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$\mathscr{L}$的公式, A为前束形范式指A呈形于

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

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

约定7.2.

(1) 将$Q_1x_1.(Q_2x_2.(\dots Q_nx_n.(B)\dots))$简记为$Q_1x_1\dots Q_nx_n.B$，且当$n=0$时，以上公式为$B$。

(2) 将$(A \to B) \wedge (B \to A)$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) $\vdash (\forall x.A \land B) \leftrightarrow \forall x.(A \land B)$;

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

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

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

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

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

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$\mathscr{L}$的公式A，存在$\mathscr{L}$的公式B，使得$\vdash A \leftrightarrow Q_1 x_1 ... Q_n x_n . B$，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形范式与其等价。

证明：对 A 的结构作归纳证明存在 B 使

$$\vdash A \leftrightarrow Q_1 x_1 ... Q_n x_n . B ...(*),$$

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$\vdash C \leftrightarrow Q_1 x_1 ... Q_m x_m . D$，

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

$\vdash E \leftrightarrow Q_1 x_1 \ldots Q_m x_m . B$

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

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

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

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

故$\vdash A \leftrightarrow Q_1 x_1 \ldots Q_m x_m Q_{m+1} z_1 \ldots . Q_{m+l} z_l . (B \wedge D)$。

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$\vdash C \leftrightarrow Q_1 x_1 \ldots Q_m x_m . B$，从而

当$x \in \{x_1, \ldots, x_n\}$时，$\vdash A \leftrightarrow Q_1 x_1 \ldots Q_m x_m . B$;

当$x \notin \{x_1, \ldots, x_n\}$时，$\vdash A \leftrightarrow Q x Q_1 x_1 \ldots Q_m x_m . B$。

$\square$

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$FV(\exists x.A)=\varnothing$，则$(\exists x.A)^s$为$(A[\frac{c}{x}])^s$,这里$c$为新常元;

(b) 若$FV(\exists x.A)\neq\varnothing$，设$FV(\exists x.A)=\{x_1,x_2,\ldots,x_n\}$

则$(\exists x.A)^s$为$(A[\frac{f(x_1,\ldots,x_n)}{x}])^s$, 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$\forall x_1\forall x_2\ldots\forall x_n.B$，$B$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) $\vDash \forall x.P(x,f(x)) \to \forall x\exists y.P(x,y)$

(2) $\nvDash \forall x\exists y.P(x,y) \to \forall x.P(x,f(x))$

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

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

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 $\forall x_1...\forall x_n\exists y.B$ 且B为前束范式，其中有k个$\exists$，从而A^s为$\forall x_1...\forall x_n.(B[\frac{f(y_1,...,y_m)}{y}])^s$，这里$FV(\exists y.B)=\{y_1,...,y_m\}$，从而由I.H.知

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

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

从而A与A^s同可满足。

不妨设$FV(\exists y.B) = \{x_1, ...x_n\}$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$(M,I) \vDash \forall \vec{x} \exists y.B$, 从而对$\vec{a} \in M^n$存在$b \in M$使对任何$\sigma$有

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

令$S_{\vec{a}} = \{b|(**)$成立$\}$，$\because S_{\vec{a}} \neq \varnothing$且$S_{\vec{a}} \in \mathcal{P}(M)$，

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

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

令$F : M^n \to M$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$(M,I') \vDash \sigma[\vec{x} := \vec{a}, y := F(\vec{a})]B$

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

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

定义7.8. 设$\mathscr{L}$–公式A为Skolem范式，以下归纳定义$\mathscr{L}$–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$\mathscr{L}$中某个常元;

(2) 若A中有常元出现，则$H_0 = \{c | c$为常元且出现在A中$\}$。

(3) $H_{n+1} = H_n \cup \{f(t_1, ..., t_m) | f$为$A$中的$m$元函数且$t_1, ..., t_m \in H_n\}$。

(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$\mathscr{L}$–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$\mathscr{L}$–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$\mathscr{L}$–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，

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

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

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

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

$I_A(P)={H_A}^m\cap I(P)$，从而

$I_A(P)=\{\langle t_1,\dots,t_m\rangle \in {H_A}^m | \mathbb{M}\vDash P(t_1,\dots,t_m)\}$。

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$I_A(f)(t_1, ..., t_m) = f(t_1, ..., t_m)$；

(3) 若项$t \in H_A$，则$t_{H_A} = t$；

(4) 若谓词P为m元且$t_1, ..., t_m \in H_A$，则
$\mathbb{H}_A \vDash P(t_1, ..., t_m) \Leftrightarrow \mathbb{M} \vDash P(t_1, ..., t_m)$。

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

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

$$\mathbb{M}\vDash A\Rightarrow\mathbb{H}_A\vDash A......(*).$$

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

对B的结构归纳来证明(**)如下：

情况1. 设B的原子公式$P(t_1,...,t_m)$，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$C\to D$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

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

$\Rightarrow$ 对任何$\sigma : V \to M$，$\mathbb{M} \vDash_{\sigma} \forall x.C$

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

（若$t \in H_A$，则$t_M \in M$）

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

（替换引理）

$\Rightarrow$ 对任何$\sigma : V \to M$，$\forall t \in H_A.\mathbb{M} \vDash_{\sigma} C[\frac{t}{x}]$

（$C[\frac{t}{x}]$为闭项）

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

（$C[\frac{t}{x}]$只含k个$\forall$且由I.H.）

$$\Rightarrow \ \forall t \in H_A.\mathbb{H}_{C[\frac{t}{x}]} \vDash C[\frac{t}{x}]$$

$(H_{C[\frac{t}{x}]} = H_A)$

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

（替换引理）

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

$(\because t \in H_A \quad \therefore \ t_{H_A} = t)$

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

$\Rightarrow$ 对任何$\sigma : V \to H_A, \mathbb{H}_A \vDash_\sigma \forall x.C$

$\Rightarrow \mathbb{H}_A \vDash A$。

因此(**)成立，归纳完成。 □

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

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

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。

$\square$

定理7.13 (Herbrand定理). 设 $\mathscr{L}$–闭公式A为Skolem范式 $\forall x_1 ... \forall x_n.B$且$B$中无量词，令$\Gamma = \{B[\frac{t_1}{x_1}]...[\frac{t_n}{x_n}] \| t_1, ..., t_n \in H_A\}$，我们有 A可满足$\Leftrightarrow \Gamma$可满足。

证明:

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

"$\Leftarrow$"：当 Γ 可满足时，有$\mathscr{L}$–结构 $\mathbb{M} = (M, I)$ 使 $\mathbb{M} \vDash \Gamma$。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$C \in \Gamma$，$\mathbb{M} \vDash C \Leftrightarrow \mathbb{H}_A \vDash C$。

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$t\in H_A$，$\mathbb{M}\vDash B[\frac{t}{x}]\Leftrightarrow \mathbb{H}_A\vDash B[\frac{t}{x}]$……(*)

情况1. B为原子公式$P(S_1,\ldots,S_m)$，

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

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

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

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

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

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

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

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

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

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，

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

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

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

$\Leftrightarrow \vDash A$

$\Leftrightarrow B$不可满足

$\Leftrightarrow \Gamma_B$不可满足

$\Leftrightarrow$存在Γ_B的一个有穷子集不可满足

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

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

$\Leftrightarrow$存在$t_1, \ldots, t_m \in H$使$\vdash P(t_1, f(t_1)), \ldots, P(t_m, f(t_m))$可证。

The End of Lecture 7