数理逻辑

讲义，第 6.3 版，2024 年

北京大学 信息与计算科学系

林作铨

linzuoquan@pku.edu.cn

6 不完全性定理

- Gödel 证明
- 可表达性
- 递归论
- Gödel 数
- 不完全性证明

Gödel 证明

回顾

完全性：$\forall \mathscr{A}$，$\models \mathscr{A} \Rightarrow \vdash \mathscr{A}$

不完全性：$\exists \mathscr{A}$，$\models \mathscr{A} \not\Rightarrow \vdash \mathscr{A}$（亦即 $\nvdash \mathscr{A}$ 且 $\nvdash \sim A$）

问题

一阶算术系统（形式数论）$\mathscr{N}$ 是否有完全性？

- 算术的标准模型不可用（基于朴素集论，而形式集论尚未知一致性）
- 朴素算术 N 作为模型
- 算术不完全性：$\exists \mathscr{A}$，$\models_N \mathscr{A} \not\Rightarrow \vdash_{\mathscr{N}} \mathscr{A}$
- 难题：$\models_N \mathscr{A}$ 如何表示？因 N 是直观的，不是规范模型

Gödel（1931）给出了 $\mathscr{N}$ 不完全性定理（简称 Gödel 定理）的证明（Gödel 证明）

Gödel 证明的思路

存在 $\mathscr{N}$ 的闭式 $\mathscr{U}$，$\mathscr{U}$ 是算术真理（在 N 中为真），但 $\mathscr{U}$ 和 $\sim\mathscr{U}$ 都不是 $\mathscr{N}$ 的定理

构造一个不可判定公式 $\Leftarrow$ 不完全性

通过显式地描述 $\mathscr{U}$，若 $\mathscr{U}$ 或 $\sim\mathscr{U}$ 都是 $\mathscr{N}$ 的定理，则导致矛盾

找出一个悖论 $\Leftarrow$ 反证

悖论 6.1 (Richard 悖论（1905）)

自然语言（汉语或法语等）的一些语句可以表示实数，如“一个圆的圆周与直径之比”就表示实数 π

把这些语句以汉语拼音（或笔划）按拼音字母（或笔划数）顺序排列，如按照语句中字母（或笔划数）的多少排列，少的在前，多的在后，相同的按字母（或笔划）先后顺序，这样就把能用语句表示的实数排成一个序列

$$r_1, r_2, \cdots, r_n, r_{n+1}, \cdots$$

可得所有能用有穷多字（字母）定义的实数，它们构成一个能枚举集 E

现用下面一个规则把这个序列改变一下生成一个实数（Cantor 对角法）

“设 E 中第 n 个数的第 n 位为 p，生成一个实数如下：

其整数部分为 0

若 p 是 8 或 9，则其第 n 位小数变成 1

若 p 不是 8 或 9，则其第 n 位小数为 $p+1$”

这个实数显然不属于 E，因它与 E 中每个数都不同；但这个数却可由上述有穷多个字组成的语句来定义，故应属于 E $\Rightarrow$ 矛盾

算术编码

任一种（自然）语言用来表达整数（算术），总是有些涉及算术性质的词汇是无法明确定义的（“一个整数为另两个整数之和”），这些词汇作为原始词汇（相当于公理），用有穷个字（母）的一些语句可定义整数，每个定义对应唯一的整数，把具有最少字（母）数的定义对应于 1，下一个定义对应于 2，依次类推，获得一个（自然数）序列

Richard-性质

每个定义都与唯一的整数相联系，整数作为定义表达句的编码

这个整数本身（不）具有与它对应的定义所指定的性质

例："不能被 1 和其自身以外的其它整数整除"——恰好对应于顺序号 17（17 个汉字），17 本身就具有表达句所定义的性质（自谓）

"某一个整数与这一整数自身的乘积"——对应于顺序号 15，15 本身不具有表达句所定义的性质（非自谓）

称这种不具有 与它对应的定义所指定的性质为 Richard-性质

Richard-数

x 是 Richard-数：x 本身不具有 与它在序列中对应的定义表达句所指定的性质

Richard 悖论（算术版）

具有 Richard-性质（这个定义表达句）

$\Rightarrow$ 用文字描述了整数的（这个）算术性质

$\Rightarrow$ 对应于序列中一个固定的位置（数），设此（位置）数为 n

n 是 Richard-数

$\Longleftrightarrow$ n 不具有与 n 对应的定义表达句所指定的性质

（非 Richard-性质）

n 没有作为 Richard-数之性质

$\Longleftrightarrow$ n 不是 Richard-数

注

- Richard 悖论的自指：

  ——对象级：对整数的纯算术性质的定义

  ——元级：描述算术性质时所用的语言的性质的定义

  $\Rightarrow$ Richard-数的定义指涉定义表达句的语言（汉语）中字（符号）的数目等元数学概念

  消除 Richard-悖论需明确把对象级和元级分割开（如类型论）

- Richard 悖论表明：把有关一个足够广泛的形式系统的元数学命题映射到这个系统本身是可能

  $\Leftarrow$ 用整数对定义表达句进行编码

  $\Rightarrow$ 在一个形式系统内部可重新构建 Richard-悖论，避免自然语言的不精确，这时看悖论是否可避免？

- Gödel 证明受到 Richard 悖论的启发

证明步骤

(Gödel 配数) $\Rightarrow$ 对每个公式和公式序列进行编码，使得公式或公式序列可由它们的编码（自然数）来表达

$\Rightarrow$ 关于（自然）数的句子可看成关于 $\mathscr{N}$ 中表达式的编码的句子

关于 $\mathscr{N}$ 中表达式的句子 $\Leftarrow$ (可表达性)

(递归论) $\Rightarrow$ 为刻画可表达性，引入递归函数 $\Rightarrow$ 递归关系

$\Rightarrow$ 一个关系在 $\mathscr{N}$ 中是可表达的，若它是递归的

(不可证性) $\Leftarrow$ 构造一种自指的句子来刻画其自身的不可证性 (unprovability)

(ω-一致性) $\Rightarrow$ 假设 $\mathscr{U}$ 是 $\mathscr{N}$ 的定理会导致矛盾

$\Rightarrow$ 对假设 $\sim\mathscr{U}$ 是 $\mathscr{N}$ 的定理会导致矛盾的情形，需要一个更强的一致性概念（技术性）

- Gödel 证明
- 可表达性
- 递归论
- Gödel 数
- 不完全性证明

可表达性

回顾

$\mathscr{L}_N$ 是一阶（算术）语言，$\mathscr{N}$ 是一阶算术，N 是（算术）模型（如朴素算术），其论域 D_N 是自然数

记号

$0^{(n)}$ 是 0 后面 n 个 $'$ 的缩写，数 $n \in D_N$ 是项 $0^{(n)}$ 在 N 中的解释

$0^{(0)}$ 代表 $\mathscr{N}$ 的常项 0

数字项

用 $0^{(n)}$ 代表 $\mathscr{N}$ 的项，但符号 n 本身不是 $\mathscr{L}_N$ 的符号，出现在 $0^{(n)}$ 中的 n 不能用变元代入

$0^{(n)}$ 为数字项（常项）

命题 6.2

令 $m, n \in D_N$

(i) 若 $m \neq n$，则 $\vdash_{\mathscr{N}} \sim(0^{(m)} = 0^{(n)})$

(ii) 若 $m = n$，则 $\vdash_{\mathscr{N}} (0^{(m)} = 0^{(n)}$ ♢

证

(i) 命题 5.27

(ii) 设 $m = n$，则 $0^{(m)}$ 和 $0^{(n)}$ 相等（即 $\mathscr{N}$ 中相同的项）

$\vdash_{\mathscr{N}} (0^{(m)} = 0^{(n)})$ 是 (E6) 的实例 □

$\mathscr{N}$ 的项集包含了一个序列 $0, 0^{(1)}, 0^{(2)}, \cdots$，它们在 N 中用自然数序列 $0, 1, 2, \cdots$ 解释，而 $\mathscr{N}$ 的公式可包含这些项，于是含这些项的 $\mathscr{N}$ 的定理在 N 中解释作算术真理

问题

如何刻画算术真理和 $\mathscr{N}$ 的定理之间的对应关系

命题 6.2 给出的这种对应关系（相等）还不够，但可导出一般的可表达性概念

例 6.3

考虑 D_N 上的关系 $\leq$

$m \leq n$ 是公式 $(\exists x_1)(0^{(m)} + x_1 = 0^{(n)})$ 的解释

在这意义下 $\leq$ 是“可表达”的

在更强意义下，$\leq$ 也是可以表达的，因

若 $m \leq n$，则

$$\vdash_{\mathscr{N}} (\exists x_1)(0^{(m)} + x_1 = 0^{(n)})$$

若 $\sim m \leq n$，则

$$\vdash_{\mathscr{N}} \sim (\exists x_1)(0^{(m)} + x_1 = 0^{(n)})$$

换言之，D_N 中两个自然数的关系是否成立可表达为一个特殊的公式，它或它的否定是 $\mathscr{N}$ 中的定理

定义 6.4 (可表达性)

一个自然数上的 k 元关系 R 在 $\mathscr{N}$ 中是可表达的 (expressible)，若存在具 k 个自由变元的公式 $\mathscr{A}(x_1, \cdots, x_n)$ 使对任意 $n_1, \cdots, n_k$，有

(i) 若 $R(n_1, \cdots, n_k)$ 在 N 中成立，则 $\vdash_{\mathscr{N}} \mathscr{A}(0^{(n_1)}, \ldots, 0^{(n_k)})$

(ii) 若 $R(n_1, \cdots, n_k)$ 在 N 中不成立，则 $\vdash_{\mathscr{N}} \sim \mathscr{A}(0^{(n_1)}, \ldots, 0^{(n_k)})$

$\diamondsuit$

注

(a) 命题 6.2 表明，N 中相等关系在 $\mathscr{N}$ 中是可表达的

(b) 若 $\mathscr{N}$ 是完全的，定义 6.4 中 (i) 和 (ii) 可合并成“当且仅当”，因 $\mathscr{A}(0^{(n_1)}, \cdots 0^{(n_k)})$ 或 $\sim\mathscr{A}(0^{(n_1)}, \cdots, 0^{(n_k)})$ 是 $\mathscr{N}$ 的定理

但对某个公式 $\mathscr{A}$ 和数 $n_1, \cdots, n_k$，

$\mathscr{A}(0^{(n_1)}, \cdots 0^{(n_k)})$ 和 $\sim\mathscr{A}(0^{(n_1)}, \cdots, 0^{(n_k)})$ 可能都不是 $\mathscr{N}$ 的定理，

定义 6.4 的两个分立条件是需要的

(c) (b) 表明，并非 $\mathscr{N}$ 中每个含自由变元的公式用这种方法都能“表达”一个关系，虽然每个这样的公式确实被解释为 N 中的一个关系

注 (续)

(d) 自然数集可看作一元关系。若 A 是 D_N 的子集，则 “$\in A$” 是 D_N 上的一元关系，它可能是也可能不是在 $\mathscr{N}$ 中可表达的

例 6.5

设 A 是偶数集，则 “$\in A$” 是公式

$$\exists x_2(x_2 \times 0^{(2)} = x_1)$$

的解释

对每一 $m \in D_N$,

$\exists x_2(x_2 \times 0^{(2)} = 0^{(m)})$ 或 $\sim\exists x_2(x_2 \times 0^{(2)} = 0^{(m)})$ 是 $\mathscr{N}$ 中的定理，

故 A 是 $\mathscr{N}$ 中可表达的

注 (续)

(e) 函数是一种特殊的关系

D_N 上的 $(k+1)$ 元关系 R 看成一个函数

若对每个 $n_1, \cdots, n_k \in D_N$, 只存在一个 $n_{k+1} \in D_N$，使得 $R(n_1, \cdots, n_k, n_{k+1})$ 成立

考虑一个函数（作为关系）是否在 $\mathscr{N}$ 中可表达，与所涉及的 $\mathscr{N}$ 的公式是否具有这样的单值性有关

定义 6.6

D_N 上的 k 元函数（即 $D_N^k \to D_N$ 的函数）在 $\mathscr{N}$ 中是可表示的（representable），若它（作为 $k+1$ 元关系）可被有 $k+1$ 个自由变元的公式 $\mathscr{A}$ 在 $\mathscr{N}$ 中表达，使对任意 $n_1, \cdots, n_k$, 有

$$\vdash_{\mathscr{N}} (\exists_1 x_{k+1}) \mathscr{A}(0^{(n_1)}, \cdots, 0^{(n_k)}, x_{k+1})$$

$\diamondsuit$

例 6.7

由 $f(m,n)=m+n$ 给出的函数 $f\colon D_N^2\to D_N$，设 $\mathscr{A}(x_1,x_2,x_3)$ 是公式 $x_3=x_1+x_2$，对任意 $m,n,p\in D_N$，证明

(i) 若 $p=m+n$，则

$$\vdash_{\mathscr{N}}(0^{(p)}=0^{(m)}+0^{(n)})$$

(ii) 若 $p\neq m+n$，则

$$\vdash_{\mathscr{N}}\sim(0^{(p)}=0^{(m)}+0^{(n)})$$

(iii) $\vdash_{\mathscr{N}}(\exists_1 x_3)(x_3=0^{(m)}+0^{(n)})$

证

设 $m, n \in D_N$，则

$$\vdash_{\mathscr{N}} (0^{(m)} + 0^{(n)} = 0^{(m+n)})$$

若 $n = 0$，这正是 (N3*)
若 $n > 0$，记 $0^{(n)}$ 为 $(0^{(n\text{-}1)})'$，由 (N4*) 有

$$\vdash_{\mathscr{N}} (0^{(m)} + 0^{(n)}) = (0^{(m)} + 0^{(n\text{-}1)})'$$

重复上面过程，得

$$\vdash_{\mathscr{N}} (0^{(m)} + 0^{(n)}) = (0^{(m)} + 0)\overbrace{'\cdots'}^{n}$$

即有

$$\vdash_{\mathscr{N}} (0^{(m)} + 0^{(n)}) = (0\overbrace{'\cdots'}^{m})\overbrace{'\cdots'}^{n}$$

亦即

$$\vdash_{\mathscr{N}} 0^{(m)} + 0^{(n)} = 0^{(m+n)}$$

证 (续)

由此，(i) 和 (ii) 据 命题 6.2 可得

对 (iii)，需证

$$\vdash_{\mathscr{N}} (\exists x_3)(x_3 = 0^{(m)} + 0^{(n)} \wedge (\forall x_i)(x_i = 0^{(m)} + 0^{(n)} \to x_i = x_3))$$

可证

$$\vdash_{\mathscr{N}} 0^{(m+n)} = 0^{(m)} + 0^{(n)} \wedge (\forall x_i)(x_i = 0^{(m)} + 0^{(n)} \to x_i = 0^{(m+n)})$$

即得 □

例 6.8

由 $f(m) = 2m$ 给出的函数 $f\colon D_N \to D_N$ 在 $\mathscr{N}$ 中是可表示的

设 $\mathscr{A}(x_1, x_2)$ 是公式 $x_2 = x_1 \times 0^{(2)}$，对任意 $m, n \in D_N$，需证

(i) 若 $n = 2m$，则 $\vdash_{\mathscr{N}} 0^{(n)} = 0^{(m)} \times 0^{(2)}$

(ii) 若 $n \neq 2m$，则 $\vdash_{\mathscr{N}} \sim 0^{(n)} = 0^{(m)} \times 0^{(2)}$

(iii) $\vdash_{\mathscr{N}} \exists_1 x_2 (x_2 = 0^{(m)} \times 0^{(2)})$

例 (续)

(i) 设 $n = 2m$, $0^{(n)} = 0^{(m)} \times 0^{(2)}$ 在 $\mathscr{N}$ 中一个证明如下

$$
\begin{aligned}
0^{(m)} \times 0^{(2)} &= 0^{(m)} \times 0'' && \text{记号} \\
&= (0^{(m)} \times 0') + 0^{(m)} && (\mathrm{N6}^*) \\
&= (0^{(m)} \times 0 + 0^{(m)}) + 0^{(m)} && (\mathrm{N6}^*) \\
&= (0 + 0^{(m)}) + 0^{(m)} && (\mathrm{N5}^*) \\
&= 0^{(m)} + 0^{(m)} && (\mathrm{N3}^*) \\
&= 0^{(m+m)} && \text{由前例} \\
&= 0^{(2m)} \\
&= 0^{(n)}
\end{aligned}
$$

例 (续)

(ii) 设 $n \neq 2m$，据 命题 6.2，$\vdash_{\mathscr{N}} \sim(0^{(2m)} = 0^{(n)})$，由 (i) 得

$$\vdash_{\mathscr{N}} 0^{(2m)} = 0^{(m)} \times 0^{(2)}$$

由 $(\mathrm{E}9')$，有

$$\vdash_{\mathscr{N}} \sim 0^{(n)} = 0^{(m)} \times 0^{(2)}$$

(iii) 证法从前

例 6.9

对任意 $m, n \in D_N$，由 $Z(m, n) = 0$ 定义的二元函数 Z 在 $\mathscr{N}$ 中是可表示的

问题

是否存在一个不可表示的函数

注

已知 D_N 上的一个函数，要验证它是可表示的，可能很困难，而要验证它是不可表示的，则可能更困难

定义 6.10

设 R 是 D_N 上的 k 元关系，R 的特征函数，记为 C_R，定义如下

- $C_R(n_1, \cdots, n_k) = 0$，若 $R(n_1, \cdots, n_k)$ 成立
- $C_R(n_1, \cdots, n_k) = 1$，若 $R(n_1, \cdots, n_k)$ 不成立 ♢

命题 6.11

令 S（如 $\mathscr{N}$）是 $\mathscr{L}_N$ 上一个带等词一阶理论且 $\vdash_S 0 \neq 0^{(1)}$，则一个关系 R 是可表达的，当且仅当 C_R 是可表示的

证

若 R 是可由

$$\mathscr{B}(x_1, \cdots, x_n)$$

表达，易证 C_R 可由

$$\left(\mathscr{B}\left(x_1, \ldots, x_n\right) \wedge y = 0\right) \vee \left(\neg \mathscr{B}\left(x_1, \ldots, x_n\right) \wedge y = 0^{(1)}\right)$$

表示

反之，若 C_R 可由 $\mathscr{B}(x_1, \cdots, x_n, y)$ 表示，用假设 $\vdash_S 0 \neq 0^{(1)}$，易证 R 可由 $\mathscr{B}(x_1, \ldots, x_n, 0)$ 表达 □

命题 6.12

并非 D_N 上的所有函数在 $\mathscr{N}$ 中都是可表示的 ♢

证

据一阶算术，$\mathscr{N}$ 中的公式集是能枚举的，因此，$\mathscr{N}$ 中可表示的函数集是能枚举的。但存在不能枚举个 D_N 上 的函数，因此，存在着 $\mathscr{N}$ 中不可表示的 D_N 上的函数 □

推论 6.13

并非 D_N 上所有的关系在 $\mathscr{N}$ 中是可表达的 ♢

问题

用什么方法刻画一个 D_N 上函数（关系）在 $\mathscr{N}$ 中是可表示（达）的

这是 Gödel 发明的关键技术

命题 6.14

D_N 上函数（关系）在 $\mathscr{N}$ 中是可表示（达）的，当且仅当 它是递归的 $\diamondsuit$

- Gödel 证明
- 可表达性
- 递归论
- Gödel 数
- 不完全性证明

递归论

递归

- 递归（recursion）是一种嵌套，如：故事里的故事，电影中的电影，画中的画，俄式洋娃娃中的俄式洋娃娃，括号说明中的括号说明，“梦中梦”，“镜中镜” $\Leftarrow$ 普遍概念
- 递归不会导致悖论，不会导致无穷回归（循环定义），正确的递归定义不以某一事物自身来定义这一事物，总是用比其自身简单一些的说法来定义这个事物
- 程序设计语言中若没有递归将无法写代码（如堆栈，递归调用，模块性，过程等，但如量子程序没有一般的递归）

定义 6.15 (递归函数)

递归函数类是用以下方式定义的（不依赖于系统 $\mathscr{N}$）

某些容易定义的函数是递归的

从这些（基本）函数出发应用三条规则而得的所有函数也是递归的

注

类似公理系统，可看成一种新的公理系统技术

基本递归函数

1. 零函数 z　$D_N \to D_N$，对每一 $n \in D_N$，由 $z(n) = 0$ 给出
2. 后继函数 s　$D_N \to D_N$，对每一 $n \in D_N$，由 $s(n) = n + 1$ 给出
3. 投影函数 p_i^k　$D_N^k \to D_N$，对每一 $n_1, \cdots, n_k \in D_N$，
   由 $p_i^k(n_1, \cdots, n_k) = n_i$ 给出
   p_1^1 是恒等函数

定义规则

I 合成　若 $g: D_N^j \to D_N$，且对 $1 \le i \le j$，$h_i: D_N^k \to D_N$，则由

$$f(n_1, \cdots, n_k) = g(h_1(n_1, \cdots, n_k), \cdots, h_j(n_1, \cdots, n_k))$$

所定义的 $f: D_N^k \to D_N$ 是从 g 和 $h_1, \cdots, h_j$ 合成的函数

II 递归　若 $g: D_N^k \to D_N$ 和 $h: D_N^{k+2} \to D_N$，则由

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

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 $f: D_N^{k+1} \to D_N$ 是从 g 和 h 由递归得到的函数

注

这里 $n_1, \cdots, n_k$ 是不影响定义的参数

注

特别地，由

$f(0) = a$ （D_N 的固定元）和

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

定义的函数是由递归所得

例 6.16

(1) Fibonacci 数列

$f(n) = f(n-1) + f(n-2), n \geq 2$ （定义递归）

$f(1) = f(2) = 1$ （递归基底）

若递归基底设为 3，则产生 Lucas 数列

(2) 算术和（积）

$x + 0 = x$

$x + s(y) = s(x + y)$

定义规则（续）

III 最小数算子　令 $g: D_N^{k+1} \to D_N$ 是任意函数，它具有这样的性质，对每一 $n_1, \cdots, n_k \in D_N$，至少存在一个 $n \in D_N$，使得 $g(n_1, \cdots, n_k, n) = 0$。由

$$f(n_1, \cdots, n_k) = \min\{n \in D_N | g(n_1, \cdots, n_k, n) = 0\}$$

定义的 $f: D_N^k \to D_N$ 是从 g 由最小数算子得到的函数 ♢

记号

使 $g(n_1, \cdots, n_k, n) = 0$ 的最小数 n 用 $\mu n[g(n_1, \cdots, n_k, n) = 0]$ 表示

注

对最小数算子规则，为保证函数 f 为全函数，即对自然数的每个 k 元组有值，函数 g 要求对任意 $n_1, \cdots, n_k$ 至少有一个 n 使

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

有时允许使用没有这个条件的最小数算子，即偏函数的概念

现只讨论全函数

例 6.17

(a) 由 $f(m,n)=m+mn$ 给出的 $f\colon D_N^2\to D_N$ 是由加、乘和射影函数用合成得到的（这里 f_1 代表加， f_2 代表乘）

$$f(m,n)=f_1(p_1^2(m,n),f_2(m,n))$$

(b) 由 $g(m,n,p)=n^2$ 给出的函数 $g\colon D_N^3\to D_N$ 是如下合成得到的

$$g(m,n,p)=f_2(p_2^3(m,n,p),p_2^3(m,n,p))$$

这里 f_2 代表乘

例 (续)

(c) 加函数是从 p_1^1，以及 s 与 p_3^3 的合成用递归得到的

$$f_1(m,0) = p_1^1(m)$$

$$f_1(m,n+1) = s(p_3^3(m,n,f_1(m,n)))$$

(d) 类似地，乘是从加函数用递归定义得到的

(e) 设 $f(n,p) = \min\{q | n+q \equiv 0 (\mathrm{mod}\ p)\} (n,p,q \in D_N)$，则 f 是从函数 g 用最小数算子得到的，这里

$$g(n,p,q) = (n+q) \text{ 被 } n \text{ 除所得的余数}$$

定义 6.18

一个 D_N 上的函数是递归的，若它由上述 1,2,3 型函数经有穷次使用规则 I,II,III 获得

递归函数类是 D_N 上包含所有的 1,2,3 型函数，以及对使用规则 I,II,III 封闭的最小函数类

一个函数是原始递归的（primitive recursive），若它由 1,2,3 型函数经有穷次使用规则 I,II 获得 ♢

注

原始递归函数类是一个比递归函数类更小的类

例 6.19

(a) 和函数是原始递归的

见 例 6.17 (c)，和函数是从投影函数和后继函数用递归规则定义的

(b) 常函数是递归的

如具值 k 的一元常函数可用投影函数 p_2^2 定义

$$f(0) = k, \qquad f(n+1) = p_2^2(n, f(n))$$

(c) 以下定义的函数 $sg, \overline{sg}: D_N \to D_N$ 是递归的

例 (续)

$$sg(n) = \begin{cases} 0, & n = 0 \\ 1, & n \neq 0 \end{cases} \qquad \overline{sg}(n) = \begin{cases} 1, & n = 0 \\ 0, & n \neq 0 \end{cases}$$

因

$$sg(0) = 0 \qquad sg(n+1) = 1 \qquad \overline{sg}(0) = 1 \qquad \overline{sg}(n+1) = 0$$

都是常函数

定义 6.20

D_N 上的关系是递归的，若它的特征函数是递归函数 ♢

例 6.21

二元递归关系 R，这里 $R(m, n)$ 成立当且仅当 $m + n$ 是偶数

例 6.22

关系 $\leq$ 是递归的

例 6.23

(a) 集 D_N 是递归的，因它的特征函数是零函数，而零函数是递归的

(b) $\emptyset$ 是递归的，因其特征函数是一个常函数

(c) 偶数集是递归的

若 R 和 S 是 k 元关系，补关系 $\overline{R}$ 对给定的 k 元关系成立 $\Longleftrightarrow$ R 对此 k 元组不成立

交关系 $R \wedge S$ 对给定的 k 元关系成立 $\Longleftrightarrow$ R 和 S 都成立

并关系 $R \vee S$ 对给定的 k 元关系成立 $\Longleftrightarrow$ R 或 S 成立

命题 6.24

若 R 和 S 是递归的 k 元关系，则关系 $\overline{R}$，$R \wedge S$，$R \vee S$ 都是递归的 $\diamondsuit$

证

由其特征函数易证 $\square$

推论 6.25

对任意递归集 A 和 B，$\overline{A}$，$A \cap B$，$A \cup B$ 都是递归集 $\Diamond$

证

据 命题 6.24，因集 A 和 B 的特征函数是关系 $\in A$ 和 $\in B$ 的特征函数 $\square$

由此可对各种特殊的函数、关系和集确定其递归性

但发现一个函数或关系是非递归的更为困难

命题 6.26

D_N 的每一单元素子集是递归的 ♢

证

由特征函数对 D_N 做归纳 □

例 6.27

(a) 每一有穷集是递归的

据命题 6.26 和 推论 6.25，有穷集可作为单元素集的有穷并

(b) $p : D_N \to D_N$ 定义为

$p(n) =$ 第 n 个奇素数，若 $n > 0$

$p(0) = 2$

则 p 是递归的。注意到，p 没有简单的代数表达式

(c) 初等数论定理：每一自然数可唯一地表示作素数幂之积，对任意 $i \in D_N$，定义

$e_i(n) = n$ 的素数幂之积表达式中素数 $p(i)$ 的指数，若 $p(i)$ 在表达式中出现；否则为 0

则对每一 i，e_i 是一个递归函数

注

并非所有 D_N 上函数都是递归的（反例）

命题 6.14

从基本函数和递归规则可定义复杂的递归函数，由特殊的递归函数可定义其它递归函数，最终可证明 命题 6.14

- Gödel 证明
- 可表达性
- 递归论
- Gödel 数
- 不完全性证明

Gödel 数

Gödel 配数

Gödel 对一阶语言 $\mathscr{L}$ 给出一种编码，配给 $\mathscr{L}$ 中每一符号、项、公式和公式序列一个数，使得根据任意给定的数，能（机械能行）找出 $\mathscr{L}$ 中所对应的表达式

定义 6.28 (函数 g)

在 $\mathscr{L}_N$ 的符号集上定义

$$g(() = 3;$$

$$g()) = 5;$$

$$g(,) = 7;$$

$$g(\sim) = 9;$$

$$g(\rightarrow) = 11;$$

$$g(\forall) = 13;$$

$$g(x_k) = 7 + 8k;\ \ k = 1, 2, \cdots;$$

$$g(a_k) = 9 + 8k;\ \ k = 1, 2, \cdots;$$

$$g(f_k^n) = 11 + 8 \times (2^n \times 3^k)\ n = 1, 2, \cdots; k = 1, 2, \cdots;$$

$$g(A_k^n) = 13 + 8 \times (2^n \times 3^k)\ n = 1, 2, \cdots; k = 1, 2, \cdots;$$

注

每个符号都被指派为一个不同的奇正整数，这样，对任意给定的奇正整数（若它对应某个符号）都能找出它对应的符号

例 6.29

(a) 对应于数 587 的符号（若有）

$$587 = 8 \times 73 + 3 = 8 \times 72 + 11$$

而 $72 = 2^3 \times 3^2$，因此 587 对应于函数符 $\hat{f}_2^3$

(b) 333 不对应 $\mathscr{L}$ 的任何符号

$$333 = 8 \times 41 + 5 = 8 \times 40 + 13$$

但 $40 = 2^3 \times 5$，这不是 $2^n \times 3^k$ 的形式，333 不对应于 $\mathscr{L}$ 中任何符号

$\mathscr{L}_N$ 中的表达式（项或公式）是 $\mathscr{L}_N$ 的（符号）串

定义 6.30 (串配数)

若 $u_0, \cdots, u_k$ 是 $\mathscr{L}_N$ 的符号，用 $u_0 u_1 \cdots u_k$ 表示串（可能是也可能不是 $\mathscr{L}_N$ 的项或公式），定义

$$g(u_0 u_1 \cdots u_k) = 2^{g(u_0)} 3^{g(u_1)} \cdots p_k^{g(u_k)}$$

这里，对每一 $i > 0$, p_i 表示第 i 个 奇素数，且 $p_0 = 2$

注

- 因每个数可以唯一地表示成素数幂之积，就有一个确定的方法求出对应于给定数的串
- 不同的串必然对应不同的数
- 命题 3.25 据此证明了一阶表达式（项、公式）是能枚举的

例 6.31

(1) $g(f_1^1(x_1)) = 2^{g(f_1^1)} \times 3^{g(()} \times 5^{g(x_1)} \times 7^{g())}$

$= 2^{59} \times 3^3 \times 5^{15} \times 7^5$

(2) $g((A_1^2(x_1, x_2) \to A_1^1(x_1)))$

$= 2^{g(()} \times 3^{g(A_1^2)} \times 5^{g(()} \times 7^{g(x_1)} \times 11^{g(,)} \times 13^{g(x_2)} \times 17^{g())}$

$\times 19^{g(\to)} \times 23^{g(A_1^1)} \times 29^{g(()} \times 31^{g(x_1)} \times 37^{g())} \times 41^{g())}$

$= 2^3 \times 3^{109} \times 5^3 \times 7^{15} \times 11^7 \times 13^{23} \times 17^5$

$\times 19^{11} \times 23^{61} \times 29^3 \times 31^{15} \times 37^5 \times 41^5$

(3) 任何数，若在其素数幂的展开式中有一个素数的幂是偶数，或在整个展开式中的素数序列中素数的出现是跳跃的，则这个数不对应于任何串

注

符号的数码是奇数

串的数码是偶数（因在串的数码中素数 2 总是以非 0 指数出现）

定义 6.32 (串的有穷序列配数)

令 $s_0, s_1, \cdots, s_r$ 都是 $\mathscr{L}_N$ 的串，定义

$$g(s_0, s_1, \cdots, s_r) = 2^{g(s_0)} 3^{g(s_1)} \cdots p_r^{g(s_r)}$$

注

一个给定的数不可能既是一个串序列的编码同时又是个别串的编码，因在序列的编码中 2 的指数是偶数，而在串的数码中 2 的指数是奇数（上注）

对 $\mathscr{L}_N$ 中的符号、串和串的有穷序列定义了函数 g

定义 6.33 (Gödel 数)

- g 在 D_N 中取值
- g 是单射的，但不是满射的
- g 是以这样的方式定义的：对 g 的值域中的任意数，存在一个能行的方法计算 g^{-1} （即用素数幂之积的表达式）

g 的值称为 Gödel 数 ♢

$\mathscr{L}_N$ 的每个项、公式、公式序列都有一一对应的 Gödel 数

算术化

一个理论的算术化是一个一一对应的函数 g，把该理论的符号集、表达式集和表达式的有限系列集映射到正整数，g 满足以下条件

- g 可计算
- 有一个有效的（effective）计算过程（即算法）通过 g 的值 m 找出对象 x，使得 $g(m) = x$

注

- Gödel 编码的目的是把元数学算术化
- 还有其它编码方案，亦可把某个数学理论算术化

自身反射

Gödel 设计这种编码系统的目的

- 把关于形式系统（如 $\mathscr{N}$）的判断（元语言，即自然语言）转换成关于数的断言
- 再把这些（数的）断言在形式系统内部（如 $\mathscr{N}$）表示出来（对象语言，即 $\mathscr{L}_N$）

判断形式系统所能作出的（元数学）断言：公式、定理和证明等

例 6.34

（元数学）判断（关系）：

一个公式的有穷序列和一个特定的公式之间存在某种关系

如“序列 $\mathscr{A}_1, \cdots, \mathscr{A}_k, \mathscr{A}$ 是 $\mathscr{A}$ 在 $\mathscr{N}$ 中的证明”

$\Leftarrow$ 关于数（Gödel 编码）的断言（可表达性）

定义 6.35 (Pf)

基于 Gödel 数，定义 D_N 上一个关系 Pf

$Pf(m, n)$ 成立 $\Longleftrightarrow$ m 是 $\mathscr{N}$ 的公式序列的 Gödel 数，这个序列是 Gödel 数为 n 的公式在 $\mathscr{N}$ 中的一个证明

$\mathscr{N}$ 的其它性质和判断可以类似的方式定义为 D_N 上的各种关系

命题 6.36 (*Pf*)

若关系 Pf 在 $\mathscr{N}$ 中是可表达的，则存在 $\mathscr{L}_N$ 的公式 $\mathscr{P}(x_1, x_2)$，使对每个 $m, n \in D_N$ 有

若 $Pf(m, n)$ 成立，则 $\vdash_{\mathscr{N}} \mathscr{P}(0^{(m)}, 0^{(n)})$

若 $Pf(m, n)$ 不成立，则 $\vdash_{\mathscr{N}} \sim \mathscr{P}(0^{(m)}, 0^{(n)})$

证

依定义 6.4（可表达性） □

这样，就存在一个公式 $\mathscr{P}(x_1, x_2)$，它在形式系统内能判定这样的“元问题”：

对任意的公式序列 $\mathscr{A}_1, \cdots, \mathscr{A}_k, \mathscr{A}$，它是否组成 $\mathscr{N}$ 的一个证明

自指

正企图用系统 $\mathscr{N}$ 作为它自己的元系统

注

表面上，这样的做法可能导致矛盾，但由于仅有 D_N 上递归关系是可表达的，用 $\mathscr{N}$ 作为自身元系统只需部分关系，矛盾是可以避免的

$\Rightarrow$ 下一步是证明在 D_N 上某些关系是递归的，这些关系刻画公式、定理和证明，且在 $\mathscr{N}$ 中可表达

命题 6.37

D_N 的下列关系是递归的，因此在 $\mathscr{N}$ 中是可表达的

(1) *Wf* $Wf(n)$ 成立 $\Longleftrightarrow$ n 是 $\mathscr{N}$ 中一个公式的 Gödel 数

(2) *Lax* $Lax(n)$ 成立 $\Longleftrightarrow$ n 是 $\mathscr{N}$ 中一个逻辑公理的 Gödel 数

(3) *Prax* $Prax(n)$ 成立 $\Longleftrightarrow$ n 是 $\mathscr{N}$ 中一个非逻辑公理的 Gödel 数

(4) *Prf* $Prf(n)$ 成立 $\Longleftrightarrow$ n 是 $\mathscr{N}$ 中一个证明的 Gödel 数

(5) *Pf* $Pf(m, n)$ 成立 $\Longleftrightarrow$ m 是以 n 为 Gödel 数的公式的一个证明的 Gödel 数

命题 (续)

(6) *Subst*　$Subst(m, n, p, q)$ 成立 $\iff$ m 是在其 Gödel 数为 n 的表达式中，对所有其 Gödel 数为 q 的自由变元替换为其 Gödel 数为 p 的项所得的结果的 Gödel 数

(7) *W*　$W(m, n)$ 成立 $\iff$ m 是公式 $\mathscr{A}(x_1)$ 的 Gödel 数，其中 x_1 在 $\mathscr{A}(x_1)$ 中自由出现，而 n 是 $\mathscr{A}(0^{(m)})$ 在 $\mathscr{N}$ 中证明的 Gödel 数

(8) *D*　$D(m, n)$ 成立 $\iff$ m 是公式 $\mathscr{A}(x_1)$ 的 Gödel 数，其中 x_1 在 $\mathscr{A}(x_1)$ 中自由出现，而 n 是公式 $\mathscr{A}(0^{(m)})$ 的 Gödel 数

♢

证

依递归论可证 □

- Gödel 证明
- 可表达性
- 递归论
- Gödel 数
- 不完全性证明

不完全性证明

证明中的一个关键技巧是使用关系 W

$W(m,n)$ 成立 $\Longleftrightarrow$ m 是公式 $\mathscr{A}(x_1)$ 的 Gödel 数，其中 x_1 在 $\mathscr{A}(x_1)$ 中自由出现，而 n 是 $\mathscr{A}(0^{(m)})$ 在 $\mathscr{N}$ 中证明的 Gödel 数

这包含用项 $0^{(m)}$（其对应的数为 m）代入公式 $\mathscr{A}(x_1)$，其 Gödel 数为 m

W 是可表达的，故存在一个公式 $\mathscr{W}(x_1, x_2)$，其中 x_1, x_2 是自由的，使得

若 $W(m, n)$ 成立，则 $\vdash_{\mathscr{N}} \mathscr{W}(0^{(m)}, 0^{(n)})$　　（可证）

若 $W(m, n)$ 不成立，则 $\vdash_{\mathscr{N}} \sim \mathscr{W}(0^{(m)}, 0^{(n)})$　　（不可证）

W 是 $\mathscr{W}$ 的解释

定义 6.38 ($\mathscr{U}$)

考虑公式 ($\mathscr{A}(x_1)$)

$$(\forall x_2) \sim \mathscr{W}(x_1, x_2)$$

令 p 为该公式的 Gödel 数，以 $0^{(p)}$ 代替 x_1 所得公式

$$(\forall x_2) \sim \mathscr{W}(0^{(p)}, x_2)$$

记为 $\mathscr{U}$

W 是 $\mathscr{W}$ 的解释，对 $\mathscr{U}$ 解释如下

“对任意 $n \in D_N$，$W(p, n)$ 不成立”

亦即

对任意 $n \in D_N$，p 是其中 x_1 自由出现的公式 $\mathscr{A}(x_1)$ 的 Gödel 数且 n 是 $\mathscr{A}(0^{(p)})$ 在 $\mathscr{N}$ 中的证明 的 Gödel 数是不成立的

这样，p 是一个其中 x_1 自由出现的公式的 Gödel 数，该公式即 $(\forall x_2) \sim \mathscr{W}(x_1, x_2)$，记为 $\mathscr{A}(x_1)$，则 $\mathscr{A}(0^{(p)})$ 就是 $\mathscr{U}$

$\mathscr{U}$ 的解释等价于

定义 6.39 (不可证性)

对任意 $n \in D_N$，n 不是 $\mathscr{U}$ 在 $\mathscr{N}$ 中的证明 的 Gödel 数

亦即公式 $\mathscr{U}$ 断言其自身的不可证性

不完全性证明需要一个更强的一致性概念

定义 6.40 (ω-一致性)

令 S 是一个与 $\mathscr{N}$ 有相同语言的一阶系统，S 是 ω-一致的 (ω-consistency)，若不存在 x_1 在其中自由出现的公式 $\mathscr{A}(x_1)$，使得对任意 $n \in D_N$，$\mathscr{A}(0^{(n)})$ 是 $\mathscr{N}$ 的定理，且 $\sim(\forall x_1)\mathscr{A}(x_1)$ 也是 $\mathscr{N}$ 的定理 $\diamondsuit$

注

- ω-一致性断言，若每个 $\mathscr{A}(0^{(n)})$ 是定理，则 $\sim(\forall x_1)\mathscr{A}(x_1)$ 不是定理（不管 $(\forall x_1)\mathscr{A}(x_1)$ 是否为定理）
- ω —自然数的基数符号

命题 6.41

设 S 是与 $\mathscr{N}$ 有相同语言的一阶系统，若 S 是 ω-一致的，则 S 是一致的 ♢

证

令 $\mathscr{A}(x_1)$ 是任一公式使得对每个 n，$\mathscr{A}(0^{(n)})$ 是 S 的定理，

如 $\mathscr{A}(x_1)$ 可为 $x_1 = x_1$，由 ω-一致性，$\sim\forall x_1\mathscr{A}(x_1)$ 不是 S 的定理，即存在一个公式不是定理，故 S 是一致的 □

命题 6.42 (不完全性定理)

在 $\mathscr{N}$ 具 ω-一致性条件下，$\mathscr{U}$ 和它的否定都不是 $\mathscr{N}$ 的定理

亦即，若 $\mathscr{N}$ 是 ω-一致的，则 $\mathscr{N}$ 是不完全的 ♢

证

设若 $\mathscr{U}$ 是 $\mathscr{N}$ 的定理，令 q 是 $\mathscr{U}$ 在 $\mathscr{N}$ 中证明的 Gödel 数

用 p 如上述 ($\mathscr{A}(x_1)$，即 $(\forall x_2)\sim\mathscr{W}(x_1, x_2)$ 的 Gödel 数)

$W(p, q)$ 成立

W 由 $\mathscr{W}$ 在 $\mathscr{N}$ 中可表达

$$\vdash_{\mathscr{N}} \mathscr{W}(0^{(p)}, 0^{(q)})$$

但由 $\vdash_{\mathscr{N}} \mathscr{U}$

$$\vdash_{\mathscr{N}} \forall x_2 \sim\mathscr{W}(0^{(p)}, x_2)$$

$$\vdash_{\mathscr{N}} \sim\mathscr{W}(0^{(p)}, 0^{(q)}) \qquad ((\mathrm{K4})\mathrm{MP})$$

与 $\mathscr{N}$ 的一致性矛盾，故 $\mathscr{U}$ 不是 $\mathscr{N}$ 的定理

证 (续)

设若 $\mathscr{U}$ 不是 $\mathscr{N}$ 的定理

不存在 $\mathscr{N}$ 中 $\mathscr{U}$ 的证明

不存在 q 是在 $\mathscr{N}$ 中 $\mathscr{U}$ 的证明的 Gödel 数

不存在 q 是 $(\forall x_2) \sim \mathscr{W}(0^{(p)}, x_2)$ 的证明的 Gödel 数

对任意 q, $W(p, q)$ 不成立

$\vdash_{\mathscr{N}} \sim \mathscr{W}(0^{(p)}, 0^{(q)})$ (任一 q)

由 ω-一致性

$\sim \forall x_2 \sim \mathscr{W}(0^{(p)}, x_2)$ 不是 $\mathscr{N}$ 的定理

故 $\sim\mathscr{U}$ 不是 $\mathscr{N}$ 的定理 □

注

- 不完全性定理的前提条件是 ω-一致性

  对 $\mathscr{N}$，考虑朴素算术 N 作为模型，可认为 $\mathscr{N}$ 是 （ω-）一致的

  考虑 $\mathscr{N}$ 的标准模型，需要其它假设（规范模型的论域，需要集论的一致性）

- 不完全性定理可推广到任何形式系统，需要满足 ω-一致性

  $\mathscr{N}$ 的各种扩充 — 数学系统

命题 6.43

设 $\mathscr{N}$ 是 ω-一致的，则 $\mathscr{N}$ 包含一个闭式，它在模型 N 中是真的，但它不是 $\mathscr{N}$ 的定理 ♢

证

即 $\mathscr{U}$（因 N 是模型，$\mathscr{U}$ 或 $\sim\mathscr{U}$ 在 N 中为真） □

命题 6.44

设 $\mathscr{N}$ 是一致的，$\mathscr{N}$ 包含一个闭式，它在模型 N 中是真的，但它不是 $\mathscr{N}$ 的定理 ♢

证

因一致性比 ω-一致性弱，通过修改命题 6.42 证明中相应条件（尤其是 $\mathscr{U}$）可证 □

命题 6.45

设 S 是 $\mathscr{N}$ 的扩充，使得 S 的合适公理的 Gödel 数集是一个递归集，则如果 S 是一致的，那么 S 是不完全的 ♢

证

(梗概) 由 S 的前提可定义关系 $Prax_S$: $Prax_S(n)$ 成立 $\iff$ n 作为 S 的合适公理的 Gödel 数是递归的，可证 命题 6.37 对 S 也是成立的 □

注

这不意味着没有一致的 S ($\mathscr{N}$) 是完全的，但若有 S 的公理 (数) 集是递归的前提，则不完全

注

- $\mathscr{N}$ 不能通过扩充一组合适公理（其 Gödel 数（有穷或无穷）为递归的前提下）获得完全性
- 特殊地，增加不可判定公式 $\mathscr{U}$ 作为合适公理的扩充 $\mathscr{N}'$ 也是不完全的
- $\mathscr{N}$ 是不完全的，难于通过修改其公理获得完全性
- 一般地，$\mathscr{N}$ 中归纳公理需用二阶语言，二阶算术其公理的 Gödel 数集仍是递归和不完全的（二阶逻辑亦是不完全的）
- 可获得一个一致且完全的一阶算术系统：把所有在模型 N 中为真的公式都作为合适公理来扩充 $\mathscr{N}$，因其公理的 Gödel 数不是递归的

注

- 任何足够强的一阶系统，它的合适公理（Gödel 数）集是递归的，又是一致的，则这个系统是不完全的

  （一个系统是足够强的，若自然数系统能在这系统中被定义，算术公理是定理，例如实数理论、群论等）

- 特别地，若 *ZF* 是一致的，则它是不完全的

- 若有一个足够强的系统，则 Gödel 定理可应用，结果该系统即是不完全的；另一方面，若一个系统不是足够强的（即不是所有原始递归真理都是定理），则该系统由于有这个缺陷，也是不完全的

推论 6.46 (Gödel 第二不完全性定理)

任意一个包含算术系统的形式系统自身不能证明它本身的一致性

证

(说明) 用一个闭式表示“若没有同时对一个公式及其否定式的证明，则是一致的”

$$\left(\left(\forall x_1\right)\left(\forall x_2\right)\left(\forall x_3\right)\left(\forall x_4\right) \sim \left(Pf\left(x_1, x_3\right) \wedge Pf\left(x_2, x_4\right) \wedge Neg\left(x_3, x_4\right)\right)\right)$$

这个公式可隐含 Gödel 公式 $\mathscr{U}$，由不完全性定理，若该系统是一致的，则该公式 (断言自身一致性) 是不可证的 □

注

这就直接否定了 Hilbert 规划

Gödel 定理的数学表述

- 数学是不可穷尽的
- 每个一致的形式数学理论一定包含不可判定的命题
- 没有既一致又完全的形式数学理论
- 数学是机械上（或算法上）不可穷尽的（或不可完全的）

Gödel（不完全性）定理的影响

- 数学

  数学的（绝对）一致性问题仍悬而未决

  数学基础的第三次危机仍未解决

- 哲学

  Gödel 定理具深刻的思想影响，涉及现代哲学的各个方面

  澄清逻辑与直观，形式与内容，机器与心智，真与可证，实在与可知之间的（辩证）关系

  推广到物理学甚至人间事物，Gödel 曾拟出一个表述：“一个完全不自由的社会（即处处按“统一”的法则行事的社会），就其行为而言或者是不一致的，或者是不完全的，即无力解决某些问题，可能是极端重要的问题。在困难的处境里，二者当然都会危及它的生存。这个说法也适用于个体的人。”

Gödel（不完全性）定理的影响

- 人工智能
  - 人的智能肯定比数学（任何足够强的一阶系统）强，人工智能系统究其本质（计算机（软件）系统）是形式系统，因此是不完全的，而人的智能能力可认为是潜在完全的
  - 人工智能系统不需或不具一致性，Gödel 定理不成立（不适用）
  - 人工智能的逻辑学超越数理逻辑，回归逻辑的原始目标，建立关于思维的科学

附 I*：不可证的算术真理

Gödel 证明：一个不可判定命题的存在性

是否有算术真理但（在 Peono 算术）不可证的命题（可构造）？

继承 n 进制

n（$n > 1$）进制：任一自然数 m 可表为

$m = a_k n^k + a_{k\text{-}1} n^{k\text{-}1} \ldots a_0 \quad (0 \leq a_i < n, a_k \neq 0)$

例：$35 = 2^5 + 2^1 + 2^0$，即二进制 100011

继承 n 进制把所有的指数改写为 n 进制，以此类推（指数的指数），直到每个出现的数都比 n 小

例：$35 = 2^{2^2+1} + 2 + 2$

Goodstein 系列

Goodstein 系列 $G(m)$（m 是一个自然数）

- 第一个元素 $G(m)(1)$ 是 m 本身
- 第 $n+1$ 个元素 $G(m)(n+1)$ 构造如次：先把 $G(m)(n)$ 写成继承 $n+1$ 进制表示，再把其中所有的 $n+1$ 改为 $n+2$（换制，小于 $n+1$ 不改），然后再减 1

  如 $G(m)(2)$：先把 m 写成继承 2 进制表示，再把其中所有的 2 改为 3，然后再减 1
- 如此直到结果为 0，此时该序列终止

例：$G(3)$ 经 6 步终止于 0，但 Goodstein 系列快速发散（步数增长）

如 $G(19)$ 的第 6 个元素为 $7^{7^7} \approx 3.8 \times 10^{694974}$

Goodstein 定理（1944）

每个 Goodstein 系列都终止于 0

使用集论（序数），易证

注

因此，Goodstein 定理是一个算术真理

但在 Peano 算术中不可证

Kirby-Paris 定理（1982）

Goodstein 定理不是 Peano 算术的定理

证明需使用非标准算术模型（含非标准数 (超自然数) 的算术模型，Skolem 1934）

附 II*：一致完全的算术

无乘法的算术，比 Peano 算术弱

Presburger 算术（1929）

Presburger 算术的（带等词）一阶语言包含 0，1 和二元函数符 +（解释为加），公理如下

(1) $\sim(0 = x+1)$

(2) $x+1 = y+1 \to x = y$

(3) $x+0 = x$

(4) $x+(y+1) = (x+y)+1$

(5) $P(0) \wedge \forall x(P(x) \to P(x+1)) \to \forall y P(y)$ （公理模式，$P(x)$ 为含自由变元 x 的谓词符）

Presburger 算术是一致、完全和可判定的，且有证明器（NP 难解，Davis, 1954/57）

附 III*：实数的完全性定理

Tarski 实闭域理论（1951）

实数上的域理论 $(R, 0, 1, +, \times)$，R 为实数集

实数比自然数要复杂，但实数的域理论是完全的，甚至是可判定的，其公理系统如次

(1) 所有关于域的公理

(2) 1 不是任意多个数的平方和

(3) 任意数和它的相反数之间至少有一个是平方数（即一个非 0 的数是正数或负数）

(4) 任意奇数次多项式必有根

注

- Tarski 实数不包含 Peano 算术

  不能由 1 生成自然数序列，即自然数在实闭域中不可定义（可逐个数用一阶公式写出 $x = 1$，$x = 10$ 等，但不能用一个一阶公式来定义它们是自然数）

  不存在实闭域公式 $\mathscr{A}(x)$ 使得 $\mathscr{A}(a)$ 在实数中为真当且仅当 $\mathscr{A}(a)$ 是一个自然数

- 代数模型论中最重要的定理之一（若实闭域可定义集可完全分类，可建立模型论和代数几何的联系）

注

- 任意特征的代数闭域理论（Tarski），以特征不是 0 为例，公理系统如次：(1) 所有关于域的公理，(2) 多个 1 相加等于 0（若是 0 则换成“任意多个 1 相加不等于 0”），(3) 任意多项式必有根
- 无端点稠密线序理论（有理数），其公理系统如次：(1) $<$ 是一个线序，(2) $<$ 没有端点（没有最大和最小元素），(3) 对任意两个元素 a 与 b，必有一个 c 在 a 和 b 之间（稠密性）。其完全性定理易证（练习）

Euclid 几何

- Euclid 几何是公理系统和数学的起点
- Euclid 几何五条公理接近一个完全的公理系统（“几乎完全”），但它还不是
  - Hilbert 给出了一个 Euclid 几何的公理系统，但不是一阶系统
  - Tarski 给出一个 Euclid 几何的一阶系统并证明了完全性，且基于实闭域理论是可判定的

数学啊，数学 ……