0032439

史前史学

A.G. 汉密尔顿著

朱 水 林 译

程 其 寒 校

华东师范大学出版社

2 022 8722 0

数理逻辑

A. G. 汉密尔顿 著
朱水林 译
程其襄 校

华东师范大学出版社

2 022 8722 0

数 理 逻 辑

朱水林 译

程其襄 校

华东师范大学出版社出版
(上海中山北路3663号)
新华书店上海发行所发行 华东师大印刷厂印刷
开本: 850×1168 1/32 印张: 8.125 字数: 210千字
1986年11月第一版 1986年11月第一次印刷
印数: 1—4000本

统一书号: 2135·010 定价: 1.65元

LOGIC FOR MATHEMATICIANS

A. G. HAMILTON

(Cambridge University 1978)

前　言

每位数学家必定知道，对于不懂数学的人提出的关于他的工作的性质的询问，他的回答如何使谈话难以继续．逻辑学家在和数学家交往中，也认识到他的职业也会招致类似的对待．数学家和普通人之间在这方面的隔阂恐怕永远消除不了(尽管应尽量缩小它)．但是逻辑学家和数学家之间的隔阂，照我看来是可以克服的．本书就是一个尝试，想通过为并不渴望成为逻辑学家的数学工作者提供一个逻辑引论，以期在两者的间隙处架起一座桥梁．

目前在许多大学中，数理逻辑已被当作数学、计算机专业的大学生课程的一部分．现今学科本身已发展得相当完整，在基础课程中所包括的基本材料已具有标准的形态．本书可以当作这样一门课程的教材，当然其中有些材料是超出了范围的．本书在材料的选取方面经过深思熟虑，按直接的方式给出，因而对主题的各个方面，无论对应用和发展方面都没有特别的偏爱．同时力图使学科处理得从数学上看宛如一个整体，并特别强调逻辑对于数学工作者的重要性．

本书设想可以为任何具有一定数学基础的人接受，包括从一年级的大学生到专业的数学工作者，只要他们希望和要求对数理逻辑有所了解．对初等代数和数论的一定程度的熟悉是被假定了的．由于可数集和不可数集的观念甚为基本，所以写了一个附录，专门描述了必要的知识．

本书的材料，是在对斯梯林大学三、四年级学生所作的、分成两门课程的十六次讲演的基础上发展形成的．第一门课程包括第一章到第四章和第五章的一部分，余下的材料构成第二门课程，是

较为高级的选修课程．第六章是本书中最为困难的，但是由于哥德尔不完全性定理的重要意义，使得在这种类型的教本中应该给出它的证明的思想．因为第七章的材料并不依赖它，所以第一次阅读时，可以略去定理的详细证明部分．

本书的内容与其它有关本学科的标准引论相比要有限一点．特别是模型论和公理集合论几乎没有接触．因此，对这些内容感兴趣的读者，可以参阅书末列出的进一步阅读材料．其中有些在课文中还会专门提及(用作者的名字)．这些材料提供了数理逻辑的最为广泛的领域，并且对本书的论题作了更为深入的阐述．

书中每节末都附有练习题．一般来说机械的例子在比较费力的例子之前，不过所有的例子都是专门为相应的章节中的材料的直接应用而设计的，其目的是为了搞清楚和巩固已学的材料，而并非为了扩充知识．在书末写出了许多练习题的提示和解答．

本书采用的符号尽可能想标准化．但是为简洁起见，也引入一些非标准的用法．这些符号对熟悉材料的读者不会带来麻烦，而对材料生疏的读者却会有所帮助．不同的作者使用不同的记法和符号体系是一件不幸的事实．由于这个原因，为便于参照，书中专门列了一张符号对照表．在整本教材中，符号 ▷ 用来表示，在被命题，例子，注记，系或定义打断后重新恢复的主要论述．

致谢(略……)

A. G. 汉密尔顿

1978 年

目　录

前言
第一章　非形式的命题演算 ……（1）
1·1　命题和联结词……（1）
1·2　真值函数和真值表……（4）
1·3　运算和代入规则……（11）
1·4　范式……（16）
1·5　联结词的完全集……（20）
1·6　论证和有效性……（24）
第二章　形式的命题演算 ……（29）
2·1　形式系统 L……（29）
2·2　L 的完备性定理……（41）
第三章　非形式的谓词演算 ……（51）
3·1　谓词和量词……（51）
3·2　一阶语言……（56）
3·3　解释……（65）
3·4　满足，真 ……（68）
第四章　形式的谓词演算 ……（82）
4·1　形式系统 K_{ε}……（82）
4·2　等值，代入 ……（91）
4·3　前束范式……（97）

4·4 K 的完备性定理 ……(108)
4·5 模型……(113)

第五章 数学系统 ……(118)

5·1 引论……(118)
5·2 带等号的一阶系统……(119)
5·3 群论……(126)
5·4 一阶算术……(131)
5·5 形式集合论……(136)
5·6 一致性和模型……(142)

第六章 哥德尔不完全性定理 ……(145)

6·1 引论……(145)
6·2 可表达性……(147)
6·3 递归函数和递归关系……(156)
6·4 哥德尔数……(165)
6·5 不完全性的证明……(170)

第七章 可计算性，不可解性，不可判定性 ……(177)

7·1 算法和可计算性……(177)
7·2 图灵机……(186)
7·3 字问题……(206)
7·4 形式系统的不可判定性……(212)

附录 可数集和不可数集 ……(223)

部分习题的提示和解答 ……(228)
参考书目 ……(248)
符号表 ……(249)

第一章　非形式的命题[1]演算

1·1　命题和联结词

逻辑或者至少逻辑数学是由演绎组成的．我们应该仔细考察精确地使用着的演绎规则，这种精确性是数学方法的特征．在这样做时，如果我们要求某种程度精确性的话，就必须使我们的语言无歧义，标准的数学处理方法是引进一种符号语言，它具有能够精确叙述其意义和使用方法的符号．首先我们将要考察的是日常语言的一个方面的内容，即联结词(或连接词，它是更一般的语法术语)．

当我们尝试着分析英语句子时，首先注意的是：这是一简单句还是一复合句．简单句只有一个主词和一个谓词(在语法意义下)，例如

拿破仑死了．

约翰欠杰姆两磅钱．

所有不是方的鸡蛋都是圆的．

主语下面都划了直线，余下部分为谓词．一个复合句由几个简单句通过联结词构成．例如

拿破仑死了并且世界正在欢腾．

如果所有鸡蛋不是方的，那么所有鸡蛋是圆的．

如果气压计下降，那么或者要下雨或者要下雪．

我们将把一切简单句看作非真必假，以此作为一个基本假设．无疑人们可以争论说，有些句子并不能看作非真必假，为此我们将使用另一个术语，简单命题和复合命题，我们的假设是一切命题都

① 原文为 Statement，一般译陈述，为与习惯相符，本书译为命题．——译者注．

非真必假.

简单命题将用大写字母 A, B, C, …表示. 因而为了表示复合命题, 我们必须引进表示联结词的符号. 最通用的联结词和用来表示它们的符号, 在下表中给出:

非 A	$\sim A$
A 和 B	$A \wedge B$
A 或 B	$A \vee B$
如果 A 那么 B	$A \rightarrow B$
A 当且仅当 B	$A \leftrightarrow B$

当然, 如果这些符号的意义要精确地加以定义的话, 我们必须有把握说, 我们确切懂得左边一列中所表达的意义. 不久我们将再讨论这些.

这样, 上述三个复合命题就可以(相应地)用符号表示为:

$$A \wedge B$$

$$C \rightarrow D$$

$$E \rightarrow (F \vee G)$$

其中 A 表示"拿破仑死了", B 表示"世界正在欢腾", C 表示"所有鸡蛋不是方的"等等.

注意, 当一个复合命题按这种方式用符号表示后, 留下的仅是个逻辑框架, 一个纯粹的命题形式, 它可能为几个不同的命题所共有. 这使得我们能精确地分析演绎. 因为演绎只能用论证中命题的'形式'进行分析, 而不依赖于它们的意义.

例 1·1

如果苏格拉底是人, 那么苏格拉底有死.

苏格拉底是人.

∴ 苏格拉底有死.

这是逻辑上适当的论证. 但是考察论证

苏格拉底是人.

∴ 苏格拉底有死.

结论也可以认为是由前提推得的，然而其所以如此是由于词'人'和'有死'的意义，而不是由于单纯的逻辑演绎. 让我们用符号来表示这些论证

$$\begin{array}{ll} A \to B & \\ A & \qquad\qquad A \\ \therefore\ B & \qquad\qquad \therefore\ B \end{array}$$

使第一式有效的在于'形式'. 任何具有这同一形式的论证应该都有效. 这是我们关于如果……那么……这样的命题的逻辑直觉. 但是第二式却并不具有这种属性. 存在着许多这种形式的论证，我们的直觉并不认为是有效的. 例如

月亮是黄的.

∴ 月亮由乳酪造成.

为此，我们研究命题形式要基于研究具体的命题. 字母 p, q, r, … 称为命题变元，它们表示任意的非特定的单个命题. 注意字母 p, q, r, … 和字母 A, B, C, … 用法之间的区别，前者是变元，可以用特殊的简单命题代入. 后者只是特殊命题的'标记'. 变元使得我们能一般地去刻划命题和联结词所具有的属性. 现在，每个简单命题非真必假，因而一个给定的命题变元可以看成取下列两真值之一：T(真)或 F(假). 一个复合命题或命题形式的真或假，是怎样依赖于构成它的简单命题或命题变元的真或假的，这是下一节的主题.

练习

1. 把下列复合命题用符号表示：

(a) 如果支付不变，价格上涨，那么流通将减少.

(b) 我们将赢得选举，如果 Jones 当选为党的领导人.

(c) 如果 Jones 没有当选为党的领导人，那么不是 Smith 就是 Robinson 退出内阁，而我们的选举将失败.

(d) 如果 x 是有理数且 y 是整数，那么 z 不是实数.

(e) 或者是杀人犯已离开国家，或者某人隐匿了他.

(f) 如果杀人犯已离开国家，那么某人隐匿了他.

(g) 两个数的和是偶数，当且仅当两数皆为偶数或两数皆为奇数.

(h) 如果 y 是整数那么 z 不是实数，假如 x 是一有理数的话.

2. (a) 从练习 1 列出的命题中挑选出具有相同形式的命题对.

(b) 从练习 1 列出的命题中，挑选出具有相同意义的命题对.

1·2 真值函数和真值表

让我们依次来考察联结词.

否定

一个命题 A 的否定，我们把它写成 $\sim A$. 显然，如果 A 真那么 $\sim A$ 假，并且如果 A 假那么 $\sim A$ 真，A 的意义是无关紧要的. 我们可用真值表加以刻划.

p	$\sim p$
T	F
F	T

这表给出了 $\sim p$ 的真值，当给定了 p 的真值时. 联结词 $\sim$ 引出一个真值函数 $f^{\sim}$，即由真值表给出的从集 $\{T, F\}$ 到自身的一个函数. 那就是

$$f^{\sim}(T)=F$$
$$f^{\sim}(F)=T$$

合取

如上，易见由两个命题 A 和 B 构成的合取 $A\wedge B$ 的真值仅依赖于 A 的真值和 B 的真值. 我们有表：

p	q	$p\wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

我们对 p、q 的真值的每种可能的组合，在表中用一行表示，最后一列给出相应于 $p\wedge q$ 的真值．因此联结词 $\wedge$ 定义了一个二元真值函数 $f^{\wedge}$．

$$f^{\wedge}(T, T)=T$$
$$f^{\wedge}(T, F)=F$$
$$f^{\wedge}(F, T)=F$$
$$f^{\wedge}(F, F)=F$$

析取

我们曾用 $A\vee B$ 表示'A 或 B'．但是，在英语中有两种不同的对'或'这个词的标准用法．'A 或 B'可以意指相容的，也可意指相斥的．为了保持我们的符号语言的精确性，我们必须仅选取其中之一作为我们的符号 $\vee$ 的意义．我们选择了前者．对此并无什么特殊理由，我们照样也可选择后者．相容析取的真值表如下：

p	q	$p\vee q$
T	T	T
T	F	T
F	T	T
F	F	F

联结词 $\wedge$ 和 $\vee$ 一样，定义了一个二元真值函数．

注记：如果 A 和 B 是简单命题，我们可以用符号表示'相斥的 A 或 B'为

$$(A\vee B)\wedge\sim(A\wedge B).$$

相应地，如果我们用'相斥的 A 或 B'定义我们的析取符号，我们可以用析取连词 $\wedge$ 和 $\sim$ 表示'相容的 A 或 B'．

条件词

$A \to B$ 用来表示命题'A 蕴涵 B'或'如果 A那么 B'. 现在,在这种情况下,规范的英语用法无助于构造一个真值表,我们所用的表是直觉上发生困难的一个共同根源. 它是

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

困难在于当 A 为假时,给 $A \to B$ 指派真值 T. 对于一些条件命题的考察,其中前件是假的,或许会使人们得出这样的结论,即这命题根本就没有真值. 人们也可能获得这样的印象,这样的命题是无用的或者是无意义的. 例如,命题:

如果草是红的,那么月亮由绿乳酪造成.

全然能说成是无意义的.

但是,我们感兴趣的主要是数学中的演绎和证明方法. 在这种情况下,一个条件命题 $A \to B$ 的意义在于,它的真使得从 A 真可以推断 B 的真,而没有什么特别的要从 A 假推出. 一个很普通的数学命题就可以说明这一点. 例如,一个全称命题:

对于每个整数 n,如果 $n>2$ 那么 $n^2>4$.

这可以看作是关于整数的一个真命题. 因此,我们可以期待,命题

如果 $n>2$ 那么 $n^2>4$

是真的,而无需过问 n 取的什么值. n 的不同取值,给出了对于'$n>2$'和'$n^2>4$'的除去 T, F 外所有可能的真值组合,取 n 为 3, -3, 1,相应地会产生组合 TT, FT, FF,这些按我们的真值表,给这个蕴涵的真值为 T. 因此这个蕴涵在直觉上的真,是真值表的合理性的某种辩护. 须记住的要点是,仅当 A 真 B 假时,命题 $A \to B$ 被看成是假的.

双条件词

我们用 $A\leftrightarrow B$ 来表示'当且仅当'，这里的情况是清楚的．当且仅当 A 和 B 有相同的真值（同真或同假）时，我们有 $A\leftrightarrow B$ 为真．因此真值表如下：

p	q	$p\leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

至此我们的联结词已全部列出．显然，任何长度的复合命题都可以用这些联结词从简单命题逐步构成．使用命题变元我们能够构成任意长度的命题形式．

定义 1·2

一个命题形式是一个含有命题变元和联结词的表达式，并且能用以下规则构成：

(i) 任何命题变元是一命题形式．

(ii) 如果 $\mathscr{A}$ 和 $\mathscr{B}$ 是命题形式，那么 $(\sim\mathscr{A})$，$(\mathscr{A}\wedge\mathscr{B})$，$(\mathscr{A}\vee\mathscr{B})$，$(\mathscr{A}\rightarrow\mathscr{B})$ 和 $(\mathscr{A}\leftrightarrow\mathscr{B})$ 是命题形式．

例 1·3

$((p\wedge q)\rightarrow(\sim(q\vee r)))$ 是一命题形式．根据 (i)，p，q，r 是命题形式．根据 (ii)，$(p\wedge q)$ 和 $(q\vee r)$ 是命题形式．根据 (ii)，$(\sim(q\vee r))$ 是命题形式．根据(ii)，$((p\wedge q)\rightarrow(\sim(q\vee r)))$ 是命题形式．

▷ 这个定义是归纳定义的一个例子．它提供了一种模式，当我们详细描述形式系统时，它将再次出现．

联结词决定简单的真值函数．使用对这些联结词的真值表，我们能够为任何给定的命题形式构造一真值表．这是指的这样一个表，它对于出现在命题形式中命题变元的任意的真值指派，指出命题形式所取的真值．真值表是一个真值函数的图表表示．这样

每个命题形式给出一个真值函数，函数的自变元个数就是出现在命题形式中的命题变元的个数．让我们用几个例子加以说明：

例 1·4

(a) $((\sim p)\vee q)$．

首先构造真值表：

p	q	$\sim p$	$((\sim p)\vee q)$
T	T	F	T
T	F	F	F
F	T	T	T
F	F	T	T

可以看到相应于这个命题形式的真值函数，与$(p\rightarrow q)$所决定的真值函数是相同的．

(b) $(p\rightarrow(q\vee r))$．

真值表：

p	q	r	$(q\vee r)$	$(p\rightarrow(q\vee r))$
T	T	T	T	T
T	T	F	T	T
T	F	T	T	T
T	F	F	F	F
F	T	T	T	T
F	T	F	T	T
F	F	T	T	T
F	F	F	F	T

这里的真值函数是三元函数，因为有三个命题变元．表格的每一行给出了字母的真值取不同组合时真值函数的值．注意，任何含有三个命题变元的命题形式的真值表，都将有八行，如同上述表格的前三列书写的模式．p，q，r 名下的 T 和 F 的这种分组方法保证了每种可能的组合能且仅能出现一次．

▷一般情况下，对一个含有 n 个不同的命题变元的命题形式（n 为任意自然数），真值函数将是 n 元函数，真值表将有 2^n 行，相

应于命题变元真值的每一种可能的组合有一行．注意，有 2^{2^n} 个不同的 n 元真值函数，它们对应于在有 2^n 行的真值表的最后一列中的 T 和 F 的 2^{2^n} 种可能的排列方式．用 n 个命题变元可能构造的命题形式的数目显然是无限的，由此可知不同的命题形式可以对应于同一个真值函数．

为了进一步的研究，我们需要某些定义．

定义 1·5

(a) 一命题形式称为重言式，如果对于其中出现的命题变元的各种可能的真值指派，它总取真值为 T．

(b) 一命题形式称为矛盾式，如果对出现的命题变元的各种可能的真值指派，它总取真值为 F．

▷ 并非每个命题形式总属于这些范畴之一．实际上，至今已考察过的，尚未有一个是这样的．

例 1·6

(a) $(p\vee\sim p)$是一重言式．

(b) $(p\wedge\sim p)$是一矛盾式．

(c) $(p\leftrightarrow(\sim(\sim p)))$是一重言式．

(d) $(((\sim p)\rightarrow q)\rightarrow(((\sim p)\rightarrow(\sim q))\rightarrow p))$是一重言式．

要证实一个给定的命题形式是否重言式或矛盾式，可用的方法是构造真值表．

▷ 从定义可知，一切含有 n 个命题变元的重言式给出同一个 n 元真值函数，即总是取值为 T 的．对于矛盾式可以看到类似的情况．

定义 1·7

设$\mathscr{A}$和$\mathscr{B}$是命题形式，我们说 $\mathscr{A}$ 逻辑蕴涵 $\mathscr{B}$，如果$(\mathscr{A}\rightarrow\mathscr{B})$是一重言式．我们说 $\mathscr{A}$ 逻辑等值 $\mathscr{B}$，如果$(\mathscr{A}\leftrightarrow\mathscr{B})$是一重言式．

例 1·8

(a) $(p\wedge q)$逻辑蕴涵 p．

(b) $(\sim(p\wedge q))$逻辑等值$((\sim p)\vee(\sim q))$。

(c) $(\sim(p\vee q))$逻辑等值$((\sim p)\wedge(\sim q))$。

对(a)：$((p\wedge q)\to p)$的真值表：

$((p$	$\wedge$	$q)$	$\to$	$p)$
T	T	T	T	T
T	F	F	T	T
F	F	T	T	F
F	F	F	T	F

对(b)：

$(\sim$	$(p$	$\wedge$	$q)$	$\leftrightarrow$	$((\sim$	$p)$	$\vee$	$(\sim$	$q)))$
F	T	T	T	T	F	T	F	F	T
T	T	F	F	T	F	T	T	T	F
T	F	F	T	T	T	F	T	F	T
T	F	F	F	T	T	F	T	T	F

这里我们引进了真值表的另一种写法，对于复杂的命题形式来说，这样构造表要容易一些．开始时，我们按上表那样的次序写出命题变元下各列的 T 和 F，以保证每种组合只出现一次．当然，在整个过程中要做到一致，然后，在各联结词下相继地插入各部分的真值，直到给出整个命题形式的真值的一列填满为止．这一列在上面例子中是用竖线围起来的．

练习

3．写出下列命题形式的真值表：

(a) $((\sim p)\wedge(\sim q))$；

(b) $\sim((p\to q)\to(\sim(q\to p)))$；

(c) $(p\to(q\to r))$；

(d) $((p\wedge q)\to r)$；

(e) $((p\leftrightarrow(\sim q))\vee q)$；

(f) $((p\wedge q)\vee(r\wedge s))$；

(g) $(((\sim p)\wedge q)\to((\sim q)\wedge r))$；

(h) $((p\to(q\to r))\to((p\to q)\to(p\to r)))$.

4. 证明命题形式$((\sim p)\vee q)$和$(p\to q)$给出同一真值函数，$((\sim p)\to(q\vee r))$和$((\sim q)\to((\sim r)\to p))$给出同一真值函数.

5. 下列命题函数，那些是重言式？

(a) $(p\to(q\to p))$；

(b) $((q\vee r)\to((\sim r)\to q))$；

(c) $((p\wedge(\sim q))\vee((q\wedge(\sim r))\vee(r\wedge(\sim p))))$；

(d) $((p\to(q\to r))\to((p\wedge(\sim q))\vee r))$.

6. 证明下列命题形式对，是逻辑等值的.

(a) $(p\to q)$，$((\sim q)\to(\sim p))$；

(b) $((p\vee q)\wedge r)$，$((p\wedge r)\vee(q\vee r))$；

(c) $(((\sim p)\wedge(\sim q))\to(\sim r))$，$(r\to(q\vee p))$；

(d) $(((\sim p)\vee q)\to r)$，$((p\wedge(\sim q))\vee r)$.

7. 证明命题形式$(((\sim p)\to q)\to(p\to(\sim q)))$不是重言式. 求命题形式$\mathscr{A}$和$\mathscr{B}$，使得$(((\sim\mathscr{A})\to\mathscr{B})\to(\mathscr{A}\to(\sim\mathscr{B})))$是一矛盾式.

1·3 运算和代入规则

命题 1·9

如果$\mathscr{A}$和$(\mathscr{A}$[illegible]是动物，因此每日刷牙[illegible]是重言式.

重[illegible]了$\mathscr{B}$不是重言式. 那

时复[illegible]元的一个真值指派，

么，存在着一个对出[illegible]

现，[illegible]言式，该指派一定给

使得$\mathscr{B}$的值为F.

式[illegible]$\mathscr{A}\to\mathscr{B})$是重言式的

$\mathscr{A}$值为T，从而给[illegible]

假设矛盾. 因此$\mathscr{B}$[illegible]到这[illegible]

▷ 考察命题形式$(p\to p)$. 容易证明这是一个重言式. 现在我们用命题形式[illegible]代入两处出现的p，我们得到

$$((r\wedge s)\to t)\to((r\wedge s)\to t)),$$

这也是一个重言式；直觉上很明显然，不管我们用什么样的命题

形式代入 p，只要我们在 p 出现的地方处处用它代入，必将出现上述情况．（命题形式 $(p\to((r\wedge s)\to t))$ 显然不是重言式．）我们把这个思想概括成一个命题．

命题 1·10

令 $\mathscr{A}$ 是一个命题形式，其中有命题变元 $p_1, p_2, \cdots, p_n$，并且令 $\mathscr{A}_1, \mathscr{A}_2, \cdots, \mathscr{A}_n$ 是任意的命题形式．如果 $\mathscr{A}$ 是一个重言式，那么由 $\mathscr{A}$ 通过用 $\mathscr{A}_i$ 到处去替换每个 p_i 的出现而得到的 $\mathscr{B}$ 也是一重言式．

证明 令 $\mathscr{A}$ 是一个重言式，$p_1, p_2, \cdots, p_n$ 是出现在 $\mathscr{A}$ 中的命题变元．再令 $\mathscr{A}_1, \mathscr{A}_2, \cdots, \mathscr{A}_n$ 是任意的命题形式．对出现在 $\mathscr{A}_1, \mathscr{A}_2, \cdots, \mathscr{A}_n$ 中的命题变元给以任意的真值指派．此时 $\mathscr{B}$ 所取的真值，和 $\mathscr{A}$ 在分别把 $\mathscr{A}_1, \mathscr{A}_2, \cdots, \mathscr{A}_n$ 所取的真值指派到 $p_1, p_2, \cdots, p_n$ 时将取的真值是相同的，即 T．所以 $\mathscr{B}$ 在任何指派下所取的值为 T，也就是说 $\mathscr{B}$ 是重言式．

▷ 命题 1·10 是我们将要遇到的几个广泛地而常不自觉地应用到的几个命题之一．作为一个例子，下面的命题就是一个有用的结果．

命题 1·11

对于任意的命题形式 $\mathscr{A}$ 和 $\mathscr{B}$，总有 $(\sim(\mathscr{A}\wedge\mathscr{B}))$ 逻辑地等值于 $((\sim\mathscr{A})\vee(\sim\mathscr{B}))$，并且 $(\sim(\mathscr{A}\vee\mathscr{B}))$ 逻辑地等值于 $((\sim\mathscr{A})\wedge(\sim\mathscr{B}))$．

证明 我们先前已看到

$$((\sim(p\wedge q)\leftrightarrow((\sim p)\vee(\sim q)))$$

是一个重言式．对于任何命题形式 $\mathscr{A}$ 和 $\mathscr{B}$，

$$((\sim(\mathscr{A}\wedge\mathscr{B}))\leftrightarrow((\sim\mathscr{A})\vee(\sim\mathscr{B})))$$

为重言式是命题 1·10 的推论．因此 $(\sim(\mathscr{A}\wedge\mathscr{B}))$ 是逻辑等值于 $((\sim\mathscr{A})\vee(\sim\mathscr{B}))$．另一部分可类似地证明．

例 1·12

对任意的命题形式 $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$ 来说，总有$(\mathscr{A}\wedge(\mathscr{B}\wedge\mathscr{C}))$逻辑等值$((\mathscr{A}\wedge\mathscr{B})\wedge\mathscr{C})$. （由此，我们通常消去内括号，写成$(\mathscr{A}\wedge\mathscr{B}\wedge\mathscr{C})$.[1]）

考察命题形式

$$(((p_1\wedge(p_2\wedge p_3))\leftrightarrow((p_1\wedge p_2)\wedge p_3))).$$

用通常的方法构造真值表便能证明这是一个重言式. 现在应用命题 1·10, 以 $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$ 分别代入 p_1, p_2, p_3, 即得所要求的结果.

例 1·13

对任何命题形式 $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$, 下列命题对是逻辑等值的.

(a) $(\mathscr{A}\vee(\mathscr{B}\vee\mathscr{C}))$和$((\mathscr{A}\vee\mathscr{B})\vee\mathscr{C})$.

(b) $(\mathscr{A}\wedge\mathscr{B})$和$(\mathscr{B}\wedge\mathscr{A})$.

(c) $(\mathscr{A}\vee\mathscr{B})$和$(\mathscr{B}\vee\mathscr{A})$.

这些命题的证明可用上例提供的同样模式.

▷ 现在考察命题形式 $((p\wedge p)\rightarrow q)$. $(p\wedge p)$ 出现在这个形式中，它逻辑等值于 p(因为$((p\wedge p)\leftrightarrow p)$是一重言式)，如果我们用 p 替换 $(p\wedge p)$，我们得 $(p\rightarrow q)$. 现在 $(p\rightarrow q)$ 是逻辑等值于$((p\wedge p)\rightarrow q)$(通过真值表检验). 这又是一个关于代入的一般命题的实例.

命题 1·14

如果 $\mathscr{B}_1$ 是由命题形式 $\mathscr{A}_1$ 通过以命题形式 $\mathscr{B}$ 代入 $\mathscr{A}_1$ 中的命题形式 $\mathscr{A}$ 的一次或多次出现而得的命题形式，又如果 $\mathscr{B}$ 逻辑等值于 $\mathscr{A}$, 那么 $\mathscr{B}_1$ 也逻辑等值于 $\mathscr{A}_1$.

证明　假设 $\mathscr{B}$ 逻辑等值 $\mathscr{A}$, $\mathscr{B}_1$ 和 $\mathscr{A}_1$ 如上所述. 我们希望证明$(\mathscr{A}_1\leftrightarrow\mathscr{B}_1)$是重言式. 对所有涉及的命题变元指派真值. $\mathscr{B}_1$ 和 $\mathscr{A}_1$ 不同之处仅在于原来 $\mathscr{A}$ 的有几处换成了 $\mathscr{B}$. 由于 $\mathscr{A}$ 和 $\mathscr{B}$ 有相同的真值，$\mathscr{B}_1$ 一定和 $\mathscr{A}_1$ 取相同的真值. 所以$(\mathscr{A}_1\leftrightarrow\mathscr{B}_1)$取值 T. 由于原来对变元指派的真值是任意的，因而可以推得

$(\mathscr{A}_1 \leftrightarrow \mathscr{B}_1)$总取值 T. 所以$(\mathscr{A}_1 \leftrightarrow \mathscr{B}_1)$是重言式，即 $\mathscr{A}_1$ 逻辑等值于 $\mathscr{B}_1$.

▷ 下一命题尽管不是理论展开的组成部分，然而我们还是将它放在此处，其原因是想让对我们后面将要使用的方法，获得一个初步的印象. 因此我们给它一个适当详细的证明.

命题 1·15

让我们把只含有联结词 ～，∧ 和 ∨ 的命题形式叫做限制的命题形式. 令 $\mathscr{A}$ 是一个限制的命题形式，并且假设 $\mathscr{A}^*$ 是由 $\mathscr{A}$ 通过在公式中相互交换 ∧ 和 ∨ 以及把每个命题变元替换成它的否定之后所得的结果. 那么 $\mathscr{A}^*$ 逻辑等值于$(\sim\mathscr{A})$.

证明 通过对出现在 $\mathscr{A}$ 中的联结词的数目 n 进行归纳而得到证明. 如果我们能够证明，对于每个自然数 n，恰好具有 n 个联结词的限制命题形式都满足该命题，那么显然就够了.

基础步骤：$n=0$($\mathscr{A}$ 不包含联结词). 在这种情况下，$\mathscr{A}$ 只能由一个命题变元 p 组成. 所以这里的 $\mathscr{A}^*$ 就是$(\sim p)$，显然 $\mathscr{A}^*$ 逻辑等值于$(\sim\mathscr{A})$.

归纳步骤：假设 $n>0$，$\mathscr{A}$ 有 n 个联结词，并且每个含有少于 n 个联结词的限制命题形式都有所要求的性质. 由于命题形式的构成方式，我们必须考察三种情况：

情形 1：$\mathscr{A}$ 有形式$(\sim\mathscr{B})$.

情形 2：$\mathscr{A}$ 有形式$(\mathscr{B}\vee\mathscr{C})$.

情形 3：$\mathscr{A}$ 有形式$(\mathscr{B}\wedge\mathscr{C})$.

对情形 1：$\mathscr{B}$ 有 $n-1$ 个联结词，所以据归纳假设 $\mathscr{B}^*$ 逻辑等值于$(\sim\mathscr{B})$. 而 $\mathscr{A}^*$ 是$(\sim\mathscr{B}^*)$，所以 $\mathscr{A}^*$ 逻辑等值于$(\sim(\sim\mathscr{B}))$即$(\sim\mathscr{A})$. 注意，这里我们几乎是在无意识的情况下使用了命题 1·14 的结果.

对情形 2：$\mathscr{B}$ 和 $\mathscr{C}$ 每个包含的联结词都少于 n，所以 $\mathscr{B}^*$ 和 $\mathscr{C}^*$ 分别逻辑等值于$(\sim\mathscr{B})$和$(\sim\mathscr{C})$. 现在 $\mathscr{A}^*$ 是$(\mathscr{B}^*\wedge\mathscr{C}^*)$. 据

命题 1·14 这逻辑等值于$((\sim\mathscr{B})\wedge\mathscr{C}^*)$，再据同一命题，它又逻辑等值于$((\sim\mathscr{B})\wedge(\sim\mathscr{C}))$. 现在我们已见到(命题 1·11)这又逻辑等值于$(\sim(\mathscr{B}\vee\mathscr{C}))$，即$(\sim\mathscr{A})$. 因此 $\mathscr{A}^*$ 逻辑等值于$(\sim\mathscr{A})$.

对于情形 3：如情况 2，$\mathscr{B}^*$ 和 $\mathscr{C}^*$ 分别逻辑等值于$(\sim\mathscr{B})$和$(\sim\mathscr{C})$. $\mathscr{A}^*$ 是$(\mathscr{B}^*\vee\mathscr{C}^*)$，逻辑等值于$((\sim\mathscr{B})\vee\mathscr{C}^*)$，也等值于$((\sim\mathscr{B})\vee(\sim\mathscr{C}))$；再等值于$(\sim(\mathscr{B}\wedge\mathscr{C}))$，即$(\sim\mathscr{A})$. 因此 $\mathscr{A}^*$ 逻辑等值于$(\sim\mathscr{A})$.

在每个含有少于 n 个联结词的限制的命题形式有所要求的性质的条件下，我们已经证明了每个含有 n 个联结词的限制的命题形式有所要求的性质. 因此，根据数学归纳法，每个限制性命题形式都具有所要求的性质.

系 1·16

如果 $p_1, p_2, \cdots, p_n$ 是命题变元，那么

$$((\sim p_1)\vee(\sim p_2)\vee\cdots\vee(\sim p_n))$$

逻辑等值于 $$(\sim(p_1\wedge p_2\wedge\cdots\wedge p_n)).$$

证明 这是命题 1·15 的特殊情况，其中 $\mathscr{A}$ 是命题形式$(p_1\wedge p_2\wedge\cdots\wedge p_n)$.

▷ 为简洁起见，我们引进一个新记号，把这结果写成

$$\left(\bigvee_{i=1}^{n}(\sim p_i)\right)\text{逻辑等值于}\left(\sim\left(\bigwedge_{i=1}^{n}p_i\right)\right).$$

我们也能用命题证明它的'对偶'，即

$$((\sim p_1)\wedge(\sim p_2)\wedge\cdots\wedge(\sim p_n))$$

逻辑等值于 $$\sim(p_1\vee p_2\vee\cdots\vee p_n),$$

即$\left(\bigwedge_{i=1}^{n}(\sim p_i)\right)$逻辑等值于$\left(\sim\left(\bigvee_{i=1}^{n}p_i\right)\right)$.

命题 1·17(德摩根规则)

令 $\mathscr{A}_1, \mathscr{A}_2, \cdots, \mathscr{A}_n$ 是任意的命题形式. 那么：

(i) $\left(\bigvee_{i=1}^{n}(\sim\mathscr{A}_i)\right)$逻辑等值于$\left(\sim\left(\bigwedge_{i=1}^{n}\mathscr{A}_i\right)\right)$.

(ii) $\left(\bigwedge_{i=1}^{n}(\sim\mathscr{A}_i)\right)$逻辑等值于$\left(\sim\left(\bigvee_{i=1}^{n}\mathscr{A}_i\right)\right)$.

证明：使用上面的系和命题1·10.

练习

8. 求证：对于任意的命题形式$\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$, 下列的命题形式对是逻辑等值的.

(a) $(\mathscr{A}\vee(\mathscr{B}\vee\mathscr{C}))$和$((\mathscr{A}\vee\mathscr{B})\vee\mathscr{C})$;

(b) $(\mathscr{A}\wedge\mathscr{B})$和$(\mathscr{B}\wedge\mathscr{A})$;

(c) $(\mathscr{A}\vee\mathscr{B})$和$(\mathscr{B}\vee\mathscr{A})$;

(d) $\mathscr{A}$和$\sim(\sim\mathscr{A})$.

9. 求证：对于任意的命题形式$\mathscr{A}$和$\mathscr{B}$, 下列命题形式是重言式.

(a) $((\mathscr{A}\wedge\mathscr{B})\rightarrow\mathscr{A})$;

(b) $((\mathscr{A}\wedge\mathscr{B})\rightarrow\mathscr{B})$.

10. 用命题1·14证明$((\sim((\sim p)\vee q))\vee r)$逻辑等值于$((p\rightarrow q)\rightarrow r)$.

11. 用命题1·14和1·17证明，命题形式$((\sim(p\vee(\sim q)))\rightarrow(q\rightarrow r))$逻辑等值于下列的每个命题形式.

(a) $((\sim(q\rightarrow p))\rightarrow((\sim q)\vee r))$;

(b) $(((\sim p)\wedge q)\rightarrow(\sim(q\wedge(\sim r))))$;

(c) $((\sim((\sim q)\vee r))\rightarrow(q\rightarrow p))$;

(d) $(q\rightarrow(p\vee r))$.

1·4 范式

让我们进一步考察我们称之为限制的命题形式. 我们显然已看到，对每个命题形式，我们能构造真值表. 现在来证明它的逆命题.

命题1·18

每个真值函数都是仅含联结词 ～，∧ 和 ∨ 的命题形式（即限制的命题形式）所确定的真值函数.

证明　假设给定的函数是一 n 元函数. 我们将用变项 $p_1, p_2, \cdots, p_n$ 构造一个命题形式 $\mathscr{A}$. 首先注意，如果对真值的每种组合真值函数都取值为 F，那么它对应于任一矛盾式，因此命题形式

$$((p_1 \wedge (\sim p_1)) \wedge p_2 \wedge p_3 \wedge \cdots \wedge p_n)$$

将符合要求.

现在假设真值函数至少有一次取值 T. 我们的方法在于构造这样的一个命题形式，在命题变元真值的 2^n 种组合中，它除对某个组合取值 T 外，对其余组合都取 F. 例如，如果 $n=3$，命题形式 $(p_1 \wedge (\sim p_2) \wedge (\sim p_3))$ 仅对 p_1, p_2, p_3 分别取真值 TFF 组合时才是真，$((\sim p_1) \wedge (\sim p_2) \wedge p_3)$ 仅对组合 FFT 才是真的. 这种特殊的命题形式称为基础合取式. 给出 $p_1, p_2, \cdots, p_n$ 的一个真值指派，对 $1 \leqslant i \leqslant n$，如果 p_i 指派为 T，我们在合取式中取 p_i；如果 p_i 指派为 F，我们在合取式中取 $(\sim p_i)$. 那么对给定的真值指派而言，每个合取项的值为 T，因而整个合取式的值为 T. 相应地，对任何其他的真值指派，至少有一个合取项的值将为 F，因此整个合取式将取值 F.

现在为证明我们的命题，考察所有使我们的真值函数取值为 T 的那些 n 个真值的组合. 令 $\mathscr{A}$ 是所有以这样的组合作为 $p_1, p_2, \cdots, p_n$ 的真值的基础合取式的析取式. 这个 $\mathscr{A}$ 就是所要求的命题形式. 要明白这点，指派 $p_1, p_2, \cdots, p_n$ 以真值. 如果我们的真值函数作用于这个组合时得到的值是 T，那么对应的基础合取式就包含在 $\mathscr{A}$ 中，并且在此真值指派下取值 T，所以 $\mathscr{A}$ 也取值为 T. 如果我们的真值函数作用于这个组合时得到的值是 F，那么对应的基础合取式就不包含在 $\mathscr{A}$ 中. 而每个在 $\mathscr{A}$ 中的不同于它的基础合取式对这个真值指派来说都取值为 F，所以 $\mathscr{A}$ 也取 F 值. 因此对任何真值指派，$\mathscr{A}$ 的真值与真值函数给出的真值相

间.

▷ 理解这个证明的最好的办法莫过于联系着一个具体例子来加以考察.

例 1·19

让我们通过表格列出一真值函数(这是三元函数).

T	T	T	T
T	T	F	T
T	F	T	F
T	F	F	F
F	T	T	F
F	T	F	F
F	F	T	F
F	F	F	T

能使函数取值为 T 的真值组合是 TTT, TTF 和 FFF. 相应地基础合取式是:

$$(p_1 \wedge p_2 \wedge p_3)$$
$$(p_1 \wedge p_2 \wedge (\sim p_3))$$
$$((\sim p_1) \wedge (\sim p_2) \wedge (\sim p_3)).$$

在证明中构造的命题形式 $\mathscr{A}$ 是

$$(p_1 \wedge p_2 \wedge p_3) \vee (p_1 \wedge p_2 \wedge (\sim p_3)) \vee ((\sim p_1) \wedge (\sim p_2) \wedge (\sim p_3)).$$

这命题形式相当于给定的真值函数, 给出的表就是这个命题形式的真值表.

系 1·20

每个非矛盾的命题形式逻辑等值于一个限制的命题形式 $\left(\bigvee_{i=1}^{m}\left(\bigwedge_{j=1}^{n} Q_{ij}\right)\right)$, 其中每个 Q_{ij} 或是一个命题变元, 或是一个命题变元的否定. 这个形式称为析取范式.

证明 两个命题形式逻辑等值当且仅当它们对应于同一真值函数. 对于给定的命题形式 $\mathscr{A}$, 求出它的真值表和它所定义的真

值函数．然后应用命题1·18的证明方法求出对应于这个真值函数的、并在形式上符合要求的命题形式．

系 1·21

每个非重言的命题形式逻辑等值于一个限制的命题形式 $\left(\bigwedge_{i=1}^{m}\left(\bigvee_{j=1}^{n} Q_{ij}\right)\right)$，其中每个 Q_{ij} 或是一个命题变元，或是一个命题变元的否定．这个形式称为合取范式．

证明 令 $\mathscr{A}$ 是一个非重言的命题形式．那么$(\sim\mathscr{A})$不是一个矛盾式，且逻辑等值于析取范式 $\left(\bigvee_{i=1}^{m}\left(\bigwedge_{j=1}^{n} Q_{ij}\right)\right)$．因此 $\mathscr{A}$ 逻辑等值于 $\sim\left(\bigvee_{i=1}^{m}\left(\bigwedge_{j=1}^{n} Q_{ij}\right)\right)$，使用德摩根规则，它逻辑等值于 $\left(\bigwedge_{i=1}^{m}\left(\bigvee_{j=1}^{n}(\sim Q_{ij})\right)\right)$．当在这个命题形式中都用 q 替换$(\sim(\sim q))$时，就可得到结果．

例 1·22

求一个合取范式，使它逻辑等值于

$$(((\sim p_1)\vee p_2)\rightarrow p_3)$$

首先求得它的否定的真值表

$\sim$	$(((\sim$	$p_1)$	$\vee$	$p_2)$	$\rightarrow$	$p_3)$
F	F	T	T	T	T	T
T	F	T	T	T	F	F
F	F	T	F	F	T	T
F	F	T	F	F	T	F
F	T	F	T	T	T	T
T	T	F	T	T	F	F
F	T	F	T	F	T	T
T	T	F	T	F	F	F

给出的值为 T 的组合是 TTF，FTF 和 FFF．所以逻辑等值于一个析取范式

$$((p_1\wedge p_2\wedge(\sim p_3))\vee((\sim p_1)\wedge p_2\wedge(\sim p_3))\vee((\sim p_1)\wedge(\sim p_2)\wedge(\sim p_3))$$

因而，已知的命题形式逻辑等值于这式的否定，据德摩根规则逻辑等值于

$$(\sim(p_1\wedge p_2\wedge(\sim p_3))\wedge\sim((\sim p_1)\wedge p_2\wedge(\sim p_3))$$
$$\wedge\sim((\sim p_1)\wedge(\sim p_2)\wedge(\sim p_3)).$$

等值于

$$(((\sim p_1)\vee(\sim p_2)\vee(\sim(\sim p_3)))\wedge((\sim(\sim p_1)\vee(\sim p_2)$$
$$\vee(\sim(\sim p_3)))\wedge((\sim(\sim p_1)\vee(\sim(\sim p_2))$$
$$\vee(\sim(\sim p_3))),$$

等值于

$$((\sim p_1)\vee(\sim p_2)\vee p_3)\wedge(p_1\vee(\sim p_2)\vee p_3)\wedge(p_1\vee p_2\vee p_3),$$

这是合取范式的形式。

练习

12．求析取范式的命题形式，使它逻辑等值于下列式：

(a) $(p\leftrightarrow q)$；

(b) $(p\rightarrow((\sim q)\vee r)$；

(c) $((p\wedge q)\vee((\sim q)\leftrightarrow r))$；

(d) $\sim((p\rightarrow(\sim q))\rightarrow r)$；

(e) $(((p\rightarrow q)\rightarrow r)\rightarrow s)$.

13．求合取范式的命题形式，使它逻辑等值于下列式：

(a) $(((\sim p)\vee q)\rightarrow r)$；

(b) $(p\leftrightarrow q)$；

(c) $(p\wedge q\wedge r)\vee((\sim p)\wedge(\sim q)\wedge r)$；

(d) $(((p\rightarrow q)\rightarrow r)\rightarrow s)$.

1.5 联结词的完全集

定义 1.23

一个联结词的完全集是这样一个集，使得每个真值函数都能由仅仅含有该集中的联结词的命题形式所表示。

▷ 上述讨论的推论之一是：{～，∧，∨} 是一个联结词的完全集．我们可利用它去求其它的完全集．

命题 1.24

对偶{～，∧}，{～，∨}和{～，→}都是联结词的完全集．

证明 首先，对任何命题 $\mathscr{A}$ 和 $\mathscr{B}$ 来说，$(\mathscr{A}\vee\mathscr{B})$是逻辑地等值于$(\sim((\sim\mathscr{A})\wedge(\sim\mathscr{B})))$，所以任何恰含有 {～，∧，∨} 的命题形式能变换为一个逻辑等值的仅含 ～ 和 ∧ 的命题形式．

其次，我们可以类似地用$(\mathscr{A}\wedge\mathscr{B})$和$(\sim((\sim\mathscr{A})\vee(\sim\mathscr{B})))$逻辑等值去证{～，∨}是完全的．

第三，我们必须找出只包含 ～ 和 → 的、且与 $(\mathscr{A}\wedge\mathscr{B})$ 和 $(\mathscr{A}\vee\mathscr{B})$逻辑等值的命题形式．

$(\mathscr{A}\wedge\mathscr{B})$逻辑等值于$(\sim(\mathscr{A}\to(\sim\mathscr{B})))$，

$(\mathscr{A}\vee\mathscr{B})$逻辑等值于$((\sim\mathscr{A})\to\mathscr{B})$．

这些使我们能把任何含 {～，∧，∨} 的命题形式变换成逻辑等值的仅含 ～ 和 → 的命题形式

例 1.25

$(((\sim p_1)\vee p_2)\to p_3)$逻辑等值于下列之一：

(a) $(\sim((\sim p_1)\vee p_2)\vee p_3)$．

(b) $\sim(\sim(p_1\wedge(\sim p_2))\wedge(\sim p_3))$．

(c) $((p_1\to p_2)\to p_3)$．

▷ 从我们的五个联结词中，有三种选择完全对的方式，不存在其它的完全对．为了搞清这一点，让我们首先来考察不含有'～'的联结词对，问：一个永假的真值函数能否用只含这样的联结词对的命题形式来表达呢？答案必然是否定的，因为给这样的命题形式中的一切命题变元以值 T，将必然给出整个命题形式的值为 T．在这样的真值指派之下，无法能使这命题形式的整体或部分取值为 F．所以没有一个只包含联结词 ∧，∨，→，↔ 的命题形式是矛盾式．因此，联结词的这种子集是不完全的．留给读者去

证明{～, ↔}不是完全集.

还有其他的联结词；事实上每一个真值表都可用来定义一个联结词，但是它们的直观含义将不会那么明显. 不过有两个却是值得一提的.

析非

用↓表示，真值表如下：

p	q	$(p\downarrow q)$
T	T	F
T	F	F
F	T	F
F	F	T

合非

用 | 表示，真值表如下

p	q	$p\|q$
T	T	F
T	F	T
F	T	T
F	F	T

所以对这些联结词感兴趣的理由(在计算机设计和研究中有重要性)具体见下面命题

命题 1.26

单元集{↓}和{|}是联结词的完全集，即每个真值函数都可由只含↓(或只含|)的命题形式表达.

证明 我们只须做到用↓(或用|)表达～和∧，或～和∨即可，因为已知{～, ∧}和{～, ∨}是完全的.

首先，　　$(\sim p)$逻辑等值于$(p\downarrow p)$,

和　　$(p\wedge q)$逻辑等值于$((p\downarrow p)\downarrow(q\downarrow q))$.

其次　　$(\sim p)$逻辑等值于$(p|p)$,

$(p\vee q)$逻辑等值于$((p|p)|(q|q))$.

验证和通常一样经由真值表构造，留作习题。

例 1·27

求一只含↓的命题形式，使它逻辑等值于$(p\to q)$

$(p\to q)$逻辑等值于$\sim(p\wedge(\sim q))$

从而等值于 $\sim(p\wedge(q\downarrow q))$

从而等值于 $\sim((p\downarrow p)\downarrow[(q\downarrow q)\downarrow(q\downarrow q)]$

从而等值于

$\{(p\downarrow p)\downarrow[(q\downarrow q)\downarrow(q\downarrow q)]\}\downarrow\{(p\downarrow p)\downarrow[(q\downarrow q)\downarrow(q\downarrow q)]\}$.

这个例子说明，如果人们只希望用一个联结词的话，他将在式子的复杂性和长度上付出多大代价。

练习

14. 求只含联结词 ～ 和 ∨ 的命题形式，使它逻辑等值于下列式：

(a) $(p\to(q\to r))$;

(b) $(((\sim p)\wedge(\sim q))\to((\sim r)\wedge s))$;

(c) $(p\leftrightarrow q)$.

15. 求只含联结词 ～ 和 ∧ 的命题形式，使它逻辑等值于下列式：

(a) $(p\to(q\to r))$;

(b) $((p\vee q\vee r)\wedge((\sim p)\vee(\sim q)\vee(\sim r)))$;

(c) $((p\leftrightarrow(\sim q))\leftrightarrow r)$.

16. 求只含联结词 ～ 和 → 的命题形式，使得逻辑等值于下列式.

(a) $((p\wedge q)\vee(r\wedge s))$;

(b) $(p\leftrightarrow q)$

(c) $(p\wedge q\vee r)$

17. (a) 证明{∧，∨}不是联结词的完全集。

(b) 较难证明{～, ↔}不是联结词的完全集.

18. 求只含联结词|的一个命题,使它逻辑等值于$(p\to q)$.

19. 证明,不存在不同于↓和|的两元联结词,其本身构成一个联结词的完全集.(提示:考察任何这样的联结词的真值表).

1·6 论证和有效性

现在,让我们回过来考察论证. 在目前我们必然地是局限于这样的论证,它的前提和结论都是本章开始时所定义的意义下的简单命题和复合命题. 我们已看到命题的'形式'比命题的意义更为重要. 所以我们将考察论证形式. 在前述的例子中,我们已遇到过命题形式

$$\begin{array}{ll} & (p\to q) \\ & p \\ \therefore & q \end{array}$$

一般来说,一个论证形式是有限个命题形式的序列,它的最后一个被看成是结论,余下部分是前提.

在判定和定义什么东西构成了一个'有效的'论证时,我们会遇到在蕴涵符号时已碰到过的同样类型的困难. 当我们对论证形式中的命题变元指派真值时,我们可能发现结论假并且有一个或几个前提也假,假前提能证明假结论为正确的吗?在一种意义下它是个无关紧要的问题,因为在正常习惯中,我们使用论证仅仅是为了证明,从已知前提确能推出某个结论. 因此,我们对一个有效论证所要求的一切,只是在任何对命题变元的真值指派下,如果所有前提都取T那么结论也要取T. 我们可以等价地作出如下定义.

定义 1·28

论证形式

$$\mathscr{A}_1, \mathscr{A}_2, \cdots, \mathscr{A}_n; \quad \therefore \quad \mathscr{A}_n$$

是无效的，如果可能对命题变元作这样的一个真值指派，使得 $\mathscr{A}_1$，$\mathscr{A}_2$，…，$\mathscr{A}_n$ 中每个取值 T 而 $\mathscr{A}$ 取值 F。否则论证是有效的。

▷ 现在我们面临着怎样检验一个给定的论证形式是否有效的问题。让我们来考察简单例子：$(p\to q)$，p；$\therefore q$。对所有出现在前提和结论中的命题形式，构造一个真值表。

p	q	$p\to q$
T	T	T
T	F	F
F	T	T
F	F	T

只在第一行，所有前提为 T，此时结论也取值 T。所以论证形式不是无效的，即是有效的。

例 1·29

研究下面论证形式的有效性：

$$(p\to q),\ ((\sim q)\to r),\ r;\quad \therefore\ p.$$

构造一个真值表：

p	$\to$	q	$((\sim$	$q)$	$\to$	$r)$	r	p	
T	T	T	F	T	T	T	T	T	←
T	T	T	F	T	T	F	F	T	
T	F	F	T	F	T	T	T	T	
T	F	F	T	F	F	F	F	T	
F	T	T	F	T	T	T	T	F	←
F	T	T	F	T	T	F	F	F	
F	T	F	T	F	T	T	T	F	←
F	T	F	T	F	F	F	F	F	

其中所有前提取值为 T 的为箭头所示的三行，但是第五、第七行的结论取值为 F。因此论证形式是无效的。

▷ 这里的方法，将使我们能在各种情况下，去判定一个论证形式的有效性。但是，如果不同的命题变元数很大时，我们的真值表就会流于笨拙而不切实用。无论如何，对我们的目的来说并不

需要整个真值表．我们的方法是搜寻一种特殊的行，我们可按一种系统的方式而不是按构造整个真值表那样的带有试验性的方式，来进行这种搜寻．其实际步骤最好是通过一个例子来描述．

例 1·30

检验下面的论证形式的有效性：

$((\sim p_1)\vee p_2),\ (p_1\rightarrow(p_3\wedge p_4)),\ (p_4\rightarrow p_2);\quad \therefore\quad (p_2\vee p_3).$

我们试图作一真值指派去证明论证形式的无效性，也就是说，要使得它前提真而结论假．为了使$(p_2\vee p_3)$取值 F，我们必须指派 p_2, p_3 每个以真值 F．因而，为了使$(p_4\rightarrow p_2)$取值 T，必须指派 p_4 以真值 F．为了使$((\sim p_1)\vee p_2)$取得 T，必须使 p_1 取值为 F．现在检验其它前提$(p_1\rightarrow(p_3\wedge p_4))$在这个指派下的真值，它是 T．因此

p_1	p_2	p_3	p_4
F	F	F	F

是这样的一个指派，它使一切前提取值为 T．而结论取值却为 F．所以论证形式是无效的．

注意，如果论证形式是有效的，我们将不能如所打算的那样指派真值．

例 1·31

检验以下论证的有效性：

$$(p_1\rightarrow(p_2\rightarrow p_3)),\ p_2;\quad \therefore\quad (p_1\rightarrow p_3).$$

我们试着给出真值指派去证明这论证形式的无效性．为了使$(p_1\rightarrow p_3)$取值 F，我们必须使 p_1 取值 T，p_3 取值 F．我们也要求 p_2 取值 T．在这个真值指派之下，其它的前提，$(p_1\rightarrow(p_2\rightarrow p_3))$取值 F．所以不可能指派真值，使得前提真而结论假，从而这个论证是有效的．

▷ 下面的命题给前面简略地提到的论证和蕴涵之间的联系精确化了．

命题 1.32

论证形式

$$\mathscr{A}_1, \cdots, \mathscr{A}_n; \quad \therefore \quad \mathscr{A}$$

是有效的，当且仅当命题形式

$$((\mathscr{A}_1 \wedge \cdots \wedge \mathscr{A}_n) \rightarrow \mathscr{A})$$

是一重言式.

证明：首先假设 $\mathscr{A}_1, \cdots, \mathscr{A}_n; \therefore \mathscr{A}$ 是一有效的论证形式，但 $((\mathscr{A}_1 \wedge \cdots \wedge \mathscr{A}_n) \rightarrow \mathscr{A})$ 不是一个重言式. 那么存在着一个对出现的命题变元的真值指派，使得 $\mathscr{A}_1 \wedge \cdots \wedge \mathscr{A}_n$ 取值 T，而 $\mathscr{A}$ 取值 F. 因此，对这个指派，每个 $\mathscr{A}_i$ 取值 $T(1 \leqslant i \leqslant n)$，而 $\mathscr{A}$ 取值 F. 这和论证形式的有效性是矛盾的，所以 $((\mathscr{A}_1 \wedge \cdots \wedge \mathscr{A}_n) \rightarrow \mathscr{A})$ 一定是重言式.

现在，相反地假设 $((\mathscr{A}_1 \wedge \cdots \wedge \mathscr{A}_n) \rightarrow \mathscr{A})$ 是重言式，但 $\mathscr{A}_1, \cdots, \mathscr{A}_n; \therefore \mathscr{A}$ 不是一有效论证形式. 那么存在一个真值指派使得每个 $\mathscr{A}_i(1 \leqslant i \leqslant n)$ 取值 T 而 $\mathscr{A}$ 取值 F，所以 $((\mathscr{A}_1 \wedge \cdots \wedge \mathscr{A}_n) \rightarrow \mathscr{A})$ 取值 F. 这和该命题形式是一重言式的假设矛盾，所以 $\mathscr{A}_1, \cdots, \mathscr{A}_n; \therefore \mathscr{A}$ 是一有效论证形式.

▷ 让我们在结束本章时，顺便说一下上面证明中，碰巧地用到的为大家熟悉的"间接证明"或归缪法的数学方法.

这样的证明在于，从要证明的命题的否定出发去推出一个矛盾. 用本章的术语来说这个程序的合法性从下面可以看出来. 如果我们有一个论证，它已知是一个有效论证形式的特例，而它的结论是假的，那么在其前提中一定至少有一个是假的. 如果除一个（假设的那个）外，其余前提都真，那么合法的推理是，假设的那个必然就是假的那个.

练习

20. 对下列每个论证，写出一个相应的论证形式，并且确定它

是有效还是无效.

(a) 如果函数 f 不是连续的，那么函数 g 不是可征的. g 是可征的、所以 f 是连续的.

(b) 如果史密斯安装了暖气设备，那么他或者卖了车或者向银行贷了款. 史密斯没有向银行贷款、所以，如果史密斯没有卖掉车，那么他没有安装暖气设备.

(c) 如果在 Polygonia 有油，那么或者专家是正确的或者政府正在骗人. Polygonia 没有油，或者专家是错误的，所以政府并没骗人.

(d) 如果 U 是 V 的子空间那么 U 是 V 的子集，U 包含零向量且 U 是闭的. U 是 V 的子空间，并且如果 U 是闭的，那么 U 包含零向量. 所以如果 U 是闭的那么 U 是 V 的子空间.

21. 假设 $\mathscr{A}_1, \mathscr{A}_2, \cdots, \mathscr{A}_n; \therefore \mathscr{A}$ 是一有效论证形式，证明 $\mathscr{A}_1, \mathscr{A}_2, \cdots, \mathscr{A}_{n-1}; \therefore (\mathscr{A}_n \rightarrow \mathscr{A})$ 也是一有效论证形式.

22. 证明下式是一有效论证形式.

$$p; (p \mid (q \mid r)); \quad \therefore \quad r.$$

第二章　形式的命题演算

2·1　形式系统 L

我们研究逻辑的目的，至少部分原因是为了分析演绎过程．在第一章我们已见到，怎样抽象出命题形式和论证形式以便更清楚地弄明白它们之间的关系和给出一个有效论证的直觉定义．但是还留有一些问题．例如，我们是否能找到一个简单的程序，使得我们能一步一步地构造一个论证，如果知道每一步论证都是有效的话？这样一个程序的基础是什么？由于我们不能从一无所有进行演绎，我们必须作一些初始的假定．为了研究这样的问题，我们引进一个形式演绎系统的观念．这本质上是我们使证明概念抽象化的抽象过程的继续．'形式'这个词，在逻辑教本中是经常出现而不加说明的．它常常用于这样的场合，该处用到了一些符号，而这些符号的作用和属性又完全由一组给定的规则所确定．在一个形式系统中，符号没有任何意义，在处理它们时，我们必须注意不要在系统中所规定的之外对它们的属性作任何的假定．只有这样，我们才能保证在整个演绎中所作的一切假定是明显的，也只有使我们的一切假定明显之后，我们才可能发现任何对逻辑来说是基本的东西．

在本书中，我们将关注两个特殊的形式系统，但有时，我们也需处理另一些由这两个系统修改而得的系统，让我们先给出构成一个形式系统的定义．

为了描述一个形式系统，我们需要：

1．一个符号库．

2．这些符号的有限串，称为合式公式的一个集．在我们的形

式语言中，这些被当作是词和句.

3. 称做公理的合式公式的一个集.

4. 有限个'演绎规则'的集，这些规则能使人们把一个合式公式，例如 $\mathscr{A}$，作为某些合式公式，例如 $\mathscr{A}_1, \cdots, \mathscr{A}_k$ 的有限集的直接后承而演绎出.

给出这四条后，我们就能从公理出发，逐项应用演绎规则来完成演绎程序(它可以同，也可以不同逻辑演绎发生关系，视所考察的特殊形式系统而定). 但要稍后我们才能将此精确化.

记法 从现在起，我们将把合式公式简称为公式.

定义 2·1

命题演算形式系统 L 定义如下：

1. 符号(无限的)库：

$$\sim, \rightarrow, (,), p_1, p_2, p_3, \cdots$$

2. 公式集. 我们不明显地给出这个集而代之以三条归纳规则(见定义 1·2)

(i) 对每个 $i \geqslant 1$，p_i 是公式.

(ii) 如果 $\mathscr{A}$ 和 $\mathscr{B}$ 是公式，那么 $(\sim\mathscr{A})$ 和 $(\mathscr{A}\rightarrow\mathscr{B})$ 也是公式.

(iii) 所有公式都由(i)和(ii)生成.

3. 公理. 有无限条公理，因此我们不能列出它们的全体. 但是我们可以通过三个公理模式来刻划它们的全体. 对任何公式 $\mathscr{A}, \mathscr{B}, \mathscr{C}$，下列公式是 L 的公理.

(L1) $(\mathscr{A}\rightarrow(\mathscr{B}\rightarrow\mathscr{A}))$.

(L2) $((\mathscr{A}\rightarrow(\mathscr{B}\rightarrow\mathscr{C}))\rightarrow((\mathscr{A}\rightarrow\mathscr{B})\rightarrow(\mathscr{A}\rightarrow\mathscr{C})))$.

(L3) $(((\sim\mathscr{A})\rightarrow(\sim\mathscr{B}))\rightarrow(\mathscr{B}\rightarrow\mathscr{A}))$.

注意，每个公理模式都有无限多个'特例'，因为 $\mathscr{A}, \mathscr{B}, \mathscr{C}$ 的变化范围是 L 的一切公式.

4. 演绎规则. 在 L 中仅有一个演绎规则，即分离规则缩写

为 MP。它说：$\mathscr{B}$ 是 $\mathscr{A}$ 和 $(\mathscr{A}\to\mathscr{B})$ 的直接后承，这里 $\mathscr{A}$ 和 $\mathscr{B}$ 是 L 中任意公式.

▷ 符号库和公式集的选取是反映前一章的论述的. 我们希望公式按某种方式代表命题形式，所以这定义密切对应于命题形式的定义. 符号 $\wedge$, $\vee$, $\leftrightarrow$ 在 L 的符号库中并不出现，因此含有这些符号的表达式也不是 L 的一部分. 但是如我们已见到的，$\{\sim, \to\}$ 是联结词的完全集，所以每个真值函数都将被 L 的某个公式所表示，并且每个命题形式也将逻辑等值于 L 的某个公式. （但要注意，命题形式和逻辑等值是第 1 章的概念，在形式系统 L 中没有它的地位.）在 L 中，为使语言简化起见，我们限制了联结词的数目，以期简化形式语言，并使公理和演绎规则也能写得紧凑一些. 如果我们在符号库中引入了，例如 $\wedge$，那么我们就必须也要引入公理和(或)演绎规则以规定其作用(并明确其与符号 $\to$ 的联系)，因为在我们的语言中的符号并没有预先假定的性质. 它们的一切性质都必须能从 L 定义中的信息导出.

L 中的演绎规则在直觉上看来是合理的. 这个规则相应于日常语言中进行论证的标准方式之一. L 的公理是系统的最不显然的部分. 读者应仔细地检验它们，要注意到，如果它们被当作命题形式的话，它们都是重言式. 公理是不能缺少的，它给我们提供演绎出发的基础. 但我们所选择的公理集并不是唯一的. 上面的公理模式恰好有利于后面两条定理，演绎定理和完备性定理的证明. 在讲解的过程中，公理选择的理由将更加清楚.

现在我们必须进而阐明 L 的演绎性质.

定义 2·2

L 中的一个证明是指公式的这样一个序列 $\mathscr{A}_1, \cdots, \mathscr{A}_n$，使得对于每个 $i(1\leqslant i\leqslant n)$，或者 $\mathscr{A}_i$ 是 L 的一个公理，或者 $\mathscr{A}_i$ 可由序列中位于 $\mathscr{A}_i$ 前面的两个公式，$\mathscr{A}_j$ 和 $\mathscr{A}_k$ $(j<i,\ k<i)$，作为应用演绎规则 MP 时的直接后承而推得. 这样的证明称为在 L 中

$\mathscr{A}_n$ 的一个证明，$\mathscr{A}_n$ 称为 L 的一条定理.

注记 2·3

(a) 在上述定义中，注意到 $\mathscr{A}_j$ 和 $\mathscr{A}_k$ 必然是形如 $\mathscr{B}$ 和 $(\mathscr{B}\to\mathscr{A}_i)$，或者倒过来.

(b) 如果 $\mathscr{A}_1, \cdots, \mathscr{A}_n$ 是 L 中的一个证明，并且 $k<n$，那么 $\mathscr{A}_1, \cdots, \mathscr{A}_k$ 也是一个 L 的证明(它显然满足定义)，所以 $\mathscr{A}_k$ 也是 L 的一条定理.

(c) L 的公理一定是 L 的定理. 它们在 L 中的证明是只含一项的序列.

例 2·4

下列序列是 L 中的一个证明.

(1) $(p_1\to(p_2\to p_1))$ ((L1)的特例)

(2) $((p_1\to(p_2\to p_1))\to((p_1\to p_2)\to(p_1\to p_1)))$ (L2)

(3) $((p_1\to p_2)\to(p_1\to p_1))$ ((1)(2)MP)

从上推得 $((p_1\to p_2)\to(p_1\to p_1))$ 是 L 的一条定理.

▷ L 中的一个证明是从公理出发的一个演绎. 我们将需要从某些给定的公式集得出的更为一般的演绎概念.

定义 2·5

令 Γ 是 L 中的公式集(可以是也可以不是 L 中的公理或定理). L 中公式的序列 $\mathscr{A}_1, \cdots, \mathscr{A}_n$ 是从 Γ 的一个演绎，如果对于每个 $i(1\leqslant i\leqslant n)$，下列之一成立:

(a) $\mathscr{A}_i$ 是 L 的公理，

(b) $\mathscr{A}_i$ 是 Γ 中的一个成员，或

(c) $\mathscr{A}_i$ 可由序列中较前的两个公式作为应用 MP 时的直接后承而得.

所以从 Γ 的一个演绎恰是这样的一个'证明'，其中 Γ 的成员被暂时当作公理. 作为从 Γ 的一个演绎的一序列的最后公式 $\mathscr{A}_n$ 称为从 Γ 可演绎的，或称为 L 中 Γ 的一个后承.

如果公式 $\mathscr{A}$ 是 Γ 的某个演绎的最后公式，我们说 Γ 产生了 $\mathscr{A}$，并且记作 $\Gamma \underset{L}{\vdash} \mathscr{A}$.

注意，L 的一条定理是从公式的空集可演绎的（L 中的一个证明是 ϕ 的一个演绎），所以如果 $\mathscr{A}$ 是 L 的一条定理，我们可以记作 $\phi \underset{L}{\vdash} \mathscr{A}$，为简便起见可更规范地写成 $\underset{L}{\vdash} \mathscr{A}$.

注记 重要的是要记住"$\vdash$"不是 L 的一个符号，所以任何出现它的表达式都不能是 L 的一部分. 例如，$\underset{L}{\vdash} \mathscr{A}$ 不是 L 的一部分而是关于 L 的一个命题，即公式 $\mathscr{A}$ 是 L 的一条定理这个命题.

例 2·6

下列是 L 中建立 $\{\mathscr{A}, (\mathscr{B} \to (\mathscr{A} \to \mathscr{C}))\} \underset{L}{\vdash} (\mathscr{B} \to \mathscr{C})$ 的一个演绎，其中 $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$ 代表 L 中的任何公式.

(1)	$\mathscr{A}$	假设
(2)	$(\mathscr{B} \to (\mathscr{A} \to \mathscr{C}))$	假设
(3)	$(\mathscr{A} \to (\mathscr{B} \to \mathscr{A}))$	(L1)
(4)	$(\mathscr{B} \to \mathscr{A})$	(1) (3) MP
(5)	$((\mathscr{B} \to (\mathscr{A} \to \mathscr{C})) \to ((\mathscr{B} \to \mathscr{A}) \to (\mathscr{B} \to \mathscr{C})))$	(L2)
(6)	$((\mathscr{B} \to \mathscr{A}) \to (\mathscr{B} \to \mathscr{C}))$	(2) (5) MP
(7)	$(\mathscr{B} \to \mathscr{C})$	(4) (6) MP

▷ 这个例子和前面的注记，揭示了一个值得强调的差别. 正如 $\underset{L}{\vdash} \mathscr{A}$ 是关于 L 的命题，这例子的结果是关于 L 的一般结果：

对于 L 的任何公式 $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$,

$$\{\mathscr{A}, (\mathscr{B} \to (\mathscr{A} \to \mathscr{C}))\} \underset{L}{\vdash} (\mathscr{B} \to \mathscr{C}).$$

关于 L 的这个结果确实不是 L 的一部分. 对我们的进程——我们正在证明关于证明的结果，存在着两个层次. 我们将用'定理'这词仅仅去指在形式系统中，在定义 2·2 意义下已经证明的公式.

'元定理'这词有时被用于上面提到过的，关于形式系统的结果. 定理是特殊类型的公式，元定理则由普通数学语言写出. 因此我们用命题①这个词是为了避免混淆. 一般地说，我们的命题是元定理.

再要注意，我们一向在使用的花体字母 $\mathscr{A}$, $\mathscr{B}$ 等也不是 L 的部分. 为了方便，我们用它们去表示 L 中任意的非特定的公式，或用来作关于 L 的一般断定.

我们已经把形式系统 L 建立成这样一个系统，其中有些公式可以被证明为定理. 自然，我们感兴趣的是 L 中哪些公式是定理. 现在我们要证明一个公式是一条定理的仅有方法，是实实在在写出构成证明的一个公式序列. 这可能是一很冗长的工作，而且，它在特殊情况下所用的方法并不总是显然的.

例 2·7

对任何 L 的公式 $\mathscr{A}$ 和 $\mathscr{B}$,

(a) $\underset{L}{\vdash}(\mathscr{A}\to\mathscr{A})$

(b) $\underset{L}{\vdash}(\sim\mathscr{B}\to(\mathscr{B}\to\mathscr{A}))$

我们在每个情况下写出 L 中的一个证明. 对于(a)

(1) $(\mathscr{A}\to((\mathscr{A}\to\mathscr{A})\to\mathscr{A}))\to((\mathscr{A}\to(\mathscr{A}\to\mathscr{A}))\to(\mathscr{A}\to\mathscr{A}))$ (L2)

(2) $(\mathscr{A}\to((\mathscr{A}\to\mathscr{A})\to\mathscr{A}))$ (L1)

(3) $((\mathscr{A}\to(\mathscr{A}\to\mathscr{A}))\to(\mathscr{A}\to\mathscr{A}))$ (1)(2) MP

(4) $(\mathscr{A}\to(\mathscr{A}\to\mathscr{A}))$ (L1)

(5) $(\mathscr{A}\to\mathscr{A})$ (3)(4) MP

对于(b)

(1) $(\sim\mathscr{B}\to(\sim\mathscr{A}\to\sim\mathscr{B}))$ (L1)

(2) $((\sim\mathscr{A}\to\sim\mathscr{B})\to(\mathscr{B}\to\mathscr{A}))$ (L3)

---

① 原文 Proposition，译为命题，一般出现在题首. 例如命题 1·9 等. ——译者注.

(3) $((\sim\mathscr{A}\to\sim\mathscr{B})\to(\mathscr{B}\to\mathscr{A}))\to(\sim\mathscr{B}\to((\sim\mathscr{A}\to\sim\mathscr{B})$
$\to(\mathscr{B}\to\mathscr{A})))$ $(L1)$

(4) $(\sim\mathscr{B}\to((\sim\mathscr{A}\to\sim\mathscr{B})\to(\mathscr{B}\to\mathscr{A}))$ (2), (3) MP

(5) $(\sim\mathscr{B}\to((\sim\mathscr{A}\to\sim\mathscr{B})\to(\mathscr{B}\to\mathscr{A})))$
$\to((\sim\mathscr{B}\to(\sim\mathscr{A}\to\sim\mathscr{B}))$
$\to(\sim\mathscr{B}\to(\mathscr{B}\to\mathscr{A})))$ $(L2)$

(6) $(\sim\mathscr{B}\to(\sim\mathscr{A}\to\sim\mathscr{B}))\to(\sim\mathscr{B}\to(\mathscr{B}\to\mathscr{A}))$
(4), (5) MP

(7) $(\sim\mathscr{B}\to(\mathscr{B}\to\mathscr{A}))$

上面在用到括号时，我们已没有以前那么严格了．在证明(b)时用到的某些表达式已不是合式公式．例如，(1)应该是$((\sim\mathscr{B})\to((\sim\mathscr{A})\to(\sim\mathscr{B})))$．但是，我们将继续使用这种方式的简写．它能获得的方便是显然的，但是我们必须注意不要省掉过多的括号以致得到有歧义的表达式．

▷ 能使定理证明较为容易的一种方法，是在证明中允许插入前面已经在 L 中证明过的公式．这相当于数学中引用已经证明过的定理的标准程序．另外一种方法是使用某些一般的元定理，其中有些具有补充推理规则的效果．主要的工具如下：

命题 2·8(演绎定理)

如果 $\Gamma\cup\{\mathscr{A}\}\underset{L}{\vdash}\mathscr{B}$，那么 $\Gamma\underset{L}{\vdash}(\mathscr{A}\to\mathscr{B})$，这里 $\mathscr{A}$ 和 $\mathscr{B}$ 是 L 的公式，Γ 是 L 的公式集(可能是空集)．

证明 我们对构成由 $\Gamma\cup\{\mathscr{A}\}$ 到 $\mathscr{B}$ 的演绎的那个序列中的公式的数目进行归纳证明．在基础步骤假设这个序列有一公式．该公式必定是 $\mathscr{B}$ 本身，因此 $\mathscr{B}$ 或者是 L 的一条公理，或者是 $\Gamma\cup\{\mathscr{A}\}$ 中的一个成员．

情形 1：$\mathscr{B}$ 是 L 的一条公理．那么下列是由 Γ 到$(\mathscr{A}\to\mathscr{B})$的一个演绎．

(1) $\mathscr{B}$ L 的公理

(2) $(\mathscr{B}\to(\mathscr{A}\to\mathscr{B}))$ $(L1)$

(3) $(\mathscr{A}\to\mathscr{B})$ (1), (2) MP

因此 $\Gamma\underset{L}{\vdash}(\mathscr{A}\to\mathscr{B})$.

情形 2: $\mathscr{B}\in\Gamma$. 下列演绎证明了 $\Gamma\underset{L}{\vdash}(\mathscr{A}\to\mathscr{B})$.

(1) $\mathscr{B}$ Γ 的成员

(2) $(\mathscr{B}\to(\mathscr{A}\to\mathscr{B})$ $(L1)$

(3) $(\mathscr{A}\to\mathscr{B})$ (1), (2) MP

情形 3: $\mathscr{B}$ 是 $\mathscr{A}$. 我们已经知道 $\underset{L}{\vdash}(\mathscr{A}\to\mathscr{A})$, 所以 $(\mathscr{A}\to\mathscr{A})$ 在 L 中的证明将可作为由 Γ 到 $(\mathscr{A}\to\mathscr{A})$ 的一个演绎. 因此在这种情况下, 我们也有 $\Gamma\underset{L}{\vdash}(\mathscr{A}\to\mathscr{B})$. 基础步骤到此结束.

现在假设, 由 $\Gamma\cup\{\mathscr{A}\}$ 到 $\mathscr{B}$ 的演绎是一有 n 个公式的序列, 其中 $n>1$, 并且对所有这样的公式 $\mathscr{C}$ 命题都成立, 这些公式 $\mathscr{C}$ 能够通过一个少于 n 个公式的序列由 $\Gamma\cup\{\mathscr{A}\}$ 演绎得到. 这时要考察四种情况.

情形 1: $\mathscr{B}$ 是 L 的一条公理. 完全和上述情况 1 一样, 我们证明了 $\Gamma\underset{L}{\vdash}(\mathscr{A}\to\mathscr{B})$.

情形 2: $\mathscr{B}\in\Gamma$. 恰如上述情况 2, $\Gamma\underset{L}{\vdash}(\mathscr{A}\to\mathscr{B})$.

情形 3: $\mathscr{B}$ 是 $\mathscr{A}$. 如情况 3.

情形 4: $\mathscr{B}$ 由演绎中较前两个公式, 通过应用 MP 而得, 这两个公式必定是 $\mathscr{C}$ 和 $(\mathscr{C}\to\mathscr{B})$ 的形式, 且其中每一个一定能由 $\Gamma\cup\{\mathscr{A}\}$, 通过一个少于 n 个公式的序列演绎得到. 在每一情况下从原来的演绎中舍去后面的公式, 保留余下的序列部分(参见注记 2·3(b)). 我们就有 $\Gamma\cup\{\mathscr{A}\}\underset{L}{\vdash}\mathscr{C}$ 和 $\Gamma\cup\{\mathscr{A}\}\underset{L}{\vdash}(\mathscr{C}\to\mathscr{B})$, 再应用归纳假设就有 $\Gamma\underset{L}{\vdash}(\mathscr{A}\to\mathscr{C})$ 和 $\Gamma\underset{L}{\vdash}(\mathscr{A}\to(\mathscr{C}\to\mathscr{B}))$.

现在所要求的由 Γ 到$(\mathscr{A}\to\mathscr{B})$的演绎可以给出如下：

$$\left.\begin{array}{l}(1)\\ \vdots\\ (k)\ (\mathscr{A}\to\mathscr{C})\end{array}\right\}\quad \text{由 } \Gamma \text{ 到}(\mathscr{A}\to\mathscr{C})\text{的演绎.}$$

$$\left.\begin{array}{l}(k+1)\\ \vdots\\ (l)\ (\mathscr{A}\to(\mathscr{C}\to\mathscr{B}))\end{array}\right\}\quad \text{由 } \Gamma \text{ 到}(\mathscr{A}\to(\mathscr{C}\to\mathscr{B}))\text{的演绎.}$$

$(l+1)\ (\mathscr{A}\to(\mathscr{C}\to\mathscr{B}))\to((\mathscr{A}\to\mathscr{C})\to(\mathscr{A}\to\mathscr{B}))$ $\quad (L2)$

$(l+2)\ (\mathscr{A}\to\mathscr{C})\to(\mathscr{A}\to\mathscr{B})$ $\quad (l),\ (l+1)\,MP$

$(l+3)\ (\mathscr{A}\to\mathscr{B})$ $\quad (k),\ (l+2)\,MP$

$\therefore\ \Gamma\underset{L}{\vdash}(\mathscr{A}\to\mathscr{B})$在所有四种情况成立.

据数学归纳原理命题总成立，不管在由 $\Gamma\cup\{\mathscr{A}\}$ 到 $\mathscr{B}$ 的演绎中，合式公式数目是多少.

注意 我们在这个命题的证明中，并没使用过$(L3)$的任何特例. 这在其它一些具有不同的公理组的形式系统的研究中有其重要性.

▷ 演绎定理的逆命题较为容易证明.

命题 2.9

如果 $\Gamma\underset{L}{\vdash}(\mathscr{A}\to\mathscr{B})$，那么 $\Gamma\cup\{\mathscr{A}\}\underset{L}{\vdash}\mathscr{B}$，其中 $\mathscr{A}$ 和 $\mathscr{B}$ 是 L 中的公式，Γ 是 L 中的公式集(可能是空集).

证明 给出一个由 Γ 到$(\mathscr{A}\to\mathscr{B})$的演绎，我们期望构造一个由 $\Gamma\cup\{\mathscr{A}\}$ 到 $\mathscr{B}$ 的演绎

$$\left.\begin{array}{l}(1)\\ \vdots\\ (k)\ (\mathscr{A}\to\mathscr{B})\end{array}\right\}\quad \text{由 } \Gamma \text{ 到}(\mathscr{A}\to\mathscr{B})\text{的演绎}$$

$(k+1)\ \mathscr{A}$ $\quad \Gamma\cup\{\mathscr{A}\}$ 的成员

$(k+2)\ \mathscr{B}$ $\quad (k),\ (k+1)\,MP.$

▷ 演绎定理的应用在下面系的证明中可以见到，它可作为一条新的演绎规则来使用.

系 2·10

对任何 L 中公式 $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$,

$$\{(\mathscr{A}\to\mathscr{B}),\ (\mathscr{B}\to\mathscr{C})\}\vdash_L(\mathscr{A}\to\mathscr{C}).$$

证明. 我们写出演绎

(1)	$(\mathscr{A}\to\mathscr{B})$	假设
(2)	$(\mathscr{B}\to\mathscr{C})$	假设
(3)	$\mathscr{A}$	假设
(4)	$\mathscr{B}$	(1), (3) MP
(5)	$\mathscr{C}$	(2), (4) MP

我们已经证明的是

$$\{(\mathscr{A}\to\mathscr{B}),\ (\mathscr{B}\to\mathscr{C}),\ \mathscr{A}\}\vdash_L\mathscr{C} \qquad (*)$$

即

$$\{(\mathscr{A}\to\mathscr{B}),\ (\mathscr{B}\to\mathscr{C})\}\cup\{\mathscr{A}\}\vdash_L\mathscr{C}$$

所以根据演绎定理，我们有

$$\{(\mathscr{A}\to\mathscr{B}),\ (\mathscr{B}\to\mathscr{C})\}\vdash_L(\mathscr{A}\to\mathscr{C}).$$

▷ 这个结果在以后将用到多次，我们称它为'假言三段论'，简记为 HS.

注意 对 (*) 可以有几种应用演绎定理的方式. 我们也可演绎出下列各条:

$$\{(\mathscr{A}\to\mathscr{B}),\ \mathscr{A}\}\vdash_L((\mathscr{B}\to\mathscr{C})\to\mathscr{C}),$$

$$\{(\mathscr{B}\to\mathscr{C}),\ \mathscr{A}\}\vdash_L((\mathscr{A}\to\mathscr{B})\to\mathscr{C}).$$

再把演绎定理用于系的结果. 我们得到

$$\{(\mathscr{A}\to\mathscr{B})\}\vdash_L((\mathscr{B}\to\mathscr{C})\to(\mathscr{A}\to\mathscr{C})),$$

因此 $\vdash_L((\mathscr{A}\to\mathscr{B})\to((\mathscr{B}\to\mathscr{C})\to(\mathscr{A}\to\mathscr{C})))$.

命题 2·11

对 L 中任意的公式 $\mathscr{A}$ 和 $\mathscr{B}$, 下列各式为 L 的定理.

(a) $(\sim\mathscr{B}\to(\mathscr{B}\to\mathscr{A}))$,

(b) $((\sim\mathscr{A}\to\mathscr{A})\to\mathscr{A})$.

证明 ((a)出现在例 2·7 中,但是我们让它重现于此,以便看到新规则 HS 的简化作用).

对(a)

(1) $(\sim\mathscr{B}\to(\sim\mathscr{A}\to\sim\mathscr{B})$ $(L1)$

(2) $(\sim\mathscr{A}\to\sim\mathscr{B})\to(\mathscr{B}\to\mathscr{A})$ $(L3)$

(3) $(\sim\mathscr{B}\to(\mathscr{B}\to\mathscr{A}))$ (1), (2) HS

对(b)

(1) $(\sim\mathscr{A}\to\mathscr{A})$ 假设

(2) $(\sim\mathscr{A}\to(\sim\sim(\sim\mathscr{A}\to\mathscr{A})\to\sim\mathscr{A})$ $(L1)$

(3) $(\sim\sim(\sim\mathscr{A}\to\mathscr{A})\to\sim\mathscr{A})\to(\mathscr{A}\to\sim(\sim\mathscr{A}\to\mathscr{A}))$ $(L3)$

(4) $(\sim\mathscr{A}\to(\mathscr{A}\to\sim(\sim\mathscr{A}\to\mathscr{A})))$ (2), (3) HS

(5) $(\sim\mathscr{A}\to(\mathscr{A}\to\sim(\sim\mathscr{A}\to\mathscr{A})))\to((\sim\mathscr{A}\to\mathscr{A})\to(\sim\mathscr{A}\to\sim(\sim\mathscr{A}\to\mathscr{A})))$ $(L2)$

(6) $(\sim\mathscr{A}\to\mathscr{A})\to(\sim\mathscr{A}\to\sim(\sim\mathscr{A}\to\mathscr{A}))$ (4), (5) MP

(7) $(\sim\mathscr{A}\to\sim(\sim\mathscr{A}\to\mathscr{A}))$ (1), (6) MP

(8) $(\sim\mathscr{A}\to\sim(\sim\mathscr{A}\to\mathscr{A}))\to((\sim\mathscr{A}\to\mathscr{A})\to\mathscr{A})$ $(L3)$

(9) $(\sim\mathscr{A}\to\mathscr{A})\to\mathscr{A}$ (7), (8) MP

(10) $\mathscr{A}$ (1), (9) MP

因此 $(\sim\mathscr{A}\to\mathscr{A})\vdash_L\mathscr{A}$

$\therefore \vdash_L ((\sim\mathscr{A}\to\mathscr{A})\to\mathscr{A})$，根据演绎定理。这些结果以后将要用到。

练习

1. 写出下列公式在 L 中的证明：

(a) $(p_1\to p_2)\to((\sim p_1\to\sim p_2)\to(p_2\to p_1))$；

(b) $((p_1\to(p_2\to p_3))\to(p_1\to p_2))\to((p_1\to(p_2\to p_3))\to(p_1\to p_3))$；

(c) $(p_1\to(p_1\to p_2))\to(p_1\to p_2)$；

(d) $(p_1\to(p_2\to(p_1\to p_2)))$。

2. 证明。对 L 中任何公式 $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$，下面的都成立。

(a) $\{(\sim\mathscr{A})\}\vdash_L(\mathscr{A}\to\mathscr{B})$；

(b) $\{(\sim(\sim\mathscr{A}))\}\vdash_L\mathscr{A}$；

(c) $\{(\mathscr{A}\to\mathscr{B}),(\sim(\mathscr{B}\to\mathscr{C})\to(\sim\mathscr{A}))\}\vdash_L(\mathscr{A}\to\mathscr{C})$；

(d) $\{(\mathscr{A}\to(\mathscr{B}\to\mathscr{C}))\}\vdash_L(\mathscr{B}\to(\mathscr{A}\to\mathscr{C}))$。

3. 用 L 中的演绎定理证明下列公式是 L 的定理，其中 $\mathscr{A}$ 和 $\mathscr{B}$ 是 L 中任意的合式公式。

(a) $(\mathscr{A}\to(\sim(\sim\mathscr{A})))$；

(b) $((\mathscr{B}\to\mathscr{A})\to((\sim\mathscr{A})\to(\sim\mathscr{B})))$；

(c) $(((\mathscr{A}\to\mathscr{B})\to\mathscr{A})\to\mathscr{A})$；

(d) $(\sim(\mathscr{A}\to\mathscr{B})\to(\mathscr{B}\to\mathscr{A}))$。

4. 设 L' 是与 L 仅仅在用公理图式 $(L'3)$ $((\sim\mathscr{A}\to\sim\mathscr{B})\to((\sim\mathscr{A}\to\mathscr{B})\to\mathscr{A}))$ 替换了 $(L3)$ 这一点有所不同的形式演绎系统，求证对任何 L(从而也是 L')中的公式 $\mathscr{A}$ 和 $\mathscr{B}$，

(i) $\vdash_L((\sim\mathscr{A}\to\sim\mathscr{B})\to((\sim\mathscr{A}\to\mathscr{B})\to\mathscr{A}))$；

和

(ii) $\underset{L'}{\vdash}((\sim\mathscr{A}\rightarrow\sim\mathscr{B})\rightarrow(\mathscr{B}\rightarrow\mathscr{A}))$.

推演；一个合式公式是 L 的定理，当且仅当它是 L' 的定理

5. 规则 HS 是 L 的演绎规则的合法补充之一例. 下列规则在同样意义下合理吗？由公式 $\mathscr{B}$ 和 $(\mathscr{A}\rightarrow(\mathscr{B}\rightarrow\mathscr{C}))$，演绎出 $(\mathscr{A}\rightarrow\mathscr{C})$.

2·2 L 的完备性定理

象我们在命题 2·11 中所作的那样去证明某个 L 的特殊合式公式为 L 的定理并非一个很值得做的练习. 如(b)所示，有时是很难知道怎样着手的，而且最后的结果可能很复杂，远不是一个直觉的证明. 不过，L 的这个方面无需引起我们关注. 定义 L 的理由首先是试图构造一个形式系统，使它能(凭类比)反映我们的演绎，有效性和真实性等直观概念，从而试图从关于这些直观概念中学到某些东西.

第一章给了我们一个"逻辑真实性"的概念，那就是重言式的概念. 看来我们有理由期望逻辑真实对应于 L 的定理，并试图以此为目的来构造 L. 本章余下部分专用于说明 L 具有这样的属性. 这个程序也将使我们对一般的形式系统的性质和属性有所认识，它在以后几章中会派用处.

尽管 L 语言中的符号只被看作纯粹的形式符号，但是 L 还是以这样的一种方式定义的，即我们能够把 L 的公式解释为命题形式，因而每个真值函数都可由某个公式表示. 因此，尽管我们谈不上完全象在第一章中那样给 L 的符号，以真值指派，我们还是能定义一个类似的程序.

定义 2·12

L 的一个赋值是一个函数 v，它的定义域是 L 的公式，值域是集 $\{T, F\}$，并且使得对 L 的任意公式 $\mathscr{A}$，$\mathscr{B}$

(i) $v(\mathscr{A}) \neq v(\sim\mathscr{A})$

且

(ii) $v(\mathscr{A}\to\mathscr{B})=F$ 当且仅当 $v(\mathscr{A})=T$ 和 $v(\mathscr{B})=F$.

注意，对 L 中符号 $p_1, p_2, \cdots$ 的一个任意'真值指派'将产生一个赋值，因为在这个指派下，L 的每个公式（作为一个命题形式）将取两个真值之一．因而(i)和(ii)将显然得到满足．

定义 2·13

L 中的一个公式 $\mathscr{A}$ 是一个重言式，如果对每个 v，有 $v(\mathscr{A})=T$．这和把 $\mathscr{A}$ 看作一个命题形式并且应用前面的定义（定义 1·5(a)）是一样的．

我们将要证明：L 的一个公式是 L 的一条定理，当且仅当它是一重言式．我们此刻已能证明该断言的一部分．

命题 2·14（可靠性定理）

L 的每个定理是一重言式．

证明　令 $\mathscr{A}$ 是 L 的一条定理．证明是通过对构成 $\mathscr{A}$ 在 L 中的证明的公式序列中公式的数目进行归纳来完成的．

基础步骤．假设 $\mathscr{A}$ 的证明只含有一个公式，即 $\mathscr{A}$ 自身．那么 $\mathscr{A}$ 一定是 L 的一条公理．L 的所有公理都是重言式，这可以通过构造真值表加以证实，留给读者作为练习．

现在假设：$\mathscr{A}$ 的证明包含 n 个公式，$n>1$，并且作为归纳假设：L 中凡少于 n 步证明的一切定理都是重言式．此时，$\mathscr{A}$ 或者是公理．在这种情况下 $\mathscr{A}$ 是重言式；$\mathscr{A}$ 或者由 MP 从证明中两个在前的公式推得．这两个公式必为 $\mathscr{B}$ 和 $(\mathscr{B}\to\mathscr{A})$ 的形式．但是，$\mathscr{B}$ 和 $(\mathscr{B}\to\mathscr{A})$ 是证明步骤少于 n 个公式的定理．（即被适当截断过的 $\mathscr{A}$ 的证明）．因此根据归纳假设 $\mathscr{B}$ 和 $(\mathscr{B}\to\mathscr{A})$ 是重言式，所以据命题 1·9，$\mathscr{A}$ 是重言式．

所以，根据数学归纳原理，L 的每条定理都是重言式．

▷ 为了证明逆命题，我们需要引进两个新概念：L 的扩充和

一致性.

L 有三个公理模式，它们是定理证明的出发点. 如果我们添加另外的公理模式，或者只是另外的单个公理将会发生什么情况呢？我们将会有较多的出发点，一般来说，我们将期待能证明较多的定理. 所有原来是定理的公式仍然是定理，也许还有某些原来不是定理的公式也成了定理. 事实上，当且仅当新的公理集包括一个原先不是定理的公式时才会产生新的定理.（读者可以很容易补上这个证明.）

定义 2·15

L 的一个扩充是一个形式系统，它通过修改或扩大公理组使得所有原来的定理仍是定理（也可能引进新的定理）而得到.

人们只需看一下几种现有的逻辑教本就会明白，用其它的公理这样去替换我们的公理模式($L1$)，($L2$) 和($L3$) 使得定理类保持不变是可能的. 例如(见练习 2·4)，($L3$)就可由公理模式

$$((\sim\mathscr{A}\to\sim\mathscr{B})\to((\sim\mathscr{A}\to\mathscr{B})\to\mathscr{A}))$$

替换而并不改变定理类.

注意　一个形式系统很可能是 L 的一个扩充，但是它和 L 没有一个共同的公理.

▷ 如果我们把 L 扩充到具有越来越多定理的系统，就越有可能会出现这种情况，即有某个公式 $\mathscr{A}$，使得 $\mathscr{A}$ 和 $(\sim\mathscr{A})$ 都是定理. 这种情况显然是不受欢迎的.

定义 2·16

L 的一个扩充是一致的，如果不存在 L 的公式 $\mathscr{A}$，使得 $\mathscr{A}$ 和 $(\sim\mathscr{A})$ 都是这个扩充的定理.

当然，这个定义没有涉及 L 本身是否一致.

命题 2·17

L 是一致的.

证明 假设 L 不一致，即存在一公式 $\mathscr{A}$，使得 $\underset{L}{\vdash}\mathscr{A}$ 和 $\underset{L}{\vdash}(\sim\mathscr{A})$. 那么据命题 2·14（可靠性定理），$\mathscr{A}$ 和 $(\sim\mathscr{A})$ 都是重言式. 这是不可能的，因为，如果 $\mathscr{A}$ 是重言式，则 $(\sim\mathscr{A})$ 是矛盾式；如果 $(\sim\mathscr{A})$ 是重言式，那么 $\mathscr{A}$ 是矛盾式. 因此 L 一定一致.

命题 2·18

L 的一个扩充 L^* 是一致的，当且仅当存在一个公式，它不是 L^* 的一条定理.

证明：设 L^* 一致. 那么，对于任何公式 $\mathscr{A}$，或者 $\mathscr{A}$ 不是或者 $(\sim\mathscr{A})$ 不是定理（两者不能都是定理）.

相反，设 L^* 不一致. 我们证明不存在不是 L^* 的定理的公式，即每个公式都是 L^* 的定理. 令 $\mathscr{A}$ 是任意公式. L^* 不一致，所以对某公式 $\mathscr{B}$，有 $\underset{L^*}{\vdash}\mathscr{B}$ 且 $\underset{L^*}{\vdash}(\sim\mathscr{B})$. 现在，据命题 2·11，$\underset{L}{\vdash}(\sim\mathscr{B}\to(\mathscr{B}\to\mathscr{A}))$，所以，$\underset{L^*}{\vdash}(\sim\mathscr{B}\to(\mathscr{B}\to\mathscr{A}))$，由于 L^* 是 L 的扩充. 现在，两次应用 MP，我们就得 $\underset{L^*}{\vdash}\mathscr{A}$. 因此每个公式都是 L^* 的定理，证毕.

关于这个命题，有两点要加以强调. 它们是：

(a) 在一个 L 的不一致的扩充中，每个公式都是一条定理. 任何时候我们用到 L 的扩充时，对一致性必须倍加小心，因为，一个其中每一公式都是定理的系统，犹如任何公式都不是定理的系统一样地没有价值.

(b) 由命题给出的一致性的充分条件是令人惊奇的弱，即，存在单个不是定理的公式即可，所以令人惊奇是因为，在许多一致系统中，确实将存在许多并非定理的公式，例如一切定理的否定都是非定理.

现在，我们遇到了一条似乎无关紧要的，技术性的定理，其实我们在以后的证明中，将会一次又一次用到它. 它描述了一种能

获得一致的扩充的情况。

命题 2·19

令 L^* 是 L 的一个一致的扩充，并且令 $\mathscr{A}$ 是 L 的一个公式且不是 L^* 的一条定理。那么 L^{**} 也是一致的，这里 L^{**} 是 L 的一个扩充，它由 L^* 补充 $(\sim\mathscr{A})$ 为公理而得到。

证明 令 $\mathscr{A}$ 是 L 的一个公式且不是 L^* 的一条定理。假如 L^{**} 不一致。那么，对某个公式 $\mathscr{B}$，将有 $\underset{L^{**}}{\vdash}\mathscr{B}$ 和 $\underset{L^{**}}{\vdash}(\sim\mathscr{B})$。现在，恰如在命题 2·18 的证明一样可以推得 $\underset{L^{**}}{\vdash}\mathscr{A}$。但是 L^{**} 和 L^* 的差别仅在于 L^{**} 有附加公理 $(\sim\mathscr{A})$，所以 $\underset{L^{**}}{\vdash}\mathscr{A}$ 等价于 $(\sim\mathscr{A})\underset{L^*}{\vdash}\mathscr{A}$。(在 L^{**} 中的一个证明，正好是 L^* 中由 $(\sim\mathscr{A})$ 出发的一个演绎。) 所以 $\underset{L^*}{\vdash}((\sim\mathscr{A})\to\mathscr{A})$，据演绎定理。但是，据命题 2·11 $\underset{L}{\vdash}(((\sim\mathscr{A})\to\mathscr{A})\to\mathscr{A})$，所以 $\underset{L^*}{\vdash}(((\sim\mathscr{A})\to\mathscr{A})\to\mathscr{A})$。现在，用 MP。我们就得 $\underset{L^*}{\vdash}\mathscr{A}$。

但是这和 $\mathscr{A}$ 不是 L^* 中的一条定理的假设是矛盾的。

▷ 关于能作为 L 的扩充中的附加公理而保持一致性的公式，显然在某处有个限度。达到这个限度是下一命题的目标，但是首先让我们把这一情况描述在一个定义中。

定义 2·20

L 的一个扩充是完全的，如果对每个公式 $\mathscr{A}$，$\mathscr{A}$ 或者 $(\sim\mathscr{A})$ 是该扩充的一条定理。

注记 (a) L 远非完全的。例如，p_1 是 L 的一个公式，p_1 和 $(\sim p_1)$ 都非 L 的定理。

(b) 任何 L 的不一致扩充显然是完全的，据命题 2·18。

(c) 如果 L^c 是 L 的一个一致的完全扩充，那么，任何一个 L 的进一步的扩充，只要它的定理类对 L^c 的定理类有所扩充，将都是不一致的。因为令 $\mathscr{A}$ 不是 L^c 的一条定理。那么 $(\sim\mathscr{A})$ 就是 L^c

的一条定理. 因此如果 $\mathscr{A}$ 是一进一步扩充的定理, $(\sim\mathscr{A})$ 也是, 所以这个进一步扩充不是一致的.

命题 2·21

令 L^* 是 L 的一致扩充. 那么存在 L^* 的一个一致的完全扩充.

(注意, 这里我们已经推广了术语. L^* 的一个扩充可以通过改变或扩大 L^* 的公理组而得到, 所以也是定理集的扩大 见定义 2·15).

证明 令 $\mathscr{A}_0, \mathscr{A}_1, \mathscr{A}_2, \cdots$ 是 L 的所有公式的枚举. 这可以用几种方式构造——建议读者试着去作一能生成这样一列的方法. (熟悉涉及无穷可数集的结构, 对于这做法是有用的)①. 我们将构造 L^* 的扩充的序列 $J_0, J_1, J_2, \cdots$ 如下. 令

$$J_0 = L^*.$$

如果

$$\underset{J_0}{\vdash} \mathscr{A}_0, \text{令 } J_1 = J_0$$

如果不能 $\underset{J_0}{\vdash} \mathscr{A}_0$, 那么加 $(\sim\mathscr{A}_0)$ 作为一新公理于 J_0, 得到 J_1.

一般地, 对于 $n \geqslant 1$, 从 J_{n-1} 构造 J_n 的方法如下: 如果 $\underset{J_{n-1}}{\vdash} \mathscr{A}_{n-1}$, 那么 $J_n = J_{n-1}$, 如果不能 $\underset{J_{n-1}}{\vdash} \mathscr{A}_{n-1}$, 那么令 J_n 是 J_{n-1} 的扩充, 它通过补充 $(\sim\mathscr{A}_{n-1})$ 为一新公理而得到.

据假设 L^* 是一致的, 即 J_0 是一致的, 据命题 2·19, 对于 $n \geqslant 1$, 如果 J_{n-1} 是一致的, 那么 J_n 是一致的. 因此根据归纳法, 每个 J_n 是一致的 $(n \geqslant 0)$. 现在定义 J 是 L 的扩充, 它把至少在 J_n 之一中为公理的一切公式都当作公理.

现在我们证明 J 是一致的, 假设情况相反. 那么存在一公式 $\mathscr{A}$, 使得 $\underset{J}{\vdash} \mathscr{A}$ 和 $\underset{J}{\vdash} (\sim\mathscr{A})$. 现在 $\mathscr{A}$ 和 $(\sim\mathscr{A})$ 在 J 中的证明是公式的有限序列, 所以每一证明仅可能包含有限多个 J 的公理的实

① 见附录.

例. 因此,必定存在 n, 它大到足以包含所有这些作为 J_n 的公理. 由此可得 $\vdash_{J_n}\mathscr{A}$ 和 $\vdash_{J_n}(\sim\mathscr{A})$. 这和 J_n 是一致的假设矛盾, 所以 J 一定是一致的.

剩下来要证明 J 是完全的. 令 $\mathscr{A}$ 是 L 的一个公式, $\mathscr{A}$ 一定在序列 $\mathscr{A}_0, \mathscr{A}_1, \mathscr{A}_2, \cdots$ 中出现, 诸如 $\mathscr{A}$ 是 $\mathscr{A}_k$. 如果 $\vdash_{J_k}\mathscr{A}_k$, 那么确实 $\vdash_J\mathscr{A}_k$, 由于 J 是 J_k 的一个扩充. 如果不能 $\vdash_{J_k}\mathscr{A}_k$, 那么据 J_{k+1} 的构造, $(\sim\mathscr{A}_{k+1})$ 是 J_{k+1} 的一条公理, 所以 $\vdash_{J_{k+1}}(\sim\mathscr{A}_k)$. 这蕴涵 $\vdash_J(\sim\mathscr{A}_k)$. 所以在任何情况下, 我们有 $\vdash_J\mathscr{A}$ 或 $\vdash_J(\sim\mathscr{A})$, 所以 J 是完全的.

命题 2·22

如果 L^* 是 L 的一个一致的扩充, 则存在一种赋值, 使得 L^* 的每个定理取值为 T.

证明　定义 L 的公式上的赋值 v 如下

$$v(\mathscr{A})=T \quad \text{如果} \quad \vdash_J\mathscr{A},$$

和

$$v(\mathscr{A})=F \quad \text{如果} \quad \vdash_J(\sim\mathscr{A}).$$

其中 J 是在命题 2·21 的证明中所给出的, L^* 的一个一致的完全扩充. 注意 v 定义在所有公式上, 因为 J 是完全的. 现在 $v(\mathscr{A})\neq v(\sim\mathscr{A})$, 对于任意公式 $\mathscr{A}$, 因为 J 是一致的, 剩下的是要证明: $v(\mathscr{A}\to\mathscr{B})=F$, 当且仅当 $v(\mathscr{A})=T$ 和 $v(\mathscr{B})=F$. 首先假设: $v(\mathscr{A})=T$, $v(\mathscr{B})=F$ 且 $v(\mathscr{A}\to\mathscr{B})=T$, 那么 $\vdash_J\mathscr{A}$, $\vdash_J(\sim\mathscr{B})$ 和 $\vdash_J(\mathscr{A}\to\mathscr{B})$. 从而由 MP 又得 $\vdash_J\mathscr{B}$, 这和 J 的一致性是矛盾的. 因此, $v(\mathscr{A})=T$ 且 $v(\mathscr{B})=F$ 蕴涵 $v(\mathscr{A}\to\mathscr{B})=F$. 反之, 假设 $v(\mathscr{A}\to\mathscr{B})=F$ 和或者 $v(\mathscr{A})=F$ 或者 $v(\mathscr{B})=T$. 那么 $\vdash_J(\sim(\mathscr{A}\to\mathscr{B}))$ 并且或者 $\vdash_J(\sim\mathscr{A})$ 或者 $\vdash_J\mathscr{B}$. 但是总有

$$\vdash_J (\sim\mathscr{A}\to(\sim\mathscr{B}\to\sim\mathscr{A})),$$

和

$$\vdash_J (\mathscr{B}\to(\mathscr{A}\to\mathscr{B})),$$

所以根据 MP,

$$\vdash_J (\sim\mathscr{B}\to\sim\mathscr{A}) \quad 或 \quad \vdash_J (\mathscr{A}\to\mathscr{B})$$

现在 $\vdash_J ((\sim\mathscr{B}\to\sim\mathscr{A})\to(\mathscr{A}\to\mathscr{B}))$, 所以在每种情况下, 我们都有 $\vdash_J (\mathscr{A}\to\mathscr{B})$, 这与 J 的一致性矛盾. 因此, $v(\mathscr{A}\to\mathscr{B})=F$ 蕴涵 $v(\mathscr{A})=T$ 和 $v(\mathscr{B})=F$. 所以 v 是一个赋值.

现在令 $\mathscr{A}$ 是 L^* 的一条定理. 因此 $\vdash_J \mathscr{A}$, 由于 J 是 L^* 的一个扩充. 所以 $v(\mathscr{A})=T$.

▷ 现在我们已能证明所要的结果.

命题 2·23(L 的完备性的定理)

如果 $\mathscr{A}$ 是一个公式且是一重言式, 那么 $\vdash_L \mathscr{A}$.

证明 令 $\mathscr{A}$ 是 L 的一个公式且是一重言式, 并且假设 $\mathscr{A}$ 不是 L 的一条定理, 那么包含 $(\sim\mathscr{A})$ 作为新公理的扩充 L^* 是一致的, 据命题 2·19. 因此存在一个赋值 v, 给 L^* 的每个定理的值为 T. 特别地, 有 $v(\sim\mathscr{A})=T$. 但是, 因为 $\mathscr{A}$ 是重言式, $v(\mathscr{A})=T$, 于是产生矛盾. 因此 $\mathscr{A}$ 是 L 的一条定理.

▷ 现在我们已经证实, 形式系统 L 具有它应该具有的主要属性, 即在系统内能得到证明的公式恰恰是那些"逻辑真"的公式. L 中的公理和演绎规则刻划了逻辑演绎的特点, 至少在命题演算中是如此. 我们对 L 的研究, 其价值在此, 而不在于 L 中的公式, 证明和定理的详细研究.

我们为了证明完备性定理所用的这些思想和方法是十分有力的, 并且将有其它的应用, 尽管他们在这里只是为了一个特殊目的, 作为工具来使用的. 在完备性定理的文献中, 有许多其它的证

明，有些用到完全不同的方法．我们之所以选用这种方法，是因为我们以后多少能用这同一程序去证明关于更为复杂的谓词演算形式系统的相应的完备性定理．事实上我们关于系统 L 所作的全部讨论主要是为了引进该主题的思想，并非只是为了它自身而研究命题演算．就后者而言，第一章的方法已给我们提供了对问题的充分的认识．真值表给了我们关于特殊的命题形式和论证形式所需要的一切信息，由于使用真值表，我们能有效地区分重言式，矛盾式和其它命题形式．这一事实对于 L 的影响是很重要和有用的，所以我们把它列为一个命题．

命题 2·24

L 是可判定的，即存在着一种能行的方法去判定给定的 L 的公式是否为 L 的定理．

证明 要断定一个公式 $\mathscr{A}$ 是否为 L 的定理，只需把它看作一个命题形式而作出它的真值表．它是定理，当且仅当它是一重言式．

注记 2·25

这使得人们没有必要，对 L 中的证明作任何进一步构造．真值表给出了一个机械的，如果不总是很快的，证明一个给定公式是否为 L 的定理的方法．但是，因为我们直到现在才知道它，所以，例如命题 2·11 的证明现在并不能改变，因为它的结果，在完备性定理的证明中需要用到．

练习

6．证明 L 的每条公理为重言式．

7．令 $\mathscr{A}$ 是 L 的一个公式，并且 L^+ 是补充 $\mathscr{A}$ 为一新公理后得到的 L 的一个扩充．证明：L^+ 的定理集不同于 L 的定理集，当且仅当 $\mathscr{A}$ 不是 L 的一条定理．

8．令 $\mathscr{A}$ 是公式 $((\sim p_1 \to p_2) \to (p_1 \to \sim p_2))$．求证．包括这

个 $\mathscr{A}$ 为新公理而得的 L^+，有比 L 扩大的定理集。L^+ 是 L 的一个一致的扩充吗？

9. 证明：如果 $\mathscr{B}$ 是矛盾式，那么 $\mathscr{B}$ 不能是 L 的任何一致扩充的定理。

10. 令 L^{++} 是包括

$$((\sim\mathscr{A}\to\mathscr{B})\to(\mathscr{A}\to\sim\mathscr{B}))$$

作为第 4 公理模式而得的 L 的扩充。求证：L^{++} 是不一致的。（提示：见第 1 章练习 7。）

11. 令 J 是 L 的一个一致完备扩充，令 $\mathscr{A}$ 是 L 的一个公式。求证：包括 $\mathscr{A}$ 为一附加公理的 L 的扩充是一致的，当且仅当 $\mathscr{A}$ 是 J 的一条定理。

12. 令 $\mathscr{A}$ 是 L 的一个公式，其中出现命题字母 $p_1, \cdots, p_n$，同时令 $\mathscr{A}_1, \mathscr{A}_2, \cdots, \mathscr{A}_n$ 是 L 的任意公式。令 $\mathscr{B}$ 是 L 的公式，它通过对 $\mathscr{A}$ 中的 p_i 代入 $\mathscr{A}_i$ 而得 $(1\leqslant i\leqslant n)$。证明：如果 $\mathscr{A}$ 是 L 的一条定理，那么 $\mathscr{B}$ 是 L 的一条定理。

第三章　非形式的谓词演算

3.1　谓词和量词

在第一章中，我们分析了句子和论证，把它们分解到作为成分的简单命题，并把这些简单命题作为基石．通过这种手段，我们能够发现构成一个有效论证的某些依据．但是，有些论证却不能容许这样的处理．例如，让我们用稍加改变的形式写下第一章中的一个例子：

所有人皆有死，
苏格拉底是人，
苏格拉底有死．

我们直觉上将把这个例子看成是有效论证，但是，如果我们试图按我们在第一章中所用的方法，用符号来表示这个论证的话，我们就得到 p, q; $\therefore r$. 根据第一章的讨论，它不是一个有效的论证形式．

在这种情况下，有效性并不依赖于作为简单命题的前提和结论之间的关系，而依赖于命题所包含的各个组成部分之间的关系和依赖于命题本身的形式．如果我们希望更清楚地说明这一点，而写出与它相应的"论证形式"，它势必呈这样的形式：

所有 A 是 B,
C 是 A,
$\therefore$ C 是 B.

有两点需要详述．第一，前提"所有 A 是 B"的一般属性；第二，用符号来表示一简单命题的各个部分．与这两点相应的就是"量词"的观念和"谓词"的观念．在英语中，每一个简单命题都有一主词和一谓词，它们都由单个词项，短语或付句组成．粗略地

说，主词是命题正要加以断定的事物，谓词则指该事物所具有的"属性"。

例 3.1

在下列各个命题中，主词下面划了直线，余下部分是谓词。

(a) 苏格拉底是人。

(b) 我写书。

(c) 平方为 -1 的数不是实数。

(d) 世界给人们以生存。

我们感到这样做是方便的，即用大写字母 $A, B, C, \cdots$ 表示谓词，用小写字母表示主词，从而把象上面那样的命题用符号表示如下：

(a) $A(s)$ 可以代表"苏格拉底是人"，其中 A 是一个谓词字母，它表示"是人"，s 代表苏格拉底。这样我们也可把"拿破仑是人"用符号表示成 $A(n)$，n 代表拿破仑。

(b) 按类似的方法，可以用 $B(b)$ 表示"我写书"。

(c) 在这种情况下，我们的谓词是一否定词，为此我们有选择的可能。我们可以选择 R 意指"不是实数"。此时该命题将有形式 $R(j)$，其中 j 代表平方是 -1 的数，或者我们可以选择 S 意指"是实数"，此时命题将是形式 $(\sim S(j))$。

(d) 类似于(a)和(b)，可以写成 $L(w)$。

至于复合命题也可以按这种方式翻译成符号，应当是清楚的，只须把一切作为成分的简单命题符号化就行了。

▷现在，我们问对于"所有人皆有死"这样的命题该怎么办？我们需要比主谓分析更多一点东西，因为这命题的意义是有赖于"所有"这个词的力量的，考察另一例子。

每个整数都有素因子。

在通常的数学符号体系中，我们可以把它写成：

对所有 x 来说，如果 x 是一整数，那么 x 有一素因子。

用刚才我们引进的那类符号语言，我们将把它写成：

对所有 x，$(I(x)\rightarrow p(x))$，

其中 $I(x)$ 代表"x 是一整数"，$p(x)$ 代表"x 有一素因子"。

类似地，我们如果用谓词符号 A 和 M 分别表示"是人"和"有死"，那么"所有人皆有死"可以写成：

对于所有 x，$(A(x)\rightarrow M(x))$。

短语"对于所有 x"称为一个全称量词，可以翻译成符号 $(\forall x)$。注意，当我们写 $(\forall x)(A(x)\rightarrow M(x))$ 时，关于 x 的属性并没有作任何假定。这里的蕴涵是"对论域之中的每个对象 x"而言的。如果 x 是人，那么 x 有死。对任何并非是人的 x 来说，它是否有死是无关紧要的。蕴涵式为真，因为它的第一部分为假（参见 $\rightarrow$ 的真值表）。

符号 x 的引进不会引起混乱，尽管它并没出现在原来的英语句子中。它的使用只是一种数学的缩写，显然所有人皆有死也可以翻译成符号如下

对于所有 y，$(A(y)\rightarrow M(y))$。

我们将把字母 x 和 y 当作变元，去表示不确定的主体。当它们如上在以量词开始的命题中被使用时，他们被称为约束变元。

还有一种量词，乍看起来在把英语命题翻译成符号时是需要的。考察句子'有些猪有翅膀'。这句话可以重写成'至少有一头猪有翅膀'，或用上面的类似方式，可以写成：

至少存在一个 x，使得 x 是一头猪并且有翅膀。

短语"至少存在一个对象 x"称为一个存在量词，它可以翻译成符号 $(\exists x)$。现在句子就可写成

$$(\exists x)(P(x)\wedge W(x)),$$

其中 $P(x)$ 和 $W(x)$，相应地，意指"x 是一头猪"和"x 有翅膀"。

更为一般地，如果 A 是一谓词符号，那么我们可以写 $(\forall x)A(x)$ 和 $(\exists x)A(x)$，它们是完全有意义的。第一个意味着"每个对象具有

由 A 决定的属性”，第二个意指“有某些对象具有由 A 所决定的属性”。

例 3.2

把下列句子转换成符号。

(a) 并非所有鸟都会飞。

(b) 任何人都能做那件事。

(c) 有些人是愚蠢的。

(d) 有一整数大于其它每个整数。

答案：(当然可以有不同的方式)。

(a) $\sim(\forall x)(B(x)\rightarrow F(x))$

(b) $(\forall x)(M(x)\rightarrow O(x))$

象在上面所做的那样检查一下我们的步骤是有益的。“任何人都能做那件事”。意指“所有人都能做那件事”，恰恰如前，这意味着“对于所有 x，如果 x 是人，那么 x 能做那件事”。$M(x)$ 代表 x 是人，$O(x)$ 代表“x 能做那件事”。

(c) $(\exists x)(M(x)\wedge S(x))$

(d) $(\exists x)(I(x)\wedge(\forall y)(I(y)\rightarrow x\geqslant y))$。

我们应看到这些实例有一个常见的，尽管不是普遍的模式。全称量词后面常常跟一个蕴涵，因为一全称命题，在极大多数情况下具有形式：‘给出任何 x，如果它具有属性 A，那么也具有属性 B’。存在量词后面常常跟一个合取，因为一存在命题，在极大多数情况下具有形式‘存在一个有属性 A 的 x，它也有属性 B’。

让我们来进一步考察(a)。众所周知，这个断言是真的，我们可以举出如象鸵鸟，鹬鸵，或企鹅的例子证实它。直觉上，我们可以通过证实‘有一只不会飞的鸟’，来证实‘并非所有鸟都会飞’。这里，两个量词之间有着一个重要的联系，稍加思考将会确信上述句子有同样的意义。让我们把它们翻译成符号

(i) $\sim(\forall x)(B(x)\rightarrow F(x))$

和

(ii) $(\exists x)(B(x)\wedge\sim F(x))$

为了进一步对它们作比较，让我们把(i)式转换成

$$\sim(\forall x)(\sim B(x)\vee F(x)),$$

根据第一章的规则，进而变成

$$\sim(\forall x)\sim(B(x)\wedge\sim F(x))$$

现在，这就和(ii)式有相仿的形式，只是用 $\sim(\forall x)\sim$ 代替了 $(\exists x)$

这些例子的考察，使我们直觉上能明白两个句子：

(i) 并非所有 x 都不具有属性 P.

(ii) 存在某个 x 具有属性 P.

有着同样的含义，而不管属性 P 指的是什么.

例 3.3

把下列各句写成符号，首先不用全称量词，然后不用存在量词.

(a) 所有鸟都会飞.

(b) 人皆不是鸟.

(c) 有些数不是有理数.

答案：

(a) $\sim(\exists x)(B(x)\wedge\sim F(x))$

$(\forall x)(B(x)\rightarrow F(x))$.

(b) $\sim(\exists x)(M(x)\wedge I(x))$

$(\forall x)(M(x)\rightarrow\sim I(x))$.

(c) $(\exists x)(N(x)\wedge\sim R(x))$

$\sim(\forall x)(N(x)\rightarrow R(x))$.

(当然，还可有另一些等价的方式.)

现在我们既然知道怎样转换成符号，那么怎样借助它去判定命题之间的关系或论证的有效性呢？把真值表的用法加以推广是不可能的，因为现在我们的句子已不是真值函数了. 变元和量词

的使用意味着，一个句子的真值并不象以前那样只依赖于成分部分的真值，而且这些部分也并不总具有真值。特别地，对于包含一个变元而又不出现量词的句子部分，例如在前面例子中的'x是鸟'，或 $B(x)$，谈论它们的真值是没有意义的。

练习

1．把下列命题，用量词，变元和谓词符号写成符号形式

(a) 并非每一函数都有导数。

(b) 存在一个函数，连续而不可导。

(c) 如果有些火车迟到，那么所有火车都迟到。

(d) 每个数或是偶的或是奇的。

(e) 没有一个数既是偶的又是奇的。

(f) 有些人憎恨每个人。

(g) 象比耗子重。

2．把下列各命题写成符号形式。先不用存在量词，然后不用全称量词。

(a) 并非所有汽车都有三只轮子。

(b) 有些人或者是懒惰的或者是愚蠢的。

(c) 没有一个耗子比任何一个象重。

(d) 每个数或者是负的或者有一平方根。

3．写出练习 1 和 2 中任何一对命题，它们具有同样的意义。

3.2 一阶语言

分析含有量词的命题和论证的一种方法是三段论逻辑。这个题材已有长期的历史，起始于亚里士多德，一直延续到今天，有兴趣的读者可以在其它书(例如，Copi 中寻找到它；这里我们将不加以详述。三段论的基础是对较少量的，直觉上知其为有效的特殊的论证形式的研究，例如我们在本章开始时提到的：

所有 A 皆是 B,

C 是 A,

∴ C 是 B.

目的是,给出一个特殊的论证之后,用一个或几个这种基本的论证形式去表示它,从而去证明它的有效性. 现代逻辑学家和数学家发现这个系统太狭窄了,因而探索了一种不同的分析方法. 已经获得的发展和我们将要予以研究的,在导向三段论逻辑所想象不到的新的丰富的研究领域方面具有巨大的数学上的价值.

我们来构造一个形式系统. 正如我们所能期待着的,它比第二章中的形式系统要复杂得多,但是它被建立于其上的原理则是相同的. 首先,我们必须描述一个形式化的语言,给出符号库和构造合式公式的规则,在这方面,我们受到上面把普通语言翻译成符号的经验的启示,因为我们的目的是构造一种形式语言,使得我们能够把这样的普通句子转换成系统中的合式公式,并把句子的逻辑性质反映到系统内的合式公式的性质中去. 在此我们再次要搞清楚,形式语言的符号不得具有在形式系统内已作规定之外的任何意义和性质. 它们有时可以按不同的方式加以解释,但是这些解释并不是系统的一个部分.

符号库如下:

$x_1, x_2, \cdots$	变元
$a_1, a_2, \cdots$	个体常元
$A_1^1, A_2^1, \cdots; A_1^2, A_2^2, \cdots; A_1^3, A_2^3, \cdots; \cdots$	谓词字母
$f_1^1, f_2^1, \cdots; f_1^2, f_2^2, \cdots; f_1^3, f_2^3, \cdots; \cdots$	函数字母
(,), ,	括号
$\sim, \rightarrow$	联结词
$\forall$	量词

注记 3.4

(a) 这里包括了个体常元,这样,在我们的语言中,就不妨有

这种公式，它可被解释为关于某个特殊事物的命题．例如，命题‘苏格拉底是人’就可以作为公式 $A_1^1(a_1)$ 的解释．

(b) 这里有谓词字母序列的序列．首先是一列一目谓词字母，专门用来解释一目谓词(如‘是人’)．跟着的一列是二目谓词字母，表示关系或二目谓词(如‘是…的父亲’)．以此类推．(日常语言中一个三目谓词的例子是命题‘点 A，B 和 C 是共线的’中的‘是共线的’．)

(c) 在我们迄今的非形式的翻译中还不曾见到任何代表函数的字母：函数的概念对数学来说是如此重要以至在形式语言中允许用字母去表示函数是有利的．这是因为我们意图中的符号的解释主要是数学的．当然，一个函数是一特殊类型的关系，因此只要有符号去表示关系(谓词字母)其实也就够了，但是我们的兴趣并不限于作出尽可能小的符号字母库．我们还用到另一个标准，那就是直觉的清晰性．今后，当我们讨论特殊的数学系统时，将会十分清楚地看到把函数字母包括进去的效果．恰如在谓词字母一样，我们有不同的函数字母序列，皆在表示带有不同数目变元的函数．在两种情形中，上标数都是指的变元或变量的数目．

(d) 在语言中只有一个量词，全称量词．我们已知存在量词可由全称量词加以定义，因此我们只需其中之一，正如我们也只需有 $\sim$ 和 $\rightarrow$，作为我们的联结词一样．

(e) 存在无限的符号列，尽管我们将只允许它们的有限组合作为合式公式(参见下面)．我们需要潜在的无限多的符号，为了使我们的语言尽可能的广泛．在应用中，我们仅对其中某些符号规定其解释，某些应用可能需要更多的符号，所以我们并不希望对能被解释的符号的数目给出上界．

▷一般地，一个一阶语言 $\mathscr{L}$ 将有这样的符号库：

变元 $x_1, x_2, \cdots$，

某些(可能没有)个体常元 $a_1, a_2, \cdots$，

某些(可能没有)谓词字母 A_i^n,

某些(可能没有)函数字母 f_i^n,

括号(,)和, ,

联结词 ~ 和 →,

量词 ∀.

显然,要视所包含的符号而定有多种不同的一阶语言. 在我们的大多数工作中,将不特别指明采用的是何种语言,因而,我们得到的结果可应用于任何语言,'一阶'一词的意义以后将说明,它和全称量词的使用有关.

为了完整地规定一形式语言,我们必须讲清楚一个合式公式是什么,但是让我们在这样做之前先考察几个例子.

例 3.5

(a) 如果我们希望我们的一阶语言能适当地表达有关自然数的算术命题,我们可以取 $\mathscr{L}$ 使具有以下符号(除包括变元,括号,联结词和量词之外):

a_1, 代表 0,

A_1^2, 代表 =,

f_1^1, 代表后继函数,

f_1^2, 代表 +,

f_2^2, 代表 ×.

那么,例如 $A_1^2(f_1^2(x_1, x_2), f_2^2(x_1, x_2))$

将被解释为'$x_1+x_2=x_1\times x_2$'.

(b) 如果我们希望一阶语言能适当地表达关于群的命题,我们可以取 $\mathscr{L}$ 使具有符号(除包括变元,括号,联结词和量词之外):

a_1, 代表恒等元

A_1^2, 代表 =,

f_1^1, 代表取每个元素的逆元的函数,

f_1^2, 代表群的二元运算.

因此，例如 $A_1^2(f_1^2(x_1, f_1^1(x_1)), a_1)$

将被解释成'$x_1x_1^{-1}$=恒等元'.

定义 3.6

在定义合式公式之前，我们需要某些准备. 令 $\mathscr{L}$ 是一阶语言. $\mathscr{L}$ 中的一个项定义如下.

(i) 变元和个体常元是项.

(ii) 如果 f_i^n 是 $\mathscr{L}$ 中的函数字母，且 $t_1, \cdots, t_n$ 是 $\mathscr{L}$ 中的项，那么 $f_i^n(t_1, \cdots, t_n)$ 是 $\mathscr{L}$ 中的项.

(iii) 所有项组成的集都按(i)和(ii)生成.

项在形式语言中将是那样一些表达式，它们可解释成对象，即函数作用于上的事物，具有某种属性的事物，对之作出某些断定的事物.

$\mathscr{L}$ 中的一个原子公式定义为：如果 A_j^k 是 $\mathscr{L}$ 中的一个谓词字母并且 $t_1, \cdots, t_k$ 是 $\mathscr{L}$ 中的项，那么 $A_j^k(t_1, \cdots, t_k)$ 是 $\mathscr{L}$ 中的一个原子公式.

原子公式是语言中可解释为断定的最简单的公式，例如某些对象具有某种性质. 这里'原子'一词当然意指不可能再分解'.

原子公式，继续术语所启示的类比，是借以构造合式公式的，它们按逻辑规则组合，所处地位相当于在我们以前的形式系统中的命题字母.

$\mathscr{L}$ 中的一个合式公式定义为：

(i) $\mathscr{L}$ 中每个原子公式是 $\mathscr{L}$ 的一个合式公式.

(ii) 如果 $\mathscr{A}$ 和 $\mathscr{B}$ 是 $\mathscr{L}$ 的合式公式，那么 $(\sim\mathscr{A})$，$(\mathscr{A}\to\mathscr{B})$ 和 $(\forall x_i)\mathscr{A}$（其中 x_i 是任何变元）也是 $\mathscr{L}$ 的合式公式.

(iii) $\mathscr{L}$ 中所有合式公式组成的集都按(i)和(ii)生成.

注记 3.7

(α) 合式公式简称公式，从原子公式建造公式和以前在 L 中的情况一样，当然除包含全称量词的情形外. 如果 $\mathscr{A}$ 是 $\mathscr{L}$ 的一个

公式，那么$(\forall x_i)\mathscr{A}$也是，其中x_i是任何变元．因此，作为一个例子，如果$A_1^1(x_2)$是$\mathscr{L}$的一个公式，那么$(\forall x_1)A_1^1(x_2)$也是一公式．因此量词和它所作用的公式没有什么必要的联系，尽管我们显然更多地关注到被约束变元确实出现在后面跟着的公式之中的情形．

(b) 如同在系统L中一样，我们只收进$\sim$和$\rightarrow$两个联结词．这是为了使语言的和基于语言之上的形式系统的性质之证明得到简化．出于同样的理由，我们没有收进符号$\exists$．但是我们以后将看到，使用符号$\exists$和联结词$\wedge$和$\vee$的方便，为此只需遵循前面的直觉引导把它们作为被定义符号而引进．

$(\exists x_i)\mathscr{A}$是$(\sim((\forall x_i)(\sim\mathscr{A})))$的缩写，

$(\mathscr{A}\wedge\mathscr{B})$是$(\sim(\mathscr{A}\rightarrow(\sim\mathscr{B})))$的缩写，

$(\mathscr{A}\vee\mathscr{B})$是$((\sim\mathscr{A})\rightarrow\mathscr{B})$的缩写．

包含这些符号的公式，严格地讲不是形式语言的公式，但是如果有必要，他们可以回复成公式．

(c) 在合式公式中用到的括号是由定义精确地给定的．但是，如我们在L中已做的，有时我们将省略它，只要不引起混淆即可．如前，符号$\sim$将预先假定适用于跟在后面的可能的最短公式，例如$(\sim\mathscr{A}\rightarrow\mathscr{B})$是$((\sim\mathscr{A})\rightarrow\mathscr{B})$的缩写．我们用类似的方式处理量词，例如$((\forall x_i)\mathscr{A}\rightarrow\mathscr{B})$实际上是一个公式，这里没有括号被省略，应该注意这个公式和公式$(\forall x_1)(\mathscr{A}\rightarrow\mathscr{B})$的区别．让我们再引进一些与此有关的术语．

定义 3.8

在公式$(\forall x_i)\mathscr{A}$中，我们称$\mathscr{A}$是量词的辖域．更一般地，当$((\forall x_i)\mathscr{A})$在公式$\mathscr{B}$中作为子公式出现时，我们说这量词在$\mathscr{B}$中的辖域是$\mathscr{A}$．

变元x_i在一个公式中的出现称为约束的，如果它出现在公式中的$(\forall x_i)$的辖域之中，或者如果x_i在$(\forall x_i)$中，如果一个变元的出

现不是约束的，它就称为自由的.

例 3.9

(a) 在公式$(\forall x_1)A_1^1(x_2)$中，量词$(\forall x_1)$的辖域是$A_1^1(x_2)$，变元x_2是自由出现，变元x_1是约束出现.

(b) $(\forall x_1)(\forall x_2)(A_1^2(x_1, x_2)\to A_1^1(x_2))$是一公式，其中所有$x_1$和$x_2$的出现都是约束的. $(\forall x_1)$的辖域是$(\forall x_2)(A_1^2(x_1, x_2)\to A_1^1(x_2))$，$(\forall x_2)$的辖域是$(A_1^2(x_1, x_2)\to A_1^1(x_2))$.

(c) $(\forall x_1)(A_1^2(x_1, x_2)\to(\forall x_2)A_1^1(x_2))$是一公式，其中$x_1$有两次约束出现，$x_2$有一次自由出现和两次约束出现. $(\forall x_1)$的辖域是$(A_1^2(x_1, x_2)\to(\forall x_2)A_1^1(x_2))$，$(\forall x_2)$的辖域是$A_1^1(x_2)$.

▷上面我们用到过并不是形式语言的一部分的符号，即$\mathscr{A}$和$\mathscr{B}$. 读者将会记起在第二章中的类似情况. 这些字母是普通数学语言的一部分，我们是在用它们去描写和讨论形式语言的，它们被允许去代表形式语言中的公式（常常是任意的）. 我们有时也写，例如$\mathscr{A}(x_1)$或$\mathscr{B}(x_1, \cdots, x_n)$，当我们对特殊的变元（或项）感兴趣时. 这样的表达式常常是指，但非永远是指，在合式公式中提到的变元是自由出现的. 如果x_i确实在$\mathscr{A}(x_i)$中自由出现，那么对于任何项t，$\mathscr{A}(t)$将指对x_i的每个自由出现都代入t后所得的结果.

例 3.10

让我们考察一下被量词约束的变元的用法，回到前面的例子$(\forall x_1)A_1^1(x_2)$. 直觉上，它是被指望按这样一条思路来解释的："不管x_1代表什么对象，由A_1^1确定的属性适合由x_2代表的对象". 这里的量词显然是多余的，在$(\forall x_1)$处换上另外一些量词同样也是多余的. $(\forall x_3)A_1^1(x_2)$有同样的直觉解释，$(\forall x_7)A_1^1(x_2)$亦如此. 但是，十分明显，$(\forall x_2)A_1^1(x_2)$的直觉解释本质上不同于上述任何一种. 它是"不管x_2代表什么对象，由A_1^1确定的属性总适合该对象". 并且，无需借助直觉的解释，$(\forall x_2)A_1^1(x_2)$和其它几个之间有

纯形式上的差别，这就是其中出现的两个变元是相同的。

有时，我们偶而也会用其它变元或项去代换某一变元，我们希望按这样的方式去做这工作，使得代换后的结果和代换前的结果在直觉解释上没有差别。就同例$(\forall x_1)A_1^1(x_2)$来说：如果用x_3代换x_2，我们得到有相同的解释的一个公式，如果我们用x_1去替换x_2，我们得到的公式，就有不同的解释。我们说x_3对$(\forall x_1)A_1^1(x_2)$中的x_2是自由的，但是x_1就不是了。更为一般地，如果我们用$f_1^2(x_1, x_3)$去替换x_2，就得到$(\forall x_1)A_1^1(f_1^2(x_1, x_3))$，量词$(\forall x_1)$和它现在的辖域之间有了相互作用。所以我们说$f_1^2(x_1, x_3)$对$(\forall x_1)A_1^1(x_2)$中的$x_2$不是自由的。但是，任何不包含变元$x_1$的项，对$(\forall x_1)A_1^1(x_2)$中的$x_2$来说都是自由的。让我们把这个观念扩充为一个一般的定义。

定义 3.11

令$\mathscr{A}$是$\mathscr{L}$中的任何公式。项t对$\mathscr{A}$中的x_i是自由的，如果x_i并不自由出现在$\mathscr{A}$的一个$(\forall x_j)$的辖域中，这里x_j是出现在t中的任何变元。

粗略地说，这意指（如上）t可以代入$\mathscr{A}$中x_i的每个自由出现，而不引起和$\mathscr{A}$中量词的任何相互作用。

例 3.12

我们在上面已经见到某些例子。较为复杂的是

$$((\forall x_1)A_1^2(x_1, x_3)\rightarrow(\forall x_3)A_2^2(x_3, x_1)).$$

例如，$f_1^2(x_1, x_4)$对x_2不是自由的，$f_2^2(x_2, x_3)$对x_2是自由的，x_2对x_1是自由的（注意：x_1仅出现一次），$f_4^2(x_1, x_3)$对x_1不是自由的。

注记 3.13

对任何公式$\mathscr{A}$和任何变元x_i（不管它在$\mathscr{A}$中是否自由出现），x_i对$\mathscr{A}$中的x_i是自由的。

▷现在，我们已经描述过我们将要使用和展开的形式语言，如我们在第二章中那样，我们将着手给出公理和演绎规则以求完成

这类形式系统的规定，我们将把它们叫做一阶谓词演算系统．但是在这样做以前，还要适当地研究一下“解释”这个有点含糊的词，我们已经几次用到过它，现在试图使它精确化．

练习

4．令 $\mathscr{L}$ 是一阶语言，它的符号库不包括函数字母．描述 $\mathscr{L}$ 的项的集．

5．描述一阶语言的项的集，它的符号库不包括个体常元并且只有一个函数符号 f_1^1．

6．下列各式是公式吗？

(a) $A_1^2(f_1^1(x_1), x_1)$

(b) $f_1^3(x_1, x_3, x_4)$

(c) $(A_1^1(x_2) \to A_1^3(x_3, a_1))$．

(d) $\sim(\forall x_2)A_1^2(x_1, x_2)$

(e) $((\forall x_2)A_1^1(x_1) \to (\sim A_1^1(x_2)))$．

(f) $A_1^7(f_2^2(x_1, x_2, x_3))$．

(g) $(\sim A_1^1(x_1) \to A_1^1(x_2))$．

(h) $(\forall x_1)A_1^3(a_1, a_2, f_1^1(a_3))$．

7．在下列公式中，x_1 的那些出现是自由的，那些出现是约束的？

(a) $(\forall x_2)A_1^2(x_1, x_2) \to A_1^2(x_2, a_1))$．

(b) $(A_1^1(x_3) \to (\sim(\forall x_1)(\forall x_2)A_1^3(x_1, x_2, a_1)))$．

(c) $((\forall x_1)A_1^1(x_1) \to (\forall x_2)A_1^2(x_1, x_2))$．

(d) $(\forall x_2)(A_1^2(f_1^2(x_1, x_2), x_1) \to (\forall x_1)A_2^2(x_3, f_2^2(x_1, x_2)))$．

项 $f_1^2(x_1, x_3)$ 对所有这些公式或其中一个公式中的 x_2 是自由的吗？

8．令 $\mathscr{A}(x_i)$ 是 $\mathscr{L}$ 中一公式，其中 x_i 自由出现，令 x_j 是在 $\mathscr{A}(x_i)$ 中并不自由出现的一变元．证明：如果 x_j 对 $\mathscr{A}(x_i)$ 的 x_i 是自

由的，那么 x_i 对 $\mathscr{A}(x_j)$ 中的 x_j 是自由的．$\mathscr{A}(x_j)$ 是对 $\mathscr{A}(x_i)$ 中 x_i 的每个自由出现代入 x_j 后的结果．

9．在下列各种情况中，令 $\mathscr{A}(x_1)$ 是给定的公式，并且令 t 是项 $f_1^2(x_1, x_3)$．写出公式 $\mathscr{A}(t)$，并且判定，在每种情况下 t 对给定的公式中的 x_1 是否自由．

(a) $((\forall x_2)A_1^2(x_2, f_1^2(x_1, x_2))\rightarrow A_1^1(x_1))$．

(b) $(\forall x_1)(\forall x_3)(A_1^1(x_3)\rightarrow A_1^1(x_1))$．

(c) $(\forall x_2)A_1^1(f_1^1(x_2))\rightarrow(\forall x_3)A_1^3(x_1, x_2, x_3)$．

(d) $(\forall x_2)A_1^3(x_1, f_1^1(x_1), x_2)\rightarrow(\forall x_3)A_1^1(f_1^2(x_1, x_3))$．

10．对下面的项 t 重做练习 6．

(a) x_2．

(b) x_3．

(c) $f_1^2(a_1, x_1)$．

(d) $f_1^3(x_1, x_2, x_3)$

3.3 解释

定义 3.14

$\mathscr{L}$ 的一个解释 I，是一非空集 D_I（I 的论域），连同一个特异元素集 $(\bar{a}_1, \bar{a}_2, \cdots)$，一个在 D_I 上的函数集 $(\bar{f}_i^n, i>0, n>0)$，和一个在 D_I 上的关系集 $(\bar{A}_i^n, i>0, n>0)$．

▷前面曾指出，按我们的意图，$\mathscr{L}$ 的变元 $x_1, x_2, \cdots$ 将被解释为"对象"．集 D_I 将是假定变元在其上取值的对象领域．特异元的集合由 $\mathscr{L}$ 中个体常元所代表的特殊对象组成．相仿地，关系和函数将是对 $\mathscr{L}$ 中谓词字母和函数字母的具体解释．注意，对一特殊语言 $\mathscr{L}$ 而言，列出的常元，函数字母和谓词字母可以是有限制的，这样的一个语言 $\mathscr{L}$ 的一个解释，将只要有足够的特异元，函数和关系去解释 $\mathscr{L}$ 中出现的符号就可以了．

现在我们能够更清楚地了解术语"一阶语言"了．这样的语

言，包含可解释为一个解释的论域中的对象的变元，和与这些变元相关联的量词．所以，在一个解释中，量词作用在域内的对象上．这是一阶语言的特征．一个二阶语言则除此之外还要包含这样的量词，它可被解释成作用在一解释域的对象之间的关系上(因而也是对象的集上)．这样的语言将有两类变元，一类是相对于对象的，另一类相对于关系．我们将把注意完全限制在一阶语言和一阶形式系统之上．

例 3.15

形式算术．其一阶语言的一个适当的描述见例 3.5(a)．它包括 a_1, A_1^2, f_1^1, f_1^2, f_2^2, 以及变元、括号、联结词和量词．我们可以定义一个解释 N 如下．令 $D_N=\{0, 1, 2, \cdots\}$，自然数集．唯一特异元为 O(个体常元 a_1 的解释)．自然数的加法和乘法，分别为两元函数字母 f_1^2 和 f_2^2 的解释，后继函数是 f_1^1 的解释．关系 $=$ 是谓词字母 A_1^2 的解释．

在这个语言中的公式，依上所述，可以被解释成关于自然数的命题．例如公式

$$(\forall x_1)(\forall x_2)\sim(\forall x_3)(\sim A_1^2(f_1^2(x_1, x_3), x_2)) \qquad (*)$$

有解释

对于所有 x、$y\in D_N$，并非对所有 $z\in D_N$ 来说，$x+z\neq y$．

等价地

对于所有 x、$y\in D_N$，存在 $z\in D_N$，使得 $x+z=y$．

▷一个不能作为适当的一阶语言中某个公式的解释的关于自然数的命题是："每个非空自然数的集都有一个最小数"．这个命题以作用于数集上的全称量词开始，因此它对应于一个关于算术的二阶语言中的公式．

仅当 $\mathscr{L}$ 的符号的解释给出后，我们才能对有关的公式的意义说些什么，因此也只有在一个解释的情景中，我们才能考察真或假．上面的公式(*)在这种解释之下原来具有假的意义，但是在不

同的解释之下，它的意义可以是真的.

例 3.16

公式(*)在解释 I 之下，具有真的意义，这里 D_I 是正有理数集，1 是 a_1 的解释，乘法是 f_1^2 的解释，除法(商函数)是 f_2^2 的解释.

(*)在 I 中被译为

对所有 x, $y \in D_I$, 存在 $z \in D_I$, 使得 $xz=y$

这是众所周知的有理数的性质.

▷我们收入最后这例子，主要想说明，对同一语言 $\mathscr{L}$ 可能有几种实质上不同的解释. 在我们列举的语言例子时，我们心中是有某些规范的特殊解释的，但是这并不能阻碍我们考察它们实际存在着的其它解释和推论.

现在，我们可以看到这种情况和第二章中的情况之间相似之处. 命题演算系统 L 的公式，凭本身不能看成真或假. 真和假只有当我们对命题变元指派了真值，或建立了一赋值时才不是无关紧要的. 此外，我们已看到，某些公式既可能真也可能假，要由赋值而定. 在我们目前的系统中，情况比较复杂，解释的概念将与真值的指派相对应. 现在，显然会提出的问题是：我们有没有重言式那样的类似物？答案是肯定的，而且定义是恰如人们所期望的，但我们将稍后一点再回过来考察它. 现在我们必须把一个解释中真实的观念予以精确化. 不管下面要讲的在表面上怎么复杂，概念本身并不困难，读者要记住我们已经建立起来的直觉的图景. 在本章剩下部分，建议对该题材陌生的读者，于第一遍阅读时，不妨略去详细的证明. 对于直觉地掌握涉及的思想，证明并不重要，太仔细地注意到细节反而会掩盖那些思想.

练习

11. 令 $\mathscr{L}$ 是一阶语言，含有(除包括变元，括号，联结词和量词之外)个体常元 a_1，函数字母 f_1^2 和谓词字母 A_2^2. 令 $\mathscr{A}$ 表示公

式

$$(\forall x_1)(\forall x_2)(A_2^2(f_1^2(x_1, x_2), a_1) \to A_2^2(x_1, x_2)).$$

定义 $\mathscr{L}$ 的一个解释 I 如下. D_I 是 $\mathbf{Z}$, $\bar{a}_1$ 是0, $\bar{f}_1^2(x, y)$ 是 $x-y$, $\bar{A}_2^2(x, y)$是 $x<y$. 写出 $\mathscr{A}$ 在 I 中的解释. 它是真命题还是假命题? 求另一解释,在其中, $\mathscr{A}$ 被解释为一个取相反真值的命题.

12. 是否存在一个解释(适当的语言 $\mathscr{L}$ 中的),能使公式

$$(\forall x_1)(A_1^1(x_1) \to A_1^1(f_1^1(x_1)))$$

被解释为一个取值为假的命题? 如果能的话,详细地描述一个. 如果不能,说明为什么.

13. 对下面的合式公式重做习题 12.

$$(\forall x_1)(A_1^2(x_1, x_2) \to A_1^2(x_2, x_1)).$$

3.4 满足,真

令 I 是以 D_I 为域的语言 $\mathscr{L}$ 的一个解释. 此后我们将采用定义 3.14 中的记号. a_i, f_i^n, A_i^n 在 I 中的解释将分别指 $\bar{a}_i$, $\bar{f}_i^n$, $\bar{A}_i^n$. 注意,对每个 i, $\bar{a}_i \in D_I$, $\bar{f}_i^n: D_I^n \to D_I$, 并且 $\bar{A}_i^n$ 是 D_I 上的 n 元关系.

定义 3.17

I 上的一个赋值是一从 $\mathscr{L}$ 的项集到集 D_I 的具有下列性质的一个函数 v:

(i) $v(a_i) = \bar{a}_i$, 对 $\mathscr{L}$ 中的每个个体常元 a_i.

(ii) $v(f_i^n(t_1, \cdots, t_n)) = \bar{f}_i^n(v(t_1), \cdots, v(t_n))$, 其中 f_i^n 是 $\mathscr{L}$ 中的任意函数字母, $t_1, \cdots, t_n$ 是 $\mathscr{L}$ 中的任意项.

因此一赋值恰是一个规则, 它对 $\mathscr{L}$ 中的每个项, 指派了 D_I 中的一个对象作为它应有的解释. 上面的条件 (ii) 保证规则是一致的.

注记 3.18

(a) 一般地,在一给定的解释下,将有多种不同的赋值.

(b) 一给定的赋值，将对 $\mathscr{L}$ 中每个变元 x_i 指派 D_I 的一个元素．赋值 v 可以通过给出 $v(x_1)$，$v(x_2)$，… 而完全确定．这是因为，$v(a_i)$ 通过(i)被给定，并且对于任意项 $f_i^n(t_1, \cdots, t_n)$，$v(f_i^n(t_1, \cdots, t_n))$ 的值，可以根据(ii)归纳地加以确定．

▷我们以后将需要同在下述意义下几乎相等的赋值打交道．

定义 3.19

两赋值 v 和 v' 称为是 i-等值的，如果 $v(x_j)=v'(x_j)$，对每个 $j\neq i$．

i-等值赋值，除在 x_i 处可能不等外，对其它每个变元都有相同的值，但是要注意，一般地说任何出现 x_i 的项，其值将是不同的．

▷现在，让我们考察 $\mathscr{L}$ 的一个公式 $\mathscr{A}$．一个给定的赋值，按下面的方式可以有"指派一个真值"给 $\mathscr{A}$ 的效果．用 $v(t)$ 替换 $\mathscr{A}$ 中出现的每个项 t，对每个函数字母和谓词字母用它们在 I 中的解释，相应地加以替换．这样所得的就是一个关于集 D_I 中元素的命题，它可真可假．如果它是真的，我们就说 v 满足 $\mathscr{A}$．我们把它精确化如下．

定义 3.20

令 $\mathscr{A}$ 是 $\mathscr{L}$ 的一个公式，I 是 $\mathscr{L}$ 的一个解释．I 中的一个赋值 v 称为满足 $\mathscr{A}$，如果能按如下四个条件归纳地表明 v 满足 $\mathscr{A}$．

(i) v 满足原子公式 $A_j^n(t_1, \cdots, t_n)$，如果 $\overline{A}_j^n(v(t_1), \cdots, v(t_n))$ 在 D_I 中为真．

(ii) v 满足 $(\sim\mathscr{B})$，如果 v 不满足 $\mathscr{B}$．

(iii) v 满足 $(\mathscr{A}\rightarrow\mathscr{B})$，如果 v 或者满足 $(\sim\mathscr{B})$，或者满足 $\mathscr{C}$．

(iv) v 满足 $(\forall x_i)\mathscr{B}$，如果每个 i-等值于 v 的赋值 v' 满足 $\mathscr{B}$．

注记 3.21

(a) 对 $\mathscr{A}$ 中任何赋值，v 或者满足 $\mathscr{A}$ 或者满足 $(\sim\mathscr{A})$．

(b) 对(iv)作某些说明或许是必要的．$(\forall x_i)\mathscr{B}$ 将被解释为某命题"对于每个 $y\in D_I$，…"，在此 y 被看成是 x_i 的解释．v 对于

出现在 $\mathscr{B}$ 中的变元提供了解释，因此如果 v 首先满足 $\mathscr{B}$，而且由 v 通过改变 $v(x_i)$ 而得的任何赋值也满足 $\mathscr{B}$，说 v 满足 $(\forall x_i)\mathscr{B}$ 是合理的。

(c) 指出上述(i)到(iv)每个付句都可看成"当且仅当"命题，可能有助于理解定义，因为每个都是定义的性质。

例 3.22

(a) 在算术解释 N 中，考虑公式 $A_1^2(f_2^2(x_1, x_2), f_2^2(x_3, x_4))$ 任何使 $v(x_1)=2$, $v(x_2)=6$, $v(x_3)=3$, $v(x_4)=4$ 的赋值，都将满足这个公式，因为 $2\times6=3\times4$ 在 D_N 中是真的。相反，任何赋值 w，使得 $w(x_1)=1$, $w(x_2)=5$, $w(x_3)=4$, $w(x_4)=2$ 时，都将不满足它。

(b) 公式 $(\forall x_1)A_1^2(f_2^2(x_1, x_2), f_2^2(x_2, x_1))$ 在 N 中被解释为："对于每个 $n\in D_N$, $nm=mn$"。一个无疑要看成真的命题。令 v 是 N 中的一个赋值。那么 $v(x_1)$ 和 $v(x_2)$ 是自然数，于是 $A_1^2(f_2^2(x_1, x_2), f_2^2(x_2, x_1))$ 被解释成 $v(x_1)\times v(x_2)=v(x_2)\times v(x_1)$，这确实是真的。所以 v 满足 $A_1^2(f_2^2(x_1, x_2), f_2^2(x_2, x_1))$。此外，如果我们改变 $v(x_1)$ 的值，得到一个新的 1-等值赋值 v'，容易看到 v' 也满足 $A_1^2(f_2^2(x_1, x_2), f_2^2(x_2, x_1))$。因此，根据上面定义(iv)，$v$ 在 N 中满足 $(\forall x_1)A_1^2(f_2^2(x_1, x_2), f_2^2(x_2, x_1))$。这样在 N 中每个赋值 v 都满足这个公式。

(c) 公式 $(\forall x_1)A_1^2(x_1, a_1)$ 直觉上被解释成"对于每个 $n\in D_N$, $n=0$"，一个假命题。令 v 是 N 中一个赋值。那么，$A_1^2(x_1, a_1)$ 可解释为"$v(x_1)=0$"。所以除非 $v(x_1)=0$, v 不满足 $A_1^2(x_1, a_1)$。因此，假设 $v(x_1)=0$，问 v 是否满足 $(\forall x_1)A_1^2(x_1, a_1)$。要能满足的话我们必须能够说，任何由 v 通过改变 $v(x_1)$ 值而得的 v' 都能满足 $A_1^2(x_1, a_1)$。显然我们不能做到。因此在 N 中的赋值都不满足 $(\forall x_1)A_1^2(x_1, a_1)$。

▷今后，用另外的变元和项去代入一个变元是一重要的技术。

下面的命题是必须的，尽管它的技巧使得证明复杂了，它示范了在这方面一个证明所采取的形式。

命题 3.23

令 $\mathscr{A}(x_i)$ 是 $\mathscr{L}$ 的一个公式，其中 x_i 自由出现，并且令 t 是在 $\mathscr{A}(x_i)$ 中对 x_i 自由的项。假设 v 是一赋值，且 v' 是 i-等值于 v 的赋值，并且有 $v'(x_i)=v(t)$。那么 v 满足 $\mathscr{A}(t)$ 当且仅当 v' 满足 $\mathscr{A}(x_i)$。

证明 首先要注意到，对于出现 x_i 的任意项 u，当我们通过以 t 处处代入 x_i 而得到一个项 u' 时，总有 $v(u')=v'(u)$。我们通过对 u 的长度(即 u 中符号的数目)进行归纳来证明。

基础步骤：u 是 x_i，所以 u' 是 t，因此

$$\begin{aligned} v'(u)&=v'(x_i)=v(t),\text{(根据 } v' \text{ 的定义)}\\ &=v(u') \end{aligned}$$

归纳步骤：u 是 $f_i^n(u_1, \cdots, u_n)$，其中 $u_1, \cdots, u_n$ 是较小长度的项。令 $u_1', \cdots, u_n'$ 是通过以 t 处处代入 x_i 而得到的，因此 $u'=f_i^n(u_1', \cdots, u_n')$。所以

$$\begin{aligned} v(u')&=\bar{f}_i^n(v(u_1'), \cdots, v(u_n'))\\ &=\bar{f}_i^n(v'(u_1), \cdots, v'(u_n))\\ \text{据归纳假设}\quad &=v'(u). \end{aligned}$$

因此 $v(u')=v'(u)$ 已被确立，对 $\mathscr{L}$ 中每个项 u。

现在，我们通过对公式 $\mathscr{A}(x_i)$ 的长度，即 $\mathscr{A}(x_i)$ 中联结词和量词数目，进行归纳而证明命题。

基础步骤：$\mathscr{A}(x_i)$ 是一原子公式，即 $A_j^n(u_1, \cdots, u_n)$，其中 $u_1, \cdots, u_n$ 是 $\mathscr{L}$ 的项。设 v' 满足 $\mathscr{A}(x_i)$。因此

$$\bar{A}_j^n(v'(u_1), \cdots, v'(u_n))\text{在解释中成立，}$$

所以 $$\bar{A}_j^n(v(u_1'), \cdots, v(u_n'))\text{在解释中成立。}$$

其中 $u_1', \cdots, u_n'$ 如上通过以 t 处处代入 x_i 而得到。(这里，我们用了上面准备的结果。)现在我们有 v 满足公式 $A_j^n(u_1', \cdots, u_n')$，即 v

满足 $A(t)$. 逆命题可以通过倒转这个论证而得到证明.

归纳步骤:

情形 1: $\mathscr{A}(x_i)$ 是 $\sim\mathscr{B}(x_i)$.

情形 2: $\mathscr{A}(x_i)$ 是 $(\mathscr{B}(x_i)\to\mathscr{C}(x_i))$.

这些直接可得, 留作练习.

情形 3: $\mathscr{A}(x_i)$ 是 $(\forall x_j)\mathscr{B}(x_i)(j\neq i)$.

假设 v 不满足 $\mathscr{A}(t)$. 我们证明 v' 也不满足 $\mathscr{A}(x_i)$. 由假设有一 j-等值于 v 的赋值 w 不满足 $\mathscr{B}(t)$. 令 w' 是 i-等值于 w 的赋值, 且有 $w'(x_i)=w(t)$. 那么通过对 $\mathscr{B}(x_i)$ 使用归纳假设, 我们有 w' 不满足 $\mathscr{B}(x_i)$ (由于 w 不满足 $\mathscr{B}(t)$). 现在由于 t 对 $(\forall x_j)\mathscr{B}(x_i)$ 中的 x_i 自由, 所以 x_j 在 t 中不出现. 因此 $v(t)$ 仅依赖 $v(x_k), k\neq j$. 但是对 $k\neq j$, $v(x_k)=w(x_k)$, 所以 $v(t)=w(t)$. 由此可知 w' 是 j-等值于 v', 因为 w 是 j-等值于 v 的. 由于 w' 不满足 $\mathscr{B}(x_i)$, 于是 v' 不满足 $(\forall x_j)\mathscr{B}(x_i)$, 即 v' 不满足 $\mathscr{A}(x_i)$. 逆命题要求一类似的论证, 留作练习

定义 3.24

一公式 $\mathscr{A}$ 在解释 I 中称为真的, 如果在 I 中每个赋值都满足 $\mathscr{A}$. $\mathscr{A}$ 在解释 I 中称为假的, 如果不存在在 I 中满足 $\mathscr{A}$ 的任何赋值.

记法 我们写 $I\models\mathscr{A}$, 表示 $\mathscr{A}$ 在 I 中为真. 这个符号不应与 $\vdash$ 混淆, 但是读者应注意, 两符号都不是形式语言中的一个符号. 它们都是我们用来讨论形式系统的元语言的一部分.

注记 3.25

(a) 可能发生这样的情况, 对一个特殊的公式, I 中有些赋值满足 $\mathscr{A}$, 有些赋值不满足. 这样的公式, 在 I 中既不真也不假.

(b) 一个解释的域, 据定义是非空的, 所以显然赋值集也是非空的. 从定义清楚地看到, 一给定的赋值或者满足或者不满足一已知的公式 $\mathscr{A}$, 因此, 对一个公式来说, 不可能在一给定的解释之

下既真又假.

(c) 在一给定的解释中，一公式 $\mathscr{A}$ 是假的，当且仅当 $(\sim\mathscr{A})$ 是真的. 这是赋值和真值定义的直接推论. 由此可知，不存在公式 $\mathscr{A}$，能使 $\mathscr{A}$ 和 $(\sim\mathscr{A})$ 同时为真.

(d) 在一给定的解释中，一公式 $(\mathscr{A}\to\mathscr{B})$ 是假的，当且仅当 $\mathscr{A}$ 真并且 $\mathscr{B}$ 假. 让我们作出一个方向的证明，以说明怎样应用定义的. 假设 $(\mathscr{A}\to\mathscr{B})$ 在 I 是假的. 那么 I 中没有赋值满足 $(\mathscr{A}\to\mathscr{B})$. 因此给出任何赋值 v，v 都不满足 $(\mathscr{A}\to\mathscr{B})$. 根据定义 3.20(iii)，$v$ 不满足 $(\sim\mathscr{A})$ 并且 v 不满足 $\mathscr{B}$. 因此 v 满足 $\mathscr{A}$，并且 v 不满足 $\mathscr{B}$，所以每个赋值都满足 $\mathscr{A}$ 而不满足 $\mathscr{B}$. 由此知 $\mathscr{A}$ 真而 $\mathscr{B}$ 假.

命题 3.26

如果，在一特殊的解释 I 中，公式 $\mathscr{A}$ 和 $(\mathscr{A}\to\mathscr{B})$ 都真，那么 $\mathscr{B}$ 也真.

证明 令 v 是 I 的赋值. 那么 v 满足 $\mathscr{A}$ 并且 v 满足 $(\mathscr{A}\to\mathscr{B})$. 因此，根据满足的定义，或者 v 满足 $(\sim\mathscr{A})$，或者 v 满足 $\mathscr{B}$. 但是 v 不能满足 $(\sim\mathscr{A})$，所以 v 必须满足 $\mathscr{B}$. 既然 $\mathscr{B}$ 为 I 中每个赋值所满足，所以 $\mathscr{B}$ 在 I 中为真.

命题 3.27

令 $\mathscr{A}$ 是 $\mathscr{L}$ 的一个公式，并且令 I 是 $\mathscr{L}$ 的一个解释，那么 $I\models\mathscr{A}$，当且仅当 $I\models(\forall x_i)\mathscr{A}$，其中 x_i 为任意变元.

证明 假设 $I\models\mathscr{A}$，并且令 v 是 I 中的任一赋值. 那么 v 满足 $\mathscr{A}$，并且由于每个赋值满足 $\mathscr{A}$，每个 i-等值于 v 的赋值 v' 也满足 $\mathscr{A}$，因而 v 满足 $(\forall x_i)\mathscr{A}$，由此知每个赋值都满足 $(\forall x_i)\mathscr{A}$，即 $I\models(\forall x_i)\mathscr{A}$.

现在假设 $I\models(\forall x_i)\mathscr{A}$，且令 v 是 I 中任意赋值. 那么 v 满足 $(\forall x_i)\mathscr{A}$. 因此每个 i-等值于 v 的赋值满足 $\mathscr{A}$，特别地，v 也满足 $\mathscr{A}$，所以每个赋值满足 $\mathscr{A}$，即 $I\models\mathscr{A}$.

系 3.28

令 $y_1, \cdots, y_n$ 是 $\mathscr{L}$ 的变元，令 $\mathscr{A}$ 是 $\mathscr{L}$ 的公式，I 是一个解释。那么 $I \models \mathscr{A}$，当且仅当 $I \models (\forall y_1)\cdots(\forall y_n)\mathscr{A}$。

证明 重复应用命题 3.27 即可。

▷这个结果，有两个方面值得注意。首先，对 $\mathscr{A}$ 中并不自由出现的一个变元加一量词而得到 $(\forall x_i)\mathscr{A}$，直觉上并没改变它的解释(参见例 3.10)，为此，在这种情况下 $\mathscr{A}$ 真，当且仅当 $(\forall x_i)\mathscr{A}$ 真，就没有什么奇怪。对 $\mathscr{A}$ 中自由出现的变元加量词而得到 $(\forall x_i)\mathscr{A}(x_i)$，本有不同的效果。但是上面结果表明，$\mathscr{A}(x_i)$ 真，当且仅当 $(\forall x_i)\mathscr{A}(x_i)$ 真，为此当我们考察一个有自由变元的公式的真或假时，就有一种表示全称量词在此被省略了的意义。

存在量词是作为被定义符号而引进形式语言中的。让我们来看它是怎样适应赋值和满足的背景的。

命题 3.29

在一个解释 I 中，一赋值 v 满足 $(\exists x_i)\mathscr{A}$，当且仅当至少存在一个 i-等值于 v 并且满足 $\mathscr{A}$ 的赋值 v'。

证明 $(\exists x_i)\mathscr{A}$ 代表 $\sim(\forall x_i)(\sim\mathscr{A})$。令 v 满足 $\sim(\forall x_i)(\sim\mathscr{A})$。那么 v 不满足 $(\forall x_i)(\sim\mathscr{A})$。因此存在一个 i-等值于 v 的赋值 v' 不满足 $(\sim\mathscr{A})$。因而这个 v' 必定满足 $\mathscr{A}$。逆命题可通过倒转上面的论证而获证。

▷命题演算的语言包括联结词 $\sim$ 和 $\rightarrow$。当然语言 $\mathscr{L}$ 也包括它们。因此，如果我们取一 L 的公式 $\mathscr{A}_0$，并且对出现的每个命题字母，都用 $\mathscr{L}$ 的一个公式去替换(处处用同一公式替换同一字母)，我们将得到 $\mathscr{L}$ 的一个公式 $\mathscr{A}$，它称为 $\mathscr{A}_0$ 在 $\mathscr{L}$ 中的一个代入特例。类似地，从 $\mathscr{L}$ 的一个公式出发，我们能见到它将和 L 的某些(通常多于一个)公式有同样的结构。例如，考察

$$(\sim(\forall x_1)A_1^1(x_1)\rightarrow((\forall x_2)A_2^2(x_1, x_2)$$
$$\rightarrow(A_1^1(x_2)\rightarrow(\forall x_1)A_3^1(x_1)))).$$

这是 L 的合式公式$(\sim p_1 \to p_2)$的一个代入特例，也是 $(\sim p_1 \to (p^2 \to p_3))$的代入特例．考察另一例子

$$((\forall x_1)A_1^1(x_1) \to (\forall x_1)A_1^1(x_1)).$$

这个 $\mathscr{L}$ 的公式是 L 的公式 $(p_1 \to p_1)$ 的代入特例．现在 $(p_1 \to p_1)$ 是重言式．我们把重言式概念推广到 $\mathscr{L}$ 的公式如下．

定义 3.30

$\mathscr{L}$ 的一个公式 $\mathscr{A}$ 称为重言式，如果它是 L 的一个重言式在 $\mathscr{L}$ 中的代入特例．

命题 3.31

$\mathscr{L}$ 的一个是重言式的公式在 $\mathscr{L}$ 的任何解释下都是真的．

证明 定义 2.12 和 3.20 之间的类似产生了我们的方法．令 $\mathscr{A}$ 是 $\mathscr{L}$ 的这样一个公式，它是 L 的公式 $\mathscr{A}_0$ 的一个代入特例．我们能够从 I 中的任何一个赋值 v 得到一个 L 中的（部分）赋值 v' 如下．令 $p_1, \cdots, p_k$ 是 $\mathscr{A}_0$ 中出现的命题字母，并令 $\mathscr{A}_1, \cdots, \mathscr{A}_k$ 是 $\mathscr{L}$ 的那些公式，当它们分别代入前者后就得到 $\mathscr{A}$ 的．对 $1 \leqslant i \leqslant k$，令

$$v'(p_i) = \begin{cases} T & \text{如果 } v \text{ 满足 } \mathscr{A}_i \\ F & \text{如果 } v \text{ 不满足 } \mathscr{A}_i. \end{cases}$$

现在我们指出：v 满足 $\mathscr{A}$ 当且仅当 $v'(\mathscr{A}_0) = T$．通过对 $\mathscr{A}_0$ 中联结词的数目进行归纳加以证明．

基础步骤：$\mathscr{A}_0$ 是一命题字母，例如 p_n，那么，根据 v' 的定义，$v'(p_n) = T$ 当且仅当 v 满足 $\mathscr{A}$．

归纳步骤：

情况 1：$\mathscr{A}_0$ 是 $\sim \mathscr{B}_0$，所以 $\mathscr{A}$ 就是 $\sim \mathscr{B}$，即 $\mathscr{B}$ 是 $\mathscr{B}_0$ 的一个代入特例．根据归纳假设，v 满足 $\mathscr{B}$ 当且仅当 $v'(\mathscr{B}_0) = T$．因此 v 不满足 $\mathscr{B}$ 当且仅当 $v'(\mathscr{B}_0) = F$．由此可知 v 满足 $\mathscr{A}$ 当且仅当 $v'(\mathscr{A}_0) = T$，这里用到定义 3.20(ii)和 2.12(i)．

情况 2：$\mathscr{A}_0$ 是$(\mathscr{B}_0 \to \mathscr{C}_0)$，所以 $\mathscr{A}$ 是$(\mathscr{B} \to \mathscr{C})$，其中 $\mathscr{B}$ 和 $\mathscr{C}$

是 $\mathscr{B}_0$ 和 $\mathscr{C}_0$ 的代入特例. 下列断定都等价.

(a) v 满足 $\mathscr{A}$.

(b) 或者 v 满足 $\sim\mathscr{B}$, 或者 v 满足 $\mathscr{C}$(据定义 3.20(iii)).

(c) 或者 v 不满足 $\mathscr{B}$, 或者 v 满足 $\mathscr{C}$.

(d) 或者 $v'(\mathscr{B}_0)=F$, 或者 $v'(\mathscr{C}_0)=T$.

(e) $v'(\mathscr{B}_0\to\mathscr{C})=T$(据定义 2.12).

(f) $v'(\mathscr{A}_0)=T$.

这就完成了归纳证明. 本命题的证明现在是简易的.

令 $\mathscr{A}$ 是 $\mathscr{L}$ 的一个公式, 且为重言式. 那么 $\mathscr{A}$ 是 L 中重言式 $\mathscr{A}_0$ 的一个代入特例. 令 v 是在解释 I 中的一个赋值. 从上我们看到, 如果 $v'(\mathscr{A}_0)=T$, v 满足 $\mathscr{A}$. 但是 $\mathscr{A}_0$ 是一重言式, 所以 v 满足 $\mathscr{A}$, 因此 $\mathscr{A}$ 在 I 中是真的.

▷我们已经看到, 在一个给定的解释下, 并不是每个公式必须是真的或假的. 例如, 我们考察公式 $A_1^1(x_1)$, 和一个解释 I, 其中 D_I 是 Z, 即整数集, 且 A_1^1 的解释是谓词'>0', 那么 $A_1^1(x_1)$ 被任何赋值 v 所满足, 其中 v 有性质 $v(x_1)>0$, 但是 A_1^1 却不被任何具有性质 $w(x_1)<0$ 的赋值 w 所满足. 直觉上说, 究竟 $A_1^1(x_1)$ 成为真, 还是假, 依赖于 x_1 的解释. 这种情况常常在我们同一个其中有自由变元出现的公式打交道时发生. 下面的主要结果说, 一个没有自由变元出现的公式在一给定解释中, 必定或真或假. 首先我们需要某些准备工作.

定义 3.32

一个 $\mathscr{L}$ 的公式 $\mathscr{A}$ 称为闭的, 如果在 $\mathscr{A}$ 中没有变元的自由出现.

命题 3.33

令 I 是 $\mathscr{L}$ 的一个解释, $\mathscr{A}$ 是 $\mathscr{L}$ 的一个公式. 如果 v 和 w 都是赋值, 并且对 $\mathscr{A}$ 的每个自由变元 x_i 有 $v(x_i)=w(x_i)$, 那么 v 满足 $\mathscr{A}$ 当且仅当 w 满足 $\mathscr{A}$.

证明　通过对 $\mathscr{A}$ 中的联结词和量词的数目进行归纳.

基础步骤: $\mathscr{A}$ 是一个原子公式, 例如 $A_i^n(t_1, \cdots, t_n)$. 赋值 v 和 w 对出现于 $t_1, \cdots, t_n$ 中的自由变元和任何个体常元都相同, 所以 $v(t_i)=w(t_i)$ 对 $1\leqslant i\leqslant n$. 因而 v 满足 $\mathscr{A}$ 当且仅当 w 满足 $\mathscr{A}$.

归纳步骤:

情形 1: $\mathscr{A}$ 是 $\sim\mathscr{B}$.

情形 2: $\mathscr{A}$ 是 $(\mathscr{B}\rightarrow\mathscr{C})$.

这两种情况很简单, 只要用确切的定义就行. 留作练习.

情形 3: $\mathscr{A}$ 是 $(\forall x_i)\mathscr{B}$.

假设 v 满足 $\mathscr{A}$, 且令 w' i-等值于 w. 那么由于 x_i 在 $(\forall x_i)\mathscr{B}$ 中不自由出现, 我们有 $v(y)=w'(y)$, 不管 y 在 $\mathscr{A}$ 中是否自由. 现在每个 i-等值于 v 的赋值 v' 都满足 $\mathscr{B}$, 所以特别地, 可令 v' 由

$$v'(x_i)=w'(x_i)$$
$$v'(x_j)=v(x_j) \quad 如果\ j\neq i$$

确定. 那么 $w'(y)=v'(y)$, 不管 y 是否 $\mathscr{B}$ 中的自由变元. 因此根据归纳假设, 由于 v' 满足 $\mathscr{B}$, 我们就有 w' 满足 $\mathscr{B}$, 所以 w 满足 $(\forall x_i)\mathscr{B}$.

用完全一样的方法, 我们可证明如果 w 满足 $(\forall x_i)\mathscr{B}$, 那么 v 满足 $(\forall x_i)\mathscr{B}$.

归纳完成了, 结果获证.

系 3.34

如果 $\mathscr{A}$ 是 $\mathscr{L}$ 的闭公式, 且 I 是 $\mathscr{L}$ 的一个解释, 那么或者 $I\models\mathscr{A}$. 或者 $I\models(\sim\mathscr{A})$.

证明　令 $\mathscr{A}$ 是一闭公式, I 是一解释. 令 v 和 w 是任何赋值. 显然, $v(y)=w(y)$ 只要 y 是 $\mathscr{A}$ 的自由变元($\mathscr{A}$ 没有自由变元), 从而 v 满足 $\mathscr{A}$ 当且仅当 w 满足 $\mathscr{A}$. 因此, 或者每个赋值满足 $\mathscr{A}$, 或者没有赋值满足 $\mathscr{A}$, 即或者 $\mathscr{A}$ 在 I 中真, 或者 $\mathscr{A}$ 在 I 中假. 因此, 根据注记 3.25(c), 或者 $I\models\mathscr{A}$, 或者 $I\models(\sim\mathscr{A})$.

▷这是一个对我们有意义的结果，因为在一个解释中'真'的概念，比起"被一个赋值满足"的概念更为重要.我们已经建立的是，对闭公式来说在一特定解释中的一切赋值，给我们关于一个给定公式可否满足的问题以同样的答案. 因而要检验一个给定的闭公式的真或假，我们只需检验是否有某个赋值能满足它. 我们也将看到，就数学本身而论闭公式更为适切，而带有自由变元的公式，有时倒显得有点不自然.

解释给 $\mathscr{L}$ 的闭公式以真值. 可能会发生，对 $\mathscr{L}$ 的一个给定的公式，所有 $\mathscr{L}$ 的解释给它的值都是真的，即 $\mathscr{A}$ 在 $\mathscr{L}$ 的所有可能的解释下都是真的.

定义 3.35

$\mathscr{L}$ 的一个合式公式 $\mathscr{A}$ 称为逻辑有效的，如果 $\mathscr{A}$ 在 $\mathscr{L}$ 的每个解释下都是真的. $\mathscr{A}$ 是矛盾的，如果它在每个解释下都是假的.

这些概念是第1章中所讨论的重言式和矛盾式概念在目前情况中的类似. 恰如那时存在某些既不是重言式也不是矛盾式的公式一样，在 $\mathscr{L}$ 中也存在某些公式，他们既非逻辑有效式也非矛盾式.

注记 3.36

(a) 命题 3.26 的一个直接推论是，如果公式 $\mathscr{A}$ 和 $(\mathscr{A}\to\mathscr{B})$ 逻辑有效，那么 $\mathscr{B}$ 也逻辑有效.

(b) 同样，命题 3.27 的一个推论是，如果合式公式 $\mathscr{A}$ 逻辑有效，那么 $(\forall x_i)\mathscr{A}$ 也逻辑有效，其中 x_i 是任何变元.

例 3.37

(a) 我们已经看到 L 中一个重言式在 $\mathscr{L}$ 中的每个代入特例都是逻辑有效的(命题 3.31). 因此要注意 $\mathscr{L}$ 的逻辑有效公式类包括重言式类.

(b) $((\forall x_i)\mathscr{A}\to(\exists x_i)\mathscr{A})$ 是逻辑有效的，对 $\mathscr{L}$ 的任何合式公

式. $\mathscr{A}$. 通过下面标准的方法可以证明.

令 I 是以 D_I 为域的解释，令 v 是 I 中的一个赋值. 如果 v 不满足$(\forall x_i)\mathscr{A}$，那么 v 满足$((\forall x_i)\mathscr{A}\rightarrow(\exists x_i)\mathscr{A})$. 如果 v 满足$(\forall x_i)\mathscr{A}$，那么每个 i-等值于 v 的赋值 v' 满足 $\mathscr{A}$. 因此显然，有一个 i 等值于 v 的赋值满足 $\mathscr{A}$. 为此，据命题 3.29v 满足 $(\exists x_i)\mathscr{A}$. 因而在这种情况下，v 也满足$((\forall x_i)\mathscr{A}\rightarrow(\exists x_i)\mathscr{A})$. 因此我们已经证明了，在任何解释下的一个任何赋值满足这个给定的公式. 因此这个公式是逻辑有效的.

(c) $((\forall x_1)(\exists x_2)A_1^2(x_1, x_2)\rightarrow(\exists x_1)(\forall x_2)A_1^2(x_1, x_2))$ 不是逻辑有效的，这个的证明也许稍欠径直，因为我们必须做的是要去找一个解释，在此解释下这个给定的公式不是真的. 我们必须选取一域 D_I，一个关于谓词字母 A_1^2 的解释，和一个不满足此公式的赋值.

令 $D_I=\mathbf{Z}$，$\overline{A}_1^2(y, z)$指"$y<z$"，显然，现在不管是那一个赋值，闭公式$(\forall x_1)(\exists x_2)A_1^2(x_1, x_2)$在这解释下都是真的，而$(\exists x_1)(\forall x_2)A_1^2(x_1, x_2)$是假的，即每个赋值满足前者而不满足后者. 因此没有赋值能满足给定的公式. 因此它在这个解释下不是真的，从而它不是逻辑有效的.

(d) $A_1^1(x_1)$不是逻辑有效的. 如我们在前面已见到，这个公式不仅不逻辑有效，而且存在着某些解释，使得它既不真也不假.

一般地，为了证明逻辑有效，我们必须证明，在任何解释之下的任何赋值都要满足有关公式. 为了证明一个公式不逻辑有效，在实际构造一个解释，使得其中有一个不满足它的赋值时通常需要一些技巧.

练习：

14. 在例 3.5 的算术解释下，求满足和不满足下列各公式的赋值.

(a) $A_1^2(f_1^2(x_1, x_1), f_2^2(x_2, x_3))$.

(b) $(A_1^2(f_1^2(x_1, a_1), x_2) \to A_1^2(f_1^2(x_1, x_2), x_3))$.

(c) $\sim A_1^2(f_2^2(x_1, x_2), f_2^2(x_2, x_3))$.

(d) $(\forall x_1) A_1^2(f_2^2(x_1, x_2), x_3)$.

(e) $((\forall x_1) A_1^2(f_2^2(x_1, a_1), x_1) \to A_1^2(x_1, x_3))$.

15. 在习题 11 所描述的解释下，求满足和不满足下列各公式的赋值.

(a) $A_2^2(x_1, a_1)$.

(b) $A_2^2(f_1^2(x_1, x_2), x_1) \to A_2^2(a_1, f_1^2(x_1, x_2))$.

(c) $\sim A_2^2(x_1, f_1^2(x_1, f_1^2(x_1, x_2)))$.

(d) $(\forall x_1) A_2^2(f_1^2(x_1, x_2), x_3)$.

(e) $(\forall x_1) A_2^2(f_1^2(x_1, a_1), x_1) \to A_2^2(x_1, x_2)$.

16. 在解释 N 之下，下列闭公式中，那些是真的，那些是假的？

(a) $(\forall x_1) A_1^2(f_1^2(x_1, a_1), x_1)$.

(b) $(\forall x_1)(\forall x_2)(A_1^2(f_1^2(x_1, a_1), x_2) \to A_1^2(f_1^2(x_2, a_1), x_1))$.

(c) $(\forall x_1)(\forall x_2)(\exists x_3) A_1^2(f_1^2(x_1, x_2), x_3)$.

(d) $(\exists x_1) A_1^2(f_1^2(x_1, x_1), f_2^2(x_1, x_1))$.

17. 在习题 11 的解释下，下列闭公式，哪些真，哪些是假的？

(a) $(\forall x_1) A_2^2(f_1^2(a_1, x_1), a_1)$.

(b) $(\forall x_1)(\forall x_2)(\sim A_2^2(f_1^2(x_1, x_2), x_1))$.

(c) $(\forall x_1)(\forall x_2)(\forall x_3)(A_2^2(x_1, x_2) \to A_2^2(f_1^2(x_1, x_3), f_1^2(x_2, x_3)))$.

(d) $(\forall x_1)(\exists x_2) A_2^2(x_1, f_1^2(f_1^2(x_1, x_2), x_2))$.

18. 证明，在一般解释下，公式$(\mathscr{A} \to \mathscr{B})$是假的，当且仅当 $\mathscr{A}$ 是真的并且 $\mathscr{B}$ 是假的. [参见注记 3.25(d)]

19. 证明下列各公式逻辑有效.

(a) $((\exists x_1)(\forall x_2) A_1^2(x_1, x_2) \to (\forall x_2)(\exists x_1) A_1^2(x_1, x_2))$.

(b) $(\forall x_1)A_1^1(x_1)\to((\forall x_1)A_2^1(x_1)\to(\forall x_2)A_1^1(x_2))$.

(c) $(\forall x_1)(\mathscr{A}\to\mathscr{B})\to((\forall x_1)\mathscr{A}\to(\forall x_1)\mathscr{B})$，对任何合式公式 $\mathscr{A}$ 和 $\mathscr{B}$.

(d) $(\forall x_1)(\forall x_2)\mathscr{A}\to(\forall x_2)(\forall x_1)\mathscr{A})$. 对任何合式公式 $\mathscr{A}$.

20. 给出一个不是闭的逻辑有效公式的例子.

21. 证明. 如果 t 是一个项，它对公式 $\mathscr{A}(x_i)$ 中的 x_i 是自由的，那么公式 $(\mathscr{A}(t)\to(\exists x_i)\mathscr{A}(x_i)$ 是一逻辑有效式.

22. 证明下列公式没有一个是逻辑有效的.

(a) $(\forall x_1)(\exists x_2)A_1^2(x_1, x_2)\to(\exists x_2)(\forall x_1)A_1^2(x_1, x_2)$.

(b) $(\forall x_1)(\forall x_2)(A_1^2(x_1, x_2)\to A_1^2(x_2, x_1))$.

(c) $(\forall x_1)((\sim A_1^1(x_1))\to(\sim A_1^1(a_1)))$.

(d) $((\forall x_1)A_1^2(x_1, x_1)\to(\exists x_2)(\forall x_1)A_1^2(x_1, x_2))$.

23. 令 $\mathscr{A}(x_i)$ 是 $\mathscr{L}$ 的一个公式，其中 x_i 自由出现，并且令 t 是一个项，它对 $\mathscr{A}(x_i)$ 中的 x_i 自由. 假设 v 是使得 $v(t)=v(x_i)$ 的赋值. 求证：v 满足 $\mathscr{A}(t)$ 当且仅当 v 满足 $\mathscr{A}(x_i)$.

第四章　形式的谓词演算

4.1　形式系统 $K_{\mathscr{L}}$

在第三章我们描述了将要用的形式语言，我们也看到了各种不同命题怎样能够翻译成恰当的一阶语言的公式的．如我们在第三章所作的那样，我们在本章中将考察一个固定的但未具体指定的一阶语言 $\mathscr{L}$，以便使我们的结果可以有一般性，而适用于所有的一阶语言，$\mathscr{L}$ 中的符号可以做多种不同的解释，但是目前我们将关心语言的纯形式方面，去考虑公式间的逻辑关系甚于去考虑依赖于特殊解释的性质．那架子和第二章中的相类似．我们定义一个形式的演绎系统，然后证明它具有那些应有的性质，即它是一致的，并且它的定理组成的类恰恰是逻辑有效的公式类．

固定一个一阶语言 $\mathscr{L}$，由下列公理组和演绎规则定义一个形式的演绎系统 $K_{\mathscr{L}}$．

公理

令 $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$ 是 $\mathscr{L}$ 中的任意公式．下面是 $K_{\mathscr{L}}$ 的公理：

$(K1)$　$(\mathscr{A}\to(\mathscr{B}\to\mathscr{A}))$.

$(K2)$　$(\mathscr{A}\to(\mathscr{B}\to\mathscr{C}))\to((\mathscr{A}\to\mathscr{B})\to(\mathscr{A}\to\mathscr{C}))$.

$(K3)$　$(\sim\mathscr{A}\to\sim\mathscr{B})\to(\mathscr{B}\to\mathscr{A})$.

$(K4)$　$((\forall x_i)\mathscr{A}\to\mathscr{A})$，如果 x_i 在 $\mathscr{A}$ 中不自由出现．

$(K5)$　$((\forall x_i)\mathscr{A}(x_i)\to\mathscr{A}(t))$，如 $\mathscr{A}(x_i)$ 是 $\mathscr{L}$ 的一个公式，t 是 $\mathscr{L}$ 的一个项，且在 $\mathscr{A}(x_i)$ 中对 x_i 自由．

$(K6)$　$(\forall x_i)(\mathscr{A}\to\mathscr{B})\to(\mathscr{A}\to(\forall x_i)\mathscr{B})$，如果 $\mathscr{A}$ 中不包含变元 x_i 的自由出现．

注意．这些是公理模式，每一个模式都有无限多个实例．

规则

(1) 分离规则，即从 $\mathscr{A}$ 和 $(\mathscr{A}\to\mathscr{B})$ 可演绎出 $\mathscr{B}$，其中 $\mathscr{A}$ 和 $\mathscr{B}$ 是 $\mathscr{L}$ 中任意公式.

(2) 概括规则，即从 $\mathscr{A}$ 可演绎出 $(\forall x_i)\mathscr{A}$，其中 $\mathscr{A}$ 是 $\mathscr{L}$ 中任意公式，x_i 是任意变元.

注记 4.1

(a) $K_{\mathscr{L}}$ 的公理模式和演绎规则包括了 L 的公理模式和规则. 补充的公理和规则，对于涉及量词性质的证明是必要的.

(b) 公理($K5$)是用它的最一般的形式叙述的. 在应用中，我们将经常遇到实例 $((\forall x_i)\mathscr{A}\to\mathscr{A})$，其中 x_i 可以是，也可以不是 $\mathscr{A}$ 的自由变元. 如果 x_i 在 $\mathscr{A}$ 中自由出现，我们可以把 $\mathscr{A}$ 写成 $\mathscr{A}(x_i)$，这时($K5$)给出 $((\forall x_i)\mathscr{A}(x_i)\to\mathscr{A}(x_i))$，因为 x_i 对 $\mathscr{A}(x_i)$ 中的 x_i 自由(注记 3.13). 如果 x_i 在 $\mathscr{A}$ 中不自由出现，那么($K4$)给我们以 $((\forall x_i)\mathscr{A}\to\mathscr{A})$.

定义 4.2

(见定义 2.2). 在 $K_{\mathscr{L}}$ 中的一个证明是指 $\mathscr{L}$ 的公式的这样一个序列 $\mathscr{A}_1, \cdots, \mathscr{A}_n$，使得对于每个 $i(1\leqslant i\leqslant n)$，或者 $\mathscr{A}_i$ 是 $K_{\mathscr{L}}$ 的一个公理，或者 $\mathscr{A}_i$ 由序列中位于 $\mathscr{A}_i$ 前面的公式通过分离成概括而得.

如果 Γ 是 $\mathscr{L}$ 中的一组合式公式，在 $K_{\mathscr{L}}$ 中从 Γ 的一个演绎是指一个和上面类似的序列，其中可以包括 Γ 的成员(参见定义 2.5)

一个公式 $\mathscr{A}$ 是 $K_{\mathscr{L}}$ 的一条定理，如果它是 $K_{\mathscr{L}}$ 中构成证明的某个序列的最后公式.

一个公式 $\mathscr{A}$ 是 $K_{\mathscr{L}}$ 中公式组 Γ 的一条后承，如果 $\mathscr{A}$ 是 $K_{\mathscr{L}}$ 中构成从 Γ 的一个演绎的某个序列的最后公式.

我们将用 $\underset{K_{\mathscr{L}}}{\vdash}\mathscr{A}$ 表示 $\mathscr{A}$ 是 $K_{\mathscr{L}}$ 的一条定理，$\Gamma\underset{K_{\mathscr{L}}}{\vdash}\mathscr{A}$ 表示"$\mathscr{A}$

是 $K_\mathscr{L}$ 中从 Γ 的一条推论”，其中 Γ 是 $K_\mathscr{L}$ 中的公式组.

为方便起见，我们将把 $K_\mathscr{L}$ 简写的 K 除非需要强调使用中的那个特殊语言.

命题 4.3

如果 $\mathscr{A}$ 是 $\mathscr{L}$ 的一个公式，且 $\mathscr{A}$ 是一重言式，那么 $\mathscr{A}$ 是 K 的一条定理.（我们将发现，与第二章的情况相反，它的逆命题是假的）.

证明 $\mathscr{L}$ 的一个公式是重言的，是指如果存在着 L 的一个公式 $\mathscr{A}_0$，使得 $\mathscr{A}$ 是由于通过把 L 的公式中的其命题变元代入 $\mathscr{L}$ 的公式而得到的，并且 $\mathscr{A}_0$ 是重言式. 现在令 $\mathscr{A}$ 是 $\mathscr{L}$ 的重言式，且令 $\mathscr{A}_0$ 是 L 中相应的公式. 那么 $\mathscr{A}_0$ 是一重言式，因而 $\vdash_L \mathscr{A}_0$. $\mathscr{A}_0$ 在 L 中的这个证明可以转换成 $\mathscr{A}$ 在 K 中的一个证明，只需简单地把命题变元处处替换成 $\mathscr{L}$ 的适当公式即可，我们所得到的确是 K 中的一个证明，这是因为公理模式($L1$)，($L2$)，($L3$)和分离规则是系统 L 和 K 所共有的. 所以我们有 $\vdash_K \mathscr{A}$，证毕.

▷有一命题类似于系统 L 的命题 2.14. 它说：K 中每个定理都是逻辑有效的. 证明沿着 2.14 证明的类似思路，开始我们必须证实 K 的公理都是逻辑有效的. ($K1$)，($K2$)和($K3$)的一切实例业已证明为逻辑有效(命题 3.29)，因为它们是重言式.

命题 4.4

公理模式($K4$)，($K5$)和($K6$)的一切实例是逻辑有效的.

证明 对 ($K4$) 来说，令 v 是在 $\mathscr{L}$ 的一个解释 I 上的赋值，令 v 满足 $(\forall x_i)\mathscr{A}$. 那么每个 i-等值于 v 的 v' 也满足 $\mathscr{A}$，特别地 v 也满足 $\mathscr{A}$. 因此在 I 上的每个赋值满足 $((\forall x_i)\mathscr{A}\to\mathscr{A})$，所以 $I\models((\forall x_i)\mathscr{A}\to\mathscr{A})$ 对每个 I 成立，即 $((\forall x_i)\mathscr{A}\to\mathscr{A})$ 是逻辑有效的.

对($K5$)来说，令 t 在公式 $\mathscr{A}(x_i)$ 中对 x_i 自由，并且令 v 是在

某个解释 I 上的一个赋值. 如果 v 不满足 $(\forall x_i)\mathscr{A}(x_i)$, 那么 v 满足 $((\forall x_i)\mathscr{A}(x_i)\to\mathscr{A}(t))$ (定义 3.20). 所以假设 v 满足 $(\forall x_i)\mathscr{A}(x_i)$. 我们来证明 v 也满足 $\mathscr{A}(t)$. 每个 i-等值于 v 的 w 满足 $\mathscr{A}(x_i)$. 特别地, v' 满足 $\mathscr{A}(x_i)$. 这里 $v'(x_i)=v(t)$ 且 $v'(x_k)=v(x_k)$ 对 $k\neq i$. 因此, 据命题 3.23, v 满足 $\mathscr{A}(t)$. 由此便知, I 上每个赋值 v 满足 $((\forall x_i)\mathscr{A}(x_i)\to\mathscr{A}(t))$, 所以 $I\models((\forall x_i)\mathscr{A}(x_i)\to\mathscr{A}(t))$, 对每个 I, 也就是说 $((\forall x_i)\mathscr{A}(x_i)\to\mathscr{A}(t))$ 是逻辑有效的.

对 $(K6)$ 来说, 令 $\mathscr{A}$ 和 $\mathscr{B}$ 是 $\mathscr{L}$ 的公式, 假设 x_i 在 $\mathscr{A}$ 中不自由出现. 令 v 为某个解释 I 上的一赋值. 证明遵循前面的模式. 假设 v 满足 $(\forall x_i)(\mathscr{A}\to\mathscr{B})$. 那么每个 i-等值于 v 的 w 满足 $(\mathscr{A}\to\mathscr{B})$. 因此每个 w, 或者不满足 $\mathscr{A}$ 或者满足 $\mathscr{B}$. 现在, 如果一个这样的 w 不满足 $\mathscr{A}$, 那么每个这样的 w 都不能满足 $\mathscr{A}$, 因为 x_i 在 $\mathscr{A}$ 并不自由出现(根据命题 3.33). v 是这样的一个 w, 所以我们有:

或者 v 不满足 $\mathscr{A}$,

或者每个 i-等值于 v 的 w 都满足 $\mathscr{B}$.

因此,

或者 v 不满足 $\mathscr{A}$ 或者 v 满足 $(\forall x_i)\mathscr{B}$.

也就是说, v 满足 $(\mathscr{A}\to(\forall x_i)\mathscr{B})$. 这样, 在 I 上的每个赋值满足 $(\forall x_i)(\mathscr{A}\to\mathscr{B})\to(\mathscr{A}\to(\forall x_i)\mathscr{B})$. 于是, 和前面一样 $(\forall x_i)(\mathscr{A}\to\mathscr{B})\to(\mathscr{A}\to(\forall x_i)\mathscr{B})$ 是逻辑有效的.

命题 4.5 (K 的可靠性定理)

对 $\mathscr{L}$ 中的任意合式公式, 如果 $\vdash_K\mathscr{A}$, 那么 $\mathscr{A}$ 是逻辑有效的.

证明 对 $\mathscr{A}$ 的证明步数进行归纳.

基础步骤: 如果 $\mathscr{A}$ 的证明只有一步, 那么 $\mathscr{A}$ 是 K 的一公理. 我们在上面业已证明过 K 的每条公理都是逻辑有效的.

归纳步骤: 假设 $\mathscr{A}$ 的证明有 n 步 $(n>1)$, 并且 K 中所有证

明步数小于 n 的定理都是逻辑有效的. $\mathscr{A}$ 出现在证明中,所以 $\mathscr{A}$ 或者是一公理,或者由证明中在前的公式通过分离或概括而得到. 如果 $\mathscr{A}$ 是一公理,那么如上它是逻辑有效的. 如果 $\mathscr{A}$ 由证明中在前的公式 $\mathscr{B}$ 和 $(\mathscr{B}\to\mathscr{A})$ 通过分离而得,此时 $\mathscr{B}$ 和 $(\mathscr{B}\to\mathscr{A})$ 有较短的证明,因而根据归纳假设是逻辑有效的,因此据注记 3.36(a), $\mathscr{A}$ 也逻辑有效. 如果 $\mathscr{A}$ 由在前的公式如 $\mathscr{C}$ 通过概括而得,因此 $\mathscr{C}$ 逻辑有效, $\mathscr{A}$ 是 $(\forall x_i)\mathscr{C}$ 也逻辑有效,据注记 3.36(b). 因此在各种情况下 $\mathscr{A}$ 是逻辑有效的.

通过归纳完成了证明.

系 4.6

K 是一致的(即, 没有合式公式 $\mathscr{A}$, 使得 $\mathscr{A}$ 和 $\sim\mathscr{A}$ 都是 K 的定理).

证明 假设 $\underset{K}{\vdash}\mathscr{A}$ 和 $\underset{K}{\vdash}(\sim\mathscr{A})$,对某个 $\mathscr{L}$ 的合式公式 $\mathscr{A}$. 那么 $\mathscr{A}$ 和 $(\sim\mathscr{A})$ 都逻辑有效, 据命题 4.5. 因而在任何解释下 $\mathscr{A}$ 和 $(\sim\mathscr{A})$ 都真.

这和注记 3.25(c)是矛盾的,所以 K 必定是一致的.

▷ 对于 K 的定理, 在 K 中寻找证明是困难的, 正如在 L 中的情形一样,我们又得寻找方法,以便有助于证明某些特殊公式是定理. 对 K 来说, 我们有一相应于演绎定理(命题 2.8) 的命题, 不过它要稍微复杂一点,让我们通过一个例子,来看一下为什么必然如此.

例 4.7

我们知道对于 K 的任何公式 $\mathscr{A}$,都有 $\mathscr{A}\underset{K}{\vdash}(\forall x_i)\mathscr{A}$ (通过概括规则可以直接得到). 但是, $\underset{K}{\vdash}(\mathscr{A}\to(\forall x_i)\mathscr{A})$ 并不是必然的.

要明白这点,让我们令 $\mathscr{A}$ 是 $A_1^1(x_i)$. 令 I 是域为整数集 Z 的解释,令 $\overline{A}_1^1$ 是谓词 "$=0$" .因此, $A_1^1(x_1)$ 可以直觉地解释为 "$x_1=$

0”. 在 I 中任何使得 $v(x_1)=0$ 的赋值将满足 $A_1^1(x_1)$. 但是任何1-等值于这样一个 v 的赋值(不同于 v 的)将不满足 $A_1^1(x_1)$. 所以在 I 中没有赋值满足 $(\forall x_1)A_1^1(x_1)$. 所以, 存在一种赋值, 它满足 $A_1^1(x_1)$ 但不满足 $(\forall x_1)A_1^1(x_1)$. 这个赋值不满足 $(A_1^1(x_1)\to(\forall x_1)A_1^1(x_1))$. 所以这个公式在 I 中不真. 因此它不是逻辑有效的, 从而据命题 4.5, 它也不是 K 的定理.

命题 4.8(K 的演绎定理)

令 $\mathscr{A}$ 和 $\mathscr{B}$ 是 $\mathscr{L}$ 中的任意公式, 并且令 Γ 是 $\mathscr{L}$ 的一组公式(可能是空集). 如果 $\Gamma\cup\{\mathscr{A}\}\underset{K}{\vdash}\mathscr{B}$, 并且演绎对涉及 $\mathscr{A}$ 中自由出现的变元没有使用过概括, 那么 $\Gamma\underset{K}{\vdash}(\mathscr{A}\to\mathscr{B})$.

证明 证明是对 n 进行归纳, n 是由 $\Gamma\cup\{\mathscr{A}\}$ 到 $\mathscr{B}$ 的演绎中所含公式的个数.

基础步骤: $n=1$. $\mathscr{B}$ 是公理, 或 $\mathscr{A}$, 或 Γ 中的一员. 我们可以按照证明 L 中的演绎定理时的完全同样的方式, 推演出 $\Gamma\underset{K}{\vdash}(\mathscr{A}\to\mathscr{B})$.

归纳步骤: 令 $n>1$. 假设: 如果 $\mathscr{F}$ 是 $\mathscr{L}$ 的一个公式, 它可由 $\Gamma\cup\{\mathscr{A}\}$ 演绎出, 于此没有对 $\mathscr{A}$ 中一自由变元应用过概括, 并且演绎中所含的公式少于 n 个, 那么 $\Gamma\underset{K}{\vdash}(\mathscr{A}\to\mathscr{F})$.

情形 1: $\mathscr{B}$ 由演绎中在前的合式公式通过分离而得, 此时证明也相同于 L.

情形 2: $\mathscr{B}$ 是公理, 或 $\mathscr{A}$, 或 Γ 中的一员. 证明也同 L 一样.

情形 3: $\mathscr{B}$ 由演绎中在前的公式通过概括而得. 即 $\mathscr{B}$ 是 $(\forall x_i)\mathscr{C}$, 而 $\mathscr{C}$ 是演绎中在前的公式. 因此 $\Gamma\cup\{\mathscr{A}\}\underset{K}{\vdash}\mathscr{C}$, 且此演绎含有的公式数目少于 n, 因为没有对 $\mathscr{A}$ 中的自由变元应用过概括. 所以 $\Gamma\underset{K}{\vdash}(\mathscr{A}\to\mathscr{C})$. x_i 也不能自由出现在 $\mathscr{A}$ 中, 因为在由

$\Gamma\cup\{\mathscr{A}\}$ 到 $\mathscr{B}$ 的演绎中，对它曾应用过概括．所以我们有由 Γ 到 $(\mathscr{A}\to\mathscr{B})$ 的一个演绎如下：

$$\left.\begin{array}{ll}(1) & \\ \vdots & \\ (k) & (\mathscr{A}\to\mathscr{C})\end{array}\right\}\text{由 }\Gamma\text{ 到}(\mathscr{A}\to\mathscr{C})\text{的演绎}$$

$$\begin{array}{lll}(k+1) & (\forall x_i)(\mathscr{A}\to\mathscr{C}) & (k),\text{概括}\\ (k+2) & (\forall x_i)(\mathscr{A}\to\mathscr{C})\to(\mathscr{A}\to(\forall x_i)\mathscr{C}) & (K6)\\ (k+3) & (\mathscr{A}\to(\forall x_i)\mathscr{C}) & (k+1),(k+2),\text{分离}\end{array}$$

所以 $\Gamma\underset{K}{\vdash}(\mathscr{A}\to\mathscr{B})$ 得证，完成了归纳证明．

▷ 这是 K 的演绎定理的最为有用的形式．有可能减弱关于使用概括的补充条件(见 Mendelson 的第 61 页)，但是我们并不需要这样做．将补充条件加强，就可得到如下常用的系．

系 4.9

如果 $\Gamma\cup\{\mathscr{A}\}\underset{K}{\vdash}\mathscr{B}$，且 $\mathscr{A}$ 是一闭公式，那么 $\Gamma\underset{K}{\vdash}(\mathscr{A}\to\mathscr{B})$．

尽管 K 的演绎定理的形式在表面上略欠一般，我们仍能恰如在 L 中那样，有益地用它去证明某些公式是定理．

系 4.10

对 $\mathscr{L}$ 的任意公式 $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$,

$$\{(\mathscr{A}\to\mathscr{B}),\ (\mathscr{B}\to\mathscr{C})\}\underset{K}{\vdash}(\mathscr{A}\to\mathscr{C}).$$

证明．它完全等同于系 2.10 的证明．

▷ 注意，因而 HS 规则，如在 L 那样，可以合法地用于 K．恰如在 L 一样，K 的演绎定理也有一逆命题．

命题 4.11

假设 $\mathscr{A}$, $\mathscr{B}$ 是 $\mathscr{L}$ 的公式，Γ 是 $\mathscr{L}$ 的公式组，且 $\Gamma\underset{K}{\vdash}(\mathscr{A}\to\mathscr{B})$，那么 $\Gamma\cup\{\mathscr{A}\}\underset{K}{\vdash}\mathscr{B}$．

证明　完全等同于命题 2.9 的证明．

例 4.12

如果 x_i 不在 $\mathscr{A}$ 中自由出现，那么

$$\vdash_K ((\mathscr{A}\to(\forall x_i)\mathscr{B})\to(\forall x_i)(\mathscr{A}\to\mathscr{B})$$

我们写出演绎.

(1)	$(\mathscr{A}\to(\forall x_i)\mathscr{B})$	假设
(2)	$(\forall x_i)\mathscr{B}\to\mathscr{B}$	$(K4)$或$(K5)$
(3)	$(\mathscr{A}\to\mathscr{B})$	(1), (2) HS
(4)	$(\forall x_i)(\mathscr{A}\to\mathscr{B})$	(3), 概括

所以我们有

$$(\mathscr{A}\to(\forall x_i)\mathscr{B})\vdash_K(\forall x_i)(\mathscr{A}\to\mathscr{B}).$$

现在在演绎中用到了概括，但是仅仅用于变元 x_i，它在 $(\mathscr{A}\to(\forall x_i)\mathscr{B})$ 中不是自由出现的. 因此我们能够使用演绎定理，得到

$$\vdash_K((\mathscr{A}\to(\forall x_i)\mathscr{B})\to(\forall x_i)(\mathscr{A}\to\mathscr{B})).$$

证毕.

例 4.13

对 $\mathscr{L}$ 中任意合式公式 $\mathscr{A}$, $\mathscr{B}$.

$$\vdash_K((\forall x_i)(\mathscr{A}\to\mathscr{B})\to((\exists x_i)\mathscr{A}\to(\exists x_i)\mathscr{B})).$$

我们再写出一个演绎，在这个演绎中的第二步，初看并不是显然的，但是在结束时我们将会明白引入它的理由.

(1)	$(\forall x_i)(\mathscr{A}\to\mathscr{B})$	假设
(2)	$(\forall x_i)(\sim\mathscr{B})$	假设
(3)	$(\forall x_i)(\mathscr{A}\to\mathscr{B})\to(\mathscr{A}\to\mathscr{B})$	$(K4)$或$(K5)$
(4)	$(\mathscr{A}\to\mathscr{B})$	(1), (3)分离
(5)	$(\mathscr{A}\to\mathscr{B})\to(\sim\mathscr{B}\to\sim\mathscr{A})$	重言式
(6)	$(\sim\mathscr{B}\to\sim\mathscr{A})$	(4), (5)分离
(7)	$((\forall x_i)(\sim\mathscr{B})\to(\sim\mathscr{B}))$	$(K4)$或$(K5)$
(8)	$(\sim\mathscr{B})$	(2), (7)分离

(9) $(\sim\mathscr{A})$ (6), (8)分离

(10) $(\forall x_i)(\sim\mathscr{A})$ (9), 概括

这证明了

$$\{(\forall x_i)(\mathscr{A}\to\mathscr{B}),\ (\forall x_i)(\sim\mathscr{B})\}\vdash_K(\forall x_i)(\sim\mathscr{A}).$$

据演绎定理,我们得

$$(\forall x_i)(\mathscr{A}\to\mathscr{B})\vdash_K((\forall x_i)(\sim\mathscr{B})\to(\forall x_i)(\sim\mathscr{A})),$$

因为 x_i 在$(\forall x_i)(\sim\mathscr{B})$不自由出现.现在我们知道

$$\vdash_K((\forall x_i)(\sim\mathscr{B})\to(\forall x_i)(\sim\mathscr{A}))$$
$$\to(\sim(\forall x_i)(\sim\mathscr{A})\to\sim(\forall x_i)(\sim\mathscr{B}))$$

所以,用分离规则,就有

$$(\forall x_i)(\mathscr{A}\to\mathscr{B})\vdash_K(\sim(\forall x_i)(\sim\mathscr{A})\to\sim(\forall x_i)(\sim\mathscr{B}))$$

即 $$(\forall x_i)(\mathscr{A}\to\mathscr{B})\vdash_K((\exists x_i)\mathscr{A}\to(\exists x_i)\mathscr{B}).$$

再次使用演绎定理,终于得到

$$\vdash((\forall x_i)(\mathscr{A}\to\mathscr{B})\to((\exists x_i)\mathscr{A}\to(\exists x_i)\mathscr{B})),$$

因为 x_i 在$(\forall x_i)(\mathscr{A}\to\mathscr{B})$中不自由出现.

练习

1. 写出下面公式在 $K_\mathscr{L}$ 中的一个证明.

$$(\forall x_i)(A_1^1(x_1)\to A_1^1(x_1)).$$

2. 证明下列为 $K_\mathscr{L}$ 中的定理.

(a) $(\exists x_i)(\mathscr{A}\to\mathscr{B})\to((\forall x_i)\mathscr{A}\to\mathscr{B})$,

(b) $((\exists x_i)\mathscr{A}\to\mathscr{B})\to(\forall x_i)(\mathscr{A}\to\mathscr{B})$, 假定 x_i 在 $\mathscr{B}$ 中不自由出现

(c) $(\sim(\forall x_i)\mathscr{A}\to(\exists x_i)\sim\mathscr{A})$.

3. (a)下面的推演有什么问题?

(1) $(\exists x_2)A_1^2(x_1, x_2)$ 假设

(2) $(\forall x_1)(\exists x_2)A_1^2(x_1, x_2)$ (1), 概括

(3) $(\forall x_1)(\exists x_2)A_1^2(x_1, x_2)\to(\exists x_2)A_1^2(x_2, x_2)$ (K5)

(4) $(\exists x_2)A_1^2(x_2, x_2)$ (2), (3) 分离

所以, $(\exists x_2)A_1^2(x_1, x_2)\underset{K}{\vdash}(\exists x_2)A_1^2(x_2, x_2)$, 因此根据演绎定理

$$\underset{K}{\vdash}(\exists x_2)A_1^2(x_1, x_2)\to(\exists x_2)A_1^2(x_2, x_2)$$

(b) 通过寻找一个适当的解释去证明, 公式 $((\exists x_2)A_1^2(x_1, x_2)\to(\exists x_2)A_1^2(x_2, x_2)$ 不是逻辑有效的, 因此它不是 K 的一条定理.

4.2 等值, 代入

注记 4.14

为方便起见, 我们引进联结词 $\leftrightarrow$ 作为我们语言中的被定义符号. 对 $\mathscr{L}$ 中的公式 $\mathscr{A}$ 和 $\mathscr{B}$, $(\mathscr{A}\leftrightarrow\mathscr{B})$ 表示 $\sim((\mathscr{A}\to\mathscr{B})\to\sim(\mathscr{B}\to\mathscr{A}))$. 再次注意, $(\mathscr{A}\leftrightarrow\mathscr{B})$ 不是 $\mathscr{L}$ 中的公式, 我们只是把它作为一个特殊公式的方便的缩写加以使用.

命题 4.15

对 $\mathscr{L}$ 中的任意公式 $\mathscr{A}$ 和 $\mathscr{B}$, $\underset{K}{\vdash}(\mathscr{A}\leftrightarrow\mathscr{B})$, 当且仅当 $\underset{K}{\vdash}(\mathscr{A}\to\mathscr{B})$ 并且 $\underset{K}{\vdash}(\mathscr{B}\to\mathscr{A})$.

证明 首先假设 $\underset{K}{\vdash}(\mathscr{A}\leftrightarrow\mathscr{B})$, 即 $\underset{K}{\vdash}\sim((\mathscr{A}\to\mathscr{B})\to\sim(\mathscr{B}\to\mathscr{A}))$. 现在, 公式 $(\sim((\mathscr{A}\to\mathscr{B})\to\sim(\mathscr{B}\to\mathscr{A}))\to(\mathscr{A}\to\mathscr{B}))$ 和 $(\sim((\mathscr{A}\to\mathscr{B})\to\sim(\mathscr{B}\to\mathscr{A})\to(\mathscr{B}\to\mathscr{A}))$ 都是重言式(验证留给读者), 所以据命题 4.3, 它们是 K 的定理. 因此, 通过分离, 我们就有

$$\underset{K}{\vdash}(\mathscr{A}\to\mathscr{B}) \text{ 和 } \underset{K}{\vdash}(\mathscr{B}\to\mathscr{A})$$

如所要求.

现在假设 $\underset{K}{\vdash}(\mathscr{A}\to\mathscr{B})$ 和 $\underset{K}{\vdash}(\mathscr{B}\to\mathscr{A})$. 我们必须证明 $\underset{K}{\vdash}\sim$

$((\mathscr{A}\to\mathscr{B})\to\sim(\mathscr{B}\to\mathscr{A}))$. 为此只需证明公式

$$(\mathscr{A}\to\mathscr{B})\to((\mathscr{B}\to\mathscr{A})\to\sim((\mathscr{A}\to\mathscr{B})\to\sim(\mathscr{B}\to\mathscr{A})))$$

是重言式就可以了,这一点通过构造一个真值表是容易做到的.

定义 4.16

如果 $\mathscr{A}$ 和 $\mathscr{B}$ 是 $\mathscr{L}$ 中的公式,并且 $\vdash_K(\mathscr{A}\leftrightarrow\mathscr{B})$,我们就说 $\mathscr{A}$ 和 $\mathscr{B}$ 在证明上是等价的.

系 4.17

对 $\mathscr{L}$ 的任意公式 $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$, 如果 $\mathscr{A}$ 和 $\mathscr{B}$ 是证明上等价的,并且 $\mathscr{B}$ 和 $\mathscr{C}$ 是证明上等价的,那么 $\mathscr{A}$ 和 $\mathscr{C}$ 也是证明上等价的.

证明 令 $\vdash_K(\mathscr{A}\leftrightarrow\mathscr{B})$, $\vdash_K(\mathscr{B}\leftrightarrow\mathscr{C})$. 那么 $\vdash_K(\mathscr{A}\to\mathscr{B})$ 和 $\vdash_K(\mathscr{B}\to\mathscr{C})$,所以据三段论,我们有 $\vdash_K(\mathscr{A}\to\mathscr{C})$.

同样也有 $\vdash_K(\mathscr{B}\to\mathscr{A})$, $\vdash_K\mathscr{C}\to\mathscr{B}$, 再次据三段论, 我们有 $\vdash_K(\mathscr{C}\to\mathscr{A})$. 因此据命题 4.15, $\vdash_K(\mathscr{A}\leftrightarrow\mathscr{C})$.

▷ 这最后一个命题, 当我们需要证明两个公式证明上等价时,将会派用场,我们只需证明两个蕴涵式都是定理即可. 在 K 的下一部分的描述中,我们就要求去应用它,在那里我们将研究怎样把部分的公式代入和怎样把变元代入. 我们在第一章中, 曾以非形式的方式这样做过. 当然由于变元的出现把这里的事情搞复杂了,以致有些证明冗长起来. 但是以后将要用到它的结果,因此它构成我们讲解的一个必要部分.

我们从考察变元怎样可以代入开始. 公式 $(\forall x_1)A_1^1(x_1)$ 将被解释(直觉地)成"对于所有 x, $\overline{A}_1^1(x)$ 成立". 同样地,公式 $(\forall x_2)A_1^1(x_2)$ 将被直觉地解释成"对于所有 x, $\overline{A}_1^1(x)$ 成立". 因此, 看来在公式中出现的实际的变元(在这种情况下)并不影响解释.所以,在形式系统 K 中,这两个公式,在某种意义下应该是等

价的．这一点将在下一命题中予以精确化．

如前，令 $\mathscr{A}(x_i)$ 表示 $\mathscr{L}$ 的一个公式，其中 x_i 自由出现(可能多于一次)．这时对于任何变元 x_j，我们用 $\mathscr{A}(x_j)$ 表示对 $\mathscr{A}(x_i)$ 中的 x_i 的每个自由出现都用 x_j 代入后得到的公式．

命题 4.18

如果 x_i 在 $\mathscr{A}(x_i)$ 中自由，且 x_j 是一个不在 $\mathscr{A}(x_i)$ 中自由或约束出现的变元，那么

$$\vdash_K ((\forall x_i)\mathscr{A}(x_i) \leftrightarrow (\forall x_j)\mathscr{A}(x_j)).$$

证明．首先看到，在所特定条件下，x_i 在 $\mathscr{A}(x_j)$ 中对 x_j 自由，x_j 在 $\mathscr{A}(x_i)$ 中对 x_i 自由．我们需要两个演绎，去证明两个蕴涵都是 K 的定理．

(1)	$(\forall x_i)\mathscr{A}(x_i)$	假设
(2)	$((\forall x_i)\mathscr{A}(x_i) \rightarrow \mathscr{A}(\overline{x_j}))$	$(K5)$
(3)	$\mathscr{A}(x_j)$	(1), (2), 分离
(4)	$(\forall x_j)\mathscr{A}(x_j)$	(3), 概括

$\therefore \quad (\forall x_i)\mathscr{A}(x_i) \vdash_K (\forall x_j)\mathscr{A}(x_j)$.

因此，根据演绎定理，

$$\vdash_K ((\forall x_i)\mathscr{A}(x_i) \rightarrow (\forall x_j)\mathscr{A}(x_j)),$$

由于 x_j 不在 $(\forall x_i)\mathscr{A}(x_i)$ 中自由．用完全相同的方法我们证明

$$\vdash_K ((\forall x_j)\mathscr{A}(x_j) \rightarrow (\forall x_i)\mathscr{A}(x_i)).$$

因此，根据命题 4.15 我们有

$$\vdash_K ((\forall x_i)\mathscr{A}(x_i) \leftrightarrow (\forall x_j)\mathscr{A}(x_j)).$$

▷ 这个命题表明，我们可以替换一个特殊的约束变元而得到一个和原公式是证明上等价的公式，假如我们适当地选择一个新的变元．这个做法的用处在以后会看得清楚．

命题 4.19

令 $\mathscr{A}$ 是 $\mathscr{L}$ 的一个公式，它的自由变元是 $y_1, \cdots, y_n$. 那么 $\underset{K}{\vdash}\mathscr{A}$, 当且仅当, $\underset{K}{\vdash}(\forall y_1)\cdots(\forall y_n)\mathscr{A}$.

证明 首先假设 $\underset{K}{\vdash}\mathscr{A}$, 我们通过对 $\mathscr{A}$ 中自由变元的个数 n 进行归纳着手证明.

基础步骤: $n=1$ (不带自由变元的公式的情况是平凡的). $\mathscr{A}$ 有一个自由变元 y_1. 如果 $\underset{K}{\vdash}\mathscr{A}(y_1)$, 那么 $\underset{K}{\vdash}(\forall y_1)A(y_1)$, 用一次概括即可.

归纳步骤: 令 $n>1$, 且设对 $\mathscr{L}$ 中每个含 $n-1$ 个自由变元的公式结果是真的. 考虑公式 $(\forall y_n)\mathscr{A}$. 它有 $n-1$ 个自由变元. 我们有 $\underset{K}{\vdash}\mathscr{A}$, 所以通过概括有 $\underset{K}{\vdash}(\forall y_n)\mathscr{A}$, 再据归纳假设就有 $\underset{K}{\vdash}(\forall y_1)\cdots(\forall y_{n-1})(\forall y_n)\mathscr{A}$.

逆命题, 假设 $\underset{K}{\vdash}(\forall y_1)\cdots(\forall y_n)\mathscr{A}$. 我们证明 $\underset{K}{\vdash}\mathscr{A}$, 只需应用公理 $(K5)$, 对 n 作类似的归纳即可.

定义 4.20

如果 $\mathscr{A}$ 是 $\mathscr{L}$ 的一个只包含自由变元 $y_1, \cdots, y_n$ 的公式, 那么合式 $(\forall y_1)\cdots(\forall y_n)\mathscr{A}$ 称为 $\mathscr{A}$ 的全称闭式. $\mathscr{A}$ 的全称闭式通常用 $\mathscr{A}'$ 表示.

注记 4.21

上述命题说对于 $\mathscr{L}$ 的任意公式 $\mathscr{A}$, $\underset{K}{\vdash}\mathscr{A}$, 当且仅当 $\underset{K}{\vdash}\mathscr{A}'$. 我们应当仔细记住, $\mathscr{A}$ 和 $\mathscr{A}'$ 一般并非证明上等值, 不难看到 $\underset{K}{\vdash}(\mathscr{A}'\to\mathscr{A})$ 总是成立的, 可是在例 4.7 中我们已经看到, $(\mathscr{A}\to\mathscr{A}')$ 并不一定是 K 的定理.

命题 4.22

令 $\mathscr{A}$ 和 $\mathscr{B}$ 是 $\mathscr{L}$ 的公式, 并且假设 $\mathscr{B}_0$ 是由 $\mathscr{A}_0$ 通过对 $\mathscr{A}_0$

中 $\mathscr{A}$ 的一次或多次出现以 $\mathscr{B}$ 代入后所得. 那么

$$\underset{K}{\vdash}((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow(\mathscr{A}_0\leftrightarrow\mathscr{B}_0).$$

证明 通过对 $\mathscr{A}_0$ 的长度(在 $\mathscr{A}_0$ 中联结词和量词的数目)进行归纳.

基础步骤: 我们必然地假设, $\mathscr{A}_0$ 包含 $\mathscr{A}$ 为子公式, 因此当 $\mathscr{A}_0$ 就是 $\mathscr{A}$ 本身时, $\mathscr{A}_0$ 具有最少的联结词和量词. 在这种情况下, $\mathscr{B}_0$ 恰是 $\mathscr{B}$. 因此 $\underset{K}{\vdash}((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow(\mathscr{A}\leftrightarrow\mathscr{B}))$ 是上面注记 4.21 提及的一个一般结果的实例.

归纳步骤: 假设 $\mathscr{A}_0$ 包含 $\mathscr{A}$ 为一真子公式. 并设对那些比 $\mathscr{A}_0$ 短的且包含 $\mathscr{A}$ 为子公式的所有公式结果为真. 和在前面证明中一样, 有三种情形要考虑.

情形 1: $\mathscr{A}_0$ 是 $\sim\mathscr{C}_0$. 那么 $\mathscr{B}_0$ 比如说是 $\sim\mathscr{D}_0$, 其中 $\mathscr{D}_0$ 是在 $\mathscr{C}_0$ 中用 $\mathscr{B}$ 代入 $\mathscr{A}$ 后所得的公式. 现在 $\mathscr{C}_0$ 比 $\mathscr{A}_0$ 有较少的联结词和量词, 所以

$$\underset{K}{\vdash}((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow(\mathscr{C}_0\leftrightarrow\mathscr{D}_0)).$$

由于 $((\mathscr{C}_0\leftrightarrow\mathscr{D}_0)\rightarrow(\sim\mathscr{C}_0\leftrightarrow\sim\mathscr{D}_0))$ 是重言式, 它是 K 的定理, 据三段论(系 4.10), 我们有

$$\underset{K}{\vdash}((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow(\sim\mathscr{C}_0\leftrightarrow\sim\mathscr{D}_0)),$$

即

$$\underset{K}{\vdash}((\mathscr{A}\leftrightarrow\mathscr{B})\rightarrow(\mathscr{A}_0\leftrightarrow\mathscr{B})).$$

情形 2: $\mathscr{A}_0$ 是 $(\mathscr{C}\rightarrow\mathscr{D}_0)$. 那么 $\mathscr{B}_0$ 比如说是 $(\mathscr{E}_0\rightarrow\mathscr{F}_0)$. 其中 $\mathscr{E}_0$ 和 $\mathscr{F}_0$ 相应地是在 $\mathscr{C}_0$ 和 $\mathscr{D}_0$ 中以 $\mathscr{B}$ 代入 $\mathscr{A}$ 后所得的结果. 现在, $\mathscr{C}_0$ 和 $\mathscr{D}_0$ 的每一个都比 $\mathscr{A}_0$ 具有较少的联结词和量词, 所以

$$\underset{K}{\vdash}((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow(\mathscr{C}_0\leftrightarrow\mathscr{E}_0)).$$

和

$$\underset{K}{\vdash}((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow(\mathscr{D}_0\leftrightarrow\mathscr{F}_0)).$$

留作为习题去证, 从这些可以推得

$$\vdash_K ((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow((\mathscr{C}_0\rightarrow\mathscr{D}_0)\leftrightarrow(\mathscr{E}_0\rightarrow\mathscr{F}_0))),$$

即
$$\vdash_K ((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow(\mathscr{A}_0\leftrightarrow\mathscr{B}_0)).$$

情形 3：$\mathscr{A}_0$ 是 $(\forall x_i)\mathscr{C}_0$，那么 $\mathscr{B}_0$ 比如说是 $(\forall x_i)\mathscr{D}_0$，其中 $\mathscr{D}_0$ 是在 $\mathscr{C}_0$ 中以 $\mathscr{B}$ 代入 $\mathscr{A}$ 后所得的结果．现在 $\mathscr{C}_0$ 比 $\mathscr{A}_0$ 具有较少的联结词和量词，所以

$$\vdash_K ((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow(\mathscr{C}_0\leftrightarrow\mathscr{D}_0)).$$

因而，据概括我们有

$$\vdash_K (\forall x_i)((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow(\mathscr{C}_0\leftrightarrow\mathscr{D}_0)).$$

现在，x_i 在 $(\mathscr{A}\leftrightarrow\mathscr{B})'$ 中不自由出现，所以作为公理 $(K6)$ 的实例，我们有

$$\vdash_K ((\forall x_i)((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow(\mathscr{C}_0\leftrightarrow\mathscr{D}_0))$$
$$\rightarrow((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow(\forall x_i)(\mathscr{C}_0\leftrightarrow\mathscr{D}_0))).$$

因此，据分离规则有

$$\vdash_K ((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow(\forall x_i)(\mathscr{C}_0\leftrightarrow\mathscr{D}_0)),$$

这就得到了我们的结果

$$\vdash_K ((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow((\forall x_i)\mathscr{C}_0\leftrightarrow(\forall x_i)\mathscr{D}_0)),$$

即
$$\vdash_K ((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow(\mathscr{A}_0\leftrightarrow\mathscr{B}_0)),$$

通过应用下面的引理，其证明留作练习．

引理：如果 $\mathscr{A}$，$\mathscr{B}$ 是 $\mathscr{L}$ 的合式公式，那么

$$\vdash_K (\forall x_i)(\mathscr{A}\leftrightarrow\mathscr{B})\rightarrow((\forall x_i)\mathscr{A}\leftrightarrow(\forall x_i)\mathscr{B}).$$

这就完成了我们的归纳证明．

系 4.23

令 $\mathscr{A}$，$\mathscr{B}$，$\mathscr{A}_0$，$\mathscr{B}_0$ 如上面命题 4.22 一样，如果 $\vdash_K(\mathscr{A}\leftrightarrow\mathscr{B})$，那么 $\vdash_K(\mathscr{A}_0\leftrightarrow\mathscr{B}_0)$．

证明 假设 $\underset{K}{\vdash}(\mathscr{A}\leftrightarrow\mathscr{B})$. 那么根据命题 4.19 有 $\underset{K}{\vdash}(\mathscr{A}\leftrightarrow\mathscr{B})'$. 又据命题 4.22, 有 $\underset{K}{\vdash}((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow(\mathscr{A}_0\leftrightarrow\mathscr{B}_0))$. 因此, 据分离规则, 我们有 $\underset{K}{\vdash}(\mathscr{A}_0\leftrightarrow\mathscr{B}_0)$.

系 4.24

如果 x_j 在公式 $\mathscr{A}(x_i)$ 中不出现(不管自由或约束), 而公式 $\mathscr{B}_0$ 是从 $\mathscr{A}_0$ 通过用 $(\forall x_j)\mathscr{A}(x_j)$ 替换 $(\forall x_i)\mathscr{A}(x_i)$ 的一次或多次出现后所得的公式, 那么 $\underset{K}{\vdash}(\mathscr{A}_0\leftrightarrow\mathscr{B}_0)$.

证明 应用命题 4.18 和系 4.23 即可.

练习

4. 证明

$$\underset{K}{\vdash}((\forall x_i)(\mathscr{A}\rightarrow\mathscr{B})\rightarrow((\forall x_i)\mathscr{A}\rightarrow(\forall x_i)\mathscr{B})),$$

对任何合式公式 $\mathscr{A}$ 和 $\mathscr{B}$.

5. 证明. 公式 $\sim(\exists x_i)\mathscr{A}$ 和 $(\forall x_i)(\sim\mathscr{A})$ 在 K 中是证明上等价的, 其中 $\mathscr{A}$ 为 $\mathscr{L}$ 中任意公式.

6. 详细证明

(a) $(\forall x_1)(\forall x_2)A_1^2(x_1, x_2)\underset{K}{\vdash}(\forall x_2)(\forall x_3)A_1^2(x_2, x_3)$

(b) $(\forall x_1)(\forall x_2)A_1^2(x_1, x_2)\underset{K}{\vdash}(\forall x_1)A_1^2(x_1, x_1)$

7. 令 $\mathscr{A}(x_i)$ 是 $\mathscr{L}$ 中的公式, 其中 x_i 自由出现, 并且令 x_j 是一在 $\mathscr{A}(x_i)$ 不自由或约束出现的变元, 证明

$$\underset{K}{\vdash}((\exists x_j)\mathscr{A}(x_i)\leftrightarrow(\exists x_j)\mathscr{A}(x_j)).$$

4.3 前束范式

在第一章中, 已经引入了范式的思想, 并且讨论了合取范式和析取范式. 范式的一种用处是能揭露在原来的公式中并不显著

的，逻辑结构方面的关系．现在，我们已有可能来描述 $\mathscr{L}$ 中公式的一种范式，不过在以前的范式中，我们仅允许某些联结词按标准方式加以使用，而在这里我们所关心的则是量词的排列．

命题 4.25

令 $\mathscr{A}$ 和 $\mathscr{B}$ 是 $\mathscr{L}$ 的公式．

(i) 如果 x_i 在 $\mathscr{A}$ 中不自由出现，那么

$$\vdash_K ((\forall x_i)(\mathscr{A}\to\mathscr{B})\leftrightarrow(\mathscr{A}\to(\forall x_i)\mathscr{B})),$$

和

$$\vdash_K ((\exists x_i)(\mathscr{A}\to\mathscr{B})\leftrightarrow(\mathscr{A}\to(\exists x_i)\mathscr{B})).$$

(ii) 如果 x_i 在 $\mathscr{B}$ 中不自由出现，那么

$$\vdash_K ((\forall x_i)(\mathscr{A}\to\mathscr{B})\leftrightarrow((\exists x_i)\mathscr{A}\to\mathscr{B})),$$

和

$$\vdash_K ((\exists x_i)(\mathscr{A}\to\mathscr{B})\leftrightarrow((\forall x_i)\mathscr{A}\to\mathscr{B})).$$

证明 在 K 中要求作八个证明．其中一个是显然的，因为涉及的公式是公理 ($K6$) 的实例，一个在例 4.12 中已经给出，另一个可从例 4.13 容易推得．其余的要求作类似的证明，只要重复使用演绎定理即可．它们都留作练习．

例 4.26

证明公式

$$(\forall x_1)A_1^1(x_1)\to(\forall x_2)(\exists x_3)A_1^2(x_2, x_3)$$

是证明上等价于公式

$$(\exists x_1)(\forall x_2)(\exists x_3)(A_1^1(x_1)\to A_1^2(x_2, x_3)).$$

我们写出一公式序列，其中每个公式证明上等价于下一个，每一步使用了命题 4.25 的一部分．

$$(\forall x_1)A_1^1(x_1)\to(\forall x_2)(\exists x_3)A_1^2(x_2, x_3),$$

$$(\exists x_1)A_1^1(x_1)\to(\forall x_2)(\exists x_3)A_1^2(x_2, x_3),$$

$$(\exists x_1)(\forall x_2)(A_1^1(x_1)\to(\exists x_3)A_1^2(x_2, x_3)),$$

$$(\exists x_1)(\forall x_2)(\exists x_3)(A_1^1(x_1)\to A_1^2(x_2, x_3)).$$

▷$\mathscr{L}$的公式可以是很复杂的，其中量词之间的关系直觉上很难看清，特别当它们分割开时．我们能使用上面关于代入和等值方面的结果去证明，每一公式在证明上都等价于一个所有量词都出现在始端的公式．

定义 4.27

$\mathscr{L}$的一个公式$\mathscr{A}$称为前束范式，如果它形如

$$(Q_1x_{i1})(Q_2x_{i2})\cdots(Q_kx_{ik})\mathscr{D},$$

其中$\mathscr{D}$是不带量词的公式，每个Q_j是$\forall$或$\exists$．（一个不带量词的公式，可以看作前束范式的平凡情况）．

命题 4.28

对$\mathscr{L}$的任意合式公式$\mathscr{A}$，总存在前束范式$\mathscr{B}$并在证明上等价于$\mathscr{A}$．

证明 根据 4.18，我们能够改变一切$\mathscr{A}$中的约束变元，使它们都不同于$\mathscr{A}$中的自由变元（但自由变元仍然照旧），这样得到一个公式$\mathscr{A}_1$，当然$\underset{K}{\vdash}(\mathscr{A}_1\leftrightarrow\mathscr{A})$．现在我们对$\mathscr{A}_1$的长度（联结词和量词的数目）进行归纳．

基础步骤：$\mathscr{A}_1$是一个原子公式．这里没有什么需要证明的，因为$\mathscr{A}_1$已经显然是前束范式．

归纳步骤：令$\mathscr{A}_1$不是原子公式，并且假设每个比$\mathscr{A}_1$较短的公式都在证明上等价于一个前束范式$\mathscr{C}_1$．有 3 种情况．

情形 1：$\mathscr{A}_1$是$\sim\mathscr{C}$．那么$\mathscr{C}$比$\mathscr{A}_1$较短，所以有一前束范式$\mathscr{C}_1$，使得$\underset{K}{\vdash}(\mathscr{C}_1\leftrightarrow\mathscr{C})$，由此推得$\underset{K}{\vdash}(\mathscr{A}_1\leftrightarrow(\sim\mathscr{C}_1))$

即 $$\underset{K}{\vdash}(\mathscr{A}_1\leftrightarrow(Q_1x_{i1})\cdots(Q_kx_{ik})\mathscr{D}).$$

所以$\underset{K}{\vdash}(\mathscr{A}_1\leftrightarrow(Q_1^*x_{i1})\cdots(Q_k^*x_{ik})(\sim\mathscr{D}))$，其中如果$Q_j$是$\forall$，那么$Q_j^*$是$\exists$，如果$Q_j$是$\exists$，那么$Q_j^*$是$\forall$，对$1\leqslant j\leqslant k$．令$\mathscr{B}$是公式$(Q_1^*x_{i1})\cdots(Q_k^*x_{ik})(\sim\mathscr{D})$．那么$\underset{K}{\vdash}(\mathscr{A}\leftrightarrow\mathscr{B})$，而$\mathscr{B}$是前束范式．

情形 2: $\mathscr{A}_1$ 是 $(\mathscr{C}\to\mathscr{D})$. 那么 $\mathscr{C}$ 和 $\mathscr{D}$ 比 $\mathscr{A}_1$ 长度较短，所以有前束范式 $\mathscr{C}_1$ 和 $\mathscr{D}_1$，使得

$$\vdash_K(\mathscr{C}_1\leftrightarrow\mathscr{C}) \text{ 和 } \vdash_K(\mathscr{D}_1\leftrightarrow\mathscr{D}).$$

根据系 4.23，那么

$$\vdash_K(\mathscr{C}\to\mathscr{D})\leftrightarrow(\mathscr{C}_1\to\mathscr{D}).$$

因此，据同一系和系 4.17

$$\vdash_K(\mathscr{C}\to\mathscr{D})\leftrightarrow(\mathscr{C}_1\to\mathscr{D}_1),$$

即

$$\vdash_K(\mathscr{A}_1\leftrightarrow(\mathscr{C}_1\to\mathscr{D}_1)).$$

因此 $\vdash_K(\mathscr{A}\leftrightarrow(\mathscr{C}_1\to\mathscr{D}_1))$，据系 4.17. 现在 $(\mathscr{C}_1\to\mathscr{D}_1)$ 具有形式

$$((Q_1x_{i1})\cdots(Q_kx_{ik})\mathscr{C}_2\to(R_1x_{j1})\cdots(R_lx_{jl})\mathscr{D}_2).$$

其中 $\mathscr{C}_2$ 和 $\mathscr{D}_2$ 不包含量词，Q 和 R 不是 $\forall$ 就是 $\exists$. 现在我们重复地应用命题 4.25，把量词都移置始端，如果必要的话 $\forall$ 和 $\exists$ 可改变. 由于 $x_{i1}, \cdots, x_{ik}, x_{j1}, \cdots, x_{jl}$ 都是不相同的，并且与 $\mathscr{C}_2$ 和 $\mathscr{D}_2$ 中出现的任何自由变元也不相同，所以我们可以这样做. 我们得到

$$\vdash_K((\mathscr{C}_1\to\mathscr{D}_1)\leftrightarrow(Q_1^*x_{i1})\cdots(Q_k^*x_{ik})(R_1x_{j1})\cdots(R_lx_{jl})(\mathscr{C}_2\to\mathscr{D}_2)).$$

这最后部分就是前束范式，它就是要求的 $\mathscr{B}$.

情形 3: $\mathscr{A}_1$ 是 $(\forall x_i)\mathscr{C}$. 那么 $\mathscr{C}$ 的长度比 $\mathscr{A}_1$ 短，而有一前束范式证明上等价于 $\mathscr{C}$，比方说

$$\vdash_K(\mathscr{C}\leftrightarrow(Q_1x_{i1})\cdots(Q_kx_{ik})\mathscr{D}).$$

因而，据概括有

$$\vdash_K(\forall x_i)(\mathscr{C}\leftrightarrow(Q_1x_{i1})\cdots(Q_kx_{ik})\mathscr{D}).$$

由此得到 $\vdash_K((\forall x_i)\mathscr{C}\leftrightarrow(\forall x_i)(Q_1x_{i1})\cdots(Q_kx_{ik})\mathscr{D})$，如在命题 4.22 的证明. 这公式 $(\forall x_i)(Q_1x_{i1})\cdots(Q_kx_{ik})\mathscr{D}$ 从而就是所要求的 $\mathscr{B}$.

归纳证明完成.

例 4.29

(a) 求一前束范式,证明上等价于公式

$$A_1^1(x_1)\to(\forall x_2)A_1^2(x_1,\ x_2)$$

这个例子,相当于上面归纳证明中的情况 2. 首先我们看到 x_2 是唯一的约束变元,而且在任何地方都没自由出现,因此我们无需改变任何变元. 我们直接应用命题 4.25(i),就可以看到

$$(\forall x_2)(A_1^1(x_1)\to A_1^2(x_1,\ x_2))$$

证明上等价于给定的公式,并且它是前束范式.

(b) 求一前束范式,证明上等价于公式

$$(((\forall x_1)A_1^2(x_1,\ x_2)\to\sim(\exists x_2)(A_1^1(x_2))$$
$$\to(\forall x_1)(\forall x_2)A_2^2(x_1,\ x_2)).$$

我们还是沿用命题 4.28 证明中的方法. 首先改变约束变元. 除了要求改变后的约束变元须互异并和自由变元不同外,我们怎样做都没有关系. 我们得到(比方说)

$$(((\forall x_1)A_1^2(x_1,\ x_2)\to\sim(\exists x_3)A_1^1(x_3))$$
$$\to(\forall x_4)(\forall x_5)A_2^2(x_4,\ x_5)),$$

它是证明上等价于给定的公式的. 现在我们按照上面归纳证明中不同情形分几步进行. 首先处理前面直接放置~的量词(情况 1),得到

$$(((\forall x_1)A_1^2(x_1,\ x_2)\to(\forall x_3)\sim A_1^1(x_3))$$
$$\to(\forall x_4)(\forall x_5)A_2^2(x_4,\ x_5)).$$

现在考察形如 $(\mathscr{B}\to\mathscr{C})$ 的部分(情况 2). 利用命题 4.25 的各个部分,我们得到一串公式,其中每个都证明上等价于下一个,

$$((\forall x_3)((\forall x_1)A_1^2(x_1,\ x_2)\to\sim A_1^1(x_3))$$
$$\to(\forall x_4)(\forall x_5)A_2^2(x_4,\ x_5)),$$
$$((\forall x_3)(\exists x_1)(A_1^2(x_1,\ x_2)\to\sim A_1^1(x_3))$$
$$\to(\forall x_4)(\forall x_5)A_2^2(x_4,\ x_5)),$$

$$(\exists x_3)(\forall x_1)((A_1^2(x_1, x_2)\to\sim A_1^1(x_3))$$
$$\to(\forall x_4)(\forall x_5)A_2^2(x_4, x_5)),$$
$$(\exists x_3)(\forall x_1)(\forall x_4)(\forall x_5)((A_1^2(x_1, x_2)$$
$$\to\sim A_1^1(x_3))\to A_2^2(x_4, x_5)).$$

最后一个是前束范式，并且证明上等价于给定的公式.

▷ 注意这个程序并不导致唯一解答. 移到公式始端的量词的次序是任意的. 例如公式

$$(\forall x_4)(\forall x_5)(\forall x_1)(\exists x_3)((A_1^2(x_1, x_2)$$
$$\to\sim A_1^1(x_3))\to A_2^2(x_4, x_5))$$

也可以是上例的解答，但是前束范式始端量词的次序是有关系的，只是在某些特殊情况下次序才可改变，而且这时只能按特殊的方式，如果所得公式须证明上等价于原来的公式的话.

前束范式导致一个量度 K 中公式复杂性的方法. 对一个前束范式来说，初看去，似乎始端量词愈多，它的解释就愈复杂. 但是考察两个公式

$$(\forall x_1)(\forall x_2)(\forall x_3)(\forall x_4)A_1^2(f_1^2(x_1, x_2), f_1^2(x_3, x_4)),$$
$$(\forall x_1)(\exists x_2)(\forall x_3)(\exists x_4)A_1^2(f_1^2(x_1, x_2), f_1^2(x_3, x_4)).$$

我们可以看到，前者较易解释得多. 例如，考虑第三章中的算术解释，这些合式公式相应地解释是

对每个 $x, y, z, t\in D_N$, $x+y=z+t$,

和　对每个 $x\in D_N$, 会有一个 $y\in D_N$, 使得对于每个 $z\in D_N$, 有一个 $t\in D_N$, 使得 $x+y=z+t$

第二个是比较复杂得多的句子，很难一眼看出它是真还是假. 这个复杂性是由交叉量词提出的，复杂性的量度是交叉的数目.

定义 4.30

(i) 令 $n>0$, 一个前束范式称为一个 Π_n 式，如果它以全称量词开始，并且有 $n-1$ 次量词的交叉.

(ii) 令 $n>0$, 一个前束范式称为一个 Σ_n 式，如果它以存在量

词开始，并且有 $n-1$ 次量词的交叉.

我们将不使用这个定义，但是它们在关于这方面的研究中是重要的.

例 4.31

(a) $(\forall x_1)(\forall x_2)(\exists x_3)A_1^3(x_1, x_2, x_3)$ 是 Π_2 式.

(b) $(\forall x_1)(A_1^1(x_1)\to A_2^1(x_2))$ 是 Π_1 式.

(c) $(\exists x_1)(\forall x_2)(\exists x_3)(\exists x_4)(A_1^2(x_1, x_2)\to A_1^2(x_3, x_4))$ 是 Σ_3 式.

练习

8. 对下列每个公式，求与之证明上等价的前束范式.

(a) $(\forall x_1)A_1^1(x_1)\to(\forall x_2)A_1^2(x_1, x_2)$

(b) $(\forall x_1)(A_1^2(x_1, x_2)\to(\forall x_2)A_1^2(x_1, x_2))$.

(c) $(\forall x_1)(A_1^1(x_1)\to A_1^2(x_1, x_2))\to((\exists x_2)A_1^1(x_2)\to(\exists x_3)A_1^2(x_2, x_3))$.

(d) $(\exists x_2)A_1^2(x_1, x_2)\to(A_1^1(x_1)\to\sim(\exists x_3)A_1^2(x_1, x_3))$.

9. 令 $\mathscr{A}(x_1)$ 是 x_2 不出现的公式，且令 $\mathscr{B}(x_2)$ 是 x_1 不出现的公式，证明公式

$$\sim((\exists x_1)\mathscr{A}(x_1)\to(\exists x_2)\mathscr{B}(x_2))$$

是证明上等价于 Π_2 和 Σ_2 式.

10. 求 $\sim\Pi_3$ 式，使之证明上等价于 Σ_3 式.

4.4 K 的完备性定理

我们最后将证明下述命题:

如果 $\mathscr{A}$ 是 $\mathscr{L}$ 的逻辑有效公式，那么 $\mathscr{A}$ 是 $K_{\mathscr{L}}$ 的定理. 但是，在我们证明之前，为了扩充和应用在 L 的完备性定理证明中使用过的观念，我们需要做一些准备工作.

首先，扩充的思想能容易地加以推广. (这里，如前，除我们希

堂强调所用的语言外，我们将用 K 代替 $K_{\mathscr{L}}$.)

定义 4.32

K 的一个扩充是指一个形式系统，它通过改变和扩大公理组而得到，并且使 K 的所有定理仍然是定理(也可能引进新的定理). 类似地，给出 K 的两个扩充，我们说其中一个是另一个的扩充，如果它的定理类更大一些(或，在平凡的情况下，是相同的).

定义 4.33

一个一阶系统是指 $K_{\mathscr{L}}$ 的一个扩充，这里 $\mathscr{L}$ 是某个一阶语言.

定义 4.34

一个一阶系统 S 称为是一致的，如果不存在公式 $\mathscr{A}$，使得 $\mathscr{A}$ 和 $(\sim\mathscr{A})$ 都是 S 的定理.

命题 4.35(参见命题 2.19)

令 S 是一个一致的一阶系统，并且令 $\mathscr{A}$ 是一个闭公式且非 S 的一个定理. 那么通过对 S 补加 $(\sim\mathscr{A})$ 为公理后得到的扩充 S^* 也是一致的.

证明 假设 S^* 是不一致的. 那么，对某个公式 $\mathscr{B}$，有 $\vdash_{S^*}\mathscr{B}$ 和 $\vdash_{S^*}(\sim\mathscr{B})$. 现在据命题 4.3，$\vdash_{S^*}(\sim\mathscr{B}\to(\mathscr{B}\to\mathscr{A}))$，因为 S^* 是 K 的一个扩充，因此，据分离规则有 $\vdash_{S^*}(\mathscr{B}\to\mathscr{A})$，再据分离规则有 $\vdash_{S^*}\mathscr{A}$.

因此，这是 $\mathscr{A}$ 在 S^* 中的一个证明. 这样的一个证明，是在 S 中从 $(\sim\mathscr{A})$ 的一个演绎. 所以我们有

$$(\sim\mathscr{A})\vdash_{S^*}\mathscr{A}.$$

由于 $(\sim\mathscr{A})$ 是闭的，我们应用演绎定理得到

$$\vdash_{S}((\sim\mathscr{A})\to\mathscr{A}).$$

但是，据命题 4.3 有

$$\vdash_S (((\sim\mathscr{A})\to\mathscr{A})\to\mathscr{A}),$$

所以用分离规则有 $\vdash_S \mathscr{A}$.

这和假设 $\mathscr{A}$ 不是 S 的定理矛盾，所以 S^* 必一致.

▷ 注意这命题是命题 2.19 的一个类似，只是我们必须加入条件：$\mathscr{A}$ 是一个闭公式. 不过在我们今后这个结果的使用中，这不至成为障碍.

定义 4.33

一阶系统 S 称为完全的，如果对于每个闭公式 $\mathscr{A}$，或者 $\vdash_S \mathscr{A}$，或者 $\vdash_S (\sim\mathscr{A})$.

注意，K 不是完全的. 例如，公式 $(\forall x_1)A_1^1(x_1)$ 既非 K 的定理，它的否定也非 K 的定理.

命题 4.37（参见命题 2.21）

令 S 是一致的一阶系统. 那么，就有一个 S 的完全的一致扩充.

证明 证明完全遵照命题 2.21 的证明模式. 令 $\mathscr{A}_0, \mathscr{A}_1, \cdots$ 是 $\mathscr{L}$ 的所有闭公式的枚举. 我们构造一个 K 的扩充序列 $S_0, S_1, \cdots$ 如下：令 S_0 是 S. 对于 $n>0$，如果 $\vdash_{S_{n-1}} \mathscr{A}_{n-1}$，令 S_n 相同于 S_{n-1}；如果 $\vdash_{S_{n-1}} \mathscr{A}_{n-1}$ 不成立，令 S_n 为 S_{n-1} 的扩充，它通过把 $(\sim\mathscr{A}_{n-1})$ 补充为公理而得到. 据命题 4.35，显然每个 S_n 都是 K 的一致扩充. 令 S_∞ 是这样的一阶系统，它以至少在 S_n 之一中为公理的一切公式作为它的公理. 和命题 2.21 的证明完全一样，我们可证明 S_∞ 是一致并且是完全的.

▷ 正是在这一点上，我们的方法不得不实质上与第二章中那些有所不同. 如果我们要把命题 2.22"转译"成谓词演算中的术语，那么我们所得到的将是：如果 S 是一致的一阶系统，那么存在 $\mathscr{L}$ 的一个解释，使 S 的每个定理在其中皆真. 我们确实将要证明

它，不过证明相当困难，而且涉及新的观念。

到目前为止，语言 $\mathscr{L}$ 是已经固定的虽然是任意的。在下面的证明中，我们将需要扩大语言，通过增添一列无限多的新的个体常元 $b_0, b_1, \cdots$。这无疑将导致在 K 内引进新的公式，新的公理和新的定理（例如，新公式 $((\forall x_1)A_1^1(x_1)\rightarrow A_1^1(b_1))$ 将是扩大语言的系统的一条公理）。但是，如果 S 是 $K_{\mathscr{L}}$ 的一致扩充，那么如上通过扩大语言而得到的新系统 S^+ 也是一致的。因为，倘若 $\mathscr{A}$ 和 $(\sim\mathscr{A})$ 是 S^+ 的定理，那么，它们的证明既是有限公式列，将只涉及有限数目的符号 $b_0, b_1, b_2, \cdots$。因而，这些证明可以转变为 S 中的证明，只须对每个这样的符号代入一个在证明中未曾出现的变元就行了。因此我们将得到 $\mathscr{L}$ 中一个公式和它的否定的证明，这是不可能的。

命题 4.38

令 S 是 $K_{\mathscr{L}}$ 的一个一致扩充。那么存在一个 $\mathscr{L}$ 的解释，其中 S 的每个定理皆真。

证明 通过增添一列新的个体常元 $b_0, b_1, b_2, \cdots$ 扩大语言 $\mathscr{L}$，用 $\mathscr{L}^+$ 表示新语言，用 S^+ 和 K^+ 分别表示由 S 和 $K_{\mathscr{L}}$ 所得的新系统。那么，如前 S^+ 是一致的。从 S^+ 开始，让我们定义一列一阶系统：$S_0, S_1, \cdots$ 如下。首先列出 $\mathscr{L}^+$ 恰含一个自由变元的所有公式：

$$\mathscr{F}_0(x_{i0}), \mathscr{F}_1(x_{i1}), \cdots$$

当然，$x_{i0}, x_{i1}, \cdots$ 并不要求都有区别。现在从序列 $b_0, b_1, b_2, \cdots$ 中选一子序列 $c_0, c_1, c_2, \cdots$ 使得

(1) c_0 在 $\mathscr{F}_0(x_{i0})$ 中不出现

和

(2) 对于 $n>0$，$c_n\notin\{c_0, \cdots c_{n-1}\}$ 并且 c_n 在 $\mathscr{F}_0(x_{i0}), \cdots \mathscr{F}_n(x_{in})$ 的任一个中都不出现。

我们能够做到这一点，因为每个公式仅能包含有限多个（如果至少

有一个的话) b_i 的出现.

对每个 k, 用 $\mathscr{G}$ 表示合式公式

$$(\sim(\forall x_{ik})\mathscr{F}_k(x_{ik})\to\sim\mathscr{F}_k(c_k)).$$

现在令 S_0 是 S^+. 令 S_1 是由补加 $\mathscr{G}_0$ 为新公理而得到的 S_0 的扩充. 对于每个 $n>1$, 令 S_n 是由补加 $\mathscr{G}_{n-1}$ 为新公理而得的 S_{n-1} 的扩充. 我们的方案是去证明每个 S_n 是一致的, 再如前去从 S_n 的序列得到一致的 S_∞, 然后据命题 4.37 去得 S_∞ 的一致完全的扩充. 这将使得我们能构造所要求的解释.

S_0 是一致的. 令 $n>0$ 并且假设 S_n 是一致的, 但 S_{n+1} 不一致, 那么存在一个 $\mathscr{L}^+$ 的公式 $\mathscr{A}$, 使得

$$\underset{S_{n+1}}{\vdash}\mathscr{A} \text{ 和 } \underset{S_{n+1}}{\vdash}(\sim\mathscr{A}),$$

现在 $\underset{S_{n+1}}{\vdash}(\mathscr{A}\to(\sim\mathscr{A}\to\sim\mathscr{B}))$, 由于 $(\mathscr{A}\to(\sim\mathscr{A}\to\sim\mathscr{B}))$ 是一重言式, 对任一公式 $\mathscr{B}$. 所以通过两次分离, 我们就得到

$$\underset{S_{n+1}}{\vdash}(\sim\mathscr{B}) \quad \text{对任一公式 } \mathscr{B}.$$

特别地 $$\underset{S_{n+1}}{\vdash}(\sim\mathscr{G}_n).$$

现在在 S_{n+1} 中的一个证明恰恰是 S_n 中从 $\mathscr{G}_n$ 的一个演绎, 所以我们有

$$\mathscr{G}_n\underset{S_n}{\vdash}(\sim\mathscr{G}_n)$$

$\mathscr{G}_n$ 是闭的, 所以根据演绎定理,

$$\underset{S_n}{\vdash}(\mathscr{G}_n\to(\sim\mathscr{G}_n)).$$

现在, 如我们前面已经看到的, 可以推得

$$\underset{S_n}{\vdash}(\sim\mathscr{G}_n),$$

即 $$\underset{S_n}{\vdash}\sim(\sim(\forall x_{in})\mathscr{F}_n(x_{in})\to\sim\mathscr{F}_n(c_n)).$$

但

$$\underset{S_n}{\vdash}(\sim(\sim(\forall x_{in})\mathscr{F}_n(x_{in})\to\sim\mathscr{F}_n(c_n))\to\sim(\forall x_{in})\mathscr{F}_n(x_{in}))$$

且 $\underset{S_n}{\vdash}(\sim(\sim(\forall x_{in})\mathscr{F}_n(x_{in})\to\sim\mathscr{F}_n(c_n))\to\mathscr{F}_n(c_n))$,

由于这些公式都是重言式的实例,因此据分离规则,我们有

$$\underset{S_n}{\vdash}\sim(\forall x_{in})\mathscr{F}_n(x_{in}) \text{ 和 } \underset{S_n}{\vdash}\mathscr{F}_n(c_n).$$

在 $\mathscr{F}_n(c_n)$ 的证明中,用 y 替换每个 c_n 的出现,其中 y 是一个不在证明中出现的变元. 我们所得的是 $\mathscr{F}_n(y)$ 在 S_n 中的一个证明,这是因为 c_n 不出现在任何公理 $\mathscr{G}_0$, $\mathscr{G}_1$, …, $\mathscr{G}_{n-1}$ 中, 而 $\mathscr{F}_n(c_n)$ 是在 S_n 中从这些公理导出的. 因此,

$$\underset{S_n}{\vdash}\mathscr{F}_n(y).$$

所以据概括 $\underset{S_n}{\vdash}(\forall y)\mathscr{F}_n(y)$,

所以 $\underset{S_n}{\vdash}(\forall x_{in})\mathscr{F}_n(x_{in})$, 据命题 4.18.

现在,我们得到了和 S_n 一致性的一个矛盾,所以我们必定有:如果 S_n 是一致的, 那么 S_{n+1} 也是一致的, 对一切 $n\geqslant 0$. 根据归纳法, S_n 对所有 n 是一致的.

令 S_∞ 是以 $\mathscr{L}^+$ 的至少是 S_n 之一的公理的一切合式公式为公理而得. S_∞ 是一致的, 因为如果它不一致, 那么只用它的有限多个公理就能导出一个矛盾, 所以, 在某一个 S_n 内也将能导出矛盾.

然后, 据命题 4.37, 令 T 是 S_∞ 的一个既一致又完全的扩充.

现在构造我们的解释的方法是某种新的并且可能产生混淆. 以前我们曾经关注过,其论域是由数学对象组成的解释,如由自然数或整数组成的. 但是,根据定义,对域所要求的只需是一非空集即可. 我们定义 $\mathscr{L}^+$ 的一个解释如下:

(a) 域 D_I 是 $\mathscr{L}^+$ 所有闭项, 即不含有任何变元的项的集(即所有个体常元和所有由它们用函数字母造成的项).

(b) 个体常元是它们自己的解释.

(c) 对 $d_1, \cdots, d_n \in D_I$, $\overline{A}_i^n(d_1, \cdots, d_n)$成立，如果$\underset{T}{\vdash} A_i^n(d_1, \cdots d_n)$；$\overline{A}_i^n(d_1, \cdots, d_n)$不成立，如果$\underset{T}{\vdash}(\sim A_i^n(d_1, \cdots d_n))$. 这是有意义的，因为 T 是完全的，且 $A_i^n(d_1, \cdots, d_n)$ 是一闭公式.

(d) 对 $d_1, \cdots, d_n \in D_I$, $\overline{f}_i^n(d_1, \cdots, d_n)$ 以 $f_i^n(d_1, \cdots, d_n)$ 为值. 注意，由于 $d_1, \cdots, d_n$ 是闭项，所以 $f_i^n(d_1, \cdots, d_n)$ 也是. 这定义了一个解释 I. 现在我们必须证明，S 的每个定理在 I 中为真.

引理：对 $\mathscr{L}^+$ 中的任一闭公式 $\mathscr{A}$, $\underset{T}{\vdash}\mathscr{A}$，当且仅当 $I \models \mathscr{A}$.]

证明 通过对 $\mathscr{A}$ 中的联结词和量词数进行归纳加以证明.

基础步骤：$\mathscr{A}$ 是原子公式，如 $A_i^n(d_1, \cdots, d_n)$，其中 $d_1, \cdots, d_n$ 一定是闭项.

如果$\underset{T}{\vdash}\mathscr{A}$，那么$\underset{T}{\vdash} A_i^n(d_1, \cdots, d_n)$，所以 $\overline{A}_i^n(d_1, \cdots, d_n)$在 I 中成立，即 $I \models \mathscr{A}$. 类似地，如果 $I \models \mathscr{A}$，我们能演绎出$\underset{T}{\vdash}\mathscr{A}$.

归纳步骤：令 $\mathscr{A}$ 不是原子公式，假设，结论对每个比 $\mathscr{A}$ 较短的公式都成立.

情形 1：$\mathscr{A}$ 是 $(\sim\mathscr{B})$. 如果$\underset{T}{\vdash}\mathscr{A}$，那么$\underset{T}{\vdash}(\sim\mathscr{B})$. 由此知 $\mathscr{B}$ 不是 T 的一条定理，因为 T 是一致的. 因此由于 $\mathscr{B}$ 是闭的，$(\sim\mathscr{B})$在 I 中为真，即 $I \models \mathscr{A}$. 反之，如果 $I \models \mathscr{A}$，那么 $I \models (\sim\mathscr{B})$，所以 $\mathscr{B}$ 在 I 中不真，所以据归纳假设，$\mathscr{B}$ 不是 T 的定理. 又由于 T 是完全的，因此$(\sim\mathscr{B})$是 T 的定理，即$\underset{T}{\vdash}\mathscr{A}$.

情形 2：$\mathscr{A}$ 是$(\mathscr{B}\to\mathscr{C})$. 假设 $\mathscr{A}$ 在 I 中不真. 那么 $\mathscr{B}$ 真而 $\mathscr{C}$ 假. 因而据归纳假设，有$\underset{T}{\vdash}\mathscr{B}$ 而没有$\underset{T}{\vdash}\mathscr{C}$. 由于 T 是完全的，我们有$\underset{T}{\vdash}\mathscr{B}$ 和$\underset{T}{\vdash}(\sim\mathscr{C})$. 现在$\underset{T}{\vdash}(\mathscr{B}\to((\sim\mathscr{C})\to\sim(\mathscr{B}\to\mathscr{C})))$，因为这公式是一重言式的实例，于是通过两次分离我们得到

$$\underset{T}{\vdash}\sim(\mathscr{B}\to\mathscr{C}), \text{ 即 } \underset{T}{\vdash}(\sim\mathscr{A}).$$

由于T是一致的，因而$\mathscr{A}$不是T的一条定理.

反之，假设$\mathscr{A}$不是T的一条定理，那么据T的完全性，有$\underset{T}{\vdash}(\sim\mathscr{A})$，从而$\underset{T}{\vdash}\sim(\mathscr{B}\to\mathscr{C})$. 但是$(\sim(\mathscr{B}\to\mathscr{C})\to\mathscr{B})$和$(\sim(\mathscr{B}\to\mathscr{C})\to\sim\mathscr{C})$是重言式，所以我们有

$$\underset{T}{\vdash}\mathscr{B} \text{ 和 } \underset{T}{\vdash}(\sim\mathscr{C}),$$

所以 $\underset{T}{\vdash}\mathscr{B}$ 和并非 $\underset{T}{\vdash}\mathscr{C}$，因为$T$是一致的.

于是，根据归纳假设，

$$I\models\mathscr{B} \text{ 和并非 } I\models\mathscr{C}$$

所以$\mathscr{B}$在I中为真而$\mathscr{C}$在I中为假. 据注记3.25(d)，因而$(\mathscr{B}\to\mathscr{C})$在$I$中为假，所以在$I$中不真.

情形3：$\mathscr{A}$是$(\forall x_i)\mathscr{B}(x_i)$. 首先，如果$x_i$在$\mathscr{B}$中不自由出现，那么$\mathscr{B}$是闭的，根据归纳假设，有$\underset{T}{\vdash}\mathscr{B}$，当且仅当$I\models\mathscr{B}$. 我们也知道$\underset{T}{\vdash}\mathscr{B}$，当且仅当$\underset{T}{\vdash}(\forall x_i)\mathscr{B}$，并且$I\models\mathscr{B}$，当且仅当$I\models(\forall x_i)\mathscr{B}$. 因此在这种情况下，$\underset{T}{\vdash}\mathscr{A}$，当且仅当$I\models\mathscr{A}$.

其次，如果x_i在$\mathscr{B}(x_i)$中自由出现，那么由于$\mathscr{A}$是闭的，它是$\mathscr{B}(x_i)$中的唯一的自由变元. 所以$\mathscr{B}(x_i)$是序列$\mathscr{F}_0(x_{i0})$，$\mathscr{F}_1(x_{i1})$，…中的一员，比方说$\mathscr{B}(x_i)$是$\mathscr{F}_m(x_{im})$. 因此，$\mathscr{A}$是$(\forall x_{im})\mathscr{F}_m(x_{im})$. 假设$I\models\mathscr{A}$. 根据命题4.4，我们有(从公理(K5))

$$I\models((\forall x_{im})\mathscr{F}_m(x_{im})\to\mathscr{F}_m(c_m)).$$

因此$I\models\mathscr{F}_m(c_m)$. 现在$\mathscr{F}_m(c_m)$比$\mathscr{A}$有较少的联结词和量词，所以根据归纳假设，$\underset{T}{\vdash}\mathscr{F}_m(c_m)$. 我们希望证明$\underset{T}{\vdash}\mathscr{A}$，所以作相反假设，即$\underset{T}{\vdash}(\sim\mathscr{A})$，由于$T$是完全的. 也就是

$$\underset{T}{\vdash}\sim(\forall x_{im})\mathscr{F}_m(x_{im}).$$

但是 $$\underset{T}{\vdash}(\sim(\forall x_{im})\mathscr{F}_m(x_{im})\to\sim\mathscr{F}_m(c_m)),$$

因为 $\mathscr{G}_m$ 是 T 的一条公理. 于是,据分离规则,

$$\vdash_T (\sim \mathscr{F}_m(c_m)).$$

这与 T 的一致性矛盾,所以我们一定会有所要求的 $\vdash_T \mathscr{A}$.

反之,令 $\vdash_T \mathscr{A}$,并且假设 $\mathscr{A}$ 在 I 中不真, 即并非 $I \models (\forall x_{im})\mathscr{F}_m(x_{im})$. 那么,必有 D_I 的一个元 d,使得 $I \models (\sim \mathscr{F}_m(d))$. 为了明白这点,注意在 I 中有一赋值不满足 $(\forall x_{im})\mathscr{F}_m(x_{im})$,从而有一不满足 $\mathscr{F}_m(x_{im})$ 的赋值 v. 现在 $v(x_{im}) \in D_I$, 即 $v(x_{im})$ 是一闭项比方说 d,这一个项必然在 $\mathscr{F}_m(x_{im})$ 中对 x_{im} 自由. 另一方面也有 $v(d)=d$,因此 $v(x_{im})=v(d)$. 于是根据练习 3.23 的结果, v 不满足 $\mathscr{F}_m(d)$,从而 $\mathscr{F}_m(d)$ 在 I 中不真,因此 $I \models (\sim F_m(d))$, 如所要求. 但是 $\vdash_T (\forall x_{im})\mathscr{F}_m(x_{im})$,所以 $\vdash_T \mathscr{F}_m(d)$, 据公理 $(K5)$ 和分离规则. 于是根据归纳假设, 就有 $I \models \mathscr{F}_m(d)$. 但是 $\mathscr{F}_m(d)$ 和 $\sim \mathscr{F}_m(d)$ 不能在 I 中都真,所以在这种情形下 $\vdash_T \mathscr{A}$ 蕴涵 $I \models \mathscr{A}$.

这完成了引理的归纳证明, 所以现在我们知道. T 的每个定理在解释 I 中皆真. 但是 S 的每条定理也是 T 的一条定理,因为 T 是由 S 仅通过扩大语言和补加新公理而得到的. 这样, $\mathscr{L}^+$ 的作为 S 的定理的每个公式在 I 中皆真. 当然 S 的每条定理是 $\mathscr{L}$ 的一个公式, 而 I 还包含不同于 $\mathscr{L}$ 的公式的那些公式的解释, 所以让我们对 I 加以限制, 通过排除个体常元 b_0, $b_1 \cdots$ 和依赖于它们的项的解释,而听任 D_I 不变. 这就给了我们一个 $\mathscr{L}$ 的解释,而 S 的每条定理在这个解释下是都真的.

▷ 我们还没有证明完备性定理,但是, 在证明前面命题 4.38 中所作的可观的努力, 将能使我们十分容易地完成完备性定理的证明.

命题 4.39($K_{\mathscr{L}}$ 的完备性定理)

如果 $\mathscr{A}$ 是 $\mathscr{L}$ 的一个逻辑有效的公式, 那么 $\mathscr{A}$ 是 $K_{\mathscr{L}}$ 的

一条定理.

证明 令 $\mathscr{A}$ 是 $\mathscr{L}$ 的一个逻辑有效公式，并且令 $\mathscr{A}'$ 是它的全称闭包. 从系 3.28 可推得 $\mathscr{A}'$ 也一定逻辑有效. 现假设 $\mathscr{A}$ 不是 $K_{\mathscr{L}}$ 的定理. 那么根据命题 4.19, $\mathscr{A}'$ 也不是 $K_{\mathscr{L}}$ 的定理. 如果我们把 $\sim\mathscr{A}'$ 作为补加公理，我们就得到了一个新的系统 $K'_{\mathscr{L}}$, 它是一致的，据命题 4.35. 因此据命题 4.38, 有一个 $\mathscr{L}$ 的解释，$K'_{\mathscr{L}}$ 的每个定理在其中皆真. 特别地，$\sim\mathscr{A}'$ 在这个解释中为真，从而 $\mathscr{A}'$ 为假 ($\mathscr{A}'$ 必然是闭的). 这和 $\mathscr{A}'$ 是逻辑有效式矛盾，所以 $\mathscr{A}$ 一定是 $K_{\mathscr{L}}$ 的一条定理.

▷ 目前我们的任务完成了. 我们已经证明了 $K_{\mathscr{L}}$ 的定理恰恰是 $\mathscr{L}$ 的逻辑有效公式. 尽管这个证明给我们带来某些困难(它首先是由哥德尔于 1930 年证明的，我们给出的证明，基本上是由亨金较后给出的)，结果并不令人惊奇. 系统 $K_{\mathscr{L}}$ 恰是这样构造的，它能证明人们用通常的方法和直觉的逻辑想要证明的每件事情，即"逻辑真理"(也就是所有逻辑有效合式公式). 虽然如此，完备性定理毕竟是一条主要定理，它确认 $K_{\mathscr{L}}$ 完成了人们所期待于它的任务.

练习

11. $K_{\mathscr{L}}$ 的一个扩充 S 是不一致的，当且仅当 $\mathscr{L}$ 的每个公式是 S 的一条定理.

12. 令 S 是一致的一阶系统，使得对 S 的每个闭公式 $\mathscr{A}$, 如果把 $\mathscr{A}$ 作为补加公理而得的系统是一致的，那么 $\mathscr{A}$ 是 S 的一条定理. 证明 S 是完全的.

13. 令 $\mathscr{A}$ 和 $\mathscr{B}$ 是 $\mathscr{L}$ 的公式，且使 $(\mathscr{A}\vee\mathscr{B})$ 是 $K_{\mathscr{L}}$ 的定理. $\mathscr{A}$ 或 $\mathscr{B}$ 是否必定是 $K_{\mathscr{L}}$ 的定理?

14. 令 $\mathscr{L}$ 是带有无限多个谓词字母的一阶语言. 证明 $K_{\mathscr{L}}$ 有无限多个不同的一致扩充.

4.5 模型

命题4.39有许多推论，我们在这里将提到一些．为了这样做，引进一个新的概念即模型的概念是方便的．

定义4.40

(i) 令Γ是$\mathscr{L}$的公式组．如果$\mathscr{L}$的一个解释，使得Γ的每个成员皆在其中为真，就称该解释为Γ的一个模型．

(ii) 如果S是一阶系统，S的一个模型是指这样一个解释，它使S的每个定理皆在其中为真．

命题4.41

令S是一阶系统，并且令I是一解释，使S的每一公理在其中为真，那么I是S的一个模型．

证明(参见命题4.5的证明)

假设I是使S中每个公理在其中皆真的解释．令$\mathscr{A}$是S的定理．我们证明$\mathscr{A}$在I中也必真，通过对$\mathscr{A}$的证明的公式数目n进行归纳．

基础步骤：$n=1$．$\mathscr{A}$是S的一条公理，因此在I中为真．

归纳步骤：$n>1$．假设每个有较短的证明的定理在I中为真．

情形1：$\mathscr{A}$可由证明中在前的公式，通过分离，比方说从$\mathscr{B}$和$(\mathscr{B}\to\mathscr{A})$而得．根据归纳假设，$\mathscr{B}$和$(\mathscr{B}\to\mathscr{A})$在$I$中为真，所以据命题3.26，$\mathscr{A}$在$I$中真．

情形2：$\mathscr{A}$在证明中由在前的公式，通过概括而得．那么，比方说$\mathscr{A}$是$(\forall x_i)\mathscr{B}$，而那个在前的公式是$\mathscr{B}$．据归纳假设，$\mathscr{B}$在I中为真，所以据命题3.27，$(\forall x_i)\mathscr{B}$在I中为真．

情形3：$\mathscr{A}$是S的公理．如前，$\mathscr{A}$一定在I中为真．

这就完成了"S的每个定理在I中为真"的归纳证明．由此可知I是S的一个模型．

▷ 我们之所揭示的乃是这个事实：定义 4.40(ii) 之下的一个一阶系统 S 的模型，与定义 4.40(i) 之下的 S 的公理组的模型是同一回事.

注意，由于 $K_{\mathscr{L}}$ 的每个定理在每个解释中皆真，所以 $\mathscr{L}$ 的任何一个解释都是 $K_{\mathscr{L}}$ 的一个模型，不外乎是命题 4.5 的平凡的推论. 因此，模型的概念在 $K_{\mathscr{L}}$ 的扩充的背景下更为重要，扩充不仅有较大的定理的类，而且还有不是模型的解释.

现在命题 4.38 可以重述成：如果一阶系统 S 是一致的，那么它有一个模型. 事实上我们有下面的命题.

命题 4.42

一阶系统 S 是一致的，当且仅当它有一模型.

证明. 定理的一方面已经证明. 假设 S 有一模型，如 I，并且假设 S 不一致. 那么，对某个 $\mathscr{A}$，有 $\underset{S}{\vdash} \mathscr{A}$ 和 $\underset{S}{\vdash}(\sim\mathscr{A})$. 现在 S 的所有定理在模型 I 中皆真，所以 $\mathscr{A}$ 和 $(\sim\mathscr{A})$ 在 I 中都真，根据注记 3.25(b)，这是不可能的，所以 S 必定是一致的.

例 4.43

令 $\mathscr{A}$ 是 $\mathscr{L}$ 的一个闭公式，且 $\mathscr{A}$ 和 $(\sim\mathscr{A})$ 都不是 K 的定理. 那么，根据命题 4.35，通过分别把 $\mathscr{A}$ 和 $(\sim\mathscr{A})$ 补加为新公理而得的系统 K^1 和 K^2 也都一致. 因此 K^1 和 K^2 都有一个模型，K^1 的模型是一个解释 I_1，在其中 $\mathscr{A}$ 真，K^2 的模型是一个解释 I_2，在其中 $(\sim\mathscr{A})$ 为真. 因此 I_1 不可能是 K^2 的模型，同样 I_2 也不可能是 K^1 的模型. 由此可知任何一致且非完全的一阶系统（即其中存在一个闭合式公式 $\mathscr{A}$，使得 $\mathscr{A}$ 和 $(\sim\mathscr{A})$ 都非定理）至少有两个本质上不同的模型.

▷ 我们必须小心地避免堕入下面的陷阱：由于一个特殊的公式在一个系统 S 的一个模型中为真，就料想它必定是 S 的一条定理. 上面的例子告诉我们这并不必然成立. 但是我们在这个方向

上，作为命题 4.42 的一个推论也能做出一些工作.

命题 4.44

令 S 是一致的一阶系统，并且令 $\mathscr{A}$ 是一个闭公式，它在 S 的每个模型中皆真. 那么 $\mathscr{A}$ 是 S 的一条定理.

证明. 令 $\mathscr{A}$ 是在 S 的每个模型上皆真的一个公式，并且假设 $\mathscr{A}$ 不是 S 的一条定理. 那么，根据命题 4.35，由 S 通过补加 $(\sim\mathscr{A})$ 为公理而得的系统 S' 是一致的. 所以，根据命题 4.42S' 有一模型 M. $(\sim\mathscr{A})$在 M 中为真，所以 $\mathscr{A}$ 在 M 中为假. 但是 M 是 S 的一个模型(因为 S' 是 S 的一个扩充). 这和 $\mathscr{A}$ 在 S 的每个模型中真的假设矛盾，所以 $\mathscr{A}$ 一定是 S 的定理.

命题 4.45(洛文海姆-斯柯兰定理)

如果一阶系统 S 有一模型，那么 S 有一域为可数集的模型(一个集是可数的，如果它的元素可以和自然数集建立 1-1 对应).

证明 如果 S 有一模型，那么据命题 4.42 S 是一致的. 如果 S 是一致的，那么命题 4.38 的证明表明 S 有一特殊性质的模型. 它的域由在扩大的语言中的闭项集组成. 这个集是可数的. 这可通过能写出一个最终包括每个闭项的序列(当然是无限的)的程序之描述来证明. 它可以有几种方法做，留作练习.

▷ 这命题有某些令人惊异的推论，正如我们在后面的一章将要看到的.

命题 4.46(紧致性定理)

如果一阶系统 S 的公理集的每个有限子集都有一模型，那么 S 本身也有一模型.

证明 假设 S 的每个有限公理集有一模型，但 S 没有模型. 那么据定理 4.42S 是不一致的. 因此 $\vdash_S \mathscr{A}$ 和 $\vdash_S (\sim\mathscr{A})$，对某个合式公式 $\mathscr{A}$. 但是这些证明仅能包含有限多个 S 中公理的实例. 令 Γ 是 S 的在这些证明中用到的所有公理的集合. Γ 是有限的，

因此有一模型. 所以存在一解释 I,在其中 Γ 的每个成员为真. 由此知 $\mathscr{A}$ 和 $(\sim\mathscr{A})$ 在 I 中都真. 这是因为分离和概括规则,在一个解释中保持它们的真实性(见命题 4.41 的证明). 但是 $\mathscr{A}$ 和 $(\sim\mathscr{A})$ 在 I 中不能都真,所以我们得到必然的矛盾,因此 S 必定有一模型.

▷ 这个命题, 有时用一种稍微不同的形式被陈述, 我们把它作为一个系.

系 4.47

令 Γ 是 $K_{\mathscr{L}}$ 的一个公式的无限集. 那么当 Γ 的每个有限子集有一模型时, Γ 有一模型.

▷ 有一种由模型产生一阶系统的方法. 令 S 是一阶系统, 并且假设 S 是一致的, 那么 S 有一模型 I. 让我们假设 S 不是完全的,所以对某个公式 $\mathscr{A}$, $\mathscr{A}$ 和 $(\sim\mathscr{A})$ 都不是 S 的定理. 但是, 在 I 中这个公式 $\mathscr{A}$ 或者真或者假, 即 $I\models\mathscr{A}$ 或 $I\models(\sim\mathscr{A})$. 模型 I 类似地对每个闭公式给出了一个'真值'. 让我们定义一个新的一阶系统 $S(I)$,它通过补加在 I 中为真的所有公式为公理而得. 那么, $S(I)$ 的定理都是 $S(I)$ 的公理, 因为在 I 中为真的合式公式的任何后承,在 I 中也将为真. $S(I)$ 是一致的,因为如果 $\underset{S(I)}{\vdash}\mathscr{A}$ 且 $\underset{S(I)}{\vdash}(\sim\mathscr{A})$, 那么 $\mathscr{A}$ 和 $(\sim\mathscr{A})$ 在 I 中皆真, 这是不可能的. 注意 I 是 $S(I)$ 的一个模型. $S(I)$ 也是完全的, 因为, 给出任何闭公式 $\mathscr{A}$,或者 $I\models\mathscr{A}$,或者 $I\models(\sim\mathscr{A})$,从而确实有 $\underset{S(I)}{\vdash}\mathscr{A}$ 或 $\underset{S(I)}{\vdash}(\sim\mathscr{A})$.

练习

15. 令 Γ 是 $\mathscr{L}$ 的公式集, 令 M 是 Γ 的一个模型, 证明. 如果 $\Gamma\underset{K_{\mathscr{L}}}{\vdash}\mathscr{A}$,那么 $\mathscr{A}$ 在 M 中为真. 逆命题成立吗?

16. 令 S 是 $K_{\mathscr{L}}$ 的一致完备扩充. 证明 S 的任意两个模型

是初等等值的，即每个在一模型中为真的闭公式，在另一模型中也真.

17. 令 S 是 $K_{\mathscr{L}}$ 的一致扩充，M 是 S 的一个模型. 定义 S 的一个扩充 S^+ 如下：把所有 $\mathscr{L}$ 的在 M 中的真的所有原子公式补加为公理. 证明 S^+ 是一致的. S^+ 必然完全吗？

18. 令 S 是 $K_{\mathscr{L}}$ 的一致扩充，M 是 S 的一个模型. 定义 S 的一个扩充 $\hat{S}$ 如下：把 $\mathscr{L}$ 的在 M 中为真的所有闭原子公式和在 M 中不真的所有闭原子公式的否定补加为公理. 证明 $\hat{S}$ 是一致的，$\hat{S}$ 必然完全吗？

19. 令 S 是 $K_{\mathscr{L}}$ 的一致扩充，这里 $\mathscr{L}$ 是包含变元，个体常元 $a_1, a_2, \cdots$，仅有一个谓词字母 A_1^1 而没有函数字母的一阶语言. $\mathscr{L}$ 的一个解释可以看作是一个集合 D_I，它有一个特异的子集 A_I，和所有由使 $\overline{A}_1^1(x)$ 在 I 中成立的 $x \in D_I$ 组成. 假设对每个 $n \geqslant 1$，存在一个 S 的模型 M_n，其中 $\bar{a}_i \in A_{M_n}$ 对 $1 \leqslant i \leqslant n$. 证明存在 S 的一个模型 M，其中 $\bar{a}_i \in A_M$ 对每个 i.

第五章 数学系统

5.1 引论

第一到第四章不是数学. 系统 L 和 $K_{\mathscr{L}}$ 是逻辑演绎系统. 为了得到命题的证明,我们曾不得不使用某些数学技巧,但是这些技巧曾具有初等性质,主要是自然数的基本属性. 对其所研究主题的基础感兴趣的数学家,企图澄清他所作的假设和他所用方法程序. 我们在这样的澄清工作中用得上系统 $K_{\mathscr{L}}$. $K_{\mathscr{L}}$ 体现了为数学家所用的逻辑演绎程序. 我们已经看到,对语言 $\mathscr{L}$ 不加限制,使我们的关于 $K_{\mathscr{L}}$ 的结果非常一般,一个给定的 $\mathscr{L}$ 的符号能按多种方式加以解释. 但是,对于任何 $\mathscr{L}$,都存在一类公式,它们的真实性并不依赖于符号的解释,那就是逻辑有效公式类,即 $K_{\mathscr{L}}$ 的定理组成的类. 如果,$\mathscr{L}$ 按数学的方式解释,如在我们的例中那样,$K_{\mathscr{L}}$ 的定理可以被解释为数学的真理. 它们之所以是真的数学命题,与其说是因为它们的数学内容,倒不如说是因为它们的逻辑结构. 例如,在算术解释 N 中,公式

$$(\forall x_1)(\forall x_2)(A_1^2(x_1, x_2)\rightarrow A_1^2(x_1, x_2)),$$

是逻辑有效的,它可以被解释成数学命题:"对于任意的自然数 x 和 y,如果 $x=y$,那么 $x=y$,按逻辑结构它是真的. 另一方面,公式

$$(\forall x_1)(\forall x_2)(A(x_1, x_2)\rightarrow A_1^2(x_2, x_1))$$

可以被解释为:"对于任意的自然数 x 和 y,如果 $x=y$,那么 $y=x$",它是真的. 但是,它的真实性主要在于"$=$"的意义,而并非只是它的逻辑结构. 确实这个公式不是逻辑有效的. 不难找到一种解释,在这种解释之下,A_1^2 不是 $=$,而这公式是假的. 由此可知这个公式并非 $K_{\mathscr{L}}$ 的定理. 因此 $K_{\mathscr{L}}$ 的定理就其本身而论是没有数

学价值的. 我们的每个数学形式系统都将是某个 $K_{\mathscr{L}}$ 的扩充，通过补加上适当的公理，使得系统的定理将能表示数学真理和逻辑真理. 如果我们的形式系统须是一个数学系统，那自然希望，凡在数学上解释为真的一切公式都是定理(或者，如果这不可能的话，我们要使这样的公式尽可能的多).

什么才算得上一个数学上的真实，这在很大程度上取决于数学上的背景. 例如，命题

$$(\forall x)(\forall y)(xy=yx)$$

当被看作关于自然数的命题时是真的，但当被看作关于任意群的元时，它就并不必然为真. 我们将通过一些例子来说明，不同的数学背景怎样可由不同的形式系统来表示，以至特别地，上述命题将是形式算术的一条定理的解释，而不是一个形式群论的定理的解释. 背景将决定语言 $\mathscr{L}$ (如在算术的情况)，它也将决定一组特有公理. 使用"特有"这个词，是为了与 $(K1)\sim(K6)$ 有所区别，后者是逻辑公理在我们所有的系统中是共同的. 在规定了 $\mathscr{L}$ 之后，特有公理是 $\mathscr{L}$ 的公式，当把它们补作为公理时，就给出了 $K_{\mathscr{L}}$ 的一个扩充，在这个扩充中，特殊背景的数学真实(如同逻辑真实一样)，就表现为定理的解释.

5.2 带等号的一阶系统

数学很少能不用相等关系的. 符号"="并不出现在我们的形式语言中，但是在我们例子中，作为谓词 A_1^2 的解释，我们已经使用了它. 在所有数学系统中，我们将都把 A_1^2 包括在语言中，并且将 = 作为它的意图中的解释. 正如我们在上面所见，公式 $(\forall x_1)(\forall x_2)(A_1^2(x_1, x_2)\rightarrow A_1^2(x_2, x_1))$ 并不是 $K_{\mathscr{L}}$ 的一条定理，但是我们希望它是 $K_{\mathscr{L}}$ 的数学扩充中的一条定理. 保证这一点的一种办法，就是把它作为每个数学系统的特有公理. 但是显然还有另外一些公式要求同样的处理，例如 $(\forall x_1)A_1^2(x_1, x_1)$. 我们无须把所

有这些公式都收进来作为公理，但是我们将取出其中一组作为相等公理，从它们可以演绎出其它的．这个组是

$(E7)\quad A_1^2(x_1, x_1)$

$(E8)\quad A_1^2(t_k, u)\to A_1^2(f_i^n(t_1, \cdots, t_k, \cdots, t_n),$
$\qquad f_i^n(t_1, \cdots, u, \cdots, t_n)),$

其中 $t_1, \cdots, t_n, u$ 是任意项，f_i^n 是 $\mathscr{L}$ 中的任意函数文字。

$(E9)\quad (A_1^2(t_k, u)\to(A_i^n(t_1, \cdots, t_k, \cdots, t_n)$
$\qquad \to A_i^n(t_1, \cdots, u, \cdots, t_n))),$

其中 $t_1, \cdots, t_n, u$ 是任意项，A_i^n 是 $\mathscr{L}$ 中的任意谓词符号．

注 5.1

(a) $(E8)$和$(E9)$是公理模式，每个都表示一系列公理，可能有无限多个，依赖于 $\mathscr{L}$ 中函数文字和谓词符号的数目。

(b) 所有这些公理，在他们之中都有自由变元出现．按这样的方式书写它们，是为了清楚起见，并且也是为了以后应用时方便一些．但是我们知道，对任意的公式 $\mathscr{A}$，它的全称闭式为 $\mathscr{A}'$，有 $\mathscr{A}\underset{K_{\mathscr{L}}}{\vdash}\mathscr{A}'$ 和 $\mathscr{A}'\underset{K_{\mathscr{L}}}{\vdash}\mathscr{A}$，所以有一组等价的公理是它们的全称闭式．

(c) 作为 (b) 和关于约束变元易名的命题 4.18 的推论，在$(E7)$中出现的变元，写成 x_1，这是没有什么深意的．例如，$A_1^2(x_5, x_5)$就是$(E7)$的一条推论，通过如下的演绎：

(1)	$A_1^2(x_1, x_1)$	$(E7)$
(2)	$(\forall x_1)A_1^2(x_1, x_2)$	(1)，概括
(3)	$(\forall x_5)A_1^2(x_5, x_5)$	(2)，命题 4.18
(4)	$(\forall x_5)A_1^2(x_5, x_5)\to A_1^2(x_5, x_5)$	$(K5)$
(5)	$A_1^2(x_5, x_5)$	(3)，(4)分离

我们想要描述的所有数学系统都将是 $K_{\mathscr{L}}$(对某个 $\mathscr{L}$ 的)扩充，它包括公理$(E7)$和$(E8)$和$(E9)$的所有适当的(依赖于 $\mathscr{L}$ 的)

实例.

注记 5.2

公理中需要包括$(E7)$应是清楚的. 它保证在任何模型中, A_1^2的解释,在某方面表现象=. $(E8)$和$(E9)$比较复杂,但是它们保证在任何模型中, A_1^2的解释在另一些方面表现象=, 即相等的可以互相替代.

定义 5.3

公理$(E7)$, $(E8)$和$(E9)$称为相等公理. 任何包括公理$(E7)$以及$(E8)$和$(E9)$的所有适当实例的K_ε的扩充称为带等号的一阶系统.

命题 5.4

令S是带等号的一阶系统,那么下列是S的定理.

(i) $(\forall x_1)A_1^2(x_1, x_1)$,

(ii) $(\forall x_1)(\forall x_2)(A_1^2(x_1, x_2)\to A_1^2(x_2, x_1))$,

(iii) $(\forall x_1)(\forall x_2)(\forall x_3)(A_1^2(x_1, x_2)\to(A_1^2(x_2, x_3)$
$\to A_1^2(x_1, x_3)))$.

证明. (i)可以由$(E7)$,直接概括得到.

(ii) 我们来给出S中的证明.

(1) $A_1^2(x_1, x_2)\to(A_1^2(x_1, x_1)\to A_1^2(x_2, x_1))$ $(E9)$

(2) $(A_1^2(x_1, x_2)\to(A_1^2(x_1, x_1)\to A_1^2(x_2, x_1)))\to$
$((A_1^2(x_1, x_2)\to A_1^2(x_1, x_1))\to(A_1^2(x_1, x_2)$
$\to A_1^2(x_2, x_1)))$ $(K2)$

(3) $(A_1^2(x_1, x_2)\to A_1^2(x_1, x_1))\to(A_1^2(x_1, x_2)$
$\to A_1^2(x_2, x_1))$ (1), (2), 分离

(4) $(A_1^2(x_1, x_1)\to(A_1^2(x_1, x_2)\to A_1^2(x_1, x_1)))$ $(K1)$

(5) $A_1^2(x_1, x_1)$ $(E7)$

(6) $(A_1^2(x_1, x_2)\to A_1^2(x_1, x_1)$ (4), (5), 分离

(7) $(A_1^2(x_1, x_2)\to A_1^2(x_2, x_1))$ (3), (6), 分离

(8) $(\forall x_1)(\forall x_2)(A_1^2(x_1, x_2) \to A_1^2(x_2, x_1))$ (7), 概括

(iii) 我们给出 S 中的证明

(1) $(A_1^2(x_2, x_1) \to (A_1^2(x_2, x_3) \to A_1^2(x_1, x_3)))$ $(E9)$

(2) $(A_1^2(x_1, x_2) \to A_1^2(x_2, x_1))$ 同(ii)

(3) $(A_1^2(x_1, x_2) \to A_1^2(x_2, x_3) \to A_1^2(x_1, x_3)))$

(1), (2) HS

(4) $(\forall x_1)(\forall x_2)(\forall x_3)(A_1^2(x_1, x_2) \to (A_1^2(x_2, x_3)$
$\to A_1^2(x_1, x_3)))$ (3) 概括

▷ 这样，由于在上述命题中，(i)，(ii)，(iii)里的每一个在 S 的任何模型中皆真，符号 A_1^2 将被解释成一个自反的，对称的和传递的关系，即等价关系．现在 $=$ 是 A_1^2 在我们意图中的解释．在一个任意的解释中，公理很可能是假的，以致 A_1^2 可能被解释成任何两元关系，但是在 S 的模型中，如前我们已经看到公理一定是真的，A_1^2 必被解释为一个等价关系．但是，公理$(E7)$，$(E8)$和$(E9)$并不保证，在 S 的任何模型中 A_1^2 的解释实际上是 $=$．

例 5.5

考察带变元 $x_1, x_2, \cdots$，函数文字 f_1^2，和谓词文字 A_1^2 的一阶语言．定义一个解释 I 如下：D_I 是所有整数的集合 Z；$\overline{f}_1^2(x, y)$ 是 $x+y$；$\overline{A}_1^2(x, y)$ 成立，当且仅当 $x \equiv y \pmod 2$，对于任意 $x, y \in Z$，在这个解释中相等公理是真的．

对于$(E7)$，它的解释是 $x \equiv x \pmod 2$，这是真的．

对于$(E8)$，作为一种特殊情况，考察

$$A_1^2(x_1, x_2) \to A_1^2(f_1^2(x_1, x_3), f_1^2(x_2, x_3)).$$

它的解释为：

如果 $x \equiv y \pmod 2$，那么 $x+z \equiv y+z \pmod 2$

这是真的．$(E8)$的全面一般的证明留作练习．

对于$(E9)$，只有两种要证明的实例，因为 L 只包含一个谓词文字．这些是

$$(A_1^2(t, u) \to (A_1^2(t, v) \to A_1^2(u, v)))$$

和 $$(A_1^2(t, u) \to (A_1^2(v, t) \to A_1^2(v, u))).$$

它们的解释是，

如果 $x \equiv y \pmod 2$，那么 $x \equiv z \pmod 2$ 蕴涵 $y \equiv z \pmod 2$

和

如果 $x \equiv y \pmod 2$，那么 $x \equiv z \pmod 2$ 蕴涵 $z \equiv y \pmod 2$.

两个都是真的.

▷ 这个例子表明，在(E7)，(E8)和(E9)的一个模型中，A_1^2 并不必然被解释成 $=$. 但是下面的命题使局面得到了恢复.

命题 5.6

如果 S 是一致的带等号一阶系统，那么 S 有一个模型，其中 A_1^2 的解释是 $=$.

证明 根据命题 4.42，如果 S 是一致的，那么 S 有一个模型 M. 由于命题 5.4，$\overline{A}_1^2$ 是一个在 D_M 上的等价关系. 用 $[x]$ 表示含 x 的等价类. 现在定义一个新的解释 M^* 如下. M^* 的域是 $\{[x]: x \in D_M\}$，a_i 被解释为 $[a_i]$，对每个 i，f_i^n 被解释为 $\hat{f}_i^n$，这里对 $y_1, \cdots, y_n \in D_M$，有

$$\hat{f}_i^n([y_1], \cdots, [y_n]) = [\overline{f}_i^n(y_1, \cdots, y_n)],$$

A_i^n 被解释为 $\hat{A}_i^n$，这里对 $y_1, \cdots, y_n \in D_M$，

$$\hat{A}_i^n([y_1], \cdots, [y_n])$$

成立，当且仅当 $\overline{A}_i^n(y_1, \cdots, y_n)$ 成立，这里 $\overline{a}_i$，$\overline{f}_i^n$，$\overline{A}_i^n$ 是 $\mathscr{L}$ 的符号在 M 中的解释.

验证这些是合式定义的和 M^* 是 S 的一个模型就是长一些但并不困难. 例如，令 f 是 $\mathscr{L}$ 的一元函数文字，$\overline{f}$ 是它在 M 中的解释. 假设 a，b 是 D_M 的成员，且 $[a] = [b]$. 我们必须证明

$$[\overline{f}(a)] = [\overline{f}(b)].$$

现在

$$\vdash_S (A_1^2(x_1, x_2) \to A_1^2(f(x_1), f(x_2))). \qquad (E8)$$

因此，由于 M 是一个模型，$(A_1^2(x_1, x_2) \to A_1^2(f(x_1), f(x_2)))$ 在 M 中真．所以 $\overline{A}_1^2(a, b)$ 蕴涵 $\overline{A}_1^2(f(a), f(b))$，即 $[a]=[b]$ 蕴涵 $[\overline{f}(a)]=[\overline{f}(b)]$．

A_1^2 在 M^* 中的解释也是 $=$．因为，$\hat{A}_1^2([x], [y])$ 成立，当且仅当 $\overline{A}_1^2(x, y)$ 成立，即当且仅当 $[x]=[y]$．

▷ 这个证明可以用上面最后的例子很好地加以说明，在那里我们给出了一个模型，在其中 A_1^2 不解释为 $=$．在那个例子中，$\overline{A}_1^2(x, y)$ 当且仅当 $x \equiv y \pmod 2$（x 和 y 是整数）．定义一个新模型，域为 $\{[0], [1]\}$，其中 f_1^2 和 A_1^2 被解释为 $\hat{f}_1^2$ 和 $\hat{A}_1^2$，分别给出如下：

$$\hat{f}_1^2([x], [y]) = [\overline{f}_1^2(x, y)] = [x+y].$$

$\hat{A}_1^2([x], [y])$ 成立，当且仅当 $\overline{A}_1^2(x, y)$ 成立．

即　当且仅当 $x \equiv y \pmod 2$

即　当且仅当 $[x] \equiv [y]$．

定义 5.7

令 S 是带等号的一阶系统，S 的一个标准模型是指一个 A_1^2 在其中被解释为 $=$ 的模型．

我们在下面所关心的主要是标准模型，因为它们关于 A_1^2 的解释方面描绘了我们意图中的数学状态．

注意．当然，我们选定 A_1^2 去代表相等，是无关紧要的．我们同样可以选 A_{17}^2，只是在这个情况下，公理 $(E7)$，$(E8)$ 和 $(E9)$ 将涉及这个谓词符号而不是 A_1^2．

▷ 本章余下部分，我们将论述带等号的一阶系统，其中 A_1^2 代表相等．命题 5.4 的证明表明重复多次书写会带来何等不便．如果把符号 $\doteq$ 引入语言去代 A_1^2，那么多少总能减轻一点．

记法　书写 $t_1 \doteq t_2$ 以代替 $A_1^2(t_1, t_2)$，其中 t_1 和 t_2 是 $\mathscr{L}$ 中的项．

现在公理 $(E7)$，$(E8)$ 和 $(E9)$ 可以写成一种简洁的形式，使得

它们的意义更为清楚.

$(E7')$ $x_1=x_1$

$(E8')$ $(t_k=u\to(f_i^n(t_1,\cdots,t_k,\cdots,t_n)=f_i^n(t_1,\cdots,u,\cdots,t_n)))$,
$t_1,\cdots,t_n,u,f_i^n$ 如在$(E8)$中一样

$(E9')$ $(t_k=u\to(A_i^n(t_1,\cdots,t_k,\cdots,t_n)\to A_i^n(t_1,\cdots,u,\cdots,t_n)))$,
$t_1,\cdots,t_n,u,A_i^n$ 如在$(E9)$中一样.

符号$=$并不是我们在原始符号库之外引入形式语言中的唯一的符号. 例如,我们用$(\exists x_i)$作为$\sim(\forall x_i)\sim$的缩写,用$(\mathscr{A}\leftrightarrow\mathscr{B})$作为$\sim((\mathscr{A}\to\mathscr{B})\to\sim(\mathscr{B}\to\mathscr{A}))$的缩写. 有时用$(\mathscr{A}\vee\mathscr{B})$作为$(\sim\mathscr{A}\to\mathscr{B})$,用$(\mathscr{A}\wedge\mathscr{B})$作为$\sim(\mathscr{A}\to\sim\mathscr{B})$的缩写是方便的. 这和我们在第一章中讲的直觉的观念是相应的. 使用这些新的符号,显然并非以任何方式对形式系统有所扩充. 只是避免冗长的重写符号而已. 在不同的场合,为了扩大应用,在可能的情况下,还会引进更多的被定义符号. 有一种有用的符号,特别在用于带等号的一阶系统时. 这就是表示"存在唯一的…使得"的符号.

记法 $(\exists_1 x_i)\mathscr{A}(x_i)$是下面公式的简写

$$(\exists x_i)(\mathscr{A}(x_i)\wedge(\forall x_j)(\mathscr{A}(x_j)\to x_i=x_j)).$$

练习

1. 在例5.5中,完整地证明公理模式$(E8)$的每个实例在解释I中是真的.

2. 令S是一个带等号的一阶系统,假设闭公式$\mathscr{A}$在S的所有标准模型中皆真. 证明$\mathscr{A}$在S的所有模型中皆真.

3. 令$\mathscr{A}(x_1)$是$\mathscr{L}$的一个公式,其中x_1自由出现,并令x_2在$\mathscr{A}(x_1)$中对x_1自由,而$\mathscr{A}(x_2)$是对$\mathscr{A}(x_1)$中的x_1的一个自由出现用x_2代入而得的结果.(注意,这和我们平时使用的记法不同). 证明公式

$$(x_1=x_2\to(\mathscr{A}(x_1)\to\mathscr{A}(x_2)))$$

是 K 的每个扩充的定理，在这扩充中 $(E7')$，$(E8')$ 和 $(E9')$ 是公理. 推导同样的结果成立，如果 $\mathscr{A}(x_2)$ 是对 $\mathscr{A}(x_1)$ 中的 x_1 的多于一次的自由出现用 x_2 代入而得.

4. 在命题 5.6 的证明中，求证 $\hat{A}_i^n$ 的定义是合式定义的，也就是说，如果 $y_1, \cdots, y_n \in D_M$, $z_1, \cdots, z_n \in D_M$，并且 $[y_i]=[z_i]$ $(1 \leqslant i \leqslant n)$，那么 $\overline{A}_i^n(y_1, \cdots, y_n)$ 成立，当且仅当 $\overline{A}_i^n(z_1, \cdots, z_n)$ 成立.

5. 怎样用带等号的一阶系统的一个公式去表达"恰恰存在 2 个…使得…".

6. 令 $\mathscr{A}$ 是包含项 $t_1, \cdots, t_n$ "自由"的一个公式，所谓'自由'的意义是，在这些项内的任一项中一个变元的每次出现在 $\mathscr{A}$ 中都是自由的. 令 S 是 $K_{\mathscr{L}}$ 的一个扩充，包括 $(E7')$，$(E8')$ 和 $(E9')$ 为公理. 证明，对任意一个不包含在 $\mathscr{A}$ 中约束出现的变元的项 u，

$$\vdash_S ((t=u) \to (\mathscr{A}(t_1, \cdots, t_k, \cdots, t_n) \to \mathscr{A}(t_1, \cdots, u, \cdots, t_n))).$$

5.3 群论

群论也许是最普通的数学分支，它是精确地建立在最简单的公理组的基础之上的，因此，让我们来利用这个"数学背景"来说明，数学系统怎样呈现为 $K_{\mathscr{L}}$ 的扩充的.

首先，我们要刻划一个适当的一阶语言 $\mathscr{L}$，为此我们令 $\mathscr{L}_G$ 是带有以下符号库的一阶语言.

变元	$x_1, x_2 \cdots$
个体常元	a_1(单位元)
函数字母	f_1^1, f_1^2(逆运算和乘法运算)
谓词字母	$=$
括号	(,),
逻辑符号	$\forall, \sim, \to$.

现在定义 $\mathscr{G}$ 为 $K_{\aleph_0}$ 的扩充，它的固有公理是 $(E7)$，$(E8)$ 和 $(E9)$ 的一切适当的实例，以及下列的：

$(G1)$ $f_1^2(f_1^2(x_1, x_2), x_3) = f_1^2(x_1, f_1^2(x_2, x_3))$ （结合律）

$(G2)$ $f_1^2(a_1, x_1) = x_1$ （左单位元）

$(G3)$ $f_1^2(f_1^1(x_1), x_1) = a_1$ （左逆元）

如前，对每个自由变元，在这些公理中要不要包括全称量词是无关紧要的，一个等价的公理组将是它们的全称闭公式。

$(G1)$，$(G2)$ 和 $(G3)$ 只是通常群公理的转译．$(G2)$ 和 $(G3)$ 通常陈述为："存在一个左单位元"和"存在一个左逆元"的形式．我们这里的公理，并不明文断定存在性．他们只是说 a_1 和 $f_1^1(x_1)$，当在一模型中解释时，必然具有那适当的性质．由于在这个系统的任何模型中 a_1 和 f_1^1 都有解释，从而单位元和逆运算将自动存在，故断定存在性没有必要，类似地，关于群运算的封闭性的公理，这里也并不必要，因为 f_1^2 在模型中的解释，必然是一个在这模型的域中取值的二元函数．

给出了这样一个群论系统后，我们能够把有关初等群论的结果在代数教科书中的任何标准证明，转换为在这个系统中的一个形式证明．这样的一个程序，很少有实际用处，因为在 $\mathscr{G}$ 中的一个形式证明必然更为复杂，大量的纯粹操作步骤将掩盖所含的直观观念，如下例所示．

例 **5.8**

在任何有单位元 e 的群 G 中，$e(ee) = e$．与此相应，让我们给出以下公式在系统 $\mathscr{G}$ 中的一个形式证明：

$$f_1^2(a_1, f_1^2(a_1, a_1)) = a_1.$$

(1) $f_1^2(a_1, x_1) = x_1$ $(G2)$

(2) $(\forall x_1(f_1^2(a_1, x_1) = x_1)$ (1)，概括

(3) $(\forall x_1)(f_1^2(a_1, x_1) = x_1) \rightarrow (f_1^2(a_1, a_1) = a_1)$ $(K5)$

(4) $f_1^2(a_1, a_1) = a_1$ (2)，(3)分离

(5) $(\forall x_1)(f_1^2(a_1, x_1)=x_1)\rightarrow(f_1^2(a_1, f_1^2(a_1, a_1))$
$=f_1^2(a_1^2, a_1))$ (K5)

(6) $f_1^2(a_1, f_1^2(a_1, a_1))=f_1^2(a_1, a_1)$ (2), (5)分离

(7) $(f_1^2(a_1, a_1)=a_1)\rightarrow(ff_1^2(a_1, f_1^2(a_1, a_1))$
$=f_1^2(a_1, a_1)\rightarrow f_1^2(a_1, f_1^2(a_1, a_1))=a_1)$ (E9)

(8) $(f_1^2(a_1, f_1^2(a_1, a_1))=f_1^2(a_1, a_1)$
$\rightarrow f_1^2(a_1, f_1^2(a_1, a_1)=a_1)$ (4), (7)分离

(9) $f_1^2(a_1, f_1^2(a_1, a_1)=a_1$ (6), (8)分离

与此相比,对任意群 $e(ee)=e$ 的标准证明,要浅显得多. 复杂一些的关于群的结果,反映在 $\mathscr{G}$ 中的形式将更加复杂. 举出特例不是很值得的,但是,试图在 $\mathscr{G}$ 中去证明公式

$$f_1^2(x_1, a_1)=x_1,$$

将进一步对所含复杂性有一个概念. 这公式相应于群的性质. 左单位元也是右单位元.

▷ 理应清楚,任何群 G 都是系统 $\mathscr{G}$ 的一个标准模型,当 a_1 解释为 G 的单位元, f_1^1 是逆运算, f_1^2 是群运算并且 $=$ 解释为相等时. 但是还有另外的模型,正如我们将要看到的.

例 5.9

构造系统 $\mathscr{G}$ 的一个解释 I 如下: 令 D_I 是整数集 Z, a_1 解释为 0,

$$\bar{f}_1^1(x)=-x \quad x\in Z$$

和

$$\bar{f}_1^2(x, y)=x+y \quad x, y\in Z,$$

并且令 $=$ 是同余 $(\bmod m)$, m 是某一固定的正整数. (虽然我们把 $=$ 用作 $\mathscr{L}_G$ 的符号,正如我们在上面所见,它并不一定总要解释为实际上的相等). I 是 $\mathscr{G}$ 的一个模型. 为了证明这点,我们必须证明 $\mathscr{G}$ 的每一公理在 I 中为真. 而 $(K1)$—$(K6)$ 的真,不必要求证明,因为它们是逻辑有效的. $(E7)$, $(E8)$ 和 $(E9)$ 为真,恰如在例 5.5 中的证明. 让我们集中注意 $(G1)$, $(G2)$ 和 $(G3)$.

(G1) 解释为

$$(x+y)+z\equiv x+(y+z) \pmod m.$$

(G2) 解释为

$$0+x\equiv x \pmod m.$$

(G3) 解释为

$$-x+x\equiv 0 \pmod m.$$

这些都是真句子，对任何 $x, y, z\in Z$. 因此 I 是 $\mathscr{G}$ 的一个模型. 但是，I 并不是一个群. 事实上它涉及同余的外部关系. 但是，对群论和数论有经验的读者将认识到，在幕后有一个等待发现的群. 从模型 I，通过命题 5.6 中的程序，我们能够构造一个标准模型 I^*. I^* 域是整数同余类 $(\bmod m)$ 的集合，a_1 解释为 O_m（含 O 的类），f_1^2 解释为 $+$（可在同余类上合式定义），f_1^1 解释为"加性逆元"（也可合式定义），$=$ 解释为相等. I^* 是标准模型，并且它是一个群.

△一般来说，任一个群都是群论的形式系统的一个标准模型，反之系统的任何标准模型一定是一个群. 所以，为了使系统具有数学意义，我们必须把注意限制于标准模型. 也许这是不幸的，但是，不可能给出相等的公理，它迫使其解释是实际的相等. 也就是说，总可以构造一个模型，其中 $=$ 将被解释为其它等价关系.

构造群论的形式系统，并不是为了得到有关群和它的元素的结果提供捷径和新方法. 正如我们已经见到的，在 $\mathscr{G}$ 中的证明方法是如此笨拙，以致对此目的毫无用处. 通过描述系统 $\mathscr{G}$ 我们所得到的是，我们已经使数学家在群论范围中所用的一切假设和程序精确化和明确化，包括逻辑的与数学的. 按这种方式，我们已经澄清了这一部分的数学.

上面已对群作了较详细的处理，类似的处理可施之另一些抽象代数系统，例如，环，域，向量空间，格，布尔代数等. 它们的每一个已知都可用有限公理组刻划其特征，这些也都可以很容易地转

译到一个适当的形式语言中去. 事实上，每个能用一组公理刻划其特征的数学领域，都可以用类似的方式加以处理. 例如，欧几里得几何可以建立在一组比较复杂和冗长的公理之上，一个形式系统必将包括专门解释为"是一个点"，"是一条线"，"相交"等等的谓词字母. 也可以对实数的公理系统加以描述，通过完备有序域的公理组进行.

当按这种方式加以处理时，有两个数学领域特别重要. 他们是算术和集合论. 对其中任一主题作完整的叙述都需要一整本书，我们将只是试图说明为什么它们具有一种特殊的地位. 一致性问题，或者不同假设之间关系的问题，或者对基本假设的看法和使用等问题，只有在一个明确的形式系统中才可能得到阐明. 集合论是一切数学的基础，所以它的逻辑基础具有压倒一切的重要性. 算术是数学的一个初等片断，它的意义在于用来说明下面论点的方法，要寻找一个能检验任何数学命题的形式系统必将是徒劳的. 任何在其中能实施普通算术的数学系统，都不可能是这样的一个万能系统，因为算术(在一个将予以精确化的意义下)的任何一致的扩充的定理集，必定至少有一真命题未被包括进去. 某些并非算术的扩充的系统(如群论)就不具有这种性质. 但是一个包括数学分析的系统，或者企图把整个数学包括进去的系统将一定包括算术，所以它们也将具有这个属性. 这个问题在第六章中将相当详细地加以讨论.

练习

7. 用不包含个体常元的形式语言去描述一个群论的一阶系统 $\mathscr{G}'$. 用一包含个体常元但没有函数符号的形式语言作同样的事情.

8. 一个半群是一个集合，在这集合上定义了一个满足结合律的二元运算. 描述半群理论的一个一阶系统 $\mathscr{S}$，使得练习 7 中的

系统 $\mathscr{G}'$ 是 $\mathscr{S}$ 的一个扩充.

9. 如果在系统 $\mathscr{G}'$(练习 7 中的)中通过在语言中补加单一的个体常元 a_1(但并不补加公理), 给系统带来的影响是什么? 在语言中补加了个体常元的整个序列 a_1, a_2, … 后, 会带来什么影响?

10. 描述一个一阶系统, 它的标准模型是一切无限群. 一阶系统能否以一切有限群为它的标准模型?

11. 详细地描述环论的一个一阶系统, 即列出适当的一阶语言的符号库, 并且写出一组公理或公理模式. 描述这个系统的一个不是环的模型.

12. 令 $\mathscr{F}$ 是域论的一个一阶系统. 这个系统的标准模型是域, 它们可以有 0 和任何素数 p 为其特征. 证明, 如果 $\mathscr{F}$ 的语言的闭公式 $\mathscr{A}$ 在一切特征为 0 的域中为真, 那么存在一个正整数 n, 使得 $\mathscr{A}$ 在一切特征为素数 $p(p>n)$ 的域中也为真.

13. 令 $\mathscr{F}$ 如在练习 12 中所描述, $\mathscr{A}$ 是一公式, 使得对一切大于某个 n 的 p, 存在着特征为 p 的一个域, 在其中 $\mathscr{A}$ 是真的. 证明: 存在一个特征为 0 的域, 在其中 $\mathscr{A}$ 是真的.

5.4 一阶算术

我们来展开在第三章中首次引入的在算术解释 N 中所涉及的思想. 作为语言 $\mathscr{L}_N$, 我们取个体变元 x_1, x_2, …, 个体常元 a_1(表示 0), 函数字母 f_1^1, f_1^2, f_2^2(表示后继, 和及积), 和谓词符号 $=$ 连同括号, 联结词和量词. 让我们用 $\mathscr{N}$ 表示一阶系统, 它是 $K_{\mathscr{L}_N}$ 的一个扩充, 通过补加公理 (E7), (E8) 和 (E9) 的所有适当的实例, 以及下面 6 条公理和一条公理模式而得到的.

(N1) $(\forall x_1)\sim(f_1^1(x_1)=a_1)$.

(N2) $(\forall x_1)(\forall x_2)(f_1^1(x_1)=f_1^1(x_2)\rightarrow x_1=x_2)$.

(N3) $(\forall x_1)(f_1^2(x_1, a_1)=x_1)$.

(N4) $(\forall x_1)(\forall x_2)(f_1^2(x_1, f_1^1(x_2)) = f_1^1(f_1^2(x_1, x_2)))$.

(N5) $(\forall x_1)(f_2^2(x_1, a_1) = a_1)$.

(N6) $(\forall x_1)(\forall x_2)(f_2^2(x_1, f_1^1(x_2)) = f_1^2(f_2^2(x_1, x_2), x_1))$.

(N7) $\mathscr{A}(a_1) \to ((\forall x_1)(\mathscr{A}(x_1) \to \mathscr{A}(f_1^1(x_1)))$
$\to (\forall x_1)\mathscr{A}(x_1))$,

对 $\mathscr{L}_N$ 的每个公式 $\mathscr{A}(x_1)$, x_1 在其中自由出现.

记法 目前我们还不知道, 例如 f_1^2 在任何标准模型中, 是否一定解释为加法(或者是一个与和函数具有同样性质的函数), 但是, 如果我们修改 $\mathscr{L}_N$, 直接地通过用符号 $+$, $\times$ 和 $'$ 相应地去代替 f_1^2, f_2^2 和 f_1^1, 那么将使系统 $\mathscr{N}$ 更为清楚, 并且上述公理将更易理解. 为了明确起见, 我们将写出

$t_1 + t_2$ 代表 $f_1^2(t_1, t_2)$,

$t_1 \times t_2$ 代表 $f_2^2(t_1, t_2)$,

和 t' 代表 $f_1^1(t)$

t, t_1, t_2 是任意项. 我们也将使用符号 0 而不用 a_1. 这样做时带来的危险必须再次加以强调. 这样做时, 我们切不可假设, 这些新的符号必定总是解释成他们标准地表示的函数和对象.

使用这些符号, 公理(N1)－(N7)可以重写如下:

(N1*) $(\forall x_1) \sim (x_1' = 0)$.

(N2*) $(\forall x_1)(\forall x_2)(x_1' = x_2' \to x_1 = x_2)$.

(N3*) $(\forall x_1)(x_1 + 0 = x_1)$.

(N4*) $(\forall x_1)(\forall x_2)(x_1 + x_2' = (x_1 + x_2)')$.

(N5*) $(\forall x_1)(x_1 \times 0 = 0)$.

(N6*) $(\forall x_1)(\forall x_2)(x_1 \times x_2' = (x_1 \times x_2) + x_1)$.

(N7*) $\mathscr{A}(0) \to ((\forall x_1)(\mathscr{A}(x_1) \to \mathscr{A}(x_1')) \to (\forall x_1)\mathscr{A}(x_1))$.

对每个公式 $\mathscr{A}(x_1)$, 其中 x_1 自由出现.

注记 5.10

(a) 熟悉皮阿诺公设的读者将认识(N1), (N2)和(N7). 皮

阿诺公设是早在我们正式研究形式系统以前就首次被明确叙述的自然数系统的一组公理．它们是：

1．0是自然数．

2．对每个自然数 n，存在另一自然数 n'．

3．没有自然数 n，使得 n' 等于 0．

4．对任意的自然数 m 和 n，如果 $m'=n'$，那么 $m=n$．

5．对任何含 0 的自然数集 A，如果对任何 $n\in A$ 有 $n'\in A$，那么 A 包含每个自然数．

注意，前面两个公设和我们系统 $\mathscr{N}$ 中的任何公理都不对应．我们并不需要这两条，因为我们在语言 $\mathscr{L}_N$ 中已经把符号包括进去（0 和 $'$，或 a_1 和 f_1^1），它们在任何模型中都一定有解释，以至在任何模型中元素 $\bar{a}_1$ 总存在，对每个 x 也必定存在元素 $\bar{f}_1^1(x)$．

(b) (N7) 和皮阿诺第 5 公设之间的对应并非严格的．两者都是数学归纳原理的说法．但是，因为在 $\mathscr{N}$ 中我们被严格限制于使用一阶语言 $\mathscr{L}_N$，公理 (N7) 不可能象皮阿诺第 5 公设那样强或包括的范围那样广．理由是，皮阿诺第 5 公设含有一个二阶量词"对于任何的自然数集"，而在我们的一阶语言中，不能表述这句话．我们所能做的最多是用公理模式的概念，使得我们在效果上有一量词"对每个公式 $\mathscr{A}(x_1)$，其中 x_1 自由出现"．注意，这样的一个公式 $\mathscr{A}(x_1)$，在任何解释中都决定了一个集合，即满足 $\mathscr{A}(x_1)$ 的解释域中的所有元素 v_1 的集．（更精确一点，是解释域的所有元素 v_1 的集合，使得每个使 $v(x_1)=v_1$ 的赋值 v 满足 $\mathscr{A}(x_1)$ 的）．

如果，我们在 $\mathscr{N}$ 的模型范围中考虑，那么，公理模式 (N7) 的每个实例都对应着关于一个特殊集的皮阿诺第 5 公设的断定．但是，仍然有本质上的差别．公理模式 (N7) 的实例形成一个 $\mathscr{L}_N$ 的公式的可数集．皮阿诺第 5 公设是关于自然数的一切集合的命题，而它们的汇集是不可数的．这样，(N7) 是归纳原理的一个很

受到限制的形式，因为它只讲到一个模型域的子集的可数汇集，这些子集就是被上面描述的 $\mathscr{L}_N$ 的公式所表现的.

(c) 皮阿诺公设并没有提及和与积. 这些函数可以用归纳原理借后继函数加以定义，但是为方便起见，我们把表示这些的符号包括到形式语言中去. 这样做了以后，公理(N3)～(N6)就是必需的，以便保证在任何模型中，这些符号的解释具有所要求的性质.

▷ 数学上来看，这种情况和群论的情况之间是有基本的差别的. 群论的形式系统，允许具有多个不同的标准模型，即所有的群，算术系统 $\mathscr{N}$ 按我们的意图则只有一个标准模型，就是自然数集合，因为，我们希望在系统中作为定理出现的就是自然数的性质. 群论所处理的，是在所有群中都成立的一般结果，相反数论所处理的是关于特殊集，即自然数集的结果. 因此，提出是否存在不同于自然数集的 $\mathscr{N}$ 系统的标准模型的问题是自然的. 另一个自然会提出的问题是：这系统是否足够的"强"，以至包括所有我们希望其为定理的公式，也就是所有对应于有关自然数的真命题的公式，作为它的定理. 这两个问题并非没有联系，我们不久就将看到.

某些读者可能熟悉皮阿诺公设唯一决定自然数集的标准证明. 令 N 和 M 是皮阿诺公设的"模型". 那么，$0\in N$，并且 $0\in M$. 令 A 是 N 的元素组成的集且这些元素也属于 M. 因此 $0\in A$. 还有，如果 $n\in A$，那么 $n\in N$ 和 $n\in M$，所以 $n'\in N$ 和 $n'\in M$，且 $n'\in A$. 因而，据皮阿诺第5公设，A 由一切自然数组成，即 $A=N$，且 $N\subseteq M$. 类似地可证 $M\subseteq N$，所以 $M=N$. 在这个证明中，第5公设的应用是根本的，而我们在前面却已注意到，(N7)并不严格地与这个公设对应. 事实上，上述证明不能转译为 $\mathscr{N}$ 中的证明. 所以，这里没有希望得到有关 $\mathscr{N}$ 的第一个问题的否定回答.

现在让我们谈一谈这个问题：$\mathscr{N}$ 是否完全？也就是说，对 $\mathscr{L}_N$ 的每个闭公式 $\mathscr{A}$，$\mathscr{A}$ 和 $\sim\mathscr{A}$ 是否总有一个是 $\mathscr{N}$ 的定理？这个

问题的意义初看并不明显，但是它和上面两个问题有联系。如果 $\mathscr{N}$ 不完全，那么它在上述意义下就不是一个足够强的系统，因为这时将存在一个闭公式 $\mathscr{A}$，使得 $\mathscr{A}$ 和 $\sim\mathscr{A}$ 都不是 $\mathscr{N}$ 的定理。现在，在任何解释之下，一个闭公式非真即假，所以在解释 N 下，或者 $\mathscr{A}$ 真，或者 $\mathscr{A}$ 假，在后面的情况下就是 $(\sim\mathscr{A})$ 真。$\mathscr{A}$ 在 N 的解释是一个关于自然数的命题，而在直觉上，$\mathscr{A}$ 或 $(\sim\mathscr{A})$ 总有一个解释是关于自然数的真命题。但是 $\mathscr{A}$ 和 $(\sim\mathscr{A})$ 却都不是 $\mathscr{N}$ 的定理。因此，如果 $\mathscr{N}$ 不完全的话，那么将存在一个关于自然数的真命题，而它在 $\mathscr{N}$ 中对应的公式却不是 $\mathscr{N}$ 的定理。一切在模型 N 中为真的公式应该都是 $\mathscr{N}$ 的定理，这是我们所希望的，并且也是构造系统 $\mathscr{N}$ 时的本来目标的一部分。但是，如果 $\mathscr{N}$ 不完全，情况就并非如此了。

如果存在一合式公式 $\mathscr{A}$，使得 $\mathscr{A}$ 和 $(\sim\mathscr{A})$ 都不是 $\mathscr{N}$ 的定理，那么（在 $\mathscr{N}$ 本身是一致的情况下）我们就可以恰如第四章所做的，得到 $\mathscr{N}$ 的两个一致的扩充，通过对第一个补加 $\mathscr{A}$ 为新公理，第二个补加 $(\sim\mathscr{A})$ 为新公理。每个扩充都将有一个标准模型（命题 5.6），这些模型无疑是 $\mathscr{N}$ 的本质上不同的模型，因为在一个模型中 $\mathscr{A}$ 为真，而在另一模型中 $(\sim\mathscr{A})$ 为真。这样，如果 $\mathscr{N}$ 是不完全的话，就必定存在一个 $\mathscr{N}$ 的标准模型，它和那个专指的标准模型并不相同。

$\mathscr{N}$ 不完全这一事实是哥德尔首先获得的重大成果之一。实际上，他证明了一个更强一些的结果，而以此作为其特例。第六章将专门讨论证明中所涉及的思想和方法，同时也考察一些它的推论。在此之前我们先考察较早提到过的另一重要的'数学领域'，即形式集合论。

练习

14. 一个算术的形式系统 $\mathscr{N}'$ 可规定如下。语言包括 f_1^1,

$f_1^2, f_2^2, A_1^1, a_0, a_1, a_2, \cdots$ 再加括号，联结词和量词．公理如在 $\mathscr{N}$，但补充 $f_1^1(a_i)=a_{i+1}$，对每个 $i>0$．直观上很清楚 N 是这个系统的一个标准模型，假如对每个正整数 k，a_k 通过 $k-1$ 加以解释（a_0 的解释是不重要的．）现在考察由 $\mathscr{N}'$ 通过补加所有公式 $\sim(a_0=a_i)$，对 $i>0$ 为公理而得的系统．证明：这个新系统是一致的，从而有一标准模型．这样的一个模型是怎样和 N 不同的呢？

5.5 形式集合论

今天数学的基础是建立在集合论之上的，从本世纪初以来数学家就已研究了必须作出的关于集合的基本假设（即公理），和在此假设上能建立一切数学的方法．开展一种形式集合论的好处在于能使假设明确化，能提供对这些假设进行评判的机会，并且能揭示它们之间的相互依赖关系．我们即将描述形式集合论的一个系统．还有其他的系统，但是我们的这个系统是标准的系统之一，而且也许是用我们已经讨论的概念，最容易描述的．对数学的集合论基础不熟悉的读者可能会对这些公理本身感到困难，但是，为了完备起见，和为了使读者对它们的性质有一点认识我们还是把它们写在这里．以后遇到的并不依赖它们．在描述系统和指出怎样由它开展集合论之外，我们没有篇幅讲更多的东西．

我们要描述的系统称为 ZF 系统．名字来自于 1905 年第一个陈述了集合论公理组的策麦洛（Ernst Zermelo），和 1920 年对它作过修改的弗兰克尔（Abraham Fraenkel）．

对 ZF 适当的一阶语言，包含通常的变元、括号、联结词和量词，还有谓词符号 $=$ 和 A_2^2（没有函数符号或常元）．A_2^2 的意图解释是 $\in$，属于关系．确实，和在 $\mathscr{L}_N$ 的情况时所警告的一样，我们将把 $\in$ 看作是专门代表 A_2^2 的语言符号，用 $t_1\in t_2$ 代替 $A_2^2(t_1, t_2)$，对任何项 t_1 和 t_2．注意，没有个体常元和函数字母意味着，项只能是变元，原子公式只能是 $x_i=x_j$ 或 $x_i\in x_j$ 这样的形式．这似乎可

能限制过多了，但是，我们引进的公理将保证，形式系统能真正反映朴素集合论的充分的一般性，我们将能对集合论的标准概念，诸如空集，并集，幂集等相应地引进被定义符号.

ZF 被定义为 $K_{\mathscr{L}}$（这里 $\mathscr{L}$ 如上面所描述）的扩充，通过补加(E7)，(E9)的一切适当实例(E8 没有非平凡实例)，和下列($ZF1$)到($ZF8$)为公理.

($ZF1$)　$(x_1=x_2\leftrightarrow(\forall x_3)(x_3\in x_1\leftrightarrow x_3\in x_2))$.

这称为外延公理，它的意图含义是：两个集合相等，当且仅当它们有相同的元素. 注意从左到右的蕴涵在(E9)已经给出，但是如果我们在这里用两方蕴涵，会使这条公理的意义更清楚些.

($ZF2$)　$(\exists x_1)(\forall x_2)\sim(x_2\in x_1)$.

这是空集公理，因为在意图的解释下，它保证了一个没有成员的集合的存在. 在任何标准模型下将只能存在一个这样的集，这是($ZF1$)的一个推论. 因此我们可以在语言中引进一个符号 $\varnothing$，充当一个个体常元，于是合式公式$(\forall x_2)\sim(x_2\in\varnothing)$是($ZF2$)所取的形式.

记法　我们引进符号 $\subseteq$ 作为下列的简写：

$$(t_1\subseteq t_2)\ \text{代表}\ (\forall x_1)(x_1\in t_1\rightarrow x_1\in t_2).$$

其中 t_1 和 t_2 是任意项.

($ZF3$)　$(\forall x_1)(\forall x_2)(\exists x_3)(\forall x_4)(x_4\in x_3$
$\leftrightarrow(x_4=x_1\vee x_4=x_2))$.

这是配对公理. 给出任何集合 x 和 y，总存在集合 z，它的成员是 x 和 y. 这个公理也断定了存在性，为方便起见我们引进符号 { 和 } 到语言中，以表示这个已断定其存在的对象. $\{x_1, x_2\}$ 将被看作一个项，而($ZF3$)于是断定了 $x_4\in\{x_1, x_2\}\leftrightarrow(x_4=x_1\vee x_4=x_2)$.

($ZF4$)　$(\forall x_1)(\exists x_2)(\forall x_3)(x_3\in x_2$
$\leftrightarrow(\exists x_4)(x_4\in x_1\wedge x_3\in x_4))$.

这是并集公理. 给出任何集合 x，总存在一个集合 y，它以 x 的一

切元素的元素为元素.

记法 我们用$\bigcup x_1$表示那个已由$(ZF4)$断定其存在的对象. 它实际上是一个项, 所以$\bigcup$实际上是一个一元函数符号. 因而我们可以通过

$$\mathscr{D}(t_1 \cup t_2) \text{ 表示 } \bigcup\{t_1, t_2\}$$

来引入$\bigcup$.

(ZF5) $(\forall x_1)(\exists x_2)(\forall x_3)(x_3 \in x_2 \leftrightarrow x_3 \subseteq x_1)$.

这是幂集公理. 给出任意x, 总存在一集合y, 它以x的一切子集为元素.

$(ZF6)$ $(\forall x_1)(\exists_1 x_2)\mathscr{A}(x_1, x_2) \rightarrow$
$(\forall x_3)(\exists x_4)(\forall x_5)(x_5 \in x_4 \leftrightarrow (\exists x_6)(x_6 \in x_3 \wedge \mathscr{A}(x_6, x_5)))$.
对每个合式公式$\mathscr{A}(x_1, x_2)$, 其中x_1, x_2自由出现(其中我们还可以不失一般性地假设, 量词$(\forall x_5)$和$(\forall x_6)$并不出现).

这是替换公理模式. 如果公式$\mathscr{A}$决定了一个函数, 那么对于任何集合x, 总存在一个集y, 它以x的成员在这个函数之下的象作为成员.

$(ZF7)$ $(\exists x_1)(\varnothing \in x_1 \wedge (\forall x_2)(x_2 \in x_1 \rightarrow x_2 \cup \{x_2\} \in x_1))$.
(注意: $\{x_2\}$是上面定义过的$\{x_2, x_2\}$的简写.).

这是无限公理. 它断定, 在任何模型中一个无限集的存在. 如果它不包括在公理之中, 势将无从保证形式系统和包括无限集的朴素集合论有任何联系.

$(ZF8)$ $(\forall x_1)(\sim x_1 = \varnothing \rightarrow (\exists x_2)(x_2 \in x_1 \wedge$
$\sim(\exists x_3)(x_3 \in x_2 \wedge x_3 \in x_1)))$.

这是基础公理. 每个非空集x包含有一个与x无公共元素的成员. 这是一条技术性的公理, 放在这里是为了避免与直觉相反的异常情形, 如一个集合可能是它自身的成员.

ZF是一集合论的形式系统. 这样选择公理是为了使得在标

准模型中，形式符号的解释表现得和集合一样．有些公理在直观上比其它一些较强些，但是这8条在描述有关集合的基本真理上已经受了时间的检验．

ZF 按下面的方式可以作为数学分析的基础．在它是一致的系统的假设之上，我们知道一个标准模型的存在．可以证明，在任何这样的模型中，存在着具有通常数系所有属性的集合．详细地叙述是冗长的，不可能在这里进行．例如，对算术系统 $\mathscr{N}$ 的一个模型，可以按下述方式定义为 ZF 的一个模型的一个子集．ϕ 在 ZF 的这个模型中的解释是 $\varnothing$．因此 $\{\varnothing\}$ 是模型的一个不同的元素（这集合仅有的元素是 $\varnothing$），而 $\{\varnothing, \{\varnothing\}\}$ 是另一个元素（这个集有两个元素，$\varnothing$ 和 $\{\varnothing\}$）．这是一个归纳过程的开始，它生成一个集合的序列．生成规则是，对于序列中的每个 x，它的后继是 $x\cup\{x\}$．容易验证，这个序列的第 $(k+1)$ 个成员有 k 个元素，而定义自然数 k 为这第 $(k+1)$ 个成员是可能的．我们已经见到，其它的算术运算能用后继函数加以定义．因此公理 (N1)…(N7) 是定义和 ZF 公理的推论．注意，为了保证这个序列的一切成员的汇集是我们的 ZF 的标准模型的一个元素，($ZF7$) 是不可少的．照这样，ZF 的每个标准模型都包含 $\mathscr{N}$ 的一个标准模型．

有数学修养的读者可能熟知如何从自然数出发，通过代数的过程，可以构造整数系，有理数系，实数系和复数系的方法．所有这些程序都可以在 ZF 中进行．那里需要大量的详尽论证，但是最终结果不外乎是确认，ZF 的每个标准模型都包含一个与复数集在外貌和表现上相像的集合．（当然这个集合有一个和实数集相像的子集）．

除了把分析建立在公理基础上之外，在本世纪初，对公理集合论的研究还有着另外的刺激因素，这就是从直觉上证明（如果可能的话），在数学中使用某些原理的正确性．人们的注意后来集中到两个特殊的原理上，选择公理（大家知道它有几个等价的陈述）和

连续统假设。研究这些原理自那时以来的某些历史，是很有启发的。有些数学家已经把它们作为集合论的补充公理，另一些把它们或者作为直觉上可疑的，或者甚至作为是错误的。

选择公理是：

(AC) 对任何非空集合 x，总存在一个集合 y，它和 x 的每个成员恰有一个公共元素。

（最熟知的两个等价表述是：曹恩（Zorn）引理；如果在一个偏序集上的每个链有一上界，那么存在这个集合的一个最大元素，和良序原理；每个集合都可良序化。）

连续统假设是：

(CH) 实数的每个无限集，或者是可数的，或者与一切实数组成的集有相同的基数。（两个集有相同基数，如果在它们间存在一个双方一一对应。）

因为数学家对这两个原理的可接受性持不同看法，当然就会提出这样的问题：他们是真实的吗？跟着的一个问题是：如果这些原理能被证明，那么这些证明所依据的原理是什么呢？策麦洛和弗兰克尔（以及其他人），列出他们所认为的集合论基本原理，问题成为：(AC)和(CH)是否能作为集合论系统 ZF 的定理而被推导出来，如果不能够，那么将一个或两个包括进来作为补充公理将是一致的吗？

哥德尔（在 1938 年）通过对集合论的形式系统所作的技术性考察，对其中一个问题作了回答。(AC)和(CH)同 ZF 是一致的。换言之，它们可以作为补加的公理，不会引出任何矛盾。思想是很简单的。在 ZF 是一致的假设下，他制造了一个模型，在这个模型中(AC)和(CH)是真的。因而，根据命题 4.41 和 4.42，补加(AC)或(CH)为公理后得到的两个系统都是一致的。顺便提一下，他也证明了，通过同时补加(AC)和(CH)为公理而得的系统也是一致的。

很久以后柯亨 (Cohen 在 1963 年)回答了另一问题，他证明 (AC) 和 (CH) 不能作为 ZF 的定理而推演出. 思想也是简单的，尽管证明并不简单. 柯亨构造了 ZF 的一个模型，在其中 (AC) 和 (CH) 的否定是真的. 现在，倘若 (AC) 和 (CH) 是 ZF 的定理，那么它们在每个模型中都将是真的，但是一个公式和它的否定不可能在任何模型中都是真的.

从这一切引出的结论是，(AC) 和 $\sim(AC)$ 都不是 ZF 的定理，它们之中任一个都可一致地补加为新公理. 对 (CH) 和 $\sim(CH)$ 也有类似的结果. 形式集合论得到了澄清，(AC) 和 (CH) 的可接受或不可接受，必然是一个直觉的问题，或是某些有待发现的数学原理的问题，该原理在将来被接受为公理之后就可确认或否认 (AC) 和 (CH). (顺便提一下，哥德尔和柯亨的工作也证明了：(AC) 和 (CH) 彼此之间也是独立的. 每一个都不是把另一个作为新公理补加到 ZF 后所得的系统的定理.)

ZF 的各种模型，$\in$ 的不同的可能解释，公理独立性，ZF 的定理类和集合论中"真"命题类之间关系，所有这些的研究是数学的一个丰富的领域，我们除了作如下的一些注记外，将不再讨论.

练习

15. 如果语言中包括了符号 a_1 (表示 $\varnothing$)，f_1^2(表示 $\{,\}$)，和 A_3^2 (表示 $\subseteq$)，这时集合论形式系统的公理组必须进行怎样的修改呢？

令自然数集如书中那样被定义为，$0=\varnothing$，且 $n+1=n\cup\{n\}$ 在 ZF 的一个模型中. 证明：在 ZF 的语言的这样一个解释中，即其域是这个集合，并且 $\in$ 和 $=$ 分别解释为实际的集合的属于和实际的相等，那么公理 $(ZF1)$，$(ZF2)$，$(ZF4)$ 和 $(ZF8)$ 是真的，而 $(ZF3)$，$(ZF5)$ 和 $(ZF7)$ 是假的. 又 $(ZF6)$ 是真还是假？

5.6 一致性和模型

任何一个一阶系统是一致的，当且仅当它有一个模型. 因此有可能这样论证：我们描述过的那些数学系统是一致的，因为在每一种情形，我们已经在公理组中反映着一个意图中模型的属性. 但是，锐敏的读者也许已经担心到我们的论证中可能有一循环，它体现在第三章中把解释作为一个带有某些运算和关系的集的定义上. 那么，我们怎样才能谈论集合论形式系统 ZF 的解释或模型而不陷入循环呢？答案应求之于前面提到过的元理论的思想，这元理论体现了证明关于形式系统的结果而必须作的假设. 例如当我们论述系统 $\mathcal{N}$ 时，可能用 ZF 作为元理论，因为在已经指出的意义下 ZF"包含" $\mathcal{N}$. 但是，当我们讨论 ZF 时，我们可以说已经达到了路线的尽头. 本来，ZF 是要适合于集合论的，从而也适合于一切数学. 但是，为了研究 ZF 我们需要不是 ZF 一部分的数学方法. ZF 的一个解释的概念，只能用关于"实"集的某些直觉的元理论加以定义. ZF 的一个模型的元素应该看作是解释 ZF 的符号的集. 但是 ZF 的模型的域，尽管它可能是一"实"集，却不能是与那个域的元素具有同样意义的集，因为它不是 ZF 的一个符号的解释.

在这些问题上，无疑存在着一定的直觉上和语义上的困难，因为这个缘故利用模型作的一致性证明一般地被认为是不适切的. 更好的方法如下述，给出两个一阶系统 S 和 S^*，我们试图证明，在 S^* 有一个模型的假设下，可以构造 S 的一个模型. 这将给出一个相对一致性的证明. 在下面一个情况中这几乎是平凡的.

命题 5.11

令 S^* 是 S 的一个扩充(在定义 4.32 中所用的"扩充"). 那么如果 S^* 是一致的，则 S 也是一致的.

证明　假设 S^* 是一致的，而 S 不一致. 那么对 S 的某个公

式 $\mathscr{A}$ 有 $\underset{S}{\vdash}\mathscr{A}$ 和 $\underset{S}{\vdash}(\sim\mathscr{A})$. 但是 $\mathscr{A}$ 也是 S^* 的一个公式；并且 S 中任何证明也是 S^* 的一个证明，所以 $\underset{S^*}{\vdash}\mathscr{A}$ 和 $\underset{S^*}{\vdash}(\sim\mathscr{A})$，这与 S^* 的一致性矛盾.

▷ 这是最容易处理的情况. 在 S^* 不是 S 在这个意义之下的扩充的情形中，例如两个系统的语言不相同情形，相对一致性的证明将比较困难，可能要从 S^* 的一个假设的模型真正构造出 S 的一个模型. 我们在证明 ZF 的一致性蕴涵 $\mathscr{N}$ 的一致性时，曾经粗略地给出过一个这样的构造.

ZF 是否一致是不知道的. 大部分逻辑学者相信它是一致的，但是任何证明它是一致的企图，将导致上面讲过的那种困难. 主要是，它将要求一个甚至比 ZF 包含得还要广泛的系统的一致性的假设. 确实，在企图否证一致性的方面并没有相应的困难. 为此所需要的一切，将只是一个公式 $\mathscr{A}$ 的特例，使得 $\mathscr{A}$ 和 $(\sim\mathscr{A})$ 都是 ZF 的定理. 上面已经暗示还不曾找到这样的公式. 七十年的无结果的探索是不存在这样的公式的证据，但是这绝不是结论性的.

最后，让我们注意关于 ZF 的模型的一个结果，它是命题 4.45 的推论. 但初看起来却似乎是矛盾的. ZF 是个一阶系统. 在 ZF 是一致的假设之下，命题 4.45 说 ZF 有一可数模型. 现在直觉上不可数集是存在的，所以为了包含这样的集，我们期待 ZF 的模型是不可数的. 这个表面上的悖论称为斯柯兰姆(Skolem)悖论，但是通过仔细地考察是什么构成一个模型，我们能够象下面那样逃避一个直接的矛盾.

说得详细一点，公理($ZF5$)被解释为"给出任何 x，总存在由 x 的一切子集组成的集". 如果 x 是一个无限可数集，那么根据集合论规则，x 有不可数个子集. 这样一个集 x 的一切子集组成的集，怎样会属于一个可数模型呢？ZF 的一个可数模型由集组成.

对于任何属于模型的"实"集 x（显然，必定有不属于模型"实"集），公理（$ZF5$）断定、属于模型的 x 的一切子集构成一个必定属于模型的集 y. 这个集 y 当看成"实"集时，将是可数的，但是当看成是模型的一个元素时，它将是不可数的、一个无限集是不可数的，如果它和自然数集之间不存在双方一一对应. 在模型中，y 和自然数集之间没有一一对应（所有"实"的这样的一一对应将以同样方式从模型中消失，犹如 x 的某些子集从模型中消失一样）.

第六章　哥德尔不完全性定理

6.1　引论

形式算术系统 $\mathscr{N}$ 是否完全？这个问题的意义在第五章中已经作过一些说明．在本章中，我们将描述一下由哥德尔所作出的 $\mathscr{N}$ 是不完全的证明．证明是高度技巧的，实际上我们将略去那些技术性最强的部分．但是由于两方面的原因我们还得较为详细地加以讨论．第一，因为这个结果对形式系统及其对数学基础的价值之研究有着基本的作用，因而搞清楚这种证明的方法，以及弄懂其中的概念是有意义的．第二，证明中引进了一些有意义的新概念，它们除这里直接要用外，还有广泛用处而本书的目的之一，就是要引进这些新概念，其中最重要的是递归函数和递归关系，哥德尔码数和可表达性．这些概念将在本章的随后几节中加以阐述，既是为了本身的目的，也为了用于哥德尔定理的证明．第七章将进一步说明递归性，对它的理解并不需要本章其它的节次的知识，故而对技术问题兴趣不大的读者可以删去第 2、4 和 5 节中详细叙述的方面，这不会影响以后的阅读．

哥德尔证明了，在 $\mathscr{N}$ 中存在着一个闭公式 $\mathscr{U}$，使得 $\mathscr{U}$ 和 $\sim\mathscr{U}$ 都不是 $\mathscr{N}$ 中的定理．他的做法是对 $\mathscr{U}$ 作出一个明显的描述，并且证明在 $\mathscr{U}$ 或 $\sim\mathscr{U}$ 是 $\mathscr{N}$ 的定理的假设下，将导致矛盾．第一个技术性的思想是编码．即给出一个方法，它对每一个公式和每一公式序列都给配上一个码数（一个正整数），使得那个公式或公式序列能容易地从它的码数返求而得．通过这种编码，关于正整数的陈述可以看成是关于 $\mathscr{N}$ 中的表达式的码数的陈述，或者甚至可以看成是关于 $\mathscr{N}$ 中的表达公式的陈述．例如，我们将要

考察一个在 D_N 上用 Pf 来表示的二元关系，它是这样定义的，$Pf(m, n)$成立，当且仅当 n 是公式的码数，m 是该公式证明的码数.

现在，$\mathscr{N}$ 中含有自由个体变元的公式，在 N 中可以被解释成非负整数之间的关系. 所以自然地会问：是否存在可用 Pf 关系作为解释的 $\mathscr{N}$ 中的公式？由于技术的原因，我们提出一个稍微不同的问题. 首先我们来考察，在 $\mathscr{N}$ 的语言中，有代表(即在 N 中解释为)非负整数 0, 1, 2, … 的项 $0, 0', 0'', \cdots$. 它们可以用 $0, 0^{(1)}, 0^{(2)}, \cdots$ 表示. 因而我们问：是否存在含二自由变元的公式 $\mathscr{P}(x_1, x_2)$，它具有如下性质：对于每个 $m, n \in D_N$，$\mathscr{P}(0^{(m)}, 0^{(n)})$还是 $\sim\mathscr{P}(0^{(m)}, 0^{(n)})$为 $\mathscr{N}$ 中的定理，恰好视 $Pf(m, n)$在 N 中是否成立而定. 如果这样的 $\mathscr{P}$ 存在的话，那么 Pf 称为在 $\mathscr{N}$ 中可用公式 $\mathscr{P}$ 表达.

下一步是去求这种可在 $\mathscr{N}$ 中表达的关系的一个充分条件，而这里正是递归性派用场的地方. 关于它的定义见 6.3 节；我们这里只说一点，如果一个关系是递归的，那么它在 $\mathscr{N}$ 中可表达. 检验递归性比检验可表达性要方便得多. 哥德尔的证明表明，正是通过递归性来说明一个特殊的关系在 $\mathscr{N}$ 中是可表达的. 上面说到过的关系 Pf 事实上是递归的，这一点要被用于关系 W 也是递归的证明之中，这里 W 是这样定义的，$W(m, n)$ 成立，当且仅当 m 是一公式 $\mathscr{A}(x_1)$的编码数，其中 x_1 自由出现，并且 n 是公式 $\mathscr{A}(0^{(m)})$ 在 $\mathscr{N}$ 中的一个证明的编码数. 化点力气去掌握 W 的意义是值得的，因为它引进了一种"自指代" (Self-reference) 方式，它是合法的，并且对于证明是关键性的.

关系 W 是递归的，因此在 $\mathscr{N}$ 中可用公式 $\mathscr{W}$ 表达. 从 $\mathscr{W}$ 出发，通过一个十分简单的步骤就可以构造公式 $\mathscr{U}$，$\mathscr{U}$ 在 N 中的解释是：对于每个 $n \in D_N$，n 不是公式 $\mathscr{U}$ 在 $\mathscr{N}$ 中的一个证明的编码数. 因此 $\mathscr{U}$ 在这一点上体现了一种令人更为惊奇的自指代

方式，即它可看作是断定了自身的不可证明性．在此只要仔细地区分公式和它的码数，项 $0^{(m)}$ 和它所代表的数，困难就可以避免．十分径直地可以证明：如果 $\mathscr{U}$ 是 $\mathscr{N}$ 中的一条定理，则可得一个矛盾；仅仅稍微难一点的是从 $\sim\mathscr{U}$ 是 $\mathscr{N}$ 的一条定理的假设导出矛盾．当然，这里有一个关于 $\mathscr{N}$ 是一致的默认的假设(否则，$\mathscr{U}$ 和 $\sim\mathscr{U}$ 都将自动地成为 $\mathscr{N}$ 的定理)．实际上，为了证明 $\sim\mathscr{U}$ 不①是一条定理，还要求 $\mathscr{N}$ 有一个较一致性更强一点的假设．

这就是证明的概要．在本章的其余部分将使这些思想具体化，而结果的某些扩充和推论则在 6.5 节给出．有些证明略去了，对技术上的细节感兴趣的读者可以参考孟德尔森 (Mendelson) 的书．

6.2 可表达性

我们在这里继续研究在第五章中已经描述过的算术系统 $\mathscr{N}$，和它的意图中的模型 N．起始于逻辑研究中的最重要的概念之一，递归性，是直接在这个形式系统和它的模型 N 之间的关系中产生的．在最近四十年间，递归函数的应用范围得到了广泛的发展，但是最初它们是很自然地从可表达性问题产生的．我们将从这里开始．

我们在前面几章中曾经关心到形式系统的符号，以及它们能以被解释的方式．当前，我们将把这一过程颠倒过来．让我们从模型 N 开始．它的论域是自然数，我们将继续用 D_N 表示．首先看到，数 0，后继函数，加，乘和相等都被系统 $\mathscr{N}$ 的符号以一种明显的方式表示于 $\mathscr{N}$ 中．但是例如考察数 5，5 是 D_N 中的元素，却不是 $\mathscr{N}$ 中的符号．不过 5 是 $\mathscr{N}$ 中的一个特殊项在 N 中的解释，这个特殊项是 O'''''，即 $f_1^1(f_1^1(f_1^1(f_1^1(f_1^1(a_1)))))$．每个自然数按类似的方式都是 $\mathscr{N}$ 中一个项的解释．我们将需要用到这些项，因而引进一个比起上面用到的两个(它们都相当笨重)都更为方便

① 原书缺"不"字，应补上——译者注

一些的记号是有用的.

记法 $O^{(n)}$ 是O后跟写 n 个撇的简写. 因此数 $n\in D_N$ 是项 $O^{(n)}$ 在 N 中的解释. 平凡地, $O^{(0)}$ 表示 $\mathscr{N}$ 中的个体常元 0.

必须注意,尽管我们用 $O^{(n)}$ 去表示 $\mathscr{N}$ 中的一个项,但是符号 n 本身却不是 $\mathscr{N}$ 的一个符号, 在 $O^{(n)}$ 中出现的 n 不能用一个变元去代替. 我们将称项 $O^{(n)}$ 为数项.

命题 6.1

令 $m, n\in D_N$.

(i) 如果 $m\neq n$, 那么 $\underset{\mathscr{N}}{\vdash}\sim(O^{(m)}=O^{(n)})$.

(ii) 如果 $m=n$, 那么 $\underset{\mathscr{N}}{\vdash}(O^{(m)}=O^{(n)})$.

证明 (i)不失一般性可假设 $m<n$. 那么存在 $k>0$, 使得 $n=m+k$. 公理(N2*)给出

$$\underset{\mathscr{N}}{\vdash}(O^{(m)}=O^{(m+k)}\rightarrow O^{(m-1)}=O^{(m+k-1)}),$$

如果 $m>0$, 重复使用上面的并且使用 HS 规则, 可得

$$\underset{\mathscr{N}}{\vdash}(O^{(m)}=O^{(m+k)}\rightarrow O^{(0)}=O^{(k)}).$$

($m=0$ 的情形是平凡的.)

现在 $k>0$, 据假设所以 $k-1\in D_N$, 且

$$\underset{\mathscr{N}}{\vdash}(O^{(k)}=(O^{(k-1)})').$$

(如果这还不清楚,可以考察

$$\underset{\mathscr{N}}{\vdash}(\overbrace{O'''\cdots'}^{k}=(\overbrace{O'''\cdots'}^{k-1})').)$$

因此我们有 $\underset{\mathscr{N}}{\vdash}(O^{(m)}=O^{(m+k)}\rightarrow O^{(0)}=(O^{(k-1)})')$.

用一个重言式,我们得到

$$\underset{\mathscr{N}}{\vdash}(\sim(O^{(0)}=(O^{(k-1)})')\rightarrow\sim(O^{(m)}=O^{(m+k)})).$$

而公理(N1*)给出

$$\vdash_{\mathscr{N}} (\sim (O^{(0)} = (O^{(k-1)})'),$$

因此据分离规则，就有

$$\vdash_{\mathscr{N}} \sim (O^{(m)} = O^{(m+k)}).$$

(ii) 假设 $m=n$，那么 $O^{(m)}$ 和 $O^{(n)}$ 是恒等的(它们是 $\mathscr{N}$ 中同一个项)．因此，$(O^{(m)}=O^{(n)})$ 是公理(E7)的特例．

▷我们看到 $\mathscr{N}$ 的项集包含一序列 O, $O^{(1)}$, $O^{(2)}$, … 它们在 N 中的解释是自然数序列．现在，$\mathscr{N}$ 的公式可以包含这些项，而 $\mathscr{N}$ 中包含这些项的定理，在 N 中是解释为算术真理的．我们将要研究的一般问题，关系到算术的真实性和 $\mathscr{N}$ 中的定理之间的对应．命题 6.1 指出了这种对应的一个十分有限的方面．但是它却把我们引向更为一般的可表达性观念．另一些例子将更清楚地说明这点．

例 6.2

考察在自然数集 D_N 上的 $\leqslant$ 关系．直觉上 $m\leqslant n$ 可以作为公式 $(\exists x_1)(O^{(m)}+x_1=O^{(n)})$ 的解释，所以 $\leqslant$ 按这意义在 $\mathscr{N}$ 中是"可表达的"．但是，它也是在更强的意义下可表达的，因为

$$\text{如果 } m\leqslant n, \text{ 那么} \vdash_{\mathscr{N}} (\exists x_1)(O^{(m)}+x_1=O^{(n)}),$$

和

$$\text{如果 } m\nleqslant n, \text{ 那么} \vdash_{\mathscr{N}} \sim (\exists x_1)(O^{(m)}+x_1=O^{(n)}).$$

换言之，在 D_N 中的两个自然数之间的这个关系成立还是不成立，取决于一个公式本身还是它的否定，是形式系统 $\mathscr{N}$ 的一条定理．在本例中所要求的一切公式都是 $\mathscr{N}$ 的定理的详细证明细节将略去．

定义 6.3

一个在自然数域上的 k 元关系 R 称为在 $\mathscr{N}$ 中可表达的，如果存在一个有 k 个自由变元的公式 $\mathscr{A}(x_1, \cdots, x_k)$，使得对任何 $n_1, n_2, \cdots, n_k \in D_N$，

(i) 如果 $R(n_1, \cdots, n_k)$ 在 N 中成立，则 $\vdash_{\mathscr{N}} \mathscr{A}(O^{(n_1)}, \cdots, O^{(n_k)})$，且

(ii) 如果 $R(n_1, \cdots, n_k)$ 在 N 中不成立，

则 $$\vdash_{\mathscr{N}} \sim\mathscr{A}(O^{(n_1)}, \cdots, O^{(n_k)}).$$

注记 6.4

(a) 命题 6.1 是说，N 中的相等关系，在这个精确意义下是可表达的.

(b) 如果 $\mathscr{N}$ 已知是完全的，定义 6.3 可以更简单地加以陈述，把(i)和(ii)合并成一句"当且仅当"的说法即可，因为我们将知道，不是 $\mathscr{A}(O^{(n_1)}, \cdots, O^{(n_k)})$ 为 $\mathscr{N}$ 中的定理，就是 $\sim\mathscr{A}$ 为 $\mathscr{N}$ 中的定理. 但是可能出现这样的情况，对某个公式 $\mathscr{A}$ 和数 $n_1, n_2, \cdots, n_k$，$\mathscr{A}(O^{(n_1)}, \cdots, O^{(n_k)})$ 和 $\sim\mathscr{A}(O^{(n_1)}, \cdots, O^{(n_k)})$ 都不是 $\mathscr{N}$ 中的定理. 因而在定义 6.3 中的两个条件都是必要的.

(c) 上述(b)的论证表明了 $\mathscr{N}$ 中的每个含自由变元的公式，并不是都能按这种方式去"表达"一个关系的可能性，反之确实每个这种公式，都可被解释成 N 中的一个关系.

(d) 自然数都可被看成这种情况下的一元关系. 如果 A 是 D_N 的一个子集，那么"$\in A$"是 D_N 的一元关系，在上述意义下，它可能是可表达的，也可能是不可表达的. 例如，令 A 是偶数集，那么"$\in A$"就是公式

$$(\exists x_2)(x_2 \times O^{(2)} = x_1)$$

的解释.

读者可以考虑，是否对于每个 $m \in D_N$，或者 $(\exists x_2)(x_2 \times O^{(2)} = O^{(m)})$，或者 $\sim(\exists x_2)(x_2 \times O^{(2)} = O^{(m)})$ 一定是 $\mathscr{N}$ 的定理，即"是偶数的"关系是否在 $\mathscr{N}$ 中可表达.

(e) 一个函数是一种特殊的关系. 一般来说，一个 D_N 上的 $(k+1)$元关系 R 是一个函数，如果对于每一个 $n_1, \cdots, n_k \in D_N$，总恰有一个 $n_{k+1} \in D_N$，使得 $R(n_1, \cdots, n_k, n_{k+1})$成立. 现在，当考察

一个函数(作为一个关系)在 $\mathscr{N}$ 中是否可表达时，至关重要的是考察该单值性是否亦为所涉及的 $\mathscr{N}$ 的公式所具有.

定义 6.5

一个在 D_N 上的 k 元函数(即一个函数 $D_N^k \to D_N$)称为在 $\mathscr{N}$ 中可表示，如果它在 $\mathscr{N}$ 中(作为 $(k+1)$ 元关系)，可由一个有 $k+1$ 个自由变元的公式 $\mathscr{A}$ 来表达，使得对于每个 $n_1, \cdots, n_k \in D_N$,

$$\underset{\mathscr{N}}{\vdash} (\exists_1 x_{k+1}) \mathscr{A}(O^{(n_1)}, \cdots, O^{(n_k)}, x_{k+1}).$$

注记 6.6

我们必须再次记住项 $O^{(n)}$ 和 D_N 的元素之间的差别. 乍看起来，条件

$$\underset{\mathscr{N}}{\vdash} (\forall x_1) \cdots (\forall x_k) (\exists_1 x_{k+1}) \mathscr{A}(x_1, \cdots, x_k, x_{k+1}) \qquad (*)$$

似乎等价于定义中的条件，其实情况并非如此，要搞清楚为什么并非如此的最容易的方法，是考察 $\mathscr{N}$ 的一个可能的不同模型. 这个模型，将不得不含有对所有项 $O, O^{(1)}, O^{(2)}, \cdots$ 的解释，但是它还将包含另外一些元素. $(*)$ 的解释将是关于这些另外元素的一个断定，所以是一个比 $(\exists_1 x_{k+1}) \mathscr{A}(O^{(n_1)}, \cdots, O^{(n_k)}, x_{k+1})$，对每个 $n_1, \cdots, n_k$，的解释的合取还要强的断定.

例 6.7

由 $f(m, n) = m+n$ 给出的函数 f: $D_N^2 \to D_N$ 在 $\mathscr{N}$ 中是可表示的.

令 $\mathscr{A}(x_1, x_2, x_3)$ 是公式 $x_3 = x_1 + x_2$. 要求对每个 $m, n, p \in D_N$，证明以下的:

(i) 如果 $p = m+n$，那么 $\underset{\mathscr{N}}{\vdash} O^{(p)} = O^{(m)} + O^{(n)}$,

(ii) 如果 $p \neq m+n$，那么 $\underset{\mathscr{N}}{\vdash} \sim (O^{(p)} = O^{(m)} + O^{(n)})$,

(iii) $\underset{\mathscr{N}}{\vdash} (\exists_1 x_3)(x_3 = O^{(m)} + O^{(n)})$.

我们能证明如下. 令 $m, n \in D_N$. 那么 $\underset{\mathscr{N}}{\vdash} O^{(m)} + O^{(n)} = O^{(m+n)}$.

如果 $n=0$ 这恰好是公理(N3*). 如果 $n>0$, 把 $O^{(n)}$ 写成 $(O^{(n-1)})'$. 根据(N4*), 于是,

$$\vdash_{\mathscr{N}} (O^{(m)}+O^{(n)})=(O^{(m)}+O^{(n-1)})'.$$

根据需要重复这个过程, 可得

$$\vdash_{\mathscr{N}} (O^{(m)}+O^{(n)})=(O^{(m)}+O)\overbrace{'\cdots'}^{n}$$

即
$$\vdash_{\mathscr{N}} (O^{(m)}+O^{(n)})=(\overbrace{O'\cdots'}^{m})\overbrace{'\cdots'}^{n}$$

即
$$\vdash_{\mathscr{N}} (O^{(m)}+O^{(n)}=O^{(m+n)}).$$

(i)和(ii)现在是命题6.1的直接推论. 对(iii)而言, 我们必须证明

$$\vdash_{\mathscr{N}} (\exists x_3)(x_3=O^{(m)}+O^{(n)}\wedge(\forall x_i)(x_i=O^{(m)}+O^{(n)}\rightarrow x_i=x_3)),$$

现在

$$\vdash_{\mathscr{N}} (O^{(m+n)}=O^{(m)}+O^{(n)})\wedge(\forall x_i)(x_i=O^{(m)}+O^{(n)}\rightarrow x_i=O^{(m+n)}).$$

(证明中细节略去了, 其实并不困难). 运用练习 3.21 的结果, 我们就得到所要的结果.

例 6.8

由 $f(m)=2m$ 给出的函数 f: $D_N\rightarrow D_N$ 在 $\mathscr{N}$ 中是可表示的.

令 $\mathscr{A}(x_1, x_2)$ 是公式 $x_2=x_1\times O^{(2)}$. 我们必须对每个 $m, n\in D_N$ 证明以下的:

(i) 如果 $n=2m$, 那么 $\vdash_{\mathscr{N}} O^{(n)}=O^{(m)}\times O^{(2)}$,

(ii) 如果 $n\neq 2m$, 那么 $\vdash_{\mathscr{N}} \sim(O^{(n)}=O^{(m)}\times O^{(2)})$,

(iii) $\vdash_{\mathscr{N}} (\exists_1 x_2)(x_2=O^{(m)}\times O^{(2)})$.

对(i). 假设 $n=2m$. 我们给出 $O^{(n)}=O^{(m)}\times O^{(2)}$ 在 $\mathscr{N}$ 中的一个证明的概要.

$$
\begin{aligned}
O^{(m)}\times O^{(2)} &= O^{(m)}\times O'' && \text{记法}\\
&= (O^{(m)}\times O')+O^{(m)} && (\mathrm{N6}^*)\\
&= ((O^{(m)}\times O)+O^{(m)})+O^{(m)} && (\mathrm{N6}^*)\\
&= (O+O^{(m)})+O^{(m)} && (\mathrm{N5}^*)\\
&= O^{(m)}+O^{(m)} && (\mathrm{N3}^*)\\
&= O^{(m+m)} && \text{前例}\\
&= O^{(2m)}\\
&= O^{(n)}.
\end{aligned}
$$

对(ii)，假设 $n\neq 2m$. 那么 $\vdash_{\mathscr{N}} \sim(O^{(2m)}=O^{(n)})$ 据命题 6.1，且如上 $\vdash_{\mathscr{N}} (O^{(2m)}=O^{(m)}\times O^{(2)}$. 因此，用公理(E9′)，我们就得到

$$\vdash_{\mathscr{N}} \sim(O^{(m)}\times O^{(2)}=O^{(n)}).$$

对(iii)，证明恰如上例.

例 6.9

由 $Z(m,n)=0$ 对每个 $m,n\in D_N$ 所定义的二元函数 Z 在 $\mathscr{N}$ 中是可表示的.

令 $A(x_1, x_2, x_3)$ 是公式

$$(x_1=x_1\wedge x_2=x_2\wedge x_3=0).$$

仍然要求验证一些公式是 $\mathscr{N}$ 的定理:

(i) 如果 $Z(m, n)=p$，那么

$$\vdash_{\mathscr{N}} (O^{(m)}=O^{(m)}\wedge O^{(n)}=O^{(n)}\wedge O^{(p)}=0),$$

(ii) 如果 $Z(m, n)\neq p$，那么

$$\vdash_{\mathscr{N}} \sim(O^{(m)}=O^{(m)}\wedge O^{(n)}=O^{(n)}\wedge O^{(p)}=0),$$

(iii) $\vdash_{\mathscr{N}} (\exists_1 x_3)(O^{(m)}=O^{(m)}\wedge O^{(n)}=O^{(n)}\wedge x_3=0.$

对每个 $m, n, p\in D_N$.

对(i)，如果 $Z(m, n)=p$，那么 $p=0$，而 $O^{(m)}=O^{(m)}$，$O^{(n)}=O^{(n)}$，$O^{(p)}=0$ 中的每一个是 $\mathscr{N}$ 的一条定理.

对(ii)，如果 $Z(m, n)\neq p$，那么 $p\neq 0$，从而 $\sim(O^{(p)}=0)$ 是 $\mathscr{N}$ 的一条定理(公理(N1*))．由此可推得

$$\vdash_{\mathscr{N}}\sim(O^{(m)}=O^{(m)}\wedge O^{(n)}=O^{(n)}\wedge O^{(p)}=0).$$

为了证明(iii)，只需证 $\vdash_{\mathscr{N}}(\exists_1 x_3)(x_3=0)$，即 $\vdash_{\mathscr{N}}(\exists x_3)(x_3=0\wedge(\forall x_i)(x_i=0\rightarrow x_i=x_3))$．这是成立的，因为

$$\vdash_{\mathscr{N}}(0=0\wedge(\forall x_i)(x_i=0\rightarrow x_i=0)).$$

这里我们再次用到练习 3.21 的结果．

▷ 关于函数在 $\mathscr{N}$ 中可表示的问题，首先可以问的是有没有不可表示的函数．给出一个 D_N 上的函数，证明它是可表示的也许很难，要证明它不可表示也许就更难．在上面已经显现了某些困难．因此一般的结果是有用的．

命题 6.10

并非 D_N 上的所有函数在 $\mathscr{N}$ 中都是可表示的．

证明 对照注记 5.10(b)中的论证．在 $\mathscr{N}$ 上的公式集是可数的，所以在 $\mathscr{N}$ 中可表示函数的集也是可数的．但是 D_N 上有不可数多个函数．因此 D_N 上有在 $\mathscr{N}$ 中不可表示的函数．

系 6.11

并非 D_N 上的所有关系，在 $\mathscr{N}$ 中都是可表达的．

证明与上面相似．

▷ 合乎逻辑地似乎可以问的第二个问题是，我们能刻划出 D_N 上的函数(关系)能在 $\mathscr{N}$ 中可表示(可表达)的特征吗？答案是一个重要的结果，并且是哥德尔关于系统 $\mathscr{N}$ 的不完全性定理的证明的关键之一．

命题 6.12

一个 D_N 上的函数(关系)是在 $\mathscr{N}$ 上可表示(可表达)的，当且仅当它是递归的．

当然．在目前这并不说明什么，事实上它的完全的证明也超

出了我们的范围，但是一旦当我们定义和描述了递归函数和递归关系时，我们将看到它是何等重要.

练习

1. 证明，对任意 $m, n \in D_N$，如果 $m \leqslant n$，则

$$\vdash_{\mathscr{N}} (\exists x_1)(O^{(m)} + x_1 = O^{(n)}).$$

2. 证明，对任意 $m, n \in D_N$，如果 $m > n$，则

$$\vdash_{\mathscr{N}} \sim (\exists x_1)(O^{(m)} + x_1 = O^{(n)}).$$

3. 写出系统 $\mathscr{N}$ 的公式，它们在 N 中的解释如下：

(a) N 不是素数.

(b) m 和 n 没有公因子.

(c) $m = \min(p, q)$；

(d) 每个 $m \in D_N$ 有一素因子；

(e) $sg(m) = n$（定义参见 p. 159）.

4. 证明下列 D_N 上的函数在 $\mathscr{N}$ 中是可表示的，而不用命题 6.21.

(a) sg　　（定义参见 p. 159）；

(b) f,　　$f(n) = n + 3$；

(c) rm_2,　$rm_2(n)$ 是 n 由 2 除后的余项.

5. 证明：函数 f：$D_N \to D_N$ 在 $\mathscr{N}$ 中是可表示的，如果有一 $\mathscr{N}$ 的公式 $\mathscr{A}$，使得

(i) 如果 $f(m) = n$，则 $\vdash_{\mathscr{N}} \mathscr{A}(O^{(m)}, O^{(n)})$,

且

(ii) 对每个 $m \in D_N$，$\vdash_{\mathscr{N}} (\exists_1 x_2)\mathscr{A}(O^{(m)}, x_2)$.

（这可以推广到多变量函数）.

6. 证明由 $p_i^k(n_1, \cdots, n_k) = n_i$，$(n_1, \cdots, n_k \in D_N)$，给出的投影函数 p_i^k：$D_N \to D_N$ 对每个 i, $k > 0$，是可表示的.

6.3 递归函数和递归关系

递归函数类是按下面方式来定义的(无需参照系统 $\mathscr{N}$). 即某些容易定义的函数是递归的,并且从这些函数出发,用下面三个规则得到的一切函数也都是递归的.

这些基本函数是:

1. 零函数 $z: D_N \to D_N$, 由 $z(n)=0$ 给定,对于每个 $n \in D_N$.

2. 后继函数 $s: D_N \to D_N$, 对每个 $n \in D_N$, 由 $s(n)=n+1$ 给定.

3. 投影函数 $p_i^k: D_N^k \to D_N$, 对每个 $n_1, \cdots, n_k \in D_N$, 由 $p_i^k(n_1, \cdots n_k)=n_i$ 给定. 注意 p_1^1 是恒等函数.

三个规则是:

I. 合成. 如果 $g: D_N^j \to D_N$ 且 $h_i: D_N^k \to D_N$, 对每个 $1 \leqslant i \leqslant j$, 那么由

$$f(n_1, \cdots, n_k)=g(h_1(n_1, \cdots, n_k), \cdots, h_j(n_1, \cdots, n_k)),$$

定义的 $f: D_N^k \to D_N$, 是通过 g 和 $h_1, \cdots, h_j$ 合成而得的.

II. 递归. 如果 $g: D_N^k \to D_N$ 且 $h: D_N^{k+2} \to D_N$, 那么由

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

和

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

定义的 $f: D_N^{k+1} \to D_N$, 叫做由 g 和 h 递归而得. 注意这里的 $n_1, \cdots, n_k$ 是并不影响定义的参数. 我们允许这些参数不出现. 由

$$f(0)=a \quad (D_N \text{ 上的一个固定数}),$$

和

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

定义的函数 f, 同样为递归所得.

III. 最小数运算. 令 $g: D_N^{k+1} \to D_N$ 是具有这样性质的任一函数, 即对每个 $n_1, \cdots, n_k \in D_N$, 至少有一个 $n \in D_N$, 使得 $g(n_1, \cdots, n_k, n)=0$. 因此由

$$f(n_1, \cdots, n_k)=\text{最小数 } n \in D_N$$

$$使得\ g(n_1, \cdots, n_k, n)=0$$

定义的函数 $f: D_N^k \to D_N$ 称为由 g 通过最小数运算而得.

记法 使得 $g(n_1, \cdots, n_k, n)=0$ 成立的最小数 n, 用 $\mu n[g(n_1, \cdots, n_k, n)=0]$ 表示.

注记 6.13

对 g 所提的条件: 对任何 $n_1, \cdots, n_k$, 至少存在一个数 n, 使得 $g(n_1, \cdots, n_k, n)=0$ 成立, 这对保证 f 是一全函数, 即对每 k 个自然数它都有一个值, 显然是必要的. 以后, 我们将经常允许使用最小数运算而无需这个条件. 这显然将导致偏函数的引进. 不过, 目前条件先保持下来, 我们所有的函数都是全函数.

例 6.14

(a) 凭 $f(m, n)=m^2+mn$ 给出的函数 $D_N^2 \to D_N$, 由加法乘法和投影函数合成如下: (其中 f_1 表示和, f_2 表示积) 因此

$$f(m, n)=f_2(p_1^2(m, n), f_1(m, n)).$$

(b) 凭 $g(m, n, p)=n^2$ 给出的函数 $g: D_N^3 \to D_N$, 由合成而得如下:

$$g(m, n, p)=f_2(p_2^3(m, n, p), p_2^3(m, n, p)),$$

其中 f_2 表示积

(c) 加法函数, 由 p_1^1 和 s 与 p_3^3 的合成, 通过递归而得如下:

$$f_1(m, 0)=p_1^1(m),$$

$$f_1(m, n+1)=s(p_3^3(m, n, f_1(m, n)).$$

(d) 类似地, 乘法函数可由加法函数通过递归而得.

(e) 令 $f(n)$ = 最小数 q, 使得 $n+q \equiv 0 \pmod p$ ($n, p, q \in D_N$). 那么 f 由函数 g, 其中

$$g(n, p, q)=n+q\ 被\ p\ 除后的余项,$$

通过最小数运算而得.

定义 6.15

D_N 上的一函数是递归的, 如果它能由上述的函数 1, 2, 3, 通

过有限次运用规则 I, II, III 而得. 因此递归函数类是所有包含 1, 2, 3 且在应用规则 I, II, III 之下封闭的函数类中的最小者.

一个函数是原始递归的, 如果它能由函数 1, 2, 3, 并且仅仅通过有限次运用规则 I, II 而得. 原始递归函数构成一严格小于递归函数类的函数类(这要求证明, 但我们将不加讨论). 它们在某些分支是重要的, 但是我们将无需专门的考察它们.

例 6.16

(a) 和函数是(原始)递归的. 为了弄清这一点, 我们转回到 6.14(c), 这里和函数是由一个投影函数和后继函数通过递归而得.

(b) 积函数是(原始)递归的. 为弄清这点, 定义函数 f_2: $D_D^2 \to D_N$ 如下:

$$f_2(m, 0) = z(m)$$
$$f_2(m, n+1) = h(m, n, f_2(m, n)),$$

其中 $h(m, n, p) = f_1(p_3^3(m, n, p), p_1^3(m, n, p))$. 这里的 f_2, 是由 z 和 h 通过递归定义的, 但 z 是递归的, 而 h 由 f_1, p_3^3, p_1^3, 通过合成而得, 也是递归的.

(c) 例 6.14(b)是一递归函数.

(d) 由 $f(n) = n!$ 给出的函数 f: $D_N \to D_N$ 是(原始)递归的. 因为 f 由

$$f(0) = 1$$
$$f(n+1) = f_2(s(n), f(n)),$$

定义, 所以是由后继和乘法函数通过递归(和合成)而得, 也是(原始)递归的.

(e) 所有常函数是递归的. 以 k 为值的常函数, 可由投影函数 p_2^2 定义如下:

$$f(0) = k$$
$$f(n+1) = p_2^2(n, f(n)).$$

一元以上的常函数，通过使用另外的投影函数，也可看出是递归的.

(f) 函数 $sg, \overline{sg}: D_N \to D_N$, 分别由

$$sg(n)=\begin{cases}0 & \text{如果 } n=0\\ 1 & \text{如果 } n\neq 0\end{cases}$$

和

$$\overline{sg}(n)=\begin{cases}1 & \text{如果 } n=0\\ 0 & \text{如果 } n\neq 0\end{cases}$$

给定，它们是递归的. 因为

$$sg(0)=0$$

$$sg(n+1)=1 \quad (\text{常函数})$$

和

$$\overline{sg}(0)=1$$

$$\overline{sg}(n+1)=0.$$

▷ 人们可能会这样想，这个定义同 $\mathscr{N}$ 中可表示函数的定义一样不便于应用，但是情况并非如此，它的归纳性质使得人们能很快地，容易地去建立一大类我们知道是递归的函数. 在讨论递归性时，我们还会遇到另外的好处，它涉及可计算性，这将在更后面说到.

递归性概念，用特征函数的思想可以推广到关系.

定义 6.17

令 R 是 D_N 上的 k 元关系，R 的特征函数(由 C_R 表示)，定义如下：

$$C_R(n_1, \cdots, n_k)=\begin{cases}0 & \text{当 } R(n_1, \cdots, n_k) \text{成立时}\\ 1 & \text{当 } R(n_1, \cdots, n_k) \text{不成立时}.\end{cases}$$

定义 6.18

一个 D_N 上的关系 R 是递归的，如果它的特征函数是一递归函数.

例 6.19

这样的二元关系 R 是递归的，即 $R(m, n)$ 成立当且仅当

$m+n$ 为偶数.

要证它,我们必须证明由

$$f(m, n)=\begin{cases}0 \text{ 当 } m+n \text{ 为偶数时} \\ 1 \text{ 当 } m+n \text{ 为奇数时}\end{cases}$$

定义的函数 f 是一递归函数. 令 rm_2: $D_N \to D_N$ 是由 $rm_2(n)=n$ 由 2 除后的余项. rm_2 是递归的,因为

$$rm_2(0)=0$$

$$rm_2(n+1)=\overline{sg}(rm_2(n))=\overline{sg}(p_2^2(n, rm_2(n))).$$

现在 $f(m, n)=rm_2(m+n)$,由于 $+$ 和 rm_2 是递归的,所以根据合成,f 也是递归的.

例 6.20

关系 $\leqslant$ 是递归的

要证它,我们必须证明,由

$$g(m, n)=\begin{cases}0 \text{ 当 } m\leqslant n \text{ 时} \\ 1 \text{ 当 } m>n \text{ 时}\end{cases}$$

定义的函数 g 是递归的. 这要求几步走. 首先,由

$$p(n)=\begin{cases}n-1 & \text{当 } n>0 \\ 0 & \text{当 } n=0\end{cases}$$

定义的函数 p 是递归的. 欲明此,

$$\left.\begin{aligned}p(0)&=0 \\ p(n+1)&=n\end{aligned}\right\} \text{用递归.}$$

其次,由

$$m \dot{-} n=\begin{cases}m-n & \text{当 } m\geqslant n \\ 0 & \text{当 } n>m,\end{cases}$$

定义的函数 $\dot{-}$ 是递归的. 欲明此,

$$\left.\begin{aligned}m \dot{-} 0&=m \\ m \dot{-} (n+1)&=p(m \dot{-} n)\end{aligned}\right\} \text{用递归}$$

注意,减函数在这里不能加以讨论,因为它会引出负数,而我们

的数域仅由非负整数组成．由 $\dot{-}$ 表示的函数是一经修改的减法．

现在，我们就会明白，怎样按照要求来定义 g．

$$g(m, n)=sg(m\dot{-}n), \text{ 用合成.}$$

▷ 递归性的定义，同样可以用于集合．如果 $A\subseteq D_N$，我们说 A 是递归的，如果 A 的特征函数是递归的(一个集合 A 的特征函数，恰是关系"$\in A$"的特征函数如象上面所定义过的．)

例 6.21

(a) 集 D_N 是递归的，因为它的特征函数是零函数，而这是递归的．

(b) $\varnothing$是递归的，因为它的特征函数是常函数．

(c) 偶数集是递归的．欲明此，必须证明，由

$$h(n)=\begin{cases}0 & \text{当 } n \text{ 是偶数时}\\ 1 & \text{当 } n \text{ 是奇数时}\end{cases}$$

给出的函数 h 是递归的．但 h 恰是例 6.19 中所定义的 rm_2．

命题 6.22

如果 R 和 S 是递归的 k 元关系，那么 $\bar{R}$，$R\wedge S$ 和 $R\vee S$ 等关系也是递归的．($\bar{R}$ 是一个这样的关系，对一给出的 k 元组满足它，当且仅当该 k 元组不满足 R．一 k 元组满足 $R\wedge S$，当且仅当该 k 元组同时满足 R 和 S．一 k 元组满足 $R\vee S$，当且仅当该组或满足 R，或满足 S.)

证明．$\bar{R}$ 的特征函数是 $\overline{sg}(C_R)$，所以它是递归的，如果已知 C_R 是递归的．再者

$$C_{R\vee S}(n_1, \cdots, n_k)=sg(C_R(n_1, \cdots, n_k)+C_S(n_1, \cdots, n_k))$$

和 $$C_{R\vee S}(n_1, \cdots, n_k)=C_R(n_1, \cdots, n_k)\times C_S(n_1, \cdots, n_k).$$

所以 $C_{R\vee S}$ 和 $C_{R\vee S}$ 是递归的，如果已知 C_R 和 C_S 是递归的．

系 6.23

对任意递归集 A 和 B，A 的补，A 和 B 的交和并都是递归的．

证明 这个结果是上述命题的特殊情况，因为集合 A 和 B 的特征函数就是"$\in A$"和"$\in B$"关系的特征函数.

▷ 人们在这里可以着手去证明某些特殊函数、关系和集合的递归性. 说实在的，为了去证明命题 6.12 和系统 $\mathscr{N}$ 中的不完全性，这是必要的. 事实上要去寻找一个不是递归的函数和关系是更加困难的，因为实际上容易描述的函数和关系都是递归的. 我们将以某种方式来进行这一工作，为了使读者对于所用方法有一种感觉，从而对描述一个非递归的函数和关系的难度有所认识.

命题 6.24

D_N 的每个单元子集都是递归的.

证明，我们必须证明，对每个 $k\in D_N$，由

$$S_k(n)=\begin{cases}0 & \text{当 } n=k,\\ 1 & \text{反之}\end{cases}$$

给出的函数 S_k: $D_N\to D_N$ 是递归的. 我们通过对 k 归纳来进行.

基础步骤:

$$S_0(n)=\begin{cases}0 & \text{当 } n=0\\ 1 & \text{当 } n\neq 0.\end{cases}$$

S_0 恰是 sg，所以它是递归的.

归纳步骤: 假设 $k>0$ 且 S_{k-1} 是递归的.

$$S_k(n)=\begin{cases}0 & \text{当 } n=k\\ 1 & \text{当 } n\neq k,\end{cases}$$

所以我们有 $$S_k(0)=1,$$

和 $$S_k(n+1)=S_{k-1}(n) \quad \text{对每个 } n\in D_N.$$

这样 S_k 是由 S_{k-1} 通过递归而得，所以是递归的.

因此，据归纳法，S_k 是递归的，对每个 $k\in D_N$，从而命题得证.

例 6.25

(a) 每一个有限集是递归的，这是命题 6.24 和系6.23 的推

论，因为一个有限集总可以写成单元集的有限并。

(b) p: $D_N \to D_N$ 定义如下：

$$p(n) = \text{第 } n \text{ 个奇素数，如果 } n > 0$$

和

$$p(0) = 2.$$

那么 p 是递归函数．这可能会使人感到奇怪，因为大家知道 p 没有简单的代数表达式．尽管如此，从定义可以证明（用一系列中间步骤）p 是递归函数类．

(c) 根据初等数论，每个自然数都可唯一地表示成素数幂的积．对每个 $i \in D_N$，可以定义一个函数 e_i

$$e_i(n) = \begin{cases} \text{在 } n \text{ 作为素数幂的表示式中素数 } p(i) \text{ 的指数，} \\ \text{如果 } p(i) \text{ 在表示式中出现．} \\ \text{反之为 } 0. \end{cases}$$

那么，对每个 i，e_i 是一递归函数．

(d) 函数 d: $D_N^2 \to D_N$，这里

$$d(m, n) = m \text{ 和 } n \text{ 的最大公因子，}$$

是递归的．

▷ 从简单的基本函数和规则，可以建造复杂的递归函数，显然在应用规则 I, II 和 III 时，对复杂性没有任何限制．命题 6.12 的证明可以在孟特尔森的著作中找到，它是十分冗长的，并且在很大程度上依赖于某些特殊的函数和关系是递归的证明，以及如何组合递归函数去给出其它的递归函数及关系等．

作为命题 6.10 和 6.12 的系，我们能够得到那个帮助并不大的结果，并非 D_N 上的所有函数都是递归的．其实这可以比较直接地，通过可数性论证而得，无需使用这些命题．

递归函数集是可数的，这个事实使得我们能够构造一个递归的函数．考察所有一元递归函数的一个枚举 $f_1, f_2, \cdots$．定义一个函数 g: $D_N^2 \to D_N$

$$g(m, n) = f_m(n).$$

那么，g 是一个非递归函数．因为假设 g 是递归的．定义 h

$$h(m)=g(m,\ m)+1 \quad (m\in D_N).$$

由于 g 递归，h 也是递归的，因此对某个 k，h 与 f_k 恒等，对这个 k，我们有

$$h(k)=f_k(k)=g(k,\ k)+1=f_k(k)+1.$$

从这个矛盾，我们推得 g 不是递归的．

练习

7．证明下列函数是递归的．

(a) e: $D_N^2\to D_N$，由 $e(m,\ n)=m^n$ 给出．

(b) min: $D_N\to D_N$.

$$\min(m,\ n)=\begin{cases} m & 当\ m\leqslant n. \\ n & 当\ m>n. \end{cases}$$

(c) q: $D_N^2\to D_N$

$$q(m,\ n)=\begin{cases} n\ 由\ m\ 除得的商 & 当\ m\neq 0 \\ 0 & 当\ m=0 \end{cases}$$

8．令 R 是 $k+1$ 元递归关系，使得对每个 $n_1,\ \cdots,\ n_k\in D_N$，至少存在一个 $n_{k+1}\in D_N$，使 $R(n_1,\ \cdots,\ n_k,\ n_{k+1})$ 成立，证明，由

$$f(n_1,\ \cdots,\ n_k)=\mu x[R(n_1,\ \cdots,\ n_k,\ x)]\ (n_1,\ \cdots,\ n_k\in D_N),$$

定义的函数 f 是递归的．

9．令 e_2: $D_N\to D_N$.

$e_2(n)=$ 在 n 作为素数幂的乘积的表示式中 2 的幂指数

$e_2(n)=0$，如果 2 在表示式中不出现）

10．重做练习 9，其中 e_2 用 e_k 代替，e_k 的值是素数 p_k 的幂指数（k 固定）．

11．令 f 和 g 是递归函数．证明函数 h

$$h(x)=f(x)g(x) \quad (x\in D_N)$$

是递归的．

12．证明，对任何 $n>1$，如果 $R_1,\ \cdots,\ R_n$ 是 k 元递归关系，么 $R_1\wedge\cdots\wedge R_n$ 和 $R_1\vee\cdots\vee R_n$ 是递归关系．

13. 证明，对 $n>1$，如果 $A_1, \cdots, A_n$ 是递归集，那么，$A_1 \cap \cdots \cap A_n$ 和 $A_1 \cup \cdots \cup A_n$ 是递归集.

14. 令 R 是 D_N 上的二元关系，令 k 是一固定的自然数. 定义 D_N 上的一元关系(即谓词)如下：

$S(n)$ 成立，当且仅当存在 $m<k$，使得 $R(m, n)$ 成立.

$T(n)$ 成立，当且仅当 $R(m, n)$ 成立，对每个 $m<k$.

证明. 如果 R 是一递归关系，则 S 和 T 也是. 你的证明能否加以修改以便适用于略去条件"$<k$"的关系吗？

6.4 哥德尔数

哥德尔在证明 $\mathscr{N}$ 的不完全性时所用的基本技巧之一，已经成了逻辑和其它领域中的一个标准程序. 这思想就是哥德尔码数. 一般来讲，信息可以呈现在英语或任何其它语言中，或在一个抽象的符号语言中. 为了讨论、传递或处理信息，把它转换成数值形式可能是方便的(甚至是本质的). 例如，当由机器来处理信息时，很常用的是首先把它转换成某种数值形式. 怎样做呢，可以看一个粗略的例子. 在一本特定的英语词典中，词都可标记以数，如 20 以上的. 标准的标点符号可以指派 20 以下的数. 因此，给出一个英语句子就可以写成一个数列.

哥德尔所做的就是给一阶语言 $\mathscr{L}$ (仍然是任意的未加指定的)以一个类似的结构，使得 $\mathscr{L}$ 中每个符号，项，公式和公式序列，都被这般地指派一个码数，以致从任意给定的码数，不难返求那对应的 $\mathscr{L}$ 表示式. 这有不同的做法，我们来描述一种. 首先，在 $\mathscr{L}$ 的符号集上定义一个函数 g.

$$g(()=3$$
$$g())=5$$
$$g(,)=7$$
$$g(\sim)=9$$

$$g(\rightarrow)=11$$
$$g(\forall)=13$$
$$g(x_k)=7+8k \quad k=1, 2, \cdots$$
$$g(a_k)=9+8k \quad k=1, 2, \cdots$$
$$g(f_k^n)=11+8\times(2^n\times 3^k) \quad n=1, 2, \cdots; k=1, 2, \cdots.$$
$$g(A_k^n)=13+8\times(2^n\times 3^k) \quad n=1, 2, \cdots; k=1, 2, \cdots.$$

注意．每个符号被指派一个不同的奇正整数．也要注意，任何给出的奇正整数(如果它果真对应任何符号的话)，也能容易地加以分解以便找到它所代表的符号．

例 6.26

(a) 找对应于数 587 的符号(如果有的话)．

如果 587 对应于某符号，它一定是 x_k, a_k, f_k^n 或 A_k^n, 中之一，所以我们必须首先找出它由 8 除后所得的余数

$$587=8\times 73+3=8\times 72+11$$

而 $72=2^3\times 3^2$，所以同587对应的是函数符号 f_2^3

(b) 证明 333 不对应 $\mathscr{L}$ 中任何符号．

$$333=8\times 41+5=8\times 40+13$$

但是 $40=2^3\times 5$，没有 $2^n\times 3^k$ 的形式，所以 333 不与 $\mathscr{L}$ 中的任何符号对应．

▷ 当然，在一种特殊的语言 $\mathscr{L}$ 中，并非所有符号都出现，所以并不是每个码数都将有用．

现在，$\mathscr{L}$ 中的一个项或公式是 $\mathscr{L}$ 中符号的一个串，我们可以对这样的串指派一个数，方法如下．如果 $u_1, \cdots, u_k$ 是 $\mathscr{L}$ 的符号，让我们用 $u_1u_2\cdots u_k$ 来表示符号串(可以是 $\mathscr{L}$ 中的项或公式，也可以不是)，并且定义

$$g(u_1u_2\cdots u_k)=2^{g(u_1)}\times 3^{g(u_2)}\times\cdots\times p_{k-1}^{g(u_k)}\text{①},$$

其中，对每个 i, p_i 表示第 i 个奇素数，而 $p_0=2$．由于每个数都可

① 原文为 $,p_k^{g(u_k)}$，可能笔误．——译注

以唯一地表示成素数幂的乘积，因此，存在一种寻找与一给定数对应的符号串的明显的程序(如果有的话)。不同的符号串也必定有不同的码数。

例 6.27

(a) $$g(f_1^1(x_1))=2^{g(f_1^1)}\times 3^{g(()}\times 5^{g(x_1)}\times 7^{g())}$$
$$=2^{59}\times 3^3\times 5^{15}\times 7^5.$$

(b) $$g((A_1^2(x_1,\ x_2)\to A_1^1(x_1)))$$
$$=2^{g(()}\times 3^{g(A_1^2)}\times 5^{g(()}\times 7^{g(x_1)}\times 11^{g(,)}\times 13^{g(x_2)}$$
$$\times 17^{g())}\times 19^{g(\to)}\times 23^{g(A_1^1)}\times 29^{g(()}\times 31^{g(x_1)}$$
$$\times 37^{g())}\times 41^{g())}=2^3\times 3^{109}\times 5^3\times 7^{15}\times 11^7$$
$$\times 13^{23}\times 17^5\times 19^{11}\times 23^{61}\times 29^3\times 31^{15}$$
$$\times 37^5\times 41^5.$$

(c) 任何一个出现素数偶次幂的数，或素数序列中出现空隙的数，都不可能对应于任何符号串。

注记 6.28

符号的码数是奇数。符号串的码数是偶数(因为带有非零指数的素数 2 总要在一个串的码数中出现)。这两种码数因而是容易区别的。

▷ 通过进一步地扩充这个过程，能为符号串的有限序列指派码数。令 $S_1,\ S_2,\ \cdots,\ S_r$ 是 $\mathscr{L}$ 的符号串，定义

$$g(s_1,\ s_2,\ \cdots,\ s_r)=2^{g(s_1)}\times 3^{g(s_2)}\times\cdots\times p_{r-1}^{g(s_r)}.$$

注意，一个给定的数，不可能既是一个序列的按此方式的码数，同时又是某一个别的符号串的码数，因为 2 的指数，在一序列的码数中是偶的，而在一个串的码数中是奇的(据注记 6.28)。

现在，我们已经定义了一个函数 g，它以 $\mathscr{L}$ 的所有符号，符号串，符号串的有限序列组成的集为定义域，而值域在 D_N 中。这个函数是 1—1 的，但是如我们已经知道的，它并不映上。按这种方式所作的定义，有一个对 g 的变域中的任何数去计算 g^{-1} 的能行

的程序(即使用素数幂的乘积这样的表示). 我们将称 g 的值为哥德尔数. $\mathscr{L}$ 的每个项或公式是一符号串, 所以有一个哥德尔数. 在 $K_{\mathscr{L}}$ 中的一个证明或演绎是符号串的一个有序列, 因而也有一个哥德尔数.

哥德尔创造这种编码系统的目的, 是为了把关于形式系统的断定(例如 $\mathscr{N}$)转换为关于数的断定, 然后在形式系统内去表示这些断定. 一个对形式系统所能作的断定都是关于公式, 定理和证明的. 例如:"序列 $\mathscr{A}_1, \cdots, \mathscr{A}_k, \mathscr{A}$ 是公式 $\mathscr{A}$ 在 $\mathscr{N}$ 中的一个证明". 这个断定说,在一有限个公式的序列和一特殊的公式之间有着某种关系成立. 依靠哥德尔数, 这就产生一个 D_N 上的关系, 比如说 Pf, 它被定义为: $Pf(m, n)$ 成立,当且仅当 m 是 $\mathscr{N}$ 上公式的一个序列的哥德尔数, 而这序列构成了哥德尔数为 n 的公式的一个在 $\mathscr{N}$ 中的证明.

$\mathscr{N}$ 的其它性质和有关断定, 在类似的方式下产生 D_N 上的关系. 正是现在, 可表达性的问题变得重要了, 因为, 继续用上例来讲,假如关系 Pf 在 $\mathscr{N}$ 内可表达的话, 就将存在一个 $\mathscr{L}_N$ 中的公式 $\mathscr{P}(x_1, x_2)$,使得对每个 $m, n \in D_N$ 有:

$$\text{如果} Pf(m, n) \text{成立,则} \vdash_{\mathscr{N}} \mathscr{P}(O^{(m)}, O^{(n)}),$$

和

$$\text{如果} Pf(m, n) \text{不成立,则} \vdash_{\mathscr{N}} \sim\mathscr{P}(O^{(m)}, O^{(n)}).$$

粗略地讲,将存在一个公式 $\mathscr{P}(x_1, x_2)$,使得能在系统内判定"元问题", 对任何公式的序列 $\mathscr{A}_1, \cdots, \mathscr{A}_k, \mathscr{A}$, 它是否构成 $\mathscr{N}$ 内的一个证明. 我们正在做的, 就是企图把系统 $\mathscr{N}$ (至少部分地)当作自身的元系统,在前一章讨论的意义之下. 从表面上看,这样的一个程序似乎是危险的, 容易引出一个矛盾, 但是我们知道: 只有在 D_N 上的递归关系才是在 $\mathscr{N}$ 内可表达的,所以肯定不能对 D_N 上的一切关系将这程序进行到底, 而把 $\mathscr{N}$ 当作它自己的元系统必

然将只是部分的，正因这样，一个矛盾才得以避免.

在哥德尔定理证明的下一步是去证明. 从关于公式、定理和证明的考查所产生的 D_N 上的某些关系是递归的，从而在 $\mathscr{N}$ 内是可表达的. 我们将删去详细的证明，只列出某些这样的关系.

命题 6.29

下列 D_N 上的关系是递归的，因此在 $\mathscr{N}$ 内是可表达的.

(i) Wf　$Wf(n)$成立，当且仅当 n 是 $\mathscr{N}$ 的一个公式的哥德尔数.

(ii) Lax　$Lax(n)$成立，当且仅当 n 是 $\mathscr{N}$ 的一条逻辑公理的哥德尔数.

(iii) $Prax$　$Prax(n)$成立，当且仅当 n 是 $\mathscr{N}$ 的一条特有公理的哥德尔数.

(iv) Prf　$Prf(n)$成立，当且仅当 n 是 $\mathscr{N}$ 的一个证明的哥德尔数.

(v) Pf　$Pf(m, n)$ 成立，当且仅当 m 是哥德尔数为 n 的公式的一个证明的哥德尔数.

(vi) $Subst$　$Subst(m, n, p, q)$ 成立，当且仅当，对哥德尔数为 n 的表示式中，用哥德尔数为 p 的项代入哥德尔数为 q 的变元的所有自由出现后所得公式的哥德尔数是 m.

(vii) W　$W(m, n)$ 成立，当且仅当 m 是一公式 $\mathscr{A}(x_1)$ 的哥德尔数，其中 x_1 自由出现，n 是 $\mathscr{A}(O^{(m)})$ 在 $\mathscr{N}$ 中的一个证明的哥德尔数.

(viii) D　$D(m, n)$成立，当且仅当 m 是一个公式 $\mathscr{A}(x_1)$ 的哥德尔数，其中 x_1 自由出现，n 是公式 $\mathscr{A}(O^{(m)})$ 的哥德尔数.

练习

15. 求对应于下列码数的 $\mathscr{L}$ 的符号(如果有的话)

(a) 65

(b) 299

(c) 109

(d) 421

16. 求对应于下列码数的 $\mathscr{L}$ 的公式:

(a) $2^{61}\times 3^{3}\times 5^{15}\times 7^{5}$;

(b) $2^{9}\times 3^{61}\times 5^{3}\times 7^{15}\times 11^{5}$;

(c) $2^{3}\times 3^{13}\times 5^{15}\times 7^{5}\times 11^{61}\times 13^{3}\times 17^{15}\times 19^{5}$.

17. 每一个自然数,通过它的素数幂乘积表示,与唯一的自然数序列对应. 例如数 $2^4\times 3\times 5^7\times 11^2$ 对应于 4, 1, 7, 0, 2. 两个序列能够通过毗连结合起来,也就是说,可以扩充一个序列,通过把另一序列的元素附加上去的办法. 例如,如果 s 是序列 2, 3, 5, t 是序列 4, 7, 9, 10, 那么 $s*t$ 是序列 2, 3, 5, 4, 7, 9, 10. 定义一个函数 f: $D_N^2\to D_N$:

$f(m, n)=s*t$ 的码数,这里 s 和 t 是码数为 m 和 n 的序列.

证明 f 是递归的.

6.5 不完全性的证明

在命题 6.29 中所定义的关系 W 是不完全性证明的关键,所以要力图掌握它的意义. 注意它涉及把项 $O^{(m)}$ (对应于数 m) 代入哥德尔数为 m 的公式 $\mathscr{A}(x_1)$ 中.

W 在 $\mathscr{N}$ 中是可表达的,所以有一公式 $\mathscr{W}(x_1, x_2)$, 其中 x_1, x_2 自由出现,使得

$$\text{如果 } W(m, n) \text{ 满足,则} \vdash_{\mathscr{N}} \mathscr{W}(O^{(m)}, O^{(n)}),$$

和

$$\text{如果 } W(m, n) \text{ 不满足,则} \vdash_{\mathscr{N}} \sim\mathscr{W}(O^{(m)}, O^{(n)}).$$

考虑公式

$$(\forall x_2)\sim\mathscr{W}(x_1, x_2).$$

令 p 是这个公式的哥德尔数,最后考察用 $O^{(p)}$ 代入 x_1 后所得

的公式，即

$$(\forall x_2)\sim(\mathscr{W}O^{(p)},\ x_2).$$

用 $\mathscr{U}$ 表示最后这个公式．在现阶段给出 $\mathscr{U}$ 的一个粗糙的解释，将有助于明了它的意义．首先，W 是 $\mathscr{W}$ 的解释．因此，$\mathscr{U}$ 可以解释为：

"对于每个 $n\in D_N$，$W(p,\ n)$ 并不成立"．

加以展开，就成为：

"对于每个 $n\in D_N$，p 是一 x_1 在其中自由出现的公式 $\mathscr{A}(x_1)$ 的哥德尔数，且 n 是 $\mathscr{A}(O^{(p)})$ 在 $\mathscr{N}$ 中的一个证明的哥德尔数，这种情况是不可能的"：

现在 p 是一个其中 x_1 自由出现的公式的哥德尔数，即 $(\forall x_2)\sim\mathscr{W}(x_1,\ x_2)$ 的哥德尔数，如果这个公式用 $\mathscr{A}(x_1)$ 来表示，那么 $\mathscr{A}(O^{(p)})$ 是公式 $\mathscr{U}$．因此 $\mathscr{U}$ 的解释相当于：

"对于每个 $n\in D_N$，n 不是公式 $\mathscr{U}$ 在 $\mathscr{N}$ 中的一个证明的哥德尔数"．

所以，在一种意义下，公式 $\mathscr{U}$ 可以看作是对它自己的不可证性的断定．

假如 $\mathscr{N}$ 不一致的话，那么它将显然是完全的，因为每个公式都将是一条定理．因此不完全性定理要求假设：$\mathscr{N}$ 是一致的．事实上，哥德尔的证明要求一个稍强一点的假设．而这个正是我们现在必须加以研究的．

定义 6.30

与 $\mathscr{N}$ 有相同语言的一阶系统 S 是 ω—一致的，如果不存在任何公式 $\mathscr{A}(x_1)$，其中 x_1 自由出现，使 $\sim(\forall x_1)\mathscr{A}(x_1)$ 是 S 的定理，而同时对每个 $n\in D_N\mathscr{A}(O^{(n)})$ 是 S 的定理．

如上面所见（参见注记 6.6），如果 $\mathscr{A}(O^{(n)})$ 是一条定理，对每个 n，$(\forall x_1)\mathscr{A}(x_1)$ 并不必定是一条定理．ω—一致性断定，如果每个 $\mathscr{A}(O^{(n)})$ 是一条定理，则 $\sim(\forall x_1)\mathscr{A}(x_1)$ 不是一条定理，而不管

$(\forall x_1)\mathscr{A}(x_1)$ 是否为一定理.

命题 6.31

令 S 是一与 $\mathscr{N}$ 有相同语言的一阶系统. 如果 S 是 ω—一致的,则 S 是一致的.

证明 令 $\mathscr{A}(x_1)$ 是任意一个公式,而 $\mathscr{A}(O^{(n)})$ 对每个 n,是 S 的一条定理. 例如, $\mathscr{A}(x_1)$ 可以是 $x_1=x_1$. 因此, 据 ω—一致性, $\sim(\forall x_1)\mathscr{A}(x_1)$ 不是 S 的一条定理. 因此 S 是一致的(因为存在一个不是定理的公式).

命题 6.32 (哥德尔不完全性定理)

在 $\mathscr{N}$ 是 ω—一致的假设下,公式 $\mathscr{U}$ 不是 $\mathscr{N}$ 的一条定理,它的否定也不是定理. 因此, 如果 $\mathscr{N}$ 是 ω—一致的, 则 $\mathscr{N}$ 是不完全的.

证明 首先假设 $\mathscr{U}$ 是 $\mathscr{N}$ 的一条定理, q 是 $\mathscr{U}$ 在 $\mathscr{N}$ 中一个证明的哥德尔数. 如前, 令 p 是 $(\forall x_2)\sim\mathscr{W}(x_1, x_2)$ 的哥德尔数. 因此. $W(p, q)$ 成立. W 在 $\mathscr{N}$ 中可由 $\mathscr{W}$ 表达, 所以我们有

$$\vdash_{\mathscr{N}} \mathscr{W}(O^{(p)}, O^{(q)}).$$

但是 $\vdash_{\mathscr{N}} \mathscr{U}$, 即 $\vdash_{\mathscr{N}} (\forall x_2)\sim\mathscr{W}(O^{(p)}, x_2)$, 所以 $\vdash_{\mathscr{N}} \sim\mathscr{W}(O^{(p)}, O^{(q)})$, 用了 $(K5)$ 和 MP. 这与 $\mathscr{N}$ 的一致性矛盾,所以 $\mathscr{U}$ 不可能是 $\mathscr{N}$ 的一条定理.

$\mathscr{U}$ 不是 $\mathscr{N}$ 的一条定理, 就是说不存在 $\mathscr{U}$ 在 $\mathscr{N}$ 中的证明, 所以不存在 q, 使得 q 是在 $\mathscr{N}$ 中 $\mathscr{U}$ 的一个证明的哥德尔数, 即 $(\forall x_2)\sim\mathscr{W}(O^{(p)}, x_2)$ 在 $\mathscr{N}$ 中不可证. 因此, $W(p, q)$ 对任意数 q 都不成立. 所以

$$\vdash_{\mathscr{N}} \sim\mathscr{W}(O^{(p)}, O^{(q)}) \text{ 对每个 } q$$

因此,根据 ω—一致性

$$\sim(\forall x_2)\sim\mathscr{W}(O^{(p)}, x_2)$$

不是 $\mathscr{N}$ 的一条定理，即$(\sim\mathscr{U})$不是一条定理。

注记 6.33

我们曾经明确地叙述了 ω-一致性的假设，尽管，利用模型N，关于 $\mathscr{N}$ 的 ω-一致性有一明显的证明。但是，如前面所提及，利用模型的论证容易牵涉其它形式系统(常是关于其一致性)的假设，从而容易流于用未经证明的假定来论证问题。命题 6.32 也可以推广到其它形式系统，$\mathscr{N}$ 的扩充中，因此，在缺乏任何特殊信息的情况下确实必须作 ω-一致性的假设。

▷本章迄今为止已经概述了哥德尔不完全性定理的证明。我们在此力图使读者对所涉方法有某些感性的体会，并希望对它的意义作出某种程度的说明。为此，现在让我们来考察某些推论和推广。

命题 6.34 (假设 $\mathscr{N}$ 是 ω 一致的)

$\mathscr{N}$ 含有一个闭公式，它在模型 N 中为真但不是 $\mathscr{N}$ 的定理。

证明。公式 $\mathscr{U}$ 是一闭公式。$\mathscr{U}$ 和$(\sim\mathscr{U})$都不是 $\mathscr{N}$ 的定理。但是，或者 $\mathscr{U}$ 在 N 中真，或者$(\sim\mathscr{U})$在 N 中真，因为 N 是一个解释。

▷事实上，在这个命题中的假设还可以减弱。

命题 6.35 (假设 $\mathscr{N}$ 是一致的)

$\mathscr{N}$ 含有一个闭合式公式，它在模型 N 中为真但不是 $\mathscr{N}$ 的定理。

证明 命题 6.32 的证明必须作修改，它在较弱的假设下仍然成立，但公式 $\mathscr{U}$ 也必须修改。我们略去详细的证明。

▷$\mathscr{N}$ 是不完全的。现在我们第一个想法可能是：我们能否使 $\mathscr{N}$ 完全？也许我们为 $\mathscr{N}$ 选择了一个不充分的公理集，也许我们把公式 $\mathscr{U}$ 增添为新公理后，这新系统可能是完全的。某些有关本章中涉及的程序的想法应已表明。增添 $\mathscr{U}$ 为新公理是无助的。令 $\mathscr{N}^{+}$ 表示由 $\mathscr{N}$ 通过增添 $\mathscr{U}$ 为新公理之后所得的系统。公理组的

这种变化并不影响结果，每个递归的关系是可表达的(虽然这可能影响逆命题)．虽然，关系 $Prax$ 和 Pf 的递归性以及其它一些用这些关系定义的项可能受到影响．但是补加单一的公理并不影响公理的哥德尔数的集合的递归性，因为任何一个单元集是递归的，并且两个递归集的并是递归的．关系 $Prax$ 仍是递归的，类似地 Pf 和另外一些关系，包括 W 也都可以看出是递归的，尽管它们的定义是参照 $\mathscr{N}^+$ 而不是参照 $\mathscr{N}$ 的．因此，与对 $\mathscr{N}$ 相同的展开可以实施，导致一个涉及不同的公式 $\mathscr{U}'$ 的不完全性定理．

沿此思路，通过更为一般的论证，我们得到了下面的命题．

命题 6.36

令 S 是 $\mathscr{N}$ 的任何扩充，它使得 S 的特有公理的哥德尔数集是递归集．那么(在 S 是一致的假设下) S 是不完全的．

注记 6.37

关于 S 的假设恰好是 $Prax_S$ 关系是递归的假设，其中 $Prax_S$ 的定义：$Prax_S(n)$ 成立，当且仅当 n 是 S 的特有公理的哥德尔数．正是这个假设，能使一个对应于命题 6.29 的命题在 S 中得以证明．

▷ 从最后一个命题可得：$\mathscr{N}$ 通过增添其哥德尔数构成有限或无限递归集的公理集，不可能成为完全的．

正如我们已经注意到的，系统 $\mathscr{N}$ 在一种特殊的意义下是有所不足的．它的公理组只包括数学归纳原理的一种弱的形式．这是因为使用了一阶语言．通过考察二阶的算术系统，能否避免不完全性的困难呢？在本书中，我们曾经有意地避免了卷入于二阶系统的额外的复杂性，所以对这个问题的任何研究都已超越了我们的范围．不过，已经知道，二阶算术系统也有同样的性质，即一个一致的二阶算术系统，当它的特有公理的(哥德尔数的)集是递归集时，它也是不完全的．

哥德尔定理的后果比这还深远得多．我们已经看到，在 ZF 形式系统中可以定义自然数系统．任何集合论的形式系统，只要它对于集合论是充分的，都将分享这个性质，并且确实地比 ZF 更为局限的系统也有分享这个性质的．（反例是我们的群论的形式系统，它过于局限了．）

命题 6.38

任何充分丰富的一致系统，如果它的特有公理的（哥德尔数的）集是递归的，那么它是不完全的．（一个系统是充分丰富的是指，在它当中可以如上定义自然数系统，从而使算术公理成为定理）．特别地，如果 ZF 是一致的，那么它是不完全的．

▷ 最后，让我们考察一个有些敏锐的读者可能已经注意到的问题：是否存在 $\mathcal{N}$ 的完全的扩充．哥德尔不完全性定理的假设包含要求：所谈及的形式系统，具有一组哥德尔数集为递归集的固有公理．这个假设对证明来说是必要的，因为在定理的证明中涉及到某些关系也是递归的证明．至于存在一个一致的且完全的一阶算术系统，因而它是不满足这个要求的，这一点用第四章中给出的程序可以看出如下．

考察 $\mathcal{N}$ 的一个扩充，它通过囊括在 N 中为真的一切 $\mathcal{N}$ 的公式为公理而得．这个扩充是完全的且是一致的，假如 $\mathcal{N}$ 是一致的（见系 4.47）．因此，据命题 6.36，这个扩充的特有公理的哥德尔数集不可能是递归的．由此可得，在 N 中为真的 $\mathcal{N}$ 的公式的哥德尔数集，就是非递归集的一个例子．

因此，如果我们允许我们的特有公理集是非递归的话，我们就能有一个一致的且完全的一阶算术系统．由这带来的问题是：当把哥德尔不完全性定理的结果看做是有意义时，使得递归集有价值的是什么呢？以下说法并不是真实的：凡一致的形式算术系统都不是完全的．我们所能说的一切只是：没有一个其公理的（哥德尔数的）集是递归的系统是完全的．那个答案在于可计算性、能行性

和算法的观念，以及它们同递归观念的关系．我们在下一章详细论述它们．

练习

18．令 $\mathscr{U}$ 如书中所定义．$\mathscr{U}$ 不是 S 的一条定理，所以通过增添($\sim\mathscr{U}$)为公理而得的 $\mathscr{N}$ 的扩充是一致的(预先假设 $\mathscr{N}$ 是一致的)．证明这个扩充不是 ω^{-} 一致的．

第七章　可计算性，不可解性，不可判定性

7.1　算法和可计算性

在1900年世界数学大会上，希尔伯特提出了值得纪念的突出的数学未解决问题的目录，其中之一（现在叫做希尔伯特第十问题）是寻找任何丢藩都多项式方程是否有一整数解的判定程序。问题的解（直到新近才找到—见戴维司(Davis)[1]）可能会使1900年时希尔伯特的听众感到惊奇（甚至可能包括希尔伯特本人），因为它并不是由所要求找的程序的一组指令组成的，而是一个这样的程序不可能存在的证明。希尔伯特第十问题是现在通常所说的"不可解问题"的例子，或者更精确地说是一个递归不可解问题。这个问题以及类似的问题的研究，在本世纪初把数学家引导去考察该问题所用到的词"程序"的意义。这种考察引出了本章所要描述的思想和应用。

在这里，和"程序"具有同样意义的另一个词是"算法"，以后一般地我们将使用后者，因为"程序"这个词还有另外的超出本课文范围的意义，容易引起误解。算法的观念是直觉的，数学上并不精确的观念我们可以定义如下。

定义　7.1

一个算法是一个计算程序（并不必定是数值的）的一个明确的能行指令集，用它可以找到给定的一类问题中的任一个的解答。

这样说了以后，自然地会提出适合于各种"问题类"的算法的存在性问题。在希尔伯特第十问题中，问题的类是

{方程 E 存在一个整数解吗？| E 是丢藩都多项式方程。}

例 7.2

人们可以考察任何的问题类，例如

(a) $\{f(n)$的值是什么？$|n\in D_N\}$ （f 是一固定函数）.

(b) $\{n$ 是集合 A 的元素吗？$|n\in D_N\}$ （A 是一固定集）.

(c) $\{\mathscr{A}$ 是 $\mathscr{N}$ 的一条定理吗？$|\mathscr{A}$ 是 $\mathscr{N}$ 的合式公式$\}$.

例 7.3

(a) $\{2$ 是 n 的因子吗？$|n\in D_N\}$.

有一种算法，它为这个问题提供解答．给出任意数 n，用 2 除后找出它的余数（使用关于除法的几个熟知的初等学校程序中的任一个）．如果余数是 0，我们回答：是的．如果余数是 1，我们回答：不是．

(b) $\{n$ 属于素数集吗？$|n\in D_N\}$.

对这个问题有一种算法．给出任意数 n，有标准的方法，求出当 n 被 m 除时的余数，对每个 $m(1<m<n)$．如这些余数没有一个为 0，那么 n 是素数．如果有一个或几个是 0，那么 n 就不是素数．

(c) $\{f(n)$的值是什么？$|n\in D_N\}$，其中 f 是 $f(n)=2n(n\in D_N)$.

在这种情况下，初等算术也提供了一种计算 f 的值的方法．

(d) $\{$方程 E 的复数解是什么？$|E$ 是整系数的 2 次方程.$\}$

有一众所周知的代数公式，为这种情况提供了一个算法．

▷要注意，“问题类”在这里是一个很一般的概念．让我们暂且限于考察与具有特殊性质的问题类有关的算法，那就是在上面的例 7.3(c) 中所显示的．换言之，让我们去考察“由算法可计算的函数”（以下简称可计算函数）的概念．在这个学科的发展历史上，它是最早引起注意的方面．几位研究者曾独立地作出了尝试，要在数学的方式下使算法的概念精确化，并在数学的方式下去刻划算法可计算函数类的特征．当然，概念的任何特殊的数学描

述是否严格对应于直觉观念，并非某种可以证明的东西．不过，如我们将要看到的，有较好的理由假设，算法的某种数学描述足够一般，以致能够包括一切直觉的算法．

由较早的研究者给出的描述取不同的形式，粗略地可以划分如下：

(a) 抽象(精确地定义的)计算机．

(b) 计算程序的形式结构．

(c) 产生函数类的形式结构．

前两种给出了算法概念本身的特征((a)和(b)两者间不存在原则上的差别)．最后一种给出了算法可计算函数类的描述．

(a) 例是图灵机，是由图灵于1930年设计的．它是关于一种理想机的设想，在一个理想的纸带上打印上编码形式的输入数，随后根据预先给出的简单的有限制的规则工作，计算结束时纸带上得到用类似的编码形式的输出数．可以断言，计算一个函数的任何算法，都认为可转换为适合这样的一部机器的指令．

(b) 例是瑟(Thue)系统，它纯粹是一形式系统，在这种系统中，符号序列可以作为其它的符号序列依靠某些规则的推论而"演绎"出来．这样，给出一个输入序列后，这些规则允许它转换为一个输出序列．

递归函数提供了(c)的一个实例．基本函数和规则是生成一函数类的形式结构．

所有这些结构都有一共同之处，即他们都包括偏函数，有理由说，一个偏函数是算法可计算的，如果存在一种算法，只要它是被定义的就能求出函数的值，在图灵机情况，这相当于允许机器的规则可导致永不结束，从而永无输出的计算．在递归函数情形，这相当于允许按无限制的方式去使用最小运算，如在注记6.13中所指出．

关键的结果是，算法可计算(偏)函数的所有不同的刻划都导

致同样的类，即递归偏函数类①．这是某种能够证明的东西，并且已经证明了的．不能够证明的是，这类偏函数类是否恰好等同于算法可计算函数类．不过，根据有正面证据而缺反面证据的情况，我们还是接受丘奇论题．那就是

算法可计算偏函数类等同于递归偏函数类．

注记 7.4

丘奇论题的接受无非是我们直觉的算法观念与已经给出的数学描述一致起来的具体化．没有证据表明，这样的做法是不合理的．

▷在丘奇论题的假设之下，关于算法的存在性问题，在数学上变得较易处理了．例如：是否存在计算一个特殊函数的值的问题就变成了函数是否递归的问题．另一个例子，是否存在判定 D_N 的给定子集的成员的问题，就变成了这个集的特征函数是否递归的问题，即这个集是否递归的问题，

丘奇论题的用处在于这样一件事实，可以用数学技术去说明一个已知函数或集合是(或不是)递归的，因而可以去证明对一个特殊的问题类有(或没有)一种算法存在．反之，已经找到了一个特殊的算法，由此推演与之相应的集或函数是递归的，也是经常要用到的．

读者可能注意到丘奇论题的一半比另一半更为充实，丘奇论题等价于以下两个命题的合取，这两个命题是：

(i) 每个算法可计算偏函数是递归的偏函数，

和

(ii) 每个递归偏函数是算法可计算的．

第二个断定是经得起证明的检验的，因为使用一个合理的直觉的算法概念，可以给出一个它的归纳"证明"．这可以从描述计算每

① 术语'偏递归函数'在文献中比'递归偏函数'要来得标准，但我们在这里使用后者是为了清楚起见．

个基本递归函数(归纳基础步骤)的算法着手，然后通过说明怎样用计算特殊函数的算法去构造能够计算从它们用规则 I, II, 和 III 得到的函数的算法.

上面说到的第一个断定是丘奇论题中不可证明的部分. 已经证明了的是,对于算法的大量的不同的数学上的精确定义,根据它们所得到的可计算的偏函数都是递归的.

从所有这一切可以看到，如果要把递归的技术用在关于特殊的问题类有无算法存在的讨论中,而如果答案是不存在算法的话,那么丘奇论题就是必不可少的.仅当假设丘奇论题成立时,我们才能从一个特殊的函数或集合不是递归的结论,推出算法的不存在.

例 **7.5**

(a) 设 f 和 g 是定义在 D_N 上的一元函数，并且它们是算法可计算的. 那么 $f\circ g$ 也是算法可计算的. 因为要计算 $f\circ g(n)$ 只须先用计算 g 的算法去算出 $g(n)$，然后再用计算 f 的算法去算出 $f(g(n))$. 这可以很容易地加以推广,应用到构造递归函数的规则 II 上面去.

(b) 令 $f: D_N\to D_N$ 是从函数 g 通过以下的式子递归定义的:

$$f(0)=k$$
$$f(n+1)=g(n, f(n)).$$

并假设 g 是算法可计算的. 我们可以给出一个算法去计算 $f(m)$，对任何 $m\in D_N$. 如果 $m=0$，那么 $f(m)=k$. 如果 $m>0$，计算 $f(1)=g(0, f(0))$，这里用关于 g 的算法，然后有 $f(2)=g(1, f(1))$，用关于 g 的算法,以此类推,最终可以求得 $f(m)$ 的值.

(c) 一个(b)的特殊情形是阶乘函数: $f(n)=n!\ (n\in D_N)$. 为了计算比如说 10!，在实际上我们做的是遵循(b)中所给的程序，依次计算 1!, 2!, 3!, …9!, 10!.

(d) 考察函数 $h: D_N\to D_N$，它由 $h(n)=1/n$ 的十进表示式中第一个非零数字给出. 有可能从定义直接证明 h 是递归的，不过

那将是一个相当复杂的程序，另一方面，我们也可以描述一个算法用来计算函数的值，然后利用丘奇论题，推出它是递归的．这算法来自标准的除法程序．首先求得 k 的最小值，使得 $n<10^k$，然后求出以 n 除 10^k 的商．

(e) 我们知道在 N 中为真的 $\mathscr{N}$ 的合式公式的哥德尔数的集不是递归的．因此，从丘奇论题可知，解答下述一类问题的算法是不存在的：

$$\{\mathscr{A}\text{ 在 }N\text{ 中是真的吗？}\mid\mathscr{A}\text{ 是 }N\text{ 的一个合式公式}\}.$$

(f) 令 A 是 D_N 的子集，它由所有可表为两个数的平方和的数所组成．A 是递归的，但是要直接证明函数 $f: D_N\to D_N$

$$f(n)=\begin{cases}0 & \text{如果存在 } p,\ q\in D_N,\text{ 使得 } n=p^2+q^2.\\ 1 & \text{相反}\end{cases}$$

的递归性是相当困难的．然而，却有一种算法能回答这类问题：$\{n$ 是否属于 A？$\mid n\in D_N\}$．我们可以把它描述如下．给出 n，计算 p，q 都小于 n 的每一对数的平方和 p^2+q^2．如果对某些对 p，q，$p^2+q^2=n$，那么答案就是肯定的，如果不存在 p，q，使得 $p^2+q^2=n$，那么答案就是否定的．于是，根据丘奇论题，A 是递归集．

▷所有这一切和命题 6.36 中的假设：特有公理的哥德尔数集必须是递归的有什么关系呢？根据丘奇论题，对于任何具有这种性质的系统 S，都将有一种算法存在，能回答下面一类问题：

$$\{\mathscr{A}\text{ 是否为 }S\text{ 的特有公理？}\mid\mathscr{A}\text{ 是 }S\text{ 的一个公式}\},$$

而由于 S（或任何一阶系统）的逻辑公理的哥德尔数集是递归的，也将存在一种算法能回答下面一类问题：

$$\{\mathscr{A}\text{ 是 }S\text{ 的一个公理吗？}\mid\mathscr{A}\text{ 是 }S\text{ 的一个公式．}\}$$

再者，对于不具有这种性质的系统，将不会存在这种算法．

按照引进形式系统思想时我们所取的观点，即试图用形式系统去反映实际的数学内容，并使之精确化，我们能够看到．一个形式系统 S，如果不存在判定 S 的一个给定的公式是否为 S 的公理

的算法，那么它是不能令人满意的．在判定哪些数学的陈述为真时它是无能为力的，因为在判定哪些陈述相应于作为公理的公式上面，不存在能行的程序，在判定一个给定的公式序列是否为一个证明上面也不存在能行的程序．研究形式系统最初的一个目标就是探求能够判定任何数学陈述是否为真的形式程序，通过把尽可能多的真公式包括到可证公式之中．一个其公理集并非递归的形式系统是不可能有用处的，而一个其公理集是递归的形式系统，确实能能够满足判定什么是公理，什么是证明的能行程序的要求．可是不完全性定理说，即使是这样的（算术的）一个系统也是没有用处的，因为系统的定理集并不包括一切真的（在解释 N 中）公式．

注记 7.6

读者可留意考察系统 $\mathcal{N}$，其中特有公理的（哥德尔数的）集是递归的，并设计一个能行程序，使 $\mathcal{N}$ 的定理集得以枚举．（提示：在哥德尔数对上的关系 Pf 是递归的，因此存在一个判定它是否由已知数对满足的算法）．这表明 $\mathcal{N}$ 的定理的（哥德尔数的）集是"能行可枚举的"．这为我们带来了一个新概念．

定义 7.7

D_N 的一个子集称为递归可枚举的，如果它是一个递归函数的值域，或者它是一个空集．

一个集是递归可枚举的，如果存在一个递归函数 f，使得 $f(0)$，$f(1)$，$f(2)$，…是该集的一切成员的一个序列（可以重复）．丘奇论题蕴涵："递归可枚举的，是等价于'能行可枚举的，．

▷我们现在直接可以提出的问题是："递归"和"递归可枚举的"是两个有区别的概念吗？是否存在"递归"而不"递归可枚举的"集合，或反过来呢？下面对这个问题的部分回答所作的证明，是一个运用丘奇论题的很好的实例．

命题 7.8

每个递归集是递归可枚举的．

证明 令 A 是一个递归集，以致它的特征函数 C_A 是算法可计算的. 我们描述一个枚举 A 的成员的算法. 依次计算 $C_A(0)$, $C_A(1)$, …的值，并且列出使得 $C_A(n)=0$ 的所有数 n 的表. 因此，根据丘奇论题，由于 A 是能行可枚举的，所以 A 是递归可枚举的.

▷逆命题不能成立. 对此有多种证明，因为我们只需要一个反例. 我们将通过证明关于系统 $\mathscr{N}$ 的一个重要结果来提供一个.

定义 7.9

一个形式系统称为递归不可判定的，如果系统中定理的哥德尔数集不是递归的.

注意，运用丘奇论题，一个形式系统 S 是递归不可判定的，当且仅当，不存在回答下列一类问题的算法.

$$\{\mathscr{A}\text{ 是一条定理吗？}\mid\mathscr{A}\text{ 是 }S\text{ 的一个公式}\}.$$

▷以后我们在某些准备之后将证明，$\mathscr{N}$ 是递归不可判定的，注记 7.6，连同丘奇论题表明，$\mathscr{N}$ 的定理的（哥德尔数的）集是递归可枚举的. $\mathscr{N}$ 的递归不可判定性意味着这个集不是递归的.

系理 7.10

存在 D_N 的一个子集，它是递归可枚举的但不是递归的.

本章后面部分的内容将关注递归不可判定性和更为一般的递归不可解性概念. 这后一概念是什么我们已经有一些想法，然而现在让我们把它精确化，以便今后参照.

定义 7.11

一类问题称为递归不可解的，如果不存在一个单一的算法，能对该类中的每个问题提供解答.（注意在这个定义中，'递归地'这个词的使用，隐含着丘奇论题的假设.）

这样，一个形式系统 S 是递归不可判定的，当且仅当问题类

$$\{\mathscr{A}\text{ 是 }S\text{ 的定理吗？}\mid\mathscr{A}\text{ 是 }S\text{ 的一公式}\}$$

是递归不可解的.

练习

1．描述为下列问题类提供解答的算法．

(a) $\{n$ 是 $\mathscr{N}$ 一个项的哥德尔数吗？$|n\in D_N\}$．

(b) $\{m$ 和 n 的最大公约数是什么？$|m, n\in D_N\}$．

(c) $\{n$ 是一完全平方数吗？$|n\in D_N\}$

(d) $\{\mathscr{A}$ 是 L 中集 Γ 的后承吗？$|\mathscr{A}$ 是 L 中的一公式$\}$（Γ 是 L 中公式的一个固定有限集）．

(e) {函数 f 的导数是什么？ $|f$ 是一个实变数的多项式函数}．

(f) $\{$第 n 个奇素数是什么？$|n\in D_N\}$．

2．求证对于 D_N 的任何子集 A，如果 A 和它的补集都是递归可枚举的，那么 A 是递归的．（提示：用丘奇论题．）推演：存在 D_N 的一个子集，它既非递归的也非递归可枚举的．

3．证明．如果一个无限集 A 按递增顺序是递归可枚举的（即，如果有一递归函数 f，使得 $f(0), f(1), f(2), \cdots$ 是 A 的全体成员，并且 $f(n)<f(n+1)$ 对每个 $n\geqslant 0$），那么 A 定递归的．

4．证明下列函数是递归的．

(a) ϕ，$\phi(n)=$ 比 n 小且和 n 没有公因子的正整数 p 的个数 $(n\in D_N)$．

(b) f，$f(m, n)=$ 大于 m/n 的最小整数，$(m, n\in D_N)$．

(c) g，

$$g(n)=\begin{cases}0 & \text{如果存在一个在 } \pi \text{ 的十进表示式中至少有 } n \text{ 个 7 的序列，}\\ 1, & \text{相反情况．}(n\in D_N)\end{cases}$$

(d) q，

$$q(m, n)=\begin{cases}\mathscr{A}\to\mathscr{B}\text{的哥德尔数}. & \text{如果 } m, n \text{ 是 } \mathscr{N} \\ & \text{中公式 } \mathscr{A} \text{ 和 } \mathscr{B} \text{ 的哥德尔数}. \\ 0, & \text{相反情况}. \ (m, n\in D_N)\end{cases}$$

5. 给出下述的实例

(a) 一个有非递归子集的递归集.

(b) 一个有无限递归子集的非递归集.

6. 证明. 每个无限的递归可枚举集,有一个无限递归子集.

7.2 图灵机

对算法概念的计算特征作深入到细节的刻划，是一个有实际价值的操作. 图灵的刻划是最有用处和最容易理解，它可以直接应用于判定性和可解性问题,正如我们将要看到的.

读者不要被机器这个词的使用引起误解. 图灵机并不是实际上在使用中的计算机. 它们是一个用数学方法精确地加以定义,使能反映计算程序的抽象的系统. 我们所用的术语,清楚地暗示"机器"的功能,而能遵循"理想的"图灵机的程序的真正的机器也的确可以制造出来.

图灵在描述他的机器时的目标，是想把计算归结为最基本的要素,以便能用简单的方式去描述某些基本的程序,它们显然是能行的，而且任何能行的程序都可归结到它们. 现在让我们来考察那些技术细节.

一个图灵机可以看作是有一纸带通过的黑箱，这纸带分成相等的方格，在方格上可以印也可以不印符号. 对一个特殊的计算而言,机器将从纸带上有限量的输入信息出发,即从只在有限多个纸带方格中打印的符号出发,机器按照某些规则处理纸带,最终可以停下来也可以永远停不下来. 如果停下来,那么在纸带上留下的就是输出信息；如果停不下来，那么计算是不确定的，而没有输出.

在进一步阐述之前，在上面提到的有两点须要说明. 输入信息是有限的要求看来无疑是合理的，说实在的，读者可能会问，有什么必要提它呢，因现实的纸带长度总是有限的，它只能由有限多个相等的方格组成. 但是，对于输入信息所要用的纸带在长度上加以一定的限制，将是不合理的. 再者当机器处理纸带时，它可能要求比原来在输入纸带上提供的，有更多的"工作空间"，为此我们将把纸带看作是可以无限制的延伸的. 还有，任何计算都只将要求有限长的纸带，但是对纸带需要的长度给以绝对的界限，也将是不合理的，所以我们将说纸带长度应该是潜在地无限的.

除了对纸带的长度不加限制外，我们对机器为计算一个特殊的算题所要化的时间也将不加限制. 在一个实际的计算机，我们总是被迫设置一个时间的界限，如果在那个时间界限内，不能产生答案，那么我们不得不放弃该程序而试图找出能缩短需要时间的另一程序. 可是，对我们的抽象机器来说，对求得答案所需步骤和时间加以一个绝对的界限，那将是一人为的限制. 我们将要求的一切是，如果有一个答案，那么机器在有限步骤后于有限时间内能将它产生出来. 因此，在一个计算过程中，我们可能不知道(一般地我们将并不知道)计算是否会终止.

为了研究这样的机器能够做些什么，必须详细说明两个方面，在纸带上可能出现的符号信息的性质，和机器能够处理它的方式.

一个图灵机有一纸带符号的字母库，它对不同的机器可以是不同的，但是它毕竟总是一有限的符号列. 每个纸带方格，在一个时刻最多可以被打印上这些符号中的一个. 在这个符号列中，按惯例总包括字母 B，它将表示一空白方格. 最简单的图灵机将仅有两个纸带符号，B 和 1.

一图灵机按下述方式操作. 在任一给定的时间，机器"读着"纸带上一个方格. 它可以用另外的符号去替换呈现在方格上的符号(如果有符号的话)；或者如果方格空白的话可以打印上一个符

号，或者保持方格不变，在这种情况下，它可以转移视线至纸带上紧靠着右边或左边的方格，所以我们有下面的操作类型：

(a) 打印上一个符号．（打印上一个符号包括首先擦去原有的符号．）擦去一个符号，即打印上 B，也属于这一类型的操作．

(b) 向左移一格．

(c) 向右移一格．

在这机器操作中的一步就是指上述类型的一次运算．

其次，我们必须详述，机器在每个阶段是怎样选择它要执行的操作的．它的行动过程是由出现在被读着的方格上的符号和机器的内状态所决定的．机器允许具备有限多个内状态的任何一个．照实际的计算机来说，内状态可以看作是在某一时刻贮存在机器中的一切信息的总和．我们对贮存的信息的机械性能和电学性能并不关心，我们只假设，黑箱有有限多个使之按某种方式行动的不同条件．

不过，显然得采取措施，使图灵机的内状态在计算过程中能够改变，因此在计算中每一步都得要求对下列四点有所指定：

(1) 机器目前的内状态．

(2) 正被读着的方格中的内容．

(3) 机器所采取的动作．

(4) 机器下一步将取到的内状态（为下一步的计算作准备）．

因此，机器在给定时刻所取的内状态将是前面计算的整个过程的一个结果，在这个意义上，它扮演了机器中"记忆"的角色．

在这里还要说一下关于加在图灵机的内状态数目上的有限性条件．实际的数字计算机确实只有有限多个内部状态，尽管通常它的这个数字非常之大．但是，如前述理由，对图灵机所允许的状态的数目加以特殊的界限是不合理的，那怕是一个极大的数字．因此，我们仅仅要求这个数是有限的．

指定一台图灵机将要遵循的程序的最方便的办法，是用如下

形式的一个有限的四元组的集合

(状态,纸带符号;所取动作;所取新状态).

为了跟踪一个计算的过程，在每一步都必须注意内状态和正被读着的纸带符号，在四元组集中搜寻一个以这个对开始的四元组，遵循这个四元组给定的动作，并取得它给定的新状态，这样，对我们的四元组集必须加上一个限制：它必须是无矛盾的，即对每个对(状态,符号)，必须至多只有一个四元组以它开始，以便图灵机有一个合适定义的程序可遵循.

由于状态数和符号数都是有限的，因此对一个特殊机器来说，它的四元组的数目是有限制的. 不过我们并不要求，每个(状态,符号)对都要出现在某个四元组的开头. 某些组合可以从不出现于计算之中. 更重要的，我们将说一个图灵机的计算终止，当且仅当现时的(状态,符号)对在任何四元组中都不出现，从而机器没有再进行怎样操作的指令.

这样一个图灵机可以把一个输入纸带转换为一输出纸带. 用纸带上的符号表示信息的方法必然依赖于信息的性质，通过几个例子我们将看到这究竟是怎么做的. 在我们的所有例子中，将用符号 q_0, q_1, q_2, …去表示内状态，我们将约定. 机器以状态 q_0 开始，读着纸带上最左边的非空白方格.（某个诸如此类的约定显然是必须的——至于取这一个并没有什么特殊的意义.）

例 7.12

$$\{(q_0 1 B q_1),\ (q_1 B R q_0)\}$$

是具有状态 q_0 和 q_1，和符号 B 和 1 的字母库的图灵机的四元组集. 这四元组本身表明问题所"实际采用"的符号. 在四元组中第三个符号可以是 L(表示"向左移")，R(表示"向右移")，或者恰好是用以替换正被读着的符号的符号. 观察当输入纸带含有 1 的有限序列时机器的操作，例如

…	B	B	1	1	1	1	1	B	B	…

↑ q_0

机器以状态 q_0 开始读着最左边的 1. 它打印上一个 B(擦去 1), 而进入状态 q_1.

…	B	B	B	1	1	1	1	B	B	…

↑ q_1

机器处于状态 q_1 读着一个 B, 向右移动一方格, 然后进入状态 q_0

…	B	B	B	1	1	1	1	B	B	…

↓ q_0

现在, 正和上面一样; 在被读着的方格中的 1 已被 B 替换, 机器进入了状态 q_1. 这样, 机器将继续运转, 向右移动, 用 B 去替换 1, 直至达到状态

…	B	B	B	B	B	B	B	B	B	…

↑ q_0

现在, 再没有四元组在这局面去指导机器操作了, 于是计算停止. 这个机器擦去了 1 的一个序列, 然后停机.

例 7.13

$$\{(q_0 1 R q_1),\ (q_1 1 R q_0),\ (q_1 B R q_2),\ (q_2 B 1 q_2)\}$$

是一图灵机的四元组集, 它用下列方式判定一个数的奇偶性. 一个数可以用纸带上 1 的序列的形式给出. 机器以状态 q_0 开始, 读着最左边的 1. 如

B	B	1	1	1	1	1	1	B	B

↑ q_0

进行如下

B	B	1	1	1	1	1	1	B	B

↑ q_1

B	B	1	1	1	1	1	1	B	B

↑ q_0

B	B	1	1	1	1	1	1	B	B

↑ q_1

B	B	1	1	1	1	1	1	B	B

↑ q_1

B	B	1	1	1	1	1	1	B	B

↑ q_1

B	B	1	1	1	1	1	1	B	B

↑ q_0

由于没有以 q_0B 开始的四元组，就在那里停机．对任何偶数输入，动作都将类似．如果输入数是奇的，我们将达到这样的局面（输入5）

	B	B	1	1	1	1	1	B	B

↑
q_1

这时计算将继续这样进行：

B	B	1	1	1	1	1	B	B

↑
q_2

B	B	1	1	1	1	1	B	1

↑
q_2

在这里停机，因此这个机器将在一个方格后打上一个1，当且仅当输入数是奇数.

例 7.14

$$\{(q_0 1 X q_0),\ (q_0 X R q_0),\ (q_0 0 Y q_0),\ (q_0 X R q_0)\}$$

是图灵机的四元组集，它在输入数为0和1时，将把它们转换成X和Y的序列. 例如101001就转换成$XYXYYX$. 问题：这个机器在转换完成时停机吗？

例 7.15

对图灵机来说，加法几乎是平凡的. 如果m和n在纸带上作为由字母A分离的1的序列而输入，具有四元组集

$$\{(q_0 1 B q_0),\ (q_0 B R q_1),\ (q_1 1 R q_1),\ (q_1 A 1 q_2)\}$$

的机器将擦去最左边的1，并且用1去替换A，然后停机. 当停机时，数$m+n$以$(m+n)$个1的序列的形式留在纸带上.

例 7.16

一个图灵机可以重新产生输入纸带上的内容. 例如，如果输入纸带上除有限个0和1的序列外都是空白，这样的机器由下面的四元组集给出：

$q_0 0 X q_1$
$q_1 X R q_1$
$q_1 0 R q_1$
$q_1 1 R q_1$
$q_1 B R q_3$
$q_3 0 R q_3$
$q_3 1 R q_3$
$q_3 B 0 q_5$

$q_0 1 Y q_2$
$q_2 Y R q_2$
$q_2 0 R q_2$
$q_2 1 R q_2$
$q_2 B R q_4$
$q_4 0 R q_4$
$q_4 1 R q_4$
$q_4 B 1 q_5$

$q_5 0 L q_5$
$q_5 1 L q_5$
$q_5 B L q_5$

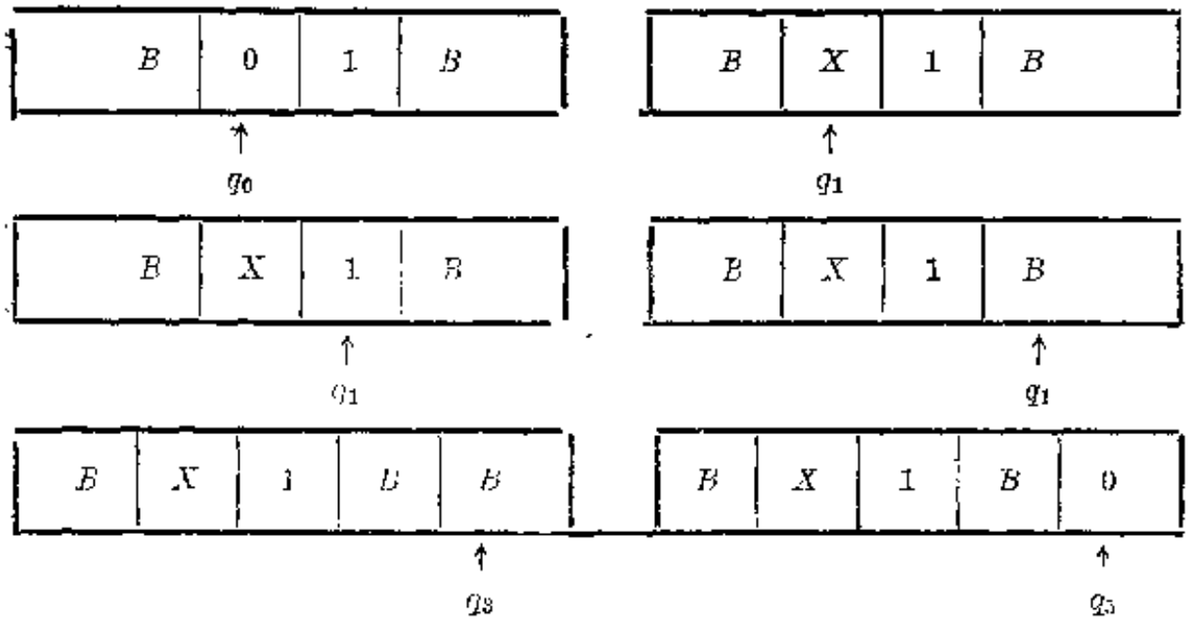
$q_5 X R q_0$

$q_5 Y R q_0$

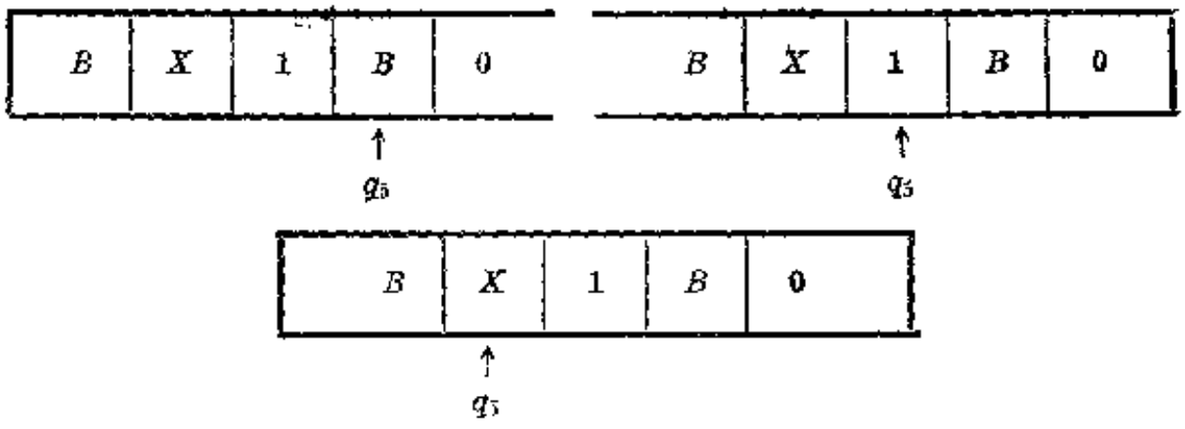
$q_0 B L q_6$
$q_6 X 0 q_6$
$q_6 Y 1 q_6$
$q_6 0 L q_6$
$q_6 1 L q_6$

这个例子显然比前面的要复杂些，四元组集按这种方式给出，是为了使机器的程序更为清楚．让我们把一个简单的例子做到底．

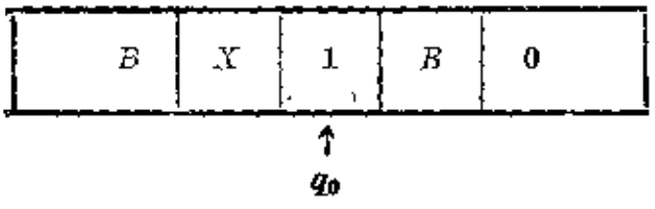
假设输入纸带除 $\boxed{0\,1}$ 之外全是空白，且机器以 q_0 状态开始，读者最左边的非空白方格．然后机器将用左边一列的四元组而纸带上将相继出现：



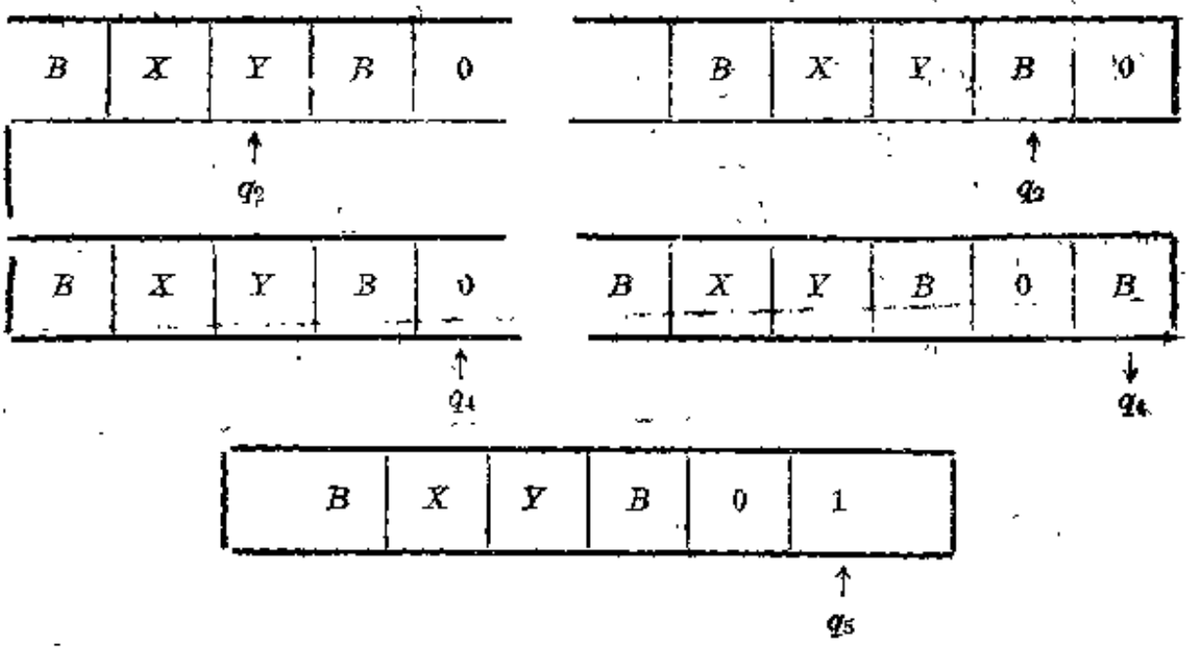
然后用中间一列的四元组，给出



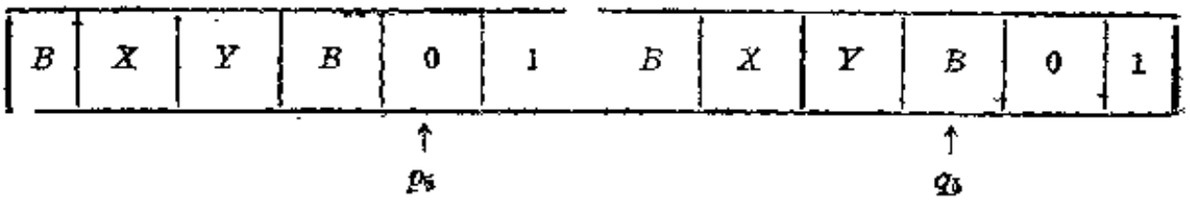
单个四元组 q_5XRq_0 给出



我们用四元组右边一列顶端的四元组



如前，状态 q_5 导致



B	X	Y	B	0	1

$\uparrow$ q_6

B	X	Y	B	0	1

$\uparrow$ q_0

现在，读着 B 的状态 q_0 使用中间一列底部的四元组，就给出

B	X	Y	B	0	1

$\uparrow$ q_6

B	X	1	B	0	1

$\uparrow$ q_6

B	X	1	B	0	1

$\uparrow$ q_6

B	0	1	B	0	1

$\uparrow$ q_6

B	0	1	B	0	1

$\uparrow$ q_6

至此机器停止运转，因为不存在以 q_6B 为开始的四元组。

▷最后一个例子阐明了一台图灵机在实施比较复杂程序时可能使用的检索，重抄，记忆，背诵的初等过程．它也阐明了怎样通过把要求实施的程序分析成一系列这样的初等过程，为一个特殊的图灵机寻求指令(即四元组)．注意纸带符号的字母库的大小对所要求的四元组数目有直接的影响．特别是，一台能复制一串 1 的机器要求与上例同样类型的程序，但将要求少得多的四元组．

例 7.17

在这个例子中，我们将并不作上面那样的详细说明，但是要求读者至少要完成一个实际的机器计算，为了考察所涉及的初等过程的组合，特别是上例中使用过重抄程序．下面的四元组给出了一台乘法图灵机，它把通过被空白方格分离的 m 和 n 个 1 的序列的形式输入的两个数 m 和 n 相乘．

$q_0 1 X q_1$	$q_5 B L q_5$
$q_1 X R q_1$	$q_5 Y 1 q_6$
$q_1 1 R q_1$	$q_6 1 R q_2$
$q_1 B R q_2$	$q_2 B L q_7$
$q_2 1 Y q_3$	$q_7 1 L q_7$
$q_3 Y R q_3$	$q_7 B L q_7$
$q_3 1 R q_3$	$q_7 X B q_8$
$q_3 B R q_4$	$q_8 B R q_0$
$q_4 B 1 q_5$	$q_0 B R q_9$
$q_4 1 R q_4$	$q_9 1 B q_{10}$
$q_5 q L q_5$	$q_{10} B R q_9$

这个机器，如果纸带上的输入为：

…	B	1	1	B	1	1	1	B	…

并以状态 q_0 开始，读着最左边的 1 的话，那么最终将在状态 q_5，以纸带上的如下输出停机

	B	1	1	1	1	1	1	B	…

$\uparrow$
q_9

这个机器，尽管是为比前例更为复杂的程序设计的，却有较少的四元组．这是因为纸带符号的字母库在此较为局限．

注记 7.18

在一个图灵机计算的任何阶段，纸带上只有有限部分不是空白的．因而我们可以用"瞬时描述"去表示该机器的状态，例如

$$11B1Bq_5B1BBB1.$$

这包括了纸带上的全部非空白的片断和机器正读着的方格．状态符号被包括在序列中，并且直接放在被读着的符号左边．重要的是要注意，一个瞬时描述并不必定仅仅包含纸带的非空白部分．例如

$$q_5BBBB11B1 \quad 和 \quad 1B11BBBq_3B$$

就是适合的瞬时描述，其中机器正在读纸带上空白部分的一个方格，但是我们决不把比正被读着的方格所必要的更多的空白包括进去.

注记 7.19

一图灵机由它的四元组系列而被确定. 通过与第六章中哥德尔相似的编码系统，有可能首先对四元组本身指派编码数，然后对四元组有限系列指派编码数. 这是因为(我们可以假设)所有可能的状态符号和纸带符号构成了一个可数集，每个图灵机只用其中有限多个. 因此，对任何图灵机我们能够指派一个编码数，并且如果描述的方法(关于初始状态以及输入和输出是如何编码的)是标准化了的话，编码数将是这样的，即所有关于相应的图灵机的重要信息都将是能行地可以返求的. 恰如前面我们这样选择编码数使得不同的编码数对应于不同的机器. 而且也有可能能行地判定，一个给定的自然数是否为一图灵机的编码数. 我们将不证明这一点，因为它依赖于所选择的编码数系统的细节，但是要给出它所产生的一个重要结果.

命题 7.20

图灵机的(编码数的)集合是能行可枚举的.

证明. 列出所有自然数，删去一切并非图灵机的编码数.

▷这个能行可枚举性使我们能够把图灵机系列和所有自然数的集合能行地联系起来. 每个图灵机将对应于由它在系列中的位置而给定的数. 因此我们能取图灵机的编码数集为全体自然数的集. 我们有下面的命题.

命题 7.21(枚举定理)

所有图灵机的集合可以按这样的方式排列为 $T_0, T_1, T_2, \cdots$ 使得每一个下标都能行地和完全地决定了它对应的机器的指令.

▷我们举出的图灵机的例子已经表明，它们能够实施各类计算. 我们感兴趣的是其中一类特殊的计算，即函数值的计算. 现在，

任何图灵机都可看成是计算一个函数的值的，假如我们规定了把输入和输出纸带的内容解释成为代表函数定义域和值域中的元素的方式. 我们的函数将是数论函数，即它的定义域和值域均由自然数组成，D_N 的一个元素 n 可以作为空白纸带上打印的 n 个 1 的序列输入任意的图灵机. 如果后来机器停止了，那时纸带上非空白方格的个数可以取作输出数. 关于这些约定没有什么特殊之处. 也没有什么理由说明，我们必须选择这些而不是那些，但是重要的是在这一点上要有所规定，因为我们要求每一图灵机和一个唯一的(偏)函数联系起来. 注意这些约定产生的是单元函数. 如果我们考察图灵机这样的计算，他们的输入纸带上有一对数(如例 7.15 中所描述的)那么机器将和二元函数相联系. 显然，我们能够类似地处理变元数更大的情况.

注记 7.22

(a) 人们已知道，对任何由图灵机可计算的数论函数 f，总存在一台能计算 f 的值的图灵机，这个机器的纸带字母库符号是 $\{B, 1\}$. 我们并不加以证明，但是要指出它是下述事实的一个推论，任何图灵机的字母库是有限的，它的符号可以用二进制来编码，其中在 0 处用符号 B 表示.

(b) 人们也已知道，对任何图灵机可计算的数论函数 f，总存在一台能计算 f 的值的并且只有两个内状态的图灵机. 对此我们也不作证明，但是我们应注意到，这种对内状态在数量上的约化，只有通过相当程度地扩大纸带符号的字母库才是可能的，或者是状态数可以约化为两个，或者是符号数可以约化为两个，但是一般地说，两者不能同时做到. (参见 Minsky, Ch. 6)

定义 7.23

一个数论(偏)函数是图灵可计算的，如果存在一台图灵机，在上面所说的关于输入和输出的约定之下能计算出函数的值.

关于单个函数按这种方式与多个图灵机对应的可能性，我们

义和递归函数定义的一切细节.要把它在这里讲述未免太冗长了。但是有兴趣的读者可以去参考 Minsky 的书本.

根据这点,当然可知,图灵论题与丘奇论题是等价的.

命题 7.26

存在单变元递归偏函数的一个能行的枚举ϕ_0, ϕ_1, ϕ_2, …, 其中每个递归偏函数出现无穷多次.

证明 这是命题 7.21, 7.24 和 7.25 的直接推论.

对于图灵机及其功能的具体描述就讲到这里. 现在让我们把话题深入一步,看在有关判定问题和不可解性方面能得些什么结果.

考察下面的算法:给出任何数对 m, $n\in D_N$, 枚举出图灵机系列T_0, T_1, T_2, …直至找列 T_m, 贯彻施于 T_m, 的输入为 n 的计算. 这是计算一个二元(偏)函数的值的一个算法. 因此, 根据图灵论题,存在着计算这个函数的值的图灵机. 这可写成下列命题

命题 7.27

存在一通用图灵机. 也就是说,存在一个图灵机 T, 当被解释为计算一个二变元m和n 的函数的值时,就实施了机器 T_m 的输入为 n 的计算.

▷因此,通用机器可以实施机器 T_0, T_1, …中的任何一个在实施单变元函数计算时的程序. 这是图灵机既是有力的又是有限的一个暗示. 通用机显然是一个复杂而有力的事物, 因为它体现了每个单变元机器的能力. 另一方面 T_0, T_1, …的复杂性要受到通用机的复杂性的限制.

考察下列算法:给出任意 $n\in D_N$, 找出递归偏函数系列中的 ϕ_n, 计算(用 T_n)$\phi_n(n)$. 如果有结果的话,那么当结果得出时对结果加上 1. 根据丘奇论题,这个算法定义一个递归偏函数, 比如说 ϕ_{k_0}. 现在让我们问 $\phi_{k_0}(k_0)$的计算结果是什么?按照这个算法, 我们得到矛盾

$$\phi_{k_0}(k_0)=\phi_{k_0}(k_0)+1.$$

可是，我们在得到这个结论时忽略了这一点，那就是 $\phi_{k_0}(k_0)$ 的计算可能不会终止．事实上我们可以从上面推知它不终止，因为在相反的情况下，无法避免矛盾．

上例说明，我们在描述算法时能怎样利用 T_0, T_1, …和 ϕ_0, ϕ_1, …的枚举．这是一个能引出有趣问题的程序．它也可以按下面的方式使用．

命题 7.28

不存在所有单变元递归(全)函数的能行枚举 f_0, f_1, …

证明 假设结论相反，即令 f_0, f_1, f_2, …是所有单变元(可能重复)递归(全)函数的一个能行枚举．考察下列算法：给定 $n\in D_N$，枚举 f_0, f_1, …直至找到 f_n．计算 $f_n(n)$，再加 1．根据丘奇论题，这个函数 h,

$$h(n)=f_n(n)+1 \quad 对每个\ n\in D_N,$$

是递归的，并且是全的，因为每个 f_n 是全的．所以必有 $h=f_k$ 对某个 k．因此

$$h(k)=f_k(k)=f_k(k)+1.$$

这次，避免不了矛盾，我们的结果获证．

▷如果对一已知的图灵机器的计算，我们能事先断定它是否将终止，那将是很方便的．因此，对给出的任何数对 m, $n\in D_N$，判定图灵机 T_m 是否将终止的问题，是一个已经考察过的问题。它称为图灵机的停机问题．它的重要性在很大程度上是基于下面的结果．

命题 7.29

图灵机的停机问题是不可解的，也就是说，不存在为下述集合中的问题提供解答的算法，

$$\{输入为\ n\ 的机器\ T_m\ 能停机吗?\mid m,\ n\in D_N\}.$$

证明 根据图灵论题，只需证明以下就够了：由下式给出的函

数 $f: D_N \to D_N$

$$f(n)=\begin{cases}0 & \text{如果 } T_n \text{ 在输入 } n \text{ 下停机}\\ 1 & \text{如果 } T_n \text{ 在输入 } n \text{ 下不停机}\end{cases}$$

不是图灵可计算的. 因为假如存在一个能解答上面给出的集合中的问题的算法,那么也就存在能解答下列集合中的问题

$$\{\text{输入 } n \text{ 的机器 } T_m \text{ 能停止吗?} \mid m, n \in D_N\}.$$

的算法, 从而存在一个能计算上述函数 f 的值的算法. 如果 f 不是图灵可计算的话,这是不可能的.

因此,让我们集中注意 f,并且假设它是图灵可计算的,而图灵机 T 能计算出它的值, 于是, 对输入 n, T 将停机, 而输出是 0 还是 1 依赖于 T_n 是否随着输入 n 而停机. 现在让我们修改 T,以得到 T',使得对于任何 n,

$$*\begin{cases}\text{如果 } T_n \text{ 随着输入 } n \text{ 停机}, T' \text{ 不随着输入 } n \text{ 停机}, \text{且}\\ \text{如果 } T_n \text{ 不随着输入 } n \text{ 停机}, T' \text{ 随着输入 } n \text{ 停机}.\end{cases}$$

T' 由 T 通过增添新的状态和四元组而得, 它们具有在 T 的任何能停机的计算上,附加一个在输出纸带上,搜寻一个非空白方格的效果. 如果搜寻成功了, T' 便停机,反之 T' 将继续不止地搜寻下去. 搜寻可以成功(当 T' 以输入 n 出发时), 当且仅当, 在最后阶段纸带上存在一个 1, 即当且仅当 T_n 随输入 n 不停机. (详细地说,我们可以增添两个新状态,比如说 q_α 和 q_β, 和以下的四元组: $q_\beta SRq_\alpha$,对于每一对 $q_\alpha S$, 只要它不出现在 T 的任何四元组的前头(S 是一纸带符号),以及 $q_\alpha BAq_\beta$, $q_\alpha ARq_\alpha$, $q_\beta ALq_\beta$, $q_\beta BAq_\alpha$.)

机器 T' 一定出现在系列 T_0, T_1, T_2, …中, 比如说 T' 是 T_{n_0}. 现在让我们提一个关键的问题. T_{n_0} 随输入 n_0 停机吗?回到上面的*. 它说的是, T_{n_0} 随输入 n_0 停机,当且仅当 T_{n_0} 随输入 n_0 不停机. 这个明显的矛盾,足以告诉我们 f 不可能是图灵可计算的,命题的结果得到了证明.

▷现在考察下面的算法: 给定任何 $n \in D_N$,在系列 $T_0, T_1, T_2,$

命题 7.31

对于任何图灵机 T，T 的域，即能使 T 以 n 输入停机的一切 $n\in D_N$ 组成的集，是一个递归可枚举集(当然，也可能是递归的)。

证明 证明与上述十分类似，随着对同一机器 T，这在不同的输入下进行计算，同时作出所有使 T 停机的输入数的表。

▷K 是图灵机和枚举定理考察中提出的非递归集的一个具体的例子，还有许多其它的例子。例如：

例 7.32

(a) $\{n\in D_N: T_n$ 对每个输入数都停机$\}$既不是递归的，也不是递归可枚举的。

(b) $\{n\in D_N: T_n$ 对所有输入数都不停机$\}$既不是递归的，也不是递归可枚举的。

(c) 对每个固定数 n_0，集$\{n\in D_N: T_n$ 以 n_0 输入停机$\}$不是递归的，但是递归可枚举的。

这些例子，根据定义 7.11 也给出了递归不可解的问题类。

(d) $\{n\in K$ 吗？$|n\in D_N\}$

(e) $\{T_n$ 对每个输入数停机吗？$|n\in D_N\}$

(f) $\{T_n$ 对某些输入数停机吗？$|n\in D_N\}$

(g) $\{T_n$ 对 n_0 输入停机吗？$|n\in D_N\}$，其中 n_0 是任何固定数。

这些问题类都是递归不可解的。

通常用来证明所有这些结果的方法都是相似的。假设集合是递归的(或者问题类是递归可解的)，然后推导出集合 K 是递归的(或推导出某些其它的非递归集是递归的)。这个方法可以从两方面去评论它。首先，它可以看作是通过矛盾的直接证明。其次，在更为广泛的含义下，它可以看成是引进一个新概念，可化归性。

…中搜寻直至达到 T_n，然后以 n 输入并遵循机器 T_n 的计算．如果计算停止的话，当停止时，给出输出 1．根据图灵论题，其值可由这个算法计算的函数是图灵可计算的．这个函数，比如说 ϕ，是由下式

$$\phi(n)=\begin{cases}1 & \text{如果 } T_n \text{ 以 } n \text{ 输入，}\\ \text{不确定，} & \text{相反情况．}\end{cases}$$

给出的．显然 ϕ 是一个偏函数，因为确实有这样的图灵机，对所有输入都不停机也存在另外一些仅对某些输入能停机．ϕ 的域，在我们的研究范围内是一重要的集合，通常用 K 表示．

$$K=\{n\in D_N: T_n \text{ 以 } n \text{ 输入停机}\}.$$

现在，命题 7.29 证明的一个推论是：K 不是一个递归集（当然，要在丘奇论题的假设之下），因为如果它是一个递归集，那么将存在一个算法，能回答 $n\in D_N$ 时 "$n\in K$" 吗？这种形式的问题，即如下集合中的问题

$$\{\text{机器 } T_n \text{ 以 } n \text{ 输入能停机吗？} \mid n\in D_N\}.$$

命题 7.30

K 是一递归可枚举的而非递归的集．

证明　K 由上知不是递归集．K 是能行可枚举的，可以通过给出一个枚举它的算法而加以证明．

步骤 1．实施以 0 输入 T_0 的计算的第一步

步骤 2．实施以 1 输入 T_1 的计算的第一步，和以 0 输入 T_0 的计算的第二步．

步骤 3．实施以 2 输入 T_2 的计算的第一步，和以 1 输入 T_1 的计算的第二步，和以 0 输入 T_0 的计算的第三步．

以此类推．不管那一个机器 T_i 停机，就把 i 置入 K 的枚举中，在此后的算法的步骤中就不必再顾及 T_i．对于每一个 $n\in K$，总会看到以 n 为输入使 T_n 停机的一步，而 n 就被置入 K 的枚举．因此 K 是能行可枚举的，并且根据丘奇论题，它是递归可枚举的．

令．设计一个能行的程序，能对预先给出的任何输入，判定 T 是否最终能停机。

13．一台图灵机，它的指令仅允许它沿着纸带的一个方向移动的，称为有限状态机，证明有限状态机的停机问题是可解的．

14．证明 $\overline{K}$ 不是递归可枚举的．

15．令 A 是 $\overline{K}$ 的一个递归可枚举子集，并且假设对某一图灵机 T_n，$A=\{x: T_n$ 以 x 输入停机．$\}$证明 $n\in\overline{K}/A$．

16．证明每个递归可枚举集是某个图灵机的域．

17．证明在例 7.32 中的每个问题类都是递归不可解的．

18．令 K_0 是集合$\{(m, n): 图灵机T_m 以输入 n 停机\}$．证明：$K$ 可约化为 K_0，K_0 可约化为 K．

7.3 字问题

代数和逻辑紧密相联的一个领域是诸如群，半群和阿贝尔群这样的代数结构的字问题的研究，半群的情形最容易描述，所以我们将用它作为范例．

令 $A=\{a_1, \cdots, a_k\}$ 是一形式符号的集合．这个集合可以看成为字母库，所谓这字母库中的字就是指取自字母库中的符号的一个有限串(对组成字的串没有什么限制)．用 S_A 表示字母库 A 中所有字组成的集合．因此 S_A 可以看作是毗连运算下的一个半群．对 S_A 中任意两个字，通过把第二个排在第一个后面恰能构成一个复合字．这种运算自然是结合的，所以 S_A 是一个半群．如果我们约定空字(没有符号构成的字)是 S_A 的一个元素，那么这个字的功能相当于半群中的恒等元．

现在，当如上述 S_A 那样的半群，被要求满足一个或几个关系时，一个字问题就被提出了．我们将通过例子来说明这些．

例 7.34

考察如上的 S_A，让我们规定字 a_1a_2 和 a_2a_1 相互是等同的．由

此，我们可以定义 S_A 上的一个等价关系如下．如果 P 和 Q 是字，那么 $Pa_1a_2Q\sim Pa_2a_1Q$ 并且 $Pa_2a_1Q\sim Pa_1a_2Q$，同时对任意的字 U 和 V，如果存在字 $W_1,\cdots,W_n$ 的一个序列，使得 $U=W_1$，$W_1\sim W_2$，$\cdots$，$W_{n-1}\sim W_n=V$ 时称为 U 等价于 V．容易证明这是一个等价关系类，而且半群运算在等价类上是合式定义的．（读者应该注意，$\sim$在这里不是等价关系，它不是传递的．）等价类的集合 S_A^* 构成一个半群，它是生成元 $a_1,\cdots a_k$ 和关系 $a_1a_2=a_2a_1$ 的半群．S_A^* 的字问题是，对任何给出的字 U 和 V，去判定它们是否等价，也就是说，它们是否代表 S_A^* 中的同一个元素．

更一般地，我们可以考察由 S_A 通过包括如下形式的一系列关系而得的半群，这些关系是 $P_1=Q_1$，$P_2=Q_2$，$\cdots$，$P_m=Q_m$，其中 $P_1,\cdots,P_m,Q_1,\cdots,Q_m$ 是在字母库 A 中的给定的字．这里我们把$\sim$定义为

$$PP_iQ\sim PQ_iQ$$

对任何 P，Q 和 $1\leqslant i\leqslant m$，我们恰如前面一样的定义等价关系．等价类的集合称为有生成元 $a_1,\cdots,a_k$ 和关系 $P_i=Q_i(1\leqslant i\leqslant m)$ 的半群．这个半群的字问题是和上面说过的类似的问题，显然它将比已有的更为复杂．

定义 7.35

一个半群称为有限提供的，如果它能象上面那样由一个有限的生成元集和一个有限的关系集得到．

有限提供的半群的字问题称为递归可解的，如果存在一个算法，对任何字对，将能判定它们是否等价．

'半群的字问题'是：是否存在一种算法，对任意给出的有限提供的半群和任意在那个半群中的一对字，该算法能判定它们是否等价？

例 7.36

令 $A=\{a_1,\ a_2\}$，考察由 A 在关系 $a_1a_2=a_2a_1$ 下生成的半群

S. 我们能看到，这个半群有递归可解的字问题. 通过描述算法如下.

每个恰含 a_1 和 a_2 的字总能够予以若干次重排，每次都利用关系 $a_1a_2=a_2a_1$，直至得到每一个 a_1 都先于每一个 a_2 这样的字. 这个字等价于最初的字. (例如，$a_2a_1a_2a_1\sim a_2a_1a_1a_2\sim a_1a_2a_1a_2\sim a_1a_1a_2a_2$.)就这个字问题来说，给定任意两字 P 和 Q，只须对每一字作出这个程序. P 和 Q 是等价的，当且仅当结果所得的字是恒等的.

▷如我们前面所见到的，如果对一特殊的问题类存在一个算法，常常没有专门的方法和假设可能找到它和描述它. 另一方面，为了要证明不存在算法，实际上对我们来说仅有的方法是通过丘奇论题. 事实上存在一个有限提供的半群，它的字问题不是递归可解的. 关于这个证明完全依赖于我们已经展开过的关于图灵机的思想和方法，为此，首先让我们来弄明白，怎样才能把图灵机和有限提供的半群两个概念联系起来.

我们已经看到一台图灵机和它在给定时刻的纸带的状态，怎样用"瞬时描述"来刻划，这个瞬时描述由一串符号组成，如

$$1B11Bq_i1B1,\ 1111B1Bq_iB.$$

我们将要做的是把这些看成字，并且把两个字看成是等价的，如果一个字通过图灵机的一系列运算能转换为另一个字. 如我们将要见到的，存在着一定的复杂性，但是我们可以把字母库 A 取成包括图灵机的所有纸带符号和状态符号，我们可以把半群关系取成由图灵机的四元组给出. 例如，如果 q_11Bq_2 是四元组之一，那么我们将说

$$Pq_11Q\sim Pq_2BQ$$

其中 P 和 Q 是取自 A 的任意符号串. 当然，只有某些取自 A 的符号串，真正具有这个图灵机的一个瞬时描述的形式——例如某些串包含的状态符号将多于 1，我们将发现这是没有关系的. 现在

让我们来说明.

令 T 是一图灵机，它停机当且仅当输入 α 属于集合 K（K 是递归可枚举的但不是递归的）. 我们将假设 T 仅有纸带符号 1 和 B，数 α 是以 α 个 1 的序列输入的. 令 T 的内状态由 q_0，…，q_n 表示，并且令 I 是 T 的四元组的集合. 取

$$A=\{q_0, q_1, \cdots, q_n, q, q', 1, B, h\},$$

考察在这个字母库中的集合 S_A（关于包括符号 q，q' 和 h 的理由将在下面说明.）用 $\mathscr{S}$ 表示带有字母库 A 和下面关系的有限提供的半群.（字母 X 和 Y 在全文中，常被用于表示任意一个纸带符号 1 或 B.）

1. $q_iX=q_jY$　如果 $q_iXYq_j\in I$.

2. $\left.\begin{array}{l} q_iXY=Xq_jY \\ q_iXh=Xq_jBh \end{array}\right\}$ 如果 $q_iXRq_j\in I$.

3. $\left.\begin{array}{l} Xq_iY=q_jXY \\ hq_iY=hq_jBY \end{array}\right\}$ 如果 $q_iYLq_j\in I$.

4. $q_iX=qX$　如果在 I 中不存在四元组，它以 q_iX 开始.

5. $qX=q$.

6. $Xq'=q'$.

7. $qh=q'h$.

我们已经不仅包含了与图灵机的指令相对应的关系，而且也包含了支配 q，q' 和 h 的行为的关系. 机器的瞬时描述应和 S_A 中以 h 为界的字相对应. 这样机器的初始条件可能是 $q_0$1111. 我们将把它看成是由字 $hq_0$1111h 所代表的. h 勾划出了纸带上的有意义部分. 机器有阶段地转换它的输入纸带，而在对应的阶段中我们的字，通过关系的应用转换成等价字. 在系关 2 和 3 中有的含 h，使得我们能在需要时通过在一个字的一端插入一个 B 以扩充我们的字（即当机器读着纸带上非空白部分之外的一个方格时）. 注意，当机器停机时会发生什么. 这时机器不再使用它的纸带，但

是我们能够继续用关系 4—7 去转换我们的字. 让我们来考察一个例子，以便弄清楚发生了什么？假设机器已经停机，那时我们的字是

$$h1BBq_i11h$$

那么在 I 没有四元组以 q_i1 开始，应用关系 4，

$$h1BBq11h$$

是一等价词. 关系 5 导致等价字

$$h1BBq1h,$$

和

$$h1BBqh$$

因此关系 7 产生

$$h1BBq'h,$$

并且关系 6 给出等价字

$$h1Bq'h,$$

$$h1q'h,$$

$$hq'h.$$

这个最后的字并不依赖纸带最后的内容. 事实上，我们能够说的是机器 T 以输入 α 停机，当且仅当字 $hq_0\alpha h$ 等价于 $hq'h$. 正是这点使我们能够证明，$\mathscr{S}$ 是一具有递归不可解字问题的半群

命题 7.37

存在一个有限提供的半群，它的字问题是递归不可解的.

证明 令 $\mathscr{S}$ 如上所描述. 假设存在一个算法，对任何 $\mathscr{S}$ 的字对，该算法能判定它们是否等价. 因此，有一个判定集合 E 的成员的算法

$$E=\{W\in S_A: W \text{ 等价于 } hq'h\}.$$

现在 T 以输入 α 停机，当且仅当 $\alpha\in K$. 因此判定 K 的成员，只需我们对给定的 α，去问一问字 $hq_0\alpha h$ 是否为 E 的一个成员. 这要用到 T 以输入 α 停机当且仅当 $hq_0\alpha h$ 等价于 $hq'h$ 这个结果（还没有完全证明）. 但是由于 K 不是递归的，所以不存在判定 K 的

成员的算法. 因此假设$\mathscr{S}$有递归可解的字问题会导致一个矛盾，命题在下面的引理之下得到了证明.

引理: T 以输入 α 停机，当且仅当字 $hq_0\alpha h$ 和 $hq'h$ 是等价的.

证明　假设 $hq_0\alpha h$ 和 $hq'h$ 等价，我们证明 T 以输入 α 停机（另一方向的蕴涵在前一命题讨论中已证明）. 字之间等价的一个证明将由使用关系 1 到 7，从 $hq_0\alpha h$ 出发以 $hq'h$ 结束的变换组成. 现在 q' 不能用不同于 7 的应用的方式引入. 由此可知 $hq_0\alpha h$ 必等价于出现符号 q 的一个字. q 只能用 4 引入. 那么，在从 $hq_0\alpha h$ 到 $hq'h$ 的等价字的序列中，考虑关系 4 的首次应用. 直到那时每一个变换必须和一图灵机的步骤对应(1, 2 或 3 的应用). 所以我们有

$$hq_0\alpha h \text{ 等价于 } hPq_iXQh,$$

其中 Pq_iXQ 是图灵机从初始状态 $q_0\alpha$ 达到的状态的瞬时描述，因为这里用到了4，q_iX 不可能出现在T 的任何四元组中，所以 T 在达到 Pq_iXQ 的停机. 这样 T 就以 α 输入停机.

命题　7.38

半群的字问题是递归不可解的.

证明　如果存在一个算法，它能对任何有限提供的半群 S 和 S 的任何字 W_1 和 W_2，判定它们是否等价，这个算法就能用于半群 $\mathscr{S}$，这和上述命题矛盾.

▷这样我们就有了所期望的关于半群的结果.

定义　7.39

一个有限提供的群可类似于一个有限提供的半群的那样加以定义，除形式的逆元可以出现在字中之外（即，字可以用符号 a_1, a_2, …, a_k, a_1^{-1}, …, a_k^{-1} 构造），在关系中必须有 $a_ia_i^{-1}=e$ 和 $a_i^{-1}a_i=e$，对 $1\leqslant i\leqslant k$，其中 e 表示空字.

由于这个显然更为复杂的情况，字问题也显得更为困难，答案只是在相当近的时期才找到.

命题 7.40

(i) 存在一有限提供的群，它的字问题是递归不可解的.

(ii) 对于群的字问题是递归不可解的.

(iii) 对阿贝尔群的字问题是递归可解的.（因为一个有限提供的阿贝尔群，关系集合中一定包括 $a_ia_j=a_ja_i$，对字母库中符号 a_i，a_j 的每个对.）

练习

19. 在下列各种情况下，描述一个算法，能解答带有给定的生成元和关系的有限提供的半群的字问题.

(a) $\{a_1, a_2\}$，$a_1a_1=a_1$.

(b) $\{a_1, a_2, a_3\}$，$a_2a_2=a_2$，$a_1a_2=a_3$.

(c) $\{a_1, a_2, a_3, a_4\}$，$a_1a_1=e$；$a_2a_2=e$，$a_3a_3=e$，$a_4a_4=e$.

20. 令 G 是带有生成元 $\{a_1, a_2, a_3\}$ 和关系 $a_1a_2=a_2a_1$，$a_2a_3=a_3a_2$，$a_3a_1=a_1a_3$ 的有限提供的群. 证明对 G 的字问题是递归可解的.

21. 令 S 是一带有递归不可解字问题的半群，令 A 是 S 的生成元集. 证明 S' 有递归不可解字问题，其中 S' 是任意有限提供的半群，它的生成元集包含 A，它的关系集与 S 相同.

22. 从命题 7.37 的结果推导出：存在一个仅带有两个生成元的有限提供的半群，它具有递归不可解字问题.

7.4 形式系统的不可判定性

读者将能回忆起第二章的结果（命题 2.24），命题演算的形式系统 L 是可判定的. 当然，那时对我们来说，对它的意义的理解比现在要少，因为我们现在能证明：

命题 7.41

L 的定理的哥德尔数的集是一递归集.

证明 首先注意，对 L 来说，我们必须定义一新的哥德尔编码数，因为 L 和我们的一阶语言 $\mathscr{L}$ 并不具有相同的符号. 这是不困难的，因为 L 比较简单. 例如，$\vee$(和)可以如前指派数 3 和 5，$\sim$ 和 $\rightarrow$ 可以对应地指派 7 和 9，每个命题字母 p_k 可以指派数 $9+2k$，对每个 $k=1, 2, \cdots$，因此，公式和公式序列可以恰如以前那样，用素数幂指派.

为了证明命题，我们要求一种能解答下述问题的算法.

$$\{n \text{ 是 } L \text{ 中一定理的哥德尔数吗？} \mid n \in D_N\}.$$

给出 $n \in D_N$，求一个与 n 对应的 L 的公式（如果存在一个的话）. 如果不存在这样的公式，答案就是否定的. 如果有一个这样的公式，可以构造它的真值表，看一看它是否为重言式.

▷递归可判定性和递归不可判定性问题，确实是一个对任何形式系统都能提出的问题. 因为哥德尔编码数可应用于所有这些系统. 因此，该问题正好就是 D_N 的一个特殊子集是递归还是非递归性的问题.

谓词演算系统 $K_{\mathscr{L}}$ 是否递归不可判定，依赖于语言 $\mathscr{L}$. 取一极端的情形，令 $\mathscr{L}_1$ 是一不包含函数字母，个体常元且仅含一个谓词字母 A_1^1 的一阶语言.

命题 7.42

$K_{\mathscr{L}_1}$ 是递归可判定的.

证明 我们来描述一个算法，能解答以下集合中的问题

$$\{\mathscr{A} \text{ 是 } K_{\mathscr{L}_1} \text{ 的一条定理吗？} \mid \mathscr{A} \text{ 是 } K_{\mathscr{L}_1} \text{ 的一公式}\}.$$

为了做到这点，我们要用第四章的一个结果：一个公式 $\mathscr{A}$ 是 $K_{\mathscr{L}_1}$ 的一条定理，当且仅当 $\mathscr{A}$ 在 $\mathscr{L}_1$ 的每个解释中皆真.

令 I 是 $\mathscr{L}_1$ 的一个解释. 那么 $D_I = D_0 \cup D_1$，其中

$$D_0 = \{x \in D_I;\ \overline{A}_1^1(x) \text{ 成立}\},$$

且

$$D_1 = \{x \in D_I;\ \overline{A}_1^1 \text{ 不成立}\}.$$

（注意，D_0 或 D_1 可以是空集，但不能皆是空集.）

现在定义一个解释 I^* 如下. I^* 的域是$\{D_0, D_1\}$, 如果 D_0 和 D_1 皆非空; 或者是$\{D_0\}$, 如果 $D_1=\varnothing$; 或者是$\{D_1\}$, 如果 $D_0=\varnothing$. A_1^1 的解释比如说是 $\overline{A}_1^1$, 于此 $\overline{A}_1^1(D_0)$成立, 而 $\overline{A}_1^1(D_1)$不成立. 对 $\mathscr{L}_1$ 中的任何公式 $\mathscr{A}$, 如果 $\mathscr{A}$ 在 I^* 中真, 那么 $\mathscr{A}$ 在 I 中也真. 这可以通过对 $\mathscr{A}$ 中的联结词和量词的数目加以归纳证明, 但是要注意, 对 I^* 的域可能有的 $\{D_0\}$, $\{D_0, D_1\}$或$\{D_1\}$等不同情形, 需要作不同的证明.

从上述可以推得. 如果 $\mathscr{A}$ 在至多包含两个元的域的每种解释中皆真, 那么 $\mathscr{A}$ 在所有解释中皆真. 因此, 我们的算法必须是一个这样的方法, 它能检验公式在由一个或两个元组成的域的每种解释中是否为真. 每一个这样的解释一定属于下述范围之一.

1. 域 $\{d\}$, $\overline{A}_1^1(d)$成立.
2. 域 $\{d\}$, $\overline{A}_1^1(d)$成立.
3. 域 $\{d_1, d_2\}$, $\overline{A}_1^1(d_1)$成立, $\overline{A}_1^1(d_2)$不成立.
4. 域 $\{d_1, d_2\}$, $\overline{A}_1^1(d_1)$, $\overline{A}_1^1(d_2)$都成立.
5. 域 $\{d_1, d_2\}$, $\overline{A}_1^1(d_1)$, $\overline{A}_1^1(d_2)$都不成立.

对任意公式 $\mathscr{A}$, 利用第三章的方法, 容易检验 $\mathscr{A}$ 在各种范围中是否为真.

这个算法可以用来判定任何给定的公式是否为一定理, 所以 $K_{\mathscr{L}}$ 是递归可判定的.

上面的证明的思想可以推广, 从而给出更为一般的结果.

命题 7.43

令 $\mathscr{L}$ 是不带函数字母或个体常元而仅包含一元谓词字母(可能有无限多个)的一阶语言. 那么 $K_{\mathscr{L}}$ 是递归可判定的.

证明 参见 Mendelson.

▷(象上述 $K_{\mathscr{L}}$ 那样的系统, 通常称为纯一阶谓词演算系统, 表示没有函数字母和个体常元.)

和上面形成对照, 现在我们有下面的命题.

命题 7.44

系统 $\mathscr{N}$ 是递归不可判定的(在它是一致的假设条件下).

证明 令 T 是 D_N 上的一元关系,定义如下:$T(n)$成立,当且仅当 n 是 $\mathscr{N}$ 的一条定理的哥德尔数. 假设 T 是递归的(即 $\mathscr{N}$ 是递归可判定的). 那么由命题 6.12, T 在 $\mathscr{N}$ 中是可表达的,所以有一公式 $\mathscr{T}(x_1)$,其中 x_1 自由出现,使得

$$\text{如果 } T(n) \text{ 成立,那么} \vdash_{\mathscr{N}} \mathscr{T}(0^{(n)}),$$

且

$$\text{如果 } T(n) \text{ 不成立,那么} \vdash_{\mathscr{N}} \sim\mathscr{T}(0^{(n)}).$$

令 D 是 D_N 上的二元关系,定义如下:$D(m, n)$成立,当且仅当,者或 m 是公式 $\mathscr{A}(x_1)$的哥德尔数,其中 x_1 自由出现,且 n 是 $\mathscr{A}(0^{(m)})$的哥德尔数;或者 m 不是这样的一个公式的哥德尔数,并且 $n=0$. 那么 D 是一个递归函数从而在 $\mathscr{N}$ 中是可表示的(参见命题 6.29),比如说,由公式 $\mathscr{D}(x_1, x_2)$.

用 $\mathscr{A}(x_1)$表示公式

$$(\forall x_2)(\mathscr{D}(x_1, x_2) \to \sim\mathscr{T}(x_2)).$$

令 s 是这个公式的哥德尔数. 那么 $\mathscr{A}(0^{(s)})$是公式

$$(\forall x_2)(\mathscr{D}(0^{(s)}, x_2) \to \sim\mathscr{T}(x_2)).$$

令 t 是这个公式的哥德尔数,那么 $D(s, t)$ 成立,所以 $\vdash_{\mathscr{N}} \mathscr{D}(0^{(s)}, 0^{(t)})$. 现在如果 $\mathscr{A}(0^{(s)})$是 $\mathscr{N}$ 的一条定理,那么使用(K5),我们得到

$$\vdash_{\mathscr{N}} (\mathscr{D}(0^{(s)}, {}^{(t)}) \to \sim\mathscr{T}(0^{(t)})).$$

由 MP 可以推得

$$\vdash_{\mathscr{N}} \sim\mathscr{T}(0^{(t)})$$

再者,如果 $\mathscr{A}(0^{(s)})$不是 $\mathscr{N}$ 的一条定理,那么 t 就不是 $\mathscr{N}$ 的一条定理的哥德尔数,所以 $T(t)$不成立,所以 $\vdash_{\mathscr{N}} \sim\mathscr{T}(0^{(t)})$. 因此,

在任何情况下，我们有

$$\vdash_{\mathscr{N}} \sim \mathscr{T}(0^{(t)}).$$

现在

$$\vdash_{\mathscr{N}} \mathscr{D}(0^{(s)}, 0^{(t)}),$$

并且由于 D 是在 $\mathscr{N}$ 中可表示的，我们有

$$\vdash_{\mathscr{N}} (\exists_1 x_2)\mathscr{D}(0^{(s)}, x_2).$$

因此

$$\vdash_{\mathscr{N}} (\mathscr{D}(0^{(s)}, x_2) \to x_2 = 0^{(t)}). \qquad (*)$$

相等公理给出

$$\vdash_{\mathscr{N}} (x_2 = 0^{(t)} \to (\sim \mathscr{T}(0^{(t)}) \to \sim \mathscr{T}(x_2))),$$

并且由于 $\vdash_{\mathscr{N}} \sim \mathscr{T}(0^{(t)})$，我们有

$$\vdash_{\mathscr{N}} (x_2 = 0^{(t)} \to \sim \mathscr{T}(x_2)).$$

由(*)，利用 HS，我们得到

$$\vdash_{\mathscr{N}} \mathscr{D}(0^{(s)}, x_2) \to \sim \mathscr{T}(x_2)),$$

通过概括，

$$\vdash_{\mathscr{N}} (\forall x_2)(\mathscr{D}(0^{(s)}, x_2) \to \sim \mathscr{T}(x_2)),$$

即

$$\vdash_{\mathscr{N}} \mathscr{A}(0^{(s)}),$$

因此 s 是 $\mathscr{N}$ 的一条定理的哥德尔数，所以

$$\vdash_{\mathscr{N}} \mathscr{T}(0^{(t)}).$$

但是 $\vdash_{\mathscr{N}} \sim \mathscr{T}(0^{(t)})$，所以这和 $\mathscr{N}$ 的一致性矛盾，证明完成。

▷如果一个系统已知是递归可判定的(或不可判定的)，我们是否能推导出关于它的扩充的递归可判定性(或不可判定性)的任何东西吗？记得一阶系统的一个扩充有相同的语言，但是有更大的定理类。表面上看来，似乎不会有什么理由，去说明为什么判定一个

定理类的成员的算法的存在(或不存在)将隐含判定其它类的成员的算法的存在(或不存在). (一个递归集可能有一个非递归的子集,一个非递归集可能有一个递归的子集. 不过,我们在某些情况下,能作出一个联系.

命题 7.45

令 S 和 S^+ 是有同样语言的系统, 且令 S^+ 是 S 的一个有限扩充,即假设有一有限公式集 $\mathscr{A}_1, \cdots \mathscr{A}_n$, 使得将它们增添为 S 的公理后, 我们就得到 S^+ 的公理集. 如果 S^+ 递归不可判定, 那么 S 也递归不可判定.

证明 假设 S 和 S^+ 如上所描述, 且 S^+ 是递归不可判定的. 不失一般性,我们可以假设 $\mathscr{A}_1, \cdots \mathscr{A}_n$ 是闭公式. 在 S^+ 中的一个证明是 S 中从 $\{\mathscr{A}_1, \cdots, \mathscr{A}_n\}$ 出发的一个演绎,所以对任何公式 $\mathscr{A}$, 用演绎定理得

$$\vdash_{S^+} \mathscr{A}, \text{当且仅当} \vdash_S (\mathscr{A}_1 \to (\cdots \to (\mathscr{A}_n \to \mathscr{A}))\cdots).$$

如果存在判定任何公式是否为 S 的定理的一个算法, 那么只要问 $(\mathscr{A}_1 \to \cdots (\mathscr{A}_n \to \mathscr{A})\cdots)$ 是否为 S 的一条定理, 我们也能判定公式 $\mathscr{A}$ 是否为 S^+ 的一条定理. 但是 S^+ 是递归不可判定的, 所以 S 一定也是递归不可判定的.

▷于是总结起来,我们发现了系统 $\mathscr{N}$ 的两个不同的限制. 它不是完全的,并且它是递归不可判定的. 第一,是说 $\mathscr{N}$ 的定理集并不与真命题集一致,第二,是说不存在算法能去判定什么样的命题和 $\mathscr{N}$ 的定理相对应. 所以似乎可以这样说, $\mathscr{N}$ 在提供一种判定算术中的命题的真假性的方法上并不十分有帮助. 如本书所讨论的算术形式系统,是受到限制的,然而也没有另外可供选择的方法.

现在转入另一重大结果(参看命题 7.42).

命题 7.46

存在一个一阶语言 $\mathscr{L}$, 使得 $K_{\mathscr{L}}$ 是递归不可判定的.

证明. 证明所用的思想与命题7.37的证明是类似的. 令T是一台图灵机，它停机，当且仅当输入数属于集合K(是递归可枚举但不是递归的). 假设T只使用了纸带符号1和B，它的内状态$q_0, \cdots, q_n$. 现在令$\mathscr{L}$是一阶语言，它的符号库包括作为个体常元的所有在下列集中的符号

$$A=\{B, 1, h, q, q', q_0, \cdots, q_n\}.$$

也包括函数字母f_2^2和谓词字母A_2^2. 我们将把f_2^2看成能使我们构成字，即$f_2^2(x_1, x_2)$须看成是字x_1x_2. 因此$\mathscr{L}$的项将对应于任意长度的字(允许出现变元)，$\mathscr{L}$的仅仅包含A的符号和字母f_2^2的闭项集将对应于集合S_A. (由于几种不同可能的括法任意给定的字将对应于几个不同的项，但是我们将在下面予以考虑.)

谓词字母A_2^2可以看成是在S_A上的等价关系，它由在命题7.37的证明中描述过的，为了确定具有不可解字问题的半群而列出的关系所生成.

一定要描述f_2^2和A_2^2的特征，下列$K_{\mathscr{L}}$的公式可以做到这一点.

(U_1) $A_2^2(f_2^2(f_2^2(x_1, x_2), x_3), f_2^2(x_1, f_2^2(x_2, x_3)))$.

$(U2)$ $A_2^2(x_1, x_2) \to A_2^2(f_2^2(x_1, x_3), f_2^2(x_2, x_3))$.

$(U3)$ $A_2^2(x_1, x_2) \to A_2^2(f_2^2(x_3, x_1), f_2^2(x_3, x_2))$.

$(U4)$ 对每个$W=W'$，取自决定带有不可解字问题的半群的关系集的，我们得到$K_{\mathscr{L}}$的闭项t, t'和$\overline{W}$, $\overline{W'}$对应，并且把一切用这种方法得到的公式

$$A_2^2(t, t')$$

作为$(U4)$. 注意只有有限多个这样的公式.

$(U5)$ $A_2^2(x_1, x_2) \to (A_2^2(x_2, x_3) \to A_2^2(x_1, x_3))$.

如果我们来考察一阶系统$K_{\mathscr{L}}^*$，它由$K_{\mathscr{L}}$通过包括所有合式公式$(U1)$—$(U5)$作为新公理而得到，那么应该清楚，对$\mathscr{L}$的对应于S_A的字W_1, W_2的任何闭项t_1, t_2，我们有

(c) 一阶域论.

(d) 一阶半群论.

(e) ZF 系统.

(ii) 下列系统是递归可判定的.

(a) 一阶阿贝尔群论.

(b) 没有乘法的一阶算术(即，这系统与 $\mathscr{N}$ 是相同的，除了不包括符号 f_2^2，且取消($N5$)和($N6$)之外).

证明 我们不做证明，有兴趣读者可以去参看 Tarski Mostowski, Robinson 的著作.

一个形式系统的递归可判定性蕴涵着，对于系统中的任意公式，都存在着一计算程序，将能判定它是否为一定理(当然，要预先假设计算机是足够大的). 因此，例如，这是可能的，用一台机器和一程序，去判定关于阿贝尔群和他们的成员的命题是否为一定理. 这样的一个程序势将非常复杂，并且对于一个复杂的命题的判定需要相当大的计算时间和容量，所以这在实践意义下并不怎么有用，但是这种可能性还是令人感兴趣的. 同样感兴趣的是寻找对于群论和上列其它递归不可判定系统的相应程序的不可能性. 特别地 ZF 的递归不可判定性蕴涵着：不存在普遍的程序，它能用以断定一般的数学命题是否为定理. 那怕最终计算机遍布世界，它们也决不能代替数学家.

练习

23 (见命题 7.42). 令 $\mathscr{L}_2$ 是不带个体常元，不带函数字母而只有两个一元谓词字母 A_1^1 和 A_2^1 的一阶语言，证明 $\mathscr{L}_2$ 的一个公式 $\mathscr{A}$ 在每个解释中皆真，如果它在包含四个元或不到四个元的个体域上的每个解释中皆真. 描述一个算法，它能判定 $\mathscr{L}_2$ 的一个给定的公式 $\mathscr{A}$ 在每个这样的解释下是否为真.

24. 证明下列集合不是递归的.

(a) $\{n\in D_N: n$ 是一公式$\sim\mathscr{A}$的哥德尔数，其中$\mathscr{A}$是$\mathscr{N}$的一条定理$\}$

(b) $\{n\in D_N: n$ 是$\mathscr{N}$的一公式$\mathscr{A}$和哥德尔数，其中$\mathscr{A}$在N中假$\}$

(c) $\{n\in D_N: n$ 是$\mathscr{N}$中并非定理的一个公式$\mathscr{A}$的哥德尔数$\}$

25. 在练习 24 中给出的集，证明(i)是递归可枚举的，(iii)不是递归可枚举的.

26. 证明练习24中的集(ii)不是递归可枚举的如下. 假设情况相反，集合通过递归函数f是可枚举的. 在D_N上定义一个关系F: $F(m, n)$成立，当且仅当m是有一个自由变元x_1的公式$\mathscr{A}(x_1)$的哥德尔数，且$f(n)$是$\mathscr{A}(0^{(m)})$的哥德尔数. 证明F是递归的用(丘奇论题). 因此F在$\mathscr{N}$中是可表示的，通过比如说公式$\mathscr{F}(x_1, x_2)$. 现在令p是公式$(\exists x_2)\mathscr{F}(x_1, x_2)$的哥德尔数，且令$\mathscr{V}$是公式$(\exists x_2)\mathscr{F}(0^{(p)}, x_2)$. 证明$\mathscr{V}$在$N$中为假，且$\mathscr{V}$的哥德尔数不是在$f$的值域中，给出了一个矛盾. (参见 6.5 节哥德尔不完全性定理的证明).

27. 让我们说，一个一阶系统S是递归可公理化的，如果存在一个一阶系统T，有与S相同的定理，使得T的公理的哥德尔数是递归的. 证明. 如果S是递归可公理化的，那么S的定理的哥德尔数是递归可枚举的. 推演如果S是递归可公理化的且完全的，那么S是递归可判定的.

〔附录〕

可数集和不可数集

定义 A1

一个集合称为可数的，如果它能和自然数集建立 1-1 对应. 换言之，一个集 A 是可数的，如果存在一个双射 $f: D_N \to A$.

注意，一可数集的元素可以写成一列，定义中给出的双射为此提供了一种方法，即枚举 $f(0), f(1), f(2), \cdots$

显然，自然数构成一个可数集.

命题 A2

如果 A 和 B 是可数集，则存在一个 A 和 B 之间的双射. 反之，如果 A 是一可数集并且存在一个 A 和 B 之间的双射，则 B 是可数的.

证明 令 $f: D_N \to A$ 和 $g: D_N \to B$ 是双射. 那么 $g \circ f^{-1}$ 是由 A 到 B 的双射.

对于逆命题，令 $f: D_N \to A$ 是一双射，且 A 可数，假设存在一个由 A 到 B 的双射. 那么 $h \circ f$ 是由 D_N 到 B 的一个双射，所以 B 是可数的.

命题 A3

一可数集的任何无限子集是可数的.

证明 令 A 是一可数集，令 $f: D_N \to A$ 是一双射且令 B 是 A 的无限子集. 则 $f(0), f(1), f(2), \cdots$ 是 A 的所有成员的列. 从这列中除去不是 B 的一切元素. 剩下的是 B 的元素列(无限的). 现在一个双射 $g: D_N \to B$ 可以如下定义

$$g(n) = \text{新列中第}(n+1)\text{个元素}(n \in D_N).$$

(它一定是第$(n+1)$个元素，因为第一个是$g(0)$，第二个是$g(1)$，依此类推)。

命题 A4

一个无限集A是可数的，当且仅当，存在一个单射$h: A\to D_N$。

证明 如果A可数，则存在一个双射$D_N\to A$，它的逆一定是一个单射$A\to D_N$。

反之，假设有一单射$h: A\to D_N$。则$h(A)\subseteq D_N$且$h(A)$无限，因为h是1-1的。根据命题A3，$h(A)$是可数的。令$g: D_N\to h(A)$是一双射。那么合成$h^{-1}\circ g$是由D_N到A的双射，且A是可数的。

▷这最后的结果，通常在证明一个特殊的集是可数时，能最方便的使用，我们很快将看到它的应用。

命题 A5

两个不相交的可数集的并是可数的。

证明 令A和B是两不相交的可数集，且令$f: D_N\to A$和$g: D_N\to B$都是双射。定义$h: D_N\to A\cup B$如下：

$$h(n)=\begin{cases} f\left(\frac{1}{2}n\right) & \text{如果 } n \text{ 是偶数.} \\ g\left(\frac{1}{2}n-\frac{1}{2}\right) & \text{如果 } n \text{ 是奇数.} \end{cases}$$

容易证明h是一双射，因此$A\cup B$是可数的(h给出了$A\cup B$的元素列$f(0), g(0), f(1), g(1), f(2), \cdots$)

系 A6

任意有限个不相交的可数集的并是可数的。

证明 通过对可数集的个数进行归纳加以证明。

基础步骤：两个不相交的可数集的并是可数的。

归纳步骤：令$n>2$，且$A_1, \cdots, A_n$是不相交的可数集。归纳假设$n-1$个可数集的并是可数的。即$A_1\cup A_2\cup\cdots\cup A_{n-1}$是可

数的．因此，据命题 A5，集$(A_1\cup A_2\cup\cdots\cup A_{n-1})\cup A_n$也是可数的．

由数学归纳原理就可得所要的结果．

注记 可以免除可数集是不相交的要求．这个证明留作读者的练习．

问题 是否存在既非有限又非可数的集？我们从上面知道D_N和它的一切子集是有限的或可数的．答案在下面的命题给出．

命题 A7

D_N的一切子集组成的集是无限且不可数的．

证明 用$P(D_N)$表示由D_N的一切子集组成的集．$P(D_N)$显然是无限的．假设它是可数的，令$f: D_N\to P(D_N)$是一个双射．那么对于每个$n\in D_N$，$f(n)$是D_N的一个子集．令

$$B=\{k\in D_N: k\notin f(k)\}.$$

B确实是D_N的一个子集(可能空的，也可能是D_N)．也有$B\neq f(n)$对任何$n\in D_N$．因为假设$B=f(n)$．如果$n\in f(n)$，因为$B=f(n)$，则$n\in B$，但是由B的定义$n\notin B$的．如果$n\notin f(n)$，因为$B=f(n)$，则$n\notin B$，但是根据定义$n\in B$．至少一种假设会导致矛盾．因此$B\neq f(n)$，对任意$n\in D_N$，所以f不是D_N和$P(D_N)$之间的双射．这与我们最初的假设矛盾，因此$P(D_N)$是不可数的．

系 A8

在D_N上的一切函数组成的集是不可数的．

证明 对D_N的每一子集A，定义一个函数$C_A: D_N\to D_N$(A的特征函数)如下．

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

集合A和函数C_A之间的对应是一个双射，它由$P(D_N)$映射到D_N上函数集的一个子集．$P(D_N)$不是可数的，所以D_N上函数集有一不可数的子集．(如果两集合间有一双射，且其中之一可数，则另一集也可数．)如果D_N的函数集是可数的，那么它的任何无

限子集也将是可数的(据命题 A3). 因为,由于它有一个不可数子集,所以 D_N 上的一切函数组成的集是不可数的.

系 A9

D_N 上的一切关系组成的集是不可数的.

证明 关系的集包括函数的集. 通过类似于上述的论证,关系组成的集不可能是可数的.

▷在课文中我们用了这样的结果,如果一个不可数集有一可数的子集,那么该子集一定是真子集. 现在这一点将是明显的,因为一个集不可能既是可数的又是不可数的.

我们也用了一个结果. 在一给定的符号语言中的合式公式集是可数的. 有几个一般的结果使我们懂得为什么会是这样.

命题 A10

令 A 是可数集. A 的一切有限子集组成的集是可数集.

证明 令 $f: D_N \to A$ 是一双射. 我们可以定义一个由 A 的一切有限子集组成的集到 D_N 的单射 g 如下. 令 F 是 A 的一个有限子集. 那么 $f^{-1}(F)$ 是 D_N 的一个有限子集. 令 $g(F)=$ 素数 p_n 的乘积,对 $n \in f^{-1}(F)$. (这里 p_i 表示第 i 个奇素数,对 $i>0$. 且 $p_0=2$.)由于在两个不同的集 F 中,不会出现同样的由素数相乘的积, 且两个不同的素数积不可能相等所以 g 是 1-1 的. 因此根据命题 A4, D_N 上一切有限子集组成的集是可数的.

命题 A11

令 A 是一个可数集. 则 A 的元素的一切有限序列组成的集是一可数集.

证明 我们在这里可以按一种稍微不同的方法去使用素数的性质. 令 $f: D_N \to A$ 是一双射,定义由 A 的元素的一切有限序列组成的集到 D_N 的双射 h 如下. 如果 $u_0, u_1, \cdots, u_k \in A$, 令

$$h(u_0, u_1, \cdots, u_k) = p_0^{f^{-1}(u_0)} \times p_1^{f^{-1}(u_1)} \times \cdots \times p_k^{f^{-1}(u_k)},$$

其中 p_i 如前面证明中所述. 因为 f 是一双射,和素数幂分解的唯

一性，h 是 1-1 的．因此，根据 $A4$，A 的元素的一切有限序列组成的集是可数的．

▷这个命题有一个可以作为系的，我们所需要的关系形式语言的结果．我们的一切形式语言都有符号库，它们是可数集．（这个证明要求使用系 $A6$）．一形式语言 $\mathscr{L}$ 的公式集，是取自 $\mathscr{L}$ 的符号库的符号的一切有限序列组成的集的一个子集．这个有限序列组成的集是可数的，所以它的任意子集也是可数的（或有限的）．但是我们知道一切公式组成的集总是无限的，这样就有了我们的结果。

部分习题的提示和解答

第一章

1(*a*) $(A\wedge B)\to C$.

(*g*) $A\leftrightarrow(B\vee C)$.

(*h*) $A\to(B\to C)$.

5 (*a*), (*b*), (*d*).

7 取 p 真和 q 真. 取 $\mathscr{A}$ 和 $\mathscr{B}$ 为任意重言式.

10 $((\sim p)\vee q)$ 逻辑等值于 $(p\to q)$.

所以 $(\sim((\sim p)\vee q)\vee r)$ 逻辑等值于 $(\sim(p\to q)\vee r)$.

12(*a*) $((p\wedge q)\vee((\sim p)\wedge(\sim q)))$.

(*d*) $((p\wedge(\sim q)\wedge(\sim r))\vee((\sim p)\wedge q\wedge(\sim r))\vee((\sim p)\wedge(\sim q)\wedge(\sim r)))$.

13(*a*) $(((\sim p)\vee(\sim q)\vee r)\wedge(p\vee(\sim q)\vee r)\wedge(p\vee q\vee r))$.

14(*b*) $((p\vee q)\vee(\sim(r\vee(\sim s))))$.

17(*b*) 考察一个包含命题变元 p 和 q, 和仅含联结词～和↔的命题形式. 可以见到它的真值表必定包含 4 个 F 或 4 个 T, 或 2 个 F 和 2 个 T. 一个完整的证明, 需要象在命题 1.15 中使用的那种归纳证明.

19. 这样的真值表, 必定有 4 行, 因而必定是 16 种可能情况之一. 而所有这 16 种都可说明其或属已知或单独不能构成完全集.

20(*b*) $(p\to(q\vee r))$, $(\sim r)$: $\therefore((\sim q)\to(\sim p))$. 有效.

(*d*) $(p\to(q\wedge r\wedge s))$, q, $(s\to r)$; $\therefore s\to p$. 无效.

第二章

1(b) (1) $(p_1\to(p_2\to p_3))\to((p_1\to p_2)\to(p_1\to p_3))$ (L2)

(2) $((p_1\to(p_2\to p_3))\to((p_1\to p_2)\to(p_1\to p_3)))$
$\to(((p_1\to(p_2\to p_3))\to(p_1\to p_2))\to((p_1$
$\to(p_2\to p_3))\to(p_1\to p_3)))$ (L2)

(3) $((p\to(p_2\to p_3))\to(p_1\to p_2))\to((p_1\to(p_2\to p_3))$
$\to(p_1\to p_3))$ 1, 2 MP

(d) (1) $p_2\to(p_1\to p_3)$ (L1)

(2) $(p_2\to(p_1\to p_3))\to(p_1\to(p_2\to(p_1\to p_3)))$ (L1)

(3) $(p_1\to(p_2\to(p_1\to p_3)))$ 1, 2 MP

2(b) (1) $(\sim\sim\mathscr{A})$ 假设

(2) $(\sim\sim\mathscr{A})\to((\sim\sim\sim\sim\mathscr{A})\to(\sim\sim\mathscr{A}))$ (L1)

(3) $(\sim\sim\sim\sim\mathscr{A})\to(\sim\sim\mathscr{A})$ 1, 2 MP

(4) $((\sim\sim\sim\sim\mathscr{A})\to(\sim\sim\mathscr{A}))\to((\sim\mathscr{A})$
$\to(\sim\sim\sim\mathscr{A}))$ (L3)

(5) $(\sim\mathscr{A})\to(\sim\sim\sim\mathscr{A})$ 3, 4 MP

(6) $((\sim\mathscr{A})\to(\sim\sim\sim\mathscr{A}))\to((\sim\sim\mathscr{A})\to\mathscr{A})$ (L3)

(7) $(\sim\sim\mathscr{A})\to\mathscr{A}$ 5, 6 MP

(8) $\mathscr{A}$ 1, 7 MP

(d) (1) $\mathscr{A}\to(\mathscr{B}\to\mathscr{C})$ 假设

(2) $(\mathscr{A}\to(\mathscr{B}\to\mathscr{C}))\to((\mathscr{A}\to\mathscr{B})\to(\mathscr{A}\to\mathscr{C}))$ (L2)

(3) $(\mathscr{A}\to\mathscr{B})\to(\mathscr{A}\to\mathscr{C})$ 1, 2 MP

(4) $\mathscr{B}\to(\mathscr{A}\to\mathscr{B})$ (L1)

(5) $\mathscr{B}\to(\mathscr{A}\to\mathscr{C})$ 3, 4 HS

3(b) (1) $\mathscr{B}\to\mathscr{A}$ 假设

(2) $(\sim\sim\mathscr{B})\to\mathscr{B}$ 习题2(b)和D演绎定理

(3) $(\sim\sim\mathscr{B})\to\mathscr{A}$ 1, 2 HS

(4) $\mathscr{A}\to(\sim\sim\mathscr{A})$ 习题 3(a)

(5) $(\sim\sim\mathscr{B})\to(\sim\sim\mathscr{A})$ 3, 4 HS

(6) $((\sim\sim\mathscr{B})\to(\sim\sim\mathscr{A}))\to(\sim\mathscr{A}\to\sim\mathscr{B})$ (L3)

(7) $(\sim\mathscr{A})\to(\sim\mathscr{B})$ 5, 6 MP

$\therefore\ (\mathscr{B}\to\mathscr{A})\underset{L}{\vdash}((\sim\mathscr{A})\to(\sim\mathscr{B}))$

所以 $\underset{L}{\vdash}(\mathscr{B}\to\mathscr{A})\to((\sim\mathscr{A})\to(\sim\mathscr{B}))$ 据演绎定理

3(d) (1) $\sim(\mathscr{A}\to\mathscr{B})$ 假设

(2) $(\mathscr{B}\to(\mathscr{A}\to\mathscr{B}))\to(\sim(\mathscr{A}\to\mathscr{B})\to\sim\mathscr{B})$ 习题 3(b)

(3) $\mathscr{B}\to(\mathscr{A}\to\mathscr{B})$ (L1)

(4) $\sim(\mathscr{A}\to\mathscr{B})\to\sim\mathscr{B}$ 2, 3 MP

(5) $\sim\mathscr{B}$ 1, 5 MP

(6) $\sim\mathscr{B}\to(\mathscr{B}\to\mathscr{A})$ 命题 2.11(a)

(7) $(\mathscr{B}\to\mathscr{A})$

$\therefore\ \sim(\mathscr{A}\to\mathscr{B})\underset{L}{\vdash}(\mathscr{B}\to\mathscr{A})$

所以 $\underset{L}{\vdash}(\sim(\mathscr{A}\to\mathscr{B})\to(\mathscr{B}\to\mathscr{A}))$ 据演绎定理

4. 注意，由于在证明中不用到(L3)，演绎定理对 L' 成立.

(i) (1) $(\sim\mathscr{A})\to(\sim\mathscr{B})$ 假设

(2) $(\sim\mathscr{A})\to\mathscr{B}$ 假设

(3) $((\sim\mathscr{A})\to(\sim\mathscr{B}))\to(\mathscr{B}\to\mathscr{A})$ (L3)

(4) $(\mathscr{B}\to\mathscr{A})$ 1, 3 MP

(5) $(\sim\mathscr{A})\to\mathscr{A}$ 2, 4 HS

(6) $((\sim\mathscr{A})\to\mathscr{A})\to\mathscr{A}$ 命题 2.11(b)

(7) $\mathscr{A}$ 5, 6 MP

(ii) (1) $(\sim\mathscr{A})\to(\sim\mathscr{B})$ 假设

(2) $\mathscr{B}$ 假设

(3) $((\sim\mathscr{A})\to(\sim\mathscr{B}))\to(((\sim\mathscr{A})\to\mathscr{B})\to\mathscr{A})$ (L'3)

(4) $((\sim\mathscr{A})\to\mathscr{B})\to\mathscr{A}$ 1, 3MP

(5) $\mathscr{B}\to((\sim\mathscr{A})\to\mathscr{B})$ ($L1$)

(6) $(\sim\mathscr{A})\to\mathscr{B}$ 2, 5MP

(7) $\mathscr{A}$ 4, 6MP

8. $\mathscr{A}$ 不是重言式，所以不是 L 的一条定理. 应用习题 7. L^+ 是一致的. 假如不然，那么 $\vdash_L(\mathscr{A}\to\mathscr{B})$ 和 $\vdash_L(\mathscr{A}\to\sim\mathscr{B})$，对某个合式公式 $\mathscr{B}$. 因此 $\vdash_L((\sim\mathscr{B})\to(\sim\mathscr{A}))$，和 $\vdash_L(\mathscr{B}\to(\sim\mathscr{A}))$，由此推得 $\vdash_L(\sim\mathscr{A})$. 但是 $\mathscr{A}$ 不是一个矛盾式；所以 $(\sim\mathscr{A})$ 不是 L 的一条定理.

10. 令 $\mathscr{A}$ 和 $\mathscr{B}$ 是重言式. 因此 $((\sim\mathscr{A}\to\mathscr{B})\to(\mathscr{A}\to\sim\mathscr{B}))$ 是一矛盾式，它的否定是 L 的一条定理，从而也是 L^{++} 的定理. 但是它是新公理模式的一个实例，因而本身是 L^{++} 的一条定理. 这样 L^{++} 是不一致的.

12. 利用命题 1.10, 2.14 和 2.23.

第三章

1(a) $\sim(\forall x)(F(x)\to D(x))$.

(c) $(\exists x)(T(x)\wedge L(x))\to(\forall x)(T(x)\to L(x))$.

(f) $(\exists x)(P(x)\wedge(\forall y)(P(y)\to H(x, y)))$.

2(a) $\sim(\forall x)(C(x)\to T(x))$

$(\exists x)(C(x)\wedge\sim T(x))$.

(v) $(\forall x)(\forall y)((M(x)\wedge E(y))\to\sim H(x, y))$

$\sim(\exists x)(\exists y)(M(x)\wedge E(y)\wedge H(x, y))$.

6. (a), (e), (g), (h).

7. $f_1^2(x_1, x_2)$ 在所有式中对 x_2 是自由的.

8. x_j 仅仅在 x_i 自由出现在 $\mathscr{A}(x_i)$ 之处，才在 $\mathscr{A}(x_j)$ 中自由

出现．这样的出现不可能在$(\forall x_i)$的辖域之中．

9．在(a)和(b)中，t对x_1是自由的．

10．(a) 在(b)和(c)中，x_2对x_1是自由的．

(d) $f_1^3(x_1, x_2, x_3)$只在(b)中对x_1是自由的．

11．$\mathscr{A}$在I中的解释是真的．

取D_I为Z，$\bar{a}_1$为0，$\bar{f}_1^2$为$+$，$\bar{A}_2^2$为$=$．

12．取D_I为Z，$\bar{A}_1^1(x)$为$x>0$，$\bar{f}_1^1(x)$为$-x$．

14．(a) 当$v(x_1)=4$，$v(x_2)=2$，$v(x_3)=6$时，v满足；

当$v(x_1)=1$，$v(x_2)=2$，$v(x_3)=4$时，v不满足．

(b) 当$v(x_1)=1$，$v(x_2)=1$，$v(x_3)=2$时，v满足；

当$v(x_1)=1$，$v(x_2)=1$，$v(x_3)=3$时，v不满足；

15．(b) 当$v(x_1)=1$，$v(x_2)=2$时，v满足；

当$v(x_1)=3$，$v(x_2)=2$时，v不满足．

(c) 当$v(x_1)=1$，$v(x_2)=1$时，v满足．

当$v(x_1)=1$，$v(x_2)=2$时，v不满足．

16．(a) 假；(b)，(c)，(d)真．

19．(a) 令I是一个解释，v是一个在I中满足$(\exists x_1)(\forall x_2)A_1^2(x_1, x_2)$的赋值．那么，存在一个1-等值于$v$的赋值$v'$，满足$(\forall x_2)A_1^2(x_1, x_2)$，比如$v'(x_1)=x$．于是，每个2-等值于$v'$的赋值$v''$满足$A_1^2(x_1, x_2)$．现在假设$v$不满足$(\forall x_2)(\exists x_1)A_1^2(x_1, x_2)$．那么就会存在一个2-等值于$v$的赋值$w$不满足$(\exists x_1)A_1^2(x_1, x_2)$，比如$w(x_2)=y$．不存在1-等值于$w$的赋值满足$A_1^2(x_1, x_2)$．但是如果$v''(x_1)=x$，$v''(x_2)=y$，$v''(x_k)=v(x_k)$ $(k>2)$，则v''是1-等值于w的，并且它满足$A_1^2(x_1, x_2)$．

(c) 令I是一个解释，v是I中满足$(\forall x_1)(\mathscr{A}\to\mathscr{B})$的赋值．那么，每个1-等值于$v$的赋值$v'$满足$(\mathscr{A}\to\mathscr{B})$．现在假设$v$不满足$(\forall x_1)\mathscr{A}\to(\forall x_1)\mathscr{B}$．那么，$v$满足$(\forall x_1)\mathscr{A}$而不满足$(\forall x_1)\mathscr{B}$，所以有1-等值于$v$的赋值$v'$，满足$\mathscr{A}$而不满足$\mathscr{B}$．这

个 v' 不满足 $\mathscr{A}\to\mathscr{B}$.

21. 用命题 3.23

22. (a) 取 D_I 为 Z, $\overline{A}_1^2$ 为 $<$.

(c) 取 D_I 为 Z, $\overline{A}_1^2(x)$ 为 $x=0$, $\overline{a}$ 为 0.

(d) 这在 N 中是假的.

23. 命题 3.23

第四章

1. 见例 2.7(a), 用一次概括.

2(a) 首先证 $\{\sim\mathscr{B}, (\forall x_i)\mathscr{A}\}\underset{K}{\vdash}(\forall x_i)\sim(\mathscr{A}\to\mathscr{B})$. 通过演绎定理, 推得

$$\sim\mathscr{B}\underset{K}{\vdash}((\forall x_i)\mathscr{A}\to(\forall x_i)\sim(\mathscr{A}\to\mathscr{B}))$$

因此 $$\sim\mathscr{B}\underset{K}{\vdash}(\sim(\forall x_i)\sim(\mathscr{A}\to\mathscr{B})\to\sim(\forall x_i)\mathscr{A})$$

现在通过使用演绎定理的逆.

$$\{\sim\mathscr{B}, (\exists x_i)(\mathscr{A}\to\mathscr{B})\}\underset{K}{\vdash}\sim(\forall x_i)\mathscr{A}$$

当 x_i 在 $\mathscr{B}$ 中不自由出现时, 我们就有 $(\exists x_i)(\mathscr{A}\to\mathscr{B})\underset{K}{\vdash}(\sim\mathscr{B}\to\sim(\forall x_i)\mathscr{A})$. (再两步就可得所要求的结果.

(b) 类似地, 首先证 $\{((\exists x_i)\mathscr{A}\to\mathscr{B}), \sim\mathscr{B}\}\underset{K}{\vdash}\sim\mathscr{A}$. 推出

$((\exists x_i)\mathscr{A}\to\mathscr{B})\underset{K}{\vdash}(\mathscr{A}\to\mathscr{B})$, 并应用概括.

(c) 只需证明 $\underset{K}{\vdash}(((\forall x_i)\sim\sim\mathscr{A})\to(\forall x_i)\mathscr{A})$.

3(b) 取 D_I 为 Z, $\overline{A}_1^2$ 为 $<$.

4. 开始 (1) $(\forall x_i)(\mathscr{A}\to\mathscr{B})$ 假设

(2) $(\forall x_i)\mathscr{A}$ 假设

5. 要求证明

$$\vdash_K (\sim(\sim\forall x_i)\sim\mathscr{A})\to(\forall x_i)(\sim\mathscr{A}))$$

和 $$\vdash_K ((\forall x_i)(\sim\mathscr{A}))\to(\sim(\forall x_i)\sim\mathscr{A})).$$

6(*a*) 用(*K*5)两次，然后概括两次.

(*b*) 按$(\forall x_2)A_1^2(x_1, x_2)\to A_1^2(x_1, x_1)$使用(*K*5).

7. 首先应用命题 4.18 于公式 $\sim\mathscr{A}(x_i)$，得到

$$\vdash_K (\forall x_i)\sim\mathscr{A}(x_i)\leftrightarrow(\forall x_j)\sim\mathscr{A}(x_j).$$

8(*a*) $(\exists x_3)(\forall x_2)(A_1^1(x_3)\to A_1^2(x_1, x_2))$.

(*c*) $(\exists x_1)(\forall x_4)(\exists x_3)((A_1^1(x_1)\to A_1^2(x_1, x_2))\to(A_1^1(x_1)$
$\to A_1^2(x_4, x_3)))$.

(注意：解答并不唯一.)

10. $((\exists x_1)(\exists x_2)A_1^2(x_1, x_2)\to(\exists x_3)A_1^1(x_3))$既可证等价于$\Pi_3$形前束范式，也可证等价于$\Sigma_2$形前束范式.

11. 参见命题 2.18. 证明基本上相同.

12. 假设 S 不完全，并用两次命题 4.35.

13. 取$\mathscr{B}$为$(\sim\mathscr{A})$. $K_\mathscr{L}$不完全，所以我们可以既取$\mathscr{A}$又取$(\sim\mathscr{A})$为非定理.

14. 没有原子公式或它的否定式能够为 $K_\mathscr{L}$ 的定理. 因此，根据命题 4.35，添上一个原子公式或它的否定式为一新公理时，将给出一个一致的扩充. 不同的谓词符号给出不同的原子公式，从而给出不同的扩充.

15. 对从 Γ 到 $\mathscr{A}$ 的演绎步数使用归纳. $K_\mathscr{L}$ 和 Γ 中的成员在 M 中都是真的，M 中的推演规则具有保真性.（参见命题 4.41 的证明.）逆命题未必成立，除非把 Γ 中的一切公式都作为新公理得到的 $K_\mathscr{L}$ 的扩充是完全的.

17. S^+ 未必完全，取 S 为 $K_\mathscr{L}$，其中 $\mathscr{L}$ 仅含一个谓词符号 A_1^1. M 可以这样构造，使得没有一个原子公式在 M 中为真；所以

$S^+=S=K_\varnothing$. $(\forall x_1)A_1^1(x_1)$和$\neg(\forall x_1)A_1^1(x_1)$都不是$K_\varnothing$的定理.

18. 所有新公理在M中真,所以据习题15,$\hat{S}$的每个定理在M中是真的. 因此,$\hat{S}$是一致的,$\hat{S}$未必是完全的.

19. 参见命题4.46的证明(考虑附加公理$A_1^1(a_i)$, $i\geqslant 1$).

第五章

1. 用命题3.27及公理($K5$)的逻辑有效性,去推得:对任意公式$\mathscr{A}(x_i)$,如果$I\models\mathscr{A}(x_i)$,那么$I\models\mathscr{A}(t)$,对在$\mathscr{A}(x_i)$中对x_i自由的任意t. 把这用于公式$A_1^2(x_1, x_2)\to A_1^2(f_1^2(x_1, x_3), f_1^2(x_2, x_3))$(3次,对每个变元代入项),类似地用于

$$A_1^2(x_1, x_2)\to A_1^2(f_1^2(x_3, x_1), f_1^2(x_3, x_2)).$$

2. 假设情况相反,再使用命题4.35和5.6.

3. 对$\mathscr{A}$的长度进行归纳. 基础步骤从($E9'$)直接得到.

归纳步骤:注意如果

$$\vdash x_1=x_2\to(\mathscr{B}(x_1)\to\mathscr{B}(x_2))$$

那么 $\vdash x_1=x_2\to(\mathscr{B}(x_2)\to\mathscr{B}(x_1))$

由于 $\vdash x_2=x_1\to(\mathscr{B}(x_2)\to\mathscr{B}(x_1))$

和 $\vdash(x_1=x_2\to x_2=x_1)$.

使用演绎定理.

4. 从$A_1^2(u_j, v_j)$ $(1\leqslant j\leqslant n)$,通过重复使用($E9$),我们能够在$S$中推得$A_1^n(u_1, \cdots, u_n)\leftrightarrow A_1^n(v_1, \cdots, v_n)$,其中$u_j$和$v_j$代表变元. 因此如果$\overline{A}_1^2(y_j, z_j)$在$M$中对每个$j$成立,那么$\overline{A}_1^n(y_1, \cdots, y_n)$在$M$中成立,当且仅当,$\overline{A}_1^n(z_1, \cdots, z_n)$成立

6. 归纳论证类似于习题3.

7. (a) 语言:变元,f_1^1, f_1^2, $=$.

把($G2$)和($G3$)换成

$$(\exists x_1)(\forall x_2)(f_1^2(x_1, x_2)=x_2\wedge f_1^2(f_1^1(x_2), x_2)=x_1).$$

(b) 语言:变元,a_1, $=$, A_1^2.

$(A_1^3(x_1, x_2, x_3)$解释为 $x_1x_2=x_3)$.

把$(G1)$—$(G3)$换成

$$(\forall x_1)(\forall x_2)(\exists_1 x_3)A_1^3(x_1, x_2, x_3),$$

$$(A_1^3(x_1, x_2, x_4)\wedge A_1^3(x_4, x_3, x_5)\wedge A_1^3(x_2, x_3, x_6)$$
$$\wedge A_1^3(x_1, x_6, x_7))\Rightarrow x_5=x_7,$$

$$(\forall x_2)(\exists x_1)A_1^3(x_1, x_2, a_1)$$

和 $$(\forall x_1)A_1^3(a_1, x_1, x_1).$$

9. 包含 a_1 具有突出模型中的一个元素即 $\bar{a}_1$ 的效果，这与选择哪个元素无关. 包含序列 $a_1, a_2, \cdots$时，情况类似，不过它们的解释不必都是不同的元素.

12. 用 kx_1 表示$\mathscr{F}$ 中 x_1 自身相加 k 次的和 $(k>1)$，用(Ok)表示$(kx_1=0)\Rightarrow(x_1=0)$($\mathscr{F}$ 中的公式). 每个(Ok)在特征为 0 的域上为真，确实，带有这些新公理的$\mathscr{F}$ 给出了特征为 0 的域论的一个系统. 现在，如果 $\mathscr{A}$ 在这个系统的每一个模型上为真，那么它是系统的一条定理. 在 $\mathscr{A}$ 的一个证明中，只用到有限多个公理，所以，比如说$(Ok)(k>n)$并没使用，特征 p 的域$(p>n)$，是带有附加公理$(O2)$，…，(On)的 $\mathscr{F}$ 的模型. $\mathscr{A}$ 是这个系统的一条定理，所以它在每个这样的模型中是真的.

13. 利用习题 12 中的思想，参见系 4.47.

14. $\mathscr{N}''$ 的公理并不专门提到 a_0，所以它的解释并没受到具有任何特殊性质的约束. 如果选择 $\bar{a}_0$ 为 r，那么公式$\sim(a_0=a_i)$在 $\mathscr{N}''$ 中为真，对每个 $i\leqslant r$. 因此对每个 r，公式集 $\{\sim(a_0=a_i): 0<i\leqslant r\}$ 有一个模型，并且从 $\mathscr{N}''$ 通过增添它们为公理而得到的系统是一致的. 因此，通过增添所有这些合式公式，对 $i>0$，而得到的系统也是一致的(通过熟知的论证—见例如命题 2.21 证明). 这样的一个模型称为算术的非标准模型，因为它包括一切自然数，并且至少还包括一个其它元素. 这个其它元素当然必定具有后继和前趋，以及与自然数和它自身的和与积等等.

15. 用$(\forall x_1)\sim(x_1\in a_1)$代替$(ZF2)$.

添上$(ZF2')$: $A_3^2(t_1, t_2)\leftrightarrow(\forall x_1)(x_1\in t_1\rightarrow x_1\in t_2)$.

用 $(\forall x_1)(\forall x_2)(\forall x_3)\ x_3\in f_1^2(x_1, x_2)\leftrightarrow x_3=x_1\vee x_3=x_2)$ 代替$(ZF3)$.

这个解释域D的元素是0, 1, 2, …, 其中$0=\varnothing$和$n=\{0, 1, \cdots, n-1\}$对$n\neq 0$. 对$(ZF1)$: 如果$m=n=0$, 那么m和n都没有成员; 如果$m=n\neq 0$, 那么每个都有元素0, 1, …, $m-1$. 相反, 如果m和n有相同的成员, 那么或者都是0, 或者$\{0, 1, \cdots, m-1\}=\{0, 1, \cdots, n-1\}$, 所以$m=n$. 对$(ZF2)$, 显然0是空集. 对$(ZF3)$, 考察$2, 3\in D$. $\{2, 3\}\notin D$, 所以$(ZF3)$是假. 对$(ZF4)$: $\bigcup 0=0$, $\bigcup 1=0$和$\bigcup\{0, 1, \cdots, m-1\}=\{0, 1, \cdots, m-2\}=m-1\in D$. 对$(ZF5)$: 集2的子集是$\varnothing$, $\{0\}$, $\{1\}$, 和$\{0, 1\}$, 这些元素并不构成D的一个元素. 对$(ZF7)$: 假设m是一集, 它的存在由$(ZF7)$肯定, 那么$m\neq 0$, 因为$0\notin 0$, 并且如果$m=\{0, 1, \cdots, m-1\}$, 那么$m-1\in m$且$(m-1)\cup\{m-1\}\notin m$, 因为$m\notin m$. 对$(ZF8)$, 如果$m=\{0, 1, \cdots, m-1\}$, 那么$0\in m$, 并且0和m没有共同元素.

$(ZF6)$是假的. 取$\mathscr{A}(x_1, x_2)$为$x_2=\{x_1\}$. 那么(例如)集2的象不是D的一个成员.

第六章

1. 据例6.7, 如果$m+r=n$, 那么$\underset{\mathscr{N}}{\vdash} 0^{(m)}+0^{(r)}=0^{(n)}$. 使用公理$(K5)$按下形式

$$(\forall x_1)\sim(0^{(m)}+x_1=0^{(n)})\rightarrow\sim(0^{(m)}+0^{(r)}=0^{(n)})$$

我们可以如愿推出$\underset{\mathscr{N}}{\vdash}\sim(\forall x_1)\sim(0^{(m)}+x_1=0^{(n)})$.

2. 令$m>n$. 那么$m=n+r$, $r>0$. 所以, 有$\underset{\mathscr{N}}{\vdash} 0^{(m)}+0^{(n)}+$

$0^{(r)}$ 和 $\vdash_{\mathscr{N}} 0^{(m)}+x_1=0^{(n)}+0^{(r)}+x_1$. 现在 $\vdash_{\mathscr{N}} 0^{(n)}+0^{(r)}+x_1=0^{(n)}$, 产生:

$\vdash_{\mathscr{N}} 0^{(r)}+x_1=0$(参见命题 6.1 的证明), 和 $\vdash_{\mathscr{N}} 0^{(r)}+x_1=(0^{(r-1)}+x_1)'$,

由$(N4^*)$, 因为 $r>0$. 因此

$$\vdash_{\mathscr{N}} 0^{(n)}+0^{(r)}+x_1=0^{(n)}\rightarrow\sim(N1^*),$$

所以 $$\vdash_{\mathscr{N}} \sim(0^{(n)}+0^{(r)}+x_1=0^{(n)}),$$

即 $$\vdash_{\mathscr{N}} \sim(0^{(m)}+x_1=0^{(n)}).$$

通过概括, $\vdash_{\mathscr{N}}(\forall x_1)\sim(0^{(m)}+x_1=0^{(n)})$ 从而得到结果.

3(*a*) $\sim(\forall x_1)(\forall x_2)\sim(x_1x_2=0^{(n)})$.

(*c*) 重写 $m=\min(p, q)$ 为: $(p\leqslant q\wedge m=p)\vee(q<p\wedge m=q)$.

(*e*) 重写成 $(m=0\wedge n=0)\vee(m\neq 0)\wedge n=1)$.

4(*a*) 对 $m=0$, $n=0$, 证明

$$\vdash_{\mathscr{N}}(0^{(0)}=0\wedge 0^{(0)}=0)\vee(0^{(0)}\neq 0\wedge 0^{(0)}=0^{(1)}).$$

对 $m\neq 0$, $n=1$, 证明

$$\vdash_{\mathscr{N}}(0^{(m)}=0\wedge 0^{(1)}=0)\vee(0^{(m)}\neq 0\wedge 0^{(1)}=0^{(1)}).$$

对 $m=0$, $n\neq 0$, 证明

$$\vdash_{\mathscr{N}}\sim(0^{(0)}=0\wedge 0^{(n)}=0)\vee(0^{(0)}\neq 0\wedge 0^{(n)}=0^{(1)}).$$

对于 $m\neq 0$, $n=0$, 证明

$$\vdash_{\mathscr{N}}\sim((0^{(m)}=0\wedge 0^{(0)}=0)\vee(0^{(m)}\neq 0\wedge 0^{(0)}=0^{(1)}).$$

最后, 对 $m=0$ 和 $m\neq 0$ 分别地证明

$$\vdash_{\mathscr{N}}(\exists_1 x_1)((0^{(m)}=0\wedge x_1=0)\vee(0^{(m)}\neq 0\wedge x_1=0^{(1)})).$$

(*b*) 令 $\mathscr{A}(x_1, x_2)$ 是公式 $x_2=x_1+0^{(3)}$.

如果 $n=m+3$, 那么 $\vdash_{\mathscr{N}} 0^{(n)}=0^{(m)}+0^{(3)}$.

如果 $n\neq m+3$, 那么 $\vdash_{\mathscr{N}} \sim(0^{(n)}=0^{(m)}+0^{(3)})$.

对任何 $m\in D_N$, 也有 $\vdash_{\mathscr{N}} (\exists_1 x_2)(x_2=0^{(m)}+0^{(3)})$.

(或用例 6.7 亦可).

(c) 令 $\mathscr{A}(x_1, x_2)$ 是 $(\exists x_3)((x_1=x_2+x_3\times 0^{(2)})\wedge(x_2=0\vee x_2=1))$.

5. 这是应用演绎定理的一个比较复杂的习题. 我们必须证明: 如果 $f(m)\neq n$, 那么 $\vdash_{\mathscr{N}} \sim\mathscr{A}(0^{(m)}, 0^{(n)})$. 令 $f(m)=p$. 我们需要证明:

$$\{0^{(n)}\neq 0^{(p)}, \mathscr{A}(0^{(m)}, 0^{(p)}), (\exists_1 x_2)\mathscr{A}(0^{(m)}, x_2)\}\vdash_{\mathscr{N}} \sim\mathscr{A}(0^{(m)}, 0^{(n)}).$$

这只需证明

$$\{0^{(n)}\neq 0^{(p)}, \mathscr{A}(0^{(m)}, 0^{(p)})\}\vdash_{\mathscr{N}} (\exists_1 x_2)\mathscr{A}(0^{(m)}, x_2)\to\sim\mathscr{A}(0^{(m)}, 0^{(n)}).$$

或

$$\{0^{(n)}\neq 0^{(p)}, \mathscr{A}(0^{(m)}, 0^{(p)})\}\vdash_{\mathscr{N}} \mathscr{A}(0^{(m)}, 0^{(n)})\to\sim(\exists_1 x_2)\mathscr{A}(0^{(m)}, x_2)$$

或

$$\{0^{(n)}\neq 0^{(p)}, \mathscr{A}(0^{(m)}, 0^{(p)}), \mathscr{A}(0^{(m)}, 0^{(n)})\}\vdash_{\mathscr{N}} \sim(\exists_1 x_2)\mathscr{A}(0^{(m)}, x_2)$$

直觉上这是显然的, 但是仍然存在技术上的困难. 我们需要

$$\{0^{(n)}\neq 0^{(p)}, \mathscr{A}(0^{(m)}, 0^{(p)}), \mathscr{A}(0^{(m)}, 0^{(n)})\}\vdash_{\mathscr{N}}$$

$$(\forall x_2)\sim(\mathscr{A}(0^{(m)}, x_2)\wedge(\forall x_3)(\mathscr{A}(0^{(m)}, x_3)\to x_3=x_2)).$$

最后一个公式等价于

$$(\forall x_2)(\mathscr{A}(0^{(m)}, x_2)\to\sim(\forall x_3)(\mathscr{A}(0^{(m)}, x_3)\to x_3=x_2)).$$

所以我们证明

$$\{0^{(n)}\neq 0^{(p)}, \mathscr{A}(0^{(m)}, 0^{(p)}), \mathscr{A}(0^{(m)}, 0^{(n)}), \mathscr{A}(0^{(m)}, x_3)\}$$

$$\vdash_{\mathscr{N}} \sim(\forall x_3)(\mathscr{A}(0^{(m)}, x_3) \to x_3 = x_2)).$$

通过证明 $\{\mathscr{A}(0^{(m)}, 0^{(p)}), \mathscr{A}(0^{(m)}, 0^{(n)}), \mathscr{A}(0^{(m)}, x_2),$

$$(\forall x_3)(\mathscr{A}(0^{(m)}, x_3) \to x_3 = x_2)\} \vdash_{\mathscr{N}} 0^{(n)} = 0^{(p)}.$$

(注意,我们在最后一步,可以不对 x_2 使用概括.

6. 令 $\mathscr{A}(x_1, \cdots, x_{k+1})$ 是 $x_{k+1} = x_k$.

7(a) $e(m, 0) = 1$

$$e(m, n+1) = m \times e(m, n).$$

现在 $e(m, 0)$ 是 m 的一个常函数,它是原始递归的. $m \times e(m, n)$ 也是 m, n 和 $e(m, n)$ 的原始递归函数. 我们可以把 $m \times e(m, n)$ 写成 $h(m, n, e(m, n))$, 其中 $h(m, n, p) = p_1^3(m, n, p) \times p_3^3(m, n, p)$. 在 $m \times e(m, n)$ 中对 n 的依赖并不明显. 由于上面的设计,这并不是必然的.

(b) $\min(m, n) = m \dot{-} (m \dot{-} n)$

(c) 首先令 $rm(m, n) = \begin{cases} n \text{ 被 } m \text{ 除后余项} & \text{如果 } m \neq 0 \\ 0 & \text{如果 } m = 0 \end{cases}$

因此

$$rm(m, 0) = 0$$

$$rm(m, n+1) = sg(m) \times sg((m \dot{-} 1) \dot{-} rm(m, n)) \times (1 + rm(m, n))$$

由于 $+$, $\times$, $\dot{-}$ 和 sg 是原始递归的,所以 rm 也原始递归. 现在

$$q(m, 0) = 0$$

$$q(m, n+1) = sg(m) \times (q(m, n) + \overline{sg}((m \dot{-} 1) \dot{-} rm(m, n)).$$

由于 $+$, $\times$, $\dot{-}$, sg, $\overline{sg}$ 和 rm 是原始递归的,所以 q 是原始递归的.

8. R 是递归的,所以 C_R 是递归的,并且 $R(n_1, \cdots, n_k, x)$ 成立,当且仅当,$C_R(n_1, \cdots, n_k, x) = 0$.

9. $$e_2(n) = \mu x[\overline{sg}(rm(2^x, n)) = 0] \dot{-} 1$$

11. 令 $k(n_1, n_2)=n_1^{n_2}$. k 是递归的，f 和 g 是递归的，所以 h 是递归的，因为 h 是以下的合成

$$h(x)=k[f(x), g(x)).$$

14. 定义一无关系 $R_1, R_2, \cdots$;

$R_i(n)$成立，当且仅当 $R(i, n)$成立.

因而 $S(n)$成立，当且仅当 $R_1 \vee R_2 \vee \cdots \vee R_{k-1}$ 成立，

$T(n)$成立，当且仅当 $R_1 \wedge R_2 \wedge \cdots \wedge R_{k-1}$ 成立.

拿去条件 '$<k$' 时，这些关系不再必定递归. 考察一个非递归集 X，列表为 $\{x_1, x_2, \cdots\}$，并且令 $X_i=\{x_1, \cdots, x_i)$，对 $i \geqslant 1$. 那么令 $R(m, n)$成立，当且仅当 $n \in X_m$. 如上定义的 R_i 是递归的，因为 X_i 是有限集；但是 $S^\infty(n)$不是递归的，于此 $S^\infty(n)$成立，当且仅当存在 m，使得 $R(m, n)$，从而 $S^\infty(n)$成立，当且仅当 $n \in X$，而 X 却不是递归的.

15(a) $65=9+8\times 7=g(a_7)$

(b) $299=11+8\times 36=11+8\times(2^2\times 3^2)=g(f_2^2)$.

(c) $109=13+8\times 12=13+8\times(2^2\times 3)=g(A_1^2)$.

(d) $421=13+8\times 51 \neq g(t)$，$t$ 为任意符号

16(a) $A_1^1(x_1)$

(b) $\sim A_1^1(x_1)$

(c) $(\forall x_1)A_1^1(x_1)$

17. 如果 $s=a_1, a_2, \cdots, a_u$, $t=b_1, b_2, \cdots, b_v$，那么 $m=p_1^{a_1}\times\cdots\times p_u^{a_u}$, $n=p_1^{b_1}\times\cdots\times p_v^{b_v}$. 现在

$$s*t=a_1, a_2, \cdots, a_u, b_1, \cdots, b_v,$$

所以 $$f(m, n)=p_1^{a_1}\times\cdots\times p_u^{a_u}\times p_{u+1}^{b_1}\times\cdots\times p_{u+v}^{b_v}.$$

但是 $b_i=e_i(n)$，$u=\mu x[\overline{sg}(rm(p_x, m))=0]\dot{-}1$，并且由于 p_x 是 x 的递归函数（见例 6.25(a)），u 是 m 的递归函数. 类似地 v 是 n 的一个递归函数，所以

$$f(m, n)=m\times p_{u+1}^{e_1(n)}\times\cdots\times p_{u+v}^{e_v(n)} \quad \text{是递归的.}$$

18. 用 $\mathscr{N}^+$ 表示扩充. 那么 $\vdash_{\mathscr{N}^+} \sim \mathscr{U}$,

$$即 \vdash_{\mathscr{N}^+} \sim (\forall x_2) \sim \mathscr{W}(0^{(p)}, x_2)$$

但是,在命题 6.32 的证明中,证明了 $\vdash_{\mathscr{N}} \sim \mathscr{W}(0^{(p)}, 0^{(q)})$ 对每个 q. 因此,$\vdash_{\mathscr{N}^+} \sim \mathscr{W}(0^{(p)}, 0^{(q)})$ 对每个 q,而 $\mathscr{N}^+$ 不是 ω-一致的.

第七章

1(a) 在第六章中,我们描述了为给定的哥德尔数寻求出相对应的符号或符号串的方法. 给定 n, 找出(如果有的话)与它对应的符号. 如果它是一个变元或常元,那么给出答案是. 如果是其它符号, 给出答案不是. 如果不存在与之对应的符号, 那么去找对应的符号串. 如果是项,那么回答是 . 如果是其它符号串或没有串,回答不是.

(c). 计算所有正整数的平方, 直到 $x^2 \geqslant n$. 如果 n 不出现在直到此时所列的表中,那么它就不是完全平方数.

(d) 对 Γ 中的所有公式和 $\mathscr{A}$ 构造真值表. $\vdash \mathscr{A}$, 当且仅当,Γ 中的所有公式取 T 时,$\mathscr{A}$ 也取 T.

(f) 通过对每个正整数的依次检验, 把素数留下,可以作成一列素数表.

2. 令 A 和 $\overline{A}$ 是递归可枚举的. 然后令 $f(0), f(1), f(2), \cdots$ 和 $g(0), g(1), g(2), \cdots$ 是 A 和 $\overline{A}$ 的能行枚举. 再令 $n \in D_N$. 写出(同时地)上列 A 和 $\overline{A}$ 的表. n 必定出现在其中之一. 当它确实出现时,它所在的表就告诉我们 $n \in A$ 或 $n \in \overline{A}$. 存在一个集 X 是非递归的. 于是 $\overline{X}$ 是非递归的(系 6.23). X 和 $\overline{X}$ 至少有一个是非递归可枚举的,因为如果两个都递归可枚举时,那么它们将都是递归的.

3. 给定 x, 枚举 A 直至找到第一个元素 $\geqslant x$. $x \in A$, 当且仅

当 x 在这个表中.

4(a) 利用丘奇论题. 给定 n, 对于每个 $p<n$, 查出 p 和 n 是否有公因子. 计数这些有公因子的 p. 这是一个计算 $\varnothing$ 的算法

(c) 或者有任意长度的 7 的序列,或者这样的序列的长度有一上界,比如 k. 在第一种情形 $g(n)=0$, 对一切 $n\in D_N$(所以 g 是递归的). 在第二种情形

$$g(n)=\begin{cases}0 & 0\leqslant n\leqslant k\\ 1 & n>k\end{cases}$$

这个函数也是递归的.

5(a) D_N.

(b) $\mathscr{N}$ 的定理的哥德尔数集. $\mathscr{N}$ 的为重言式的公式的哥德尔数集是一个递归子集.

6. 参见习题 3. 给定一集 A 的一个能行枚举, 选出子集 B 的一个递增的枚举. B 将是递归的.

7. 初始纸带, 在非空白部分的右边将需要一个标记, 比如 M. 添加四元组 (q_0BRq_0) 和 (q_0MBq_3).

9. $\{(q_0BRq_3), (q_01Rq_0)\}$

或 $\{(q_0BRq_1), (q_01Rq_1), (q_1BLq_0), (q_01Lq_0)\}$.

10. $\{(q_01Aq_1), (q_1ARq_2), (q_21Rq_2), (q_2BXq_3), (q_3XRq_3), (q_3B1q_4), (q_31Rq_3), (q_41Lq_4), (q_4XLq_4), (q_4ARq_0), (q_0XLq_5), (q_5A1q_5), (q_51Lq_5)\}$. 机器以 q_0 状态读最左边的 1 开始

11. 参见例 7.13 $\{(q_01Rq_1), (q_11Rq_0), (q_0BRq_0)\}$(如果输入数是偶的,四元组 (q_0BRq_0) 保证机器决不停止). 为了得到 T', 删去 (q_0BRq_0), 补上四元组 (q_0BLq_2), (q_01Bq_3), (q_3BLq_3), 考察一切递归偏函数表 ϕ_0, ϕ_1, $\cdots$. 那么 $f(n)=\phi_n(n)+1$ 是一个不能扩充成递归全函数的递归偏函数. 因为假设 ϕ_k 是一个全函数, 并且 $\phi_k(n)=\phi_n(n)+1$, 只要 $\phi_n(n)$ 存在. 现在 ϕ_k 是全的, 所以 $\phi_k(k)$ 存在,并且 $\phi_k(k)=\phi_k(k)+1$. 矛盾. (参见命题 7.28 前的

例子).

12. 假设纸带符号的字母库含 n 个符号，并且有 k 个内状态. 如果机器在 $nk+1$ 步并不移开一给定的方格，那么它将决不停机，因为在那时，它必定重复着一个(状态，读着的符号)对，此后它永远重复一个循环作用. (当然它可以在 $nk+1$ 步之前停机.)如果开始时，纸带的非空白部分由 p 个方格组成，那么在 $p(nk+1)$ 步之后，我们确信机器会停机，或者移开纸带上非空白部分的右端，或者进入了如上的、稳定的循环. 如果移开纸带上非空白部分的右端，那么它最多向右移开 $k+1$ 方格，而没有重复一个(状态，空白)组合. 因此，如果它移开 $k+1$ 格，那么它必定进入一个重复的模式. 现在，在 $(k+1)(nk+1)$ 步后，它将停机或进入一个稳定循环，或者再右移 $k+1$ 格. 因此我们能够进一步说，如果机器终将停机，它将在 $(p+k+1)(nk+1)$ 步或不到这一步时，所以开动机器直到停机，或者到 $(p+k+1)(nk+1)$ 步组成了算法.

15. 假设 $n\in K$，那么 T_n 以 n 输入停机，所以 $n\in A$. 但是 $A\subseteq K$，所以 $n\in K$，矛盾. 现在假设 $n\in A$. 那么 T_n 以 n 输入停机，所以 $n\in K$. 矛盾，从而 $n\notin A$. 因此 $n\in \overline{K}\setminus A$.

16. 令 X 是递归可枚举的. 假设 X 由递归函数 f 枚举. 定义 g 通过

$$g(y)=\mu x[f(x)=y].$$

因为 f 是递归的，故 g 是递归偏函数，它的域是 X. 据 7.25，g 是图灵可计算的，所以存在域为 X 的图灵机.

17(e) $\{T_n$ 是否对每个输入数都停机? $|n\in D_N\}$. 考虑算法：令 m 固定. 给定 n，实施 T_m 输 m 入的计算；如果停机，给出输出 n. 这个算法首先可以翻译成一个图灵机的指令，其次可以转换为图灵机 $T_{k(m)}$ 的码数 $k(m)$. $T_{k(m)}$ 具有性质：如果 T_m 以 m 输入停机，那么 $T_{k(m)}$ 对每一个输入停机；如果 T_m 以 m 输入不停机，那么 $T_{k(m)}$ 对任何输入都不停机. 现在为了判定 T_m 以 m 输入是否停

机，我们只需去计算 $k(m)$，并回答问题：$T_{k(m)}$ 对每一个输入停机吗？因此提出的这一问题类的可解性将蕴涵 K 的递归性.

$(f)\{T_n$ 对某个输入数停机吗？$|n\in D_N\}$.

$T_{k(m)}$（在上面(e)中）或者对所有输入都不停机，或者对每个输入都停机，这要视 m 而定. 因此，如果我们能判定 $T_{k(m)}$ 是否对某个输入数停机，那么我们就能如(e)判定 K 的元素是什么.

(18) 判定 K_0 的成员的算法，显然将产生判定 K 的成员的一种算法，所以 K 可以化归为 K_0. 现在假设，对于 K 存在一种算法. 考虑算法：令 m, n 是固定的. 给定 p，遵循 T_m 以 m 作为输入的计算；如果它停机了，给出 p. 如在习题 17(e)中，这个算法产生了作为一个图灵机的指令组，因此也给出了这个机器的一个编码数 $k(m, n)$，$T_{k(m,n)}$ 对每一个输入都停机还是对每个输入都不停机，依赖于 T_m 以 m 作为输入时是停机还是不停机. 因此，为了判定(m, n)是否属于 K_0，我们只需计算 $k(m, n)$，并且回答以下问题：$T_{k(m,n)}$ 以 $k(m, n)$作为输入时是否停机？也就是说：$k(m, n)$ 是否属于 K？

19(a) 任何给定的字，可以容易地证明等价于下列标准形式之一中的一个字：

$$a_1a_2^{k_1}a_1a_2^{k_2}a_1\cdots a_1a_{12}^{k_n}a_1 \quad (n\geqslant 1),$$
$$a_1^{k_1}a_1a_1^{k_2}a_1\cdots a_1a_2^{k_n}a_1 \quad (n\geqslant 0),$$
$$a_2^{k_1}a_1a_2^{k_2}a_1\cdots a_1a_2^{k_n} \quad (n\geqslant 1).$$

标准形式的两个字是等价的，当且仅当它们相等，所以两个给定的字等价，当且仅当它们可以如上化归为同一标准形式.

(b) 注意 $\quad a_3a_3\sim a_1a_2a_2\sim a_1a_2\sim a_3$.

任一给定的字，可以证明等价于下列形式的一个字

$$a_1^{k_1}a_3^{k_2}a_1^{k_3}\cdots a_1^{k_{n-1}}a_3^{k_n},$$

其中 a_2 的所有出现都已被"吸收".

20. G 是一个阿贝尔群，符号 a_1^{-1}, a_2^{-1}, a_3^{-1} 和其它符号以及

它们之间的可交换性是一种关于乘法的练习．例如：

$$e\sim a_2^{-1}a_1^{-1}a_1a_2\Rightarrow e\sim a_2^{-1}a_1^{-1}a_2a_1$$

$$\Rightarrow ea_1^{-1}\sim a_2^{-1}a_1^{-1}a_2a_1a_1^{-1}\sim a_2^{-1}a_1^{-1}a_2\Rightarrow a_1^{-1}a_2^{-1}\sim a_2^{-1}a_1^{-1}$$

和 $a_1a_2^{-1}a_1^{-1}a_2\sim a_1a_1^{-1}a_2^{-1}a_2\sim e$

因而有 $a_1a_2^{-1}a_1^{-1}a_2a_2^{-1}\sim a_2^{-1}$

和 $a_1a_2^{-1}a_1^{-1}a_1\sim a_2^{-1}a_1$

即 $a_1a_2^{-1}\sim a_2^{-1}a_1$

任一给定字都可化归为标准形式 $a_1^{r_1}a_2^{r_2}a_3^{r_3}$，其中 $r_1, r_2, r_3\in z$．两个给定的字等价，当且仅当它们的标准形式相同．

22．恰如图灵机可以用一个等价的，只使用两个纸带符号的机器替代一样(注记7.22)，所以，我们也能仅用两个符号去构造本质上相同的定理 7.37 中的半群 $\mathscr{S}$．$\mathscr{S}$ 的符号可用一进行编码，开始时用 0 作为一个标记．例如．q_0 是 01，q_4 是 011111 和字 $q_0q_4q_1$ 将是 01011111011．

24(a) $\{n\in D_N: n$ 是 $\sim\mathscr{A}$ 的哥德尔数，其中 $\mathscr{A}$ 是 $\mathscr{N}$ 的一条定理$\}$不是递归的．给定 $n\in D_N$，查出它是否 $\mathscr{N}$ 中公式 $\mathscr{A}$ 的哥德尔数．如果它是的，计算$(\sim\mathscr{A})$的哥德尔数(这可以有效地作到，参见 6.4 节)．如果这给定的集是递归的，那么 $\mathscr{N}$ 的定理的哥德尔数集是递归的．

(b) $\{n\in D_N: n$ 是 $\mathscr{A}$ 的哥德尔数，其中 $\mathscr{A}$ 在 $\mathscr{N}$ 中真$\}$不是递归的(第 6 章)．$\mathscr{A}$ 在 $\mathscr{N}$ 中真，当且仅当$(\sim\mathscr{A})$假．因此给定的集的递归性将会产生一个矛盾．

26．如果 $\mathscr{V}$ 在 N 中真，那么对某个 $s\in D_N$，$F(p, s)$成立，所以 $f(s)$对某个 s 来说，是$(\exists x_2)\mathscr{F}(0^{(p)}, x_2)$的哥德尔数，所以 $\mathscr{V}$ 在 N 中假．$\mathscr{V}$ 是闭的，所以在 N 中必定假．如果 $q=f(k)$(q 是 $\mathscr{V}$ 的哥德尔数)，那么 $f(k)$是$(\exists x_2)\mathscr{F}(0^{(p)}, x_2)$的哥德尔数，所以 $F(p, k)$成立．因此 $\vdash_{\mathscr{N}}\mathscr{F}(0^{(p)}, 0^{(k)})$，从而 $\vdash_{\mathscr{N}}(\exists x_2)F(0^{(p)}, x_2)$，即

$\underset{\mathscr{N}}{\vdash}\mathscr{V}$，所以 $\mathscr{V}$ 在 N 中真．矛盾，所以 q 不在 f 的值域中．

27．如果 T 的公理（的哥德尔数）的集是递归的，那么 T 的定理（的哥德尔数）的集是递归可枚举的（注记 7.6）．系统 S 和 T 有相同的定理集．如果 S 是完全的，并且它的定理（的哥德尔数）的集是递归可枚举的，那么，给定任意的 $n\in D_N$，如果它是 S 的一个公式 $\mathscr{A}$ 的哥德尔数，那么枚举所有 S 的定理（的哥德尔数）．我们将最终查出或者 $\mathscr{A}$、或者 $\sim\mathscr{A}$ 是 S 的定理．因此 S 是递归可判定的．

参 考 书 目

COHEN, P., J, *Set Theory and the Continuum Hypothesis*, Addison-Wesley, 1966.

COPI, I. M, *Introduction to Logic*, Macmillan, 1961.

DAVIS, M(1), *Hilbert's tenth problem is unsolvable, American Mathematical Monthly*, Vol. 80(1973) p. 233.

DAVIS, M(2), *Computability and Unsolvability*, McGraw-Hill, 1958.

HALMOS, P. R, *Naive Set Theory*, Van Nostrand, 1960.

HILBERT, D, *Mathematical problems, Bulletin of the American Mathematical Society*, Vol 8(1901-2)p. 437.

KLEENE, S. C, *Introduction to Matamathematics*, Van Nostrand, 1952.

MENDELSON, E, *Introduction to Mathematical Logic*, Van Nostrand, 1964.

MINSKY, M, *Computation: Finite and Infinite Machines*, Prentice-Hall, 1967.

ROBINSON, A, *Introduction to Model Theory and to the Matamathematics of Algebra*, North-Holland, 1965.

ROGERS, H., *Introduction to the Theory of Recursive Functions and Effective Computability*, McGraw-Hill, 1967.

SHOENFIELD, J. R, *Mathematical Logic*, Addison-Wesley, 1967.

TARSKI, A, MOSTOWSKI, A, AND ROBINSON, R. M, *Undecidable Theories*, North-Holland, 1953.

VAN HEIJENOORT, J, *From Frege to Gödd: A Source Book in Mathematical Logic* 1879~1931, Harvard University Press, 1967

符 号 表

符号分类如下：英语字母，希腊字母，数学符号，逻辑符号.

a_i	个 体常元
$\bar{a}_i$	个体常元的解释
$A, B, C, \cdots$	命题字母
A_i^n	谓词字母
$\bar{A}_i^n$	谓词字母的解释
$\hat{A}_i^n$	谓词字母的解释
$\mathscr{A}, \mathscr{B}, \mathscr{C}, \cdots$	命题形式
$\mathscr{A}, \mathscr{B}, \mathscr{C}, \cdots$	合式公式
$\mathscr{A}'$	$\mathscr{A}$ 的全称闭式
(AC)	选择公理
B	图灵机纸带符号(空白)
C_R	特征函数
(CH)	连续统假设
D_I	解释 I 的域
$D(m, n)$	D_n 上的关系
D_N	自然数集
$\mathscr{D}(x_1, x_2)$	$\mathscr{N}$ 中的合式公式
$(E7), (E8), (E9)$	公理
$(E7'), (E8'), (E9')$	公理
f_i^n	函数字母
$\bar{f}_i^n$	函数字母的解释
$\hat{f}_i^n$	函数字母的解释
F	真值假

$\mathscr{F}$	一阶域论的系统
$\mathscr{F}_k(x_{i_k})$	$\mathscr{L}$ 的公式
$\mathscr{G}$	一阶群论的系统
$\mathscr{G}_k$	$\mathscr{L}$ 的公式
$(G1)$, $(G2)$, $(G3)$	公理
HS	推演规则
I	解释
J	L 的一致完全扩充
K	一阶谓词演算系统
K	与图灵机表相联的集
$K_{\mathscr{L}}$	一阶谓词演算系统
$(K1)$, $\cdots$, $(K6)$	公理
$K_{\mathscr{L}_N}$	带算术语言的一阶谓词演算系统
L	命题演算系统
L	图灵机纸带符号(左移)
$(L1)$, $(L2)$, $(L3)$	公理
$\mathscr{L}$	一阶语言
$\mathscr{L}_G$	一阶群论的语言
$\mathscr{L}_N$	一阶算术的语言
MP	推演规则
N	算术的解释
$(N1)$, $\cdots$, $(N7)$	公理
$(N1^*)$, $\cdots$, $(N7^*)$	公理
$\mathscr{N}$	一阶算术系统
$p_1, p_2, p_3, \cdots$	L 的符号
$p, q, r, \cdots$	命题变元
p_i	第 i 个奇素数
p_i^j	射影函数

Pf	D_N 上的关系
P_{rem}	D_N 上的关系
P_{rem_2}	D_N 上的关系
$\mathscr{P}(x_1, x_2)$	$\mathscr{N}$ 的公式
$q_0, q_1, q_2, \cdots$	图灵机的内状态
Q_j	任意量词
Q_j^*	任意量词
Q_{ij}	命题变元或它的否定
rm_2	用 2 除后余项
R	图灵机纸带符号(右移)
$R, S, \cdots$	D_N 上的任意关系
$\bar{R}$	R 的补
s	后继函数
sg	D_N 上的函数
$\overline{sg}$	D_N 上的函数
S_A	在 A 上的一切字的集
S_A^*	字的等价类的集
$S(\mathrm{I})$	模型 I 的一阶系统
$\mathscr{S}$	一阶半群论系统
T	真值真
T	K 的一致完全扩充
$T_0, T_1, T_2, \cdots$	图灵机的枚举
$T(n)$	D_N 上的关系
$\mathscr{T}(x_1)$	$\mathscr{N}$ 的公式
$\mathscr{U}$	$\mathscr{N}$ 的公式
$v(\mathscr{A})$	公式 $\mathscr{A}$ 的真值
$v(x_i)$	变元 x_i 的赋值
$v(t)$	项 t 的赋值

封面页
书名页
版权页
前言
目录
正文