数理逻辑

杨睿之

复旦大学哲学学院

2021 年秋季

前情提要

- 命题逻辑的语言：符号、合式公式
- 命题语言的唯一可读性
- 命题逻辑的一个公理系统

希尔伯特式的命题逻辑公理系统

公理集 Λ：

(A1) $\alpha \to \beta \to \alpha$

(A2) $(\alpha \to \beta \to \gamma) \to (\alpha \to \beta) \to (\alpha \to \gamma)$

(A3) $(\neg\beta \to \neg\alpha) \to (\neg\beta \to \alpha) \to \beta$

分离规则（*modus ponens*,MP)：

从 $\alpha, \alpha \to \beta$ 可以推出 β

希尔伯特系统的证明

定义 (推演/证明/演绎（deduction）)

从公式集 Γ 到公式 φ 的一个推演 （或 证明 或 演绎 ）是一个有穷的公式序列 $\langle \alpha_0, \alpha_1, \ldots, \alpha_n \rangle$，满足 $\alpha_n = \varphi$，并且对所有 $i \leq n$，或者

(a) α_i 属于 $\Gamma \cup \Lambda$；或者

(b) 存在 $j, k < i$, 使得 $\alpha_k = \alpha_j \to \alpha_i$

一些元定理

引理

对任意合式公式 α 有，$\vdash \alpha \to \alpha$

证明.

对每个公式 α，有如下推演：

1. $(\alpha \to (\alpha \to \alpha) \to \alpha) \to (\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha)$
2. $\alpha \to (\alpha \to \alpha) \to \alpha$
3. $(\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha)$
4. $\alpha \to (\alpha \to \alpha)$
5. $\alpha \to \alpha$

引理

对任意合式公式 α 有，$\vdash \alpha \to \alpha$

证明.

对每个公式 α，有如下推演：

1. $(\alpha \to (\alpha \to \alpha) \to \alpha) \to (\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha)$
2. $\alpha \to (\alpha \to \alpha) \to \alpha$
3. $(\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha)$
4. $\alpha \to (\alpha \to \alpha)$
5. $\alpha \to \alpha$

引理

对任意合式公式 α 有，$\vdash \alpha \to \alpha$

证明.

对每个公式 α，有如下推演：

1. $(\alpha \to (\alpha \to \alpha) \to \alpha) \to (\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha)$
2. $\alpha \to (\alpha \to \alpha) \to \alpha$
3. $(\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha)$
4. $\alpha \to (\alpha \to \alpha)$
5. $\alpha \to \alpha$

一些元定理

引理

对任意合式公式 α 有，$\vdash \alpha \to \alpha$

证明.

对每个公式 α，有如下推演：

1. $(\alpha \to (\alpha \to \alpha) \to \alpha) \to (\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha)$
2. $\alpha \to (\alpha \to \alpha) \to \alpha$
3. $(\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha)$
4. $\alpha \to (\alpha \to \alpha)$
5. $\alpha \to \alpha$

一些元定理

引理

对任意合式公式 α 有，$\vdash \alpha \rightarrow \alpha$

证明.

对每个公式 α，有如下推演：

1. $(\alpha \rightarrow (\alpha \rightarrow \alpha) \rightarrow \alpha) \rightarrow (\alpha \rightarrow (\alpha \rightarrow \alpha)) \rightarrow (\alpha \rightarrow \alpha)$
2. $\alpha \rightarrow (\alpha \rightarrow \alpha) \rightarrow \alpha$
3. $(\alpha \rightarrow (\alpha \rightarrow \alpha)) \rightarrow (\alpha \rightarrow \alpha)$
4. $\alpha \rightarrow (\alpha \rightarrow \alpha)$
5. $\alpha \rightarrow \alpha$

一些元定理

引理

对任意合式公式 α 有，$\vdash \alpha \to \alpha$

证明.

对每个公式 α，有如下推演：

1. $(\alpha \to (\alpha \to \alpha) \to \alpha) \to (\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha)$
2. $\alpha \to (\alpha \to \alpha) \to \alpha$
3. $(\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha)$
4. $\alpha \to (\alpha \to \alpha)$
5. $\alpha \to \alpha$

一些元定理

引理

对任意合式公式 α 有，$\vdash \alpha \to \alpha$

证明.

对每个公式 α，有如下推演：

1. $(\alpha \to (\alpha \to \alpha) \to \alpha) \to (\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha)$
2. $\alpha \to (\alpha \to \alpha) \to \alpha$
3. $(\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha)$
4. $\alpha \to (\alpha \to \alpha)$
5. $\alpha \to \alpha$

一些元定理

定理 (演绎定理)

$\Gamma \cup \{\alpha\} \vdash \beta$，当且仅当 $\Gamma \vdash \alpha \to \beta$

证明.

把已有的推演改造成我们想要的推演

$(\Leftarrow)$

$(\Rightarrow)$

一些元定理

定理 (演绎定理)

$\Gamma \cup \{\alpha\} \vdash \beta$，当且仅当 $\Gamma \vdash \alpha \to \beta$

证明.

把已有的推演改造成我们想要的推演

($\Leftarrow$)

($\Rightarrow$)

一些元定理

定理 (演绎定理)

$\Gamma \cup \{\alpha\} \vdash \beta$，当且仅当 $\Gamma \vdash \alpha \to \beta$

证明.

把已有的推演改造成我们想要的推演

($\Leftarrow$)

($\Rightarrow$)

一些元定理

定理 (演绎定理)

$\Gamma \cup \{\alpha\} \vdash \beta$，当且仅当 $\Gamma \vdash \alpha \to \beta$

证明.

把已有的推演改造成我们想要的推演

($\Leftarrow$)

($\Rightarrow$)

命题逻辑的语义

命题逻辑的语义

命题逻辑中，命题是语义的最小载体。且经典命题逻辑只关心“真”、“假”

定义 (真值指派)

我们说 v 是一个 真值指派，当且仅当 v 是以由命题符号组成的集合 $\mathcal{A}$ 为定义域、以真值集合 $\{0,1\}$ 为值域的函数

$v : \mathcal{A} \to \{0,1\}$

命题逻辑的语义

命题逻辑中，命题是语义的最小载体。且经典命题逻辑只关心“真”、“假”

定义 (真值指派)

我们说 v 是一个 真值指派 ，当且仅当 v 是以由命题符号组成的集合 $\mathscr{A}$ 为定义域、以真值集合 $\{0,1\}$ 为值域的函数 $v:\mathscr{A}\to\{0,1\}$

命题逻辑的语义

命题联词的语义何以体现?

定义 (命题联词的语义)

任给真值指派 v，我们定义 v 的扩展 $\bar{v} : \mathcal{F} \to \{0, 1\}$

0 对 $A \in \mathcal{A}$，$\bar{v}(A) = v(A)$

1 对任意公式 α, β,

$$\bar{v}(\neg\alpha) = \begin{cases} 1 & 若\ \bar{v}(\alpha) = 0 \\ 0 & 否则 \end{cases}$$

命题逻辑的语义

命题联词的语义何以体现?

定义 (命题联词的语义)

任给真值指派 v，我们定义 v 的扩展 $\bar{v} : \mathcal{F} \to \{0, 1\}$

0. 对 $A \in \mathcal{A}$，$\bar{v}(A) = v(A)$
1. 对任意公式 α, β,

$$\bar{v}(\alpha \wedge \beta) = \begin{cases} 1 & \text{若 } \bar{v}(\alpha) = 1 \text{ 并且 } \bar{v}(\beta) = 1 \\ 0 & \text{否则} \end{cases}$$

命题逻辑的语义

命题联词的语义何以体现?

定义 (命题联词的语义)

任给真值指派 v，我们定义 v 的扩展 $\bar{v} : \mathcal{F} \to \{0, 1\}$

0. 对 $A \in \mathcal{A}$，$\bar{v}(A) = v(A)$
1. 对任意公式 α, β,

$$\bar{v}(\alpha \vee \beta) = \begin{cases} 1 & \text{若 } \bar{v}(\alpha) = 1 \text{ 或者 } \bar{v}(\beta) = 1 \\ 0 & \text{否则} \end{cases}$$

命题逻辑的语义

命题联词的语义何以体现?

定义 (命题联词的语义)

任给真值指派 v，我们定义 v 的扩展 $\bar{v}: \mathcal{F} \to \{0, 1\}$

0. 对 $A \in \mathcal{A}$，$\bar{v}(A) = v(A)$
1. 对任意公式 α, β，

$$\bar{v}(\alpha \to \beta) = \begin{cases} 0 & \text{若 } \bar{v}(\alpha) = 1 \text{ 并且 } \bar{v}(\beta) = 0 \\ 1 & \text{否则} \end{cases}$$

命题逻辑的语义

命题联词的语义何以体现?

定义 (命题联词的语义)

任给真值指派 v，我们定义 v 的扩展 $\bar{v} : \mathcal{F} \to \{0, 1\}$

0. 对 $A \in \mathcal{A}$，$\bar{v}(A) = v(A)$
1. 对任意公式 α, β,

$$\bar{v}(\alpha \leftrightarrow \beta) = \begin{cases} 1 & \text{若 } \bar{v}(\alpha) = \bar{v}(\beta) \\ 0 & \text{否则} \end{cases}$$

命题逻辑的语义

注意:

- 对 $\bar{v}$ 的定义是一个递归定义
  - 它告诉我们，给定一个真值指派，如何计算一个具体公式的真值

命题联词

我们对诸命题联词的语义解释，就体现在对“如何从 v 得到 $\bar{v}$”的定义。

例如：

$$\bar{v}(\alpha \to \beta) = \begin{cases} 0 & \text{若 } \bar{v}(\alpha) = 1 \text{ 并且 } \bar{v}(\beta) = 0 \\ 1 & \text{否则} \end{cases}$$

命题联词

我们对诸命题联词的语义解释，就体现在对“如何从 v 得到 $\bar{v}$ ”的定义。

例如：

$$\bar{v}(\alpha \to \beta) = \begin{cases} 0 & 若\ \bar{v}(\alpha) = 1\ 并且\ \bar{v}(\beta) = 0 \\ 1 & 否则 \end{cases}$$

命题联词

或用真值表表示:

$\bar{v}(\alpha)$	$\bar{v}(\beta)$	$\bar{v}(\alpha \to \beta)$
1	1	1
0	1	1
1	0	0
0	0	1

命题联词

或用真值表表示:

x	y	$B_{\to}(x, y)$
1	1	1
0	1	1
1	0	0
0	0	1

命题联词

我们赋予二元联词 $\to$ 的意义就是一个二元函数:

$$B_{\to} : \{0, 1\}^2 \to \{0, 1\}$$

而赋予一元联词 $\neg$ 的意义是一个一元函数

$$B_{\neg} : \{0, 1\} \to \{0, 1\}$$

我们称这种以 $\{0,1\}$（或其任意 n 维卡氏积）为定义域和值域的函数为 布尔函数 （Boolean function）

命题联词

我们赋予二元联词 $\to$ 的意义就是一个二元函数：

$$B_{\to} : \{0,1\}^2 \to \{0,1\}$$

而赋予一元联词 $\neg$ 的意义是一个一元函数

$$B_{\neg} : \{0,1\} \to \{0,1\}$$

我们称这种以 $\{0,1\}$（或其任意 n 维卡氏积）为定义域和值域的函数为 布尔函数 （Boolean function）

命题联词

我们赋予二元联词 $\to$ 的意义就是一个二元函数：

$$B_{\to} : \{0, 1\}^2 \to \{0, 1\}$$

而赋予一元联词 $\neg$ 的意义是一个一元函数

$$B_{\neg} : \{0, 1\} \to \{0, 1\}$$

我们称这种以 $\{0,1\}$（或其任意 n 维卡氏积）为定义域和值域的函数为 布尔函数　(Boolean function)

命题联词

问题：

- 有多少种一元联词?
- 有多少种二元联词?
- 有多少种 n 元联词?

命题联词

问题:

- 有多少种不同意义的一元联词?
- 有多少种二元联词?
- 有多少种 n 元联词?

命题联词

问题：

- 有多少种一元布尔函数？
- 有多少种二元联词？
- 有多少种 n 元联词？

命题联词

问题:

- 有多少种一元联词?
- 有多少种二元联词?
- 有多少种 n 元联词?

问题:

- 有多少种一元联词?
- 有多少种二元联词?
- 有多少种 n 元联词?

命题联词

命题联词的合成

x	y	$B_\neg(x)$	$B_\vee(x,y)$	$B_\top(x)$	$B_\downarrow(x,y)$
1	1	0	1	1	0
0	1	1	1	1	0
1	0		1		0
0	0		0		1

则 $B_\top(x) = B_\vee(B_\neg(x), x)$，而 $B_\downarrow(x,y) = B_\neg(B_\vee(x,y))$

命题联词

假设 α 是一个至多含有命题符号 $A_1, \ldots, A_n$ 的合式公式，那么 α 就决定了一个 n 元布尔函数 $B_\alpha^n : \{0,1\}^n \to \{0,1\}$

$v(A_1), \ldots, v(A_n)$		$\bar{v}(\alpha)$
$v_1(A_1), \ldots, v_1(A_n)$	$= 1, \ldots, 1$	$\bar{v}_1(\alpha)$
$\ldots$	$\ldots$	$\ldots$
$v_{2^n}(A_1), \ldots, v_{2^n}(A_n)$	$= 0, \ldots, 0$	$\bar{v}_{2^n}(\alpha)$

命题联词

假设 α 是一个至多含有命题符号 $A_1, \ldots, A_n$ 的合式公式，那么 α 就决定了一个 n 元布尔函数 $B_\alpha^n : \{0,1\}^n \to \{0,1\}$

$v(A_1), \ldots, v(A_n)$	$x_1, \ldots, x_n$	$B_\alpha^n(x_1, \ldots, x_n)$	$\bar{v}(\alpha)$
$v_1(A_1), \ldots, v_1(A_n)$	$= 1, \ldots, 1$	$B_\alpha^n(1, \ldots, 1) =$	$\bar{v}_1(\alpha)$
$\cdots$	$\cdots$	$\cdots$	$\cdots$
$v_{2^n}(A_1), \ldots, v_{2^n}(A_n)$	$= 0, \ldots, 0$	$B_\alpha^n(0, \ldots, 0) =$	$\bar{v}_{2^n}(\alpha)$

定义

令 α 是至多含有命题符号 $A_1, \ldots, A_n$ 的公式。定义函数

$B_\alpha^n : \{0,1\}^n \to \{0,1\}$，使得

$$B_\alpha^n(x_1, \ldots, x_n) = \bar{v}(\alpha)$$

其中，$v(A_i) = x_i \quad (1 \leq i \leq n)$

命题联词

一个命题逻辑公式 α 在意义上等同于 $\star(A_1, \ldots, A_n)$，其中 $\star$ 是某个 n 元命题联词。

问题：是否对每个 n 元命题联词，我们都可以找到一个具有相同意义的合式公式？即 $\neg$、$\wedge$、$\vee$、$\rightarrow$ 和 $\leftrightarrow$ 是否够用？也即，是否只用 $B_{\neg}$、$B_{\wedge}$、$B_{\vee}$、$B_{\rightarrow}$ 和 $B_{\leftrightarrow}$ 就可以通过复合得到任意 n 元布尔函数？

命题联词

一个命题逻辑公式 α 在意义上等同于 $\star(A_1, \ldots, A_n)$，其中 $\star$ 是某个 n 元命题联词。

问题: 是否对每个 n 元命题联词，我们都可以找到一个具有相同意义的合式公式？即 $\neg$、$\wedge$、$\vee$、$\rightarrow$ 和 $\leftrightarrow$ 是否够用？

也即，是否只用 $B_{\neg}$、$B_{\wedge}$、$B_{\vee}$、$B_{\rightarrow}$ 和 $B_{\leftrightarrow}$ 就可以通过复合得到任意 n 元布尔函数？

命题联词

一个命题逻辑公式 α 在意义上等同于 $\star(A_1, \ldots, A_n)$，其中 $\star$ 是某个 n 元命题联词。

问题：是否对每个 n 元命题联词，我们都可以找到一个具有相同意义的合式公式？即 $\neg$、$\wedge$、$\vee$、$\rightarrow$ 和 $\leftrightarrow$ 是否够用？也即，是否只用 $B_\neg$、$B_\wedge$、$B_\vee$、$B_\rightarrow$ 和 $B_\leftrightarrow$ 就可以通过复合得到任意 n 元布尔函数？

定理

对任意 n 元布尔函数 $G:\{0,1\}^n \to \{0,1\}$（$n \geq 1$），都存在一个命题逻辑合式公式 α，使得 $B_\alpha^n = G$

命题联词

例:

x_1	x_2	x_3	$M(x_1, x_2, x_3)$
1	1	1	1
0	1	1	1
1	0	1	1
0	0	1	0
1	1	0	1
0	1	0	0
1	0	0	0
0	0	0	0

令

$$\begin{aligned}\alpha = \quad & (A_1 \wedge A_2 \wedge A_3) \\ & \vee (\neg A_1 \wedge A_2 \wedge A_3) \\ & \vee (A_1 \wedge \neg A_2 \wedge A_3) \\ & \vee (A_1 \wedge A_2 \wedge \neg A_3)\end{aligned}$$

检验: $M = B_\alpha^3$

命题联词

例:

x_1	x_2	x_3	$M(x_1, x_2, x_3)$
1	1	1	1
0	1	1	1
1	0	1	1
0	0	1	0
1	1	0	1
0	1	0	0
1	0	0	0
0	0	0	0

令

$$\begin{aligned} \alpha = \quad & (A_1 \wedge A_2 \wedge A_3) \\ & \vee (\neg A_1 \wedge A_2 \wedge A_3) \\ & \vee (A_1 \wedge \neg A_2 \wedge A_3) \\ & \vee (A_1 \wedge A_2 \wedge \neg A_3) \end{aligned}$$

检验: $M = B_\alpha^3$

命题联词

例:

x_1	x_2	x_3	$M(x_1, x_2, x_3)$
1	1	1	1
0	1	1	1
1	0	1	1
0	0	1	0
1	1	0	1
0	1	0	0
1	0	0	0
0	0	0	0

令

$$\begin{aligned}\alpha = \ & (A_1 \wedge A_2 \wedge A_3) \\ & \vee (\neg A_1 \wedge A_2 \wedge A_3) \\ & \vee (A_1 \wedge \neg A_2 \wedge A_3) \\ & \vee (A_1 \wedge A_2 \wedge \neg A_3)\end{aligned}$$

检验: $M = B_\alpha^3$

证明.

对一般情况的证明

习题

- 2.3.8*, 2.3.9
- 2.5.1, 2.5.5

下期预告

- 命题逻辑的语义（续）
- 命题逻辑公理系统的可靠性与完全性