证明导论介绍
Methods of proof

注：学生自己学习，不作考试要求

引言

- 在数学研究中提出的两个重要问题
- 什么时候数学论证是正确的？
- 什么方法可以用来构造数学论证？
  - 通过描述各种形式的正确与不正确的数学论证来帮助回答这些问题。
- 定理：可以被证明为真的命题。
- 证明：用一系列命题来证明一条定理为真，这些命题就形成一项论证。

- 在证明中用到的命题包括：
  - 公理或公设：某门学科中不需要证明而必须加以承认的某些陈述或命题，即“不证自明”的命题。
  - 被证明定理本身的前提
  - 从前证明过的定理
- 推理规则把证明的各个步骤联系起来

- 引理：
  - 在其他定理的证明中所用的简单定理
  - 当使用了一系列的引理时，一些复杂的证明通常会更容易别理解
  - 其中每个引理都被单独地证明

- 推论：
  - 从已经证明了的定理直接证实的命题
- 猜想：
  - 真值未知的命题，当发现了猜想的证明时，这个猜想就称为定理。猜想不是定理。

谬误

- 常见的谬误来源于不正确的论证
- 这些谬误看上去像推理规则，但它们是基于偶然事件而不是重言式
- 肯定结论谬误
- 否定假设谬误
- 循环论证

肯定结论谬误

- $[(p\to q)\wedge q]\to p$
- 不是重言式，因为当p为假而q为真时，它为假。
- 存在许多把它当做重言式的不正确论证
- “若你做本书的每一道练习，则你将学习离散数学。你学习过离散数学。

因此，你做过本书的每一道题。”

否定假设谬误

- $[(p \to q) \wedge \neg p] \to \neg q$
- 不是重言式，因为当p为假而q为真时，它为假
- “若你做本书的每一道练习，则你将学习离散数学。你没做过本书里的每一道练习。

那么，你没有学习过离散数学。”

循环论证

- 回避正题的谬误
- 当证明中的一步或多步是基于被证明的命题为真时，就出现这种谬误
- 当用命题自身或与其等价的命题去证明该命题时就产生这种谬误

循环论证

- 证明：每当n^2是偶数时，n就是偶数。

  假定n^2是偶数，则对某个整数k来说有 $n^2=2k$；

  设对某个整数l来说有$n=2l$；

  这就证明了n是偶数。
- 证明里出现的“设对某个整数l来说有$n=2l$”没有给出任何论证来证明它为真；
- 这个命题等价于被证明的命题。

证明定理的方法

- 如何证明不同类型的命题
- 证明蕴含式的技术：
  - 直接证明
  - 间接证明
  - 空证明
  - 平凡证明
  - 归谬证明
  - 分情形证明

直接证明

- 若p为真则q也必然为真
- 假定p为真，并且使用推理规则和已经证明的定理，来证明q也必然为真
- 例：给出定理"若n是奇数，则n^2是奇数"的直接证明。

间接证明

- 因为$p \rightarrow q$等价于它的逆否命题$\neg q \rightarrow \neg p$
- 所以可以通过证明它的逆否命题为真，来证明$p \rightarrow q$
- 例：给出定理“若$3n+2$是奇数，则n是奇数”的间接证明。

空证明

- 假定$p \rightarrow q$的前件p为假，则$p \rightarrow q$为真
- 因为该命题形如**F→T**或**F→F**
- 若可以证明p为假，则可以给出$p \rightarrow q$的证明，这就称为空证明

- 常常用来证明一些定理的特殊情形
- 这些定理：对所有正整数来说，一个蕴含式为真（$\forall nP(n)$）
- 例：证明命题$P(0)$为真，其中$P(n)$是命题函数“若$n>1$，则$n^2>n$”。
- 解：命题$P(0)$是蕴含式“若$0>1$，则$0^2>0$”。

平凡证明

- 假定p→q的后件q为真，则p→q为真
- 因为该命题形如T→T或F→T
- 若可以证明q为真，则可以给出p→q的证明，这就称为平凡证明

- 当证明定理的特殊情形时，以及在数学归纳法中，平凡证明常常是重要的
- 例：设$P(n)$是命题“若a和b是满足$a \geq b$的正整数，则$a^n \geq b^n$”。证明命题$P(0)$为真。
- 解：命题$P(0)$是“若$a \geq b$，则$a^0 \geq b^0$”。

归谬证明

- 要证明p为真
- 假定可以找到矛盾式q使得$\neg p \to q$为真，即$\neg p \to F$为真，于是命题$\neg p$必然为假，所以p必然为真。
- 当可以找到矛盾式（比如$r \wedge \neg r$）使得有可能证明$\neg p \to (r \wedge \neg r)$为真时，就可以使用该技术。

- 例：利用归谬证明来证明$\sqrt{2}$是无理数。
- 解：设p是命题“$\sqrt{2}$ 是无理数”。
- 假定$\neg p$为真，则 $\sqrt{2}$是有理数。
- 需要证明它导致矛盾。
- 如果$\sqrt{2}$是有理数，则存在整数a和b，满足
  $\sqrt{2} = a/b$，其中a和b没有公因子。
- 两边平方，$2=a^2/b^2$。

- 两边平方，$2=a^2/b^2$。
- 因此，$2b^2=a^2$。这就意味着a^2是偶数，它蕴含着a是偶数。
- 因为a是偶数，所以对某个整数c来说有$a=2c$。因此$2b^2=4c^2$，所以，$b^2=2c^2$。
- 这意味着b^2是偶数，因此b也是偶数。

- 已经证明了$\neg p$蕴含着 $\sqrt{2}=a/b$，其中a和b没有公因子，以及2整除a和b。
- 令r是命题：a和b是没有公因子的整数。
- $\neg p \to (r \wedge \neg r)$，因此$\neg p$为假。
- 所以p为真。

- 对于一个蕴含式的间接证明可以改写成归谬证明。
- 在$p \to q$的间接证明里，假定$\neg q$为真而证明$\neg p$也必为真；
- 改写为归谬证明：假定p和$\neg q$都为真，然后利用间接证明的步骤来证明$\neg p$也必然为真。这样就得出矛盾式$p \wedge \neg p$，由此完成归谬证明。

- 例：给出定理“若$3n+2$是奇数，则n是奇数”的归谬证明。
- 解：假定$3n+2$是奇数，而n不是奇数，即n是偶数。
- 按照间接证明的步骤，可以证明若n是偶数则$3n+2$是偶数。
- 这与$3n+2$是奇数的假定矛盾，证毕。

- 有时为了证明$p \to q$为真，可以用析取式$p_1 \vee p_2 \vee \ldots \vee p_n$代替$p$作为蕴含式的前件，其中$p$与$p_1 \vee p_2 \vee \ldots \vee p_n$等价。
- 例：证明蕴含式“若n是不能被3整除的整数，则$n^2 \equiv 1 \pmod 3$”。
- 解：p:n不能被3整除；q:$n^2 \equiv 1 \pmod 3$
- p_1:$n \equiv 1 \pmod 3$；p_2:$n \equiv 2 \pmod 3$
- $p = p_1 \vee p_2$

停机问题

- 计算机科学中最著名的定理之一
- 存在一个不能用任何过程来解决的问题（存在一个不可解的问题）

- 不能简单地运行一个程序来判断它是否停机
- 如果停止了，能得出结论
- 但如果经过了任何固定的时间之后它仍运行，则不能判断
- 很容易写出一个需要经过10亿年以后才停止的程序