证明方法

2023,3,18

南京大学计算机科学与技术系

推理与证明

定义 17.2.2

自然推理系统 P 定义如下.

1. 字母表

   ❶ 命题变项符号: $p, q, r, \cdots, p_i, q_i, r_i, \cdots$, 其中 $i \geqslant 1$.

   ❷ 联结词符号: $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$.

   ❸ 括号与逗号: $(,), ,$.

2. 合式公式

   同定义 15.2.1.

3. 推理规则

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是自由变元，则$\exists xP$和$\forall xP$是**逻辑公式；**

●若P和Q是**逻辑公式**，则 $\neg P$, $P\wedge Q$, $P\vee Q$, $P\rightarrow Q$, $P\leftrightarrow Q$是**逻辑公式。**

●只有有限次应用上述规则形成的符号串才是**逻辑公式**

内容提要

- 定理和定理证明
- 证明方法
  - 直接证明法
  - 反证法
  - 归谬法
- 若干种证明策略
  - 分情形证明
  - 唯一性证明
  - 存在性证明

引言

- 定理（Theorem）(引理，推论)
  - 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（argument）。
- 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$\forall x \forall y\ (P(x, y) \rightarrow Q(x, y))$**

请注意，我们仍然
没有在证明结论为真

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

- **猜想（conjecture）**
  - **尚未被证明为真的陈述，通常是比较重要的陈述。**
    - **哥德巴赫猜想，四色图猜想**
  - **尚未有效论证，也没有被证伪。**

猜想

有效的证明方法

公理 定理 理论

概念：C_1,… …, C_m

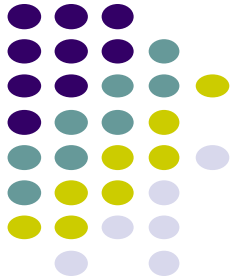
术语：T_1,… …, T_n

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

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

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

- 证明方法
  - 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$x' = x/(x+y)$, $y' = y/(x+y)$
  - $x < x^r$， $y < y^r \Rightarrow x+y < x^r+y^r \Rightarrow (x+y)^r < x^r+y^r$

当结论是析取式时：

- 原理：
  - $p \rightarrow (q \vee r) \equiv \sim p \vee q \vee r \equiv \sim(p \wedge \sim q) \vee r \equiv (p \wedge \sim q) \rightarrow r$

    因此，可以通过证明$\boldsymbol{p, \sim q \rightarrow r}$来证明$\boldsymbol{p \rightarrow (q \vee r)}$
- 证明: $n^2=m^2$ 仅当 $m=n$ 或 $m= -n$

  证： $n^2=m^2 \rightarrow n^2-m^2=0 \rightarrow (n+m)(n-m)=0$

  since $m \neq n$, we have $n-m \neq 0$, so, $n+m=0$

  So, $m= -n$

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。
    - $1729=10^3+9^3=12^3+1^3$
  - 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$(a-b)$**
- $2b=b$
- $2=1$

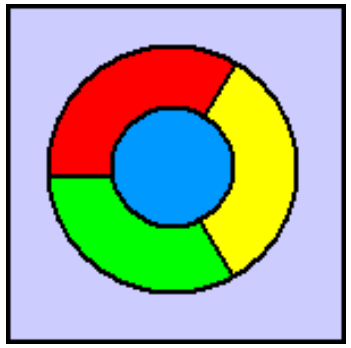
数学与猜想（费马大定理）

- **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

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