助教：陈剑豪、黄祥、包子恒（计算机811室）

答疑：地点：计算机7楼808室
时间：周五下午1点钟）

周天24：00前提交！

命题逻辑

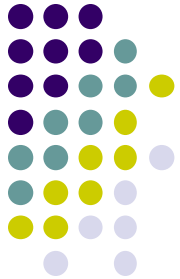
期末：50%

期中：20%

瞿裕忠 教授

南京大学计算机科学与技术系

命题逻辑(1)



- 为何要学数理逻辑？
- 什么是命题？

命题

- 命题是一个陈述语句，即一个陈述事实的句子
  - 要么真，要么假
  - 不能既真又假
- 判断下列句子是否为命题
  - ✓ 税收下降了
  - ✓ 1+1=2
  - ✓ 今天是星期五
  - ✗ 你会说英语吗?
  - ✗ $3-x=5$
  - ✗ 我们走吧!
  - ✓ 任一足够大的偶数一定可以表示为两个素数之和。
  - ✗ 他是个多好的人呀！
  - ✗ “我现在说的是假话。”

原子命题与复合命题

- 复合命题
  - 并非外面在下雨。
  - 张挥与王丽都是三好学生。
  - 张晓静不是江西人就是安徽人。
  - 如果2+3=6，则π是有理数。
  - $\sqrt{3}$是无理数当且仅当加拿大位于亚洲。

复合命题是否为真，取决于：

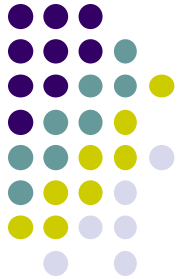
作为复合成分的子命题的真假

逻辑运算符（联接词）的语义

小结

- 为何要学数理逻辑？
  - 日常生活，计算机专业，数学专业
  - 表达，推理
- 什么是命题？
  - 真 或者假，必是其一
  - 复杂命题是原子命题的逻辑组合

命题逻辑(2)

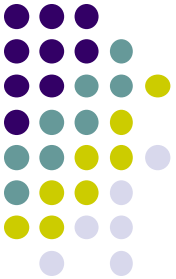


- 命题表达式
  - 命题变元
  - 逻辑运算符

命题变元

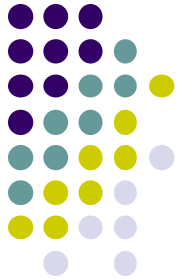
- 一个（原子）命题可以用命题变元来表示
  - p: 该男孩的额头上有泥
  - q: 该女孩的额头上有泥
  - r：1+1=2
- 常用小写字母来表示命题变元，如： p, q, r
- 命题变元的取值范围为： {T, F}，{1, 0}

命题表达式（命题逻辑公式）



- 命题变元是命题表达式；
- 若p是命题表达式，则（$\neg p$）也是；
- 若p和q是命题表达式，则$(p \wedge q)$, $(p \vee q)$, $(p \rightarrow q)$, $(p \leftrightarrow q)$也是；
- 只有有限次应用上述规则形成的符号串才是命题表达式。

命题表达式（命题逻辑公式）



- 哪些是命题表达式？
  - $(p \rightarrow q) \wedge (q \leftrightarrow r)$, $p \rightarrow (q \rightarrow r)$是命题公式（省略了外层括号）
  - $pq \rightarrow r$以及 $p \rightarrow \wedge q$都不是命题公式
  - $p \vee q \rightarrow r$， $\neg p \wedge q$ ， $(\neg p) \wedge q$是命题公式
- 运算符的优先级： $\neg$， $\wedge$， $\vee$， $\rightarrow$，$\leftrightarrow$
- 下面分别介绍这些运算符的确切定义

否定（运算符，联接词）

$\neg p$：“非p”

$\neg p$的真值表

p	$\neg p$
0	1
1	0

p所有可能的取值

合取（运算符）

$p \wedge q$：“p 并且 q”

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

$p \wedge q$=1 iff

p和q均为1

(p,q) 所有可能的取值

析取（运算符）

$p \vee q$：“p 或 q”

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

$p \vee q$=0 iff

p和q均为0

蕴含（运算符）

$p \rightarrow q$：“若 p，则 q”（条件语句） p称为假设，q称为结论

p	q	$p \rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

$p \rightarrow q$ =0 iff

p为1而q为0

关于蕴含

- $p \rightarrow q$：“若 p ，则 q”（条件语句）
- 想得奖，仅当/只有考试得85分以上（想q, 只有p）
  - 考不到85分以上，甭想得奖（ $\neg p \rightarrow \neg q$ ）
  - “得奖” $\rightarrow$ “考试得85分以上” （ $q \rightarrow p$）
- 不能玩游戏，除非做完作业（ $\neg q$, 除非 p ）
  - 没有做完作业，就不能玩游戏（ $\neg p \rightarrow \neg q$ ）

双蕴含（运算符）

$p \leftrightarrow q$：“p当且仅当 q”（双条件语句）

p	q	$p \leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

$p \leftrightarrow q$ =1 iff

p和q有相同的真值

小结

- 命题表达式
  - 命题变元（$p, q, r, \ldots$）
  - 运算符的含义：运算表（基本逻辑电路）
  - 复杂逻辑电路（复杂命题）：由基本逻辑电路组合而来
- 复杂命题表达式
  - 多个命题变元，多个运算符
  - 运算符优先级（$\neg$， $\wedge$， $\vee$， $\rightarrow$，$\leftrightarrow$）可以简化表达式
  - 生活中也有比较复杂的命题表达式（举例）

将自然语言翻译成命题表达式

除非你满16周岁, 否则只要你身高不足4英尺就不能玩游乐车.

假设原子命题如下：

p: 你满16周岁

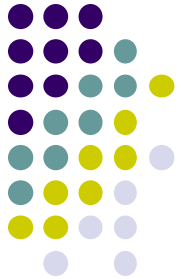
q: 你身高不足4英尺

r: 你能玩游乐车

句子转化为 $p \vee (q \rightarrow \neg r)$，也可以是 $(\neg p \wedge q) \rightarrow \neg r$

备注：这两个命题是逻辑等价的（后面能证明）

命题逻辑(3)



- 命题的真值表
- 命题的逻辑等价
- 常用的命题等价式

命题的真值表

- 含n个变元的一个命题可以看做 $B^n \to B$ 中的一个函数，其中，$B=\{0,1\}$, $B^n = B\times \ldots \times B$.
- 成真指派：对于变元的一种指派（赋值），使得命题为真。
- 成假指派：对于变元的一种指派（赋值），使得命题为假。

$(p\to q)$的成假指派只有一个(1,0), 即 $p=1$, $q=0$.

其他3个都是成真指派

p	q	$p\to q$
0	0	1
0	1	1
1	0	0
1	1	1

真值表举例 $(\neg p \wedge q) \rightarrow \neg r$

3个变元，$2^3=8$个**指派，只有一个成假指派**

p	q	r	$\neg p$	$\neg p \wedge q$	$\neg r$	$(\neg p \wedge q) \rightarrow \neg r$
0	0	0	1	0	1	1
0	0	1	1	0	0	1
0	1	0	1	1	1	1
0	1	1	1	1	0	0
1	0	0	0	0	1	1
1	0	1	0	0	0	1
1	1	0	0	0	1	1
1	1	1	0	0	0	1

永真式、矛盾式

- 永真式（重言式）：取值总是真的，无论其中出现的命题变元如何赋值。比如：$p \vee \neg p$
- 矛盾式：取值总是假的，无论其中出现的命题变元如何赋值。比如：$p \wedge \neg p$

p	$\neg p$	$p \vee \neg p$	$p \wedge \neg p$
1	0	1	0
0	1	1	0

逻辑等价

- φ_1与φ_2等价，记为 $\varphi_1 \equiv \varphi_2$
  - 对任意的变元赋值，φ_1和φ_2取值相同。
  - 也就是说，$\varphi_1 \leftrightarrow \varphi_2$ 是永真式。

命题等价（举例）

$$\neg p \vee q \equiv p \rightarrow q$$

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

命题等价（举例）

$$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$$

p	q	$p \rightarrow q$	$q \rightarrow p$	$(p \rightarrow q) \wedge (q \rightarrow p)$	$p \leftrightarrow q$	$(p \leftrightarrow q) \leftrightarrow ((p \rightarrow q) \wedge (q \rightarrow p))$
0	0	1	1	1	1	1
0	1	1	0	0	0	1
1	0	0	1	0	0	1
1	1	1	1	1	1	1

$(p \leftrightarrow q) \leftrightarrow ((p \rightarrow q) \wedge (q \rightarrow p))$ 永真

常用的逻辑等价(1)

对称

按序

名称	等价
双重否定律	$p \equiv \neg\neg p$
幂等律	$p \equiv p \vee p,\ p \equiv p \wedge p$
交换律	$p \vee q \equiv q \vee p,\ p \wedge q \equiv q \wedge p$
结合律	$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
分配律	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
德摩根律	$\neg(p \vee q) \equiv \neg p \wedge \neg q$ $\neg(p \wedge q) \equiv \neg p \vee \neg q$
吸收律	$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$

常用的逻辑等价(2)

名称	等价
支配律	$p \vee \mathrm{T} \equiv \mathrm{T},\ p \wedge \mathrm{F} \equiv \mathrm{F}$
恒等律	$p \vee \mathrm{F} \equiv p,\ p \wedge \mathrm{T} \equiv p$
排中律	$p \vee \neg p \equiv \mathrm{T}$
矛盾律	$p \wedge \neg p \equiv \mathrm{F}$
	$p \rightarrow q \equiv \neg p \vee q$
	$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$
假言易位	$p \rightarrow q \equiv \neg q \rightarrow \neg p$
	$p \leftrightarrow q \equiv \neg q \leftrightarrow \neg p$
归缪论	$(p \rightarrow q) \wedge (p \rightarrow \neg q) \equiv \neg p$

逆否命题

仅证

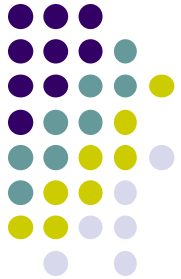
小结

- 命题的真值表
  - 一个函数: $\mathbf{B}^n \rightarrow \mathbf{B}$
- 命题的逻辑等价
  - $\varphi_1 \equiv \varphi_2$ *iff* 对任意的变元赋值，φ_1和φ_2取值相同
  - $\varphi_1 \equiv \varphi_2$ *iff* $\varphi_1 \leftrightarrow \varphi_2$ 永真
- 常用的命题等价式
  - 20个常用等价式，要牢记

命题逻辑(续)

瞿裕忠 教授
南京大学计算机科学与技术系

命题逻辑(4)



- 语义蕴涵
- 推理问题

语义蕴涵（Semantic Entailment）

- $\varphi_1 \vDash \varphi_2$：对于$\varphi_1$的任意一个成真指派，$\varphi_2$均为真

可以是复杂命题

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

举例说明

$\neg p \wedge q \vDash p \rightarrow q$

$\neg p \wedge q \vDash \neg p$

语义蕴涵

- $\varphi_1 \vDash \varphi_2$ iff $(\varphi_1 \rightarrow \varphi_2)$永真

一般情形

- $\varphi_1, \ldots \varphi_n \vDash \varphi$ *iff* $(\varphi_1 \wedge \ldots \wedge \varphi_n \rightarrow \varphi)$永真

- **语义蕴涵可归结为 “判断某个命题是否永真”**

语义蕴涵

- φ 是永真的，iff $\models\varphi$ （φ is valid）
- 举例说明

p	$\neg p$	$p\vee\neg p$
1	0	1
0	1	1

$\models p\vee\neg p$

$p\vee\neg p$ 是永真的

命题逻辑的推理问题

- **给定两个命题，它们是否有语义蕴涵关系?**

  $\varphi_1 \vDash \varphi_2$ *iff* $\varphi_1 \rightarrow \varphi_2$ 永真

- **给定两个命题，它们是否逻辑等价?**

  φ_1与φ_2等价 (记为 $\varphi_1 \equiv \varphi_2$) *iff* $\varphi_1 \leftrightarrow \varphi_2$ 永真

- **给定命题表达式，它是否可满足?**

  φ 可满足 *iff* $\neg\varphi$ 不是永真式

- **上述问题，均可归结为 “判断某个命题是否永真”**

命题逻辑推理（举例）

- $p \wedge q \rightarrow p \vee q$ 是否永真？

$$p \wedge q \rightarrow p \vee q \equiv \neg(p \wedge q) \vee (p \vee q)$$

$$\equiv (\neg p \vee \neg q) \vee (p \vee q)$$

$$\equiv \neg p \vee p \vee \neg q \vee q$$

$$\equiv \mathrm{T}$$

- $\neg(p \rightarrow q)$和$p \wedge \neg q$ 是否逻辑等价？

$$\neg(p \rightarrow q) \equiv \neg(\neg p \vee q)$$

$$\equiv \neg(\neg p) \wedge \neg q$$

$$\equiv p \wedge \neg q$$

SAT（The Satisfiability Problem）

- $(p \vee q) \wedge (\neg p \vee \neg q)$ 是否可满足？若可满足，求成真指派。

  $(p \vee q) \wedge (\neg p \vee \neg q) \equiv ((p \vee q) \wedge \neg p) \vee ((p \vee q) \wedge \neg q)$

  $\equiv (\neg p \wedge q) \vee (p \wedge \neg q)$ //析取范式 DNF

  答案：可满足，当$p=0, q=1$; 或$p=1, q=0$ 时，该命题为真

- 给定命题φ，它是否可满足？即，$\varphi=1$是否有解？
  - 有求解的方法（在下一讲中细说）只有指数级算法
  - 但是还没有时间复杂度在多项式内的算法
  - 该问题是NP完全的（Stephen Cook）

Sudoku谜题（九宫格数独游戏）

- $3^2 \times 3^2$的网格，3^2个3×3的子网格。
- 每行、每列及每宫填入数字1-9且不能重复。

4 →

138	2	9				4		
38	3678	3678	5		4	1		
138	4							
				4	2			
6							7	
5								
7			3					5
2348	1			9				
							6	

Sudoku谜题（SAT问题的应用）

- s_{xyz}：第x行第y列的格子里填上数字z.

$$\bigwedge_{x=1}^{9}\bigwedge_{y=1}^{9}\bigvee_{z=1}^{9}s_{xyz}$$

每行每列存在一个z使其为1.

$$\bigwedge_{x=1}^{9}\bigwedge_{y=1}^{9}\bigwedge_{z=1}^{8}\bigwedge_{i=z+1}^{9}(\neg s_{xyz}\vee\neg s_{xyi})$$

8个数字　没有z　没有z+1.

$$\bigwedge_{x=1}^{9}\bigwedge_{z=1}^{9}\bigvee_{y=1}^{9}s_{xyz}$$

$$\bigwedge_{y=1}^{9}\bigwedge_{z=1}^{9}\bigvee_{x=1}^{9}s_{xyz}$$

……

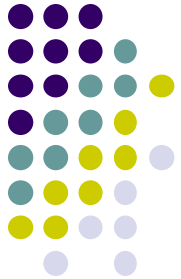
设计Sudoku谜题，使得它有（唯一）解。

开发数独程序，依次加难？引导？

小结

- 语义蕴涵
  - 基于真值表的视角来定义的
  - 命题表达式相当于$\mathbf{B}^n \rightarrow \mathbf{B}$中的函数
- 推理问题
  - 等价问题、蕴涵和可满足问题等推理任务均可归结为“永真”问题
  - **是否有一般的方法来“判断任何给定命题表达式是否永真”?**

命题逻辑(5)



- 命题逻辑的可判定性
- 命题的范式

命题逻辑的判定性

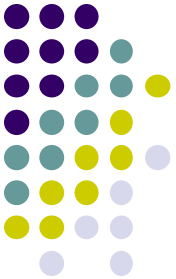
- 命题逻辑的推理问题可归结为：“判定命题的永真性”
- 是否有通用的算法，对任一命题，都能够判断其是否永真？
  - 有的√
- 命题逻辑是可判定的（**decidable**）

命题的合取范式

- **Conjunctive normal form (CNF)**
  - 举例：$(p \vee q) \wedge (\neg p \vee \neg q)$
  - 一般：$\phi = \ldots \wedge (L_1 \vee \ldots \vee L_n) \wedge \ldots$

    L_k 要么是原子命题，要么是原子命题的否定。

命题的合取范式（CNF）



- 求 $(p \rightarrow q) \leftrightarrow r$ 的合取范式
  - $(\neg p \vee q) \leftrightarrow r$ （消去→）
  - $((\neg p \vee q) \wedge r) \vee (\neg(\neg p \vee q) \wedge \neg r)$ （消去↔）
  - $((\neg p \vee q) \wedge r) \vee ((p \wedge \neg q) \wedge \neg r)$ （内移 ¬）
  - $((\neg p \vee q) \vee (p \wedge \neg q \wedge \neg r)) \wedge (r \vee (p \wedge \neg q \wedge \neg r))$ （内移 ∨）
  - $(\neg p \vee q \vee \neg r) \wedge (r \vee (p \wedge \neg q \wedge \neg r))$ （分配律,结合律）
  - $(\neg p \vee q \vee \neg r) \wedge (r \vee p) \wedge (r \vee \neg q)$ //不是永真的，为何？

- 有通用的方法，把任一命题转化与之等价的CNF

CNF的命题，其永真性是可判定的

- 命题逻辑公式的合取范式（CNF）
  - $\ldots \wedge (L_1 \vee L_2 \vee \ldots \vee L_n) \wedge \ldots$
  - L_i 是原子命题、或原子命题的否定
- $L_1 \vee L_2 \vee \ldots \vee L_n$ 的永真性是可判定的
  - $\models L_1 \vee L_2 \vee \ldots \vee L_n$ *iff* 存在i和j, L_i是L_j的否定

$\Rightarrow$ 命题的永真性是可判定的$\Rightarrow$命题逻辑是可判定的

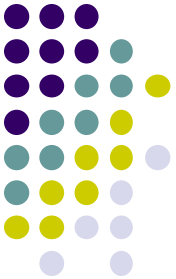
命题的析取范式

- **Disjunctive normal form (DNF)**
  - 举例：$(p \wedge \neg q) \vee (\neg p \wedge q)$
  - 一般：$\phi = \ldots \vee (L_1 \wedge \ldots \wedge L_n) \vee \ldots$

    L_k 要么是原子命题，要么是原子命题的否定。

- 有通用的方法，把任一命题转化与之等价的DNF

命题的析取范式（DNF）



- 求 $(p \rightarrow q) \leftrightarrow r$ 的析取范式
  - $(\neg p \vee q) \leftrightarrow r$ （消去→）
  - $((\neg p \vee q) \wedge r) \vee (\neg(\neg p \vee q) \wedge \neg r)$ （消去↔）
  - $((\neg p \vee q) \wedge r) \vee ((p \wedge \neg q) \wedge \neg r)$ （内移 ¬）
  - $(\neg p \wedge r) \vee (q \wedge r) \vee (p \wedge \neg q \wedge \neg r)$ （内移 ∧）
- 求解该命题的成真指派（SAT）
  - p=0, q=*, r=1, 001, 011
  - p=*, q=1, r=1, 011, 111
  - p=1, q=0, r=0, 100

主析取范式（唯一性）

- 求 $(p \rightarrow q) \leftrightarrow r$ 的主析取范式
  - $(\neg p \wedge r) \vee (q \wedge r) \vee (p \wedge \neg q \wedge \neg r)$ （析取范式）

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

  - $(\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge q \wedge r) \vee (p \wedge \neg q \wedge \neg r)$
  - $(\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (p \wedge q \wedge r)$
  - 001　　011　　100　　111

命题的表达能力

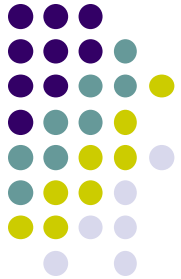
- ***n*个变元的函数/命题表达式（假设变元有顺序）**
  - **成真指派，按自然顺序排列，e.g. 001,011,100,111**
  - **指派的个数为$(2\uparrow^{n}n)$，其子集有$2\uparrow(2\uparrow^{n}n)$ 个**
  - **命题的DNF, e.g. $(\neg p\wedge\neg q\wedge r)\vee(\neg p\wedge q\wedge r)\vee(p\wedge\neg q\wedge\neg r)\vee(p\wedge q\wedge r)$**

- **任何一个 $B^n\rightarrow B$ 的函数，都可以用命题表达式来表示**

小结

- 命题逻辑是可判定的
  - 推理问题一定能够得出Y/N的结果
  - SAT问题是 NP完全的（复杂性理论）
- 命题表达式的范式
  - 合取范式（CNF）适合于 判断命题是否永真
  - 析取范式（DNF）适合于 求解命题的成真指派（SAT）
- 发展趋势：寻找近似算法（比如九宫格游戏）

命题逻辑(6)

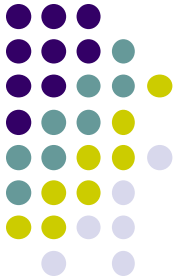


- 基于规则的推理
- 命题逻辑的正确性及完备性

命题逻辑

- **命题表达式**
  - 运算符（ ¬， ∧， ∨， →，↔）
  - 还可以定义其他运算符，比如， ⊕ （对称差）
  - 可以表达 $\mathbf{B}^n \rightarrow \mathbf{B}$中任何一个函数（足够强大）
  - 基本运算符可以裁剪，{¬， ∧， ∨}， {¬， ∧}
- **基于真值表的推理**
  - 永真、可满足、语义蕴涵、等价
- **基于规则的推理?**

命题逻辑的“自然演绎规则”



p

$p \rightarrow q$

$\therefore q$

假言推理

$\neg q$

$p \rightarrow q$

$\therefore \neg p$

取拒式

$p \rightarrow q$

$q \rightarrow r$

$\therefore p \rightarrow r$

假言三段论

$p \vee q$

$\neg p$

$\therefore q$

析取三段论

p

$\therefore p \vee q$

附加律

$p \wedge q$

$\therefore p$

化简律

p

q

$\therefore p \wedge q$

合取律

$p \vee q$

$\neg p \vee r$

$\therefore q \vee r$

消解律

自然演绎规则

- 假言推理 $p,\ p\rightarrow q\ \vdash q$
- 取拒式 $\neg q,\ p\rightarrow q\ \vdash \neg p$
- 假言三段论 $p\rightarrow q,\ q\rightarrow r\ \vdash\ p\rightarrow r$
- 析取三段论 $\neg p,\ p\vee q\ \vdash q$
- 附加律 $p\ \vdash p\vee q$
- 化简律 $p\wedge q\vdash\ p$
- 合取律 $p, q\vdash p\wedge q$
- 消解律 $p\vee q, \neg p\vee r\ \vdash q\vee r$

用推理规则建立论证

- “今天下午不出太阳并且比昨天冷”，“只有今天下午出太阳，我们才去游泳”，“若我们不去游泳，则我们将乘独木舟游览”，“若我们乘独木舟游览，则我们将在黄昏时回家”，结论“我们将在黄昏时回家”。
- p: 今天下午出太阳，
- q: 今天比昨天冷，
- r: 我们将去游泳，
- s: 我们将乘独木舟游览，
- t: 我们将在黄昏时回家。

- $\neg p \wedge q$
- $r \rightarrow p$
- $\neg r \rightarrow s$
- $s \rightarrow t$

用推理规则建立论证

$\neg p \wedge q,\ r \rightarrow p,\ \neg r \rightarrow s,\ s \rightarrow t \vdash\ t$

- $\neg p \wedge q \vdash \neg p$ 化简
- $\neg p,\ r \rightarrow p \vdash \neg r$ 取拒式
- $\neg r,\ \neg r \rightarrow s \vdash s$ **假言推理**
- $s,\ s \rightarrow t \vdash t$ **假言推理**

$$\phi_1, \ldots, \phi_n \vdash \phi$$

在假设的前提下，（多次）使用规则，推导出结论。

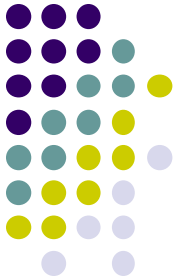
命题逻辑的正确性与完备性

自然演绎规则是正确的，完备的

$$\phi_1,\ldots,\phi_n \vdash \phi \text{ is valid } \textit{iff } \phi_1,\ldots,\phi_n \models \phi \text{ holds}$$

基于自然演绎规则的推导	≡	基于真值表的语义蕴涵

用推理规则及逻辑等价建立论证



- 已知$(p\wedge q)\vee r$和 $r\rightarrow s$, $p\vee s$ 是否为真?
  - $(p\wedge q)\vee r \equiv (p\vee r)\wedge(q\vee r)$
  - $r \rightarrow s \equiv \neg r\vee s$

$(p\vee r)\wedge(q\vee r)$	$\vdash p\vee r$	化简
$p\vee r, \neg r\vee s$	$\vdash p\vee s$	消解

So $(p\vee r)\wedge(q\vee r), \neg r\vee s \vdash p\vee s$

So $(p\wedge q)\vee r, r\rightarrow s \vdash p\vee s$

用语义蕴涵进行推理

- 已知$(p \wedge q) \vee r$和 $r \rightarrow s$, $p \vee s$ 是否为真？

$$(p \wedge q) \vee r ,\ r \rightarrow s \models p \vee s$$

问题转化为：

$$((p \wedge q) \vee r) \wedge (r \rightarrow s) \rightarrow (p \vee s)$$ **是否永真?**

把这个命题表达式转化为CNF（合取范式），即可判断

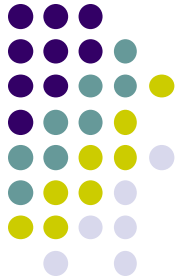
小结

- 基于自然演绎规则的推理是正确的，且完备的
- 命题逻辑的推理（Theorem Proving的一个部分）
  - 命题等价
  - 推理规则
  - 语义蕴涵

谓词逻辑初步

瞿裕忠 教授
南京大学计算机科学与技术系

谓词逻辑(1)



- 引言
- 逻辑公式
  - 谓词
  - 量词

一阶逻辑（first-order logic，FOL）
一阶谓词逻辑（first-order predicate logic）
一阶谓词演算（first-order predicate calculus）

引言

- 知识表示
  - $\forall n\ (odd(n) \rightarrow odd(n^2))$
  - $brother(z, y) \wedge father(y, x) \rightarrow uncle(z, x)$

    // *z is uncle of x*
  - $father(z, y) \wedge father(y, x) \rightarrow grandfather(z, x)$

上述知识无法用命题逻辑表达！

引言

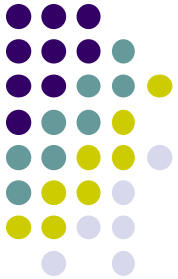
- 任一大于2的偶数都可写成两个质数之和。
  - $\forall n(even(n) \wedge (n>2) \rightarrow \exists m \exists k(p(m) \wedge p(k) \wedge (n = m+k)))$

    $even(n)$: n is a even number 偶数

    $p(x)$: x is a prime number 质数

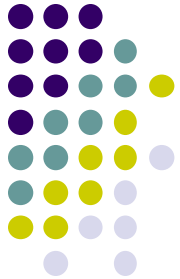
这个断言无法用命题逻辑表达！（命题逻辑的局限性）

谓词（Predicate）



- 如果x是整数，“x 大于2” 不是命题，它的真值依赖于x的取值
  - 可以将“x大于2”表示为 $P(x)$。//论域为实数
- 一元谓词$P(\cdot)$：给定x, $P(x)$ 要么为真，要么为假.
  - 如 $p(x)$: x is a prime number // x是变量，论域为正整数
- 二元谓词$Q(\cdot, \cdot)$
  - 如 $Q(x, y)$：$x=y+3$ // 2个变量
  - 如 $uncle(z, x)$：z *is uncle of* x //论域？

逻辑公式（formula）



原子陈述：

- $P(t_1,\ldots t_n)$，**其中**P**是**n**元谓词，** t_i**是常量、变量或函数取值**

逻辑公式（有时称为“陈述”）：

- **原子陈述是逻辑公式；**
- 若P**是逻辑公式，**x**是自由变量，** 则$\exists xP$和$\forall xP$**是逻辑公式；**
- 若P和Q**是逻辑公式，** 则 $\neg P$, $P\wedge Q$, $P\vee Q$, $P\rightarrow Q$ **是逻辑公式。**

备注：量词的优先级高于其它逻辑运算符。

举例： $\forall x\,(x \le 0 \vee \exists y\,(y>0 \wedge x = y^2))$

量化公式中的变元

- 约束变元
  - $\forall x \exists y(y>x)$ 是 $\forall x(\exists y(y>x))$ 简写，x和y都是约束变元
  - $\exists y(y>x) \wedge \exists z(x>z)$ ，y和z都是约束变元
- 自由变元
  - $\exists y(y>x) \wedge \exists z(x>z)$ ，x是自由变元
  - $\exists y(y>x) \wedge (x+2>y)$，$x$是自由变元，后面那个$y$也是自由变元
- 量词作用域
  - 前面那个$\exists y$的作用域是 $(y>x)$
- 重命名（约束变元）
  - $\exists y(y>x) \wedge (x+2>y) \equiv \exists z(z>x) \wedge (x+2>y)$
  - $\exists y(y>x) \wedge \exists y(x>y) \equiv \exists y(y>x) \wedge \exists z(x>z)$

量化公式的真假

- $\forall x$（全称量词）
  - $\forall x P(x)$ 为真 *iff* 对所有的x, $P(x)$为真

    //论域， domain of discourse
- $\exists x$（存在量词）
  - $\exists x P(x)$为真 *iff* 存在某个x, $P(x)$为真 //论域
- $\forall x(x>2)$为假， $\exists x(x>2)$为真　//论域为实数
- $\forall x \exists y(y>x)$为真，$\exists y \forall x\ (y>x)$为假　//论域为实数

多个量词并用

- $\forall x \forall y P(x,y) \equiv \forall y \forall x P(x,y)$

  举例： $P(x,y)$ **表示** $x+y=y+x$。 **论域为实数集**

- $\exists x \exists y P(x,y) \equiv \exists y \exists x P(x,y)$

  举例： $P(x,y)$ **表示**$x=y+1$。

- $\forall x \exists y P(x,y)$ 与 $\exists y \forall x P(x,y)$ 不一定等价

  举例： $P(x,y)$ **表示“**$y>x$**”。**

语义蕴涵

- $\varphi_1 \vDash \varphi_2$ iff $(\varphi_1 \rightarrow \varphi_2)$永真

一般情形

- $\varphi_1, \ldots \varphi_n \vDash \varphi$ *iff* $(\varphi_1 \wedge \ldots \wedge \varphi_n \rightarrow \varphi)$永真

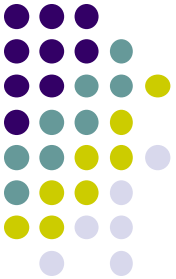
一阶逻辑公式的永真性判定有相当的难度！

$\forall n(even(n) \wedge (n>2) \rightarrow \exists m \exists k(p(m) \wedge p(k) \wedge (n= m+k)))$

哥德巴赫猜想（1740s年），就是这个逻辑公式，至今无法判定其真假

变量的论域（domain of discourse)：无限与有限，天壤之别

将自然语言翻译成逻辑公式



- 任意实数的平方都是正数
  - $\forall x P(x)$，其中 $P(x)$表示$x^2>0$，论域为实数
- 所有美国人都吃汉堡包
  - $\forall x\ C(x)$，其中$C(x)$表示“x吃汉堡包”，论域为美国人
  - $\forall x(A(x)\rightarrow C(x))$ //论域为人类
  - $A(x)$表示“x是美国人”， $C(x)$表示“x吃汉堡包”
- 有的政治家是诚实的
  - $P(x)$表示“x是政治家”， $H(x)$表示“x是诚实的”
  - $\exists x(P(x)\wedge H(x))$ //外层的( )不能缺 //论域为政治家

将自然语言翻译成逻辑公式

这个班上的每个学生都学过微积分课程.

$S(x)$: x是这个班上的学生

$C(x)$: x学过微积分课程

$\forall x\,(S(x) \rightarrow C(x))$

这个班上的每个学生都或去过加拿大，或去过墨西哥.

$\forall x\,(S(x) \rightarrow V(x, c) \vee V(x, m))$

其中，c代表“加拿大”， m代表“墨西哥”，

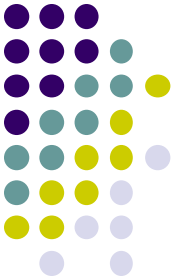
$V(x, y)$表示“x访问过（去过）y”

小结

- 逻辑公式
  - 原子公式（谓词：由具体应用需求而定）
  - 量化公式（量词：∀，∃）
  - 逻辑运算符（¬，∧，∨，→）

  谓词、变量和量词的引入，增强了逻辑表达能力
- 语义蕴涵
  - 可归结为判断逻辑公式的永真性
  - 论域的无限性，加深了推理的困难

谓词逻辑(2)



- 常用逻辑等价式
- 基于规则的推理
- FOL的一些定论

常用逻辑等价式

- $\neg\forall xP(x) \equiv \exists x\neg P(x)$
  - $\forall xP(x)$: **对所有实数x, 其平方是正数** // $P(x)$表示$x^2>0$
  - **否定：存在某个实数 x, 其平方不是正数。**
- $\neg\exists xP(x) \equiv \forall x\neg P(x)$
  - $\exists xP(x)$: **存在实数x，x的平方是正数.**
  - **否定：对任意实数x, 其平方不是正数**

常用逻辑等价式

- $\forall x(P(x)\wedge Q(x)) \equiv (\forall xP(x)) \wedge (\forall xQ(x))$
- $\exists x(P(x)\vee Q(x)) \equiv (\exists xP(x)) \vee (\exists xQ(x))$

反向蕴涵×：是奇数或偶数

- $(\forall xP(x)) \vee (\forall xQ(x)) \models \forall x(P(x) \vee Q(x))$
- $\exists x(P(x) \wedge Q(x)) \models (\exists xP(x)) \wedge (\exists xQ(x))$

- $\forall x(P(x) \vee R) \equiv (\forall xP(x)) \vee R$
- $\exists x(P(x) \wedge R) \equiv (\exists xP(x)) \wedge R$

R与x无关.

常用逻辑等价式（可以证明）

- $\forall x(R \rightarrow P(x)) \equiv R \rightarrow \forall x P(x)$
- $\exists x(R \rightarrow P(x)) \equiv R \rightarrow \exists x P(x)$
- $\forall x(P(x) \rightarrow R) \equiv (\exists x P(x)) \rightarrow R$
- $\exists x(P(x) \rightarrow R) \equiv (\forall x P(x)) \rightarrow R$

$\forall x(\neg R \vee P(x)) \equiv \neg R \vee (\forall x P(x))$

特殊化.

等价. 找出一个特合的x.

$\exists x(\neg P(x) \vee R) \equiv (\exists x \neg P(x)) \vee R \equiv \neg(\forall x P(x)) \vee R$

注意：这里x不在R中出现

前束范式（Prenex Normal Form）

$\forall x\,(x \le 0 \vee \exists y\,(y>0 \wedge x = y^2))$ //不是前束范式

$\forall x\,\exists y\,(x \le 0 \vee (y>0 \wedge x = y^2))$ //前束析取范式

有通用方法，把任意一阶逻辑公式转化为PNF（PDNF/PCNF）

转化为前束范式（举例说明）

$\exists z(\exists x Q(x, z) \vee \exists x P(x)) \rightarrow \neg(\neg \exists x P(x) \wedge \forall x \exists z Q(z, x))$

$\equiv \neg \exists z(\exists x Q(x, z) \vee \exists x P(x)) \vee \neg(\neg \exists x P(x) \wedge \forall x \exists z Q(z, x))$ （消去$\rightarrow$）

$\equiv \forall z(\forall x \neg Q(x, z) \wedge \forall x \neg P(x)) \vee (\exists x P(x) \vee \exists x \forall z \neg Q(z, x))$ （内移 $\neg$ ）

$\equiv \forall z \forall x(\neg Q(x, z) \wedge \neg P(x)) \vee \exists x(P(x) \vee \forall z \neg Q(z, x))$ （简化）

$\equiv \forall z \forall x(\neg Q(x, z) \wedge \neg P(x)) \vee \exists y(P(y) \vee \forall w \neg Q(w, y))$ （重命名）

$\equiv \forall z \forall x \exists y((\neg Q(x, z) \wedge \neg P(x)) \vee P(y) \vee \forall w \neg Q(w, y))$ （前移量词）

$\equiv \forall z \forall x \exists y \forall w((\neg Q(x, z) \wedge \neg P(x)) \vee P(y) \vee \neg Q(w, y))$ （前移量词）

$\equiv \forall z \forall x \exists y \forall w((\neg Q(x, z) \vee P(y) \vee \neg Q(w, y)) \wedge (\neg P(x) \vee P(y) \vee \neg Q(w, y)))$

前束合取范式PCNF

前束合取范式（举例说明）

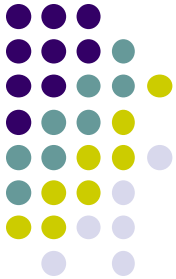
$$\forall z \forall x \exists y \forall w((\neg Q(x, z) \vee P(y) \vee \neg Q(w, y)) \wedge (\neg P(x) \vee P(y) \vee \neg Q(w, y)))$$

$$\forall x \forall y \forall z ((\neg B(z, y) \vee \neg F(y, x) \vee U(z, x)) \wedge (\neg F(z, y) \vee \neg F(y, x) \vee G(z, x)))$$

$$brother(z, y) \wedge father(y, x) \rightarrow uncle(z, x)$$

$$father(z, y) \wedge father(y, x) \rightarrow grandfather(z, x)$$

Prolog (Programming in Logic)



- 若z是y的兄弟，且y是x的父亲，则z是x的叔叔。
  - $brother(z, y) \wedge father(y, x) \rightarrow uncle(z, x)$

```
uncle(z, x) :- brother(z, y), father(y, x)
```

- 事实
  - *brother*(*Klopp*, *Karl*)
  - *brother*(*Klinsmann*, *Karl*)
  - *brother*(*Karl*, *Loew*)
  - *father*(*Karl*, *Neuer*)
- 查询：？ *uncle*(*z*, *Neuer*)

量词相关的“自然演绎规则”

$\forall x\, P(x)$

$\therefore P(c)$

全称例示

$P(c)$对任意的c

$\therefore\ \forall x\, P(x)$

全称生成

$\exists x\, P(x)$

$\therefore P(c)$对于某个c

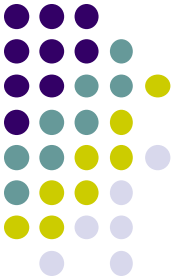
存在例示

$P(c)$对某个c

$\therefore\ \exists x\, P(x)$

存在生成

基于规则的推理（举例）



- **前提**
  - 在这个班上的某个学生没有读过这本书
  - 班上的每个人都通过了第一门考试
- **结论：通过第一门考试的某个人没有读过这本书**
- **$C(x)$: x在这个班上**
- **$B(x)$: x读过这本书了**
- **$P(x)$: x通过了第一门考试**
  - $\exists x(C(x) \wedge \neg B(x))$
  - $\forall x(C(x) \rightarrow P(x))$
  - $\exists x(P(x) \wedge \neg B(x))$

基于规则的推理（举例）

$\exists x(C(x) \wedge \neg B(x)), \forall x(C(x) \rightarrow P(x)) \Rightarrow \exists x(P(x) \wedge \neg B(x))$

因为 $\exists x(C(x) \wedge \neg B(x))$ **//这是前提**

根据存在例示，有某个a，$C(a) \wedge \neg B(a)$**成立。**

根据化简，得到$C(a)$ **成立，** $\neg B(a)$**成立。**

因为$\forall x(C(x) \rightarrow P(x))$ **//这是前提**

根据全称例示，得到 $C(a) \rightarrow P(a)$

根据**假言推理**，得到 $P(a)$

根据合取律，得到 $P(a) \wedge \neg B(a)$

根据存在生成，得到 $\exists x(P(x) \wedge \neg B(x))$

一阶谓词逻辑的定论

自然演绎规则（含量词相关的）是正确的、完备的

不可判定的（Undecidable）

No program exists which, given any ϕ, decides whether $\vDash \phi$

小结

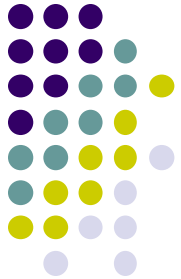
- 常用逻辑等价式
- 前束范式
  - 转化方法
  - 逻辑公式的复杂性
- 基于规则的推理
  - 量词相关的“自然演绎规则”
  - 自然演绎规则的正确性与完备性
- **一阶谓词逻辑的不可判定性及推理复杂性**

证明方法

瞿裕忠 教授

南京大学计算机科学与技术系

证明方法(1)



- 引言
- 证明方法（上）

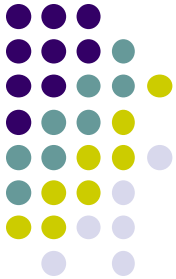
引言

- 定理（Theorem）
  - 能够被证明为真的陈述，通常是比较重要的陈述。
- 证明（Proof）
  - 表明陈述（定理）为真的有效论证。
- 定理证明中可以使用的陈述
  - （当前）定理的前提
  - 术语的定义
  - 公理（假定）
  - 已经证明的定理（推论、命题、引理）

引言

- 定理的陈述（举例）
  - **如果$x>y$，其中x和y是正实数，那么 $x^2>y^2$。**
- **形式化表示（逻辑公式）**
  - **对所有正实数x和y，如果$x>y$，那么 $x^2>y^2$。**
  - $\forall x \forall y((x>y) \rightarrow (x^2>y^2))$ //论域为**正实数**
- **如何证明**
  - 定理的陈述为：$\forall x\ \forall y\ (P(x, y) \rightarrow Q(x, y))$
  - **先证明，对论域中的任一元素a和b, $P(a, b) \rightarrow Q(a, b)$**
  - **再使用全称生成，得到$\forall x \forall y\ (P(x, y) \rightarrow Q(x, y))$**

引言

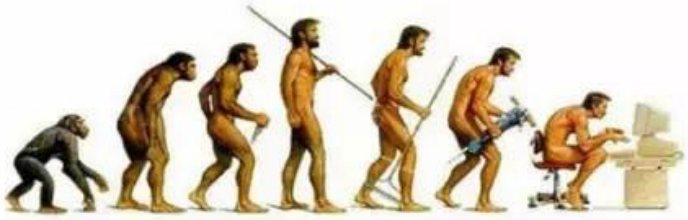


- **更严格的证明**
  - **对论域中的任一元素a，要证明 $\forall y\,(P(a, y)\rightarrow Q(a, y))$**
    - **对论域中的任一元素b,** 给出 $P(a, b)\rightarrow Q(a, b)$ 的证明
    - **再使用全称生成，得到**$\forall y\,(P(a, y)\rightarrow Q(a, y))$
  - **再使用全称生成，得到**$\forall x\forall y\,(P(x, y)\rightarrow Q(x, y))$
- 有效的证明方法
  - 明确的证明框架，比如，反证法（广义）和数学归纳法
  - 严格的逻辑基础（遵循一阶谓词逻辑的有效论证）

引言 有效的证明方法

- **猜想（conjecture）**
  - **尚未被证明为真的陈述，通常是比较重要的陈述。**
  - **尚未有效论证，也没有被证伪。//哥德巴赫猜想**

备注：一阶谓词逻辑是不可判定的



猜想

有效的证明方法

公理 定理 理论

概念：C_1,… …, C_m

术语：T_1,… …, T_n

引言

- 证明方法
  - 逻辑基础
  - 基本框架
- 证明方法（上）
  - 直接证明
  - 反证法
  - 归谬法
  - 等价性证明

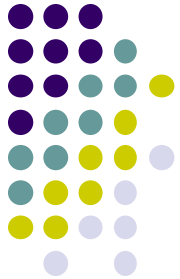
直接证明

- 定义
  - 整数n是偶数，如果存在一个整数k使得n=2k;整数n是奇数，如果存在一个整数k使得n=2k+1。
  - 备注：一个整数要么是偶数，要么是奇数。
- 定理：若n是奇数，则n^2是奇数。 $\forall n\ (Odd(n) \rightarrow Odd(n^2))$
  - 任意给定一个奇数n，存在一个整数k ， n=2k+1
  - $n^2=2(2k^2+2k)+1$
  - n^2是奇数
  - 所以，对任意奇数n，n^2是奇数。

反证法 证明逆否命题

- 原理
  - $p \rightarrow q \equiv \neg q \rightarrow \neg p$
- 证明框架
  - $\neg q \vdash \neg p$
  - 所以，$p \rightarrow q$ 成立

反证法（举例）

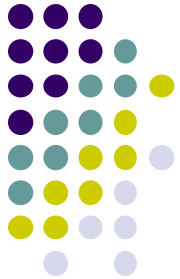


- **若3n+2是奇数，则n是奇数。**
  - //直接证明的设想不奏效。3n+2 =2k+1 ⇒？
  - 假设结论不存立($\neg q$)
  - n是偶数，存在一个整数k使得n=2k
  - 3n+2=2(3k+1)
  - 3n+2是偶数 ($\neg p$)
  - 因此，若3n+2是奇数，则n是奇数 ($p \rightarrow q$)

归谬法

- 原理
  - $q \equiv \neg q \rightarrow \mathbf{F}$
- 证明框架
  - $\neg q \vdash$ **Contradiction**（矛盾，比如$r \wedge \neg r$)
  - 所以，q 成立

归谬法（举例）

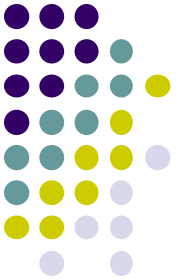


- **There is no rational number whose square is 2.**
- **Proof**
  - **Extra hypothesis: $(p/q)^2=2$, and *p,q* are integers which have no common factors except for 1.**
  - **Then, $p^2=2q^2 \Rightarrow p^2$ is even $\Rightarrow p$ is even $\Rightarrow p^2$ is multiple of 4 $\Rightarrow q^2$ is even $\Rightarrow q$ is even $\Rightarrow p, q$ have 2 as common factor $\Rightarrow$ *contradiction***

反证法（广义）

- 原理
  - $p_1 \wedge ... \wedge p_n \rightarrow q \equiv \neg q \wedge p_1 \wedge ... \wedge p_n \rightarrow \mathbf{F}$
- 证明框架
  - $\neg q, p_1, ..., p_n \vdash$ **Contradiction**（矛盾，比如$p_1 \wedge \neg p_1$)
  - 所以， $p_1 \wedge ... \wedge p_n \rightarrow q$

反证法（广义）:史上最难奥数题



- 设正整数a, b满足$ab+1$可以整除a^2+b^2，证明 $(a^2+b^2)/(ab+1)$ 是某个整数的平方。（传奇的第6题，IMO 1988）
- 证明. 采用广义反证法，设有正整数a及b满足 $(a^2+b^2)/(ab+1)=k$，其中k是非平方数的正整数。

  在满足条件的众多组正整数a、b中，必有一组他们的和是最小的，我们设它为a_1与b。不妨假设 $a_1 \geq b$。

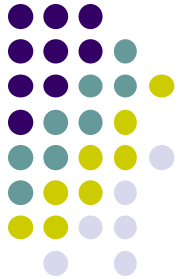
  无穷递降法，找到另一组a_2和b满足条件，但是 $a_2 < a_1$，产生矛盾。

  - $x^2 - kbx + (b^2-k) = 0 \leftrightarrow (x^2+b^2) = k(xb+1)$
  - $a_1 + a_2 = kb \rightarrow a_2$为整数$\rightarrow a_2 \geq 0$
  - $a_1 a_2 = b^2-k \rightarrow a_2 = (b^2-k)/a_1 < a_1$ 且$a_2 \neq 0$

等价性证明

- 原理
  - $[p_1 \leftrightarrow p_2 \leftrightarrow \ldots \leftrightarrow p_n] \leftrightarrow [(p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \ldots \wedge (p_n \rightarrow p_1)]$
- 证明框架
  - $p_1 \vdash p_2$
  - $p_2 \vdash p_3$
  - …
  - $p_n \vdash p_1$
  - 因此，$p_1 \leftrightarrow p_2 \leftrightarrow \ldots \leftrightarrow p_n$。

证明方法(2)

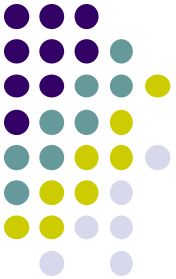


- 证明方法（下）
  - 分情形证明
  - 存在性证明
  - 唯一性证明
  - 寻找反例
- 数学与猜想

分情形证明

- 原理
  - $p_1 \vee \ldots \vee p_n \rightarrow q \equiv (p_1 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)$
- 证明框架
  - $p_1 \vdash q$
  - …
  - $p_n \vdash q$
  - 因此，$p_1 \vee \ldots \vee p_n \rightarrow q$

分情形证明（举例）



- 当n是一个正整数，且$n \le 4$时，$(n+1)^3 \ge 3^n$。
  - n=1, 2, 3, 4.（穷举）
- 当n是一个整数时，有$n^2 \ge n$。
  - $n \le 0$
  - $n \ge 1$
- $(x+y)^r < x^r+y^r$, 这里x, y是正实数, r是$0<r<1$的实数.
  - 不失一般性，假设$x+y=1$. 否则，令$x' = x/(x+y)$, $y' = y/(x+y)$
  - $x < x^r$， $y < y^r \Rightarrow x+y < x^r+y^r \Rightarrow (x+y)^r < x^r+y^r$

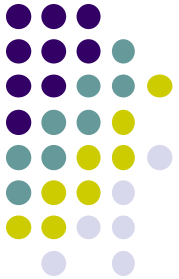
存在性证明

- 证明目标
  - $\exists x\, P(x)$
- 构造性证明
  - 存在这样的正整数，有两种方式表示为正整数的立方和。
  - $1729=10^3+9^3=12^3+1^3$
- 非构造性证明
  - 存在无理数x和y 使得x^y是有理数
  - $y^2=2$，$x=y^y$，$x^y=(y^y)^y=y^2=2$
  - 若x是无理数， x和y即为所求；否则，y和y即为所求。

唯一性证明

- **证明目标**
  - $\exists x\,(P(x) \wedge \forall y\,(y \neq x \rightarrow \neg P(y))\,)$
  - $\exists x\,P(x) \wedge \forall y\,\forall z\,(P(y) \wedge P(z) \rightarrow y = z)$
- **举例，设$a \neq 0$, $ax+b=c$有唯一的解。**

寻找反例



- **原理**
  - $\neg\forall x\, P(x) \equiv \exists x\, \neg P(x)$
- 举例
  - 每个正整数都是两个整数的平方和
  - **3**
  - 每个正整数都是三个整数的平方和
  - **7**
  - 每个正整数都是四个整数的平方和？

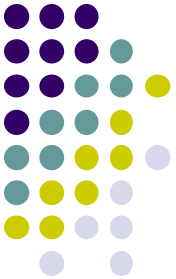
证明中的错误

- **以下证明“2=1”，错在哪里?**
- $a=b$ **假设a和b是两个相等的正整数**
- $a^2=ab$ **两边乘以a**
- $a^2-b^2=ab-b^2$ **两边减去b^2**
- $(a-b)(a+b)=(a-b)b$
- $(a+b)=b$ **两边除以$(a-b)$**
- $2b=b$
- $2=1$

数学与猜想（费马大定理）

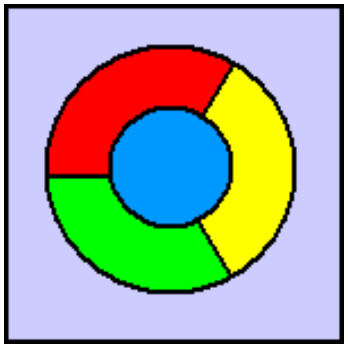
- **Pierre de Fermat (1601-1665), France**
  - **Fermat's Last Theorem (1637)** （费马大定理）
  - $x^n+y^n=z^n$ (n>2, $xyz\neq0$)没有整数解
- **Andrew Wiles (1953-), Oxford, England**
  - **1994/1995完成了费马大定理的证明（约10年时间）**
  - **椭圆曲线理论**

数学与猜想（哥德巴赫猜想）



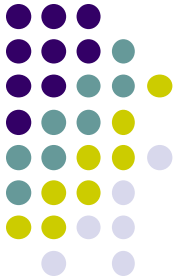
- **Goldbach Conjecture**（1742年给欧拉的信中）
  - 任一大于2的整数都可写成三个质数之和。
- 欧拉版本（在给哥德巴赫的回信中）
  - 任一大于2的偶数都可写成两个质数之和。
  - $\forall n(even(n)\wedge(n>2)\rightarrow\exists m\exists k(p(m)\wedge p(k)\wedge(n=m+k)))$
- “*a*+*b*”猜想
  - 任一充分大的偶数都可以表示成为一个素因子个数不超过*a*个的数与另一个素因子不超过*b*个的数之和。
- 1966年陈景润（1933－1996）证明了“1+2”猜想

数学与猜想（四色猜想）



- **Four Color Theorem**
  - **Proposed by Francis Guthrie in 1852**
  - **Proven in 1976 by Kenneth Ira Appel (1932-2013) and Wolfgang Haken (1928-)**
    - **Percy John Heawood (1861-1955, Britain) proved the five color theorem in 1890**

世界数学难题



- **Hilbert's problems (23), ICM'1900, Paris**
- **Millennium Prize Problems (7) by the Clay Mathematics Institute in 2000**

1. P versus NP problem

2. Hodge conjecture

3. Poincaré conjecture (solved by Perelman)

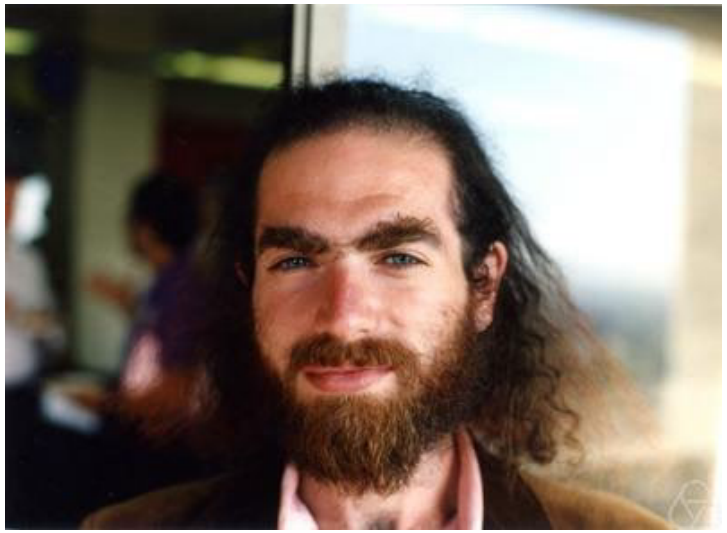
4. Riemann hypothesis

5. Yang–Mills existence and mass gap

6. Navier–Stokes existence and smoothness

7. Birch and Swinnerton-Dyer conjecture

Grigori Perelman (1966-, Russian)



In November 2002, Perelman posted the first of a series of eprints to the arXiv, ...

He declined to accept

Fields Medal award in 2006

Millennium Prize award in 2010

小结

- 证明方法的重要性
- 有难度的证明
  - 广义反证法
  - 分情形证明法
  - 数学归纳法
- 猜想的重要性

集合及其运算

瞿裕忠 教授

南京大学计算机科学与技术系

集合及其运算(1)

- 集合及其描述
- 集合相等、子集关系
- 幂集、笛卡尔乘积

集合的定义

- 直观的定义
  - 一个集合是一组无序的对象，这些对象称为这个集合的元素或成员。
  - $a \in A$表示a是集合A的一个成员， $a \notin A$ 表示a不是A的成员。
- **Georg Cantor**的描述
  - **A set is a collection into a whole of definite, distinct objects of our intuition or our thought. The objects are called elements (member) of the set.**

Naïve set theory，朴素集合论

集合的描述

- 罗列、枚举
  - $V=\{a, e, i, o, u\}$
  - $\{1, 3, 5, 7, 9\}$
- 集合构造符号
  - $Z^{+}=\{x \in Z \mid x>0\}$
  - $Q=\{ p/q \mid p \in Z , q \in Z, q \neq 0\}$
  - $[a, b]=\{x \in R \mid a \leq x \leq b\}$

$N=\{0, 1, 2, 3, \ldots\}$

$Z=\{\ldots, -2, -1, 0, 1, 2, \ldots\}$

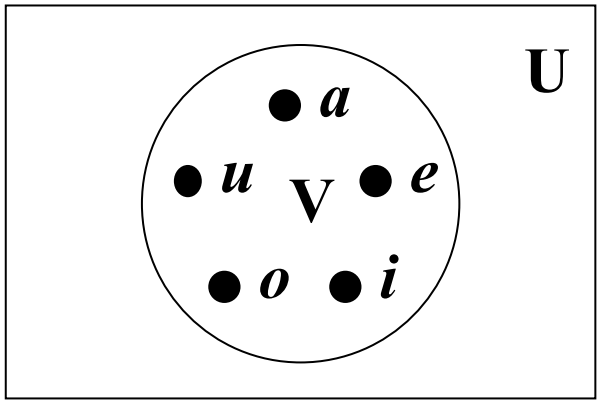
R: 实数集

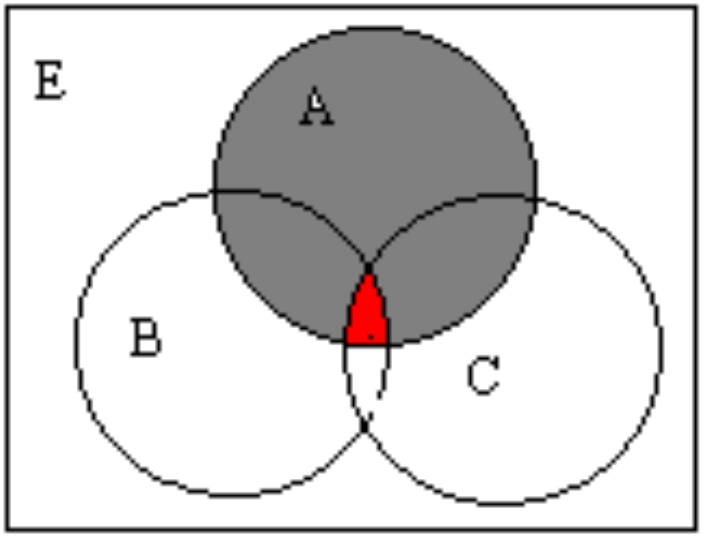
$\{N, Z, Q, R\}$

$\{\}$ 空集

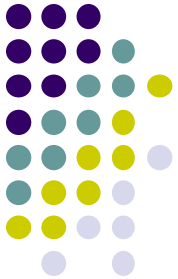
集合的描述

- 文氏图（Venn diagrams ）//John Venn 韦恩图





集合相等、子集关系



- 集合相等当且仅当它们有同样的元素
  - **A=B** 当且仅当 $\forall x(x \in A \leftrightarrow x \in B)$ //外延原则
- 集合A称为集合B的子集， 记作$A \subseteq B$
  - $\forall x\,(x \in A \rightarrow x \in B)$
- 如果$A \subseteq B$, 但$A \neq B$，则A是B的真子集，记作$A \subset B$
- 对任意集合A和B, A=B 当且仅当:
  - $A \subseteq B$, 且$B \subseteq A$

子集关系的一个性质

- 证明：如果$X \subseteq Y$且$Y \subseteq Z$, 则$X \subseteq Z$
- 要证明：“对任意的 a, 如果 $a \in X$, 则 $a \in Z$”
- 证明：
  - 对任意的 $a \in X$
  - 根据已知的“$X \subseteq Y$”，可得：$a \in Y$
  - 根据已知的“$Y \subseteq Z$”，可得：$a \in Z$
  - 所以，$\forall a\,(a \in X \rightarrow a \in Z)$, 即$X \subseteq Z$

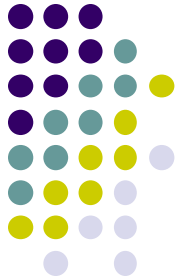
空集

- 存在一个没有任何元素的集合：空集Ø
- 关于空集的一些性质：
  - 空集是任何集合的子集。
    - $\emptyset \subseteq A$，即 $\forall x(x \in \emptyset \rightarrow x \in A)$
  - 空集是唯一的，可以用 Ø表示
    - 如果 $\emptyset_1, \emptyset_2$都是空集，则 $\emptyset_1 \subseteq \emptyset_2$ 和 $\emptyset_2 \subseteq \emptyset_1$ 均为真

关于空集的讨论

- 空集本身可以是一个对象，可以是某个集合的元素
  - $\emptyset \in \{\emptyset\}, \emptyset \subseteq \{\emptyset\}$ 集合可以作为一个元素
- 事实上，我们从空集开始构造整个集合世界！
  - 自然数
  - 有理数
  - 实数（幂集运算）
  - …

有限集合的基数（大小）

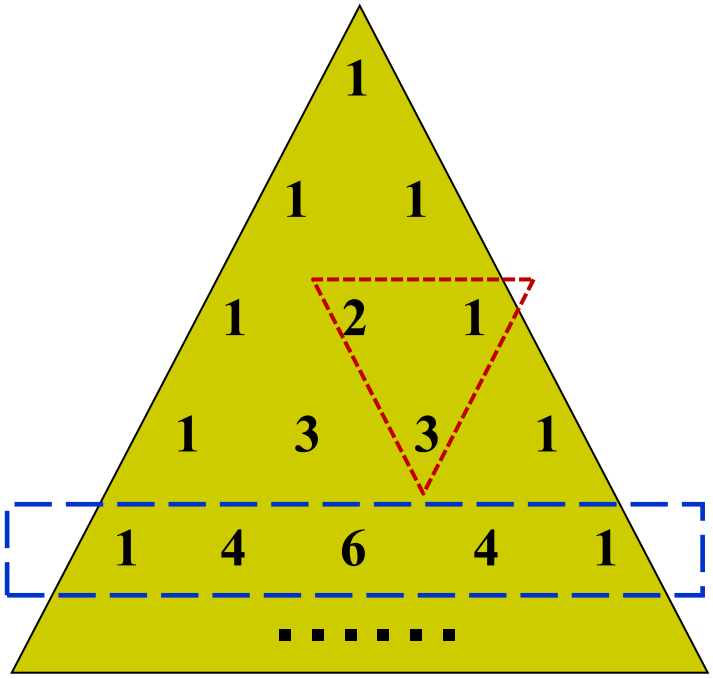


- 有限集合及其基数
  - 若S恰有n个不同的元素，n是自然数，就说S是有限集合，而n是S的基数，记作$|S|=n$。
- 无限集合
  - 如果一个集合不是有限的，就说它是无限的。

幂集

- S是一个集合，S的幂集是S的所有子集的集合
  - $\rho(S)=\{x \mid x \subseteq S\}$
- 举例
  - $\rho(\{a, b\}) = \{\varnothing,\{a\},\{b\},\{a, b\}\}$
  - $\rho(\varnothing) = \{\varnothing\}$
  - $\rho(\{\varnothing\}) = \{\varnothing, \{\varnothing\}\}$
- △ $\rho(N)$，N的一个子集对应于一个“0~1无穷序列”
  - 空集 → 000…　0代表不属于该子集
  - 全集 → 111…

有限集合的所有子集



A={1, .., *n*}

如果 |A|=*n*, 则 |ρ(A)|=2^n $|P(A)| = 2^{|A|}$

幂集的另一种记法: 2^A $P(A) = 2^A$

$C_n^r = C_{n-1}^{r-1} + C_{n-1}^r$

C(*n*, *r*) = C(*n*-1, *r*-1) + C(*n*-1, *r*)

$C_4^0 + C_4^1 + C_4^2 + C_4^3 + C_4^4 = 2^4$

C(4, 0)+ C(4, 1)+ C(4, 2)+ C(4, 3)+ C(4, 4) =2^4

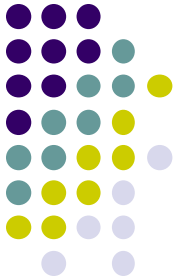
$\Sigma_{k=0\ldots n}\, C(n, k) = 2^n$

$$\sum_{k=0}^{n} C_n^k = 2^n$$

笛卡尔乘积

- 集合A和B的笛卡尔乘积
  - $A\times B=\{(a, b)\mid a\in A \wedge b\in B\}$
- 何种情形下，$A\times B=B\times A$ $A=B \vee (A=\phi \vee B=\phi)$
- 集合$A_1, A_2, \ldots, A_n$的笛卡尔乘积
  - $A_1\times A_2\times \ldots \times A_n=\{(a_1, a_2, \ldots, a_n)\mid a_i\in A_i, i=1,2,\ldots n\}$

集合与谓词逻辑



- 在量化逻辑公式中使用集合符号
  - $\forall x \in S(P(x))$代表$\forall x(x \in S \rightarrow P(x))$
  - $\exists x \in S(P(x))$代表$\exists x(x \in S \wedge P(x))$
  - 举例
    - $\forall x \in R(x^2 \geq 0)$: $\forall x(x \in R \rightarrow (x^2 \geq 0))$
    - $\exists x \in Z(x^2 = 1)$: $\exists x(x \in Z \wedge x^2 = 1)$
- 逻辑公式的真值集合，$\{x \in D \mid P(x)\}$
  - 举例： $\{x \in R \mid |x| = x\}$， $\{x \in R \mid x^2 = 2\}$， $\{x \mid x \in R \wedge x^2 = 2\}$

集合悖论

- $A=\{x \mid P(x)\}$, 实际上不能保证：对任意的性质 P，这样的定义都有意义。 存在矛盾
- 例如：
  - 是否有这样的集合，它包含所有“不以自己为元素的集合”
  - $\{x|x\notin x\}$是否存在？
- **Russell 悖论**

  定义 $R=\{x \mid x\notin x\}$。如果R存在，则有: $R\in R$ *iff* $R\notin R$
  - 理发师悖论：“我给所有不给自己理发的人理发”

公理集合论（Axiomatic set theory）

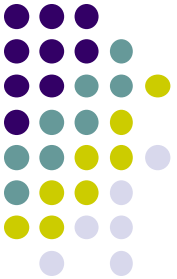
- 用公理来约束集合世界，以摆脱悖论
  - 集合相等（=）和元素属于集合的关系（∈）
  - 给定合法集合构造原则，即若干种集合存在性
- Zermelo–Fraenkel set theory with the axiom of Choice（策梅洛-弗兰克尔集合论，ZFC集合论）参见附录

外延公理	替代公理模式
正则公理	无穷公理
分离公理模式	幂集公理
配对公理	选择公理
并集公理	

小结

- 构造集合的有效途径
  - 枚举
  - 递归定义
  - 逻辑公式限定
  - 幂集
  - 笛卡尔乘积
  - 其他运算（下一讲）
- 公理集合论：集合构造原则

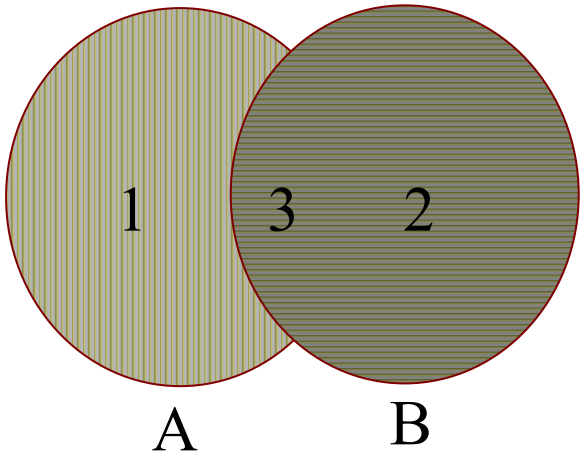
集合及其运算(2)



- 并、交、补
- 集合恒等式
- 集合相关性质的证明方法
- 其他运算（对称差、广义并/交）

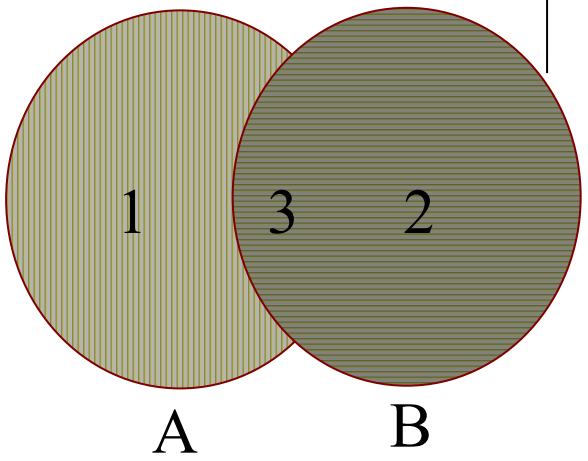
集合运算：并、交

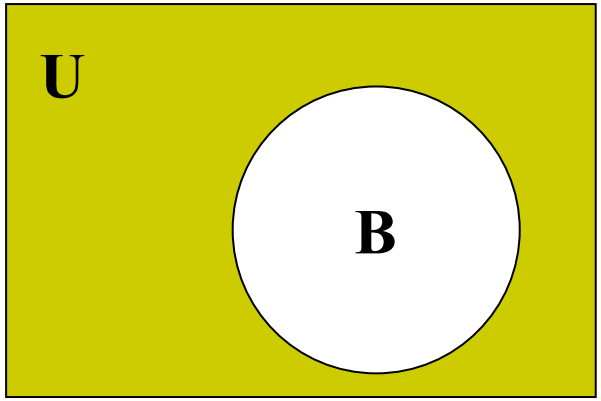
- 运算定义的基本方式：将结果定义为一个新的集合
  - 并：$A \cup B = \{ x \mid x \in A \vee x \in B \}$
    - 并集: {1, 2 , 3}
  - 交：$A \cap B = \{ x \mid x \in A \wedge x \in B \}$
    - 交集: {3}



相对补（差）

- B对于A的补集
  - $A-B=\{x \mid x \in A \wedge x \notin B\}$
- 举例，A-B={1}
- 若有一个我们关心的“所有”对象的集合，称为全集，常用U表示，U-B称为B的“补集”，记为~B
  - $x \in \sim B \leftrightarrow x \notin B$





运算的重要性质

- 包含关系下两个集合的最小上界和最大下界
  - 最小上界：
    - $A \subseteq A \cup B$, $B \subseteq A \cup B$ ----A和B的上界
    - 对任意X，若$A \subseteq X$, $B \subseteq X$,则$A \cup B \subseteq X$ ----最小上界

A∪B是最小上界

  - 最大下界：
    - $A \cap B \subseteq A$, $A \cap B \subseteq B$ ----A和B的下界
    - 对任意X，若$X \subseteq A$, $X \subseteq B$,则$X \subseteq A \cap B$ ----最大下界

A∩B是最大上界

集合恒等式（1）

等 式	名 称
$A \cup \varnothing = A$ $A \cap U = A$	恒等律
$A \cup U = U$ $A \cap \varnothing = \varnothing$	支配律
$A \cup A = A$ $A \cap A = A$	幂等律
$\sim(\sim A) = A$	补集律
$A \cup B = B \cup A$ $A \cap B = B \cap A$	交换律

集合恒等式（2）

等 式	名 称
$A\cup(B\cup C)=(A\cup B)\cup C$ $A\cap(B\cap C)=(A\cap B)\cap C$	结合律
$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$ $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$	分配律
$\sim(A\cup B)=\sim A\cap\sim B$ $\sim(A\cap B)=\sim A\cup\sim B$	德摩根定律
$A\cup(A\cap B)=A$ $A\cap(A\cup B)=A$	吸收律
$A\cup\sim A=U$ $A\cap\sim A=\varnothing$	补律

集合相关命题的基本证明方法

- 直接使用集合包含、相等定义　相当于逻辑推理
  - $A \cup B = B \Rightarrow A \subseteq B$
  - 证明：

    对任何x, 假设$x \in A$.

    由集合并定义：$x \in A \cup B$

    由已知条件：　$A \cup B = B$

    $\therefore x \in B$

    因此：　$A \subseteq B$

基本证明方式

- 利用成员表证明集合恒等式　相当于真值表
  - $A \cup (A \cap B) = A$

A	B	A∩B	A∪(A∩B)
1	1	1	1
1	0	0	1
0	1	0	0
0	0	0	0

基本证明方式

- 利用运算定义作逻辑等值式推演
  - 例：A-(B∪C) = (A-B)∩(A-C)

$$A-(B\cup C)=\{x|x\in A\wedge x\notin B\cup C\}$$

$$=\{x|\ x\in A\wedge(x\notin B\wedge x\notin C)\}$$

$$=\{x|(x\in A\wedge x\notin B)\wedge(x\in A\wedge x\notin C)\}$$

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

等价的描述方式：

$$x\in A-(B\cup C)\Leftrightarrow(x\in A)\wedge(x\notin(B\cup C))\Leftrightarrow x\in A\wedge x\notin B\wedge x\notin C$$

$$\Leftrightarrow(x\in A\wedge x\notin B)\wedge(x\in A\wedge x\notin C)$$

$$\Leftrightarrow(x\in(A-B))\wedge(x\in(A-C))$$

$$\Leftrightarrow x\in(A-B)\cap(A-C)$$

基本证明方法

- 利用已知恒等式或等式作集合代数推演
  - 例：$A \cap B = A \Leftrightarrow A - B = \varnothing$

$A \cap B = A \Rightarrow A - B = \varnothing$:

$A - B = A \cap \sim B$

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

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

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

$A - B = \varnothing \Rightarrow A \cap B = A$:

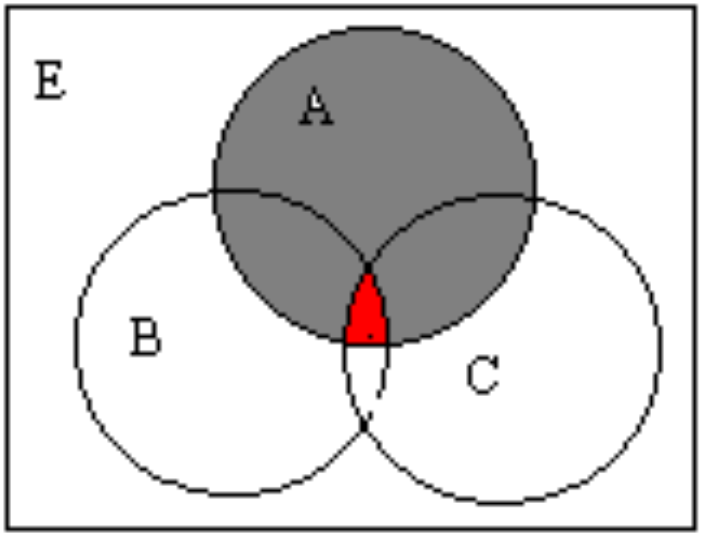
$A \cap B = (A \cap B) \cup (A \cap \sim B)$

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

文氏图与数学证明

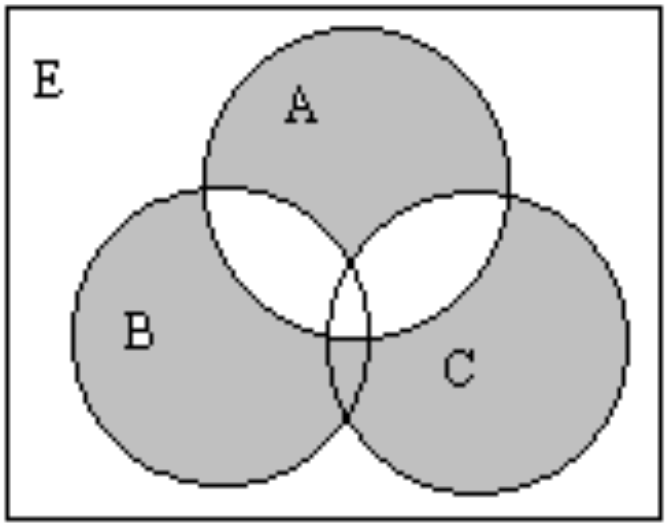
- 文氏图不能代替数学证明, 但可以帮助推测结论
- 例子：
  - **(A-B)∪(A-C)=A?**

充要条件：A∩B∩C=Ø



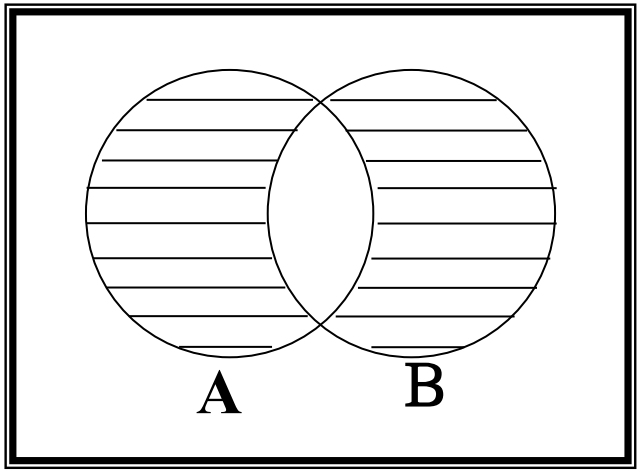
文氏图的更多例子

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



对称差

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



$A \oplus A = \phi \quad A \oplus \phi = A$

对称差（运算）满足的性质

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

- 结合律、交换律、消去律、…
- 消去律：若A⊕B=A⊕C, 则 B=C

$$
\begin{aligned}
B &= \varnothing \oplus B \\
&= (A \oplus A) \oplus B \\
&= A \oplus (A \oplus B) \\
&= A \oplus (A \oplus C) \\
&= C
\end{aligned}
$$

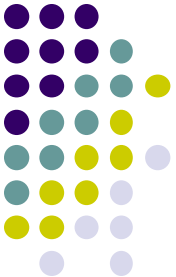
广义并和广义交

- 广义并 $\cup A = \bigcup_{i=1}^{n} A_i$
  - 设A为集合，A的所有元素的并，记为∪A; 定义为 $\cup A = \{x | \exists y \in A, x \in y\}$
  - 举例：$A=\{A_i | i \in N\}$, $\cup A = A_0 \cup A_1 \cup \ldots \ldots$
- 广义交 $\cap A = \bigcap_{i=1}^{n} A_i$
  - 设A为非空集合，A的所有元素的交，记为∩A, 定义为： $\cap A = \{x | \forall y \in A, x \in y\}$
    - 注意：限制条件为“A非空”，∩Ø无意义

小结

- 集合运算及其性质
  - 并、交、补
  - 对称差
  - 广义并/交
- 集合相关性质的证明方法

Zermelo–Fraenkel set theory with the axiom of choice



- 外延公理
- 正则公理
- 分离公理模式
- 配对公理
- 并集公理
- 替代公理模式
- 无穷公理
- 幂集公理
- 选择公理（或，良序定理）

ZFC公理

- 外延公理（Axiom of extensionality）
  - 如果两个集合含有同样的元素，则它们是相等的。

$$\forall x \forall y [\forall z (z \in x \Leftrightarrow z \in y) \Rightarrow x = y].$$

- 正则/基础公理（Axiom of regularity/foundation）
  - 任意非空集x包含一个成员y，x与集合y是不相交的

$$\forall x [\exists a (a \in x) \Rightarrow \exists y (y \in x \wedge \neg \exists z (z \in y \wedge z \in x))].$$

ZFC公理

- 分离公理模式（Axiom schema of separation）
  - 对任意集合z和任意对z的元素x有定义的逻辑谓词$\phi(x)$，存在z的子集y，使$x \in y$当且仅当$x \in z$而且$\phi(x)$为真。

$$\forall z \forall w_1 \ldots w_n \exists y \forall x [x \in y \Leftrightarrow (x \in z \wedge \phi)].$$

- 配对公理（ Axiom of pairing）

$$\forall x \forall y \exists z (x \in z \wedge y \in z).$$

- 并集公理（Axiom of union ）

$$\forall \mathcal{F} \exists A \forall Y \forall x [(x \in Y \wedge Y \in \mathcal{F}) \Rightarrow x \in A].$$

ZFC公理

- 替代公理模式（Axiom schema of replacement）

$$\forall A \forall w_1, \ldots, w_n \left[\forall x (x \in A \Rightarrow \exists! y \, \phi) \Rightarrow \exists B \forall x \big(x \in A \Rightarrow \exists y (y \in B \wedge \phi) \big) \right].$$

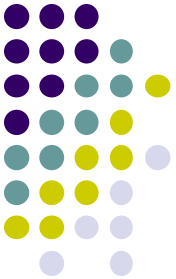
- 无穷公理（Axiom of infinity ）
  - S(y)是指 $y \cup \{y\}$

$$\exists X \left[\varnothing \in X \wedge \forall y (y \in X \Rightarrow S(y) \in X) \right].$$

- 幂集公理（Axiom of power set）

$$\forall x \exists y \forall z \left[z \subseteq x \Rightarrow z \in y \right].$$

ZFC公理



- 选择公理（Axiom of choice ）
  - 任一非空集合族 $(S_i)_{i\in I}$, 均存在元素族$(s_i)_{i\in I}$, $\forall i\in I.\ s_i\in S_i$

- 或，良序定理（Well-ordering theorem ）

$$\forall X \exists R (R \text{ well-orders } X).$$

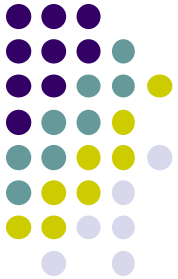
参考： Zermelo–Fraenkel set theory @Wiki

函数及其运算

瞿裕忠 教授

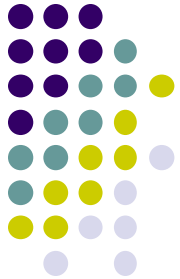
南京大学计算机科学与技术系

函数及其运算(1)



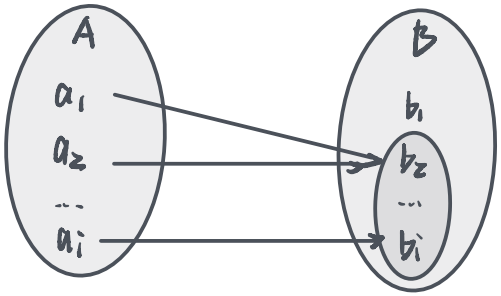
- 函数的定义
- 子集的像
- 单射与满射
- 反函数

函数(function)的定义



- 设A和B为非空集合，从集合A到B的函数*f*是对元素的一种指派，对A的每个元素恰好指派B的一个元素。记作$f:A\to B$。
  - *f* 的定义域（domain）是A
  - *f* 的伴域（codomain）是B
  - 如果*f* 为A中元素*a*指派的B中元素为*b*，就写成 $f(a)=b$。此时，称*b*是*a*的像，而*a*是*b*的一个原像。
  - A中元素的像构成的集合称为*f*的值域（ *f*的像）。
- 函数也称为映射(mapping)或变换(transformation)

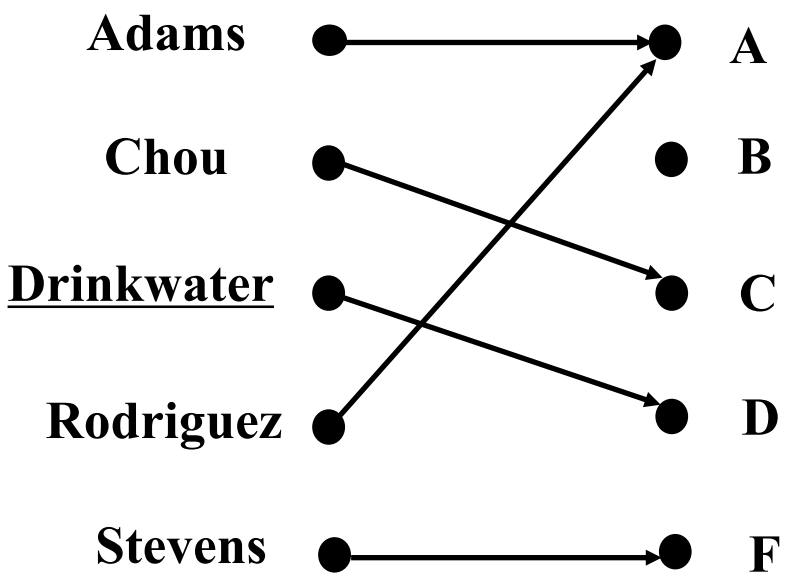
函数(function)的定义



- 备注
  - 函数在其定义域中的每个元素都有唯一的取值
  - 函数的值域是其伴域的子集
  - 函数相等 $f=g$ iff
    - $\mathrm{dom}(f)=\mathrm{dom}(g)$
    - $\forall x(x\in\mathrm{dom}(f) \rightarrow f(x)=g(x))$
    - $\mathrm{codom}(f)=\mathrm{codom}(g)$ (可有可无)
  - 若A和B皆是非空的有限集合，从A到B的不同的函数有$|B|^{|A|}$个。($a_1, a_2,\ldots, a_{|A|}$的像, 均有|B|种选择)

函数举例

- 某课程成绩

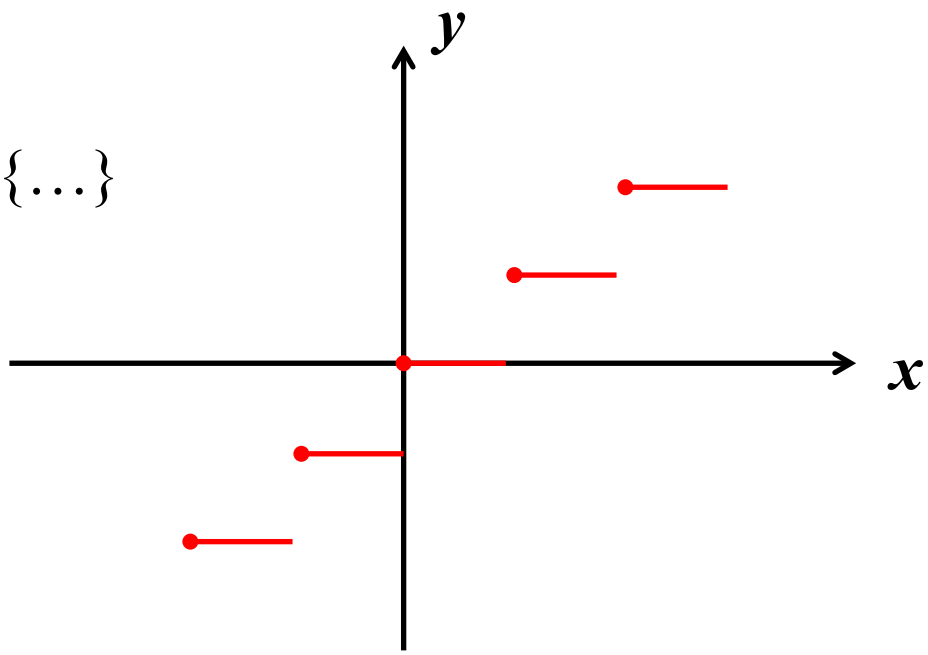


函数举例

- 下取整函数$\lfloor x \rfloor$: $\mathbf{R} \rightarrow \mathbf{Z}$ [,)

Java Program

```
int  floor(float real) {…}
```

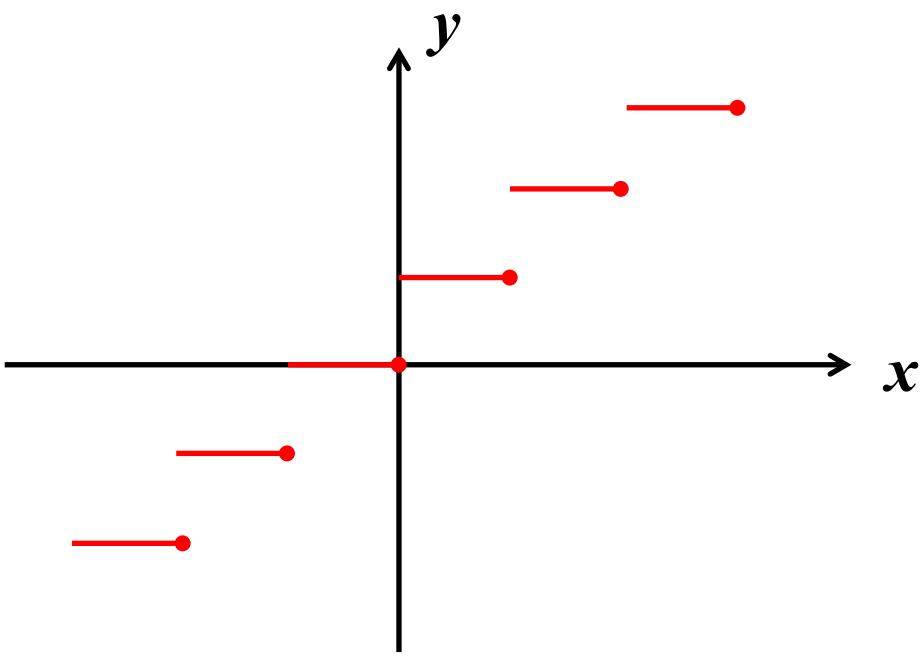


- 函数f的图像: $\{(a, b) \mid a \in \mathbf{A} \wedge f(a)=b\}$

$\{(a, f(a)) \mid a \in A\}$

函数举例

- 上取整函数$\lceil x \rceil$：$\mathbf{R} \rightarrow \mathbf{Z}$ （*ceiling function*）(,]



函数举例

- 对于任意实数x，$\lfloor -x \rfloor = -\lceil x \rceil$
- 对于任意实数x，$\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + 1/2 \rfloor$
  - $x = n + \varepsilon, 0 \le \varepsilon < 1$. 采用分情形证明方法
  - $0 \le \varepsilon < 1/2$
  - $1/2 \le \varepsilon < 1$
- × 对于任意实数x和y，$\lceil x+y \rceil = \lceil x \rceil + \lceil y \rceil$
- 反例: $x = y = 1/2$

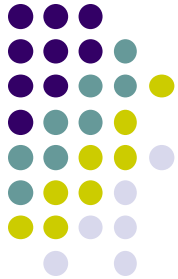
函数举例

- 设A为非空集合，A上的**恒等函数**ι_A:A→A定义为
  - $\iota_A(x)=x$，$x\in A$

    // ι: [iota] 约塔
- 设U为非空集合，对任意的A⊆U，**特征函数**χ_A:U→{0,1}定义为：
  - $\chi_A(x)=1$，$x\in A$
  - $\chi_A(x)=0$，$x\in U-A$

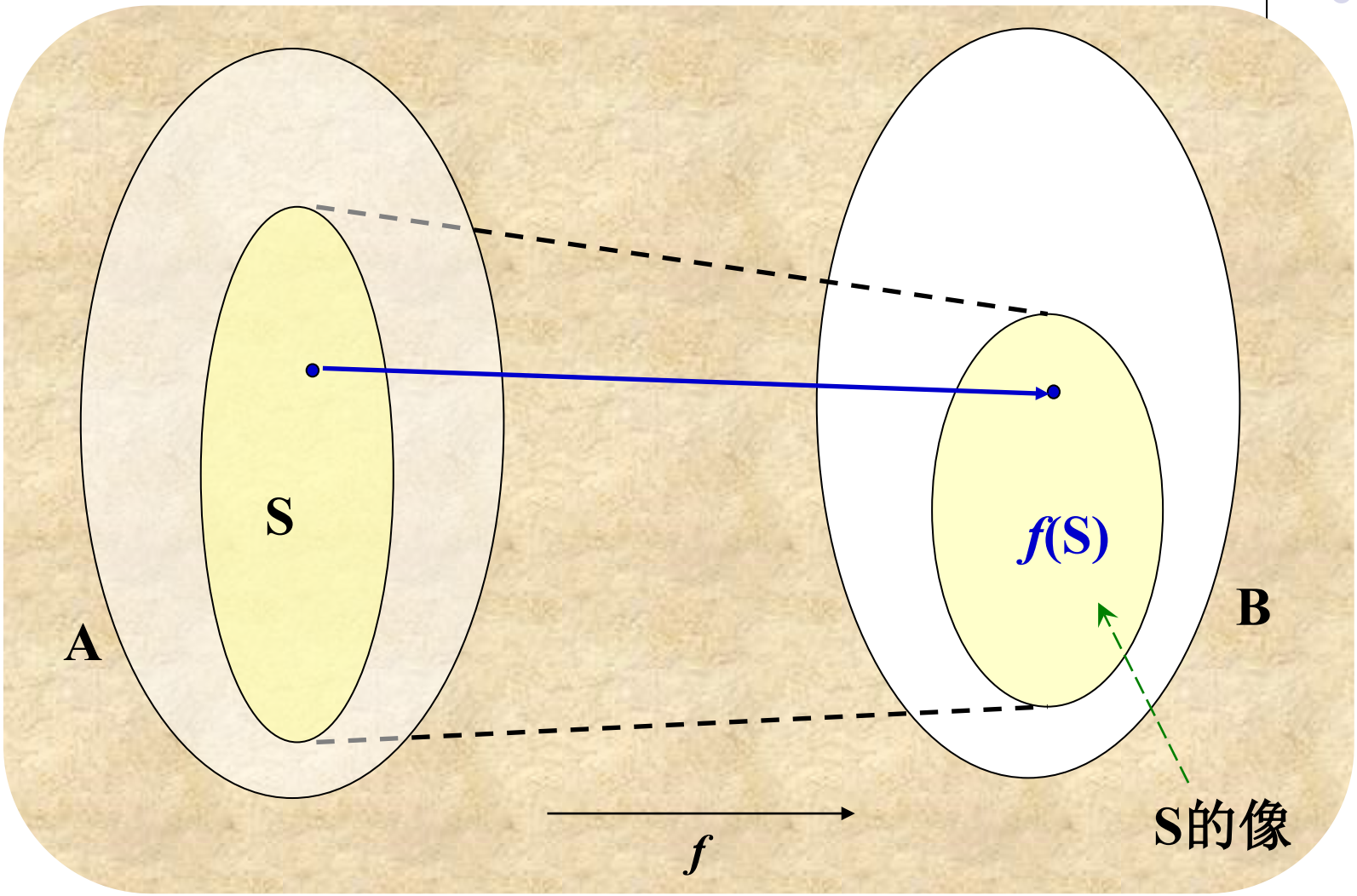
    // χ: [chi] 西

子集在函数下的像



- 设*f*是从集合A到B的函数，S是A的一个子集。S在*f*下的像，记为*f*(S)，定义如下：
  - $f(S) = \{ t \mid \exists s \in S\ (t = f(s)) \}$　// $\{ f(s) \mid s \in S \}$
- 备注：*f*(A)即为*f*的值域。

S的像



并集的像

- 设函数f: A→B，且X，Y是A的子集，则$f(X\cup Y)=f(X)\cup f(Y)$
- 证明:
  - $f(X\cup Y)\subseteq f(X)\cup f(Y)$

    对任意的t，若$t\in f(X\cup Y)$，则存在$s\in X\cup Y$，满足$f(s)=t$；假设$s\in X$，则$t\in f(X)$，假设$s\in Y$，则$t\in f(Y)$，$\therefore t\in f(X)\cup f(Y)$
  - $f(X)\cup f(Y)\subseteq f(X\cup Y)$

    对任意的t，若$t\in f(X)\cup f(Y)$

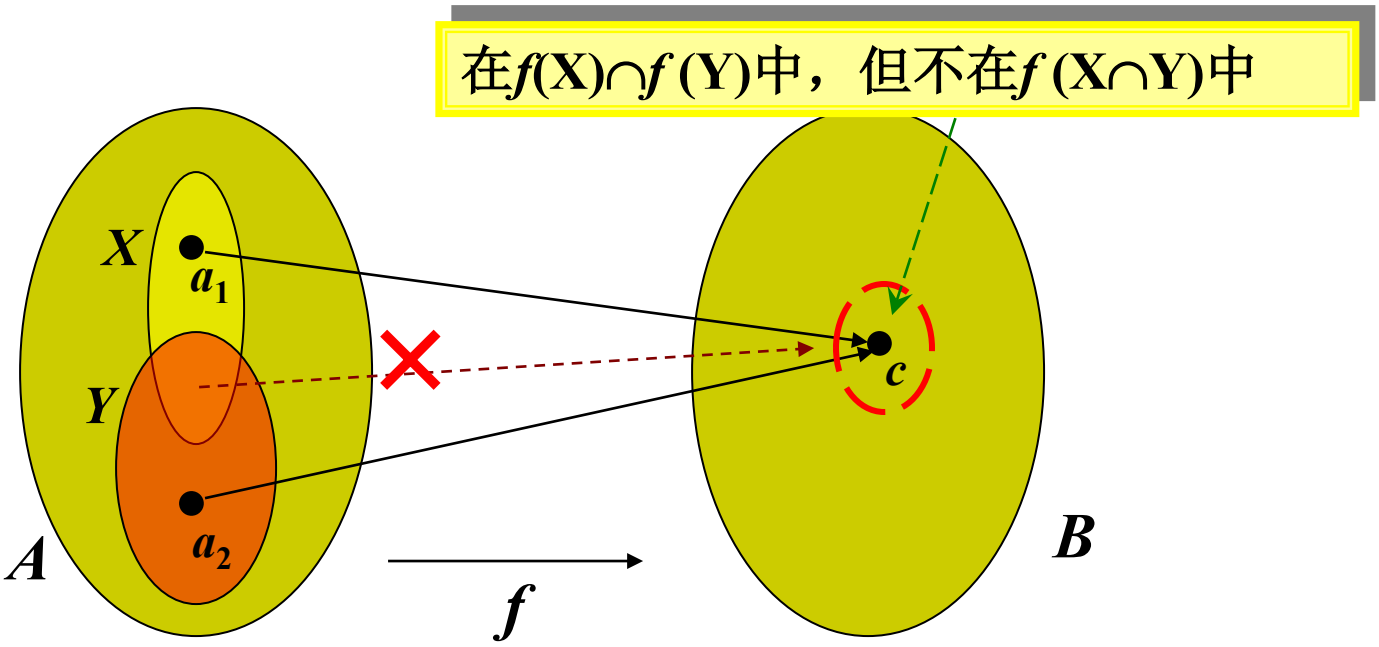
    情况1：$t\in f(X)$，则存在$s\in X\subseteq X\cup Y$，满足$f(s)=t$，$\therefore t\in f(X\cup Y)$

    情况2：$t\in f(Y)$，同样可得$t\in f(X\cup Y)$

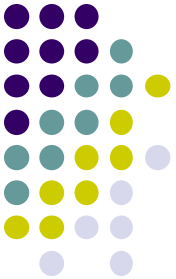
    $\therefore t\in f(X\cup Y)$

交集的像

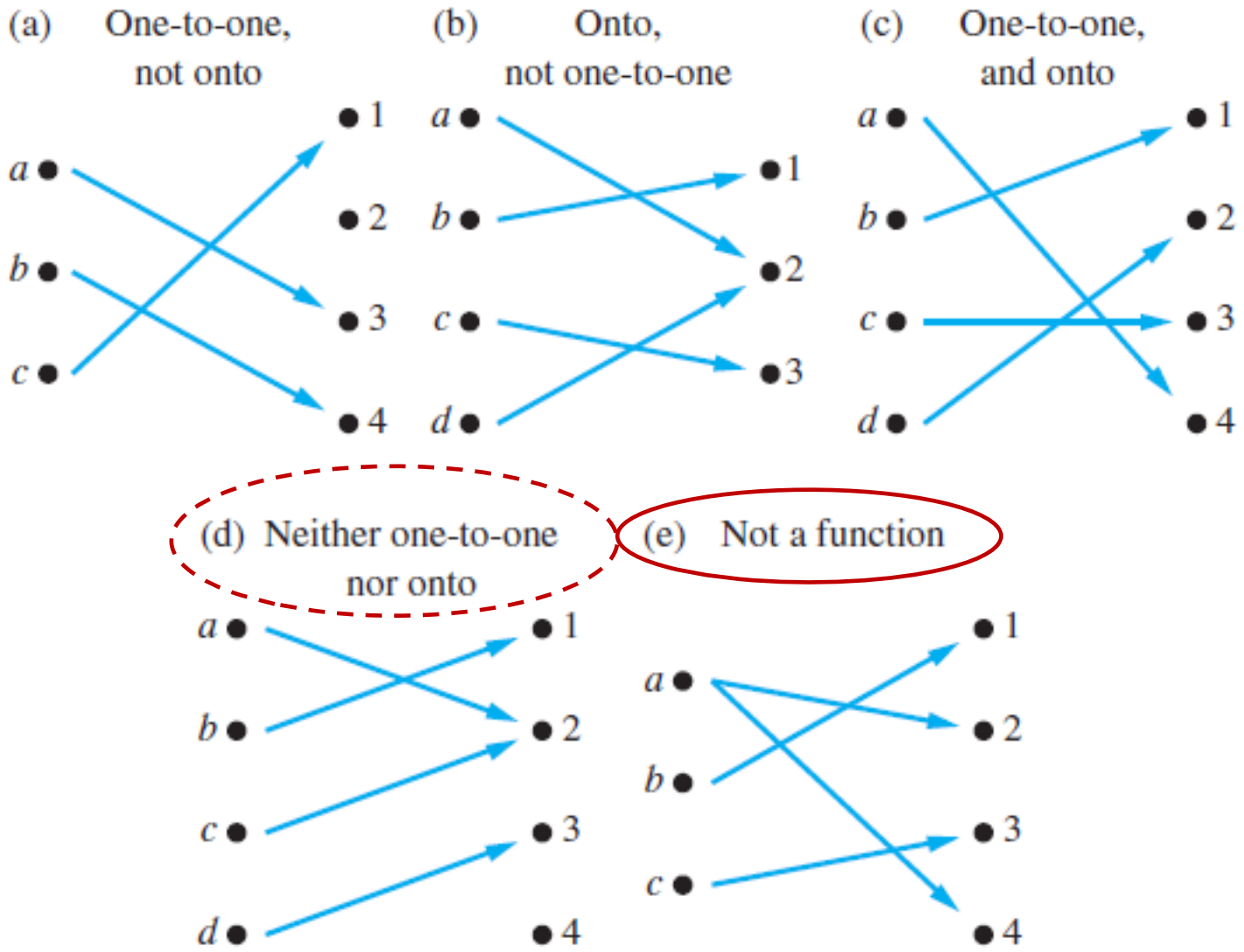
- 设函数f：A→B，且X，Y是A的子集，则
  - $f(X\cap Y)\subseteq f(X)\cap f(Y)$



函数性质



- **f:A→B是单射（一对一的, one-to-one, *injective*）**
  - $\forall x_1, x_2 \in A$, 若$x_1 \neq x_2$，则$f(x_1) \neq f(x_2)$
  - //等价的说法：$\forall x_1, x_2 \in A$, 若$f(x_1) = f(x_2)$，则$x_1 = x_2$
- **f:A→B是满射（到上的/映上的, onto, *surjective*）**
  - $\forall y \in B, \exists x \in A$, 使得$f(x)=y$
  - //等价的说法：$f(A)=B$
- **双射（一一对应, *bijective*）**
  - 既是单射, 又是满射


(a) One-to-one, not onto
a
b
c
1
2
3
4
(b) Onto, not one-to-one
a
b
c
d
1
2
3
(c) One-to-one, and onto
a
b
c
d
1
2
3
4
(d) Neither one-to-one nor onto
a
b
c
d
1
2
3
4
(e) Not a function
a
b
c
1
2
3
4

函数性质的证明

- 判断$f:R\times R\to R\times R$, $f((x,y))=(x+y, x-y)$的性质
- 单射？
  - 令$f((x_1, y_1))=f((x_2, y_2))$
    - $x_1+y_1=x_2+y_2$且$x_1-y_1=x_2-y_2$，易得：$x_1=x_2$且$y_1=y_2$
    - $(x_1, y_1)=(x_2, y_2)$
- 满射？
  - 任取$(a, b)\in \mathbf{R}\times\mathbf{R}$，总存在$((a+b)/2,(a-b)/2)$,使得
  - $f((a+b)/2,(a-b)/2)=(a, b)$

函数性质的证明

- 设A是有限非空集合，f是从A到A的函数。f是单射当且仅当f是满射。
- 证明：
- f是单射 $\Rightarrow$ f是满射
  - $|f(A)| = |A|$ 元素个数相等
- f是满射 $\Rightarrow$ f是单射
  - 假设f不是单射，$|f(A)| < |A|$，值域是A的真子集。
  - f不是满射，矛盾。

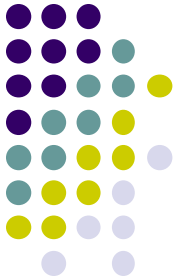
反函数

- 设f是从A到B的一一对应，f的反函数是从B到A的函数，它指派给B中元素b的是A中满足$f(a)=b$的（唯一的）a。f的反函数记作f^{-1}。
  - $f(a)=b$ 当且仅当 $f^{-1}(b)=a$
- 备注：切勿将f^{-1}与$1/f$混淆。
- 例子
  - $f: N\times N\to N$, $f(i,j)=2^i(2j+1)-1$是双射，
  - $f^{-1}(2^i(2j+1)-1)=(i,j)$

小结

- 函数的基本概念
  - 定义域中的每个元素有唯一的像
  - 子集的像、值域
  - 单射、满射、双射（反函数）

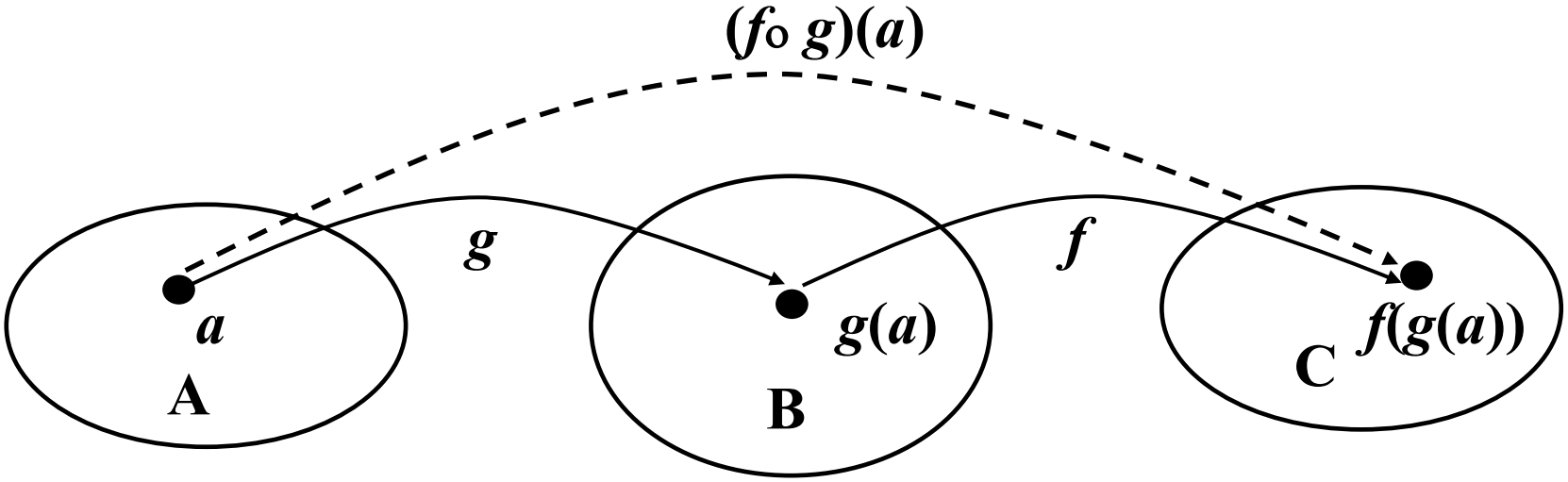
函数及其运算(2)



- 函数的复合
- 函数的四则运算//值域有要求
- 偏函数
- 函数构成的集合
- 序列

函数的合成（composition） 复合

- 设g是从A到B的函数，f是从B到C的函数，f和g的合成（composition）用$f \circ g$表示，定义为：
  - $(f \circ g)(x) = f(g(x))$， $x \in A$



复合运算的性质

- 函数的复合满足结合律
  - $(f \circ g) \circ h = f \circ (g \circ h)$
- 满射的复合是满射
- 单射的复合是单射
- 双射的复合是双射
- 设f是从A到B的双射
  - $f^{-1} \circ f = \iota_A$
  - $f \circ f^{-1} = \iota_B$

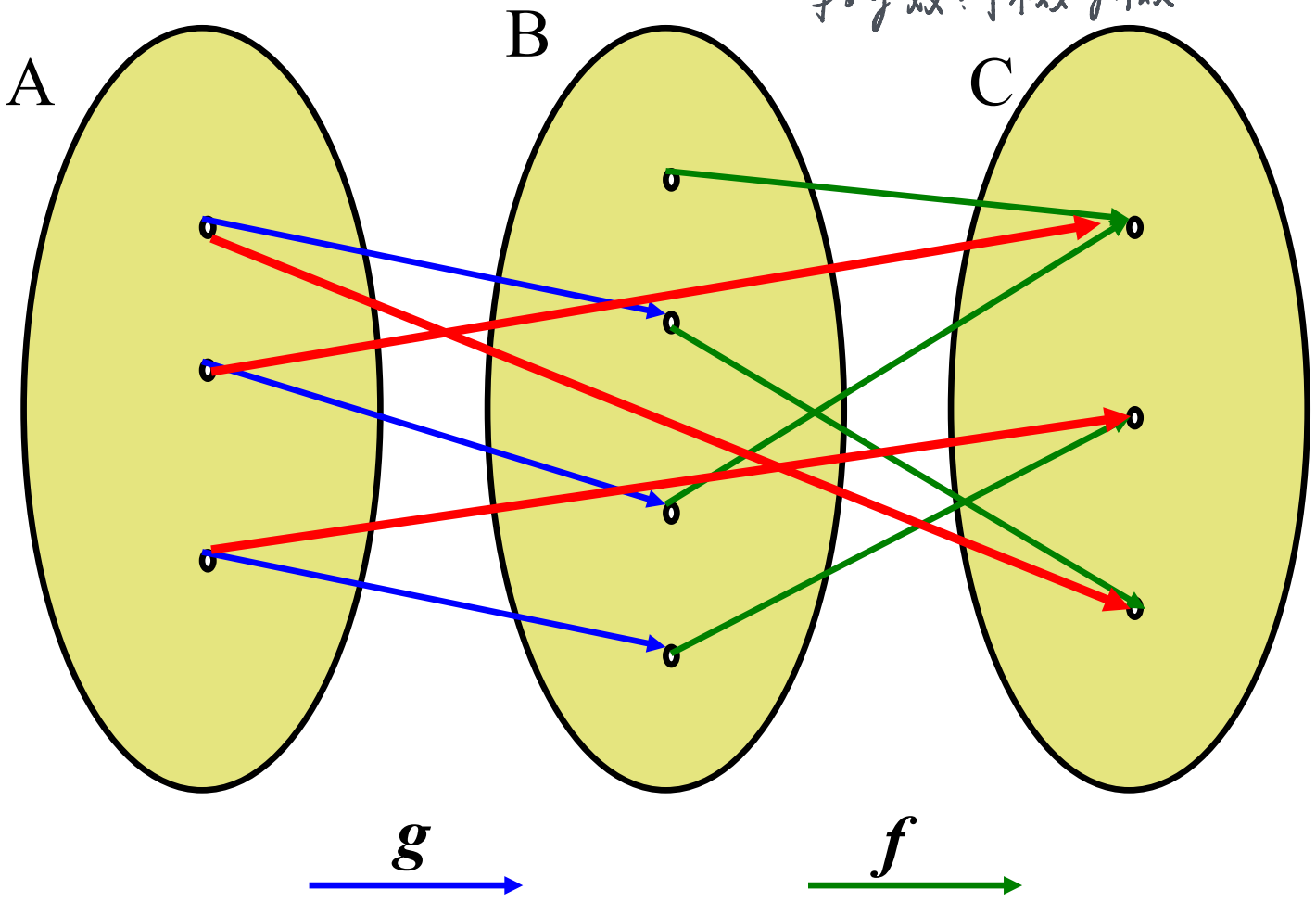
但是…

- 若$f \circ g$是满射，能推出f和g是满射吗？
  - f*一定*是满射，g*不一定*是满射。
- 若$f \circ g$是单射，能推出f和g是单射吗？
  - g*一定*是单射，f*不一定*是单射。

$f \circ g$ 满：f 满 g 不满

$f \circ g$ 单：f 不单 g 单

$f \circ g$ 双：f 不双 g 不双



函数的加法、乘法

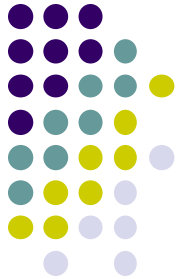
- 设f和g是从A到R的函数，那么 $f+g$ 和 $f\ g$也是从A到R的函数，其定义为
  - $(f+g)(x) = f(x) + g(x)$， $x \in A$
  - $f\ g(x) = f(x)\ g(x)$， $x \in A$

//类似地，可以定义除法，注意定义域有限定

递增（递减）函数

- 设f的定义域和伴域都是实数的子集，
- f是递增的
  - $\forall x\, \forall y\, (x<y \rightarrow f(x) \leq f(y))$
- f是严格递增的
  - $\forall x\, \forall y\, (x<y \rightarrow f(x) < f(y))$
- 严格递增函数一定是一对一的？

偏函数（Partial Functions）



- 从集合A到B的偏函数f是对元素的一种指派，对A的某些元素恰好指派B的一个元素。记作$f:A\rightarrow B$。
  - 对A中某些元素，偏函数f没有定义。
  - 有定义的元素全体构成函数的定义域。
- 举例
  - $f:Z\rightarrow R$
  - $f(n)=\sqrt{n}$

函数构成的集合（回顾）

- 初等函数（R→R）
  - 基本初等函数：常函数、幂函数、指数函数、对数函数、三角函数、反三角函数
  - 四则运算
  - 函数的复合

导函数、隐函数、不定积分

- 微积分
  - 基本初等函数
  - 连续？可导？可积分？
  - 运算（加、乘、除、复合）之后，连续？可导？可积分？
  - 多元函数？ $R^n \to R$

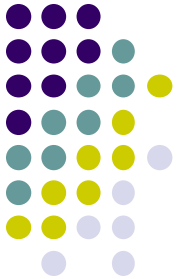
函数构成的集合

$B^A = \{f: A \to B\}$

- B^A： A到B的所有函数构成的集合，A和B皆非空。
  - 若A和B皆有限， $|B^A| = |B|^{|A|}$
  - 若$|A| = 1$， $|B^A| = |B|$
  - 若$|B| = 1$， $|B^A| = 1$
  - 若 $B=\{0,1\}$， B^A 等同于 $\rho(A)$，为何$\rho(A)$有时记为 2^A ？

A的所有子集、幂集

序列（ sequence ）



- 一个序列是从Z的一个子集（通常是N或Z^+）到某个集合S的一个函数。我们用a_n代表整数n的像，称为这个序列的项，$\{a_n\}$代表这个序列。
  - 有限序列vs无穷序列
  - $\{1/n\}, n\in Z^+$；$\{n^2\}$；$\{a_n\}$, 其中$a_{2k}=0, a_{2k+1}=1, k\in N$
- 一个0~1无穷序列是N到{0,1}的一个函数，等同N的某个子集
- $(\{0,1\})^N$：0~1无穷序列全体构成的集合，也可记为 2^N
- 区间[0, 1)中的一个实数是否可以表示为一个0~1序列？

一个例子

- 自然数1,2,3,…,n^2+1的任何一种排列中，必然含一个长度不小于$n+1$的严格递增子序列或严格递减子序列。
  - 所给序列中，以k开始的最长严格递增子序列的长度为I(k)，以k开始的最长严格递减子序列长度为D(k)。
  - 举例：(1, 3, 5, 9, 7, 10, 4, 8, 2, 6）
  - I(7)=2, (7, 10);　　D(7)=3, (7, 4, 2);
  - I(3)=4, (3, 5, 7, 10);　　D(4)=2, (4, 2);
  - I(3) > I(7) , D(7) > D(4)

一个例子

- 自然数1,2,3,…,n^2+1的任何一种排列中，必然含一个长度不小于$n+1$的严格递增链或严格递减链。
  - F: $k \rightarrow (I(k), D(k))$, $k \in \{1,2,\ldots, n^2+1\}$
  - 对于$k_1<k_2$，如果k_1排在k_2前面，则$I(k_1)>I(k_2)$，如果k_2排在k_1前面，则$D(k_2)>D(k_1)$。因此，F是单射。
  - 假设严格递增与递减子序列最大长度均不大于n:
  - $I(k) \leq n$, $D(k) \leq n$, F的值域最多有n^2个元素。
  - F是单射，且定义域含 n^2+1个元素，矛盾。

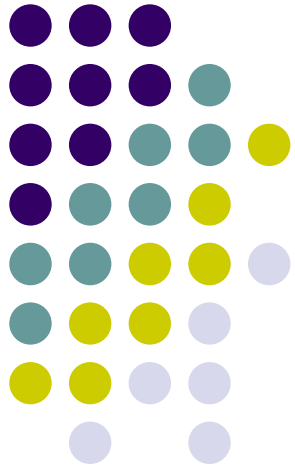
小结

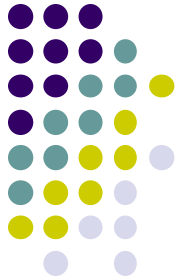
- 函数构成的集合
  - 加法、乘法、除法、函数的复合
  - 偏函数
- 序列
  - 一种特殊的函数
  - 0~1无穷序列

自然数及数论初步

离散数学—集合论

南京大学计算机科学与技术系





内容提要

- **自然数**
  - 自然数的集合论构造
  - 自然数的公理化定义
  - 自然数基本运算定义
- **整数及基本运算**
  - 整数除法与同余算术
  - 素数与算术基本定理
  - 同余方程与中国剩余定理
  - 费马小定理与欧拉定理

用集合定义自然数

- 设a为集合, 称$a \cup \{a\}$为a的后继, 记为$s(a)$， 或a^+。
  - $\varnothing$
  - $s(\varnothing)$：$\varnothing \cup \{\varnothing\} = \{\varnothing\}$
  - $s(s(\varnothing))$：$\{\varnothing\} \cup \{\{\varnothing\}\} = \{\varnothing, \{\varnothing\}\}$
  - $s(s(s(\varnothing)))$：$\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$
  - …

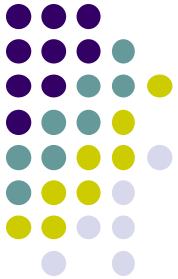
用集合定义自然数

- 设A是集合，若A满足下列条件，称A为归纳集：
  - $\varnothing \in A$
  - $\forall a(a \in A \rightarrow s(a) \in A)$
- 自然数集合N:是所有归纳集的交集。
  - 因此：$N = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}, \ldots\}$
  - N的每一个元素称为一个自然数。
  - $\varnothing$记为0，s(0)记为1，s(1)记为2， s(2)记为3，以此类推

具体一点

- 符号0表示：　　Ø
- 符号1表示s(0)：{Ø}
- 符号2表示s(1)：{Ø,{Ø}}
- 符号3表示s(2)：{Ø,{Ø}, {Ø,{Ø}}}
- $1 \in 3$　$2 \in 3$
- $1 \subseteq 3$　$2 \subseteq 3$
- $1 \cup 3 = 3$　$2 \cap 3 = 2$

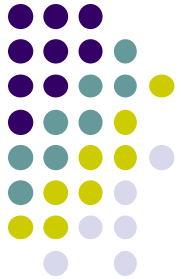
皮亚诺公理
(Peano axioms for natural numbers)



- 零是个自然数.
- 每个自然数都有一个后继（也是个自然数）. 无限集
- 零不是任何自然数的后继.
- 不同的自然数有不同的后继.
- （归纳公理）设由自然数组成的某个集合含有零，且每当该集合含有某个自然数时便也同时含有这个数的后继，那么该集合定含有全部自然数. 最小集合

- 备注：另有4个与自然数相等有关的公理

皮亚诺公理
(Peano axioms for natural numbers)



1. $0 \in \mathbf{N}$
2. $x \in \mathbf{N} \rightarrow S(x) \in \mathbf{N}$
3. $x \in \mathbf{N} \rightarrow S(x) \neq 0$
4. $x \in \mathbf{N} \wedge y \in \mathbf{N} \wedge S(x) = S(y) \rightarrow x = y$
5. $0 \in M \wedge \forall x(x \in M \rightarrow S(x) \in M) \rightarrow \mathbf{N} \subseteq M$ for any property M (axiom of induction).

自然数上的运算

- 加法（递归定义）
  - $m + 0 = m$
  - $m + s(n) = s(m+n)$
- 乘法（递归定义）
  - $m * 0 = 0$
  - $m * s(n) = m + m*n$
- 回答“小朋友的问题”

$$1 + 2 = 1 + S(1) = S(1+1) = S(1+S(0))$$

$$= S(S(1+0)) = S(S(1)) = S(2) = 3$$

自然数上的运算（性质）

- 试证明： $0 + m = m$

  证明： 对 m 作归纳.

  基础步骤： $0 + 0 = 0.$

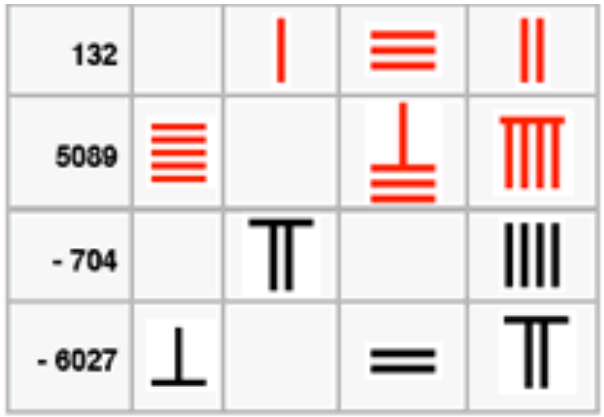
  归纳步骤：假设 $0 + k = k,$ 则

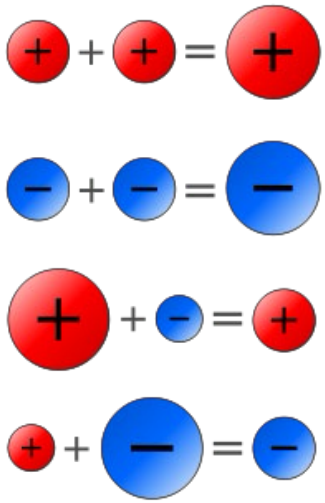
  $$0 + S(k) = S(0 + k) = S(k).$$

  证毕。

- 【练习】
  - 试证明：自然数的加法满足结合律。
  - 试证明：自然数的加法满足交换律。
  - 试证明：自然数的乘法对加法满足分配律。

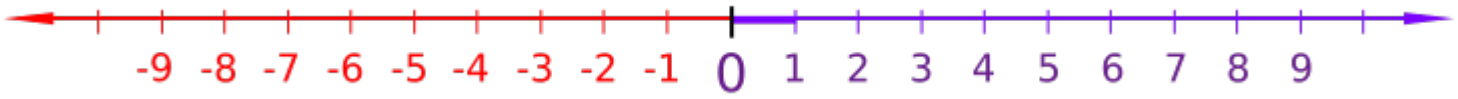
正整数(N^+)、零、负整数





刘徽(A.D. 225-295)

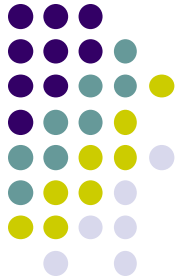
$$4x + 20 = 4$$



整数 $\mathbb{Z}$ （减法）

	Addition	multiplication
Closure Property	a +b=an integer example 6+2=8	ax b=an integer example 3x4=12
Associative	a+(b +c)=(a +b)+c example 9+(2+4)=(9+2)+4=15	ax(b x c)=(ax b)x c example 3x[-2)x4]= [3x(-2)]x4=-24
Distributive	ax(b +c)=(ax b)+(a x c), (a +b) x c=(a x c)+(b x c) example5x[2+(-3)]=[5x2]+[5x(-3)]=10-15=-5	
Commutative	a+ b=b +a example 3+(-2)=(-2)+3=1	ax b=b x a example 3x(-2)=(-2)x3=-6
Identity	a+0=a example 6+0=6	ax1=a example (-6)x1=-6
Inverse element	a+(-a)=0 example 6+(-6)=0	No inverse element
Zero product property		If a x b=0,then either a=0, or b=0 or both=0

整数之间的整除



- 对任意整数a和b, $a \neq 0$, 我们说a整除b (记作$a|b$) , 如果存在整数c使得 $b = a\ c$.
- 设a, b和c是整数， $a \neq 0$,
  - 若$a|b$，且 $a|c$，则 $a|(b+c)$
  - 若$a|b$，则 $a|(b\ c)$
  - 若$a|b$，且 $b|c$，则 $a|c$

带余除法

- 令a为整数，d为正整数，则存在唯一的整数q和r，且 $0 \le r < d$，满足 $a = d\,q + r$.
  - d为除数，a为被除数，q为商，r为余数。
  - 记作 $q = a \text{ div } d$，$r = a \bmod d$. 举例：$-11 \bmod 3 = ?$
- 证明：

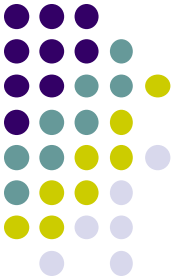
$-11 = 3 \times (-4) + 1$

  - $S=\{r \in N \mid \exists\, q \in Z.\ r = a-dq\}$是N的非空子集
  - N是良序的，S有最小元素，记为r_0，即$r_0 = a-dq_0$
  - 用反证法易证$r_0<d$, 否则r_0-d是S中比r_0更小的元素, 矛盾
  - 唯一性证明， $0 \le r_1 - r_0 = d\,(q_0-q_1) < d$，因此，$q_1=q_0$

带余除法（续）

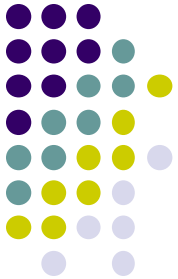
- 令a和b为整数，d为正整数，则
  - $(a + b) \bmod d = (a \bmod d + b \bmod d) \bmod d$.
  - $(a\ b) \bmod d = ((a \bmod d)\ (b \bmod d)) \bmod d$.

同余算术 (高斯, Gauss)



- 设a和b为整数，m为正整数，如果m整除$(b-a)$，就说a模m同余b. 记作 $a \equiv b \pmod{m}$.
- $a \equiv b \pmod{m}$ *iff* $a \pmod{m} = b \pmod{m}$
- $a \equiv b \pmod{m}$ *iff* $\exists k \in \mathbf{Z}.\ a = b + km$
- 举例 $-1 \equiv 5 \pmod 6$, $-2 \equiv 4 \pmod 6$, …, $-5 \equiv 1 \pmod 6$
  - $[0] = \{\ldots, -6, 0, 6, \ldots\}$
  - $[1] = \{\ldots -5, 1, 7, \ldots\}$
  - $[2] = \{\ldots, -4, 2, 8, \ldots\}$
  - …

同余算术 (高斯, Gauss)

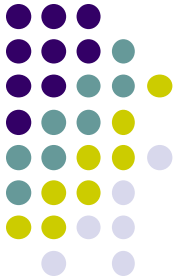


- 设$a \equiv b \pmod{n}$；k 为非负整数；

  $a_1 \equiv b_1 \pmod{n}$ 且 $a_2 \equiv b_2 \pmod{n}$；

  - $k\,a \equiv k\,b \pmod{n}$
  - $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$
  - $a_1 - a_2 \equiv b_1 - b_2 \pmod{n}$
  - $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{n}$
  - $a^k \equiv b^k \pmod{n}$
  - $p(a) \equiv p(b) \pmod{n}$, $p(x)$ 为任意整系数多项式

素数



- 大于1的正整数p称为素数，如果p仅有的正因子是1和p。大于1又不是素数的正整数称为合数。
- 正整数n是合数 $iff \exists a \in \mathbf{N}.\ 1 < a < n$, 且 $a \mid n$.
- 算术基本定理：每个大于1的正整数都可以唯一地写为一个素数或者若干个素数的乘积，其中素数因子以非递减序出现。
  - $n = p_1^{\alpha 1} p_2^{\alpha 2} \ldots p_k^{\alpha k}$
- 素数举例：2, 3, 5, 7, 11, 13, 17, 19, …
- 合数举例：$100 = 2^2 5^2$. $999 = 3^3 37$, $1024 = 2^{10}$.

埃拉托色尼筛选法(Eratosthenes, BC276–195)

- 用筛选法求素数（以25以内的为例）

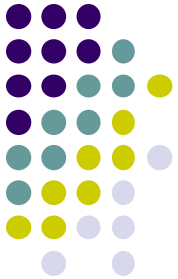
2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

[2] 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

[3] 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

[5] 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

素数（续）



- 下列自然数哪些是素数？
  - 101
  - 2^2-1，2^3-1，2^5-1，…，2^p-1,…
  - 2^{11}-1=2047=23·89 （大数的因数分解有点难）
  - （搜寻尽可能大的梅森素数）
- 如果n是合数，那么n必有不大于$\sqrt{n}$的一个素因子.
- 存在无限多个素数
  - 证明. 反证法，假设只有有限个素数，$p_1, p_2 \ldots, p_k$
  - 令q=1+$p_1p_2 \ldots p_k$，q的素因子是新的素数，矛盾。

威尔逊定理

- 设p为大于1的正整数，则 p为素数 iff $(p-1)! \equiv -1 \pmod{p}$
- **证明：必要性** ⇒

  若p是素数，令A={1,2,3,...,p-1}; 则任意$i \in A$,存在唯一的$j \in A$, 使得:

  $$i * j \equiv 1 \pmod{p}$$

  若 $x * x \equiv 1 \pmod{p}$，则 $x = 1$ 或 $p - 1$

  对于$1 < x < p - 1$，存在唯一的$y \in A$， $x * y \equiv 1 \pmod{p}$，且$y \neq x$

  这些x和y两两配对; 故而 $(p - 1)! \equiv 1 * (p - 1) \equiv -1 \pmod{p}$
- **充分性** ⇐ **不妨假设** $p>4$, 反证法，假设p不是素数

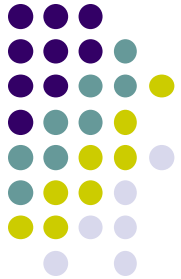
  若p不是完全平方数，则存在两个不等的因子a和b使得$ab=p$，

  $(p-1)!=nab \equiv 0 \pmod{p}$，矛盾；

  若p是完全平方数，即$p=k^2$，因为$p>4$, 所以$k>2$，$2k<p$，

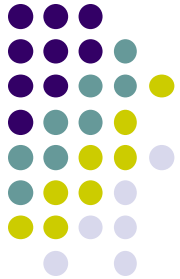
  $(p-1)! = m\,(k*2k) \equiv 0 \pmod{p}$，矛盾。

最大公约数



- 能整除两个（正）整数的最大正整数称为这两个（正）整数的最大公约数。记法：gcd(*a*, *b*)
  - gcd(*a*, *b*) = *max*{ *d*∈Z^+ | *d*|*a*, *d*|*b*}，*a*≠0 或者*b*≠0
  - 我们称*a*和*b*是互素的，如果gcd(*a*, *b*) = 1
- 若$a = p_1^{\alpha 1} p_2^{\alpha 2} \ldots p_k^{\alpha k}$，$b = p_1^{\beta 1} p_2^{\beta 2} \ldots p_k^{\beta k}$，
  则 $\gcd(a, b) = p_1^{\gamma 1} p_2^{\gamma 2} \ldots p_k^{\gamma k}$，$\gamma_i = \min\{\alpha_i, \beta_i\}$
- 求两个正整数的最大公约数
  - gcd(*a*, *b*) = gcd(*a*, *b*-*a*) //不妨假设 *a*<*b*。

欧几里德算法（求最大公约数）

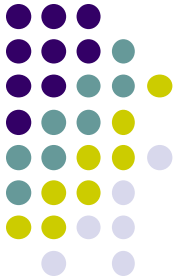


```
function gcd(a, b)  // a>0, b>0
  while a ≠ b
        if a > b
              a := a − b
        else
              b := b − a
  return a
```

```
function gcd(a, b)  // 不全为0的自然数
  while b ≠ 0
        t := b
        b := a mod b
        a := t
  return a
```

```
function gcd(a, b)  // a≥b≥0, a>0
  if b=0
        return a
 else
        return gcd(b, a mod b)
```

最大公约数（续）



- **gcd(a, b)一定是a和b的线性组合，即：**

  $\exists s, t \in Z$， gcd(a, b)=$sa+tb$

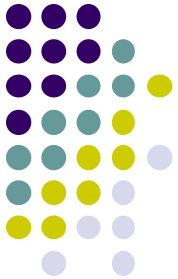
  //欧几里德算法得出结论

- **裴蜀定理 (Bézout's identity)**

  $ax + by = c$有整数解当且仅当 $\gcd(a,b) \mid c$.

- **非零整数a和b是互素的 *iff* $\exists s, t \in Z$. $sa+tb=1$**
  - 必要性显然。以下证明充分性。假设$\exists s, t \in Z$. $sa+tb=1$.
  - 假设gcd(a, b)=d， $\exists a_1, b_1 \in Z$. $a=a_1 d$, $b=b_1 d$.
  - 我们有$sa_1 d+tb_1 d=1$. 即 $(sa_1+tb_1)d=1$.
  - 因此$d=1$. 即gcd(a, b)=1。

中国剩余定理（孙子算经，5世纪）



例子:

《孙子算经》:

今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？
答曰：‘二十三’。

$$(S):\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

$$(S):\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad\vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

一般情况何时可解? 如何解?

中国剩余定理（孙子算经，5世纪）

$$(S):\ \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

- 假设正整数$m_1, m_2, \ldots, m_n$两两互素，一元线性同余方程组（S）有解，<u>在模M同余下是唯一的</u>。

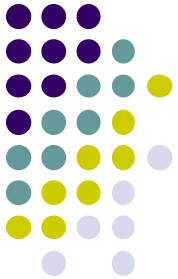
$$M = m_1 \times m_2 \times \cdots \times m_n = \prod_{i=1}^{n} m_i \qquad M_i = M/m_i,\ \forall i \in \{1,2,\cdots,n\}$$

$$x = \sum_{i=1}^{n} a_i t_i M_i \ . \ \text{mod } (M) \qquad t_i M_i \equiv 1 \pmod{m_i},\ \forall i \in \{1,2,\cdots,n\}.$$

- 解的唯一性，需要证明：

$m_1|y, \ldots, m_n|y \rightarrow (m_1 \ldots m_n)|y$

中国剩余定理（孙子算经，5世纪）



- 需要下列引理：

  设a, b和c是正整数, a和b是互素的, 若$a|bc$, 则$a|c$。

  证明： $\exists s, t \in \mathbf{Z}.\ sa+tb=1.\ c=(sa+tb)c=sac+tbc$, 因此, $a|c$。

- 设a, b和c是正整数, a和b是互素的, 若$a|c$,若$b|c$,则$ab|c$。

证明： $c=ua=vb$, $a|vb$, $a|v$. (a和b互素)

$v=ka$, $c=kab$, 因此, $ab|c$.

欧拉

Euler's totient (ϕ函数)

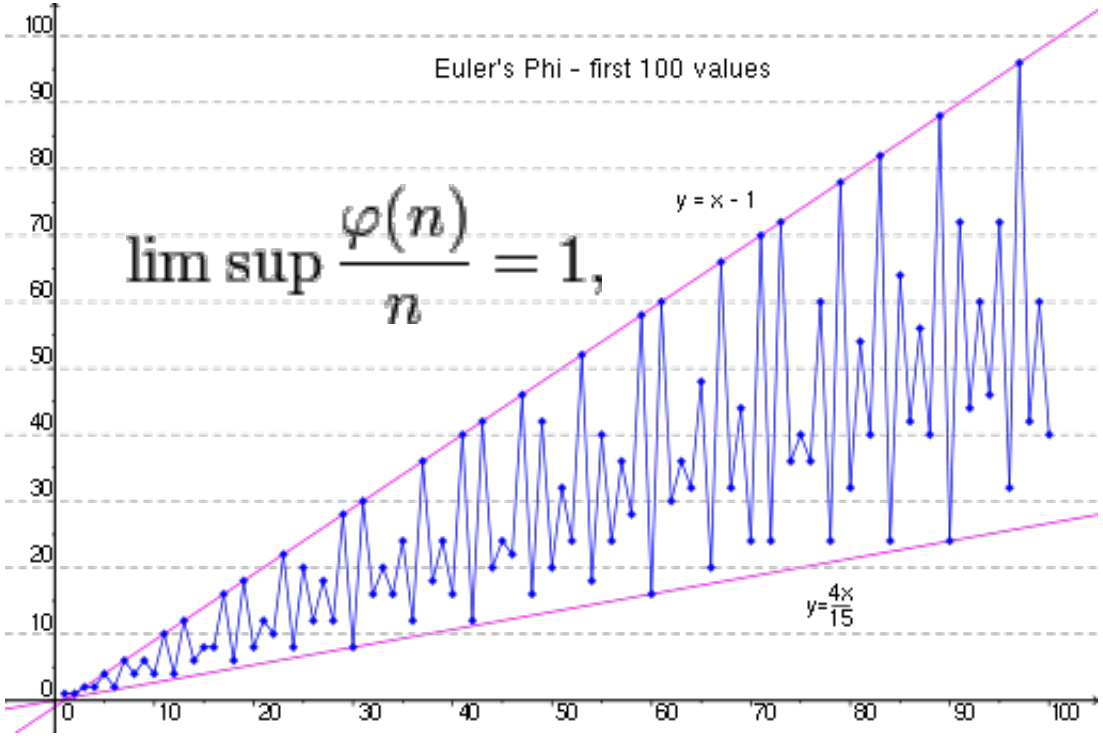
- 不大于n且与n互素的正整数的个数，记为 $\phi(n)$ 。
- $\phi(n) = |\{ k \mid 1 \le k \le n , \gcd(k, n) = 1\}|, n \in N^+$
  - $\phi(3) = 2, \phi(4) = 2, \phi(12) = 4$
- 设 $n = p_1^{\alpha 1} p_2^{\alpha 2} \ldots p_k^{\alpha k}$
- 令 $A_i = \{ x \mid 1 \le x \le n , p_i$整除$x\}$
- $\phi(n) = | \sim A_1 \cap \sim A_2 \cap \ldots \cap \sim A_k |$

$$= n - (n/p_1 + \ldots + n/p_k) + (n/p_1p_2 + \ldots + n/p_{k-1}p_k)$$

$$- \ldots + (-1)^k n/p_1p_2 \ldots p_k$$

$$= n(1 - 1/p_1)(1 - 1/p_2) \ldots (1 - 1/p_k)$$

欧拉函数(phi)



$$\limsup \frac{\varphi(n)}{n} = 1,$$

$$\liminf \frac{\varphi(n)}{n} \log\log n = e^{-\gamma}.$$

欧拉常数 γ = 0.577215665...

欧拉函数(phi)

- ϕ(*p*)=*p*-1，*p*是素数
- 如果*m*与*n*互素，则φ(*mn*) = φ(*m*)φ(*n*).

$$\varphi(n) = n\prod_{p|n}\left(1-\frac{1}{p}\right),$$

Fermat小定理

- 设正整数 a 不是素数 p 的倍数，则 $a^p \equiv a \pmod{p}$
  - 证明概要
    - $a^p = (1+1+\cdots+1)^p = \sum_{k_1,k_2,\ldots,k_a} \frac{p!}{k_1!,k_2!\ldots k_a!}$，　$\sum_{i=1}^{a} k_i = p$
      (这是多项式系数)
    - 考虑 $\frac{p!}{k_1!,k_2!\ldots k_a!}$，若其中没有$k_i = p$，则 $\frac{p!}{k_1!,k_2!\ldots k_a!} \equiv 0 \pmod{p}$，若有$k_i = p$，则其它$k_j = 0$，于是 $\frac{p!}{k_1!,k_2!\ldots k_a!} \equiv 1 \pmod{p}$；
    - 总共恰有a个$k_i = p$.

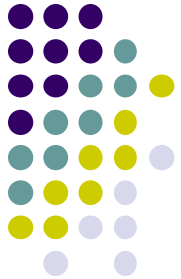
欧拉定理

- **Euler定理. 若正整数*a*与*n*互素，则**

$$a^{\varphi(n)} \equiv 1 \mod n.$$

- 备注：Fermat小定理是欧拉定理的特例，学习群论之后，可较容易地证明欧拉定理。

模幂运算 (modular exponentiation)



- 综合运用中国剩余定理和欧拉/费马小定理，求

$$a^b \bmod c$$

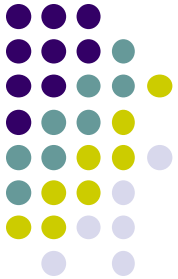
例如：　　$10^{130} \bmod 48$

备注：本周作业内容之一

小结

- 数论的基本内容
  - 整除，同余算术
  - 素数，威尔逊定理
  - 互素, 最大公约数,裴蜀定理
  - 中国剩余定理
  - 费马小定理, 欧拉定理

数学史：数论四大定理



- 《The Elements》，古希腊，**欧几里德**，公元前300年
- 《九章算术》，张苍，耿寿昌，公元前200年
  - 《九章算术注》，**刘徽**（约225年—约295年）
- 《孙子算经》，约400年
- **数论四大定理**
  - 孙子定理（中国剩余定理），约400+年
  - 费马小定理， 1640年提出，欧拉于1736年证明
  - 欧拉定理，1736年证明
  - 威尔逊定理，1770年提出，拉格朗日于1773年证明

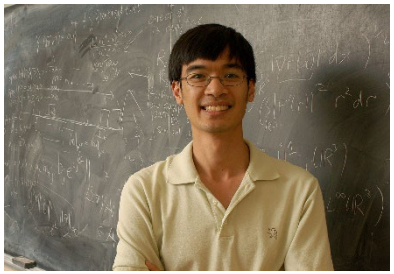
数学史：数论中的猜想

- **哥德巴赫猜想**，1742
  - 1+1：任一大于2的偶数都可以写成2个素数之和？
  - 1+2（陈景润，1966）

- **孪生素数猜想**，1900（23个希尔伯特问题中的第8个）
  - 存在无穷多个素数对 $(p, p+2)$？
  - 存在无穷多组间距小于定值的素数对 (张益唐, 2013)

数学史：素数的分布

- **不超过*n*的素数有多少个？**
  - **接近于*n* / ln *n* (*n*充分大时）**
- **梅森素数 $M_p=2^p-1$**
  - **欧几里德在**《原本》第九章论述了完全数与 2^p-1型素数的关系。
  - **梅森**对这类数做了研究，1644年在《物理数学随感》书中有断言。
  - 搜寻尽可能大的梅森素数，目前只确定51个。
- **任意给定*K*，存在*K*个成等差级数的素数 (陶哲轩,格林, 2004)**
  - 举例：当K=3时，我们有3, 7, 11。



拓展：思考题

证明：$4k+1$ 型的素数有无穷多个.

证明：$4k+3$ 型的素数有无穷多个.

证明：$4k+1$ 型的素数等于两个正整数的平方和.

拓展：RSA的数学基础

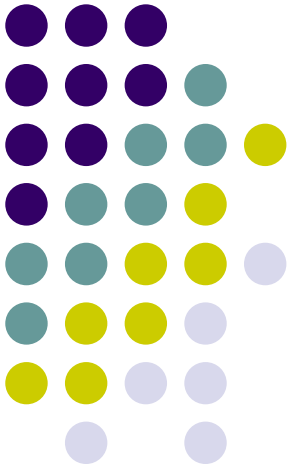
RSA是广泛应用的非对称加密算法. 其可靠性基于大数分解的困难性.

- 若a与n互质，则 $a^{\varphi(n)} \equiv 1 \pmod{n}$,
  - 若$\alpha \equiv 1 \pmod{\varphi(n)}$ ，则 $a^{\alpha} \equiv a \pmod{n}$
- 若$n=pq$, $\alpha \equiv 1 \pmod{\varphi(n)}$, $0<m<n$, 则$m^{\alpha} \equiv m \pmod{n}$
- 选取大质素p, q: $n=pq$ (n难以分解成质素乘积）.
- 令 $k= \varphi(n)$ (不知道n的质因子，k难以求出）.
- 设e为公钥，d为私钥，满足 $ed \equiv 1 \pmod{k}$.
- 加密：$S = m^e \pmod{n}$.
- 解密：$t = S^d \pmod{n}$. ($t = m$，why?)

集合的基数
(Cardinal Number)

离散数学—集合论

南京大学计算机科学与技术系



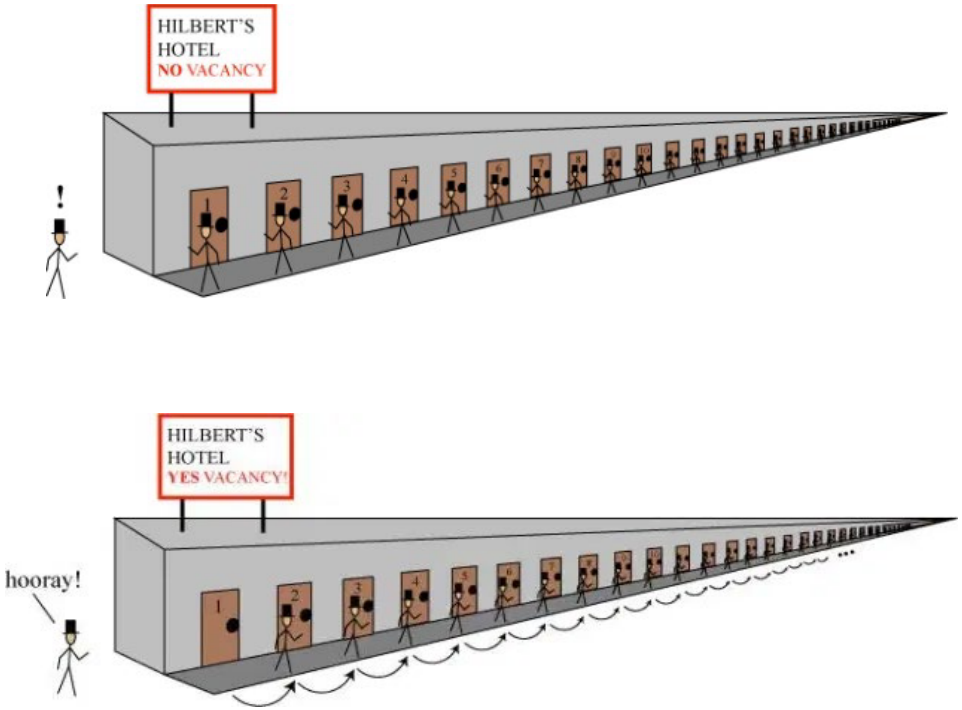
集合的基数

- 引言：有限与无限
- 集合的等势关系
- 集合的基数
- 可数集(Countable set)
- Cantor定理
- 优势关系
- Bernstein定理

我们怎么比较集合的大小

- “数得清”的我们就数元素个数。
- “数不清”的咋办？
  - “常识”不一定经得起追问。

反直觉的无限： Hilbert's Hotel



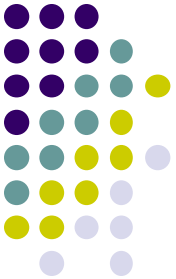
啊?客满啦?
没关系，我让现在住在 k 号房间 的客人移到 k+1 号. 你就住进第 1号房间吧!

再来一百个、一千个客人?
再来“无限”个?

有限与无限：怎样的差别

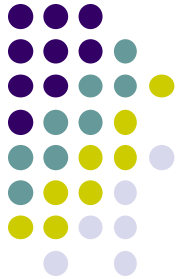
- 传统观点：“整体大于部分”
- {1, 2, 3,…}与{1^2, 2^2, 3^2,…}一一对应

集合的等势关系



- **等势（Equipotent）：** 如果存在从集合A到B的双射，则称集合A与B等势.
  - 记为: $A \approx B$. 不等势记为: $A \not\approx B$.
  - 等势的集合被认为“一样大”, 即$|A|=|B|$, 否则$|A| \neq |B|$.
  - 意味着：A，B中的元素可以“一一对应”.
  - 要证明A≈B，只要找出一个从A到B的双射.
- 等势概念是对“靠数数判断大小一致”的推广

等势关系是等价关系



- 自反性
  - I_A:A→A
- 对称性
  - 如果f:A→B是双射，则f的反函数f^{-1}: B→A，也是双射。
- 传递性
  - 若f:A→B, g :B→C均是双射，则$g \circ f$是从A到C的双射。
- 例子
  - 与自然数集等势的所有集合构成一个等价类。

有限集与无限集

- S是有限集合 *iff* 存在自然数n，使得S与n等势
- S不是有限集合(无限集、无穷集)， *iff* 存在S的真子集S’，使得S与S’等势

⇒ S一定包含一个与自然数集合等势的子集$M = \{a_0, a_1, a_2, \ldots\}$

令$S' = S - \{a_0\}$，可以定义$f: S \to S'$如下：

对于任意$a_i \in M$, $f(a_i) = a_{i+1}$； 对于任意$x \in S - M$, $f(x) = x$.

显然这是双射，即S与其真子集S'等势。

⇐ 假设S是有限集，令$|S| = n$, 则对S的任意真子集S', 若$|S'| = m$，必有$m < n$, 因此S'到S没有双射, 就不可能等势, 矛盾。

集合A的基数

- 若A与自然数n等势，则 $|A| = n$
- 若A与自然数集合N等势，则 $|A| = \aleph_0$
- 若A与实数集合R等势，则 $|A| = \aleph$
- 如果存在从A到N的单射，则称A为可数集，或可列集。$|A| \leq \aleph_0$

无限可数集（无穷可列集）

- 与自然数集等势的集合称为无限可数集
  - 直观上说：集合的元素可以按确定的顺序线性排列，所谓“确定的”顺序是指对序列中任一元素，可以说出：它“前”、“后”元素是什么。
- 整数集(包括负数)与自然数集等势

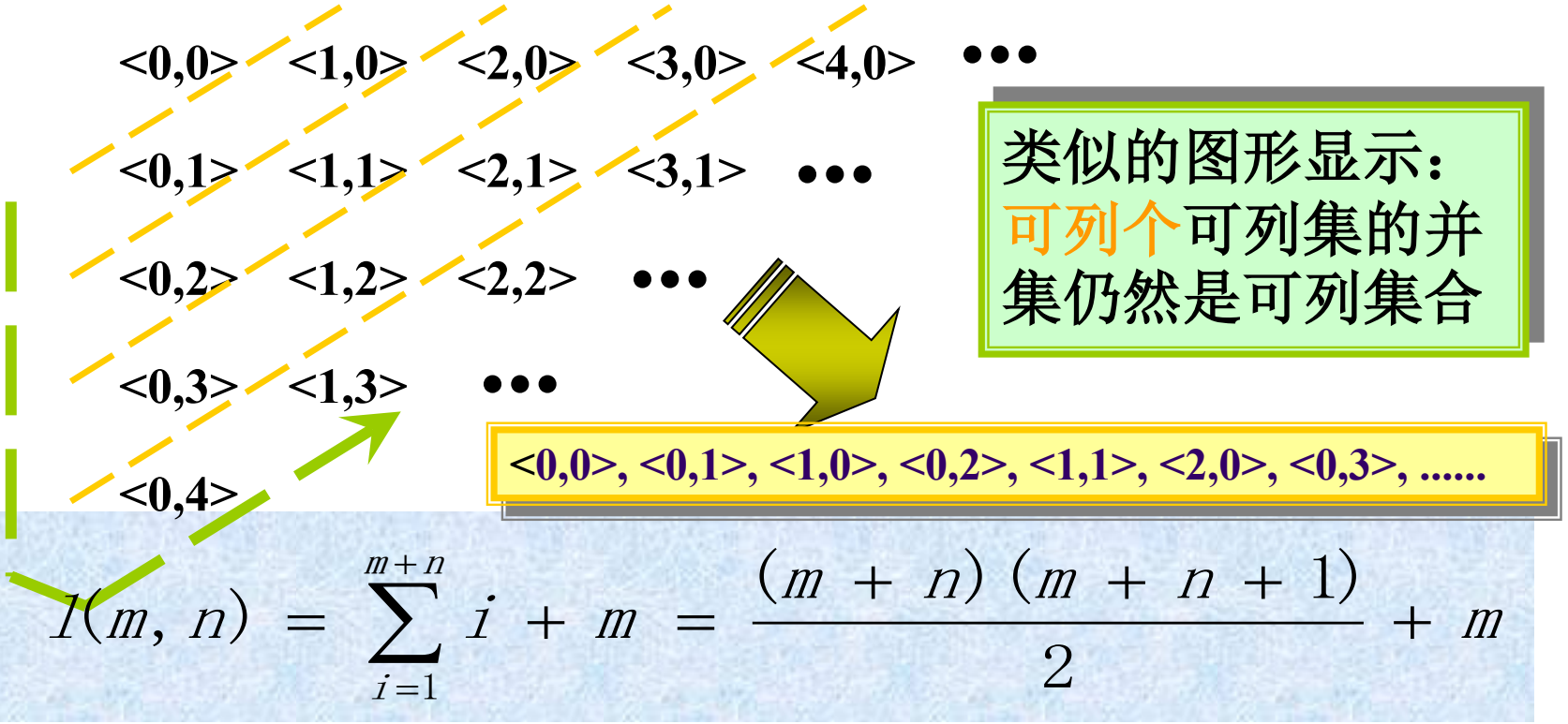
0, -1, 1, -2, 2, -3, 3, -4, ...

0, 1, 2, 3, 4, 5, 6, 7, ...

$$g(n)=\begin{cases} 2n & n>=0 \\ -2n-1 & n<0 \end{cases}$$

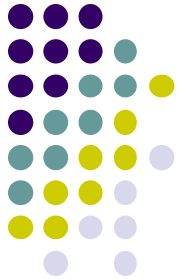
自然数集的笛卡儿积是可列集

- 所有的自然数对构成的集合与自然数集等势



$$I(m, n) = \sum_{i=1}^{m+n} i + m = \frac{(m + n)(m + n + 1)}{2} + m$$

证明无限集等势的例子



- **(0,1)与整个实数集等势** $f:(0,1)\to R:f(x)=\tan(\pi x-\frac{\pi}{2})$
  - 双射：$f:(0,1)\to R:f(x)=\mathrm{tg}(\pi x-\frac{\pi}{2})$
- 对任意不相等的实数a, b $(a<b)$, **[0,1]与[a, b]等势**
  - 双射：$f:[0,1]\to[a,b]:f(x)=(b-a)x+a$

    (这实际上意味着：任意长的线段与任意短的线段等势)

实数集不是可列集

- (0,1)不是可数集 //注意：(0,1)与实数集合等势
  - “对角线证明法”

    假设(0,1)中的所有元素可以按照某种顺序列出：

    $0.b_{11}b_{12}b_{13}b_{14}\cdots$

    $0.b_{21}b_{22}b_{23}b_{24}\cdots$

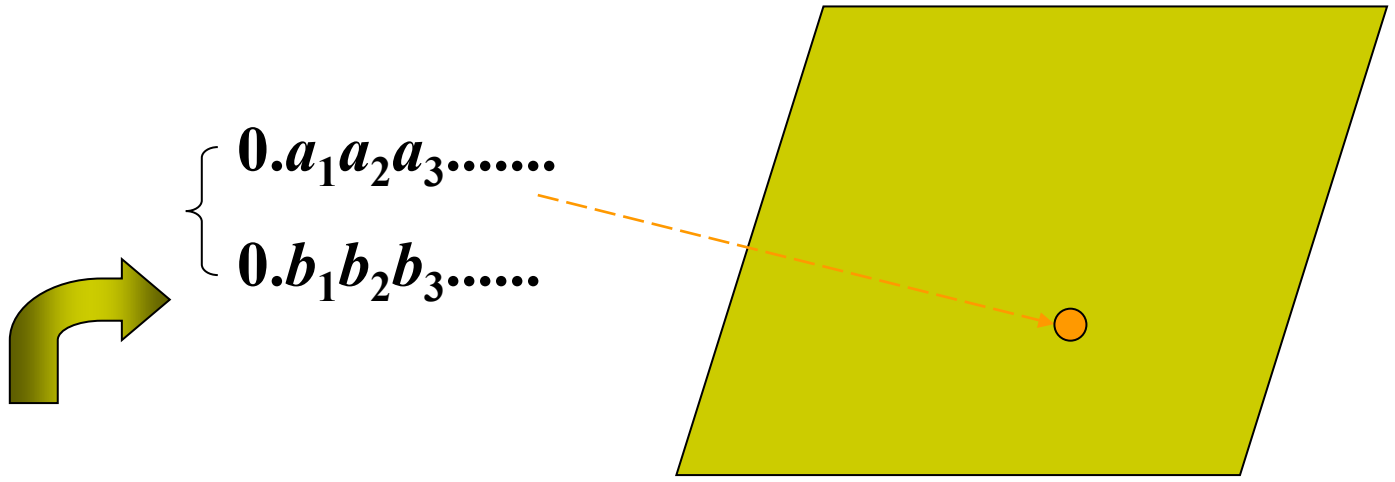
    $0.b_{31}b_{32}b_{33}b_{34}\cdots$

    $0.b_{41}b_{42}b_{43}b_{44}\cdots$

    $\vdots$

    则$0.\ b_1b_2b_3,\ldots(b_i\neq 9,\ b_i\neq b_{ii})$不在上述序列中。

直线上的点集与平面上的点集等势



$0.a_1b_1a_2b_2a_3b_3.....$

这意味着直线上的点与任意有限维空间的点“一样多”！

Cantor（康托尔）定理

- 任何集合与其幂集不等势，即：$A \not\approx \rho(A)$
  - 反证法：设g是从A到ρ(A)的一个双射

    构造集合B如下：

    $$B=\{x \in A \mid x \notin g(x)\}$$

    显然$B \in \rho(A)$，

    由于g是满射，应存在$x_0 \in A$，使得$g(x_0)=B$。

    从而 $x_0 \in B \leftrightarrow x_0 \notin B$。矛盾

  因此，A到ρ(A)的双射并不存在，即 $A \not\approx \rho(A)$ 。

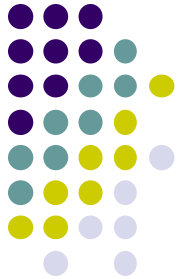
$P(A) = 2^A$

$|P(A)| = 2^{|A|} > |A|$

集合的优势关系

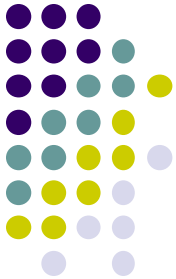
- 如果存在从集合A到集合B的单射，则称“集合B**优势于**集合A”，记为 $|A| \leq |B|$ 或 $A \preccurlyeq \bullet B$
- 如果集合B优势于集合A，且B与A**不等势**，则称“集合B**真优势于**集合A”，记为$|A| < |B|$或$A \prec \bullet B$
- 对任意集合A，A的幂集真优势于集合A
  - 实数集真优势于自然数集 $|\mathbb{N}| < |\mathbb{R}|$

集合优势关系的性质



- 对于任意集合A, 有|A| = |A| (自反性)
  - 显然.
- 若|A| ≤ |B| 且 |B| ≤ |C|, 则 |A| ≤ |C| (传递性)
  - 单射的复合仍然是单射.
- 若|A| ≤ |B| 且 |B| ≤ |A|, 则 |A| = |B| (反对称性)
  - 这个需要仔细证明: Bernstein定理

Bernstein定理的证明

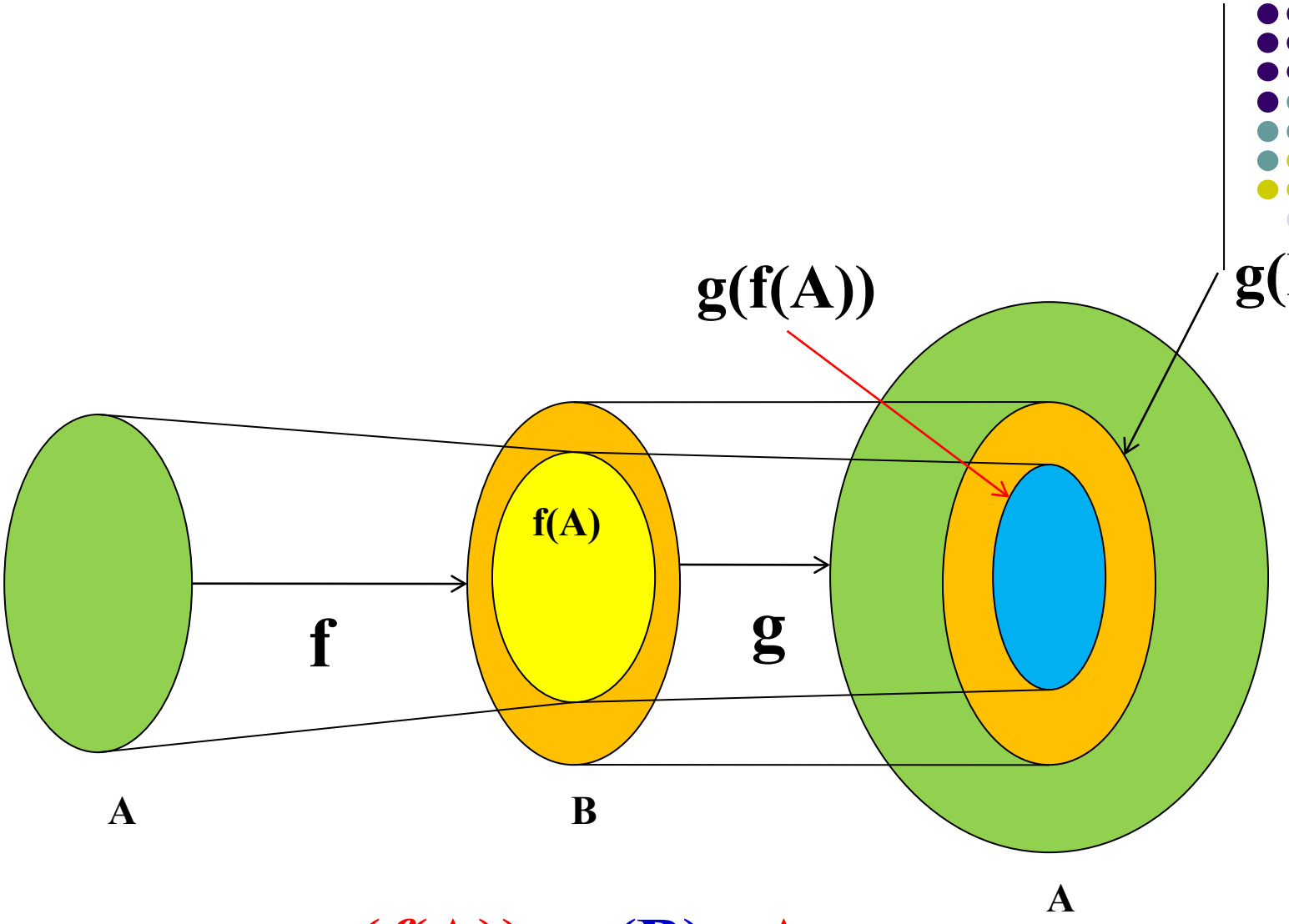


- 若|A| ≤ |B| 且 |B| ≤ |A|, 则 |A| = |B|.
- 证明思路：

由|A| ≤ |B|可知,存在从A到B的单射f，同样，由|B| ≤ |A|,可知，存在从B到A的单射g，于是：$g \circ f$是从A到A的单射。

因为$g \circ f$和g都是单射，所以$g(f(A)) \approx A$, $g(B) \approx B$。

显然$g(f(A)) \subseteq g(B) \subseteq A$, 根据“三明治”引理，$A \approx g(B)$, 从而A≈B。

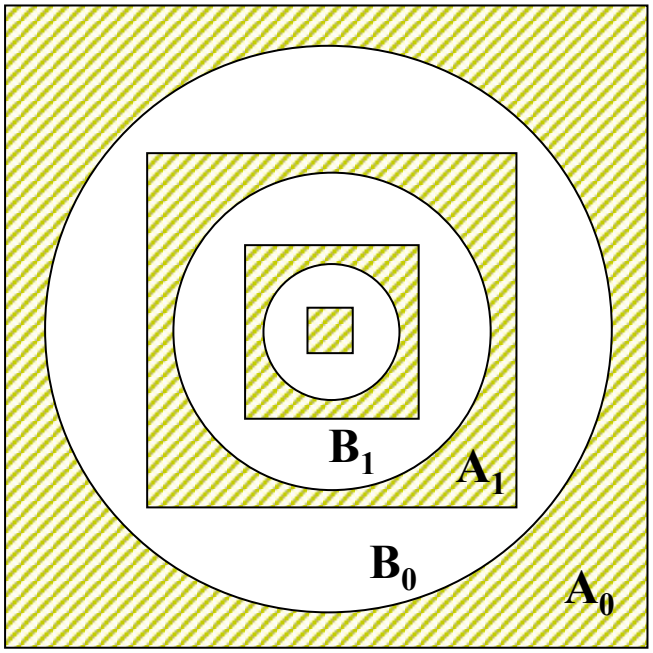


$$g(f(A)) \subseteq g(B) \subseteq A$$

$$g(f(A)) \approx A,\ g(B) \approx B$$

“三明治”引理的证明

- 若$A_1 \subseteq B \subseteq A$, 且$A_1 \approx A$, 则：$B \approx A$



1. 令$A_0=A$, $B_0=B$.

2. 设f是从A_0到A_1的一一对应函数（$A_0 \approx A_1$）令$A_{n+1}=f(A_n)$, $B_{n+1}=f(B_n)$, 递归地得到序列：

$A_0, A_1, \ldots, A_n, \ldots$ 以及 $B_0, B_1, \ldots, B_n, \ldots$

3. 由$A_1 \subseteq B_0 \subseteq A_0$, 得$A_{n+1} \subseteq B_n \subseteq A_n$

4. 令$C_n=A_n-B_n$, $\cup C_n=C$（C即左图阴影部分）, $D=A-C$（图中白色部分）

可以定义从A_0到B_0 的一一对应函数g如下：

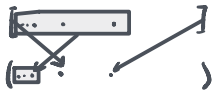
$$g(x)=\begin{cases} f(x) & \text{若} x \in C \quad \text{阴影部分} \\ x & \text{若} x \in D \quad \text{白色部分} \end{cases}$$

证明等势

- 证明实数集的两个子集(0,1)和[0,1]等势。
  - 直接找双射不太容易

关键是如何安排在[0,1]中但不在(0,1)中的0和1。

想象那个“宇宙旅馆”。我们可以取(0,1)的一个与自然数集合等势的子集(一定有)$\{a_1, a_2, a_3, ...\}$, “腾出”前两个位置安排0和1



一种证法：

$$f(x)=\begin{cases}\dfrac{1}{2} & x=0\\ \dfrac{1}{2^2} & x=1\\ \dfrac{1}{2^{n+2}} & x=\dfrac{1}{2^n},\ n=1,2,3...\\ x & x\text{为其它值}\end{cases}$$

证明等势 (续)

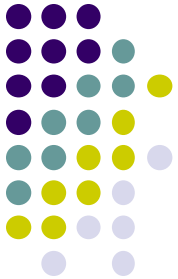
- 证明实数集的两个子集(0,1)和[0,1]等势。
  - 分别找两个单射往往比找一个双射容易

$$f:(0,1)\to[0,1]:f(x)=x$$

$$g:[0,1]\to(0,1):g(x)=\frac{1}{2}+\frac{x}{4}$$

注意：$g([0,1])=[\frac{1}{2},\frac{3}{4}]$

实数集与ρ(N)等势



- $[0, 1) \approx \{0, 1\}^N$ 从而 $R \approx \rho(N)$
  - [0,1)中的数唯一地表示为$0.b_1b_2b_3b_4\ldots$
    不容许连续无数个1，比如1/2=0. 1000… (NOT 0.0111…)
  - $f: [0, 1) \to \{0, 1\}^N$
    $0.b_1b_2b_3b_4\ldots \to b_1, b_2, b_3, b_4\ldots$
    f是单射
  - $g: \{0, 1\}^N \to [0, 1)$
    $b_1, b_2, b_3, b_4\ldots \to 0.b_1b_2b_3b_4\ldots$ //看做十进制数
    g是单射
  - 根据Bernstein定理，得证

连续统假设

不存在集合S：

$\aleph_0 < \text{card } S < \aleph$

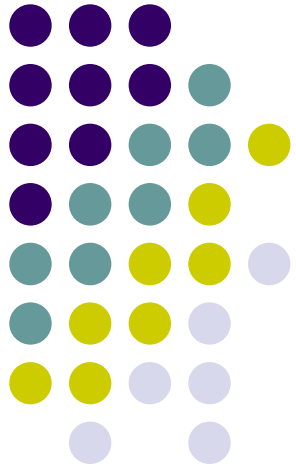
小结

- 无限集比大小的途径: 等势与优势
- 有限集、无限集、可数集、不可数集
- Cantor定理, Bernstein定理
- 集合基数的判定技巧

归纳与递归

离散数学—归纳与递归

南京大学计算机科学与技术系



内容提要

- 数学归纳法
- 强数学归纳法
- 运用良序公理来证明
- 递归定义
- 结构归纳法
- 递归算法

数学归纳法

- 证明目标
  - $\forall n\ P(n)$　//n的论域为正整数集合
- 证明框架
  - 基础步骤：$P(1)$为真
  - 归纳步骤：证明$\forall k\ (P(k) \rightarrow P(k+1))$
    - //对任意正整数k，给出 $P(k) \vdash P(k+1)$ 的论证步骤.
    - …
  - 因此，对任意正整数n, $P(n)$ 成立. // 即：$\forall n\ P(n)$

数学归纳法（有效性）

- 良序公理
  - 正整数集合的非空子集都有一个最小元素
- 数学归纳法的有效性（采用反证法）
  - 假设$\forall n\ P(n)$不成立，则 $\exists n\ (\neg P(n))$成立.
  - 令$S=\{ n \in Z^+ \mid \neg P(n)\}$，S是非空子集.
  - 根据良序公理，S有最小元素，记为m, $m \neq 1$
  - $(m-1) \notin S$, 即$P(m-1)$成立.
  - 根据归纳步骤，$P(m)$成立，即$m \notin S$，矛盾.
  - **因此，** $\forall n\ P(n)$成立.

数学归纳法（举例）

- $H_k=1+1/2+\ldots+1/k$ （k为正整数）
- 证明：$H_2^n \geq 1+n/2$ （n为正整数）
  - 基础步骤：$P(1)$为真， $H_2=1+1/2$
  - 归纳步骤：对任意正整数k, $P(k) \Rightarrow P(k+1)$.

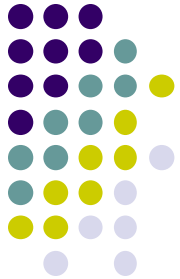
    $H_2^{k+1} = H_2^k +1/(2^k+1)+\ldots+1/2^{k+1}$

    $\geq (1+k/2)+2^k(1/2^{k+1}) = 1+(1+k)/2$
  - **因此**，对任意正整数n, $P(n)$ 成立.

数学归纳法（举例）

- 猜测前n个奇数的求和公式，并证明之。
  - 1=1
  - 1+3=4
  - 1+3+5=9
  - 1+3+5+7=16
  - …
  - $1+3+\ldots+(2n-1)=n^2$（n为正整数）
  - 运用数学归纳法证明（练习）

运用数学归纳法时犯的错误

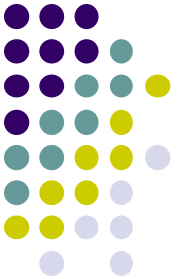


- 平面上任何一组相互间不平行的直线必相交于一点.
  - 基础步骤：$P(2)$为真
  - 归纳步骤：对任意正整数k, $P(k) \vdash P(k+1)$.
    - 前k条交于p_1.
    - 后k条交于p_2.
    - $p_1=p_2$

强数学归纳法

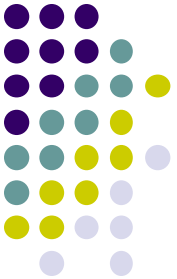
- 证明目标
  - $\forall n\ P(n)$　//n的论域为正整数集合
- 证明框架
  - 基础步骤：$P(1)$为真
  - 归纳步骤：证明$\forall k\ (P(1)\wedge\ldots\wedge P(k)\rightarrow P(k+1))$
    - //对任意正整数k，给出 $P(1), \ldots, P(k) \vdash P(k+1)$ 的论证步骤.
    - …
  - 因此，对任意正整数n, $P(n)$ 成立. // 即：$\forall n\ P(n)$

强数学归纳法（一般形式）



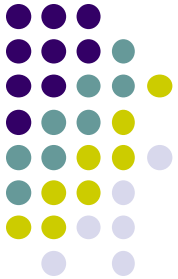
- 设$P(n)$是与整数n有关的陈述， a和b是两个给定的整数，且$a \le b$.
- 如果能够证明下列陈述
  - $P(a), P(a+1), \ldots, P(b)$.
  - 对任意$k \ge b$, $P(a) \wedge \ldots \wedge P(k) \rightarrow P(k+1)$
- 则下列陈述成立
  - 对任意$n \ge a$, $P(n)$.

强数学归纳法（有效性）



- $\{ n \in \mathbf{Z} \mid n \geq a \}$是良序的
  - 良序集：该集合的非空子集都有一个最小元素
- 强数学归纳法的有效性（采用反证法）
  - 假设$\forall n\ P(n)$不成立，则 $\exists n\ (\neg P(n))$成立.
  - 令$S=\{ n \in \mathbf{Z} \mid (n \geq a) \wedge \neg P(n) \}$，S是非空子集.
  - 根据良序公理，S有最小元素，记为m, $m>b$
  - $a, \ldots, (m-1) \notin S$, 即$P(a), \ldots, P(m-1)$成立, 其中 $m-1 \geq b$.
  - 根据归纳步骤，$P(m)$成立，即$m \notin S$，矛盾.
  - **因此，** $\forall n\ P(n)$成立.

强数学归纳法（举例）



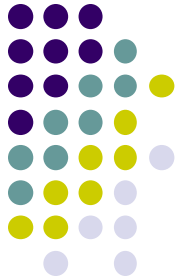
- 任意整数$n(n \geq 2)$可分解为（若干个）素数的乘积
  - $n = 2$.
  - 考察 $n+1$.
- 用4分和5分就可以组成12分及以上的每种邮资.
  - $P(12), P(13), P(14), P(15)$.
  - 对任意$k \geq 15$, $P(12) \wedge \ldots \wedge P(k) \rightarrow P(k+1)$

(强）数学归纳法（举例）

- 对每个正整数$n \geq 4$，$n! > 2^n$
  - 基础步骤：$P(4)$为真，$24 > 16$
  - 归纳步骤：对任意正整数$k \geq 4$, $P(k) \rightarrow P(k+1)$.

    $(k+1)! = (k+1)\, k! > (k+1)\, 2^k > 2^{k+1}$
  - **因此**，对任意正整数$n \geq 4$, $P(n)$ 成立.

运用良序公理来证明（举例）



- 设a是整数, d是正整数, 则存在唯一的整数q和r满足
  - $0 \le r < d$
  - $a = dq + r$
- 证明
  - 令$S=\{a-dq \mid q \in Z, 0 \le a-dq\}$，S非空.
  - 非负整数集合具有良序性
  - S有最小元，记为$r_0 = a-dq_0$.
  - 可证 $0 \le r_0 < d$
  - 唯一性证明， $0 \le r_1 - r_0 = d(q_0-q_1) < d$，因此，$q_1=q_0$

运用良序公理来证明（举例）

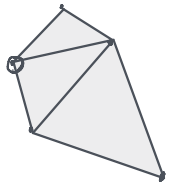
- 在循环赛胜果图中，若存在长度为m（$m\geq 3$）的回路，则必定存在长度为3的回路。

  备注：$a_i \rightarrow a_j$表示a_i赢了a_j

证明

- 设最短回路的长度为k //良序公理的保证
- 假设 $k>3$
- $a_1 \rightarrow a_2 \rightarrow a_3 \rightarrow \ldots \rightarrow a_k \rightarrow a_1$
- 若$a_3 \rightarrow a_1$, 存在长度为3的回路，矛盾。
- 若$a_1 \rightarrow a_3$, 存在长度为$(k-1)$的回路，矛盾。

Odd Pie Fights （奇数个馅饼的对抗）

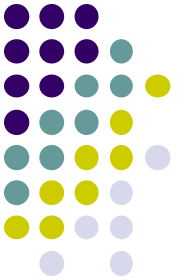


- Placing an odd number of people in the plane, in such a way that every pair of people has a distinct distance between them. At a signal, each person will throw a pie at the closest other person.
- At least one person does not get hit with a pie?
  - 2k+1 → 2k+3 (Let A and B be closest pair of people …)

内容提要

- 数学归纳法
- 强数学归纳法
- 运用良序公理来证明
- 递归定义
- 结构归纳法
- 递归算法

递归定义（N上的函数）



- 递归地定义自然数集合N上的函数。
  - 基础步骤：指定这个函数在0处的值；
  - 递归步骤：给出从较小处的值来求出当前的值之规则。
- **举例，阶乘函数F(n)=n!的递归定义**
  - **F(0)=1**
  - **F(n)=n·F(n-1) for n>0**

斐波那契序列（Fibonacci Sequence）

- 斐波那契序列 $\{f_n\}$ 定义如下
  - $f_0 = 0,$
  - $f_1 = 1,$
  - $f_n = f_{n-1} + f_{n-2},$ 对任意 $n \geq 2.$
- 其前几个数
  - 0, 1, 1, 2, 3, 5, 8, …
- 证明：对任意 $n \geq 0$，

$$f_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

其中，$\alpha = \frac{1+\sqrt{5}}{2}, \beta = \frac{1-\sqrt{5}}{2}.$

归纳证明:斐波那契序列

- 验证：当n=0,1时，陈述正确。
- 对于k+1，$f_{k+1} = f_k + f_{k-1}$

$$= \frac{\alpha^k - \beta^k}{\alpha - \beta} + \frac{\alpha^{k-1} - \beta^{k-1}}{\alpha - \beta}$$

$$= \frac{\left(\alpha^k + \alpha^{k-1}\right) - \left(\beta^k + \beta^{k-1}\right)}{\alpha - \beta}$$

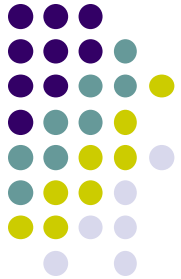
$$= \frac{\alpha^{k+1} - \beta^{k+1}}{\alpha - \beta}.$$

注意：$\alpha^2 = \alpha + 1$，且$\alpha^{n+1} = \alpha^n + \alpha^{n-1}$ 对任意$n \geq 1$.

归纳证明:斐波那契序列

- 证明：当$n \geq 3$时，$f_n > \alpha^{n-2}$
- 基础步骤
  - 当n=3时，$f_3 = 2 > \alpha = (1+\sqrt{5})/2$
  - 当n=4时，$f_4 = 3 > \alpha^2 = (3+\sqrt{5})/2$
- 归纳步骤
  - $n \geq 4$时，$f_{n+1} = f_n + f_{n-1} > \alpha^{n-2} + \alpha^{n-3} = \alpha^{n-1}$.
- 所以，当$n \geq 3$时，$f_n > \alpha^{n-2}$.

递归定义（集合）

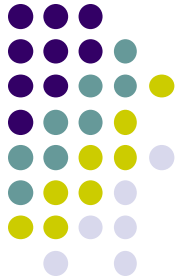


- 递归地定义集合。
  - 基础步骤：指定一些初始元素；
  - 递归步骤：给出从集合中的元素来构造新元素之规则；
  - 排斥规则（只包含上述步骤生成的那些元素）默认成立
- **举例，正整数集合的一个子集S，定义如下：**
  - **$2 \in S$**
  - **若$x \in S$且$y \in S$，则 $x+y \in S$。** 正偶数的集合.

递归定义（举例）

- 字母表Σ上的字符串集合Σ^*。
  - 基础步骤：$\lambda \in \Sigma^*$ （λ表示空串）；
  - 递归步骤：若$\omega \in \Sigma^*$且$x \in \Sigma$，则$\omega x \in \Sigma^*$。
- 字符串的长度（Σ^*上的函数l）。
  - 基础步骤：$l(\lambda)=0$;
  - 递归步骤：$l(\omega x) = l(\omega) +1$, 若$\omega \in \Sigma^*$且$x \in \Sigma$

递归定义（举例）

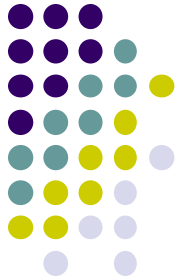


- Σ^*上的字符串连接运算。
  - 基础步骤：若$\omega \in \Sigma^*$，则 $\omega \cdot \lambda = \omega$;
  - 递归步骤：若$\omega_1 \in \Sigma^*$ 且$\omega_2 \in \Sigma^*$ 以及$x \in \Sigma$，则 $\omega_1 \cdot (\omega_2 x) = (\omega_1 \cdot \omega_2) x$ 。
  - // $\omega_1 \cdot \omega_2$通常也写成$\omega_1 \omega_2$

递归定义（举例）

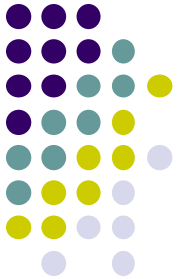
- 复合命题的合式公式。
  - 基础步骤：T, F, *p*都是合式公式，其中*p*是命题变元;
  - 递归步骤：若E和F是合式公式，则 (¬E)、(E∧F)、(E∨F)和(E→F) 都是合式公式。

结构归纳法



- 关于递归定义的集合的命题，进行结构归纳证明。
  - 基础步骤：证明对于初始元素来说，命题成立；
  - 递归步骤：针对产生新元素的规则，若相关元素满足命题，则新元素也满足命题
- 结构归纳法的有效性源于自然数上的数学归纳法

结构归纳法（举例）



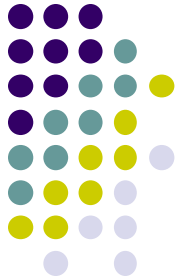
- $l(xy) = l(x) + l(y)$, x和y属于 Σ^* 。
- 证明
  - 设$P(y)$表示：每当x属于 Σ^* ，就有$l(xy) = l(x) + l(y)$ 。
  - 基础步骤： $P(\lambda)$为真
    - 每当x属于 Σ^* ，就有$l(x\lambda) = l(x) + l(\lambda)$ 。
  - 递归步骤：假设$P(y)$为真，a属于 Σ, 要证$P(ya)$为真。
    - 即：每当x属于 Σ^* ，就有$l(xya) = l(x) + l(ya)$
    - $P(y)$为真，$l(xy) = l(x) + l(y)$
    - $l(xya)= l(xy)+1= l(x) + l(y)+1=l(x) + l(ya)$

广义结构归纳法（举例）

- 递归定义$a_{m,n}$
  - $a_{0,0} = 0$
  - $a_{m,n} = a_{m-1,n} + 1 \quad (n=0, m>0)$
  - $a_{m,n} = a_{m,n-1} + n \quad (n>0)$
- 归纳证明 $a_{m,n} = m + n(n+1)/2$

0	1	3
1	2	4
2	3	5

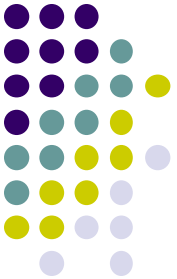
递归算法（欧几里德算法）



```
function gcd(a, b)  // a≥b≥0, a>0
 if b=0
        return a
 else
        return gcd(b, a mod b)
```

- 递归算法的正确性
- 递归算法的复杂性 （时间、空间）

欧几里德算法的复杂性

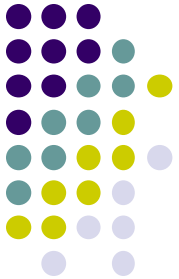


- 拉梅定理: 设a和b是满足$a \geq b$的正整数。则欧几里德算法为求出gcd(a, b)而使用除法的次数小于或等于b的十进制位数的5倍。$5(\lfloor \log_{10} b \rfloor + 1)$

- 令$r_0 = a$, $r_1 = b$.
- $r_0 = r_1 q_1 + r_2 \qquad 0 \leq r_2 < r_1$
- $r_1 = r_2 q_2 + r_3 \qquad 0 \leq r_3 < r_2$
- …
- $r_{n-1} = r_n q_n + r_{n+1} \quad 0 = r_{n+1} < r_n$
- gcd(a, b) = r_n使用了n次除法

- $q_i \geq 1$ for $1 \leq i < n$
- $q_n \geq 2$ because $q_n = r_{n-1}/r_n > 1$
- $r_n \geq 1 = f_2$, $r_{n-1} \geq 2r_n \geq 2 = f_3$
- $b = r_1 \geq r_2 + r_3 \geq f_n + f_{n-1} = f_{n+1} > \alpha^{n-1}$
- $\log_{10} b > (n-1)\log_{10} \alpha$ for $n \geq 2$
- $\log_{10} \alpha > 1/5$
- $n - 1 < 5 \log_{10} b$

递归算法的设计



- a^n
- $b^n \ mod \ m$

基本计数技术

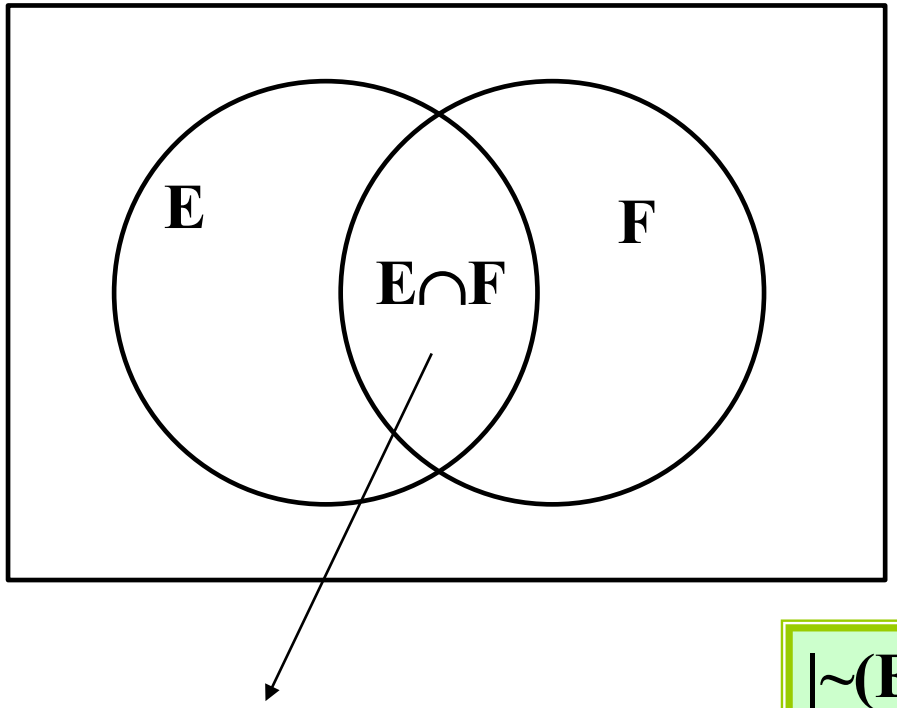
瞿裕忠

南京大学计算机科学与技术系

内容提要

- 容斥原理
- 错位排列
- 鸽巢原理

有限集的基数（如何计算？）



既学英语，又学法语的同学

假设全班共100人，记为

$$|U| = 100$$

学英语的50人，学法语的30人，分别记为：

$$|E| = 50;\ |F| = 30$$

既不学英语，也不学法语的人数可能多于20人。

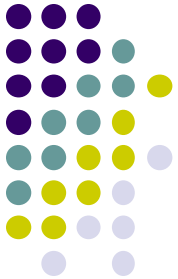
$$|\sim(E \cup F)| = |U| - |E \cup F|$$

$$= |U| - ((|E|+|F|) - |E \cap F|)$$

多少种排法？

- 将0,1,2,...,9排成一列，要求第1个数字大于1，最后一个数字小于8，共有多少种排法？
  - 这10个数字所有的排法构成全集U, |U|=10!
  - 第1个数字不大于1的排法构成子集A(即所有以0或者1开头的排法), |A|=2•9!
  - 最后一个数字不小于8的排法构成子集B(即所有以8或者9结束的排法), |B|=2•9!
  - $|A \cap B|=2 \cdot 2 \cdot 8!$
  - 题目要求的排法构成子集$(\sim A \cap \sim B)$
  - $|(\sim A \cap \sim B)| = |U| - |A \cup B| = |U| - |A| - |B| + |A \cap B| = 10! - 4 \cdot 9! + 4 \cdot 8! = 2{,}338{,}560$

三个集合的并集（计算基数）



- 假设定义全集的三个子集A,B,C。则：

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

- 证明：

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

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

$$=|A|+|B|-|A\cap B|+|C|-|(A\cap C)|-|(B\cap C)|+|(A\cap B\cap C)|$$

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

关于选课的例子

- 全班共有160个学生
  - 选数学课64人，选计算机课94人，选金融课58人
  - 选数学与金融的28人，选数学与计算机的26人，选计算机与金融的22人
  - 三种课全选的14人。
- 问：这三种课都没选的是多少？只选一门计算机的有多少？

问题的解

- M-数学、C-计算机、F-金融
- 包含-排斥原理

  |M∪C∪F|=|M|+|C|+|F|-|M∩F|-|M∩C|-|C∩F|+|M∩C∩F|

  =64+94+58-28-26-22+14

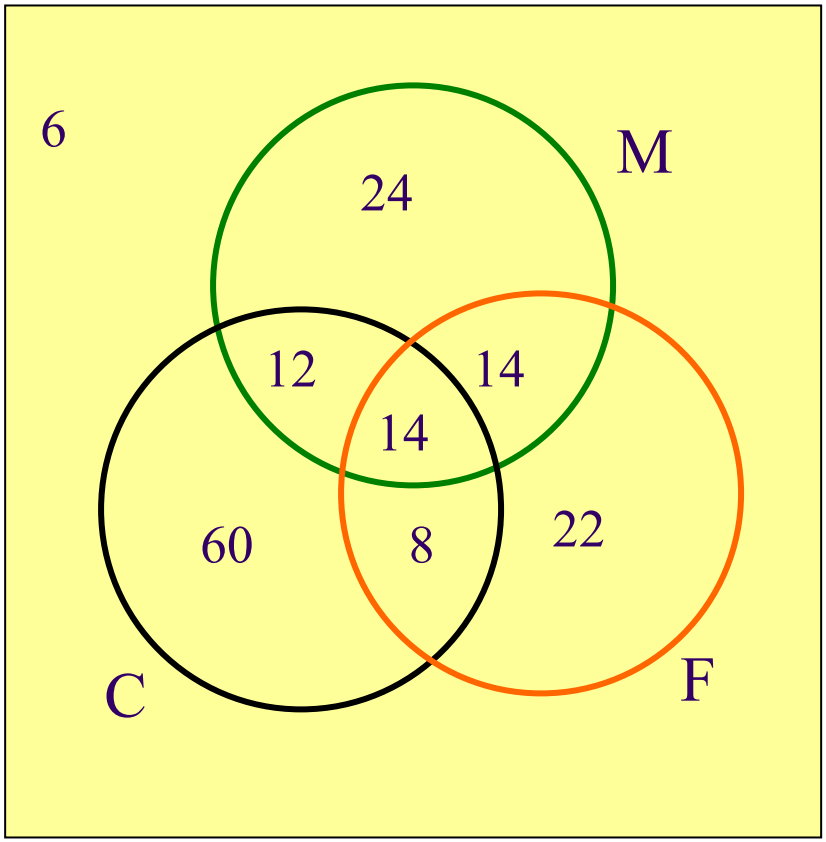
  =154

未选课的6人。

只选了计算机课的60人

|C|-|C∩(M∪F)|=

|C|-|M∩C|-|C∩F|+ |M∩C∩F|



容斥原理 (Inclusion-Exclusion Principle)

假设全集含N个元素，$A_1, A_2, ..., A_n$是分别满足相应性质的元素构成的子集合。则不满足任何性质的集合的元素个数是：

$$N(\overline{A_1}\,\overline{A_2}\ldots\overline{A_n}) = N - S_1 + S_2 + \ldots + (-1)^k S_k + \ldots + (-1)^n S_n$$

其中，$S_k = \sum_{1\le i_1\le i_2\le\ldots\le i_k\le n} |A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}|$　　$k = 1,2,...,n$

例如：4个子集的公式为：

$$N - (|S_1| + |S_2| + |S_3| + |S_4|)$$
$$+ (|S_1 \cap S_2| + |S_1 \cap S_3| + |S_1 \cap S_4| + |S_2 \cap S_3| + |S_2 \cap S_4| + |S_3 \cap S_4|)$$
$$- (|S_1 \cap S_2 \cap S_3| + |S_1 \cap S_2 \cap S_4| + |S_1 \cap S_3 \cap S_4| + |S_2 \cap S_3 \cap S_4|)$$
$$+ |S_1 \cap S_2 \cap S_3 \cap S_4|$$

埃拉托色尼筛选法(Sieve of Eratosthenes)

- 用筛选法求质数（以25以内的为例）

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

[2] 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

[3] 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

[5] 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

100以内有多少质数

- **100以内的任意合数必有不大于其平方根的质数为其因子。这样的质数只有4个：{2, 3, 5, 7}**
- **设A_2, A_3, A_5, A_7 分别是可被相应质数整除的100以内大于1的自然数的集合。则100以内质数的数量为：**

why?　　[2..100]

$$N(\overline{A_2}\,\overline{A_3}\,\overline{A_5}\,\overline{A_7})+4=99-\left\lfloor\frac{100}{2}\right\rfloor-\left\lfloor\frac{100}{3}\right\rfloor-\left\lfloor\frac{100}{5}\right\rfloor-\left\lfloor\frac{100}{7}\right\rfloor$$

$$+\left\lfloor\frac{100}{2\cdot3}\right\rfloor+\left\lfloor\frac{100}{2\cdot5}\right\rfloor+\left\lfloor\frac{100}{2\cdot7}\right\rfloor+\left\lfloor\frac{100}{3\cdot5}\right\rfloor+\left\lfloor\frac{100}{3\cdot7}\right\rfloor+\left\lfloor\frac{100}{5\cdot7}\right\rfloor$$

$$-\left\lfloor\frac{100}{2\cdot3\cdot5}\right\rfloor-\left\lfloor\frac{100}{2\cdot3\cdot7}\right\rfloor-\left\lfloor\frac{100}{2\cdot5\cdot7}\right\rfloor-\left\lfloor\frac{100}{3\cdot5\cdot7}\right\rfloor+\left\lfloor\frac{100}{2\cdot3\cdot5\cdot7}\right\rfloor+4$$

$$=99-50-33-20-14+16+10+7+6+4+2-3-2-1-0+0+4$$

$$=25$$

Euler's totient (ϕ函数, Phi)

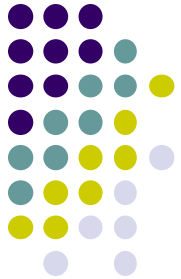
- $\phi(n) = |\{ k \mid 1 \le k \le n , \gcd(k, n) = 1\}|, n \in Z^+$
  - $\phi(3) = 2, \phi(4) = 2, \phi(12) = 4$
- 设 $n = p_1^{\alpha 1} p_2^{\alpha 2} \ldots p_k^{\alpha k}$
- 令 $A_i = \{ x \mid 1 \le x \le n , p_i$整除$x\}$
- $\phi(n) = | \sim A_1 \cap \sim A_2 \cap \ldots \cap \sim A_k |$

$$= n - (n/p_1 + \ldots + n/p_k) + (n/p_1p_2 + \ldots + n/p_{k-1}p_k)$$

$$- \ldots + (-1)^k n/p_1p_2 \ldots p_k$$

$$= n(1 - 1/p_1)(1 - 1/p_2) \ldots (1 - 1/p_k)$$

粗心的衣帽间管理员



- 剧场的衣帽管理间新来了一个粗心的管理员,他忘了给每个客人的帽子夹上号码牌。散场时他只好随意地将帽子发还给客人。没有任何人拿到自己的帽子的概率是多少？
- 这可以看作一个排列问题：对标号为1,2,3,…,n的n个帽子重新排列，新的序号为$i_1, i_2, i_3,\ldots,i_n$。上述问题即：满足对任意k $(1\le k\le n)$, $i_k\neq k$的排列出现的概率是多少？
- 这样的排列称为“错位排列”(derangement)。

错位排列的个数 – 推导

- 我们将$i_k=k$称为“性质A_k”，满足该性质的排列构成一个集合A_k。

错位排列的个数为：

$$N(\overline{A_1}\,\overline{A_2}\,\overline{A_3}\ldots\overline{A_n}) = N - S_1 + S_2 - S_3 + \ldots + (-1)^k S_k + \ldots + (-1)^n S_n$$

其中：$N = n!$

S_k如前面的定义，即 $\sum_{1\le i_1\le i_2\ldots\le i_k\le n} |\, A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k} \,|$

注意：保持k项不变的置换，即其余$n-k$项可任意排列。

所以：

$$S_1 = \binom{n}{1}(n-1)!;\ S_2 = \binom{n}{2}(n-2)!;\ \ldots,\ S_k = \binom{n}{k}(n-k)! = \frac{n!}{k!}$$

错位排列的个数 – 计算

我们已经知道错位排列的个数为：

$$N(\overline{A_1}\,\overline{A_2}\,\overline{A_3}\ldots\overline{A_n}) = N - S_1 + S_2 - S_3 + \ldots + (-1)^k S_k + \ldots + (-1)^n S_n$$

其中：$N = n!$

将诸$S_k = \binom{n}{k}(n-k)! = \frac{n!}{k!}(k = 1,2,3,\ldots,n)$代入上面的式子：

$$\therefore N(\overline{A_1}\,\overline{A_2}\,\overline{A_3}\ldots\overline{A_n}) = n!\sum_{k=0}^{n}\frac{(-1)^k}{k!};\quad \therefore \text{要求的概率是:}\sum_{k=0}^{n}\frac{(-1)^k}{k!}$$

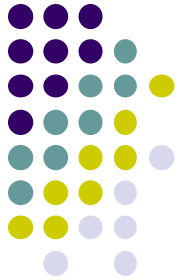
注意：$\sum_{k=0}^{\infty}\frac{(-1)^k}{k!} = e^{-1}$，所以这概率值与$e^{-1} \approx 0.367879$误差小于$\frac{1}{n!}$；

换句话说，除了较小的n，所求概率约为0.36788。

Pigeonhole Principle (Dirichlet, 1834)

- If n pigeons are assigned to m pigeonholes, and $m<n$, then at least one pigeonhole contains two or more pigeons.

Extended Pigeonhole Principle

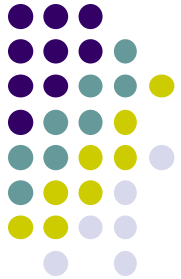


- If n pigeons are assigned to k pigeonholes, then one of the pigeonholes must contain at least $\lceil n/k \rceil$ pigeons.
  - Proof by contradiction

    If each pigeonhole contains no more than $\lceil n/k \rceil - 1$, then there are at most $k(\lceil n/k \rceil - 1) < n$ pigeons.

    It's a contradiction.

Pigeonhole (birthday example)



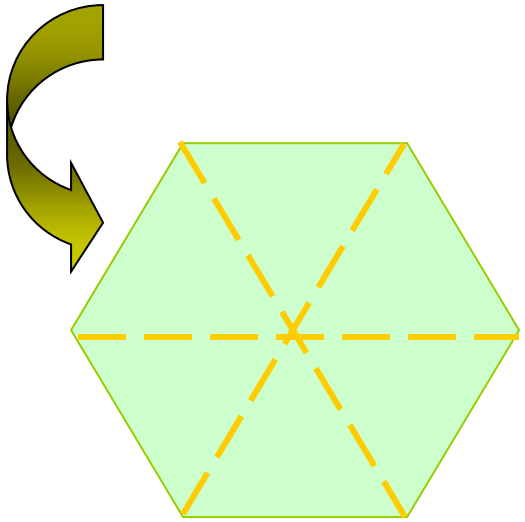
- There are 75 students in our class. How many students at least were born in the same month?
- Solution
  - $\lceil 75/12 \rceil = 7$
  - Among 13 persons, there are at least 2 persons who born in the same month.

Examples

- **Show that if any five numbers from 1 to 8 are chosen, then two of them will add to 9**
  - **Mathematical modeling?**
- **If any 11 numbers are chosen from the set {1,2,…20}, then one of them will be a multiple of another**
  - $a_j = 2^{kj} q_j$ **([1], [3], [5], [7], ….[19])**

Not Too Far Apart

Problem: We have a region bounded by a regular hexagon whose sides are of length 1 unit. Show that if any seven points are chosen in this region, then two of them must be no farther apart than 1 unit.



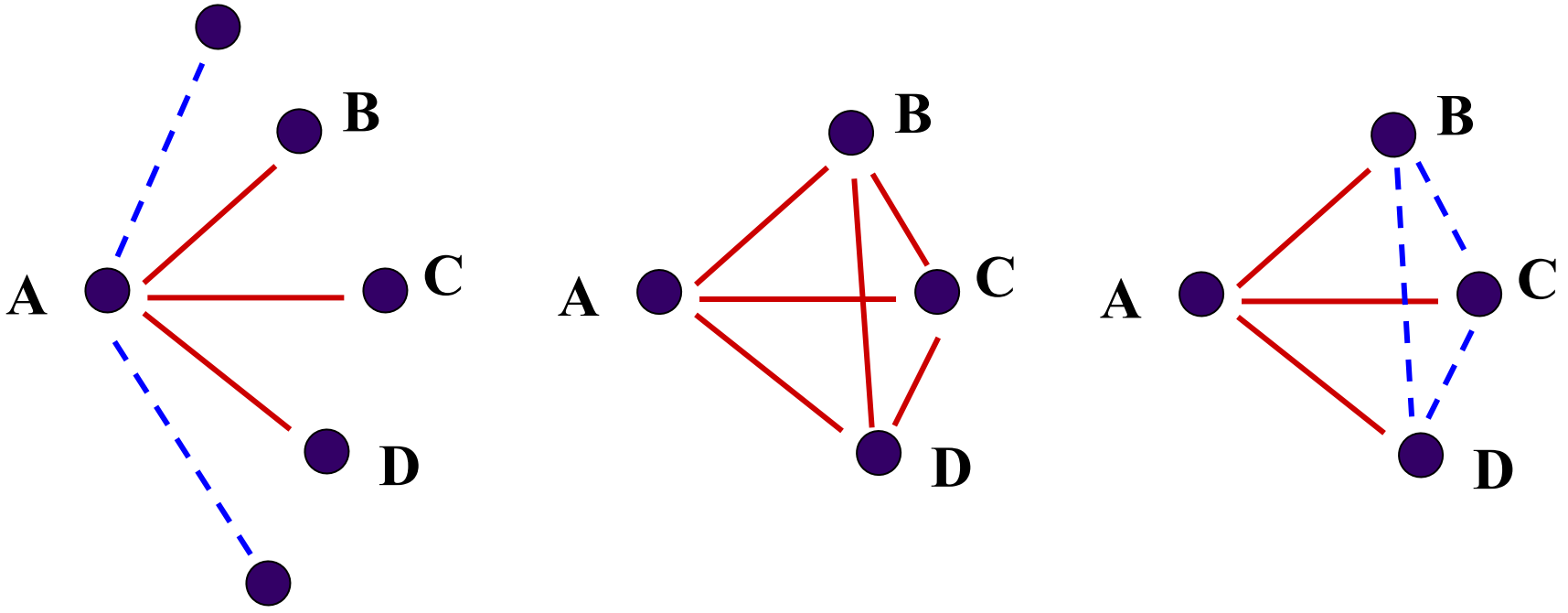
The region can be divided into six equilateral triangles, then among 7 points randomly chosen in this region must be two located within one triangle.

再例

- 任给一个正整数*n*，总存在一个它的倍数，其十进制表示中只有0和1两个数字符
  - 任给*n*，构造*n*+1个数的数列
    - 1，11，111，1111，…,，11**11
  - *n*+1个数必有两个数模*n*同余
  - 这个两个数的差：*n*的倍数，只有0和1

朋友和陌生人定理

任意6人中, 至少有3人相互认识, 或者至少有3人互不相识.



计数 – 排列组合

南京大学计算机科学与技术系

引言–算法分析中的计数

- k:=0
- for i:=1 to m
  k:=k+1
- for j:=1 to n
  k:=k+1

* k:=0
* for i:=1 to m
  for j:=1 to n
  k:=k+1

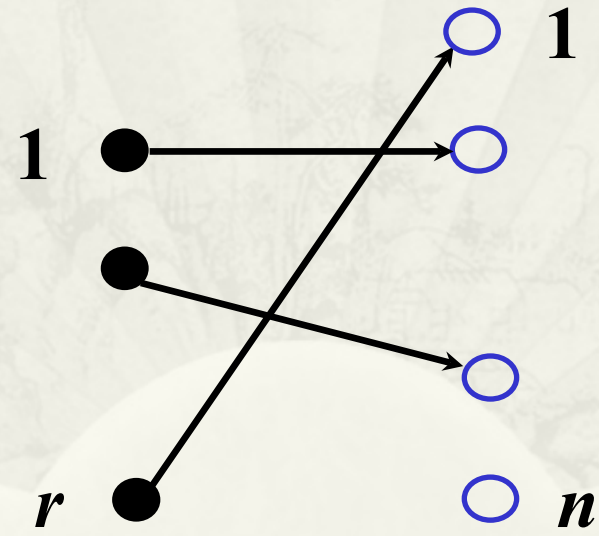
* k:=0
* for i_1:=1 to n
  for i_2:=1 to i_1
  for i_3:=1 to i_2
  k:=k+1

基本原则

- 加法原则
  - 一件事情有两种做法，第一种做法有n种方式，第二种做法有m种方式，则完成这件事情共有$m+n$种方式
  - 例：
    - 在37位教师和83位学生中选一位校委会代表，多少种选择？
- 乘法原则
  - 做一件事有两个步骤，第一步有n种完成方式，第二步m种完成方式，则完成这件事情共有$m \times n$种方法
  - 例:
    - A是有限集合，$|A|=n$. A的幂集有几个元素？
      - $|p(A)| = 2^n$

n个元素的r排列

- 在n个元素的集合中，有序取出r个元素，元素不重复，有多少种可能？
  - $P(n,r)= n(n-1)\ldots(n-r+1)=n!/(n-r)!$　//$P(n,0)=1$



*r*个“对象”到*n*个对象的单射

例题

- 从52张扑克牌中发5张牌，如果考虑发牌次序，共有多少种牌型？
- 密码是字母开头8位长英文字母和数字串，总共可以设计多少个密码？
- 密码是字母开头8位长英文字母和数字串，如果不允许字母或者数字重复，总共可以设计多少个密码？
- 将26个英文字母进行排列，有多少种排列以NJU开头？
- 将26个英文字母进行排列，有多少种排列中含有NJU串？

r组合

- 考察有n个元素的集合，如果取r个元素出来，共有多少种取法？
  - 含有r个元素的子集的个数
  - r组合：$c(n,r)=P(n,r)/r! = n!/[r!(n-r)!]$

用乘法原则来证明！

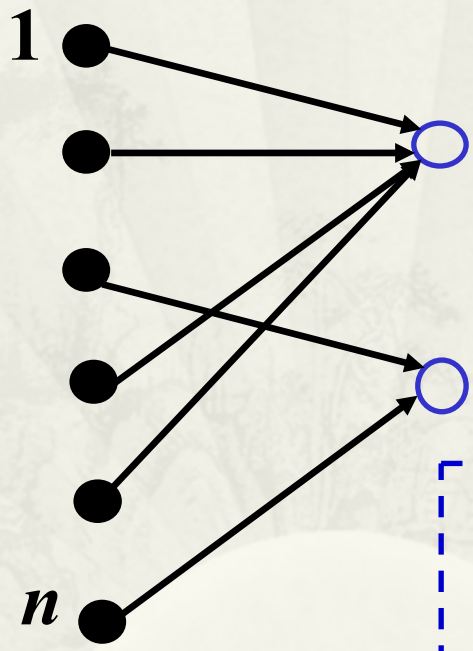
r组合：$\mathbf{c(n, r) = c(n, n-r)}$

示例

- 从52张扑克牌中发47张牌，如果不考虑发牌次序，共有多少种牌型？
- 从5个妇女和15个男性中选出一个包含2名妇女的5人委员会，有多少种可能？
- 从5个妇女和15个男性中选出一个至少包含2名妇女的5人委员会，有多少种可能？

*r*组合

- n个元素的集合到{Y, N}的函数，共有2^n个



$|f^{-1}(Y)|=r$

$\Sigma_r\, c(n,r)=2^n$

含有r个1的n位0-1串

园排列

- 从n个不同元素中，取r个不重复的元素排成一个圆圈，有$\mathrm{P}(n,r)/r$种排列方法

$$\frac{A_n^r}{r}$$

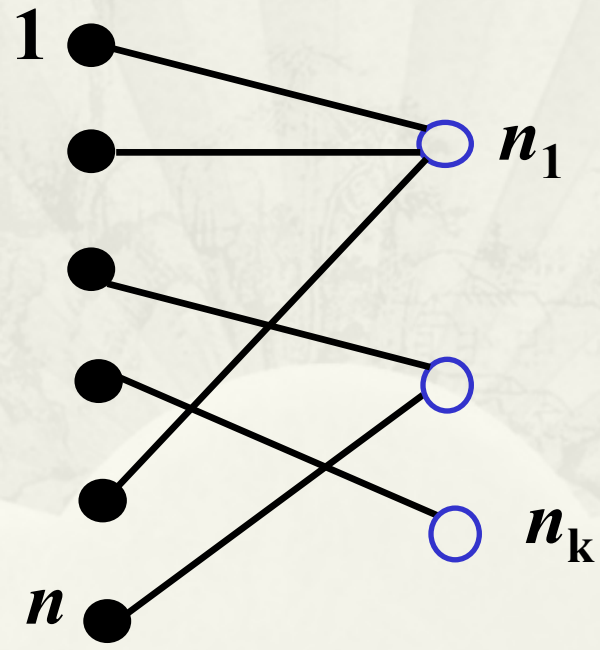
有重复（不可区分）物体的排列

- 把单词“**mathematics**”中的字母重新排列，可以得到多少个不同的字符串（单词）？
- 2个*m*，2个*a*，2个*t*，1个h，1个*e*，1个*c*, 1个*i*, 1个*s*.
- 11个位置(2+2+2+1+1+1+1+1)，选2个放置*m*，
- 乘下的9个位置，选2个放置*a*，
- …
- C(11, 2) C(9, 2) C(7, 2) C(5, 1) C(4, 1) C(3, 1) C(2, 1) C(1, 1)
- 11!/(2! 2! 2! 1! 1! 1! 1! 1!)

有重复的排列

- 在n个有不可区分项的对象集中，若有k类对象，各类对象的数目分别为$n_1, \ldots, n_k$, n排列的个数是：
- $n!/(n_1! \ldots n_k!)$, 其中 $n=n_1+\ldots+n_k$

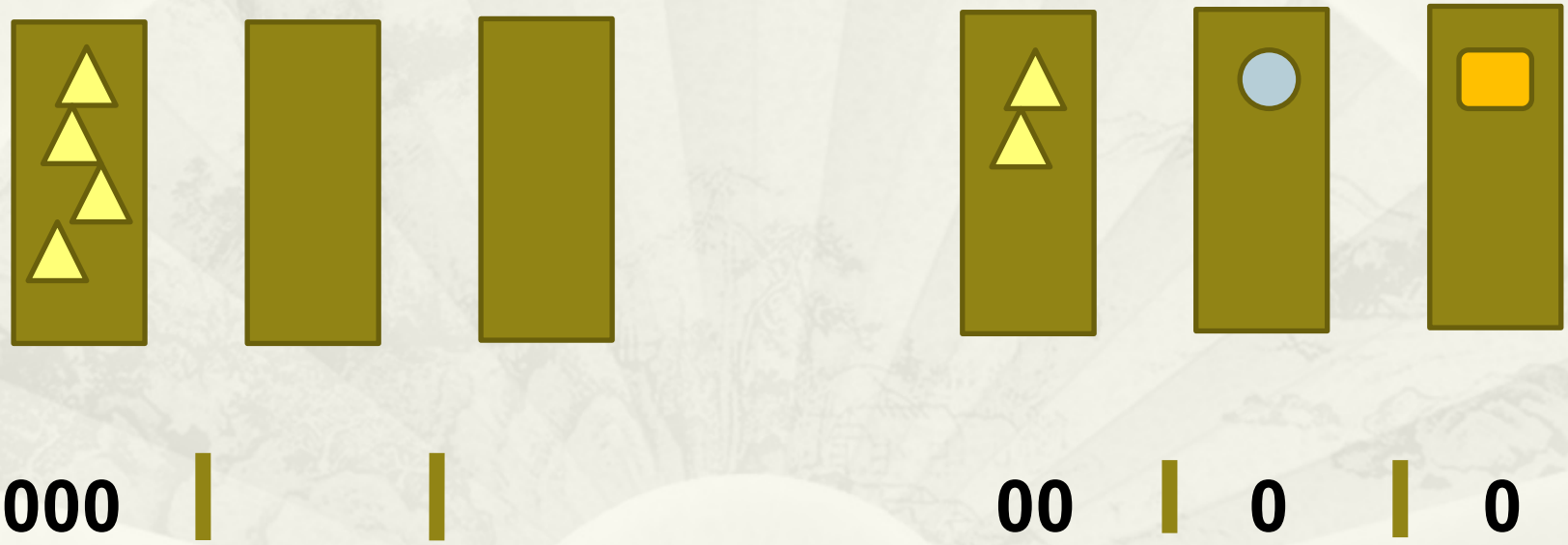
$$\frac{(\sum_{i=1}^{k} n_i)!}{\prod_{i=1}^{n}(n_i!)}$$



n个不同位置赋予k个类别，各类别的数量为$n_1,\ldots,n_k$

有重复的组合

- 厨房有三种水果，每样都足够多（超过4个）。从厨房取4个水果，有多少种取法？



一种取法对应于一个有4个0和2个1构成的0-1串，C(6, 4)

n种不同元素中，可重复的r组合

* C(r+n-1, r)
  * 含r个0和(n-1)个1的0-1串，这种0-1串的个数
* 例
  * 甜点店4种面包，买6个面包的买法有几种？

```
k:=0
for i1:=1 to n
    for i2:=1 to i1
        for i3:=1 to i2
            k:=k+1
```

可重复地从{1, …,n}中选取3个数：$n \geq i_1 \geq i_2 \geq i_3 \geq 1$

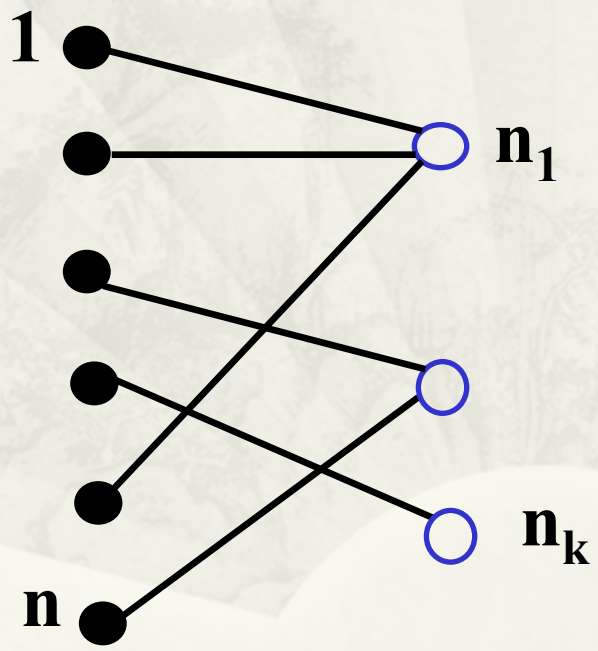
C(n+2, 3)

n种不同元素中，可重复的r组合

- $x+y+z=11$有多少组解？其中x,y,z是非负整数
  - 3种水果足够多，取11个水果的方案 C_{13}^{3}
- 如果$x\geq 1, y\geq 2, z\geq 3$时，上述方程有多少组解？
  - $(x'+1)+(y'+2)+(z'+3)=11$，其中x', y', z'是非负整数
  - $x'+y'+z'=5$，其中x', y', z'是非负整数 C_{7}^{3}

不同物体分配到不同盒子

- n个不同物体分配到k个不同的盒子中，使得第i个盒子包含n_i个物体（i=1,…,k），有多少种分配方案？

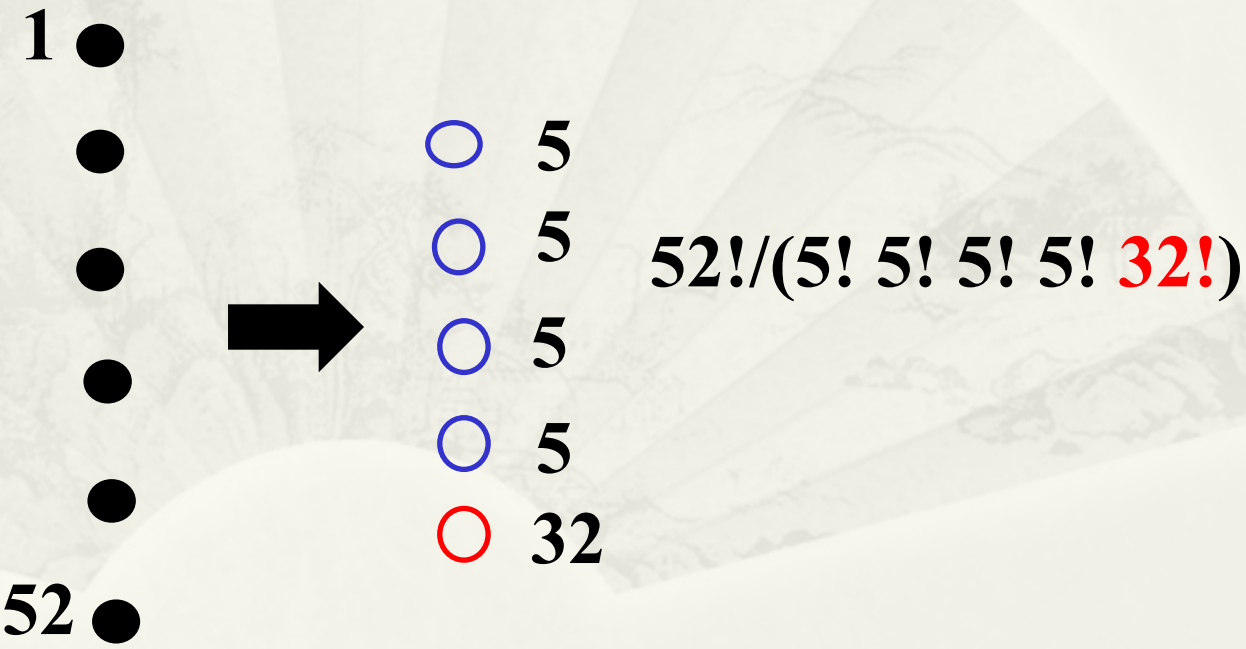


$C(n, n_1)\, C(n-n_1, n_2)\ldots$

$n!/(n_1!\ \ldots n_k!)$

不同物体分配到不同盒子（示例）

- 52张扑克牌发给4个人使得每人5张
  - 意味着“第5人”拿到32张



相同物体分配到不同盒子

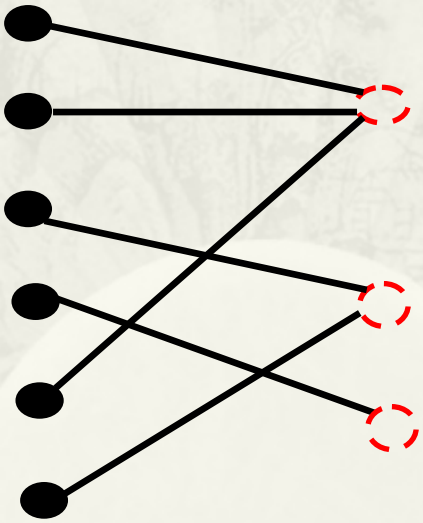
- n个相同物体分配到k个不同的盒子中，有多少种分配方案？

$x_1+\ldots+x_k=n$ 的非负整数解

含n个0和$(k-1)$个1的0-1串，$C(n+k-1, n)$

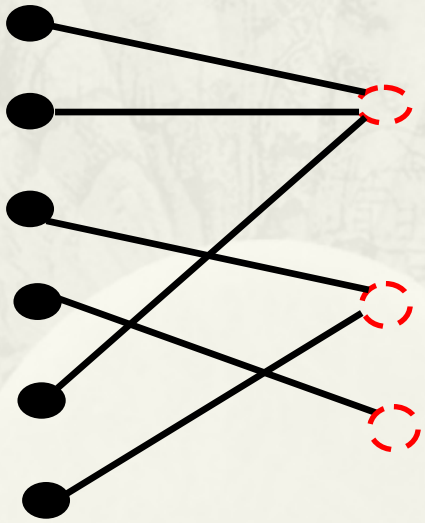
不同物体分配到不可辨别的盒子

- S(n, k): Stirling number of the second kind
  - n个物体分配到k个不可辨别的盒子中，不允许空盒
  - k-划分 (n≥k)
- S(n+1, k) = k * S(n, k) + S(n, k-1), S(0, 0)=1



Stirling number of the second kind

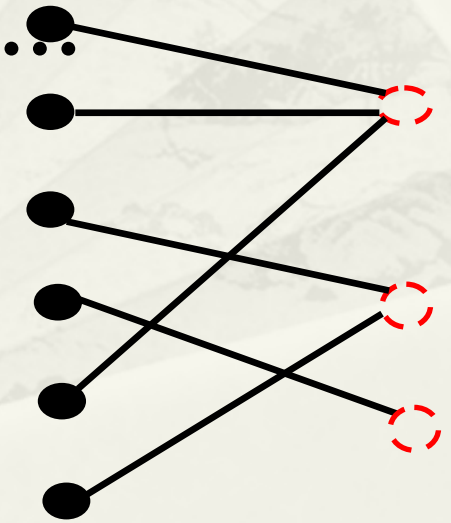
- S(n, k), 或 $\left\{ {n \atop k} \right\}$
  - n个不同物体分配到k个不可辨别的盒子，不允许空盒
  - k-划分 (n≥k)
- k! S(n, k): [1..n] → [1..k] 满射的个数



Stirling number of the second kind

- **[1..n] → [1..k] 满射的个数？ （Section 8.6）**
- **U={ f | f :[1..n] → [1..k] },**
- **A_j={$f \in U \mid f(x) \neq j, x=1, \ldots n\}$, j=1,..,k**
- **k^n-C(k, 1) $(k-1)^n$+C(k, 2) $(k-2)^n$- ...**

$$\left\{ {n \atop k} \right\} = \frac{1}{k!} \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} j^n.$$



不同物体分配到不可辨别的盒子

- n个不同物体分配到k个不可辨别的盒子，允许空盒
  - $\Sigma_{j=1..k}\ S(n,j)$
- n个元素上的等价关系（个数）
  - $B_n=\Sigma_{j=1..n}\ S(n,j)$ // Bell number
  - $B_0=B_1=1$

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k.$$

相同物体分配到不可辨别的盒子

- k个盒子，不允许空盒
  - $x_1+\ldots+x_k=n$ 的正整数解，$x_1\geq\ldots\geq x_k\geq 1$
- k个盒子，允许空盒
  - $x_1+\ldots+x_j=n$ 的正整数解，$x_1\geq\ldots\geq x_j\geq 1$，$j\leq k$

离散概率

离散数学课程组

南京大学计算机科学与技术系

内容提要

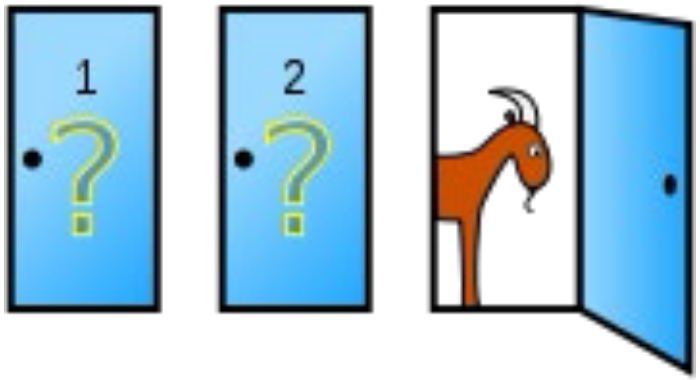
- 概率分析：示例
- 概率分析：基本方法
- 条件概率与贝叶斯定理
- 随机变量及其期望与方差

蒙蒂·霍尔游戏（电视节目, Monty Hall Puzzle）

- 参赛者挑选一个门，主持人打开一扇没有大奖的门
- 保持原来选择，或者，选择剩下的那道门？

概率分析

- 常见问题：两个事件中哪个更有可能发生？
  - 蒙蒂·霍尔游戏



  - 1/3 （总是不变）
  - 2/3 （总是改变）

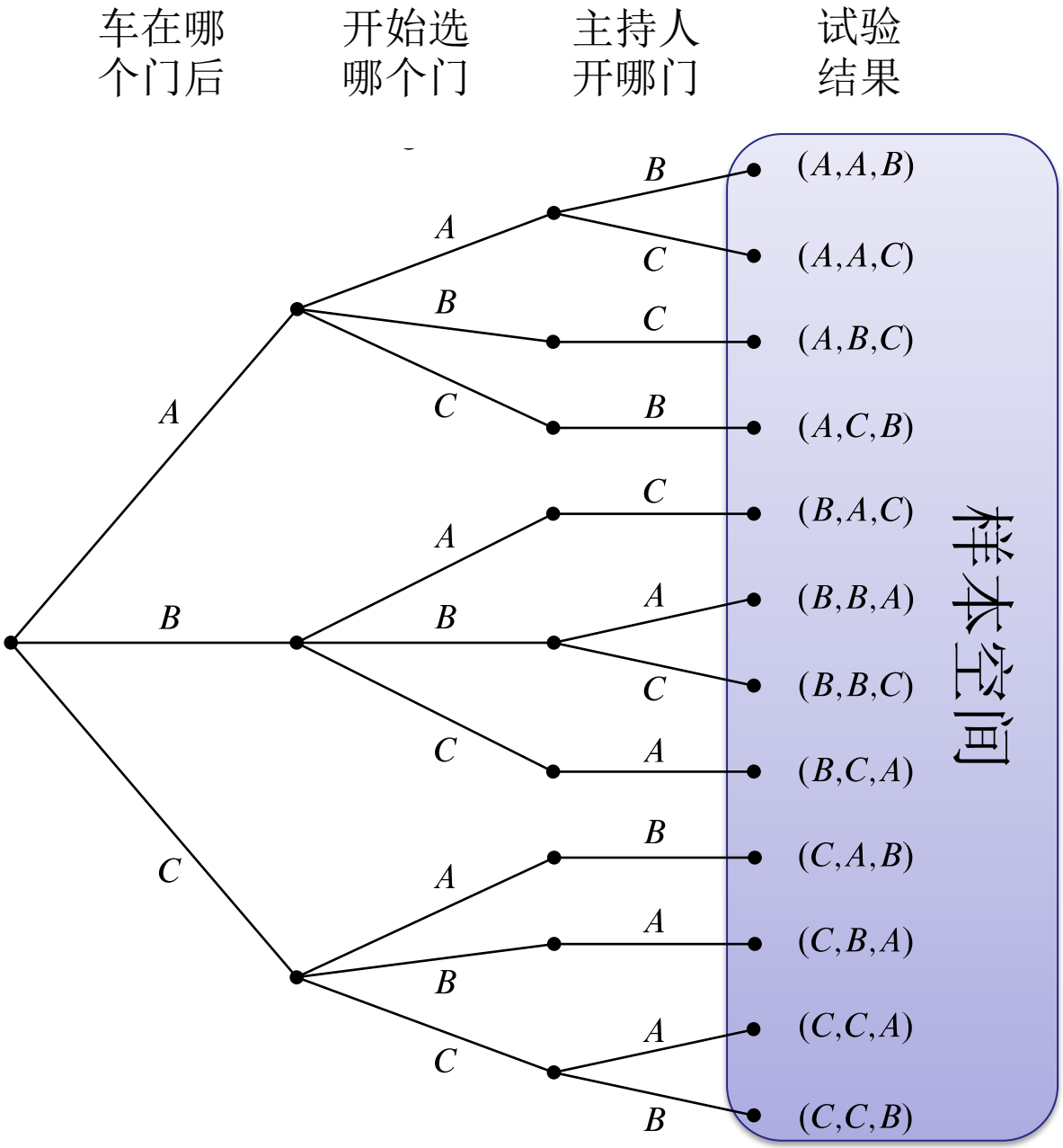
概率分析

- 四步法
  1. 选定样本空间 (Find the sample space)
  2. 定义相关事件 (Define events of interests)
  3. 确定结果概率 (Determine outcome probabilities)
  4. 计算事件概率 (Compute event probabilities)

第一步： 选定样本空间

- **试验**：从一组可能的结果中得出一个结果的过程
  - 试验的某个特定“**结果**”通常是由若干随机因素的某种选择而导致的。这里
    - 因素一：大奖（车）在哪个门后？
    - 因素二：你开始选的哪个门？
    - 因素三：主持人打开哪个门？

- **样本空间**：所有可能结果的集合


车在哪
个门后
开始选
哪个门
主持人
开哪门
试验
结果
A
B
C
A
B
C
A
B
C
A
B
C
A
B
C
A
B
C
B
C
B
C
A
B
C
A
B
C
A
B
(A,A,B)
(A,A,C)
(A,B,C)
(A,C,B)
(B,A,C)
(B,B,A)
(B,B,C)
(B,C,A)
(C,A,B)
(C,B,A)
(C,C,A)
(C,C,B)
样本空间

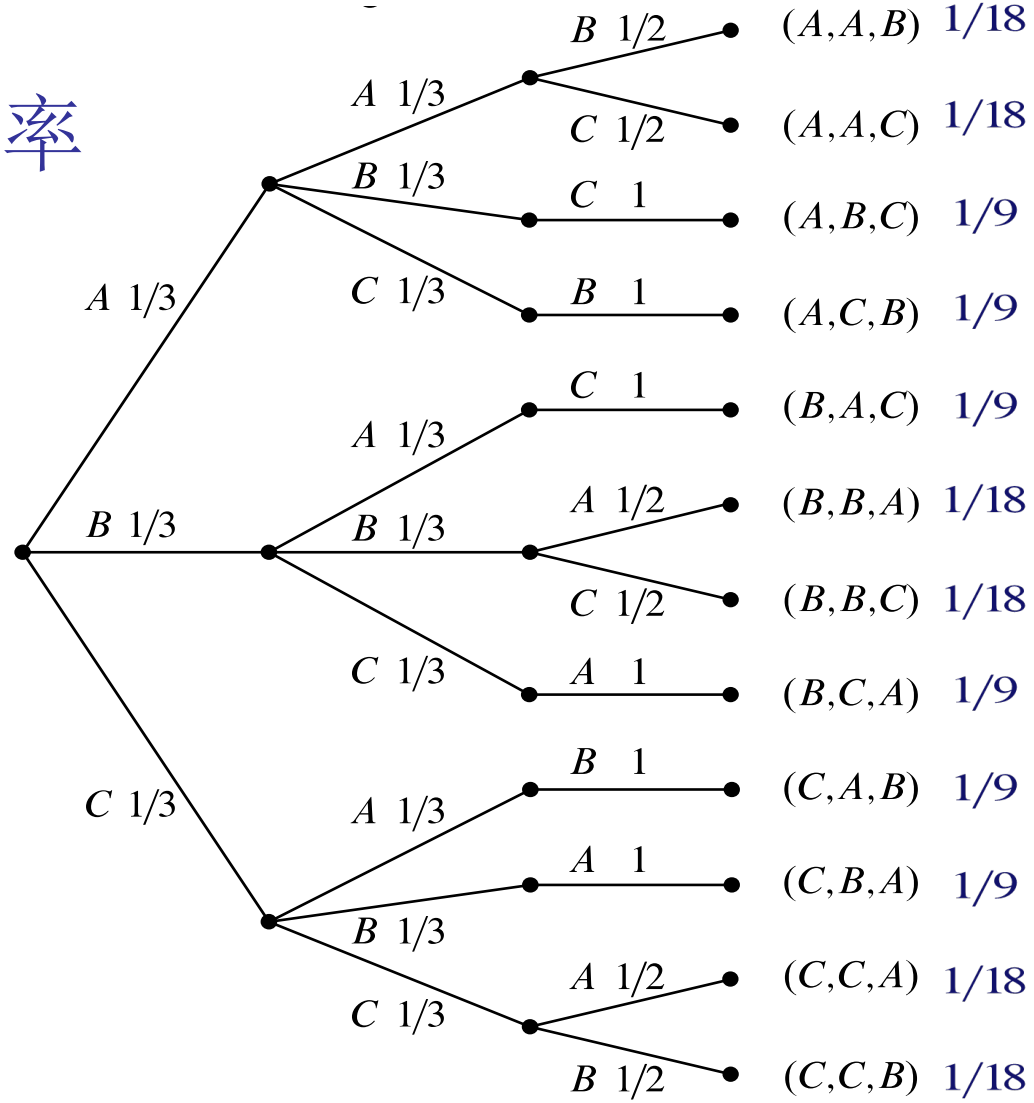
第二步：定义相关事件

- **事件**：样本空间的一个子集
  - 例如：
    - 车在C门后：{(C, A, B), (C, B, A), (C, C, A), (C, C, B) }
    - 第一次就选中有车的门：
      {(A, A, B), (A, A, C), (B, B, A), (B, B, C), (C, C, A), (C, C, B)}
    - 改变选择才赢的情况：
      {(A, B, C), (A, C, B), (B, A, C), (B, C, A), (C, A, B), (C, B, A)}

6对6，似乎换不换都一样？

第三步：确定结果概率

- 给每个边确定概率



- 计算各结果概率

$$\Pr[(A,A,B)] = \frac{1}{3}\cdot\frac{1}{3}\cdot\frac{1}{2} = \frac{1}{18}$$

第四步：计算事件概率

$$\Pr[\text{改变选择而赢}]$$
$$= \Pr[(A,B,C)] + \Pr[(A,C,B)] +$$
$$\Pr[(B,A,C)] + \Pr[(B,C,A)] +$$
$$\Pr[(C,A,B)] + \Pr[(C,B,A)]$$
$$= \frac{1}{9} + \frac{1}{9} + \frac{1}{9} + \frac{1}{9} + \frac{1}{9} + \frac{1}{9}$$
$$= \frac{2}{3}$$

概率空间：基于集合论给概率以数学定义

- 定义：可数**样本空间** S 乃一个可数集合。
  - S 的每一个元素 ω 称为一个**结果**。
- 定义：满足下列条件的函数 $\Pr: S \to \mathbb{R}$ 称为样本空间 S 上的一个**概率函数**：
  - $\forall \omega \in S. \Pr[\omega] \geq 0$，且
  - $\Sigma_{\omega \in S} \Pr[\omega] = 1.$
- 定义：S 的一个子集 $E \subseteq S$ 称为一个**事件**。
  - **事件 E 的概率** $\Pr[E] ::= \sum_{\omega \in E} \Pr[\omega]$

基于集合论的概率计算

- **定理 1**：设 E 是样本空间 S 中的一个事件，事件 $\bar{E}$（事件 E 的**补事件**）的概率为：

$$\Pr[\bar{E}] = 1 - \Pr[E]$$

- **定理 2**：设 E_1 和 E_2 是样本空间 S 中的事件，那么

$$\Pr[E_1 \cup E_2] = \Pr[E_1] + \Pr[E_2] - \Pr[E_1 \cap E_2]$$

基于集合论的概率计算

- 例：从不超过**100**的正整数中随机选一个,它能被**2**或**5**整除的概率?

- 解：设E_1是选出一个被2整除的事件，E_2是选出一个被5 整除的事件。则$E_1 \cap E_2$是选出一个被10整除的事件。

$$\Pr[E_1 \cup E_2] = \Pr[E_1] + \Pr[E_2] - \Pr[E_1 \cap E_2]$$

$$= \frac{50}{100} + \frac{20}{100} - \frac{10}{100} = \frac{3}{5}$$

均匀分布

- 定义：假设S是一个含 n 个元素的样本空间. 均匀分布 (***uniform distribution***) 赋给 S 中每个结果$1/n$ 的概率.
  - 举例：对于均匀的硬币 $\Pr[H] = \Pr[T] = \frac{1}{2}$
  - 举例：公平的骰子 $\Pr[X] = \frac{1}{6}$， $X = 1 \cdots 6$
- 均匀分布下事件的概率可通过对其中的元素计数求得

条件概率

- 定义： 设E和F是事件,且$\Pr[F] > 0$. E在给定F条件下的概率, 记作$\Pr[E \mid F]$, 定义为

$$\Pr[E \mid F] ::= \frac{\Pr[E \cap F]}{\Pr[F]}$$

条件概率

- 例：在至少有一个男孩的条件下,有两个孩子的家庭正好均是男孩的条件概率?假设BB, BG, GB, 和GG是等可能的。

- 解：令E是家庭有两个男孩的事件, F是家庭至少有一 个男孩的事件。我们有$E = \{\text{BB}\}$, $F = \{\text{BB}, \text{BG}, \text{GB}\}$, $E \cap F = \{\text{BB}\}$.
  - $\Pr[F] = \frac{3}{4}$, $\Pr[E \cap F] = \frac{1}{4}$
  - $\Pr[E \mid F] = \frac{\Pr[E \cap F]}{\Pr[F]} = \frac{1}{3}$

贝叶斯定理

- 设 E 和 F 是样本空间 S 中的事件, $\Pr[E] \neq 0, \Pr[F] \neq 0$, 则

$$\Pr[F \mid E] = \frac{\Pr[E|F]\Pr[F]}{\Pr[E]}$$

$$= \frac{\Pr[E|F]\Pr[F]}{\Pr[E|F]\Pr[F]+\Pr[E|\bar{F}]\Pr[\bar{F}]}$$

贝叶斯定理的推导

- 由条件概率定义

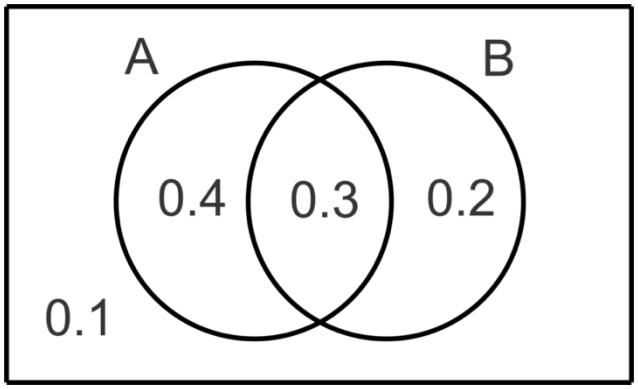
$$\Pr[F \mid E]\Pr[E] = \Pr[F \cap E]$$
$$= \Pr[E \cap \mathrm{F}] = \Pr[E \mid F]\Pr[F]$$

- 又

$$\Pr[E] = \Pr[(E \cap F) \cup (E \cap \bar{F})]$$
$$= \Pr[(E \cap F)] + \Pr[(E \cap \bar{F})]$$
$$= \Pr[E \mid F]\Pr[F] + \Pr[E \mid \bar{F}]\Pr[\bar{F}]$$

贝叶斯定理

- 一些常用说法
  - $\Pr[A]$ 是 A 的**先验概率**。之所以称为“先验”是因为它不考虑任何 B 方面的因素。
  - $\Pr[A \mid B]$ 是已知 B 发生后 A 的条件概率或**后验概率**。
  - $\Pr[B \mid A]$ 是已知 A 发生后 B 的条件概率或**后验概率**。
  - $\Pr[B]$ 是 B 的**先验概率**，也作标准化常量（normalizing constant）。



贝叶斯定理的应用

- 假设有一种罕见的疾病，100,000人只有1人会得这种病。如果某人得了此病，检测准确率高达99%；如果某人没有得此病，检测准确率为99.5%.
  - 疾病检测呈阳性，得此病的概率多大？
  - 疾病检测呈阴性，没有得此病的概率多大？

解：设D是某人得此病的事件，E是疾病检测呈阳性的事件。需要计算 $\Pr[\mathrm{D} \mid E]$, $\Pr[\overline{D} \mid \overline{E}]$ 。

贝叶斯定理的应用（续）

- $\Pr[D] = \frac{1}{100000} = 0.00001,\ \Pr[\bar{D}] = 1 - \Pr[D] = 0.99999$
- $\boldsymbol{Pr[E \mid D]} = \mathbf{0.99},\ \Pr[\bar{E} \mid D] = 0.01,$
  $\Pr[E \mid \bar{D}] = 0.005,\ \boldsymbol{Pr[\bar{E} \mid \bar{D}]} = \mathbf{0.995}$

$$\Pr[D \mid E] = \frac{\Pr[E|D]\Pr[D]}{\Pr[E|D]\Pr[D]+\Pr[E|\bar{D}]\Pr[\bar{D}]}$$

$$= \frac{0.99\times0.00001}{0.99\times0.00001+0.005\times0.99999}$$

$$\approx 0.002$$

为何结果如此小？

呈阳性，也不必太担心！

贝叶斯定理的应用（续）

$$\Pr[\bar{D} \mid \bar{E}] = \frac{\Pr[\bar{E}|\bar{D}]\Pr[\bar{D}]}{\Pr[\bar{E}|\bar{D}]\Pr[\bar{D}]+\Pr[\bar{E}|D]\Pr[D]}$$

$$= \frac{0.995\times 0.99999}{0.995\times 0.99999+0.01\times 0.00001}$$

$$\approx 0.9999999$$

$$\Pr[D \mid \bar{E}] = 1 - \Pr[\bar{D} \mid \bar{E}] = 0.0000001$$

呈阴性，高枕无忧！

事件独立性

- 定义：事件 E 和 F 是相互**独立**的当且仅当

$$\Pr[E \cap F] = \Pr[E] \cdot \Pr[F]$$

例：一个有两个孩子的家庭有四种情形 (BB, GG, BG,GB), 假设是等可能的。事件 E是两个孩子的家庭有两个男孩, 事件 F 是两个孩子的家庭至少有一个男 孩。事件 E 和 F 是否独立?

解：$\Pr[E] = \frac{1}{4}, \Pr[F] = \frac{3}{4}, \Pr[E \cap F] = \frac{1}{4}$

$$\Pr[E] \cdot \Pr[F] = \frac{3}{16} \neq \frac{1}{4} = \Pr[E \cap F]$$

故E 和 F 不是相互独立的。

随机变量

- 一个随机变量 X 是一个定义域为某样本空间 S 的函数 。
  - 其伴域(codomain)可为任意非空集合，但通常取实数集$\mathbb{R}$。即：$X: S \to \mathbb{R}$
  - 一个随机变量是一个函数。它既不是一个变量，也不是随机的。

随机变量（续）

- 举例: 假设一个硬币被掷 3 次. 令 $X(t)$ 是头像在结果 t 中出现的次数。那么随机变量 $X(t)$ 取值如下:
  - $X(HHH) = 3,\ \ X(TTT) = 0,$
  - $X(HHT) = X(HTH) = X(THH) = \ 2,$
  - $X(TTH) = X(THT) = X(HTT) \ = \ 1.$
  - 8 种结果的每一个出现的概率为1/8. 因此, $X(t)$的(概率)分布

$$\Pr[X = 3] = \frac{1}{8},\ \ \Pr[X = 2] = \frac{3}{8},$$

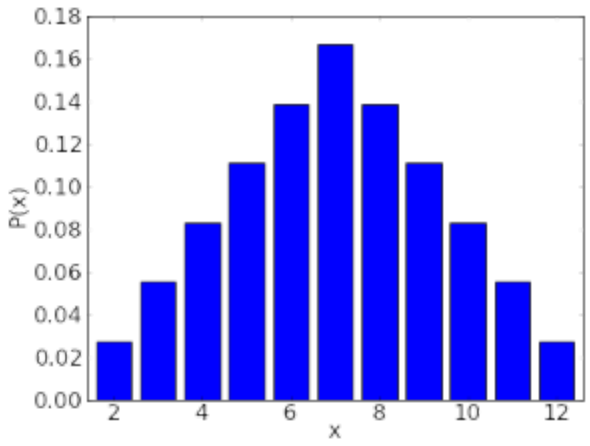
$$\Pr[X = 1] = \frac{3}{8},\ \ \Pr[X = 0] = \frac{1}{8},$$

随机变量的分布

- **定义**: X 是样本空间 S 上的随机变量, X的分布是形如 $(r, \Pr[X = r])$的二元组集合,其中 $r \in X(S)$, $\Pr[X = r]$是 X 取值为 r 的概率。

随机变量分布特征的刻画

- 如何刻画随机变量取值分布的**整体特征**？
  - “平均”取值？
    - 当以概率加权之
  - “离散”程度？
    - 当以平均取值为基准，考虑偏差程度



期望值

- **定义**：对于定义在样本空间 S 上的一个随机变量 X，其**期望值**为
  - 以概率加权的随机变量平均取值

$$\mathrm{Ex}[X] = \sum_{\omega \in S} X(\omega)\Pr[\omega]$$

$X(\omega) - \mathrm{Ex}[X]$ 称为 X 在 ω 处的偏差(deviation)

期望值的直接计算

- 例：求扔一个骰子所得点数的期望值。

$$\mathrm{Ex}[X] = \frac{1}{6}\cdot 1 + \frac{1}{6}\cdot 2 + \frac{1}{6}\cdot 3 + \frac{1}{6}\cdot 4 + \frac{1}{6}\cdot 5 + \frac{1}{6}\cdot 6 = \frac{21}{6} = \frac{7}{2}$$

- 例：扔三个硬币，求头面朝上硬币个数的 期望值。

$$\mathrm{Ex}[X] = \frac{1}{8}[X(HHH) + X(HHT) + X(HTH) + X(HTT) + X(THH) + X(THT) + X(TTH) + X(TTT)]$$

$$= \frac{1}{8}(3 + 2 + 2 + 2 + 1 + 1 + 1 + 0) = \frac{3}{2}$$

例：求扔两个骰子所得点数之和的期望值。

$$\Pr[X=2]=\Pr[X=12]=\frac{1}{36}$$
$$\Pr[X=3]=\Pr[X=11]=\frac{1}{18}$$
$$\Pr[X=4]=\Pr[X=10]=\frac{1}{12}$$
$$\Pr[X=5]=\Pr[X=9]=\frac{1}{9}$$
$$\Pr[X=6]=\Pr[X=8]=\frac{5}{36}$$
$$\Pr[X=7]=\frac{1}{6}$$

$$\begin{aligned}\mathrm{Ex}[X] &= 2\cdot\frac{1}{36}+3\cdot\frac{1}{18}+4\cdot\frac{1}{12}+5\cdot\frac{1}{9}+6\cdot\frac{5}{36}+7\cdot\frac{1}{6}\\ &\quad+8\cdot\frac{5}{36}+9\cdot\frac{1}{9}+10\cdot\frac{1}{12}+11\cdot\frac{1}{18}+12\cdot\frac{1}{36}\\ &= 7.\end{aligned}$$

期望的线性特性

- 定理：对于样本空间 S 上的一组任意的随机变量 X_i，（$i = 1,2,\ldots,n$）和任意实数 a,b，有
  - $\mathrm{Ex}[X_1 + X_2 + \cdots + X_n] = \mathrm{Ex}[X_1] + \mathrm{Ex}[X_2] + \cdots + \mathrm{Ex}[X_n]$
  - $\mathrm{Ex}[aX + b] = a\mathrm{Ex}[X] + b$

  - 由上述定理可知，扔两个骰子所得点数之和的期望值等于第一个骰子点数期望值与第二个骰子点数期望值之和，即 $7/2 + 7/2 = 7$.

例：Expected Value in the Hatcheck Problem

- 负责寄存帽子的服务生把帽子搞乱了，只能随机发还。问他可以期望还对几个？
  - 令$X_i = 1$ 若第 i 个客人拿到他的帽子；否则 $= 0$。

$$X = X_1 + X_2 + \cdots + X_n$$

$$\mathrm{Ex}[X_i] = 1 \cdot \Pr[X_i = 1] + 0 \cdot \Pr[X_i = 0] = \frac{1}{n}$$

$$\mathrm{Ex}[X] = \mathrm{Ex}[X_1] + \mathrm{Ex}[X_2] + \cdots + \mathrm{Ex}[X_n] = n \cdot \frac{1}{\mathrm{n}} = 1$$

独立随机变量

- 样本空间 S 上的随机变量 X 和 Y 若满足 $\Pr[X = r_1 \text{且} Y = r_2] = \Pr[X = r_1] \cdot \Pr[Y = r_2]$，则称它们相互**独立**。
  - 例：扔两个骰子，第一个骰子点数与第二个骰子点数二者是否独立？
  - 例：扔两个骰子，第一个骰子点数与两个骰子点数之和二者是否独立？

- 对于样本空间 S 上**独立的**随机变量 X 和 Y 有 $\mathrm{Ex}[XY] = \mathrm{Ex}[X]\mathrm{Ex}[Y]$

方差

- 样本空间 S 上的随机变量X的方差(variance)

$$\mathrm{Var}[X] ::= \mathrm{Ex}[(X - \mathrm{Ex}[X])^2]$$

$$Var(X) = E(X - E(X)^2)$$

$$\mathrm{Var}[X] = \mathrm{Ex}[(X - \mathrm{Ex}[X])^2] = \sum_{\omega \in S} (X(\omega) - \mathrm{Ex}[X])^2 \Pr[\omega]$$

  - 方差是随机变量X在ω处偏差的平方的加权平均
  - $\sqrt{\mathrm{Var}[X]}$ 称为X的标准差 (standard deviation)
    记为 σ_X (或者$\sigma(X)$)

方差

- **定理：** 样本空间S 上的随机变量X的方差

$$\mathrm{Var}[X] = Ex[X^2] - \mathrm{Ex}^2[X]$$

$$Var(x) = E(X^2) - (E(x))^2$$

- 例：扔一个骰子所得点数的方差

$$\mathrm{Var}[X] = Ex[X^2] - \mathrm{Ex}^2[X]$$

$$= \frac{1}{6}(1^2 + 2^2 + 3^2 + 4^2 + 5^2 + 6^2) - \left(\frac{7}{2}\right)^2$$

$$= \frac{35}{12}$$

Bienaymé's formula（比安内梅公式）

- 对于样本空间 S 上**独立的**随机变量 X 和 Y 有

$$\mathrm{Var}[X+Y]=\mathrm{Var}[X]+\mathrm{Var}[Y]$$

并可推广至 n 个两两相互独立的随机变量

$$\mathrm{Var}[X_1+X_2+\cdots+X_n]$$
$$=\mathrm{Var}[X_1]+\mathrm{Var}[X_2]+\cdots+\mathrm{Var}[X_n]$$

比安内梅公式的应用

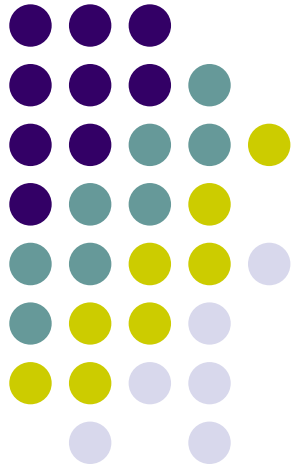
- 例：求扔两个骰子点数之和的方差
  - 第一个骰子点数与第二个骰子点数两个随机变量相互独立；故可使用Bienaymé公式

$$\mathrm{Var}[X_1 + X_2] = \mathrm{Var}[X_1] + \mathrm{Var}[X_2]$$
$$= \frac{35}{12} + \frac{35}{12} = \frac{35}{6}$$

关系及其运算

离散数学—关系

南京大学计算机科学与技术系



关系及其运算

- 关系的定义
- 关系的运算
- 关系的性质
- 0-1矩阵运算

有序对（Ordered pair）

- (a, b)是集合$\{\{a\}, \{a, b\}\}$的简写
- 次序的体现
  - $(x,y)=(u,v)$ iff $x=u$ 且 $y=v$

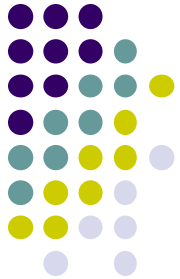
若$\{\{x\},\{x,y\}\}=\{\{u\},\{u,v\}\}$，则$\{x\}=\{u\}$或$\{x\}=\{u,v\}$, 因此$x=u$。

假设$y\neq v$

(1) 若$x=y$, 左边$=\{\{x\}\}$, 而$v\neq x$, ∴右边$\neq\{\{x\}\}$;

(2) 若$x\neq y$,则必有$\{x,y\}=\{u,v\}$, 但y既不是u,又不是v, 矛盾。

笛卡尔乘积（Cartesian Product）



- 对任意集合A, B
  笛卡尔积 $A \times B = \{(a, b) | a \in A, b \in B\}$

- 例：$\{1,2,3\} \times \{a,b\} = \{(1, a), (2, a), (3, a), (1, b), (2, b), (3, b)\}$

- 若A和B都是有限集合，$|A \times B| = |A| \times |B|$

（二元）关系的定义

- 若A, B是集合,从A到B的一个关系是$A \times B$的一个子集.
  - 子集可以是空集
  - 集合的元素是有序对
- 关系意味着什么？
  - 两类对象之间建立起来的联系！

从A到B的二元关系

- 笛卡尔乘积的子集
  - “从A到B的关系”R；$R \subseteq A \times B$
  - 若A=B： 称为“集合A上的（二元）关系”
- 例子
  - 常用的数学关系：不大于、整除、集合包含等
  - 网页链接、文章引用、相互认识

特殊的二元关系

- 集合A上的空关系∅: 空关系即空集
- 全域关系E_A: $E_A = \{ (x, y) \mid x, y \in A \}$
- 恒等关系I_A : $I_A = \{(x, x) \mid x \in A \}$

函数是一种特殊的关系

- 函数 $f:A\to B$
- $R=\{(x, f(x)) \mid x\in A\}$是一个从A到B的一个关系
- 何种关系可以看做一个函数？ 不存在一对多

关系的表示

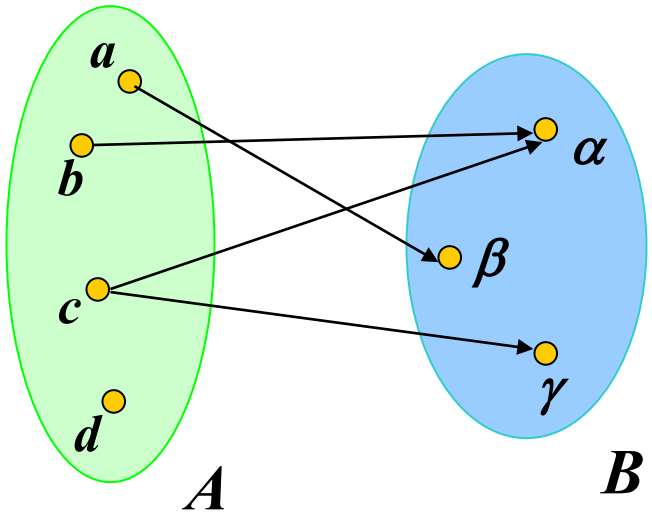
假设A={*a*, *b*, *c*, *d*}, B={α, β, γ} // 假设为有限集合

- 集合表示: $R_1=\{(a, \beta), (b, \alpha), (c, \alpha), (c, \gamma)\}$

0-1矩阵

$$\begin{array}{c} \\ a \\ b \\ c \\ d \end{array}\begin{array}{c} \begin{array}{ccc} \alpha & \beta & \gamma \end{array} \\ \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \end{array}$$

有向图



关系的基本符号

- 定义域和值域等有关记法
  - $\mathbf{dom}R = \{x \mid \exists y\ (x, y) \in R\}$ {1, 2, 3, 5}
  - $\mathbf{ran}R = \{y \mid \exists x\ (x, y) \in R\}$ {2, 3, 4, 5}
  - $\mathbf{Fld}R = \mathbf{dom}R \cup \mathbf{ran}R$ {1, 2, 3, 4, 5}
  - $R \upharpoonright A = \{(x, y) \mid x \in A \wedge xRy\} \subseteq R$ ($x \in A \wedge (x,y) \in R$) {(1,2), (1,4), (2,3), (3,5), (5,2)}.
  - $R[A] = \{y \mid \exists x\ (x \in A \wedge (x,y) \in R)\} = \mathbf{ran}(R \upharpoonright A) \subseteq \mathbf{ran}R$ {2, 3, 4, 5}
- 例： A={1,2,3,4,5}, B={1,3,5}, A上关系R:

  R={(1,2), (1,4), (2,3), (3,5), (5,2)},

  求 $R \upharpoonright$B、R[B]、R(1)和R(2)：与1/2有关的元素

  $R \upharpoonright B = R$　　$R[B] = \{2, 3, 4, 5\}$

关系的逆

- 关系R的逆
  - $R^{-1} = \{(y, x) \mid (x, y) \in R\}$
    - 注意:如果R是从A到B的关系,则R^{-1}是从B到A的。
  - $(R^{-1})^{-1} = R$
  - 例子：$(R_1 \cup R_2)^{-1} = R_1^{-1} \cup R_2^{-1}$
    - $(x, y) \in (R_1 \cup R_2)^{-1} \Leftrightarrow (y, x) \in (R_1 \cup R_2)$
    - $\Leftrightarrow (y, x) \in R_1$ 或 $(y, x) \in R_2$
    - $\Leftrightarrow (x, y) \in R_1^{-1}$ 或 $(x, y) \in R_2^{-1}$

关系的运算

- 关系是集合, 所有的集合运算对关系均适用
  - 例子:
    - 自然数集合上: “<” ∪ “=” 等同于 “≤”
    - 自然数集合上: “≤” ∩ “≥”等同于“=”
    - 自然数集合上: “<” ∩ “>”等同于∅

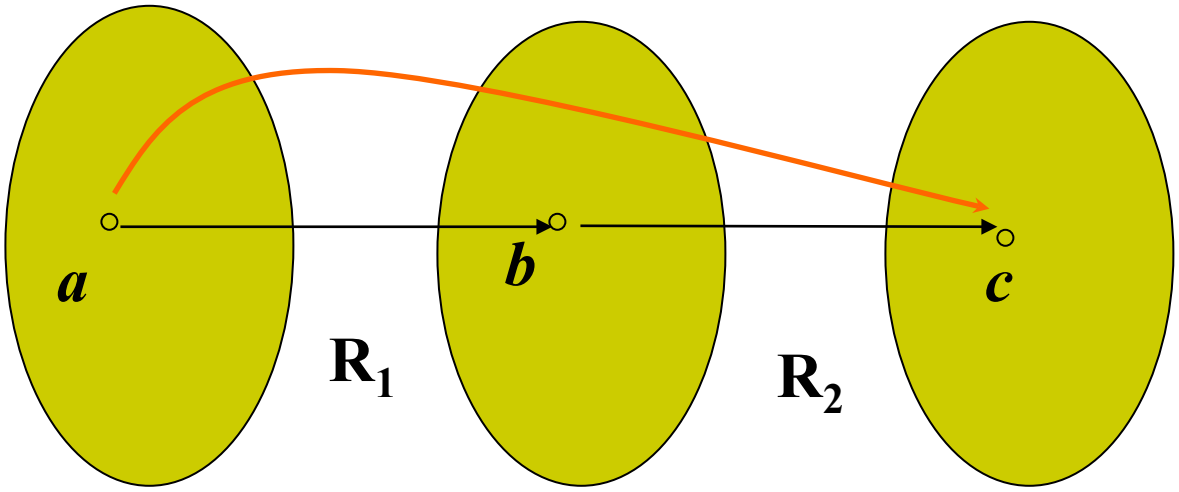
关系的复合（合成）

- 关系的复合（合成）

  设$R_1 \subseteq A \times B$, $R_2 \subseteq B \times C$,

  R_1与 R_2的复合（合成），记为 $R_2 \circ R_1$, 定义如下：

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



关系的复合运算：举例

- 设A={*a*, *b*, *c*, *d*}, R_1, R_2为A上的关系，其中：

  $R_1 = \{ (a, a), (a, b), (b, d)\}$

  $R_2 = \{(a, d), (b, c), (b, d), (c, b)\}$

  则：

  $R_2 \circ R_1 = \{(a, d), (a, c)\}$

  $R_1 \circ R_2 = \{(c, d)\}$

  $R_1^2 = \{(a, a), (a, b), (a, d)\}$

复合运算的性质（1）

- 结合律
  - 给定$R_1 \in A \times B$, $R_2 \in B \times C$, $R_3 \in C \times D$, 则：

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

- 证明左右两个集合相等.

复合运算的性质（2）

- 复合关系的逆关系
  - 给定$R_1 \in A \times B$, $R_2 \in B \times C$, 则：

$$(R_2 \circ R_1)^{-1} = R_1^{-1} \circ R_2^{-1}$$

- 同样，证明左右两个集合相等
  - $(x, y) \in (R_2 \circ R_1)^{-1} \Leftrightarrow (y, x) \in R_2 \circ R_1 \Leftrightarrow$

$$\exists t \in B\ ((y, t) \in R_1 \wedge (t, x) \in R_2) \Leftrightarrow$$

$$\exists t \in B\ ((t, y) \in R_1^{-1} \wedge (x, t) \in R_2^{-1}) \Leftrightarrow$$

$$(x, y) \in R_1^{-1} \circ R_2^{-1}$$

复合运算的性质（3）

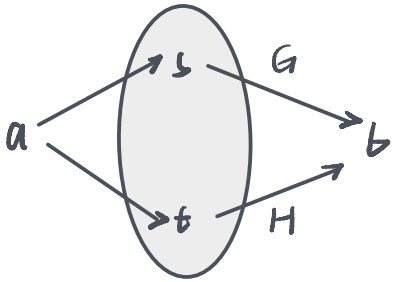
- 对集合并运算满足分配律
  - 给定$F \in A \times B$, $G \in B \times C$, $H \in B \times C$, 则：

    $(G \cup H) \circ F = (G \circ F) \cup (H \circ F)$
- 对集合交运算：$(G \cap H) \circ F \subseteq (G \circ F) \cap (H \circ F)$
  - 注意：等号不成立。

    $A=\{a\}$, $B=\{s, t\}$, $C=\{b\}$;

    $F=\{(a, s), (a, t)\}$, $G=\{(s, b)\}$, $H=\{(t, b)\}$;

    $G \cap H=\varnothing$, $(G \circ F) \cap (H \circ F)=\{(a, b)\}$ 。



关系的性质：自反性

- 集合A上的关系R:
  - 自反：对所有的 $a \in A, (a,a) \in R$
  - 反自反：对所有的$a \in A, (a,a) \notin R$

注意区分"非"与"反"

- 设 $A=\{1,2,3\}$, $R \subseteq A \times A$
  - {(1,1), (1,3), (2,2), (2,1), (3,3)} 是自反的
  - {(1,2), (2,3), (3,1)} 是反自反的
  - {(1,2), (2,2), (2,3),(3,1)} 既不是自反的，也不是反自反的

理解自反性

0-1矩阵的对角线全为1

- R 是 A 上的自反关系 $\Leftrightarrow I_A \subseteq R$,

  这里I_A是集合A上的恒等关系,即:$I_A = \{(a,a) \mid a \in A\}$

  - 直接根据定义证明：
  - $\Rightarrow$ 只需证明：对任意(a, b)，若$(a, b) \in I_A$, 则$(a, b) \in R$
  - $\Leftarrow$ 只需证明：对任意的a, 若$a \in A$, 则$(a, a) \in R$

关系的性质：对称性

- 集合A上的关系R：
  - 对称的：若 $(a,b)\in R$, 则 $(b,a)\in R$ 0-1矩阵主对称 | 转置相等
  - 反对称的：若$(a,b)\in R$ 且$(b,a)\in R$ ， 则$a=b$
- 设 $A=\{1,2,3\}$, $R\subseteq A\times A$
  - {(1,1),(1,2),(1,3),(2,1),(3,1),(3,3)} 是对称的
  - {(1,2),(2,3),(2,2),(3,1)} 是反对称的

理解对称性

- 关系 R满足对称性：对任意a和b，若 $(a,b)\in R$, 则 $(b,a)\in R$

$A^T = A$

- 注意：∅是对称关系。

- 反对称并不是对称的否定：
  - 设$A=\{1,2,3\}$, $R\subseteq A\times A$
  - $\{(1,1),(2,2)\}$ 既是对称的，也是反对称的
  - ∅是对称关系，也是反对称关系。

理解对称性

- R 是集合A上的对称关系 $\Leftrightarrow R^{-1}=R$
  - $\Rightarrow$ 证明一个集合等式 $R^{-1}=R$
    - 若$(a, b)\in R^{-1}$, 则$(b, a)\in R$, 由R的对称性可知$(a, b)\in R$, 因此：$R^{-1}\subseteq R$; 同理可得：$R\subseteq R^{-1}$;
  - $\Leftarrow$ 只需证明：对任意的(a,b)，若$(a, b)\in R$, 则$(b, a)\in R$

关系的性质：传递性

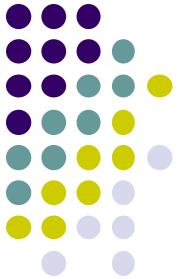
- 集合A上的关系R是传递的，如果下列性质成立：
  - 若 $(a, b)\in R, (b, c)\in R$, 则 $(a, c) \in R$
- 设 $A=\{1,2,3\}$, $R\subseteq A\times A$
  - {(1,1),(1,2),(1,3),(2,1),(2,2),(2,3),(3,3)} 是传递的
  - {(1,2),(2,3),(3,1)} 不是传递的
  - {(1,3)}? 是（→闭性质）
  - ∅? 是

R是传递关系 $\Leftrightarrow \forall a \forall b \forall c(((a, b) \in R \wedge (b, c) \in R) \rightarrow (a, c) \in R)$

理解传递性

- 关系的复合(乘)运算满足结合律，可以用R^n表示$R\circ R\circ\ldots\circ R$ (n是正整数)
- 命题：$(a,b)\in R^n$ 当且仅当：存在$t_1,t_2,\ldots,t_{n-1}\in A$, 满足：$(a,t_1),(t_1,t_2),\ldots,(t_{n-2},t_{n-1}),(t_{n-1},b)\in R$。
  - 对n>=2用数学归纳法：奠基n=2,直接由关系复合的定义可得；归纳基于：$R^n=R^{n-1}\circ R$
- 集合A上的关系R是传递关系 $\Leftrightarrow R^2\subseteq R$
  - 必要性：$\Rightarrow$任取$(a, b)\in R^2$,根据上述命题以及R的传递性可得$(a, b)\in R$
  - 充分性：$\Leftarrow$ 若$(a, b)\in R$, $(b, c)\in R$, 则$(a, c)\in R^2$, 由$R^2\subseteq R$可得$(a, c)\in R$，则 R是传递关系

二元关系和有向图



关系 $R \subseteq A \times B$ ⟷ 有向图 (V_D, E_D)

A和B是集合

有序对集合

$(x, y) \in R$

顶点集 $V_D = A \cup B$

有向边集E_D

从x到y有一条边

0-1矩阵运算

- 令0-1矩阵$M_1=[a_{ij}]$,$M_2=[b_{ij}]$:
  - $C=M_1 \wedge M_2$: $c_{ij}=1$ iff. $a_{ij}=b_{ij}=1$
  - $C=M_1 \vee M_2$: $c_{ij}=1$ iff. $a_{ij}=1$或$b_{ij}=1$
- 令r×s矩阵$M_1=[a_{ij}]$； s×t矩阵$M_2=[b_{ij}]$:
  - $C=M_1 \otimes M_2$: $c_{ij}=1$ iff. $\exists k(a_{ik}=1 \wedge b_{kj}=1)$

布尔积

$c_{ij}>0$,则$c_{ij}=1$

复合关系

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

关系运算的矩阵法（1）

- 命题

$$M_{R_1 \cup R_2} = M_{R_1} \vee M_{R_2}$$

$$M_{R_1 \cap R_2} = M_{R_1} \wedge M_{R_2}$$

$$M_{R_2 \circ R_1} = M_{R_1} \otimes M_{R_2}$$

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

$$M_{R_2 \circ R_1} = M_{R_1} \otimes M_{R_2}$$

- 证明：

令$R_1 : X \to Y; R_2 : Y \to Z;$

令$\mathrm{A} = \mathrm{M}_{\mathrm{R}_1}$， $\mathrm{B} = \mathrm{M}_{\mathrm{R}_2}$， $\mathrm{C} = \mathrm{M}_{\mathrm{R2} \circ \mathrm{R1}}$， $\mathrm{D} = \mathrm{M}_{\mathrm{R}_1} \otimes \mathrm{M}_{\mathrm{R}_2}$有

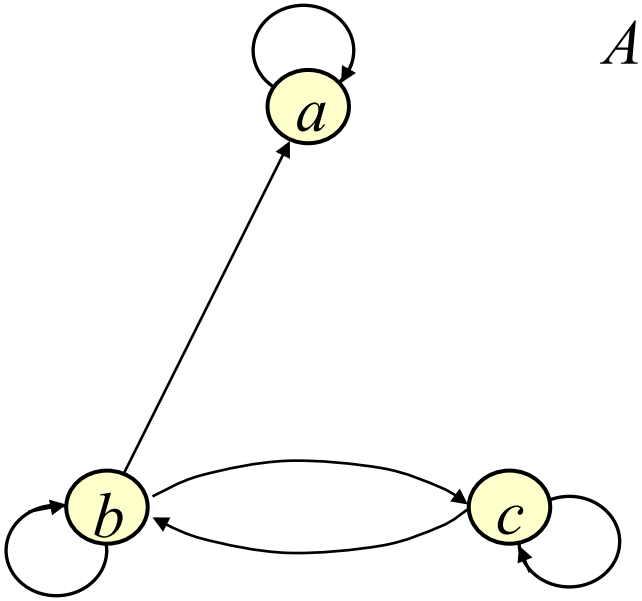
$$c_{ij} = 1 \Leftrightarrow \langle x_i, z_j \rangle \in R_2 \circ R_1 \Leftrightarrow \exists y_k \in Y(\langle x_i, y_k \rangle \in R_1 \wedge \langle y_k, z_j \rangle \in R_2)$$

$$\Leftrightarrow a_{ik} = 1 \wedge b_{kj} = 1 \Leftrightarrow d_{ij} = 1$$

For $n \geq 2$, and R a relation on a finite set A, we have

$$M_{R^n} = M_R \otimes M_R \otimes \cdots \otimes M_R \quad (n \text{ factors})$$

自反关系的有向图和0-1矩阵

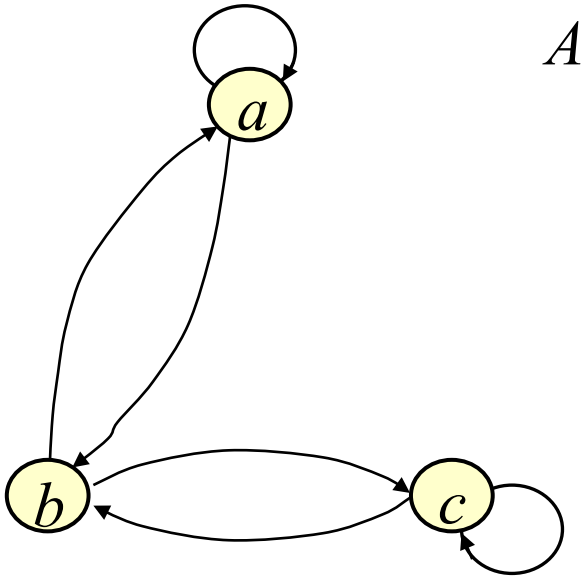


$A=\{a,b,c\}$

对角线全为1

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

对称关系的有向图和0-1矩阵

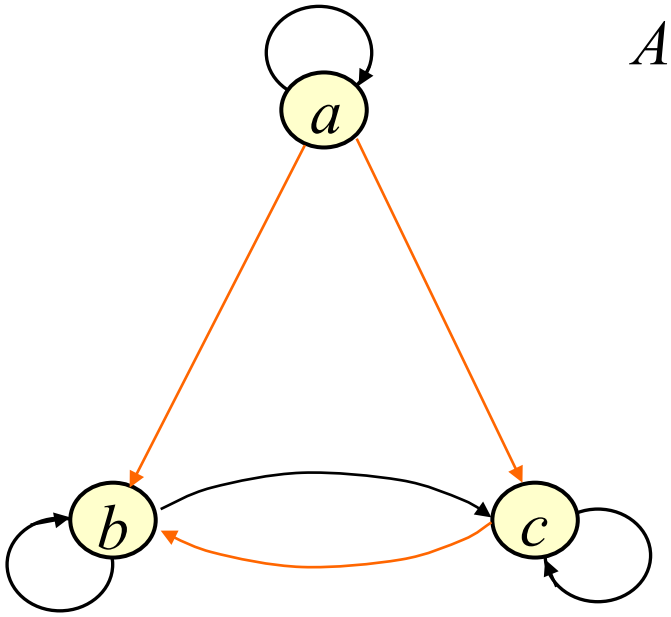


$A=\{a,b,c\}$

实对称

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

传递关系的有向图和0-1矩阵



$A=\{a,b,c\}$

$R^2 = R$

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

一些常用关系的性质

整除　等价　全集

	$=$	$\leq$	$<$	$\mid$	$\equiv_3$	$\varnothing$	E
自反	✓	✓	✗	✓	✓	✗	✓
反自反	✗	✗	✓	✗	✗	✓	✗
对称	✓	✗	✗	✗	✓	✓	✓
反对称	✓	✓	✓	✓	✗	✓	✗
传递	✓	✓	✓	✓	✓	✓	✓

对角阵

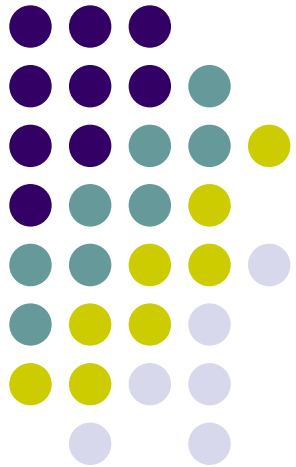
关系运算与性质的保持

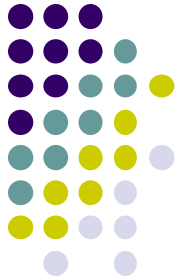
	自反	反自反	对称	反对称	传递
R_1^{-1}	✓	✓	✓	✓	✓
$R_1 \cap R_2$	✓	✓	✓	✓	✓
$R_1 \cup R_2$	✓	✓	✓	✗	✗
$R_2 \circ R_1$	✓	✗	✗	✗	✗

关系的闭包、等价关系

离散数学—关系

南京大学计算机科学与技术系





内容提要

- 闭包的定义
- 闭包的计算公式
- 传递闭包的Warshall算法
- 等价关系
- 等价类
- 划分

关系的闭包：一般概念

- 设R是集合A上的关系，P是给定的某种性质（如：自反、对称、传递），满足下列所有条件的关系R_1称为R的关于P的闭包：
  - $R \subseteq R_1$
  - R_1 满足性质P
  - 对于A上的任意一个关系R'，如果R'包含R且满足性质P，则$R_1 \subseteq R'$
- 自反闭包r(R)、对称闭包s(R)、传递闭包t(R)

自反闭包（reflexive closure）

- 设 R的是集合A上的关系，其自反闭包$r(R)$也是A上的关系，且满足：
  - $r(R)$满足自反性；
  - $R \subseteq r(R)$;
  - 对A上的任意关系R', 若R'包含R且满足自反性，则$r(R) \subseteq R'$

最小的

- 例子
  - 令A={1,2,3}, R={(1,1), (1,3), (2,3), (3,2)}。则$r(R)$={(1,1), (1,3), (2,3), (3,2), (2,2), (3,3)}。

自反闭包的计算公式

- $r(R) = R \cup I_A$, I_A是集合A上的恒等关系

  (证明所给表达式满足自反闭包定义中的三条性质)

  1. 对任意 $x \in A$, $(x,x) \in I_A$, 因此, $(x,x) \in R \cup I_A$

  2. $R \subseteq R \cup I_A$

  3. 设 R' 集合A 上的自反关系，且$R \subseteq R'$.

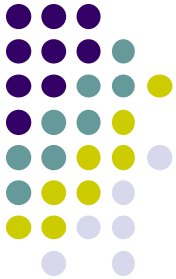
     因为自反性，所以 $I_A \subseteq R'$, 从而 $R \cup I_A \subseteq R'$.

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

$$\| \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$$

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

对称闭包（symmetric closure）



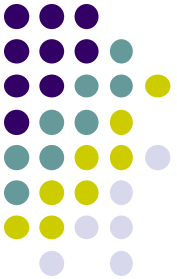
- $s(R) = R \cup R^{-1}$, 这里R^{-1}是R的逆关系
  - $s(R)$是对称的
    - $s(R)^{-1} = (R \cup R^{-1})^{-1} = R^{-1} \cup (R^{-1})^{-1} = R^{-1} \cup R = s(R)$
  - $R \subseteq s(R)$
  - 设R'是集合A上的对称关系, 并且$R \subseteq R'$
    - $R^{-1} \subseteq (R')^{-1} = R'$
    - $R \cup R^{-1} \subseteq R'$
    - 因此, $s(R) \subseteq R'$

连通关系

- 定义集合A上的“连通”关系R^*如下：
  - 对任意$a,b\in A$, $a\ R^*b$ 当且仅当：存在$t_0, t_1 \ldots t_k \in A$($k$是正整数)，满足$t_0=a$, $t_k=b$, $(t_{i-1}, t_i)\in R$, $i=1\ldots k$。(可以表述为：从a到b之间存在长度至少为1的通路)
  - 显然：对任意$a,b\in A$, $a\ R^*\ b$ 当且仅当存在某个正整数k，使得aR^kb。
  - 于是：$R^* = R^1 \cup R^2 \cup R^3 \cup \ldots R^i \cup \ldots = \bigcup_{k=1}^{\infty} R^k$

$$R^* = R^1 \cup R^2 \cup R^3 \cdots \cup R^i \cup \cdots = \bigcup_{k=1}^{\infty} R^k$$

传递闭包（transitive closure）



$t(R) = R^*$

1. 若 $(x,y) \in R^*, (y,z) \in R^*$, 则有 $s_1, s_2, ..., s_j$ 以及 $t_1, t_2, ..., t_k$,

   满足: $(x,s_1), \cdots, (s_j,y), (y,t_1), \cdots, (t_k,z) \in R$,

   因此, $(x,z) \in R^*$.

2. $R \subseteq R^*$

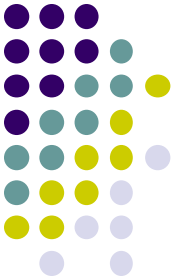
3. 设 R' 是集合 A 上的传递关系, 且包含 R。若 $(x,y) \in R^*$,

   则有 $t_1, t_2, ..., t_k$, 满足: $(x,t_1), \cdots, (t_k,y) \in R$,

   于是 $(x,t_1), (t_1,t_2), \cdots, (t_k,y) \in R'$

   根据 R' 的传递性, $(x,y) \in R'$.

对称闭包的自反闭包vs自反闭包的对称闭包



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

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

$$= (R \cup I_A) \cup (R^{-1} \cup I_A^{-1})$$ (注意：$I_A = I_A^{-1}$, 还有幂等律)

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

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

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

注意：$r(s(R))$一般省略为$rs(R)$

对称关系的传递闭包是对称的

证明：$st(R) \subseteq ts(R)$

$t(R) \subseteq ts(R)$

续证 $st(R) \subseteq ts(R)$

$s(t(R)) \subseteq ts(R)$

注意：左边是$t(R)$的对称闭包，根据定义，我们只需证明：

(1) $ts(R)$满足对称性；(2)$t(R) \subseteq ts(R)$

证明(1)：对任意$(x, y) \in ts(R)$，$\exists t_1, t_2, \ldots, t_k$，满足

$(x, t_1) \in s(R), (t_1, t_2) \in s(R), \ldots, (t_k, y) \in s(R)$，而$s(R)$满足对称性，$\therefore (y, t_k) \in s(R), \ldots, (t_2, t_1) \in s(R), (t_1, x) \in s(R)$，于是：$(y, x) \in ts(R)$，$\therefore ts(R)$满足对称性。

证明(2)，考虑到左边是R的传递闭包，我们只需要证明：

(i) $R \subseteq ts(R)$ (显然)，(ii) $ts(R)$满足传递性(显然)。

注意：传递关系的对称闭包不一定是传递的。比如：{(1,3)}

有限集合上的传递闭包

假如$|A|=n$, 则A上的关系R的传递闭包是：

$$t(R)=\bigcup_{i=1}^{n} R^i = R \cup R^2 \cup \cdots \cup R^n$$

上述公式和：$t(R)=R^*=\bigcup_{i=1}^{\infty} R^i$有何差别？有限与无限.

A **中只有** ***n*** **个不同的元素，如果在*R*中存在一条从*a*到*b*的长度至少为1的通路，那么存在一条长度不超过*n*的从*a*到*b*的通路。**

若 xR^*y, 则存在某个自然数 k, $1\le k\le n$, 满足 xR^ky.

用矩阵乘法计算传递闭包

有限集合上关系的传递闭包：$t(R)=\bigcup_{i=1}^{n} R^i = R \cup R^2 \cup \cdots \cup R^n$

$$\therefore M_{t(R)} = M_R \vee M_R^2 \vee M_R^3 \vee \ldots \vee M_R^n$$

算法概要：

1. 输入M_R;
2. 计数器 k 置初值n-1;
3. $M_{TR} \leftarrow M_R$; $M' \leftarrow M_R$;
4. $M' \leftarrow M' \otimes M_R$;
5. $M_{TR} \leftarrow M_{TR} \vee M'$;
6. $k \leftarrow k-1$; 若k>0则转4;
7. 输出M_{TR};

n×n矩阵相乘，结果中每1项，要做(2n-1次)布尔运算(积与和)，总共需要计算n^2项。

n×n矩阵相加,要做n^2次布尔运算(和)

本算法共进行n-1次矩阵乘和加。

总运算量$(n^2(2n-1)+n^2)(n-1)=2n^3(n-1)$

Warshall算法原理

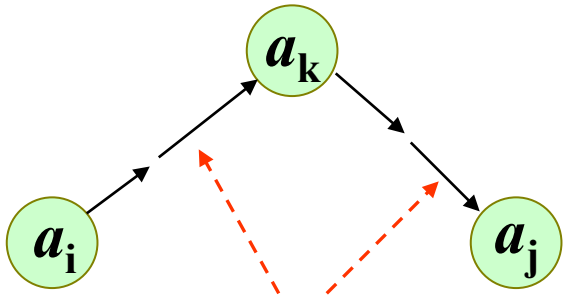
不直接计算 M_R的乘幂, Warshall算法迭代式地用W_{i-1} 计算W_i

这里： 1. W_0 即为R的关系矩阵, M_R。

2. 对$k=1,2,\cdots,n, W_k[i,j]=1$ 当且仅当 从a_i到a_j

存在中间节点均在集合 $\{a_1,a_2,\cdots,a_k\}$内的通路。

3. W_n 即 $M_{t(R)}$, 也就是所需的结果。



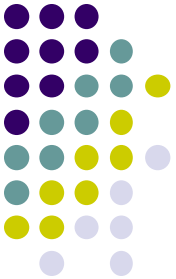
all interior vertices in $\{a_1,..., a_{k-1}\}$

$W_k[i,j]=1$ iff

$W_{k-1}[i,j]=1$, or

$W_{k-1}[i,k]=1$ and $W_{k-1}[k,j]=1$

Warshall算法过程



- ALGORITHM *WARSHALL* (M_R : n×n的0-1矩阵）
- 1. W := M_R
- 2. FOR *k* :=1 to *n*
- FOR *i* :=1 to *n*
- FOR *j* :=1 to *n*
- $W[i,j] \leftarrow W[i,j] \vee (W[i,k] \wedge W[k,j])$
- 3. Output W
- END OF ALGORITHM WARSHALL

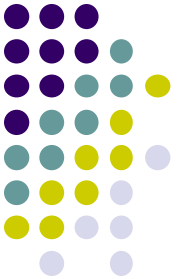
这个语句在三重循环内，执行n^3次，每次执行2个布尔运算（和与积）

总运算量: $2n^3$

内容提要

- 闭包的定义
- 闭包的计算公式
- 传递闭包的Warshall算法
- 等价关系
- 等价类
- 划分

等价关系的定义



- 满足性质：自反、对称、传递。
- “等于”关系的推广
- 例子
  - 对3同余关系: $R \subseteq Z \times Z$， xRy 当且仅当 $\frac{|x-y|}{3}$ 是整数。
  - $R \subseteq N \times N$， xRy iff 存在正整数k,l，使得$x^k=y^l$。
    - 自反: 若x是任意自然数，当然$x^k=x^k$；
    - 对称：若有k,l, 使$x^k=y^l$；也就有l,k, 使$y^l=x^k$；
    - 传递：若有k,l, 使$x^k=y^l$；并有m, n, 使$y^n=z^m$；则有 $x^{kn}=z^{ml}$

等价类

- R是集合A上的等价关系，

  $\forall x \in A$，等价类$[x]_R = \{y \mid xRy\}$

- 每个等价类是A的一个非空子集

- 举例，对3同余是整数集合上的一个等价关系

  - 3 个等价类：　[0]={…, -6, -3, 0, 3, 6, 9, …};

    [1]={…, -5, -2, 1, 4, 7, …};

    [2]={…, -4, -1, 2, 5, 8, 11, …}

等价类的代表元素

- 对于等价类$[x]_R=\{ y \mid y\in A \wedge xRy \}$，$x$称为这个等价类的代表元素.
- 事实上，该等价类的每个元素都可以做代表元素：若xRy，则$[x]=[y]$
  - 证明：对任意元素t, 若$t\in[x]$, 则xRt, 又 xRy，根据R的对称性与传递性，可得yRt，因此，$t\in[y]$, 所以$[x]\subseteq[y]$；同理可得$[y]\subseteq[x]$。

商集

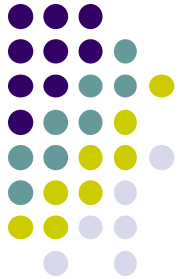
- ***R*是非空集合A上的等价关系，其所有等价类的集合称为*商集*，A/R**
- 集合$A=\{a_1,a_2, \ldots, a_n\}$上的恒等关系$I_A$是等价关系，商集$A/I_A=\{\{a_1\},\{a_2\},\ldots,\{a_n\}\}$
- 定义自然数集的笛卡儿乘积上的关系*R*:

  $(a, b)R(c,d)$ 当且仅当 $a+d=b+c$

  证明这是等价关系，并给出其商集.

a+d=b+c
c+f=d+e.
a+f=b+e.
(a,b)R(c,d)
(c,d)R(e,f)
⇒ (a,b)R(e,f). 传递
*. (a,b)R(a,b). a+b=b+a. 自反.
(a,b)R(c,d) (c,d)R(a,b). 对称

等价关系的一个例子

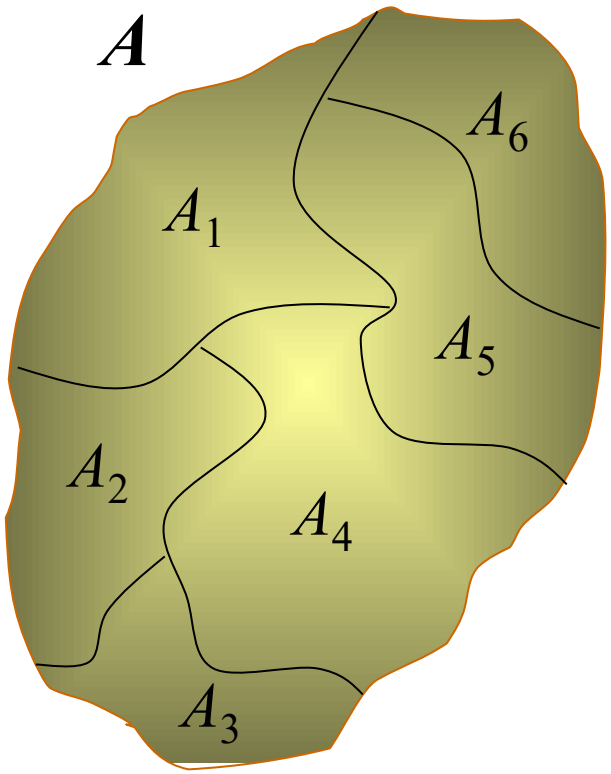


- R_1,R_2分别是集合X_1,X_2上的等价关系。定义$X_1\times X_2$上的关系S：

  $(x_1,x_2)S\,(y_1,y_2)$ 当且仅当 $x_1R_1y_1$ 且 $x_2R_2y_2$

- 证明：S是$X_1\times X_2$上的等价关系
  - [自反性] 对任意$(x,y)\in X_1\times X_2$, 由R_1,R_2满足自反性可知，$(x,x)\in R_1$, $(y,y)\in R_2$; $\therefore (x,y)S(x,y)$; S自反。
  - [对称性] 假设$(x_1,x_2)S\,(y_1,y_2)$, 由S的定义以及R_1,R_2满足对称性可知: $(y_1,y_2)S\,(x_1,x_2)$; $\therefore$ S对称。
  - [传递性] 假设$(x_1,x_2)S\,(y_1,y_2)$, 且$(y_1,y_2)S\,(z_1,z_2)$, 则$x_1R_1y_1$, $y_1R_1z_1$, $x_2R_2y_2$, $y_2R_2z_2$, 由R_1,R_2满足传递性可知：$x_1R_1z_1$, 且$x_2R_2z_2$, 于是：$(x_1,x_2)S\,(z_1,z_2)$; $\therefore$ S传递。

集合的划分



集合A的 划分, π, 是A的一组非空子集的集合，即 $\pi \subseteq \rho(A)$, 且满足：

1. 对任意 $x \in A$, 存在某个 $A_i \in \pi$, 使得 $x \in A_i$.

$$\text{i.e. } \bigcup_i A_i = A$$

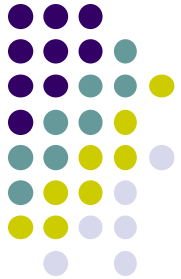
2. 对任意 $A_i, A_j \in \pi$, 如果 i≠j, 则：

$$A_i \cap A_j = \phi$$

由等价关系定义的划分

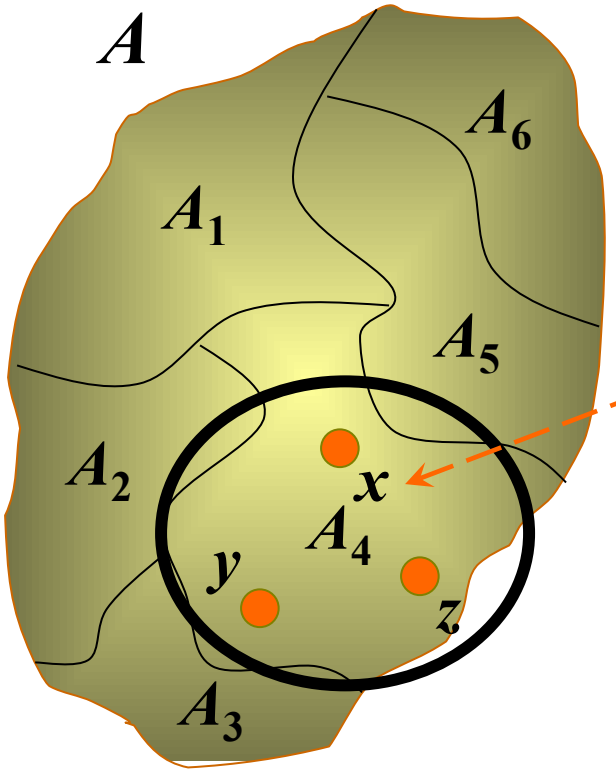
- 假设R是集合A上的等价关系，给定$a \in A$, $R(a)$是由R 所诱导的等价类。
- $Q=\{R(x)|x \in A\}$是相应的商集。
- 容易证明，这样的商集即是A的一个划分：
  - 对任意 $a \in A$, $a \in R(a)$ (R 是自反的)
  - 对任意 $a,b \in A$
    - $(a,b) \in R$ 当且仅当 $R(a)=R(b)$, 同时
    - $(a,b) \notin R$ 当且仅当 $R(a) \cap R(b)=\varnothing$

商集即划分– 证明



- 不相等的等价类必然不相交。换句话说，有公共元素的任意两个等价类必然相等。
- 证明：
  - 假设$R(a)\cap R(b)\neq\varnothing$, 设$c$是一个公共元素。
  - 根据等价类的定义，$(a,c)\in R$, $(b,c)\in R$
  - 对任意$x\in R(a)$, $(a, x)\in R$, 由R的传递性和对称性，可得$(c,x)\in R$, 由此可知$(b, x)\in R$, 即$x\in R(b)$, $\therefore R(a)\subseteq R(b)$
  - 同理可得：$R(b)\subseteq R(a)$。因此，$R(a)=R(b)$。

根据一个划分定义等价关系



给定 A 上一个划分，可以如下定义A 上的等价关系 R：

$\forall x,y \in A, (x,y) \in R$ 当且仅当：

x,y 属于该划分中的同一块。

显然，关系 R 满足自反性、对称性、传递性。因此，R 是等价关系。

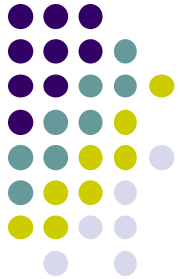
利用等价类解题

- 下列结论是否成立：

  从1,2,...,2000中任取1001个数，其中必有两个数 x, y，满足$x/y=2^k$。 (k为整数)

想起鸽笼原理没？

等价关系与划分：示例的解

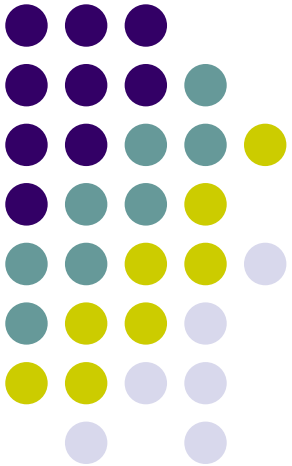


- 建立1000个集合，每个集合包括1至2000之间的一个奇数以及该奇数与2的k次幂的乘积，但最大不超过2000。可以证明这1000个集合的集合是集合{1,2,3,...，2000}上的一个划分。
- 定义集合{1,2,3,...，2000}上的一个关系R，任意x,y ，xRy当且仅当$x/y=2^k$。易证这是一个等价关系。其商集即上面的划分。

偏序集与格

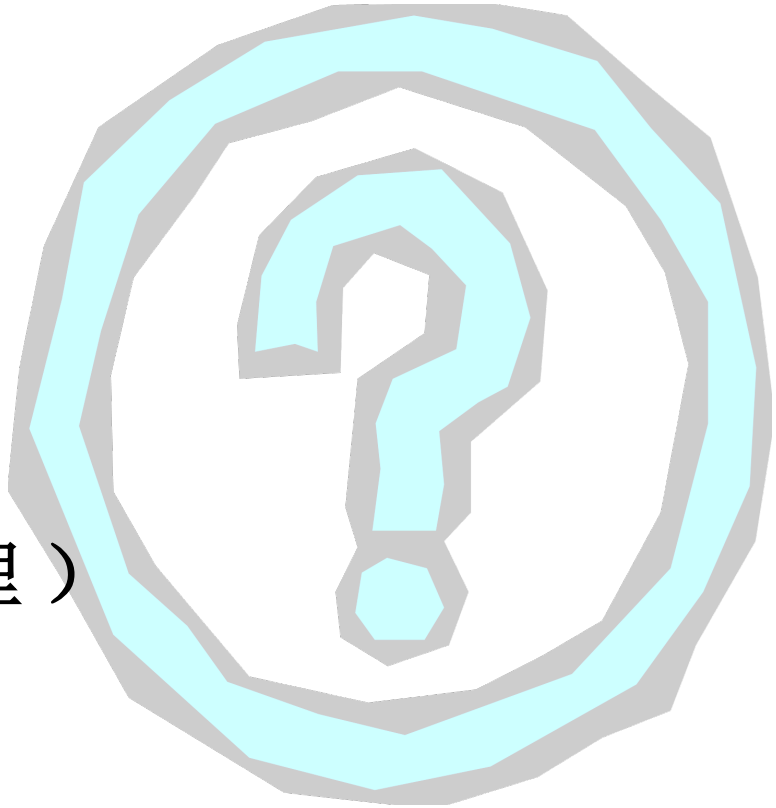
离散数学—关系

南京大学计算机科学与技术系



内容提要

- 偏序与全序
- 哈斯图
- 极大 (小)元、最大(小)元
- 上(下)界、上(下)确界
- 良序
- 链与反链（ Dilworth定理 ）
- 格及其性质



偏序关系的定义(Partial Order)

等价关系：自反、对称、传递

- 偏序关系：集合上的自反的、反对称的、传递的关系
  - 通常记作 $\preccurlyeq$

e.g. 实数上的 $\leq$ 关系、$\geq$ 关系

- 定义了偏序关系的集合称为偏序集，记作$(A, \preccurlyeq)$
- 举例
  - 集合包含关系 $(2^A, \subseteq)$, 其中A是集合
  - $(Z^+, |)$，Z^+是正整数集，“$|$”是整除关系
- 既是偏序又是等价的关系
  - 非空集合A上的恒等关系I_A

“字典顺序”

- 设$\preccurlyeq$是非空集合A上的偏序关系，定义A×A上的关系R如下：

$$(x_1, y_1)\ R\ (x_2, y_2) \quad iff.$$

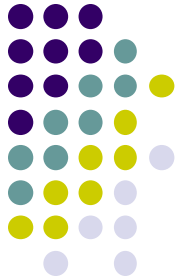
$$x_1 \neq x_2 \text{且} x_1 \preccurlyeq x_2, \text{或者} x_1 = x_2 \text{且} y_1 \preccurlyeq y_2$$

  - 易证R是A×A上的偏序关系

- 给定有限字符集合Σ，若在Σ上有一个偏序关系，类似上述办法，可以对任意正整数k,定义Σ^k(由Σ中字符构成的长度为k的串的集合)上的偏序关系。加以适当的技术处理，则容易定义Σ^+(由Σ中字符构成的长度为任意正整数的串的集合)上的偏序关系：字典关系

  - 注意：在通常的字典关系中，任何两个元素均可比。

全序：一种特殊的偏序关系

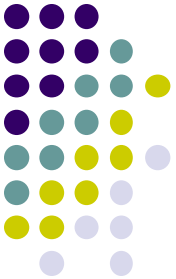


- 如果对$a, b \in A$，$a \preccurlyeq b$和$b \preccurlyeq a$中有一个成立，则a,b可比。

- 设R是A上的偏序关系，如果A中的任意两个元素都是可比的，则称R是A上的全序关系（或线序关系）

- 举例（全序）
  - 实数集上的“不大于” 关系≤、基于拉丁字母表的字典顺序

偏序集上的“小于”关系及覆盖



- 设$(A, \preccurlyeq)$是偏序集
- A上的“小于”关系$\prec$定义如下：

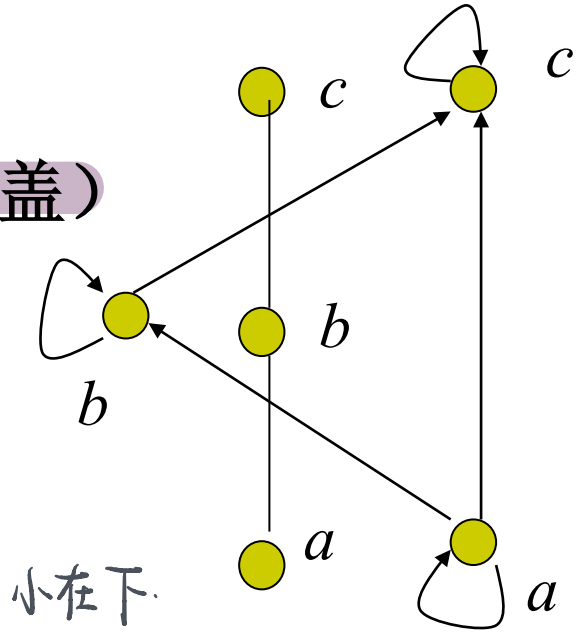
$$x \prec y \text{ iff } x \preccurlyeq y \wedge x \neq y$$

- 元素y覆盖x定义如下：

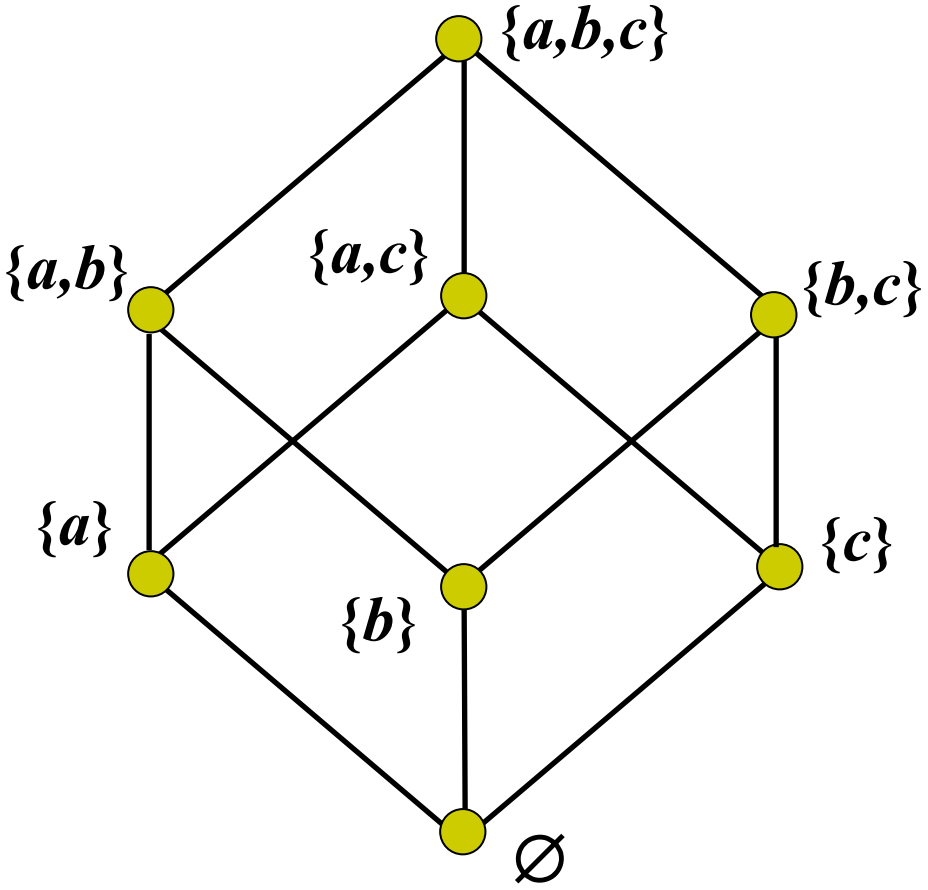
$x \prec y$，且不存在$z \in A$使得$x \prec z \prec y$

哈斯图

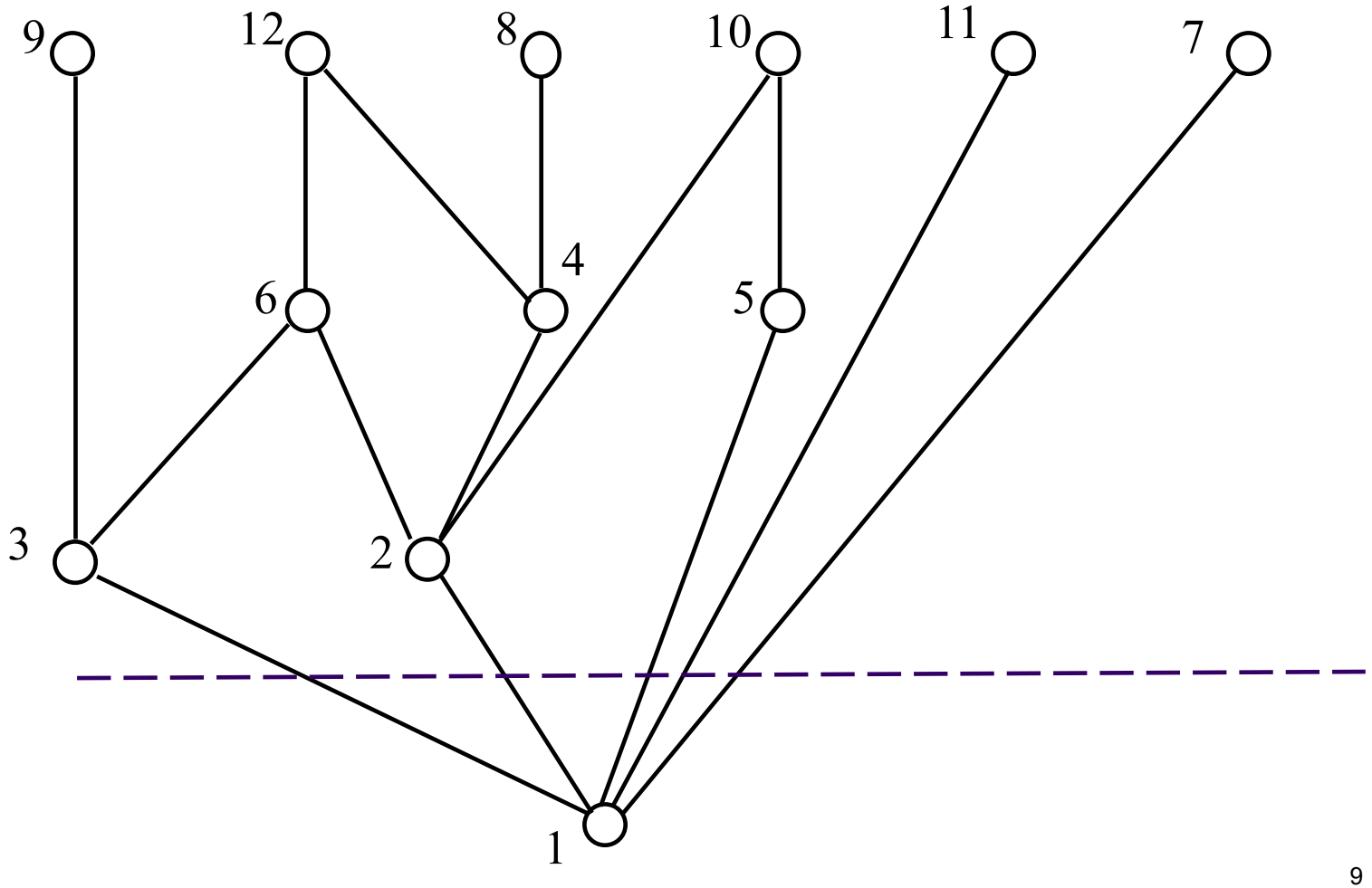
- 一般的关系图可以表示偏序关系
- **哈斯图(Hasse)：** 利用特定性质简化图示方法
  - 利用自反性省略圈
  - 利用反对称性省略箭头
  - 利用传递性省略部分连线（覆盖）



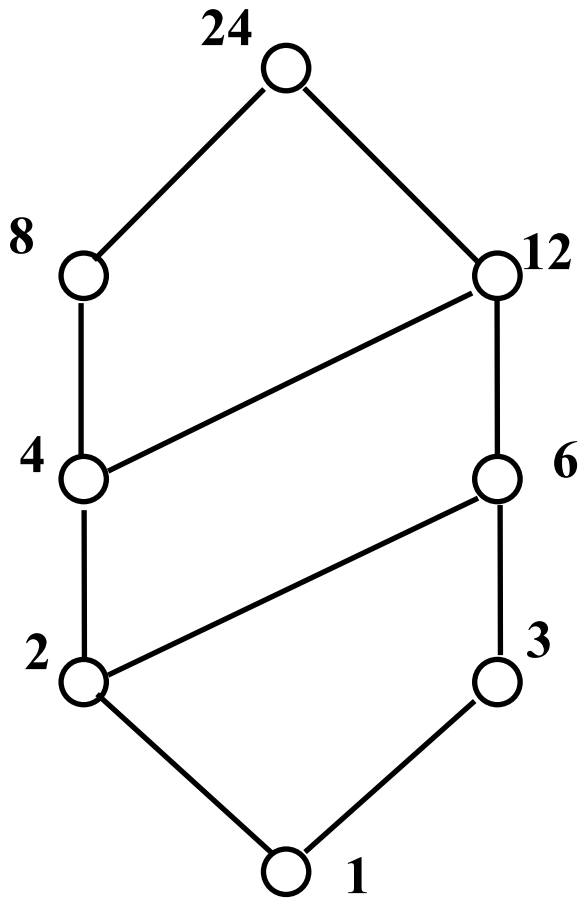
ρ({*a*, *b*, *c*})上的包含关系



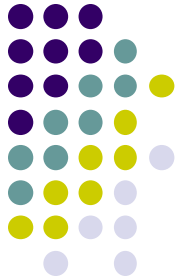
{1,2,...,12}上的整除关系



{1,2,3,4,6,8,12,24}上的整除关系



偏序集中的特殊元素： 极大(小)



- x是偏序集$(A,\preccurlyeq)$中的极大元 iff.
  - 对任意$y \in A$,若$x \preccurlyeq y$, 则$x=y$

没有比它更大（小）的了！

- x是偏序集$(A,\preccurlyeq)$中的极小元 iff.
  - 对任意$y \in A$,若$y \preccurlyeq x$, 则$x=y$

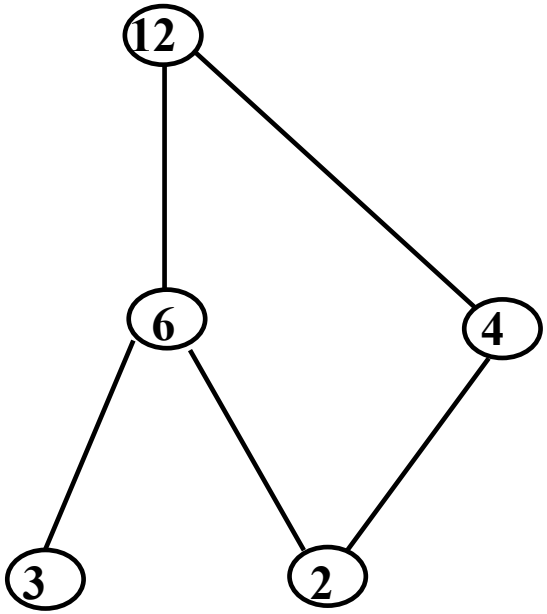
- 有关极大元与极小元的讨论
  - 不一定存在，但是，有穷集合一定有极大(小)元
  - 不一定唯一
  - 一个元素可能兼为极大(小)元

偏序集中的特殊元素： 最大(小)

- x是偏序集$(A,\preccurlyeq)$中的最大元 *iff*.
  - 对任意$y \in A$, $y \preccurlyeq x$

它比谁都要大（小）!

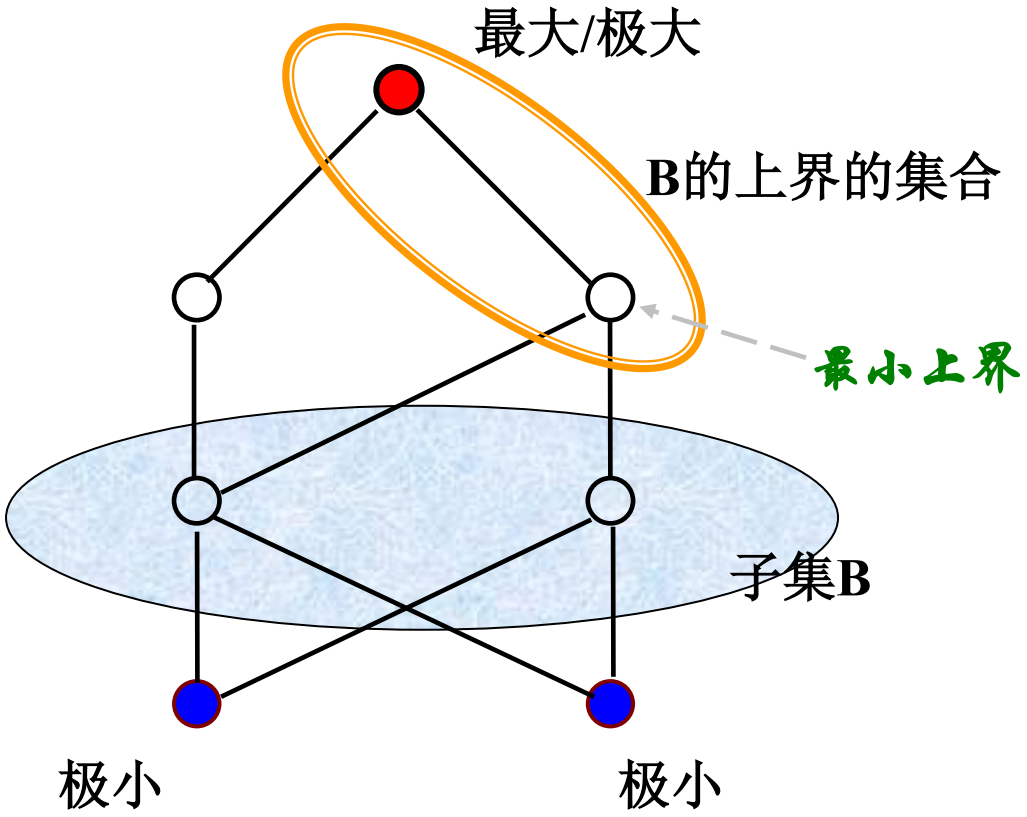
- x是偏序集$(A,\preccurlyeq)$中的最小元 *iff*.
  - 对任意$y \in A$, $x \preccurlyeq y$
- 有关最大元与最小元的讨论
  - 可能不存在
  - 若存在，必唯一。



偏序集中的特殊元素 ：上(下)确界

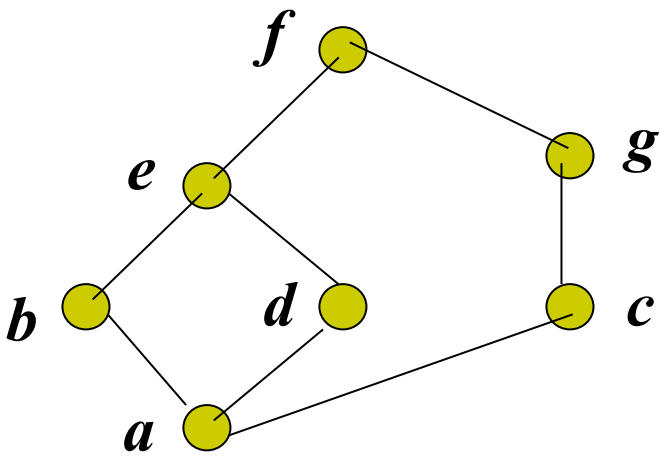
- 上界：对于偏序集$(A,\preccurlyeq)$和A的子集B，若存在$y\in A$，对B中任意元素x, 均有$x\preccurlyeq y$,则y是B的上界。
- 最小上界：如果B的上界构成的偏序集有最小元，则该最小元为B的最小上界（lub），上确界。
- 类似地可以定义下界、最大下界（glb），下确界。
- 有关上(下)界的讨论
  - 不一定存在；
  - 最小上界若存在，则必唯一。

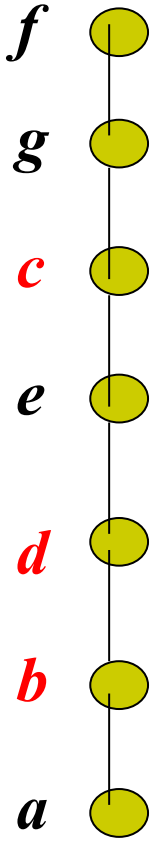
从哈斯图看特殊元素

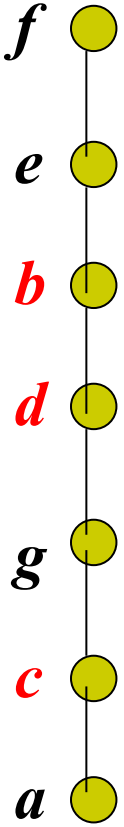


拓扑排序（Topological sorting）

有向无环图上构造一种线性序





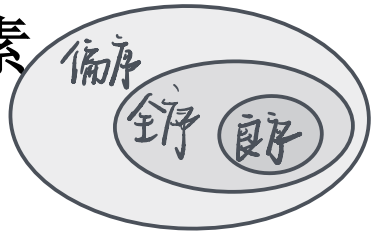


良序

- 定义：给定集合A上的偏序$\preccurlyeq$，若A的任一非空子集均存在最小元素，则该偏序为良序。
- 良序必为全序
  - 对任意$a,b\in A$, $\{a,b\}$必有最小元，则a,b一定可比
- 实际上，“反对称性 + 任一非空子集存在最小元”就能够保证全序性质（偏序性质+任何两个元素均可比）。
  - 自反性：对任意$a\in A$, $\{a\}$也必有最小元，即$a\preccurlyeq a$
  - 传递性：假设$a\preccurlyeq b$, $b\preccurlyeq c$, $\{a, b, c\}$的最小元素只能是a, 因此$a\preccurlyeq c$
  - 任何两个元素可比，上面已证明。

关于次序关系的进一步讨论

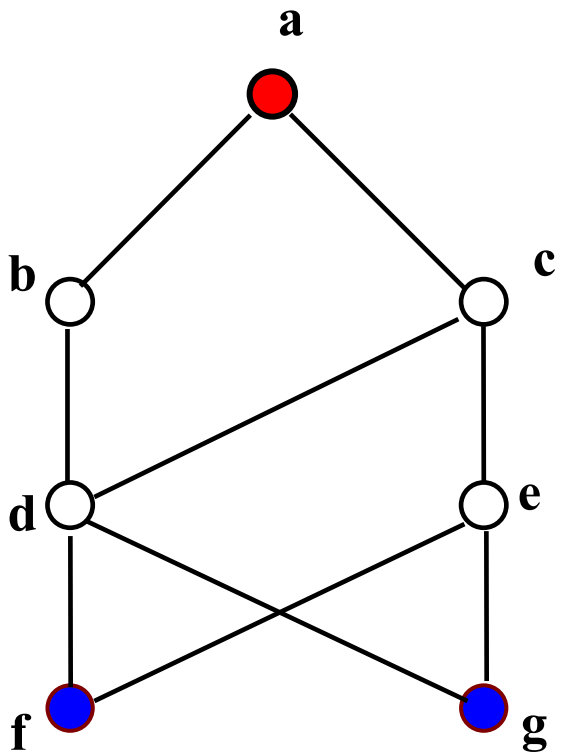
- 注意：良序结构上可以实施数学归纳法
- 全序是否一定是良序？
- 当A是无穷集合时，全序不一定是良序
  - 例如： $(\mathbf{R}, \leq)$, 任何开区间上没有最小元素
- 良序 →全序 →偏序
- 偏序/全序/良序的逆关系是否仍为偏序/全序/良序？
- 良序的逆关系不一定是良序
  - 例如$(\mathbf{N}, \leq)$



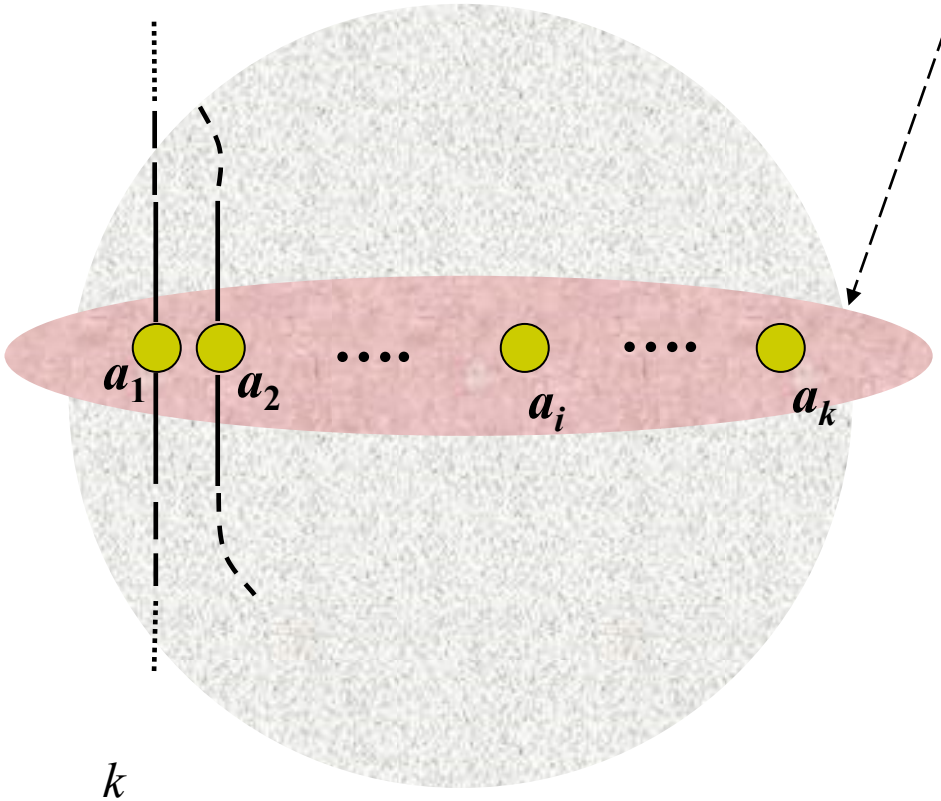
链与反链

- 链与反链
  - 设C是偏序集$(P,\preccurlyeq)$的一个子集
  - 如果C中任何两个元素均可比，则C构成一个链
  - 如果C中任何两个元素均不可比，则B构成一个反链

链与反链（示例）

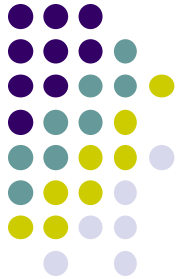


元素个数最多的反链，含k个元素



$$\bigcup_{i=1}^{k} C_i = P(C_i\text{互不相交})$$

Dilworth定理



- 链覆盖 是(P,≤)中一组互不相交的链, 它们一起包含了P中的所有元素.
- **Dilworth 定理 (1950)**

  在任意有限偏序集(P,≤)中, 覆盖P的最小链数等于P中最长反链的长度（元素个数）.
- 注：覆盖P的链数 ≥ P中任一反链的元素个数.

  等价结论:有限偏序集中存在一个链覆盖和一个反链，它们大小相等

Dilworth定理的归纳证明

- 证明. 按照P中元素个数（|P|=1, 2 …）进行归纳证明.

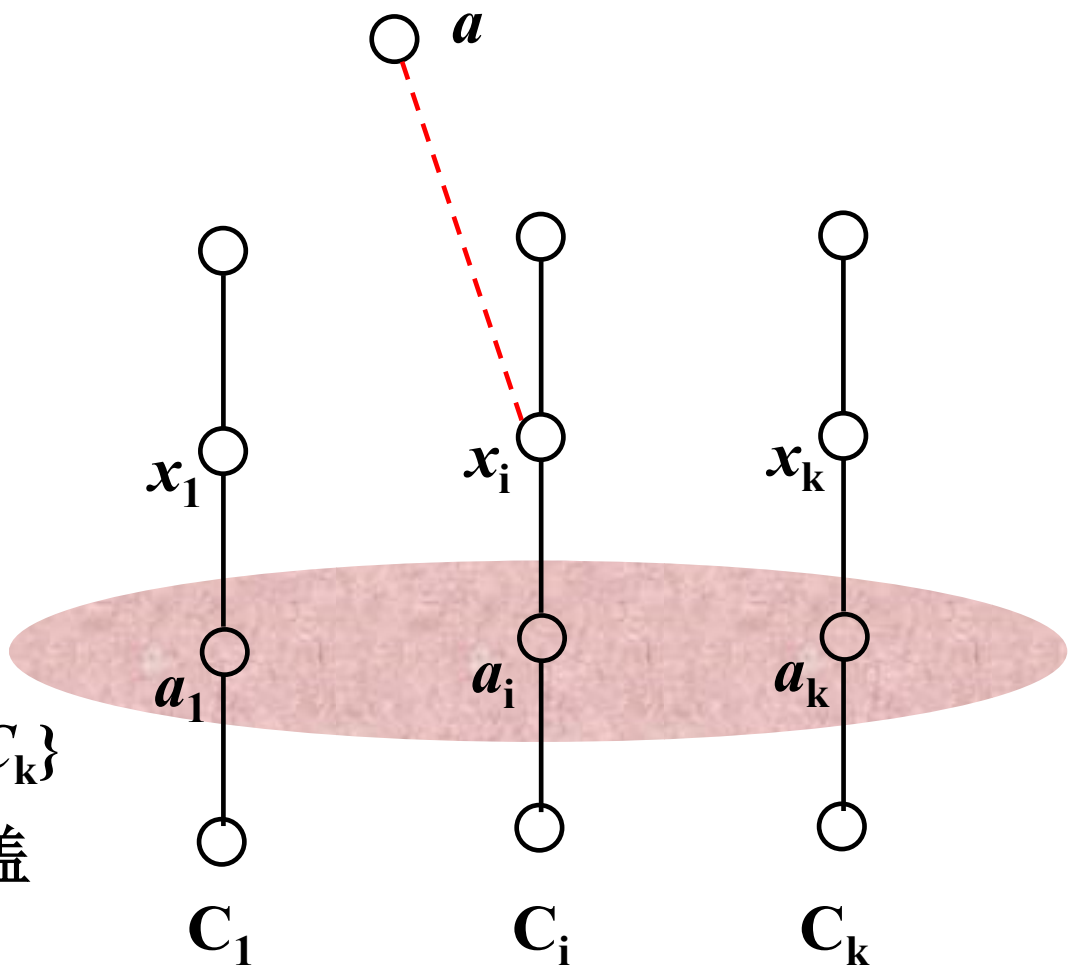
  设a为P中的一个极大元素，P’ =P-{a}

- 设(P’,≼)有一个大小为k的反链{$a_1, a_2, \ldots, a_k$}，并有一个规模为k的链覆盖{$C_1, C_2, \ldots, C_k$}.

- 对任意C_i , P’中大小为k的任一反链均有唯一的元素属于C_i，这些元素有一个最大元，记为x_i.

- A={$x_1, x_2, \ldots, x_k$}必是反链。否则，不妨假设A中有两个元素$x_i \preccurlyeq x_j$. 根据x_j的定义，P’中必有一个大小为k的反链A_j, x_j是A_j和C_j的公共元素，假设y是A_j和C_i的公共元素，则$y \preccurlyeq x_i$. 从而$y \preccurlyeq x_j$.与A_j是反链矛盾.

Dilworth定理的归纳证明（图示）



P’的反链

{C1, C2, …, Ck}
为P’的链覆盖

Dilworth定理的归纳证明（续）

- 如果 $\{a, x_1, x_2, \ldots, x_k\}$是P中的反链，而P的链覆盖$\{\{a\}, C_1, C_2, \ldots, C_k\}$就是规模为k+1的覆盖. 得证.
- 如果 $\{a, x_1, x_2, \ldots, x_k\}$不是P中的反链，即:存在某个$x_m$使得 $x_m \preccurlyeq a$.（a是极大元，不会出现 $a \preccurlyeq x_m$.）

令 $K = \{a\} \cup \{ z \in C_m \mid z \preccurlyeq x_m \}$. 显然K是P中的一条链. P-K中最大反链的大小为k-1（P-K中没有含k个元素的反链, 否则，与x_m的定义矛盾）. 由归纳假设，P-K有大小为k-1的一个链覆盖，该覆盖与K构成P的链覆盖（链数为k）， 已知$\{x_1, x_2, \ldots, x_k\}$ 是P中的反链（含k个元素）. 得证.

“道是无序却有序”

- 自然数1,2,3,…,n^2+1的任何一种排列中，必然含一个长度不小于n+1的严格递增链或严格递减链。

建立问题的偏序模型

- 给定1, 2 …n^2+1(=m)的一种排列 $v_1v_2\ldots v_m$，定义集合：
  - A={ (i,v_i) |i=1,2,…,n^2+1}
- 建立两个偏序关系R_1和R_2
  - $(i, v_i)R_1(j, v_j)$ *iff.* （i<j并且v_i<v_j）或者 (i, v_i)=(j, v_j)
  - $(i, v_i)R_2(j, v_j)$ *iff.* （i<j并且v_i>v_j）或者 (i, v_i)=(j, v_j)
- $R_1 \cap R_2 = I_A$, R_1的链是R_2反链。
- 问题：一定存在A的一个至少含n+1个元素的子集，它是R_1的链或者R_2的链。
  - 若R_1链的长度均≤n, 即R_2反链的大小均≤n，则存在个数k ≤n的R_2覆盖，其中必有长度超过n的R_2链.

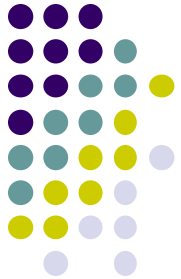
格

lub : “least upper bound”

glb : “greatest lower bound

- 定义：
  - 设$(S,\preccurlyeq)$是偏序集
  - $\forall x, y \in S$, 存在$\{x,y\}$的最小上界**lub**$\{x,y\}$, 记为$x \vee y$。
  - $\forall x, y \in S$, 存在$\{x,y\}$的最大下界**glb**$\{x,y\}$, 记为$x \wedge y$。
  - 则称S关于$\preccurlyeq$构成格。

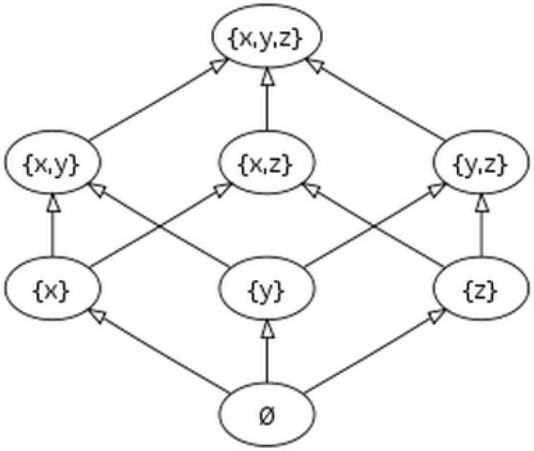
格的例子



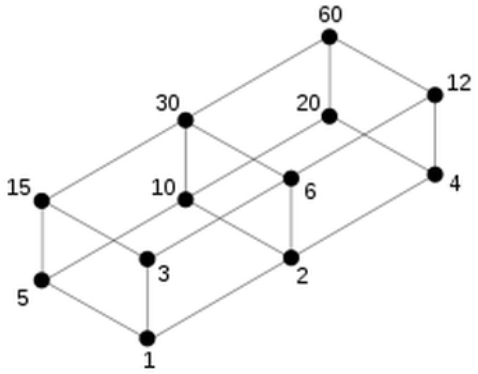
- $(\rho(B), \subseteq)$
  - $x \wedge y = x \cap y$, $x \vee y = x \cup y$
- $(\{x \in Z^+ \mid x|60\}, |)$，60的正因子集合及整除关系
  - $x \wedge y = \gcd(x,y)$, $x \vee y = \mathrm{lcm}(x,y)$
- $(Z, \leq)$
  - $x \wedge y = \min\{x,y\}$, $x \vee y = \max\{x,y\}$

格（示例）

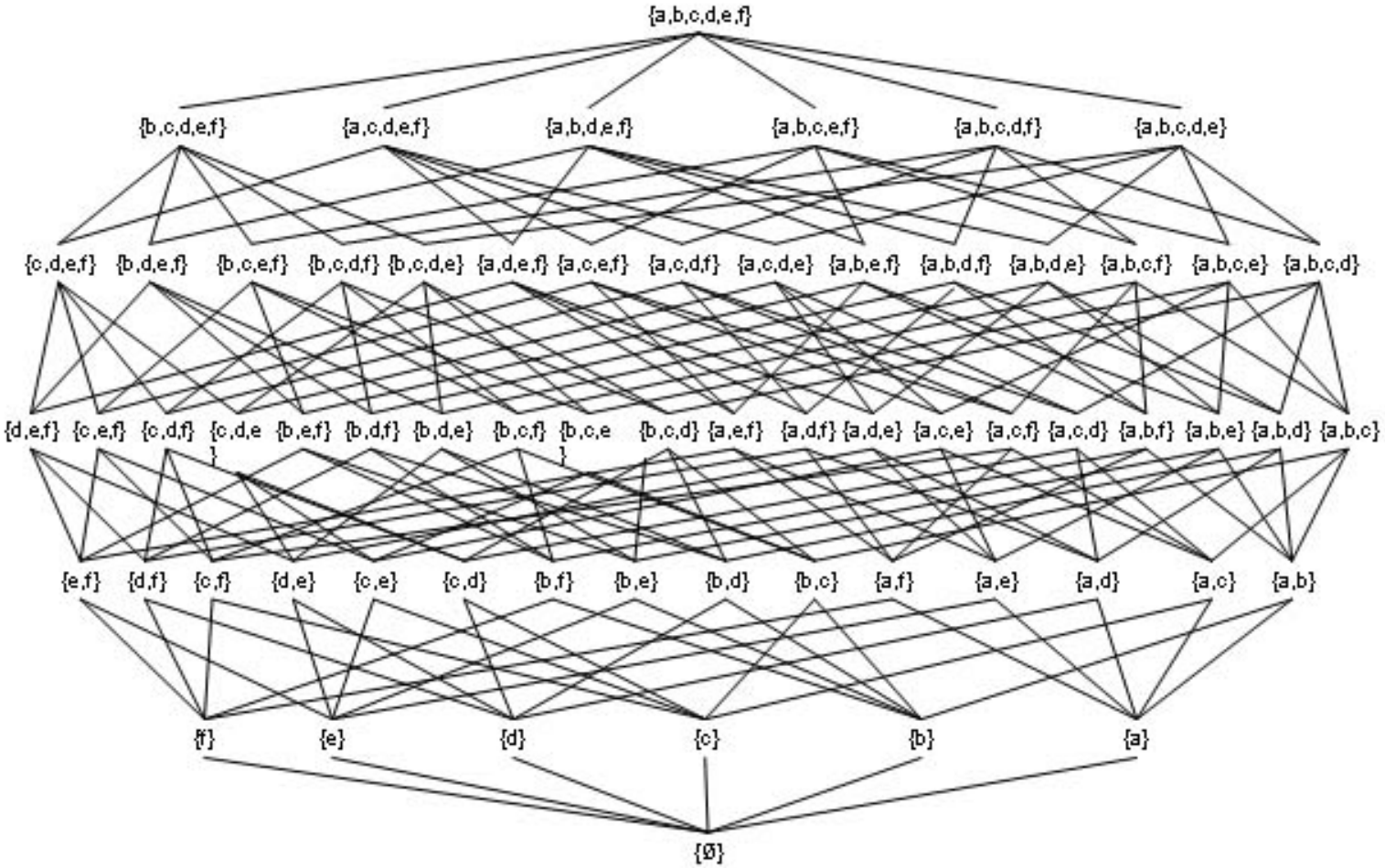
- The power set of { *x*, *y*, *z* } partially ordered by inclusion, has the Hasse diagram:



- The set *A* = { 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60 } of all divisors of 60, partially ordered by divisibility, has the Hasse diagram:

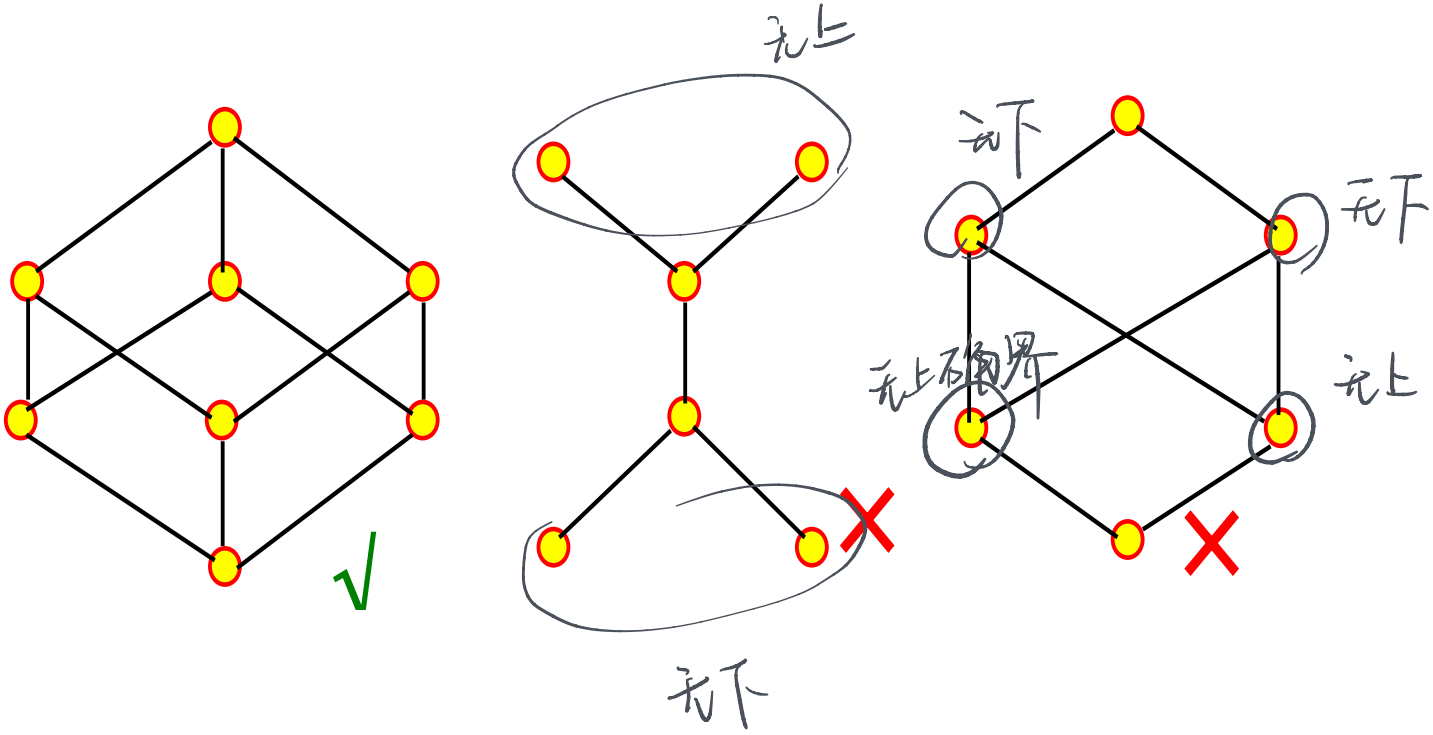


格（示例）

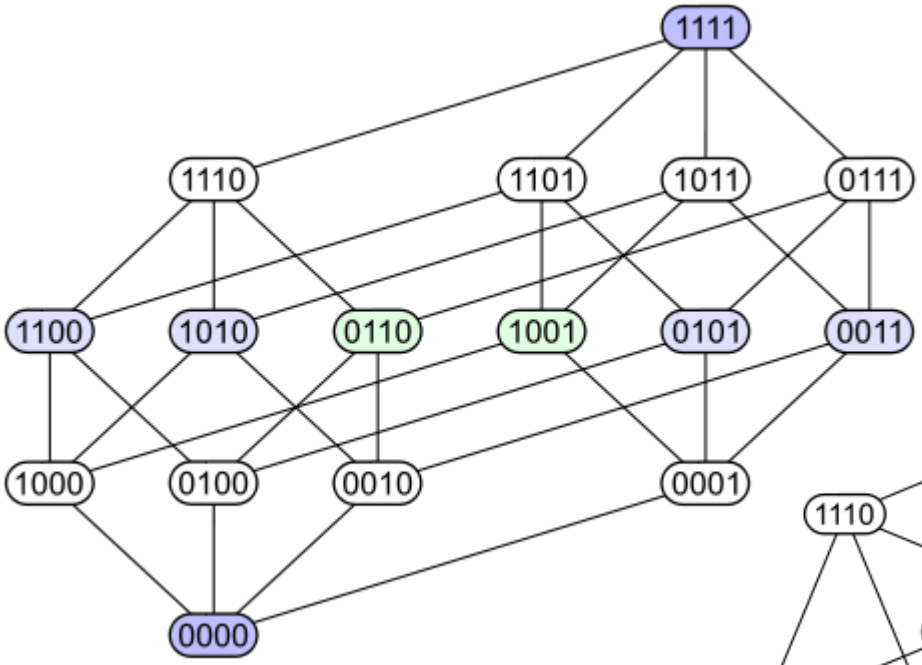

{a,b,c,d,e,f}
{b,c,d,e,f}
{a,c,d,e,f}
{a,b,d,e,f}
{a,b,c,e,f}
{a,b,c,d,f}
{a,b,c,d,e}
{c,d,e,f}
{b,d,e,f}
{b,c,e,f}
{b,c,d,f}
{b,c,d,e}
{a,d,e,f}
{a,c,e,f}
{a,c,d,f}
{a,c,d,e}
{a,b,e,f}
{a,b,d,f}
{a,b,d,e}
{a,b,c,f}
{a,b,c,e}
{a,b,c,d}
{d,e,f}
{c,e,f}
{c,d,f}
{c,d,e}
{b,e,f}
{b,d,f}
{b,d,e}
{b,c,f}
{b,c,e}
{b,c,d}
{a,e,f}
{a,d,f}
{a,d,e}
{a,c,e}
{a,c,f}
{a,c,d}
{a,b,f}
{a,b,e}
{a,b,d}
{a,b,c}
{e,f}
{d,f}
{c,f}
{d,e}
{c,e}
{c,d}
{b,f}
{b,e}
{b,d}
{b,c}
{a,f}
{a,e}
{a,d}
{a,c}
{a,b}
{f}
{e}
{d}
{c}
{b}
{a}
{Ø}

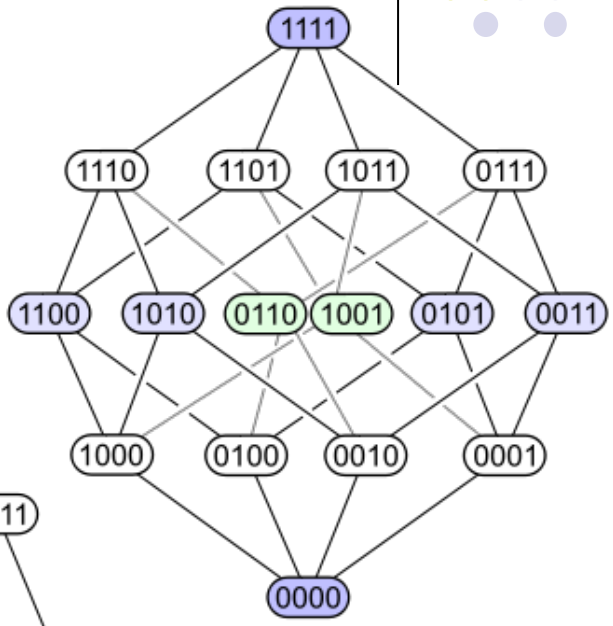
格与哈斯图

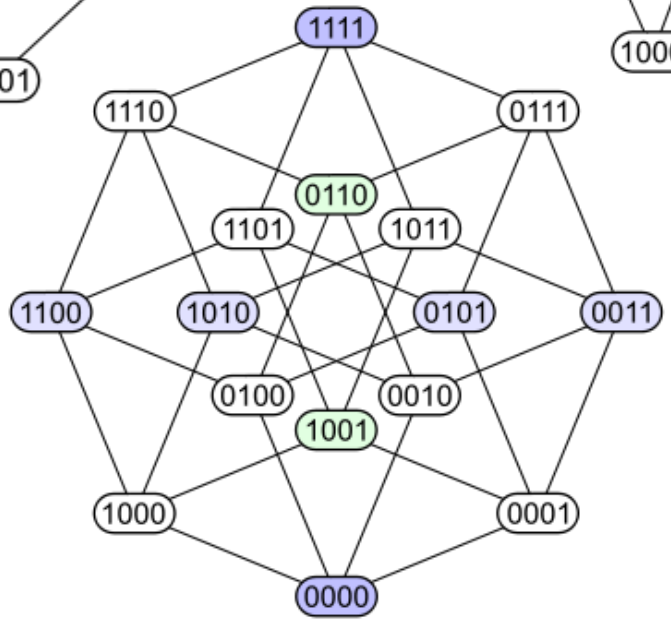
- 右边两个哈斯图所表示的偏序集不是格



格与哈斯图（续）


1111
1110
1101
1011
0111
1100
1010
0110
1001
0101
0011
1000
0100
0010
0001
0000


1111
1110
1101
1011
0111
1100
1010
0110
1001
0101
0011
1000
0100
0010
0001
0000


1111
1110
0111
0110
1101
1011
1100
1010
0101
0011
0100
0010
1001
1000
0001
0000

格的基本关系式

- 根据“最小上界”和“最大下界”的定义，有如下关系式：
  - $a \preccurlyeq c,\ b \preccurlyeq c \Rightarrow a \vee b \preccurlyeq c$
  - $c \preccurlyeq a,\ c \preccurlyeq b \Rightarrow c \preccurlyeq a \wedge b$

格的性质

- 若(S, ≼)是格，则：$\forall a, b \in S$:

$$a \preccurlyeq b \Leftrightarrow a \wedge b = a \Leftrightarrow a \vee b = b$$

  - 可以采用循环证明
  - $a \preccurlyeq b \Rightarrow a \wedge b = a$
  - $a \wedge b = a \Rightarrow a \vee b = b$
  - $a \vee b = b \Rightarrow a \preccurlyeq b$

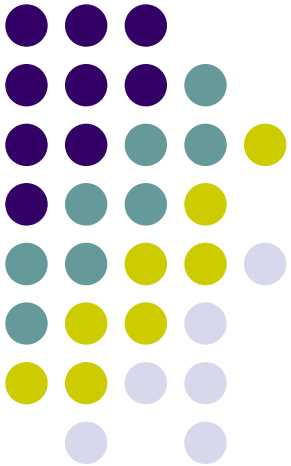
格的性质

- 设$(S, \preccurlyeq)$是格，则$(S, \wedge, \vee)$有下列性质：
  - 结合律：$(a \wedge b) \wedge c = a \wedge (b \wedge c)$，$(a \vee b) \vee c = a \vee (b \vee c)$
  - 交换律：$a \wedge b = b \wedge a$，$a \vee b = b \vee a$
  - 吸收律：$a \wedge (a \vee b) = a$，$a \vee (a \wedge b) = a$

代数格

离散数学—代数结构

南京大学计算机科学与技术系



内容提要

- 代数格的定义
- 格的对偶原理
- 子格
- 格同态、格同构
- 分配格
- 有界格
- 有补格
- 有补分配格

格（回顾）

- $(S,\preccurlyeq)$的一个（偏序）格，如果下列条件成立：
  - 设$(S,\preccurlyeq)$是偏序集
  - $\forall x, y \in S$, 存在$\{x,y\}$的最小上界**lub**$\{x,y\}$, 记为$x \vee y$。
  - $\forall x, y \in S$, 存在$\{x,y\}$的最大下界**glb**$\{x,y\}$, 记为$x \wedge y$。
- 设$(S, \preccurlyeq)$是格，则$(S, \wedge, \vee)$有下列性质：
  - 结合律：$(a \wedge b) \wedge c = a \wedge (b \wedge c)$, $(a \vee b) \vee c = a \vee (b \vee c)$
  - 交换律：$a \wedge b = b \wedge a$, $a \vee b = b \vee a$
  - 吸收律：$a \wedge (a \vee b) = a$, $a \vee (a \wedge b) = a$

格的代数性质

结合律　交换律　吸收律　幂等律

吸收律 ⇨ 幂等律

$x \wedge x = x \wedge (x \vee (x \wedge x)) = x$ （两次应用吸收律）

同理可证：$x \vee x = x$

代数格（定义）

- 设L是一个集合，∧和∨是L上的二元运算，且满足结合律、交换律、吸收律，则称(L, ∧, ∨)是代数格。

等　式	名　称
$x\wedge(y\wedge z)=(x\wedge y)\wedge z$ $x\vee(y\vee z)=(x\vee y)\vee z$	结合律
$x\wedge y = y\wedge x$ $x\vee y = y\vee x$	交换律
$x\vee(x\wedge y) = x$ $x\wedge(x\vee y) = x$	吸收律

代数格中的偏序关系

- $\forall\, x, y \in \mathbf{B}, x \wedge y = x$ *iff* $x \vee y = y$
  - 若 $x \wedge y = x$，则 $x \vee y = (x \wedge y) \vee y = y$ //吸收律
  - 若 $x \vee y = y$，则 $x \wedge y = x \wedge (x \vee y) = x$ //吸收律
- $\forall\, x, y \in \mathbf{B}$, 定义 $x \preccurlyeq y$ *iff* $x \wedge y = x$ (即 $x \vee y = y$)
  - 证明这个关系满足自反性、反对称性、传递性。
  - 这个偏序构成一个格。
    - **lub**$\{x, y\}$ 即为 $x \vee y$。//需要验证
    - **glb**$\{x, y\}$ 即为 $x \wedge y$。//需要验证
- 代数格等同于（偏序）格

关于格的对偶命题

- 对偶命题的例子
  - $a \wedge b \preccurlyeq a$和$a \vee b \succcurlyeq a$互为对偶命题
- 对偶命题构成规律
  - 格元素名不变
  - $\preccurlyeq$与$\succcurlyeq$，$\wedge$与$\vee$全部互换。

格的对偶原理

- 如果命题P对一切格为真，则P的对偶命题P^*也对一切格为真。
  - 证明思路：证明P^*对任意格$(S, \preccurlyeq)$为真
  - 定义S上的二元关系$\preccurlyeq^*$, $\forall a,b\in S$, $a\preccurlyeq^* b \Leftrightarrow b\preccurlyeq a$, 显然$\preccurlyeq^*$是偏序。
  - $\forall a,b\in S$, $a\wedge^* b=a\vee b$, $a\vee^* b=a\wedge b$ 所以$(S, \preccurlyeq^*)$也是格
    - 这里$a\wedge^* b$, $a\vee^* b$分别是a,b关于偏序$\preccurlyeq^*$的最大下界和最小上界。
  - P^*在$(S, \preccurlyeq)$中为真*当且仅当*P在$(S, \preccurlyeq^*)$中为真。
  - P在一切格中为真，$\therefore P^*$在一切格中为真。

子 格

- 子格（sub lattice）是格的子代数。设$\langle L,\wedge,\vee\rangle$是格，非空集合$S \subseteq L$，若$S$关于$L$中的运算$\wedge,\vee$仍构成格，称$\langle S,\wedge,\vee\rangle$是$L$的子格。

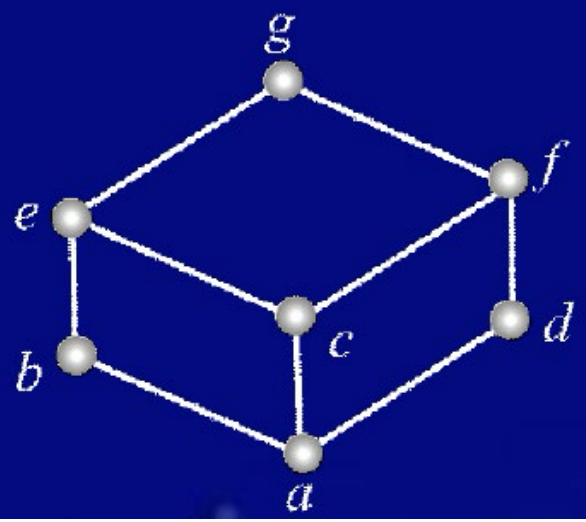
例 13.5 设格 L 如图 3 所示. 令

$S_1=\{a, e, f, g\}$, $S_2=\{a, b, e, g\}$

S_1 不是 L 的子格, 因为

$e, f \in S_1$ 但 $e \wedge f = c \notin S_1$.

S_2 是 L 的子格.



格同态

定义 13.5 设 L_1 和 L_2 是格，

$$f: L_1 \to L_2,$$

若 $\forall a,b \in L_1$ 有

$$f(a \wedge b) = f(a) \wedge f(b),$$

$$f(a \vee b) = f(a) \vee f(b)$$

成立，则称 f 为格 L_1 到 L_2 的同态映射，简称格同态.

格同态与格同构

- 定理（同态保序）：设f是格L_1到L_2的映射，

(1) 若f为格同态映射，则f保序，即

$$(\forall x, y \in L_1)(x \preccurlyeq y \rightarrow f(x) \preccurlyeq f(y))$$

(2) 若f为双射，则f为格同构映射当且仅当

$$(\forall x, y \in L_1)(x \preccurlyeq y \Leftrightarrow f(x) \preccurlyeq f(y))$$

格同态的保序性（续）

例　设 $L_1=<S_{12},D>$, $L_2=<S_{12},\leq>$是格，其中：

S_{12} 是 12 的所有正因子构成的集合，

D 为整除关系，$\leq$为通常数的小于或等于关系.

令

$$f:S_{12}\rightarrow S_{12}, f(x)=x$$

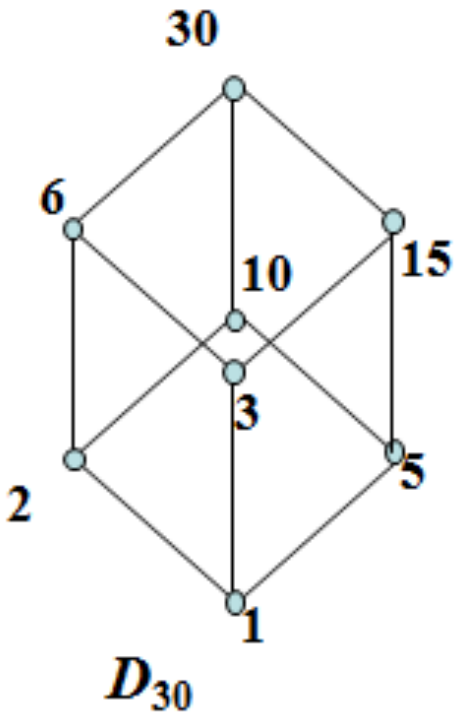
f 是双射，但不是格 L_1 到 L_2 的同构映射.

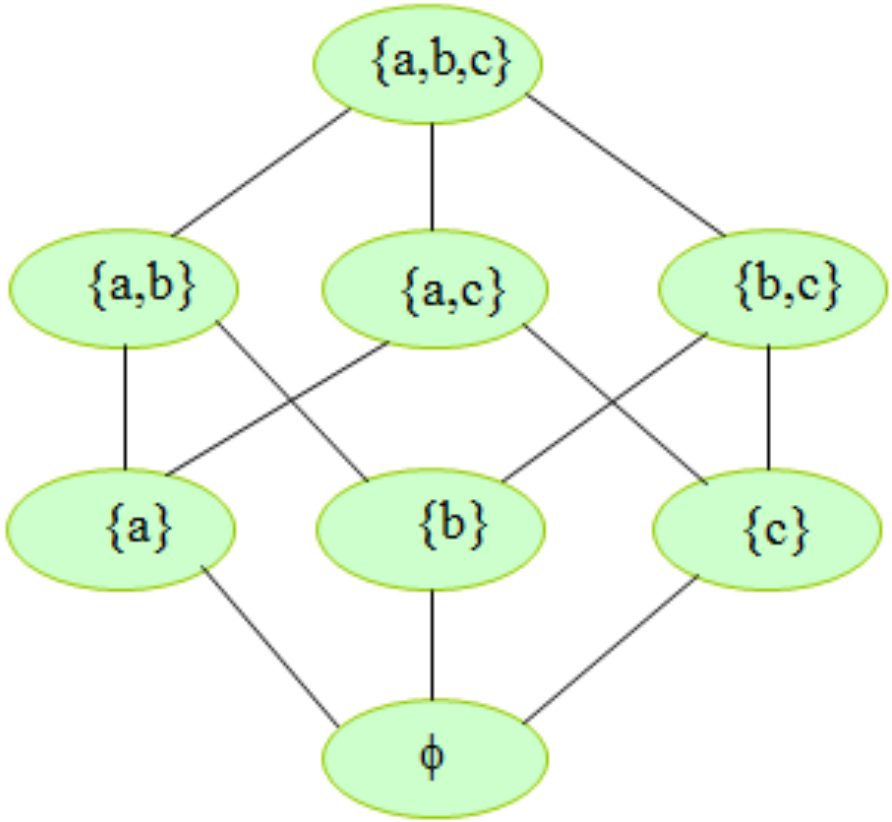
因为 $f(2)\leq f(3)$，但 2 不整除 3.

根据上述定理可知 f 不是同构映射

格同构的直观特征

- 观察以下2个格的哈斯图：

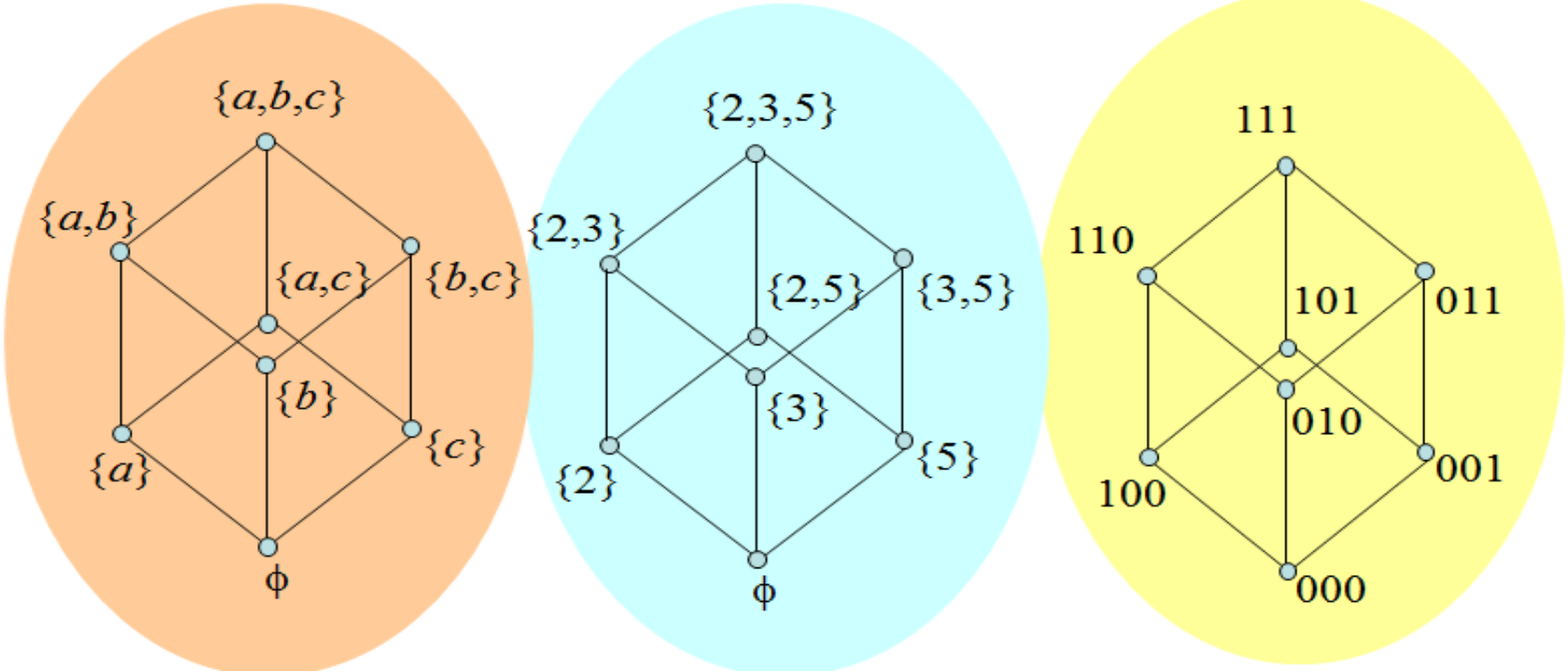




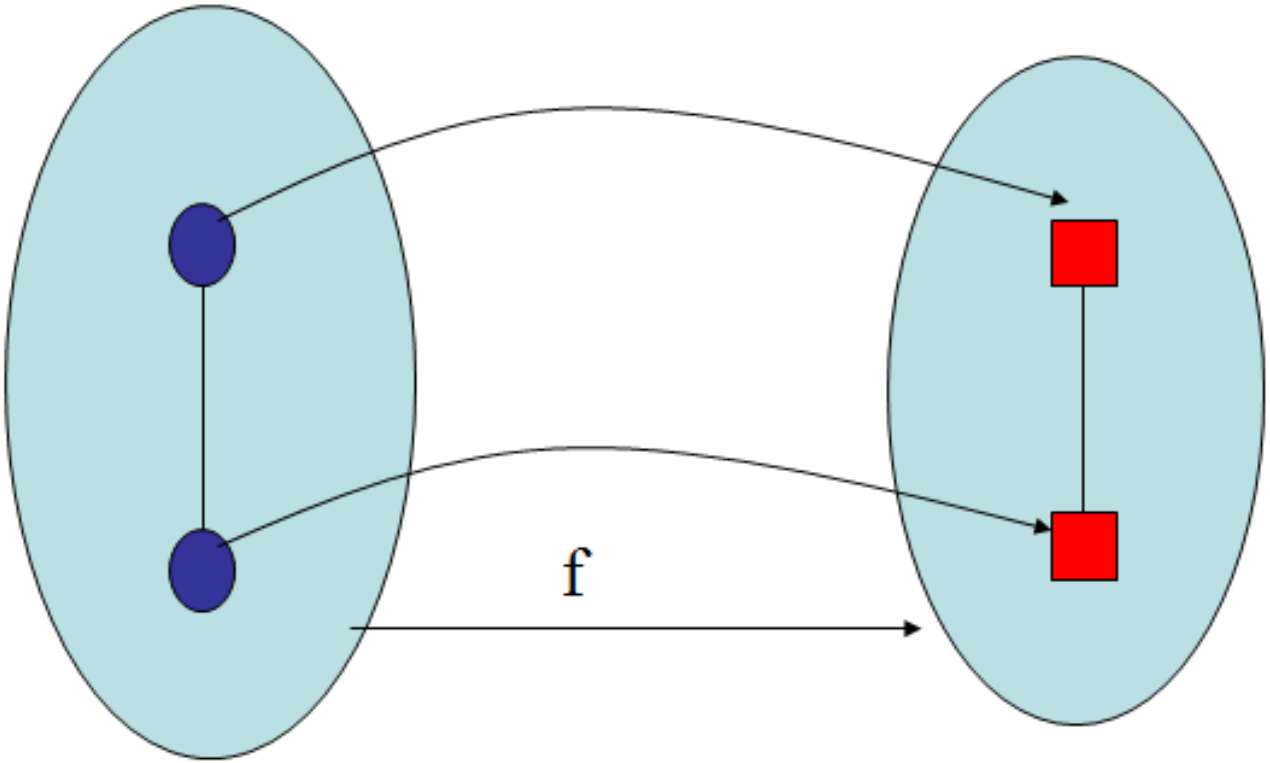
格同构的直观特征（续）

- Iso ⇨ same
- Morph ⇨ shape

⇒ Isomorphic lattices have same Hasse diagrams' shape



格同构的直观特征（续）



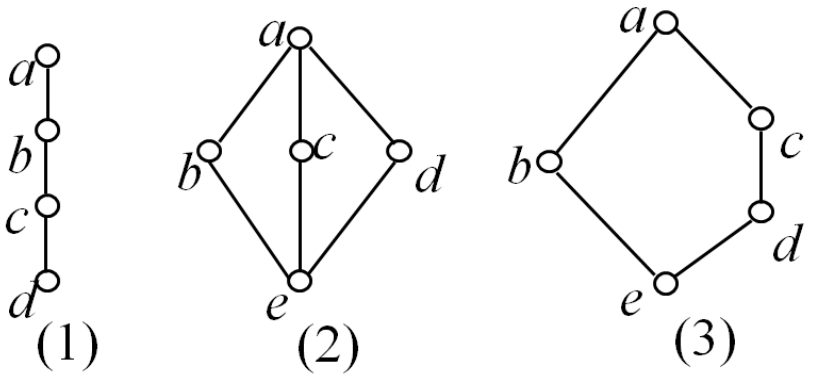
几种典型的格

- 定义（三种典型的格）：

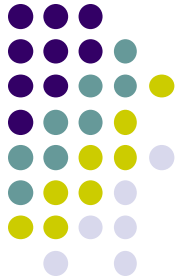
  (1) 链（chain）

  (2) 钻石格（diamond lattice, M_3）

  (3) 五角格（pentagon lattice, N_5）



分配格



- 定义（分配格）：设$\langle L,\wedge,\vee\rangle$为格，若$\forall a,b,c\in L$，

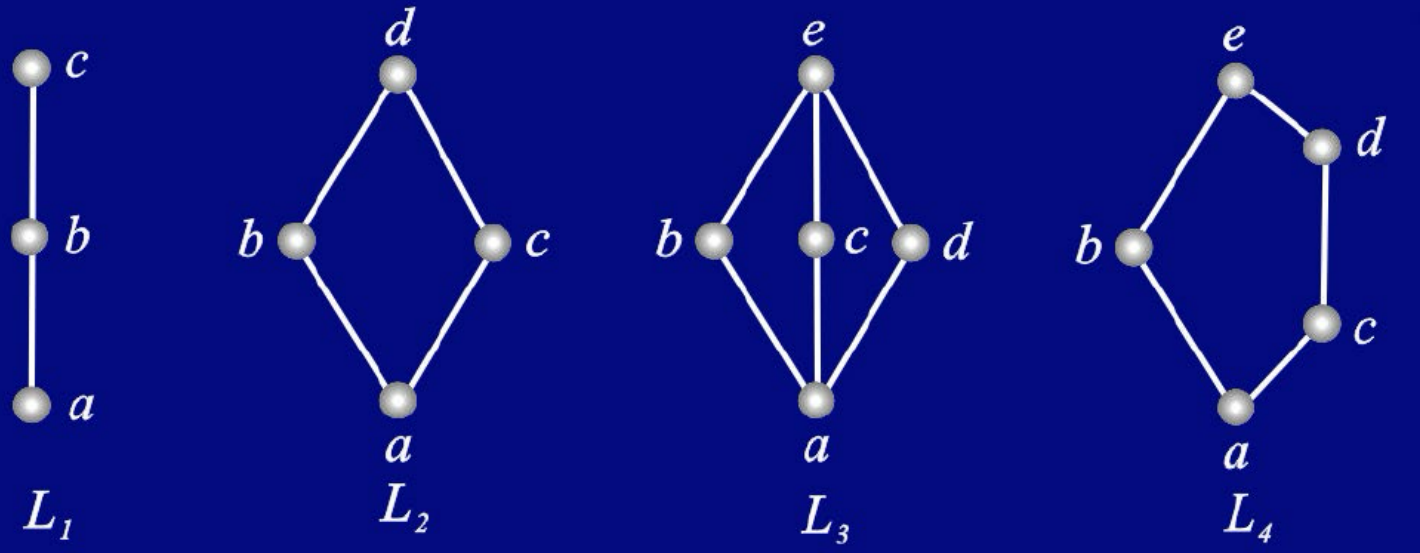
$$\boldsymbol{a\wedge(b\vee c)=(a\wedge b)\vee(a\wedge c)}$$

$$\boldsymbol{a\vee(b\wedge c)=(a\vee b)\wedge(a\vee c)}$$

则称L为分配格（distributive lattice）

分配格（续）

例　参见下图



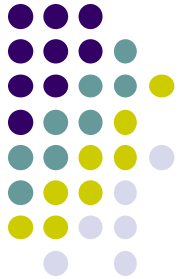
L_1　L_2　L_3　L_4

L_1 和 L_2 是分配格，L_3 和 L_4 不是分配格.　　图5

在 L_3 中，$b \wedge (c \vee d) = b \wedge e = b$，$(b \wedge c) \vee (b \wedge d) = a \vee a = a$

在 L_4 中，$c \vee (b \wedge d) = c \vee a = c$，$(c \vee b) \wedge (c \vee d) = e \wedge d = d$

分配格的判定定理



- 定理（分配格判定定理一）：设L为格，则L是分配格当且仅当L不含有与M_3（钻石格）或N_5（五角格）同构的子格
- 推论
  - 小于五元的格皆为分配格
  - 任何链皆为分配格

分配格的判定定理（续）

例　说明图 6 中的格是否为分配格，为什么？

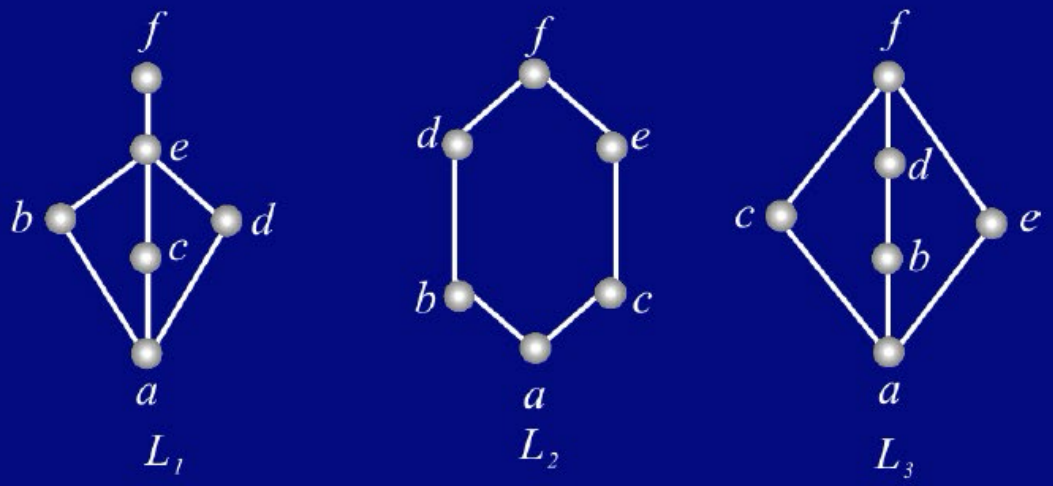


图 6

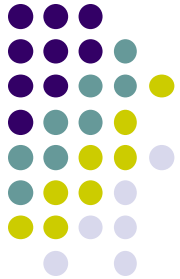
解　L_1, L_2 和 L_3 都不是分配格.

$\{a, b, c, d, e\}$ 是 L_1 的子格，并且同构于钻石格；

$\{a, b, c, e, f\}$ 是 L_2 的子格，并且同构于五角格；

$\{a, c, b, e, f\}$ 是 L_3 的子格，也同构于钻石格.

分配格的判定定理（续）



- 定理（分配格判定定理二）：设L为格，则L是分配格当且仅当

$$(\forall a,b,c \in L)((a \wedge b = a \wedge c \text{且} a \vee b = a \vee c) \rightarrow b = c)$$

分配格的判定定理（续）

证 必要性. $\forall a,b,c \in L$, 有

$$
\begin{aligned}
b &= b \vee (a \wedge b) && \text{(吸收律,交换律)} \\
&= b \vee (a \wedge c) && \text{(已知条件代入)} \\
&= (b \vee a) \wedge (b \vee c) && \text{(分配律)} \\
&= (a \vee c) \wedge (b \vee c) && \text{(已知条件代入,交换律)} \\
&= (a \wedge b) \vee c && \text{(分配律)} \\
&= (a \wedge c) \vee c && \text{(已知条件代入)} \\
&= c && \text{(交换律,吸收律)}
\end{aligned}
$$

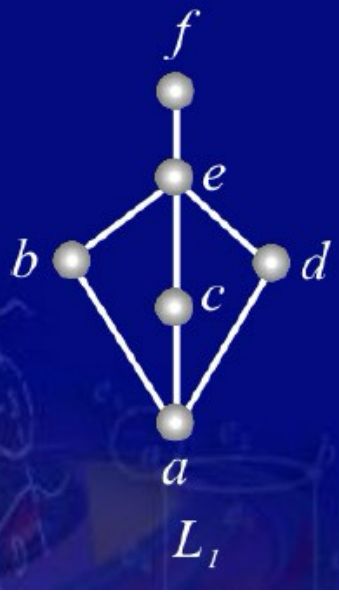
分配格的判定定理（续）

例　以下三个格都不是分配格.

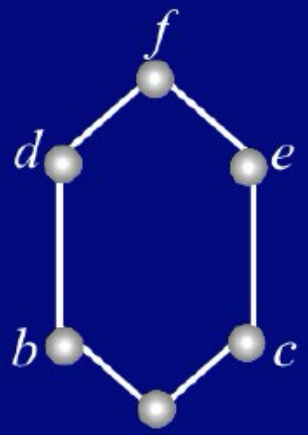
在 L_1 中有 $b \vee c = b \vee d, b \wedge c = b \wedge d,$ 但 $c \neq d$

在 L_2 中有 $b \wedge c = b \wedge e, b \vee c = b \vee e,$ 但 $c \neq e$

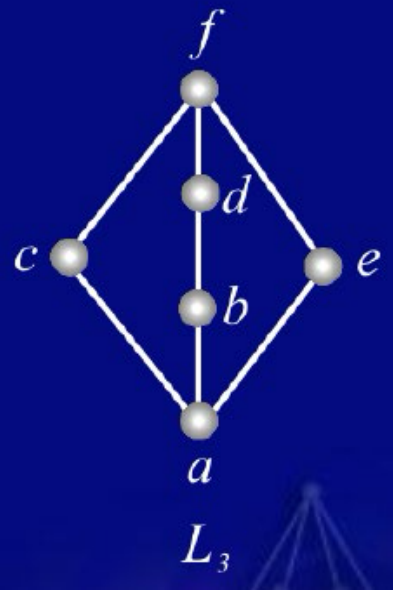
在 L_3 中有 $c \wedge b = c \wedge d, c \vee b = c \vee d,$ 但 $b \neq d$



L_1



L_2



L_3

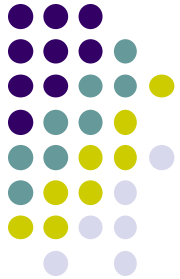
图7

有界格

- 定义（有界格）：设L为格，
  - 若存在$b \in L$，使得$\forall x \in L$有$b \preccurlyeq x$，则称元素b是格L的全下界（bottom）
  - 若存在$t \in L$，使得$\forall x \in L$有$x \preccurlyeq t$，则称元素t是格L的全上界（top）

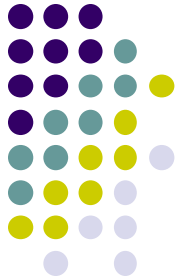
此时格L称为有界格（bounded lattice）

有界格（续）



- 注意
  - 若格L中存在全下界或全上界，则一定唯一
  - 一般将格L的全下界记为$\mathbf{0}$，全上界记为$\mathbf{1}$
  - 有界格L一般记为$\langle L,\wedge,\vee,\mathbf{0},\mathbf{1}\rangle$
    - $\forall a \in L:\ a \vee \mathbf{0} = a,\ a \wedge \mathbf{1} = a$

有界格（续）

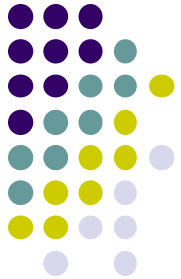


- 事实
  - 有限格皆为有界格，设$L = \{a_1, a_2, \cdots, a_n\}$，则

    $a_1 \wedge a_2 \wedge \cdots \wedge a_n$是$L$的全下界

    $a_1 \vee a_2 \vee \cdots \vee a_n$是$L$的全上界
  - 求涉及有界格的命题之对偶命题，须将全下界与全上界对换

有界格（续）



- 有界格$\langle L,\wedge,\vee,0,1\rangle$满足同一律、支配律
  - 同一律：$\forall a \in L,\ a \vee \mathbf{0} = a,\ a \wedge \mathbf{1} = a$
  - 支配律：$\forall a \in L,\ a \wedge \mathbf{0} = \mathbf{0},\ a \vee \mathbf{1} = \mathbf{1}$
  - **0**是关于∨ 运算的单位元，∧运算的零元；
  - **1**是关于∧ 运算的单位元，∨运算的零元。

有补格

- 定义（有界格的补元）：设$\langle L,\wedge,\vee,0,1\rangle$为有界格，

  $a \in L$，若存在$b \in L$使得

  $$a \wedge b = \mathbf{0} \text{ 且 } a \vee b = \mathbf{1}$$

  则称元素b是a的补元（complement）

有补格（续）

例 考虑下图中的四个格. 针对不同的元素，求出所有的补元.

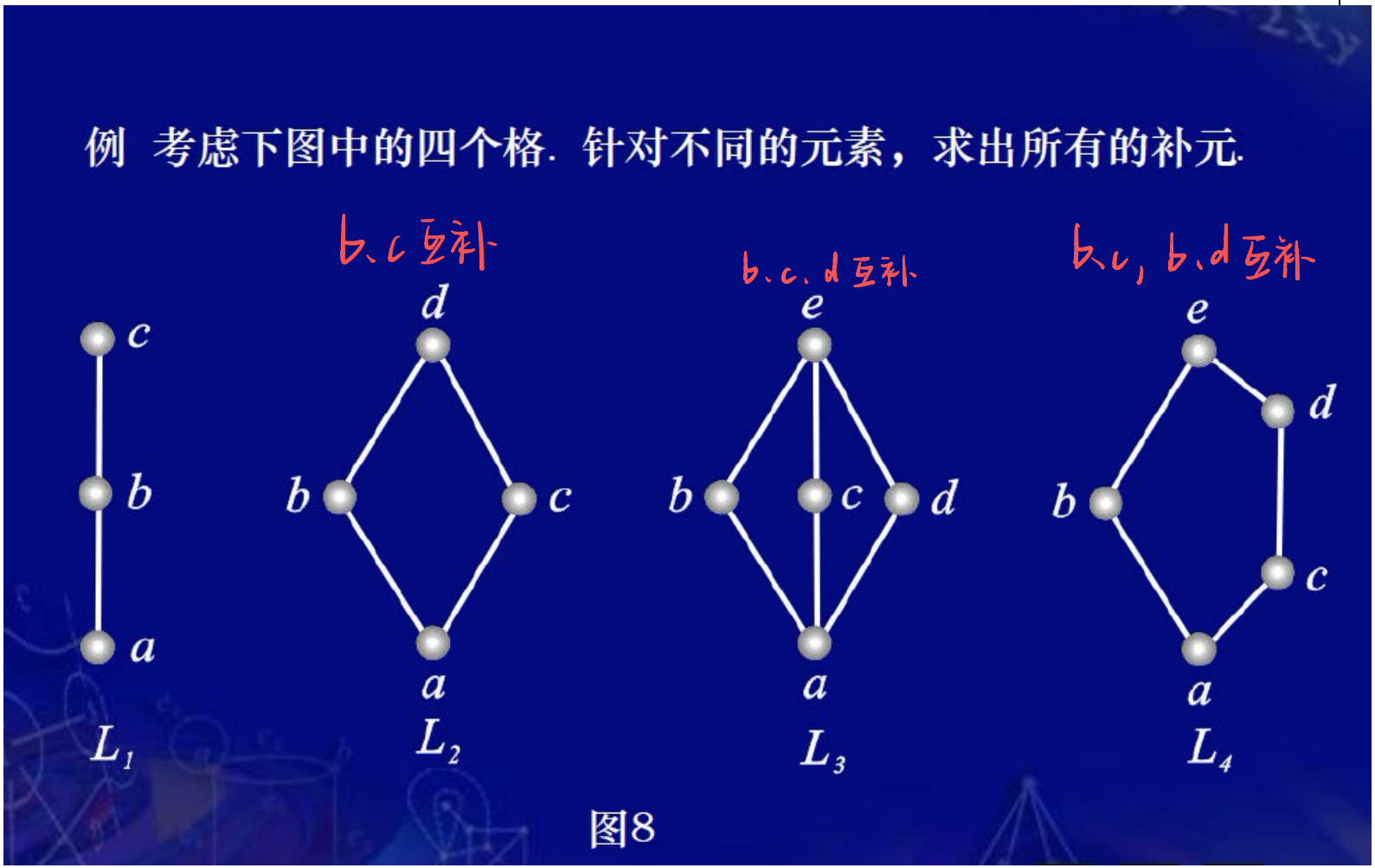
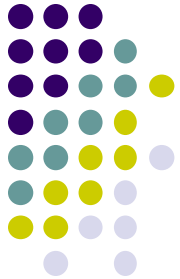


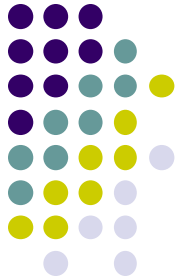
图8

有补格（续）



- 事实
  - 任何有界格中，全上界1和全下界0互补
  - 对于一般元素，可能不存在补元
  - 补元若存在，可能有多个（不保证唯一）
  - 对于有界分配格，补元若存在则唯一

有补格（续）

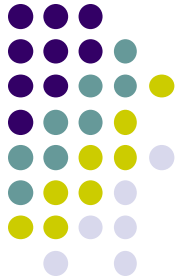


- 定理（有界分配格的补元唯一）：设$\langle L,\wedge,\vee,0,1\rangle$为有界分配格，$a\in L$，若$a$存在补元则其补元唯一
- 证明：假设b,c皆为a之补元，则有

$$a\vee c=\mathbf{1},a\wedge c=\mathbf{0};a\vee b=\mathbf{1},a\wedge b=\mathbf{0}$$

由于全上界和全下界唯一，从而有$a\vee c=a\vee b$，，$a\wedge c=a\wedge b$。由于L是分配格，故$b=c$. □

有补格（续）



- 定义（有补格）：设$\langle L,\wedge,\vee,0,1\rangle$为有界格，

  若L中所有元素皆存在补元，则称L为有补格

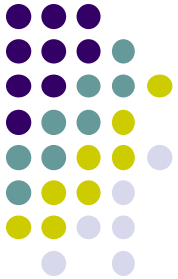
  （complemented lattice）

- 例：钻石格M_3和五角格N_5皆为有补格

有补分配格

- 代数格：结合律、交换律、吸收律、（幂等律）
- 分配格：分配律
- 有　界：同一律、0、1（支配律）
- 有　补：补　律、（双重补律、德摩根律）

有补分配格（代数性质）



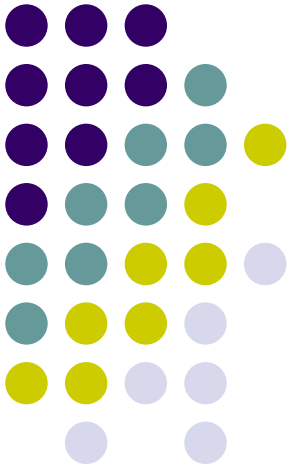
结合律　交换律　分配律　同一律　补律

吸收律　幂等律　支配律　双重补律　德摩根律

布尔代数

离散数学—代数结构

南京大学计算机科学与技术系



内容提要

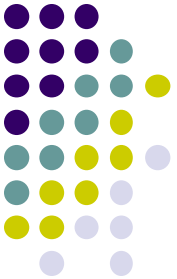
- 布尔代数的抽象定义
- 布尔代数的性质
- 有限布尔代数
- 布尔函数
- 布尔代数
- 布尔代数与数字逻辑电路设计

布尔代数的抽象定义

- 一个布尔代数是一个集合B，它有二元运算∨和∧、一元运算¯以及特殊元素0和1，且∀$x, y, z \in B$，下列性质成立：

$x \vee (y \vee z) = (x \vee y) \vee z$ $x \wedge (y \wedge z) = (x \wedge y) \wedge z$	结合律
$x \wedge y = y \wedge x$ $x \vee y = y \vee x$	交换律
$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$	分配律
$x \vee 0 = x$ $x \wedge 1 = x$	同一律
$x \vee \bar{x} = 1$ $x \wedge \bar{x} = 0$	补　律

布尔代数（举例）



- $(\{0, 1\}, +, \cdot, \bar{}, 0, 1)$为布尔代数
  - 布尔和: $1+1=1,\ 1+0=1,\ 0+1=1,\ 0+0=0$
  - 布尔积: $1\cdot 1=1,\ 1\cdot 0=0,\ 0\cdot 1=0,\ 0\cdot 0=0$
  - 补: $\bar{0}=1,\ \bar{1}=0$
- $B^n=\{(x_1, \ldots, x_n) \mid x_i \in B, i=1, \ldots, n\}$构成布尔代数
  - $x=(a_1, \ldots, a_n),\ y=(b_1, \ldots, b_n),\ a_i \in B,\ b_i \in B$
  - $x \wedge y = (c_1, \ldots, c_n)$, where $c_i=a_i \wedge b_i$
  - $x \vee y = (d_1, \ldots, d_n)$, where $d_i=a_i \vee b_i$
  - $\bar{x} = (e_1, \ldots, e_n)$, where $e_i=\bar{a}_i$
- A的幂集构成一个布尔代数$(\rho(A), \cap, \cup, \sim, \varnothing, A)$

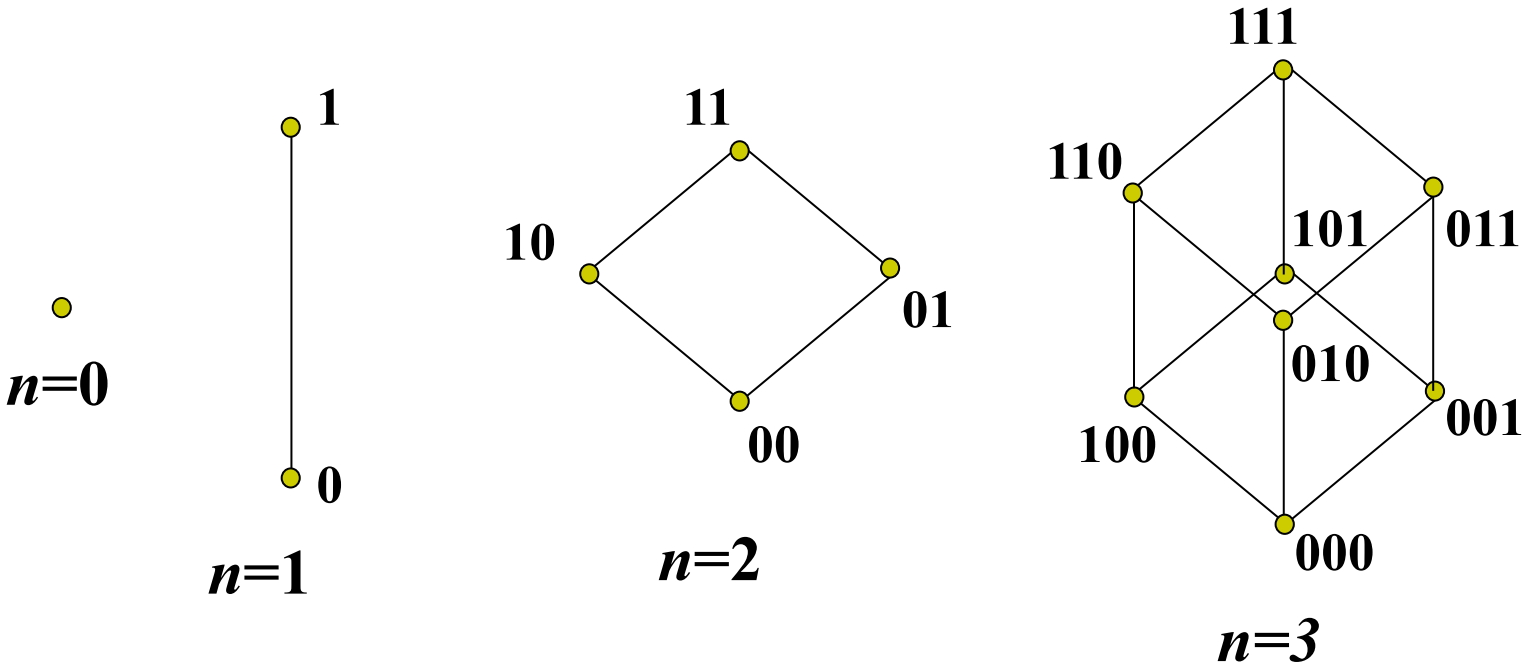
B^n as Product of n B's

- **B^1, ($\{0,1\}$, $\wedge$, $\vee$, $^-$, 0, 1), is denoted as B.**
- **For any $n \geq 1$, $B^n = B \times B \times \ldots \times B$, where $B \times B \times \ldots \times B$ is given the product partial order.**

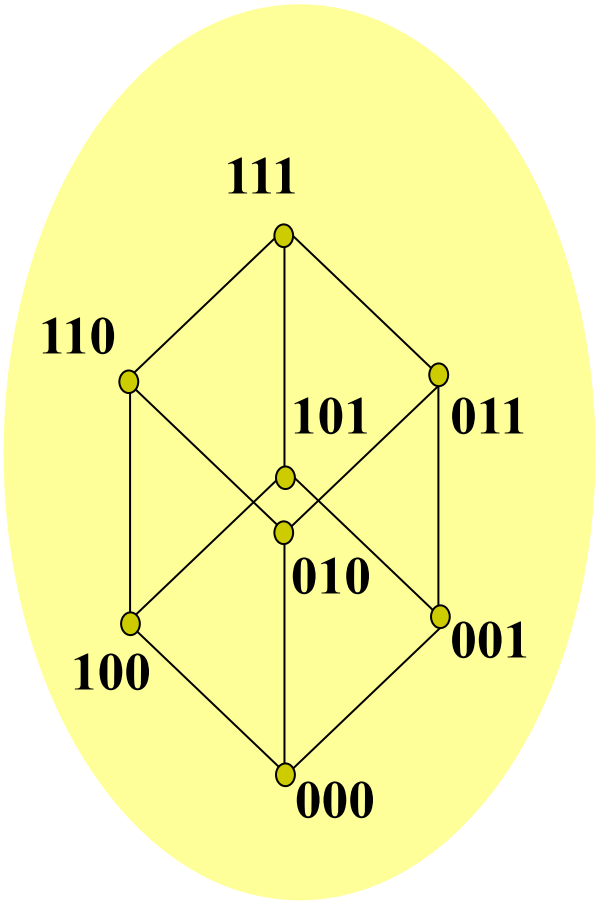
$$x \leq y \text{ if and only if } x_k \leq y_k \text{ for each } k.$$

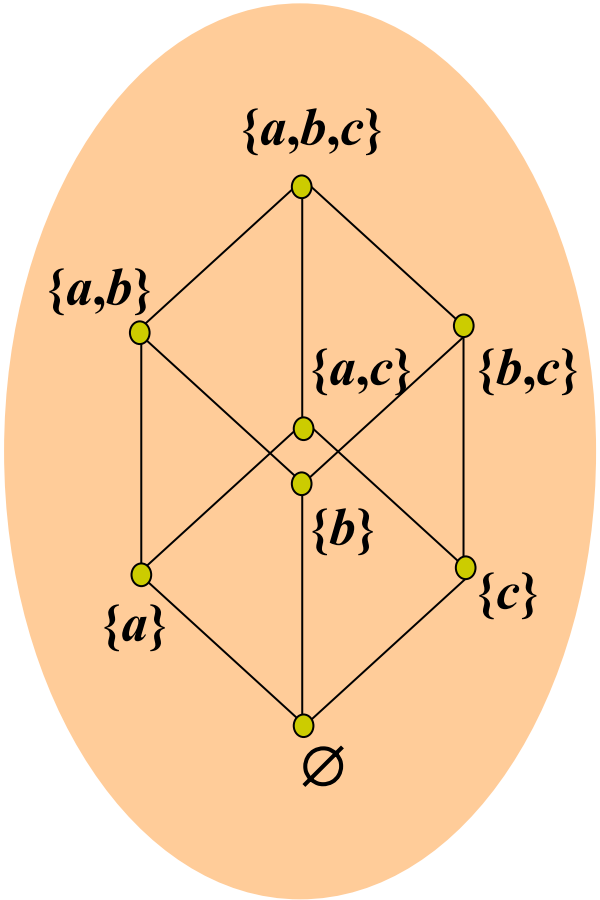
布尔代数

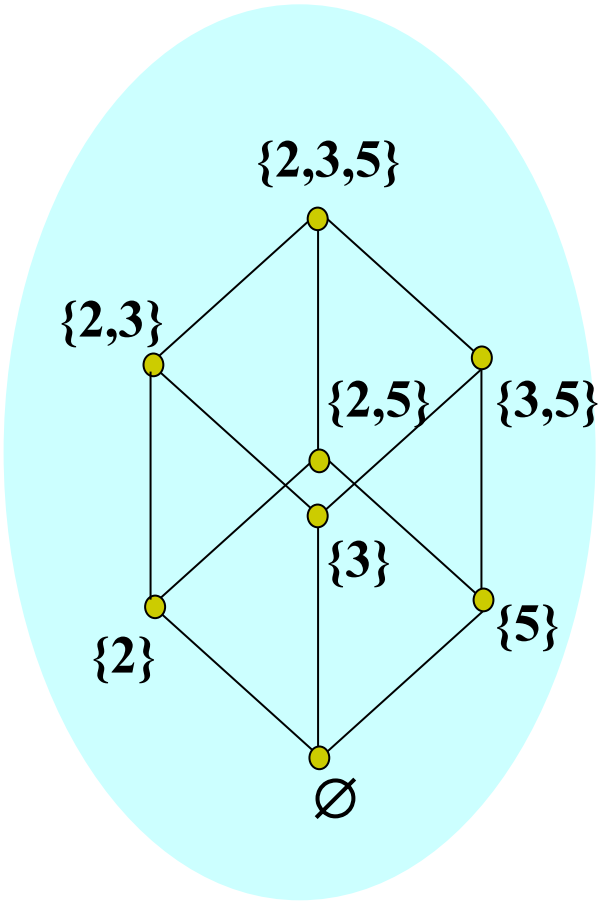
B^n与含n个元素的集合的幂集代数同构



Hasse Diagrams of Isomorphic Lattices

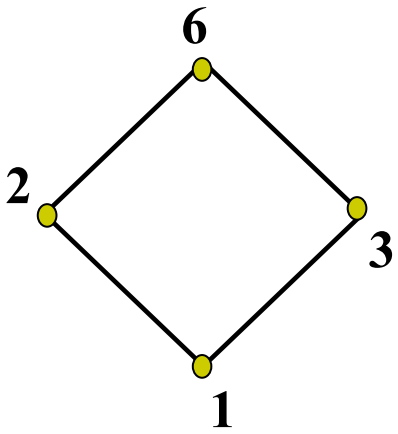




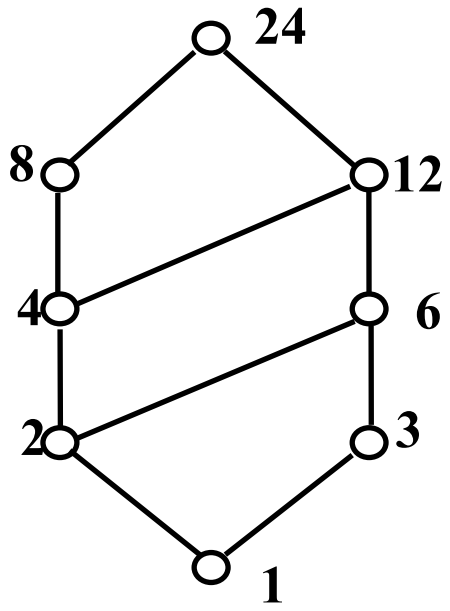


Examples

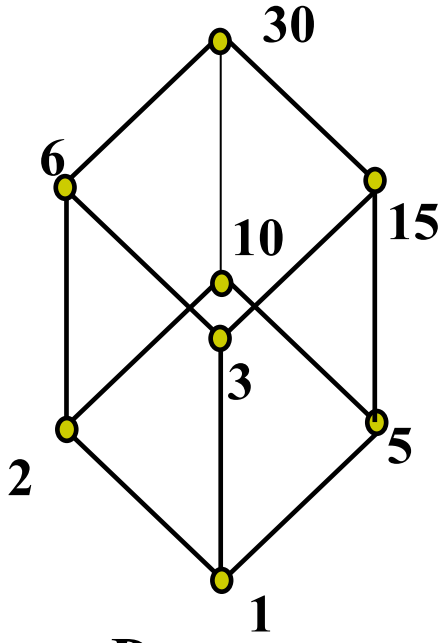
D_n is the set of all positive divisors of n with the partial order "divisibility".



D_6

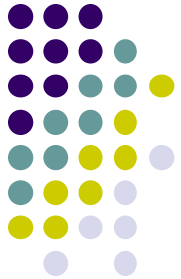


D_{24} is not a Boolean algebra



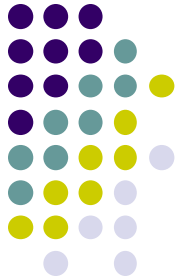
D_{30}

D_n as Boolean Algebra



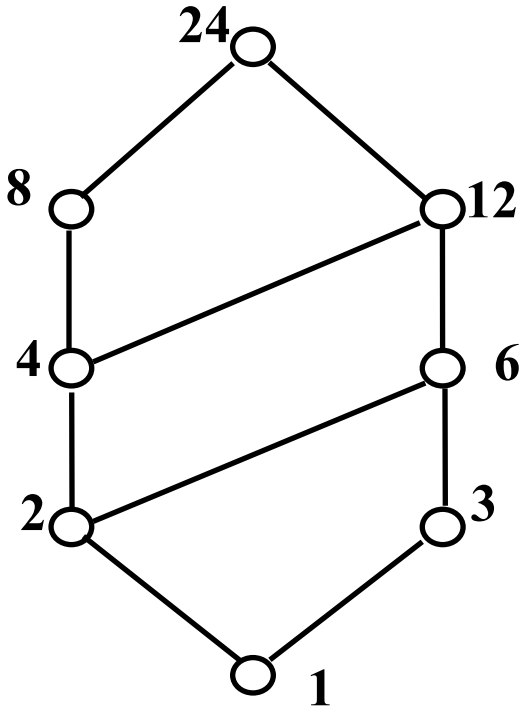
- Let $n=p_1p_2...p_k$, where the p_i are distinct primes. Then D_n is a Boolean algebra.
  - Let $S=\{p_1, p_2, ... p_k\}$, and for any subset T of S, a_T is the product of the primes in T.
  - Note: any divisor of n must be some a_T. And we have $a_T|n$ for any T.
  - For any subsets V,T, $V\subseteq T$ iff. $a_V|a_T$, *and* $a_V\wedge a_T=\text{GCD}(a_V, a_T)$ and $a_V\vee a_T=\text{LCM}(a_V, a_T)$.
  - f: $P(S)\rightarrow D_n$ given by $f(T)= a_T$ is an isomorphism from $P(S)$ to D_n.

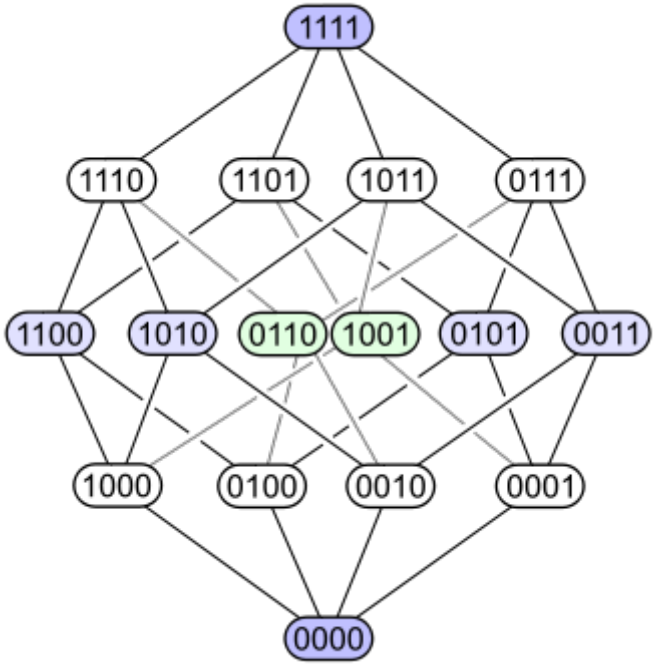
Proof of Non-Boolean Algebra



- If n is a positive integer and $p^2|n$, where p is a prime number, then D_n is not a Boolean algebra.
- Proof
  - Since $p^2|n$, $n= p^2q$ for some positive integer q. Note that p is also an element of D_n, then if D_n is a Boolean algebra, p must have a complement p', which means GCD(p, p')=1 and LCM(p, p')=n. So, $pp'=n$, which leads to $p'=pq$. So, GCD(p, pq)=1, contradiction.

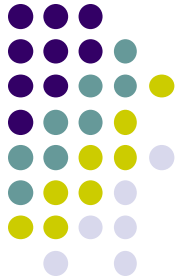
下列格是否构成布尔代数？





格、有界、有补、分配？

布尔代数的性质



- 结合律、交换律、分配律、同一律、补律
  - 蕴含：支配律、吸收律、幂等律、双重补律、德摩根律
- 证明支配律： $\forall x \in B, x \vee 1=1,\ x \wedge 0=0$
  - $x \vee 1= 1 \wedge (x \vee 1)= (x \vee \bar{x}) \wedge (x \vee 1)= x \vee (\bar{x} \wedge 1)= x \vee \bar{x}=1$
  - $x \wedge 0= 0 \vee (x \wedge 0) =(x \wedge \bar{x}) \vee (x \wedge 0)= x \wedge (\bar{x} \vee 0)= x \wedge \bar{x}=0$

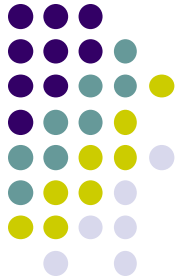
布尔代数的性质

- 证明吸收律
  - $x \vee (x \wedge y) = (x \wedge 1) \vee (x \wedge y) = x \wedge (1 \vee y) = x \wedge 1 = x$
  - $x \wedge (x \vee y) = (x \vee 0) \wedge (x \vee y) = x \vee (0 \wedge y) = x \vee 0 = x$
- 证明幂等律
  - $x \wedge x = x \wedge (x \vee 0) = x$ (应用同一律、吸收律)

吸收律 ⇨ 幂等律

$x \wedge x = x \wedge (x \vee (x \wedge x)) = x$ (两次应用吸收律)

布尔代数的性质

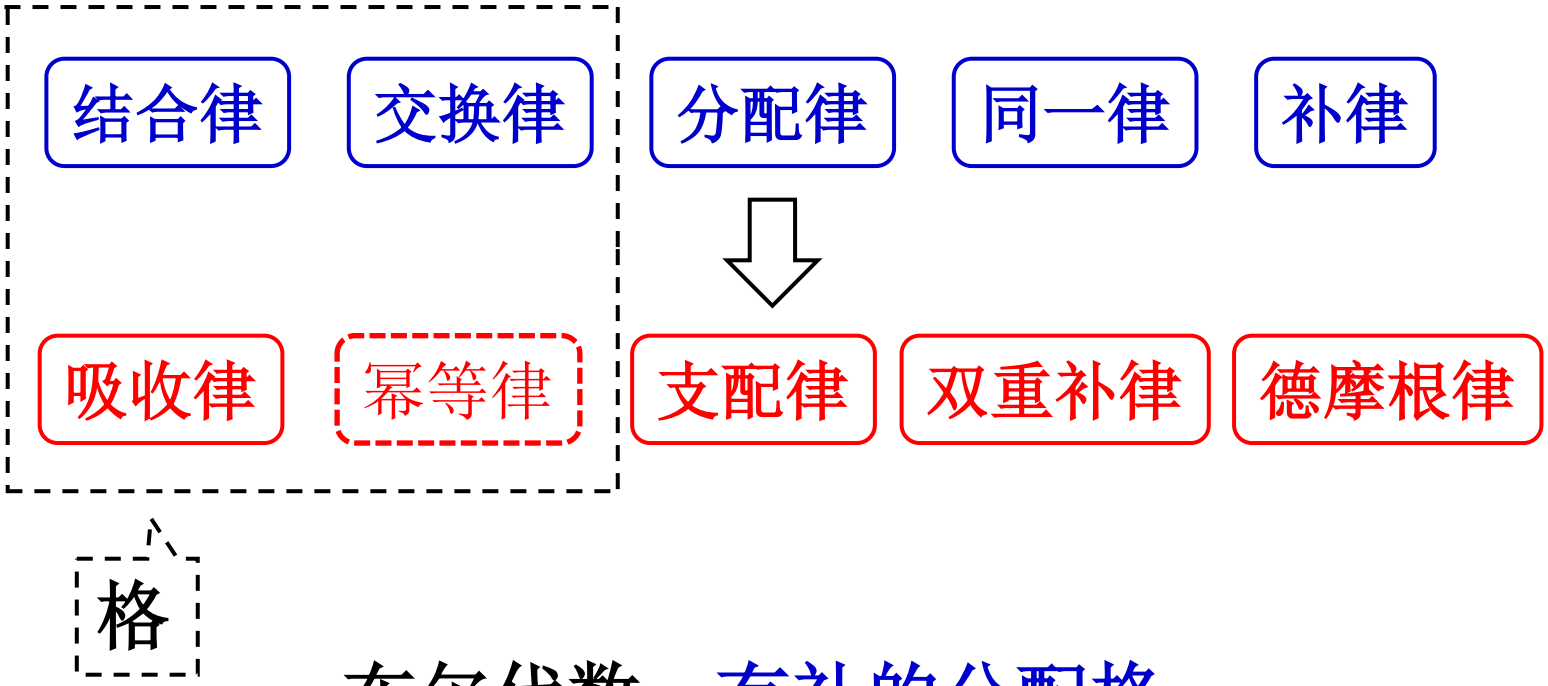


- 引理：$\forall x, y, z \in \mathbf{B}$, 若 $x \wedge z = y \wedge z$ 且 $x \vee z = y \vee z$ ， 则 $x = y$
  - $x = x \vee (x \wedge z) = x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ //吸收律/分配律
  - $y = y \vee (y \wedge z) = y \vee (x \wedge z) = (y \vee x) \wedge (y \vee z)$
- 证明双重补律
  - $x \vee \bar{x} = 1 = \bar{\bar{x}} \vee \bar{x}$
  - $x \wedge \bar{x} = 0 = \bar{\bar{x}} \wedge \bar{x}$
  - $x = \bar{\bar{x}}$

布尔代数的性质

- 证明德摩根律：$\forall x, y \in B, \overline{(x \wedge y)} = \overline{x} \vee \overline{y}$;
  - 根据补元的唯一性，只需证明$\overline{x} \vee \overline{y}$是$x \wedge y$的补元。
  - $(x \wedge y) \vee (\overline{x} \vee \overline{y}) = (x \vee \overline{x} \vee \overline{y}) \wedge (y \vee \overline{x} \vee \overline{y}) = 1$
  - $(x \wedge y) \wedge (\overline{x} \vee \overline{y}) = (x \wedge y \wedge \overline{x}) \vee (x \wedge y \wedge \overline{y}) = 0$

布尔代数的性质



布尔代数：有补的分配格

格中的原子

- 定义：设L是格，L中有最小元(全下界)0，给定元素$a\neq 0$, 若$\forall x\in L$, 有：

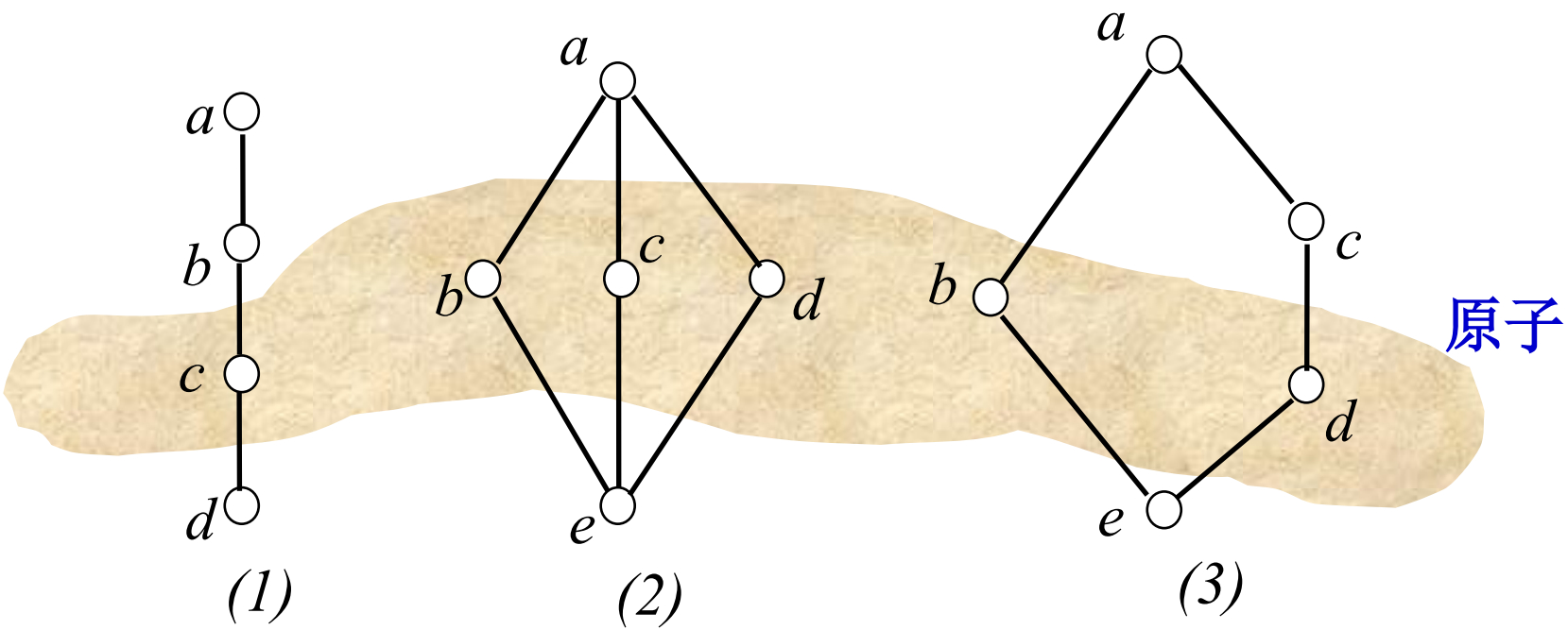
  $$0\prec x\preccurlyeq a \Rightarrow x=a$$

  则称a是L中的原子

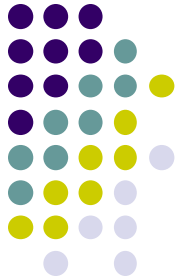
  （原子是覆盖最小元的那些元素。）

- 设a, b是格L中的原子，若$a\neq b$, 则$a\wedge b=0$
  - 假设$a\wedge b\neq 0$, 注意：$a\wedge b\preccurlyeq a$且$a\wedge b\preccurlyeq b$，由原子的定义：$a\wedge b=a$, $a\wedge b=b$, $\therefore a=b$, 矛盾。

格中的原子



有限布尔代数的表示定理

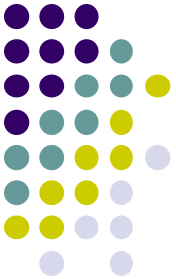


- 任一有限布尔代数B 同构于 B中所有的原子构成的集合A的幂集代数系统$P(A)$。

  即$(B, \wedge, \vee, ', 0, 1) \cong (P(A), \cap, \cup, \sim, \varnothing, A)$

- 备注（关于无限布尔代数）
  - 2^N，即无限的0/1序列$x_0, x_1, x_2, \ldots$
    - 这一无限布尔代数有原子
  - 2^N的一个子代数：周期序列（Periodic sequence）
    - 这个布尔代数没有原子

有限布尔代数基数是2的整数次幂



- 任何有限布尔代数的基数为2^n, n是自然数。
  - 设B是有限代数系统，A是B中所有原子的集合。

  则：$B \cong P(A)$, $\therefore |B| = |P(A)| = 2^{|A|}$
- 等势的有限布尔代数均同构

布尔函数

- 令B={0, 1}, $B^n=\{(x_1, \ldots, x_n) | x_i \in B, i=1, \ldots, n\}$, 从$B^n$到B的函数称为*n*元布尔函数， $f: B^n \to B$。
- 取值范围为B的变元称为布尔变元，$x \in B$。
- *n*元布尔函数的个数：$2\uparrow 2^n$ (2^2, 2^4, 2^8, …)
- 三种说法
  - *n*元布尔函数 $f: B^n \to B$
  - 有*n*个输入和一个输出的逻辑电路
  - 含*n*个命题变量的命题逻辑表达式

布尔函数上的运算

- 布尔和
  - $(f+g)(x_1, \ldots, x_n)= f(x_1, \ldots, x_n)+g(x_1, \ldots, x_n)$
- 布尔积
  - $(f \cdot g)(x_1, \ldots, x_n)=f(x_1, \ldots, x_n) \cdot g(x_1, \ldots, x_n)$
- 补函数
  - $\bar{f}(x_1, \ldots, x_n)=\overline{f(x_1, \ldots, x_n)}$

布尔代数

- ***n*元布尔函数全体也构成一个布尔代数**
  - 布尔和
  - 布尔积
  - 补函数
  - 全取0的函数、全取1的函数

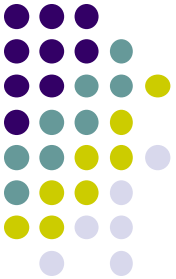
布尔恒等式（1）

等 式	名 称
$x+(y+z)=(x+y)+z$ $x\cdot(y\cdot z)=(x\cdot y)\cdot z$	结合律
$x+y=y+x$ $x\cdot y=y\cdot x$	交换律
$x+(y\cdot z)=(x+y)\cdot(x+z)$ $x\cdot(y+z)=x\cdot y+x\cdot z$	分配律
$x+0=x$ $x\cdot 1=x$	同一律
$x+\bar{x}=1$ $x\cdot\bar{x}=0$	补律

布尔恒等式（2）

等 式	名 称
$x+(x\cdot y)=x$ $x\cdot (x+y)=x$	吸收律
$x+x=x$ $x\cdot x=x$	幂等律
$x+1=1$ $x\cdot 0=0$	支配律
$\bar{\bar{x}}=x$	双重补律
$\overline{(x\cdot y)}=\bar{x}+\bar{y}$ $\overline{(x+y)}=\bar{x}\cdot\bar{y}$	德摩根律

布尔代数与数字逻辑电路设计



- 一个有n个输入、一个输出的逻辑电路对应于一个用含n个布尔变量的布尔代数表达式定义的布尔函数f：$B^n \rightarrow B$。
- 布尔函数的表达式：{和、积、补}是函数完全的。
- 用门电路元件（并、交、否）搭出所需的逻辑电路。
  - 电路极小化：卡诺图、奎因-莫可拉斯基

回顾：命题表达式的主析取范式

- 求 $(p \rightarrow q) \leftrightarrow r$ 的主析取范式
  - $(\neg p \wedge r) \vee (q \wedge r) \vee (p \wedge \neg q \wedge \neg r)$ （析取范式）

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

  - $(\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge q \wedge r) \vee (p \wedge \neg q \wedge \neg r)$
  - $(\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (p \wedge q \wedge r)$
  - 001　　011　　100　　111

一个逻辑电路设计的例子

- 举重比赛中三个裁判中两个或者两个以上判定为成功则该次成绩有效, 设计一个电子打分器, 输出一个结果: “成功”或”失败”。

定义一个布尔函数: $f(x,y,z)=1$ iff. x,y,z 至少有两个为1。

相应的布尔表达式:

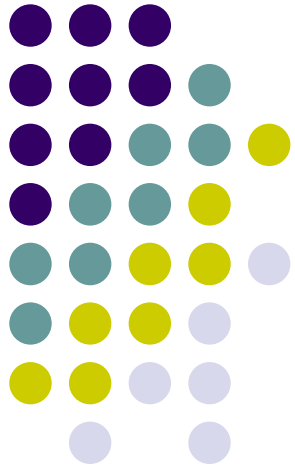
$(\bar{x}\wedge y\wedge z)\vee(x\wedge\bar{y}\wedge z)\vee(x\wedge y\wedge\bar{z})\vee(x\wedge y\wedge z)$

x	y	z	$f(x,y,z)$
0	0	0	0
0	0	1	0
0	1	0	0
1	0	0	0
0	1	1	1
1	0	1	1
1	1	0	1
1	1	1	1

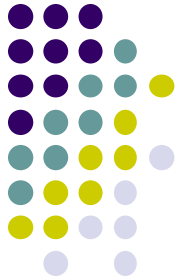
代数系统引论

瞿裕忠 教授

南京大学计算机科学与技术系



本讲内容

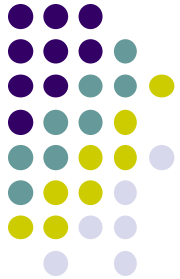


- 运算及其封闭性
- 代数系统
- 代数系统的性质
  - 结合性、交换性、分配性
  - 单位元、零元、逆元
- 代数系统的同构与同态

引 子

- 代数系统一般称为“抽象代数”（abstract algebra）或者“近世代数”（modern algebra），20世纪初被命名，但其研究的主要内容却肇始于19世纪。
- 代数系统研究的主要内容：代数结构、群、环、域、模、格、布尔代数、李代数 等

运算的函数定义



- 函数$f: A^n \to B$称为(从A到B的) n元运算。以下主要讨论二元运算
  - 例如：利用普通四则运算定义实数集上的一个新运算“$*$”：

$$x * y = x + y - xy$$

则：$2 * 3 = -1$；$0.5 * 0.7 = 0.85$

运 算 表

- 通常用于定义有限集合上的二元运算 (如在集合 $\{a, b, c, d\}$上定义如下的运算$*$)

*	a	b	c	d
a	1	®	✱	M
b	&	6	K	M
c	7	6	Q	0
d	G	#	~	◘

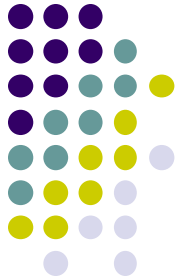
运算的封闭性

- 对于运算$f: A^n \to B$，若$B \subseteq A$，则称该运算在集合A上封闭（closeness）
- 例：
  - 加法在自然数集上封闭，但减法在自然数集上不封闭
  - 减法在整数集上封闭，但除法在整数集上不封闭
  - 对集合$A = \{1,2,3,\cdots,10\}$，gcd运算封闭，lcm则否

代数系统

- 定义（代数系统）：
  - 给定1个非空集合（其元素可以是任何对象）；
  - 给定1个或者若干个运算；
  - 给定的所有运算对上述集合封闭.
- 记法：$\langle S,\circ\rangle$，$\langle S,\wedge,\vee\rangle$，等等
- 例子：
  - 整数集与普通加法构成一个代数系统$\langle\mathbb{Z},+\rangle$

一个较复杂的代数系统的例子



- 设集合$S = \mathbb{R} - \{0,1\}$，定义S上的6个函数如下：
  - $f_1(x) = x$, $f_2(x) = (1-x)^{-1}$
  - $f_3(x) = x^{-1}(x-1)$, $f_4(x) = x^{-1}$
  - $f_5(x) = x(x-1)^{-1}$, $f_6(x) = 1-x$
- 则$\langle\{f_1, f_2, f_3, f_4, f_5, f_6\}, \circ\rangle$是代数系统，其中$\circ$是函数的复合运算

只需考虑运算的封闭性。例如：$f_2 \circ f_3 = f_1$, $f_4 \circ f_5 = f_2$, $f_3 \circ f_6 = f_4$等（注：上例采用复合左先制，即$f \circ g(x) = g(f(x))$，易验证右先制依然满足封闭性）

函数本身作为运算对象

- 在集合 $S = \mathbb{R} - \{0,1\}$上定义函数如下：
  - $f_1(x) = x,$ $f_2(x) = (1-x)^{-1}$
  - $f_3(x) = x^{-1}(x-1),$ $f_4(x) = x^{-1}$
  - $f_5(x) = x(x-1)^{-1},$ $f_6(x) = 1-x$
- 要明$f_4 \circ f_5 = f_2$，$\forall x \in S, f_5(f_4(x)) = f_2(x)$

$$f_5(f_4(x)) = f_5\left(\frac{1}{x}\right) = \left(\frac{1}{x}\right)\left(\frac{1}{x}-1\right)^{-1} = \left(\frac{1}{x}\right)\left(\frac{x}{1-x}\right) = \left(\frac{1}{1-x}\right)$$

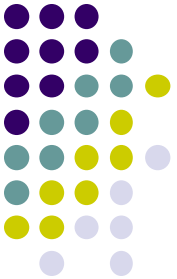
结合性（associativity）

- 集合A上的运算$\circ$具有结合性定义为：

$$\forall x, y, z \in A, (x \circ y) \circ z = x \circ (y \circ z)$$

- 如果$\circ$满足结合性，表达式$x_1 \circ x_2 \circ \cdots \circ x_n$可以在保持诸$x_i$先后次序不变的前提下按照任何顺序进行计算

交换性（commutativity）



- 集合A上的运算$\circ$具有交换性定义为：

$$\forall x, y \in A, x \circ y = y \circ x$$

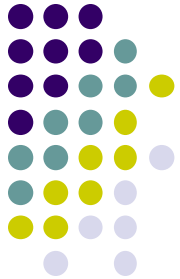
- 如果$\circ$同时满足交换律和结合律，表达式$x_1 \circ x_2 \circ \cdots \circ x_n$可以按照任何顺序进行计算，包括可以随便重新排列诸$x_i$的先后次序

分配性（distributivity）

- 分配性涉及两个不同的运算
- 集合A上的运算$\circ$对$*$满足分配性定义为：

$$\forall x, y, z \in A, x \circ (y * z) = (x \circ y) * (x \circ z)$$

单位元（identity element）



- 对于实数集$\mathbb{R}$上的普通乘法$(\cdot)$，实数1满足对任意实数$x \in \mathbb{R}$，有$1 \cdot x = x \cdot 1$
- 元素e是代数系统$\langle S, \circ \rangle$的单位元当且仅当

$$\forall x \in S, e \circ x = x \circ e = x$$

- 单位元可记为$\mathbf{1}_S$，或简记为$\mathbf{1}$（读作幺）
- 代数系统不一定有单位元

左单位元和右单位元

- e_L称为系统的左单位元(或左幺)当且仅当

$$\forall x \in S, e_L \circ x = x$$

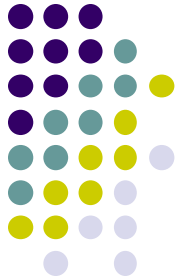
- 可以相应地定义系统的右单位元(右幺) e_R

$$\forall y \in S, y \circ e_R = y$$

*	a	b	c	d
a	a	b	c	d
b	a	b	c	d
c	a	b	c	d
d	a	b	c	d

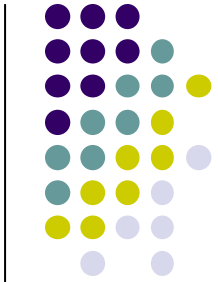
*	a	b	c	d
a	a	d	c	a
b	b	d	c	b
c	c	d	c	c
d	d	d	b	d

关于单位元的进一步讨论



- 左、右单位元不一定存在
- 左、右单位元不一定唯一
- 假设一个代数系统同时有左、右单位元，则左、右单位元必相等且唯一；即系统的单位元（幺元）
  - $e_L = e_L \circ e_R = e_R$
- 系统若有单位元，必是唯一的
  - $e_1 = e_1 \circ e_2 = e_2$

逆元（inverse element）



- 这里，只对存在单位元的代数系统讨论逆元
- 给定系统S中的元素x，若存在S中的元素x'，满足$x' \circ x = \mathbf{1}_S$，则称$x'$是$x$的左逆元；若存在$x''$，满足$x \circ x'' = \mathbf{1}_S$，则称$x''$是$x$的右逆元
- 给定系统S中的元素x，如果存在S中的元素x^*，满足$x \circ x^* = x^* \circ x = \mathbf{1}_S$，则称$x^*$是$x$的逆元，一般记为$x^{-1}$
  - 逆元既是左逆元，又是右逆元
  - 如果y是x的逆元，则x也是y的逆元

一个关于逆元的例子

*	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	a	c	a
d	d	b	c	d

- 注意

(1) b的左、右逆不同；

(2) c有2个右逆，无左逆；

(3) d有左逆，无右逆

关于逆元的进一步讨论

- 如果代数系统$\langle S,\circ\rangle$具有结合性：
  - 若给定的元素既有左逆，又有右逆，二者必相等且唯一
    - 设S中给定的元素x的左逆是x'，右逆是x''：

$$x' = x' \circ \mathbf{1}_S = x' \circ (x \circ x'') = (x' \circ x) \circ x'' = \mathbf{1}_S \circ x'' = x''$$

  - 若每个元素均有左逆，则左逆即右逆，且逆元唯一
    - 任给S中元素a，设a的左逆是b，b的左逆是c，则

$$a \circ b = (\mathbf{1}_S \circ a) \circ b = \big((c \circ b) \circ a\big) \circ b$$

$$= \big(c \circ (b \circ a)\big) \circ b = (c \circ \mathbf{1}_S) \circ b = c \circ b = \mathbf{1}_S$$

零 元

- 对于实数集上的普通乘法，实数0满足对任意实数x，

  $0 \cdot x = x \cdot 0 = 0$

- 元素t是代数系统$\langle S, \circ \rangle$的零元当且仅当

  $$\forall x \in S, t \circ x = x \circ t = t$$

- 零元可记为$\mathbf{0}_S$，或简记为$\mathbf{0}$

- 一个代数系统不一定存在零元

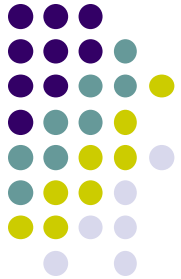
一个例子

- 定义实数集上的二元运算“$\circ$”如下：

$$\forall x, y \in \mathbb{R}, x \circ y = x + y - xy$$

  - 交换性：显然
  - 结合性：$(x \circ y) \circ z = x \circ (y \circ z) = x + y + z - xy - xz - yz + xyz$
  - 单位元：0；零元：1
  - $x\ (x \neq 1)$ 的逆元为：$\frac{x}{x-1}$，1无逆元

一个与编码有关的代数系统



- 设字母表$A=\{0,1\}$，A^*是A上的长度为n的字符串的集合
- 定义A^*上的运算$\oplus$如下：

  $\forall x,y\in A^*$，$x\oplus y$是长度为n的二进数字串，第i位$(i=0,1,\cdots,n-1)$为1当且仅当x,y的相应位互异
- $\langle A^*,\oplus\rangle$是代数系统
- 该系统满足：交换性、结合性、有单位元、每个元素均有逆元

“相似”的系统

- 比较$\langle\{F,T\},\vee\rangle$（逻辑或）与$\langle\{0,1\},+\rangle$（布尔和）两代数系统：

$\vee$	F	T
F	F	T
T	T	T

$+$	0	1
0	0	1
1	1	1

- 若不考虑符号的形式及其含义，则两系统的“本质”没有差别

同构与同构映射

- 代数系统$\langle S_1,\circ\rangle$与$\langle S_2,*\rangle$同构（isomorphism）(记$S_1 \cong S_2$) 当且仅当存在双射函数$f: S_1 \to S_2$，满足：$\forall x,y \in S_1, f(x \circ y) = f(x) * f(y)$。其中的双射函数$f$称作同构映射

- 同构关系是等价关系

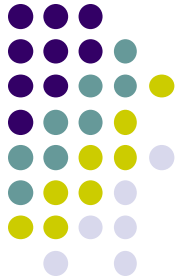
同态与同态映射

- 代数系统$\langle S_1, \circ \rangle$与$\langle S_2, * \rangle$同态（homomorphism，记$S_1 \sim S_2$）当且仅当 存在函数$f: S_1 \to S_2$，满足：

$$\forall x, y \in S_1, f(x \circ y) = f(x) * f(y)$$

- 若上述f是满射，则称两系统满同态(epimorphism)
- 例：整数加系统$\langle \mathbb{Z}, + \rangle \sim \langle \mathbb{Z}_3, \oplus_3 \rangle$（模3剩余加系统）
  - 同态映射：$f: \mathbb{Z} \to \mathbb{Z}_3: f(x) = [x]_3$

练习题



- 设代数系统$\boldsymbol{Z}_n = \langle \mathbb{Z}_n, \oplus_n \rangle$，$\oplus_n$为模$n$剩余加，$f: \mathbb{Z}_{12} \to \mathbb{Z}_3$，$f([x]_{12}) = [x \bmod 3]_3$.证明：$f$是满同态

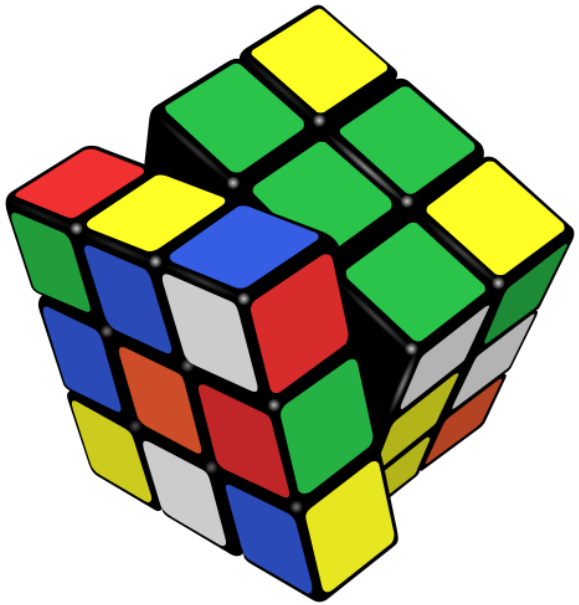
群论导引

离散数学—代数结构

南京大学计算机科学与技术系

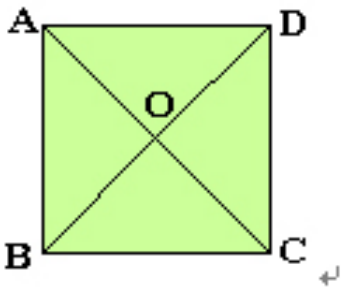
内容提要

- 引言
- 半群
- 么半群
- 群
- 群的性质
- 群的术语
- 群方程*

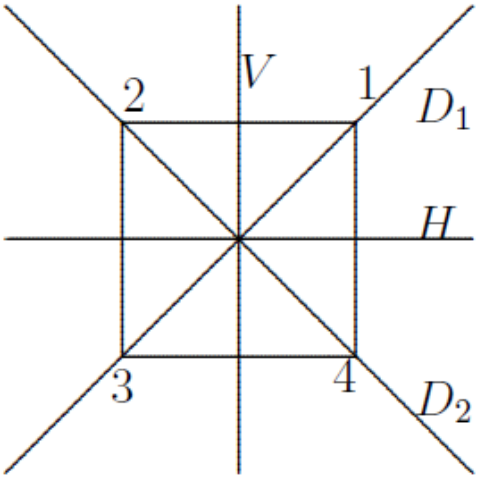


引言：对称变换

- 正方形的刚体运动是从四个顶点集到它本身的一一对应（变换），保持相邻点之间距离不变



引言：对称变换（续）



设正方形的4个顶点为1、2、3、4；重心为O，对角线为D_1和D_2，水平中线为H，垂直中线为V。以下将从$\{1,2,3,4\}$到$\{1,2,3,4\}$的一一对应记成$\begin{pmatrix} 1 & 2 & 3 & 4 \\ i_1 & i_2 & i_3 & i_4 \end{pmatrix}$.

我们现在找出正方形所有的对称

引言：对称变换（续）

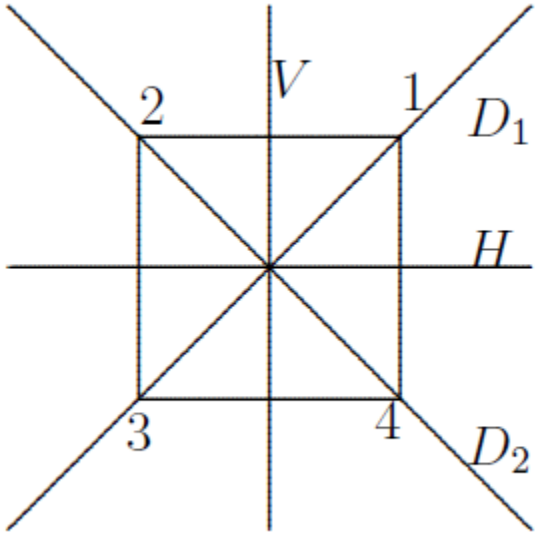
旋转对称：由以下刚体运动完成

R_1：绕O顺时针转$90°$，易见$R_1 = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 4\ 1\ 2\ 3 \end{pmatrix}$

R_2：绕O顺时针转$180°$，易见$R_2 = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 3\ 4\ 1\ 2 \end{pmatrix}$

R_3：绕O顺时针转$270°$，易见$R_3 = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 2\ 3\ 4\ 1 \end{pmatrix}$

R_0：绕O顺时针转$360°$，易见$R_0 = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 1\ 2\ 3\ 4 \end{pmatrix}$

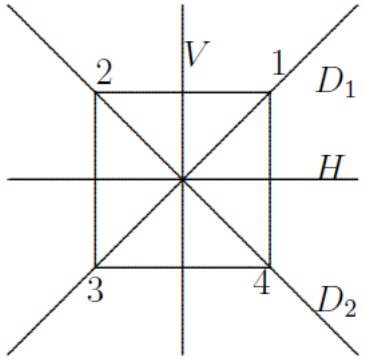


引言：对称变换（续）

反射对称：由以下刚体运动完成

H：对于水平中线H的反射。D_1：对于对角线D_1的反射。

V：对于垂直中线V的反射。D_2：对于对角线D_2的反射。

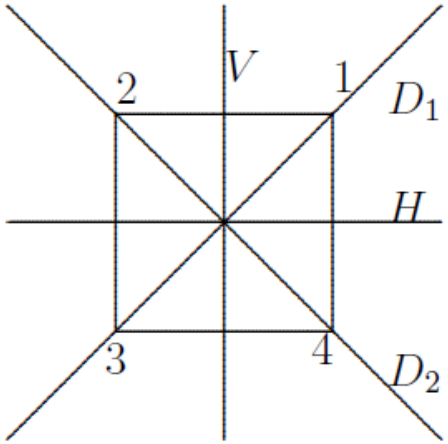


$$H = \begin{pmatrix} 1\,2\,3\,4 \\ 4\,3\,2\,1 \end{pmatrix} \quad V = \begin{pmatrix} 1\,2\,3\,4 \\ 2\,1\,4\,3 \end{pmatrix} \quad D_1 = \begin{pmatrix} 1\,2\,3\,4 \\ 1\,4\,3\,2 \end{pmatrix} \quad D_2 = \begin{pmatrix} 1\,2\,3\,4 \\ 3\,2\,1\,4 \end{pmatrix}$$

引言：对称变换（续）

- 两个对称变换的连续作用依然是对称变换

- 例如：$R_1 * H$指先右转$90°$，后做水平反射，结果得D_1，故$R_1 * H = D_1$；而$H * R_1 = D_2$；由此可以看出$R_1 * H \neq H * R_1$



引言：对称变换（续）

Cayley Table

故R_0是单位元

·	R_0	R_{90}	R_{180}	R_{270}	V	H	D_1	D_2
R_0	R_0	R_{90}	R_{180}	R_{270}	V	H	D_1	D_2
R_{90}	R_{90}	R_{180}	R_{270}	R_0	D_2	D_1	V	H
R_{180}	R_{180}	R_{270}	R_0	R_{90}	H	V	D_2	D_1
R_{270}	R_{270}	R_0	R_{90}	R_{180}	D_1	D_2	H	V
V	V	D_1	H	D_2	R_0	R_{180}	R_{90}	R_{270}
H	H	D_2	V	D_1	R_{180}	R_0	R_{270}	R_{90}
D_1	D_1	H	D_2	V	R_{270}	R_{90}	R_0	R_{180}
D_2	D_2	V	D_1	H	R_{90}	R_{270}	R_{180}	R_0

引言：对称变换（续）

令$S=\{R_0,\ R_1,\ R_2,\ R_3,\ V,\ H,\ D_1,\ D_2\}$

$*$为S上的两元运算

事实上可通过函数的复合来计算积。例如

$(1\to4)*(4\to1)\Rightarrow 1\to1$

$$R_1 * H = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & & & \\ 4 & 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ & & & \downarrow \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & & & \\ 1 & 4 & 3 & 2 \end{pmatrix} = D_1$$

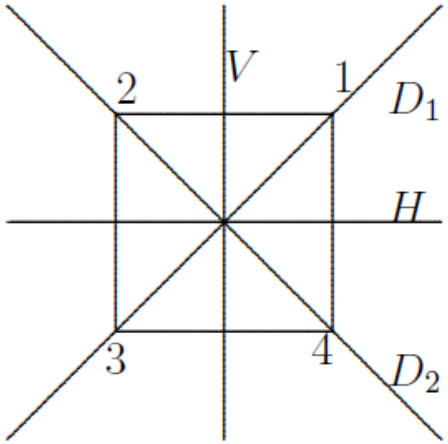
通过运算可知

(1) $*$对于S是封闭的，即$(\forall x,\ y \in S)(x * y \in S)$ 封闭

(2) $(\forall x,\ y,\ z \in S)(x*(y*z)=(x*y)*z)$ 结合律

(3) $(\forall x \in S)(R_0 * x = x * R_0 = x)$ 单位元

(4) $(\forall x \in S)(\exists y \in S)(x * y = y * x = R_0)$ 逆元



群 论

Je n'ai pas le temps.

——Evariste Galois

半 群

定义 设$(S, *)$为代数系统，$(S, *)$为半群（Semigroup）指

(1) $(\forall x, y \in S)(x * y \in S)$ 封闭的

(2) $(\forall x, y, z \in S)((x * y) * z = x * (y * z))$ 结合律

若$(\forall x, y \in S)(x * y = y * x)$(对称) 交换律 则称$(S, x)$为交换半群（abelian半群）

- “代数系统”+“结合性”=“半群”
- 例：代数系统$\langle\{1,2\},*\rangle$为半群，其中$*$定义为

$\forall x, y \in \{1,2\}, x * y = y$

幺半群（Monoid）

定义 设$(S, *)$为代数系统，$(S, *)$为Monoid（Semigroup with unit）指

(1) $(\forall x, y \in S)(x * y \in S)$

(2) $(\forall x, y, z \in S)((x * y) * z = x * (y * z))$

(3) $(\exists e \in S)(\forall x \in S)(e * x = x * e = x)$

- “半群”+“单位元”=“Monoid”
- 注意：代数系统中左右单位元若存在则必相等且唯一

幺半群（续）

- 例1：$S=\left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} | a,b \in \mathbb{R}\right\}$，$T=\left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} | a \in \mathbb{R}\right\}$

  则集合S与T关于矩阵的乘法皆构成Monoid

- 例2：$\langle \mathbb{Z}^+, + \rangle$为半群，但非Monoid "0"

- 例3：$\langle \mathbb{Z}_n, \oplus_n \rangle$为Monoid，$\oplus_n$是模$n$加法 "0"

- 例4：$\langle A^A, \circ \rangle$ 为Monoid，$\circ$是函数复合运算 恒等函数

- 例5：$\langle \mathcal{P}(B), \oplus \rangle$为Monoid，$\oplus$为对称差运算 "$\phi$"

群（Group）

- $(G,*)$为群当且仅当有$e \in G$和G上的一元运算$^{-1}$使

(0) $G \neq \emptyset$

(1) $(\forall x, y \in G)(x * y \in G)$ ……代数系统 封闭性

(2) $(\forall x, y, z \in G)(x * (y * z) = (x * y) * z)$ …半群 结合律

(3) $(\forall x \in G)(x * e = e * x = x)$ …… 幺半群 单位元

(4) $(\forall x \in G)(x * x^{-1} = x^{-1} * x = e)$ ……群 逆元

(1) ~(4)有时被称为群论公理

群（续）

- 群的等价描述：
- 设G为非空集合，$*$为G上的二元运算，$\langle G,* \rangle$为群指$\langle G,* \rangle$为Monoid，其单位元为e，且满足：

$$(\forall x \in G)(\exists y \in G)(x * y = y * x = e)$$

- 注意：可结合的代数系统中逆元若存在则唯一

群（续）

命题 设$\langle G, *, e\rangle$为群，任何元素之逆是唯一的。

证：设y，z为x之逆，从而

$$x * y = y * x = e = x * z = z * x$$

$$\because x * y = e \longrightarrow z * (x * y) = z * e$$

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

$$\longrightarrow e * y = z$$

$$\longrightarrow y = z$$

$$\therefore y = z \quad \square$$

群（续）

- 示例
  - $\langle \mathbb{R}, + \rangle, \langle \mathbb{Z}, + \rangle$为群，但$\langle \mathbb{N}, + \rangle$不为群（1无逆） 单位元 0.
  - $\langle \mathbb{R}\text{-}\{0\}, * \rangle$，非零实数乘法群；$a$的逆元素为$1/a$ 单位元 1. 逆元：相反数
  - $\langle \mathbb{Z}_n, \oplus_n \rangle$为群，$i$之逆为$n - i$ 单位元 0.
  - 正方形的对称变换集与乘积构成群
  - $T_A = \{f : A \to A | f\text{为双射}\}$，单位元$I_A$，$f$的逆元$f^{-1}$
  - $A = \{f : \mathbb{R} \to \mathbb{R} | \text{呈形} f(x) = ax + b\}$，$\langle A, \circ \rangle$是群？

单位元 $\begin{cases} f(x)=b & a=1 \\ f(x)=\dfrac{b}{1-a} \end{cases}$

群（续）

设$f(x)=ax+b\ (a,\ b\in\mathbb{R})\ f\in A$ f有逆吗?

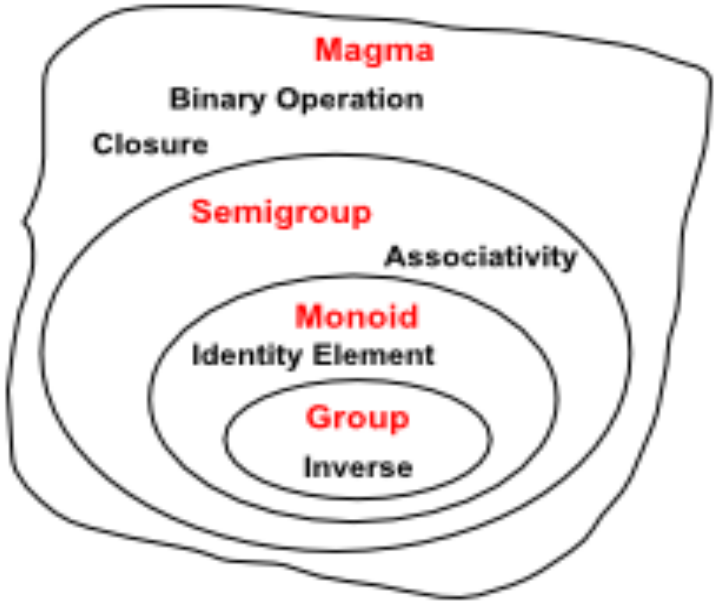
设$g(x)=cx+d\ (c,\ d\in\mathbb{R})$为$f$之逆，从而$f(g(x))=g(f(x))=x$。

因此，$a(cx+d)+b=x$，$c(ax+b)+d=x$；$acx+ad+b=x$，$acx+cb+d=x$；$ac=1$，$ad+b=cb+d=0$；$c=1/a$，$d=-b/a$。

故当$a=0$时f无逆，当$a\neq 0$时f的逆为$g(x)=x/a-b/a$。

然而令$A'=\{f:\mathbb{R}\to\mathbb{R}|f$呈形$f(x)=ax+b$且$a\neq 0\}$，$(A',\circ)$为群。

群（续）


Magma
Binary Operation
Closure
Semigroup
Associativity
Monoid
Identity Element
Group
Inverse

群的性质

定理 设$(G, *, e, ^{-1})$为群

(1) $(a^{-1})^{-1} = a$

(2) $(ab)^{-1} = b^{-1}a^{-1}$

(3) $ab = ac \rightarrow b = c$（左消去律）

(4) $ba = ca \rightarrow b = c$（右消去律）

(5) 方程$ax = b$和$ya = b$在G中对x，y有唯一解

有限群的运算表中每行（列）均为群中所有元素的一种排列，不同行（列）不可能出现同样的排列。

群的术语：元素的乘幂（次方）

- 定义

  $a^0 = e$ （e是单位元素）

  $a^{n+1} = a^n \circ a$ (n是非负整数)

  $a^{-k} = (a^{-1})^k$ (k为正整数)

- 性质

  $a^n \circ a^m = a^{n+m}$

  $(a^n)^m = a^{nm}$

群的术语：元素的阶

- 设G是群，$a \in G$， a的阶（周期）定义如下：
  - $|a| = \min\{k \in \mathbb{Z}^+ \mid a^k = e\}$
  - 如果这样的k不存在，a为无限阶元
- 性质
  - 有限群不存在无限阶元
  - 群中元素及其逆元具有相同的阶
  - 有限群中阶大于2的元素有偶数个
  - 偶数群中阶为2的元素有奇数个 $(a = a^{-1})$

群的术语：群的阶

(1) 若G为有穷集，则称$(G,*)$为有限群。当$|G|=n$时称$(G,*)$之阶为n且称G为n阶群

(2) 若G为无穷集，则称$(G,*)$为无限群

(3) 若群$(G,*)$满足$(\forall x,y\in G)(xy=yx)$，则称$G$为交换群(abelian群)

下面我们给出1，2，3，4阶全部不同构的群

(1) 若$(G,*)$为1阶群，从而设$G=\{e\}$有$ee=e$。故1阶群在同构意义下只有一个。

(2) 若$(G,*)$为2阶群，从而设$G=\{e,a\}(a\neq e)$，易见$ea=ae=a$，$ee=e$但aa呢？

若$aa=a$则$a=e$矛盾，故$aa=e$。故2阶群在同构意义下只有一个。

乘法表见下:

$*$	e	a
e	e	a
a	a	e

有关群的术语（续）

(3) 若$\langle G,*\rangle$为3阶群，从而可设$G=\{e,a,b\}$，e,a,b互异。若$a*a=e$,则$a*b=b$, 矛盾，故$a*a=b$。运算表唯一。因此，3阶群在同构意义下只有一个。

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

有关群的术语（续）

- **证明：**四阶群皆为Abel群

证：设$G=\{e,a,b,c\}$，e为幺。现证$ab=ba$

情况1. $ab=e$从而ba只能为e或c，若$ba=c$则$aba=ac$，从而$ea=ac$，从而$c=e$矛盾，故$ba=e$。

情况2. $ab=c$，同理$ba=c$

同理$bc=cb$，$ac=ca$。 □

- **证明：**四阶群中元素的阶为1、2或者4（不为3）.

或 $a^3=e$. 有 $a^2\cdot a=e \Rightarrow a^{-1}=a^2$

假设有个元素*a*的阶为3，$\{e, a, a^2, b\}$, ab=?（矛盾）

要么 $ab=e \Rightarrow a^3b=a^2 \Rightarrow b=a$ (矛盾)

要么 $ab=a^2 \Rightarrow b=a$ (矛盾)

有关群的术语（续）

(4) 只有两种四阶群

- 有个元素的阶为**4**：

  $\{e, a, a^2, a^3\}$

  模4的加法群

  与$\langle \mathbb{Z}_4, \oplus_4 \rangle$同构

- 元素的阶均不为**4**：

  Klein四元群

$*$	e	a	ba^2	ca^3
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

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

全为二阶

群方程*

封闭性 结合律,

定理 若代数系统$(G,*)$为半群且在G中方程$ax=b$与$ya=b$有唯一解，则$(G,*)$为群 单位元、逆元.

证：第一步 证明有左幺$e_l \in G$使$(\forall a \in G)(e_l a = a)$

取定$b \in G$，$xb=b$有唯一解，设为e_l。对任何$a \in G$下证$e_l a = a$。

$\because bx=a$有解c，$\therefore e_l a = e_l(bc) = (e_l b)c = bc = a$

第二步 证明$(\forall a \in G)(\exists a^{-1} \in G)(a^{-1}a = e_l)$即左逆存在

令a^{-1}为$ya=e_l$的唯一解即可

第三步 证明$aa^{-1}=e_l$即左逆=右逆

$\because a^{-1} \in G \quad \therefore ya^{-1}=e_l$有唯一解$a'$，从而$a'a^{-1}=e_l$从而

$aa^{-1}=e_l(aa^{-1}) = (a'a^{-1})(aa^{-1}) = a'(a^{-1}a)a^{-1} = a'e_l a^{-1} = a'a^{-1} = e_l$

第四步 $(\forall a \in G)(ae_l = a)$ 即左幺=右幺

$\because ae_l = a(a^{-1}a) = (aa^{-1})a = e_l a = a \quad \therefore ae_l = a$

因此$(G,*,e,^{-1})$为群 □

群的方程定义*

- 群有以下二种等价的定义：
- (1) 若$\langle G,*\rangle$为半群且方程$ax=b$与$ya=b$有唯一解，则称$\langle G,*\rangle$为群
- (2) 若$\langle G,*\rangle$为半群，存在左单位元，且每个元素都具有左逆元，则$\langle G,*\rangle$称为群

群的方程定义*（续）

对于半群$\langle G,*\rangle$，设e_l为其左幺元（题设），对任意$a \in G$，a_l为其左逆元（题设），故~~$a * a_l = e_l$~~，因为$a_l \in G$，故对于a_l，$\exists a^{-1} \in G$，使得$a^{-1} * a_l = e_l$，则立即有：$a * a_l = e_l * (a * a_l) = (a^{-1} * a_l) * (a * a_l) = a^{-1} * (a_l * a) * a_l = a^{-1} e_l a_l = a^{-1} a_l = e_l$. 故左逆元=右逆元；

下证e_l即为右幺：$\forall a \in G$，$a * e_l = a * (a_l * a) = (a * a_l) * a = e_l * a = a$，故$e_l$即为系统的幺元，$\forall a \in G$，$a_l$为$a$之逆. 综上，$\langle G,*\rangle$即为群.

群的方程定义*（续）

推论 设$(G,*)$为半群且$|G|$有穷，若$(G,*)$满足消去律，则$(G,*)$为群

证：设$G=\{a_1,\cdots,a_n\}$，$\forall a,b\in G$下证明方程$ax=b$有唯一解，令$aG=\{aa_i|i=1,2,\cdots,n\}$

$\because$ 左消去律 $\therefore |aG|=n$从而$aG=G$而$b\in G$故有$a_i\in G$使$aa_i=b$从而$ax=b$有解，

又$\because$ 左消去律 $\therefore$解唯一。同理可证$ya=b$有唯一解。因此$(G,*)$为群。 □

有穷代数系统若满足结合律和消去律，则必为群。

$\langle\mathbb{Z}^+,*\rangle$（普通乘法）满足结合律和消去律，但不是群 单位元1 逆元不存在

Niels Abel (1802-1829):天才与贫困

阿贝尔的第一个抱负不凡的冒险，是试图解决一般的五次方程。…失败给了他一个非常有益的打击；它把他推上了正确的途径，使他怀疑一个代数解是否是可能的。1824年，他发表了《一元五次方程没有代数一般解》的论文。

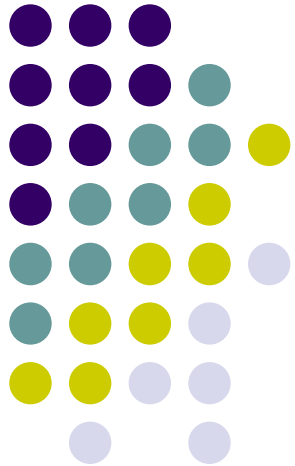
阿贝尔的《关于非常广泛的一类超越函数的一般性质的论文》呈交给巴黎科学院。这就是勒让德后来用贺拉斯的话描述为“永恒的纪念碑”的工作，埃尔米特说：“他给数学家们留下了够他们忙上五百年的东西。”它是现代数学的一项登峰造极的成就。(摘自贝尔：《数学精英》)

这篇论文的一个评阅人勒让德74岁，发现这篇论文很难辨认，而另一位评阅人，39岁的柯西正处于自我中心的顶峰，把论文带回家，不知放在何处，完全忘了。4年后，当柯西终于将它翻出来时，阿贝尔已经不在人世。作为补偿，科学院让阿贝尔和雅可比一起获得1830年的数学大奖。

子群与拉格朗日定理

离散数学—代数结构

南京大学计算机科学与技术系



子群与拉格朗日定理

- 子群的定义及其判定
- 生成子群与元素的阶
- 子群的陪集与划分
- 拉格朗日定理
- 拉格朗日定理的推论

子群的定义

- 设(G, ∘)是群，H是G的非空子集，如果H关于G中的运算构成群，即(H, ∘)也是群，则H是G的子群。
  - 记作(H, ∘) ≤ (G, ∘), 简记为 H≤G。
- 例子：偶数加系统是整数加群的子群
- 平凡子群 单位元构成 / 原来的群

注意：结合律在G的子集上均成立。

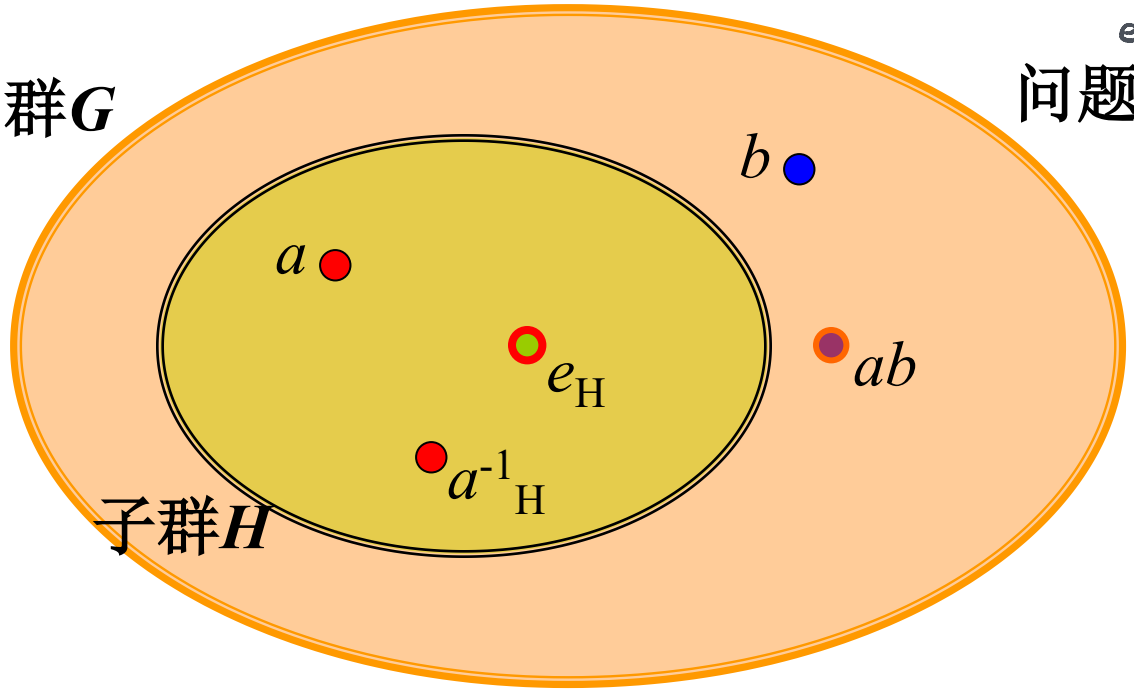
关于子群定义的进一步思考

问题1：e_H是否一定是e_G?

$e_H e_H = e_H \rightarrow e_H = e_G$

$e_H = e_H \cdot e_G$

$e_H \cdot e_H = e_H \cdot e_H \cdot e_G = e_H \cdot e_G \Rightarrow e_H = e_G$



问题2：*ab*应该在哪儿？

$a^{-1}ab \in H$

$b \in H$

子群的判定 – 判定定理一

- G是群，H是G的非空子集。H是G的子群当且仅当：
  - $\forall a,b \in H, ab \in H$, 并且
  - $\forall a \in H, a^{-1} \in H$

（注意：这里a^{-1}是a在G中的逆元，当H确定为群后，它也是a在H中的逆元）

- 证明
  - 必要性显然（注意群中逆元素的唯一性）
  - 充分性：只须证明G中的单位元也一定在H中，它即是H的单位元素。

子群的判定 – 判定定理二

- **G是群，H是G的非空子集。H是G的子群当且仅当：**

  $\forall a,b \in H,\ ab^{-1} \in H$

- 证明
  - 必要性易见
  - 充分性：
    - 单位元素：因为H非空，任取$a \in H$, $e=aa^{-1} \in H$
    - 逆元素： $\forall a \in H$, 因为$e \in H$, 所以 $a^{-1}=ea^{-1} \in H$
    - 封闭性： $\forall a,b \in H$, 已证$b^{-1} \in H$，所以$ab=a(b^{-1})^{-1} \in H$

子群的判定 – 有限子群

- G是群，H是G的非空有限子集。H是G的子群当且仅当：

  $\forall a,b\in H,\ ab\in H$

- 证明. 必要性显然. 下证充分性。

  只须证明， $\forall b\in H,\ b^{-1}\in H$

  - 若H中只含G的单位元，H显然是子群。
  - 否则，任取H中异于单位元的元素b, 考虑序列

    $$b,\ b^2,\ b^3,\ \ldots$$

    注意：该序列中各项均为有限集合H中的元素，因此，必有正整数i, j(j>i), 满足：$b^i=b^j$, 因此：

    $$b^{-1}=b^{j-i-1}\in H$$

生成子群

- 设G是群，$a \in G$，构造G的子集H如下：

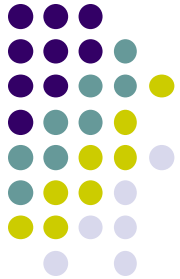
$$H = \{a^k \mid k\text{是整数}\}$$

则H构成G的子群，称为a生成的子群$\langle a \rangle$

- 证明：
  - H非空：a在H中
  - 利用判定定理二：

$$\forall a^m, a^n \in H,\ a^m (a^n)^{-1} = a^{m-n} \in H,$$

群中元素的阶



- **定义（元素的阶）**

设$(G, *)$为群，$n \in Z$, $a \in G$，以下定义a^n:

若$n \geq 0$，则a^n已在上讲定义。

若$n < 0$，则$a^n = (a^{-n})^{-1}$。

若$(\exists n \in \mathbb{N}^+)(a^n = e)$，则称$a$的阶(order)是有穷的且记$a$的阶$| a | = min\{n > 0 | a^n = e\}$。

若$\neg (\exists n \in \mathbb{N}^+)(a^n = e)$，则称$a$的阶是无穷的，且记$a$的阶$| a | = \infty$。

性质:

$a^m a^n = a^{m+n}$

$(a^n)^m = a^{nm}$

群中元素的阶（续）

- 例：Kleine 四元群，非单位元的阶均为2.

在Kleine 4群$(V, *)$中，$|e|=1$，当$a \neq e$时，$|a|=2$。

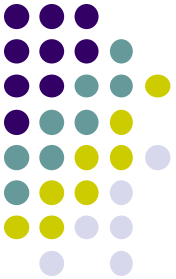
在$(\mathbb{Z}_7, +_7)$中，$|0|=1$，$a \neq 0$，$|a|=7$。

在$(\mathbb{Z}_6, +_6)$中，$|0|=1$

元素	0	1	2	3	4	5
阶	1	6	3	2	3	6

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

群中元素的阶（续）



- 定理（元素的阶的性质）

设$(G, *)$, $a, b \in G$, $|a|$, $|b|$为有穷

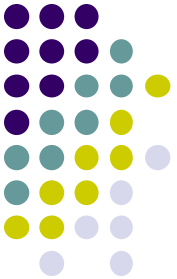
(1) 对$k \in \mathbb{Z}^+$, $a^k = e \Leftrightarrow |a| \mid k$

(2) $|a| = |a^{-1}|$

(3) $|ab| = |ba|$

(4) $|b^{-1}ab| = |a|$

群中元素的阶（续）



- (1) 对$k \in \mathbb{Z}^+$，$a^k = e \Leftrightarrow |a| | k$

证明：(1) “⇒”，设$|a| = m > 0,\ m = min\{k \mid a^k = e \wedge k > 0\}$

故$k \geq m$，从而$k = q \times m + r$，这里$0 \leq r < m$

$\because a^k = a^{qm} * a^r = (a^m)^q * a^r = e^q * a^r = a^r$

$\therefore a^r = e$

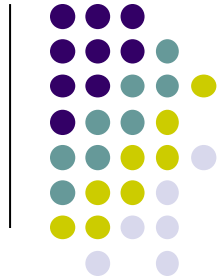
$\because r < m$

$\therefore r = 0$，从而$k = q \times m$，故$m \mid k$。

“⇐”，设$|a| = r$

$|a| \mid k \to r \mid k \to k = n \times r \to a^k = a^{n \times r} = (a^r)^n = e^n = e$

群中元素的阶（续）



(2)令$|a| = r$

$\because (a^{-1})^r = (a^r)^{-1} = e^{-1} = e$

$\therefore |a^{-1}| \mid |a|$，同理$|a| \mid |a^{-1}|$，故$|a^{-1}| = |a|$。

(3)$(ab)^{n+1} = abab\cdots ab = a(ba)^n b$

Case 1: ab的阶有穷，设为r

从而$(ab)^{r+1} = a(ba)^r b$

从而$ab = a(ba)^r b$，故$(ba)^r = e$

故ba的阶有穷，设为r'，由(1)知$r' \mid r$

同理$|ba| = r'$时有$|ab|$有穷，若为r,则$r \mid r'$

因此$|ab| = |ba|$.　　(4) $|b^{-1}ab| = |abb^{-1}| = |ae| = |a|$

群的中心

- 设G是群，构造G的子集C如下：

$$C = \{a \mid a \in G, \text{且} \forall x \in G, ax = xa\}$$

则C构成G的子群，称为G的中心

像是种对称关系

证明：

- C非空：单位元在C中
- 利用判定定理二：即证明对任意的$a, b \in C$, (即$ax=xa$, $bx=xb$对G中一切x成立)，

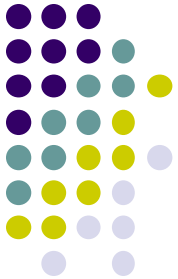
$$(ab^{-1})x = x(ab^{-1}) \text{ 也对G中一切}x\text{成立}$$

$$(ab^{-1})x = a(b^{-1}(x^{-1})^{-1}) = a(x^{-1}b)^{-1} = a(bx^{-1})^{-1} = a(xb^{-1}) = x(ab^{-1})$$

$bx=xb$

$ax=xa$

左(右)陪集及其表示



- 若H是群G的一个子群，a是G中的任意一个元素，定义：$aH = \{ ah \mid h \in H \}$
- aH称为H的一个左陪集
  - 由群的封闭性可知，aH也是G的子集
  - $\forall h \in H.\ ah \in H \ iff\ a \in H$ $aH = H$
- 相应地可定义右陪集

陪集与划分

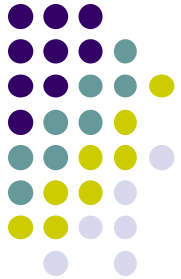
$aH \approx H$

- 设H是群G的子群，则H的所有左陪集构成G的划分
  - G中任意元素a一定在某个左陪集中：$a \in aH$
  - $\forall a,b \in G$, $aH=bH$或者$aH \cap bH=\varnothing$
    - 假设$aH \cap bH \neq \varnothing$, 即存在$c \in aH \cap bH$, 令$c=ah_1=bh_2$,
    - 则$a=bh_2h_1^{-1}$, 从而$aH \subseteq bH$，
    - 同理可得： $bH \subseteq aH$. 所以 $aH=bH$
- 注意：a, b属于同一左陪集

  iff $a \in bH$且$b \in aH$

  iff $b^{-1}a \in H$

陪集与划分（续）



- 定理（**陪集与划分**）：设$\langle H,*\rangle \leq \langle G,*\rangle$，

(1)$eH = H$

(2) $\cup \{aH | a \in G\} = G$

(3) $(a,b \in G)\ aH = bH$ 或者 $aH \cap bH = \emptyset$

(4) $\{aH | a \in G\}$为$\boldsymbol{G}$之划分

陪集与划分（示例）

- 例1：令$H=\{2n|n\in\mathbb{Z}\}$，$\langle H,+\rangle<\langle\mathbb{Z},+\rangle$，$a\in\mathbb{Z}$，$aH=\{2n+a|n\in\mathbb{Z}\}$，$\because(2k+1)H=\mathbb{Z}-H$，$(2k)H=H$，易见$\mathbb{Z}=\cup\{\boldsymbol{aH}|\boldsymbol{a}\in\mathbb{Z}\}=0H\cup1H$
- 例2：$\langle\mathbb{Z}_6,\oplus_6\rangle$为群，令$H=\{0,3\}$，则$\langle H,\oplus_6\rangle<\langle\mathbb{Z}_6,\oplus_6\rangle$，且$H0=H,H1=\{1,4\},H2=\{2,5\}$

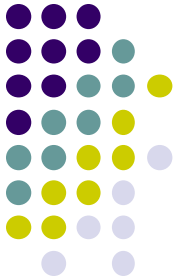
  $H3=\{3,0\}=H,H4=\{4,1\}=H1,H5=\{5,2\}=H2$

  ，易见$\mathbb{Z}_6=\cup\{\boldsymbol{Ha}|\boldsymbol{a}\in\mathbb{Z}_6\}=H0\cup H1\cup H2$

左陪集关系

- 设H是群G的子群，定义G上的二元关系R如下：
  $\forall a,b\in G$, $(a,b)\in R$当且仅当$b^{-1}a\in H$ $\Leftrightarrow a\in bH$
- R是G上的等价关系
  - 自反性：$\forall a\in G$, $a^{-1}a=e$
  - 对称性：注意$a^{-1}b=(b^{-1}a)^{-1}$
  - 传递性：如果$b^{-1}a\in H$, $c^{-1}b\in H$, 则
    $$c^{-1}a=c^{-1}(bb^{-1})a=(c^{-1}b)(b^{-1}a)\in H$$
- $[a]_R=aH$：$x\in[a]_R \Leftrightarrow aRx \Leftrightarrow x^{-1}a\in H \Leftrightarrow x\in aH$

Lagrange（拉格朗日）定理



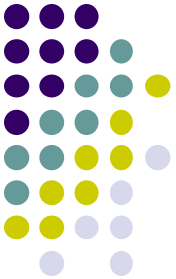
- 引理（陪集的势）

  设$\langle H,*\rangle \leq \langle G,*\rangle$，$a \in G$，则$H \approx Ha \approx aH$

- **证明：**

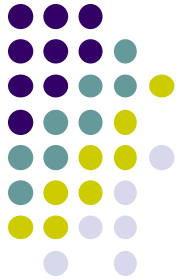
  令$\tau: H \to Ha$为$\tau(h) = ha$，$\sigma: H \to aH$为$\sigma(h) = ah$，由消去律可知τ, σ为1-1，易见τ, σ亦为onto，故$H \approx Ha$，$H \approx aH$

Lagrange 定理（续）



- G被划分为若干个（子群）H在G中的左(或右)陪集，这些陪集等势。H在G中的不同左(或右)陪集的个数称为H在G中的指数(index)，记为$[G:H]$。

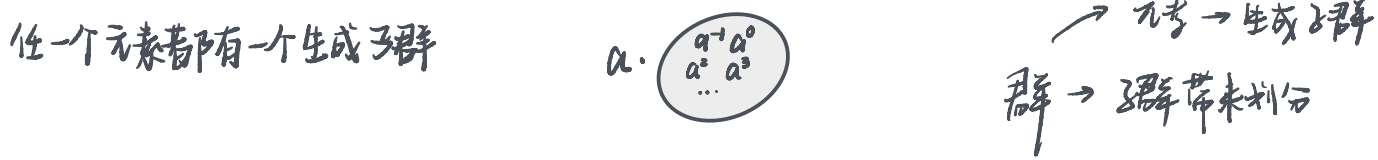
Lagrange 定理（续）



- Lagrange定理：设$\langle G,*\rangle$为有限群，$\langle H,*\rangle \leq \langle G,*\rangle$，则$|G| = |H| \cdot [G:H]$
- **证明：** 由于$|G|$有穷，故$[G:H]$有穷且设为N，从而有$a_1, \cdots, a_N \in G$使$\{Ha_i | 1 \leq i \leq N\}$为$G$之划分，故$G = \bigcup_{i=1}^{N} Ha_i$；由引理，对任意$i,j$，$|Ha_i| = |Ha_j| = |H|$ $\therefore |G| = |H| \cdot N$即$|G| = |H| \cdot [G:H]$. □

Lagrange 定理（续）

- 推论1：设$\langle G,*\rangle$为有限群，$a \in G$，则$|a|$为$|G|$的因子
- 证明*：$\because \langle\langle a\rangle,*\rangle \leq \langle G,*\rangle \therefore |\langle a\rangle|$为$|G|$的因子，又由于$|a|$有穷，故$|\langle a\rangle| = |a|$，故$|a|$为$|G|$的因子. □
  - 注：$\langle a\rangle = \{a^n | n \in \mathbb{Z}\}$，$\langle\langle a\rangle,*\rangle$称元素$a$的生成子群



Lagrange 定理（续）

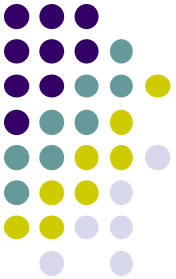
- 推论2*：设$\langle G,*\rangle$为p阶群，若p为质数，则$(\exists a \in G)(\langle a\rangle = G)$

证：设$|G| = p$为素数，可以取$a \neq e,\ a \in G$,由上推论知

$|\langle a\rangle|$为$|G|$的因子，$\because |\langle a\rangle| \geq 2\ \ \therefore |\langle a\rangle| = p$

故$G = \langle a\rangle$

拉格朗日定理的应用

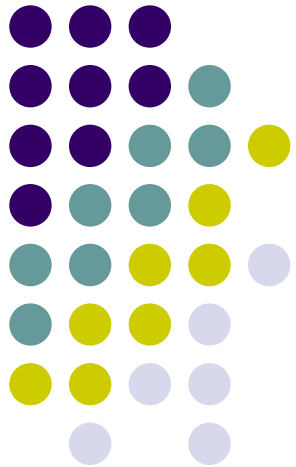


- 6阶群G必含3阶子群
- 证明
  - 如果G中有6阶元素a, 则$b=aa$是3阶元素，因此$\langle b\rangle$是3阶子群
  - 如果G中没有6阶元素，则根据拉格郎日定理的推论，G中元素的阶只可能是1,2或3。
    - 如果没有3阶元素，即$\forall x\in G, x^2=e$, 那么$\forall x, y\in G, xy=(yx)^2(xy)=yx$, 即G是交换群。
    - 因此$\{e,a,b,ab\}$构成4阶子群，但4不能整除6，矛盾。
  - 所以G中必含3阶元素a, 即由a生成的子群是3阶子群。

循环群与群同构

离散数学—代数结构

南京大学计算机科学与技术系



循环群与群同构

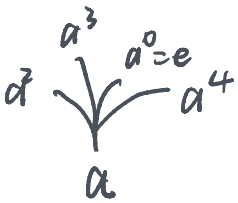
- 循环群与生成元
- 循环群的子群
- 群的同构与同态
- 无限循环群的同构群
- 有限循环群的同构群
- (循环)群的直积

循环群与生成元

- 定义（循环群）

$\langle G,*\rangle$为循环群（cyclic group）是指：

$$(\exists a \in G)(G = \langle a \rangle)$$



不一定唯一

像是一个群的“根”

这里，$\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$，$a$称为$G$之生成元（generator）

循环群与生成元（续）

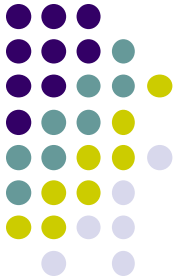
- 定义（有限循环群）：若循环群G的生成元a的阶为n，则称G为有限循环群，即n阶循环群。

  $\boldsymbol{G=\{a^0,a^1,a^2,\cdots,a^{n-1}\}}$，其中$a^0$为单位元。

- 定义（无限循环群）：若循环群G的生成元a为无限阶元，则称G为无限循环群。

  $\boldsymbol{G=\{a^0,a^{\pm1},a^{\pm2},\cdots\}}$，其中$a^0$为单位元。

循环群与生成元（续）



- 例1：无限循环群$\langle \mathbb{Z}, + \rangle$

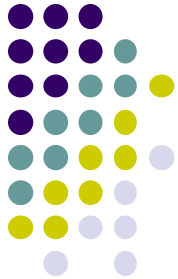
$\langle \mathbb{Z}, + \rangle$是循环群，恰有2个生成元：1和 -1

$\because n$为$\mathbb{Z}$之生成元$\Leftrightarrow \mathbb{Z} = \langle n \rangle \Leftrightarrow (\exists k \in \mathbb{Z}) n^k =$

$1 \Leftrightarrow (\exists k \in \mathbb{Z})(k \cdot n = 1) \Leftrightarrow n \in \{1, -1\}$

$\therefore$ 1和 -1均是其生成元

循环群与生成元（续）



- 例2：有限循环群

模6剩余加群$\langle \mathbb{Z}_6, \oplus_6 \rangle$是循环群，有2个生成元：1 和 5

$$5^0 = 0,\ 5^1 = 5,\ 5^2 = 4,$$

$$5^3 = 3,\ 5^4 = 2,\ 5^5 = 1.$$

循环群与生成元（续）

- 例3：非循环群

Klein四元群$(V,*)$不是循环群，

对非单位元$x \in V$，

$\langle x \rangle = \{e, x\}$：

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

无限循环群的生成元

- 命题：若a是无限循环群的生成元，则a^{-1}也是该无限循环群的生成元

➢ 设群$G = \langle a \rangle = \{a^k | a \in G, k \in \mathbb{Z}\}$，$a^k = (a^{-1})^{-k}$，

令$p = -k$，则$G = \{(a^{-1})^p | p \in \mathbb{Z}\}$，故$G = \langle a^{-1} \rangle$

无限循环群的生成元（续）

- 命题：无限循环群有且只有2个生成元
- 证明：∵ 设群$G = \langle a \rangle = \{a^k \mid a \in G, k \in \mathbb{Z}\}$，若$b$亦为$G$的生成元，则：$(\exists m, t \in \mathbb{Z})(a^m = b \wedge b^t = a)$，故$a = b^t = (a^m)^t = a^{mt}$，由消去律，$a^{mt-1} = e$ ∵ a是无限阶元∴ $mt - 1 = 0 \Rightarrow (m = t = 1) \vee (m = t = -1)$，故有$b = a$或者$b = a^{-1}$

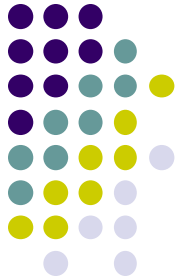
有限循环群的生成元

- **命题：** 设有限群$G = \langle a \rangle$，且$|a| = n$，则对任意不大于n的正整数r，$\boldsymbol{G = \langle a^r \rangle \Leftrightarrow \gcd(n, r) = 1}$

  $G=\langle a\rangle$
  $G=\langle a^r\rangle$

  - “$\Leftarrow$”：设$\gcd(n, r) = 1$，则$(\exists u, v \in \mathbb{Z})(ur + vn = 1)$，因此$a = a^{ur+vn} = (a^r)^u(a^n)^v = (a^r)^u$。故而$G$中任意元素$a^k$可表为$(a^r)^{uk}$，故有$G = \langle a^r \rangle$；
  - “$\Rightarrow$”：设a^r是G的生成元，令$\gcd(n, r) = d$且$r = dt$，则$(a^n)^t = (a^n)^{r/d} = (a^r)^{n/d} = e$，故$|a^r| | (n/d)$，但$|a^r| = n$故$n | \frac{n}{d} \Rightarrow d = 1$，故有$\gcd(n, r) = 1$即$n$与$r$互质

有限循环群的生成元（续）



- n阶循环群G的生成元的个数恰好等于不大于n且与n互质的正整数的个数，即Euler函数$\varphi(n)$，其生成元集为：

$$\{a^i \mid 1 \le i \le n \wedge \gcd(i,n) = 1\}$$

循环群的生成元（续）

$12=2^2\times3$

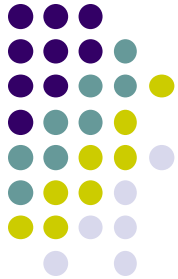
$\varphi(12)=12\times(1-\frac{1}{2})(1-\frac{1}{3})=4$

例 (1) 设 $G=\{e,a,\ldots,a^{11}\}$ 是 12 阶循环群，则 $\varphi(12)=4$. 小于或等于 12 且与 12 互素的数是 1, 5, 7, 11，由定理 11.19 可知 a，a^5，a^7 和 a^{11} 是 G 的生成元.

(2) 设 $G=\langle Z_9,\oplus\rangle$ 是模 9 的整数加群，则 $\varphi(9)=6$. 小于或等于 9 且与 9 互素的数是 1, 2, 4, 5, 7, 8. 根据定理 11.19，G 的生成元是 1, 2, 4, 5, 7 和 8.

(3) 设 $G=3Z=\{3z \mid z\in Z\}$，G 上的运算是普通加法. 那么 G 只有两个生成元：3 和 −3.

循环群的子群



- 命题：设$G=\langle a\rangle$为循环群

(1) G的子群为循环群

(2) 若$|a|=\infty$，则G的子群除$\{e\}$外皆为无限循环群

证:

(1) 令$(H,\ *)\leqslant(G,\ *)$,从而$H\subseteq\langle a\rangle$,若$H=\{e\}$自然成立

否则取a^m为H中最小正方幂元.下证$H=\langle a^m\rangle$只需证$H\subseteq\langle a^m\rangle$,任取$h\in H\subseteq\langle a\rangle$,故$h=a^n$。

令$n=qm+r,\ 0\leq r<m$,从而$h=a^n=a^{qm+r}=(a^m)^q a^r$,从而$a^r=h(a^m)^{-q}\in H$，故由$m$的最小性得$r=0$，从而$h=(a^m)^q\in\langle a^m\rangle$，因此$H$为循环群。

(2) 设$H\leqslant G$，由(1)得$H=\langle a^m\rangle$，若$H\neq\{e\}$则$m\neq 0$,从而若$|H|$有穷则$|a^m|$有穷与$|a|$无穷矛盾。

循环群的子群（续）

- 命题：对n的每个因子d，n阶循环群G中恰有一个d阶子群
- 证明：
  - 令$H=\langle a^{n/d}\rangle$，显然H是G的d阶子群
  - 若令$H_1=\langle a^m\rangle$亦为d阶子群，则$(a^m)^d=a^{md}=e$，故有$n|md$，即$\frac{n}{d}|m$，因此$a^m=\left(a^{n/d}\right)^k\in H$，即$H_1\subseteq H$，但$H_1\approx H$，故有$H_1=H$

循环群的子群（续）

$G=Z_{12}$ 是 12 阶循环群. 12 的正因子是 1,2,3,4,6 和 12，因此 G 的子群是:

1 阶子群　　$\langle 12\rangle=\langle 0\rangle=\{0\}$

2 阶子群　　$\langle 6\rangle=\{0,6\}$

3 阶子群　　$\langle 4\rangle=\{0,4,8\}$

4 阶子群　　$\langle 3\rangle=\{0,3,6,9\}$

6 阶子群　　$\langle 2\rangle=\{0,2,4,6,8,10\}$

12 阶子群　　$\langle 1\rangle=Z_{12}$

群同构与同构映射

- **定义（群同构）**：群$\langle G_1,\circ\rangle$与$\langle G_2,*\rangle$同构($G_1 \cong G_2$)当且仅当存在双射函数$f: G_1 \to G_2$，满足：

$$\forall x, y \in G_1,\ f(x \circ y) = f(x) * f(y)$$

- 举例

正实数乘群$\langle \mathbb{R}^+,\cdot\rangle$和实数加群$\langle \mathbb{R},+\rangle$，同构映射

$f: \mathbb{R}^+ \to \mathbb{R}: f(x) = \ln x$

$f(xy) = \ln xy = \ln x + \ln y$.

群同构与同构映射（续）

- 任意两个三阶群同构

$0 \to a \quad 1 \to b \quad 2 \to c$

$\circ$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

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

群同构与同构映射（续）

- 2个不同构的四阶群

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

四元循环群 $\langle \mathbb{Z}_4, \oplus_4 \rangle$

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Klein四元群 全部为二阶

同态与同态映射

- 定义（群同态）：群$\langle G_1,\circ\rangle$与$\langle G_2,*\rangle$同态$(G_1 \sim G_2)$当且仅当存在函数$f: G_1 \to G_2$，满足：只需映射

$$\forall x, y \in G_1,\ f(x \circ y) = f(x) * f(y)$$

- 如果上述映射是满射，则称为满同态；如映射是单射，则称为单同态；若$G_1 = G_2$，则称φ为自同态

同态与同态映射（续）

- 命题：设f为从群$\langle G,*\rangle$到群$\langle H,\circ\rangle$的同态，则

(1) $\boldsymbol{f(e_G)=e_H}$；

(2) $\boldsymbol{f(a^{-1})=(f(a))^{-1},\ \forall a\in G}$

证明：(1) $\because f(e_G)=f(e_Ge_G)=f(e_G)f(e_G)$

$\therefore f(e_G)=f(e_G)(f(e_G))^{-1}=e_H$

(2) $\because f(a^{-1})f(a)=f(a^{-1}a)=f(e_G)=e_H$

$f(a)f(a^{-1})=f(aa^{-1})=f(e_G)=e_H$

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

同态与同态映射（续）

- 举例：整数加系统$\langle \mathbb{Z}, + \rangle$与模3剩余加系统$\langle \mathbb{Z}_3, \oplus_3 \rangle$同态，同态映射为

$$f: \mathbb{Z} \to \mathbb{Z}_3，\ f(3k + r) = r，\ k \in \mathbb{Z}$$

该态射亦为满同态

- 趣味问题：由$1, 2, \cdots, 1000$这一千个自然数按照任意的组合进行加减，能否得到1001？

同态与同态映射（续）

- **趣味问题：** 由$1, 2, \cdots, 1000$这一千个自然数按照任意的组合进行加减，能否得到1001？
- **定义系统（奇偶加群）：** $\langle \{e, o\}, * \rangle$，运算表如下：

$*$	e	o
e	e	o
o	o	e

则 $f: \mathbb{Z} \to \{e, o\}$ 与 $\langle \mathbb{Z}_2, \oplus_2 \rangle$ 同构

$$f(x) = \begin{cases} e & x\text{是偶数} \\ o & x\text{是奇数} \end{cases}$$

是从$(\mathbb{Z}, +)$到$(\{e, o\}, *)$的满同态映射

无限循环群的同构群

- 定理：设$\langle G,*\rangle$为无限循环群，则$\langle G,*\rangle \cong \langle \mathbb{Z},+\rangle$
- 证明：$|a|=\infty$，令$f:\mathbb{Z}\to G$如下：$f(n)=a^n$，

$\because f(n+m)=a^{n+m}=a^n*a^m=f(n)*f(m)\therefore f$为同态；又$\because f(n)=f(m)\Rightarrow a^n=a^m\Rightarrow a^{|n-m|}=e\Rightarrow |n-m|=0\Rightarrow n=m\therefore f$为1-1，onto易见，从而$\langle G,*\rangle \cong \langle \mathbb{Z},+\rangle$

有限循环群的同构群

- **定理：** 设$\langle G,*\rangle$为有限循环群，则$\langle \boldsymbol{G},*\rangle \cong \langle \mathbb{Z}_{\boldsymbol{n}},\oplus_{\boldsymbol{n}}\rangle$
- **证明：** $|a|=n>0$从而$G=\{a^0,a^1,\cdots,a^{n-1}\}$，令$f:\mathbb{Z}_n\to G$如下：$f(i)=a^i(i=0,1,\cdots,n-1)$，由于$f(i\oplus_n j)=a^{i\oplus_n j}=a^i*a^j=f(i)*f(j)$，故$f$为同态。又由于$f(i)=f(j)\Rightarrow a^i=a^j\Rightarrow a^{|i-j|}=e\Rightarrow n||i-j|\Rightarrow i\equiv j(\mathrm{mod}\,n)\Rightarrow i=j$，故$f$为单射，$f$的满射性易见，因此$\langle G,*\rangle\cong\langle \mathbb{Z}_n,\oplus_n\rangle$

循环群的同构群

- 定理：设$\langle G,* \rangle$为无限循环群，则$\langle \boldsymbol{G},* \rangle \cong \langle \mathbb{Z},+ \rangle$
- 定理：设$\langle G,* \rangle$为有限循环群，则$\langle \boldsymbol{G},* \rangle \cong \langle \mathbb{Z}_{\boldsymbol{n}},\oplus_{\boldsymbol{n}} \rangle$

推论：循环群皆为阿贝尔群

群的直积

- 给定两个群: $(S, \circ)$, $(T, *)$, 定义笛卡儿乘积$S \times T$上的运算$\otimes$如下：

  $\langle s_1, t_1 \rangle \otimes \langle s_2, t_2 \rangle = \langle s_1 \circ s_2, t_1 * t_2 \rangle$

- $(S \times T, \otimes)$是群
  - 结合律： $\langle (r_1 \circ s_1) \circ t_1, (r_2 * s_2) * t_2 \rangle$

    $= \langle r_1 \circ (s_1 \circ t_1), r_2 * (s_2 * t_2) \rangle$
  - 单位元素：$\langle e_S, e_T \rangle$
  - 逆元素：$\langle s, t \rangle$ 的逆元素是 $\langle s^{-1}, t^{-1} \rangle$

    (其中： $s, s^{-1} \in S$, $t, t^{-1} \in T$)

循环群的直积

- $C_m \times C_n \cong C_{mn}$ *iff* m与n互质。其中C_k表示k阶循环群。
  - ⇐若m与n互质，只需证明$C_m \times C_n$含有阶为mn的元素。
    - $(a,b)^{mn} = e$, 其中a,b分别是C_m和C_n的生成元素。
    - 若$(a,b)^k = e$, k必是m,n的公倍数，因m与n互质，故k是mn的倍数。所以，(a,b)的阶是mn。
  - ⇒若$C_m \times C_n \cong C_{mn}$，则$C_m \times C_n$是循环群，设其生成元是(s,t), 则(s,t)的阶是mn, 若gcd(m,n)=k>1, 则$(s,t)^{mn/k} = e$, 这与(s,t)的阶是mn矛盾。

注意：$s^m = e_1$, $t^n = e_2$,

欧拉函数(phi)

- 如果m与n互质，则 φ(m)φ(n) =φ(mn).

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{k_1})\varphi(p_2^{k_2})\cdots\varphi(p_r^{k_r}) \\ &= p_1^{k_1}\left(1-\frac{1}{p_1}\right)p_2^{k_2}\left(1-\frac{1}{p_2}\right)\cdots p_r^{k_r}\left(1-\frac{1}{p_r}\right) \\ &= p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right) \\ &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right).\end{aligned}$$

$$\varphi(n) = n\prod_{p|n}\left(1-\frac{1}{p}\right),$$

欧拉函数(phi)

- C_n中元素按其阶分类，d阶元素共有$\varphi(d)$个，$d|n$.

$$\sum_{d|n} \varphi(d) = n,$$

- (Euler定理) 若正整数a与n互质，则

$$a^{\varphi(n)} \equiv 1 \mod n.$$

$\{r \mid 1 \le r \le n \wedge gcd(r,n)=1\}$
单位元：1

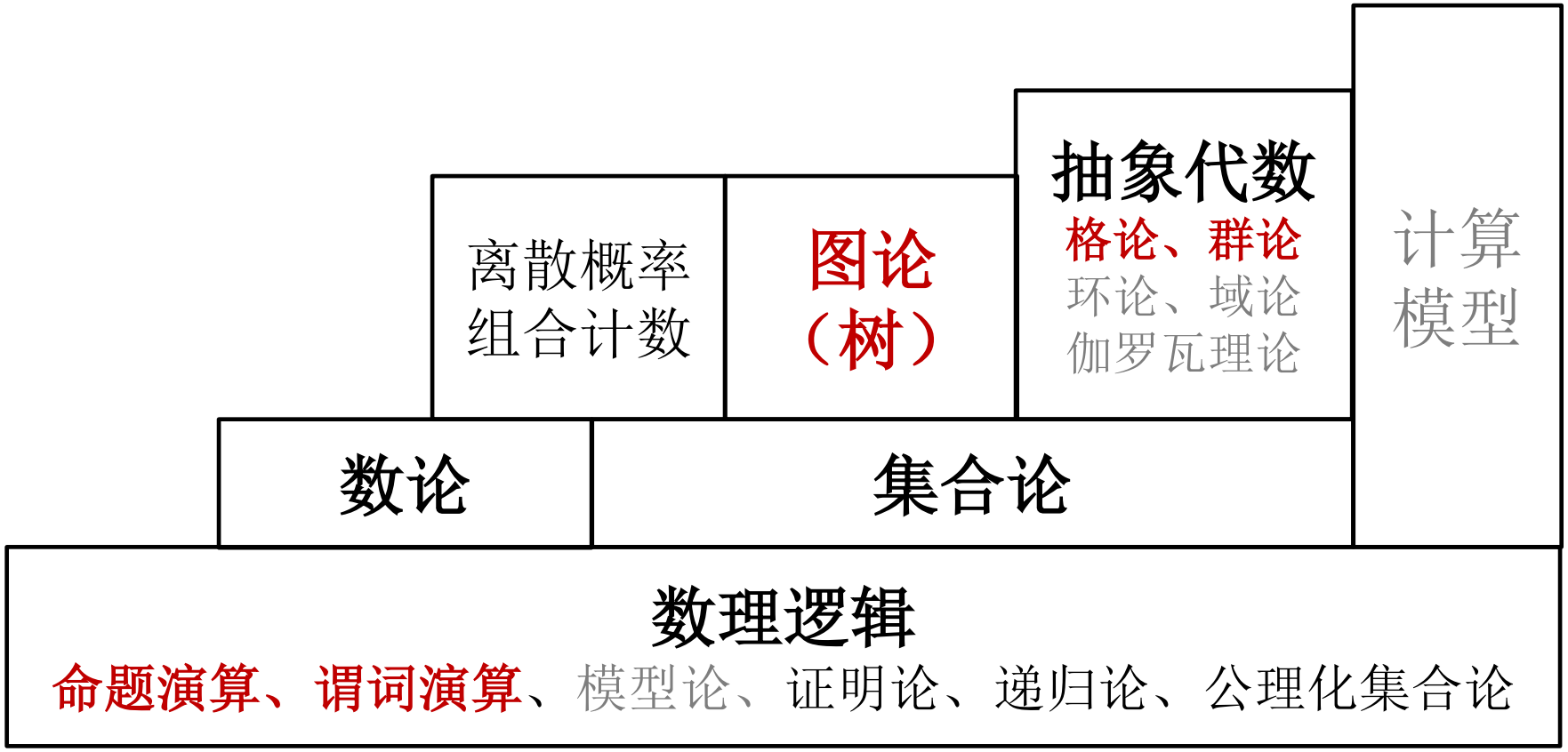
小于n且与n互质的正整数及乘法（模n）构成一个群

图论:基本概念

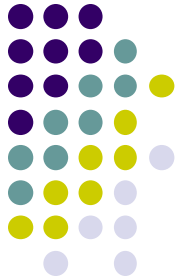
瞿裕忠 教授

南京大学计算机科学与技术系

离散数学知识体系

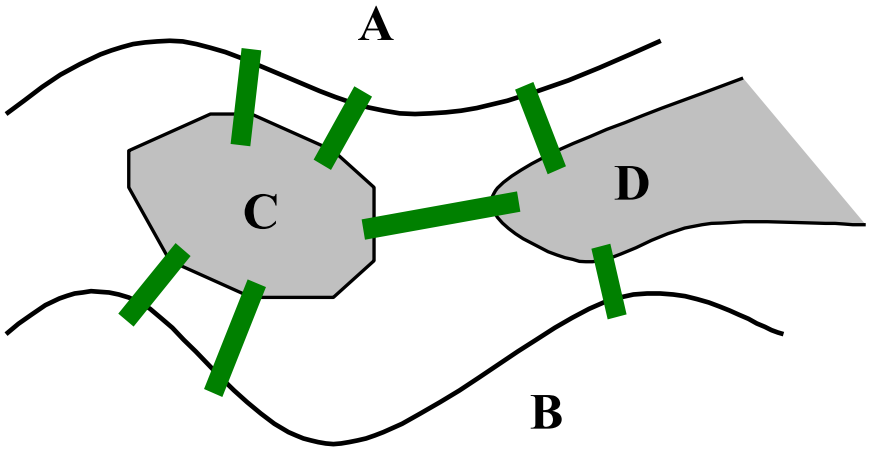

抽象代数
格论、群论
环论、域论
伽罗瓦理论
计算
模型
离散概率
组合计数
图论
（树）
数论
集合论
数理逻辑
命题演算、谓词演算、模型论、证明论、递归论、公理化集合论

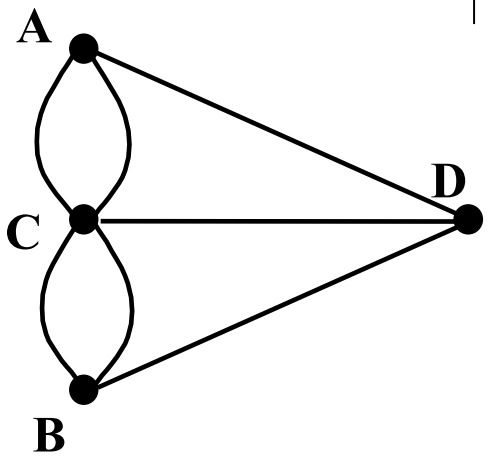
基本概念（1）



- 图的定义
- 图的术语
- 握手定理
- 图模型

柯尼斯堡(Königsberg)七桥问题





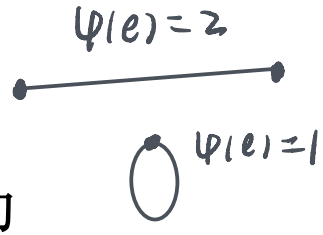
可否：从四块陆地中任一块出发，恰好通过每座桥一次，再回到起点。

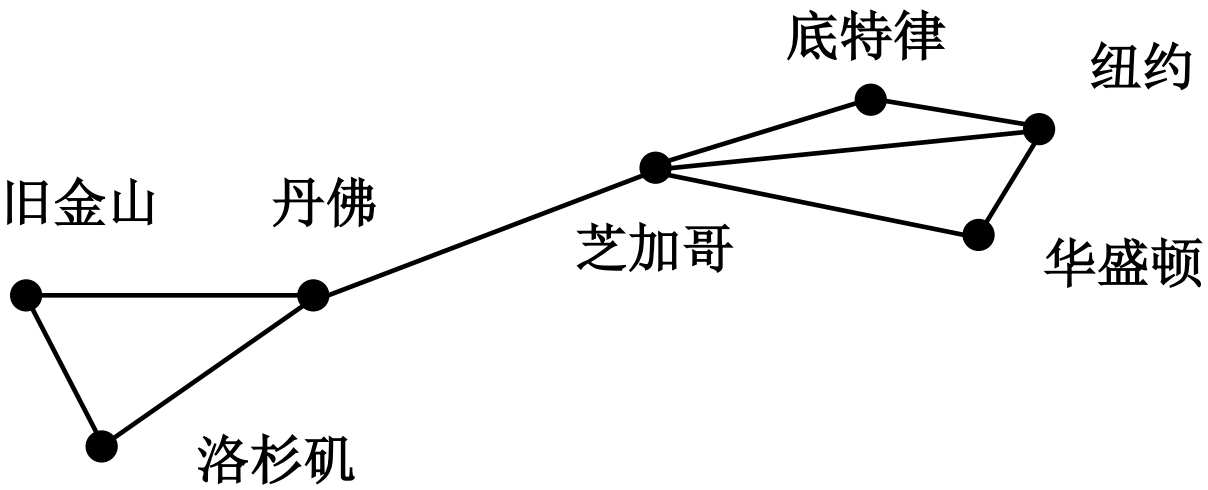
“一笔画”问题

- 问题的抽象（欧拉于1736年）
  - 用顶点表示对象-“地块”
  - 用边表示对象之间的关系-“有桥相连”
  - 观察：各顶点所关联的边数均为奇数

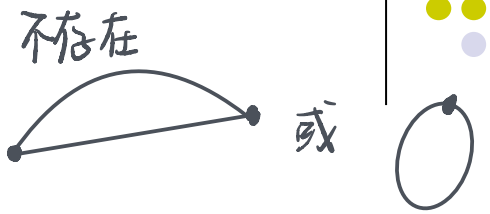
图的定义

- **图G是一个三元组：G =(V, E, φ)**
  - **V是代表顶点的非空集合，E是代表边的集合，且V∩E=ϕ；**
  - **φ: E → P(V), 且∀*e*∈ E. 1≤|φ(*e*)|≤2. φ(*e*)称为边*e*的端点集.**
- **举例（数据中心、通信链接）**





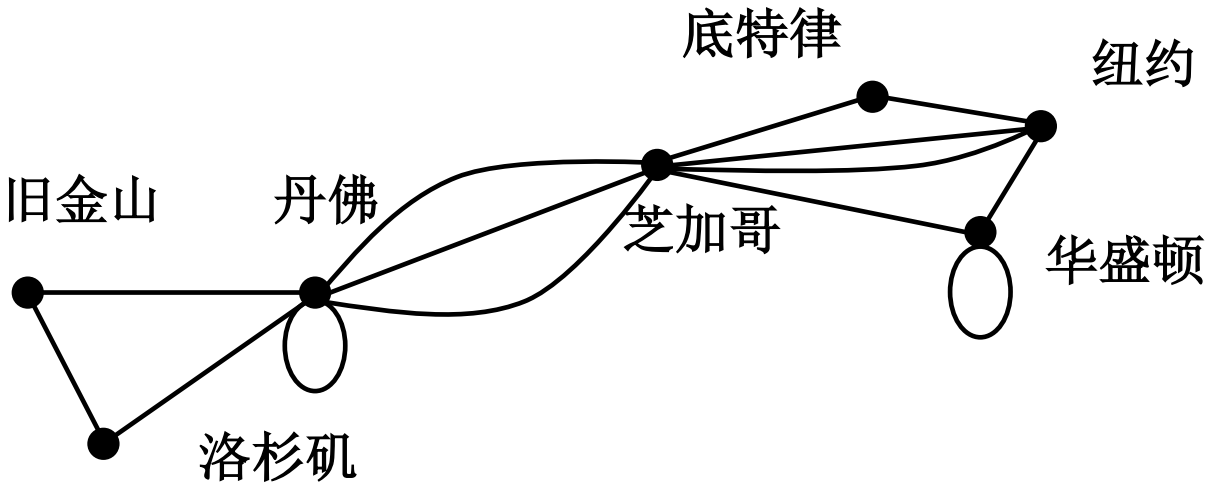
图的定义（续）



- 图G = (V, E, φ)是简单图，如果
  - 每条边有2个端点，即： $\forall e \in E. |\varphi(e)| = 2$，并且
  - 不同边有不同端点集，即：如果$e_1 \neq e_2$，则$\varphi(e_1) \neq \varphi(e_2)$
- 图G = (V, E, φ)是伪图，如果 存在上述情况
  - 存在一条只有1个端点的边，即: $\exists e_0 \in E.|\varphi(e_0)| = 1$，或者
  - 有两条边具有相同的端点集，即:$\exists\ e_1 \neq e_2.\varphi(e_1)=\varphi(e_2)$

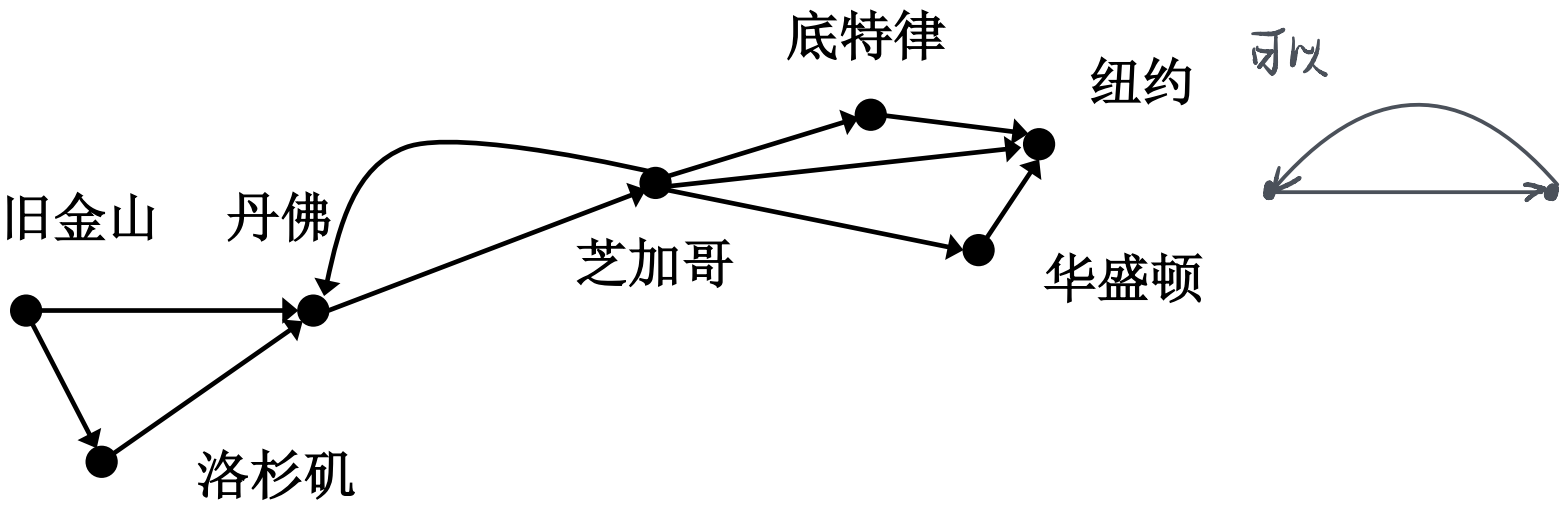
图的定义（续）

- 伪图（包含自环或者多重边）示例



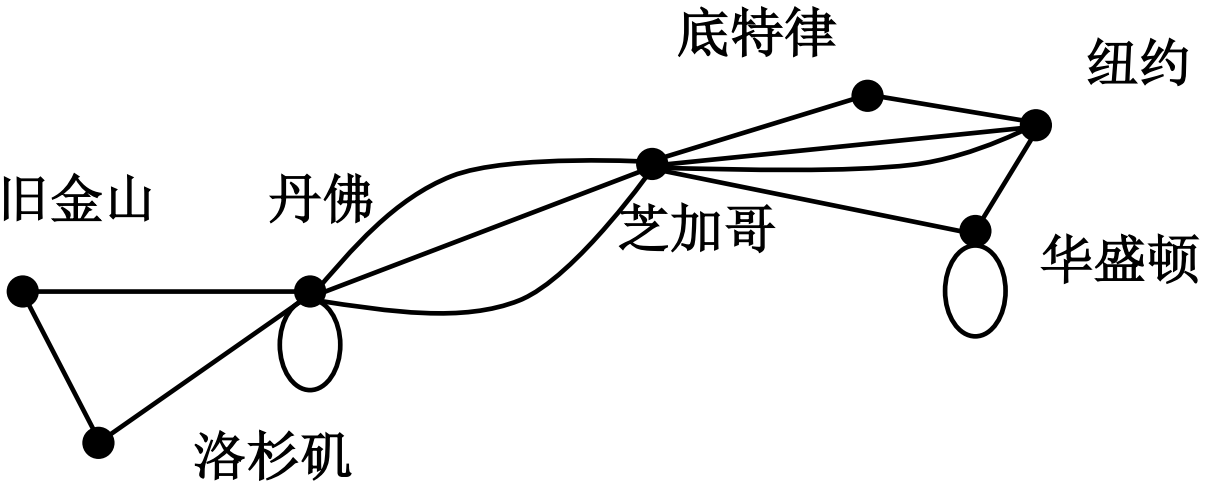
图的定义（有向图）

- 有向图G是一个三元组：G= (V, E, φ)
  - V是非空顶点集，E是有向边（弧）集，且V∩E=ϕ；
  - φ:E→V×V, 若φ(*e*)=(*u*, *v*), 则*u*和*v*分别称为*e*的起点和终点.
- 简单有向图: φ 是单射，并且边的起点和终点不同。



图的术语

- 无向图G = (V, E, φ), φ(*e*)={*u*, *v*} , *u*≠*v*
  - *u*和*v*在G中邻接（相邻）
  - *e*关联（连接）顶点*u*和*v*
- 图G中顶点*v*的度, deg(*v*)， $d_G(v)$
  - 与该顶点关联的边数，自环为顶点的度做出双倍贡献。



图的术语（续）

- 有向图G =(V, E, φ), φ(*e*)=(*u*, *v*)
  - *u*是*e*的起点，*v*是*e*的终点
  - 假设 *u*≠*v*，*u*邻接到*v*，*v*从*u*邻接
- 有向图中顶点的出度和入度
  - $d_G^+(v)$ = 以*v*为始点的边的条数， $\deg^+(v)$
  - $d_G^-(v)$ = 以*v*为终点的边的条数， $\deg^-(v)$
- 有向图中各顶点的出度之和等于入度之和。

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

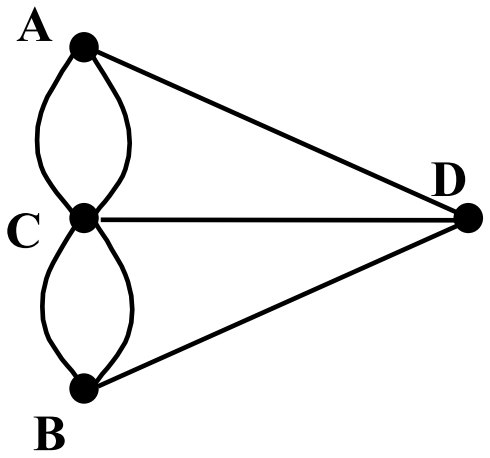
- 有向图的底图：把每条有向边替换为无向边.

握手定理

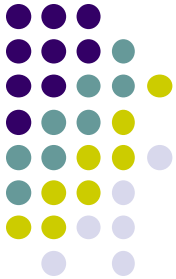
- 无向图G有m条边，n个顶点$v_1, \ldots v_n$.

$$\sum_{i=1}^{n} d(v_i) = 2m$$

- 推论：无向图中奇数度顶点必是偶数个。

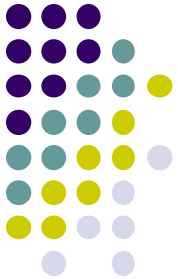


图模型



- 交通网络
  - 航空、公路、铁路
- 信息网络
  - 万维网图（Web Graph）
  - 引用图（Citation Graph）
- 社会网络
  - 熟人关系图
  - 合作图，好莱坞图
  - 呼叫图
- 体育（循环赛的图模型）

基本概念（2）

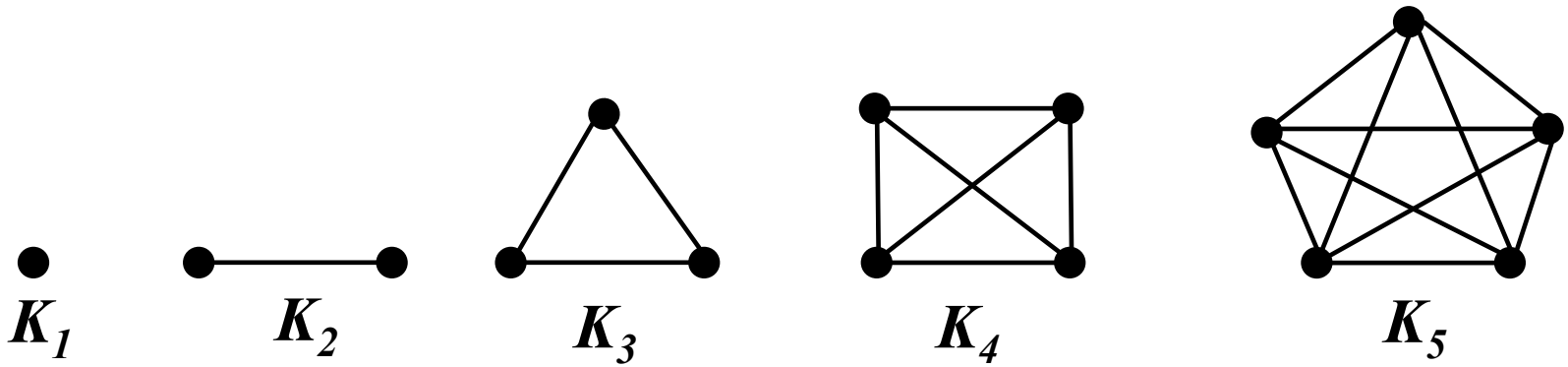


- 几种特殊的图
- 子图
- 图的运算
- 图结构上的经典问题

特殊的简单图（完全图）

- 若简单图G中任意两点均相邻，则称为完全图。记为K_n, 其中n是图中顶点数。
  - K_n中每个顶点皆为n-1度，总边数为$n(n-1)/2$。
  - 边数达到上限的简单图。

n个顶点，n-1条线，每条线算2次

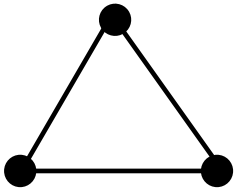


$$deg = \frac{n(n+1)}{2}$$

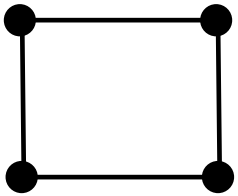
特殊的简单图（圈图与轮图）

每个顶点度为2且连通

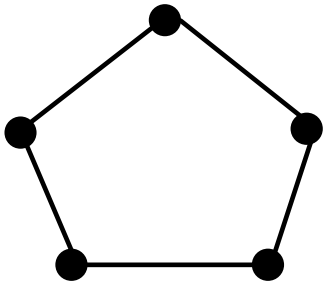
Cycle



C_3



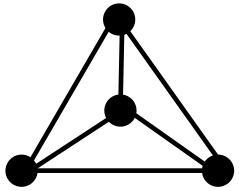
C_4



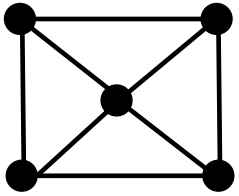
C_5

平面

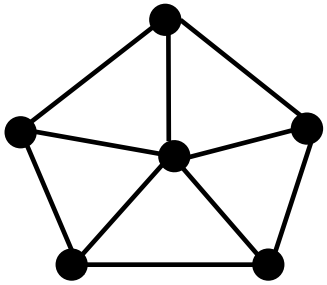
Wheel



W_3



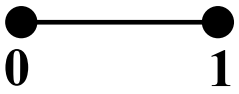
W_4



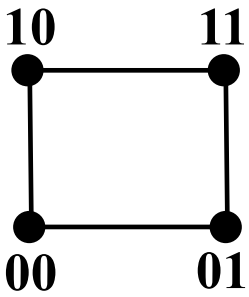
W_5

特殊的简单图（立方体图）

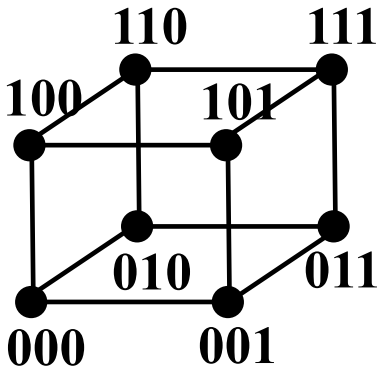
***n*-cube**



Q_1



Q_2

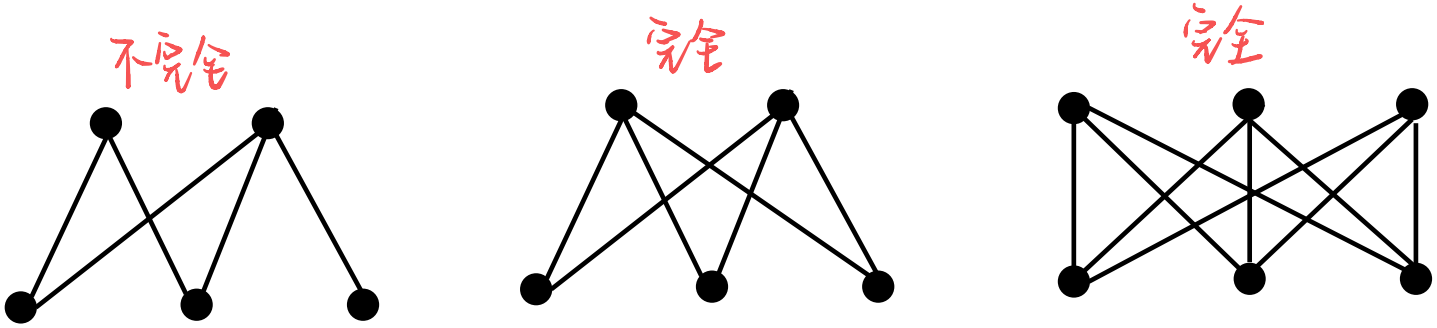


Q_3

正则图：顶点度相同的简单图

二部图（bipartite graph）

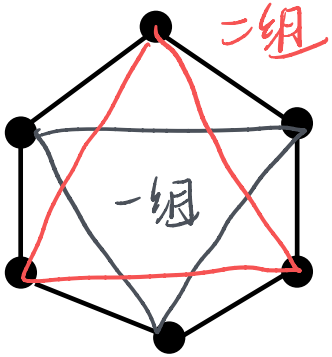
- 二部图：顶点集划分为2个类别（不相交），边的端点在不同类别中。
- 完全二部图：来自不同类别的两个顶点均有边。



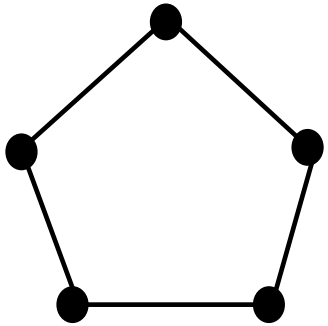
G　　$K_{2,3}$　　$K_{3,3}$

二部图的判定 ⇔每个圈的长度均为偶数

- C_6是否是二部图？



- 二种颜色对顶点着色，相邻顶点赋以不同颜色



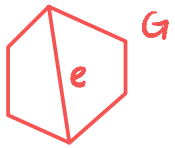
二部图？ 不是

子图

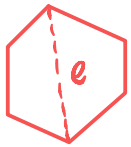
- 设G=<V,E>, G'=<V',E'>, 如果V'⊆V, E'⊆E, 则称G'是G的子图。
- 如果V'⊂V, 或者E' ⊂E, 则称为真子图。
- 诱导（导出）子图：可以由顶点集的子集，或者由边集的子集导出一个子图。

图的运算

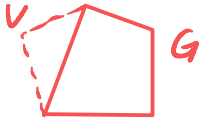
- 加新边:G+*e*



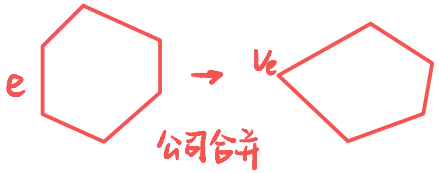
- 减边或边集： G-*e*

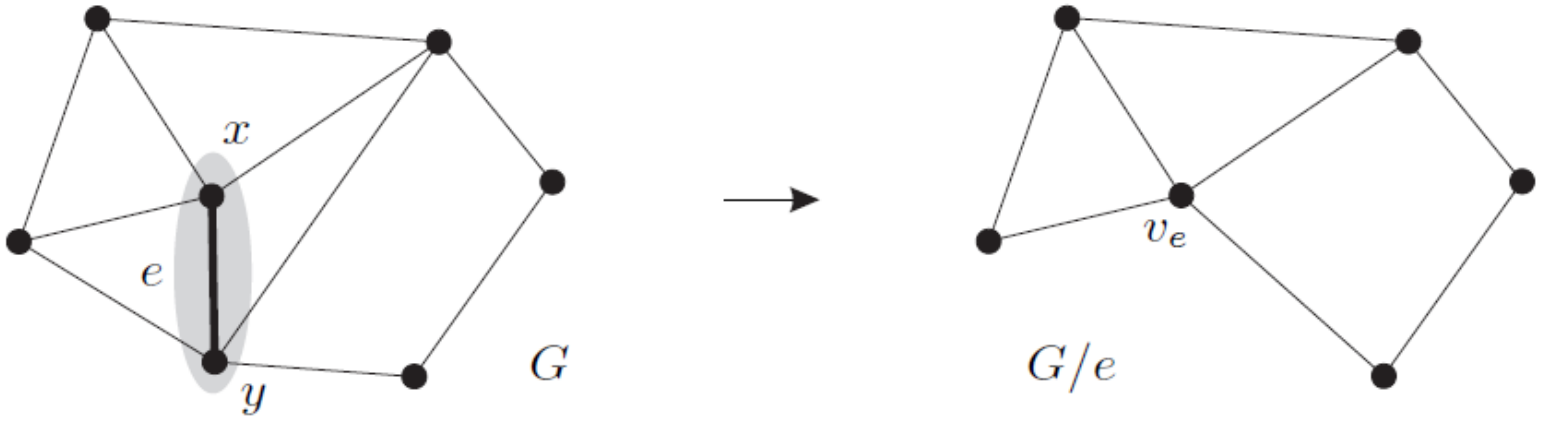


- 减点或点集: G-*v* （同时删除与*v*关联的边）



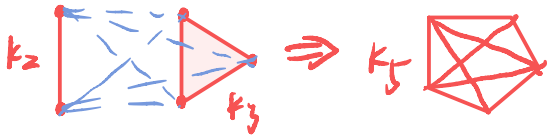
- 边的收缩: G/*e*





图的运算

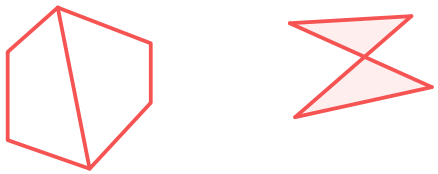
- G∪G’：以V(G)∪V(G’)中的顶点组成的集合为顶点集,以E(G)∪E(G’)为边集。 //简单图的并
- 假设G和G’是不交的无向图, 定义G*G’如下：
  - 以V(G)∪V(G’)为顶点集
  - 以E(G)∪E(G’)∪{{x, y}| x∈V(G), y∈V(G’)}为边集
  - 举例, $K_2 * K_3 = K_5$.



- 简单图G的补图（complement graph），记为 $\overline{G}$
  - G=(V, E) 的补图定义为 (V, [V]^2 \E)

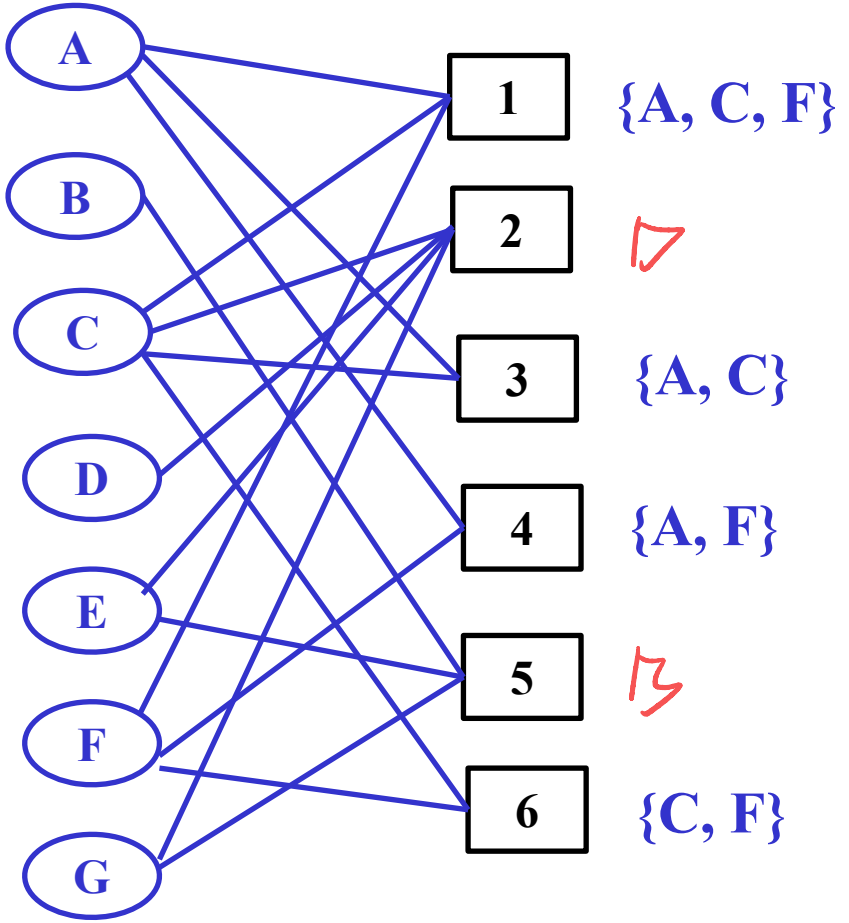
完全图的补图：(V, ψ, φ)

φ: ψ → P(V)



图结构上的经典问题：二部图匹配

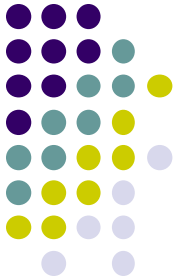
- 孤岛上有*m*个男子和*n*个女子，每个人均有一个可选配偶列表，如何成就尽可能多的幸福婚姻？
- 最大匹配问题。



中国邮递员问题（管梅谷，1960）

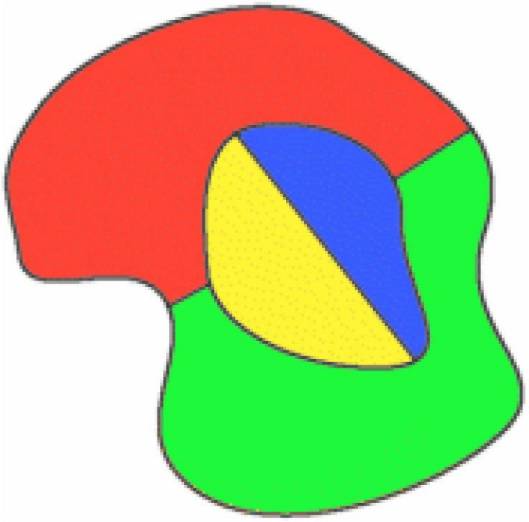
- 邮递员从邮局出发，走过辖区内每条街道至少一次，再回邮局，如何选择最短路线？
- Euler回路？添加重复边（权和最小）。

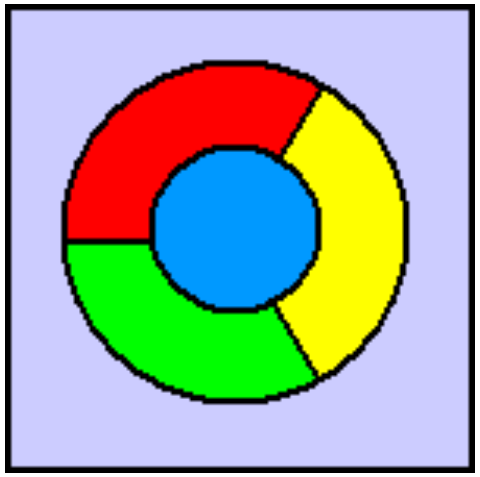
旅行商(TSP)问题



- ***n***个城市间均有道路，但距离不等，旅行商从某地出发，走过其它***n*-1**个城市，且只经过一次，最后回到原地，如何选择最短路线？
- 最短Hamilton回路。

地图与平面图着色（四色猜想）





图的表示与同构

瞿裕忠 教授

南京大学计算机科学与技术系

内容提要

- 图的表示
- 邻接矩阵的运算
- 图的同构

图的表示

- 邻接矩阵
- 邻接表
- 关联矩阵

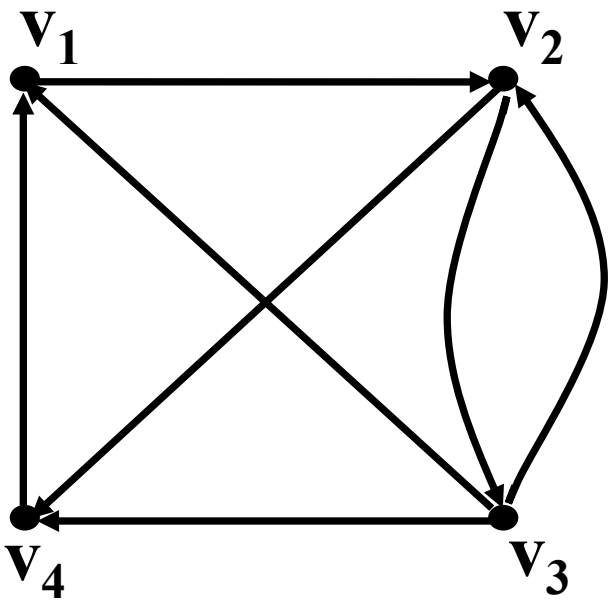
邻接矩阵(*adjacency matrix*)

- 简单有向图$G=(V, E, \varphi)$，设$V=\{v_1, \ldots, v_n\}$，$E=\{e_1, \ldots, e_m\}$。
- $A(G)=[a_{ij}]$称为G的邻接矩阵($n\times n$ 阶矩阵)，其中

$$a_{ij}=\begin{cases}1 & \text{如果}v_i\text{邻接到}v_j\\ 0 & \text{否则}\end{cases}$$

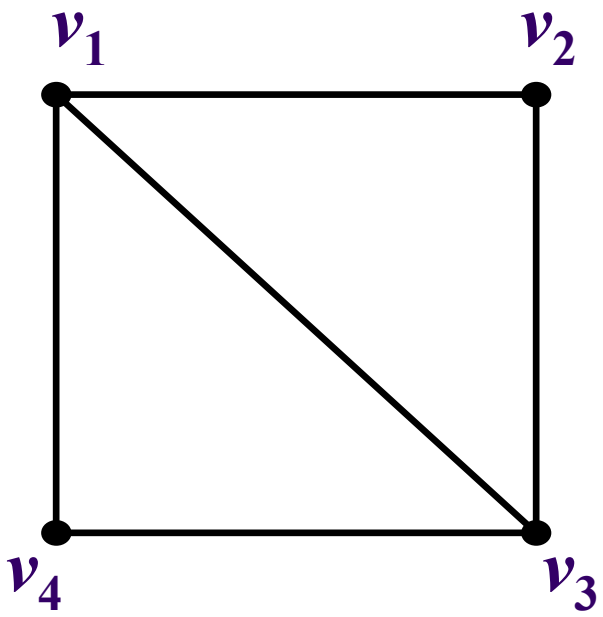
$\exists e\in E.\ \varphi(e)=(v_i, v_j)$

举例（邻接矩阵）



$$A(G)=\begin{Bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{Bmatrix}$$

简单无向图的邻接矩阵



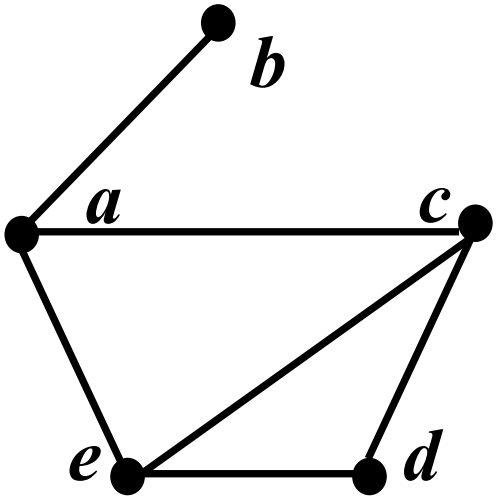
$$A(G)=\begin{Bmatrix}0&1&1&1\\1&0&1&0\\1&1&0&1\\1&0&1&0\end{Bmatrix}$$

简单无向图的邻接矩阵是对称矩阵

邻接表

φ是单射

- 若图G = (V, E, φ) 没有多重边，列出这个图的所有边。对每个顶点，列出与其邻接的顶点。

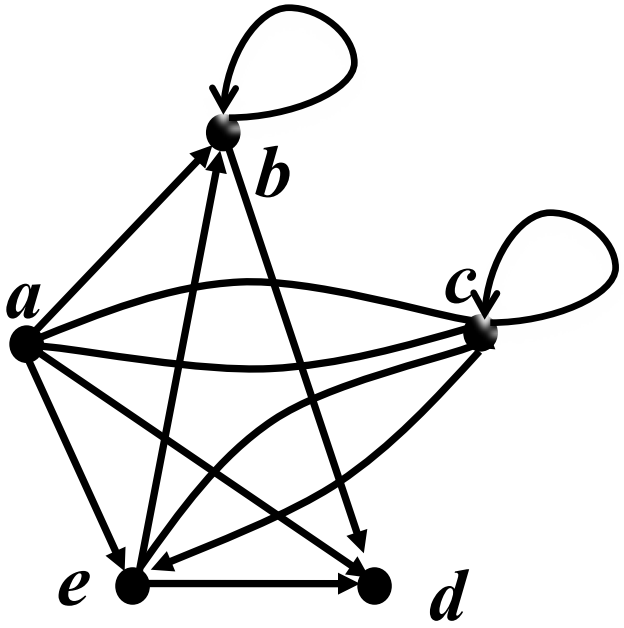


顶 点	相邻顶点
a	*b, c, e*
b	*a*
c	*a, d, e*
d	*c, e*
e	*a, c, d*

邻接表（有向图）

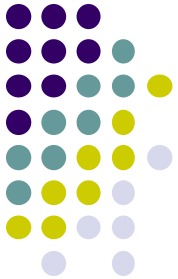
φ是单射

- 若图G = (V, E, φ) 没有多重边，列出这个图的所有边。对每个顶点，列出从该顶点邻接到的顶点。



顶 点	相邻顶点
a	*b, c, d, e*
b	*b, d*
c	*a, c, e*
d	
e	*b, c, d*

关联矩阵(*incidence matrix*)



- 无向图$G=(V, E, \varphi)$，不妨设$V=\{v_1, \ldots, v_n\}$，$E=\{e_1, \ldots, e_m\}$。
- $M(G)=[m_{ij}]$称为G的关联矩阵($n\times m$ 阶矩阵), 其中

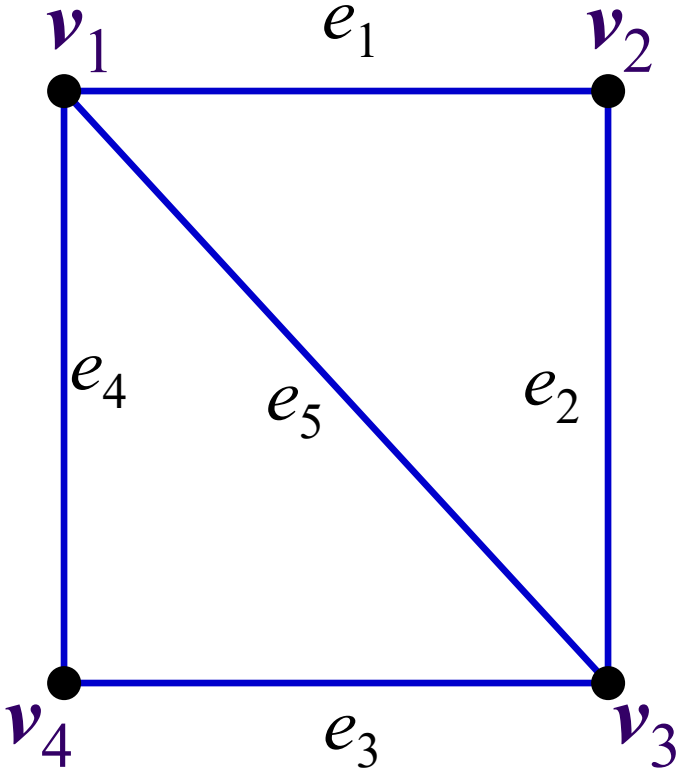
$$m_{ij}=\begin{cases}1 & \text{如果} e_j \text{关联} v_i \\ 0 & \text{否则}\end{cases}$$

$v_i \in \varphi(e_j)$

- 无向图G可以是伪图（含自环或多重边）。

举例（关联矩阵）

$m_{ij}=1$，e_j关联v_i

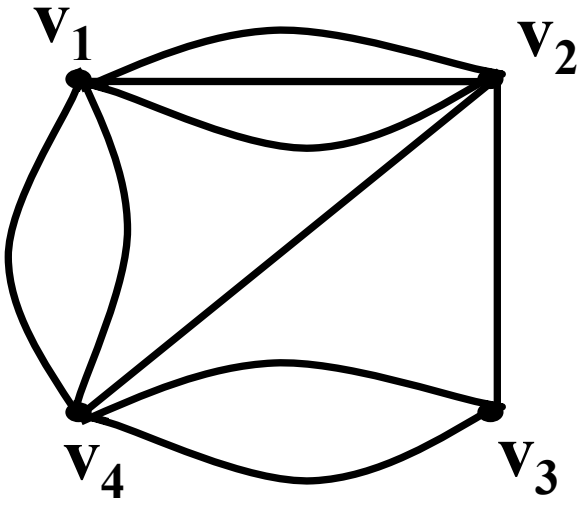


$$M(G)=\begin{matrix} e_1 & e_2 & e_3 & e_4 & e_5 \end{matrix}\begin{Bmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{Bmatrix}$$

并不直接适合于有向图

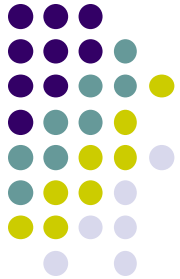
关于邻接矩阵

- 通常，邻接矩阵中的元素为0和1，称为布尔矩阵。
- 邻接矩阵也可表示包含多重边的图，此时的矩阵不是布尔矩阵。

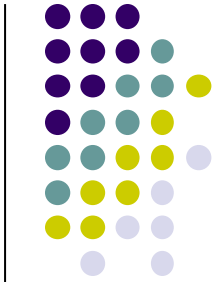


$$A = \begin{Bmatrix} 0 & 3 & 0 & 2 \\ 3 & 0 & 1 & 1 \\ 0 & 1 & 0 & 2 \\ 2 & 1 & 2 & 0 \end{Bmatrix}$$

关于邻接矩阵



- 当有向图中的有向边表示关系时，邻接矩阵就是关系矩阵。无向图的邻接矩阵是对称的。
- 图的邻接矩阵表示，顶点的次序并不紧要，行与行、列与列进行相应交换，可得到另一个矩阵。
  - 两个简单有向图，对应两个邻接矩阵，若对某一矩阵行与行、列与列之间的相应交换后得到的矩阵（酉变换）与另一矩阵相同，则这两个图同构。酉矩阵：$UU^T = U^TU = I$ 即 $U^T = U^{-1}$

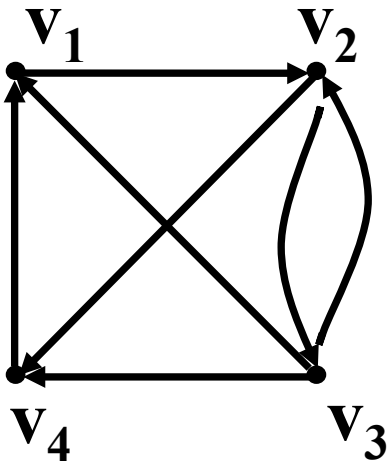


内容提要

- 图的表示
- 邻接矩阵的运算
- 图的同构

邻接矩阵的运算

- 顶点的度（以有向图为例）
  - 行中1的个数就是行中相应顶点的出度
  - 列中1的个数就是列中相应顶点的入度



$$A=\begin{Bmatrix}0&1&0&0\\0&0&1&1\\1&1&0&1\\1&0&0&0\end{Bmatrix}$$

$Deg^+(1)=1, Deg^-(1)=2$

$Deg^+(2)=2, Deg^-(2)=2$

$Deg^+(3)=3, Deg^-(3)=1$

$Deg^+(4)=1, Deg^-(4)=2$

邻接矩阵的运算

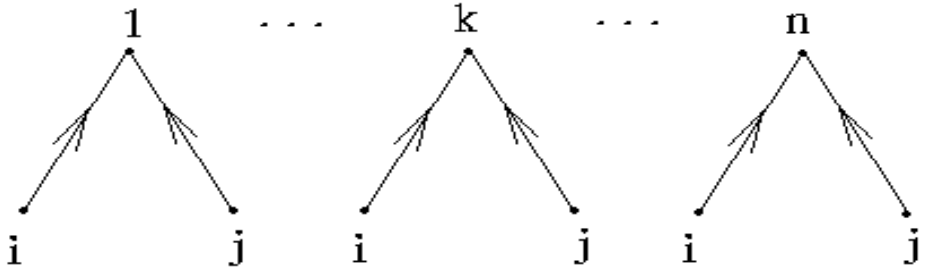
- 逆图（转置矩阵）
  - 设G的邻接矩阵为A，则G的逆图的邻接矩阵是A的转置矩阵，用A^T表示。

$$A=\begin{bmatrix}0&1&0&0\\0&0&1&1\\1&1&0&1\\1&0&0&0\end{bmatrix}\qquad A^T=\begin{bmatrix}0&0&1&1\\1&0&1&0\\0&1&0&0\\0&1&1&0\end{bmatrix}$$

邻接矩阵的运算

$$A \times A^T = B = [b_{ij}]$$

$$b_{ij} = \sum_{k=1}^{n} a_{ik} \times a_{jk} = a_{i1} \times a_{j1} + a_{i2} \times a_{j2} + \cdots + a_{in} \times a_{jn}$$



- b_{ij}表示顶点i和顶点j均有边指向的那些顶点的个数；
- 若$i=j$，则b_{ii}表示顶点i的出度。

邻接矩阵的运算

$$A=\begin{bmatrix}0&1&0&0\\0&0&1&1\\1&1&0&1\\1&0&0&0\end{bmatrix}\qquad A^T=\begin{bmatrix}0&0&1&1\\1&0&1&0\\0&1&0&0\\0&1&1&0\end{bmatrix}$$

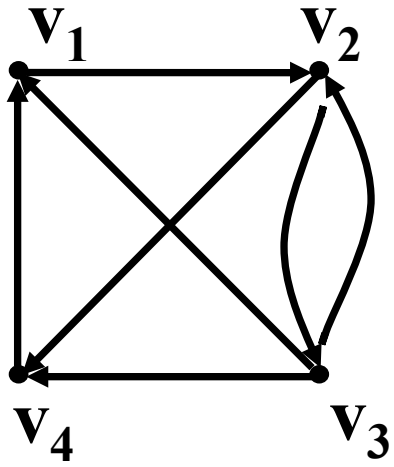
$A^TA=\begin{pmatrix}2&1&0&1\\1&2&0&1\\0&0&1&1\\1&1&1&1\end{pmatrix}$ 入度为3

$$A^T\times A=C=[C_{ij}]$$

$$C_{ij}=\sum_{k=1}^{n}a_{ki}\times a_{kj}=a_{1i}\times a_{1j}+a_{2i}\times a_{2j}+\cdots+a_{ni}\times a_{nj}$$

- C_{ij}表示同时有边指向顶点i和顶点j的那些顶点的个数；
- 若$i=j$，则C_{ii}表示顶点i的入度。

邻接矩阵的运算



$$A=\begin{Bmatrix}0&1&0&0\\0&0&1&1\\1&1&0&1\\1&0&0&0\end{Bmatrix}$$

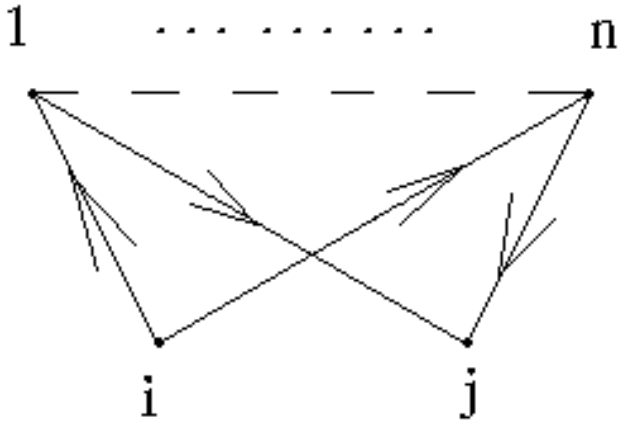
$$A\times A^T=\begin{bmatrix}1&0&1&0\\0&2&1&0\\1&1&3&1\\0&0&1&1\end{bmatrix}$$

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

邻接矩阵的运算

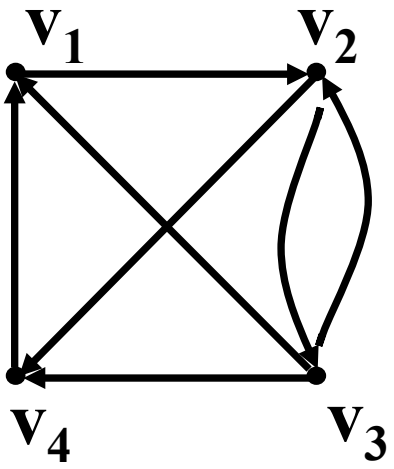
$$A \times A = A^2 = D = [d_{ij}]$$

$$d_{ij} = \sum_{k=1}^{n} a_{ik} \times a_{kj} = a_{i1} \times a_{1j} + \cdots + a_{in} \times a_{nj}$$



- 若$a_{ik} \times a_{kj} = 1$，则表示有$i \to k \to j$长度为2的有向通路；
- d_{ij}表示i和j之间具有长度为2的通路个数。

邻接矩阵的运算



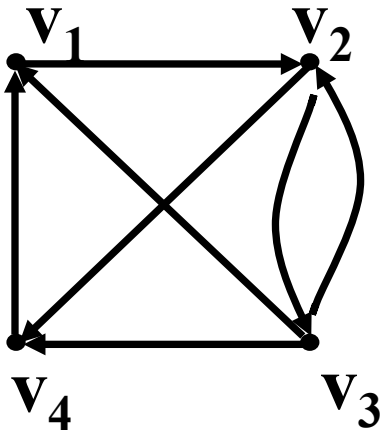
$$A=\begin{Bmatrix}0&1&0&0\\0&0&1&1\\1&1&0&1\\1&0&0&0\end{Bmatrix}$$

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

$$A^3=A^2\times A=\begin{bmatrix}2&1&0&1\\1&2&1&1\\2&2&1&2\\0&0&1&1\end{bmatrix}$$

- 从$v_2\rightarrow v_1$，有二条长度为2的通路；有一条长度为3的通路

邻接矩阵的运算



$$A=\begin{Bmatrix}0&1&0&0\\0&0&1&1\\1&1&0&1\\1&0&0&0\end{Bmatrix}$$

$$B_4=A^1+A^2+A^3+A^4=\begin{bmatrix}3&4&2&3\\5&5&4&6\\7&7&4&7\\3&2&1&2\end{bmatrix}$$

- 长度不大于4的通路个数

内容提要

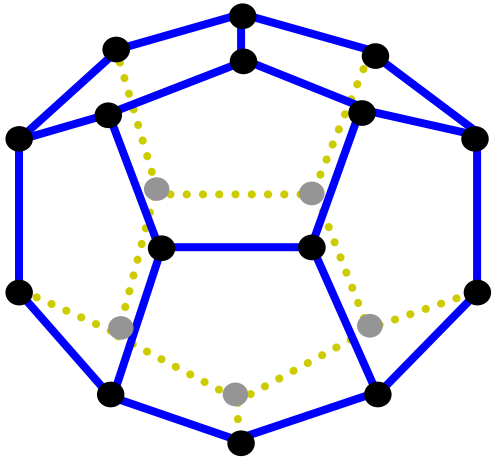
- 图的表示
- 邻接矩阵的运算
- 图的同构

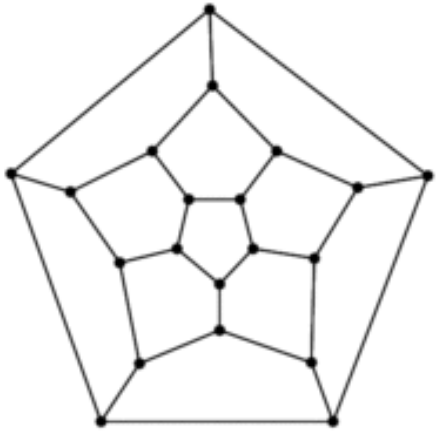
图的同构

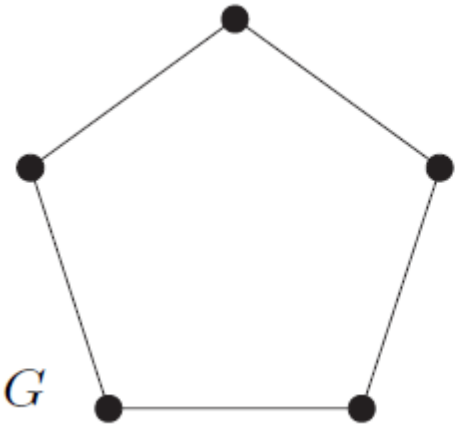
- 图同构的定义
  - 设$G_1=(V_1, E_1, \varphi_1)$和$G_2=(V_2, E_2, \varphi_2)$是两个简单无向图。若存在双射$f: V_1 \to V_2$, u和v在G_1中相邻当且仅当$f(u)$和$f(v)$在G_2中相邻。此时称f是一个同构函数。(只需顶点对应)
  - 设$G_1=(V_1, E_1, \varphi_1)$和$G_2=(V_2, E_2, \varphi_2)$是两个无向图。若存在双射$f: V_1 \to V_2$, $g: E_1 \to E_2$, (顶点对应+边对应)

$\forall e \in E_1, \varphi_1(e)=\{u, v\}$当且仅当$g(e) \in E_2, \varphi_2(g(e))=\{f(u), f(v)\}$

图同构的例子

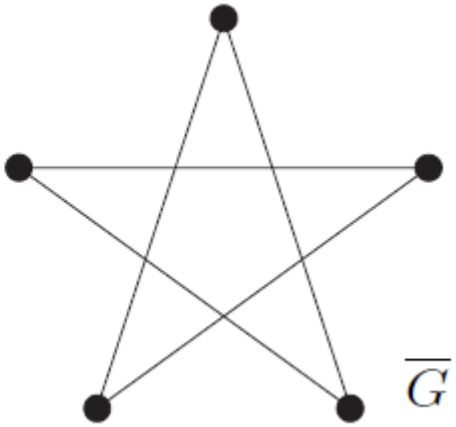






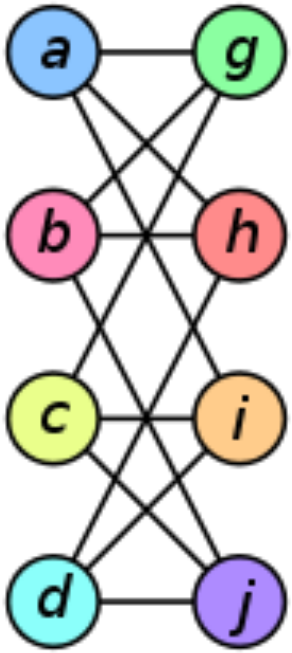
G

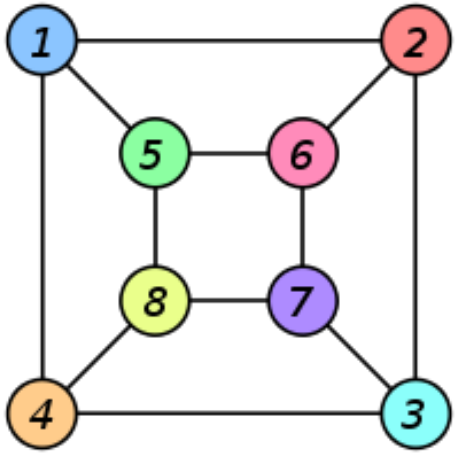
G 与 $\overline{G}$ 同构



$\overline{G}$

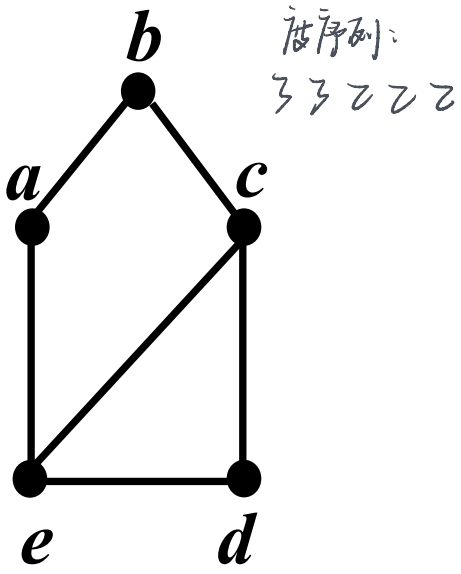
图同构的例子



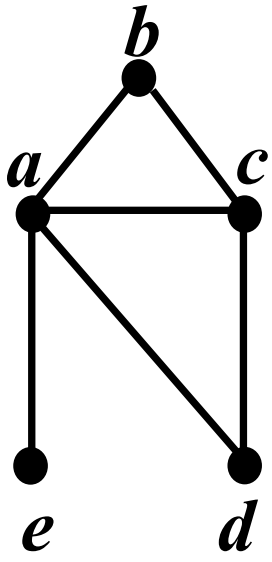


检测两个简单图是否同构

- 图同构下保持的性质称为图不变的
  - 顶点数、度序列、…
- 利用图不变的性质（没有保持）来推断出不同构

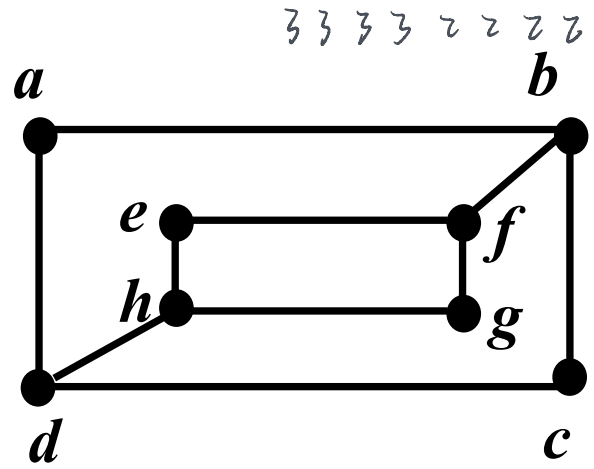


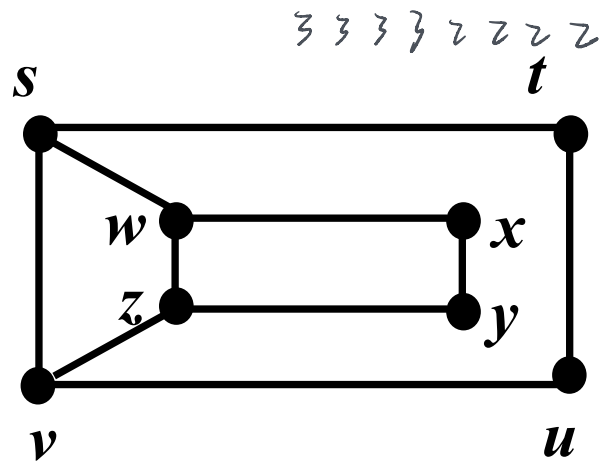
图G



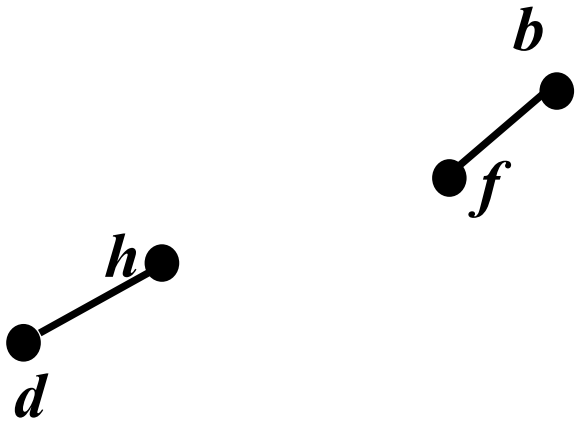
图H

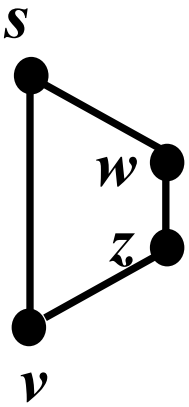
检测两个简单图是否同构



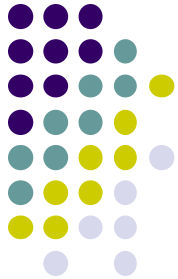


3度顶点导出子图



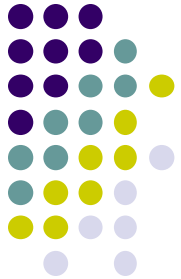


检测两个简单图是否同构



- 若图G与H同构，则对于任意自然数k,
  - 在G或H存在k度顶点的前提下，G的k度顶点导出子图与H的k度顶点导出子图同构
- 若对于任意自然数k，在G或H存在k度顶点的前提下，G的k度顶点导出子图与H的k度顶点导出子图同构，G与H是否同构？
  - 肯定的话，请证明之。
  - 否定的话，请举反例。

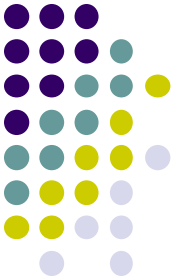
“图同构”问题



- 尚未证明：图同构问题是NP-完全的（NP-Complete）
- 尚未找到多项式时间复杂度的算法
- **Luks, 1983:** $\exp(O(\sqrt{n \log n}))$
- **László Babai, 2017:** $(\exp((\log n)^{O(1)}))$

quasipolynomial time

“子图同构”问题



- 给定简单图G和H，G是否与H的某个子图同构？
- 已经证明：子图同构问题是NP-完全的。
- 那么，对于一些特殊类型的图G呢？
  - K_m
  - C_m

图的连通性

瞿裕忠 教授

南京大学计算机科学与技术系

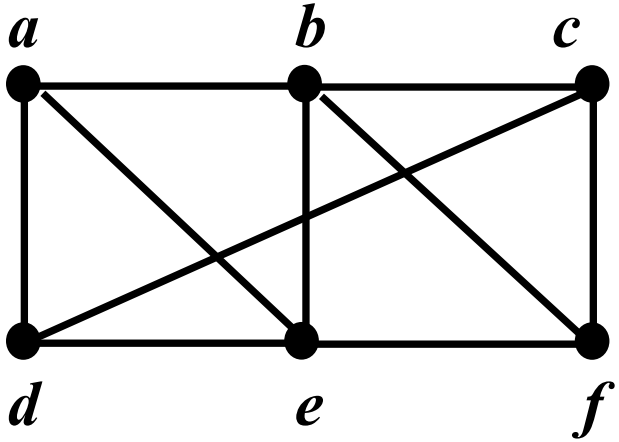
内容提要

- 通路与连通图
  - 通路与回路
  - 无向连通图
- 无向图的连通性
- 有向图的连通性

通路的定义

- 定义：图G中从v_0到v_n的长度为n的通路是G的n条边$e_1,\ldots, e_n$的序列，满足下列性质
  - 存在$v_i \in V(0<i\leq n-1)$，使得v_{i-1}和v_i是e_i的两个端点 $(0<i\leq n)$。
- 相关点
  - 长度为0的通路由单个顶点组成。
  - 不必区分多重边时，可以用相应顶点的序列表示通路。
  - 回路：起点与终点相同，长度大于0。
  - 简单通路： 边不重复，即，$\forall i, j, i\neq j \rightarrow e_i \neq e_j$

通路（举例）

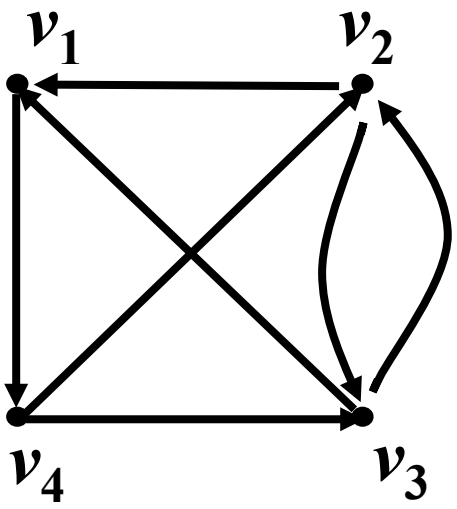


- 简单通路：*a, d, c, f, e*。 长度为4。
- 通路：*a, b, e, d, a, b*。 长度为5。
- 回路：*b, c, f, e, b*。长度为4。
- 不是通路：*d, e, c, b*。

通路的定义（有向图）

- 定义：有向图G中从v_0到v_n的长度为n的通路是G的n条边$e_1,\ldots, e_n$的序列，满足下列性质
  - 存在$v_i \in V(0<i\leq n-1)$,使v_{i-1}和v_i分别是e_i的起点和终点$(0<i\leq n)$
- 相关点
  - 长度为0的通路由单个顶点组成。
  - 不必区分多重边时，可以用相应顶点的序列表示通路。
  - 回路：起点与终点相同，长度大于0。
  - 简单通路： 边不重复，即，$\forall i, j, i\neq j \rightarrow e_i \neq e_j$

通路（举例）

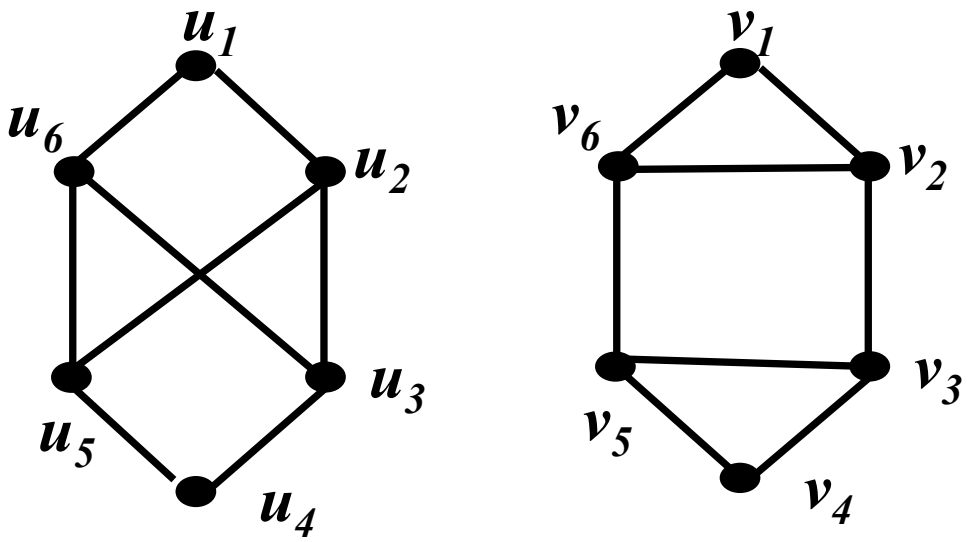


- 简单通路：v_1, v_4, v_2, v_3。 长度为3。
- 通路： $v_2, v_3, v_1, v_4, v_2, v_3$ 。 长度为5。
- 回路： v_2, v_1, v_4, v_2。长度为3。

通路与同构

- 设图G的邻接矩阵为A
  - $(A^k)_{i,j}$: v_i到v_j的长度为k的通路个数($k \geq 1$)
  - $(A^k)_{i,i}$: v_i到v_i的长度为k的回路个数($k \geq 1$)
- 同构图的不变量：长度为k的回路的存在性。
  - $B=U \cdot A \cdot U^{-1} \rightarrow B^k=U \cdot A^k \cdot U^{-1}$（对角线元素之和相等？）

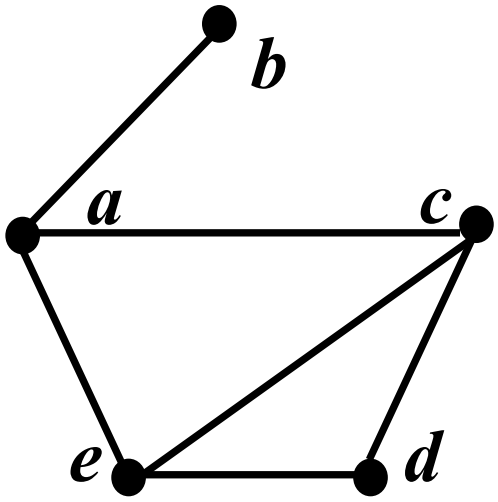
通路与同构



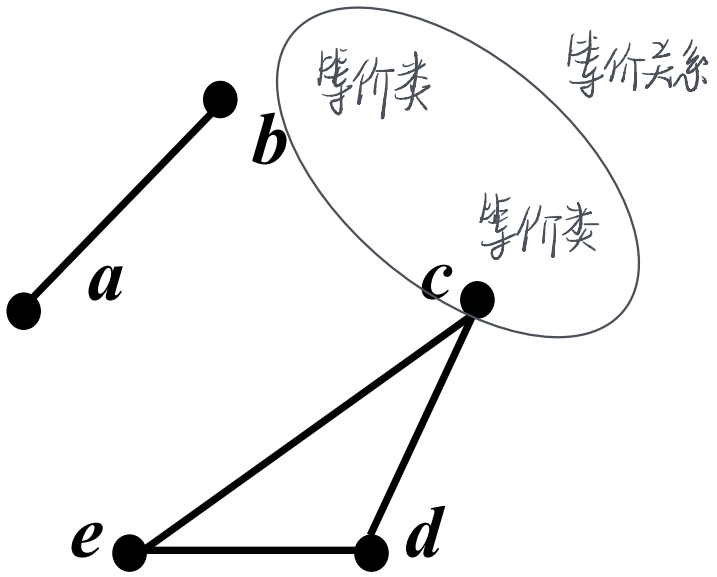
- 若同构，则长度为k的回路个数相同。

无向连通图

- 定义：无向图G称为是连通的，如果G中任意两个不同顶点之间都有通路。



G_1



G_2

连通分支

- 连通分支
  - 极大连通子图
- 每个无向图是若干个互不相交的连通分支的并。
  - “顶点之间存在通路”是一个等价关系，任一等价类上的导出子图即为一个连通分支。
- 若图G中存在从u到v的通路，则一定有从u到v的简单通路。
  - 证明：最短通路必是简单的，事实上，它没有重复顶点。

内容提要

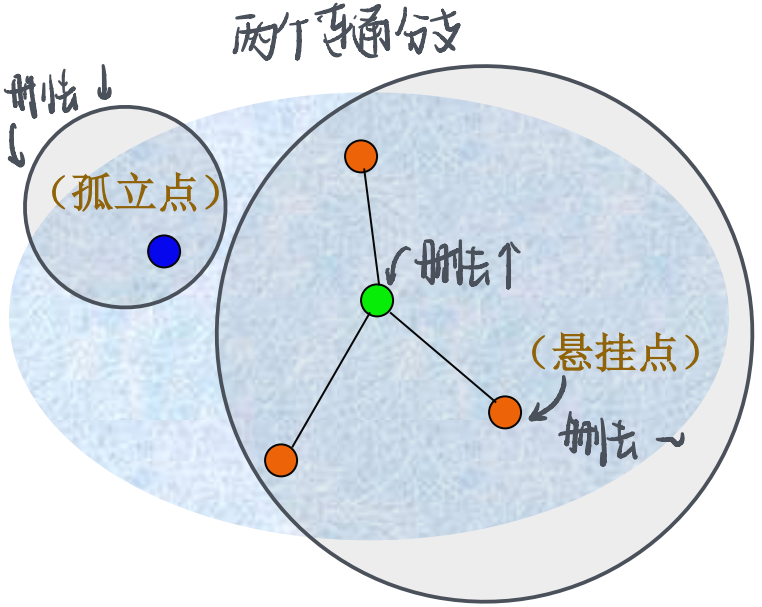
- 图中的通路
- 无向图的连通性
  - 割点、割边
  - 2-连通图、2-边连通图
  - 连通度、边连通度
- 有向图的连通性

点的删除与连通分支数量的增减

- p(G-*v*)(其中*v*是G中的一个顶点)的情况比较复杂

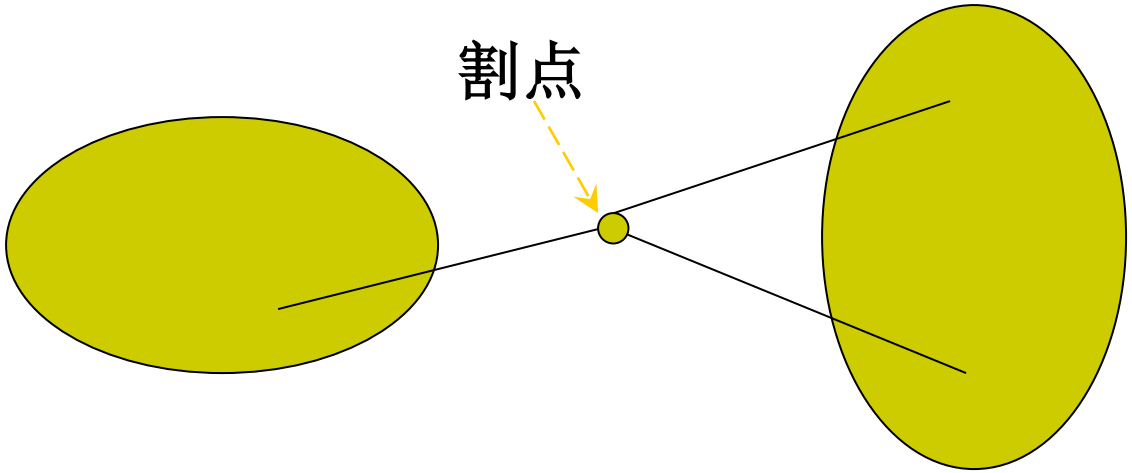
（注意：删除顶点意味着同时删除该点关联的边）

- 可能会……
  - 减少 (删除孤立点)
  - 不变 (例如：删除悬挂点)
  - 增加很多个 (例如：star)



割点

- 定义：G是图, $v \in V_G$, 若$p(G-v)>p(G)$, 则称v是割点



注意：只需考虑割点所在的连通分支，不妨只考虑连通图

关于割点的三个等价命题

- 对于连通图G，以下三个命题等价：

  (1)v是割点。

  (2)存在V-{v}的划分{V_1,V_2}, 使$\forall u \in V_1, w \in V_2$,uw-通路均包含$v$。

  (3)存在顶点u,w($u \neq v$, $w \neq v$)，使得任意的uw-通路均包含v。

- 证明：

  (1)⇒(2) ∵v是割点，G-v至少存在两个连通分支，设其中一个的顶点集是V_1。令V_2=V-($V_1 \cup$ {v}), 则$\forall u \in V_1$, $w \in V_2$, u,w一定在G-v的不同的连通分支中。∴在G中，任何uw-通路必含v。

  (2)⇒(3) 特例。

  (3)⇒(1) G-v中不可能还有uw-通路，∴G-v不连通，∴v是割点。

边的删除与连通分支数量的增加

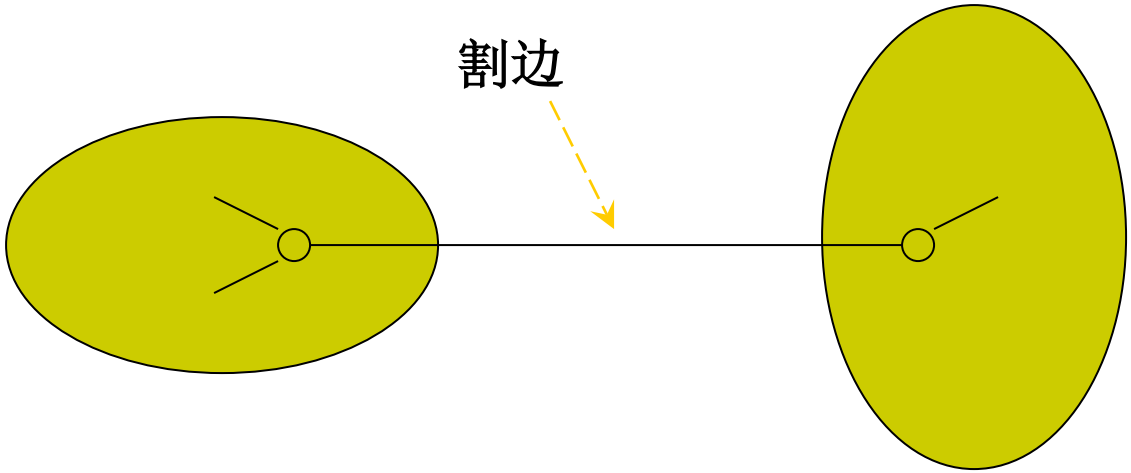
- 设p(G)表示图G中连通分支数，则：

  $p(G) \le p(G-e) \le p(G)+1$，其中$e$是G中任意一条边

  - 删除一条边，不会减少连通分支，最多增加一个；
  - 增加一条边，最多只能将两个连通分支连成一个。

割边

- 设G是图，$e \in E_G$, 若p(G-*e*)>p(G), 则称*e*是G中的割边。



注意：只需考虑割边所在的连通分支，不妨只考虑连通图

有关割边的四个等价命题

- 以下四个命题等价：

(1) e是割边。

(2) 存在V的划分$\{V_1, V_2\}$, 使$\forall u \in V_1, \forall w \in V_2$, uw-通路均包含$e$。

(3) 存在顶点u,w，使得任意的uw-通路均包含e。

(4) e不在G的任一简单回路上。//割点没有相应结论

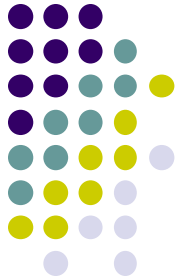
割边与回路

- ***e*是割边当且仅当*e*不在G的任一简单回路上。**
- ***e*不是割边当且仅当*e*在G的某个简单回路上。**
- 证明：

  ⇐假设*e*在某个简单回路C上，易证： *e*不是割边。

  ⇒假设*e*=*xy*不是割边。则G-*e*仍连通，设P是G-*e*中的*xy*-通路，
  不妨假设是简单通路，P中不含*e*, 则：P+*e*是G中的简单回路。

连通图“连接的牢固度”不一样



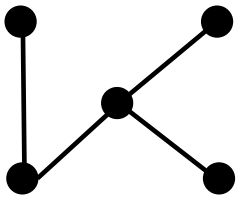
- **2-连通图**
  - 使得该图不连通，至少删除2个顶点。//没有割点
- **2-边连通图**
  - 使得该图不连通，至少删除2个条边。//没有割边

内容提要

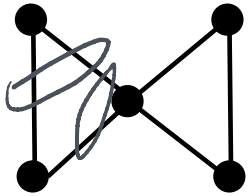
- 图中的通路
- 无向图的连通性
  - 割点、割边
  - 2-连通图、2-边连通图
  - 连通度、边连通度
- 有向图的连通性

连通图“连接的牢固度”不一样

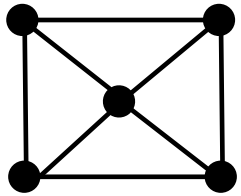
- 图G_1中删除任意一条边都不连通了。
- 图G_2则至少删除两条边，或删除中间那个顶点，才不连通。
- 图G_3删除任意一个点依然连通。
- 图G_4至少要删除四条边才可能不连通，且不可能通过删除顶点使其不连通。



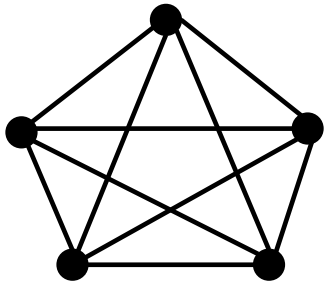
G_1



G_2



G_3



G_4

图的连通度

对非平凡图，删除足够多的顶点，变成不连通图或平凡图。

- 定义：使非平凡连通图G成为不连通图或者平凡图需要删除的最少顶点数称为图G的(点)连通度，记为κ(G)。

  备注：这并不意味着任意删除κ(G)个点就使该图不连通

  约定：不连通图或平凡图的连通度为0，而$\kappa(K_n)=n-1$

- 若图G的连通度不小于k ($\kappa(G)\geq k$), 则称G是k-连通图；

  k-连通图：删除少于k个顶点，它依然连通。

  $\kappa(G)=k$： k-连通图，且存在k个顶点，删除它们就不连通。

图的边连通度

对非平凡图，删除足够多的边，变成不连通图或平凡图。

- 使非平凡连通图G变成不连通，需要删除的最少边数称为图G的边连通度，记为λ(G)。

  备注：这并不意味着任意删除λ(G)条边就使该图不连通

  约定：不连通图或平凡图的边连通度为0，而$\lambda(K_n)=n-1$

- 若图G的边连通度不小于k ($\lambda(G)\geq k$),, 则称G是k-边连通图。

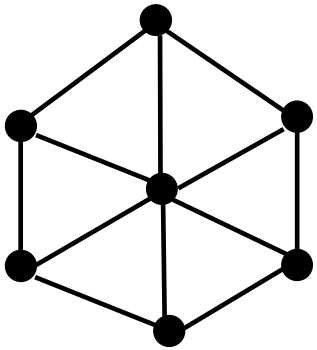
  k-边连通图：删除少于k条边，它依然连通。

  $\lambda(G)=k$： k-边连通图，且有k条边，删除它们就不连通。

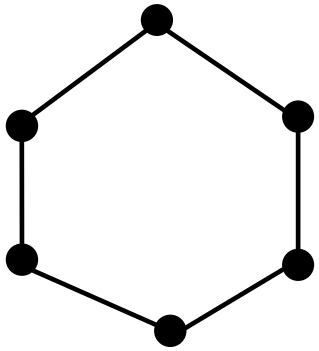
关于连通度的例子

- W_6(轮)：$\kappa=\lambda=3=\delta$
- C_6(圈)：$\kappa=\lambda=2=\delta$
- $K_{2,3}$(完全二部图)：$\kappa=\lambda=2=\delta$
- G：$\kappa=1$，$\lambda=2$，$\delta=3$

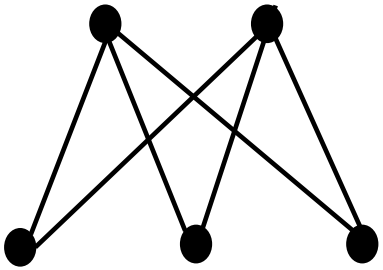
δ表示图中最小顶点度



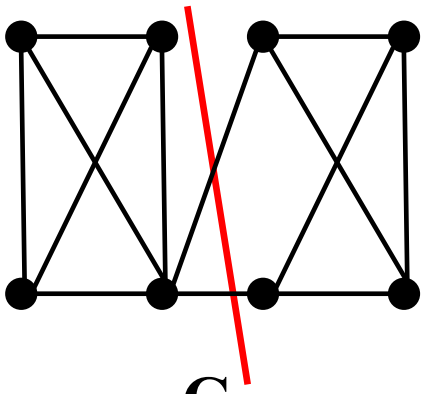
W_6



C_6



$K_{2,3}$



G

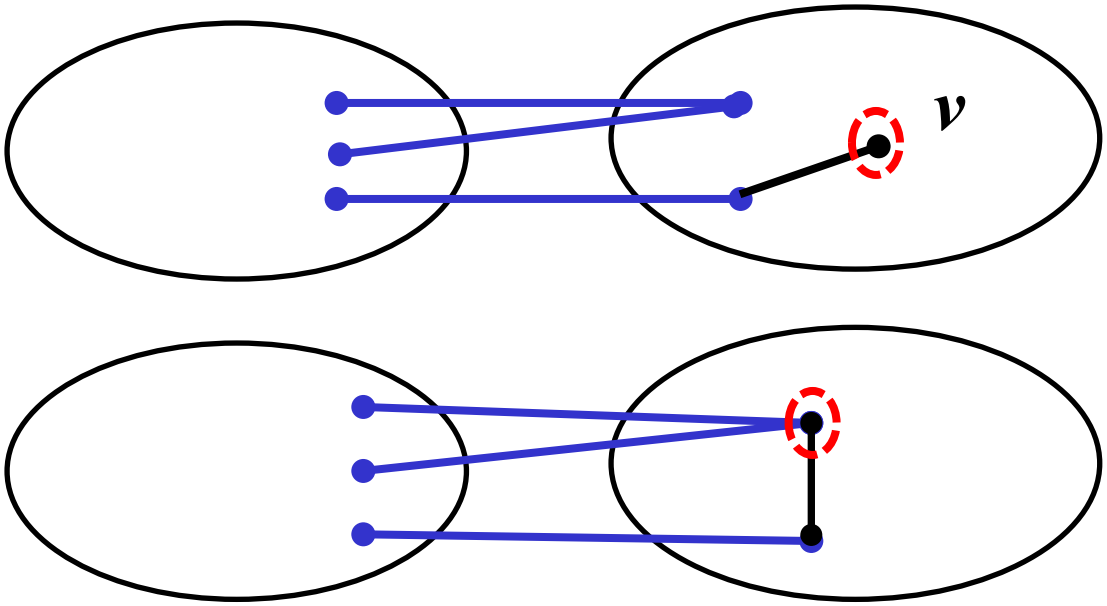
连通度的上限（续）

- 设G=(V, E)是非平凡的简单图, 则 $\kappa(G) \leq \lambda(G) \leq \delta(G)$
- 易证$\lambda(G) \leq \delta(G)$。
- 下面证明$\kappa(G) \leq \lambda(G)$。设F为E的极小子集使得G-F不连通，只需证明$\kappa(G) \leq |F|$。

  （下面分情形加以证明）

连通度的上限（续）

- 若G中存在不与F中的边相关联的点，设为v。令C为G-F中v所在的连通分支。F中的任一边，其两个端点不会都在C中（F的极小性）。C中与F中边相关联的顶点（集合）分隔v与G-C，$\kappa(G) \leq |F|$。



$d_G(v) \leq |F|$

连通度的上限（续）

- 若G中的各顶点均和F中的某条边关联。对任意顶点v,令C是G-F中包含v的连通分支。考虑v的任一邻居w。若w在C中，则w必定和F中的某条边关联；若w在G-C中，则边vw属于F。因此，$|N(v)| \le |F|$, 即$d_G(v) \le |F|$.

  （1）若$V-N(v)-v \neq \Phi$, 则删除$N(v)$后, v和$V-N(v)-v$不连通, 从而$\kappa(G) \le |F|$。

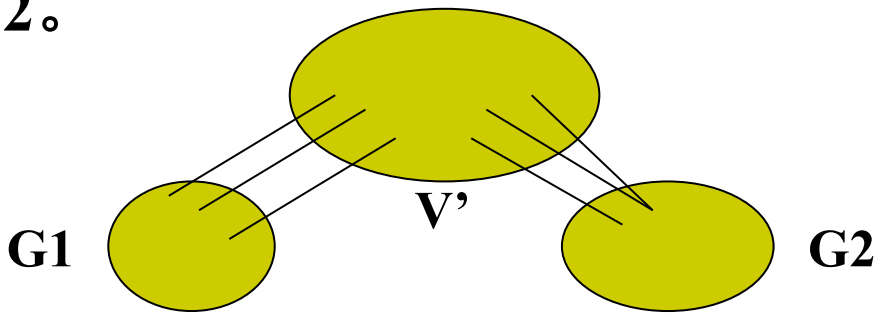
  （2）若$V-N(v)-v=\Phi$,则取其它节点以满足条件（1）。若所有节点均有$V-N(u)-u=\Phi$，则图G为完全图，从而$\kappa(G)=\lambda(G)=|G|-1$。

达到连通度上限的图

- 设G是简单图，$|G|=n\geq 3$, 且$\delta_G \geq n-2$, 则$\kappa(G)=\delta_G$

  (注意：任一点最多与一个点不相邻，此时$\lambda(G)$也必为δ_G)

- 证明：设$V' \subseteq V_G$，使得$G-V'$含两个连通分支G_1，G_2，不妨设$|G_1| \leq |G_2|$，则$|G_1| \leq (n-|V'|)/2$。



- $\delta_G \leq (|G_1|-1)+|V'| \leq (n-|V'|)/2 + |V'| -1$
- $2\delta_G \leq n-2+|V'| \leq \delta_G + |V'|$, 所以 $|V'| \geq \delta_G$
- 所以 $\kappa(G) \geq \delta_G$

连通度与点不相交的通路

(基本观察：对图G中任意两点*u*,*v*, 如果有*k*条顶点不相交的*uv*-通路连接*u*和*v*, 那么要使*u*,*v*不连通，至少须删除*k*个顶点。)

- **Whitney定理**

  图G(|G|≥3)是2-连通图 当且仅当 G中任意两点被至少2条除端点外顶点不相交的路径所连接。

注意：“G中任意两点被至少2条除端点外顶点不相交的路径所连接”等价于“任意两点均处在某个初级回路中”。

Whitney定理的证明

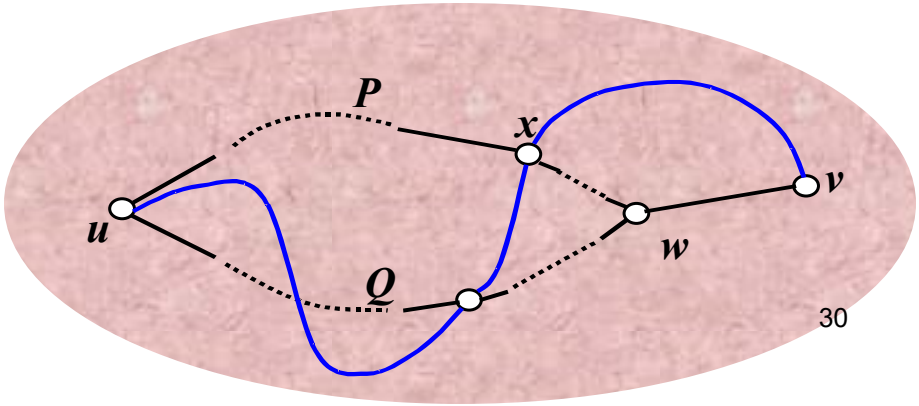
- ⇒ 设u,v是图G中的任意两点。下面对距离$d(u,v)$进行归纳证明。

  当$d(u,v)=1$, $uv \in E_G$, 因为G是2-连通图，G-uv仍连通，则G中除边uv外，必有另一条不含uv的路径。

  假设当$d(u,v) < k$时，至少存在两条中间点不相交的通路。

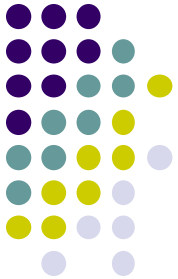
  若$d(u,v)=k$, 设u,v间的一条最短路径是$u\ldots wv$。则$d(u,w)<k$, 由归纳假设u,w之间存在两条中间点不相交的路径，设为P, Q。因为G是2-连通图，G-w中仍有(不含w的)uv-路径P'，且它与P, Q有公共点(u就是一个)。

  假设这样的公共点中距离v最近的是x(不妨假设它在P上)，则$Q+wv$边以及P上的ux-段+P'上的xv-段是u,v之间两条中间点不相交的通路。



- ⇐ 充分性显然

连通性的一般性质

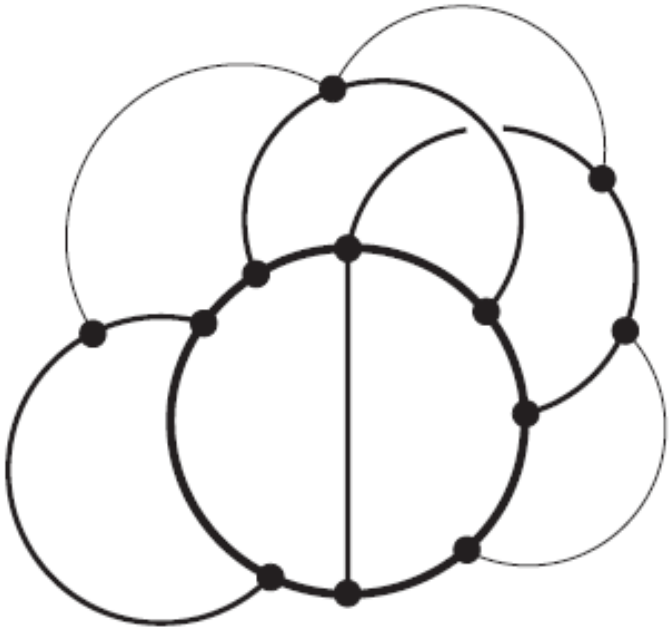


- **Menger定理（Whitney定理的推广）**
  - 图G是*k*-连通图 当且仅当 G中任意两点被至少*k*条除端点外顶点不相交的路径所连接。
  - 图G是*k*-边连通图 当且仅当 G中任意两点被至少*k*条边不相交的路径所连接。

2-连通图

- 命题. 一个图是2-连通的 ⇔

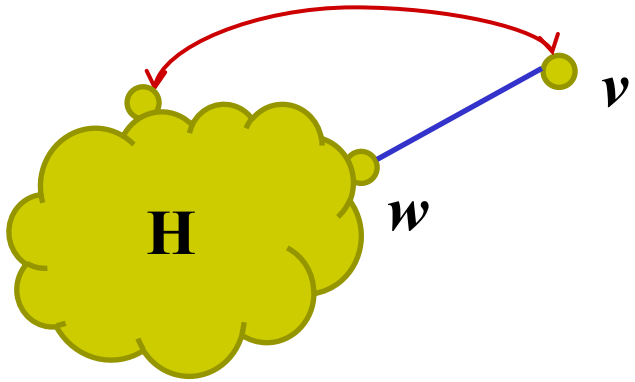
  它是一个回路(cycle), 或者在H(已有的2-连通图)上依次增加 H-path.



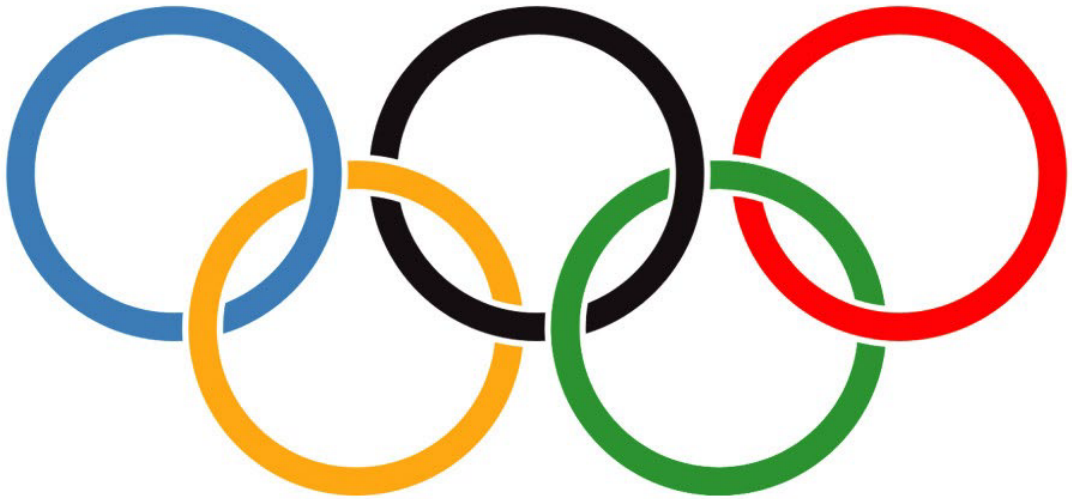
2-连通图

- 证明. 充分条件显然成立. 下证必要条件.

设G是2-连通的. G 必包含回路C, 设 H 是包含C，依次增加H-Path得到的极大子图. H必是G的导出子图. 倘若$H \neq G$, 则存在$v \in G-H$, $w \in H$, $vw \in G$. G是 2-连通的, G-w连通, v到H有路径P, wvP是H-Path, 矛盾.



2-连通图

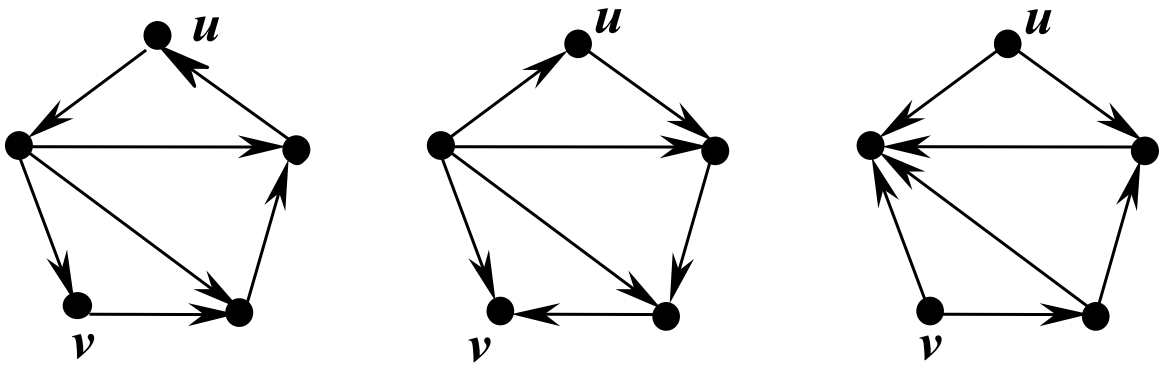


内容提要

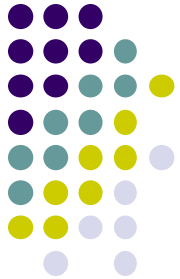
- 图中的通路
- 无向图的连通性
- 有向图的连通性
  - 无向图的定向

有向图的连通性

- 若将有向图D各边的方向去掉，所得的无向图(称为D的底图)连通，则D称为弱连通有向图。(见下右图: 既无uv-, 又无vu-有向通路)
- $\forall u, v \in V_D$,存在一条 (u,v)-有向通路或者(v,u)-有向通路，则D称为单连通有向图。 (见下中图: 有uv-, 但无vu-有向通路)
- $\forall u, v \in V_D$,均存在 (u,v)-有向通路和(v,u)-有向通路，则D称为强连通有向图。 (见下左图)



强连通的充分必要条件



- 有向图D是强连通的当且仅当D中的所有顶点在同一个有向回路上。
  - 证明：

⇐ 显然

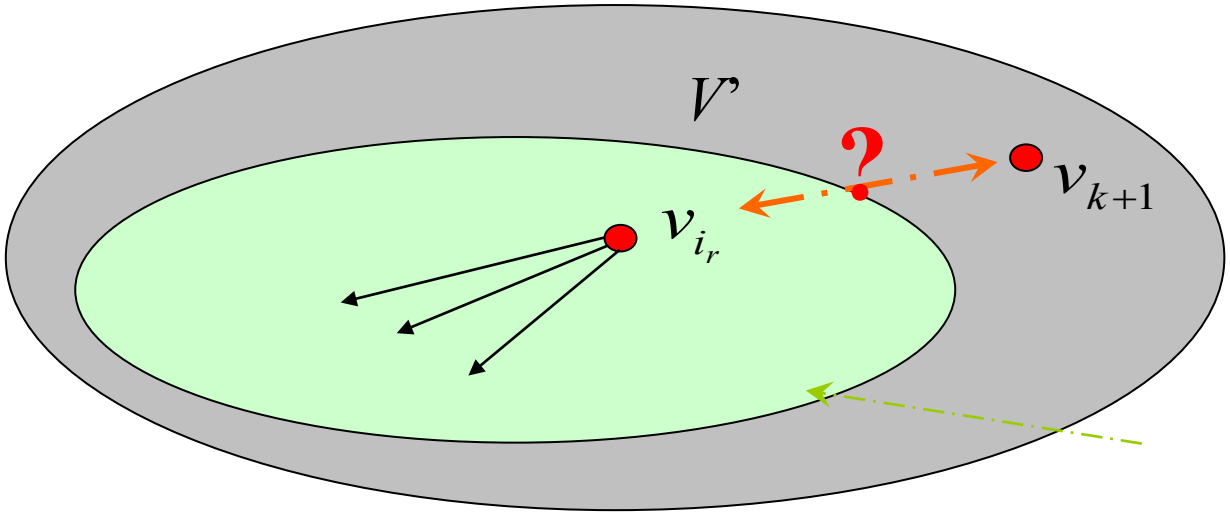
⇒ 设$V_D=\{v_1,v_2,\ldots,v_n\}$，令$\Gamma_i$是$v_i$到$v_{i+1}$的有向通路$(i=1,\ldots,n-1)$，令$\Gamma_n$是$v_n$到$v_1$的有向通路，则$\Gamma_1$，$\Gamma_2,\ldots\Gamma_n$依次连接是包含$D$中一切顶点的回路。

单向连通图中处处可达的顶点

- 若有向图D是单向连通，则$\forall$非空集$V' \subseteq V_D$，$\exists v' \in V'$，使得v'可达V'中的所有顶点(规定顶点到其自身是可达的)。

  注意：当V'足够小，上述条件一定成立。

- 证明：（注意：按照非空子集的大小进行归纳证明）



单向连通的充分必要条件

- 有向图D是单向连通的当且仅当D中的所有顶点在同一个有向通路上。

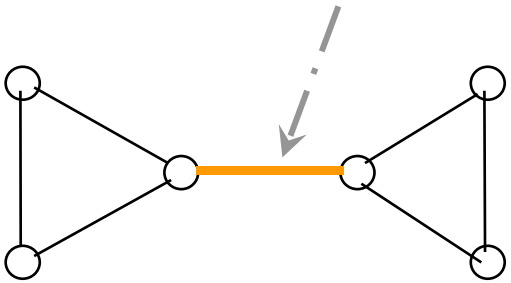
  充分性显然，下面证明必要性

  - 设$V_D=\{v_1,\ldots v_n\}$，令$V_1=V_D$，则V_1中存在可达所有顶点的顶点，不妨假设它就是v_1，令$V_{i+1}=V_i-\{v_i\}$，其中i=1,2,…,n-1；而且诸V_i中均有可达该子集中所有顶点的顶点(不妨假设其就是v_i)，于是：将诸v_iv_{i+1}-通路连接起来即包含D中所有顶点的有向通路。

无向图的边定向

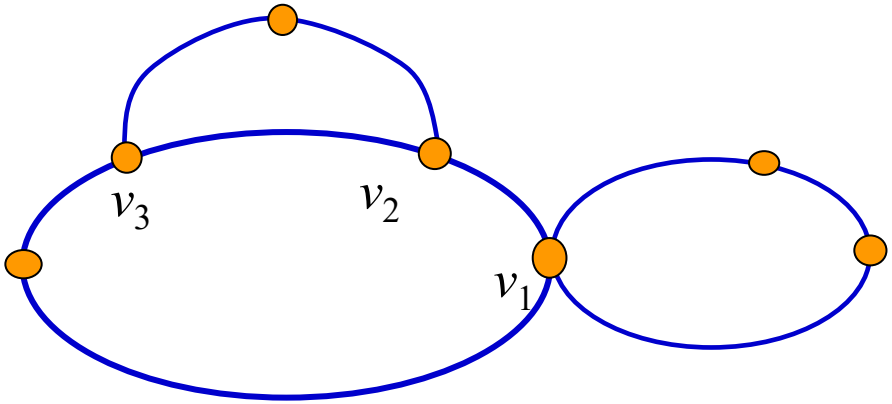
问题：何种道路网可以用规定单行道的办法来改善交通？

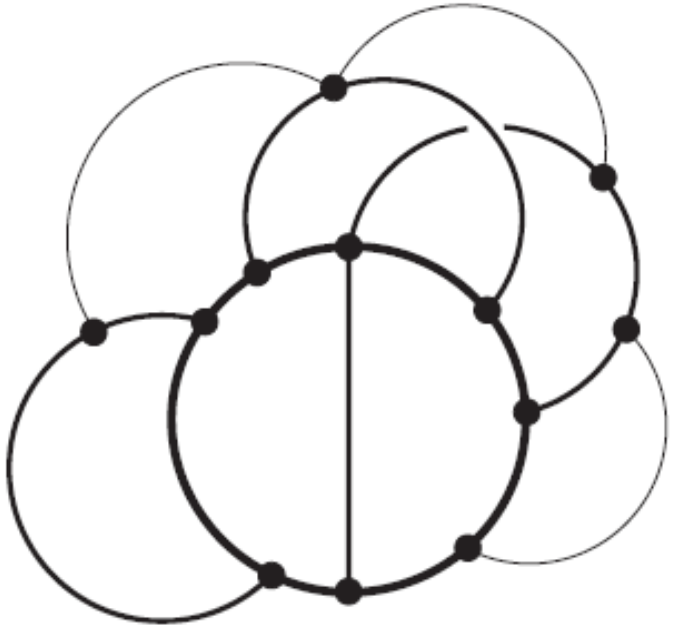
- 在图模型中，该问题表述为：什么样的无向图G可通过边定向成强连通有向图 .
  - 显然G中不能有割边，否则定向后，割边端点之间不能双向可达。



G的“2-边连通”是个**必要**条件，它是否也是**充分**条件呢？

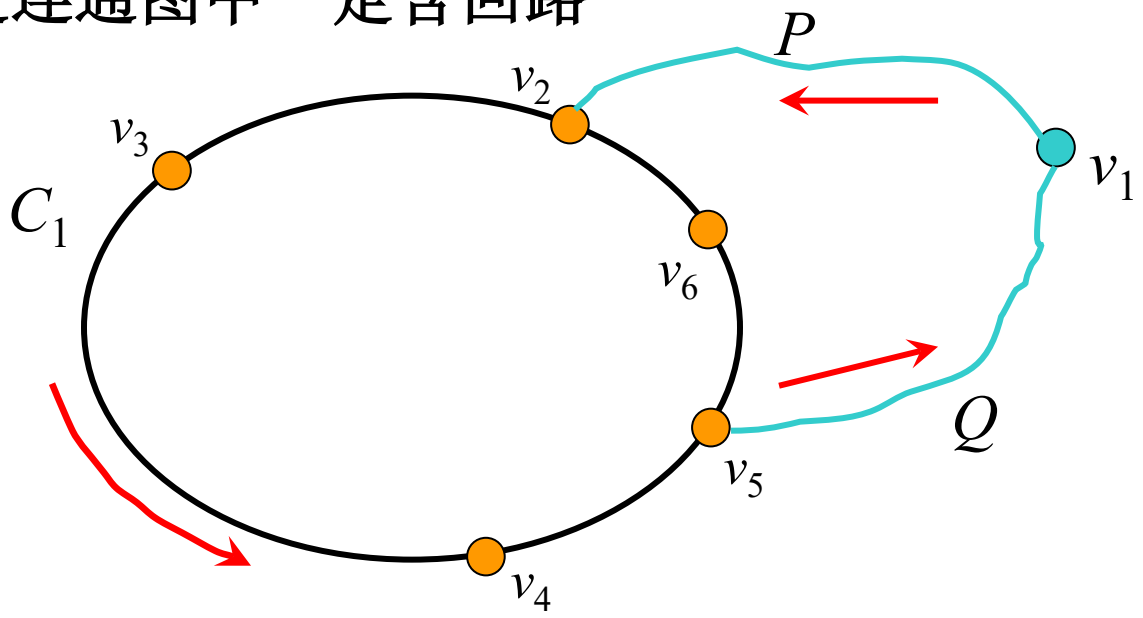
2-边连通与2-连通（无向图）





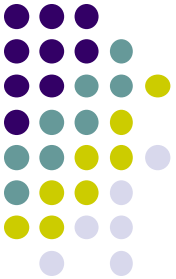
2-边连通无向图的边定向

2-边连通图中一定含回路



构作有向通路$C_2=C_1+QP$,..., 总会得到包括图中所有点的强连通有向图。顶点穷尽后，余下的边任意定向。

无向图边定向算法



- 输入：无自环2-边连通无向图G（设$V_G=\{v_1,v_2,\cdots,v_n\}$）
- 输出：以G为底图的强连通有向图
- 过程：

(1) 令$V_1=\{v_1\}$, i=1。

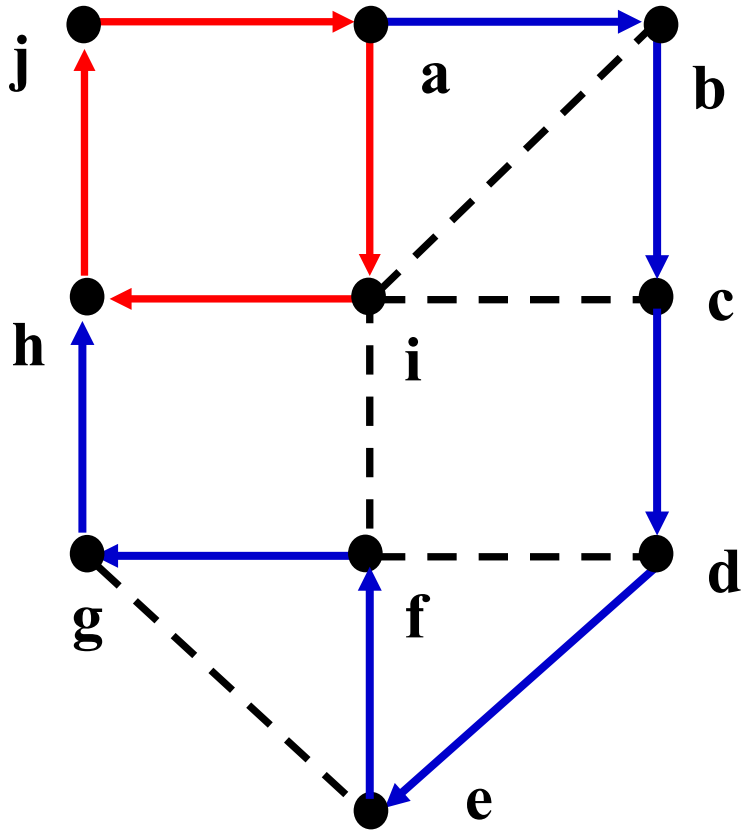
(2) 若$V_i=V_G$, 对未定向边任意定向，算法结束。否则转3。

(3) 取边 $v_{i_0}v_{i_1}$, 使得 $v_{i_0}\in V_i, v_{i_1}\in V_G-V_i$ (一定可取到所要的边)。从 $v_{i_0}v_{i_1}$ 开始找一条初级通路或回路，满足始点和终点在V_i中，而中间点均在V_G-V_i中，加方向使之成为有向通路。

(4) $V_{i+1}=V_i \cup$ {**上述通路或回路中所有中间点**}, 转2。

无向图边定向算法(续)

- 示例



参考文献

1. 高随祥. 《图论与网络流理论》，高等教育出版社
2. Reinhard Diestel. Graph Theory. Springer, Heidelberg, 2005. (Section 1.3 and section 3.1)

欧拉图

瞿裕忠 教授

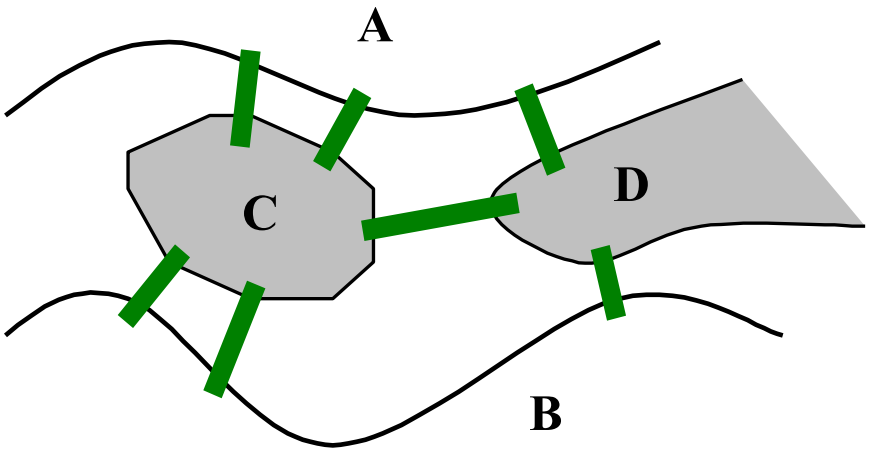
南京大学计算机科学与技术系

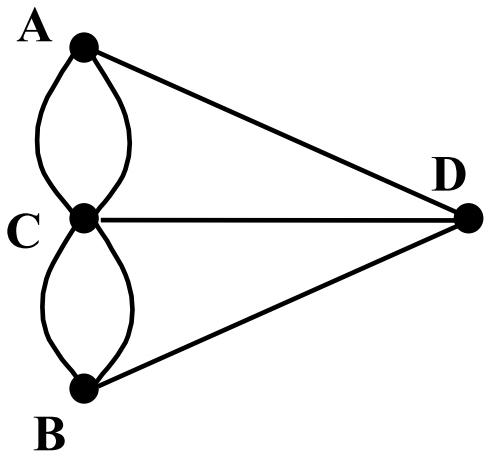
内容提要

- 欧拉通路/回路
- 欧拉图的充要条件
- 半欧拉图的充要条件
- 构造欧拉回路的Fleury算法
- 随机欧拉图

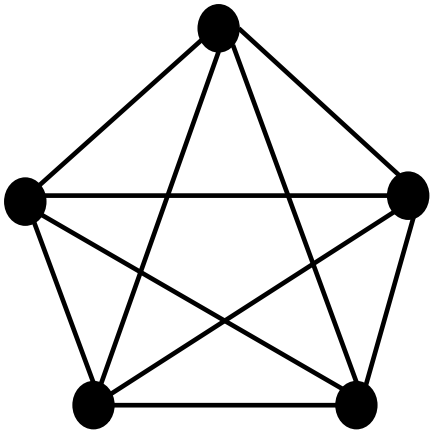
Königsberg七桥问题

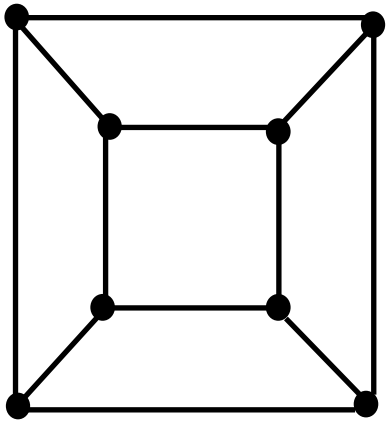
- 问题的抽象：
  - 用顶点表示对象-“地块”
  - 用边表示对象之间的关系-“有桥相连”
  - 原问题等价于：“右边的图中是否存在包含每条边一次且恰好一次的回路？”

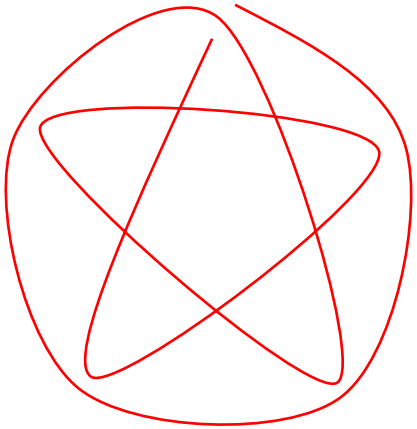




“一笔划”问题







?

欧拉通路和欧拉回路

边不重复

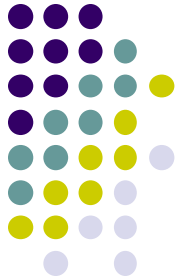
- 定义：包含图（无向图或有向图）中每条边的简单通路称为*欧拉通路*。

注意：欧拉通路是简单通路（边不重复），但顶点可重复

- 定义：包含图中每条边的简单回路称为*欧拉回路*。
- 如果图G中含欧拉回路，则G称为*欧拉图*。如果图G中有欧拉通路，但没有欧拉回路，则G称为*半欧拉图*。

//备注：通常假设G是连通的。

欧拉图中的顶点度数



连通图G是欧拉图 当且仅当 G中每个顶点的度数均为偶数。

- 证明：

⇒设C是G中的欧拉回路，则$\forall v \in V_G$, $d(v)$必等于v在C上出现数的2倍(起点与终点看成出现一次)。

⇐可以证明：

（1）G中所有的边可以分为若干个相互没有公共边的简单回路。

（2）这些回路可以串成一个欧拉回路。

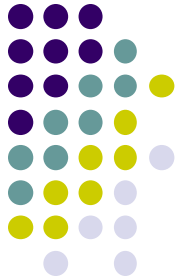
全偶度图中的回路

- 若图G中任一顶点均为偶度点，则G中所有的边包含在若干个相互没有公共边的简单回路中。
- 证明：根据G的边数m进行归纳证明。
  - 当m=1, G是环，结论成立。
  - 对于$k\geq 1$，假设当$m\leq k$时结论成立。
  - 考虑$m=k+1$的情况：注意$\delta_G\geq 2$, G中必含简单回路，记为C，令$G'=G-E_C$，设G'中含s个连通分支，显然，每个连通分支内各点均为偶数(包括0)，且边数不大于k。则根据归纳假设，每个非平凡的连通分支中所有边含于没有公共边的简单回路中，注意各连通分支以及C两两均无公共边，因此，结论成立。

若干小回路串成欧拉回路

- 若连通图G中所有的边包含在若干个相互没有公共边的简单回路中，则G中含欧拉回路。
  - 证明：对G中简单回路个数d施归纳法。当d=1时显然。
  - 假设$d \le k(k \ge 1)$时结论成立。考虑$d=k+1$.
  - 按某种方式对k+1个简单回路排序，令G'=G-E(C_{k+1})，设G'中含s个连通分支，则每个非平凡分支所有的边包含在相互没有公共边的简单回路中，且回路个数不大于k。由归纳假设，每个非平凡连通分支G_i均为欧拉图，设其欧拉回路是C_i'。因G连通，故C_{k+1}与诸C_i'都有公共点。
  - G中的欧拉回路构造如下：从C_{k+1}上任一点(设为v_0)出发遍历C_{k+1}上的边，每当遇到一个尚未遍历的C_i'与C_{k+1}的交点(设为v_i'), 则转而遍历C_i'上的边，回到v_i'继续沿C_{k+1}进行。

关于欧拉图的等价命题



- 设G是非平凡连通图，以下三个命题等价：

  (1) G是欧拉图。

  (2) G中每个顶点的度数均为偶数。

  (3) G中所有的边包含在若干个相互没有公共边的简单回路中。

半欧拉图的判定

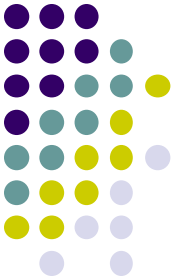
- 设G是连通图，G是半欧拉图 *当且仅当* G恰有两个奇度点。
  - 证明:

⇒ 设*P*是G中的欧拉通路(非回路)，设*P*的始点与终点分别是*u*,*v*, 则对G中任何一点*x*, 若*x*既非*u*也非*v*，则*x*的度数等于在*P*中出现次数的2倍，而*u*,*v*的度数则是它们分别在*P*中间位置出现的次数的两倍再加1。

⇐ 设G中两个奇度顶点是*u*,*v*, 则G+*uv*是欧拉图，设欧拉回路是C, 则C中含*uv*边，∴C-*uv*是G中的欧拉通路。

(若一笔画出一个半欧拉图，则必以两个奇度顶点为始点和终点。)

有向欧拉图



- 有向图中含所有边的有向简单回路称为有向欧拉回路。
- 存在有向欧拉回路的有向图称为有向欧拉图。

下面的等价命题可以用于有向欧拉图的判定：

- 若G是弱连通的有向图（看作无向图连通），则下列命题等价：
  - G中存在有向欧拉回路。
  - G中任一顶点的入度等于出度。
  - G中所有边位于若干条相互没有公共边的有向简单回路中。

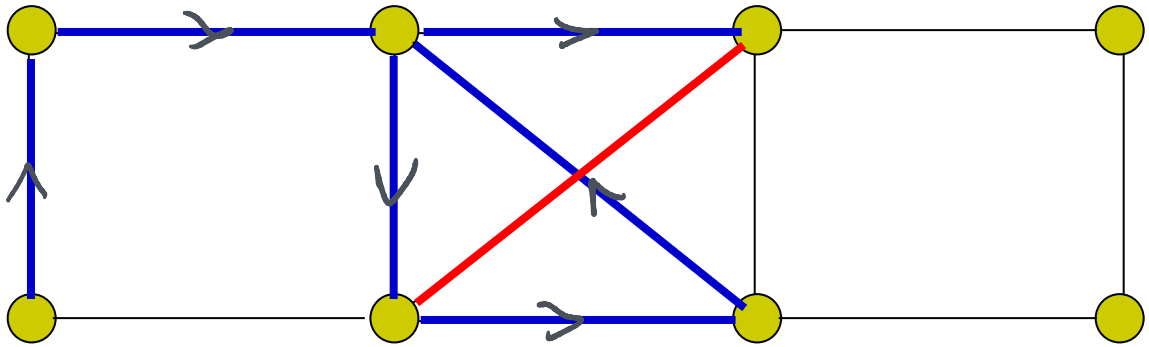
(证明与无向欧拉图类似。)

内容提要

- 欧拉通路/回路
- 欧拉图的充要条件
- 半欧拉图的充要条件
- **构造欧拉回路的Fleury算法**
- **随机欧拉图**

构造欧拉回路

思想：在画欧拉回路时，画过的边不能再用。因此，在构造欧拉回路过程中的任何时刻，假设将画过的边删除，剩下的边必须仍在同一连通分支当中。

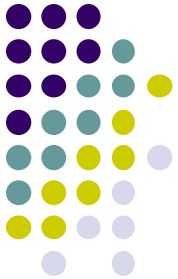


构造欧拉回路

- **Fleury（弗勒里）算法**
  - 输入：欧拉图G
  - 输出：简单回路$P = v_0e_1v_1e_2,\ldots,e_iv_ie_{i+1},\ldots,e_mv_m$, 其中包含了$E_G$中所有的元素。

1. 任取$v_0 \in V_G$, 令$P_0=v_0$;
2. 设$P_i=v_0e_1v_1e_2,\ldots,e_iv_i$, 按下列原则从$E_G-\{e_1,e_2,\ldots,e_i\}$中选择$e_{i+1}$。
   (a) e_{i+1}与v_i相关联;
   (b) 除非别无选择，否则e_{i+1}不应是$G-\{e_1,e_2,\ldots,e_i\}$中的割边。
3. 反复执行第2步，直到无法执行时终止。

Fleury算法的证明



- 算法的终止性显然。
- 设算法终止时，$P_m = v_0e_1v_1e_2,\ldots,e_iv_ie_{i+1},\ldots,e_mv_m$,
- 其中诸e_i互异是显然的。只须证明：

  (1) $v_0=v_m$ (即P_m是回路)

  (2) P_m包括了G中所有的边

  令$G_i=G-\{e_1,e_2,\ldots,e_i\}$

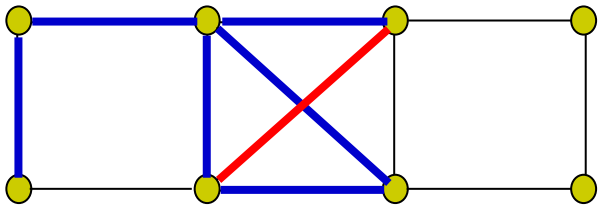
  (1) 假设$v_0\neq v_m$。由算法终止条件，在G_m中已没有边与v_m相关联。假设除最后一次外，v_m在P_m中出现k次，则v_m的度数是$2k+1$, 与G中顶点度数是偶数矛盾。

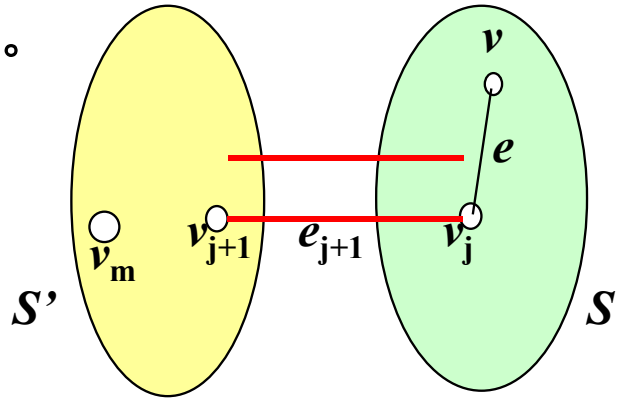
Fleury算法的证明(续)

(2) 假设P_m没有包括G中所有的边，令G_m中所有非零度顶点集合为S（非空）, 令$S'=V_G-S$, 则$v_m \in S'$。

考察序列$e_1,\ldots e_j,e_{j+1},\ldots,e_m$。假设j是满足$v_j \in S$, 而$v_{j+1} \in S'$的最大下标。 如果没有这样的j，G就不连通，矛盾。另外，e_{j+1}一定是G_j中的割边。

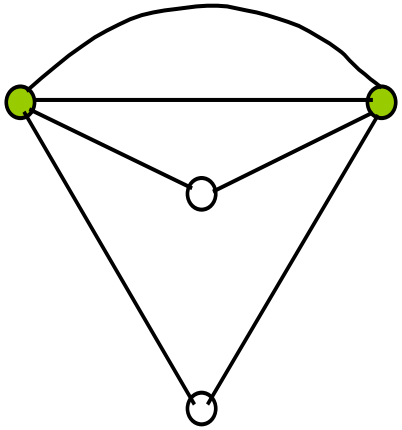
令e是在G_j中与v_j相关联的异于e_{j+1}的边(非零度点一定有)，根据算法选择e_{j+1}(割边)的原则，e也一定是割边。但是，G_m中任意顶点的度数必是偶数，e在G_m中的连通分支是欧拉图，e在G_m的某个欧拉回路中，不可能是G_j的割边。矛盾。





附：随机欧拉图

- 设G是欧拉图，$v \in V_G$，从v开始，每一步从当前点所关联边中随机选边，均可构造欧拉回路，则G称为以v为始点的随机欧拉图。
- 注意，若G是以v为始点的随机欧拉图，则任何一个以v为始点的不包含G中所有边的回路都应该能扩充成欧拉回路。反之，若G不是以v为始点的随机欧拉图，则一定存在已经包含了v所关联的所有边，却未包含G中所有边的简单回路。



随机欧拉图的判定

- 欧拉图G是以*v*为始点的随机欧拉图*当且仅当* G中任一回路均包含*v*。

  ⇒ 若G是以*v*为始点的随机欧拉图，*假设有回路C不包含v*. 令G‘=G-C, (G’可能不连通)，G’中包含*v*的那个连通分支一定是欧拉图，相应的欧拉回路包含了*v*关联的所有边，但不包含G中的所有边，与G是以*v*为始点的随机欧拉图矛盾。

  ⇐ 若欧拉图G中任意回路均包含*v*。假设G不是以*v*为始点的随机欧拉图，则一定存在已经包含了*v*所关联的所有边，却未包含G中所有边的简单回路C，假设*e*是不在C中的一条边，*e*的端点必异于*v*，设一个是*u*。令从G中删除C中所有边的图为G’，显然在G’中*v*是孤立点。而包含*u*的连通分支是欧拉图，因此*u*必包含在一回路中，但此回路不含*v*，矛盾。 (易推知：欧拉图G是以任一顶点为始点的随机欧拉图 当且仅当G本身是一个初级回路)

哈密顿图

瞿裕忠 教授

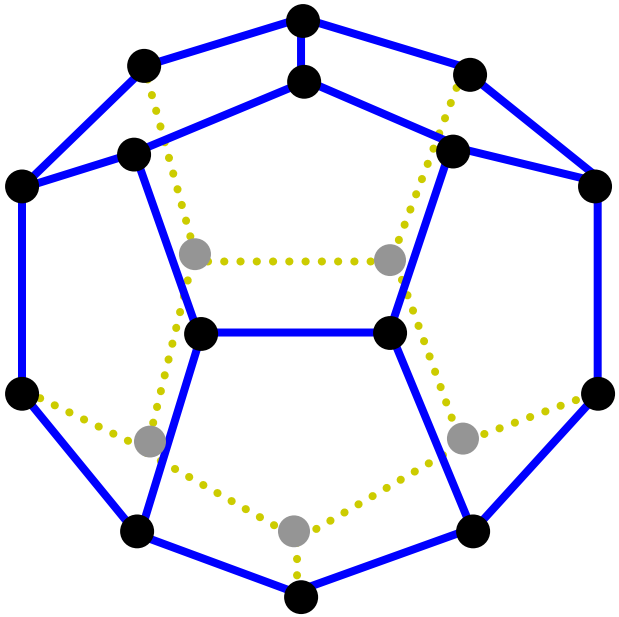
南京大学计算机科学与技术系

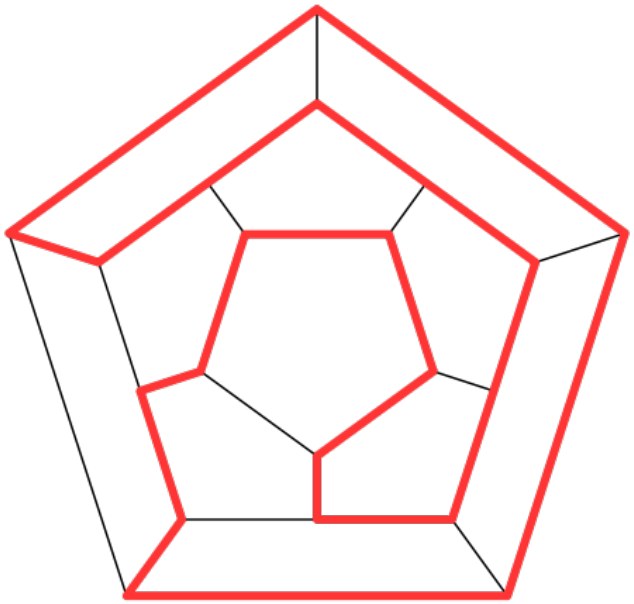
内容提要

- 哈密顿通路/回路
- 哈密顿图的必要条件
- 哈密顿图的充分条件
- 哈密顿图的应用
- 竞赛图与有向哈密顿通路

周游世界的游戏

沿着正十二面体的棱寻找一条旅行路线, 通过每个顶点恰好一次，回到出发点. **(Hamilton 1857)**





Hamilton通路/回路

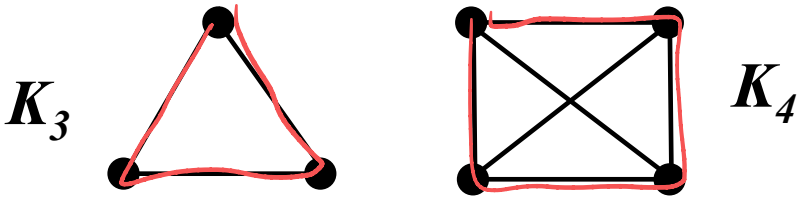
- G中Hamilton通路
  - 包含G中所有顶点
  - 通路上各顶点不重复
- G中Hamilton回路
  - 包含G中所有顶点
  - 除了起点与终点相同之外，通路上各顶点不重复。
- Hamilton通路问题可转化为Hamilton回路问题
  - $G'=G*K_1$

Hamilton回路的基本特性

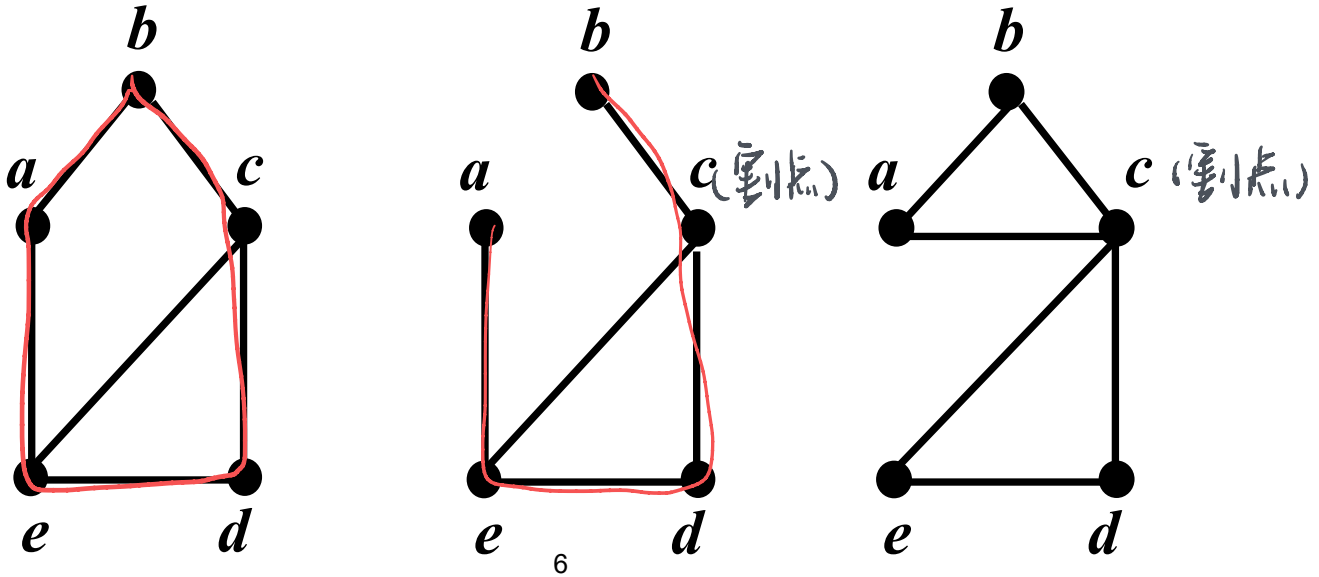
- **Hamilton回路:无重复地遍历（游走）图中诸点,**

  Euler回路:无重复地遍历（游走）图中诸边。
- **若图中有*n*个顶点, 则Hamilton回路恰有*n*条边。**
- **设图G中有一顶点的度大于2, 若有Hamilton回路, 则只用其中的两条边。**
- **若图G中有一顶点的度为1, 则无Hamilton回路。**
- **注：Hamilton回路问题主要针对简单图。**

Hamilton回路的存在性问题



$K_n(n\geq 3)$有Hamilton回路



一个基本的必要条件

- 如果图G=(V, E)是Hamilton图，则对V的任一非空子集S，都有

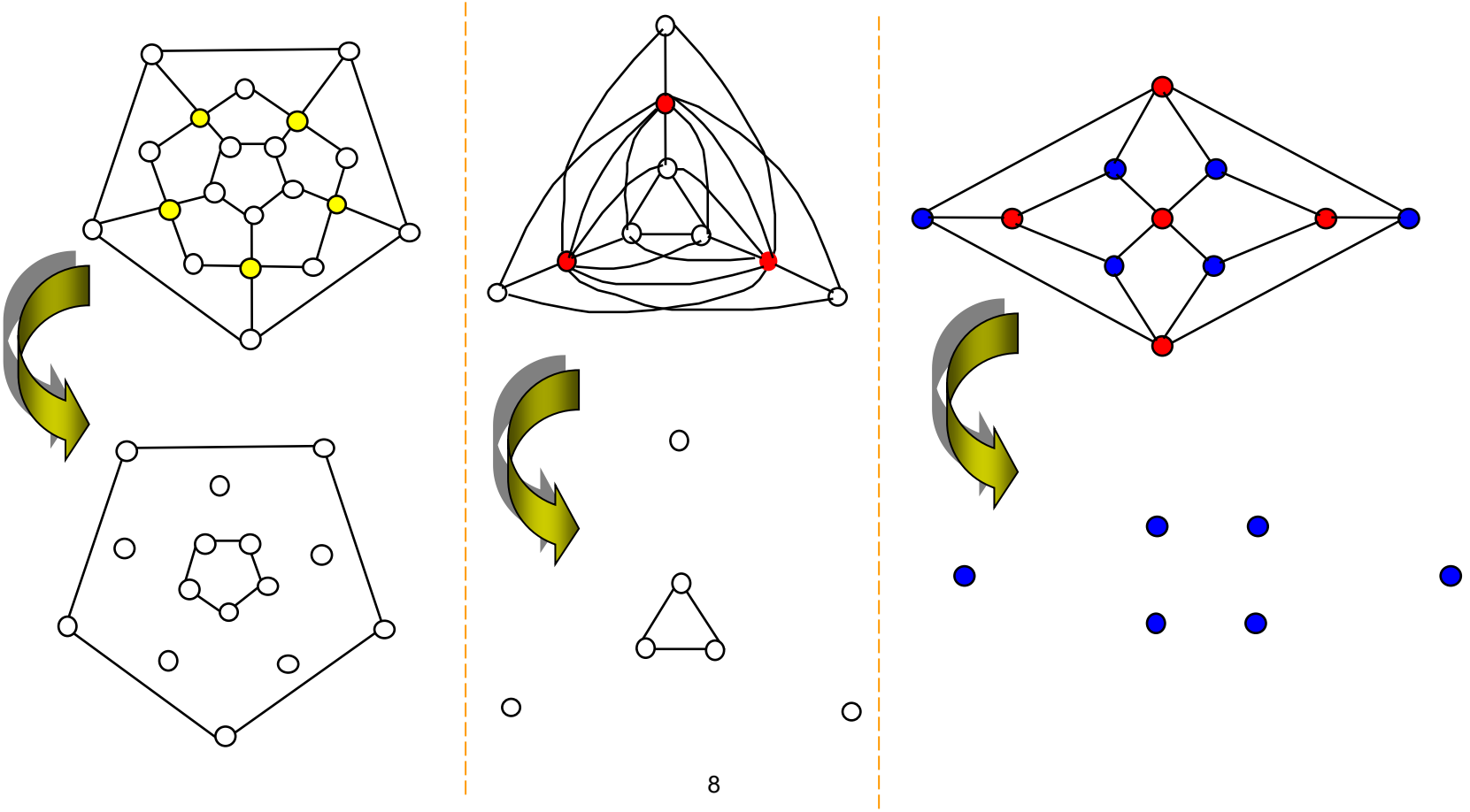
$$P(G-S) \leq |S|$$

其中， P(G-S)表示图G-S的连通分支数.

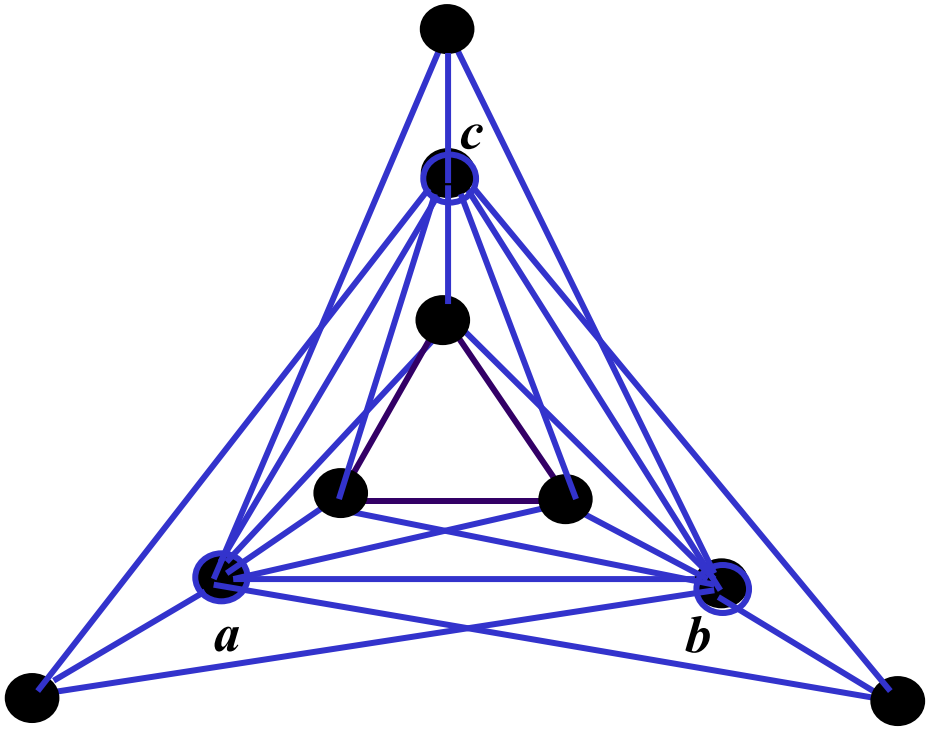
理由：设C是G中的Hamilton回路, $P(G-S) \leq P(C-S) \leq |S|$

向一个图中顶点之间加边不会增加连通分支。

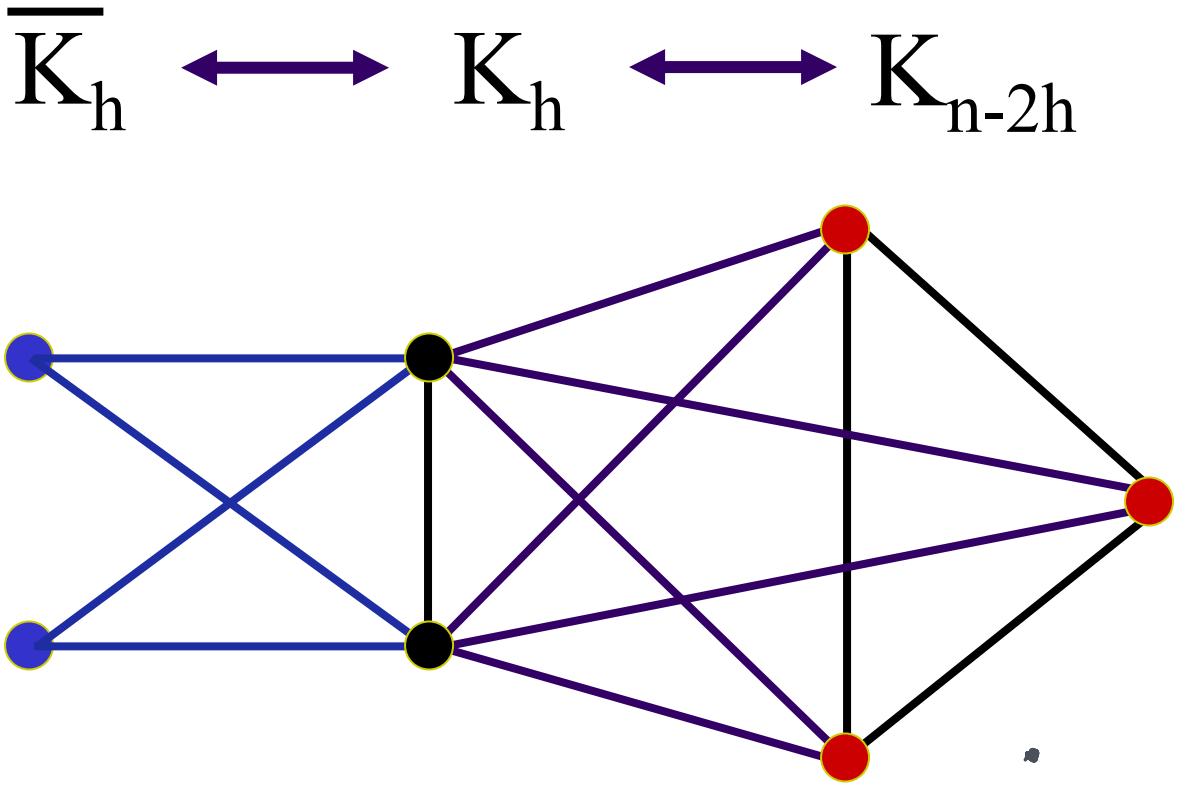
必要条件的应用



举例

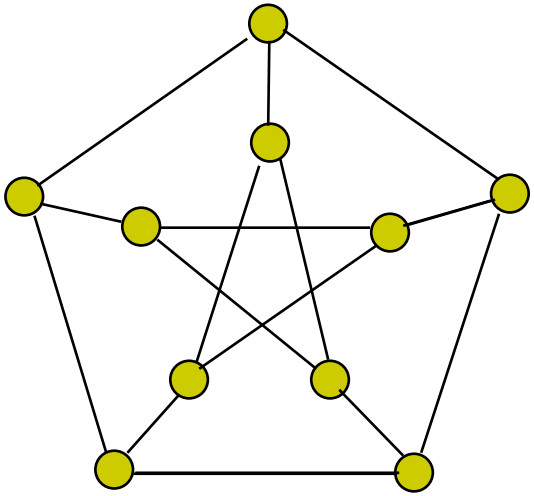


将图中点*a, b, c*的集合记为S, G-S有4个连通分支,而|S|=3. G不是Hamilton图.



$C_{2,7}$ (h=2, n=7)

必要条件的局限性



Petersen图满足上述必要条件，但不是哈密顿图。

内容提要

- 哈密顿通路/回路
- 哈密顿图的必要条件
- 哈密顿图的充分条件
- 哈密顿图的应用
- 竞赛图与有向哈密顿通路

哈密顿图的充分条件

- **Dirac定理（狄拉克, 1952）**

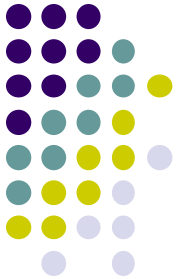
  设G是无向简单图，|G|=n≥3 ， 若δ (G)≥ n/2，则G有哈密顿回路.

- **Ore定理（奥尔, 1960）**

  设G是无向简单图，|G|=n≥3 ，若G中任意不相邻的顶点对u,v均满足： $d(u)+d(v)\geq n$ ，则G有哈密顿回路。

- **设G是无向简单图，|G|=n≥2，若G中任意不相邻的顶点对u,v均满足：$d(u)+d(v)\geq n-1$，则G是连通图。**
  - 假设G不连通，则至少含2个连通分支，设为G_1，G_2。取$x\in V_{G1}$，$y\in V_{G2}$，则：$d(x)+d(y)\leq(n_1-1)+(n_2-1)\leq n-2$ (其中n_i是G_i的顶点个数)，矛盾。

Ore定理的证明



- **Ore定理（1960）**

  设G是无向简单图，$|G|=n\geq 3$，若

  对G中任意不相邻的顶点u和v, $d(u)+d(v)\geq n$ （*）

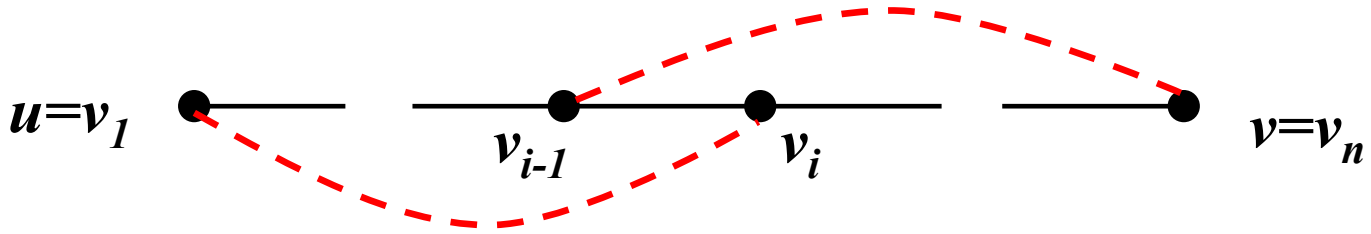
  则G有哈密顿回路。

- 证明.反证法, 若存在满足（*）的图G，但没有Hamilton回路.

  不妨假设G是边数极大的非Hamilton图，且满足（*）。若G不是边数极大的非Hamilton图，则可以不断地向G增加边,把G变成边数极大的非Hamilton图G’，G’依然满足（*），因为对$\forall v\in V(G)$, $d_{G'}(v)\geq d_G(v)$ 。

Ore定理的证明

设u, v是G中不相邻的两点，于是G+uv是Hamilton图，且其中每条Hamilton回路都要通过边uv. 因此，G中有起点为u，终点为v的Hamilton通路:



不存在两个相邻的顶点 v_{i-1}和v_i,使得v_{i-1}与v相邻且v_i 与u相邻. 若不然, (v_1,v_2, … v_{i-1}, v_n, …, v_i, v_1)是G的Hamilton回路. 设在G中u与v_{i1}, v_{i2}, …, v_{ik}相邻, 则v与v_{i1-1}, v_{i2-1}, …v_{ik-1}都不相邻, 因此 $d(u)+d(v) \le k+[(n-1)-k]<n$. 矛盾.

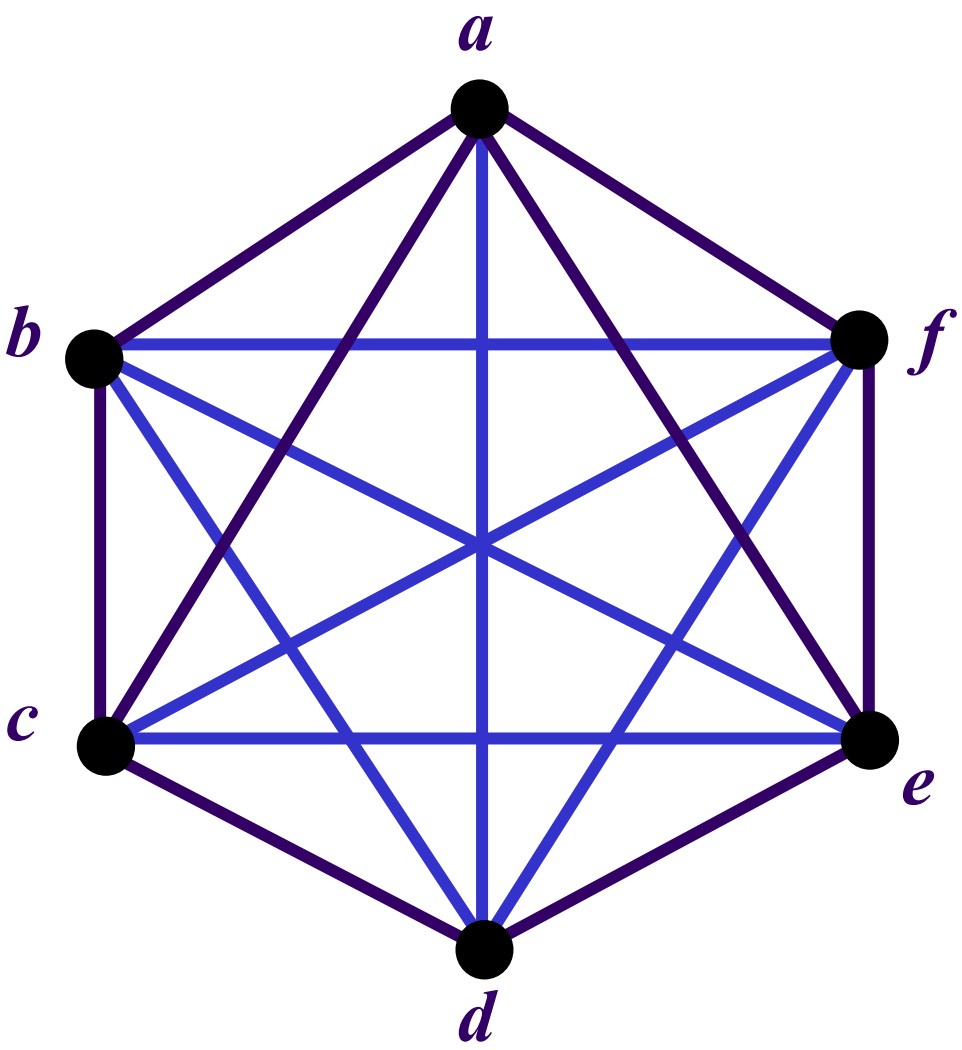
Ore定理的延伸

- 引理. 设G是有限图，u, v是G中不相邻的两个顶点，并且满足：$d(u)+d(v) \geq |G|$，则

  G是Hamilton图 $\Leftrightarrow$ $G \cup \{uv\}$是Hamilton图.
- 证明：类似于Ore定理的证明.

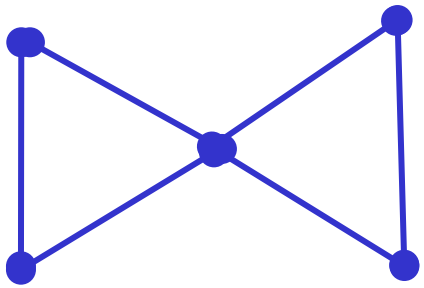
- G的闭合图, 记为C(G): 连接G中不相邻的并且其度之和不小于 |G| 的点对, 直到没有这样的点对为止.
- 有限图G是Hamilton图充分必要其闭合图C(G)是Hamilton图.

闭合图(举例)



充分条件的讨论

- Dirac定理“δ (G)≥ *n*/2”不能减弱为：δ (G)≥ $\lfloor n/2 \rfloor$
- 举例，*n*=5，δ (G)=2 . G不是Hamilton图.

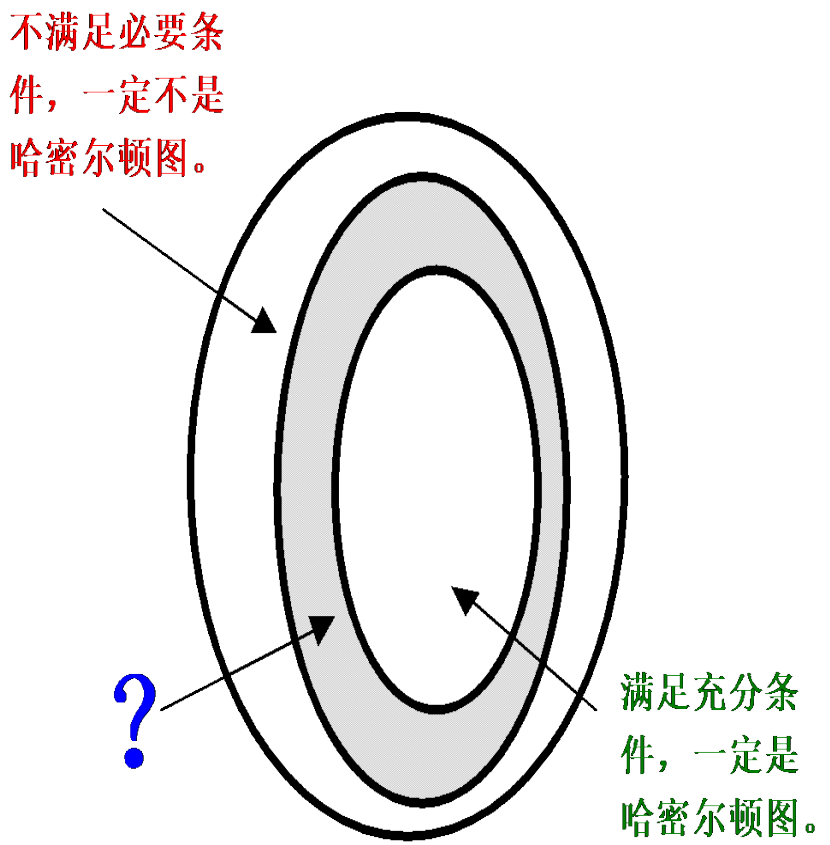


- 存在哈密顿通路的充分条件（Ore定理的推论）

  设G是无向简单图，|G|=*n*≥2 ，若G中任意不相邻的顶点对*u*,*v*均满足： *d*(u)+*d*(v)≥*n*-1 ，则G有哈密顿通路。

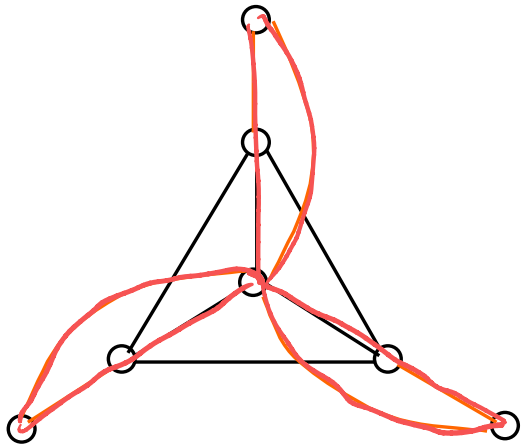
判定定理的盲区

- 从“常识”出发个案处理
  - 一顶点关联的边中恰有两条边在哈密顿回路中。
  - 哈密顿回路中不能含真子回路。
  - 利用对称性
  - 利用二部图特性
  - …

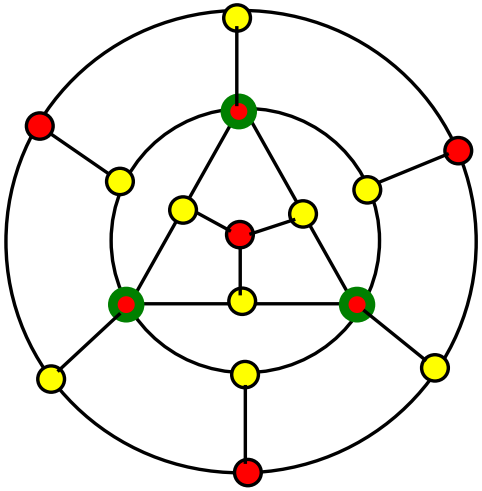


判定哈密顿图的例子

下列图中只有右图是哈密顿图。

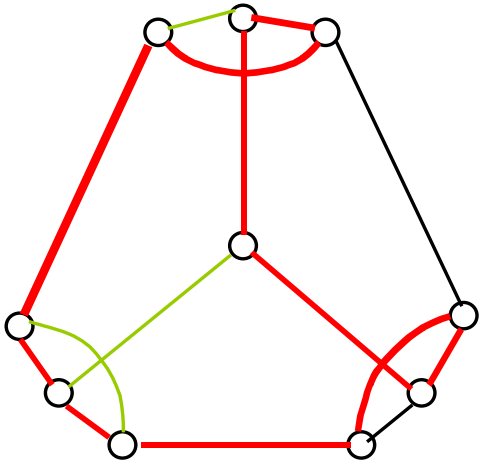


先找Deg=2的顶点和边



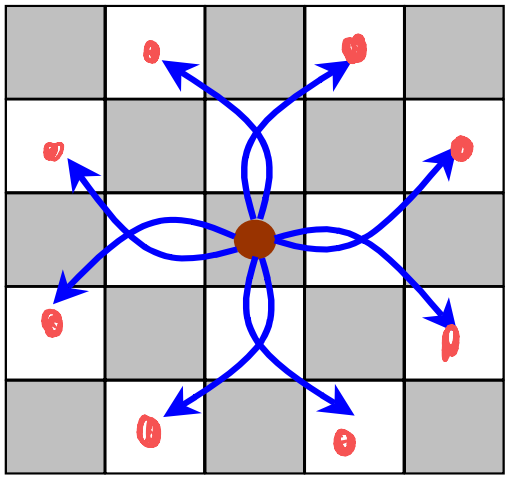
去掉红色点.

(9/3): 8 > 7



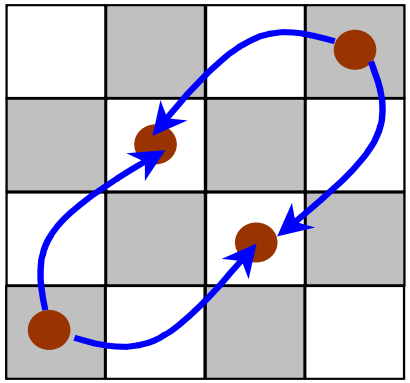
棋盘上的哈密顿回路问题

- 在4×4或5×5的缩小了的国际象棋棋盘上，马(Knight)不可能从某一格开始，跳过每个格子一次，并返回起点。



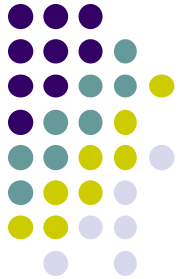
灰（13个） VS 白（12个）

12.13二部图



8.8二部图

哈密顿图问题



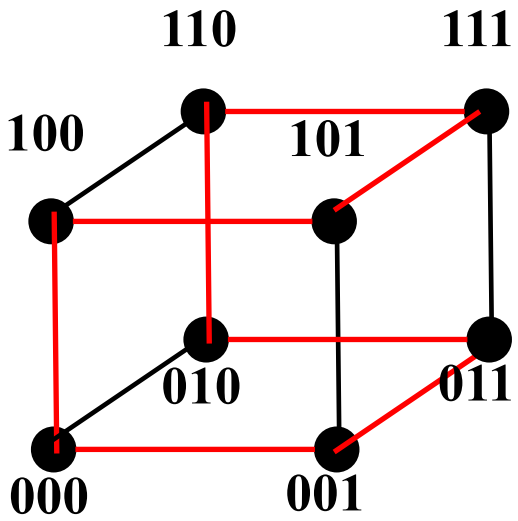
- 基本问题
  - 判定哈密顿回路的存在性
  - 找出哈密顿回路/通路 （NP完全的）
- 尚未找到时间复杂性为多项式的算法

内容提要

- 哈密顿通路/回路
- 哈密顿图的必要条件
- 哈密顿图的充分条件
- 哈密顿图的应用
- 竞赛图与有向哈密顿通路

应用（格雷码）

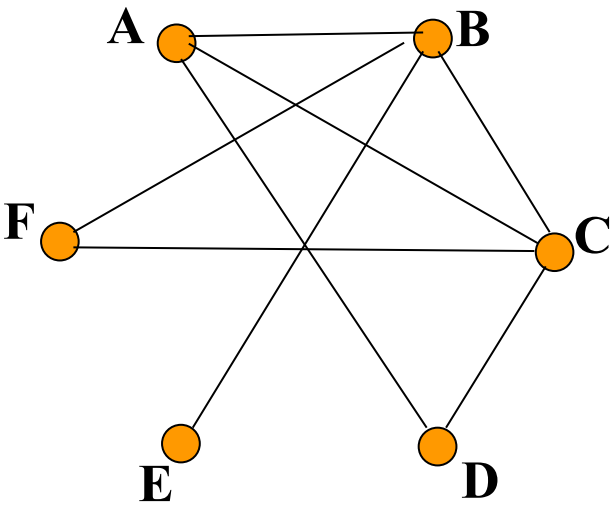
给定一个立方体图，求出哈密顿回路

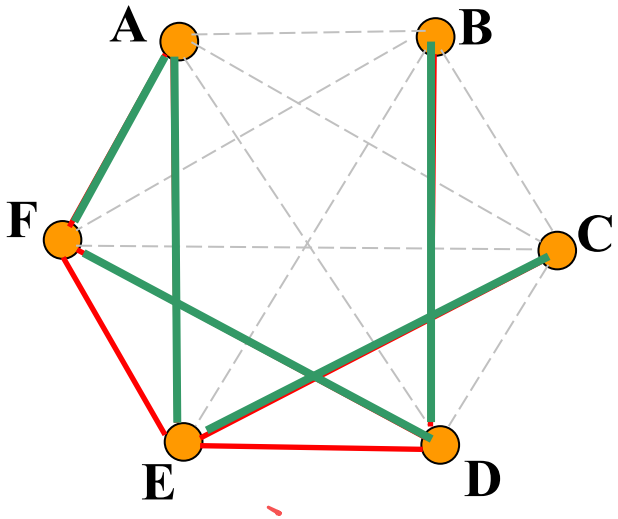


Q_3

安排考试日程（哈密顿通路）

- 问题: 在6天里安排6门课 – A,B,C,D,E,F -的考试，每天考1门。假设课程选修的情况有4类：DCA，BCF，EB，AB。如何安排日程，使得没有人连续两天有考试？

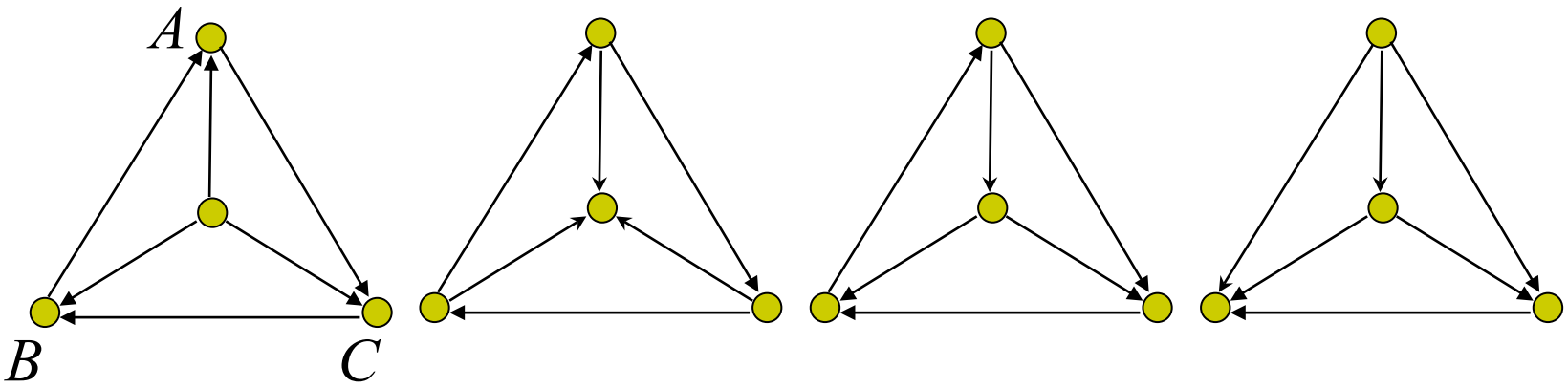




补图 求哈密顿通路

竞赛图

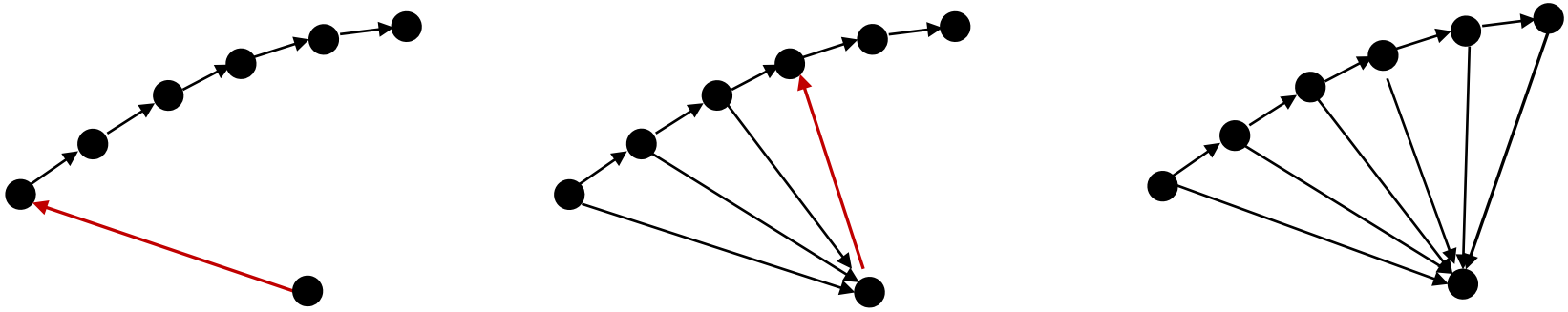
底图为K_4的竞赛图：



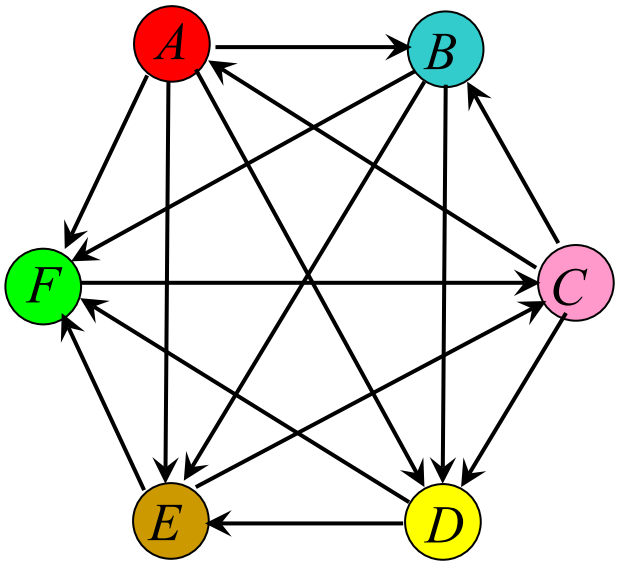
以上每个图可以看作4个选手参加的循环赛的一种结果

竞赛图与有向哈密顿通路

- 底图是完全图的有向图称为竞赛图。
- 利用归纳法可以证明竞赛图含有向哈密顿通路。



循环赛该如何排名次



按照某条有向Hamilton通路(一定存在)上的顺序排名：

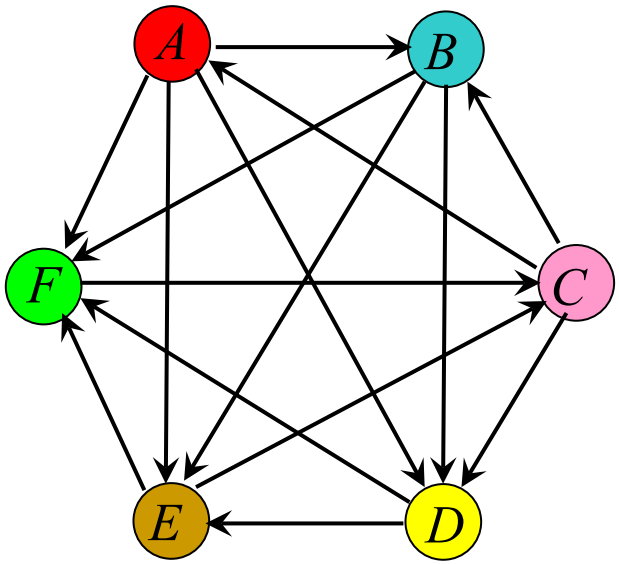
C A B D E F

问题：Hamilton通路路不是唯一的，例如：也可以得到另一排名

A B D E F C

C 从第一名变成了最后一名

循环赛该如何排名次

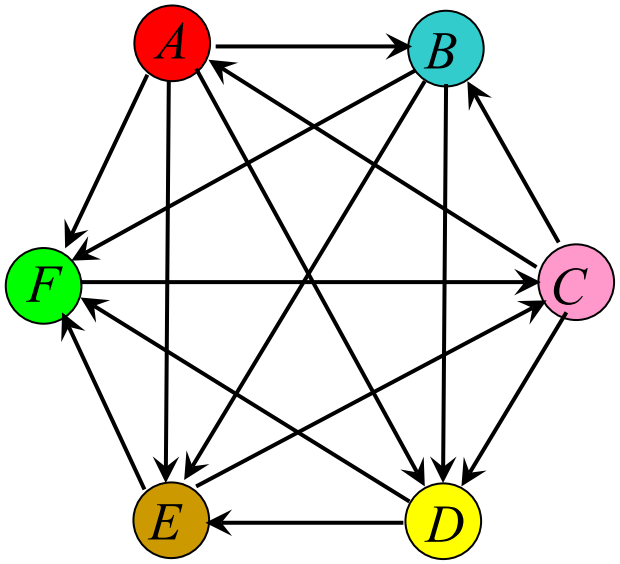


按照得胜的竞赛场次(得分)排名：

A(胜4) B,C(胜3) D, E(胜2) F(胜1)

问题：很难说B,C并列第二名是否公平，毕竟C战胜的对手比B战胜的对手的总得分更高(9比5)。

循环赛该如何排名次



建立对应与每个对手得分的向量

$$s_1 = (a_1, b_2, c_3, d_4, e_5, f_6)$$

然后逐次求第k级的得分向量s_k, 每个选手的第k级得分是其战胜的对手在第k-1级得分的总和。

对应于左图所示的竞赛结果，得分向量：

s_1=(4,3,3,2,2,1)　s_2=(8,5,9,3,4,3)

s_3=(15,10,16,7,12,9)　s_4=(38,28,32,21,25,16)

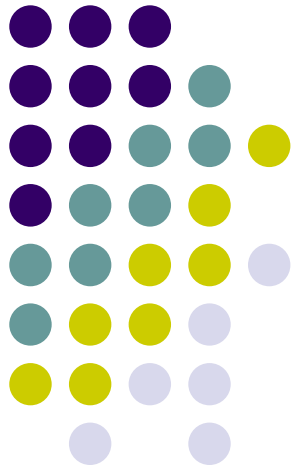
s_5=(90,62,87,41,48,32)　.....

这个序列收敛于一个固定的排列（排名）：A C B E D F。

最短通路问题

离散数学—图论初步

南京大学计算机科学与技术系

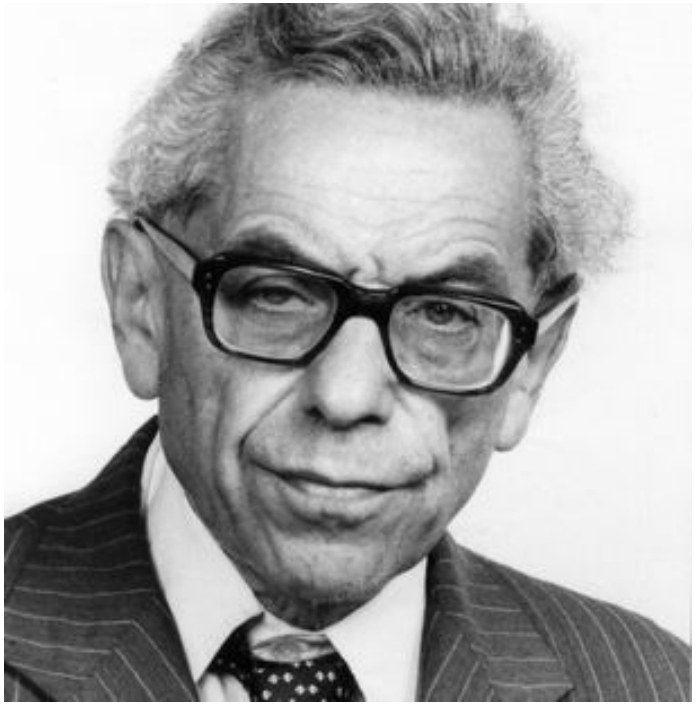


内容提要

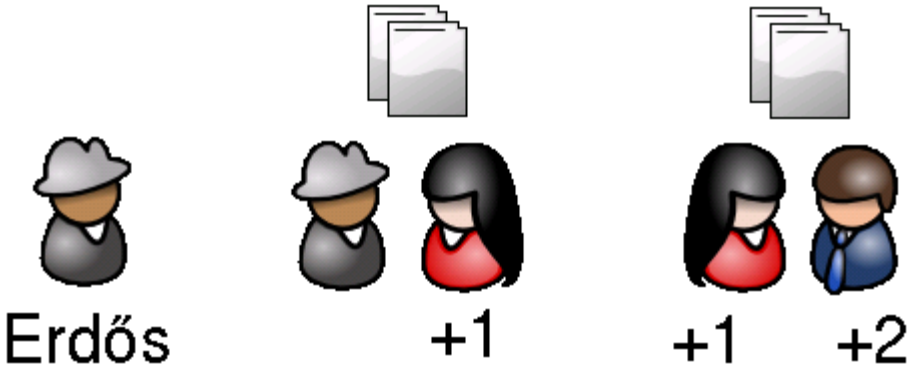
- 引言
- **Dijkstra算法**
- **旅行商问题（TSP）**

埃德斯数（Erdős number）

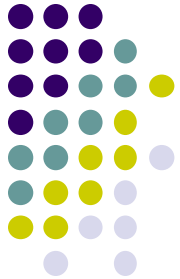
Paul Erdös (1913-1996), Hungary, U.S.A., Israel



Erdős number



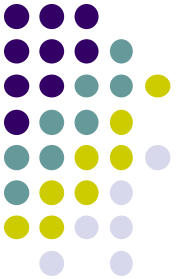
带权图与最短通路问题



- 带权图：三元组 (V, E, W)，(V, E)是图，W是从E到非负实数集的一个函数。$W(e)$表示边e的权。
- 一条通路上所有边的权的和称为该通路的长度。
- 两点之间长度最小的通路称为两点之间的最短通路，不一定是唯一的。
- 单源点最短路问题

  给定带权图 $G(V, E, W)$，并指定一个源点，确定该源点到图中其它各顶点的最短路（长度和路径）。

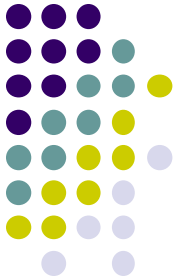
Dijkstra最短路径的算法思想(1959)



- 源点*s*到顶点*v*的最短路径若为*s…uv*，则*s…u*是*s*到*u*的最短路径。 有点像仅序例归纳法
- *n*条最短路径按照其长度的非减次序求得，设它们的相应端点分别为$u_1, \ldots u_n$，最短路径长度记为$d(s, u_i)$，　$i=1,\ldots n$.
- 假设前*i*条最短路径已知，第(*i*+1)条最短路径长度：

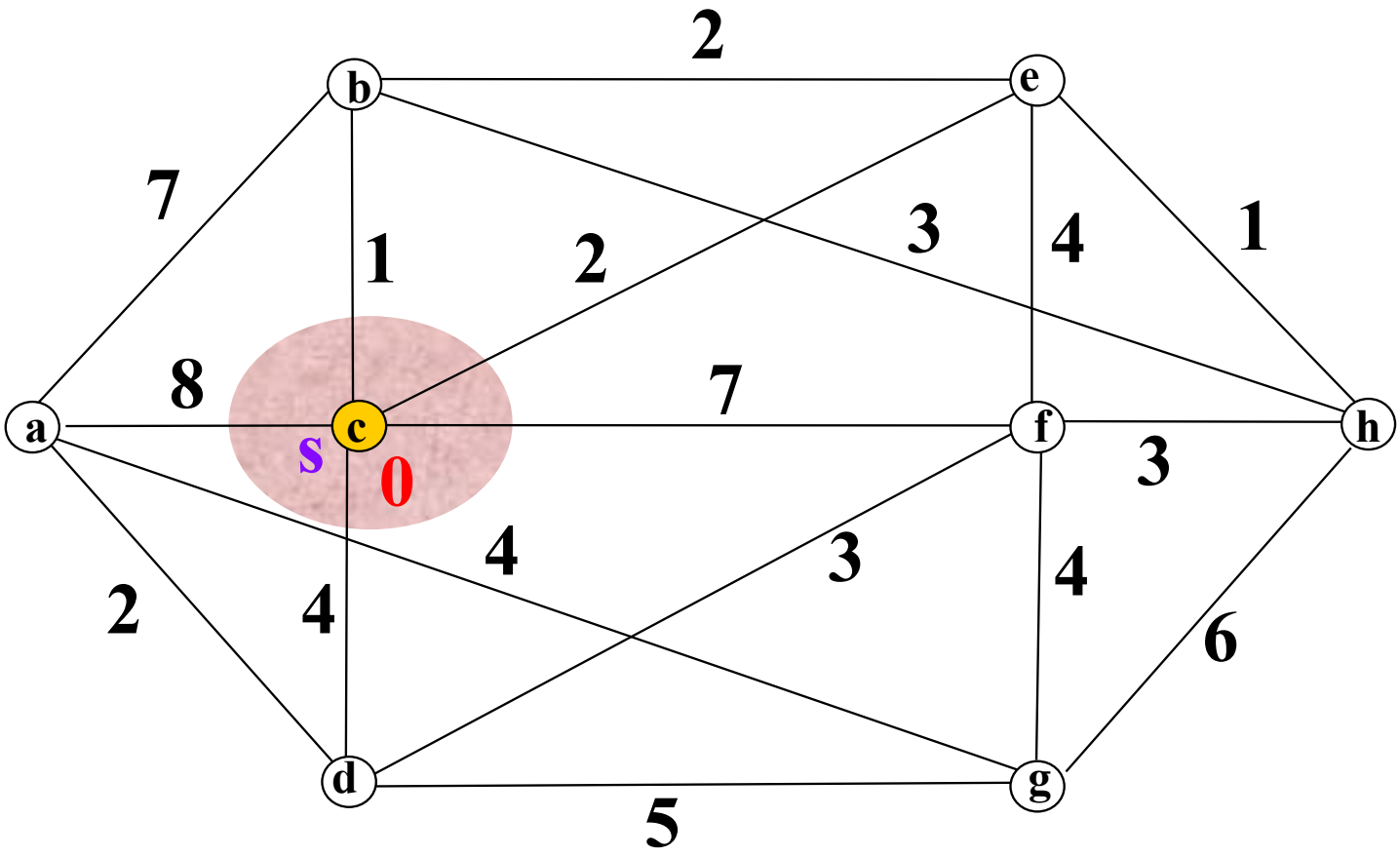
$$d(s, u_{i+1})=\min\{d(s, u_j) +W(u_j, u_{i+1})\mid j=1,\ldots i\}$$

求最短路径的Dijkstra算法

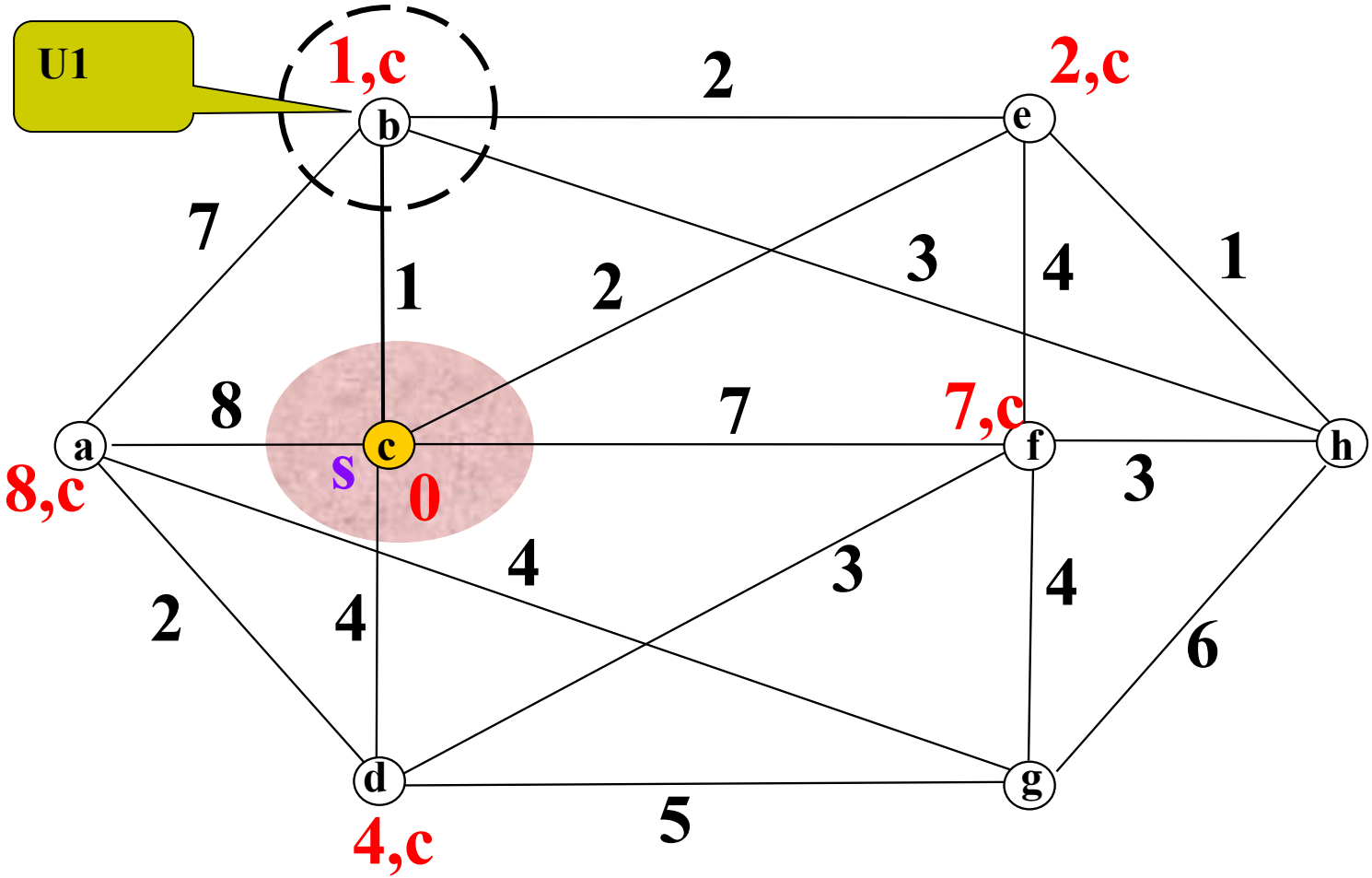


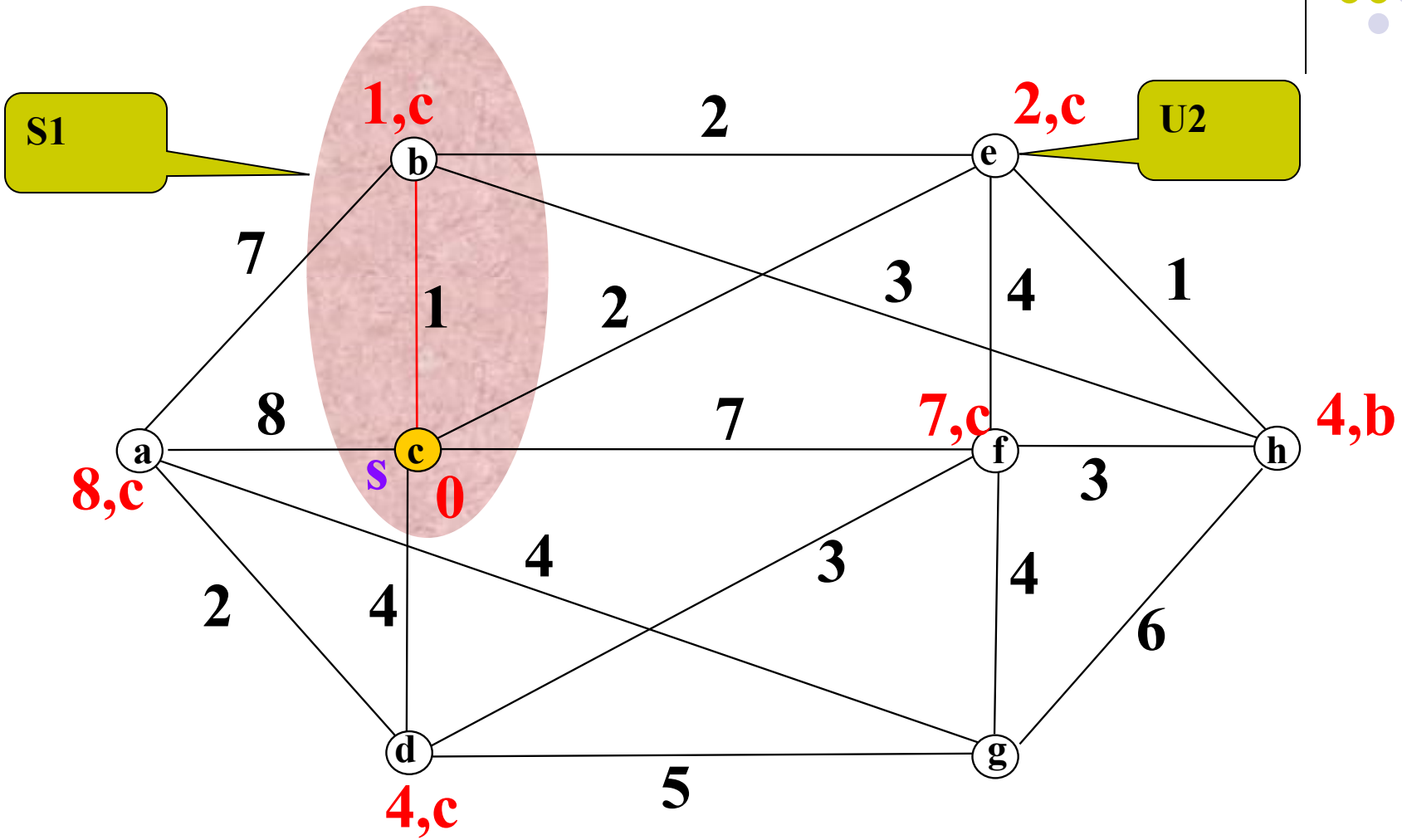
- 输入：连通带权图G，$|V_G|=n$, 指定顶点$s \in V_G$
- 输出：每个顶点v的标注$(L(v), u)$, 其中：
  - $L(v)$即从s到v的最短路径长度（目前可得的）
  - u是该路径上v的前一个顶点。

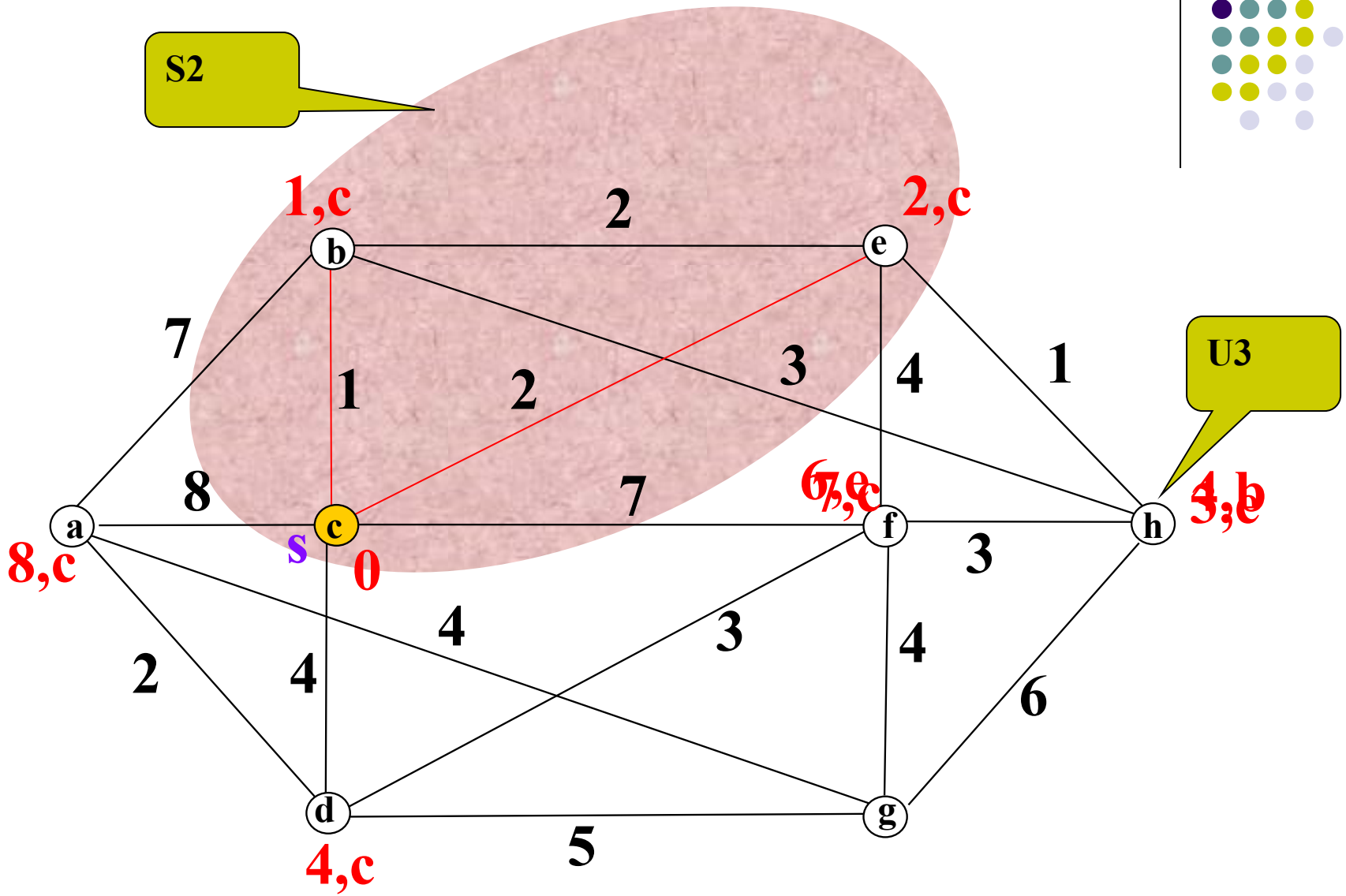
求最短路的一个例子

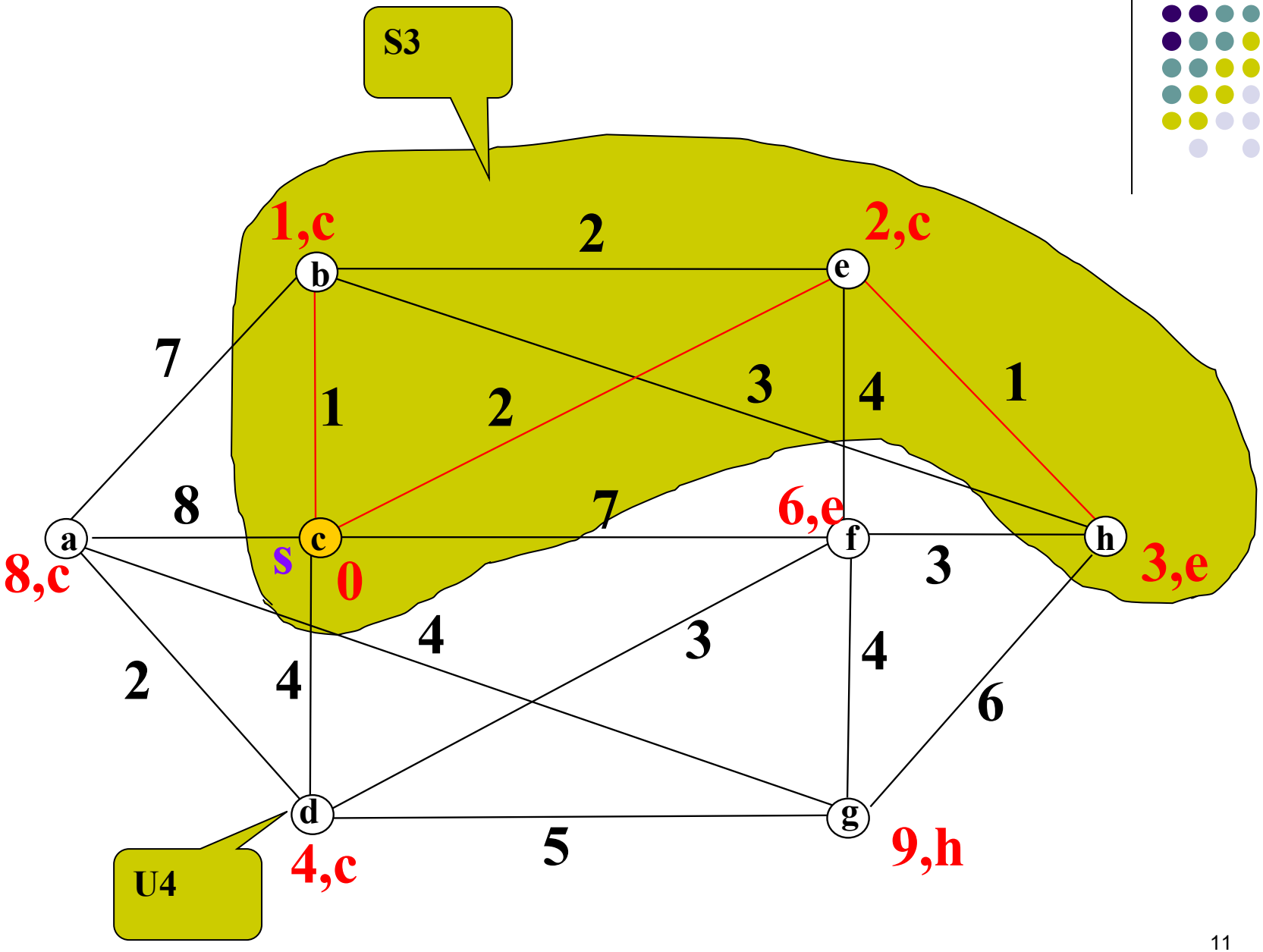


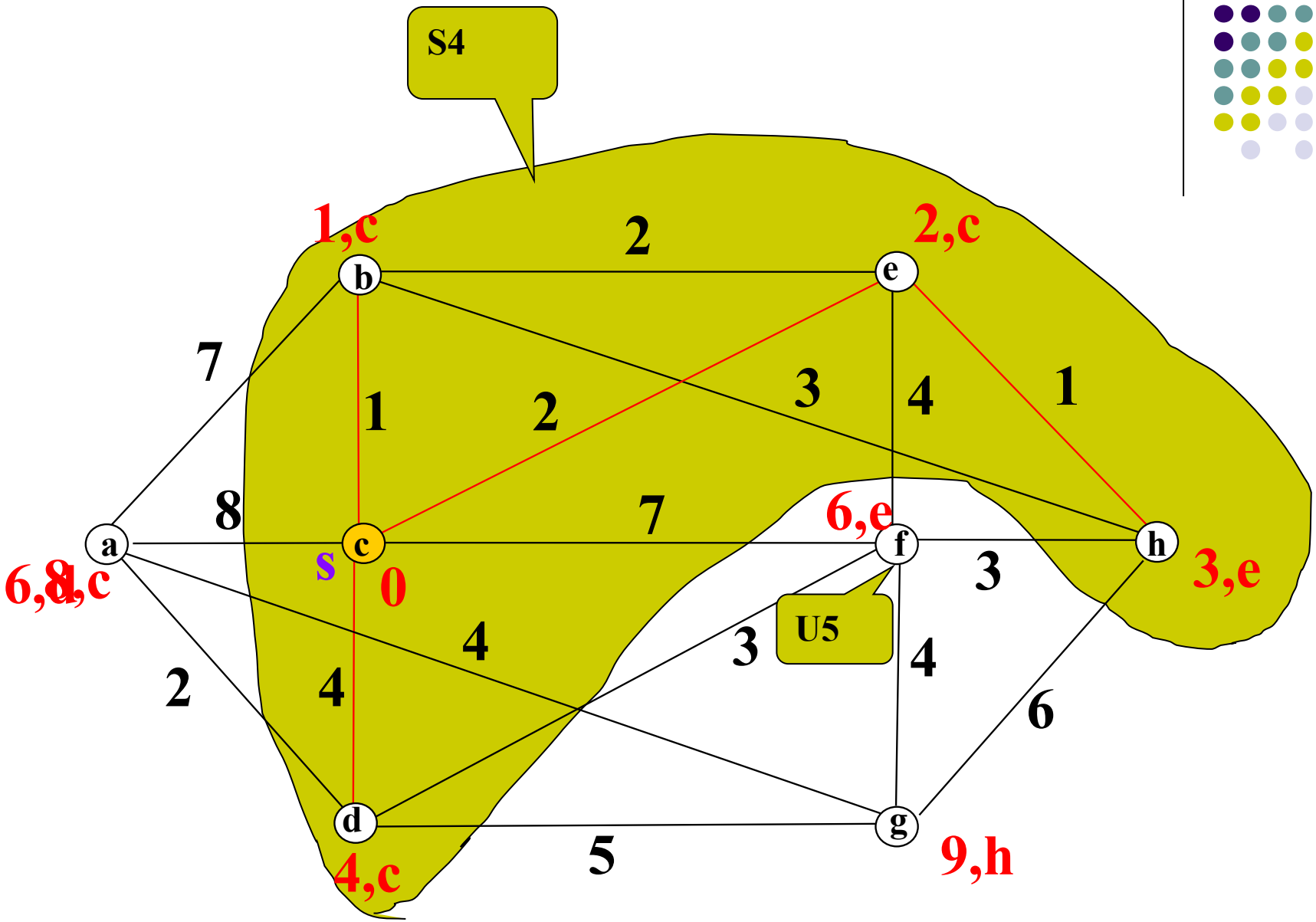
求最短路的一个例子



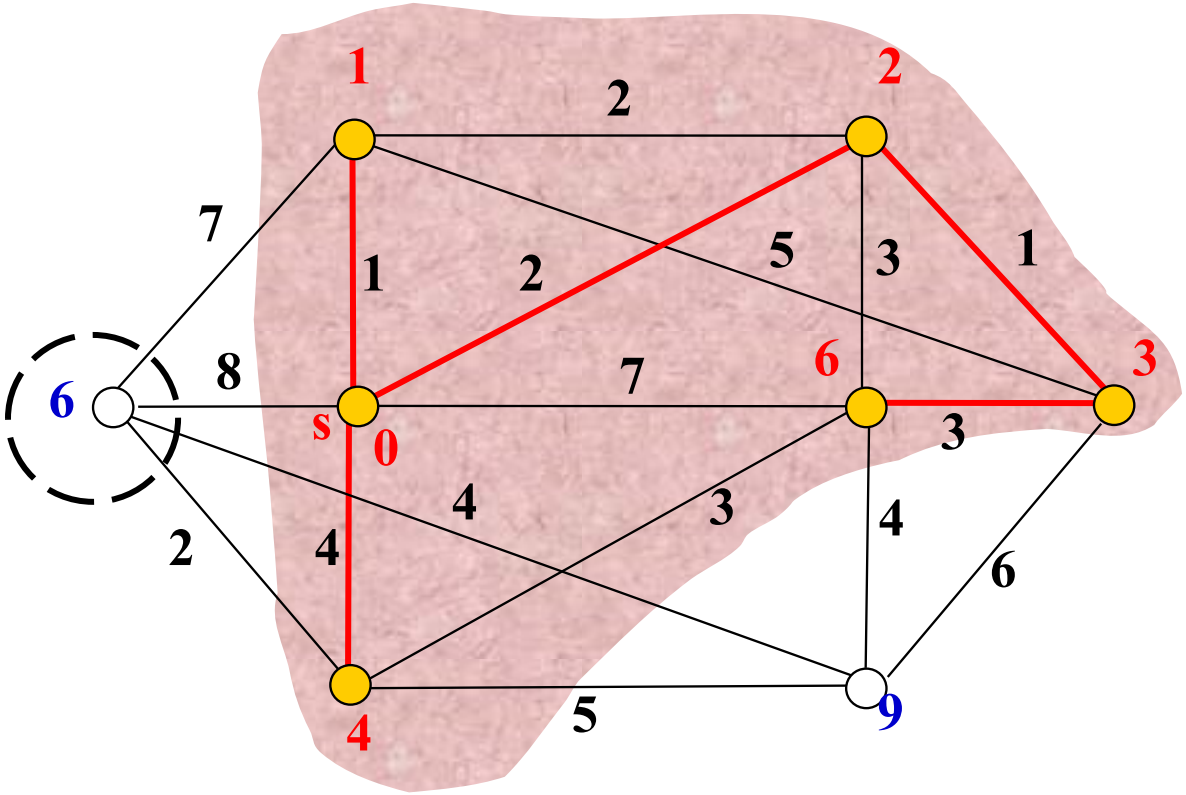

S1
U2
1,c
2,c
b
e
2
7
1
2
3
4
1
8
7
7,c
4,b
a
c
f
h
s
0
8,c
3
4
3
4
2
4
6
d
g
5
4,c


S2
U3
1,c
2
2,c
b
e
7
1
2
3
4
1
8
7
6,c
4,b
a
c
f
h
s
0
8,c
3
4
3
4
2
4
6
d
g
5
4,c

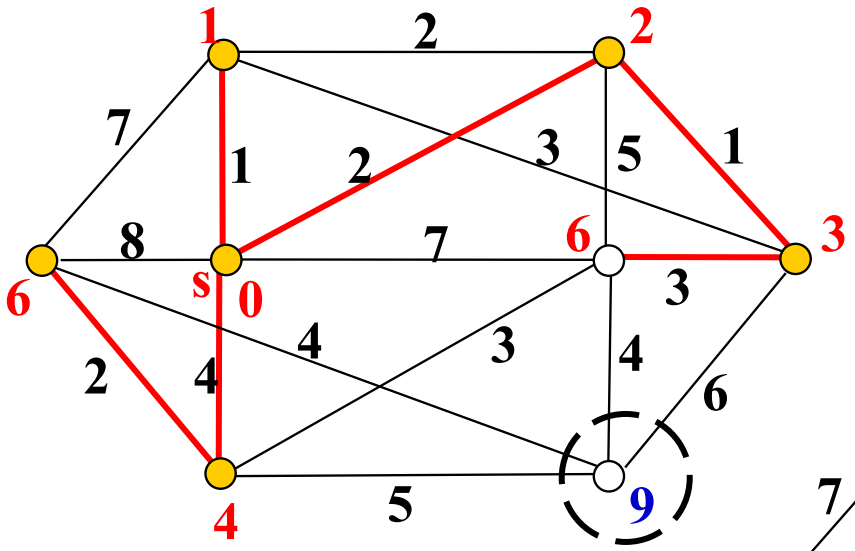

S3
1,c
2
2,c
b
e
7
1
2
3
4
1
8
7
6,e
a
c
f
h
s
8,c
0
3
3,e
4
3
4
2
4
6
d
g
5
9,h
4,c
U4

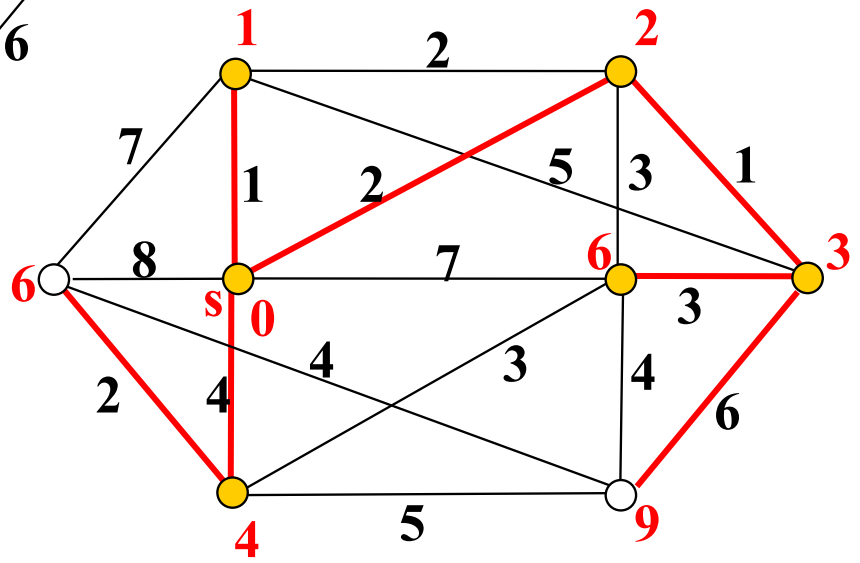

S4
1,c
2
2,c
b
e
7
1
2
3
4
1
8
7
6,e
a
c
f
h
s
0
3
3,e
U5
3
4
4
2
4
6
d
g
5
9,h
4,c

求最短路的一个例子(续)

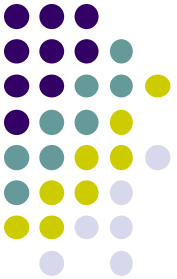


求最短路的一个例子(续)


1
2
2
7
1
2
3
5
1
8
7
6
3
s
0
3
6
4
3
4
2
4
6
4
5
9

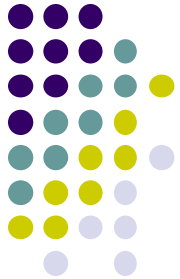

1
2
2
7
1
2
5
3
1
8
7
6
3
s
0
3
4
3
4
2
4
6
4
5
9

Dijkstra算法的描述



1. 初始化：$i=0$, $S_0=\{s\}$, $L(s)=0$, 对其它一切$v \in V_G$, 将$L(v)$ 置为∞。
   若$n=1$，结束。
2. $\forall v \in S_i' = V_G - S_i$, 比较$L(v)$和$L(u_i)+W(u_i, v)$的值 ($u_i \in S_i$)
   如果$L(u_i)+W(u_i, v)<L(v)$, 则将v的标注更新为$(L(u_i)+W(u_i, v), u_i)$,
   即： $L(v)=\min\{ L(v), \min_{u \in Si}\{L(u)+W(u,v)\} \}$
3. 对所有S_i'中的顶点，找出具有最小$L(v)$的顶点v, 作为u_{i+1}
4. $S_{i+1} = S_i \cup \{u_{i+1}\}$
5. $i = i+1$; 若$i=n-1$, 终止。否则：转到第2步。

Dijkstra算法的分析

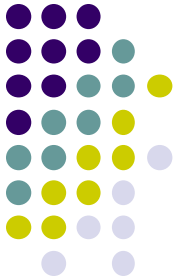


- 可终止性
  - 计数控制
- 正确性

  需证明当算法终止时
  - L(v)=d(s, v)对一切v成立。
  - 由标记中的诸u_i确定的路径是一条最短路径

    (这里$d(s,v)$是s到v的最短路径长度，即距离。)
- 复杂性
  - O(n^2)

旅行商问题
(Travelling Salesman Problem, TSP)

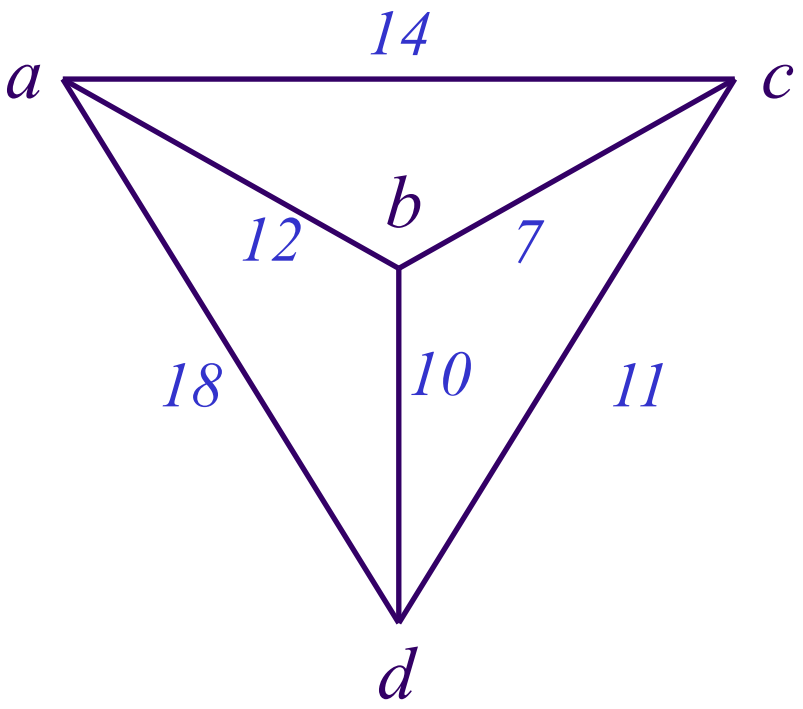


- *n*个城市间均有道路，但距离不等，旅行商从某地出发，走过其它*n*-1城市各一次，最后回到原地，如何选择最短路线？
- 数学模型：
  - 无向带权图G：顶点对应于城市，边对应于城市之间的道路，道路长度用相应边的权表示。
  - 问题的解：权最小的哈密尔顿回路。
  - G是带权完全图，总共有(*n*-1)!/2条哈密尔顿回路。因此，问题是如何从这(*n*-1)!/2条中找出最短的一条。

(包含25个顶点的完全图中不同的哈密尔顿回路有约3.1×10^{23}条，若机械地检查，每秒处理10^9条，需N万年。)

旅行商问题

- 一位旅行商（销售员）生活在城市*a*，假定访问的城市是*d*, *b*, *c*，然后回到*a*，求完成这次访问的最短路径的距离.



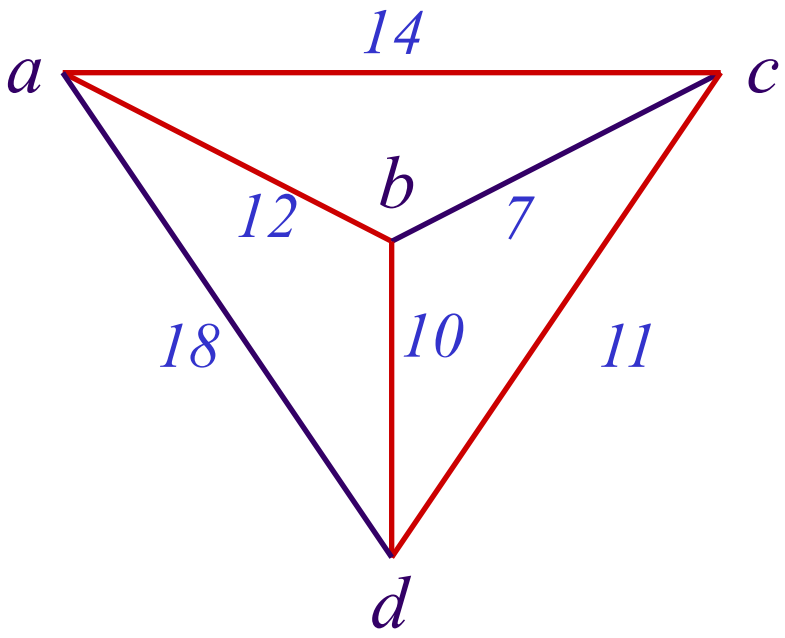
旅行商问题

- 解：列出哈密尔顿回路，并求其距离：

  （1）（*abcda*）=（12+7+11+18）= 48

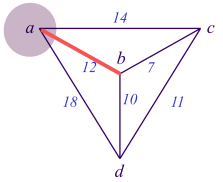
  （2）（*acbda*）=（14+7+10+18）= 49

  （3）（*abdca*）=（12+10+11+14）= 47



旅行商问题 局部最优 ≠ 全局最优

- 哈密尔顿回路（路径）的最短路径问题！
- 下面介绍一种<u>最邻近算法</u>：贪心算法

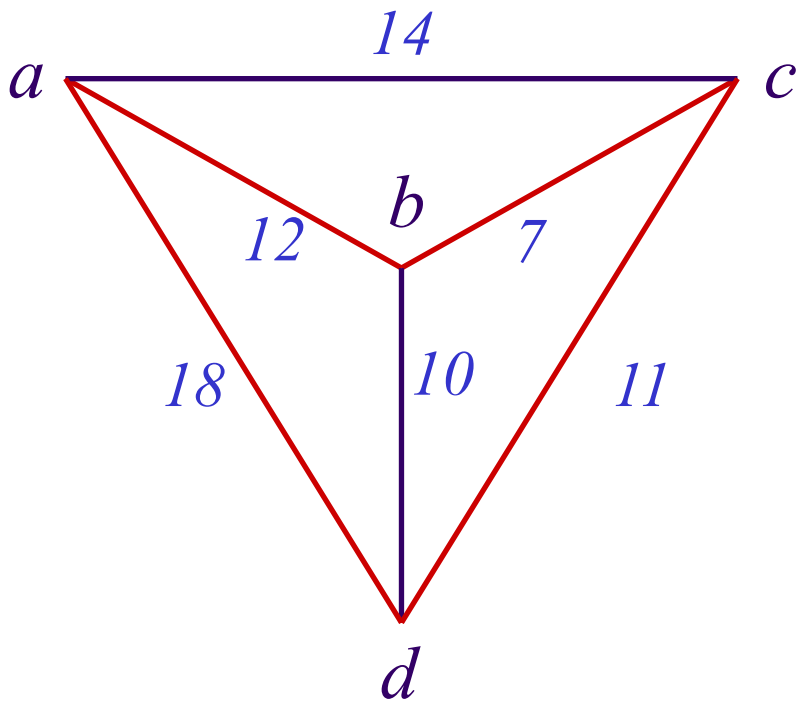


（1）选择任一顶点作为始点，找出离始点距离最小的顶点，形成一条边的初始路径；

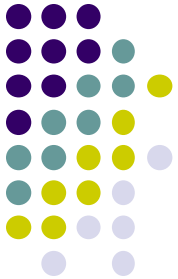
（2）设*u*是最新加到这条路径上的顶点，从不在这条路径上的所有顶点中选择一个与*u*距离最小的顶点，把连接*u*与此结点的边加入路径中；重复执行直到G中的各顶点均含在这条路径中。

旅行商问题

（3）把始点到最后加入的顶点的边放入路径中得到一条哈密尔顿回路，并为近似最短的哈密尔顿回路.



旅行商问题(TSP)的研究进展



- （在最坏情况下）时间复杂性为多项式的算法？
- （在最坏情况下）时间复杂性为多项式的近似算法
  - 保证: **W≤W'≤ cW (c=3/2), 误差为50%**
- 实际应用中，已有好的算法能够在几分钟内处理**1000个节点的规模，误差在2%。**

二部图中的匹配

离散数学课程组

南京大学计算机科学与技术系

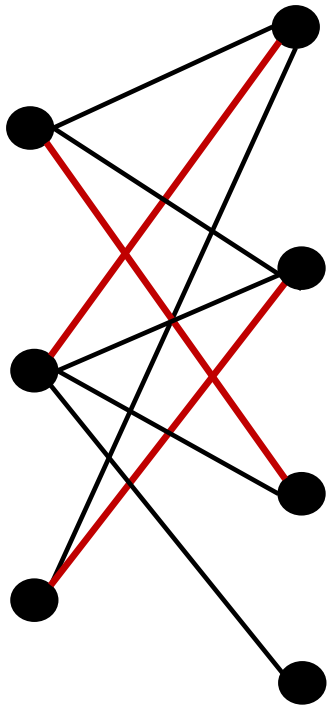
内容提要

- 引言
- 二部图中完备匹配（Hall定理）
- 二部图中的最大匹配
- 二部图中的稳定匹配

孤岛上的婚姻

- 成就最多幸福婚姻的配对方案

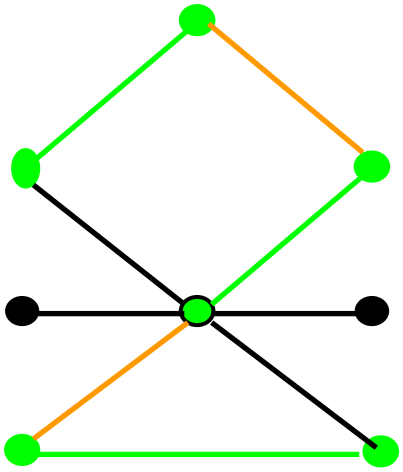
互不相邻的边集

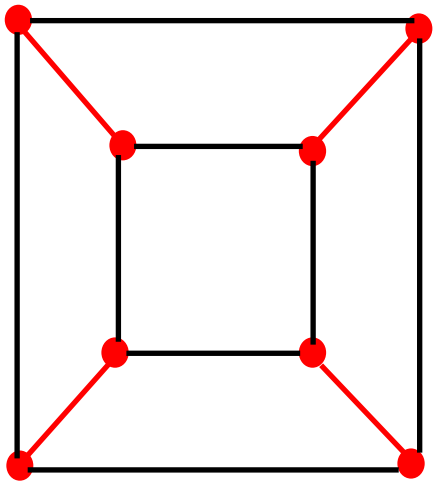


图中的匹配

- 匹配（边独立集）：互不相邻的边的集合
- M-饱和点：M中各边的端点 被选择即饱和.

匹配数
$\beta_1=3$





匹配数
$\beta_1=4$

(选择当前边后不能再增加)

极大匹配

最大匹配
(边的个数最大)

M-饱和点

包含所有顶点、

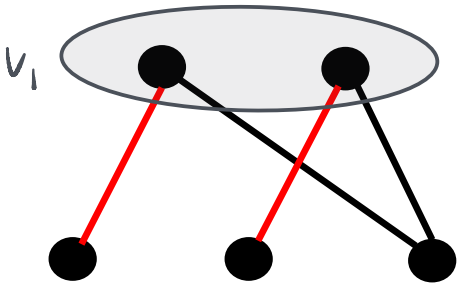
完美匹配

M-饱和点

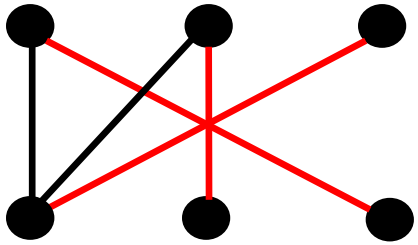
二部图中的完备匹配

- 定义：设G是二部图，二部划分为$<V_1,V_2>$，若G中的匹配M饱和V_1中所有顶点，则称M为V_1到V_2的完备匹配。

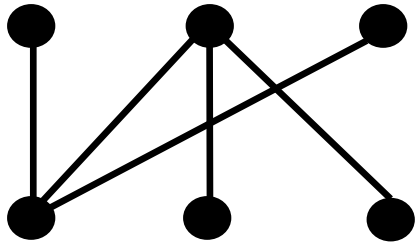
注意：完备匹配一定是最大匹配，但仅当$|V_1|=|V_2|$才是完美匹配。



V_1到V_2的完备匹配



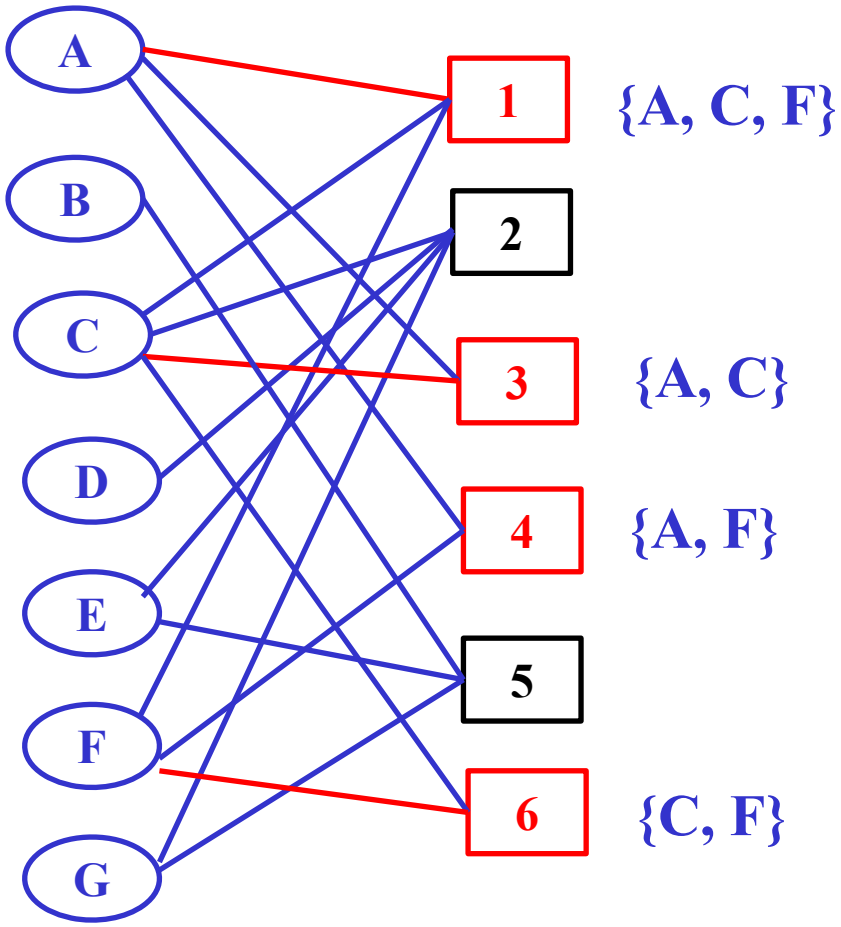
存在完美匹配



无完备匹配？

二部图中的完备匹配（举例）

- V_1={1, 2, 3, 4, 5, 6}，是否存在饱和V_1的配对方案？



饱和{1, 3, 4, 6}？

Hall定理

- **Hall定理(1935, Marriage Theorem)**

  设二部图$G=<V_1, V_2, E>$, 则G有V_1到V_2的完备匹配 ⇔

  $A \subseteq V_1$， $|N(A)| \geq |A|$ 对V中的子集都至少有等量的令陪

- 证明. 必要性易证，下证充分性（使用强归纳法）。

  如果 $|V_1|=1$, 充分性命题显然成立。

  假设当$|V_1| \leq k$ ($k \geq 1$) 时充分性命题均成立, 要证:当$|V_1|=k+1$时充分性命题也成立。分二种情形来证明。

  (1)对V_1的任意真子集A， $|N(A)| > |A|$

  (2)存在 V_1的一个真子集A’， $|N(A')| = |A'|$

Hall定理

- 归纳证明.

(1)对V_1的任意真子集A , $|N(A)| > |A|$

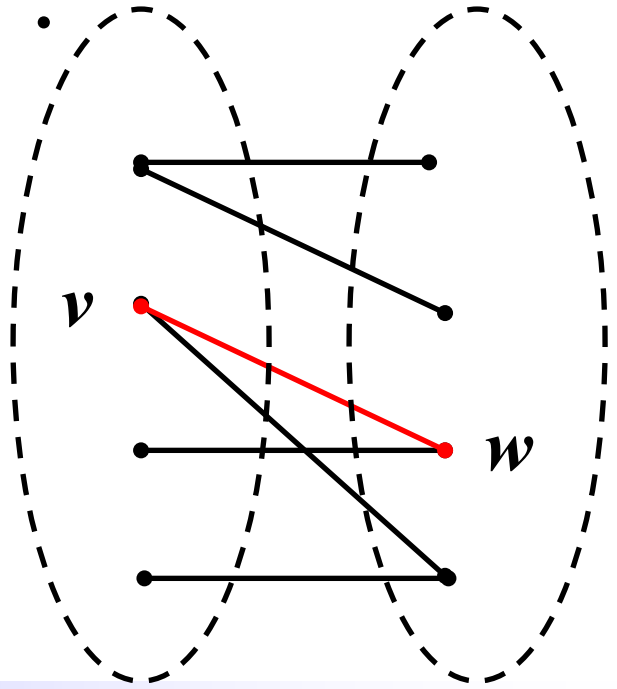
任取一个顶点$v \in V_1$, 任取$w \in N(\{v\})$.

$H=G-\{v, w\}$是一个二部图（非空）.

H满足归纳假设的条件, 从而

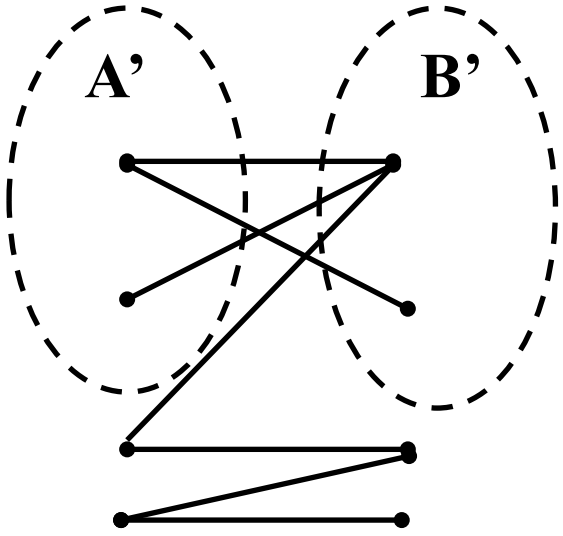
H有$V_1 - \{v\}$到$V_2 - \{w\}$的完备匹配.

这个匹配加上边(v, w)构成G的从V_1到V_2的完备匹配.



Hall定理

(2)存在 V_1的一个真子集A’, |N(A’)| =|A’ |. 记B’= N(A’).



据归纳假设,存在A’到B’ 的完备匹配.

二部图H=G-A’-B’ 满足归纳假设条件.

否则, 存在C $\subseteq V_1$-A’. $|N_H(C)|<|C|$.

$|N_G(C\cup A')|\leq |N_H(C)|+|B'| < |C|+|B'|=|C|+|A'|= |C\cup A'|$.

矛盾.

据归纳假设,存在V_1-A’到V_2-B’的完备匹配.

合并上述两个匹配得到一个V_1到V_2的完备匹配. 得证

Hall定理的推论

- 设二部图G是一个k-正则的($k \geq 1$), 则G有完美匹配.
- 证明. 不妨设$G = < A, B, E>$, $k|A| = k|B|$, 所以$|A| = |B|$.

每个顶点都引生k条边

下证G有A到B的完备匹配.

对任一$S \subseteq A$，S与N(S)之间总共有$k|S|$ 条边，而与N(S)相关的边总共有$k|N(S)|$ 条边。

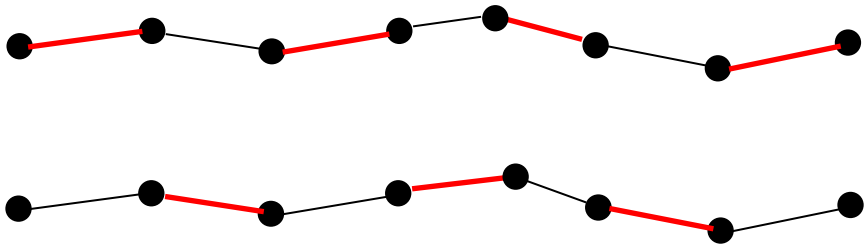
$$\therefore k|S| \leq k|N(S)|$$

$$\therefore |N(S)| \geq |S|$$

根据Hall定理，G有A到B的完备匹配，因 $|A| = |B|$，该匹配是完美匹配。

交错路径与可增广交错路径

- 定义：设M是G中一个匹配。若G中路径*P*中M与E_G-M中的边交替出现，则称*P*为M-交错路径(也可以是回路)；若*P*的起点与终点都是M-非饱和点（没有被匹配的顶点），则称*P*是可增广交错路径（增广路径）。



可增广交错路

最大匹配

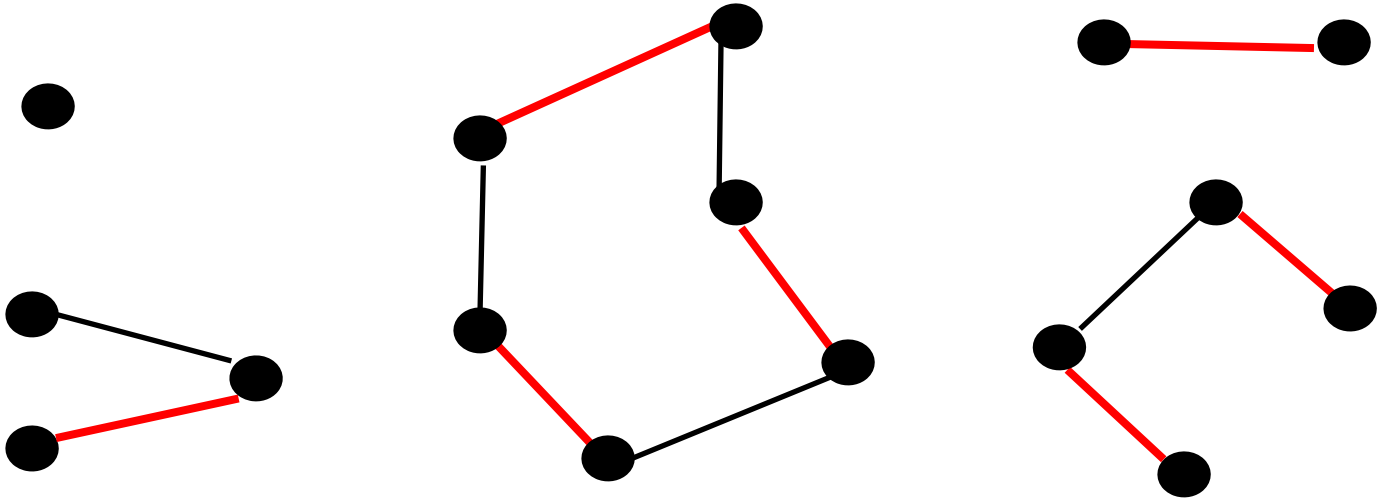
- **Berge's Lemma (1957).** M是最大匹配 ⇔相对于M没有增广路径
- 证明. 容易证明必要性，下证充分性, 采用反证法.

  假设有一个更大的匹配M′. 令G′ = (V, M⊕M′).

  G′中各顶点的度最多为2. 因此, G′的各连通分支要么是路径(孤立点也看作路径), 要么是回路.

  无论是路径还是回路，来自M 的边与来自M′的边一定是交错的.

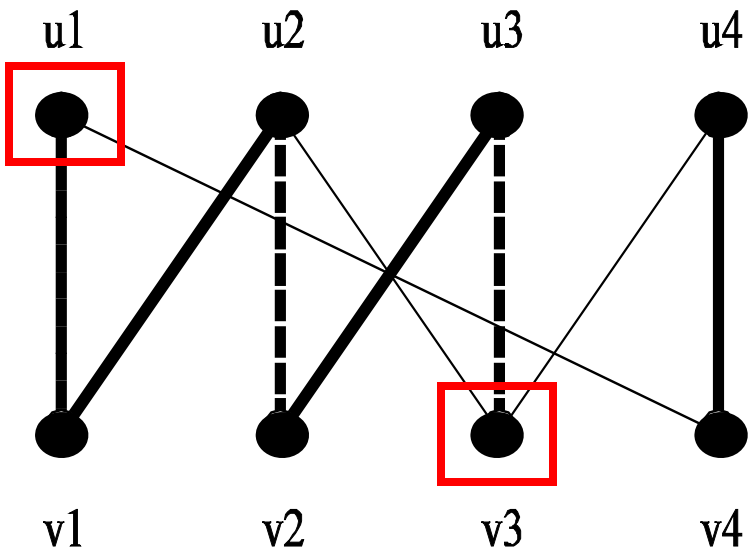
最大匹配

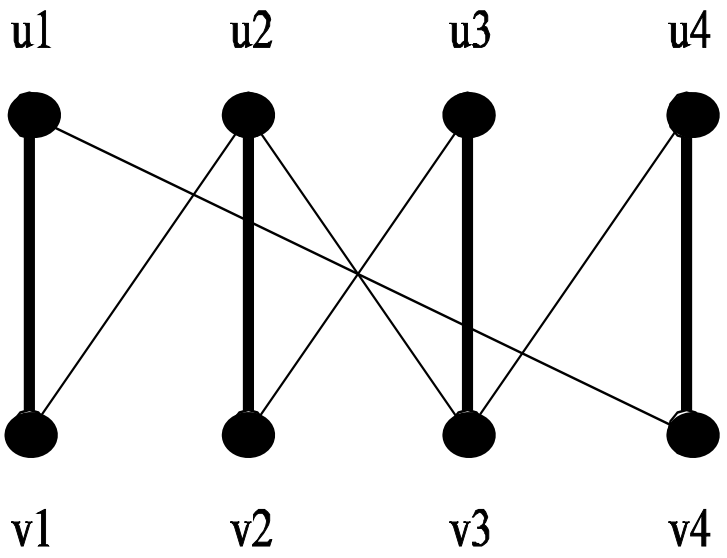


- 若是回路, 来自M 的边数等于来自M′的边数. 由于 |M′| >|M|, 故必有一条路径包含M′的边多于M的边, 从而是相对于M的增广路径，矛盾. 得证

增广路径的算法思想

- 在二部图中直接使用增广路径的匹配算法
  - 找增广路径, 对M进行增广 , 一直至没有增广路径.
  - 复杂度 O(|V||E|)，最大匹配的元素个数≤|V|/2



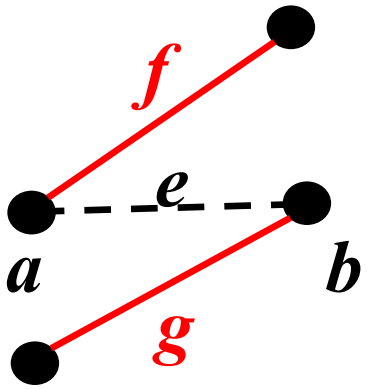


稳定匹配（稳定的婚姻）

- G的一个偏好集

  一族线性序 $(\leq_v)_{v\in V}$， 其中，$\leq_v$是E(v)上的线性序。

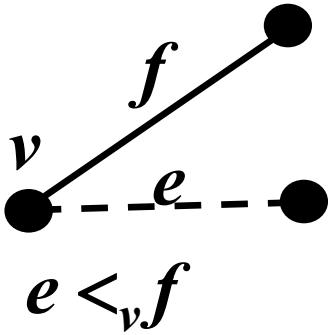
- **Unstable: If M is a matching and $e=(a, b)$ is an edge not in M such that both a and b prefer e to their current matching edge.**



- G中一个匹配M 是稳定的

  对任意一个$e\in E\backslash M$，存在 $f\in M$满足：

  (i) e 和f 有公共端点v，(ii) $e <_v f$.



稳定匹配（稳定的婚姻）

- 定理 (Gale & Shapley 1962)

  任意给定一个偏好集，二部图G有一个稳定的匹配。

- 思路
  - 男子向尚未拒绝他的最喜爱的女子求婚。
  - 女子接受目前为止最如意的求婚提议，但是，倘若有更如意的求婚者，会改变主意。

稳定匹配（稳定的婚姻）

- **Example.** Given men *x, y, z, w*, women *a, b, c, d*, and preferences listed below, the matching {*xa, yb, zd, wc*} is a stable matching.

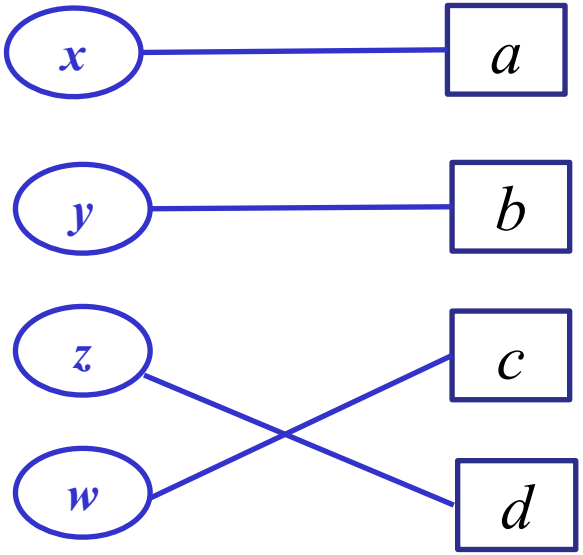
Men{ *x, y, z, w*} Women {*a, b, c, d*}

x*: *a* > *b* > *c* > *d ***a*: *z* > *x* > *y* > *w***

y*: *a* > *c* > *b* > *d ***b*: *y* > *w* > *x* > *z***

z*: *c* > *d* > *a* > *b ***c*: *w* > *x* > *y* > *z***

w*: *c* > *b* > *a* >*d ***d*: *x* > *y* > *z* > *w***



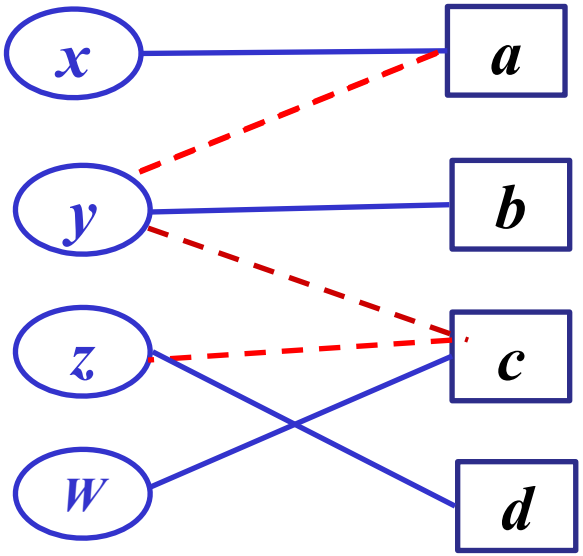
稳定匹配（稳定的婚姻）

x: a > b > c > d　*a: z > x > y > w*

y: a > c > b > d　*b: y > w > x > z*

z: c > d > a > b　*c: w > x > y > z*

w: c > b > a >d　*d: x > y > z > w*



稳定匹配（稳定的婚姻）– 术语

- 给定M，$a \in A$可被$b \in B$接受
  - $(a, b) \in E \backslash M$，并且
  - 若存在$(a', b) \in M$，则 $(a', b) <_b (a, b)$.
- $a \in A$对M满意
  - a是一个尚未配对的顶点，或者
  - 存在$(a, b) \in M$，若a可被b'接受，则 $(a, b) >_a (a, b')$

稳定匹配（稳定的婚姻）– 算法

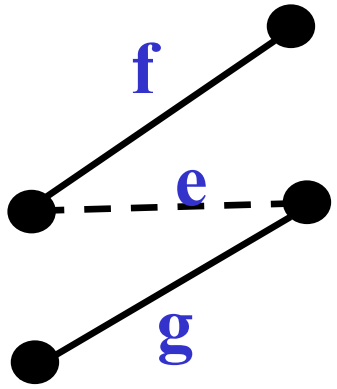
- 从一个空的边集开始，构造（更新）匹配M，保持“A中的所有顶点对M满意”这一特性。
- 给定这样的一个M,
  - 对于A中尚未配对的某顶点a，若$\{(a, b) \mid a$可被b接受$\}$非空. 按照线性序$\leq_a$找出最大元，记为(a, b_j)，删除M中以b_j为端点的边（假如有的话），将(a, b_j)添加到M中。
  - 对于A中尚未配对的所有顶点a，$\{(a, b) \mid a$可被b接受$\}$均为空.（结束）

稳定匹配（稳定的婚姻）– 算法正确性分析

- 结束之时
  - A中的所有顶点对M满意
  - A中未配对的顶点均没有可被接受的对象
- 结束之时，M是稳定的

对任意一个$e \in E \setminus M$，存在$f \in M$满足：

(i) e 和f 有公共端点; (ii) $e <_v f$.



稳定匹配（稳定的婚姻）– 算法正确性分析

- 算法是否会结束？
  - M越来越好，至于不能更好。
- 何为“好”：M 比M’好
  - 对于B中任一顶点b，若b是某个边$f' \in M'$的端点，则b必是某个边$f \in M$的端点，且$f' \leq_b f$.（B中顶点有更好的配对）

工作分配问题

- 问题：n个毕业生有可供选择的m个岗位，每个毕业生给出若干个志愿，是否存在每个人都满意的分配方案。
- 数学模型：建立二部图，V_1中每个点对应一个毕业生，V_2中每个点对应一个可选的岗位，$uv \in E$当且仅当u对应的毕业生愿意选择v对应的岗位。
- 问题的解：问题有解当且仅当G有饱和V_1中所有顶点的完备匹配。

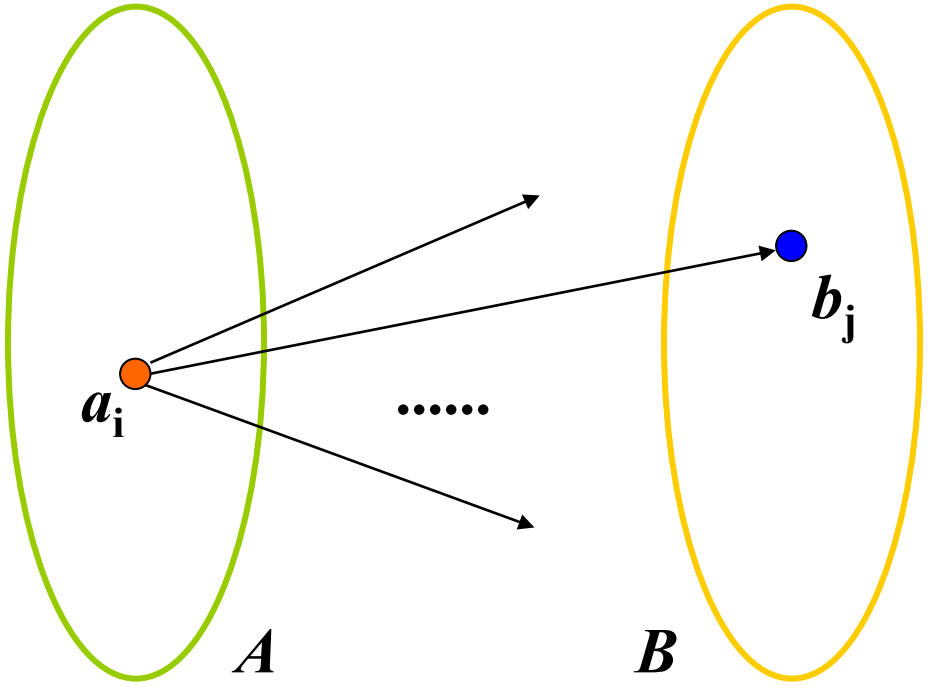
工作分配问题的一般形式

- 工作分配问题
  - 某机构提供m个空缺职位, 有n个申请者。每个申请者满足某些职位的要求。

- 是否可能使每个申请者得到一个他/她适合的职位？
- 若不能，最多多少申请者能够被分配到合适的职位？
- 如何实现一个最佳分配方案？

工作分配问题的求解模型

申请者集合

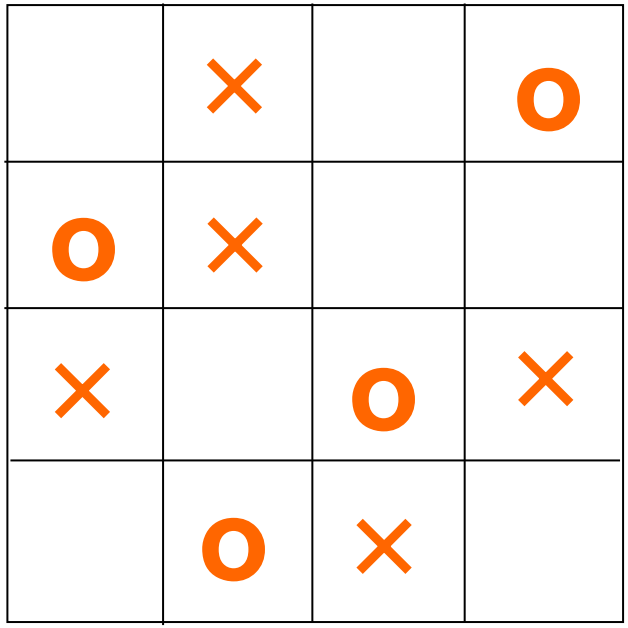


职位的集合

在此模型中如何解释问题的解？

$a_i b_j \in E_G$ iff. a_i 适合于 b_j

棋盘上的士兵



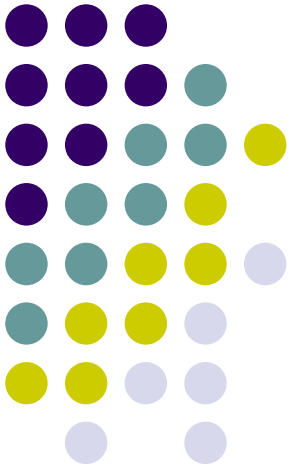
要在左图所示的棋盘上放置4个士兵，任何一行或者一列恰好放一个，但不能放在有标记的格子中。

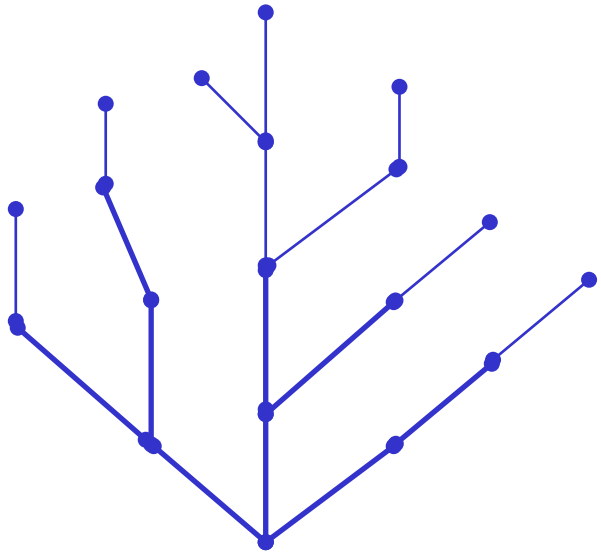
构造一个二步图，a_i表示行，b_j表示列。$a_ib_j \in E$ 当且仅当第i行第j列的方格没有标记。

树的基本概念

离散数学—树

南京大学计算机科学与技术系






fotolia
fotolia
fotolia
fotolia
fotolia
fotolia
fotolia
fotolia
fotolia

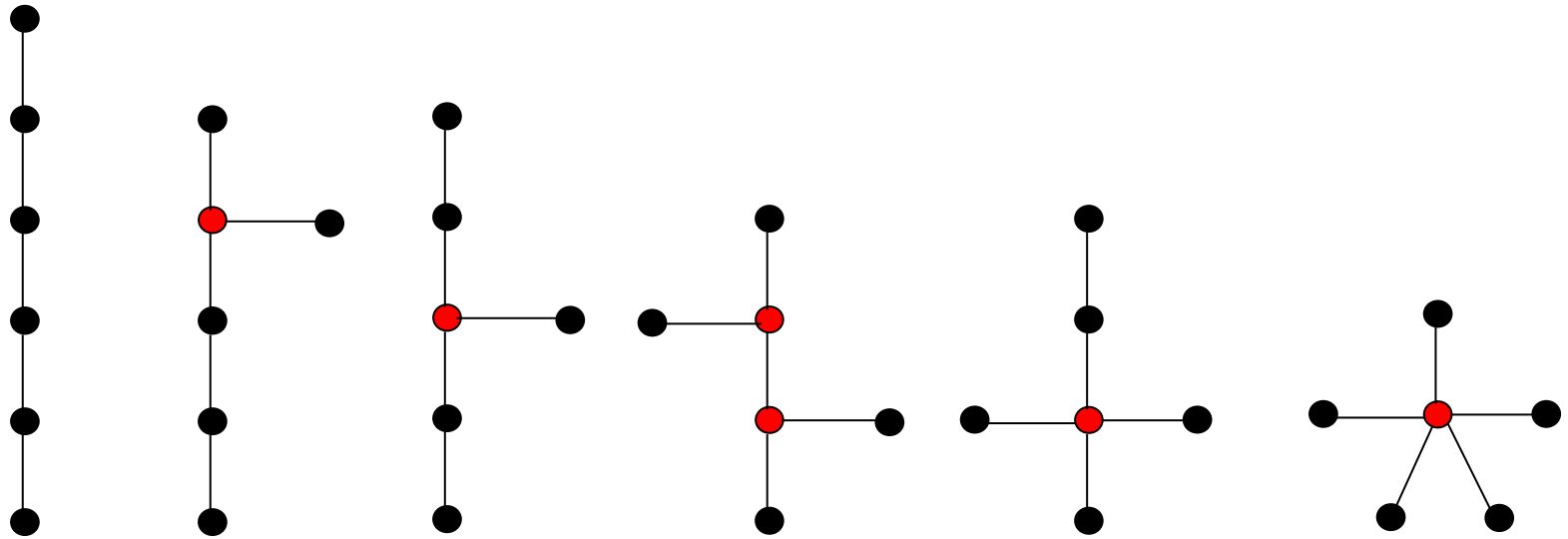
内容提要

- 树的定义
- 树的性质
- 根树
- 有序根树的遍历

树的定义

- 定义：不包含简单回路的连通无向图称为树。
  - 树叶/分支点（度为1？）

// 森林（连通分支为树）无回路的图

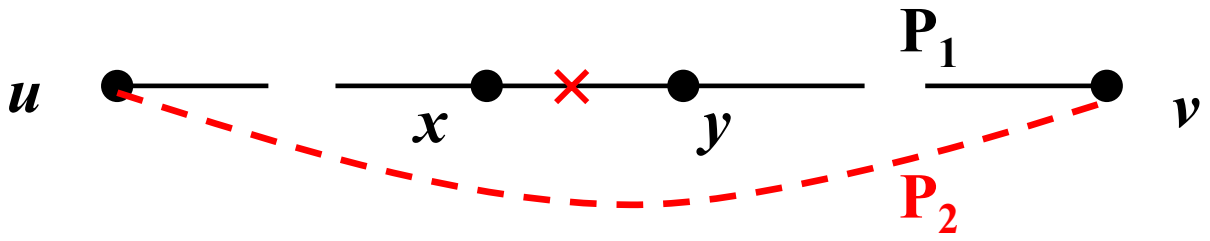


互不同构的6个顶点的树

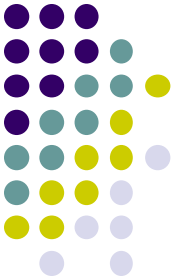
树中的通路

- 设T是树，则$\forall u,v\in V_T$, T中存在唯一的 uv-简单通路。
  - 证明：T是连通图，$\therefore \forall u,v\in V_T$, T中存在uv-简单通路。

  假设T中有两条不同的uv-简单通路P_1, P_2。不失一般性，存在$e=(x,y)$满足：$e\in P_1$但$e\notin P_2$，且在路径P_1上x比y靠近u。令$T^*=T-\{e\}$，则T^*中包含P_2, 于是(P_1中的xu-段)+P_2+(P_1中的vy-段)是T^*中的xy-通路，$\therefore T^*$中含xy-简单通路(记为P')，则P'+e是T中的简单回路，与树的定义矛盾。



有关树的几个等价命题



- 设T是简单无向图，下列四个命题等价：

  (1) T是不包含简单回路的连通图。//树的定义

  (2) T中任意两点之间有唯一简单通路。

  (3) T连通，但删除任意一条边则不再连通。

  (4) T不包含简单回路，但在任意不相邻的顶点对之间加一条边则产生唯一的简单回路。

- 备注：
  - 树是边最少的连通图
  - 树是边最多的无简单回路的图

树中边和点的数量关系

- 设T是树，令$n=|V_T|$, $m=|E_T|$, 则$m=n-1$。
- 证明. 对n进行归纳证明。当$n=1$, T是平凡树，结论显然成立。

  假设当$n\le k$是结论成立。

  若$n=k+1$。因为T中每条边都是割边，任取$e\in E_T$, $T-\{e\}$含两个连通分支，设其为T_1, T_2, 并设它们边数分别是m_1, m_2, 顶点数分别是n_1, n_2, 根据归纳假设：$m_1=n_1-1$, $m_2=n_2-1$。注意：$n_1+n_2=n$, $m_1+m_2=m-1$。

  $\therefore m= m_1+m_2+1=n-1$。

连通图边数的下限

- 顶点数为n ($n\geq 2$) 的连通图，其边数$m\geq n-1$。

  (对于树，$m=n-1$，“树是边最少的连通图”)

  - 证明：对n进行归纳证明。当$n=2$时结论显然成立。

    设G是边数为m的连通图，且$|V_G|=n>2$。任取$v\in V_G$，令G'=G-v,设G'有$\omega(\omega\geq 1)$个连通分支$G_1,G_2,\ldots,G_\omega$，且G_i的边数和顶点数分别是m_i和n_i。

    我们有$n=n_1+\ldots+n_\omega+1$, $m\geq m_1+\ldots+m_\omega+\omega$ (每个连通分支中至少有一个顶点在G中与v相邻)。

    由归纳假设，$m_i\geq n_i-1(i=1,2,\ldots\omega)$。

    所以：$m\geq m_1+\ldots+m_\omega+\omega\geq n_1+\ldots+n_\omega-\omega+\omega=n-1$。

与边点数量关系有关的等价命题

- 设T是简单无向图，下列三个命题等价：

  (1) T是树。

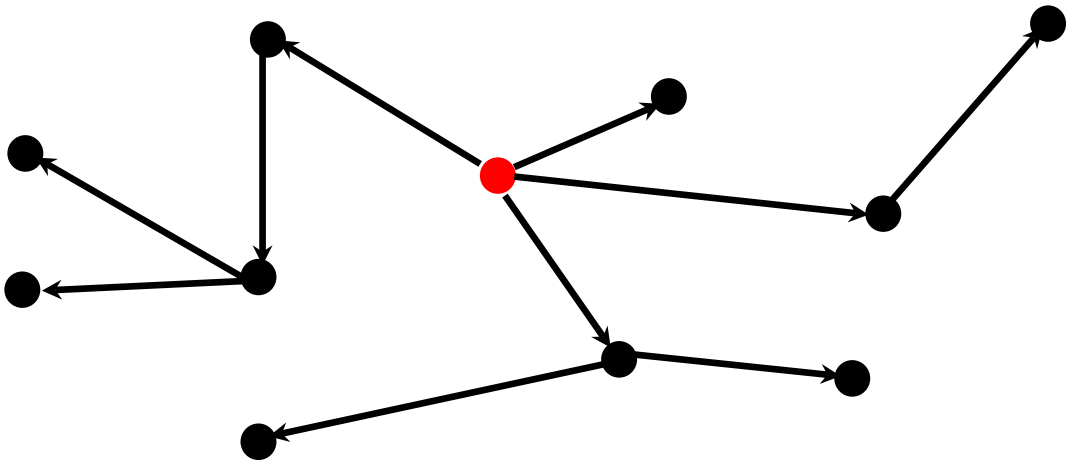
  (2) T连通，且$m=n-1$。

  (3) T不含简单回路，且$m=n-1$。

  - (1)⇒(2)，已证。
  - (2)⇒(3)，若含简单回路，则删除回路中的一条边之后依然连通，因而 $m-1 \geq n-1$，所以$m \geq n$，矛盾。
  - (3)⇒(1)，若不连通，分支数$\omega \geq 2$，各分支为树（无简单回路、连通），则$m=n-\omega<n-1$，矛盾。

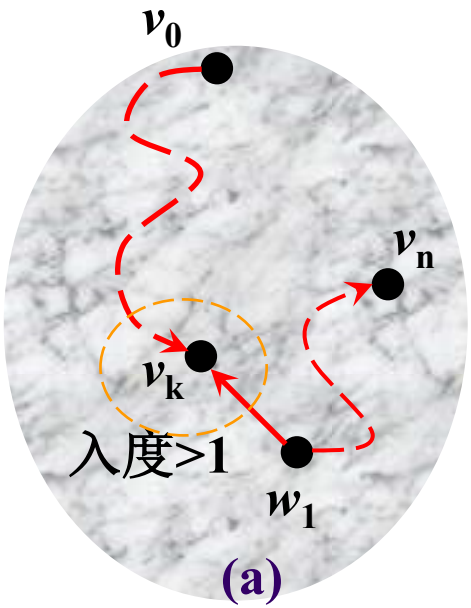
根树的定义

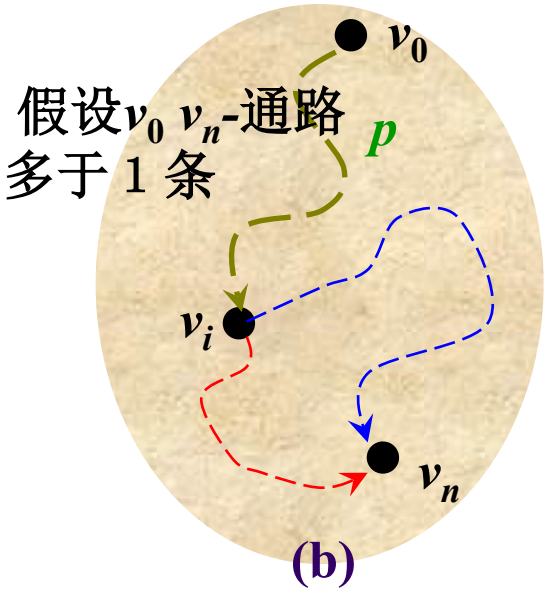
- 定义：底图为树的有向图称为*有向树*。
- 定义：若有向树恰含一个入度为0的顶点，其它顶点入度均为1，则该有向树称为*根树*，那个入度为0的顶点称为*根*。

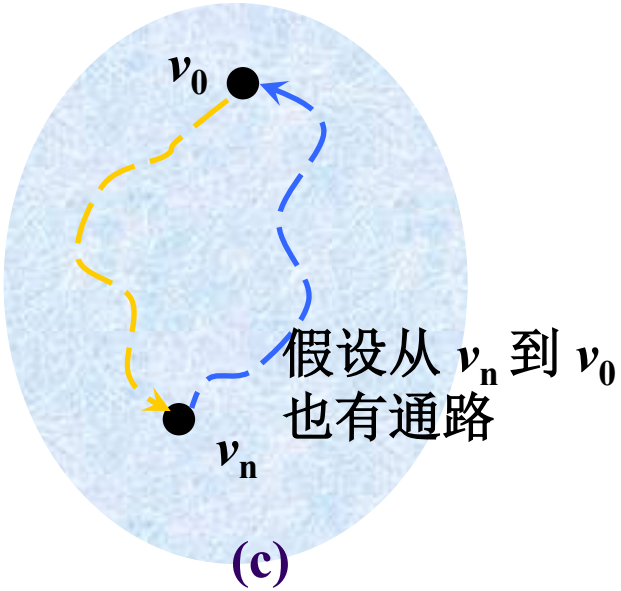


根树中的有向通路

- 若v_0是根树T的根,则对T中任意其它顶点v_n ,存在唯一的有向v_0v_n-通路,但不存在v_nv_0-通路。



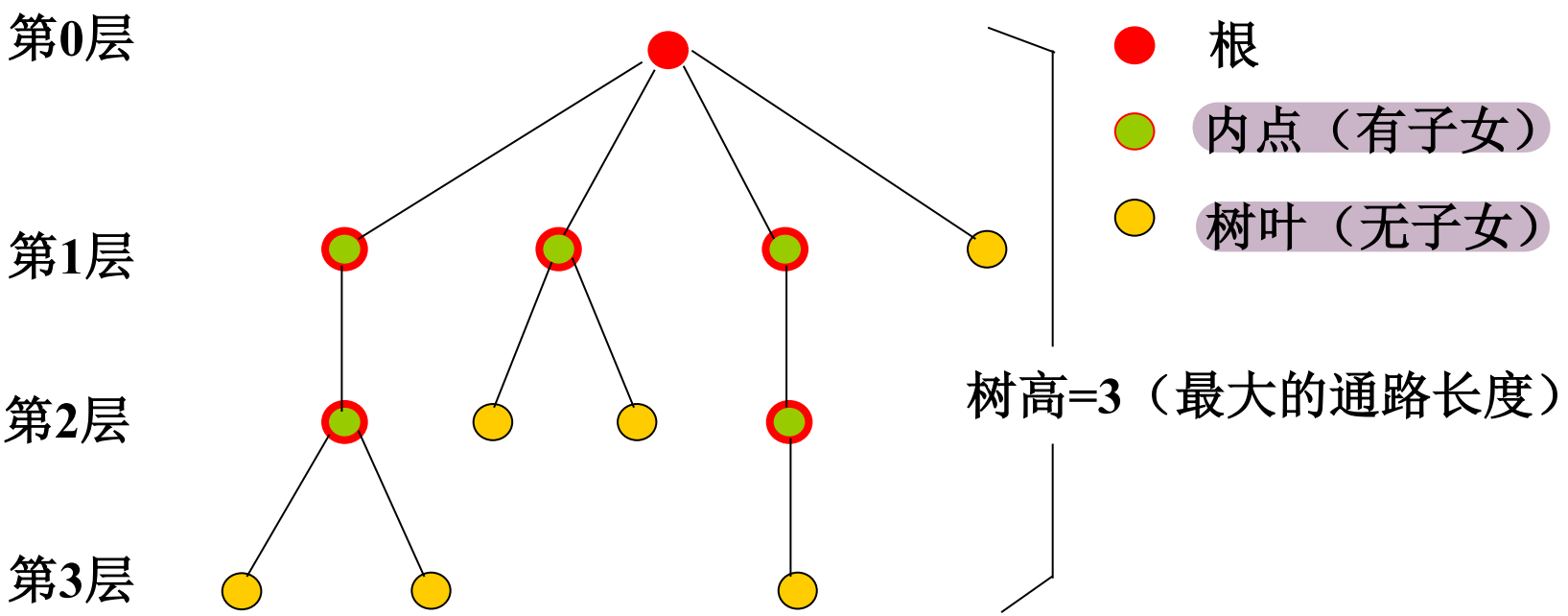




根树的图形表示

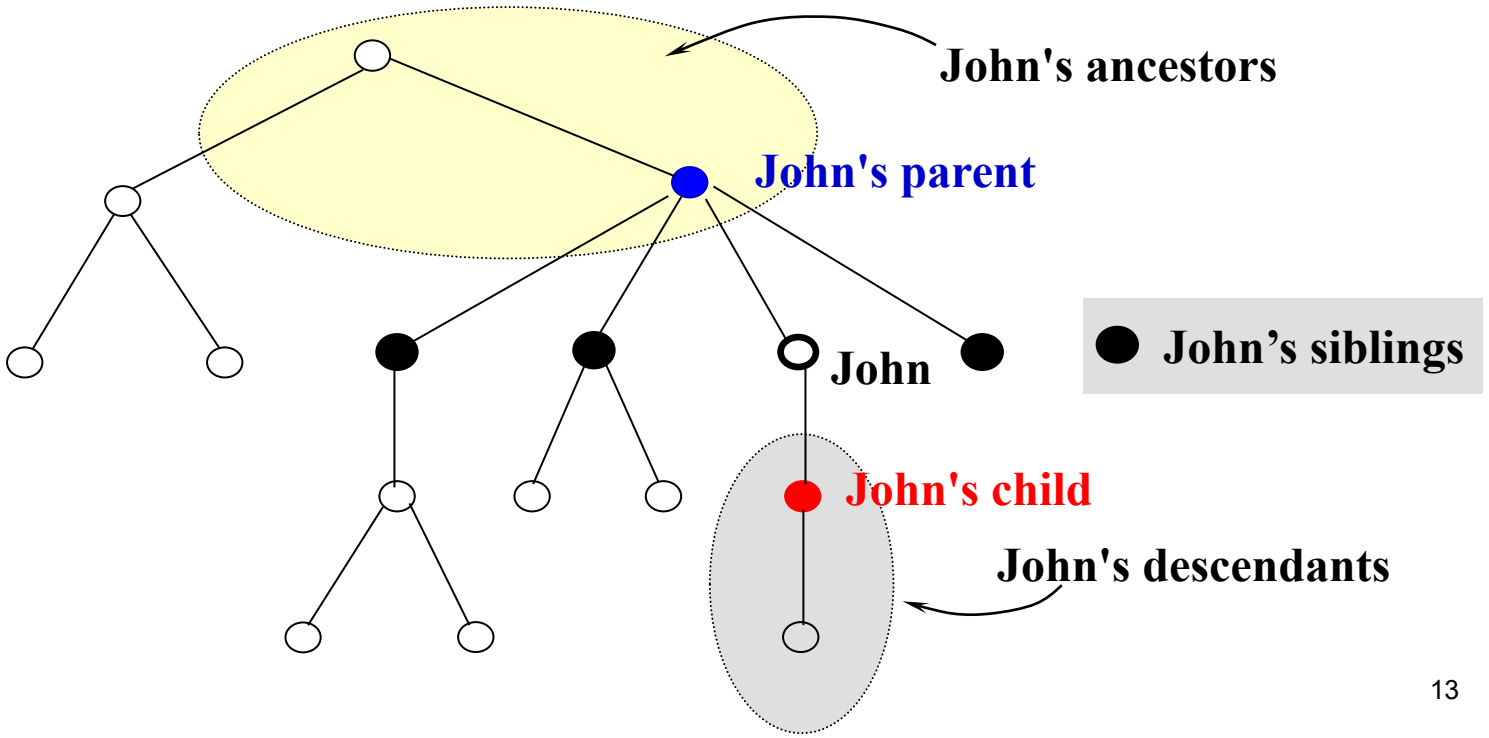
- 边上的方向用约定的位置关系表示

根也是内点，除非它是图中唯一顶点。



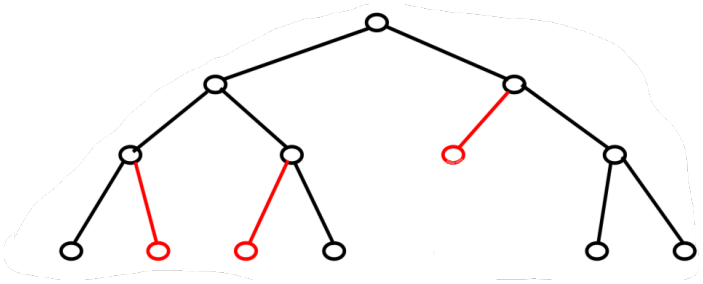
根树与家族关系

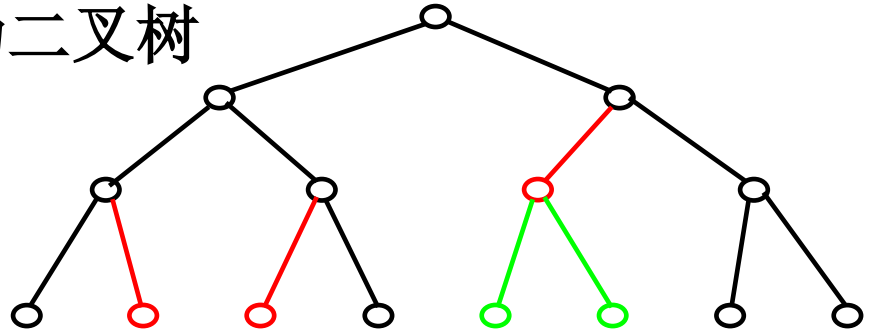
- 用根树容易描述家族关系，反之，家族关系术语被用于描述根树中顶点之间的关系。



根树的几个术语

- ***m*叉树：每个内点至多有*m*个子女**
  - **2叉树也称为二叉树**
- **满*m*叉树(*full* m-ary tree)**
  - **每个内点恰好有*m*个子女**
- **平衡：树叶都在*h*层或(*h*-1)层, *h*为树高。**
- **有序：同层中每个顶点排定次序**
  - **有序二叉树通常也简称为二叉树**

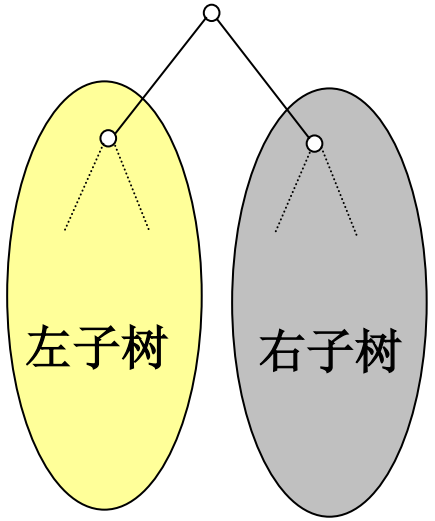




根树的几个术语（续）

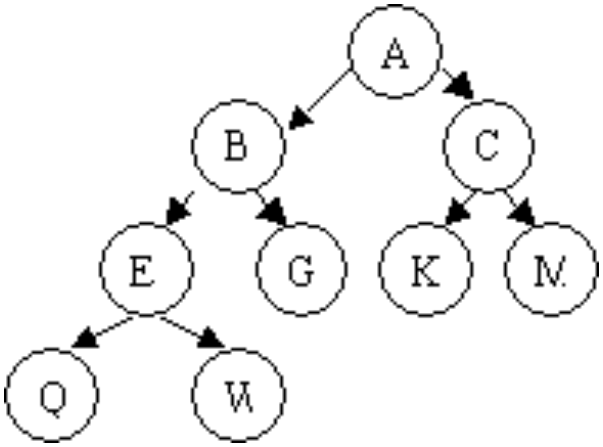
- 定义：设T是根树，T中任一顶点v及其所有后代的导出子图显然也是根树(以v为根)，称为T的根子树。
- 有序二叉树的子树分为左子树和右子树

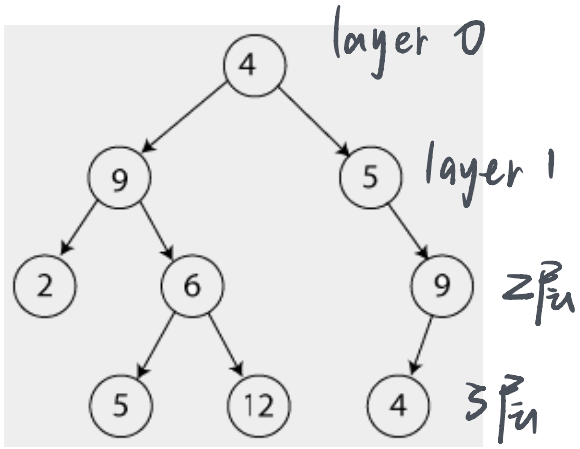
即使不是满二叉数，也可以
分左、右，必须注意顶点位置

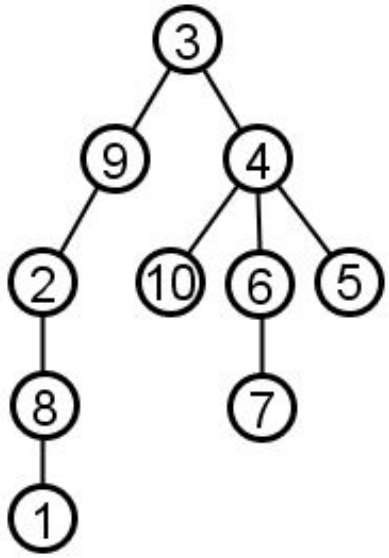


根树（举例）

- 树的高度、各顶点所处的层数
- 满、平衡







满m叉树的顶点数

- 设T是满m叉树，
  - 若T有n个顶点, 则有$i=(n-1)/m$个内点和$l=[(m-1)n+1]/m$个树叶.
  - 若T有i个内点，则有n=$mi+1$顶点和$l=(m-1)i+1$个树叶.
  - 若T有l个树叶，则有$n=(ml-1)/(m-1)$ 个顶点和$i=(l-1)\ )/(m-1)$ 个内点.

$n-1 = m \times i$ （入度总数=出度总数）

$n = i + l$ （顶点分为内点和树叶）

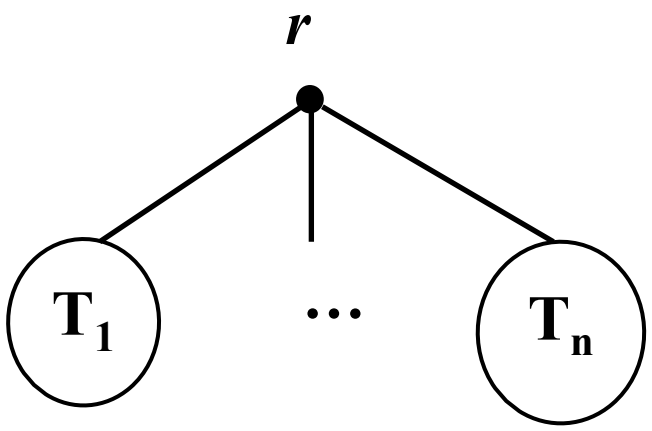
高度为h的m叉树的顶点数

- 高度为h的m叉树最多有个m^h个树叶。
  - 按照高度h进行归纳证明。（第1层顶点最多为m个）
- 若高度为h的m叉树有l个树叶，则$h \geq \lceil \log_m l \rceil$.
  - 如果这棵树是满的且平衡的，则有$h = \lceil \log_m l \rceil$.

$$m^{h-1} < l \leq m^h$$

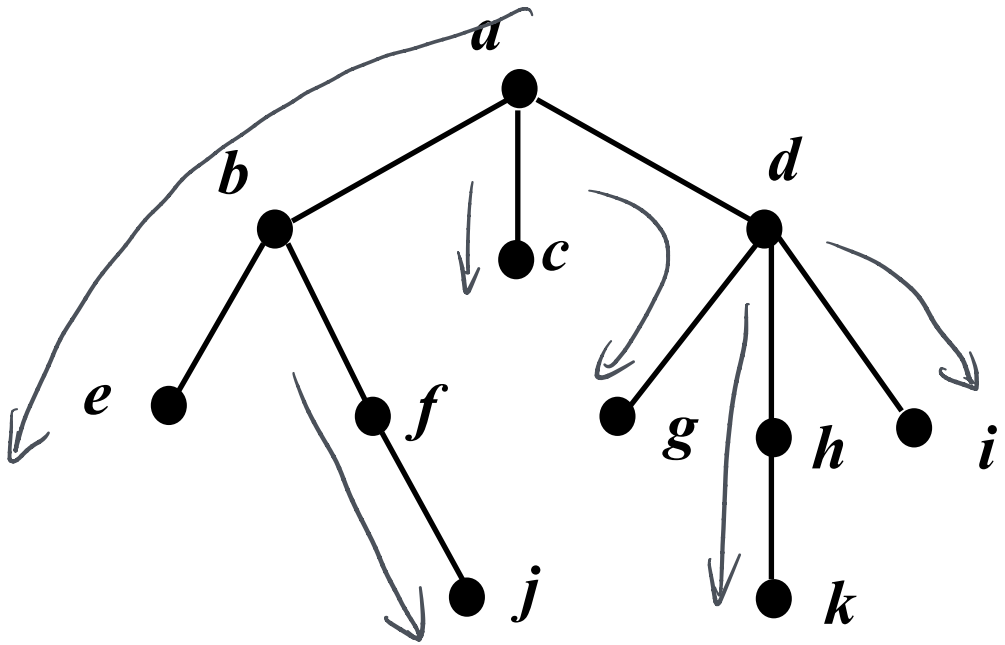
有序根树的遍历

- 前序遍历 （preorder）
  - T只包含根*r*，则为 *r*;
  - T的子树为T_1, …, T_n, 则为 *r*, preorder(T_1), …, preorder(T_n)



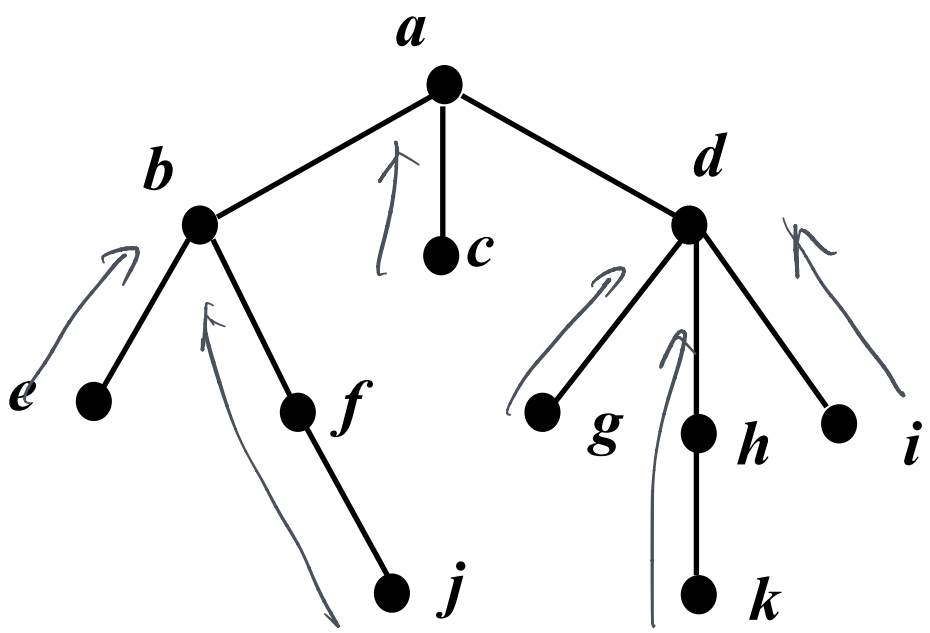
有序根树的遍历

- 前序遍历 （preorder） 深度优先搜索 DFS



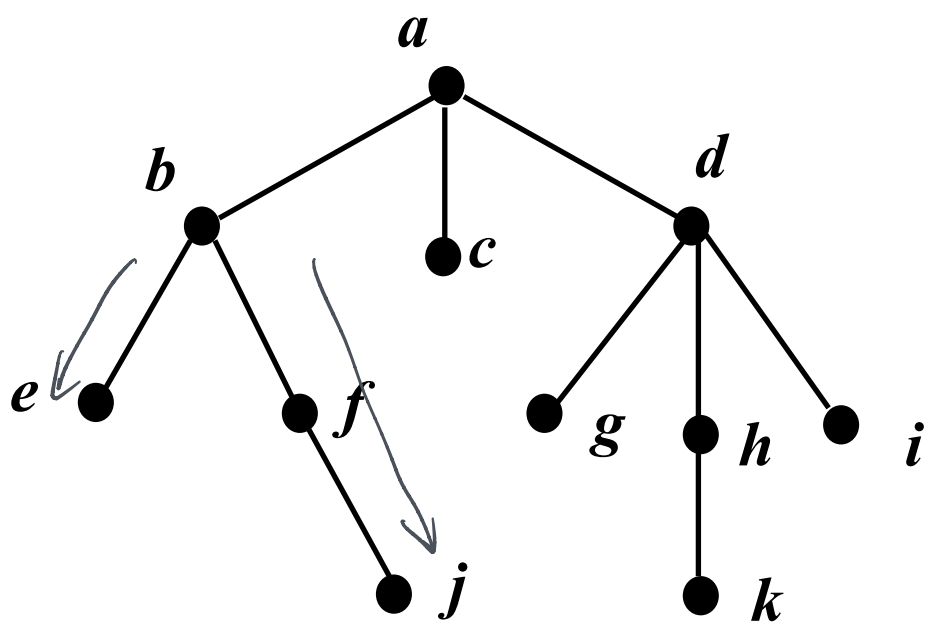
有序根树的遍历

- 后序遍历 （postorder）



有序根树的遍历

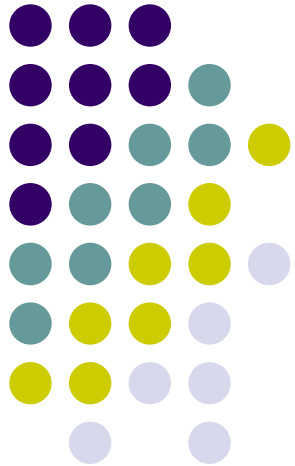
- 中序遍历 （inorder）//先访问第一棵子树



树的应用

离散数学—树

南京大学计算机科学与技术系

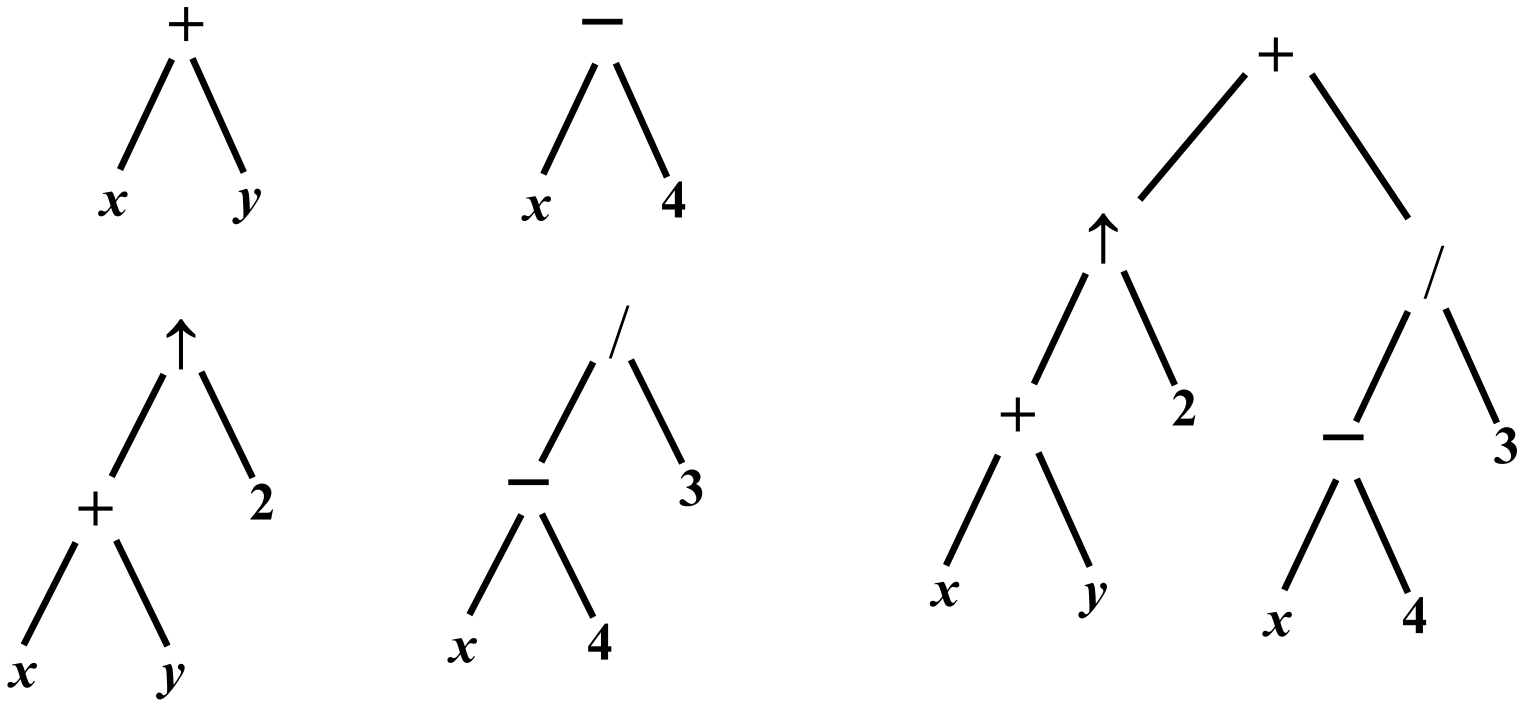


内容提要

- 表达式的（逆）波兰记法
- 二叉搜索树
- 决策树
- 前缀码
- **Huffman编码（算法）**

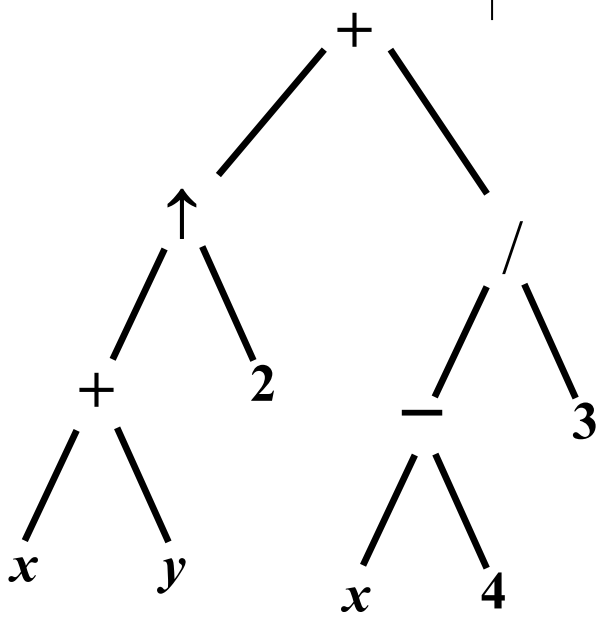
表达式的根树表示

- 用根树表示表达式：内点对应于运算符，树叶对应于运算分量。
- 举例：((*x*+*y*)↑2+ ((*x*-4)/3)



表达式的（逆）波兰表示法

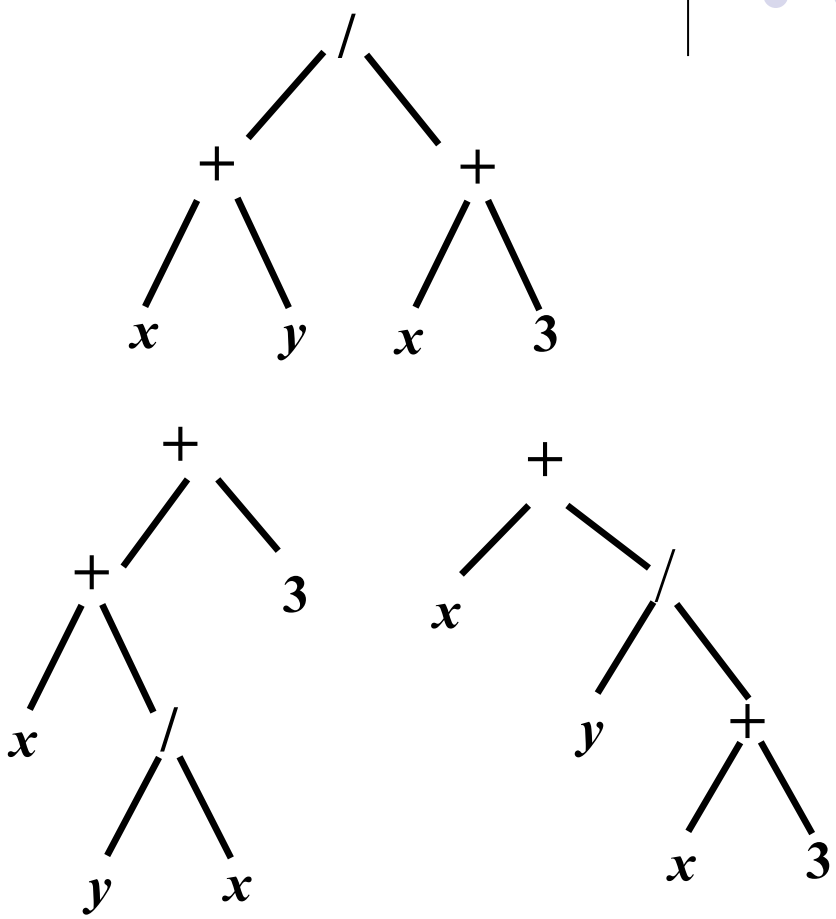
- **(*x*+*y*)↑2+ ((*x*-4)/3)**
- 前缀形式（波兰表示法）
  - **+↑+*xy*2 / -*x*43**
- 后缀形式（逆波兰表示法）
  - ***xy*+2↑ *x*4- 3/+**
- 中缀形式
  - ***x*+*y*↑2+ *x*-4/3**



中缀表示法的缺陷

- 中缀形式：*x*+*y*/*x*+3
  - 有3种解释:
  - (*x*+*y*)/(*x*+3)
  - *x*+*y*/*x*+3
  - *x*+*y*/(*x*+3)

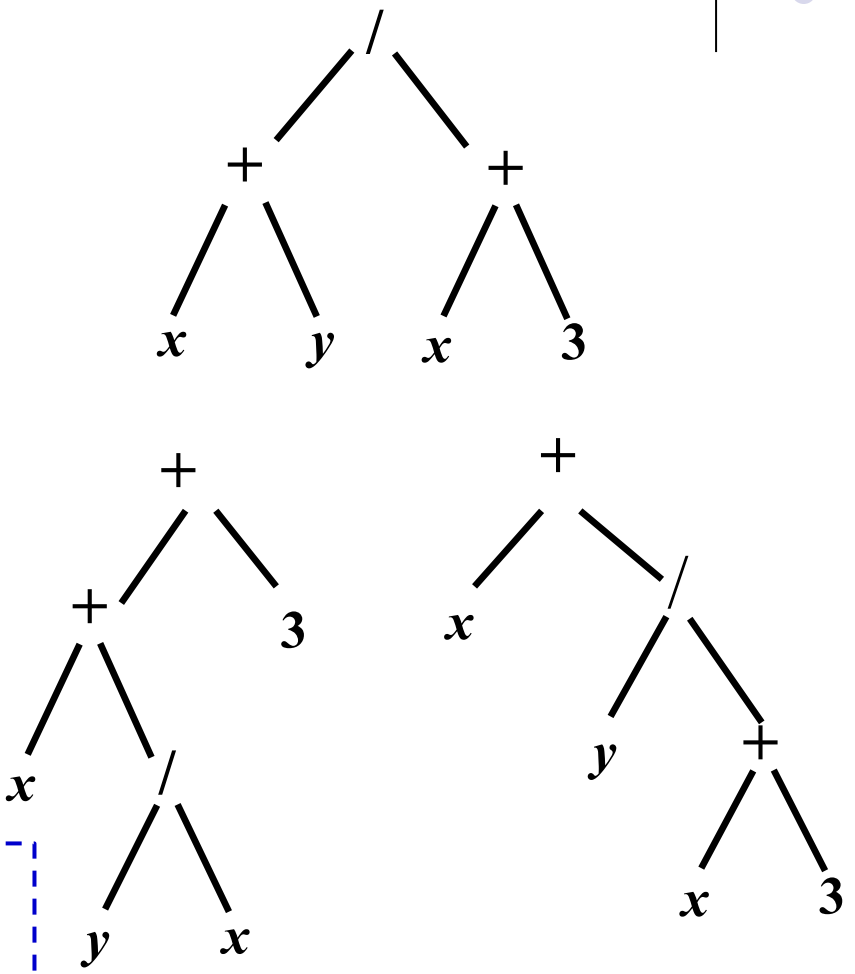
不同的根树有相同的中缀形式。



前缀与后缀则有一定的唯一性。(p. 666: 26-27题)

前缀表示法（波兰表示法）

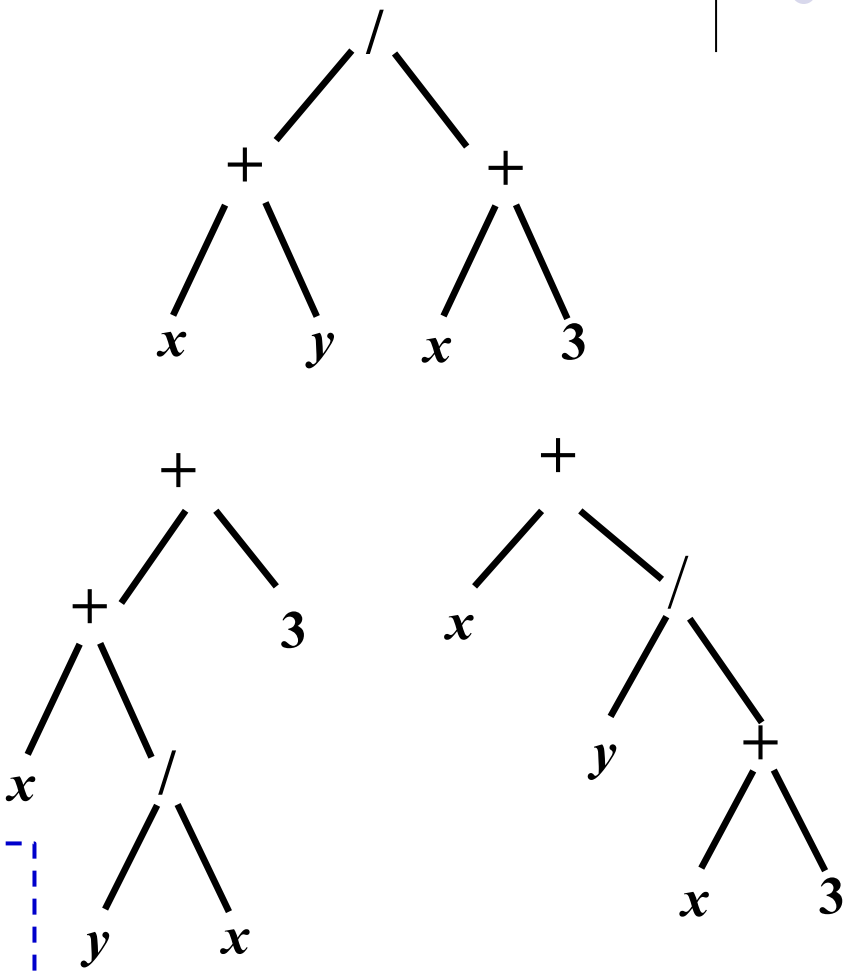
- (*x*+*y*)/(*x*+3)
  - /+*xy*+*x*3
- *x*+*y*/*x*+3
  - ++*x*/*yx*3
- *x*+*y*/(*x*+3)
  - +*x*/*y*+*x*3



从右向左，遇到运算符，对右边紧接着的2个运算对象进行运算

后缀表示法（逆波兰表示法）

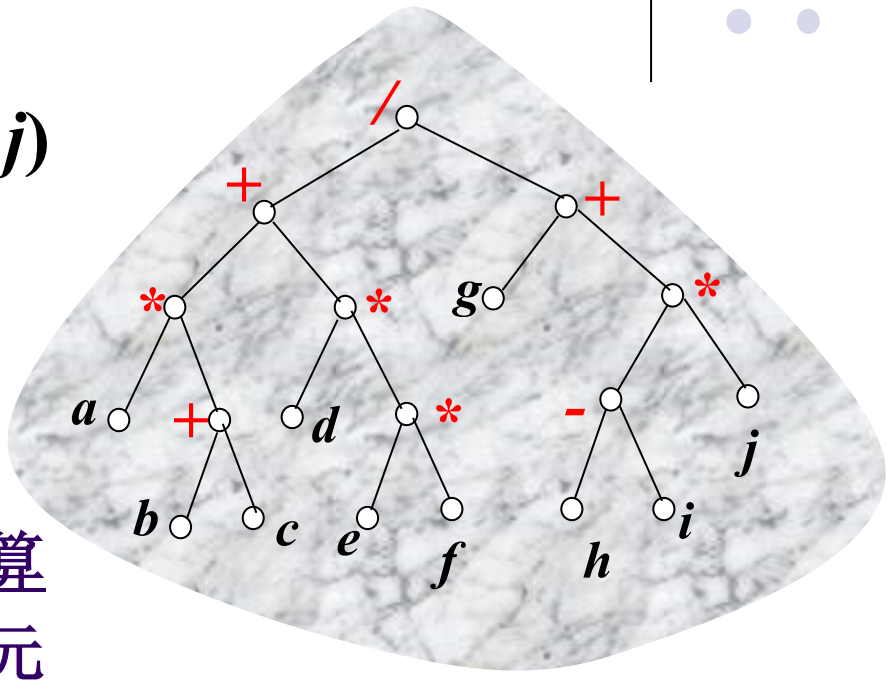
- $(x+y)/(x+3)$
  - $xy+x3+/$
- $x+y/x+3$
  - $xyx/+3+$
- $x+y/(x+3)$
  - $xyx3+/+$



从左向右，遇到运算符，对左边紧接着的2个运算对象进行运算

后缀表示法（逆波兰表示法）

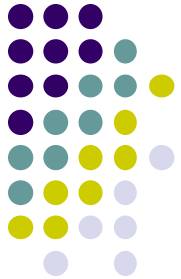
- ***(a*(b+c)+d*(e*f))/(g+(h-i)*j)***
- 逆波兰表示
  - ***abc+*def**+ghi-j*+/***



从左往右，遇到运算符，根据运算符所需运算分量个数确定前面的元素作为运算分量。

不需要括弧唯一地表示计算顺序。

后缀表达式求值



7 2 3 * - 4 ↑ 9 3 / +

7 6 - 4 ↑ 9 3 / +

1 4 ↑ 9 3 / +

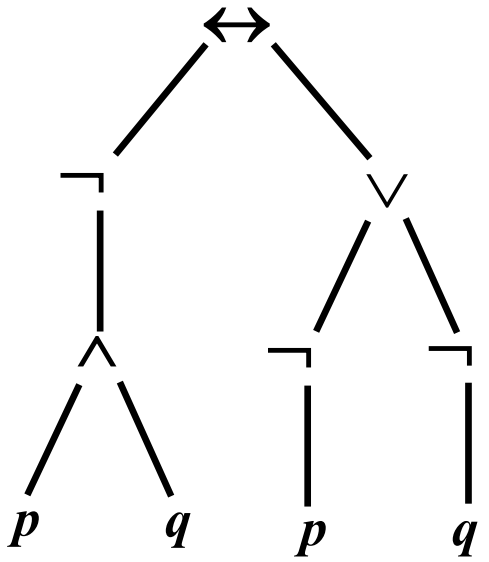
1 9 3 / +

1 3 +

4

复合命题的根树表示

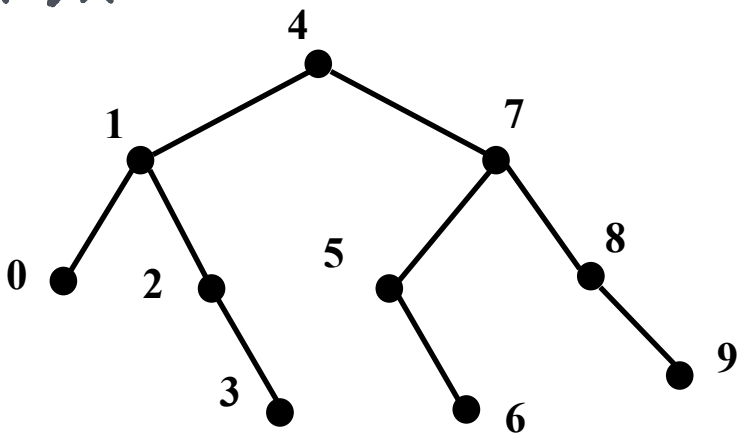
命题：$(\neg(p \wedge q)) \leftrightarrow (\neg p \vee \neg q)$



后缀形式：$pq\wedge\neg p\neg q\neg\vee\leftrightarrow$

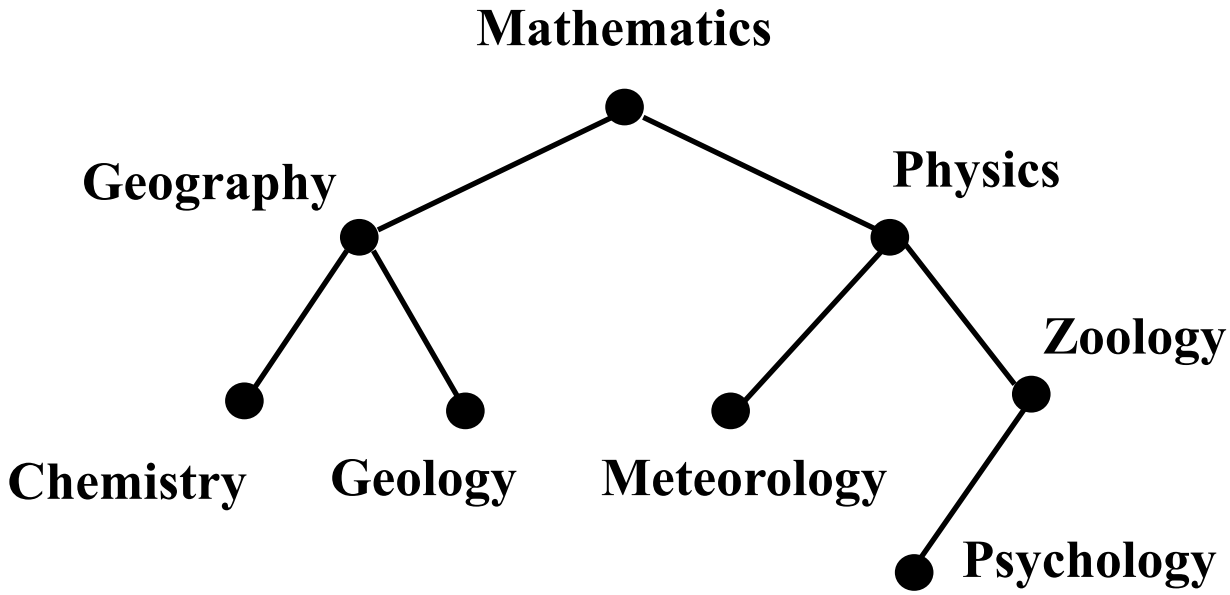
二叉搜索树

- 二叉搜索树满足下列条件
  - 二叉树，各顶点的子女非左即右，左或右都不超过一个。
  - 每个顶点有一个唯一的标号，该标号取自一个全序集。
  - 若*u*是树中任意的顶点，则：左小右大
    - *u* 的左子树中任意顶点的标号小于*u* 的标号。
    - *u* 的右子树中任意顶点的标号大于*u* 的标号。



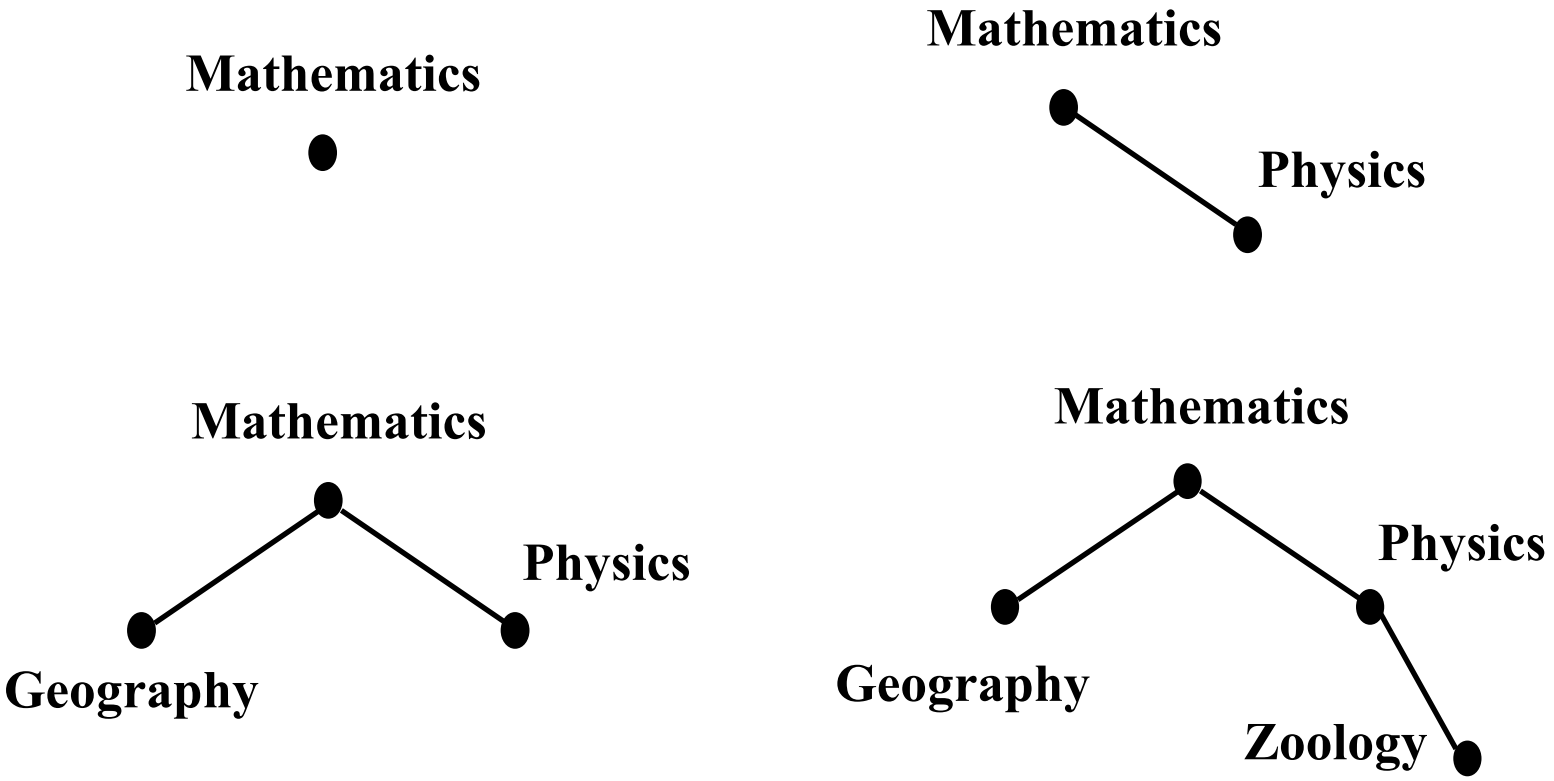
构造二叉搜索树（举例）

mathematics, physics, geography, zoology, meteorology, geology, psychology, chemistry



构造二叉搜索树（举例）

mathematics, physics, geography, zoology, …



二叉搜索树算法

Procedure insertion(T: binary search tree, *x*:item) //定位或添加

v:=root of T //*v*可能为null

while *v* !=null and label(*v*) != *x* {

if *x* < label(*v*) **then**

if left child of *v* !=null then *v*:= left child of *v*

else add *new vertex* as a left child of *v* and set *v*:=null

else

if right child of *v* !=null then *v*:= right child of *v*

else add *new vertex* as a right child of *v* and set *v*:=null

}

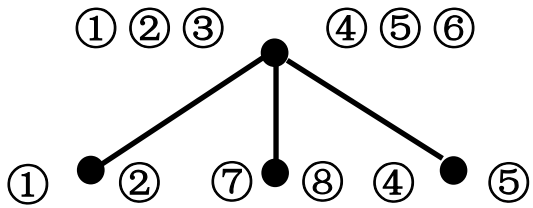
if root of T = null **then** label *new vertex* with *x* and let *v* be this *new vertex*

else if *v*=null or label(*v*) != *x then* label *the new vertex* with *x*

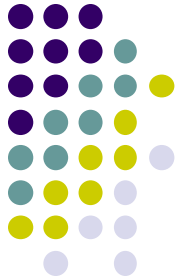
return *v*

决策树

- 这样的根树，每个内点对应一次决策，子树对应于该决策的后果。根到树叶的通路为一个解。
- 举例：8枚硬币，其中7个等重，一个重量较轻的是伪币，使用天平找出伪币，至少多少次称重？
  - 3叉树，至少2次称重才能确保找到。

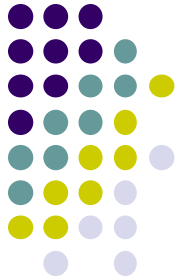


决策树



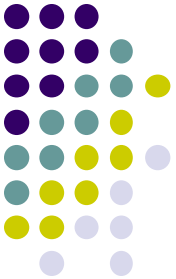
- 以决策树为模型，排序算法最坏情形复杂性的下界。
- 基于二叉比较的排序算法至少需要$\lceil \log (n!) \rceil$次比较。
  - n！个树叶，其二叉树的高度至少为$\lceil \log (n!) \rceil$
  - $\Omega(n \log n)$

编码



- 如何从信号流中识别字符
  - 等长度编码 vs. 不等长度编码
- 例子：对包含{a(45),b(13),c(12),d(16),e(9),f(5)}6个字符的10万个字符的数据文件编码，每个字符后面的数字表示该字符出现的频率(%)。
  - 编码方案一：a(000), b(001), c(010), d(011), e(100), f(101); 则文件总长度30万字位。
  - 编码方案二：a(0), b(101), c(100), d(111), e(1101), f(1100); 则文件总长度22.4万字位，空间节省四分之一。

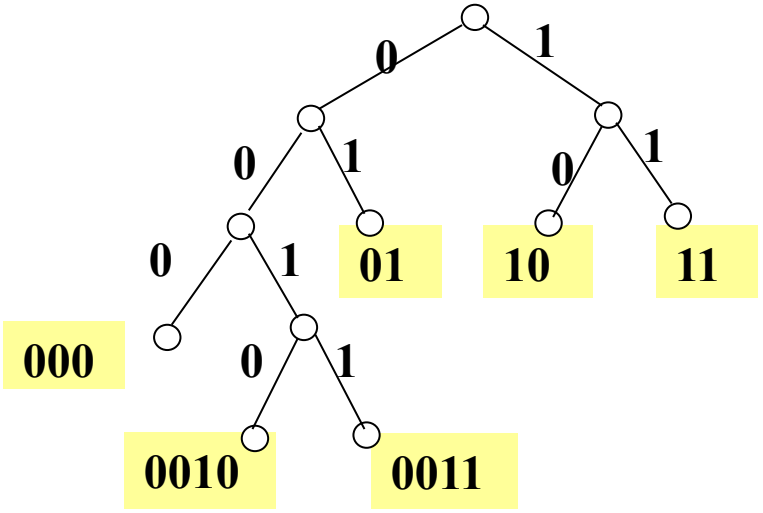
不等长编码的分隔



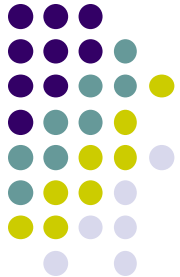
- 如何从信号流中识别不等长编码表示的字符
  - 显式表示长度：专用位或特定结束信号
  - 匹配的唯一性（比如，前缀码）
- 如果符号串α可以表示成符号串β_1和β_2的并置，则β_1称为α的一个前缀。(注意：β_1和β_2可以是空串。)
- 设$A=\{\beta_1,\beta_2,\ldots,\beta_m\}$是符号串的集合，且对任意$\beta_i,\beta_j \in A$, 若$i \neq j$, β_i与β_j互不为前缀，则称A为前缀码。
- 若A中的任意串β_i只含符号0和1, 则称A是二元前缀码。

用二叉树生成二元前缀码

- 生成方法
  - 给边标号：对内点，对其出边标号，左为0，右为1。
  - 给叶编号：从根到每个树叶存在唯一的通路，构成该通路的边的标号依次并置，所得作为该树叶的编号。
- 给定一棵满二叉树，可以产生唯一的二元前缀码。



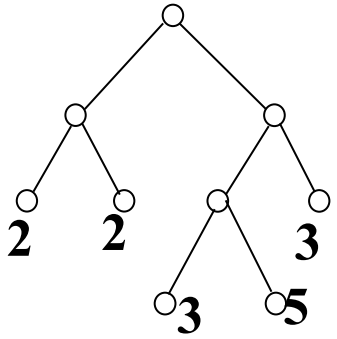
最优前缀码



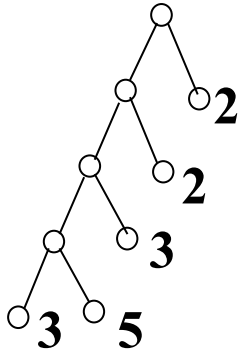
- 问题：二元前缀码$A=\{\beta_1,\beta_2,\ldots,\beta_m\}$表示m个不同的字母，如果各字母使用频率不同，如何设计编码方案可以使总传输量最少。
- 基本思想：使用频率高的字母用尽量短的符号串表示。
- 问题的解：若用频率(相对值)作为树叶的权，最佳二元前缀码对应的二叉树是最优二叉树。

最优二叉树

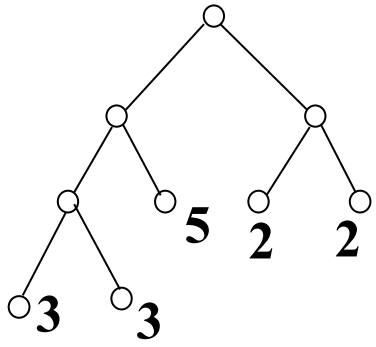
- 若T是二叉树，且每个叶$v_1,v_2,\ldots,v_t$带数值权$w_1,w_2,\ldots w_t$，则二叉树T的权$W(T)$定义为：$\Sigma^t_{i=1} w_i l(v_i)$，其中：$l(v_i)$表示$v_i$的层数。
- 具有相同权序列的二叉树中权最小的一棵树称为最优二叉树。



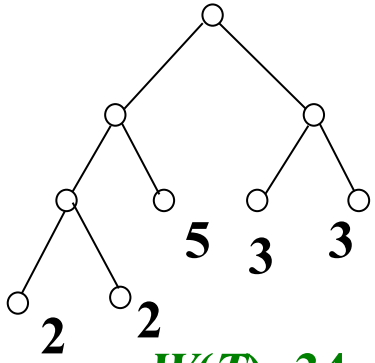
$W(T)=38$



$W(T)=47$



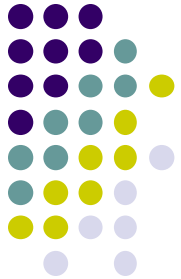
$W(T)=36$



$W(T)=34$

注意：最优二叉树一定是满二叉树（$t \geq 2$）

Huffman Coding (1952)

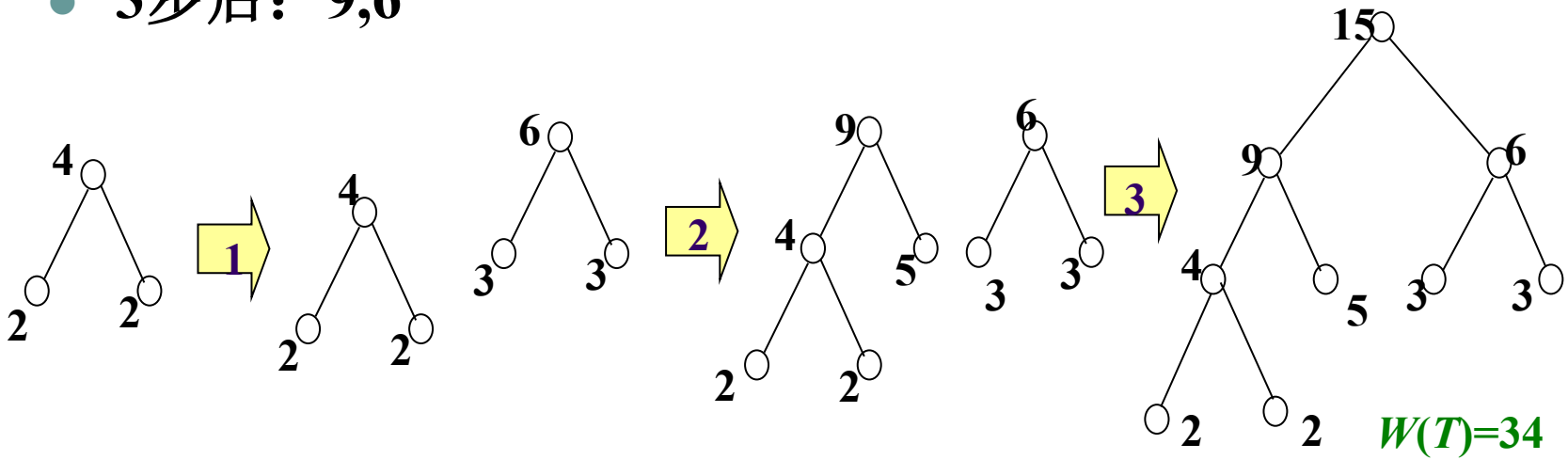


- 输入：正实数序列$w_1,w_2,\ldots,w_t$。
- 输出：具有t个树叶，其权序列为$w_1,w_2,\ldots,w_t$的最优二叉树。
- 过程：
  - T棵根树（森林），其根的权分别是$w_1,w_2,\ldots,w_t$。
  - 选择根权最小的两棵树，以它们为左、右子树（合并）生成新的二叉树，其根权等于两棵子树的根权之和。
  - 重复第2步，直至形成一棵树。

注意：结果可能不唯一(如果“当前”权最小顶点对不唯一)。

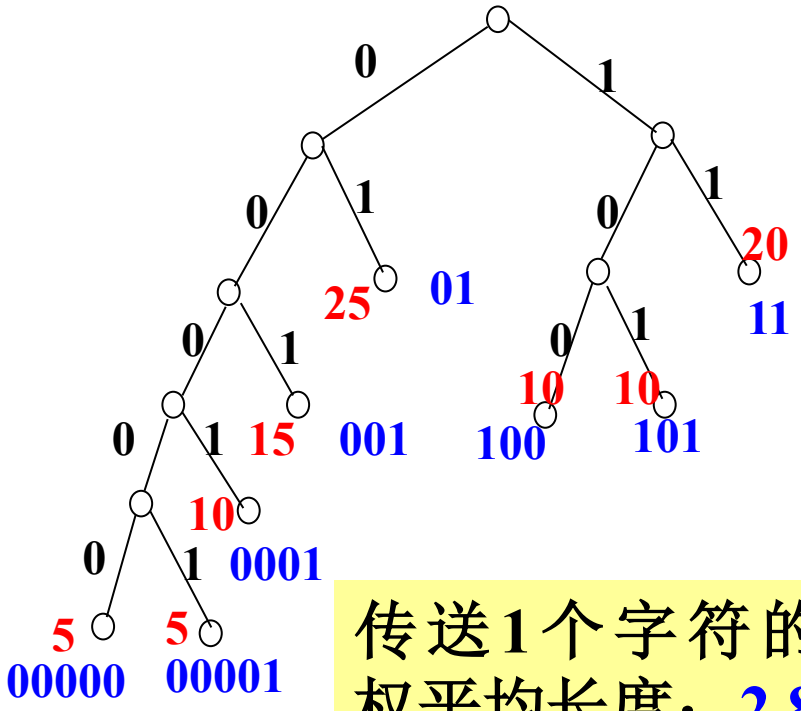
霍夫曼编码: 举例

- 例子 ：开始序列：2,2,3,3,5
  - 1步后：4,3,3,5
  - 2步后：4,6,5
  - 3步后：9,6



一个应用示例

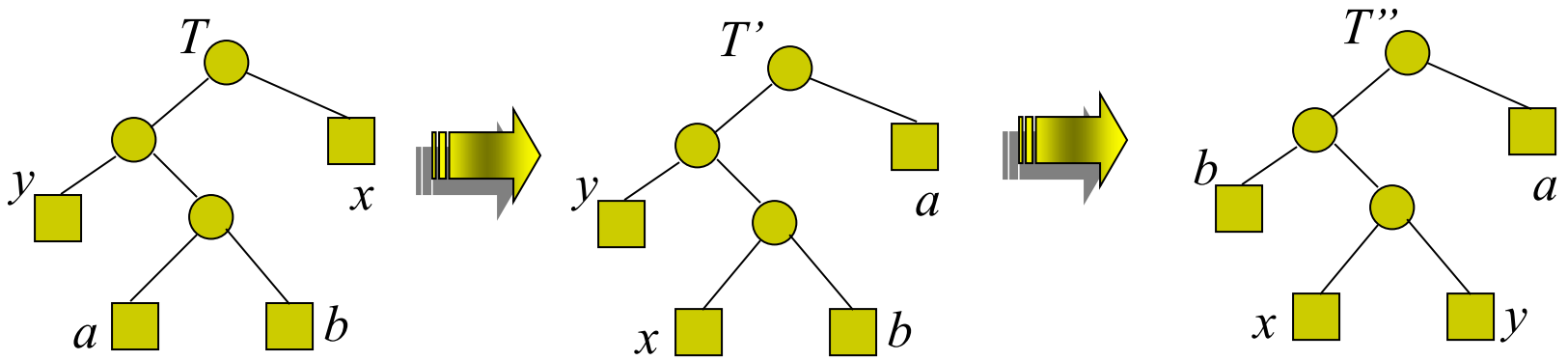
- 八个字符的传输问题
  - 假设八个字符的频率如下：
    - 0：25%　1: 20%
    - 2: 15%　3: 10%
    - 4: 10%　5: 10%
    - 6: 5%　7: 5%
  - 则对应的权为：
    - 5,5,10,10,10,15,20,25



传送1个字符的加权平均长度：2.85

Huffman算法的正确性

设C是字母表，其中每个字符c的频率为$f[c]$。若x,y是两个频率最小的字符，则必存在C的一种最优前缀码，使得x,y的编码仅有最后一位不同。



T为任意最优前缀码

在上图的变换中，二叉树的权保持不变，即：$W(T) \geq W(T') \geq W(T'') \geq W(T)$

保持权不变的变换

不妨假设$f[a] \le f[b], f[x] \le f[y]$; 于是$f[x] \le f[a], f[y] \le f[b]$

$$W(T) - W(T') = \sum_{c \in C} f(c) d_T(c) - \sum_{c \in C} f(c) d_{T'}(c)$$

$$= f[x] d_T(x) + f[a] d_T(a) - f[x] d_{T'}(x) - f[a] d_{T'}(a)$$

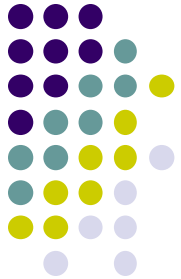
$$= f[x] d_T(x) + f[a] d_T(a) - f[x] d_T(a) - f[a] d_T(x)$$

$$= (f[a] - f[x])(d_T(a) - d_T(x)) \ge 0$$

$\therefore W(T) \ge W(T')$; 同理, $W(T') \ge W(T'')$; 但$W(T)$最小

$\therefore W(T) = W(T') = W(T'')$

Huffman算法的正确性（续）



C是字母表，$f[c]$为字符c的频率，x,y是两个频率最小的字符。令$C'=C-\{x,y\}\cup\{z\}$，$f[z]=f[x]+f[y]$，若T'是C'的最优二叉树，则将顶点z替换为分支点，并以x,y为其子女，所得T是C的一棵最优二叉树。

$d_T(x) = d_T(y) = d_{T'}(z) + 1,$

因此, $f[x]d_T(x) + f[y]d_T(y) = (f[x] + f[y])(d_{T'}(z) + 1)$

$= f[z]d_{T'}(z) + (f[x] + f[y])$

于是, $W(T) = W(T') + (f[x] + f[y])$

如果存在 T'' 满足 $W(T'') < W(T)$, 不失一般性，x与y在T''中为sibling

将x, y连同它们的父结点替换为一叶结点z, 并令$f[z] = f[x] + f[y]$,

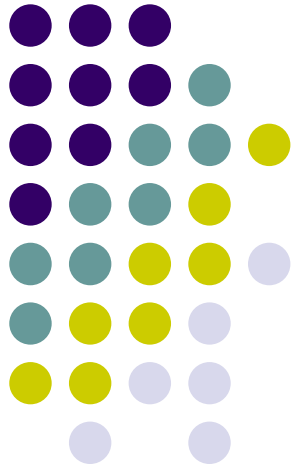
设得到的新树为T''', 则:

$W(T''') = W(T'') - f[x] - f[y] < W(T) - f[x] - f[y] = W(T')$, 矛盾

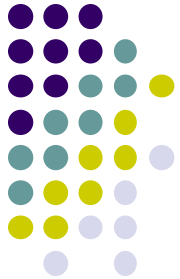
生成树

离散数学—树

南京大学计算机科学与技术系



内容提要



- 生成树
- 深度优先搜索
- 广度优先搜索
- 有向图的深度优先搜索
- 回溯
- 最小生成树算法

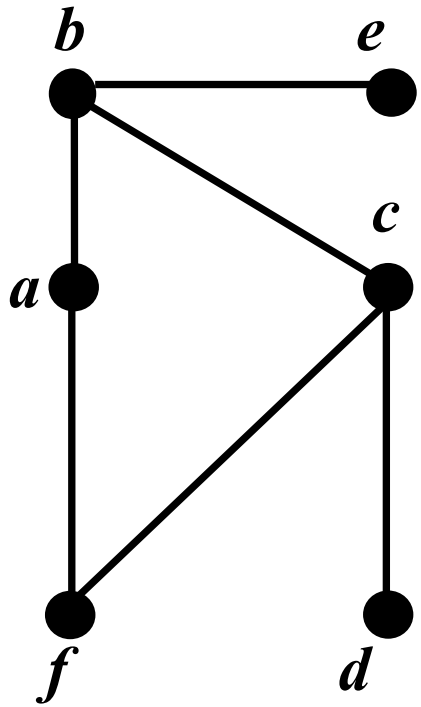
生成树

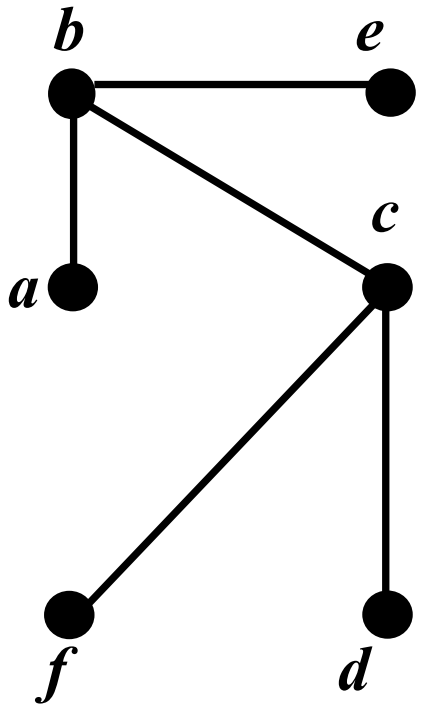
- 定义：若图G的一个子图包含G的所有顶点，且本身是一棵树，则该子图称为G的生成树。
- 无向图G连通 当且仅当 G有生成树
  - 证明(充分性显然)：

  ⇒ 若G是有简单回路的连通图，删除回路上的一条边，G中的回路一定减少。(因此，用“破圈法”总可以构造连通图的生成树)
- 简单无向图G是树 当且仅当 G有唯一的生成树。

  注意：G中任一简单回路至少有三条不同的边。

构造生成树：深度优先搜索





深度优先搜索算法

Procedure DFS(G: 带顶点v_1, …,v_n的连通图)

T:=只包含顶点v_1的树；

visit(v_1)；

Procedure visit(v: G的顶点)

for v每个邻居w {

if w不在T中 then {

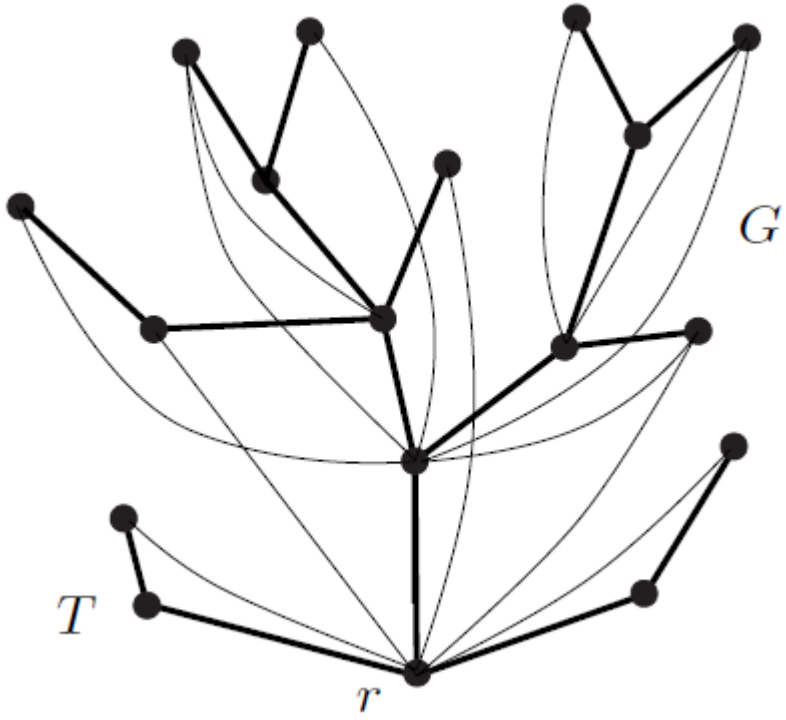
加入顶点w和边{v, w}到T；

visit(w)；

}

}

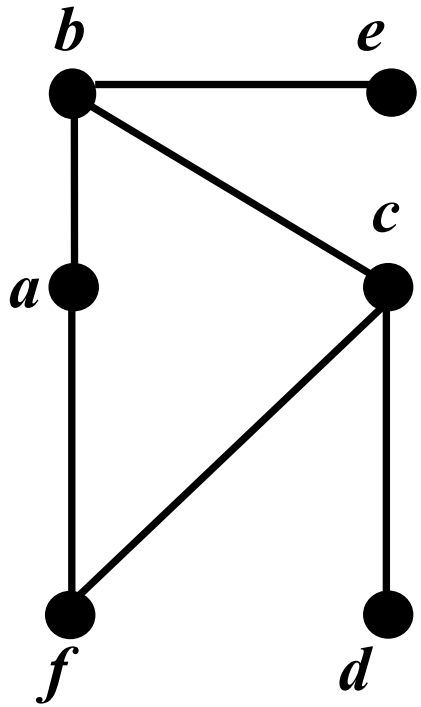
depth-first search tree

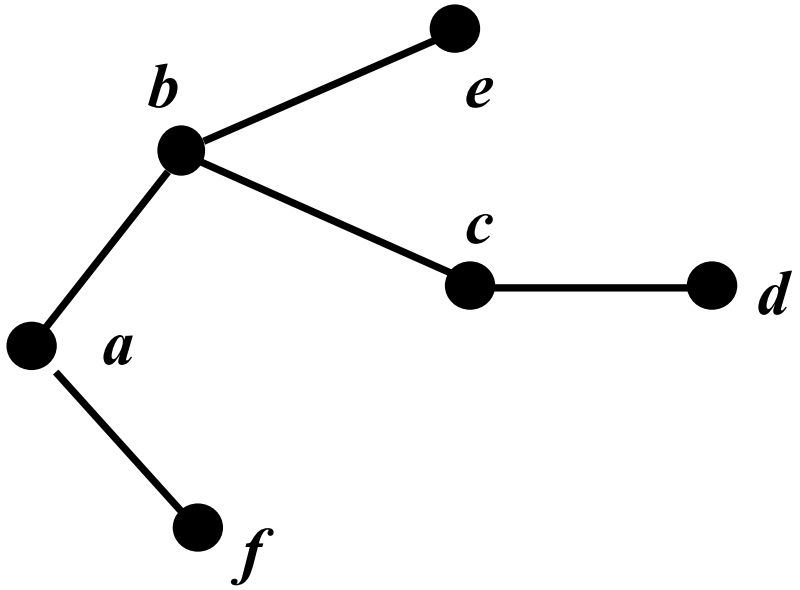


A depth-first search tree with root r

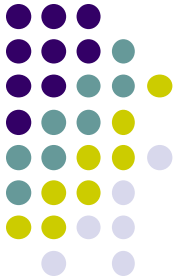
- Normal spanning trees are also called *depth-first search trees*.

构造生成树：广度优先搜索





广度优先搜索算法



Procedure BFS(G: 带顶点v_1, …,v_n的连通图)

T:=只包含顶点v_1的树; L:=空表; 把v_1放入表L中

While L非空 {

删除L中的第一个顶点*v*;

for *v*的每个邻居*w* {

if *w*既不在L中也不在T中 then {

加入*w*到L的末尾;

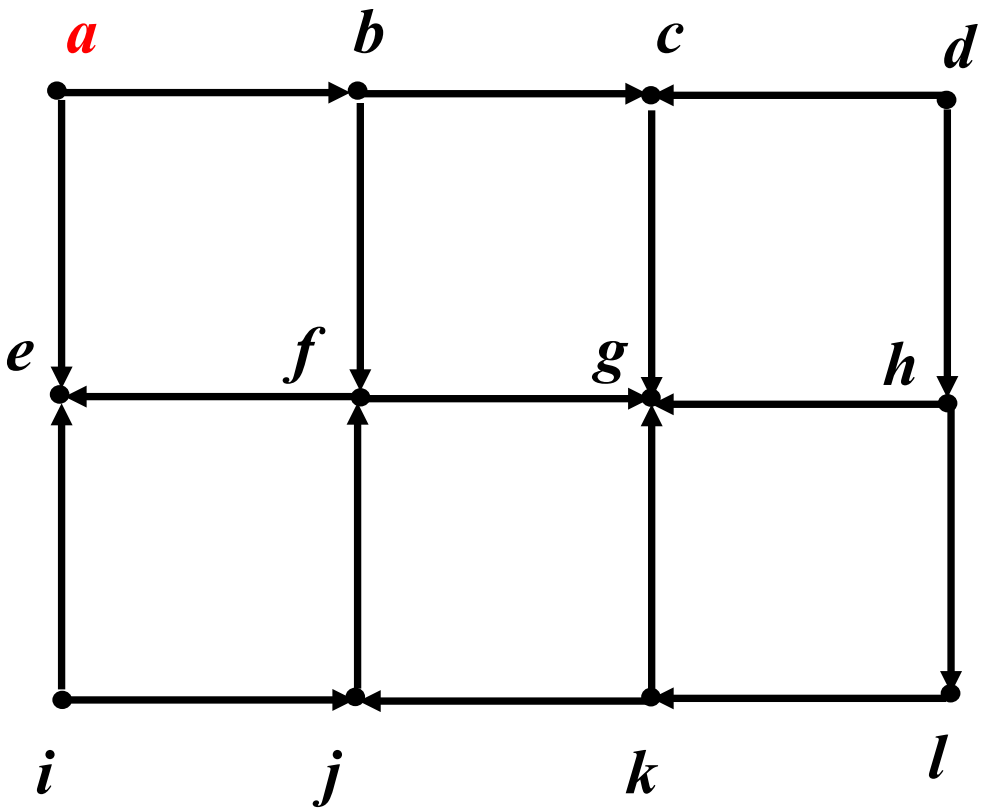
加入顶点*w*和边{*v*, *w*}到T;

}

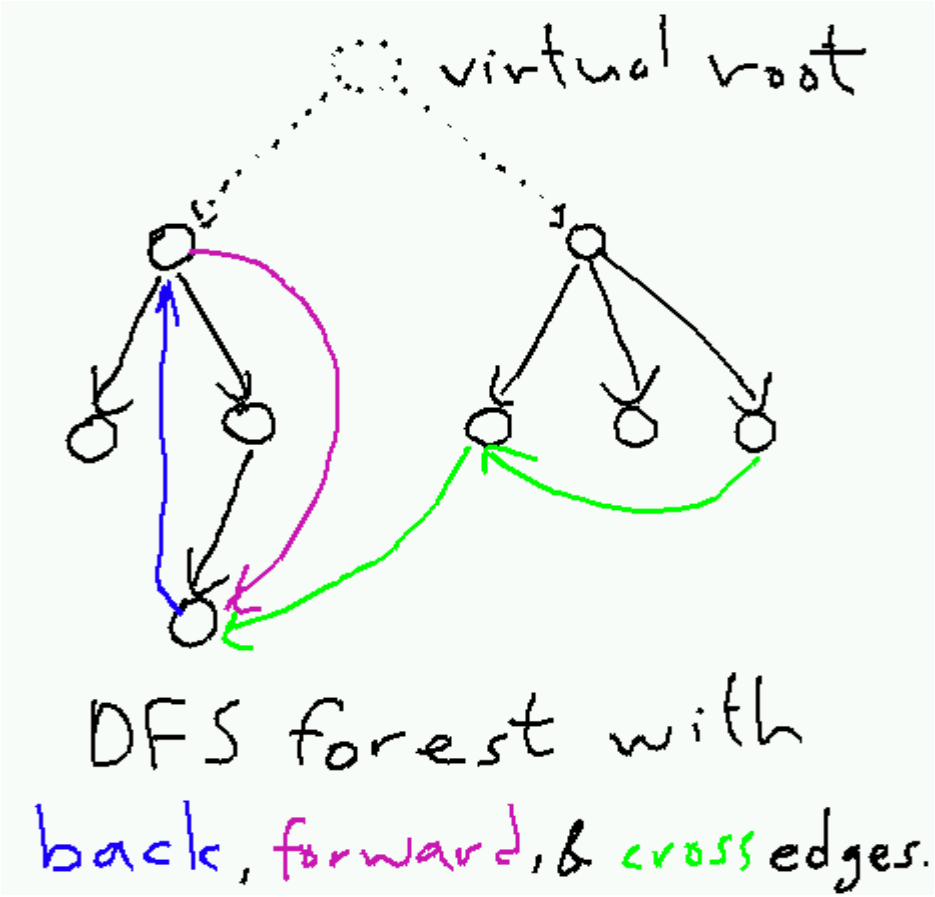
}

}

有向图的深度优先搜索



有向图的深度优先搜索



http://pine.cs.yale.edu/pinewiki/DepthFirstSearch

回溯（八皇后）

在$n \times n$格的棋盘上放置彼此不受攻击的n个皇后。

从空棋盘开始

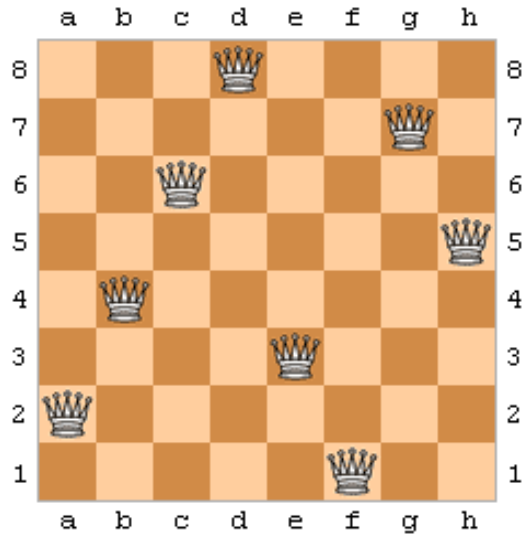
尝试第1列，第1行，… n行；

尝试第2列，第1行，… n行；

….

尝试第k+1列，第1行，… n行；

…



回溯（子集和）

给定一组正整数$x_1, \ldots, x_n$，和为M的一个子集？

从空子集开始

尝试添加一项，

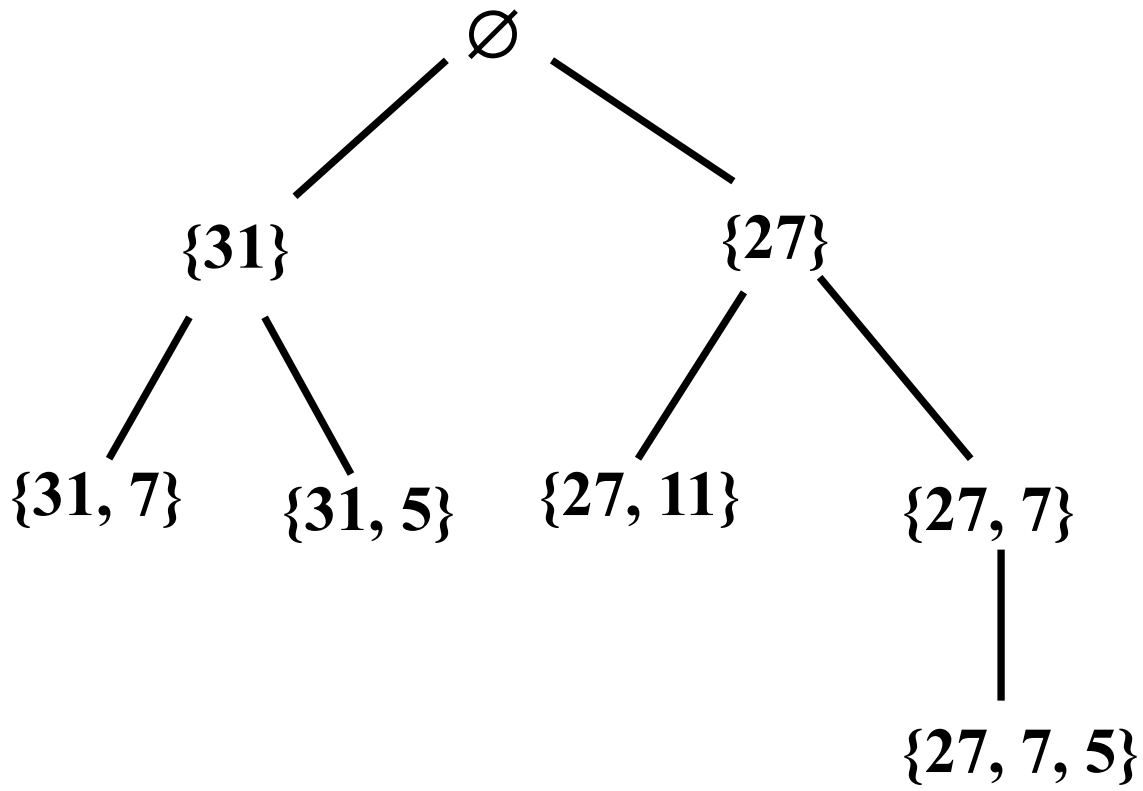
和等于M，结束；

和不超过M，子集包含它；

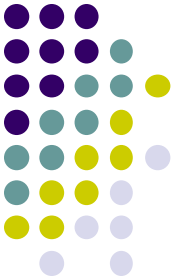
没有合适添加项，去掉和的最后一项，

回溯（子集和）

举例：{31, 27, 15, 11, 7, 5}, 和为39的子集？



Prim算法（求最小生成树）



1: E={*e*}, *e*是权最小的边

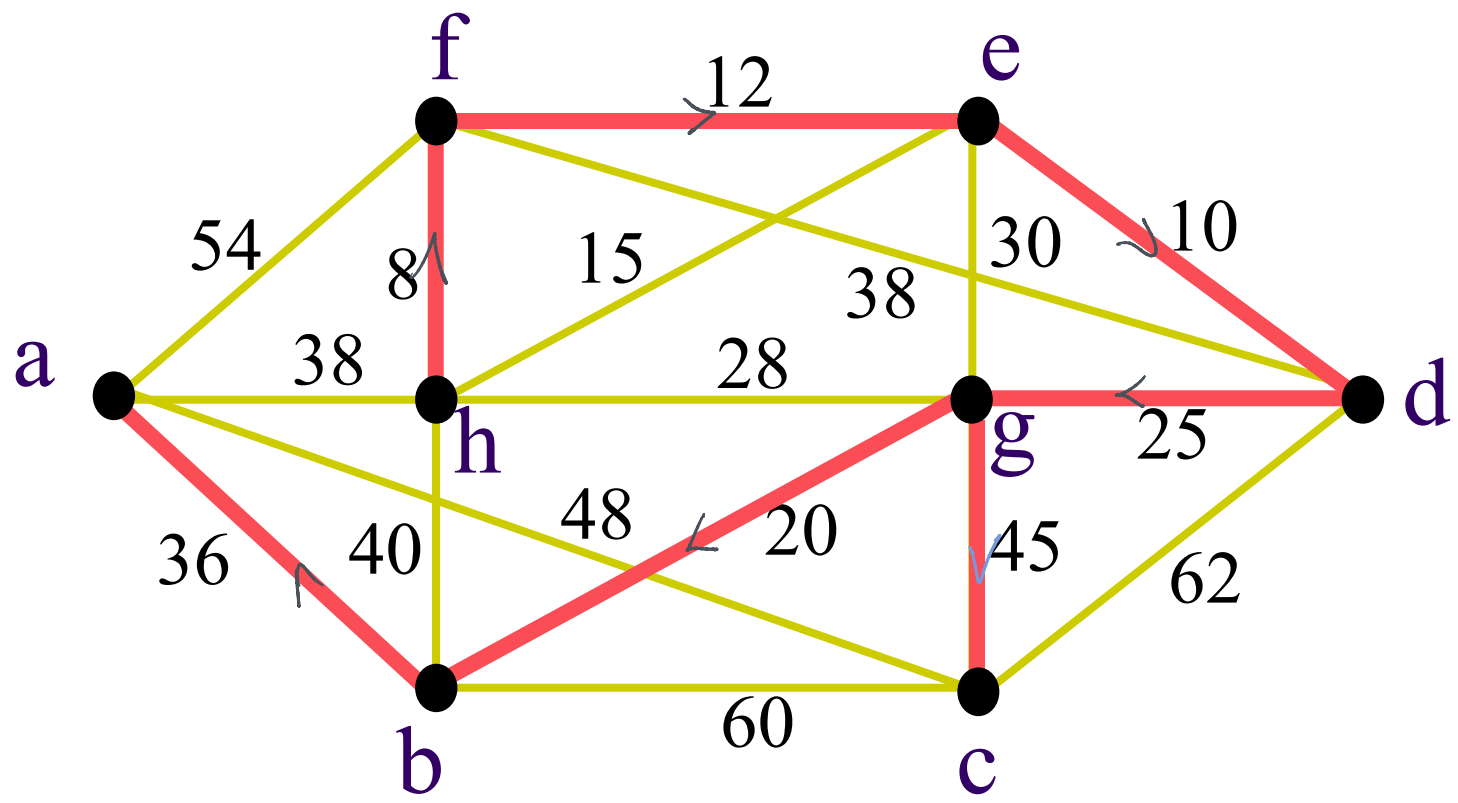
2: 从E以外选择与E里顶点关联，又不会与E中的边构成回路的权最小的边加入E

3: 重复第2步，直到E中包含*n*-1条边

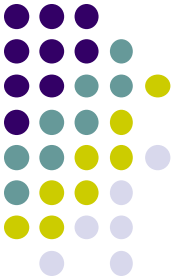
算法结束

Prim算法（举例）

- 铺设一个连接各个城市的光纤通信网络（单位：万元）。



Kruskal算法（求最小生成树）



1: E={ }

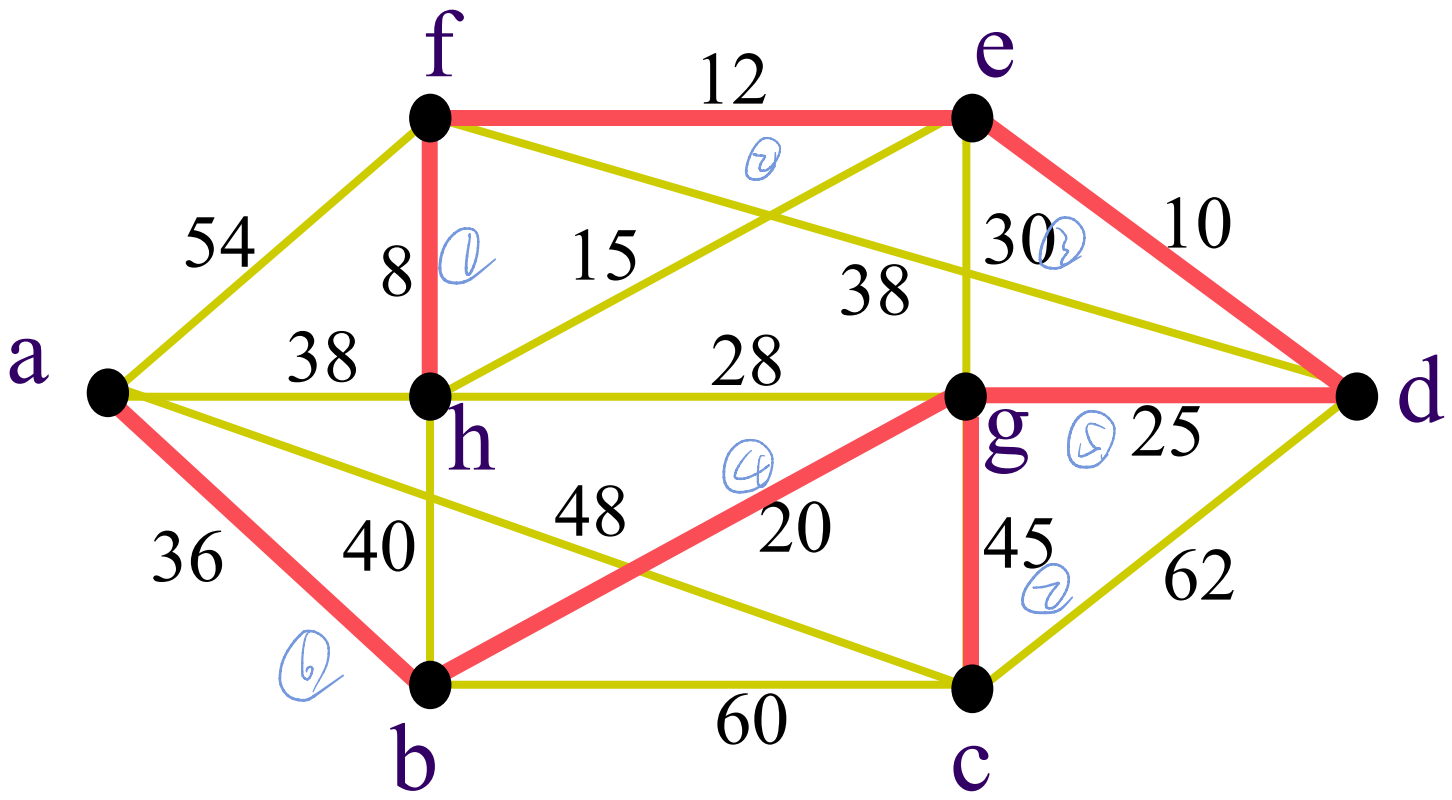
2: 从E以外选择不会与E中的边构成回路的权最小的边加入E

3: 重复第2步，直到E中包含 *n*-1条边

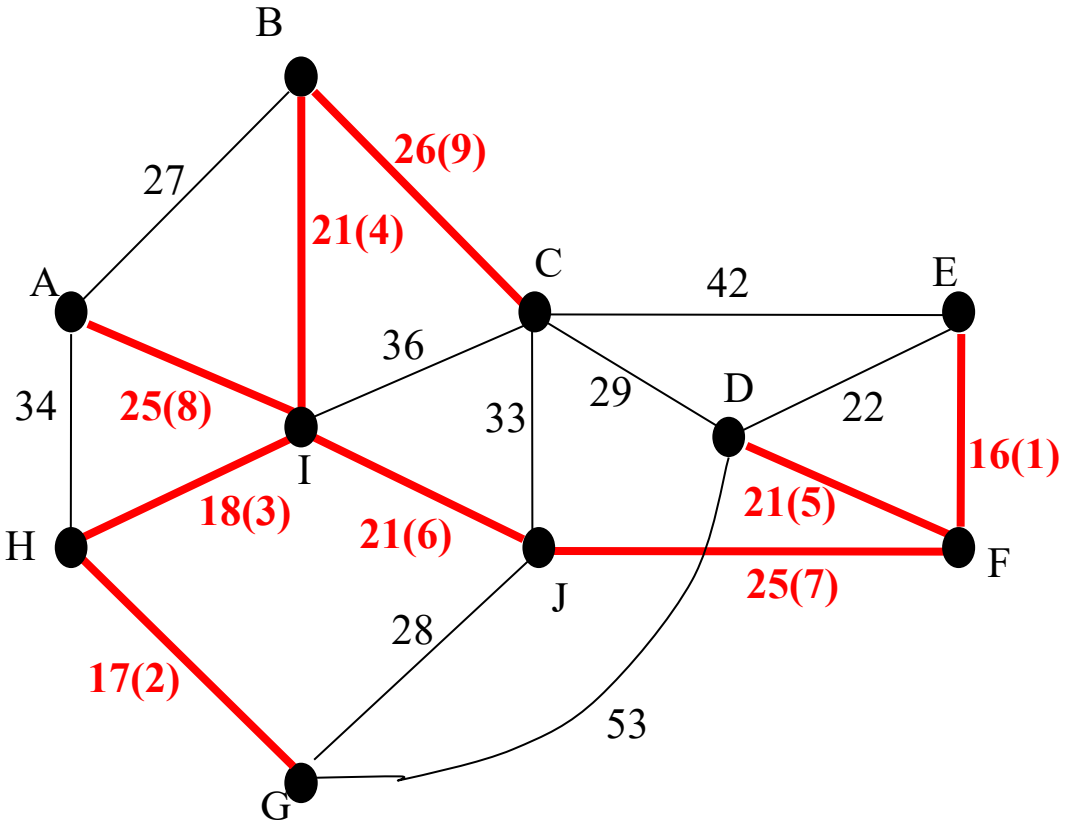
算法结束

Kruskal算法（举例）

- 铺设一个连接各个城市的光纤通信网络（单位：万元）。



Kruskal算法（举例）



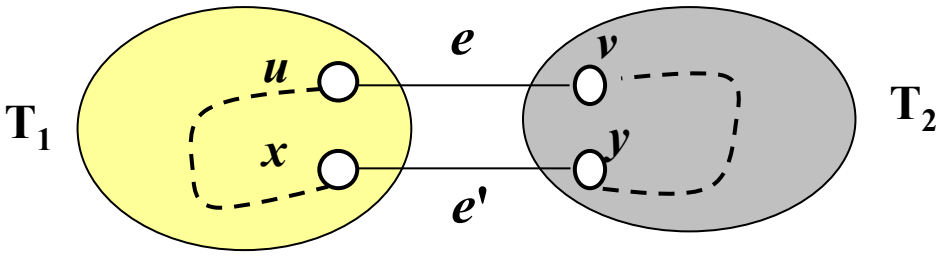
后面证明：Kruskal算法的正确性

引理（更换生成树的边）

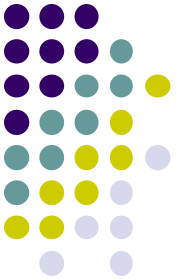
- T与T'均是图G的生成树，若$e \in E_T$且$e \notin E_{T'}$，则必有$e' \in E_{T'}$，$e' \notin E_T$，且$(T-\{e\}) \cup \{e'\}$和$(T'-\{e'\}) \cup \{e\}$均是G的生成树。

  - 设$e=uv$，T-{e}必含两个连通分支，设为T_1，T_2。因T'是连通图，T'中有uv-通路，其中必有一边满足其两个端点x,y分别在T_1, T_2中，设其为e'，显然$(T-\{e\}) \cup \{e'\}$是生成树。

    而T'-{e'}中x,y分属两个不同的连通分支，但在$T^*=(T'-\{e'\}) \cup \{e\}$中，$xu$-通路+$e$+$vy$通路是一条$xy$-通路，因此$T^*$连通，从而 T^*是生成树。

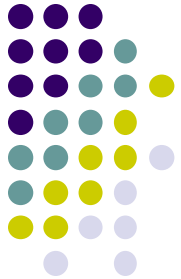


Kruskal算法的正确性



- 显然T是生成树。
- 按算法中加边顺序，T中边是$e_1,e_2,\cdots e_{k-1}, e_k,\cdots e_{n-1}$。
- 假设T不是最小生成树。对于任意给定的一棵最小生成树T', 存在唯一的k, 使得$e_k \notin E_{T'}$，且$e_i \in E_{T'}$, $(1 \le i < k)$. 设T'是这样的一棵最小生成树，使得上述的k达到最大。
- 根据前述引理，T'中存在边e'，e'不属于T, 使得$T^*=(T'-\{e'\})\cup\{e_k\}$也是生成树。 $e' \in T'$与$e_1,e_2,\cdots e_{k-1}$不会构成回路，因此$w(e') \ge w(e_k)$. 所以$w(T^*) \le w(T')$, 即T^*也是最小生成树。但T^*包含$e_1,e_2,\cdots e_{k-1}, e_k$，矛盾。

“避圈法”与“破圈法”



- 上述算法都是贪心地增加不构成回路的边，以求得最优树，通常称为“避圈法”；
- 从另一个角度来考虑最优树问题，在原连通带权图G中逐步删除构成回路中权最大的边，最后剩下的无回路的子图为最优树。我们把这种方法称为“破圈法”。

期末复习习题课

助教：刘翔宇，田晓滨

知识点回顾

- 命题逻辑与证明
- 集合论与函数
- 归纳与递归
- 抽象代数：代数系统、群论
- 图论：连通性、欧拉图、哈密顿图、带权图、有向图、匹配、树

命题逻辑 – 梳理

- 命题的概念
- 联结词
- 命题符号化
- 常用的逻辑等价
- 自然推理系统的推理规则
- 永真式的证明/逻辑等价的判定
- 析（合）取范式

命题逻辑

- 命题：可判断真假的陈述句
- 常用联结词：否定¬、合取∧、析取∨、蕴含→、等价↔
  - 注意联结词的运算优先级
- 命题符号化：自然语言和命题符号的相互转换
  - 例：令p、q和r为如下命题：p：你得流感了。q：你错过了期中考试。r：这门课你及格了。
  - “你错过了期中考试，所以你这门课没及格。” q ⟶ ¬r
  - p∧¬r “你得流感了，并且你这门课没有及格。”

命题逻辑

- 自然推理系统的推理规则

附加	1. $A \Rightarrow (A \vee B)$
化简	2. $(A \wedge B) \Rightarrow A$
假言推理	3. $A \to B, A \Rightarrow B$
取拒式	4. $A \to B, \neg B \Rightarrow \neg A$
析取三段论	5. $A \vee B, \neg B \Rightarrow A$
假言三段论	6. $A \to B, B \to C \Rightarrow A \to C$
消解	7. $A \vee B, \neg A \vee C \Rightarrow B \vee C$
合取引入	8. $A, B \Rightarrow A \wedge B$

前提⇒结论

前提

结论

$$\frac{p \quad p \to q}{\therefore q}$$ 假言推理

$$\frac{\neg q \quad p \to q}{\therefore \neg p}$$ 取拒式

$$\frac{p \to q \quad q \to r}{\therefore p \to r}$$ 假言三段论

$$\frac{p \vee q \quad \neg p}{\therefore q}$$ 析取三段论

$$\frac{p}{\therefore p \vee q}$$ 附加

$$\frac{p \wedge q}{\therefore p}$$ 化简

$$\frac{p \quad q}{\therefore p \wedge q}$$ 合取引入

$$\frac{p \vee q \quad \neg p \vee r}{\therefore q \vee r}$$ 消解

命题逻辑

- 永真式证明/逻辑等价的判定
  - 真值表
  - 命题的等价变换
- 析（合）取范式
  - 析取范式：由有限简单合取式组成的析取式;
  - 合取范式：由有限简单析取式组成的合取式;

谓词逻辑

- 谓词：$P(x_1, x_2, \cdots, x_n)$，给定个体时为一个确定的命题
- 量词：
  - 全称量词 。∀xP(x)，指命题“对所有论域中的 x，P(x)为真。”
  - 存在量词 。∃xP(x)，指命题“存在论域中的某个 x，P(x)为真。”
  - 量词公式的否定
- 自然语言与谓词逻辑表达式的互换
  - 定义谓词和论域
  - 根据语义加入量词、联结词
- 含量词的推理规则
  - 全称例示，全称引入，存在例示，存在引入
  - 命题逻辑的推理规则

证明方法

- 证明命题为真:
  - 直接证明法
  - 间接证明法
  - 归谬法（反证法）
  - 穷举法
  - 空证明法
  - 平凡证明法
- 证明结论为假:
  - 反例证明法

集合论 – 梳理

- 集合的概念与表示方法
- 集合的关系
- 集合的运算
- 集合代数
- 集合的基数
- 集合的等势关系、优势关系
- Cantor定理

集合论

- 集合的概念与表示方法
  - 列举法。{1,2,3,4,5,6}
  - 谓词描述法。{x|x是南京大学的学生}
- 集合的关系
  - 子集、真子集
  - 相交
  - 相等
  - 互补

集合论

- 集合的运算
  - 交、并、相对补、对称差
  - 幂集
  - 广义交、广义并
- 集合代数
  - 交换律、结合律、分配律
  - 幂等律、空集性质
  - 德摩根律、幂集性质

集合的基数

- 集合基数：集合A中所包含元素的个数称为集合A的基数或称A的势，记为|A| 或 card A
- 有限集：存在自然数n使得|A| =n，则称A为有限集
- 无穷集：如果A不是有限集，则称A为无穷集
  - 可数集：若A ≈ $\mathbb{N}$ ，则称A为可数集， |A|=$\aleph_0$
  - 若$A \approx \mathbb{R}$，则记 |A|=$\aleph_1$

集合的基数

- 等势：设A，B为集合，A和B等势当且仅当存在从A 到B 的双射，记作A ≈ B
- 等势的证明
  - 构造从A到B（或从B到A）的一一对应
  - 分别构造从A到B和从B到A的一对一函数
- 优势：A,B为集合，存在从A到B的单射函数，则称集合 B优势于集合A
- 真优势：若集合B优势于集合A且集合B与集合A不等势，则称集合B真优势于集合A

集合的基数

- Cantor对角线法
- Cantor 定理
  - $\mathbb{N} \not\approx \mathbb{R}$
  - 对于任意集合A，$A \not\approx \mathcal{P}(A)$

关系 - 梳理

- 有序对与笛卡尔积
- 关系及二元关系的定义
- 关系的运算
- 关系的性质
- 等价关系、等价类
- 关系的闭包

二元关系

- 有序对（序偶）：(a, b)
- 笛卡尔积：任给集合A与B，A与B的笛卡尔积定义为 {(a, b)|a ∈ A ∧ b ∈ B}，记为A × B
- 二元关系：设A, B为集合，若$R \subseteq A \times B$，称R为从A到B的二元关系，当$A = B$时，称R为A上的二元关系，在无歧义时一般可简称关系
- 与关系R有关的3个重要集合：
  - R的定义域
  - R的值域

二元关系

- 三种特别的二元关系：
  - 空关系（empty relation）$\emptyset$：$\emptyset \subseteq A \times A$
  - 全关系（entire relation）E_A：$E_A = \{(x, y) | x, y \in A\}$
  - 恒同关系（identical relation）I_A：$I_A = \{(x, x) | x \in A\}$
- 自然数集上常见的关系
  - 小于关系：$<$ $\stackrel{\text{def}}{=}$ $\{(n, m) | n < m \wedge n, m \in \mathbb{N}\}$
  - 整除关系：$|$ $\stackrel{\text{def}}{=}$ $\{(n, m) | n | m \ \wedge \ n, m \in \mathbb{N}\}$
  - 相等关系：$=$ $\stackrel{\text{def}}{=}$ $I_{\mathbb{N}}$

二元关系

- 二元关系的表示
  - 集合：集合{(a,b)|…}
  - 当R为有穷集时
    - $m \times n$ 的矩阵
    - 有向图（关系图）
- 关系的运算：
  - 逆　$R^{-1} = \{(x,y)|(y,x) \in R\}$
  - 复合　$R \circ S = \{(x,y)|(\exists t \in B)((x,t) \in S \wedge (t,y) \in R)\}$
  - 幂　$R^0 = \boldsymbol{I_A}$，$R^{n+1} = R \circ R^n$

关系的性质

- 自反性、反自反性
  - R在A上自反（reflexive）指：$(\forall x \in A)(xRx)$
  - R在A上反自反（irreflexive）指：$(\forall x \in A)(\neg xRx)$
- 对称性、反对称性
  - R在A上对称（symmetric）指：

    $$(\forall x, y \in A)(xRy \rightarrow yRx)$$

  - R在A上反对称（anti-symmetric）指：

    $$(\forall x, y \in A)(xRyRx \rightarrow x = y)$$

关系的性质

- 传递性
  - R在A上传递（transitive）指：

$$(\forall x, y, z \in A)(xRyRz \rightarrow xRz)$$

	自反性	反自反性	对称性	反对称性	传递性
集合表达式	$I_A \subseteq R$	$R \cap I_A = \varnothing$	$R = R^{-1}$	$R \cap R^{-1} \subseteq I_A$	$R \circ R \subseteq R$
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 也有边

关系的性质

- 等价关系：满足自反性、对称性、传递性
- 等价类、代表元素、商集
- 闭包：设R为集合A上的关系，P为某个性质（即自反性，对称性，传递性之一），若存在$S \subseteq A \times A$，使得：

  (1) $R \subseteq S$
  (2) S具有性质P
  (3) $\forall T(R \subseteq T \wedge T$ 具有性质$P \rightarrow S \subseteq T)$

  则称S为“相对于P的R的闭包（简称R的P闭包）”

关系的性质

- 闭包的实用构造

  设$R \subseteq A \times A$,

  - (1) R的自反闭包 $r(R) = R \cup R^0 = R \cup I_A$
  - (2) R的对称闭包 $s(R) = R \cup R^{-1}$
  - (3) R的传递闭包 $t(R) = R \cup R^2 \cup R^3 \cup \cdots = \cup\{R^n | n \in \mathbb{N}^+\}$

- 求传递闭包的Warshall算法

函数 - 梳理

- 函数的定义
- 函数的性质
- 函数的复合
- 反函数

函数

- 函数的定义： $(\forall x,y,z)(xFy \wedge xFz \rightarrow y = z)$
- 函数的定义域、值域、陪域
  - F:A→B，定义域Dom(F)=A，值域Ran(F)，陪域B
- 函数的性质
  - 满射（surjection / onto）Ran(f)=B
  - 单射（injection / 1-1）(∀x,y∈A)(f(x)=f(y)→x=y)
  - 双射（bijection /1-1 correspondence）f既是单射又是满射

函数

- 函数的运算
  - 复合
    - 函数的复合(f ∘ g) (x) = f(g(x)) (g(f(x)亦可)
    - 函数的复合具有结合性： (f ∘ g) ∘ h = f ∘ (g ∘ h)
    - 若f, g为单射/满射/双射， 则f ∘ g亦然
  - 反函数
    - 函数的逆不一定是函数，可能只是一个二元关系。
    - 若f是双射函数，则f的逆关系称为f的反函数。

归纳与递归

- 数学归纳法
  - 奠基： P(1)为真
  - 归纳假设：对于k, P(k)为真，(k的范围)
  - 归纳步骤 $\forall k\,(P(k) \rightarrow P(k+1))$
- 递归结构法（证递归构造的集合中元素具有特定性质）
  - 奠基：集合初始元素具有性质
  - 归纳假设：根据证明目标而定
  - 归纳步骤：根据规则产生新元素其中含有归纳假设中的元素

计数原理

- 容斥原理:

容斥原理（Principle of Inclusion and Exclusion, PIE）的一般表述为：假设有穷全集含N个元素，$A_1, A_2, \cdots, A_n$是分别满足相应性质的元素构成的子集。则不满足任何性质的集合的元素个数是：

$$|\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}|$$
$$= N - S_1 + S_2 - S_3 + \cdots + (-1)^k S_k + \cdots + (-1)^n S_n$$

其中，$S_k = \sum_{1 \le i_1 \le i_2 \le \cdots \le i_k \le n} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}|, k = 1,2,\cdots,n$

计数原理

- 乘法原则、加法原则
- r −排列：对n元集合中r个元素的有序安排（次序不同认为是不同的安排）称为r −排列

$$P(n,r) = n(n-1)(n-2)\cdots(n-r+1) = \frac{n!}{(n-r)!}$$

- r −组合：对n元集合中r个元素的无序组合（相同元素不同次序的出现认为是相同的组合）称为r −组合

$$C(n,r) = \binom{n}{r} = \frac{P(n,r)}{P(r,r)} = \frac{n!}{r!\,(n-r)!}$$

- 求方程根

抽象代数 – 梳理

- 运算
- 代数系统及其性质
- 半群、Monoid、群、子群、陪集
- 布尔代数

代数系统

- 运算：函数$f: A^n \to B$称为(从A^n到B的) n元运算
- 运算表
- 运算的封闭性：对于运算$f: A^n \to B$，若$B \subseteq A$，则称该运算在集合A上封闭
- 代数系统：
  - 给定1个非空集合（其元素可以是任何对象）
  - 给定1个或者若干个运算
  - 给定的所有运算对上述集合封闭

代数系统

- 代数系统的性质
  - 结合性：$\forall x,y,z \in A, (x \circ y) \circ z = x \circ (y \circ z)$
  - 交换性：$\forall x,y \in A, x \circ y = y \circ x$
  - 分配性：$\forall x,y,z \in A, x \circ y * z = x \circ y * (x \circ z)$
  - 单位元：$\forall x \in S, e \circ x = x \circ e = x$
  - 零元：$\forall x \in S, e \circ x = x \circ e = x$
  - 逆元：$x \circ x^* = x^* \circ x = 1_S$
- 同构：代数系统$\langle S_1,\circ \rangle$ 与 $\langle S_2,* \rangle$同构 (记作$S_1 \cong S_2$) 当且仅当存在双射函数$f: S_1 \to S_2$，满足：$\forall x,y \in S_1, f(x \circ y) = f(x) * f(y)$
- 同态：代数系统 $\langle S_1,\circ \rangle$ 与 $\langle S_2,* \rangle$同态 (记作$S_1 \sim S_2$)当且仅当存在函数$f: S_1 \to S_2$，满足：$\forall x,y \in S_1, f(x \circ y) = f(x) * f(y)$

群论

- 半群:

定义 设$(S, *)$为代数系统，$(S, *)$为半群（Semigroup）指

(1) $(\forall x, y \in S)(x * y \in S)$

(2) $(\forall x, y, z \in S)((x * y) * z = x * (y * z))$

若$(\forall x, y \in S)(x * y = y * x)$则称$(S, x)$为交换半群（abelian半群）

- Monoid（幺半群）

定义 设$(S, *)$为代数系统，$(S, *)$为Monoid（Semigroup with unit）指

(1) $(\forall x, y \in S)(x * y \in S)$

(2) $(\forall x, y, z \in S)((x * y) * z = x * (y * z))$

(3) $(\exists e \in S)(\forall x \in S)(e * x = x * e = x)$

群论

- 群：设G为非空集合，$*$为G上的二元运算，<G,$*$>为群指 <G,$*$> 为Monoid，其单位元为e，且满足：$(\forall x \in G)\ (\exists y \in G)\ (x*y = y*x = e)$
- 有限群、n阶群、无限群
- 交换群：$(\forall x,y \in G)\ (xy = yx)$

群论

- 群的性质

定理：设$\langle G,*\rangle$为群，对任意$a,b,c \in G$，有：

(1) $(a^{-1})^{-1} = a$

(2) $(ab)^{-1} = b^{-1}a^{-1}$

(3) $ab = ac \rightarrow b = c$（左消去律）

(4) $ba = ca \rightarrow b = c$（右消去律）

(5) 方程$ax = b$和$ya = b$在G中对x，y有唯一解

群论

- 子群：设$\langle G,*,e,^{-1}\rangle$为群，$H \subseteq G$，若：
  - (1) $(\forall x,y\in H)(x*y\in H)$（运算封闭性）
  - (2) $e\in H$（单位元封闭性）
  - (3) $(\forall x \in H)(x^{-1}\in H)$（逆元封闭性）

  则称 $<H,*>$ 为 $<G,*>$ 的子群，记为 $<H,*> \leq <G,*>$，若$H \subset G$，称 $<H,*>$ 为 $<G,*>$ 的真子群，记为 $<H,*> < <G,*>$
- 平凡子群：设$\langle G,*,e,^{-1}\rangle$为群，则 $<\{e\},*> \leq <G,*>$ 和 $<G,*> \leq <G,*>$ 称为G 的平凡子群
- 子群判定定理
- 有限子群判定定理

群论

- 群中元素的阶及其性质
- 陪集：设 $<H,*> \leq <G,*>$，$a \in G$，令：$Ha = \{ha \mid h \in H\}$，$aH = \{ah \mid h \in H\}$ 称Ha(或aH)为子群H在G中的右(或左)陪集，H在G中右(或左)陪集的个数称为H在G中的指数，记为$[G: H]$
- 陪集与划分
- 陪集等价关系
- 陪集与群的分解
- Lagrange定理：设 $<G,*>$ 为有限群，$<H,*> \leq <G,*>$，则 $|G| = |H| \cdot [G: H]$

群论

- 循环群：设 $<G,*>$ 为循环群指：$(\exists a \in G)\,(G = <a>)$。这里，$<a> = \{a^n \mid n \in \mathbb{Z}\}$，$a$称为$G$之生成元
- 有限循环群、无限循环群
- 循环群的生成元
- 循环群的子群
- 群同构、群同态

图论 – 梳理

- 图的定义与表示
- 图的连通性
- 欧拉图、哈密顿图
- 带权图与最短路
- 二部图与匹配
- 树、生成树、二叉树
- 有向图

图的定义与表示

- 图：

定义： 无向图$G=\langle V,E,\gamma\rangle$ 由集合 V,E 和函数 γ 组成，其中

(1) $V\neq\emptyset$ 为点集，V 之元素称为点(vertex, vertices[复])。

(2) E 为边集，E 之元素称边(edge)。

(3) $\gamma: E\to\{\{u,v\}\mid u,v\in V\}$

- 若对于 $e\in E$ 有$\gamma(e)=\{u,v\}$，则称u和v为e的端点。
- 若对于 $e_1,e_2\in E$ 有$\gamma(e_1)=\gamma(e_2)$，则称e_1和e_2为重边(multiedge)。
- 对于 $e\in E$，e 的重数 $=|\{e'\in E\mid\gamma(e')=\gamma(e)\}|$。
- 若对 $e\in E$ 有 $\gamma(e)$ 呈形 $\{u,u\}$ 则称 e 为环(loop)。
- 若 G 有重边但无环则称 G 为多重图。
- 若 G 既无环又无重边，则称 G 为简单图(simple graph)。

约定：通常 $G=\langle V,E,\gamma\rangle$ 中的 γ 被省略，直接写 $\langle V,E\rangle$ 且 $V\cap E=\emptyset$。

图的定义与表示

- 关联关系、相邻关系

定义： 设 $G=\langle V,E\rangle$ 为有穷无向图

1. G 的点集记为 V_G，边集记为 E_G；G 的点数为 $|V_G|$，记为 v_G；G 的边数为 $|E_G|$，记为 e_G。
2. 若 $v_G=n$，称 G 为 n 阶图。
3. 若G为简单图，$v_G=n, e_G=m$，称G为(n,m)图。若G的点和边用字母标定，是称G为标定图。
4. 设 $u,v\in V$，若边 e 的两个端点为 u,v，则称 u 与 v 邻，记为 $u-v$，并称 e 与 u,v 关联。
5. 设 $e\in E, G-e=$ 在 G 中去边 e。
6. 设 $v\in V, G-v=$ 在 G 中去点 v 及其关联的边。
7. 设 $u,v\in V, G+(u,v)=$ 在 G 中加端点的 u,v 的新边。

图的定义与表示

- 度、出度、入度
- 最大度$\Delta(G)$、最小度$\delta(G)$
- 握手定理：$\sum_{i=1}^{|V_G|} d(v_i) = 2|E_G|$
- 子图、母图、生成子图
- 图的同构
- 特殊的简单图：n阶零图($\mathrm{N_n}$)，线图($\mathrm{L_n}$)，圈图(C_n)，轮图($\mathrm{W_n}$)，超立方体图($\mathrm{Q_n}$)

图的定义与表示

- 完全图：若n阶无向简单图G中每个顶点均与其余$n-1$个顶点相邻：$(\forall u,v \in V)(u \neq v \rightarrow u-v)$，称$G$为$n$阶无向完全图，记作$K_n$
- 正则图：若 $\forall v \in V, d(v) = k$，则称$G$为$k$ -正则图
- 二部图：无向图$G=<V,E>$，若能将V分为不交的两部分 V_1 和 V_2 ，使得G中每条边的两个端点均分属V_1和V_2，则称G为二部图（或偶图），记为$\langle V_1, V_2, E\rangle$
- 完全二部图：G为简单二部图，V_1中每个顶点均与V_2中所有顶点相邻，记为$K_{|v_1|,|v_2|}$
- 补图：单图G的补图$\bar{G}$以V为点集但两个顶点在 $\bar{G}$中相邻当且仅当它们在G中不相邻

图的定义与表示

- 图的基本运算：减边或边集、减点或点集、边收缩、加新边
- 图的通路、回路
- 通路存在性定理：n阶图G中，若从顶点v_i到v_j存在通路，则从v_i到v_j存在长度小于或等于$n-1$的通路。

图的连通性

- 无向图顶点间的连通关系： $v_i \sim v_j$若v_i与v_j之间存在通路
- 无向图的连通性： $\forall u,v \in V(G),\ u \sim v$
- 连通分支：计数为$p(G) = k$
- 连通图：平凡图或任何两顶点均连通
- 点连通度、点割集、$\boldsymbol{k}$ −连通图
- 边连通度、边割集、$\boldsymbol{k}$ −边连通图
- $\boldsymbol{\kappa(G) \leq \lambda(G) \leq \delta(G) \leq \left\lfloor \frac{2|E_G|}{|v_G|} \right\rfloor}$

欧拉回路与欧拉图

- 欧拉回路、欧拉图
- 欧拉通路、半欧拉图
- 欧拉图判定定理：G是欧拉图当且仅当G是连通图且G中每个顶点的度数均为偶数
- 半欧拉图判定定理：设G是连通图，G是半欧拉图当且仅当G恰有两个奇度顶点
- 关于欧拉图的等价命题
- 构造欧拉回路的Fleury算法

哈密顿回路与哈密顿图

- 哈密顿回路、哈密顿图
- 哈密顿通路、半哈密顿图
- 哈密顿图的必要条件：对任意非空真子集V_1，$p(G-V_1) \leq |V_1|$
- 半哈密顿图的充分条件：设G是n阶无向简单图（$n \geq 2$），G中任意不相邻的顶点对u,v均满足：$\boldsymbol{d(u)+d(v) \geq n-1}$
- 哈密顿图的充分条件：设n（$n \geq 3$）阶图G为无向简单图，G中任意不相邻的顶点对u,v满足：$\boldsymbol{d(u)+d(v) \geq n}$

哈密顿回路与哈密顿图

- 闭图：设G是n阶简单图，若两个不相邻的顶点u,v满足$\boldsymbol{d(u)+d(v)\geq n}$，则将新边$(u,v)$加入$G$中，得到$G+(u,v)$，如此加边直到无边可加。这样得到的图称为图$G$的闭图。
- 哈密顿图的一个充分必要条件：G为$H-$图当且仅当G的闭图为$H-$图

带权图与最短路

- 带权图、通路的权
- 求单源最短路的Dijkstra算法

二部图与匹配

- 二部图、完全二部图
- 二部图的判定定理：G为简单二部图当且仅当$G(|G|\geq 2)$中不包含奇圈
- 匹配、极大匹配、匹配数、最大匹配
- 设M为G中的一个匹配：M-饱和点、M-非饱和点、完美匹配
- 交错路径、可增广交错路径（可增广路）、增广路、交错圈
- 最大匹配的判定
- 二部图完备匹配的充分必要条件（Hall定理）

树

- 树：不含回路的连通简单图称为树
- 树中路径的唯一性
- 树的边数的极限：
  - 树是边最少的连通图（割边）
  - 树是边最多的无回路图
- 树中边和点的数量关系：$\boldsymbol{m=n-1}$
- 连通图的必要条件：$\boldsymbol{m\geq n-1}$

生成树

- 生成树：若图G的生成子图是树，则该子图称为G的生成树
- 生成树存在定理：无向图G有生成树当且仅当G连通
- 子图的权、最小生成树
- 求最小生成树的Kruskal算法

根树与二叉树

- 有向树：底图为树的有向图称为有向树
- 根树：若$n(n\geq 2)$阶有向树恰含一个入度为0的顶点，其它顶点入度均为1，则该有向树称为根树，其入度为0的顶点称为根
- 根数相关术语：有序、r叉、r叉正则、完全
- 子树、左子树、右子树
- 特殊的二叉树：二叉搜索树、二叉平衡树、有序二叉树
- 求最优二叉树的Huffman算法

有向图

- 有向图、始点、终点
- 出度、入度
  - 有向图D中所有顶点的出度之和与入度之和相等
- 有向通路与回路
- 弱连通、单向连通、强连通
  - 强连通的充分必要条件
  - 单向连通的充分必要条件
- 有向欧拉回路、有向欧拉回图
- 竞赛图、有向哈密顿通路