

# 可计算性理论

杨睿之

复旦大学哲学学院

2021 年春季

# 课程信息

- 时间地点:

- 周二 18:30 - 21:05, HGX401

- 网站:

<https://aplacenearby.ggr.fun/recursion2021>

- 教材: André Nies, *Computability and Randomness*,  
Oxford University Press, 2009

《递归论：算法与随机性基础》，复旦大学出版社

- 参考: 《数理逻辑：证明及其限度》(第二版)

# 课程信息

## 考核

- 论文：带回去做的一组证明题

## 课程团队

- 杨睿之

邮箱：yangruizhi@fudan.edu.cn

- 刘桢

邮箱：19210160030@fudan.edu.cn

# 前情回顾

## 可计算性与随机性理论研究的对象

- 自然数集  $A \in P(\mathbb{N})$
- 自然数上的函数  $f \in \mathbb{N}^{\mathbb{N}}$
- 无穷 01 序列  $f \in 2^{\mathbb{N}}$
- 二叉树  $T \subset 2^{<\omega}$

## 前情回顾

### 定义 (部分递归函数)

假设  $\psi$  是自然数上的  $k$  元部分函数 ( $\text{dom } \psi \subset \mathbb{N}^k$  且  $\text{ran } \psi \subset \mathbb{N}$ ), 我们称  $\psi$  是部分可计算的 (partial computable), 当且仅当存在图灵机 (或计算机程序)  $P$  满足: 对任意  $x_1, \dots, x_k \in \mathbb{N}$ , 若  $(x_1, \dots, x_k) \in \text{dom } \psi$  (记作  $\psi(x_1, \dots, x_k) \downarrow$ ), 则有  $y \in \mathbb{N}$ ,  $\psi(x_1, \dots, x_k) = y$  且程序  $P$  在输入  $(x_1, \dots, x_k)$  后能停机并输出  $y$ ; 若  $(x_1, \dots, x_k) \notin \text{dom } \psi$  (记作  $\psi(x_1, \dots, x_k) \uparrow$ ), 则程序  $P$  在输入为  $(x_1, \dots, x_k)$  后不停机或没有输出。

# 前情回顾

## 定义

- 此时, 我们称  $P$  计算  $\psi$
- 如果  $\text{dom } \psi = \mathbb{N}^k$ , 我们称  $\psi$  是可计算的 (computable)
- 我们称集合  $A \subset \mathbb{N}$  是可计算的, 当且仅当它的特征函数是可计算的

# 前情回顾

## 记法

- 固定对  $k$  元输入程序的枚举  $\{P_e^{(k)}\}_{e \in \mathbb{N}}$ 。对每个  $e$ , 存在唯一的部分函数  $\psi$ , 使得  $P_e$  计算  $\psi$ , 记作  $\Phi_e^{(k)}$ 。此时, 称  $e$  是  $\psi$  的 **编号** (index)。通常仅考虑一元的输入, 省略上标 ( $k$ )。
- 任给部分函数  $\Phi, \Psi$ , 我们用  $\Phi(\bar{x}) = \Psi(\bar{y})$  表示: 或者  $\Phi, \Psi$  分别在  $\bar{x}$  和  $\bar{y}$  上有定义且值相等 (又记作  $\Phi(\bar{x}) \downarrow = \Psi(\bar{y}) \downarrow$ ), 或者两者都没定义 (即  $\Phi(\bar{x}) \uparrow$  且  $\Psi(\bar{y}) \uparrow$ )

## *s-m-n* 引理

### 引理

参数引理 (Parameter Lemma) 对每个二元的部分可计算函数  $\Theta$ , 存在一个严格递增的可计算函数  $q$ , 使得

$$\forall x \forall y \Phi_{q(x)}(y) = \Theta(x, y)$$

并且  $q$  的一个编号 ( $\ulcorner q \urcorner$ ) 可以由  $\Theta$  的编号能行且一地得到



## $s$ - $m$ - $n$ 引理

### 引理 ( $s$ - $m$ - $n$ 引理)

任给  $m, n \geq 1$ , 存在一一的可计算函数  $s : \mathbb{N}^{m+1} \rightarrow \mathbb{N}$ , 使得对任意  $e \in \mathbb{N}$ ,  $(x_1, \dots, x_m) \in \mathbb{N}^m$  和  $(y_1, \dots, y_n) \in \mathbb{N}^n$ , 都有

$$\Phi_{s(e, \bar{x})}^{(n)}(\bar{y}) = \Phi_e^{(n+m)}(\bar{x}, \bar{y})$$

$s$  的一个编号可以由  $m$  能行得到

**注意:** 递归论中, 常常可以通过 **统一性** (uniformity) 获得一个定理更一般的形式

# 通用图灵机

## 事实

存在通用图灵机（计算的部分递归函数） $\Xi$ ，对任意  
 $e, x \in \mathbb{N}$  有

$$\Xi(e, x) = \Phi_e(x)$$

# 充数定理

## 引理 (充数定理 (Padding Lemma) )

任给  $e$  和  $m$ , 可以**能行地**得到  $e' > m$  使得程序  $\Phi_{e'} = \Phi_e$ 。

注意:

- 充数定理的构造是统一的
- 充数定理常被用来构造——、严格递增的可计算函数

# 递归定理

定理 (不动点定理 (Fixed Point Theorem) )

令  $g : \mathbb{N} \rightarrow \mathbb{N}$  是可计算函数, 那么存在  $e$  使得  $\Phi_{g(e)} = \Phi_e$

我们称  $e$  是  $g$  的不动点。  $e$  可以通过  $g$  的编号能行地得到

证明.

令  $\Theta(z, x) = \Xi(g(\Phi_z(z)), x) = \Phi_{g(\Phi_z(z))}(x)$ 。由参数引理, 存在

可计算函数  $q$  使得  $\forall z \forall x \Phi_{q(z)}(x) = \Theta(z, x) = \Phi_{g(\Phi_z(z))}(x)$ 。取

$d$  使得  $q = \Phi_d$ 。则  $e = q(d) = \Phi_d(d)$  是所求的不动点

# 递归定理

## 定理 (带参数的递归定理)

令  $g : \mathbb{N}^2 \rightarrow \mathbb{N}$  是可计算函数, 那么存在可计算函数  $f$  使得

$$\Phi_{g(f(n),n)} = \Phi_{f(n)}$$

对所有  $n \in \mathbb{N}$  成立。且  $f$  (的编号) 可以由  $g$  (的编号) 能行得到。

# 递归可枚举集

## 定义

称集合  $A \subset \mathbb{N}$  是 **递归可枚举的** (r.e.) / **可计算可枚举的** (c.e.), 当且仅当  $A$  是某个部分可计算函数的定义域

由于可以能行地枚举所有 (一元) 部分可计算函数  $\{\Phi_e\}_{e \in \mathbb{N}}$ , 也可以能行地枚举所有递归可枚举集

$$W_e = \text{dom } \Phi_e$$

# 递归可枚举集

## 记法

我们称集合序列  $\langle S_e \rangle_{e \in \mathbb{N}}$  是 **统一地递归可枚举的** (uniformly computable enumerable), 当且仅当集合  $\{(e, x) \mid x \in S_e\}$  是递归可枚举的

## 事实

- $\langle W_e \rangle_{e \in \mathbb{N}}$  是统一地递归可枚举的。
- 若  $\langle S_e \rangle_{e \in \mathbb{N}}$  是统一地 c.e. 的, 则存在可计算函数  $q$  使得

$$\forall e \ S_e = W_{q(e)}$$

# 递归可枚举集

## 记法

我们称集合  $A \subset \mathbb{N}$  是 **可计算的**，当且仅当它的特征函数是可计算函数。

## 事实

集合  $A \subset \mathbb{N}$  是可计算的，当且仅当  $A$  和  $\mathbb{N} \setminus A$  是 c.e. 的



# 递归可枚举集

例

停机问题 (halting problem)

$$\emptyset' = \{e \mid e \in W_e\} = \{e \mid \Phi_e(e) \downarrow\}$$

是 c.e. 的, 但不是可计算的

# 递归可枚举集

## 记法

我们用  $\Phi_{e,s}(x) = y$  或  $\Phi_{e,s}(x) \downarrow = y$  表示程序  $P_e$  输入  $x$  在允许  $s$  步内停机并输出  $y$ 。用  $\Phi_{e,s}(x) \downarrow$  表示

$\exists y \Phi_{e,s}(x) = y$ ，否则用  $\Phi_{e,s}(x) \uparrow$  表示。

此外，定义  $W_{e,s} = \text{dom } \Phi_{e,s}$

# 递归可枚举集

## 事实

下列是可计算的

- 集合  $\{(e, s, x) \mid \Phi_{e,s}(x) \downarrow\}$
- 函数

$$f(e, s, x) = \begin{cases} \Phi_{e,s}(x) + 1, & \text{若 } \Phi_{e,s}(x) \downarrow, \\ 0, & \text{否则} \end{cases}$$

直观上,  $(e, s) \mapsto W_{e,s}$  也是可计算的

# 递归可枚举集

## 定义

定义对有穷自然数集合的编码, 令

- $D_0 = \emptyset$
- 对  $n = 2^{x_1} + \dots + 2^{x_r}$ , 其中  $x_1 < \dots < x_r \in \mathbb{N}$ , 令

$$D_n = \{x_1, \dots, x_r\}$$

我们称  $n$  是  $D_n$  的 **强编码** (strong index)

## 事实

函数  $(e, s) \mapsto W_{e,s}$  (的强编码) 是可计算的

# 递归可枚举集

## 定义

我们定义集合  $A$  的一个 **可计算枚举** (computable enumeration) 是一个有穷自然数集 (的强编码) 序列  $\langle A_s \rangle_{s \in \mathbb{N}}$ , 其中每个  $s$  有  $A_s \subset A_{s+1}$ , 并且  $\bigcup_s A_s = A$

**注意:** 总是可以要求一个可计算枚举满足  $|A_{s+1} \setminus A_s| \leq 1$

## 事实

- 若  $A$  有一个可计算枚举  $\langle A_s \rangle_{s \in \mathbb{N}}$ , 则  $A$  是 c.e. 的
- 对每个  $e \in \mathbb{N}$ ,  $\langle W_{e,s} \rangle_{s \in \mathbb{N}}$  是  $W_e$  的一个可计算枚举

# 递归可枚举集

## 事实

- 对每个部分可计算函数  $\Phi$ ,  $\text{ran } \Phi$  是 c.e. 的
- 任给 c.e. 集合  $A$ , 可以统一地得到部分可计算函数  $\Psi$  使得  $\text{dom } \Psi$  是  $\mathbb{N}$  的前段且  $\text{ran } \Psi = A$  (习题)

因而集合  $A$  是 c.e. 的, 当且仅当  $A$  是某个部分可计算函数的值域

# 多一归约

## 定义

称集合  $X$  可以多一归约到  $Y$  (many-one reducible), 记作  $X \leq_m Y$ , 当且仅当存在一个可计算函数  $f: \mathbb{N} \rightarrow \mathbb{N}$  使得对任意  $n$  有

$$n \in X \leftrightarrow f(n) \in Y$$

## 例

- $0' \leq_m \{(e, n) \mid \Phi_e(n) \downarrow\}$
- 若  $X$  是可计算的,  $Y \neq \emptyset$  且  $Y \neq \mathbb{N}$ , 则  $X \leq_m Y$

## 多一归约

### 定理

集合  $A$  是 c.e. 的, 当且仅当  $A \leq_m 0'$ 。并且我们可以能行地从  $A$  的一个递归可枚举集编号 (例如  $A = W_e$  的  $e$ ) 得到一个见证  $A \leq_m 0'$  的多一归约函数的编号

我们称  $0'$  是  $m$ -完全的 c.e. 集, 即对任何 c.e. 集  $A$  有  $A \leq_m 0'$



# 图灵归约

## 定义

- 我们用  $P_e$  表示以  $e$  为编号的带信息源的图灵机程序, 用  $\Phi_e^Y$  表示程序  $P_e$  在信息源  $Y$  下运行对应的部分函数。其中  $\Phi_e$  被称作一个 **图灵函项** (Turing functional)
- 我们称一个完全函数  $f$  可以**图灵归约到**  $Y$  (Turing reducible) 或 **在  $Y$  中可计算**, 记作  $f \leq_T Y$ , 当且仅当存在  $e$  使得  $f = \Phi_e^Y$ 。
- 集合  $X \leq_T Y$ , 当且仅当  $X$  的特征函数在  $Y$  中可计算

# 图灵跃迁

## 定义 (图灵跃迁)

- 令部分函数  $J^Y(e) = \Phi_e^Y(e)$ 。定义集合  $Y' = \text{dom } J^Y$ , 称为  $Y$  的图灵跃迁 (Turing jump), 我们把映射  $Y \mapsto Y'$  称作跃迁算子 (jump operator)
- 递归定义  $Y^{(n)}$ :  $Y^{(0)} = Y$ ,  $Y^{(n+1)} = (Y^{(n)})'$

# 相对化

通过定义、证明的相对化 (relativization), 很容易把一些概念和定理改造成带信息源的版本

例

记法

$\Phi_e^Y(n)$ 、 $\Phi_e^Y(n) \downarrow$ 、 $\Phi_e^Y(n) \uparrow$ 、 $\Phi_{e,s}^Y(n) \downarrow$ ,  $W_e^Y$  .....

事实

$\{(e, s, x) \mid \Phi_{e,s}^Y(x) \downarrow\}$ 、函数  $(e, s) \mapsto W_{e,s}^Y$  都是  $Y$  中可计算的

# 相对化

## 定义

称集合  $A$  是  $Y$  中 c.e. 的, 当且仅当存在  $e$  使得

$$A = W_e^Y = \text{dom } \Phi_e^Y$$

## 事实

集合  $A$  是  $Y$  中可计算的, 当且仅当  $A$  和  $\mathbb{N} \setminus A$  是  $Y$  中 c.e. 的

# 相对化

## 引理 (带信息源的参数引理)

对任何图灵函项  $\Theta$ , 存在可计算的函数  $q$ , 使得对任意信息源  $Y$ , 任意  $e, x$  有

$$\Phi_{q(e)}^Y(x) = \Theta^Y(e, x)$$

# 相对化

## 定理 (带信息源带参数的递归定理)

对每个可计算的二元函数  $g$ , 存在可计算函数  $f$  使得, 对任意信息源  $Y$  任意  $n$ ,

$$\Phi_{g(f(n),n)}^Y = \Phi_{f(n)}^Y$$

# 相对化

## 事实

$A$  是  $Y$  中 c.e. 的, 当且仅当  $A \leq_m Y'$

特别地,  $Y'$  是  $Y$  中 c.e. 的。此外,  $Y \leq_m Y'$

## 事实

$Y' \not\leq_T Y$ , 故  $Y <_T Y'$ 。进一步, 对所有  $n$  有  $Y^{(n)} <_m Y^{(n+1)}$

# 相对化

## 事实

$X \leq_T Y$ , 当且仅当  $X' \leq_m Y'$

## 证明.

( $\Rightarrow$ )  $X'$  在  $X$  中 c.e., 因而在  $Y$  中 c.e., 故  $X' \leq_m Y'$

( $\Leftarrow$ ) 由  $X \leq_m X' \leq_m Y'$  且  $\mathbb{N} \setminus X \leq_m X' \leq_m Y'$ , 故  $X$  和  $\mathbb{N} \setminus X$  都在  $Y$  中 c.e.



## 习题

1.1.7, 1.1.12\*, 1.1.17 - 1.1.20, 1.2.4, 1.2.5\*, 1.2.7

# 下期预告

- 使用函数
- 真值表与弱真值表归约
- 集合的定义复杂度