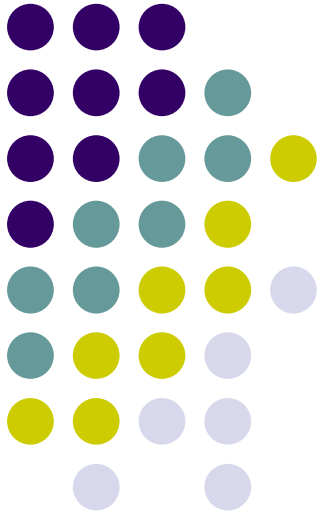
南京大学
Nanjing University

第十一讲 一阶语言的重要定理



内容提要

- 紧性定理：无穷和有穷
  - 基于完全性定理的紧性定理证明
  - 构造性的紧性定理证明

- 勒文海姆-斯科伦定理：可数无穷和不可数无穷
  - 向下勒文海姆-斯科伦定理
  - 向上勒文海姆-斯科伦定理

- 埃尔布朗定理：谓词逻辑和命题逻辑
  - 斯科伦范式与斯科伦定理
  - 埃尔布朗域与埃尔布朗定理

Part1- 紧性定理

紧性定理 Compactness

- 公式集Γ可满足的当且仅当它的所有用穷子集均可满足

- **矛盾的有限性**
  - 如果一个公式集Γ不协调，那么一定存在一个有穷子集Δ不协调
  - 如果程序有问题，那么它一定是某行代码上出了问题，即使这个程序有无穷行代码
- **有穷的推理能够保障无穷的真理**
  - 基于有限个算术规则，但描述所有自然数的运算
  - 程序验证：一个网站系统的所有有限步骤执行都是安全的

基于完全性定理的紧性定理证明

定理11.19. （一阶逻辑的紧性定理）设 Γ 为句子集，

若 Γ 的任何有穷子集可满足，则 Γ 可满足。

证明: 设 Γ 为公式集，我们有 $con(\Gamma) \Leftrightarrow \Gamma$ 可满足;

若 Γ 的每个有穷子集可满足，则 Γ 的每个有穷子集协调;

反设 Γ 不可满足，从而 Γ 不协调，因此 $\Gamma \vdash \bot$，

这样存在有穷$\Delta \subseteq \Gamma$ 使 $\Delta \vdash \bot$，与 $con(\Delta)$ 矛盾。 □

构造性的紧性定理证明

如何找到满足Γ的模型？

- Lindenbaum扩充，将Γ扩充为极大协调集合Δ
- 构建Δ的可满足模型
  - 命题逻辑：模型即赋值，直接指派Δ中所有命题符的赋值即可
  - 一阶语言：模型=论域+映射+赋值

路线1：基于语言符号
从0开始构建模型
- **Henkin集**处理存在量词
- **Hintikka集的典范模型**处理等词

路线2：基于有穷子集模型
聚合构建模型
- 利用**直积**进行模型聚合
- 利用**滤**决定聚合的结果
- **Zorn引理**保证了可行性

命题逻辑紧性定理的证明

定义1.28 称 Δ 为有穷可满足指 Δ 的任何有穷子集可满足。

引理1.29 所有命题可被排列为 $A_0, A_1, \ldots, A_n, \ldots \quad (n \in \mathbf{N})$。

引理1.30 设 Δ 为有穷可满足，A 为命题。若 $\Delta \cup \{A\}$ 不为有穷可满足，
则 $\Delta \cup \{\neg A\}$ 为有穷可满足。

证明: 设 $\Delta \cup \{A\}$ 不为有穷可满足，反设 $\Delta \cup \{\neg A\}$ 也不为有穷可满足，
从而存在 $\Delta_1, \Delta_2 \subseteq \Delta$ 使 Δ_1, Δ_2 皆有穷且 $\Delta_1 \cup \{A\}$ 与 $\Delta_2 \cup \{\neg A\}$ 皆不可满足。
由于 $\Delta_1 \cup \Delta_2$ 为 Δ 的有穷子集，故有 v 使 $v \vDash \Delta_1 \cup \Delta_2$，然

(1) 当 $v \vDash A$ 时，$v \vDash \Delta_1 \cup \{A\}$，从而矛盾。

(2) 当 $v \nvDash A$ 时，$v \vDash \Delta_2 \cup \{\neg A\}$，从而矛盾。

故 $\Delta \cup \{\neg A\}$ 有穷可满足。 □

命题逻辑紧性定理的证明

证明: 令

$$\Gamma_0 = \Gamma$$

$$\Gamma_{n+1} = \begin{cases} \Gamma_n \cup \{A_n\} & ，若\ \Gamma_n \cup \{A_n\}\ 有穷可满足， \\ \Gamma_n \cup \{\neg A_n\} & ，否则。 \end{cases}$$

先对 n 归纳证明 Γ_n 有穷可满足.....(*)。

Basis $n = 0$ 时，易见 (*) 成立。

I.H. 设 Γ_n 有穷可满足。

Ind. Step 若 $\Gamma_n \cup \{A_n\}$ 有穷可满足，则 Γ_{n+1} 有穷可满足，否则由引理 1.30 知 $\Gamma_n \cup \{\neg A_n\}$ 有穷可满足，即 Γ_{n+1} 有穷可满足。归纳完成。

令 $\Delta = \bigcup\{\Gamma_n | n \in \mathbf{N}\}$，我们有 Δ 为有穷可满足。

设 Φ 为 Δ 的有穷子集，从而有 k 使 $\Phi \subseteq \{A_0, A_1, \ldots, A_k\}$，故 $\Phi \subseteq \Gamma_{k+1}$，因此 Δ 有穷可满足。

对任何命题变元 p_i，$p_i \in \Delta$ 或 $\neg p_i \in \Delta$ 且恰具其一。

设 p_i 为 A_l。若 $p_i \notin \Delta$，则 $A_l \notin \Delta$，从而 $\Gamma_l \cup \{A_l\}$ 不为有穷可满足，
因此 $\neg A_l \in \Gamma_{l+1}$，故 $\neg p_i \in \Delta$。

又反设 $p_i, \neg p_i \in \Delta$，从而 Δ 的子集 $\{p_i, \neg p_i\}$ 不可满足，
故 Δ 不为有穷可满足。

令
$$v(p_i) = \begin{cases} T & ，若\ p_i \in \Delta \\ F & ，若\ \neg p_i \in \Delta \end{cases}$$

以下对 A 的结构归纳证明：若 $A \in \Delta$ 则 $v \vDash A$，否则 $v \nvDash A$.....(*)。

情形 1. A 为命题变元 p_i，由上知 (*) 成立。

情形 2. A 为 $\neg B$。

1. 当 $A \in \Delta$ 时，Δ 为有穷可满足，所以 $B \notin \Delta$，
   从而由 I.H.知 $v \nvDash B$，从而 $v \vDash \neg B$。

2. 当 $A \notin \Delta$ 时，即 $\neg B \notin \Delta$，设 B 为 A_l，
   从而 $\Gamma_l \cup \{B\}$ 有穷可满足(若不然,有 $\neg B \in \Gamma_{l+1}$，与 $\neg B \notin \Delta$ 矛盾)。
   故 $B \in \Delta$，由 I.H. 知 $v \vDash B$，从而 $v \nvDash A$。

情形 3. A 为 $B \wedge C$。

1. 当 $A \in \Delta$ 时，有 $B \in \Delta$。
   反设 $B \notin \Delta$，从而 $\neg B \in \Delta$，但 $\{A, \neg B\}$ 不可满足，矛盾。
   因此 $B \in \Delta$，同理 $C \in \Delta$。
   由 I.H.知 $v \vDash B, v \vDash C$，从而 $v \vDash B \wedge C$，即 $v \vDash A$。

2. 当 $A \notin \Delta$ 时，有 $B \notin \Delta$ 或 $C \notin \Delta$。
   反设 $B \in \Delta$ 且 $C \in \Delta$，从而由 $A \notin \Delta$ 知 $\neg A \in \Delta$，
   然 $\{\neg A, B, C\}$ 不可满足，故矛盾。
   因此 $B \notin \Delta$ 或 $C \notin \Delta$。
   不妨设 $B \notin \Delta$，从而 $v \nvDash B$，因此 $v \nvDash A$。

其他情形同理可证 (*) 成立。

因此我们有 $v \vDash \Delta$，故 Δ 可满足，从而 Γ 可满足。 □

一阶语言紧性定理的语义证明

目标：如何基于Γ的有穷子集集合的模型，构造Γ的模型？

核心思路：把所有模型聚合到一起，再通过“少数服从同属原则”决定Γ中每一个句子的真值

能找到一个切合所有平行宇宙的正史蜘蛛侠嘛？

寻找正史蜘蛛侠

- 所有自称蜘蛛侠的生物
  - **数学表示：直积**
  - 直积的元素是一条跨宇宙连接各个“蜘蛛侠”的序列
    - Name = (Gwen Stancy, Miles Morales, Perter Parker,…)
- 正史判定 / 织网事件 Canon Event
  - **数学表示：超滤**
  - 能够决定一个事件是否对大多数蜘蛛侠而言是织网事件
    - 被蜘蛛咬了/ 和MJ谈恋爱
- 正史蜘蛛侠
  - **数学表示：超积**
  - 提出“非正史”噪音后的所有宇宙公认的蜘蛛侠概念体

直积：如何描述选举结果

- $\{\mathcal{M}_i \mid i \in I\}$ 是一个索引为I的模型簇。 它们的直积 $\prod\mathcal{M}_i$ 是一个新的模型$\mathcal{M}$
  - $\mathcal{M}$的论域是所有 $\mathcal{M}_i$ 论域的 笛卡尔积
    - 元素是一个序列f ， f(i)是第i个模型 $\mathcal{M}_i$ 中的元素。
  - $\mathcal{M}$的解释是对所有$\mathcal{M}_i$的解释进行分量处理
    - 常量：序列
    - 函数：分别作用于各个分量上映射
    - 谓词：如果一个关系存在于所有$\mathcal{M}_i$的谓词中，则该关系存在于$\mathcal{M}$的谓词中

滤和超滤：如何描述少数服从多数

- 直观理解：对于一个给定的集合I，滤$\mathcal{F}$决定了I的哪些子集A是“多数”
  - $\mathcal{F}$是I的幂集的子集，也就是I的某些子集的集合
- 形式化定义：
  - 非空性：$\emptyset \notin \mathcal{F}$，且 $I \in \mathcal{F}$
  - 向上封闭：若 $A \in \mathcal{F}$ 且 $A \subseteq B$，则 $B \in \mathcal{F}$
  - 交集封闭：若 $A \in \mathcal{F}$ 且 $B \in \mathcal{F}$，则 $A \cap B \in \mathcal{F}$
- 超滤：消除滤无法处理的模糊地带
  - 对于I的任意子集 A，要么 $A \in U$，要么$I - A \in U$

超积：少数服从多数的选举结果

- 直观解释：在直积$\prod \mathcal{M}_i$的基础上，加上“少数服从多数”这条规则

- 超滤U：
  - 索引集I的超滤
  - 序列等价关系$\sim_U$：$f \sim_U g \Leftrightarrow \{i \in I \mid f(i)=g(i)\} \in U$
- 超积：直积$\prod \mathcal{M}_i$模超滤U的商$\prod \mathcal{M}_i/U$
  - 元素是序列的等价类$[f]_U$
  - $\prod \mathcal{M}_i/U \models A$，当且仅当所有$\mathcal{M}_i \models A$的$i$的序列属于U
  - 如果大多数模型说A是真的，超积就说A是真的

Zorn引理：超积的存在性保障

- 如果一个非空偏序集P的每一个链在P中都有上界，那么 P 至少拥有一个极大元。

- 给定$\mathbf{I}$的有穷可满足子集模型$\mathcal{M}_i$，用于构造超积$\prod\mathcal{M}_i/\mathbf{U}$的超滤$\mathbf{U}$是存在的
  - $\mathbf{I}$上的一个超滤$\mathbf{U}$是无法用外延法进行定义的
  - 但所有的滤$\mathcal{F}$组成了一个偏序集
  - 所以根据Zorn引理，我们可以从任一$\mathcal{F}$出发，构造出一个满足要求的超滤$\mathbf{U}$
  - **虽然看不见，但超滤就在那里**

Part2-勒文海姆-斯科伦定理

勒文海姆-斯科伦定理
Löwenheim–Skolem Theorem

- 如果一个公式集合Γ拥有一个无穷大可满足模型M，那么对于任何无限的基数，它一定也拥有一个对应规模的模型M'。
  - **向上推论：**如果一个公式集合Γ有可数模型，它就一定有不可数模型
  - **向下推论：**如果一个公式集合Γ描述了不可数集，它也会有一个**“看上去不可数”**的可数模型。

- 一阶语言无法精确地描述无穷大
- **斯科伦悖论：一阶语言构建的实数理论其实是可数的**

向上/向下勒文海姆-斯科伦定理

- **向下勒文海姆-斯科伦定理 (Downward Löwenheim-Skolem Theorem)**：设Γ是可数一阶语言$\mathcal{L}$上的一个公式集合。如果Γ是可满足的（即Γ有一个模型），那么Γ必有一个可数模型（即模型的论域基数$|D| \leq \aleph_0$）。

- **向上勒文海姆-斯科伦定理 (Upward Löwenheim-Skolem Theorem)**：设Γ是可数一阶语言$\mathcal{L}$上的公式集合。如果Γ有一个无穷模型，那么对于任意基数$\kappa \geq \aleph_0$，Γ都有一个基数为κ的模型。

向下勒文海姆-斯科伦定理的证明

- 设Γ是可数一阶语言$\mathcal{L}$上的一个公式集合。如果Γ是可满足的（即Γ有一个模型），那么Γ必有一个可数模型（即模型的论域基数$|D| \leq \aleph_0$）。

- 证明思路：基于完全性定理的证明过程
  - Γ可满足，所以Γ是协调的，
  - 通过Lindenbaum扩充构造Γ的极大协调集Γ^*，
  - 利用典范模型Canonical Model $\mathcal{M}$证明Γ^*可满足，
  - 可数一阶语言$\mathcal{L}$的典范模型$\mathcal{M}$的论域基数是可数的，
  - 可数模型$\mathcal{M} \models \Gamma^*$，所以$\mathcal{M} \models \Gamma$

Hintikka集的典范模型$\mathcal{M}$

- 典范模型：
  - 对于任意句子A：$\mathcal{M} \models A$当且仅当$A \in \Gamma^*$
  - 论域：所有闭项的等价类，$\mathcal{M}$ ={[t]|t是$\mathcal{L}$中的闭项}
  - 映射：
    - 常量：$c^M = [c]$
    - 函数：$f^M([t_1],\ldots, [t_n]) = [f(t_1,\ldots, t_n)]$
    - 谓词：$([t_1],\ldots, [t_n]) \in P^M$当且仅当
      $P(t_1,\ldots, t_n) \in \Gamma^*$

典范模型$\mathcal{M}$的基数可数

- 可数的语言$\mathcal{L}$的字母表Σ也是可数的，即$|\Sigma| = \aleph_0$
- 长度为n的项的集合是可数的
  - 每一个项都是由Σ中符号组成的有限长度序列
  - Σ^n表示长度为n的所有符号序列的集合
  - $|\Sigma^n| = |\Sigma| \times |\Sigma| \times \ldots \times |\Sigma| = \aleph_0$
- 所有项的集合S是可数的
  - S是所有Σ^n的并集：$S = \bigcup_{n=1,2,\ldots} \Sigma^n$
- 闭项集合T是S的子集，所以T是可数的，故$\mathcal{M}$的基数可数

□

向上勒文海姆-斯科伦定理的证明

- 设Γ是可数一阶语言$\mathcal{L}$上的公式集合。如果Γ有一个无穷模型M，那么对于任意基数$\kappa \geq \aleph_0$，Γ都有一个基数为κ的模型。

- 证明思路：基于紧性定理和向下勒文海姆-斯科伦定理
  - 引入常量：设K是一个基数为κ的新常量符号集合：$K=\{k_\alpha \mid \alpha<\kappa\}$。我们将$K$加入语言$\mathcal{L}$中得到扩充语言$\mathcal{L}'$
  - 构造公式集Δ：在Γ的基础上，加入一组断言“所有新常量互不相等”的公理集Σ：$\Sigma=\{\neg(k_\alpha=k_\beta) \mid \alpha,\beta<\kappa,\alpha\neq\beta\}$，令$\Delta=\Gamma\cup\Sigma$
  - 证明Δ是有穷可满足的
  - 基于紧性定理，存在语言$\mathcal{L}'$的模型$\mathcal{N}$使得$\mathcal{N}\models\Delta$
  - 基于向下勒文海姆-斯科伦定理，证明存在基数为κ的模型$\mathcal{M}$使得$\mathcal{M}\models\Delta$

公式集Δ有穷可满足

证明Δ = Γ ∪ {¬(k_α=k_β)|α≠β}是有穷可满足的

- 对于Δ的任意子集Δ_fin = Γ_fin ∪ Σ_fin
  - 设Σ_fin涉及m个新常量k_1,k_2,…, k_m
- 设Γ的无穷模型M的论域为D，则D为无穷集
  - 可以从D中取出m个互不相同的元素d_1,d_2,…, d_m
- 基于M，构造扩张模型$\mathcal{N}$
  - 论域相同
  - I(k_1)=d_1,…,I(k_m)=d_m
- $\mathcal{N}$⊨ Σ_fin,所以$\mathcal{N}$⊨ Δ_fin

□

从$\mathcal{N}(\kappa \leq |\mathcal{N}|)$到$\mathcal{M}(\kappa = |\mathcal{M}|)$

已知$\mathcal{N} \models \Delta$，证明存在$\mathcal{M} \models \Delta$,且$|\mathcal{M}| = \kappa$

- 向下勒文海姆-斯科伦定理的广义形式：

  设$\mathcal{N}$是语言$\mathcal{L}'$的模型，κ是一个基数且满足

  $$\max(|\mathcal{L}'|, \aleph_0) \leq \kappa \leq |\mathcal{N}|,$$

  则$\mathcal{N}$存在一个子模型$\mathcal{M}$，使得$|\mathcal{M}| = \kappa$，且$\mathcal{M}$是$\mathcal{N}$的初等子结构

  - 基数限制
    - $\kappa \leq |\mathcal{N}|$：$\mathcal{M}$是基于$\mathcal{N}$构建的
    - $\max(|\mathcal{L}'|, \aleph_0) \leq \kappa$ ：$\mathcal{M}$不小于语言$\mathcal{L}'$本身
  - 初等子结构
    - 对于语言$\mathcal{L}$的任何句子A， $\mathcal{M} \models A$ 当且仅当$\mathcal{N} \models A$

Part3-埃尔布朗定理

埃尔布朗定理 Herbrand Theorem

- 如何判断一阶语言公式**A**是否可满足？
  - 模型的选择是不可数的，所以无法穷举所有可能性

一阶公式A是不可满足的，当且仅当它对应的某一组命题逻辑命题是不可满足的

- 命题逻辑实例：**Herbrand实例**
- 去掉量词，**用具体的项替换变量**，从而将**A**“降级”为一系列命题逻辑的命题
- 虽然降级过程可能是无限的，**但是如果存在反例，那么反例的降级过程一定是有限的！**
  - 现代定理证明器/逻辑求解器的基石

证明思路：如何处理无限的模型

- Step1：斯科伦化
  - 目标：去除公式**A**的可满足模型的非确定性
  - 动作：用一个具体的函数**f()**替代存在量词**∃x**
- Step2：构建**Herbrand结构**
  - 目标：去除公式**A**的可满足模型的论域的语义
  - 动作：基于函数**f()**和常量**c**，构建一个符号世界“沙盒”
- Step3：**Herbrand定理**
  - 目标：建立公式**A**与命题逻辑命题集合**Γ**的对应
  - 动作：将一个“沙盒”元素带入公式**A**，得到一个命题**A′**
  - 结论：如果命题**A′**不可满足，则原公式**A**不可满足

Part3.1-斯科伦范式与斯科伦定理

斯科伦化 The Skolemization

- 可满足模型的非确定性
  - ∃x(P(x)) 只声明了一个元素的存在性，但是没有提供如何找到这个元素的线索
  - ∀ door ∃ key Open(door, key)
- 斯科伦的应对方法：建立这个元素和其他元素的联系
  - 引入一个函数f()，能够基于door，产生对应的“key”
    - 严格而言产生的是f(door)，而不是key！
    - 除了∃x外有其他变元： f()的定义域是所有其他变元
    - 除了∃x外没有其他变元： f()的定义域是一个常元c
  - 斯科伦化的公式中只有全称量词
- **斯科伦定理：斯科伦范式可满足等价于原公式可满足**

前束范式

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

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

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$(A \to B) \wedge (B \to A)$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$\forall$。

前束范式的性质(1)

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 $\vdash Qx.B \leftrightarrow Qy.B[\frac{y}{x}]$。

前束范式的性质(2)

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

前束范式的存在性与等价性

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$\vdash A \leftrightarrow Q_1x_1...Q_nx_n.B$，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

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

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

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

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

这里 B, C 中无量词。从而有互异的新变元$z_1, ..., z_l$

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

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

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

情况4. A为$E \to F$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$\vdash C \leftrightarrow Q_1 x_1 ... Q_m x_m . B$，从而

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

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

□

斯科伦范式 Skolem Normal Form

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$FV(\exists x.A) = \{x_1, x_2, ..., x_n\}$

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

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

(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。

斯科伦定理

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$S_{\vec{a}}=\{b|(**)\text{成立}\}$，$\because S_{\vec{a}}\neq\varnothing$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。 □

Part3.2-埃尔布朗结构与埃尔布朗定理

Herbrand结构

- 利用公式**A**的符号本身构建模型
  - 模型对应于公式自身，而非外部世界
  - 常量：某个符号　　函数：某些符号的拼接
- 论域：**Herbrand域**
  - 由所有可能的闭项组成的集合**H={c,f(c),g(c,c), f(f(c)),...}**
- 映射：
  - 常量：自身 **I(c) = "c"**
  - 函数：字符串的拼接 **I(f)(t_1,t2)=“f(t_1, t2)”**
  - 谓词：根据公式的具体情况，可以随意指派

关联Herbrand结构

- 如果给定目标公式**A**的模型$\mathcal{M}$，则可做出该模型在**Herbrand域**上的投影$\mathcal{H}$，称为**关联Herbrand结构**
- 谓词映射：$\mathcal{H} \models P(t_1,\ldots,t_n) \Leftrightarrow \mathcal{M} \models P(t_1^m,\ldots,t_n^m)$
  - 如果符号**t**在$\mathcal{M}$中指代的对象具有**P**性质，那么该符号在$\mathcal{H}$中也具有**P**性质

Herbrand定理

- 斯科伦化的公式呈形$\forall x_1 \ldots \forall x_n \ M(x_1,\ldots,x_n)$
  - M内部无量词，只有自由变元
  - $\forall x_1 \ldots \forall x_n$意味着模型对变元的赋值没有任何限制
- Herbrand域 {c, f(c), f(f(c)), ... }
  - 描述了公式中所有可能的符号组合
- 基实例 $M([x_1/t_1],\ldots,[x_n/t_n])$
  - 把Herbrand域中的元素，依次替换M的变元
  - 替换是任意且可以重复的

$M([x_1/t_1],\ldots,[x_n/t_n])$不可满足，则原公式不可满足

Herbrand域

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。

关联Herbrand结构

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，

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

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

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

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

$I_A(P)={H_A}^m\cap I(P)$，从而

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

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
$\mathbb{H}_A \vDash P(t_1, ..., t_m) \Leftrightarrow \mathbb{M} \vDash P(t_1, ..., t_m)$。

$\mathcal{H}$与$\mathcal{M}$的等价性

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。 □

Herbrand定理

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$\Leftrightarrow$ Γ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$P(S_1, ..., S_m)$，

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

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

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

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。 □