JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST-3EXAMINATION- 2025

B.Tech-V Semester (CSE/IT)

COURSE CODE (CREDITS): 25B1WCI511 (2) MAX. MARKS: 35

COURSE NAME: PROMPT ENGINEERING

COURSE INSTRUCTORS: VANI SHARMA MAX. TIME: 2 Hours

Note: *(a) All questions are compulsory.*

(b) The candidate is allowed to make Suitable numeric assumptions wherever required for solving problems

(c) Use of calculator is allowed

Q.No	Question	CO	Marks
Q1	You are designing an enterprise LLM system that handles these workload categories: A. High-volume, low-complexity factual queries B. Medium-complexity classification tasks with noisy inputs C. High-stakes numerical reasoning with strict correctness requirements D. Open-ended strategic decision support requiring exploration of alternatives E. Multi-step workflows involving interdependent sub-tasks For each category: a) Choose two prompting techniques that could be applied and compare them in terms of performance, reliability, safety, and interpretability. b) Select the optimal technique and justify why the alternatives are inferior for that category. c) Explain the consequences of incorrect prompting-method selection.	3	[6]
Q2	A research team uses meta prompts like:"First decide your reasoning strategy, then solve the problem accordingly."The model improves in structure but becomes slower and sometimes over thinks simple tasks. Analyze the benefits and drawbacks of meta prompting in this situation. When meta prompting should be avoided, and how can the prompt be optimized?	3	[4]
Q4	Explain the concept of prompt sensitivity inLLMs. Discuss how variations in wording, structure, and context of a prompt influence model behavior. Provide suitable examples and elaborate on factors that increase or decrease sensitivity.	4	[4]

Q5	a) Define LLM hallucination. Describe different types of hallucinations (factual, logical, and contextual) with examples. Discuss why hallucinations occur from a model architecture and training-data perspective. b) What is prompt leaking? Explain with examples how attackerscan extract hidden system prompts or confidential instructions embedded in the model. Discuss the vulnerability of LLMs to prompt leaking due to their architecture.	4	[5+3]
Q6	Given the following query, key and value vectors for a simplified Transformer with dimension $d_k = 4$: $Q = [1,2,1,0]$ $K_1 = [2,1,3,1]$ $K_2 = [0,4,1,2]$ $K_3 = [3,0,2,4]$ $V_1 = [1,3,2,1]$ $V_2 = [4,1,0,2]$ $V_3 = [2,2,5,3]$ Compute the following: a) Attention scores for each key. b) Attention probability distribution using the scaled Softmax function: $P_i = \frac{e^{score(Q,K_i)/\sqrt{d_k}}}{\sum_j e^{score(Q,K_j)/\sqrt{d_k}}}$ c) Final attention vector	3	[4+3+3]
Q7	Rewrite the following prompt to use chain-of-thought: "Solve: A shop sells pens at ₹10. If Riya buys 7 pens, how much does she pay?"	3	[3]