合式公式

定义 合式公式

(1) 原子公式是合式公式.

(2) 若A是合式公式，则 $(\neg A)$也是合式公式.

(3) 若A, B是合式公式，则$(A\wedge B)$, $(A\vee B)$, $(A\to B)$, $(A\leftrightarrow B)$也是合式公式.

(4) 若A是合式公式，则$\forall xA$, $\exists xA$也是合式公式.

(5) 只有有限次地应用(1)~(4)形成的符号串是合式公式.

合式公式又称为谓词公式，简称公式

自由出现与约束出现

定义

- 在公式$\forall xA$和$\exists xA$中，称x为**指导变项**，A为相应量词的**辖域**.
- 在$\forall x$和$\exists x$的**辖域**中，x的所有出现都称为**约束出现**，
- A中不是约束出现的其他变项均称为是**自由出现**.
- 不含自由出现的个体变项的公式称为**闭式**.

例如, 在公式 $\forall x(F(x,y)\rightarrow G(x,z))$ 中,

$A=(F(x,y)\rightarrow G(x,z))$为$\forall x$的辖域,

x为指导变项, A中x的两次出现均为约束出现,

y与z均为自由出现，故不是闭式.

解释和赋值

定义 解释

(a) 非空个体域D;

(b) 对每一个个体常项 a 指定一个D上的元素;

(c) 对每一个函数变项符号 f 指定一个D上的函数;

(d) 对每一个谓词变项符号 F 指定一个D上的谓词;

- 在给定的解释下, 闭式公式都成为命题.

解释和赋值

定义 赋值

- 给定解释I，对公式中每一个自由出现的命题变项x指定一个值$\sigma(x)\in D_I$, 称作在解释I下的赋值.

- 公式 A 在解释 I 和赋值 σ 下的含义：取个体域 D，并将公式中出现的a、f、F 分别解释成$\bar{a}$ 、$\bar{f}$、 $\bar{F}$, 把自由出现的x换成$\sigma(x)$后所得到的命题.
- 在给定的解释和赋值下, 任何公式都成为命题.

定理 量词否定等值式

- 设$A(x)$是任意的公式
  - $\neg\forall x A(x) \Leftrightarrow \exists x \neg A(x)$
  - $\neg\exists x A(x) \Leftrightarrow \forall x \neg A(x)$

等值式

定理 量词辖域收缩与扩张等值式(1)

- 设$A(x)$是含x自由出现的任意公式，而公式B中不含x的自由出现，则关于全称量词：

1) $\forall x(A(x) \vee B) \Leftrightarrow \forall x A(x) \vee B$

2) $\forall x(A(x) \wedge B) \Leftrightarrow \forall x A(x) \wedge B$

3) $\forall x(A(x) \rightarrow B) \Leftrightarrow \exists x A(x) \rightarrow B$

4) $\forall x(B \rightarrow A(x)) \Leftrightarrow B \rightarrow \forall x A(x)$

定理 量词辖域收缩与扩张等值式(2)

- 设$A(x)$是含x自由出现的任意公式，而公式B中不含x的自由出现，则关于存在量词：

1) $\exists x(A(x) \vee B) \Leftrightarrow \exists x A(x) \vee B$

2) $\exists x(A(x) \wedge B) \Leftrightarrow \exists x A(x) \wedge B$

3) $\exists x(A(x) \rightarrow B) \Leftrightarrow \forall x A(x) \rightarrow B$

4) $\exists x(B \rightarrow A(x)) \Leftrightarrow B \rightarrow \exists x A(x)$

等值式

定理　量词分配等值式

- 设$A(x)$、$B(x)$是含x自由出现的公式，则：

1) $\forall x(A(x) \wedge B(x)) \Leftrightarrow \forall xA(x) \wedge \forall xB(x)$

2) $\exists x(A(x) \vee B(x)) \Leftrightarrow \exists xA(x) \vee \exists xB(x)$

等值式

注意：

- ∀对∨无分配律，∃对∧无分配律, 即

1) $\forall x(A(x) \vee B(x)) \not\Leftrightarrow \forall xA(x) \vee \forall xB(x)$

2) $\exists x(A(x) \wedge B(x)) \not\Leftrightarrow \exists xA(x) \wedge \exists xB(x)$

等值式

定理

- 设$A(x, y)$是含x、y自由出现的谓词公式，则：

  1) $\forall x \forall y A(x, y) \Leftrightarrow \forall y \forall x A(x, y)$

  2) $\exists x \exists y A(x, y) \Leftrightarrow \exists y \exists x A(x, y)$

定义 前束范式

- 设 A 为一个一阶逻辑公式, 若 A 具有如下形式

$$Q_1x_1Q_2x_2\cdots Q_kx_kB\,,$$

则称 A 为前束范式, 其中 $Q_i\,(1\le i\le k)$ 为 $\forall$ 或 $\exists$, B 为不含量词的公式.

❑ 换名规则

将一个指导变项及其在量词辖域中的所有约束出现替换成公式中未曾出现过的个体变项符号，公式中其余部分不变，则所得公式与原来的公式等值.

❖ 例如：

- $\forall xF(x)\wedge\forall xG(x) \Leftrightarrow \forall xF(x)\wedge\forall tG(t)$
- $\forall x(F(x,y,z))\rightarrow\exists yG(x,y,z))$

$$\Leftrightarrow\forall x(F(x,y,z))\rightarrow\exists wG(x, w, z))$$

前束范式

例 求下列公式的前束范式

(1) $\neg \exists x(M(x) \wedge F(x))$

解: $\Leftrightarrow \forall x(\neg M(x) \vee \neg F(x))$ (量词否定等值式)

$\Leftrightarrow \forall x(M(x) \rightarrow \neg F(x))$

❖ 两步结果都是前束范式，前束范式不惟一.

前束范式

(2) $\forall xF(x) \land \neg\exists xG(x)$

解: $\Leftrightarrow \forall xF(x) \land \forall x\neg G(x)$ (量词否定等值式)

$\Leftrightarrow \forall x(F(x) \land \neg G(x))$ (量词分配等值式)

或

$\forall xF(x) \land \neg\exists xG(x)$

$\Leftrightarrow \forall xF(x) \land \forall x\neg G(x)$ (量词否定等值式)

$\Leftrightarrow \forall xF(x) \land \forall y\neg G(y)$ (换名规则)

$\Leftrightarrow \forall x(F(x) \land \forall y\neg G(y))$ (量词辖域扩张)

$\Leftrightarrow \forall x\forall y(F(x) \land \neg G(y))$ (量词辖域扩张)

前束范式

(4) $\forall x(F(x,y) \to \exists y(G(x,y) \wedge H(x,z)))$

解: $\Leftrightarrow \forall x(F(x,y) \to \exists u(G(x,u) \wedge H(x,z)))$ (换名规则)

$\Leftrightarrow \forall x \exists u(F(x,y) \to G(x,u) \wedge H(x,z)))$ (量词辖域扩张)

❖ 注意:

- 上式中∀与∃不能颠倒顺序
- 前束范式各指导变项应各不相同
- 原公式自由出现的变项仍为自由出现

离散数学复习

郝杰
haojie@bupt.edu.cn
北京邮电大学信息安全中心

北京邮电大学 Beijing University of Posts and Telecommunications

3.1 集合的基本概念

3.2 集合的基本运算

3.3 集合中元素的计数

3.1 集合的基本概念

- 集合的定义与表示
- 集合与元素
- 集合之间的关系
- 空集
- 全集
- 幂集

集合基本运算

- 集合运算指以集合作为运算对象，结果还是集合的运算

1) 并集 (**union**)

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

例如：$\{1,2,5\} \cup \{1,3,4\} = \{1,2,3,4,5\}$

2) 交集 (**intersection**)

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

例如：$\{1,2,5\} \cap \{2,3\} = \{2\}$

集合基本运算

Beijing University of Posts and Telecommunications 北京邮电大学

3) 相对补集 (差集, difference)

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

例如： $\{1,2,5\}-\{1,3,4\}=\{2,5\}$

4) 绝对补集 (补集, complement)

定义： $\sim A = E - A = \{x \mid x \in E \wedge x \notin A\}$

或： $\sim A = \{x \mid x \notin A\}$

例如： $E = \{0,1,2,3\}$, $A = \{0,1,2\}$, $\sim A = \{3\}$

集合基本运算

5) 对称差 (symmetric difference)

定义： $A \oplus B = (A-B) \cup (B-A)$

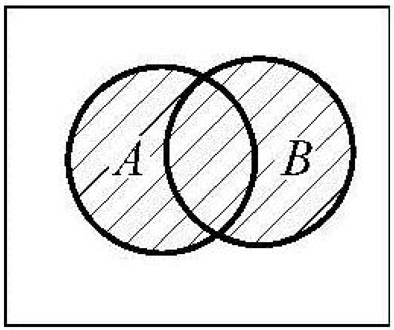
$= (A \cup B) - (A \cap B)$

例如： $A = \{0,1,2\}, B=\{2,3\}.$

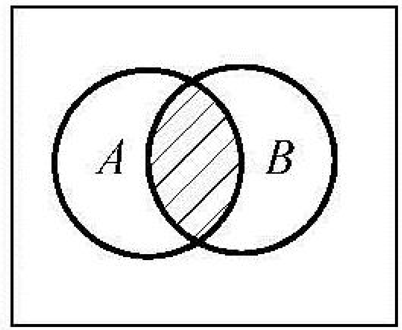
$A \oplus B = \{0,1\} \cup \{3\} = \{0,1,3\}$

$= \{0,1,2,3\} - \{2\} = \{0,1,3\}.$

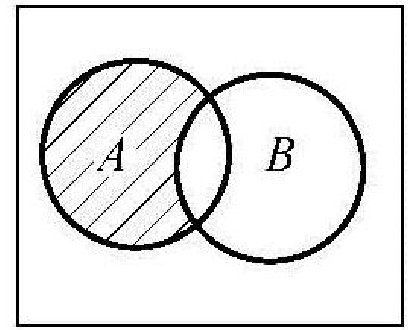
文氏图（ Venn Diagram ）



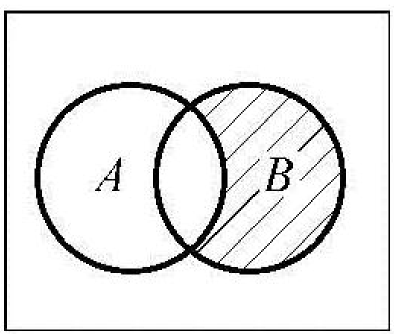
$A \cup B$



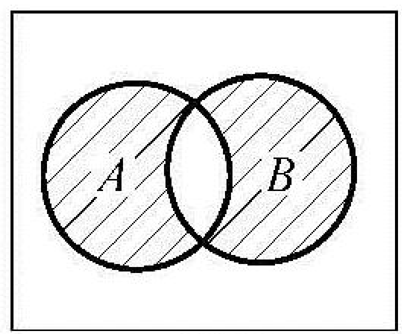
$A \cap B$



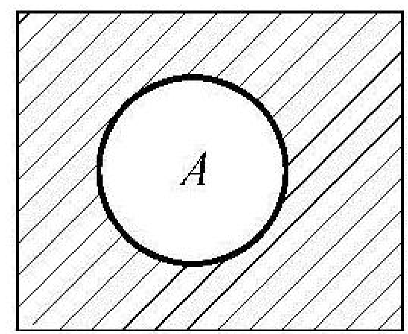
$A - B$



$B - A$



$A \oplus B$



$\sim A$

集合运算的算律

- 幂等律：$A \cup A = A \qquad A \cap A = A$
- 交换律：$A \cup B = B \cup A$

$$A \cap B = B \cap A$$

- 结合律：

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

- 分配律：

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

集合运算的算律

- 同一律：$A \cup \varnothing = A \quad A \cap E = A$
- 零律：$A \cap \varnothing = \varnothing \quad A \cup E = E$
- 排中律：$A \cup {\sim}A = E$
- 矛盾律：$A \cap {\sim}A = \varnothing$
- 吸收律：$A \cup (A \cap B) = A$

  $A \cap (A \cup B) = A$
- 双重否定律：${\sim}{\sim}A = A$

集合运算的算律

❑ 德·摩根律：

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

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

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

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

$$\sim\varnothing=E$$

$$\sim E=\varnothing$$

常用集合运算性质

- $A \cap B \subseteq A,\quad A \cap B \subseteq B$
- $A \subseteq A \cup B,\ B \subseteq A \cup B$
- $A - B \subseteq A$
- $A - B = A \cap \sim B$
- $A \subseteq B \Leftrightarrow A \cup B = B \Leftrightarrow A \cap B = A \Leftrightarrow A - B = \varnothing$

常用集合运算性质

北京郵電大學 Beijing University of Posts and Telecommunications

- $A \oplus B = B \oplus A$
- $(A \oplus B) \oplus C = A \oplus (B \oplus C)$
- $A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$
- $A \oplus \varnothing = A \quad A \oplus A = \varnothing$
- $A \oplus B = A \oplus C \Rightarrow B = C$

例1：试证明 $(A - B) \cup B = A \cup B$.

证明：$(A - B) \cup B = (A \cap \sim B) \cup B$

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

$= (A \cup B) \cap E$

$= A \cup B$

例2：已知$A \subseteq B$, 证明：$\sim B \subseteq \sim A$.

证明：由 $A \subseteq B$, 得 $B \cap A = A$, 由德•摩根律：

$\sim B \cup \sim A = \sim(B \cap A) = \sim A$,

于是可得 $\sim B \subseteq \sim A$

包含排斥原理

北京邮电大学 Beijing University of Posts and Telecommunications

定理

- 设 S 为有穷集，$P_1, P_2, \ldots, P_m$ 是 m 种性质，A_i 是 S 中具有性质 P_i 的元素构成的子集, $i = 1, 2, \ldots, m$, 则 S 中不具有性质 $P_1, P_2, \ldots, P_m$ 的元素数为

$$
\begin{aligned}
&|\overline{A_1} \cap \overline{A_2} \cap \ldots \cap \overline{A_m}| \\
&= |S| - \sum_{i=1}^{m} |A_i| + \sum_{1 \le i < j \le m} |A_i \cap A_j| - \sum_{1 \le i < j < k \le m} |A_i \cap A_j \cap A_k| + \ldots \\
&+ (-1)^m |A_1 \cap A_2 \cap \ldots \cap A_m|
\end{aligned}
$$

包含排斥原理

推论

- S中至少具有一条性质的元素数为

$$|A_1 \cup A_2 \cup \ldots \cup A_m|$$

$$= \sum_{i=1}^{m} |A_i| - \sum_{1 \le i < j \le m} |A_i \cap A_j| + \sum_{1 \le i < j < k \le m} |A_i \cap A_j \cap A_k| + \ldots$$

$$+ (-1)^{m-1} |A_1 \cap A_2 \cap \ldots \cap A_m|$$

证明：$|A_1 \cup A_2 \cup \ldots \cup A_m|$

$$= |S| - |\overline{A_1 \cup A_2 \cup \ldots \cup A_m}|$$

$$= |S| - |\overline{A_1} \cap \overline{A_2} \cap \ldots \cap \overline{A_m}|$$

将包含排斥定理代入即可

离散数学复习

郝杰

haojie@bupt.edu.cn

北京邮电大学信息安全中心

4.1 集合的笛卡儿积与二元关系

4.2 关系的运算

4.3 关系的性质

4.4 关系的闭包

4.5 等价关系和偏序关系

4.6 函数的定义和性质

4.7 函数的复合和反函数

二元关系

定义 二元关系

- 如果一个集合满足以下条件之一，则称该集合为一个二元关系，一般记作 R.

 1) 集合非空，且集合中的元素都是有序对;

 2) 集合是空集.

- 如果$\langle x, y\rangle \in R$, 则记作 xRy；如果$\langle x, y\rangle \notin R$, 则记作$x \not R\, y$.

例如：$R = \{\langle 1,2\rangle, \langle a,b\rangle\}$，且 $1R2$, aRb, $a \not R\, c$ 等.

二元关系

定义

- 设 A, B 为集合，$A\times B$的任何子集所定义的二元关系称做**从 A 到 B 的二元关系**, 特别地,当 $A=B$ 时, 称做 **A上的二元关系**.

例：$A=\{0, 1\}$, $B=\{1, 2, 3\}$, $R_1=\{<0, 2>\}$, $R_2= A\times B$, $R_3=\{<0,1>\}$. 则 R_1, R_2, R_3是从 A到 B 的二元关系, R_3也是 A 上的二元关系.

- 当$|A| = n$, $|A\times A| = n^2$ 时, $A\times A$的子集有2^{n^2}个. 所以 A上有 2^{n^2} 种不同的二元关系.

关系的表示

1) 关系矩阵

- 若$A = \{a_1, a_2, \ldots, a_m\}$, $B = \{b_1, b_2, \ldots , b_n\}$，$R$ 是从 A 到 B 的关系, R 的关系矩阵是布尔矩阵

$$M_R = [\, r_{ij} \,]_{m\times n}\,,$$

其中 $r_{ij} = 1$, 当$<a_i, b_j> \in R$; $r_{ij} = 0$, 当$<a_i, b_j> \notin R$.

- 例如：

$A=\{1, 2, 3, 4\}$.

$R=\{<1,1>, <1,2>, <2,3>, <2,4>, <4,2>\}$.

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

关系的表示

2) 关系图

- 若$A=\{x_1, x_2, \ldots, x_m\}$, R 是A上的关系, 其关系图为

$$G_R = <V, E>,$$

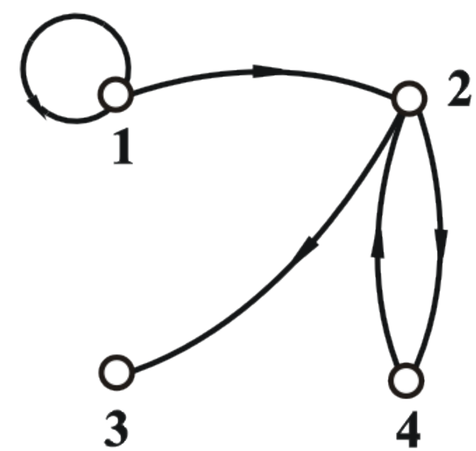
其中$V = A$为结点集, E 为边集. 如果$<x_i, x_j>$属于关系 R, 则从 x_i 到 x_j 的有向边 $<x_i, x_j> \in E$.

❖ 例如:

$A=\{1, 2, 3, 4\}$.

$R=\{<1, 1>, <1, 2>, <2, 3>,$

$<2, 4>, <4, 2>\}$.



关系的基本运算

1. 关系 R 的逆记作R^{-1}, 定义为:

$$R^{-1} = \{<y, x> \mid <x, y>\in R\}.$$

❖ 例如: $R = \{<1, 2>, <2, 3>, <1, 4>, <2, 2>\}.$

$R^{-1} = \{<2, 1>, <3, 2>, <4, 1>, <2, 2>\}.$

2. 关系 R 和S的合成记作 $R\circ S$, 定义为:

$$R\circ S = |<x, z> \mid \exists y(<x, y>\in S \wedge <y, z>\in R)\}.$$

➢ 注意: 左复合, S 先起作用, 然后将R复合到S上.

关系的基本运算

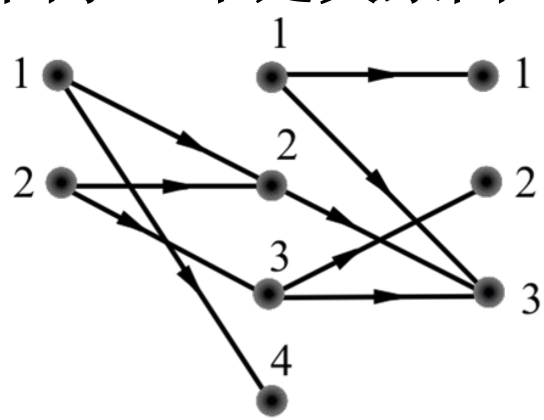
❖ 例如：$R = \{\langle 1, 1\rangle, \langle 1, 3\rangle, \langle 2, 3\rangle, \langle 3, 2\rangle, \langle 3, 3\rangle\}$.

$S = \{\langle 1, 2\rangle, \langle 2, 3\rangle, \langle 1, 4\rangle, \langle 2, 2\rangle\}$.

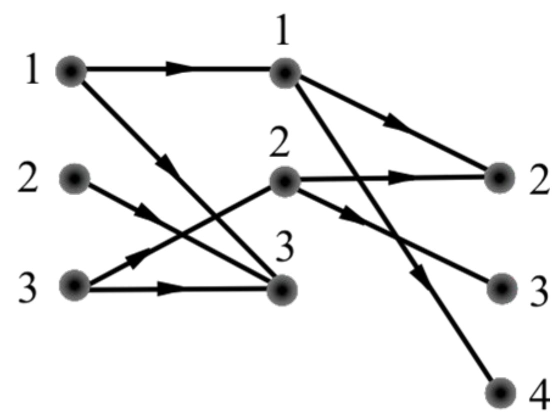
$R\circ S = \{\langle 1, 3\rangle, \langle 2, 2\rangle, \langle 2, 3\rangle\}$.

$S\circ R = \{\langle 1, 2\rangle, \langle 1, 4\rangle, \langle 3, 2\rangle, \langle 3, 3\rangle\}$.

➢ 利用图示（不是关系图）方法求合成



$R\circ S$



$S\circ R$

关系的基本运算

北京郵電大學
Beijing University of Posts and Telecommunications

❖ 例如: $R = \{<1, 1>, <1, 3>, <2, 3>, <3, 2>, <3, 3>\}$.

$S = \{<1, 2>, <2, 3>, <1, 4>, <2, 2>\}$.

$R \circ S = \{<1, 3>, <2, 2>, <2, 3>\}$.

➢ 关系矩阵相乘求合成

$$R \circ S = \begin{bmatrix} 0 & 1 & 0 & 1 \\ \boxed{0 \quad 1 \quad 1 \quad 0} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & \boxed{1} & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

运算中加法‘+’是逻辑加:

$0 + 0 = 0, \quad 0 + 1 = 1, \quad 1 + 0 = 1, \quad 1 + 1 = 1.$

关系的基本运算

北京邮电大学 Beijing University of Posts and Telecommunications

3. 关系 R 在集合A的上的**限制**记作 $R\upharpoonright A$, 定义为:

$$R\upharpoonright A = \{<x, y> \mid xRy \wedge x\in A\}.$$

4. 集合A 在R下的**像**记作 $R[A]$, 定义为:

$$R[A] = \mathrm{ran}(R\upharpoonright A).$$

❖ 例如: $R=\{<1, 2>, <2, 3>, <1, 4>, <2, 2>\}$.

$$R\upharpoonright\{1\} = \{<1,2>,<1,4>\}.$$

$$R[\{1\}] = \{2,4\}.$$

$$R[\{1,2\}] = \{2,3,4\}.$$

定理

- 设F、G、H是任意的关系, 则有

  1) $(F^{-1})^{-1} = F$;

  2) $\mathrm{dom}F^{-1} = \mathrm{ran}F$, $\mathrm{ran}F^{-1} = \mathrm{dom}F$;

  3) $(F \circ G) \circ H = F \circ (G \circ H)$;

  4) $(F \circ G)^{-1} = G^{-1} \circ F^{-1}$.

- $(F \circ G)^{-1} = G^{-1} \circ F^{-1}$.
- 证明： 任取$<x, y>$,

$$
\begin{aligned}
&<x, y> \in (F \circ G)^{-1} \\
&\Leftrightarrow <y, x> \in F \circ G \\
&\Leftrightarrow \exists t\,(<y, t> \in G \wedge (t, x) \in F) \\
&\Leftrightarrow \exists t\,(<x, t> \in F^{-1} \wedge (t, y) \in G^{-1}) \\
&\Leftrightarrow <x, y> \in G^{-1} \circ F^{-1}.
\end{aligned}
$$

定理

- 设F、G、H是任意的关系, 则有
  1) $F\circ(G\cup H) = F\circ G \cup F\circ H$;
  2) $F\circ(G\cap H) \subseteq F\circ G \cap F\circ H$;
  3) $(G\cup H)\circ F = G\circ F \cup H\circ F$;
  4) $(G\cap H)\circ F \subseteq G\circ F \cap H\circ F$.

A上关系的幂运算

定义

- 设 R 为 A 上的关系, n为自然数, 则 R 的 n 次幂为:

  (1) $R^0 = \{<x, x> \mid x \in A\} = I_A$;

  (2) $R^{n+1} = R^n \circ R$, $n \geq 0$.

➢ 注意:

- 对于A上的任何关系R_1和R_2都有

$$R_1^0 = R_2^0 = I_A.$$

- 对于A上的任何关系 R 都有

$$R^1 = R.$$

幂运算的性质

定理

- 则 R 是 A 上的关系, $m, n\in \mathrm{N}$, 则

  1) $R^m \circ R^n = R^{m+n}$

  2) $(R^m)^n = R^{mn}$

- 证明: (1)对于任意给定的$m\in \mathrm{N}$, 对n进行归纳.
  - 若n=0, 则有

    $$R^m\circ R^0=R^m\circ I_A=R^m=R^{m+0};$$
  - 假设 $R^m\circ R^n=R^{m+n}$, 则有

    $$R^m\circ R^{n+1} = R^m\circ(R^n\circ R) = (R^m\circ R^n)\circ R = R^{m+n+1},$$

    故对一切 $m, n\in \mathrm{N}$有$R^m\circ R^n=R^{m+n}$.

关系的性质

- 自反性 (**reflexive**)
- 反自反性 (**irreflexive**)
- 对称性 (**symmetric**)
- 反对称性 (**antisymmetric**)
- 传递性 (**transitive**)

自反性与反自反性

定义

- 设 R 为 A 上的关系

1) 若$\forall x(x\in A \rightarrow \langle x, x\rangle \in R)$, 则称 R 在 A 上是自反的.

2) 若$\forall x(x\in A \rightarrow \langle x, x\rangle \notin R)$, 则称 R 在 A 上是反自反的.

- 实例:

- 自反关系：A上的全域关系 E_A, 恒等关系 I_A
  小于等于关系 L_A, 整除关系 D_A
- 反自反关系：实数集上的小于关系
  幂集上的真包含关系

对称性与反对称性

北京邮电大学 Beijing University of Posts and Telecommunications

定义

- 设 R 为 A 上的关系

1) 若 $\forall x \forall y(x, y \in A \land <x, y> \in R \rightarrow <y, x> \in R)$，则称 R 为 A 上对称的关系.

2) 若 $\forall x \forall y(x, y \in A \land <x, y> \in R \land <y, x> \in R \rightarrow x = y)$，则称 R 为 A 上的反对称关系.

- 实例：
  - 对称关系：全域关系 E_A, 恒等关系 I_A 和空关系 $\varnothing$.
  - 反对称关系：恒等关系 I_A，空关系 $\varnothing$.

传递性

定义

- 设 R 为 A 上的关系，若

$$\forall x \forall y \forall z\,(\,x, y, z \in A \land \langle x, y\rangle \in R \land \langle y, z\rangle \in R \rightarrow \langle x, z\rangle \in R\,),$$

则称 R 是 A 上的传递关系.

- 实例：

A上的全域关系 E_A，恒等关系 I_A和空关系 $\varnothing$.

小于等于关系，小于关系，整除关系，包含关系，真包含关系

□ 关系性质判别

	自反	反自反	对称	反对称	传递
表达式	$I_A \subseteq R$	$R \cap I_A = \varnothing$	$R = R^{-1}$	$R \cap R^{-1} \subseteq I_A$	$R \circ R \subseteq R$
关系矩阵	主对角线元素全是1	主对角线元素全是0	矩阵是对称矩阵	若$r_{ij}=1$, 且$i \neq j$, 则$r_{ji}=0$	对M^2中1所在位置, M中相应位置都是1
关系图	每个顶点都有环	每个顶点都没有环	如果两个顶点之间有边, 是一对方向相反的边(无单边)	如果两点之间有边, 是一条有向边(无双向边)	如果顶点x_i到x_j有边, x_j到x_k有边, 则从 x_i到x_k 有边

闭包的定义

定义

- 设 R 为非空集合 A 上的关系, R 的自反（对称或传递）闭包是 A 上的关系 R', 使得 R' 满足以下条件:
  1) R'是自反的（对称的或传递的）;
  2) $R \subseteq R'$;
  3) 对 A 上任何包含 R 的自反（对称或传递）关系 R'' 有 $R' \subseteq R''$.

- 一般将 R 的自反闭包记作 $r(R)$, 对称闭包记作 $s(R)$, 传递闭包记作 $t(R)$.

闭包的构造方法

北京郵電大學 Beijing University of Posts and Telecommunications

定理

- 设 R 为非空集合 A 上的关系, 则有
  1) $r(R) = R \cup R^0$;
  2) $s(R) = R \cup R^{-1}$;
  3) $t(R) = R \cup R^2 \cup R^3 \cup \ldots$.

- 说明
  - 对于有穷集合 A ($|A| = n$), 3)中的并最多不超过 R^n.
  - 若 R 是自反的, 则 $r(R)=R$; 若 R 是对称的, 则 $s(R)=R$; 若 R 是传递的, 则 $t(R)=R$.

定义 等价关系

- 设 R 为 A 上的关系. 如果 R 是自反的、对称的和传递的, 则称 R 为 A 上的等价关系. 设 R 是一个等价关系, 若 $\langle x, y\rangle \in R$, 称 x 等价于 y, 记做 $x \sim y$.

- 实例:

设 $A=\{1, 2, \ldots, 8\}$, 如下定义 A 上的关系 R:

$$R = \{ \langle x, y\rangle \mid x, y \in A \wedge x \equiv y \pmod 3 \},$$

其中 $x \equiv y \pmod 3$ 叫做 x 与 y 模3相等, 即 x 除以3的余数与 y 除以3的余数相等.

等价关系

定义 等价类

- 设 R 非空集合A上的等价关系. 对于$\forall x \in A$，令

$$[x]_R = \{ y \mid y \in A \land xRy \}$$

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

- 实例:

集合 $A=\{1, 2, \ldots, 8\}$上模 3 等价关系的等价类:

$$[1] = [4] = [7] = \{1, 4, 7\};$$
$$[2] = [5] = [8] = \{2, 5, 8\};$$
$$[3] = [6] = \{3, 6\}.$$

等价类

北京邮电大学 Beijing University of Posts and Telecommunications

定理 等价类的性质

- 设 R 是非空集合 A 上的等价关系, 则

1) $\forall x \in A$, $[x]$是 A 的非空子集.

2) $\forall x, y \in A$, 如果 $x\,R\,y$, 则 $[x] = [y]$.

3) $\forall x, y \in A$, 如果 $x \not R\, y$, 则 $[x]$ 与 $[y]$ 不交.

4) $\cup\{\,[x] \mid x \in A\}=A$,即所有等价类的并集就是$A$.

2018年秋季学期

商集

定理 商集

- 设 R 是非空集合 A 上的等价关系,以R的所有等价类作为元素的集合称为 A 关于 R 的商集,记做A/R,即 $A/R = \{ [x]_R \mid x \in A \}$

- 实例:

  集合 $A=\{1, 2, \ldots, 8\}$上模 3 等价关系 R 的等价类为:

$$[1] = [4] = [7] = \{1, 4, 7\};$$
$$[2] = [5] = [8] = \{2, 5, 8\};$$
$$[3] = [6] = \{3, 6\}.$$

  等价关系R的商集为 $A/R = \{ \{1,4,7\}, \{2,5,8\}, \{3,6\} \}$.

定义 偏序关系

- 设 R 为 A 上的关系. 如果 R 是自反的、反对称的和传递的, 则称 R 为 A 上的偏序关系, 简称偏序, 记作$\preccurlyeq$. 设 R 是一个偏序关系, 若$\langle x, y\rangle \in R$, 记作 $x \preccurlyeq y$, 读作 x "小于或等于" y.

- 实例:

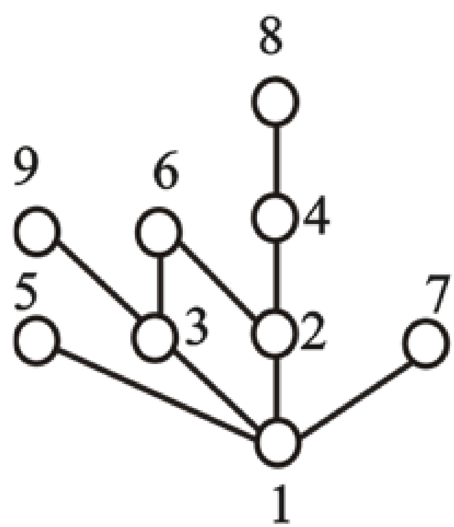
  大于等于关系, 小于等于关系, 整除关系.

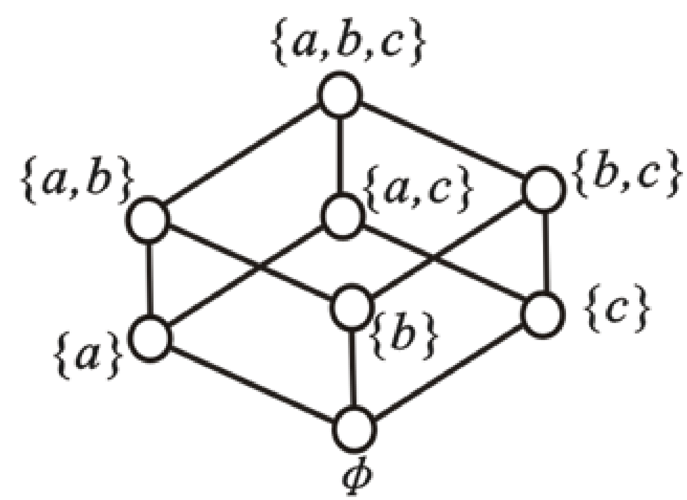
  集合上的包含关系.

哈斯图 (Hasse Diagrams)

- 利用偏序自反、反对称、传递性简化的关系图
  - 如果 y 覆盖 x, 则在结点 y 和 x 之间连一条线.
  - 结点位置按照它们在偏序中的次序从底向上排列.
- 例如：

$<\{1, 2, 3, 4, 5, 6, 7, 8, 9\}, R_{整除}>$ $<P(\{a, b, c\}), R_{\subseteq}>$





离散数学复习

郝杰
haojie@bupt.edu.cn
北京邮电大学信息安全中心

第5章 图的基本概念

北京邮电大学 Beijing University of Posts and Telecommunications

5.1 无向图及有向图

- 无向图与有向图
- 顶点的度数
- 握手定理
- 简单图
- 完全图
- 子图
- 补图

图论基本定理——握手定理

定理 任意无向图和有向图的所有顶点度数之和都等于边数的2倍，并且有向图的所有顶点入度之和等于出度之和等于边数.

- 证明:
  - G 中每条边（包括环）均有两个端点,
  - G 中各顶点度数之和, m条边共提供$2m$度.
  - 有向图的每条边提供一个入度和一个出度, 故所有顶点入度之和等于出度之和等于边数.

推论 任意无向图和有向图的奇度顶点个数必为偶数.

图的同构

定义 设$G_1 = <V_1, E_1>$, $G_2 = <V_2, E_2>$为两个无向图 (有向图), 若存在双射函数 $f: V_1 \to V_2$, 使得对于任意的顶点 $v_i, v_j \in V_1$, 有

$$(v_i, v_j) \in E_1 \ (<v_i, v_j> \in E_1),$$

当且仅当

$$(f(v_i), f(v_j)) \in E_2 \ (<f(v_i), f(v_j)> \in E_2),$$

并且,

(v_i, v_j) ($<v_i, v_j>$) 与 $(f(v_i), f(v_j))$ ($<f(v_i), f(v_j)>$)的重数相同，则称 G_1与 G_2是同构的，记作$G_1 \cong G_2$.

图的同构

- **几点说明：**

➢ 图之间的同构关系具有自反性、对称性和传递性.

➢ 有多条同构的必要条件，但它们都不是充分条件：

① 边数相同，顶点数相同；

② 度数列相同(不计度数的顺序)；

③ 对应顶点的关联集及邻域的元素个数相同，等等

➢ 若不满足必要条件，则两图不同构

至今没有找到判断两个图同构的多项式时间算法

子图

定义 设 $G=<V,E>$, $G'=<V',E'>$ 是两个图

(1) 若$V'\subseteq V$ 且 $E'\subseteq E$, 则称G'为G的子图, G为G'的母图, 记作$G'\subseteq G$.

(2) 若$G'\subseteq G$ 且$V'=V$，则称G'为G的生成子图.

(3) 若$V'\subset V$ 或$E'\subset E$，称G'为G的真子图.

(4) 设$V'\subseteq V$ 且$V'\neq\varnothing$, 以V'为顶点集, 以两端点都在V'中的所有边为边集的G的子图称作V'的导出子图，记作 $G[V']$.

(5) 设$E'\subseteq E$且$E'\neq\varnothing$, 以E'为边集, 以E'中边关联的所有顶点为顶点集的G的子图称作E'的导出子图, 记作 $G[E']$.

5.2 通路、回路和图的连通性

- 简单通(回)路, 初级通(回)路, 复杂通(回)路
- 无向图的连通性

  无向连通图, 连通分支
- 有向连通图

  弱连通图, 单向连通图, 强连通图
- 点割集与割点
- 边割集与割边(桥)

5.2 通路、回路和图的连通性

- 简单通(回)路, 初级通(回)路, 复杂通(回)路
- 无向图的连通性

  无向连通图, 连通分支
- 有向连通图

  弱连通图, 单向连通图, 强连通图
- 点割集与割点
- 边割集与割边(桥)

通路与回路

北京邮电大学 Beijing University of Posts and Telecommunications

定理 在 n 阶图 G 中, 若从顶点u到v $(u \neq v)$ 存在通路, 则从 u 到 v 存在长度小于等于 $n-1$ 的通路.

证明:

设$\Gamma = v_0e_1v_1e_2\ldots e_lv_l$为从 $u=v_0$ 到 $v= v_l$ 的通路.

如果$l > n-1$, 由于图中有n个顶点, $v_0, v_1, \ldots, v_l$ 必有2个相同, 设$v_i = v_j$, 则存在v_i到 v_j 的回路.

删除这条回路, 得到 $v_0e_1v_1e_2\ldots v_ie_{j+1}\ldots e_lv_l$仍为从 $u=v_0$ 到 $v= v_l$的通路, 长度减少 $j-i$.

重复此过程, 得到长度不超过 $n-1$ 的通路.

点割集

记 $G-v$: 从 G 中删除 v 及关联的边.

$G-V'$: 从 G 中删除 V'中所有的顶点及关联的边.

$G-e$: 从 G 中删除 e .

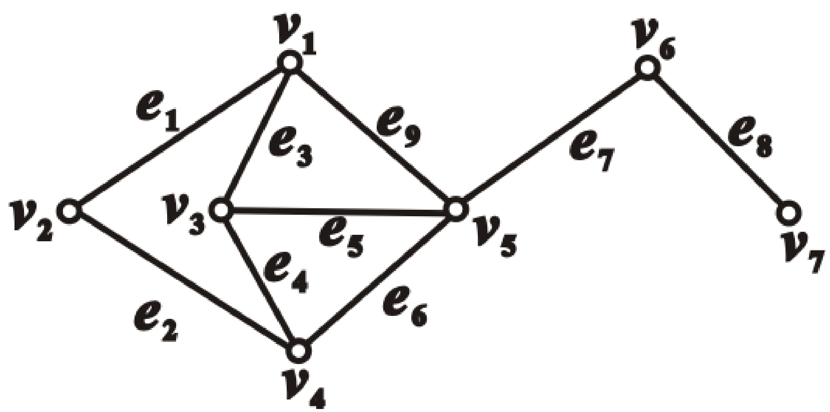
$G-E'$: 从 G 中删除 E' 中所有边.

定义 设无向图 $G=<V,E>$, $V'\subset V$, 若 $p(G-V')>p(G)$ 且$\forall V''\subset V'$, $p(G-V'')=p(G)$, 则称V'为G的点割集. 若$\{v\}$为点割集, 则称v为割点.

边割集

定义 设无向图 $G = <V, E>$, $E' \subseteq E$, 若$p(G-E')>p(G)$ 且$\forall E'' \subset E'$, $p(G-E'')=p(G)$, 则称E'为G的**边割集**. 若$\{e\}$为边割集, 则称e为**割边**或**桥**.

- 例 $\{e_1, e_2\}$, $\{e_1, e_3, e_5, e_6\}$, $\{e_8\}$等是边割集, e_8是桥, $\{e_7, e_9, e_5, e_6\}$不是边割集



5.3 图的矩阵表示

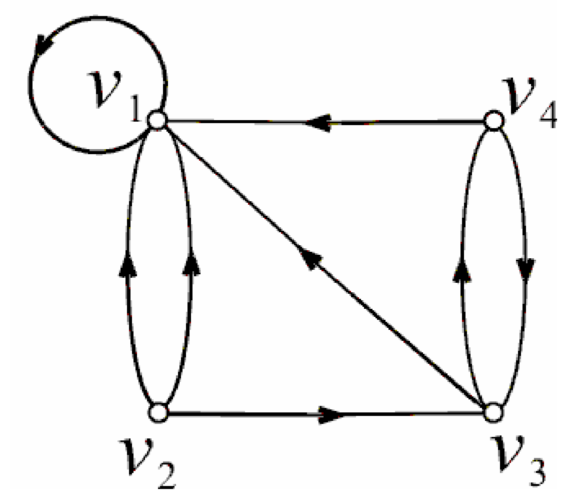
- 无向图的关联矩阵
- 有向图的关联矩阵
- 有向图的邻接矩阵
- 有向图的可达矩阵

有向图的邻接矩阵

定义 设有向图 $D=<V, E>$, $V=\{v_1, v_2, \ldots, v_n\}$, $E=\{e_1, e_2, \ldots, e_m\}$, 令 $a_{ij}^{(1)}$为顶点 v_i邻接到 v_j的边的条数, 称$(a_{ij}^{(1)})_{m\times n}$为 ***D* 的邻接矩阵**, 记作 $A(D)$, 简记为 A.

■ 例

$$A=\begin{bmatrix} 1 & 0 & 0 & 0 \\ 2 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$



D中的通路及回路数

定理 设 A 为 n 阶有向图 D 的邻接矩阵, 则 $A^l\,(l \ge 1)$ 中的下列元素

1. $a_{ij}^{(l)}$ 为 D 中 v_i 到 v_j 长度为 l 的通路数;
2. $a_{ii}^{(l)}$ 为 v_i 到自身长度为 l 的回路数;
3. $\sum\limits_{i=1}^{n}\sum\limits_{j=1}^{n} a_{ij}^{(l)}$ 为 D 中长度为 l 的通路总数;
4. $\sum\limits_{i=1}^{n} a_{ii}^{(l)}$ 为 D 中长度为 l 的回路总数.

5.4 最短路径, 关键路径与着色

- 带权图
- 最短路径与Dijkstra标号法
- 项目网络图与关键路径
- 着色问题

标号法 (E.W.Dijkstra, 1959)

北京邮电大学 Beijing University of Posts and Telecommunications

- 设带权图 $G=<V, E, w>$, 其中 $\forall e \in E$, $w(e) \geq 0$.

➢ 设 $V = \{v_1, v_2, \ldots, v_n\}$, 求$v_1$到其余各顶点的最短路径

1. 令 $l_1 \leftarrow 0$, $p_1 \leftarrow \lambda$, $l_j \leftarrow +\infty$, $p_j \leftarrow \lambda$, $j = 2, 3, \ldots, n$,

   $P = \{v_1\}$, $T = V - \{v_1\}$, $k \leftarrow 1$, $t \leftarrow 1$.   // λ表示空

   2. 对所有的 $v_j \in T$ 且 $(v_k, v_j) \in E$

      令 $l \leftarrow \min\{l_j, l_k + w_{kj}\}$,

   若 $l = l_k + w_{kj}$, 则令 $l_j \leftarrow l$, $p_j \leftarrow v_k$.

3. 求 $l_i = \min\{l_j \mid v_j \in T_t\}$.

   令 $P \leftarrow P \cup \{v_i\}$, $T \leftarrow T - \{v_i\}$, $k \leftarrow i$.

4. 令 $t \leftarrow t + 1$,

   若 $t < n$, 则转 2.

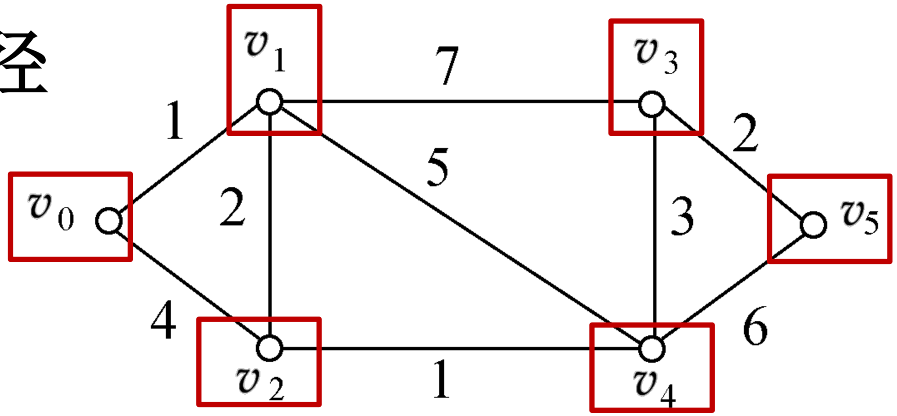
标号法 (E.W.Dijkstra, 1959)

北京郵電大學 Beijing University of Posts and Telecommunications

- 例 求v_0到v_5的最短路径

解：v_0到v_5的最短路径为：

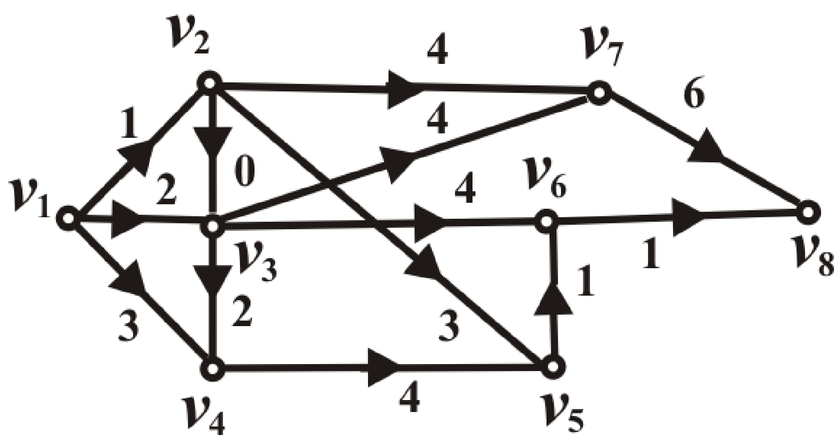
- ➢ $v_0v_1v_2v_4v_3v_5$
- ➢ $d(v_0,v_5)=9$



t	v_0	v_1	v_2	v_3	v_4	v_5
1	$(0, \lambda)^*$	$(+\infty, \lambda)$	$(+\infty, \lambda)$	$(+\infty, \lambda)$	$(+\infty, \lambda)$	$(+\infty, \lambda)$
2		$(1,v_0)^*$	$(4,v_0)$	$(+\infty, \lambda)$	$(+\infty, \lambda)$	$(+\infty, \lambda)$
3			$(3,v_1)^*$	$(8,v_1)$	$(6,v_1)$	$(+\infty, \lambda)$
4				$(8,v_1)$	$(4,v_2)^*$	$(+\infty, \lambda)$
5				$(7,v_4)^*$		$(10,v_4)$
6						$(9,v_3)^*$

关键路径

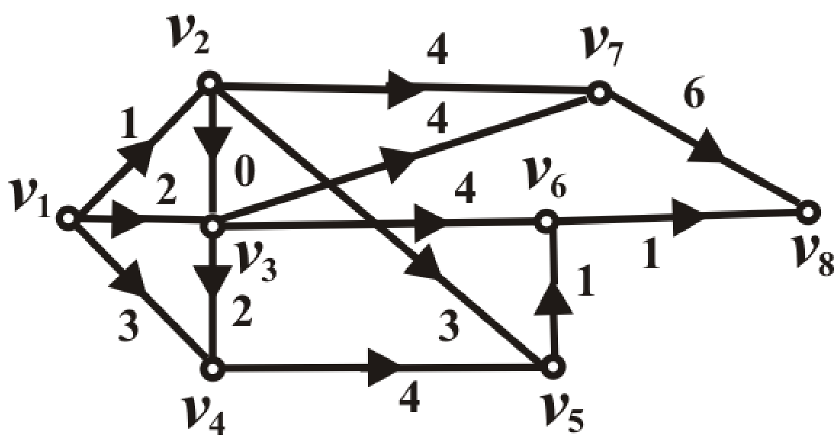
- 例 各事项的最早开始时间:



1. $ES(1) = 0$
2. $ES(2) = \max\{0+1\} = 1$
3. $ES(3) = \max\{0+2, 1+0\} = 2$
4. $ES(4) = \max\{0+3, 2+2\} = 4$
5. $ES(5) = \max\{1+3, 4+4\} = 8$
6. $ES(6) = \max\{2+4, 8+1\} = 9$
7. $ES(7) = \max\{1+4, 2+4\} = 6$
8. $ES(8) = \max\{9+1, 6+6\} = 12$

关键路径

- 例 各事项的最晚完成时间:

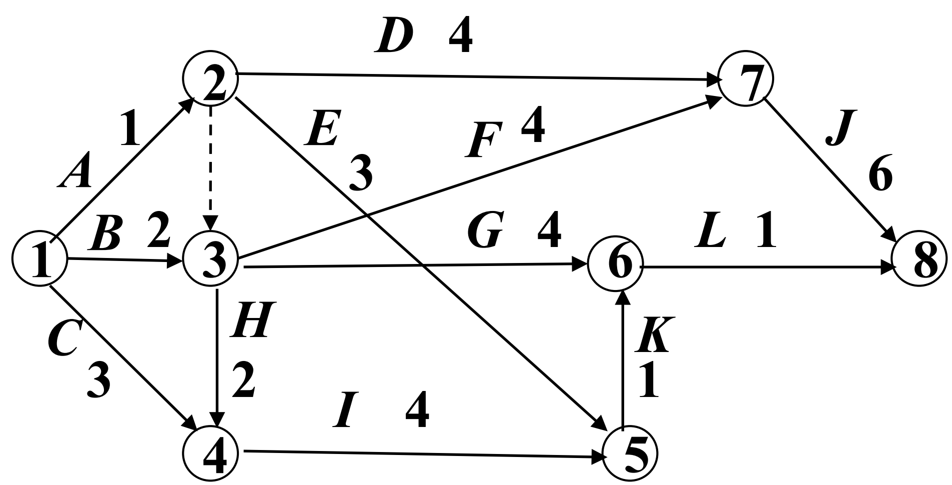


1. $LF(8) = 12$
2. $LF(7) = \min\{12-6\}=6$
3. $LF(6) = \min\{12-1\}=11$
4. $LF(5) = \min\{11-1\}=10$
5. $LF(4)=\min\{10-4\}=6$
6. $LF(3)=\min\{6-2,11-4,6-4\}=2$
7. $LF(2)=\min\{2-0,10-3,6-4\}=2$
8. $LF(1)=\min\{2-1,2-2,6-3\}=0$

关键路径

活动	*A*	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*
ES	0	0	0	1	1	2	2	2	4	6	8	9
EF	1	2	3	5	4	6	6	4	8	12	9	10
LS	1	0	3	2	7	2	7	4	6	6	10	11
LF	2	2	6	6	10	6	11	6	10	12	11	12
SL	1	0	3	1	6	0	5	2	2	0	2	2

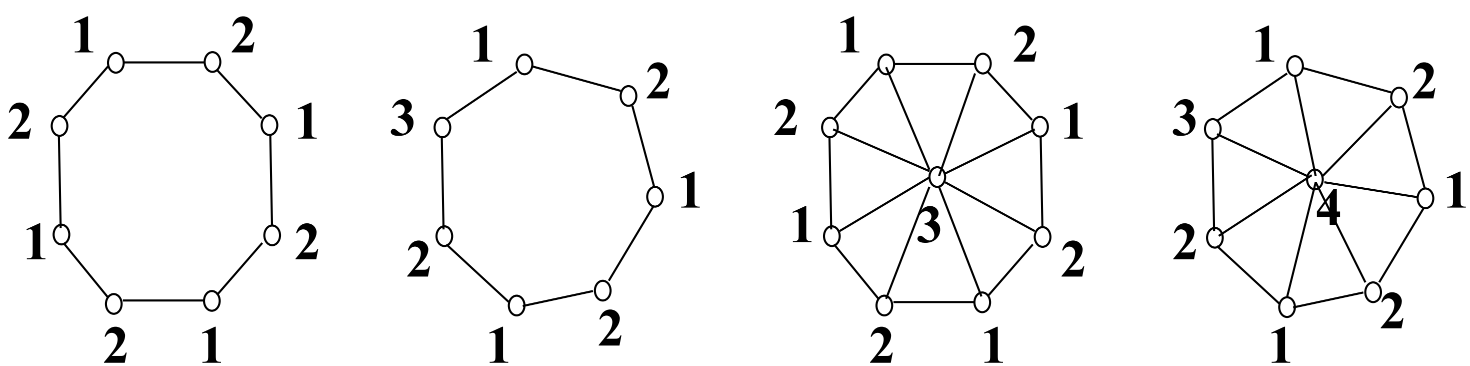
- 总工期: 12天
- 关键路径： $v_1 v_3 v_7 v_8$
- 关键活动: *B*, *F*, *J*



着色

- **定义** 设无向图 G 无环, 对 G 的每个顶点涂一种颜色，使相邻的顶点涂不同的颜色，称为图 G 的一种**点着色**，简称**着色**．若能用k种颜色给G的顶点着色，则称G是**k-可着色**的.
- **图的着色问题**: 用尽可能少的颜色给图着色.

■ 例如



北京邮电大学
Beijing University of Posts and Telecommunications

祝各位同学都取得好成绩