(35)

ISLAMIC UNIVERSITY OF TECHNOLOGY (IUT)

ORGANISATION OF ISLAMIC COOPERATION (OIC)

Department of Computer Science and Engineering (CSE)

SEMESTER FINAL EXAMINATION — SUMMER SEMESTER, 2022-2023

DURATION: 3 HOURS — FULL MARKS: 100

CSE 4809: Algorithm Engineering

Programmable calculators are not allowed. Do not write anything on the question paper.

Answer **all 6 (six)** questions. Figures in the right margin indicate full marks of questions with corresponding COs and POs in parentheses.

---

1. a) GPU parallelism is most suited for matrix multiplication type of operations. It helped Deep Learning algorithms to speed up the training process dramatically. Explain the speed up mechanism in brief. — 4 (CO1) (PO1)

   b) RNN based networks are slow in training — why? Provide proper reasoning behind your answer. — 4 (CO1) (PO1)

   c) Transformers are very fast in training. How did transformers overcome the barriers of RNN in training speed? — 4 (CO1) (PO1)

   d) RNN based seq-to-seq models inherently model sequence information, while the Encoder-Decoder architecture of transformers is incapable of modeling sequence. How is the sequence information retained in transformer models then? Explain. — 4 (CO1) (PO1)

2. a) What is the importance of Nonce in PoW based Block Chain consensus mechanism? Will Nonce be necessary in PoS consensus mechanism? — 4 (CO1) (PO1)

   b) How does merkel tree and merkel hash ensures the integrity of a block in a blockchain? — 4 (CO1) (PO1)

   c) Why cannot a miner start calculating a block ahead of time? As we know, in Bitcoin, a hash challenge is thrown every ten minutes and a crafted miner may want to participate in a future round skipping few rounds. — 4 (CO1) (PO1)

   d) PBFT algorithm claims that a peer-to-peer distributed network will not be compromised as long as maximum $\frac{1}{3}$ of the participating nodes are faulty. Provide a proof of the claim. — 4 (CO1) (PO1)

3. a) What is the theoretical validity of RSA algorithm that encrypted message using public key will be decrypted as the same message using private key? — 4 (CO1) (PO1)

   b) Bloom Filter is used in new user creation process in websites now-a-days. Explain the mechanism. Is it possible that the mechanism generates false positives for occupied user names? — 4 (CO1) (PO1)

   c) Min-hash and Bloom filter can be used to find similarity in big documents. Explain the mechanism. — 8 (CO1) (PO1)

4. a) List 5 (five) algorithms for finding shortest path in a graph and explain in which scenario the particular algorithm can be used. There is no need to write the algorithms themselves. — 10 (CO1) (PO1)

b) WER (Word Error Rate) finding algorithm matches output vector/sentence with the matching vector/sentence and generates WER. WER will just count how many word insertions, deletions, and substitutions happened in total to match. A percentage score is reported. Can you think of an algorithm that was covered in your course suitable to be applied to find WER? Briefly outline the algorithm. 4 (CO1) (PO1)

c) Write short answers for the followings: 3×2 (CO1) (PO1)

i. How does B+ Tree maintain balance during insertion and deletion operations?

ii. Write two applications of memory based balanced tree.

iii. Why cannot we use memory based balanced tree in disk-based searching?

5. a) Define P, NP, NP-Hard, and NP-Complete. 4 (CO1) (PO1)

b) What is reduction? Why reduction is very important in dealing with NP problems? 4 (CO1) (PO1)

c) Prove that 2-CNF SAT is satisfiable. 4 (CO1) (PO1)

d) Prove that Halting problem is not decidable. 4 (CO1) (PO1)

6. a) What is approximation ratio? Define ρ and ϵ in approximation. Which of the two approximation algorithms defined by the following complexities will be good and why? 4 (CO1) (PO1)

$$O(n^{\frac{2}{\epsilon}}),\ O((\frac{1}{\epsilon})^2 n^3)$$

b) Prove that GREEDY-SET-COVER is a polynomial-time $\rho(n)$-approximation algorithm, where $\rho(n) = H(max|S| : S \in \mathcal{F})$. 4 (CO1) (PO1)

c) Prove that the randomized algorithm for MAX-3-CNF satisfiability discussed in your book is an $\frac{8}{7}$ approximation algorithm. 4 (CO1) (PO1)

d) Write a 2-approximation algorithm for the Travelling Salesman Problem (TSP). 4 (CO1) (PO1)