CSE665: Large Language Models
End-term Examinations [9 May, 2024]

Name:
Roll Number:

Instructions:

1. Duration of the exam is 2 hours. Total marks are 90.
2. Write Name/ Roll number/ Project group on the answer sheet and questions paper both.
3. Choose the most appropriate answer for MCQs.
4. No Negative marking
5. Write theory based answers in 150 words and reasoning based until you cover all points mentioned in the question

Multiple choice Questions [3 marks x 20 Questions]

1. What is the primary goal of differential privacy in data analysis?
    A. Maximizing the accuracy of the analysis.
    B. Minimizing the computational complexity of algorithms.
    C. Ensuring the privacy of individuals' sensitive data.
    D. Optimizing the scalability of data processing systems.

2. Which of the following best describes the primary function of the CLIP model?
    A. Generating realistic images from textual descriptions.
    B. Converting images to text.
    C. Analyzing images and text to understand their relationship.
    D. Identifying patterns in audio files.

3. Which of the following best characterizes the BLIP model in multimodal learning?
    A. It focuses solely on visual information processing.
    B. It integrates linguistic and visual information hierarchically.
    C. It emphasizes auditory cues over visual stimuli.
    D. It disregards sequential processing of multimodal inputs.

4. In the ViT model, what does the term "self-attention" refer to?
    A. The ability to focus on different image regions simultaneously
    B. The mechanism for learning global dependencies between image patches
    C. The process of reducing model complexity
    D. The method for enhancing image contrast

5. What does the Stereotype Score (SS) represent in language models?
    A. The percentage of instances where the model chooses neutral language over biased language.
    B. The measure of how often the model selects stereotypical language compared to anti-stereotypical language.
    C. The degree of accuracy in detecting stereotypes within text.
    D. The proportion of times the model generates creative language versus conventional language.

6. What are the numerical values used to evaluate the outcomes of actions taken by an agent?
    A. Observations
    B. Rewards
    C. Policies
    D. Loss Functions

7. In transformer-based models, what is the “position encoding” used for?
    A. To indicate the order of words in a sequence, as the transformer architecture does not have built-in positional information
    B. To encode the geographical positions of data samples
    C. To encode the position of the model's parameters
    D. To control the learning rate

8. What is the significance of the “pre-training” and “fine-tuning” approach used in Large Language Models?

    A. Pre-training refers to training a model from scratch, while fine-tuning adapts it to specific tasks
    B. Pre-training involves optimizing the model for a specific task, while fine-tuning is a general training phase
    C. Pre-training is the process of compressing the model, while fine-tuning is for model expansion
    D. Pre-training and fine-tuning are synonymous and used interchangeably

9.Which of the following techniques can be employed to extract memorized text from Large Language Models (LLMs)?

    A. Probing tasks involving specific tests or tasks
    B. Increasing the temperature parameter during decoding
    C. Applying Laplace smoothing to the model's probability estimates

D. Fine-tuning the model on random unrelated data

10. Which defensive strategy is widely recognized for its effectiveness in countering membership inference attacks by obscuring information?

A. Introducing random noise to the model's predictions
B. Employing dropout regularization during training
C. Utilizing advanced encryption techniques on model parameters
D. Implementing privacy-preserving mechanisms like differential privacy

11. Which discounting method involves redistributing probability mass from frequent n-grams to unseen or less frequent ones?

A. Katz back-off
B. Kneser-Ney smoothing
C . Witten-Bell smoothing
D . Laplace (add-on smoothing)

12. What is the purpose of the time step parameter in an RNN?

A. To determine the number of recurrent layers in the network
B. To adjust the learning rate during training
C. To specify the length of the input sequence
D. None of the above

13. What is the significance of the “attention mechanism” in transformer-based LLMs?

A. It controls the learning rate during training
B. It determines the number of layers in the network
C. It decides the batch size for training
D. It allows the model to focus on specific parts of the input sequence when making predictions

14. How does GPT-3 typically generate text output?

A. By memorizing and regurgitating predefined responses
B. By applying deterministic rules and heuristics
C. By sampling from a probability distribution over words, using a combination of learned patterns and context to generate text
D. By performing keyword-based searches on the internet

15. . What is “knowledge distillation” in the context of Large Language Models ?

A. The process of extracting knowledge from a human teacher and transferring it to an LLM
B. A technique for increasing the model's capacity by adding more layers
C. The process of converting LLM-generated text into a distilled, shorter form
D. A method for training smaller models to mimic the behavior of a larger pre-trained LLM by transferring its knowledge

16. When designing prompts for a language model, which of the following is the most important consideration for addressing bias and fairness issues?

A. Ensuring that prompts contain explicit constraints on model behavior
B. Incorporating comprehensive demographic information in prompts
C. Crafting prompts that are free of cultural and gender-specific references
D. Implementing post-processing filters to modify model outputs

17. Which activation function is commonly used in the recurrent layers of an RNN?

A. ReLU (Rectified Linear Unit)
B. Tanh (Hyperbolic Tangent
C. Sigmoid
D. Softmax

18. How does GPT-3 typically generate text output?

A. By memorizing and regurgitating predefined responses
B. By applying deterministic rules and heuristics
C. By sampling from a probability distribution over words, using a combination of learned patterns and context to generate text
D. By performing keyword-based searches on the internet

19. Which of the following is NOT a typical component of the reinforcement learning process?

A. Environment
B. Feature engineering
C. Reward
D. Agent

20. What is “few-shot learning” in the context of LLMs?

A. Learning with only a small amount of data
B. Learning with a small number of input features
C. Learning with a small learning rate
D. A technique for fine-tuning pre-trained models

Theory based Questions [5 marks x 4 Questions]
Answer any 4 Questions

21. Explain the Membership Inference in LLMs. .

22. Explain Smoothing and Discounting Techniques .

23. Write down the risk of Large language models with respect to its downstream applications .

24. Explain the Misalignment of Models using different methods .

25. Explain StereoSet Dataset , Significance with Real world examples .
26. How to extract Memorized Text in LLMs ?
27. How can bias be mitigated with human-in-the-loop approaches when developing LLMs?

Reasoning based Questions [10 marks x 1 Questions]
Solve any 1 Questions

Hint: Discuss how the model can leverage ML, NLP, and HCI techniques to achieve the required goal with reasoning to back your claims. Discuss the importance of each component used such as why RLHF is necessary or unsupervised learning and so on. Do not skip the explanation for the finetuning or prompt engineering used in your proposed method.

28. Design a Multimodal LLM for personalized workout routine generation. Explain in detail the (i) Methodology (ii) Experimentation and (ii) Testing of the proposed model. Lastly, explain in what situations, if any, the system can fail.
29. Design a Multimodal and Multilingual LLM for personalized learning in education using RLHF. Explain in detail the (i) Methodology (ii) Experimentation and (ii) Testing of the proposed model. How can this system be used to enhance educational outcomes? Lastly, discuss the potential challenges of this approach in improving personalized learning experiences for students.