2019

COMPUTER SCIENCE

Paper : CSM-303

(Theory of Computation)

Full Marks : 70

The figures in the margin indicate full marks.

Candidates are required to give their answers in their own words as far as practicable.

Answer ***question nos.* 1, 2;** and ***any four*** questions from the rest.

1. Answer ***any five*** questions : 2×5

(a) State the Pumping Lemma for Regular Languages.

(b) Give an example of a Turing recognizable language that is not Turing decidable.

(c) Consider the set of all strings of odd length on the alphabet {0, 1}. Express this set in the form of a regular expression.

(d) Let R_1 be a regular set on the alphabet {0, 1} and let R_2 = {00, 101, 110, 011}. Is the difference set $R = R_1 - R_2$ necessarily a regular set?

(e) List three major points of difference (in features and/or method of operation) between a pushdown automaton (PDA) and a Turing Machine (TM).

(f) What are different normal forms of CFGs? State their significances.

(g) What is left recursive grammar? Cite an example.

(h) What is post-correspondence problem? Give an example.

(i) What is the basic difference between recursive language and recursively enumerable language?

(j) What is the difference between NP and co-NP problem?

2. Answer ***any five*** questions :4×5

(a) Let L_1 be the following language defined over the input alphabet $\sum = \{0, 1\}$.

$L_1 = \{\alpha \mid$ the string α does not contain the substring '00'$\}$

Thus the strings 101101 and 01110 are both in L_1, but the string 1001 is not in L_1. Give regular expression for L_1. 4

(b) Consider the set of strings $\{0^p 1^q 0^p \mid p > 0, q > 0\}$ on the alphabet {0, 1}. Give a type 2 grammar G that generates this set. 4

(c) Consider the set S of all strings α on the alphabet set {0, 1, 2} such that α contains at least one 0, at least 2 1's and at least three 2's. Is S a regular set? Justify. 4

Please Turn Over

(d) Write a pseudo program to translate a regular expression to finite automata. 4

(e) Split out the logical steps to convert an NDFA to its equivalent DFA. 4

(f) Briefly explain what is meant by 'Universal Turing Machine'. Can every effective procedure be implemented by a UTM assuming the input is appropriately supplied? 4

(g) Are deterministic PDA and non-deterministic PDA equivalent? Justify your answer with suitable example. 4

(h) Explain with suitable example : elimination of useless symbol(s) and unit production(s) from context free grammars. 2+2

(i) State and proof Rice's theorem. 4

(j) Prove by example that regular languages are closed over union and intersection. 2+2

3. State the pumping lemma for context free languages. Prove using pumping lemma that the following language L is not context free

$$L = \{0^m 1^{2m} 0^{3m} \mid m > 0 \}.$$ 10

4. (a) Design a single track-single-head Turing machine to compare two strings of unary symbols. Clearly state your assumptions.

(b) What do you mean by decidability and undecidability? Give suitable examples. 7+3

5. (a) What are the alternatives forms of Push Down Automata (PDA)? How will you justify the equivalence of alternative forms of PDA?

(b) Design a PDA M to accept the following context-free language on the input alphabet {0, 1}

$L = \{\alpha \mid$ the string α contains more 0's that 1's$\}$ 4+6

6. (a) Comment on the closure properties of regular sets. What is quotients of languages?

(b) Test the membership of the string 'baaba' for the following grammar :

$S \rightarrow AB \mid BC$

$A \rightarrow BA \mid a$

$B \rightarrow CC \mid b$

$C \rightarrow AB \mid a$ 5+5

7. (a) Prove or disprove the following for regular expression a, b, c :

$1(01 + 1)^*0 = 00^*1(00^*1)^*$

$(a + b)^* = a^* + b^*$

(b) Construct a deterministic finite automaton M on the input alphabet {0, 1, 2} that accepts a string α if and only if α is contained in all regular expression 0^*1^*. 5+5

8. (a) Define grammar.
   (b) Discuss Chomsky classification of grammar with suitable examples.
   (c) How can you design a DFA from a grammar of Type-3? Explain the process with suitable example. 2+5+3

9. (a) Differentiate tractable problem and intractable problem.
   (b) How to solve an intractable problem?
   (c) Define cellular automata. Discuss different types of it in brief. 2+3+2+3

2019

COMPUTER SCIENCE

Paper : CSM-302

(Advances in Operating System)

Full Marks : 70

The figures in the margin indicate full marks.

Candidates are required to give their answers in their own words as far as practicable.

Answer ***question* 1, 2** and ***any four*** from the remaining questions. All answers should be precise

1. Answer ***any five*** out of the following : 2×5

(a) What is global state of a system?

(b) Define access transparency.

(c) State at least two different motivations behind process migration.

(d) Why are token based algorithms said to be inherently safe?

(e) What would be the nature of a global state recording curve on the time-line of an event trace diagram?

(f) Define the condition for precedence between two events e_p and e_k.

(g) Name a cell semantics supported in SUN RPC implementation for synchronous mode of operation.

(h) State the condition for Happens Before relation between events.

(i) What are commonly used methods to solve thrashing problem in a DSM System?

2. Comment on the correctness of the following statements and justify your opinion–answer ***any five*** : 4×5

(a) *'Failure of liveness is not a major concern for deadlock detection algorithms'*

(b) 'Recording Global State for a distributed system is impossible'—

(c) 'Lamport's Clock model generates unique time stamp for each and every event in a distributed system'

(d) 'In a distributed system, resource migration is more challenging than migration of codes for a process'

(e) 'Call by reference is not a suitable option for parameter passing in RPC'

(f) 'Termination Detection using weight throwing approach maintains both safeness and liveness'

(g) 'Raymond's algorithm may grant access to processes' out of order.

3. (a) What is false sharing? Can this problem had to any other problem in a DSM system? Give reason for your answer.

(b) What is stub? How stubs are generated? Explain how the use of stubs helps in making an RPC machanism transparent. (2+3)+(1+1+3)

4. (a) Define condition of consistency in terms of processes and channels in a distributed system.

(b) State the assumptions and conditions for Lamport's logical clock model.

(c) 'Two unrelated events X and Y occur in two different nodes. The Lamport's logical clock time-stamp values for the two events are TS(X), and TS(Y) respectvely such that TS(X) > TS(Y). It cannot be inferred from these statements that physically Y has occurred before X'— give your opinion on the validity of the statements above and justify the same. 3+3+4

5. (a) Describe a token based algorithm for mutual exclusion in distributed system.

(b) What would be the best and worst-case control message complexity for the above algorithm for a system with N competing processes? Justify your assessment.

(c) Compare symmetric algorithms vis-a-vis token based algorithms for mutual exclusion. 4+3+3

6. (a) Describe the Ho-Ramamurthy's deadlock detection algorithm for distributed environment. Illustrate the same with an example.

(b) Comment on the safety and liveness properties of Ho-Ramamurthy's deadlock detection algorithm. 6+4

7. (a) Define pre-emptive and non pre-emptive process migration.

(b) Name two alternate metrics that may be used to measure load in a node.

(c) State two diffrent motivations for process migration other than load balancing.

(d) State the merits and demerits of sender initiated versus receiver initiated process migration approaches. 2+2+2+4

8. (a) Explain the process of stub generation in SUN RPC using Interface Definition Language.

(b) What is Orphan call? Why is it important to detect an Orphan Call?

(c) What is the role of binding agent in RPC?

(d) Suggest the appropriate call semantics to be used (among may-be, last-of-many, at-least-once or exactly-once) for the following applications.

(i) To request a time server to get the current time;

(ii) To request a booking server to reserve a seat;

Present brief explanation for your choices in each of the cases. 3+1+2+(2+2)

9. Derive the D^-, D^+ and D matrices for the following Petri Net.

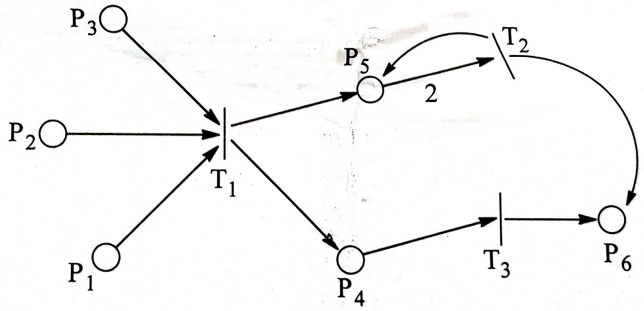


Fig-1 A Petri Net Model.

Given an initial marking of lu = [4, 3, 3, 0, 1, 0], draw the reachability tree for the Petri Net in Fig-1 Is it possible to reach a state with 4 token in P_6 for the above initial marking? Justify your opinion and list the firing sequence for the transitions accordingly. 4+3+3

2019

COMPUTER SCIENCE

Paper : CSM-301

(Introduction to Soft Computing)

Full Marks : 70

The figures in the margin indicate full marks.

Candidates are required to give their answers in their own words as far as practicable.

Answer ***question nos.*** **1, 2** and ***any four*** from the rest.

1. Answer ***any five*** questions : 2×5

(a) State the difference between fuzziness and probability with the help of an example.

(b) What do you mean by perceptron?

(c) Prove that height (F) = 1 where F is normal fuzzy set.

(d) Explain why mutation operator for GA is used to exit from stuck at local optima problem.

(e) State the basic objective of a fuzzy cruise controller.

(f) Let us consider the fuzzy set M on the U = {a, b, c, d, e} described as

M = 0.375/a + 0.5/c + 1.0/d + 0.875/e;

Find out support(M), core(M) and |M|?

(g) The height h(A) of a fuzzy set A is defined as h(A) = sup A(x) where x belongs to A. What is the condition for a fuzzy set A to be normal?

(h) Consider two fuzzy sets :

P = Beautiful flowers = 0.3/jasmine + 0.9/rose + 1.0/lotus + 0.7/daffodil

Q = Fragrant flowers = 1.0/jasmine + 1.0/rose + 0.5/lotus + 0.2/daffodil

Compute fuzzy sets R, where R = disjunctive sum (P, Q)

(i) Write the formula for the interpretation of fuzzy rule using Mamdabi's interpretation.

2. Answer ***any five*** questions : 4×5

(a) Consider the following definition :

'Persons of age 0 to 35, 20 to 60, 45 to 80 are known as young, middle-aged, old respectively.' Now construct the membership graph and membership functions for linguistic variables young, middle-aged and old. 4

(b) The fuzzy 'if then else rule' under consideration is R : if 'distance is long' then 'drive at high speed' else 'drive at moderate speed'. The relevant sets are Distance = {100, 500, 1000, 5000} is the universe of the fuzzy set long distance, speed = {30, 50, 70, 90, 120} is the universe of the fuzzy sets high-speed as well as moderate speed;

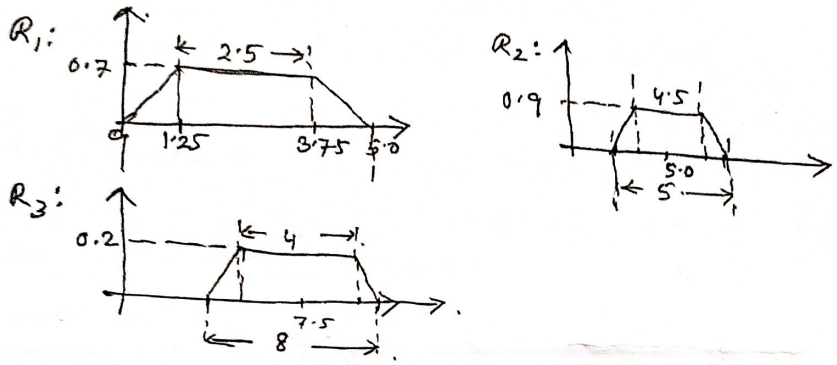
long-distance = 0.1/100 + 0.3/500 + 0.7/1000 + 1.0/5000

high-speed = 0.1/30 + 0.3/50 + 0.5/70 + 0.7/90 + 0.9/120

moderate-speed = 0.3/30 + 0.8/50 + 0.6/70 + 0.4/90 + 0.1/120

Compute the relation matrix of R using Zadeh's interpretation. 4

(c) Explain the use of defuzzification in the Fuzzy Inference System. Use CoS method for the following output fuzzy rules to get the crisp output. 2+2



(d) Let A = {mimi, bob, kitty, jina} be a set of four children and B = {tintin, asterix, phantom, mickey} be a set of four comic characters; and C = {funny, cute, dreamy} be a set of three nature attributes. The fuzzy relations R = x likes y is defined on A X B and S = x IS y is defined on B X C as shown in Table 1 and Table 2. Find out the fuzzy relation T = x IS y defined on A X C. 4

Table : 1 :- R = x likes y on AXB

	Tintin	asterix	phantom	mickey
mimi	0.8	0.5	0.7	0.8
bob	0.4	0.9	0.3	0.3
kitty	0.6	0.7	0.4	0.9
jina	0.3	0.8	0.2	0.5

Table : 2 :- S = x IS y on BXC

	funny	cute	dreamy
tintin	0.6	0.7	0.3
asterix	0.8	0.4	0.2
phantom	0.1	0.2	0.1
mickey	0.9	0.8	0.3

(e) What do you mean by learning rule for ANN? State the working procedure of 'Delta learning rule'. 2+2

(f) State Modus Ponens, Modus Tollens, Universal Specialization and Chain Rule with the help of examples. 4

(g) (i) State crossover process of genetic algorithm with the help of examples.

(ii) What do you mean by multi-objective optimization? Explain with an example. 2+2

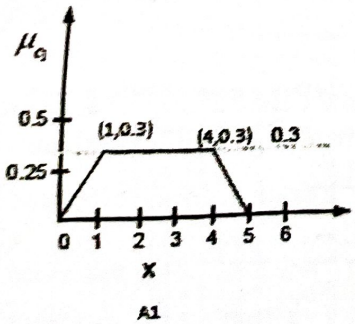
(h) Find the max-product composition of following given two fuzzy relations. Also find the total projection of this resultant relation. 2+2

$$R_1 = \begin{bmatrix} 0.1 & 0.2 & 0.0 & 1.0 & 0.7 \\ 0.3 & 0.5 & 0.0 & 0.2 & 1.0 \\ 0.8 & 0.0 & 1.0 & 0.4 & 0.3 \end{bmatrix}$$

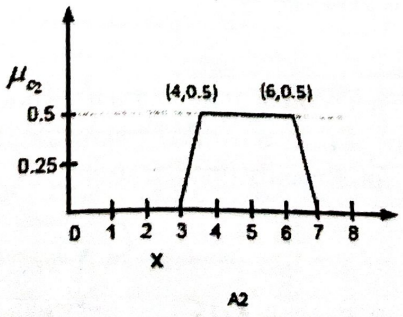
$$R_2 = \begin{bmatrix} 0.9 & 0.0 & 0.3 & 0.4 \\ 0.2 & 1.0 & 0.8 & 0.0 \\ 0.8 & 0.0 & 0.7 & 1.0 \\ 0.4 & 0.2 & 0.3 & 0.0 \\ 0.0 & 1.0 & 0.0 & 0.8 \end{bmatrix}$$

3. Define linear separability. Show that XDR-Gate is not Linearly separable. State the features of McCulloch-Pitts Neural net. Implement OR-Gate using this net. 2+3+2+3

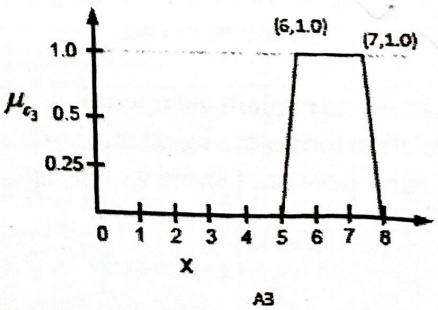
4. (a) There are three fuzzy sets A1, A2, A3 in the following figures. Find out the defuzzified value of the aggregated fuzzy set (A1, A2, A3) using centre of gravity method.



A1



A2



A3

(b) Compute error values after 1st iteration of multilayer feed forward network (3-2-1) using the back propagation leaning. Consider **Table 1** with following initialization :

Table-1

X1	1	input
X2	0	input
X3	1	input
W14	0.2	weight
W15	–0.3	weight
W24	0.4	weight
W25	0.1	weight
W34	–0.5	weight
W35	0.2	weight
W46	–0.3	weight
W56	–0.2	weight
Θ4	–0.4	Bias
Θ5	0.2	Bias
Θ6	0.1	Bias
1	0.9	Leaning rate
Class label	1	

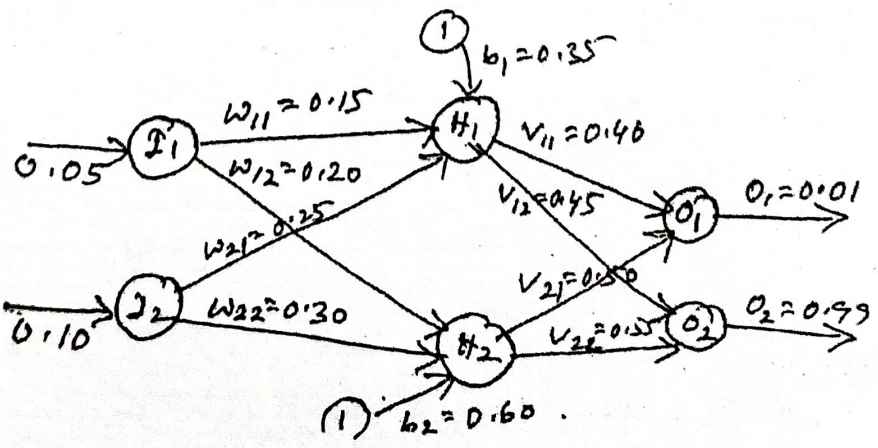
(c) (i) Define L-R type fuzzy numbers with various operations.

(ii) Draw the l-m-n fuzzy back-propagation architecture and state the learning and inference algorithm of the network.

3+2+(3+2)

5. Draw and explain the operations of back propagation neural network. Established a matrix based mathematical relation formula to calculate the output of such network. Demonstrate the working of following back-propagation neural network (Show weight updation for only one iteration).

3+2+5



6. Define λ-cut. Apply λ-cut for the following fuzzy set operations :

$$A = \left\{ \frac{0.2}{x_1} + \frac{0.3}{x_2} + \frac{0.4}{x_3} + \frac{0.7}{x_4} + \frac{0.1}{x_5} \right\}$$

$$B = \left\{ \frac{0.4}{x_1} + \frac{0.5}{x_2} + \frac{0.6}{x_3} + \frac{0.8}{x_4} + \frac{0.9}{x_5} \right\}$$

(i) $(\bar{A})_{\lambda=0.7}$

(ii) $(A \cap B)_{\lambda=0.6}$

(iii) $(\bar{A} \cup B)_{\lambda=0.7}$

State the importance of fuzzy extension principle. 2+(2×3)+2

7. Illustrate how GA can be used to solve the following optimization problem :

max $f(x_1 x_2) = f(x_1 - 5)^2 + (x_1 - 6)^2 : 1 \le x_1 \le 8^2 \le x_2 \le 5.$

x_1, x_2

Assume the followings :

(a) for selection roulette wheel is used

(b) Single point cross over

(c) Real encoding GA

(d) Cross over and mulation probabilities respectively 0.3^{ad}, 0.2.

(e) Population size = 3.

Show 2-iterations.

Mention how GA is different from traditional algorithm. 7+3

8. (a) State stability and plasticity dilemma.

(b) Draw and illustrate the simplified architecture of Adaptive Resonance Theory (ART1)

(c) State the learning algorithm of Adaptive Resonance Theory (ART1) 2+(1+3)+4

9. (a) State the difference between Hetero-associative and Auto-associative memory.

(b) Suppose here 3 pattern pairs given by

A1 = 100001	B1 = 11000
A2 = 011000	B2 = 10100
A3 = 001011	B3 = 01110

Retrieve pattern B3 after knowing the associated pattern A3 = 001011 using Kosko's Bi-directional associative memory

(c) State the K-SOM architecture and learning algorithm. 2+4+4

2019

COMPUTER SCIENCE

Paper : CSM-304

(Cryptography and Network Security)

Full Marks : 70

The figures in the margin indicate full marks.

Candidates are required to give their answers in their own words as far as practicable.

Answer ***question no.*** **1, 2** and ***any four*** from the rest.

1. Answer ***any five*** from the following : 2×5

(a) Distinguish between Diffusion and Confusion.

(b) Find out the multiplicative inverse of each non zero element in Z_5.

(c) Is it possible to perform encryption operations in parallel on multiple blocks of plaintext?

(d) What is Euler's Totient function? Compute the value of $\phi(231)$.

(e) Is AES a Feistel cipher? Justify your answer.

(f) State the Extended Euclidian algorithm. What is it's application in cryptography?

(g) State the importance of Galois field in cryptography.

(h) What do you mean by Packet sniffing?

(i) Give an example of 'reflection attack'.

2. Answer ***any five*** from the following : 4×5

(a) Describe the utility of Trap-door-one way function in context of RSA encryption.

(b) Compute 21^{24} mod 8 using fast exponentiation. Show each steps.

(c) Show that the group $< Z_{10}, X >$ is s cyclic group.

(d) Discuss the role of Key Distribution Centre in Secret Key cryptography.

(e) 'Meet-in the Middle' attack is a specific attack for 2-DES'– Explain.

(f) State the principle of Zero Knowledge authentication. Is it better than Challenge-Response approach?

(g) Determine the multiplicative inverse of $X^3 + X + 1$ in GF (2^4) with irreducible polynomial $X^4 + X + 1$.

(h) What is Key wrapping? Comment on the strength of this approach.

3. Describe the block diagram of AES encryption. "Mixing transformation i.e. "Mix-column" is needed in AES but not needed in DES"– Comment on the statement with justification. Compare the performance of AES over DES. 3+5+2

4. Describe the possible classification of attacks, based on the information known to an attacker. Discuss a possible attack on RSA. Is there any advantage(s) of using Eliptic curve over RSA? 4+3+3

5. State the conditions that a has h function should satisfy. Prove that the difficulty of an alternative collision attack in message integrity is proportional to $2^{n/2}$. Is there any difference between Message Authentication Code and Message Digest? Justify your answer. 3+5+2

6. How the problem of Key exchange is addressed in IP Sec? State the purpose of a firewell. How an application gateway firewall offers the security? State the difference between http and https protocol. 5+1+3+1

7. "Sub-key generation process also affects the strength of an encrytion technique"– Discuss the issue in context of DES algorithm. Discuss the Miller Rabin test for primality testing. State the principal difference between Tunnel mode and Transport mode implementation of IP Sec. 3+4+3

8. In context of ElGamal cryptosystem, Describe the Key generation and encryption-decryption process. Comment on the security of the system. How it can be used to prepare digital signature? 4+2+4

9. How is SHTTP different from SSL? State the role of CA and RA. What are the basic approache(s) to bundle SA? State the purpose of DMZ. 2+2+4+2
