第一章 命题演算

刘贵全

gqliu@ustc.edu.cn

§0 预备知识

内容提要

0.0 发展历史
0.1 集合论
0.2 Peano自然数公理
0.3 可数集

§0.0 发展历史

- **形式逻辑始于亚里士多德**
  - 对概念、判断、推理及基本思维规律作了系统研究。
  - 局限：研究对象范围狭窄，限于主宾式语句和三段论；未对量词加以研究，等等。
- **莱布尼兹**设想能通过计算实现逻辑推理：确定几个基本概念(并符号化)，基本概念之间不得自相矛盾；所有概念都可通过基本概念复合得到。
  - 布尔部分实现了莱布尼兹的愿望：布尔代数
  - 弗雷格、罗素、怀特海等逻辑学家、哲学家对现代逻辑学作出了创造性贡献：《数学原理》

§0.0 发展历史

- **逻辑学**的发展与数学的公理化和形式化进程是互相推进的。
  - **Hilbert规划**（一切能证明的都要证明）
  - **Gödel不完备性定理**
- **逻辑的应用**
  - 人工智能：知识表示、推理与证明、规划…
  - 自然语言理解
  - 程序验证（科创验证学习平台：https://www.kcv4c.com）
  - 此外，为证明歌德尔定理而提出和发展起来的递归函数论是整个计算机科学的理论基础。无论是研究算法，研究编程语言，研究程序，还是研究程序数据，它都是必需的基本理论。

§0.0 发展历史

- **几个概念**
  - **元语言与形式语言**
  - **元系统与形式系统**
- **课程规划**
  - 以可数语言为基础的一阶逻辑系统
  - 命题演算和谓词演算的可靠性与完全性
  - 递归函数、歌德尔定理、图灵机等将在进阶课程中讲授。

§0.1 集合论初等概念

- 子集与包含($\subseteq$)
- 集合的相等：$A=B \Leftrightarrow A\subseteq B$ 且 $B\subseteq A$
- 幂集
- 集合的运算：并($\cup$)，交($\cap$)，差(-)
- 集合与集合的积($\times$)集，n元关系与二元关系
- 等价关系
- 映射，等势
- n元函数与n元运算：集合A上的n元函数(映射) $f: A^n \rightarrow A$叫做A上的n元运算。

§0.2 Peano自然数公理

- 把自然数集**N**看成满足以下五条公理的集：
  - $0 \in \mathbf{N}$.
  - 若$x \in \mathbf{N}$，则x有且只有一个后继$x' \in \mathbf{N}$.
  - 对任意$x \in \mathbf{N}$，$x' \neq 0$.
  - 对任意$x_1, x_2 \in \mathbf{N}$，$x_1' \neq x_2'$.
  - 设$M \subseteq \mathbf{N}$. 若$0 \in M$，且当$x \in M$时也有$x' \in M$，则$M = \mathbf{N}$.
- 基于上述公理，自然数的很多性质可建立，如：非空的自然数集中必有最小数。

§0.2 Peano自然数公理

- **定理1(强归纳法)** 假设关于自然数n的命题P(n)满足以下条件:
  1) P(0)成立;
  2) 对于m>0，若k<m时P(k)都成立，则P(m)也成立。

  那么对任何自然数n， P(n)都成立。

  - 证明：集合S={n|P(n)不成立}= Φ。

- 数论函数、递归定义

§0.3 可数集

- **有限集**：空集或与{0,1,…,n}等势的集($n\in\mathbf{N}$)
- **可数集**：与N等势的集
- 本节的命题及其证明同学们自己课下看看，课堂上不讲证明过程。

§1 命题逻辑

内容提要

1.1 命题联结词与真值表
1.2 命题演算(L)的建立
1.3 命题演算的语义
1.4 命题演算L的可靠性与完全性
1.5 命题演算的其他课题

§1.1 命题联结词与真值表

- **命题与真值**

  命题：判断结果惟一的陈述句

  命题的**真值**：判断的结果

  真值的取值：真(1)与假(0)

  真命题与假命题

- **注意**：

  感叹句、祈使句、疑问句都不是命题

  陈述句中判断结果不惟一确定的不是命题

§1.1 命题联结词与真值表

- **否定词(¬)**

设p是任意给定的命题，则¬p表示一新命题，读作“非p”,为“命题p的否定命题”。

¬p为真 ⇔ p为假

p	¬*p*
0	**1**
1	**0**

§1.1 命题联结词与真值表

- **合取词(∧)**

设p,q是任意命题，则p∧q表示p与q的合取命题，读作“p与(并且)q”。

p∧q为真 ⇔ p与q都为真

p	*q*	*p*∧*q*
0	0	0
0	1	0
1	0	0
1	1	1

§1.1 命题联结词与真值表

- **析取词(∨)**

设p,q是任意命题，则p∨q表示p与q的析取命题，读作“p或q”。

p∨q为真 ⇔ p为真或q为真

➢ 可兼或与不可兼或

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

§1.1 命题联结词与真值表

- **蕴涵词(→)**

设p,q是任意命题，则p→q表示命题 “若p，则q”。

p→q为假 ⇔ p为真且q为假

p	q	$p \to q$
0	0	1
0	1	1
1	0	0
1	1	1

蕴涵式p→q中， p叫做该式的“前件”，q叫做该式的“后件”

§1.1 命题联结词与真值表

- **等价词(↔)**

  设p,q是任意命题，则p↔q表示命题 “p当且仅当q”。

  p↔q为真 ⇔ p与q同为真或同为假

p	*q*	*p*↔*q*
0	0	1
0	1	0
1	0	0
1	1	1

§1.1 命题联结词与真值表

- 通过真值表确定复合命题的真值(真、假)

例1 (¬p)∧q的真值表如下

$(\neg\ p)$		∧	q
1	0	0	0
1	0	1	1
0	1	0	0
0	1	0	1

(0,1)称为(¬p)∧q的**成真指派**， p与q的其他真值组合称为**成假指派**。

§1.1 命题联结词与真值表

例2 $(p \vee q) \rightarrow (\neg r \wedge q)$的真值表

$(p \vee q)$		$\rightarrow$	$(\neg r \wedge q)$	
0	0		0	0
0	0		1	0
0	1		0	1
0	1		1	1
1	0		0	0
1	0		1	0
1	1		0	1
1	1		1	1

§1.1 命题联结词与真值表

- 通过真值表确定复合命题的真值(真、假)

例3 $(p\vee q)\leftrightarrow((\neg p)\rightarrow q)$的真值表如下

$(p$	$\vee$	$q)$	$\leftrightarrow$	$((\neg$	$p)$	$\rightarrow$	$q)$
0	0	0	1	1	0	0	0
0	1	1	1	1	0	1	1
1	1	0	1	0	1	1	0
1	1	1	1	0	1	1	1

永真式与永假式

§1.2 命题演算的建立

- 命题演算的形式化、公理化：只用¬、→

1.2.1 命题演算公式集

- 命题演算公式形成规则

1) (可数)命题变元$x_1,x_2,\ldots,x_n,\ldots$中的每一个都是公式；
2) 若p是公式，则$\neg p$是公式；若p,q是公式，则$p\rightarrow q$是公式；
3) 任一公式皆由1)、2)的有限次使用所形成。

- 记$X=\{x_1,x_2,\ldots,x_n,\ldots\}$. 用L(X)表示所有公式构成的集合，则L(X)可进行分层

$$L(X)=L_0\cup L_1\cup\ldots L_n\cup\ldots$$

§1.2.1 命题演算公式集

其中

$$L_0=X=\{x_1,x_2,\ldots,x_n,\ldots\},$$

$$L_1=\{\neg x_1,\ \neg x_2,\ldots,\ \neg x_n,\ldots,$$

$$x_1\to x_1,\ x_1\to x_2,\ \ldots,\ x_1\to x_n,\ \ldots,$$

$$x_2\to x_1,\ x_2\to x_2,\ \ldots,\ x_2\to x_n,\ \ldots,$$

$$\ldots,\ x_n\to x_1,\ x_n\to x_2,\ \ldots,\ x_n\to x_n,\ \ldots\},$$

$$L_2=\{\neg(\neg x_1),\ \neg(\neg x_2),\ldots,\ \neg(\neg x_n),\ldots,$$

$$x_1\to(\neg x_1),\ (\neg x_1)\to x_1,\ \ldots,\ x_1\to(\neg x_n),\ \ldots,$$

$$(\neg x_1)\to x_n,\ \ldots\},$$

……

§1.2.1 命题演算公式集

- 说明

1) L_1中公式由L_0中变元经过一次运算得来, L_2中公式由L_0中变元经过二次运算得来, …

2) L(X)具有分层性——不同层次之间无公共元素。

3) $L_i(i\in N)$都是可数集，故L(X)是可数集。

- 有时从集合$X_n=\{x_1,x_2,\ldots,x_n\}$以同样方式建立公式集$L(X_n)$，$L(X_n)$与L(X)具有相同的性质

- 附1和附2大家看看。

§1.2.2 命题演算L

- **定义1(命题演算L)**

命题变元集X={x_1,x_2,…}上的命题演算L是指带有下面规定的“公理”和“证明”的命题代数L(X):

1) “公理”

取L(X)中如下模式的公式作为“公理”

(L1) $p\rightarrow(q\rightarrow p)$ (肯定后件律)

(L2) $(p\rightarrow(q\rightarrow r))\rightarrow((p\rightarrow q)\rightarrow(p\rightarrow r))$ (蕴涵词分配律)

(L3) $(\neg p\rightarrow\neg q)\rightarrow(q\rightarrow p)$ (换位律)

其中$p,q,r\in L(X)$是任意公式。

§1.2.2 命题演算L

- **命题演算L**

2) “证明”

设$\Gamma \subseteq L(X)$， $p \in L(X)$。“**公式p从公式集Γ可证**”，指存在L(X)的公式的**有限序列**$p_1,\ldots,p_n(=p)$，且$p_k(k=1,\ldots,n)$满足：

(i) $p_k \in \Gamma$，或

(ii) p_k为“公理”，或

(iii) 存在$i,j<k$使$p_j=p_i \to p_k$.

具有上述性质的有限序列$p_1,\ldots,p_n$叫做p从Γ的“证明”。

§1.2.2 命题演算L

- 说明

1) 命题演算L以L(X)为基础框架，增加了新的逻辑结构。

2) 这里的“公理”和“证明”是命题演算L 中的数学概念(“公理” 是L(X)中的一些特殊公式,“证明” 是L(X)中的一些公式组成的具有特殊性质的有限序列)。 “证明”也叫形式证明；后面常把引号去掉。

3) “公理”中的p,q,r是L(X)的任意元素，因此(L1),(L2),(L3)是三种(公理)模式，有无数条公式。

4) “公理”的取法不唯一。

5) 若p从Γ可证，则“证明”不唯一。

6) “证明”中规则(iii)说的是，如果序列前面已有p_i和$p_i \rightarrow p_k$，则可在后面写出p_k。

§1.2.2 命题演算L

- **定义2 (语法推论)**

1) 若公式p从公式集Γ可证，则写成Γ⊢p，必要时也可写成Γ⊢ $_L$ p。Γ中的公式叫做“假定”，p叫做假定集Γ的**语法推论**。

2) 若∅⊢p，则称p为L的“定理”，记作⊢p，这时p的证明简称为p在L中的证明。

3) 在一个证明中，当$p_j=p_i\rightarrow p_k(i,j<k)$时，就说$p_k$由 p_i, $p_i\rightarrow p_k$使用假言推理(Modus Ponens)规则而得，或简单地说“使用MP而得”。

§1.2.2 命题演算L

- “证明”的一些性质

1) 若p是L的公理，则对任意公式集Γ，都有Γ⊢p。

2) 若 ⊢ p (即p为L的定理)，则对任意公式集Γ，都有Γ ⊢ p。

3) 若p∈Γ，则Γ⊢p。

4) {p, p→q}⊢q。

5) 若Γ⊢p_n且p_1,…,p_n是p_n从Γ的一个证明，则对于k=1,…,n,有Γ⊢p_k且p_1,…,p_k是p_k从Γ的一个证明。

6) 若Γ是无限集且Γ⊢p，则存在Γ的有限子集Δ使Δ⊢p。

例1 证明 {p}⊢q→p.

§1.2.2 命题演算L

例2 证明 $\vdash(x_1\to x_2)\to(x_1\to x_1)$.

例3 证明 $\{x_1, x_2\to(x_1\to x_3)\}\vdash x_2\to x_3$.

命题1 $\vdash p\to p$ (同一律)

证 下面给出$p\to p$在L中的一个证明：

(1) $p\to((p\to p)\to p)$ (L1)

(2) $(p\to((p\to p)\to p))\to((p\to(p\to p))\to(p\to p))$ (L2)

(3) $(p\to(p\to p))\to(p\to p)$ (1),(2),MP

(4) $p\to(p\to p)$ (L1)

(5) $p\to p$ (3),(4),MP

§1.2.2 命题演算L

命题2 $\vdash \neg q \rightarrow (q \rightarrow p)$ **(否定前件律)**

证 下面给出一个证明：

(1) $(\neg p \rightarrow \neg q) \rightarrow (q \rightarrow p)$ (L3)

(2) $((\neg p \rightarrow \neg q) \rightarrow (q \rightarrow p)) \rightarrow (\neg q \rightarrow ((\neg p \rightarrow \neg q) \rightarrow (q \rightarrow p)))$ (L2)

(3) $\neg q \rightarrow ((\neg p \rightarrow \neg q) \rightarrow (q \rightarrow p))$ (1),(2),MP

(4) $(\neg q \rightarrow ((\neg p \rightarrow \neg q) \rightarrow (q \rightarrow p))) \rightarrow$
$((\neg q \rightarrow (\neg p \rightarrow \neg q)) \rightarrow (\neg q \rightarrow (q \rightarrow p)))$ (L2)

(5) $(\neg q \rightarrow (\neg p \rightarrow \neg q)) \rightarrow (\neg q \rightarrow (q \rightarrow p))$ (3),(4),MP

(6) $\neg q \rightarrow (\neg p \rightarrow \neg q)$ (L1)

(7) $\neg q \rightarrow (q \rightarrow p)$ (5),(6),MP

§1.2.2 命题演算L

定义3(无矛盾公式集) 如果对任何公式q，Γ⊢q和Γ⊢ ¬q二者都不同时成立，就称公式集Γ为**无矛盾公式集**，否则称Γ是**有矛盾公式集**。

命题3 若Γ是有矛盾公式集，则对任意公式p, 都有Γ ⊢ p。

证 若Γ是有矛盾公式集，则存在公式q，使得Γ⊢q和Γ⊢ ¬q同时成立，于是可得p从Γ的一个证明：

…, q, …, ¬q, ¬q→(q→p), q→p, p

上面用到了命题2的结论。

§1.2.3 演绎定理

定理 (演绎定理) $\Gamma\cup\{p\}\vdash q \Leftrightarrow \Gamma\vdash p\to q$。

证 ($\Leftarrow$) 假定$\Gamma\vdash p\to q$。由定义，$p\to q$在L中有一个从Γ的证明$p_1,\ldots,p_n(=p\to q)$，于是

$$p_1,\ldots,p_n(=p\to q), q$$

为q在L中从$\Gamma\cup\{p\}$的证明。

($\Rightarrow$) 假定$\Gamma\cup\{p\}\vdash q$，并设$q_1,\ldots,q_n(=q)$是q从$\Gamma\cup\{p\}$的一个证明。下面对以上证明的长度n归纳地证明$\Gamma\vdash p\to q$。

1) n=1时，有三种可能：$q=p$, $q\in\Gamma$或q是公理。这时都有$\Gamma\vdash p\to q$：$q=p$时，由1.2.2命题1知$\Gamma\vdash p\to p$，也就是$\Gamma\vdash p\to q$；当$q\in\Gamma$或q是公理时，下面即为$p\to q$从Γ的一个证明

$$q, q\to(p\to q), p\to q$$

§1.2.3 演绎定理

2) n>1时，有四种可能：q=p, q∈Γ, q是公理或q是使用MP而得。

下面只需讨论q由q_i及$q_j=q_i\to q$使用MP而得的情形。因为i,j<n，由归纳假设

$$\Gamma\cup\{p\}\vdash q_i \Leftrightarrow \Gamma\vdash p\to q_i$$

$$\Gamma\cup\{p\}\vdash q_j \Leftrightarrow \Gamma\vdash p\to q_j \text{ 即}\Gamma\vdash p\to(q_i\to q)$$

于是可得到p→q从Γ的一个证明：

(1) ……

……

(k) $p\to q_i$

} $p\to q_i$从Γ的一个证明

§1.2.3 演绎定理

$(k+1)$ ……
……
(l) $p\rightarrow(q_i\rightarrow q)$

} $p\rightarrow(q_i\rightarrow q)$从Γ的一个证明

$(l+1)$ $(p\rightarrow(q_i\rightarrow q))\rightarrow((p\rightarrow q_i)\rightarrow(p\rightarrow q))$ (L2)

$(l+2)$ $(p\rightarrow q_i)\rightarrow(p\rightarrow q)$ $(l),(l+1)$,MP

$(l+3)$ $p\rightarrow q$ $(k),(l+2)$,MP

以上就完成了归纳过程。

§1.2.3 演绎定理

推论 (假设三段论) $\{p\to q, q\to r\} \vdash p\to r$。

证 由演绎定理，只需证$\{p\to q, q\to r, p\} \vdash r$。我们很容易写出r从$\{p\to q, q\to r, p\}$的证明：

- 假设三段论记作HS，以后可作为推理规则直接引用。
- 在演绎定理的证明过程中没有用到(L3)，说明把(L3)去掉或换成别的公理，演绎定理对新的命题演算系统仍然成立。

§1.2.3 演绎定理

例1 重新证明 $\vdash \neg q \rightarrow (q \rightarrow p)$ 。

证 由演绎定理，只要证$\{\neg q\} \vdash q \rightarrow p$。下面是$q \rightarrow p$从$\{\neg q\}$的证明：

(1)	$\neg q \rightarrow (\neg p \rightarrow \neg q)$	(L1)
(2)	$\neg q$	假定
(3)	$(\neg p \rightarrow \neg q)$	(1),(2),MP
(4)	$(\neg p \rightarrow \neg q) \rightarrow (q \rightarrow p)$	(L3)
(5)	$q \rightarrow p$	(3),(4),MP

§1.2.3 演绎定理

命题1(否定肯定律) 重新证明 $\vdash (\neg p \to p) \to p$ 。

证 由演绎定理，只用证$\{\neg p \to p\} \vdash p$。下面是p从$\{\neg p \to p\}$的证明：

(1) $\neg p \to (p \to \neg(\neg p \to p))$	(否定前件律)
(2) $(\neg p \to (p \to \neg(\neg p \to p))) \to ((\neg p \to p) \to (\neg p \to \neg(\neg p \to p))$	(L2)
(3) $(\neg p \to p) \to (\neg p \to \neg(\neg p \to p))$	(1),(2),MP
(4) $\neg p \to p$	假定
(5) $\neg p \to \neg(\neg p \to p)$	(3),(4),MP
(6) $(\neg p \to \neg(\neg p \to p)) \to ((\neg p \to p) \to p)$	(L3)
(7) $(\neg p \to p) \to p$	(5),(6),MP
(8) p	(4),(7),MP

§1.2.4 反证律与归谬律

定理1(反证律)

$$\left.\begin{array}{l}\Gamma \cup \{\neg p\} \vdash q \\ \Gamma \cup \{\neg p\} \vdash \neg q\end{array}\right\} \Rightarrow \Gamma \vdash \mathrm{p}$$

证 由于q和¬q都从Γ∪ {¬p}可证，于是可以给出p从Γ∪ {¬p}的证明：

$$\left.\begin{array}{ll}(1) & \cdots\cdots \\ & \cdots\cdots \\ (k) & q\end{array}\right\} \quad \mathrm{q从\Gamma \cup \{\neg p\}的一个证明}$$

$$\left.\begin{array}{ll}(k+1) & \cdots\cdots \\ & \cdots\cdots \\ (l) & \neg q\end{array}\right\} \quad \neg\mathrm{q从\Gamma \cup \{\neg p\}的一个证明}$$

§1.2.4 反证律与归谬律

(l+1) ¬q → (q→p) 否定前件律

(l+2) q→p (l),(l+1),MP

(l+3) p (k),(l+2),MP

至此证明了Γ∪ {¬p} ⊢ p (但未达到Γ ⊢ p)。我们用一次演绎定理可得Γ ⊢ ¬p→p，由此可将p从Γ的证明构造出来：

(1) .....

.....

(m) ¬p→p

} ¬p→p从Γ的一个证明

(m+1) (¬p→p)→p 否定肯定律

(m+2) p (m),(m+1),MP

于是有 Γ ⊢ p。

§1.2.4 反证律与归谬律

- 反证律与我们熟悉的反证法原理一致：为证一个命题，先否定它，如果推出矛盾，就可以肯定它。
- 反证律的证明没直接应用(L3)，但使用的否定前件律和否定肯定律都需要(L3)。

例1 证明 $\vdash (\neg p\to\neg q)\to((\neg p\to q)\to p)$.

证 由演绎定理，只用证$\{\neg p\to\neg q, \neg p\to q\}\vdash p$。为用反证律，将$\neg p$作为新假定，则以下公式从$\{\neg p\to\neg q, \neg p\to q, \neg p\}$可证：

(1) $\neg p$	假定
(2) $\neg p\to\neg q$	假定
(3) $\neg q$	(1),(2),MP
(4) $\neg p\to q$	假定
(5) q	(1),(4),MP

§1.2.4 反证律与归谬律

由(3),(5)用反证律即得{¬p→¬q, ¬p→q} ⊢ p。 毕

而只用演绎定理证明则要长一些。

定理1的推论 (双重否定律)

1) {¬¬p} ⊢ p,

2) ⊢ ¬¬p→p

证 用反证律证1)，把¬p作为新假定，然后可得

(i) {¬¬p, ¬p} ⊢ ¬p,

(ii) {¬¬p, ¬p} ⊢ ¬(¬p).

由(i),(ii)用反证律即得{¬¬p} ⊢ p，再用演绎定理可得2)。

§1.2.4 反证律与归谬律

定理2 (归谬律)

$$\left.\begin{array}{l}\Gamma \cup \{p\} \vdash q \\ \Gamma \cup \{p\} \vdash \neg q\end{array}\right\} \Rightarrow \Gamma \vdash \neg p$$

证 由于Γ∪{p} ⊢ q，故存在q从Γ∪{p}的证明，在该证明中所有出现的p之前都插入¬¬p和¬¬p→p这两项，于是该证明就变成了q从Γ∪{¬¬ p}的证明，从而

(1) Γ∪{¬¬ p} ⊢ q,

同理由已知条件Γ∪{p} ⊢ ¬q可以得到

(2) Γ∪{¬¬ p} ⊢ ¬q.

由(1),(2)用反证律即得Γ ⊢ ¬ p。这样从反证律推出了归谬律。

§1.2.4 反证律与归谬律

例2 证明 $\vdash p\to(\neg q \to \neg(p\to q))$.

由演绎定理，只用证$\{p,\neg q\} \vdash \neg(p\to q)$。再把$p\to q$ 作为新假定，立即可得…

定理2的推论 (第二双重否定律)

1) $\{p\} \vdash \neg\neg p$,

2) $\vdash p\to\neg\neg p$

证 因为

(i) $\{p, \neg p\} \vdash p$,

(ii) $\{p, \neg p\} \vdash \neg p$.

由(i),(ii)用归谬律即得$\{p\} \vdash \neg\neg p$，再用演绎定理可得2)。

§1.2.5 析取、合取与等值

在{¬, →}型代数L(X)中，可定义二元运算∨(析取)、∧(合取)、↔(等值)：

$$p \vee q =_{df} \neg p \rightarrow q$$

$$p \wedge q =_{df} \neg(p \rightarrow \neg q)$$

$$p \leftrightarrow q =_{df} (p \rightarrow q) \wedge (q \rightarrow p)$$

命题1

1) $\vdash p \rightarrow (p \vee q)$,
2) $\vdash q \rightarrow (p \vee q)$,
3) $\vdash (p \vee q) \rightarrow (q \vee p)$,
4) $\vdash (p \vee p) \rightarrow p$,
5) $\vdash \neg p \vee p$. (排中律)

§1.2.5 析取、合取与等值

证 1) 由否定前件律$\vdash \neg p \rightarrow (p \rightarrow q)$及演绎定理(两次)，得

$\{\neg p, p\} \vdash q$

再重新用两次演绎定理便得$\vdash p \rightarrow (\neg p \rightarrow q)$，此即1)。

2) $q \rightarrow (\neg p \rightarrow q)$是(L1)型公理。

4) $(p \vee p) \rightarrow p$就是否定肯定律。

5) 排中律就是双重否定律。

命题2

1) $\vdash (p \wedge q) \rightarrow p$,

2) $\vdash (p \wedge q) \rightarrow q$,

3) $\vdash (p \wedge q) \rightarrow (q \wedge p)$,

§1.2.5 析取、合取与等值

4) $\vdash p \to (p \wedge p)$,

5) $\vdash p \to (q \to (p \wedge q))$,

6) $\vdash \neg(p \wedge \neg p)$. (矛盾律)

证 1) 即要证$\vdash \neg(p \to \neg q) \to p$，以下是一个证明

(1) $\neg p \to (p \to \neg q)$	否定前件律
(2) $(\neg p \to (p \to \neg q)) \to (\neg(p \to \neg q) \to \neg\neg p)$	换位律
(3) $\neg(p \to \neg q) \to \neg\neg p$	(1),(2),MP
(4) $\neg\neg p \to p$	双重否定律
(5) $\neg(p \to \neg q) \to p$	(3),(4),HS

矛盾律$\neg(p \wedge \neg p)$就是$\neg\neg(p \to \neg\neg p)$，用第二双重否定律进行证明。其余的证明都是类似的。

§1.2.5 析取、合取与等值

命题3

1) $\vdash (p \leftrightarrow q) \rightarrow (p \rightarrow q)$,
2) $\vdash (p \leftrightarrow q) \rightarrow (q \rightarrow p)$,
3) $\vdash (p \leftrightarrow q) \rightarrow (q \leftrightarrow p)$,
4) $\vdash (p \leftrightarrow q) \rightarrow (\neg p \leftrightarrow \neg q)$,
5) $\vdash (p \rightarrow q) \rightarrow ((q \rightarrow p) \rightarrow (p \leftrightarrow q))$.

命题4 (De. Morgan律)

1) $\vdash \neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$,
2) $\vdash \neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$,

§1.3 命题演算的语义

1.3.1 真值函数

记$\mathbf{Z}_2$={0,1}.

定义1 (真值函数) 函数$f: \boldsymbol{Z_2^n} \to \mathbf{Z}_2$ (即$\mathbf{Z}_2$上的n元运算)叫做n元真值函数。

一元真值函数共有4个，分别用f_1, f_2, f_3, f_4表示：

$v \in \mathbf{Z}_2$	$f_1(v)$	$f_2(v)$	$f_3(v)$	$f_4(v)$
1	1	1	0	0
0	1	0	1	0

f_1和 f_4是常函数。 f_2是恒等函数$f_2(v)= v$。 f_3叫做“非”运算或“否定”运算，也用¬表示： $f_3(v)= \neg v = 1- v$.

§1.3.1 真值函数

二元真值函数共有16个：

v_1	v_2	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
1	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0
0	1	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0

其中，f_4 和 f_6是坐标函数；f_5叫做“蕴涵”运算，也用$\rightarrow$表示：

$$v_1 \rightarrow v_2 = f_5(v_1, v_2) = 1 - v_1 + v_1 v_2$$

- 容易看出，$\mathbf{Z}_2$上的运算$\neg$和$\rightarrow$与L(X)具有相似性。实际上，$\mathbf{Z}_2$也是一种$\{\neg, \rightarrow\}$型代数。

§1.3.1 真值函数

公式1 $\neg\neg v = v$,

公式2 $1 \to v = v$,

公式3 $v \to 1 = 1$,

公式4 $v \to 0 = \neg v$,

公式5 $0 \to v = 1$.

现将16个二元真值函数中的f_2, f_8, f_7分别用$\vee$, $\wedge$, $\leftrightarrow$表示。

公式6 $v_1 \vee v_2 = \neg v_1 \to v_2$,

公式7 $v_1 \wedge v_2 = \neg(v_1 \to \neg v_2)$,

公式8 $v_1 \leftrightarrow v_2 = (v_1 \to v_2) \wedge (v_2 \to v_1)$.

- n元真值函数有2^{2^n}个。

§1.3.1 真值函数

命题1 任一真值函数都可用一元运算¬和二元运算→表示出来。

证 对真值函数的元数n应用归纳法。

n=1时，$f_1(v) = 1 = v \to v$，$f_2(v) = v$，

$f_3(v) = \neg v$，$f_4(v) = 0 = \neg(v \to v)$.

命题正确。

n>1时，对任意n元真值函数$f: \mathbf{Z}_2^n \to \mathbf{Z}_2$，以及任意$v_1, v_2, \ldots, v_n \in \mathbf{Z}_2$，令

$$g(v_1, v_2, \ldots, v_{n-1}) = f(v_1, v_2, \ldots, v_{n-1}, 1),$$

$$h(v_1, v_2, \ldots, v_{n-1}) = f(v_1, v_2, \ldots, v_{n-1}, 0),$$

$$k(v_1, v_2, \ldots, v_{n-1}, v_n) = (h(v_1, v_2, \ldots, v_{n-1}) \to v_n) \to (\neg(g(v_1, v_2, \ldots, v_{n-1}) \to \neg v_n))$$

§1.3.1 真值函数

这样定义了三个新的真值函数：g, h和k；g和h是n-1元的，k是n元的。由归纳假设， g和h可用¬和→表示出来，于是k也可用¬和→表示出来。

下证 k = f，从而f 也具有这种性质。

$$k(v_1, v_2,\ldots, v_{n-1}, 1) = (h(v_1, v_2,\ldots, v_{n-1}) \to 1)\to$$
$$(\neg(g(v_1, v_2,\ldots, v_{n-1}) \to 0)) = 1 \to \neg\neg g(v_1, v_2,\ldots, v_{n-1})$$
$$= g(v_1, v_2,\ldots, v_{n-1}) = f(v_1, v_2,\ldots, v_{n-1}, 1)$$

$$k(v_1, v_2,\ldots, v_{n-1}, 0) = (h(v_1, v_2,\ldots, v_{n-1}) \to 0)\to$$
$$(\neg(g(v_1, v_2,\ldots, v_{n-1}) \to 1)) = \neg h(v_1, v_2,\ldots, v_{n-1}) \to 0$$
$$= h(v_1, v_2,\ldots, v_{n-1}) = f(v_1, v_2,\ldots, v_{n-1}, 0)$$

以上说明任意$v_1, v_2, \ldots, v_n \in \mathbf{Z}_2$，都有

$$k(v_1, v_2,\ldots, v_{n-1}, v_n) = f(v_1, v_2,\ldots, v_{n-1}, v_n) \quad \ldots$$

§1.3.2 赋值与语义推论

- 下面在L(X)与$\mathbf{Z}_2$之间建立适当联系。
- 在L(X)中，公式有分层性，$\neg\neg x_1 \neq x_1$；而在$\mathbf{Z}_2$中$\neg\neg v = v$.

定义1(赋值) 具有“保运算性”的映射v: L(X)→$\mathbf{Z}_2$叫做L(X)的赋值。映射v具有保运算性，是指对任意p、q∈L(X)，v都满足：

(1) v(¬p) = ¬v(p),

(2) v(p→q) = v(p)→v(q).

此时，对任意公式p∈L(X)，v(p)叫做p的**真值**。具有保运算性的映射v: L(X_n)→$\mathbf{Z}_2$叫做L(X_n) 的赋值，$X_n=\{x_1,x_2,\ldots,x_n\}$。

- 赋值不能随意定义。
- **思考**：赋值的存在性(赋值的良定义性)。

§1.3.2 赋值与语义推论

命题1 设v: L(X)→$\mathbf{Z}_2$是L(X) 的赋值，则v对∨、∧、↔也具有保运算性，即对任意p、q∈L(X)，有：

$$v(p \vee q) = v(p) \vee v(q),\ v(p \wedge q) = v(p) \wedge v(q),$$

$$v(p \leftrightarrow q) = v(p) \leftrightarrow v(q).$$

证 $v(p \vee q) = v(\neg p \rightarrow q) = v(\neg p) \rightarrow v(q)$

$$= \neg v(p) \rightarrow v(q)$$

$$= v(p) \vee v(q)\ 。$$

…

定义2(真值指派) 映射v_0: X→$\mathbf{Z}_2$叫做命题变元的真值指派。若把X 换成$X_n=\{x_1,x_2,\ldots,x_n\}$，则$v_0$叫做$x_1,x_2,\ldots,x_n$的真值指派。

§1.3.2 赋值与语义推论

定理1 命题变元的任一真值指派，必可**唯一地**扩张成L(X)的赋值；$x_1,x_2,\ldots,x_n$的任一真值指派，必可**唯一地**扩张成$L(X_n)$的赋值。

证 对于给定的命题变元真值指派$v_0: X\to \mathbf{Z}_2$，归纳定义映射$v: L(X)\to \mathbf{Z}_2$如下，

首先，令$v(x_i)=v_0(x_i)$, $i\in \mathbf{N}$.

对L(X)其他层次的公式p，

(i) 当$p = \neg q$时，令$v(p) = \neg v(q)$,

(ii) 当$p = q\to r$时，令$v(p) = v(q)\to v(r)$.

于是v自然满足赋值所需的条件(见定义1)，且v是v_0的扩张。

§1.3.2 赋值与语义推论

扩张的唯一性：假设另有L(X)的赋值v′也是v_0的扩张，下面对(任一)公式p在L(X)中的层次归纳证明v(p)=v′(p).

p = x_i时，有v′(x_i)=v_0(x_i)=v(x_i). (v与v′都是v_0的扩张)

p = ¬q时，有 v′(p)=v′(¬q)=¬v′(q) (赋值条件(1))

=¬v(q) (用归纳假设)

=v(¬q) (赋值条件(1))

=v(p)

p = q→r时，有

v′(p)=v′(q→r)=v′(q)→v′(r) (赋值条件(2))

= v(q)→v(r) (用归纳假设)

=v(q→r) (赋值条件(2))

=v(p)

§1.3.2 赋值与语义推论

因此v′ = v。$L(X_n)$部分的证明与上面完全是一样的。 □

- $L(X_n)$中的任一公式常写为$p(x_1,x_2,\ldots,x_n)$. 这表示公式p所包含的命题变元在X_n中，并不要求$x_1,x_2,\ldots,x_n$全部出现在p中。
- 对于公式$p(x_1,x_2,\ldots,x_n)$及$v_1,v_2,\ldots,v_n \in \mathbf{Z}_2$，用$v_1,v_2,\ldots,v_n$分别替换$p(x_1,x_2,\ldots,x_n)$中对应的$x_1,x_2,\ldots,x_n$的全部出现所得结果，记为$p(v_1, v_2,\ldots, v_n)$。

  显然，$p(v_1, v_2,\ldots, v_n) \in \mathbf{Z}_2$.

例 设$p(x_1,x_2)=(x_1\to x_2) \to \neg x_2$。 $v_1=1,v_2=0$。则

$$p(v_1, v_2)=(v_1\to v_2) \to \neg v_2 = (1 \to 0) \to \neg 0$$
$$= 0 \to 1$$
$$=1$$

§1.3.2 赋值与语义推论

命题2 设m≥n, v是$L(X_m)$ 或 L(X)的赋值。若v满足$v(x_i)=v_i$，$1\le i\le n$；则$L(X_n)$的任一公式$p(x_1,x_2,\ldots,x_n)$的真值是

$$v(p(x_1, x_2,\ldots, x_n))=p(v_1, v_2,\ldots, v_n)$$

其中$p(v_1, v_2,\ldots, v_n)$是用$v_1,v_2,\ldots,v_n$分别替换$p(x_1,x_2,\ldots,x_n)$中对应的$x_1,x_2,\ldots,x_n$的全部出现所得的结果。

证 对$p(x_1, x_2,\ldots, x_n)$在$L(X_n)$中的层次进行归纳，

(i) $p(x_1, x_2,\ldots, x_n) = x_i$， 则$p(v_1, v_2,\ldots, v_n) = v_i$, 此时有

$$v(p(x_1, x_2,\ldots, x_n)) = v(x_i) = v_i =p(v_1, v_2,\ldots, v_n)$$

(ii) $p(x_1, x_2,\ldots, x_n) = \neg q(x_1, x_2,\ldots, x_n)$， 此时$p(v_1, v_2,\ldots, v_n) = \neg q(v_1, v_2,\ldots, v_n)$， 于是

$$v(p(x_1, x_2,\ldots, x_n)) = v(\neg q(x_1, x_2,\ldots, x_n)) = \neg v(q(x_1, x_2,\ldots, x_n))$$
$$= \neg q(v_1, v_2,\ldots, v_n) = p(v_1, v_2,\ldots, v_n)$$

§1.3.2 赋值与语义推论

(iii) $p(x_1, x_2,\ldots, x_n) = q(x_1, x_2,\ldots, x_n) \rightarrow r(x_1, x_2,\ldots, x_n)$，类似可证. □

- 命题2说明，$L(X_n)$中的公式$p(x_1, x_2,\ldots, x_n)$的真值只与其所含命题变元的真值指派有关，而与其他变元的真值指派无关。(用真值表研究公式真值的基础)
- 命题变元表示简单命题，其他层次的公式表示复合命题。**(只有)命题变元的真值可随意指定**，且在命题变元真值指定之后，**涉及这些命题变元的所有公式**的真值也随之唯一确定。

§1.3.2 赋值与语义推论

- 设$p \in L(X_n)$。任取 $v_1,v_2,\ldots,v_n \in \mathbf{Z}_2$，将 $v_1,v_2,\ldots,v_n$分别指派给$x_1,x_2,\ldots,x_n$，然后将此指派扩张成赋值$v: L(X_n) \to \mathbf{Z}_2$，这时p就有了唯一确定的真值

$$v(p(x_1, x_2,\ldots, x_n))=p(v_1, v_2,\ldots, v_n) \in \mathbf{Z}_2$$

将此值对应于$v_1,v_2,\ldots,v_n$的函数值，就得到一个由公式p所确定的**真值函数**(简称**p的真值函数**)。

- 公式的真值表就是该公式的真值函数的函数值表。

一些例子

§1.3.2 赋值与语义推论

定义3(永真式) 若公式p的真值函数取常值1，则p叫做命题演算L的永真式或重言式(tautology)，记作⊨p.

⊨p ⇔ L(X)的任意赋值v都使v(p)=1
(p只有成真指派)

定理2 (代换定理)

$$\vDash p(x_1, x_2, \ldots, x_n) \Rightarrow \vDash p(p_1, p_2, \ldots, p_n),$$

其中 $p(x_1, x_2, \ldots, x_n) \in L(X_n)$，而$p_1, p_2, \ldots, p_n \in L(X)$; $p(p_1, p_2, \ldots, p_n)$是分别用$p_1, p_2, \ldots, p_n$替换$x_1, x_2, \ldots, x_n$的全部出现所得的结果。

§1.3.2 赋值与语义推论

定理2 (代换定理)

$$\vDash p(x_1, x_2,\ldots, x_n) \Rightarrow \vDash p(p_1, p_2,\ldots, p_n),$$

证 设v是L(X)的任一赋值，记

$$u_1=v(p_1),\ldots, u_n=v(p_n).$$

将$u_1,u_2,\ldots, u_n$分别指派给$x_1, x_2,\ldots, x_n$且将此真值指派扩张成$L(X_n)$的赋值u. 于是u满足：

(1) $u(x_i)= u_i = v(p_i)$, $1\le i\le n$.

下证

(2) $v(p(p_1, p_2,\ldots, p_n)) = u(p(x_1, x_2,\ldots, x_n))$

§1.3.2 赋值与语义推论

用层次归纳法。

(i) $p(x_1, x_2,\ldots, x_n) = x_i$时， $p(p_1, p_2,\ldots, p_n) = p_i$, 此时由(1)知(2)成立。

(ii) $p(x_1, x_2,\ldots, x_n) = \neg q(x_1, x_2,\ldots, x_n)$时，有

$$
\begin{aligned}
v(p(p_1, p_2,\ldots, p_n)) &= v(\neg q(p_1, p_2,\ldots, p_n)) \\
&= \neg v(q(p_1, p_2,\ldots, p_n)) && \text{(赋值条件(1))} \\
&= \neg u(q(x_1, x_2,\ldots, x_n)) && \text{(归纳假设)} \\
&= u(\neg q(x_1, x_2,\ldots, x_n)) && \text{(u的保运算性)} \\
&= u(p(x_1, x_2,\ldots, x_n))
\end{aligned}
$$

(iii) $p(x_1, x_2,\ldots, x_n) = q(x_1, x_2,\ldots, x_n) \rightarrow r(x_1, x_2,\ldots, x_n)$时类似可证.

§1.3.2 赋值与语义推论

于是

$$\vDash p(x_1, x_2, \ldots, x_n) \Rightarrow u(p(x_1, x_2, \ldots, x_n))=1$$
$$\Rightarrow v(p(p_1, p_2, \ldots, p_n))=1$$
$$\Rightarrow \vDash p(p_1, p_2, \ldots, p_n).$$ □

- 定理2的逆不成立。

命题3 L的所有公理都是永真式，即对任意$p, q, r \in L(X)$

1) $\vDash p \to (q \to p)$
2) $\vDash (p \to (q \to r)) \to ((p \to q) \to (p \to r))$
3) $\vDash (\neg p \to \neg q) \to (q \to p)$

证 ……

§1.3.2 赋值与语义推论

- 一些常见的永真式见书P41。

定义4(永假式与可满足式) 若¬p是永真式，则p叫做永假式(矛盾式)。非永假式叫做可满足公式。

定义5(语义推论) 设$\Gamma \subseteq L(X)$，$p \in L(X)$。如果Γ中所有公式的任何公共成真指派都一定是公式p的成真指派，则说p是公式集Γ的**语义推论**，记作 $\Gamma \models p$ 。

简单性质

1) $\varnothing \models p \Leftrightarrow$ L(X)的任意赋值v都使v(p)=1 $\Leftrightarrow \models p$

2) $p \in \Gamma \Rightarrow \Gamma \models p$

3) $\models p \Rightarrow \Gamma \models p$, Γ是任意公式集。

§1.3.2 赋值与语义推论

命题4 $\{\neg p\} \vDash p \to q$; $\{q\} \vDash p \to q$.

证 对L(X)的任意赋值v，

$$v(\neg p)=1 \Rightarrow v(p)=0 \Rightarrow v(p \to q)=1$$

$$v(q)=1 \Rightarrow v(p \to q)=1$$

□

命题5 $\Gamma \vDash p$且$\Gamma \vDash p \to q \Rightarrow \Gamma \vDash q$.

证 每当$v(p)=1$且$v(p \to q)=1$时，就有

$$v(q) = 1 \to v(q)$$

$$= v(p) \to v(q)$$

$$= v(p \to q) = 1$$

□

- 命题5是MP规则的语义形式。

§1.3.2 赋值与语义推论

命题6 (语义演绎定理)

$$\Gamma \cup \{p\} \vDash q \quad \Leftrightarrow \quad \Gamma \vDash p \to q.$$

证 ($\Rightarrow$) 设$\Gamma \cup \{p\} \vDash q$，且设v是使$\Gamma$中公式的真值都为1的赋值。若$v(p) = 1$，则由语义推论定义得 $v(q) = 1$，此时$v(p \to q) = 1 \to 1 = 1$；若$v(p) = 0$，则$v(p \to q) = 0 \to v(q) = 1$。这就证明了 $\Gamma \vDash p \to q$。

($\Leftarrow$) 设$\Gamma \vDash p \to q$。因为当$v(p) = 1$且$v(p \to q) = 1$ 时，必有 $v(q) = 1 \Rightarrow v(p) = 1$且v是$\Gamma$中公式的公共成真指派时$v(q) = 1 \Rightarrow \Gamma \cup \{p\} \vDash q$ □

- 命题6推广到一般形式：

$$\{p_1, p_2, \ldots, p_n\} \vDash q \quad \Leftrightarrow \quad \vDash (p_1 \wedge p_2 \wedge \ldots \wedge p_n) \to q$$

第一章 命题演算

刘贵全

gqliu@ustc.edu.cn

§1 命题逻辑

内容提要

1.1 命题联结词与真值表
1.2 命题演算(L)的建立
1.3 命题演算的语义
1.4 命题演算L的可靠性与完全性
1.5 命题演算的其他课题

§1.4 命题演算L的可靠性与完全性

$$\Gamma \vdash p \Leftrightarrow \Gamma \models p \quad (\vdash p \Leftrightarrow \models p)$$

定理1 (L的可靠性) $\Gamma \vdash p \Rightarrow \Gamma \models p$

证 设$\Gamma \vdash p$，则存在p从Γ的证明: $p_1,\ldots, p_n(=p)$. 现对n用归纳法证明$\Gamma \models p$ 。

n=1时，$p_1=p$；此时p或者是L的公理(永真式)、或者$p\in\Gamma$，两种情形都有$\Gamma \models p$。

n>1时，如果p是L的公理或$p\in\Gamma$，显然一样有$\Gamma \models p$。若p是由MP而得，即存在i,j<n使$p_j=p_i\rightarrow p_n$；此时有$\Gamma \vdash p_i$和 $\Gamma \vdash p_j$，根据归纳假设得$\Gamma\models p_i$和 $\Gamma\models p_j$ $(=p_i\rightarrow p_n)$，再由1.3.2命题5便得$\Gamma \models p$。 □

§1.4 命题演算L的可靠性与完全性

推论1 (L的无矛盾性) 命题演算L是无矛盾的，即不存在公式p使 $\vdash p$ 和 $\vdash \neg p$ 同时成立。

证 反设存在公式p使 $\vdash p$ 和 $\vdash \neg p$ 同时成立。由定理1，$\vDash p$ 和 $\vDash \neg p$ 同时成立，于是对L(X)的任一赋值v，$v(p)=v(\neg p)=1$. 但这是不可能的。

定义1(公式集的完备性) 设 $\Gamma \subseteq L(X)$，Γ是完备的，是指对任一公式p，$\Gamma \vdash p$ 和 $\Gamma \vdash \neg p$ 必有一个成立。

- 完备公式集是下面完全性定理证明的一个基础：证明过程中需要对无矛盾公式集进行完备扩张。

§1.4 命题演算L的可靠性与完全性

定理2 (L的完全性) $\Gamma \vDash p \Rightarrow \Gamma \vdash p$

证 反设$\Gamma \vdash p$不成立，接下来设法构造L(X)的一个赋值v，它使Γ中公式的真值为1，但使v(p)=0，从而与$\Gamma \vDash p$矛盾。

L(X)是可数集，故可以把L(X)中公式排成一列，设为

$$p_0, p_1, p_2, \cdots\cdots$$

令$\Gamma_0 = \Gamma \cup \{\neg p\}$。

n>0时，令

$$\Gamma_n = \begin{cases} \Gamma_{n-1}, & \text{若} \Gamma_{n-1} \vdash p_{n-1} \\ \Gamma_{n-1} \cup \{\neg p_{n-1}\}, & \text{若} \Gamma_{n-1} \nvdash p_{n-1} \end{cases}$$

这样就定义出一系列公式集Γ_n：$\Gamma_0 \subseteq \Gamma_1 \subseteq \Gamma_2 \subseteq \ldots$。

§1.4 命题演算L的可靠性与完全性

下面对n归纳证明每个Γ_n都是无矛盾的。

首先，Γ_0是无矛盾的，否则由$\Gamma \cup \{\neg p\} \vdash q, \neg q \Rightarrow \Gamma \vdash p$，与假设矛盾。

现设Γ_{n-1}无矛盾，进而证Γ_n无矛盾。若Γ_n有矛盾，则存在公式q使

(1) $\Gamma_n \vdash q, \neg q$

这时有$\Gamma_n \neq \Gamma_{n-1}$(因为$\Gamma_{n-1}$无矛盾)。于是由$\Gamma_n$的定义知

(2) $\Gamma_{n-1} \nvdash p_{n-1}$

(3) $\Gamma_n = \Gamma_{n-1} \cup \{\neg p_{n-1}\}$

结合(1)(3)用反证律即得$\Gamma_{n-1} \vdash p_{n-1}$，这与(2)矛盾。以上说明每个$\Gamma_n$都是无矛盾的。

作

§1.4 命题演算L的可靠性与完全性

$$\Gamma^*=\bigcup_{n=0}^{\infty}\Gamma_n$$

Γ*也是无矛盾的。这是因为若Γ* ⊢ q, ¬q. 则必然存在某个充分大的n使$\Gamma_n \vdash q, \neg q$。

Γ*还具有完备性：对于L(X)的任一公式p_n， Γ* ⊢ p_n 与Γ* ⊢ $\neg p_n$ 二者必居其一。实际上，若Γ* ⊬ p_n ，则有：

$\Gamma_n \nvdash p_n$ $(\Gamma_n \subseteq \Gamma^*)$

$\Gamma_{n+1} = \Gamma_n \cup \{\neg p_n\}$ (由Γ_n的定义式)

$\Gamma^* \vdash \neg p_n$ $(\Gamma_{n+1} \subseteq \Gamma^*)$

- Γ*叫做Γ的**无矛盾完备扩张**。

利用Γ*的无矛盾性和完备性可定义一个映射v: L(X)→$\mathbf{Z}_2$:

§1.4 命题演算L的可靠性与完全性

$$v(q)=\begin{cases}1, & \text{若}\Gamma^* \vdash q;\\ 0, & \text{若}\Gamma^* \vdash \neg q.\end{cases}$$

v是良定义的，因为对L(X)的任一公式q，$\Gamma^*\vdash q$ 与$\Gamma^*\vdash\neg q$ 这二者必居其一(因Γ^*完备)，且只居其一(因Γ^*无矛盾)。

下证以上定义的v具有保运算性，从而是L(X)的一个赋值。

对任一公式q，由v的定义可得

$$v(\neg q)=\begin{cases}1, & \text{若}\Gamma^* \vdash \neg q;\\ 0, & \text{若}\Gamma^* \vdash \neg\neg q.\end{cases}$$

与v(q)的定义式相对比即知：

§1.4 命题演算L的可靠性与完全性

(4) $v(\neg q)= \neg v(q)$

另外还需要证明$v(q\to r) = v(q)\to v(r)$，分两种情形：

情形1 $v(q)\to v(r)=1$，此时又有两种情况： $v(q)=0$或$v(r)=1$ 。

$v(q)=0 \Rightarrow \Gamma* \vdash \neg q$ (由v的定义)

$\Rightarrow \Gamma* \vdash q\to r$ (否定前件律)

$\Rightarrow v(q\to r) = 1$ (由v的定义)

$v(r)=1 \Rightarrow \Gamma* \vdash r$ (由v的定义)

$\Rightarrow \Gamma* \vdash q\to r$ (肯定后件律)

$\Rightarrow v(q\to r) = 1$ (由v的定义)

情形2 $v(q)\to v(r)=0$，此时有： $v(q)=1$且 $v(r)=0$ 。

□

§1.4 命题演算L的可靠性与完全性

情形2 $v(q)\to v(r)=0$，此时有： $v(q)=1$且 $v(r)=0$ 。

$$\Gamma^* \vdash q \text{且} \Gamma^* \vdash \neg r \qquad \text{(由v的定义)}$$

$$\Rightarrow \Gamma^* \vdash \neg(q\to r) \qquad \text{(由1.2.4例子)}$$

$$\Rightarrow v(q\to r) = 0 \qquad \text{(由v的定义)}$$

总之都有

(5) $v(q\to r) = v(q)\to v(r)$.

(4)与(5)说明v具有保运算性，因而是L(X)的赋值。

最后，可以看出，对赋值v来说Γ 中公式的真值都为1：

$$q\in\Gamma \Rightarrow q\in\Gamma^* \Rightarrow \Gamma^* \vdash q \Rightarrow v(q) = 1$$

但是$\neg p \in \Gamma_0 \subseteq \Gamma^*$，故$\Gamma^* \vdash \neg p \Rightarrow v(p) = 0 \Rightarrow \Gamma \vDash p$ 不成立。

□

§1.5 命题演算的其他课题

1.5.1 等值公式与对偶律

定义1(等值公式) 若 $\vDash p \leftrightarrow q$, 则称p与q等值($p \leftrightarrow q$为永真式)。

设$p,q \in L(X_n)$.

p与q等值$\Leftrightarrow$ $L(X_n)$的任一赋值v都使$v(p)=v(q)$

$\Leftrightarrow$ $L(X)$的任一赋值v都使$v(p)=v(q)$

$\Leftrightarrow$ p与q有相同的成真指派与成假指派

$\Leftrightarrow$ p与q有相同的真值函数

$\Leftrightarrow$ 对$x_1,x_2,\ldots,x_n$的任何指派$v_1, v_2,\ldots, v_n$都有

$p(v_1, v_2,\ldots, v_n) = q(v_1, v_2,\ldots, v_n)$

§1.5.1 等值公式与对偶律

命题1 1) $\vDash p \leftrightarrow p$

2) $\vDash p \leftrightarrow q \Rightarrow \vDash q \leftrightarrow p$

3) $\vDash p \leftrightarrow q$ 且 $\vDash q \leftrightarrow r \Rightarrow \vDash p \leftrightarrow r$

- 命题1说明等值是$L(X)(L(X_n))$上的等价关系. 同一等价类的公式有相同的真值函数。
- 不同的n元真值函数有2^{2^n} 种，于是$L(X_n)$有2^{2^n} 种不同的等价类，即$L(X_n)$中语义不同的公式只有2^{2^n} 种。

命题2 1) $\vDash p \leftrightarrow q \Rightarrow \vDash \neg p \leftrightarrow \neg q$

2) $\vDash p \leftrightarrow p'$ 且 $\vDash q \leftrightarrow q' \Rightarrow \vDash (p \rightarrow q) \leftrightarrow (p' \rightarrow q')$

§1.5.1 等值公式与对偶律

命题2 1) $\vDash p\leftrightarrow q \Rightarrow \vDash \neg p\leftrightarrow\neg q$

2) $\vDash p\leftrightarrow p'$ 且 $\vDash q\leftrightarrow q' \Rightarrow \vDash (p\rightarrow q)\leftrightarrow(p'\rightarrow q')$

证 设v是L(X)的任一赋值。

1) $v(p)=v(q) \Rightarrow v(\neg p)=v(\neg q)$

2) $v(p)=v(p')$ 且 $v(q)=v(q') \Rightarrow$

$v(p\rightarrow q) = v(p)\rightarrow v(q) = v(p')\rightarrow v(q') = v(p'\rightarrow q')$ □

- 用p=…q…表示q是p的子公式： q是p的组成部分，并且q本身是公式。
- 若q是p的子公式且q≠p，则在L(X)中q比p的层次低。

§1.5.1 等值公式与对偶律

定理1 (子公式等值可替换)

设p=…q…，用公式q′替换p的子公式q(一处替换)所得结果记为p′=…q′…，那么

$$\vDash q \leftrightarrow q' \Rightarrow \vDash p \leftrightarrow p'$$

证 对p在L(X)的层次归纳。

p为命题变元时，只能是p=q，因而p′=q′，显然 $\vDash p \leftrightarrow p'$。

若p所在层次大于0，则有两种情形：

(1) $p = \neg r$

最后运算是¬，可设q是r的子公式，这时$p' = \neg r'$ (r′是用q′替换r中的子公式q而得，下同)，于是有

$\vDash r \leftrightarrow r'$ (归纳假设)

$\Rightarrow \vDash \neg r \leftrightarrow \neg r'$ (命题2-1)

§1.5.1 等值公式与对偶律

(2) $p = r \rightarrow s$

形成p的最后运算是$\rightarrow$，可设q是r或s的子公式。于是$p' = r' \rightarrow s$ 或$p' = r \rightarrow s'$。由归纳假设，$\vDash r \leftrightarrow r'$或$\vDash s \leftrightarrow s'$；由命题2-2知$\vDash (r \rightarrow s) \leftrightarrow (r' \rightarrow s)$ 或 $\vDash (r \rightarrow s) \leftrightarrow (r \rightarrow s')$，都有

$$\vDash p \leftrightarrow p'$$

□

- 可用定理1若干次进行多处替换。

定义2(公式的对偶) 设公式p已被写成只含命题变元和运算$\neg, \vee, \wedge$ 的形式。把p中命题变元全部改为各自的否定、把$\vee$全改为$\wedge$、把$\wedge$全改为$\vee$，这样得到的公式p*叫做p的**对偶**。

§1.5.1 等值公式与对偶律

定理2(对偶律) $\vDash p^* \leftrightarrow \neg p$， p^*为公式p的对偶。

证 对p中$\neg,\vee,\wedge$ 出现的总次数n进行归纳。

n=0时， 设$p = x_i$， 则$p^* = \neg x_i$， 故$\vDash p^* \leftrightarrow \neg p$。

n>0时，有三种情形：

Case 1: $p = \neg q$. 此时$p^* = \neg q^*$， q中$\neg,\vee,\wedge$ 出现的次数为n-1，由归纳假设有$\vDash q^* \leftrightarrow \neg q$；再由命题2-1得$\vDash \neg q^* \leftrightarrow \neg\neg q$，即$\vDash p^* \leftrightarrow \neg p$。

Case 2: $p = q \vee r$. 此时$p^* = q^* \wedge r^*$，q、r中$\neg,\vee,\wedge$ 出现的次数均小于n，由归纳假设有 $\vDash q^* \leftrightarrow \neg q$ 及 $\vDash r^* \leftrightarrow \neg r$；两次用子公式等值可替换性定理得

$$\vDash (q^* \wedge r^*) \leftrightarrow (\neg q \wedge r^*)$$

$$\vDash (\neg q \wedge r^*) \leftrightarrow (\neg q \wedge \neg r)$$

§1.5.1 等值公式与对偶律

证 (续)　再由De. Morgan律得

$$\vDash (\neg q \wedge \neg r) \leftrightarrow \neg(q \vee r)$$

由上及等值传递性得$\vDash (q^* \wedge r^*) \leftrightarrow \neg(q \vee r)$，即$\vDash p^* \leftrightarrow \neg p$

Case 3: $p = q \wedge r$. 此时$p^* = q^* \vee r^*$，证明与情形2类似。

□

推论 (推广的De. Morgan律)

1) $\vDash (\neg p_1 \vee \ldots \vee \neg p_n) \leftrightarrow \neg(p_1 \wedge \ldots \wedge p_n)$

2) $\vDash (\neg p_1 \wedge \ldots \wedge \neg p_n) \leftrightarrow \neg(p_1 \vee \ldots \vee p_n)$

由代换定理，1)和2)分别是$p= x_1 \wedge \ldots \wedge x_n$与$p= x_1 \vee \ldots \vee x_n$时的特例。

- 记号$\bigwedge_{i=1}^{n} y_i = y_1 \wedge \ldots \wedge y_n$，　$\bigvee_{i=1}^{n} y_i = y_1 \vee \ldots \vee y_n$

§1.5.2 析取范式与合取范式

定义1 (基本析取式与基本合取式) 形为 $y_1 \vee \ldots \vee y_n$ 和形为 $y_1 \wedge \ldots \wedge y_n$ 的公式分别叫做基本析取式和基本合取式，其中每个 y_i 是命题变元或命题变元的否定。

- 基本析取式可判断是否为永真式 (若不是，则有唯一的成假指派)。
- 基本合取式可判断是否为永假式 (若不是，则有唯一的成真指派)。

定义2 (析取范式与合取范式) 形为 $\bigvee_{i=1}^{m}(\bigwedge_{j=1}^{n} y_{ij})$ 和形为 $\bigwedge_{i=1}^{m}(\bigvee_{j=1}^{n} y_{ij})$ 的公式分别叫做**析取范式**和**合取范式**，其中每个 y_{ij} 是命题变元或命题变元的否定。

- **析取支与合取支**

§1.5.2 析取范式与合取范式

- $(x_1 \wedge \neg x_2) \vee (x_1 \wedge x_2 \wedge x_3)$，$(\neg x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee x_2 \vee \neg x_3)$
- $x_1 \wedge \neg x_2 \wedge x_3$既是析取范式，也是合取范式。
- 析取范式为永假式、合取范式为永真式的快速判定。
- 找出与某给定公式等值的析取(合取)范式的步骤：
  1) 消去→与↔。先用(p→q) ∧ (q→p) 等值替换 p↔q，再用¬p ∨ q 等值替换 p → q。
  2) 把否定号¬等值变换到命题变元之前：运用De. Morgan律和双重否定律。
  3) 用交换律、结合律及分配律作等值变换，直到得出所需形式。

例1 求与$(x_1 \wedge (\neg x_2 \rightarrow x_1)) \rightarrow x_2$等值的析取范式与合取范式。

§1.5.2 析取范式与合取范式

定义3 (主析取范式与主合取范式) L(X)(L(X_n))中的主析取范式是满足以下条件的析取范式：其每个析取支中，每个命题变元$x_1, \ldots, x_n$(带否定号或不带否定号)按下标由小到大的次序都出现且只出现一次。主合取范式同样定义，只要把“析取支”改为“合取支”即可。

定理1 每个非永假式必有与之等值的主析取范式。

证 设p=p($x_1, \ldots, x_n$)不是永假式，那么它有成真指派。令所有成真指派(最多2^{2^n}个)为

$$(v_1, \ldots, v_n),\ldots$$

分别作出与这些成真指派对应的基本合取式

$$(y_1 \wedge \ldots \wedge y_n),\ldots$$

§1.5.2 析取范式与合取范式

方法是，令

$$y_i=\begin{cases} x_i, & 若v_i=1 \\ \neg x_i, & 若v_i=0 \end{cases}$$

如此$(v_1, \ldots, v_n)$是 $y_1\wedge\ldots\wedge y_n$ 的(唯一)成真指派。最后以每个这样的基本合取式为析取支，全部拿来作析取式

$$q = (y_1\wedge\ldots\wedge y_n)\vee(\ldots)\vee\ldots$$

则q为所求的主析取范式。理由是：(1) q的每个析取支中，每个命题变元按下标从小到大的次序都唯一的出现了一次；(2) q与p有相同的真值函数，因而等值，实际上，任给真值指派$(v_1, \ldots, v_n)$：

i) 若$p(v_1, \ldots, v_n)=1$, 即$(v_1, \ldots, v_n)$是p的成真指派，按q的作法，q有一析取支 $y_1\wedge\ldots\wedge y_n$ 与$(v_1, \ldots, v_n)$ 对应，$(v_1, \ldots, v_n)$

§1.5.2 析取范式与合取范式

也是q的成真指派，故 $q(v_1, \ldots, v_n)=1$。

ii) 若$p(v_1, \ldots, v_n)=0$, $(v_1, \ldots, v_n)$不是p的成真指派，q没有析取支与之对应，故 $q(v_1, \ldots, v_n)=0$。 □

例 求$\neg x_2 \rightarrow x_1$的主析取范式

定理2 每个非永真式必有与之等值的主合取范式。

证 设p为非永真式，则¬p为非永假式；由定理1，¬p有等值的主析取范式，设为$\bigvee_{i=1}^{m}(\bigwedge_{j=1}^{n} y_{ij})$。

于是p等值于$\neg \bigvee_{i=1}^{m}(\bigwedge_{j=1}^{n} y_{ij})$和$\bigwedge_{i=1}^{m}(\bigvee_{j=1}^{n} \neg y_{ij})$，把最后一个公式中的$\neg\neg x_k$ 换成 x_k 即得所求的主合取范式。 □

例子

§1.5.3 运算的完全组

定义1(运算的完全组) $\mathbf{Z}_2$上的一些运算构成完全组，是指任一真值函数都可用该运算组中的运算表示出来。

- $\{\neg,\rightarrow\}$是完全组。

命题1 $\{\neg,\vee\}$和$\{\neg,\wedge\}$都是完全组。

证 对任意的$u, v\in\mathbf{Z}_2$，有恒等式

$$u\rightarrow v=\neg u\vee v,\quad u\rightarrow v=\neg(u\wedge v)\ \ldots$$ □

命题2 $\{\vee,\wedge,\rightarrow,\leftrightarrow\}$不是完全组。

证 先证以下命题*：

任一一元真值函数$f:\mathbf{Z}_2\rightarrow\mathbf{Z}_2$若能用$\vee,\wedge,\rightarrow,\leftrightarrow$这四种运算表示出来，则恒有$f(1)=1$。

§1.5.3 运算的完全组

对表示 f 所用$\vee, \wedge, \rightarrow, \leftrightarrow$这四种运算的次数k归纳。

k=0时，$f(v)=v \Rightarrow f(1)=1$。

k>0时，有四种可能情况：

1) $f(v) = g(v) \vee h(v)$

2) $f(v) = g(v) \wedge h(v)$

3) $f(v) = g(v) \rightarrow h(v)$

4) $f(v) = g(v) \leftrightarrow h(v)$

无论哪种情况，由归纳假设都有$g(1)=h(1)=1 \Rightarrow f(1)=1$。

当 f 是恒为0的一元常值函数时，$f(1)=0\neq1$；由命题*，f 不能由$\vee, \wedge, \rightarrow, \leftrightarrow$表示出来。 □

- 命题2说明了否定“¬”的重要特殊地位。

§1.5.3 运算的完全组

命题3 $\{\neg, \leftrightarrow\}$不是完全组。

证 假设二元真值函数f 能用$\neg, \leftrightarrow$这两种运算表示出来。对表示 f 所用运算$\neg, \leftrightarrow$的总次数k归纳证明 f 具有性质：

“$f(1,1), f(1,0), f(0,1), f(0,0)$中1出现偶数次”。

k=0时，$f(v_1, v_2) = v_1$或v_2，这时 $f(1,1)$, $f(1,0)$, $f(0,1)$, $f(0,0)$中有且只有两个1。

k>0时有两种可能：

$f(v_1, v_2) = \neg g(v_1, v_2)$ 或 $f(v_1, v_2) = g(v_1, v_2) \leftrightarrow h(v_1, v_2)$

由归纳假设，$g(1,1), g(1,0), g(0,1), g(0,0)$中，以及

$h(1,1), h(1,0), h(0,1), h(0,0)$中，

1都出现偶数次。分别对不同情况进行计算便知上述结论成立。而二元真值函数$\vee$和 $\wedge$不具有上述性质…

□

§1.5.3 运算的完全组

推论1 {¬}不是完全组。

推论2 {¬,↮}不是完全组。

v_1	v_2	$v_1 \nleftrightarrow v_2$
1	1	0
1	0	1
0	1	1
0	0	0

证 显然 $v_1 \nleftrightarrow v_2 = \neg(v_1 \leftrightarrow v_2)$… □

- “↮”作为L(X)的运算($p \nleftrightarrow q = \neg(p \leftrightarrow q)$)解释为“不可兼或”。

§1.5.3 运算的完全组

定义2(“与非”运算、“或非”运算) 两个运算分别用“|”和“↓”表示。

v_1	v_2	$v_1 \mid v_2$	$v_1 \downarrow v_2$
1	1	0	0
1	0	1	0
0	1	1	0
0	0	1	1

命题4 {|}和{↓}都是完全组。

证 对任意的$v_1, v_2 \in \mathbf{Z}_2$，有等式

§1.5.3 运算的完全组

$$\neg v_1 = v_1 | v_1 = v_1 \downarrow v_1$$

$$v_1 \vee v_2 = (v_1 | v_1) \mid (v_2 | v_2)$$

$$v_1 \wedge v_2 = (v_1 \downarrow v_1) \downarrow (v_2 \downarrow v_2)$$

利用{¬,∨}和{¬, ∧}的完全性，命题得证。 □

命题5 除 |, ↓外，没有其他二元运算单独构成完全组。

§1.5.4 应用举例

例1 前提：1) a_1为奇数或a_2为偶数；

2) a_1若为偶数，则a_3与a_4皆为偶数；

3) a_4若为偶数，则a_2也为偶数。

结论：a_2与a_3至少有一个为偶数。

解 用 x_i 表示“a_i为偶数”，i=1,2,3,4. 则上述推理可形式化为

$$\{\neg x_1 \vee x_2, x_1 \rightarrow (x_3 \wedge x_4), x_4 \rightarrow x_2\} \vdash x_2 \vee x_3$$

方法1：用1.2尝试直接推导，但当推理不成立时无效。

方法2：用语义的方法。

§1.5.4 应用举例

简便方法是：检查是否有前提的公共成真指派为结论的成假指派。如果有，则推理不成立；否则推理成立。

对于本题，即检查下面的真值方程组(1)~(4)是否有解：

(1) $\neg v_1 \vee v_2 = 1$

(2) $v_1 \rightarrow (v_3 \wedge v_4) = 1$

(3) $v_4 \rightarrow v_2 = 1$

(4) $v_2 \vee v_3 = 0$

由(4)得

(5) $v_2 = 0$ 且

(6) $v_3 = 0$

由(3)、(5)得

(7) $v_4 = 0$

§1.5.4 应用举例

由(1)、(5)得

(8) $v_1 = 0$

将(6)、(7)、(8)代入(2)式左边得

$$v_1 \to (v_3 \wedge v_4) = 0 \to (0 \wedge 0) = 1$$

说明(0,0,0,0)是(1)~(4)的解，所以题中的论证(推理)不成立。

例2 检查下面推理的正确性

$\{x_1, x_2, x_3, x_4, (x_1 \wedge x_2) \to (x_5 \wedge x_6), (x_3 \wedge x_4) \to x_7, (x_6 \wedge x_7) \to x_8\} \vdash x_8$

§1.5.4 应用举例

例2 检查下面推理的正确性

$\{x_1, x_2, x_3, x_4, (x_1 \wedge x_2) \rightarrow (x_5 \wedge x_6), (x_3 \wedge x_4) \rightarrow x_7, (x_6 \wedge x_7) \rightarrow x_8\} \vdash x_8$

解 解真值方程组：

(1) $v_1 = v_2 = v_3 = v_4 = 1$

(2) $(v_1 \wedge v_2) \rightarrow (v_5 \wedge v_6) = 1$

(3) $(v_3 \wedge v_4) \rightarrow v_7 = 1$

(4) $(v_6 \wedge v_7) \rightarrow v_8 = 1$

(5) $v_8 = 0$

由(1)、(2)得 $v_5 \wedge v_6 = 1 \Rightarrow v_5 = v_6 = 1$；由(1)、(3)得 $v_7 = 1$；由 $v_6 = v_7 = 1$ 以及(4)得 $v_8 = 1$，这与(5)相矛盾。所以方程组(1)~(5)无解，推理正确。

§1.5.4 应用举例

例3 一案案情涉及a,b,c,d四人，根据已有线索知

(1) 若a,b均未作案，则c,d也均未作案；

(2) 若c,d均未作案，则a,b也均未作案；

(3) 若a与b同时作案，则c与d有且只有一人作案；

(4) 若b与c同时作案，则a与d同时作案或同未作案。

办案人员由此推出： a是作案者。这是否成立？

解 用x_1, x_2, x_3, x_4分别表示a,b,c,d作案。办案人员的推理形式化为

$$\{(\neg x_1 \wedge \neg x_2) \leftrightarrow (\neg x_3 \wedge \neg x_4),\ (x_1 \wedge x_2) \rightarrow ((x_3 \vee x_4) \wedge \neg(x_3 \wedge x_4)),$$
$$(x_2 \wedge x_3) \rightarrow ((x_1 \wedge x_4) \vee (\neg x_1 \wedge \neg x_4))\} \vdash x_1$$

§1.5.4 应用举例

$\{ (\neg x_1 \wedge \neg x_2) \leftrightarrow (\neg x_3 \wedge \neg x_4),\ (x_1 \wedge x_2) \rightarrow ((x_3 \vee x_4) \wedge \neg (x_3 \wedge x_4)),\ (x_2 \wedge x_3) \rightarrow ((x_1 \wedge x_4) \vee (\neg x_1 \wedge \neg x_4)) \} \vdash x_1$

解真值方程组：

(1) $(\neg v_1 \wedge \neg v_2) \leftrightarrow (\neg v_3 \wedge \neg v_4) = 1$

(2) $(v_1 \wedge v_2) \rightarrow ((v_3 \vee v_4) \wedge \neg (v_3 \wedge v_4)) = 1$

(3) $(v_2 \wedge v_3) \rightarrow ((v_1 \wedge v_4) \vee (\neg v_1 \wedge \neg v_4)) = 1$

(4) $v_1 = 0$

$v_1 = 0$时(2)自动成立；若$v_2 = 0$，则(3)也自动成立。此时，为让(1)成立，可取$v_3 = v_4 = 0$。即方程组(1)~(4)有解(0,0,0,0)，说明推论无效。

§1.5.4 应用举例

- 给定两个假设P1、P2和两个可能结论C1、C2如下。判断在命题逻辑中，从P1、P2能否推出C1、C2，并证明你的判断。

  P1：逻辑是很难的或没有很多学生喜欢逻辑；

  P2：如果哲学是容易的，则逻辑不是很难的；

  C1：如果有很多学生喜欢逻辑，则哲学不是容易的；

  C2：如果哲学不是容易的，则没有很多学生喜欢逻辑。

第二章 谓词演算

刘贵全

gqliu@ustc.edu.cn

命题演算的不足

- 命题没有概括能力
  - 1是整数，2是整数，…，100是整数…；用命题可表示为：$x_1, x_2, \ldots, x_{100}, \ldots$
- 只能表达固定的判断，不能表达变化的判断和关系。
  - 例如：北京是城市 (恒真)，乌鸦是白的 (恒假)
  - 例如：图论中节点之间的相邻关系在命题中表达不出来。
- 难以在判断(知识)之间建立联系、不能表达递归等。
  - 如三段论的有效性
  - 其他例子

§2 谓词演算

内容提要

2.1 谓词演算(K)的建立
2.2 谓词演算(K)的语义
2.3 K的可靠性
2.4 K的完全性

§2.1 谓词演算K的建立

2.1.1 项与原子公式

- (可数)**个体变元**集X=$\{x_1,x_2,\ldots,x_n,\ldots\}$. x_i表示**个体对象**，用 x, y, z 表示也行。
- **个体常元**集(可数或有限)C=$\{c_1,c_2,\ldots,c_n,\ldots\}$. c_i表示确定的个体对象。
- **运算**集(可数或有限) F=$\{f_1^1, f_2^1,\ldots, f_1^2, f_2^2,\ldots, f_1^3, f_2^3,\ldots\}$. f_i^n叫做第i个n元运算符或函数词，用来表示(某)个体对象集上的n元运算。
- **谓词**集(可数或有限非空) R=$\{R_1^1, R_2^1,\ldots, R_1^2, R_2^2,\ldots, R_1^3, R_2^3,\ldots\}$. R_i^n叫做第i个n元谓词。

§2.1.1 项与原子公式

- **项的形成规则**(用T表示项集)

  (i) 个体变元与个体常元都是项；

  (ii) 若$t_1,t_2,\ldots,t_n$是项，则$f_i^n(t_1,t_2,\ldots,t_n)$也是项($f_i^n \in F$)；

  (iii) 任何项都是有限次使用(i)、(ii)形成。

  F=∅时，规定T=X∪C.

  F≠∅时，T可如下分层：

  $T=T_0 \cup T_1 \cup T_2 \cup \ldots \cup T_k \cup \ldots$，其中

  $T_0=X \cup C$

  $T_1=\{f_1^1(x_1), f_1^1(x_2),\ldots, f_1^1(c_1), f_1^1(c_2), \ldots,$

  $f_1^2(x_1,x_1), f_1^2(x_1,x_2),\ldots$

  $f_1^3(x_1,x_1,x_1),\ldots\ldots\},\ldots\ldots$

§2.1.1 项与原子公式

T_k 中元素(项) 含有k个运算符。T是由集合X∪C生成的F型代数。

例1 C=$\{c_1\}$， F=$\{f_1^1, f_2^1\}$

定义1(闭项) 只含个体常元的项叫闭项。

- 所有闭项的集是由C生成的F型代数。

定义2(原子公式集) 原子公式集定义为

$$Y=\{(R_i^n, t_1,t_2,\ldots,t_n)\mid R_i^n\in R, t_1,t_2,\ldots,t_n\in T\}.$$

- 原子公式$(R_i^n, t_1,t_2,\ldots,t_n)$以后写成$R_i^n(t_1,t_2,\ldots,t_n)$。

§2.1.2 谓词演算公式集

- 谓词演算公式(以下简称公式)形成规则

  (i) 每个原子公式是公式;

  (ii) 若p,q是公式，则$\neg p$、$p\rightarrow q$、$\forall x_i p(i=1,2,\ldots)$都是公式;

  (iii) 任一公式都是有限次使用(i)、(ii)所形成。

- **“唯一读法”**
- 用K(Y)表示谓词演算全体公式的集合。 K(Y)可数、分层。
- 在K(Y)上定义逻辑运算$\vee$、$\wedge$、$\leftrightarrow$及$\exists x_i$:

$$p\vee q=_{df} \neg p\rightarrow q$$

$$p\wedge q=_{df} \neg(p\rightarrow\neg q)$$

$$p\leftrightarrow q=_{df} (p\rightarrow q)\wedge(q\rightarrow p)$$

$$\exists x_i p =_{df} \neg\forall x_i\neg p$$

§2.1.2 谓词演算公式集

定义1(变元的自由出现与约束出现) 在一个公式里, 个体变元x的出现如果不是在$\forall x$中或在$\forall x$的范围中，则叫做**自由出现**；否则叫做**约束出现**。

举例

定义2(闭式) 不含自由变元的公式叫做**闭式**。

定义3 用项t去代换公式p中的自由变元x时，若在代换后的新公式里，t的变元**都是**自由的，则说t对p中x是**可自由代换**的；简称t对p中x是可代换的，或t对p中x是自由的。

- 若用t代换公式p中的自由变元x后，t中有变元受到约束，则说t对p中x是“不自由的”。

§2.1.2 谓词演算公式集

- 下列情形，t对p中x自由：

  1) t是闭项；

  2) x在p中不自由出现。

- x_i(作为项)对x_i自己总是自由的。

- 谓词演算中，p(x)中的x指的是自由出现的x，而不是约束出现的x。其中x可以不自由出现或根本不出现，且不排除其他变元在p(x)中出现。

§2.1.3 谓词演算K

定义1(谓词演算K) 是指带有如下规定的“公理”和证明的公式集K(Y):

1) “公理”

(K1) $p\rightarrow(q\rightarrow p)$

(K2) $(p\rightarrow(q\rightarrow r))\rightarrow((p\rightarrow q)\rightarrow(p\rightarrow r))$

(K3) $(\neg p\rightarrow\neg q)\rightarrow(q\rightarrow p)$

(K4) $\forall x p(x)\rightarrow p(t)$, 其中项$t$对$p(x)$中$x$自由

(K5) $\forall x(p\rightarrow q)\rightarrow(p\rightarrow\forall x q)$, 其中$x$不在p中自由出现。

$p,q,r,p(x)\in K(Y)$是任意公式。

§2.1.3 谓词演算K

2) “证明”

设$\Gamma \subseteq K(Y)$， $p \in K(Y)$。**p从Γ可证**，记作$\Gamma \vdash p$，是指存在公式的**有限序列**$p_1,\ldots,p_n(=p)$，且$p_k(k=1,\ldots,n)$满足：

(i) $p_k \in \Gamma$，或

(ii) p_k是“公理”，或

(iii) 存在$i,j<k$使$p_j=p_i \rightarrow p_k$，或

(iv)存在$j<k$使$p_k = \forall x p_j$. 此时说p_k由p_j使用“Gen(推广)”规则得到，x叫做Gen变元。

符合上述条件的有限序列$p_1,\ldots,p_n(=p)$叫做p从Γ的证明。p叫做假定集Γ的语法推论。

- 若$\varnothing \vdash p$ ($\vdash p$)，则p叫做K的定理。

§2.1.3 谓词演算K

定理1 设$x_1,x_2,\ldots,x_n$是命题演算L的命题变元，$p(x_1,x_2,\ldots,x_n)$是$L(X_n)$中公式，则

$$\vdash_L p(x_1,x_2,\ldots,x_n) \Rightarrow \vdash_K p(p_1,p_2,\ldots,p_n)$$

其中$p_1,p_2,\ldots,p_n \in K(Y)$，$p(p_1,p_2,\ldots,p_n)$是用$p_1,p_2,\ldots,p_n$分别代换$p(x_1,x_2,\ldots,x_n)$中的$x_1,x_2,\ldots,x_n$所得结果。

证 因为L的公理模式(L1), (L2), (L3)与K的公理模式(K1), (K2), (K3)形式上完全相同；L的推理规则MP也在K中保留，所以$p(x_1,x_2,\ldots,x_n)$在L中的证明可直接转换成$p(p_1,p_2,\ldots,p_n)$在K中的证明，只要把所有命题变元x_i换成对应p_i的即可。

§2.1.3 谓词演算K

定义2 若$p(x_1,x_2,\ldots,x_n)\in L(X_n)$是命题演算L的永真式，则对任意$p_1,p_2,\ldots,p_n\in K(Y)$，$p(p_1,p_2,\ldots,p_n)$叫做K的命题演算型永真式，简称**永真式**。

- 由定理1，K的永真式一定是K的定理；但反过来不成立(K的定理不一定是永真式)。
- K是在L的基础上进行了改进，L的结论、方法等在K中都得到了保留。

命题1 $\Gamma\subseteq K(Y)$，Γ有矛盾 $\Rightarrow$ K的所有公式从Γ可证。

§2.1.3 谓词演算K

例1 $\{\neg\exists x\neg p\} \vdash \forall x\, p$.

命题2 ($\exists_1$规则) 设项t对$p(x)$中的x自由，则有

$$\vdash p(t)\to \exists x\, p(x).$$

证 已知t对$p(x)$中的x自由，故

$$\forall x\, \neg p(x)\to \neg p(t)$$

是(K4)型公理。由此式及永真式

$$(q \to \neg p) \to (p \to \neg q)$$

可得

$$\vdash p(t)\to \neg\forall x\, \neg p(x)$$

即

$$\vdash p(t)\to \exists x\, p(x).$$

§2.1.3 谓词演算K

例2 $\{\forall x\,(p\to q), \forall x\neg q\}\vdash \forall x\,\neg p$，其证明中除变元$x$外不使用其他Gen变元。

定理2 (演绎定理)

1) 若$\Gamma\vdash p\to q$，则$\Gamma\cup\{p\}\vdash q$;

2) 若$\Gamma\cup\{p\}\vdash q$，且证明中所用Gen变元不在p中自由出现，则不增加新的Gen变元即可得$\Gamma\vdash p\to q$。

证 1) 由MP立即可得。

2) 设$q_1,\ldots,q_n(=q)$是q在K中从$\Gamma\cup\{p\}$的一个证明。由已知，证明中所用Gen变元不在p中自由出现，下面对n归纳地证明$\Gamma\vdash p\to q$。

§2.1.3 谓词演算K

n=1时， q_1=q。此时有三种可能：q=p, q∈Γ或q是公理。这时都有Γ⊢p→q，且不用Gen规则。

n>1时，只用考虑q是使用Gen规则而得的情形 (其他情形与命题演算时的证明相同，且不涉及Gen)。设q= $\forall x\, q_i$，i<n，且Gen变元x不在p中自由出现。这时因Γ∪{p} ⊢ q_i，由归纳假设，有Γ⊢ p→ q_i，且不增加新的Gen变元。于是有

(1) ……
……
(k) $p \to q_i$

} p→q_i从Γ的一个证明

(k+1) $\forall x(p \to q_i)$ (k), Gen

(k+2) $\forall x(p \to q_i) \to (p \to \forall x q_i)$ (K5)

(k+3) p→ $\forall x q_i$ 即p→q (k+1),(k+2),MP

§2.1.3 谓词演算K

推论1 当p为闭式时，有

$$\Gamma \cup \{p\} \vdash q \Leftrightarrow \Gamma \vdash p \rightarrow q$$

命题3 $\vdash \forall x(p \rightarrow q) \rightarrow (\exists x p \rightarrow \exists x q)$，除$x$外不用其他Gen变元。

证 用演绎定理进行证明…

定理3(反证律) 若$\Gamma \cup \{\neg p\} \vdash q$及$\neg q$，且所用Gen变元不在p中自由出现，则不增加新的Gen变元便可得$\Gamma \vdash p$。

定理4(归谬律) 若$\Gamma \cup \{p\} \vdash q$及$\neg q$，且所用Gen变元不在p中自由出现，则不增加新的Gen变元便可得$\Gamma \vdash \neg p$。

§2.1.3 谓词演算K

例3 $\{\forall x p\} \vdash \exists x p$

证 用归谬律。$\exists x p$即$\neg\forall x\neg p$，以下公式从$\{\forall x p, \forall x\neg p\}$可证

……

命题4 ($\exists_2$规则) 设$\Gamma\cup\{p\} \vdash q$，其证明中所用Gen变元不在p中自由出现，且x不在q中自由出现；那么有$\Gamma\cup\{\exists x p\} \vdash q$，且除了$x$不增加其他Gen变元。

证 已知$\Gamma\cup\{p\} \vdash q$，且Gen变元不在p中自由出现，于是以下公式从Γ可证：

(1) $p\rightarrow q$ 由演绎定理

(2) $(p\rightarrow q) \rightarrow (\neg q\rightarrow \neg p)$ 永真式

……

§2.1.3 谓词演算K

命题5 对K中任意公式p,q,r有

1) $\vdash p \leftrightarrow p$

2) $\vdash p \leftrightarrow q \Rightarrow \vdash q \leftrightarrow p$

3) $\vdash p \leftrightarrow q$ 且 $\vdash q \leftrightarrow r \Rightarrow \vdash p \leftrightarrow r$

证 1) $p \leftrightarrow p$是永真式。

2) 已知$\vdash p \leftrightarrow q$而$(p \leftrightarrow q) \rightarrow (q \leftrightarrow p)$是永真式…

3) 由已知及永真式$(p \leftrightarrow q) \rightarrow ((q \leftrightarrow r) \rightarrow (p \leftrightarrow r))$…

定义3(可证等价) 若$\vdash p \leftrightarrow q$，则称p与q可证等价。

命题6 $\Gamma \vdash p \leftrightarrow q \Leftrightarrow \Gamma \vdash p \rightarrow q$且$\Gamma \vdash q \rightarrow p$

§2.1.3 谓词演算K

命题7 1) $\vdash \forall x p(x) \leftrightarrow \forall y p(y)$

2) $\vdash \exists x p(x) \leftrightarrow \exists y p(y)$

其中y不在$p(x)$中出现。

证 1) 先证$\{\forall x p(x)\} \vdash \forall y p(y)$.

(1) $\forall x p(x)$

(2) $\forall x p(x) \rightarrow p(y)$

(3) $p(y)$

(4) $\forall y p(y)$

Gen变元y不在$\forall x p(x)$中自由出现，由演绎定理就可得到

$\vdash \forall x p(x) \rightarrow \forall y p(y)$

同样可得$\vdash \forall y p(y) \rightarrow \forall x p(x)$…。 由此也可得2)

§2.1.3 谓词演算K

命题8 1) $\vdash \neg\forall x p \leftrightarrow \exists x \neg p$

2) $\vdash \neg\exists x p \leftrightarrow \forall x \neg p$

证 1) 用(K4)、双重否定律及Gen分别证明

$\forall x \neg\neg p \rightarrow \forall x p$和$\forall x p \rightarrow \forall x \neg\neg p$

用换位律后得$\vdash \neg\forall x p \leftrightarrow \neg\forall x \neg\neg p$

2) $\neg\neg\forall x \neg p \leftrightarrow \forall x \neg p$是永真式。

§2.1.4 对偶律与前束范式

定理1 (子公式等价可替换性) 设q是p的子公式：p=…q…，用公式q′替换p中的q(一处替换)所得结果记为p′=…q′…，则

$$\Gamma \vdash q \leftrightarrow q' \Rightarrow \Gamma \vdash p \leftrightarrow p'$$

证 对p在K(Y)的层次n归纳。

n=0时，p是原子公式，故p=q，p′=q′，显然命题成立。

n>0时，除p=q这种情形外，还有以下三种可能情形：

(i) $p = \neg r$

此时q是r的子公式，$p' = \neg r'$，由归纳假设有

$$\Gamma \vdash q \leftrightarrow q' \Rightarrow \Gamma \vdash r \leftrightarrow r'$$

而$(r \leftrightarrow r') \leftrightarrow (\neg r \leftrightarrow \neg r')$是永真式。

§2.1.4 对偶律与前束范式

(ii) $p = r \to s$

q是r或s的子公式。于是$p' = r' \to s$ 或$p' = r \to s'$。我们有永真式

$$(r \leftrightarrow r') \to ((r \to s) \leftrightarrow (r' \to s))$$

及

$$(s \leftrightarrow s') \to ((r \to s) \leftrightarrow (r \to s'))$$

再加上归纳假设即可。

(iii) $p = \forall x\, r$，q是r的子公式，$p' = \forall x\, r'$。

由归纳假设有$\Gamma \vdash q \leftrightarrow q' \Rightarrow \Gamma \vdash r \leftrightarrow r'$。下证$\Gamma \vdash \forall x\, r \leftrightarrow \forall x\, r'$，由对称性，只用证$\Gamma \vdash \forall x\, r \to \forall x\, r'$。再由演绎定理，给出$\Gamma \cup \{\forall x\, r\} \vdash \forall x\, r'$的证明如下

§2.1.4 对偶律与前束范式

(1) $\forall x\ \mathrm{r}$

(2) $\forall x\ \mathrm{r} \rightarrow \mathrm{r}$

(3) r

(4) $\mathrm{r} \rightarrow ((\mathrm{r} \leftrightarrow \mathrm{r}') \rightarrow \mathrm{r}')$

(5) $(\mathrm{r} \leftrightarrow \mathrm{r}') \rightarrow \mathrm{r}'$

(6) $\mathrm{r} \rightarrow \mathrm{r}'$

(7) r'

(8) $\forall x\ \mathrm{r}'$

- 上述证明中，除x外，无其他Gen变元。

§2.1.4 对偶律与前束范式

定理2(对偶律) 设公式p已表示成只含原子公式和¬, ∨, ∧, ∀, ∃的形式。现把p中原子公式全部改为它们的否定、把∨与∧互换、∀与∃互换，这样得到的公式p*叫做p的**对偶**。则有

$$\vdash p^* \leftrightarrow \neg p$$

证 对p中¬,∨,∧,∀,∃ 出现的总次数n进行归纳。

n=0时，p是原子公式，则$p^* = \neg p$。

n>0时，有五种可能：$p = \neg q$, $p = q \vee r$, $p = q \wedge r$, $p = \forall x\, q$, $p = \exists x\, q$. 由归纳假设，总有$\vdash q^* \leftrightarrow \neg q$, $\vdash r^* \leftrightarrow \neg r$。分别讨论如下

Case 1: $p = \neg q$. 在p^* $(= \neg q^*)$中用¬q 等价替换q^*，由定理1有

$\vdash q^* \leftrightarrow \neg q \Rightarrow \vdash \neg q^* \leftrightarrow \neg\neg q$，即$\vdash p^* \leftrightarrow \neg p$。

§2.1.4 对偶律与前束范式

Case 2: $p = q \vee r$, $p^* = q^* \wedge r^*$，在p^*中先后分别用$\neg q$和$\neg r$ 替换q^*和r^*得

$$\vdash p^* \leftrightarrow (\neg q \wedge \neg r)$$

再用De. Morgan律得

$$\vdash p^* \leftrightarrow \neg (q \vee r)，即 \vdash p^* \leftrightarrow \neg p$$

Case 3: $p = q \wedge r$, 其证明与上一种情形完全相同。

Case 4: $p = \forall x\, q$， $p^* = \exists x\, q^*$。此时有

$$\vdash q^* \leftrightarrow \neg q$$

$$\vdash \exists x\, q^* \leftrightarrow \exists x\, \neg q$$

$$\vdash \exists x\, q^* \leftrightarrow \neg \forall x\, \neg\neg q$$

$$\vdash \neg \forall x\, \neg\neg q \leftrightarrow \neg \forall x\, q$$

$$\vdash \exists x\, q^* \leftrightarrow \neg \forall x\, q \qquad (即 \vdash p^* \leftrightarrow \neg p)$$

§2.1.4 对偶律与前束范式

Case 5: $p = \exists x\, q$， $p^* = \forall x\, q^*$。证明同情形4。

命题1 若x不在p中自由出现，则

1) $\vdash \forall x(p \to q) \leftrightarrow (p \to \forall x\, q)$

2) $\vdash \exists x(p \to q) \leftrightarrow (p \to \exists x\, q)$

若x不在q中自由出现，则

3) $\vdash \forall x(p \to q) \leftrightarrow (\exists x\, p \to q)$

4) $\vdash \exists x(p \to q) \leftrightarrow (\forall x\, p \to q)$

证 2) 只证$\vdash \exists x(p \to q) \to (p \to \exists x\, q)$。再由演绎定理，只用证$\{\exists x(p \to q), p\} \vdash \exists x\, q$ $(\neg\forall x\, \neg q)$，证明过程中除了x外不用其他Gen变元即可。从$\{\exists x(p \to q), p, \forall x\, \neg q\}$可证……

§2.1.4 对偶律与前束范式

3) 只证⊢ $\forall x(p\to q)\to(\exists x\, p\to q)$。

以下公式从$\{\forall x(p\to q), \exists x p, \neg q\}$可证……

4) 只证⊢ $(\forall x p\to q)\to\exists x(p\to q)$。

以下公式从$\{\forall x p\to q, \forall x\neg(p\to q)\}$可证……

定义1(前束范式) 前束范式指的是形如

$$Q_1x_1\ldots Q_nx_np$$

的公式，其中$Q_1,\ldots,Q_n$表示∀或∃，而p是不含量词的谓词公式。

§2.1.4 对偶律与前束范式

命题2 用Q表示∀或∃，Q*表示Q的对偶符号(∀、∃互为对偶)，那么

1) 若y不在p(x)中出现，则

$$\vdash Qx\ p(x) \leftrightarrow Qy\ p(y)$$

2) 若x不在p中自由出现，则

$$\vdash (p \rightarrow Qx\ q) \leftrightarrow Qx(p \rightarrow q)$$

若x不在q中自由出现，则

$$\vdash (Qx\ p \rightarrow q) \leftrightarrow Q^*x(p \rightarrow q)$$

3) $\vdash \neg Qx\ p \leftrightarrow Q^*x\ \neg p$

§2.1.4 对偶律与前束范式

例1 找出与公式

$$p = \neg(\forall x_1 \exists x_2 R_1^3(c_1, x_1, x_2) \rightarrow \exists x_1(\neg \forall x_2 R_1^2(x_2, c_2) \rightarrow R_1^1(x_1)))$$

等价的前束范式。

解 对p中约束变元适当改名得等价公式q_1：

$$q_1 = \neg(\forall x_3 \exists x_4 R_1^3(c_1, x_3, x_4) \rightarrow \exists x_1(\neg \forall x_2 R_1^2(x_2, c_2) \rightarrow R_1^1(x_1)))$$

从q_1出发反复应用命题2进行等价变换：

$$q_2 = \neg \exists x_3 \forall x_4 (R_1^3(c_1, x_3, x_4) \rightarrow \exists x_1(\neg \forall x_2 R_1^2(x_2, c_2) \rightarrow R_1^1(x_1)))$$

$$q_3 = \neg \exists x_3 \forall x_4 (R_1^3(c_1, x_3, x_4) \rightarrow \exists x_1(\exists x_2 \neg R_1^2(x_2, c_2) \rightarrow R_1^1(x_1)))$$

$$q_4 = \neg \exists x_3 \forall x_4 (R_1^3(c_1, x_3, x_4) \rightarrow \exists x_1 \forall x_2(\neg R_1^2(x_2, c_2) \rightarrow R_1^1(x_1)))$$

$$q_5 = \neg \exists x_3 \forall x_4 \exists x_1 \forall x_2 (R_1^3(c_1, x_3, x_4) \rightarrow (\neg R_1^2(x_2, c_2) \rightarrow R_1^1(x_1)))$$

$$q_6 = \forall x_3 \exists x_4 \forall x_1 \exists x_2 \neg (R_1^3(c_1, x_3, x_4) \rightarrow (\neg R_1^2(x_2, c_2) \rightarrow R_1^1(x_1)))$$

§2.1.4 对偶律与前束范式

命题3 1) $\vdash (\forall x\, p \wedge \forall x\, q) \leftrightarrow \forall x\, (p \wedge q)$

2) $\vdash (\exists x\, p \vee \exists x\, q) \leftrightarrow \exists x\, (p \vee q)$

若x不在p中自由出现，则

3) $\vdash (p \vee Qx\, q) \leftrightarrow Qx\, (p \vee q)$

4) $\vdash (p \wedge Qx\, q) \leftrightarrow Qx\, (p \wedge q)$

§2.1.4 对偶律与前束范式

例1* 找出与公式

$$p = \neg(\forall x_1 \exists x_2 R_1^3(c_1, x_1, x_2) \rightarrow \exists x_1(\neg \forall x_2 R_1^2(x_2, c_2) \rightarrow R_1^1(x_1)))$$

等价的前束范式。

解 首先，消去$\rightarrow$：

$$q_1 = \neg(\neg \forall x_1 \exists x_2 R_1^3(c_1, x_1, x_2) \vee \exists x_1(\neg\neg \forall x_2 R_1^2(x_2, c_2) \vee R_1^1(x_1)))$$

继续进行等价变换：

$$q_2 = \forall x_1 \exists x_2 R_1^3(c_1, x_1, x_2) \wedge \neg \exists x_1 \forall x_2 (R_1^2(x_2, c_2) \vee R_1^1(x_1))$$

$$q_3 = \forall x_1 \exists x_2 R_1^3(c_1, x_1, x_2) \wedge \forall x_1 \exists x_2 (\neg R_1^2(x_2, c_2) \wedge \neg R_1^1(x_1))$$

$$q_4 = \forall x_1 (\exists x_2 R_1^3(c_1, x_1, x_2) \wedge \exists x_2 (\neg R_1^2(x_2, c_2) \wedge \neg R_1^1(x_1)))$$

$$q_5 = \forall x_1 (\exists x_3 R_1^3(c_1, x_1, x_3) \wedge \exists x_2 (\neg R_1^2(x_2, c_2) \wedge \neg R_1^1(x_1)))$$

$$q_6 = \forall x_1 \exists x_3 \exists x_2 (R_1^3(c_1, x_1, x_3) \wedge \neg R_1^2(x_2, c_2) \wedge \neg R_1^1(x_1))$$

§2.1.4 对偶律与前束范式

定义2 设n>0，若前束范式是由全称量词开始，从左至右改变n-1次词性，则叫做Π_n型前束范式；若是由存在量词开始，从左至右改变n-1次词性，则叫做Σ_n型前束范式。

例2 $p = \forall x_1 \exists x_2 R_1^2(x_1, x_2) \rightarrow \forall x_3 \exists x_4 R_1^2(x_3, x_4)$

§2.2 谓词演算K的语义

2.2.1 K的解释域与项解释

定义1(K的解释域) 设非空集合M具有以下性质

1) 对K的每个个体常元 c_i，都有M的元素$\overline{c_i}$ 与之对应：

$c_i \mapsto \overline{c_i}, \overline{c_i} \in M$

2) 对K的每个运算符f_i^n，都有M的n元运算$\overline{f_i^n}$ 与之对应：

$f_i^n \mapsto \overline{f_i^n}, \overline{f_i^n}$是M上的n元运算

3) 对K的每个谓词R_i^n，都有M的n元关系$\overline{R_i^n}$与之对应：

$R_i^n \mapsto \overline{R_i^n}, \overline{R_i^n}$是M上的n元关系

带有上述三个映射的非空集M叫做K的解释域。

2.2.1 K的解释域与项解释

- 解释域是有内部结构的非空集。当K的运算符集F≠∅时，解释域是个代数系统。
- 解释域也叫“解释”或“结构”，其元素叫个体对象。
- 给定解释域M，K中只涉及闭项的原子公式便可解释为关于M的元素的命题。

例1 设K中的C=$\{c_1\}$，F=$\{f_1^1, f_1^2, f_2^2\}$，R=$\{R_1^2\}$。下面是K的一个解释域：

N=$\{0, 1, 2, \ldots\}$.

$\overline{c_1}$ =0

$\overline{f_1^1}$: 后继函数 $\overline{f_1^1}$(n)=n+1, $\overline{f_1^2}$: 加法(+)，$\overline{f_2^2}$: 乘法(×)

$\overline{R_1^2}$: 相等(=)

2.2.1 K的解释域与项解释

还可以给出K的另外一个解释域：

Q$^+$: 正有理数集.

$\overline{c_1}$: 1

$\overline{f_1^1}$: 倒数函数, $\overline{f_1^2}$: 乘法(×)，$\overline{f_2^2}$: 除法(÷)

$\overline{R_1^2}$: 相等(=)

设p=$R_1^2(f_1^2(f_1^1(c_1), c_1), f_2^2(f_1^1(c_1), c_1))$

在**N**中，p解释成

在**Q**$^+$中，p解释成

2.2.1 K的解释域与项解释

- **项解释**

设M是给定的解释域，映射φ_0: X→M叫做个体变元的对象指派，在此基础上递归定义项解释φ: T→M

(1) $\varphi(x_i)=\varphi_0(x_i)$， $\varphi(c_i)=\overline{c_i}$

若$\varphi(t_1),\ldots,\varphi(t_n)$已有定义，则令

(2) $\varphi(f_i^n(t_1,\ldots,t_n))=\overline{f_i^n}(\varphi(t_1),\ldots,\varphi(t_n))$

(2)称作项解释的“保运算性”。

- 给定解释域M，只要变元进行了指派，便有了确定的项解释(每个项都在M中有了解释)。
- 对固定的解释域M，记 $\Phi_M=\{\varphi \mid \varphi: T\rightarrow M是项解释\}$

2.2.1 K的解释域与项解释

定义2(项解释的变元变通) 设x是某个给定的个体变元，y是任意的个体变元，且φ、$\varphi' \in \Phi_M$满足条件

(3) $y \neq x \Rightarrow \varphi'(y)=\varphi(y)$

则把φ'叫做φ的x变通。(φ与φ'互为对方的x变通)

- 变元的指派φ_0确定 $\Rightarrow$ 原子公式的解释便确定
- 记$\bar{x} = \varphi_0(x) = \varphi(x)$, $\bar{t}= \varphi(t)$

2.2.2 公式的赋值函数

定义1(公式的赋值函数) 给定解释域M和K中任一公式p。如下归纳定义的函数|p|: $\Phi_M \to \mathbf{Z}_2$叫做**公式p的赋值函数**。

对任一项解释$\varphi \in \Phi_M$.

(1) 当p为原子公式$R_i^n(t_1,t_2,\ldots,t_n)$时，令

$$|p|(\varphi)=\begin{cases}1, \text{若}(\overline{t_1},\ldots,\overline{t_n}) \in \overline{R_i^n}\\ 0, \text{若}(\overline{t_1},\ldots,\overline{t_n}) \notin \overline{R_i^n}\end{cases}$$

(2) 当p是¬q或q→r时，令

$|\neg q|(\varphi) = \neg|q|(\varphi)$，　$|q\to r|(\varphi) = |q|(\varphi)\to|r|(\varphi)$

(3) 当p是$\forall x$ q时, 令

$$|\forall x\, q|(\varphi)=\begin{cases}1, \text{若}\varphi\text{的任一}x\text{变通}\varphi'\text{都使}|q|(\varphi') = 1\\ 0, \quad \text{若存在}\varphi\text{的}x\text{变通}\varphi'\text{使}|q|(\varphi') = 0\end{cases}$$

2.2.2 公式的赋值函数

- 一旦解释域M给定，K中任一公式p就有了确定的赋值函数|p|。 |p|的自变量是项解释$\varphi \in \Phi_M$， 函数值|p|(φ)为1或0.

例子

命题1 1) $|p \vee q|(\varphi) = |p|(\varphi) \vee |q|(\varphi)$

2) $|p \wedge q|(\varphi) = |p|(\varphi) \wedge |q|(\varphi)$

3) $|p \leftrightarrow q|(\varphi) = |p|(\varphi) \leftrightarrow |q|(\varphi)$

4) $|\exists x\, q|(\varphi) = 1 \Leftrightarrow$ 存在φ的x变通φ'都使$|q|(\varphi') = 1$

2.2.3 闭式的语义特征

命题1 设M是K的解释域，$\varphi、\psi \in \Phi_M$.

1) 若对项t中的任一变元x都有$\varphi(x)=\psi(x)$，则$\varphi(t) = \psi(t)$

2)若对公式p中任一自由变元x都有$\varphi(x)=\psi(x)$，则$|p|(\varphi) = |p|(\psi)$。

证 2) 对p在K(Y)中的层次k进行归纳。

k=0时，设p= $R_j^n(t_1,t_2,\ldots,t_n)$，此时项$t_1,t_2,\ldots,t_n$中出现的变元在p中都是自由出现的。由1)，$\varphi(t_i) = \psi(t_i)$，i=1,…,n.

于是 $|p|(\varphi) = 1 \Leftrightarrow (\varphi(t_1), \ldots, \varphi(t_n)) \in \overline{R_j^n}$

$\Leftrightarrow (\psi(t_1), \ldots, \psi(t_n)) \in \overline{R_j^n} \Leftrightarrow |p|(\psi) = 1$

k>0时有三种情形：

(i) $p = \neg q$.

2.2.3 闭式的语义特征

(i) $p = \neg q$.

$$|\neg q|(\varphi) = 1 \Leftrightarrow |q|(\varphi) = 0$$
$$\Leftrightarrow |q|(\psi) = 0 \qquad \text{(归纳假设)}$$
$$\Leftrightarrow |\neg q|(\psi) = 1$$

(ii) $p = q \rightarrow r$.

$$|q \rightarrow r|(\varphi) = 1 \Leftrightarrow |q|(\varphi) \rightarrow |r|(\varphi) = 1$$
$$\Leftrightarrow |q|(\psi) \rightarrow |r|(\psi) = 1 \quad \text{(归纳假设)}$$
$$\Leftrightarrow |q \rightarrow r|(\psi) = 1$$

(iii) $p = \forall x\, q$. 设$|\forall x\, q|(\varphi) = 1$. 对$\psi$的任一$x$变通$\psi'$，作$\varphi$的$x$变通$\varphi'$使$\varphi'(x)=\psi'(x)$。$x$在q中可能自由出现，而在q中自由出现的其他变元$y(\neq x)$一定也在p中自由出现，于是

2.2.3 闭式的语义特征

$$\varphi'(y) = \varphi(y) \qquad (\varphi'是\varphi的x变通)$$
$$= \psi(y) \qquad (已知条件)$$
$$= \psi'(y) \qquad (\psi'是\psi的x变通)$$

所以对q来说，φ'和ψ'满足所要求的条件，由归纳假设$|q|(\psi') = |q|(\varphi')$。又因已假设$|\forall x\ q|(\varphi) = 1$，故$|q|(\varphi') = 1$因而$|q|(\psi') = 1$，于是$|\forall x\ q|(\psi) = 1$。

同样可证

$$|\forall x\ q|(\psi) = 1 \Rightarrow |\forall x\ q|(\varphi) = 1$$

这说明 $|\forall x\ q|(\varphi) = |\forall x\ q|(\psi)$。

2.2.3 闭式的语义特征

定义1(公式在解释域的恒真与恒假) 公式p在解释域M中恒真，记作$|p|_M=1$，是指对任一$\varphi\in\Phi_M$，$|p|(\varphi)=1$；若对任一$\varphi\in\Phi_M$，$|p|(\varphi)=0$，则称p在解释域M中恒假，记作$|p|_M=0$.

解释域M中的非恒假公式叫做M中的可满足公式。

例1 设K中的C=$\{c_1\}$，F=$\{f_1^1\}$，R=$\{R_1^2\}$；解释域为**N**。设p_1是公式$R_1^2(x_1,x_1)$，p_2是$\forall x_1 R_1^2(x_1,c_1)$，$p_3$是$R_1^2(x_1,c_1)$。

c_1解释为$\overline{c_1}=0$, R_1^2解释为$\overline{R_1^2}$: 相等(=)。则

$|p_1|_N=1$

$|p_2|_N=0$

p_3在**N**中既非恒真也非恒假，p_3是**N**中可满足公式。

2.2.3 闭式的语义特征

定理1 对给定的解释域M，任一闭式p在M中恒真与恒假二者必居其一： $|p|_M=1$或$|p|_M=0$.

(闭式不含自由变元)

例2 设K中的C=$\{c_1\}$，F=$\{f_1^1\}$，R=$\{R_1^1\}$。而p是公式 $\forall x_1(R_1^1(x_1)\rightarrow R_1^1(f_1^1(x_1))$。

1) 取M_1=**Z**，$\overline{c_1}$ =0，$\overline{f_1^1}$为后继函数， **Z**上一元关系$\overline{R_1^1}$为$\mathbf{Z}^+$。易验证 $|p|_{M1}=1$.

2) M_2=**Z**，取 $\overline{R_1^1}$ 为偶数集，则$|p|_{M2}=0$.

2.2.3 闭式的语义特征

命题2 $|p|_M=1 \Leftrightarrow |\forall x p|_M=1$.

证 ($\Rightarrow$)

$|p|_M=1 \Rightarrow$ 对任意$\varphi\in\Phi_M$及φ的任一x变通φ'，有$|p|(\varphi')=1$

$\Rightarrow$ 对任意$\varphi\in\Phi_M$， $|\forall x p|(\varphi)=1$

$\Rightarrow |\forall x p|_M=1$

($\Leftarrow$)

$|\forall x p|_M=1 \Rightarrow$ 对任意$\varphi\in\Phi_M$， $|\forall x p|(\varphi)=1$

$\Rightarrow$ 对任意$\varphi\in\Phi_M$， $|p|(\varphi)=1$ (φ是自己的x变通)

$\Rightarrow |p|_M=1$

2.2.3 闭式的语义特征

定义2 设$x_{i1},\ldots,x_{in}$是p中自由出现的全体变元，则

$$\forall x_{i1}\ldots\forall x_{in}\mathrm{p}$$

叫做p的全称闭式。

命题3 设p′是p的全称闭式，则$|\mathrm{p}|_M=1 \Leftrightarrow |\mathrm{p}'|_M=1$.

命题4 $|\mathrm{p}|_M=0 \Rightarrow |\forall x\mathrm{p}|_M=0$.

证 $|\mathrm{p}|_M=0$时对任意$\varphi\in\Phi_M$，有$|\mathrm{p}|(\varphi)=0$；于是$|\forall x\mathrm{p}|(\varphi)=0$。$\varphi$是任意的，故$|\forall x\mathrm{p}|_M=0$。

2.2.3 闭式的语义特征

推论1 $|p|_M=0 \Rightarrow |p'|_M=0$. p'是p的全称闭式。

命题5 $|p|_M=1$且 $|p\rightarrow q|_M=1 \Rightarrow |q|_M=1$.

证 任取$\varphi\in\Phi_M$，有

$|p|(\varphi)=1$且 $|p\rightarrow q|(\varphi)=1 \Rightarrow |q|(\varphi)=1$ 。

2.2.4 语义推论与有效式

定义1(模型) 设M是K的一个解释域。若公式集Γ的每个公式都在M中恒真，则称M是Γ的**模型**：

$$r \in \Gamma \Rightarrow |r|_M = 1.$$

- Γ=∅时任何解释域都是Γ的模型。

定义2 (语义推论) 公式p是公式集Γ的语义推论，记作Γ⊨ p, 指p在Γ的所有模型中恒真(Γ的任何模型都是Γ∪{p}的模型)：

$$\Gamma \models p \Leftrightarrow \text{当每个} r \in \Gamma \text{ 都有 } |r|_M = 1 \text{时，也有} |p|_M = 1.$$

定义3 (有效式与可满足公式) ∅ ⊨ p时, p叫做K的**有效式**, 记为⊨ p。若¬p不是有效式，则p叫做K的**可满足公式**。

- ⊨ p ⇔ p在K的所有解释域中恒真。

2.2.4 语义推论与有效式

命题1 K中命题演算型永真式都是有效式。

证 由2.1.3的定义2，K的命题演算型永真式是指形为$p(p_1, p_2,\ldots, p_n)$的公式，它由K的任意公式$p_1,p_2,\ldots,p_n$分别代换命题演算L的永真式 $p(x_1,x_2,\ldots,x_n)$ 中的命题变元$x_1,x_2,\ldots,x_n$所得结果。注意$p(p_1, p_2,\ldots, p_n)$ 由$p_1, p_2,\ldots, p_n$经过$\neg,\rightarrow$两种运算得到。任取K的解释域M和$\varphi\in\Phi_M$。根据赋值对$\neg,\rightarrow$的保运算性，有

$$|p(p_1, p_2,\ldots, p_n)|(\varphi) = p(|p_1|(\varphi), |p_2|(\varphi),\ldots, |p_n|(\varphi))$$

因为$p(x_1, x_2,\ldots, x_n)$是L的永真式，而$|p_1|(\varphi), |p_2|(\varphi),\ldots, |p_n|(\varphi)\in\{0,1\}$，故上式右端为1. φ是任意的，于是

$$|p(p_1, p_2,\ldots, p_n)|_M=1$$

又因M是任意的，最后得到 $\vDash p(p_1, p_2,\ldots, p_n)$。

2.2.4 语义推论与有效式

推论1 (K1),(K2),(K3)这三种模式的公理都是有效式。

证 它们都是命题演算型永真式。

命题2 $\Gamma \vDash p$且$\Gamma \vDash p \to q \Rightarrow \Gamma \vDash q$.

证 设M是Γ的任一模型，当$\Gamma \vDash p$且$\Gamma \vDash p \to q$时，有

$$|p|_M=1 \text{ 且 } |p \to q|_M=1$$

根据2.2.3命题5，又有$|q|_M=1$，所以$\Gamma \vDash q$。

例1 $\{R_1^1(x_1)\} \vDash \forall x_1 R_1^1(x_1)$

因为$|R_1^1(x_1)|_M=1 \Rightarrow |\forall x_1 R_1^1(x_1)|_M=1$.

2.2.4 语义推论与有效式

例2 $\not\models R_1^1(x_1) \to \forall x_1 R_1^1(x_1)$

命题3 $\Gamma \models p \Leftrightarrow \Gamma \models \forall x p$.

证 $\Gamma \models p \Leftrightarrow$ 对于Γ的任一模型M，$|p|_M=1$

$\Leftrightarrow$ 对于Γ的任一模型M，$|\forall x p|_M=1$

$\Leftrightarrow \Gamma \models \forall x p$.

命题4 设p'是p的全称闭式，则有

$\Gamma \models p \Leftrightarrow \Gamma \models p'$.

第二章 谓词演算

刘贵全

gqliu@ustc.edu.cn

§2 谓词演算

内容提要

2.1 谓词演算(K)的建立
2.2 谓词演算(K)的语义
2.3 K的可靠性
2.4 K的完全性

2.2.3 闭式的语义特征

命题1 设M是K的解释域，$\varphi、\psi \in \Phi_M$.

1) 若对项t中的任一变元x都有$\varphi(x)=\psi(x)$，则$\varphi(t) = \psi(t)$.

2) 若对公式p中任一自由变元x都有$\varphi(x)=\psi(x)$，则$|p|(\varphi) = |p|(\psi)$。

证 2) 对p在K(Y)中的层次k进行归纳。

k=0时，设p= $\overline{R_j^n}(t_1,t_2,\ldots,t_n)$，此时项$t_1,t_2,\ldots,t_n$中出现的变元在p中都是自由出现的。由1)，$\varphi(t_i) = \psi(t_i)$，i=1,…,n.

于是 $|p|(\varphi) = 1 \Leftrightarrow (\varphi(t_1), \ldots, \varphi(t_n)) \in \overline{R_j^n}$

$\Leftrightarrow (\psi(t_1), \ldots, \psi(t_n)) \in \overline{R_j^n} \Leftrightarrow |p|(\psi) = 1$

k>0时有三种情形：

(i) $p = \neg q$.

2.2.3 闭式的语义特征

(i) $p = \neg q$.

$$|\neg q|(\varphi) = 1 \Leftrightarrow |q|(\varphi) = 0$$
$$\Leftrightarrow |q|(\psi) = 0 \qquad \text{(归纳假设)}$$
$$\Leftrightarrow |\neg q|(\psi) = 1$$

(ii) $p = q \rightarrow r$.

$$|q \rightarrow r|(\varphi) = 1 \Leftrightarrow |q|(\varphi) \rightarrow |r|(\varphi) = 1$$
$$\Leftrightarrow |q|(\psi) \rightarrow |r|(\psi) = 1 \quad \text{(归纳假设)}$$
$$\Leftrightarrow |q \rightarrow r|(\psi) = 1$$

(iii) $p = \forall x\, q$. 设$|\forall x\, q|(\varphi) = 1$. 对$\psi$的任一$x$变通$\psi'$，作$\varphi$的$x$变通$\varphi'$使$\varphi'(x)=\psi'(x)$。$x$在q中可能自由出现，而在q中自由出现的其他变元$y(\neq x)$一定也在p中自由出现，于是

2.2.3 闭式的语义特征

$$\varphi'(y) = \varphi(y) \qquad (\varphi'是\varphi的x变通)$$
$$= \psi(y) \qquad (已知条件)$$
$$= \psi'(y) \qquad (\psi'是\psi的x变通)$$

所以对q来说，φ'和ψ'满足所要求的条件，由归纳假设$|q|(\psi') = |q|(\varphi')$。又因已假设$|\forall x\ q|(\varphi) = 1$，故$|q|(\varphi') = 1$因而$|q|(\psi') = 1$，于是$|\forall x\ q|(\psi) = 1$。

同样可证

$$|\forall x\ q|(\psi) = 1 \Rightarrow |\forall x\ q|(\varphi) = 1$$

这说明 $|\forall x\ q|(\varphi) = |\forall x\ q|(\psi)$。

2.2.3 闭式的语义特征

定义1(公式在解释域的恒真与恒假) 公式p在解释域M中恒真，记作$|p|_M=1$，是指对任一$\varphi\in\Phi_M$，$|p|(\varphi)=1$；若对任一$\varphi\in\Phi_M$，$|p|(\varphi)=0$，则称p在解释域M中恒假，记作$|p|_M=0$.

解释域M中的非恒假公式叫做M中的可满足公式。

例1 设K中的C=$\{c_1\}$，F=$\{f_1^1\}$，R=$\{R_1^2\}$；解释域为**N**。设p_1是公式$R_1^2(x_1,x_1)$，p_2是$\forall x_1 R_1^2(x_1,c_1)$，$p_3$是$R_1^2(x_1,c_1)$。

c_1解释为$\overline{c_1}=0$, R_1^2解释为$\overline{R_1^2}$: 相等(=)。则

$|p_1|_N=1$

$|p_2|_N=0$

p_3在**N**中既非恒真也非恒假，p_3是**N**中可满足公式。

2.2.3 闭式的语义特征

定理1 对给定的解释域M，任一闭式p在M中恒真与恒假二者必居其一： $|p|_M=1$或$|p|_M=0$.

(闭式不含自由变元)

例2 设K中的C=$\{c_1\}$，F=$\{f_1^1\}$，R=$\{R_1^1\}$。而p是公式 $\forall x_1(R_1^1(x_1)\rightarrow R_1^1(f_1^1(x_1))$。

1) 取M_1=**Z**，$\overline{c_1}$ =0，$\overline{f_1^1}$为后继函数， **Z**上一元关系$\overline{R_1^1}$为$\mathbf{Z}^+$。易验证 $|p|_{M1}=1$.

2) M_2=**Z**，取 $\overline{R_1^1}$ 为偶数集，则$|p|_{M2}=0$.

2.2.3 闭式的语义特征

命题2 $|p|_M=1 \Leftrightarrow |\forall x p|_M=1$.

证 ($\Rightarrow$)

$|p|_M=1 \Rightarrow$ 对任意$\varphi\in\Phi_M$及φ的任一x变通φ'，有$|p|(\varphi')=1$

$\Rightarrow$ 对任意$\varphi\in\Phi_M$， $|\forall x p|(\varphi)=1$

$\Rightarrow |\forall x p|_M=1$

($\Leftarrow$)

$|\forall x p|_M=1 \Rightarrow$ 对任意$\varphi\in\Phi_M$， $|\forall x p|(\varphi)=1$

$\Rightarrow$ 对任意$\varphi\in\Phi_M$， $|p|(\varphi)=1$ (φ是自己的x变通)

$\Rightarrow |p|_M=1$

2.2.3 闭式的语义特征

定义2 设$x_{i1},\ldots,x_{in}$是p中自由出现的全体变元，则

$$\forall x_{i1}\ldots\forall x_{in}\mathrm{p}$$

叫做p的**全称闭式**。

命题3 设p′是p的全称闭式，则$|\mathrm{p}|_M=1 \Leftrightarrow |\mathrm{p}'|_M=1$.

命题4 $|\mathrm{p}|_M=0 \Rightarrow |\forall x\mathrm{p}|_M=0$.

证 $|\mathrm{p}|_M=0$时对任意$\varphi\in\Phi_M$，有$|\mathrm{p}|(\varphi)=0$；于是$|\forall x\mathrm{p}|(\varphi)=0$。$\varphi$是任意的，故$|\forall x\mathrm{p}|_M=0$。

2.2.3 闭式的语义特征

推论1 $|p|_M=0 \Rightarrow |p'|_M=0$. p'是p的全称闭式。

命题5 $|p|_M=1$且 $|p\to q|_M=1 \Rightarrow |q|_M=1$.

证 任取$\varphi\in\Phi_M$，有

$|p|(\varphi)=1$且 $|p\to q|(\varphi)=1 \Rightarrow |q|(\varphi)=1$ 。

2.2.4 语义推论与有效式

定义1(模型) 设M是K的一个解释域。若公式集Γ的每个公式都在M中恒真，则称M是Γ的**模型**：

$$r \in \Gamma \Rightarrow |r|_M = 1.$$

- Γ=∅时任何解释域都是Γ的模型。

定义2 (语义推论) 公式p是公式集Γ的语义推论，记作Γ⊨ p, 指p在Γ的所有模型中恒真(Γ的任何模型都是Γ∪{p}的模型)：

$$\Gamma \models p \Leftrightarrow \text{当每个} r \in \Gamma \text{ 都有 } |r|_M = 1 \text{时，也有} |p|_M = 1.$$

定义3 (有效式与可满足公式) ∅ ⊨ p时, p叫做K的**有效式**, 记为⊨ p。若¬p不是有效式，则p叫做K的**可满足公式**。

- ⊨ p ⇔ p在K的所有解释域中恒真。

2.2.4 语义推论与有效式

命题1 K中命题演算型永真式都是有效式。

证 由2.1.3的定义2，K的命题演算型永真式是指形为$p(p_1, p_2,\ldots, p_n)$的公式，它由K的任意公式$p_1,p_2,\ldots,p_n$分别代换命题演算L的永真式 $p(x_1,x_2,\ldots,x_n)$ 中的命题变元$x_1,x_2,\ldots,x_n$所得结果。注意$p(p_1, p_2,\ldots, p_n)$ 由$p_1, p_2,\ldots, p_n$经过$\neg,\rightarrow$两种运算得到。任取K的解释域M和$\varphi\in\Phi_M$。根据赋值对$\neg,\rightarrow$的保运算性，有

$$|p(p_1, p_2,\ldots, p_n)|(\varphi) = p(|p_1|(\varphi), |p_2|(\varphi),\ldots, |p_n|(\varphi))$$

因为$p(x_1, x_2,\ldots, x_n)$是L的永真式，而$|p_1|(\varphi), |p_2|(\varphi),\ldots, |p_n|(\varphi)\in\{0,1\}$，故上式右端为1. φ是任意的，于是

$$|p(p_1, p_2,\ldots, p_n)|_M=1$$

又因M是任意的，最后得到 $\vDash p(p_1, p_2,\ldots, p_n)$。

2.2.4 语义推论与有效式

推论1 (K1),(K2),(K3)这三种模式的公理都是有效式。

证 它们都是命题演算型永真式。

命题2 $\Gamma \vDash p$且$\Gamma \vDash p \to q \Rightarrow \Gamma \vDash q$.

证 设M是Γ的任一模型，当$\Gamma \vDash p$且$\Gamma \vDash p \to q$时，有

$$|p|_M=1 \text{ 且 } |p \to q|_M=1$$

根据2.2.3命题5，又有$|q|_M=1$，所以$\Gamma \vDash q$。

例1 $\{R_1^1(x_1)\} \vDash \forall x_1 R_1^1(x_1)$

因为$|R_1^1(x_1)|_M=1 \Rightarrow |\forall x_1 R_1^1(x_1)|_M=1$.

2.2.4 语义推论与有效式

例2 $\not\models R_1^1(x_1) \to \forall x_1 R_1^1(x_1)$

命题3 $\Gamma \models p \Leftrightarrow \Gamma \models \forall x p$.

证 $\Gamma \models p \Leftrightarrow$ 对于Γ的任一模型M，$|p|_M=1$

$\Leftrightarrow$ 对于Γ的任一模型M，$|\forall x p|_M=1$

$\Leftrightarrow \Gamma \models \forall x p$.

命题4 设p'是p的全称闭式，则有

$\Gamma \models p \Leftrightarrow \Gamma \models p'$.

2.3 K的可靠性

K的可靠性指

$$\Gamma\vdash p \Rightarrow \Gamma\models p \quad (\vdash p \Rightarrow \models p)$$

引理1 对给定的解释域，设φ′是项解释φ的x变通，且满足φ′(x)=φ(t)。t是某个项 .

1) 若u(x)是项，则φ′(u(x))=φ(u(t)).

2) 若t对公式p(x)中的x自由，则

$$|p(x)|(\varphi')=|p(t)|(\varphi)$$

证 1) 对u(x)在项集T中的层次数k归纳.

k=0时，有三种可能的情形(x可以不在u中出现)：

(i) u(x)=c_i，φ′(c_i)=φ(c_i).

2.3 K的可靠性

(ii) u(x)=y, $y \neq x$. 这时u(t)=y, φ′是φ的x变通，它与φ对y的取值是相同的，即φ′(y)=φ(y).

(iii) u(x)=x. 此时u(t)=t, 要证的等式φ′(u(x))=φ(u(t)) 即已知条件φ′(x)=φ(t).

k>0时，设u(x) = $f_i^n(t_1(x),t_2(x),\ldots,t_n(x))$，$t_1(x),t_2(x),\ldots,t_n(x)$是较低层次的项。这时

$$u(t) = f_i^n(t_1(t),t_2(t),\ldots,t_n(t))$$

于是有

$$\varphi'(u(x)) = \varphi'(f_i^n(t_1(x),t_2(x),\ldots,t_n(x)))$$
$$= \overline{f_i^n}(\varphi'(t_1(x)), \varphi'(t_2(x)),\ldots, \varphi'(t_n(x)))$$
$$= \overline{f_i^n}(\varphi(t_1(t)), \varphi(t_2(t)),\ldots, \varphi(t_n(t)))$$
$$= \varphi(f_i^n(t_1(t),t_2(t),\ldots,t_n(t))) = \varphi(u(t))$$

2.3 K的可靠性

2) 对公式p(x)在K(Y)中的层次数k归纳.

k=0时，p(x)是原子公式，设

$$p(x) = R_i^n(t_1(x),t_2(x),\ldots,t_n(x))$$

于是

$$p(t) = R_i^n(t_1(t),t_2(t),\ldots,t_n(t))$$

这时

$$|R_i^n(t_1(x),t_2(x),\ldots,t_n(x))|(\varphi') = 1$$

$$\Leftrightarrow (\varphi'(t_1(x)), \varphi'(t_2(x)),\ldots, \varphi'(t_n(x)))\in \overline{R_i^n}$$

$$\Leftrightarrow (\varphi(t_1(t)), \varphi(t_2(t)),\ldots, \varphi(t_n(t)))\in \overline{R_i^n}$$

$$\Leftrightarrow |R_i^n(t_1(t),t_2(t),\ldots,t_n(t))|(\varphi) = 1$$

$|p(x)|(\varphi')=|p(t)|(\varphi)$成立。

2.3 K的可靠性

k>0时，分四种情况进行讨论：

(i) 若$p(x) = \neg q(x)$，则$p(t) = \neg q(t)$，这时

$$|p(x)|(\varphi') = 1 \Leftrightarrow |q(x)|(\varphi') = 0$$
$$\Leftrightarrow |q(t)|(\varphi) = 0$$
$$\Leftrightarrow |p(t)|(\varphi) = 1$$

(ii) 若$p(x) = q(x) \rightarrow r(x)$，则$p(t) = q(t) \rightarrow r(t)$，这时

$$|p(x)|(\varphi') = 0 \Leftrightarrow |q(x)|(\varphi') = 1 \text{且} |r(x)|(\varphi') = 0$$
$$\Leftrightarrow |q(t)|(\varphi) = 1 \text{且} |r(t)|(\varphi) = 0$$
$$\Leftrightarrow |p(t)|(\varphi) = 0$$

(iii) 若$p(x) = \forall y q(x)$但x不在$p(x)$中自由出现，这时$p(t) = p(x)$。根据2.2.3小节命题1-2，有$|p(x)|(\varphi')=|p(t)|(\varphi)$.

2.3 K的可靠性

(iv) 若p(x) = ∀yq(x)且x在p(x)中自由出现，则y≠x且p(t) = ∀yq(t)(因t对公式p(x)中的x自由，故t中不含y。现证明

$$|p(x)|(\varphi') = 0 \quad \Leftrightarrow \quad |p(t)|(\varphi) = 0$$

先证(⇐).

设|p(t)|(φ) = 0，即|∀yq(t)|(φ) = 0。这时存在φ的y变通ψ使|q(t)|(ψ) = 0。再作ψ的x变通ψ′，使

(1) ψ′(x) = ψ(t).

于是由归纳假设可得

(2) |q(x)|(ψ′) = 0　　(上面已有|q(t)|(ψ) = 0)

ψ是φ的y变通，它与φ在除y之外的变元指派上都是一致的，而t不含y，利用2.2.3小节命题1-1得

(3) ψ(t) =φ(t).

2.3 K的可靠性

现证ψ′是φ′的y变通。为此要证 $z\neq y$时总有ψ′(z)=φ′(z)。$z\neq y$ 时，又分两种可能：$z\neq x$和$z=x$.

$z\neq x$时， ψ′(z) = ψ(z)　　(ψ′是ψ的x变通)

= φ(z)　　(ψ是φ的y变通)

= φ′(z)　　(φ′是φ的x变通)

$z=x$时， ψ′(z) = ψ′(x) = ψ(t)　　(由(1))

= φ(t)　　(由(3))

= φ′(x)　　(已知条件)

= φ′(z)　　($z=x$)

这说明ψ′是φ′的y变通，再由(2)式得

|∀yq(x)|(φ′) = 0　即　|p(x)|(φ′) = 0。

2.3 K的可靠性

再证另一个方向：

$$|p(x)|(\varphi') = 0 \Rightarrow |p(t)|(\varphi) = 0$$

设$|p(x)|(\varphi') = 0$，即 $|\forall y q(x)|(\varphi') = 0$。这时有$\varphi'$的$y$变通$\psi'$使

(4) $|q(x)|(\psi') = 0$

再作ψ'的x变通ψ，使$\psi(x)=\varphi(x)$. ψ和φ在除y之外的变元指派上都是一致的，所以ψ是φ的y变通。前面的(3)式这时仍然成立，于是

$$\begin{aligned} \psi(t) &= \varphi(t) && \text{(由(3))} \\ &= \varphi'(x) && \text{(已知条件)} \\ &= \psi'(x) && (\psi'\text{是}\varphi'\text{的}y\text{变通而}y\neq x) \end{aligned}$$

再由归纳假设及(4)得

$$|q(t)|(\psi) = |q(x)|(\psi') = 0$$

2.3 K的可靠性

由此即得 (ψ是φ的y变通)

$$|\forall y q(t)|(\varphi) = 0 \text{ 即 } |p(t)|(\varphi) = 0$$

到此完成了2)的整个归纳过程。

引理2 K的公理都是有效式。

证明 只用证(K4)、(K5)的有效性：

1) (K4)是有效式。

设项t对$p(x)$中的x自由。为证$\vDash \forall x p(x) \to p(t)$, 任取解释域M及任一$\varphi \in \Phi_M$，并设

$$|\forall x p(x)|(\varphi) = 1$$

这时对于φ的任一x变通φ′，总有$|p(x)|(\varphi') = 1$。现取φ的一个特殊x变通φ′，使其满足$\varphi'(x)=\varphi(t)$；由引理1，

2.3 K的可靠性

$|p(t)|(\varphi) = |p(x)|(\varphi') = 1$，这说明

$$|\forall x p(x) \to p(t)|(\varphi) = 1$$

而上式当$|\forall x p(x)|(\varphi) = 0$时当然是成立的。由于M与φ都是任取的，所以$\forall x p(x) \to p(t)$是有效式。

2) (K5)是有效式。

要证$\vDash \forall x(p \to q) \to (p \to \forall x q)$ (其中x不在p中自由出现)，即证任意解释域M及任一$\varphi \in \Phi_M$，下式成立

$$|\forall x(p \to q) \to (p \to \forall x q)|(\varphi) = 1$$

该式在$|\forall x(p \to q)|(\varphi) = 0$或$|p|(\varphi) = 0$时是明显成立的，所以只要证明当

(5) $|\forall x(p \to q)|(\varphi) = |p|(\varphi) = 1$

时，$|\forall x q|(\varphi) = 1$就可以了。

2.3 K的可靠性

(5) $|\forall x(p\to q)|(\varphi) = |p|(\varphi) = 1$

现设(5)式成立，这时对于φ的任一x变通φ′， 有

(6) $|p\to q|(\varphi') = 1$

再由2.2.3小节命题1可得

(7) $|p|(\varphi') = |p|(\varphi) = 1$

由(6), (7)得$|q|(\varphi') = 1$，进而得$|\forall xq|(\varphi) = 1$。

定理1(K的可靠性) $\Gamma\vdash p \Rightarrow \Gamma\models p$.

证 设有 p从Γ的证明$p_1,\ldots,p_n(=p)$。现对n归纳证明$\Gamma\models p$。

n=1时，若$p\in\Gamma$，则自然有$\Gamma\models p$；若p为公理，由引理2，显然也有$\Gamma\models p$。

n>1时，有以下三种情形：

2.3 K的可靠性

(i) $p\in\Gamma$或p为公理，与n=1的情形相同。

(ii) 若有i,j<n使$p_j=p_i\to p$，则由归纳假设可得$\Gamma\vDash p_i$和$\Gamma\vDash p_i\to p$，再用2.2.4小节命题2得$\Gamma\vDash p$。

(iii) 若$p=\forall x p_i$, i<n，则由归纳假设得$\Gamma\vDash p_i$，再用2.2.4小节命题3得$\Gamma\vDash\forall x p_i$。

推论1(K的无矛盾性) K是无矛盾的，即$\vdash p$与$\vdash\neg p$不可能同时成立。

证 反设有公式p使$\vdash p$与$\vdash\neg p$同时成立，则由K的可靠性定理得$\vDash p$与$\vDash\neg p$。这样，对任一解释域M及任一$\varphi\in\Phi_M$，有

$$|p|(\varphi)=1\text{且}|\neg p|(\varphi)=1$$

但这是不可能的。

2.4 K的完全性

K的完全性指

$$\Gamma \models p \Rightarrow \Gamma \vdash p \quad (\models p \Rightarrow \vdash p)$$

定理1 无矛盾公式集一定有可数集模型。

证 设Γ无矛盾公式集，下面给Γ构造一个可数集模型M。

分六步来进行：

1. 作扩大的谓词演算K^+

取可数个新的个体常元$b_1,b_2,\ldots,b_n,\ldots$，$B=\{b_1,b_2,\ldots,b_n,\ldots\}$与原来的个体常元集$C=\{c_1,c_2,\ldots,c_n,\ldots\}$不相交.

扩大K，以$C\cup B$为新的个体常元集，X、F、R保持不变，得到新的谓词演算记作K^+。K的项集T是K^+的项集T^+的真子集。

2.4 K的完全性

K和K^+的原子公式集分别用Y和Y^+表示，则$Y \subset Y^+$。公式集 $K(Y) \subset K(Y^+)$.

2. 作扩大的无矛盾公式集$\Gamma' \supset \Gamma$

把K^+中所有**只含一个自由变元**的公式(可数个)全部取出排成不重复的一列：

$$p_0(y_0), p_1(y_1), \ldots, p_n(y_n), \ldots$$

其中$y_n(=x_{i_n} \in X)$可以重复出现。

在B中取出一串$b_{i_0}, b_{i_1}, \ldots$, 使之满足：

(i) b_{i_0}不在$p_0(y_0)$中出现,

(ii) n>0时，b_{i_n}不在$p_0(y_0), \ldots, p_n(y_n)$中出现, 且$b_{i_n} \notin \{b_{i_0}, \ldots, b_{i_{n-1}}\}$.

2.4 K的完全性

记

$$r_n = p_n(b_{in}) \rightarrow \forall y_n\, p_n(y_n),$$

并记

$$\Gamma' = \Gamma \cup \{r_0, r_1, r_1, \ldots\}.$$

则Γ′是无矛盾的公式集，因为：若存在K^+中的公式q使$\Gamma' \vdash_{K^+} q$与$\Gamma' \vdash_{K^+} \neg q$同时成立，那么必存在充分大的n使

$$\Gamma \cup \{r_0, \ldots, r_n\} \vdash_{K^+} q \text{及} \neg q.$$

但我们可以对$\{r_0, \ldots, r_n\}$中的公式数归纳证明这是不可能的。

2.4 K的完全性

3. 作Γ′的完备无矛盾扩张Γ*

把K(Y⁺)中的所有闭式排成不重复的一列：

$$p_0^*, p_1^*, p_2^*, \cdots$$

令

$$\Gamma_0 = \Gamma',$$

$$\Gamma_n = \begin{cases} \Gamma_{n-1}, & \text{若}\Gamma_{n-1} \vdash_{K^+} p_{n-1}^* \\ \Gamma_{n-1} \cup \{\neg p_{n-1}^*\}, & \text{若}\Gamma_{n-1} \nvdash_{K^+} p_{n-1}^* \end{cases}$$

显然有

$$\Gamma_0 \subseteq \Gamma_1 \subseteq \Gamma_2 \subseteq \cdots$$

现对n归纳证明Γ_n是无矛盾的。

n=0时，$\Gamma_0 = \Gamma'$已证是无矛盾的。

2.4 K的完全性

n>0时，假设Γ_n有矛盾，即有q使

(1) $\Gamma_n \vdash_{K^+} q$及$\neg q$

由归纳假设，Γ_{n-1}无矛盾，所以$\Gamma_n \neq \Gamma_{n-1}$。于是从$\Gamma_n$的定义知

(2) $\Gamma_{n-1} \nvdash_{K^+} p_{n-1}^*$

且

(3) $\Gamma_n = \Gamma_{n-1} \cup \{\neg p_{n-1}^*\}$

将(3)式右边代入(1)，用反证律可得(p_{n-1}^*是闭式)

$$\Gamma_{n-1} \vdash_{K^+} p_{n-1}^*$$

这与(2)式矛盾。由此证明了Γ_n的无矛盾性。

作

$$\Gamma^* = \bigcup_{n=0}^{\infty} \Gamma_n$$

2.4 K的完全性

Γ*也是无矛盾的。这是因为若$\Gamma^* \vdash q, \neg q$. 则必然存在某个充分大的n使$\Gamma_n \vdash_{K^+} q, \neg q$； 与$\Gamma_n$的无矛盾性冲突。

Γ*还是完备的，即对K^+中的任一闭式 p_k^*, $\Gamma^* \vdash_{K^+} p_k^*$与$\Gamma^* \vdash_{K^+} \neg p_k^*$二者必居其一。实际上，

$$\Gamma^* \nvdash_{K^+} p_k^* \Rightarrow \Gamma_k \nvdash_{K^+} p_k^*$$
$$\Rightarrow \Gamma_{k+1} = \Gamma_k \cup \{\neg p_k^*\}$$
$$\Rightarrow \Gamma_{k+1} \vdash_{K^+} \neg p_k^*$$
$$\Rightarrow \Gamma^* \vdash_{K^+} \neg p_k^*$$

这就证明了Γ*是Γ′的完备无矛盾扩张。

2.4 K的完全性

4. 作K^+的解释域M

令

M = K^+的所有闭项组成的集，

M是由B∪C生成的以F为运算集的代数系统，是可数集。

首先，让M成为K^+的解释域：令$\overline{b_i}=b_i$, $\overline{c_i}=c_i$, $\overline{f_i^n}=f_i^n$，即都解释为自身。再规定M中与的n元谓词R_i^n对应的n元关系$\overline{R_i^n}$如下：

对任意闭项$t_1,\ldots,t_n \in M$,

当$\Gamma^* \vdash_{K^+} R_i^n(t_1,\ldots,t_n)$时，令$(t_1,\ldots,t_n) \in \overline{R_i^n}$;

当$\Gamma^* \vdash_{K^+} \neg R_i^n(t_1,\ldots,t_n)$时，令$(t_1,\ldots,t_n) \notin \overline{R_i^n}$.

Γ^*的完备无矛盾性保证了$\overline{R_i^n}$的定义是合理的。

2.4 K的完全性

M自然也是K的解释域。

同时，M具有如下性质：对K^+的任何项解释φ^+和任一闭项$t(t\in M)$，总有$\bar{t} = \varphi^+(t)= t$, 这是因为常元$b_i$, c_i与运算符f_i^n都解释为自己。

下证M是Γ的模型。

5. 命题 *

$$(*)\quad \Gamma^* \vdash_{K^+} q \quad \Leftrightarrow \quad |q|_M=1.$$

q是K^+的任一闭式。

现对闭式q在$K(Y^+)$中的层次数k归纳证明 (*)。

2.4 K的完全性

k=0时，q是原子公式，设q= $R_i^n(t_1,\ldots,t_n)$, 其中每个t_i是闭项。对任取的项解释φ^+，因t_i是闭项，故$\varphi^+(t_i)= t_i$. 于是

$$\Gamma^* \vdash_{K^+} q \quad \Leftrightarrow \quad (t_1,\ldots,t_n) \in \overline{R_i^n}$$

$$\Leftrightarrow \quad (\varphi^+(t_i),\ldots, \varphi^+(t_i)) \in \overline{R_i^n}$$

$$\Leftrightarrow \quad |R_i^n(t_1,\ldots,t_n)|(\varphi^+) = 1$$

因φ^+是任取的，所以

$$\Gamma^* \vdash_{K^+} q \quad \Leftrightarrow \quad |R_i^n(t_1,\ldots,t_n)|_M = 1，\text{即 } |q|_M=1.$$

k>0时，分四种情形进行讨论：

情形1　q=¬r，其中r也是闭式，此时有

2.4 K的完全性

$\Gamma^* \vdash_{K^+} \neg r \Leftrightarrow \Gamma^* \nvdash_{K^+} r$ (Γ*完备无矛盾)

$\Leftrightarrow |r|_M=0$ (由归纳假设)

$\Leftrightarrow |\neg r|_M=1$

情形2 $q = r \to s$，其中r,s都是闭式，此时有

$\Gamma^* \nvdash_{K^+} r \to s \Leftrightarrow \Gamma^* \vdash_{K^+} \neg(r \to s)$ (Γ*完备无矛盾)

$\Leftrightarrow \Gamma^* \vdash_{K^+} r$ 且 $\Gamma^* \vdash_{K^+} \neg s$ (用永真式)

$\Leftrightarrow \Gamma^* \vdash_{K^+} r$ 且 $\Gamma^* \nvdash_{K^+} s$

(Γ*完备、无矛盾)

$\Leftrightarrow |r|_M=1$ 且 $|s|_M=0$ (由归纳假设)

$\Leftrightarrow |r \to s|_M=0$

2.4 K的完全性

情形3 $q = \forall x\, r$且r是闭式，此时有

$$\Gamma^* \vdash_{K^+} \forall x\, r \Leftrightarrow \Gamma^* \vdash_{K^+} r \quad ((K4), MP及Gen)$$

$$\Leftrightarrow |r|_M = 1 \quad (由归纳假设)$$

$$\Leftrightarrow |\forall x\, r|_M = 1$$

情形4 $q = \forall x\, r$，其中x在r中自由出现。因q是闭式，故$r(x)$只含有一个自由出现的变元x，此时$r(x)$必在第2步中列出的公式中出现。设$r(x)=p_m(y_m)$, $y_m = x$. 于是$q = \forall y_m\, p_m(y_m)$，下面对(*)的两个方向证明如下

($\Rightarrow$) 反设

(4) $\Gamma^* \vdash_{K^+} \forall y_m\, p_m(y_m)$, 但

(5) $|\forall y_m\, p_m(y_m)|_M = 0$

由(5)知，存在项解释φ^+使

2.4 K的完全性

(6) $|p_m(y_m)|(\varphi^+)=0$

记$\varphi^+(y_m)$为t，由$t\in M \Rightarrow t$是K^+的闭项，所以

$$\varphi^+(t) = t = \varphi^+(y_m)$$

由上一节引理1-2(φ^+是自己的y_m变通)进一步得

$$|p_m(t)|(\varphi^+)= |p_m(y_m)|(\varphi^+)$$

$p_m(t)$是闭式，由上式及(6)又得

(7) $|p_m(t)|_M=0$

另一方面，由(4)可得$\Gamma^* \vdash_{K^+} p_m(t)$ (用(K4)及MP)，再结合归纳假设得$|p_m(t)|_M=1$，与(7)矛盾。

(⇐) 设 $|\forall y_m\ p_m(y_m)|_M=1$.

因为公理都是有效式，故

2.4 K的完全性

$$|\forall y_m\, p_m(y_m) \to p_m(b_{i_m})|_M=1$$

这样由2.2.3小节命题5可得$|p_m(b_{i_m})|_M=1$。由归纳假设，有

(8) $\Gamma^* \vdash_{K^+} p_m(b_{i_m})$

由2、3中几个公式集的定义，$r_m \in \Gamma^* \Rightarrow \Gamma^* \vdash_{K^+} r_m$，即

$$\Gamma^* \vdash_{K^+} p_m(b_{i_m}) \to \forall y_m\, p_m(y_m)$$

此式结合(8)即得

$$\Gamma^* \vdash_{K^+} \forall y_m\, p_m(y_m)$$

至此完成了命题(*)的归纳过程。

6. 整个证明的完成

任取 $p \in \Gamma \subset \Gamma^*$，当然有$\Gamma^* \vdash_{K^+} p$。设p′是p的全称闭式，

2.4 K的完全性

6. 整个证明的完成

任取 $p \in \Gamma \subset \Gamma^*$，当然有$\Gamma^* \vdash_{K^+} p$。设$p'$是p的全称闭式，则也有$\Gamma^* \vdash_{K^+} p'$，由命题(*)得到$|p'|_M=1$。由此及2.2.3命题3最后得到$|p|_M=1$。这说明M是p的(可数集)模型。

定理2(K的完全性) $\Gamma \models p \Rightarrow \Gamma \vdash p$

证 反设 $\Gamma \nvdash p$.设p'是p的全称闭式，则$\Gamma \cup \{\neg p'\}$是无矛盾的，否则由反证律得$\Gamma \vdash p'$，从而 $\Gamma \vdash p$成立。由定理1知$\Gamma \cup \{\neg p'\}$一定有模型，设M是$\Gamma \cup \{\neg p'\}$的模型，于是 $|\neg p'|_M=1 \Rightarrow |p'|_M=0$. 由此可知$\Gamma \not\models p'$，再由2.2.4命题4得$\Gamma \not\models p$，与已知条件矛盾。

安全C语言串行程序的验证系统介绍

报告人：陈意云
中国科大计算机学院，中科国创高可信软件公司
0551-63607043, yiyun@ustc.edu.cn
http://staff.ustc.edu.cn/~yiyun/

报 告 提 纲

1. 程序验证与Hoare逻辑
   - Hoare三元式、赋值公理与推理规则
2. 演绎推理程序验证的基本概念
   - 基于产生验证条件的自上而下演算的验证
     - 实例1：累加实现两个自然数的相乘
3. 科创程序验证系统的技术特色
   - 操作易变数据结构的程序的验证
     - 实例2：有序单向链表的插入函数
4. 科创验证学习平台使用入门

程序验证与Hoare 逻 辑

- 程序验证
  - 用数学的方法来证明程序的性质
- 演绎验证
  - 用演绎推理的逻辑方法来证明程序具备所期望的性质
  - 就所期望的性质而言，演绎验证可保证程序无错
- 程序逻辑
  - 对程序进行推理的逻辑。**Hoare逻辑是一种程序逻辑**
- **Hoare逻辑推理规则**
  - 基于简单编程语言（赋值、顺序、条件和循环等语句）
  - **C. A. R. Hoare. "An axiomatic basis for computer programming“ Volume 12 / Number 10 / October, 1969 Comm. of the ACM 576~583**

Hoare逻辑推理规则

- 程序状态的逻辑表示
  - 语法形式：**{*P*} S {*Q*}**，称为 **Hoare三元式**

    (1) **S是代码段**，遵循相应编程语言的语法

    (2) ***P*和*Q*是关于程序状态**（变量到值的映射）**的断言**

    ***P*/*Q*是S的前/后断言。断言是谓词逻辑的合式公式**

    (3) 例： $\{x == 1 \wedge y < 5\}\ x = x + 1\ \{x == 2 \wedge y < 5\}$
  - **{*P*} S {*Q*}的含义：**

    在满足断言 ***P*** 的状态下执行代码 **S**，若执行终止，则终止状态满足断言 ***Q***

例：$\{x > 1 \wedge y < 5\}\ x = x + 1\ \{x > 0 \wedge y < 5\}$ 成立

$\{x > 2 \wedge y < 5\} \Rightarrow \{x > 0 \wedge y < 5\}$

Hoare 逻辑推理规则

- 赋值公理
  - 形式：$\{Q[E/x]\}\ x = E\ \{Q\}$

    $Q[E/x]$表示Q中出现的变量x用表达式 E 代换
  - 例：$\{x + 1 > 6\}\ x = x + 1\ \{x > 6\}$ 是赋值公理的实例
  - 特点： $x + 1 > 6$ （即$x > 5$）是语句$x = x+1$和后断言$x > 6$的最弱前断言

    (1) $x > 5.1$可作为前断言，因为有 $x > 5.1 \Rightarrow x > 5$

    (2) $x > 4.9$不可作为前断言，因为 $x > 4.9 \Rightarrow x > 5$不成立
- 逆向推理
  - Hoare的赋值公理采用的是逆向推理的演算，即由代码段S和后断言Q，根据赋值公理和推理规则推导出前断言P

Hoare 逻辑推理规则

- 正向推理
  - 形式：$\{P\}\ x = E\ \{\exists x'.P[x'/x]\ \&\&\ x == E[x'/x]\}$
    后断言Q由2部分的构成：存在一个表达式x'，将P 中出现的变量x用 x′ 代换，合取由代码段（如赋值语句）构成的断言x == E，并将E中出现的变量x也用 x′ 代换
  - 特点：正向推理演算得到的是最强后断言
  - 例：{x > 5} x = x +1 {Q}

    P = {x > 5} , x′ = x-1，E = {x + 1}

    Q = {x-1 > 5 && x == x-1+1}

    = {x > 6 && x==x} ={x > 6}

    ∴ {x > 5} x = x +1 {x > 6}

(1) x > 5.1可作为后断言，因为有 x > 6 ⇒ x > 5.1 成立

(2) x > 6.1不可作为后断言，因为 x > 6 ⇒ x > 6.1 不成立

Hoare 逻辑推理规则

- 结构化语句的推理规则
  - 顺序语句

$$\frac{\{P\}\ S_1\ \{R\} \qquad \{R\}\ S_2\ \{Q\}}{\{P\}\ S_1;\ S_2\ \{Q\}}$$

  - 条件语句（也可用其它形式表示，E为条件）

$$\frac{\{P \wedge E\}\ S_1\ \{Q\} \qquad \{P \wedge \neg E\}\ S_2\ \{Q\}}{\{P\}\ \text{if } E \text{ then } S_1 \text{ else } S_2\ \{Q\}}$$

  - 插曲：推论规则

$$\frac{P' \Rightarrow P \quad \{P\}\ S\ \{Q\} \quad Q \Rightarrow Q'}{\{P'\}\ S\ \{Q'\}}$$

Hoare 逻辑推理规则

- 结构化语句的推理规则（续）
  - 循环语句

$$\frac{\{I \wedge E\}\ S\ \{I\}}{\{I\}\ \text{while}\ E\ \text{do}\ S\ \{I \wedge \neg E\}}$$

I 为循环不变式

E 为循环条件

  - 例：用自然数加法来完成自然数m和n相乘

```
x = 0; y = 0;
while (y < n) {   // 循环不变式 I：(x == m×y) ∧ (y ≤ n)
      x = x + m; y = y + 1;   // 语句 S
} // x == m × n
```

- 演算得到语句*S*和后断言*I*的最弱前条件：

$$x+m == m\times(y+1) \wedge y+1 \leq n$$

Hoare逻辑推理规则

- 结构化语句的推理规则（续）
  - 循环语句

$$\frac{\{I \wedge E\}\ S\ \{I\}}{\{I\}\ \text{while}\ E\ \text{do}\ S\ \{I \wedge \neg E\}}$$

I 被称为循环不变式

*E*为循环条件

  - 例：用自然数加法来完成自然数m和n相乘

```
x = 0; y = 0;
while (y < n) {   //循环不变式：(x == m×y) ∧ (y ≤ n)
      x = x + m; y = y + 1;
} // x == m × n
```

- 证明 I ∧ E ⇒ 语句S和后断言I的最弱前条件：

$$(x == m \times y \wedge y \leq n \wedge y < n) \Rightarrow (x+m == m \times (y+1) \wedge y+1 \leq n)$$

报 告 提 纲

1. 程序验证与Hoare逻辑
2. 基于演绎推理进行程序验证的基本概念
   - 基于产生验证条件的自上而下演算的验证
     - 实例1：累加实现两个自然数的相乘
3. 科创程序验证系统的技术特色
   - 操作易变数据结构的程序的验证
     - 实例2：有序单向链表的插入函数
4. 科创验证学习平台使用入门

基于演绎推理的程序验证

- 原理
  - 程序员提供程序标注
  - 验证器基于Hoare 逻辑进行演算推理
  - 在关键程序点（如循环出入口等）产生验证条件
  - 调用定理证明器证明这些验证条件是否满足
  - 如果所有程序点的验证条件都得证，则认为程序是正确的
- 实现
  - 以函数为单位，从函数协议的前件开始，自上而下进行演算推导
  - 在循环入出口、函数调用和函数结束等程序点自动生成验证条件
  - 所有验证条件的可满足性均交由定理证明器验证
  - 对数值溢出、数据区访问越界、除数为0、空指针访问和内存泄漏等程序中可能的缺陷，系统默认会进行验证、报错

实例1：加运算实现乘法的函数

```
// 通过循环累加被乘数m实现m*n的乘法运算
int mult(const int m, const int n) {
    int x, y;
    x = 0;

    y = 0;
    // 验证条件1：循环入口处
    while (y < n) {

        x = x + m;

        y = y + 1;
    // 验证条件2：循环体结束
    }
    return x;    // 验证条件3：函数结束/返回
}
```

// 本函数的验证会产生3个验证条件，即与循环迭代计算有关的循环入口、循环体结束，和函数结束返回处。

实例1：加运算实现乘法的函数

```
/*@ requires 0 <= n < 5000 && 0 <= m < 5000; //函数协议：前件
      ensures \result == m * n; */ // 函数协议：后件
int mult(const int m, const int n) {  // 给定n和m的上界是为了回避计算溢出
    int x, y; // 橙色表示自上而下的演算产生的当前程序点断言
    0 <= n < 5000 && 0 <= m <5000
    x = 0;    // 为变量x生成一个临时变量，%1x。用于记录对应变量的赋值前的值
    0 <= n < 5000 && 0 <= m < 5000 && x == 0
    y = 0;    // 为变量y生成临时变量，%1y
    0 <= n < 5000 && 0 <= m < 5000 && x == 0 && y == 0
    while (y < n) {
            // 程序点断言暂略

        x = x + m; // 程序点断言暂略，为x生成新的临时变量，%2x
        y = y + 1;  // 程序点断言暂略，为y生成新的临时变量，%2y
    }
    return x;
}
```

实例1：加运算实现乘法的函数

```
    y = 0;
    0 <= n < 5000 && 0 <= m < 5000 && x == 0 && y == 0
/*@ loop invariant
        0 <= m < 5000 && 0 <= n < 5000 &&   // 来自函数前件
        0 <= y  && y <= n && x == m * y;  // 循环中的性质
*/
    while (y < n) {

        x = x + m;

        y = y + 1;

    }
    return x;
}
```

第 1 个验证条件：

循环入口程序点断言蕴含循环不变式

```
0 <= n < 5000 && 0 <= m < 5000 &&
x == 0 && y == 0
```

==>

```
0 <= m < 5000 && 0 <= n < 5000 &&
0 <= y && y <= n && x == m * y
```

实例1：加运算实现乘法的函数

```
/*@ loop invariant
      0 <= m < 5000 && 0 <= n < 5000 &&
      0 <= y && y <= n && x == m * y;    */
  while (y < n) {
    // 循环开始点的断言 ==“循环不变式 合取 循环条件”
    0 <= m < 5000 && 0 <= n < 5000 &&
    0 <= y && y <= n && x == m * y && y < n

    x = x + m;

    y = y + 1;

  }
  return x;
}
```

实例1：加运算实现乘法的函数

```
/*@ loop invariant
      0 <= m < 5000 && 0 <= n < 5000 &&
      0 <= y && y <= n && x == m * y;    */
  while (y < n) {
     0 <= m < 5000 && 0 <= n < 5000 &&
     0 <= y && y <= n && x == m * y && y < n
     x = x + m; // x的旧值（赋值前）： %2x
     x == %2x + m && 0 <= m < 5000 && 0 <= n < 5000 &&
     0 <= y && y <= n && %2x == m * y && y < n
     y = y + 1 ; // y的旧值（赋值前）： %2y
     x == %2x + m && 0 <= m < 5000 && 0 <= n < 5000 &&
     0 <= %2y && %2y <= n && %2x == m * %2y &&
     %2y < n && y == %2y + 1
  }
  return x;
}
```

实例1：加运算实现乘法的函数

```
/*@ loop invariant
      0 <= m < 5000 && 0 <= n < 5000 &&
      0 <= y && y <= n && x == m * y;    */
  while (y < n) {// %2x和%2y分别代表赋值前x和y的值
    x = x + m;    y = y + 1;
    x == %2x + m && 0 <= m < 5000 && 0 <= n < 5000 &&
    0 <= %2y && %2y <= n && %2x == m * %2y &&
    %2y < n && y == %2y + 1
  }

  return x;
}
```

第 2 个验证条件：

循环体执行完结的程序点断言蕴含循环不变式

```
x == %2x + m && 0 <= m < 5000 && 0 <= n < 5000 &&
0 <= %2y && %2y <= n && %2x == m * %2y &&
%2y < n && y == %2y + 1
```

==>

```
0 <= m <  5000 && 0 <= n < 5000 &&
0 <= y && y <= n && x == m * y
```

实例1：加运算实现乘法的函数

```
int mult(const int m, const int n) {
    int x, y;
    x = 0;
    y = 0;

    while (y < n) {
        x = x + m;
        y = y + 1;
    }

    return x;
}
```

由自动定理证明器
完成3个验证条件的证明

第3个验证条件：

函数结束点断言蕴含函数协议的后件

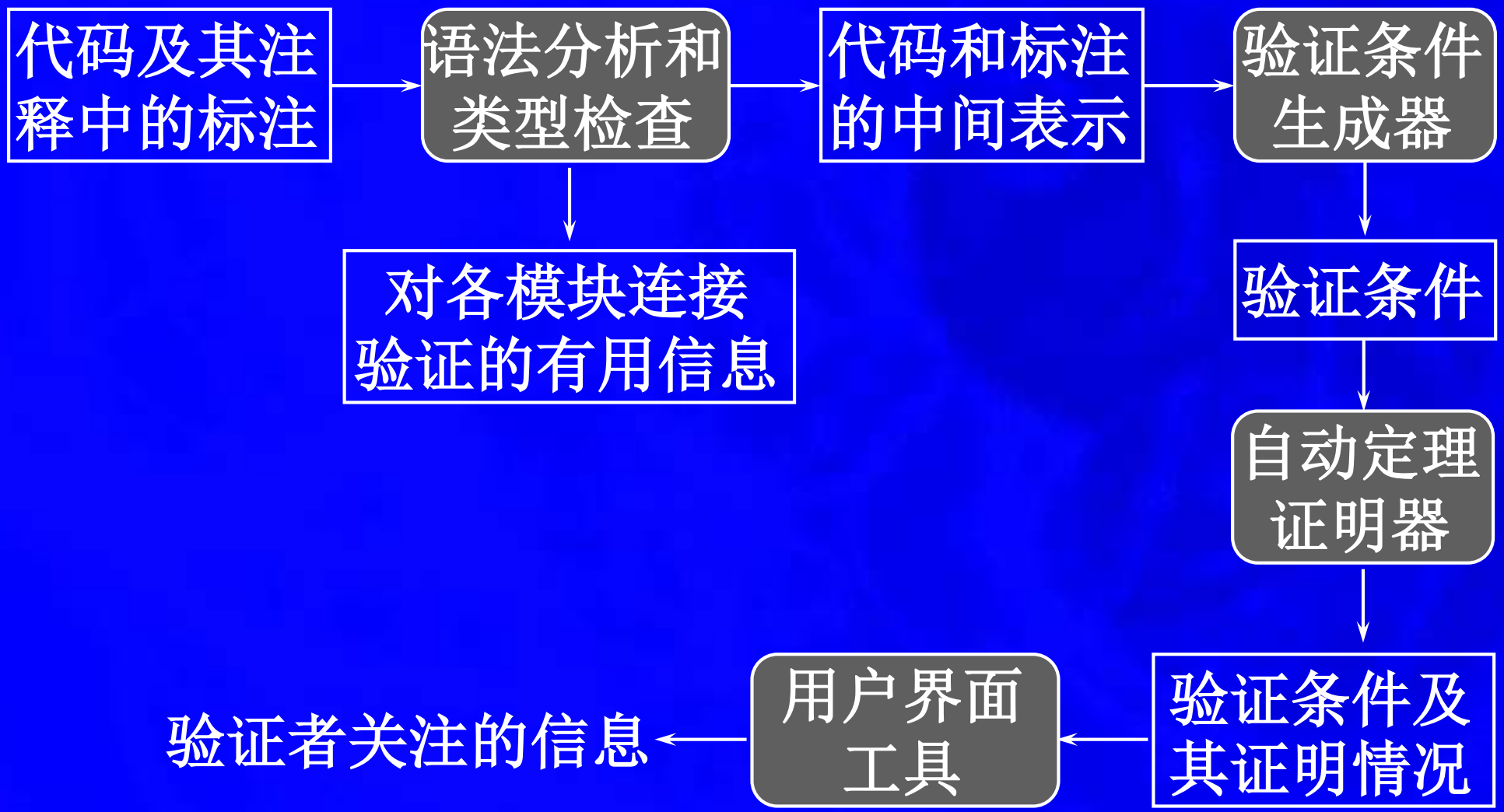
```
x == m * y && $result == x && 0 <= n < 5000 &&
0 <= m< 5000 && 0 <= y && y <= n && y >= n
```

==>

```
$result == m * n
```

基于演绎推理的验证器工作流程

对一个.c文件(称为模块)验证的数据流程图



报 告 提 纲

1. 程序验证与Hoare逻辑
2. 基于演绎推理进行程序验证的基本概念
   - 基于产生验证条件的自上而下演算的验证
     - 实例1：累加实现两个自然数的相乘
3. 科创程序验证系统的技术特色
   - 操作易变数据结构的程序的验证
     - 实例2：有序单向链表的插入函数
4. 科创验证学习平台使用入门

科创程序验证系统的技术特色

- 科创验证器学习平台的技术特色
  - 把最弱前条件演算改成最强后条件演算，以符合程序员的推理习惯，满足验证需穷尽所有执行路径的要求
  - 克服Hoare逻辑赋值公理不能用于有别名的情况
  - 能验证操作单向链表和二叉树的程序，并避免使用难以理解的分离逻辑
  - 进一步拓展到能验证双向链表和循环双向链表的程序，避开了它们不能抽象为代数数据类型的障碍
- 举例：有序单向链表的插入
  - 介绍对操作易变数据结构程序的验证
  - 程序员用符号断言描述形状图，系统依据描述构造形状图

形状图逻辑的主要特点

- **Hoare逻辑三元式: {*Q*} S {*Q′*}，{*Q*}和{*Q′*}是符号断言**
- **用形状图逻辑扩展后的Hoare逻辑三元式:**

$$\{G \wedge Q\}\ S\ \{G' \wedge Q'\}$$

1. *G*和*Q*分别是形状图和符号断言，形状图是堆指针断言的图形表示

2. 把{*G* } S {*G′*}单独可看成形状图逻辑的三元式

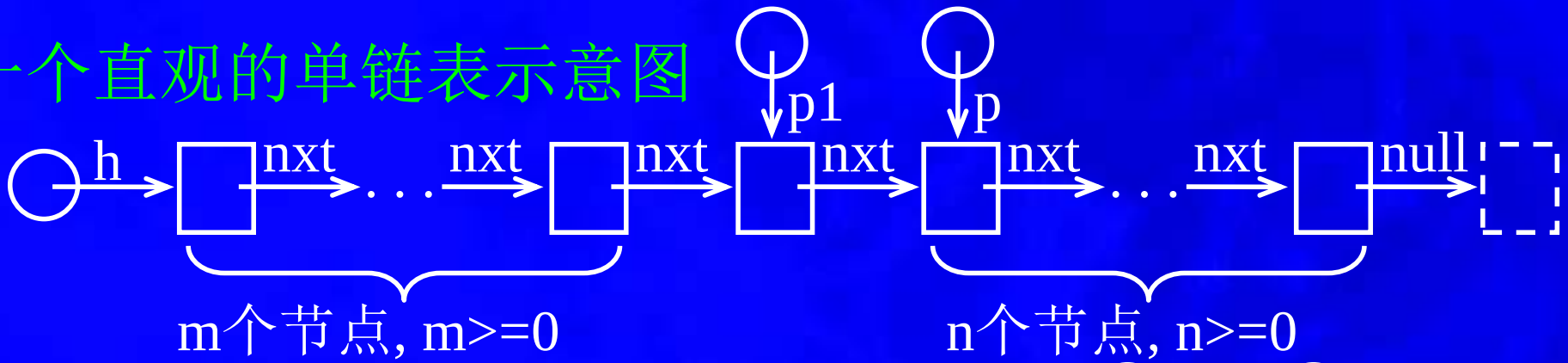
3. 形状图逻辑描述{*G* } S {*G′*}这样的公式之间的推理规则

- **安全C语言程序的推理，使用扩展后的*VC*演算**

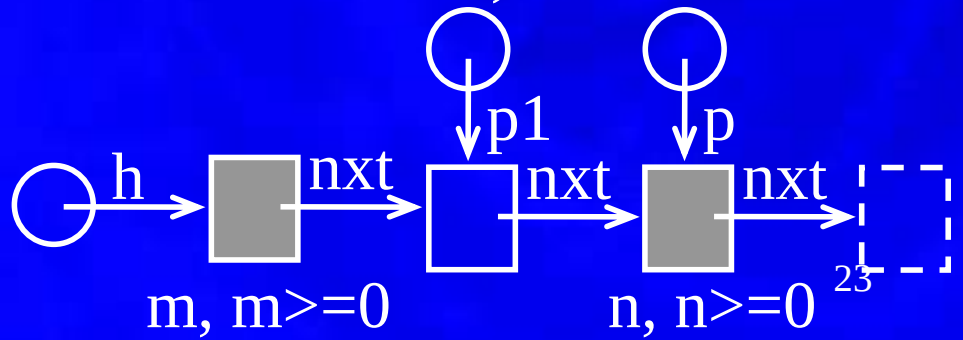
形 状 图

- 形状图的语法
  - 描述静态声明的堆指针和动态分配的结构体中域指针的指向的一种有向图
  - 能准确地表达指针有效性和指针之间的相等关系
  - 可直接作为指针断言

一个直观的单链表示意图



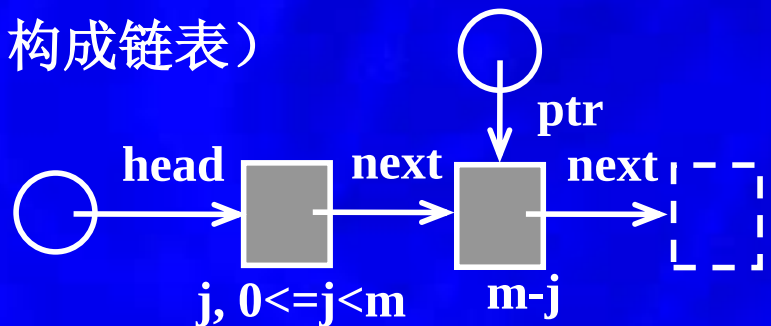
用形状图浓缩表示为



单向链表与它的表段

- 单向链表需要看成由两部分组成
  - 在函数入口，允许外来指针指向链表中某个节点
    - 在函数入口，**head**指向完整的链表
    - 允许有外来的指针(如**ptr**)指向链表中某个节点
  - 在循环代码的迭代计算过程中，遍历链表的指针如下前进
    - 随着遍历节点数**j**增大，左右两边浓缩节点代表的节点数也随之变化
    - 在遍历过程中，链表被分成两部分：逐步增加的已遍历的节点（构成表段）和逐步缩短的尚未遍历链表（构成链表）

// 程序员用符号断言描述形状图，
系统依据描述构造形状图



实例2：有序单向链表的插入函数

- 有序单向链表和表段的归纳（谓词）定义

```
/*@   // 有序单向链表：分成三种情况从右向左进行归纳
inductive sorted_list(Node* p) =
    p == \null ||
    p != \null && p->next == \null ||
    p != \null && p->next != \null &&
          p->data <= p->next->data && sorted_list(p->next);
// 有序单向链表表段：分成二种情况从右向左进行归纳
inductive sorted_seg(Node *p, Node *q) =
    p == q && p != \null ||
    p != q && p != \null && p->next != \null &&
          p->data <= p->next->data && sorted_seg(p->next, q);
*/
```

```
typedef struct node {//节点类型
    struct node * next;
    int data;
} Node;//@ shape next : list;
```

实例2：有序单向链表的插入函数

- 有序单向链表中有关表段的引理
  - 表段的定义：从右向左归纳
    - 左边节点+右边表段，得到增加一个节点的表段
  - 迭代计算时链表的逐点访问：从左向右归纳
    - 左边表段+右边节点，得到增加一个节点的表段
  - 逻辑定义与程序执行的方向不一致导致需添加引理

```
/*@ lemma property1:  // 左边表段 + 右边节点, 得增一个点表段
      \forall Node *p, Node *q. sorted_seg(p, q) &&
                q->next != \null && q->data <= q->next->data
    ==>
      sorted_seg(p, q->next);
*/
```

实例2：有序单向链表的插入函数

- 有序单向链表中有关表段的引理
  - 表段的定义：从右向左归纳
    - 左边节点+右边表段，得到增加一个节点的表段
  - 迭代计算时链表的逐点访问：从左向右归纳
    - 左边表段+右边节点，得到增加一个节点的表段
  - 方向不一致导致需要引理

```
/*@ lemma property2:  // 左边表段 + 右边链表，构成较长链表
      \forall Node *p, Node *q.
                sorted_seg(p, q) && sorted_list(q)
  ==>
      sorted_list(p);*/
```

实例2：有序单向链表的插入函数

- 函数概述

```
Node* listInsert(Node* head, const int data, const int m) {
   Node *ptr, *ptr1, *p;     //@ ghost int j;  // j是幽灵变量
   p = (Node*)malloc(sizeof(Node));  if (p == NULL) {exit(1);}
   p->data = data; p->next = NULL;

   if (head == NULL) {head = p;}        // 生成仅一个元素的表
   else if (p->data <= head->data){p->next = head; head = p;} //新节点插入在表头
   else {    ptr1 = head; ptr = head->next; //@ ghost int j = 0;

            while ((ptr != NULL) && (ptr->data < p->data)) {
               ptr1 = ptr; ptr = ptr->next; //@ ghost j = j + 1;
            }
            p->next = ptr1->next;  ptr1->next = p;
   }
   return head;
}
```

实例：有序单向链表的插入函数

- 函数协议

```
//@ logic Node *oldhead;
/*@ requires sorted_list(head) && \length(head, next) == m &&
             oldhead == head && m > 0;
    assigns *oldhead;
    exits \exit_status == 1;
    ensures   sorted_list(\result) && \length(\result, next) == m+1 &&
            (   oldhead == \result && m > 0    || // 插入在表中或表尾
                oldhead == \null && m == 0     || // 单节点的表
                oldhead == \result->(next:1) && m > 0 // 插入在表头
            );
*/
Node* listInsert(Node* head, int data, const int m);
```

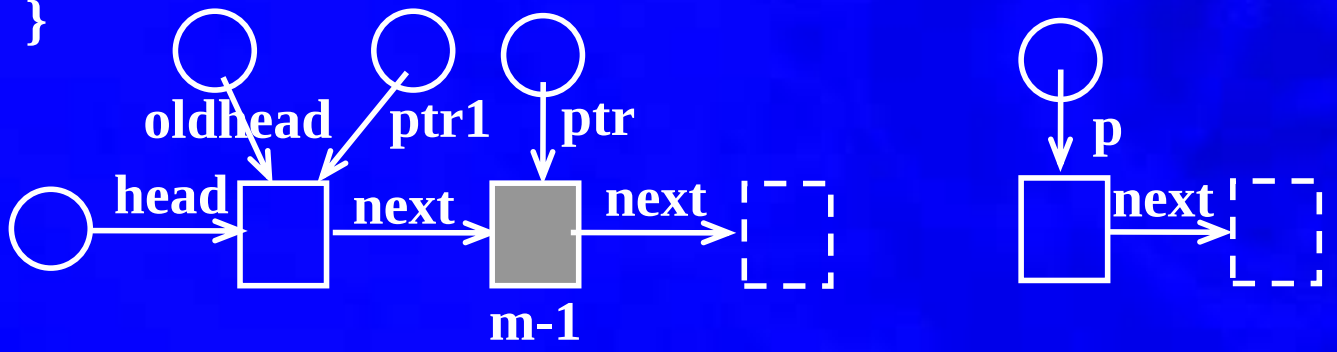
  - oldhead是逻辑变量, 用来指明对应形参head的实参指在结果链表的什么位置。形参m表示链表长度

实例2：有序单向链表的插入函数

循环不变式和循环不变形状图

在while循环语句之前循环不变形状图

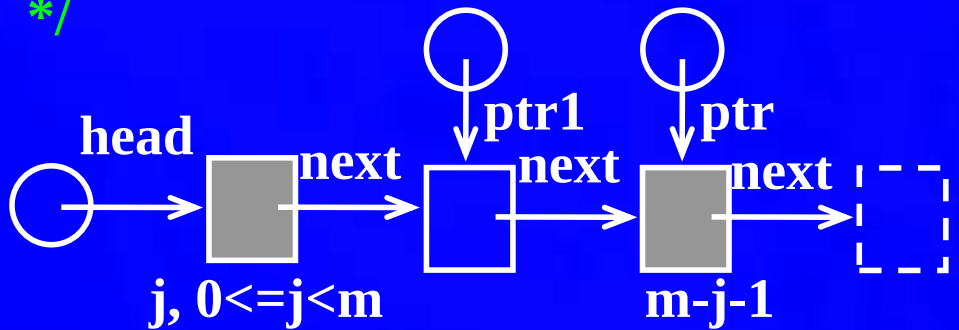
```
p = (Node*)malloc(sizeof(Node));  if (p == NULL) {exit(1);}
p->data = data; p->next = NULL;
... ...
ptr1 = head; ptr = head->next;
while ((ptr != NULL) && (ptr->data < p->data)) {
      ptr1 = ptr; ptr = ptr->next;
      //@ ghost j = j + 1;
}
```

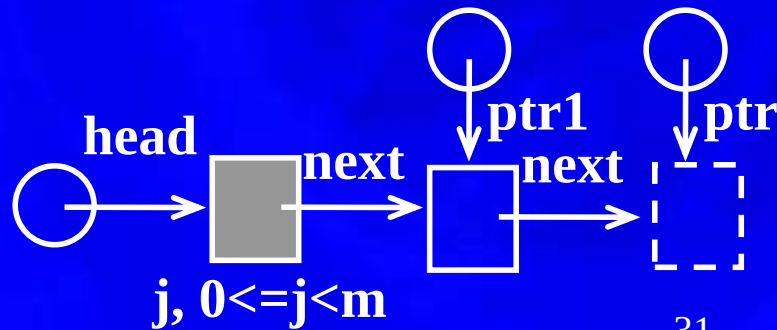


实例2：有序单向链表的插入函数

循环不变式和循环不变形状图

```
/*@ loop invariant          // 分成插在表中和表尾两种情况
   (ptr != \null && ptr==ptr1->next && ptr1->data <= ptr->data  &&
      sorted_list(ptr) && \length(ptr, next) == m-j-1 //插在表中
  ||
    ptr == \null && ptr1->next == \null && sorted_list(ptr1) &&
      \length(ptr1, next) == m-j  // 插在表尾
   )
   && oldhead == head && sorted_seg(head, ptr1) &&
    ptr1==head->(next:j) && ptr1->data < p->data &&
        \list(p) && \length(p, next) == 1 && m > 0 && 0 <= j < m;
 */
```

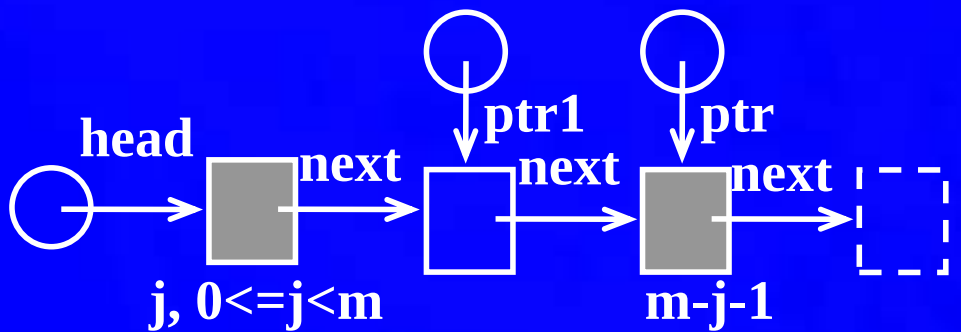


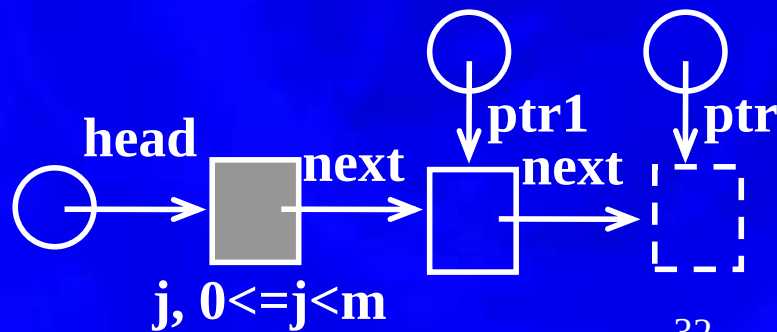


实例2：有序单向链表的插入函数

循环操作与循环不变式和循环不变形状图变化的对应

- 循环体：**ptr1 = ptr;　ptr = ptr->next;　//@ ghost j = j + 1;**
- 循环体每迭代一次，**ptr1**和**ptr**前进一步，表段 **\list_seg(head, ptr1)** 和链表 **sorted_list(ptr)** 也随着分别增加和减少一个节点，引起循环不变形状图和循环不变式同步变化。即循环不变式中的逻辑谓词在迭代计算中变动其囊括的节点数 **j**。





安全C语言串行程序验证系统小结

- 小结
  - 讲座通过二个实例介绍了基于演绎推理的程序验证的基本概念和科创验证系统的技术特色，并简单说明了科创验证学习平台的使用
  - 对于学习和了解基于演绎推理的安全C语言串行程序验证系统来说，这只是一个非常初步的介绍
  - 有了这个开端之后，对基于演绎推理的程序验证感兴趣者，可以通过多阅读并理解验证系统学习平台提供的实例，参考这些实例，动手写出自己的验证程序实例，逐步提高对程序验证的理解。通过学习，一名程序员完全可以成为程序验证方面的熟练技术人员

报 告 提 纲

1. 程序验证与Hoare逻辑
2. 基于演绎推理进行程序验证的基本概念
   - 基于产生验证条件的自上而下演算的验证
     - 实例1：累加实现两个自然数的相乘
3. 科创程序验证系统的技术特色
   - 操作易变数据结构的程序的验证
     - 实例2：有序单向链表的插入函数
4. 科创验证学习平台使用入门

Thank You

www.kcv4c.com

科创验证学习平台

形式化方法与形式验证

- **形式化方法**
  - 是基于严格的数学基础，对计算机硬件和软件系统进行描述（形式规约）、开发和验证的技术
  - 这个数学基础建立在形式语言、语义和推理证明三位一体的形式逻辑之上
  - 在软件成为社会基础设施的当今时代，形式化方法将与人工智能、网络空间安全、量子计算、生物计算等领域和方向交叉融合，得到更广泛的应用
- **形式验证**
  - 形式验证是证明不同形式规约之间需要满足的正确性需求的逻辑关系
  - 形式化开发被称为是构造即正确的开发，是通过构造、证明形式规约之间的等价转换和精化关系，并逐步精化，开发出满足需求的系统的方法

高可信软件
High-Confidence Software

高可信软件 是指可靠和安全标准极高的软件

- 可靠安全性(safety) 是指软件具有设计要求的功能，在运行时不引起危险、灾难的能力
- 保密安全性(security) 是指软件具有对数据和信息提供保密性、完整性、可用性、和真实性的保障能力
- 程序的正确性 是指程序具有用户所期望的性质，安全、可靠
- 软件质量保障手段 功能测试、静态分析和形式验证