证明方法

回顾

问题1：如何基于命题逻辑进行推理?

- 蕴含永真式导出推理规则

问题2：什么是(一阶)谓词逻辑?

- 命题逻辑+谓词+量词；量化表达式

问题3：如何基于谓词逻辑进行推理?

- 命题逻辑的推理+全称/存在 例示/生成

本节提要

问题1：什么叫证明？
问题2：常见的证明方法有哪些？
问题3：什么是猜想？有哪些有意思的猜想？

定理与证明

- 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:
  - 公理(不证自明的基本事实)
  - (当前)定理的前提
  - 已经证明的定理(推论、命题、引理)

例

- 定理的陈述(举例)
  - 如果$x>y$，其中x和y是正实数，那么 $x^2>y^2$。
- 如何表达
  - $\forall x \forall y((x>y) \rightarrow (x^2>y^2))$ //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， $P(c) \rightarrow Q(c)$
  - 再使用全称引入，得到$\forall x (P(x) \rightarrow Q(x))$

归纳推理的证明方式

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：

- 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

- 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

- 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。

本节提要

问题1：什么叫证明?

- 表明定理为真的有效论证（演绎推理）

问题2：常见的证明方法有哪些?

问题3：什么是猜想？有哪些有意思的猜想?

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. $\square$

间接证明法

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

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$\emptyset$是任何集合的子集.

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

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”$\Longrightarrow$“$A \rightarrow B$为真”
- **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. □
- 这种证明方式常在数学归纳法的“**莫基**”中出现

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$3n+2$为偶数，与题设矛盾！原命题得证. $\square$

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. $\square$

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：**$A_1 \wedge A_2 \wedge \cdots \wedge A_k \wedge \neg B \Rightarrow \perp \Leftrightarrow A_1 \wedge A_2 \wedge \cdots \wedge$

  $A_k \Longrightarrow B$

穷举法(分情形证明)

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

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

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

穷举法

- 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$n^2 \ge n$。
  - $n \le 0$
  - $n \ge 1$

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≠0, a*x*+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$\boldsymbol{x} = (\boldsymbol{n} + \mathbf{1})!$，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. □

反例法(命题为假的证明)

- **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. □

证明中的错误

- 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

本节提要

问题1：什么叫证明?

- 表明定理为真的有效论证；演绎推理

问题2：常见的证明方法有哪些?

- 直接证明、间接证明、归谬法、分情形证明、等价性证明、存在性证明、唯一性证明

问题3：什么是猜想？有哪些有意思的猜想?

猜想

- 猜想
  - 被认为是真的（有意思的）陈述，还未证明其真假
  - 被证明为真：定理
    - 例：庞加莱猜想、四色猜想、费马猜想
  - 被证明为假：推翻
    - 例：费马曾经根据首四个费马数是素数，便猜想所有费马数都是素数
  - 被证明为不可证明
    - 例：连续统假设在集合论公理系统内不可证明/证伪

费马猜想->费马大定理

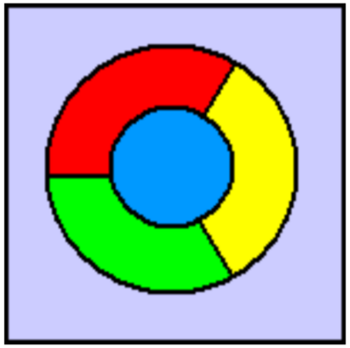
- Pierre de Fermat (1601-1665), France
  - Fermat's Last Theorem (1637) （费马大定理）
  - $x^n+y^n=z^n$ ($n>2$, $xyz\neq0$)没有正整数解

- 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
  - 谷山-志村猜想

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

四色猜想->四色定理



- **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**

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

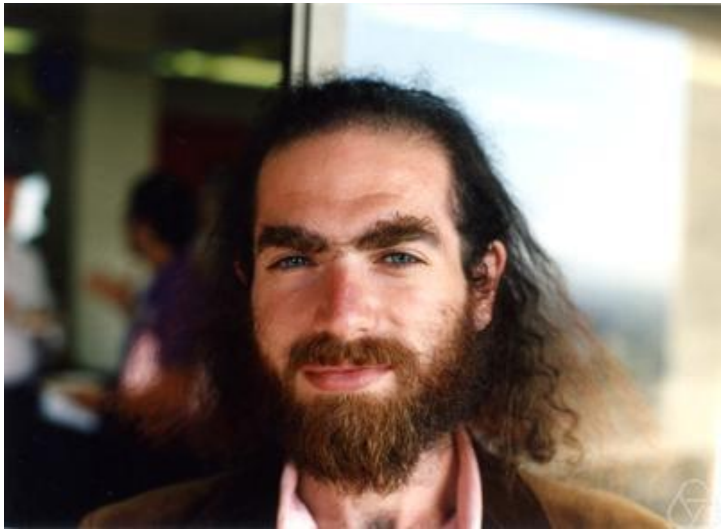
Grigori Perelman (1966-, Russian)

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 (100万美元)



"To do great work, you have to have a pure mind. You can think only about the mathematics. Everything else is human weakness. Accepting prizes is showing weakness."

本节提要

问题1：什么叫证明?

- 表明定理为真的有效论证；演绎推理

问题2：常见的证明方法有哪些?

- 直接证明、间接证明、归谬法、分情形证明、等价性证明、存在性证明、唯一性证明

问题3：什么是猜想？有哪些有意思的猜想?

- 尚未被证明的可能为真的陈述：费马大定理、四色定理、哥德巴赫猜想、庞加莱定理、黎曼猜想

作业

- 见课程主页