Prompt Engineering

Take Home Exercise Review

Have a conversation with ChatGPT and Google Gemini.

- Try asking the model the same question multiple times.
- Try asking the same question to both models.
- Try asking the model a broad question and then a detailed question.
- Are the any noticeable differences between the responses?

Identifying undesirable responses

The current AI systems are impressive and helpful, but they do have some faulty/undesirable responses which can minimize their effectiveness.

- **Generation failure - When the AI doesn't produce a response due to a timeout or internal issue.**
- **Hallucinations - When an AI generates inaccurate, biased, or otherwise unintended information as a response.**
- **Safety responses - When an AI generates a formulaic safety response instead of responding to the prompt.**
  - **Most AI models have safety guardrails to prevent it from generating harmful information.**

What is Prompt Engineering?

- **Prompt engineering is a way to guide AI to generate desired responses.**
  - **This is done by optimizing the input prompt.**
- **This helps reduce the risk of hallucinations and improves the efficiency of the AI model.**
- **The more experience you have with AI models, the better you will get at creating prompts that invoke the model to respond the way you want.**

Prompting Best Practices

- **Specificity: The more specific the prompt, the better the AI can understand what is wanted and tailor its response.**
- **Context: Give the AI relevant information and context to work with. This can include background information, datasets, or even a desired perspective to have when responding.**
- **Desired Output: Directly ask for the kind of response you want. Is it creative writing, or is it a factual summary? Response format can also be specified.**

Exercise

Look at the Home Practice of last class and come up with 3 examples of making the prompts more effective.

Prompt Engineering Techniques

Chain-of-Thought Prompting

Break down complex tasks into a series of steps (all in one prompt), allowing the AI to reason through the problem.

Meta-Prompting

Creating a universal prompt that can be adapted to various tasks with minimal changes.

Few Shot Prompting

Supplying example prompt and response pairs for the AI to understand the task better and follow the output format.

Least to Most Prompting

Start with a broad prompt and gradually add details to refine the AI's answer.

Iterative Prompting

Refine your prompt based on the AI's initial responses to get progressively better results.

Where do we implement prompt engineering?

- **Input (prompt) text box - [Chat GPT](#)**
- **System message - [OpenAI Playground](#)**
- **Langchain API - [Input](#)/[Output](#) Formatting**

Walkthrough using OpenAI Playground

Exercise

Have students use the OpenAI Playground and build a helpful system message for a better response.

- What are the characteristics of the response that we value?
- What belongs in the user prompt and system message?

Take Home Exercise

1. Use OpenAI Playground to build an AI assistant that generates a summary of a book.
2. Use the system message to focus on specific elements and properly format the response.
3. Save and share the preset link.