计算理论作业 1

颜俊梁 MF21330103

2022 年 5 月 29 日

题目 1.1. 证明: 对于固定的 $k \in \mathbb{N}$, $x + k \in \mathcal{BF}$.

解答. 对 k 归纳, 记一元数论函数 $x + k$ 为 f_k.

奠基: 当 $k = 0$, 有 $f_0 = P_1^1 \in \mathcal{EF}$.

归纳假设: 当 $k = i$ 时有 $f_i \in \mathcal{EF}$.

那么 $f_{i+1} = S \circ f_i \in \mathcal{EF}$.

所以, 对于固定的 $k \in \mathbb{N}$, $x + k \in \mathcal{BF}$.

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

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

其中 $\|\vec{x}\| = \max\{x_i : 1 \leq i \leq k\}$.

解答. 对 f 结构归纳.

当 $f \in \mathcal{IF}$ 时:

1. 若 $f = Z$, 存在 $h = 1$, $f(x) = 0 < 1 < x + 1$;
2. 若 $f = S$, 存在 $h = 2$, $f(x) = x + 1 < x + 2$;

3. 若 $f = P_i^n$, 存在 $h = 1$,

$$f(x_1, x_2, \ldots, x_n) = x_i < \max\{x_i : 1 \le i \le n\} + 1$$

当 $f_{i+1} = \mathbf{Comp}_m^n[f_i, g_1, g_2, \ldots, g_m]$ 时, 其中 $f_i, g_1, g_2, \ldots, g_m \in \mathcal{BF}$.

根据归纳假设有 $f_i(\vec{x}) < \|\vec{x}\| + h_f$, $g_1(\vec{x}) < \|\vec{x}\| + h_1$, $g_2(\vec{x}) < \|\vec{x}\| + h_2$, $\cdots$, $g_m(\vec{x}) < \|\vec{x}\| + h_m$.

$$\begin{aligned}
f_{i+1}(\vec{x}) &= f_i(g_1(\vec{x}), g_2(\vec{x}), \ldots, g_m(\vec{x})) \\
&< \max\ \{\ g_i(\vec{x}) : 1 \le i \le m\ \} + h_f \\
&= \max\ \{\ \|\vec{x}\| + h_i : 1 \le i \le m\ \} + h_f \\
&= \|\vec{x}\| + (\max\ \{\ h_i : 1 \le i \le m\ \} + h_f)
\end{aligned}$$

令 $h = \max\ \{\ h_i : 1 \le i \le m\ \} + h_f$, 有 $f_{i+1}(\vec{x}) < \|\vec{x}\| + h$.

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

解答. 反证法.

假设 $x + y \in \mathcal{BF}$, 根据 1.2 的引理, 存在 $h \in \mathbb{N}$, 满足 $\forall x, y \in \mathbb{N}.\ x + y < \max\{x, y\} + h$. 注意到这样任意大的 h 并不存在, 矛盾.

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

解答. 首先证明一个引理, 对于任何 $f \in \mathbb{N}^k \to \mathbb{N}, \vec{x} \in \mathbb{N}^k$, $f(\vec{x})$ 的值至多与 $\vec{x}$ 当中的一维有关. 形式化地, 存在 $a, b \in \mathbb{N}$, 要么 $f = \mathbf{Comp}_2^k[+, Z \circ S^b, P_a^k]$, 要么 $f = Z \circ S^b$.

对 f 作结构归纳. 奠基, 显然当 $f \in \mathcal{IF}$ 时, 均满足以上形式.

假设 $f_0, f_1, f_2, \ldots, f_k \in \mathcal{BF}$ 都至多与输入中的某一维有关, 且 $f_0 \in \mathbb{N}^k \to \mathbb{N}$, $f_1, f_2, \ldots, f_k \in \mathbb{N}^m \to \mathbb{N}$. 于是, $f_{k+1} = \mathbf{Comp}_k^m[f_0, f_1, f_2, \ldots, f_k]$, 根据归纳假设, f_0 的结果只会至多与 $f_1, f_2, \ldots, f_k$ 中的某一个有关, 而这 k 个函数也只会与输入的至多某一维有关, 因此 f_{k+1} 也满足以上形式.

回到原题, 有了以上引理, 我们注意到二元数论函数 $x \dot{-} y$ 的结果会与输入的两个维度均有关, 因此 $x \dot{-} y \notin \mathcal{BF}$.

题目 1.5. 设 $pg(x, y) = 2^x(2y + 1) - 1$.

证明: 存在初等函数 $K(x)$ 和 $L(x)$ 使得

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

解答.

$$\begin{aligned} K(z) &= ep(0, z + 1) \\ L(z) &= \mathrm{div}(\left\lfloor \frac{z+1}{2^{K(z)}} \right\rfloor - 1, 2) \\ pg(K(z), L(z)) &= 2^{ep(0,z+1)}(2 \times \mathrm{div}(\left\lfloor \frac{z+1}{2^{K(z)}} \right\rfloor - 1, 2) + 1) - 1 \\ &= 2^{ep(0,z+1)} \left\lfloor \frac{z+1}{2^{ep(0,z+1)}} \right\rfloor - 1 \\ &= z \end{aligned}$$

说明: 上述计算中的取整函数都是不必要的. 因为根据算术基本定理, 任意正整数 n 可以写成 $n = 2^l \cdot b$ ($l \in \mathbb{N}, b \in \mathbb{N}^+, 2 \nmid b$) 的形式, 于是 $\left\lfloor \frac{z+1}{2^{K(z)}} \right\rfloor$ 就是将 $z + 1$ 的因子 2 全部除掉，其结果是一个奇数.

题目 1.6. 设 $f:\mathbb{N}\to\mathbb{N}$, 证明: f 可以作为配对函数的 K 函数, 当且仅当对于任何 $i\in\mathbb{N}$,

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

解答. 先证明, f 可以作为配对函数的 K 函数 $\Longrightarrow \forall i\in\mathbb{N}.|\{x\in\mathbb{N}:f(x)=i\}|=\aleph_0$.

反证法.

存在 $i\in\mathbb{N}$ 使得 $\{x\in\mathbb{N}:f(x)=i\}$ 与自然数集不等势. 也就是 $|\{y\in\mathbb{N}:f(pg(i,y))=i\}|$ 与自然数集不等势, 即它是自然数的一个有限子集. 那么必定存在 $y_1\neq y_2\in\mathbb{N}$ 满足 $z=pg(i,y_1)=pg(i,y_2)$, 不妨设 $L(z)=y_1$, 那么 $L(pg(x,y_2))=L(z)=y_1\neq y_2$ 矛盾.

再证明, $\forall i\in\mathbb{N}.|\{x\in\mathbb{N}:f(x)=i\}|=\aleph_0\Longrightarrow f$ 可以作为配对函数的 K 函数.

根据 $\aleph_0$ 的定义，可知 $\{x\in\mathbb{N}:f(x)=i\}$ 和 $\mathbb{N}$ 之间存在一一映射，不妨设为 $f_i:\{x\in\mathbb{N}:f(x)=i\}\to\mathbb{N}$，也相应存在逆映射 $f_i^{-1}:\mathbb{N}\to\{x\in\mathbb{N}:f(x)=i\}$.

于是有对于任意的 $y\in\mathbb{N}$, $z=f_i^{-1}(y)\in\{x\in\mathbb{N}:f(x)=i\}$, 因此 $f(z)=i$, $f(f_i^{-1}(y))=i$.

构造 $pg(x,y)=f_x^{-1}(y)$, $L(z)=f_{K(z)}(z)$, 有

$$K(pg(x,y))=f(f_x^{-1}(y))=x$$
$$L(pg(x,y))=f_{K(pg(x,y))}(f_x^{-1}(y))=f_x(f_x^{-1}(y))=y$$

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

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

解答. 根据 **引理 1.12**, 只需要构造出绝对差函数和有界叠加算子即可.

首先, 构造一些工具函数.

$$N(x) = \prod_{i=1}^{x} Z(i)$$
$$\mathrm{leq}(x,y) = \prod_{i=x}^{y} Z(i)$$
$$\mathrm{geq}(x,y) = \prod_{i=y}^{x} Z(i)$$

通过幂运算构造相等函数 (当 $x = 0, k > 1$ 时, $\mathrm{pow}(x,k) = 0$).

$$\mathrm{pow}(x,k) = \prod_{i=1}^{k} x$$
$$\mathrm{eq}(x,y) = \mathrm{pow}(\mathrm{leq}(x,y), N(\mathrm{geq}(x,y)))$$

通过 log 运算构造有界叠加算子.

$$\log(x) = \prod_{i=0}^{x} \mathrm{pow}(i, N(\mathrm{eq}(2^i, x)))$$
$$\sum_{i=n}^{m} f(i,\vec{y}) = \log \prod_{i=n}^{m} \mathrm{pow}(2, f(i,\vec{y}))$$

最后, $x \dot{-} y = (\sum\limits_{i=x+1}^{y} 1) + (\sum\limits_{i=y+1}^{x} 1)$.

题目 1.8. 设

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

证明:

$$M(x)=\begin{cases} 91 & \text{若 } x\le 100\\ x-10 & \text{若 } x>100\end{cases}$$

解答. 当 $90 \le x \le 100$, $M(x) = M(M(x+11))$, 而 $x+1 > 100$, $M(x+11) = x+1$, $M(x) = M(x+1)$. 因此, $M(90) = M(91) = \cdots = M(100) = M(101) = 91$.

当 $0 \le x < 90$, 存在 $k \in \mathbb{N}$, 使得 $x + 11k \in [90, 100]$ (区间 $[90, 100]$ 内有 11 个数). 从而 $M(x) = M(M(x+11)) = M^2(x+1\cdot 11) = \cdots = M^{k+1}(x+k\cdot 11) = M^k(M(x+k\cdot 11)) = M^K(91) = 91$.

题目 1.9. 证明:

$$\min_{x\le n}.[f(x,\vec{y})] = n \dot{-} \max_{x\le n}.[f(n\dot{-}x,\vec{y})]$$
$$\max_{x\le n}.[f(x,\vec{y})] = n \dot{-} \min_{x\le n}.[f(n\dot{-}x,\vec{y})]$$

解答. 情况 1. 没有 $0 \le x \le n$ 满足 $f(x,\vec{y}) = 0$，那么

$$\min_{x\le n}.[f(x,\vec{y})] = \min_{x\le n}.[f(n\dot{-}x,\vec{y})] = n$$
$$\max_{x\le n}.[f(x,\vec{y})] = \max_{x\le n}.[f(n\dot{-}x,\vec{y})] = 0$$

成立.

情况 2. 令 $a = \min_{x\leq n} .[f(x,\vec{y})]$. 因此对于任意的 $x < a$, $f(x,\vec{y}) \neq 0$, 也就是任意的 $x' = n - x > n - a$, $f(x',\vec{y}) \neq 0$. 根据 max-算子的定义, $\max_{x\leq n} .[f(n \dot- x,\vec{y})] = n - a$, 第一行等式成立. 类似地，根据对称性可以证明第二行等式也成立.

题目 1.10. 证明: $\mathcal{EF}$ 对有界 max-算子封闭.

解答. 对于任意 $f \in EF$,

$$\max_{x\leq n} [f(x,\vec{y})] = n \dot- \sum_{i=0}^{n} \Big\{ \prod_{j=0}^{i} [N^2(f(n-j,\vec{y}))] \Big\} \dot- \prod_{j=0}^{i} [N^2(f(j,\vec{y}))]$$

具体地,

$$\max_{x\leq n} [f] = \mathbf{Comp}_2^{k+1}[\dot-, \mathbf{Comp}_2^{k+1}[\dot-, P_1^{k+1}, \prod_{j=0}^{n}\{N^2 \circ f\}], h]$$

$$h = \mathbf{Comp}_{k+2}^{k+1}[\sum_{i=0}^{n}[g], P_1^{k+1}, P_1^{k+1}, P_2^{k+1}, \ldots, P_{k+1}^{k+1}]$$

$$g = \prod_{j=0}^{i} \Big\{ N^2 \circ \mathbf{Comp}_{k+1}^{k+2}[f, \mathbf{Comp}_2^{k+2}[\dot-, P_2^{k+2}, P_1^{k+2}], P_3^{k+2}, \ldots, P_{k+2}^{k+2}] \Big\}$$

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

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

证明: $\varphi \in \mathcal{EF}$.

解答. 根据算术基本定理, $n = p_0^{a_0} \times p_1^{a_1} \times \ldots p_l^{a_l}$ $(a_0, a_1, \ldots a_l \geq 1)$, 于是有

$$\varphi(n) = \prod_{i=0}^{l} p_i^{a_i - 1}(p_i - 1)$$

构造

$$
\begin{aligned}
\varphi(n) &= \left\lfloor \frac{n}{f(n)} \right\rfloor \times g(n) \\
f(n) &= \prod_{i=0}^{n} [\operatorname{check}(i,n) \times i + N(\operatorname{check}(i,n))] \\
g(n) &= \prod_{i=0}^{n} [\operatorname{check}(i,n) \times (i \dot{-} 1) + N(\operatorname{check}(i,n))] \\
\tau(x) &= \sum_{i=0}^{x} [N(\operatorname{rs}(x,i))] \\
\operatorname{prime}(x) &= N^2(\tau(x) \dot{-} 2) \\
\operatorname{check}(i,n) &= \operatorname{prime}(i) \times N^2(i \dot{-} 1) \times N(rs(n,i))
\end{aligned}
$$

题目 1.12. 设 $h(x)$ 为 x 的最大素因子下标, 约定 $h(0)=0$, $h(1)=0$.

证明: $h \in \mathcal{EF}$.

解答. 构造一:

$$h(x) = \pi(\max_{i \le x}.\left\{ \operatorname{prime}(i) + N^2(\operatorname{rs}(x,i)) \right\}) \dot{-} 1$$

其中

$$
\begin{aligned}
\tau(x) &= \sum_{i=0}^{x} [N(\operatorname{rs}(x,i))] \\
\operatorname{prime}(x) &= N^2(\tau(x) \dot{-} 2) \\
\pi(x) &= \sum_{i=0}^{x} \operatorname{prime}(i)
\end{aligned}
$$

构造二:

$$h(n) = \max_{x \le n} [N(\operatorname{ep}(x,n))]$$

其中 max 算子的上界为 n, 因为 $p(n) \gg n$.

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

$$f(0)=1$$
$$f(1)=1$$
$$f(x+2)=f(x)+f(x+1)$$

证明:

1. $f\in\mathcal{PRF}$
2. $f\in\mathcal{EF}$

解答.

1. 令 $g(n)=\langle f(n),f(n+1)\rangle$

$$\begin{aligned} g(0)&=\langle f(0),f(1)\rangle=2^1\cdot 3^1=6\\ g(n+1)&=\langle f(n+1),f(n+2)\rangle\\ &=\langle f(n+1),f(n)+f(n+1)\rangle\\ &=\langle ep_1(g(n)),ep_0(g(n))+ep_1(g(n))\rangle\\ &=G(g(n)) \end{aligned}$$

其中 $G(x)=\langle ep_1(x),ep_0(x)+ep_1(x)\rangle\in\mathcal{PRF}$, 因此 $f\in\mathcal{PRF}$.

2. 法一, 直接构造出具体的 $\mathcal{EF}$ 形式.

有通项公式 $f(n)=\frac{1}{\sqrt{5}}\big((\frac{1+\sqrt{5}}{2})^n+(\frac{1-\sqrt{5}}{2})^n\big)$.

上式在 $\mathcal{Q}[\sqrt{5}]$ 域上运算, 只需要求出它的有理系数.

$$
\begin{aligned}
f(n) &= (\sum_{i=0}^{\lfloor\frac{n-1}{2}\rfloor}\binom{n}{2i+1}\sqrt{5}^{2i+1}+\sum_{i=0}^{\lfloor\frac{n-1}{2}\rfloor}\binom{n}{2i+1}(-\sqrt{5})^{2i+1})\Big/2^n\sqrt{5} \\
&= 2\sum_{i=0}^{\lfloor\frac{n-1}{2}\rfloor}\binom{n}{2i+1}5^i\Big/2^n
\end{aligned}
$$

构造 $\mathcal{EF}$

$$
f(n)=\lfloor 2\times\sum_{i=0}^{n}(rs(i,2)\times\binom{n}{i}5^{\lfloor i/2\rfloor})\Big/2^n\rfloor\in\mathcal{EF}
$$

其中组合数 $\binom{n}{m}=\dfrac{n!}{m!(n-m)!}$, $n!=\prod_{i=0}^{n}N(i)+i$, 因此 $\binom{n}{m}\in\mathcal{EF}$.

法二, 利用定理 1.31 证明.

定理. *设 $f:\mathbb{N}\to\mathbb{N}\in\mathcal{EF}$, $g:\mathbb{N}^3\to\mathbb{N}^{\in}\mathcal{EF}$. 设 $h:\mathbb{N}^2\to\mathbb{N}$ 由以下递归式定义:*

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

若存在 $b:\mathbb{N}^2\to\mathbb{N}\mathcal{EF}$ 使得 $\forall x,y\in\mathbb{N}.h(x,y)\le b(x,y)$, 则 $h(x,y)\in\mathcal{EF}$.

首先 $G(x)=\langle ep_1(x),ep_0(x)+ep_1(x)\rangle=2^{ep_1(x)}\cdot 3^{ep_0(x)+ep_1(x)}\in\mathcal{EF}$.

然后, $g(n)=\langle f(n),f(n+1)\rangle=2^{f(n)}\cdot 3^{f(n+1)}$. 通过数学归纳法可以证明 $f(n)\le 2^n$. 于是 $g(n)\le 2^{2^n}\cdot 3^{2^{n+1}}$. 又因为 $g'(n)=2^{2^n}\cdot 3^{2^{n+1}}\in\mathcal{EF}$ 且 $g(n)\le g'(n)$, 因此根据定理 1.31 有 $g\in\mathcal{EF}$.

题目 1.14. 设数论谓词 $Q(x,y,z,v)$ 定义为

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

其中 $p(n)$ 表示第 n 个素数, $\langle x,y,z\rangle$ 是 x,y,z 的哥德尔编码. 证明: $Q(x,y,z)$ 是初等的.

解答. $\langle x,y,z\rangle = 2^x3^y5^z$ 和 $p(n)$ 都属于初等函数, 因此 $p(\langle x,y,z\rangle) \in \mathcal{EF}$. 于是 $Q(x,y,z,v) = N(rs(v,p(\langle x,y,z\rangle))) \in \mathcal{EF}$.

题目 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: $f \in \mathcal{PRF}$.

解答.

$$\begin{aligned}
g(0) &= \langle 1,4,6\rangle\\
g(x+1) &= \langle ep(1,G(x)), ep(2,G(x)), ep(0,G(x)) + (ep(1,G(x))^2 + (ep(2,G(x)))^3)\rangle\\
f(x) &= ep(0,g(x)) \in \mathcal{PRF}
\end{aligned}$$

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

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

证明: $f\in\mathcal{PRF}-\mathcal{EF}$.

解答. 引入一个新函数 $g(m,n)=\underbrace{(m+n)^{\cdot^{\cdot^{\cdot^{m+n}}}}}_{n\text{ 个 }(m+n)}$, 于是 $f(n)=g(0,n)$.

1. $g\in\mathcal{PRF}$.

$$\begin{aligned} g(m,0) &= 0 = Z(m) \\ g(m,n+1) &= \underbrace{(m+n+1)^{\cdot^{\cdot^{\cdot^{m+n+1}}}}}_{n+1\text{ 个 }(m+n+1)} \\ &= (m+n+1)^{g(m+1,n)} \\ &= G(m,n,g(m+1,n)) \end{aligned}$$

其中 $G(x,y,z)=(x+y+1)^z\in\mathcal{PRF}$.

于是 $g\in\mathcal{PRF}$, 从而 $f\in\mathcal{PRF}$.

2. $f\notin\mathcal{EF}$.

也就是证明 f 不能被 $G(k,n)$ 控制.

反证法. 假设 f 被 G 控制, 则存在 $k_0\in\mathbb{N}$, 使得 $\forall n\in\mathbb{N}$, $f(n)\le G(k_0,n)=\underbrace{2^{\cdot^{\cdot^{\cdot^{2^n}}}}}_{k_0\text{ 个 }2}$.

令 $n = k_0 + 2$, $f(n) = \underbrace{(k_0+2)^{\cdot^{\cdot^{\cdot^{k_0+2}}}}}_{k_0+2\text{ 个 }k_0+2} > \underbrace{2^{\cdot^{\cdot^{\cdot^{2^{(k_0+2)}}}}}}_{k_0\text{ 个 }2}$.

因此导出矛盾, 所以 $f \notin \mathcal{EF}$.

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

题目 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: $f \in \mathcal{PRF}$.

解答. 使用数学归纳法证明 $f(x,y) = g^{2^{y-1}}(x) = \mathrm{It}[g](x, 2^{y-1}) \in \mathcal{PRF}$.

奠基: $f(x,0) = g^{2^0} = g(x)$.

归纳假设: $\forall 0 \le y \le k, f(x,y) = g^{2^y}(x)$.

递推:

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

因此, $f(x,y) = g^{2^{y-1}}(x) = \mathrm{It}[g](x, 2^{y-1}) \in \mathcal{PRF}$.

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

解答. 由于对称性, 只需要证明当 $g \in \mathcal{GRF}$ 时, $f \in \mathcal{GRF}$.

设所有取值不同的点的有限集合 $S = \{x_1, x_2, \ldots, x_k\}$. 因此, 若 $x \in S$, $f(x)$ 的值已知, 否则 $x \notin S$, $f(x) = g(x)$.

$$\begin{aligned} f(x) = (&f(x_1) \times N(x \dot{-} x_1) + \cdots + f(x_k) \times N(x \dot{-} x_k)) \\ &+ N(N(x \dot{-} x_1) + \cdots + N(x \dot{-} x_k)) \times g(x) \end{aligned}$$

因为 S 是有限集合, 上述函数是可以被有限地构造出来的, 因此 $f \in \mathcal{GRF}$.

题目 1.19. 证明:

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

   为初等函数.

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

   为初等函数.

解答.

1.

$$f(n) = \max_{x \le 2n}\left[x \le \left\lfloor (\frac{\sqrt{5}+1}{2})n \right\rfloor\right]$$
$$f(n) = \max_{x \le 2n}\left[x^2 \dot- nx \dot- n^2 = 0\right]$$
$$f(n) = \max_{x \le 2n}\left[N^2(x^2 \dot- nx \dot- n^2)\right] \in \mathcal{EF}$$

2. 构造函数 $h(n) = (\frac{\sqrt{5}+1}{2})^n + (\frac{1-\sqrt{5}}{2})^n$, 易知 $h(1) = 1, h(2) = 3$.

又注意到

$$\begin{aligned} h(n+1) + h(n) &= \frac{3+\sqrt{5}}{2}(\frac{\sqrt{5}+1}{2})^n + \frac{3-\sqrt{5}}{2}(\frac{1-\sqrt{5}}{2})^n \\ &= (\frac{1+\sqrt{5}}{2})^{n+2} + (\frac{1-\sqrt{5}}{2})^{n+2} \\ &= h(n+2) \end{aligned}$$

实际上, h 就是 Fibonacci 数列, 根据题目 1.13 易知 $h \in \mathcal{EF}$.

因为 $\left|(\frac{1-\sqrt{5}}{2})^n\right| < 1$, 且 n 为偶数时 $(\frac{1-\sqrt{5}}{2})^n$ 否则其 < 0. 因此

$$h(n) = \begin{cases} (\frac{\sqrt{5}+1}{2})^n & n \text{ 为奇数} \\ (\frac{\sqrt{5}+1}{2})^n + 1 & n \text{ 为偶数} \end{cases}$$

所以

$$f(n) = h(n) \dot- N(rs(n,2)) \in \mathcal{EF}$$

题目 1.20. 证明: $\mathrm{Ack}\,(4,n) \in \mathcal{PRF} - \mathcal{EF}$.

解答. 1. 证明 $\mathrm{Ack}\,(4,n) \in \mathcal{PRF}$.

证明一个更强命题: 对于固定的 i, $f_i(n) = \mathrm{Ack}\,(i,n) \in \mathcal{PRF}$.

奠基: $\mathrm{Ack}\,(0,n) = n+1 \in \mathcal{PRF}$.

归纳假设: 当 $i = k$ 时, $f_k(n) = \mathrm{Ack}\,(k,n) \in \mathcal{PRF}$.

递推: $\mathrm{Ack}\,(k+1,0) = \mathrm{Ack}\,(k,1)$, $\mathrm{Ack}\,(k+1,n+1) = \mathrm{Ack}\,(k,\mathrm{Ack}\,(k+1,n))$, 因此可以构造 $f_{k+1} = h$:

$$h(0) = f_k(1)$$
$$h(n+1) = f_k(h(n))$$

因为 $f_k \in \mathcal{PRF}$, 所以 $f_{k+1} = h \in \mathcal{PRF}$.

因此 $Ack(4,n) = f_4(n) \in \mathcal{PRF}$.

2. 证明 $\mathrm{Ack}\,(4,n) \notin \mathcal{EF}$.

根据上述归纳过程, 我们可以计算出 $\mathrm{Ack}\,(1,n), \mathrm{Ack}\,(2,n), \mathrm{Ack}\,(3,n), \mathrm{Ack}\,(4,n)$ 的具体形式.

$$\mathrm{Ack}\,(1,n) = 2+n$$
$$\mathrm{Ack}\,(2,n) = 2n+3$$
$$\mathrm{Ack}\,(3,n) = 2^{n+3}-3$$
$$\mathrm{Ack}\,(4,n) = \underbrace{2^{\cdot^{\cdot^{2}}}}_{n+3\text{ 个 }2} - 3$$

然后证明 $\mathrm{Ack}\,(4,n)$ 不能被 $G(k,n)$ 控制.

反证法. 假设 $\mathrm{Ack}\,(4,n)$ 被 G 控制, 则存在 $k_0 \in \mathbb{N}$, 使得 $\forall n \in \mathbb{N}$, $\mathrm{Ack}\,(4,n) \leq G(k_0,n) = \underbrace{2^{\cdot^{\cdot^{2^n}}}}_{k_0\text{ 个 }2}$.

令 $n = k_0$, $\mathrm{Ack}\,(4,n) = \underbrace{2^{\cdot^{\cdot^{2}}}}_{k_0+3\text{ 个 }2} - 3 > \underbrace{2^{\cdot^{\cdot^{2^{k_0}}}}}_{k_0\text{ 个 }2}$, 矛盾.

因此 $\mathrm{Ack}\,(4,n) \notin \mathcal{EF}$.

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

题目 1.21. 设 $f:\mathbb{N}\to\mathbb{N}$, f 为一一映射, 证明: $f\in\mathcal{GRF}\Leftrightarrow f^{-1}\in\mathcal{GRF}$,

解答. 先证明充分性, $f\in\mathcal{GRF}\Rightarrow f^{-1}\in\mathcal{GRF}$. 构造

$$f^{-1}=\mu_y[f(y)-x]$$

因为 f 是一一映射, 因此 $f(y)=x$ 的根 y 必定是存在且唯一的.

对于必要性, 因为 $(f^{-1})^{-1}=f$ 且 f^{-1} 也是一一映射, 用类似上述构造容易证明.

题目 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: $f\in\mathcal{RF}$.

解答. 令 $p(x)=b_nx^n+b_{n-1}x^{n-1}+\cdots+b_0$, 令 $S=\{i\mid b_i\geq 0\}$, $T=\{i\mid b_i<0\}$. 于是

$$p(x)-a=\sum_{i\in S}b_ix^i-(a+\sum_{i\in T}|b_i|x^i)\in\mathcal{EF}$$

因此 $f=\mu_x[p(x)-a]\in\mathcal{RF}$.

题目 1.23. 设

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

证明: $f\in\mathcal{RF}$.

解答. $f(x,y)=\mu_k.[x\dot{-}k\times y]+\mu_k.[N(x+y)]\in\mathcal{RF}$.

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

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

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

解答. 定义 $h:\mathbb{N}\to\mathbb{N}$ 满足

$$\begin{aligned} h(0) &= 0 \\ h(1) &= 1 \\ h(n+2) &= 2002h(n+1)+2003h(n) \end{aligned}$$

首先有一个引理: 对于任意 $x\in\mathbb{N}$, $g(x)=rs(h(x),2005)$.

使用数学归纳法证明.

奠基, $g(0)=rs(h(0),2005)=0$, $g(1)=rs(h(1),2005)=1$.

归纳假设, 对于 $x=k,k+1$ 成立, $g(k)=rs(h(k),2005)$, $g(k+1)=rs(h(k+1),2005)$. 于是有

$$\begin{aligned} g(k+2) &= rs(2002g(k+1)+2003g(k), 2005) \\ &= rs(2002\cdot rs(g(k+1),2005)+2003\cdot rs(g(k),2005), 2005) \\ &= rs(2002\cdot h(k+1)+2003\cdot h(k), 2005) \\ &= rs(h(k+2), 2005) \end{aligned}$$

因此, 结论对于 $x=k+2$ 也成立, 证毕.

使用生成函数技术, 可以计算出 $h(n)=\frac{(-1)^{n+1}+2003^n}{2004}$.

1. 问题也就是求 $h(2006)=\frac{2003^{2006}-1}{2004} \bmod 2005$.

首先, $2003 \equiv -2 (\mathrm{mod}\ 2005)$, $2003^{2006} \equiv 2^{2006} (\mathrm{mod}\ 2005)$.

根据费马小定理, 对于质数 p 有 $a^{p-1} \equiv 1(\bmod\ p)$. 因为 $2005 = 5 \cdot 401$. 对于因子 5, $2006 \equiv 2 (\mathrm{mod}\ 4)$, 所以 $2^{2006} \equiv 2^2 \equiv 4 (\mathrm{mod}\ 5)$. 对于因子 401, $2006 \equiv 6 (\mathrm{mod}\ 400)$, 所以 $2^{2006} \equiv 2^6 \equiv 64 (\mathrm{mod}\ 401)$. 最后使用中国剩余定理, $2^{2006} \equiv 64 (\mathrm{mod}\ 2005)$.

所以 $h(2006) \equiv \frac{2003^{2006}-1}{2004} \equiv 2005 - (64-1) \equiv 1942 (\mathrm{mod}\ 2005)$, $g(2006) = 1942$.

2. 因为 $h(n) = \frac{(-1)^{n+1}+2003^n}{2004} \in \mathcal{EF}$, 所以 $g(n) = rs(h(n), 2005) \in \mathcal{EF}$.

   也可以使用定理 1.31, 注意到 $g(x) \le 2005$, 所以 $g \in \mathcal{EF}$.

题目 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: $f \in \mathcal{GRF}$.

解答. Leibniz 公式 $\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \dots$.

定义 $L(n,k)$ 表示 Leibniz 公式的前 $n+1$ 项和乘 k 下取整的值, $L(n,k) = \sum_{i=0}^{n} (-1)^i \frac{k}{2i+1} = \left(\sum_{i=0}^{n} N(rs(i,2)) \cdot \frac{k}{2i+1} \right) - \left(\sum_{i=0}^{n} rs(i,2) \cdot \frac{k}{2i+1} \right) \in \mathcal{EF}$.

所以, $f(n) = rs(L(100^n, 4 \cdot 10^n), 10)$.