 Ref. No. : Ex/CSE/PC/B/T/325/2023

B.E. COMPUTER SCIENCE AND ENGINEERING THIRD YEAR SECOND SEMESTER - 2023
Subject: DESIGN AND ANALYSIS OF ALGORITHMS

Time: 3 hours Full Marks: 100

Answer Question No. 1 **(compulsory)** and question no. **2 or 3** from Group A and question no. **4 or 5** from Group B and question no. **6 or 7** from Group C

1. a) $O(n^2) = O(n^3) = O(n^{10})$. Is this a correct? Justify.

b) Write the outline of the faster algorithm for computing the nth Fibonacci number in time $O(\log n)$.

c) Write the time complexity of Dijktra's shortest path finding algorithm with priority queue implementation for the following two situations : i) when the input graph is densely connected, ii) When the input graph is loosely connected. Give reasons in support of your answers.

d) Differentiate between Dynamic Programming and "Divide and Conquer" approach.

e) If X is NP-complete and X is solvable in polynomial time complexity, P=NP. Is this statement true? Justify with example.

5 x 5 = 25 marks

Group A

(Answer question no. 2 or 3 from this group)

2.a) Write the efficient algorithm for matrix multiplication which is faster than the standard matrix multiplication algorithm. Does this algorithm follow the basic characteristics of the Divide and Conquer Approach?-Explain. Compute the asymptotic order of the worst case running time for this algorithm.

b) Solve the following recurrence: $T(n) = 2T(\sqrt{n}) + 1$, T(1)= 1.

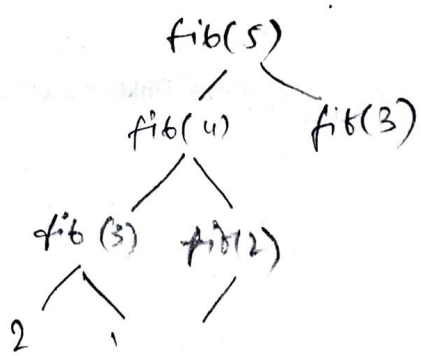
c) Explain the basic steps of a greedy algorithm used for solve optimization problems? What are the advantages and disadvantages of greedy algorithms..

(5+5+5)+5+5 = 25 marks

3. a) . Use Master theorem to find the value of the following recurrence:

$$T(n) = 5T(n/5) + O(\sqrt{n}),\ T(1) = 1,\ T(0) = 0$$

b) If $f(n) = n^3/2$ and $g(n) = 37n^2 + 120n + 17$, using the limit method , show that $g(n) \in O(f(n))$, but $f(n) \notin O(g(n))$



c) For some divide and conquer algorithms, the combination step is costlier than the division step and, for some divide and conquer algorithms, the division step is costlier than the combination step- Justify this statement with examples.

d) Represent the time complexity of the Mergesort algorithm using a recurrence equation. Solve this recurrence equation using recursion tree.

e) Explain with a suitable example how memoization can help in improving running time of a dynamic programming algorithm.

5 x 5 = 25 marks

Group B

(Answer question no. 4 or 5 from this group)

4. a) Compute the time complexity of the brute force method for finding the minimum spanning tree from a connected, weighted and undirected graph?

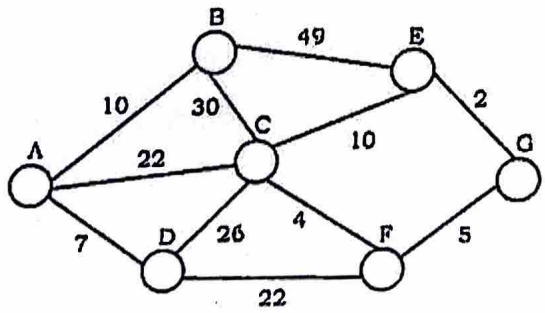
b) Write Prim's algorithm with priority queue implementation and compute time complexity of this algorithm.

c) Write an MST-based data clustering algorithm and give its time complexity analysis.

5+10+10=25 marks

5. a) Compute time complexity for the brute force method for finding the shortest path in a directed graph which is connected , and weighted. What is the input size for the Dijktra's shortest path finding algorithm?

b) Consider that the nodes of the following graph are the data points and the edge weights are the Euclidean distances between the corresponding data points. Do the necessary transformations to the edge weights and apply the MST-based clustering algorithm for finding 3 clusters. Use prim's algorithm for finding minimum spanning tree(MST) .



Prims

c) Under what situations, Dijktra's shortest path finding algorithm may fail? Justify your answer with an example.

5+ 15+ 5=25 marks

Group C

(Answer question no. 6 or 7 from this group)

6. a) Use the dynamic programming approach and develop an algorithm for the coin changing problem. Compute the time complexity of this algorithm. Is it a polynomial time algorithm?- Explain.

b) Let S be an NP-complete problem and Q and R be two other problems not known to be in NP. Q is polynomial time reducible to S and S is polynomial-time reducible to R. Which one of the following statements is true? Give reasons in support of your correct answer. Explain also why other options are incorrect.

i. R is NP-complete
ii. R is NP-hard
iii. Q is NP-complete
iv. Q is NP-hard.

c) What is halting problem? Does it belong to the class NP?-Explain.

d) State Cook's theorem.

(5+5) + 5+5+5=25 marks

7. a) Derive a dynamic programming algorithm for finding the minimum edit distance between two strings. Using this algorithm, find the minimum distance between two strings, "MEAN" and "NAME". Show how many insertions, deletions and substitution operations are performed to convert MEAN" to "NAME".

b) What does NP stands for? Does *Boolean Satisfiability Problem* (SAT) belong to the class NP?- explain.

c) Explain how reduction can be used in proving that an new search problem is NP complete.

d) Does the minimum spanning tree finding problem belong to the class P? - Give reasons.

10 + 5 +5+5 = 25 marks

non-

Ref. No.: Ex/CSE/PC/B/T/325/2023(S)

B.E. COMPUTER SCIENCE AND ENGINEERING THIRD YEAR SECOND SEMESTER SUPPLEMENTARY EXAM 2023

Subject-Design and Analysis of Algorithms

Time: **3 hours** Full Marks: **100**

*Answer Question No. 1(**compulsory**) and question no. (**2 or 3**) and question no.(**4 or 5**) and question no. (**6 or 7**) and question no.(**8 or 9**)*

1. State whether the following statements is TRUE or FALSE with proper justifications.
   a) $O(n/100) = O(n) = O(n^2)$
   b) An algorithm with time complexity of $O(n!)$ is better than the algorithm with time complexity of $O(2^n)$
   c) The combination step of Divide and Conquer Algorithm for a problem should take running time of $O(n^k)$, where k is a constant
   d) Greedy algorithm can always give the correct solution to a problem.
   e) In Dynamic programming approach, a problem is solved by solving a collection of overlapping sub-problems.
   f) If a problem is in NP, it may not be NP-hard.
   g) Prim's algorithm is a greedy algorithm
   h) Master Theorem can be applied to solving recurrence equation for the running time of any recursive algorithm.
   i) For any connected undirected weighted graph G=(V,E), the Prim's algorithm always finds minimum spanning tree .
   j) Dijktra's algorithm can only find the shortest path from source node to the farthest node from the source. **4 x 10 = 40 marks**

Group A

2. a)Suppose you are choosing between the following two algorithms
   I) Algorithm A solves problems of size *n* by recursively solving two sub-problems of size *n-1* and then combining the solutions in constant time
   II) Algorithm B solves problem of size *n* by dividing them into nine sub-problems of size n/3, recursively solving each sub-problem , and then combining the solutions in $O(n^2)$ time

   Compute the running time for the algorithms A & B. Then show which one is better in terms of running time.

   b) State Master Theorem. Can we solve the following recurrence equation using Master Theorem ?-explain. $T(n) = 2T(\sqrt{n}) + 1$, T(1)= 1. Solve this recurrence equation

   c) If $f(n) = n^3/2$, and $g(n) = 37n^2 + 120n + 17$, using the limit method , show that $g(n) \in O(f(n))$, but $f(n) \notin O(g(n))$ 5+5+5=15 marks

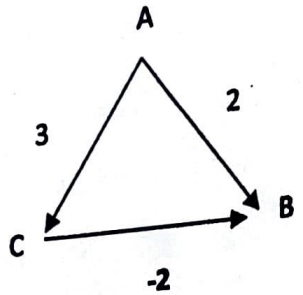
[Turn over

OR

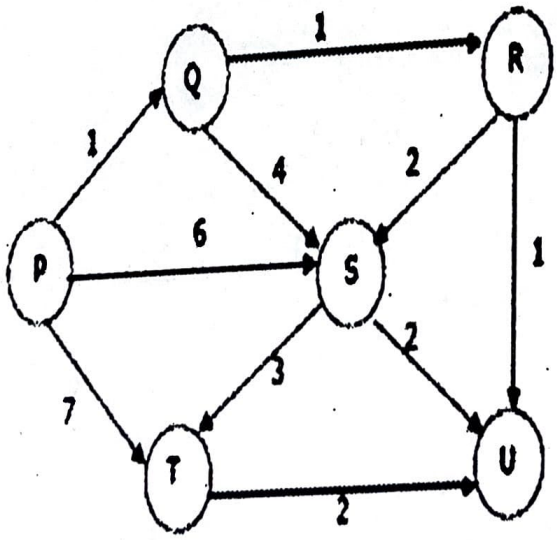
3. Write the school level algorithm for multiplying two large n-digit numbers. Compute its time complexity. Write an efficient Divide and Conquer algorithm for multiplying two large n-digit numbers. Compute its time complexity. 5 + 10 =15 marks

Group B

4. a) Consider the following directed graph and source node A, and explain whether Dijkstra's algorithm will give the correct solution or not.



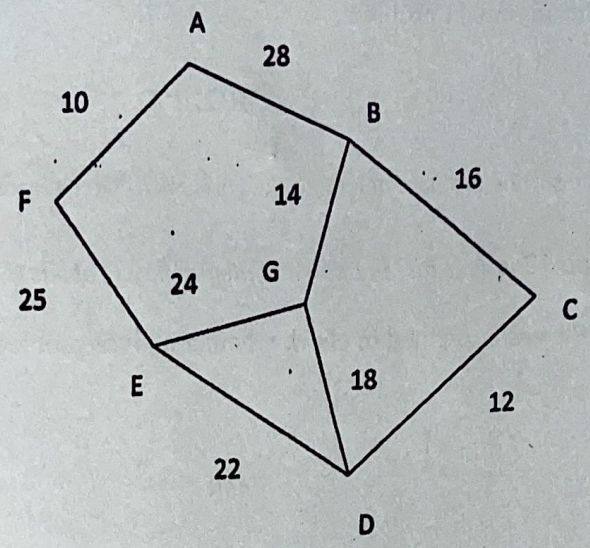
b) Consider the directed graph given below and use Dijkstra's single source shortest-path algorithm on this graph starting with **node p** (show step by step progress of the algorithm with the updates in the priority queue and node values).



5+10=15 marks

OR

5. Considering A as the source node , find out minimum spanning tree for the following graph using Prim's algorithm. Show the steps clearly.



Compute the time complexity of the Prim's algorithm if priority queue is used in its implementation process. 10+5=15 marks

GROUP C

6. a) In the longest increasing subsequence problem, the input is a sequence of numbers: $a_1, a_2..a_n$. A subsequence is any subset of these numbers taken in order, of the form $a_{i_1}, a_{i_2} \dots a_{i_k}$, where $1 \le i_1 < i_2 < \cdots i_k \le n$, and an increasing sequence is one in which numbers are getting strictly larger. The task is to find the increasing subsequence of greatest length. For instance, the longest increasing subsequence of 5, 2, 8, 6, 3, 6, 9, 7 is 2, 3, 6, 9.

Explain the dynamic programming algorithm with DAG based input representation for finding the increasing subsequence of greatest length. Compute the time complexity of the algorithm.

b) Use the dynamic programming approach to find minimum edit distance and the optimal alignment between the strings the strings "E X P O N E N T I A L" and "P O L Y N O M I A L". Show only the table of computations, min edit distance and final optimal alignment. 7+8=15 marks

OR

7. Describe recursive solution and dynamic programming solution to finding n-th Fibonacci number. Compare time complexity for both the versions.

What is time complexity of the brute force method and dynamic programming method for solving string alignment problem. 10 +5=15 marks

GROUP D

8. a) Does the sorting problem belong to the class NP? - Give reasons.

b) What does NP stands for? Is *Boolean Satisfiability Problem* (SAT) NP-complete? - explain.

c) Explain the easier method to check whether a given problem is NP-complete or not 5 x 3=15 marks

OR

9. a) Consider that a minimum cost communication network will be set up among the major cities of a country in such a way that there will a communication path between any two cites. You may consider each city as a vertex and each communication link as the edge between two vertices. The weight of an edge is the cost of constructing the link represented by the edge. Every connected sub -graph that includes all the vertices represents a feasible solution. Under the assumption that all weights are non-negative, suggest an efficient algorithm for finding the optimal solution with minimum-cost. Formulate the problem as the graph problem first and discuss which and how the efficient graph algorithms can be used to solve this problem. How the running time of your algorithm differs from the brute force algorithm?

b) Define (i) the class NP, (ii) the NP-completeness 10 + 5 = 15 marks

Ref. No. Ex/CSE/PC/B/T/321/2023

BCSE 3rd Year 2nd Semester Examination, 2023

Database Management Systems

Full marks: 100 **Time: 3 hours**

Group A[CO1: Understand the fundamental concepts of DBMS and relational model]:15 Marks

1) a) i) In relational model, what is a relation? 3.5
ii) Mention the role of database manager. 2
iii) Under what condition intersection can be applied on two relations? 2
iv) Compare relational calculus and relational algebra. 1.5

OR

b) i) Define foreign key and mention its implication on referencing relation. 3
ii) Cite the examples for model based constraints in relational model? 2
iii) In relational algebra, represent division using basic operations. 2
iv) What is the utility of data dictionary? 2

2) Consider the following relations:

ITEM (ICODE, INAME, PRICE)
ORDER (ORDER_ID, ORDER_DT)
ORDER_DETAILS (ORDER_ID, ICODE, QTY)

ITEM and ORDER contain list of all items and all orders respectively. For every requested item in an order, an entry is there in ORDER_DETAILS.

i) Write down the relational algebra expression to find out the ORDER_IDs with requests for three or more different items. 3
ii) Write down the relational calculus expression to find out the INAMEs for the items which are not ordered at all. 3

Group B[CO2: Represent the database using Entity-Relation Model and design the database]:20 Marks

3) a) i) What is weak entity type? How will you implement the same in a database? 4
ii) Consider A is a super class and B, C, D are the subclasses. Consider the specialization is disjoint. Discuss, how will you design the database? 4

OR

b) i) Discuss, how will you implement one to many relation by avoiding null value. 4
ii) Explain union in EER model and compare with shared subclass. 4

4) Draw the ER diagram for the following system:
In an academic institute number of programs (like, UG-CSE, UG-ETC etc.) are there. Each program has program-id (unique), program name. In each program numbers of subjects are taught. Same subject may also be taught in number of programs. Faculty members are there who can teach one or more subjects. For a subject multiple faculties capable of teaching may exist. But, in a program one faculty is allotted for a subject in an academic session. System must be able to provide the information like, what are the programs, subjects taught in the programs, subject details, faculty details, for a subject who are the corresponding faculty members capable of teaching, in an academic session who have taught what and in which program. Consider suitable attributes and assume that sub code, faculty id, session id are unique for subject, faculty and academic session. Show the structural constraints also.
Identify the tables along with the primary key and foreign keys, if applicable. 7 5

Group C[CO3: Understand functional dependency and normalize the database]:20 Marks

5) Consider a schema to store project information as follows: (Proj_id, Proj_name, Proj_co-ord,Fund_agency, Co-ord_phone, co-ord_email, Emp_id, Emp_name, Basic, DOB, Dt_jn_in_proj, End_dt_in_proj)

In a project, multiple employees can work. Explain the problems with such schema.

Assume the following FDs:

Proj_id → Proj_id, Proj_name, Proj_co-ord

Proj_co-ord → Co-ord_phone, co-ord_email

Emp_id → Emp_name, Basic, DOB

Proj_id, Emp_id → Dt_jn_in_proj, End_dt_in_proj

Normalize up to 3NF showing the steps. Identify primary and foreign keys at each step.

Discuss, if an employee works in multiple projects whether that can be supported with the normalized schemas or not. 4+8+2

6) a) i) BCNF may not be dependency preserving – explain. 3
ii) In order to be in 3NF a schema must be in 2NF. Explain. 3

OR

b) i) What is denormalization? Why is it required? 3
ii) 4NF is a consequence of 1NF – explain. 3

Group D[CO4: Interact with database using SQL, PL/SQL, Trigger]:30 Marks

7) Consider the following tables:

SUBJECT(SCODE, SNAME, FULL_MARKS, PASS_MARKS)

STUDENT(ROLL, NAME)

RESULT(ROLL, SCODE, SCORE)

SUBJECT and STUDENT tables contains list of all subjects and students respectively. For every student there is an entry in RESULT corresponding to every subject he/she has appeared in the exam.

Write down the SQL statements for the following:

a) Find out the name and total score for the students with total score more than 400. The list must appear in the descending order of total score. 4

b) Find the name of the subjects in which nobody has failed (only considering those appeared in the exam for the subject). 4

c) Find the ROLL and SCODE combinations denoting the student has not appeared for the subject in the examination. 4

d) Delete the Student record from STUDENT table for those who were absent in the exam for all subjects. 4

e) Change the score as pass marks provided the student has failed in the subject with shortfall of 5 marks at the most. 4

8) a) i) What is the utility of PL/SQL in Oracle? 3

ii) Consider the following tables:

SUBJECT(SCODE, SNAME, FULL_MARKS, PASS_MARKS)

STUDENT(ROLL, NAME)

RESULT(ROLL, SCODE, SCORE)

PROMOTED(ROLL)

SUBJECT and STUDENT tables contains list of all subjects and students respectively. For every student there is an entry in RESULT corresponding to every subject he/she has appeared in the exam.

Write a PL/SQL block to store roll number of the students who have appeared and passed in all subjects and aggregate score is not less than 50% in PROMOTED table. 7

OR

b) i) Describe the attributes of implicit cursor in Oracle. 4

ii) Consider the tables as follows:

SUBJECT(SCODE, SNAME, FULL_MARKS, PASS_MARKS)

STUDENT(ROLL, NAME)

RESULT(ROLL, SCODE, SCORE)

SUBJECT and STUDENT tables contains list of all subjects and students respectively. For every student there is an entry in RESULT corresponding to every subject he/she has appeared in the exam.

Write a trigger so that while adding a row or updating SCORE in RESULT table score must be non negative and it must not exceed the full marks of the subject. 6

Group E[COs: Conceptualize the principles of query optimization, transaction processing, concurrency control, recovery]: 15 Marks

9) a) i) With a suitable example of concurrent example show that lost update problem does not occur in case of two-phase locking protocol. Explain what will happen for the schedule in case of time-stamp based protocol. 8

ii) Why is steal/no-force approach preferred in a concurrent environment? 4

iii) Compare the merge and hash join strategy? 3

OR

b) i) Discuss the recoverability issue in a concurrent schedule with an example. Show that two-phase locking protocol does not ensure the recoverability. What measures will you take to ensure the recoverability? 6

ii) Consider a concurrent environment that follows steal/no-force approach. How will you carry out log based recovery? 6

iii) How can you optimize $\sigma_{A=\text{"xxx"}}(R)$ where A is an attribute of R? 3

Subject Code: EX/CSE/PC/B/T/326

B. E. COMPUTER SCIENCE AND ENGINEERING 3rd YEAR 2nd SEMESTER EXAMINATION, 2023

ARTIFICIAL INTELLIGENCE

Total Marks 100

Time : 3 Hours

Q1: Answer either (a) or (b) [CO1]
Answer any two from Q2, Q3 and Q4 [CO2]
Answer any one from Q5 and Q6 [CO3]
Q7: Answer either (a) or (b) [CO4]
Q8 is compulsory [CO5]

Answer different parts of the same Question together

---

1. (a) Discuss on the Aim(s) of Artificial Intelligence. 5

   How many different approaches are followed in Artificial Intelligence (AI) for solving problems? What are they? Discuss any one. 5

OR

   (b) What is Turing test? What conclusions can be made from Turing test in connection to the 'intelligence' of a machine? 4+2

   Discuss on research trends in AI. 4

2. (a) What is an Agent? How do you view an Agent as a Search process? 2+4

   (b) Draw the differences between Rational Agent and Learning Agent. Indicate the points of differences. 4

   (c) How do you evaluate the performance of a search algorithm? 6

   (d) Can you devise a search algorithm where the time complexity will be lesser than $O(b^d)$? Provide reasons in support of your answer. 4

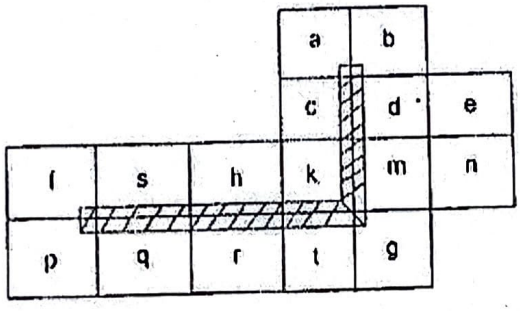
   (e) How do you formalize a search problem? How do you formalize the same for bidirectional framework? 5

3. (a) In the following maze the successors of a cell include any cell directly to the east, south, west or north of the current cell except that no transition may pass through the central barrier. The search problem is to find a path from s to g. Assume that you always try to expand East first, then South, then West, then North.

i) You decide to use a Manhattan-distance heuristic function, where h(state) = shortest number of steps from state to g if there were no barriers. Is this heuristic function admissible? – Discuss. 5

ii) Assume that you use best first greedy search using heuristic h (a version that never re-explores the same state twice). Find out all the states expanded, in the order they are expanded until the algorithm expands the goal state. 5

iii) Assume you use A* search with the same heuristic h and run until it terminates using the conventional A* termination rule. Find out all the states expanded, in the order they are expanded. 5



(b) Justify the following statements with suitable reasoning and/or example. 5+5

(i) Breadth first search and depth first search are special cases of best first search.

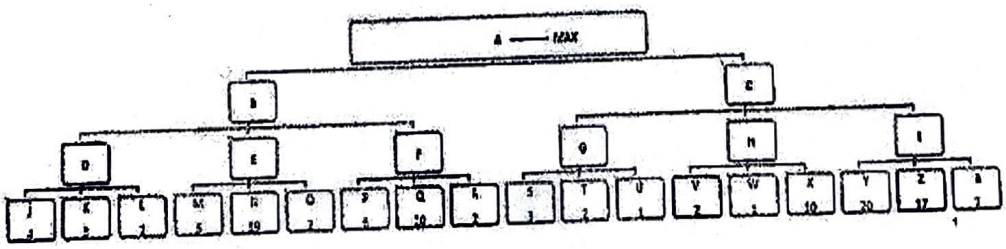
(ii) Iterative Broadening (IB) search is beneficial over Iterative Deepening (ID) search under certain circumstances.

4. (a) Consider the following game tree in which static scores are all from first player's point of view. The static scores at the leaf nodes from left to right are as follows: 4 3 2 5 19 2 6 20 2 3 2 1 2 1 10 20 17 7)

(i) Which path will be chosen if Minimax algorithm is used?

(ii) Which branches will be pruned if α-β pruning algorithm is used? 3+7

(Show all intermediate values)



(b) Consider α-β pruning algorithm using a tree with depth *d* and branching factor *b*. Estimate the amount of static evaluations you may require if you want maximum pruning. 4

(c) Why is Hill Climbing method called as an irrevocable search algorithm? 3

(d) How do you draw the correspondence between physical annealing technique and simulate the same method for solving an optimization problem? 4

(e) How can we control the resolution of a search space in Genetic Algorithm? 4

5.(a) Convert the following in Predicate Calculus *WFFs*.

(i) Bill has at least one sister.

(ii) Bill has at most two sisters.

(iii) Every student takes at least one optional course. 6

(b) Justify with explanation: While converting Clauses from Well Formed Formula, order of Quantifiers is irrelevant. 4

(c) What is Skolemization? Eliminate Existential Quantifier from the following *WFF*: 3+4

$$\forall x \ [\exists y \ Animal(y) \wedge \neg Loves(x,y)] \vee [\exists z \ Loves(z,x)]$$

(d) Find out the resolvents for the following pair of clauses: {P(z,b), Q(z)} and {~P(a,z), R(z)} 3

(e) Convert the following *WFF* into *clause* form:
All Romans who know Marcus either hate Caesar or think that anyone who hates anyone is crazy. 5

6. (a) Find the *mgu* of the following: {P(A, x, f(g(y))), P(z, f(z), f(u))} 4

(b) Consider the following axioms:

1. Jack owns a dog
2. Tuna is a cat
3. Cats are animals
4. Every dog owner is an animal lover
5. No animal lover kills an animal
6. Either Jack or Curiosity killed the cat, who is named Tuna

Use Resolution to answer: *Did Curiosity kill the cat?* 10

(c) What are the components of a Non Monotonic Reasoning System? What type of information one can obtain by looking at the "SL-justification" part? 3+4

(d) Model 'old' man using suitable membership function. From this, graphically represent "not very old". 4

7. (a) Draw the differences among Supervised, Unsupervised and Reinforcement Learning. Write down the points of distinction. 6

How do you evaluate the performance of a Machine Learning Model? 4

OR

(b) What is Supervised Learning? Who is acting as a "supervisor" here? What is a Decision Tree? What are the characteristics of a good clustering algorithm? 3+2+3+2

8. Discuss on Ethical issues in AI. 5

=====o=====

Ref. No.: Ex/CSE/PC/B/T/322/2023

B.E. COMPUTER SCIENCE & ENGINEERING 3rd YEAR 2nd SEMESTER EXAMINATION- 2023

INTERNET TECHNOLOGIES

Time: 3 hours | Full Marks: 100

Group A (Total Marks: 20) [CO1 and CO2]

Answer ANY TWO questions.

1.	a) Decompress and show the complete unabbreviated IPv6 address: AAAA:A:AA::1234 b) What is an IPv6 multicast addresses? Describe uses of permanent and transient multicast group addresses. c) What is IPv6 autoconfiguration? d) How does IPv6 handle fragmentation?	2+3+3+2 =10
2.	a) At any time instant local time at host H1 is 1500 and at host H2 is 1200. H1 wants to synchronize its clock with H2 using ICMP. H1 sends an ICMP Timestamp Request message at its local time 1500 and receives the corresponding reply at local time 1600. H2 receives the request at its local time 1300 and sends the reply immediately at local time 1300. Describe the actual messages exchanged (with probable values of different fields, except the checksum) and the steps how H1 adjusts its clock. b) Explain the uses of ICMP router advertisement and ICMP router solicitation messages.	6+4=10
3.	a) Assume that, in a TCP connection the initial sequence numbers chosen by the client and the server are 8000 and 9000 respectively. Clearly show values of sequence no., acknowledgement no. fields and flag bits (if any) of segments exchanged (i) During connection establishment (ii) When client sends a segment containing the message "Hello server" and the server answers with a segment containing the message "Hi client" (iii) During connection termination b) In a connection, the value of cwnd is 3000 and the value of rwnd is 5000. The host has sent 2,000 bytes, which have not been acknowledged. How many more bytes can be sent?	7+3=10

Group B (Total Marks: 10) [CO3]

Answer ANY ONE question.

4.	a) Briefly state the objectives of the SSL Handshake protocol. b) Explain how SSL Record protocol secures application data. c) Give examples of two cases when SSL alert protocol messages are generated.	3+5+2=10

5.	a) State the motivation for using design patterns for developing web applications. b) How does a web container provide different outputs for different clients when the same URL is requested? c) State the essential components of a web application framework.	3+4+3=10

Group C (Total Marks: 30) [CO4]
Answer ANY TWO questions.

6.	a) Implement a message passing application using Node.js where a user can send a message to other users who are connected and other users get notified when a user gets disconnected. Comment on how the various function calls are invoked at the server side-direct/CPS/callbacks. Did you use Event Emitter design pattern? Discuss how is it used. b) State a feature of Node.js/Express that is not supported by Servlets/Spring. Justify.	(5+4+4)+2=15
7.	a) Write a Node.JS application that takes two inputs-student name and Course. It collects these inputs from a user and stores them in Mongo DB. b) What is callback hell problem? Discuss 2 strategies to solve it. c) State the pros and cons of Websocket protocol.	5+5+5=15
8.	a)There are two currency classes-INR and GBP. For an online retail store that handles international customers, how can you calculate the total price of a cart with respective indirect taxes (based on respective countries regulations)? Write the basic components of dependency injection for this application and the structure of the Spring Controller class. b) How is front controller design pattern utilized here by the Spring framework? c) Discuss automatic data marshalling w.r.t Spring framework. Give suitable code snippets.	8+4+3=15

49

Group D (Total Marks: 40) [CO5]
Answer ANY FOUR questions.

9.	a) What is authorization? b) How can you enable authorization check for a URL in Spring? Only write the filter chain part. c) How is user authentication invoked in the request-response workflow by the Spring framework?	2+5+3=10
10.	a) A web server hosts a forum. It does not check the comments posted by the users for any security threat. How could this web server pose security threat to another web application hosted at a different server? b) Discuss about the session-fixation vulnerability. State how could it be handled using Spring framework.	5+5=10

11.	a) Discuss the advantages of (i) asynchronous code execution and (ii) synchronous code execution in Node.js with suitable use cases. b) How can injection attacks be avoided in Node.js?	6+4=10
12.	a) Differentiate between symmetric and asymmetric key cryptography. b) Explain how authentication and confidentiality can be achieved using asymmetric key cryptography. c) Explain the RSA key generation process.	2+4+4=10
13.	a) What is a secure hash function? What are the properties that a secure hash function must satisfy? b) What are the usages of digital certificates? Explain the role of a certification authority (CA). c) Assume users A and B in two different networks. User A owns a public-key certificate (PUB−CERT-A) that is digitally signed by a certificate authority (CA1). CA1's public-key certificate (PUB−CERT−CA1) is digitally signed by another certificate authority (CA2). User A trusts CA1 and User B trusts CA2. i. Explain how you would send a message M from user A to user B such that it provides integrity and authentication. ii. What would be the sequence of steps executed by receiver B to extract the message M?	3+3+4=10
14.	a) Assume that you can only use a hash function H and a symmetric-key encryption algorithm that takes a secret key K. Show how would you transmit a message M from user A to user B so that the following are guaranteed: (I) Message Authentication and Integrity (ii) Confidentiality (iii) Message Authentication, Integrity and Confidentiality. b) Assume that you can only use a hash function H and a secret S. Show how would you transmit a message M from user A to user B so that both message authentication and integrity are guaranteed. You should not use any encryption.	6+4=10

Ref. No.:EX/CSE/PC/B/T/324/2023

B.E. COMPUTER SCIENCE AND ENGG. 3rd YR 2nd SEM. Exam.-2023

SOFTWARE ENGINEERING

Time: Three Hours **Full Marks:100**

GROUP-A

Answer any 40 questions **40×2=80**

Choose the unique correct answer.

1. A high value of cyclomatic complexity of a program
(a) indicates that the code is complex
(b) creates problems in maintaining code
(c) is due to the presence of too many decision boxes
(d) all of the above

2. The primary purpose of dynamic dataflow testing is
(a) to uncover possible bugs in data usage during the execution of the code
(b) to analyse data flow during compilation
(c) to check data types
(d) none of the above

3. In Equivalence Class Partitioning
(a) many test cases are taken from each partition
(b) testing time is increased, as compared to exhaustive testing
(c) invalid inputs are never considered
(d) only one value from each partition is needed to evaluate the behaviour of the program for the related partition

4. If component A is a layer above component B, a top-down integration will require
(a) a stub to simulate A
(b) a stub to simulate B
(c) a driver to simulate A
(d) a driver to simulate B

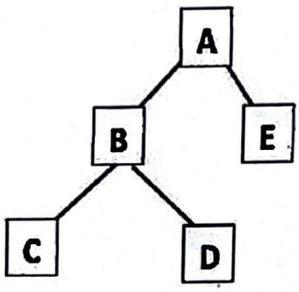
5. Consider the segment of pseudocode

```
if A and B and C then
    x := y + z
else
    x := u + v
```

In order to achieve condition-coverage, a test with
A = true, B =false, C = false is done.
The other test required to achieve condition-coverage is

(a) A = false, B = true, C = false
(b) A = false, B = true, C = true
(c) A = false, B = false, C = true
(d) none of the above

6.Consider the following graph of the modules of a piece of software:



A bottom-up integration of modules is carried out. First D and B are integrated. Then C and B are integrated and so on. The final step integration involves
(a) B, C, D
(b) B, A
(c) E, A
(d) D, B, C, A, E

7. A decision-table based testing is carried out on a piece of software. There are 7 conditions in the Condition Stub and there are 8 rules. There are 5 actions in the Action Stub. The minimum number of test cases required is
(a) 5
(b) 6
(c) 7
(d) 8

For Q8-Q12: Answer the following with respect to System Requirements Specifications (SRS):

8. Inputs, Processing, and Outputs are described under
(a) Quality Characteristics
(b) Design Constraints
(c) Functional Requirements
(d) Performance Requirements

9. Usability is described under
(a) External Interface Requirements
(b) Quality Characteristics
(c) Design Constraints
(d) Other Requirements

10. If a database is to be developed as a part of the product, it is described under
(a) Functional Requirements
(b) External Interface Requirements
(c) Design Constraints
(d) Other Requirements

11. An SRS includes ALL significant requirements. This characteristic is related to
(a) Correctness
(b) Completeness
(c) Consistency
(d) Unambiguousness

12. If there is no conflict between individual requirements, the SRS is
(a) correct
(b) complete
(c) consistent
(d) unambiguous

Answer Q13-Q19 in the context of Software Quality Assurance.

13. The metric "Weighted Methods/Class" is related to
(a) complexity
(b) number of methods that can be executed in response to a message
(c) depth of the Inheritance Tree
(d) none of the above

14. If the software process and products are quantitatively understood and controlled, the maturity level is
(a) defined
(b) managed
(c) repeatable
(d) optimizing

15. The software quality factor of "Flexibility" is related to the following Quality criterion:
(a) Machine Independence
(b) Operability
(c) Conciseness
(d) Expandability

16. In a structured walkthrough, the evaluation of the work product is carried out by
(a) reviewers
(b) moderator
(c) author
(d) scribe

17. The DMAIC methodology in Six Sigma is used when
(a) an existing product or process is not meeting customer specification
(b) a non-existent product or process needs to be developed

18. A Quality Assurance Analyst asks a developer which requirement of an SRS his code has implemented. Such a question is classified as
(a) Design Validation
(b) Quality Planning
(c) Functional Traceability
(d) Configuration Management

19. A Pareto Chart
(a) is used in Project Scheduling
(b) finds the main causes behind defects
(c) is used for cost analysis of projects
(d) none of the above.

---

20. The process model in which the user is involved in all phases of the life-cycle – not only requirements definition, but also design, development, test, and final delivery, is
(a) Waterfall
(b) Prototype
(c) Spiral
(d) RAD

21. The evaluation of alternatives and risk assessment is addressed most thoroughly in
(a) Waterfall
(b) Prototype
(c) Spiral
(d) RAD

22. In developing user interfaces, the preferred process model is
(a) Waterfall
(b) Prototype
(c) Spiral
(d) RAD

23. If the project is an enhancement to an existing system, the appropriate process model is
(a) Waterfall
(b) Prototype
(c) Spiral
(d) RAD

24. If the system is expected to be modified in unanticipated ways after deployment, the following process model is appropriate
(a) Waterfall
(b) Prototype
(c) RAD
(d) all of the above

25. When porting an existing product to a new platform, the preferred process model is
(a) Waterfall
(b) Prototype
(c) RAD
(d) Spiral

26. The first step in developing a Risk Management Plan is to construct
(a) a decision tree
(b) a risk categorization table
(c) a use case model
(d) none of the above

27. A table of top software project risks is constructed. For a particular row in the table, the probability of risk is 20 and the associated loss is 9. The Risk Exposure is
(a) 120
(b) 150
(c) 180
(d) 200

28. The Risk Response Report is discussed in weekly project status meetings. This table has the following entry for each important risk.
(a) the date by which action is due
(b) the person(s) who is responsible for the action
(c) the resolution approach
(d) all of the above

29. The Weekly Risk Change Report contains
(a) the risk exposure
(b) the rank of the risk in the current week
(c) the number of weeks for which an item was found to be in the list
(d) both (b) and (c)

For Q30-Q32: A project has the following information domain characteristics:

No. of user inputs = 24
No. of user outputs = 65
No. of user inquiries = 12
No. of files = 12
No. of external interfaces = 4

All the Complexity Adjustment Values are "moderate."

30. The Raw Function Point Count is
(a) 89
(b) 117
(c) 617
(d) none of the above

31. The Complexity Adjustment Factor (CAF) is
(a) 0.5
(b) 1.23
(c) 14
(d) 28

32. The Adjusted Function Points is
(a) 120
(b) 325
(c) 617
(d) 759

---

33. Utility systems, e.g. compilers and database systems, are associated with the following COCOMO mode:
(a) Organic
(b) Semidetached
(c) Embedded
(d) all of the above

34. Phase-sensitive effort multipliers are used in the following COCOMO level:
(a) Basic
(b) Intermediate
(c) Detached
(d) none of the above

35.The Project Duration Estimate in the Embedded Mode of the COCOMO Basic level is
(a) $2.5 \times (E)^{0.32}$
(b) $2.5 \times (E)^{0.35}$
(c) $2.5 \times (E)^{0.38}$
(d) none of the above

where E is the effort in staff-months.

36. In the Critical Path Method, the latest start dates for activities are calculated in the
(a) forward pass
(b) backward pass
(c) both (a) and (b)
(d) neither (a) and (b)

37. In a PERT network, an activity has duration estimates as given below:
Optimistic: 8
Most likely: 10
Pessimistic:15
The expected duration is
(a) 11
(b) 13
(c) 9.5
(d) 10.5

38. In Earned Value Analysis, Schedule Variation (Cost) is given by
(a) BCWP – BCWS
(b) ACWP – BCWP
(c) ACWP – BCWS
(d) none of the above

39. When a module only performs a single computation, and returns a result, without having side-effects, it achieves
(a) Communicational cohesion
(b) Functional cohesion
(c) Layer cohesion
(d) Procedural cohesion

40. Software Design Principle advises a designer to
(a) reduce coupling
(b) increase coupling
(c) ignore coupling
(d) none of the above

41. In Software Design, the level of abstraction should be
(a) as high as possible
(b) as low as possible

42. The design goal "Design for flexibility" is achieved by
(a) increasing coupling and increasing cohesion
(b) reducing coupling and increasing cohesion
(c) reducing coupling and reducing cohesion
(d) increasing coupling and reducing cohesion