



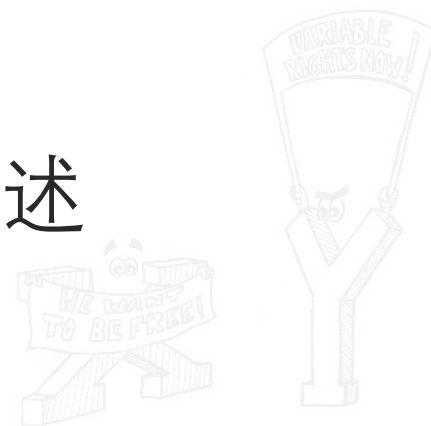
离散数学

Discrete Mathematics

第四讲：证明方法概述

吴 楠

南京大学计算机科学与技术系



2020 年 10 月 15 日



前情提要



- 谓词与量词
- 谓词逻辑
- 谓词逻辑的推理系统
- 谓词逻辑的推理实例
- 谓词逻辑的应用举例*





本讲主要内容



- 证明的本质
- 逻辑推理的形式结构
- 常用的证明方法与证明策略
 - 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
 - 构造性证明法，反例证明法



什么是证明 (proof) ?



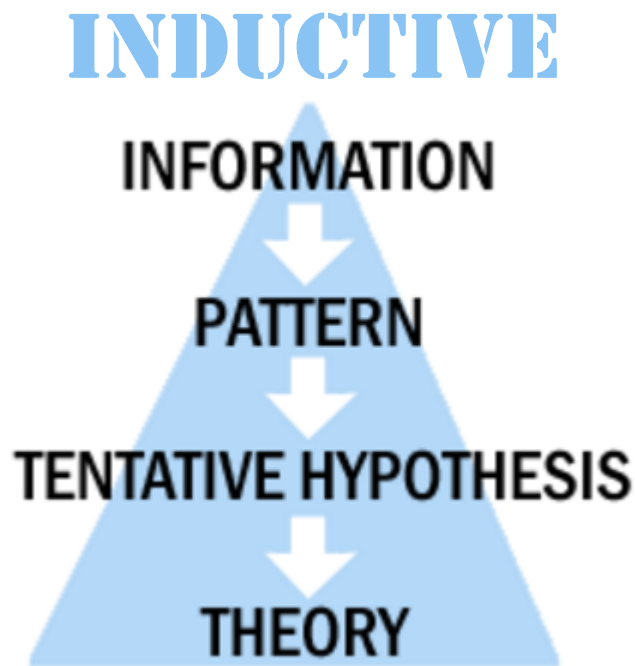
- 证明的本质是“保证真实性”，其涵义根据领域的不同有所差异：
 - 实验科学中的“证明”指利用归纳推理 (inductive reasoning) 去证实 (prove) 某个假设 (hypothesis)
 - 人们将大量特定的信息收集 (归纳) 起来并根据自身的知识和经验去观察，并推断 (推理) 哪些是真实的
 - 此类“证明”不产生定论 (mathematical certainty)



归纳推理的证明方式



- 归纳推理 (*i.e.* 推测、推证) 的逻辑过程

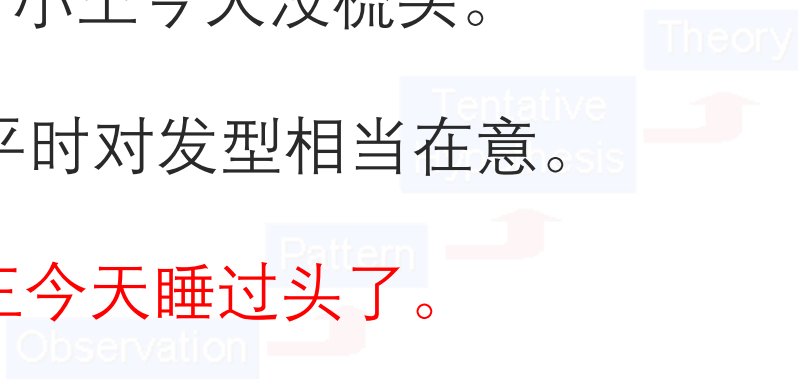




归纳推理的证明方式（续）



- 日常生活中“证明”的例子：
 - (premise) 我们观察到：小王今早上课迟到了。
 - (premise) 我们观察到：小王今天没梳头。
 - (premise) 经验：小王平时对发型相当在意。
 - (conclusion) 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），在**前提真实**的情况下每一步都必须提供确信的证据来支持中间结论，最终的逻辑推论称为系统中的**定理**（theorem）



演绎推理的证明方式（续）



- 演绎推理 (*i.e.* 证明) 的逻辑过程

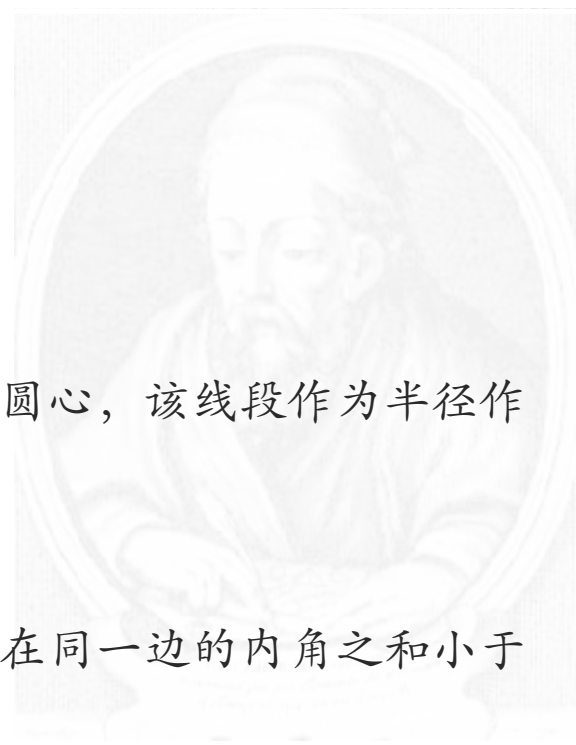




形式化证明 (formal proof)



- 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。

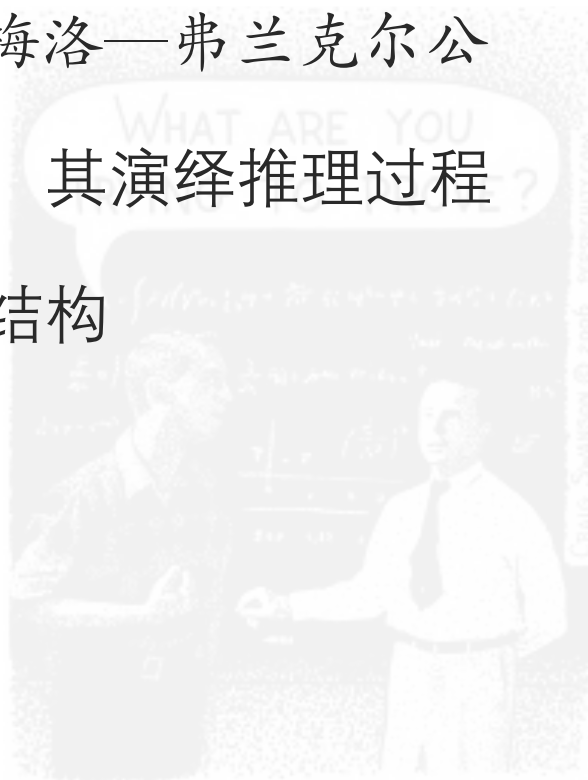




形式化证明 (formal proof)



- 对于本课程所涉及的所有形式化证明，其基于的公理化系统均为ZFC系统（含选择公理的策梅洛—弗兰克尔公理化集合论系统，在第五讲中介绍），其演绎推理过程可描述为一个一般的框架式逻辑证明结构





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 (i.e. 蕴含重言式) 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, \dots, 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 (续)




- (1) “若 A , 则 B ” :

$$A \rightarrow B$$

- (2) “ A 当且仅当 B ” :

$$A \leftrightarrow B$$

- (3) “证明 B ” :

 $\Rightarrow B$

- 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” \Leftrightarrow “ $A \rightarrow B$ 为真”
- 例：

证明：若 n 是奇数，则 n^2 也是奇数.

证：因为 $\exists k \in \mathbb{N}$, $n = 2k + 1$, 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 亦为偶数，从而原命题得证. \square



归谬法（反证法）



- **证明方法**：假设 A 真且 $\neg B$ 真，推出矛盾，即 $A \wedge \neg B \Rightarrow \perp$
- **理论依据**：“ $A \wedge \neg B \Rightarrow \perp$ ”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 $3n + 2$ 亦为偶数，矛盾！从而原命题得证. □



归谬法 (续)



■ 例2 :

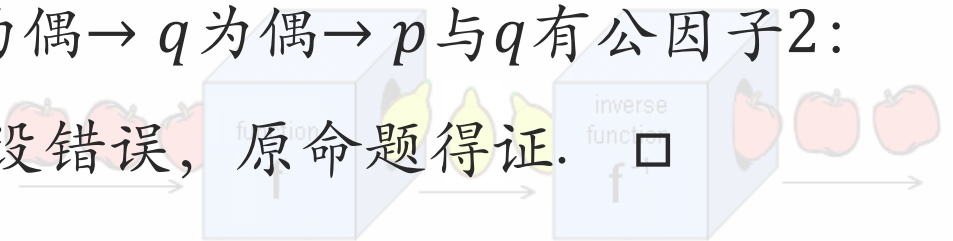
证明: $\sqrt{2}$ 是无理数.

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

的形式, 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. \square





广义归谬法



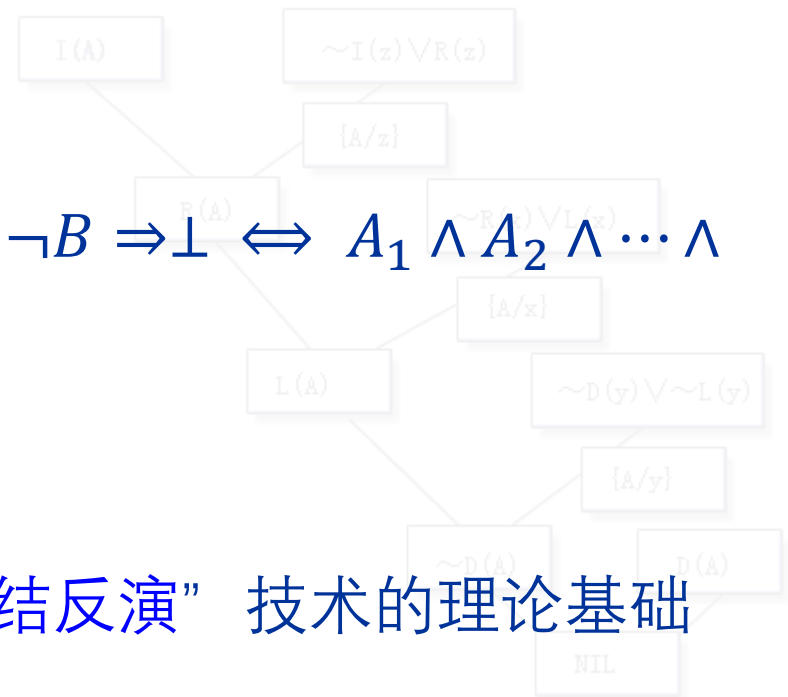
- **证明方法**：假设 A_1, A_2, \dots, A_k 真且 $\neg B$ 真，推出矛盾，即

$$A_1 \wedge A_2 \wedge \dots \wedge A_k \wedge \neg B \Rightarrow \perp$$

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

$$A_k \Rightarrow B$$

- 广义归谬法为人工智能中“归结反演”技术的理论基础





穷举法（分情形证明法）



- 证明目标： $A_1 \vee A_2 \vee \cdots \vee A_k \rightarrow B$
- 证明方法：证明 $A_1 \rightarrow B$, $A_2 \rightarrow B$, $\cdots A_k \rightarrow B$ 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 (续)



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

证: 见下表.

情况	$u = \max(b, c)$	$\max(a, u)$	$v = \max(a, b)$	$\max(v, c)$
$a \leq b \leq c$	c	c	b	c
$a \leq c \leq b$	b	b	b	b
$b \leq a \leq c$	c	c	a	c
$b \leq c \leq a$	c	a	a	a
$c \leq a \leq b$	b	b	b	b
$c \leq b \leq a$	b	a	a	a



构造性证明法



- **证明目标**：证明 $A \rightarrow B$ ，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 $x = (n + 1)!$ ，则 $2|(x + 2)$ ， $3|(x + 3)$ ，
 $\cdots n|(x + n)$ ， $(n + 1)|(x + n + 1)$ 这 n 个连续的正整数
为合数，命题得证. \square



空证明法（前件假证明法）



- 证明方法：要证 “ $A \rightarrow B$ 为真”，可证 “ A 为矛盾式”
- 理论依据：“ A 为矛盾式” \Rightarrow “ $A \rightarrow B$ 永真”
- 例：

证明：空集 \emptyset 是任何集合的子集.

证：根据子集的定义 $A \subseteq B \Leftrightarrow \forall x(x \in A \rightarrow x \in B)$ ，令

$A = \emptyset$ ，则对于任意集合 B ， $\emptyset \subseteq B \Leftrightarrow \forall x(x \in \emptyset \rightarrow x \in B)$

$\Leftrightarrow \forall x(\perp \rightarrow x \in B) \Leftrightarrow T$ ，命题得证.

□

	A	B	$A \rightarrow B$
(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 “ $A \rightarrow B$ 为真”，可证 “ B 为永真式”
- 理论依据：“ B 为永真式” \Rightarrow “ $A \rightarrow B$ 永真”
- 例：

证明：若 $a \leq b$ ，则 $a^0 \leq b^0$ 。

证：因为 $a^0 \leq b^0$ 恒为真，故命题得证。 \square

- 这种证明方式常在归纳证明的“奠基”中出现

	A	B	$A \rightarrow B$
(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 “ $\forall xP(x)$ 为假”，可找一个使 “ $\neg P(x)$ 为真” 的特例
- **理论依据**：“ $\neg \forall xP(x)$ ” \Leftrightarrow “ $\exists x \neg P(x)$ ”
- **例**：

证明：“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3个整数的平方和，故原命题为假命题. \square



命题为假的证明 (续)



- 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



本次课后作业



- 教材内容：[Rosen] 1.7–1.8节
- 课后习题：
 - Problem Set 4
- 提交时间：10月19日

