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

5 数学基础

- 数学系统
- 带等词一阶系统
- 群论
- 一阶算术
- 形式集论
- 一致性问题

数学系统

一阶系统与数学

- 逻辑演算是刻画形式推理，尤其是数学中的精确推理
- 一阶语言 $\mathscr{L}$ 是普适的，$\mathscr{L}$ 中的符号可以不同方式解释
- 一阶逻辑 $K_{\mathscr{L}}$ 是足够一般的，$K_{\mathscr{L}}$ 中的定理可解释为真理
- 对任一 $\mathscr{L}$，有一类公式不依赖于对符号的解释，即逻辑有效的公式，亦即 $K_{\mathscr{L}}$ 中的定理
- 当 $\mathscr{L}$ 中的（非逻辑）符号用数学方式解释，$K_{\mathscr{L}}$ 中的定理可解释为数学中的真理，它们之所以为数学真理是基于逻辑的结构，而不依赖于具体的数学背景

注

数学中的逻辑主义

例 5.1

对一个算术解释，A_1^2 解释为 “=”

$\forall x_1 \forall x_2 (A_1^2(x_1, x_2) \to A_1^2(x_1, x_2))$ 是有效的，可解释为数学真理

$\forall x_1 \forall x_2 (A_1^2(x_1, x_2) \to A_1^2(x_2, x_1))$ 可解释为数学真理，但不是 $K_{\mathscr{L}}$ 的定理 $(\forall x_1 \forall x_2 (\mathscr{A}(x_1, x_2) \to \mathscr{B}(x_2, x_1)))$

$\Leftarrow$ 需要补充有关 “=” 的公理

定义 5.2 (一阶理论)

一个一阶理论 (first-order theory，简称理论) 作为一阶系统是 $K_{\mathscr{L}}$ 的某个通过增加公理的扩充，通过引入合适公理集来扩充逻辑公理 (K1-5)。一个一阶理论的模型是一个解释，使其所有公理为真

一个数学系统作为一阶理论引入合适公理集来扩充 $K_{\mathscr{L}}$，使得系统中的定理表示某个数学领域 (尽可能多) 的数学定理以及逻辑定理

注

希望一个数学系统具有完全性

例 5.3

给定一个一阶语言 $\mathscr{L}$

只有一个谓词符 A_1^2（没有函项符和常元）

把 $A_1^2(x_i, x_j)$ 记为 $x_i < x_j$，一个一阶理论通过增加以下合适公理

(P1) $\forall x_1(\sim x_1 < x_1)$ （非自反性）

(P2) $\forall x_1 \forall x_2 \forall x_3(x_1 < x_2 \wedge x_2 < x_3 \to x_1 < x_3)$ （传递性）

该一阶理论的模型称为偏序理论，作为数学系统（在数学中）称偏序结构

Hilbert 论题

一阶逻辑之外无逻辑

- 为显式地表达数学（逻辑外）的假设，所需的公理总能用一阶逻辑表达
- 数学中非形式化的证明能用一阶逻辑中形式化的证明精确地表达

注

(1) 数学中的形式主义，Hilbert 规划

(2) 见下例 5.20

(3) 已有多个一阶逻辑和数学形式证明的软件
(LCF/FOL/Isabelle/Hyperproof 等)
如 Lean，Coq 是常用的交互式定理证明器，可对一阶逻辑、数学定理和程序正确性进行形式化和形式证明

(4) E-prover (E 2.3, github.com/eprover): 带等词 FOL 证明器（开源）

(5) 大部分数学还没有形式化，一个 Kepler 猜想的形式化花了 20 人年

- 数学系统
- 带等词一阶系统
- 群论
- 一阶算术
- 形式集论
- 一致性问题

带等词一阶系统

令 $\mathscr{L}$ 为一个（带等词的）一阶语言，$\mathscr{L}$ 中 A_1^2 解释为“=”

定义 5.4 (等词公理)

(E6) $A_1^2(x_1, x_1)$

(E7) $A_1^2(t_k, u) \to A_1^2(f_i^n(t_1, \ldots, t_k, \ldots, t_n), f_i^n(t_1, \ldots, u, \ldots, t_n))$，

$t_1, \ldots, t_n, u$ 是（$\mathscr{L}$ 的）任意项，f_i^n 是任意函项符

(E8) $(A_1^2(t_k, u) \to (A_i^n(t_1, \ldots, t_k, \ldots, t_n) \to A_i^n(t_1, \ldots, u, \ldots, t_n)))$，

$t_1, \ldots, t_n, u$ 是任意项，A_i^n 是任意谓词符

注

- 等词公理可有自由变元出现

  已知：对任意公式 $\mathscr{A}$，它的全称闭式是 $\mathscr{A}'$

  $$\mathscr{A} \vdash_{K_{\mathscr{L}}} \mathscr{A}' \text{ 且 } \mathscr{A}' \vdash_{K_{\mathscr{L}}} \mathscr{A}$$

  可写成这些公理的全称闭式

- 据关于约束变元换名的 命题 4.28，在 (E6) 中用变元名 x_1 是无关紧要的

  例如，$A_1^2(x_5, x_5)$ 就是 (E6) 的推论，其演算如次

$$\begin{aligned}
&(1)\ A_1^2(x_1, x_1) && \text{(E6)}\\
&(2)\ (\forall x_1)A_1^2(x_1, x_1) && (1)\text{Gen}\\
&(3)\ (\forall x_5)A_1^2(x_5, x_5) && (2)(\text{命题 } 4.28)\\
&(4)\ (\forall x_5)A_1^2(x_5, x_5) \to A_1^2(x_5, x_5) && \text{(K4)}\\
&(5)\ A_1^2(x_5, x_5) && (3)(4)\text{MP}
\end{aligned}$$

注（续）

- (E6)：确保在任意模型中，A_1^2 的解释就是 $=$（等号）
- (E7)(E8)：确保在任意模型中，A_1^2 的解释起到 $=$ 的作用，即相等的东西可彼此代替

  （t_k 只替换 u 一次，重复应用可进行多个替换）
- (E7)(E8) 都是公理模式

定义 5.5 (数学系统)

数学系统（作为一阶理论）都是 $K_{\mathscr{L}}$（对某个 $\mathscr{L}$）的扩充，它们通常包括公理 (E6)，以及 (E7)(E8) 的所有适用的（与 $\mathscr{L}$ 有关的）实例 ♢

定义 5.6 (等词系统)

(E6)(E7)(E8) 称为 等词公理

任意包括 (E6)(E7)(E8) 适当实例的 $K_{\mathscr{L}}$ 的扩充称为 带等词一阶系统 (first-order systems with equality)，亦即一个一阶理论，一个（基本的）数学系统 ♢

注 (带等词一阶逻辑)

- 把包含 (K1-5)，(E6-8) 的形式系统称 带等词 FOL，记 $K_{\mathscr{L}_=}$
- 通常，FOL 都指带等词的

等价的带等词一阶逻辑 *

一个等价的带等词一阶逻辑：在 (K1-5) 上增加如下公理

(K6) $\forall x_1(x_1 = x_1)$　　（等词自反）

(K7) $x_1 = x_2 \to (A(x_1, x_1) \to A(x_1, x_2))$，$A(x_1, x_1)$ 是不含常元的原子公式，x_2 在 $A(x_1, x_1)$ 中对 x_1 自由　　（等词替换）

注

在 (K1-5) 上，从 (K6-7) 可推出 (E6-8) ((K6) 即 (E6))，推导过程较长，可作练习（提示：先证 (K7) 的原子 $A(x_1, x_1)$ 换成任意公式 $\mathscr{A}(x_1, x_1)$ 亦成立）

带等词一阶公理的独立性（证明思路）*

- (K1-3) 的独立性需重新考虑，因可能有 $t = s$ 实例，可把它看成形式 $A \to A$
- (K4-6) 可把量词和项去掉看成形式 $B \to B$，(K7) 看成形式 $(B \to B) \to (C \to C)$
- 设计多值表可证

命题 5.7

设 S 是带等词的一阶系统，则下列各式是 S 的定理

(1) $(\forall x_1)A_1^2(x_1, x_1)$

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

(3) $(\forall x_1)(\forall x_2)(\forall x_3)(A_1^2(x_1, x_2) \to (A_1^2(x_2, x_3) \to A_1^2(x_1, x_3)))$

$\diamondsuit$

证

(1) 由 Gen 即得

证 (续)

(2)

(1) $A_1^2(x_1, x_2) \to (A_1^2(x_1, x_1) \to A_1^2(x_2, x_1))$ (E8)

(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)MP

(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) $A_1^2(x_1, x_1)$ (E6)

(6) $A_1^2(x_1, x_2) \to A_1^2(x_1, x_1)$ (4)(5)MP

(7) $A_1^2(x_1, x_2) \to A_1^2(x_2, x_1)$ (3)(6)MP

(8) $(\forall x_1)(\forall x_2)(A_1^2(x_1, x_2) \to A_1^2(x_2, x_1))$ (7)Gen

证 (续)

(3)

$$(1)\ A_1^2(x_2, x_1) \to (A_1^2(x_2, x_3) \to A_1^2(x_1, x_3)) \qquad (E8)$$

$$(2)\ (A_1^2(x_1, x_2) \to A_1^2(x_2, x_1)) \qquad (2)$$

$$(3)\ A_1^2(x_1, x_2) \to (A_1^2(x_2, x_3) \to A_1^2(x_1, x_3)) \qquad (1)(2)\mathrm{HS}$$

$$(4)\ (\forall x_1)(\forall x_2)(\forall x_3)(A_1^2(x_1, x_2) \to (A_1^2(x_2, x_3) \to A_1^2(x_1, x_3))) \qquad (3)\mathrm{Gen}$$

□

注

命题 5.7 (1-3) 的每一个在 S 的任意模型中必然为真

符号 A_1^2 在任意模型中都可用一个自反、对称和传递的关系（即等价关系）来解释

但 (E6-8) 并不能保证在 S 中 A_1^2 的解释一定是 $=$

例 5.8

考虑一个一阶语言 $\mathscr{L}$，其变元是 $x_1, x_2, \ldots$，函项符有 f_1^2，谓词符有 A_1^2

定义一个解释 I 如下：

- D_I 是所有整数的集合 $\mathbb{Z}$
- $\bar{f}_1^2(x, y)$ 代表 $x + y$
- $\bar{A}_1^2(x, y)$ 成立 当且仅当 对 $x, y \in \mathbb{Z}$, $x \equiv y \pmod 2$

在此解释下，等词公理都为真

例 (续)

(E6)：其解释是 $x \equiv x \pmod 2$，这是真的

(E7)：考虑一个特殊情形（可推广到一般情形）

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

可解释为

$$\text{若 } x \equiv y \pmod 2, \text{ 则 } x + z \equiv y + z \pmod 2$$

这是真的

例 (续)

(E8)：因 $\mathscr{L}$ 只含一个谓词符，故仅有两个实例需证

$$(A_1^2(t,u) \to (A_1^2(t,v) \to A_1^2(u,v)))$$

和

$$(A_1^2(t,u) \to (A_1^2(v,t) \to A_1^2(v,u)))$$

其解释分别为

$$\text{若 } x \equiv y \pmod 2, \text{ 则 } x \equiv z \pmod 2 \text{ 蕴涵 } y \equiv z \pmod 2$$

和

$$\text{若 } x \equiv y \pmod 2, \text{ 则 } z \equiv x \pmod 2 \text{ 蕴涵 } z \equiv y \pmod 2$$

它们都是真的 ♢

命题 5.9

若 S 是一致的带等词一阶系统，则 S 有一个模型，其对 A_1^2 的解释是 $=$

$\diamondsuit$

证

据 命题 4.62，若 S 是一致的，则 S 有模型，设为 M

据 命题 5.7，$\bar{A}_1^2$ 是 D_M 上的等价关系，用 $[x]$ 表示 x 的等价类

定义一个新的解释 M^* 如下

证 (续)

M^* 的论域是 $\{[x] : x \in D_M\}$，对每一 i，a_i 用 $[\bar{a}_i]$ 解释，f_i^n 用 $\hat{f}_i^n$ 解释，使对 $y_1, \ldots, y_n \in D_M$，

$$\hat{f}_i^n([y_1], \ldots, [y_n]) = [\bar{f}_i^n(y_1, \ldots, y_n)]$$

A_i^n 用 $\hat{A}_i^n$ 解释，使对 $y_1, \ldots, y_n \in D_M$

$$\hat{A}_i^n([y_1], \ldots, [y_n]) \text{ 成立 当且仅当 } \bar{A}_i^n(y_1, \ldots, y_n) \text{ 成立}$$

这里 $\bar{a}_i, \bar{f}_i^n, \bar{A}_i^n$ 是 $\mathscr{L}$ 的符号在 M 中的解释

可验证这些定义都是良定义的，且 M^* 是 S 的模型

(处处可定义，公理在此模型下为真) □

例 5.10 (例 5.8 续)

定义一个新的模型：论域为 $\{[0],[1]\}$，f_1^2 用 $\hat{f}_1^2$ 解释，A_1^2 用 $\hat{A}_1^2$ 解释，并给定

$$\hat{f}_1^2([x],[y]) = [\bar{f}_1^2(x,y)] = [x+y]$$

$\hat{A}_1^2([x],[y])$ 成立 当且仅当 $\bar{A}_1^2(x,y)$ 成立， 当且仅当

$$x \equiv y \pmod 2, \quad \text{当且仅当}$$

$$[x] = [y]$$

定义 5.11 (规范模型)

令 S 是带等词一阶系统，S 的 规范模型（normal model）是 A_1^2 解释为 $=$ 的模型，亦简称模型 ♢

命题 5.12

任何一致的带等词一阶系统 S（带等词一阶逻辑 $K_{\mathscr{L}_=}$）都有有穷或能枚举无穷规范模型

证

据命题 4.65（Löwenheim-Skolem 定理），S 有能枚举模型，S 的模型可收缩为对应的规范模型（命题 5.9），其能枚举论域是等价类的集，而等价类的集是有限或能枚举的 □

推论 5.13 (推广的 Löwenheim-Skolem 定理)

对任何带等词一阶系统 S，若 S 有一个无穷规范模型，则它有一个能枚举无穷规范模型

证

留作练习 □

仍以 $\vdash$，$\models$ 表示推理关系，考虑 FOL 是带等词的，不会引起混淆

命题 5.14

带等词一阶系统 S（或带等词一阶逻辑 $K_{\mathscr{L}_=}$）具有可靠与完全性定理

即 $\vdash \mathscr{A}$ 当且仅当 $\models \mathscr{A}$

证

可靠性易对等词公理验证
完全性只需考虑闭式 $\mathscr{A}$（任一有效的（或可证的）公式等价于它的全称闭式），若 $\mathscr{A}$ 是有效的，设 $\nvdash_S \mathscr{A}$，据命题 4.51，把 $\sim\mathscr{A}$ 加入 S 所得扩充 S' 是一致的，据命题 5.12，S' 有一个规范模型 M，
因 $\sim\mathscr{A}$ 是 S' 的公理，$\sim\mathscr{A}$ 在 M 中为真，但已设 $\mathscr{A}$ 是有效，
$\mathscr{A}$ 在 M 中为真，这是不可能的 □

注

这是证明完全性定理的另一种方式，即先给出 Löwenheim-Skolem 定理，再给出完全性结果

命题 5.15

带等词一阶系统 S 具有一致性

证

类似 K 一致性可证 □

记号

用 $t_1 = t_2$ 代表 $A_1^2(t_1, t_2)$

$(t_1 \neq t_2) =_{def} \sim(t_1 = t_2)$，这里 t_1 和 t_2 是（$\mathscr{L}_=$ 中的）项

(E6-8) 的简化形式

等词公理

($E6'$) $x_1 = x_1$

($E7'$) $t_k = u \to (f_i^n(t_1, \ldots, t_k, \ldots, t_n) = f_i^n(t_1, \ldots, u, \ldots, t_n))$

($E8'$) $t_k = u \to (A_i^n(t_1, \ldots, t_k, \ldots, t_n) \to A_i^n(t_1, \ldots, u, \ldots, t_n))$

命题 5.16

令 t，s，r 为任意项

(1) $\vdash t = t$

(2) $\vdash t = s \to s = t$

(3) $\vdash t = s \to (s = r \to t = r)$ □

证

(1) 由 (E6′) 和 Gen，$\vdash \forall x_1(x_1 = x_1)$，据 (R3)，$\vdash t = t$

(2) 令 x，y 是不在 t 或 s 中出现的变元，$\mathscr{A}(x, x)$ 为 $x = x$，$\mathscr{A}(x, y)$ 为 $y = x$，易见

$$\vdash x = y \to (x = x \to y = x)$$

是公理模式 (E8′) 的实例

证 (续)

由 (1)

$$\vdash x = x$$

用重言式 $(\mathscr{A} \to (\mathscr{B} \to \mathscr{C})) \to (\mathscr{B} \to (\mathscr{A} \to \mathscr{C}))$，并用两次 MP，有

$$\vdash x = y \to y = x$$

再用两次 Gen，得到

$$\vdash (\forall x)(\forall y)(x = y \to y = x)$$

最后，用两次 (R3) 得

$$\vdash t = s \to s = t$$

(3) 留作练习 □

定义 5.17 (存在唯一量词)

- 存在量词（至少存在一个）：$(\exists x_i)\mathscr{A}(x_i)$
- 存在唯一量词

$$(\exists_1 x_i)\mathscr{A}(x_i) =_{def} (\exists x_i)(\mathscr{A}(x_i) \wedge (\forall x_j)(\mathscr{A}(x_j) \to x_i = x_j))$$

亦如

$$(\exists! x_i)\mathscr{A}(x_i) =_{def} (\exists x_j)(\forall x_i)(\mathscr{A}(x_i) \leftrightarrow x_i = x_j)$$

其中 x_j 是不在 $\mathscr{A}$ 中自由出现且不同于 x_i 的（第一个）变元

- 至多存在一个量词（但不一定存在）

$$(\exists!! x_i)\mathscr{A}(x_i) =_{def} (\forall x_i)(\forall x_j)(\mathscr{A}(x_i) \wedge \mathscr{A}(x_j) \to x_i = x_j)$$

注

- 验证：对任意解释 I，$I \models (\exists! x_i)\mathscr{A}(x_i)$ 当且仅当存在唯一 $d \in D_I$ 使得 $I \models \mathscr{A}(x_i/d)$
- 可证：$\vdash \exists! x_i \mathscr{A}(x_i) \leftrightarrow \exists x_i \mathscr{A}(x_i) \wedge \exists!! x_i \mathscr{A}(x_i)$

摹状（description）词

$\iota x A(x)$：那个有 A 性质的 x

如 $A(x)$：x 是大于 3 的最小素数，就有 $\iota x A(x) = 5$

规定：对给定谓词 A，当有唯一的 x 使得 $A(x)$ 成立时，就说 $\iota x A(x)$ 是存在的，即 $\iota x A(x)$ 有某种性质；否则，就是假的

如 $A(x)$：x 是 7 和 11 之间的素数，说 $\iota x A(x)$ 存在或 $\iota x A(x) = 11$ 等都是假的

注

- 摹状词类似冠词有不定摹状词和定摹状词之分，这里专指定摹状词（存在唯一）
- 自 Frege 就通过逻辑定义引入，Russull 发展摹状词理论来解决“存在”等哲学问题（如消除某些对象的不合理的本体论承诺）

摹状词

$\iota x A(x)$ 有性质 B，即存在唯一的使得 $A(x)$ 成立的 x 并且这个 x 有性质 B

$$(\iota)B(\iota x A(x)) =_{def} \exists y(\forall x(A(x) \leftrightarrow x = y) \wedge B(y))$$

- $\iota x A(x)$：摹状词
- ιx：摹状算子
- $A(x)$ 是 ιx 的辖域
- ι：摹状符
- x：摹状变元
- $B(\iota x A(x))$ 为 $\iota x A(x)$ 的辖域
- (ι) 为 $\iota x A(x)$ 的（辖域的）标志符，根据 (ι) 在公式中用以上定义式把摹状词替除后，x 在其中是约束的

摹状词演算 *

- 摹状词可用来定义项，如 $a =_{def} \iota x A(x)$
- 由此可进行演算

$$E!\iota x A(x) =_{def} \exists y(\iota x A(x) = y)$$

其中 y 不在 A 中出现

$E!\iota x A(x)$ 当且仅当 $\exists! x A(x)$

注

在一阶系统中，摹状词不是必要的，可通过引入新的函项和常元取代

函项符的消去 *

在带等词的一阶语言 $\mathscr{L}$ 中，函项符可消去（即不是必要的），一个 n 元函项符可用一个 $n+1$ 元谓词符来表示

如 $< t_1, \cdots, t_n, s > \in \bar{P}$ iff $\bar{f}(t_1, \cdots, t_n) = s$

如 $\mathscr{A}^*$ 是把 $\mathscr{A}$ 中函项符替换为相应的谓词符中变元

$$\forall x_1 \cdots \forall x_n \exists! x_{n+1} P(x_1, \cdots, x_n, x_{n+1}) \wedge \mathscr{A}*$$

- 反过来看，就是引入新的函项符
- 消去或引入常元可看成函项符的特殊情况

纯谓词演算 *

纯谓词演算

不含函项符和常元的谓词演算

n 元谓词符（有时只用一元谓词符）可能无穷多个

斯科伦前束范式：全部 $\exists$（若有）在 $\forall$（若有）之前的前束范式

命题（等价性定理）：在纯谓词演算中，对任一公式 $\mathscr{A}$ 与其斯科伦前束范式 $\mathscr{A}^S$，有 $\vdash \mathscr{A}$ 当且仅当 $\vdash \mathscr{A}^S$（$\models \mathscr{A}$ 当且仅当 $\models \mathscr{A}^S$）

注

- 数学中，如算术运算，使用函项符（函数）比较方便，也是必要的
- 可计算性上，不含函项符的一阶理论计算复杂度较低，但把一个含函项符的一阶理论通过消去函项符得到的等价的一阶理论需要考虑新引入替换公式的计算，计算复杂性是一样的

等词的消去 *

在带等词的一阶语言 $\mathscr{L}_=$ 中，等词可消去：可在不带等词的一阶语言 $\mathscr{L}'$ 中通过引入一个（特殊的）谓词符 E，对任一 $\mathscr{L}_=$ 的公式 $\mathscr{A}$ 中每次出现的 $=$ 都用 E 替换得到对应 $\mathscr{L}'$ 的公式 $\mathscr{A}^*$，并令 $\mathscr{A}^\#$ 为

$$\forall x_1 E(x_1, x_1) \wedge \mathscr{P}_1 \wedge \cdots \wedge \mathscr{P}_k \wedge A^*$$

设 P_i 为 $\mathscr{A}$ 中出现的（有限个）n_i 元谓词符，令 $\mathscr{P}_i$ 为如下公式

$$\forall x_1 \cdots \forall x_{2n_i}(E(x_1, x_{n_i+1}) \to E(x_2, x_{n_i+2}) \to \cdots \to E(x_{n_i}, x_{2n_i})$$
$$\to P_i(x_1, \cdots, x_{n_i}) \to P_i(x_{n_i+1}, \cdots, x_{2n}))$$

则一个 $\mathscr{L}_=$ 的解释 $I \models \mathscr{A}$ 当且仅当一个 $\mathscr{L}'$ 的一个解释 $I' \models \mathscr{A}^\#$

- 数学系统
- 带等词一阶系统
- 群论
- 一阶算术
- 形式集论
- 一致性问题

群论

定义 5.18 (群语言 $\mathscr{L}_G$)

令 $\mathscr{L}_G$ 是具有下述字符表的一阶语言

- 变元 $x_1, x_2, \ldots$
- 个体常元 a_1 (单位元)
- 函项符 f_1^1, f_1^2 (逆，积)
- 谓词符 $=$
- 技术性符号 $(,), ,$
- 逻辑符 $\forall, \sim, \rightarrow$

定义 5.19 (群系统 $\mathscr{G}$)

$\mathscr{G}$ 为 $K_{\mathscr{L}_G}$ 的扩充，其合适公理包含 (E6-8) 的所有适当实例，并增加以下公理

群公理

(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）

这些公理中的变元可考虑等价的全称闭式

注

(G4) $f_1^2(x_1, x_2) = f_1^2(x_2, x_1)$ （交换律）

增加 (G4) 即 Abel 群

定义（群）

一个非空集 G 称为一个群，如果下列条件成立

- 给定一个运算法则，对 G 中的每对元素 a 和 b，都有集合中的第三个元素与之对应，这个元素通常称为 a 和 b 积，记作 ab 或 $a \cdot b$
- 结合律　对 G 中的任意三个元素 a，b 和 c，等式
$$ab \cdot c = a \cdot bc$$
- G 中存在（至少）一个（左）单位元素 e，它具有下列性质：
对 G 中所有元素 a
$$ea = a$$
- 对 G 中每个元素 a，G 中存在（至少）一个（左）逆元素 a^{-1}，它具有性质
$$a^{-1}a = e,$$
在这个等式中，出现于右端的总是同一个（左）单位元素 e

代数学（p.24），[荷] 范德瓦尔登著（1930-1931），丁石孙等译（1963）

注

- 数学中（基本）群（论）G 的定义是群公理的非形式陈述，对照上述定义
  - 第一点由 $\mathscr{L}_G$ 规定
  - 其余三点即 (G1-3)
- “代数学”书由 Van der Waerden 据 Noether & Artin 讲稿而撰，其时正逢一阶逻辑成熟，其后公理化方法教科书由 Bourbaki 继承

例 5.20

在任何有单位元 e 的群 G 中，$e(ee) = e$

在 $\mathscr{G}$ 中形式化为公式

$$f_1^2(a_1, f_1^2(a_1, a_1)) = a_1$$

形式证明如下

注

在群论中（非形式）证明 $e(ee) = e$ 是简单的，但严格的证明步骤可通过形式证明验证

复杂的群论（数学）定理及证明同样可被形式化（Hilbert 论题）

例 (续)

(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)Gen

(3) $\forall x_1(f_1^2(a_1, x_1) = x_1) \to (f_1^2(a_1, a_1) = a_1)$ (K4)

(4) $f_1^2(a_1, a_1) = a_1$ (2)(3)MP

(5) $\forall x_1(f_1^2(a_1, x_1) = x_1) \to (f_1^2(a_1, f_1^2(a_1, a_1)) = f_1^2(a_1, a_1))$ (K4)

(6) $(f_1^2(a_1, f_1^2(a_1, a_1)) = f_1^2(a_1, a_1))$ (2)(5)MP

(7) $(f_1^2(a_1, a_1) = a_1) \to (f_1^2(a_1, f_1^2(a_1, a_1)) = f_1^2(a_1, a_1) \to$
$f_1^2(a_1, f_1^2(a_1, a_1)) = a_1)$ (E8')

(8) $f_1^2(a_1, f_1^2(a_1, a_1)) = f_1^2(a_1, a_1) \to f_1^2(a_1, f_1^2(a_1, a_1)) = a_1$ (4)(7)MP

(9) $f_1^2(a_1, f_1^2(a_1, a_1)) = a_1$ (6)(8)MP

解释

若 a_1 解释为（任意群 G 的）单位元，f_1^1 解释为逆，f_1^2 解释为群的运算，$=$ 解释为相等，则任意群 G 都是群系统 $\mathscr{G}$ 的一个模型

但还存在着其它的模型

例 5.21

构造 $\mathscr{G}$ 的一个解释 I 如下

- D_I 是整数集 $\mathbb{Z}$,
- a_1 解释为 0,
- $\bar{f}_1^1(x) = -x, \quad x \in \mathbb{Z}$,
- $\bar{f}_1^2(x, y) = x + y, \quad x, y \in \mathbb{Z}$;
- $=$ 解释为 $(\mathrm{mod}\ m)$ 同余，这里 m 是一个确定的正整数

I 是 $\mathscr{G}$ 的模型

证

需证 $\mathscr{G}$ 的每一公理在 I 下为真

(K1-5) 为真，因它们是有效的

(E6-8) 为真（见例 5.8）

需考察 (G1-3) 在 I 下为真

(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 $-x+x \equiv 0 \pmod{m}$

对任意 $x, y, z \in \mathbb{Z}$，上面语句都是真的

故 I 是 $\mathscr{G}$ 的模型 □

例 (续)

但 I 不是一个群（包含了额外的同余关系）

对模型 I 用 命题 5.9 的方法，构造一个规范模型 I^* 如下

- 论域是整数的同余类 $(\mathrm{mod}\ m)$ 的集
- a_1 解释作 0_m（含 0 的类）
- f_1^2 用 $+$ 解释
- f_1^1 解释作 “加性逆元”
- $=$ 解释作相等

I^* 是一个规范模型，且是一个群

定义 5.22 (群解释)

任意群 G 是群系统 $\mathscr{G}$ 的一个规范模型，群系统 $\mathscr{G}$ 的任一规范模型是一个群 G

问题

群系统 $\mathscr{G}$ 是否具有完全性定理？

计算系统 *

类似于数学系统，一个计算系统（关于可计算或计算机的形式系统）亦可作为一阶系统，扩充为某个领域的计算机理论

程序语言

设 P 是一个包含赋值、条件和迭代语句的程序设计语言

给出 $\mathscr{L}_P$ 作为关于 P 的一阶语言

扩充关于三个程序语句的公理的一阶系统是一个程序语言系统 $\mathscr{P}$

$\mathscr{P}$ 可作为 P 的公理化语义（Hoare 逻辑）

问题

P 与 $\mathscr{P}$ 之间的关系（如完全性定理）？

应用

（数学）定理自动证明和（计算机）程序（正确性）自动验证

非标准分析 *

无穷小：标准分析通过极限理论严格使用无穷小（无穷小缺乏直观意义）

实无穷小：非标准分析严格定义存在无穷小，并通过构造模型，使之（基本）等价（但不同构）于实数的有序域

令 R 是实数集，$\mathscr{K}_R$ 是广义带等词 FOL，其一阶语言 $\mathscr{L}_R$ 规定

- 对任一实数 r，有一个常元 a_r
- 对 R 任一 n 元操作 ϕ，有一个函项符 f_ϕ
- 对 R 任一 n 元关系 Φ，有一个谓词符 A_ϕ

R 作为 $\mathscr{K}_R$ 的模型 $\mathscr{R}$ 的论域，这样的 $\mathscr{R}$ 可被构造获得（非标准）实数（包含无穷小和无穷大）

分析可逐次展开，如 $\lim s_n = c$，c 是一个实数

$$(\forall \varepsilon)\left(\varepsilon > 0 \to (\exists n)\left(n \in \omega \wedge (\forall k)\left(k \in \omega \wedge k \geq n \to \left|s_k - c\right| < \varepsilon\right)\right)\right)$$

如实数集 B 上函数 f 在 $c \in B$ 连续

$$(\forall \varepsilon)(\varepsilon > 0 \to (\exists \delta)(\delta > 0 \wedge (\forall x)(x \in B \wedge |x - c| < \delta \to |f(x) - f(c)| < \varepsilon)))$$

许多标准分析的定理可在非标准分析得到更简单的证明，甚至得到更强的结果

非标准分析方法可推广到现代分析领域

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

5 数学基础

- 数学系统
- 带等词一阶系统
- 群论
- 一阶算术
- 形式集论
- 一致性问题

一阶算术

自然数和算术

数系：“自然数是上帝给的，其它东西都是人造的”（Kronecker）

逻辑上，自然数也是人造的

$$\mathbb{N} \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{R} \to \mathbb{C} \to \mathbb{H}$$

（自然数-整数-有理数-实数-复数-四元数）

算术化：把一个理论一一对应地映射到自然数，使得关于这个理论的对象可有一个有效的计算过程（算术）通过自然数找出对象

$$\mathbb{H} \Rightarrow \mathbb{C} \Rightarrow \mathbb{R} \Rightarrow \mathbb{Q} \Rightarrow \mathbb{Z} \Rightarrow \mathbb{N}$$

注

- 直觉主义：自然数是数学的基础，数学是由此构造的（构造是不能形式化的，而是直觉）
- 逻辑主义：数学是逻辑的一部分，自然数由逻辑定义，如数“2”定义为 $(\exists x)(\exists y)(P(x) \wedge P(y) \wedge x \neq y \wedge \forall z(P(z) \rightarrow z = x \vee z = y))$
  - 人（数学家）的智能活动不是这样思考数论的，因此逻辑主义只能作为一种数学哲学
  - 但是，人工智能活动可能跟人不一样，逻辑主义可作为人工智能的基础（人工智能的逻辑基础）
- 形式主义：自然数是由公理定义的（形式系统）
  - 每个数学理论都是形式系统，但还未能做到一个统一的（或足够广泛的）数学的形式系统

(朴素) 算术 N 的形式系统

N 是否可作为一个算术模型?

定义 5.23 (算术语言 $\mathscr{L}_N$)

令 $\mathscr{L}_N$ 是一个关于算术 (N) 的一阶语言，除变元、连接词、量词和技术性符号外，包括如下非逻辑符号

- 常元: a_1 (代表 0)
- 函项符: f_1^1, f_1^2, f_2^2 (后继、和与积)
- 谓词符: $=$

$\diamondsuit$

定义 5.24 (算术系统)

$\mathscr{N}$ 表示（一阶）算术系统（或称 Peano 算术 (PA)），它是增加了以下合适公理而得到的 $K_{\mathscr{L}_N}$ 的扩充（一阶理论）

- (E6-8) 的合适实例
- 下列六个公理及一个公理模式

定义（续）：算术公理

(N1) $(\forall x_1) \sim (f_1^1(x_1) = a_1)$

(N2) $(\forall x_1)(\forall x_2)(f_1^1(x_1) = f_1^1(x_2) \to x_1 = x_2)$

(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

记号

在 $\mathscr{L}_N$ 中，定义符号 $+$，$\times$ 和 $'$ 分别代替 f_1^2，f_2^2 和 f_1^1，即约定

- $t_1 + t_2$ 代表 $f_1^2(t_1, t_2)$
- $t_1 \times t_2$ 代表 $f_2^2(t_1, t_2)$
- t' 代表 $f_1^1(t)$
- 0 代表 a_1
- $f_1^1(x_1) \neq a_1$ 代表 $\sim(f_1^1(x_1) = a_1)$

$\mathscr{N}$ 中 (N1-7) 可重写成如下形式

算术公理

(N1*) $x_1' \neq 0$

(N2*) $x_1' = x_2' \to x_1 = x_2$

(N3*) $x_1 + 0 = x_1$

(N4*) $x_1 + x_2' = (x_1 + x_2)'$

(N5*) $x_1 \times 0 = 0$

(N6*) $x_1 \times x_2' = (x_1 \times x_2) + x_1$

(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 $\mathscr{A}(x_1)$，x_1 在其中自由出现

注

- (N1*-7*) 等价于它们（对变元 x_1，x_2）的全称闭式
- 由 (N7*) 用 MP 即归纳规则（导出规则，数学归纳法）

$$\mathscr{A}(0), \forall x(\mathscr{A}(x) \to \mathscr{A}(x')) \vdash_{\mathscr{N}} \forall x \mathscr{A}(x)$$

Peano 公设

(1) 0 是自然数

(2) 对每一自然数 n，存在另一自然数 n'

(3) 没有自然数 n，使得 n' 等于 0

(4) 对任意自然数 m 和 n，若 $m' = n'$，则 $m = n$

(5) 对任意包含 0 的自然数集 A，若当 $n \in A$ 时，$n' \in A$，则 A 包含每一个自然数

注

(a) 前两个 Peano 公设在 $\mathscr{N}$ 中没有任何对应的公理

因在 $\mathscr{L}_N$ 中，已包括了这些符号（0 和 $'$，或 a_1 和 f_1^1），它们在任一模型中有解释，即元素 $\bar{a}_1$ 存在，且对每个 x，元素 $\bar{f}_1^1(x)$ 存在，所以 $\mathscr{N}$ 不需要这两条公设

(b) (N7) 和 Peano 第五公设之间不是恰好对应的，它们都是数学归纳法原理的表达

- $\mathscr{N}$ 基于一阶语言 $\mathscr{L}_N$
- (N7) 是模式，有无穷个实例，因此 $\mathscr{N}$ 不是有限公理化
- Peano 第五公设包含二阶量词 “对任意的自然数集 A”，这需在二阶语言中表示

$$\forall A(A(0) \wedge \forall x(A(x) \to A(x+1)) \to \forall x A(x))$$

注（续）

(N7) 的实例形成 $\mathscr{L}_N$ 的公式的能枚举集，Peano 第五公设是关于自然数的所有集的语句，而所有集的集是不能枚举的，因此 (N7) 是有更多限制的归纳法原理的形式

- Peano 第五公设需要二阶逻辑（对应的是二阶算术）
- 一般地，二阶逻辑的公式不能等价规约到一阶逻辑的公式（完整的二阶逻辑是不完全的）

能枚举的 (N7) 的实例使得在逻辑中可使用数学归纳法证明

(c) Peano 公设并没有包含“和”或“积”的概念，这些函数（项）可用后继函数应用归纳法原理来定义，但在形式语言中包括这些符号是方便的

为确保在任意模型中，这些符号的解释有需要的性质，公理 (N3-6) 就是必要的

Peano 算术思想

- 朴素算术的概念不是最基本的，如“素数”“立方数”等是与一个数所具有的因子有关的，而这些因子又与乘法有关，有少数短语反复地出现，由此定义算术语言的基本成分
- 不致力于把推理的原则加以形式化，力图给出一个自然数性质的最小的集，从它出发，其余的算术性质能由推理而得

问题

PA 的元数学性质如何：完全性和一致性？（后面讨论）

搞怪公设

Peano 公设：试用一个未经定义的术语“神怪”来替代“自然数”，用两个未定义项“怪物”与“元”

- 怪物是一个神怪
- 每个神怪有一个元（它也是一个神怪）
- 怪物不是任何神怪的元
- 不同的神怪有不同的元
- 如果怪物有 x，且每个神怪都把 x 递送给它的元，那么所有的神怪都得到 x

注

- “自然数”概念是一个设法去定义的东西，Peano 公设所施加的限制是如此之强，以至于如果两个不同的人在心里对这些概念形成意象，这两个意象会有完全同构的结构，这“神怪”就是“自然数”
- 几何公设类似，如“点”，“线”，“面”可被替换为“椅子”，“桌子”，“水瓶”，这样几何画图的直觉就可不用（虽然数学直觉是很重要的）

命题 5.25

令 t, s 是 $\mathscr{L}_N$ 的项，下列公式是 $\mathscr{N}$ 的定理

(N1′) $t' \neq 0$

(N2′) $t' = s' \to t = s$

(N3′) $t + 0 = t$

(N4′) $t + s' = (t + s)'$

(N5′) $t \times 0 = 0$

(N6′) $t \times s' = (t \times s) + t$

证

(N1′-6′) 分别由 (N1*-6*) 推出：首先，用 Gen 考虑其全称闭式，用变元换名使得所有约束变元不出现在 t, s 中，最后，用 (R3) 于 t, s 即得 □

命题 5.26

对任意（$\mathscr{L}_N$ 的）项 t，s，r，下列公式是 $\mathscr{N}$ 的定理

(a) $t = r \to (t = s \to r = s)$

(b) $t = t$

(c) $t = r \to r = t$

(d) $t = r \to (r = s \to t = s)$

(e) $r = t \to (s = t \to r = s)$

(f) $t = r \to t + s = r + s$

(g) $t = r \to s + t = s + r$

(h) $t = r \to t \times s = r \times s$

(i) $t = r \to s \times t = s \times r$

(j) $t \times (r + s) = (t \times r) + (t \times r)$ （分配律）

证

(a) (E8) 实例

(b)

(1) $t+0=t$ (N3′)

(2) $(t+0=t)\to(t+0=t\to t=t)$ (a)

(3) $t+0=t\to t=t$ (1)(2)MP

(4) $t=t$

(j)

对 x_3 归纳证 $\vdash_{\mathscr{N}} x_1\times(x_2+x_3)=(x_1\times x_2)+(x_1\times x_3)$

其余留作练习 □

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

$0^{(n)}$ 称为数字项 ，数字项是闭项

命题 5.27

令 $m, n \in D_N$，若 $m \neq n$，则 $\vdash_{\mathscr{N}} \sim(0^{(m)} = 0^{(n)})$ ♢

证

不失一般性，设 $m < n$，则存在 $k > 0$，使得 $n = m + k$

由 (N2*) 可得

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

证 (续)

若 $m > 0$ ($m = 0$ 的情形是平凡的)

反复用 (N2*)，又用规则 HS，得

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

因 $k > 0$，$k\text{-}1 \in D_N$，且

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

实即 $\vdash_{\mathscr{N}} 0\overbrace{''\cdots'}^{k} = (0\overbrace{''\cdots'}^{k\text{-}1})'$，有

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

证 (续)

利用一个重言式，有

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

但 (N1*) 给出

$$\vdash_{\mathscr{N}} \sim(0^{(0)} = (0^{(k\text{-}1)})')$$

由 MP

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

□

命题 5.28

任何 $\mathscr{N}$ 的模型都是无穷的

证

据命题 5.27，任一 $\mathscr{N}$ 的模型中对象所对应的数字项是不同的，有（能枚举）无穷多的数字项

□

注

- $t < s$ 表示 $(\exists r)(r \neq 0 \wedge r + t = s)$，类似地，可引入不等式
- 完全归纳：$\vdash_{\mathscr{N}} (\forall x)((\forall z)(z < x \to \mathscr{A}(z)) \to \mathscr{A}(x)) \to (\forall x)\mathscr{A}(x)$
- 最小数归纳：$\vdash_{\mathscr{N}} (\exists x)\mathscr{A}(x) \to (\exists y)\mathscr{A}(y) \wedge (\forall z)(z < y \to \neg\mathscr{A}(z))$
- 其它如因子分解等都容易形式化，如 $t \mid s$ 表示 $(\exists z)(s = t \times z)$，由此展开形式数论

$\mathscr{N}$ 是一个带等词一阶系统

定义 5.29

一个解释 $\mathfrak{N}$，其中

- 论域是正整数
- 0 作为符号 0 的解释
- 后继操作（$+1$）是函数 $'$（即 f_1^1）的解释
- 朴素算术的加和乘是 $+$ 和 $\times$ 的解释
- 相等关系是 $=$ 的解释

是 $\mathscr{N}$ 的（规范）模型，称为标准模型

注

规范模型所需的等价类论域对正整数就是自身

一致性问题：标准模型

- $\mathscr{N}$ 的公理是否在 $\mathfrak{N}$ 为真尚未验证，直观上先认为可验证为真
- 若接受 $\mathfrak{N}$ 作为 $\mathscr{N}$ 的模型，则 $\mathscr{N}$ 是具有一致性，但这种论证是成问题

  因 $\mathfrak{N}$ 包含（朴素）集论（其论域及有关推理），这样证明的一致性是不牢靠的（依赖于集论的一致性）
- 若 $\mathfrak{N}$ 是一个模型，即 $\mathscr{N}$ 是一致的，对 $\mathscr{N}$ 任意（算术）公式 $\mathscr{A}$，$\mathscr{A}$ 或 $\sim\mathscr{A}$ 为真；若 $\mathscr{A}$ 或 $\sim\mathscr{A}$ 在 $\mathscr{N}$ 可证，则 $\mathscr{N}$ 就是完全的

$\mathscr{N}$ 有完全性定理与否取决于一致性

一致性问题：朴素模型

(朴素) 算术 N 应是一个算术模型，但 N 是算术系统 $\mathscr{N}$ 的（规范）模型吗？

若 N 是一个模型，即 $\mathscr{N}$ 是一致的，则 $\mathscr{N}$ 就是完全的

注

设 N 是算术模型，则可由 N 生成一个完全的一阶（算术）系统（定义 4.68），当然这个一阶系统不能有限公理化，亦不是 Peano 算术系统

没人怀疑算术的一致性，怎么办？

思路

算术系统 $\mathscr{N}$ 是不完全的（Gödel 不完全性定理）

若 $\mathscr{N}$ 是不完全的，则存在一个算术公式 $\mathscr{B}$，使得 $\mathscr{B}$ 或 $\sim\mathscr{B}$ 都不是定理，即 $\mathscr{B}$ 是不可判定的

注

设若 $\mathscr{N}$ 是完全的，则如同一阶逻辑，算术系统也是半可判定的，数论专家就得赋闲了：只要有足够的时间（姑且不考虑 NP 难解问题），他们领域里的任何问题都能够用机器证明

算术系统的一致性问题依赖于集论的一致性，而朴素集论发现了 Russell 悖论 $\Rightarrow$ 数学基础（危机）问题

- 数学系统
- 带等词一阶系统
- 群论
- 一阶算术
- 形式集论
- 一致性问题

形式集论

朴素集论（naive set theory）

一个集（合）是具有一定性质的对象的全体（相当于没定义的直观概念）

$$S = \{x \mid A(x)\}$$

隶属关系：$x \in S$

子集关系：若 $\forall x,\ x \in S \Rightarrow x \in S'$，则 S 包含于 S'，即 $S \subseteq S'$

S 是 S' 的子集

集中成员（元素）可以是集

问题

包含所有集的集是个什么集？

注

Cantor 不能枚举集和 Russell 悖论揭示存在非常大的对象，之前数学尚未能观察其结构

悖论 5.30 (Russell 悖论)

令 $R = \{x \mid x \notin x\}$，则 $R \in R \iff R \notin R$ ♢

R 定义为一个所有不含自身作为成员的集的集

若 $R \in R$，即 R 包含自身作为成员，按 R 的定义 $\Rightarrow$

R 为不含自身作为成员的集，即 R 不属于 R

则 $R \notin R$

若 $R \notin R$，即 R 不含自身作为成员，按 R 的定义 $\Rightarrow$

R 为不含自身作为成员的集，即 R 属于 R

则 $R \in R$

Russell 悖论

设 $\mathscr{R}(x)$ 为任一（含一个自由变元 x 的）公式

考虑　$\vdash \exists y \forall x(x \in y \leftrightarrow \mathscr{R}(x))$

令　$\mathscr{R}(x)$ 为 $x \notin x$ $(\sim x \in x)$，即 Russell 集

演算：消去存在量词和全称量词，可推出矛盾

$$y \in y \leftrightarrow y \notin y$$

语义：由 $\forall x(x \in y \leftrightarrow x \notin x) \models y \in y \leftrightarrow y \notin y$　$[\forall x \mathscr{A}(x) \models \mathscr{A}(x/y)]$

显然　$y \in y \leftrightarrow y \notin y$ 是不可满足的

因此　$\forall x(x \in y \leftrightarrow x \notin x)$ 亦不可满足

故　$\models \sim \exists y \forall x(x \in y \leftrightarrow x \notin x)$

即 Russell 集不存在

悖论反证 *

反证法：可通过构造一个悖论，如 Russell 悖论，证明不存在性结果

例

任何集不与它的幂集双射

证

设若一集 X 其幂集能从 X 枚举，即 $2^X = \{A_x \mid x \in X\}$

考虑集 $Y = \{x \in X \mid x \notin A_x\}$ 由所有不被包含在所枚举的 X 的子集的 X 中元素组成

因 Y 是 X 的子集，就有对某个 $y \in X$，$A_y = Y$

这样，若 $y \in Y$ 则 $y \notin Y$，若 $y \notin Y$ 则 $y \in Y$ □

取代 Cantor 对角线证法

注

- 符号 $\in$ 可不做隶属关系，以上证明就不只针对朴素集论，这个悖论具有普遍意义
- 自谓：语言的一种自指，即能陈述语言表达式自身的一种性质；否则，称为非自谓（“它谓”）

  如，“汉语”是自谓的，而“英语”是非自谓的

  “这个句子有九个汉字”是自谓的

  一般地，否定的自谓表达式会导致悖论

  如，“这个句子没有十个汉字”
- Russell 悖论与语义悖论是相通的

注

Russell （1901，Zermelo 1900）提出的悖论引发了第三次数学危机

Cantor 提出集论，即成为数学基础概念，Russell 悖论表明集的概念是不一致的，因此数学基础的危机本质上就是不能保证一致性

消除 Russell 悖论（1908）

- Russell 的类型论（type theory）
  1. 保留朴素集论：对集的抽象有所限制
  2. 改变语言：对象语言涉及自指需在元语言表达，从而避免悖论；元语言涉及自指需在元元语言表达，依次类推
- Zermelo 的公理化集论（axiomatic set theory）
  1. 公理化集的概念：对集的抽象不加限制
  2. 保留一阶语言：公理集论作为一阶系统（形式集论，描述集论）

公理化集论：ZF（Zermelo-Fraenkel）系统

定义 5.31 (一阶 ZF 语言)

ZF 的一阶语言 $\mathscr{L}_{ZF}$：变元、连接词、量词和技术性符号外

- 谓词符：$=$ (A_1^2)，A_2^2
- 没有函项符和常元

A_2^2 解释为隶属关系 $\in$，记 $t_1 \in t_2$ 表示 $A_2^2(t_1, t_2)$，$t_1 \notin t_2$ 表示 $\sim A_2^2(t_1, t_2)$

$\vdash_{ZF}$ 是 $\mathscr{L}_{ZF}$ 上的推理关系（简记 $\vdash$） ♢

注

- 没有常元和函项符意味着变元是唯一的项
- 变元 x_i 解释为集
- 原子公式只有形式 $x_i = x_j$ 或 $x_i \in x_j$

定义 5.32 (*ZF*)

ZF 作为 $K_{\mathscr{L}}$ 的扩充（带等词一阶理论）

- (E6) 和 (E8) 的所有合适的实例

  ((E7) 没有非平凡实例)

- 下述的公理 (ZF1) 到 (ZF8)

外延公理 (Axiom of Extensionality)

(ZF1) $(x_1 = x_2 \leftrightarrow (\forall x_3)(x_3 \in x_1 \leftrightarrow x_3 \in x_2))$

两集相等 当且仅当 它们有相同的元素

注

从左到右的蕴涵其实已由 (E9) 给出

记号

引入 $\subseteq$ 作为缩写符号

$t_1 \subseteq t_2$: $(\forall x_1)(x_1 \in t_1 \to x_1 \in t_2)$

t_1 和 t_2 是任意 ($\mathscr{L}_{ZF}$ 的) 项

$t_1 \subset t_2$: $t_1 \subseteq t_2 \wedge t_1 \neq t2$

注

易证如 $\vdash_{ZF} x_1 = x_2 \leftrightarrow (x_1 \subseteq x_2 \wedge x_2 \subseteq x_1)$ 等朴素集论命题 (子集)

空集公理 (Null Set Axiom)

(ZF2) $(\exists x_1)(\forall x_2)\sim(x_2 \in x_1)$

存在没有元素的集

注

在任何（规范）模型中，空集只有一个，这是作为 (ZF1) 的直接推论

记号

引入符号 $\varnothing$ 记空集，它起着常项的作用

(ZF2)： $(\forall x_2)\sim(x_2 \in \varnothing)$。

对集公理 (Axiom of Pairing)

(ZF3) $(\forall x_1)(\forall x_2)(\exists x_3)(\forall x_4)(x_4 \in x_3 \leftrightarrow (x_4 = x_1 \vee x_4 = x_2))$

给定任意集 x 和 y，存在其元素是 x 或 y 的集 z

注

该公理断言存在性 $(\exists x_3)$，易证

$$(\forall x_1)(\forall x_2)(\exists_1 x_3)(\forall x_4)(x_4 \in x_3 \leftrightarrow (x_4 = x_1 \vee x_4 = x_2))$$

可引入符号 $\{,\}$，$\{x_1, x_2\}$ 看作是项（无序对）

(ZF3)：$x_4 \in \{x_1, x_2\} \leftrightarrow (x_4 = x_1 \vee x_4 = x_2)$

有序对 $\langle x_1, x_2\rangle$ 表示为 $\{\{x_1\}, \{x_1, x_2\}\}$

并集公理 (Axiom of Unions)

(ZF4) $(\forall x_1)(\exists x_2)(\forall x_3)(x_3 \in x_2 \leftrightarrow (\exists x_4)(x_4 \in x_1 \wedge x_3 \in x_4))$

给定任意集 x，存在一个集 y，它以 x 的元素的所有元素为元素

记号

用 $\cup x_1$ 表示 (ZF4) 中断言存在的对象，把它看作一个项，引入 $\cup$ 作为函项 $(t_1 \cup t_2)$ 代表 $\cup\{t_1, t_2\}$

注

$x_1 \cap x_2$ 可定义为 $(\forall x_3)x_3 \in x_1 \cap x_2 \Leftrightarrow x_3 \in x_1 \wedge x_3 \in x_2$，$\bar{x_1}$ 可定义为 $(\forall x_2)x_2 \in \bar{x_1} \Leftrightarrow x_2 \notin x_1$，由此可推出有关集的并、交、补等运算

幂集公理 (Power Set Axiom)

(ZF5) $(\forall x_1)(\exists x_2)(\forall x_3)(x_3 \in x_2 \leftrightarrow x_3 \subseteq x_1)$

给定任意集 x，存在以 x 的所有子集作为元素的集 y

注

Cartesian 积 $x_1 \times x_2$ 可定义为

$$(\forall x_3)\left(x_3 \in x_1 \times x_2 \Leftrightarrow (\exists x_4)(\exists x_5)\left(x_3 = \langle x_4, x_5\rangle \wedge x_4 \in x_1 \wedge x_5 \in x_2\right)\right)$$

x_1^n 表示 $x_1^{n-1} \times x_1$，余如集上关系等可引入

替换公理模式 (Axiom Scheme of Replacement)

(ZF6) $(\forall x_1)(\exists_1 x_2)\mathscr{A}(x_1, x_2) \to$

$$(\forall x_3)(\exists x_4)(\forall x_5)(x_5 \in x_4 \leftrightarrow (\exists x_6)(x_6 \in x_3 \wedge \mathscr{A}(x_6, x_5)))$$

对每个公式 $\mathscr{A}(x_1, x_2)$，x_1, x_2 在其中自由出现

(不失一般性，假定量词 $(\forall x_5)$ 和 $(\forall x_6)$ 不在其中出现)

若公式 $\mathscr{A}$ 确定一个函项，则对任意集 x，存在一个集 y，它以所有 x 的元素在这函项下的象作为元素

无穷公理 (Axiom of Infinity)

(ZF7) $(\exists x_1)(\varnothing \in x_1 \wedge (\forall x_2)(x_2 \in x_1 \to x_2 \cup \{x_2\} \in x_1))$

$\{x_2\}$ 是 $\{x_2, x_2\}$ 的缩写

在任意模型中，无穷集存在

注

- 假若不把 (ZF7) 包括在公理组中，就无法保证形式系统与包括无穷集在内的朴素集合论有任何关系
- $\{\varnothing\} \in x_1, \{\varnothing, \{\varnothing\}\} \in x_1, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} \in x_1 \cdots$
- 令 0 表示 $\varnothing$，1 表示 $\{\varnothing\}$，2 表示 $\{\varnothing, \{\varnothing\}\} \cdots$，则对 $n \geq 0$，$\varnothing \neq 1$，$\varnothing \neq 2, 1 \neq 2$，$\varnothing \neq 3$，$1 \neq 3$，$2 \neq 3 \cdots$

  (von Neumann 定义自然数)

基础公理 (Axiom of Foundation)

(ZF8) $(\forall x_1)(\sim x_1 = \varnothing \to (\exists x_2)(x_2 \in x_1 \wedge \sim(\exists x_3)(x_3 \in x_2 \wedge x_3 \in x_1)))$

每一非空集 x 包含一个与 x 不相交的元素

注

这是为避免反直观的悖论，排除集以自身作为其元素的可能性而列入的技术性公理（排除 Russell 悖论，即 $\{x_1 \mid x_1 \in x_1\}$ 不合法）

- 进一步，形式化基数、序数等，可证明如超限归纳等，展开形式集论
- *ZF* 在排除 Russell 悖论前提下，保留了数学中所需用的（朴素）集论

注

ZF 变元解释为集，集中元素都是集，不能处理元素为非集的个体（如人、分子、公司等个体），但有推广的 *ZF* 系统可处理个体作为元素

ZFA (ZF with Atoms)：对象可为原子 (atoms/urelements)，原子可是集的元素，但不能是由其它元素组成

问题

ZF 是否还包含其它未发现的悖论？

数学基础

集 (论) 作为数学基础

$\Rightarrow$ 一个代数结构（如群）是一个集，其上有一些操作，满足一些公理

$\Rightarrow$ 一个空间（如拓扑）是一个集，其上有一些操作，满足一些公理

$\cdots\ \cdots$

ZF 作为数学（公理化）基础

假若 *ZF* 具有一致性，则它有（规范）模型

$\Rightarrow$ 算术系统 $\mathscr{N}$ 的模型可定义为 *ZF* 模型的子集

$\Rightarrow$ 自然数、后继函数和算术公理基于 *ZF* 模型的解释定义

$\Rightarrow$ 由自然数基于代数分析定义有理数、实数和复数

$\Rightarrow$ （可测集 $\Rightarrow$Lebesgue 测度论 $\Rightarrow$ 概率论

Dedekind 分割 $\Rightarrow$ 实数 $\Rightarrow$ 极限理论 $\Rightarrow$ 微积分）

ZF 的模型包含一个复数集，亦包含实数集作为子集

选择公理 (Axiom of Choice)

(AC) 对任一由互不相交的非空集组成的集 x，存在至少一个集 y，它与 x 的每一元素（非空集）恰好有一个公共元素

与以下两个等价陈述

Zorn 引理

若一个偏序集的每条链存在一个上确界，则该偏序集存在一个极大元

良序原理

每个集都是良序的（所有非空子集在全序关系下都存在最小元素）

注

- (AC) 独立于 ZF

注

- 选择公理被普遍使用，但有争议，如用选择公理可构造不可测集，但测度论需要（Lebesgue）可测集
- Banach-Tarski 悖论（分球问题）：把一个单位球体分成有限个点集（最少可分成五份），通过一些刚体运动（旋转和平移）再重新组合后可成为两个单位球体

  ——存在不可测集的结果

公理化集论 $ZFC = ZF + (AC)$

注

- 若 ZF 是一致的，则 ZFC 也是一致的
- (AC) 不会产生悖论，但可能导致反直觉的结果

  （如 Banach-Tarski 悖论）

类 *

- 基于形式集论，集不会导致 Russell 悖论，作为数学中集的概念
- 数学中（如 Bourbaki 学派），认为集作为数学基础是没危机的，一旦发现悖论总能通过引入新的公理加以限制或消除
- 朴素集改称为类（class），这样，类包含集；把不能作为（*ZFC*）集的类称为真（proper）类，这样，全体集是一个真类（类似地，全体代数结构（群）/空间（拓扑）是真类）（这种大对象通过范畴论处理）
- NGB 系统（von Neumann–Bernays–Gödel）通过排除真类的公理定义集，从而避免 Russell 悖论
- 计算机科学中，如程序语言，用类的概念（不需 ZFC 作为基础），通常不是真类，并引入过程机制（如 Python 类中方法），但有时需要处理真类的悖论问题（如 OWL (Web Ontology Lanuguage)），并与（数据）类型相关

Hilbert 无穷旅馆悖论

假设有一个拥有无穷（能枚举）多个房间的旅馆，且所有的房间均已客满。设想此时这一旅馆将可再接纳新的客人

一个新客人：由于旅馆拥有无穷个房间，因而可将在 1 号房间原有的客人安置到 2 号房间、2 号房间原有的客人安置到 3 号房间，以此类推，这样就空出了 1 号房间留给新的客人

类推之

有穷个新客人

无穷个新客人

无穷个客车且每个客车有无穷客人

有穷对无穷

该“悖论”事实上并不矛盾，仅是与直觉相悖

无穷集的性质与有穷集的性质并不相同

注（实无穷与潜无穷）

Hilbert 悖论常被用于反对实无穷的存在

哲学家 William Lane Craig 证明上帝的存在

“尽管在数学上这种旅馆（或任何无穷的事物）并非是不可能的，但从直觉上这样的事物永远不可能存在，不仅如此，任何实无穷都不可能存在。如果一个时间序列能够无穷地回退到过去那就会建立起一个实无穷，既然实无穷不存在，那时间就必然有个“起点”。每个事物都有其发生的原因，而时间起始的原因不可能是其他事物，只能是上帝。”

基数

基数：集中包含元素的“个数”（大小，通过映射定义）

自然数集 $\mathbb{N}$：与 $\mathbb{N}$ 能一一对应的集为能枚举集

$\mathbb{N}$ 的所有无穷子集都能与 $\mathbb{N}$ 一一对应

$\mathbb{N}$ 的基数记 $\aleph_0$（最小的无穷集基数）

实数集是不能枚举的（Cantor 对角证法或悖论反证）

实数集的基数，记作 c，代表连续统（直线）

构作逐个大的集，而这些巨集的元素已不可如实数描述

$\Rightarrow$ 需要集论

基数序列：$\aleph_0, \aleph_1, \cdots, \aleph_n \cdots$

注意 $c = 2^{\aleph_0}$

猜想

$c = \aleph_1$

连续统假设

(*CH*)　每个实数的无穷集或是能枚举的，或与全部实数有相同的基数

推广之，$\aleph_{n+1} = 2^{\aleph_n}$

广义连续统假设

(*GCH*)　对所有无穷基数 $\aleph$，都不存在介乎 $\aleph$ 与 $2^{\aleph}$ 之间的基数

注

Cantor（1874）提出，亦是 Hilbert（1900）提出的 23 个数学问题中的第一个

结果

- 一致性（Gödel 1938，内模型法）：(*AC*) 和 (*CH*) 都与 *ZF* 一致
- 独立性（Cohen 1963，力迫法）：(*AC*) 和 (*CH*) 都与 *ZF* 独立

- 数学系统
- 带等词一阶系统
- 群论
- 一阶算术
- 形式集论
- 一致性问题

一致性问题

任何一阶系统是一致的 当且仅当 它有一个模型

数学系统的一致性 $\Leftrightarrow$ 模型 ？

算术系统 $\mathscr{N}$ 的一致性 $\Leftrightarrow$ 算术模型 N ??

问题

考虑 *ZF* 的模型（解释）需要集的概念（解释的论域），如何回避由此引起的循环？

悖论 5.33 (Skolem 悖论)

按 Löwenheim-Skolem 定理，*ZF* 具有能枚举模型，而不能枚举集存在，*ZF* 似应有不能枚举模型 □

命题 5.34 (相对一致性)

令 S 是一个一阶系统，S^* 是 S 的扩充，若 S^* 是一致的，则 S 也是一致的 ♢

证

设 S^* 是一致的，但 S 是不一致的

对 S 的某个公式 $\mathscr{A}$，$\vdash_S \mathscr{A}$ 且 $\vdash_S \sim\mathscr{A}$

$\mathscr{A}$ 也是 S^* 的公式

且 S 中证明也是 S^* 的证明

$\vdash_{S^*} \mathscr{A}$ 且 $\vdash_{S^*} \sim\mathscr{A}$

这与 S^* 的一致性矛盾 □

例 5.35

由 ZF 的一致性可推出 $\mathscr{N}$ 的一致性

数学基础问题：绝对一致性

一阶逻辑具有绝对一致性，作为一阶系统是否有某个数学系统（如最基本的 *ZF*）具有一致性？

注

- Euclud 几何（经 Hilbert 改正）被认为有“几乎接近”完全性（因此有“几乎接近”一致性）

未解问题

尚未知 *ZF* 是否具有一致性

数学基础危机问题

- 数学第三次危机仍未解决
- 至今尚未发现明确的思想和技术路线解决 *ZF* 一致性问题（或其它数学系统的绝对一致性问题）
- 不建议在没有充分准备条件下立志解决这个数学的根本问题

数学基础问题 *

随堂讨论

范畴作为数学基础？

- 范畴（category）论（Eilenberg & Mac Lane，1942–45）：一个范畴包含对象和箭头（arrow，态射），其公理系统

  (1) 箭头的复合具有结合性

  (2) 有一个单（位）箭头

  范畴之间的映射称函子（functor），函子亦箭头，由范畴和函子可构造新范畴，函子亦对象，函子之间态射称自然变换。集（作为对象）范畴仅考虑结构（同构），而不需朴素集的构造（因此一致性是无关的）

- Topos （理）论：对集范畴，其公理系统

  (1) A 的子集 B 与其特征函数 $X : A \mapsto \{Truen, False\}$ 之间一一映射且对 A 中元素 a，$X(a) = true$ 当且仅当 a 在 B 中

  (2) 给定一个 A 中的 a 和一个函数 $h : A \mapsto A$，存在唯一个函数 $f : \mathbb{N} \mapsto A$ 使得 $f(n) = h^n(a)$

范畴作为数学基础？

- 集、群、自然数、序、序数等都定义为各种范畴
- 范畴论研究不同抽象数学结构之间的联系，需要全体对象（如幺半群）的结构性质，不可避免地会遇到大量的真类（因此一致性是有关的）
- 所有类放在一起不再是一个类，而是一个更高一级的类，以此类推，类似类型论，但用 Grothendieck 全集（universe）概念
- Grothendieck 全集是一个满足下列条件的集 U:
  - 若 $x \in u$ 且 $u \in U$，则 $x \in U$
  - 若 $u \in U$ 且 $v \in U$，则 $\{u, v\} \in U$
  - 若 $x \in u$，则 $P(x) \in U$（幂集）
  - 全体自然数集 $N \in U$
  - 若 $I \in U$ 且对任意 $x_i \in I$，则 $\cup_i x_i \in U$

  可证 U 是 ZFC 的模型

范畴作为数学基础？

- 基于 U，满足 $x \in U$ 的 x 称为 （U）小集；满足 $x \subset U$ 但 $x \notin U$ 的 x（不是 U 的元素的子集）称为（U）大集（取代真类），这样，在小集上可定义几乎一切数学结构（群、空间等），而全体对象（群、空间等）归为大集
- 全集公理：对任意集 x，存在一个 Grothendieck 全集 U 使得 $x \in U$

  例如，“全体大集”超出了 U 自身的范围，把它放到另一个更大的 Grothendieck 全集 V 中（类似于更高一层的类型）

范畴作为数学基础？

- Lawvere 基于 Grothendieck 的代数几何（范畴 + 拓扑，1950-1960）提出范畴论（尤其是 Topos）作为数学基础，Topos 论与直觉主义类型论直接相关（每个 Topos J 的内部语言 $\mathscr{L}(J)$ 是直觉主义类型论，每个直觉主义类型论 $\mathscr{L}$ 生成一个 topos $\mathcal{T}(\mathscr{L})$，通过范畴摹状词描述，它们之间构成不交的函子），而 Gödel 完全性定理和不完全性定理 仍然成立（逻辑 $\Leftrightarrow$ 范畴）
- Langlands 纲领（1967/1979）企图建立数学的统一理论，仍致力于解决一些基本数学问题（素数分类算术，猜想），未涉及元数学问题
- 无穷范畴（Jacob Lurie：Higher topos theory (pp.944, arxiv, 2006)，Higher algebra (pp.1553, 2011)）是一个新的数学基础（如，用等价取代相等），被认为是继代数几何后数学最大的进展之一，是近二十来数学的新发展，但未涉及数学基础危机问题
- 数学仍是诸侯（分支）封建，（统一的）数学基础尚未形成