“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 $+_k = \underbrace{S \circ S \circ \ldots \circ S}_{k-1 \text{ times}} \in \mathcal{BF}$ for all $k \geq 1$. □

1.2 Prove: for any $k \in \mathbb{N}^+, f : \mathbb{N}^k \to \mathbb{N}$, 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 ℓ 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 ℓ satisfy $f(\mathbf{x}) < \|\mathbf{x}\| + h_n$.

In the case of $\ell = n + 1$, assume that f is constructed by sequence $f_0, f_1, \ldots, f_n, f$. If $f \in \mathcal{IF}$, it is trivial that $f(x) \leq S(x) < \|\mathbf{x}\| + 2h_n$. Elsewise, $f = \mathrm{Comp}_k^m[f_{i_0}, f_{i_1}, \ldots, f_{i_k}]$. 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. □

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

Proof. We have already proved that for any $k \in \mathbb{N}^+, f : \mathbb{N}^k \to \mathbb{N}$, 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 $x + x = 2x = 2\|\mathbf{x}\| < \|\mathbf{x}\| + h$, 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 $f_0, f_1, \ldots, f_n, \text{pred}$. 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 $K(x) = \text{ep}_0(x + 1), L(x) = \dfrac{1}{2}\left(\dfrac{x+1}{2^{K(x)}} - 1\right)$, we have

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

1.6 Let $f : \mathbb{N} \to \mathbb{N}$. 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 $f_i : N_i \to \mathbb{N}$ 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 Π:

$$N(x) = \prod_{i=1}^{x} Z(i), N^2(x) = \prod_{i=1}^{N(x)} Z(i)$$
$$\text{leq}(x, y) = \prod_{i=x}^{y} Z(i), \text{geq}(x, y) = \prod_{i=y}^{x} Z(i)$$
$$\text{gt}(x, y) = N(\text{leq}(x, y)), \text{lt}(x, y) = N(\text{geq}(x, y)).$$

Then, we can conjunct and disjunct between predicates by

$$\wedge(x, y) = \prod_{i=1}^{N(x)} y, \vee(x, y) = N(N(x) \wedge N(y)),$$

therefore $\text{eq}(x, y) = N(\text{gt}(x, y)) \wedge N(\text{lt}(x, y))$.

On the other hand, we construct Σ operator in the following way:

$$\text{pow}(x, k) = \prod_{i=1}^{k} P_2^2(i, x),$$
$$\log(x) = \prod_{i=0}^{x} i^{N(\text{eq}(2^i, x))},$$
$$\sum_{i=n}^{m} f(i, \mathbf{x}) = \log \prod_{i=n}^{m} 2^{f(i, \mathbf{x})},$$

and the rest of our proof is trivial: $x \times y = \sum_{i=1}^{x} y$, $x + y = \log(2^x \times 2^y)$, $x - y = \sum_{i=0}^{x} N(\text{eq}(i + y, x)) \times i$ and $|x - y| = \text{gt}(x, y) \times (x - y) + \text{lt}(x, y) \times (y - x)$. □

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 $0 \leq x \leq 100$. □

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

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

If there is no $0 \le x \le n$ 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 $f(x,\mathbf{y}) \ne 0$ for all $x < a$, and $f(n-x,\mathbf{y}) \ne 0$ 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. □

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

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

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

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

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

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

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

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

$$F(0) = \mathrm{pg}(1,0)$$
$$F(x+1) = \mathrm{pg}(K(F(x)) + L(f(x)), K(F(x))),$$

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

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

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 $Q(x, y, z) = \mathrm{eq}(\mathrm{rs}(v, p(\langle x, y, z\rangle)), 0) \in \mathcal{EF}$. $\square$

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

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

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

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

1.16 Let $f(n) = n^{n^{\cdots^{n}}}$, 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, $G(k, x) = 2^{2^{\cdots^{x}}}$ is one among the control functions of $\mathcal{EF}$. If $f \in EF$, 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 $g : \mathbb{N} \to \mathbb{N} \in \mathcal{PRF}, f : \mathbb{N}^2 \to \mathbb{N}$ satisfies that $f(x, 0) = g(x)$, $f(x, y+1) = f(f(\ldots f(f(x, y), y-1), \ldots), 0)$. Prove that $f \in \mathcal{PRF}$.

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

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,

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

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

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

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

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

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

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 $\text{Ack}(4,n) = f(n+3) - 3 \in \mathcal{PRF}$.

$G(k,x) = 2^{2^{\cdot^{\cdot^{\cdot^{x}}}}}$ 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 $\text{Ack}(4,n) \in \mathcal{PRF} - \mathcal{EF}$. □

1.21 1.21

1.22 1.22

1.23 1.23

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

Proof. We have $g(n) = \mathrm{rs}\left(\frac{(-1)^{n+1} + 2003^n}{2004}, 2005\right)$ 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 $a^{p-1} \equiv 1 \bmod p$ for all prime p, $2^{2006} \equiv 2^2 \equiv 4 \bmod 5, 2^{2006} \equiv 2^6 \equiv 64 \bmod 401$. According to the Chinese remainder theorem, $2^{2006} \equiv 64 \bmod 2005$. Therefore, $g(2006) \equiv 63 \times 2004 \equiv 1942 \bmod 2005$. □

1.25 1.25