Ve203 Discrete Mathematics (Fall 2020)

Assignment 7: Counting, Probability and Monte Carlo Algorithms

Date Due: 12:10 PM, Thursday, the 5th of November 2020

JOINT INSTITUTE
交大密西根学院

This assignment has a total of **(31 Marks)**.

Exercise 7.1

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

Exercise 7.2

Use the Pigeonhole Principle or Theorem 15.21 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)

Exercise 7.3

In this question, $R(m, n)$ denotes the Ramsey number and we assume that in a group of people, any two people are either friends or enemies.

i) Show that in a group of five people there are not necessarily either three mutual enemies or three mutual friends. Hence, $R(3, 3) > 5$.
(2 Marks)

ii) Show that in a group of 10 people there are either three mutual friends or four mutual enemies, and there are either three mutual enemies or four mutual friends. This implies $R(4, 3) \leq 10$.
(2 Marks)

iii) Use ii) to show that among any group of 20 people there are either four mutual friends or four mutual enemies. (Actually, $R(4, 4) = 18$, so this result is not optimal.)[1]
(2 Marks)

iv) Show that $R(2, n) = n$ for $n \in \mathbb{N}$, $n \geq 2$.
(1 Mark)

v) Show that $R(m, n) \leq R(m-1, n) + R(m, n-1)$. Hence $R(4, 3) \leq 10$.
(2 Marks)

vi) Prove that $R(4, 3) \leq 9$ as follows: In a party of size 9, every person has at least four enemies or at least four friends (by the generalized pigeonhole principle). Consider first the case where there is one person with four friends and then the case where no one has four friends, i.e., everyone has five or more enemies.
(2 Marks)

vii) Show that $R(4, 3) > 8$ by giving a suitable example of an 8-member party. Conclude $R(4, 3) = 9$.
(2 Marks)

[1] From http://www.cut-the-knot.org/arithmetic/combinatorics/Ramsey44.shtml: Noga Alon and Michael Krivelevich [The Princeton Companion to Mathematics, p. 562] present a story of the Ramsey number $R(4, 4)$:

> "In the course of an examination of friendship between children some fifty years ago, the Hungarian sociologist Sandor Szalai observed that among any group of about twenty children he checked he could always find four children any two of whom were friends, or else four children no two of whom were friends. Despite the temptation to try to draw sociological conclusions, Szalai realized that this might well be a mathematical phenomenon rather than a sociological one. Indeed, a brief discussion with the mathematicians Erdös, Turán, and Sós convinced him this was the case."

Exercise 7.4
At a given party of at least two people, any two participants are either mutual friends or not. Show that there are two people at such a party that have the same number of friends.
(2 Marks)

Exercise 7.5
Show that if $k, n \in \mathbb{N}$ with $1 \leq k \leq n$, then

$$\binom{n}{k} \leq \frac{n^k}{2^{k-1}}$$

(2 Marks)

Exercise 7.6
Show that if A and B are events and P is a probability function, then $P[A \cap B] \geq P[A] + P[B] - 1$. This is known as *Bonferroni's inequality.*
(2 Marks)

Exercise 7.7
Devise a Monte Carlo algorithm that determines whether a permutation of the integers 1 through n has already been sorted (that is, in increasing order), or, instead, is a random permutation. A step of the algorithm should answer "true" if it determines the list is not sorted and "unknown" otherwise. After k steps the algorithm decides that the numbers are sorted if the answer is "unknown" in each step. Estimate the probability that the algorithm produces an incorrect answer as a function of k and n.

Hint: For each step, whether two randomly selected elements are in the correct order. Make sure these tests are independent!
(4 Marks)

Exercise 7.8
Let $n \in \mathbb{N} \setminus \{0\}$ such that $n - 1 = 2^s t$ for $s \in \mathbb{N}$ and $t = 2k + 1$ for some $k \in \mathbb{N}$. We say that n passes Miller's test for the base b if either $b^t \equiv 1 \mod n$ or $b^{2^j t} \equiv -1 \mod n$ for some j with $o \leq j \leq s - 1$. It can be shown that a composite integer passes Miller's test for fewer than $n/4$ bases b with $1 < b < n$. A composite integer that passes Miller's test to the base b is called a *strong pseudoprime to the base b*

i) Show that if n is prime and $b \in \mathbb{N} \setminus \{0\}$ with $b \nmid n$, then n passes Miller's test for the base b.
(3 Marks)

ii) Show that 2047 passes Miller's test to the base 2, but that it is composite.
(1 Mark)