第4.7节 证明导论

Section 4.7: Introduction to Proofs

目录

知识要点

4.7.1 证明

- 证明是建立数学语句真实性的有效论证.
- 在数学, 计算机等学科中, 有时**非形式化证明**也会经常使用.
  - 证明过程中通常使用多个推理规则.
  - 推理规则可能隐式地被使用.
  - 更容易理解和向他人解释.

4.7.1 证明

- 证明在计算机领域有许多实际应用, 例如:
  - 验证计算机程序是否正确;
  - 确定操作系统是安全的;
  - 编写的程序能够在人工智能中做出推论;
  - 表明系统规范是一致的;
  - ……

4.7.1 证明

- 论证一个性质相对于论域(例如整数或实数)中的所有元素都成立．虽然描述需要全称量词, 但数学里通常**省略全称量词**.
  - 例如“如果$x > y$，其中x和y是正实数，那么$x^2 > y^2$”实际上表示“对于所有的正实数x和y, 如果$x > y$, 那么$x^2 > y^2$”

4.7.2 证明p→q

- 为了证明定理$\forall x\big(P(x) \rightarrow Q(x)\big)$，引入$c$表示论域$U$中的任意一个元素，然后采用全称引入规则，以上语句的真实性如:$P(c) \rightarrow Q(c)$. 所以，我们必须证明$p \rightarrow q$.

4.7.2 直接证明法证明p→q

- 立储风波:

《明朝那些事儿》: **朱棣**问“你认为该立谁?” **解缙**答“世子(指朱高炽)仁厚, 当为太子.” 朱棣不说话. 解缙再答“好圣孙(指朱瞻基)!” 朱棣笑了, 解缙也笑了, 事情就此定局.

- 【**直接证明法**】:
  - 第一步, 假设p为真;
  - 第二步, 用推理规则构造;
  - 第三步, 表明q也必须为真.

4.7.2 奇/偶数, 有/无理数的定义回顾

华中科技大学
计算机科学与技术学院
School of Computer Science &Technology, HUST

- 回顾奇/偶数, 有/无理数的定义, 在接下来的例子中会用到.

- 定义:如果存在整数k使得$n = 2k$, 整数n是**偶数**. 如果存在整数k使得$n = 2k + 1$, 则n是**奇数**. 注意每个整数是偶数或奇数, 但是没有整数既是偶数, 又是奇数.

- 定义:如果存在整数p和q, 其中$q \neq 0$, 使得$r = \frac{p}{q}$, 则实数r是**有理数**. 不是有理数的实数称为**无理数**.

4.7.2 直接证明法证明p→q

- 例:使用直接证明法证明"如果n是一个奇数, 那么n^2是奇数."

4.7.2 直接证明法证明p→q

- 例:使用直接证明法证明“如果n是一个奇数, 那么n^2是奇数.”
- 解:
  - 假设n是奇数. 那么存在整数k, $n = 2k + 1$.
  - 公式两边取平方可以得到$n^2=(2k+1)^2= 4k^2+4k+1= 2(2k^2+2k)+1 = 2r+1$, 其中$r$为整数, $r=2k^2+2k$. 根据奇数的定义, n^2是奇数.
  - 因此, 我们证明n是奇数, 那么n^2也是奇数.

4.7.2 直接证明法证明p→q

- 例:使用直接证明法证明两个有理数的和是有理数.

4.7.2 直接证明法证明p→q

- 例:使用直接证明法证明两个有理数的和是有理数.
- 解:假设r和s是两个有理数. 那么必须有整数p, q和t, u满足:

$$r=\frac{p}{q}, s=\frac{t}{u}, u \neq 0, q \neq 0$$

那么可得r和s的和为

$$r+s=\frac{p}{q}+\frac{t}{u}=\frac{pu+qt}{qu}=\frac{v}{w}, v=pu+qt, w=qu \neq 0$$

根据有理数的定义，可知r和s的和也是有理数.

4.7.3 间接证明法证明p→q

- 优孟马谏:

  楚庄王之时,有所爱马,衣以文绣,置之华屋之下,席以露床,啖以枣脯.马病肥死,使群臣丧之,欲以棺椁大夫礼葬之.左右争之,以为不可.王下令曰: “有敢以马谏者,罪至死” **优孟**闻之,入殿门.仰天大哭.王惊而问其故.优孟曰:“马者王之所爱也,以楚国堂堂之大,何求不得,而以大夫礼葬之,薄.请以人君礼葬之”王曰: “何如”对曰:“臣请以雕玉为棺,文梓为椁,齐、赵陪位于前,韩、魏翼卫其后,庙食太牢,奉以万户之邑.诸侯闻之,皆知大王贱人而贵马也”王曰:“寡人之过一至此乎!为之奈何?”优孟曰:“请为大王六畜葬之.以垅灶为椁,铜历为棺,赍以姜枣,荐以木兰,祭以粮稻,衣以火光,葬之于人腹肠”于是王乃使以马属太官,无令天下久闻也.

- 有时直接证明法会走向死胡同. 不采用直接证明法, 即不从前提开始, 以结论结束来证明的方法叫做**间接证明法**. 其中, 一类非常有用的间接证明法称为**反证法**.

4.7.3 间接证明法-反证法证明p→q

- 【**反证法**】 假设$\neg q$为真, 然后证明$\neg p$为真. 如果证明$\neg q \rightarrow \neg p$, 那么相当于证明了$p \rightarrow q$.
- 备注: $p \rightarrow q \equiv \neg q \rightarrow \neg p$, 条件语句和它的逆否命题是逻辑等价.

4.7.3 间接证明法-反证法证明p→q

- 例:反证法证明如果n是整数且$3n+2$是奇数, 则n是奇数.

4.7.3 间接证明法-反证法证明p→q

- 例:反证法证明如果n是整数且$3n+2$是奇数, 则n是奇数.
- 解:
  - 假设n是偶数. 因此存在整数k, $n=2k$. 那么$3n+2=3(2k)+2=6k+2=2(3k+1)=2j$, 其中$j=3k+1$. 因此$3n+2$是偶数.
  - 由于我们已经证明了$\neg q \to \neg p$, 那么$p \to q$也就成立. 也就是说"如果n是整数并且$3n+2$是奇数(不是偶数), 则n是奇数(不是偶数)".

4.7.3 间接证明法-反证法证明p→q

- 例:反证法证明对于整数n, 如果n^2为奇数, 则n为奇数.