- 1. Prompt engineering is a challenging yet crucial task for optimizing the performance of large language models on customized tasks. It involves crafting input prompts that guide the model to produce desired outputs, incorporating complex reasoning and analysis of model responses. Effective prompt engineering can significantly enhance the accuracy and appropriateness of LLM responses across numerous applications.
- 2. Prompt injection refers to manipulating the input prompts given to language models to alter their behavior or outputs. Such manipulation can lead to unpredicted results, which can be categorized into different types like adversarial injection, which targets vulnerabilities in models; context injection, which can mislead the model; and instruction injection, which redirects model functionality or intent.
- **3.** RAG provides access to extensive external data sources, ensuring updated and relevant content in generated outputs. The system combines retrieval techniques with generation, thus improving accuracy and context-awareness in responses. This dual approach enables LLMs to leverage real-time information, making them more robust.
- **4.**The ReAct (Reasoning and Acting) framework comprises components that facilitate decision-making: reasoning prompts guide the model through critical analysis before response generation, while action prompts drive the model to perform specific tasks based on the reasoning provided. Feedback mechanisms also enhance learning from past interactions, allowing continuous improvement in response quality.
- **5.** Dense retrieval offers more accurate information retrieval by utilizing vector representations for better semantic matching compared to the term-based approach of sparse retrieval. This allows for improved relevance in query responses and a speedier query processing experience, which are significant for efficient model performance.
- **6.** In top-k sampling with k=3, the candidate words from the provided distribution are Word C (0.45), Word D (0.20), and Word A (0.15) as they represent the highest probabilities.
- **7.** For top-p sampling with p=0.7, the smallest candidate set includes Word A (0.45), Word B (0.25), and Word C (0.15), as their cumulative probability equals 0.45+0.25+0.15=0.85, exceeding the threshold.

- **8.** The temperature setting affects the randomness and diversity of generated outputs by controlling the sampling process. A higher temperature results in more diverse and creative responses, whereas a lower temperature tends to lead to more deterministic and focused outputs.
- **9.** Chain-of-Thought (COT) prompting enhances reasoning capabilities compared to ZERO-SHOT. COT guides the model to explicitly outline its reasoning process, leading to more structured and logically coherent outputs, especially during complex tasks.
- **10.** Auto-COT automates the reasoning structure in prompts, streamlining the process and reducing human effort involved in prompt creation. This can lead to more consistent response quality while ensuring efficient utilization of model capabilities.
- **11.** Meta prompting, which involves generating prompts that adapt based on context or task requirements, enhances the flexibility and user-friendliness of interaction with LLMs. This adaptability allows for more tailored and effective responses based on user needs.
- **12.**For creative writing, experimentation with higher temperature settings (e.g., between 0.7 and 1.0) can foster diversity and innovation in outputs. Additionally, setting a moderate top-k value (e.g., 5-10) balances variety while maintaining relevance. This combination encourages lively and imaginative text generation without sacrificing quality.