

计算机问题求解-论题1-3

常用证明方法及其逻辑正确性

陶先平

2015年10月8日

Outlines

- 反证法及其逻辑正确性
- 分情形证明法及其逻辑正确性
- 数学归纳法及其逻辑正确性
- 鸽笼原理证明法及其逻辑正确性

$\sqrt{2}$ is not rational (Pythagoreans)?

Proof.

Suppose, to the contrary, that $\sqrt{2}$ is rational. Then there exist integers p and q (with q nonzero) such that $\sqrt{2} = p/q$. We may assume that p and q have no common factor, for if they did, we would simplify and begin again. Now, we have that $\sqrt{2}q = p$. Squaring both sides, we obtain $2q^2 = p^2$. Thus p^2 is even. Therefore, we know from Problem 3.1 that p must be even, so $p = 2m$ for some integer m . This means that $2q^2 = (2m)^2 = 4m^2$, so we see that $q^2 = 2m^2$. But this means that q^2 is even. From Problem 3.1 that q is even. So p and q have a common factor of 2, which is completely absurd, since we assumed they had no common factor. Therefore our assumption that $\sqrt{2}$ is rational must be wrong and we have completed the proof of the theorem. ■

你有没有怀疑过
这个“therefore”
的正确性？

There are infinitely many prime numbers.

Proof.

To prove this statement suppose, to the contrary, that there are finitely many primes. Then we may write these finitely many primes in ascending order as

$$2, 3, 5, \dots, N,$$

where N is the largest prime. Now consider the number M defined by

$$M = (2 \cdot 3 \cdot 5 \cdot \dots \cdot N) + 1.$$

If M is prime, then M is a prime that is larger than the largest prime N . Therefore, we must conclude that M is not prime, and so it is divisible by some prime number, P . However, P must appear in the list of primes

$$2, 3, 5, \dots, N,$$

which we gave earlier. But when we divide M by P , we obtain a remainder of 1. Therefore, P cannot be a factor of M , and we have contradicted our assumption that there are finitely many primes. Thus, there exist infinitely many primes. ■

We set a contrary of our theorem and use this assumption to start

Then we get a contradiction through a valid argument

Then we get the theorem quickly

反证法的逻辑正确性必定来自于逻辑！

• 令：A表示 $\sqrt{2}$ 不是有理数；B(p,q)表示m和n互质

• 假定 $\neg A$ 成立

• 推理：

• $\neg A$

• $\exists p \exists q \left(\sqrt{2} = \frac{p}{q} \wedge B(p, q) \right)$

• $p^2 = 2q^2$

• p是偶数，令 $p=2m$

• q是偶数

• $B(p, q) \wedge \neg B(p, q)$

• False

• $A=T$

//注意以下推理中p和q的辖域

其实，这两步之间的逻辑还挺复杂，更为本质！

$(\neg A, \text{若干数学定理}) \rightarrow F$

$T \rightarrow \neg(\neg A \wedge \text{若干数学定理})$

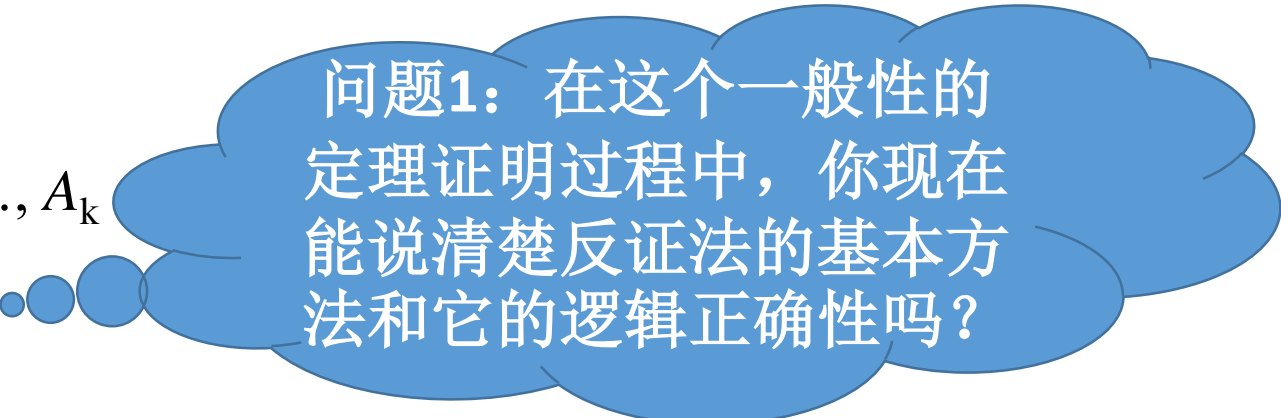
$(\neg A \wedge \text{若干数学定理}) = F$

$\neg A = F$

$A=T$

反证法的逻辑正确性必定来自于逻辑！

- 定理证明：
 - 前提：一组命题公式 A_1, A_2, \dots, A_k
 - 结论：一个命题公式 B
- 如果是这样：
 - 前提：一组命题公式 $\neg B, A_1, A_2, \dots, A_k$
 - 结论：F
 - 即： $\neg B, A_1, A_2, \dots, A_k \Rightarrow F$
 - $\neg B \wedge A_1 \wedge A_2 \wedge \dots \wedge A_k = F$
 - A_1, A_2, \dots, A_k 为真
 - $\neg B = F$
 - $B = T$



问题1：在这个一般性的定理证明过程中，你现在能说清楚反证法的基本方法和它的逻辑正确性吗？

问题2

- 反证法有时比直接证明法更好用。你能说说为什么吗？
- 如果需要你证明如下定理，你有什么想法？
 - 前提： A_1, A_2, \dots, A_m
 - 结论： B_1 或者 B_2 或者 ... 或者 B_n

Theorem 5.3.

Let x and y be real numbers. Then $|xy| = |x||y|$.

Proof.

First, suppose that $x > 0$ and $y > 0$. Then $xy > 0$ and we have $|xy| = xy$, $|x| = x$, and $|y| = y$. Therefore,

$$|xy| = xy = |x||y|,$$

and we have established the result in this case.

Second, suppose that $x < 0$ and $y < 0$. Then $xy > 0$ and we have $|xy| = xy$, $|x| = -x$, and $|y| = -y$. Therefore,

$$|xy| = xy = (-x)(-y) = |x||y|,$$

and we have the result for this case as well.

Third, suppose that either $x = 0$ or $y = 0$. Then $xy = 0$ and we have $|xy| = 0$, and either $|x| = 0$ or $|y| = 0$. Therefore,

$$|xy| = 0 = |x||y|,$$

establishing the result in this case too.

For our final case, suppose that one number is positive and the other is negative. Thus, we may assume that $x < 0$ and $y > 0$. Then $xy < 0$ and we have $|xy| = -(xy)$, $|x| = -x$, and $|y| = y$. Therefore,

$$|xy| = -(xy) = (-x)y = |x||y|.$$

We have now established the result for all four possible cases and we may conclude that $|xy| = |x||y|$ for all real numbers x and y . ■

问题3：这种证明方法为什么被称为分情形证明法？

问题5：有的时候，我们在证明时会用到“不失一般性”这个词，你理解这是什么意思吗？

问题4：这种证明方法最“令人担心”的是什么？

问题6：你能用学过的逻辑知识说明分情形证明法的正确性吗？

- 证明 $p \rightarrow q$ ，如果恰有 $p \equiv p_1 \vee p_2 \vee \dots \vee p_n$ ，则有：
 - $(p \rightarrow q) \equiv (p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \dots \wedge (p_n \rightarrow q)$
- 因此：
 - $p \equiv p_1 \vee p_2 \vee \dots \vee p_n$ 成为关键所在，成为这种证明方法的“令人担心”的地方

存在性证明

- 证明具有某种性质的对象的存在性
 - $\exists x p(x)$
- 基本方法：
 - 构造法：找到一个 a , $p(a)=T$
 - 非构造法：归谬证明 $\forall x \neg p(x) = F$
- 讨论题：
 - Chomp游戏，你该如何幸存？

关于数学归纳法

- 数学归纳法通常可以用于证明形如以下的命题：
 - $\forall xP(x)$

问题7：对于这个说法，你有什么感想？你心目中印象最深刻的用数学归纳法证明的定理是什么？

数学归纳法的逻辑基础是什么？

- 其合理性来自证明对象的结构：
- 自然数的结构：
 - 0(或者1)是自然数；
 - 如果 k 是自然数， k 的“后继”也是自然数；
 - 自然数只能通过使用上述规则有限次得到
- 一般来讲，我们用良序性来描述上述类似结构：

Well-ordering principle of \mathbb{N} .

Every nonempty subset of the natural numbers contains a minimum.

数学归纳法的逻辑正确性会在哪儿被质疑？

Theorem 17.1 (Principle of mathematical induction).

For an integer n , let $P(n)$ denote an assertion. Suppose that

(i) (The base step) $P(1)$ is true, and

(ii) (The induction step) for all positive integers n , if $P(n)$ is true, then $P(n + 1)$ is true.

Then *$P(n)$ holds for all positive integers n .*

$P(1), \forall n(P(n) \rightarrow P(n + 1))$ 能否推理出 $\forall nP(n)$?

$P(1) \wedge \forall n(P(n) \rightarrow P(n + 1)) \rightarrow \forall nP(n)$ 是否永真

Proof.

Suppose the induction principle were false. Then there would exist an assertion P that would satisfy conditions (i) and (ii) of the theorem, but $P(n)$ would be false for some $n \in \mathbb{Z}^+$. So let $A = \{k \in \mathbb{Z}^+ : P(k) \text{ is false}\}$. Our supposition implies that A is nonempty. By the well-ordering principle [p. 135], the set A has a minimum. Let m denote this minimum. By condition (i), $m \neq 1$. Since $m \in \mathbb{Z}^+$, it follows that $m \geq 2$. Consider the integer $n = m - 1 \geq 1$. Since $n < m$ and m is the minimum of A , we know that $n \notin A$. Thus $P(n)$ is true. By condition (ii), $P(n + 1)$ is true too. But $P(n + 1) = P(m)$, so $P(m)$ must also be true, a contradiction. ■

- 几个问题：
- 1, 良序性如果没有, 数学归纳法会出什么问题?
 - 2, 两个前提条件分别在哪里被使用?

两个范例

- 用数学归纳法证明用4分和5分就可以组成12分及以上的每种邮资：

- 奠基：3个4分硬币组成12分
- 假设： k 分邮资可以由4分和5分硬币组成
- 归纳：
 - 如果 k 分邮资组合中含有4分硬币，用5分硬币替换；
 - 如果 k 分邮资组合中不含有4分硬币， ???

- 所有的马都是白马

- 令 $p(n)$:任意 n 匹马都是同一种颜色
- 奠基： $p(1)$ 成立
- 假设： $p(k)$ 成立
- 归纳： $(p(k) \rightarrow p(k+1))$
 - 将 $k+1$ 匹马分为两群：前 k 匹马同色（不失一般性，为白马），后 k 匹马同色，这两群马均同色，为白马
 - $k+1$ 匹马均为白色，同色
- 结论为真，证明结束



问题出在哪里？

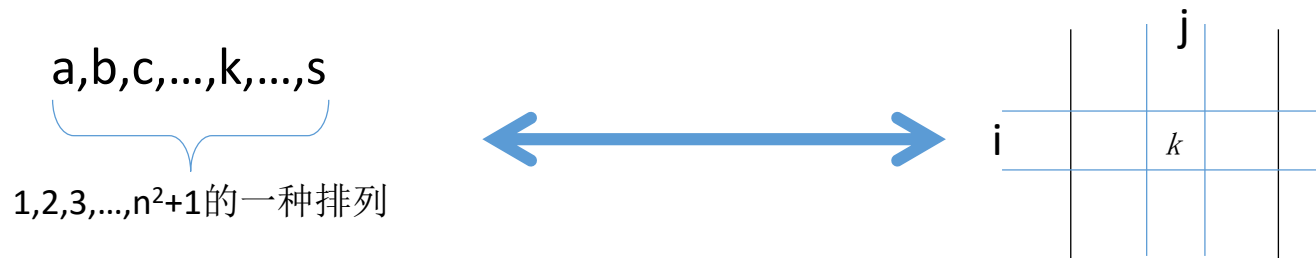
关于鸽笼原理的讨论

- 为什么以下定理被命名为鸽笼原理？
- Let A and B be finite sets and let $f:A \rightarrow B$. If $|A| > |B|$, then f is not one to one function. If $|A| < |B|$, then f is not onto.

不可能是单射，意味着什么？

看不见的鸽笼，看不见的鸽子

- 自然数 $1,2,3,\dots,n^2+1$ 的任何一种排列中，必然含一个长度不小于 $n+1$ 的严格递增链或严格递减链
- 假设严格递增与递减序列最大长度均不大于 n ，建立 $n*n$ 矩阵 M 如下：
 - $M[i,j]=k(k \in \{1,2,\dots,n^2+1\})$ iff 在所给的序列中以 k 开始的严格递增序列长度为 i ，以 k 开始的严格递减序列长度为 j

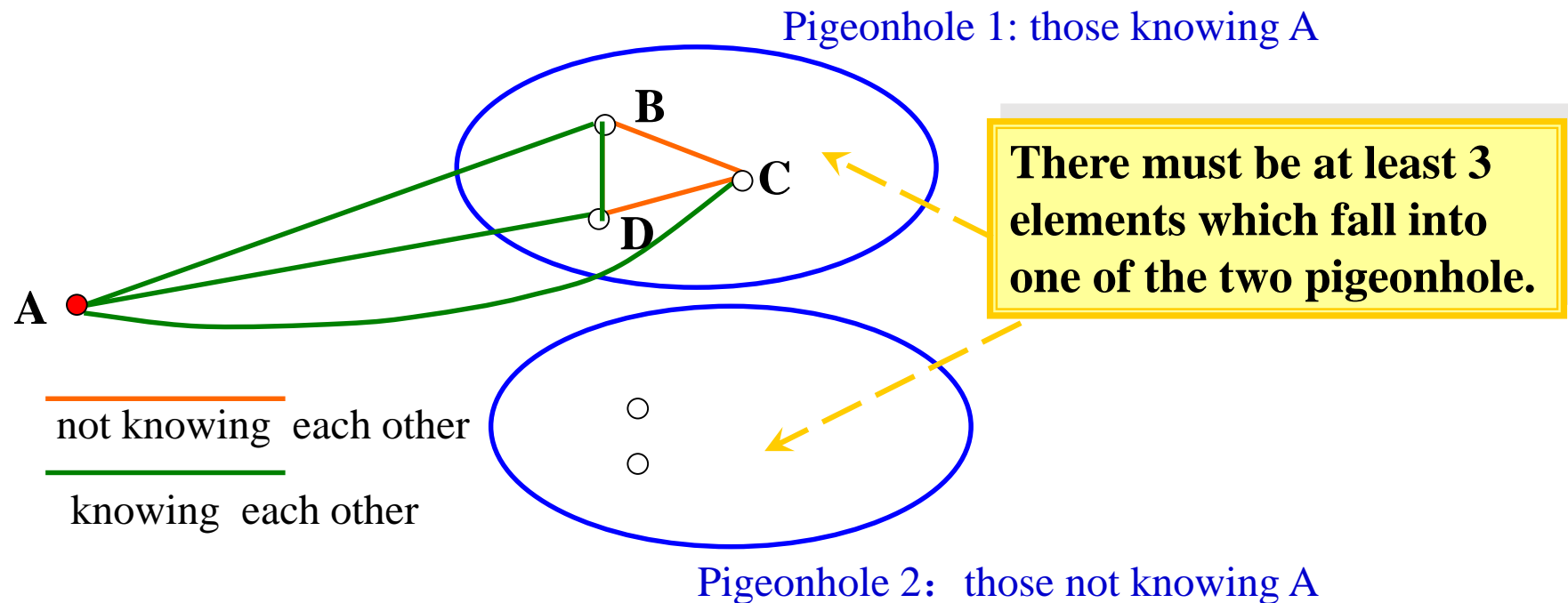


排列中的每个元素都一定会出现在矩阵 M 中，矩阵 M 最多有 n^2 个位置=》必有两个元素在同一个位置

假设有 p, q 都落入了 $M[i, j]$ 中，分析 p, q 大小和 p, q 在排列中出现的位置，有若干情况 $p < q; p > q; p$ 在 q 前; p 在 q 后：
无论何种情况，如 $p < q; p$ 在 q 前，从 p 的递增序列长度一定大于 i 。
矛盾！

Knowing Each Other or Not

Problem: show that among any 6 persons, there are 3 who know each other, or there are 3 who don't know any two others.



最后几个问题：

- 1, 一个证明的正确性是由哪些方面保证的？
- 2, 一个正确的结论是由哪些方面保证的？
- 3, 证明方法在证明过程中起到了什么作用？