《计算模型导引》教材习题解答

"Introduction to Models of Computation" Textbook Exercises' Solutions

---

By Haitao Huang

2022.6 Edition 1.1

第一版声明

本习题解答与南京大学宋方敏教授编著的《计算模型导引》配套。

所有习题解答都是经过本人的思考，与周围人的讨论，以及来自大佬的讲解得到，所以整个题解并未完成所有的题目，也不能保证答案的严谨性和正确性，因此仅供参考。由于使用此答案造成的任何后果，请自行承担，本人概不负责。

本解答中许多灵感启发来自于蒋炎岩前辈提供的一份英文版参考解答，张强同学、李浩同学的解答，以及来自助教的解答，在此表示特别感谢。

同时殷切盼望各位大佬能对这份解答做出哪怕一点微小的贡献，包括但不限于：尚未解出题目的解答，不同于已有解答的另外的解题方法，对已有解答描述不够严谨甚至是错误的部分的补充、纠正或指出，对已有解答推理或描述不够清晰部分的补充或指出，公式中的错误，错别字等。任何的补充指正和提问，都感激不尽。

作者：Haitao Huang

2019 年于南京大学

第 1.1 版声明

感谢 Haitao Huang 花费了巨大心血完成教材习题解答第一版 (这里称为 1.0 版)。1.1 版习题解答对 1.0 版的第一章、第三章和五章部分解答做出了小的补充和修定，同时加上了几道有意思的练习题。由于新版只在原来基础上进行了小幅度修改，故命名新版本为 1.1 版。本人深知对习题解答进行补充修订的贡献量与第一版作者贡献量相比如同萤火虫与皓月的差距，故不吹嘘本人功劳。在这向 Haitao Huang 大佬致敬！

感谢宋方敏老师传授向无知的我传授计算模型知识！在没学这门课程之前，我不懂什么是“计算”，“计算的范围有多大”，也不敢说我是学过计算机的。尽管我这门课我只懂一些皮毛，很多知识我还没有完全明白、吃透，但是我仍然觉得这门课很有价值，有意义！我发自内心的喜欢这门课。希望南大以后能够一直将这门必修课开设下去，给学生们涨涨“内力”，让学生们体会到“计算”之美。

感谢 Liangchuan Luo 一直无私地为我解答相关问题，感谢 Jingsong Dai 和 Feng Chen 帮我核验个人的解答过程。

由于个人并不精通本门课程，没有掌握其精髓，加之时间有限，习题解答中一定有疏漏和不足之处，希望读者批评指正。

作者：Shizhe Liu

2022 年于南京大学

1 递归函数

1.1 证明: 对于固定的 k, 一元数论函数 $x+k \in \mathcal{BF}$.

证明. 对第一版答案做出补充说明.

证法一: 因为 $S(x)=x+1$(page 1 定义 1.2), 记 $S^k \circ (x) = \underbrace{S \circ S \circ \cdots \circ S(x)}_{k\text{个}S}$, 其中 $\circ$ 是定义 1.4 的复合算子 (page 4), 规定 $k=0$ 时,$S^k \circ (x) = x$.

由定理 1.2(page 6) 知:$S^k \circ (x) = x+k \in \mathcal{BF}$.

证法二: 令 $f_k(x)=x+k$.

1) 当 $k=0$ 时, $f_0(x)=x=P_1^1(x) \in \mathcal{IF}$, 命题成立; 当 $k=1$ 时, $f_1(x)=x+1=S(x) \in \mathcal{IF}$, 命题成立;

2) 假设当 $k=k_0(k_0 \geqslant 1, k_0 \in \mathbb{N})$ 时 $f_{k_0} \in \mathcal{BF}$;

3) 当 $k=k_0+1$ 时,$f_{k_0+1}=x+k_0+1=S(x+k_0)=S \circ f_{k_0}(x)=\mathrm{Comp}_1^1[S, f_{k_0}] \in \mathcal{BF}$.

由数学归纳法可知, 命题成立. □

1.2 证明: 对任意 $k \in \mathbb{N}^+, f : \mathbb{N}^k \to \mathbb{N}$, 若 $f \in \mathcal{BF}$, 则存在 h, 使得

$$f(\vec{x}) < \|\vec{x}\| + h.$$

其中 $\|x\| \equiv \max\{x_i : 1 \leqslant i \leqslant k\}$.

证明. 分情况讨论.

1. 当 $f \in \mathcal{IF}$ 时, 由于 $S(x)=x+1<\|x\|+2, Z(x)=0<\|x\|+2, P(\vec{x}) \leqslant \|\vec{x}\| < \|\vec{x}\|+2$, 所以令 $h=2$ 即可让题中式子对于 $f \in \mathcal{IF}$ 均成立;
2. 当 $f \in \mathcal{BF}-\mathcal{IF}$ 时, 假设 f 的构造长度 ℓ 满足 $0 \leqslant l \leqslant k$ 时, 命题均成立, 那么对这样的函数 f, 必然存在一个自然数 h_k 使得 $f(\vec{x}) < \|\vec{x}\|+h_k$ 恒成立. 对于 $f \in \mathcal{IF}$, 其构造长度可视为 0, 故令 $h_0=2$.
   当 f 的构造长度为 $k+1$ 时, 设其构造过程为数论函数序列 $f_0, f_1, \cdots, f_k, f$, 那么对于任一函数 $f_i(0 \leqslant i \leqslant k)$, 其构造长度不大于 i, 自然也不大于 k, 所以有
   $$\begin{aligned} f &= \mathrm{Comp}_n^m[f_{i_0}, f_{i_1}, \cdots, f_{i_n}] \\ &= f_{i_0}(f_{i_1}(\vec{x}), \cdots, f_{i_n}(\vec{x})) \\ &< \|f_{i_1}(\vec{x}), \cdots, f_{i_n}(\vec{x})\| + h_k \end{aligned} \tag{1}$$
   其中 $f_{i_0}, f_{i_1}, \cdots, f_{i_n}$ 从 $f_0, f_1, \cdots, f_k$ 中选择 (可重复), 所以式 (1) 最后出现的 $f_{i_1}(\vec{x})$, $\cdots$, $f_{i_n}(\vec{x})$ 的所有值均小于 $\|\vec{x}\|+h_k$, 可得 $\|f_{i_1}(\vec{x}), \cdots, f_{i_n}(\vec{x})\| < \|\vec{x}\|+h_k$, 因此 $f < \|\vec{x}\|+2h_k$, 也就是说, 当 f 的构造长度 l 满足 $0 \leqslant l \leqslant k+1$ 时, $f(\vec{x}) < \|\vec{x}\|+2h_k$ 恒成立, 即 $h_{k+1}=2h_k$ 是满足要求的.

又因为 $h_0=2$, 可得 $h_k=2^{k+1}$ 对于构造长度不大于 k 的函数都能使不等式 $f(\vec{x}) < \|\vec{x}\|+h_k$ 恒成立. 而对一个特定的 $f \in \mathcal{BF}$, 它肯定有一个构造长度 ℓ, 所以令 $h=2^{\ell+1}$ 即可使得题中不等式成立. □

1.3 证明: 二元数论函数 $x+y \notin \mathcal{BF}$.

证明. 由 1.2 的结论可知, 若二元数论函数 $f \in \mathcal{BF}$, 则存在自然数 h 使得 $f(x,y) < \max\{x,y\}+h$ 恒成立.

假设 $x+y \in \mathcal{BF}$, 那么存在自然数 h 使得 $x+y < \max\{x,y\}+h$ 恒成立.

因为 $x+y = \max\{x,y\}+\min\{x,y\}$, 可推出该自然数 h 使得 $\min\{x,y\} < h$ 对于任意的自然数 x,y 都成立, 这显然是错误的, 任给定一个 h, 只需让 x,y 都大于 h 就可使不等式不成立. 所以 $x+y \notin \mathcal{BF}$. □

1.4 证明: 二元数论函数 $x \dot{-} y \notin \mathcal{BF}$.

证明. 对第一版答案做出补充说明.

证法一: 通过引理来证明. 引理: 若 $f: N^k \to N$, 其中 $k \in N^+, f \in \mathcal{BF}$, 则 $f(\vec{x})$ 仅与 $\vec{x}$ 某一分量有关, 与其他分量无关.

证明: 由于 $f \in \mathcal{BF}$, 故存在 $f_0, f_1, \cdots, f_n$ 使得 $f = f_n$.

对 n 做归纳:

1) 当 $n=0$ 时,$f_0 \in \mathcal{IF}$,

情况 1: 若 f_0 为 Z 或 S, 结论成立;

情况 2: 若 f_0 为 P, 则 $P_i^n(\vec{x}) = x_i$, 仅与 $\vec{x}$ 的 i 分量有关, 结论成立;

2) 假设 $0 \leqslant i \leqslant n$ 时, 对 f_i 结论成立;

3) 当 $i=n+1$ 时,$f_{n+1}(\vec{x}) = f_{i0}(f_{i1}(\vec{x}), \cdots, f_{in}(\vec{x}))$, 由于 $f_{i0}(\vec{x})$ 仅与 $\vec{x}$ 某一分量有关, 设为 t, 则,$f_{n+1}(\vec{x})$ 仅与 $\vec{x}$ 第 t 分量有关. 故引理成立.

而对于 $x \dot{-} y$ 来说, 其与 x,y 都有关, 因此 $x \dot{-} y \notin \mathcal{BF}$.

证法二: 假设 $x \dot{-} y \in \mathcal{BF}$, 因为 $\text{pred} = \text{Comp}_2^1[\dot{-}, P_1^1, S \circ Z]$, 所以 $\text{pred} \in \mathcal{BF}$. 所以, 要证明出题目的命题, 只要证明 $\text{pred} \notin \mathcal{BF}$ 即可.

显然 $\text{pred} \notin \mathcal{IF}$, 那么若 $\text{pred} \in \mathcal{BF}$, 则 pred 拥有最短构造过程, 设其为 $f_0, f_1, \cdots, f_n$, pred. 显然,pred 是通过 $f_0, f_1, \cdots, f_n$ 中的某些函数通过复合运算得来.

$f_0, f_1, \cdots, f_n$ 中不可能出现投影函数 P, 首先, 由于 pred 是一元函数, 如果序列中投影函数, 它们的定义域为 $\mathbb{N}^k$. 这个投影函数如若使用, 就必须接受 k 个自然数, 这 k 个自然数就只能表示成 $g_1(x), g_2(x), \cdots, g_k(x)$ 的形式, $g_i(x) \in \mathcal{BF}, 1 \leqslant i \leqslant k$. 那么问题在于, 投影函数只会固定选用其中一个, P_i^k 就只会选 $g_i(x)$, 那么根本不用 P_i^k 的参与, 只用 $g_i(x)$ 就能参与之后的构造, 所以对于一元函数的**最短**构造过程来说, 投影函数是无用的. 那么 $f_0, f_1, \cdots, f_n$ 要么就是 S, Z, 要么就是由 S, Z 复合而来.

这样一来, 每一步构造都是 $\mathbb{N} \to \mathbb{N}$. 在这时, 函数的复合满足结合律. 因此, pred 可表示成 $F_1 \circ F_2 \circ \cdots \circ F_k$ 的形式, $F_i \in S, Z$.

而 $Z \circ F_i \circ \cdots \circ F_k = 0$ 恒成立, 因此上式可表示成 $S^a \circ Z^b$, 其中, $a \in \mathbb{N}, b \in \{0,1\}$ 且 a, b 不同时为 0. 这里

$$F^a \equiv \underbrace{F \circ F \circ \cdots \circ F}_{a}$$

当 $a > 0$ 时, 令 $x = 0$, 结果肯定不为 0; 当 $a = 0$ 时, 式子就是 Z, 同样不对. 因此 $\text{pred} \notin \mathcal{BF}$, 从而 $x \dot{-} y \notin \mathcal{BF}$. □

1.5 设 $\mathrm{pg}(x,y)=2^x(2y+1)\dot{-}1$, 证明: 存在初等函数 $K(x)$ 和 $L(x)$ 使得

$$\begin{aligned}K(\mathrm{pg}(x,y))&=x,\\ L(\mathrm{pg}(x,y))&=y,\\ \mathrm{pg}(K(z),L(z))&=z.\end{aligned}$$

证明. 当 $x,y\in\mathbb{N}$ 时, 可知 $2^x(2y+1)\geqslant 1$ 恒成立, 因此 $\mathrm{pg}(x,y)=2^x(2y+1)-1$(就是把 $\dot{-}$ 换成了普通的减号 $-$).

又因为 $2\nmid(2y+1)$, 所以可使 $K(z)=\mathrm{ep}_0(z+1), L(z)=\frac{1}{2}\left(\frac{z+1}{2^{\mathrm{ep}_0(z+1)}}-1\right)$ 使得 $K(\mathrm{pg}(x,y))=x, L(\mathrm{pg}(x,y))=y$.

且

$$\mathrm{pg}(K(z),L(z))=2^{\mathrm{ep}_0(z+1)}\frac{z+1}{2^{\mathrm{ep}_0(z+1)}}-1=z.$$

□

1.6 设 $f:\mathbb{N}\to\mathbb{N}$, 证明: f 可以作为配对函数的左函数当且仅当对任何 $i\in\mathbb{N}$,

$$|\{x\in\mathbb{N}:f(x)=i\}|=\aleph_0.$$

证明. 记 $\mathcal{X}_i=\{x\in\mathbb{N}:f(x)=i\}$.

先证明必要性.

显然, $\mathcal{X}_i\subseteq\mathbb{N}$, 因此只需要证明该集合内的元素个数无限即可. [1]

假设 $\mathcal{X}_i$ 是有限集.

考虑与之对应的配对函数 $\mathrm{pg}:\mathbb{N}^2\to\mathbb{N}$ 和右函数 $g:\mathbb{N}\to\mathbb{N}$, 记 $\mathcal{Y}=\{g(x)|x\in\mathcal{X}_i\}$, 那么显然 $\mathcal{Y}$ 也是有限集, 集合 $\mathbb{N}-\mathcal{Y}$ 非空.

任取 $j\in\mathbb{N}-\mathcal{Y}$, 若 $\mathrm{pg}(i,j)\in\mathcal{X}_i$, 则 $j=g(\mathrm{pg}(i,j))\in\mathcal{Y}$, 与 $j\in\mathbb{N}-\mathcal{Y}$ 矛盾; 若 $\mathrm{pg}(i,j)\notin\mathcal{X}_i$, 则 $f(\mathrm{pg}(i,j))\neq i$, 与配对函数的定义矛盾. 故 $\mathcal{X}_i$ 是无限集, 因而命题成立.

再证明充分性.

对任意的 $i\in\mathbb{N}$, 都有 $|\{x\in\mathbb{N}:f(x)=i\}|=\aleph_0$, 那么 $\mathcal{X}_i$ 可以与 $\mathbb{N}$ 建立一个双射, 记为函数 $F_i:\mathbb{N}\to\mathcal{X}_i$ 及其反函数 $F_i^{-1}:\mathcal{X}_i\to\mathbb{N}$.

现在, 可以定义 $g:\mathbb{N}\to\mathbb{N}$ 如下:

$$g(x)=\begin{cases}j, & \text{若}x=F_i(j),\\ 0, & \text{否则}.\end{cases}$$

那么, 当 $x=F_i(j)$ 时, 因为 $F_i(j)\in\mathcal{X}_i$, $f(x)=i$ 成立; 同时 $g(x)=j$ 成立. 所以, 令 $\mathrm{pg}(i,j)=F_i(j)$ 即可, f 即为 pg 的左函数. □

[1]根据可数选择公理 (axiom of countable choice), $\aleph_0$ 即自然数集等无限可数集的基数是所有无限集的基数里面最小的.

1.7 证明: 从本原函数出发, 经复合和算子 $\prod\limits_{i=n}^{m}[\cdot]$ 可以生成所有的初等函数. 这里

$$\prod_{i=n}^{m}[f(i)] = \begin{cases} f(n)\cdot f(n+1)\cdot \quad \cdots \quad \cdot f(m), & \text{若} m \geqslant n, \\ 1, & \text{若} m < n. \end{cases}$$

证明. 由初等函数的定义和引理 1.12, 只需要证明 $\ddot{-}$, 有界迭加算子 $\Sigma[\cdot]$ 和有界迭乘算子 $\Pi[\cdot]$ 能用复合以及算子 $\prod\limits_{i=n}^{m}[\cdot]$ 表示.

有界迭乘算子是算子 $\prod\limits_{i=n}^{m}[\cdot]$ 中 $n = 0$ 的特例.

首先不难构造出以下几个函数:

指数函数[2]

$$x^y = \prod_{i=1}^{y}[P_1^1(x)]$$

取反函数

$$N(x) = \prod_{i=1}^{x}[Z(i)]$$

$x \leqslant y$ 的特征函数

$$\mathrm{leq}(x, y) = \prod_{i=x}^{y}[Z(i)]$$

$x \geqslant y$ 的特征函数

$$\mathrm{geq}(x, y) = \prod_{i=y}^{x}[Z(i)]$$

然后:

$x = y$ 的特征函数

$$\mathrm{eq}(x, y) = \mathrm{leq}(x, y)^{N(\mathrm{geq}(x,y))}$$

$$2^x = \prod_{i=1}^{x}[S \circ S \circ Z(i)]$$

令

$$\log(x) = \begin{cases} \log_2 x, & \text{若} \log_2 x \in \mathbb{N}, \\ 1, & \text{否则}. \end{cases}$$

那么

$$\log(x) = \prod_{i=0}^{x}[i^{N(\mathrm{eq}(2^i, x))}]$$

$$\log(2^x) = \prod_{i=0}^{2^x}[i^{N(\mathrm{eq}(2^i, 2^x))}]$$

[2] 这里约定 $0^0 = 1$.

所以

$$\sum_{i=n}^{m} f(i,\vec{x}) = \log(2^{\sum_{i=n}^{m} f(i,\vec{x})}) = \log(\prod_{i=n}^{m} 2^{f(i,\vec{x})})$$

$$x \ddot{-} y = \sum_{i=y+1}^{x} [S \circ Z(i)] + \sum_{i=x+1}^{y} [S \circ Z(i)]$$

综上, 证明完毕. □

1.8 设

$$M(x) = \begin{cases} M(M(x+11)), & 若 x \leqslant 100, \\ x-10, & 若 x > 100, \end{cases}$$

证明:

$$M(x) = \begin{cases} 91, & 若 x \leqslant 100, \\ x-10, & 否则. \end{cases}$$

证明. 显然, 我们只要证明当 $0 \leqslant x \leqslant 100$ 时, $M(x) = 91$ 即可.

当 $90 \leqslant x \leqslant 100$ 时, $M(x) = M(M(x+11)) = M(x+1)$, 因此 $M(90) = M(91) = \cdots = M(100) = M(101) = 91$, 注意 $M(91) = 91$;

当 $0 \leqslant x \leqslant 100$ 时, 存在自然数 k 使得 $90 \leqslant x + 11k \leqslant 100$ 成立. 因此 $M(x) = M^2(x + 11 \cdot 1) = M^{k+1}(x + 11k) = M^k M(x + 11k) = M^k(91) = 91$. □

1.9 证明:

$$\min x \leqslant n.[f(x,\vec{y})] = n \dot{-} \max x \leqslant n.[f(n \dot{-} x, \vec{y})],$$

$$\max x \leqslant n.[f(x,\vec{y})] = n \dot{-} \min x \leqslant n.[f(n \dot{-} x, \vec{y})].$$

证明. 分情况讨论.

1. 当 $f(x,\vec{y})$ 在 $[0,n]$ 有零点时, 设 $\min x \leqslant n.[f(x,\vec{y})] = k$.
   那么有 $f(k) = 0$, 从而 $f(n \dot{-} (n \dot{-} k)) = 0$, $n \dot{-} k$ 是函数 $f(n \dot{-} x)$ 的零点.
   因为 k 为 $f(k)$ 最小的零点, 那么 $n \dot{-} k$ 是 $f(n \dot{-} x)$ 在 $[0,n]$ 的最大零点. 因为如果有比 $n \dot{-} k$ 大的 $f(n \dot{-} x)$ 的零点 z 存在, 那么 $f(n \dot{-} z) = 0$ 且 $n \dot{-} z < k$, 与 k 为 $f(x)$ 最小零点矛盾.
   于是 $\min x \leqslant n.[f(x,\vec{y})] = n \dot{-} \max x \leqslant n.[f(n \dot{-} x, \vec{y})]$ 成立.
2. 当 $f(x,\vec{y})$ 在 $[0,n]$ 没有零点时, $\min x \leqslant n.[f(x,\vec{y})] = n$, $\max x \leqslant n.[f(n \dot{-} x, \vec{y})] = 0$, 因此式子依然成立.

同理可证, $\max x \leqslant n.[f(x,\vec{y})] = n \dot{-} \min x \leqslant n.[f(n \dot{-} x, \vec{y})]$ 成立. □

1.10 证明: $\mathcal{EF}$ 对有界 max-算子封闭.

证明. 因为

$$\max x \leqslant n.[f(x,\vec{y})] = n \dot{-} \min x \leqslant n.[f(n \dot{-} x,\vec{y})],$$

又因为引理 1.12(5) 和引理 1.14, $\mathcal{EF}$ 对 $\dot{-}$ 和有界 μ-算子封闭, 故 $\mathcal{EF}$ 对有界 max-算子封闭. □

1.11 Euler 函数 $\varphi : \mathbb{N} \to \mathbb{N}$ 定义为

$$\varphi(n) = |\{x : 0 < x \leqslant n \wedge \gcd(x,n) = 1\}|,$$

即 $\varphi(n)$ 表示小于等于 n 且与 n 互素的正整数个数. 例如 $\varphi(1) = 1$, 因为 1 与其本身互素; $\varphi(9) = 6$, 因为 9 与 1,2,4,5,7,8 互素. 证明: $\varphi \in \mathcal{EF}$.

证明.

$$\varphi(n) = \sum_{i=1}^{n} N(\gcd(i,n) \dot{-} 1)$$

$$\gcd(x,y) = \max\{z : (z|x) \wedge (z|y)\} = \max z \leqslant x.[\mathrm{rs}(x,z) + \mathrm{rs}(y,z)]$$

综上, $\varphi \in \mathcal{EF}$. □

1.12 设 $h(x)$ 为 x 的最大素因子的下标, 约定 $h(0) = 0, h(1) = 0$. 例如 $h(88) = 4$, 因为 $88 = 2^3 \times 11$ 的最大素因子 11 是第 4 个素数 p_4, 其下标为 4. 证明: $h \in \mathcal{EF}$.

证明. 由命题 1.30 知, $\mathrm{ep}_n(x) \in \mathcal{EF}$. 而 $h(x) = \max y \leqslant x.[1 \dot{-} \mathrm{ep}_y(x)]$, 所以 $h \in \mathcal{EF}$. □

1.13 设 $f : \mathbb{N} \to \mathbb{N}$ 满足:

$$\begin{aligned} f(0) =& 1, \\ f(1) =& 1, \\ f(x+2) =& f(x) + f(x+1), \end{aligned}$$

证明:

(1) $f \in \mathcal{PRF}$;

(2) $f \in \mathcal{EF}$.

证明. 令 $F(n) = 2^{f(n)}3^{f(n+1)}$, 有 $F(0) = 2^1 \cdot 3^1 = 6$,

$$\begin{aligned} F(n+1) &= 2^{f(n+1)}3^{f(n+2)} \\ &= 2^{f(n+1)}3^{f(n+1)+f(n)} \\ &= 2^{\mathrm{ep}_1(F(n))}3^{\mathrm{ep}_1(F(n))+\mathrm{ep}_0(F(n))} \\ &= H(F(n)) \end{aligned}$$

这里 $H(x) = 2^{\mathrm{ep}_1(x)}3^{\mathrm{ep}_1(x)+\mathrm{ep}_0(x)}$, 由于 $x^y, +, \times, \mathrm{ep} \in \mathcal{EF}$, 所以 $H(x) \in \mathcal{EF}$. 自然 $H(x) \in \mathcal{PRF}$.

因为 $F(0) = 6, F(n+1) = H(F(n)) = H \circ P_2^2(n, F(n))$, 所以 $F = \mathrm{Prim}^0(6, H \circ P_2^2) \in \mathcal{PRF}$.

因为 $f(n) = \mathrm{ep}_0(F(n))$, 所以 $f \in \mathcal{PRF}$.

现在证明 $f \in \mathcal{EF}$.

首先证明 $f(x) \leqslant 2^x$.

因为 $f(0) = 1 \leqslant 2^0, f(1) = 1 \leqslant 2^1, f(x+2) = f(x) + f(x+1) \leqslant 2^x + 2^{x+1} \leqslant 2^{x+1} + 2^{x+1} = 2^{x+2}$, 所以由数学归纳法可证明 $f(x) \leqslant 2^x$.

那么令 $G(n) = 2^{2^n}3^{2^{n+1}}$, 有 $F(n) = 2^{f(n)}3^{f(n+1)} \leqslant 2^{2^n}3^{2^{n+1}} = G(n)$, 而 $G(n) \in \mathcal{EF}$, 那么可以如下构造一番:

$$F \circ P_2^2(x, 0) = F(0) = 6 = S^6 Z(x)$$

$$F \circ P_2^2(x, n+1) = H \circ P_3^3(x, n, F \circ P_2^2(x, n))$$

$$G \circ P_2^2(x, n) \equiv G(n)$$

显然 $S^6 Z \in \mathcal{EF}, H \circ P_3^3 \in \mathcal{EF}, G \circ P_2^2 \in \mathcal{EF}$(前面已经证明 $H \in \mathcal{EF}$), 所以根据定理 1.31, $F \circ P_2^2 \in \mathcal{EF}$, 那么 $F = P_1^1 \circ (F \circ P_2^2) \in \mathcal{EF}$, 因为 $f(n) = \mathrm{ep}_0(F(n))$, 所以 $f \in \mathcal{EF}$. □

1.14 设数论谓词 $Q(x, y, z, v)$ 定义为

$$Q(x, y, z, v) \equiv p(\langle x, y, z \rangle) | v,$$

其中 $p(n)$ 代表第 n 个素数, $\langle x, y, z \rangle$ 是 x, y, z 的 Gödel 编码. 证明: $Q(x, y, z, v)$ 是初等的.

证明. $Q(x, y, z, v)$ 的特征函数为

$$\chi_Q(x, y, z, v) = N^2(\mathrm{rs}(v, p(\langle x, y, z \rangle))),$$

由于 $\langle x, y, z \rangle = 2^x 3^y 5^z \in \mathcal{EF}, N^2, \mathrm{rs}, p \in \mathcal{EF}$

所以 $\chi_Q(x, y, z, v) \in \mathcal{EF}$, 故 $Q(x, y, z, v)$ 是初等的. □

1.15 设 $f : \mathbb{N} \to \mathbb{N}$ 满足:

$$\begin{aligned} f(0) &= 1, \\ f(1) &= 4, \\ f(2) &= 6, \\ f(x+3) &= f(x) + (f(x+1))^2 + (f(x+2))^3, \end{aligned}$$

证明: $f \in \mathcal{PRF}$.

证明. 令 $g(x)=\langle f(x),f(x+1),f(x+2)\rangle$, 那么有 $f(x)=\mathrm{ep}_0(g(x)),g(0)=\langle 1,4,6\rangle$,

$$g(x+1)=\langle \mathrm{ep}_1(g(x)),\mathrm{ep}_2(g(x)),\mathrm{ep}_0(g(x))+(\mathrm{ep}_1(g(x)))^2+(\mathrm{ep}_2(g(x)))^3.$$

令 $H(x)=\langle \mathrm{ep}_1(x),\mathrm{ep}_2(x),\mathrm{ep}_0(x)+(\mathrm{ep}_1(x))^2+(\mathrm{ep}_2(x))^2\rangle$, 那么有 $H(x)\in\mathcal{PRF},g(x+1)=H(g(x))=H\circ P_2^2(x,g(x))$, 也就是

$$g=\mathrm{Prim}^0[\langle 1,4,6\rangle,H\circ P_2^2],$$

所以 $g(x)\in\mathcal{PRF}$, 所以 $f(x)\in\mathcal{PRF}$. □

1.16 设 $f:\mathbb{N}\to\mathbb{N}$ 满足:

$$\begin{aligned}
f(0)&=0,\\
f(1)&=1,\\
f(2)&=2^2,\\
f(3)&=3^{3^3},\\
&\cdots\cdots\cdots\cdots\\
f(n)&=\underbrace{n^{\cdot^{\cdot^{n}}}}_{n\text{个}n},
\end{aligned}$$

证明:$f\in\mathcal{PRF}-\mathcal{EF}$**.**

证明. 令

$$g(n,m)=\underbrace{n^{\cdot^{\cdot^{n}}}}_{m\text{个}n},$$

且 $g(0,0)=0$, 那么 $g(n,m+1)=n^{g(n,m)}$, 也就是说

$$g(n,0)=N^2(n),$$

$$g(n,m+1)=\mathrm{Comp}_2^2[\mathrm{pow},P_1^3,P_3^3](n,m,g(n,m))$$

于是

$$g=\mathrm{Prim}^1[N^2,\mathrm{Comp}_2^2[\mathrm{pow},P_1^3,P_3^3]],$$

得到 $g\in\mathcal{PRF}$, 而 $f(n)=g(n,n)$, 故 $f\in\mathcal{PRF}$.

假设 $f\in\mathcal{EF}$, 那么由定理 1.34, 有

$$\exists k\in\mathbb{N}.\forall x\in\mathbb{N}.f(x)\leqslant G(k,x).$$

其中

$$G(0,x)=x,G(k,x)=\underbrace{2^{\cdot^{\cdot^{2^x}}}}_{k\text{个}2}.$$

取 $x=k+2$, 那么当 $k=0$ 时,$f(2)>G(0,2)$, 当 $k>0$ 时,

$$f(k+2)=\underbrace{(k+2)^{\cdot^{\cdot^{(k+2)}}}}_{(k+2)\text{个}(k+2)},$$

$$G(k,k+2)=\underbrace{2^{\cdot^{\cdot^{2^{k+2}}}}}_{k\text{个}2},$$

显然

$$f(k+2)>\underbrace{(k+2)^{\cdot^{\cdot^{(k+2)}}}}_{(k+1)\text{个}(k+2)}>\underbrace{2^{\cdot^{\cdot^{2^{k+2}}}}}_{k\text{个}2}=G(k,k+2),$$

因此不存在 k 使得 $\forall x\in\mathbb{N}.f(x)\leqslant G(k,x)$, 所以假设不成立, $f\notin\mathcal{EF}$.

综上, $f\in\mathcal{PRF}-\mathcal{EF}$. □

1.17 设 $g:\mathbb{N}\to\mathbb{N}\in\mathcal{PRF}, f:\mathbb{N}^2\to\mathbb{N}$, 满足

$$\begin{aligned}f(x,0)&=g(x),\\ f(x,y+1)&=f(f(\cdots f(f(x,y),y-1),\cdots),0),\end{aligned}$$

证明:$f\in\mathcal{PRF}$.

证明. 先证明 $f(x,y)=g^{2^{y-1}}(x)$ 当 $y\geqslant 1$ 时成立.

当 $y=1$ 时, $f(x,y)=f(x,0)=g(x)$, 成立;

假设当 $y\leqslant k$ 时命题成立, 那么有 $f(x,y)=g^{2^{y-1}}(x)$ 在 $1\leqslant y\leqslant k$ 时对任意的 $x\in\mathbb{N}$ 均成立.

当 $y=k+1$ 时,

$$\begin{aligned}f(x,k+1)&=f(f(\cdots f(f(x,k),k-1),\cdots),0)\\&=f(f(\cdots f(g^{2^{k-1}}(x),k-1),\cdots),0)\\&=f(f(\cdots g^{2^{k-2}}(g^{2^{k-1}}(x)),\cdots),0)\\&=f(g^{2^0}\circ g^{2^1}\circ\cdots\circ g^{2^{k-2}}\circ g^{2^{k-1}}(x),0)\\&=g(g^{\frac{1-2^k}{1-2}}(x))\\&=g^{2^k}(x)\end{aligned}$$

由数学归纳法可知, $f(x,y)=g^{2^{y-1}}(x)$.

现在只要证明 $g^{2^{y-1}}(x)\in\mathcal{PRF}$.

由于 $g(x)\in\mathcal{PRF}$, 所以 $G(x,n)=g^n(x)\in\mathcal{PRF}$(由定义 1.27 可知 $G(x,n)\in\mathcal{ITF}$, 而 $\mathcal{ITF}=\mathcal{PRF}$). 所以只要证明

$$F(y)=\begin{cases}2^{y-1}, & y>0\\ 1, & y=0,\end{cases}$$

$F(y)\in\mathcal{PRF}$ 即可. 而

$$F(y)=\left\lfloor\frac{2^yN^2(y)+2N(y)}{2}\right\rfloor,$$

所以 $F(y)\in\mathcal{PRF}$. 综上, $f\in\mathcal{PRF}$. □

1.18 设 $k \in \mathbb{N}^+$, 函数 $f : \mathbb{N}^k \to \mathbb{N}$ 和 $g : \mathbb{N}^k \to \mathbb{N}$ 仅在有穷个点取不同值, 证明: f 为递归函数当且仅当 g 为递归函数.

证明. 根据对称性, 只要证明 f 为递归函数可以推出 g 为递归函数即可.

由于 f 和 g 仅在有穷个点取不同值, 这些取不同值的点构成一个有穷的集合, 记为 $\mathcal{S}$, 这样, $f(\vec{x}) \neq g(\vec{x})$ 当且仅当 $\vec{x} \in \mathcal{S}$, $f(\vec{x}) = g(\vec{x})$ 当且仅当 $\vec{x} \in \mathbb{N}^k - \mathcal{S}$.

设 $\mathcal{S}$ 有 k 个元素, 那么其可表示为 $\mathcal{S} = \{\vec{x}_1, \vec{x}_2, \cdots, \vec{x}_k\}$, 那么, 有

$$g(\vec{x}) = f(\vec{x})(\prod_{i=1}^{k} \mathrm{eq}(\vec{x}, \vec{x}_i)) + \sum_{i=1}^{k} N(\mathrm{eq}(\vec{x}, \vec{x}_i))g(\vec{x}_i)$$

上式中,eq 被扩展为 $\mathbb{N}^a \times \mathbb{N}^a \to \mathbb{N}$ 的函数, 这不影响其依然是初等函数, 因为可以表示成

$$N^2(\sum_{i=1}^{a} \mathrm{eq}(P_i^a(\vec{x}), P_i^a(\vec{x}_i))).$$

因此, 若 $f \in \mathcal{GRF}$, 即可得到 $g \in \mathcal{GRF}$. □

1.19 证明:

$$f(n) = \left\lfloor \left(\frac{\sqrt{5}+1}{2}\right) n \right\rfloor$$

为初等函数.

证明. 因为 $\frac{\sqrt{5}+1}{2} \leqslant 2$, 所以 $f(n) \leqslant 2n$, 也就是说

$$f(n) = \max x \leqslant 2n. \left[x \leqslant \left(\frac{\sqrt{5}+1}{2}\right) n\right]$$

即在 $[0, 2n]$ 内不大于 $\left(\frac{\sqrt{5}+1}{2}\right)$ 的最大自然数.

$$\begin{aligned}
& x \leqslant \left(\frac{\sqrt{5}+1}{2}\right) n \\
\Leftrightarrow & 2x \leqslant (\sqrt{5}+1)n \\
\Leftrightarrow & 2x - n \leqslant \sqrt{5}n \\
\Leftrightarrow & 4x^2 - 4xn + n^2 \leqslant 5n^2 \\
\Leftrightarrow & x^2 - xn - n^2 \leqslant 0 \\
\Leftrightarrow & x^2 \dot{-} xn \dot{-} n^2 = 0
\end{aligned}$$

所以 $f(n) = \max x \leqslant 2n.[N^2(x^2 \dot{-} xn \dot{-} n^2)] \in \mathcal{EF}$. □

1.20 证明:$\mathrm{Ack}(4, n) \in \mathcal{PRF} - \mathcal{EF}$, 其中 $\mathrm{Ack}(x, y)$ 是 Ackermann 函数.

证明. 记 $f(n) = \mathrm{Ack}(4, n) + 3 = \underbrace{2^{\cdot^{\cdot^{2}}}}_{n+3\text{个}2}$.

令 $g(x, y) = 2^y$, 那么有 $f(0) = 2^{2^2}, f(n+1) = g(n, f(n))$, 即 $f = \mathrm{Prim}^0[2^{2^2}, g]$, 因为 $g \in \mathcal{PRF}$, 所以 $f \in \mathcal{PRF}$, 自然 $\mathrm{Ack}(4, n) \in \mathcal{PRF}$.

假设 $f \in \mathcal{EF}$, 那么对于 $\mathcal{EF}$ 的控制函数 $G(k,x) = \underbrace{2^{2^{\cdot^{\cdot^{2^x}}}}}_{k\text{个}2}$, 存在 $k \in \mathbb{N}$ 使得

$$\forall x \in \mathbb{N}. f(x) \leqslant G(k,x)$$

.

然而, 令 $x = 2k$, 就有

$$f(2k) = \underbrace{2^{\cdot^{\cdot^{2}}}}_{(2k+3)\text{个}2} = G(k, \underbrace{2^{\cdot^{\cdot^{2}}}}_{k+3\text{个}2}) > G(k, 2k) = G(k,x),$$

矛盾, 故 $f \notin \mathcal{EF}$.

而且, $\underbrace{2^{\cdot^{\cdot^{2}}}}_{(2k+3)\text{个}2} - \underbrace{2^{\cdot^{\cdot^{2k}}}}_{(k+1)\text{个}2}$ 在 $k = 0$ 时最小, 此时的值也大于 3, 因此 $\mathrm{Ack}(4,n) \notin \mathcal{EF}$.

综上, $\mathrm{Ack}(4,n) \in \mathcal{PRF} - \mathcal{EF}$. □

1.21 设 $f : \mathbb{N} \to \mathbb{N}$,$f$ 为单射 (1-1) 且满射 (onto), 证明:$f \in \mathcal{GRF} \Leftrightarrow f^{-1} \in \mathcal{GRF}$.

证明. $f^{-1}(y)$ 的值是使得 $f(x) = y$ 的 x 值, 因为 f 为单射, 这样的 x 值是唯一的, 因此

$$f^{-1}(y) = \mu x.[f(x) \ddot{-} y]$$

由于 f 是满射, 因此

$$\forall y \in \mathbb{N}.\ \exists x \in \mathbb{N}\ s.t.\ f(x) \ddot{-} y = 0$$

所以 $F(x,y) = f(x) \ddot{-} y$ 是正则的.

$\mathcal{GRF}$ 对正则 μ-算子封闭, 因此

$$f \in \mathcal{GRF} \Rightarrow f^{-1} \in \mathcal{GRF}$$

因为 f 为单射且满射, 所以 f^{-1} 也是单射且满射, 且 $(f^{-1})^{-1} = f$, 所以 $f^{-1} \in \mathcal{GRF} \Rightarrow f \in \mathcal{GRF}$.

综上, $f \in \mathcal{GRF} \Leftrightarrow f^{-1} \in \mathcal{GRF}$. □

1.22 设 $p(x)$ 为整系数多项式, 令 $f : \mathbb{N} \to \mathbb{N}$ 定义为 $f(a) = p(x) - a$ 对于 x 的非负整数根, 证明: $f \in \mathcal{RF}$.

证明. 令 $p(x) = a_n x^n + \cdots + a_1 x + a_0, \mathcal{P} = \{i | a_i > 0\}, \mathcal{N} = \{i | a_i < 0\}$, 有

$$|p(x) - a| = \sum_{i \in \mathcal{P}} |a_i| x^i \ddot{-} \left(a + \sum_{i \in \mathcal{N}} |a_i| x^i \right)$$

此时 $\ddot{-}$ 两边的式子都是正整系数多项式, 因此 $|p(x) - a| \in \mathcal{EF}$.

而 $f = \mu x.[|p(x) - a|]$, 即 $f(a)$ 是让 $|p(x) - a| = 0$ 的最小解[3]($|p(x) - a|$ 处处有定义).

所以 $f \in \mathcal{RF}$. □

[3] 题目中只是说明了 $f(a)$ 对于 x 的非负整数根, 但 $f(a)$ 的非负整数根可能不止一个, 此题可能有些问题.

1.23 设

$$f(x)=\begin{cases} x/y, & \text{若}y\neq 0\text{且}y\mid x,\\ \uparrow, & \text{否则}. \end{cases}$$

证明:$f\in\mathcal{RF}$.

证明. 可以看出,$f(x)$ 是使得 $ay=x$ 成立的 a, 且要求 $y\neq 0$ 时才有定义, 故

$$f(x)=\mu a.[(x\dot{-}ay)+N(y)]$$

所以 $f\in\mathcal{RF}$.

□

1.24 设 $g:\mathbb{N}\to\mathbb{N}$ **满足:**

$$\begin{aligned} g(0)&=0,\\ g(1)&=1,\\ g(n+2)&=\mathrm{rs}((2002g(n+1)+2003g(n)),2005), \end{aligned}$$

(1) 试求 $g(2006)$**, (2) 证明** $g\in\mathcal{EF}$**.**

证明. 先考虑这么一个数列:$a_1=0,a_2=1,a_{n+2}=2002a_{n+1}+2003a_n$.

我们希望把上面的递推式改写成 $a_{n+2}-ba_{n+1}=c(a_{n+1}-ba_n)$ 的形式, 那么需要得到合适的 b,c 使得 $b+c=2002,-bc=2003$.

根据韦达定理[4], 上式中的 b,c 是方程 $x^2-2002x+2003=0$ 的两个根, 解得其两个根为-1 和 2003.

有 $a_{n+2}+a_{n+1}=2003(a_{n+1}+a_n)$ 且 $a_{n+2}-2003a_{n+1}=-(a_{n+1}-2003a_n)$, 那么有 $a_{n+1}+a_n=2003^{n-1}(a_2+a_1)=2003^{n-1}$ 且 $a_{n+1}-2003a_n=(-1)^{n-1}(a_2-2003a_1)=(-1)^{n-1}$, 联立解得:

$$a_n=\frac{2003^{n-1}-(-1)^{n-1}}{2004}$$

现在证明 $g(n)\equiv a_{n+1}\pmod{2005}$.

当 $n=0,1$ 时, 显然成立.

假设当 $n\leqslant k(k\geqslant 1)$ 时命题成立, 那么 $g(k)\equiv a_{k+1}\pmod{2005}, g(k-1)\equiv a_k\pmod{2005}$.

当 $n=k+1$ 时, $g(k+1)=\mathrm{rs}((2002g(k)+2003g(k-1)),2005)$, 显然 $g(k+1)\equiv(2002g(k)+2003g(k-1))\pmod{2005}$.

由于 $g(k)\equiv a_{k+1}\pmod{2005}$, 可得 $2002g(k)\equiv 2002a_{k+1}\pmod{2005}$.[5]

由于 $g(k-1)\equiv a_k\pmod{2005}$, 可得 $2003g(k-1)\equiv 2003a_k\pmod{2005}$.

所以 $2002g(k)+2003g(k-1)\equiv 2002a_{k+1}+2003a_k\pmod{2005}$.[6]

[4]一元二次方程 $ax^2+bx+c=0(a\neq 0)$ 的两个根 x_1,x_2 满足 $x_1+x_2=-\frac{b}{a}, x_1x_2=\frac{c}{a}$.

[5]$a\equiv b\pmod m\Rightarrow an\equiv bn\pmod m, \forall n\in\mathbb{Z}$.

[6]$a\equiv b\pmod m, c\equiv d\pmod m\Rightarrow a\pm c\equiv b\pm d\pmod m$.

所以 $g(k+1) \equiv 2002a_{k+1} + 2003a_k \pmod{2005}$,[7] 即 $g(k+1) \equiv a_{k+2} \pmod{2005}$ 成立. 由数学归纳法得, 命题成立.

故

$$\begin{aligned} g(n) &= \mathrm{rs}(a_{n+1}, 2005) \\ &= \mathrm{rs}(\frac{2003^n - (-1)^n}{2004}, 2005) \\ &= \mathrm{rs}(\frac{2003^n + 1}{2004}\mathrm{rs}(n, 2) + \frac{2003^n - 1}{2004}N(\mathrm{rs}(n, 2)), 2005), \end{aligned}$$

所以 $g \in \mathcal{EF}$.

现在开始求 $g(2006)$.

首先 $g(2006) = \mathrm{rs}(\frac{2003^{2006}-1}{2004}, 2005)$, 即有 $\frac{2003^{2006}-1}{2004} \equiv g(2006) \pmod{2005}$.

因为 $2005 = 5 \cdot 401$, 5 和 401 均为素数, 根据费马小定理[8], 有 $2^4 \equiv 1 \pmod 5, 2^{400} \equiv 1 \pmod{401}$. 我们还有 $2^{400} \equiv 1 \pmod 5$(令 $a = 2^{100}$ 由费马小定理得到). 而 401 和 5 的最小公倍数为 2005, 故 $2^{400} \equiv 1 \pmod{2005}$.[9].

因为 $m \mid (m-a)^2 - a^2$, 所以 $(m-a)^2 \equiv a^2 \pmod m$. 也就是说, $2003^2 \equiv 2^2 \pmod{2005}, 2004^2 \equiv 1^2 \pmod{2005}$. 那么 $2003^{2006} \equiv 2^{2006} \pmod{2005}$.[10]

那么, $\frac{2003^{2006}-1}{2004} \cdot 2004^2 \equiv g(2006) \cdot 1 \pmod{2005}$.[11]即 $(2003^{2006} - 1) \cdot 2004 \equiv g(2006) \pmod{2005}$.

而 $(2003^{2006} - 1) \cdot 2004 \equiv (2^{2006} - 1) \cdot 2004 \pmod{2005}$.

又因为 $2^{400} \equiv 1 \pmod{2005}$, 所以 $2^{2000} \equiv 1 \pmod{2005}, 2^{2006} \equiv 2^6 \pmod{2005}$. 所以 $(2^{2006} - 1) \cdot 2004 \equiv (2^6 - 1) \cdot 2004 \pmod{2005}$. 于是我们得到 $g(2006) \equiv (2^6 - 1) \cdot 2004 \pmod{2005}$, 只要计算 $(2^6 - 1) \cdot 2004$ 除以 2005 的余数即可得到 $g(2006)$.

而 $2004 \equiv -1 \pmod{2005}$, 所以 $63 \cdot 2004 \equiv -63 \pmod{2005}$, 所以 $63 \cdot 2004 \equiv -63 + 2005 \pmod{2005}$, 所以 $g(2006) = 2005 - 63 = 1942$.

□

1.25 设 $f : \mathbb{N} \to \mathbb{N}$ 定义为

$$f(n) = \pi\text{的十进制展开式中第}n\text{位数字}.$$

例如 $f(0) = 3, f(1) = 1, f(2) = 4$. **证明:** $f \in \mathcal{GRF}$.

证明. 由 Hutton's Formula[12]知, $\frac{\pi}{4} = 2\arctan(\frac{1}{3}) + \arctan(\frac{1}{7})$.

而

$$\arctan x = \int_0^x \frac{1}{1+t^2}\mathrm{d}t,$$

[7] $a \equiv b \pmod m, b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$.

[8] 若 a 是一个整数, p 是一个素数, 且 a 不是 p 的倍数, 则有 $a^{p-1} \equiv 1 \pmod p$.

[9] 设 $m_1, m_2, \cdots, m_n$ 的最小公倍数为 $[m_1, m_2, \cdots, m_n]$, 且 $\forall i = 1, 2, \cdots, n. a \equiv b \pmod{m_i}$, 则有 $a \equiv b \pmod{[m_1, m_2, \cdots, m_n]}$

[10] $a \equiv b \pmod m \Rightarrow a^n \equiv b^n \pmod m$.

[11] $a \equiv b \pmod m, c \equiv d \pmod m \Rightarrow ac \equiv bd \pmod m$.

[12] 实际上, 类似 Hutton's Formula 的公式还有许多, 应用最广泛的是梅钦公式 (Machin's Formula), 这一类公式因此也被称为类梅钦公式 (Machin-like Formulas), 详见 `http://mathworld.wolfram.com/Machin-LikeFormulas.html`

$\frac{1}{1+t^2}$ 应用牛顿广义二项式定理[13]展开, $k=n$ 之后的项利用等比数列求和公式, 得到:

$$\frac{1}{1+t^2}=\sum_{i=0}^{n}[(-1)^i x^{2i}]+\frac{(-1)^{n+1}x^{2n+2}}{1+x^2}$$

因此

$$\begin{aligned}\arctan x&=\sum_{i=0}^{n}(-1)^i\int_0^x t^{2i}\mathrm{d}t+\int_0^x\frac{(-1)^{n+1}}{1+t^2}t^{2n+2}\mathrm{d}t\\&=\sum_{i=0}^{n}(-1)^i\frac{x^{2i+1}}{2i+1}+\int_0^x\frac{(-1)^{n+1}}{1+t^2}t^{2n+2}\mathrm{d}t\end{aligned}\tag{*}$$

为了让余项为正且估计更加精确, 在 (*) 中取 $n=2k+1$.

$$\begin{aligned}\pi&=8\arctan(\frac{1}{3})+4\arctan(\frac{1}{7})\\&=8\sum_{i=0}^{2k+1}(-1)^i\frac{1}{(2i+1)3^{2i+1}}+8\int_0^{\frac{1}{3}}\frac{t^{4k+4}}{1+t^2}\mathrm{d}t\\&+4\sum_{i=0}^{2k+1}(-1)^i\frac{1}{(2i+1)7^{2i+1}}+4\int_0^{\frac{1}{7}}\frac{t^{4k+4}}{1+t^2}\mathrm{d}t\end{aligned}$$

令

$$\begin{aligned}t_k&=8\sum_{i=0}^{2k+1}(-1)^i\frac{1}{(2i+1)3^{2i+1}}+4\sum_{i=0}^{2k+1}(-1)^i\frac{1}{(2i+1)7^{2i+1}}\\r_k&=8\int_0^{\frac{1}{3}}\frac{t^{4k+4}}{1+t^2}\mathrm{d}t+4\int_0^{\frac{1}{7}}\frac{t^{4k+4}}{1+t^2}\mathrm{d}t\\&\leqslant 8\int_0^{\frac{1}{3}}t^{4k+4}\mathrm{d}t+4\int_0^{\frac{1}{7}}t^{4k+4}\mathrm{d}t\\&=8\cdot\frac{1}{3^{4k+5}\cdot(4k+5)}+4\cdot\frac{1}{7^{4k+5}\cdot(4k+5)}\\&<8\cdot\frac{1}{3}\cdot\frac{1}{3^{4k+4}}+4\cdot\frac{1}{7}\cdot\frac{1}{7^{4k+4}}\leqslant\frac{1}{3^{4k}}\leqslant\frac{1}{80^k}\end{aligned}$$

于是 $\pi=t_k+r_k$, 且 $0<r_k<\frac{1}{80^k}$. t_k 无论 k 取多少都为有理数. 这样的话, 我们取 t_k 的第 k 位为 π 的第 k 位时, 由于 $10^k t_k<10^k\pi=10^k(t_k+r_k)<10^k t_k+\frac{1}{8^k}\leqslant 10^k t_k+1$, 这样的误差会使得当 t_k 的第 k 位为 9 以外的数时, 其前面的结果都是准确无误的. (比如, 当我们知道 $3.14<\pi<3.15$ 时, 我们可以保证 3.1 是正确的. 但是思考 0.9999... 的情形, 它的确实结果是 1, 从第 0 位开始就错了)

现在要求当 t_k 的第 k 位为 9 时, 其前面的结果也准确无误. 可以发现, 如果此时 t_{k+1} 的第 $k+1$ 位非 9 时, 由于精度更进了一层, 所以 π 的第 k 位就必然为 9. 由数学归纳法可知, 当 t_k 的第 k 位非 9 时, 必然能保证其估计的 π 值的前 k 位均正确. 但是, 如果从第 l 位出现连续的 9, 那么就无法确定第 $l-1$ 位是 t_{l-1} 的第 $l+1$ 位还是它的值加 1. 设 t_k 的十进制展开式为

$$t_k=a_{k,0}a_{k,1}a_{k,2}\cdots a_{k,n}\cdots$$

[13] $(x+y)^\alpha=\sum_{k=0}^{\infty}\binom{\alpha}{k}x^{\alpha-k}y^k$. 其中 $\binom{\alpha}{k}=\frac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{k!}$

现在需要证明, 对于任意的 $n \in \mathbb{N}$, 存在 $l \geqslant n+1$ 使得 t_l 满足以下数字不全为 9: $a_{l,n+1}, a_{l,n+2}, \cdots, a_{l,l}$. 这样做就能保证我们那个非 9 所在位之前的数均是正确的.

假设这样的 l 不存在, 那么这意味着从第 $n+1$ 位起, 后面的数字均为 9, 出现了循环, 那么这就说明 π 是有理数, 矛盾. 因此上面的命题是正确的.

这样还能带来一个好处, 就是取第 k 位时, 第 k 位也是正确的, 因为 0.9999... 的情形不用再考虑了, 当知道 $2.9 < a < 3$ 时, 我们也能确定 a 展开式以 2.9 开头.

令 $l = l(n) = \mu l.[l \geqslant n+1$ 且在 $a_{l,n+1}, \cdots, a_{l,l}$ 并不全为 9$]$,$a(l,i) = a_{l,i} = t_l$ 展开式的第 i 个数字 $= \mathrm{rs}(\lfloor t_l \cdot 10^i \rfloor, 10) \in \mathcal{EF}$.

现在能保证 t_l 展开式中 l 所在位及其之前的数均正确, 即 $f(n) = a(l,n)$. 而

$$l(n) = \mu l.\left[(l \geqslant n+1) \wedge \prod_{i=n+1}^{l} [a_{l,i} \dot{-} 9 \neq 0]\right] \in \mathcal{GRF}.^{14}$$

因此

$$f(n) = a(l(n), n) \in \mathcal{GRF}.$$

□

---

[14]若知道 π 的展开式中连续 9 的个数有上界, 则 $l(n) \in \mathcal{EF}$.

2 算盘机

2.1 构造 AM 计算函数 $f(x)=2x$.

解. $f=\langle S_1A_2A_3\rangle_1\,\mathrm{move}_{2,1}\mathrm{move}_{3,1}$ □

2.2 构造 AM 计算函数 $f(x)=\lfloor x/2\rfloor$.

解. $f=A_1\langle S_1S_1A_2\rangle_1\,\mathrm{move}_{2,1}S_1$. □

2.3 构造 AM 计算函数 $f(x,y)=x\cdot y$.

解. $f=\mathrm{move}_{1,3}\left\langle\mathrm{copy}_{3,1,4}S_2\right\rangle_2 Z_3$ □

2.4 构造 AM 计算函数 $f(x)=2^x$.

解. $f=\mathrm{move}_{1,2}A_1\left\langle\mathrm{copy}_{1,3}\mathrm{move}_{3,1}S_2\right\rangle_2$. □

2.5 设 $f:\mathbb{N}\to\mathbb{N}$ 且 $F\in$AM 计算函数 f, 构造算盘机 G 使得

$$(0,0,0,\cdots,0,\cdots)G=\begin{cases}(a,0,0,\cdots) & ,\text{若}a\text{为}f\text{的最小根},\\ \uparrow & ,\text{若}f\text{无根}.\end{cases}$$

解. 思路如下: 一个档专门表示自变量 x, 假设 f 需要再额外用到 k 个档, 先计算 $f(0)$, 若为 0, 不进行操作. $k+2$ 档即 x 自增 1, 清除 1 档结果后复制到 1 档, 计算 $f(x)$, 如果 1 档 (即 f 的值) 的数不为 0 则重复, 到达 0 后, 移动到 1 档, 完成. 如果没有根, 这个算盘机将永远算下去.

若 f 需要 k 个档, 这个算盘机可表示为

$$f\left\langle A_{k+2}Z_1\mathrm{copy}_{k+2,1,k+3}f\right\rangle_1\mathrm{move}_{k+2,1}.$$

□

3 λ-演算

3.1 证明括号引理: 对于任何 $M \in \Lambda$, 在 M 中出现的左括号的个数等于在 M 中出现的右括号的个数.

证明. 令 $L(M)$ 为在 M 中出现的左括号的个数, $R(M)$ 为在 M 中出现的右括号的个数. 现在只要证明: 对于任何 $M \in \Lambda$, $L(M) = R(M)$.

当 $M \in \nabla$ 时, $L(M) = R(M) = 0$, 命题成立.

假设当 $M, N \in \Lambda$ 时, $L(M) = R(M)$, $L(N) = R(N)$, 那么令 $C = (MN)$, 有 $L(C) = L(M) + L(N) + 1$, $R(C) = R(M) + R(N) + 1$, 可得 $L(C) = R(C)$.

假设当 $M \in \Lambda, x \in \nabla$ 时, $L(M) = R(M)$, 那么令 $F = (\lambda x.M)$, 有 $L(F) = L(M) + 1, R(F) = R(M) + 1$, 可得 $L(F) = R(F)$.

由结构归纳法可得, 命题成立. □

3.2 试求 $SSSS$ 的 β-nf.

解. 对第一版答案做出补充说明.根据定义, $S \equiv \lambda xyz.xz(yz)$. 注意: 对于 SS，第一个 S 和第二个 S 的变元不同. 不妨令第一个 S 为 $S \equiv \lambda xyz.xz(yz)$, 第一个 S 为 $S \equiv \lambda abf.af(bf)$. 首先化简 SS，再化简 $SSSS$.

那么

$$
\begin{aligned}
SS &=_\beta \lambda yz.Sz(yz) \\
&=_\beta \lambda yz.\ (\lambda abf.af(bf))\ z(yz) \\
&=_\beta \lambda yz.\lambda f.zf((yz)f) \\
&\equiv \lambda yzf.zf(yzf) \\
&\equiv \lambda xyz.yz(xyz)
\end{aligned}
$$

接下来再求 $SSSS$ 的值, 由于 $SSSS =_\beta SS(SS)$, 一直进行规约化简有 (注意第一个 SS 和第二个 SS 的变元不同):

$$
\begin{aligned}
SSSS &=_\beta SS(SS) \\
&=_\beta \lambda yz.yz(SSyz) \\
&=_\beta \lambda yz.yz(\lambda f.zf(yzf)) \\
&\equiv \lambda xy.xy(\lambda z.yz(xyz)) \qquad (*)
\end{aligned}
$$

到了 (*) 式后, 已经没有含有 β-可约式的子项, 故 (*) 式即为 $SSSS$ 的 β-nf. □

3.3 证明: $(\lambda x.xxx)(\lambda x.xxx)$ 没有 β-nf.

证明.

$$
\begin{aligned}
(\lambda x.xxx)(\lambda x.xxx) &\to_\beta (\lambda x.xxx)(\lambda x.xxx)(\lambda x.xxx) \\
&\to_\beta (\lambda x.xxx)(\lambda x.xxx)(\lambda x.xxx) \\
&\to_\beta (\lambda x.xxx)(\lambda x.xxx)(\lambda x.xxx)(\lambda x.xxx)
\end{aligned}
$$

可以看出, 若令 $(\lambda x.xxx) = N$, 记 $\underbrace{NN\cdots N}_{k\text{个}N}$ 为 N^k, 那么可以发现对任意 $k > 1$, $N^k \to_\beta N^{k+1}$, 因此每次做 β-归约一次, 得到的式子都包含 NN 这个有 β-可约式, 永远都无法归约得到 β-nf. 所以 $(\lambda x.xxx)(\lambda x.xxx)$ 没有 β-nf. □

3.4 设 $F \in \Lambda$ 呈形 $\lambda x.M$, 证明:

(1) $\lambda z.Fz =_\beta F$;

(2) $\lambda z.yz \neq_\beta y$.

注意, 对于一般的 F, $\lambda z.Fz \neq_\beta F$, **但** $\lambda z.Fz =_\eta F$.

证明. 对第一版答案做出了补充说明.呈形英文: is of the form, 即表示其表达式呈现出这样.
$\lambda z.Fz \equiv \lambda z.(\lambda x.M)z =_\beta \lambda z.M[x := z] \equiv F \quad (\lambda z.M[x := z]$ 呈现出 $\lambda x.M$ 形状，故其恒等于 $F)$.

$\lambda z.yz$ 本身已是 β-nf, 其无法 β-归约到 y. □

3.5 证明二元不动点定理: 对于任何 $F, G \in \Lambda$, 存在 $X, Y \in \Lambda$, 满足

$$FXY = X,$$

$$GXY = Y.$$

证明. 根据一元不动点定理, 一定存在 Y 使得 $GXY = Y$, 这可以表示为 $Y = \mathbf{\Theta}(GX)$, 其中 $\mathbf{\Theta}$ 为不动点组合子.

那么现在只要证明, 对于任何 $F, G \in \Lambda$, 存在 $X \in \Lambda$, 满足 $FX(\mathbf{\Theta}(GX)) = X$.

而 $FX(\mathbf{\Theta}(GX)) = X \Rightarrow (\lambda x.Fx(\mathbf{\Theta}(Gx)))X = X$ (根据 $(\beta), (\sigma), (\tau)$), 于是

$$X = \mathbf{\Theta}(\lambda x.Fx\mathbf{\Theta}(Gx)).$$

再将求得的 X 解带入到 Y 中，消去 X，有：

$$\begin{aligned} X =& \mathbf{\Theta}(\lambda x.Fx(\mathbf{\Theta}(Gx))), \\ Y =& \mathbf{\Theta}(G\mathbf{\Theta}(\lambda x.Fx(\mathbf{\Theta}(Gx)))) \end{aligned}$$

此时的 X 和 Y 对任何 $F, G \in \Lambda$ 满足 $FXY = X, GXY = Y$. □

3.6 证明: 对任何 $M, N \in \Lambda^\circ$, 方程 $xN = Mx$ 对于 x 有解.

证明. 令 x 呈形 $\lambda a.B$, 那么有 $xN = B$ 成立, 问题可转化为 $B = M\lambda a.B$ 对 B 有解.

$$B = M(\lambda a.B) \Rightarrow B = (\lambda b.M(\lambda a.b))B.$$

令 $\mathbf{Y}$ 为不动点组合子, 那么 $B = \mathbf{Y}(\lambda b.M(\lambda a.b))$.

因此 x 有解, $x = \lambda c.\mathbf{Y}(\lambda b.M(\lambda a.b))$ 可使等式 $xN = Mx$ 成立. □

3.7 证明: 对任何 $P, Q \in \Lambda$, 若 $P \twoheadrightarrow_\beta Q$, 则存在 $n \geqslant 0$ 以及 $P_0, \cdots, P_n \in \Lambda$, 满足

(1) $P \equiv P_0$;

(2) $Q \equiv P_n$;

(3) 对任何 $i < n, P_i \rightarrow_\beta P_{i+1}$.

证明. 由于关系 $\twoheadrightarrow_\beta$ 是关系 $\rightarrow_\beta$ 的自反传递闭包, 因此对于所有的 $P, Q \in \Lambda$,

$$\twoheadrightarrow_\beta = \bigcup_{i \in \mathbb{N}} (\rightarrow_\beta)^i.$$

因此, $P \twoheadrightarrow_\beta Q$ 可以等价地表述为: 存在 $n \in \mathbb{N}$, 使得 $P(\rightarrow_\beta)^n Q$.

因此, 对任意 $i = 1, 2, \cdots, n-1$, 令 $P(\rightarrow_\beta)^i P_i$, 即可满足题中所给的 3 个条件. □

3.8 证明: 对于任意 $P, Q \in \Lambda$, 若 $P \twoheadrightarrow_\beta Q$, 则 $\lambda z.P \twoheadrightarrow_\beta \lambda z.Q$.

证明. 根据题 3.7 的结论, $P \twoheadrightarrow_\beta Q$ 可得到存在 $P_0, \cdots, P_n \in \Lambda$ 使得 $P \equiv P_0, Q \equiv P_n, P_i \equiv P_{i+1}$.

由于 $\rightarrow_\beta$ 是 β 的合拍闭包, 因此可得对任意 $A, B \in \Lambda$, 若 $A \rightarrow_\beta B$, 则 $\lambda x.A \rightarrow_\beta \lambda x.B$. 于是有 $\lambda z.P_i \rightarrow_\beta \lambda z.P_{i+1}$ 对任意自然数 $i, i < n$ 都成立.

因此, $\lambda z.P \twoheadrightarrow_\beta \lambda z.Q$. □

3.9 证明: 对于任意 $P, Q \in \Lambda$, 若 $P =_\beta Q$, 则存在 $n \in \mathbb{N}$ 以及 $P_0, \cdots, P_n \in \Lambda$, 满足

(1) $P \equiv P_0$;

(2) $Q \equiv P_n$;

(3) 对任何 $i < n$, $P_i \rightarrow_\beta P_{i+1}$ 或 $P_{i+1} \rightarrow_\beta P_i$.

证明. 由于 $=_\beta$ 是 $\twoheadrightarrow_\beta$ 的对称闭包, 因此 $=_\beta = \{\twoheadrightarrow_\beta, \twoheadrightarrow_\beta^{-1}\}$, 后者定义为, $A, B \in \Lambda, A \twoheadrightarrow_\beta B$ 当且仅当 $B \twoheadrightarrow_\beta^{-1} A$.

再由题 3.7, 可得

$$=_\beta = \bigcup_{i \in \mathbb{N}} (\rightarrow_\beta \cup \rightarrow_\beta^{-1})^i.$$

因此, 对任意 $i = 1, 2, \cdots, n-1$, 令 $P(=_\beta)^i P_i$, 即可满足题中所给的 3 个条件. □

3.10 证明定理 3.12.

定理 3.12 表述为:

对任何 $M, N \in \Lambda$,

$$M =_\beta N \Leftrightarrow \lambda\beta \vdash M = N.$$

证明. $\lambda\beta$ 的公理表明 $M = M$, $(\lambda x.M)N = M[x := N]$.

由于 $\beta \equiv \{((\lambda x.M)N, M[x := N]) : M, N \in \Lambda \wedge x \in \nabla\}$, 故 $(\lambda x.M)N =_\beta M[x := N]$.

由于 $=_\beta$ 是自反的, 故 $M =_\beta M$.

假设对于所有构造长度不大于 ℓ 的公式 $M=N$ 都有 $\lambda\beta\vdash M=N\Rightarrow M=_\beta N$. 那么对于构造长度为 $\ell+1$ 的公式, 有:

1. $(\sigma): M=N\vdash N=M$, 由于 $=_\beta$ 是对称的, 因此 $N=_\beta M$ 成立.
2. $(\tau): M=N, N=L\vdash M=L$, 由于 $=_\beta$ 是传递的, 因此 $M=_\beta L$ 成立.
3. $(\mu): M=N\vdash ZM=ZN$, 由于 $=_\beta$ 是合拍的, 因此 $ZM=_\beta ZN$ 也成立.
4. $(\nu): M=N\vdash MZ=NZ$, 由于 $=_\beta$ 是合拍的, 因此 $MZ=_\beta NZ$ 也成立.
5. $(\xi): M=N\vdash \lambda x.M=\lambda x.N$, 由于 $=_\beta$ 是合拍的, 因此 $\lambda x.M=\lambda x.N$ 也成立.

因此, $\lambda\beta\vdash M=N\Rightarrow M=_\beta N$.

现在证明 $M=_\beta N\Rightarrow\lambda\beta\vdash M=N$.

$M=_\beta N$ 要么满足 $(M,N)\in\beta$, 这时由二元关系 β 的定义知 $M=N$; 要么 (M,N) 在 (M',N') 的合拍闭包中, 其中 $(M',N')\in\beta$.

由题 3.9 可知, 对所有 $M=_\beta N$, 存在 $n\in\mathbb{N}$ 以及 $P_0,\cdots,P_n\in\Lambda$, 满足 $M\equiv P_0, N\equiv P_n$, 对任何 $i<n$, $P_i\to_\beta P_{i+1}$ 或 $P_{i+1}\to_\beta P_i$.

当 $n=0$ 时, $M=_\beta M\Rightarrow\lambda\beta\vdash M=M$ 由自反性知显然成立.

那么当 $n=k$ 时, 我们假设构造长度为 $m(m<n)$ 时, 所有 $A=_\beta B\Rightarrow\lambda\beta\vdash M=M$. 这样的话, 对于构造序列 $M=P_0,\cdots,P_{n-1},P_n=N$, 有 $\lambda\beta\vdash M=P_{n-1}$. 因为 $P_{n-1}\to_\beta P_n$ 或 $P_n\to_\beta P_{n-1}$ 就是说 $\lambda\beta\vdash P_{n-1}=P_n$, 由 (τ), $\lambda\beta\vdash M=P_{n-1}=P_n=N$. 所以 $M=_\beta N\Rightarrow\lambda\beta\vdash M=N$.

综上, 命题成立. □

3.11 证明定理 3.13.

定理 3.13 表述为:

对任何 $M,N\in\Lambda$,

$$M=_{\beta\eta}N\Leftrightarrow\lambda\beta\eta\vdash M=N.$$

证明. 在题 3.10 的基础上, 只要证明 $\lambda x.Mx=_{\beta\eta}M$ 即可. 而这从二元关系 η 的定义就可以直接得出. □

3.12 证明: 对于任何 $M,N\in\Lambda$, 若 $M=_\beta N$, 则存在 T 使 $M\twoheadrightarrow_\beta T$ 且 $N\twoheadrightarrow_\beta T$. 这就是对于 $=_\beta$ 的 CR 性质.

证明. 对第一版答案做出了补充说明.

方法一: 由习题 3.9 知: $\exists P_0,\cdots,P_n$ 使 $M\equiv P_0, N\equiv P_n$ 且 $\forall i<n$ 有 $P_i\to_\beta P_{i+1}$ 或 $P_i\leftarrow_\beta P_{i+1}$.

下面证明:

$$\exists T_i\ s.t.\ P_0\twoheadrightarrow_\beta T_i\ and\ P_i\twoheadrightarrow_\beta T_i\quad(\star)$$

对 i 做归纳证明.

1) 当 $i=0$ 时, 取 T_0 为 M 即可, 此时 $(\star)$ 成立;

2) 假设 $i=k$ 时,$\exists T_k\ s.t.\ P_0\twoheadrightarrow_\beta T_k\ and\ P_k\twoheadrightarrow_\beta T_k$;

3) 当 $i = k+1 < n$ 时, 有 $P_0 \twoheadrightarrow_\beta T_k$ *and* $P_k \twoheadrightarrow_\beta T_k$（归纳假设）, 则

情况 1:$P_k \twoheadrightarrow_\beta P_{k+1}$, 从而由 CR 性质,$\exists T_{k+1}$ *s.t.* $T_k \twoheadrightarrow_\beta T_{k+1}$ *and* $P_{k+1} \twoheadrightarrow_\beta T_{k+1}$, 从而 $(\star)$ 成立;

情况 2:$P_k \leftarrow_\beta P_{k+1}$, 取 T_{k+1} 为 P_k 即可, 此时 $(\star)$ 也成立.

于是归纳完成.

因此有 $\exists T_n$ *s.t.* $P_0 \twoheadrightarrow_\beta T_n$ *and* $P_n \twoheadrightarrow_\beta T_n$, 取 T 为 T_n 即有 $M \twoheadrightarrow_\beta T$ *and* $N \twoheadrightarrow_\beta T$.

方法二: $M =_\beta N$ 蕴含

$$(M, N) \in \bigcup_{i \in \mathbb{N}} (\rightarrow_\beta \cup \leftarrow_\beta)^k.$$

当 $k = 0$ 时, $M =_\beta N$. 假设对所有 $(M, N) \in (\rightarrow_\beta \cup \leftarrow_\beta)^k$, 存在 $T \in \Lambda$ 使得 $M \twoheadrightarrow_\beta T$ 且 $N \twoheadrightarrow_\beta T$.

那么当 $(M, N) \in (\rightarrow_\beta \cup \leftarrow_\beta)^{k+1}$ 时, 要么有 $M \rightarrow_\beta P =_\beta N$, 要么有 $M \leftarrow_\beta P =_\beta N$, 其中 $(P, N) \in (\rightarrow_\beta \cup \leftarrow_\beta)^k$. 那么存在 T_0 使得 $P \twoheadrightarrow_\beta T_0$ 且 $N \twoheadrightarrow_\beta T_0$. 由于 $\twoheadrightarrow_\beta$ 是传递的, 所以 $M \twoheadrightarrow_\beta T_0$.

由于 $\twoheadrightarrow_\beta$ 的 CR 性质, $P \twoheadrightarrow_\beta M$ 且 $P \twoheadrightarrow_\beta T_0$ 可得到, 存在 $T \in \Lambda$ 使得 $M \twoheadrightarrow_\beta T$ 且 $T_0 \twoheadrightarrow_\beta T$. 由于 $\twoheadrightarrow_\beta$ 是传递的, 有 $N \twoheadrightarrow_\beta T_0$ 且 $T_0 \twoheadrightarrow_\beta T$, 因此 $N \twoheadrightarrow_\beta T$.

因此对所有的 $k \in \mathbb{N}$, 这样的 T 都存在. 命题成立. □

3.13 证明: 若在系统 $\lambda\beta$ 中加入如下公理

$$\textbf{(A)} \qquad \lambda xy.x = \lambda xy.y,$$

则对任何的 $M, N \in \Lambda$, $\lambda\beta + (A) \vdash M = N$.

证明. 对第一版答案做出了补充. 碰到这种题目, 如果有两个以上的不同变元, 使用标准组合子 $\mathbf{I}, \mathbf{K}, \mathbf{K}^*, \mathbf{S}$(page 78) 来推导即可.

证明方法一：对于所有的 $M, N \in \Lambda$,

$$\lambda xy.x = \lambda xy.y$$

$$\Rightarrow (\lambda xy.x)MN = (\lambda xy.y)MN$$

$$\Rightarrow M = N$$

证明方法二 (推荐):

$$\lambda xy.x = \lambda xy.y$$

$$\Rightarrow (\lambda xy.x)\mathbf{I}M = (\lambda xy.y)\mathbf{I}M$$

$$\Rightarrow \mathbf{I} = M$$

同理, 可以推导出:

$$\mathbf{I} = N$$

$$\Rightarrow M = N$$

故有 $\lambda\beta + (A) \vdash M = N$.

□

3.14 证明命题 3.14.

命题 3.14 表述为:

设 R 是 Λ 上的一个二元关系, $M \in \mathrm{NF}_R$, 则

(1) 不存在 $N \in \Lambda$ 使得 $M \to_R N$;

(2) $M \twoheadrightarrow_R N \Rightarrow M \equiv N$.

证明. (1) 由 NF_R 的定义可知其成立;

(2) 假设 $M \not\equiv N$. $M \twoheadrightarrow_R N$ 表示存在 $M = P_0, \cdots, P_n = N$ 使得对任意 $i < n, P_i \to_R P_{i+1}$. 由于 $M \not\equiv N$, $n \geqslant 1$. 但是这样就存在 N 使得 $M \to_R N$, 与 (1) 矛盾. 因此 $M \equiv N$. □

3.15 证明引理 3.16.

引理 3.16 表述为:

若 $M \rhd_{\mathrm{mcd}} M'$ 且 $N \rhd_{\mathrm{mcd}} N'$, 则 $MN \rhd_{\mathrm{mcd}} M'N'$.

证明. $M \rhd_{\mathrm{mcd}} M'$ 说明存在序列 $M_1, M_2, \cdots, M_n$ 将 M 归约到 M', $N \rhd_{\mathrm{mcd}} N'$ 同理.

由于 M_i 恒为剩余序列的极小可约式, 所以 $MN \rhd_{\mathrm{mcd}} M'N'$. □

3.16 试找出 $A \in \Lambda^\circ$ 使 A λ-定义函数 $f(x, y) = x + y$.

解. 对第一版答案做出了修正.(遇到这种题目需要反推. 只要知道 $\lambda fx.f^n x \Leftarrow \lambda fx.\ulcorner n \urcorner fx$ 就好做了)

因为 $\ulcorner n \urcorner \equiv \lambda ab.a^n b$, 于是 $\lambda fx.\ulcorner n \urcorner fx = \lambda fx.((\lambda ab.a^n b)fx) = \lambda fx.f^n x$.

构造 $A\ulcorner n \urcorner \ulcorner m \urcorner = \ulcorner n + m \urcorner = \lambda fx.f^{n+m}x = \lambda fx.f^n(f^m x)$. 于是有:

$$\begin{aligned}\lambda fx.f^n(f^m x) &= \lambda fx.\ulcorner n \urcorner f(\ulcorner m \urcorner fx) \\ &= (\lambda vfx.\ulcorner n \urcorner f(vfx))\ulcorner m \urcorner \\ &= (\lambda uvfx.uf(vfx))\ulcorner n \urcorner \ulcorner m \urcorner.\end{aligned}$$

因此, $A \equiv \lambda uvfx.uf(vfx)$ λ-定义函数 $f(x, y) = x + y$. □

3.17 试找出 $F \in \Lambda^\circ$ 使 F λ-定义函数 $f(x) = 3x$.

解. 与上一题很类似. 得知道 $\lambda fx.f^n x \Leftarrow \lambda fx.\ulcorner n \urcorner fx$.

构造 $F\ulcorner n \urcorner = \ulcorner 3n \urcorner = \lambda fx.f^n(f^n(f^n x))$.

$$\begin{aligned}\lambda fx.f^n(f^n(f^n x)) &= \lambda fx.f^n(f^n(\ulcorner n \urcorner fx)) \\ &= \lambda fx.f^n(\ulcorner n \urcorner f(\ulcorner n \urcorner fx)) \\ &= \lambda fx.\ulcorner n \urcorner f(\ulcorner n \urcorner f(\ulcorner n \urcorner fx)) \\ &= [\lambda nfx.nf(nf(nfx))]\ulcorner n \urcorner.\end{aligned}$$

因此, $F \equiv \lambda xyz.xy(xy(xyz))$ λ-定义函数 $f(x) = 3x$. □

3.18 令 $D \equiv \lambda xyz.z(Ky)x$，证明：对于任意的 $X, Y \in \Lambda$，

$$DXY\ulcorner 0\urcorner = X,$$
$$DXY\ulcorner n+1\urcorner = Y.$$

这里 $K \equiv \lambda xy.x, \ulcorner n\urcorner \equiv \lambda fx.f^n x$。

证明. $DXY\ulcorner 0\urcorner = \ulcorner 0\urcorner(\lambda y.Y)X = (\lambda fx.x)(\lambda y.Y)X = X$, 且

$$\begin{aligned} DXY\ulcorner n+1\urcorner &= \ulcorner n+1\urcorner(\lambda y.Y)X \\ &= (\lambda fx.f^{n+1}x)(\lambda y.Y)X \\ &= (\lambda x.(\lambda y.Y)^{n+1}x)X \\ &= (\lambda x.(\lambda y.Y)^n Y)X \\ &= (\lambda x.Y)X = Y. \end{aligned}$$

□

3.19 设 $\text{Exp} \equiv \lambda xy.yx$，证明：对于任意的 $n \in \mathbb{N}$ 和 $m \in \mathbb{N}^*$，

$$\text{Exp}\ulcorner n\urcorner\ulcorner m\urcorner =_\beta \ulcorner n^m\urcorner.$$

(Exp 由 Rosser 教授作出)

证明. 将 Exp 展开, 得:

$$\begin{aligned} \text{Exp}\ulcorner n\urcorner\ulcorner m\urcorner &= (\lambda xy.yx)(\lambda fx.f^n x)(\lambda fx.f^m x) \\ &= (\lambda fx.f^m x)(\lambda fx.f^n x) \\ &= (\lambda x.(\lambda fy.f^n y)^m x). \end{aligned}$$

当 $m = 1$ 时, $(\lambda fy.f^n y)x = \lambda y.x^n y$. 假设 $(\lambda fy.f^n y)^m x = \lambda y.x^{n^m} y$, 有

$$\begin{aligned} (\lambda fy.f^n y)^{m+1} x &= (\lambda fy.f^n y)[(\lambda fy.f^n y)^m x)] \\ &= (\lambda fy.f^n y)(\lambda y.x^{n^m} y) \\ &= \lambda y.(\lambda z.x^{n^m} z)^n y \\ &= \lambda y.x^{n^{m+1}} y. \end{aligned}$$

因此, $\text{Exp}\ulcorner n\urcorner\ulcorner m\urcorner = \lambda xy.x^{n^m} y = \ulcorner n^m\urcorner$ 对任意自然数 $m > 0$ 都成立. □

3.20 构造 $F \in \Lambda^\circ$ 使得对于任何 $n \in \mathbb{N}$，

$$F\ulcorner n\urcorner =_\beta \ulcorner 2^n\urcorner.$$

解. 对第一版答案进行了补充说明.

方法一: 由引理 3.33(page 97) 得, 存在 $D \in \Lambda^\circ$, 使得其能够完成 if-else 功能.

注意到 $\text{Exp} \equiv \lambda xy.yx$ 能够实现一个指数函数功能，但是指数的取值为 $\mathbb{N}^*$. 这一题给定的指数范围是 $\mathbb{N}$, 于是使用 D 来实现 if-else 判断. 构造结果如下:

$$F \equiv \lambda x.Dx\ulcorner 1\urcorner(\text{Exp}\ulcorner 2\urcorner x).$$

方法二: 设 H $\lambda-$ 定义函数 $h(x)=2x$.

$$\begin{aligned}\lambda fx.f^n(f^n x) &= \lambda fx.\ulcorner n\urcorner f(\ulcorner n\urcorner fx)\\ &= (\lambda vfx.vf(vfx))\ulcorner m\urcorner.\end{aligned}$$

于是 $H\equiv \lambda vfx.vf(vfx)$ $\lambda-$ 定义函数 $h(x)=2x$. 注意到:

$$\ulcorner 2^x\urcorner = \ulcorner 2\cdot 2^{x-1}\urcorner = H\ulcorner 2^{x-1}\urcorner = H(H\ulcorner 2^{x-2}\urcorner) = H^x\ulcorner 2^0\urcorner = H^x\ulcorner 1\urcorner = \ulcorner x\urcorner F\ulcorner 1\urcorner = (\lambda x.xH\ulcorner 1\urcorner)\ulcorner x\urcorner$$

令 $F\equiv \lambda x.xH\ulcorner 1\urcorner$, 则对于任何 $n\in\mathbb{N}, F\ulcorner n\urcorner =_\beta \ulcorner 2^n\urcorner$.

□

3.21 设 $f,g:\mathbb{N}\to\mathbb{N}, f=\mathrm{Itw}[g]$, 即

$$f(0)=0,$$
$$f(n+1)=g(f(n)),$$

且 $G\in\Lambda^\circ$ λ-定义函数 g. 试求 $F\in\Lambda^\circ$ 使得 F λ-定义函数 f.

证明. 令 $D\equiv[U_3^3,U_1^2]$, 于是将 f 用 $if-else$ 语句表示有:

$$\begin{aligned}F\ulcorner n\urcorner &= D\ulcorner n\urcorner\ulcorner 0\urcorner G(F(\mathrm{pred}\ulcorner n\urcorner))\\ &= \lambda x.Dx\ulcorner 0\urcorner G(F(\mathrm{pred}\ x))\ulcorner n\urcorner\\ &= \Big(\lambda fx.\mathrm{D}x\ulcorner 0\urcorner G\big(f(\mathrm{pred}\ x)\big)\Big)F\ulcorner n\urcorner.\end{aligned}$$

由一元不动点定理 (page 93 定理 3.22) 可以求出 F, 用 Θ 表示不动点组合子.
于是 $F\equiv\Theta\Big(\big(\lambda fx.\mathrm{D}x\ulcorner 0\urcorner G\big(f(\mathrm{pred}\ x)\big)\big)\Big)$ λ-定义函数 f.

□

3.22 证明引理 3.39.

引理 3.39 表述为:
存在一般递归函数 $\mathrm{var},\mathrm{app},\mathrm{abs},\mathrm{num}:\mathbb{N}\to\mathbb{N}$ 使得:

(1) $\forall n\in\mathbb{N}.\mathrm{var}(n)=\sharp(v^{(n)})$;

(2) $\forall M,N\in\Lambda.\mathrm{app}(\sharp M,\sharp N)=\sharp(MN)$;

(3) $\forall x\in\nabla, M\in\Lambda.\mathrm{abs}(\sharp x,\sharp M)=\sharp(\lambda x.M)$;]

(4) $\forall n\in\mathbb{N}.\mathrm{num}(n)=\sharp\ulcorner n\urcorner$.

证明. 对第一版答案进行了补充说明.取 $[x,y]=2^x{\cdot}3^y, \Pi_1=ep_1, \Pi_2=ep_1$, 从而 $[\cdot,\cdot],\Pi_1,\Pi_2\in\mathcal{EF}$.

(1) 由于 $v^{(n)}=[0,n]\in\mathcal{EF}$, 取 $\mathrm{var}(n)$=$[0,n]$ 即可;

(2) 取 $\mathrm{app}(m,n)$=$[1,[m,n]]\in\mathcal{EF}$, 则 $\mathrm{app}(\sharp M,\sharp N)=\sharp(MN)$;

(3) 取 $\mathrm{abs}(n,m)$=$[2,[\mathrm{var}(n),m]]\in\mathcal{EF}$, 易验证 $\mathrm{abs}(\sharp v^{(n)},\sharp M)=\sharp(\lambda v^{(n)}.M)$;

(4) 下面证 $\forall n \in \mathbb{N}.\mathrm{num}(n) = \sharp\ulcorner n \urcorner$, 且 $\mathrm{num}(n)$ 是递归的:

$$\begin{aligned}\ulcorner n+1 \urcorner &= \sharp(\lambda fx.f^{n+1}x)\\ &= \left[2, \left[\sharp f, [2, [\sharp x, \sharp f^{n+1}x]]\right]\right]\\ &= \left[2, \left[\sharp f, \left[2, \left[\sharp x, [1, [\sharp f, \sharp f^n x]]\right]\right]\right]\right]\end{aligned}$$

$$\begin{aligned}\ulcorner n \urcorner &= \sharp(\lambda fx.f^n x)\\ &= \left[2, \left[\sharp f, [2, [\sharp x, \sharp f^n x]]\right]\right]\end{aligned}$$

故有:

$$\sharp f^n x = \Pi_2(\Pi_2(\Pi_2(\Pi_2(\sharp\ulcorner n \urcorner)))) = \Pi_2^4(\sharp\ulcorner n \urcorner)$$

于是

$$\ulcorner n+1 \urcorner = \left[2, \left[\sharp f, \left[2, \left[\sharp x, [1, [\sharp f, \Pi_2^4(\sharp\ulcorner n \urcorner)]]\right]\right]\right]\right]$$

令 $h(z) = \left[2, \left[\sharp f, \left[2, \left[\sharp x, [1, [\sharp f, \Pi_2^4(z)]]\right]\right]\right]\right]$,$\mathrm{num}(0) = \ulcorner 0 \urcorner$, 于是:

$$\mathrm{num}(n+1) = h(\mathrm{num}(n))$$

因此 $\mathrm{num} \in \mathcal{PRF}$,$\mathrm{num}(n) = \ulcorner n \urcorner$.

□

3.23 设 $f(n)$ 为习题 1.16 中定义的函数，试构造 $F \in \Lambda^\circ$ 使 $F\ulcorner n \urcorner = \ulcorner f(n) \urcorner$ 对 $n \in \mathbb{N}^+$ 成立.

证明. 对第一版答案做出了修正. 习题 1.16 定义的函数 $f(n)$ 为:

$$\begin{aligned}f(0) &= 0,\\ f(n) &= \underbrace{n^{\cdot^{\cdot^{n}}}}_{n\text{个}n},\end{aligned}$$

令 $w_n = \lambda x.\underbrace{x \cdots x}_{n\text{个}x}$,$n \in \mathbb{N}^+$,$x$ 为 $v^{(0)}$. 令 $[x, y] = 2^x \cdot 3^y$, $\Pi_2[x, y] = y$. 于是

$$\sharp v^{(0)} = [0, 0] = 1$$

则 $\sharp x = [0, 0] = 1$.

令 $h(n) = \sharp w_n (n \geqslant 1)$, 于是

$$h(n) = \sharp w_n = [2, [\sharp x, \sharp \underbrace{x \cdots x}_{n\text{个}x}]]$$

补充定义 $h(0) = 0$. 现证明 $h(n) \in \mathcal{PRF}$:

$$\begin{aligned}h(n+1) &= \sharp w_{n+1}\\ &= [2, [\sharp x, \sharp \underbrace{x \cdots x}_{n+1\text{个}x}]]\\ &= [2, [\sharp x, [1, [\sharp \underbrace{x \cdots x}_{n\text{个}x}, \sharp x]]]] \quad \text{(according to definition 3.36(2))}\end{aligned}$$

注意到:

$$\sharp\underbrace{x\cdots x}_{n个x}=\Pi_2(\Pi_2(h(n)))=\Pi_2^2(h(n))$$

根据 $\sharp x=[0,0]=1$ 和 $h(n+1)=[2,[\sharp x,[1,[\sharp\underbrace{x\cdots x}_{n个x},\sharp x]]]]$, 有:

$$h(n+1)=[2,[1,[1,[\Pi_2^2(h(n)),1]]]]$$

于是 $h(n)\in\mathcal{PRF}$.

由定理 3.41(page 101), 存在枚举子 E, 使得:

$$E(H\ulcorner n\urcorner)=E\ulcorner w_n\urcorner=w_n$$

取 $M\equiv\lambda z.(E(Hz))z$, 于是:

$$\begin{aligned}M\ulcorner n\urcorner &= (E(H\ulcorner n\urcorner))\ulcorner n\urcorner\\ &= w_n\ulcorner n\urcorner\\ &= \underbrace{\ulcorner n\urcorner\cdots\ulcorner n\urcorner}_{n个n}\\ &= \ulcorner\underbrace{n^{\cdot^{\cdot^{n}}}}_{n个n}\urcorner\quad(n\geqslant 1)\end{aligned}$$

由于 $n\in\mathbb{N}$, 因此 M 此时不能完全 $\lambda-$可定义 $f(n)$, 缺少 $n=0$ 的情况. 由引理 3.33, 令 $D\equiv[U_3^3,U_1^2]$.

取 $L\equiv\lambda z.Dz\ulcorner 0\urcorner(Mz)$, 此时 L $\lambda-$可定义 $f(n)$.

□

3.24 构造 $H\in\Lambda^\circ$, 使得对于任意 $n\in\mathbb{N},x_1,\cdots,x_n\in\Lambda$, 有

$$H\ulcorner n\urcorner x_1\cdots x_n=_\beta\lambda z.zx_1\cdots x_n.$$

证明. 对第一版答案做出了补充.

证法一 (严格证法): 令 $L_n\equiv[x_1,\cdots,x_n]\equiv\lambda z.zx_1\cdots x_n$ $(n\in\mathbb{N})$. 这里 x_i 为第 i 个变元,z 为 $v^{(0)}$, 则 $\sharp z=1$.

设 $l(n)=\sharp L_n$, 约定 $l(0)=0$. 下面证 $l(n)\in\mathcal{GRF}$:

令 $h(n)=\sharp zx_1\cdots x_n$, 则 $l(n)=[2,[\sharp z,\sharp zx_1\cdots x_n]]=[2,[1,h(n)]]$.

$$h(1)=\sharp zx_1=[1,[1,\sharp z_1]]=[1,[1,[0,1]]]$$

$$h(n+1)=\sharp zx_1\cdots x_nx_{n+1}=[2,[h(n),\sharp x_{n+1}]]=[2,[h(n),[0,n+1]]]$$

补充 $h(0)=0$, 故 $h(n)\in\mathcal{PRF}$.

于是

$$l(n)=\begin{cases}0, & if\ n=0,\\ [2,[1,h(n)]], & otherwise.\end{cases}$$

因此 $l(n)\in\mathcal{PRF}$.

令 $M_n = \lambda x_1 \cdots x_n.[x_1, \cdots, x_n]$,$g(n) = \sharp M_n$, 于是有:

$$g(n) = \sharp M_n = [2, [\sharp x_1, [2, \cdots [2, [x_n, l(n)]] \cdots]]]$$

其中 $\sharp x_i = [0, i]$. 令 $f(i, y) = [2, [[0, i], y]] \in \mathcal{PRF}$. 则

$$g(n) = f(1, f(2, \cdots, f(n-1, f(n, l(n))) \cdots))$$

类比于习题 1.17, 可证 $g(n) \in \mathcal{PRF}$. 故存在 $G \in \Lambda^\circ, G$ $\lambda-$ 定义 g. 从而 $G\ulcorner n \urcorner = \ulcorner M_n \urcorner$.

由定理 3.21(page 101), 存在 E, 使得 $E(G\ulcorner n \urcorner) = E(\ulcorner M_n \urcorner) = M_n$, 令 $H \equiv \lambda z.E(Gz)$, 从而:

$H\ulcorner n \urcorner x_1 \cdots x_n = \lambda z.E(Gz) x_1 \cdots x_n = M_n x_1 \cdots x_n = [x_1, \cdots, x_n] = \lambda z.z x_1 \cdots x_n$.

证法二 (简单证法):

可知我们需要找到 H 使得 $H\ulcorner n \urcorner = \lambda x_1 x_2 \cdots x_n z.z x_1 \cdots x_n$.

我们可以令 $M_n = \lambda x_1 x_2 \cdots x_n z.z x_1 \cdots x_n$, 那么其编码

$$g(n) = \sharp M_n = [2, [\sharp x_1, \sharp(\lambda x_2 \cdots x_n.z x_1 \cdots x_n)]]$$

而 $\sharp(z x_1 \cdots x_n)$ 是递归的, 因此 g 是递归的. 设 $G \in \Lambda^\circ$ λ-定义了 g, 从而 $G\ulcorner n \urcorner =_\beta \ulcorner M_n \urcorner$, 因此

$$E(G\ulcorner n \urcorner) =_\beta E\ulcorner M_n \urcorner =_\beta M_n$$

取 $H \equiv \lambda x.E(Gx)$ 即可.

□

3.25 证明: 存在 $\Theta_2 \in \Lambda^\circ$, 使得对于任意 $F \in \Lambda^\circ$, 有

$$\Theta_2 \ulcorner F \urcorner =_\beta F \ulcorner \Theta_2 \ulcorner F \urcorner \urcorner.$$

证明. 对第一版答案进行了修正. 令 $W \equiv \lambda xy.Ey(\text{App}(\text{App } x(\text{Num } x))(\text{Num } y))$, $\Theta_2 = W\ulcorner W \urcorner$, 对于 $F \in \Lambda^\circ$ 有 $E\ulcorner F \urcorner = F$, 这里 E 是枚举子. 则:

$$\begin{aligned}
\Theta_2 \ulcorner F \urcorner &\equiv W \ulcorner W \urcorner \ulcorner F \urcorner \\
&=_\beta E \ulcorner F \urcorner (\text{App}(\text{App } \ulcorner W \urcorner (\text{Num } \ulcorner W \urcorner))(\text{Num } \ulcorner F \urcorner)) \\
&=_\beta F(\text{App}(\text{App} \ulcorner W \urcorner \ulcorner \ulcorner W \urcorner \urcorner)) \ulcorner \ulcorner F \urcorner \urcorner \\
&=_\beta F \text{App} \ulcorner W \ulcorner W \urcorner \urcorner \ulcorner \ulcorner F \urcorner \urcorner \\
&\equiv F \ulcorner \Theta_2 \ulcorner F \urcorner \urcorner
\end{aligned}$$

因此结论成立. □

3.26 (附加证明题) 证明定理 3.41 的证明过程中提到的 λ-项 B 的存在性.

证明. We can compute **min** by a recursive procedure that keeps a table of variable substitution, and log the minimum unused number in each abstraction operation (very complicated, though). Since every function in $\mathcal{PRF}$ can be represented in λ-calculus, $\mathbf{min} \in \Lambda^\circ$ exists. Also, we have $\mathbf{minus} \in \Lambda^\circ$ such that $\mathbf{minus}\ulcorner x \urcorner \ulcorner y \urcorner = \ulcorner |x - y| \urcorner$. Therefore, let

$$B = \lambda fxyz.\mathbf{D}(\mathbf{minus}(\mathbf{min}y)(\mathbf{min}z))x(fz),$$

$F_{[\ulcorner x \urcorner \mapsto x]} =_\beta BFx\ulcorner x \urcorner$ is achieved.

□

3.27 (附加证明题) 证明: 若在系统 $\lambda\beta$ 中加入

$$(A) \quad \mathbf{I} = \mathbf{S}.$$

做为额外公理, 则对任何的 $M, N \in \Lambda, \lambda\beta + (A) \vdash M = N$.

证明. 碰到这种题目, 如果有两个以上的不同变元, 使用标准组合子 $\mathbf{I}, \mathbf{K}, \mathbf{K}^*, \mathbf{S}$(page 78) 来推导即可.

$$\mathbf{I} = \mathbf{S}$$

$$\Rightarrow \mathbf{IIIK} = \mathbf{SIIK}$$

$$\Rightarrow \mathbf{K} = \mathbf{IK}(\mathbf{IK})$$

$$\Rightarrow \mathbf{K} = \mathbf{KK}$$

$$\Rightarrow \mathbf{KI}M = \mathbf{KKI}M$$

$$\Rightarrow \mathbf{I} = \mathbf{K}M$$

$$\Rightarrow \mathbf{II} = \mathbf{K}M\mathbf{I}$$

$$\Rightarrow \mathbf{I} = M$$

同理，可推到出 $\mathbf{I} = N$. 于是 $M = N$, 因此 $\lambda\beta + (A) \vdash M = N$.

注意: 最好右乘 Λ 项, 因为右乘不需要加括号, 左乘需要加括号. 举个左乘不加括号的错误例子: $\mathbf{I} = \mathbf{I} \Rightarrow \mathbf{I} = \mathbf{II} \Rightarrow \mathbf{KI} = \mathbf{KII} \Rightarrow \mathbf{KI} = \mathbf{I} \Rightarrow \mathbf{KI}M = \mathbf{I}M \Rightarrow \mathbf{I} = M$.

上述推理得 $I = M$, 岂不怪哉? 问题在于 $\mathbf{I} = \mathbf{II} \nRightarrow \mathbf{KI} = \mathbf{KII}$, 即左乘没有加括号. 正确推到过程应该是:$\mathbf{I} = \mathbf{II} \Rightarrow \mathbf{KI} = \mathbf{K}(\mathbf{II})$.

□

3.28 (附加证明题) 证明: 若在系统 $\lambda\beta$ 中加入

$$(A) \quad \lambda x.x = \lambda x.xx.$$

做为额外公理, 则对任何的 $M, N \in \Lambda, \lambda\beta + (A) \vdash M = N$.

证明. 目前只有一个变元, 需要使用投影算子来证明. 令 $U^n_m = \lambda x_1 \cdots x_n.x_m (0 \leqslant m \leqslant n)$, 则 $U^n_m X_1 \cdots X_n = X_m$.

$$\lambda x.x = \lambda x.xx$$

$$\Rightarrow (\lambda x.x)U_1^2 = (\lambda x.xx)U_1^2$$

$$\Rightarrow U_1^2 = U_1^2 U_1^2$$

$$\Rightarrow U_1^2\mathbf{I} = U_1^2 U_1^2\mathbf{I}$$

$$\Rightarrow U_1^2\mathbf{I} = U_1^2$$

$$\Rightarrow U_1^2\mathbf{I}N = U_1^2 N$$

$$\Rightarrow \mathbf{I} = U_1^2 N$$

$$\Rightarrow \mathbf{I}M = U_1^2 NM$$

$$\Rightarrow \mathbf{I}M = N$$

$$\Rightarrow M = N$$

故 $\lambda\beta + (A) \vdash M = N$.

$\square$

4 组合逻辑

4.1 求 $\lambda^* xy.xyy$.

解. $\square$

4.2 令 $C \in \mathbb{C}$ 定义为

$$C \equiv S(BBS)(KK).$$

证明: 对于任意的 $X, Y, Z \in \mathbb{C}, CXYZ = XZY$.

证明. $\square$

4.3 证明: 若 $xP_1 \cdots P_m =_{\mathrm{w}} yQ_1 \cdots Q_n$, 则 $x \equiv y, m \equiv n$, 而且对于任意 $i \leqslant m$, 有 $P_i =_{\mathrm{w}} Q_i$.

证明. $\square$

4.4 证明: $P =_{\mathrm{w}} Q$ 当且仅当 $\mathrm{CL}_{\mathrm{w}} \vdash P = Q$.

证明. $\square$

4.5 证明: $(\lambda^* x.M)N =_{\mathrm{w}} M[x := N]$.

证明. $\square$

4.6 令 $B \equiv S(KS)K$, 证明: 对于任意 $P, Q, R \in \mathbb{C}, BPQR =_{\mathrm{w}} P(QR)$.

证明. $\square$

4.7 在 CL 中, 定义 $\overline{n} \equiv (SB)^n(KI)$, 其中 $n \in \mathbb{N}$, B 如习题 4.6 中所定义. 证明: 对于一般递归函数 $\varphi : \mathbb{N} \to \mathbb{N}$, 存在组合子 $\overline{\varphi} \in \mathbb{C}^{\circ}$, 使得

$$\forall n \in \mathbb{N}. \bar{\varphi}\bar{n} = \overline{\varphi(n)}.$$

(此性质由 Kleene 教授证明)

证明. $\square$

4.8 证明: 对于任意 $P, Q \in \mathbb{C}$, 若 $P =_{\mathrm{w}} Q$, 则 $P_\lambda =_\beta Q_\lambda$.

证明. $\square$

4.9 证明: $(SKK)_\lambda =_\beta \lambda x.x$.

证明. $\square$

4.10 证明引理 4.13.

引理 4.13 表述为:

设 $M, N \in \Lambda, x \in V$, 则

$$(M[x := N])_{\mathrm{CL}} \equiv M_{\mathrm{CL}}[x := N_{\mathrm{CL}}].$$

证明. □

5 Turing 机

5.1 构造机器计算函数 $f(x,y,z)=y$.

解. 对第一版答案做出了修正. $f(x,y,z)=y$ 由表 1定义的机器 $\boxed{\mathrm{P}_2^3}$ 计算:

表 1: 机器 $\boxed{\mathrm{P}_2^3}$

	0	1
1	$0R2$	$0R1$
2	$0R3$	$1R2$
3	$0L4$	$0R3$
4	$0L4$	$1L5$
5	$0R6$	$1L5$

对于 $\boxed{\mathrm{P}_2^3}$ 输入 $0\underset{\uparrow}{1}^{x+1}01^{y+1}01^{z+1}0\cdots$, 输出 $0^{x+3}\underset{\uparrow}{1}^{y+1}0\cdots$. □

5.2 构造机器 $\boxed{\mathrm{copy}_1}$ 使 $\boxed{\mathrm{copy}_1}|0\underset{\uparrow}{1}^x0\cdots \twoheadrightarrow 01^x0\underset{\uparrow}{1}^x0\cdots$.

解. 对第一版答案做出了修正. 第一版答案求解思路是每删除一个 1, 在其后面对应的位置加两次 1, 这样做确实能够实现拷贝功能, 但是其最终的输出开头的 0 数量超过 1 个, 与题意不符.

求解思路：$0\underset{\uparrow}{1}^x0\cdots \twoheadrightarrow 01\underset{\uparrow}{0}^{x-1}010\cdots \twoheadrightarrow 0\underset{\uparrow}{1}1^{x-1}011^{x-1}0\cdots$. 注意考虑特殊情况，即当 $x=0$ 时候，输出为 $01\underset{\uparrow}{0}1\cdots$.

表 2定义了机器 $\boxed{\mathrm{copy}_1}$:

表 2: 机器 $\boxed{\mathrm{copy}_1}$

	0	1
1		$1R2$
2	$0R5$	$0R3$
3	$0R4$	$0R3$
4	$1L7$	$1R5$
5	$1L6$	$1R5$
6	$0L7$	$1L6$
7	$0L8$	$1R11$
8	$0L8$	$1R9$
9	$1R10$	
10	$0R10$	$1R5$
11	$0R12$	

输入 $0\underset{\uparrow}{1}^x0\cdots$，输出 $0\underset{\uparrow}{1}^x01^x0\cdots$. □

5.3 构造机器计算函数 $f(x,y)=x\times y$.

解. $f(x,y)=x\times y$ 由表 3定义的机器 $\boxed{\text{mul}}$ 计算:

表 3: 机器 $\boxed{\text{mul}}$

	0	1
1		$0R2$
2	$0R14$	$0R3$
3	$0R4$	$1R3$
4	$0R5$	$0R5$
5	$0R16$	$0R6$
6	$0R7$	$1R6$
7	$1L8$	$1R7$
8	$0L9$	$1L8$
9	$1R5$	$1L9$
10	$0L11$	$1L10$
11	$0L12$	
12	$0R14$	$1L13$
13	$0R2$	$1L13$
14	$0R14$	$0R15$
15	$1O18$	$0R15$
16	$1L17$	$1L17$
17	$0L10$	$0L10$

对于 $\boxed{\text{mul}}$ 输入 $1:0\underset{\uparrow}{1}{}^{x+1}01^{y+1}0\cdots$, 在 $y=0$ 时输出 $18:0^{x+6}\underset{\uparrow}{1}0\cdots$, 在 $y\neq 0$ 时输出 $18:0^{x+y+4}\underset{\uparrow}{1}{}^{x\times y+1}0\cdots$. □

5.4 构造机器计算函数 $f(x)=2^x$.

解. 由定理 5.13 的证明过程, 可如此构造: 令 y 恒为 1, 令 $f(x+1,y)=g(f(x,y))$, 其中 $g(x)=2x$, 于是有 $f(x)=2^x$.

首先, 构造出初始值 $(y)1$, 使用机器 M_1, 定义如表 4:

易知 $M_1|1:0\underset{\uparrow}{1}{}^{x+1}00\cdots\twoheadrightarrow 7:0\underset{\uparrow}{1}{}^{x+1}01100\cdots$.

定义机器 M_2 为表 5:

易知 $x>0$ 时 $M_2|1:0\underset{\uparrow}{1}{}^{x+1}01100\cdots\twoheadrightarrow 4:001^x0\underset{\uparrow}{1}100\cdots$ (在 $x=0$ 时输出为 $u:000\underset{\uparrow}{1}100\cdots$).

令 $M_3=M_2\Rightarrow\boxed{\text{double}}+3\Rightarrow\boxed{\text{compress}}\Rightarrow\boxed{\text{shiftl}}$, 从而

若 $x=0$, 则 $M_3|1:0\underset{\uparrow}{1}{}^{x+1}01^{y+1}0\cdots\twoheadrightarrow v:000\underset{\uparrow}{1}{}^{y+1}0\cdots$

若 $x>0$, 则 $M_3|1:0\underset{\uparrow}{1}{}^{x+1}01^{y+1}0\cdots\twoheadrightarrow w:00\underset{\uparrow}{1}{}^x01^{2y+1}0\cdots$

$M_4=\text{repeat } M_3$, 即 $M_4=M_3[w:=1]$, 机器 $\boxed{\text{f}}=M_1\Rightarrow M_4$ 为所求.

表 4: 题 5.4 机器 M_1

	0	1
1	$0R2$	$1R1$
2	$1R3$	
3	$1L4$	
4		$1L5$
5	$0L6$	
6	$0R7$	$1L6$

表 5: 题 5.4 机器 M_2

	0	1
1		$0R2$
2	$0Ru$	$1R3$
3	$0R4$	$1R3$

□

5.5 设机器 M_1 定义如表 5.24.
对于输入 $\bar{x}$, 求输出.

表 5.24

	0	1
1	$0L3$	$1R2$
2	$0L3$	$0R1$
3	$0L3$	$1L3$

解. 对第一版答案做出了修正. M_1 的操作为把第偶数次读到的 1 写成 0, 读到 0 后一直向左倒带到第一个位置的左端（越界）, 从而无法读取从而停机. 因此当其输入为 $\bar{x}$ 时, 输出为 $\underset{\uparrow}{}\underbrace{0101\cdots01}_{\lfloor\frac{x}{2}\rfloor+1\text{个}01}0\cdots.$ □

5.6 设机器 M_2 定义如表 5.25.

对于输入 $(2,1): 01^n01^m01^k00\cdots$, 其中 $n,m,k \in \mathbb{N}^+$, 求输出.

表 5.25

	0	1
1	$0R2$	$0R1$
2	$1R3$	$0R1$
3	$1R4$	
4	$1R5$	
5	$1L6$	
6	$0R7$	$1L6$

解. 对于输入 $(2,1): 01^n01^m01^k00\cdots$, 机器 M_2 有如下计算过程:

$$1:0\underset{\uparrow}{1}{}^n01^m01^k00\cdots \qquad (0R1)$$

$$1:0^{n+1}\underset{\uparrow}{0}1^m01^k00\cdots \qquad (0R2)$$

$$2:0^{n+2}\underset{\uparrow}{1}{}^m01^k00\cdots \qquad (0R1)$$

当 $m=1$ 时, 计算过程为:

$$1:0^{n+3}\underset{\uparrow}{0}1^k00\cdots \qquad (0R2)$$

$$2:0^{n+4}\underset{\uparrow}{1}{}^k00\cdots \qquad (0R1)$$

当 $m>1$ 时, 计算过程为:

$$1:0^{n+3}\underset{\uparrow}{1}{}^{m-1}01^k00\cdots \qquad (0R1)$$

$$1:0^{n+m+2}\underset{\uparrow}{0}1^k00\cdots \qquad (0R2)$$

$$2:0^{n+m+3}\underset{\uparrow}{1}{}^k00\cdots \qquad (0R1)$$

此时机器都处于状态为 2, 输入为 $0^{n+m+3}\underset{\uparrow}{1}{}^k00\cdots$ 的时刻.

当 $k=1$ 时, 计算过程与 $m=1$ 时类似, 当 $k>1$ 时, 计算过程与 $m>1$ 时类似, 机器

都会处于状态 2, 输入为 $0^{n+m+k+4}\underset{\uparrow}{0}0\cdots$ 的时刻. 接下来的计算过程为:

$$2 :0^{n+m+k+4}\underset{\uparrow}{0}0\cdots \tag{1R3}$$

$$3 :0^{n+m+k+4}1\underset{\uparrow}{0}0\cdots \tag{1R4}$$

$$4 :0^{n+m+k+4}11\underset{\uparrow}{0}0\cdots \tag{1R5}$$

$$5 :0^{n+m+k+4}111\underset{\uparrow}{0}0\cdots \tag{1L6}$$

$$6 :0^{n+m+k+4}11\underset{\uparrow}{1}10\cdots \tag{1L6}$$

$$6 :0^{n+m+k+3}\underset{\uparrow}{0}11110\cdots \tag{0R7}$$

$$7 :0^{n+m+k+3}\underset{\uparrow}{1}1110\cdots \tag{停}$$

因此机器的输出就是 $7 : 0^{n+m+k+3}\underset{\uparrow}{1}1110\cdots$, 即计算函数 $f(x, y, z) = 3$. □

5.7 构造机器计算函数 $f(x) = \lfloor\sqrt{x}\rfloor$.

解. 令 $y = \lfloor\sqrt{x}\rfloor$, 那么有 $y \leqslant \sqrt{x} < y + 1$, 有 $y^2 \leqslant x < (y + 1)^2$.

因此 $f(x) = \mu y.[x < (y+1)^2]$, 即表示在给定 x 的情况下使得 $x < (y+1)^2$ 恒成立的最小 y 值. 由于 $x, (y + 1)^2 \in \mathbb{N}$, 所以 $x + 1 \leqslant (y + 1)^2$.

所以我们有 $f(x) = \mu y.[S(x) \dot{-} \mathrm{sq}(S(y))]$. 其中, $\mathrm{sq}(x) = x^2$.

函数 sq 可以通过 $\boxed{\mathrm{copy}_1}$ ⇒ $\boxed{\mathrm{shiftl}}$ ⇒ $\boxed{\mathrm{mul}}$ 计算, 机器 $\boxed{\mathrm{mul}}$ 即表 3定义的机器, 计算 S 函数的机器 $\boxed{\mathrm{S}}$ 已在书中给出, 计算 $x \dot{-} y$ 的机器 $\boxed{\mathrm{sub}}$ 见题 5.11.

因此总体思路如下: 输入为 $\overline{x}$, 整个转化过程为:

$$\overline{x} \to \overline{(x + 1, y)} \to \overline{(x + 1, y, x + 1, y)} \to \overline{(x + 1, y, f(x + 1, y))}$$

当 $f(x,y)$ 为 0 时, 抹掉 $f(x,y)$ 和 x, 指向 y. 否则, 抹掉 $f(x,y)$, y 加 1, 再复制一次 x, y.

先定义机器 M_0 如表 6:

表 6: 题 5.7 机器 M_0

	0	1
1	$1R2$	$1R1$
2	$0R3$	
3	$1L4$	
4	$0L4$	$1L5$
5	$0R6$	$1L5$

易知 $M_0|1 : 0\underset{\uparrow}{1}^{x+1}0\cdots \twoheadrightarrow 6 : 0\underset{\uparrow}{1}^{x+2}010\cdots$, 这完成了 $\overline{x} \to \overline{(x + 1, y)}$ 的步骤.

$\overline{(x + 1, y)} \to \overline{(x + 1, y, x + 1, y)} \to \overline{(x + 1, y, f(x + 1, y))}$ 的步骤由 $\boxed{\mathrm{copy}_2}^2$ ⇒ $\boxed{\mathrm{f}}$ ⇒ $\boxed{\mathrm{compress}}$ 完成. $\boxed{\mathrm{f}}$ 计算函数 $f(x, y) = x \dot{-} \mathrm{sq}(S(y))$(注意不是 $S(x)$ 而是 x, 因为加 1 操

作已经在 M_0 完成), $\boxed{\text{f}} = \boxed{\text{shiftr}} \Rightarrow \boxed{\text{S}} \Rightarrow \boxed{\text{copy}_1} \Rightarrow \boxed{\text{shiftl}} \Rightarrow \boxed{\text{mul}} \Rightarrow \boxed{\text{compress}} \Rightarrow \boxed{\text{shiftl}} \Rightarrow \boxed{\text{sub}}$.

再定义机器 M_1 如表 7:

表 7: 题 5.7 机器 M_1

	0	1
1		$0R2$
2	$0L8$	$0R3$
3	$0L4$	$0R3$
4	$0L4$	$1R5$
5	$1L6$	
6	$0L7$	$1L6$
7	$0R12$	$1L7$
8	$0L8$	$1L9$
9	$0L10$	$1L9$
10	$0R11$	$0L10$
11	$0R11$	$1Ou$

易知:

$M_1|1 : 01^{x+1}01^{y+1}0\underset{\uparrow}{1}0\cdots \twoheadrightarrow u : 0^{x+3}\underset{\uparrow}{1}^{y+1}00\cdots$

$M_1|1 : 01^{x+1}01^{y+1}0\underset{\uparrow}{1}^{z+1}0\cdots \twoheadrightarrow 12 : 0\underset{\uparrow}{1}^{x+1}01^{y+2}00\cdots (z > 0)$

那么, 令 $M_2 = \boxed{\text{copy}_2}^2 \Rightarrow \boxed{\text{f}} \Rightarrow \boxed{\text{compress}} \Rightarrow M_1$, $M_3 = \text{repeat}M_2$, 则机器 $M = M_0 \Rightarrow M_3$ 可以计算 $f(x) = \lfloor\sqrt{x}\rfloor$. □

5.8 设机器 $\boxed{\text{f}_1}$ 计算函数 f_1, 机器 $\boxed{\text{f}_2}$ 计算函数 f_2, 这里 f_1, f_2 为一元数论函数. 构造机器 $\boxed{\text{f}}$ 计算函数 $f(x) = f_1(x) + f_2(x)$.

解. $\boxed{\text{f}} = \boxed{\text{copy}_1} \Rightarrow \boxed{\text{f}_1} \Rightarrow \boxed{\text{compress}} \Rightarrow \boxed{\text{shiftl}} \Rightarrow \boxed{\text{copy}_2} \Rightarrow \boxed{\text{shiftr}} \Rightarrow \boxed{\text{f}_2} \Rightarrow \boxed{\text{compress}} \Rightarrow \boxed{\text{shiftl}}^2 \Rightarrow \boxed{\text{erase}} \Rightarrow \boxed{\text{add}}$. □

5.9 设 $f(x) = h(g_1(x), g_2(x), g_3(x))$, 试由机器 $\boxed{\text{g}_1}, \boxed{\text{g}_2}, \boxed{\text{g}_3}$ 和 $\boxed{\text{h}}$ 构造机器 $\boxed{\text{f}}$.

解.

$$\begin{aligned}\boxed{\text{f}} = \boxed{\text{copy}_1} &\Rightarrow \boxed{\text{g}_1} \Rightarrow \boxed{\text{compress}} \Rightarrow \boxed{\text{shiftl}}\\ &\Rightarrow \boxed{\text{copy}_2} \Rightarrow \boxed{\text{shiftr}} \Rightarrow \boxed{\text{g}_2} \Rightarrow \boxed{\text{compress}} \Rightarrow \boxed{\text{shiftl}}^2\\ &\Rightarrow \boxed{\text{copy}_3} \Rightarrow \boxed{\text{shiftr}}^2 \Rightarrow \boxed{\text{g}_3} \Rightarrow \boxed{\text{compress}} \Rightarrow \boxed{\text{shiftl}}^3\\ &\Rightarrow \boxed{\text{erase}} \Rightarrow \boxed{\text{h}}.\end{aligned}$$

□

5.10 设 $f:\mathbb{N}\to\mathbb{N}$ 定义如下:

$$f(0)=0,$$
$$f(x+1)=g(f(x)).$$

证明: 若 g 为 Turing-可计算, 则 f 为 Turing-可计算.

证明. 按照定理 5.14 的证明方式, 令 y 恒为 0. 因此首先在原来的输入上添加 0 作为 y, 构建机器 M_1 如表 8:

表 8: 题 5.10 机器 M_1

	0	1
1	$0R2$	$1R1$
2	$1L3$	
3	$0L4$	
4	$0R5$	$1L4$

易知 $M_1|1:0\underset{\uparrow}{1}^{x+1}0\cdots\twoheadrightarrow 5:0\underset{\uparrow}{1}^{x+1}010\cdots$.

由于 g 是 Turing-可计算的, 所以存在机器 $\boxed{\mathrm{g}}$ 计算函数 g.

构造机器 M_2 如表 9所示:

表 9: 题 5.4 机器 M_2

	0	1
1		$0R2$
2	$0Ru$	$1R3$
3	$0R4$	$1R3$

令 $M_3=M_2\Rightarrow\boxed{\mathrm{g}}+3\Rightarrow\boxed{\mathrm{compress}}\Rightarrow\boxed{\mathrm{shiftl}}$, 并令 $\boxed{\mathrm{f}}=\mathrm{repeat}M_3$, $M=M_1\Rightarrow\boxed{\mathrm{f}}$ 即为能计算 f 的机器, 因此 f 为 Turing-可计算. □

5.11 构造机器计算函数 $f(x,y)=x\dot{-}y$.

解. 基本思想: x 和 y 每回各消去 1, 直到有一个为 0 为止. $f(x,y)=x\dot{-}y$ 由表 10定义的机器 $\boxed{\mathrm{sub}}$ 计算:

对于 $\boxed{\mathrm{sub}}$ 输入 $1:0\underset{\uparrow}{1}^{x+1}01^{y+1}0\cdots$, 在 $x\leqslant y$ 时输出 $13:0^{x+y+4}\underset{\uparrow}{1}0\cdots$, 在 $x>y$ 时输出 $13:0^{y+2}\underset{\uparrow}{1}^{x-y+1}0\cdots$. □

表 10: 题 5.11 机器 $\boxed{\text{sub}}$

	0	1
1		$0R2$
2	$0R8$	$1R3$
3	$0R4$	$1R3$
4	$0R4$	$0R5$
5	$0L10$	$1L6$
6	$0L6$	$1L7$
7	$0R1$	$1L7$
8	$0R8$	$0R9$
9	$1O13$	$0R9$
10	$0L10$	$1R11$
11	$1L12$	
12	$0R13$	$1L12$

5.12 证明: $\mathrm{Even} = \{2x : x \in \mathbb{N}\}$ 是 Turing-可计算的.

证明. 只要能够构造出这样的机器 M, 它满足

$$M|1 : 0\underset{\uparrow}{1}^{2x}0\cdots \twoheadrightarrow u : 0\cdots 01\underset{\uparrow}{1}0\cdots$$

$$M|1 : \underset{\uparrow}{0}1^{2x+1}0\cdots \twoheadrightarrow v : 0\cdots 0\underset{\uparrow}{1}0\cdots$$

构造如表 11所示: □

表 11: 题 5.12 机器 M

	0	1
1	$1R3$	$0R2$
2	$1O4$	$0R1$
3	$1L4$	

5.13 证明: $S = \{a_1, a_2, \cdots, a_k\}$ 是 Turing-可计算的.

证明. 对第一版答案做出了修正. 构造 $\chi_S = N^2\big(\prod_{i=1}^{k}(x \dot{-} a_i)\big)$, 于是有:

$$\chi_S = \begin{cases} 0, & 若 x \in S, \\ 1, & 否则. \end{cases}$$

故 $\chi_S \in \mathcal{EF}$. 由定理 5.18(page 138) 知 χ_S 是 Turing-可计算的.

□

5.14 设 $f:\mathbb{N}\to\mathbb{N}$ 是 Turing-可计算的, 构造机器 M 使其输出 f 的最小零点.

证明. 基本思路为: 从 0 开始计算 f 的值, 一旦发现 f 的值为 0, 输出, 否则加 1 再算.

这里不知道 M 的输入是什么, 假定 M 的输入为 $0\underset{\uparrow}{1}000\cdots$, 即自然数 0. 令计算 f 的机器为 $\boxed{\text{f}}$.

定义机器 M_1 如表 12:

表 12: 题 5.14 机器 M_1

	0	1
1		$0R2$
2	$0L3$	$0R5$
3	$0L3$	$1L4$
4	$0Ru$	$1L4$
5	$0L6$	$0R5$
6	$0L6$	$1R7$
7	$1L8$	
8	$0R9$	$1L8$

易知:

$M_1|1:01^{x+1}0\cdots0\underset{\uparrow}{1}0\cdots\twoheadrightarrow u:0\underset{\uparrow}{1}^{x+1}0\cdots$

当 $y>0$ 时, $M_1|1:01^{x+1}0\cdots0\underset{\uparrow}{1}^{y+1}0\cdots\twoheadrightarrow 9:0\underset{\uparrow}{1}^{x+2}0\cdots$

到达 u 状态表示无论如何都停机. (可以改成 $0R7$, 因为下一位肯定是 1)

那么令 $M_2=\boxed{\text{copy}_1}\Rightarrow\boxed{\text{f}}\Rightarrow M_1$, 则 $M=\text{repeat}M_2$ 为所求. 在函数 f 没有零点时, 机器 M 将永不停机. □

5.15 证明定理 5.21 中函数 g 为一般递归函数.

证明. 这里需要使用题 5.17 的结论.

当 $m\notin S$ 时, 有 $g(m)=0$.

否则, 可以解码出编码 m 对应的机器 M 的行数和各个行的内容.

而 M_1 计算常值函数 m 的机器可通过 $\boxed{\text{Z}}\Rightarrow\boxed{\text{S}}^m$ 构造, 显然可以通过 m 由一般递归函数计算.

而 $\hat{M}=M_1\Rightarrow M$, 这意味着 M 的所有行都要自加 m, 这个映射也是一般递归的.

因此最终整个函数都是一般递归的. □

5.16 证明引理 5.25 中的函数 $e(m,l)$ 为初等函数.

证明. 利用题 5.17 的结论, 由 m 可以通过一般递归函数计算每一行的内容 $\sharp j$, $\sharp x$, $\sharp y$, $\sharp z$, $\sharp u$, $\sharp v$, $\sharp w$.

同时, 由 l 也可以通过一般递归函数计算纸带的编码长度 t 和纸带位置 $(j,k):a_1,a_2,\cdot,a_t$.

通过循环, 比较, 分支等步骤, 可以计算出 $\sharp d(a_j,k), \sharp p(a_j,k), \sharp s(a_j,k)$.

因此 $e(m,l) = \langle \sharp d(a_j,k), \sharp p(a_j,k), \sharp s(a_j,k)\rangle \in \mathcal{GRF}$. □

5.17 令 $S = \{\sharp M : M$为 Turing 机$\}$, 证明 S 为 Turing-可计算.

证明. 这相当于用一个 Turing 机来解码一个数判断其是否为合法的 Turing 机编码.

首先确定机器的行数 k, $k = \max a \leqslant \sharp M.P(a-1)|\sharp M$. $P(n)$ 代表第 n 个素数, n 从 0 开始计数, 即 $P(0)=2, P(1)=3, P(2)=5, \cdots$.

然后是每一行的编码, $r_i = \mathrm{ep}(i, \sharp M)$.

然后是对行内的元素进行解码, 对于机器的一行 $\boxed{j \mid xyz \mid uvw}$, 可得

$$\sharp j = \mathrm{ep}(0, r_i), \sharp x = \mathrm{ep}(1, r_i), \cdots, \sharp w = \mathrm{ep}(6, r_i)$$

每个数都会得到一个结果, 但是结果需要合法:

首先, 1 和 2 肯定不合法.

如果解析得到某行 $\sharp x = 2$, 则应该有 $\sharp y = \sharp z = 2$, 即 LLL, 否则, $\sharp x < 2 \wedge \sharp y \in \{2,3,4\}$. 其余情况均不合法.

如果解析得到某行 $\sharp u = 4$, 则应该由 $\sharp v = \sharp w = 4$, 即 RRR, 否则, $\sharp u < 2 \wedge \sharp v \in \{2,3,4\}$. 其余情况均不合法.

$\forall m, n \leqslant k, m \neq n. \sharp j(r_m) \neq \sharp_j(r_n)$. 即每一行的标号都不同.

这里已经明确给出了计算流程, 显然我们可以通过编程在有限时间内输出某个自然数是否合法的 Turing 机编码, 其自然是 Turing-可计算的. □

5.18 由 CT 证明函数 $g(n)$ 可计算, 这里

$$g(n) = \text{在自然对数之底e的十进制展开式中第}n\text{个数字}.$$

证明. 根据泰勒公式,

$$\mathrm{e}^x = \sum_{i=0}^{n} \frac{1}{i!} + \frac{\mathrm{e}^\theta}{(n+1)!}, \quad 0 < \theta < 1.$$

令 $f(n) = \lfloor \mathrm{e} \cdot n! \rfloor$, 我们证明 $f \in \mathcal{PRF}$.

$f(0) = f(1) = 2$, 当 $n \geqslant 2$ 时, $f(n) = \sum_{i=0}^{n} \frac{n!}{i!} + \frac{\mathrm{e}^\theta}{n+1}$, 而此时 $0 < \frac{\mathrm{e}^\theta}{n+1} < 1$, 所以 $f(n) = \sum_{i=0}^{n} \frac{n!}{i!}$. 显然 $f(n) \in \mathcal{PRF}$.

令 $h(n) = \lfloor \mathrm{e} \cdot n \rfloor$, 那么有 $h(0) = 0$, $h(n) = \left\lfloor \frac{f(n)}{(n-1)!} \right\rfloor (n > 0)$, 因此 $h(n) \in \mathcal{PRF}$.

那么 $g(1) = 2$, $g(n) = h(10^n) \dot{-} h(10^{n \dot{-} 1}) \cdot 10 (n > 0)$, 因此 $g(n) \in \mathcal{PRF}$, 所以 $g(n)$ 可计算. □

5.19 (1) 什么是停机问题?
(2) 什么是可判定问题 (decision problem)?
(3) 停机问题可判定吗?

解. (1) 是否存在能行过程来判定机器对所有输入皆停机?

(2) 设 A 为 $\mathbb{N}$ 的子集, A 是可判定的指 A 的特征函数 χ_A 是 Turing-可计算的, 即有机器 M_A, 其对于输入 $\bar{x}$, 若 $x \in A$, 则输出 $\bar{0}$; 否则, 输出 $\bar{1}$.

(3) 停机问题不可判定.

□

5.20 (1) 什么是通用 Turing 机 (universal Turing machine)?
(2) 通用 Turing 机起什么作用?

解. (1) 机器 U 是通用 Turing 机, 当其满足对任何机器 M 和任何 $(n_1, \cdots, n_k) \in \mathbb{N}^k$,

$$M|\overline{(n_1, \cdots, n_k)} \twoheadrightarrow \overline{y} \Leftrightarrow U|\overline{(\sharp M, n_1, \cdots, n_k)} \twoheadrightarrow \overline{y}.$$

(2) 其凭自身就能完成任何 Turing 机可能做到的任何事, 可以模拟任何其他 Turing 机, 在早期程序储存式计算机的研制中起到了重要的促进作用.

□