Chap1 The Foundations: Logic and Proofs

Part III: Proofs

Jin-Hui Wu

2026-03-12

大纲

- ❑ 命题逻辑
- ❑ 谓词逻辑
- ❑ 证明方法

大纲

- 推理规则 (1.6)
  - 命题逻辑推理规则
  - 谓词逻辑推理规则
- 证明方法

命题逻辑推理规则

- 论证 (argument)
  - 论证是一系列命题
  - 最后一个之外的称为前提 (premise)
  - 最后一个称为结论 (conclusion)

命题逻辑推理规则

- 论证 (argument)
  - 论证是一系列命题
  - 最后一个之外的称为前提 (premise)
  - 最后一个称为结论 (conclusion)

  - 当前提可以得出结论时，论证是有效的 (valid)
  - $(p_1 \land p_2 \land \ldots \land p_n) \rightarrow q$ 是永真式

命题逻辑推理规则

- 论证 (argument)
  - 论证是一系列命题
  - 最后一个之外的称为前提 (premise)
  - 最后一个称为结论 (conclusion)

  - 当前提可以得出结论时，论证是有效的 (valid)
  - $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \to q$ 是永真式

- 推理规则 (inference rule)
  - 简单且有效的论证，可用于复杂论证中

命题逻辑推理规则

- 肯定前件 / 假言推理 (Modus Ponens)

$$\begin{array}{l} p \to q \\ p \\ \hline \therefore q \end{array}$$

- 对应永真式

$$(p \wedge (p \to q)) \to q$$

  - 前件为假时，蕴含为真
  - 只需验证前件为真时，结论也为真

命题逻辑推理规则

- 否定后件 / 拒取 (Modus Tollens)

$$\boxed{\begin{array}{l} p \rightarrow q \\ \neg q \\ \hline \therefore \neg p \end{array}}$$

- 对应永真式

$$(\neg q \land (p \rightarrow q)) \rightarrow \neg p$$

命题逻辑推理规则

- 假言三段论 (Hypothetical Syllogism)

$$\boxed{\begin{array}{l} p \to q \\ q \to r \\ \hline \therefore p \to r \end{array}}$$

- 对应永真式

$$((p \to q) \wedge (\mathrm{q} \to r)) \to (p \to r)$$

命题逻辑推理规则

- 析取三段论 (Disjunctive Syllogism)

$$\boxed{\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore q \end{array}}$$

- 对应永真式

$$(\neg p \wedge (p \vee q)) \rightarrow q$$

命题逻辑推理规则

- 附加 (Addition)

$$\boxed{\begin{array}{l} p \\ \hline \therefore p \lor q \end{array}}$$

- 对应永真式

$$p \to (p \lor q)$$

命题逻辑推理规则

- 化简 (Simplification)

$$\boxed{\begin{array}{c} p \land q \\ \hline \therefore q \end{array}}$$

- 对应永真式

$$(p \land q) \to q$$

命题逻辑推理规则

- 合取 (Conjunction)

$$\boxed{\begin{array}{l} p \\ q \\ \hline \therefore p \wedge q \end{array}}$$

- 对应永真式

$$((p) \wedge (q)) \rightarrow (p \wedge q)$$

命题逻辑推理规则

- 消解 (Resolution)

$$\begin{array}{|l|}\hline \quad \neg p \vee r \\ \quad p \vee q \\ \hline \quad \therefore q \vee r \\ \hline \end{array}$$

- 对应永真式

$$((\neg p \vee r) \wedge (p \vee q)) \rightarrow (q \vee r)$$

命题逻辑推理规则

中文名	英文名	推理规则
肯定前件	Modus Ponens	$(p \wedge (p \rightarrow q)) \rightarrow q$
否定后件	Modus Tollens	$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$
假言三段论	Hypothetical Syllogism	$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$
析取三段论	Disjunctive Syllogism	$(\neg p \wedge (p \vee q)) \rightarrow q$
附加	Addition	$p \rightarrow (p \vee q)$
化简	Simplification	$(p \wedge q) \rightarrow p$
合取	Conjunction	$((p) \wedge (q)) \rightarrow (p \wedge q)$
消解	Resolution	$((\neg p \vee r) \wedge (p \vee q)) \rightarrow (q \vee r)$

例

- From $p \land (p \to q) \land r$, show that q is a conclusion

中文名	英文名	推理规则
肯定前件	Modus Ponens	$(p \land (p \to q)) \to q$
否定后件	Modus Tollens	$(\neg q \land (p \to q)) \to \neg p$
假言三段论	Hypothetical Syllogism	$((p \to q) \land (q \to r)) \to (p \to r)$
析取三段论	Disjunctive Syllogism	$(\neg p \land (p \lor q)) \to q$
附加	Addition	$p \to (p \lor q)$
化简	Simplification	$(p \land q) \to p$
合取	Conjunction	$((p) \land (q)) \to (p \land q)$
消解	Resolution	$((\neg p \lor r) \land (p \lor q)) \to (q \lor r)$

例

- “It is not sunny this afternoon and it is colder than yesterday.”
- “We will go swimming only if it is sunny.”
- “If we do not go swimming, then we will take a canoe trip.”
- “If we take a canoe trip, then we will be home by sunset.”
- Conclusion: “We will be home by sunset.”

中文名	英文名	推理规则
肯定前件	Modus Ponens	$(p \wedge (p \rightarrow q)) \rightarrow q$
否定后件	Modus Tollens	$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$
假言三段论	Hypothetical Syllogism	$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$
析取三段论	Disjunctive Syllogism	$(\neg p \wedge (p \vee q)) \rightarrow q$
附加	Addition	$p \rightarrow (p \vee q)$
化简	Simplification	$(p \wedge q) \rightarrow p$
合取	Conjunction	$((p) \wedge (q)) \rightarrow (p \wedge q)$
消解	Resolution	$((\neg p \vee r) \wedge (p \vee q)) \rightarrow (q \vee r)$

大纲

- ❑ 推理规则 (1.6)
  - ❑ 命题逻辑推理规则
  - ❑ 谓词逻辑推理规则
- ❑ 证明方法

谓词逻辑推理规则

- 谓词逻辑中有联结词
- 可以使用命题逻辑推理规则

- 谓词逻辑中还有变量、谓词和量词
- 有新的谓词逻辑推理规则

谓词逻辑推理规则

❑ 全称实例 (Universal Instantiation)

$$\boxed{\begin{array}{l} \forall x P(x) \\ \hline \therefore P(c) \end{array}}$$

Example:

Our domain consists of all dogs and Fido is a dog.

“All dogs are cuddly.”

“Therefore, Fido is cuddly.”

谓词逻辑推理规则

- 全称引入 (Universal Generalization)

$$\boxed{\begin{array}{l} P(c) \text{ for an arbitrary } c \\ \hline \therefore \forall x P(x) \end{array}}$$

- 通常隐式地用于数学证明中

谓词逻辑推理规则

- 存在实例 (Existential Instantiation)

$$\boxed{\begin{array}{l} \exists x P(x) \\ \hline \therefore P(c) \text{ for some element } c \end{array}}$$

Example:

"There is someone who got an A in the course."

"Let's call her *a* and say that *a* got an A"

谓词逻辑推理规则

- 存在引入 (Existential Generalization)

$$\begin{array}{l} P(c) \text{ for some element } c \\ \hline \therefore \exists x P(x) \end{array}$$

Example:

"Michelle got an A in the class."

"Therefore, someone got an A in the class."

谓词逻辑推理规则

中文名	英文名	推理规则
肯定前件	Modus Ponens	$(p \land (p \to q)) \to q$
否定后件	Modus Tollens	$(\neg q \land (p \to q)) \to \neg p$
假言三段论	Hypothetical Syllogism	$((p \to q) \land (q \to r)) \to (p \to r)$
析取三段论	Disjunctive Syllogism	$(\neg p \land (p \lor q)) \to q$
附加	Addition	$p \to (p \lor q)$
化简	Simplification	$(p \land q) \to p$
合取	Conjunction	$((p) \land (q)) \to (p \land q)$
消解	Resolution	$((\neg p \lor r) \land (p \lor q)) \to (q \lor r)$
全称实例	Universal Instantiation	$\forall x P(x) \to P(c)$
全称引入	Universal Generalization	$P(c)$ for any $c \to \forall x P(x)$
存在实例	Existential Instantiation	$\exists x P(x) \to P(c)$ for some c
存在引入	Existential Generalization	$P(c)$ for some $c \to \exists c P(c)$

例 (p25)

- "Every man has two legs."
- "John Smith is a man."
- Conclusion: "John Smith has two legs"

中文名	英文名	推理规则
肯定前件	Modus Ponens	$(p \land (p \to q)) \to q$
否定后件	Modus Tollens	$(\neg q \land (p \to q)) \to \neg p$
假言三段论	Hypothetical Syllogism	$((p \to q) \land (q \to r)) \to (p \to r)$
析取三段论	Disjunctive Syllogism	$(\neg p \land (p \lor q)) \to q$
附加	Addition	$p \to (p \lor q)$
化简	Simplification	$(p \land q) \to p$
合取	Conjunction	$((p) \land (q)) \to (p \land q)$
消解	Resolution	$((\neg p \lor r) \land (p \lor q)) \to (q \lor r)$
全称实例	Universal Instantiation	$\forall x P(x) \to P(c)$
全称引入	Universal Generalization	$P(c)$ for any $c \to \forall x P(x)$
存在实例	Existential Instantiation	$\exists x P(x) \to P(c)$ for some c
存在引入	Existential Generalization	$P(c)$ for some $c \to \exists c P(c)$

例 (p26)

- ❑ "A student in this class has not read the book."
- ❑ "Everyone in this class passed the first exam."
- ❑ Conclusion: "Someone who passed the first exam has not read the book."

中文名	英文名	推理规则
肯定前件	Modus Ponens	$(p \land (p \to q)) \to q$
否定后件	Modus Tollens	$(\neg q \land (p \to q)) \to \neg p$
假言三段论	Hypothetical Syllogism	$((p \to q) \land (q \to r)) \to (p \to r)$
析取三段论	Disjunctive Syllogism	$(\neg p \land (p \lor q)) \to q$
附加	Addition	$p \to (p \lor q)$
化简	Simplification	$(p \land q) \to p$
合取	Conjunction	$((p) \land (q)) \to (p \land q)$
消解	Resolution	$((\neg p \lor r) \land (p \lor q)) \to (q \lor r)$
全称实例	Universal Instantiation	$\forall x P(x) \to P(c)$
全称引入	Universal Generalization	$P(c)$ for any $c \to \forall x P(x)$
存在实例	Existential Instantiation	$\exists x P(x) \to P(c)$ for some c
存在引入	Existential Generalization	$P(c)$ for some $c \to \exists c P(c)$

大纲

- 推理规则
  - 命题逻辑推理
  - 谓词逻辑推理
- 证明方法 (1.7-1.8)
  - 基本概念
  - 直接与间接证明
  - 分情况讨论
  - 存在性证明
  - 任意性证明
  - 应用与猜想

基本概念

- 证明 (proof)
  - 是有效的论证 (valid argument)
  - 用于建立目标语句的正确性

- 推理 vs 证明
  - 推理：每一步都来自推理规则
    - 严谨但复杂，可用于计算机自动证明
  - 证明：可跳步骤，推理规则不显示写明
    - 可读性高，常用于数学、计算机科学中

基本概念

- 原理 (axiom)
  - 默认正确的语句，通常无法被证明
  - 如：过直线外一点，有且仅有一条直线与已知直线平行

基本概念

- 原理 (axiom)
  - 默认正确的语句，通常无法被证明
- 引理 (lemma)
  - 可被证明，用于辅助定理证明
- 定理 (theorem)
  - 可被证明
- 推论 (corollary)
  - 可被证明，从定理可以直接得出

基本概念

- 原理 (axiom)
  - 默认正确的语句，通常无法被证明
- 引理 (lemma)
  - 可被证明，用于辅助定理证明
- 定理 (theorem)
  - 可被证明
- 推论 (corollary)
  - 可被证明，从定理可以直接得出
- 猜想 (conjecture)
  - 尚未证明或证伪的语句，倾向于认为正确

大纲

- 推理规则
  - 命题逻辑推理
  - 谓词逻辑推理
- 证明方法 (1.7-1.8)
  - 基本概念
  - 直接与间接证明
  - 分情况讨论
  - 存在性证明
  - 任意性证明
  - 应用与猜想

直接证明

- 目标：证明 $p \rightarrow q$
- 直接证明 (direct proof)
  - 假设 p 为真
  - 使用原理和推理规则
  - 证明 q 为真

直接证明

- 目标：证明 $p \to q$

- 直接证明 (direct proof)
  - 假设 p 为真
  - 使用原理和推理规则
  - 证明 q 为真

  - 平凡证明 (trivial proof)：知道q为真
  - 空证明 (vacuous proof)：知道p为假

直接证明：例

- Prove that if n is an odd integer, then n^2 is odd.

间接证明

- 目标：证明 $p \to q$

- 反证法 (proof by contraposition)
  - 证明 $\neg q \to \neg p$

间接证明

- 目标：证明 $p \rightarrow q$

- 反证法 (proof by contraposition)
  - 证明 $\neg q \rightarrow \neg p$

- 归谬证明发 (proof by contradiction)
  - 假设$\neg q$，推出矛盾
  - 反证法中$\neg p \land p$是一种矛盾

间接证明：例

- Prove that if n is an integer and $3n + 2$ is odd, then n is odd.

间接证明：例

- Prove that $\sqrt{2}$ is irrational.

- Irrational number: 无理数

大纲

- ❑ 推理规则
  - ❑ 命题逻辑推理
  - ❑ 谓词逻辑推理
- ❑ 证明方法 (1.7-1.8)
  - ❑ 基本概念
  - ❑ 直接与间接证明
  - ❑ 分情况讨论
  - ❑ 存在性证明
  - ❑ 任意性证明
  - ❑ 应用与猜想

分情况讨论

- 穷举证明法 (exhaustive proof)
  - 对每个对象都证明结论成立
  - 适用于有限对象

分情况讨论：例

- If n is a positive integer and n<5, prove that $(n+1)^3 \geq 3^n$.

分情况讨论

- 穷举证明法 (exhaustive proof)
  - 适用于有限对象
  - 对每个对象都证明结论成立

- 分情况讨论 (proof by cases)
  - 将对象进行分组
  - 对每组对象证明结论成立

$$
\begin{aligned}
&[(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q] \leftrightarrow \\
&\qquad [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)]
\end{aligned}
$$

分情况讨论：例

- Let $a @ b = \max\{a, b\}$.
- Show that for all real numbers a, b, c

$$(a @ b) @ c = a @ (b @ c)$$

分情况讨论

- 穷举证明法 (exhaustive proof)
  - 适用于有限对象
  - 对每个对象都证明结论成立
- 分情况讨论 (proof by cases)
  - 将对象进行分组
  - 对每组对象证明结论成立
- 不失一般性 (without loss of generality)
  - 当情况间有对称性时，可以只讨论一次

分情况讨论：不失一般性

- Show that if x and y are integers and both $x \cdot y$ and $x+y$ are even, then both x and y are even.

大纲

- 推理规则
  - 命题逻辑推理
  - 谓词逻辑推理
- 证明方法 (1.7-1.8)
  - 基本概念
  - 直接与间接证明
  - 分情况讨论
  - 存在性证明
  - 任意性证明
  - 应用与猜想

存在性证明

- 存在性证明 (existence proof)
  - 目标：证明 $\exists x P(x)$

存在性证明

- 存在性证明 (existence proof)
  - 目标：证明 $\exists x P(x)$

  - 构造性证明 (constructive proof)
    - 构造c，使得P(c)为真

例

- Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.

- $1729 = 10^3 + 9^3 = 12^3 + 1^3$

存在性证明

- 存在性证明 (existence proof)
  - 目标：证明 $\exists x P(x)$
- 构造性证明 (constructive proof)
  - 构造c，使得P(c)为真
- 非构造性证明 (nonconstructive proof)
  - 假设不存在c满足P(c)，推导矛盾

例

- Show that there exist irrational numbers x and y such that x^y is rational.

反例

- 反例 (counterexample)
  - 通过找到c使得P(c)为假，以证伪 $\forall x P(x)$

反例

- 反例 (counterexample)
  - 通过找到c使得P(c)为假，以证伪 $\forall x P(x)$

- 例
  - Every positive integer is the sum of the squares of 3 integers.
  - 反例：7

唯一性证明

- 唯一性证明 (uniqueness proof)
  - 目标：$\exists! x\, P(x)$

唯一性证明

- 唯一性证明 (uniqueness proof)
  - 目标：$\exists! x\, P(x)$
  - 存在性 (existence)
    - 构造性或非构造性证明

唯一性证明

- 唯一性证明 (uniqueness proof)
  - 目标：$\exists! x\, P(x)$
  - 存在性 (existence)
    - 构造性或非构造性证明
  - 唯一性 (uniqueness)
    - 若P(a)和P(b)均为真，则a=b

例

- Show that if a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

大纲

- ❑ 推理规则
  - ❑ 命题逻辑推理
  - ❑ 谓词逻辑推理
- ❑ 证明方法 (1.7-1.8)
  - ❑ 基本概念
  - ❑ 直接与间接证明
  - ❑ 分情况讨论
  - ❑ 存在性证明
  - ❑ 任意性证明
  - ❑ 应用与猜想

任意性证明

- 任意性证明
  - 目标：$\forall x P(x)$
  - 取定义域U中任意元素c
  - 证明P(c)为真
  - 根据全称引入完成证明

例

- Prove that:

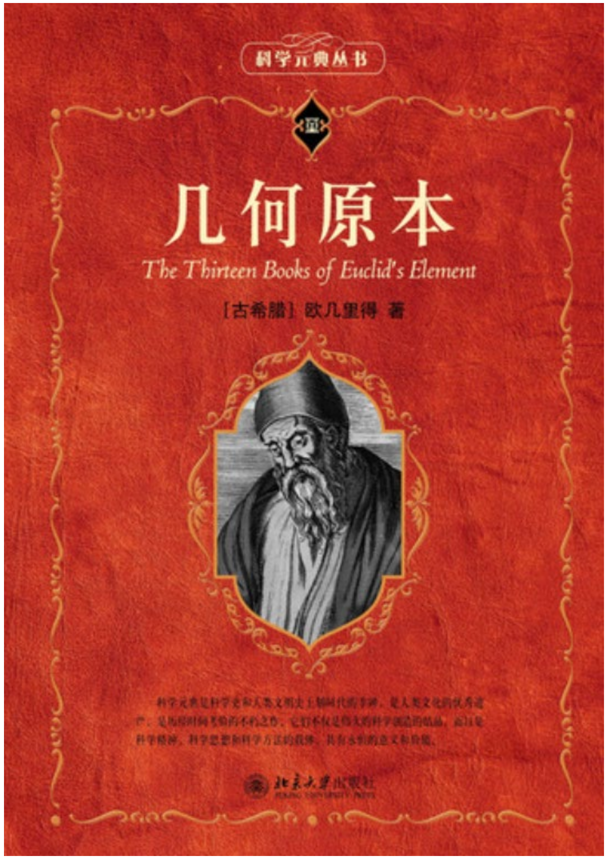
  an integer x is even if and only if x^2 is even.

大纲

- ❑ 推理规则
  - ❑ 命题逻辑推理
  - ❑ 谓词逻辑推理
- ❑ 证明方法 (1.7-1.8)
  - ❑ 基本概念
  - ❑ 直接与间接证明
  - ❑ 分情况讨论
  - ❑ 存在性证明
  - ❑ 任意性证明
  - ❑ 应用与猜想

几何原本的形式化证明

- 命题15
  - 两直线相交，对顶角相等
- 公理化系统
  - 希尔伯特公理系统
  - 塔斯基初等几何系统



开放问题

- 开放问题 (open problem)
  - 是否正确尚无定论的语句

- 费马大定理
  - $x^n + y^n = z^n$在$n \geq 3$时无非零解
  - Andrew Wiles在1995年发表了证明

- 考拉兹猜想 ($3x+1$猜想)
  - 任何正整数经过f的迭代，均会得到1

$$f(n) = \begin{cases} n/2 & \text{if } n \equiv 0 \\ 3n+1 & \text{if } n \equiv 1 \end{cases} \pmod{2}.$$

- NP $\neq$ P
  - 广泛用于现代计算机理论

更多证明方法

- 数学归纳法
  - 证明结论对可数集成立，如$\mathbb{N}$、$\mathbb{Z}^n$等
- 结构归纳法
  - 证明结论对一类结构成立，如列表、树等
- 康托对角论证法
  - 证明实数集不可数
- 组合证明法
  - 证明组合恒等式、握手定理等
- …………

拓展：不完备性

- 如果人类有
  - 足够多的证明方法
  - 足够多的天才
- 是否能证明所有结论和猜想？

- 哥德尔不完备性第一定理
  - 任意一个包含谓词逻辑与初等算术的形式系统，都存在一个命题，它在这个系统中既不能被证明为真，也不能被证明为否。

拓展：不完备性

- https://www.bilibili.com/video/BV19u4y1D7GT/?spm_id_from=333.337.search-card.all.click&vd_source=58d536aafbdced4f5e20033168c26ed7
- 9:40 到 23:40

总结

- 推理规则
- 证明方法
  - 直接
  - 反证
  - 讨论
  - 存在
  - 任意

中文名	英文名	推理规则
肯定前件	Modus Ponens	$(p \wedge (p \to q)) \to q$
否定后件	Modus Tollens	$(\neg q \wedge (p \to q)) \to \neg p$
假言三段论	Hypothetical Syllogism	$((p \to q) \wedge (q \to r)) \to (p \to r)$
析取三段论	Disjunctive Syllogism	$(\neg p \wedge (p \vee q)) \to q$
附加	Addition	$p \to (p \vee q)$
化简	Simplification	$(p \wedge q) \to p$
合取	Conjunction	$((p) \wedge (q)) \to (p \wedge q)$
消解	Resolution	$((\neg p \vee r) \wedge (p \vee q)) \to (q \vee r)$
全称实例	Universal Instantiation	$\forall x P(x) \to P(c)$
全称引入	Universal Generalization	$P(c)$ for any $c \to \forall x P(x)$
存在实例	Existential Instantiation	$\exists x P(x) \to P(c)$ for some c
存在引入	Existential Generalization	$P(c)$ for some $c \to \exists c P(c)$