

Discrete mathematics final exam

Time: 2 hours

Section A

Instructions:

- (i) Attempt all Questions in this section.
- (ii) Read Questions keenly before selecting the appropriate option(s).
- (iii) The items carry different weight/marks.

- 1) Which of the following statements is incorrect? (1 mk)
 - a) A transposition is of length of 2.
 - b) Permutation is an arrangement of objects.
 - c) Permutation function is a bijection of a set onto itself.
 - d) Transposition ciphers are block ciphers.
 - e) Permutations form symmetric groups.
- 2) Which statement is correct? (1 mk)
 - a) The composite of two identities permutations is not necessarily an identity.
 - b) The identity permutation fixes all elements.
 - c) It is possible to tell the cardinality of a set given its permutation function.
 - d) Given a permutation of length n , then its set is of cardinality n .
 - e) A cryptosystem is a 4-tuples.
- 3) Which statement is incorrect? (1 mk)
 - a) A graph consists of a set V whose elements are called vertices and a set E whose elements are called edges.
 - b) A complete graph is a directed graph.
 - c) A directed graph consists of a set V of vertices and a set E of ordered pairs of vertices called edges.
 - d) A graph G is strongly connected if for any pair of vertices u and v in G , there is a path from u to v and a path from v to u .
 - e) A tree is a connected cycle-free graph.
- 4) Which one of the following statements is false? (1 mk)
 - a) A spanning tree is a subgraph H of a graph G .
 - b) A spanning tree is a tree that contains all the vertices of G .
 - c) A spanning tree is unique.
 - d) If a graph G has a spanning tree T , then there is a path between any pair of vertices in G along the tree T .
 - e) Breadth-first search an algorithm relevant for finding a spanning tree T of a graph G .

- 5) Which statement is incorrect? (1 mk)
- The gcd of two numbers a and b can be expressed as a linear combination of a and b .
 - Caesar cipher with a key 5 is a shift cipher.
 - Linear congruence can be used to determine an error the parity check digit.
 - Arithmetic modular cannot slow operations involving large digits.
 - An axiom is a proposition that is assumed to be true.
- 6) Negate the statement; *All students do not take coffee.* (do not use the statement, it is not the case...or it is not true....) (1 mk)
- 7) Determine the check digit for the ISBN – 13 digit 978-8-120-31502 (2 mks)
- 8) Outline an area where each of the following concepts can be applied in technology, graph theory, permutation functions, logic. (3 mks)
- 9) Explain a cryptosystem (2 mks)
- 10) Explain rule of inference and give an example. (2 mks)
- 11) State without proof the De Morgan's laws of logic (2 mks)
- 12) Explain a mathematical proof (1 mk)
- 13) Use the Euclidean algorithm to show that the gcd (846 , 264) satisfy the Bezout's theorem. (4 mks)
- 14) Explain a major weakness of shift cipher and explain how affine cipher address this. (2 mks)
- 15) Define the following terms and illustrate each with a relevant example: a proposition, a theorem, and an axiom (6 mks)

Section B

Instructions

Attempt Question 1 (compulsory) and any other question.

Question 1 (Compulsory – 20 marks)

- a) Consider the following permutation functions: $p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}; p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$
hence evaluate; $p_2^{-1} \circ p_2 \circ p_1^{-1}$ (2 marks)
- b) Consider the statement; *If I do not read then I will not go home.* Write down its converse and design a logic gate for the negation of the converse. (3 marks)
(Use p : I will not read; q : I will not go home)
- c) Let set $A = \{1,2,3,4\}$ with relation $R = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,3), (3,4), (2,4), (4,1), (4,4)\}$. Hence.
- Write M_R (1 mark)
 - Construct the diagraph for the relation (1 mark)

- d) Show whether the following is a rule of inference. (2 marks)

$$\frac{\neg q}{p \rightarrow q} \therefore \neg p$$
- e) Determine the inverse of 17 (mod 31) using the Euclidean algorithm method (show working). (4 marks)
- f) Solve the following linear congruence (show working); (4 marks)

$$13x \equiv 7 \pmod{33}$$
- 1) Show that if n is a positive integer then $(n^3 + n)$ is even (3 marks)

Question 2 (10 marks) – Optional

- a) Use logic connectives to write the following statements.
- (i) It is not the case that for every student x there exists a student y such that student x works smarter than y. (1 mark)
- (ii) Some students are illogical or not all phones are smartphone. (1 mark)
- b) Consider the argument.
- If 11 is less than 6, then 11 is not a prime number
11 is not less than 6
 \therefore 11 is a prime number
- Let p: 11 is less than 6, and q: 11 is a prime number. Hence.
- (i) Write the following argument using logic connectives. (2 marks)
- (ii) Determine the validity of the argument. (3 marks)
- c) Evaluate; $(12345) \circ (5634)(27) \circ (4652317)$ and determine the number and length of the cycles of the solution. (3 marks)

Question 3 (10 marks) – Optional

- a) Using the transposition cipher based on the permutation of the set {1,2,3,4,5} with $p(1) = 5, p(2) = 3, p(3) = 4, p(4) = 1, p(5) = 2$, to.
- i) Encrypt the plaintext; THE DUST STORM AND A FOOL (2 marks)
- ii) Decrypt the ciphertext; NEJEM DTYEOLISHFRSSAAYMDOEEHRT (2 marks)
- b) Use Fermat's Little theorem to simplify; (3 marks)

$$7^{65} \pmod{19}$$
- c) Prove by mathematical induction that for all positive integers n (3 marks)

$$3 + 11 + \dots + (8n - 5) = 4n^2 - n$$

'And now, Lord, what wait I for? My hope is in thee.'
Psalms 39:7 (RSV)