Ve203 Discrete Mathematics (Fall 2016)

Assigment 6: Recurrence and Combinatrics

Date Due: 4:00 PM, Thursday, the 10^{th} of Noevmber 2016

JOINT INSTITUTE
交大密西根学院

This assignment has a total of **(27 Marks)**.

Exercise 6.1
In this question, assume that f is an increasing function satisfying the recurrence relation $f(n) = af(n/b) + cn^d$ with $a \geq 1$, $b \in \mathbb{N} \setminus \{0, 1\}$, $c, d \in \mathbb{R}_+$. Our goal is to prove the Master Theorem 2.3.19 of the lecture.

i) Show that if $a = b^d$ and n is a power of b, then $f(n) = f(1)n^d + cn^d \log_b n$.
(2 Marks)

ii) Show that if $a = b^d$, then $f(n) = O(n^d \log n)$.
(1 Mark)

iii) Show that if $a \neq b^d$ and n is a power of b, then

$$f(n) = C_1 n^d + C_2 n^{\log_b a}, \qquad C_1 = \frac{b^d c}{b^d - a}, \qquad C_2 = f(1) + \frac{b^d c}{a - b^d}.$$

(2 Marks)

iv) Show that if $a < b^d$, then $f(n) = O(n^d)$.
(1 Mark)

v) Show that if $a > b^d$, then $f(n) = O(n^{\log_b a})$.
(1 Mark)

Exercise 6.2
A recursive algorithm for modular exponentiation is given in Example 3 of Section 4.4, page 312 of the textbook.

i) Set up a divide-and-conquer recurrence relation for the number of modular multiplications required to compute $a^n \bmod m$, where $a, m, n \in \mathbb{Z}_+$.
(2 Marks)

ii) Construct a big-O estimate for the number of modular multiplications required to compute $a^n \bmod m$.
(1 Mark)

Exercise 6.3
Prove that in a bit string, the string 01 occurs at most one more time than the string 10.
(2 Marks)

Exercise 6.4
Consider the scheme for counting fractions shown below and let

$$\varphi\colon \mathbb{N}^* \times \mathbb{N}^* \to \mathbb{N}^*, \qquad \varphi(p, q) = \frac{(p + q - 1)(p + q - 2)}{2} + p,$$

where $N^* = \mathbb{N} \setminus \{0\}$. The goal of this question is to prove that, in the scheme shown, traversing successive diagonals from top to bottom, the fraction p/q is indeed the $\varphi(p, q)$th fraction encountered and that φ gives a bijection $N^* \times \mathbb{N}^* \to \mathbb{N}^*$.

i) Write the traversal of the fractions as a recursively defined sequence of pairs (p_n, q_n).

(1 Mark)

ii) Prove that for any $(p, q) \in \mathbb{N}^* \times \mathbb{N}^*$ there exists an $n \in \mathbb{N}$ such that $(p, q) = (p_n, q_n)$.

(2 Marks)

iii) Prove (by induction in n) that $\varphi(p_n, q_n) = n$.

(2 Marks)

iv) Deduce that φ is bijective.

(0.5 Marks)

v) Find the inverse of φ.

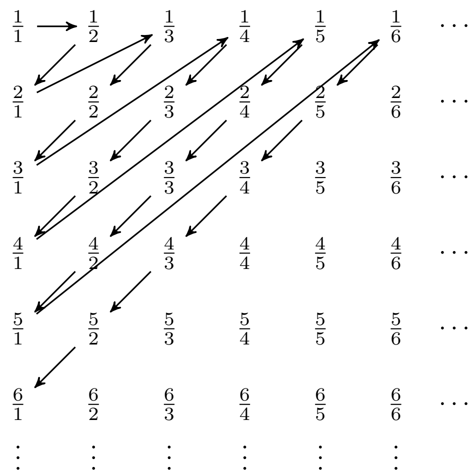
(2 Marks)

vi) How can φ be modified to give a bijective map $\mathbb{N} \times \mathbb{N}^* \to \mathbb{N}$?

(1 Mark)

vii) How can φ be modified to give a bijective map $\mathbb{Z} \times \mathbb{N}^* \to \mathbb{N}$?

(0.5 Marks)



Exercise 6.5

Show that the countable union of countable sets is countable, i.e., if $\{A_i\}_{i=0}^{\infty}$ is an infinite family of sets, each of which is countable, then $\bigcup_{i\in\mathbb{N}} A_i$ is countable. *Hint:* Let a_{ij} denote the ith element of A_j...

(2 Marks)

Exercise 6.6

Let M, N be finite sets with $\operatorname{card} M = \operatorname{card} N$ and $M \subset N$. Prove that $M = N$.

(2 Marks)

Exercise 6.7

Use the Pigeonhole Principle or Theorem 2.4.21 of the lecture to prove the following theorem:

> Let M, N be finite sets with $\operatorname{card} M > \operatorname{card} N$ and $f\colon M \to N$. Then f is not injective.

(2 Marks)