Study Assistant - Summary & Quiz

Summary

Prompt Engineering Summary:

I. Introduction to Prompt Engineering:

* Prompt engineering optimizes prompts (instructions & context) to efficiently use Language Models (LLMs) for various tasks.

* It's a crucial skill for AI engineers and researchers.

* Prompts consist of instructions, context, input data, and an output indicator.

* Decoding parameters (temperature & top_p) control the randomness and repetitiveness of LLM responses. Lower values yield more deterministic, less creative outputs.

II. Prompt Engineering Techniques for Different Tasks:

* **Text Summarization:** Condensing text into concise summaries.

* **Question Answering:** Extracting answers from provided context.

* **Text Classification:** Categorizing text (e.g., sentiment analysis).

* **Role Playing:** Simulating conversations with specific personas.

* **Code Generation:** Generating code snippets based on instructions.

* **Reasoning:** Solving problems requiring logical steps.

III. Advanced Prompt Engineering Techniques:

* **Few-shot prompting:** Providing examples within the prompt to guide the LLM.

* **Chain-of-thought (CoT) prompting:** Instructing the model to reason step-by-step. Zero-shot CoT adds "Let's think step by step" to the prompt.

* **Self-Consistency:** Sampling multiple reasoning paths and selecting the most consistent answer.

* **Knowledge Generation Prompting:** Generating and incorporating knowledge into the prompt to improve complex reasoning.

* **Program-aided Language Models (PAL):** Using LLMs to generate programs as intermediate reasoning steps, offloading execution to a runtime.

* **ReAct:** LLMs generate reasoning traces and actions interleaved, allowing interaction with external tools and knowledge bases.

* **Directional Stimulus Prompting:** Using a policy LM to generate hints guiding a frozen LLM to produce desired summaries.

IV. Risks of Prompt Engineering:

* **Prompt Injection:** Hijacking LLM output by injecting malicious commands.

* **Prompt Leaking:** Forcing the model to reveal information about its own prompt.

* **Jailbreaking:** Bypassing safety and moderation features to elicit undesirable responses.

Quiz Questions

Q: Which of the following is NOT a core component of a prompt in prompt engineering?

A. Instructions

B. Output indicator

C. Decoding parameters

D. Input data

Answer: C. Decoding parameters. Decoding parameters (temperature and top_p) influence the *generation* of the LLM response, not the core structure of the prompt itself.

Q: Which advanced prompt engineering technique involves guiding a language model to reason step-by-step, potentially adding a phrase like "Let's think step by step" to the prompt?

A. Self-Consistency

B. ReAct

C. Chain-of-Thought (CoT) prompting

D. Knowledge Generation Prompting

Answer: C. Chain-of-Thought (CoT) prompting. The description directly matches the definition of Chain-of-Thought prompting.