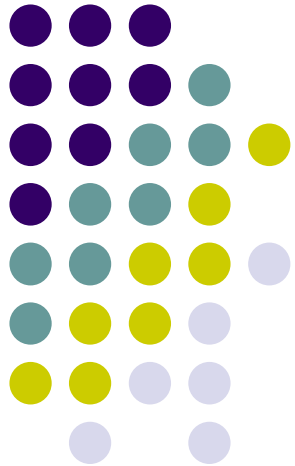
证明方法

离散数学—逻辑和证明

南京大学计算机科学与技术系



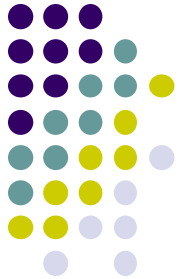
回顾

- 谓词逻辑
  - 谓词，量词，论域
  - 谓词的否定与嵌套
  - 逻辑等价
- 逻辑推理
  - 有效论证形式
  - 推理规则与及用推理规则来论证
  - 有关谓词逻辑的论证

内容提要

- 引言
- 直接证明
- 反证法
- 分情形证明
- 等价性证明
- 存在性证明
- 唯一性证明
- 寻找反例
- 数学与猜想

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
  - 已经证明的定理（推论、命题、引理）
  - 公理
  - 术语的定义

猜想（**conjecture**）

引言

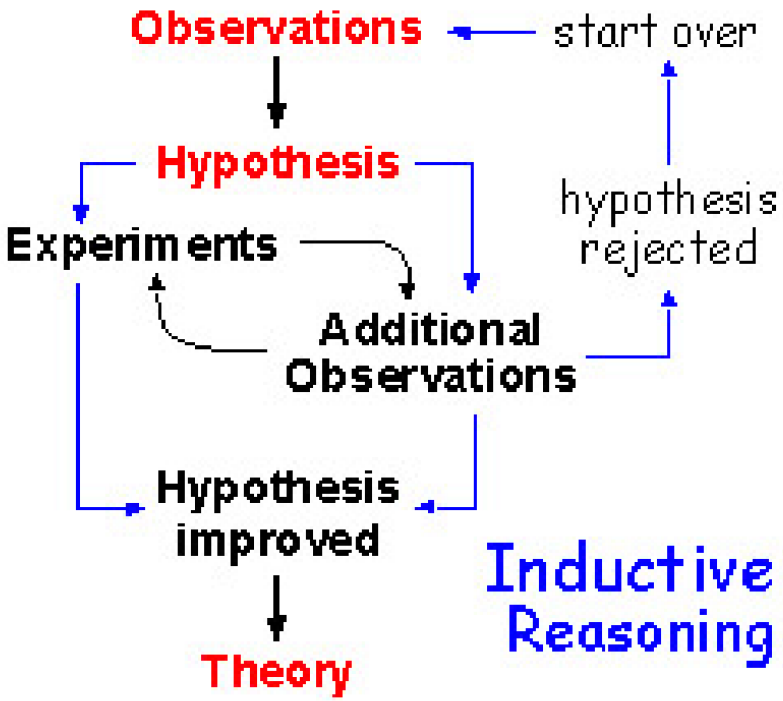
- 定理的陈述（举例）
  - 如果$x>y$，其中x和y是正实数，那么 $x^2>y^2$。
- 如何理解
  - 对所有正实数x和y，如果$x>y$，那么 $x^2>y^2$。
  - $\forall x \forall y((x>y) \rightarrow (x^2>y^2))$ //论域为正实数
- 如何证明
  - 定理的陈述为：$\forall x\,(P(x) \rightarrow Q(x))$
  - 先证明，对论域中的任一元素c， $P(c) \rightarrow Q(c)$
  - 再使用全称生成，得到$\forall x\,(P(x) \rightarrow Q(x))$

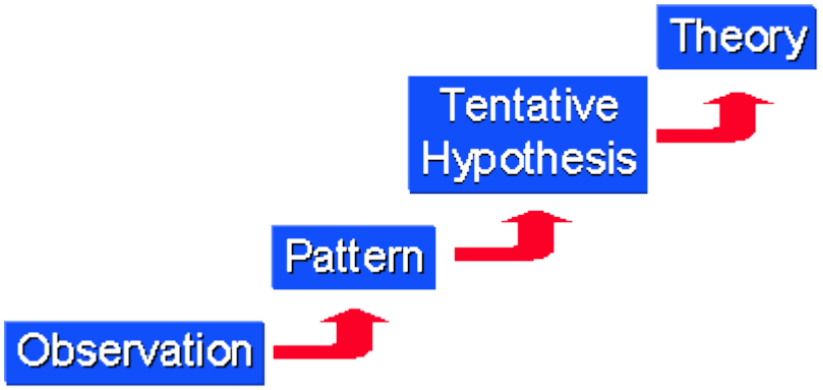
证明的本质？

- 证明的本质是“保证真实性”，其涵义根据领域的不同有所差异：
  - 科学中的“证明”指利用归纳推理（inductive reasoning）去证实（prove）某个假设（hypothesis）
  - 人们将大量特殊的信息收集（归纳）起来并根据自身的知识和经验去观察，并推断（推理）哪些是真实的
  - 此类“证明”不产生定论（mathematical certainty)

归纳推理的证明方式

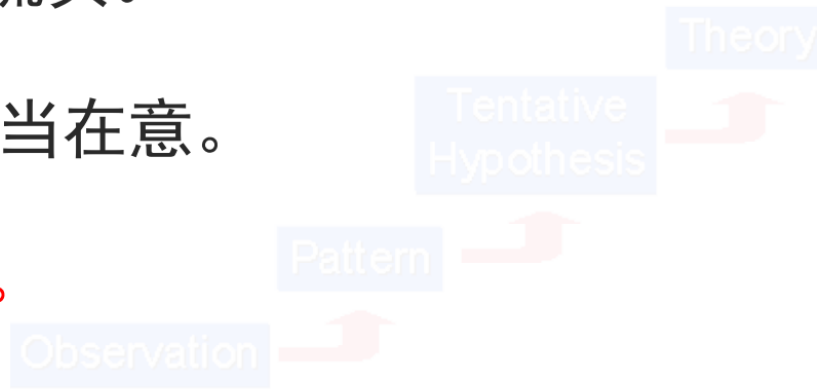
- 归纳推理的逻辑过程





归纳推理的证明方式

- 日常生活中“证明”的例子：
  - 我们观察到：小王今早上课迟到了。
  - 我们观察到：小王今天没梳头。
  - 经验： 小王平时对发型相当在意。
  - **结论：**小王今天睡过头了。
- 这类“证明”方式一般在数学中用于提出假设

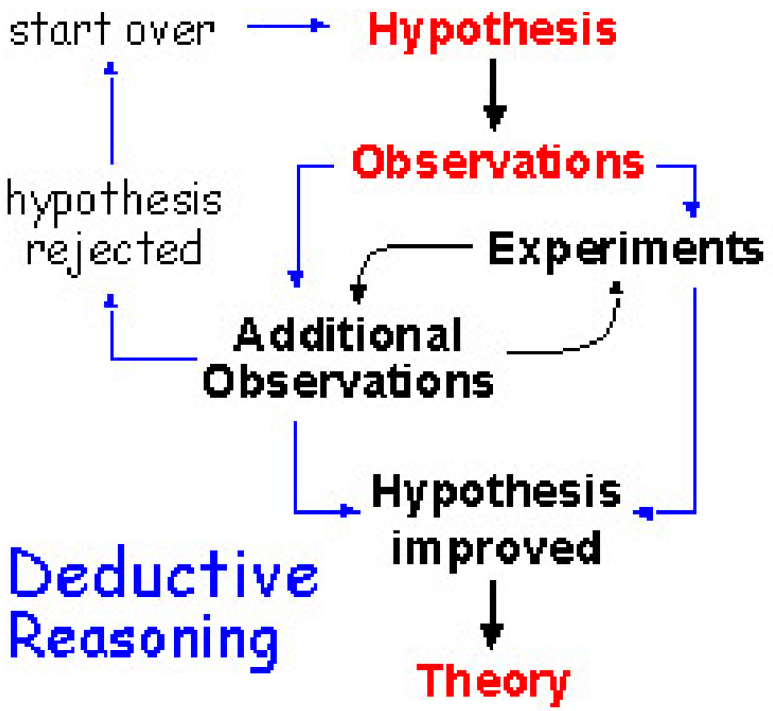


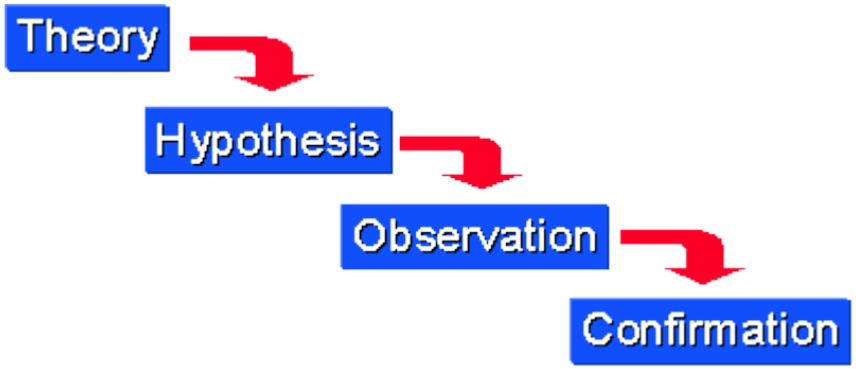
演绎推理的证明方式

- 证明的本质是“保证真实性”，其涵义根据领域的不同有所差异：
  - 数学中的“证明”指利用演绎推理（deductive reasoning）和逻辑规则去推证某个命题
  - 数学证明中每一步推理过程都根据某些前提条件（premise）展示出一个结论——称为逻辑推论
  - 所有的证明过程必须是严密的（rigorous），每一步都必须提供确信的证据来支持中间结论，最终结论称为系统中的定理（theorem）

演绎推理的证明方式

- 演绎推理的逻辑过程





形式化证明

- 用于数学的证明方式称为形式化证明或推导（derivation）
- 定义（形式化证明）：对一个命题的基于公理化系统的一系列逻辑演绎的有限过程
- 例：欧几里德平面几何的公理集合
  - 公理1. 任意两点可以通过一条直线连接。
  - 公理2. 任意线段可无限延伸为一条直线。
  - 公理3. 给定任意线段，可以以其一个端点作为圆心，该线段作为半径作一个圆。
  - 公理4. 所有直角都全等。
  - 公理5. 若两条直线都与第三条直线相交，并且在同一边的内角之和小于两个直角，则这两条直线在这一边必定相交。

逻辑推理的形式结构

- 逻辑推理的形式化结构为：

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

当上式为永真式时，可写为：

$$A_1 \wedge A_2 \wedge \cdots \wedge A_k \Rightarrow B$$

此时称为“推理有效”或者“推理正确”，亦称B为前提$A_1, A_2, \cdots, A_k$的有效（逻辑）结论；否则称推理不正确

	A	B	$A \rightarrow B$
(1)	0	0	1
(2)	0	1	1
(3)	1	0	0
(4)	1	1	1

(1), (2), (4)推理正确
(3) 推理不正确
(1) 中B是A的逻辑结论,但不是正确结论; (2)和(4)中B既是逻辑结论, 又是正确结论.

逻辑推理的形式结构

- (1)“若A，则B”：

$$A \rightarrow B$$

- (2)“A当且仅当B”：

$$A \leftrightarrow B$$

- (3)“证明B”：

$$B$$

- 以上三种形式皆可归结为形式(1)

直接证明法

- 证明方法：证明“若A为真，则B为真”
- 理论依据：“若A为真，则B为真”$\Longrightarrow$“$A \to B$为真”
- 例：

证明：若n是奇数，则n^2也是奇数.

证：因为n是奇数，故$\exists k \in \mathbb{N}$使$n = 2k + 1$，于是有：

$$n^2 = (2k+1)^2 = 2(2k^2 + 2k) + 1,$$

故n^2是奇数. □

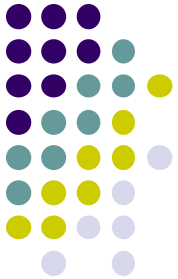
间接证明法

- 证明方法：证明逆否命题“$\neg B \rightarrow \neg A$”为真
- 理论依据：“$A \rightarrow B$为真”$\Leftrightarrow$“$\neg B \rightarrow \neg A$”为真
- 例：

证明：若n^2是奇数，则n也是奇数.

证：只需证**若n是偶数，则n^2也是偶数.** 假设$\exists k \in \mathbb{N}$, $n = 2k$，于是有：$n^2 = (2k)^2 = 2(2k^2)$，故n^2为偶数，从而原命题得证. □

归谬法（反证法）



- 证明方法：假设A真且$\neg B$真，推出矛盾，即$A \wedge \neg B \Longrightarrow \perp$
- 理论依据：“$A \wedge \neg B \Longrightarrow \perp$”为真$\Leftrightarrow$“$A \wedge \neg B$”为假$\Leftrightarrow$“$\neg(A \wedge \neg B)$”为真$\Leftrightarrow$“$\neg A \vee B$”为真$\Leftrightarrow$“$A \rightarrow B$”为真
- 例1：

证明：若$3n+2$是奇数，则n也是奇数.

证：反设在题设条件下n为偶数，即$\exists k \in \mathbb{N}, n = 2k$，于是有：$3n+2 = 6k+2 = 2(3k+1)$，故$3n+2$为偶数，与题设矛盾！原命题得证. □

归谬法

- 例2：

证明：$\sqrt{2}$是无理数.

证：反设$\sqrt{2}$为有理数，则其可写为$\frac{p}{q}$ $(p,q \in \mathbb{N} \wedge (p,q)=1)$

之形式，且$\left(\frac{p}{q}\right)^2 = 2$；那么有：$p^2 = 2q^2 \rightarrow p^2$为偶$\rightarrow p$亦

为偶$\rightarrow p^2$为4的倍数$\rightarrow q^2$为偶$\rightarrow q$为偶$\rightarrow p$与q有公因子2.

这与$(p,q)=1$矛盾，故假设错误，原命题得证. □

广义归谬法

- 证明方法：假设$A_1, A_2, \cdots, A_k$真且$\neg B$真，推出矛盾，即

  $A_1 \wedge A_2 \wedge \cdots \wedge A_k \wedge \neg B \Longrightarrow \perp$

- 理论依据：$A_1 \wedge A_2 \wedge \cdots \wedge A_k \wedge \neg B \Rightarrow \perp \Leftrightarrow A_1 \wedge A_2 \wedge \cdots \wedge$

  $A_k \Longrightarrow B$

- 广义归谬法为人工智能中“归结反演”技术的理论依据

穷举法（分情形证明）

- 证明目标：$A_1 \vee A_2 \vee \cdots \vee A_k \rightarrow B$
- 证明方法：证明$A_1 \rightarrow B$，$A_2 \rightarrow B$，…，$A_k \rightarrow B$皆为真
- 理论依据：$A_1 \vee A_2 \vee \cdots \vee A_k \rightarrow B \Leftrightarrow \neg(A_1 \vee A_2 \vee \cdots \vee A_k) \vee B \Leftrightarrow (\neg A_1 \wedge \neg A_2 \wedge \cdots \wedge \neg A_k) \vee B \Leftrightarrow (\neg A_1 \vee B) \wedge (\neg A_2 \vee B) \wedge \cdots \wedge (\neg A_k \vee B) \Leftrightarrow (A_1 \rightarrow B) \wedge (A_2 \rightarrow B) \wedge \cdots \wedge (A_k \rightarrow B)$
- 例：

证明：$\max(a, \max(b, c)) = \max(\max(a, b), c)$.

证：见下表.

穷举法

- 证明：$\max(a, \max(b, c)) = \max(\max(a, b), c)$.

  证： 见下表.

情 况	u=max(b,c)	max(a,u)	v=max(a,b)	max(v,c)
$a \le b \le c$	c	c	b	c
$a \le c \le b$	b	b	b	b
$b \le a \le c$	c	c	a	c
$b \le c \le a$	c	a	a	a
$c \le a \le b$	b	b	b	b
$c \le b \le a$	b	a	a	a

分情形证明（举例）

- 当n是一个正整数，且$n \leq 4$时，$(n+1)^3 \geq 3^n$。
  - n=1, 2, 3, 4.（穷举）
- 当n是一个整数时，有$n^2 \geq n$。
  - $n \leq 0$
  - $n \geq 1$

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
  - $p_1 \Rightarrow p_2$
  - $p_2 \Rightarrow p_3$
  - …
  - $p_n \Rightarrow p_1$
  - 因此， $p_1 \leftrightarrow p_2 \leftrightarrow \ldots \leftrightarrow p_n$。

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。

构造性证明法

- 证明目标：证明$A \to B$，其中B具有某种性质的对象
- 证明方法：在保证A为真的条件下构造出具有这种性质的对象
- 例：

证明：对于每个正整数n，存在n个连续的正合数.

证：令$\boldsymbol{x = (n+1)!}$，则$2|(x+2)$，$3|(x+3)$，$\cdots$，$n|(x+n)$，$\cdots$，$(n+1)|(x+n+1)$这n个连续的正整数为合数，命题得证. □

空证明法（前件假证明法）

- **证明方法：**要证“$A \to B$为真”，可证“A为矛盾式”
- **理论依据：**“A为矛盾式”$\Longrightarrow$“$A \to B$为真”
- **例：**

证明：空集$\varnothing$是任何集合的子集.

证：根据子集的定义$A \subseteq B \Leftrightarrow \forall x(x \in A \to x \in B)$，令$A = \varnothing$，则$\varnothing \subseteq B \Leftrightarrow \forall x(x \in \varnothing \to x \in B) \Leftrightarrow \forall x(\bot \to x \in B) \Leftrightarrow \boldsymbol{T}$，命题得证. □

	A	B	$A \to B$
(1)	0	0	1
(2)	0	1	1
(3)	1	0	0
(4)	1	1	1

平凡证明法（后件真证明法）

- 证明方法：要证“$A \to B$为真”，可证“B为永真式”
- 理论依据：“B为永真式”$\Longrightarrow$“$A \to B$为真”
- 例：

  证明：若$a \le b$，则$a^0 \le b^0$.

  证：因为$a^0 \le b^0$恒为真，故命题得证. □

- 这种证明方式常在数学归纳法的“奠基”中出现

	A	B	$A \to B$
(1)	0	0	1
(2)	0	1	1
(3)	1	0	0
(4)	1	1	1

命题为假的证明-举反例

- 证明方法：要证“$\forall x P(x)$为假”，可找一个使“$\neg P(x)$为真”的特例
- 理论依据：“$\neg \forall x P(x)$” $\Leftrightarrow$ “$\exists x \neg P(x)$”
- 例：

证明：命题“每个正整数都是三个整数的平方和”为假命题.

证：根据题设，正整数7无法表为三个整数的平方和形式，故原命题为假命题. □

命题为假的证明-举反例

- 数学证明要求每一步均严格按照规则去推理，不要忽略隐式的规则
- 例：

$a = b$ 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

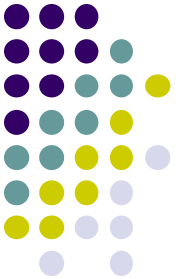
$(a-b)(a+b) = b(a-b)$ 分解

$a + b = b$ 两边同除以$a-b$

$2b = b$

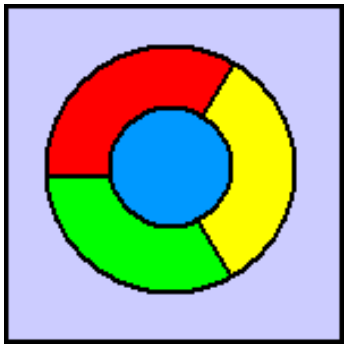
$\therefore 2 = 1$ 两边同除以b

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5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。
- **“*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 in Francis Guthrie 1852**
  - **Proven in 1976 by Kenneth Ira Appel (1932-, New York) and Wolfgang Haken (1928-, Berlin)**
    - **Percy John Heawood (1861-1955, Britain) proved the five color theorem in 1890**

作业

- 教材内容：[Rosen] 1.6—1.7节
- 课后习题：
  - pp.64-65（对应英文教材 pp.85-86，第七版 pp.77-78）：

    25, 35, 39, 41
  - pp.75-76（对应英文教材 p.103）：11, 23, 29（将中文版“整数”改为“正整数”）, 30
    - 第七版pp.90-91, *13,24,31,32*