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

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（假定）
  - 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$\forall x\ (P(x) \rightarrow Q(x))$

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。
  - 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。

$$\forall n\,(Odd(n) \rightarrow Odd(n^2))$$

反证法

- 原理
  - $p \rightarrow q \equiv \neg q \rightarrow \neg p$
- 证明框架
  - $\neg q \Rightarrow \neg p$
  - 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。
  - **假设结论不存立(¬*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 (¬*p*)**
  - 因此，若**3n+2**是奇数，则**n**是奇数 **(*p*→ *q*)**

归谬法

- 原理
  - $q \equiv \neg q \rightarrow \mathbf{F}$
- 证明框架
  - $\neg q \Rightarrow r \wedge \neg r$
  - 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
  - $p_1 \wedge \ldots \wedge p_n \rightarrow q \equiv \neg q \wedge p_1 \wedge \ldots \wedge p_n \rightarrow \mathrm{F}$
- 证明框架
  - $\neg q, p_1, \ldots, p_n \Rightarrow$ 矛盾 (比如$p_1 \wedge \neg p_1$)
  - 所以， $p_1 \wedge \ldots \wedge p_n \rightarrow q$

分情形证明

- 原理
  - $p_1 \lor \ldots \lor p_n \to q \equiv (p_1 \to q) \land \ldots \land (p_n \to q)$
- 证明框架
  - $p_1 \Rightarrow q$
  - …
  - $p_n \Rightarrow q$
  - 因此， $p_1 \lor \ldots \lor p_n \to q$

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$x+y=1$.
  - $x < x^r$，$y < y^r \Rightarrow x+y < x^r+y^r \Rightarrow (x+y)^r < x^r+y^r$

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
  - $\exists x\ (P(x) \land \forall y\ (y \neq x \rightarrow \neg P(y)\ )$
  - $\exists x\ P(x) \land \forall y\ \forall z\ (P(y) \land P(z) \rightarrow y = z)$
- 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$(a-b)$
- $2b = b$
- $2 = 1$

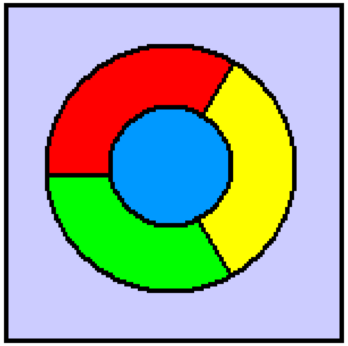
数学与猜想（费马大定理）

- **Pierre de Fermat (1601-1665), France**
  - **Fermat's Last Theorem (1637)** （费马大定理）
  - $x^n+y^n=z^n$ **(n>2,** $xyz\neq 0$**)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）



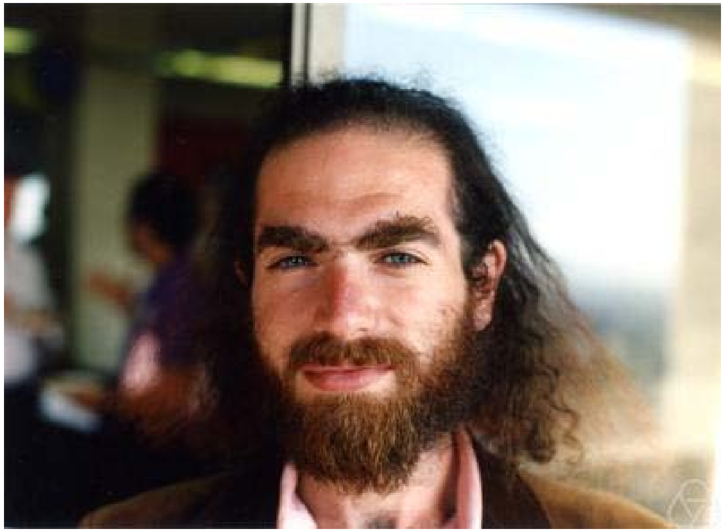
- Four Color Theorem
  - Proposed by in Francis Guthrie 1852
  - Proven in 1976 by Kenneth Ira Appel (1932-, New York) and Wolfgang Haken (1928-, Berlin)
    - Percy John Heawood (1861-1955, Britain) proved the five color theorem in 1890

世界数学难题

- <u>Hilbert's problems (23)</u>, ICM'1900, Paris
- <u>Millennium Prize Problems(7)</u> 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

作业

- 教材[1.6]
  - P64-65：25, 35, 39, 41
- 教材[1.7]
  - P75-76：11, 23, 29, 30