Hochschule Konstanz
Fakultät Elektrotechnik
und Informationstechnik

Prompt engineering as an essential competency for modern engineers

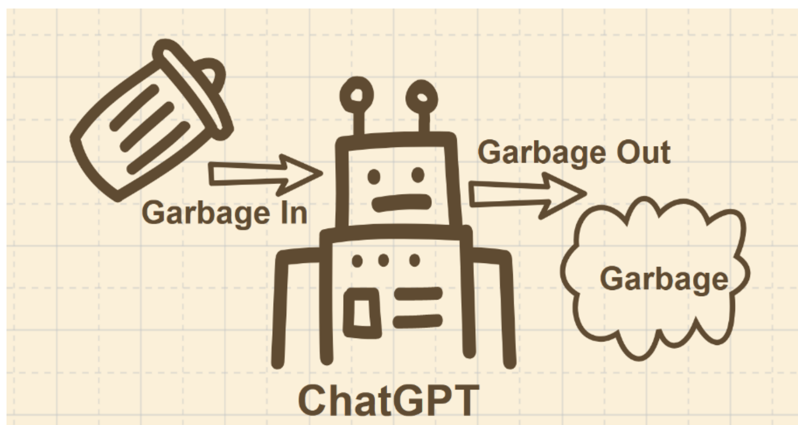
Jonas Woerner, Chin-I Feng

Content

Introduction

Purpose of the Research:

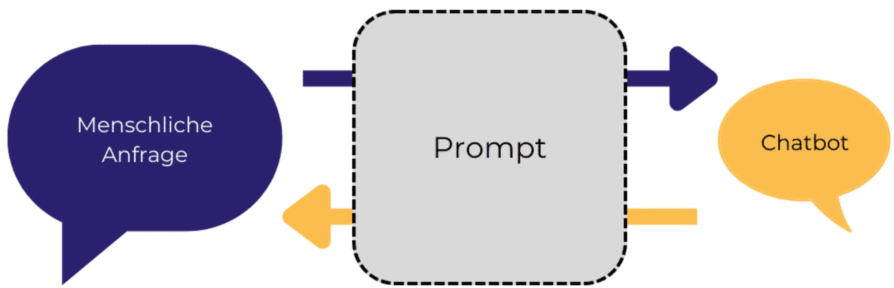
- It focuses on Prompt Engineering, a method to make Large Language Models (LLMs) work better by designing good prompts.
- Particularly in applications of Generative AI.
- Demonstrate how well-designed prompts improve the performance of LLMs.



Introduction

Why is this important?

- LLMs like ChatGPT (OpenAI) and LaMDA (Google) are powerful tools, but their results depend on how people ask questions or give instructions.
- Prompt Engineering helps connect what the user wants with what the model can do, making tasks faster and more accurate.



Source: Srivastava/Rastogi/Rao et al., 2022

Introduction

Main Questions:

- Why should engineers learn Prompt Engineering?
- How can a well-crafted prompt improve the quality of LLM outputs?

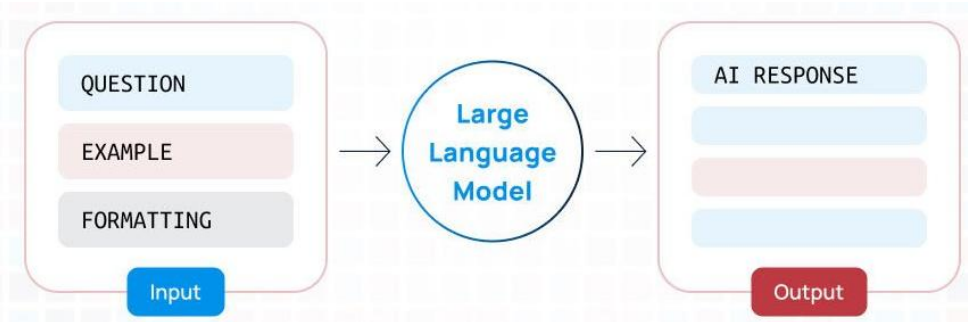
How we answered these questions:

1. Searched Google Scholar using keywords such as: *"Prompt Engineering", "Large Language Models"*, *"Prompt Optimization".*
2. Categorized papers based on their relevance to the research questions.
3. Consolidated results into a structured summary.

Prompt Engineering

Definition:
- Prompt Engineering is the process of creating and improving prompts (Inputs) to guide LLMs to produce the results (Outputs) you want.
- It helps users make LLMs work better for specific tasks without needing to train or change the model itself (fine-tuning).

Applications:
- Code Generation
- Text Summarization



Source: Zhou/Muresanu/Han et al., 2022

Prompt Engineering

Who can use this?

- **Software Engineers:** Create optimized prompts for generating clean, maintainable code or ensuring compliance with coding standards.
- **Data Scientists:** Use prompts to structure data analysis and extract meaningful insights from large datasets.
- **Machine Learning Engineers:** Design prompts for effective integration of LLMs into AI pipelines, reducing development time for specific tasks.

Two primary methods:

- In-Context Learning
- Step-by-Step Reasoning

In-Context Learning

Concept

Definition:

- A technique where LLMs learn tasks directly from examples provided in the input prompt, without requiring additional training.

How it works?

- LLMs interpret patterns in the prompt examples (input-output pairs) and generalize these to predict new outputs.

Analogy:

- Like a well-trained chef using a recipe to cook a new dish, leveraging prior experience to interpret instructions in the moment.

Source: Dong/Li/Dai et al., 2022

In-Context Learning

Flipped-Label Experiment

Setup:

- Models were given prompts with incorrect labels in the examples, creating a conflict with the model's prior knowledge (what the model knows).
- The goal of this experiment was to test how prompts with incorrect examples affect the model's performance.

Result:

- The more incorrect examples in the prompt, the lower the model's accuracy.

Findings:

- Accuracy depends on the proportion of incorrect examples in the prompt.

Source: Wei/Tay/Tran et al., 2023

In-Context Learning

Structured Datasets Experiment

Setup:

- Models were given numerical vectors as inputs, each matched to a specific category (output).
- Prompts included examples of inputs and their correct outputs to guide the model.
- The goal was to test if the model could predict correct outputs for unseen inputs.

Result:

- Clear and structured examples improved the model’s classification accuracy.

Findings:

- Well-designed prompts help models handle classification tasks more effectively.

Source: Wei/Tay/Tran et al., 2023

Step-by-Step Reasoning

Concept

Definition:

- A method where LLMs break down complex tasks into smaller, logical steps within a prompt, enabling them to handle multi-step problems effectively.
- Also known as Chain-of-Thought (CoT) Learning.

How it works?

- The model follows a structured reasoning process, interpreting each step outlined in the prompt to arrive at a final solution.

Analogy:

- Like solving a math problem step by step, where each calculation builds on the previous one to ensure the correct answer.

Source: Wei/Wang/Schuurmans et al., 2022

Step-by-Step Reasoning

Math-Solving Experiment

Setup:

- Benchmarks tested with math word problems requiring multi-step reasoning.
- Compared two methods:
  - Standard Prompting (Directly asks for answers)
  - CoT Prompting (Solves problems step by step)

Result:

- Step-by-Step Reasoning significantly outperformed Standard Prompting, especially for larger models.

Findings:

- Step-by-Step Reasoning enhances multi-step reasoning capabilities by guiding the model through structured logical steps.

Source: Wei/Wang/Schuurmans et al., 2022

Discussion

In-Context Learning

Challenges:

- Risk of exposing sensitive information when including proprietary functions or code snippets in prompts.
- Dependence on high-quality prompts to ensure accurate outputs, requiring careful crafting and domain-specific knowledge.

Potential Solutions:

- Develop tools to anonymize sensitive data in prompts automatically.
- Create templates for standard use cases to simplify prompt crafting.

Discussion

Step-by-Step Reasoning

Challenges:

- Requires users to manually break down complex tasks into smaller subtasks, which can be cognitively demanding.
- In some cases, developers must have a deep understanding of the problem to construct effective reasoning chains.

Potential Solutions:

- Introduce AI-assisted tools to guide users in breaking tasks into smaller steps.
- Use visual aids or automated suggestions to simplify reasoning chain creation.

Conclusion

Summary of Findings:

- In-Context Learning enables models to generalize from examples without additional training.
- Step-by-Step Reasoning helps LLMs solve complex problems by breaking them into logical steps.

Future Directions:

- Explore ways to automate and optimize prompt design for greater efficiency.
- Focus on improving data security when using In-Context Learning in sensitive domains.
- Develop tools to simplify task decomposition for Step-by-Step Reasoning, making it more accessible to users.

Takeaway Message:

- Effective Prompt Engineering bridges the gap between human intent and LLM capabilities, making it a crucial skill for engineers and researchers in the era of AI.

Thank you!

References

- A. Srivastava, A. Rastogi, A. Rao, A. A. M. Shoeb, A. Abid, A. Fisch, and G. Wang et al., “Beyond the imitation game: Quantifying and extrapolating the capabilities of language models,” arXiv preprint arXiv:2206.04615, 2022.
- Y. Zhou, A. I. Muresanu, Z. Han, K. Paster, S. Pitis, H. Chan, and J. Ba, “Large language models are human-level prompt engineers,” arXiv preprint arXiv:2211.01910, 2022.
- Q. Dong, L. Li, D. Dai, C. Zheng, J. Ma, R. Li, and Z. Sui et al., “A survey on In-context learning,” arXiv preprint arXiv:2301.00234, 2022.
- J. Wei, Y. Tay, D. Tran, A. Webson, Y. Lu, and T. Ma et al., “Larger language models do In-context learning differently,” arXiv preprint arXiv:2303.03846, 2023.
- J. Wei, X. Wang, D. Schuurmans, M. Bosma, F. Xia, E. Chi, and D. Zhou et al., “Chain-of-thought prompting elicits reasoning in large language models,” arXiv preprint arXiv:2201.11903, 2022.

Source of Figures

- https://blog.iamwajidkhan.com/p/what-is-chatgpt-and-how-it-works
- https://datasolut.com/was-ist-prompt-engineering/
- https://cloudkitect.com/why-prompt-engineering-is-useful-for-generative-ai-models/