VE203
Assignment 6

Jiang Yicheng
515370910224

November 9, 2016

Exercise 6.1

i)

We prove by induction that if $a = b^d$, $\forall k \in \mathbb{N}, n = b^k, f(n) = f(1)n^d + cn^d log_b n$

1. When $n = b^0$, $f(n) = f(1) = f(1) \cdot 1^d + c \cdot 1^d log_b 1$. So the statement holds for $k = 0$
2. Assume that for $k = m$ the statement holds, i.e. $f(b^m) = f(1)(b^m)^d + c(b^m)^d log_b b^m$ then

$$\begin{aligned} f(b^{m+1}) &= af(b^{m+1}/b) + c(b^{m+1})^d \\ &= a(f(1)(b^m)^d + c(b^m)^d log_b b^m) + c(b^{m+1})^d \\ &= af(1)(b^m)^d + c(b^{m+1})^d(\frac{a}{b^d} log_b b^m + 1) \\ &= b^d f(1)(b^m)^d + c(b^{m+1})^d(log_b b^m + log_b b) \\ &= f(1)(b^{m+1})^d + c(b^{m+1})^d log_b b^{m+1} \end{aligned}$$

   So the statement also holds when $k = m + 1$.

To sum up, if $a = b^d$ and n is a power of b, then $f(n) = f(1)n^d + cn^d log_b n$.

ii)

Choose $n = 0$, we can get that $f(0) = af(0)$. Since $a \geqslant 1$, $f(0) = 0$. Since f is an increasing function, $\forall n \geqslant 0$, $f(n) \geqslant f(0) = 0$.

If n is a power of b,

$$f(n) = f(1)n^d + cn^d log_b n \leqslant f(1)n^d log_b n + cn^d log_b n < (f(1) + 2c)b^d n^d log_b n$$

If $b^k < n < b^{k+1}$ for some $k \in \mathbb{N}$

$$\begin{aligned} f(n) &\leqslant f(b^{k+1}) = f(1)(b^{k+1})^d + c(k+1)(b^{k+1})^d \\ &< \frac{(f(1) + c)(b^{k+1})^d}{(b^k)^d} n^d log_b n + cb^d k(b^k)^d \\ &< (f(1) + c)b^d n^d log_b n + cb^d n^d log_b n \\ &< (f(1) + 2c)b^d n^d log_b n \end{aligned}$$

So $\forall n \in \mathbb{N}$, $|f(n)| = f(n) < (f(1) + 2c)b^d n^d log_b n = (f(1) + 2c)b^d |n^d log_b n|$. So $f(n) = O(n^d log_b n)$.

iii)

We prove by induction that if $a \neq b^d$, $\forall k \in \mathbb{N}, n = b^k, f(n) = \frac{b^d c}{b^d - a} n^d + (f(1) + \frac{b^d c}{a - b^d}) n^{log_b a}$

1. When $n = b^0$, $f(n) = f(1) = \frac{b^d c}{b^d - a} 1^d + (f(1) + \frac{b^d c}{a - b^d}) 1^{log_b a}$. So the statement holds for $k = 0$

2. Assume that for $k = m$ the statement holds, i.e. $f(b^m) = \frac{b^d c}{b^d - a}(b^m)^d + (f(1) + \frac{b^d c}{a - b^d})(b^m)^{log_b a}$ then

$$\begin{aligned} f(b^{m+1}) &= af(b^{m+1}/b) + c(b^{m+1})^d \\ &= a(\frac{b^d c}{b^d - a}(b^m)^d + (f(1) + \frac{b^d c}{a - b^d})(b^m)^{log_b a}) + c(b^{m+1})^d \\ &= \frac{ac}{b^d - a}(b^{m+1})^d + a(f(1) + \frac{b^d c}{a - b^d})a^m + c(b^{m+1})^d \\ &= \frac{b^d c}{b^d - a}(b^{m+1})^d + (f(1) + \frac{b^d c}{a - b^d})a^{m+1} \\ &= \frac{b^d c}{b^d - a}(b^{m+1})^d + (f(1) + \frac{b^d c}{a - b^d})(b^{m+1})^{log_b a} \end{aligned}$$

So the statement also holds when $k = m + 1$.

To sum up, if $a \neq b^d$ and n is a power of b, then $f(n) = \frac{b^d c}{b^d - a}n^d + (f(1) + \frac{b^d c}{a - b^d})n^{log_b a}$.

iv)

Since $a < b^d$, $log_b a < d$. If $b^k < n < b^{k+1}$ for some $k \in \mathbb{N}$

$$\begin{aligned} f(n) \leqslant f(b^{k+1}) &= \frac{b^d c}{b^d - a}(b^{k+1})^d + (f(1) + \frac{b^d c}{a - b^d})(b^{k+1})^{log_b a} \\ &< (\frac{b^d c}{b^d - a} + f(1))(b^{k+1})^d \\ &= (\frac{b^d c}{b^d - a} + f(1))b^d(b^k)^d \\ &< (\frac{b^d c}{b^d - a} + f(1))b^d n^d \end{aligned}$$

If n is a power of b, since $b > 1$

$$f(n) = \frac{b^d c}{b^d - a}n^d + (f(1) + \frac{b^d c}{a - b^d})n^{log_b a} < (\frac{b^d c}{b^d - a} + f(1))n^d < (\frac{b^d c}{b^d - a} + f(1))b^d n^d$$

So $\forall n \in \mathbb{N}$, $|f(n)| = f(n) < (\frac{b^d c}{b^d - a} + f(1))b^d n^d = (\frac{b^d c}{b^d - a} + f(1))b^d |n^d|$. So $f(n) = O(n^d)$.

v)

Since $a > b^d$, $log_b a > d$. If $b^k < n < b^{k+1}$ for some $k \in \mathbb{N}$

$$\begin{aligned} f(n) \leqslant f(b^{k+1}) &= \frac{b^d c}{b^d - a}(b^{k+1})^d + (f(1) + \frac{b^d c}{a - b^d})(b^{k+1})^{log_b a} \\ &< (\frac{b^d c}{a - b^d} + f(1))(b^{k+1})^{log_b a} \\ &= (\frac{b^d c}{a - b^d} + f(1))b^{log_b a}(b^k)^{log_b a} \\ &< (\frac{b^d c}{b^d - a} + f(1))an^{log_b a} \end{aligned}$$

If n is a power of b, since $a > 1$

$$f(n) = \frac{b^d c}{b^d - a}n^d + (f(1) + \frac{b^d c}{a - b^d})n^{log_b a} < (\frac{b^d c}{a - b^d} + f(1))n^{log_b a} < (\frac{b^d c}{a - b^d} + f(1))an^d log_b a$$

So $\forall n \in \mathbb{N}$, $|f(n)| = f(n) < (\frac{b^d c}{b^d - a} + f(1))an^{log_b a} = (\frac{b^d c}{a - b^d} + f(1))a|n^{log_b a}|$. So $f(n) = O(n^{log_b a})$.

Exercise 6.2

i)

We can find that if n is even, it need one more modular multiplication besides the ones needed for $n/2$; if n is odd, it need two more modular multiplication besides the ones needed for $(n-1)/2$. That is if we set the number of modular multiplications required to compute a^n mod m as $f(n)$, then $f(2n) = f(n) + 1, f(2n+1) = f(n) + 2$, so

$$f(n) = f(\frac{n}{2}) + \frac{3}{2} - \frac{1}{2} \cdot (-1)^n$$

is a divide-and-conquer recurrence relation for the number of modular multiplications required to compute a^n mod m.

ii)

For the recurrence relation $f(n) = f(\frac{n}{2}) + \frac{3}{2} - \frac{1}{2} \cdot (-1)^n$, we find that

$$a = 1, b = 2, c = \frac{3}{2} - \frac{1}{2} \cdot (-1)^n, d = 0$$

then according to Master Theorem, since $a = 1 = 2^0 = b^d$

$$f(n) = O(n^0 logn) = O(logn)$$

So the number of modular multiplications required to compute a^n mod m is $O(logn)$.

Exercise 6.3

Set the number for 01 is m and 10 is n in a bit string. We can form the bit string by inserting 1 into 0 which is a string:

At initial, $m = n = 0$

1. If we insert 1 before the first 0, then $m \leftarrow m, n \leftarrow n + 1$. This can be done only once.
2. If we insert 1 after the final 0, then $m \leftarrow m + 1, n \leftarrow n$. This can be done only once.
3. If we insert 1 between two 0s, then $m \leftarrow m + 1, n \leftarrow n + 1$.
4. If we insert 1 between 1 and 0, then $m \leftarrow m, n \leftarrow n$.
5. If we insert 1 between 0 and 1, then $m \leftarrow m, n \leftarrow n$.
6. If we insert 1 between two 1s, then $m \leftarrow m, n \leftarrow n$.

So we can see that the only way to change the difference between m and n is through 1 or 2, which can only be done once and therefore they can enlarge (do 1 or do 2 only) or reduce (did 1 before doing 2 or did 2 before doing 1) the difference between m and n by 1. And the other ways will keep the difference between m and n. Since $m = n = 0$ at initial, the maximum difference between m and n is 1. So in a bit string, the string 01 occurs at most one more time than the string 10.

Exercise 6.4

i)

For $n \in \mathbb{N}$,

1. $(p_0, q_0) = (1, 1)$
2. $(p_{n+1}, q_{n+1}) = \begin{cases} (p_n + 1, q_n - 1), q_n > 1 \\ (1, p_n + 1) \qquad\quad , q_n = 1 \end{cases}$

ii)

$\forall n \in \mathbb{N}$, we can see that

$$p_{n+1} + q_{n+1} = p_n + q_n (q_n > 1), p_{n+1} + q_{n+1} = p_n + q_n + 1 (q_n = 1)$$

and

$$(p_{n+q_n-1}, q_{n+q_n-1}) = (p_{n+q_n-2} + 1, q_{n+q_n-2} - 1) = (p_n + q_n - 1, q_n - q_n + 1) = (p_n + q_n - 1, 1)$$

so

$$(p_{n+q_n}, q_{n+q_n}) = (1, p_n + q_n)$$

then

$$(p_{n+q_n+p_n+q_n}, q_{n+q_n+p_n+q_n}) = (1, p_n + q_n + 1)$$

since $(p_0, q_0) = (1, 1)$, then $\forall k \in \mathbb{N}^*, \exists n \in \mathbb{N}, (p_n, q_n) = (1, k)$. Then $\forall (p, q) \in \mathbb{N}^* \times \mathbb{N}^*$, $\exists n \in \mathbb{N}, (p_n, q_n) = (1, p + q - 1)$. And

$$(p_{n+p-1}, q_{n+p-1}) = (p_{n+p-2} + 1, q_{n+p-2} - 1) = (p_n + p - 1, q_n - p + 1) = (p, q)$$

so $\forall (p, q) \in \mathbb{N}^* \times \mathbb{N}^*$, $\exists n \in \mathbb{N}, (p_n, q_n) = (p, q)$.

iii)

We prove by induction that $\varphi(p_n, q_n) = n$

1. When $n = 0$, $\varphi(p_1, q_1) = \dfrac{(1 + 1 - 1)(1 + 1 - 2)}{2} + 1 = 1$. So the statement holds for $k = 0$
2. Assume that for $n = k$ the statement holds, i.e. $\varphi(p_k, q_k) = k$ then
   (a) $q_k = 1$, then $(p_{k+1}, q_{k+1}) = (1, p_k + 1)$. So

$$\begin{aligned}\varphi(p_{k+1}, q_{k+1}) &= \frac{(1 + p_k + 1 - 1)(1 + p_k + 1 - 2)}{2} + 1 \\ &= \frac{(1 + p_k - 1)(1 + p_k - 2) + 2p_k}{2} + 1 \\ &= \frac{(1 + p_k - 1)(1 + p_k - 2)}{2} + p_k + 1 \\ &= k + 1\end{aligned}$$

   (b) $q_k > 1$, then $(p_{k+1}, q_{k+1}) = (p_k + 1, q_k - 1)$. So

$$\begin{aligned}\varphi(p_{k+1}, q_{k+1}) &= \frac{(p_k + 1 + q_k - 1 - 1)(p_k + 1 + q_k - 1 - 2)}{2} + p_k + 1 \\ &= \frac{(p_k + q_k - 1)(p_k + q_k - 2)}{2} + p_k + 1 \\ &= k + 1\end{aligned}$$

   So the statement also holds when $n = k + 1$.

To sum up, $\varphi(p_n, q_n) = n$.

iv)

We can see that if $(p_n, q_n) = (p_k, q_k)$, then $n = k$. And $\varphi(p_n, q_n) = n$, so φ is injective. $\forall n \in \mathbb{N}^*$, we can find that $\varphi(p_n, q_n) = n$. So φ is surjective.

So φ is bijective.

v)

Set $f(n) = (\dfrac{2n + \lfloor\sqrt{2n}\rfloor - \lfloor\sqrt{2n}\rfloor^2}{2}, \dfrac{\lfloor\sqrt{2n}\rfloor^2 + \lfloor\sqrt{2n}\rfloor - 2n + 2}{2})$.

We can see that $\frac{2n+\lfloor\sqrt{2n}\rfloor-\lfloor\sqrt{2n}\rfloor^2}{2}, \frac{\lfloor\sqrt{2n}\rfloor^2+\lfloor\sqrt{2n}\rfloor-2n+2}{2} \in \mathbb{N}^*$ since we know that $\lfloor\sqrt{2n}\rfloor > \sqrt{2n}-1$, and

$$\begin{aligned}
&\frac{(\frac{2n+\lfloor\sqrt{2n}\rfloor-\lfloor\sqrt{2n}\rfloor^2}{2}+\frac{\lfloor\sqrt{2n}\rfloor^2+\lfloor\sqrt{2n}\rfloor-2n+2}{2}-1)}{2}\\
&\cdot(\frac{2n+\lfloor\sqrt{2n}\rfloor-\lfloor\sqrt{2n}\rfloor^2}{2}+\frac{\lfloor\sqrt{2n}\rfloor^2+\lfloor\sqrt{2n}\rfloor-2n+2}{2}-2)\\
&+(\frac{2n+\lfloor\sqrt{2n}\rfloor-\lfloor\sqrt{2n}\rfloor^2}{2})\\
=&\frac{\lfloor\sqrt{2n}\rfloor(\lfloor\sqrt{2n}\rfloor-1)}{2}-(\frac{2n+\lfloor\sqrt{2n}\rfloor+\lfloor\sqrt{2n}\rfloor^2}{2})\\
=&n
\end{aligned}$$

so $\varphi(f(n))=n$. Since φ is bijective, $f(n)=\varphi^{-1}(n)$.

So $\varphi^{-1}(n)=(\frac{2n+\lfloor\sqrt{2n}\rfloor-\lfloor\sqrt{2n}\rfloor^2}{2}, \frac{\lfloor\sqrt{2n}\rfloor^2+\lfloor\sqrt{2n}\rfloor-2n+2}{2})$

vi)

$\forall p \in \mathbb{N}, q \in \mathbb{N}^*$

$$\varphi(p,q)=\begin{cases}2(q-1) & ,p=0\\ 2(\frac{(p+q-1)(p+q-2)}{2}+p)+1 & ,p>0\end{cases}$$

vii)

$\forall p \in \mathbb{Z}, q \in \mathbb{N}^*$

$$\varphi(p/q)=\begin{cases}3(q-1) & ,p=0\\ 3(\frac{(p+q-1)(p+q-2)}{2}+p)+1 & ,p>0\\ 3(\frac{(-p+q-1)(-p+q-2)}{2}-p)+2 & ,p<0\end{cases}$$

Exercise 6.5

First, we treat all sets as countably infinite and the union is infinite. Denote these sets as $A_0, A_1, A_2, \cdots$

Let a_{ij} denote the i^{th} element of A_j ($i=0,1,2\cdots$, let elements in each set be in a sequence). Then this a_{ij} is a bijective function $\mathbb{N}\times\mathbb{N}\to\bigcup_{i\in\mathbb{N}}A_i$. Also, according to Exercise 6.4 *vii*), we can find a bijective function $f:\mathbb{N}\to\mathbb{N}\times\mathbb{N}$. Then $a_{f(\cdot)}:\mathbb{N}\to\bigcup_{i\in\mathbb{N}}A_i$ is a bijective function. So $\bigcup_{i\in\mathbb{N}}A_i$ is countable.

Then if there is finite finite sets in total, we can arrange all elements at the begining of the sequence and let elements in other sets after them. And we can see this is also a bijective function from $\mathbb{N}$ to $\bigcup_{i\in\mathbb{N}}A_i$. So $\bigcup_{i\in\mathbb{N}}A_i$ is countable.

If there is infinite finite sets $B_0^{i_0}, B_1,^{i_1}, \cdots$ where i_k is the number of elements in set B_k. Then we can arrange all elements in a sequence as the $x^{th}(x = 1, 2 \cdots, i_y)$ element in B_y at $\big(\sum_{j=0}^{y-1} i_j + x\big)^{th}$ in the new sequences. And we can see this is also a bijective function from $\mathbb{N}$ to $\bigcup_{i\in\mathbb{N}} B_i$. So $C_0 = \bigcup_{i\in\mathbb{N}} B_i$ is countable. Then denote other finite sets as $C_1, C_2, \cdots$. If there are infinite sets C, then we can conclude that $\bigcup_{i\in\mathbb{N}} A_i = \bigcup_{i\in\mathbb{N}} C_i$ is countable. If there are finite sets C, set the number is l. Then denote i^{th} element of C_j $(i = 0, 1, 2 \cdots, j = 0, 1, \cdots, l-1)$ as a_{li+j}. This is a bijective function from $\mathbb{N}$ to $\bigcup_{i\in\mathbb{N}} C_i$. So we can conclude that $\bigcup_{i\in\mathbb{N}} A_i = \bigcup_{i\in\mathbb{N}} C_i$ is countable.

To sum up, countable union of countable sets is countable.

Exercise 6.6

Since card$M$=card$N$ and M,N are finite sets, then M and N has the same number of elements in them.

Assume that $M \neq N$, then since $M \subset N$, there exists some $x \in N$ such that $x \notin M$, and $\forall y \in M, y \in N$. So there is at least one more element in N than in M. This leads to contradiction.

So $M = N$.

Exercise 6.7

Assume that f is injective.

Since M, N are finite sets, according to Pigeonhole Principle, f is also surjective. Then there exists a bijective function $f : M \to N$. So card$M$=card$N$. This leads to contradiction. So our assumption is wrong.

So f is not injective.