●普通高等学校“十一五”规划教材●

Shuli Luoji

# 数理逻辑

（第2版）

汪芳庭　编著

中国科学技术大学出版社

普通高等学校“十一五”规划教材

Shuli Luoji

# 数理逻辑

（第2版）

汪芳庭　编著

中国科学技术大学出版社

## 内容简介

本书内容分两部分：第一部分属数理逻辑基础，包含命题演算与谓词演算的基本知识。第二部分为形式算术与 Gödel 不完备性定理。

本书对 Gödel 第一不完备性定理、Gödel-Rosser 定理、Tarski 定理及形式算术的不可判定性定理等都提供了完整的证明。结合对 Church 论题与 Turing 论题的介绍，对这些定理的意义进行了讨论。书中还提出了 Gödel 第二不完备性定理的一种易证形式。

本书可用作计算机专业研究生或高年级本科生教材，并可供数学、哲学、逻辑等专业研究及教学人员参考。

**图书在版编目(CIP)数据**

数理逻辑/汪芳庭编著．—2 版．—合肥：中国科学技术大学出版社，2010.9
ISBN 978-7-312-02708-6

Ⅰ．数…　Ⅱ．汪…　Ⅲ．数理逻辑—研究生—教材　Ⅳ．O141

中国版本图书馆 CIP 数据核字(2010)第 152563 号

**出版**　中国科学技术大学出版社
安徽省合肥市金寨路 96 号，230026
网址：http://press.ustc.edu.cn
**印刷**　合肥现代印务有限公司
**发行**　中国科学技术大学出版社
**经销**　全国新华书店
**开本**　710 mm×960 mm　1/16
**印张**　13.5
**字数**　272 千
**版次**　1990 年 9 月第 1 版　2010 年 9 月第 2 版
**印次**　2010 年 9 月第 2 次印刷
**定价**　22.00 元

# 再 版 前 言

这次修改, 全面仔细, 但全书的框架与主要内容均无太大变动. 前两章 (命题、谓词演算) 突出了基本内容, 比原来的更有层次. 读者若以 Gödel 不完备性定理为主要目标, 则可专注这两个演算的建立及各自的可靠性、完全性, 略去其他课题 (包括几处所附材料) 后进入第 3 章.

在一些不同场合, 曾多次听见如下 (或类似的) 说法: 按 Gödel 定理, 数学中有不可证明的真命题. 这种似是而非的说法, 属对定理的误读. Gödel 不完备性定理是对 20 世纪 Hilbert 的形式主义学派研究规划的否定. 这种否定, 从人类数学思维的创造性本质来看, 更具有积极意义. 该定理揭示了数学思维中特定的形式化方法所带有的局限性. 这种揭示, 并非针对一般的数学思维. 正是该定理所具有的积极意义, 成为 Gödel 本人所持的理性乐观主义的根据之一. 这种乐观主义恰是对 Hilbert 式乐观主义的继承. (关于对不完备性定理意义的讨论, 详见书中 4.1.4 小节及 4.5 节.)

本书作为数理逻辑基础教材，所涉及的形式系统均采用可数语言. 含不可数语言的更一般理论, 通常归属数理逻辑更专门的领域——模型论.

原计划与中国科学技术大学计算机科学与技术学院陈小平教授共同完成这次修订, 但因他承担的教研及其他任务太重, 故未能如愿. 他提出了不少好的意见和建议, 已被采纳.

关于不完备性定理的意义及证明, 曾与秦一明、金钊 (中国科学技术大学数学系 2001 级同学) 进行过多次有益的讨论. 这使本书第二不完备性定理（初版中提出的易证形式）的证明细节有了进一步改进.

舒其望、张卜天及喻良在提供资料信息方面曾对作者给予帮助. 书稿打字由黄岭梅完成.

在此谨向以上各位表示感谢.

汪芳庭

2010.3.29

# 前　言

从 1982 年起，中国科学技术大学计算机系为加强离散数学的教学，单独开设了数理逻辑课，并由我编写了这门课的教材. 该教材几经修改和增补，成了此书.

为了建立数学模型的方便，并考虑到集论知识已越来越普及，本书在元语言中大量使用了集论，以减少非形式的叙述. 所用的集论概念和结论列在预备知识中. 除了集论，还用了一些初等数论及代数知识. 不要求读者事先熟悉这些知识，而是对用到的有关命题给出自足的证明.

命题演算和谓词演算是数理逻辑的基础内容. 本书前两章里作为代数系统分别建立了这两种演算，先介绍语法，再介绍语义，然后证明它们各自的可靠性、完全性定理. 整个第 3 章讨论形式算术，证明了"递归"与"可表示"的等同性，从而为证明不完备性定理作了准备. 在第 4 章里，对 Gödel 第一不完备性定理、Gödel-Rosser 定理、Tarski 定理和形式算术的不可判定性定理都给出了完整的证明. 结合对 Church 论题和 Turing 论题的介绍，对这些定理的意义进行了一些讨论.

由于 Gödel 第二不完备性定理的证明十分复杂，在具有教材性质的逻辑书中介绍这个定理是件值得探索的事情. 作为尝试，本书提出了无矛盾性不可证性定理的一种易证形式.

练习题大都给以提示. 这些练习有助于理解本文内容，一般与后文无直接联系.

高恒珊、张尚水、康宏逵同志曾给予作者热情的鼓励，并对本书初稿提出过不少意见和建议. 中国科学技术大学计算机系陈友君、许胤龙同志在教材编写修改过程中给予作者很大的帮助和支持. 在此向以上各位谨致谢意.

还要感谢中国科学技术大学计算机系的历届同学，他们对本书内容的改进起过重要的作用.

本书不妥之处敬请读者指正.

汪芳庭

1990 年 1 月于中国科学技术大学数学系

# 目录

# 引　言

历史上，首先明确地提出来要用数学方法去研究逻辑推理的人是莱布尼茨 (G. W. Leibniz，1646~1716). 他在 1714 年写的一封信中曾说：“要是我少受干扰，或者我更年轻，或者有青年人来帮助我，我有望作出一种一般代数，用它可将推理的正确性全都化为计算.”

莱布尼茨提出的美好希望能否实现？在什么程度上能够实现？数理逻辑的发展已对此作出了一定程度的回答.

数理逻辑奠基人之一弗雷格 (G. Frege，1848~1925) 认为：“数学的本质就在于，一切能证明的都要证明.”

什么叫数学证明？数理逻辑的一项重要任务就是试图回答这个问题，设法把“证明”这个概念 (与此相关的还有可计算性的概念) 精确化. 我们将讨论精确化所用的方法，考察在这个精确化过程中出现的问题和得出的结论. 所得出的结论中，最重要的就是著名的 Gödel 不完备性定理.

20 世纪初，数学基础领域出现了一场规模空前的学术运动，Gödel 不完备性定理是这场运动的结果之一. 这一定理的建立除对数学基础本身产生了深远影响，还对推动人类计算机时代的到来起过重要的作用. 王浩先生曾在评价哥德尔 (K. Gödel，1906~1978) 的工作时说：“哥德尔的工作与计算机的联系可能要比爱因斯坦的工作与原子弹的联系密切一点.” (参见参考文献 [16]，279 页) 当我们完整地学习了 Gödel 不完备性定理及其证明后，会对此有所认识.

为了达到精确化，数理逻辑在研究推理时要建立数学模型. 命题演算与谓词演算这两种基本的形式系统，就是为研究推理而建立的数学模型. 对形式系统进行研究，必须要用普通的自然语言. 我们把这种自然语言叫做“元语言”，以区别于形式系统的那种形式语言. 于是我们有两种系统：“元系统”与“形式系统”. 比如，形式系统中的“定理”、“证明”等有特定的含义，是我们研究的对象，而研究得到的结论则表现为元数学的定理，这是用元语言给出来的.

在元语言中，我们有时用符号“$\Rightarrow$”表示“蕴涵”，用“$\Leftrightarrow$”表示“当且仅当”. 本书中，等号 ($=$) 仅限于元语言使用；我们的形式语言里，等词采用符号“$\approx$”.

# 0 预备知识

## 0.1 集论初等概念

这里列出在我们的元语言中要用到的一些集论初等概念以及它们的符号表示.

集 $A$ 是集 $B$ 的子集，记作 $A \subseteq B$, 意思是: 凡是 $A$ 的元素都是 $B$ 的元素.

二集相等，意为二集有完全相同的元素:

$$A = B \quad \Leftrightarrow \quad A \subseteq B \text{ 且 } B \subseteq A.$$

集 $A$ 的幂集用 $\mathcal{P}(A)$ 表示，它是由 $A$ 的全体子集所形成的集:

$$\mathcal{P}(A) = \{a \mid a \subseteq A\}.$$

例如，若 $A = \{1, 2, 3\}$, 则

$$\mathcal{P}(A) = \{\{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}, \varnothing\},$$

其中 $\varnothing$ 是空集. $\varnothing$ 是任何集的子集.

集 $A$ 与集 $B$ 的并，指

$$A \cup B = \{x \mid x \in A \text{ 或 } x \in B\}.$$

集 $A$ 与集 $B$ 的交，指

$$A \cap B = \{x \mid x \in A \text{ 且 } x \in B\}.$$

作为集的运算，并和交都满足交换律、结合律和分配律. 以后，我们把有限次的并 $A_1 \cup A_2 \cup \cdots \cup A_n$ 记作 $\bigcup_{i=1}^n A_i$, 把有限次的交 $A_1 \cap A_2 \cap \cdots \cap A_n$ 记作 $\bigcap_{i=1}^n A_i$.

设有一列集 $A_0, A_1, A_2, \cdots, A_n, \cdots$ . 我们记

$$\bigcup_{i \in \mathbf{N}} A_i (= \bigcup_{i=0}^{\infty} A_i) = \{x \mid \text{存在} i \text{使} x \in A_i\},$$

$$\bigcap_{i \in \mathbf{N}} A_i (= \bigcap_{i=0}^{\infty} A_i) = \{x \mid \text{对任意} i \text{都有} x \in A_i\}.$$

集 $B$ 在集 $A$ 中的余集，指

$$A - B = \{x \mid x \in A \text{ 且 } x \notin B\}.$$

集 $A$ 与集 $B$ 的积集，指

$$A \times B = \{(a,b) \mid a \in A, b \in B\}.$$

它由以 $A$ 的元素为第一元素，以 $B$ 的元素为第二元素形成的有序对 $(a,b)$ 的全体所构成. 有序对 $(a,b)$ 的基本性质是

$$(a_1,b_1) = (a_2,b_2) \quad \Rightarrow \quad a_1 = a_2 \text{ 且 } b_1 = b_2.$$

$n$ 个集 $A_1,\cdots,A_n$ 的积集，指

$$\begin{aligned}\prod_{i=1}^{n} A_i &= A_1 \times \cdots \times A_n \\ &= \{(a_1,\cdots,a_n) \mid a_1 \in A_1,\cdots,a_n \in A_n\}.\end{aligned}$$

$n$ 元有序组 $(a_1,\cdots,a_n)$ 具有性质:

$$(a_1,\cdots,a_n) = (b_1,\cdots,b_n) \quad \Rightarrow \quad a_1 = b_1,\cdots,a_n = b_n.$$

用 $A^n$ 表示 $n$ 个 $A$ 的积集 $A \times A \times \cdots \times A$ $(n > 1)$. 规定 $A^0 = \varnothing, A^1 = A$.

若 $R \subseteq A \times B$, 则说 $R$ 是 $A$ 到 $B$ 的关系. 若 $R \subseteq A^n$, 则说 $R$ 是 $A$ 上的 $n$ 元关系. $A$ 上的一元关系就是 $A$ 的子集.

$A$ 上的二元关系 $R(\subseteq A \times A)$ 若具有以下三条性质，就叫做 $A$ 上的等价关系.

1° 自反性: 对任意 $x \in A$, $(x,x) \in R$.

2° 对称性: 对任意 $x,y \in A$,

$$(x,y) \in R \quad \Rightarrow \quad (y,x) \in R.$$

3° 可递性: 对任意 $x,y,z \in A$,

$$(x,y) \in R \text{ 且 } (y,z) \in R \quad \Rightarrow \quad (x,z) \in R.$$

若 $R$ 是 $A$ 上的等价关系，且 $(a,b) \in R$, 则说 $a$ 与 $b$ 等价，记作 $a \sim b$. $A$ 中与 $a(\in A)$ 等价的所有元素形成的集叫做由 $a$ 形成的 $R$ 等价类，记作

$$[a] = \{x \mid x \in A, x \sim a\}.$$

不同的等价类之间没有公共元素，所以 $A$ 上的任何等价关系 $R$ 都确定了 $A$ 的一个分类.

设 $R$ 是 $A$ 上的等价关系，我们把所有 $R$ 等价类的集叫做商集，记作 $A/R$.

设 $f$ 是集 $X$ 到集 $Y$ 的一个关系 (即 $f \subseteq X \times Y$). 如果 $f$ 还满足条件: 对任意 $x \in X$, 有且仅有一个 $y \in Y$ 使 $(x,y) \in f$, 那么我们说 $f$ 是从 $X$ 到 $Y$ 的函数或映射，并写 $f : X \to Y$; 这时若 $(x_0,y_0) \in f$, 则说 $y_0$ 是 $x_0$ 的象，$x_0$ 是 $y_0$ 的原象，并写 $x_0 \mapsto y_0$, 或写 $y_0 = f(x_0)$. $X$ 叫做 $f$ 的定义域. $X$ 中元素在 $Y$ 中的象的全体是 $Y$ 的一个子集，叫做 $f$ 的值域.

如果映射 $f : x \to y$ 的值域就是 $Y$, 则把 $f$ 叫做从 $X$ 到 $Y$ 的满射.

如果映射 $f: X \to Y$ 满足对任意 $x_1, x_2 \in X$ 都有

$$x_1 \neq x_2 \quad \Rightarrow \quad f(x_1) \neq f(x_2),$$

则把 $f$ 叫做从 $X$ 到 $Y$ 的单射.

如果 $f: X \to Y$ 既是单射又是满射，则叫做从 $X$ 到 $Y$ 的双射，此时我们说 $X$ 与 $Y$ 之间存在着一一对应，或者说 $X$ 与 $Y$ 等势，也说 $X$ 与 $Y$ 有相同的基数.

双射 $f$ 的逆映射 $f^{-1}: Y \to X$ 也是双射. ($f^{-1}$ 是 $f$ 的逆映射，意思是 $f^{-1}$ 满足: $f^{-1}(y) = x \quad \Leftrightarrow \quad f(x) = y$.)

双射 $f: X \to Y$ 与双射 $g: Y \to Z$ 的复合映射 $g \circ f: X \to Z$ 也是双射 (复合映射 $g \circ f$ 由下式定义: $g \circ f(x) = g(f(x))$).

集 $A$ 上的 $n$ 元函数 $f: A^n \longrightarrow A$ 叫做 $A$ 上的 $n$ 元运算.

## 0.2 Peano 自然数公理

按照“一切能证明的都要证明”这一想法，证明关于自然数的命题，通常采用下面的 Peano 自然数公理 (公理 1~ 公理 5) 作为出发点.

我们把自然数集 $\mathbf{N}$ 看成是满足以下五条公理的集.

**公理 1** $0 \in \mathbf{N}$.

**公理 2** 若 $x \in \mathbf{N}$, 则 $x$ 有且只有一个后继 $x' \in \mathbf{N}$.

**公理 3** 对任意 $x \in \mathbf{N}, x' \neq 0$.

**公理 4** 对任意 $x_1, x_2 \in \mathbf{N}$, 若 $x_1 \neq x_2$, 则 $x_1' \neq x_2'$.

**公理 5** 设 $M \subseteq \mathbf{N}$. 若 $0 \in M$, 且当 $x \in M$ 时也有 $x' \in M$, 则 $M = \mathbf{N}$.

五条公理中含有两个没有给出定义的概念: 0 和后继. 公理 3 的意思是: 0 是自然数集的开头元素，而不是任何自然数的后继. 公理 4 是说，不同的自然数有不同的后继. 公理 5 就是归纳法原理. 根据公理 5，要证明 $\mathbf{N}$ 的子集 $M$ 与 $\mathbf{N}$ 相等，先证 $0 \in M$, 然后作归纳假设 $x \in M$, 由此来证明 $x' \in M$ 便可. $0'$ 记作 1，$0''$ 记作 2，……

由以上五条公理出发，定义自然数的加法、乘法等运算以及序的概念，便能证明关于自然数性质的一系列结论，例如，“非空的自然数集一定含有该集的最小数”，等等. 在自然数理论的基础上，可进一步建立起有理数、实数和复数的理论. Peano 自然数公理是古典数学的源头. (参见参考文献 [15]，21-26 页)

下面来证明一个常用的结论.

**定理 1 (强归纳法)** 假设与自然数 $n$ 有关的命题 $P(n)$ 满足以下两个条件:

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 $P(n)$ 对所有自然数 $n$ 都成立.

**证** 只要证明集合 $S = \{n \mid P(n)\text{不成立}\}$ 是空集就可以了.

反设 $S \neq \varnothing$, 那么 $S$ 必含有它的最小数. 设 $S$ 的最小数是 $m$. 因 $m \in S$, 故由 $S$ 的定义知 $P(m)$ 不成立. 又已知 $P(0)$ 成立 (条件 1°), 所以必有 $m > 0$. 注意 $m$ 在 $S$ 中是最小的，故当 $k < m$ 时，必有 $k \notin S$, 从而 $P(k)$ 一定成立. 再由已知条件 2° 知 $P(m)$ 成立. 但前面知 $P(m)$ 不成立，矛盾. □

本书中我们把函数 $f : \mathbf{N}^k \to \mathbf{N} (k \in \mathbf{N})$ 叫做 $k$ 元数论函数 (即 $\mathbf{N}$ 上 $k$ 元运算).

设 $m \in \mathbf{N}$ 和二元数论函数 $h$ 为已知，则唯一存在函数 $f : \mathbf{N} \to \mathbf{N}$ 满足

$$f(0) = m,$$

$$f(n+1) = h(n, f(n)).$$

此时说 $f$ 是由常数 $m$ 及函数 $h$ 递归定义得到的函数.（递归定义合理性的证明可参见 [15]，82-86 页）

更一般的递归定义原理是:

任给 $k$ 元数论函数 $g$ 和 $k+2$ 元数论函数 $h$, 唯一存在 $k+1$ 元数论函数 $f$ 满足

$$f(n_1, \cdots, n_k, 0) = g(n_1, \cdots, n_k),$$

$$f(n_1, \cdots, n_k, n+1) = h(n_1, \cdots, n_k, n, f(n_1, \cdots, n_k, n)),$$

其中 $n_1, \cdots, n_k \in \mathbf{N}$.

## 0.3 可 数 集

有限集，是指空集或与 $\{0, 1, \cdots, n\}$ 等势的集 ($n \in \mathbf{N}$).

本书中的可数集，皆指与自然数集 $\mathbf{N}$ 等势的集. 可数集彼此互相等势. 与可数集等势的集也是可数集. 自然数集 $\mathbf{N}$ 当然也是可数集.

设 $A$ 是可数集，即存在双射 $f : \mathbf{N} \to A$. 由此知可数集的特征是: 它的全部元素都可用自然数编号，可一个不漏且不重复地排成一列:

$$a_0, a_1, a_2, \cdots, a_n, \cdots,$$

其中 $a_n = f(n)$.

**命题 1** 可数集的无限子集也是可数集.

**证** 设无限集 $B \subseteq A$，且设 $A$ 是可数集，$A$ 的全部元素不重复地形成一无限序列: $a_0, a_1, a_2, \cdots$. 在这个序列中， $B$ 的全部元素不重复地形成了无限子序列: $a_{n_0}$, $a_{n_1}$, $a_{n_2}, \cdots$, 所以也是可数集. □

**命题 2** 若存在无限集 $B$ 到可数集 $A$ 的单射，则 $B$ 为可数集.

**证** 记 $B$ 到 $A$ 的单射为 $f$, 设 $f$ 的值域为 $C(\subseteq A)$. 因 $f: B \to A$ 是单射，故若把 $A$ 换为 $C$, 则 $f: B \to C$ 为双射. $B$ 是无限集，则 $C$ 也是无限集. 由命题 1，$C$ 作为 $A$ 的无限子集是可数集. $B$ 与 $C$ 等势，所以 $B$ 也是可数集. □

**命题 3** 1° 若 $A$ 可数且 $B$ 非空有限或可数，则 $A \times B$ 和 $B \times A$ 都可数.

2° 若 $A_1, \cdots, A_n$ 中至少有一个可数而其他为非空有限或可数，则 $A_1 \times \cdots \times A_n$ 可数.

**证** 1° 设 $A = \{a_0, a_1, a_2, \cdots\}, B = \{b_0, b_1, \cdots, b_n\}$ 或 $B = \{b_0, b_1, b_2, \cdots\}$. 作映射 $f: A \times B \to \mathbf{N}$, 使 $f(a_i, b_j) = 2^i 3^j$. 于是 $f$ 是单射 (当 $i \neq k$ 或 $j \neq l$ 时总有 $2^i 3^j \neq 2^k 3^l$). 由命题 2 知 $A \times B$ 可数. 类似可知 $B \times A$ 也可数.

2° 对 $n$ 归纳，利用 1° 的结论便可. □

**命题 4** 若 $A$ 可数，且若 $B$ 有限或可数，则 $A \cup B$ 也可数.

**证** 设 $A = \{a_0, a_1, a_2, \cdots\}$.

情形 1 $B$ 为有限集. 此时设 $B = \{b_0, b_1, \cdots, b_n\}$ ($B = \varnothing$ 时 $A \cup B = A$). 若 $A \cap B = \varnothing$, 则 $A \cup B$ 的全部元素形成不重复的无限序列

$$a_0, b_0, a_1, b_1, \cdots, a_n, b_n, a_{n+1}, a_{n+2}, \cdots,$$

所以是可数集. 若 $A \cap B \neq \varnothing$, 则令 $B_1 = B - A$. 这时 $B_1 \cap A = \varnothing$, 故 $A \cup B_1$ 为可数集. 而 $A \cup B = A \cup B_1$.

情形 2 $B$ 为可数集. 设 $B = \{b_0, b_1, b_2, \cdots\}$. 若 $A \cap B = \varnothing$, 则 $A \cup B$ 的全部元素形成不重复的序列 $a_0, b_0, a_1, b_1, \cdots$ . 若 $A \cap B \neq \varnothing$, 记 $C = B - A$, 则 $C \subseteq B, A \cap C = \varnothing$ 且 $A \cup B = A \cup C$. 这时当 $C$ 为有限集时，$A \cup C$ 可数 (属情形 1)，因而 $A \cup B$ 可数; 当 $C$ 为无限集时，由命题 1 知 $C$ 可数，且因 $A \cap C = \varnothing$, 故 $A \cup C$(从而 $A \cup B$) 可数. □

**命题 5** 若 $A_1, \cdots, A_n$ 中至少有一个可数，而其他为有限或可数，则 $\bigcup_{i=1}^n A_i$ 也可数.

**证** 对 $n$ 归纳，用命题 4 便可. □

**命题 6** 若 $A$ 可数，则 $\bigcup_{n=1}^\infty A^n$ 可数.

**证** 用 $p_n$ 表示第 $n$ 个素数:

$$p_0 = 2,\ p_1 = 3,\ p_2 = 5, \cdots .$$

把可数集 $A$ 的全部元素不重复地排列如下:

$$a_0,\ a_1,\ a_2,\ \cdots,\ a_n,\ \cdots,$$

设 $n \geqslant 1$, 任取 $n$ 个自然数 $i_0, i_1, \cdots, i_{n-1}$(可重复). 对 $(a_{i_0}, a_{i_1}, \cdots, a_{i_{n-1}}) \in A^n$, 令

$$f(a_{i_0}, a_{i_1}, \cdots, a_{i_{n-1}}) = p_0^{i_0} p_1^{i_1} \cdots p_{n-1}^{i_{n-1}},$$

便得到单射 $f: \bigcup_{n=1}^\infty A^n \to \mathbf{N}$. $f$ 的单射性源于正整数素幂积分解式的唯一性. 因 $\bigcup_{n=1}^\infty A^n$ 是无限集，故由命题 2 知 $\bigcup_{n=1}^\infty A^n$ 可数. □

命题 6 的意思是: 由可数集的元素形成的有序有限元组的全体构成可数集.

**命题 7** 若 $A$ 可数，则所有由 $A$ 的元素形成的有限序列构成的集 $B$ 也可数.

**证** 对任一由 $A$ 的元素构成的有限序列 $a_{i_0},\cdots,a_{i_n}$, 令

$$f(a_{i_0},\cdots,a_{i_n})=(a_{i_0},\cdots,a_{i_n})\in A^{n+1}.$$

这样的 $f:B\to\bigcup_{n=1}^{\infty}A^n$ 是单射. $B$ 是无限集，由命题 6 及命题 2 知 $B$ 可数. □

**命题 8** 若每个 $A_i$ 有限或可数，且 $\bigcup_{i\in\mathbf{N}}A_i$ 是无限集，则 $\bigcup_{i\in\mathbf{N}}A_i$ 可数.

**证** 当 $A_i$ 为有限集时，设 $A_i=\{a_{i0},\cdots,a_{in}\}$; 当 $a_i$ 为可数集时，设 $A_i=\{a_{i0},a_{i1},a_{i2},\cdots\}$. 分以下两种情形来证明.

1° 如果不同的 $A_i$ 之间没有共同元素，即当 $i\neq j$ 时 $A_i\cap A_j=\varnothing$, 就令 $f(a_{ij})=2^i3^j$, 这样得到的 $f:\bigcup_{i\in\mathbf{N}}A_i\to\mathbf{N}$ 是单射. 利用命题 2 便可.

2° 如果某些不同的 $A_i$ 之间有共同元素，则作出一列新的集 $A_0',A_1',A_2',\cdots$, 作的过程是

$$A_0'=A_0,\ A_1'=A_1-A_0,\ \cdots,\ A_n'=A_n-\bigcup_{0\leqslant i\leqslant n-1}A_i',\ \cdots.$$

这样当 $i\neq j$ 时，$A_i'\cap A_j'=\varnothing$, 由 1° 知 $\bigcup_{i\in\mathbf{N}}A_i'$ 是可数集，而 $\bigcup_{i\in\mathbf{N}}A_i=\bigcup_{i\in\mathbf{N}}A_i'$. □

根据下面的 Cantor 定理，存在着大量的不可数的无限集.

**定理 (Cantor)** 集 $A$ 和 $A$ 的幂集 $\mathcal{P}(A)$ 不等势.

**证** 反设 $A$ 与 $\mathcal{P}(A)$ 等势，即存在双射 $f:A\to\mathcal{P}(A)$. 作一集

$$B=\{a\in A\mid a\notin f(a)\}.$$

因 $B$ 也是 $A$ 的子集，故 $B\in\mathcal{P}(A)$. $f$ 是满射，必然存在 $B$ 在 $A$ 中的原象 $b$, 使 $f(b)=B$. 这时有两种可能: $b\in B$ 或 $b\notin B$. 但按 $B$ 的定义都会导致矛盾:

$$b\in B\ \Rightarrow\ b\notin f(b)=B;$$

$$b\notin B\ \Rightarrow\ b\in f(b)=B.$$

□

由此定理即知: $\mathbf{N}$ 的所有子集构成的集 $\mathcal{P}(\mathbf{N})$ 不可数，$\mathbf{N}$ 上所有二元关系的集 $\mathcal{P}(\mathbf{N}^2)$ 不可数，$\mathbf{N}$ 上所有 $n$ 元关系的集 $\mathcal{P}(\mathbf{N}^n)$ 不可数.

设 $A\subset\mathbf{N}$. $A$ 的特征函数 $C_A:\mathbf{N}\to\{0,1\}$ 由下式定义:

$$C_A(n)=\begin{cases}1 & n\in A;\\ 0 & n\notin A.\end{cases}$$

现用 $F_C$ 表示 $\mathbf{N}$ 的子集的特征函数的全体:

$$F_C=\{C_A\mid A\subset\mathbf{N}\}.$$

因 $\mathbf{N}$ 的不同子集有不同的特征函数，故存在着 $\mathcal{P}(\mathbf{N})$ 到 $F_C$ 的双射，即 $F_C$ 与 $\mathcal{P}(\mathbf{N})$ 等势，于是 $F_C$ 不可数. 又因 $\mathbf{N}$ 的每个子集的特征函数都是一元数论函数，故所有一元数论函数构成的集不可数 (由命题 1)，进而知所有数论函数构成的集不可数.

# 1 命 题 演 算

命题演算是我们要建立的最简单、最基本的形式系统. 这种系统是用来表现较为简单的逻辑推理的一种数学模型. 命题演算的简单性表现在: 当它把复合命题分解成最简单的命题后，就把简单命题视为最小的考察对象，不再继续对简单命题进行分解了. 研究这种系统，除去为了直接应用，还为研究谓词演算 (用来表现更为复杂的推理的形式系统) 打下基础.

## 1.1 命题联结词与真值表

在建立命题演算形式系统之前，先直观考察五种常用命题联结词的含义.

数学中迄今惯用的命题逻辑仍是古典二值逻辑: 任何命题只允许出现“真”或“假”的情形而没有其他情形. 我们约定，一命题若为真，则说该命题的真值为 1; 若为假，则说该命题的真值为 0.

本节对联结词的描述是非形式的. 所作描述与数学中及日常语言中的习惯大体一致，但也有些需要注意的地方.

本节中字母 $p,q,r$ 等用来表示命题.

**(1) 否定词**

否定词用符号 $\neg$ 表示. 给定命题 $p$, 则 $\neg p$ 表示一新命题，叫做“命题 $p$ 的否定”，二命题间的关系是

$$\neg p\text{为真} \Leftrightarrow p\text{为假}.$$

对应的真值表是

| $p$ | $\neg p$ |
|---|---|
| 1 | 0 |
| 0 | 1 |

**(2) 合取词**

合取词用符号 $\wedge$ 表示，含义相当于中文的“与”(或“且”). 由命题 $p,q$ 用 $\wedge$ 连接得到新命题 $p\wedge q$ 与 $p,q$ 有以下关系:

$$p\wedge q \text{ 为真} \quad \Leftrightarrow \quad p \text{ 与 } q \text{ 皆为真}.$$

也就是说，当且仅当 $p$ 与 $q$ 二者至少有一为假时 $p\wedge q$ 为假. 对应的真值表是

| $p$ | $q$ | $p\wedge q$ |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 0 |
| 0 | 0 | 0 |

**(3) 析取词**

析取词用符号 $\vee$ 表示，含义相当于中文的“或”. 由命题 $p,q$ 用 $\vee$ 连接得到的新命题 $p\vee q$ 与 $p,q$ 有以下关系:

$$p\vee q \text{ 为真} \quad \Leftrightarrow \quad p \text{ 为真或 } q \text{ 为真 (可同时为真)}.$$

换句话说，当且仅当 $p$ 和 $q$ 同时为假时 $p\vee q$ 为假. 对应的真值表是

| $p$ | $q$ | $p\vee q$ |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 0 | 1 |
| 0 | 1 | 1 |
| 0 | 0 | 0 |

联结词“或”有两种: 可兼的“或”与不可兼的“或”. 这里的析取“$\vee$”用来表示可兼或. 使用中，特别在数学使用中，可兼或比不可兼或更合用，更方便灵活. (参见 1.5.3 小节中推论 2 之后的一段说明.)

**(4) 蕴涵词**

蕴涵词用符号 $\rightarrow$ 表示，含义相当于中文的“如果 $\cdots$ 那么 $\cdots$”. 由命题 $p,q$ 用 $\rightarrow$ 连接得到的命题 $p\rightarrow q$ 与 $p,q$ 的关系是

$$p\rightarrow q \text{ 为假} \quad \Leftrightarrow \quad p \text{ 为真且 } q \text{ 为假}.$$

相应的真值表是

| $p$ | $q$ | $p\rightarrow q$ |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 1 |
| 0 | 0 | 1 |

蕴涵式 $p \to q$ 中的 $p$ 叫做该式的“前件”，$q$ 叫做该式的“后件”. 当 $p \to q$ 的前件为假时 $p \to q$ 总为真；当 $p \to q$ 的后件为真时 $p \to q$ 也总为真；除此之外，$p \to q$ 为假. 这种真值关系是符合数学上的实际习惯的. 例如

$$a^2 < 1 \ \Rightarrow \ a^2 < 8$$

是真命题，这是因为前件“$a^2 < 1$”真而同时后件“$a^2 < 8$”假的情形不会发生，只会发生以下三种情形中的一种:

$$a^2 < 1 \text{ 真且 } a^2 < 8 \text{ 真 (如} a = 0);$$

$$a^2 < 1 \text{ 假但 } a^2 < 8 \text{ 真 (如} a = 2);$$

$$a^2 < 1 \text{ 假且 } a^2 < 8 \text{ 假 (如} a = 3).$$

用“$\to$”表示“如果 $\cdots$ 那么 $\cdots$”又是与日常对蕴涵词的理解有差别. 按日常的理解，前件与后件这二者之间有某种因果关系. 在形式系统里，我们不对“$\to$”提这种要求，而是把具体的内容撇在一边. 关于这一点，其他几个联结词的情形是类似的.

**(5) 等价词 (或等值词)**

等价词用符号 $\leftrightarrow$ 表示，含义相当于中文的“当且仅当”. $p,q$ 与 $p \leftrightarrow q$ 的关系是

$$p \leftrightarrow q \text{ 为真} \ \Leftrightarrow \ p \text{ 与 } q \text{ 同为真或同为假.}$$

相应的真值表是

| $p$ | $q$ | $p \leftrightarrow q$ |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 0 |
| 0 | 0 | 1 |

明确了五种命题联结词的作用之后，我们便可讨论命题逻辑的基本问题之一: 复合命题的真假如何由构成它的支命题的真假来确定?

方法很简单: 列出该复合命题的真值表即可.

**例 1** $(\neg p) \wedge q$ 的真值表

| $(\neg\ p)$ | $\wedge$ | $q$ |
|---|---|---|
| 0 1 | 0 | 1 |
| 0 1 | 0 | 0 |
| 1 0 | 1 | 1 |
| 1 0 | 0 | 0 |

列表过程是: 先把构成它的支命题 $p$ 与 $q$ 的所有可能的真值组合分别在 $p$ 与 $q$ 的下方一一写出. 组合共有四种 (1，1；1，0；0，1；0，0)，故真值表有 4 行. 然后按命题中联结词作用次序将每次作用所得的真值写在该联结词下方. 最后得到的一列结果写在最后一个联结词下，并用竖线标出.

从表中可以看出，只在支命题 $p$ 与 $q$ 分别取真值 0 与 1 时，命题 $(\neg p)\wedge q$ 才为真. 我们说，(0, 1) 是 $(\neg p)\wedge q$ 的“成真指派”，其他三种真值指派 ((1，1) (1，0) (0，0)) 都是 $(\neg p)\wedge q$ 的“成假指派”.

更一般地，如一复合命题中含有 $n$ 个不同的支命题，则可能的真值组合 (真值指派) 共有 $2^n$ 种，故相应的真值表有 $2^n$ 行.

**例 2** $(p\vee q)\rightarrow(\neg r\wedge q)$ 有三个支命题，故真值表有 8 行:

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

由上表看出，在八组不同的真值指派中，(1，1，0)，(0，1，0)，(0，0，1) 及 (0，0，0) 是成真指派，其余四组是成假指派.

列真值表时，注意在复合命题中反复出现的同一支命题 (如例 2 中的 $q$) 的下面，指派的真值应前后相同.

**例 3** 复合命题 $(p\vee q)\leftrightarrow((\neg p)\rightarrow q)$ 的真值表是

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

表中最后一列全为 1. 这说明: 不管它的支命题取何真值，该复合命题总为真. 这样命题是永真式 (永真式的形式定义见 1.3.2 小节定义 3).

类似可得另两个永真式:

(1) $(p\wedge q)\leftrightarrow\neg(p\rightarrow(\neg q))$;

(2) $(p \leftrightarrow q) \leftrightarrow ((p \to q) \wedge (q \to p))$.

上面的三个永真式显示: 我们所讨论的五个联结词相互之间是有关联的. 从语义上看, 联结词 $\vee$ 可用 $\neg$ 与 $\to$ 这两个联结词取代 (例 3); 同样, $\wedge$ 与 $\leftrightarrow$ 也都可用 $\neg$ 与 $\to$ 来取代 (见 (1) 与 (2)). 这一观察为我们后面建立并研究形式系统带来方便.

一般来说, 构成复合命题的支命题本身还可能再分解成更简单的命题. 但在上面的例子中, 为列出给定的复合命题的真值表, 我们先列出支命题 ($p, q, r$ 等) 的全部可能有的真值组合; 而这样做相当于把支命题当作"命题变元", 忽略支命题的内部构造. 支命题与简单命题是有区别的. 这里及后面说的"简单命题", 约定不能再分解成更简单的命题. 而支命题可能再分解. 我们能肯定例 3 中的公式是永真式. 但能否用同样方法肯定公式 $p \to q$ 是或不是永真式? 回答是: 若 $p, q$ 都是简单命题, 则 $p \to q$ 肯定不是永真式; 若 $p$ 或 $q$ 不是简单命题, 则 $p \to q$ 有可能是永真式. (详见 1.3.2 小节定理 2 后的讨论. ) 正因为如此, 下面我们建造命题逻辑的形式系统, 要把用于表示简单命题的命题变元作为基本建筑材料.

### 练习 1

1. 列出以下复合命题的真值表. (其中支命题 $p, q, r, s$ 视为命题变元. )

   1° $\neg p \wedge p$.

   2° $\neg((p \to q) \to (\neg(q \to p)))$.

   3° $p \to (q \to r)$.

   4° $(p \wedge q) \to r$.

   5° $(p \leftrightarrow \neg q) \vee q$.

   6° $(p \wedge q) \vee (r \wedge s)$.

   7° $(\neg p \wedge q) \to (\neg q \wedge r)$.

   8° $(p \to q) \to (p \to r)$.

   9° $\neg(p \vee (q \wedge r)) \leftrightarrow ((p \vee q) \wedge (p \vee r))$.

   10° $(((\neg p \to (p \wedge \neg q)) \to r) \wedge q) \vee \neg r$.

   11° $(p \to q) \leftrightarrow (\neg p \vee q)$.

   12° $\neg(p \wedge q) \leftrightarrow ((\neg p) \vee (\neg q))$.

## 1.2 命题演算的建立

为了用数学方法研究命题逻辑, 需要将命题逻辑形式化, 建立一种形式语言. 为此先要选用确定的字母表. 考虑五个基本联结词之间的关联, 为简洁起见, 除采

用一列命题变元符号外，我们的字母表只含两个联结词符号: $\neg$(否定) 及 $\to$ (蕴涵).

本节对建立的形式语言进行初步研究时，先把它的语义全放一边，只进行纯形式、纯语法的考察.（语义研究留到下节.）简单地说，先只考察该形式语言中“句子”及“文章”的结构，暂不管其中的实际逻辑含义.

### 1.2.1 命题演算公式集

我们采用的字母表由下面两类符号组成.

(1) 两个运算符: $\neg$ , $\to$ .

$\neg$ (否定词) 是个一元运算符，$\to$(蕴涵词) 是个二元运算符.

(2) 命题变元的可数序列:

$$x_1, x_2, \cdots, x_n, \cdots .$$

有了这张字母表，就可用来形成命题演算的公式集. (这里的“公式”，通常称“合式公式”，或称“形式命题”.)

公式的形成规则如下:

(i) 命题变元 $x_1, x_2, \cdots, x_n, \cdots$ 中的每一个都是公式.

(ii) 若 $p$ 是公式，则 $\neg p$ 是公式；若 $p, q$ 是公式，则 $p \to q$ 是公式.

(iii) 任一公式皆由规则 (i), (ii) 的有限次使用形成.

记 $X = \{x_1, x_2, \cdots, x_n, \cdots\}$. 用 $L(X)$ 表示所有公式构成的集. 公式集 $L(X)$ 可以进行如下分层:

$$L(X) = L_0 \cup L_1 \cup \cdots \cup L_n \cup \cdots,$$

其中

$$\begin{aligned}
L_0 &= X = \{x_1, x_2, \cdots, x_n, \cdots\},\\
L_1 &= \{\neg x_1, \neg x_2, \cdots, \neg x_n, \cdots\\
&\qquad x_1 \to x_1, x_1 \to x_2, x_2 \to x_1, \cdots, x_i \to x_j, \cdots\},\\
L_2 &= \{\neg(\neg x_1), \neg(\neg x_2), \cdots, \neg(x_1 \to x_1), \cdots\\
&\qquad x_1 \to (\neg x_1), (\neg x_1) \to x_1, \cdots\\
&\qquad x_1 \to (x_1 \to x_1), (x_1 \to x_1) \to x_1, \cdots\},\\
&\cdots\cdots
\end{aligned}$$

**说明**

(1) 一层 $L_1$ 中公式由命题变元经过一次运算得来，二层 $L_2$ 中公式由命题变元经过二次运算得来，以下类推.

(2) 公式集 $L(X)$ 具有分层性——不同层次之间没有公共元素. 如果没有这一性质，那么后面要对公式集进行的归纳 (递归) 定义就失去了合理性. (例如下节要依 $L(X)$ 的层次归纳定义出赋值函数，使每个公式都有且只有唯一的一个真假值.)

本节附 2 中给出了 $L(X)$ 的更明确的构造过程及分层性的证明. 在那里，我们将看见公式集 $L(X)$ 是一种特殊的命题代数 (带有一元运算 $\neg$ 和二元运算 $\rightarrow$)，且具有分层性的特点.

(3) 从层 $L_2$ 的公式开始，便出现了左括号和右括号. 括号不是我们字母表中的符号. 但这不要紧. 通常加上括号是为了让人读起来更习惯. 至于要让机器读懂公式，则不用括号也一样方便. (详见本节附 1.)

(4) 每个公式都是命题演算字母表中有限个字母按上述形成规则形成的符号串，即字母的有限序列. 由 0. 3 节命题 7 及命题 1(注意有的符号串不是公式) 即知公式集 $L(X)$ 是可数集.

在一些场合，往往只需要涉及有限个命题变元. 这时我们不是从可数集 $X$ 出发，而是从集 $X_n = \{x_1, \cdots, x_n\}$ 出发，可用完全相同的方式建立起公式集 $L(X_n)$. $L(X_n)$ 也具有分层性与可数性.

## 练习 2

1. 写出由 $X_1 = \{x_1\}$ 生成的公式集 $L(X_1)$ 的前几个层次: $L_0, L_1, L_2$ 和 $L_3$.
2. 写出由 $X_2 = \{x_1, x_2\}$ 生成的公式集 $L(X_2)$ 的三个层次: $L_0, L_1$ 和 $L_2$.
3. 由 $X_3 = \{x_1, x_2, x_3\}$ 生成的 $L(X_3)$ 中，$L_1, L_2$ 和 $L_3$ 各有多少个元素?

## 1.2 附 1 命题演算公式的唯一读法

从命题演算的字母表

$$\{\neg, \rightarrow, x_1, x_2, \cdots, x_n, \cdots\}$$

中任取有限个符号形成一符号串，问是否是个公式? 如果是公式，是哪个层次的公式? 回答都是明确的，唯一的，即具有“唯一读法”. 下面就来说明这一点.

为了避用括号，这里我们暂把公式中的二元运算符“$\rightarrow$”全都由“中置式”改为“前置式”，即把 $p \rightarrow q$ 一律写成 $\rightarrow pq$.

首先给字母表的每个字母 $u$ 指定一个“权重” $w(u)$:

$$w(\neg) = 0,\ w(\rightarrow) = -1,\ w(x_i) = 1,\ \ i \in \mathbf{N}.$$

然后给每个字母串也规定一个权重 (是整数):

$$w(u_1 \cdots u_n) = w(u_1) + \cdots + w(u_n).$$

此外，空串的权重规定为 0.

例如，

$$w(x_1x_2x_3 \to) = 1 + 1 + 1 + -1 = 2,$$

$$w(\to \neg x_1x_2) = -1 + 0 + 1 + 1 = 1.$$

符号串“$\to \neg x_1x_2$”是公式 (即公式 $(\neg x_1) \to x_2$), 而“$x_1x_2x_3 \to$”不是公式.

一字母串的真前段，是指由该字母串去掉尾部 (右端) 相邻一串字母 (至少去掉最后一个字母) 所剩下的字母串. 它可以是空串.

**命题 1** 若一字母串是公式，则该串的权重必是 1，而该串的任一真前段的权重都小于 1.

**证** 对该公式 (字母串) 的长度 $k$ 归纳.

$k = 1$ 时，该串是公式，只可能是命题变元 $x_i$, 按指定，$w(x_i) = 1$; 该串的真前段只有空串，权重为 0.

$k > 1$ 时，有两种可能: $\neg p$, $\to pq$. 此时作归纳假设: $w(p) = w(q) = 1$, 而 $p$ 与 $q$ 的真前段的权重都小于 1. 于是:

$w(\neg p) = w(\neg) + w(p) = 0 + 1 = 1$; 因 $w(\neg) = 0$, $\neg p$ 的真前段的权重就是 $p$ 的真前段的权重，故小于 1;

$w(\to pq) = w(\to) + w(p) + w(q) = -1 + 1 + 1 = 1$, 而 $\to pq$ 的真前段的权重因 $w(\to) = -1$ 故小于 1. □

仅是权重为 1，不足以说明符号串一定是公式. 例如符号串“$x_1\neg$”不是公式，它虽权重为 1，但不满足“真前段权重都小于 1”的要求.

**命题 2** 若一字母串是由两个公式并接而成，则并接的方式是唯一的.

**证** 设一字母串由两个公式并接而成: $pq$, 同时它又是另外两个公式并接而成: $rs$. 此时公式 $p$ 与 $r$ 只存在两种可能的关系: $p$ 是 $r$ 的真前段或 $r$ 是 $p$ 的真前段. 但这两种情形都不会发生，否则与命题 1 矛盾. □

现在我们有了确定任给字母串是否是公式的算法:

1° 计算权重，权重不为 1 时排除.

2° 权重为 1 时，若该串是单个字母，那只能是 $x_i$.

3° 权重为 1 且长度大于 1 时，有三种可能.

(1) 该串以 $x_i$ 开头，则肯定不是公式 (由命题 1 的后一结论知).

(2) 该串以 $\neg$ 开头，则去掉 $\neg$ 后对剩下的较短的字母串进行检查，决定于较短字母串是否是公式.

(3) 该串以 $\to$ 开头，则去掉 (权重为 $-1$ 的)$\to$ 后，检查剩下较短的字母串 (权重为 2) 是否是两个公式的并接. 若是，则并接的方式是唯一的 (按命题 2).

公式所在的层次，由公式中出现的运算符的总数决定.

## 1.2 附2 命题演算公式集的代数结构

前面 1.2.1 小节中由命题变元集 $X = \{x_1, x_2, \cdots, x_n, \cdots\}$ 出发得到了可数的公式集 $L(X)$. 为了更清楚地认识 $L(X)$ 的代数结构及它的分层性，下面更形式化地把 $L(X)$ 作为一种 $\{\neg, \rightarrow\}$ 型代数构造出来.

我们由两个集——可数集 $X$ 及二元集 $\{1,2\}$ 出发. (直观上，这里的 1 与 2 分别被视为“否定”与“蕴涵”二词的代码. )

先如下定义一列集 $(L_0, L_1, L_2, \cdots)$ :

$$\begin{aligned}
L_0 &= X = \{x_1, x_2, \cdots, x_n, \cdots\},\\
L_1 &= (\{1\} \times L_0) \cup (\{2\} \times L_0 \times L_0)\\
&= \{(1, x_1), (1, x_2), \cdots, (1, x_n), \cdots\\
&\quad (2, x_1, x_1), (2, x_1, x_2), (2, x_2, x_1), \cdots\},\\
L_2 &= (\{1\} \times L_1) \cup (\{2\} \times L_0 \times L_1) \cup (\{2\} \times L_1 \times L_0)\\
&= \{(1, (1, x_1)), (1, (1, x_2)), \cdots, (1, (2, x_1, x_1)), \cdots\\
&\quad (2, x_1, (1, x_1)), \cdots, (2, x_1, (2, x_1, x_1)), \cdots\\
&\quad (2, (1, x_1), x_1), \cdots, (2, (2, x_1, x_1), x_1), \cdots\},\\
&\cdots\cdots
\end{aligned}$$

这一列集的归纳定义可如下写出:

$$\begin{aligned}
L_0 &= X,\\
L_k &= (\{1\} \times L_{k-1}) \cup (\bigcup\nolimits_{i+j=k-1} \{2\} \times L_i \times L_j), \quad k > 0.
\end{aligned}$$

将这一列集并在一起，用 $L(X)$ 表示:

$$L(X) = \bigcup\nolimits_{k=0}^{\infty} L_k.$$

集 $L(X)$ 中的元素随所在层次的增高越来越复杂，但形式上不外三种: $x_i$, $(1, p)$, $(2, p, q)$. 若 $(1, p) \in L_k$，则 $p \in L_{k-1}$; 若 $(2, p, q) \in L_k$, 则 $p$ 与 $q$ 所在层次的序数之和为 $k-1$.

**命题 1 ($L(X)$ 的分层性)** $i < j$ 时 $L_i \cap L_j = \varnothing$.

**证** 对 $i$ 归纳.

$i = 0$ 时，$L_0 = \{x_1, x_2, \cdots\}$, 而 $L_j (j > 0)$ 的元素只有两种形式 $(1, p)$ 与 $(2, p, q)$, 所以对于任何 $j > 0$, $L_0$ 与 $L_j$ 没有公共元素.

$i > 0$ 时，对任意 $j > i$, 要证明 $L_j$ 与 $L_i$ 没有公共元素. 事实上，$L_i$ 的元素有两种类型: $(1, p)$ 和 $(2, p_1, p_2)$; $L_j$ 的元素有两种类型: $(1, q)$ 和 $(2, q_1, q_2)$. 因为 $p, p_1, p_2$ 属于比 $L_i$ 更低的层次，所以对它们可用归纳假设. 首先，$p$ 属于 $i-1$ 层，而 $q$ 属于

$j-1$ 层 (见 $L_k$ 的定义)，又因 $j-1>i-1$, 所以 $p\neq q$, 进而 $(1,p)\neq(1,q)$. 剩下要证明 $L_i$ 中另一种类型的元素 $(2,p_1,p_2)$ 与 $L_j$ 中相应类型的元素 $(2,q_1,q_2)$ 不会相等. 如果 $(2,p_1,p_2)=(2,q_1,q_2)$, 便有 $p_1=q_1$ 且 $p_2=q_2$, 而这是不可能的，因为根据定义，$p_1$ 与 $p_2$ 所在层次数之和为 $i-1$, 而 $q_1$ 与 $q_2$ 所在层次数之和为 $j-1$. 总之，$j>i$ 时，$L_i$ 与 $L_j$ 没有公共元素. □

$L(X)$ 的分层性是后面的一些归纳定义的依据.

至此，集 $L(X)$ 中尚无代数结构，在其中尚未定义运算. 下面在 $L(X)$ 中定义一个一元运算 $\neg$ 和一个二元运算 $\rightarrow$.

对于任意 $p,q\in L(X)$, 令

$$\neg p = (1,p),$$

$$p\rightarrow q = (2,p,q).$$

由于带有运算 $\neg$ 和 $\rightarrow$, 公式集 $L(X)$ 现在成了一种特殊的代数系统——命题代数 $L(X)$. 其中除 0 层元素 (命题变元) 外，按运算的上述定义，$L(X)$ 中其他各层的所有元素都可用运算来表示: $(1,p)$ 可写成 $\neg p$, $(2,p,q)$ 可写成 $p\rightarrow q$. 于是我们可以把命题代数 $L(X)$ 的各个层元素视为运算的结果如下写出:

$$\begin{aligned}
&L_0=\{x_1,x_2,\cdots\},\\
&L_1=\{\neg x_1,\neg x_2,\cdots,x_1\rightarrow x_1,x_1\rightarrow x_2,x_2\rightarrow x_1,\cdots\},\\
&L_2=\{\neg\neg x_1,\neg\neg x_2,\cdots,\neg(x_1\rightarrow x_1),\neg(x_1\rightarrow x_2),\cdots,\\
&\qquad x_1\rightarrow\neg x_1,\cdots,x_1\rightarrow(x_1\rightarrow x_1),\cdots,\\
&\qquad \neg x_1\rightarrow x_1,\cdots,(x_1\rightarrow x_1)\rightarrow x_1,\cdots\},\\
&\cdots\cdots
\end{aligned}$$

$L_k$ 中的元素 (第 $k$ 层元素) 由命题变元经 $k$ 次运算得来.

上面得到的 $L(X)$ 通常叫做由集 $X$ 生成的 $\{\neg,\rightarrow\}$ 型代数. 每当出现“由某某集生成的某某型代数”这样的对象，指的都是由类似于上面的过程得到的代数系统.

把上面的 $X$ 换成 $X_n=\{x_1,\cdots,x_n\}$, 用相同的方法可以构造出命题代数 $L(X_n)$, 即由集 $X_n$ 生成的 $\{\neg,\rightarrow\}$ 型代数. 不同的是，现在的 $L_0=\{x_1,\cdots,x_n\}$. $L(X_n)$ 同样具有分层性. 从构造过程看出，$L(X_n)\subseteq L(X)$. $L(X_n)$ 叫做命题代数 $L(X)$ 的子代数.

**注** 代数上，$L(X)$ 叫做集 $X$(自由生成元集) 上的自由 $\{\neg,\rightarrow\}$ 型代数. 它在同构的意义下是唯一的. (参见参考文献 [4] 中第一章.) 上面我们构造 $L(X)$ 的过程给出了它的存在性的证明. 构造过程中选用什么符号是无关紧要的. 例如二元集 $\{1,2\}$ 可改为直接用 $\{\neg,\rightarrow\}$.

### 1.2.2 命题演算 $L$

有了公式集 $L(X)$ 这个命题代数，便能以它为基础建立起命题演算 $L$.

**定义 1 (命题演算 $L$)** 命题变元集 $X = \{x_1, x_2, \cdots\}$ 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 $L(X)$ 的具有以下形状的公式作为“公理”：

(L1) $p \to (q \to p)$, (肯定后件律)

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

(L3) $(\neg p \to \neg q) \to (q \to p)$, (换位律)

其中 $p, q, r \in L(X)$.

(2) “证明”

设 $\Gamma \subseteq L(X), p \in L(X)$. 当我们说“公式 $p$ 是从公式集 $\Gamma$ 可证的”，是指存在着 $L(X)$ 的公式的有限序列 $p_1, \cdots, p_n$, 其中尾项 $p_n = p$, 且每个 $p_k (k = 1, \cdots, n)$ 满足:

(i) $p_k \in \Gamma$, 或

(ii) $p_k$ 是“公理”，或

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

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

让我们对这个定义作些解释和说明.

1° 命题演算 $L$ 是用公式集 $L(X)$ 定义的，但 $L$ 比 $L(X)$ 有更多的内容. $L$ 以 $L(X)$ 为框架，同时又有一些 $L(X)$ 原来没有的新的逻辑结构.

2° 定义中的“公理”和“证明”加上了引号，是为了说明这里的概念是命题演算 $L$ 这个形式系统中的数学概念 (“公理”是 $L(X)$ 的一些特殊公式,“证明”则是由 $L(X)$ 的一些公式组成的具有特殊性质的有限序列)，以便把它们和元系统中的公理和证明区别开来. 以后在不引起混淆时，常把所加的引号取掉. 这里的“证明”，通常也叫做形式证明.

3° “公理”中的 $p, q, r$ 是 $L(X)$ 的任意元素，故 $L$ 的“公理”不是三条而是无穷多条，它们被分成 (L1)，(L2)，(L3) 这三种模式. 例如，下面三个公式都是 (L1) 型的“公理”：

$$x_1 \to (x_1 \to x_1),$$

$$\neg x_7 \to (x_{10} \to \neg x_7),$$

$$(\neg x_2 \to x_3) \to (\neg\neg x_4 \to (\neg x_2 \to x_3)).$$

4° 取 $L(X)$ 的一些特殊公式作为“公理”，取法不是唯一的. 不同的取法可得到不同类型的命题演算.

5° 按定义，$p$ 从 $\Gamma$ 可证，是指存在着“证明”：$p_1\cdots,p_n$. 这样的证明如果存在，一定不是唯一的. 比如，我们可以在任一个“证明”中多插进任一条“公理”而得到另一个“证明”.

6° 写出一个 $L$ 中的“证明”，有三条规则，其中规则 (iii) 的意思是，如果在序列的前面已经写出了 $p_i$ 和 $p_i\to p_k$, 则可在后面写出 $p_k$：

$$\cdots,p_i\to p_k,\cdots,p_i,\cdots,p_k,\cdots,$$

其中 $p_i$ 也可出现在 $p_i\to p_k$ 之前.

**定义 2 (语法推论)** 建立了命题演算 $L$ 之后，进一步规定:

(1) 如果公式 $p$ 从公式集 $\Gamma$ 可证，那么我们写 $\Gamma\vdash p$, 必要时也可写成 $\Gamma\vdash_L p$. 这时 $\Gamma$ 中的公式叫做“假定”，$p$ 叫做假定集 $\Gamma$ 的语法推论.

(2) 若 $\varnothing\vdash p$, 则称 $p$ 是 $L$ 的“定理”，记为 $\vdash p$. $p$ 在 $L$ 中从 $\varnothing$ 的证明 $p_1,\cdots,p_n$ 简称为 $p$ 在 $L$ 中的证明.

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

本章中出现的 $p,q,r$ 等字母用于表示 $L$ 的任意公式. 注意它们和命题变元的关系. 命题变元 $x_i$ 是 $L(X)$ 的零层公式，而 $p,q,r$ 等则是 $L(X)$ 的任意公式，可以是命题变元，也可以是其他层次的公式.

至此我们看到，命题演算 $L$ 是一种具有特殊逻辑结构的代数系统，是为了研究命题逻辑而建立的一种具体数学模型. 这种形式系统能不能用来表现实际的推理过程，在多大程度上能用来表现实际的推理过程，正是我们所要研究的事情.

“证明”的定义搞清楚了，便可以立即得出以下几点结论.

1° 若 $p$ 是 $L$ 的公理，则 $\Gamma\vdash p$ 对于任一公式集 $\Gamma$ 都成立.

2° 若 $\vdash p$ (即 $p$ 是 $L$ 的定理)，则 $\Gamma\vdash p$ 对于任一公式集 $\Gamma$ 都成立.

3° 若 $p\in\Gamma$, 则 $\Gamma\vdash p$.

4° $\{p,p\to q\}\vdash q$.

5° 若 $\Gamma\vdash p_n$, 且已知 $p_1,\cdots,p_n$ 是 $p_n$ 从 $\Gamma$ 的证明，则当 $1\leqslant k\leqslant n$ 时，有 $\Gamma\vdash p_k$, 且 $p_1,\cdots,p_k$ 是 $p_k$ 从 $\Gamma$ 的证明.

6° 若 $\Gamma$ 是无限集，且 $\Gamma\vdash p$, 则存在 $\Gamma$ 的有限子集 $\Delta$ 使 $\Delta\vdash p$.

写出一个符合要求的 $L$ 中的证明，往往并不容易. 下们先看几个简单的例子.

**例 1** 证明 $\{p\}\vdash q\to p$.

为证 $\{p\}\vdash q\to p$, 我们构造 $q\to p$ 从 $\{p\}$ 的一个“证明”如下:

| | |
|---|---|
| (1) $p$ | 假定 |
| (2) $p\to(q\to p)$ | (L1) |
| (3) $q\to p$ | (1)，(2)，MP |

我们把“证明”中公式的编号写在该公式的左边，而把写出该公式的依据写在该行的最右端. 这些编号和依据并不是“证明”的一部分. 本例中的“证明”，是由三个公式构成的有限序列:

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

例 1 的结论 $\{p\} \vdash q \to p$ 是 (L1) 的变形，有时也叫做“肯定后件律”.

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

下面是 $(x_1 \to x_2) \to (x_1 \to x_1)$ 在 $L$ 中的一个证明:

(1) $x_1 \to (x_2 \to x_1)$ (L1)

(2) $(x_1 \to (x_2 \to x_1)) \to ((x_1 \to x_2) \to (x_1 \to x_1))$ (L2)

(3) $(x_1 \to x_2) \to (x_1 \to x_1)$ (1), (2), MP

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

下面是所要的一个证明:

(1) $x_2 \to (x_1 \to x_3)$ 假定

(2) $(x_2 \to (x_1 \to x_3)) \to ((x_2 \to x_1) \to (x_2 \to x_3))$ (L2)

(3) $(x_2 \to x_1) \to (x_2 \to x_3)$ (1), (2), MP

(4) $x_1$ 假定

(5) $x_1 \to (x_2 \to x_1)$ (L1)

(6) $x_2 \to x_1$ (4), (5), MP

(7) $x_2 \to x_3$ (3), (6), MP

**命题 1** $\vdash p \to p$ **(同一律)**

**证** 下面是 $p \to p$ 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

□

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

**证** 下面是所要的证明:

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

(2) $((\neg p \to \neg q) \to (q \to p)) \to (\neg q \to ((\neg p \to \neg q) \to (q \to p)))$ (L1)

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

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

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

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

(7) $\neg q \to (q \to p)$ (5)，(6)，MP

□

命题 2 的证明中开始用了 (L3) 型公理，而以前的例题和命题并未用 (L3).

**定义 3 (无矛盾公式集)** 如果对任何公式 $q$, $\Gamma \vdash q$ 和 $\Gamma \vdash \neg q$ 二者都不同时成立，就称公式集 $\Gamma$ 是无矛盾公式集，否则称 $\Gamma$ 为有矛盾公式集.

**命题 3** 若 $\Gamma$ 是有矛盾公式集，则对 $L$ 的任一公式 $p$, 都有 $\Gamma \vdash p$.

**证** 设 $\Gamma$ 有矛盾，即存在公式 $q$ 使 $\Gamma \vdash q$ 和 $\Gamma \vdash \neg q$ 同时成立. 于是对任一公式 $p$, 存在着 $p$ 从 $\Gamma$ 的证明:

$$\cdots, q, \cdots, \neg q, \cdots, \neg q \to (q \to p), q \to p, p.$$

这里利用了命题 2 的结论 (否定前件律). □

为一个从 $\Gamma$ 可证的公式 $p$ 写出一个符合定义要求的从 $\Gamma$ 的证明，构造的方法往往不容易想出来，这种证明往往还要写得很长. 例如，可以证明，公式 $(\neg p \to p) \to p$ 是 $L$ 的定理，但我们若要严格按照定义写出它在 $L$ 中的一个证明，要写出 19 步.

下面介绍的三个语法定理——演绎定理、反证律和归谬律将会帮助我们更容易建立 $\Gamma \vdash p$ 这种形式的结果. 但在开头，还是有必要做一些按照定义写出证明的练习.

## 练习 3

1. 证明 $L$ 中所有能写出的“证明”构成的集是可数集.
2. 写出以下公式在 $L$ 中的“证明”(即证明它们是 $L$ 的定理).

   1° $(x_1 \to x_2) \to ((\neg x_1 \to \neg x_2) \to (x_2 \to x_1))$.

   2° $((x_1 \to (x_2 \to x_3)) \to (x_1 \to x_2)) \to ((x_1 \to (x_2 \to x_3)) \to (x_1 \to x_3))$.

   3° $x_1 \to (x_2 \to (x_1 \to x_2))$.
3. 证明下面的结论.

   1° $\{\neg p\} \vdash p \to p$.

   2° $\{\neg\neg p\} \vdash p$.

   3° $\{p \to q, \neg(q \to r) \to \neg p\} \vdash p \to r$.

   4° $\{p \to (q \to r)\} \vdash q \to (p \to r)$.

   5° $\{p \to q, q \to r\} \vdash p \to r$.
4. 试证，若 $\Gamma \vdash q$ 且 $\Gamma \cup \{q\} \vdash p$, 则 $\Gamma \vdash p$.
5. 试证 $\vdash (\neg p \to p) \to p$. (按定义写出在 $L$ 中的证明.)

### 1.2.3 演绎定理

我们很快会看到，在研究命题演算 $L$ 的过程中，下面的演绎定理是很有用的重要结论.

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

**证** ($\Leftarrow$) 假定 $\Gamma \vdash p \to q$. 由定义，$p \to q$ 在 $L$ 中有一个从 $\Gamma$ 的证明 $p_1, \cdots, p_n$，其中 $p_n = p \to q$. 于是

$$p_1, \cdots, p_n, p, q$$

便是 $q$ 在 $L$ 中从 $\Gamma \cup \{p\}$ 的证明.

($\Rightarrow$) 假定 $\Gamma \cup \{p\} \vdash q$, 并设 $q_1, \cdots, q_n (= q)$ 是 $q$ 从 $\Gamma \cup \{p\}$ 的一个证明. 我们对这个证明的长度 $n$ 用归纳法来证明 $\Gamma \vdash p \to q$.

1° $n = 1$ 时，有三种可能: $q = p$, $q \in \Gamma$, 或 $q$ 是公理. 不管哪种情况出现，都有 $\Gamma \vdash p \to q$. 事实上，当 $q = p$ 时，由 1.2.2 小节命题 1 知 $\vdash p \to p$, 于是有 $\Gamma \vdash p \to p$ 即 $\Gamma \vdash p \to q$; 当 $q \in \Gamma$ 或 $q$ 为公理时，序列

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

就是 $p \to q$ 从 $\Gamma$ 的证明.

2° $n > 1$ 时，有四种可能的情形: $q = p$, $q \in \Gamma$, $q$ 是公理，或 $q$ 由于使用 MP 而得. 前三种情形与 1° 中的三种情形同样处理就可以了. 下面只用讨论 $q$ 由 $q_i$ 及 $q_j = q_i \to q$ 使用 MP 而得的情形. 因 $i, j < n$, 由归纳假设，

$$\Gamma \cup \{p\} \vdash q_i \quad \Rightarrow \quad \Gamma \vdash p \to q_i,$$

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

于是我们有 $p \to q$ 从 $\Gamma$ 的证明:

$$\left.\begin{array}{ll} (1) & \cdots\cdots \\ & \cdots\cdots \\ (k) & p \to q_i \end{array}\right\} p \to q_i \text{ 从 } \Gamma \text{ 的证明}$$

$$\left.\begin{array}{ll} (k+1) & \cdots\cdots \\ & \cdots\cdots \\ (l) & p \to (q_i \to q) \end{array}\right\} p \to (q_i \to q) \text{ 从 } \Gamma \text{ 的证明}$$

| | | |
|---|---|---|
| $(l+1)$ | $(p \to (q_i \to q)) \to ((p \to q_i) \to (p \to q))$ | (L2) |
| $(l+2)$ | $(p \to q_i) \to (p \to q)$ | $(l), (l+1)$, MP |
| $(l+3)$ | $p \to q$ | $(k), (l+2)$, MP |

这就完成了归纳过程. □

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

**证** 根据演绎定理，为了证明 $\{p \to q, q \to r\} \vdash p \to r$, 只用证明 $\{p \to q, q \to$

$r, p\} \vdash r$ 就可以了. 不难看出,

$$p,\ p \to q,\ q,\ q \to r,\ r$$

就是 $r$ 从 $\{p \to q,\ q \to r,\ p\}$ 的证明. □

假设三段论 (Hypothetical Syllogism) 简记作 HS，以后可作为一条新推理规则直接引用.

为了建立 $\Gamma \vdash p \to q$ 这种形式的结果，使用演绎定理往往是比较方便的. 这是因为，引进了一个新假定 $p$ 以后，证明 $\Gamma \cup \{p\} \vdash q$ 一般要比证明 $\Gamma \vdash p \to q$ 容易得多. 为了看清这一点，只要把上面推论的证明与练习 3 题 3 – 5° 中的结论的证明加以比较就可以了.

注意，在证明演绎定理的过程中没有用到 (L3) 型公理. 这说明如果在建立 $\Gamma \cup \{p\} \vdash q$ 的过程中没有用 (L3)，那么不用 (L3) 就可以建立 $\Gamma \vdash p \to q$, 而且反过来也是如此. 换句话说，如果在命题演算 $L$ 的定义中把 (L3) 去掉或换成别的公理，但其他都保持不变，那么演绎定理对新的命题演算系统仍然成立.

**例 1** 重新证明 $\vdash \neg q \to (q \to p)$. (试与 1.2.2 小节命题 2 的证明加以比较. )

根据演绎定理，只用证 $\{\neg q\} \vdash q \to p$.

下面是 $q \to p$ 从 $\{\neg q\}$ 的证明:

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

**命题 1 (否定肯定律)** $\vdash (\neg p \to p) \to p$.

**证** 按演绎定理，只用证明 $\{\neg p \to p\} \vdash p$.

下面是 $p$ 从 $\{\neg p \to p\}$ 的一个证明.

| | |
|---|---|
| (1) $\neg p \to (p \to \neg(\neg p \to p))$ | (由 1.2.2 命题 2) |
| (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 |

□

命题 1 的证明中列出的“证明”已经不是原来定义所要求的严格意义下的“证明”，因为这里已经引用了前面建立的结论 (即 1.2.2 小节命题 2——否定前件律的特殊情形). 尽管如此，仍足以证明所要建立的结论是正确的. (参见练习 3 题 4. )

## 练习 4

1. 先根据定义直接证明

$$\vdash (x_1 \to (x_1 \to x_2)) \to (x_1 \to x_2),$$

然后再利用演绎定理来证明它.

2. 利用演绎定理证明以下公式是 $L$ 的定理.

1° $p \to \neg\neg p$.

2° $(q \to p) \to (\neg p \to \neg q)$. (换位律)

3° $((p \to q) \to p) \to p$. (Peirce 律)

4° $\neg(p \to q) \to (q \to p)$.

### 1.2.4 反证律与归谬律

这里要建立的两个语法定理 (反证律与归谬律)，同演绎定理一样，对进行形式推理有很大帮助.

**定理 1 (反证律)**

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

**证** 根据已知条件 ($q$ 和 $\neg q$ 都存在从 $\Gamma\cup\{\neg p\}$ 的证明)，可以先写出 $p$ 从 $\Gamma\cup\{\neg p\}$ 的证明如下:

$$\left.\begin{array}{ll} (1) & \cdots\cdots \\ & \cdots\cdots \\ (k) & q \end{array}\right\} q \text{ 从 } \Gamma\cup\{\neg p\} \text{ 的证明}$$

$$\left.\begin{array}{ll} (k+1) & \cdots\cdots \\ & \cdots\cdots \\ (l) & \neg q \end{array}\right\} \neg q \text{ 从 } \Gamma\cup\{\neg p\} \text{ 的证明}$$

| | | |
|---|---|---|
| $(l+1)$ | $\neg q \to (q \to p)$ | 否定前件律 |
| $(l+2)$ | $q \to p$ | $(l)$, $(l+1)$, MP |
| $(l+3)$ | $p$ | $(k)$, $(l+2)$, MP |

至此证明了 $\Gamma \cup \{\neg p\} \vdash p$. (尚未达到目的: $\Gamma \vdash p$.) 用一次演绎定理，可得 $\Gamma \vdash \neg p \to p$. 由此可将 $p$ 从 $\Gamma$ 的证明如下构造出来:

$$\left.\begin{array}{ll}(1) & \cdots\cdots \\ & \cdots\cdots \\ (m) & \neg p \to p\end{array}\right\} \neg p \to p \text{ 从 } \Gamma \text{ 的证明}$$

(m+1) $(\neg p \to p) \to p$ 否定肯定律

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

于是有 $\Gamma \vdash p$. □

反证律与通常的反证法原理是一致的: 为证明一个命题，先否定它；若推出了矛盾，就可以肯定它.

在证明反证律的过程中并未直接用到 (L3)，但用到了否定前件律和否定肯定律，这“二律”的证明都是要用 (L3) 的.

下例用来说明反证律的应用.

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

由演绎定理，只用证 $\{\neg p \to \neg q, \neg p \to q\} \vdash p$. 为用反证律，我们把 $\neg p$ 作为新假定. 以下公式从 $\{\neg p \to \neg q, \neg p \to q, \neg p\}$ 都是可证的.

(1) $\neg p$ 新假定

(2) $\neg p \to \neg q$ 假定

(3) $\neg p \to q$ 假定

(4) $\neg q$ (1)，(2)，MP

(5) $q$ (1)，(3)，MP

由 (4)，(5) 用反证律即得 $\{\neg p \to \neg q, \neg p \to q\} \vdash p$.

作一比较，下面不用反证律给出 $p$ 从 $\{\neg p \to \neg q, \neg p \to q\}$ 的一个证明.

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

(2) $\neg p \to \neg q$ 假定

(3) $q \to p$ (1)，(2)，MP

(4) $\neg p \to q$ 假定

(5) $\neg p \to p$ (3)，(4)，HS

(6) $(\neg p \to p) \to p$ 否定肯定律

(7) $p$ (5)，(6)，MP

这个证明更长. 问题还在于这种构造证明的方法不容易想出来.

**定理 1 推论 (双重否定律)**

1° $\{\neg\neg p\} \vdash p$,

2° $\vdash \neg\neg p \to p$.

**证** 用反证律证 1° (由 1° 用演绎定理即可得出 2°)，把 $\neg p$ 作为新假定，便有

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

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

由 (1)，(2) 用反证律即得 $\{\neg\neg p\} \vdash p$. □

(试把证明与练习 3 题 3 – 2° 未用反证律的证明加以比较.)

**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** 因已知 $\Gamma \cup \{p\} \vdash q$, 故存在 $q$ 从 $\Gamma \cup \{p\}$ 的证明. 在这个证明中所有出现的假定 $p$ 之前，都插入 $\neg\neg p$ 和 $\neg\neg p \to p$ (双重否定律) 这两项，于是该证明就变成了 $q$ 从 $\Gamma \cup \{\neg\neg p\}$ 的一个证明，从而得到

(1) $\Gamma \cup \{\neg\neg p\} \vdash q$.

同理由已知条件 $\Gamma \cup \{p\} \vdash \neg q$ 可得

(2) $\Gamma \cup \{\neg\neg p\} \vdash \neg q$.

由 (1)，(2) 用反证律得 $\Gamma \vdash \neg p$. 这样便由反证律推出了归谬律. □

下例用来说明归谬律的应用.

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

按演绎定理，只用证 $\{p, \neg q\} \vdash \neg(p \to q)$. 把 $p \to q$ 作为新假定，立即可得

(1) $\{p, \neg q, p \to q\} \vdash q$,

(2) $\{p, \neg q, p \to q\} \vdash \neg q$.

由 (1), (2) 用归谬律便得 $\{p, \neg q\} \vdash \neg(p \to q)$.

**定理 2 推论 (第二双重否定律)**

1° $\{p\} \vdash \neg\neg p$,

2° $\vdash p \to \neg\neg p$.

**证** 因

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

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

由 (1), (2) 用归谬律即得 $\{p\} \vdash \neg\neg p$. □

可以看出，演绎定理、反证律和归谬律的共同点是: 用增加新假定的办法使形式证明更易于进行.

反证律和归谬律有什么不同? 从形式上看，似乎差别不大. 反证律是将待证公式先否定，把否定的待证公式作为新假定，若推出矛盾，则肯定这个待证公式; 归谬律是将待证的否定式先肯定，去掉前面的否定号后作为新假定，若推出矛盾，则证明了原否定式. 对我们的系统来说，反证律和归谬律的差别是不重要的. 前者常用来证明肯定式，后者常用来证明否定式. 但对于其他某些系统来说，它们的差别是本质的. (见 1.2 附 3)

前面我们曾多次提到，有些证明用了 (L3)，而有些证明则与 (L3) 无关. 许多不同的系统之间的差别，集中表现在对公理模式 (L3) 态度上.

一些系统不承认 (L3)，在这些系统中，(L3) 被换成了强弱不等但都比 (L3) 弱的形式. 它们的共同点往往是: 不承认反证律，但承认归谬律.

现把一些重要结论列出如下，以后可以直接引用.

$\vdash p \to p$ (同一律)

$\vdash \neg q \to (q \to p)$ (否定前件律)

$\vdash (\neg p \to p) \to p$ (否定肯定律)

$\vdash (p \to q) \to ((q \to r) \to (p \to r))$ (HS，即假设三段论)

$\vdash \neg\neg p \to p$ (双重否定律)

$\vdash p \to \neg\neg p$ (第二双重否定律)

$\vdash (p \to q) \to (\neg q \to \neg p)$ (换位律，见练习 4 题 2 – 2°.)

## 练习 5

1. 证明

1° $\vdash (p \to \neg q) \to (q \to \neg p)$.

2° $\vdash (\neg p \to q) \to (\neg q \to p)$.

3° $\vdash \neg(p \to q) \to \neg q$.

4° $\vdash \neg(p \to q) \to p$.

5° $\vdash (p \to q) \to ((\neg p \to q) \to q)$.

2. 不用 (L3)，试由归谬律和双重否定律 (即定理 1 推论 $\vdash \neg\neg p \to p$) 推出反证律.

### 1.2.5 析取，合取与等值

在 $\{\neg, \to\}$ 型代数 $L(X)$ 中，还可以定义三个新的二元运算 $\vee$(析取), $\wedge$(合取)及 $\leftrightarrow$ (等值) 如下:

$$p \vee q = \neg p \to q,$$

$$p \wedge q = \neg(p \to \neg q),$$

$$p \leftrightarrow q = (p \to q) \wedge (q \to p).$$

**命题 1**

1° $\vdash p \to (p \vee q)$.

2° $\vdash q \to (p \vee q)$.

3° $\vdash (p \vee q) \to (q \vee p)$.

4° $\vdash (p \vee p) \to p$.

5° $\vdash \neg p \vee p$. (排中律)

**证** 1° 由否定前件律 (或 1.2.2 小节命题 3) 即可得

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

用两次演绎定理，便有 $\vdash p \to (\neg p \to q)$, 此即 $\vdash p \to (p \vee q)$.

2° $q \to (\neg p \to q)$ 是 (L1) 型公理.

3° 留作练习.

4° $(p \vee p) \to p$ 就是否定肯定律 $(\neg p \to p) \to p$.

5° 排中律 $\neg p \vee p$ 就是双重否定律 $\neg\neg p \to p$. □

**命题 2**

1° $\vdash (p \wedge q) \to p$.

2° $\vdash (p \wedge q) \to q$.

3° $\vdash (p \wedge q) \to (q \wedge p)$.

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° 要证 $\vdash (p \wedge q) \to p$, 即要证 $\vdash \neg(p \to \neg q) \to p$. 下面是所要的一个证明:

| | |
|---|---|
| (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 $\neg(p \wedge \neg p)$ 按 $\wedge$ 的定义就是

$$\neg\neg(p \to \neg\neg p),$$

证明时要两次应用第二双重否定律.

其余结论的证明细节略去，方法是类似的，都是先把 $\wedge$ 按定义换成用 $\neg$ 和 $\to$ 来表示. □

**命题 3**

1° $\vdash (p \leftrightarrow q) \to (p \to q)$.

2° $\vdash (p \leftrightarrow q) \to (q \to p)$.

3° $\vdash (p \leftrightarrow q) \leftrightarrow (q \leftrightarrow p)$.

4° $\vdash (p \leftrightarrow q) \leftrightarrow (\neg p \leftrightarrow \neg q)$.

5° $\vdash (p \to q) \to ((q \to p) \to (p \leftrightarrow q))$.

**命题 4 (De. Morgan 律)**

1° $\vdash \neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$.

2° $\vdash \neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$.

## 练习 6

1. 证明命题 1-3°.
2. 证明命题 2-2°, 3°, 4°.
3. 证明命题 3-4°.
4. 证明命题 4-1°.

## 1.2 附 3 命题演算的其他系统介绍

在建立命题演算时采用哪些公式作为公理，可以有不同的选择，从而可以得到不同的系统.

**1. 古典命题演算系统**

把 $L$ 中的（L3）型公理去掉，换上

$$(\mathrm{L}'3) \quad \neg q \to (q \to p) \quad (\text{否定前件律})$$

$$(\mathrm{L}'4) \quad (\neg p \to p) \to p \quad (\text{否定肯定律})$$

而其他皆保持不变，得到的命题演算记作 $L'$.

把 $L$ 中的 (L3) 去掉，但允许使用反证律，得到的系统记作 $F$.

把 $L$ 中的 (L3) 去掉，但允许使用归谬律，且以双重否定律 (即 $\neg\neg p \to p$) 为公理，得到的系统记作 $F'$.

这样我们就有了四个不同的命题演算系统，它们之间的区别是:

$L$ 有 (L3),

$L'$ 有 (L′3), (L′4),

$F$ 有反证律,

$F'$ 有归谬律和 $\neg\neg p \to p$.

**定理 1** $L, L', F, F'$, 四个系统等价，即: 对任一公式 $p \in L(X)$,

$$\vdash_L p \quad \Leftrightarrow \quad \vdash_{L'} p \quad \Leftrightarrow \quad \vdash_F p \quad \Leftrightarrow \quad \vdash_{F'} p.$$

**证** 因为 (L1) 和 (L2) 是这些系统共有的，所以演绎定理对它们都成立. (见 1.2.3 小节例 1 前的一段说明.)

先来证 $F$ 和 $F'$ 的等价性.

由反证律可推出 $\neg\neg p \to p$ (1.2.4 小节定理 1 推论)，并进而可推出归谬律 (1.2.4 小节定理 2)，证明过程中，都没有直接使用 (L3). 这就说明，凡在 $F'$ 中能证的公式

在 $F$ 中也能证，即

$$\vdash_{F'} p \quad \Rightarrow \quad \vdash_F p.$$

反之，由归谬律和 $\neg\neg p \to p$ 能推出反证律，证明过程中不用 (L3). (见练习 5 题 2.) 于是有

$$\vdash_F p \quad \Rightarrow \quad \vdash_{F'} p.$$

下面证明 $L, L', F$ 三者等价.

前面已建立事实

$$\vdash_L \neg q \to (q \to p), \quad (\text{否定前件律})$$

$$\vdash_L (\neg p \to p) \to p, \quad (\text{否定肯定律})$$

这说明

$$\vdash_{L'} p \quad \Rightarrow \quad \vdash_L p.$$

在 $L'$ 中可以导出反证律 (注意 1.2.4 小节定理 1 的证明和随后例 1 前的说明). 所以有

$$\vdash_F p \quad \Rightarrow \quad \vdash_{L'} p.$$

剩下只用证明 $\vdash_L p \ \Rightarrow \ \vdash_F p$ 就可以了. 为此，只需要下面的结果:

$$\vdash_F (\neg p \to \neg q) \to (q \to p). \quad (\text{即(L3)})$$

事实上，我们有

1° $\{\neg p \to \neg q,\ q, \neg p\} \vdash_F q$,

2° $\{\neg p \to \neg q,\ q, \neg p\} \vdash_F \neg q$,

由 1°, 2° 用反证律得

$$\{\neg p \to \neg q, q\} \vdash_F p,$$

再用两次演绎定理便可. □

$L, L', F, F'$ 以及任何与它们等价的系统都叫做古典命题演算系统.

$\neg\neg p \to p$ 由反证律 (不直接用 (L3)) 立即可证 (见 1.2.4 小节定理 1 推论)，但下面我们很快会看到，将反证律换成归谬律却办不到这一点.

**2. 极小系统**

在 $L$ 中去掉 (L3)，但允许使用归谬律，这样得到的系统 (也可以说由 $F'$ 去掉 $\neg\neg p \to p$ 所得的系统) 叫做极小系统，记作 $G$.

因归谬律在 $L$ 中成立，故有

$$\vdash_G p \quad \Rightarrow \quad \vdash_L p.$$

但反之不成立: 存在着 $L$ 的定理在 $G$ 中得不到证明.

**命题 1** $\vdash_G \neg\neg p \to p$ 和 $\vdash_G \neg q \to (q \to p)$ 不恒成立.

**证** 先给每一个公式都规定一个"权重" $w$ :

(1) 命题变元的权重为 0，即 $w(x_i) = 0$;

(2) 否定式的权重为 1，即 $w(\neg p) = 1$;

(3) 若 $w(p) = 1$ 且 $w(q) = 0$, 则令 $w(p \to q) = 0$, 否则令 $w(p \to q) = 1$.

由简单的计算可知以下结论成立.

1° (L1) 型和 (L2) 型公理的权重恒为 1.

2° 由权重为 1 的公式经使用 MP 得出的公式权重也恒为 1，即

$$w(p) = w(p \to q) = 1 \ \Rightarrow \ w(q) = 1.$$

3° 用归谬律推出的公式 (都是否定式) 权重恒为 1.

由以上三个结论立即推出

$$\vdash_G p \ \Rightarrow \ w(p) = 1.$$

但我们有

$$w(\neg\neg x_1 \to x_1) = 0,$$

$$w(\neg\neg x_1 \to (\neg x_1 \to x_1)) = 0.$$

这说明 $\neg\neg x_1 \to x_1$ 和 $\neg\neg x_1 \to (\neg x_1 \to x_1)$ 都不是 $G$ 的定理，而前者是双重否定律 $\neg\neg p \to p$ 的特例，后者是否定前件律 $\neg q \to (q \to p)$ 的特例. □

$L$ 与 $F$ 等价，说明 (L3) 与反证律等价；$L$ 比 $G$ 强，说明 (L3) 比归谬律强，即反证律比归谬律强.

注意，$\vdash_G \neg\neg p \to p$ 不恒成立. 但 $\vdash_G p \to \neg\neg p$ 却恒成立. (见 1.2.4 小节定理 2 推论及其证明. ) 所以双重否定律与第二双重否定律是有区别的.

**3. Heyting 系统**

把 $L$ 中的 (L3) 换成

$$\text{(L}'\text{3)} \qquad \neg q \to (q \to p) \ \ \textbf{(否定前件律)}$$

同时允许使用归谬律 (即由极小系统 $G$ 增加公理 (L′3)) 得到的系统叫做 Heyting 系统，记作 $H$.

**命题 2** $\vdash_H \neg\neg p \to p$ 不恒成立.

**证** 给每个公式规定权重如下:

(1) $w(x_1) = 0$.

(2) $w(p) = 0$ 时令 $w(\neg p) = 2$,
$w(p) = 1$ 时令 $w(\neg p) = 2$,
$w(p) = 2$ 时令 $w(\neg p) = 1$.

(3) $w(p) = 1$ 且 $w(q) = 0$ 时令 $w(p \to q) = 0$,
$w(p) = 0$ 且 $w(q) = 2$ 时令 $w(p \to q) = 2$,

$w(p)=1$ 且 $w(q)=2$ 时令 $w(p\to q)=2$.

其他情形规定 $w(p\to q)=1$.

权重的取值范围是 $\{0,1,2\}$.

注意，在演绎定理成立的任何系统中，允许使用归缪律，相当于增加形为

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

的公式为公理. 这些公式连同 (L1) 型、(L2) 型公理，以及所有形为 $\neg q\to(q\to p)$ 的公式，它们的权重全都恒为 1. (验证留给读者) 同时，由权重为 1 的公式使用 MP 得到的公式权重也为 1. 这些事实说明

$$\vdash_H p \quad\Rightarrow\quad w(p)=1,$$

但是我们有

$$w(\neg\neg x_1\to x_1)=0. \qquad \square$$

上面介绍了两种非古典命题演算系统: 极小系统 $G$ 和 Heyting 系统 $H$. 此外还有其他的非古典系统，它们强弱不等，但共同点是不承认双重否定律 $\neg\neg p\to p$ (即排中律 $\neg p\vee p$).

一种叫做直觉主义的学派，否认排中律在数学中可以无限制地运用，要求数学在涉及到一个对象的存在性时，应给出具体的构造方法，认为没有构造方法而只基于排中律给出的关于存在性的证明没有什么意义.

对于什么是数学上的“证明”，并不存在一个大家完全一致的回答.

## 1.3 命题演算的语义

作为一种形式系统，一种具体的形式语言，命题演算 $L$ 的建立只涉及这种语言的语法. 在建构系统的过程中，符号的内容被暂撇一边. 用字母串来形成公式的规则，相当于句法；而用公式的有限序列来构造形式证明，则相当于文章构成法.

我们现在要转向命题演算这种形式语言的语义研究，随后将讨论语法与语义之间的关系. 这里的研究不仅为了直接应用，更是为下章研究谓词演算作准备.

### 1.3.1 真值函数

真值函数是用来研究命题演算的重要数学工具.

记 $\mathbf{Z}_2=\{0,1\}$.

**定义 1 (真值函数)** 函数 $f:\mathbf{Z}_2^n\to\mathbf{Z}_2$ (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 $f_4$ 是常数函数.

$f_2$ 是恒等函数，$f_2(v) = v$.

$f_3$ 叫做“非”运算或“否定”运算，也用 $\neg$ 表示:

$$\neg v = f_3(v) = 1 - v.$$

二元真值函数一共有 16 个，可将它们的函数值列成下表:

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

在这 16 个二元真值函数中，$f_4$ 和 $f_6$ 是坐标函数:

$$f_4(v_1, v_2) = v_1,$$

$$f_6(v_1, v_2) = v_2.$$

$f_5$ 叫做“蕴涵”运算，也用符号 $\to$ 表示. 它的计算公式为

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

现在把一元非运算 $\neg$ 和二元蕴涵运算 $\to$ 的表单独列出如下:

| $v$ | $\neg v$ |
|---|---|
| 1 | 0 |
| 0 | 1 |

| $v_1$ | $v_2$ | $v_1 \to v_2$ |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 1 |
| 0 | 0 | 1 |

我们看到，$\mathbf{Z}_2$ 也是一种 $\{\neg, \to\}$ 型代数，是与 $L(X)$ 不同的另一种命题代数.

由上表很容易验证以下公式成立:

**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 $f_2, f_8$ 及 $f_7$ 分别用 $\vee, \wedge, \leftrightarrow$ 表示:

| $v_1$ | $v_2$ | $v_1 \vee v_2$ | $v_1 \wedge v_2$ | $v_1 \leftrightarrow v_2$ |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 |
| 1 | 0 | 1 | 0 | 0 |
| 0 | 1 | 1 | 0 | 0 |
| 0 | 0 | 0 | 0 | 1 |

容易验证:

**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** $v_1 \leftrightarrow v_2 = (v_1 \to v_2) \wedge (v_2 \to v_1)$.

以上公式中的 $v, v_1, v_2 \in \mathbf{Z}_2$.

因 $n$ 元真值函数的定义域 $\mathbf{Z}_2^n$ 有 $2^n$ 个元素，故对给定的 $n > 0$, 不同的 $n$ 元真值函数有 $2^{2^n}$ 个.

下面当我们说 $n$ 元真值函数 $f$ 可用一元运算 $\neg$ 和二元运算 $\to$ 表示出来，意思是说函数值 $f(v_1, \cdots, v_n)$ 可由 $v_1, \cdots, v_n (\in \mathbf{Z}_2)$ 经有限次这两种运算 ($\neg$ 和 $\to$) 得到.

**命题 1** 任一真值函数都可用一元运算 $\neg$ 和二元运算 $\to$ 表示出来.

**证** 对真值函数的元数 $n$ 归纳.

$n = 1$ 时，命题正确:

$$f_1(v) = 1 = v \to v,$$

$$f_2(v) = v,$$

$$f_3(v) = \neg v,$$

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

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

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

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

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

这样就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 $h$ 可由 $\neg$ 及 $\to$ 表示出来; 按照上面 $k$ 的定义式，$k$ 也具有这种性质.

下面证明 $k = f$, 从而 $f$ 也具有这种性质.

$$\begin{aligned} k(v_1, \cdots, v_{n-1}, 1) &= (h(v_1, \cdots, v_{n-1}) \to 1) \to \neg(g(v_1, \cdots, v_{n-1}) \to 0) \\ &= 1 \to \neg\neg g(v_1, \cdots, v_{n-1}) && \text{(由公式 3, 4)} \\ &= 1 \to g(v_1, \cdots, v_{n-1}) && \text{(由公式 1)} \\ &= g(v_1, \cdots, v_{n-1}) && \text{(由公式 2)} \end{aligned}$$

$$
\begin{aligned}
&= f(v_1,\cdots,v_{n-1},1). && (g\text{ 的定义})\\
k(v_1,\cdots,v_{n-1},0) &= (h(v_1,\cdots,v_{n-1})\to 0)\to\neg(g(v_1,\cdots,v_{n-1})\to 1)\\
&= \neg h(v_1,\cdots,v_{n-1})\to 0 && (\text{由公式4, 3, 及}\neg 1=0)\\
&= \neg\neg h(v_1,\cdots,v_{n-1}) && (\text{由公式4})\\
&= h(v_1,\cdots,v_{n-1}) && (\text{由公式1})\\
&= f(v_1,\cdots,v_{n-1},0). && (h\text{的定义})
\end{aligned}
$$

所得结果说明对任意 $v_1,\cdots,v_n\in\mathbf{Z}_2$, 都有

$$k(v_1,\cdots,v_n)=f(v_1,\cdots,v_n),$$

于是 $f=k$. □

上面关于真值函数的讨论虽用了 $\neg$ 和 $\to$ 等逻辑符号，但所作讨论全属于数学.

### 1.3.2 赋值与语义推论

$L(X)$ 和 $\mathbf{Z}_2=\{0,1\}$ 是我们研究过的两种命题代数 (即 $\{\neg,\to\}$ 型代数). 现在要在这二者之间建立起适当的联系.

注意 $L(X)$ 与 $\mathbf{Z}_2$ 的差异. $L(X)$ 中的运算对公式实行，而在 $\mathbf{Z}_2$ 中，运算对 0, 1 实行. 在 $L(X)$ 中，按分层性，有 $\neg\neg x_i\neq x_i$, 而在 $\mathbf{Z}_2$ 中总有 $\neg\neg v=v$.

**定义 1 (赋值)** 具有“保运算性”的映射 $v:L(X)\to\mathbf{Z}_2$ 叫做 $L(X)$ 的赋值. 映射 $v$ 具有保运算性，是指对任意 $p,q\in L(X)$, $v$ 满足条件:

(1) $v(\neg p)=\neg v(p)$,

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

对任意公式 $p\in L(X)$, $v(p)$ 叫做 $p$ 的真值. 同样，具有保运算性 (满足 (1), (2)) 的映射 $v:L(X_n)\to\mathbf{Z}_2$ 叫做 $L(X_n)$ 的赋值. ($X_n=\{x_1,\cdots,x_n\}$.)

**命题 1** 设 $v:L(X)\to\mathbf{Z}_2$ 是 $L(X)$ 的赋值，则 $v$ 对 $\vee,\wedge,\leftrightarrow$ 也具有保运算性，即对任意 $p,q\in L(X)$, 有

$$v(p\vee q)=v(p)\vee v(q),\quad v(p\wedge q)=v(p)\wedge v(q),\quad v(p\leftrightarrow q)=v(p)\leftrightarrow v(q).$$

**证**
$$
\begin{aligned}
v(p\vee q) &= v(\neg p\to q) && (1.2.5\text{小节中 }\vee\text{ 的定义})\\
&= v(\neg p)\to v(q) && (\text{保运算性条件(2)})\\
&= \neg v(p)\to v(q) && (\text{保运算性条件(1)})\\
&= v(p)\vee v(q). && (1.3.1\text{小节公式(6)})
\end{aligned}
$$

后两式证法相同. □

**定义 2 (真值指派)** 映射 $v_0:X\to\mathbf{Z}_2$ 叫做命题变元的真值指派. 若把其中 $X$ 换成 $X_n=\{x_1,\cdots,x_n\}$, 则 $v_0$ 叫做 $x_1,\cdots,x_n$ 的真值指派.

**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; $x_1,\cdots,x_n$ 的任一真值指派，必可唯一地扩张成 $L(X_n)$ 的赋值.

**证** 对给定的命题变元的真值指派 $v_0 : X \to \mathbf{Z}_2$, 可归纳定义映射 $v : L(X) \to \mathbf{Z}_2$ 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 $v$ 自然满足赋值所需要的条件 (1), (2) (定义 1 中), 且 $v$ 是 $v_0$ 的扩张.

唯一性: 假设另有 $L(X)$ 的赋值 $v'$ 也是 $v_0$ 的扩张，则对公式 $p$ 在 $L(X)$ 中的层次归纳可证 $v(p) = v'(p)$.

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

$p = \neg q$ 时，有

$$\begin{aligned} v'(p) &= v'(\neg q) \\ &= \neg v'(q) && \text{(赋值条件(1))} \\ &= \neg v(q) && \text{(用归纳假设)} \\ &= v(\neg q) && \text{(赋值条件(1))} \\ &= v(p). \end{aligned}$$

$p = q \to r$ 时，有

$$\begin{aligned} v'(p) &= v'(q \to r) \\ &= v'(q) \to v'(r) && \text{(赋值条件(2))} \\ &= v(q) \to v(r) && \text{(用归纳假设)} \\ &= v(q \to r) && \text{(赋值条件(2))} \\ &= v(p). \end{aligned}$$

至此得 $v' = v$. 定理后一半同样证明. □

常把 $L(X_n)$ 中的任一公式写为 $p(x_1, \cdots, x_n)$. 这样写，并不要求 $x_1, \cdots, x_n$ 的每一个全都一定在 $p(x_1, \cdots, x_n)$ 中出现.

对给定的公式 $p(x_1, \cdots, x_n)$ 及 $v_1, \cdots, v_n \in \mathbf{Z}_2 = \{0, 1\}$, 用 $v_1, \cdots, v_n$ 分别替换 $p(x_1, \cdots, x_n)$ 中对应的 $x_1, \cdots, x_n$ 的全部出现所得结果记为 $p(v_1, \cdots, v_n)$. 这一代换使 $p(x_1, \cdots, x_n)$ 中的运算转化为 $\mathbf{Z}_2$ 中 0, 1 运算，故 $p(v_1, \cdots, v_n) \in \{0, 1\}$. 例如，用 $v_1 = 1, v_2 = 0$ 分别替换公式 $p(x_1, x_2) = (x_1 \to x_2) \to x_1$ 中的 $x_1$(有两处) 与 $x_2$ 得

$$\begin{aligned} p(v_1, v_2) &= (1 \to 0) \to 1 \\ &= 0 \to 1 \\ &= 1. \end{aligned}$$

**命题 2** 设 $m \geqslant n$, $v$ 是 $L(X_m)$ 或 $L(X)$ 的赋值. 若 $v$ 满足 $v(x_1) = v_1, \cdots, v(x_n) = v_n$, 则 $L(X_n)$ 的任一公式 $p(x_1, \cdots, x_n)$ 的真值是

$$v(p(x_1, \cdots, x_n)) = p(v_1, \cdots, v_n),$$

其中 $p(v_1,\cdots,v_n)$ 是用 $v_1,\cdots,v_n$ 分别代换 $p(x_1,\cdots,x_n)$ 中的 $x_1,\cdots,x_n$ 所得的结果.

**证** 对 $p(x_1,\cdots,x_n)$ 在 $L(X_n)$ 中的层次归纳.

先设 $p(x_1,\cdots,x_n)=x_i$, 则 $p(v_i,\cdots,v_n)=v_i$. 此时有

$$v(p(x_1,\cdots,x_n))=v(x_i)=v_i=p(v_1,\cdots,v_n).$$

$p(x_1,\cdots,x_n)=\neg q(x_1,\cdots,x_n)$ 时，有 $p(v_1,\cdots,v_n)=\neg q(v_1,\cdots,v_n)$. 此时

$$\begin{aligned}
v(p(x_1,\cdots,x_n)) &= v(\neg q(x_1,\cdots,x_n)) \\
&= \neg v(q(x_1,\cdots,x_n)) && \text{(赋值的条件(1))} \\
&= \neg q(v_1,\cdots,v_n) && \text{(用归纳假设)} \\
&= p(v_1,\cdots,v_n).
\end{aligned}$$

$p(x_1,\cdots,x_n)=q(x_1,\cdots,x_n)\to r(x_1,\cdots,x_n)$ 时证明类似. □

由命题 2 可知，$L(X_n)$ 的公式 $p(x_1,\cdots,x_n)$ 作为 $L(X)$ 的成员或作为 $L(X_m)$ 的成员 $(m>n)$, 其真值只与它所含有的命题变元的真值指派有关，而与其他变元的真值指派无关.

我们还看到，与其他层次的公式不同，命题变元在命题演算中起着特殊的作用. 对于命题变元，我们可以随意指定真值；这些变元的真值一经指定，凡涉及这些变元的所有公式的真值也都随之唯一确定.

命题演算在表现实际推理的过程中，是用公式来表示命题的. 其中用命题变元来表示任意的简单命题，而用 $L(X)$ 其他层次的公式表示复合命题.

在 1.1 节中我们已经熟悉，可以用真值表的方法由支命题的真假来确定复合命题的真假. 现可在形式系统内将这一方法表述得更明确.

设公式 $p\in L(X_n)$. 给定了这个公式 $p(x_1,\cdots,x_n)$, 便自然地按如下方式确定了一个 $n$ 元真值函数. 任取 $v_1,\cdots,v_n\in\mathbf{Z}_2$, 将 $v_1,\cdots,v_n$ 分别指派给 $x_1,\cdots,x_n$, 然后将此真值指派 (按定理 1) 唯一地扩张成赋值 $v:L(X_n)\to\mathbf{Z}_2$, 这时公式 $p$ 便有了确定的真值 (见命题 2):

$$v(p(x_1,\cdots,x_n))=p(v_1,\cdots,v_n)\in\mathbf{Z}_2.$$

以此值作为对应于 $v_1,\cdots,v_n$ 的函数值，便得到一个由给定公式 $p$ 所确定的真值函数，简称为 $p$ 的真值函数. $p$ 的真值表，就是 $p$ 的真值函数的函数值表.

**例 1** 公式 $(x_1\vee x_2)\to x_1$ 的真值函数，用 $(v_1\vee v_2)\to v_1$ 计算:

| $v_1$ | $v_2$ | $v_1\vee v_2$ | $(v_1\vee v_2)\to v_1$ |
|---|---|---|---|
| 1 | 1 | 1 | 1 |
| 1 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 |
| 0 | 0 | 0 | 1 |

简写以上过程，便得真值表：

| $(x_1$ | $\vee$ | $x_2)$ | $\to$ | $x_1$ |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 | 0 |
| 0 | 0 | 0 | 1 | 0 |

由表看出，(1，1)，(1，0)，(0，0) 是该公式的成真指派，成假指派只有 (0，1).

**例 2** 公式 $(x_1 \vee x_2) \to x_3$ 的真值表是

| $(x_1$ | $\vee$ | $x_2)$ | $\to$ | $x_3$ |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 1 | 0 | 0 |
| 1 | 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 0 | 0 |
| 0 | 1 | 1 | 1 | 1 |
| 0 | 1 | 1 | 0 | 0 |
| 0 | 0 | 0 | 1 | 1 |
| 0 | 0 | 0 | 1 | 0 |

由表看出 $(x_1 \vee x_2) \to x_3$ 的成真指派是 (1，1，1)，(1，0，1)，(0，1，1)，(0，0，1) 和 (0，0，0)，其他指派都是成假指派.

**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 $\vDash p$.

由此定义即知，永真式就是只有成真指派 (没有成假指派) 的公式，换句话说：

$$\vDash p \quad \Leftrightarrow \quad L(X) \text{ 的任何赋值 } v \text{ 都使 } v(p) = 1.$$

按命题 2，若 $p \in L(X_n)$，则上面断言中的 "$L(X)$ 的任何赋值" 可改成 "$L(X_n)$(或 $L(X_m), m \geqslant n$) 的任何赋值".

列出以下公式的真值表，即知它们都是永真式：

$$x_1 \to x_1, \qquad \neg x_1 \vee x_1, \qquad \neg(\neg x_1 \wedge x_1).$$

**定理 2 (代换定理)**

$$\vDash p(x_1, \cdots, x_n) \quad \Rightarrow \quad \vDash p(p_1, \cdots, p_n),$$

其中 $p(x_1, \cdots, x_n) \in L(X_n)$，而 $p_1, \cdots, p_n \in L(X)$；$p(p_1, \cdots, p_n)$ 是用 $p_1, \cdots, p_n$ 分别全部替换 $p(x_1, \cdots, x_n)$ 中的 $x_1, \cdots, x_n$ 所得结果.

**证** 设 $v$ 是 $L(X)$ 的任一赋值. 记

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

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

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

现需证明下面的 (2) 式:

(2) $v(p(p_1,\cdots,p_n))=u(p(x_1,\cdots,x_n)).$

对 $p(x_1,\cdots,x_n)$ 在 $L(X_n)$ 中的层次归纳.

$p(x_1,\cdots,x_n)=x_i$ 时, $p(p_1,\cdots,p_n)=p_i$. 此时由 (1) 式知 (2) 式成立.

当 $p(x_1,\cdots,x_n)$ 形为 $\neg q(x_1,\cdots,x_n)$ 时, 有

$$\begin{aligned}
v(p(p_1,\cdots,p_n)) &= v(\neg q(p_1,\cdots,p_n)) && \\
&= \neg v(q(p_1,\cdots,p_n)) && (v\text{的保运算性})\\
&= \neg u(q(x_1,\cdots,x_n)) && (\text{用归纳假设})\\
&= u(\neg q(x_1,\cdots,x_n)) && (u\text{的保运算性})\\
&= u(p(x_1,\cdots,x_n)).
\end{aligned}$$

当 $p(x_1,\cdots,x_n)$ 形为 $q(x_1,\cdots,x_n)\to r(x_1,\cdots,x_n)$ 时, (2) 式的证明类似.

有了 (2) 便可得

$$\begin{aligned}
\vDash p(x_1,\cdots,x_n) &\Rightarrow u(p(x_1,\cdots,x_n))=1\\
&\Rightarrow v(p(p_1,\cdots,p_n))=1\\
&\Rightarrow \vDash p(p_1,\cdots,p_n).
\end{aligned}$$ □

注意, 定理 2 的逆定理不成立. 原来不是永真式, 经过代换却可能成为永真式. 例如 $x_1\to x_2$ 肯定不是永真式, 但若将其中的 $x_2$ 用公式 $x_2\to x_2$ 去替换, 得到的 $x_1\to(x_2\to x_2)$ 却成了永真式. $x_1\vee x_2$ 肯定不是永真式, 但 $p\vee q$ 却可能是永真式 (例如取 $p,q$ 都为 $x_1$).

定理中的代换只能对命题变元进行代换. 用公式代换某个命题变元, 是指用这个公式对在永真式中出现的该命题变元全部进行替换.

**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** 只证 1°.

由下面的真值表

| $x_1$ | $\to$ | $(x_2 \to x_1)$ |
|---|---|---|
| 1 | 1 | 1 1 1 |
| 1 | 1 | 0 1 1 |
| 0 | 1 | 1 0 0 |
| 0 | 1 | 0 1 0 |

知 $\vDash x_1 \to (x_2 \to x_1)$, 再用代换定理便可. □

设 $p, q, r$ 是 $L$ 的任意公式，以下是常用的永真式.

$\vDash p \to p$, (同一律)

$\vDash \neg p \vee p$, (排中律)

$\vDash \neg(\neg p \wedge p)$, (矛盾律)

$\vDash ((p \vee q) \vee r) \leftrightarrow (p \vee (q \vee r))$, (析取结合律)

$\vDash (p \vee q) \leftrightarrow (q \vee p)$, (析取交换律)

$\vDash ((p \wedge q) \wedge r) \leftrightarrow (p \wedge (q \wedge r))$, (合取结合律)

$\vDash (p \wedge q) \leftrightarrow (q \wedge p)$, (合取交换律)

$\vDash (p \wedge (q \vee r)) \leftrightarrow ((p \wedge q) \vee (p \wedge r))$, (分配律)

$\vDash (p \vee (q \wedge r)) \leftrightarrow ((p \vee q) \wedge (p \vee r))$, (分配律)

$\vDash \neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$,

$\vDash \neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$. (De. Morgan 律)

注意一个事实: 以上这些语义结论都有相应的语法结论. 此事后面还将作深入讨论.

**定义 4 (永假式与可满足公式)** 若 $\neg p$ 是永真式，则 $p$ 叫做永假式. 非永假式叫做可满足公式.

永真式只有成真指派，永假式只有成假指派. 可满足公式一定有成真指派，但也可以有成假指派，也可以没有成假指派. 可满足公式可以是永真式，也可以不是.

**定义 5 (语义推论)** 设 $\Gamma \subseteq L(X)$, $p \in L(X)$. 如果 $\Gamma$ 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 $\Gamma$ 的语义推论，记作 $\Gamma \vDash p$.

换句话说，$\Gamma \vDash p$, 当且仅当 $L(X)$ 的任一赋值 $v$ 具有性质: 每当使任一 $q \in \Gamma$ 都有 $v(q) = 1$ 时，也使 $v(p) = 1$.

由定义 4 立即可得出以下结论.

1° $\varnothing \vDash p \iff L(X)$ 的任一赋值 $v$ 都使 $v(p) = 1$

$\iff \vDash p$ (即 $p$ 是永真式).

2° $p \in \Gamma \Rightarrow \Gamma \vDash p$.

3° $\vDash p \Rightarrow \Gamma \vDash p$, 即永真式是任何公式集 $\Gamma$ 的语义推论.

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

**证** 对于 $L(X)$ 的任一赋值 $v$,

$$\begin{aligned} v(\neg p)=1 &\Rightarrow v(p)=0 \\ &\Rightarrow v(p\to q)=1; \\ v(q)=1 &\Rightarrow v(p\to q)=1. \end{aligned}$$

□

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

**证** 每当 $v(p)=1$ 且 $v(p\to q)=1$ 时，便有

$$\begin{aligned} v(q) &= 1\to v(q) && \text{(1.3.1 小节公式 2)} \\ &= v(p)\to v(q) \\ &= v(p\to q)=1. \end{aligned}$$

□

命题 5 是 MP 规则的语义形式.

**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 $\Gamma$ 中成员的真值都为 1 的赋值. 若有 $v(p)=1$, 则由所设条件可得 $v(q)=1$, 此时 $v(p\to q)=1\to 1=1$. 若有 $v(p)=0$, 则 $v(p\to q)=0\to v(q)=1$. 这就证明了 $\Gamma\vDash p\to q$.

($\Leftarrow$) 设 $\Gamma\vDash p\to q$. 当 $v(p)=1$ 且 $v(p\to q)=1$ 时，必有 $v(q)=1$. 这说明 $\Gamma\cup\{p\}\vDash q$. □

更一般地，有

$$\{p_1,\cdots,p_n\}\vDash p \quad\Leftrightarrow\quad \vDash (p_1\wedge\cdots\wedge p_n)\to p.$$

## 练习 7

1. 试证

   1° 二永真式的合取仍是永真式.

   2° 二永真式的析取仍是永真式.

   3° 后件是永真式的蕴涵式是永真式.

   4° 前件是永假式的蕴涵式是永真式.

2. 下面的公式哪些恒为永真式?

   1° $(p\wedge q)\to p$.

   2° $(p\wedge q)\to q$.

   3° $(q\vee r)\to(\neg r\to q)$.

   4° $(p\wedge\neg q)\vee((q\wedge\neg r)\wedge(r\wedge\neg p))$.

   5° $(p\to(q\to r))\to((p\wedge\neg q)\vee r)$.

3. 以下结论是否正确? 为什么?

1° $\vDash p(x_1,\cdots,x_n) \Leftrightarrow \vDash p(\neg x_1,\cdots,\neg x_n)$.

2° $\vDash (p \to q) \leftrightarrow (p' \to q') \Rightarrow \vDash p \leftrightarrow p'$ 且 $\vDash q \leftrightarrow q'$.

4. 公式 $(\neg x_1 \to x_2) \to (x_1 \to \neg x_2)$ 是永真式吗? 能否找出公式 $p$ 和 $q$ 使$(\neg p \to q) \to (p \to \neg q)$ 是永假式?

# 1.4 命题演算 L 的可靠性与完全性

现在开始讨论命题演算 $L$ 的语法和语义这二者之间的关系，最终证明 $L$ 的重要性质——语法推论和语义推论的一致性:

$$\varGamma \vdash p \quad \Leftrightarrow \quad \varGamma \vDash p.$$

这是我们在着手建立 $L$ 时就希望它能具有的性质. 特殊情况，当 $\varGamma = \varnothing$ 时，上述性质变为

$$\vdash p \quad \Leftrightarrow \quad \vDash p,$$

即: $L$ 中的定理集与永真式集重合.

**定理 1 ($L$ 的可靠性)** $\varGamma \vdash p \quad \Rightarrow \quad \varGamma \vDash p$.

**证** 设 $\varGamma \vdash p$, 则存在 $p$ 从 $\varGamma$ 的证明: $p_1,\cdots,p_n$, 其中 $p_n = p$. 现对此证明的长度 $n$ 归纳证明 $\varGamma \vDash p$.

$n = 1$ 时，$p_1 = p$. 此时 $p$ 或者是 $L$ 的公理，因而是永真式 (1.3.2 小节命题 3)；或者 $p \in \varGamma$. 不管哪种情形出现，都有 $\varGamma \vDash p$.

$n > 1$ 时，如果 $p$ 是 $L$ 的公理，或 $p \in \varGamma$, 这时与 $n = 1$ 时的情形一样，都有 $\varGamma \vDash p$. 还有一种情形是 $p$ 由 MP 得来 (这是一般情形)，即存在 $i, j < n$, 使 $p_j = p_i \to p$. 这时由 $\varGamma \vdash p_i$ 和 $\varGamma \vdash p_j$ 用归纳假设可得 $\varGamma \vDash p_i$ 和 $\varGamma \vDash p_j$, 后者就是 $\varGamma \vDash p_i \to p$. 再用 1.3. 2 小节命题 5 便得 $\varGamma \vDash p$. □

**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 $p$ 同时使 $\vdash p$ 和 $\vdash \neg p$ 成立.

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

下面在证明 $L$ 具有完全性的过程中，要用到完备公式集的概念.

**定义 1 (公式集的完备性)** 设 $\varGamma \subseteq L(X)$. $\varGamma$ 是完备的，意指对任一公式 $p$, $\varGamma \vdash p$ 与 $\varGamma \vdash \neg p$ 必有一个成立.

**定理 2 ($L$ 的完全性)** $\varGamma \vDash p \quad \Rightarrow \quad \varGamma \vdash p$.

**证** 反设 $\varGamma \vdash p$ 不成立. 要做的事情是: 设法构造 $L(X)$ 的一个赋值 $v$, 它使 $\varGamma$ 中所有公式的真值为 1，但使 $v(p) = 0$, 从而与 $\varGamma \vDash p$ 矛盾.

$L(X)$ 是可数集. 把 $L(X)$ 所有的公式排成一列，设为

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

令

$$\Gamma_0 = \Gamma \cup \{\neg p\},$$

而当 $n > 0$ 时，令

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

这样就归纳定义出一列 $\Gamma_n$： $\Gamma_0 \subseteq \Gamma_1 \subseteq \Gamma_2 \subseteq \cdots$.

现对 $n$ 归纳证明每个 $\Gamma_n$ 都是无矛盾的.

首先，$\Gamma_0 = \Gamma \cup \{\neg p\}$ 是无矛盾的，否则由 $\Gamma \cup \{\neg p\} \vdash q$ 及 $\neg q$ 利用反证律便得 $\Gamma \vdash p$, 而我们已假设这是不成立的.

现设 $\Gamma_{n-1}$ 无矛盾，进而证明 $\Gamma_n$ 无矛盾. 假如 $\Gamma_n$ 有矛盾，则存在 $q$ 使

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

这时 $\Gamma_n \neq \Gamma_{n-1}$ (因$\Gamma_{n-1}$ 无矛盾而 $\Gamma_n$ 有矛盾). 于是由 $\Gamma_n$ 的定义式知

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

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

将 (3) 中 $\Gamma_n$ 代入 (1) 左端，用反证律即得 $\Gamma_{n-1} \vdash p_{n-1}$, 这与 (2) 矛盾. 这就证明了每个 $\Gamma_n$ 的无矛盾性.

作

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

$\Gamma^*$ 也是无矛盾的. 这是因为由 $\Gamma^* \vdash q,\ \neg q$ 可得出结论: 对某个充分大的 $n$, $\Gamma_n \vdash q,\ \neg q$ 成立. (注意 1.2.2 小节例 1 之前的结论 6°)

$\Gamma^*$ 具有完备性: 对于 $L(X)$ 的任一公式 $p_n$, $\Gamma^* \vdash p_n$ 与 $\Gamma^* \vdash \neg p_n$ 二者必居其一. 事实上，如果 $\Gamma^* \nvdash p_n$, 那么便有以下结论:

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

$\Gamma_{n+1} = \Gamma_n \cup \{\neg p_n\}$, $\qquad$ (注意 $\Gamma_n$ 的定义式)

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

$\Gamma^*$ 叫做 $\Gamma$ 的无矛盾完备扩张. 利用 $\Gamma^*$ 的无矛盾性和完备性，我们就可以定义一个映射 $v : L(X) \to \mathbf{Z}_2$, 定义式是

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

$v$ 的这个定义是合理的，因为对任一 $L(X)$ 的公式 $q$, $\Gamma^* \vdash q$ 与 $\Gamma^* \vdash \neg q$ 这二者必居其一 (因 $\Gamma^*$ 完备)，且只居其一 (因 $\Gamma^*$ 无矛盾).

下面证明这样定义的 $v$ 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

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

将此式与 $v(q)$ 的定义式比较一下便知

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

为了证明 $v(q\to r)=v(q)\to v(r)$, 分以下两种情形来讨论.

**情形 1** $v(q)\to v(r)=1$. 此时又有两种可能: $v(q)=0$ 或 $v(r)=1$.

$$\begin{aligned}
v(q)=0 \quad &\Rightarrow \Gamma^*\vdash\neg q && \text{(由}v\text{的定义)}\\
&\Rightarrow \Gamma^*\vdash q\to r && \text{(由否定前件律}\neg q\to(q\to r))\\
&\Rightarrow v(q\to r)=1, && \text{(由}v\text{的定义)}\\
v(r)=1 \quad &\Rightarrow \Gamma^*\vdash r && \text{(由}v\text{的定义)}\\
&\Rightarrow \Gamma^*\vdash q\to r && (r\to(q\to r)\text{是(L1)型公理})\\
&\Rightarrow v(q\to r)=1. && \text{(由}v\text{的定义)}
\end{aligned}$$

**情形 2** $v(q)\to v(r)=0$. 此时有

$$\begin{aligned}
&v(q)=1 \text{ 且 } v(r)=0, &&\\
&\Gamma^*\vdash q \text{ 且 } \Gamma^*\vdash\neg r, && \text{(由 }v\text{ 的定义)}\\
&\Gamma^*\vdash\neg(q\to r), && \text{(见 1.2.4 例 2)}\\
&v(q\to r)=0. && \text{(由 }v\text{ 的定义)}
\end{aligned}$$

总之，不管情形 1 还是情形 2，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.

最后我们可以看到，对赋值 $v$ 来说，$\Gamma$ 中公式的真值皆为 1:

$$\begin{aligned}
q\in\Gamma \ &\Rightarrow\ q\in\Gamma^*\\
&\Rightarrow\ \Gamma^*\vdash q\\
&\Rightarrow\ v(q)=1.
\end{aligned}$$

但与此同时，因 $\neg p\in\Gamma_0\subseteq\Gamma^*$, 故有 $\Gamma^*\vdash\neg p$, 进而有 $v(p)=0$. 这个 $v$ 就是我们所要找的赋值，它使 $\Gamma$ 中公式为真而使 $p$ 为假. 这种 $v$ 的存在说明 $\Gamma\vDash p$ 不成立. □

回顾定理 2 的证明过程，关键是把无矛盾公式集 $\Gamma_0$ 扩张成完备的公式集 $\Gamma^*$. 我们看见，过程中包含了下面重要结论的证明:

**命题** * 无矛盾公式集必有无矛盾的完备扩张.

下面来讨论命题演算 $L$ 的可判定性.

1° $L$ 的语义可判定性

我们说命题演算 $L$ 是语义可判定的，意思是说存在着算法可用来确定 $L$ 中任

给的公式 $p(x_1,\cdots,x_n)$ 是不是永真式.

这样的算法是存在的: 任给 $L$ 中的公式 $p(x_1,\cdots,x_n)$, 我们来一一计算它的真值函数的函数值 $p(v_1,\cdots,v_n)$, 如果对所有 $v_1,\cdots,v_n\in\mathbf{Z}_2$ 都有 $p(v_1,\cdots,v_n)=1$ (即真值表的最后一列全为 1), 则 $p$ 是永真式, 否则 $p$ 不是永真式.

2° $L$ 的语法可判定性

我们说 $L$ 是语法可判定的, 是指存在算法可用以确定 $L$ 的任意公式 $p$ 是不是 $L$ 的定理.

这样的算法是存在的: 根据 $L$ 的可靠性和完全性, 看公式 $p$ 是不是定理, 就看它是不是永真式.

以上讨论说明, $L$ 的语义可判定导致了 $L$ 的语法可判定.

如果世上所有的推理过程都能在命题演算 $L$ 的框架内得到形式化, 那么从理论上来说, 莱布尼茨通过计算解决争论的愿望就完全实现了, 但可惜并非人类所进行的全部推理都能在 $L$ 中形式化. 我们还需要建立比 $L$ 更细致的数学模型.

**练习 8**

1. 求证

$$\vdash p(x_1,\cdots,x_n) \quad\Rightarrow\quad \vdash p(p_1,\cdots,p_n),$$

其中 $p_1,\cdots,p_n$ 是任意的公式.

2. (紧致性定理) 求证, 若 $\Gamma\vDash p$, 则定有 $\Gamma$ 的有限子集 $\Sigma$ 使 $\Sigma\vDash p$.

# 1.5 命题演算的其他课题

## 1.5.1 等值公式与对偶律

不同的公式可能有相同的真值函数. 例如 $\neg x_1\wedge\neg x_2, \neg(x_1\vee x_2)$ 和 $\neg(\neg x_1\to x_2)$ 这三个公式的真值函数是相同的:

$$\neg v_1\wedge\neg v_2=\neg(v_1\vee v_2)=\neg(\neg v_1\to v_2).$$

可以看出, 以下三句话的意思是相同的:

"数 $a$ 既不大于零, 也不等于零";

"数 $a$ 不是大于零或等于零的";

"并非如此: 数 $a$ 不大于零时便等于零".

**定义 1 (等值公式)** $p$ 与 $q$ 等值, 是指 $p\leftrightarrow q$ 为永真式.

由此定义及永真式的定义立即可知, 当 $p,q\in L(X_n)$ 时,

$$
\begin{aligned}
& p \text{ 与 } q \text{ 等值 (即} \vDash p \leftrightarrow q) \\
\Leftrightarrow\ & L(X_n) \text{ 的任一赋值 } v \text{ 都使 } v(p) = v(q) \\
\Leftrightarrow\ & L(X) \text{ 的任一赋值 } v \text{ 都使 } v(p) = v(q) \\
\Leftrightarrow\ & p \text{ 与 } q \text{ 有相同的成真指派和成假指派} \\
\Leftrightarrow\ & p \text{ 与 } q \text{ 有相同的真值函数} \\
\Leftrightarrow\ & \text{对 } x_1, \cdots, x_n \text{ 的任何指派 } v_1, \cdots, v_n, \text{ 都有} \\
& \qquad p(v_1, \cdots, v_n) = q(v_1, \cdots, v_n).
\end{aligned}
$$

由定义 1 还立即可得

**命题 1** 1° $\vDash p \leftrightarrow p$; (等值的反身性)

2° $\vDash p \leftrightarrow q \ \Rightarrow\ \vDash q \leftrightarrow p$; (等值的对称性)

3° $\vDash p \leftrightarrow q$ 及 $\vDash q \leftrightarrow r \ \Rightarrow\ \vDash p \leftrightarrow r$. (等值的可递性)

命题 1 指出，等值所确定的 $L(X)$ 上的二元关系是等价关系，从而给出了 $L(X)$ 的一个分类. 同样，也给出了 $L(X_n)$ 的分类. 互相等值的公式属于同一等价类. 同一类中的等值公式有同一个真值函数.

不同的 $n$ 元真值函数总共有 $2^{2^n}$ 种. 这意味着 $L(X_n)$ 中有 $2^{2^n}$ 种不同的等价类. 这也就是说，尽管 $L(X_n)$ 中有无穷多个公式，但本质上语义不同的公式只有 $2^{2^n}$ 种.

永真式有无穷多个，它们构成了一个等价类. 所有永假式 (也有无穷多个) 则构成另一等价类. 任一公式 $p$ 与以下形式的公式

$$p \wedge (\text{永真式}), \quad p \vee (\text{永假式})$$

都是互相等值的，因此属于同一等价类. 这说明每个等价类中都会有无穷多个互相等值的公式.

下面讨论等值公式的替换问题.

**命题 2** 1° $\vDash p \leftrightarrow q \ \Rightarrow\ \vDash \neg p \leftrightarrow \neg q$;

2° $\vDash p \leftrightarrow p'$ 且 $\vDash q \leftrightarrow q' \ \Rightarrow\ \vDash (p \to q) \leftrightarrow (p' \to q')$.

**证** 设 $v$ 是 $L(X)$ 的任一赋值.

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

2° $v(p) = v(p')$ 及 $v(q) = v(q') \ \Rightarrow$

$$v(p \to q) = v(p) \to v(q) = v(p') \to v(q') = v(p' \to q'). \qquad \square$$

我们用 $p = \cdots q \cdots$ 表示 $q$ 是公式 $p$ 的子公式. 此时 $q$ 是 $p$ 的组成部分，但 $q$ 本身也是公式. ($p$ 最长的子公式是 $p$ 自己.) 作为 $p$ 的子公式，$q$ 如果不是 $p$ 本身，则在 $L(X)$ 中的层次比 $p$ 所在的层次低.

**定理 1 (子公式等值可替换性)**

设 $q$ 是 $p$ 的子公式: $p = \cdots q \cdots$, 用公式 $q'$ 替换 $p$ 中的子公式 $q$ (一处替换) 所得结果记为 $p' = \cdots q' \cdots$. 那么

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

**证** 对 $p$ 在 $L(X)$ 中的层次归纳.

$p$ 是命题变元时，只能 $p = q$, 因而 $p' = q'$, 结论成立.

若 $p$ 所在层次数大于零，则有两种可能的情形.

情形 1 $p = \neg r$

因最后的运算是 $\neg$, 故可设 $q$ 为 $r$ 的子公式. 这时 $p' = \neg r', r'$ 是用 $q'$ 替换 $r$ 中的子公式 $q$ 得来. 于是

$$\vDash r \leftrightarrow r' \qquad \text{(归纳假设)}$$

$$\vDash \neg r \leftrightarrow \neg r' \qquad \text{(命题 } 2-1°\text{)}$$

情形 2 $p = r \to s$

因形成 $p$ 的最后一次运算是 $\to$, 这时设 $q$ 或是 $r$ 的子公式，或是 $s$ 的子公式，于是 $p' = r' \to s$ 或 $p' = r \to s'$. 由归纳假设，$\vDash r \leftrightarrow r'$ 或 $\vDash s \leftrightarrow s'$. 利用命题 $2-2°$, 便有 $\vDash (r \to s) \leftrightarrow (r' \to s)$ 或 $\vDash (r \to s) \leftrightarrow (r \to s')$. 总之，有 $\vDash p \leftrightarrow p'$. □

定理 1 中的替换指的是一处替换. 若要多处替换，则可用定理若干次.

因为有析取结合律，所以可把 $(p_1 \vee p_2) \vee p_3$ 简写成 $p_1 \vee p_2 \vee p_3$, 把 $((p_1 \vee p_2) \vee p_3) \vee p_4$ 简写成 $p_1 \vee p_2 \vee p_3 \vee p_4$, 等等. 对于合取 $\wedge$, 也有同样的做法.

作为一例，根据定理 1，由 $\vDash \neg\neg x_2 \leftrightarrow x_2$ 可断言

$$\vDash (\neg x_1 \wedge \neg\neg x_2 \wedge \neg x_3) \leftrightarrow (\neg x_1 \wedge x_2 \wedge \neg x_3).$$

**定义 2 (公式的对偶)** 设公式 $p$ 已被写成只含有命题变元和运算 $\neg, \vee, \wedge$ 的形式. 把 $p$ 中的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 $p^*$ 叫做公式 $p$ 的对偶.

例如，$p = (x_1 \vee \neg x_2) \wedge x_3$ 的对偶是

$$p^* = (\neg x_1 \wedge \neg\neg x_2) \vee \neg x_3.$$

**定理 2 (对偶律)** $\vDash p^* \leftrightarrow \neg p$, 其中 $p^*$ 是 $p$ 的对偶.

**证** 对 $p$ 中 $\neg, \vee, \wedge$ 出现的总次数 $n$ 归纳.

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

$n > 0$ 时，有以下三种情形.

情形 1 $p = \neg q$. 此时 $p^* = \neg q^*$. $q$ 中运算 $\neg, \vee, \wedge$ 出现的次数为 $n - 1$, 由归纳假设有 $\vDash q^* \leftrightarrow \neg q$. 再对此用命题 $2-1°$, 得 $\vDash \neg q^* \leftrightarrow \neg\neg q$, 此即 $\vDash p^* \leftrightarrow \neg p$.

情形 2 $p = q \vee r$. 此时 $p^* = q^* \wedge r^*$. 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

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

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

再由 De. Morgan 律得

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

由以上三式及等值的可递性便得 $\vDash (q^* \wedge r^*) \leftrightarrow \neg (q \vee r)$, 此即 $\vDash p^* \leftrightarrow \neg p$.

情形 3　$p = q \wedge r$. 此时 $p^* = q^* \vee r^*$. 与情形 2 的讨论类似，可得 $\vDash (q^* \vee r^*) \leftrightarrow \neg (q \wedge r)$, 此即 $\vDash p^* \leftrightarrow \neg p$. □

**推论 (推广的 De. Morgan 律)**

1° $\vDash (\neg p_1 \vee \cdots \vee \neg p_n) \leftrightarrow \neg (p_1 \wedge \cdots \wedge p_n)$;

2° $\vDash (\neg p_1 \wedge \cdots \wedge \neg p_n) \leftrightarrow \neg (p_1 \vee \cdots \vee p_n)$,

其中 $p_1, \cdots, p_n$ 是任意公式.

**证**　只证 1°. 由代换定理，只用证

$$\vDash (\neg x_1 \vee \cdots \vee \neg x_n) \leftrightarrow \neg (x_1 \wedge \cdots \wedge x_n),$$

而这是定理 2 当 $p = x_1 \wedge \cdots \wedge x_n$ 时的特例. □

推广的 De. Morgan 律以后仍称为 De. Morgan 律，常写成

1° $\vDash \bigvee_{i=1}^{n} \neg p_i \leftrightarrow \neg \bigwedge_{i=1}^{n} p_i$;

2° $\vDash \bigwedge_{i=1}^{n} \neg p_i \leftrightarrow \neg \bigvee_{i=1}^{n} p_i$.

在进行语义分析的时候，往往需要对公式进行等值变换，以便使这种分析更容易进行. 通过等值变换，可使新公式具有我们所希望的逻辑结构. 例如，可利用 $\neg p \vee q$ 与 $p \to q$ 的等值而消去 $\to$, 使新的公式只含有 $\neg, \vee, \wedge$. 以上定理和命题提供了对公式进行等值变换的工具.

## 练习 9

1. 证明以下各对公式是等值的.

   1° $p \to q$ 和 $\neg q \to \neg p$.

   2° $(\neg p \wedge \neg q) \to \neg r$ 和 $r \to (q \vee p)$.

   3° $(\neg p \vee q) \to r$ 和 $(p \wedge \neg q) \vee r$.

   4° $\neg(\neg p \vee q) \vee r$ 和 $(p \to q) \to r$.

2. 证明 $\neg(x_1 \vee \neg x_2) \to (x_2 \to x_3)$ 与以下公式都等值.

   1° $\neg(x_2 \to x_1) \to (\neg x_2 \vee x_3)$.

   2° $(\neg x_1 \wedge x_2) \to \neg(x_2 \wedge \neg x_3)$.

3° $\neg(\neg x_2 \vee x_3) \to (x_2 \to x_1)$.

4° $x_2 \to (x_1 \vee x_3)$.

3. 设公式 $p$ 与 $q$ 都已写成只含有命题变元和 $\neg, \vee, \wedge$ 三种运算. 把 $p$ 和 $q$ 中所有 $\vee$ 改为 $\wedge$, $\wedge$ 改为 $\vee$, 分别得到 $p^d$ 和 $q^d$. 证明

$$\vDash p \leftrightarrow q \quad \Rightarrow \quad \vDash p^d \leftrightarrow q^d.$$

### 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 $y_1 \vee y_2 \vee \cdots \vee y_n$ 和形为 $y_1 \wedge y_2 \wedge \cdots \wedge y_n$ 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.

任给一个基本析取式，很容易判定它是不是永真式，这只要看式中是否有某个 $x_k$ 和 $\neg x_k$ 同时出现. 如果式中有这样一对同时出现，那么该式就是永真式；否则就不是永真式 (可以很快找出它的成假指派). 例如，$x_1 \vee \neg x_2 \vee \neg x_1$ 是永真式. $x_1 \vee \neg x_2 \vee x_3$ 不是永真式，因为它有成假指派 (0，1，0) (这是它唯一的成假指派).

同样，任给一个基本合取式，很容易鉴别它是否是永假式. 如果式中同时出现某个 $x_k$ 和 $\neg x_k$，则为永假式；否则就是可满足公式 (可以很容易指出它的成真指派). 例如 $\neg x_1 \wedge x_2 \wedge \neg x_2$ 是永假式，$\neg x_1 \wedge x_2 \wedge x_3$ 是可满足公式，因为它有成真指派 (0，1，1) (这是它唯一的成真指派). 注意，一个基本析取式只可能有唯一的一个成假指派. 同样，一个基本合取式只可能有一个成真指派.

**定义 2 (析取范式与合取范式)** 形为 $\bigvee_{i=1}^{m}(\bigwedge_{j=1}^{n_i} y_{ij})$ 的公式叫做析取范式，形为 $\bigwedge_{i=1}^{m}(\bigvee_{j=1}^{n_i} y_{ij})$ 的公式叫做合取范式，其中每个 $y_{ij}$ 是某个命题变元 $x_k$ 或它的否定 $\neg x_k$.

换句话说，析取范式就是以若干基本合取式为析取支的析取式；合取范式就是以若干基本析取式为合取支的合取式. 例如，公式

$$(x_1 \wedge \neg x_3) \vee (x_3 \wedge x_1 \wedge \neg x_2) \vee (x_5 \wedge x_4 \wedge \neg x_1)$$

是析取范式，公式

$$(x_1 \vee \neg x_3) \wedge (x_2 \vee x_1 \vee \neg x_2) \wedge (x_5 \vee x_4 \vee \neg x_1)$$

是合取范式. 公式

$$x_1 \wedge \neg x_2 \wedge x_3$$

既是析取范式，又是合取范式. 作为析取范式，它只有一个析取支；作为合取范式，它有三个合取支.

可以快速判定任一析取范式是不是永假式. 这只要扫描一遍就可以了：每个析

取支都是基本合取式，一看便知它们是不是永假式. 原析取范式是永假式，当且仅当每个析取支都是永假式. 但是，要想判定任一析取范式是不是永真式，当命题变元数目多时，则比较麻烦.

相反，可以快速判定任一合取范式是不是永真式，因为每个合取支都是基本析取式，容易确定它们是不是永真式. 合取范式是永真式，当且仅当它的每个合取支都是永真式. 同样，要想判定任一合取范式是不是永假式，当命题变元数目多时，则比较麻烦.

给一个公式，要找出与它等值的析取范式或合取范式，大致可采取以下步骤.

1° 消去 $\rightarrow$ 与 $\leftrightarrow$. 先用

$$p \leftrightarrow q = (p \rightarrow q) \wedge (q \rightarrow p) \quad (1.2.5\text{ 小节中 } \leftrightarrow \text{ 的定义})$$

消去 $\leftrightarrow$, 再用 $\vDash (p \rightarrow q) \leftrightarrow (\neg p \vee q)$ 消去 $\rightarrow$.

2° 把否定号 $\neg$ 等值变换到命题变元之前. 这要用到以下几个等值式:

$$\vDash \neg(p \vee q) \leftrightarrow \neg p \wedge \neg q,$$
$$\vDash \neg(p \wedge q) \leftrightarrow \neg p \vee \neg q,$$
$$\vDash \neg\neg p \leftrightarrow p.$$

3° 利用交换律、结合律及分配律作等值变换，直到得出所需要的形式为止.

**例 1** 求与 $(x_1 \wedge (x_2 \rightarrow x_3)) \rightarrow x_2$ 等值的析取范式与合取范式.

**解** 以下各公式与原公式等值:

$$\neg(x_1 \wedge (\neg x_2 \vee x_3)) \vee x_2, \qquad (\text{消去} \rightarrow)$$
$$\neg x_1 \vee \neg(\neg x_2 \vee x_3) \vee x_2,$$
$$\neg x_1 \vee (\neg\neg x_2 \wedge \neg x_3) \vee x_2,$$
$$\neg x_1 \vee (x_2 \wedge \neg x_3) \vee x_2.$$

后式是与原式等值的析取范式. 再继续作等值变换:

$$\neg x_1 \vee x_2 \vee (x_2 \wedge \neg x_3), \qquad (\text{用了交换律})$$
$$(\neg x_1 \vee x_2 \vee x_2) \wedge (\neg x_1 \vee x_2 \vee \neg x_3), \qquad (\text{分配律})$$
$$(\neg x_1 \vee x_2) \wedge (\neg x_1 \vee x_2 \vee \neg x_3). \qquad (\text{用了} \vDash (x_2 \vee x_2 \leftrightarrow x_2))$$

最后两式都是与原式等值的合取范式.

**定义 3 (主析取范式与主合取范式)** $L(X)$ 中的主析取范式是这样的析取范式，在它的每个析取支中，每个命题变元 $x_1, \cdots, x_n$ (带否定号或不带否定号) 按下标由小到大的次序都出现且都只出现一次. 主合取范式同样定义，只用把“每个析取支”改为“每个合取支”.

**定理 1** 每个非永假式必有与它等值的主析取范式.

**证** 设 $p = p(x_1, \cdots, x_n)$ 不是永假式，那么它有成真指派. 令 $p$ 的所有成真指派

(最多有 $2^n$ 个) 为

$$(v_1, v_2, \cdots, v_n),\ \cdots,$$

一一作出分别与这些成真指派对应的基本合取式

$$y_1 \wedge y_2 \wedge \cdots \wedge y_n,\ \cdots.$$

作的方法是，令

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

(这样做的目的是使 $(v_1, v_2, \cdots, v_n)$ 也是 $y_1 \wedge y_2 \wedge \cdots \wedge y_n$ 的成真指派，而且是 $y_1 \wedge y_2 \wedge \cdots \wedge y_n$ 唯一的成真指派.) 最后，以每个这样的基本合取式为析取支，全部拿来作成析取式

$$q = (y_1 \wedge y_2 \wedge \cdots \wedge y_n) \vee (\cdots) \vee \cdots,$$

于是 $q$ 为所求的主析取范式. 这是因为: 第一，$q$ 的每个析取支中，每个 $x_i$ 按下标由小到大的次序都出现且都只出现一次；第二，$q$ 与 $p$ 有相同的真值函数，因而等值. 事实上，任给 $(v_1, \cdots, v_n) \in \mathbf{Z}_2^n$,

(i) 若 $p(v_1, \cdots, v_n) = 1$, 即 $(v_1, \cdots, v_n)$ 是 $p$ 的成真指派，这时按上面 $q$ 的做法，$q$ 有一析取支 $y_1 \wedge \cdots \wedge y_n$ 与 $(v_1, \cdots, v_n)$ 对应，$(v_1, \cdots, v_n)$ 也是 $y_1 \wedge \cdots \wedge y_n$ 的成真指派. 于是 $q(v_1, \cdots, v_n) = 1$.

(ii) 若 $p(v_1, \cdots, v_n) = 0$, 这时 $(v_1, \cdots, v_n)$ 不是 $p$ 的成真指派，因而不是 $q$ 的任何析取支的成真指派，故 $q(v_1, \cdots, v_n) = 0$. □

定理 1 的证明过程提供了主析取范式的一种求法.

**例 2** 求 $x_1 \to x_2$ 的等值主析取范式.

**解** $x_1 \to x_2$ 的成真指派是 (1, 1), (0, 1), (0, 0). 按定理 1 证明中指出的方法，先分别写出与三个成真指派相对应的基本合取式: $x_1 \wedge x_2, \neg x_1 \wedge x_2, \neg x_1 \wedge \neg x_2$, 然后以它们为析取支构成析取范式，便得所求:

$$(x_1 \wedge x_2) \vee (\neg x_1 \wedge x_2) \vee (\neg x_1 \wedge \neg x_2).$$

**定理 2** 每个非永真式必等值于一主合取范式.

**证** $p$ 为非永真式，则 $\neg p$ 为非永假式. 由定理 1 知 $\neg p$ 有等值的主析取范式，设为

$$\bigvee_{i=1}^{m} \Big( \bigwedge_{j=1}^{n} y_{ij} \Big).$$

于是 $p$ 等值于

$$\neg\left(\bigvee_{i=1}^{m}\left(\bigwedge_{j=1}^{n} y_{ij}\right)\right) \quad 和 \quad \bigwedge_{i=1}^{m}\left(\bigvee_{j=1}^{n} \neg y_{ij}\right).$$

把后式中所有出现的 $\neg\neg x_k$ 换成 $x_k$，便得到所求的主合取范式. □

注意，永假式没有等值主析取范式，永真式没有等值主合取范式. 这是因为主析取范式有成真指派，而主合取范式有成假指派.

**例 3** 求 $p = (x_1 \to x_2) \to x_3$ 的等值主析取范式和等值主合取范式.

**解** $p$ 的成真指派是

$$(1,1,1),\ (1,0,1),\ (1,0,0),\ (0,1,1),\ (0,0,1).$$

$\neg p$ 的成真指派是

$$(1,1,0),\ (0,1,0),\ (0,0,0).$$

$p$ 的等值主析取范式是

$$(x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge \neg x_2 \wedge x_3) \vee (x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (\neg x_1 \wedge x_2 \wedge x_3) \vee (\neg x_1 \wedge \neg x_2 \wedge x_3).$$

$\neg p$ 的等值主析取范式是

$$(x_1 \wedge x_2 \wedge \neg x_3) \vee (\neg x_1 \wedge x_2 \wedge \neg x_3) \vee (\neg x_1 \wedge \neg x_2 \wedge \neg x_3),$$

由此得 $p$ 的等值主合取范式是

$$(\neg x_1 \vee \neg x_2 \vee x_3) \wedge (x_1 \vee \neg x_2 \vee x_3) \wedge (x_1 \vee x_2 \vee x_3).$$

## 练习 10

1. 求以下公式的等值主析取范式.

   1° $x_1 \leftrightarrow x_2$.

   2° $x_1 \to (\neg x_2 \vee x_3)$.

   3° $(x_1 \wedge x_2) \vee (\neg x_2 \leftrightarrow x_3)$.

   4° $\neg((x_1 \to \neg x_2) \to x_3)$.

   5° $((x_1 \to x_2) \to x_3) \to x_4$.

2. 求以下公式的等值主合取范式.

   1° $(\neg x_1 \vee x_2) \to x_3$.

   2° $x_1 \leftrightarrow x_2$.

   3° $(x_1 \wedge x_2 \wedge x_3) \vee (\neg x_1 \wedge \neg x_2 \wedge x_3)$.

   4° $((x_1 \to x_2) \to x_3) \to x_4$.

### 1.5.3　运算的完全组

1.5.1 小节中已经指出，等值关系是公式集 $L(X)$ 上的一个等价关系，它确定了 $L(X)$ 的一个分类，每个等价类中的公式有共同的语义性质——它们的真值函数相同. 所以从语义上来说，对 $L(X)$ 的研究本质上可化为对真值函数的研究.

**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.

按此定义，1.3.1 小节中命题 1 (任一真值函数都可用 $\neg$ 和 $\rightarrow$ 表示) 可改述为"$\{\neg\ \rightarrow\}$ 是完全组".

**命题 1**　$\{\neg, \vee\}$ 和 $\{\neg, \wedge\}$ 都是运算完全组.

**证**　对任意 $u, v \in \mathbf{Z}_2$, 有恒等式

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

前式说明涉及"$\rightarrow$"的运算都可用 $\neg$ 和 $\vee$ 来代替，后式则说明可用 $\neg$ 和 $\wedge$ 来代替. 这样，由 $\{\neg, \rightarrow\}$ 的完全性便可推出 $\{\neg, \vee\}$ 及 $\{\neg, \wedge\}$ 的完全性. □

$\mathbf{Z}_2$ 和 $L(X)$ 都是 $\{\neg, \rightarrow\}$ 型代数，都可用基本运算 $\neg$ 与 $\rightarrow$ 来定义其他运算. $\mathbf{Z}_2$ 上的每种运算都对应着 $L(X)$ 上的用相同符号表示的同名运算. 于是与命题 1 相对应，有关于 $L(X)$ 的命题:

"任一公式必等值于一个只含命题变元及 $\neg, \vee$ 两种运算的公式，且必等值于另一个只含命题变元及 $\neg, \wedge$ 两种运算的公式."

同样，关于 $\mathbf{Z}_2$ 的其他这类命题也都有相应的关于 $L(X)$ 的命题.

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

**证**　先证命题 $*$:

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 $f(1) = 1$.

对表示 $f$ 所用的上述四种运算的次数 $k$ 归纳.

$k = 0$ 时，$f(v) = v$, 故 $f(1) = 1$.

$k > 0$ 时，有以下四种可能的情况:

(i) $f(v) = g(v) \vee h(v)$,

(ii) $f(v) = g(v) \wedge h(v)$,

(iii) $f(v) = g(v) \rightarrow h(v)$,

(iv) $f(v) = g(v) \leftrightarrow h(v)$.

这四种情况中不管哪一种发生，都有 $f(1) = 1$, 因为由归纳假设，$g(1) = h(1) = 1$. 这就证明了命题 $*$.

现取 $f$ 为恒取零值的一元常值函数，有 $f(1) = 0$. 根据命题 $*$, $f$ 不能只由 $\vee, \wedge, \rightarrow, \leftrightarrow$ 这四种运算表示出来. □

相应于命题 2 的关于 $L(X)$ 的命题是:

"存在着这样的公式，它不与任何只含命题变元及 $\vee,\wedge,\to,\leftrightarrow$ 四种运算的公式等值."

命题 2 说明了否定运算"$\neg$"在命题代数中具有重要的特殊地位. 它所起的特殊作用是不能用 $\vee,\wedge,\to,\leftrightarrow$ 这四种 (甚至更多的) 运算可以代替的. 这种特殊作用正是"否定"这个概念在哲学中所起的重要作用的一种逻辑表现.

光有否定运算也不行. 因为

**命题 3** $\{\neg,\leftrightarrow\}$ 不是完全组.

**证** 假设二元真值函数 $f$ 可用 $\neg$ 和 $\leftrightarrow$ 这两种运算表示. 现对表示 $f$ 所用运算 $\neg$ 和 $\leftrightarrow$ 的次数 $k$ 归纳证明 $f$ 具有这样的性质:

"$f(1,1)$, $f(1,0)$, $f(0,1)$, $f(0,0)$ 这四个数中，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，

$$g(1,1),\ g(1,0),\ g(0,1),\ g(0,0)$$

四个数中以及

$$h(1,1),\ h(1,0),\ h(0,1),\ h(0,0)$$

四个数中，1 都出现偶数次. 分别对不同情况进行简单的计算，便知

$$f(1,1), f(1,0),\ f(0,1),\ f(0,0)$$

这四个数中 1 也出现偶数次.

二元真值函数 $\vee$ 和 $\wedge$ 没有上述性质. 例如 $1\vee 1$, $1\vee 0$, $0\vee 1$, $0\vee 0$ 这四个数中有三个 1. 这说明 $\vee$ 和 $\wedge$ 不能只用 $\neg,\leftrightarrow$ 两种运算表示，所以 $\{\neg,\leftrightarrow\}$ 不是完全组. □

**推论 1** 独元集 $\{\neg\}$ 不是完全组.

**推论 2** $\{\neg,\nleftrightarrow\}$ 不成完全组，其中 $\nleftrightarrow$ 是如下规定的:

| $v_1$ | $v_2$ | $v_1 \nleftrightarrow v_2$ |
|---|---|---|
| 1 | 1 | 0 |
| 1 | 0 | 1 |
| 0 | 1 | 1 |
| 0 | 0 | 0 |

**证** 因 $v_1\leftrightarrow v_2=\neg(v_1\nleftrightarrow v_2)$, 故若 $\{\neg,\nleftrightarrow\}$ 是完全组，则 $\{\neg,\leftrightarrow\}$ 也是完全组. □

“$\nleftrightarrow$”作为 $L(X)$ 运算 (定义式是 $p \nleftrightarrow q = \neg(p \leftrightarrow q)$) 解释为“不可兼或”:

$$p \nleftrightarrow q \text{ 为真} \quad \Leftrightarrow \quad p \text{ 和 } q \text{ 二者必有且只有一个为真}.$$

注意 $\{\neg, \nleftrightarrow\}$ 不是完全组，而 $\{\neg, \vee\}$ 是完全组. 这是我们用“$\vee$”表示“或”而不用“$\nleftrightarrow$”表示“或”的原因之一.

**定义 2 (“与非”运算和“或非”运算)** 与非运算用算符“|”表示，或非运算用算符“$\downarrow$”表示；他们的定义式分别是

$$v_1 \mid v_2 = \neg(v_1 \wedge v_2),$$

$$v_2 \downarrow v_2 = \neg(v_1 \vee v_2).$$

由计算可得

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

**命题 4** 独元集 $\{|\}$ 和独元集 $\{\downarrow\}$ 都是完全组.

**证** 对任意 $v_1, v_2 \in \boldsymbol{Z}_2$, 有等式 (证明留作练习):

$$\neg v_1 = v_1 \mid v_1 = v_1 \downarrow v_1,$$

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

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

利用 $\{\neg, \vee\}$ 和 $\{\neg, \wedge\}$ 的完全性，命题得证. □

在 $L(X)$ 中令

$$p \mid q = \neg(p \wedge q),$$

$$p \downarrow q = \neg(p \vee q).$$

相应于命题 4，有关于 $L(X)$ 的命题:

“$L(X)$ 中任一公式都必和一个由命题变元经一种运算 | (或 $\downarrow$) 得到的公式等值.”

与非算符“|”叫做 Sheffer 竖.

**例 1** 分别找出与 $x_1 \to x_2$ 及 $x_1 \to (x_2 \to x_1)$ 等值的只含 $x_1, x_2$ 及运算 | 的公式.

**解** $x_1 \to x_2$ 与 $\neg x_1 \vee x_2$ 等值，又与 $\neg(x_1 \wedge \neg x_2)$ 即 $x_1 \mid \neg x_2$ 等值，所以与 $x_1 \mid (x_2 \mid x_2)$ 等值. 由此便知 $x_1 \to (x_2 \to x_1)$ 与下面的公式等值:

$$x_1 \mid ((x_2 \mid (x_1 \mid x_1)) \mid (x_2 \mid (x_1 \mid x_1))).$$

此例说明，只用一种运算，往往使公式的表示更冗长，更不直观.

**命题 5** 除 $|$, $\downarrow$ 外，没有其他二元运算单独构成完全组.

**证** 先将全部 16 种二元运算列出如下:

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

$f_9$ 就是 $|$, $f_{15}$ 就是 $\downarrow$. 对其余二元运算分成三类进行讨论.

(i) $\{f_1, f_2, \cdots, f_8\}$ 不是完全组，证明与命题 2 的证明完全一样. (这里的 $f_2, f_5, f_7, f_8$ 分别就是 $\vee, \rightarrow, \leftrightarrow, \wedge$).

(ii) $\{f_{11}, f_{13}\}$ 不是完全组，这是因为，对于任意 $v_1, v_2 \in \mathbf{Z}_2$, 有

$$f_{11}(v_1, v_2) = \neg v_2,$$

$$f_{13}(v_1, v_2) = \neg v_1.$$

如果 $\{f_{11}, f_{13}\}$ 是完全组，那么 $\{\neg\}$ 也成了完全组，与推论 1 矛盾.

(iii) $\{f_{10}, f_{12}, f_{14}, f_{16}\}$ 不是完全组，证明过程与命题 2 的类似，区别仅在于先证明一个稍有不同的命题 $*$:

“任一一元真值函数 $f: \mathbf{Z}_2 \rightarrow \mathbf{Z}_2$ 若能用 $f_{10}, f_{12}, f_{14}, f_{16}$ 这四种运算表示，则恒有 $f(0) = 0$.”

恒等于 1 的一元常值函数不具有这种性质，故不能仅由这四种运算来表示. □

本段关于真值函数的结论除了有相应的命题逻辑的解释，还有相应的电路理论的解释.

## 练习 11

1. 证明等式

$$\neg v_1 = v_1 \mid v_1 = v_1 \downarrow v_1,$$
$$v_1 \vee v_2 = (v_1 \mid v_1) \mid (v_2 \mid v_2),$$
$$v_1 \wedge v_2 = (v_1 \downarrow v_1) \downarrow (v_2 \downarrow v_2),$$

其中 $v_1, v_2 \in \mathbf{Z}_2$.

2. 分别找出只含有运算 $\neg$ 和 $\wedge$ 的公式，使之与以下各公式等值:

1° $x_1 \rightarrow (x_2 \rightarrow x_3$.

2° $(x_1 \vee x_2 \vee x_3) \wedge (\neg x_1 \vee \neg x_2 \vee \neg x_3)$.

3° $(x_1 \leftrightarrow \neg x_2) \leftrightarrow x_3$.

3. 分别找出只含有运算 $\neg$ 和 $\vee$ 的公式，使之与以下各公式等值:

   1° $x_1 \to (x_2 \to x_3)$.

   2° $(\neg x_1 \wedge \neg x_2) \to (\neg x_3 \wedge x_4)$.

   3° $x_1 \leftrightarrow x_2$.

4. 给出与 $x_1 \to x_2$ 等值的只含运算 $\downarrow$ 的公式.

### 1.5.4 应用举例

在应用中，$\Gamma \vdash p$ 或 $\Gamma \vDash p$ 中的假定集 $\Gamma$ 常常是有限集. 当我们需要从语法上证明

$$\{r_1, \cdots, r_n\} \vdash p$$

时，易见可以改为从语义上检查 $(r_1 \wedge \cdots \wedge r_n) \to p$ 是不是永真式. 为此，只要写出真值表就可以了. 但是当命题变元的个数比较多时，这种一般的写真值表的方法太烦，甚至实际上行不通. 这时就需要灵活采用其他一些特殊方法.

**例 1** 检查下面的论证是否正确.

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”，$i = 1, 2, 3, 4$. 于是题中的论证可形式化为

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

检查它的正确性，可用从语义上进行，检查 $\neg x_1 \vee x_2$，$x_1 \to (x_3 \wedge x_4)$ 和 $x_4 \to x_2$ 这三个公式的所有公共成真指派是否都是 $x_2 \vee x_3$ 的成真指派. 为此，只用检查是否存在使前三个公式为真而使 $x_2 \vee x_3$ 为假的指派. 如果存在这种指派，那么原结论不成立. 这样，问题就归结为下面的真值方程组 (1)~(4) 是否有解:

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

(2) $v_1 \to (v_3 \wedge v_4) = 1$;

(3) $v_4 \to v_2 = 1$;

(4) $v_2 \vee v_3 = 0$.

由 (4) 式可得

(5) $v_2 = 0$, 且

(6) $v_3 = 0$.

由 (3) 式与 (5) 式得

(7) $v_4 = 0$.

由 (1) 式与 (5) 式得

(8) $v_1=0$.

将 (6)、(7)、(8) 式代入 (2) 式的左边，得

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

所得结果说明: (0，0，0，0) 是 (1)~(4) 式的解. 它是前三个公式 (“前提”) 的公共成真指派，但却是 $(x_2\vee x_3)$ (“结论”) 的成假指派，所以题中的论证不能成立.

**例 2** 检查下面结果的正确性，

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

**解** 若用真值表法，则要进行 $2^8=256$ 行的计算. 现在仍用前例中的方法，解真值方程组 (1)~(5):

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

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

(3) $(v_3\wedge v_4)\to v_7=1$;

(4) $(v_6\wedge v_7)\to v_8=1$;

(5) $v_8=0$.

由 (4)，(5) 得

(6) $v_6\wedge v_7=0$.

由 (1)，(2) 得

(7) $v_5\wedge v_6=1$.

由 (1)，(3) 得

(8) $v_7=1$.

由 (6)，(8) 得

(9) $v_6=0$.

(7) 与 (9) 矛盾，所以方程组 (1)~(5) 无解. 这说明题中原结论成立.

不难看出例 2 中结论的成立给出了下面的化学问题的肯定回答.

“现有 MgO，$H_2$，C，$O_2$ 四种化学物质，且已知

$$MgO+H_2\to Mg+H_2O,$$

$$C+O_2\to CO_2,$$

$$H_2O+CO_2\to H_2CO_3.$$

问: 能否用现有物质制造出 $H_2CO_3$ (碳酸)?”

**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 $d$ 有一人且只有一人作案;

4° 若 $b$ 与 $c$ 同时作案，则 $a$ 与 $d$ 同时作案或同未作案.
办案人员由此得出结论: $a$ 是作案者. 这个结论是否正确?

**解** 用 $x_1, x_2, x_3, x_4$ 分别表示 $a, b, c, d$ 作案. 办案人员的推理可形式化为

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

解方程组

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

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

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

(4) $v_1 = 0$.

$v_1 = 0$ 时 (2) 自动成立，不管 $v_2$ 取何值. 试取 $v_2 = 1$. 在 (3) 中，若 $v_3 = 0$, 则 (3) 也自动成立. 把这几个数据代入 (1)，得

$$0 \leftrightarrow (1 \wedge \neg v_4) = 1.$$

此式当 $v_4 = 1$ 时是成立的. 于是得到方程组 (1)~(4) 的一个解 (0，1，0，1). 这说明，还没有理由断言“$a$ 是作案者.”

## 练习 12

把以下论证形式化，并判断是否合理.

1. 如果函数 $f$ 不连续，那么函数 $g$ 不可微. 但已知 $g$ 是可微的. 所以 $f$ 是连续函数.

2. $A, B, C, D$ 为四个事件. 已知: $A$ 和 $B$ 不同时发生; 若 $A$ 发生，则 $C$ 不发生而 $D$ 发生; 若 $D$ 发生，则 $B$ 不发生. 结论: $B$ 和 $C$ 不同时发生.

3. 例 3 中如果办案人员作出的判断是: “$a$, $b$, $c$ 三人中至少有一人未作案”，判断是否正确?

# 2 谓词演算

上一章建立的命题演算 $L$ 中，命题变元用于表示简单命题，是不能再分割的最小单位——$L$ 的“原子”. 这一点使 $L$ 这个模型比较简单，但也限制了 $L$ 的应用范围. 比如，古典三段论法就不能很好地纳入到 $L$ 中去. 让我们考察下面的推理实例:

“金属都是导电体.

铜是金属，所以铜是导电体.”

这个推理方法无法在命题演算 $L$ 的框架内得到正确表现. 它可以在 $L$ 中形式化为 $\{x_1, x_2\} \vdash x_3$, 但这在 $L$ 中并不成立. 要表现这种推理方式，须建立新的模型. 在新的系统中，首先要涉及“原子命题”的内部结构. 此外，还涉及引入量词的问题. 让我们看下面的例子.

设 $A = \{1, 2, \cdots, 100\}$. 考察推理:

$A$ 中数皆大于零. 5 是 $A$ 中的数，所以 5 大于零.

用 $x_n$ 表示“$n \in A$”，用 $y_n$ 表示“$n > 0$” $(n = 1, 2, \cdots)$. 上面的推理可以在 $L$ 中形式化为下面正确的结果:

$$\{(x_1 \to y_1) \wedge \cdots \wedge (x_{100} \to y_{100}),\ x_5\} \vdash y_5.$$

但若把 $A$ 改成全体正实数集，则上面的形式化就遇到了麻烦，遇到从有限的个体对象到无限的个体对象的转变. 为此也要求有新的形式化的方法. 下面讨论的谓词演算对命题演算的改进在于: 深入分析“原子命题”内部结构，同时引进量词运算. 这是一种更细致、更复杂的数学模型，它能更深入、更广泛地表现实际的推理过程.

## 2.1 谓词演算的建立

### 2.1.1 项与原子公式

先来分解一个数学命题 (不论其真假):

一数的平方与一数的立方之和大于零.

分析一下这个命题便可知道:

第一，命题涉及的个体对象是某一个数 (记为 $x_1$)，另一个数 (记为 $x_2$), 及一个常数 $c_1 = 0$;

第二，命题中含有三个函数，一个一元函数是平方函数 (记为 $f_1^1$)，第二个一元函数是立方函数 (记为 $f_2^1$), 还有一个二元函数“求和”(记为 $f_1^2$);

第三，命题中还含有一个关于数的二元关系——“大于”(记为 $R_1^2$).

用引进的记号可以把原命题表示成

$$R_1^2(f_1^2(f_1^1(x_1),\ f_2^1(x_2)),\ c_1).$$

它的真假取决于对 $x_1$ 和 $x_2$ 所作的解释. 若将 $x_1$ 和 $x_2$ 解释为正整数，则它为真.

总之，分解这个“原子”命题，得到的是:

1° 一些“个体对象”及对它们进行的一些“运算”;

2° 关于这些对象的一个“关系”，正因为有这个“关系”，原子命题才得以形成.

基于以上分析，可以着手建立新的模型.

我们由四个集出发: 个体变元集 $X$, 个体常元集 $C$, 运算 (函数) 集 $F$, 谓词集 $R$. 用不同的 $C, F$ 和 $R$ 可构造出不同的谓词演算系统.

个体变元集 $X = \{x_1, x_2, \cdots\}$ 是可数集. 个体变元 $x_i$ 可用来表示某个个体对象. 有时为了方便，我们也用 $x, y, z$ 等来表示个体变元.

个体常元集 $C = \{c_1, c_2, \cdots\}$ 是可数集，也可以是有限集 (包括空集). 个体常元 $c_i$ 可用来表示确定的个体对象.

运算集 $F = \{f_1^1, f_2^1, \cdots, f_1^2, f_2^2, \cdots, f_1^3, f_2^3, \cdots\}$ 是可数集，也可以是有限集 (包括空集). $f_i^n$ 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. 注意符号 $f_i^n$ 的上标 $n$ 是该运算符的元数.

谓词集 $R = \{R_1^1, R_2^1, \cdots, R_1^2, R_2^2, \cdots, R_1^3, R_2^3, \cdots\}$ 是可数集，也可以是有限集，但不能是空集. $R_i^n$ 叫做第 $i$ 个 $n$ 元谓词，用来表示某种个体对象集上的 $n$ 元关系. $R_i^n$ 的上标 $n$ 是该谓词的元数.

建立谓词演算的第一步是建立项集 $T$, 项的形成规则是:

(i) 个体变元 $x_i (\in X)$ 与个体常元 $c_i (\in C)$ 都是项.

(ii) 若 $t_1, \cdots, t_n$ 是项，则 $f_i^n(t_1, \cdots, t_n)$ 也是项 $(f_i^n \in F)$.

(iii) 任一项皆如此形成，即皆由规则 (i)，(ii) 的有限次使用形成.

当运算符集 $F = \varnothing$ 时，规定项集 $T = X \cup C$.

按上述规则，当 $F \neq \varnothing$ 时，项集 $T$ 可如下分层:

$$T = T_0 \cup T_1 \cup T_2 \cup \cdots \cup T_k \cup \cdots$$

其中

$$
\begin{aligned}
T_0 = &\ X \cup C = \{x_1,\ x_2,\ \cdots,\ c_1,\ c_2,\ \cdots\},\\
T_1 = &\ \{f_1^1(x_1),\ f_1^1(x_2),\ \cdots,\ f_1^1(c_1),\ \cdots\\
&\ f_2^1(x_1),\ \cdots,\ f_2^1(c_1),\ \cdots\\
&\ \cdots\cdots\\
&\ f_1^2(x_1,\ x_1),\ \cdots\\
&\ \cdots\cdots\\
&\ f_1^3(x_1,\ x_1,\ x_1),\ \cdots\\
&\ \cdots\cdots\},\\
T_2 = &\ \{f_1^1(f_1^1(x_1)),\ \cdots,\ f_1^2(x_1,\ f_1^1(x_1)),\ \cdots\},\\
&\ \cdots\cdots
\end{aligned}
$$

第 $k$ 层项 ($T_k$ 的元素) 含有 $k$ 个运算符. 换句话说，第 $k$ 层项由零层项 (个体常元、个体变元) 经 $k$ 次运算得来. 更简单地说: 项集 $T$ 是由 $X \cup C$ 生成的 $F$ 型代数 (即以 $F$ 为运算集的代数系统).

项集 $T$ 具有分层性，即 $T$ 的各个层次之间没有公共元素. $T$ 的生成过程类似于命题代数 $L(X)$ (参见 1. 2 小节附 2).

**例 1** 设 $C = \{c_1\}, F = \{f_1^1, f_1^2\}$, 项集 $T$ 的前三个层次是

$$
\begin{aligned}
T_0 = &\ \{c_1,\ x_1,\ x_2,\ \cdots\},\\
T_1 = &\ \{f_1^1(c_1),\ f_1^1(x_1),\ f_1^1(x_2),\ \cdots\\
&\ f_1^2(c_1,\ c_1),\ f_1^2(c_1,\ x_1),\ \cdots\},\\
T_2 = &\ \{f_1^1(f_1^1(c_1)),\ f_1^1(f_1^1(x_1)),\ \cdots\\
&\ f_1^1(f_1^2(c_1,\ c_1)),\ f_1^1(f_1^2(c_1,\ x_1)),\ \cdots\\
&\ f_1^2(c_1,\ f_1^1(c_1)),\ f_1^2(f_1^1(c_1),\ c_1),\ \cdots\}.
\end{aligned}
$$

**定义 1 (闭项)** 只含个体常元的项叫做闭项.

例 1 中写出的 $f_1^1(c)$, $f_1^2(c_1,\ c_1)$, $f_1^1(f_1^1(c_1))$, $f_1^1(f_1^2(c_1,\ c_1))$ 等就是闭项，而 $f_1^1(x_1)$, $f_1^2(c_1,\ x_1)$ 等都不是闭项.

由项集的生成过程可以看出，所有闭项的集是由个体常元集 $C$ 生成的 $F$ 型代数.

**定义 2 (原子公式集)** 原子公式集是指

$$Y = \bigcup_{i,n} \Big(\{R_i^n\} \times \underbrace{T \times \cdots \times T}_{n\ 个\ T}\Big)$$

即

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

以后常把原子公式 $(R_i^n, t_1, \cdots, t_n)$ 写成 $R_i^n(t_1, \cdots, t_n)$.

在谓词演算中，原子公式是用来表示命题的最小单位，而命题演算是用单个命题变元来表示简单命题的. 研究谓词演算，必须重视项集这一层次. 项是构成原子公式的基础.

## 练习 13

1. 设 $C=\varnothing$, $F=\{f_1^1\}$. 试给出项集 $T$.

2. 设 $C=\{c_1\}$, $F=\{f_1^2,f_2^2\}$, $R=\{R_1^2\}$. 试写出三四个不同的原子公式. 如果 $x_1,x_2,\cdots$ 分别表示自然数 $n_1,n_2,\cdots$, $c_1$ 表示 0, $f_1^2$ 表示 +, $f_2^2$ 表示 ×, $R_1^2$ 表示 =, 指出你所写的原子公式的算术解释.

### 2.1.2 谓词演算公式集

建立谓词演算公式集前，先列出我们所采用的这种形式语言的字母表如下:

个体变元 $x_1, x_2, \cdots$ (可数个)

个体常元 $c_1, c_2, \cdots$ (可数或有限个)

运算符 $f_1^1, f_2^1, \cdots, f_1^2, f_2^2, \cdots$ (可数或有限个)

谓词 $R_1^1, R_2^1, \cdots, R_1^2, R_2^2, \cdots$ (可数或有限个，至少一个)

联结词 $\neg, \rightarrow$

全称量词 $\forall$

左右括号、逗号 ( , ) ,

形成谓词演算公式集的过程与命题演算类似，不同的是:

第一，现由原子公式集 $Y$ 出发，而不是由命题变元集出发;

第二，除了一元运算 $\neg$ (否定) 与二元运算 $\rightarrow$ (蕴涵) 外，现还增加了可数个一元全称量词运算“$\forall x_i$” $(i=1,2,\cdots)$.

谓词演算公式的形成规则是:

(i) 每个原子公式是公式.

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

(iii) 任一公式皆如此形成，即皆由规则 (i), (ii) 的有限次使用形成.

每个项及公式都可视为由字母表中的符号形成的有限序列. 在项与公式的形成中，为符合人们阅读习惯而使用的括号与逗号都可省去. (省去括号与逗号的做法是: 把项 $f_i^n(t_1,\cdots,t_n)$, 原子公式 $R_i^n(t_1,\cdots,t_n)$ 及形为 $p\rightarrow q$ 的公式分别改写成 $f_1^n t_1\cdots t_n$, $R_i^n t_1\cdots t_n$ 及 $\rightarrow p\,q$. 这样做的“唯一读法”，参见 1.2 节附 1 及 3.6.1 小节.)

用 $K(Y)$ 表示谓词演算全体公式的集. 由 0.3 节命题 5 知谓词演算字母表的符号集是可数集. 再由 0.3 节命题 7 及命题 1 便知项集 $T$, 原子公式集 $Y$ 及公式集 $K(Y)$ 都是可数集.

公式集 $K(Y)$ 也具有分层性，它的零层由原子公式组成，第 $k$ 层公式由原子公式经 $k$ 次运算得来.

除了 $\neg, \rightarrow$ 和 $\forall x_i$, 还可在 $K(Y)$ 上定义新的运算 $\vee, \wedge, \leftrightarrow$ 及 $\exists x_i$ (存在量词运算)，定义式是:

$$p \vee q = \neg p \rightarrow q,$$
$$p \wedge q = \neg(p \rightarrow \neg q),$$
$$p \leftrightarrow q = (p \rightarrow q) \wedge (q \rightarrow p),$$
$$\exists x_i p = \neg \forall x_i \neg p.$$

注意公式 $\forall x(p \rightarrow q)$ 和公式 $\forall x p \rightarrow q$ 的区别. 前者 $\forall x$ 的作用范围 (简称“范围”) 是 $p \rightarrow q$, 而后者 $\forall x$ 的范围是 $p$.

**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.

比如，在 $\forall x_1 (R_1^2(x_1, x_2) \rightarrow \forall x_2 R_1^1(x_2))$ 中，$x_1$ 约束出现两次，$x_2$ 约束出现两次且自由出现一次.

**定义 2 (闭式)** 公式若不含自由出现的变元，则叫做闭式.

例如，公式 $\forall x_1(R_1^2(x_1, x_2) \rightarrow \forall x_2 R_1^1(x_2))$ 不是闭式，因为 $x_2$ 在其中自由出现一次. 公式 $\forall x_1 (R_1^2(x_1, c_1) \rightarrow \forall x_2 R_1^1(x_2))$ 是闭式.

可能由于量词的存在而产生“变元干扰”，是谓词演算中的一件麻烦事. 例如，在用项去替换公式中的个体变元时就可能出现这种干扰. 项所含的变元本是自由而不受约束的，但若需要用某个项去替换一个公式中自由出现的变元时，该项中的变元可能会受约束.

为明确区分项对公式中的某变元是否可“自由代换”，需要下面的定义:

**定义 3 (项 $t$ 对公式 $p$ 中变元 $x$ 是自由的)** 用项 $t$ 去代换公式 $p$ 中自由出现的个体变元 $x$ 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，或简称 $t$ 对 $p$ 中 $x$ 是自由的.

换句话说，用 $t$ 代换 $p$ 中自由出现的 $x$ 时，若 $t$ 中有变元在代换后受到约束，则说 $t$ 对 $p$ 中的 $x$ 是“不自由的”(或“不可自由代换的,”或“不可代换的”).

下面两种情形，$t$ 对 $p$ 中 $x$ 是自由的:

1° $t$ 是闭项;

2° $x$ 在 $p$ 中不自由出现.

此外，在任何公式中，$x_i$ (作为项) 对 $x_i$ 自己总是自由的.

在 $\forall x_1 R_1^1(x_2)$ 中，项 $f_1^2(x_1, x_3)$ 对 $x_2$ 是不自由的，而项 $f_1^2(x_4, x_3)$ 对 $x_2$ 是自由的. 在 $\forall x_1 R_1^1(x_2)$ 中，任何不含 $x_1$ 的项对 $x_2$ 是自由的，任何含有 $x_1$ 的项对 $x_2$ 是不自由的.

在 $\forall x_1 R_1^2(x_1,x_2) \to \forall x_3 R_2^2(x_3,x_1)$ 中，$f_1^2(x_1,x_4)$ 对 $x_2$ 是不自由的；$f_2^2(x_2,x_3)$ 对 $x_2$ 是自由的，但对 $x_1$ 是不自由的；$f_3^2(x_1,x_3)$ 对 $x_1,x_2$ 都是不自由的；$x_2$ 对 $x_1$ 是自由的；$x_1$ 对 $x_2$ 是不自由的. 以上列出的项对该公式中 $x_3,x_4,x_5$ 都是自由的，因为 $x_3,x_4,x_5$ 在该公式中没有自由出现. ($x_4,x_5$ 根本不出现. )

定义 3 的另一种说法是: 若对项 $t$ 中所含任一变元 $y$, $p$ 中自由出现的某变元 $x$ 全都不出现在 $p$ 中 $\forall y$ 的范围内，则说 $t$ 对 $p$ 中 $x$ 是自由的.

以后如不另加说明，$p(t)$ 表示用项 $t$ 去代换公式 $p(x)$ 中所有自由出现的变元 $x$ 所得结果.

还要注意: 我们写 $p(x)$, 其中 $x$ 是指该公式中自由出现的 $x$, 而不是指约束出现的 $x$. 写 $p(x)$ 时 $x$ 可以不在 $p(x)$ 中自由出现或根本不出现，且不排除有其他变元在 $p(x)$ 中出现.

比如，当 $p(x_1) = R_1^1(x_1) \to \forall x_1 R_1^2(x_1,c_1)$ 时，$p(t) = R_1^1(t) \to \forall x_1 R_1^2(x_1,c_1)$; 当 $p(x_1) = R_1^1(x_2) \to \forall x_2 R_1^2(x_2,c_1)$ 或当 $p(x_1) = R_1^1(x_2) \to \forall x_1 R_1^2(x_1,c_1)$ 时，都有 $p(t) = p(x_1)$.

**注** 定义 3 中及别处所用“代换”一词，在本书中的含义是“全部替换”而不同于“一处替换”

## 练习 14

1. 下面哪些符号串是谓词演算的公式? 其中有没有闭式?

   1° $\forall x_1 R_1^2(f_1^1(x_1), x_1)$.

   2° $f_1^3(x_1, x_3, x_4)$.

   3° $R_1^1(x_2) \to R_1^3(x_3, c_1)$.

   4° $\neg \forall x_2 R_1^2(x_1, x_2)$.

   5° $\forall x_2 R_1^1(x_1) \to \neg R_1^1(x_2)$.

   6° $R_1^3(f_2^3(x_1, c_2, x_2))$.

   7° $\neg R_1^1(x_1) \to R_1^1(x_2)$.

   8° $R_1^3(c_1, c_2, f_1^1(c_3))$.

2. 在以下公式中，哪些 $x_1$ 的出现是自由的? 哪些 $x_1$ 的出现是约束的? 项 $f_1^2(x_1,x_3)$ 对这些公式中的 $x_2$ 是不是自由的?

   1° $\forall x_2 (R_1^2(x_1, x_2) \to R_2^2(x_2, c_1))$.

   2° $R_1^1(x_3) \to \neg \forall x_1 \forall x_2 R_1^3(x_1, x_2, c_1)$.

   3° $\forall x_1 R_1^1(x_1) \to \forall x_2 R_1^2(x_1, x_2)$.

   4° $\forall x_2 R_1^2(f_1^2(x_1, x_2), x_1) \to \forall x_1 R_2^2(x_3, f_2^2(x_1, x_2))$.

3. 设 $t$ 是项 $f_1^2(x_1, x_3)$, $p(x_1)$ 是下面的公式. 确定 $t$ 对 $p(x_1)$ 中的 $x_1$ 是否自由? 如果是自由的, 写出 $p(t)$.

1° $\forall x_1 R_1^2(x_2, f_1^2(x_1, x_2)) \to R_1^1(x_1)$.

2° $\forall x_1 \forall x_3 (R_1^1(x_3) \to R_1^1(x_1))$.

3° $\forall x_2 R_1^1(f_1^1(x_2)) \to \forall x_3 R_1^3(x_1, x_2, x_3)$.

4° $\forall x_2 R_1^3(x_1, f_1^1(x_1), x_2) \to \forall x_3 R_1^1(f_1^2(x_1, x_3))$.

4. 用以下项 $t$ 重复第 3 题的练习.

(1) $x_2$; (2) $x_3$; (3) $f_1^2(c_1, x_1)$; (4) $f_1^3(x_1, x_2, x_3)$.

5. 设个体变元 $x$ 在公式 $p(x)$ 中自由出现, 个体变元 $y$ 不在公式 $p(x)$ 中自由出现. 试证, 如果 $y$ 对 $p(x)$ 中的 $x$ 是自由的, 那么 $x$ 对 $p(y)$ 中的 $y$ 也是自由的.

### 2.1.3 谓词演算 $K$

谓词演算 $K$ 是为研究推理而建立的更细致的数学模型, 应用范围相当广泛. 它把涉及量词的推理中"证明"的概念精确化. 用通常的话说, 在系统 $K$ 中, 项、公式与"证明"的形成, 分别就是这种语言的组词、造句与作文.

谓词演算 $K$ 是用公式集 $K(Y)$ 来定义的, 与命题演算 $L$ 的定义方式类似.

**定义 1 (谓词演算 $K$)** 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"

取 $K(Y)$ 中以下形状的公式作为"公理".

(K1) $p \to (q \to p)$;

(K2) $(p \to (q \to r)) \to ((p \to q) \to (p \to r))$;

(K3) $(\neg p \to \neg q) \to (q \to p)$;

(K4) $\forall x p(x) \to p(t)$, 其中项 $t$ 对 $p(x)$ 中的 $x$ 是自由的;

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

以上给出的是五种公理模式, 其中 $p, q, r, p(x)$ 都是任意的公式.

2° "证明"

设 $p$ 是某个公式, $\Gamma$ 是某个公式集. $p$ 从 $\Gamma$ 可证, 记作 $\Gamma \vdash p$, 是指存在着公式的有限序列 $p_1, \cdots, p_n$, 其中 $p_n = p$, 且对每个 $k = 1, \cdots, n$ 有

(i) $p_k \in \Gamma$, 或

(ii) $p_k$ 为公理, 或

(iii) 存在 $i, j < k$, 使 $p_j = p_i \to p_k$ (此时说由 $p_i$, $p_i \to p_k$ 使用 MP 得到 $p_k$), 或

(iv) 存在 $j < k$, 使 $p_k = \forall x p_j$. 此时说由 $p_j$ 使用"Gen"("推广")这条推理规则得到 $p_k$. $x$ 叫做 Gen 变元 (Gen 是 Generalization 的缩写).

符合上述条件的 $p_1,\cdots,p_n$ 叫做 $p$ 从 $\Gamma$ 的"证明". $\Gamma$ 叫做假定集, $p$ 叫做 $\Gamma$ 的语法推论.

若 $\varnothing \vdash p$, 则 $p$ 叫做 $K$ 的定理, 记作 $\vdash p$.

公理 (K1)~(K3) 和命题演算 $L$ 的公理 (L1)~(L3) 形式上完全一样, 但内容不同, 这里的 $p,q,r \in K(Y)$.

注意公理模式 (K4) 中所加的条件 ("$t$ 对 $p(x)$ 中的 $x$ 是自由的") 不可少. 例如,

$$\forall x_1\, p(x_1) \to p(x_1) \quad \text{和} \quad \forall x_1 \forall x_2\, R_1^2(x_1,x_2) \to \forall x_2\, R_1^2(x_3,x_2)$$

都是 (K4) 型公理, 但

$$\forall x_1\, \forall x_2\, R_1^2(x_1,x_2) \to \forall x_2\, R_1^2(x_2,x_2)$$

却不是 (K4) 型公理, 因为 $x_2$ 对 $\forall x_2\, R_1^2(x_1,x_2)$ 中的 $x_1$ 是不自由的.

下面是个跨演算的定理, 注意 $K(Y)$ 中也有用 $\neg, \to$ 表示的同名运算.

**定理 1** 设 $x_1,\cdots,x_n$ 是命题演算 $L$ 的命题变元, $p(x_1,\cdots,x_n) \in L(X_n)$. 我们有

$$\vdash_L\ p(x_1,\cdots,x_n) \quad \Rightarrow \quad \vdash_K\ p(p_1,\cdots,p_n),$$

其中 $p_1,\cdots,p_n \in K(Y)$, $p(p_1,\cdots,p_n)$ 是用 $p_1,\cdots,p_n$ 分别代换 $p(x_1,\cdots,x_n)$ 中的 $x_1,\cdots,x_n$ 所得结果.

**证** 因为 $L$ 中的公理模式 (L1), (L2), (L3) 和 $K$ 中的公理模式 (K1), (K2), (K3) 形式上完全相同, $L$ 中的推理规则 MP 也在 $K$ 中保留着, 所以 $p(x_1,\cdots,x_n)$ 在 $L$ 中的证明可转换成 $p(p_1,\cdots,p_n)$ 在 $K$ 中的证明, 只要把所有命题变元 $x_i$ 全都换成对应的 $p_i$ 即可. □

**定义 2 (命题演算型永真式, 简称永真式)** 若 $p(x_1,\cdots,x_n) \in L(X_n)$ 是命题演算 $L$ 中的永真式, 则对任意 $p_1,\cdots,p_n \in K(Y)$, $p(p_1,\cdots,p_n)$ 叫做 $K$ 的命题演算型永真式, 简称为永真式.

定理 1 的另一种陈述是: $K$ 的永真式一定是 $K$ 的定理. 逆定理不成立: 并非 $K$ 的定理一定都是 (命题演算型) 永真式. 例如, $\forall x_1\, R_1^1(x_1) \to \forall x_1\, R_1^1(x_1)$ 是永真式, 也是 $K$ 的定理, 而 $\forall x_1\, R_1^1(x_1) \to R_1^1(x_1)$ 是 $K$ 的定理而不是永真式.

定理 1 告诉我们, 谓词演算 $K$ 这个新的数学模型并不是将命题演算 $L$ 全部推倒, 而是对 $L$ 的改进. $K$ 保存了 $L$ 的精华. $L$ 中的结论、方法和技巧都将在 $K$ 中继续起作用 (特别是通过定理 1).

按照定理 1, 以下各式在 $K$ 中仍然成立.

$\vdash p \to p,$ (同一律)

$\vdash \neg q \to (q \to p),$ (否定前件律)

$\vdash (\neg p \to p) \to p,$ (否定肯定律)

$\vdash \neg\neg p \to p,$ (双重否定律)

$$\vdash (p \to q) \to ((q \to r) \to (p \to r)) \qquad \text{(HS)}$$

等等. 当然，这里的 $p, q, r$ 都是 $K$ 的公式.

一公式集 $\Gamma$ 是无矛盾的，仍指对任何公式 $q$, $\Gamma \vdash q$ 与 $\Gamma \vdash \neg q$ 二者不同时成立.

**命题 1** $\Gamma$ 有矛盾 $\Rightarrow$ $K$ 的任一公式从 $\Gamma$ 可证.

证明与 1.2.2 小节命题 3 的证明完全相同.

**例 1** $\{\neg\exists x \neg p\} \vdash \forall x p$, 这是因为 (注意 2.1.2 小节中 $\exists x$ 的定义) $\forall x p$ 有从 $\{\neg\neg\forall x \neg\neg p\}$ 的一个证明:

(1) $\neg\neg\forall x \neg\neg p$, 假定

(2) $\neg\neg\forall x \neg\neg p \to \forall x \neg\neg p$, 永真式

(3) $\forall x \neg\neg p$, (1)，(2)，MP

(4) $\forall x \neg\neg p \to \neg\neg p$, (K4)

(5) $\neg\neg p$, 3)，(4)，MP

(6) $\neg\neg p \to p$, 永真式

(7) $p$, (5)，(6)，MP

(8) $\forall x p$. (7)，Gen

**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，故公式

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

是 (K4) 型公理. 由此式及永真式

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

可得

$$\vdash \ p(t) \to \neg\forall x \neg p(x). \qquad \square$$

$\exists_1$ 规则是后面经常要用到的.

**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. 以下是所需要的证明.

(1) $\forall x(p \to q)$, 假定

(2) $\forall x(p \to q) \to (p \to q)$, (K4)

(3) $p \to q$, (1)，(2)，MP

(4) $\forall x \neg q$, 假定

(5) $\forall x \neg q \to \neg q$, (K4)

(6) $\neg q$, (4)，(5)，MP

(7) $(p \to q) \to (\neg q \to \neg p)$, 永真式

(8) $\neg q \to \neg p$, (3)，(7)，MP

(9) $\neg p$, (6)，(8)，MP

(10) $\forall x \neg p$. Gen

以上证明最后一步使用了 Gen 变元 $x$, 但没有使用其他 Gen 变元.

$K$ 中也有演绎定理，但要注意此时在定理中所加的新条件.

**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 变元就可得 $\Gamma \vdash p \to q$.

**证** 1° 由 MP 即得.

2° 设 $q_1, \cdots, q_n$ 是 $q$ 在 $K$ 中从 $\Gamma \cup \{p\}$ 的证明. 由已知条件，该证明中涉及的 Gen 变元不在 $p$ 中自由出现.

现对 $n$ 归纳.

$n = 1$ 时，$q_1 = q$. 此时有三种可能: $q = p$, $q \in \Gamma$ 或 $q$ 是公理. (参见命题演算中演绎定理的证明) 这时不管哪种情形都不用 Gen 规则便可证得 $\Gamma \vdash p \to q$.

$n > 1$ 时，只用考虑当 $q$ 是使用 Gen 规则而得的情形 (其他情形下的证明都与命题演算中演绎定理的证明相同，且不涉及 Gen). 设 $q = \forall x q_i$, $i < n$, 且 Gen 变元 $x$ 未在 $p$ 中自由出现. 这时因 $\Gamma \cup \{p\} \vdash q_i$, 由归纳假设，有 $\Gamma \vdash p \to q_i$, 且不增加新的 Gen 变元.

以下是 $p \to q$ 从 $\Gamma$ 的一个证明:

$$\left.\begin{array}{l} (1)\ \cdots\cdots \\ \quad\ \ \cdots\cdots \\ (k)\ p \to q_i \end{array}\right\} p \to q_i \text{ 从 } \Gamma \text{ 的证明}$$

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

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

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

以上过程中，除 $x$ 外没有使用别的 Gen 变元. 上面在使用公理 K5 时，需要“Gen 变元不在 $p$ 中自由出现”这一条件. □

**推论 1** 当 $p$ 是闭式时，有

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

**命题 3** $\vdash \forall x (p \to q) \to (\exists x p \to \exists x q)$, 除了 $x$ 外不用其他 Gen 变元.

**证** 依次有

(1) $\{\forall x (p \to q), \forall x \neg q\} \vdash \forall x \neg p$ (例 2，其中只用了 $x$ 为 Gen 变元)

(2) $\{\forall x (p \to q)\} \vdash \forall x \neg q \to \forall x \neg p$ (由 (1) 用演绎定理)

(3) $\{\forall x(p \to q)\} \vdash \neg\forall x\neg p \to \neg\forall x\neg q$ (由 (2) 使用永真式 (换位律))

(4) $\vdash \forall x(p \to q) \to (\exists xp \to \exists xq)$ (由 (3) 再用演绎定理)

以上除 (1) 中用的 $x$, 没有用别的 Gen 变元. □

**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 $\Gamma \vdash p$.

**证** 以下公式从 $\Gamma \cup \{\neg p\}$ 可证:

(1) $q$, 已知

(2) $\neg q$, 已知

(3) $\neg q \to (q \to p)$, 永真式

(4) $q \to p$, (2)，(3)，MP

(5) $p$. (1)，(4)，MP

于是以下公式从 $\Gamma$ 可证:

(6) $\neg p \to p$, 由演绎定理

(7) $(\neg p \to p) \to p$, 永真式

(8) $p$. (6)，(7)，MP

以上过程没有出现新的 Gen 变元. □

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

**证** 由已知条件及双重否定律 $\neg\neg p \to p$ 可得

(1) $\Gamma \cup \{\neg\neg p\} \vdash q$,

(2) $\Gamma \cup \{\neg\neg p\} \vdash \neg q$.

由 (1)，(2) 用反证律得 $\Gamma \vdash \neg p$, 且不涉及新的 Gen 变元. □

**例 3** $\{\forall xp\} \vdash \exists xp$.

现用归谬律来证明. 以下公式从 $\{\forall xp, \forall x\neg p\}$ 可证:

(1) $\forall xp$, 假定

(2) $\forall x\neg p$, 假定

(3) $\forall x\neg p \to \neg p$, (K4)

(4) $\forall xp \to p$, (K4)

(5) $p$, (1)，(4)，MP

(6) $\neg p$. (2)，(3)，MP

由 (5)，(6) 用归谬律得

$$\{\forall xp\} \vdash \neg\forall x\neg p, \text{此即 } \exists xp.$$

**命题 4 ($\exists_2$ 规则)** 设 $\Gamma \cup \{p\} \vdash q$, 其证明中 Gen 变元不在 $p$ 中自由出现，且 $x$ 不在 $q$ 中自由出现，那么有 $\Gamma \cup \{\exists xp\} \vdash q$, 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 $\Gamma$ 可证:

(1) $p \to q$, 由演绎定理

(2) $(p \to q) \to (\neg q \to \neg p)$, 永真式

(3) $\neg q \to \neg p$, (1)，(2)，MP

(4) $\forall x(\neg q \to \neg p)$, (3)，Gen

(5) $\forall x(\neg q \to \neg p) \to (\neg q \to \forall x \neg p)$, (K5)

(6) $\neg q \to \forall x \neg p$, (4)，(5)，MP

(7) $(\neg q \to \forall x \neg p) \to (\neg \forall x \neg p \to q)$, 永真式

(8) $\neg \forall x \neg p \to q$, 即 $\exists xp \to q$. (6)，(7)，MP

以上建立 $\Gamma \vdash \exists xp \to q$ 的过程除了 $x$ 外未用其他新的 Gen 变元. 再用一次演绎定理便得 $\Gamma \cup \{\exists xp\} \vdash q$. □

$\exists_2$ 规则在后面也是常要用到的.

**命题 5** 对 $K$ 中任意公式 $p, q, r$, 有

1° $\vdash p \leftrightarrow p$; (自反性)

2° $\vdash p \leftrightarrow q \quad \Rightarrow \quad \vdash q \leftrightarrow p$; (对称性)

3° $\vdash p \leftrightarrow q$ 且 $\vdash q \leftrightarrow r \quad \Rightarrow \quad \vdash p \leftrightarrow r$. (可递性)

**证** 1° $p \leftrightarrow p$ 是永真式.

2° 若已知 $\vdash p \leftrightarrow q$, 则有以下 $q \leftrightarrow p$ 在 $K$ 中的证明:

$$\left.\begin{array}{l}(1)\ \cdots\cdots \\ \quad\ \ \cdots\cdots \\ (k)\ p \leftrightarrow q\end{array}\right\} p \leftrightarrow q \text{ 在 } K \text{ 中的证明}$$

$(k+1)$ $(p \leftrightarrow q) \to (q \leftrightarrow p)$ 永真式

$(k+2)$ $q \leftrightarrow p$ $(k)$, $(k+1)$, MP

3° 若已知 $\vdash p \leftrightarrow q$ 和 $\vdash q \leftrightarrow r$, 由永真式

$$(p \leftrightarrow q) \to ((q \leftrightarrow r) \to (p \leftrightarrow r))$$

两次用 MP 即得 $\vdash p \leftrightarrow r$. □

**定义 3 (可证等价)** $p$ 与 $q$ 可证等价 (简称为等价)，指 $\vdash p \leftrightarrow q$ 成立.

由命题 5 可知，“可证等价”给出了 $K(Y)$ 上的一个等价关系，它确定了 $K(Y)$ 的一个分类.

为确定两个公式是否等价，常用的命题是:

**命题 6** $\Gamma \vdash p \leftrightarrow q \quad \Leftrightarrow \quad \Gamma \vdash p \to q$ 且 $\Gamma \vdash q \to p$.

**证** $(\Rightarrow)$ 利用永真式

$$(p \leftrightarrow q) \to (p \to q), \quad (p \leftrightarrow q) \to (q \to p).$$

(⇐) 利用永真式

$$(p \to q) \to ((q \to p) \to (p \leftrightarrow q)).$$ □

**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) $\forall x p(x)$, 假定

(2) $\forall x p(x) \to p(y)$, (K4)

(3) $p(y)$, (1), (2), MP

(4) $\forall y p(y)$, (3), Gen

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

$$\vdash \forall x p(x) \to \forall y p(y).$$

同样的过程可以得到

$$\vdash \forall y p(y) \to \forall x p(x),$$

但在证明过程中使用 (K4) 时要用到事实: $x$ 对 $p(y)$ 中的 $y$ 是自由的. (这是因为: 在用 $x$ 代换 $p(y)$ 中的 $y$ 后还原的 $p(x)$ 中，$x$ 是自由的.)

2° 由 1° 及 $\exists x$ 的定义可得. □

在对公式进行等价变换时，命题 7 可用于按照需要更换约束变元. 更换约束变元是避免变元干扰的简单方法. 在公式中，约束变元所起的作用类似于积分 $\int_a^b f(x)\mathrm{d}x = \int_a^b f(t)\mathrm{d}t$ 中积分变元 $x$ 和 $t$ 所起的作用.

**命题 8** 1° $\vdash \neg\forall xp \leftrightarrow \exists x\neg p$,

2° $\vdash \neg\exists xp \leftrightarrow \forall x\neg p$.

**证** 1° 用（K4)，双重否定律及 Gen 分别证明

$$\forall x\neg\neg p \to \forall xp \quad 及 \quad \forall xp \to \forall x\neg\neg p,$$

用换位律后进而得 $\vdash \neg\forall xp \leftrightarrow \neg\forall x\neg\neg p$.

2° $\neg\neg\forall x\neg p \leftrightarrow \forall x\neg p$ 是永真式. □

## 练习 15

1. 写出 $\forall x_1(R_1^1(x_1) \to R_1^1(x_1))$ 在 $K$ 中的证明.

2. 试证对任意公式 $p$ 与 $q$, 有

$$\vdash \forall x(p \to q) \to (\forall xp \to \forall xq).$$

3. 求证:

1° $\{\forall x_1\forall x_2 R_1^2(x_1, x_2)\} \vdash \forall x_1 R_1^2(x_1, x_1)$.

2° $\{\forall x_1 \forall x_2 R_1^2(x_1, x_2)\} \vdash \forall x_2 \forall x_3 R_1^2(x_2, x_3)$.

(要求写出在 $K$ 中的证明.)

4. 设 $x$ 不在 $p$ 中自由出现. 求证:

1° $\vdash (p \to \forall x q) \to \forall x(p \to q)$.

2° $\vdash (p \to \exists x q) \to \exists x(p \to q)$.

5. 以下推理是否正确?

1° 由 $R_1^1(x_1)$ 使用 Gen 规则得 $\forall x_1 R_1^1(x_1)$. 这证明了

$$\{R_1^1(x_1)\} \vdash \forall x_1 R_1^1(x_1).$$

再由此用演绎定理便得 $\vdash R_1^1(x_1) \to \forall x_1 R_1^1(x_1)$.

2° 因 $\{\exists x_1 R_1^1(x_1), \neg R_1^1(x_1)\} \vdash \forall x_1 \neg R_1^1(x_1)$ 及 $\neg \forall x_1 \neg R_1^1(x_1)$, 故用反证律便得 $\{\exists x_1 R_1^1(x_1)\} \vdash R_1^1(x_1)$. 再由演绎定理得

$$\vdash \exists x_1 R_1^1(x_1) \to R_1^1(x_1).$$

### 2.1.4 其他课题: 对偶律与前束范式

**定理 1 (子公式的等价可替换性)** 设公式 $q$ 是公式 $p$ 的子公式: $p = \cdots q \cdots$. 用公式 $q'$ 替换 $p$ 中的 $q$ (一次替换) 所得结果记为 $p' = \cdots q' \cdots$. 则有

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

**证** 对 $p$ 在 $K(Y)$ 中的层次数 $n$ 归纳.

$n = 0$ 时，$p$ 是原子公式，故 $p = q$, $p' = q'$, 命题成立.

$n > 0$ 时，除去 $p = q$ 这种平凡情形外，还有以下三种可能的情形.

(i) $p = \neg r$ 时，$q$ 是 $r$ 的子公式，替换的结果是 $p' = \neg r'$. 由归纳假设，

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

再利用下面的永真式便可:

$$(r \leftrightarrow r') \leftrightarrow (\neg r \leftrightarrow \neg r').$$

(ii) $p = r \to s$ 时，$q$ 或是 $r$ 的子公式 (此时 $p' = r' \to s$), 或是 $s$ 的子公式 (此时 $p' = r \to s'$). 对于前者，用永真式

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

对于后者，用永真式

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

加上归纳假设，便得结果.

(iii) $p = \forall x r$ 时，$p' = \forall x r'$. 由归纳假设，有 $\Gamma \vdash r \leftrightarrow r'$. 为证 $\Gamma \vdash \forall x r \leftrightarrow \forall x r'$,

考虑对称性，只用证一个方向: $\Gamma \vdash \forall x r \to \forall x r'$. 以下是 $\forall x r'$ 从 $\Gamma \cup \{\forall x r\}$ 的一个证明，注意，除了 $x$, 没有其他 Gen 变元，故进而可用演绎定理.

| | |
|---|---|
| (1) $\forall x r$ | 假定 |
| (2) $\forall x r \to r$ | (K4) |
| (3) $r$ | (1)，(2)，MP |
| (4) $r \to ((r \leftrightarrow r') \to r')$ | 永真式 |
| (5) $(r \leftrightarrow r') \to r'$ | (3)，(4)，MP |
| (6) $r \leftrightarrow r'$ | 由归纳假设 |
| (7) $r'$ | (5)，(6)，MP |
| (8) $\forall x r'$ | (7)，Gen |

□

**定理 2 (对偶律)** 设公式 $p$ 已表示成含原子公式及 $\neg, \vee, \wedge, \forall, \exists$ 的公式. 现把 $p$ 中所有原子公式都改为它们的否定，$\vee$ 与 $\wedge$ 互换，$\forall$ 与 $\exists$ 互换，得公式 $p^*$, 则有

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

**证** 对 $p$ 中 $\neg, \wedge, \vee, \forall$ 及 $\exists$ 出现的次数 $n$ 归纳.

$n = 0$ 时，$p$ 是原子公式，故 $p^* = \neg p$.

$n > 0$ 时，有以下五种可能: $p = \neg q$, $p = q \vee r$, $p = q \wedge r$, $p = \forall x q$ 及 $p = \exists x q$. 由归纳假设，总有 $\vdash q^* \leftrightarrow \neg q$, $\vdash r^* \leftrightarrow \neg r$. 对五种可能分别讨论如下.

(i) $p = \neg q$ 时，在 $p^*(= \neg q^*)$ 中用 $\neg q$ (等价) 替换 $q^*$, 由定理 1，有

$$\vdash q^* \leftrightarrow \neg q \quad \Rightarrow \vdash \neg q^* \leftrightarrow \neg\neg q, \text{ 即 } \vdash p^* \leftrightarrow \neg p.$$

(ii) $p = q \vee r$ 时，$p^* = q^* \wedge r^*$. 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 律便得

$$\vdash p^* \leftrightarrow \neg(q \vee r), \text{ 即 } \vdash p^* \leftrightarrow \neg p.$$

(iii) $p = q \wedge r$ 时，证明同 (ii).

(iv) $p = \forall x q$ 时，$p^* = \exists x q^*$. 此时有

| | |
|---|---|
| $\vdash q^* \leftrightarrow \neg q$, | (归纳假设) |
| $\vdash \exists x q^* \leftrightarrow \exists x \neg q$, | (子公式等价替换) |
| $\vdash \exists x q^* \leftrightarrow \neg \forall x \neg\neg q$, | (即上式) |
| $\vdash \neg \forall x \neg\neg q \leftrightarrow \neg \forall x q$, | (子公式等价替换) |
| $\vdash \exists x q^* \leftrightarrow \neg \forall x q$, | (由上两式用可递性) |

最后的结论即为 $\vdash p^* \leftrightarrow \neg p$.

(v) $p = \exists x q$ 时，证明同 (iv). □

除了上面两个语法定理，下面的命题 1 也是谓词演算 $K$ 的常用命题.

**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** 1° 一个方向是 (K5)，另一个方向是练习 15 题 4-1°.

2° 一个方向是练习 15 题 4-2°, 另一个方向是要证明

$$\vdash \exists x(p \to q) \to (p \to \exists x q).$$

为此只用证 $\{\exists x(p \to q), p\} \vdash \exists x q$ (即 $\neg \forall x \neg q$)，过程中除了 $x$ 外不用别的 Gen 变元便可.

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

| | |
|---|---|
| (1) $\forall x \neg q$ | 假定 |
| (2) $\forall x \neg q \to \neg q$ | (K4) |
| (3) $\neg q$ | (1)，(2)，MP |
| (4) $p$ | 假定 |
| (5) $p \to (\neg q \to \neg (p \to q))$ | 永真式 |
| (6) $\neg q \to \neg (p \to q)$ | (4)，(5)，MP |
| (7) $\neg (p \to q)$ | (3)，(6)，MP |
| (8) $\forall x \neg (p \to q)$ | (7)，Gen |
| (9) $\neg \forall x \neg (p \to q)$ | 假定 |

由 (8)，(9) 用归谬律得

$$\{\neg \forall x \neg (p \to q), p\} \vdash \neg \forall x \neg q.$$

3° 先证 $\vdash \forall x(p \to q) \to (\exists x p \to q)$, 为此只用证 $\{\forall x(p \to q), \exists x p\} \vdash q$, 过程中不使用除 $x$ 外的 Gen 变元.

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

| | |
|---|---|
| (1) $\forall x(p \to q)$ | 假定 |
| (2) $\forall x(p \to q) \to (p \to q)$ | (K4) |
| (3) $p \to q$ | (1)，(2)，MP |
| (4) $\neg q$ | 假定 |
| (5) $(p \to q) \to (\neg q \to \neg p)$ | 永真式 |
| (6) $\neg q \to \neg p$ | (3)，(5)，MP |
| (7) $\neg p$ | (4)，(6)，MP |

(8) $\forall x \neg p$ (7)，Gen

(9) $\neg\forall x \neg p$ 假定

因 $x$ 不在 $q$ 中自由出现，由 (8)，(9) 用反证律得

$$\{\forall x(p \to q), \neg\forall x \neg p\} \vdash q.$$

另一个方向系练习 16 题 1–1°.

4° 一个方向是 $\vdash \exists x(p \to q) \to (\forall x p \to q)$, 系练习 16 题 1–2°. 最后要证另一个方向

$$\vdash (\forall x p \to q) \to \exists x(p \to q).$$

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

(1) $\forall x \neg(p \to q)$ 假定

(2) $\forall x \neg(p \to q) \to \neg(p \to q)$ (K4)

(3) $\neg(p \to q)$ (1)，(2)，MP

(4) $\neg(p \to q) \to \neg q$ 永真式

(5) $\neg(p \to q) \to p$ 永真式

(6) $\neg q$ (3)，(4)，MP

(7) $p$ (3)，(5)，MP

(8) $\forall x p$ (7)，Gen

(9) $\forall x p \to q$ 假定

(10) $q$ (8)，9)，MP

因 Gen 变元 $x$ 不在假定中自由出现，由 (6)，(10) 用归谬律得

$$\{\forall x p \to q\} \vdash \neg\forall x \neg(p \to q).$$

再用演绎定理便可. □

**定义 1 (前束范式)** 前束范式，指形如

$$Q_1 x \cdots Q_n y\, p$$

的公式，其中 $Q_1, \cdots, Q_n$ 表示量词符号 $\forall$ 或 $\exists$, 尾部 $p$ 是不含有量词的公式.

例如，$\exists x_1(R_1^1(x_1) \to \forall x_2 R_1^2(x_1, x_2))$ 不是前束范式，而 $\exists x_1 \forall x_2(R_1^1(x_1) \to R_1^2(x_1, x_2))$ 是与之等价的前束范式.

现可把前面一些结论集中在一起:

**命题 2** 用 $Q$ 表示量词符号 $\forall$ 或 $\exists$, 用 $Q^*$ 表示 $Q$ 的对偶符号 ( $Q$ 为 $\forall$ 时 $Q^*$ 为 $\exists$, $Q$ 为 $\exists$ 时 $Q^*$ 为 $\forall$ ). 那么有

1° 若 $y$ 不在 $p(x)$ 中出现，则

$$\vdash Q x p(x) \leftrightarrow Q y p(y).$$

2° 若 $x$ 不在 $p$ 中自由出现，则

$$\vdash (p \to Qxq) \leftrightarrow Qx(p \to q);$$

若 $x$ 不在 $q$ 中自由出现，则

$$\vdash (Qxp \to q) \leftrightarrow Q^* x(p \to q).$$

3° $\vdash \neg Qxp \leftrightarrow Q^* x \neg p$.

**证** 1° 即 2.1.3 小节命题 7.

2° 即命题 1.

3° 即 2.1.3 小节命题 8. □

命题 2 是为得到前束范式而进行等价变换的工具. 对任给的公式 $p$, 反复用命题 2 可以找到与 $p$ 等价的前束范式 $q$. 方法是: 先利用命题 2-1° 及子公式等价替换定理 (定理 1)，适当调整、更换 $p$ 中的约束变元 (如有必要的话)，使新的公式与 $p$ 等价，且满足使用命题 2-2° 所需要的条件. 然后利用命题 2-2° 或命题 2-3°, 逐步把量词往左边移. 重复这种步骤，直到所有的量词都移到左边，得到了等价的前束范式 $q$ 为止.

**例 1** 找出与公式

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

等价的前束范式.

**解** 适当改变 $p$ 中的约束变元得到等价的 $q_1$：

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

由 $q_1$ 出发，反复利用命题 2-2° 与 2-3°, 得到以下的等价公式 $q_2 \sim q_6$：

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

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

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

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

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

$q_6$即为所求.

等价的前束范式并不是唯一的. 比如，例 1 中所取的量词的排列顺序不是唯一的，下面的 $q$ 也是与 $p$ 等价的前束范式:

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

下面的命题 3 也是进行等价变换的工具.

**命题 3** 1° $\vdash (\forall xp \wedge \forall xq) \leftrightarrow \forall x(p \wedge q)$,

2° $\vdash (\exists xp \vee \exists xq) \leftrightarrow \exists x(p \vee q)$.

若 $x$ 不在 $p$ 中自由出现，则有 ($Q$ 仍表示 $\forall$ 或 $\exists$)

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

$4°\ \vdash (p \wedge Qxq) \leftrightarrow Qx(p \wedge q)$.

**证** 1° 先证 $\{\forall xp \wedge \forall xq\} \vdash \forall x(p \wedge q)$.

下面是所要的证明:

| | |
|---|---|
| (1) $\forall xp \wedge \forall xq$ | 假定 |
| (2) $(\forall xp \wedge \forall xq) \to \forall xp$ | 永真式 |
| (3) $(\forall xp \wedge \forall xq) \to \forall xq$ | 永真式 |
| (4) $\forall xp$ | (1),(2),MP |
| (5) $\forall xq$ | (1),(3),MP |
| (6) $\forall xp \to p$ | (K4) |
| (7) $\forall xq \to q$ | (K4) |
| (8) $p$ | (4),(6),MP |
| (9) $q$ | (5),(7),MP |
| (10) $p \to (q \to (p \wedge q))$ | 永真式 |
| (11) $q \to (p \wedge q)$ | (8),(10),MP |
| (12) $p \wedge q$ | (9),(11),MP |
| (13) $\forall x(p \wedge q)$ | (12),Gen |

因 $x$ 不在假定中自由出现,用演绎定理得

$$\vdash (\forall xp \wedge \forall xq) \to \forall x(p \wedge q).$$

类似可证另一个方向:

$$\vdash \forall x(p \wedge q) \to (\forall xp \wedge \forall xq).$$

2° 记 $p_1 = \exists xp \vee \exists xq$.

$p_1$ 与以下各公式等价:

| | |
|---|---|
| $p_2 = \neg(\neg(\exists xp \vee \exists xq))$, | (双重否定) |
| $p_3 = \neg(\forall xp^* \wedge \forall xq^*)$, | (用对偶律) |
| $p_4 = \neg\forall x(p^* \wedge q^*)$, | (由 1°) |
| $p_5 = \exists x((p^*)^* \vee (q^*)^*)$, | (用对偶律) |
| $p_6 = \exists x(p \vee q)$, | (由后面练习 16 题 2) |

$\vdash p_1 \leftrightarrow p_6$ 即为 2°.

3° 由命题 2-2°, 有

$$\vdash (\neg p \to Qxq) \leftrightarrow Qx(\neg p \to q),\ \text{此即 } 3°.$$

4° 记 $p_1 = p \wedge Qxq$, 即 $p_1 = \neg(p \to \neg Qxq)$.

$p_1$ 与以下各式等价:

| | |
|---|---|
| $p_2 = \neg(p \to Q^*x\neg q)$, | (由命题 2-3°) |

$p_3 = \neg Q^* x(p \to \neg q)$, (由命题 2-2°)

$p_4 = Q x \neg (p \to \neg q) = Q x (p \wedge q)$. (由命题 2-3°)

$\vdash p_1 \leftrightarrow p_4$ 即为 4°. □

利用命题 3，可找出例 1 中 $p$ 的另一种等价前束范式.

首先，因 $(r \to s) \leftrightarrow (\neg r \vee s)$ 是永真式，例 1 中的 $p$ 等价于下面的 $q_1$：

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

由 $q_1$ 出发，可得以下等价公式 $q_2 \sim q_8$：

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

(由 De. Morgan 律和双重否定律)

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

(由命题 3-3°)

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

(由命题 2-3°)

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

(由命题 3-1°)

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

(由命题 2-1°)

$$q_7 = \forall x_1 \exists x_2 (\exists x_3 R_1^3(c_1, x_1, x_3) \wedge \neg (R_1^2(x_2, c_2) \vee R_1^1(x_1))),$$

(由命题 3-4°)

$$q_8 = \forall x_1 \exists x_2 \exists x_3 (R_1^3(c_1, x_1 . x_3) \wedge \neg (R_1^2(x_2, c_2) \vee R_1^1(x_1))).$$

(由命题 3-4°)

$q_8$ 为另一种与例 1 中 $p$ 等价的前束范式.

前束范式常比其他形式的公式有更容易理解的逻辑结构.

一般说来，前束范式解释上的复杂性依赖于量词词性改变的次数. 考察以下两个公式:

$$\forall x_1 \forall x_2 \forall x_3 \forall x_4 R_1^2(f_1^2(x_1, x_2), f_1^2(x_3, x_4)),$$

$$\forall x_1 \exists x_2 \forall x_3 \exists x_4 R_1^2(f_1^2(x_1, x_2), f_1^2(x_3, x_4)),$$

前者比后者更容易理解和解释.

**定义 2 ($\Pi_n$ 型和 $\Sigma_n$ 型前束范式)** 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 $\Pi_n$ 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 $\Sigma_n$ 型前束范式.

**例 2** 设 $p = \forall x_1 \forall x_2 R_1^2(x_1, x_2) \to \forall x_3 \exists x_4 R_1^2(x_3, x_4)$.
$p$ 等价于

$$p_1 = \exists x_1 \exists x_2 \forall x_3 \exists x_4 (R_1^2(x_1, x_2) \to R_1^2(x_3, x_4)),$$

又等价于

$$p_2 = \forall x_3 \exists x_4 \exists x_1 \exists x_2 (R_1^2(x_1, x_2) \to R_1^2(x_3, x_4)),$$

$p_1$ 是 $\Sigma_3$ 型，而 $p_2$ 是 $\Pi_2$ 型.

### 练习 16

1. 设 $x$ 不在 $q$ 中自由出现. 求证

   1° $\vdash (\exists x p \to q) \to \forall x (p \to q)$.

   2° $\vdash \exists x (p \to q) \to (\forall x p \to q)$.

2. 设 $p^*$ 是定理 2 中定义的 $p$ 的对偶公式. 求证

$$\vdash (p^*)^* \leftrightarrow p.$$

3. 找出与所给公式等价的前束范式.

   1° $\forall x_1 R_1^1(x_1) \to \forall x_2 R_1^2(x_1, x_2)$.

   2° $\forall x_1 (R_1^2(x_1, x_2) \to \forall x_2 R_1^2(x_1, x_2))$.

   3° $\forall x_1 (R_1^1(x_1) \to R_1^2(x_1, x_2)) \to (\exists x_2 R_1^1(x_2) \to \exists x_3 R_1^2(x_2, x_3))$.

   4° $\exists x_1 R_1^2(x_1, x_2) \to (R_1^1(x_1) \to \neg \exists x_3 R_1^2(x_1, x_3))$.

4. 设 $y$ 不在 $p(x)$ 中出现，$x$ 不在 $q(y)$ 中出现. 证明公式 $\exists x p(x) \to \exists y q(y)$ 与一 $\Pi_2$ 型前束范式等价，也与一 $\Sigma_2$ 型前束范式等价.

5. 找一 $\Pi_3$ 型前束范式，它与一 $\Sigma_2$ 型前束范式等价.

## 2.2 谓词演算的语义

研究谓词演算这种形式系统的语义，需用系统外部的某种结构对该系统给以解释. 这里说的外部结构往往正是我们想要研究的某类数学结构.

### 2.2.1 谓词演算 $K$ 的解释域与项解释

**定义 1 ($K$ 的解释域)** 设非空集 $M$ 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 $M$ 上的 $n$ 元运算 $\overline{f_i^n}$ 与之对应:

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

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

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

带有上述三个映射的非空集 $M$ 叫做 $K$ 的解释域.

上面的定义指出，解释域是有内部结构的非空集，其中规定有特殊元素 $\overline{c_i}$ 及特殊 $n$ 元关系 $\overline{R_i^n}$; 当 $K$ 的运算符集 $F \neq \varnothing$ 时，解释域是个代数系统 ($\overline{f_i^n}$ 是其上的 $n$ 元运算).

解释域的元素叫做个体对象. 解释域通常也叫做“解释”或“结构”.

给定了解释域 $M$, $K$ 中只涉及闭项 (即不含有个体变元的项) 的原子公式便有了实际含义，立即可解释为关于 $M$ 的元素的命题.

**例 1** 设 $K$ 中的 $c = \{c_1\}$, $F = \{f_1^1, f_1^2, f_2^2\}$, $R = \{R_1^2\}$. 下面的 $\mathbf{N}$ 是 $K$ 的一个解释域:

$\mathbf{N} = \{0, 1, 2, \cdots\}$,

$\overline{c_1} = 0$,

$\overline{f_1^1}$ : 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 (=).

还可如下给出 $K$ 的另一个解释域:

$\mathbf{Q}^+$ : 正有理数全体,

$\overline{c_1} = 1$,

$\overline{f_1^1}$ : 倒数函数,

$\overline{f_1^2}$ : 乘法 (×),

$\overline{f_2^2}$ : 除法 (÷),

$\overline{R_1^2}$ : 相等 (=).

现考察 $K$ 中只含有闭项的原子公式 $p$ :

$$R_1^2(f_1^2(f_1^1(c_1), c_1),\ f_2^2(f_1^1(c_1), c_1)).$$

$p$ 在解释域 $\mathbf{N}$ 中解释成

$$(0 + 1) + 0 = (0 + 1) \times 0,$$

这是假命题. 但 $p$ 在第二个解释域 $\mathbf{Q}^+$ 中解释成

$$\frac{1}{1} \times 1 = \frac{1}{1} \div 1,$$

这是真命题.

以上讨论说明，有了解释域才有可能谈论 $K$ 中公式的真假值. 但是光有解释域还不能立即给所有公式 (例如含有个体变元的原子公式 $R_1^2(x_1,x_2)$) 都赋以确定的真假值，这是因为个体变元的解释还没有明确. 更一般地，还需要引入“项解释”，先把项集 $T$ 与给定的解释域联系起来.

现设 $M$ 是已经给定的一个解释域，此时每个常元 $c_i$ 对应有 $\overline{c_i}\in M$, 每个 $f_i^n$ 对应有 $M$ 的 $n$ 元运算 $\overline{f_i^n}$. 为引入项解释的定义，先回忆项集 $T$ 的构造. $T$ 中的项仅有以下形式:

(i) 变元 $x_i$ 是项，常元 $c_i$ 是项;

(ii) 若 $t_1,\cdots,t_n$ 是项，则 $f_i^n(t_1,\cdots,t_n)$ 也是项.

我们把映射 $\varphi_0:X\to M$ 叫做个体变元的 (个体) 对象指派. $\varphi_0$ 给变元 $x_i$ 指派的个体对象是 $\varphi_0(x_i)\ (\in M)$. 有了变元指派 $\varphi_0$, 便可按层递归定义项解释 $\varphi:T\to M$ 如下. 首先令

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

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

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

上式右边是 $M$ 中进行的运算. (2) 式称作项解释 $\varphi$ 的“保运算性”.

特殊情形，当 $K$ 中的运算集 $F=\varnothing$ 时，项解释就是满足 $\varphi(c_i)=\overline{c_i}$ 的映射

$$\varphi:X\cup C\to M.$$

上述定义可概括为:

对给定的解释域 $M$, 项解释 $\varphi$ 是指具有性质 (1) 与 (2) 的映射 $\varphi:T\to M$.

项解释 $\varphi$ 由个体变元的指派 $\varphi_0$ 完全确定. $\varphi_0$ 可随意取. 只要 $\varphi_0$ 取定，变元有了指派，则每个项都随之有了由 (1) 与 (2) 所确定的解释. 不同的 (变元) 指派确定了不同的项解释. 反之，不同的项解释对应着不同的 (变元) 指派. (由给定的指派 $\varphi_0$ 所确定的项解释 $\varphi$ 的唯一性，对项的层次归纳即可证明. ) 对同一解释域 $M$, 可有许多不同的变元指派，因而存在许多不同的项解释.

一句话: 给定解释域 $M$, 只要变元有了解释 (指派)，便有了确定的项解释，即每个项都在 $M$ 中有了解释.

对固定的解释域 $M$, 把所有的项解释组成的集记作 $\Phi_M$ :

$$\Phi_M=\{\varphi\mid\varphi:T\to M\ \text{是项解释}\}.$$

**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 $\varphi,\varphi'\in\Phi_M$ 满足条件

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

则把 $\varphi'$ 叫做 $\varphi$ 的 $x$ 变通. (此时 $\varphi$ 与 $\varphi'$ 互为对方的 $x$ 变通. )

由定义知，互为 $x$ 变通的 $\varphi$ 与 $\varphi'$ 的差别仅在于对变元 $x$ 的指派可能不同 (也可

以相同)，而它们对其他变元的指派则全都相同. 这个概念将用于对含有量词的公式的解释.

在固定的解释域 $M$ 中，变元的指派 $\varphi_0$ 一经给定 (因而对应有确定的项解释 $\varphi$) 之后，每个原子公式便立即可解释为关于 $M$ 中个体对象的命题.

本章中用 $\bar{x}$ 表示对变元 $x$ 的指派，即 $\varphi_0(x)=\bar{x}$.

回到例 1 中的 $K$ 和它的解释域 $\mathbf{N}$. 考察原子公式 $p$:

$$R_1^2(f_1^2(x_1,x_2),\ f_2^2(x_3,f_1^1(x_4))).$$

在 $\mathbf{N}$ 中，若指派 $\overline{x_1}=5$, $\overline{x_2}=6$, $\overline{x_3}=7$, $\overline{x_4}=8$ (其余的变元可任意指派)，则 $f_1^2(x_1,x_2)$ 和 $f_2^2(x_3,f_1^1(x_4))$ 在 $\mathbf{N}$ 中分别解释为 $\overline{f_1^2}(\overline{x_1},\overline{x_2})$ 和 $\overline{f_2^2}(\overline{x_3},\overline{f_1^1}(\overline{x_4}))$, 即

$$\overline{x_1}+\overline{x_2}\,(=5+6)$$

和

$$\overline{x_3}\times(\overline{x_4}+1)\,(=7\times(8+1)).$$

这时公式 $p$ 在 $\mathbf{N}$ 中解释为

$$5+6=7\times(8+1),$$

这是假命题.

若重新指派 $\overline{x_1}=6$, $\overline{x_2}=8$, $\overline{x_3}=7$, $\overline{x_4}=1$, 则 $p$ 在 $\mathbf{N}$ 中解释为

$$6+8=7\times(1+1).$$

这是真命题.

## 练习 17

1. 设 $K$ 中 $C=\{c_1\}$, $F=\varnothing$, $R=\{R_1^1,R_2^1,R_1^2\}$. 已知 $E_1$, $E_2\subseteq\mathbf{Q}$, $\mathbf{Q}$ 为有理数集. 令 $\overline{c_1}=0$, $\mathbf{Q}$ 上一元关系 $\overline{R_1^1}$ 为 $E_1$, $\overline{R_2^1}$ 为 $E_2$, 二元关系 $\overline{R_1^2}$ 为 “$>$”. 这样, $\mathbf{Q}$ 便成了 $K$ 的解释域. 现已知关于 $\mathbf{Q}$ 中元素的两个命题:

命题甲: “若数集 $E_1$ 中某数比零大，则数集 $E_2$ 中所有数都比零大.”

命题乙: “并非 $E_1$ 中的数都小于或等于 $E_2$ 中的每个数.”

试把命题甲，乙分别按以下要求用 $K$ 中公式表示出来:

(1) 出现全称量词.

(2) 不出现全称量词.

(3) 写成前束范式.

2. 设 $\varphi$, $\psi\in\Phi_M$. 求证: 若对项 $t$ 中的任一变元 $x$ 都有 $\varphi(x)=\psi(x)$, 则 $\varphi(t)=\psi(t)$.

3. 设 $t\in T$, $\varphi$ 和 $\varphi'\in\Phi_M$, $\varphi'$ 是 $\varphi$ 的 $x$ 变通，且 $\varphi'(x)=\varphi(t)$. 用项 $t$ 代换项 $u(x)$ 中 $x$ 所得的项记为 $u(t)$. 求证 $\varphi'(u(x))=\varphi(u(t))$.

### 2.2.2 公式的赋值函数

讨论 $K$ 中公式的真假，复杂性在于: 这种真假首先与解释域有关; 其次与变元指派 (因而与项解释) 有关; 第三，当公式中有量词出现时，与项解释的变元变通有关.

现在可以完整地给出 $K$ 中公式真值概念的定义. 具体的做法是: 先固定解释域 $M$, 然后把公式的真值作为项解释 $\varphi$ 的函数进行归纳定义. 定义从原子公式开始，对公式的所在层次归纳. 注意谓词 $R_i^n$ 解释为 $M$ 上的 $n$ 元关系 $\overline{R_i^n}$.

记 $\bar{x}=\varphi(x)$ (意思是: 给 $x$ 指派 $M$ 中的个体 $\bar{x}$)，并记 $\bar{t}=\varphi(t)$ (意思是: 项 $t$ 解释为 $M$ 中的个体 $\bar{t}$).

**定义 1 (公式的赋值函数)** 设 $M$ 是给定的解释域，$p$ 是 $K$ 中任一公式. 由公式 $p$ 按下面的方式归纳定义的函数 $|p|: \Phi_M \to \mathbf{Z}_2$ 叫做公式 $p$ 的赋值函数.

对任一项解释 $\varphi \in \Phi_M$,

(i) 当 $p$ 为原子公式 $R_i^n(t_1,\cdots,t_n)$ 时，令

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

(ii) 当 $p$ 是 $\neg q$ 或 $q\to r$ 时，令

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

$$|q\to r|(\varphi)=|q|(\varphi)\to|r|(\varphi);$$

(iii) 当 $p$ 是 $\forall xq$ 时，令

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

由上面的定义可知，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 $|p|$. 它的自变量是项解释 $\varphi\in\Phi_M$, 函数值 $|p|(\varphi)$ 取 1 或 0. 若 $|P|(\varphi)=1$, 则说公式 $p$ 对于给定解释域 $M$ 和给定的项解释 $\varphi$ 为真; 若 $|p|(\varphi)=0$, 则说 $p$ 对于该 $M$ 和 $\varphi$ 为假.

定义 1 (i) 中对原子公式真值的规定，体现了 $M$ 上的 $n$ 关系 $\overline{R_i^n}$ 正是 $R_i^n$ 的解释.

定义 1 (ii) 保证了公式的赋值函数的计算在涉及到 $\neg$ 和 $\to$ 时与命题演算一致，仍具有赋值对 $\neg$ 和 $\to$ 所具有的保运算性.

定义 1 (iii) 对 $|\forall xq|(\varphi)$ 的规定，符合对以全称量词开头的公式 $\forall xq$ 的直观理解: 若不论重新指派 $x$ 为哪一个个体对象 (其他变元的指派不变) 时，$q$ 所表示的性质都成立 ($|q|(\varphi')=1$)，则规定 $|\forall xq|(\varphi)=1$; 若重新指派 $x$ 为某个个体对象时，$q$ 所表示的性质不成立 ($|q|(\varphi')=0$), 则规定 $|\forall xq|(\varphi)=0$.

**例 1** 仍用 2.2.1 例 1 中的 $K$ 和它的解释域 $\mathbf{N}$. 设

$p_1$ 是公式 $R_1^2(f_2^2(x_1,x_2),\ f_2^2(x_3,x_4))$,

$p_2$ 是公式 $\forall x_1 R_1^2(f_1^2(x_1,x_2),\ f_1^2(x_2,x_1))$,

$p_3$ 是公式 $\forall x_1 R_1^2(x_1,f_1^1(f_1^1(c_1)))$.

取项解释 $\varphi$ 满足

| | | | | | |
|---|---|---|---|---|---|
| $x_i$: | $x_1$ | $x_2$ | $x_3$ | $x_4$ | $\cdots$ |
| $\overline{x_i}$: | 2 | 6 | 3 | 4 | $\cdots$ |

下面来计算 $|p_1|(\varphi)$, $|p_2|(\varphi)$, $|p_3|(\varphi)$. (计算前最好从直观上把所给公式的涵义看清楚，例如 $p_1$ 的直观意思是 $x_1\times x_2=x_3\times x_4$.) 计算中注意项解释的性质 (2.2.1 小节中 (1) 与 (2)).

1° 所给 $p_1$ 是原子公式. 为了计算 $|p_1|(\varphi)$, 只用检验是否有

$$(\overline{f_2^2(x_1,x_2)},\ \overline{f_2^2(x_3,x_4)})\in\overline{R_1^2},$$

即看是否有 $\overline{f_2^2(x_1,x_2)}=\overline{f_2^2(x_3,x_4)}$. 简单地计算指出 $|p_1|(\varphi)=1$. 事实上，

$$\overline{f_2^2(x_1,x_2)}=\overline{f_2^2}(\overline{x_1},\overline{x_2})=\overline{x_1}\times\overline{x_2}=2\times 6,$$

$$\overline{f_2^2(x_3,x_4)}=\overline{f_2^2}(\overline{x_3},\overline{x_4})=\overline{x_3}\times\overline{x_4}=3\times 4.$$

2° 把 $R_1^2(f_1^2(x_1,x_2),\ f_1^2(x_2,x_1))$ 记为 $q$, 则 $p_2$ 是 $\forall x_1 q$.

设 $\varphi'$ 是 $\varphi$ 的任意 $x_1$ 变通. 为计算 $|q|(\varphi')$, 注意:

$$\begin{aligned}\varphi'(f_1^2(x_1,x_2)) &= \overline{f_1^2}(\varphi'(x_1),\ \varphi'(x_2))\\ &= \varphi'(x_1)+\varphi'(x_2)\\ &= \varphi'(x_1)+\varphi(x_2)\\ &= \varphi'(x_1)+6,\\ \varphi'(f_1^2(x_2,x_1)) &= \varphi(x_2)+\varphi'(x_1)=6+\varphi'(x_1).\end{aligned}$$

这说明

$$(\varphi'(f_1^2(x_1,x_2)),\ \varphi'(f_1^2(x_2,x_1)))\in\overline{R_1^2},$$

故 $|q|(\varphi')=1$. 由 $\varphi'$ 的任意性及定义 1 (iii) 便知 $|p_2|(\varphi)=1$.

3° 把 $R_1^2(x_1,f_1^1(f_1^1(c_1)))$ 记为 $q$, 则 $p_3$ 是 $\forall x_1 q$. 现取 $\varphi$ 的 $x_1$ 变通 $\varphi'$ 满足 $\varphi'(x_1)=3$, 则有 $|q|(\varphi')=0$. 这是因为

$$\varphi'(f_1^1(f_1^1(c_1)))=\overline{f_1^1}(\overline{f_1^1}(0))=(0+1)+1=2\neq\varphi'(x_1).$$

根据定义 1 (iii)，$|p_3|(\varphi)=0$.

**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 $\varphi$ 的 $x$ 变通 $\varphi'$ 使 $|q|(\varphi')=1$.

**证** 只证 1°, 4°. (2°, 3° 与 1° 类似.)

$$
\begin{aligned}
1^\circ\ |p \vee q|(\varphi) &= |\neg p \to q|(\varphi) && \text{(2.1.2 小节中 } \vee \text{ 的定义)}\\
&= |\neg p|(\varphi) \to |q|(\varphi) && \text{(定义 1 (ii))}\\
&= \neg |p|(\varphi) \to |q|(\varphi) && \text{(定义 1 (ii))}\\
&= |p|(\varphi) \vee |q|(\varphi). && \text{(1. 3. 1 小节中公式 6)}
\end{aligned}
$$

$4^\circ\ |\neg \forall x \neg q|(\varphi) = 1$

$\Leftrightarrow\ \neg |\forall x \neg q|(\varphi) = 1$ (定义 1 (ii))

$\Leftrightarrow\ |\forall x \neg q|(\varphi) = 0$

$\Leftrightarrow$ 存在 $\varphi$ 的 $x$ 变通 $\varphi'$ 使 $|\neg q|(\varphi') = 0$ (定义 1 (iii))

$\Leftrightarrow$ 存在 $\varphi$ 的 $x$ 变通 $\varphi'$ 使 $\neg |q|(\varphi') = 0$

$\Leftrightarrow$ 存在 $\varphi$ 的 $x$ 变通 $\varphi'$ 使 $|q|(\varphi') = 1$. □

命题 1-1°, 2°, 3° 说明赋值函数的计算对 $\vee, \wedge$ 及 $\leftrightarrow$ 仍有保运算性.

命题 1-4° 说明 $|\exists x q|(\varphi) = 1$ 的意思与直观相符: $M$ 中存在着这样的个体对象, 当它作为 $x$ 的解释时, $q$ 所表示的性质成立.

## 练习 18

1. 设 $K$ 中的 $C = \{c_1\}$, $F = \{f_1^1, f_1^2, f_2^2\}$, $R = \{R_1^2\}$. 它的一个解释域是 $\mathbf{N} = \{0, 1, 2, \cdots\}$, $\overline{c_1} = 0$, $\overline{f_1^1}$ 是后继函数, $\overline{f_1^2}$ 是 $+$, $\overline{f_2^2}$ 是 $\times$, $\overline{R_1^2}$ 是 $=$. 试对以下公式分别找出 $\varphi, \psi \in \Phi_{\mathbf{N}}$, 使 $|p|(\varphi) = 1$, $|p|(\psi) = 0$, 其中 $p$ 为:

1° $R_1^2(f_1^2(x_1, x_1), f_2^2(x_2, x_3))$.

2° $R_1^2(f_1^2(x_1, c_1), x_2) \to R_1^2(f_1^2(x_1, x_2), x_3)$.

3° $\neg R_1^2(f_2^2(x_1, x_2), f_2^2(x_2, x_3))$.

4° $\forall x_1 R_1^2(f_2^2(x_1, x_2), x_3)$.

5° $\forall x_1 R_1^2(f_2^2(x_1, c_1), x_1) \to R_1^2(x_1, x_2)$.

2. 已知 $K$ 中 $C = \{c_1\}$, $F = \{f_1^2\}$, $R = \{R_1^2\}$, 还已知 $K$ 的解释域 $\mathbf{Z}$ (整数集), $\overline{c_1} = 0$, $\overline{f_1^2}$ 是减法, $\overline{R_1^2}$ 是 “$<$”. 试给出 $\varphi, \psi \in \Phi_{\mathbf{Z}}$, 使 $|p|(\varphi) = 1$, $|p|(\psi) = 0$, 其中 $p$ 为:

1° $R_1^2(x_1, c_1)$.

2° $R_1^2(f_1^2(x_1, x_2), x_1) \to R_1^2(c_1, f_1^2(x_1, x_2))$.

3° $\neg R_1^2(x_1, f_1^2(x_1, f_1^2(x_1, x_2)))$.

4° $\forall x_1 R_1^2(f_1^2(x_1, x_2), x_3)$.

5° $\forall x_1 R_1^2(f_1^2(x_1, c_1), x_1) \to R_1^2(x_1, x_2)$.

6° $\forall x_1 \forall x_2 (R_1^2(f_1^2(x_1, x_2), c_1) \to R_1^2(x_1, x_2))$.

### 2.2.3 闭式的语义特征

一个直观上明显的事实是：项的解释只与在该项中出现的变元的指派有关，与其他变元的指派无关；公式的真值也只与在该公式中出现的自由变元指派有关，而与其他变元的指派无关. 这就是下面的命题 1.

**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 $p$ 中任一自由出现的变元 $x$ 都有 $\varphi(x) = \psi(x)$, 则 $|p|(\varphi) = |p|(\psi)$.

**证** 1° 见练习 17 题 2.

2° 对 $p$ 在 $K(Y)$ 中的层次数 $k$ 归纳.

$k = 0$ 时，设 $p$ 是 $R_j^n(t_1, \cdots, t_n)$, 此时项 $t_1, \cdots, t_n$ 中出现的变元都是在 $p$ 中自由出现的. 由已知条件和 1°, 有

$$\varphi(t_i) = \psi(t_i), \quad i = 1, \cdots, n.$$

于是

$$\begin{aligned} |p|(\varphi) = 1 &\Leftrightarrow (\varphi(t_1), \cdots, \varphi(t_n)) \in \overline{R_j^n} && \text{(2.2.2小节定义 1(i))} \\ &\Leftrightarrow (\psi(t_1), \cdots, \psi(t_n)) \in \overline{R_j^n} \\ &\Leftrightarrow |p|(\psi) = 1, \end{aligned}$$

这说明 $|p|(\varphi) = |p|(\psi)$.

$k > 0$ 时有以下三种情形.

(i) $p$ 为 $\neg q$, 此时

$$\begin{aligned} |\neg q|(\varphi) = 1 &\Leftrightarrow |q|(\varphi) = 0 \\ &\Leftrightarrow |q|(\psi) = 0 && \text{(由归纳假设)} \\ &\Leftrightarrow |\neg q|(\psi) = 1. \end{aligned}$$

(ii) $p$ 为 $q \to r$ 时，

$$\begin{aligned} |q \to r|(\varphi) = 1 &\Leftrightarrow |q|(\varphi) \to |r|(\varphi) = 1 \\ &\Leftrightarrow |q|(\psi) \to |r|(\psi) = 1 && \text{(由归纳假设)} \\ &\Leftrightarrow |q \to r|(\psi) = 1. \end{aligned}$$

(iii) $p$ 为 $\forall x q$ 时，先设 $|\forall x q|(\varphi) = 1$, 由此来证明 $|\forall x q|(\psi) = 1$.

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. 在 $q$ 中自由出现的其他任何变元 $y (\neq x)$ 也在 $p$ 中自由出现. 于是有

$$\begin{aligned} \varphi'(y) &= \varphi(y) && \text{($x$ 变通的定义)} \\ &= \psi(y) && \text{(已知)} \\ &= \psi'(y). && \text{($x$ 变通的定义)} \end{aligned}$$

这样，对 $q$ 来说，$\varphi'$ 和 $\psi'$ 满足命题 1-2° 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 $|q|(\varphi') = 1$, 且得 $|q|(\psi') = 1$. 这就证明了 $|\forall x q|(\psi) = 1$.

完全对称地有

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

所以 $|\forall x q|(\varphi) = |\forall x q|(\psi)$. □

**定义 1 (公式在解释域中恒真与恒假)** 公式 $p$ 在解释域 $M$ 中恒真，记作 $|p|_M = 1$, 是指对任一 $\varphi \in \Phi_M$, $|p|(\varphi) = 1$;

公式 $p$ 在解释域 $M$ 中恒假，记作 $|p|_M = 0$, 是指对任一 $\varphi \in \Phi_M$, $|p|(\varphi) = 0$;

在解释域 $M$ 中非恒假公式叫做在 $M$ 中可满足公式.

**例 1** 仍用 2.2.1 小节例 1 中的 $K$ 和它的解释域 $\mathbf{N}$. 设 $p_1$ 是 $R_1^2(x_1, x_1)$, $p_2$ 是 $\forall x_1 R_1^2(x_1, c_1)$, $p_3$ 是 $R_1^2(x_1, c_1)$.

$|p_1|_{\mathbf{N}} = 1$. 这是因为对任意 $\varphi \in \Phi_{\mathbf{N}}$, $\varphi(x_1) = \varphi(x_1)$ 总成立，所以有

$$|R_1^2(x_1, x_1)|(\varphi) = 1.$$

$|p_2|_{\mathbf{N}} = 0$, 这是因为对任意 $\varphi \in \Phi_{\mathbf{N}}$, 总可作 $\varphi$ 的 $x_1$ 变通 $\varphi'$ 使 $\varphi'(x_1) = 1 \neq 0$, 因而使 $|R_1^2(x_1, c_1)|(\varphi') = 0$. 于是 $|\forall x_1 R_1^2(x_1, c_1)|(\varphi) = 0$.

$p_3$ 在 $\mathbf{N}$ 中既非恒真也非恒假:

取 $\varphi(x_1) \neq 0$ 时， $|R_1^2(x_1, c_1)|(\varphi) = 0$;

取 $\varphi(x_1) = 0$ 时， $|R_1^2(x_1, c_1)|(\varphi) = 1$.

$p_3$ 是在 $\mathbf{N}$ 中可满足公式.

下面的定理指出了闭式 (不含自由变元的公式) 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: 或 $|p|_M = 1$, 或 $|p|_M = 0$.

**证** 假设闭式 $p$ 在 $M$ 中不恒真，则有 $\varphi \in \Phi_M$ 使 $|p|(\varphi) = 0$. 任取 $\psi \in \Phi_M$. 因 $p$ 中没有自由变元，根据命题 1-2°, 有 $|p|(\psi) = |p|(\varphi) = 0$. 这样，$p$ 在 $M$ 中恒假. □

**例 2** 设 $K$ 中 $C = \{c_1\}$, $F = \{f_1^1\}$, $R = \{R_1^1\}$, $p$ 是公式 $\forall x_1 (R_1^1(x_1) \to R_1^1(f_1^1(x_1)))$. 可以给出解释域 $M_1$ 和 $M_2$, 使 $|p|_{M_1} = 1$ 而 $|p|_{M_2} = 0$.

1° 取 $M_1 = \mathbf{Z}$ (整数集)，$\overline{c_1} = 0$, $\overline{f_1^1}$ 为后继函数，$\mathbf{Z}$ 上一元关系 $\overline{R_1^1}$ 为 $\mathbf{Z}^+$ ($\mathbf{Z}^+$ 是正整数集).

对任一 $\varphi \in \Phi_{M_1}$, 任取 $\varphi$ 的 $x_1$ 变通 $\varphi'$, 有

$$\begin{aligned} |R_1^1(x_1)|(\varphi') = 1 &\Rightarrow \varphi'(x_1) \in \mathbf{Z}^+ \\ &\Rightarrow \varphi'(f_1^1(x_1)) = \overline{f_1^1}(\varphi'(x_1)) = \varphi'(x_1) + 1 \in \mathbf{Z}^+ \\ &\Rightarrow |R_1^1(f_1^1(x_1))|(\varphi') = 1, \end{aligned}$$

由此得

$$|R_1^1(x_1) \to R_1^1(f_1^1(x_1))|(\varphi')$$

$$= |R_1^1(x_1)|(\varphi') \to |R_1^1(f_1^1(x_1))|(\varphi') = 1.$$

$\varphi'$ 是 $\varphi$ 的任取的 $x_1$ 变通，故又得

$$|\forall x_1(R_1^1(x_1) \to R_1^1(f_1^1(x_1)))|(\varphi) = 1.$$

最后由 $\varphi$ 的任意性得 $|p|_{M_1} = 1$.

2° 取 $M_2 = \mathbf{Z}$, $\overline{c_1} = 0$, $\overline{f_1^1}$ 为后继函数，$\overline{R_1^1}$ 为偶数集. 此时对任意 $\varphi \in \Phi_{M_2}$, 可取 $\varphi$ 的 $x_1$ 变通 $\varphi'$ 使 $\varphi'(x_1)$ 是偶数. 这时有

$|R_1^1(x_1)|(\varphi') = 1$ 但 $|R_1^1(f_1^1(x_1))|(\varphi') = 0$,

$|R_1^1(x_1) \to R_1^1(f_1^1(x_1))|(\varphi') = 0$,

$|\forall x_1(R_1^1(x_1) \to R_1^1(f_1^1(x_1)))|(\varphi) = 0$.

因 $\varphi$ 是任意的，故 $|p|_{M_2} = 0$.

在建立 $K$ 时我们了解，为了证明 $\Gamma \vdash p$ 这样的结论，希望假定集 $\Gamma$ 中的闭式越多越好. 在用演绎定理、反证律和归谬律时，若涉及到的假定是闭式时，则可不必顾及对 Gen 变元所加的限制条件. 现在此事可从语义上找到一些解释. 因为闭式中不含有自由出现的变元，因此它的真值与变元的指派无关，与项解释无关. 对给定的解释域，闭式的真假具有确定性: 要么恒真，要么恒假. “确定性”是对“前题”的合理要求.

在进行语义讨论时，常要用到下面的命题 2.

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

**证** $(\Rightarrow)$

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

$\Rightarrow |p|_M = 1$. □

上面例 2 的前一部分讨论因命题 2 可得一点简化: 只要证明

$$|R_1^1(x_1) \to R_1^1(f_1^1(x_1))|_{M_1} = 1$$

就行了.

**定义 2 (全称闭式)** 设 $x_{i_1}, \cdots, x_{i_n}$ 是在 $p$ 中自由出现的全部变元，则

$$\forall x_{i_1} \cdots \forall x_{i_n} p$$

叫做 $p$ 的全称闭式.

**命题 3** 设 $p'$ 是 $p$ 的全称闭式，则

$$|p|_M = 1 \quad \Leftrightarrow \quad |p'|_M = 1.$$

**证** $n$ 次利用命题 2. □

当 $p$ 不是闭式时，$|p'|_M$ 总有意义，但 $|p|_M$ 不一定有意义. 而命题 3 告诉我们，尽管 $p$ 可能不是闭式，但只要 $|p'|_M = 1$, $|p|_M$ 便一定有意义，而且等于 1. 当 $|p'|_M = 0$ 时，有两种可能: $|p|_M = 0$, 或 $|p|_M$ 没有意义.

**命题 4** $|p|_M = 0 \quad \Rightarrow \quad |\forall x\, p|_M = 0.$

**证** $|p|_M = 0$ 时，对任意 $\varphi \in \Phi_M$, $|p|(\varphi) = 0$. 于是 $|\forall x\, p|(\varphi) = 0$. (若 $|\forall x\, p|(\varphi) = 1$, 则 $|p|(\varphi) = 1$.) $\varphi$ 是任意的，故 $|\forall x\, p|_M = 0$. □

**推论 1** $|p|_M = 0 \quad \Rightarrow \quad |p'|_M = 0$, 这里 $p'$ 是 $p$ 的全称闭式.

命题 4 的逆命题不真. 仍以 2.2.1 小节例 1 中的 $K$ 和 $\mathbf{N}$ 为例，有 $|\forall x_1 R_1^2(x_1, c_1)|_{\mathbf{N}} = 0$, 但 $|R_1^2(x_1, c_1)|_{\mathbf{N}}$ 没有意义. (取 $\varphi(x_1) = 0$ 时，$|R_1^2(x_1, c_1)|(\varphi) = 1$; 而取 $\varphi(x_1) = 1$ 时 $|R_1^2(x_1, c_1)|(\varphi) = 0$.)

**命题 5** $|p|_M = 1$ 且 $|p \to q|_M = 1 \quad \Rightarrow \quad |q|_M = 1$,

**证** 任取 $\varphi \in \Phi_M$, 有

$$|p|(\varphi) = 1 \text{ 且 } |p \to q|(\varphi) = 1 \quad \Rightarrow \quad |q|(\varphi) = 1.$$ □

## 练习 19

1. 对 2.2.1 小节例 1 中的 $K$ 和 $\mathbf{N}$, 计算 $|p|_{\mathbf{N}}$, 其中 $p$ 为:

   1° $\forall x_1 R_1^2(f_2^2(x_1, c_1), x_1)$,

   2° $\forall x_1 \forall x_2 (R_1^2(f_1^2(x_1, c_1), x_2) \to R_1^2(f_1^2(x_2, c_1), x_1))$,

   3° $\forall x_1 \forall x_2 \exists x_3 R_1^2(f_1^2(x_1\, x_2), x_3)$,

   4° $\exists x_1 R_1^2(f_1^2(x_1, x_1),\ f_2^2(x_1, x_1))$.

2. 设 $K$ 中 $C = \{c_1\}$, $F = \{f_1^2\}$, $R = \{R_1^2\}$, 解释域 $\mathbf{Z}$ 是整数集. $\overline{c_1} = 0$, $\overline{f_1^2}$ 是减法, $\overline{R_1^2}$ 是"<". 求 $|p|_{\mathbf{Z}}$, 其中 $p$ 为:

   1° $\forall x_1 R_1^2(f_1^2(c_1, x_1), c_1)$,

   2° $\forall x_1 \forall x_2 \neg R_1^2(f_1^2(x_1, x_2), x_1)$,

   3° $\forall x_1 \forall x_2 \forall x_3 (R_1^2(x_1, x_2) \to R_1^2(f_1^2(x_1, x_3), f_1^2(x_2, x_3)))$,

   4° $\forall x_1 \exists x_2 R_1^2(x_1, f_1^2(f_1^2(x_1, x_2), x_2))$.

3. 设 $K$ 中 $C = \{c_1\}$, $F = \{f_1^2\}$, $R = \{R_1^2\}$. 试给出 $K$ 的两个解释域 $M_1$ 和 $M_2$, 使 $|p|_{M_1} = 1$ 而 $|p|_{M_2} = 0$, 其中 $p$ 为:

   1° $\forall x_1 \forall x_2 (R_1^2(f_1^2(x_1, x_2), c_1) \to R_1^2(x_1, x_2))$,

   2° $\forall x_1 (R_1^2(x_1, x_2) \to R_1^2(x_2, x_1))$.

4. 试证 $|p|_M = 1 \quad \Rightarrow \quad |\exists x\, p|_M = 1$. 反向是否成立? 说明理由.

### 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. $M$ 是公式集 $\Gamma$ 的模型，指 $\Gamma$ 的每个公式都在 $M$ 中恒真:

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

$\Gamma = \varnothing$ 时任何解释域都是 $\Gamma$ 的模型.

**定义 2 (语义推论)** 公式 $p$ 是公式集 $\Gamma$ 的语义推论，记作 $\Gamma \models p$, 指 $p$ 在 $\Gamma$ 的所有模型中都恒真，即: 在使 $\Gamma$ 的每个成员都恒真的解释域中，$p$ 也恒真；或者说，$\Gamma$ 的任何模型也都是 $\Gamma \cup \{p\}$ 的模型.

定义 2 也可写成

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

**定义 3 (有效式与满足公式)** $\varnothing \models p$ 时，$p$ 叫做 $K$ 的有效式，记为 $\models p$.

若 $\neg p$ 不是有效式，则 $p$ 叫做 $K$ 的可满足公式.

由有效式的定义可知

$$\models p \quad \Leftrightarrow \quad p \text{ 在 } K \text{ 的所有解释域中恒真}.$$

**命题 1** $K$ 中 (命题演算型) 永真式都是有效式.

**证** $K$ 的 (命题演算型) 永真式 (见 2.1.3 小节定义 2) 是指形为 $p(p_1, \cdots, p_n)$ 的公式，它由 $K$ 中的任意公式 $p_1, \cdots p_n$ 分别代换命题演算 $L$ 的永真式 $p(x_1, \cdots, x_n)$ 中的命题变元 $x_1, \cdots, x_n$ 所得. 注意 $p(p_1, \cdots, p_n)$ 由 $p_1, \cdots, p_n$ 经过 $\neg, \rightarrow$ 两种运算得到. 任取 $K$ 的解释域 $M$ 和 $\varphi \in \Phi_M$. 根据赋值计算对 $\neg\ \rightarrow$ 的保运算性，有

$$|p(p_1, \cdots, p_n)|(\varphi) = p(|p_1|(\varphi), \cdots, |p_n|(\varphi)).$$

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

$$|p(p_1, \cdots, p_n)|_M = 1.$$

又因 $M$ 是任意的，最后得 $\models p(p_1, \cdots, p_n)$. □

**推论 1** (K1), (K2), (K3) 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. □

注意命题 1 的逆命题不成立. $K$ 中有效式并非一定是 $K$ 中永真式 (见下面练习 20 题 1).

**命题 2** $\Gamma \models p$ 且 $\Gamma \models p \rightarrow q \quad \Rightarrow \quad \Gamma \models q$.

**证** 设 $M$ 是 $\Gamma$ 的任一模型. 当 $\Gamma \models p$ 且 $\Gamma \models p \rightarrow q$ 时，有

$$|p|_M = 1 \text{ 且 } |p \rightarrow q|_M = 1.$$

根据 2.2.3 小节命题 5，又有 $|q|_M = 1$, 所以 $\Gamma \models q$. □

**例 1** $\{R_1^1(x_1)\} \vDash \forall x_1 R_1^1(x_1)$. 事实上，根据 2.2.3 小节的命题 2，有

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

**例 2** $\nvDash R_1^1(x_1) \to \forall x_1 R_1^1(x_1)$ (即公式 $R_1^1(x_1) \to \forall x_1 R_1^1(x_1)$ 不是有效式). 为证此式，取 $M$ 为 $\mathbf{Z}$ (整数集)，$\overline{R_1^1}$ : "$> 0$". 再取 $\varphi \in \Phi_{\mathbf{Z}}$ 和 $\varphi$ 的 $x_1$ 变通 $\varphi'$ 使它们满足 $\varphi(x_1) = 2$, $\varphi'(x_1) = -2$. 这时有

$$|R_1^1(x_1)|(\varphi) = 1 \text{ 和 } |R_1^1(x_1)|(\varphi') = 0.$$

由后式得 $|\forall x_1 R_1^1(x_1)|(\varphi) = 0$. 这说明

$$|R_1^1(x_1) \to \forall x_1 R_1^1(x_1)|(\varphi) = 0,$$

即公式 $R_1^1(x_1) \to \forall x_1 R_1^1(x_1)$ 并非在任何解释域中都恒真. 回忆在建立 $K$ 的演绎定理时我们对 Gen 变元所加的限制. 语法上，我们有 $\{R_1^1(x_1)\} \vdash \forall x_1 R_1^1(x_1)$ (使用一次 Gen 规则就可以了). 但我们不能由此而利用演绎定理得出结论 $\vdash R_1^1(x_1) \to \forall x_1 R_1^1(x_1)$, 这是因为 Gen 变元 $x_1$ 在 $R_1^1(x_1)$ 中是自由的. 当我们把刚才的例 1 和例 2 加以比较后会发现，语法上对 Gen 变元所加的限制是有语义根据的. 例 1 的结论是合理的: 作为推理的前提条件，被假设为恒真的公式 $R_1^1(x_1)$ 中自由出现的变元 $x_1$ 可以推广. 而例 2 的公式 $R_1^1(x_1) \to \forall x_1 R_1^1(x_1)$ 直观上就能看出它有"以偏概全"的可能，它不是有效式.

**命题 3** $\Gamma \vDash p \quad \Leftrightarrow \quad \Gamma \vDash \forall x p$.

**证** $\Gamma \vDash p \;\Leftrightarrow\;$ 对于 $\Gamma$ 的任一模型 $M$, $|p|_M = 1$

$\Leftrightarrow\;$ 对于 $\Gamma$ 的任一模型 $M$, $|\forall x p|_M = 1$ (由 2.2.3 小节命题 2)

$\Leftrightarrow\; \Gamma \vDash \forall x p$. □

**命题 4** 设 $p'$ 是 $p$ 的全称闭式，则有

$$\Gamma \vDash p \quad \Leftrightarrow \quad \Gamma \vDash p'.$$

**证** 用命题 3 若干次. □

## 练习 20

1. 证明

   1° $\vDash \exists x_1 \forall x_2 R_1^2(x_1, x_2) \to \forall x_2 \exists x_1 R_1^2(x_1, x_2)$.

   2° $\vDash \forall x_1 R_1^1(x_1) \to (\forall x_1 R_2^1(x_1) \to \forall x_2 R_1^1(x_2))$.

   3° $\vDash \forall x(p \to q) \to (\forall x p \to \forall x q)$.

   4° $\vDash \forall x \forall y p \to \forall y \forall x p$.

2. 给出一个非闭的 $K$ 中有效式的例子.
3. 证明 $K$ 中以下公式都不是有效式.

   1° $\forall x_1 \exists x_2 R_1^2(x_1, x_2) \to \exists x_2 \forall x_1 R_1^2(x_1, x_2)$.

2° $\forall x_1 \forall x_2 (R_1^2(x_1, x_2) \to R_1^2(x_2, x_1))$.

3° $\forall x_1 (\neg R_1^1(x_1) \to \neg R_1^1(c_1))$.

4° $\forall x_1 R_1^2(x_1, x_1) \to \exists x_2 \forall x_1 R_1^2(x_1, x_2)$.

5° $\exists x_1 R_1^1(x_1) \to R_1^1(x_1)$.

4. 在 $K$ 中增加新的个体常元 $b_1, b_2, \cdots$, 其他不变，得到新的扩大的谓词演算 $K^+$. 设 $M$ 是 $K^+$ 的解释域 (也同时可看成是 $K$ 的解释域). 已知 $\varphi^+$ 和 $\varphi$ 分别是 $K^+$ 和 $K$ 的项解释，且满足 $\varphi^+(x_i) = \varphi(x_i)$, $i = 1, 2, \cdots$ . 求证:

(i) 对 $K$ 中的任何项 $t$, $\varphi^+(t) = \varphi(t)$,

(ii) 对 $K$ 中的任何公式 $p$, $|p|(\varphi^+) = |p|(\varphi)$.

## 2.3 $K$的可靠性

谓词演算 $K$ 的可靠性，是指

$$\Gamma \vdash p \quad \Rightarrow \quad \Gamma \models p.$$

特殊情形，当 $\Gamma = \varnothing$ 时，是指

$$\vdash p \quad \Rightarrow \quad \models p,$$

即 $K$ 的定理都是有效式.

为了证明 $K$ 的可靠性，还需要做的主要准备工作是证明 (K1)~(K5) 型公理是有效式. 先需要建立下面的引理. 注意下面在形为 $u(x)$ 的项与形为 $p(x)$ 的公式中，允许含有除 $x$ 以外的其他变元，还允许 $x$ 不在其中出现.

**引理 1** 对给定的解释域，设 $\varphi'$ 是项解释 $\varphi$ 的 $x$ 变通，且满足 $\varphi'(x) = \varphi(t)$, $t$ 是某个项.

1° 若 $u(x)$ 是项，则 $\varphi'(u(x)) = \varphi(u(t))$.

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 (注意 $x$ 可以不在 $u$ 中出现).

(i) $u(x) = c_i$, 此时 $u(t) = c_i$, $\varphi'(c_i) = \varphi(c_i)$.

(ii) $u(x) = y$, $y \neq x$, 此时也有 $u(t) = y$. $\varphi'$ 是 $\varphi$ 的 $x$ 变通，它与 $\varphi$ 对 $y$ 的取值是相同的，即 $\varphi'(y) = \varphi(y)$.

(iii) $u(x) = x$, 此时 $u(t) = t$, 所要证的等式 $\varphi'(u(x)) = \varphi(u(t))$ 就是已知条件 $\varphi'(x) = \varphi(t)$.

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

$$u(t)=f_i^n(t_1(t),\cdots,t_n(t)).$$

我们有

$$\begin{aligned}
\varphi'(u(x)) &= \varphi'(f_i^n(t_1(x),\cdots,t_n(x))) \\
&= \overline{f_i^n}(\varphi'(t_1(x)),\cdots,\varphi'(t_n(x))) && (\varphi'\text{是项解释}) \\
&= \overline{f_i^n}(\varphi(t_1(t)),\cdots,\varphi(t_n(t))) && (\text{由归纳假设}) \\
&= \varphi(f_i^n(t_1(t),\cdots,t_n(t))) && (\varphi\text{是项解释}) \\
&= \varphi(u(t)).
\end{aligned}$$

至此，证明 1° 的归纳过程完成.

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

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

于是

$$p(t)=R_i^n(t_1(t),\cdots,t_n(t)).$$

此时 $|p(x)|(\varphi')=|p(t)|(\varphi)$ 成立，即

$$|R_i^n(t_1(x),\cdots,t_n(x))|(\varphi')=|R_i^n(t_1(t),\cdots,t_n(t))|(\varphi)$$

成立，是因为

$$\begin{aligned}
&|R_i^n(t_1(x),\cdots,t_n(x))|(\varphi')=1 \\
&\Leftrightarrow\quad (\varphi'(t_1(x)),\cdots,\varphi'(t_n(x)))\in\overline{R_i^n} \\
&\Leftrightarrow\quad (\varphi(t_1(t)),\cdots,\varphi(t_n(t)))\in\overline{R_i^n} \\
&\qquad\qquad\qquad (\text{由}1^\circ, \varphi'(t_l(x))=\varphi(t_l(t)), l=1,\cdots,n) \\
&\Leftrightarrow\quad |R_i^n(t_1(t),\cdots,t_n(t))|(\varphi)=1
\end{aligned}$$

$k>0$ 时，分以下四种情形讨论.

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

$$\begin{aligned}
|p(x)|(\varphi')=1 &\Leftrightarrow\ |q(x)|(\varphi')=0 \\
&\Leftrightarrow\ |q(t)|(\varphi)=0 && (\text{归纳假设}) \\
&\Leftrightarrow\ |p(t)|(\varphi)=1.
\end{aligned}$$

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

$$|p(x)|(\varphi')=0\ \Leftrightarrow\ |q(x)|(\varphi')=1 \text{ 且 } |r(x)|(\varphi')=0$$

$$\Leftrightarrow \quad |q(t)|(\varphi) = 1 \text{ 且 } |r(t)|(\varphi) = 0 \qquad \text{(归纳假设)}$$

$$\Leftrightarrow \quad |p(t)|(\varphi) = 0.$$

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

(iv) 若 $p(x) = \forall y q(x)$ 且 $x$ 在 $p(x)$ 中自由出现，则 $y \neq x$ 且 $p(t) = \forall y q(t)$ (注意 $t$ 中不含 $y$，因已知 $t$ 对 $p(x)$ 中 $x$ 是自由的). 这时我们来证明

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

先证明向左的方向 ($\Leftarrow$).

设 $|p(t)|(\varphi) = 0$, 即 $|\forall y q(t)|(\varphi) = 0$. 这时存在 $\varphi$ 的 $y$ 变通 $\psi$ 使 $|q(t)|(\psi) = 0$. 再作 $\psi$ 的 $x$ 变通 $\psi'$, 使

(1) $\psi'(x) = \psi(t)$.

于是由归纳假设 (上面已有 $|q(t)|(\psi) = 0$) 可得

(2) $|q(x)|(\psi') = 0$.

$\psi$ 是 $\varphi$ 的 $y$ 变通，它与 $\varphi$ 对 $y$ 的指派可能不一致，对其他变元的指派都一致，而 $t$ 中不含 $y$, 利用 2.2.3 小节命题 1-1° 得

(3) $\psi(t) = \varphi(t)$.

现在可以证明 $\psi'$ 是 $\varphi'$ 的 $y$ 变通. 为此，要证当 $z \neq y$ 时总有 $\psi'(z) = \varphi'(z)$. 而当 $z \neq y$ 时，又有两种可能: $z \neq x$ 和 $z = x$.

$z \neq x$ 时，

$$\begin{aligned} \psi'(z) &= \psi(z) && (\psi'\text{是}\psi\text{的}x\text{变通}) \\ &= \varphi(z) && (\psi\text{是}\varphi\text{的}y\text{变通}) \\ &= \varphi'(z); && (\varphi'\text{是}\varphi\text{的}x\text{变通}) \end{aligned}$$

$z = x$ 时，

$$\begin{aligned} \psi'(z) = \psi'(x) &= \psi(t) && (\text{由(1)}) \\ &= \varphi(t) && (\text{由(3)}) \\ &= \varphi'(x) && (\text{原已知条件}) \\ &= \varphi'(z). && (z = x) \end{aligned}$$

这就证明了 $\psi'$ 是 $\varphi'$ 的 $y$ 变通，再由 (2) 式便得

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

剩下还要证明另一方向:

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

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

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

有了 $\psi'$, 再作 $\psi'$ 的 $x$ 变通 $\psi$, 使 $\psi(x)=\varphi(x)$. 这样, $\psi$ 和 $\varphi$ 除了对 $y$ 的指派可能不一致, 其他都是一致的, 所以 $\psi$ 是 $\varphi$ 的 $y$ 变通. 前面的 (3) 式这时仍然成立. 于是

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

再由归纳假设及 (4) 得

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

由此 (注意 $\psi$ 是 $\varphi$ 的 $y$ 变通) 即得

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

这就完成了证明 2° 的整个归纳过程. □

**引理 2** $K$ 的公理都是有效式.

**证** 1° (K1), (K2), (K3) 型公理都是永真式, 故都是有效式. (见 2.2.4 小节推论 1)

2° (K4) 是有效式, 验证如下:

设项 $t$ 对 $p(x)$ 中 $x$ 自由. 为证 $\models \forall x\, p(x)\to p(t)$, 任取解释域 $M$ 且任取 $\varphi\in\Phi_M$, 并先设

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

这时对于 $\varphi$ 的任一 $x$ 变通 $\varphi'$, 总有 $|p(x)|(\varphi')=1$. 现取 $\varphi$ 的一个特殊的 $x$ 变通 $\varphi'$, 使它满足 $\varphi'(x)=\varphi(t)$. 由引理 1-2° 得 $|p(t)|(\varphi)=|p(x)|(\varphi')=1$, 这说明

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

此式当 $|\forall x\, p(x)|(\varphi)=0$ 时是当然成立的. 由于 $\varphi$ 和 $M$ 都是任取的, 所以 $\forall x\, p(x)\to p(t)$ 是有效式.

3° (K5) 是有效式, 验证如下:

要证 $\models \forall x(p\to q)\to(p\to\forall x q)$, 其中 $x$ 不在 $p$ 中自由出现. 为此要证明对于任意的 $M$ 和任意的 $\varphi\in\Phi_M$, 下式成立

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

此式当 $|\forall x(p\to q)|(\varphi)=0$ 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. 现设 (5) 式成立, 这时对于 $\varphi$ 的任一 $x$ 变通 $\varphi'$, 有

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

又由 2.2.3 小节命题 1-2° 可得 (注意 $x$ 不在 $p$ 中自由出现)

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

由 (6)，(7) 得 $|q|(\varphi') = 1$, 进而可得 $|\forall x q|(\varphi) = 1$. □

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

**证** 设有 $p$ 从 $\Gamma$ 的证明 $p_1, \cdots, p_n$. 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，也有 $\Gamma \models p$.

$n > 1$ 时，有以下三种情形:

(i) 若 $p \in \Gamma$ 或 $p$ 为公理，则与 $n = 1$ 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 $\Gamma \models p_i$ 和 $\Gamma \models p_i \to p$. 再用 2.2.4 小节命题 2 得 $\Gamma \models p$.

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

**推论 1 (*K* 的无矛盾性)** $K$ 是无矛盾的，即: 对任何公式 $p$, $\vdash p$ 与 $\vdash \neg p$ 不同时成立.

**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 $\models p$ 和 $\models \neg p$. 这样，对任一解释域 $M$ 和任一 $\varphi \in \Phi_M$, 有

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

这是不可能的. □

**推论 2** $\Gamma$ 有模型 $\Rightarrow$ $\Gamma$ 是无矛盾的.

证明与推论 1 的证明类似. 留作练习.

我们已知道不能由 $\{R_1^1(x_1)\} \vdash \forall x_1 R_1^1(x_1)$ 用演绎定理推出 $\vdash R_1^1(x_1) \to \forall x_1 R_1^1(x_1)$. 前者是正确的，后者是否成立? 现在我们可以肯定地说，后者是不成立的. 如果它成立，那么由 $K$ 的可靠性得出 $\models R_1^1(x_1) \to \forall x_1 R_1^1(x_1)$, 而这是不成立的 (见 2.2.4 小节例 2).

## 练习 21

1. 证明推论 2: 有模型的公式集是无矛盾的.
2. $\vdash \exists x_2 R_1^2(x_1, x_2) \to \exists x_2 R_1^2(x_2, x_2)$ 是否成立?

## 2.4 K 的完全性

谓词演算 $K$ 的完全性是指

$$\Gamma \vDash p \quad \Rightarrow \quad \Gamma \vdash p.$$

作为特殊情况，指

$$\vDash p \quad \Rightarrow \quad \vdash p,$$

即 $K$ 的有效式一定是 $K$ 的定理.

证明 $K$ 的完全性，主要的工作是先证明下面的定理 1.

**定理 1** 无矛盾公式集一定有可数集模型.

**证** 设 $\Gamma$ 是个无矛盾公式集. 我们来给 $\Gamma$ 构造一个可数集模型 $M$.

整个过程分成以下六个步骤进行.

**1. 作扩大的谓词演算 $K^+$**

取可数个新的个体常元 $b_0, b_1, b_2, \cdots, B = \{b_0, b_1, b_2, \cdots\}$ 与原个体常元集 $C = \{c_0, c_1, c_2, \cdots\}$ 不相交.

扩大 $K$, 以 $C \cup B$ 为新的个体常元集，但个体变元集 $X$, 函数词集 $F$ 和谓词集 $R$ 保持不变，得到的新的谓词演算记作 $K^+$. $K$ 的项集 $T$ 是 $K^+$ 的项集 $T^+$ 的真子集.

$K$ 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 (有可数个) 全部取出排成不重复的一列:

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

其中 $y_n (= x_{i_n} \in X)$ 这些变元可以重复出现.

在 $B$ 中取出一串 $b_{i_0}, b_{i_1}, \cdots$, 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 $p_0(y_0), \cdots, p_n(y_n)$ 中出现，且 $b_{i_n} \notin \{b_{i_0}, \cdots, b_{i_{n-1}}\}$.

记

$$r_n = p_n(b_{i_n}) \to \forall y_n\, p_n(y_n),$$

并记

$$\Gamma' = \Gamma \cup \{r_0, r_1, r_2, \cdots\}.$$

现用反证法证明这样作出的 $\Gamma'$ 是无矛盾的公式集. 反设存在 $K^+$ 中的公式 $q$ 使

$\Gamma' \vdash_{K^+} q$ 与 $\Gamma' \vdash_{K^+} \neg q$ 同时成立，那么必有足够大的 $n$ 使

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

这是不可能的，现对上式左边 $r_i$ 的个数归纳证明这一点.

首先，$r_i$ 的个数为零时"$\Gamma \vdash_{K^+} q$ 及 $\neg q$"是不可能的. 这是因为: 如果 $\Gamma \vdash_{K^+} q$ 及 $\neg q$, 那么我们把 $q$ 和 $\neg q$ 从 $\Gamma$ 的两个证明中出现的所有新个体常元 $b_i$ 全部换成不在证明中出现的个体变元，便得到 $q$ 和 $\neg q$ 在 $K$ 中从 $\Gamma$ 的证明，这与 $\Gamma$ 的无矛盾性相矛盾.

$r_i$ 的个数大于 0 时，$\Gamma \cup \{r_0, \cdots, r_n\} \vdash_{K^+} q$ 及 $\neg q$ 是不能同时成立的. 如果同时成立，因 $r_n$ 是闭式 (注意 $r_n$ 的定义式)，用归谬律立即得

$$\Gamma \cup \{r_0, \cdots, r_{n-1}\} \vdash_{K^+} \neg r_n,$$

此即

$$\Gamma \cup \{r_0, \cdots, r_{n-1}\} \vdash_{K^+} \neg (p_n(b_{i_n}) \to \forall y_n\, p_n(y_n)).$$

由此可得 (用永真式 $\neg(p \to q) \to p$ 及 $\neg(p \to q) \to \neg q$)

$$\Gamma \cup \{r_0, \cdots, r_{n-1}\} \vdash_{K^+} p_n(b_{i_n}) \text{ 及 } \neg \forall y_n\, p_n(y_n).$$

把证明中出现的所有 $b_{i_n}$ 都换成不在证明中出现的个体变元 $x$, 并使用一次 Gen 规则 (注意 $b_{i_n}$ 的取法，它不在 $r_0, \cdots, r_{n-1}$ 中出现)，再注意 2.1.3 小节命题 7-1° 便得

$$\Gamma \cup \{r_0, \cdots, r_{n-1}\} \vdash_{K^+} \forall x\, p_n(x) \text{ 及 } \neg \forall x\, p_n(x),$$

按归纳假设，这是不可能的. 这就完成了 $\Gamma'$ 的无矛盾性的归纳证明.

**3. 作 $\Gamma'$ 的完备无矛盾扩张 $\Gamma^*$**

把 $K(Y^+)$ 中的所有闭式 (有可数个) 排成不重复的一列:

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

令

$$\Gamma_0 = \Gamma',$$

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

这样归纳定义的每个 $\Gamma_n$ 都是无矛盾的，且有

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

现对 $n$ 归纳证明 $\Gamma_n$ 是无矛盾的.

$n = 0$ 时，$\Gamma_0 = \Gamma'$，已知无矛盾 (见 2).

$n > 0$ 时，假设 $\Gamma_n$ 有矛盾，即有 $q$ 使

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

由归纳假设，$\Gamma_{n-1}$ 无矛盾. 这时有 $\Gamma_n \neq \Gamma_{n-1}$. 于是从 $\Gamma_n$ 的定义可知

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

且有

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

将 (3) 的 $\Gamma_n$ 代入 (1) 的左端，用反证律 (注意 $\neg p_{n-1}^*$ 是闭式) 便可得

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

这与 (2) 相矛盾. $\Gamma_n$ 的无矛盾性的归纳证明完成.

作

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

$\Gamma^*$ 也是无矛盾的，否则由 $\Gamma^* \vdash_{K^+} q$ 及 $\neg q$ 可推出对于充分大的 $n$, 有 $\Gamma_n \vdash_{K^+} q$ 及 $\neg q$, 这与 $\Gamma_n$ 的无矛盾性相矛盾.

$\Gamma^*$ 还是完备的，即对 $K^+$ 中任一闭式 $p_k^*$, $\Gamma^* \vdash_{K^+} p_k^*$ 与 $\Gamma^* \vdash_{K^+} \neg p_k^*$ 二者必居其一. 事实上，

$$\begin{aligned} \Gamma^* \nvdash_{K^+} p_k^* \Rightarrow\ & \Gamma_k \nvdash_{K^+} p_k^* && (\Gamma_k \subseteq \Gamma^*) \\ \Rightarrow\ & \Gamma_{k+1} = \Gamma_k \cup \{\neg p_k^*\} && (\text{由}\Gamma_n\text{的定义}) \\ \Rightarrow\ & \Gamma_{k+1} \vdash_{K^+} \neg p_k^* && (\neg p_k^* \in \Gamma_{k+1}) \\ \Rightarrow\ & \Gamma^* \vdash_{K^+} \neg p_k^*. && (\Gamma_{k+1} \subseteq \Gamma^*) \end{aligned}$$

至此便证明了 $\Gamma^*$ 是 $\Gamma'$ 的完备无矛盾扩张.

**4. 作 $K^+$ 的解释域 $M$**

令

$$M = \ K^+ \text{ 的所有闭项组成的集}.$$

$M$ 是从形式系统 $K^+$ 自身取出的非空集. 作为 $T^+$ 的子集，闭项集 $M$ 是由 $B \cup C$ 生成的以 $F$ 为运算集的代数系统，是可数集. 我们希望能把它构造成 $\Gamma$ 的模型.

首先让 $M$ 成为 $K^+$ 的解释域. 常元与运算符在 $M$ 中的解释是现成的: 令 $\overline{b_i} = b_i$, $\overline{c_i} = c_i$, $\overline{f_i^n} = f_i^n$, 即皆解释为自身. 再规定 $M$ 中与 $n$ 元谓词 $R_i^n$ 对应的 $n$ 元关系 $\overline{R_i^n}$ 如下:

对任意闭项 $t_1, \cdots, t_n \in M$,

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

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

$\Gamma^*$ 的完备无矛盾性保证了 $\overline{R_i^n}$ 的定义是合理的. 这样，$M$ 便成了 $K^+$ 的解释域. 忽略对所有新常元 $b_i$ 的解释，$M$ 也自然是 $K$ 的解释域. 下面要进一步证明 $M$ 是 $\Gamma$ 的模型.

注意 $M$ 的一个性质: 按上面的规定，对 $K^+$ 的任何项解释 $\varphi^+$ 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.

**5. 命题 ***

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

其中 $q$ 是 $K^+$ 的任一闭式.

现对闭式 $q$ 在 $K(Y^+)$ 中的层次数 $k$ 归纳证明命题 $*$.

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

$$\begin{aligned}
\Gamma^* \vdash_{K^+} q \Leftrightarrow\ & (t_1, \cdots, t_n) \in \overline{R_i^n} && (\overline{R_i^n}\text{的定义}) \\
\Leftrightarrow\ & (\varphi^+(t_1), \cdots, \varphi^+(t_n)) \in \overline{R_i^n} && (\varphi^+(t_i) = t_i) \\
\Leftrightarrow\ & |R_i^n(t_1, \cdots, t_n)|(\varphi^+) = 1.
\end{aligned}$$

因 $\varphi^+$ 是任取的，故

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

$k > 0$ 时，分以下四种情形讨论.

情形 1　$q = \neg r$, 其中 $r$ 也是闭式. 此时有

$$\begin{aligned}
\Gamma^* \vdash_{K^+} \neg r \ & \underset{(\Gamma^*\text{完备})}{\overset{(\Gamma^*\text{无矛盾})}{\overset{\Rightarrow}{\Leftarrow}}} \ \Gamma^* \nvdash_{K^+} r \\
& \Leftrightarrow |r|_M = 0 && (\text{由归纳假设}) \\
& \Leftrightarrow |\neg r|_M = 1.
\end{aligned}$$

情形 2　$q = r \to s$, 其中 $r, s$ 是闭式. 此时有

$$\begin{aligned}
\Gamma^* \nvdash_{K^+} r \to s \Leftrightarrow\ & \Gamma^* \vdash_{K^+} \neg(r \to s) && (\Gamma^*\text{的完备无矛盾性}) \\
\Leftrightarrow\ & \Gamma^* \vdash_{K^+} r \text{ 且 } \Gamma^* \vdash_{K^+} \neg s && (\text{用永真式}) \\
\Leftrightarrow\ & \Gamma^* \vdash_{K^+} r \text{ 但 } \Gamma^* \nvdash_{K^+} s && (\Gamma^*\text{完备、无矛盾}) \\
\Leftrightarrow\ & |r|_M = 1 \text{ 且 } |s|_M = 0 && (\text{由归纳假设}) \\
\Leftrightarrow\ & |r \to s|_M = 0.
\end{aligned}$$

上面第二步用了三个永真式:

$$\neg(r \to s) \to r,$$

$$\neg(r \to s) \to \neg s,$$

$$r \to (\neg s \to \neg(r \to s)).$$

情形 3 $q = \forall x r$ 且 $r$ 是闭式，此时有

$$\begin{aligned} \Gamma^* \vdash_{K^+} \forall x r \Leftrightarrow\ & \Gamma^* \vdash_{K^+} r && \text{((K4)，MP 及 Gen)} \\ \Leftrightarrow\ & |r|_M = 1 && \text{(归纳假设)} \\ \Leftrightarrow\ & |\forall x r|_M = 1. && \text{(2.2.3小节命题2)} \end{aligned}$$

情形 4 $q = \forall x r(x)$, 其中 $x$ 在 $r(x)$ 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 2 中列出的公式列里出现. 设 $r(x) = p_m(y_m)$, $y_m = x$. 于是 $q = \forall y_m\, p_m(y_m)$. 在此情形下，对命题 $*$ 的两个方向分别进行证明如下:

($\Rightarrow$) 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 $\varphi^+$ 使

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

把 $\varphi^+(y_m)$ 记为 $t$. 既然 $t \in M$, 那么 $t$ 是 $K^+$ 的闭项，所以又有

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

由此用 2.3 小节引理 1-2°($\varphi^+$ 是自己的 $y_m$ 变通) 进而得

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

因 $p_m(t)$ 是闭式，故由上式及 (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). 再由此及归纳假设得 $|p_m(t)|_M = 1$, 这与 (7) 相矛盾.

($\Leftarrow$) 设 $|\forall y_m\, p_m(y_m)|_M = 1$.

因为公理都是有效式，故有

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

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

注意 $r_m \in \Gamma^*$ (见 2，3 中 $\Gamma_n, \Gamma'$ 和 $\Gamma^*$ 的定义)，故 $\Gamma^* \vdash_{K^+} r_m$, 即

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

由此及 (8) 立即可得

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

至此完成了证明命题 $*$ 的归纳过程.

**6. 整个证明的完成**

任取 $p \in \Gamma \subseteq \Gamma^*$, 当然有 $\Gamma^* \vdash_{K^+} p$. 设 $p'$ 是 $p$ 的全称闭式，则也有 $\Gamma^* \vdash_{K^+} p'$. 这

时可用命题 * 得到 $|p'|_M = 1$. 由此及 2.2.3 小节命题 3 最后得

$$|p|_M = 1.$$

这就证明了 $M$ 是 $\Gamma$ 的模型，是所要找的可数集模型. □

有了定理 1，$K$ 的完全性定理立即可证.

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

**证** 反设 $\Gamma \nvdash p$. 设 $p'$ 是 $p$ 的全称闭式. 这时 $\Gamma \cup \{\neg p'\}$ 是无矛盾的，否则用反证律立即得 $\Gamma \vdash p'$, 以致 $\Gamma \vdash p$ 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，于是有 $|\neg p'|_M = 1$, 从而 $|p'|_M = 0$. 由此可知 $\Gamma \nvDash p'$. 最后又由 2.2.4 小节命题 4 得知 $\Gamma \nvDash p$, 这与已知条件相矛盾. □

把 $K$ 的可靠性和 $K$ 的完全性结合起来，我们就得到关于谓词演算 $K$ 的 Gödel 完备性定理:

$$\Gamma \vdash p \quad \Leftrightarrow \quad \Gamma \models p.$$

这个定理指出了 $K$ 的语法和语义的一致性.

在谓词演算 $K$ 中，有没有类似于命题演算 $L$ 的可判定性的结论? 是否存在一种算法，用它可以确定 $K$ 的任一公式是不是 $K$ 的定理即 $K$ 的有效式? 在谓词演算 $K$ 的范围内，莱布尼茨的通过计算解决争论的设想是否能够完全实现?

后面我们将要就一种特殊的谓词演算系统——形式算术 $K_{\mathrm{N}}$ 来回答问题.

## 练习 22

1. 设 $\Gamma$ 是 $K$ 的无矛盾公式集. 求证: $\Gamma$ 是完备的，当且仅当 $K$ 的任一闭式若在 $\Gamma$ 的某个模型中恒真，则在 $\Gamma$ 的所有模型中都恒真.

($\Gamma$ 是完备的，指: 对 $K$ 的任一闭式 $p$, $\Gamma \vdash p$ 与 $\Gamma \vdash \neg p$ 必有一个成立.)

2. (紧致性定理) 若 $\Gamma$ 的每个有限子集都有模型，则 $\Gamma$ 也定有模型.

# 3 形式算术与递归函数

## 3.1 带等词的谓词演算

现在来研究一类特殊的谓词演算，它们都有一个特殊的二元谓词 $R_1^2$，叫做等词. 各种形式数学系统 (包括形式算术 $K_{\mathrm{N}}$) 都是带等词的谓词演算.

等词在我们的心目中用来形式地表示“相等”这个通常的数学概念，但是对它也可以作其他解释.

**定义 1 (等词公理)** 在带有等词 $R_1^2$ 的谓词演算 $K$ 中，以下三种形式的公式叫做等词公理.

(E1) $R_1^2(t,t)$,

(E2) $R_1^2(t_k,u) \to R_1^2(f_i^n(t_1,\cdots,t_k,\cdots,t_n), f_i^n(t_1,\cdots,u,\cdots,t_n))$,

(E3) $R_1^2(t_k,u) \to (R_i^n(t_1,\cdots,t_k,\cdots,t_n) \to R_i^n(t_1,\cdots,u,\cdots,t_n))$,

其中 $t,t_1,\cdots,t_n,u$ 是任意的项，$k=1,\cdots,n$.

所有等词公理组成的集记为 $E$.

不涉及具体的解释域，这些等词公理的实际涵义是灵活的. 我们可以在自己任意设想的解释域中大致想象它们的直观意义: (E1) 涉及的是反身性质，(E2) 与 (E3) 涉及到替换性质.

为书写方便，下面用“$\approx$”表示等词，把 $R_1^2(t,u)$ 写成 $t \approx u$. 这样，可将等词公理更直观地写出:

(E1) $t \approx t$,

(E2) $t_k \approx u \to (f_i^n(t_1,\cdots,t_k,\cdots,t_n) \approx f_i^n(t_1,\cdots,u,\cdots,t_n))$,

(E3) $t_k \approx u \to (R_i^n(t_1,\cdots,t_k,\cdots,t_n) \to R_i^n(t_1,\cdots,u,\cdots,t_n))$.

注意，这些等词公理并不是有效式. 下面用简单的例子来说明这一点.

**例 1** 设 $K$ 中 $C=\varnothing, F=\varnothing, R=\{\approx\}$, 则等词公理集 $E$ 中只包含

(E1) $x \approx x$,

(E3) $x \approx y \to (x \approx z \to y \approx z)$,

$x \approx y \to (z \approx x \to z \approx y)$,

其中 $x, y, z$ 是任意变元. 此外没有其他形式的等词公理.

考察此 $K$ 的一个解释域 $\mathbf{N}$ (自然数集)，其中等词“$\approx$”解释为“$>$”. $\mathbf{N}$ 不是 $E$ 的模型. 事实上，对任意项解释 $\varphi$, 总有

$$|x \approx x|(\varphi) = 0;$$

当项解释 $\varphi$ 满足 $\varphi(x) = 3, \varphi(y) = 1, \varphi(z) = 2$ 时，

$$|x \approx y \to (x \approx z \to y \approx z)|(\varphi) = 0.$$

上例说明，等词公理并非在 $K$ 的任何解释域中都恒真. 但是当等词“$\approx$”在解释域中解释为“相等”时，该解释域一定是 $E$ 的模型.

**命题 1** 在 $K$ 的解释域 $M$ 中，若等词 $\approx$ 解释为相等，则 $M$ 是等词公理集 $E$ 的模型.

**证** 任取项解释 $\varphi \in \Phi_M$. 先考察 (E1). 因总有 $\varphi(t) = \varphi(t)$, 故总有

$$|t \approx t|(\varphi) = 1.$$

再考察 (E2) 和 (E3). 设 $|t_k \approx u|(\varphi) = 1$, 于是有 $\varphi(t_k) = \varphi(u)$. 此时两次用项解释 $\varphi$ 的保运算性 (见 2. 2. 1 小节中 (2) 式)，有

$$\begin{aligned}\varphi(f_i^n(t_1, \cdots, t_k, \cdots, t_n)) &= \overline{f_i^n}(\varphi(t_1), \cdots, \varphi(t_k), \cdots, \varphi(t_n)) \\ &= \overline{f_i^n}(\varphi(t_1), \cdots, \varphi(u), \cdots, \varphi(t_n)) \\ &= \varphi(f_i^n(t_1, \cdots, u, \cdots, t_n)).\end{aligned}$$

于是

$$|f_i^n(t_1, \cdots, t_k, \cdots, t_n) \approx f_i^n(t_1, \cdots, u, \cdots, t_n)|(\varphi) = 1.$$

这说明

$$|t_k \approx u \ \to \ (f_i^n(t_1, \cdots, t_k, \cdots, t_n) \approx f_i^n(t_1, \cdots, u, \cdots, t_n))|(\varphi) = 1.$$

此时还有

$$\begin{aligned}|R_i^n(t_1, \cdots, t_k, \cdots, t_n)|(\varphi) = 1 &\Rightarrow \ (\varphi(t_1), \cdots, \varphi(t_k), \cdots, \varphi(t_n)) \in \overline{R_i^n} \\ &\Rightarrow \ (\varphi(t_1), \cdots, \varphi(u), \cdots, \varphi(t_n)) \in \overline{R_i^n} \\ &\Rightarrow \ |R_i^n(t_1, \cdots, u, \cdots, t_n)|(\varphi) = 1,\end{aligned}$$

这说明

$$|t_k \approx u \ \to \ (R_i^n(t_1, \cdots, t_k, \cdots, t_n) \ \to \ R_i^n(t_1, \cdots, u, \cdots, t_n))|(\varphi) = 1.$$

$\varphi$ 是任意的，故以上讨论表明所有等词公理在 $M$ 中恒真. □

对于任何带等词的谓词演算，总可以给出一个解释域，使等词在其中解释为相等. 换句话说，(根据命题 1) 等词公理集 $E$ 总可以找到自己的模型. 再根据 2.3 节推

论 2，我们便知道等词公理集 $E$ 是无矛盾的.

命题 1 还说明，等词公理形式地表示出“相等”所必须具有的“反身性”和“可替换性”. 但是，等词公理并没有形式地表示出“相等”的全部特征. 这是因为，命题 1 的逆命题并不成立: 等词 $\approx$ 不解释为“相等”的解释域，也可能是等词公理集 $E$ 的模型. 了解这一点，只用看下面的例子.

**例 2** 仍用例 1 中的 $K$, 其中 $C=\varnothing, F=\varnothing, R=\{\approx\}$. 现考察 $K$ 的另一解释域 $\mathbf{Z}$ (全体整数集). 设在 $\mathbf{Z}$ 中等词 $\approx$ 不解释为相等，而是解释为“有相同奇偶性”. 这时所有等词公理在 $\mathbf{Z}$ 中恒真. 事实上，任取 $\varphi \in \Phi_{\mathbf{Z}}$, 便有

$1^\circ\ |x \approx x|(\varphi)=1$,

$2^\circ\ |x \approx y \to (x \approx z \to y \approx z)|(\varphi)=1$,

$3^\circ\ |x \approx y \to (z \approx x \to z \approx y)|(\varphi)=1$.

式 $1^\circ$ 成立，是因为 $\varphi(x)$ 与 $\varphi(x)$ 自己有相同的奇偶性. 式 $2^\circ$ 的意思是: 若 $\varphi(x)$ 与 $\varphi(y)$ 有相同奇偶性且 $\varphi(x)$ 与 $\varphi(z)$ 有相同的奇偶性，则 $\varphi(y)$ 与 $\varphi(z)$ 也有相同奇偶性. 式 $3^\circ$ 与式 $2^\circ$ 同理.

例 2 说明，不能强迫等词 $\approx$ 在等词公理集 $E$ 的模型中非解释为“相等”不可. 但是下面证明，在 $E$ 的任何模型中等词 $\approx$ 所解释的二元关系必定是等价关系.

**命题 2** $1^\circ\ E \vdash t \approx t$,

$2^\circ\ E \vdash t \approx u \to u \approx t$,

$3^\circ\ E \vdash t \approx u \to (u \approx v \to t \approx v)$.

以上 $t, u$ 和 $v$ 是任意的项.

**证** $1^\circ$ $t \approx t$ 是等词公理.

$2^\circ$ 先证 $E \cup \{t \approx u\} \vdash u \approx t$, 再用演绎定理. 以下是所需证明:

| | |
|---|---|
| (1) $t \approx u \to (t \approx t \to u \approx t)$ | (E3) |
| (2) $t \approx u$ | 假定 |
| (3) $t \approx t \to u \approx t$ | (1), (2), MP |
| (4) $t \approx t$ | (E1) |
| (5) $u \approx t$ | (3), (4), MP |

$3^\circ$ 以下是所需证明:

| | |
|---|---|
| (1) $t \approx u \to u \approx t$ | 由 $2^\circ$ |
| (2) $u \approx t \to (u \approx v \to t \approx v)$ | (E3) |
| (3) $t \approx u \to (u \approx v \to t \approx v)$ | (1), (2), HS |

□

**命题 3** 若 $M$ 是 $E$ 的模型，则等词 $\approx$ 必解释为 $M$ 上的等价关系.

**证** 由命题 2 利用可靠性定理得

$$|x_1 \approx x_1|_M = 1,$$

$$|x_1 \approx x_2 \to x_2 \approx x_1|_M = 1,$$

$$|x_1 \approx x_2 \to (x_2 \approx x_3 \to x_1 \approx x_3)|_M = 1.$$

任取 $\varphi \in \Phi_M$. 设 $\approx$ 解释为 $M$ 上的二元关系 $\overline{R_1^2}$, 上面三式分别立即给出:

1° $(\varphi(x_1), \varphi(x_1)) \in \overline{R_1^2}$, (反身性)

2° $(\varphi(x_1), \varphi(x_2)) \in \overline{R_1^2} \ \Rightarrow\ (\varphi(x_2), \varphi(x_1)) \in \overline{R_1^2}$, (对称性)

3° $(\varphi(x_1), \varphi(x_2)) \in \overline{R_1^2}$ 且 $(\varphi(x_2), \varphi(x_3)) \in \overline{R_1^2}$

$\Rightarrow\ (\varphi(x_1), \varphi(x_3)) \in \overline{R_1^2}$. (可递性)

因 $\varphi$ 是任取的，故 $\varphi(x_1), \varphi(x_2), \varphi(x_3)$ 是 $M$ 的任意元素. 于是 1°, 2°, 3° 说明 $\overline{R_1^2}$ 是 $M$ 上的等价关系. □

下面两个等项替换的命题是以后常用的.

**命题 4** (**等项替换，(E2)的推广**)

$$E \vdash u \approx v \to t(u) \approx t(v),$$

其中项 $u$ 是项 $t(u)$ 的子项，$t(v)$ 是将 $t(u)$ 中某一处出现的 $u$ 替换成项 $v$ 所得结果.

**证** 设 $t(u)$ 是由待替换的 $u$ 经 $m$ 次运算得来. 现对 $m$ 归纳.

$m = 0$ 时，$t(u)$ 就是 $u$, $t(v)$ 就是 $v$, 用同一律便可.

$m > 0$ 时，设 $t(u)$ 是 $f_i^n(t_1, \cdots, t_k(u), \cdots, t_n)$, 其中 $t_k(u)$ 是由待替换的 $u$ 经过少于 $m$ 次的运算得来. 此时 $t(v)$ 是 $f_i^n(t_1, \cdots, t_k(v), \cdots, t_n)$. 我们有:

(1) $u \approx v \to t_k(u) \approx t_k(v)$ 归纳假设

(2) $t_k(u) \approx t_k(v) \to f_i^n(t_1, \cdots, t_k(u), \cdots, t_n) \approx f_i^n(t_1, \cdots, t_k(v), \cdots, t_n)$

即 $t_k(u) \approx t_k(v) \to t(u) \approx t(v)$ (E2)

(3) $u \approx v \to t(u) \approx t(v)$ (1), (2), HS

□

**命题 5** (**等项替换，(E3) 的推广**)

$$E \vdash t \approx u \to (p(t) \to p(u)),$$

其中 $p(u)$ 是将公式 $p(t)$ 中某一处出现的项 $t$ 用项 $u$ 替换后所得结果，且 $t$ 和 $u$ 的变元都不在替换处受约束.

**证** 对公式 $p(t)$ 的层次数归纳.

当 $p(t)$ 是原子公式 $R_i^n(t_1, \cdots, t_k(t), \cdots, t_n)$ 时，$p(u)$ 是

$$R_i^n(t_1, \cdots, t_k(u), \cdots, t_n).$$

此时有:

(1) $t \approx u \to t_k(t) \approx t_k(u)$ 命题 4

(2) $t_k(t) \approx t_k(u) \to (R_i^n(t_1, \cdots, t_k(t), \cdots, t_n) \to R_i^n(t_1, \cdots, t_k(u), \cdots, t_n))$ (E3)

(3) $t \approx u \to (p(t) \to p(u))$ (1)，(2)，HS

$p(t)$ 不是原子公式时，有以下三种可能:

(i) $p(t) = \neg q(t), p(u) = \neg q(u)$. 此时有:

(1) $t \approx u \to u \approx t$ 命题 2-2°

(2) $u \approx t \to (q(u) \to q(t))$ 归纳假设

(3) $(q(u) \to q(t)) \to (\neg q(t) \to \neg q(u))$ 永真式

(4) $t \approx u \to (\neg q(t) \to \neg q(u))$ 两次 HS

(ii) $p(t) = q(t) \to r$ 或 $p(t) = q \to r(t)$.

对前者，以下公式从 $E$ 可证:

(1) $t \approx u \to u \approx t$ 命题 2-2°

(2) $u \approx t \to (q(u) \to q(t))$ 归纳假设

(3) $(q(u) \to q(t)) \to ((q(t) \to r) \to (q(u) \to r))$ 永真式

(4) $t \approx u \to ((q(t) \to r) \to (q(u) \to r))$ 两次 HS

对后者 (即 $p(t) = q \to r(t)$), 以下公式从 $E$ 可证:

(1) $t \approx u \to (r(t) \to r(u))$ 归纳假设

(2) $(r(t) \to r(u)) \to ((q \to r(t)) \to (q \to r(u)))$ 永真式

(3) $t \approx u \to ((q \to r(t)) \to (q \to r(u)))$ (1)，(2)，HS

(iii) $p(t) = \forall x q(t)$, $p(u) = \forall x q(u)$. 由已知条件 ($t$ 和 $u$ 的变元都不在替换处受约束) 知，$t$ 和 $u$ 中都不含有 $x$. 此时以下公式从

$$E \cup \{t \approx u, \forall x q(t)\}$$

可证:

(1) $t \approx u$ 假定

(2) $t \approx u \to (q(t) \to q(u))$ 归纳假设

(3) $q(t) \to q(u)$ (1)，(2)，MP

(4) $\forall x q(t) \to q(t)$ (K4)

(5) $\forall x q(t)$ 假定

(6) $q(u)$ (5)，(4)，(3)，MP

(7) $\forall x q(u)$ (6)，Gen

因 Gen 变元 $x$ 不在假定 $t \approx u$ 及 $\forall x q(t)$ 中自由出现，两次用演绎定理便得

$$E \vdash t \approx u \to (\forall x q(t) \to \forall x q(u)).$$

□

### 练习 23

1. 设 $K$ 中 $F=\{f_1^1,f_1^2,f_2^2\}, R=\{\approx\}$, 试写出 (E2), (E3) 型等词公理的各种形式.

2. 在例 1 的 $K$ 的解释域 **N** 中，若等词 $\approx$ 改为解释成“有不同的奇偶性”，那么等词公理在 **N** 中是否都恒真? 是否都恒假?

3. 设项 $t,u$ 都对公式 $p(x)$ 中 $x$ 自由，且不含 $x$. 求证

$$E\cup\{\exists!\,x\,p(x),p(t)\}\vdash\ p(u)\to u\approx t,$$

这里规定

$$\exists!\,x\,p(x)=\exists\,x(p(x)\wedge\forall\,y(p(y)\to x\approx y)),$$

其中 $y$ 不在 $p(x)$ 中出现.

## 3.2 形式算术$K_{\mathbf{N}}$

形式算术 $K_{\mathbf{N}}$ 指的是一种特殊的带等词的谓词演算，它有一个个体常元 $c_1$, 有三个函数词—— $f_1^1,f_1^2,f_2^2$, 有一个二元谓词 $\approx$.

$K_{\mathbf{N}}$ 有一个自然的解释域——自然数集 $\mathbf{N}=\{0,1,2,\cdots\}$. 在 **N** 中 $c_1$ 解释为 0; $f_1^1$, $f_1^2,f_2^2$ 分别解释为一元后继函数，二元求和函数，二元乘积函数；等词 $\approx$ 解释为 **N** 中的相等 ($=$). 当然，除了上面这个解释域，$K_{\mathbf{N}}$ 还可以有其他的解释域.

由于 **N** 是我们心目中意想的解释域，往后我们把个体常元 $c_1$ 写成 $\bar{0}$, 而把 $f_1^1$, $f_1^2$ 和 $f_2^2$ 符号上等同于各自意想的解释，即把 $f_1^1(t),f_1^2(t_1,t_2)$ 和 $f_2^2(t_1,t_2)$ 分别写成 $t',t_1+t_2,t_1\times t_2$. (注意这里 $\bar{0}$ 是个体常元符，它在 **N** 中解释为 0，这与 2.2 节中的符号用法不同.)

在 $K_{\mathbf{N}}$ 的解释域 **N** 中，因常元 $\bar{0}$ 解释为 0，故项 $\bar{0}'$ 解释为 $0'$ (即 1)，$\bar{0}''$ 解释为 $0''$ (即 2)，……

往后把闭项 $\bar{0}',\bar{0}'',\bar{0}''',\cdots$ 分别写作 $\bar{1},\bar{2},\bar{3},\cdots$. 我们把这些形为 $\bar{n}$ 的闭项叫做 $K_{\mathbf{N}}$ 的数字.

在 **N** 中，$\bar{n}$ 解释为 $n$. 事实上，对任意项解释 $\varphi\in\Phi_{\mathbf{N}}$, 总有

$$\begin{aligned}\varphi(\bar{n})&=\varphi(\bar{0}''\cdots'\ ^{(n\text{个}')})\\&=\varphi(\bar{0})''\cdots' &&(\text{项解释}\varphi\text{的保运算性})\\&=0''\cdots' &&(\text{项解释}\varphi\text{使}\varphi(\bar{0})=0)\\&=n.\end{aligned}$$

**定义 1 (算术公理，Peano 形式算术)** $K_{\mathbf{N}}$ 中所有的等词公理和所有以下形式的

公式都叫做算术公理.

(N1) $t' \not\approx \overline{0}$ (即 $\neg(t' \approx \overline{0})$),

(N2) $t_1' \approx t_2' \to t_1 \approx t_2$,

(N3) $t + \overline{0} \approx t$,

(N4) $t_1 + t_2' \approx (t_1 + t_2)'$,

(N5) $t \times \overline{0} \approx \overline{0}$,

(N6) $t_1 \times t_2' \approx t_1 \times t_2 + t_1$,

(N7) $p(\overline{0}) \to (\forall x(p(x) \to p(x')) \to \forall x p(x))$,

其中 $t, t_1, t_2$ 是任意的项，$p(x)$ 是任意的公式.

算术公理的集记作 $\mathcal{N}$. 带有算术公理集 $\mathcal{N}$ 的 $K_{\mathrm{N}}$ 叫做 Peano 形式算术.

直观上看，$\mathcal{N}$ 中所有上述公理在意想的解释域 **N** 中都显然恒真. 研究形式算术的语法问题，常直接假定 $\mathcal{N}$ 是无矛盾公式集，而暂避模型 **N** 的存在.

除了以上七种模式外，注意 $\mathcal{N}$ 也把等词公理包括在内. 等词公理在这里也视为算术公理. 除了算术公理，$K_{\mathrm{N}}$ 的公理还包括原有的谓词演算公理 (K1)~(K5).

在 (N1)~(N7) 这七种公理模式中，(N1) 和 (N2) 相应于 Peano 公理 3 和公理 4 (见 0. 2 节)，(N3) 与 (N4) 相应于 Peano 算术中加法的归纳定义式，(N5) 与 (N6) 相应于乘法的归纳定义式，(N7) 就是形式归纳原理.

我们为算术理论建立了形式系统 $K_{\mathrm{N}}$——Peano 形式算术. 往下想做的重要事情是: 考察 $K_{\mathrm{N}}$ 这一系统究竟有多强的形式演绎能力. 为此需要做大量的细致工作.

若 $\mathcal{N} \vdash p$, 则把 $p$ 叫做 Peano 形式算术的 (形式) 定理.

下面建立一些后面将要用到的 (形式) 定理. 我们从 $\overline{1} + \overline{1} \approx \overline{2}, \overline{1} + \overline{2} \approx \overline{3}$ 开始.

**命题 1**　$\mathcal{N} \vdash \overline{m} + \overline{n} \approx \overline{m+n}$.

**证**　对 $n$ 归纳.

$n = 0$ 时，$\overline{m} + \overline{0} \approx \overline{m}$ 是 (N3) 型公理.

$n > 0$ 时，以下公式从 $\mathcal{N}$ 可证:

(1) $\overline{m} + \overline{n-1}' \approx (\overline{m} + \overline{n-1})'$　(N4)

(2) $\overline{m} + \overline{n-1} \approx \overline{m+n-1}$　归纳假设

(3) $\overline{m} + \overline{n-1} \approx \overline{m+n-1} \to (\overline{m} + \overline{n-1})' \approx \overline{m+n-1}'$　(E2)

(4) $(\overline{m} + \overline{n-1})' \approx \overline{m+n-1}'$　(2)，(3)，MP

(5) $\overline{m} + \overline{n-1}' \approx \overline{m+n-1}'$　(1)，(4)，等词性质

此即 $\overline{m} + \overline{n} \approx \overline{m+n}$.　□

作为特例，有 $\mathcal{N} \vdash \overline{1} + \overline{1} \approx \overline{2}$.

命题 1 的证明用的是通常关于自然数命题的归纳法，而不是用 (N7).

**命题 2**　$\mathcal{N} \vdash \overline{m} \times \overline{n} \approx \overline{m \times n}$.

**证**　对 $n$ 归纳.

$n=0$ 时，$\overline{m}\times\overline{0}\approx\overline{0}$ 是 (N5) 型公理.

$n>0$ 时，以下公式从 $\mathcal{N}$ 可证:

(1) $\overline{m}\times\overline{n-1}'\approx\overline{m}\times\overline{n-1}+\overline{m}$ 　(N6)

(2) $\overline{m}\times\overline{n-1}\approx\overline{m\times(n-1)}$ 　归纳假设

(3) $\overline{m}\times\overline{n-1}'\approx\overline{m\times(n-1)}+\overline{m}$ 　(1)，(2)，等项替换

(4) $\overline{m}\times\overline{n-1}'\approx\overline{m\times(n-1)+m}$ 　(3)，命题 1

此即 $\overline{m}\times\overline{n}\approx\overline{m\times n}$. □

**命题 3** $\mathcal{N}\vdash\ \overline{0}+t\ \approx\ t$, 其中 $t$ 为任意项. (注意与 (N3) 的区别. )

**证** 下面是从 $\mathcal{N}$ 的证明:

(1) $\overline{0}+\overline{0}\approx\overline{0}$ 　(N3)

(2) $(\overline{0}+x)'\approx\overline{0}+x'$ 　(N4)

(3) $\overline{0}+x\approx x\ \to\ (\overline{0}+x)'\approx x'$ 　(E2)

(4) $\overline{0}+x\approx x\ \to\ \overline{0}+x'\approx x'$ 　(2)，(3)，等项替换

(5) $\forall x(\overline{0}+x\approx x\ \to\ \overline{0}+x'\approx x')$ 　(4)，Gen

(6) $\forall x(\overline{0}+x\approx x)$ 　(1)，(5)，(N7)，MP

(7) $\overline{0}+t\approx t$ 　(6)，(K4)，MP

□

上面的 (6) 在使用 (N7) 时，是以 $\overline{0}+x\approx x$ 作为 $p(x)$ 的.

命题 3 的证明中使用了一次 Gen 规则. 选择哪一个个体变元 $x$ 作为 Gen 变元，与我们所作的证明没有关系. 由于这里使用的 Gen 变元 $x$ 可以任意地选择，而可供选择的个体变元足够多 (有可数个)，所以每当后面要用到命题 3 时，都可以不必考虑所使用的 Gen 可能会产生什么样的变元干扰，因为干扰总是可以用另选 Gen 变元的方式避开的. 后面还会碰到类似的情况，但不再重复这一说明.

**命题 4** $\mathcal{N}\vdash\ t_1'+t_2\ \approx\ (t_1+t_2)'$, 其中 $t_1,t_2$ 是任意的项. (注意与 (N4) 的区别. )

**证** 下面是从 $\mathcal{N}$ 的证明:

(1) $t_1'+\overline{0}\approx t_1'$ 　(N3)

(2) $(t_1+\overline{0})'\approx t_1'$ 　(N3)，(E2)

(3) $t_1'+\overline{0}\approx(t_1+\overline{0})'$ 　由 (1)，(2)

(4) $t_1'+x\approx(t_1+x)'\ \to\ (t_1'+x)'\approx(t_1+x)''$ 　(E2)

(5) $(t_1'+x)'\approx t_1'+x'$ 　(N4)

(6) $(t_1+x)''\approx(t_1+x')'$ 　(N4)，(E2)

(7) $\forall x(t_1'+x\approx(t_1+x)'\ \to\ t_1'+x'\approx(t_1+x')')$ 　由 (4)，(5)，(6)，Gen

(8) $\forall x(t_1'+x\approx(t_1+x)')$ 　(7)，(3)，(N7)，MP

(9) $t_1'+t_2\approx(t_1+t_2)'$ 　(8)，(K4)，MP

□

**命题 5** **(加法交换律)**

$$\mathcal{N} \vdash t_1 + t_2 \approx t_2 + t_1,$$

其中 $t_1, t_2$ 是任意的项.

**证** 下面是从 $\mathcal{N}$ 的证明:

| | |
|---|---|
| (1) $\bar{0} + t_2 \approx t_2$ | 命题 3 |
| (2) $t_2 + \bar{0} \approx t_2$ | (N3) |
| (3) $\bar{0} + t_2 \approx t_2 + \bar{0}$ | 由 (1), (2) |
| (4) $x + t_2 \approx t_2 + x \ \rightarrow\ (x + t_2)' \approx (t_2 + x)'$ | (E2) |
| (5) $(x + t_2)' \approx x' + t_2$ | 由命题 4 |
| (6) $(t_2 + x)' \approx t_2 + x'$ | (N4) |
| (7) $\forall x(x + t_2 \approx t_2 + x \ \rightarrow\ x' + t_2 \approx t_2 + x')$ | 由 (4), (5), (6), Gen |
| (8) $\forall x(x + t_2 \approx t_2 + x)$ | (7), (3), (N7), MP |
| (9) $t_1 + t_2 \approx t_2 + t_1$ | (8), (K4), MP |

□

**命题 6** **(加法结合律)**

$$\mathcal{N} \vdash (t_1 + t_2) + t_3 \approx t_1 + (t_2 + t_3),$$

其中 $t_1, t_2, t_3$ 是任意的项.

**证** 下面是从 $\mathcal{N}$ 的证明:

| | |
|---|---|
| (1) $(t_1 + t_2) + \bar{0} \approx t_1 + t_2$ | (N3) |
| (2) $t_1 + (t_2 + \bar{0}) \approx t_1 + t_2$ | (N3), (E2) |
| (3) $(t_1 + t_2) + \bar{0} \approx t_1 + (t_2 + \bar{0})$ | 由 (1), (2) |
| (4) $(t_1 + t_2) + x \approx t_1 + (t_2 + x) \ \rightarrow\ ((t_1 + t_2) + x)' \approx (t_1 + (t_2 + x))'$ | (E2) |
| (5) $((t_1 + t_2) + x)' \approx (t_1 + t_2) + x'$ | (N4) |
| (6) $(t_1 + (t_2 + x))' \approx t_1 + (t_2 + x')$ | 两次 (N4) |
| (7) $\forall x((t_1 + t_2) + x \approx t_1 + (t_2 + x) \ \rightarrow\ (t_1 + t_2) + x' \approx t_1 + (t_2 + x'))$ | 由 (4), (5), (6), Gen |
| (8) $\forall x((t_1 + t_2) + x \approx t_1 + (t_2 + x))$ | (3), (7), (N7) |
| (9) $(t_1 + t_2) + t_3 \approx t_1 + (t_2 + t_3)$ | (8), (K4), MP |

□

**命题 7** **(加法消去律)**

$$\mathcal{N} \vdash t_1 + t_2 \approx t_2 \rightarrow t_1 \approx \bar{0},$$

其中 $t_1, t_2$ 是任意的项.

**证** 下面是从 $\mathcal{N}$ 的证明:

(1) $t_1+\overline{0}\approx t_1$ (N3)

(2) $t_1+\overline{0}\approx\overline{0}\ \to\ t_1\approx\overline{0}$ 由 (1) 及 (E3)

(3) $t_1+x'\approx x'\ \to\ (t_1+x)'\approx x'$ (N4)，(E3)

(4) $(t_1+x)'\approx x'\ \to\ t_1+x\approx x$ (N2)

(5) $t_1+x'\approx x'\ \to\ t_1+x\approx x$ (3)，(4)，HS

(6) $\forall x((t_1+x\approx x\ \to\ t_1\approx\overline{0})\ \to\ (t_1+x'\approx x'\ \to\ t_1\approx\overline{0}))$

由 (5)，永真式 $(p\to q)\to((q\to r)\to(p\to r))$,MP，Gen

(7) $\forall x(t_1+x\approx x\ \to\ t_1\approx\overline{0})$ (2)，(6)，(N7)

(8) $t_1+t_2\approx t_2\ \to\ t_1\approx\overline{0}$ (7)，(K4)，MP

□

**命题 8**

$$\mathcal{N}\vdash\ t_1+t_2\approx\overline{0}\ \to\ t_1\approx\overline{0},$$

其中 $t_1,t_2$ 是任意的项.

**证** 下面是从 $\mathcal{N}$ 的证明:

(1) $t_1+\overline{0}\approx\overline{0}\ \to\ t_1\approx\overline{0}$ 由命题 7

(2) $(t_1+x)'\not\approx\overline{0}$ (N1)

(3) $t_1+x'\not\approx\overline{0}$ 由 (2)，(N4)

(4) $t_1+x'\approx\overline{0}\ \to\ t_1\approx\overline{0}$ 由 (3) 及永真式 $\neg q\to(q\to p)$

(5) $\forall x((t_1+x\approx\overline{0}\to t_1\approx\overline{0})\ \to\ (t_1+x'\approx\overline{0}\ \to\ t_1\approx\overline{0}))$

由 (4)，永真式 $p\to(q\to p)$ 及 Gen

(6) $\forall x(t_1+x\approx\overline{0}\to t_1\approx\overline{0})$ (1)，(5)，(N7)

(7) $t_1+t_2\approx\overline{0}\ \to\ t_1\approx\overline{0}$ (6)，(K4)，MP

□

**命题 9**

$$\mathcal{N}\vdash\ t_3+t_1\approx t_2\ \to\ (t_4+t_2\approx t_1\ \to\ t_1\approx t_2),$$

其中 $t_1,t_2,t_3,t_4$ 是任意的项.

**证** 以下是 $t_1\approx t_2$ 从

$$\mathcal{N}\cup\{t_3+t_1\approx t_2,t_4+t_2\approx t_1\}$$

的证明:

(1) $t_3+t_1\approx t_2$ 假定

(2) $t_4+t_2\approx t_1$ 假定

(3) $t_3+(t_4+t_2)\approx t_2$ (1)，(2)，等项替换

(4) $(t_3+t_4)+t_2\approx t_2$ (3)，结合律

(5) $t_3 + t_4 \approx \overline{0}$ (4)，消去律

(6) $t_3 \approx \overline{0}$ (5)，命题 8

(7) $t_1 \approx t_2$ 由 (1)，(6)

再用演绎定理便可. □

**命题 10**

$$\mathcal{N} \vdash \exists x(x+t_1 \approx t_2) \to (\exists x(x+t_2 \approx t_1) \to t_1 \approx t_2),$$

其中项 $t_1, t_2$ 皆不含 $x$.

**证** 在命题 9 中取 $t_3$ 为 $x$, 取 $t_4$ 为 $y(\neq x)$, 且 $y$ 也不含于 $t_1, t_2$, 则立即有

$$\mathcal{N} \cup \{x+t_1 \approx t_2, y+t_2 \approx t_1\} \vdash t_1 \approx t_2,$$

由此两次用 $\exists_2$ 规则 (见 2. 1. 3 小节命题 4)，再用 2. 1. 3 小节命题 7-2° 及演绎定理便得结果. □

往后，公式 $\exists x(x+t_1 \approx t_2)$ (其中 $t_1, t_2$ 不含有 $x$) 常简写为 $t_1 \leqslant t_2$, 于是命题 10 可写成

$$\mathcal{N} \vdash t_1 \leqslant t_2 \to (t_2 \leqslant t_1 \to t_1 \approx t_2).$$

**命题 11** $\mathcal{N} \vdash t \not\approx \overline{0} \to \overline{1} \leqslant t$.

**证** 下面是从 $\mathcal{N}$ 的证明:

(1) $\overline{0} \approx \overline{0}$ (E1)

(2) $\overline{0} \not\approx \overline{0} \to \exists y(y+\overline{1} \approx \overline{0})$ 由 (1) 及永真式 $q \to (\neg q \to p)$

(3) $(x+\overline{0})' \approx x'$ (N3)，(E2)

(4) $(x+\overline{0})' \approx x+\overline{1}$ (N4)

(5) $x+\overline{1} \approx x'$ (3)，(4)

(6) $x+\overline{1} \approx x' \to \exists y(y+\overline{1} \approx x')$ $\exists_1$ 规则 (下面有说明)

(7) $\exists y(y+\overline{1} \approx x')$ (5)，(6)，MP

(8) $x' \not\approx \overline{0} \to \exists y(y+\overline{1} \approx x')$ 由 (7)，公理 $p \to (q \to p)$ 及 MP

(9) $(x \not\approx \overline{0} \to \exists y(y+\overline{1} \approx x)) \to (x' \not\approx \overline{0} \to \exists y(y+\overline{1} \approx x'))$

由 (8) 及公理 $p \to (q \to p)$

(10) $\forall x(x \not\approx \overline{0} \to \exists y(y+\overline{1} \approx x))$ (2)，(9)，Gen，(N7)

(11) $t \not\approx \overline{0} \to \exists y(y+\overline{1} \approx t)$ (10)，(K4)

此即 $t \not\approx \overline{0} \to \overline{1} \leqslant t$. 上面证明中所用的 $x, y$ 选择为不在 $t$ 中出现的变元，且 $x \neq y$. □

**说明** 步骤 (6) 使用了一次 $\exists_1$ 规则 (见 2. 1. 3 小节命题 2):

$$\vdash p(t) \to \exists y\, p(y),$$

这里取 $p(y)$ 为 $y+\overline{1}\approx x'$, 取 $t$ 为 $x$, $t$ (即 $x$) 对 $p(y)$ 中的 $y$ 自由，用 $t$ 代换 $p(y)$ 中的 $y$ 得到的 $p(t)$ 是 $x+\overline{1}\approx x'$.

**命题 12 (命题 11 的推广)** $n>0$ 时，有

$$\mathcal{N}\vdash\ (t\not\approx\overline{0}\wedge\cdots\wedge t\not\approx\overline{n-1})\ \to\ \overline{n}\leqslant t.$$

**证** 对 $n$ 归纳.

$n=1$ 时，即命题 11.

现假设结论对 $n$ 成立，要证对 $n+1$ 也成立:

$$\mathcal{N}\vdash\ (t\not\approx\overline{0}\wedge\cdots\wedge t\not\approx\overline{n})\ \to\ \overline{n+1}\leqslant t.$$

为此先证明下面的命题 $*$.

$$(*)\quad \mathcal{N}\cup\{t\not\approx\overline{1}\wedge\cdots\wedge t\not\approx\overline{n}, y+\overline{1}\approx t\}\vdash\exists x(x+\overline{n+1}\approx t),$$

其中 $y,x$ 不在 $t$ 中出现，且 $y\neq x$.

以下是命题 $*$ 所需要的证明:

| | |
|---|---|
| (1) $(y+\overline{0})'\approx y'$ | (N3)，(E2) |
| (2) $y+\overline{1}\approx y'$ | 由 (1)，(N4) |
| (3) $y+\overline{1}\approx t$ | 假定 |
| (4) $y'\approx t$ | 由 (2)，(3) |
| (5) $y'\not\approx\overline{1}\wedge\cdots\wedge y'\not\approx\overline{n}$ | 由 (4) 及假定 |
| (6) $y'\not\approx\overline{i'}$, $i=0,\cdots,n-1$ | 由 (5) |
| (7) $y\approx\overline{i}\ \to\ y'\approx\overline{i'}$, $i=0,\cdots,n-1$ | (E2) |
| (8) $y\not\approx\overline{i}$, $i=0,\cdots,n-1$ | (6)，(7)，$(p\to q)\to(\neg q\to\neg p)$ |
| (9) $y\not\approx\overline{0}\wedge\cdots\wedge y\not\approx\overline{n-1}$ | 由 (8) |
| (10) $\overline{n}\leqslant y$ 即 $\exists x(x+\overline{n}\approx y)$ | (9)，归纳假设 |
| (11) $x+\overline{n}\approx y\to(x+\overline{n})'\approx y'$ | (E2) |
| (12) $\forall x(x+\overline{n}\approx y\ \to\ x+\overline{n+1}\approx y')$ | (11)，(N4)，Gen |
| (13) $\exists x(x+\overline{n+1}\approx y')$ | (12)，(10)，2.1.3 小节命题 3 |
| (14) $\exists x(x+\overline{n+1}\approx t)$ | (4)，(13)，(E3) |

这就证明了命题 $*$. 由命题 $*$ 用 $\exists_2$ 规则得

$$\mathcal{N}\cup\{t\not\approx\overline{1}\wedge\ldots\wedge t\not\approx\overline{n}, \exists y(y+\overline{1}\approx t)\}\vdash\exists x(x+\overline{n+1}\approx t);$$

由命题 11，又有

$$\mathcal{N}\cup\{t\not\approx\overline{0}\}\vdash\exists y(y+\overline{1}\approx t).$$

二者结合，便得

$$\mathcal{N}\cup\{t\not\approx\overline{0}\wedge t\not\approx\overline{1}\wedge\cdots\wedge t\not\approx\overline{n}\}\vdash\exists x(x+\overline{n+1}\approx t).$$

归纳过程完成. □

**命题 13** $\mathcal{N} \vdash (t \not\approx \overline{0} \wedge \cdots \wedge t \not\approx \overline{n}) \rightarrow t \nleqslant \overline{n}$.

**证** 以下公式从 $\mathcal{N} \cup \{t \not\approx \overline{0} \wedge \cdots \wedge t \not\approx \overline{n}, x + t \approx \overline{n}\}$ 可证:

(1) $(x+t)' \approx \overline{n'}$ 由假定，(E2)

(2) $x' + t \approx \overline{n+1}$ (1)，命题 4

(3) $\exists y(y + t \approx \overline{n+1})$ (2), $\exists_1$ 规则

(4) $\exists z(z + \overline{n+1} \approx t)$ (即 $\overline{n+1} \leqslant t$) 由假定及命题 12

(5) $t \approx \overline{n+1}$ (3)，(4)，命题 10

(6) $x' + t \approx t$ (2)，(5)，(E3)

(7) $x' \approx \overline{0}$ (6)，命题 7

(8) $x' \not\approx \overline{0}$ (N1)

上面的 $x, y, z$ 取为不在 $t$ 中出现的三个不同的变元. 由 (7)，(8) 用归谬律得

$$\mathcal{N} \cup \{t \not\approx \overline{0} \wedge \cdots \wedge t \not\approx \overline{n}\} \vdash \neg(x + t \approx \overline{n}).$$

使用 Gen 规则及 2. 1. 3 小节命题 8-2° (量词与否定词交换次序)，便又得

$$\mathcal{N} \cup \{t \not\approx \overline{0} \wedge \cdots \wedge t \not\approx \overline{n}\} \vdash \neg \exists x(x + t \approx \overline{n}).$$

再用演绎定理即可. □

**命题 14** 设公式 $p(x)$ 中只含一个自由变元 $x$, 则有

$$\mathcal{N} \vdash (p(\overline{0}) \wedge \cdots \wedge p(\overline{n})) \rightarrow (x \leqslant \overline{n} \rightarrow p(x)).$$

**证** 利用演绎定理和换位律，只用证

$$\mathcal{N} \cup \{p(\overline{0}) \wedge \cdots \wedge p(\overline{n}), \neg p(x)\} \vdash x \nleqslant \overline{n}.$$

以下是所需要的证明:

(1) $x \approx \overline{k} \rightarrow (p(\overline{k}) \rightarrow p(x))$, $k = 0, \cdots, n$ 等项替换

(2) $p(\overline{k}) \rightarrow (\neg p(x) \rightarrow x \not\approx \overline{k})$, $k = 0, \cdots, n$

由 (1) 及永真式 $(p \rightarrow (q \rightarrow r)) \rightarrow (q \rightarrow (\neg r \rightarrow \neg p))$

(3) $p(\overline{k})$, $k = 0, \cdots, n$ 由假定

(4) $\neg p(x)$ 假定

(5) $x \not\approx \overline{k}$, $k = 0, \cdots, n$ (2)，(3)，(4)，MP

(6) $x \not\approx \overline{0} \wedge \cdots \wedge x \not\approx \overline{n}$ 由 (5)

(7) $x \nleqslant \overline{n}$ 由 (6) 及命题 13

□

**命题 15** 若 $n > 0$, 则

$$\mathcal{N} \vdash x \nleqslant \overline{n} \rightarrow \overline{n} \leqslant x.$$

**证** 只用证

$$\mathcal{N}\cup\{\neg\exists y(y+x\approx\overline{n})\}\vdash\exists y(y+\overline{n}\approx x),$$

其中选用 $y\neq x$.

(1) $\neg\exists y(y+x\approx\overline{n})$ 假定

(2) $\forall y\neg(y+x\approx\overline{n})$ 由 (1) 及 2. 1. 3 小节命题 8-2°

(3) $\forall y(y+x\not\approx\overline{n})\ \to\ \overline{n-k}+x\not\approx\overline{n},\ k=0,\cdots,n-1$ (K4)

(4) $\overline{n-k}+x\not\approx\overline{n},\ k=0,\cdots,n-1$ (2), (3), MP

(5) $\overline{n}\approx\ \overline{n-k}+\overline{k}$ 命题 1

(6) $x\approx\overline{k}\ \to\ \overline{n-k}+x\approx\overline{n-k}+\overline{k},\ k=0,\cdots,n-1$ (E2)

(7) $\overline{n-k}+x\not\approx\overline{n-k}+\overline{k}$ 由 (4), (5)

(8) $x\not\approx\overline{k},\ k=0,\cdots,n-1$ 由 (6), (7) 及换位律

(9) $x\not\approx\overline{0}\wedge\cdots\wedge x\not\approx\overline{n-1}$ 由 (8)

(10) $\exists y(y+\overline{n}\approx x)$ 由 (9) 及命题 12

□

**命题 16** 对任意自然数 $m$ 和 $n$,

(i) $m=n$ 时, $\mathcal{N}\vdash\overline{m}\approx\overline{n}$;

(ii) $m\neq n$ 时, $\mathcal{N}\vdash\overline{m}\not\approx\overline{n}$.

**证** (i) $\overline{m}\approx\overline{m}$ 是 (E1) 型公理.

(ii) $m\neq n$ 时, 不妨设 $m=n+k, k>0$. 这时以下公式从 $\mathcal{N}$ 可证:

(1) $\overline{n+k}\approx\overline{k}+\overline{n}$ 命题 1

(2) $\overline{n+k}\approx\overline{n}\ \to\ \overline{k}+\overline{n}\approx\overline{n}$ 由 (1) 及 (E3)

(3) $\overline{k}+\overline{n}\approx\overline{n}\ \to\ \overline{k}\approx\overline{0}$ 命题 7

(4) $\overline{n+k}\approx\overline{n}\ \to\ \overline{k}\approx\overline{0}$ (2), (3), HS

(5) $\overline{k}\not\approx\overline{0}\ \to\ \overline{n+k}\not\approx\overline{n}$ 由 (4) 及换位律

(6) $\overline{k}\not\approx\overline{0}$ (N1)(注意 $k>0, \overline{k}=\overline{k-1}'$)

(7) $\overline{n+k}\not\approx\overline{n}$ (5), (6), MP

此即 $\overline{m}\not\approx\overline{n}$. □

通常的数学证明可大量地翻译成形式证明. 但建立形式系统的目的, 不是用形式证明去完全代替通常的数学证明. 建立形式算术的主要目的之一, 是用以探讨关于自然数的性质, 我们究竟能精确而机械地抓住些什么.

## 练习 24

1. 证明当 $n=2k$ 时, $\mathcal{N}\vdash\exists x(x\times\overline{2}\approx\overline{n})$.

2. 证明 $\mathcal{N}\vdash\ t\approx\ \overline{n}+\overline{3}\ \to\ t\approx\overline{n+3}$.

3. 证明

(i) $\mathcal{N} \vdash t+\overline{1} \approx t'$,

(ii) $\mathcal{N} \vdash t\times\overline{2} \approx t+t$.

4. 证明 $\mathcal{N} \vdash t_1' + t_2 \not\approx t_1$.

*5. 在 $K_{\mathrm{N}}$ 中把个体常元由一个 (即 $c_1 = \overline{0}$) 增加为一列

$$c_0, c_1, \cdots$$

得到扩张的系统 $K_{\mathrm{N}}^{+}$. $\mathcal{N}$ 在增加如下公理后记为 $\mathcal{N}^{+}$:

$$c_i' \approx c_{i+1}, c_0 \not\approx c_i \ (i > 0).$$

求证 $\mathcal{N}^{+}$ 也是无矛盾的，且有不同于 $\mathbf{N}$ 的模型.

# 3.3 可表示函数与关系

我们以自然数集 $\mathbf{N}$ 为意想的解释域，建立了形式算术 $K_{\mathrm{N}}$. 现在要来深入研究 $K_{\mathrm{N}}$ 对自然数性质的表现能力究竟如何. 首先要研究的是 $K_{\mathrm{N}}$ 对数论函数、数论关系的表示能力. 研究过程中应注意，数论函数与数论关系是元系统中的概念.

## 3.3.1 什么是可表示

后面如不说明,“$k$ 元函数”皆指 $k$ 元数论函数 $f:\mathbf{N}^k \to \mathbf{N}$,“$R$ 是 $k$ 元关系”皆指 $R$ 是 $k$ 元数论关系，即 $R \subseteq \mathbf{N}^k$.

**定义 1 (可表示函数)** $k$ 元函数 $f$ 在 $K_{\mathrm{N}}$ 中可表示，是指存在着含 $k+1$ 个自由变元的公式 $p(x_1,\cdots,x_k,y)$, 它具有以下性质: 对任意 $n_1,\cdots,n_k,m \in \mathbf{N}$,

(i) $f(n_1,\cdots,n_k) = m \quad \Rightarrow \quad \mathcal{N} \vdash p(\overline{n_1},\cdots,\overline{n_k},\overline{m})$,

(ii) $f(n_1,\cdots,n_k) \neq m \quad \Rightarrow \quad \mathcal{N} \vdash \neg p(\overline{n_1},\cdots,\overline{n_k},\overline{m})$,

(iii) $\mathcal{N} \vdash \ p(\overline{n_1},\cdots,\overline{n_k},t) \ \to \ t \approx \overline{f(n_1,\cdots,n_k)}$,

其中 $t$ 是任意的对 $p(x_1,\cdots,x_k,y)$ 中 $y$ 自由的项. 这时还说 $f$ 用公式 $p(x_1,\cdots,x_k,y)$ 可表示.

下面证明，可表示函数的定义 (定义 1) 中的性质 (ii) 是多余的. 定义中加上它，是为了应用方便.

**命题 1** $k$ 元函数 $f$ 用公式 $p(x_1,\cdots,x_k,y)$ 在 $K_{\mathrm{N}}$ 中可表示的充要条件是: 对任意 $n_1,\cdots,n_k$ 及项 $t$ ($t$ 对 $p(x_1,\cdots,x_k,y)$ 中 $y$ 自由),

1° $\mathcal{N} \vdash p(\overline{n_1},\cdots,\overline{n_k},\overline{f(n_1,\cdots,n_k)})$,

2° $\mathcal{N} \vdash p(\overline{n_1},\cdots,\overline{n_k},t) \to t \approx \overline{f(n_1,\cdots,n_k)}$.

**证** 只用证由这里的条件可以推出定义 1 中的性质 (ii). (性质 (i) 由条件 1° 易得.) 事实上，在 $f(n_1,\cdots,n_k)\neq m$ 的假定之下，以下公式从 $\mathcal{N}$ 可证:

(1) $\overline{m}\not\approx\overline{f(n_1,\cdots,n_k)}$ 3.2 节命题 16 (ii)

(2) $p(\overline{n_1},\cdots,\overline{n_k},\overline{m})\to\overline{m}\approx\overline{f(n_1,\cdots,n_k)}$ 由条件 2°

(3) $\overline{m}\not\approx\overline{f(n_1,\cdots,n_k)}\to\neg p(\overline{n_1},\cdots,\overline{n_k},\overline{m})$ (2)，换位律

(4) $\neg p(\overline{n_1},\cdots,\overline{n_k},\overline{m})$ (1)，(3)，MP

□

命题 1 也可作为可表示函数的定义 (等价于定义 1). 但若要讨论一个已知的可表示函数 $f$ 的性质，从定义 1 出发比较方便 ($f$ 具有定义 1 中的性质 (i)，(ii)，(iii))；而若要证明一个函数可表示，则从命题 1 出发更方便 (证明它满足命题 1 的条件 1° 与 2° 便可).

先考虑一个问题: 是否每个 $K_N$ 中的公式都一定可用来表示一个数论函数?

回答是否定的. 例如，$x_1\approx x_1\wedge y\not\approx y$ 这个公式便不可能用来表示任何一个一元函数，因为定义 1 的性质 (i) 所要求的

$$\mathcal{N}\vdash\overline{n_1}\approx\overline{n_1}\wedge\overline{m}\not\approx\overline{m}$$

对任何 $n_1,m\in\mathbf{N}$ 都不会成立.

第二个问题是: 同一公式 $p(x_1,\cdots,x_k,y)$ 是否可用来表示两个不同的 $k$ 元函数?

回答也是否定的. 若 $f_1$ 和 $f_2$ 是两个不同的 $k$ 元函数，则有 $n_1,\cdots,n_k\in\mathbf{N}$ 使

(1) $f_2(n_1,\cdots,n_k)\neq f_1(n_1,\cdots,n_k)$.

设 $f_1$ 用 $p(x_1,\cdots,x_k,y)$ 可表示，按定义 1 中性质 (i)，有

(2) $\mathcal{N}\vdash p(\overline{n_1},\cdots,\overline{n_k},\overline{f_1(n_1,\cdots,n_k)})$.

又假设 $f_2$ 也是用 $p(x_1,\cdots,x_k,y)$ 可表示，那么按定义 1 的性质 (ii) (对 $f_2$ 而言，注意 (1) 式)，有

(3) $\mathcal{N}\vdash\neg p(\overline{n_1},\cdots,\overline{n_k},\overline{f_1(n_1,\cdots,n_k)})$.

(2) 与 (3) 导致了 $\mathcal{N}$ 是有矛盾的.

关于数论函数与 $K_N$ 公式之间联系的第三个问题是: 是否每个数论函数都可用 $K_N$ 的公式来表示? 回答还是否定的. 事实上，所有数论函数构成的集是不可数集 (参见 0. 3 节)，而 $K_N$ 中所有公式构成可数集，其中已经知道有的公式还不能用来表示任何函数，又知道能用来表示函数的公式只能各自唯一地表示某一个函数. 所以在 $K_N$ 中可表示函数的全体是个可数集.

以上的讨论说明，大量的数论函数在 $K_N$ 中是不可表示的. 但至今积累的经验表明，凡是“算法可计算的”数论函数都在 $K_N$ 中可表示. 后面我们将要深入地讨论这个问题.

**定义 2 (投影函数)** $k$ 元投影函数 $\mathrm{p}_i^k$ 是指由下式规定的函数

$$\mathrm{p}_i^k(n_1,\cdots,n_k)=n_i,\quad (i=1,\cdots,k).$$

**命题 2** 函数 $+,\times$ 和 $\mathrm{p}_i^k$ 在 $K_{\mathrm{N}}$ 中是可表示的.

**证** (1) 二元和函数 + 是用公式 $x_1+x_2\approx y$ 表示的. 事实上，由 3.2 节命题 1，首先有

$$\mathcal{N}\vdash\ \overline{n_1}+\overline{n_2}\ \approx\overline{n_1+n_2},$$

又由此用等词性质可得

$$\mathcal{N}\vdash\ \overline{n_1}+\overline{n_2}\ \approx t\ \rightarrow\ t\approx\overline{n_1+n_2},$$

这说明命题 1 中的条件 1° 与 2° 都得满足.

(2) 二元乘积函数 × 是用公式 $x_1\times x_2\ \approx y$ 表示的. 理由相同，只是要改用 3.2 节命题 2.

(3) $\mathrm{p}_i^k$ 是用公式 $x_1\approx x_1\wedge\cdots\wedge x_k\approx x_k\wedge y\approx x_i$ 表示的. 事实上，因 $\mathrm{p}_i^k(n_1,\cdots,n_k)=n_i$，用 3.2 节命题 16 (i) 及等词性质可得

1° $\mathcal{N}\vdash\ \overline{n_1}\approx\overline{n_1}\wedge\cdots\wedge\overline{n_k}\approx\overline{n_k}\wedge\ \overline{\mathrm{p}_i^k(n_1,\cdots,n_k)}\approx\overline{n_i}$,

2° $\mathcal{N}\vdash\ \overline{n_1}\approx\overline{n_1}\wedge\cdots\wedge\overline{n_k}\approx\overline{n_k}\wedge\ t\approx\overline{n_i}\ \rightarrow\ t\approx\overline{\mathrm{p}_i^k(n_1,\cdots,n_k)}$,

于是命题 1 的条件 1°, 2° 得到满足. □

**定义 3 (可表示关系)** $\mathbf{N}$ 上的 $k$ 元关系 $R$ 在 $K_{\mathrm{N}}$ 中可表示，是指存在着含有 $k$ 个自由变元的公式 $p(x_1,\cdots,x_k)$, 它具有以下性质: 对任意 $n_1,\cdots,n_k\in\mathbf{N}$,

(i) $(n_1,\cdots,n_k)\in R\ \Rightarrow\ \mathcal{N}\vdash p(\overline{n_1},\cdots\overline{n_k})$,

(ii) $(n_1,\cdots,n_k)\notin R\ \Rightarrow\ \mathcal{N}\vdash\neg p(\overline{n_1},\cdots\overline{n_k})$.

这时我们说 $R$ 用公式 $p(x_1,\cdots,x_k)$ 在 $K_{\mathrm{N}}$ 中可表示.

现在考察: 是否每个 $K_{\mathrm{N}}$ 的公式 $p(x_1,\cdots,x_k)$ 都一定可用来表示某个 $k$ 元关系?

这个问题的回答与 $\mathcal{N}$ 的“完备性”有关. 如果存在公式 $p(x_1,\cdots,x_k)$ 及 $n_1,\cdots,n_k\in\mathbf{N}$ 使

$$\mathcal{N}\nvdash p(\overline{n_1},\cdots,\overline{n_k})\ \text{且}\ \mathcal{N}\nvdash\neg p(\overline{n_1},\cdots,\overline{n_k}),$$

那么我们说闭式 $p(\overline{n_1},\cdots,\overline{n_k})$ 是一个从 $\mathcal{N}$ 不可判定的公式，并且说 $\mathcal{N}$ 不完备. 这时公式 $p(x_1,\cdots,x_k)$ 便不能用来表示任何一个关系. 理由很简单: 如果 $k$ 元关系 $R$ 用它可表示，那么依据定义 3，$\mathcal{N}\vdash p(\overline{n_1},\cdots,\overline{n_k})$ 与 $\mathcal{N}\vdash\neg p(\overline{n_1},\cdots,\overline{n_k})$ 必有一个成立 (这是因为 $(n_1,\cdots,n_k)\in R$ 与 $(n_1,\cdots,n_k)\notin R$ 二者必居其一)，于是闭式 $p(\overline{n_1},\cdots,\overline{n_k})$ 就成了可判定公式.

相反，如果 $\mathcal{N}$ 是完备的，那么任何含 $k$ 个自由变元的公式 $p(x_1,\cdots,x_k)$ 都一定表示了某个 $k$ 元关系，因为这时对任意 $n_1,\cdots,n_k\in\mathbf{N}$, $\mathcal{N}\vdash p(\overline{n_1},\cdots,\overline{n_k})$ 与 $\mathcal{N}\vdash\neg p(\overline{n_1},\cdots,\overline{n_k})$ 必有一个成立.

算术公理集 $\mathcal{N}$ 是否完备，即是否不存在从 $\mathcal{N}$ 不可判定的闭式，这是下面要讨论的中心课题. "可表示关系"的定义正是服务于这个中心课题而提出的.

**例 1** 二元关系"相等"在 $K_{\mathrm{N}}$ 中用公式 $x_1 \approx x_2$ 可表示. 事实上，由 3.2 节命题 16，我们有

$$n_1 = n_2 \quad \Rightarrow \quad \mathcal{N} \vdash \overline{n_1} \approx \overline{n_2},$$

$$n_1 \neq n_2 \quad \Rightarrow \quad \mathcal{N} \vdash \overline{n_1} \not\approx \overline{n_2}.$$

下面的命题 3 指出，每个可表示的关系都伴随着一个可表示函数——该关系的特征函数. 这样，对可表示关系的研究联系着对可表示函数的研究.

首先回忆特征函数的定义. $k$ 元关系 $R(\subseteq \mathbf{N}^k)$ 的特征函数 $C_R: \mathbf{N}^k \to \{0,1\}$ 是用下式定义的:

$$C_R(n_1, \cdots, n_k) = \begin{cases} 1, & (n_1, \cdots, n_k) \in R; \\ 0, & (n_1, \cdots, n_k) \notin R. \end{cases}$$

**命题 3** 关系 $R$ 可表示 $\Leftrightarrow$ $R$ 的特征函数 $C_R$ 可表示.

**证** 先设 $k$ 元关系 $R$ 用公式 $p(x_1, \cdots, x_k)$ 可表示. 我们来证明，$R$ 的特征函数 $C_R$ 用下面的公式可表示:

$$(p(x_1, \cdots, x_k) \wedge y \approx \overline{1}) \vee (\neg p(x_1, \cdots, x_k) \wedge y \approx \overline{0}),$$

也就是要证明此公式与 $C_R$ 满足命题 1 中的条件 1° 和 2°. 现分别验证如下:

1° 要证明对任意 $n_1, \cdots, n_k \in \mathbf{N}$, 总有

(1) $\mathcal{N} \vdash (p(\overline{n_1}, \cdots, \overline{n_k}) \wedge \overline{C_R(n_1, \cdots, n_k)} \approx \overline{1})$
$\vee (\neg p(\overline{n_1}, \cdots, \overline{n_k}) \wedge \overline{C_R(n_1, \cdots, n_k)} \approx \overline{0}).$

事实上，当 $(n_1, \cdots, n_k) \in R$ 时，因定义 3 的性质 (i) 成立及 $C_R(n_1, \cdots, n_k) = 1$, 故有

$$\mathcal{N} \vdash p(\overline{n_1}, \cdots, \overline{n_k}) \wedge \overline{C_R(n_1, \cdots, n_k)} \approx \overline{1},$$

于是 (1) 成立; 而当 $(n_1, \cdots, n_k) \notin R$ 时，因定义 3 的性质 (ii) 成立及 $C_R(n_1, \cdots, n_k) = 0$, 故有

$$\mathcal{N} \vdash \neg p(\overline{n_1}, \cdots, \overline{n_k}) \wedge \overline{C_R(n_1, \cdots, n_k)} \approx \overline{0},$$

此时 (1) 也成立. 这里两次用到 3.2 节命题 16 (i).

2° 要证明

$$\mathcal{N} \cup \{(p(\overline{n_1}, \cdots, \overline{n_k}) \wedge t \approx \overline{1}) \vee (\neg p(\overline{n_1}, \cdots, \overline{n_k}) \wedge t \approx \overline{0})\} \vdash t \approx \overline{C_R(n_1, \cdots, n_k)}.$$

为此，分以下两种情形讨论:

当 $(n_1, \cdots, n_k) \in R$ 时 (此时 $C_R(n_1, \cdots, n_k) = 1$)，有如下证明:

(1) $p(\overline{n_1}, \cdots, \overline{n_k})$ 定义 3 (i)

(2) $\neg(\neg p(\overline{n_1}, \cdots, \overline{n_k}) \wedge t \approx \overline{0})$ 由 (1) 及永真式 $p \to \neg(\neg p \wedge q)$

(3) $(p(\overline{n_1},\cdots,\overline{n_k})\wedge t\approx\overline{1})\vee(\neg p(\overline{n_1},\cdots,\overline{n_k})\wedge t\approx\overline{0})$ 假定

(4) $p(\overline{n_1},\cdots,\overline{n_k})\wedge t\approx\overline{1}$ 由 (2)，(3) 及永真式 $(p\vee q)\to(\neg q\to p)$

(5) $t\approx\overline{1}$ 由 (4) 及永真式 $(p\wedge q)\to q$

(6) $t\approx\overline{C_R(n_1,\cdots,n_k)}$ 由（5）及 $C_R(n_1,\cdots,n_k)=1$

当 $(n_1,\cdots,n_k)\notin R$ 时（此时 $C_R(n_1,\cdots,n_k)=0$），有如下证明:

(1) $\neg p(\overline{n_1},\cdots,\overline{n_k})$ 定义 3 (ii)

(2) $\neg(p(\overline{n_1},\cdots,\overline{n_k})\wedge t\approx\overline{1})$ 由 (1) 及永真式 $\neg p\to\neg(p\wedge q)$

(3) $(p(\overline{n_1},\cdots,\overline{n_k})\wedge t\approx\overline{1})\vee(\neg p(\overline{n_1},\cdots,\overline{n_k})\wedge t\approx\overline{0})$ 假定

(4) $\neg p(\overline{n_1},\cdots,\overline{n_k})\wedge t\approx\overline{0}$ (2)，(3) 及永真式 $p\vee q\to(\neg p\to q)$

(5) $t\approx\overline{0}$ 由 (4) 及永真式 $(p\wedge q)\to q$

(6) $t\approx\overline{C_R(n_1,\cdots,n_k)}$ 由（5）及 $C_R(n_1,\cdots,n_k)=0$

至此，由命题 1 知 $C_R$ 是可表示的.

相反的方向，设 $C_R$ 用公式 $p(x_1,\cdots,x_k,y)$ 可表示，则可证明 $R$ 用

$$p(x_1,\cdots,x_k,\overline{1})$$

可表示. 事实上，

(i) $(n_1,\cdots,n_k)\in R \quad\Rightarrow\quad C_R(n_1,\cdots,n_k)=1$

$\qquad\qquad\Rightarrow\quad \mathcal{N}\vdash p(\overline{n_1},\cdots,\overline{n_k},\overline{1})$,

这里对 $C_R$ 用了定义 1 (i);

(ii) $(n_1,\cdots,n_k)\notin R$ 时，$C_R(n_1,\cdots,n_k)=0$. 此时以下公式从 $\mathcal{N}$ 可证:

(1) $p(\overline{n_1},\cdots,\overline{n_k},\overline{1})\ \to\ \overline{1}\approx\overline{C_R(n_1,\cdots,n_k)}$ 对 $C_R$ 用定义 1 (iii)

(2) $p(\overline{n_1},\cdots,\overline{n_k},\overline{1})\ \to\ \overline{1}\approx\overline{0}$ 由 (1) 及 $C_R(n_1,\cdots,n_k)=0$

(3) $\overline{1}\not\approx\overline{0}\ \to\ \neg p(\overline{n_1},\cdots,\overline{n_k},\overline{1})$ (2)，换位律

(4) $\overline{1}\not\approx\overline{0}$ (N1)

(5) $\neg p(\overline{n_1},\cdots,\overline{n_k},\overline{1})$ (3)，(4)，MP

□

**命题 4** 二元关系“$\leqslant$”是可表示关系，从而它的特征函数 $C_{\leqslant}$ 是可表示函数.

**证** 二元关系“$\leqslant$”用公式 $\exists z(z+x_1\approx x_2)$ 可表示. 对此需要验证定义 3 中的条件 (i)，(ii) 成立.

(i) 验证 $n_1\leqslant n_2 \quad\Rightarrow\quad \mathcal{N}\vdash\exists z(z+\overline{n_1}\approx\overline{n_2})$.

事实上，当 $n_1\leqslant n_2$ 时，有

$\mathcal{N}\vdash\overline{n_2-n_1}+\overline{n_1}\approx\overline{n_2}$, 3.2 节命题 1

$\mathcal{N}\vdash\overline{n_2-n_1}+\overline{n_1}\approx\overline{n_2}\ \to\ \exists z(z+\overline{n_1}\approx\overline{n_2})$, $\exists_1$ 规则

$\mathcal{N}\vdash\exists z(z+\overline{n_1}\approx\overline{n_2})$.

(ii) 验证 $n_1>n_2 \quad\Rightarrow\quad \mathcal{N}\vdash\neg\exists z(z+\overline{n_1}\approx\overline{n_2})$.

事实上，当 $n_1 > n_2$ 时，设 $n_1 = n_2 + k, k > 0$, 这时以下公式从 $\mathcal{N} \cup \{z + \overline{n_1} \approx \overline{n_2}\}$ 可证:

(1) $z + \overline{n_1} \approx \overline{n_2}$ 假定

(2) $\overline{n_1} \approx \overline{k} + \overline{n_2}$ 由 3.2 节命题 1

(3) $z + (\overline{k} + \overline{n_2}) \approx \overline{n_2}$ (1)，(2) 等项替换

(4) $(\overline{k} + z) + \overline{n_2} \approx \overline{n_2}$ (3)，结合律，交换律

(5) $\overline{k} + z \approx \overline{0}$ (4)，3.2 节命题 7

(6) $\overline{k} \approx \overline{0}$ 即 $\overline{k-1}' \approx \overline{0}$ (5)，3.2 节命题 8

(7) $\overline{k-1}' \not\approx \overline{0}$ (N1)

由 (6)，(7) 用归谬律得

$\mathcal{N} \vdash \neg(z + \overline{n_1} \approx \overline{n_2})$,

$\mathcal{N} \vdash \forall z \neg(z + \overline{n_1} \approx \overline{n_2})$, Gen

$\mathcal{N} \vdash \neg\exists z(z + \overline{n_1} \approx \overline{n_2})$. 由 2. 1. 3 小节命题 8-2°

□

因为同一个公式不能用来表示两个不同的关系 (证明留作练习)，所以大量的关系是不可表示的. $K_{\mathrm{N}}$ 中所有的公式构成可数集，而自然数集 **N** 上所有关系构成的集是不可数集. (参见 0. 3 节)

### 练习 25

1. 证明一元零函数 z 和后继函数 s 是可表示的 ($\mathrm{z}(n) = 0, \mathrm{s}(n) = n + 1$).

2. 证明 $K_{\mathrm{N}}$ 中的同一个公式不能用来表示两个不同的关系.

3. 若把定义 3 中的性质 (i) 和 (ii) 换成一条:

$$(n_1, \cdots, n_k) \in R \quad \Leftrightarrow \quad \mathcal{N} \vdash p(\overline{n_1}, \cdots, \overline{n_k}),$$

得到的是不是等价的定义?

4. 设 $k$ 元关系 $R$ 用 $p(x_1, \cdots, x_k)$ 可表示，$C_R$ 为 $R$ 的特征函数. 试证明

$$C_R(n_1, \cdots, n_k) = |p(\overline{n_1}, \cdots, \overline{n_k})|_{\mathrm{N}}.$$

## 3.3.2 函数的复合和 $\mu$ 算子保持可表示性

这里要建立两个关于数论函数和 $K_{\mathrm{N}}$ 中公式之间关系的更深入的结果，它们的建立是证明递归函数在 $K_{\mathrm{N}}$ 中可表示的重要步骤.

为了书写简短，把 $n_1, \cdots, n_k$ 简写成 $\alpha$; 把 $\overline{n_1}, \cdots, \overline{n_k}$ 简写成 $\overline{\alpha}$.

**定理 1** 函数的复合保持可表示性. 具体地说，设 $j$ 元函数 $g$ 和 $j$ 个 $k$ 元函数

$h_1,\cdots,h_j$ 都是可表示的，那么如下定义的 $k$ 元函数 $f$ 也是可表示的:

$$f(n_1,\cdots,n_k)=g(h_1(n_1,\cdots,n_k),\cdots,h_j(n_1,\cdots,n_k)),$$

此式简写为

$$f(\alpha)=g(h_1(\alpha),\cdots,h_j(\alpha)).$$

**证**　设 $g,h_1,\cdots,h_j$ 分别用公式

$$q(x_1,\cdots,x_j,y),r_1(x_1,\cdots,x_k,y),\cdots,r_j(x_1,\cdots,x_k,y)$$

表示. 现在来证明 $k$ 元函数 $f$ 用下面的公式可表示

$$\exists y_1\cdots\exists y_j(r_1(x_1,\cdots,x_k,y_1)\wedge\cdots\wedge r_j(x_1,\cdots,x_k,y_j)\wedge q(y_1,\cdots,y_j,y)),$$

其中 $y_1,\cdots,y_j$ 是 $j$ 个不在

$$q(x_1,\cdots,x_j,y),r_1(x_1,\cdots,x_k,y),\cdots,r_j(x_1,\cdots,x_k,y)$$

中出现的变元.

为此，按照 3.3.1 小节命题 1，要证明以下两点:

1° $\mathcal{N}\vdash\exists y_1\cdots\exists y_j(r_1(\overline{\alpha},y_1)\wedge\cdots\wedge r_j(\overline{\alpha},y_j)\wedge q(y_1,\cdots,y_j,\overline{f(\alpha)}))$.

2° $\mathcal{N}\vdash\exists y_1\cdots\exists y_j(r_1(\overline{\alpha},y_1)\wedge\cdots\wedge r_j(\overline{\alpha},y_j)\wedge q(y_1,\cdots,y_j,t))\to t\approx\overline{f(\alpha)}$.

先证 1°. 因 $h_1,\cdots,h_j$ 分别用 $r_1(x_1,\cdots,x_k,y),\cdots,r_j(x_1,\cdots,x_k,y)$ 表示，故由 3.3.1 小节命题 1 中性质 1° 知，对任意 $n_1,\cdots,n_k\in\mathbf{N}$, 有

(1) $\mathcal{N}\vdash r_1(\overline{\alpha},\overline{h_1(\alpha)}),\cdots,\mathcal{N}\vdash r_j(\overline{\alpha},\overline{h_j(\alpha)})$.

因 $g$ 用 $q(x_1,\cdots,x_j,y)$ 表示，故对 $h_1(\alpha),\cdots,h_j(\alpha)$ 这 $j$ 个自然数，有

(2) $\mathcal{N}\vdash q(\overline{h_1(\alpha)},\cdots,\overline{h_j(\alpha)},\overline{g(h_1(\alpha),\cdots,h_j(\alpha))})$.

注意 (2) 中的 $g(h_1(\alpha),\cdots,h_j(\alpha))$ 就是 $f(\alpha)$, 由 (1)，(2) 立即得

$$\mathcal{N}\vdash r_1(\overline{\alpha},\overline{h_1(\alpha)})\wedge\cdots\wedge r_j(\overline{\alpha},\overline{h_j(\alpha)})\wedge q(\overline{h_1(\alpha)},\cdots,\overline{h_j(\alpha)},\overline{f(\alpha)}),$$

由此 $j$ 次应用 $\exists_1$ 规则便证明了 1°.

再证 2°. 对 $h_1,\cdots,h_j$ 用 3.3.1 小节命题 1 中性质 2°, 便可得

(3) $\mathcal{N}\vdash r_1(\overline{\alpha},y_1)\to y_1\approx\overline{h_1(\alpha)}$,

……

$(j+2)$　$\mathcal{N}\vdash r_j(\overline{\alpha},y_j)\to y_j\approx\overline{h_j(\alpha)}$.

于是以下公式从

$$\mathcal{N}\cup\{r_1(\overline{\alpha},y_1)\wedge\cdots\wedge r_j(\overline{\alpha},y_j)\wedge q(y_1,\cdots,y_j,t)\}$$

可证:

| | | |
|---|---|---|
| $(j+3)$ | $y_1\approx\overline{h_1(\alpha)}$ | (3)，假定，MP |
| | …… | |
| $(2j+2)$ | $y_j\approx\overline{h_j(\alpha)}$ | $(j+2)$，假定，MP |

$(2j+3)\quad q(y_1,\cdots,y_j,t)$ 假定

$(2j+4)\quad q(\overline{h_1(\alpha)},\cdots,\overline{h_j(\alpha)},t)$ $(2j+3)$，等项替换

$(2j+5)\quad q(\overline{h_1(\alpha)},\cdots,\overline{h_j(\alpha)},t)\ \to\ t\approx\overline{g(h_1(\alpha),\cdots,h_j(\alpha))}$

对 $g$ 用 3.3.1 小节命题 1 的性质 2°

$(2j+6)\quad t\approx\overline{g(h_1(\alpha),\cdots,h_j(\alpha))}$ $(2j+4),(2j+5)$, MP

此即 $t\approx\overline{f(\alpha)}$. 于是我们证明了

$$\mathcal{N}\cup\{r_1(\overline{\alpha},y_1)\wedge\cdots\wedge r_j(\overline{\alpha},y_j)\wedge q(y_1,\cdots,y_j,t)\}\vdash t\approx\overline{f(\alpha)},$$

最后，$j$ 次应用 $\exists_2$ 规则便证明了 2°. □

有了定理 1，我们就能从已知的可表示函数出发用复合的方式得到更多新的可表示函数.

**定义 1 (最小数算子，即 $\mu$ 算子)** 设 $k+1$ 元函数 $g$ 满足“根存在性条件”: 对任意 $n_1,\cdots,n_k$ 都存在自然数 $x$ 使 $g(n_1,\cdots,n_k,x)=0$. 现用下式来定义 $k$ 元函数 $f$:

$$f(n_1,\cdots,n_k)=\min\{x\,|\,g(n_1,\cdots,n_k,x)=0\},$$

即把 $f(n_1,\cdots,n_k)$ 定义为满足 $g(n_1,\cdots,n_k,x)=0$ 的 $x$ 的最小值. 我们把这样定义的 $k$ 元函数 $f$ 说成是由已给的 $k+1$ 元函数 $g$ 使用最小数算子或 $\mu$ 算子得来的，并写

$$f(n_1,\cdots,n_k)=\mu x[g(n_1,\cdots,n_k\,x)=0].$$

由定义立即可知，如果 $f$ 是由 $g$ 使用 $\mu$ 算子得来，那么以下两点自然成立.

(i) $f(n_1,\cdots,n_k)$ 是“根”:

$$g(n_1,\cdots,n_k,f(n_1,\cdots,n_k))=0,\text{即 } g(\alpha,f(\alpha))=0.$$

(ii) $f(n_1,\cdots,n_k)$ 这个根具有“最小性”:

$$g(n_1,\cdots,n_k,x)=0\ \Rightarrow\ f(n_1,\cdots,n_k)\leqslant x\text{ 即 } f(\alpha)\leqslant x.$$

下面涉及到 $\mu$ 算子时，如不作说明，都算已假设根的存在性条件得到满足. 若根的存在性不满足，就会出现偏函数 (指可能在一些点没有定义的函数)，而现在暂只讨论全函数，即处处有定义的函数.

**定理 2** $\mu$ 算子保持可表示性. 具体地说，设 $k+1$ 元函数 $g$ 在 $K_{\mathrm{N}}$ 中可表示，那么由 $g$ 使用 $\mu$ 算子得到的 $k$ 元函数 $f$ 也在 $K_{\mathrm{N}}$ 中可表示.

**证** 设 $k+1$ 元函数 $g$ 用 $q(x_1,\cdots,x_k,x_{k+1},y)$ 可表示. 现在来证明由 $g$ 使用 $\mu$ 算子得到的 $k$ 元函数 $f$ 用下面的公式可表示:

$$q(x_1,\cdots,x_k,y,\overline{0})\wedge\forall x(q(x_1,\cdots,x_k,x,\overline{0})\to y\leqslant x),$$

其中 $x$ 取成不在 $q(x_1,\cdots,x_k,y,\overline{0})$ 中出现的变元. 为此需要证明 3.3.1 小节命题 1 中的条件 1°, 2° 得到满足.

首先来证明

1° $\mathcal{N} \vdash q(\overline{\alpha}, \overline{f(\alpha)}, \overline{0}) \wedge \forall x(q(\overline{\alpha}, x, \overline{0}) \rightarrow \overline{f(\alpha)} \leqslant x)$.

因 $g$ 是用 $q(x_1, \cdots, x_{k+1}, y)$ 表示的，又因 $g(\alpha, f(\alpha)) = 0$ ($f(\alpha)$ 是“根”)，故立即由 3.3.1 小节命题 1 中的条件 1° 知

$$\mathcal{N} \vdash q(\overline{\alpha}, \overline{f(\alpha)}, \overline{0}).$$

这样，问题归结为要证明

$$(*) \quad \mathcal{N} \vdash \forall x(q(\overline{\alpha}, x, \overline{0}) \rightarrow \overline{f(\alpha)} \leqslant x).$$

分两种情形来证明 (*).

情形 1 $f(\alpha) = 0$

$\mathcal{N} \vdash x + \overline{f(\alpha)} \approx x$, (N3)

$\mathcal{N} \vdash \exists z(z + \overline{f(\alpha)} \approx x)$ 即 $\overline{f(\alpha)} \leqslant x$, ($\exists_1$ 规则，下面有说明)

$\mathcal{N} \vdash q(\overline{\alpha}, x, \overline{0}) \rightarrow \overline{f(\alpha)} \leqslant x$, (肯定后件律)

用一次 Gen 规则便可. 上面的中间一步使用了 $\exists_1$ 规则 (见 2. 1. 3 小节命题 2):

$$\vdash p(t) \rightarrow \exists z p(z),$$

这里公式 $p(z)$ 取为 $z + \overline{f(\alpha)} \approx x$, 项 $t$ 取为 $x$, $t$(即 $x$) 对 $p(z)$ 中的 $z$ 是自由的，用 $t$ 代换 $p(z)$ 中的 $z$ 得到的 $p(t)$ 是 $x + \overline{f(\alpha)} \approx x$.

情形 2 $f(\alpha) > 0$

因 $f(\alpha)$ 是“最小根”，故有

$$g(\alpha, 0) \neq 0,$$
$$\cdots\cdots$$
$$g(\alpha, f(\alpha) - 1) \neq 0.$$

对 $g$ 用 3.3.1 小节定义 1 的性质 (ii)，有

$$\mathcal{N} \vdash \neg q(\overline{\alpha}, \overline{0}, \overline{0}),$$
$$\cdots\cdots$$
$$\mathcal{N} \vdash \neg q(\overline{\alpha}, \overline{f(\alpha) - 1}, \overline{0}).$$

由此，注意以下等词性质

$$\mathcal{N} \vdash x \approx \overline{0} \rightarrow (q(\overline{\alpha}, x, \overline{0}) \rightarrow q(\overline{\alpha}, \overline{0}, \overline{0})),$$
$$\cdots\cdots$$
$$\mathcal{N} \vdash x \approx \overline{f(\alpha) - 1} \rightarrow (q(\overline{\alpha}, x, \overline{0}) \rightarrow q(\overline{\alpha}, \overline{f(\alpha) - 1}, \overline{0})),$$

用永真式

$$(\neg r \wedge q \wedge (p \rightarrow (q \rightarrow r))) \rightarrow \neg p$$

便得

$$\mathcal{N}\cup\{q(\overline{\alpha},x,\overline{0})\}\vdash x\not\approx\overline{0},$$

$$\cdots\cdots$$

$$\mathcal{N}\cup\{q(\overline{\alpha},x,\overline{0})\}\vdash x\not\approx\overline{f(\alpha)-1}.$$

再根据 3.2 节命题 12 得

$$\mathcal{N}\cup\{q(\overline{\alpha},x,\overline{0})\}\vdash \overline{f(\alpha)}\leqslant x,$$

使用演绎定理和 Gen 规则便证明了 (*). 这就证明了条件 1° 得到满足.

剩下还要证明 $f$ 满足

2° $\mathcal{N}\vdash (q(\overline{\alpha},t,\overline{0})\wedge\forall x(q(\overline{\alpha},x,\overline{0})\to t\leqslant x))\to t\approx\overline{f(\alpha)}.$

公式 $t\approx\overline{f(\alpha)}$ 从

$$\mathcal{N}\cup\{q(\overline{\alpha},t,\overline{0})\wedge\forall x(q(\overline{\alpha},x,\overline{0})\to t\leqslant x)\}$$

可证，下面就是所需要的证明:

| | |
|---|---|
| (1) $q(\overline{\alpha},t,\overline{0})$ | 假定 |
| (2) $\forall x(q(\overline{\alpha},x,\overline{0})\to t\leqslant x)$ | 假定 |
| (3) $q(\overline{\alpha},\overline{f(\alpha)},\overline{0})$ | 由 1° |
| (4) $\forall x(q(\overline{\alpha},x,\overline{0})\to \overline{f(\alpha)}\leqslant x)$ | 由 1° |
| (5) $q(\overline{\alpha},\overline{f(\alpha)},\overline{0})\to t\leqslant\overline{f(\alpha)}$ | (2)，(K4)，MP |
| (6) $q(\overline{\alpha},t,\overline{0})\to \overline{f(\alpha)}\leqslant t$ | (4)，(K4)，MP |
| (7) $t\leqslant\overline{f(\alpha)}$ | (3)，(5)，MP |
| (8) $\overline{f(\alpha)}\leqslant t$ | (1)，(6)，MP |
| (9) $t\approx\overline{f(\alpha)}$ | (7)，(8)，3.2 节命题 10 |

□

## 练习 26

以下函数和关系用什么公式可表示?

1. $f(n)=2$.
2. $f(n)=n+2$.
3. $f(n_1,n_2)=2(n_1+n_2)$.
4. 二元关系“>”.

# 3.4 递归函数

现在我们要暂时离开形式系统 $K_N$ 而对一类重要的数论函数进行一些数学研究，然后再回来继续讨论数论函数与 $K_N$ 中公式之间的关系.

在数论函数中，我们对递归函数有特殊的兴趣. 本节建立递归函数、递归关系和递归集的概念，这些在证明 Gödel 不完备性定理的过程中起着重要作用.

## 3.4.1 递归函数的一般定义

**定义 1 (递归函数)** 基本函数以及由它们经有限次使用下面的规则 I, II, III 得到的函数叫做递归函数 (或叫做一般递归函数)，这里的基本函数是指以下三种函数:

(1) 一元零函数 z, $z(n) = 0$,

(2) 一元后继函数 s, $s(n) = n + 1$,

(3) $k$ 元投影函数 $p_i^k$, $p_i^k(n_1, \cdots, n_k) = n_i$, $i = 1, \cdots, k$.

规则 I ——复合:

一个 $j$ 元函数 $g$ 和 $j$ 个 $k$ 元函数 $h_1, \cdots, h_j$ 复合成一个 $k$ 元函数 $f$, $f$ 的定义式为

$$f(n_1, \cdots, n_k) = g(h_1(n_1, \cdots, n_k), \cdots, h_j(n_1, \cdots, n_k));$$

规则 II ——递归:

由 $k$ 元函数 $g$ 和 $k+2$ 元函数 $h$ 使用递归规则生成 $k+1$ 元函数 $f$, 生成的方式是

$$f(n_1, \cdots, n_k, 0) = g(n_1, \cdots, n_k),$$

$$f(n_1, \cdots, n_k, n+1) = h(n_1, \cdots, n_k, n, f(n_1, \cdots, n_k, n)),$$

$k = 0$ 时，由给定的自然数 $g$ 和二元函数 $h$ 使用递归规则生成一元函数 $f$ 的方式是

$$f(0) = g,$$

$$f(n+1) = h(n, f(n));$$

规则 III —— $\mu$ 算子 (3.3.2 小节定义 1):

若 $k$+1 元函数 $g$ 满足根存在性条件 (对任意 $n_1, \cdots, n_k$ 都存在 $x$ 使 $g(n_1, \cdots, n_k, x) = 0$), 则可由 $g$ 使用 $\mu$ 算子生成 $k$ 元函数 $f$,

$$f(n_1, \cdots, n_k) = \mu x[g(n_1, \cdots, n_k, x) = 0].$$

若去掉规则 III，只允许使用规则 I 与 II，其他都不变，则定义的函数叫做原始递归函数. 若去掉规则 III 中的根存在性条件这个限制，则定义的函数叫做递归偏函数.

递归偏函数不一定处处有定义. $\mu$ 算子的根存在性条件不一定处处得到满足是产生递归偏函数的原因. 在使用 $\mu$ 算子生成递归全函数 (即处处有定义的递归函数) 时，必须要检查根存在性条件是否处处满足.

按照定义证明一个函数的递归性，应说明它是由哪些基本函数依何种次序、用什么规则生成的. 但以后不必每次都由三种基本函数出发来进行递归描述. 在描述过程中可以使用已经得到的已知递归函数.

下面由三种基本函数出发，使用三种规则，一个接一个地生成一系列常用递归函数.

1° $k$ 元常值函数 $\mathrm{c}_m$，定义式是

$$\mathrm{c}_m(n_1,\cdots,n_k)=m.$$

$\mathrm{c}_m$ 是递归函数，这是因为 (对 $m$ 归纳):

$$\mathrm{c}_0(n_1,\cdots,n_k)=\mathrm{z}(\mathrm{p}_1^k(n_1,\cdots,n_k)),$$
$$\mathrm{c}_{m+1}(n_1,\cdots,n_k)=\mathrm{s}(\mathrm{c}_m(n_1,\cdots,n_k)).$$

$\mathrm{c}_0$ 是一元零函数 z 和 $k$ 元投影函数 $\mathrm{p}_1^k$ 的复合；$\mathrm{c}_{m+1}$ 是后继函数 s 和 $\mathrm{c}_m$ 的复合.

2° 二元和函数+

$$n_1+0=\mathrm{p}_1^1(n_1),$$
$$n_1+(n+1)=(n_1+n)+1=\mathrm{s}(\mathrm{p}_3^3(n_1,n,n_1+n)),$$

这里是由一元函数 $\mathrm{p}_1^1$ 和三元函数 $h$ 使用递归规则 II 生成二元和函数的，其中 $h$ 由下式定义:

$$h(n_1,n_2,n_3)=\mathrm{s}(\mathrm{p}_3^3(n_1,n_2,n_3)).$$

如果用 $f$ 表示二元和函数，那么可以更清楚地写为

$$f(n_1,0)=\mathrm{p}_1^1(n_1),$$
$$f(n_1,n+1)=h(n_1,n,f(n_1,n)).$$

$\mathrm{p}_1^1$ 和 $h$ 是递归的，故二元和函数也是递归的.

3° 二元积函数×

$$n_1\times 0=\mathrm{z}(n_1),$$
$$n_1\times(n+1)=\mathrm{p}_3^3(n_1,n,n_1\times n)+\mathrm{p}_1^3(n_1,n,n_1\times n).$$

这里也使用了规则 II.

4° 前邻函数 $\mathrm{p}^-$ 的定义式是

$$\mathrm{p}^-(n)=\begin{cases}0, & n=0,\\ n-1, & n>0.\end{cases}$$

$\mathrm{p}^-$ 是递归的，因为

$$\mathrm{p}^-(0)=0\ (\text{定数}),$$

$$\mathrm{p}^-(n+1)=n=\mathrm{p}_1^2(n,\mathrm{p}^-(n)).$$

5° 截差函数 $\dot{-}$ 的定义式是

$$n_1 \dot{-} n_2=\begin{cases} n_1-n_2, & n_1 \geqslant n_2, \\ 0, & n_1<n_2. \end{cases}$$

截差函数是递归的，因为

$$n_1 \dot{-} 0=n_1=\mathrm{p}_1^1(n_1),$$

$$n_1 \dot{-}(n+1)=\mathrm{p}^-(n_1 \dot{-} n)=\mathrm{p}^-(\mathrm{p}_3^3(n_1,n,n_1 \dot{-} n)).$$

有了截差函数，以后就可以把前邻函数写成

$$\mathrm{p}^-(n)=n \dot{-} 1.$$

6° 一元函数 sg 的定义式是

$$\mathrm{sg}(n)=\begin{cases} 1, & n>0, \\ 0, & n=0. \end{cases}$$

sg 是递归的，因为

$$\mathrm{sg}(0)=0\ (\text{定数}),$$

$$\mathrm{sg}(n+1)=1=\mathrm{c}_1(n,\mathrm{sg}(n)).$$

其中函数 $\mathrm{c}_1$ 见 1°.

7° 一元函数 $\overline{\mathrm{sg}}$ 的定义式是

$$\overline{\mathrm{sg}}(n)=\begin{cases} 0, & n>0, \\ 1, & n=0. \end{cases}$$

$\overline{\mathrm{sg}}$ 是递归函数，因为

$$\overline{\mathrm{sg}}(n)=1 \dot{-} \mathrm{sg}(n).$$

sg 和 $\overline{\mathrm{sg}}$ 的函数值是 0 或 1，常用于构作集合和关系的特征函数.

在继续列举新的递归函数之前，先建立一个命题，利用它常可使递归描述更便于进行.

**命题 1** 由 $k$ 元递归函数 $f$ 用下式定义出的 $l$ 元函数 $g$ 也是递归的:

$$g(n_1,\cdots,n_l)=f(n_{m_1},\cdots,n_{m_k}),$$

其中对每个 $i=1,\cdots,k$, 有 $1 \leqslant m_i \leqslant l$.

**证** $g$ 可如下复合而成:

$$g(n_1,\cdots,n_l)=f(\mathrm{p}_{m_1}^l(n_1,\cdots,n_l),\cdots,\mathrm{p}_{m_k}^l(n_1,\cdots,n_l)),$$

故 $g$ 也是递归函数. □

命题 1 可用来“减元”. 例如，由已知的三元递归函数 $f$ 可如下生成二元函数 $u, g$ 和 $h$:

$$u(n_1, n_2) = f(n_1, n_2, n_2),$$

$$g(n_1, n_2) = f(n_1, n_1, n_2),$$

$$h(n_1, n_2) = f(n_2, n_1, n_2).$$

也可由 $f$ 生成一元函数 $r$:

$$r(n) = f(n, n, n).$$

根据命题 1，$u$, $g$, $h$, $r$ 也都是递归的.

还可用命题 1 来交换变元次序或“增元”. 例如由已知的三元递归函数 $f$ 可得三元递归函数 $g$ 和四元递归函数 $h$:

$$g(n_1, n_2, n_3) = f(n_3, n_2, n_1),$$

$$h(n_1, n_2, n_3, n_4) = f(n_3, n_1, n_4).$$

下面继续列举一些常用递归函数.

8° 绝对差 $\ddot{-}$ 的定义式是

$$n_1 \ddot{-} n_2 = |n_1 - n_2|.$$

绝对差是二元递归函数，因为

$$n_1 \ddot{-} n_2 = (n_1 \dot{-} n_2) + (n_2 \dot{-} n_1).$$

9° min 与 max ($k$元, $k > 1$) 的定义是

$\min(n_1, \cdots, n_k) =$ $n_1, \cdots, n_k$ 中的最小数，

$\max(n_1, \cdots, n_k) =$ $n_1, \cdots, n_k$ 中的最大数.

现对 $k$ 归纳证明 min 的递归性.

$k = 2$ 时，$\min(n_1, n_2) = n_1 \dot{-} (n_1 \dot{-} n_2)$.

$k > 2$ 时，$\min(n_1, \cdots, n_k) = \min(\min(n_1, \cdots, n_{k-1}), n_k)$.

max 的情形是类似的.

10° 指数函数 $n_1^{n_2}$ ($0^0$ 规定为 0)

$$n_1^{\,0} = \mathrm{sg}(n_1),$$

$$n_1^{n+1} = n_1^n \times n_1.$$

11° 余数函数 rem 的定义式是

$$\mathrm{rem}(n_1, n_2) = \begin{cases} \text{用 } n_1 \text{ 除 } n_2 \text{ 所得余数}, & n_1 > 0, \\ 0, & n_1 = 0. \end{cases}$$

先将 $\mathrm{rem}(n_1,n+1)$ 用 $\mathrm{rem}(n_1,n)$ 表示出来:

$$\mathrm{rem}(n_1,n+1)=\begin{cases}\mathrm{rem}(n_1,n)+1, & \mathrm{rem}(n_1,n)+1<n_1,\\ 0, & \mathrm{rem}(n_1,n)+1\geqslant n_1.\end{cases}$$

由此即可证明 rem 的递归性:

$$\mathrm{rem}(n_1,0)=0,$$

$$\mathrm{rem}(n_1,n+1)=(\mathrm{rem}(n_1,n)+1)\,\mathrm{sg}(n_1\dot{-}(\mathrm{rem}(n_1,n)+1)).$$

下面的符号 $\Sigma$ 与 $\Pi$ 分别表示求和与求积.

12° 设 $f$ 是 $k+1$ 元递归函数. 由 $f$ 可定义新的 $k$ 元函数 $g$ 和 $k+1$ 元函数 $h$:

$$g(n_1,\cdots,n_k)=\sum_{i\leqslant n_k}f(n_1,\cdots,n_k,i),$$

$$h(n_1,\cdots,n_{k+1})=\sum_{i\leqslant n_{k+1}}f(n_1,\cdots,n_k,i).$$

$g$ 和 $h$ 都是递归的，因为

$$\begin{aligned}&g(n_1,\cdots,n_k)=h(n_1,\cdots,n_k,n_k),\\&h(n_1,\cdots,n_k,0)=f(n_1,\cdots,n_k,0),\\&h(n_1,\cdots,n_k,n+1)=\sum_{i\leqslant n}f(n_1,\cdots,n_k,i)+f(n_1,\cdots,n_k,n+1)\\&\qquad=h(n_1,\cdots,n_k,n)+f(n_1,\cdots,n_k,n+1).\end{aligned}$$

13° 设 $f$ 是 $k+1$ 元递归函数. 定义新的 $k$ 元函数 $g$ 和 $k+1$ 元函数 $h$:

$$g(n_1,\cdots,n_k)=\sum_{i<n_k}f(n_1,\cdots,n_k,i),$$

$$h(n_1,\cdots,n_{k+1})=\sum_{i<n_{k+1}}f(n_1,\cdots,n_k,i).$$

当 $n_k=0$ 时，规定 $g$ 的函数值为零；当 $n_{k+1}=0$ 时，规定 $h$ 的函数值为零.

$g$ 和 $h$ 都是递归的，因为

$$g(n_1,\cdots,n_k)=h(n_1,\cdots,n_k,n_k),$$

$$h(n_1,\cdots,n_k,0)=0,$$

$$h(n_1,\cdots,n_k,n+1)=h(n_1,\cdots,n_k,n)+f(n_1,\cdots,n_k,n).$$

14° 设 $f$ 是 $k+1$ 元递归函数. 定义新的 $k$ 元函数 $g_1$, $g_2$ 和 $k+1$ 元函数 $h_1$, $h_2$:

$$g_1(n_1,\cdots n_k)=\prod_{i\leqslant n_k}f(n_1,\cdots,n_k,i),$$

$$h_1(n_1,\cdots,n_{k+1})=\prod_{i\leqslant n_{k+1}}f(n_1,\cdots,n_k,i),$$

$$g_2(n_1,\cdots,n_k)=\prod_{i<n_k}f(n_1,\cdots,n_k,i),$$

$$h_2(n_1,\cdots,n_{k+1})=\prod_{i<n_{k+1}}f(n_1,\cdots,n_k,i),$$

$n_k = 0$ 时，规定 $g_2$ 的函数值为 1； $n_{k+1} = 0$ 时，规定 $h_2$ 的函数值为 1.

这四个新函数都是递归的. 证明与 12°, 13° 类似.

15° 设 $g$ 是 $k+1$ 元递归函数. 作 $k$ 元函数 $f$：

$$f(n_1, \cdots, n_k) = \min\{x \mid g(n_1, \cdots, n_k, x) = 1\}.$$

$f$ 是递归的 (证明留作练习). 此时仍称 $f$ 由 $g$ 使用 $\mu$ 算子得来，并写

$$f(n_1, \cdots, n_k) = \mu x[g(n_1, \cdots, n_k, x) = 1].$$

还有一些要用到的递归函数，后面在需要的时候随时引入.

## 练习 27

1. 已知二元函数 $f$ 是递归函数. 试证由 $f$ 定义出的以下函数 (一元函数 $g$, 二元函数 $h$, 三元函数 $r$) 也是递归的.

$$g(n) = f(n, n),$$
$$h(n_1, n_2) = f(n_2, n_1),$$
$$r(n_1, n_2, n_3) = f(n_3, n_1).$$

2. 证明以下函数是递归的.

(1) $f(n) = n^2$.

(2) $f(n_1, n_2) = n_2^2$.

(3) $\max(n_1, n_2)$.

(4) $f(n) = n!$.

(5) $h(n) = f(n)^{g(n)}$, 已知 $f$ 和 $g$ 是一元递归函数.

(6) 对任一定数 $k$,

$$f_k(n) = \begin{cases} 1, & n = k, \\ 0, & n \neq k. \end{cases}$$

(7) 商函数

$$q(n_1, n_2) = \begin{cases} \text{用 } n_1 \text{ 除 } n_2 \text{ 所得商}, & n_1 > 0, \\ 0, & n_1 = 0. \end{cases}$$

(8) $h(n_1, n_2) = \sum\limits_{i<n_1} g(n_1, n_2, i)$, 已知 $g$ 是三元递归函数.

(9) 本段 14° 中的 $g_1$, $h_1$, $h_2$.

(10) 本段 15° 中的 $f$.

3. 证明所有递归函数构成的集是可数集.

### 3.4.2 递归关系和递归集

先回忆 $\mathbf{N}$ 上 $k$ 元关系 $R$ 的特征函数 $C_R$ 的定义式:

$$C_R(n_1,\cdots,n_k)=\begin{cases}1, & (n_1,\cdots,n_k)\in R,\\ 0, & (n_1,\cdots,n_k)\notin R.\end{cases}$$

**定义 1 (递归关系与递归集)** 若特征函数 $C_R$ 是递归函数，则关系 $R$ 叫做递归关系. 一元递归关系叫做 $\mathbf{N}$ 的递归子集，简称为递归集.

**例 1** 二元关系 $\leqslant,=,<$ 都是递归关系. 事实上

$$C_{\leqslant}(n_1,n_2)=\overline{\mathrm{sg}}(n_1\dot{-}n_2),$$

$$C_{=}(n_1,n_2)=\overline{\mathrm{sg}}(n_1\ddot{-}n_2),$$

$$C_{<}(n_1,n_2)=\mathrm{sg}(n_2\dot{-}n_1).$$

**命题 1** 1° 若 $R$ 是 $k$ 元递归关系，则 $\overline{R}$ 也是 $k$ 元递归关系，这里的 $\overline{R}$ 是 $R$ 的余集: $\overline{R}=\mathbf{N}^k-R$.

2° 若 $R_1,R_2$ 都是 $k$ 元递归关系，则 $R_1\cup R_2$ 和 $R_1\cap R_2$ 也都是 $k$ 元递归关系.

**证** $C_{\overline{R}}(n_1,\cdots,n_k)=1-C_R(n_1,\cdots,n_k)$,

$C_{R_1\cup R_2}(n_1,\cdots,n_k)=\mathrm{sg}(C_{R_1}(n_1,\cdots,n_k)+C_{R_2}(n_1,\cdots,n_k))$,

$C_{R_1\cap R_2}(n_1,\cdots,n_k)=C_{R_1}(n_1,\cdots,n_k)\times C_{R_2}(n_1,\cdots,n_k)$. □

**例 2** 设 $R$ 是 $k+1$ 元递归关系 $(k>0)$. 用 $R$ 作一新的 $k$ 元关系:

$$Q=\{(n_1,\cdots,n_k)\mid \text{存在 } x<n_k \text{ 使 } (n_1,\cdots,n_k,x)\in R\}.$$

$Q$ 也是递归关系，因为

$$C_Q(n_1,\cdots,n_k)=\mathrm{sg}\Big(\sum_{x<n_k}C_R(n_1,\cdots,n_k,x)\Big).$$

这里要利用 3.4.1 小节中的 13°.

**命题 2** $\mathbf{N}$，$\varnothing$, 独元集 $\{a\}$, 有限集 $\{a_1,\cdots,a_n\}$ 都是递归集. $(a,a_1,\cdots,a_n\in\mathbf{N})$

**证** $C_{\mathbf{N}}(n)=1$,

$C_{\varnothing}(n)=0$,

$C_{\{a\}}(n)=C_{=}(n,a)$,

$\{a_1,\cdots,a_n\}=\{a_1\}\cup\cdots\cup\{a_n\}$. □

**例 3** 二元关系

$$\mathrm{Divi}=\{(n_1,n_2)\mid n_1=0 \text{ 或 } n_1 \text{ 能整除 } n_2\}$$

是递归关系. 事实上，

$$C_{\mathrm{Divi}}(n_1,n_2)=\overline{\mathrm{sg}}(\mathrm{rem}(n_1,n_2)).$$

**例 4** 全体素数构成的集记作 Prm，它是递归集. 理由如下:

检查 $n$ 是不是素数，可以检查在不大于 $n$ 的数中有多少个是 $n$ 的因子 (包括 0 在内). $n>1$ 时，若因子多于 3 个，则 $n$ 不是素数. 所以有

$$C_{\mathrm{Prm}}(n)=\Big(4\dot{-}\sum_{i\leqslant n}C_{\mathrm{Divi}}(i,n)\Big)\times \mathrm{sg}(n\dot{-}1).$$

**例 5** 设 $p(n)=$ 第 $n$ 个素数 ($p(0)=2,p(1)=3,p(2)=5,\cdots$). $p$ 是一元递归函数，因为

$$p(0)=2,$$

$$p(n+1)=\mu x[C_{<}(p(n),x)\times C_{\mathrm{Prm}}(x)=1].$$

第二式的意思是: $p(n+1)$ 是比 $p(n)$ 大的最小素数.

以后常把 $p(n)$ 简写成 $p_n$.

## 练习 28

1. 证明 $\mathbf{N}_1=\{0,2,4,6,\cdots\}$ 和 $\mathbf{N}_2=\{3,4,5,6,\cdots\}$ 是递归集.

2. 设 $A,B$ 是递归集，证明 $A\times B$ 是二元递归关系.

3. 设 $A$ 是非递归集，证明 $A\times A$ 是非递归的二元关系.

4. 证明 $G$ 是递归集，这里

$$G=\{n\mid n\text{ 为奇数，或 }n\leqslant 2,\text{或 }n\text{ 等于二素数之和}\}.$$

5. 设 $k$ 元关系 $R_1,\cdots,R_l$ 都是递归的，且满足 $R_1\cup\cdots\cup R_l=\mathbf{N}^k$ 和 $R_i\cap R_j=\varnothing\ (i\neq j)$. (这时说 $R_1,\cdots,R_l$ 给出了 $\mathbf{N}^k$ 的一个递归剖分.) 又设 $k$ 元函数 $g_1,\cdots,g_l$ 都是递归的，且

$$f(n_1,\cdots,n_k)=\begin{cases}g_1(n_1,\cdots,n_k), & (n_1,\cdots,n_k)\in R_1;\\ \cdots\cdots & \\ g_l(n_1,\cdots,n_k), & (n_1,\cdots,n_k)\in R_l.\end{cases}$$

求证 $f$ 是递归函数.

6. 设 $A$ 与 $A_1$ 是递归集，且 $A=A_1\cup A_2$. $A_2$ 一定是递归集吗?

7. 不用 $\mu$ 算子证明例 5 中函数 $p$ 的递归性.

# 3.5 递归函数的可表示性

现在回到数论函数和 $K_{\mathbf{N}}$ 的公式之间关系的讨论. Gödel 不完备性定理的证明中,“递归函数在 $K_{\mathbf{N}}$ 中皆可表示”这一结论起着重要作用.

先引入三个记号: REP，REC 和 REC*.

REP = 在 $K_{\mathbf{N}}$ 中可表示的函数的全体构成的集.

REC = 递归函数的全体构成的集.

REC* 的定义与 REC 的类似，但稍有不同:

**定义 1 (函数集 REC*)** REC* 是指 $+, \times, \mathrm{p}_i^k, C_{\leqslant}$ 这四种函数以及由它们经有限次使用复合（规则 I）和 $\mu$ 算子（规则 III）得到的函数的全体所构成的函数集.

回忆 3.4.1 小节的 2°, 3° 和 3.4.2 小节的例 1，立即可知下面的命题 1 成立:

**命题 1** REC* ⊆ REC.

再回忆 3.3 节中关于可表示性所得到的结果 (3.3.1 小节命题 2 和命题 4，3.3.2 小节定理 1 和定理 2)，又立即可知下面的命题 2 成立:

**命题 2** REC* ⊆ REP.

本节的任务是证明 REC ⊆ REC*. 这个事实与命题 1 结合，便说明定义 1 是递归函数的另一等价定义；与命题 2 结合便得到了递归函数的可表示性.

**引理 1** 函数 z，s，sg，$\overline{\mathrm{sg}}, C_{=}, \dot{-}$, rem 都是 REC* 的成员.

**证** 1° 注意 $C_{\leqslant}(n,n)$ 恒为 1，于是

$$\mathrm{s}(n)=n+1=n+C_{\leqslant}(n,n)=\mathrm{p}_1^1(n)+C_{\leqslant}(\mathrm{p}_1^1(n),\mathrm{p}_1^1(n)).$$

2° $\mathrm{z}(n)=C_{\leqslant}(n+1,n)=C_{\leqslant}(\mathrm{s}(n),\mathrm{p}_1^1(n))$.

3° $\mathrm{sg}(n)=C_{\leqslant}(1,n)=C_{\leqslant}(\mathrm{s}(\mathrm{z}(n)),\mathrm{p}_1^1(n))$.

4° $\overline{\mathrm{sg}}(n)=C_{\leqslant}(\mathrm{p}_1^1(n),\mathrm{z}(n))$.

5° $C_{=}(n_1,n_2)=C_{\leqslant}(n_1,n_2)\times C_{\leqslant}(n_2,n_1)$

$$=C_{\leqslant}(n_1,n_2)\times C_{\leqslant}(\mathrm{p}_2^2(n_1,n_2),(\mathrm{p}_1^2(n_1,n_2)).$$

6° 注意当 $n_1\leqslant n_2$ 时，对任意 $x$ 都有

$$C_{\leqslant}(n_1,n_2+x)=1;$$

当 $n_1>n_2$ 时，

$$C_{\leqslant}(n_1,n_2+x)=\begin{cases}1, & x\geqslant n_1-n_2,\\ 0, & x<n_1-n_2.\end{cases}$$

于是

$$\begin{aligned}n_1\dot{-}n_2&=\mu x[C_{\leqslant}(n_1,n_2+x)=1]\\&=\mu x[\overline{\mathrm{sg}}(C_{\leqslant}(n_1,n_2+x))=0]\\&=\mu x[\overline{\mathrm{sg}}(C_{\leqslant}(\mathrm{p}_1^3(n_1,n_2,x),\mathrm{p}_2^3(n_1,n_2,x)+\mathrm{p}_3^3(n_1,n_2,x)))=0].\end{aligned}$$

7° $\mathrm{rem}(n_1,n_2)=$

$$\mathrm{sg}(n_1)\times(n_2\dot{-}(n_1\times(\mu x[\mathrm{sg}(n_1)\times C_{\leqslant}(n_1\times x,n_2)=0]\dot{-}1))).$$

详细地写，上式方括号内的 $n_1,n_2$ 与 $x$ 应分别写成 $\mathrm{p}_1^3(n_1,n_2,x),\mathrm{p}_2^3(n_1,n_2,x)$ 与 $\mathrm{p}_3^3(n_1,n_2,x)$( 与 6° 中类似 )；方括号外的 $n_1,n_2$ 与 1 应分别写成 $\mathrm{p}_1^2(n_1,n_2),\mathrm{p}_2^2(n_1,n_2)$

与 $s(z(p_1^2(n_1,n_2)))$. 方括号内加上因子 $sg(n_1)$ 是为了当 $n_1=0$ 时使根存在性条件得到满足. □

现在已经知道递归函数定义中的三种基本函数 $z, s, p_i^k$ 都是 $REC^*$ 的成员. 为了完成 $REC \subseteq REC^*$ 的证明，剩下只要证明一件事: $REC^*$ 对递归规则 II 封闭，即由 $REC^*$ 中的函数 $g,h$ 利用规则 II 得到的函数 $f$ 仍在 $REC^*$ 中. 为证明这一点，要用到孙子定理 (即下面的引理 3，它常被称为中国剩余定理).

**引理 2** 若正整数 $m$ 与 $n$ 互素，则存在整数 $s$ 和 $t$ 使 $sm+tn=1$.

**证** 对给定的 $m,n$ 作一集 $A$:

$$A=\{u \mid 存在整数\ s\ 和\ t\ 使\ u=sm+tn, 且\ u>0\}.$$

$A$ 是自然数的非空集 (例如 $m+n$ 是 $A$ 的成员)，故必有最小值. 设 $A$ 中的最小值是 $u_0=s_0m+t_0n$, 其中 $s_0,t_0$ 是整数. 再设

$$m=qu_0+r, \quad 0\leqslant r<u_0.$$

这时有

$$\begin{aligned} r &= m-qu_0 \\ &= m-q(s_0m+t_0n) \\ &= (1-qs_0)m+(-qt_0)n. \end{aligned}$$

如果 $r>0$, 那么上式说明 $r$ 也是集 $A$ 的成员，且因 $r<u_0$ 而与 $u_0$ 的最小性矛盾，所以只有 $r=0$ 才行. 也就是说，$u_0$ 必能整除 $m$.

同理，$u_0$ 也必能整除 $n$. 又因 $m$ 与 $n$ 互素，故 $u_0=1$, 即 $s_0m+t_0n=1$. □

**引理 3 (孙子定理)** 已知自然数 $a_1,\cdots,a_k$. 设另有自然数 $n_1,\cdots,n_k$ 两两互素，且 $n_1>a_1,\cdots,n_k>a_k$, 则存在无限多个自然数 $m$ 使

$$\mathrm{rem}(n_i,m)=a_i, \quad i=1,\cdots,k.$$

**证** 令 $z_i=n_1n_2\cdots n_k/n_i$. $z_i$ 就是 $n_1,\cdots,n_k$ 中除去 $n_i$ 后的各数之积. 因 $n_i$ 与 $n_1,\cdots,n_k$ 中其他各数互素，故 $n_i$ 与 $z_i$ 互素. 由引理 2 知，存在整数 $s_i,t_i$ 使

$$s_iz_i+t_in_i=1, \quad i=1,\cdots,k.$$

由此可得

$$a_is_iz_i+a_it_in_i=a_i,$$

$$a_is_iz_i=(-a_it_i)n_i+a_i, \quad 0\leqslant a_i<n_i,$$

$$(*) \qquad \mathrm{rem}(n_i,a_is_iz_i)=a_i, \quad i=1,\cdots,k.$$

现取

$$m=a_1s_1z_1+\cdots+a_ks_kz_k+ln_1\cdots n_k,$$

其中 $l$ 可取为任意使 $m>0$ 的自然数，有无限多个. $m$ 即为所求，因为 (注意 $z_i$ 的定义及 (*) 式) 有

$$\mathrm{rem}(n_i,m)=a_i,\quad i=1,\cdots,k. \qquad \square$$

由孙子定理便可得到下面的引理 4.

**引理 4** 对于给定的 $a_1,\cdots,a_k\in\mathbf{N}$, 一定存在 $n,m\in\mathbf{N}$ 使 $n\leqslant m$, 且使

$$\mathrm{rem}(1+in,m)=a_i,\quad i=1,\cdots,k.$$

**证** 令 $b=\max\{a_1,\cdots,a_k,k\}$ 并取 $n=b!$. 取定 $n$ 以后，因

$$1+in>a_i\geqslant 0,\quad i=1,\cdots,k,$$

由引理 3 知一定存在 $m\geqslant n$ 使

$$\mathrm{rem}(1+in,m)=a_i,\quad i=1,\cdots,k.$$

但在用引理 3 时，需要验证满足 "$1+n,\cdots,1+kn$ 这 $k$ 个数两两互素" 这一条件.

反设某个 $1+in$ 和某个 $1+jn$ $(1\leqslant i<j\leqslant k)$ 有素公因子 $p$. 这时 $p$ 能整除 $(j-i)n$. 但因

$$0<j-i<k\leqslant b\leqslant b!=n,$$

这说明 $j-i$ 是 $b!$ 即 $n$ 的因子，进而导致 $p$ 能整除 $n$. 已假设 $p$ 能整除 $1+in$, 这只有 $p=1$ 才行，与 $p$ 是素数矛盾. $\square$

下面建立本节的主要定理，在这个过程中，除了要用到引理 4，还要注意引理 1 中的结论不止一次用到.

**定理 1** 设 $k+1$ 元函数 $f$ 满足

$$f(n_1,\cdots,n_k,0)=g(n_1,\cdots,n_k),$$
$$f(n_1,\cdots,n_k,n+1)=h(n_1,\cdots,n_k,n,f(n_1,\cdots,n_k,n)).$$

若其中函数 $g,h\in\mathrm{REC}^*$, 则 $f\in\mathrm{REC}^*$.

**证** 和 3.3.2 小节一样，也把 $n_1,\cdots,n_k$ 简记成 $\alpha$. 于是函数 $f$ 所满足的已知条件可写成

(1) $f(\alpha,0)=g(\alpha)$,

(2) $f(\alpha,n+1)=h(\alpha,n,f(\alpha,n))$.

作出三个新函数 $F_1(k+2元)$, $F_2(k+3元)$ 和 $F_3(k+3元)$, 方法是

$$F_1(\alpha,x,y)=C_=(\mathrm{rem}(1+y,x),g(\alpha)),$$

$$F_2(\alpha,x,y,i)=C_=(\mathrm{rem}(1+(i+2)y,x),\ h(\alpha,i,\mathrm{rem}(1+(i+1)y,x))),$$

$$F_3(\alpha,n,x,y)=F_1(\alpha,x,y)\times C_\leqslant(n,\mu i[F_2(\alpha,x,y,i)\times C_\leqslant(i,n)=0]).$$

$F_3$ 的定义使用了 $\mu$ 算子. 其中方括号内有因子 $C_\leqslant(i,n)$, 这是为了保证根存在性条件肯定得到满足，从而使 $F_3$ 是个全函数. (使方括号内等式成立的 $i$ 总是存在

的，例如取 $i=n+1$.)

根据引理 1，$F_1,F_2,F_3$ 的定义式中所涉及的函数 $C_=$, rem 等都是 REC* 的成员，又已知 $g,h\in \mathrm{REC}^*$, 所以 $F_1,F_2,F_3\in\mathrm{REC}^*$.

这三个函数的作法使以下三个结论是等价的. 这三个结论是:

(3) $F_3(\alpha,n,x,y)=1$,

(4) $\begin{cases}\mathrm{rem}(1+y,x)=g(\alpha),\\ \mathrm{rem}(1+(i+2)y,x)=h(\alpha,i,\mathrm{rem}(1+(i+1)y,x)),\ i=0,\cdots,n-1,\end{cases}$

(5) $\mathrm{rem}(1+(i+1)y,x)=f(\alpha,i),\ i=0,\cdots,n.$

现在来证明 (3)，(4)，(5) 的等价性.

(3) $\Leftrightarrow$ (4) :

$$\begin{aligned}(3)\ &\Leftrightarrow\ F_1(\alpha,x,y)=1\ \text{且}\ C_\leqslant(n,\mu i[F_2(\alpha,x,y,i)\times C_\leqslant(i,n)=0])=1\\ &\Leftrightarrow\ C_=(\mathrm{rem}(1+y,x),g(\alpha))=1\ \text{且}\ n\leqslant \mu i[F_2(\alpha,x,y,i)\times C_\leqslant(i,n)=0]\\ &\Leftrightarrow\ \mathrm{rem}(1+y,x)=g(\alpha)\ \text{且当}\ i<n\ \text{时}\ F_2(\alpha,x,y,i)=1\\ &\Leftrightarrow\ (4).\end{aligned}$$

(5) $\Rightarrow$ (4) :

(5) 中 $i=0$ 时，由 (1) 便得 (4) 的第一式. 又

$$\begin{aligned}\mathrm{rem}(1+(i+2)y,x)&=f(\alpha,i+1) &&(\text{由(5)})\\ &=h(\alpha,i,f(\alpha,i)) &&(\text{由(2)})\\ &=h(\alpha,i,\mathrm{rem}(1+(i+1)y,x)),i=0,\cdots,n-1, &&(\text{由(5)})\end{aligned}$$

这就得到 (4) 的其他各式.

(4) $\Rightarrow$ (5) :

$$\begin{aligned}\mathrm{rem}(1+y,x)&=g(\alpha)=f(\alpha,0) &&(\text{(4) 的第一式及 (1)})\\ \mathrm{rem}(1+2y,x)&=h(\alpha,0,\mathrm{rem}(1+y,x)) &&(\text{(4)的第二式},i=0)\\ &=h(\alpha,0,f(\alpha,0)) &&(\text{已得的结果代入})\\ &=f(\alpha,1) &&(\text{由(2)})\\ &\cdots\cdots\\ \mathrm{rem}(1+(n+1)y,x)&=h(\alpha,n-1,\mathrm{rem}(1+ny,x)) &&(\text{(4)的第二式},i=n-1)\\ &=h(\alpha,n-1,f(\alpha,n-1)) &&(\text{已得的结果代入})\\ &=f(\alpha,n) &&(\text{由(2)})\end{aligned}$$

至此证明了 (3)，(4)，(5) 的等价性.

利用 $F_3$ 再作一个新函数 $F_4$ ($k+2$元) :

$$F_4(\alpha,n,x)=C_\leqslant(\mu y[\mathrm{sg}(F_3(\alpha,n,x,y)+C_\leqslant(x+1,y))=1],x),$$

式中方括号内的 $C_\leqslant(x+1,y)$ 使根的存在性条件肯定满足. $F_4\in\mathrm{REC}^*$, 且 $F_4$ 的作法使下面的结论 (6) 和结论 (7) 是等价的. 它们是:

(6) $F_4(\alpha,n,x)=1$,

(7) 存在 $y\leqslant x$ 使 $F_3(\alpha,n,x,y)=1$.

(6) 与 (7) 等价，是因为

$$\begin{aligned} F_4(\alpha,n,x,)=1 &\Leftrightarrow \mu y[\mathrm{sg}(F_3(\alpha,n,x,y)+C_{\leqslant}(x+1,y))=1]\leqslant x \\ &\Leftrightarrow \text{存在 } y\leqslant x \text{ 使 } \mathrm{sg}(F_3(\alpha,n,x,y)+C_{\leqslant}(x+1,y))=1 \\ &\Leftrightarrow \text{存在 } y\leqslant x \text{ 使 } \mathrm{sg}(F_3(\alpha,n,x,y))=1 \\ &\Leftrightarrow (7).\ (\text{注意 } F_3 \text{ 的定义，} F_3 \text{ 的函数值只取 0 或 1.}) \end{aligned}$$

下面再用 $F_4$ 作一新的 $k+1$ 元函数 $F_5$ :

$$F_5(\alpha,n)=\mu x[F_4(\alpha,n,x)=1].$$

$F_5$ 是否对任意的 $\alpha,n$ 都有定义? 也就是问: 生成 $F_5$ 的 $\mu$ 算子的根存在性条件是否总能满足?

引理 4 回答了这个关键问题.

我们有以下结论:

任意给定 $\alpha,n$. 对 $f(\alpha,0),\cdots,f(\alpha,n)$ 这 $n+1$ 个自然数，一定存在自然数 $x$ 及 $y\leqslant x$ 使上页 (5) 成立;

(根据引理 4)

对任意给定的 $\alpha,n$, 存在 $x$ 及 $y\leqslant x$ 使 $F_3(\alpha,n,x,y)=1$;

((5) 与 (3) 等价)

对任意给定的 $\alpha,n$, 存在 $x$ 使 $F_4(\alpha,n,x)=1$.

((6) 与 (7) 等价)

得到的结论说明，$F_5$ 是定义好的全函数，且 $F_5\in \mathrm{REC}^*$.

按 $F_5$ 的定义式，自然有

$$F_4(\alpha,n,F_5(\alpha,n))=1.$$

此式意味着 (注意 (6) 与 (7) 等价):

$$\text{存在 } y\leqslant F_5(\alpha,n) \text{ 使 } F_3(\alpha,n,F_5(\alpha,n),y)=1.$$

这一事实保证了可以作出下面的全函数 $F_6$ ($k+1$元) :

$$F_6(\alpha,n)=\mu y[F_3(\alpha,n,F_5(\alpha,n),y)=1].$$

$F_6\in \mathrm{REC}^*$, 且 $F_6$ 的定义使下式自然成立:

$$F_3(\alpha,n,F_5(\alpha,n),F_6(\alpha,n))=1.$$

由此注意 (3) 与 (5) 的等价性，立即得

$$\mathrm{rem}(1+(i+1)F_6(\alpha,n),F_5(\alpha,n))=f(\alpha,i),\ i=0,\cdots,n.$$

特殊地取 $i=n$, 最后便得

$$\mathrm{rem}(1+(n+1)F_6(\alpha,n),F_5(\alpha,n))=f(\alpha,n).$$

这就是我们所需要的最后结论，它指出 $f\in \mathrm{REC}^*$. □

**推论 1** REC $\subseteq$ REC$^*$.

**证** 由引理 1 及定理 1 即得. □

**推论 2** REC = REC$^*$.

**证** 由推论 1 及命题 1 即得. □

**推论 3 (递归函数的可表示性)** REC $\subseteq$ REP.

**证** 由推论 1 及命题 2 即得. □

**推论 4** 递归关系在 $K_N$ 中可表示.

**证** $R$ 是递归关系 $\Rightarrow$ $C_R \in$ REC (递归关系的定义)

$\Rightarrow$ $C_R \in$ REP (推论 3)

$\Rightarrow$ $R$ 在 $K_N$ 中可表示 (3.3.1 小节命题 3)

□

## 练习 29

1. 直接证明 sg 的可表示性.
2. 给出一个可用来表示 $\dot{-}$ 的公式.

# 3.6 对$K_N$的递归分析

本节里要完成证明关于形式算术的 Gödel 不完备性定理的全部准备工作. 作为一个附带的结果 (见 3.6 附), 将得到结论: 所有在 $K_N$ 中可表示的函数都是递归的, 于是有

$$\text{REC} = \text{REP},$$

即, 递归性就是在 $K_N$ 中的可表示性.

## 3.6.1 唯一读法引理

对一种人工的形式语言 (例如形式算术 $K_N$), 我们通常都要提出一个要求——具有唯一读法. 拿 $K_N$ 具体地说, 从 $K_N$ 这种形式语言的字母表中任意取出的一些字母所构成的一个有限字母串, 是以下三种情况的哪一种——是项, 是公式, 或既非项又非公式——必须是唯一确定的. 如果是项, 是哪个层次的哪一种项; 如果是公式, 是哪个层次的哪一种公式, 这些也都必须是唯一确定的.

为了方便, 在下面进行的语法分析中, 把项与公式的写法由中置式全部改成前置式, 具体做法是: 把所有形为 $t_1 + t_2, t_1 \times t_2, t', t_1 \approx t_2$ 和 $p \to q$ 的项或公式分别写成

$+t_1t_2, \times t_1t_2, 't, \approx t_1t_2$ 和 $\to pq$.

**例 1** 采用前置式，$K_N$ 中的几种等词公理模式可写成:

(E1) $\approx tt$,

(E2) $\to\approx tu\approx 't'u$,

$\to\approx t_1u\approx +t_1t_2+ut_2$,

$\to\approx t_2u\approx +t_1t_2+t_1u$,

$\to\approx t_1u\approx \times t_1t_2\times ut_2$,

$\to\approx t_2u\approx \times t_1t_2\times t_1u$,

(E3) $\to\approx t_1u\to\approx t_1t_2\approx ut_2$,

$\to\approx t_2u\to\approx t_1t_2\approx t_1u$.

采用前置式，括号可从字母表中省去. 这时 $K_N$ 的字母表只需要以下字母或符号:

| | |
|---|---|
| $x_1, x_2, \cdots, x_n, \cdots$ | (个体变元) |
| $\bar{0}$ | (个体常元) |
| $'$, $+, \times$ | (函数词) |
| $\approx$ | (等词) |
| $\neg, \to, \forall$ | (逻辑符号) |

为了证明 $K_N$ 这种形式语言有唯一读法，类似于命题演算 (见 1. 2 节附 1)，先给 $K_N$ 的每个字母 $u$ 指定一个权重 $w(u)$:

$$w(x_i)=w(\bar{0})=1,$$
$$w(')=w(\neg)=0,$$
$$w(+)=w(\times)=w(\approx)=w(\to)=w(\forall)=-1.$$

再给每个字母串规定权重，把一个字母串的权重规定为组成该串的各字母权重之和:

$$w(u_1\cdots u_n)=w(u_1)+\cdots+w(u_n).$$

此外，空串的权重规定为 0.

**命题 1** 若字母串构成项或公式，则该串的权重为 1，而该串的真前段的权重不足 1. (字母串的真前段是指由该字母串去掉尾部最后一个或最后多个相邻字母后所剩下的字母串，它可以是空串.)

**证** 对构成项或公式的字母串的长度 $k$ 归纳.

$k=1$ 时，该串只可能是项 $x_i$ 或 $\bar{0}$, 按规定，权重为 1；该串的真前段只有空串，权重为 0.

$k>1$ 时，有七种可能: $'t, +t_1t_2, \times t_1t_2, \approx t_1t_2, \neg p, \to p_1p_2, \forall x_ip$. 这时要作归纳假设:

$t, t_1, t_2, p, p_1, p_2$ 的权重皆为 1，而它们的真前段的权重都不足 1.

$'t$ 的权重为 1，因 $w(')=0$; $'t$ 的真前段的权重就是 $t$ 的真前段的权重，不足 1. $\neg p$ 的情形与 $'t$ 类似.

$+t_1t_2$ 权重为 1，因 $w(+)=-1$. $+t_1t_2$ 的真前段的权重也都因 $w(+)=-1$ 而不足 1. $\times t_1t_2, \approx t_1t_2, \to p_1p_2$ 的情形与 $+t_1t_2$ 类似.

因 $w(\forall)=-1$ 而 $w(x_i)=1$, 故 $\forall x_i p$ 的情形与 $'t$ 和 $\neg p$ 类似. □

**命题 2 (唯一读法引理)**

(i) 一个项或一个公式的真前段不再是项或公式.

(ii) 若一字母串是由两个项或两个公式并接而成的，则并接的方式是唯一的.

**证** (i) 由命题 1 即得.

(ii) 假设一符号串由两个项并接而成: $t_1t_2$, 同时它又以不同的方式由另外两个项并接而成: $s_1s_2$. 这时项 $t_1$ 和 $s_1$ 有两种可能的关系: $t_1$ 是 $s_1$ 的真前段，或 $s_1$ 是 $t_1$ 的真前段. 因为 $t_1, s_1$ 都是项，所以这两种情形都不会发生，否则与 (i) 相矛盾. 关于两个公式的并接，讨论是相同的. □

为确定一个字母串是不是项或公式，先看它的权重是不是 1. 若是 1，且以 $'$, $+$ 或 $\times$ 开头，则该串可能是项; 若以 $\approx, \to, \neg$ 或 $\vee$ 开头，则该串可能是公式. 然后再分别对不同情况去掉开头字母后剩下的较短的字母串依序进行检查. 项或公式的任何尾部缩短或尾部加长都不再是项或公式 (加长后若是项或公式，则原串就不是). 在形为 $+t_1t_2, \times t_1t_2$, $\approx t_1t_2$ 的项或公式中，$t_1$ 和 $t_2$ 是唯一确定的; 在公式 $\to pq$ 中，前件 $p$ 和后件 $q$ 是唯一确定的. 这些都是说明了 $K_N$ 具有唯一读法.

## 练习 30

1. 把 (K1)~(K5) 及 (N1)~(N7) 全部改写成前置式.
2. 把以下前置式还原为通常中置式.

   1° $\approx \times \bar{0}\,\bar{0}\,\bar{0}$,

   2° $\approx + x_1\, x_2 + x_2\, x_1$,

   3° $\approx \times \times x_1\, x_2\, x_3 \times x_1 \times x_2\, x_3$,

   4° $\to \approx + x_1\, x_2\, x_2 \approx x_1\, \bar{0}$,

   5° $\to \neg \approx x_1\, \bar{0} \neg \forall x_2 \neg \approx + x_2{}' \bar{0}\, x_1$,

   6° $\to \neg \forall x_3 \neg \approx + x_3\, x_1\, x_2 \to \neg \forall x_4 \neg \approx + x_4\, x_2\, x_1 \approx x_1\, x_2$.
3. 举例说明命题 1 的逆命题不成立，权重为 1 的字母串可能既非项又非公式.

### 3.6.2 Gödel 数

现在我们要将 $K_N$ 算术化，具体地说，给 $K_N$ 这种形式语言进行编码 (或称配

数)，以便把有关 $K_N$ 这种形式系统的结论转化成数值形式，变成关于自然数的结论. 从算术到 $K_N$, 从 $K_N$ 到算术，再回到 $K_N$, 一些重要的结论就是在这样来回反复的研究中建立起来的.

配数的方法可以有很多种，下面使用其中的一种.

**1. 字母的 Gödel 数**

对每个字母 $u$ 都指定一个 Gödel 数 $g(u)$ 如下:

| $u$ | $'$ | $+$ | $\times$ | $\neg$ | $\to$ | $\forall$ | $\approx$ | $\bar{0}$ | $x_i$ |
|---|---|---|---|---|---|---|---|---|---|
| $g(u)$ | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 | 15+2$i$ |

不同的字母有不同的 Gödel 数，但都是奇数. 每个奇数都是某个字母的 Gödel 数.

**2. 字母串的 Gödel 数**

字母串 $u_0 u_1 \cdots u_k$ 的 Gödel 数规定为

$$g(u_0 u_1 \cdots u_k) = 2^{g(u_0)} 3^{g(u_1)} \cdots p_k^{g(u_k)}.$$

这样就把 Gödel 配数扩张到对任意非空字母串都有定义，且保持了单射性:

1° 字母串的 Gödel 数与字母的 Gödel 数不会相同，前者是偶数，后者是奇数;

2° 不同的字母串对应有不同的 Gödel 数 (这是因为自然数的素幂积分解式具有唯一性).

**例** $g(+x_3\bar{0}) = 2^3 3^{15+6} 5^{15}$,

$g(\bar{3}) = g(''' \bar{0}) = 2^1 3^1 5^1 7^{15}$,

$g(\neg \approx x_1' x_2) = 2^7 3^{13} 5^{17} 7^1 11^{19}$,

$g(+\forall \neg \approx) = 2^3 3^{11} 5^7 7^{13}$.

对任一偶数进行素幂积分解，便可确定它是不是某个字母串的 Gödel 数. 如果是字母串的 Gödel 数，这个字母串可能是项或公式，也可能是没有意义的字母串. 如上例中的 $+\forall\neg\approx$.

有一点值得注意，字母的 Gödel 数与该字母作为独元字母串的 Gödel 数是不同的，前者是奇数，后者是偶数. 例如，$x_3$ 作为字母的 Gödel 数是 21，而 $x_3$ 作为独元字母串的 Gödel 数是 $2^{21}$. 问题是: $x_3$ 何时作为单个字母，何时作为独元字母串? 在具体场合，这一点必须明确. 事实上，在后面所有具体场合，这一点都是明确的，不会产生混淆.

**3. 字母串的有限序列的 Gödel 数**

设 $s_0, s_1, \cdots, s_n$ 是字母串的一个有限序列. 现把 Gödel 配数 g 进一步扩张成对每个字母串有限序列都有定义:

$$g(s_0, s_1, \cdots, s_n) = 2^{g(s_0)} 3^{g(s_1)} \cdots p_n^{g(s_n)}.$$

这种扩张保持了单射性. 首先，素幂积展开的唯一性决定了不同的字母串有限序列有不同的 Gödel 数. 此外，字母串有限序列的 Gödel 数是偶数 (这使它有别于单个字母的 Gödel 数)，同时它的素幂积展开式中每个素数的指数也都是偶数，从而又使它有别于字母串的 Gödel 数.

同样要注意，一个公式作为字母串的 Gödel 数与该公式作为字母串的独元序列的 Gödel 数是不相同的. 例如，公式 $\approx x_1 x_1$ 作为字母串，Gödel 数是 $2^{13}3^{17}5^{17}$; 作为字母串的独元序列，Gödel 数是 $2^{2^{13}3^{17}5^{17}}$. 在后面的每个具体场合，每个公式以什么身份出现都是明确的.

这样，我们完成了对 Gödel 配数的规定. 按照这种配数法，给出了字母、字母串或字母串有限序列，便能确定地算出相应的 Gödel 数. 反过来，任给一个自然数，通过对它进行素幂积分解 (并利用字母的配数表) 便可确定它是不是 Gödel 数. 如果是，还可进一步具体地确定它是哪一种 Gödel 数——项的，公式的，公式的有限序列的，一串无意义字母的，或一列无意义字母串的.

## 练习 31

1. 写出以下项、公式或公式列的 Gödel 数 (先将项或公式改写成前置式).

   1° $x_i \times \overline{0}$.

   2° $x_1' \times (x_2 + x_3)$.

   3° $\forall x_1(x_1 \times \overline{0} \approx \overline{0})$.

   4° $x_2 \approx \overline{0} \to (x_1 \approx x_2 \to x_1 \approx \overline{0})$.

   5° $\exists x_3 (x_3 + x_1 \approx x_2')$.

   6° $x_2 \not\approx \overline{0}, x_1 \approx x_2, x_1 \not\approx \overline{0}$.

### 3.6.3 过程值递归

有了 Gödel 配数，我们可以使 $K_N$ 算术化，并可用递归论的工具来深入研究 $K_N$. 在这之前还要做下面一些准备工作.

前面已经讨论过 (见 3.4.2 小节例 3，例 4 和例 5) 二元递归关系 Divi:

$$\text{Divi} = \{(n_1, n_2) \mid n_1 = 0 \text{ 或 } n_1 \text{ 能整除 } n_2\},$$

一元递归关系 Prm (素数集) 和一元递归函数

$$p(n) = \text{第 } n \text{ 个素数}\ \ (p(n) \text{ 常用 } p_n \text{ 表示}).$$

由此出发，下面继续引进一些与研究 $K_N$ 的语法有关的递归函数.

**命题 1** 当 $n_1 > 1$ 时，设 $n_1 = 2^{e_0}3^{e_1}\cdots p_k^{e_k}$, 则下式定义的二元函数是递归的:

$$(n_1)_{n_2}=\begin{cases} e_{n_2}, & n_1>1, \\ 0, & n_1=0 \text{ 或 } 1. \end{cases}$$

($n_1>1$ 时，$(n_1)_{n_2}$ 就是 $n_1$ 的素幂积分解式中 $p_{n_2}$ 的指数.)

**证** 为了求 $(n_1)_{n_2}$ 的值，可以这样做: 依次用 $p_{n_2}^{0+1}, p_{n_2}^{1+1}, p_{n_2}^{2+1}, \cdots$ 去除 $n_1$, 若其中第一个不能整除 $n_1$ 的是 $p_{n_2}^{x+1}$, 则 $(n_1)_{n_2}=x$. 按照这个算法，我们有

$$(n_1)_{n_2}=\mu x[\operatorname{sg}(n_1)\times\overline{\operatorname{sg}}(\operatorname{rem}(p_{n_2}^{x+1},n_1))=0].$$

方括号中的因子 $\operatorname{sg}(n_1)$ 是用于照顾 $n_1=0$ 时的根存在性条件. □

**命题 2** 一元函数 lh 是递归的，这里 lh 的定义式是

$$\operatorname{lh}(n)=\begin{cases} 0, & n=0 \text{ 或 } 1, \\ n \text{ 的素幂积分解式中非零指数的个数}, & n>1. \end{cases}$$

(例如，当 $n=2^{e_0}3^{e_1}\cdots p_k^{e_k}$ 且 $e_0, e_1, \cdots, e_k$ 皆非零时，有 $\operatorname{lh}(n)=k+1$.)

**证** 逐一检查不比 $n$ 大的素数是否能整除 $n$, 并对能整除 $n$ 的素数进行计数:

$$\operatorname{lh}(n)=\sum_{x\leqslant n}(C_{\mathrm{Prm}}(x)\times C_{\mathrm{Divi}}(x,n)).$$ □

**推论 1** 二元并接函数 $*$ 是递归的，这里的函数 $*$ 由下式定义

$$n_1 * n_2 = n_1\times\prod_{x<\operatorname{lh}(n_2)} p_{\operatorname{lh}(n_1)+x}^{(n_2)_x}.$$

**证** 由命题 2 及 3.4.1 小节中的 14° 等可得其递归性. □

如果

$$n_1=2^{a_0}3^{a_1}\cdots p_k^{a_k},$$

$$n_2=2^{b_0}3^{b_1}\cdots p_l^{b_l},$$

且 $a_0, a_1, \cdots, a_k$ 皆非零，那么

$$n_1 * n_2 = 2^{a_0}3^{a_1}\cdots p_k^{a_k}p_{k+1}^{b_0}p_{k+2}^{b_1}\cdots p_{k+l+1}^{b_l}.$$

**例** 设

$$n_1=\mathrm{g}(\forall x_1 \neg \approx)=2^{11}3^{17}5^7 7^{13},$$
$$n_2=\mathrm{g}(\prime\, x_1\,\overline{0})=2^1 3^{17}5^{15},$$

则

$$n_1 * n_2 = 2^{11}3^{17}5^7 7^{13}11^1 13^{17}17^{15},$$

这个数就是字母串 $\forall x_1\neg\approx$ 和字母串 $\prime x_1\overline{0}$ 并接后所得字母串 $\forall x_1\neg\approx\prime x_1\overline{0}$ 的 Gödel 数.

回忆由 $k$ 元函数 $g$ 和 $k+2$ 元函数 $h$ 使用规则 II 生成 $f$ 的递归式:

$$f(\alpha,0)=g(\alpha),\quad (\alpha \text{ 是 } n_1,\cdots,n_k \text{ 的简写})$$

$$f(\alpha, n+1) = h(\alpha, n, f(\alpha, n)).$$

$f$ 在点 $(\alpha, n+1)$ 的值依赖于 $f$ 在点 $(\alpha, n)$ 的值.

下面在分析有关 $K_N$ 的性质时，常要遇到另一种性质的函数，它在点 $(\alpha, n+1)$ 的值不是仅依赖于它在点 $(\alpha, n)$ 的值，而是依赖于它在 $(\alpha, 0), \cdots, (\alpha, n-1), (\alpha, n)$ 这些点或这些点中某些点的值. 这时，关于它的递归性有下面的结论.

**命题 3 (过程值递归)** 设 $k+2$ 元函数 $h$ 是递归的，且 $k+1$ 元函数 $f$ 满足“过程值递归条件”:

$$f(n_1, \cdots, n_k, n_{k+1}) = h(n_1, \cdots, n_k, n_{k+1}, f^\sharp(n_1, \cdots, n_k, n_{k+1})),$$

其中

$$f^\sharp(n_1, \cdots, n_k, n_{k+1}) = \prod_{x<n_{k+1}} p_x^{f(n_1, \cdots, n_k, x)},$$

那么 $f$ 也是递归函数.

**证** 注意 3.4.1 小节中的 14° 中的规定,

$$f^\sharp(\alpha, n_{k+1}) = \begin{cases} 2^{f(\alpha,0)} \cdots p_{n_{k+1}-1}^{f(\alpha, n_{k+1}-1)}, & n_{k+1} > 0, \\ 1, & n_{k+1} = 0. \end{cases}$$

要证明 $f$ 是递归的，按 $f$ 所满足的过程值递归条件，只用证明 $f^\sharp$ 是递归函数就可以了.

事实上，我们有

$$\begin{aligned} &f^\sharp(\alpha, 0) = 1, \\ &f^\sharp(\alpha, n+1) = 2^{f(\alpha,0)} \cdots p_{n-1}^{f(\alpha,n-1)} \times p_n^{f(\alpha,n)} \\ &\qquad = f^\sharp(\alpha, n) \times p_n^{f(\alpha,n)} = f^\sharp(\alpha, n) \times p_n^{h(\alpha,n,f^\sharp(\alpha,n))}. \end{aligned}$$

这里是用的规则 II——一般的递归规则. □

作为命题 3 的特例，当 $f$ 为一元函数时，我们有

**推论 2 (一元过程值递归)** 设 $h$ 是二元递归函数，且一元函数 $f$ 满足过程值递归条件:

$$f(n) = h(n, f^\sharp(n)),$$

其中

$$f^\sharp(n) = 2^{f(0)} 3^{f(1)} \cdots p_{n-1}^{f(n-1)},$$

则 $f$ 也是递归函数.

关于 $f$ 和 $f^\sharp$ 的关系，根据 $f^\sharp$ 的定义式，当 $x < n_{k+1} (\neq 0)$ 时，自然有下面的结论 (♯):

(♯) $$f(n_1, \cdots, n_k, x) = (f^\sharp(n_1, \cdots, n_k, n_{k+1}))_x.$$

作为 (♯) 式的特例，当 $f$ 为一元函数且 $x < n$ 时，有

$$f(x) = (f^{\sharp}(n))_x.$$

## 练习 32

1. 对于并接函数 $*$, 结合律

$$(n_1 * n_2) * n_3 = n_1 * (n_2 * n_3)$$

是否成立?

2. 设 $H$ 是 $k+2$ 元递归关系. 若 $k+1$ 元关系 $R$ 满足

$$(n_1, \cdots, n_{k+1}) \in R \quad \Leftrightarrow \quad (n_1, \cdots, n_{k+1}, C_R^{\sharp}(n_1, \cdots, n_{k+1})) \in H,$$

则 $R$ 也是递归关系.

3. 证明 Fibonacci 函数 $f$ 是递归函数. $f$ 的定义式是

$$f(0) = 1, f(1) = 2,$$

$$f(n+2) = f(n) + f(n+1).$$

4. 证明函数 $g$ 的递归性，$g$ 的定义是

$$g(0) = 1, g(1) = 2, g(2) = 3,$$

$$g(n+3) = g(n) + g(n+1) + g(n+2).$$

### 3.6.4 $K_N$ 的一些递归性质

下面开始对 $K_N$ 的语法进行细致的递归分析，以完成证明 Gödel 不完备性定理的最后准备工作.

本段中，个体变元 $x_i$ 和个体常元 $\bar{0}$ 都作为项被视为独元字母串，而不被视为单个字母.

**命题 1** N 的以下子集是递归集.

1° VS = $\{2^{15+2k} \mid k \geqslant 1\}$, VS 就是所有个体变元 (作为独元字母串) 的 Gödel 数构成的集.

2° TM: 所有 $K_N$ 的项的 Gödel 数构成的集.

3° YF: 所有 $K_N$ 的原子公式的 Gödel 数构成的集.

4° FM: 所有 $K_N$ 的公式的 Gödel 数构成的集.

**证** 1° 把 VS 的定义改写成

$$n \in \mathrm{VS} \quad \Leftrightarrow \quad \exists k < n(k \geqslant 1 \wedge n = 2^{15+2k}).$$

上面右边的符号 ∃ 和 ∧ 在这里分别是“存在某个”和“并且”这两个中文用语的简

写，属于元语言. 以下出现的类似情形不再一一说明. 另外，本段以下出现的 $x,y,z$ 等不表示个体变元，而表示自然数.

VS 的特征函数是递归的:

$$C_{VS}(n) = \sum_{k<n}(C_{\geqslant}(k,1)\times C_{=}(n,2^{15+2k})).$$

2° 任给一个项，都恰为以下几种可能形式中的一种: $\bar{0}$, $x_i$, $'t$, $+t_1t_2$, $\times t_1t_2$, 其中 $t$, $t_1$, $t_2$ 分别属于比各自所在的项较低的层次. 我们有

$$n\in \mathrm{TM} \quad\Leftrightarrow\quad n=2^{15} \vee n\in \mathrm{VS} \vee \exists x<n(n=2^1*x \wedge x\in \mathrm{TM})$$
$$\vee\ \exists x<n\exists y<n((n=2^3*x*y \vee n=2^5*x*y)\wedge x\in \mathrm{TM}\wedge y\in \mathrm{TM}).$$

这里的右边出现了 $x\in \mathrm{TM}$ 和 $y\in \mathrm{TM}$, 但 $x,y<n$. 这时要考虑会涉及过程值递归.

按照上面对 $n\in \mathrm{TM}$ 的描述，可如下给出 TM 的特征函数 $C_{TM}$ 所满足的关系式:

$$C_{TM}(n) = C_{=}(n,2^{15})+C_{VS}(n)+\sum_{x<n}(C_{=}(n,2^1*x)\times C_{TM}(x))$$
$$+\sum_{n<n}\sum_{y<n}((C_{=}(n,2^3*x*y)+C_{=}(n,2^5*x*y))\times C_{TM}(x)\times C_{TM}(y)).$$

上式在把右边所有出现的 $C_{TM}(x), C_{TM}(y)$ 分别换成 $(C^{\sharp}_{TM}(n))_x$, $(C^{\sharp}_{TM}(n))_y$ (利用 3.6.3 小节 ($\sharp$) 式) 后，就成了 $C_{TM}$ 所满足的过程值递归条件，于是便可利用 3.6.3 小节命题 3 后的推论 2 断定 $C_{TM}$ 具有递归性.

3° 原子公式的结构比较简单，只有 $\approx t_1t_2$ 这样一种形式，故有

$$n\in \mathrm{YF} \quad\Leftrightarrow\quad \exists x<n\exists y<n(x\in \mathrm{TM}\wedge y\in \mathrm{TM}\wedge n=2^{13}*x*y).$$

这可翻译成 YF 的特征函数 $C_{YF}$ 的计算公式:

$$C_{YF}(n)=\sum_{x<n}\sum_{y<n}C_{TM}(x)\times C_{TM}(y)\times C_{=}(n,2^{13}*x*y),$$

这就由 TM 的递归性得到 YF 的递归性.

4° $K_N$ 的公式，除了原子公式，便具有 $\neg q, q\to r$ 和 $\forall x_i q$ 这三种形式中的一种 (其中 $q,r$ 属于较低的层次). 于是公式的 Gödel 数全体的集 FM 满足

$$n\in \mathrm{FM} \quad\Leftrightarrow\quad n\in \mathrm{YF}\vee \exists x<n(x\in \mathrm{FM}\wedge n=2^7*x)$$
$$\vee\exists x<n\exists y<n(x\in \mathrm{FM}\wedge y\in \mathrm{FM}\wedge n=2^9*x*y)$$
$$\vee\exists x<n\exists y<n(x\in \mathrm{VS}\wedge y\in \mathrm{FM}\wedge n=2^{11}*x*y),$$

这可翻译成

$$C_{FM}(n)=C_{YF}(n)+\sum_{x<n}C_{FM}(x)\times C_{=}(n,2^7*x)$$
$$+\sum_{x<n}\sum_{y<n}C_{FM}(x)\times C_{FM}(y)\times C_{=}(n,2^9*x*y)$$
$$+\sum_{x<n}\sum_{y<n}C_{VS}(x)\times C_{FM}(y)\times C_{=}(n,2^{11}*x*y).$$

把上式中 $C_{FM}(x), C_{FM}(y)$ 都分别换成 $(C^{\sharp}_{FM}(n))_x$ 和 $(C^{\sharp}_{FM}(n))_y$, 便得 $C_{FM}$ 所满足的过

程值递归条件，然后用 3.6.3 小节命题 3 后的推论 2 便可. □

分别对 $i=1,\cdots,5$ 把所有 ($K_i$) 型公理的 Gödel 数构成的集记为 $LA_i$.

**命题 2** $LA_1, LA_2, LA_3$ 是递归集.

**证** $n\in LA_1 \Leftrightarrow \exists x<n\exists y<n(x\in FM\wedge y\in FM\wedge n=2^9*x*2^9*y*x)$,

$$C_{LA_1}(n)=\sum_{x<n}\sum_{y<n}C_{FM}(x)\times C_{FM}(y)\times C_=(n,\ 2^9*x*2^9*y*x).$$

由 FM 的递归性可得 $LA_1$ 的递归性.

$LA_2$ 和 $LA_3$ 的情形是类似的. □

要证明 $LA_4$ 的 $LA_5$ 递归性，困难在于要设法递归地表示出这样的关系：在 Gödel 数为 $n_3$ 的项 $u(x_i)$ 或公式 $p(x_i)$ (以下简称为 "$n_3$ 项 $u(x_i)$" 或 "$n_3$ 公式 $p(x_i)$") 中，用 Gödel 数为 $n_2$ 的项 $t$ (简称为 "$n_2$ 项 $t$") 去替换 Gödel 数为 $n_1$ 的变元 $x_i$ (简称为 "$n_1$ 变元 $x_i$") 的所有自由出现所得结果 $u(t)$ 或 $p(t)$ 的 Gödel 数是 $n_4$.

下面就来讨论这样的关系. 它本应该是四元关系，但为了避免出现更复杂的 (涉及两个自然数变量的) 过程值递归，特采用这样的办法：令 $\gamma=2^{n_3}3^{n_4}\cdots$，于是 $(\gamma)_0=n_3,(\gamma)_1=n_4$. 这样就把对上述四元关系的研究转化为对一个三元关系的研究.

以后把变元在项中的出现都叫做自由出现.

**命题 3** 三元关系 SBS 是递归关系，这里 SBS 的定义是：

$(n_1,n_2,\gamma)\in SBS \Leftrightarrow n_1\in VS, n_2\in TM, (\gamma)_0\in TM\cup FM, (\gamma)_1$ 是用 $n_2$ 项去替换 $(\gamma)_0$ 项或 $(\gamma)_0$ 公式中的 $n_1$ 变元的全部自由出现所得结果的 Gödel 数.

**证** 为了证明 SBS 的递归性，首先分析一下用项 $t$ 去替换项 $u(x_i)$ 中或公式 $p(x_i)$ 中所有自由的 $x_i$, 会有哪些可能的类型.

**类型 1** (最简型) $u(x_i)=x_i$, 此时 $u(t)=t$.

**类型 2** (确定不变型)

(i) $u(x_i)=\bar{0}$ 或 $x_j$($\neq x_i$, 即$x_i$不在$u(x_i)$中出现), 此时 $u(t)=u(x_i)$;

(ii) $p(x_i)=\forall x_i q(x_i)$ (无自由 $x_i$)，此时 $p(t)=p(x_i)$.

($p(x_i)=\forall x_j q(x_i)$ $(x_j\neq x_i)$ 的情形属下面的类型 4 (v).)

**类型 3** ($'$, $\neg$ 型)

(i) $u(x_i)={}'t_1(x_i)$, 此时 $u(t)={}'t_1(t)$;

(ii) $p(x_i)=\neg q(x_i)$, 此时 $p(t)=\neg q(t)$.

**类型 4** (其他)

(i) $u(x_i)=+t_1(x_i)t_2(x_i), u(t)=+t_1(t)t_2(t)$;

(ii) $u(x_i)=\times t_1(x_i)t_2(x_i), u(t)=\times t_1(t)t_2(t)$;

(iii) $p(x_i)=\approx t_1(x_i)t_2(x_i), p(t)=\approx t_1(t)t_2(t)$;

(iv) $p(x_i)=\rightarrow q(x_i)r(x_i), p(t)=\rightarrow q(t)r(t)$;

(v) $p(x_i) = \forall x_j q(x_i)(x_j \neq x_i), p(t) = \forall x_j q(t)$.
此外不会有别种情形发生.

基于以上分析，我们可以写出

$$
\begin{aligned}
&(n_1, n_2, \gamma) \in \mathrm{SBS} \quad \Leftrightarrow \\
&\quad n_1 \in \mathrm{VS} \wedge n_2 \in \mathrm{TM} \wedge (\gamma)_0 \in \mathrm{TM} \cup \mathrm{FM} \wedge \\
&\quad [((\gamma)_0 = n_1 \wedge (\gamma)_1 = n_2) \vee && \text{(类型 1)}\\
&\quad \exists x<(\gamma)_0((((\gamma)_0 = 2^x \wedge (\gamma)_0 \neq n_1) \vee (\gamma)_0 = 2^{11} * n_1 * x) \wedge (\gamma)_1 = (\gamma)_0) \vee \\
&&& \text{(类型 2)}\\
&\quad \exists x < (\gamma)_0 \exists y < (\gamma)_0 \exists z < (\gamma)_1 ((\gamma)_0 = 2^x * y \wedge \\
&\qquad\qquad (\gamma)_1 = 2^x * z \wedge (n_1, n_2, 2^y 3^z) \in \mathrm{SBS}) \vee && \text{(类型 3)}\\
&\quad \exists x < (\gamma)_0 \exists y < (\gamma)_0 \exists z < (\gamma)_0 \exists u < (\gamma)_1 \exists v < (\gamma)_1 \\
&\qquad\qquad (\gamma)_0 = 2^x * y * z \wedge (x \neq 11 \vee y \neq n_1) \wedge (\gamma)_1 = 2^x * u * v \wedge \\
&\qquad\qquad (n_1, n_2, 2^y 3^u) \in \mathrm{SBS} \wedge (n_1, n_2, 2^z 3^v) \in \mathrm{SBS})]. && \text{(类型 4)}
\end{aligned}
$$

由此可得到 $C_{\mathrm{SBS}}$ 所满足的过程值递归条件. □

有了与替换有关的三元递归关系 SBS 以后，现在要继续考察: 用 $n_2$ 项 $t$ 去替换 $n_3$ 项 $u(x_i)$ 中或 $n_3$ 公式 $p(x_i)$ 中所有自由的 $n_1$ 变元 $x_i$, 所得结果 $u(t)$ 或 $p(t)$ 的 Gödel 数是多少，能否递归地算出来?

先尝试一下，看是否可以这样表示出上述替换结果的 Gödel 数:

$$\mu x[C_{\mathrm{SBS}}(n_1, n_2, 2^{n_3} 3^x) = 1].$$

这样做还不行，因为根存在性条件不能保证得到满足，例如当 $n_1 \notin \mathrm{VS}$ 时，方括号内左端便为零. 但只要作一点修改就可以了. 在方括号内等式左边增加一项 $C_{\leqslant}(m, x)$, 这里的 $m$ 取得充分大，大到使它不可能是上述替换结果的 Gödel 数，例如取 $m = (p_{n_2 n_3})^{n_2^2 n_3^2}$. 这时，对任意 $n_1, n_2, n_3$, 总有 $x$ 使方括号内新等式成立. 于是有

**命题 4** 三元函数 Sub 是递归函数，Sub 由下式定义:

$$\mathrm{Sub}(n_1, n_2, n_3) = \mu x[C_{\mathrm{SBS}}(n_1, n_2, 2^{n_3} 3^x) + C_{\leqslant}((p_{n_2 n_3})^{n_2^2 n_3^2}, x) = 1].$$

按 SBS 的定义，可以把上式更具体地写成

$$\mathrm{Sub}(n_1, n_2, n_3) = \begin{cases} \mathrm{g}(u(t)), \text{ 若 } n_1 = \mathrm{g}(x_i), n_2 = \mathrm{g}(t), n_3 = \mathrm{g}(u(x_i)); \\ \mathrm{g}(p(t)), \text{ 若 } n_1 = \mathrm{g}(x_i), n_2 = \mathrm{g}(t), n_3 = \mathrm{g}(p(x_i)); \\ (p_{n_2 n_3})^{n_2^2 n_3^2}, \quad \text{其他情形.} \end{cases}$$

其中 $\mathrm{g}(u(t))$ 是用 $n_2$ 项 $t$ 替换 $n_3$ 项 $u(x_i)$ 中所有自由的 $n_1$ 变元 $x_i$ 所得结果 $u(t)$ 的 Gödel 数. $\mathrm{g}(p(t))$ 与之类似. 往后如不另作说明，符号 g 用来表示 Gödel 配数.

断定 $\mathrm{LA}_4$ 和 $\mathrm{LA}_5$ (它们分别是 (K4) 和 (K5) 型公理的 Gödel 数集) 的递归性，还需要下面的结论.

**命题 5** 以下关系是递归关系.

1° $\mathrm{FR} = \{(n_1, n_2) \mid n_1$ 变元在 $n_2$ 项或 $n_2$ 公式中自由出现$\}$.

2° $\mathrm{FRT} = \{(n_1, n_2, n_3) \mid n_2$ 项对 $n_3$ 公式中的 $n_1$ 变元是自由的$\}$.

**证** 1° 为了确定 $n_1$ 变元是否在 $n_2$ 项或 $n_2$ 公式中自由出现，可采用如下方法：用不同于 $n_1$ 变元 $x_i$ 的另一变元 (例如用 $x_{i+1}$) 去替换 $n_2$ 项或 $n_2$ 公式中所有自由出现的 $n_1$ 变元 $x_i$. 替换结果不引起任何变化，则说明 $n_1$ 变元不自由出现；否则说明自由出现. (注意 $\mathrm{g}(x_{i+1}) = n_1 \times 2^2$.) 于是有

$$
\begin{aligned}
&(n_1, n_2) \in \mathrm{FR} \quad \Leftrightarrow \\
&\qquad n_1 \in \mathrm{VS} \ \wedge \ n_2 \in \mathrm{TM} \cup \mathrm{FM} \ \wedge \ (n_1, n_1 \times 2^2, 2^{n_2} 3^{n_2}) \notin \mathrm{SBS}.
\end{aligned}
$$

2° 如果项 $t$ 对公式 $p$ 中 $x_i$ 是自由的，那么恰有以下四种情形中的一种出现：

(i) $p$ 是原子公式；

(ii) $p = \neg q$ 或 $\to q\,r$, 这时 $t$ 对 $q$ 及 $r$ 中 $x_i$ 是自由的；

(iii) $p = \forall x_i\, q$;

(iv) $p = \forall x_j\, q, x_j \neq x_i$, 这时或者 $q$ 中没有自由的 $x_i$, 或者 $t$ 中没有 $x_j$ 而 $t$ 对 $q$ 中 $x_i$ 是自由的.

以上分析说明

$$
\begin{aligned}
(n_1, n_2, n_3) \in \mathrm{FRT} \quad \Leftrightarrow \quad & n_1 \in \mathrm{VS} \ \wedge \ n_2 \in \mathrm{TM} \ \wedge \ n_3 \in \mathrm{FM} \ \wedge \\
& (n_3 \in \mathrm{YF} \ \vee \ \exists x < n_3 \, (n_3 = 2^7 * x \wedge (n_1, n_2, x) \in \mathrm{FRT}) \vee \\
& \exists x < n_3 \, \exists y < n_3 \, (n_3 = 2^9 * x * y \wedge (n_1, n_2, x) \in \mathrm{FRT} \wedge (n_1, n_2, y) \in \mathrm{FRT}) \vee \\
& \exists x < n_3 \, \exists y < n_3 \, (n_3 = 2^{11} * x * y \wedge \ x \in \mathrm{VS} \wedge \\
& \qquad (x = n_1 \ \vee \ (n_1, y) \notin \mathrm{FR} \ \vee \ ((x, n_2) \notin \mathrm{FR} \wedge (n_1, n_2, y) \in \mathrm{FRT})))).
\end{aligned}
$$

由此可写出 $C_{\mathrm{FRT}}$ 所满足的过程值递归条件. □

**命题 6** $\mathrm{LA}_4, \mathrm{LA}_5$ 是递归集，从而（注意命题 2）

$$\mathrm{LA} = \mathrm{LA}_1 \cup \cdots \cup \mathrm{LA}_5$$

是递归集. 就是说，$K_{\mathrm{N}}$ 的所有逻辑公理 ((K1)~(K5)) 的 Gödel 数构成的集是递归集.

**证** $\mathrm{LA}_4$ 是所有形为 $\to \forall x_i\, p(x_i)\, p(t)$ (其中 $t$ 对 $p(x_i)$ 中 $x_i$ 自由) 的公式的 Gödel 数构成的集. 所以有

$$
\begin{aligned}
& n \in \mathrm{LA}_4 \quad \Leftrightarrow \\
& \quad \exists x < n \, \exists y < n \, \exists z < n \, (x \in \mathrm{VS} \ \wedge \ y \in \mathrm{TM} \ \wedge \ z \in \mathrm{FM} \ \wedge \\
& \qquad\qquad (x, y, z) \in \mathrm{FRT} \ \wedge \ n = 2^9 * 2^{11} * x * z * \mathrm{Sub}(x, y, z)).
\end{aligned}
$$

由 Sub，FRT 等的递归性便得 $\mathrm{LA}_4$ 的递归性.

$\mathrm{LA}_5$ 是所有形为 $\to \forall x_i \to p\,q \to p \forall x_i\, q$ (其中 $x_i$ 不在 $p$ 中自由出现) 的公式的 Gödel 数集. 所以有

$$
\begin{aligned}
& n \in \mathrm{LA}_5 \quad \Leftrightarrow \\
& \quad \exists x < n \, \exists y < n \, \exists z < n \, (x \in \mathrm{VS} \ \wedge \ y \in \mathrm{FM} \ \wedge \ z \in \mathrm{FM} \ \wedge
\end{aligned}
$$

$$n = 2^9 * 2^{11} * x * 2^9 * y * z * 2^9 * y * 2^{11} * x * z \ \wedge \ (x, y) \notin \mathrm{FR}).$$

由 FR 等的递归性可得 $\mathrm{LA}_5$ 的递归性. □

下面讨论算术公理 Gödel 数集的递归性，讨论中不再有新的困难.

**命题 7** PA——所有 $\mathcal{N}$ 中公式 (即算术公理) Gödel 数集——是递归集. 从而

$$\mathrm{AX} = \mathrm{LA} \cup \mathrm{PA}$$

是递归集. (AX 就是包括逻辑公理和算术公理都在内的所有 $K_{\mathrm{N}}$ 公理的 Gödel 数的全体构成的集. )

**证** $\mathrm{PA} = \mathrm{EA}_1 \cup \mathrm{EA}_2 \cup \mathrm{EA}_3 \cup \mathrm{NA}_1 \cup \cdots \cup \mathrm{NA}_7$, 其中 $\mathrm{EA}_i$ 是 (E$i$) 型等词公理 Gödel 数全体的集; $\mathrm{NA}_i$ 是 (N$i$) 型算术公理 Gödel 数全体的集.

$\mathrm{EA}_1$ 是所有形为 $\approx tt$ ($t$ 是任意的项) 的公式 Gödel 数集，所以有

$$n \in \mathrm{EA}_1 \quad \Leftrightarrow \quad \exists x < n\,(x \in \mathrm{TM} \wedge n = 2^{13} * x * x).$$

由 TM 等的递归性可得 $\mathrm{EA}_1$ 的递归性.

完全类似地可得 $\mathrm{EA}_2, \mathrm{EA}_3, \mathrm{NA}_1 \sim \mathrm{NA}_6$ 的递归性. 至于 $\mathrm{NA}_7$, 它是所有形为

$$\rightarrow\ p(\bar{0}) \rightarrow \forall x_i \rightarrow p(x_i)\, p(' x_i) \forall x_i\, p(x_i)$$

的公式的 Gödel 数集，所以有:

$$n \in \mathrm{NA}_7 \quad \Leftrightarrow \quad \exists x < n \exists y < n\,(x \in \mathrm{VS} \ \wedge \ y \in \mathrm{FM} \wedge$$
$$n = 2^9 * \mathrm{Sub}(x, 2^{15}, y) * 2^9 * 2^{11} * x * 2^9 * y * \mathrm{Sub}(x, 2^1 * x, y) * 2^{11} * x * y).$$

由 Sub 等的递归性得 $\mathrm{NA}_7$ 的递归性. □

公理 Gödel 数全体的集 $\mathrm{AX} = \mathrm{LA} \cup \mathrm{PA}$ 是递归集这一事实的重要性在于，由它决定了另一重要事实——所有从 $\mathcal{N}$ 的证明的 Gödel 数构成的集 PF 是递归集.

**命题 8** 以下关系与集是递归的. (g 仍表示 Gödel 配数).

1° $\mathrm{MP} = \{(n_1, n_2, n_3) \mid n_1 = \mathrm{g}(p), n_2 = \mathrm{g}(p \rightarrow q), n_3 = \mathrm{g}(q)\}$,

2° $\mathrm{GEN} = \{(n_1, n_2) \mid n_1 = \mathrm{g}(p), n_2 = \mathrm{g}(\forall x_i\, p)\}$,

3° $\mathrm{PF} = \{n \mid n$ 是从 $\mathcal{N}$ 的证明的 Gödel 数$\}$,

4° $\mathrm{PRF} = \{(n_1, n_2) \mid n_1 = \mathrm{g}(p), n_2$ 是 $p$ 从 $\mathcal{N}$ 的证明的 Gödel 数$\}$.

**证** 1° $(n_1, n_2, n_3) \in \mathrm{MP} \quad \Leftrightarrow \quad n_1 \in \mathrm{FM} \wedge n_3 \in \mathrm{FM} \ \wedge \ n_2 = 2^9 * n_1 * n_3$.

2° $(n_1, n_2) \in \mathrm{GEN} \quad \Leftrightarrow$

$$n_1 \in \mathrm{FM} \ \wedge \ \exists x < n_2\,(x \in \mathrm{VS} \ \wedge \ n_2 = 2^{11} * x * n_1).$$

3° $n \in \mathrm{PF} \quad \Leftrightarrow \quad \exists x < n\,(n = 2^x \ \wedge \ x \in \mathrm{AX}) \vee$

$$\exists x < n \exists y < n \exists z < n \exists w < n\,(n = x * 2^y \ \wedge \ x \in \mathrm{PF} \wedge$$
$$(((x)_z, (x)_w, y) \in \mathrm{MP} \ \vee \ ((x)_z, y) \in \mathrm{GEN} \ \vee \ y \in \mathrm{AX})).$$

由此可得 $C_{\mathrm{PF}}$ 满足的过程值递归条件.

4° $(n_1, n_2) \in \mathrm{PRF} \quad \Leftrightarrow \quad n_2 \in \mathrm{PF} \wedge \ n_1 = (n_2)_{\mathrm{lh}(n_2) \dot{-} 1}$. □

让我们注意命题 8-3° 的证明. 这个证明的过程说明, PF 的递归性依赖于 AX 的递归性, 但仅仅依赖于"AX 是递归的"这一点, 而与 AX 中所包含的是哪些具体公理的 Gödel 数无关. 不管是减少一些公理, 还是改变一些公理, 甚至再增加更多的公理, 只要保持 AX 的递归性, 便都不改变 PF 的递归性. 对于这个事实, 后面还要作深入讨论.

**命题 9** 一元函数 Num 是递归函数, 它的定义式是

$$\mathrm{Num}(n) = \mathrm{g}(\overline{n}), \text{即数字 } \overline{n} \text{ 的 Gödel 数.}$$

**证** $\mathrm{Num}(0) = \mathrm{g}(\overline{0}) = 2^{15}$,

$\mathrm{Num}(n+1) = \mathrm{g}(\overline{n+1}) = \mathrm{g}(\prime\overline{n}) = 2^1 * \mathrm{g}(\overline{n}) = 2^1 * \mathrm{Num}(n)$. □

## 练习 33

1. 试写出 $C_{\mathrm{SBS}}, C_{\mathrm{FRT}}$ 和 $C_{\mathrm{PF}}$ 所满足的过程值递归条件.
2. 若先知道 PF 是递归集, 试反过来证明 AX 是递归集.
3. 证明二元关系 $W$ 的递归性, 其中

$$W = \{(n_1, n_2) \mid n_1 \text{ 是 } p(x_1) \text{ 的 Gödel 数}, \\ n_2 \text{ 是 } p(\overline{n_1}) \text{ 从 } N \text{ 的证明的 Gödel 数}\}.$$

### 3.6 附 可表示函数的递归性

利用已得结果, 顺便可以证明可表示函数的递归性. 下面在证明 Gödel 不完备性定理时并不用这个结论.

**定理 1 (可表示函数的递归性)** REP ⊆ REC. 即: 在 $K_{\mathrm{N}}$ 中可表示的函数必为递归函数.

**证** 设 $k$ 元函数 $f$ 用公式 $p(x_1,\cdots,x_k,y)$ 可表示, 其中 $y$ 是不同于 $x_1,\cdots,x_k$ 的个体变元 (可取 $y = x_{k+1}$). 把 $p(x_1,\cdots,x_k,y)$ 的 Gödel 数记为 $\alpha_0$ :

$$\alpha_0 = \mathrm{g}(p(x_1,\cdots,x_k,y)).$$

$f$ 给定之后, 且用以表示它的公式 $p(x_1,\cdots,x_k,y)$ 取定之后, $\alpha_0$ 是个定数. 现利用已有的公式 $p(x_1,\cdots,x_k,y)$ 作出一个 $k+2$ 元关系 $W_p$ :

$W_p = \{(n_1,\cdots,n_{k+2}) \mid n_{k+2}$ 是 $p(\overline{n_1},\cdots,\overline{n_{k+1}})$ 从 $N$ 的证明的 Gödel 数$\}$.

把 $p(\overline{n_1},x_2,\cdots,x_k,y), p(\overline{n_1},\overline{n_2},x_3,\cdots,x_k,y),\cdots, p(\overline{n_1},\overline{n_2},\cdots,\overline{n_{k+1}})$ 的 Gödel 数分别记为

$$\alpha_1(n_1),\ \alpha_2(n_1,n_2),\cdots,\alpha_{k+1}(n_1,\cdots,n_{k+1}),$$

这是一串递归函数:

$$\alpha_1(n_1) = \mathrm{g}(p(\overline{n_1},x_2,\cdots,x_k,y)) = \mathrm{Sub}(2^{15+2},\mathrm{Num}(n_1),\alpha_0),$$

$$\alpha_2(n_1,n_2)=g(p(\overline{n_1},\overline{n_2},x_3,\cdots,x_k,y))$$
$$=\mathrm{Sub}(2^{15+4},\ \mathrm{Num}(n_2),\alpha_1(n_1)),$$
$$\cdots,$$
$$\alpha_{k+1}(n_1,\cdots,n_{k+1})=g(p(\overline{n_1},\overline{n_2},\cdots,\overline{n_{k+1}}))$$
$$=\mathrm{Sub}(2^{15+2(k+1)},\ \mathrm{Num}(n_{k+1}),\alpha_k(n_1,\cdots,n_k)).$$

现在由 $W_p$ 的定义立即可知 $W_p$ 是递归的:

$$C_{W_p}(n_1,\cdots,n_{k+2})=C_{\mathrm{PRF}}(\alpha_{k+1}(n_1,\cdots,n_{k+1}),n_{k+2}),$$

又因已设 $f$ 用 $p(x_1,\cdots,x_k,y)$ 可表示，故有

$$\mathcal{N}\vdash p(\overline{n_1},\cdots,\overline{n_k},\overline{f(n_1,\cdots,n_k)}).\qquad (由 3.3.1 小节命题 1\text{-}1°)$$

把 $p(\overline{n_1},\cdots,\overline{n_k},\overline{f(n_1,\cdots,n_k)})$ 从 $\mathcal{N}$ 的一个证明的 Gödel 数记为 $m$. 按 $W_p$ 的定义，我们有

$$(n_1,\cdots,n_k,f(n_1,\cdots,n_k),m)\in W_p.$$

这说明，对于任意的 $n_1,\cdots,n_k$, 一定存在 $x\in\mathbf{N}$ 使

$$(n_1,\cdots,n_k,(x)_0,(x)_1)\in W_p.$$

(例如取 $x=2^{f(n_1,\cdots,n_k)}3^m$ 便可.) 这个事实保证了下面定义的 $k$ 元函数 $x^*$ 是处处有定义的递归全函数:

$$x^*(n_1,\cdots,n_k)=\mu x[C_{W_p}(n_1,\cdots,n_k,(x)_0,(x)_1)=1].$$

于是自然有

$$C_{W_p}(n_1,\cdots,n_k,(x^*(n_1,\cdots,n_k))_0,(x^*(n_1,\cdots,n_k))_1)=1,$$

即

$$(n_1,\cdots,n_k,(x^*(n_1,\cdots,n_k))_0,(x^*(n_1,\cdots,n_k))_1)\in W_p.$$

由此及 $W_p$ 的定义便得

(1) $\mathcal{N}\vdash p(\overline{n_1},\cdots,\overline{n_k},\overline{(x^*(n_1,\cdots,n_k))_0})$.

现假设

(2) $f(n_1,\cdots,n_k)\neq(x^*(n_1,\cdots,n_k))_0$.

由此假设及 3.3.1 小节定义 1(ii) 立即得

(3) $\mathcal{N}\vdash\neg p(\overline{n_1},\cdots,\overline{n_k},\overline{(x^*(n_1,\cdots,n_k))_0})$.

$\mathcal{N}$ 是无矛盾的，故 (1) 与 (3) 不能同时成立，这说明所作的假设 (2) 是不能成立的，除非 $\mathcal{N}$ 有矛盾. 这样，我们就在 $\mathcal{N}$ 无矛盾的假定之下证明了可表示函数 $f$ 具有递归性:

$f(n_1,\cdots,n_k)=(x^*(n_1,\cdots,n_k))_0$

$$= (\mu x [ C_{w_p} ( n_1, \cdots, n_k, (x)_0, (x)_1 ) = 1 ] )_0. \qquad \square$$

把定理 1 与 3.5 节推论 3 合起来，我们得到

$$\text{REC} = \text{REP},$$

即递归性与在 $K_N$ 中的可表示性是一回事.

## 练习 34

修改可表示性的定义 (3.3.1 小节定义 1)，把原定义中的 $\mathcal{N}$ 换成 $\mathcal{N}$ 的无矛盾扩张 $\mathcal{N}^*$, 但保持 $\mathcal{N}^*$ 中公理的 Gödel 数集的递归性 (这时说 $\mathcal{N}^*$ 是 $\mathcal{N}$ 的递归无矛盾扩张). 试问 REC = REP* 是否成立?(REP* 指扩张的系统中可表示函数全体的集.)

# 4 不完备性定理

## 4.1 Gödel 不完备性定理

有了前面的准备工作，下面要证明关于形式算术 $K_N$ 的一个重要结论—— $K_N$ 的公理集 $N$ 是不完备的，即 $K_N$ 中存在着闭式，它和它的否定都从 $N$ 不可证 (这样的闭式叫做 $N$ 的不可判定公式). 能否用增加 $N$ 中公理或其他办法来达到完备? 我们也要回答这个问题.

### 4.1.1 Gödel 定理

$K_N$ 中公式集 $\Gamma$ 是完备的，是指对 $K_N$ 中的任一闭式 $p$, $\Gamma \vdash p$ 与 $\Gamma \vdash \neg p$ 二者必居其一. 为证 $N$ 不完备，只要构造一个闭式 $p$, 它是 $N$ 不可判定的，即 $N \nvdash p$ 且 $N \nvdash \neg p$.

我们已经知道，自然数集 $\mathbf{N}$ 上的函数与关系是否递归，等同于是否在 $K_N$ 中可表示. 关于 $K_N$ 的结论可以通过 Gödel 配数转化成关于自然数的结论. 而关于自然数的结论又可大量地在 $K_N$ 中形式化. 我们将会看到，利用 $\mathbf{N}$ 与 $K_N$ 之间的上述密切联系，能够自然地产生出一种“自相关”，构造出一种具有“自相关”特征的公式，这种公式从语义上恰恰对自身有所断定，特别是对自己的可证性有所申明. 在下面的讨论过程中让我们注意仔细观察这种“自相关”特征的产生和所起的作用.

Gödel 在建立自己的结论时，引进了“$\omega$-无矛盾”的概念.

公式集 $\Gamma$ 是无矛盾的，指对任何公式 $p$, $\Gamma \vdash \neg p$ 与 $\Gamma \vdash \neg p$ 不会同时成立. “$\omega$-无矛盾”是比“无矛盾”更强的条件.

**定义 1 ($\omega$-无矛盾)** 公式集 $\Gamma$ 是 $\omega$-无矛盾的，意为对 $K_N$ 中任一含有自由变元 $x$ 的公式 $p(x)$, 以下两条都不会同时成立:

1° 对所有 $n \in \mathbf{N}$, $\Gamma \vdash p(\overline{n})$;

2° $\Gamma \vdash \neg \forall x\, p(x)$.

**命题 1** 若 $\Gamma$ $\omega$-无矛盾，则 $\Gamma$ 无矛盾.

**证** 反设 $\Gamma$ 有矛盾. 由 2.1.3 小节命题 1 便知任何公式都从 $\Gamma$ 可证，从而对任一含自由变元 $x$ 的公式 $p(x)$, 定义 1 中的条件 $1^\circ$ 与 $2^\circ$ 都同时成立，于是 $\Gamma$ 并非 $\omega$-无矛盾. □

为讨论 $\mathcal{N}$ 的不完备性，先引入一个二元关系 $W$:

$$W=\{(n_1,n_2)\mid n_1\text{是某个公式}p(x_1)\text{的Gödel数，}\\ n_2\text{是}p(\overline{n_1})\text{从}\mathcal{N}\text{的证明的Gödel 数}\}.$$

换一种方式，可写:

$$(n_1,n_2)\in W \quad\Leftrightarrow\quad n_1\in \mathrm{FM}\ \wedge\ (\mathrm{Sub}(2^{15+2},\mathrm{Num}(n_1),n_1),n_2)\in \mathrm{PRF}.$$

$W$ 是递归的，它的特征函数是

$$C_W(n_1,n_2)=C_{\mathrm{FM}}(n_1)\times C_{\mathrm{PRF}}(\mathrm{Sub}(2^{17},\mathrm{Num}(n_1),n_1),n_2),$$

其中 FM，Sub，Num 和 PRF 递归性已在 3.6.4 小节中得到证明.

二元关系 $W$ 是递归的，所以在 $K_{\mathrm{N}}$ 中可表示. 设 $W$ 用公式 $w(x_1,x_2)$ 可表示:

$$(n_1,n_2)\in W \quad\Rightarrow\quad \mathcal{N}\vdash w(\overline{n_1},\overline{n_2});$$

$$(n_1,n_2)\notin W \quad\Rightarrow\quad \mathcal{N}\vdash \neg w(\overline{n_1},\overline{n_2}).$$

记

$$\mathrm{p}(x_1)=\forall x_2\neg w(x_1,x_2).$$

它只含一个自由变元 $x_1$. 把它的 Gödel 数设为 $m$:

$$m=\mathrm{g}(\mathrm{p}(x_1)),$$

然后用 $\overline{m}$ 去替换 $\mathrm{p}(x_1)$ 中所有自由出现的 $x_1$, 得一闭式 (*):

$$(*)\qquad \mathrm{p}(\overline{m})=\forall x_2\neg w(\overline{m},x_2).$$

这是一个有自相关特点的公式. 我们先直观地分析一下它的自相关特性.

注意 $W$ 的定义以及 $W$ 用 $w(x_1,x_2)$ 可表示这一事实. 公式 $\mathrm{p}(\overline{m})$ (即 $\forall x_2\neg w(\overline{m},x_2)$) 的直观意思是: 对于任何自然数 $n$, 都有 $(m,n)\notin W$. 换句话说，不存在自然数 $n$, 使 $(m,n)\in W$. 这是什么意思呢?$m$ 是 $\mathrm{p}(x_1)$ 的 Gödel 数. 用 $\overline{m}$ 代换 $x_1$, 得 $\mathrm{p}(\overline{m})$. 是否存在自然数 $n$ 成为 $\mathrm{p}(\overline{m})$ 从 $\mathcal{N}$ 的证明的 Gödel 数 (即 $(m,n)\in W$)? $\mathrm{p}(\overline{m})$ 自己回答: 不存在这样的自然数.

直截了当地说，$\mathrm{p}(\overline{m})$ 自我声明:

“我从 $\mathcal{N}$ 不可证!”

**定理 1 (Gödel)**

(i) 若 $\mathcal{N}$ 无矛盾，则 $\mathcal{N}\nvdash \mathrm{p}(\overline{m})$,

(ii) 若 $\mathcal{N}$ $\omega$-无矛盾，则 $\mathcal{N}\nvdash \neg\mathrm{p}(\overline{m})$,

其中 $\mathrm{p}(\overline{m})$ 是上面的闭式 $(*)$.

**证** (i) 反设 $\mathcal{N} \vdash \mathrm{p}(\overline{m})$, 即

(1) $\mathcal{N} \vdash \forall x_2 \neg w(\overline{m}, x_2)$.

把 $\mathrm{p}(\overline{m})$ 从 $\mathcal{N}$ 的一个证明的 Gödel 数记为 $n$, 则 $(m,n) \in W$. 因 $W$ 是用 $w(x_1,x_2)$ 表示的，故

(2) $\mathcal{N} \vdash w(\overline{m},\overline{n})$.

由 (1) 使用 (K4) 和 MP 即可得

$$\mathcal{N} \vdash \neg w(\overline{m},\overline{n}),$$

它与 (2) 说明了 $\mathcal{N}$ 是有矛盾的.

(ii) 再反设 $\mathcal{N} \vdash \neg \mathrm{p}(\overline{m})$, 即

(3) $\mathcal{N} \vdash \neg \forall x_2 \neg w(\overline{m}, x_2)$.

已知 $\mathcal{N} \vdash \mathrm{p}(\overline{m})$ 不成立 (由 (i)). 根据 $W$ 的定义便知对于任何自然数 $n$, 都有 $(m,n) \notin W$. 又因 $W$ 用 $w(x_1,x_2)$ 可表示，故对所有 $n$, 都有

$$\mathcal{N} \vdash \neg w(\overline{m},\overline{n}).$$

这个事实与 (3) 结合起来，说明 $\mathcal{N}$ 并非 $\omega$-无矛盾. □

定理 1 告诉我们，如果 $\mathcal{N}$ 是 $\omega$-无矛盾的，(因而也是无矛盾的，) 那么 $\mathrm{p}(\overline{m})$ 是 $\mathcal{N}$ 的不可判定闭式. 这说明必定存在着在 **N** 中恒真的公式而从 $\mathcal{N}$ 不可证.(注意闭式的语义特征，任一闭式 $p$ 和它的否定 $\neg p$ 二者必有一个在 **N** 中恒真.)

为证明 $\mathcal{N}$ 的不完备性,“$\omega$-无矛盾”这个更强的假定并不是必要的. 4.1.2 小节中的 Gödel-Rosser 定理就是在“无矛盾”的假定之下证明了 $\mathcal{N}$ 的不完备性.

通常把定理 1 叫做 Gödel 第一不完备性定理.

## 练习 35

1. 证明 $|\mathrm{p}(\overline{m})|_{\mathbf{N}} = 1$. (这里 $\mathrm{p}(\overline{m})$ 是正文中的闭式 $*$, 下题同.)
2. 证明 $\mathcal{N} \cup \{\neg \mathrm{p}(\overline{m})\}$ 是无矛盾的，但并非 $\omega$-无矛盾.
3. 已知公式 $r(x_1)$. 试证下面的二元关系是递归的:

$$W_1 = \{(n_1,n_2) \mid n_1 = \mathrm{g}(q),\ n_2 \text{ 是公式 } \neg r(\overline{n_1}) \to \neg q \text{从 } \mathcal{N} \text{ 的证明的 Gödel数}\},$$

其中 $r(\overline{n_1})$ 是用 $\overline{n_1}$ 代换给定的公式 $r(x_1)$ 中自由出现的 $x_1$ 所得结果.

### 4.1.2 Gödel-Rosser 定理

$\mathcal{N}$ 的不完备性能否用增加公理的办法予以消除? 现在来回答这个问题.

下面的定理是形式算术不完备性定理的比较一般的形式.

**定理 1 (Gödel-Rosser)** $\mathcal{N}$ 的任何递归无矛盾扩张 $\mathcal{N}^*$ 都不完备，即如果扩张的公理集 $\mathcal{N}^*(\supseteq \mathcal{N})$ 无矛盾，且 PA$^*$(= $\mathcal{N}^*$ 中全部公理的 Gödel 数构成的集) 是递归集，那么 $\mathcal{N}^*$ 不完备.

**证** 把 3.6.4 小节命题 7 中的 PA 改为 PA$^*$, 得到新的递归集 AX$^*$ = LA $\cup$ PA$^*$. 然后，把 3.6.4 小节命题 8 中 PF 和 PRF 的定义式里的 $\mathcal{N}$ 改为 $\mathcal{N}^*$, 这并不改变 PF 的 PRF 的递归性，为方便，计 PF 和 PRF 的符号不变.

作二元关系 $W$ 和 $W^*$ :

$$W = \{(n_1, n_2) \mid n_1 \text{ 是某公式 } p(x_1) \text{ 的 Gödel 数}, \quad n_2 \text{ 是} p(\overline{n_1}) \text{从} \mathcal{N}^* \text{的证明的Gödel 数}\}.$$

$$W^* = \{(n_1, n_2) \mid n_1 \text{ 是某公式 } p(x_1) \text{ 的 Gödel 数}, \quad n_2 \text{ 是} \neg p(\overline{n_1}) \text{从} \mathcal{N}^* \text{的证明的Gödel数}\}.$$

$W$ 的定义与 4.1.1 小节中的定义不同的是把 $\mathcal{N}$ 换成了 $\mathcal{N}^*$, 但其递归性的证明与原来的一样.

$W^*$ 也是递归的，它的特征函数可写成

$$C_{W^*}(n_1, n_2) = C_{\text{FM}}(n_1) \times C_{\text{PRF}}(\text{Sub}(2^{15+2}, \text{Num}(n_1), 2^7 * n_1), n_2).$$

设 $W$ 和 $W^*$ 分别用 $w(x_1, x_2)$ 和 $w^*(x_1, x_2)$ 可表示. 记

$$\text{p}(x_1) = \forall x_2 (w(x_1, x_2) \to \exists y (y \leqslant x_2 \wedge w^*(x_1, y))),$$

其中 $y$ 取为不在 $w(x_1, x_2)$ 和 $w^*(x_1, x_2)$ 中出现的某个变元. 把 $\text{p}(x_1)$ 的 Gödel 数记为 $m$ :

$$m = \text{g}(\text{p}(x_1)).$$

于是

$$\text{p}(\overline{m}) = \forall x_2 (w(\overline{m}, x_2) \to \exists y (y \leqslant x_2 \wedge w^*(\overline{m}, y))).$$

$\text{p}(\overline{m})$ 的直观意思是: “如果我有一个 Gödel 数为 $x_2$ 的从 $\mathcal{N}^*$ 的证明，那么我的否定有一个 Gödel 数为 $y$ 的从 $\mathcal{N}^*$ 的证明，且 $y \leqslant x_2$.” 简单地说，$\text{p}(\overline{m})$ 自我声明: “我若从 $\mathcal{N}^*$ 可证，则我的否定也从 $\mathcal{N}^*$ 可证且证明更简单.”

为证 $\mathcal{N}^*$ 是不完备的，只用证 $\text{p}(\overline{m})$ 是 $\mathcal{N}^*$ 的不可判定公式就可以了，即要证:

$$\mathcal{N}^* \nvdash \text{p}(\overline{m}) \text{ 且 } \mathcal{N}^* \nvdash \neg \text{p}(\overline{m}).$$

先反设 $\mathcal{N}^* \vdash \text{p}(\overline{m})$, 即

(1) $\mathcal{N}^* \vdash \forall x_2 (w(\overline{m}, x_2) \to \exists y (y \leqslant x_2 \wedge w^*(\overline{m}, y)))$.

设 $\text{p}(\overline{m})$ 从 $\mathcal{N}^*$ 的一个证明的 Gödel 数为 $n$, 则 $(m, n) \in W$. 于是有以下结论:

(2) $\mathcal{N}^* \vdash w(\overline{m}, \overline{n})$ 由 3.3.1 小节定义 3–(i)

(3) $\mathcal{N}^* \vdash w(\overline{m}, \overline{n}) \to \exists y (y \leqslant \overline{n} \wedge w^*(\overline{m}, y))$ (1), (K4), MP

(4) $\mathcal{N}^* \vdash \exists y(y \leqslant \bar{n} \land w^*(\bar{m},y))$ (2), (3), MP

(5) $\mathcal{N}^* \nvdash \neg \mathrm{p}(\bar{m})$ 否则 $\mathcal{N}^*$ 有矛盾

(6) 对任意 $k \in \mathbf{N}, (m,k) \notin W^*$, 从而 $\mathcal{N}^* \vdash \neg w^*(\bar{m},\bar{k})$

由 (5), $W^*$ 的定义, 及 3.3.1 小节定义 3-(ii)

(7) $\mathcal{N}^* \vdash \neg w^*(\bar{m},\bar{0}) \land \cdots \land \neg w^*(\bar{m},\bar{n})$ 由 (6)

(8) $\mathcal{N}^* \vdash y \leqslant \bar{n} \to \neg w^*(\bar{m},y)$ 由 (7) 及 3.2 节命题 14

(9) $\mathcal{N}^* \vdash \forall y \neg(y \leqslant \bar{n} \land w^*(\bar{m},y))$ (8), 永真式 $(p \to \neg q) \to \neg(p \land q)$, Gen

(10) $\mathcal{N}^* \vdash \neg \exists y(y \leqslant \bar{n} \land w^*(\bar{m},y))$ 由 (9) 及 2.1.3 小节命题 8

(4) 与 (10) 说明 $\mathcal{N}^*$ 有矛盾, 所以 $\mathcal{N}^* \nvdash \mathrm{p}(\bar{m})$.

再反设 $\mathcal{N}^* \vdash \neg \mathrm{p}(\bar{m})$. 将$\neg \mathrm{p}(\bar{m})$ 从 $\mathcal{N}^*$ 的一个证明的 Gödel 数记为 $n$, 则 $(m,n) \in W^*$, 进而 $\mathcal{N}^* \vdash w^*(\bar{m},\bar{n})$. 于是有以下结论:

(1) $\mathcal{N}^* \cup \{\bar{n} \leqslant x_2\} \vdash \bar{n} \leqslant x_2 \land w^*(\bar{m},\bar{n})$

(2) $\mathcal{N}^* \cup \{\bar{n} \leqslant x_2\} \vdash \exists y(y \leqslant x_2 \land w^*(\bar{m},y))$ 由 (1) 用 $\exists_1$ 规则

(3) $\mathcal{N}^* \vdash \bar{n} \leqslant x_2 \to \exists y(y \leqslant x_2 \land w^*(\bar{m},y))$ 由 (2)

(4) 对任意 $k \in \mathbf{N}$, $(m,k) \notin W$, 从而 $\mathcal{N}^* \vdash \neg w(\bar{m},\bar{k})$ 已证 $\mathcal{N}^* \nvdash \mathrm{p}(\bar{m})$

(5) $\mathcal{N}^* \vdash \neg w(\bar{m},\bar{0}) \land \cdots \land \neg w(\bar{m},\bar{n})$ 由 (4)

(6) $\mathcal{N}^* \vdash x_2 \leqslant \bar{n} \to \neg w(\bar{m},x_2)$ 由 (5) 及 3.2 节命题 14

(7) $\mathcal{N}^* \vdash w(\bar{m},x_2) \to x_2 \nleqslant \bar{n}$ (6), 换位律

(8) $\mathcal{N}^* \vdash x_2 \nleqslant \bar{n} \to \bar{n} \leqslant x_2$ 3.2 节命题 15

(9) $\mathcal{N}^* \vdash w(\bar{m},x_2) \to \exists y(y \leqslant x_2 \land w^*(\bar{m},y))$ (7), (8), (3), HS

(10) $\mathcal{N}^* \vdash \mathrm{p}(\bar{m})$ (9), Gen

前面已证过 (10) 不成立, 故上面的假设错误, 必有 $\mathcal{N}^* \nvdash \neg \mathrm{p}(\bar{m})$. 至此知 $\mathcal{N}^*$ 是不完备的.

□

## 练习 36

1. "$\mathcal{N}$ 的任何无矛盾扩张都不可能完备" 这一说法是否正确? 能否给出 $\mathcal{N}$ 的完备无矛盾扩张的例子?

2. 求证 $|\mathrm{p}(\bar{m})|_{\mathrm{N}} = 1$, 这里的 $\mathrm{p}(\bar{m})$ 是 Gödel-Rosser 定理证明中的闭式.

### 4.1.3 Church论题

为了理解不完备性定理的深刻含义, 我们先来考察一下算法的概念. 算法, 可直观地理解为关于计算过程的一串有限的、确定的指令. 这里的计算过程不一定是纯数值的.

考察问题类:

$$\{n\text{ 是偶数吗?}\mid n\in\mathbf{N}\}.$$

回答该类问题的算法是存在的: 给定 $n$, 除以 2，若余数为零，则回答 $n$ 是偶数; 若余数为 1，则回答 $n$ 不是偶数.

对一 $k$ 元函数 $f$, 考察问题类:

$$\{f(n_1,\cdots,n_k)\text{ 的值是什么?}\mid n_1,\cdots,n_k\in\mathbf{N}\}.$$

如果存在着算法可用来回答该类问题的任一问题，那么函数 $f$ 叫做算法可计算函数.

三种基本递归函数 (零函数 z，后继函数 s 和投影函数 $\mathrm{p}_i^k$) 都是算法可计算函数，它们都有很简单的算法.

设算法可计算的 $j$ 元函数 $g$ 和算法可计算的 $j$ 个 $k$ 元函数 $h_1,\cdots,h_j$ 复合成一个 $k$ 元函数 $f$. $f$ 也是算法可计算的，因为有如下的算法: 对任意 $n_1,\cdots,n_k\in\mathbf{N}$, 先用 $h_1,\cdots,h_j$ 的算法计算出

$$h_1(n_1,\cdots,n_k),\cdots,h_j(n_1,\cdots,n_k),$$

把它们记作 $m_1,\cdots,m_j$. 接着再用 $g$ 的算法算出 $g(m_1,\cdots,m_j)$, 它就是 $f(n_1,\cdots,n_k)$. 这说明，复合规则保持着算法可计算性.

由类似的讨论可知，递归规则和 $\mu$ 算子也保持着算法可计算性. 于是得出了结论，所有递归函数都是算法可计算的.

相反的问题是: 算法可计算函数是否都是递归函数?

有名的 Church 论题对此作了肯定的回答.

**Church论题:** 算法可计算函数 = 递归函数.

Church 论题是一经验事实，但还未发现反例. 经验告诉我们，一个函数的函数值计算如果存在着算法，那就总能找到该函数的递归描述. 所以我们可以把递归函数作为“算法可计算函数”这一直观概念的数学定义.

前面已经证明，递归意味着在 $K_{\mathrm{N}}$ 中可表示. 按 Church 论题，递归性又意味着算法可计算性. 于是 $K_{\mathrm{N}}$ 中的可表示函数可视为算法可计算函数的另一数学模型.

Church 论题对偏函数也是适用的. 偏函数 $f$ 是算法可计算的，应理解为: 存在一种算法，在 $f$ 有定义的点可用该算法算出 $f$ 的函数值.(并不要求算法能确定 $f$ 何时有定义.)

利用 Church 论题，如果证明了一个函数的递归性，也就肯定了用于计算该函数的算法的存在性; 如果找到了计算函数值的算法，就可肯定该函数是递归的.

3.6.4 小节中，我们证明了 FM (所有公式的 Gödel 数的集) 和 PF (所有从 $N$ 的证明的 Gödel 数集) 是递归集. 因为它们的特征函数是递归函数，按 Church 论题; 我

们便知道分别存在着算法能用来确定任给的 $n \in \mathbf{N}$ 是否属于 FM 或 PF. 也就是说，存在着算法能够用以确定任意字母串是不是 $K_{\mathrm{N}}$ 的公式，还存在着算法能够用以确定任给的公式的有限序列是不是从 $\mathcal{N}$ 的一个证明.

### 练习 37

1. 说明递归规则和 $\mu$ 算子保持函数的算法可计算性.
2. 试给出计算 $C_{\mathrm{VS}}(n)$ 和 $C_{\mathrm{TM}}(n)$ 的算法. (参见 3.6.4 小节命题 1.)

## 4.1.4 关于不完备性定理的一些讨论

不完备性定理的建立是 20 世纪数学乃至整个人类数学最杰出的成就之一. 现从以下几方面谈谈对它的理解.

**1. “可证”与“真”不是同一概念**

人们建立形式系统，是想使“证明”这一概念精确化. 针对一个具体的理论建立起一个具体的形式系统，自然希望在这个形式系统中按照精确化的证明的概念能够抓住该理论的所有真命题，即希望这个形式系统具有完备性.

我们针对自然数理论建立了形式算术 $K_{\mathrm{N}}$, 其中以 $\mathcal{N}$ (或 $\mathcal{N}$ 的递归无矛盾扩张 $\mathcal{N}^*$) 作为公理集，希望能够从 $\mathcal{N}$ (或 $\mathcal{N}^*$) 出发证明出所有在 $\mathbf{N}$ 中恒真的公式，希望能够抓住全部“算术真”. 不完备性定理指出，上面的这种希望是不能实现的.

定理给出的否定结论告诉我们,“可证”与“真”并不是同一概念. 实践中人们相信，一个不含混的算术命题和它的否定命题二者应有一真; 但现在知道，把二者形式化为 $K_{\mathrm{N}}$ 中的闭式，却可能从 $\mathcal{N}$ 都不可证.

什么叫证明? 什么叫可证? 直观上人们可以有不同的理解，形式系统中人们可以下不同的定义，可以提出不同的精确化的方式. 但是真和假，不应因形式化的方式而异.

既然“可证”与“真”是两个不同的概念，那么在一个形式系统中存在着不可证的“真”这一事实就不足为奇，而只说明形式化本身存在着局限性.

**2. 不完备性定理并不导致不可知**

$K_{\mathrm{N}}$ 的一个在 $\mathbf{N}$ 中恒真的公式从 $\mathcal{N}$ 不可证，并不意味着我们用其他方法也不可能知道它的“真”. 4.1.1 小节中的公式 $\mathrm{p}(\overline{m})$ 从 $\mathcal{N}$ 不可证，但恰恰正是它的不可证这一点证实了它的“真”.(见练习 35 题 1.)

作为另一个例子，我们来讨论 Goldbach 猜想. 设

$$G = \{n \mid n \leqslant 2, \text{ 或 } n \text{ 为奇数，或 } n \text{ 为二素数之和}\}.$$

$G$ 是递归集 (见练习 28 题 4)，故在 $K_{\mathrm{N}}$ 中可表示. 设 $G$ 用公式 $q(x_1)$ 可表示

$$n \in G \quad \Rightarrow \quad \mathcal{N} \vdash q(\overline{n}),$$

$$n \notin G \quad \Rightarrow \quad \mathcal{N} \vdash \neg q(\bar{n}).$$

记 $p = \forall x_1 q(x_1)$, 它就是 Goldbach 猜想的形式化. 现假设 $p$ 是不可判定的，即 $\mathcal{N} \vdash p$ 和 $\mathcal{N} \vdash \neg p$ 都不成立. (这只是一种假设，并未得到证明.) 如果真如此，那么 Goldbach 猜想便得到证实，因为我们可以证明此时 $p$ 在 $\mathbf{N}$ 中恒真. 下面来证明这一点.

反设 $|p|_{\mathbf{N}} = 0$, 即 $|\forall x_1 q(x_1)|_{\mathbf{N}} = 0$, 于是就有以下结论:

(1) 存在项解释 $\varphi$ 使 $|q(x_1)|(\varphi) = 0$　2.2.3 小节定义 1 及 2.2.2 小节定义 1 (iii)

(2) 记 $k = \varphi(x_1)$, 则 $|q(\bar{k})|(\varphi) = 0$　2.3 节引理 1-2°, 因 $\varphi(\bar{k}) = k = \varphi(x_1)$

(3) $k \notin G$　否则有 $\mathcal{N} \vdash q(\bar{k})$, $\mathcal{N} \models q(\bar{k})$, $|q(\bar{k})|_{\mathbf{N}} = 1$, 与 (2) 矛盾

(4) $\mathcal{N} \vdash \neg q(\bar{k})$　由 (3)

(5) $\mathcal{N} \vdash \exists x_1 \neg q(x_1)$　由 (4) 用 $\exists_1$ 规则

(6) $\mathcal{N} \vdash \neg \forall x_1 q(x_1)$　由 (5)

(6) 即为 $\mathcal{N} \vdash \neg p$. 这与 $p$ 不可判定的假设相矛盾.

不完备性定理告诉我们，不管是 $\mathcal{N}$ 还是 $\mathcal{N}$ 的递归无矛盾扩张 $\mathcal{N}^*$, 都有不可判定公式. 上面的例子告诉我们，一个公式的“不可判定”这一信息本身甚至有可能导致该公式为真或为假的证实.

**3. 不能从不完备性定理简单地得出结论: 形式算术不能完备化，$\mathcal{N}$ 没有完备的无矛盾扩张**

下面先说明，$\mathcal{N}$ 的完备无矛盾扩张是存在的. 例如可以仿照 2.4 节中证明 $K$ 的完全性时的做法，给出一个 $\mathcal{N}$ 的完备无矛盾扩张 $\Gamma^*$. (从 $\Gamma_0 = \mathcal{N}$ 出发，利用 $K_{\mathbf{N}}$ 的所有闭式，归纳定义出一串 $\mathcal{N}$ 的无矛盾扩张 $\Gamma_0, \Gamma_1, \Gamma_2, \cdots$, 然后令 $\Gamma^* = \bigcup_{n=0}^{\infty} \Gamma_n$.) 对于 $K_{\mathbf{N}}$ 中的每个闭式 $p$, $\Gamma^* \vdash p$ 和 $\Gamma^* \vdash \neg p$ 二者必居其一. 如果我们把 $\Gamma^*$ 作为扩张的算术公理集，那么我们就达到了完备化.

这样的完备化有什么意义呢?

按照 Gödel-Rosser 定理，上述 $\Gamma^*$ 中公理 Gödel 数之集只能是非递归集，否则 $\Gamma^*$ 就不会完备. 按照 Church 论题，不存在算法可以用来确定任给的公式是不是 $\Gamma^*$ 中的公理，进而不存在算法可用来确定任给的有限公式序列是不是从 $\Gamma^*$ 的证明. 不能用算法明确地判断一篇文章是不是证明，这样的理论虽然完备，但看不出有何实际价值.

再给一个 $\mathcal{N}$ 的完备扩张的例子. 将所有在 $\mathbf{N}$ 中恒真的 $K_{\mathbf{N}}$ 的公式构成的集记为 Tr. Tr 也是 $\mathcal{N}$ 的完备无矛盾扩张，因而 Tr 中公式的 Gödel 数的集 TR 是非递归集 (见练习 38 题 1). 把 Tr 作为扩张的算术公理集，虽然完备，但这相当于把所有真理都当作公理，然后说:“我证明了所有真理!”

**4. 能否用其他方法达到完备**

Gödel-Rosser 定理说明，单靠增加 $\mathcal{N}$ 中的公理达不到有意义的完备. 能否用其他方法做到这一点?

我们对 $K_{\mathrm{N}}$ 和 $\mathcal{N}$ 作如下扩张.

(1) 扩大 $K_{\mathrm{N}}$ 的字母表 (例如增加个体常元，函数词和谓词)，但要使新得到的谓词演算系统在进行配数后保持 TM，FM，LA，Sub 的递归性;

(2) 增加 $K_{\mathrm{N}}$ 的推理规则，并把 $\mathcal{N}$ 无矛盾地扩张成 $\mathcal{N}^*$，但使 PF，PRF 保持递归性.

按照 Church 论题，上述 (1)，(2) 中提出的递归性的要求也就是相应算法存在性的要求. 比如，PF 具有递归性，意味着存在算法可用来确定任给的公式串是不是新的形式系统中的一个从 $\mathcal{N}^*$ 的证明. 这样的要求是合理的，是对一个有意义的形式系统的起码要求.

回忆 Gödel-Rosser 定理的证明. 其中除了用到谓词演算的一般语法性质外，还用到以下事实: 递归函数是可表示的，FM，Sub，PRF 等是递归的. 这就说明对我们新的扩张的形式系统来说，该定理的证明仍然有效，结论仍然成立——新系统的 $\mathcal{N}^*$ 仍然是不完备的. 这除了因为上述变动没有改变一些基本语法关系的递归特征以外，还因为上述变动并不改变“递归函数具有可表示性”这一基本事实. 扩张的系统的表示能力不会比 $K_{\mathrm{N}}$ 更弱，可表示定义 (3.3.1 小节定义 1) 中的性质 ((i)~(iii)) 对新的扩张的形式系统更容易成立.

可以证明，如把 Peano 形式算术字母表中的乘号 (×) 去掉，把含乘号的公式都丢掉，则这样得到的系统 (被称作 Presburger 算术) 具有完备性. 但该系统作为“算术”，内容太贫乏了.

总之，任何把 Peano 形式算术包含在内的数学形式系统，只要有算法能用来确定该系统的任一篇文章 (即公式的有限序列) 是不是一个证明 (这时说该系统是“递归可公理化”的)，这样的形式系统就一定不完备.

有一定丰富内容的形式系统的这种局限性是在人们企图把“证明”这个概念精确化时必然出现的. 不管是整个数学还是 (包括算术在内的) 数学的一部分，都有着极其丰富的内容，都不可能一劳永逸地、机械地被抓住. 正因为如此，寻求新的证明方法和新的证明原则应该说属于数学中最富有创造性的活动.

## 练习 38

1. 利用 Gödel-Rosser 定理证明所有在 **N** 中恒真公式 Gödel 数的集

$$\mathrm{TR} = \{\, g(p) \mid |p|_{\mathrm{N}} = 1 \,\}$$

是非递归集.

2. 设二元递归关系 PRF (见 3.6.4 小节命题 8) 用公式 $\mathrm{prf}(x_1, x_2)$ 表示. 记

$$\mathrm{pr}(x_1) = \exists x_2\, \mathrm{prf}(x_1, x_2).$$

试证

$$\mathcal{N} \vdash q \quad \Rightarrow \quad \mathcal{N} \vdash \mathrm{pr}(\ulcorner q \urcorner),$$

这里规定 $\ulcorner q \urcorner = \overline{\mathrm{g}(q)}$, $q$ 是任一公式.

3. 题 2 中公式 $\mathrm{pr}(x_1)$ 是否可用来表示集 $\mathrm{TH} = \{\mathrm{g}(q) \mid q$ 从 $\mathcal{N}$ 可证$\}$, 从而说明 TH 是递归集?

### 4.1.5 Gödel 第二不完备性定理

20 世纪 20 年代初, Hilbert 针对数学基础中出现的问题提出了自己的解决方案, 试图用有穷的方法证明包括初等数论在内的古典数学形式系统是无矛盾的. Gödel 用自己的不完备性定理否定了这个方案. Gödel 的第二不完备性定理断言: 如果包括初等数论在内的数学形式系统是无矛盾的, 那么这种无矛盾性不可能在此系统中得到证明.

Gödel 第二不完备性定理的证明建立在第一不完备定理之上, 需要把第一定理的前半部分 (4.1.1 小节定理 1(i)) 的证明在系统内再次形式化. 证明过程层次重叠, 精细而冗长.

在这里, 我们就形式算术 $K_{\mathcal{N}}$ 这一系统给出无矛盾性不可证性定理 (即 Gödel 第二不完备性定理) 的一种易证形式. 同以前一样, 仍用 g 表示 Gödel 配数.

由 3.6.4 小节命题 8-4° 知, 二元关系

$$\mathrm{PRF} = \{(n_1, n_2) \mid n_1 = \mathrm{g}(q),\ n_2 \text{ 是 } q \text{ 从 } \mathcal{N} \text{ 的证明的 Gödel 数}\}$$

是递归的. 设 PRF 用公式 $\mathrm{prf}(x_1, x_2)$ 表示. 再记

$$\mathrm{pr}(x_1) = \exists x_2\, \mathrm{prf}(x_1, x_2).$$

**引理 1 (第一可推性条件)** 对任一公式 $q$,

$$\mathcal{N} \vdash q \quad \Rightarrow \quad \mathcal{N} \vdash \mathrm{pr}(\ulcorner q \urcorner),$$

其中 $\ulcorner q \urcorner$ 是 $\overline{\mathrm{g}(q)}$ 的简写.

**证** 记 $m = \mathrm{g}(q)$, 则 $\overline{m} = \ulcorner q \urcorner$. 设 $n$ 是 $q$ 从 $\mathcal{N}$ 的一个证明的 Gödel 数, 则有 $(m, n) \in \mathrm{PRF}$, 进而有

$$\mathcal{N} \vdash \mathrm{prf}(\overline{m}, \overline{n}).$$

由此用 $\exists_1$ 规则 (2.1.3 小节命题 2) 便得

$$\mathcal{N} \vdash \exists x_2\, \mathrm{prf}(\overline{m}, x_2) \text{ 即 } \mathrm{pr}(\ulcorner q \urcorner). \qquad \square$$

$\mathrm{pr}(\ulcorner q \urcorner)$ 的直观意思是: “$q$ 从 $\mathcal{N}$ 可证.”

回忆 3.6.4 小节中的定义，递归函数 Num 和 Sub 分别满足

$$\mathrm{Num}(n)=\mathrm{g}(\overline{n}),$$

$$\mathrm{Sub}(\mathrm{g}(x_i),\mathrm{g}(t),\mathrm{g}(p(x_i)))=\mathrm{g}(p(t)).$$

现用 Sub 和 Num 定义出一个新的二元递归函数 Su:

$$\mathrm{Su}(n_1,n_2)=\mathrm{Sub}(\mathrm{g}(x_1),\mathrm{Num}(n_1),n_2),\ \text{其中}\ \mathrm{g}(x_1)=2^{17}.$$

Su 满足

$$\mathrm{Su}(n_1,\mathrm{g}(p(x_1)))=\mathrm{g}(p(\overline{n_1})).$$

设 Su 用公式 $\mathrm{su}(x_1,x_2,y)$ 可表示.

**引理 2 (对角线引理)** 对于任一以 $x_1$ 为仅有的自由变元的公式 $p(x_1)$, 必定存在闭式 $q_0$ 满足

$$\mathcal{N}\vdash q_0 \leftrightarrow p(\ulcorner q_0 \urcorner).$$

(我们把具有这种性质的 $q_0$ 叫做公式 $p(x_1)$ 的不动点.)

**证** 记

$$r(x_1)=\exists y(p(y)\wedge \mathrm{su}(x_1,x_1,y)),$$

$$m=\mathrm{g}(r(x_1)),$$

$$q_0=r(\overline{m}),$$

$$k=\mathrm{g}(q_0).$$

我们来证明 $q_0$ 即为所求的 $p(x_1)$ 不动点.

按 Su 的定义，有

$$\mathrm{Su}(m,m)=\mathrm{g}(r(\overline{m}))=k,$$

$$\mathcal{N}\vdash \mathrm{su}(\overline{m},\overline{m},\overline{k}).$$

于是有

$$\mathcal{N}\cup\{p(\overline{k})\}\vdash p(\overline{k})\wedge \mathrm{su}(\overline{m},\overline{m},\overline{k}),$$

$$\mathcal{N}\cup\{p(\overline{k})\}\vdash \exists y(p(y)\wedge \mathrm{su}(\overline{m},\overline{m},y)), \qquad (\text{用了 } \exists_1 \text{ 规则})$$

右端就是 $q_0(=r(\overline{m}))$. 这就证明了所要证的一半:

$$\mathcal{N}\vdash p(\overline{k})\rightarrow q_0 \ \text{ 即 }\ p(\ulcorner q_0 \urcorner)\rightarrow q_0. \qquad (\text{按约定，}\ulcorner q_0 \urcorner=\overline{\mathrm{g}(q_0)})$$

已设 Su 是用 su $(x_1,x_2,y)$ 表示的，故有

$$\mathcal{N}\vdash \mathrm{su}(\overline{m},\overline{m},y)\rightarrow y\approx\overline{k}.$$

(注意 $\mathrm{Su}(m,m)=k$ 及 3.3.1 小节定义 1 (iii))

由此可得

$$\mathcal{N}\cup\{p(y)\wedge \mathrm{su}(\overline{m},\overline{m},y)\}\vdash p(\overline{k}).$$

用 $\exists_2$ 规则，又得

$$\mathcal{N}\cup\{\exists y(p(y)\wedge \mathrm{su}(\overline{m},\overline{m},y))\}\vdash p(\overline{k}),$$

此即 $\mathcal{N}\cup\{q_0\}\vdash p(\ulcorner q_0\urcorner)$. □

现再引入一个新的二元关系 PRF*：

PRF* = $\{(n_1,n_2)\mid n_1=\mathrm{g}(q),\ n_2$ 是 $\mathrm{pr}(\overline{n_1})\to\neg q$ 从 $\mathcal{N}$ 的证明的 Gödel 数$\}$.

PRF* 是递归的，因为 (记 $\alpha_0=\mathrm{g}(\mathrm{pr}(x_1))$)

$$C_{\mathrm{PRF}^*}(n_1,n_2)=C_{\mathrm{FM}}(n_1)\times C_{\mathrm{PRF}}(2^9*\mathrm{Su}(n_1,\alpha_0)*2^7*n_1,n_2).$$

设 PRF* 用公式 $\mathrm{prf}^*(x_1,x_2)$ 表示，并记

$$\mathrm{pr}^*(x_1)=\exists x_2\,\mathrm{prf}^*(x_1,x_2).$$

引入记号 $\mathrm{con}_{\mathcal{N}}$：

$$\mathrm{con}_{\mathcal{N}}=\forall x_1\neg(\mathrm{pr}(x_1)\wedge \mathrm{pr}^*(x_1)).$$

按 PRF 与 PRF* 的定义不难理解，公式 $\mathrm{con}_{\mathcal{N}}$ 的直观意思是“$\mathcal{N}$ 无矛盾”：“任何公式 $q$ 都不会使 $\mathcal{N}\vdash q$ 与 $\mathcal{N}\vdash \mathrm{pr}(\ulcorner q\urcorner)\to\neg q$ 同时成立”，或（注意引理 1）“任何公式 $q$ 都不会使 $\mathcal{N}\vdash q$ 与 $\mathcal{N}\vdash\neg q$ 同时成立”.

现考察公式 (1):

(1) $\mathrm{pr}(x_1)\ \to\ \mathrm{pr}^*(x_1)$,

其中 $x_1$ 是它仅有的自由变元. 按对角线引理 (引理 2)，可取出公式 (1) 的不动点 $q_0$，它满足:

(2) $\mathcal{N}\vdash\ q_0\leftrightarrow(\mathrm{pr}(\ulcorner q_0\urcorner)\to\mathrm{pr}^*(\ulcorner q_0\urcorner))$.

利用这个不动点 $q_0$, 我们来证明下面的定理 1——Gödel 第二不完备性定理的一种易证形式:

**定理 1** 若 $\mathcal{N}$ 无矛盾，则 $\mathcal{N}\nvdash\mathrm{con}_{\mathcal{N}}$.

**证** 反设 $\mathcal{N}\vdash\mathrm{con}_{\mathcal{N}}$, 即 $\mathcal{N}\vdash\forall x_1\neg(\mathrm{pr}(x_1)\wedge\mathrm{pr}^*(x_1))$.

由此可得

(3) $\mathcal{N}\vdash\neg(\mathrm{pr}(\ulcorner q_0\urcorner)\wedge\mathrm{pr}^*(\ulcorner q_0\urcorner))$,

其中 $q_0$ 取为 (1) 的不动点. 注意永真式 $\neg(p\wedge q)\leftrightarrow(p\to\neg q)$, 由 (3) 可得

(4) $\mathcal{N}\cup\{\mathrm{pr}(\ulcorner q_0\urcorner),q_0\}\vdash\neg\mathrm{pr}^*(\ulcorner q_0\urcorner)$.

由 (2) 可得

(5) $\mathcal{N}\cup\{\mathrm{pr}(\ulcorner q_0\urcorner),q_0\}\vdash\mathrm{pr}^*(\ulcorner q_0\urcorner)$.

由 (4)，(5) 用归谬律便得

$$\mathcal{N}\cup\{\mathrm{pr}(\ulcorner q_0\urcorner)\}\vdash\neg q_0,$$

$$\mathcal{N}\vdash\ \mathrm{pr}(\ulcorner q_0\urcorner)\to\neg q_0.$$

此时取 $k$ 为 $\mathrm{pr}(\ulcorner q_0 \urcorner) \to \neg q_0$ 从 $\mathcal{N}$ 的一个证明的 Gödel 数. 按二元关系 PRF* 的定义，有

$$(\mathrm{g}(q_0), k) \in \mathrm{PRF}^*. \qquad (注意 \ulcorner q_0 \urcorner = \overline{\mathrm{g}(q_0)})$$

已设 PRF* 用公式 $\mathrm{prf}^*(x_1 x_2)$ 可表示，故有

$$\mathcal{N} \vdash \mathrm{prf}^*(\ulcorner q_0 \urcorner, \bar{k}),$$

$$\mathcal{N} \vdash \exists x_2\, \mathrm{prf}^*(\ulcorner q_0 \urcorner, x_2), \qquad (用了 \exists_1 规则)$$

此即

(6) $\mathcal{N} \vdash \mathrm{pr}^*(\ulcorner q_0 \urcorner)$.

由 (6) 用 (K1) 及 MP 又得

$$\mathcal{N} \vdash \mathrm{pr}(\ulcorner q_0 \urcorner) \to \mathrm{pr}^*(\ulcorner q_0 \urcorner).$$

由此及 $q_0$ 的不动点性质 (2) 即得 $\mathcal{N} \vdash q_0$, 进而由引理 1 得

(7) $\mathcal{N} \vdash \mathrm{pr}(\ulcorner q_0 \urcorner)$.

最后由 (6)，(7) 得 $\mathcal{N} \vdash \mathrm{pr}(\ulcorner q_0 \urcorner) \wedge \mathrm{pr}^*(\ulcorner q_0 \urcorner)$, 这与 (3) 矛盾. □

我们说定理 1 是一种易证形式，是因为在它的证明过程中仅用了易证的第一可推性条件 (引理 1)

D.1 $\quad \mathcal{N} \vdash q \quad \Rightarrow \quad \mathcal{N} \vdash \mathrm{pr}(\ulcorner q \urcorner)$,

而未用到另外两个证明较难的第二与第三可推性条件:

D.2 $\quad \mathcal{N} \vdash \mathrm{pr}(\ulcorner q \urcorner) \to \mathrm{pr}(\ulcorner \mathrm{pr}(\ulcorner q \urcorner) \urcorner)$,

D.3 $\quad \mathcal{N} \vdash \mathrm{pr}(\ulcorner q \to r \urcorner) \to (\mathrm{pr}(\ulcorner q \urcorner) \to \mathrm{pr}(\ulcorner r \urcorner))$.

如果假定 D.2 和 D.3 也成立，那么可以证明

$$\mathcal{N} \vdash \neg(\mathrm{pr}(\ulcorner q_0 \urcorner) \wedge \mathrm{pr}^*(\ulcorner q_0 \urcorner)) \leftrightarrow \neg\, \mathrm{pr}(\ulcorner \bar{0} \not\approx \bar{0} \urcorner).$$

这时，Gödel 第二不完备定理的一种通常的形式

$$\text{“}\mathcal{N} \nvdash \neg\, \mathrm{pr}(\ulcorner \bar{0} \not\approx \bar{0} \urcorner)\text{”}$$

与这里的定理 1 等价.

## 4.2 形式算术的不可判定性定理

作为 Gödel-Rosser 定理的推论，已经证明 TR——$K_{\mathrm{N}}$ 在 **N** 中恒真公式 Gödel 数全体构成的集——是非递归集 (见练习 38 题 1). 按照 Church 论题，不存在算法能用来确定任给的公式是否在 **N** 中恒真. 我们把这个事实叫做 $K_{\mathrm{N}}$ 的语义不可判定性.

本节讨论的 $K_{\mathrm{N}}$ 的不可判定性，指的是语法不可判定性.

把从 $\mathcal{N}$ 可证的公式 Gödel 数全体构成的集记作 TH:

$$\mathrm{TH} = \{ \mathrm{g}(p) \mid \mathcal{N} \vdash p \}.$$

由谓词演算的可靠性定理立即可知

$$\mathrm{TH} \subseteq \mathrm{TR}.$$

**定理 1 ($K_{\mathrm{N}}$ 的不可判定性)** 若 $\mathcal{N}$ 无矛盾，则 TH 是非递归集.

**证** 反设 TH 是递归的，并设它用公式 $p(x_1)$ 可表示:

$$n \in \mathrm{TH} \quad \Rightarrow \quad \mathcal{N} \vdash p(\overline{n});$$

$$n \notin \mathrm{TH} \quad \Rightarrow \quad \mathcal{N} \vdash \neg p(\overline{n}).$$

作一元递归函数 $f$:

$$f(n) = \mathrm{Sub}(2^{15+2}, \mathrm{Num}(n), n),$$

其中 $\mathrm{Num}(n) = \mathrm{g}(\overline{n})$ 即 $\overline{n}$ 的 Gödel 数. 如果 $n$ 是某公式的 Gödel 数，那么 $f(n)$ 就是用 $\overline{n}$ 去替换该公式中所有自由的 $x_1$ 所得结果的 Gödel 数.

设一元递归函数 $f$ 用公式 $s(x_1, y)$ 可表示:

$$\mathcal{N} \vdash s(\overline{n}, \overline{f(n)}),$$

$$\mathcal{N} \vdash s(\overline{n}, t) \to t \approx \overline{f(n)}. \qquad \text{(见 3.3.1 小节命题 1)}$$

记

$$\mathrm{r}(x_1) = \forall x_2 (s(x_1, x_2) \to \neg p(x_2)),$$

$$m = \mathrm{g}(\mathrm{r}(x_1)),$$

$$k = \mathrm{g}(\mathrm{r}(\overline{m})).$$

按 $f$ 的定义，$f(m) = k$. 由此可得

(1) $\mathcal{N} \vdash s(\overline{m}, \overline{k})$,

(2) $\mathcal{N} \vdash s(\overline{m}, x_2) \to x_2 \approx \overline{k}$.

注意:

(3) $\mathrm{r}(\overline{m}) = \forall x_2 (s(\overline{m}, x_2) \to \neg p(x_2))$,

它也是一个断言自己不可证的具有自相关特点的公式. 下面当我们实际考察它的可证性时，便立即出现矛盾.

先假设 $\mathcal{N} \vdash \mathrm{r}(\overline{m})$, 即 $k \in \mathrm{TH}$. 于是

(4) $\mathcal{N} \vdash p(\overline{k})$ 已设 TH 用 $p(x_1)$ 表示

注意 (3)，用 (K4) 及 MP 可得

$$\mathcal{N} \vdash s(\overline{m}, \overline{k}) \to \neg p(\overline{k}).$$

由此及 (1) 又得 $\mathcal{N} \vdash \neg p(\overline{k})$, 与 (4) 相矛盾.

再假设 $\mathrm{r}(\overline{m})$ 从 $\mathcal{N}$ 不可证，即 $k \notin \mathrm{TH}$. 于是有

(5) $\mathcal{N} \vdash \neg p(\overline{k})$ TH 用 $p(x_1)$ 表示

(6) $\mathcal{N} \vdash \overline{k} \approx x_2 \to (\neg p(\overline{k}) \to \neg p(x_2))$ 等项替换

(7) $\mathcal{N} \vdash \overline{k} \approx x_2 \to \neg p(x_2)$

(由 (5)，(6) 及永真式 $q \to ((p \to (q \to r)) \to (p \to r))$)

(8) $\mathcal{N} \vdash s(\overline{m}, x_2) \to \neg p(x_2)$ (2)，(7)，HS

(9) $\mathcal{N} \vdash \forall x_2 (s(\overline{m}, x_2) \to \neg p(x_2))$ (8)，Gen

此即 $\mathcal{N} \vdash \mathrm{r}(\overline{m})$, 与假设 ($\mathrm{r}(\overline{m})$ 从 $\mathcal{N}$ 不可证) 相矛盾.

不管假设 $\mathrm{r}(\overline{m})$ 从 $\mathcal{N}$ 可证还是不可证，都出现矛盾. 所以开头所作 TH 是递归集的假设错了. □

按照 CHurch 论题，定理 1 指出，不存在算法可用来确定 $K_{\mathrm{N}}$ 中任意给定的公式是否从 $\mathcal{N}$ 可证. 确定任给的某个公式是不是 Peano 形式算术的定理，不可能有统一的算法可以依靠.

尝试对 $K_{\mathrm{N}}$ 和 $\mathcal{N}$ 作如下改变:

(i) 扩大 $K_{\mathrm{N}}$ 的字母表以增加 $K_{\mathrm{N}}$ 的语言，但使新的系统保持 TM，FM，Sub 的递归性;

(ii) 增加 $K_{\mathrm{N}}$ 的推理规则且使 $\mathcal{N}$ 递归无矛盾地扩张成 $\mathcal{N}^*$.

作了这些改变之后，对于新的系统，定理 1 的证明仍然适用，定理 1 的结论仍然正确，新的形式理论仍然是不可判定的. 这是因为所有上述变动并不改变递归函数具有可表示性这一基本事实.

## 练习 39

1. 3.6.4 小节命题 8-3° 指出集

$$\mathrm{PF} = \{n \mid n \text{ 是从 } \mathcal{N} \text{ 的证明的 Gödel 数}\}$$

是递归集. 现用它的算法逐一列出它的全体成员:

$$n_1, n_2, n_3, \cdots$$

然后算出

$$(*) \qquad (n_1)_{\mathrm{lh}(n_1) \dot{-} 1},\ (n_2)_{\mathrm{lh}(n_2) \dot{-} 1},\ (n_3)_{\mathrm{lh}(n_3) \dot{-} 1},\ \cdots$$

对任一 $m \in \mathbf{N}$, 若 $m$ 在 (*) 中出现，则 $m \in \mathrm{TH}$; 若 $m$ 不在 (*) 中出现，则 $m \notin \mathrm{TH}$. 这是否给出了计算 TH 成员的算法从而说明 TH 是递归集?

# 4.3 递归可枚举集与算术集

现在已经知道 TR (在 **N** 中恒真的公式 Gödel 数全体的集) 和 TH (从 $\mathcal{N}$ 可证的公式 Gödel 数全体的集) 都是非递归集，而且它们之间有区别: 不完备性定理已经证明 TR 和 TH 并不是同一集合. 下面将续继讨论它们之间的差异，从另一角度更深入地认识不完备性定理.

## 4.3.1 可证公式集的递归可枚举性

**定义 1 (递归可枚举集)** 空集以及一元递归函数的值域叫做递归可枚举集.

按此定义，非空集 $A$ 是递归可枚举集，意味着存在一元递归函数 $f$ 使

$$A = \{a \mid \text{有某个 } n \in \mathbf{N} \text{ 使 } a = f(n)\}.$$

根据 Church 论题，存在算法用来计算 $f$ 这个递归函数的函数值，从而能把 $A$ 的成员一个不漏 (但允许重复) 地全部枚举出来:

$$f(0),\ f(1),\ f(2),\ \cdots$$

枚举允许重复，是因为 $f$ 这个递归函数可以不是单射.

首先来讨论递归可枚举集与递归集的关系.

**命题 1** 递归集一定是递归可枚举集.

**证** 设 $A$ 是递归集，且 $A \neq \varnothing$. 任意取出 $A$ 的元素 $a_0$. 取定 $a_0$ 之后，下式定义的递归函数 $f$ 的值域就是 $A$:

$$f(n) = n\,C_A(n) + a_0\,\overline{\mathrm{sg}}(C_A(n)). \qquad \square$$

直观地说，用计算 $C_A$ 的算法逐一计算函数值 $C_A(0)$, $C_A(1)$, $\cdots$, 取出所有使 $C_A(n)$ 为 1 的 $n$, 就枚举出 $A$ 的所有成员来.

命题 1 的逆命题不成立. 非递归的递归可枚举集是存在的，TH 就是这种集的重要例子.

**定理 1** TH 是递归可枚举集.

**证** 任取 $m \in$TH. (比如取 $m$ 为某一公理的 Gödel 数.) 作递归函数 $f$:

$$f(n) = (n)_{\mathrm{lh}(n) \dot{-} 1} \times C_{\mathrm{PF}}(n) + m\overline{\mathrm{sg}}(C_{\mathrm{PF}}(n)).$$

$f$ 的值域给出了 TH. $\square$

直观地说，利用 $C_{\mathrm{PF}}$ 的算法，逐一拿出从 $\mathcal{N}$ 的证明文章 (公式的有限序列)，取出文章的最后一个公式，这样便可枚举出所有从 $\mathcal{N}$ 可证的公式.

对定理 1 可作与以前类似的说明. 定理 1 是针对 $K_{\mathrm{N}}$ (以 $\mathcal{N}$ 为公理集) 建立的. 但不管是扩大 $K_{\mathrm{N}}$ 的语言，增加它的推理规则，还是扩张它的公理集，只要保持 PF

的递归性 (使得可以用算法来确定任一篇文章是不是一篇证明，从而可称该系统是"递归可公理化"的)，那么定理 1 的证明表明，该形式系统所有定理 (即可证公式) 的 Gödel 数构成的集就一定是递归可枚举集.

一句话，可证公式 (Gödel 数) 集的递归可枚举性是递归可公理化形式系统共有的基本性质.

非递归可枚举集是存在的. TH 是递归可枚举的非递归集，TH 的余集 $\overline{\mathrm{TH}}$ 就不能是递归可枚举集，理由是:

**命题 2** 若 $A$ 和 $A$ 的余集 $\overline{A}$ 都是递归可枚举集，则 $A$ 是递归集. (这里 $\overline{A} = \mathbf{N}-A$.)

**证** 设 $A$ 和 $\overline{A}$ 都是非空集.($A = \varnothing$ 或 $\overline{A} = \varnothing(A = \mathbf{N})$ 时 $A$ 自然都是递归集.) 再设 $A$ 是一元递归函数 $f$ 的值域，$\overline{A}$ 是一元递归函数 $h$ 的值域. 于是 $A$ 的递归性由下式给出:

$$C_A(n) = \overline{\mathrm{sg}}(n \mathbin{\dot{-}} f(\mu x[(f(x) \mathbin{\dot{-}} n)(h(x) \mathbin{\dot{-}} n) = 0])),$$

其中 $\mu$ 算子的根存在性条件是满足的: 对任何 $n$, 若 $n \in A$, 则存在 $x$ 使 $f(x) = n$; 若 $n \in \overline{A}$, 则存在 $x$ 使 $h(x) = n$. □

$\overline{\mathrm{TH}}$ 不是递归可枚举集. 否则由命题 2，TH 就成了递归集.

由 0.3 节的 Cantor 定理知道，$\mathbf{N}$ 的幂集 $\mathcal{P}(\mathbf{N})$ (即 $\mathbf{N}$ 的所有子集构成的集) 是不可数的无限集. 它是个层次万千的世界. 所有 $\mathbf{N}$ 的有限子集是它的很小一部分成员. 所有递归集和所有递归可枚举集在 $\mathcal{P}(\mathbf{N})$ 内部占据的范围越来越大，但也都只占 $\mathcal{P}(\mathbf{N})$ 内部很小的一部分. $\overline{\mathrm{TH}}$ 超出了这部分的范围. 我们将要证明 TR 也超出了这部分的范围. 不仅如此，还将证明在 $\mathcal{P}(\mathbf{N})$ 中，TR 与 $\overline{\mathrm{TH}}$ 分属于另外的性质不同的层次—— $\overline{\mathrm{TH}}$ 是算术集，而 TR 超出了算术集的范围.

## 练习 40

1. 证明所有递归可枚举集构成可数集.

2. 设 $A$ 是递归可枚举的无限集，且存在递增的递归枚举，即存在递增的递归函数给出了 $A$ 的全部成员的枚举: $f(0), f(1), f(2), \cdots$, 列中 $f(n) < f(n+1)$. 求证 $A$ 是递归集.

3. 证明每个递归可枚举的无限集都有递归的无限子集.

4. 证明递归可枚举集必为某个递归偏函数的定义域.

5. 求证: $A$ 是递归可枚举集，当且仅当 $A = \varnothing$ 或 $A$ 是某个 $k$ 元递归函数的值域，$k \geqslant 1$.

### 4.3.2 递归可枚举集的算术可定义性

下面引进算术集的概念，讨论它和递归集、递归可枚举集之间的关系.

**定义 1 (算术可定义函数)** $k$ 元函数 $f$ 是算术可定义函数，指存在着 $K_N$ 的含有 $k+1$ 个自由变元的公式 $p(x_1,\cdots,x_k,y)$, 对任意 $n_1,\cdots,n_k,m\in\mathbf{N}$, 满足

$$f(n_1,\cdots,n_k)=m \quad\Leftrightarrow\quad |p(\overline{n_1},\cdots,\overline{n_k},\overline{m})|_{\mathbf{N}}=1.$$

此时说 $f$ 用公式 $p(x_1,\cdots,x_k,y)$ 在 $K_N$ 中可定义.

**定义 2 (算术关系和算术集)** $k$ 元关系 $R$ 是算术可定义关系 (简称为算术关系), 指存在着 $K_N$ 的含有 $k$ 个自由变元的公式 $p(x_1,\cdots,x_k)$, 对任意 $n_1,\cdots,n_k\in\mathbf{N}$, 满足

$$(n_1,\cdots,n_k)\in R \quad\Leftrightarrow\quad |p(\overline{n_1},\cdots,\overline{n_k})|_{\mathbf{N}}=1.$$

此时说 $R$ 用公式 $p(x_1,\cdots,x_k)$ 在 $K_N$ 中可定义. 一元算术关系简称为算术集.

由定义可见，算术可定义性与 $K_N$ 的语义有关，而可表示性则只与 $K_N$ 的语法有关. 往下的讨论在涉及 $K_N$ 的语义时，注意常用到以下结论: $\mathbf{N}$ 是 $\mathcal{N}$ 的模型.

**命题 1** 可表示导致算术可定义. 详细地说: 可表示函数也是可定义的，且所用的公式相同; 可表示关系也是用相同的公式可定义的.

**证** 设 $k$ 元函数 $f$ 用公式 $p(x_1,\cdots,x_k,y)$ 可表示，那么当 $f(n_1,\cdots,n_k)=m$ 时，有

$$\begin{aligned}
&\mathcal{N}\vdash p(\overline{n_1},\cdots,\overline{n_k},\overline{m}), && (f \text{ 用 } p \text{ 可表示})\\
&\mathcal{N}\vDash p(\overline{n_1},\cdots,\overline{n_k},\overline{m}), && (K_N \text{ 的可靠性})\\
&|p(\overline{n_1},\cdots,\overline{m})|_{\mathbf{N}}=1;
\end{aligned}$$

当 $f(n_1,\cdots,n_k)\neq m$ 时，有

$$\begin{aligned}
&\mathcal{N}\vdash \neg p(\overline{n_1},\cdots,\overline{n_k},\overline{m}), && (f \text{ 用 } p \text{ 可表示})\\
&\mathcal{N}\vDash \neg p(\overline{n_1},\cdots,\overline{n_k},\overline{m}), && (K_N \text{ 的可靠性})\\
&|\neg p(\overline{n_1},\cdots,\overline{n_k},\overline{m})|_{\mathbf{N}}=1,\\
&|p(\overline{n_1},\cdots,\overline{n_k},\overline{m})|_{\mathbf{N}}=0.
\end{aligned}$$

这说明 $f$ 在 $K_N$ 中用 $p(x_1,\cdots,x_k,y)$ 可定义.

再设 $k$ 元关系 $R$ 用 $p(x_1,\cdots,x_k)$ 可表示. 于是

$$\begin{aligned}
(n_1,\cdots,n_k)\in R &\Rightarrow \mathcal{N}\vdash p(\overline{n_1},\cdots,\overline{n_k})\\
&\Rightarrow |p(\overline{n_1},\cdots,\overline{n_k})|_{\mathbf{N}}=1;\\
(n_1,\cdots,n_k)\notin R &\Rightarrow \mathcal{N}\vdash \neg p(\overline{n_1},\cdots,\overline{n_k})\\
&\Rightarrow |p(\overline{n_1},\cdots,\overline{n_k})|_{\mathbf{N}}\neq 1.
\end{aligned}$$

这说明 $R$ 用 $p(x_1,\cdots,x_k)$ 可定义. □

命题 1 的另一种说法是: 递归导致算术可定义，即

**推论 1** 递归函数必为算术可定义函数，递归关系必为算术可定义关系. 作为后者的特殊情形，递归集必为算术集.

事实上还可进一步得到:

**定理 1** 递归可枚举集必为算术集.

**证** 易知 $\varnothing$ 是算术集. 设 $A$ 是非空递归可枚举集，并设它是一元递归函数 $f$ 的值域. 再设 $f$ 用公式 $p(x_1, y)$ 表示. 根据命题 1，$f$ 用 $p(x_1, y)$ 可定义.

下面证明集 $A$ 用公式 $\exists x\, p(x, x_1)$ 可定义 (因而是算术集)，即 $A$ 满足

$$n \in A \quad \Leftrightarrow \quad |\exists x\, p(x, \overline{n})|_{\mathbf{N}} = 1.$$

($\Rightarrow$) 设 $n \in A$. 因 $A$ 是 $f$ 的值域，故存在 $m \in \mathbf{N}$ 使 $f(m) = n$, 由此 (注意 $f$ 用 $p(x_1, y)$ 可定义) 知

$$|p(\overline{m}, \overline{n})|_{\mathbf{N}} = 1.$$

此时对任意项解释 $\varphi \in \Phi_{\mathbf{N}}$, 都有

$$|p(\overline{m}, \overline{n})|(\varphi) = 1.$$

取 $\varphi$ 的 $x$ 变通 $\varphi'$ 使之满足 $\varphi'(x) = m$. 因

$$\varphi(\overline{m}) = m = \varphi'(x), \qquad \text{(见 3.2 节定义 1 前的说明)}$$

故由 2.3 节引理 1-2° 可得

$$|p(x, \overline{n})|(\varphi') = |p(\overline{m}, \overline{n})|(\varphi) = 1.$$

再由 2.2.2 小节命题 1-4° 便得

$$|\exists x\, p(x, \overline{n})|(\varphi) = 1.$$

$\varphi$ 是任意的，于是有 $|\exists x\, p(x, \overline{n})|_{\mathbf{N}} = 1$.

($\Leftarrow$) 设 $|\exists x\, p(x, \overline{n})|_{\mathbf{N}} = 1$, 则有以下结论:

任取 $\varphi \in \Phi_{\mathbf{N}}$, 有 $|\exists x\, p(x, \overline{n})|(\varphi) = 1$,

存在 $\varphi$ 的 $x$ 变通 $\varphi'$ 使 $|p(x, \overline{n})|(\varphi') = 1$,

记 $\varphi'(x) = m$, 则有 $|p(\overline{m}, \overline{n})|(\varphi) = |p(x, \overline{n})|(\varphi') = 1$,

(由 2.3 节引理 1-2° 及 $\varphi(\overline{m}) = m = \varphi(x')$)

存在 $m$ 使 $|p(\overline{m}, \overline{n})|_{\mathbf{N}} = 1$, (注意 $p(\overline{m}, \overline{n})$ 是闭式)

存在 $m$ 使 $f(m) = n$, ($f$ 用 $p(x_1, y)$ 可定义)

$n \in A$. ($A$ 是 $f$ 的值域)

□

把 4.3.1 小节定理 1 和本段定理 1 结合起来，便可得出结论: TH 是递归可枚举集，因而是算术集.

定理 1 之逆并不正确. 不是递归可枚举集，但可能是算术集. 换句话说，算术集的类要比递归可枚举集的类更大. 下面的命题 2 蕴涵了这一事实.

已经知道，TH 是递归可枚举集而 $\overline{\text{TH}}$ 不是递归可枚举集.

**命题 2** TH 和 $\overline{\text{TH}}$ 都是算术集.

**证** TH 是递归可枚举集，所以是算术集. 设 TH 用公式 $p(x_1)$ 可定义. $\overline{\text{TH}}$ 也是算术集，因为 $\overline{\text{TH}}$ 用公式 $\neg p(x_1)$ 可定义:

$$n \in \overline{\mathrm{TH}} \iff n \notin \mathrm{TH}$$
$$\iff |p(\bar{n})|_{\mathrm{N}} = 0 \qquad (\mathrm{TH}\text{ 用 } p(x_1)\text{ 可定义})$$
$$\iff |\neg p(\bar{n})|_{\mathrm{N}} = 1. \qquad \square$$

## 练习 41

1. 含有 $k+1$ 个自由变元的公式 $p(x_1,\cdots,x_k,y)$ 是否一定可用来定义一个 $k$ 元函数 $f$? 含有 $k$ 个自由变元的公式 $p(x_1,\cdots,x_k)$ 是否一定可用来定义一个 $k$ 元关系 $R$? 请说明理由.

2. 证明: $R$ 是算术关系，当且仅当 $C_R$ 是算术可定义函数.

### 4.3.3 真公式集的非算术可定义性

现在来证明 TR (形式算术 $K_{\mathrm{N}}$ 在 **N** 中恒真公式的 Gödel 数的全体) 是非算术集，因而有

$$\mathrm{TH} \neq \mathrm{TR},$$

这说明 TH 是 TR 的真子集.

仍用 g 表示 Gödel 配数.

**定理 1 ( Tarski)** TR 不是算术集.

**证** 反设 TR 是算术集，并设它用公式 $p(x_1)$ 可定义:

(1) $n \in \mathrm{TR} \iff |p(\bar{n})|_{\mathrm{N}} = 1.$

作一元递归函数 $f$:

$$f(n) = \mathrm{Sub}(2^{15+2},\ \mathrm{Num}(n), n),$$

其中 $\mathrm{Num}(n) = \mathrm{g}(\bar{n})$. 若 $n = \mathrm{g}(q(x_1))$, 则 $f(n) = \mathrm{g}(q(\bar{n}))$.

设 $f$ 用公式 $s(x_1,y)$ 可表示，并令

$$\mathrm{r}(x_1) = \forall y(s(x_1,y) \to \neg p(y)),$$

$$m = \mathrm{g}(\mathrm{r}(x_1)),$$

$$k = \mathrm{g}(\mathrm{r}(\overline{m})),$$

其中

$$\mathrm{r}(\overline{m}) = \forall y(s(\overline{m},y) \to \neg p(y)).$$

按函数 $f$ 的定义，$f(m) = k$. 又因 $f$ 用 $s(x_1,y)$ 可表示，故有

(2) $\mathcal{N} \vdash s(\overline{m},\bar{k})$,

(3) $\mathcal{N} \vdash s(\overline{m},t) \to t \approx \bar{k}$, $t$ 是任意项.

(注 以上我们采用了与在证明 TH 的非递归性时 (见 4.2 节定理 1) 所采用的几

乎相同的程序，也得到了具有自相关特点的公式 $r(\overline{m})$. 不过这里的 $r(\overline{m})$ 有着另一种语义. ( $p(x_1)$ 的内容变了.) 现在我们遇到了“说谎者悖论”. 注意 TR 用 $p(x_1)$ 可定义，$f$ 用 $s(x_1, y)$ 可表示以及 TR 和 $f$ 的定义，可以看到，公式 $r(\overline{m})$ 关于自己的真假自我声明:“我不真!”)

考察 $r(\overline{m})$ 的真假，立即会导致矛盾. 在这之前，先证明结论 (*) :

(*) 若对 $k = f(m)$ 有 $|s(\overline{m},\overline{k}) \to \neg p(\overline{k})|_{\mathrm{N}} = 1$, 则对任意 $n \in \mathbf{N}$, 总有

$$|s(\overline{m},\overline{n}) \to \neg p(\overline{n})|_{\mathrm{N}} = 1.$$

对给定的 $n$, 若 $|s(\overline{m},\overline{n})|_{\mathrm{N}} = 0$, 当然有

$$|s(\overline{m},\overline{n}) \to \neg p(\overline{n})|_{\mathrm{N}} = 1,$$

所以，为了证明结论 (*), 可设 $|s(\overline{m},\overline{n})|_{\mathrm{N}} = 1$. 由 (3) 有

$$\mathcal{N} \vdash s(\overline{m},\overline{n}) \to \overline{n} \approx \overline{k},$$

由此得 $|s(\overline{m},\overline{n}) \to \overline{n} \approx \overline{k})|_{\mathrm{N}} = 1$, 进而有:

$|\overline{n} \approx \overline{k}|_{\mathrm{N}} = 1$,

对任一项解释 $\varphi \in \Phi_{\mathrm{N}}$, $\varphi(\overline{n}) = \varphi(\overline{k})$,

$n = k$, (注意 3.2 节定义 1 前的说明: $\varphi(\overline{n}) = n$)

$|s(\overline{m},\overline{n}) \to \neg p(\overline{n})|_{\mathrm{N}} = 1$.

这就证明了结论 (*).

现在来考察 $r(\overline{m})$ 的真假. 我们有

$|r(\overline{m})|_{\mathrm{N}} = 1 \quad \Leftrightarrow \quad |\forall y(s(\overline{m},y) \to \neg p(y))|_{\mathrm{N}} = 1$

$\Leftrightarrow \quad |s(\overline{m},y) \to \neg p(y)|_{\mathrm{N}} = 1$ (2.2.3 小节命题 2)

$\Leftrightarrow$ 对任意项解释 $\varphi \in \Phi_{\mathrm{N}}$, $|s(\overline{m},y) \to \neg p(y)|(\varphi) = 1$

$\Leftrightarrow$ 对任意 $n \in \mathbf{N}$, 有某个项解释 $\varphi \in \Phi_{\mathrm{N}}$ 使 $|s(\overline{m},\overline{n}) \to \neg p(\overline{n})|(\varphi) = 1$

(由 2.3 节引理 1-2° 及 $\varphi(\overline{n}) = n$)

$\Leftrightarrow$ 对任意 $n \in \mathbf{N}$, $|s(\overline{m},\overline{n}) \to \neg p(\overline{n})|_{\mathrm{N}} = 1$

($s(\overline{m},\overline{n}) \to \neg p(\overline{n})$ 是闭式)

$\Leftrightarrow \quad |s(\overline{m},\overline{k}) \to \neg p(\overline{k})|_{\mathrm{N}} = 1$ (用结论 (*))

$\Leftrightarrow \quad |\neg p(\overline{k})|_{\mathrm{N}} = 1$ (由 (2) 知 $|s(\overline{m},\overline{k})|_{\mathrm{N}} = 1$)

$\Leftrightarrow \quad |p(\overline{k})|_{\mathrm{N}} = 0$

$\Leftrightarrow \quad k \notin \mathrm{TR}$ (由 (1))

$\Leftrightarrow \quad |r(\overline{m})|_{\mathrm{N}} = 0.$ (TR 的定义及 $k = g(r(\overline{m}))$)

矛盾的根源是假定了“TR 是算术集”. □

Tarski 定理的意思是:“算术真”是“算术不可定义的”. 有了 Tarski 定理，我们对不完备性定理便有了更进一步的认识. 形式算术 $K_{\mathrm{N}}$ 中，从 $\mathcal{N}$ 可证公式 Gödel 数

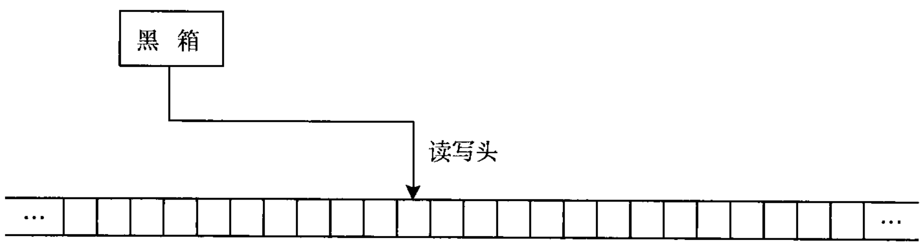
的集 TH 不但是算术集. 而且还是递归可枚举集; 真公式 Gödel 数的集 TR 不但不是递归可枚举集，而且连算术集也不是. 这些事实指出了 TH 和 TR 二着之间有着相当大的差距.

## 4.4 Turing 机与 Turing 论题

从 20 世纪 30 年代起，自 Gödel 不完备性定理问世之后，对定理的持续关注推动人们对递归论与可计算性理论进行了大量深入研究，取得许多重要成果.

按照 Church 论题，递归函数是可计算函数的一种数学模型. 前一章中，我们证明了函数的递归性与函数在 $K_N$ 中的可表示性是同一性质 (3.5 节定理 1 推论 3，3.6 附). 这说明，形式算术 $K_N$ 中的可表示函数也是可计算函数的一种数学模型. 可计算函数还有其他的数学模型，其中最有名的是 Turing (1912~1954) 提出的模型. Turing 在仔细分析人的计算方式和计算过程的基础上提出了 Turing 机的概念.

直观上说，Turing 机的构造是: 一个具有有限内部状态的黑箱通过读写头联系着一条两端可无限延伸的纸带，纸带上是一串 (无限个) 大小相等的方格，在每个方格内都可写上一个取自有限字母表的符号. 读写头每次只瞄准一个方格.




Turing 机的一步动作，指以下三种动作之一:

1° 擦去读写头所瞄方格内原有的符号，然后在该格内写上一个新符号;

2° 读写头向左移动一格;

3° 读写头向右移动一格.

Turing 机的一步计算是指由当时的内部状态和被瞄方格的符号确定出机器的一步动作和下一个内部状态.

字母表中包含一个特殊字母 0. 印着 0 的方格表示空格. 输入的信息是用字母表中的符号印在纸带的有限个方格内，其他方格印 0.

约定开始状态为 $q_0$，读写头开始指着输入纸带最左边的非空格. 按照指令对给定的输入进行一步步计算，停机时纸带便给出了输出信息.

以上对 Turing 机作了一个大概的直观描述. Turing 机不同于一台实际的计算机，是一种抽象的理想计算机，是一个数学概念. 下面我们给出 Turing 机的数学定义.

设 $\Sigma$ 是一有限字母表，其中有 0，还至少有一个非 0 字母；$Q$ 是一有限内部状态集，其中至少有一个内部状态 $q_0$.

带有有限字母表 $\Sigma$ 和有限内部状态集 $Q$ 的 Turing 机 $T$，是指偏映射

$$T:\ Q\times\Sigma \to (\Sigma\cup\{L,R\})\times Q.$$

($T$ 是偏映射，意为它的定义域是 $Q\times\Sigma$ 的子集而不一定是整个 $Q\times\Sigma$.) $T$ 无定义时表示停机. $L$ 表示向左，$R$ 表示向右.

$Q$ 和 $\Sigma$ 都是有限集，故 $T$ 的定义域是有限集. 定义一个 Turing 机，只要给出它所包含的全部四元组便可，四元组 (a，b，c，d) 中 $a,d\in Q$, $b\in\Sigma$, $c\in(\Sigma\cap\{L,R\})$. $(a,b,c,d)$ 简写成 $abcd$. 一个四元组对应着“一步计算”：由当时的内部状态 $a$ 和被瞄方格内的字母 $b$ 确定机器的下一状态 $d$, 并确定机器所采取的由 $c$ 所示的动作: 若 $c\in\Sigma$, 则把方格内的 $b$ 改成 $c$; 若 $c$ 是 $L$, 则读写头左移一格; 若 $c$ 是 $R$, 则读写头右移一格. 下面的例子中，内部状态符号都写在被瞄方格的上方.

**例 1** 设 $\Sigma=\{0,1,A\}$, $Q=\{q_0,q_1\}$, 且设 Turing 机 $T$ 含三个四元组:

$$T=\{q_0\,1\,0\,q_1,\ q_1\,0\,R\,q_0,\ q_0\,A\,0\,q_0\}.$$

列成表格，$T$ 可表示成:

| | 0 | 1 | $A$ |
|---|---|---|---|
| $q_0$ | | $0q_1$ | $0q_0$ |
| $q_1$ | $Rq_0$ | | |

对连续三个 1 接着一个 $A$ 的输入，$T$ 的计算过程如下:

1. $0\ \overset{q_0}{1}\ 1\ 1\ A\ 0$
2. $0\ \overset{q_1}{0}\ 1\ 1\ A\ 0$
3. $0\ 0\ \overset{q_0}{1}\ 1\ A\ 0$
4. $0\ 0\ \overset{q_1}{0}\ 1\ A\ 0$
5. $0\ 0\ 0\ \overset{q_0}{1}\ A\ 0$
6. $0\ 0\ 0\ \overset{q_1}{0}\ A\ 0$
7. $0\ 0\ 0\ 0\ \overset{q_0}{A}\ 0$
8. $0\ 0\ 0\ 0\ \overset{q_0}{0}\ 0$

$T$ 对 $(q_0,0)$ 没有定义，故擦去了三个 1 和 $A$ 后停机. $T$ 是可用于计算一元零函数的 Turing 机.

**例 2** 已知 Turing 机:

| | 0 | 1 | 2 | $X$ | $Y$ |
|---|---|---|---|---|---|
| $q_0$ | | $Xq_0$ | $Yq_0$ | $Rq_0$ | $Rq_0$ |

它只有一个内部状态 $q_0$，字母表 $\Sigma=\{0, 1, 2, X, Y\}$. 对输入 12122，它的计算过程如下 (结果是把 1 和 2 分别改换成 $X$ 和 $Y$):

1. $0\ \overset{q_0}{1}\ 2\ 1\ 2\ 2\ 0$
2. $0\ \overset{q_0}{X}\ 2\ 1\ 2\ 2\ 0$
3. $0\ X\ \overset{q_0}{2}\ 1\ 2\ 2\ 0$
4. $0\ X\ \overset{q_0}{Y}\ 1\ 2\ 2\ 0$
5. $0\ X\ Y\ \overset{q_0}{1}\ 2\ 2\ 0$
6. $0\ X\ Y\ \overset{q_0}{X}\ 2\ 2\ 0$
7. $0\ X\ Y\ X\ \overset{q_0}{2}\ 2\ 0$
8. $0\ X\ Y\ X\ \overset{q_0}{Y}\ 2\ 0$
9. $0\ X\ Y\ X\ Y\ \overset{q_0}{2}\ 0$
10. $0\ X\ Y\ X\ Y\ \overset{q_0}{Y}\ 0$
11. $0\ X\ Y\ X\ Y\ Y\ \overset{q_0}{0}$

**例 3** 加法 Turing 机:

| | 0 | $A$ | 1 |
|---|---|---|---|
| $q_0$ | $Rq_1$ | | $0q_0$ |
| $q_1$ | | $1q_2$ | $Rq_1$ |
| $q_2$ | | | |

计算 $3+2=5$ 的过程是

1. $0\ \overset{q_0}{1}\ 1\ 1\ A\ 1\ 1\ 0$
2. $0\ \overset{q_0}{0}\ 1\ 1\ A\ 1\ 1\ 0$
3. $0\ 0\ \overset{q_1}{1}\ 1\ A\ 1\ 1\ 0$
4. $0\ 0\ 1\ \overset{q_1}{1}\ A\ 1\ 1\ 0$
5. $0\ 0\ 1\ 1\ \overset{q_1}{A}\ 1\ 1\ 0$

$$\begin{array}{l} \qquad\qquad\quad q_2 \\ 6.\quad 0\ 0\ 1\ 1\ 1\ 1\ 1\ 0 \end{array}$$

**例 4** 可做乘法运算的 Turing 机:

| | 0 | 1 | $X$ | $Y$ | $A$ |
|---|---|---|---|---|---|
| $q_0$ | $Rq_9$ | $Xq_1$ | | | |
| $q_1$ | $Rq_2$ | $Rq_1$ | $Rq_1$ | | $0q_1$ |
| $q_2$ | $Lq_7$ | $Yq_3$ | | | |
| $q_3$ | $Rq_4$ | $Rq_3$ | | $Rq_3$ | |
| $q_4$ | $1q_5$ | $Rq_4$ | | | |
| $q_5$ | $Lq_5$ | $Lq_5$ | | $1q_6$ | |
| $q_6$ | | $Rq_2$ | | | |
| $q_7$ | $Lq_7$ | $Lq_7$ | $0q_8$ | | |
| $q_8$ | $Rq_0$ | | | | |
| $q_9$ | | $0q_{10}$ | | | |
| $q_{10}$ | $Rq_9$ | | | | |

它计算 $3\times 2=6$ 的过程是由输入

$$\begin{array}{l} \quad q_0 \\ 0\ 1\ 1\ 1\ A\ 1\ 1\ 0 \end{array}$$

开始，到以下输出停机:

$$\begin{array}{l} q_9 \\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 0 \end{array}$$

**例 5** 对任何输入都不停机的 Turing 机，如

$$T=\{q_0 0 0 q_1,\ q_0 1 0 q_1,\ q_1 0 R q_0\},$$

这里 $\Sigma=\{0,1\}$, $Q=\{q_0,q_1\}$.

借助于 Turing 机，便可以提出 Turing 可计算函数的概念.

采用下面的方法，每个 Turing 机都可用来定义一个一元偏函数 $\varphi$.

不妨设 $T$ 的字母表除含有 0 外还含有 1. 如果以

$$\cdots\cdots 0\,1\,0\,\overbrace{1\,1\cdots 1}^{n\text{个}1}\,0\cdots\cdots$$

的纸带输入 $T$ (简称“以 $n$ 输入 $T$”) 经运算后能停机，则令

$$\varphi(n)=\text{输出纸带上的非空格总数};$$

若不停机，则 $\varphi(n)$ 无定义.

输入纸带上 $n$ 个 1 前面有“$\cdots 010$”，这是为了使自然数 0 作为自变量的值能够输入.

同样，每个 Turing 机 $T$ 也都可用来如下定义一个二元偏函数 $\psi$. 以

$$\cdots\cdots 010\ \overbrace{1\cdots 1}^{m\text{个}1}\ 0\ \overbrace{1\cdots 1}^{n\text{个}1}\ 0\cdots\cdots$$

的纸带输入 $T$(简称“以 $(m,n)$ 输入 $T$”)，若经运算后停机，则令

$$\psi(m,n) = \text{输出纸带上非空格总数};$$

若 $T$ 不停机，则 $\psi(m,n)$ 无定义.

以此类推，每个 Turing 机都可用来定义一个三元、四元 $\cdots\cdots$ 偏函数.

一个数论函数，若存在某个 Turing 机可用来定义它并用来计算它的函数值，就叫做 Turing 可计算函数. 对于偏函数，也同样定义.

Turing 可计算函数当然是算法可计算函数. 反之如何? Turing 对此提出了下面有名的论题.

**Turing 论题:**

$$\text{算法可计算函数} = \text{Turing 可计算函数}.$$

和 Church 论题一样，Turing 论题也是一个经验事实. 值得注意的是，可以严格地证明下面的重要结论:

$$\text{Turing 可计算函数} = \text{递归函数}.$$

就是说，任何 Turing 可计算函数都是递归函数; 而对任何递归函数都可设计出计算它的函数值的 Turing 机.(参见参考文献 [9].)

这个结论和 Turing 论题也适合于偏函数类.

### 练习 42

1. 为以下二元函数设计 Turing 机，并分别给出计算在点 (1，2) 的函数值的过程.

   1° 二元零函数 $\mathrm{z}(n_1,n_2)=0$.

   2° 二元投影函数 $\mathrm{p}_2^2(n_1,n_2)=n_2$.

2. 给出两三种对任何输入都不停机的 Turing 机. ($\Sigma=\{0, 1\}$)

## 4.4 附 停机问题

我们假定所有 Turing 机的字母表都取自一张通用字母表

$$\Sigma^* = \{A_0, A_1, A_2, \cdots\},$$

内部状态符号都取自通用的状态符号集

$$Q^* = \{q_0, q_1, q_2, \cdots\},$$

其中 $A_0$ 对应于“空白”(即前面所用的 0)，$q_0$ 对应于初始内部状态.

如果两个 Turing 机的差别仅在于它们使用的字母符号和内部状态符号不一样，那么我们就把它们视为同一 Turing 机，因为它们实际上进行的是本质上相同的计算.

下面给每个 Turing 机指定码数.

1° 先定义单个符号的码数:

$$\begin{aligned} &\mathrm{g}(L) = 1, \\ &\mathrm{g}(R) = 3, \\ &\mathrm{g}(A_i) = 4i + 5, \\ &\mathrm{g}(q_i) = 4i + 7, \quad i = 0, 1, 2, \cdots. \end{aligned}$$

2° 再定义四元组 $(a, b, c, d)$ 的码数为

$$\mathrm{g}(abcd) = 2^{\mathrm{g}(a)} 3^{\mathrm{g}(b)} 5^{\mathrm{g}(c)} 7^{\mathrm{g}(d)}.$$

3° 最后定义 Turing 机 $T = \{\sigma_0, \sigma_1, \cdots, \sigma_n\}$ ($\sigma_i$ 为四元组) 的码数为

$$\mathrm{g}(T) = 2^{\mathrm{g}(\sigma_0)} 3^{\mathrm{g}(\sigma_1)} \cdots p_n^{\mathrm{g}(\sigma_n)},$$

其中 $p_n$ 是第 $n$ 个素数，并规定 $T$ 中四元组有限序列 $\sigma_0, \sigma_1, \cdots, \sigma_n$ 的排列顺序是自然字典顺序. 例如，$q_1 A_i A_j q_k$ 在 $q_3 A_l A_m q_n$ 前，$q_i A_0 A_j A_k$ 在 $q_i A_4 A_l q_m$ 前，$q_i A_j L q_k$ 在 $q_i A_j R q_l$ 前，$q_i R A_j q_k$ 在 $q_i A_l A_m q_n$ 前，等等.

这样一来，每个 Turing 机都被指定了唯一的码数. 从上面的规定可知，不同的 Turing 机有不同的码数. 进行素幂积分解，我们就可确定任一自然数是不是某个 Turing 机的码数; 若是某个 Turing 机的码数，则可由该自然数将与之对应的 Turing 机的所有指令 (即四元组) 写出来.

4.4 节例 5 中 Turing 机的码数 (0 和 1 分别看成 $\Sigma^*$ 中的 $A_0$ 和 $A_1$) 是

$$2^{2^7 3^5 5^5 7^{11}} 3^{2^7 3^9 5^5 7^{11}} 5^{2^{11} 3^5 5^3 7^7}.$$

按照 Turing 机码数大小，我们可把所有 Turing 机一个不漏地枚举如下:

$$T_0, T_1, T_2, \cdots, T_n, \cdots$$

借助于 Turing 机的这种枚举，我们可以定义出一个一元函数 $f^*$:

$$f^*(n) = \begin{cases} 0, & T_n \text{ 输入 } n \text{ 后会停机}, \\ 1, & T_n \text{ 输入 } n \text{ 后不停机}. \end{cases}$$

下面来证明，$f^*$ 是非 Turing 可计算的，因而是非递归的. 假如 $f^*$ 是 Turing 可计算函数，那么存在某个 Turing 机 $T$ 来计算 $f^*$ 的函数值，即: 对任意 $n \in \mathbf{N}$,

$$f^*(n) = 0 \quad \Leftrightarrow \quad T \text{ 输入 } n \text{ 后输出 } 0,$$

$$f^*(n)=1 \quad \Leftrightarrow \quad T \text{ 输入 } n \text{ 后输出 } 1.$$

注意 $f^*$ 是处处有定义的全函数，故 $T$ 对任何输入都会停机. 利用 $T$ 可构造一个新的 Turing 机 $T'$, 它包含 $T$ 的全部四元组，并增加两个新的内部状态 $q_\alpha, q_\beta\,(\in Q^*)$ 和一个新字母 $A\,(\in \Sigma^*)$, 然后增加新的四元组

$$q_\alpha\, 0\, A\, q_\beta,\ q_\beta\, 0\, A\, q_\alpha,\ q_\alpha\, A\, R\, q_\alpha,\ q_\beta\, A\, L\, q_\beta.$$

此外，对 $T$ 原来没有定义的每个 $q_i\,S$, 增加四元组 $q_i\,S\,R\,q_\alpha$.

将任意 $n\,(\in \mathbf{N})$ 输入 $T'$ 后，按 $T'$ 构造，$T'$ 仍先按 $T$ 的指令动作. 对 $T$ 来说，或输出 0 (空带输出)，或输出 1 (输出纸带上有一个非空格)，取决于 $f^*(n)=0$ 或 $f^*(n)=1$. 对 $T'$ 来说，由新增加的指令决定了机器将继续动作: 若碰上非空格，则 $T'$ 必停机 (说明 $f^*(n)=1$); 若找不到非空格，则 $T'$ 不会停机 (说明 $f^*(n)=0$).

现以 $f^*(n)=0$ 的情形为例来看这个过程.

当 $f^*(n)=0$ 时，以 $n$ 输入 $T'$ :

$$0\ \overset{q_0}{1}\ 0\ \overbrace{1\cdots 1}^{n\text{个}1}\ 0$$

(由此先按 $T$ 的指令动作)

......

$$0\ 0\ 0\ 0\ \overset{q_i}{0}\ 0\ 0\ 0$$

$$0\ 0\ 0\ 0\ 0\ \overset{q_\alpha}{0}\ 0\ 0$$

(至此，$T$ 空带输出，并继续执行 $T'$ 的新指令，来回寻找除 $A$ 外的非空格，故不会停机.)

$$0\ 0\ 0\ 0\ 0\ \overset{q_\beta}{A}\ 0\ 0$$

$$0\ 0\ 0\ 0\ \overset{q_\beta}{0}\ A\ 0\ 0$$

$$0\ 0\ 0\ 0\ \overset{q_\alpha}{A}\ A\ 0\ 0$$

$$0\ 0\ 0\ 0\ A\ \overset{q_\alpha}{A}\ 0\ 0$$

$$0\ 0\ 0\ 0\ A\ A\ \overset{q_\alpha}{0}\ 0$$

$$0\ 0\ 0\ 0\ A\ A\ \overset{q_\beta}{A}\ 0$$

......

$$0\ 0\ 0\ \overset{q_\alpha}{A}\ A\ A\ A\ 0$$

......

总之，结论 (*) 成立:

(*) $T$ 输入 $n$ 后输出 1 $\ \Leftrightarrow\ $ $T'$ 输入 $n$ 后会停机.

$T'$ 必出现在 $T_0, T_1, T_2, \cdots$ 之中. 设 $T'=T_k$. 这样就出现了矛盾:

$T_k$ (即 $T'$) 输入 $k$ 后会停机

$\Leftrightarrow$ $T$ 输入 $k$ 后输出 1 (结论 (*))

$\Leftrightarrow$ $f^*(k)=1$ ($f^*$ 的函数值由 $T$ 计算)

$\Leftrightarrow$ $T_k$ 输入 $k$ 后不停机. ($f^*$ 的定义)

至此证明了 $f^*$ 不是 Turing 可计算函数.

$f^*$ 的非递归性引出了另一个重要结论: 停机问题是不可判定的，即不存在算法对问题类

$$\{\text{Turing 机 } T_m \text{ 在输入 } n \text{ 后是否会停机?} \mid m, n \in \mathbf{N}\}$$

中的问题提供答案. 理由是: 如果存在这样的算法，那么 $f^*$ 也就有了计算其值的算法，从而成了递归函数.

## 4.5 人与机器

在 Gödel 不完备性定理的证明过程中，递归函数起着重要作用. 对形式系统中不完备现象的探究，紧密联系着递归与可计算理论. 我们见到了结论 (3.5 节推论 3 与 3.6 附):

$$\text{在形式算术 } K_{\mathrm{N}} \text{ 中可表示的函数} = \text{递归函数.}$$

我们在 4.1.3 小节和 4.4 节中还见到了两个经验事实:

**Church 论题** 算法可计算函数 = 递归函数.

**Turing 论题** 算法可计算函数 = Turing 可计算函数.

另外 4.4 结尾处还提到一个结论:

$$\text{Turing 可计算函数} = \text{递归函数.}$$

按后面这一结论，Church 论题和 Turing 论题成了等价命题. 或者说，这两个论题给出了可计算函数的等价定义. 此外，人们为可计算函数还建立了不少数学模型，这些模型尽管形式上彼此很不相同，但都给出了相同的函数类——递归函数类. 这说明，不管人们沿着何种途径使可计算性这一概念精确化，至今得到的都是同样的结果. 这就使我们有理由相信，递归函数或 Turing 可计算函数确实给出了可计算函数这个概念很好的数学描述.

简单地说,“算法可计算”就是“人可计算”，而“Turing 可计算”就是“机器可计算”(这里所谈的是理论上的而不是实际上的可计算). 不难理解，凡机器可计算的，也一定是人可计算的 (只要有足够的时间和精力); 反过来，Turing 论题指出，凡是人可以计算的，机器也可以计算. 理论上，就数论函数是否可计算这一点而言，机器与人有相同的能力——这便是 Turing 论题的实质. 几十年来，人们沿着这个方向努力，使计算机事业取得了巨大的进展，这种进展极大地改变了整个人类社会的面貌. 今后人们将会沿着这个方向继续努力.

当我们把可证性与可计算性这两个基本的数学哲学概念加以比较，就会发现可证性没有可计算性所具有的上述那种比较容易把握的稳定性——在试图把可计

算性概念精确化时，得到了不依赖于具体的精确化方式的结果. 关于计算性得到的这种结果是令人比较满意的.

关于可证性，让我们回忆一下前面得到的一些结果.

我们建立形式系统，想把证明的概念精确化. 我们希望所建立的形式系统能够抓住该系统所要描述的具体理论的全部真命题，但同时还要求该系统是“递归可公理化的”，即要求对该系统的任一篇文章能够用机械的算法确定出该文章是不是一篇证明文章. 前面已经证明，上述想法是不能实现的. 从递归无矛盾的公理集出发，在我们建立的形式系统内不可能证明出全部形式化的真命题.

想要达到机器也能鉴别证明，理论便失去了完备性 (只要它的内容不是太贫乏). 这就是不完备性定理得出的结论.

我们还证明了关于形式算术的不可判定性定理，得到了结论: 对算术公理集 $\mathcal{N}$ 或它的无矛盾的扩张，不存在算法能用来机械地确定任给的公式是否从该公理集可证. 由此可知，莱布尼茨的通过计算解决争论的设想即便是对算术这一局部数学理论来说，也是不能一劳永逸地完全实现的.

以上这些关于可证性的结论指出了机器的局限性，机器在创造性工作领域内的局限性，但没有理由说这种局限性是人类智慧或人类理性的局限性.

如今，人类创造的计算机已成为脑力劳动及社会运行必不可少的工具. 我们对计算机事业的发展前途充满信心. 与此同时，我们对人自身的创造能力和人类的智慧，更加可以充满信心.

# 部分练习答案或提示

## 练习 2

1. $L_3$ 有 22 个元素.
2. $L_2$ 有 30 个元素.
3. $L_2$ 有 84 个元素，$L_3$ 有 732 个元素.

## 练习 3

1. 注意公式集 $L(X)$ 是可数集，而每个 $L$ 中证明都是公式的有限序列. 用 0.3 节命题 7 及命题 1.

2. 1° $(\neg x_1 \to \neg x_2) \to (x_2 \to x_1)$ 是 (L3) 型公理. 要用例 1 的方法.

   2° 两次用 (L2) 型公理.

   3° $x_2 \to (x_1 \to x_2)$ 是 (L1) 型公理.

3. 1° 用命题 2.

   2° 要用到以下公理:

$$\neg\neg p \to (\neg\neg\neg\neg p \to \neg\neg p),$$
$$(\neg\neg\neg\neg p \to \neg\neg p) \to (\neg p \to \neg\neg\neg p),$$
$$(\neg p \to \neg\neg\neg p) \to (\neg\neg p \to p).$$

   3° 用 (L3) 和 (L2) 各一次.

   4° 两次用 ($L$2), 并用 ($L$1) 型公理:

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

   5° 要用公理:

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

4. 设 $q_1,\cdots,q_n$ 是 $q$ 从 $\Gamma$ 的一个证明. 把 $p$ 从 $\Gamma\cup\{q\}$ 的证明中所出现的 $q$ 全都用 $q_1,\cdots,q_n$ 代替, 便得到 $p$ 从 $\Gamma$ 的一个证明.

## 练习 4

1. 直接证明时, 注意 $x_1\to((x_1\to x_2)\to x_1)$ 是公理. 还用练习 3 题 2-2° 的方法证明:

$$((x_1\to(x_1\to x_2))\to(x_1\to x_1))\to((x_1\to(x_1\to x_2))\to(x_1\to x_2)).$$

2. 1° 由练习 3 题 3-2° (其中以 $\neg p$ 代 $p$), 用演绎定理得

$$\vdash\neg\neg\neg p\to\neg p,$$

再用 (L3) 及 HS.

2° 只用证 $\{q\to p\}\vdash\neg p\to\neg q$. 利用以前建立的结果:$\neg\neg q\to q$ 及 $p\to\neg\neg p$, 两次用 HS.

3° 为证 $\{(p\to q)\to p\}\vdash p$, 由 $\neg p\to(p\to q)$ 用 HS 得 $\neg p\to p$, 再用命题 1 的结果.

4° 注意 $\neg(p\to q)\to((p\to q)\to p)$ 及 $((p\to q)\to p)\to p$.

## 练习 5

1. 1° $\{p\to\neg q, q, p\}\vdash q,\neg q$.

3° $\{\neg(p\to q), q\}\vdash p\to q,\neg(p\to q)$.

4° $\{\neg(p\to q),\neg p\}\vdash p\to q,\neg(p\to q)$.

5° $\{p\to q,\neg q\}\vdash\neg p$,

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

2. 由 $\Gamma\cup\{\neg p\}\vdash q,\neg q$ 用归谬律可得 $\Gamma\vdash\neg\neg p$.

## 练习 6

1. $\{\neg p\to q,\neg q,\neg p\}\vdash q,\neg q$.

4. 利用命题 3-5°, 先证:

$$\vdash\neg\neg(p\to\neg q)\to(\neg\neg p\to\neg q),$$
$$\vdash(\neg\neg p\to\neg q)\to\neg\neg(p\to\neg q).$$

## 练习 7

1. 1° $v(p\wedge q)=v(p)\wedge v(q)=1$.

2. 恒为永真式的有 1°, 2°, 3°.
3. 1° 正确，2° 不正确.
4. 不是. 取 $p$ 与 $q$ 都是永真式时 $(\neg p \to q) \to (p \to \neg q)$ 为永假式.

## 练习 8

1. 用可靠性定理，代换定理及完全性定理.
2. 先用完全性定理，最后用可靠性定理.

## 练习 9

3. 设 $p = p(x_1, \cdots, x_n)$, $q = q(x_1, \cdots, x_n)$. 由代换定理,

$$\begin{aligned}
&\vDash p(x_1, \cdots, x_n) \leftrightarrow q(x_1, \cdots, x_n) \\
&\quad \Rightarrow \ \vDash p(\neg x_1, \cdots, \neg x_n) \leftrightarrow q(\neg x_1, \cdots, \neg x_n) \\
&\quad \Rightarrow \ \vDash \neg p(\neg x_1, \cdots, \neg x_n) \leftrightarrow \neg q(\neg x_1, \cdots, \neg x_n) \\
&\quad \Rightarrow \ \vDash (p(\neg x_1, \cdots, \neg x_n))^* \leftrightarrow (q(\neg x_1, \cdots, \neg x_n))^* \qquad \text{(由对偶律)} \\
&\quad \Rightarrow \ \vDash (p(\neg\neg x_1, \cdots, \neg\neg x_n))^d \leftrightarrow (q(\neg\neg x_1, \cdots, \neg\neg x_n))^d \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(由 } p^* \text{ 和 } p^d \text{ 的定义)} \\
&\quad \Rightarrow \ \vDash (p(x_1, \cdots, x_n))^d \leftrightarrow (q(x_1, \cdots, x_n))^d.
\end{aligned}$$

## 练习 10

1. 1° $(x_1 \wedge x_2) \vee (\neg x_1 \wedge \neg x_2)$.

   2° $(x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge \neg x_2 \wedge x_3) \vee (x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (\neg x_1 \wedge x_2 \wedge x_3)$
   $\vee(\neg x_1 \wedge x_2 \wedge \neg x_3) \vee (\neg x_1 \wedge \neg x_2 \wedge x_3) \vee (\neg x_1 \wedge \neg x_2 \wedge \neg x_3)$.

   3° $(x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge x_2 \wedge \neg x_3) \vee (x_1 \wedge \neg x_2 \wedge x_3) \vee (\neg x_1 \wedge x_2 \wedge \neg x_3)$
   $\vee(\neg x_1 \wedge \neg x_2 \wedge x_3)$.

   4° $(x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (\neg x_1 \wedge x_2 \wedge \neg x_3) \vee (\neg x_1 \wedge \neg x_2 \wedge \neg x_3)$.

   5° $(x_1 \wedge x_2 \wedge x_3 \wedge x_4) \vee (x_1 \wedge x_2 \wedge \neg x_3 \wedge x_4) \vee (x_1 \wedge \neg x_2 \wedge x_3 \wedge x_4)$
   $\vee(x_1 \wedge x_2 \wedge \neg x_3 \wedge \neg x_4) \vee (x_1 \wedge \neg x_2 \wedge \neg x_3 \wedge x_4) \vee (\neg x_1 \wedge x_2 \wedge x_3 \wedge x_4)$
   $\vee(\neg x_1 \wedge x_2 \wedge \neg x_3 \wedge x_4) \vee (\neg x_1 \wedge x_2 \wedge \neg x_3 \wedge \neg x_4) \vee (\neg x_1 \wedge \neg x_2 \wedge x_3 \wedge x_4)$
   $\vee(\neg x_1 \wedge \neg x_2 \wedge \neg x_3 \wedge x_4) \vee (\neg x_1 \wedge \neg x_2 \wedge \neg x_3 \wedge \neg x_4)$.

2. 1° $(\neg x_1 \vee \neg x_2 \vee x_3) \wedge (x_1 \vee \neg x_2 \vee x_3) \wedge (x_1 \vee x_2 \vee x_3)$.

   2° $(\neg x_1 \vee x_2) \wedge (x_1 \vee \neg x_2)$.

   3° $(x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee \neg x_2 \vee x_3) \wedge (x_1 \vee \neg x_2 \vee \neg x_3) \wedge (\neg x_1 \vee x_2 \vee \neg x_3)$
   $\wedge(\neg x_1 \vee \neg x_2 \vee x_3) \wedge (\neg x_1 \vee x_2 \vee x_3)$.

4° $(x_1 \vee x_2 \vee \neg x_3 \vee x_4) \wedge (x_1 \vee \neg x_2 \vee \neg x_3 \vee x_4) \wedge (\neg x_1 \vee x_2 \vee x_3 \vee x_4)$
$\wedge(\neg x_1 \vee x_2 \vee \neg x_3 \vee x_4) \wedge (\neg x_1 \vee \neg x_2 \vee \neg x_3 \vee x_4)$.

## 练习 11

1. $v_1 \vee v_2 = \neg\neg(v_1 \vee v_2) = \neg(\neg v_1 \wedge \neg v_2)$
$= (\neg v_1) | (\neg v_2) = (v_1 | v_1) | (v_2 | v_2)$.

2. 3° $\neg(\neg(x_1 \wedge x_2) \wedge \neg(\neg x_1 \wedge \neg x_2) \wedge \neg x_3)$
$\wedge\neg(x_3 \wedge \neg(\neg(x_1 \wedge x_2) \wedge \neg(\neg x_1 \wedge \neg x_2)))$.

4. $((x_1 \downarrow x_1) \downarrow x_2) \downarrow ((x_1 \downarrow x_1) \downarrow x_2)$.

## 练习 12

1. 用 $x_1, x_2$ 分别表示“$f$ 连续”,“$g$ 可微”. $\{\neg x_1 \to \neg x_2, x_2\} \models x_1$, 论证合理.
2. 不合理.
3. 正确.

## 练习 13

1. $T = \bigcup_{n=0}^{\infty} T_n$, $T_0 = \{x_1, x_2, \cdots\}$,

$$T_n = \{\overbrace{f_1^1(\cdots(f_1^1}^{n\uparrow f_1^1}(x_1))\cdots), \overbrace{f_1^1(\cdots(f_1^1}^{n\uparrow f_1^1}(x_2))\cdots), \cdots\}.$$

## 练习 14

1. 1°, 4°, 5°, 7°, 8° 是公式, 其中 1° 与 8° 是闭式.

2. 1° $x_1$ 自由出现 1 次. $f_1^2(x_1, x_3)$ 对 $x_2$ 自由.
4° $x_1$ 先自由出现两次, 后约束出现两次. $f_1^2(x_1, x_3)$ 对 $x_2$ 不自由.

3. 1° $t$ 对 $p(x_1)$ 中 $x_1$ 自由.
$$p(t) = \forall x_1 R_1^2(x_2, f_1^2(x_1, x_2)) \to R_1^1(f_1^2(x_1, x_3)).$$
2° 自由. $p(t) = p(x_1)$.
3° 不自由.
4° 不自由.

4. (1) 1° 自由.
$$p(x_2) = \forall x_1 R_1^2(x_2, f_1^2(x_1, x_2)) \to R_1^1(x_2).$$
2° 自由.

3° 自由.

4° 不自由.

(2) 1° 自由.

2° 自由.

3° 不自由.

4° 不自由.

(3) 1° ~ 4° $t$ 对 $x_1$ 都是自由的.

(4) 1° 自由.

2° 自由.

3° 不自由.

4° 不自由.

5. $x$ 对 $p(y)$ 中 $y$ 是自由的，因为 $p(y)$ 中的 $y$ 不可能自由地出现在 $\forall x$ 的范围内. 事实上，

(i) $p(y)$ 中原有的 $y$ 不自由出现;

(ii) $p(y)$ 中新替换 $x$ 的 $y$ 又不会出现在 $\forall x$ 的范围内.

## 练习 15

1. 最后用一次用 Gen.
2. 用演绎定理两次，Gen 一次.
3. 1° 两次用 (K4). 第二次用的是 $\forall x_2 R_1^2(x_1, x_2) \to R_1^2(x_1, x_1)$.

   2° 可先证明 $\{\forall x_1 \forall x_2 R_1^2(x_1, x_2)\} \vdash \forall x_1 \forall x_3 R_1^2(x_1, x_3)$. (两次 (K4)，两次 Gen)
4. 1° 先证 $\{p \to \forall x q\} \vdash \forall x(p \to q)$,

   (1) $p \to \forall x q$.

   (2) $\forall x q \to q, \cdots$.

   2° 先证 $\{p \to \exists x q, \forall x \neg(p \to q)\} \vdash \forall x \neg q$ 及 $\neg \forall x \neg q$, 用归谬律即可. 注意 $\neg(p \to q) \to p$ 和 $\neg(p \to q) \to \neg q$ 是永真式.
5. 1° 演绎定理的条件未满足.

   2° 反证律的条件未满足.

## 练习 16

1. 1° 先证 $\{\exists x p \to q\} \vdash \forall x(p \to q)$:

   (1) $\neg \forall x \neg p \to q$,

   (2) $(\neg \forall x \neg p \to q) \to (\neg q \to \neg\neg \forall x \neg p)$,

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

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

$\cdots\cdots$

2° 用反证律证明 $\{\exists x(p \to q), \forall x p\} \vdash q$.

3. 3° $\forall x_4 \exists x_3 \exists x_1((R_1^1(x_1) \to R_1^2(x_1, x_2)) \to (R_1^1(x_4) \to R_1^2(x_2, x_3)))$.

4° $\forall x_4 \forall x_3 (\neg R_1^2(x_4, x_2) \vee \neg R_1^1(x_1) \vee \neg R_1^2(x_1, x_3))$.

5. $\exists x_1 R_1^1(x_1) \to \exists x_2 \forall x_3 R_1^2(x_2, x_3)$ 与 $\Pi_3$ 型前束范式等价，也与一 $\Sigma_2$ 型前束范式等价.

## 练习 17

1. 甲:

(1) $\exists x_1 (R_1^1(x_1) \wedge R_1^2(x_1, c_1)) \to \forall x_2 (R_2^1(x_2) \to R_1^2(x_2, c_1))$,

(2) $\exists x_1 (R_1^1(x_1) \wedge R_1^2(x_1, c_1)) \to \neg \exists x_2 \neg (R_2^1(x_2) \to R_1^2(x_2, c_1))$,

(3) $\forall x_1 \forall x_2 (((R_1^1(x_1) \wedge R_1^2(x_1, c_1)) \to (R_2^1(x_2) \to R_1^2(x_2, c_1)))$.

乙:

(1) $\neg \forall x_1 (R_1^1(x_1) \to \forall x_2 (R_2^1(x_2) \to \neg R_1^2(x_1, x_2)))$,

(2) $\exists x_1 (R_1^1(x_1) \wedge \exists x_2 (R_2^1(x_2) \wedge R_1^2(x_1, x_2)))$,

(3) $\exists x_1 \exists x_2 (R_1^1(x_1) \wedge R_2^1(x_2) \wedge (R_1^2(x_1, x_2))$.

2. 对 $t$ 在 $T$ 中的层次数 $k$ 归纳. $k = 0$ 时，$t = x_i$ 或 $t = c_i, \cdots$ .

3. 对 $u$ 在 $T$ 中的层次数 $k$ 归纳. 注意 $x$ 不一定在 $u(x)$ 中出现，故 $k = 0$ 时有三种可能的情形: $u(x) = c_i$, $u(x) = x$, $u(x) = y(\neq x)$.

详见正文 2.3 节引理 1-1° 的证明.

## 练习 18

1. 1° 取 $\varphi$ 满足 $\varphi(x_1) = 1$, $\varphi(x_2) = 1$, $\varphi(x_3) = 2$;

取 $\psi$ 满足 $\psi(x_1) = \psi(x_2) = \psi(x_3) = 1$.

2. 1° 取 $\varphi$ 满足 $\varphi(x_1) = -1$; 取 $\psi$ 满足 $\psi(x_1) = 1$.

## 练习 19

1. 1° 0;

2° 1;

3° 1;

4° 1.

2. 1° 0;

2° 0;

3° 1;

4° 1.

3. 1° 取 $M_1 = \mathbf{Z}$ (整数集), $\overline{c_1} = 0$, $\overline{f_1^2}$ 是减法, $\overline{R_1^2}$ 是相等, 则 $|p|_{M_1} = 1$; 取 $M_2 = \mathbf{Z}$, $\overline{c_1} = 0$, $\overline{f_1^2}$ 是加法, $\overline{R_1^2}$ 是相等, 则 $|p|_{M_2} = 0$.

4. $|p|_M = 1 \Rightarrow |\neg p|_M = 0 \Rightarrow |\forall x \neg p|_M = 0 \Rightarrow |\exists x p|_M = 1$.

反向不成立. 对 2.2.1 小节例 1 中的 $\mathbf{N}$,

$$|\exists x_1 R_1^2(x_1, c_1)|_{\mathbf{N}} = 1 \text{ 但 } |R_1^2(x_1, c_1)|_{\mathbf{N}} \neq 1.$$

## 练习 20

1. 1° 任取解释域 $M$, 再任取 $\varphi \in \Phi_M$. 设 $|\exists x_1 \forall x_2 R_1^2(x_1, x_2)|(\varphi) = 1$, 于是有 $\varphi$ 的 $x_1$ 变通 $\varphi'$ 使

$$|\forall x_2 R_1^2(x_1, x_2)|(\varphi') = 1. \tag{1}$$

对 $\varphi$ 的任一 $x_2$ 变通 $\varphi_2$, 作 $\varphi_2$ 的 $x_1$ 变通 $\varphi_1$, 使 $\varphi_1(x_1) = \varphi'(x_1)$. 这样 $\varphi_1$ 成了 $\varphi'$ 的 $x_2$ 变通, 由 (1) 有 $|R_1^2(x_1, x_2)|(\varphi_1) = 1$. 这说明 $|\exists x_1 R_1^2(x_1, x_2)|(\varphi_2) = 1$ (因 $\varphi_1$ 是 $\varphi_2$ 的 $x_1$ 变通), 进而说明 $|\forall x_2 \exists x_1 R_1^2(x_1, x_2)|(\varphi) = 1$.

2° 设 $|\forall x_1 R_1^1(x_1)|(\varphi) = 1$, 只用证 $|\forall x_2 R_1^1(x_2)|(\varphi) = 1$. 对 $\varphi$ 的任一 $x_2$ 变通 $\varphi_2$, 作 $\varphi$ 的 $x_1$ 变通 $\varphi_1$ 使 $\varphi_1(x_1) = \varphi_2(x_2)$. 于是

$$\begin{aligned}|\forall x_1 R_1^1(x_1)|(\varphi) = 1 &\Rightarrow |R_1^1(x_1)|(\varphi_1) = 1 \Rightarrow \varphi_1(x_1) \in \overline{R_1^1} \\ &\Rightarrow \varphi_2(x_2) \in \overline{R_1^1} \Rightarrow |R_1^1(x_2)|(\varphi_2) = 1 \Rightarrow |\forall x_2 R_1^1(x_2)|(\varphi) = 1.\end{aligned}$$

4° 设 $|\forall y \forall x p|(\varphi) = 0$. 则有 $\varphi$ 的 $y$ 变通 $\varphi_2$ 和 $\varphi_2$ 的 $x$ 变通 $\varphi_1$ 使 $|p|(\varphi_1) = 0$. 作 $\varphi$ 的 $x$ 变通 $\varphi'$ 使 $\varphi'(x) = \varphi_1(x)$. 再作 $\varphi'$ 的 $y$ 变通 $\varphi''$ 使 $\varphi''(y) = \varphi_1(y)$. 故可得 $\varphi'' = \varphi_1$, 因而有 $|p|(\varphi'') = 0$, 进而得 $|\forall y p|(\varphi') = 0$, $|\forall x \forall y p|(\varphi) = 0$.

2. $R_1^1(x_1) \to R_1^1(x_1)$.

3. 1° 取 $M = \mathbf{N}$, $\overline{R_1^2}$ 为 $\leqslant$, 则

$$|\forall x_1 \exists x_2 R_1^2(x_1, x_2) \to \exists x_2 \forall x_1 R_1^2(x_1, x_2)|_M = 0.$$

5° 取 $\overline{R_1^1}$ 为 “$= 0$”, 则 $|\exists x_1 R_1^1(x_1)|_{\mathbf{N}} = 1$, 而当 $\varphi(x_1) = 1$ 时 $|R_1^1(x_1)|(\varphi) = 0$.

4. (i) 对项 $t$ 的层次数 $k$ 归纳.

(ii) 对公式 $p$ 的层次数 $k$ 归纳.

$k = 0$ 时, 设 $p = R_i^n(t_1, \cdots, t_n)$, $t_i \in T$. 此时

$$\begin{aligned}|p|(\varphi^+) = 1 &\Leftrightarrow (\varphi^+(t_1), \cdots, \varphi^+(t_n)) \in \overline{R_i^n} \\ &\Leftrightarrow (\varphi(t_1), \cdots, \varphi(t_n)) \in \overline{R_i^n} \qquad \text{(由 (i))} \\ &\Leftrightarrow |p|(\varphi) = 1.\end{aligned}$$

$k > 0$ 时，若 $p = q \to r$ 或 $p = \neg q$, 则较简单. 现设 $p = \forall x_i q$. 若 $\varphi'$ 是 $\varphi$ 的任一 $x_i$ 变通，且 $\varphi^{+\prime}$ 是 $K^+$ 的和 $\varphi'$ 有相同变元指派的项解释，则 $\varphi^{+\prime}$ 是 $\varphi^+$ 的 $x_i$ 变通. 反之，对于 $\varphi^+$ 的任一 $x_i$ 变通 $\varphi^{+\prime}$, 和 $\varphi^{+\prime}$ 有相同变元指派的 $K$ 的项解释 $\varphi'$ 是 $\varphi$ 的 $x_i$ 变通. 于是有

$$
\begin{aligned}
|p|(\varphi^+) = 1 \quad &\Leftrightarrow \text{ 对任一 } \varphi^+ \text{ 的 } x_i \text{ 变通} \varphi^{+\prime},\ |p|(\varphi^{+\prime}) = 1 \\
&\Leftrightarrow \text{ 对任一 } \varphi \text{ 的 } x_i \text{ 变通 } \varphi',\ |q|(\varphi') = 1 \\
&\qquad\qquad\qquad\qquad\qquad\qquad \text{(用归纳假设)} \\
&\Leftrightarrow |\forall x_i q|(\varphi) = 1,\ \text{即 } |p|(\varphi) = 1.
\end{aligned}
$$

## 练习 21

2. 不成立. 用可靠性定理从语义上进行讨论.

## 练习 22

1. ($\Rightarrow$) 由可靠性定理及 $\Gamma$ 的完备性，$\Gamma \vDash p$ 与 $\Gamma \vDash \neg p$ 二者必居其一.

($\Leftarrow$) 设 $\Gamma$ 不完备，即存在闭式 $p$ 使 $\Gamma \vdash p$ 与 $\neg p$ 都不成立，那么 $\Gamma \cup \{p\}$ 和 $\Gamma \cup \{\neg p\}$ 都是无矛盾集，各有模型 $M_1$ 和 $M_2$. 于是 $|p|_{M_1} = 1$ 而 $|p|_{M_2} = 0$.

2. 用反证法证明 $\Gamma$ 无矛盾. 使用定理 1 及 2.3 节推论 2.

## 练习 23

1. (E2) 有五种形式:

$$
\begin{aligned}
&t \approx u \ \to\ f_1^1(t) \approx f_1^1(u), \\
&t_1 \approx u \ \to\ f_1^2(t_1, t_2) \approx f_1^2(u, t_2), \\
&t_2 \approx u \ \to\ f_1^2(t_1, t_2) \approx f_1^2(t_1, u), \\
&\cdots\cdots
\end{aligned}
$$

(E3) 有两种形式.

2. (E1) 型公理此时在 **N** 中恒假.

3. 先证 $E \cup \{p(t),\ p(x) \wedge \forall y(p(y) \to x \approx y)\} \vdash p(u) \to u \approx t$. 要用两次 (K4):

$$
\begin{aligned}
&\forall y(p(y) \to x \approx y) \to (p(u) \to x \approx u), \\
&\forall y(p(y) \to x \approx y) \to (p(t) \to x \approx t).
\end{aligned}
$$

## 练习 24

1. 由命题 2 有 $N \vdash \bar{k} \times \bar{2} \approx \overline{2k}$. 再用 $\exists_1$ 规则，

$$N \vdash \bar{k} \times \bar{2} \approx \overline{2k} \ \to\ \exists x(x \times \bar{2} \approx \overline{2k}).$$

4. 用 (N7) 证明 $\mathcal{N} \vdash \forall x(x' + t_2 \not\approx x)$.

5. 记 $\mathcal{N}_k = \mathcal{N} \cup \{c_i' \approx c_{i+1},\ i > 0\} \cup \{c_0 \not\approx c_i,\ 0 < i \leqslant k\}$. **N** 是 $\mathcal{N}_k$ 的模型，其中 $c_0$ 解释为 $k$, $c_i$ 解释为 $i-1$, $0 < i \leqslant k$，所以 $\mathcal{N}_k$ 无矛盾. 因

$$\mathcal{N}^+ = \cup_{k \in \mathbf{N}} \mathcal{N}_k ,$$

且每个 $\mathcal{N}_k$ 无矛盾，故 $\mathcal{N}^+$ 也无矛盾. 根据 2.4 节定理 1，$\mathcal{N}^+$ 有模型. 在 $\mathcal{N}^+$ 的模型中，若仍把 $c_i\ (i > 0)$ 的解释叫做自然数，则 $c_0$ 的解释一定是与所有自然数皆不相同的另外一个新元素. $\mathcal{N}^+$ 的这个模型是一种非标准算术模型.

## 练习 25

2. 否则与 $\mathcal{N}$ 的无矛盾性相矛盾.

3. 不等价. 按题中条件，任何公式都表示了一个 $k$ 元关系. 参见跟随定义 3 (可表示关系) 后的说明.

4. 注意 $\mathcal{N} \vdash p \ \Rightarrow \ |p|_{\mathbf{N}} = 1$.

## 练习 26

1. $x_1 \approx x_1 \ \wedge \ x_2 \approx \overline{2}$.

4. $\neg \exists z (z + x_1 \approx x_2)$.

## 练习 27

1. $r(n_1, n_2, n_3) = f(n_3, n_1)$
$$= f(\mathrm{p}_3^3(n_1, n_2, n_3),\ \mathrm{p}_1^3(n_1, n_2, n_3)).$$

2. (3) $\max(n_1, n_2) = n_1 + (n_2 \dot{-} n_1)$.

(4) $f(0) = 1$,
$f(n+1) = \mathrm{s}(n) \times f(n)$.

(6) $f_k(n) = \overline{\mathrm{sg}}(n \ddot{-} k) = \overline{\mathrm{sg}}(n \ddot{-} C_k(n))$.

(7) $q(n_1, 0) = 0$.
$q(n_1, n+1) = \mathrm{sg}(n_1) \times (q(n_1, n) + \overline{\mathrm{sg}}(n_1 \dot{-} (\mathrm{rem}(n_1, n) + 1)))$.

(8) $f(n_1, n_2, n_3) = \Sigma_{i<n_3}\, g(n_1, n_2, i)$,
$h(n_1, n_2) = f(n_1, n_2, n_1)$.

3. 所有基本函数构成的集 $F_0$ 是可数集.

把由基本函数使用 $n$ 次规则生成的所有函数构成的集记为 $F_n$. 对 $n$ 归纳可证每个 $F_n$ 都是可数集.(这里不考虑规则 III 的根存在性条件.)

于是所有递归偏函数构成的集就是 $\bigcup_{n=0}^{\infty} F_n$. 它是可数集. (见 0.3 节命题 8) 作为它的无限子集，所有递归函数构成的集也是可数集.(见 0.3 节命题 1)

## 练习 28

1. $C_{N_1}(n) = \overline{\mathrm{sg}}(\mathrm{rem}(2, \mathrm{n}))$,
   $C_{N_2}(n) = \overline{\mathrm{sg}}(n \dot{-} 2)$.
2. $C_{A\times B}(n_1, n_2) = C_A(n_1) \times C_B(n_2)$.
3. 用反证法, $C_A(n) = C_{A\times A}(n, n)$.
4. $C_G(n) = \mathrm{sg}((3 \dot{-} n) + \mathrm{rem}(2, n))$
   $$+\Sigma_{x<n}\Sigma_{y<n}(C_=(n, x+y)C_{\mathrm{prm}}(x)C_{\mathrm{prm}}(y)).$$
5. $f(n, \cdots, n_k) = \Sigma_{i\leqslant l}\ g_i(n_1, \cdots, n_k)C_{R_i}(n_1, \cdots, n_k)$.
6. 不一定. 如取 $A = A_1 = \mathbf{N}$, $A_2$ 为任一非递归集.
7. 归纳可证 $p(n) \leqslant 2^{2^n}$.
   $$p(n) = \Sigma_{k=0}^{2^{2^n}} \Pi_{l=0}^{k}\, \mathrm{sg}\,[n + 1 \dot{-} \Sigma_{j=0}^{l}\, \overline{\mathrm{sg}}\,(3 \dot{-} \Sigma_{i=0}^{j}\, \overline{\mathrm{sg}}\,(\mathrm{rem}(i, j)))].$$

## 练习 29

1. 利用 3.3.1 小节命题 1 证明 sg 用公式 $p(x_1, y)$ 可表示，这里的 $p(x_1, y)$ 是
   $$(x_1 \approx \overline{0} \wedge y \approx \overline{0}) \vee (x_1 \not\approx \overline{0} \wedge y \approx \overline{1}).$$
2. $(\exists z(z + x_1 \approx x_2) \wedge y \approx \overline{0}) \vee (\neg\exists z(z + x_1 \approx x_2) \wedge x_1 \approx x_2 + y)$.

## 练习 30

3. 例如字母串 $\neg'\neg x_i$ 权重为 1，且真前段权重不足 1，但它不是项，也不是公式.

## 练习 31

1. (5) $2^7\, 3^{11}\, 5^{21}\, 7^7\, 11^{13}\, 13^3\, 17^{21}\, 19^{17}\, 23^1\, 29^{19}$.
   (6) $2^{2^7 3^{13} 5^{19} 7^{15}}\, 3^{2^{13} 3^{17} 5^{19}}\, 5^{2^7 3^{13} 5^{17} 7^{15}}$.

## 练习 32

1. 不一定成立. 当 $n_1 = 2^{a_0}, \cdots p_k^{a_k}$, $n_2 = 2^{b_0}, \cdots p_l^{b_l}$ 且 $a_0, \cdots, a_k, b_0, \cdots, b_l$ 都不为零时，该式成立.

2. $C_R(n_1,\cdots,n_{k+1})=C_H(n_1,\cdots,n_{k+1},\ C_R^\sharp(n_1,\cdots,n_{k+1}))$.

3. $f(n)=\overline{\mathrm{sg}}(n)+2\,\overline{\mathrm{sg}}(n\mathbin{\ddot{-}}1)$
$$+\ \mathrm{sg}(n\mathbin{\dot{-}}1)((f^\sharp(n))_{n\dot{-}1}+(f^\sharp(n))_{n\dot{-}2}).$$

## 练习 33

1. $$\begin{aligned}C_{\mathrm{SBS}}(n_1,n_2,\gamma)=\ & C_{\mathrm{VS}}(n_1)C_{\mathrm{TM}}(n_2)(C_{\mathrm{TM}}((\gamma)_0)+C_{\mathrm{FM}}((\gamma)_0))\\ &\times[C_=((\gamma)_0,n_1)C_=((\gamma)_1,n_2)\\ &+\Sigma_{x<(\gamma)_0}((C_=((\gamma)_0,2^x)C_{\neq}((\gamma)_0,n_1)\\ &+C_=((\gamma)_0,2^{11}*n_1*x))C_=((\gamma)_1,(\gamma)_0))\\ &+\Sigma_{x<(\gamma)_0}\Sigma_{y<(\gamma)_0}\Sigma_{z<(\gamma)_1}C_=((\gamma)_0,\ 2^x*y)\\ &\times C_=((\gamma)_1,\ 2^x*z)C_{\mathrm{SBS}}(n_1,n_2,2^y3^z)\\ &+\Sigma_{x<(\gamma)_0}\Sigma_{y<(\gamma)_0}\Sigma_{z<(\gamma)_0}\Sigma_{u<(\gamma)_1}\Sigma_{v<(\gamma)_1}C_=((\gamma)_0,\ 2^x*y*z)\\ &\times(C_{\neq}(x,11)+C_{\neq}(y,n_1))C_=((\gamma)_1,\ 2^x*u*v)\\ &\times C_{\mathrm{SBS}}(n_1,n_2,2^y3^u)C_{\mathrm{SBS}}(n_1,n_2,2^z3^v)],\end{aligned}$$

其中

把 $C_{\mathrm{SBS}}(n_1,n_2,2^y3^z)$ 换成 $(C^\sharp_{\mathrm{SBS}}(n_1,n_2,\gamma))_{2^y3^z}$,

把 $C_{\mathrm{SBS}}(n_1,n_2,2^y3^u)$ 换成 $C^\sharp_{\mathrm{SBS}}(n_1,n_2,\gamma))_{2^y3^u}$,

把 $C_{\mathrm{SBS}}(n_1,n_2,2^z3^v)$ 换成 $C^\sharp_{\mathrm{SBS}}(n_1,n_2,\gamma))_{2^z3^v}$,

就得 $C_{\mathrm{SBS}}$ 所满足的过程值递归条件.

2. 因 $n\in\mathrm{AX}\ \Leftrightarrow\ 2^n\in\mathrm{PF}$, 故 $C_{\mathrm{AX}}(n)=C_{\mathrm{PF}}(2^n)$.

3. 参见 4.1.1 小节.

## 练习 34

1. 结论仍然成立. 首先, 原来满足可表示条件的函数在公理增加之后仍满足可表示条件, 所以递归函数仍然是可表示的. 反过来, 在新的意义下可表示函数仍一定是递归函数, 证明与定理 1 的证明完全相同, 只要把出现的 $\mathcal{N}$ 全部改成 $\mathcal{N}^*$. 注意 3.6.4 小节命题 8 中也要作同样的改动. 改动后, PRF 的递归性并没有改变.

## 练习 35

1. (反证)

$|\mathrm{p}(\overline{m})|_{\mathrm{N}}=0\ \Rightarrow$ 存在 $\varphi\in\Phi_{\mathrm{N}}$ 使 $|\neg w(\overline{m},x_2)|(\varphi)=0$

$\Rightarrow$ 存在$\varphi$, $|w(\overline{m},\overline{n})|(\varphi)=|w(\overline{m},x_2)|(\varphi)=1$

(记 $\varphi(x_2) = n = \varphi(\overline{n})$)

$\Rightarrow$ 存在$n$, $|w(\overline{m},\overline{n})|_{\mathrm{N}} = 1$ ($w(\overline{m},\overline{n})$是闭式)

$\Rightarrow$ $(m,n) \in W$ (否则 $\mathcal{N} \vdash \neg w(\overline{m},\overline{n})$ 导致 $|w(\overline{m},\overline{n})|_{\mathrm{N}} = 0$)

$\Rightarrow$ $\mathcal{N} \vdash \mathrm{p}(\overline{m})$ ($W$ 的定义)

这与定理 1 (i) 相矛盾.

2. $\mathcal{N} \cup \{\neg \mathrm{p}(\overline{m})\}$是无矛盾的，否则用反证律得 $\mathcal{N} \vdash \mathrm{p}(\overline{m})$. 注意以下两点:

(1) $\mathcal{N} \cup \{\neg \mathrm{p}(\overline{m})\} \vdash \neg \forall x_2 \neg w(\overline{m}, x_2)$ (即 $\neg \mathrm{p}(\overline{m})$);

(2) $\mathcal{N} \cup \{\neg \mathrm{p}(\overline{m})\} \vdash \neg w(\overline{m},\overline{n})$, $n = 0, 1, 2, \cdots$,

其中 (2) 见正文定理 1 (ii) 的证明. (1) 与 (2) 说明 $\mathcal{N} \cup \{\neg \mathrm{p}(\overline{m})\}$ 非 $\omega$-无矛盾.

3. 设 $\alpha_0 = \mathrm{g}(r(x_1))$. 于是

$C_{W_1}(n_1, n_2) =$

$$C_{\mathrm{FM}}(n_1) \times C_{\mathrm{PRF}}(2^9 * 2^7 * \mathrm{Sub}(2^{17}, \mathrm{Num}(n_1), \alpha_0) * 2^7 * n_1, n_2).$$

## 练习 36

1. 参见 4.1.4 小节.

2. $|\mathrm{p}(\overline{m})|_{\mathrm{N}} = 0$ $\Rightarrow$ 存在 $\varphi \in \Phi_{\mathrm{N}}$ 使 $|w(\overline{m}, x_2)|(\varphi) = 1$

$\Rightarrow$ 记 $\varphi(x_2) = n (= \varphi(\overline{n}))$, 有 $|w(\overline{m},\overline{n})|(\varphi) = 1$

$\Rightarrow$ $|w(\overline{m},\overline{n})|_{\mathrm{N}} = 1$ ($w(\overline{m},\overline{n})$是闭式)

$\Rightarrow$ $(m,n) \in W$

(否则 $\mathcal{N}^* \vdash \neg w(\overline{m},\overline{n})$ 导致 $|w(\overline{m},\overline{n})|_{\mathrm{N}} = 0$)

$\Rightarrow$ $\mathcal{N}^* \vdash \mathrm{p}(\overline{m})$.

## 练习 38

1. 反设 TR 是递归集. 记所有在 **N** 中恒真的公式集为 $\mathcal{N}^+$, 则 $\mathcal{N}^+$ 是 $\mathcal{N}$ 的递归无矛盾扩张. (**N** 是 $\mathcal{N}^+$ 的模型，所以 $\mathcal{N}^+$ 是无矛盾的.) 根据 Gödel-Rosser 定理，$\mathcal{N}^+$ 是不完备的，即存在闭式 $p$, 使 $p$ 和 $\neg p$ 从 $\mathcal{N}^+$ 都不可证，当然 $p$ 和 $\neg p$ 都不能是 $\mathcal{N}^+$ 的成员. 但 $|p|_{\mathrm{N}} = 1$ 和 $|\neg p|_{\mathrm{N}} = 1$ 二者必居其一，这与 $\mathcal{N}^+$ 的定义相矛盾.

2. 见 4.1.5 引理 1.

3. 不能说明 TH 是递归集，题 2 的结论只说明

$$m \in \mathrm{TH} \ \Rightarrow \ \mathcal{N} \vdash \mathrm{pr}(\overline{m}).$$

要证明 TH 是递归集，还要证明

$$m \notin \mathrm{TH} \ \Rightarrow \ \mathcal{N} \vdash \neg \mathrm{pr}(\overline{m}),$$

而这是不可能证明的. (见 4.2 节定理 1.)

## 练习 39

1. 题中给出的方法不符合算法的“有限性”. 无法在有限步骤之内断定不属于 TH 的 $m$ 肯定不在 (*) 中出现 (从而能断定 $m \notin$TH ).

## 练习 40

1. 递归可枚举集的全体构成的集到一元递归函数全体的集存在着单射，而后者是可数集.

2. 对 $n$ 归纳可证 $n \leqslant f(n)$.

$$C_A(n) = \mathrm{sg}\,(\Sigma_{i<n} C_=(f(i), n)).$$

3. 从一无限枚举中总可取出递增枚举.

4. 设 $A$ 是递归可枚举集. $A = \varnothing$ 时，它是递归偏函数 $g$ :

$$g(n) = \mu x[n + x + 1 = 0]$$

的定义域. $A \neq \varnothing$ 时，可设 $A$ 是递归函数 $f$ 的值域. 这时 $A$ 是递归偏函数 $g$ :

$$g(n) = \mu x[f(x) = n]$$

的定义域.

5. 一个 $k$ 元递归函数 $g$ 的值域，也是一个一元递归函数 $f$ 的值域，$f$ 满足

$$f(n) = g((n)_0, (n)_1, \cdots, (n)_{k-1}).$$

## 练习 41

1. 对第一个问题的回答是否定的，例如公式 $x_1 \approx x_1 \wedge y \not\approx y$ 不能用来定义任何一个一元函数; 对第二个问题的回答是肯定的.

2. 若 $R$ 用 $p(x_1, \cdots, x_k)$ 可定义，则 $C_R$ 用 $p(x_1, \cdots, x_k) \wedge y \approx \overline{1}$ 可定义; 若 $C_R$ 用 $p(x_1, \cdots, x_k, y)$ 可定义，则 $R$ 用 $p(x_1, \cdots, x_k, \overline{1})$ 可定义.

## 练习 42

1. 取 $\Sigma = \{0, 1, A\}$, $Q = \{q_0, q_1\}$. 对应于 $(n_1, n_2)$ 的输入纸带被规定为

$$\cdots 0\,\overbrace{1 \cdots 1}^{n_1 \text{个} 1}\,A\,\overbrace{1 \cdots 1}^{n_2 \text{个} 1}\,0 \cdots .$$

1° $T_1 = \{q_0\,1\,0\,q_1,\ q_0\,A\,0\,q_1,\ q_1\,0\,Rq_0\}$.

2° $T_2 = \{q_0\,1\,0\,q_1,\ q_0\,A\,0\,q_0,\ q_1\,0\,Rq_0\}$.

# 符 号 汇 集

| 符号 | 节次 |
| --- | --- |
| $\mathcal{P}$ | 0. 1 |
| $\sim$, $[a]$ | 0. 1 |
| $\mathbf{N}$ | 0. 2 |
| $C_A$ | 0. 3 |
| $\neg$, $\rightarrow$ | 1. 1, 1. 2. 1, 2. 1. 2 |
| $\vee$, $\wedge$, $\leftrightarrow$ | 1. 1, 1. 2. 5, 2. 1. 2 |
| $L(X)$, $L(X_n)$ | 1. 2. 1 |
| $L$, (L1) ~ (L3) | 1. 2. 2 |
| $\vdash$ | 1. 2. 2, 2. 1. 3 |
| MP | 1. 2. 2, 2. 1. 3, 3. 6. 4 |
| HS | 1. 2. 3, 2. 1. 3 |
| $L'$, (L′3), (L′4) | 1. 2 附 |
| $F$, $F'$, $G$, $H$ | 1. 2 附 |
| $\mathbf{Z}_2$ | 1. 3. 1 |
| $\models$ | 1. 3. 2, 2. 2. 4 |
| $\mid$, $\downarrow$ | 1. 5. 3 |
| $c_i$, $f_i^n$, $R_i^n$, $Y$ | 2. 1. 1 |
| $K(Y)$ | 2. 1. 2 |
| $\forall$, $\exists$ | 2. 1. 2 |
| $K$, (K1) ~ (K5) | 2. 1. 3 |
| Gen | 2. 1. 3 |
| $\exists_1$, $\exists_2$ | 2. 1. 3 |
| $\Pi_n$, $\Sigma_n$ | 2. 1. 4 |
| $\overline{c_i}$ | 2. 2. 1 |
| $\Phi_M$ | 2. 2. 1 |
| $\lvert p \rvert$ | 2. 2. 2 |
| $\lvert p \rvert_M$ | 2. 2. 3 |
| $\approx$ | 3. 1 |
| $E$, (E1) ~ (E3) | 3. 1 |
| $K_{\mathbf{N}}$ | 3. 2 |

# 参 考 文 献

[1] 胡世华, 陆钟万. 数理逻辑基础: 上, 下册 [M]. 北京：科学出版社,1981,1982.

[2] 王宪均. 数理逻辑引论 [M]. 北京：北京大学出版社,1982.

[3] 莫绍揆. 数理逻辑教程 [M]. 武汉：华中工学院出版社,1982.

[4] BARNES D W, MACK J M. An Algeberaic Introduction to Mathematical Logic[M]. 1975.

[5] BARWISE J, et al. Handbook of Mathematical Logic[M]. North-Holland, 1977.

[6] BELL J, et al. A Course in Mathematicel Logic[M]. North-Holland, 1977.

[7] HAMILTON A G. Logic for Mathematicians[M]. Cambridge University Press, 1978.

[8] KNEEBONE G T. Mathematical Logic and the Foundations of Mathematics[M]. Van Nostrand,1963.

[9] MALITZ J. Lntroduction to Mathematical Logic[M]. Springer-Verlag, 1979.

[10] MANIN Y I. A Course in Mathematical Logic[M]. Springer-Verlag, 1977.

[11] MENDELSON E. Introduction to Mathematical Logic[M]. Fourth Edition. Chapman- Hall, 1997.

[12] SHOENFIELD J R. Mathematical Logic[M]. Addison-Wesley, 1967.

[13] 王浩. 数理逻辑通俗讲话 [M]. 北京：科学出版社,1981.

[14] 汪芳庭. 数理逻辑文集 I:An easily porved form of the theorem of unprovability of consistency[M]. 北京：北京大学出版社,1989.

[15] 汪芳庭. 数学基础 [M]. 北京：科学出版社,2001.

[16] 王浩. 哥德尔 [M]. 康宏逵, 译. 上海译文出版社,1997.

[17] 秦一明. 形式 Peano 算术的 Gödel 不完备性定理的一个简单证明 [J]. 中国科学技术大学学报, 2003,33(6).

[18] A Tribute to Kurt Gödel[J]. Notices of the American Mathematical Society, 2006,4(53).

[19] 刘晓力. 理性的生命：哥德系思想研究 [M]. 长沙：湖南教育出版社，2000.

[20] 马丁 • 戴维斯. 逻辑的引擎 [M]. 张卜天，译. 长沙：湖南科学技术出版社，2005.

选题编辑　肖向兵
责任编辑　孔庆勇
封面设计　汇鑫文化

定价：22.00 元

ISBN 978-7-312-02708-6