希尔伯特风格公理系统

课堂笔记整理：顾小伊

2008年12月7日

语法

给定有限或可数集合

$$X = \{x_1, x_2, \ldots, x_n, \ldots\}\text{，}$$

命题P的产生式规则为

$$P \to X \mid P \supset P \mid (P)\text{；}$$

或者写成下面完整的形式文法

$$G \equiv (\Sigma, T, S, Q)\text{；}$$

其中

$$\Sigma = X \cup \{\supset\} \cup \{P\} \cup \{(\} \cup \{)\}\text{，}\quad N = \{P\}\text{，}\quad S = \{P\}\text{。}$$

我们规定$\supset$是右结合的，以下形如$P \supset (Q \supset R)$的命题常简写为$P \supset Q \supset R$。

在命题P上定义的函数经常呈现递归的形式。对于命题P、Q，可递归定义替换函数$[Q/x]P$

$$[Q/x]y = \begin{cases} Q, & \text{若}x = y\text{；} \\ y, & \text{否则；} \end{cases}$$

$$[Q/x](P_1 \supset P_2) = [Q/x]P_1 \supset [Q/x]P_2\text{。}$$

进一步，符号$[Q_1/x_1, \ldots, Q_n/x_n]P$代表对命题$P$中$n$个变量的同时替换。

公理和证明

在如上所引入的形式文法上，我们引入如下两条“公理”：

1. $P \supset (Q \supset P)$

2. $(P \supset (Q \supset R)) \supset ((P \supset Q) \supset (P \supset R))$

其中的变量P，Q，R称为变量模式，可以代表任意合法形式的命题。以下把加入了该公理的形式系统称为G。

将命题集合$\Gamma = \{P_1, P_2, \ldots, P_n, \ldots\}$称为环境，我们称命题$P$从环境$\Gamma$语法可证，记作$\Gamma \vdash P$，称为语法断言，是指存在一个有限的命题序列

$$Q_1, Q_2, \ldots, Q_n$$

其中$Q_n = P$，而且对于每个$Q_i (1 \le i \le n)$至少都满足下列三个条件中的一个：

1. $Q_i \in \Gamma$，

2. Q_i是一条公理，

3. 存在$j, k < i$，且$Q_k = Q_j \supset Q_i$。

最后一条规则称为MP规则。

根据公理1，我们立刻可以得到下面的

命题 1: $\{P\} \vdash Q \supset P$。

证明: 可构造如下序列作为证明：

$$P, P \supset (Q \supset P), Q \supset P\text{。}$$

证毕

如果对一个语法断言的证明存在，则有无穷多个。不难证明下面的序列同样是语法断言$\{P\} \vdash Q \supset P$的证明：

$$P, P, P \supset (Q \supset P), Q \supset P\text{。}$$

结合公理1和公理2，我们有

命题 2: $\vdash (P \supset Q) \supset (P \supset P)$。

证明: 可构造如下的序列：

$$P \supset (Q \supset P), (P \supset (Q \supset P)) \supset ((P \supset Q) \supset (P \supset P)), (P \supset Q) \supset (P \supset P)\text{。}$$

证毕

作为公理1，2的最后一个直接应用，我们证明

命题 3 (**同一律**): $\vdash P \supset P$。

证明: 把该序列的每一项写在一行：

1. $P \supset ((P \supset P) \supset P)$

2. $(P \supset ((P \supset P) \supset P)) \supset ((P \supset (P \supset P)) \supset (P \supset P))$

3. $(P \supset (P \supset P)) \supset (P \supset P)$

4. $P \supset (P \supset P)$

5. $P \supset P$

证毕

特别的，对任意的环境Γ，我们有$\Gamma \vdash P \supset P$。

直接利用公理1和公理2来证明语法断言一般非常麻烦和冗长，简化这种证明步骤可利用如下重要的

定理 4 (**演绎定理**): $\Gamma \cup \{P\} \vdash Q \Longleftrightarrow \Gamma \vdash P \supset Q$。

证明: 先证($\Leftarrow$)。假设有$\Gamma \vdash P \supset Q$，设该语法断言的证明序列是

$$Q_1, Q_2, \ldots, Q_n = P \supset Q。$$

因此，序列

$$Q_1, Q_2, \ldots, Q_n, P, Q$$

是语法断言$\Gamma \cup \{P\}$的证明。

再证($\Rightarrow$)。假设$\Gamma \cup \{P\} \vdash Q$，证明的目标是$\Gamma \vdash P \supset Q$。对$\Gamma \cup \{P\} \vdash Q$的证明长度$n$进行归纳：

（1）当$n = 1$时，有

$$Q_1 = Q。$$

分三种情况讨论：

1. 若Q是一个公理，可以构造如下的序列：

$$Q, Q \supset (P \supset Q), P \supset Q。$$

2. 若$Q = P$，由命题3，可以证明

$$\Gamma \vdash P \supset P。$$

3. 若$Q \in \Gamma$，可构造如下的序列：

$$Q, Q \supset (P \supset Q), P \supset Q。$$

（2）若$n > 1$，有证明序列

$$Q_1, Q_2, \ldots, Q_n = Q$$

我们仅仅在这里讨论MP，其它的和（1）中类似。由MP规则，存在$i, j < n$使得

$$Q_j = Q_i \supset Q$$

从归纳假设，可以得出

$$\begin{aligned} &\Gamma \cup \{P\} \vdash Q_i \Rightarrow \Gamma \vdash P \supset Q_i \\ &\Gamma \cup \{P\} \vdash Q_j \Rightarrow \Gamma \vdash P \supset Q_j \qquad (\text{即}\Gamma \vdash P \supset (Q_i \supset Q)) \end{aligned}$$

即有下面两个证明序列：

$$\begin{aligned} M_1, \ldots, M_s &= P \supset Q_i \\ N_1, \ldots, N_t &= P \supset (Q_i \supset Q)。 \end{aligned}$$

从而由此构建一个$P \supset Q$的证明序列

$$M_1, \ldots, M_s, N_1, \ldots, N_t, A_2, (P \supset Q_i) \supset (P \supset Q), P \supset Q。$$

其中$A_2 = (P \supset (Q_i \supset Q)) \supset ((P \supset Q_i) \supset (P \supset Q))$。 证毕

作为演绎定理的直接应用，我们证明

命题 5: $\{P, Q \supset (P \supset R)\} \vdash Q \supset R$。

证明: 只需要证明$\{P, Q \supset (P \supset R), Q\} \vdash R$。 证毕

为了扩展系统G，我们在系统G的产生式规则P中加入$\neg$得到

$$P \to X \mid P \supset P \mid (P) \mid \neg P$$

但是系统G的表达能力太弱了，因为许多逻辑演绎都不能有这个系统表达出来。所以，我们再引入一个公理：

3. $(\neg P \supset \neg Q) \supset (Q \supset P)$

以下把加入了公理集1、2、3得到的系统称作“L”。

利用公理3，我们可以证明

命题 6 (**否定前件律**): $\vdash \neg P \supset (P \supset Q)$。

证明: 由演绎定理，只需证明

$$\{\neg P\} \vdash P \supset Q。$$

该语法断言的一个证明序列是

$$\neg P \supset (\neg Q \supset \neg P), \neg P, \neg Q \supset \neg P, (\neg Q \supset \neg P) \supset (P \supset Q), P \supset Q。$$

证毕

公理3的另外一个重要的应用是证明重要的

命题 7 (**反证律**): 若$\Gamma \cup \{\neg P\} \vdash Q$且$\Gamma \cup \{\neg P\} \vdash \neg Q$，则$\Gamma \vdash P$。

证明: 由$\Gamma \cup \{\neg P\} \vdash Q$和$\Gamma \cup \{\neg P\} \vdash \neg Q$，我们可以分别写出两个语法断言的证明序列

$$M_1, \ldots, M_s = Q，$$
$$N_1, \ldots, N_t = \neg Q。$$

由此，利用上面证明的命题6，可写出语法断言

$$\Gamma \cup \{\neg P\} \vdash P$$

的证明序列

$$M_1, \ldots, M_s, N_1, \ldots, N_t, \neg Q \supset (Q \supset P), Q \supset P, P。$$

由演绎定理，我们有

$$\Gamma \cup \{\neg P\} \vdash P \Longrightarrow \Gamma \vdash \neg P \supset P。$$

因此只需证明

$$\Gamma \vdash (\neg P \supset P) \supset P，$$

即

$$\Gamma \cup \{\neg P \supset P\} \vdash P。$$

可构造如下该断言的证明序列

1. $\neg P \supset (P \supset \neg(\neg P \supset P))$

2. $(\neg P \supset (P \supset \neg(\neg P \supset P))) \supset ((\neg P \supset P) \supset (\neg P \supset \neg(\neg P \supset P)))$

3. $(\neg P \supset P) \supset (\neg P \supset \neg(\neg P \supset P))$

4. $\neg P \supset \neg(\neg P \supset P)$

5. $(\neg P \supset \neg(\neg P \supset P)) \supset ((\neg P \supset P) \supset P)$

6. $(\neg P \supset P) \supset P$

7. P

证毕

反证律的重要推论是如下的

命题 8 (**双重否定律**): $\{\neg\neg P\} \vdash P$。

证明: 只需证明$\{\neg\neg P, \neg P\} \vdash \neg P$和$\{\neg\neg P, \neg P\} \vdash \neg(\neg P)$。 证毕

和反证律形式相似的是如下的

命题 9 (**归谬律**): 若$\Gamma \cup \{P\} \vdash Q$且$\Gamma \cup \{P\} \vdash \neg Q$，则$\Gamma \vdash \neg P$。

证明: 由双重否定律，给定的条件相当于

$$\Gamma \cup \{\neg\neg P\} \vdash Q, \qquad \Gamma \cup \{\neg\neg P\} \vdash \neg Q。$$

由反证律立刻可得结论。 证毕

其它连接词可看成$\supset$和$\neg$的语法美化，特别的，对于连接词$\wedge$，$\vee$和$\leftrightarrow$，我们定义

$$\begin{aligned} P \wedge Q &\triangleq \neg(P \supset \neg Q) \\ P \vee Q &\triangleq \neg P \supset Q \\ P \leftrightarrow Q &\triangleq (P \supset Q) \wedge (Q \supset P) \end{aligned}$$

作为上述定义的一个直接应用，我们证明

命题 10 (**排中律**): $\Gamma \vdash P \vee \neg P$并且$\Gamma \vdash \neg P \vee P$。

证明: 只需要证明

$$\Gamma \vdash \neg P \supset \neg P \qquad \text{和} \qquad \Gamma \vdash \neg\neg P \supset P。$$

前者可利用同一律，后者利用双重否定律。 证毕

语义

回想一下前面的形式系统L的产生式规则

$$P \to X \mid P \supset P \mid (P) \mid \neg P$$

语义学的目的是确定在什么条件下命题P为“真”。为此，重新回忆一下布尔代数

$$B = (\{0,1,(,),\supset',\neg',P'\}, \{0,1,(,),\supset',\neg'\}, P', A),$$

其中

$$P' \to 0 \mid 1 \mid P' \supset' P' \mid \neg' P' \mid (P')。$$

我们的目的是把$\supset'$和$\neg'$都看成普通的算符，从而每个公式P'都可以“计算”到0或者1，为此，我们可以建立如下的计算法则

	$\neg'$
0	1
1	0

		$\supset'$
0	0	1
0	1	1
1	0	0
1	1	1

为了建立形式系统L和B的关系，我们定义一个*真值赋值函数*$\mathcal{V}_0$：

$$\mathcal{V}_0 : X \to \{0,1\}。$$

进一步，把映射$\mathcal{V}_0$扩张成从L的产生式规则P到系统B的产生式P'的映射$\mathcal{V} : P \to P'$

$$\mathcal{V}(X) = \mathcal{V}_0(X)$$
$$\mathcal{V}(\neg P) = \neg\prime\mathcal{V}(P)$$
$$\mathcal{V}(P_1 \supset P_2) = \mathcal{V}(P_1) \supset \prime\mathcal{V}(P_2)$$

以下称映射$\mathcal{V}$为赋值。

作为例子，我们证明如下的

命题 11: *对于任意的赋值$\mathcal{V}$，我们有$\mathcal{V}(x_1 \supset (x_2 \supset x_1))$=1。*

证明: 对所有可能的四种真值赋值函数$\mathcal{V}_0$枚举。例如，对于

$$\mathcal{V}_0(x_1) = 0 \qquad 且 \qquad \mathcal{V}_0(x_2) = 0,$$

有

$$\begin{aligned}
\mathcal{V}(x_1 \supset (x_2 \supset x_1)) &= \mathcal{V}(x_1) \supset' \mathcal{V}(x_2 \supset x_1) \\
&= \mathcal{V}_0(x_1) \supset' \mathcal{V}(x_2 \supset x_1) \\
&= 0 \supset' \mathcal{V}(x_2 \supset x_1) \\
&= 0 \supset' (\mathcal{V}(x_2) \supset' \mathcal{V}(x_1)) \\
&= 0 \supset' (\mathcal{V}_0(x_2) \supset' \mathcal{V}(x_1)) \\
&= 0 \supset' (0 \supset' \mathcal{V}(x_1)) \\
&= 0 \supset' (0 \supset' \mathcal{V}_0(x_1)) \\
&= 0 \supset' (0 \supset' 0)
\end{aligned}$$

不难计算得到最后公式的值为1。其它三种情况类似可证。 证毕

一般的，如果命题P对任意的赋值$\mathcal{V}$，都有$\mathcal{V}(P) = 1$，就称命题P为重言式，记作$\models P$。显然，我们已经证明了$\models x_1 \supset (x_2 \supset x_1)$，注意到它实际上是上面小节给出的公理模式1的一种特殊情况，为了进一步证明公理模式1是重言式，即

$$\models P \supset (Q \supset P),$$

我们需要

定理 12 (**替代定理**): 对于任意命题P、Q_i（$1 \leq i \leq n$），有

$$\models P \quad \Longrightarrow \quad \models [Q_1/x_1, \ldots, Q_n/x_n]P。$$

证明: 构造一个映射$\mathcal{U} : X \to P$如下

$$\begin{aligned} \mathcal{U}(x_i) &= Q_i, \\ \mathcal{U}(\neg P) &= \neg \mathcal{U}(P), \\ \mathcal{U}(P_1 \supset P_2) &= \mathcal{U}(P_1) \supset \mathcal{U}(P_2)。 \end{aligned}$$

由此，对任意的赋值$\mathcal{V}$，我们有

$$\begin{aligned} &\models P \\ &\Rightarrow \mathcal{V} \circ \mathcal{U}(P) = 1 \\ &\Rightarrow \mathcal{V}(\mathcal{U}(P)) = 1 \\ &\Rightarrow \mathcal{V}([Q_1/x_1, \ldots, Q_n/x_n]P) = 1 \\ &\Rightarrow \models [Q_1/x_1, \ldots, Q_n/x_n]P。 \end{aligned}$$

证毕

由此，不难证明公理模式1是重言式。

进一步把重言式推广，对于给定的环境$\Gamma = \{Q_1, \ldots, Q_n\}$，如果命题$P$对于任意的赋值$\mathcal{V}$，每当$\mathcal{V}(Q_i) = 1 (1 \leq i \leq n)$，都有$\mathcal{V}(P) = 1$，则称命题$P$从环境$\Gamma$语义可证，记为$\Gamma \models P$。

下面证明和命题1相对应的

命题 13: $\{P\} \models Q \supset P$。

证明: 设$\mathcal{V}(P) = 1$，可以得到

$$\begin{aligned} \mathcal{V}(Q \supset P) &= \mathcal{V}(Q) \supset' \mathcal{V}(P) \\ &= \mathcal{V}(Q) \supset' 1 \\ &= 1 \end{aligned}$$

证毕

作为最后一个例子，我们证明演绎定理的语义形式

定理 14 (**语义演绎定理**): $\Gamma \cup \{P\} \models Q \Longleftrightarrow \Gamma \models P \supset Q$。

证明: 先证($\Rightarrow$)。由已知得$\mathcal{V}(P) = 1$和$\mathcal{V}(Q) = 1$，因此

$$\begin{aligned}\mathcal{V}(P \supset Q) &= \mathcal{V}(P) \supset' \mathcal{V}(Q)\\ &= 1 \supset' 1\\ &= 1,\end{aligned}$$

故有

$$\Gamma \models P \supset Q。$$

再证($\Leftarrow$)。已知$\mathcal{V}(P \supset Q) = 1$，又假设$\mathcal{V}(P) = 1$，可以得到$\mathcal{V}(Q) = 1$，故有

$$\Gamma \cup \{P\} \models Q。$$

证毕