一阶逻辑（一）

第六章 - 递归论基础

姚宁远

复旦大学哲学学院

November 1, 2021

目录

初始函数的定义

定义

自然数 $\mathbb{N}$ 中的以下三类函数称为初始函数：

1. 零函数 $Z(x) = 0$；
2. 后继函数 $S(x) = x + 1$；
3. 投射函数 $\pi_i^n(x_1, ..., x_i, ..., x_n) = x_i$；

注

投射函数 $\pi_1^1(x)$ 是恒等函数 $x \mapsto x$；

函数的原始递归

定义

设 $g:\mathbb{N}^n \to \mathbb{N}$ 与 $h:\mathbb{N}^{n+2} \to \mathbb{N}$ 分别为 n-元与 $n+2$-元函数。我们称 $f:\mathbb{N}^{n+1} \to \mathbb{N}$ 是从 g 和 h经原始递归而得到的，如果

1. $f(\bar{x}, 0) = g(\bar{x})$;
2. $f(\bar{x}, n+1) = h(\bar{x}, f(\bar{x}, n), n)$;

注：单变量递归函数

当 $n = 0$ 时，$g = c$ 是常函数。

1. $f(0) = c$;
2. $f(n+1) = h(f(n), n)$;

原始递归函数的定义

定义

全体原始递归函数的集合 C 是最小的满足以下条件的自然数上的函数集合：

(1) 初始函数 $\subseteq C$;

(2) C 对复合封闭;

(3) C 对原始递归封闭;

称 C 中的元素为原始递归函数。

注

- 定义 $\mathcal{C}$ 为满足条件 (1)，(2)，(3) 的函数的集合。则

  $$C = \bigcap \mathcal{C}$$

  是原始递归函数的集合。

- 定义 $\mathcal{C}_0$ 为初等函数的集合；

  设 C_n 已定义

  则 C_{n+1} 为 C_n 中的函数通过复合运算和原始递归而得到的函数集合；

  $$C = \bigcup_{n \in \mathbb{N}} \mathcal{C}_n.$$

  是原始递归函数的集合。

自然数上的加法

- $x + 0 = x$
- $x + (y + 1) = S(x + y)$

加法的生成序列

- $S(x_1)$
- $\pi_1^1(x_1) = x_1$
- $\pi_3^3(x_1, x_2, x_3) = x_3$
- $h(x_1, x_2, x_3) = S \circ \pi_3^3(x_1, x_2, x_3) = S(x_3)$
- $f(x_1, 0) = \pi_1^1(x_1)$
- $f(x_1, x_2 + 1) = h(x_1, x_2, f(x_1, x_2))$

引理

下列函数都是原始递归函数。

1. n-元常函数 $C_k^n(x_1, \ldots, x_n) = k$；
2. $x \cdot y$， x^y， $x!$
3. 非零检查函数与零检测函数

$$\sigma(x) = \begin{cases} 0, & \text{如果} x = 0 \\ 1, & \text{如果} x \neq 0 \end{cases} \qquad \delta(x) = \begin{cases} 1, & \text{如果} x = 0 \\ 0, & \text{如果} x \neq 0 \end{cases}$$

4. 前驱函数 $\mathrm{pred}(x)$
5. 截断减法

$$x \dot{-} y = \begin{cases} 0, & \text{如果} x < y \\ x - y, & \text{如果} x \geq y. \end{cases}$$

证明： n-元常函数是原始递归函数

- $\pi_1^n(x_1, ..., x_n) = x_1$;
- $Z(x_1) = 0$;
- $S^k(0) = k$;

证明： $x \cdot y$， x^y， $x!$ 是原始递归函数

- $x \cdot 0 = 0$;
- $x \cdot (n+1) = (x \cdot n) + x$;

- $x^0 = 1$;
- $x^{n+1} = (x^n) \cdot x$;

- $0! = 1$;
- $(n+1)! = n! \cdot (n+1)$;

证明：非零检测函数与零检测函数是原始递归函数

- $\sigma(0) = 0$;
- $\sigma(n+1) = C_1^2(n, \sigma(n))$;

- $\delta(0) = 1$;
- $\delta(n+1) = C_0^2(n, \delta(n))$;

证明：前驱函数是原始递归函数

- $\mathsf{pred}(0) = 0$;
- $\mathsf{pred}(n+1) = \pi^2_1(n, \mathsf{pred}(n))$;

证明：截断减法是原始递归函数

- $x \dot{-} 0 = x$;
- $x \dot{-} (y+1) = \mathrm{pred}(x \dot{-} y)$;

引理

设 $f : \mathbb{N}^k \to \mathbb{N}$ 是原始递归函数。定义一个新的函数 $g : \mathbb{N}^r \to \mathbb{N}$ 为

$$g(x_1, ..., x_r) = f(y_1, ..., y_k)$$

其中 y_j 或者是 x_i 或者是常数。则 g 也是原始递归函数。

证明:

定义一组函数 $h_1, ..., h_k : \mathbb{N}^r \to \mathbb{N}$ 为

- 若 y_j 是变元 x_i, 则 $h_j(x_1, ..., x_r) = \pi_i^r(x_1, ..., x_r)$;
- 若 y_j 是常数 $k \in \mathbb{N}$, 则 $h_j(x_1, ..., x_r) = C_k^r(x_1, ..., x_r)$.

则

$$g(x_1, ..., x_r) = f(h_1(x_1, ..., x_r), ..., h_k(x_1, ..., x_r)).$$

原始递归集合

特征函数

设 $R \subseteq \mathbb{N}^k$，则 R 的特征函数 $\chi_R : \mathbb{N}^k \to \{0,1\}$ 定义为

$$\chi_R(\bar{x}) = \begin{cases} 1, & \text{如果}\bar{x} \in R \\ 0, & \text{如果}\bar{x} \notin R. \end{cases}$$

特征函数

称 $\mathbb{N}^k$ 的子集 A（或者一个 k-元谓词 P）是原始递归的，如果其特征函数是原始递归的。

引理

1. 如果 $A, B \subseteq \mathbb{N}^k$ 是原始递归的，则 $\mathbb{N}^k \backslash A$, $A \cup B$ 和 $A \cap B$ 也是原始递归的；
2. 如果 P, Q 是原始递归谓词，则 $\neg P$， $P \vee Q$， $P \wedge Q$ 也是原始递归的。

证明：

设 χ_A, χ_B 是原始递归函数，则

- $\chi_{\mathbb{N}^k \setminus A}(x) = 1 \dot{-} \chi_A(x)$ 是原始递归的;
- $\chi_{A \cup B}(x) = \sigma(\chi_A(x) + \chi_B(x))$ 是原始递归的;
- $\chi_{A \cap B}(x) = \chi_A(x) \cdot \chi_B(x)$ 是原始递归的;

注

如果 $f : \mathbb{N}^k \to \mathbb{N}$ 是原始递归函数，则

$$\{x \in \mathbb{N}^k |\ f(x) = 0\}$$

$$\{x \in \mathbb{N}^k |\ f(x) > 0\}$$

都是原始递归的。

引理

如果 f_1, f_2 都是 k-元原始递归函数，P 是原始递归谓词，则

$$f(\bar{x}) = \begin{cases} f_1(\bar{x}), & \text{如果} P(\bar{x}) \\ f_2(\bar{x}), & \text{否则}, \end{cases}$$

也是原始递归的。

证明

$$f(x) = \chi_p(x) f_1(x) + (1 \dot{-} \chi_P(x)) f_2(x).$$

商 $\mathrm{quo}(x, y)$ 与余数 $\mathrm{rem}(x, y)$

商 $\mathrm{quo}(x, y)$ 与余数 $\mathrm{rem}(x, y)$

1. $\mathrm{quo}(x, y)$ 表示 x 除 y 的商；
2. $\mathrm{rem}(x, y)$ 表示 x 除 y 的余数；
3. $y = \mathrm{quo}(x, y)x + \mathrm{rem}(x, y)$，$\mathrm{rem}(x, y) < x$。

商 $\mathrm{quo}(x, y)$ 与余数 $\mathrm{rem}(x, y)$

引理

函数 $\mathrm{quo}(x, y)$ 和 $\mathrm{rem}(x, y)$ 都是原始递归的。

证明 I

$$\mathrm{rem}(x, y+1) = \begin{cases} \mathrm{rem}(x, y)+1, & \text{如果 } \mathrm{rem}(x, y)+1 < x \\ 0, & \text{否则。} \end{cases}$$

$$\mathrm{quo}(x, y+1) = \begin{cases} \mathrm{quo}(x, y), & \text{如果 } \mathrm{rem}(x, y)+1 < x \\ \mathrm{quo}(x, y)+1, & \text{否则。} \end{cases}$$

证明 II

$$\mathrm{rem}(x,0)=0,\ \mathrm{rem}(x,y+1)=(\mathrm{rem}(x,y)+1)\sigma(x-\mathrm{rem}(x,y)-1)$$

$$\begin{aligned}\mathrm{quo}(x,0)=0,\ \mathrm{quo}(x,y+1)=&\,\mathrm{quo}(x,y)\sigma(x-\mathrm{rem}(x,y)-1)+\\&(\mathrm{quo}(x,y)+1)\delta(x-\mathrm{rem}(x,y)-1)\end{aligned}$$

有界量词

有界量词

1. 定义 $(\exists x < a)\phi(x)$ 为 $\exists x(x < a \wedge \phi(x))$；
2. 定义 $(\forall x < a)\phi(x)$ 为 $\forall x(x < a \to \phi(x))$；

称形如 $(\exists x < a)$ 和 $(\forall x < a)$ 的量词为**有界量词**。

有界极小算子 μ

定义

设 $P(\bar{x}, z)$ 是一个 $k+1$-元谓词。定义

$$(\mu z \leq y) P(\bar{x}, z) = \begin{cases} \text{最小的满足} P(\bar{x}, z) \text{且} \leq y \text{的} z, & \text{如果它存在} \\ y+1, & \text{否则。} \end{cases}$$

$$P(\bar{x}, 0)?, \quad P(\bar{x}, 1)?, \quad \ldots \quad P(\bar{x}, k)? \quad \ldots$$

引理

如果 $f(\bar{x}, y)$ 是原始递归的，则有界和与有界积

$$\sum_{y \leq z} f(\bar{x}, y), \quad \Pi_{y \leq z} f(\bar{x}, y)$$

都是原始递归的。

证明

引理

令

$$F(\bar{x}, z) = \sum_{y \leq z} f(\bar{x}, y), \quad G(\bar{x}, z) = Pi_{y \leq z} f(\bar{x}, y)$$

则

$$F(\bar{x}, 0) = f(\bar{x}, 0), \quad F(\bar{x}, n+1) = F(\bar{x}, n) + f(\bar{x}, n+1),$$

且

$$G(\bar{x}, 0) = f(\bar{x}, 0), \quad F(\bar{x}, n+1) = F(\bar{x}, n) \times f(\bar{x}, n+1),$$

引理

如果 $P(\bar{x}, y)$ 是原始递归的谓词，则

1. 谓词
$$E(\bar{x}, y) := (\exists z \leq y) P(\bar{x}, z) \text{ 和 } A(\bar{x}, y) := (\forall z \leq y) P(\bar{x}, z)$$
都是原始递归的；
2. 函数
$$f(\bar{x}, y) := (\mu z \leq y) P(\bar{x}, z)$$
是原始递归的。

证明

1. $$\chi_E(\bar{x}, y) = \sigma(\sum_{z \le y} \chi_P(\bar{x}, z))$$

2. $$(\forall z \le y)P(\bar{x}, z) \iff \neg(\exists z \le y)\neg P(\bar{x}, z)$$

3. $(\mu z \le y)P(\bar{x}, z)$ 可以用 χ_P 计算

$$(\mu z \le y)P(\bar{x}, z) = \sum_{k \le y} \prod_{z \le k}(1 - \chi_P(\bar{x}, z))$$

引理

1. 谓词“x 整除 y”是原始递归的；
2. 谓词“x 是合数”与“x 是素数”是原始递归的；
3. 函数 $p : \mathbb{N} \to \mathbb{N}$，$n \mapsto$“第 n 个素数”是原始递归的。

证明

1. $$x \mid y \iff x \le y \wedge \mathrm{rem}(x,y)=0 \iff \exists z < y(y = x \times z)$$

2. 谓词“x 是合数” $\iff \exists z < x(z \mid x \wedge z > 1)$；

3. “x 是素数” $\iff \forall z < x(z > 1 \to z \nmid x)$；

4. $$p(0)=2,\ p(n{+}1) = \left(\mu z \le y\right)(z > p(n) \wedge z\text{是素数} \wedge y = (p(n)!+1$$

用 p_k 表示第 k 个素数，2 是第 0 个素数。

哥德尔数

- $<a_0, ..., a_n>$ 表示 $p_0^{a_0+1}...p_n^{a_{n+1}+1}$，称之为序列 $(a_0, ..., a_n)$ 的哥德尔数；
- 空序列 $<>$ 的哥德尔数是 1；
- 定义函数 $\mathrm{lh} : \mathbb{N} \to \mathbb{N}$ 为 $\mathrm{lh}(a) = \mu k \leq a(p_k \nmid a)$，称 lh 为长度函数;
- 对任意的哥德尔数 $a =< a_0, ..., a_n >$，$\mathrm{lh}(a) = n + 1$;
- 定义函数 $(a)_i : \mathbb{N}^2 \to \mathbb{N}$ 为 $(a)_i = (\mu k \leq a)(p_i^{k+2} \nmid a)$，称 $(a)_i$ 为分量函数;
- 对任意的哥德尔数 $a =< a_0, ..., a_n >$，$(a)_i = a_i$;
- 定义串接函数 $\hat{}: \mathbb{N}^2 \to \mathbb{N}$ 为

$$a\hat{}b = a \cdot \prod_{i<\mathrm{lh}(b)} p_{\mathrm{lh}(a)+i}^{(b)_i+1}.$$

引理

1. 哥德尔数的集合是原始递归的；
2. $\mathrm{lh}(a)$ 和 $(a)_i$ 是原始递归的；
3. 函数 $a\hat{}b$ 是原始递归的且

$$< a_0, ..., a_n > \hat{} < b_0, ..., b_m > = < a_0, ..., a_n, b_0, ..., b_m > .$$

证明

1. x 是哥德尔数

$$\exists n \leq x \left(\forall i \leq n (p_i \mid x) \;\wedge\; \forall j \leq x (j > n \to p_j \nmid x) \right)$$

2. $\mathrm{lh}(a) = \mu k \leq a (p_k \nmid a)$ 和 $(a)_i = \mu k \leq a (p_i^{k+2} \nmid a)$ 显然是原始递归的。

3.
$$a \hat{} b = a \cdot \prod_{i < \mathrm{lh}(b)} p_{\mathrm{lh}(a)+i}^{(b)_i+1}.$$

显然原始递归。

$$< a_0, ..., a_n > \hat{} < b_0, ..., b_m > = p_0^{a_0+1} ... p_n^{a_{n+1}+1} \cdot \prod_{i<m+1} p_{n+1+i}^{(b)_i+1}$$
$$=< a_0, ..., a_n, b_0, ..., b_m > .$$

强递归

设 $f(\bar{x}, y)$ 是一个函数，定义

$$F(\bar{x}, n) = p_0^{f(\bar{x},0)+1} \dots p_n^{f(\bar{x},n)+1}$$

即 $F(x, n)$ “存储”了 $f(x, 0)$, ..., $f(x, n)$ 的值。

定义

设 $g(\bar{x})$ 与 $h(\bar{x}, y, z)$ 是两个函数。称 $f(\bar{x}, y)$ 是从 g 与 h 经**强递归**得到的，如果

$$f(\bar{x}, 0) = g(\bar{x});$$

$$f(\bar{x}, n+1) = h(\bar{x}, n, F(\bar{x}, n)).$$

引理

如果 $f(\bar{x}, y)$ 是从 g 与 h 经强递归得到的，且 g 与 h 均是原始递归的，则 f 也是原始递归的。

证明

$$F(\bar{x},0)=2^{f(\bar{x},0)+1}=2^{g(\bar{x})+1}$$

$$F(\bar{x},n+1)=F(\bar{x},n)p_{n+1}^{f(\bar{x},n+1)+1}=F(\bar{x},n)p_{n+1}^{h(\bar{x},n,F(\bar{x},n))+1}$$

故 $F(\bar{x},y)$ 是原始递归的。$f(\bar{x},y)=F(\bar{x},y)_y$ 显然是原始递归的。

目录

非原始递归函数

1. 存在一个“程序”可以枚举所有的原始递归函数；
2. 设 $g_0, g_1, g_2, \ldots$ 是所有原始递归函数的枚举；
3. 令 $F : \mathbb{N} \to \mathbb{N}$ 为 $F(n) = g_n(n) + 1$；
4. 直观上 F 是可计算的，但不是原始递归的。

阿克曼函数

阿克曼函数

阿克曼函数 $A(x,y)$ 定义如下：

$$A(0,y) = y+1, \quad A(x+1,0) = A(x,1)$$

$$A(x+1),y+1) \;=\; A(x, A(x+1,y))$$

习题：阿克曼函数不是原始递归的。

正则 μ-算子

定义

令 $f:\mathbb{N}^{n+1}\to\mathbb{N}$ 是一个全函数。我们称函数 $g(\bar{x})$ 是从 f 通过正则极小化或正则μ-算子得到的，如果

- $\forall\bar{x}\exists y f(\bar{x},y)=0$;
- $g(\bar{x})$ 是使得 $f(\bar{x},y)=0$ 的最小的 y。

记作 $g(\bar{x})=\mu y\big(f(\bar{x},y)=0\big)$.

注

正则性条件不是“计算”出来的，而是我们利用数学证明获得的知识（类似于费马定理，四色定理等）

定义

1. 全体递归函数的集合为最小的包含所有初始函数，并且对复合、原始递归、正则极小化封闭的函数集合。
2. 称一个集合 $A \subseteq \mathbb{N}^k$ 是递归集，如果 χ_A 是递归函数。

1. 正则性 $\forall \bar{x} \exists y f(\bar{x}, y) = 0$ 的检验是非常复杂的
2. 去掉正则性的后果可能是会使得在某个 $\bar{x}_0$ 处对“解” y 的搜索永远不会停止，从而 $g(\bar{x}) = \mu y \big(f(\bar{x}, y) = 0 \big)$ 在 $\bar{x}_0$ 处没有定义；
3. 设 $f \subseteq A \times B$ 是一个函数；
4. $f(x) \downarrow$ 表示 f 在 x 处有定义（收敛）；
5. $f(x) \uparrow$ 表示 f 在 x 处没有定义（发散）。
6. 称 $f : A \to B$ 是一个部分函数。

1 原始递归函数

2 递归函数
- 非原始递归函数
- 递归函数
- 部分的归函数

3 图灵机

4 图灵可计算与部分递归函数

5 递归可枚举集

定义

设 f 是一个部分函数。称函数 g 是从 f 通过极小化或者由 μ-算子得到的，如果

$$g(\bar{x}) = \mu y\Big(\forall z \leq y(f(x,z)\downarrow) \wedge f(x,y) = 0\Big)$$

注

1. 条件 $\forall z \leq y(f(x, z)\downarrow)$ 是用来保证可计算性与准确性；
2. 为了找到最小的 y，必须逐一计算 $f(\bar{x}, 0), f(\bar{x}, 1), f(\bar{x}, 2)\dots$，直到找到 0；
3. 如果在以上步骤中，遇到一个 z_0 使得 $f(\bar{x}, z_0)\uparrow$，则计算不会终止，此时没有输出；
4. 不能跳过 z_0 继续寻找。
5. 函数 $\mu y\Big(f(x, y) = 0\Big)$ 没有“可计算性”；

定义

全体部分递归函数的集合为最小的包含所有初始函数，并且对复合、原始递归、极小化封闭的函数集合。

引理

阿克曼函数

$$A(0,y)=y+1,\quad A(x+1,0)=A(x,1)$$

$$A(x+1),y+1) \;=\; A(x,A(x+1,y))$$

是部分递归函数。

证明

称一个三元组的有穷集合 S 是好的，如果

1. 如果 $(0, y, z) \in S$，则 $z = y + 1$
2. 如果 $(x+1, 0, z) \in S$，则 $(x, 1, z) \in S$;
3. 如果 $(x+1, y+1, z) \in S$，则存在自然数 u 使得 $(x+1, y, u) \in S$ 且 $(x, u, z) \in S$;

即，如果 S 是好的三元组集，则当 $(x, y, z) \in S$ 时，一定有

1. $z = A(x, y)$
2. S 包含了计算 $A(x, y)$ 所需的所有三元组 $(x', y', A(x', y'))$.

证明

1. 三元组 (x, y, z) 可以编码为哥德尔数 $< x, y, z >= 2^{x+1}3^{y+1}5^{z+1}$;
2. 三元组编码的有穷集合 $\{u_0, ..., u_k\}$ 可以编码为哥德尔数 $< u_0, ..., u_k >$;
3. 任何一个有穷三元组集合 S 可以编码为一个哥德尔数 v
4. 用 S_v 表示 v 解码有穷三元组集合
5. 四元谓词 $P(x, y, z, v)$: $(x, y, z) \in S_v$ 是原始递归的。

$$(x, y, z) \in S_v \iff \exists i < v((v)_i =< x, y, z >)$$

证明

断言

“S_v 是好的三元组集”是原始递归的。

1. v 是三元组的集合（编码）
2. $\forall y, z < v((0, y, z) \in S_v \to z = y + 1)$;
3. $\forall x, z < v((x + 1, 0, z) \in S_v \to (x, 1, z) \in S_v)$;
4. $\forall x, y, z < v\Big((x + 1, y + 1, z) \in S_v \to \exists u < v((x + 1, y, u) \in S_v \ \wedge \ (x, u, z) \in S_v)\Big)$;

证明

断言

谓词

$R(x,y,v) :=$ v是好的三元组集的编码 $\wedge\ \exists z < v((x,y,z) \in S_v)$

是原始递归的。$R(x,y,v)$ 表示 (x,y) 在 v 中被计算过。

$$f(x,y) = \mu v\ R(x,y,v) \quad \text{寻找计算过}(x,y)\text{的三元组集合}$$

$$A(x,y) = \mu z((x,y,z) \in S_{f(x,y)}) \quad \text{输出计算机结果}$$

目录

图灵机的物理描述

1. 一条双向无限延伸的纸带，被分成一个个小格子，或者空白 (0)，或者写有字符;
2. 有穷字母表 $A = \{0, a_1, ..., a_n\}$;
3. 读写头：每次可以扫描一个格子，可以识别格子中的字符，可以写入字符，可以抹去字符，可以左右移动，每次一格；
4. 有穷状态集 $Q = \{q_1, ..., q_m\}$，在任何一个给定时刻，图灵机都处于某个状态 q_i。

图灵机的数学定义

定义

一台图灵机是由以下几个部分组成的：

1. 有穷字母表 A；
2. 方向符 L,R；
3. 有穷状态集 Q；
4. 有穷指令集 δ

其中每个指令是一个具有下列形式的四元组：

1. $qaq'a'$，其中 $q,q' \in Q$，$a,a' \in A$；
2. $qaLq'$，其中 $q,q' \in Q$，$a \in A$；
3. $qaRq'$，其中 $q,q' \in Q$，$a \in A$；

此外，还假定对任意的状态 q 和字符 a，至多有一条指令以 qa 开头。

注

1. 指令集 $\delta \subseteq (Q \times A) \times (A \cup \{R, L\} \times Q)$ 是一个部分函数，称之为转换函数；
2. 指令 $qaq'a'$ 的解读：若图灵机的当前状态为 q，当前读写头读到字符 a，则将 a 改为 a'，状态改为 q'；
3. 指令 $qaLq'$ 与 $qaRq'$ 的含义类似；

图灵机的其他模型

1. 单向无穷纸带 / 双向无穷纸带；
2. 字母表的选取；
3. 五元组指令 $qaa'q'D$，其中 D 是 L、R、S；
4. 非确定图灵机：以状态 q 和字符 a 开头的指令可以有多条；

格局

格局是图灵机在某个时刻的全部信息，包含：

1. 纸带上所有字符的信息；
2. 读写头的位置；
3. 当前状态；

记作

$$C = u\,q\,a\,v$$

其中 q 是状态，a 是读写头当前读到的字符，u 是 a 左边的字符串，v 是 a 右边的字符串。

格局的转换

设 $C = u\ q\ a\ v$ 是一个格局，如果不存在以 qa 开头的指令，则称 C 是一个终止格局。否则，可根据指令定义新的格局 C' 如下

1. 如果 $qaa'q' \in \delta$，则 $C' = u\ q'\ a'\ v$；
2. 如果 $qaRq' \in \delta$，则 $C' = u'\ q'\ b\ v'$，其中 $u' = u\ a$，$v = b\ v$；
3. 如果 $qaLq' \in \delta$，则 $C' = u'\ q'\ b\ v'$，其中 $u = b\ u'$，$v' = a\ v$；

称格局 C 产生 C'。

1. 图灵机的一个计算是一个格局的序列 (C_i)；
2. 如果 C_i 不是终止格局，则 C_i 产生 C_{i+1}；
3. 为了方便起见，假定图灵机有两个特殊状态 q_s 与 q_h；
4. 所有的计算以状态 q_s 开始；
5. 如果遇到终止格局 C，且不是停机状态，则要将其转换到停机状态。
6. 规定输入向量为 $(x_1, ..., x_n)$ 时，初始格局应为

$$q_s 1^{x_1+1} 0 1^{x_2+1} 0 ... 0 1^{x_k+1}.$$

7. 规定输出时，初始格局应为 $q_h 1^y$，表示输出值为 y;

图灵可计算

定义

称一个部分函数 $f : \mathbb{N}^k \to \mathbb{N}$ 是被图灵机 M 所计算的，或者说图灵机 M 计算函数 f，如果

$$f(x) = \begin{cases} y, & \text{如果}M\text{对输入}x\text{的输出为}y \\ \text{没有定义}, & \text{如果计算过程无限 / 没有终止格局} \end{cases}$$

称部分函数 f 为图灵可计算的，如果存在一个图灵机 M 计算它。

作业

习题 7.1， 习题 7.2， 习题 7.3

目录

图灵可计算与部分递归函数

定理

一个函数是图灵可计算的当且仅当它是部分递归的。

引理

每个初始函数都是图灵可计算的。

引理

任何一台标准图灵机 M_1 都可以被一台纸袋是单向无穷的图灵机 M_2 模拟。

证明-纸带变换

...	z	y	x	a	b	c	...

$\Downarrow$

2*$	a	b	c	...	...	...	...
	x	y	z	...	...	...	...

$\Downarrow$

$	(a,x)	(b,y)	(c,z)	...	...	...	..

证明-定义字母表与状态集

- M_1 的字母表是 A;
- 则 M_2 的字母表是 $A \times A$;
- (a, b) 表示上轨道为 a，下轨道为 b；
- M_1 的状态集是 Q;
- 则 M_2 的字母表是 $Q \times \{1, 2\}$;
- (q, i) 模拟轨道 i 上的计算；

证明-定义指令集

设 M_1 的指令集为 δ_1, 定义 M_2 的指令集 δ_2 如下

上轨道模拟

- 如果 $qaa'q' \in \delta_1$，则对每个 $b \in A$，有

$$(q,1)(a,b)(a',b)(q',1) \in \delta_2$$

- 如果 $qaLq' \in \delta_1$，则对每个 $b \in A$，有

$$(q,1)(a,b)L(q',1) \in \delta_2$$

- 如果 $qaRq' \in \delta_1$，则对每个 $b \in A$，有

$$(q,1)(a,b)R(q',1) \in \delta_2$$

证明-定义指令集

下轨道模拟

- 如果 $qbb'q' \in \delta_1$，则对每个 $a \in A$，有

$$(q,2)(a,b)(a,b')(q',2) \in \delta_2$$

- 如果 $qbLq' \in \delta_1$，则对每个 $a \in A$，有

$$(q,2)(a,b)L(q',2) \in \delta_2$$

- 如果 $qbRq' \in \delta_1$，则对每个 $a \in A$，有

$$(q,2)(a,b)R(q',2) \in \delta_2$$

证明-定义指令集

轨道转换

- 上轨道变下轨道：

$$(q, 1)\$R(q, 2) \in \delta_2$$

- 下轨道变上轨道：

$$(q, 2)\$R(q, 1) \in \delta_2$$

证明-计算模拟

- M_1 的格局集合 $\mathcal{C}$ 与 M_2 的格局集合 $\mathcal{D}$ 一一对应

$$\eta : \mathcal{C} \to \mathcal{D}$$

- 如果格局 $C_1 \in \mathcal{C}$ 产生格局 C_2，则 $\eta(C_1) \in \mathcal{D}$ 产生格局 $\eta(C_2)$

引理

任何一台标准图灵机 M_1 都可以被一台纸带是单向无穷的图灵机 M_2 模拟。

推论

任何图灵可计算函数 h 都可以被一台加了如下限制的图灵机计算：

1. 在初始格局中，纸带中有一个不在字母表中的新字符 $\$$，可以在任何实现给定的位置，只要不混在输入字符串中间；
2. 在计算完成后，$\$$ 左边的内容不变；
3. 输出字符串的位置起始于 $\$$ 右边第一格。

...	□	□	□	$	a	b	c	...

引理

图灵可计算函数类对符合运算封闭。设 g 与 $h_1, ..., h_r$ 均是图灵可计算的，则

$$f(x_1, ..., x_n) = g(h_1(x_1, ..., x_n), ..., h_r(x_1, ..., x_n))$$

也是图灵可计算的。

证明

- 引入 $r+1$ 个新字母 $\$_1,\ldots,\$_{r+1}$。
- 输入纸带如下

...	$\bar{x}$	$\$_1$	0	0	0	...

- 根据推论，存在计算 h_1 的图灵机/程序使得计算完后输出为

...	$\bar{x}$	$\$_1$	$h_1(\bar{x})$	$\$_2$	0	0	...

- 存在计算 h_2 的图灵机/程序使得计算完后输出为

...	$\bar{x}$	$\$_1$	$h_1(\bar{x})$	$\$_2$	$h_2(\bar{x})$	$\$_3$	0	...

- 存在计算 h_2 的图灵机/程序使得计算完后输出为

...	$\bar{x}$	$\$_1$	$h_1(\bar{x})$	$\$_2$	$h_2(\bar{x})$	$\$_3$	...	$\$_{r+1}$	$g(h_1(\bar{x}),\ldots,h_r($

引理

图灵可计算函数类对原始递归和极小算子封闭。

证明 I

设 $f(x,0)=g(x)$, $f(x,y+1)=h(x,y,f(x,y))$

- 引入 1 个新字母 $\$$。
- 输入纸带如下

...	0	x	y	$\$$	0	0	0	...

- 在第 0 步，存在计算 g 的图灵机/程序使得计算完后输出为

...	0	x	y	$\$$	$g(x)$	0	0	0	...

- 在第 1 步，存在计算 h 的图灵机/程序使得计算完后输出为

...	1	x	y	$\$$	$h(0,x,f(x,0))$	0	0	0	...

- 在第 $k+1$ 步，存在计算 h 的图灵机/程序使得计算完后输出为

...	k+1	x	y	$\$$	$h(k,x,f(x,k))$	0	0	0	...

即可以设计一个循环程序，使得 $k+1=y$ 时输出结果。

证明 II

设 $f(x) = \mu y\Big(\forall z \le y(h(x,z)\downarrow) \wedge h(x,y) = 0\Big)$.

- 引入 1 个新字母 $\$$。
- 输入纸带如下

...	0	x	$\$$	0	0	0	...

- 在第 0 步，存在计算 h 的图灵机/程序使得计算完后输出为

...	1	x	$\$$	$h(x,0)$	0	0	0	...

- 如果 $h(x,0) = 0$, 则输出 0，且停机，否则在下一步计算 $h(x,1)$, 计算完后输出为

...	2	x	$\$$	$h(x,1)$	0	0	0	...

- 一般地，在第 $k+1$ 步，如果 $h(x,k) = 0$, 则输出 k，且停机，否则在下一步计算 $h(x,k+1)$, 计算完后输出为

...	k+2	x	$\$$	$h(x,k+1)$	0	0	0	...

即可以设计一个循环程序，计算 $f(x)$.

定理

任何部分递归函数都是图灵可计算的。

接下来证明：任何图灵可计算函数都是部分递归的。

图灵机的编码

符号的编码

图灵机 M 的符号

1. 字母表 $A = \{0, 1\}$
2. R，L
3. 状态集 Q。

的编码为

$$\ulcorner 0 \urcorner = 0,\ \ulcorner 1 \urcorner = 1,\ \ulcorner L \urcorner = 2,\ \ulcorner R \urcorner = 3,\ \ulcorner q_s \urcorner = 4, \ldots, \ulcorner q_h \urcorner = n$$

符号集编码为 n.

图灵机的编码

指令集的编码

1. 图灵机 M 的指令 $qaXq'$ 编码为

$$<\ulcorner q\urcorner,\ulcorner a\urcorner,\ulcorner X\urcorner,\ulcorner q'\urcorner>=2^{\ulcorner q\urcorner+1}3^{\ulcorner a\urcorner+1}5^{\ulcorner X\urcorner+1}7^{\ulcorner q'\urcorner+1}$$

2. 指令集 δ 对于一个数集

$$\{s_1,...,s_m\}$$

3. δ 的编码为哥德尔数

$$\ulcorner\delta\urcorner=<n,s_1,...,s_m>$$

$e=\ulcorner\delta\urcorner$ 包含了图灵机 M 的全部信息，规定它为图灵机 M 的编码，即 $e=\ulcorner M\urcorner$

引理

下列谓词是原始递归的：

1. e 是图灵机
2. s 是图灵机 e 的指令
3. q 是图灵机 e 停机状态。

证明

e 是图灵机当且仅当

1. e 是哥德尔数且 $e_0 = n \geq 5$;
2. $\forall i \leq e(i > 0 \to e_i$是哥德尔数且$lh(e_i) = 4)$;
3. $$\forall 0 < i \leq e\Big((4 \leq (e_i)_0, (e_i)_3 \leq n) \ \wedge \ (e_i)_1 \leq 1 \ \wedge \ (e_i)_2 \leq 3\Big)$$

格局的编码

格局

设 $C = \ldots b_1 b_0 qac_0 c_1 \ldots$ 是一个格局。

1. $x = \sum_i b_i 2^i$
2. $y = \sum_i c_i 2^i$
3. C 的编码 $\ulcorner C \urcorner$ 为

$$\ulcorner C \urcorner = < x, \ulcorner q \urcorner, \ulcorner a \urcorner, y >= 2^{x+1} 3^{\ulcorner q \urcorner + 1} 5^{\ulcorner a \urcorner + 1} 7^{y+1}$$

引理

c 是一个格局的编码是原始递归的。

证明

c 是 (e 的) 一个格局的编码当且仅当

1. c 是哥德尔数；
2. $4 \leq c_1 \leq e_0$；
3. $c_2 \leq 1$。

给定一个图灵机 $e = \ulcorner M \urcorner$

1. 输入函数 $IN(x_1, ..., x_n) = \ulcorner C_0 \urcorner$，其中 C_0 是初始格局；
2. 转换函数 $NEXT(e, c)$ 当且仅当格局 c 产生格局 d。
3. 谓词 $TREM(e, c)$ 表示 c 是 e 的终止格局的编码。
4. 转换函数 $OUT(c) = y$ 当且仅当格局 c 终止格局 $C = q_h 1^y$ 的编码。

引理

函数 IN，OUT $NEXT$, 和谓词 $TERM$ 都是原始递归的。

克林尼 T 谓词

定义

$T(e, x, z)$ 表示 z 是图灵机 e 对输入 x 的计算过程（格局序列）的编码。

引理

克林尼谓词 $T(e, x, z)$ 是原始递归的。

克林尼 T 谓词

证明

$T(e, x, z)$ 当且仅当

1. e 是图灵机；
2. z 是 e 的格局序列 $<\ulcorner C_0 \urcorner, ..., \ulcorner C_k \urcorner>$；
3. $\ulcorner C_0 \urcorner = IN(x)$；
4. $\forall i < k \ulcorner C_{i+1} \urcorner = Next(e, \ulcorner C_i \urcorner)$ 是初始格局；
5. $TERM(e, \ulcorner C_k \urcorner)$；

引理

如果 f 是图灵可计算的，则它是部分递归的。

证明

设 f 被图灵机 e 计算。则

$$g(x) = \mu z T(e, x, z),$$

$$h(z) = \mu m(TERM(e, (z)_{\mathrm{lh}(z)}) \wedge (z)_{\mathrm{lh}(z)} = m),$$
$$f(x) = OUT(h(g(x)))$$

丘奇论题

丘奇论题

直观上的可计算函数类就是部分递归函数。

克林尼正规型定理

定理

存在原始递归函数 $U : \mathbb{N} \to \mathbb{N}$ 和原始递归谓词 $T(e, x, z)$ 使得对任意的部分递归函数 $f : \mathbb{N} \to \mathbb{N}$，都存在自然数 e 使得 $f(x) = U(\mu z T(e, x, z))$.

推论

一个函数是递归的当且仅当它是部分递归的全函数。

1. $\Rightarrow$: 递归函数是部分递归的，且是全函数；
2. $\Leftarrow$: 部分递归的全函数 $f(x) = U(\mu z T(e, x, z))$ 满足正则性，从而是递归函数。

通用函数定理

存在一个通用的部分递归函数；即存在二元函数 $\Phi : \mathbb{N}^2 \to \mathbb{N}$ 使得对任何一元的部分递归函数 $f : \mathbb{N} \to \mathbb{N}$ 都存在一个自然数 e 使得对搜有的 x 有 $f(x) = \Phi(e, x)$.

令 $e_0, e_1, \ldots$ 是图灵机的一个枚举，则 $\phi_0(x), \phi_1(x), \ldots$ 是对应的对全体部分函数的枚举。即 $\phi_i(x) = \Phi(e_i, x)$.

定理

对递归函数来说，不存在通函数，即，不存在递归函数 $T : \mathbb{N}^2 \to \mathbb{N}$ 使得对任何的一元递归函数 $f : \mathbb{N} \to \mathbb{N}$ 都存在一个自然数 e 使得对搜有的 x 有 $f(x) = T(e, x)$.

例

存在一个部分递归函数 f 使得对任何递归全函数 g，都存在 $n \in \mathrm{dom}(f)$ 使得 $f(n) \neq g(n)$.

1. $f(n) = \Phi(n, n) + 1$;
2. $g(x) = \Phi(m, x)$;
3. $f(m) = \Phi(m, m) + 1$, $m \in \mathrm{dom}(f)$;
4. $f(m) \neq g(m)$.

f 不是任何递归全函数 g 在 $\mathrm{dom}(f)$ 上的限制。

目录

递归可枚举集

定义

称 $A \subseteq \mathbb{N}$ 是递归可枚举的，简称 r.e. 的，如果 $A = \emptyset$ 或者 A 是某个递归全函数 $f : \mathbb{N} \to \mathbb{N}$ 的值域，即，

$$A = \{y | \exists x f(x) = y\}$$

注

直观上，

1. A 中的元素可以通过 f 有效枚举；
2. 如果 $y \in A$，则可以知道 $y \in A$;
3. 如果 $y \notin A$，则不知道 y 是否属于 A;
4. A 是递归关系加存在量词而得到的。

引理

设 $A \subseteq \mathbb{N}$，则下列命题等价：

1. A 是递归可枚举的；
2. A 是空集或者某个原始递归函数的值域；
3. A 是某个部分递归函数的值域；
4. A 的部分特征函数是部分递归的。

$$\chi_{A_P}(x) = \begin{cases} 1, & \text{如果} x \in A \\ \text{没有定义}, & \text{否则} \end{cases}$$

5. A 是某个部分递归函数的定义域；
6. 存在一个二元递归 / 原始递归谓词 $R(x, y)$ 使得

$$A = \{x \mid \exists y \ R(x, y)\}$$

证明 I

1. (1)⇒(2)：设 A 是 $f(x) = U(\mu z T(e,x,z))$ 的值域，任取 $a_0 \in A$，定义

$$F(x,n) = \begin{cases} U(\mu y \leq n T(e,x,n)), & \text{如果} \exists y \leq n\ T(e,x,y) \\ a_0, & \text{否则} \end{cases}$$

   则 $F(\mathbb{N}^2) = f(\mathbb{N})$。
2. (2)⇒(3)：显然;
3. (3)⇒(4)：设 $A = f(\mathbb{N})$，可以假设 f 是原始递归的则

$$\chi_{A_P}(y) = C_1^1(\mu x\ f(x) = y)$$

4. (4)⇒(5)：显然;

证明 II

5. (5)⇒(6)：设 $f(x) = U(\mu z T(e, x, z))$，则

$$\mathrm{dom}(f) = \{x \mid \exists z T(e, x, z)\}$$

6. (6)⇒(1)：令

$$A = \{x \mid \exists y\ R(x, y)\}, \quad g(y) = x * C_1^1(\mu x R(x, y))$$

定理

一个自然数的集合 A 是递归的当且仅当 A 和它的补集 $\mathbb{N}\backslash A$ 都是递归可枚举的。

证明

设 A 是 $f_1 : 2\mathbb{N} \to \mathbb{N}$ 的值域，$\mathbb{N}\backslash A$ 是 $f_2 : 2\mathbb{N}+1 \to \mathbb{N}$ 的值域，$R_i(x,y) \iff y = f_i(x)$

$$h(y) = \mu x\ (R_1(x,y) \vee R_2(x,y)),\ \ \chi_A(y) = 1 \iff h(y)\text{是偶数}$$

定义

设 $\phi : \mathbb{N}^k \to \mathbb{N}$ 是原始递归的双射，称 $A \subseteq \mathbb{N}^k$ 是递归可枚举的，如果 $\phi(A) \subseteq \mathbb{N}$ 是递归可枚举的。

定理

设 $A, B \subseteq \mathbb{N}^k$ 是递归可枚举的，则

1. $A \cup B$ 和 $A \cap B$ 都是递归可枚举的；
2. A 的投射也是对可枚举的，即

$$\{x \in \mathbb{N}^{k-1} \mid \exists y(x, y) \in A\}$$

是递归可枚举的。

定理

集合 $K = \{e \in \mathbb{N} \mid \Phi(e, e)\ 有定义\}$ 是递归可枚举集，但不是递归的。

证明

1. K 是 $\Phi(x, x)$ 的定义域，从而是递归可枚举的；
2. 反设 K 是递归的，则 K 的补集也是递归的。以此 $x \in K$ 与 $x \notin K$ 都是递归谓词。从而函数

$$f(x) = \begin{cases} \Phi(x, x) + 1, & \text{如果} x \in K \\ 0, & \text{否则} \end{cases}$$

也是递归函数。以此存在一个自然数 e 使得 $f(x) = \Phi(e, x)$。如果 $e \in K$，则 $f(e) = \Phi(e, e) + 1$，矛盾。如果 $e \notin K$，则 $\Phi(e, e) \uparrow$，而 $f(e) = 0$，矛盾。

推论

递归可枚举集对补运算不封闭。

Thanks!