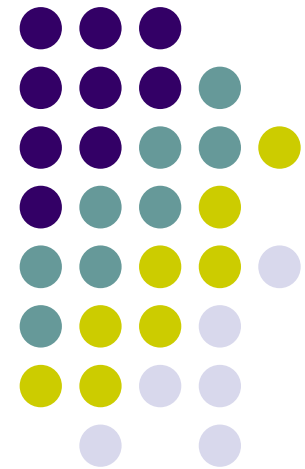




南京大学  
Nanjing University

# 第7讲-Herbrand定理





Herbrand定理 是数理逻辑的基本定理之一，它由法国 Jacques Herbrand博士（1908-1931）于1930年给出，此定理的表现形式有若干种 (参见文献[6]), 它提供了

1. 从一阶逻辑化归（reduce）到命题逻辑的一种形式；
2. 一阶逻辑中公式不可满足性问题的半可判定算法。



定义7.1. 设 $A$ 为一阶语言 $\mathcal{L}$ 的公式,  $A$ 为前束范式指 $A$ 呈形于

$$Q_1x_1.(Q_2x_2.(...Q_nx_n.(B)...)),$$

这里  $Q_i \in \{\forall, \exists\} (i \leq n)$  且  $B$  中无量词。

约定7.2.

- (1) 将 $Q_1x_1.(Q_2x_2.(...Q_nx_n.(B)...))$ 简记为 $Q_1x_1...Q_nx_n.B$ ,  
且当 $n = 0$ 时, 以上公式为 $B$ 。
- (2) 将 $(A \rightarrow B) \wedge (B \rightarrow A)$ 简记为 $A \leftrightarrow B$ 。
- (3)  $Qx.A$ 指 $\forall x.A$ 或 $\exists x.A$ .  $Q^*$ 为 $Q$ 的对偶,  
即若 $Q$ 为 $\forall$ , 则 $Q^*$ 为 $\exists$ ; 若 $Q$ 为 $\exists$ , 则 $Q^*$ 为 $\forall$ 。



命题7.3. 在一阶逻辑中, 我们有

- (1) 若  $x \notin FV(B)$ , 则  $\vdash Qx.B \leftrightarrow B$ ;
- (2) 若  $y$  为新变元, 则  $\vdash Qx.B \leftrightarrow Qy.B[\frac{y}{x}]$ 。



命题7.4. 在一阶逻辑中, 我们有

$$(1) \vdash \neg \forall x.A \leftrightarrow \exists x.\neg A;$$

$$(2) \vdash \neg \exists x.A \leftrightarrow \forall x.\neg A;$$

以下(3)-(8), 满足条件 $x \notin FV(B)$ 。

$$(3) \vdash (\forall x.A \wedge B) \leftrightarrow \forall x.(A \wedge B);$$

$$(4) \vdash (\exists x.A \vee B) \leftrightarrow \exists x.(A \vee B);$$

$$(5) \vdash (\forall x.A \rightarrow B) \leftrightarrow \exists x.(A \rightarrow B);$$

$$(6) \vdash (\exists x.A \rightarrow B) \leftrightarrow \forall x.(A \rightarrow B);$$

$$(7) \vdash (B \rightarrow \forall x.A) \leftrightarrow \forall x.(B \rightarrow A);$$

$$(8) \vdash (B \rightarrow \exists x.A) \leftrightarrow \exists x.(B \rightarrow A);$$

命题 7.3 和 7.4 的证明留作习题。



**定理7.5.** 对任何一阶语言 $\mathcal{L}$ 的公式 $A$ , 存在 $\mathcal{L}$ 的公式 $B$ , 使得  $\vdash A \leftrightarrow Q_1x_1...Q_nx_n.B$ , 这里  $x_1,...,x_n$  互异且 $B$ 中无量词。此定理说明任何公式皆有一个前束范式与其等价。

**证明:** 对  $A$  的结构作归纳证明存在  $B$  使

$$\vdash A \leftrightarrow Q_1x_1...Q_nx_n.B...(*),$$

这里  $x_1,...,x_n$  互异, 且  $B$  无量词。

情况1.  $A$ 为原子公式,  $(*)$ 当然成立。

情况2.  $A$ 为 $\neg C$ , 由I.H.知, 有 $D$ 使 $\vdash C \leftrightarrow Q_1x_1...Q_mx_m.D$ ,

这里 $x_1,...,x_m$ 互异且 $D$ 中无量词, 从而由命题7.4(1)知

$\vdash A \leftrightarrow Q_1^*x_1...Q_m^*x_m.\neg D$ , 故 $(*)$ 成立。



情况3.  $A$ 为 $E \wedge F$ .

由I.H.知有  $B, C$  使

$$\vdash E \leftrightarrow Q_1x_1 \dots Q_mx_m.B$$

$$\vdash F \leftrightarrow Q_{m+1}x_{m+1} \dots Q_{m+l}x_{m+l}.C$$

这里  $B, C$  中无量词。从而有互异的新变元  $z_1, \dots, z_l$

$$\text{使 } \vdash F \leftrightarrow Q_{m+1}z_1 \dots Q_{m+l}z_l.D$$

这里  $D$  为  $C[\frac{z_1}{x_{m+1}}] \dots [\frac{z_l}{x_{m+l}}]$ 。

$$\text{故 } \vdash A \leftrightarrow Q_1x_1 \dots Q_mx_m Q_{m+1}z_1 \dots Q_{m+l}z_l.(B \wedge D)。$$

情况4.  $A$ 为 $E \rightarrow F$ 或 $A$ 为 $E \vee F$ .与上同理可证。

情况5.  $A$ 为 $Qx.C$ .

由I.H.知有  $B$  使  $\vdash C \leftrightarrow Q_1x_1 \dots Q_mx_m.B$ , 从而

当  $x \in \{x_1, \dots, x_n\}$  时,  $\vdash A \leftrightarrow Q_1x_1 \dots Q_mx_m.B$ ;

当  $x \notin \{x_1, \dots, x_n\}$  时,  $\vdash A \leftrightarrow QxQ_1x_1 \dots Q_mx_m.B$ 。



下面我们引入Skolem范式的概念。

**定义7.6.** 设公式 $A$ 呈前束形, $A$ 的Skolem范式 $A^s$ 归纳定义如下:

- (1) 若 $A$ 中无量词, 则 $A^s$ 为 $A$ ;
- (2)  $(\forall x.A)^s$ 为 $\forall x.(A^s)$ ;
- (3) 对于 $(\exists x.A)^s$ 分情况定义:
  - (a) 若 $FV(\exists x.A) = \emptyset$ , 则 $(\exists x.A)^s$ 为 $(A[\frac{c}{x}])^s$ , 这里 $c$ 为新常元;
  - (b) 若 $FV(\exists x.A) \neq \emptyset$ , 设 $FV(\exists x.A) = \{x_1, x_2, \dots, x_n\}$   
则 $(\exists x.A)^s$ 为 $(A[\frac{f(x_1, \dots, x_n)}{x}])^s$ , 这里 $f$ 为 $n$ 元新函数。

易见 $A$ 的Skolem范式中无量词 $\exists$ , 其呈形于 $\forall x_1 \forall x_2 \dots \forall x_n. B$ ,  
 $B$ 中无量词, 它通过引入新常元或函数来消除前束范式中的量词 $\exists$ 。





**例7.1.** 设 $A$ 为 $\forall x \exists y. P(x, y)$ 且 $P$ 为谓词,从而 $A^s$ 为 $\forall x. P(x, f(x))$ , 这里 $f$ 为函数。不难证明:

$$(1) \models \forall x. P(x, f(x)) \rightarrow \forall x \exists y. P(x, y)$$

$$(2) \not\models \forall x \exists y. P(x, y) \rightarrow \forall x. P(x, f(x))$$

$$(3) \forall x. P(x, f(x)) \text{ 可满足} \Leftrightarrow \forall x \exists y. P(x, y) \text{ 可满足。}$$

这说明 $A$ 与 $A^s$ 同可满足, 但 $A$ 与 $A^s$ 不一定同真假。



更一般地，我们有

**命题7.7.** 设 $A$ 为闭前束范式， $A$ 可满足 $\Leftrightarrow A^s$ 可满足。

**证明:** 设 $A$ 为闭前束范式, 以下对 $A$ 中的量词 $\exists$ 的个数 $n$ 作归纳证明

$A$ 可满足 $\Leftrightarrow A^s$ 可满足.....(\*).

**奠基:** 当 $n = 0$ 时，这时 $A$ 中无量词 $\exists$ ，从而 $A^s$ 为 $A$ ，故(\*)成立。

**归纳假设(I.H.):** 当 $n = k$ 时，(\*)成立。

**归纳步骤:** 当 $n = k + 1$ 时，设 $A$ 呈形于  $\forall x_1 \dots \forall x_n \exists y. B$  且 $B$ 为前束范式，其中有 $k$ 个 $\exists$ ，从而 $A^s$ 为 $\forall x_1 \dots \forall x_n. (B[\frac{f(y_1, \dots, y_m)}{y}])^s$ ，这里 $FV(\exists y. B) = \{y_1, \dots, y_m\}$ ，从而由I.H.知

$B[\frac{f(y_1, \dots, y_m)}{y}]$ 与 $(B[\frac{f(y_1, \dots, y_m)}{y}])^s$ 同可满足。

余下只需证 $\forall \vec{x} \exists y. B$ 与 $\forall \vec{x} B[\frac{f(y_1, \dots, y_m)}{y}]$ 同可满足，

从而 $A$ 与 $A^s$ 同可满足。



不妨设  $FV(\exists y.B) = \{x_1, \dots, x_n\}$  且  $y \in FV(B)$ ,

从而我们需证  $\forall \vec{x} \exists y.B$  可满足  $\Leftrightarrow \forall \vec{x}.B[\frac{f(\vec{x})}{y}]$  可满足。

“ $\Leftarrow$ ”：易见。

“ $\Rightarrow$ ”：设  $(M, I) \models \forall \vec{x} \exists y.B$ , 从而对  $\vec{a} \in M^n$  存在  $b \in M$  使对任何  $\sigma$  有

$$(M, I) \models \sigma[\vec{x} := \vec{a}, y := b]B \dots\dots (**),$$

令  $S_{\vec{a}} = \{b \mid (**) \text{ 成立}\}$ ,  $\therefore S_{\vec{a}} \neq \emptyset$  且  $S_{\vec{a}} \in \mathcal{P}(M)$ ,

$\therefore$  由选择公理 AC 知, 有  $\rho: \mathcal{P}(M) \rightarrow M$  使  $\rho(S_{\vec{a}}) \in S_{\vec{a}}$ 。因此

$$(M, I) \models \sigma[\vec{x} := \vec{a}, y := \rho(S_{\vec{a}})]B,$$

令  $F: M^n \rightarrow M$  如下:  $F(\vec{a}) = \rho(S_{\vec{a}}) (\vec{a} \in M^n)$ ,

又令  $I'$  为  $I$  的扩展使  $I'(f) = F$ 。

从而  $(M, I') \models \sigma[\vec{x} := \vec{a}, y := F(\vec{a})]B$

因此  $(M, I') \models \sigma[\vec{x} := \vec{a}]B[\frac{f(\vec{x})}{y}]$

从而  $(M, I') \models \forall \vec{x}.B[\frac{f(\vec{x})}{y}]$ , 这样  $(*)$  成立。

□



**定义7.8.** 设 $\mathcal{L}$ -公式 $A$ 为Skolem范式，以下归纳定义 $\mathcal{L}$ -项的集合 $H_n$ :

- (1) 若 $A$ 中无常元出现，则 $H_0 = \{c_0\}$ ，这里 $c_0$ 为 $\mathcal{L}$ 中某个常元;
- (2) 若 $A$ 中有常元出现，则 $H_0 = \{c | c \text{ 为常元且出现在 } A \text{ 中}\}$ 。
- (3)  $H_{n+1} = H_n \cup \{f(t_1, \dots, t_m) | f \text{ 为 } A \text{ 中的 } m \text{ 元函数且 } t_1, \dots, t_m \in H_n\}$ 。
- (4) 令 $H_A = \cup \{H_n | n \in \mathbb{N}\}$ 被称为 $A$ 的Herbrand域。

易见 $H_A$ 中元素皆为 $\mathcal{L}$ -闭项其由 $A$ 中常元（或某个常元 $c_0$ ）和 $A$ 中函数组成。



**定义7.9.** 设 $\mathcal{L}$ -公式 $A$ 为Skolem范式, $H_A$ 为 $A$ 的Herbrand域且 $c_0$ 为 $H_A$ 中的某个常元。对于一个 $\mathcal{L}$ -结构 $\mathbb{M} = (M, I)$ , 定义 $A$ 对应于 $\mathbb{M}$ 的Herbrand结构 $\mathbb{H}_A = (H_A, I_A)$ 如下:

(1) 对于常元 $c$ ,

$$I_A(c) = \begin{cases} c, & \text{若 } c \in H_A; \\ c_0, & \text{否则。} \end{cases}$$

(2) 对于 $m$ 元函数 $f$ , 定义 $I_A(f) : H_A^m \rightarrow H_A$ 如下:

$$I_A(f)(t_1, \dots, t_m) = \begin{cases} f(t_1, \dots, t_m), & \text{若 } f \text{ 出现于 } A; \\ c_0, & \text{否则。} \end{cases}$$

(3) 对于 $m$ 元谓词 $P$ , 定义 $I_A(P) \subseteq H_A^m$ 如下:

$$I_A(P) = H_A^m \cap I(P), \text{ 从而}$$

$$I_A(P) = \{ \langle t_1, \dots, t_m \rangle \in H_A^m \mid \mathbb{M} \models P(t_1, \dots, t_m) \}.$$



易见

### 命题7.10.

- (1) 若  $c \in H_A$ , 则  $I_A(c) = c$ ;
- (2) 若  $f$  出现于  $A$ , 则  $I_A(f)(t_1, \dots, t_m) = f(t_1, \dots, t_m)$ ;
- (3) 若项  $t \in H_A$ , 则  $t_{H_A} = t$ ;
- (4) 若谓词  $P$  为  $m$  元且  $t_1, \dots, t_m \in H_A$ , 则  
 $\mathbb{H}_A \models P(t_1, \dots, t_m) \Leftrightarrow \mathbb{M} \models P(t_1, \dots, t_m)$ 。



**命题7.11.** 设 $\mathcal{L}$ -闭公式 $A$ 为Skolem范式,  $\mathbb{M} = (M, I)$  为 $\mathcal{L}$ -结构,  $\mathbb{H}_A = (H_A, I_A)$  为 $A$ 对应于  $\mathbb{M}$  的Herbrand 结构, 若  $\mathbb{M} \models A$  则  $\mathbb{H}_A \models A$ 。

证明: 不妨设  $A$  为  $\forall x_1, \dots, \forall x_n. B$ , 这里  $x_1, \dots, x_n$  互异且  $FV(B) = \{x_1, \dots, x_n\}$ ,  $B$ 中无量词。对 $n$ 作归纳证明

$$\mathbb{M} \models A \Rightarrow \mathbb{H}_A \models A \dots (*)$$

奠基: 当 $n = 0$ 时, 欲证 $\mathbb{M} \models B \Leftrightarrow \mathbb{H}_A \models B \dots (**)$

对 $B$ 的结构归纳来证明(\*\*)如下:

情况1. 设 $B$ 的原子公式 $P(t_1, \dots, t_m)$ , 这里 $t_i$ 为项且

$t_i \in H_A$ , 从而由命题 7.10(4)知(\*\*)成立。

情况2. 设 $B$ 呈 $\neg C, C \wedge D, C \vee D$ 或 $C \rightarrow D$ 形时易见(\*\*)成立。

因此当 $n = 0$ 时, (\*)成立。



归纳假设(I.H.): 当  $n = k$  时,  $(*)$ 成立。

归纳步骤: 设  $n = k + 1$  时, 这时  $A$  呈形  $\forall x.C$ , 其中  $C$  为含  $n$  个  $\forall$  的 Skolem 范式且只含自由变元  $x$ 。因为

$$\mathbb{M} \models \forall x.C$$

$$\Rightarrow \text{对任何 } \sigma : V \rightarrow M, \mathbb{M} \models_{\sigma} \forall x.C$$

$$\Rightarrow \text{对任何 } \sigma : V \rightarrow M, \forall a \in M. \mathbb{M} \models_{\sigma[x:=a]} C$$

(若  $t \in H_A$ , 则  $t_M \in M$ )

$$\Rightarrow \text{对任何 } \sigma : V \rightarrow M, \forall t \in H_A. \mathbb{M} \models_{\sigma[x:=t_M]} C$$

(替换引理)

$$\Rightarrow \text{对任何 } \sigma : V \rightarrow M, \forall t \in H_A. \mathbb{M} \models_{\sigma} C\left[\frac{t}{x}\right]$$

( $C\left[\frac{t}{x}\right]$  为闭项)

$$\Rightarrow \forall t \in H_A. \mathbb{M} \models C\left[\frac{t}{x}\right]$$

( $C\left[\frac{t}{x}\right]$  只含  $k$  个  $\forall$  且由 I.H.)





$$\Rightarrow \forall t \in H_A. \mathbb{H}_{C[\frac{t}{x}]} \models C[\frac{t}{x}]$$
$$(H_{C[\frac{t}{x}]} = H_A)$$

$$\Rightarrow \forall t \in H_A. H_A \models C[\frac{t}{x}]$$

(替换引理)

$$\Rightarrow \text{对任何 } \sigma : V \rightarrow H_A, \forall t \in H_A. \mathbb{H}_A \models_{\sigma[x:=t_{H_A}]} C$$
$$(\because t \in H_A \quad \therefore t_{H_A} = t)$$

$$\Rightarrow \text{对任何 } \sigma : V \rightarrow H_A, \forall t \in H_A. \mathbb{H}_A \models_{\sigma[x:=t]} C$$

$$\Rightarrow \text{对任何 } \sigma : V \rightarrow H_A, \mathbb{H}_A \models_{\sigma} \forall x. C$$

$$\Rightarrow \mathbb{H}_A \models A.$$

因此(\*\*)成立, 归纳完成。

□



推论7.12. 设 $\mathcal{L}$ -闭公式  $A$  为Skolem 范式,

$A$ 可满足 $\Leftrightarrow A$ 在某个Herbrand 结构中可满足。

证明:

“ $\Leftarrow$ ”: 显然。

“ $\Rightarrow$ ”:  $A$ 可满足 $\Rightarrow A$ 在某个 $\mathbb{M} = (M, I)$ 结构中可满足  
 $\Rightarrow A$ 在 $\mathbb{H}_A = (H_A, I_A)$ 中可满足。

□



**定理7.13** (Herbrand定理). 设  $\mathcal{L}$ -闭公式  $A$  为 Skolem 范式

$\forall x_1 \dots \forall x_n. B$  且  $B$  中无量词, 令  $\Gamma = \{B[\frac{t_1}{x_1}] \dots [\frac{t_n}{x_n}] \mid t_1, \dots, t_n \in H_A\}$ ,

我们有  $A$  可满足  $\Leftrightarrow \Gamma$  可满足。

证明:

“ $\Rightarrow$ ”: 设  $B_1, \dots, B_m \in \Gamma$ , 从而  $\vdash A \rightarrow B_i (i \leq m)$ , 因此  
 $\vdash A \rightarrow (B_1 \wedge B_2 \wedge \dots \wedge B_m)$ , 当  $A$  可满足时,  $\{B_1, \dots, B_m\}$  可满足,  
而  $B_1, \dots, B_m$  可从  $\Gamma$  中任意选取, 故由紧性定理知  $\Gamma$  可满足。

“ $\Leftarrow$ ”: 当  $\Gamma$  可满足时, 有  $\mathcal{L}$ -结构  $\mathbb{M} = (M, I)$  使  $\mathbb{M} \models \Gamma$ 。

令  $\mathbb{H}_A = (H_A, I_A)$  为  $A$  的对应于  $\mathbb{M}$  的 Herbrand 结构, 以下证明  
对任何  $C \in \Gamma$ ,  $\mathbb{M} \models C \Leftrightarrow \mathbb{H}_A \models C$ 。



为了方便, 不妨设 $A$ 为 $\forall x.B$ , 以下对 $B$ 的结构归纳证明

对任何 $t \in H_A$ ,  $\mathbb{M} \models B[\frac{t}{x}] \Leftrightarrow \mathbb{H}_A \models B[\frac{t}{x}] \dots (*)$

情况1.  $B$ 为原子公式 $P(S_1, \dots, S_m)$ ,

对于 $t \in H_A$ , 令 $S_i' \equiv S_i[\frac{t}{x}]$ , 从而 $B[\frac{t}{x}] \equiv P(S_1', \dots, S_m')$ ,

易见 $S_i' \in H_A$ , 从而 $\mathbb{M} \models B[\frac{t}{x}] \Leftrightarrow \mathbb{M} \models P(S_1', \dots, S_m')$

$\Leftrightarrow \mathbb{H}_A \models P(S_1', \dots, S_m') \Leftrightarrow \mathbb{H}_A \models B[\frac{t}{x}]$ 。

情况2.  $B$ 呈形 $\neg C, C \wedge D, C \vee D, C \rightarrow D$ 时, 由I.H.知 $(*)$ 成立。

这样  $\because \mathbb{M} \models \Gamma$ ,  $\therefore$  对任何 $t \in H_A$ ,  $\mathbb{M} \models B[\frac{t}{x}]$

由 $(*)$ 知对任何 $t \in H_A$ ,  $\mathbb{H}_A \models B[\frac{t}{x}]$ , 再由替换引理知,

对 $H_A$ 上的任意赋值 $\sigma: V \rightarrow H_A$ 有 $\mathbb{H}_A \models_{\sigma} B[\frac{t}{x}]$ ,

从而 $\mathbb{H}_A \models_{\sigma[:=t_{H_A}]} B$ ,  $\because t_{H_A} = t$ ,  $\therefore$  对任何 $t \in H_A$ .  $\mathbb{H}_A \models_{\sigma[x:=t]} B$

故 $\mathbb{H}_A \models \forall x.B$ , 从而 $A$ 可满足。

□



**例7.2.** 设 $A$ 为 $\exists x \forall y. P(x, y)$ 其中 $P$ 为二元谓词, 从而 $\neg A$ 的前束范式为 $B \equiv \forall x \exists y. \neg P(x, y)$ ,  $B$ 的Skolem范式为 $\forall x \neg P(x, f(x))$ 。

令 $c$ 为个体常元,

$H = H_B = \{c, f(c), \dots, f^n(c), \dots\}$ . 因此

$$\Gamma_B = \{\neg P(t, f(t)) \mid t \in H\} = \{\neg P(f^n(c), f^{n+1}(c)) \mid n \in \mathbb{N}\}$$

$$\vdash \exists x \forall y. P(x, y)$$

$$\Leftrightarrow \models A$$

$$\Leftrightarrow B \text{ 不可满足}$$

$$\Leftrightarrow \Gamma_B \text{ 不可满足}$$

$$\Leftrightarrow \text{存在 } \Gamma_B \text{ 的一个有穷子集不可满足}$$

$$\Leftrightarrow \text{存在有穷个 } t_1, \dots, t_m \in H \text{ 使 } \{\neg P(t_1, f(t_1)), \dots, \neg P(t_m, f(t_m))\} \text{ 不可满足}$$

$$\Leftrightarrow \text{存在有穷个 } t_1, \dots, t_m \in H \text{ 使 } \neg(\neg P(t_1, f(t_1)) \wedge \dots \wedge \neg P(t_m, f(t_m))) \text{ 永真}$$

$$\Leftrightarrow \text{存在 } t_1, \dots, t_m \in H \text{ 使 } \vdash P(t_1, f(t_1)), \dots, P(t_m, f(t_m)) \text{ 可证。}$$



# The End of Lecture 7