

# “Introduction to Models of Computation” Solutions

Yanyan Jiang

Spring, 2012

## 1 Chapter 1

**1.1 Prove: for any fixed  $k$ , unary number theoretic function  $x + k \in \mathcal{BF}$ .**

**Proof.** We have  $+_0 = P_1^1$  and  $+_k = \underbrace{S \circ S \circ \dots \circ S}_{k-1 \text{ times}} \in \mathcal{BF}$  for all  $k \geq 1$ .  $\square$

**1.2 Prove: for any  $k \in \mathbb{N}^+$ ,  $f : \mathbb{N}^k \rightarrow \mathbb{N}$ , there always exists  $h$  satisfying  $f(\mathbf{x}) < \|\mathbf{x}\| + h$  if  $f \in \mathcal{BF}$ .**

**Proof.** We perform a structural induction on the constructive length  $\ell$  of basic function  $f$ .

When  $\ell = 0$ ,  $f \in \mathcal{IF}$ . Thus  $f(x) \leq S(x) < x + 2$  for all  $x$ . Let  $h_0 = 2$ .

We assume when  $0 \leq \ell \leq n$ , all functions  $f$  with constructive length no longer than  $\ell$  satisfy  $f(\mathbf{x}) < \|\mathbf{x}\| + h_n$ .

In the case of  $\ell = n + 1$ , assume that  $f$  is constructed by sequence  $f_0, f_1, \dots, f_n, f$ . If  $f \in \mathcal{IF}$ , it is trivial that  $f(x) \leq S(x) < \|\mathbf{x}\| + 2h_n$ . Elsewise,  $f = \text{Comp}_k^m[f_{i_0}, f_{i_1}, \dots, f_{i_k}]$ . By inductive hypothesis we have  $f_{i_j} < h_n$  for all  $j$ , thus  $f(\mathbf{x}) < \max\{f_{i_j}(\mathbf{x})\} + h_n < \|\mathbf{x}\| + 2h_n$ . Therefore, by letting  $h = 2^{\ell+1}$ ,  $f(\mathbf{x}) < \|\mathbf{x}\| + h$  always holds.  $\square$

**1.3 Prove: binary number theoretic function  $x + y \notin \mathcal{BF}$ .**

**Proof.** We have already proved that for any  $k \in \mathbb{N}^+$ ,  $f : \mathbb{N}^k \rightarrow \mathbb{N}$ , there always exists  $h$  satisfying  $f(\mathbf{x}) < \|\mathbf{x}\| + h$  if  $f \in \mathcal{BF}$ .

If  $x + y \in \mathcal{BF}$ , there is  $h$  such that  $x + x = 2x = 2\|x\| < \|x\| + h$ , which implies  $x < h$ , leading to contradiction.  $\square$

#### 1.4 Prove: binary number theoretic function $x - y \notin \mathcal{BF}$ .

**Proof.** Since  $\text{pred} = \text{Comp}_2^1[P_1^1, S \circ Z]$ , proving  $\text{pred} \notin \mathcal{BF}$  is enough to show  $x - y \notin \mathcal{BF}$ . Assume there exists shortest construction procedure  $f_0, f_1, \dots, f_n, \text{pred}$ . There are two cases:

Case 1.  $f_n \in \{S, Z, P\}$  is not the case.

Case 2.  $f_n$  is a composition of  $S, Z$  or  $P$ .  $f_n$  cannot be composition of  $S$  because  $S(x) > 0$  for all  $x$ , and  $\text{pred}(1) = 0$ . Also,  $f_n$  cannot be composition of  $Z$  because  $\text{pred}(x)$  can be arbitrarily large. Finally,  $f_n$  cannot be composition of  $P$  because this contradicts the shortest construction assumption.  $\square$

#### 1.5 Let $\text{pg}(x, y) = 2^x(2y + 1) - 1$ . Prove that there exists elementary function $K(x)$ and $L(x)$ such that $K(\text{pg}(x, y)) = x$ , $L(\text{pg}(x, y)) = y$ and $\text{pg}(K(z), L(z)) = z$ .

**Proof.** Let  $K(x) = \text{ep}_0(x + 1)$ ,  $L(x) = \frac{1}{2} \left( \frac{x + 1}{2^{K(x)}} - 1 \right)$ , we have

$$\text{pg}(K(z), L(z)) = 2^{\text{ep}_0(z+1)} \left( \frac{z + 1}{2^{\text{ep}_0(z+1)}} \right) - 1 = z. \quad \square$$

#### 1.6 Let $f : \mathbb{N} \rightarrow \mathbb{N}$ . Prove that $f$ could be left function in a pairing function if and only if $|\{x \in \mathbb{N} : f(x) = i\}| = \aleph_0$ for all $i \in \mathbb{N}$ .

**Proof.** The necessity is trivial by a simple contradiction. For the sufficiency,  $|\{x \in \mathbb{N} : f(x) = i\}| = \aleph_0$  implies that there exists onto mapping  $f_i : N_i \rightarrow \mathbb{N}$  such that  $N_i = \{x \mid f(x) = i\}$  for all  $i$ , which implies that  $f_i^{-1}$  exists for all  $i$ . By letting  $\text{pg}(x, y) = f_x^{-1}(y)$ , we have  $K(z) = f(f_x^{-1}(z)) = x$  and  $L(z) = f_x(z) = f_x(f_x^{-1}(y)) = y$ .  $\square$

#### 1.7 Prove that all elementary function can be generated by applying composition and $\prod_{i=n}^m [\cdot]$ operator.

**Proof.** We first build some function by the conditioning ability of  $\Pi$ :

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

Also, we can construct integral power and thus equality by

$$\begin{aligned} \text{pow}(x, k) &= \prod_{i=1}^k x, \\ \text{eq}(x, y) &= \text{leq}(x, y)^{N(\text{geq}(x, y))}, \end{aligned}$$

and finally  $\Sigma$  operator by creating logarithm:

$$\begin{aligned} \log(x) &= \prod_{i=0}^x i^{N(\text{eq}(2^i, x))}, \\ \sum_{i=n}^m f(i, \mathbf{x}) &= \log \prod_{i=n}^m 2^{f(i, \mathbf{x})}. \end{aligned}$$

Notice that  $x \times y = \sum_{i=1}^x y$ ,  $x + y = \log(2^x \cdot x^y)$ , and  $|x - y| = \left( \sum_{i=x+1}^y 1 \right) + \left( \sum_{i=y+1}^x 1 \right)$ , our proof is complete.  $\square$

**1.8 Let  $M(x)$  be  $M(M(x+11))$  when  $x \leq 100$  and  $x-10$  when  $x > 100$ . Prove  $M(x) = 91$  when  $x \leq 100$ .**

**Proof.** The basic case is  $M(99) = M(M(110)) = M(100) = M(M(111)) = M(101) = 91$ , and  $M(x) = M(M(x)) = M(x+1)$  when  $90 \leq x \leq 100$ . An induction on  $x$  shows  $M(x) = 91$  for all  $0 \leq x \leq 100$ .  $\square$

**1.9 Prove:**  $\min x \leq n.[f(x, \mathbf{y})] = n - \max x \leq n.[f(n-x, \mathbf{y})]$ , and  $\max x \leq n.[f(x, \mathbf{y})] = n - \min x \leq n.[f(n-x, \mathbf{y})]$ .

**Proof.** For simplicity, let  $m = \min x \leq n.[f(x, \mathbf{y})]$  and  $M = \max x \leq n.[f(n-x, \mathbf{y})]$ .

If there is no  $0 \leq x \leq n$  satisfying  $f(x, \mathbf{y}) = 0$ , we have  $m = n$  and  $M = 0$ , hence  $m + M = n$ . Otherwise, let  $a$  be the minimum root of  $f(x, \mathbf{y})$ , thus  $f(x, \mathbf{y}) \neq 0$  for all  $x < a$ , and  $f(n-x, \mathbf{y}) \neq 0$  for all  $x > n-a$ . By definition, we can easily see that  $m + M = n$ . Since both  $m$  and  $M$  will not exceed  $n$ ,  $m + M = n$  yields  $m = n - M$  and  $M = n - m$ .

The another case is trivial by symmetry.  $\square$

**1.10 Prove:  $\mathcal{EF}$  is closed under the bounded max operator.**

**Proof.** For any  $f \in \mathcal{EF}$ ,

$$\max x \leq n.[f(x, \mathbf{y})] = \sum_{i=0}^n \left[ \left[ \left( \sum_{x=0}^i N(x, \mathbf{y}) \right) / \left( \sum_{x=0}^n N(x, \mathbf{y}) \right) \right] \times i \right]. \quad \square$$

**1.11 Prove: Euler's totient function  $\varphi \in \mathcal{EF}$ .**

$$\textbf{Proof. } \varphi(x) = \left\{ \sum_{y=0}^n N \left[ \left( \sum_{d=0}^{x+y} |\text{rs}(x, d) - \text{rs}(y, d)| \right) - 2 \right] \right\} - 1. \quad \square$$

**1.12 Let  $h(x)$  be subscript of the greatest prime factor. Assume that  $h(0) = h(1) = 0$ , prove that  $h \in \mathcal{EF}$ .**

$$\textbf{Proof. } h(x) = \max i \leq x. \left\{ N^2 \left| \sum_{j=0}^i [N(\text{rs}(i, j))] - 2 \right| + N^2[\text{rs}(x, i)] \right\}. \quad \square$$

**1.13 Prove that the Fibonacci sequence  $f(0) = f(1) = 1, f(x+2) = f(x) + f(x+1) \in \mathcal{EF}$  and  $\mathcal{PRF}$ .**

**Proof.** Let  $\{\text{pg}, K, L\}$  be any paring function in  $\mathcal{PRF}$ . Let

$$\begin{aligned} F(0) &= \text{pg}(1, 0) \\ F(x+1) &= \text{pg}(K(F(x)) + L(f(x)), K(F(x))), \end{aligned}$$

we have  $F$  is in  $\mathcal{PRF}$  and  $K(F(x)) = f(x)$ , therefore  $f \in \mathcal{PRF}$ .

On the other hand,  $f(x)$  is the number of binary strings of length  $x-1$  without successive 1s. Therefore

$$f(x) = \sum_{i=0}^{2^{n-1}} \sum_{j=0}^{n-2} N(\text{eq}(\text{rs}(i, 2^j), \text{rs}(i, 2^{j+1}))) \times \text{eq}(\text{rs}(i, 2^j), 0) \in \mathcal{EF}. \quad \square$$

**1.14 Prove that the number theoretic function  $Q(x, y, z, v) \equiv p(\langle x, y, z \rangle) \mid v$  is elementary.**

**Proof.** We have already seen that  $p(n) \in \mathcal{EF}$  and  $\langle x, y, z \rangle = 2^x \cdot 3^y \cdot 5^z \in \mathcal{EF}$ . Therefore  $Q(x, y, z) = \text{eq}(\text{rs}(v, p(\langle x, y, z \rangle)), 0) \in \mathcal{EF}$ .  $\square$

**1.15 Let  $f : \mathbb{N} \rightarrow \mathbb{N}$ ,  $f(0) = 1, f(1) = 4, f(2) = 6, f(x+3) = f(x) + f^2(x+1) + f^3(x+2)$ . Prove that  $f \in \mathcal{PRF}$ .**

**Proof.** Let  $G(0) = \langle 1, 4, 6 \rangle$  and

$$G(x+1) = \langle \text{ep}_1(G(x)), \text{ep}_2(G(x)), \text{ep}_0(G(x)) + \text{ep}_1^2(G(x)) + \text{ep}_2^3(G(x)) \rangle,$$

we have  $\text{ep}_0(G(x)) = f(x)$ .  $\square$

**1.16 Let  $f(n) = n^{n^{\dots^n}}$ , prove that  $f \in \mathcal{PRF} - \mathcal{EF}$ .**

**Proof.** Let  $g(n, 0) = 0$  and  $g(n, x+1) = n^{g(n, x)}$ . Thus  $g \in \mathcal{PRF}$  and  $g(n, n) = f(n)$ , therefore  $f \in \mathcal{PRF}$ . On the other hand,  $G(k, x) = 2^{2^{\dots^x}}$  is one among the control functions of  $\mathcal{EF}$ . If  $f \in \mathcal{EF}$ , there exists  $k$  such that  $G(k, n) > f(n)$  for all  $n$ . However, this is impossible because  $f(k+2)$  is always greater than  $G(k, k)$ .  $\square$

**1.17 Let  $g : \mathbb{N} \rightarrow \mathbb{N} \in \mathcal{PRF}$ ,  $f : \mathbb{N}^2 \rightarrow \mathbb{N}$  satisfies that  $f(x, 0) = g(x)$ ,  $f(x, y+1) = f(f(\dots f(f(x, y), y-1), \dots), 0)$ . Prove that  $f \in \mathcal{PRF}$ .**

**Proof.** Let  $G(x, 0) = x$  and  $G(x, y+1) = g(G(x, y))$ ,  $F(0) = 1, F(x+1) = F(x) + \sum_{i=0}^x F(i)$ . it is obvious that  $G \in \mathcal{PRF}$ , and  $F(x) = \text{Fib}(2x) \in \mathcal{PRF}$ .

We now prove that  $f(x, y) = G(x, F(y))$ . The basis is  $f(x, 0) = G(x, 1) = g(x)$ , and we assume that  $f(x, y^*) = G(x, F(y^*))$  For all  $y^* \leq y$ . Therefore,

$$\begin{aligned} f(x, y+1) &= \underbrace{g(g(\dots g( f(x, y)) \dots))}_{\sum_{i=0}^y F(i) \text{ times}} \\ &= \underbrace{g(g(\dots g( x) \dots))}_{F(y) + \sum_{i=0}^y F(i) \text{ times}} \\ &= G(x, F(y+1)), \end{aligned}$$

which means  $f(x, y) = G(x, F(y)) \in \mathcal{PRF}$ .  $\square$

**1.18** If  $f, g : \mathbb{N} \rightarrow \mathbb{N}$  differs for only finitely many values. Prove that  $f \in \mathcal{GRF}$  if and only if  $g \in \mathcal{GRF}$ .

**Proof.** For the necessity, we have  $g \in \mathcal{GRF}$  and  $S = \{s_0, s_1, \dots, s_k\}$  satisfies that for all  $x \in \mathbb{N} \setminus S$ ,  $f(x) = g(x)$ .

Let  $F(x) = \sum_{i=0}^k g(s_i) \cdot N(\text{eq}(s_i, x)) + N\left(\sum_{i=0}^k N(\text{eq}(s_i, x))\right) g(x)$ , because the  $\Sigma$  in  $F$  is walked through finitely many of values,  $F$  is in  $\mathcal{GRF}$ , and  $f(x) = F(x)$  for all  $x$ , thus  $f \in \mathcal{GRF}$ . Also, the sufficiency case is trivial by symmetry.  $\square$

**1.19** Prove that  $\left\lfloor \left( \frac{\sqrt{5}+1}{2} \right)^n \right\rfloor \in \mathcal{EF}$ .

**Proof.** Let  $\varphi = \frac{\sqrt{5}+1}{2}$ , we can rewrite the solution of  $y = \lfloor \varphi n \rfloor$  by

$$\begin{aligned} y &= \max_{x \in \mathbb{N}} x \\ \text{s.t. } & \varphi n \leq x, \end{aligned}$$

therefore  $y = \sum_{i=0}^{2n} i \times N \left\{ \text{eq} \left[ \sum_{j=i}^{2n} N(\text{eq}(i^2 - in - n^2, 0)), 1 \right] \right\}$ .  $\square$

**1.20** Prove that  $\text{Ack}(4, n) \in \mathcal{PRF} - \mathcal{RF}$ .

**Proof.** Let  $f(0) = 1$ ,  $f(n+1) = 2^{f(n)}$ , we immediately have  $f \in \mathcal{PRF}$ , therefore  $\text{Ack}(4, n) = f(n+3) - 3 \in \mathcal{PRF}$ .

$G(k, x) = 2^{2^{\dots^x}}$  is the control function of  $\mathcal{EF}$ . Assume that  $\text{Ack}(4, n) \in \mathcal{EF}$ , thus  $G'(k, x) = \text{Ack}(4, x+k) + 3 \in \mathcal{EF}$ . However,  $G(k, x) < G'(k, x)$  contradicts the assumption, yielding  $\text{Ack}(4, n) \in \mathcal{PRF} - \mathcal{EF}$ .  $\square$

**1.21** Let  $f : \mathbb{N} \rightarrow \mathbb{N}$  and being 1-1 and onto. Prove that  $f \in \mathcal{GRF}$  if and only if  $f^{-1} \in \mathcal{GRF}$ .

**Proof.** The sufficiency can be shown by the fact that

$$f^{-1}(x) = \mu y. |f(y) - x|$$

because there exists unique  $y$  such that  $f(y) = x$ , and hence the root of  $|f(y) - x|$ . Therefore,  $\mu y. |f(y) - x|$  is the unique value of  $y$  satisfying  $f(y) = x$ , i.e.,  $y = f^{-1}(x)$ . Also because  $(f^{-1})^{-1} = f$ , the case of necessity is trivial by symmetry.  $\square$

**1.22** Let  $p$  be a polynomial with integral coefficient, and  $f : \mathbb{N} \rightarrow \mathbb{N}$  defined by the non-negative root of  $f(a) = p(x) - a$ . Prove that  $f \in \mathcal{RF}$ .

**Proof.** Let  $p(x) = a_n x^n + \dots + a_1 x + a_0$ ,  $S = \{i \mid a_i > 0\}$ , and  $T = \{i \mid a_i < 0\}$ , we have

$$|p(x) - a| = \left| \sum_{i \in S} |a_i| x^i - \left( a + \sum_{i \in T} |a_i| x^i \right) \right| \in \mathcal{EF}.$$

Therefore,  $f(a) = \mu x. |p(x) - a| \in \mathcal{RF}$ .  $\square$

**1.23** Let  $f(x, y) = x/y$  if  $y \neq 0 \wedge y \mid x$  and  $\uparrow$  otherwise. Prove that  $f \in \mathcal{RF}$ .

**Proof.**  $f(x, y) = \mu k. |x - ky| + \mu k. N(x + y) \in \mathcal{RF}$ .  $\square$

**1.24** Define  $g : \mathbb{N} \rightarrow \mathbb{N}$  by  $g(0) = 0, g(1) = 1, g(n + 2) = \text{rs}((2002g(n + 1) + 2003g(n)), 2005)$ . Find  $g(2006)$ .

**Proof.** We have  $g(n) = \text{rs}\left(\frac{(-1)^{n+1} + 2003^n}{2004}, 2005\right)$  and  $2005 = 5 \cdot 401$ , therefore

$$\begin{aligned} g(2006) \bmod 2005 &= \left( (2003^{2006} - 1) \times 2004^{-1} \right) \bmod 2005 \\ &= \left( (2^{2006} - 1) \times 2004 \right) \bmod 2005. \end{aligned}$$

Since  $a^{p-1} \equiv 1 \pmod{p}$  for all prime  $p$ ,  $2^{2006} \equiv 2^2 \equiv 4 \pmod{5}$ ,  $2^{2006} \equiv 2^6 \equiv 64 \pmod{401}$ . According to the Chinese remainder theorem,  $2^{2006} \equiv 64 \pmod{2005}$ . Therefore,  $g(2006) \equiv 63 \times 2004 \equiv 1942 \pmod{2005}$ .  $\square$

**1.25** Let  $f : \mathbb{N} \rightarrow \mathbb{N}$  be the  $n$ -th digit in the decimal representation of  $\pi$ . Prove that  $f \in \mathcal{GRF}$ .

**Proof.** Given a  $m$  by  $m$  grid, we count the integral point of  $(x, y)$  within a circle centered at  $(0, 0)$  with radius  $m$  by

$$S = \left| \{(x, y) \mid x, y \in \mathbb{N} \text{ and } x^2 + y^2 \leq m^2\} \right|$$

to approximately find  $\pi$ .  $S$  is elementary because

$$S(m) = \sum_{i=0}^m \sum_{j=0}^m N(i^2 + j^2 - m^2).$$

Area of the circle is  $S_c(m) = \pi m^2/4$ , and by the fact that the circle intersects with at most  $2m$   $1 \times 1$  blocks, we have  $|S(m) - S_c(m)| < 2m$ , therefore

$$\left| \frac{S(m)}{m^2} - \frac{\pi}{4} \right| = \frac{1}{m^2} |S(m) - S_c(m)| < 2m^{-1}, \text{ and } |4S(m) - m^2\pi| < 8m.$$

To compute  $f(n)$ , we need an exponentially large grid, say,  $m = 10^k$ . Then we have  $|4S(10^k) - 10^{2k} \cdot \pi| < 10^{k+1}$ . We know that  $4S(10^k)$  has  $2k$  digits and last  $k$  of them is inaccurate, so we use regular  $\mu$  operator to enumerate  $k$  until we met a non-zero digit between the first  $n+1$  digits and the last  $k$  digits:

$$K(n) = \mu k. \left\{ n+1-k + N \left[ \text{rs} \left( \frac{S(10^k)}{10^k}, 10^{k-n-1} \right) \right] \right\}.$$

Since there is no infinitely long successive zeros in decimal representation of  $\pi$  (otherwise  $\pi$  will be rational), regularity is ensured and thus  $K \in \mathcal{GRF}$ , therefore  $f(n) = \text{rs} \left[ \frac{S(10^{K(n)})}{10^{K(n)+1}}, 10 \right] \in \mathcal{GRF}$ .  $\square$

## 2 Chapter 2