Mastering LLMs

Lecture 11: Prompt Engineering

Harito

September 15, 2025

Recap: LLMs and Their Capabilities

In previous labs, we've seen LLMs can generate text, summarize, and answer questions.

- They possess vast knowledge learned during pre-training.
- They can follow instructions.

But how do we get them to perform *exactly* what we want, especially for complex tasks?

What is Prompt Engineering?

Definition

Prompt Engineering is the art and science of crafting effective inputs (prompts) to guide Large Language Models (LLMs) to generate desired outputs.

It's about communicating with the LLM in a way that maximizes its potential for a given task.

Why is it important?

- Unlocks complex capabilities without fine-tuning.
- Improves accuracy and relevance of outputs.
- Essential for building LLM-powered applications.

Chain-of-Thought (CoT) Prompting

CoT prompting encourages the LLM to show its reasoning steps before providing the final answer.

Why it works:

- Allows the LLM to break down complex problems into smaller, manageable steps.
- Improves accuracy for multi-step reasoning tasks (e.g., math word problems, logical puzzles).
- Makes the LLM's thought process more transparent.

Example Prompt (for a math problem): "Let's think step by step. [Problem description]"

Role-playing and Persona Prompting

You can instruct the LLM to adopt a specific role or persona.

Example

"You are a helpful customer service agent. Respond to the following customer complaint: [Complaint text]"

Benefits:

- Guides the tone, style, and content of the LLM's response.
- Useful for chatbots, content creation, or simulating different perspectives.

Best Practices for Prompt Design

- **Be Clear and Specific**: Avoid ambiguity. Use precise language.
- **Provide Context**: Give the LLM all necessary background information.
- **Use Delimiters**: Clearly separate instructions from context or examples (e.g., XML tags).
- **Specify Output Format**: Ask for JSON, bullet points, a specific length, etc.
- **Iterate and Refine**: Prompt engineering is often an iterative process of trial and error.
- **Break Down Complex Tasks**: For multi-step problems, guide the LLM through each step.

Next Steps

Time for Lab 11!

Objective:

- Implement few-shot classification.
- Design prompts for Chain-of-Thought reasoning.
- Experiment with role-playing prompts.