公理集合论初步

集合论

集合与属于

1. **朴素集合论**

   具有给定性质的对象的全体定义为集合. “属于关系”是集合与元素之间的关系.

2. **公理集合论**

   给定集合论语言$\mathscr{L} = \{\in\}$ 及该语言的一个模型$\langle V, \in \rangle$.

   集合论语言的模型的元素称为该模型中的集合, 语言中二元关系符号的解释称为属于关系, 用 $\in$ 表示.

ZFC

集合论有 10 条公理:

1. 外延公理
2. 空集公理
3. 偶对公理
4. 并集公理
5. 子集公理
6. 幂集公理
7. 无穷公理
8. 替换公理
9. 正规公理
10. 选择公理

一般意义下的集合论的模型满足这些公理的中的一部分公理.

公理集合论是理论研究的基础理论

在集合论的公理中,

1. 外延公理用于判断集合相等.
2. 正规公理限制集合属于关系.
3. 其他的公理都是保证集合存在的.
4. 子集公理、替换公理都是公理模式, 对于一个公式, 都有一条公理.

集合论公理使得数学对象可以基于有限操作形式生成, 有严格的定义.

基本概念

在集合论语言之下, 在该语言的一个模型里, 有一些可定义的元素、谓词、函数.

1. 空集

   $\emptyset$ 表示空集:
   $$\neg\exists x(x\in\emptyset).$$

2. 二元组

   $\langle a,b\rangle$ 表示二元组,是指以下集合:
   $$\{\{a\},\{a,b\}\}.$$

3. 交集

   $a\cap b$ 表示交集:
   $$a\cap b=\{x|x\in a\wedge x\in b\}.$$

4. 差集

   $a-b$ 表示差集:
   $$a-b=\{x|x\in a\wedge x\notin b\}.$$

5. 包含于

   $\subseteq$ 表示包含关系:
   $$a\subseteq b\,\text{当且仅当}\,\forall x(x\in a\rightarrow x\in b).$$

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

6. 函数

   $func(a)$ 表示a 是一个函数:
   $$\phi_1\wedge\phi_2.$$

   其中

(a) ϕ_1 是公式 $\forall x(x \in a \to \exists uv(x = \langle u, v\rangle))$.

(b) ϕ_2 是公式 $\forall uvw(\langle u, v\rangle \in a \wedge \langle u, w\rangle \in a \to v = w)$.

公式 ϕ_2 表示第二坐标具有唯一性.

7. 定义域

$dom(a)$ 表示函数 a 的定义域:

$$dom(a) = \{u | \exists v(\langle u, v\rangle \in a)\}.$$

8. 值域

$ran(a)$ 表示一个函数 a 的值域:

$$ran(a) = \{v | \exists u(\langle u, v\rangle \in a)\}.$$

9. 象

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

$$\langle b, a(b)\rangle \in a.$$

函数 a 也写为:

$$\begin{array}{rccl} a: & dom(a) & \to & ran(a) \\ & b & \mapsto & a(b) \end{array}$$

10. 卡氏积

对于集合 a 及 b, 它们的卡氏积 $a \times b$是以下集合:

$$\{\langle u, v\rangle | u \in a \wedge v \in b\}.$$

11. 自然数

自然数:

(a) 以 0 表示 $\emptyset$

(b) 以 1 表示 $\{0\}$

(c) 以 2 表示 $\{0, 1\}$

(d) 以 3 表示$\{0, 1, 2\}$

(e) $\cdots$

外延公理

公理

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

含义

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

公理

$$\exists x \forall y \neg (y \in x).$$

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

记满足 $\forall y(y \notin x)$ 的 x 为 $\emptyset$， 称为空集.

含义

上述公理保证空集是存在的.

集合论的任意模型中都包含空集.

空集是唯一的

若 $\emptyset'$ 是另一个空集.

从 $\forall y(y \notin \emptyset)$, 可知

$$\forall z(z \in \emptyset \to z \in \emptyset').$$

从 $\forall y(y \notin \emptyset')$ 可知

$$\forall z(z \in \emptyset' \to z \in \emptyset).$$

所以

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

因而 $\emptyset = \emptyset'$.

偶对公理

公理

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

含义

对于集合 x, y, 记满足

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

的 u 为$\{x, y\}$.

有限集合的存在性

此公理与下面的并集公理可以保证存在任意多元素的有限集合:

1. 单元素集合

假设 x 是集合, 则存在集合 $\{x\}$:

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

2. 三元素集合

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

公理

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

含义

对于集合 x, 记满足

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

的 u 为$\cup x$.

一个集合的并集, 是由这个集合的元素的元素组成的.

$\cup$ 是一元函数

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 $\{\langle a, b\rangle, \langle c, d\rangle\}$ 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

$$\cup \cup f \supseteq dom(f), \cup \cup f \supseteq ran(f).$$

$\cup\emptyset=\emptyset$

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 $\exists y(y\in\{\emptyset\}\wedge x\in y)$ 等值于

$$x\in\emptyset$$

是永假的, 所以 $\cup\{\emptyset\}=\emptyset$.

$\cup A=\cup\{A\}$?

对一般集合,

$$\cup A\neq\cup\{A\}.$$

函数的并

假设 f,g 是两个函数, 则 $f\cup g$ 是函数当且仅当

$$\forall x(x\in dom(f)\cap dom(g)\rightarrow f(x)=g(x)).$$

证明: 首先 $f\cup g$ 是二元组的集合, 而上述条件可以保证第二坐标有唯一性, 所以 $f\cup g$ 还是函数.

函数集合的并

假设 u 是函数的集合,即

$$\forall x(x\in u\rightarrow func(x)).$$

假设 u 满足以下性质,

$$\forall xfg(f\in u\wedge g\in u\wedge x\in dom(f)\cap dom(g)\rightarrow f(x)=g(x)).$$

则 $\cup u$ 是函数.

交集

定义集合 x 的交集为满足以下条件的集合 v:

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

对于集合 x, 记上述 v 为 $\cap x$.

而

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

被严格地写为$\cap\{A_0, A_1, A_2, \cdots\}$. 一个集合的交集, 是这个集合的元素作为一组集合在朴素集合论意义下的交集.

由定义可知, 若$\cap x$ 存在, 则对任意的 $y \in x$, 有

$$y \supseteq \cap x.$$

$\cap\emptyset$

不存在集合,它是空集的交集.

证明: 若存在这样的集合 μ 则

$$\forall z(z \in \mu \leftrightarrow \forall y(y \in \emptyset \to z \in y)).$$

所以对任意的 z,

$$\forall y(y \in \emptyset \to z \in y) \to z \in \mu.$$

但是 $\forall y(y \in \emptyset \to z \in y)$ 是永真的, 所以

$$z \in \cap\emptyset.$$

因而$\cap\emptyset$ 包含任意一个集合, 这是不可能的, 所以不存在集合 μ.

子集公理

公理

假设 ϕ 是集合论语言的公式， 仅出现自由变元 $x_1, \cdots, x_n, x, z$, 不出现变元 y,则

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

含义

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

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

集合 y 是 x 的子集, 所以该公理称为子集公理.

子集公理是一个公理模式.

幂集公理

公理

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

含义

对于给定的 x, 满足

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

的 y 称为 x 的幂集, 记为 $\rho(x)$, 也记为 2^x.

一个集合的幂集, 是该集合的所有子集构成的集合.

无穷公理

公理

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

其中 y^+ 表示集合 $y \cup \{y\}$.

含义

1. 满足

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

的集合称为归纳集

2. 无穷公理保证一类特殊集合是存在的

替换公理

公理

假设 ϕ 是集合论语言的公式， 仅出现自由变元 $x_1, \cdots, x_n, u, v$, 不出现变元 y, 则

$$\forall x_1 \cdots x_n \forall x(\psi \to \exists y \forall v(v \in y \leftrightarrow \exists u \in x \phi(u, v))),$$

其中 ψ 是以下公式:

$$\forall u \in x \forall v_1 v_2(\phi(u, v_1) \wedge \phi(u, v_2) \to v_1 = v_2).$$

这里所定义的集合 y 也写为

$$\{v | \exists u(u \in x \wedge \phi(u, v))\}.$$

含义

该公理可以保证一类函数的存在性.

假设 x 是集合, $\phi(u, v)$ 是函数型公式, 则可定义函数 f:

$$\begin{array}{rccc} f: & x & \to & y \\ & u & \mapsto & v \end{array}$$

其中 $y = \{v | \exists u(u \in x \wedge \phi(u, v))\}$, u 与 v 满足 $\phi(u, v)$.

这样的函数是存在的.

该公理可以保证一类集合的存在性.

由集合

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

的存在性,可知存在集合

$$\{\underbrace{0}_{0\text{重}}, \underbrace{\{0\}}_{1\text{重}}, \underbrace{\{\{0\}\}}_{2\text{重}}, \underbrace{\{\{\{0\}\}\}}_{3\text{重}}, \cdots\}.$$

证明上述集合的存在性,需要自然数的逻辑理论.

正规公理

公理

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

含义

1. 集合与它的元素的公共元素

对于集合

$$\{0, \{0\}\},$$

它与它的元素 $\{0\}$ 的交集是 $\{0\}$.

2. $\emptyset$

若 $\emptyset \in x$, 则 x 适合

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

这时的 y 可取为 $\emptyset$.

3. 无限序列

x 不满足正规公理

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

否则可以取得元素无限序列

$$x \ni x_1 \ni x_2 \ni \cdots$$

4. $x = \{x\}$

正规公理保证不存在这样的集合:

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

5. $x \in x$

若定义 $y = \{x\}$, 则 $x \cap y = y$, 所以正规公理保证不存在这样的 x.

选择公理

公理

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

其中

1. ϕ_1 是
$$func(y) \wedge dom(y) = \rho(x) - \{\emptyset\} \wedge ran(y) \subseteq x,$$
定义一个函数使得有给定的定义域及值域.

2. ϕ_2 是
$$\forall z(z \subseteq x \wedge \neg z = \emptyset \to y(z) \in z),$$
指定了取值特点.

含义

选择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

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

使得 $f(x) \in x$.

卡氏集

对于有限个非空集合 $A_1, \cdots, A_n$, 它们的乘积 $A_1 \times \cdots \times A_n$ 肯定是不空的, 但对于无限多个非空集合 $A_1, A_2, A_3 \cdots$, 只有选择公理才可以保证它们的乘积

$$A_1 \times A_2 \times A_3 \cdots$$

是不空的.

公理的相容性

1. 有限性质

   假设 U_f 是以下集合
$$\rho(\emptyset) \cup \rho(\rho(\emptyset)) \cup \rho(\rho(\rho(\emptyset))) \cup \cdots$$
   它是由一些有限集合构成的, 将 $\in$ 解释为一般意义下的元素属于集合, 则可得集合论语言的一个模型:
$$\langle U_f, \in \rangle.$$
   这一类集合满足除无穷公理之外的所有公理, 有以下性质:

(a) 这样的有限个有限集合的并集还是有限的.

(b) 这样的有限集合的子集还是有限的.

(c) 这样的有限集合的幂集还是有限的.

(d) 这样的有限集合在任意函数之下的象还是有限的.

所以这些公理:

(a) 是相容的

(b) 不能推出存在无限集合

(c) 不能推出无穷公理

2. 无穷公理

ZFC 的相容性是不可证的.

3. 非空集合

对于集合论模型

$$\langle \{\emptyset\}, \in \rangle.$$

空集公理、外延公理、并集公理、子集公理、替换公理、正规公理、选择公理都成立, 同时以下语句成立:

$$\forall x(x = \emptyset).$$

所以上述公理不能推出存在非空集合. 在此模型里不存在全集.

公理的独立性
偶对公理可以由其他公理推出.

1. 一个单元素集合

空集 $\emptyset$, 也记为 0, 它的子集只有空集, 所以它的幂集 2^0 是 $\{\emptyset\}$. 记该集合为 1.

2. 一个双元素集合

集合 1 的幂集 2^1 :

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

是由两个不同的元素 0 及 1 组成的.

3. 一个函数型公式

假设 a 与 b 是两个集合, 考虑以下公式 $\phi(x, y)$:

$$(x = 0 \to y = a) \wedge (\neg x = 0 \to y = b).$$

它满足

$$\forall xyz((\phi(x,y) \wedge \phi(x,z)) \rightarrow y = z)$$

4. 一般的两元集合

   因为存在集合 $\{0,1\}$, 根据替换公理, 由上述公式, 可知存在集合 $\{a,b\}$.

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:

1. $\emptyset \in u$.

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

记号

集合 $a \cup \{a\}$ 记为 a^+. 因而

1. $0^+ = 0 \cup \{0\} = 1$

2. $1^+ = 1 \cup \{1\} = \{0,1\} = 2$

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

4. $\cdots$

公式

以 $Ind(x)$ 表示以下公式:

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

则集合 u 是归纳集当且仅当 $Ind[u]$ 成立.

性质

归纳集有以下性质:

1. 两个归纳集的并集及交集还是归纳集.

2. 若存在集合

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

   则它是一个归纳集.

3. 无穷公理保证这样的集合是存在的.

   这样的集合不唯一.

4. 归纳集是朴素意义下的无限集.

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 ω,即满足以下公式

$$Ind[\omega] \wedge \forall x(Ind[x] \rightarrow \omega \subseteq x).$$

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:

1. 对于每个 $n \in \omega$, 因为 $n \in n^+, n^+ \in \omega$, 所以 $n \in \cup\omega$.

2. 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

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

则 $u = \omega.$

证明

这时的 u 是一个归纳集合, 又是 ω 的子集, 所以等于 ω.

推论–第一归纳法

假设 $\phi(x)$ 是集合论语言的一个公式, 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 ω 的子集, 根据 ϕ 所满足的性质, 可知

$$0 \in u \land \forall x(x \in u \to x^+ \in u),$$

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

推论–第二归纳法

假设 $\phi(x)$ 是集合论语言的一个公式, 包含一个自由变元 x, 且

$$\forall x(\forall y(y \in x \to \phi(x)) \to \phi(x)).$$

成立, 则对任意的自然数 n,都有 $\phi(n)$ 成立.

证明

考虑集合

$$u = \{n \in \omega | \forall y(y \in n \to \phi(n))\}.$$

根据子集公理, 可知它是集合, 还是 ω 的子集.

1. 从
$$\forall y(y \in 0 \to \phi(0))$$
成立, 可知 $0 \in u$.

2. 若 $n \in u$, 则
$$\forall y(y \in n \to \phi(n))$$
成立. 这时 $\phi(n)$ 成立, 而 $n^+ = n \cup \{n\}$, 所以
$$\forall y(y \in n^+ \to \phi(n^+))$$
成立, 即 $n^+ \in u$.

所以 $u = \omega$.

因为 $n \in n^+$, 从 $n^+ \in u$ 可知 $\phi(n)$ 成立. 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 $\phi(x)$:

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

1. $\phi[0]$ 成立, 是因为 $0^+ = \{0\}$ 不是空集.

2. 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 $\phi(x)$:

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

1. $\phi[0]$ 成立, 是因为 $\neg 0 = 0$ 是假的.

2. 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.

例子

对于任意的 $m \in \omega$, 若 $n \in m$, 则$n \in \omega$. 证明

考虑以下关于 x 的公式 $\phi(x)$:

$$\forall y(y \in x \to y \in \omega).$$

1. $\phi[0]$ 成立, 是因为在以下公式

$$\forall y(y \in 0 \to y \in \omega)$$

中, $y \in 0$ 是假的.

2. 若 $m \in \omega$ 且 $\phi[m]$ 成立, 则 $\phi[m^+]$ 成立: 当 $y \in m^+ = m \cup \{m\}$ 时, 或者 $y \in m$ 或者 $y = m$.

  (a) 若 $y \in m$, 则从 $\phi[m]$ 成立, 可知 $y \in \omega$

  (b) 若 $y = m$.则直接可得 $y \in \omega$

  所以总有 $y \in \omega$.

所以 $\forall x \phi(x)$ 成立. 这个就是“对于任意的 $m \in \omega$, 若 $n \in m$, 则 $n \in \omega$ ”.

例子

对于任意的 $a, b, c \in \omega$, 若 $a \in b, b \in c$, 则$a \in c$. 证明

考虑以下关于 x 的公式$\phi(x)$:

$$\forall zy(z \in y \wedge y \in x \to z \in x).$$

1. $\phi[0]$ 成立, 是因为在以下公式

$$\forall zy(z \in y \wedge y \in 0 \to z \in 0)$$

中, $y \in 0$ 是假的.

2. 若 $m \in \omega$ 且 $\phi[m]$ 成立, 则 $\phi[m^+]$ 成立: 假设 $z \in y, y \in m^+$. 从 $y \in m \cup \{m\}$ 可知:

    (a) 若 $y \in m$, 则根据 $\phi[m]$ 可知 $z \in m$, 从而 $z \in m^+$.

    (b) 若 $y = m$, 则直接可得 $z \in m$, 所以 $z \in m^+$.

所以 $\forall x \phi(x)$ 成立, 这就是需证的.

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:

1. $dom(r) = \omega$.

2. $r(0) = a$.

3. 对任意的自然数 m, 都有 $r(m^+) = f(r(m))$.

推广

函数型公式

假设 $\phi(x, y)$ 是集合论语言的一个函数型公式, 即满足

1. $\forall x \exists y \phi[x, y]$.

2. $\forall xyz(\phi[x, y] \wedge \phi[x, z] \to y = z)$.

这时记相应于 x 的 y 为 x_ϕ.

若将上述性质中的 $f(x)$ 替换为 x_ϕ, 则结论仍然成立.

多元迭代函数

假设 a 是一个集合, $f(x, y)$ 是二元函数, 则存在一个函数r 满足:

1. $dom(r) = \omega$.

2. $r(0) = a$.

3. 对任意的自然数 m, 都有 $r(m^+) = f(r(m), m)$.

应用——无限集

性质

存在集合$\{0,\{0\},\{\{0\}\},\{\{\{0\}\}\},\cdots\}$.

证明

在递归定义中,

1. 取 a 为 0

2. 取公式 ϕ 为 $y=\{x\}$

可以定义出函数 r 满足:

1. $r(0)=0$

2. $r(1)=\{r(0)\}=\{0\}$

3. $r(2)=\{r(1)\}=\{\{0\}\}$

4. $\cdots$

r 的值域即为上述集合.

命题直觉主义逻辑

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:

1. 直觉反证法:

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

2. 不协调前提:

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

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:

1. $A \vdash A$.

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

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

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

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

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

从 $A \vdash_c \neg\neg A$ 可知

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

不是 $\vdash_c$-协调的, 所以

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

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

$\{A \to B, \neg B, A\}$ 可以推出矛盾.

相应的推演序列是:

1. $A \to B \vdash A \to B$.

2. $A \to B, A \vdash A \to B$.

3. $A \vdash A$.

4. $A \to B, A \vdash A$.

5. $A \to B, A \vdash B$.

6. $A \to B, A, \neg B \vdash B$.

7. $\neg B \vdash \neg B$.

8. $A \to B, A, \neg B \vdash \neg B$.

9. $A \to B, \neg B \vdash \neg A$.

10. $A \to B \vdash \neg B \to \neg A$.

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:

1. $\neg A \to B \vdash_c \neg B \to A$

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

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

其中

(a) v 使得 $v(p) = 0$ 及 $v(q) = 0$,

(b) w 使得 $w(p) = 1$ 及 $w(q) = 0$.

这时 $q^{\mathscr{K}, v} = 0$, $q^{\mathscr{K}, w} = 0$, 所以

$$(\neg q)^{\mathscr{K}, v} = 1.$$

但是 $p^{\mathscr{K}, v} = 0$, 所以

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

另一方面,

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

所以

$$(\neg p \to q)^{\mathscr{K}, v} = 1.$$

即在模型 $\mathscr{K}$ 的第一层, 左边取 1 而右边取 0. 因而上述公式是不永真的, 因而是不可证的.

2. $\neg A \to \neg B \vdash_c B \to A$

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

$$V = \{v_1, v_2\}, R = \{(v_1, v_1), (v_1, v_2), (v_2, v_2)\}.$$

其中

(a) v_1 使得 $v_1(p) = 0$ 及 $v_1(q) = 1$,

(b) v_2 使得 $v_2(p) = 1$ 及 $v_2(q) = 1$.

这时 "若 $v_1(q) = 1$ 则 $v_1(p) = 1$" 不成立, 所以

$$(q \to p)^{\mathscr{K}, v_1} = 0.$$

另一方面, $(\neg p)^{\mathscr{K}, v_1} = 0$ 及 $(\neg p)^{\mathscr{K}, v_2} = 0$, 所以

$$(\neg p \to \neg q)^{\mathscr{K}, v_1} = 1.$$

3. $\vdash_c \neg\neg A \to A$

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

(a) v 使得 $v(p) = 0$,

(b) w 使得 $w(p) = 1$.

这时

	v	w
p	0	1
$\neg p$	0	0
$\neg\neg p$	1	1
若 $\neg\neg p$ 成立则p 成立	0	1
$\neg\neg p \to p$	0	1

所以

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

所以 $\nvdash_c \neg\neg p \to p$.

4. $\vdash_c A \vee \neg A$

这表明排中律不成立.
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

(a) v 使得 $v(p) = 0$,

(b) w 使得 $w(p) = 1$.

这时 $p^{\mathscr{K}, v} = 0$, 但 $(\neg p)^{\mathscr{K}, v} = 0$, 所以

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

所以 $\nvdash_c p \vee \neg p$.

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

1. **非空集合** V **的每个元素对应于命题逻辑的一个赋值**
2. R **是** V **上的一个二元关系, 具有自反性及传递性**
3. **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:**

1. $\langle\{v_1\}, \{(v_1, v_1)\}\rangle$
2. $\langle\{v_1, v_2\}, \{(v_1, v_1), (v_2, v_2)\}\rangle$

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** $A^{\mathscr{K},v}$**:**

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

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

3. $(A \vee B)^{\mathscr{K},v} = 1$ **当且仅当**

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

4. $(A \to B)^{\mathscr{K},v} = 1$ **当且仅当**

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

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

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

6. $(\neg A)^{\mathscr{K},v} = 1$ **当且仅当**

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

根据定义可知:

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

$A^{\mathscr{K},v}=v(A)$ 是可能的.

1. R 是平凡的

2. 所有 v 对应于同一个赋值

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

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

事实: “$A^{\mathscr{K},v}=1$ 且 $(\neg A)^{\mathscr{K},v}=1$” 是不成立的.

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

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

证明: 对公式的长度归纳.

1. 若 A 是命题变元, 则直接根据模型的定义可知此性质成立.

2. 假设定理的结论对公式 A 成立, 则定理对 $\neg A$ 也成立.

   若 $(\neg A)^{\mathscr{K},v}=1$, 则根据定义, 可知对任意的 v':

$$\text{当 } vRv' \text{ 时, } A^{\mathscr{K},v'}=0.$$

   对于定理条件中的 w, 考虑任意的 w': wRw'.

   根据 R 的传递性, 可知 vRw', 所以

$$A^{\mathscr{K},w'}=0.$$

   所以

$$(\neg A)^{\mathscr{K},w}=1.$$

3. 假设定理的结论对公式 A 及 B 成立, 则定理对 $A\wedge B$ 也成立.

   若 $(A\wedge B)^{\mathscr{K},v}=1$ 且 vRw, 则根据定义可知

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

根据归纳假设可知

$$A^{\mathscr{K},w}=1 \text{ 且 } B^{\mathscr{K},w}=1.$$

由定义可知

$$(A\wedge B)^{\mathscr{K},w}=1.$$

4. 同理可证定理对其他情形是成立的.

定义:(c−逻辑推论) 假设 Σ 是命题逻辑公式集合, A 是命题逻辑公式, 定义 $\Sigma\models_c A$ 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 Σ 是命题逻辑公式集合, A 是命题逻辑公式,则

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

证明: 根据 c-可证的定义, 只需证明命题直觉主义逻辑证明系统的每个规则都是可靠的.

规则$\frac{\Sigma,A\vdash B \text{ 且 } \Sigma,A\vdash\neg B}{\Sigma\vdash\neg A}$ 是可靠的. 即

$$\text{若 } \Sigma,A\models_c B \text{ 及 } \Sigma,A\models_c\neg B, \text{ 则 } \Sigma\models_c\neg A.$$

是成立.

假设$\Sigma\models_c\neg A$ 不成立, 则存在分层模型 $\mathscr{K}=\langle V,R\rangle$ 及 $v\in V$,

$$\text{使得 } \Sigma^{\mathscr{K},v}=1 \text{ 但 } (\neg A)^{\mathscr{K},v}=0.$$

但是从 $(\neg A)^{\mathscr{K},v}=0$ 可知:

$$\text{存在} w\in V,\ vRw \text{ 使得 } A^{\mathscr{K},w}=1.$$

这时 $\Sigma^{\mathscr{K},w}=1$. 所以

$$(\Sigma\cup\{A\})^{\mathscr{K},w}=1.$$

但

$$\text{从 } \Sigma,A\models_c B \text{ 推出 } B^{\mathscr{K},w}=1.$$
$$\text{从 } \Sigma,A\models_c\neg B \text{ 推出 } (\neg B)^{\mathscr{K},w}=1.$$

这个矛盾表明规则 $(\neg+)$ 是可靠的.

规则$\frac{\Sigma\vdash A \text{ 且 } \Sigma\vdash A\to B}{\Sigma\vdash B}$ 是可靠的. 即

$$\text{若 } \Sigma\models_c A \text{ 及 } \Sigma\models_c A\to B, \text{ 则 } \Sigma\models_c B.$$

是成立.

对任意的分层模型 $\mathscr{K} = \langle V, R\rangle$ 及 $v \in V$, 若 $\Sigma^{\mathscr{K},v} = 1$, 以下证明 $B^{\mathscr{K},v} = 1$:

1. 从 $\Sigma \models_c A$, 可知 $A^{\mathscr{K},v} = 1$
2. 从 $\Sigma \models_c A \to B$, 可知
$$(A \to B)^{\mathscr{K},v} = 1,$$
所以当 $A^{\mathscr{K},v} = 1$ 时 $B^{\mathscr{K},v} = 1$

由此可知 $B^{\mathscr{K},v} = 1$.

同理可证其他证明规则的可靠性.

模态命题逻辑

性质

逻辑系统的特征: 语法,语义, 推演, 协调, 可靠, 完备.

以下介绍模态三个逻辑.

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.

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

例子

若 p, q 是命题变元， 则以下是公式:

1. $\Diamond\Diamond p$
2. $p \to \Diamond p$
3. $\neg p \to \neg\Diamond\Box q$

定义(推导规则)

假设 A, B 是公式, Σ 是公式集合, 定义以下规则

1. 规则一: $\frac{\Sigma\vdash\Box A}{\Sigma\vdash A}$
2. 规则二: $\frac{\Sigma\vdash\Box A \text{ 且 } \Sigma\vdash\Box(A\to B)}{\Sigma\vdash\Box B}$

3. 规则三: $\frac{\vdash A}{\vdash \Box A}$

4. 规则四: $\frac{\Sigma \vdash \Box A}{\Sigma \vdash \Box\Box A}$

5. 规则五: $\frac{\Sigma \vdash \Diamond A}{\Sigma \vdash \Box\Diamond A}$

三个模态推理系统:

1. T: 命题逻辑的推导规则, 规则一, 规则二, 规则三

2. S_4: T, 规则四

3. S_5: T, 规则五

可以定义推演三个关系:

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

给定公式集合 Σ:

1. 若存在公式 A, 使得 $\Sigma \nvdash_T A$, 则称 Σ 是 $T-$协调的.

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

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

例子
例子 $A \vdash_T \Diamond A$.
证明:

1. $\Box\neg A \vdash_T \Box\neg A$.

2. $\Box\neg A \vdash_T \neg A$.

3. $\neg\neg A \vdash_T \neg\Box\neg A$.

4. $A \vdash_T \neg\Box\neg A$.

即

$$A \vdash_T \Diamond A.$$

例子
$\vdash_T (\Box(A \to B) \wedge \Box(B \to A)) \leftrightarrow (\Box A \leftrightarrow \Box B)$.
$\vdash_T \Box(A \wedge B) \leftrightarrow (\Box A \wedge \Box B)$.
$\vdash_T \Diamond(A \vee B) \leftrightarrow (\Diamond A \vee \Diamond B)$.
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 $A^{\mathfrak{M},v}$:

1. 若 p 是命题变元, 则 $p^{\mathfrak{M},v} = v(p)$.

2. $(A \wedge B)^{\mathfrak{M},v} = 1$ 当且仅当

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

3. $(A \vee B)^{\mathfrak{M},v} = 1$ 当且仅当

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

4. $(A \to B)^{\mathfrak{M},v} = 1$ 当且仅当

$$\text{若 } A^{\mathfrak{M},v} = 1 \text{ 则 } B^{\mathfrak{M},v} = 1.$$

5. $(A \leftrightarrow B)^{\mathfrak{M},v} = 1$ 当且仅当

$$A^{\mathfrak{M},v} = 1 \text{ 等价于 } B^{\mathfrak{M},v} = 1.$$

6. $(\neg A)^{\mathfrak{M},v} = 1$ 当且仅当

$$A^{\mathfrak{M},v} = 0.$$

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

$$\text{对任意的 } v' \in V, \text{ 若 } vRv', \text{ 则 } A^{\mathfrak{M},v'} = 1.$$

$(\Diamond A)^{\mathfrak{M},v} = 1$ 当且仅当

$$\text{存在 } v' \in V, \text{ 使得 } vRv', \text{ 且 } A^{\mathfrak{M},v'} = 1.$$

以上是模态逻辑真值的定义.

对于命题逻辑联结词, 在一层的真值仅与本层相关.

“必然”意味着对每个情况都成立.

“存在”意味着有一个情况成立.

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

T-可靠性

针对模态命题逻辑模型类 $\mathscr{K}_T$:

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

定义: 对于公式集合 Σ 及公式 A, 有以下定义

1. **$T-$可满足的:**
   若存在 $\mathfrak{M} = \langle V, R\rangle \in \mathscr{K}_T$ 及 $v \in V$, 使得 $\Sigma^{\mathfrak{M},v} = 1$.

2. **$T-$有效的:**
   若对任意的 $\mathfrak{M} = \langle V, R\rangle \in \mathscr{K}_T$ 及 $v \in V$, 都有 $\Sigma^{\mathfrak{M},v} = 1$.

3. **$\Sigma \models_T A$:**
   若对任意的 $\mathfrak{M} = \langle V, R\rangle \in \mathscr{K}_T$ 及 $v \in V$, 当 $\Sigma^{\mathfrak{M},v} = 1$ 时 $A^{\mathfrak{M},v} = 1$.

定理($T-$可靠性): 对于任意的公式集合 Σ 及公式 A,

$$\text{若 } \Sigma \vdash_T A, \text{ 则 } \Sigma \models_T A.$$

证明: 只需证明以下事实:

1. $\frac{\Sigma \models_T \Box A}{\Sigma \models_T A}$.
   对任意 $\mathfrak{M} = \langle V, R\rangle \in \mathscr{K}_T$ 及 $v \in V$, 以下证明:

$$\text{当 } \Sigma^{\mathfrak{M},v} = 1 \text{ 时, } A^{\mathfrak{M},v} = 1.$$

   当 $\Sigma^{\mathfrak{M},v} = 1$ 时, 从 $\Sigma \models_T \Box A$ 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

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

2. $\frac{\Sigma \models_T \Box A \text{ 且 } \Sigma \models_T \Box(A \to B)}{\Sigma \models_T \Box B}$.
   对任意 $\mathfrak{M} = \langle V, R\rangle \in \mathscr{K}_T$ 及 $v \in V$, 以下证明:

$$\text{当 } \Sigma^{\mathfrak{M},v} = 1 \text{ 时, } (\Box B)^{\mathfrak{M},v} = 1.$$

   当 $\Sigma^{\mathfrak{M},v} = 1$ 时,

(a) 从 $\Sigma \models_T \Box A$. 可知

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

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

3. $\frac{\models_T A}{\models_T \Box A}$.

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

$$\models_T A$$

可知 $A^{\mathfrak{M},v} = 1$, 所以

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

所以上述规则是可靠的.

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 Σ 及公式 A, 有以下定义

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

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

3. $\Sigma \models_{S_4} A$:
   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 $A^{\mathfrak{M},v} = 1$.

定理(S_4-可靠性): 对于任意的公式集合 Σ 及公式 A,

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

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 Σ 及公式 A, 有以下定义

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

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

3. $\Sigma \models_{S_5} A$:
   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 Σ 及公式 A,

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

不可证

$\Diamond p \vdash_T \Box p$ 是否成立?

解答

不成立.

定义一个模型 $\mathfrak{M}$: 假设有两个赋值 v_1 及 v_2, 使得 $v_1(p) = 1$ 而 $v_2(p) = 0$; 规定 $v_1 R v_2$, $v_1 R v_1$, $v_2 R v_2$.

这时 $\Diamond p^{\mathfrak{M},v_1} = 1$, 但是 $\Box p^{\mathfrak{M},v_1} = 0$. 所以 $\Diamond p \nvdash_T \Box p$.

非平凡

模态 T 推演不是平凡的, 即

$$\nvdash_T p.$$

证明: 若 $\vdash_T p$ 则$\models_T p$, 因而对任意的模型 $\mathfrak{M} = \langle V, R\rangle$ 及 $v \in V$, 都有 $p^{\mathfrak{M},v} = 1$, 这意味着对任意的赋值 v, 都有 $v(p) = 1$. 这是不可能的. 所以 $\nvdash_T p$.

几何基础

高等几何:

研究几何体系而非仅仅证明几何定理.

欧氏几何:

Euclid《几何原本》

1. 23 个定义

2. 5 个公设

3. 5 个公理

4. 467 个命题

对当时的几何知识进行系统整理, 形成公理化思想.

23 个定义

1. 点是没有部分的.

2. 线只有长度而没有宽度.

3. 面只有长度与宽度.

4. $\cdots$

这是基本的几何概念.

都不像定义, 其实不是定义, 这正是公理化的"不定义"思想: 概念没有严格定义, 仅有以公理描述的性质, 通过对概念的解释, 建立各种形式的"语义".

解析几何中对点线圆等的定义正是对几何的一种解释:

点: (a, b), 其中 $a, b \in \mathbb{R}$.

线: $\{(x, y) \in \mathbb{R}^2 | ux + vy + w = 0\}$, 其中 $u, v, w \in \mathbb{R}$ 且 $uv \neq 0$..

圆: $\{(x, y) \in \mathbb{R}^2 | (x-u)^2 + (y-v)^2 = r^2\}$, 其中 $u, v, r \in \mathbb{R}$.

解析几何只是对平面几何的一种语义解释, 但并不是平面几何.

5 条公设

1. 经过两个不同的两点有且仅有一条直线.

2. 可以任意延长线段.

3. 以任意一点为圆心、任意长为半径，可作一个圆.

4. 直角都是相等的.

5. 两条直线被第三条直线所截,如果同侧两内角和小于两个直角, 则这两直线段的延长线必定相交.

5 条公理

1. 等量代换: 等于同一个量相等的两个量相等.

$$\text{若 } a = c \text{ 且 } b = c\text{，则 } a = b.$$

2. 等量加法: 等量加等量，其和相等.

$$若\ a=b\ 且\ c=d，则\ a+c=b+d.$$

3. 等量减法:等量减等量，其差相等.

$$若\ a=b\ 且\ c=d，则\ a-c=b-d$$

4. 移形叠合: 完全叠合的两个图形是全等的.

5. 全量大于部分: 全量大于部分.

$$a+b>a.$$

其中 $a,b,c,d>0$.

第五公设又称为平行公设, 它等价于:

在同一平面内，过直线外一点，有且只有一条直线与此直线平行.

平面几何公理集合除去第五公设称为绝对几何.

罗氏几何:

Lobachevsky将平行公设代以:

过直线外一点，至少有两条直线与此直线平行.

可以基于纯粹逻辑方法证明以下性质:

欧氏几何	罗氏几何
同一直线的垂线和斜线相交	同一直线的垂线和斜线不一定相交
垂直于同一直线的两条直线平行	垂直于同一直线的两条直线离散到无穷
三角形内角和等于 π	三角形内角之和小于 π
存在相似的多边形	不存在相似但不全等的多边形
过不在同一直线上的三点有且只有一个圆	过不在同一直线上的三点，不一定有一个圆

这两个几何中的结论是相互矛盾的. 相关研究

1. Bolyai

   1832 年, Bolyai 发表相关成果(双曲几何), 但一时不得支持.

2. Beltrami

   1868年，Beltrami 证明非欧几何相对相容性.

3. **Poincaré**

   Poincaré 圆盘

   直线是:

$$\text{垂直于圆周的圆弧或者直径}$$

黎曼几何:
Riemann改造平面几何,引进新公理:

1. 在同一平面内任何两条直线都有相交.

2. 直线可以无限延长，但总长度有限.

黎曼几何的模型是一个经过适当“改进”的球面:

1. 点: 一对对径点为一个点

2. 线: 大圆

独立证明:

1. 逻辑推理的可靠性

   若 $\Gamma \vdash A$ 则 $\Gamma \models A$.
   一阶逻辑是可靠的.

2. 平行公设是独立的

   (a) 几何推理是一阶的.

   (b) 解析几何满足绝对几何, 但不满足平行公设的反面,
   所以

   $$\text{绝对几何} \vdash \neg\text{平行公设}$$

   不成立.

   (c) 黎曼几何满足绝对几何, 但不满足平行公设的正面
   所以

   $$\text{绝对几何} \vdash \text{平行公设}$$

   不成立.

   (d) 平行公设独立于绝对几何: 绝对几何有两个解释, 分别满足平行公设的正面及反面, 所以是独立的.

欧氏几何与完备性

1. 不完备

2. Hilbert 给出完备的平面几何公理集合

几何应用:
欧氏几何、罗氏几何、黎曼几何都是相容的公理体系.

1. 欧氏几何:一般科学研究, Newton 的空间模型

2. 罗氏几何:宇宙学,原子物理学

3. 黎曼几何:航海航空

命题逻辑——两个推理系统

逻辑研究的基本特征
逻辑研究关注语法及语义之间的联系, 建立以下概念:

1. 公式

2. 公理,规则,推演序列,可证的,协调性

3. 真值,可满足性

4. 可靠性,完备性

命题逻辑的 Hilbert 推演系统

1. 公理:

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

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

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

2. 规则:

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

其中 A, B, C 是任意公式.

推演序列: 假设 Γ 是公式集合, 公式序列 $\langle A_1, A_2, \cdots, A_n \rangle$ 被称为 $\Gamma-$推演序列, 若对每个 A_i, 满足:

1. 或者 $A_i \in \Gamma$;

2. 或者 A_i 是公理;

3. 或者存在 $j,k < i$, 使得 A_k 是公式 $A_j \to A_i$.

可证性:

1. 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.

2. A 是 Γ 可证的记为 $\Gamma \vdash A$.

3. $\emptyset-$推演序列、 $\emptyset-$可证分别称为推演序列、可证.

4. $\emptyset \vdash A$ 记为 $\vdash A$.

例: $\langle A_1, A_2, A_3, A_4, A_5 \rangle$ 是一个推演序列, 其中

1. A_1: $p \to ((p \to p) \to p)$.

2. A_2: $(A_1) \to ((p \to (p \to p)) \to (p \to p))$.

3. A_3: $(p \to (p \to p)) \to (p \to p)$.

4. A_4: $p \to (p \to p)$.

5. A_5: $p \to p$.

所以$\vdash p \to p$.

单调性

性质:若 $\Gamma \vdash A$, 则 $\Gamma, B \vdash A$.

证明:

若 $\Gamma \vdash A$, 则存在有限序列 $\langle A_1, A_2, \cdots, A_n, A \rangle$ 使得

1. 或者 $A_i \in \Gamma$;

2. 或者 A_i 是公理;

3. 或者存在 $j,k < i$, 使得 A_k 是公式 $A_j \to A_i$.

则上述序列是 $\Gamma \cup \{B\}-$推演序列, 因而 $\Gamma, B \vdash A$.

命题逻辑的自然推演系统

1. 公理:

$$A \vdash A.$$

2. 规则:

(a) $\frac{\Sigma \vdash A}{\Sigma, \Sigma' \vdash A}$. 单调性

(b) $\frac{\Sigma, \neg A \vdash B \text{ 且 } \Sigma, \neg A \vdash \neg B}{\Sigma \vdash A}$. 反证法

(c) $\frac{\Sigma \vdash A \text{ 且 } \Sigma \vdash A \to B}{\Sigma \vdash B}$. 三段论

(d) $\frac{\Sigma, A \vdash B}{\Sigma \vdash A \to B}$. 演绎定理

(e) $\frac{\Sigma \vdash A \wedge B}{\Sigma \vdash A}$, $\frac{\Sigma \vdash A \wedge B}{\Sigma \vdash B}$.

(f) $\frac{\Sigma \vdash A \text{ 且 } \Sigma \vdash B}{\Sigma \vdash A \wedge B}$.

(g) $\frac{\Sigma, A \vdash C \text{ 且 } \Sigma, B \vdash C}{\Sigma, A \vee B \vdash C}$.

(h) $\frac{\Sigma \vdash A}{\Sigma \vdash A \vee B}$, $\frac{\Sigma \vdash A}{\Sigma \vdash B \vee A}$.

(i) $\frac{\Sigma \vdash A \leftrightarrow B \text{ 且 } \Sigma \vdash A}{\Sigma \vdash B}$, $\frac{\Sigma \vdash A \leftrightarrow B \text{ 且 } \Sigma \vdash B}{\Sigma \vdash A}$.

(j) $\frac{\Sigma, A \vdash B \text{ 且 } \Sigma, B \vdash A}{\Sigma \vdash A \leftrightarrow B}$.

其中Σ, Σ' 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: 以下是一个推演序列:

1. $p \vdash p$
2. $\vdash p \to p$

所以$\vdash p \to p$.

例: 以下是一个推演序列:

1. $S_1 : \neg A \vdash \neg A$
2. $S_2 : \neg A, \neg\neg A \vdash \neg A$
3. $S_3 : \neg\neg A \vdash \neg\neg A$
4. $S_4 : \neg A, \neg\neg A \vdash \neg\neg A$
5. $S_5 : \neg\neg A \vdash A$

所以 $\neg\neg A \vdash A$.

协调性

给定命题逻辑的公式集合 Σ, 称:

1. Σ 是不协调的:
   存在命题逻辑公式 A, 使得

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

2. Σ 是协调的:
   Σ 不是不协调的.

可满足

1. 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 $v(A) = 1$.
2. 公式集合的真值
   假设 Γ 是一个公式集合, 定义 $v(\Gamma) = 1$ 为

$$\text{对每个 } A \in \Gamma, \text{ 都有 } v(A) = 1.$$

3. 集合与公式
   假设 Γ 是一个公式集合, A 是公式, 定义 $\Gamma \models A$ 为

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

解释与赋值

定义3.1(解释)

给定一个一阶语言 $\mathscr{L}$. 语言 $\mathscr{L}$ 的解释 I 是指以下四元组.

$$\langle D^I, \{a^I | a \in \mathscr{L}_1\}, \{f^I | f \in \mathscr{L}_2\}, \{P^I | P \in \mathscr{L}_3\} \rangle$$

其中

1. $\mathscr{L}_1$ 是$\mathscr{L}$ 的常元构成的子集.
2. $\mathscr{L}_2$ 是 $\mathscr{L}$ 的函数符号构成的子集.
3. $\mathscr{L}_3$ 是 $\mathscr{L}$ 的谓词符号构成的子集.

4. D^I 是一个非空集合,称为论域.

5. $a^I \in D^I$, 即常元被解释为论域的一个元素.

6. 若 f 是 n 元函数符号, 则 f^I 是 D^I 上的 n 元函数;

7. 若 P 是 n 元关系符号, 则 P^I 是 D^I 上的 n 元关系.

8. 若 $\equiv \in \mathscr{L}$, 则 $\equiv$ 的解释 $\equiv^I$ 是 D^I 上的“等于”关系.

若语言中常元、函数符号、关系符号都仅有有限多个, 即

$$\mathscr{L} = \{a_1, \cdots a_k,\ f_1, \cdots, f_n,\ P_1, \cdots, P_m\}$$

则解释 I 可以记为:

$$\langle D^I, a_1^I, \cdots a_k^I, f_1^I, \cdots, f_n^I, P_1^I, \cdots, P_m^I \rangle$$

解释 I 的论域 D^I 也被记为 $|I|$.

例3.1

假设 $\mathscr{L} = \emptyset$, A 是任意一个非空集合, 则 $\langle A \rangle$ 是 $\mathscr{L}$ 的一个解释.

例3.2

假设 $\mathscr{L} = \{P\}$. 其中 P 是二元谓词符号. 则

$$\langle \mathbb{R}, < \rangle$$

是 $\mathscr{L}$ 的一个解释. 其中

1. $\mathbb{R}$ 是实数集合.

2. “$<$” 是实数集合上“小于”关系.

例3.3

假设 $\mathscr{L} = \{c, f\}$. 其中 c 是常元, f 是一元函数符号. 则

$$\langle \mathbb{N}, 0, \sigma \rangle$$

是 $\mathscr{L}$ 的一个解释. 其中

1. $\mathbb{N}$ 是自然数集合.

2. 0 是自然数零.

3. σ 是自然数集合上的后继函数:

$$\begin{array}{rccc} \sigma: & \mathbb{N} & \to & \mathbb{N}, \\ & n & \mapsto & n+1. \end{array}$$

以下的

$$\langle \mathbb{N} \cup \{-1\}, -1, \tau \rangle$$

也是$\mathscr{L}$ 的一个解释. 其中

1. $\mathbb{N}$ 是自然数集合..

2. $-1 \in \mathbb{R}$ 是一个负整数.

3. τ 是以下函数:

$$\begin{array}{rccc} \tau: & \mathbb{N} \cup \{-1\} & \to & \mathbb{N} \cup \{-1\}, \\ & n & \mapsto & n+1. \end{array}$$

例3.4

假设 $\mathscr{L} = \{0, 1, +, \cdot, <, =\}$ 是算术语言, $\mathbb{N}$ 是自然数集合, 则

$$\langle \mathbb{N}, 0, 1, +, \cdot, <, = \rangle$$

是 $\mathscr{L}$ 的一个解释.

定义3.2(赋值)

给定一阶语言 $\mathscr{L}$ 及它的解释 I, 由所有变元构成的集合 $var_{\mathscr{L}}$

$$var_{\mathscr{L}} = \{x, y, z, x_1, y_1, z_1, \cdots\}$$

到解释 I 的论域 D^I 的一个函数v 称为 I 的一个赋值.

$$\begin{array}{rccc} v: & var_{\mathscr{L}} & \to & D^I, \\ & x & \mapsto & v(x) \in D^I. \end{array}$$

定义3.4(项的值)

给定一阶语言 $\mathscr{L}$ 及它的一个解释 I, 假设 v 是解释 I 的一个赋值, t 是一个项, 如下定义 t 在 I 及 v 之下的值 $v^I(t)$:

1. 若 t 是变元 x, 则$v^I(t) = v(x)$.

2. 若 t 是常元 a, 则 $v^I(t) = a^I$.

3. 若 t 是项 $f(t_1, \cdots, t_n)$, 其中 f 是 n 元函数符号, $t_1, \cdots, t_n$ 是项, 则

$$v^I(t) = f^I(v^I(t_1), \cdots, v^I(t_n)).$$

例3.6

假设一阶语言 $\mathscr{L}=\{a,f,g,P\}$, 其中 a 是常元, f,g 是二元函数符号, P 是二元谓词符号. 定义一个解释 $I=\langle D^I,a^I,f^I,g^I,P^I\rangle$： D^I 是自然数集合,
$a^I=2$,
f^I 是自然数加法函数,
g^I 是自然数乘法函数,
P^I 是自然数小于关系.

假设 v 是 I 的一个赋值, 使得 $v(x)=1$.

以下计算项t: $f(g(a,x),a)$ 在 I 及 v 之下的值. 计算方式一

$$
\begin{aligned}
& v^I(t) \\
&= v^I(f(g(a,x),a)) \\
&= f^I(v^I(g(a,x)),v^I(a)) \\
&= f^I(g^I(v^I(a),v^I(x)),v^I(a)) \\
&= f^I(g^I(a^I,v(x)),a^I) \\
&= f^I(g^I(2,1),2) \\
&= f^I((2\cdot 1),2) \\
&= (2\cdot 1)+2 \\
&= 4
\end{aligned}
$$

计算方式二

$$
\begin{aligned}
& v^I(f(g(a,x),a)) \\
&= v^I(f(y,a)^y_{g(a,x)}) \\
&= 4 \\
&= v[y/2]^I(f(y,a)) \\
&= v[y/v^I(g(a,x))]^I(f(y,a)).
\end{aligned}
$$

定理3.1(项取值的存在唯一性)

给定一阶语言 $\mathscr{L}$ 及它的一个解释 I. 假设 v 是解释 I 的一个赋值, t 是一个项. 则 $v^I(t)\in D^I$, 且是唯一的.

定义3.5(公式的值)

给定一阶语言 $\mathscr{L}$ 及它的一个解释 I, 假设 v 是解释 I 的一个赋值, A 是一个公式, 如下定义公式 A 在 I 及 v 之下的值 $v^I(A)$:

1. 若 A 是原子公式 $P(t_1,\cdots,t_n)$, 其中 P 是 n 元谓词符号, $t_1,\cdots,t_n$ 是项, 则

$$v^I(A)=P^I(v^I(t_1),\cdots,v^I(t_n)).$$

2. 若 A 是公式 $\neg B$, 其中 B 是公式, 则

$$v^I(A) = \neg v^I(B).$$

3. 若 A 是公式 $B \to C$, 其中 B, C 是公式, 则

$$v^I(A) = v^I(B) \to v^I(C).$$

4. 若 A 是公式 $\forall x B$, 其中 B 是公式, x 是变元, 则

$$v^I(A) = \begin{cases} 1, & \text{若对于任意的 } d \in D^I, v[x/d]^I(B) = 1, \\ 0, & \text{否则}. \end{cases}$$

例3.7

对于上述例子, 计算

$$v^I(\forall x P(g(x, a), f(a, a))).$$

1. 基于定义

记 A 为 $P(g(x, a), f(a, a))$. 对于公式 A, 在 $v_1(x) = 0$ 时是成立的,而当 $v_2(x) = 2$ 时是不成立的.

所以

$$v[x/0]^I(A) = 1 \text{ 且 } v[x/2]^I(A) = 0.$$

根据全称量词的定义可知

$$v^I(\forall x P(g(x, a), f(a, a))) = 0.$$

2. 代入计算

假设 B 公式 $\forall x P(g(x, a), y)$.

考虑赋值

$$v' = v[y/4] = v[y/v^I(f(a, a))],$$

从

$$v^I(B) = 0,$$

可知

$$v^I(B^y_{f(a,a)}) = 0,$$

即

$$v^I(\forall x P(g(x, a), f(a, a))) = 0.$$

例3.8

给定一阶语言 $\mathscr{L}$. 假设 x, y 是两个不同的变元, P 是该语言的二元关系符号. 则对该语言的任意的解释 I 及 I 的任意赋值 v, 都有

$$v^I(\forall x \forall y P(x, y)) = v^I(\forall y \forall x P(x, y)).$$

证明:

1. 假设 $v^I(\forall x \forall y P(x, y)) = 1$, 根据定义可知:

   $$\text{对任意的 } d_1 \in D^I\text{: } v[x/d_1]^I(\forall y P(x, y)) = 1.$$

   由此可知

   $$\text{对任意的 } d_1, d_2 \in D^I\text{: } v[x/d_1][y/d_2]^I(P(x, y)) = 1.$$

   即对任意的 $d_1, d_2 \in D^I$ 都有 $P^I(d_1, d_2) = 1$.

   可证 $v^I(\forall x \forall y P(x, y)) = 1$ 当且仅当对任意的 $d_1, d_2 \in D^I$ 都有 $P^I(d_1, d_2) = 1$.

2. 同理可知: $v^I(\forall y \forall x P(x, y)) = 1$ 当且仅当对任意的 $d_2, d_1 \in D^I$ 都有 $P^I(d_2, d_1) = 1$.

由此可得上述结论.

定理3.2(公式真值的存在唯一性)

给定一阶语言 $\mathscr{L}$ 及它的一个解释 I, 而 v 是解释 I 的一个赋值, A 是一个公式. 则$v^I(A) \in \{0, 1\}$, 且是唯一的.