FAST National University of Computer and Emerging Sciences, Karachi.

Discrete Structures (CS 211)

Assignment 2, Fall 2018

Time Allowed: 10 Days (Due Date: 13 Dec, 2018) Total Points: 57

Instructors: Dr. Nouman M Durrani Dated: 26 December, 2016

Note: 1. Answer all the questions and its subsequent parts in the given order. If your solution is not a planner graph, all marks of the planner graphs will be deducted.
2. Show proper and neat working. One point means everything related to the solution.

Propositional Logic and Rules of Inference [2+2+4 points]

Q. 1 (i) [Solve here] Express these system specifications using the propositions *p* "The message is scanned for viruses" and *q* "The message was sent from an unknown system" together with logical connectives (including negations).

a) "The message is scanned for viruses whenever the message was sent from an unknown system."

____

b) "The message was sent from an unknown system but it was not scanned for viruses."

____

c) "It is necessary to scan the message for viruses whenever it was sent from an unknown system."

____

d) "When a message is not sent from an unknown system it is not scanned for viruses."

____

(ii) Are the following statements logically equivalent? If yes, show the proof. If no, provide a counterexample. DO NOT use truth table.

a) $\neg(p \leftrightarrow q)$ and $p \leftrightarrow \neg q$

b) $(p \wedge q) \rightarrow r$ and $(p \rightarrow r) \wedge (q \rightarrow r)$

(iii) For each of these collections of premises, what relevant conclusion or conclusions can be drawn? Explain the rules of inference used to obtain each conclusion from the premises.

a) "If I take the day off, it either rains or snows." "I took Tuesday off or I took Thursday off." "It was sunny on Tuesday." "It did not snow on Thursday."

b) "The file is either a binary file or a text file. If it is a binary file, then my program won't accept it. My program will accept the file. Therefore, the file is a text file."

c) "Marry, a student in this class, knows how to write programs in JAVA. Everyone who knows how to write programs in JAVA can get a high-paying job. Therefore, someone in this class can get a high-paying job."

d) Show that the argument form with premises $(p \wedge t) \rightarrow (r \vee s)$, $q \rightarrow (u \wedge t)$, $u \rightarrow p$, and $\neg s$ and conclusion $q \rightarrow r$ is valid

Sets and Functions [2+1+1 points]

Q. No 2 Solve the following:

(i) Let *A* and *B* be sets. Using Set Builder form, show that

a) $(A \cap B) \subseteq A$.

b) $A \cap (B - A) = \emptyset$.

(ii) Determine whether the function is *onto* and whether it is *one-to-one*:

$f : R \rightarrow R$, $f(n) = n^2 + 1$ from **Z** to **Z**.

(iii) Show that the function $f(x) = |x|$ from the set of real numbers to the set of nonnegative real numbers is not invertible, but if the domain is restricted to the set of nonnegative real numbers, the resulting function is invertible.

Theorem Proofs: [1 x 6 points]

Q No. 3 Prove the following theorems:

(i) Let $n \in Z^+$, with $n \geq 2$. If the sum of the divisors of n is equal to n+1, then n is prime.

(ii) Prove that $\sqrt{2}$ is irrational by giving a proof by contradiction.

(iii) If n is an integer and 3n + 2 is odd, then n is odd.

(iv) Prove using cases: Every multiple of 4 equals $1+ (-1)^n (2n -1)$ for some $n \in N$.

(v) A finite set, S, has $2^{|S|}$ distinct subsets.

(vi) Let a, b, c be integers, where $a \neq 0$. If a\b and a\c, then a \ (b + c).

Number Theory [4+1+1+1 points]

Q No. 4 (i) Jessica breeds rabbits. She's not sure exactly how many she has today, but as she was moving them about this morning, she noticed some things. When she fed them, in groups of 27, she had 1 left over. When she bathed them, in groups of 12, she had a group of 4 left over. She took them outside to romp in groups of 15, but then the last group consisted of only 7. She's positive that there are fewer than 2700 rabbits - but how many does she have?

In this problem, you are supposed to state and use of the following Theorems:

a. Chinese Remainder Theorem
b. The Euclidean Algorithm Lemma
c. Bézout's Theorem
d. Linear congruences

(ii) State the Fermat's little theorem and use it to evaluate 9^{2527} mod 79. [Hint: Modular Exponentiation to solve high order exponents in the given case]

(iii) Suppose that (n, e) is an RSA encryption key, with $n = p \cdot q$ where p and q are large primes and $\gcd(e, (p - 1)(q - 1)) = 1$. Furthermore, suppose that d is an inverse of e modulo $(p - 1)(q - 1)$. Suppose that $C \equiv M^e \pmod{pq}$. The congruence $C^d \equiv M \pmod{pq}$ holds when $\gcd(M, pq) = 1$. Show that this decryption congruence also holds when $\gcd(M, pq) > 1$. [Hint: Use congruences modulo p and modulo q and apply the Chinese remainder theorem.]

(iv) What is the original message encrypted using the RSA system with $n = 43 \cdot 59$ and $e = 13$ if the encrypted message is 0667? [Hint: You could also use Modular Exponentiation to solve high order exponents in the given case]

Combinatorics and Discrete Probability [Solve here] [1 x 13 points]

Q No 5 Solve all the questions in the space provided below.

(i) Every student in a discrete mathematics class is either a computer science or a mathematics major or is a joint major in these two subjects. How many students are in the class if there are 38 computer science majors (including joint majors), 23 mathematics majors (including joint majors), and 7 joint majors?

(ii) The name of a variable in the JAVA programming language is a string of length between 1 and 65,535 characters, inclusive, where each character can be an uppercase or a lowercase letter, a dollar sign, an underscore, or a digit, except that the first character must not be a digit. Determine the number of different variable names in JAVA.

(iii) A wired equivalent privacy (WEP) key for a wireless fidelity (WiFi) network is a string of either 8, 12, or 16 hexadecimal digits. How many different WEP keys are there?

(iv) A professor writes 50 discrete mathematics true/false questions. Of the statements in these questions, 23 are true. If the questions can be positioned in any order, how many different answer keys are possible?

(v) A multiple-choice test contains 50 questions. There are four possible answers for each question.

a) In how many ways can a student answer the questions on the test if the student answers every question?

b) In how many ways can a student answer the questions on the test if the student can leave answers blank?

(vi) Suppose that every student in a discrete mathematics class of 25 students is a freshman, a sophomore, or a junior.

a) Show that there are at least nine freshmen, at least nine sophomores or at least nine juniors in the class.

b) Show that there are either at least three freshmen, at least 19 sophomores, or at least five juniors in the class.

(vii) Seven women and nine men are on the faculty in the mathematics department at a school.

a) How many ways are there to select a committee of five members of the department if at least one woman must be on the committee?

b) How many ways are there to select a committee of five members of the department if at least one woman and at least one man must be on the committee?

(viii) A coin is flipped eight times where each flip comes up either heads or tails. How many possible outcomes:

a) are there in total?

b) contain exactly three heads?

c) contain at least three heads?

d) contain the same number of heads and tails?

(ix) There are 10 questions on a discrete mathematics final exam. How many ways are there to assign scores to the problems if the sum of the scores is 100 and each question is worth at least 5 points?

(x) Use Stirling approximation to calculate lower and upper bound of 20!. [Hint: $n! \sim \sqrt{2\pi n}(n/e)^n$]

(ix) What is the probability that a card selected at random from a standard deck of 52 cards is an ace or a heart?

(x) A fair coin is flipped three times. Are the events A="the first coin toss came up heads" and B="an even number of coin tosses came up head", independent?

(xi) The final exam of a discrete structures course consists of 50 true/false questions, each worth two points, and 25 multiple-choice questions, each worth four points. The probability that Hareesh answers a true/false question correctly is 0.9, and the probability that she answers a multiple-choice question correctly is 0.8. What is her expected score on the final?

(xii) A biased coin is tossed 6 times. The probability of heads on any toss is 0.3. Let X denote the number of heads that come up. Calculate P(X= 2).

(xiii) A wedding party of eight people is lined up in a random order.
(a) What is the probability that the bride is next to the groom?
(b) What is the probability that maid of honor is in the leftmost position?
(c) Determine whether the two events are independent. Give your reasoning.

Partial Relations: [1+1+1 points]

Q. No. 6 Solve all the questions from this section.

(i) Let R be the relation on the set {0,1,2,3} containing the ordered pairs (1,1), (1,0), (1,2), (2,1), (2,2), (3,0).
Check if the above relation R is a partial order? Also, find the:
a) reflexive closure of R
b) antisymmetric closure of R and
c) transitive closure of R

(ii) Construct the Hasse diagram for ({ 1,2,3,4,6,8,12}, |) }

(iii) List all the permutations of {1,2,3} in lexicographic order.

Graph Theory [Solve here] [1 x 16 points]

Q. No. 7 Answer all the questions, in the space provided below:

(i) What kind of graph can be used to model a highway system between major cities where
a) there is an edge between the vertices representing cities if there is an interstate highway between them?

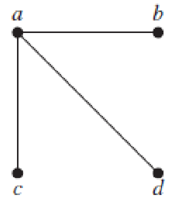
b) there is an edge between the vertices representing cities for each interstate highway between them, and there is a loop at the vertex representing a city if there is an interstate highway that circles this city?

(ii) The **intersection graph** of a collection of sets $A1, A2, \ldots, An$ is the graph that has a vertex for each of these sets and has an edge connecting the vertices representing two sets if these sets have a nonempty intersection. Construct the intersection graph of these collections of sets.
$A1 = \{0, 2, 4, 6, 8\}$, $A2 = \{0, 1, 2, 3, 4\}$,
$A3 = \{1, 3, 5, 7, 9\}$, $A4 = \{5, 6, 7, 8, 9\}$,
$A5 = \{0, 1, 8, 9\}$

(iii) How can a graph that models e-mail messages sent in a network be used to find people who have recently changed their primary e-mail address?

(iv) How many edges does a graph have if its degree sequence is 5, 2, 2, 2, 2, 1? Draw such a graph.

(v) Draw all subgraphs of this graph.



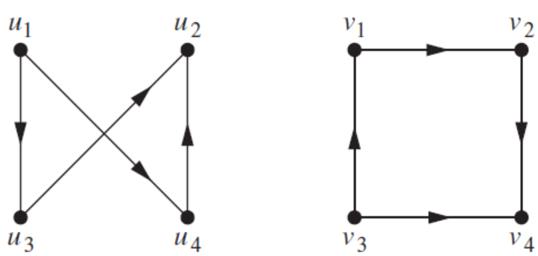
(vi) How many vertices does a regular graph of degree four with 10 edges have?

(vii) Describe an algorithm to decide whether a graph is bipartite based on the fact that a graph is bipartite if and only if it is possible to color its vertices with two different colors so that no two vertices of the same color are adjacent.

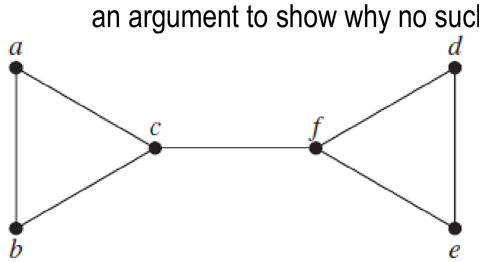
(viii) Are the simple graphs with the following adjacency matrices isomorphic?

$$\begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

(ix) Determine whether the given pair of directed graphs are isomorphic.

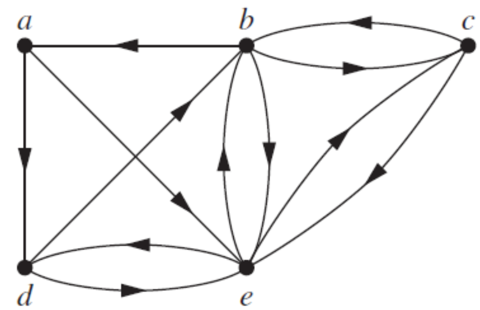


(x) Does the graph in the below figure have a Hamilton path? If so, find such a path. If it does not, give an argument to show why no such path exists.

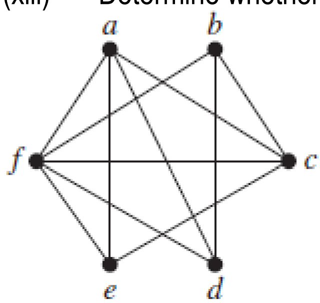


(xi) Suppose that a connected planar graph has eight vertices, each of degree three. Into how many regions is the plane divided by a planar representation of this graph?

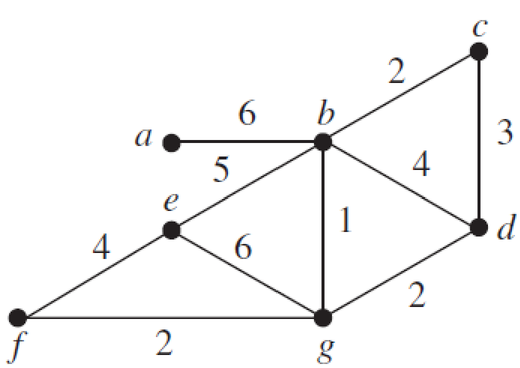
(xii) Determine whether the given graph has an Euler circuit. Construct such a circuit when one exists. If no Euler circuit exists, determine whether the graph has an Euler path and construct such a path if one exists.



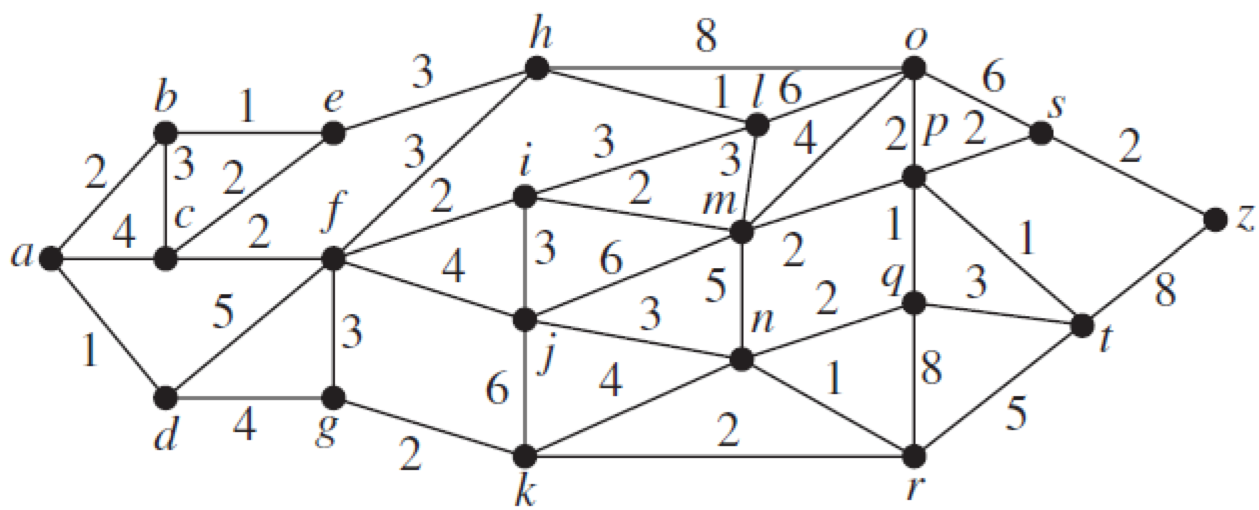
(xiii) Determine whether the given graph is planar. If so, draw it so that no edges cross.



(xiv) Find a minimum spanning tree of each of these graphs where the degree of each vertex in the spanning tree does not exceed 2.



(xv) Find the length of a shortest path between a and z in the given weighted graph. Use Dijkstra's Algorithm.



(xvi) Find the chromatic number of the given graphs. [Properly color the following graph]