"Introduction to Models of Computation" Solutions

Yanyan Jiang

Spring, 2012

1 Recursive Functions

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

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

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 1-1 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:

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

Also, we can construct integral power and thus equality by

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

and finally Σ operator by creating logarithm:

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

Notice that $x \times y = \sum_{i=1}^{x} y$, $x + y = \log(2^x \cdot 2^y)$, 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 $x \le 100$ and $x-10$ when $x > 100$. Prove $M(x) = 91$ when $x \le 100$.

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 $90 \le x \le 100$. An induction on x shows $M(x) = 91$ for all $0 \le x \le 100$. $\square$

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 $f \in \mathcal{EF}$,

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

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

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

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

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

$$f(x) = \sum_{i=0}^{2^{n-1}-1} N\left[\sum_{j=0}^{n-2} \mathrm{neq}\left(\frac{\mathrm{rs}(i,2^j)}{2^{j-1}},1\right)\mathrm{neq}\left(\frac{\mathrm{rs}(i,2^{j+1})}{2^j},1\right)\right] \in \mathcal{EF}. \qquad \square$$

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 $G(k,k+2)$. $\square$

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 $G(x,y+1) = g(G(x,y))$. A simple induction shows that $f(x,y) = g^{2^{y-1}}(x)$, thust $f(x,y) = G(x, 2^{y-1}) \in \mathcal{PRF}$. $\square$

1.18 If $f,g : \mathbb{N} \to \mathbb{N}$ 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 $S = \{s_0, s_1, \ldots, s_k\}$ satisfies that for all $x \in \mathbb{N} \setminus S$, $f(x) = g(x)$.

Let $F(x) = \sum_{i=0}^{k} g(s_i) \cdot N(\text{eq}(s_i, x)) + N\left(\sum_{i=0}^{k} N\Big(\text{eq}(s_i, x)\Big)\right) g(x)$, because the Σ 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

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

therefore $y = \max x \leq 2n.\text{eq}(x^2 - nx - n^2, 0)$. $\square$

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

$G(k, x) = 2^{2^{\cdots^{x}}}$ 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 $f : \mathbb{N} \to \mathbb{N}$ 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 $\left(f^{-1}\right)^{-1} = f$, the case of necessity is trivial by symmetry. $\square$

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

Proof. Let $p(x) = a_n x^n + \ldots + a_1 x + a_0$, $S = \{i \mid a_i > 0\}$, 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 $g : \mathbb{N} \to \mathbb{N}$ by $g(0) = 0, g(1) = 1, g(n+2) = \mathrm{rs}((2002 g(n+1) + 2003 g(n)), 2005)$. Find $g(2006)$.

Proof. We have $g(n) = \mathrm{rs}\left(\dfrac{(-1)^{n+1} + 2003^n}{2004}, 2005 \right)$ 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, $g(2006) \equiv 63 \times 2004 \equiv 1942 \bmod 2005$. $\square$

1.25 Let $f : \mathbb{N} \to \mathbb{N}$ be the n-th digit in the decimal representation of π. 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 π. 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 $2m$ 1×1 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 μ 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 π (otherwise π will be rational), regularity is ensured and thus $K \in \mathcal{GRF}$, therefore $f(n) = \text{rs} \left[\frac{S\left(10^{K(n)}\right)}{10^{K(n)+1}}, 10 \right] \in \mathcal{GRF}$. □

2 Abacus Machines

2.1 Construct AM for $f(x) = 2x$.

Proof. $f = \langle \mathbf{S}_1 \mathbf{A}_2 \mathbf{A}_3 \rangle_1 \, \mathbf{move}_{2,1} \mathbf{move}_{3,1}$. □

2.2 Construct AM for $f(x) = \lfloor x/2 \rfloor$.

Proof. $f = \mathbf{A}_1 \langle \mathbf{S}_1 \mathbf{S}_1 \mathbf{A}_2 \rangle_1 \, \mathbf{move}_{2,1} \mathbf{S}_1$. □

2.3 Construct AM for $f(x) = x \cdot y$.

Proof. $f = \mathbf{move}_{1,3} \left\langle \mathbf{copy}_{3,1,4} \mathbf{S}_2 \right\rangle_2 \mathbf{Z}_3$. □

2.4 Construct AM for $g(x) = \mu y.[f(x, y)]$ assuming that $\mathbf{F} \in$ AM defines f.

Proof. Assume that $\mathbf{F}$ uses at most k pillars. If x, y is located at position $k+1, k+2$, respectively, we can compute $f(x, y)$ by

$$\mathbf{M} = \mathbf{copy}_{k+1,1} \mathbf{copy}_{k+2,2} \mathbf{F}.$$

Therefore, g can be constructed by repeatedly enumerate y until f becomes zero:

$$g = \mathbf{move}_{1,k+1} \mathbf{M} \left\langle \mathbf{A}_{k+2} \mathbf{copy}_{k+1,1} \mathbf{copy}_{k+2,2} \mathbf{M} \right\rangle_1 \mathbf{move}_{k+2,1} \mathbf{Z}_{k+1}.$$ □

2.5 Construct AM for $f(x) = 2^x$.

Proof. $f = \mathbf{move}_{1,2} \mathbf{Z}_1 \mathbf{A}_1 \left\langle \mathbf{copy}_{1,3} \mathbf{move}_{3,1} \mathbf{S}_2 \right\rangle_2$. □

3 λ-calculus

3.1 Prove the *Parenthesis Lemma*: for all $M \in \Lambda$, the occurrence of left parenthesis is equal to the occurrence of right parenthesis.

Proof. Let $p(M)$ be the difference of the occurrence of left and right parenthesis in M, We have $p(x) = 0$, $p[(M_1 M_2)] = p(M_1) + p(M_2)$ and $p[(\lambda x.M)] = p(M)$. A formal proof comes from a simple structural induction. □

3.2 Find β-nf of $SSSS$.

Proof. According to $S \equiv \lambda xyz.xz(yz)$ and $SS =_\beta \lambda xyz.yz(xyz)$, we have

$$\begin{aligned} SSSS &=_\beta SS(SS) \\ &=_\beta \lambda xy.[xy(SSxy)] \\ &=_\beta \lambda xy.xy(\lambda z.yz(xyz)) = M. \end{aligned}$$

$M =_\beta SSSS$ is β-nf of $SSSS$ because it has no redex. □

3.3 Prove that there is no β-nf for $(\lambda x.xxx)(\lambda x.xxx)$.

Proof. Let $N = \lambda x.xxx$ and $M = NN$, we have $\text{Sub}(M) = \{N, NN\}$. It is trivial that $NN \in \text{Sub}(M)$. If $\text{Sub}(A) = \bigcup_{i=1}^{k} N^k$ and $A \to_\beta B$, $\text{Sub}(B)$ will be either $\text{Sub}(A)$ or $\text{Sub}(A) \cup N^{k+1}$, hence $NN \in \text{Sub}(M')$ holds for all $M \twoheadrightarrow_\beta M'$.

Assume that the β-nf of M is M_β, we have $NN \in \text{Sub}(M_\beta)$ which leads to a contradiction. □

3.4 Let $F \in \Lambda$ with the form of $\lambda x.M$. Prove that $\lambda z.Fz =_\beta F$ and $\lambda z.yz \neq_\beta y$.

Proof. $\lambda z.Fz \equiv \lambda z.(\lambda x.M)z \to_\beta \lambda z.(M[x := z]) \equiv M$. □

3.5 Prove the fixed-point theorem for two variables: for all $F, G \in \Lambda$, exists $X, Y \in \Lambda$ such that $FXY = X$ and $GXY = Y$.

Proof. According to the equation $(GX)Y = Y$, let Y be the fixed-point of GX, say $\mathbf{Y}(GX)$, we have $FX(\mathbf{Y}(GX)) = X$, thus

$$\lambda x.[Fx(\mathbf{Y}(Gx))]X = X.$$

We can now derive a solution by letting $X = \mathbf{Y}[\lambda x.Fx(\mathbf{Y}(Gx))]$ and $Y = \mathbf{Y}(GX)$. □

3.6 Prove for all $M, N \in \Lambda^\circ$, there is a solution for $xN = Mx$.

Proof. Let x be the form of $\lambda a.T$, this makes $(\lambda a.T)N = T$. This reduces rest of our proof to finding a solution to

$$T = M(\lambda a.T) = [\lambda t.M(\lambda a.t)]T.$$

Let $T = \mathbf{Y}[\lambda t.M(\lambda a.t)]$ hence $x = \lambda x.\mathbf{Y}[\lambda y.M(\lambda z.y)]$, $xN = Mx$ is satisfied. □

3.7 Prove that for all $P, Q \in \Lambda$, $P \twoheadrightarrow_\beta Q$ implies the existence of $n \geq 0$ and $P_0, \ldots, P_n \in \Lambda$ satisfying $P \equiv P_0$, $Q \equiv P_n$ and $P_i \rightarrow_\beta P_{i+1}$ for all $i < n$.

Proof. According to the fact that

$$\twoheadrightarrow_\beta = \bigcup_{i=0}^{\infty} (\rightarrow_\beta)^i,$$

for all $P, Q \in \Lambda$, $P \twoheadrightarrow_\beta Q$ implies existence of k such that $P(\rightarrow_\beta)^k Q$. A structural induction on k directly leads to a proof. □

3.8 Prove that for all $P, Q \in \Lambda$, $P \twoheadrightarrow_\beta Q$ implies $\lambda z.P \twoheadrightarrow_\beta \lambda z.Q$.

Proof. According to 3.7, sequence $P_0, \ldots, P_n \in \Lambda$ with $P \equiv P_0$, $Q \equiv P_n$ and $P_i \rightarrow_\beta P_{i+1}$. Also because $\rightarrow_\beta$ is the compatible closure of β, we have $\lambda z.A \rightarrow_\beta \lambda z.B$ for all $A \rightarrow_\beta B$. Thus for all $i < n$,

$$\lambda z.P_i \rightarrow_\beta \lambda z.P_{i+1}$$

in $\lambda z.P_0, \lambda z.P_1, \ldots, \lambda z.P_n$ always holds, that is, $\lambda z.P \twoheadrightarrow_\beta \lambda z.Q$. □

3.9 Prove that for all $P, Q \in \Lambda$, $P =_\beta Q$ implies the existence of $n \geq 0$ and $P_0, \ldots, P_n \in \Lambda$ satisfying $P \equiv P_0$, $Q \equiv P_n$ and $P_i \rightarrow_\beta P_{i+1}$ or $P_{i+1} \rightarrow_\beta P_i$ for all $i < n$.

Proof. The technique used is exactly the same as in problem 3.7, except we are using $=_\beta = \bigcup_{k=0}^{\infty} \left(\rightarrow_\beta \cup \rightarrow_\beta^{-1}\right)^k$. □

3.10 Prove that for all $M, N \in \Lambda$, $M =_\beta N$ if and only if $\lambda\beta \vdash M = N$.

Proof. The axiom of $\lambda\beta$ shows that $M = M$ and $(\lambda x.M)N = M[x := N]$. Also because $\beta \equiv \{((\lambda x.M)N, M[x := N]) : M, N \in \Lambda \wedge x \in V\}$ and $=_\beta$ is reflexive, $M =_\beta M$ and $(\lambda x.M)N =_\beta M[x := N]$ holds. This serves our inductive basis.

Assume that $\lambda\beta \vdash M = N$ implies $M =_\beta N$ for all formula $M = N$ with construction length less or equal to ℓ. A formula of construction length $\ell + 1$ will be within either of the following cases:

1. $(\sigma) : M = N \vdash N = M$, $=_\beta$ is symmetric makes $N =_\beta M$;
2. $(\tau) : M = N, N = L \vdash M = L$, $=_\beta$ is transitive makes $N =_\beta M$;
3. $(\mu) : M = N \vdash ZM = ZN$, $=_\beta$ is compatible makes $ZM =_\beta ZN$;
4. $(\nu) : M = N \vdash MZ = NZ$, $=_\beta$ is compatible makes $MZ =_\beta NZ$;
5. $(\xi) : M = N \vdash \lambda x.M = \lambda x.N$, $=_\beta$ is compatible makes $\lambda x.M =_\beta \lambda x.N$.

Therefore, $\lambda\beta \vdash M = N$ implies $M =_\beta N$.

On the other side, $M \to_\beta N$ implies $M =_\beta N$ because either $M\beta N$ thus $M = N$ by (β), or (M, N) is in the compatible closure of $\{(M', N')\}$ for some $M'\beta N'$.

By the theorem proved in 3.9, for all $M =_\beta N$, there exists $n \geq 0$ and $P_0, \ldots, P_n \in \Lambda$ such that $P \equiv P_0, Q \equiv P_n$ and either $P_i \to_\beta P_{i+1}$ or $P_{i+1} \to_\beta P_i$ for all $i < n$. Take the case of $n = 0$, which is that $M =_\beta M$ implies $\lambda\beta \vdash M = M$ as inductive basis, we perform an induction on the shortest construction length of n.

Assuming that for all $A =_\beta B$ with construction length of m less than n, $\lambda\beta \vdash A = B$ holds. For construction sequence $M = P_0, \ldots, P_{n-1}, P_n = N$, we have $\lambda\beta \vdash M = P_{n-1}$ by the inductive hypothesis. Because $P_{n-1} \to_\beta P_n$ or $P_n \to_\beta P_{n-1}$ means that $\lambda\beta \vdash P_{n-1} = P_n$, according to (τ), $\lambda\beta \vdash M = P_{n-1} = P_n = N$, therefore $A =_\beta B$ implies $\lambda\beta \vdash A = B$.

In summary, $=_\beta$ is equivalent to the formal system of $\lambda\beta$. □

3.11 Prove that for all $M, N \in \Lambda$, $M =_{\beta\eta} N$ if and only if $\lambda\beta\eta \vdash M = N$.

Proof. Exactly the same technique used in problem 3.10 can be applied to this problem. □

3.12 (This problem is duplicated with 3.16.)

3.13 Prove that by extending $\lambda\beta$ by axiom of $\lambda xy.x = \lambda xy.y$, $\lambda\beta^* \vdash M = N$ for all $M, N \in \Lambda$.

Proof. For all $M, N \in \Lambda$, $\lambda xy.x = \lambda xy.y \Rightarrow (\lambda xy.x)M = (\lambda xy.y)N \Rightarrow (\lambda xy.x)MN = (\lambda xy.y)MN \Rightarrow (\lambda xy.x)MN = (\lambda xy.y)MN \Rightarrow M = (\lambda xy.y)MN \Rightarrow M = N$. □

3.14 Prove that for binary relation R on Λ, $M \in NF_R$ implies: (1) there is no $N \in \Lambda$ such that $M \to_R N$; (2) $M \twoheadrightarrow_R N \Rightarrow M \equiv N$.

Proof. (1) Trivial by the definition of NF_R that, M has no redex.
(2) Assume that $M \not\equiv N$. $M \twoheadrightarrow_R N$ implies existence of $M = P_0, \ldots, P_n = N$ that, $P_i \to_R P_{i+1}$ for $i < n$. We must have $n \geq 1$ because $M \not\equiv N$. This leads to contradiction because there exists N such that $M \to_R N$. □

3.15 Prove that $M \rhd_{\mathrm{mcd}} M'$ and $N \rhd_{\mathrm{mcd}} N'$ implies $MN \rhd_{\mathrm{mcd}} M'N'$.

Proof. $M \rhd_{\mathrm{mcd}} M'$ means that there exists sequence $M_1, M_2, \ldots, M_n$ reduces M to M', and so does $N \rhd_{\mathrm{mcd}} N'$. Merging the two sequences will yield minimal complete development from MN to $M'N'$ because M_i will always be minimal redex of the remaining sequence. □

3.16 Prove that for all $M, N \in \Lambda$, $M =_\beta N$ implies the existence of T such that $M \twoheadrightarrow_\beta T$ and $N \twoheadrightarrow_\beta T$.

Proof. $M =_\beta N$ implies that

$$(M, N) \in \bigcup_{k=0}^{\infty} (\to_\beta \cup \leftarrow_\beta)^k.$$

We take the basis case of $k = 0$, that is, $M \equiv N$ as our basis. Assume that for all $(M, N) \in (\to_\beta \cup \leftarrow_\beta)^k$, there exists $T \in \Lambda$ such that $M \twoheadrightarrow_\beta T$ and $N \twoheadrightarrow_\beta T$. For the case of $(M, N) \in (\to_\beta \cup \leftarrow_\beta)^{k+1}$, either

$$(1)\ M \to_\beta P =_\beta N$$

or

$$(2)\ M \leftarrow_\beta P =_\beta N$$

holds where $(P, N) \in (\rightarrow_\beta \cup \leftarrow_\beta)^k$. According to the inductive hypothesis, there exists T_0 such that $P \twoheadrightarrow_\beta T_0$ and $N \twoheadrightarrow_\beta T_0$. Because $\twoheadrightarrow_\beta$ is transitive, We have $M \twoheadrightarrow_\beta T_0$ in the case (1).

In the case (2), according to the CR-property of $\twoheadrightarrow_\beta$, $P \twoheadrightarrow_\beta M$ and $P \twoheadrightarrow_\beta T_0$ implies the existence of $T \in \Lambda$ that, $M \twoheadrightarrow_\beta T$ and $T_0 \twoheadrightarrow_\beta T$. Again because the transitivity of $\twoheadrightarrow_\beta$, $N \twoheadrightarrow_\beta T_0$ and $T_0 \twoheadrightarrow_\beta T$ yields $N \twoheadrightarrow_\beta T$. Therefore such a T exists for all $k \in \mathbb{N}$. $\square$

3.17 Find $F \in \Lambda^\circ$ such that F λ-defines $f(x) = 3x$.

Proof. We are to construct $F\ulcorner n \urcorner = \ulcorner 3n \urcorner = \lambda fx.f^n(f^n(f^n x))$.

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

Therefore, $F \equiv \lambda xyz.xy(xy(xyz))$ λ-defines $f(x) = 3x$. $\square$

3.18 Let $\mathbf{D} \equiv \lambda xyz.z(\mathbf{K}y)x$. Prove that for all $X, Y \in \Lambda$, $\mathbf{D}XY\ulcorner 0 \urcorner = X$ and $\mathbf{D}XY\ulcorner n+1 \urcorner = Y$.

Proof. We have $\mathbf{D}XY\ulcorner 0 \urcorner = \ulcorner 0 \urcorner(\lambda y.Y)X = (\lambda fx.x)(\lambda y.Y)X = X$, and

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

$\mathbf{D}$ is very powerful because it have the ability of separating cases. $\square$

3.19 Let $\mathbf{Exp} \equiv \lambda xy.yx$. Prove that for all $n \in \mathbb{N}$ and $m \in \mathbb{N}^+$, $\mathbf{Exp}\ulcorner n \urcorner \ulcorner m \urcorner =_\beta \ulcorner n^m \urcorner$.

Proof. We simply expand **Exp** by

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

For $m = 1$, $(\lambda fy.f^n y)x = \lambda y.x^n y$. Assume that $(\lambda fy.f^n y)^m x = \lambda y.x^{n^m} y$, we have

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

This implies $\mathbf{Exp}\ulcorner n \urcorner \ulcorner m \urcorner = \lambda xy.x^{n^m} y = \ulcorner n^m \urcorner$ for all $m > 0$. □

3.20 Find $\mathbf{F} \in \Lambda^\circ$ such that for all $n \in \mathbb{N}$, $\mathbf{F}\ulcorner n \urcorner =_\beta \ulcorner 2^n \urcorner$.

Proof. $\mathbf{F} \equiv \lambda x.\mathbf{D}x\ulcorner 1 \urcorner(\mathbf{Exp}\ulcorner 2 \urcorner x)$. □

3.21 Let $f, g : \mathbb{N} \to \mathbb{N}$, $f(0) = 0$ and $f(n+1) = g(f(n))$. If $G \in \Lambda^\circ$ λ-defines g, find $F \in \Lambda^\circ$ such that F λ-defines f.

Proof. Our goal is to achieve

$$\begin{aligned}F\ulcorner n \urcorner &= \mathbf{D}\ulcorner n \urcorner \ulcorner 0 \urcorner G[F(\mathbf{pred}\ulcorner n \urcorner)]\\ &= \{\lambda n.\mathbf{D}n\ulcorner 0 \urcorner G[F(\mathbf{pred}n)]\}\ulcorner n \urcorner\\ &= \{(\lambda fn.\mathbf{D}n\ulcorner 0 \urcorner G[f(\mathbf{pred}n)])F\}\ulcorner n \urcorner.\end{aligned}$$

Therefore, $F \equiv \mathbf{Y}(\lambda xy.\mathbf{D}y\ulcorner 0 \urcorner G[x(\mathbf{pred}y)])$ λ-defines f. □

3.22 Prove that there are $\mathrm{var}, \mathrm{app}, \mathrm{abs}, \mathrm{num} : \mathbb{N} \to \mathbb{N} \in \mathcal{GRF}$ such that (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) $\forall x \in V, M \in \Lambda$, $\mathrm{abs}(\sharp x, \sharp M) = \sharp(\lambda x.M)$; (4) $\forall n \in \mathbb{N}$, $\mathrm{num}(n) = \sharp\ulcorner n \urcorner$.

Proof. (1)-(3) is trivial because $\sharp(v^{(n)}) = [0, n]$, $\sharp(MN) = [1, [\sharp M, \sharp N]]$ and $\sharp(\lambda x.M) = [2, [\sharp x, \sharp M]]$ are both elementary. Also,

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

Thus we only need to show that $\sharp(f^n x)$ is recursive by the fact that $\sharp(f^n x) = \sharp(f(f^{n-1}x)) = [1,[\sharp f,\sharp(f^{n-1}x)]$. $\square$

3.23 Prove that there exists $B \in \Lambda^\circ$ such that $F_{[\ulcorner x\urcorner \mapsto x]} =_\beta BFx\ulcorner x\urcorner$.

Proof. We first construct the minimum representation of a λ term to identify the $\equiv$ relationship of Λ° such that

$$\mathbf{min}X = \operatorname*{argmin}_{M\in\Lambda^\circ, M\equiv X} \ulcorner M\urcorner.$$

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. $\square$

3.24 Find $\mathbf{H} \in \Lambda^\circ$ such that for all $n \in \mathbb{N}$ and $x_1,\ldots,x_n \in \Lambda$, $\mathbf{H}\ulcorner n\urcorner x_1\ldots x_n =_\beta \lambda z.zx_1\ldots x_n$.

Proof. We are to find $\mathbf{H}\ulcorner n\urcorner = \lambda x_1\ldots x_n z.zx_1\ldots x_n$. We use the technique to encode $M_n \equiv \lambda x_1\ldots x_n z.zx_1\ldots x_n$ and to decode it with $\mathbf{E}$. $\sharp M_n$ is recursive because

$$\sharp M_n = [2,[\sharp x_1,\sharp(\lambda x_2\ldots x_n.zx_1\ldots x_n)]]$$

and

$$\sharp(zx_1\ldots x_n)$$

is recursive. Therefore, there is $G \in \Lambda^\circ$ λ-defines $f(n) = \sharp M_n$, thus $\mathbf{H} = \lambda x.\mathbf{E}(Gx)$ is our solution. $\square$

3.25 Prove that there is $\mathbf{H}_2 \in \Lambda^\circ$ such that for all $F \in \Lambda$, $\mathbf{H}_2 \ulcorner F \urcorner =_\beta F \ulcorner \mathbf{H}_2 \ulcorner F \urcorner \urcorner$.

Proof. I have not solved it yet. If you have any idea about this problem, please contact me. $\square$