# 无限集合初步

## 基本约定

**约定2.1:** 以下是一些常用的集合:

- $\mathbb{N}$ 是自然数集合
- $\mathbb{Z}$ 是整数集合
- $\mathbb{Q}$ 是有理数集合
- $\mathbb{R}$ 是实数集合

□

## 集合论性质

**事实2.1(集合论性质)**
在集合论中，一个核心概念是无限，是理论研究的工具，在计算机科学中有广泛应用.
全部

- 无限集合
  集合论中的无限是 Cantor严格定义，是数学领域内第一次独立于古希腊数学的创造.

□

- 公理
  - 外延公理
  - 空集公理
  - 偶对公理
  - 并集公理
  - 子集公理
  - 幂集公理
  - 无穷公理
  - 替换公理

- 正规公理
- 选择公理

□

- ZF 与 ZFC
  - ZF: 前 $9$ 条公理的集合.
  - ZFC: 全部 $10$ 条公理.

□

□

## 映射

**定义2.1(单射,满射,双射)**
假设 $f$ 是集合 $A$ 到 $B$ 的函数:

- $f$ 是单射: $\forall\ xy \in A(f(x)=f(y) \to x=y)$
- $f$ 是满射: $\forall\ y \in B \exists\ x \in A(f(x)=y)$
- $f$ 是双射: $f$ 是单射且 $f$ 是满射

□

## 单射与满射之间的关系

**定理2.1:** 假设集合 $A, B$ 都不是空集. 若存在 $A$ 到 $B$ 的满射, 则存在 $B$ 到 $A$ 的单射.
**定理2.2:** 假设集合 $A, B$ 都不是空集. 若存在 $A$ 到 $B$ 的单射, 则存在 $B$ 到 $A$ 的满射.

□

## 等势

**定义2.2(等势)** 给定集合 $A,B$ .

- 若存在从 $A$ 到 $B$ 的单射, 则称 $A$ 的势小于等于 $B$ 的势.
  记为 $A\preceq B$ , $B\succeq A$ .
- 若存在从 $A$ 到 $B$ 的双射, 则称 $A$ 与 $B$ 等势, 也称为有相同的基数.
  记为 $A\sim B$ .
- 若 $A\preceq B$ 且 $A\not\sim B$ , 则记为 $A\prec B$ , $B\succ A$ .

※

□

## 基数

**事实2.2(基数):** 存在一类集合, 它们互不等势, 任意一个集合都与这类集合中的某一个等势, 这些集合可以列举为:

$$0,1,2,\cdots,\aleph_0,\aleph_1,\aleph_2,\cdots,\aleph_\omega,\aleph_{\omega+1},\cdots,\aleph_{\omega^2},\cdots,\aleph_{\aleph_0},\cdots$$

这类集合的每一个称为基数.

若集合 $A$ 与某个基数 $\lambda$ 等势, 则称 $A$ 的势是 $\lambda$ 、元素个数是 $\lambda$ , 记为 $|A|=\lambda$ .

假设 $n$ 是自然数, 当集合 $A$ 的元素个数为 $n$ 时,

$$A\sim n.$$

□

## 等势关系的基本性质

**定理2.3(传递性)** 对于集合 $A,B,C$ , 若 $A\preceq B$ 且 $B\preceq C$ , 则 $A\preceq C$ .

**定理2.4** 对于集合 $A, B, C$，若 $A \sim B$ 且 $B \sim C$，则 $A \sim C$ .

**定理2.5** 对于集合 $A, B, C, D$，若 $A \preceq B$，$C \sim A$ 且 $B \sim D$，则 $C \preceq D$ .

**定理2.6** 对于集合 $A, B, C, D$，假设 $A \sim B$ 且 $C \sim D$，则

$$A \times C \sim B \times D, \quad 2^A \sim 2^B.$$

□

## Schröder-Bernstein 定理

**定理2.7:** 若 $A \preceq B, B \preceq A$，则 $A \sim B$ .

※

□

## 应用

**定理2.8:** $(0,1) \sim \mathbb{R}$ .

**证明:** 以下构造从 $\mathbb{R}$ 到 $[0,1)$ 的映射 $f$ . 定义 $f(0)=0$，而对于每个非 $0$ 实数 $x$，按照以下方式定义 $f(x)$ :

如下定义整数 $m=m_x, n=n_x, v_i=v_i^x$ :

. 若 $x<0$ 则 $m=0$ ， 否则 $m=1$
. $n$ 是 $|x|$ 的整数部分
. “$0.v_0, v_1, v_2, \cdots$ ” 是 $x-n$ 的二进制表达式

以三进制小数形式表示 $(0,1)$ 内的实数. 定义 $f(x)$ 为以下形式的数:

$$0.m\underbrace{22\cdots 2}_{n+1\text{ 个 }2}v_0v_1v_2\cdots.$$

$f$ 是一个单射, 所以 $\mathbb{R}\preceq[0,1)$ . 又因为 $[0,1)\preceq\mathbb{R}$ , 所以

$$[0,1)\sim\mathbb{R},$$

$$(0,1)\sim\mathbb{R}.$$

□

## 无限集合

**定义2.3(有限的,可数,可数无限,不可数)** 给定集合 $A$ :

- 若存在 $A$ 到 $\mathbb{N}$ 的单射, 则称 $A$ 为可数的.
  $A$ 是可数的当且仅当 $A\preceq\mathbb{N}$ .
- 若存在 $A$ 到 $\mathbb{N}$ 的双射, 则称 $A$ 为可数无限的.
  可数无限集合的基数记为 $\aleph_0$ .
- 若 $A$ 与某个自然数是等势的, 则称 $A$ 为有限的.
- 若 $A$ 不是可数的, 则称 $A$ 为不可数的.
  第一个不可数的基数记为 $\aleph_1$ .
- 若 $A$ 不是有限的, 则称 $A$ 为无限的.

※

□

□

## Cantor 定理

**定理2.12:** 对任意的集合 $A$ , 都有 $A \prec 2^A$ .

**证明:** 可以假设 $A$ 不是空集. 由以下两个事实可得上述结论.

- $A \preceq 2^A$ .

  这是因为存在 $A$ 到 $2^A$ 的单射:

$$\begin{aligned} f: \ & A \to 2^A. \\ & x \mapsto \{x\}. \end{aligned}$$

- $A \not\sim 2^A$ . 事实上,不存在 $A$ 到 $2^A$ 的满射.

  若存在这样的映射 $g: A \to 2^A$ , 则可以定义以下集合

$$B = \{x \in A \mid x \notin g(x)\},$$

  是 $A$ 的子集, 属于 $2^A$ . 因为 $g$ 是满射, 所以存在 $x \in A$ 使得 $B = g(x)$ .
  - 若 $x \in g(x)$ , 则根据 $B$ 的定义可知 $x \notin B$ , 即 $x \notin g(x)$ .
  - 若 $x \notin g(x)$ , 则根据 $B$ 的定义可知 $x \in B$ , 即 $x \in g(x)$ .

  上述矛盾表明不存在 $A$ 到 $2^A$ 的满射.

由上述分析可知 $A \prec 2^A$ .

□

**推论2.2:** 对任意集合 $A$ , 有

$$A \prec 2^A \prec 2^{2^A} \prec 2^{2^{2^A}} \prec \cdots,$$

因而可以得到势充分大的集合; 若 $A$ 是可数集, 则上述集合中除 $A$ 之外都是不可数的.

□

## 自然数集合的一些乘积

- **定理2.13:** $\mathbb{N} \sim \mathbb{N} \times \mathbb{N}$ .
- **推论2.3:** $\mathbb{N} \sim \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ , $\mathbb{N} \sim \mathbb{N} \times \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ , ⋯
- **推论2.4**: $\mathbb{N} \sim \mathbb{Q}$ .
- **定理2.14:** $\mathbb{N}^{\omega}$ 是不可数的.
- **定理2.15:** $\mathbb{N}^{\omega} \sim 2^{\mathbb{N}}$ .
- **推论2.5**: 有限个可数集合的卡氏积是可数的.
- **推论2.6:** 可数个可数集合的并集是可数的.

□

## 一些可数的字符串集合

- **定理2.16:** 有限符号表上有限长字符串集合是可数的.
- **推论2.7:** 可数的一阶语言的公式的集合是可数的.
- **推论2.8:** 自然语言的语句集合是可数的.

□

## 代数数与超越数

**定义2.4(代数数,超越数)**

- 满足整系数一元多项式方程的复数称为代数数.
  一个复数若是代数数且是实数,则称它为实代数数.
- 不是代数数的复数称为超越数.
  一个复数若是超越数且是实数,则称它为实超越数.

**例2.2:**

- 有理数 $\frac{m}{n}$ 是代数数.
- $\sqrt{2}$ 是代数数.
- $i$ 是代数数.
- 实数$1+\frac{1}{10^{1!}}+\frac{1}{10^{2!}}+\frac{1}{10^{3!}}+\cdots$ 是实超越数.
- $\pi$ 是实超越数.

**定理2.17:**存在实超越数.

**证明:** 有以下事实:

- 整系数一元 $1$ 次多项式的集合$S_1$ 是可数的.
- 整系数一元 $2$ 次多项式的集合$S_2$ 是可数的.
- 整系数一元 $3$ 次多项式的集合 $S_3$ 是可数的.
- $\cdots$

所以整系数一元多项式的集合 $S$:

$$S_1 \cup S_2 \cup S_3 \cup \cdots$$

是可数的. 每个多项式 $f$ 最多只有有限个根, 它的实根的集合 $\{r \in \mathbb{R} \mid f(r)=0\}$ 是可数的. 所有整系数多项式的实根可以表示为以下集合

$$\cup_{f \in S}\{r \in \mathbb{R} \mid f(r)=0\}.$$

所以实代数数的集合是可数的. 但是实数集合是不可数的, 所以一定存在实超越数.

□

讨论:
如何保证 Cantor 证明时正确的? 在常规数学公理基础上添加一些公理,

这是否保证相容呢？ 若前提矛盾，则无法保证证明正确． 正确性是以公理化方法保证的， 这是不可证的， 已经证明是不可证的．

□

□

## 可定义的实数

**定义2.5(可定义的实数)** 假设 $r$ 是一个实数, 若存在形式语言的仅包含一个自由变元 $x$ 的公式$\phi$ , 使得在实数范围内有

- $\phi_r^x$ 成立
- 若 $\phi_s^x$ 成立， 则 $s=r$

则称 $r$ 是可定义的实数, $r$ 由 $\phi$ 定义, $\phi$ 是定义$r$ 的公式.

**例2.3:**

- $\sqrt{2}$ 是可定义的.
- $\pi$ 是可定义的.
- $e$ 是可定义的.

※

□

□

## 可计算函数

**定义2.7(可计算函数)** 假设一个程序$P$ 在一台计算机上运行, 接收输入字符串 $x$ , 记 $P(x)$ 为相应的输出. 若不停机则记输出为 $\infty$ .
给定一个接收自然数输入的程序, 以下函数

$$\begin{aligned} f:\ \mathbb{N} &\rightarrow \mathbb{N}\cup\{\infty\} \\ n &\mapsto P(n) \end{aligned}$$

称为可计算的函数.

**定理2.20:**存在不可计算函数.

**证明:** 因为

- $\mathbb{N}$ 到 $\mathbb{N}\cup\{\infty\}$ 的函数有不可数个
- 可计算函数只有可数个

所以存在不可计算的函数.

□

□

# 公理集合论初步

给定一阶语言 $\mathscr{L}=\{\in\}$ 及该语言的一个模型 $<V,\in>$.

上述模型的元素称为集合, 二元谓词符号 $\in$ 表示属于关系.

集合的存在性是由公理确保的, 且不区分集合与元素.

**集合论有 10 条公理.**

- 外延公理
- 空集公理
- 偶对公理
- 并集公理
- 子集公理
- 幂集公理
- 无穷公理
- 替换公理
- 正规公理
- 选择公理

□

在集合论语言之下, 在一个模型里, 有一些可定义的元素、谓词、函数. 这里的 $a$ 及 $b$ 是两个集合.

- 空集
  $\emptyset$ 表示空集, 它满足以下性质:

$$\neg\exists x(x\in\emptyset).$$

□

- 包含于
  $\subseteq$ 表示包含关系:

$$a\subseteq b \text{ 当且仅当 } \forall x(x\in a\to x\in b).$$

  同时

$$a\supseteq b \text{ 当且仅当 } \forall x(x\in b\to x\in a).$$

□

- 二元组
  $<a,b>$表示二元组, 是指以下集合:

$$\{\{a\},\{a,b\}\}.$$

□

- 交集
  $a\cap b$ 表示交集:

$$a\cap b=\{x|x\in a\wedge x\in b\}.$$

□

- 差集
  $a-b$ 表示差集:

$$a-b=\{x|x\in a\wedge x\notin b\}.$$

□

- 函数
  func($a$) 表示 $a$ 是一个函数:

$$\phi_1\wedge\phi_2.$$

  其中
  - $\phi_1$ 是公式 $\forall x(x\in a\to\exists uv(x=<u,v>))$.
  - $\phi_2$ 是公式 $\forall uvw(<u,v>\in a\wedge<u,w>\in a\to v=w)$.

□

- 定义域
  dom($a$) 表示函数 $a$ 的定义域:

$$\mathrm{dom}(a)=\{u|\exists v(<u,v>\in a)\}.$$

□

- 值域
  ran($a$) 表示一个函数 $a$ 的值域:

$$\mathrm{ran}(a)=\{v|\exists u(<u,v>\in a)\}.$$

□

- 象
  若 $a$ 是一个函数, $b\in\mathrm{dom}(a)$ , 则 $a(b)$ 表示满足以下条件的集合:

$$<a,a(b)>\in a.$$

□

- 卡氏积
  对于集合 $a$ 及 $b$ , 它们的卡氏积 $a\times b$ 是以下集合:

$$\{<u,v>|u\in a\wedge v\in b\}.$$

□

- 自然数
  自然数:
  - $\emptyset$ 是 $0$ .
  - $\{0\}$ 是 $1$ .

- $\{0,1\}$ 是 $2$ .
- $\{0,1,2\}$ 是 $3$ .
- …

□

公理集合论是数学研究的基础.

外延公理

$$\forall xy(\forall z(z\in x\leftrightarrow z\in y)\to x=y)$$

**直观解释是**: 两个集合若有相同的元素, 则这两个集合是相等的.

□

空集公理

$$\exists x\forall y(y\notin x).$$

记上述 $x$ 为 $\emptyset$.
上述公理保证空集是存在的, 根据外延公理, 可知空集是唯一的:

若 $\emptyset'$ 是另一个空集, 则从它满足 $\forall y(y\notin\emptyset')$ 可知

$$\forall z(z\in\emptyset\leftrightarrow z\in\emptyset'),$$

所以 $\emptyset=\emptyset'$.

□

偶对公理

$$\forall xy\exists u\forall z(z\in u\leftrightarrow z=x\vee z=y).$$

对于集合 $x,y$ , 记相应的 $u$ 为 $\{x,y\}$. 由此可知: 对于集合 $x,y$ 存在一个仅以它们为元素的集合 $\{x,y\}$ .

**事实:** 此公理与下面的并集公理可以保证存在任意的有限集合

假设 $x,y,z$ 是集合, 则存在集合 $\{x,y,z\}$ :

$$\{x,y,z\}=\{x,y\}\cup\{z,z\}.$$

□

并集公理

$$\forall x\exists u\forall y(y\in u\leftrightarrow(\exists z(z\in x\wedge y\in z))).$$

记上述 $u$ 为 $\cup x$. 由定义可知, 对任意的 $y\in x$ , 有 $y\subseteq\cup x$ .

一般意义下的 $A\cup B$ 在严格意义下被写为 $\cup\{A,B\}$ .
而

$$A_0\cup A_1\cup A_2\cup\cdots$$

被严格地写为$\cup\{A_0,A_1,A_2,\cdots\}$ .

**例:** 若 $a,b,c$ 是集合, 则 $\cup\{\{a\},\{b,c\}\}=\{a,b,c\}$.

**例:** 若 $a,b,c,d$ 是四个不同的集合, 则 $\{<a,b>,<c,d>\}$ 是一个函数 $f$ . 这时,根据定义可知:

$$f=\{\{\{a\},\{a,b\}\},\{\{c\},\{c,d\}\}\}.$$

所以

$$\cup f=\{\{a\},\{a,b\},\{c\},\{c,d\}\},$$

$$\cup\cup f=\{a,a,b,c,c,d\}.$$

可见

$$\cup\cup f\supseteq\mathrm{dom}(f),\cup\cup f\supseteq\mathrm{ran}(f).$$

$\cup\emptyset=\emptyset$ .
根据定义可知

$$\forall x(x\in\cup\emptyset\leftrightarrow\exists y(y\in\emptyset\wedge x\in y)).$$

但是 $\exists y(y\in\emptyset\wedge x\in y)$ 是永假的, 所以 $\cup\emptyset=\emptyset$ .

□

$\cup\{\emptyset\}=\emptyset$ .
根据定义可知

$$\forall x(x\in\cup\{\emptyset\}\leftrightarrow\exists y(y\in\{\emptyset\}\wedge x\in y)).$$

但是 $\exists y(y\in\{\emptyset\}\wedge x\in y)$ 是永假的, 所以 $\cup\{\emptyset\}=\emptyset$ .

□

**函数的并.**

**函数集合的并.**

定义集合 $x$ 的交集$v$ 为满足以下条件的集合:

$$\forall z(z\in v\leftrightarrow\forall y(y\in x\rightarrow z\in x)).$$

被记为 $v=\cap x$ . 而

$$A_0 \cap A_1 \cap A_2 \cap \cdots$$

被严格地写为 $\cap\{A_0, A_1, A_2, \cdots\}$ .

---

**$\cap\emptyset$ 是不存在的.**

□

子集公理
假设 $\phi$ 是$\mathscr{L}$ – 公式， 仅出现自由变元 $x_1, \cdots, x_n, z$ , 不出现变元 $y$ ,则

$$\forall x_1, \cdots, x_n \forall x \exists y \forall z (z \in y \leftrightarrow z \in x \wedge \phi).$$

对于给定的 $x_1, \cdots, x_n, z$ , 这样定义的集合 $y$ 被记为

$$y = \{z \in x \mid \phi\}.$$

这样定义的集合 $y$ 是 $x$ 的子集, 所以该公理被称为是子集公理.

□

幂集公理

$$\forall x \exists y (\forall z (z \in y \leftrightarrow z \subseteq x)).$$

对于给定的 $x$ , 相应的 $y$ 称为 $x$ 的幂集, 记为 $\rho(x)$ , 也记为 $2^x$ .

□

无穷公理

$$\exists x (\emptyset \in x \wedge (\forall y (y \in x \rightarrow y^+ \in x))),$$

其中 $y^+$ 表示集合 $y \cup \{y\}$ .
该公理用于定义自然数集合.

□

替换公理
假设 $\phi$ 是 $\mathscr{L}$ – 公式， 仅出现自由变元 $x_1, \cdots, x_n, u, z$ , 不出现变元 $y$ , 则

$$\forall x_1, \cdots, x_n \forall x (\psi \rightarrow \exists y \forall z (z \in y \leftrightarrow \exists u \in x \phi[u, z])),$$

其中 $\psi$是以下公式:

$$\forall u \in x \forall z_1 z_2 (\phi[u, z_1] \wedge \phi[u, z_2] \rightarrow z_1 = z_2).$$

这里所定义的集合 $y$ 也被写为

$$\{z \mid \exists u(u \in x \wedge \phi[u,z])\}.$$

该公理可以保证一类集合的存在性.

□

## 正规公理

$$\forall x(x \neq \emptyset \to \exists y(y \in x \wedge y \cap x = \emptyset)).$$

这条公理保证不存在这样的集合：

$$x = \{x\}.$$

这用于证明集合论模型的相关性质.

□

## 选择公理

$$\forall x(x \neq \emptyset \to \exists y(\phi_1 \wedge \phi_2)).$$

其中

- $\phi_1$ 是

$$\mathrm{func}(y) \wedge \mathrm{dom}(y) = \rho(x) - \{\emptyset\} \wedge \mathrm{ran}(y) \subseteq x,$$

定义一个函数使得有给定的定义域及值域.
- $\phi_2$ 是

$$\forall z(z \subseteq x \to y(z) \in z),$$

指定了取值特点.

该公理保证存在选择函数:
假设 $a$ 是一个非空集合，则存在一个选择函数

$$\begin{aligned} f:\ 2^a - \{\emptyset\} &\to a, \\ x &\mapsto f(x). \end{aligned}$$

使得 $f(x) \in x$ .

- 1940 年 Gödel 证明 $\mathrm{ZF} \nvdash \neg$ AC.
- 1963 年 Cohen 证明 $\mathrm{ZF} \nvdash$ AC.

该公理可以保证一类集合的存在性.

□

# 自然数逻辑理论

## 归纳集

### 定义

**定义1(归纳集):** 满足以下两个条件的集合 $u$ 称为归纳集:

- $\emptyset \in u$ .
- 若 $a \in u$ , 则 $a \cup \{a\} \in u$ .

### 记号

集合 $a \cup \{a\}$ 记为 $a^+$ . 因而

- $0^+ = 0 \cup \{0\} = 1$
- $1^+ = 1 \cup \{1\} = \{0, 1\} = 2$
- $2^+ = 2 \cup \{2\} = \{0, 1, 2\} = 3$
- …

### 公式

以 $\mathrm{Ind}(x)$ 表示以下公式:

$$\emptyset \in x \wedge \forall y (y \in x \to y^+ \in x).$$

则集合 $u$ 是归纳集当且仅当 $\mathrm{Ind}[u]$ 成立.

### 性质

**归纳集有以下性质:**

- 两个归纳集的并集 及交集还是归纳集.
- 若存在集合

  $$\{0, 1, 2, \cdots\}$$

  则它是一个 归纳集.
- 无穷公理保证这样的无限集合是存在的.

  这样的集合不唯一 .
- 若 $u$ 是归纳集, 则它是 无限集.

# 自然数集合与自然数

## 定义

**定义2(自然数集合):** 最小的归纳集 $\omega$ ,即满足以下公式

$$\text{Ind}[\omega]\wedge\forall x(\text{Ind}[x]\to\omega\subseteq x).$$

的 集合称为自然数集合.

## 性质

根据定义可知

$$0,1,2,\cdots\in\omega.$$

自然数集合的元素称为 自然数.

## 应用

整数集合、有理数集合、实数集合、复数集合等的存在性可以由无穷公理等保证.

## 例子

$\cup\omega=\omega.$

**证明**: 考虑以下两个情况:

- 对于每个 $n\in\omega$ , 因为 $n\in n^{+},n^{+}\in\omega$ , 所以 $n\in\cup\omega$ .
- 若 $x\in\cup\omega$ , 则存在 $n\in\omega$ 使得 $x\in n$ , 必有 $x\in\omega$ .

根据外延公理,可知 $\cup\omega=\omega$. .

# 归纳法

**性质1(自然数的归纳法)**

假设 $u\subseteq\omega$ , 且满足

$$0\in u\wedge\forall x(x\in u\to x^{+}\in\omega),$$

则 $u=\omega$.

**证明**
这时的 $u$ 是一个归纳集合，又是 $\omega$ 的子集，所以等于 $\omega$ .

---

**推论**
假设 $\phi(x)$ 是集合论语言的一个语句, 包含一个自由变元 $x$, 且

$$\phi[0]\wedge\forall x(x\in\omega\wedge\phi[x]\rightarrow\phi[x^{+}])$$

成立, 则对任意的自然数 $n$ ,都有 $\phi[n]$ 成立.

---

**证明**
考虑集合

$$u=\{n\in\omega|\phi[n]\}.$$

根据子集公理, 可知它是集合, 还是 $\omega$ 的子集, 根据 $\phi$ 所满足的性质, 可知

$$0\in u\wedge\forall x(x\in u\rightarrow x^{+}\in\omega),$$

所以 $u=\omega$ , 即对任意的自然数 $n$ ,都有 $\phi[n]$ 成立.

---

例子
对于任意的 $n\in\omega$ , 有 $n^{+}\neq 0$ .
**证明**
考虑以下关于 $x$ 的公式 $\phi(x)$ :

$$\neg x^{+}=0.$$

- $\phi[0]$ 成立, 是因为 $0^{+}=\{0\}$ 不是空集.
- 若 $m\in\omega$ 且 $\phi[m]$ 成立, 则 $\phi[m^{+}]$ 必然成立, 是因为 $(m^{+})^{+}$ 不是空集.

所以 $\forall x\phi(x)$ 成立. 这就是需证明的.

例子
对于任意的 $m\in\omega, m\neq 0$ , 都存在 $n\in\omega$ , 使得 $n^{+}=m$ .
**证明**
考虑以下关于 $x$ 的公式 $\phi(x)$ :

$$\neg x=0\rightarrow\exists y(y\in\omega\wedge y^{+}=x).$$

- $\phi[0]$ 成立, 是因为 $\neg 0=0$ 是假的.
- 若 $m\in\omega$ 且 $\phi[m]$ 成立, 则 $\phi[m^+]$ 必然成立, 这是可取相应的 $y$ 为 $m$ .

所以 $\forall x\phi(x)$ 成立. 这就是需证明的.

## 递归定义

**定理2**

递归定义的合理性:

假设 $a$ 是 一个集合, $f$ 是一个函数, 则存在 一个函数 $r$ 满足:

- $\mathrm{dom}(r)=\omega$ .
- $r(0)=a$ .
- 对任意的自然数 $m$ , 都有 $r(m^+)=f(r(m))$ .

**证明**

#### 描述函数的公式

定义以下公式 $\theta(x,t)$:

$$(x=0\rightarrow t=\{<0,a>\})\wedge(x\neq 0\rightarrow\phi_1\wedge\phi_2).$$

其中

- $\phi_1$ 是: $\mathrm{func}(t)\wedge\mathrm{dom}(t)=x^+$ .
- $\phi_2$ 是: $\forall y(y\in\mathrm{dom}(t)\wedge y^+\in\mathrm{dom}(t)\rightarrow t(y^+)=f(t(y)))$ .

---

#### 第二坐标唯一性

以下证明:

对于每个 $m\in\omega$ 存在唯一的 $t$ , 使得 $\theta[m,t]$ . (*)

考虑以下关于 $x$ 的公式 $\psi(x)$ :

$$\exists t\theta[x,t]\wedge(\forall t_1t_2(\theta[x,t_1]\wedge\theta[x,t_2]\rightarrow t_1=t_2)).$$

. $\psi[0]$ 成立，这时相应的 $t$ 的函数只能是 $\{<0,a>\}$ .
. 若 $m\in\omega$ 且 $\psi[m]$ 成立，则相应于 $m$ 有唯一的函数 $t$ ，这时定义函数 $t'$ 为

$$t\cup\{<m^+,f(t(m))>\},$$

是 相应于 $m^+$ 的唯一函数，所以 $\psi[m^+]$ 成立.

由归纳法可知 (*) 成立.

#### 函数型公式

对于公式 $\phi(x,y)$

$$\exists\, t(\theta(x,t)\wedge y=t(x)),$$

根据上述证明可知

$$\forall\, x\exists\,!y(x\in\omega\rightarrow\phi(x,y)).$$

#### 定义函数

根据替换公理, 可知存在集合

$$\{y|\exists\, x(x\in\omega\wedge\phi(x,y))\}.$$

因而可定义以下函数 $r$

$$\{<x,y>|x\in\omega\wedge\phi(x,y)\}$$

即为所求的函数 $r$ .

## Peano 公理

假设集合 $\mathbb{N}$ 上可以定义一个一元函数 $s$ 使得

. $0\in\mathbb{N}$ .
. $\forall\, x(x\in\mathbb{N}\rightarrow s(x)\in\mathbb{N})$ .
. $\forall\, x\neg(s(x)=0)$ .
. $\forall\, xy(s(x)=s(y)\rightarrow x=y)$ .

- 对任意的 $A \subseteq \mathbb{N}$, 若 $0 \in u$, 且当 $n \in A$ 时, $s(n) \in A$, 则 .

则称 $\mathbb{N}$ 是自然数集合, $s$ 是 $\mathbb{N}$ 上的后继函数.

---

在 $\omega$ 上定义函数 $s$ 为

$$\begin{aligned} s:\ \omega &\to \omega \\ n &\mapsto n^{+} \end{aligned}$$

则此 $s$ 满足上述公理, 因而 $\omega$ 为 Peano 意义下的自然数集合.

全部

# 命题逻辑——两个推理系统

## 命题逻辑的推演系统(Hilbert 系统)

- 公理:
  - $A \to (B \to A)$.
  - $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$.
  - $(A \to B) \to (\neg B \to \neg A)$.
- 规则:

$$\frac{A, A \to B}{B}.$$

---

**推演序列:** 假设 $\Gamma$ 是公式集合, 公式序列 $< A_1, A_2, \cdots, A_n >$ 被称为 $\Gamma-$ 推演序列, 若对每个 $A_i$:

- 或者 $A_i \in \Gamma$;
- 或者 $A_i$ 是公理;
- 或者存在 $j, k < i$, 使得对 $A_j, A_k$ 应用证明规则之后可得 $A_i$.

**可证性:**

- 若存在一个$\Gamma-$ 推演序列, 它的最后一个公式是 $A$, 则称 $A$ 是 $\Gamma$ 可证的.
- $A$ 是 $\Gamma$可证的记为 $\Gamma \vdash A$.
- $\emptyset-$ 推演序列、 $\emptyset-$ 可证分别称为推演序列、可证.

---

**例:** $< A_1, A_2, A_3, A_4, A_5 >$是一个推演序列, 其中

- $A_1 : p \to ((p \to p) \to p)$.
- $A_2 : A_1 \to (A_4 \to (p \to p))$.
- $A_3 : A_4 \to (p \to p)$.
- $A_4 : p \to (p \to p)$.
- $A_5 : p \to p$.

所以 $\vdash p \to p$.

## 命题逻辑的推演系统(II)

- 公理:

$$A \vdash A.$$

- 规则:
  - $\dfrac{\Sigma \vdash A}{\Sigma, \Sigma' \vdash A}$. 单调性
  - $\dfrac{\Sigma, \neg A \vdash B \text{ 且 } \Sigma, \neg A \vdash \neg B}{\Sigma \vdash A}$. 反证法
  - $\dfrac{\Sigma \vdash A \text{ 且 } \Sigma \vdash A \to B}{\Sigma \vdash B}$. 三段论
  - $\dfrac{\Sigma, A \vdash B}{\Sigma \vdash A \to B}$. 演绎定理
  - $\dfrac{\Sigma \vdash A \wedge B}{\Sigma \vdash A}, \dfrac{\Sigma \vdash A \wedge B}{\Sigma \vdash B}$.
  - $\dfrac{\Sigma \vdash A \text{ 且 } \Sigma \vdash B}{\Sigma \vdash A \wedge B}$.
  - $\dfrac{\Sigma, A \vdash C \text{ 且 } \Sigma, B \vdash C}{\Sigma, A \vee B \vdash C}$.
  - $\dfrac{\Sigma \vdash A}{\Sigma \vdash A \vee B}, \dfrac{\Sigma \vdash A}{\Sigma \vdash B \vee A}$.
  - $\dfrac{\Sigma \vdash A \leftrightarrow B \text{ 且 } \Sigma \vdash A}{\Sigma \vdash B}, \dfrac{\Sigma \vdash A \leftrightarrow B \text{ 且 } \Sigma \vdash B}{\Sigma \vdash A}$.
  - $\dfrac{\Sigma, A \vdash B \text{ 且 } \Sigma, B \vdash A}{\Sigma \vdash A \leftrightarrow B}$.

其中$\Sigma, \Sigma'$ 是公式集合, $A, B, C$ 是公式.
上述规则中的公式

$$A, B, \neg A, \neg B, A \to B, A \wedge B, A \vee B, A \leftrightarrow B$$

称为相应规则的主公式.

---

**可证性:** 有限次应用公理及规则可以生成 $\Sigma \vdash A$ , 则称 $\Sigma \vdash A$ 成立.

**例:** 以下是一个推演过程:

- $A \vdash A$

- $\vdash A \to A$

---

**例:** 以下是一个推演过程:

- $\neg\neg A \vdash \neg\neg A$
- $\neg A, \neg\neg A \vdash \neg\neg A$
- $\neg A \vdash \neg A$
- $\neg A, \neg\neg A \vdash \neg A$
- $\neg\neg A \vdash A$

---

**紧致性**

给定公式集合 $\Sigma$ 及公式 $A$ , 若 $\Sigma \vdash A$ , 则存在有限的 $\Gamma \subseteq \Sigma$ 使得

$$\Gamma \vdash A.$$

证明

---

**协调性**

给定命题逻辑的公式集合 $\Sigma$ , 称:

- $\Sigma$ 是不协调的:
  存在命题逻辑公式 $A$ , 使得
  $$\Sigma \vdash A \text{ 且 } \Sigma \vdash \neg A.$$
- $\Sigma$ 是协调的:
  $\Sigma$ 不是不协调的.

---

**可满足**

- ---
  一个公式的真值
  假设 $v$ 是一个赋值, $A$ 是公式, 可以根据真值表定义 $v(A)=1$
  .
- ---
  公式集合的真值
  假设 $\Gamma$ 是一个公式集合, 定义 $v(\Gamma)=1$ 为
  $$\text{对每个 } A \in \Gamma, \text{ 都有 } v(A)=1.$$
- ---
  集合与公式
  假设 $\Gamma$ 是一个公式集合, $A$ 是公式, 定义 $\Gamma \vDash A$ 为

对任意的赋值 $\boldsymbol{v}$ ，当 $\boldsymbol{v}(\boldsymbol{\Gamma})=\mathbf{1}$ 时，$\boldsymbol{v}(\boldsymbol{A})=\mathbf{1}.$

## 可靠性与完备性

- 可靠性
  若 $\boldsymbol{\Sigma} \vdash \boldsymbol{A}$ ，则 $\boldsymbol{\Sigma} \vDash \boldsymbol{A}$ .
- 完备性
  若 $\boldsymbol{\Sigma} \vDash \boldsymbol{A}$ ，则 $\boldsymbol{\Sigma} \vdash \boldsymbol{A}$ .

全部

# 命题逻辑的完备性

**定理**(完备性):
在命题逻辑中, 假设 $A$ 是公式. 有以下结论:

$$若\ \vDash A\ ,\ 则\ \vdash A\ .$$

□

**证明**(完备性的证明):

---

假设$A$ 中仅出现命题变元 $p_1,p_2,\cdots,p_n$ . 假设 $v$ 是一个真值赋值.
定义文字 $L_{v,i}$:

$$L_{v,i}=\begin{cases} p_i, & 若\ v(p_i)=1, \\ \neg p_i, & 否则. \end{cases}$$

则有以下两个事实:

- 若 $v(A)=1$ 则 $L_{v,1},\cdots,L_{v,n}\vdash A$ .
- 若 $v(A)=0$ 则 $L_{v,1},\cdots,L_{v,n}\vdash\neg A$ .

---

对 $A$ 中包含的逻辑联结词的数量归纳, 可以证明上述结论.

- 若 $A$ 是命题变元, 则结论成立.
- 若 $A$ 是 $\neg B$ , 且上述结论对 $B$ 成立. 以下证明
  - 若 $v(A)=0$ 则 $L_{v,1},\cdots,L_{v,n}\vdash\neg A$ .
    当 $v(A)=0$ 时, 从 $A$ 是 $\neg B$ 可知 $v(B)=1$ . 根据归纳假设可知:
    $$L_{v,1},\cdots,L_{v,n}\vdash B\ .$$
    从 $B\vdash\neg\neg B$ 可知
    $$L_{v,1},\cdots,L_{v,n}\vdash\neg A\ .$$
  - 若 $v(A)=1$ 则 $L_{v,1},\cdots,L_{v,n}\vdash A$ . 同理可证.
- 同理, 当 $A$ 是 $B\to C$ 时, 上述结论成立.

---

进一步地, 若 $\Sigma$ 是公式集,$B$ , $C$ 是公式, 则:

$$\text{从 } \Sigma, B \vdash C \text{ 及 } \Sigma, \neg B \vdash C \text{ 可知 } \Sigma \vdash C \text{ .}$$

---

若 $A$ 是永真的, 则对任意的赋值 $v$ 都有 $v(A)=1$ .
所以对于由 $p_1, p_2, \cdots, p_n$ 生成的每个文字集合

$$\{L_{v,1}, \cdots, L_{v,n}\},$$

都有

$$L_{v,1}, \cdots, L_{v,n} \vdash A.$$

而对于赋值 $v$ , 考虑文字集合

$$\{L_{v,1}, \cdots, L_{v,n-1}\},$$

因为

$$L_{v,1}, \cdots, L_{v,n-1}, \quad p_n \vdash A,$$

$$L_{v,1}, \cdots, L_{v,n-1}, \neg p_n \vdash A,$$

所以 $L_{v,1}, \cdots, L_{v,n-1} \vdash A.$

---

由上述结论可知: 若 $A$ 是永真的, 则对任意的赋值 $v$ 都有:

$$\begin{aligned}
&L_{v,1}, L_{v,2} \cdots, L_{v,n-3}, L_{v,n-2} \vdash A, \\
&L_{v,1}, L_{v,2} \cdots, L_{v,n-3}, \vdash A, \\
&\cdots, \\
&L_{v,1}, L_{v,2} \vdash A, \\
&L_{v,1} \vdash A, \\
&\vdash A.
\end{aligned}$$

由此可知: 若 $A$ 是永真的, 则 $A$ 是可证的, 即 $\vdash A$ .

□

---

定理(完备性):
对任意的公式集合 $\Sigma$ 及公式 $A$ ,

$$\text{若 } \Sigma \vDash A \text{ , 则 } \Sigma \vdash A \text{ .}$$

□

**定义**(极大协调集合):
满足以下条件的公式集合 $\Sigma$ 被称为是极大协调的.

- $\Sigma$ 是协调的.
- 对任意的 $A \notin \Sigma$, 公式集合 $\Sigma \cup \{A\}$ 是不协调的.

□

**例子**(极大协调集合):
假设 $v$ 是一个赋值, 定义

$$\Sigma_v = \{A \mid v(A) = 1\}.$$

则 $\Sigma_v$ 是一个极大协调集合.

□

**定理**(推出与属于):
对任意的公式集合 $\Sigma$ 及公式 $A$, 若 $\Sigma$ 是极大协调集合, 则

$$A \in \Sigma \text{ 当且仅当 } \Sigma \vdash A.$$

□

**定理**(逻辑联结词与属于):
对任意的极大协调集合 $\Sigma$ 及公式 $A, B$, 有以下性质:

- $\neg A \in \Sigma$ 当且仅当 $A \notin \Sigma$.
- $A \wedge B \in \Sigma$ 当且仅当 $A \in \Sigma$ 并且 $B \in \Sigma$.
- $A \vee B \in \Sigma$ 当且仅当 $A \in \Sigma$ 或者 $B \in \Sigma$.
- $A \to B \in \Sigma$ 当且仅当 $A \in \Sigma$ 蕴涵 $B \in \Sigma$.
- $A \leftrightarrow B \in \Sigma$ 当且仅当 $A \in \Sigma$ 等价于 $B \in \Sigma$.

□

**定理**(极大协调集合与赋值):
若 $\Sigma$ 是极大协调集合, 定义赋值 $v$ 使得

$$v(p) = 1 \text{ 当且仅当 } p \in \Sigma.$$

则对任意的公式 $A$,

$$v(A)=1 \text{ 当且仅当 } A\in\Sigma .$$

□

定理(扩充定理):
假设 $\Sigma$ 是协调的公式集合, 则

存在极大协调集合 $\Sigma'$, 使得 $\Sigma\subseteq\Sigma'$.

**证明:** 这里假设仅有可数个命题变元, 因而全部公式可以列举为:

$$B_0, B_1, B_2, \cdots$$

按照以下方式定义集合 $\Sigma_n:(n=0,1,2,\cdots)$

1. $\Sigma_0=\Sigma$.
2. 若已定义 $\Sigma_n$, 则

$$\Sigma_{n+1}=\begin{cases}\Sigma_n\cup\{B_n\}, & \text{若}\Sigma_n\cup\{B_n\}\text{是协调的},\\ \Sigma_n, & \text{否则}.\end{cases}$$

根据定义可知每个 $\Sigma_n$ 都是协调的.

定义

$$\Sigma'=\Sigma_0\cup\Sigma_1\cup\Sigma_2\cup\cdots.$$

则必有$\Sigma\subseteq\Sigma'$.

$\Sigma'$ 是协调的

假设 $A$ 是任意取定公式.
若 $\Sigma'$ 不是协调的, 则它可以推出任何一个公式. 所以

$$\Sigma'\vdash\neg A\wedge A.$$

则存在 $A_1,\cdots,A_m$, 使得

$$A_1,\cdots,A_m\vdash\neg A\wedge A.$$

假设这些 $A_i$ 都属于 $\Sigma_n$, 则

$$\Sigma_n \vdash \neg A \wedge A.$$

这与 $\Sigma_n$ 的协调性相矛盾.

□

---

$\Sigma'$ 是极大的

对于 $A \notin \Sigma'$ ，可以假设它是$B_n$ ，根据定义可知

$$\Sigma_n \cup \{B_n\} \text{ 是不协调的.}$$

所以 $\Sigma' \cup \{A\}$ 是不协调的.

□

---

由上述性质可知, 上面定义的 $\Sigma'$ 满足定理的要求.

□

---

定理(完备性的证明):

对任意的公式集合 $\Sigma$ 及公式 $A$ ,

$$\text{若 } \Sigma \vDash A \text{ ，则 } \Sigma \vdash A \text{ .}$$

**证明:**

假设$\Sigma \nvdash A$ .

---

这时 $\Sigma \cup \{\neg A\}$ 是协调的, 因而可以扩充为极大协调集合 $\Sigma'$ .

由集合 $\Sigma'$ 可以定义赋值 $v$ 使得:

$$v(A) = 1 \text{ 当且仅当 } A \in \Sigma' \text{ .}$$

赋值 $v$ 具有以下性质:

- $v(\Sigma) = 1.$
- $v(A) = 0.$

但这与 $\Sigma \vDash A$ 矛盾.

全部

---

由反证法可知 $\Sigma \vdash A$ .

□

□

# 命题逻辑公理的独立性

## 弱推演系统

- 公理:
  - $\phi_2$ : $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$ .
  - $\phi_3$ : $(\neg A \to B) \to ((\neg A \to \neg B) \to A)$ .
- 规则:

$$\frac{A, A \to B}{B}.$$

假设 $\phi_1$ 是以下公式:

$$A \to (B \to A).$$

全部 ※

定义:(语义)

假设真值可以取 $\{0,1,2\}$ , 对于 $\to$及 $\neg$ , 按照以下方式定义真值表:

| $\to$ | 0 | 1 | 2 | $\neg$ |
|---|---|---|---|---|
| 0 | 0 | 2 | 2 | 2 |
| 1 | 2 | 2 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 |

在上述规定的基础上, 重新定义命题逻辑的相关概念:

- 赋值是命题变元的集合到 $\{0,1,2\}$ 的函数.
- 可以定义 $\nu(A)$ 的取值.
- 可以定义 $\nu(\Gamma)$ 的取值.
- 定义 $\Gamma \vDash A$ 为:

$$\nu \qquad \nu(\Gamma)=0 \qquad \nu(A)=0.$$

其中 $\boldsymbol{A}$ 是公式, $\boldsymbol{\Gamma}$ 是公式集合.

※

---

定义:(推演序列)
假设 $\boldsymbol{\Gamma}$ 是公式集合, 公式序列 $<\boldsymbol{A}_1, \boldsymbol{A}_2, \cdots, \boldsymbol{A}_n>$ 被称为 $\boldsymbol{\Gamma}-$ 推演序列, 若对每个 $\boldsymbol{A}_i$ :

- 或者 $\boldsymbol{A}_i \in \boldsymbol{\Gamma}$;
- 或者 $\boldsymbol{A}_i$ 是 $\boldsymbol{\phi}_2$ 或 $\boldsymbol{\phi}_3$ ;
- 或者存在 $\boldsymbol{j}, \boldsymbol{k} < \boldsymbol{i}$ , 使得 $\boldsymbol{A}_k$ 是 $\boldsymbol{A}_j \rightarrow \boldsymbol{A}_i$ .

---

可证性: 若存在一个$\boldsymbol{\Gamma}-$ 推演序列, 它的最后一个公式是 $\boldsymbol{A}$ , 则称 $\boldsymbol{A}$ 是 $\boldsymbol{\Gamma}-$ 可证的, 记为 $\boldsymbol{\Gamma} \vdash \boldsymbol{A}$ .
$\emptyset \vdash \boldsymbol{A}$ 记为 $\vdash \boldsymbol{A}$ .

---

可靠性: 若 $\boldsymbol{\Gamma} \vdash \boldsymbol{A}$ , 则 $\boldsymbol{\Gamma} \vDash \boldsymbol{A}$ .

※

---

独立性: 对于命题变元 $\boldsymbol{p}, \boldsymbol{q}$ , 若取 $\boldsymbol{\nu}(\boldsymbol{p}) = 0, \boldsymbol{\nu}(\boldsymbol{q}) = 1$ , 则 $\boldsymbol{\nu}(\boldsymbol{p} \rightarrow (\boldsymbol{q} \rightarrow \boldsymbol{p})) = 2$ .
所以,

$$\nvDash \boldsymbol{p} \rightarrow (\boldsymbol{q} \rightarrow \boldsymbol{p}),$$

$$\nvdash \boldsymbol{p} \rightarrow (\boldsymbol{q} \rightarrow \boldsymbol{p}),$$

所以 $\boldsymbol{\phi}_1$ 独立于 $\{\boldsymbol{\phi}_2, \boldsymbol{\phi}_3\}$ .

---

多值逻辑:

---

规则独立性:

**基本思路:**

证明某一个规则是独立的:

- 找出某个推演，基于此规则可以得出，但不能由其他规则得出，由此表明给定规则是不可取代的，这就是独立性.
- 为了证明在某些规则之下一个推演关系 $\Sigma \vdash A$ 不成立，所采用方式是修改逻辑联结词的定义，得到一个新逻辑推出关系 $\vDash'$ ，使得这些规则都具有可靠性，但 $\Sigma \nvDash' A$ .

---

单调性规则是独立的

在单调规则之外的规则，前提都不增加，若不使用此规则，则以下推演关系是不可证的:

$$A, B \vdash A.$$

由此可得独立性证明.

□

反证法规则是独立的

对于任意的真值赋值 $v$ 及公式 $A$ ，定义

$$v(\neg A) = 1.$$

可以得到新的逻辑推出关系 $\vDash'$ . 除反证法规则之外，其他规则都是可靠的. 使用反证法规则可得推演关系

$$\neg\neg p \vdash p.$$

但

$$\neg\neg p \nvDash' p.$$

由此可得独立性的证明.

□

三段论规则是独立的
演绎定理规则是独立的

---

证明其他规则的独立性, 对于相关 $\wedge$ 及 $\vee$ 等的规则, 需要对一些逻辑联结词定义新的真值表, 而不是采用基于 $\neg$ 及 $\rightarrow$的定义方式.

# 命题直觉主义逻辑的公理系统

定义:(公式)
命题直觉主义逻辑的公式等同于命题逻辑的公式.

□

定义:(公理系统)
在命题逻辑的自然推演系统中, 将反证法规则替换为两个规则:

- 直觉反证法:

$$若\ \Sigma, A \vdash B\ 及\ \Sigma, A \vdash \neg B\ ,\ 则\ \Sigma \vdash \neg A\ .$$

- 不协调前提:

$$若\ \Sigma \vdash A\ 及\ \Sigma \vdash \neg A\ ,\ 则\ \Sigma \vdash B\ .$$

**它们是互相独立的.**

定义:($c$ -可演算,$c$ -可证)
$\Sigma$ 是命题逻辑公式集合, $A$ 是命题逻辑公式. 称 $\Sigma \vdash A$ 是 $c$ -可演算的, 若存在

$$\Sigma_i \vdash A_i\ (i = 0, \cdots, n),$$

使得 $\Sigma_n \vdash A_n$ 是 $\Sigma \vdash A$ , 且对每个 $i$ , 有 $\Sigma_i \vdash A_i$ 满足:

- 或者是自反规则的一个实例;
- 或者存在 $j < i$ 使得 $\Sigma_i \vdash A_i$ 是通过 $\Sigma_j \vdash A_j$ 应用某个规则得到的;
- 或者存在 $j, k < i$ 使得 $\Sigma_i \vdash A_i$ 是通过 $\Sigma_j \vdash A_j$ 及 $\Sigma_k \vdash A_k$ 应用某个规则得到的.

若 $\Sigma \vdash A$ 是 $c$ -可演算的, 则记为 $\Sigma \vdash_c A$ .

定义:(协调)

给定命题逻辑的公式集合 $\Sigma$ , 称:

- $\Sigma$ 是不协调的:
  存在命题逻辑公式 $A$ , 使得

$$\Sigma \vdash_c A \text{ 且 } \Sigma \vdash_c \neg A.$$

- $\Sigma$ 是协调的:
  $\Sigma$ 不是不协调的.

性质:(命题直觉主义逻辑与命题逻辑)

- 直觉主义公理系统对于命题逻辑的语义是可靠的.
- 在命题逻辑中的证明, 若证明过程不出现 $(\neg -)$ , 则此证明也是直觉主义逻辑的一个证明.

可证关系: 假设 $A$ 与 $B$ 是命题逻辑语句, 则有以下 $c$ -可证明的序列:

$A \vdash_c \neg\neg A$

因为从 $A, \neg A$ 可以 $c$ -推出矛盾.

相应的推演序列是:

. $A \vdash A$ .

. $A, \neg A \vdash A$ .

. $\neg A \vdash \neg A$ .

. $A, \neg A \vdash \neg A$ .

. $A \vdash_c \neg\neg A$ .

□

$\neg\neg\neg A \vdash_c \neg A$

从 $A \vdash_c \neg\neg A$ 可知

$$\{\neg\neg\neg A, A\}$$

不是 $\vdash_c$ -协调的, 所以

$$\neg\neg\neg A \vdash_c \neg A.$$

□

$A \rightarrow B \vdash_c \neg B \rightarrow \neg A$

$A \rightarrow B \vdash_c \neg\neg A \rightarrow \neg\neg B$

$\vdash_c \neg(A \wedge \neg A)$

$\vdash_c \neg\neg(A \vee \neg A)$

$\vdash_c \neg\neg(\neg\neg A \rightarrow A)$

$\neg(A \vee B) \vdash_c \neg A \wedge \neg B.$

$\neg A \wedge \neg B \vdash_c \neg(A \vee B).$

$A \vee B \vdash_c \neg(\neg A \wedge \neg B)$.

$\neg A \vee \neg B \vdash_c \neg(A \wedge B)$.

$A \wedge B \vdash_c \neg(\neg A \vee \neg B)$.

$A \wedge B \vdash_c \neg(A \to \neg B)$.

---

不可证关系: 假设 $A$ 与 $B$ 是命题逻辑语句, 则有以下非 $c$ -可证明的序列:

- $\neg A \to B \vdash_c \neg B \to A$
- $\neg A \to \neg B \vdash_c B \to A$
- $\vdash_c \neg\neg A \to A$

  这是双重否定消除规则.

  假设 $A$ 是命题变元 $p$ . 构造模型 $\mathscr{K} = \langle V, R \rangle$ , 使得

$$V = \{v, w\}, R = \{(v, v), (v, w), (w, w)\}.$$

  其中
  - $v$ 使得 $v(p) = 0$ ,
  - $w$ 使得 $w(p) = 1$ .

  这时

| | $v$ | $w$ |
|---|---|---|
| $p$ | 0 | 1 |
| $\neg p$ | 0 | 0 |
| $\neg\neg p$ | 1 | 1 |
| $\neg\neg p$ $\quad$ $p$ | 0 | 1 |
| $\neg\neg p \to p$ | 0 | 1 |

  所以

$$(\neg\neg p\rightarrow p)^{\mathscr{K},v}=0.$$

所以 $\nvdash_c \neg\neg p\rightarrow p$ .

□

. $\vdash_c A\vee\neg A$
. $\vdash_c ((A\rightarrow B)\rightarrow A)\rightarrow A$
. $\neg(\neg A\wedge\neg B)\vdash_c A\vee B$
. $\neg(\neg A\vee\neg B)\vdash_c A\wedge B$
. $\neg(A\wedge B)\vdash_c \neg A\vee\neg B$
. $\neg A\rightarrow B\vdash_c A\vee B$
. $\neg(A\rightarrow\neg B)\vdash_c A\wedge B$
. $\neg(A\wedge\neg B)\vdash_c A\rightarrow B$

全部

# 命题直觉主义逻辑的语义

定义:(分层模型)
对于命题逻辑, 直觉主义逻辑的一个模型$\mathscr{K}$ 是指一个二元组

$$\langle V, R\rangle,$$

其中

- 非空集合 $V$ 的每个元素对应于命题逻辑的一个赋值
- $R$ 是 $V$ 上的一个二元关系, 具有自反性及传递性
- 对于任意的命题变元 $p$ 及 $v_1, v_2 \in K$, 有:

$$\text{若 } v_1(p)=1 \text{ 且 } v_1 R v_2\text{, 则 } v_2(p)=1$$

例子:(模型) 假设 $v_1, v_2$ 表示两个赋值, 它们在每个命题变元上的取值都是 $0$, 则有以下分层模型:

全部

- $\langle\{v_1\},\{(v_1,v_1)\}\rangle$
- $\langle\{v_1,v_2\},\{(v_1,v_1),(v_2,v_2)\}\rangle$

定义:(真值) 给定分层模型 $\mathscr{K}=\langle V, R\rangle$, 假设 $v\in V$. 对于命题逻辑的任意公式 $A$, 按照以下方式定义 $A^{\mathscr{K},v}$:

- 若 $p$ 是命题变元, 则 $p^{\mathscr{K},v}=v(p)$.
- $(A\wedge B)^{\mathscr{K},v}=1$ 当且仅当

$$A^{\mathscr{K},v}=1 \text{ 及 } B^{\mathscr{K},v}=1.$$

- $(A\vee B)^{\mathscr{K},v}=1$ 当且仅当

$$A^{\mathscr{K},v}=1 \text{ 或 } B^{\mathscr{K},v}=1.$$

- $(A\to B)^{\mathscr{K},v}=1$ 当且仅当

  对任意适合 $vRw$ 的 $w$, 若 $A^{\mathscr{K},w}=1$ 则 $B^{\mathscr{K},w}=1$.

- $(A\leftrightarrow B)^{\mathscr{K},v}=1$ 当且仅当

对任意适合 $vRw$ 的 $w$ , $A^{\mathscr{K},w}=1$ 等价于 $B^{\mathscr{K},w}=1$.

. $(\neg A)^{\mathscr{K},v}=1$ 当且仅当

对任意适合 $vRw$ 的 $w$ , 有 $A^{\mathscr{K},w}=0$ .

---

根据定义可知:

对任意的公式 $A$ , 对任意的 $v\in V$ , $A^{\mathscr{K},v}=0$ 或 $1$.

**$A^{\mathscr{K},v}=v(A)$ 是可能的.**

---

对于公式集合 $\Sigma$ , 定义 $\Sigma^{\mathscr{K},v}=1$ 为:

对任意 $A\in\Sigma$ , 都有 $A^{\mathscr{K},v}=1$ .

※

---

定理:(真值的传递性) 假设 $A$ 是命题逻辑公式. 给定分层模型 $\mathscr{K}=\langle V,R\rangle$ , 假设 $v,w\in V$ 满足 $vRw$ . 则

当 $A^{\mathscr{K},v}=1$ 时 $A^{\mathscr{K},w}=1$ .

※

---

定理:(真值的保持性) 给定分层模型 $\mathscr{K}=\langle V,R\rangle$ , 若 $v\in V$ 使得

对任意的 $w:vRw$ , 都有 $w$ 与 $v$ 是同一个赋值,

则对任意的命题逻辑公式 $A$ 都有:

$$A^{\mathscr{K},v}=v(A).$$

特别地, 若 $v$ 是 $R$ 的一个极大元, 则上述性质成立.

※

**定义**:( $c-$ 逻辑推论) 假设 $\Sigma$ 是命题逻辑公式集合, $A$ 是命题逻辑公式, 定义 $\Sigma \vDash_c A$ 为:

对任意分层模型 $\mathscr{K}=\langle V,R\rangle$ 及 $v\in V$ ，当 $\Sigma^{\mathscr{K},v}=1$ 时 $A^{\mathscr{K},v}=1$ .

**性质**:(直觉主义逻辑的可靠性) 假设 $\Sigma$ 是命题逻辑公式集合, $A$ 是命题逻辑公式,则

$$\text{若 } \Sigma\vdash_c A \text{ ，则 } \Sigma\vDash_c A \text{ .}$$

※

**定义**:(Heyting 代数)

二维实平面 $\mathbb{R}^2$ , 对于开集 $A$ 与 $B$ , 定义:

- $0$ 为 $\emptyset$
- $1$ 为 $\mathbb{R}^2$
- $A\wedge B$ 为 $A\cap B$
- $A\vee B$ 为 $A\cup B$
- $A\to B$ 为 $(A^c\cup B)^\circ$
- $\neg A$ 为 $A\to 0$ 即 $A^{c\circ}$

---

$\neg(A\wedge\neg A)$ 是永真的

---

$A\vee\neg A$ 不是永真的

**Boole 代数**

对任意的非空集合 $X$ , 假设 $A$ 与 $B$ 是 $X$ 的子集, 定义:

定义:

- $0$ 为 $\emptyset$

- $1$ 为 $X$
- $A \wedge B$ 为 $A \cap B$
- $A \vee B$ 为 $A \cup B$
- $A \to B$ 为 $(A^c \cup B)$
- $\neg A$ 为 $A \to 0$ 即 $A^c$

---

定义:(力迫)
考虑三元组

$$(R, \leq, \{v_p | p \in R\}),$$

其中

- $(R, \leq)$ 是偏序集
- $v_p$ 是赋值,且当 $p \leq q$ 时, 对每个命题变元 $u$ , 都有

$$v_p(u) \leq v_q(u).$$

---

对于 $p \in R$ 及命题逻辑语句 $A$ 及 $B$ , 定义 $p \Vdash A$ :

- 若 $A$ 是命题变元,则 $p \Vdash A$ :

$$v_p(u) = 1.$$

- $p \Vdash A \to B$ :

对任意的 $q \geq p$ , $q \Vdash A$ 蕴涵 $q \Vdash B$ .

- $p \Vdash \neg A$ :

对任意的 $q \geq p$ , $q \nVdash A$ .

- $p \Vdash A \wedge B$ :

$p \Vdash A$ 且 $p \Vdash B$ .

- $p \Vdash A \vee B$ :

$p \Vdash A$ 或 $p \Vdash B$ .

# 模态命题逻辑

定义(公式)
定义
假定 $\Box$ 及 $\Diamond$ 是两个一元逻辑联结词，按照命题逻辑的方式，可以定义模态命题逻辑的公式.

$\Box$

例子

- $\Box$ 及 $\Diamond$ 分别表示“必然”“可能”.
- $\Diamond A$ 等同于 $\neg\Box\neg A$.

$\Box$

例子
若 $p, q$ 是命题变元，则以下是公式:

- $\Diamond\Diamond p$
- $p \to \Diamond p$
- $\neg p \to \neg\Diamond\Box q$

$\Box$

$\Box$

定义(推导规则)
假设 $A, B$ 是公式, $\Sigma$ 是公式集合, 定义以下规则

- $(\Box-)$ :

$$\frac{\Sigma \vdash \Box A}{\Sigma \vdash A}$$

- $(\to-(\Box))$:

$$\frac{\Sigma\vdash\Box A\text{ 且 }\Sigma\vdash\Box(A\to B)}{\Sigma\vdash\Box B}$$

- $(\Box+)$:

$$\frac{\vdash A}{\vdash\Box A}$$

- $(\Box+\Box)$:

$$\frac{\Sigma\vdash\Box A}{\Sigma\vdash\Box\Box A}$$

- $(\Box+\Diamond)$:

$$\frac{\Sigma\vdash\Diamond A}{\Sigma\vdash\Box\Diamond A}$$

---

三个模态推理系统:

- $T$:
  命题逻辑的推导规则，$(\Box-)$，$(\to-(\Box))$，$(\Box+)$.
- $S_4$:
  $T$，$(\Box+\Box)$.
- $S_5$:
  $T$，$(\Box+\Diamond)$.

---

可以定义推演三个关系:

$$\vdash_T,\vdash_{S_4},\vdash_{S_5},$$

给定公式集合 $\Sigma$：

- 若存在公式 $A$，使得 $\Sigma \nvdash_T A$，则称 $\Sigma$ 是 $T-$ 协调的.
- 若存在公式 $A$，使得 $\Sigma \nvdash_{S_4} A$，则称 $\Sigma$ 是 $S_4-$ 协调的.
- 若存在公式 $A$，使得 $\Sigma \nvdash_{S_5} A$，则称 $\Sigma$ 是 $S_5-$ 协调的.

□

## 例子

例子 $A \vdash_T \Diamond A$.

证明:

- $\Box \neg A \vdash_T \Box \neg A$.
- $\Box \neg A \vdash_T \neg A$.
- $\neg \neg A \vdash_T \neg \Box \neg A$.
- $A \vdash_T \neg \Box \neg A$.

即

$$A \vdash_T \Diamond A.$$

□

## 例子

$\vdash_T (\Box(A \to B) \land \Box(B \to A)) \leftrightarrow (\Box A \leftrightarrow \Box B)$.

$\vdash_T \Box(A \wedge B) \leftrightarrow (\Box A \wedge \Box B)$.
$\vdash_T \Diamond(A \vee B) \leftrightarrow (\Diamond A \vee \Diamond B)$.

□

---

定义(语义)
模态命题逻辑的一个模型 $\mathfrak{M}$ 是指一个二元组

$$\langle V, R \rangle ,$$

其中集合 $V$ 的每个元素相应于命题逻辑的一个赋值, $R$ 是 $V$ 上二元关系.

---

给定模态命题逻辑的模型 $\mathfrak{M} = \langle V, R \rangle$ , 假设 $v \in V$ . 对于模态命题逻辑的任意公式 $A$ , 按照以下方式定义 $A^{\mathfrak{M}, v}$ :

- 若 $p$ 是命题变元, 则 $p^{\mathfrak{M}, v} = v(p)$ .
- $(A \wedge B)^{\mathfrak{M}, v} = 1$ 当且仅当
$$A^{\mathfrak{M}, v} = 1 \text{ 及 } B^{\mathfrak{M}, v} = 1 .$$
- $(A \vee B)^{\mathfrak{M}, v} = 1$ 当且仅当
$$A^{\mathfrak{M}, v} = 1 \text{ 或 } B^{\mathfrak{M}, v} = 1 .$$
- $(A \to B)^{\mathfrak{M}, v} = 1$ 当且仅当
$$\text{若 } A^{\mathfrak{M}, v} = 1 \text{ 则 } B^{\mathfrak{M}, v} = 1 .$$
- $(A \leftrightarrow B)^{\mathfrak{M}, v} = 1$ 当且仅当
$$A^{\mathfrak{M}, v} = 1 \text{ 等价于 } B^{\mathfrak{M}, v} = 1.$$
- $(\neg A)^{\mathfrak{M}, v} = 1$ 当且仅当
$$A^{\mathfrak{M}, v} = 0 .$$
- $(\Box A)^{\mathfrak{M}, v} = 1$ 当且仅当
$$\text{对任意的 } v' \in V \text{ , 若 } v R v' \text{ , 则 } A^{\mathfrak{M}, v'} = 1 .$$

对于公式集合 $\boldsymbol{\Sigma}$ , 若对任意的公式 $\boldsymbol{A} \in \boldsymbol{\Sigma}$ , 都有 $\boldsymbol{A}^{\mathfrak{M},v}=\mathbf{1}$ , 则记

□

## $\boldsymbol{T}$ -可靠性

针对模态命题逻辑模型类 $\mathscr{K}_{\boldsymbol{T}}$ :

$$\{\mathfrak{M} \mid \mathfrak{M}=\langle \boldsymbol{V}, \boldsymbol{R} \rangle \text{ 且 } \boldsymbol{R} \text{ 具有自反性 }\}$$

定义: 对于公式集合 $\boldsymbol{\Sigma}$ 及公式 $\boldsymbol{A}$ , 有以下定义

- $\boldsymbol{T}-$ 可满足的:
  若存在 $\mathfrak{M}=\langle \boldsymbol{V}, \boldsymbol{R} \rangle \in \mathscr{K}_{\boldsymbol{T}}$ 及 $v \in \boldsymbol{V}$ , 使得 $\boldsymbol{\Sigma}^{\mathfrak{M},v}=\mathbf{1}$ .
- $\boldsymbol{T}-$ 有效的:
  若对任意的 $\mathfrak{M}=\langle \boldsymbol{V}, \boldsymbol{R} \rangle \in \mathscr{K}_{\boldsymbol{T}}$ 及 $v \in \boldsymbol{V}$ , 都有 $\boldsymbol{\Sigma}^{\mathfrak{M},v}=\mathbf{1}$ .
- $\boldsymbol{\Sigma} \vDash_{\boldsymbol{T}} \boldsymbol{A}$ :
  若对任意的 $\mathfrak{M}=\langle \boldsymbol{V}, \boldsymbol{R} \rangle \in \mathscr{K}_{\boldsymbol{T}}$ 及 $v \in \boldsymbol{V}$ , 当 $\boldsymbol{\Sigma}^{\mathfrak{M},v}=\mathbf{1}$ 时 $\boldsymbol{A}^{\mathfrak{M},v}=\mathbf{1}$ .

**定理($\boldsymbol{T}-$ 可靠性)**: 对于任意的公式集合 $\boldsymbol{\Sigma}$ 及公式 $\boldsymbol{A}$ ,

$$\text{若 } \boldsymbol{\Sigma} \vdash_{\boldsymbol{T}} \boldsymbol{A} \text{ , 则 } \boldsymbol{\Sigma} \vDash_{\boldsymbol{T}} \boldsymbol{A} \text{ .}$$

**证明:** 只需证明以下事实:

- $\dfrac{\boldsymbol{\Sigma} \vDash_{\boldsymbol{T}} \Box \boldsymbol{A}}{\boldsymbol{\Sigma} \vDash_{\boldsymbol{T}} \boldsymbol{A}}$.
  对任意 $\mathfrak{M}=\langle \boldsymbol{V}, \boldsymbol{R} \rangle \in \mathscr{K}_{\boldsymbol{T}}$ 及 $v \in \boldsymbol{V}$ , 以下证明:
  $$\boldsymbol{\Sigma}^{\mathfrak{M},v}=\mathbf{1} \qquad \boldsymbol{A}^{\mathfrak{M},v}=\mathbf{1}$$
  当 $\boldsymbol{\Sigma}^{\mathfrak{M},v}=\mathbf{1}$ 时, 从 $\boldsymbol{\Sigma} \vDash_{\boldsymbol{T}} \Box \boldsymbol{A}$ 可知,

$$(\Box A)^{\mathfrak{M},v}=1.$$

即对任意的 $v'\in V$ ，若 $vRv'$ ，则

$$A^{\mathfrak{M},v'}=1.$$

因为 $R$ 具有自反性，所以 $vRv$ 是成立的. 由此可知

$$A^{\mathfrak{M},v}=1.$$

□

$\cdot\dfrac{\Sigma\vDash_T\Box A \text{ 且 } \Sigma\vDash_T\Box(A\to B)}{\Sigma\vDash_T\Box B}.$

对任意 $\mathfrak{M}=\langle V,R\rangle\in\mathscr{K}_T$ 及 $v\in V$ ，以下证明:

$$\Sigma^{\mathfrak{M},v}=1 \qquad (\Box B)^{\mathfrak{M},v}=1$$

当 $\Sigma^{\mathfrak{M},v}=1$ 时，

。从 $\Sigma\vDash_T\Box A$ . 可知

$$(\Box A)^{\mathfrak{M},v}=1.$$

。从 $\Sigma\vDash_T\Box(A\to B)$ . 可知

$$(\Box(A\to B))^{\mathfrak{M},v}=1.$$

任取 $v'\in V$ ，使得 $vRv'$ ，则

$$A^{\mathfrak{M},v'}=(A\to B)^{\mathfrak{M},v'}=1.$$

所以

$$B^{\mathfrak{M},v'}=1.$$

即 $(\Box B)^{\mathfrak{M},v}=1$ .

□

. $\dfrac{\vDash_T A}{\vDash_T \Box A}$.

对任意 $\mathfrak{M}=\langle V,R\rangle\in\mathscr{K}_T$ 及 $v\in V$ ，从

$$\vDash_T A$$

可知 $A^{\mathfrak{M},v}=1$ ，所以

$$(\Box A)^{\mathfrak{M},v}=1.$$

□

□

## $S_4$-可靠性

针对模态命题逻辑模型类 $\mathscr{K}_{S_4}$ :

$$\{\mathfrak{M}|\mathfrak{M}=\langle V,R\rangle \text{ 且 } R \text{ 具有自反性及传递性 }\}$$

定义: 对于公式集合 $\Sigma$ 及公式 $A$ , 有以下定义

. $S_4$– 可满足的:

若存在 $\mathfrak{M}=\langle V,R\rangle\in\mathscr{K}_{S_4}$ 及 $v\in V$ ，使得 $\Sigma^{\mathfrak{M},v}=1$ .

. $S_4$– 有效的:

若对任意的 $\mathfrak{M}=\langle V,R\rangle\in\mathscr{K}_{S_4}$ 及 $v\in V$ ，都有 $\Sigma^{\mathfrak{M},v}=1$ .

. $\Sigma\vDash_{S_4} A$ :

若对任意的 $\mathfrak{M}=\langle V,R\rangle\in\mathscr{K}_{S_4}$ 及 $v\in V$ ，当 $\Sigma^{\mathfrak{M},v}=1$ 时

.

**定理**($S_4-$ 可靠性): 对于任意的公式集合 $\Sigma$ 及公式 $A$ ,

$$\text{若 } \Sigma\vdash_{S_4}A\text{ ，则 }\Sigma\vDash_{S_4}A\text{ .}$$

□

## $S_5$ -可靠性

针对模态命题逻辑模型类 $\mathscr{K}_{S_5}$ :

$$\{\mathfrak{M}|\mathfrak{M}=\langle V,R\rangle\text{ 且 }R\text{ 是一个等价关系 }\}$$

定义: 对于公式集合 $\Sigma$ 及公式 $A$ , 有以下定义

- $S_5-$ 可满足的:
  若存在 $\mathfrak{M}=\langle V,R\rangle\in\mathscr{K}_{S_5}$ 及 $v\in V$ ，使得 $\Sigma^{\mathfrak{M},v}=1$ .
- $S_5-$ 有效的:
  若对任意的 $\mathfrak{M}=\langle V,R\rangle\in\mathscr{K}_{S_5}$ 及 $v\in V$ ，都有 $\Sigma^{\mathfrak{M},v}=1$ .
- $\Sigma\vDash_{S_5}A$ :
  若对任意的 $\mathfrak{M}=\langle V,R\rangle\in\mathscr{K}_{S_5}$ 及 $v\in V$ ，当 $\Sigma^{\mathfrak{M},v}=1$ 时 $A^{\mathfrak{M},v}=1$ .

**定理**($S_5-$ 可靠性): 对于任意的公式集合 $\Sigma$ 及公式 $A$ ,

$$\text{若 } \Sigma\vdash_{S_5}A\text{ ，则 }\Sigma\vDash_{S_5}A\text{ .}$$

□

### 可靠性的应用

对于三个推演系统: $T$, $S_4$, $S_5$ 从它们的可靠性可知,

对于相应的可满足公式集合, 使用给定系统的证明规则, 都不可能得出矛盾结论.

全部 ☐

...