哥德尔证明.

1. 导论.

① 几何学 ：定理：与人们的知觉一致

命题：作为一个明确的逻辑证明的结论而被确立

"公理化方法" (axiomatic method)

- 不加证明地接受某些命题为公理或公设. 基础
- 由公理推导出该系统所有其他命题作为定理. 上层结构

② 公理化方法有其固有的局限性. (连那熟悉的整数都无法被完全公理化)

→ 很大一类演绎系统（例如数论）都不可能建立在其内在的逻辑一致性.

（除非使用令人怀疑的推理原则）

2. 一致性问题

① 在给定的系统中，可以证明某些命题的不可能性.

(par excellence)

- 数学：仅是给出一组公理（或公设）得出其逻辑上蕴涵着的必然结论的学科.
  （而不管所给出的公理是否为真.） necessary logical consequence
- 数学的日益抽象

② 一致性：逻辑上不相容的陈述不可能同时都为真

（因此若一组陈述为真，则他们就是一致）

- 能否推出一对相互矛盾的定理？能否证明不能？

思路：为抽象公理找到一个"模型" model 从而令系统的每一个公理都可以转换为关于该模型的一个真陈述. （等价变换） (conjugacy)

但 · 模型是否存在的
· 公理适用的元素是否存在的.

③ 罗素悖论. 一类：
- 不包含自身为其元素 (normal)
- 包含自身为其元素 (non-normal)

∴ "N"是所有正常(normal)的类组成的类

3. 一致性的绝对证明 (希尔伯特)

①. 将演绎系统完全形式化 (complete formalization)

- (剥去词的符号，抽取意义)　公理/定理 → "符号串"
- 关于形式化数学系统的符号的陈述：元数学 (meta-mathematics) 陈述
  (它们是关于式的名称 name)

→ 研究对象本身和关于这个对象的讨论的区分
(数学)　(元数学)

②. "有穷性方法"：不能涉及公式的无穷多个结构属性，不能涉及对公式进行无穷的运算.
(finitistic)　将这样的一致性证明称"绝对的" (absolute)

③. "想要"一个这样的证明.

4. 形式逻辑的系统化　怀特海，罗素，《数学原理》

① 数学证明上常常会遗漏一些 思考认可的推论规则或逻辑定理.
(他们常被用得以致无意识的行为)
→ 形式逻辑的不完整

②. 乔治·布尔 (George Boole) 1847 《逻辑的数学分析》，发展逻辑代数
- 符号逻辑

③ 19世纪 ："算术化"代数和 infinitesimal calculus
- 证明了数学分析中使用的各种概念都可以只用数论的词汇 (整数及整数运算) 定义.

④ a. 罗素试图证明：所有的数论概念都可以纯逻辑的概念来定义.
- 所有的数论公理都可以从很少几条、可以被确认为纯逻辑 (logical truth) 的基本命题中演绎出来.

(数论一致性 → 形式逻辑一致性)

⑤ a). 提供了合适的记号系统. (以编码纯数学的陈述)
b). 明确了数学证明中所用的大部分形式推论规则.

5. 一致性的绝对证明：数中之例

① 《数学原理》：初等命题逻辑的形式化

a). 准备 vocabulary ; b). formation rules (sentences, grammar)
c) transformation rules (推论规则)
d) choose axioms (primitive formulas). 公理

→ 推论出 theorem of the system (定理)

with proof (demonstration): 公式的有穷序列.

② · "句子变元" (sentential variables)

· 句子联结词 (sentential connectives): "~" 非, "∨" 或, "⊃" 如果,那么, "∧" 且

③ "公式": 基本符号的组合 (常见有句子形式), 定义出某个公式.

· 变元是公式

· 变元通过联结词组合起来的是公式

④ transformation rules:

a) (对句子变元的) 替换规则 (rule of substitution)

(统一替换公式中的变元以得到新的公式)

b) 分离规则 (rule of detachment, modus ponens)

(从具有 S_1 和 $S_1 \supset S_2$ 形式的公式, 总允许推出公式 S_2.)

⑤ 公理:

a) $(p \vee p) \supset p$

b) $p \supset (p \vee q)$

c) $(p \vee q) \supset (q \vee p)$

d) $(p \supset q) \supset ((r \vee p) \supset (r \vee q))$

Q 元数学的句子应该可以作为变元代入这些公理中去.

⑥ 证明这组公理不矛盾 (i.e. 不能推出 S, 又 ~S)

eg. Th: $p \supset (\sim p \supset q)$ (todo. prove it.)

· 若 S, we have $S \supset (\sim S \supset q) \Rightarrow \sim S \supset q$.

· since ~S we have q.

→ 不一致的公理可以推出任何公式

Q (元数学的推理) ← 这一部分的逻辑也应该公理化? 否则的话 元数学的推论的正确性由什么保证?

b) 证明思路: 如果不是每个公式都是一个定理, 那么这个演算是一致的.

→ left to prove. 至少有一个公式不能从这组公理推导出来.

· 找到满足以下条件的公式特征:

i) 这种特性四条公理共有

ii) 这个特性对转换规则具"遗传性" → 所有的定理都具这种特性

iii) 这个特性不能属于每一个按照系统的形成规则得到的公式 → ∃ 公式不具这种特性 (这个公式就不是从这些公理推出的定理)

· 重言属性 (tautology)

(Def: 排除了没有逻辑可能性的陈述. e.g. $p \vee \sim p$) always true.

6、映射观念及其在数学中的应用

（1931年 哥德尔证明：严格遵循希尔伯特及其后继的所有努力必然会失败。）

① 结论：a) 不可能为一个以包括整个算术的系统的一致性给出一个元数学的证明，

（除非该证明本身所用的推理规则在某些本质方面不同于在该系统内推导定理所用的转换规则）（"[illegible]"）

b) 证明了公理化方法有着根本的局限性

（《数学原理》或任何其他能在其中发展出的算术系统在本质上是不完全的）

（总有算术真理，不是形式上可推导的。）

（又一个系统能否证明本身是一致的或者是不一致的？）

② 方法：参照"理查德悖论"(Richard. Paradox)

• 首先（定义）把定义按字母数字排序，并与整数一一对应（映射）

• 一个整数可能会拥有与它相联系的定义指定的属性 → "非理查德数"

• "理查德属性"的定义 → 对应的整数为 n、 （~罗素悖论）

"n 为理查德数"同时为真又为假

• 问题：这个定义不属于先前的序列，这个定义是元数学的相关条件。

③ "映射"map：在"对象"的一个领域中具体化的相关抽象结构，可以被证明在另外一个领域的"对象"之间也成立。

（例：希腊将几何映射到代数上）

• 把形式化算术系统里的元数学陈述翻译（映射）成这个系统本身之内的算术陈述。

• 哥德尔的论证方法

7、哥德尔的证明

1、哥德尔编号（《数学原理》系统的改编）"PM"

"哥德尔数"

• 可以给每个基本符号、每个公式（符号串）以及每一个证明（公式有穷序列）指定唯一一个数

① 常项符号："~", "V", "⊃", "=", "0", "+", "×"

"(", ")", ",", "∃", "S" (immediate successor)

（前者具有通常的系统含义，但在演绎中是纯粹形式）

·1931年(定理五)，存在一个PM定理的类，其中每一条定理，按常规翻译后解释，都表达一个算术真理

Corresponding Lemma

·存在一个映射，将多种算术真理组成的类，其中每个真理，如果通过常规方式转换为形式陈述，都会得到PM的一条定理。

(陈述性真(定)理 与 符号形式真(定)理 的一一映射关系)

② 变元
- 数字变元 numerical variables (x, y, z) → {k}
- 句子变元 sentential variables (p, q, r) → {k^2}
- 谓词变元 predicate variables (P, Q, R) (以定义…) → {k^3}

(k>12，k为素数)

③
·以"(∃x)(x=sy)" as example) 唯一对应了一串数的序列 (a b c d e f g …)

·可以给这个序列指派一个唯一的数：(素数幂的积) ($2^a 3^b 5^c 7^d 11^e 13^f 17^g \ldots$)

⇒ 对应的哥德尔数

·证明的公式序列为：(m, n, j, k …) ⇒ ($2^m 3^n 5^j 7^k \ldots$)

⇒ 公式序列对应的哥德尔数

④ 从哥德尔数出发：
- x < 12 ：符号
- x > 12
  - 素数(或2/3次幂)：变元
  - 其他：变元与符号的组合，或公式，或公式序列…

{变元, 符号, 公式, 公式序列} ⟷ 哥德尔数 ⟷ $\mathbb{Z}^+$ (正整数集合)

2、元数学的算术化

① 关于形式演算中表达式的结构属性的所有元数学陈述，都可以被精确地反射到这个演算自身

· PM中每个表达式都与一个数相关联，因而关于形式表达式及其相互之间 typographical relation 的元数学陈述都可以被解释为关于相应的数及相互之间算术关系的陈述

② 元数学断言可以映射到整数域及其属性. (PM可以忠实地谈论它自己)

· "哥德尔数为x的公式序列是哥德尔数为z的公式(在PM中)的证明" ≡ Dem(x, z) (注意其形式性)

x与z之间的算术关系

例：Dem($\underbrace{ss\ldots sso}_{(x)}$, $\underbrace{ss\ldots sso}_{(z)}$)

~Dem(ss…sso, ss…sso)

③ (∃x)(x=sy) (17) → (m 哥德尔数)

代入

(∃x)(x=$\underbrace{s\ldots s}_{m+1个s}$o) → r 对应的哥德尔数

这个替换的操作 ⇒ sub(m, 17, m) 原始递归函数

这个操作本身不能叫真或假，因而不是个公式

(i.e. 在哥德尔数为m的公式中，把所有的"y"(17)用m替换)

三、核心

i) 公式G："使用PM的规则，公式G不是可证明的。"

ii) G是可证明的，当且仅当它的形式否定~G是可证明的。（若G和~G都可证明，则PM不一致）

iii) 尽管G不是形式地可证明的，它却是一个真的算术公式。

G在下述意义上为真：它认为，由某确切所定 义的某个算术属性不被任何整数所拥有。

iv) 由于G既是真的，又是（在PM中）形式不可判定的，因此PM一定是不完全的(incomplete)

（i.e. 我们不能从PM的公理和规则演绎出所有的算术真理）

v) A："PM是一致的"。

"A⊃G"在PM中形式地可证明，，A在PM中不可证明。

⇒ PM的一致性是无法用可以被反映在PM本身组成的形式推理系统中的任何逻辑推理链条来建立的。

证明细节：

i) "Dem(x, z)"　　"(∃x) Dem(x, z)" (PM系统内) (i.e. 哥德尔数为z的公式是可证明的)

"~(∃x)Dem(x, z)" (i.e. 哥德尔数为z的公式不可证明)

n⇒ "~(∃x) Dem(x, Sub(y, 17, y))" (i.e. 哥德尔数为 sub(y, 17, y) 的公式不可证明)

g= "~(∃x) Dem(x, Sub(n, 17, n))" (G) (没有未被约束的变元，G的意义是确定的)

g= sub(n, 17, n)

⟺ "~(∃x) Dem(x, g)" (i.e. G不可证明) □

ii) 若(G)可证明，则"(∃x) Dem(x, g)"即(~G)是可证明的。

(这里没有恶性循环的谬误，因为PM可以描述自己)

→ "G是可证明的 iff ~G可证明"

如果PM是一致的，那么G必然是形式不可判定的。

iii) "没有G的PM证明"，那么G断言了真理，G为真。

iv) Def (completeness)：每个能在此系统内表达的真陈述都是从公理出发根据规则可形式地推演的。

→ PM是不完全的 (前提假定PM是一致的)

且PM不仅是不完全的，且在本质上就是不完全的：即使给G添加一系列新的公理，扩充了的系统仍然不足以形式地产生所有算术真理。（扩张后的系统中仍可构造出一个新的G'）

(2) <u>如果PM是一致的，那么它是不完全的。</u>（可作形式化在PM中表征）

- ∴ $(\exists y)\sim(\exists x)Dem(x,y)$ (A) （i.e. PM是一致的）

（由G5，不一致的公理系统可以推出任何定理，那么只要有一个公式是不可推出的，则这个系统是一致的）

$(\exists y)\sim(\exists x)Dem(x,y) \supset \sim(\exists x)Dem(x, Sub(n,17,n))$ i.e. <u>"A→G"</u>

（可形式化地证明，这里省略）

- 假设A可证明，那么G可证明，那么PM不一致。→ A不可证明

8、总结性思考