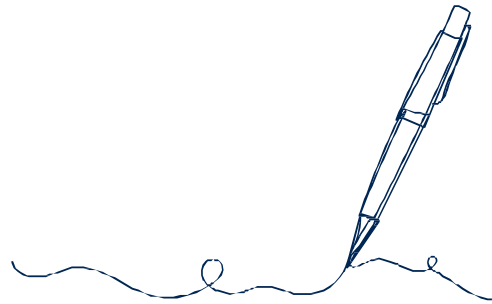
Prompt-Engineering

Large Language Models
Introduction

- A type of deep learning model designed to process and understand natural language data (NLP).
- Called „*large*“ since they are trained on large amount of data.
- **Generativ AI** vs. **Large Language Models**
  - Gen AI: is a special type of AI that generates new information (images, videos, text, …)
  - Gen AI encompasses various types of different models (image, text, videos, … -generation)
  - LLMs belongs to the class of Gen AI and focus on natural language processing (NLP)
- They are built on the **Transformer** neural network architecture.
- Introduced in 2017 by Google.
- Becomes popular in 2022(23) since ChatGPT was released.

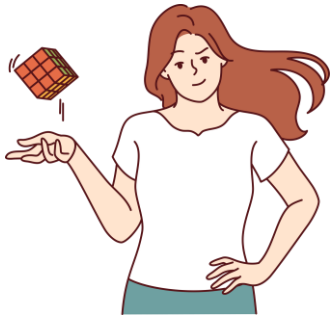
Role of Prompts in GenAI

What is a Prompt?



- Input to an AI model in natural language
  - AI model understands query semantically
  - Then performs desired task

  → *keyword searches are NOT prompts*
- Via text interface, API, ...or microphone
- Sequence of prompts: *Prompt Chains!*



Benefits & Limitations

- Describe tasks in NL
  → *precisely & creatively*
- No expert skills needed
  → *e.g. Boolean; Code*
- Multi-lingual inputs

- Limited no. words per prompt
- Limited prompts per chain
- Lack of transparency
- Lack of repeatability

…many more

What is Prompt Engineering?

= Craft of guiding GenAI to produce desired outcomes, efficiently using natural language instructions.

- Foundational AI literacy skill
- Synonyms: Prompting; Prompt Design

5 Purposes:

- 1: Maximize consistency; improve reliability & repeatability
- 2: Leverage an AI model's sophisticated capabilities
- 3: Individualize GenAI outcomes → from generic to specific
- 4: Address GenAI-related pitfalls
- 5: Safety-tests; Jailbreaking

What is Prompt Engineering?

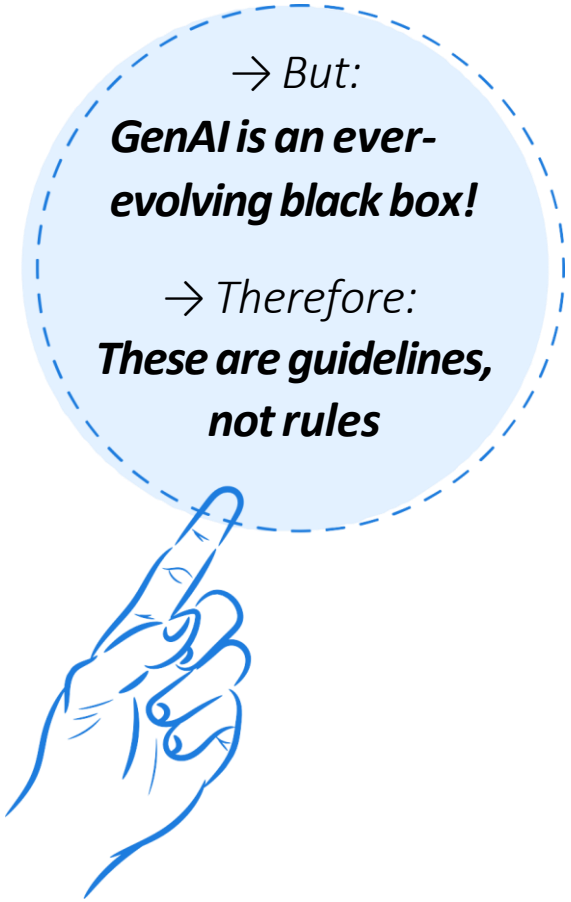
Role of Prompts in GenAI

= Craft of guiding GenAI to produce desired outcomes, efficiently using natural language instructions.

- Foundational AI literacy skill
- Synonyms: Prompting; Prompt Design

5 Purposes:

- 1: Maximize consistency; improve reliability & repeatability
- 2: Leverage an AI model's sophisticated capabilities
- 3: Individualize GenAI outcomes → from generic to specific
- 4: Address GenAI-related pitfalls
- 5: Safety-tests; Jailbreaking



7 Principles For Good Prompt Design

0

Most important one?

Be creative & have fun!

1 Be concise.

- Aim for brevity & clarity
- Use language that is as simple as possible

- **Cluttered prompt & question format**

  "Can you provide me with a detailed explanation of the photosynthetical process and the significance of this biochemical reaction?"

- **More concise prompt & instructive format**

  "Explain the process of photosynthesis and its significance in detail."

2 Be clear.

- Avoid vague & ambiguous wording
- Be as specific as necessary

- **Prompt in ambigious wording and question format:**

  "How do I produce a paper?"

- **Clearer, less ambigious and imperative format:**

  "Explain the common steps of writing a research paper for a peer reviewed academic journal."

3 Include context & logical structure.

- Provide context to improve reasoning
- Build structured & coherent prompts

- **Unstructured prompt without context:**
  "Mention tasks involved in writing a research paper."

- **Structured prompt, including context:**
  "List the steps involved in writing a research paper for a student assignment. Begin with selecting a topic, end with proofreading the final draft."

4 Break down complex tasks.

In one prompt, avoid...

- combining several tasks
- asking for various formats

Divide multi-step or -topic tasks...

- into separate prompts
- or prompt chains

EXAMPLE

*"**Design** a comprehensive marketing campaign for a new eco-friendly product, detailing the target audience, key messaging, and promotional strategies. **Provide specific examples** of advertising mediums such as social media, print, and television, and create a visual mockup of an advertisement in a modern minimalist style. **Write** meaningful alt-text for the advertisement, summarizing its content for enhanced accessibility. Finally, **draft** a 2-minute pitch script for presenting this marketing campaign to potential investors."*

5 Specify desired output.

- Style & tone
- Depth & length
- Format, language, or content type
- Temperature → controls precision & creativity

- **Style & Tone:**
  "Draft a paragraph on XYZ in the simplistic style of a tabloid paper. Use a sensational tone."
- **Depth & length:**
  "Provide a high-level legal argumentation on the topic of XYZ that does not exceed 500 words."
- **Format, language, content type:**
  For example: A three-column table; a poem in Swahili; a script in Python
- **Temperature:**
  Balance creativity & precision, depending on task

6 Reflect & adapt your approach.

- Continuously evaluate outcomes
- Be flexible, fine-tune, & improve
- Adjust, then re-run!

- By applying the other principles
- By using a different prompting technique

→ *No improvement? Even with adjustments? ---* ***Start fresh!***

7 Combine these principles.

- These principles complement each other
- Mix and match modularly for optimum results

- **Earlier example, already improved (tone and style):**

"Draft a paragraph on climate change in the simplistic style of a tabloid paper. Use a sensational tone."

- **Improved further: clarity, context, temperature, length:**

"Draft a newspaper paragraph of 500 words including a headline, on the effects of climate change. Apply the simplified grammar of a tabloid paper, and use sensational language. Be creative when describing climate change's effects."

Framework for effective Prompts

Goal

For what you want to use the LLM

„summarize the following document“

+

Context

Context information of the Goal?

„…with a brief overview of the key points that I will discuss with my team during tomorrow's sales meeting…“

+

Sources

"Which information or examples should be used by the LLM?"

„…the section about the competition analysis.“

+

Response Format

How should the LLM best respond to your request?

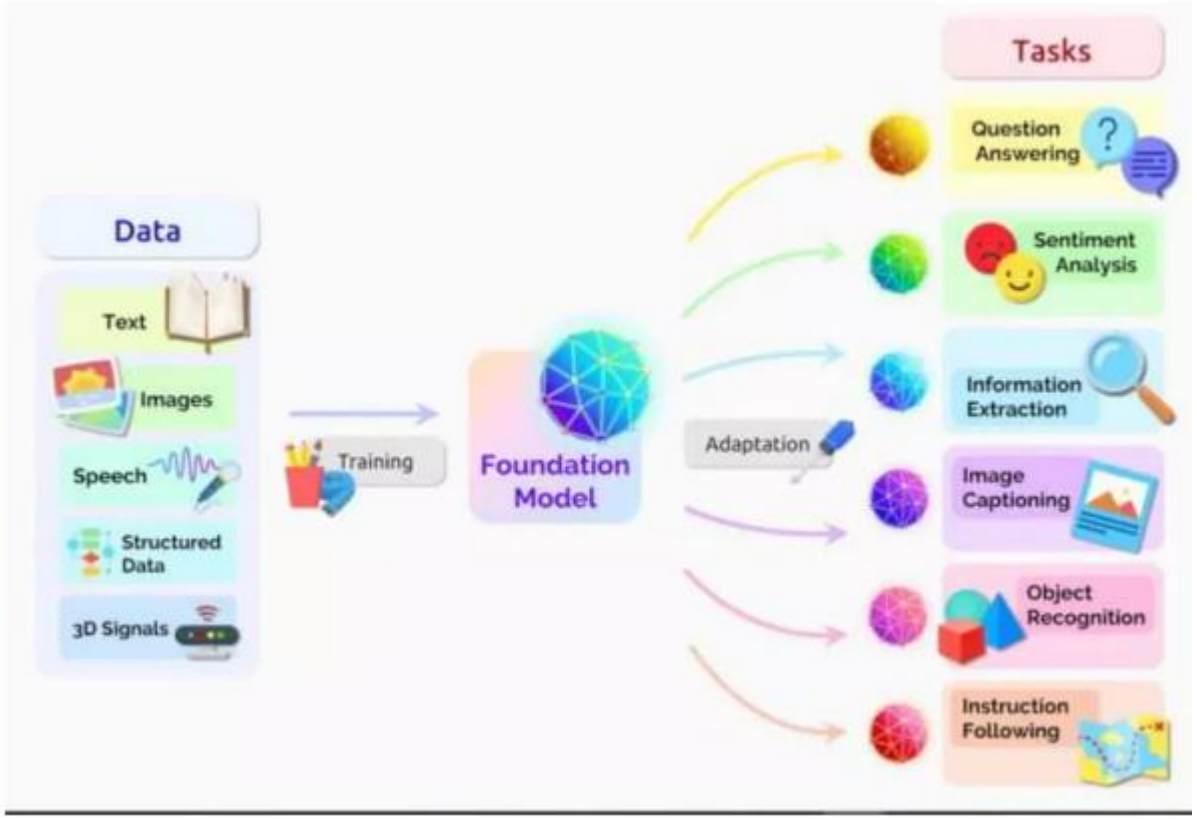
„Please limit the summary to 5 key points and use simple language.."

=

Final Prompt

Summarize the following document with a brief overview of the key points that I will discuss with my team during tomorrow's sales meeting focus on the section about the competition analysis. Please limit the summary to 5 key points and use simple language.

Large Language Models
Transformer Architecture



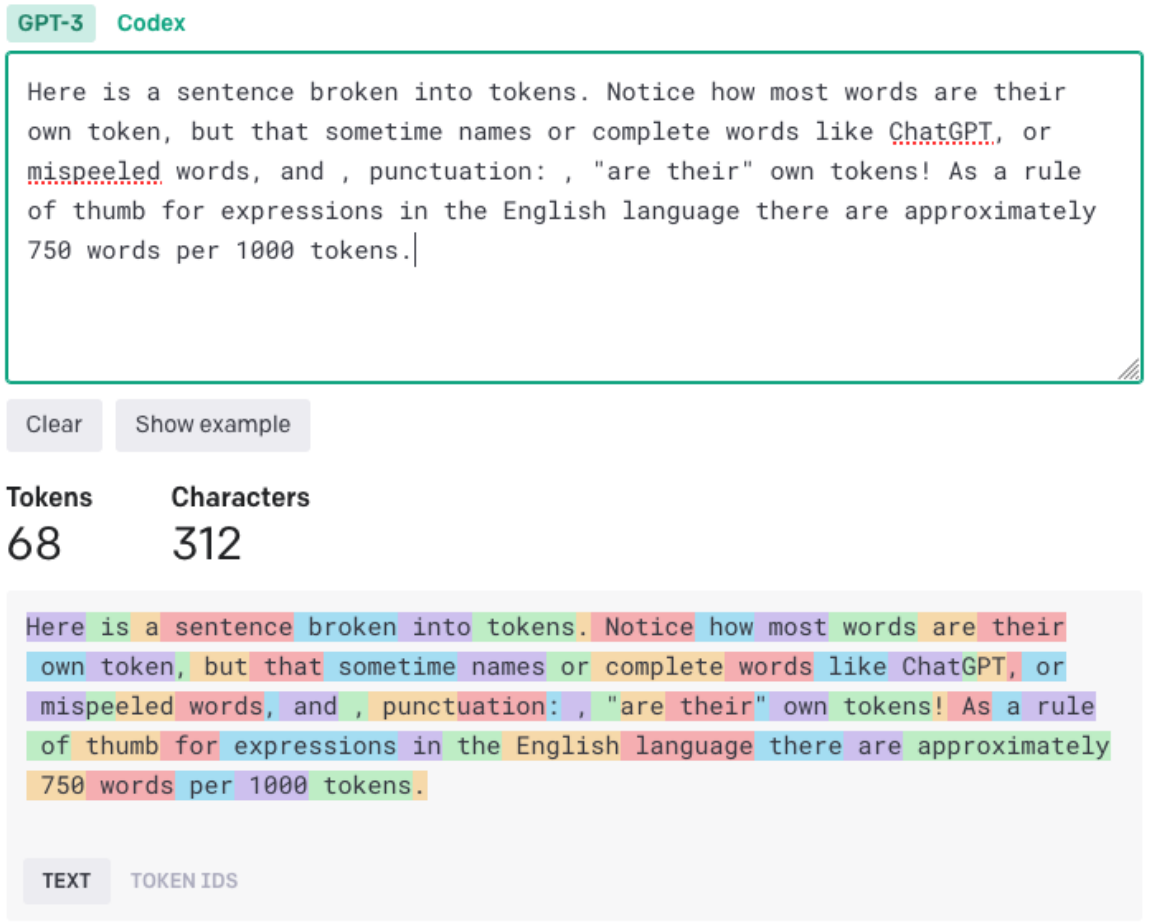
- A Transformer model is a
  - Neural network that learns context and thus meaning by tracking relationships in sequential data like the words in sentences.

- Transformer models apply an evolving set of mathematical techniques, called attention or self-attention,
  - to detect subtle ways even distant data elements in a series influence and depend on each other

Large Language Models
Token Limit

- Token limits limit the input per prompt.

- Not a real issue anymore:
  - **GPT 5.x** (and mini): 400,000 tokens (272k input + 128k output)
  - **Claude** code 200K tokens
  - **Gemini** pro 1 million tokens

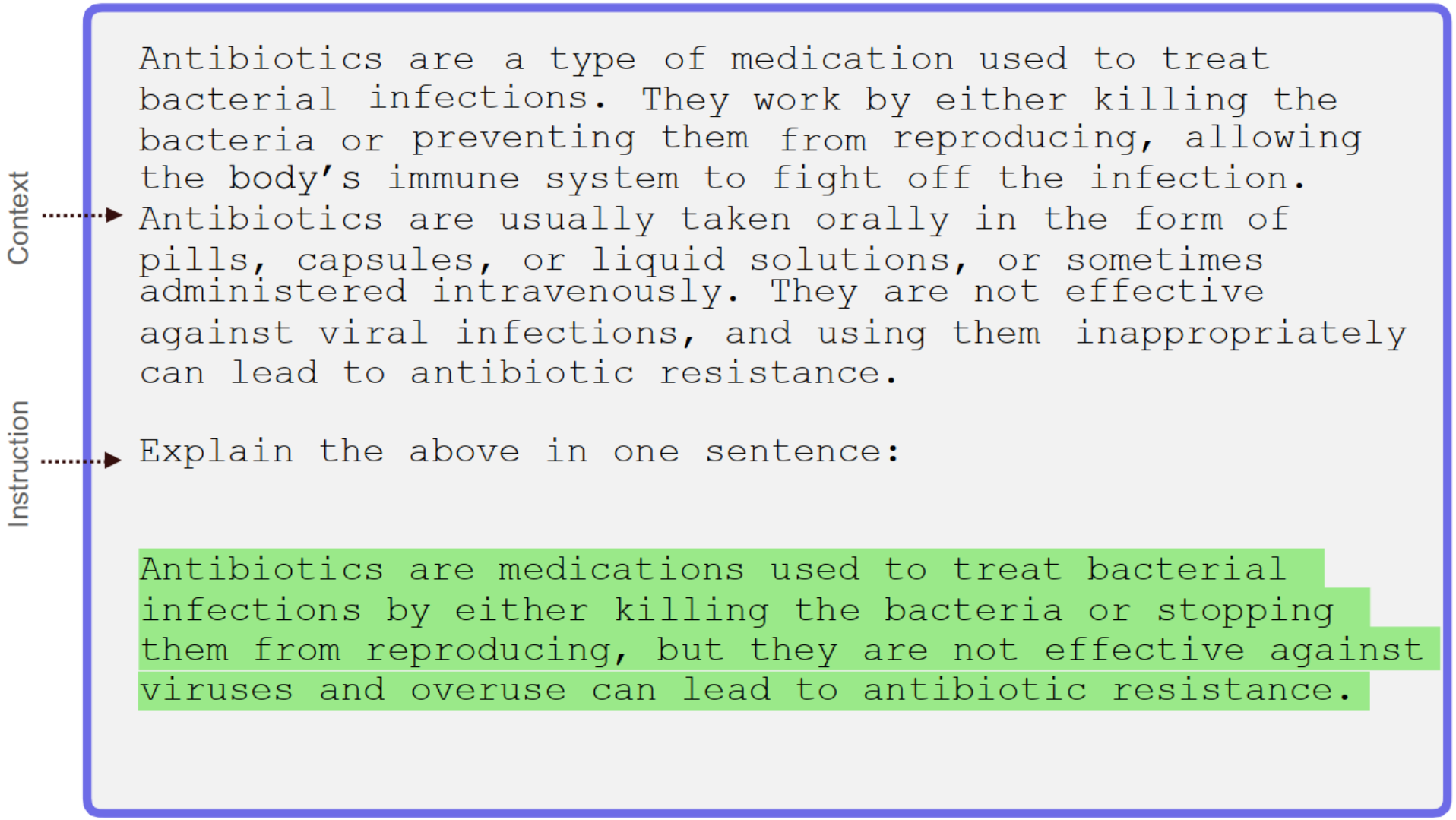


Basics
Different Prompts for Different Tasks

- In the next few slides, we will cover a few examples of common tasks using different prompts.
- **An LLM is not deterministic!**

- Tasks covered:
  - Text Summarization
  - Question Answering
  - Text Classification
  - Role Playing
  - Code Generation
  - Reasoning

Basics
Text Summarization



Lab

- Open the test application at lab-s1
- Ask Copilot chat about
  - the purpose of the software suite,
  - what tools are used,
  - what website is used/tested,
  - what's settings/dependencies are required to run the software suite,
  - what steps are required to run it,
  - … anything you need to know to be able to start.
- Go further until you understand what the solution is doing and the solution is started successfully.

Basics
Question Answering

```
Answer the question based on the context below. Keep the
answer short and concise. Respond "Unsure about answer"
if not sure about the answer.

Context: Teplizumab traces its roots to a New Jersey drug
company called Ortho Pharmaceutical. There, scientists
generated an early version of the antibody, dubbed OKT3.
Originally sourced from mice, the molecule was able to
bind to the surface of T cells and limit their cell-
killing potential. In 1986, it was approved to help
prevent organ rejection after kidney transplants, making
it the first therapeutic antibody allowed for human use.

Question: What was OKT3 originally sourced from?

Answer: Mice.
```

Lab

- Ask Github Copilot where the **Gherkin** definitions are located.
- Ask how the definitions are applied to the system under test.

- Ask what steps are required to add own/more **Gherkin** definitions.

Basics
Text Classification

```
Classify the text into neutral, negative or positive.

Text: I think the food was okay.

Sentiment: Neutral
```

Lab

- Ask Copilot what his opinion to the test suite is and classify is between good, ok, worst.

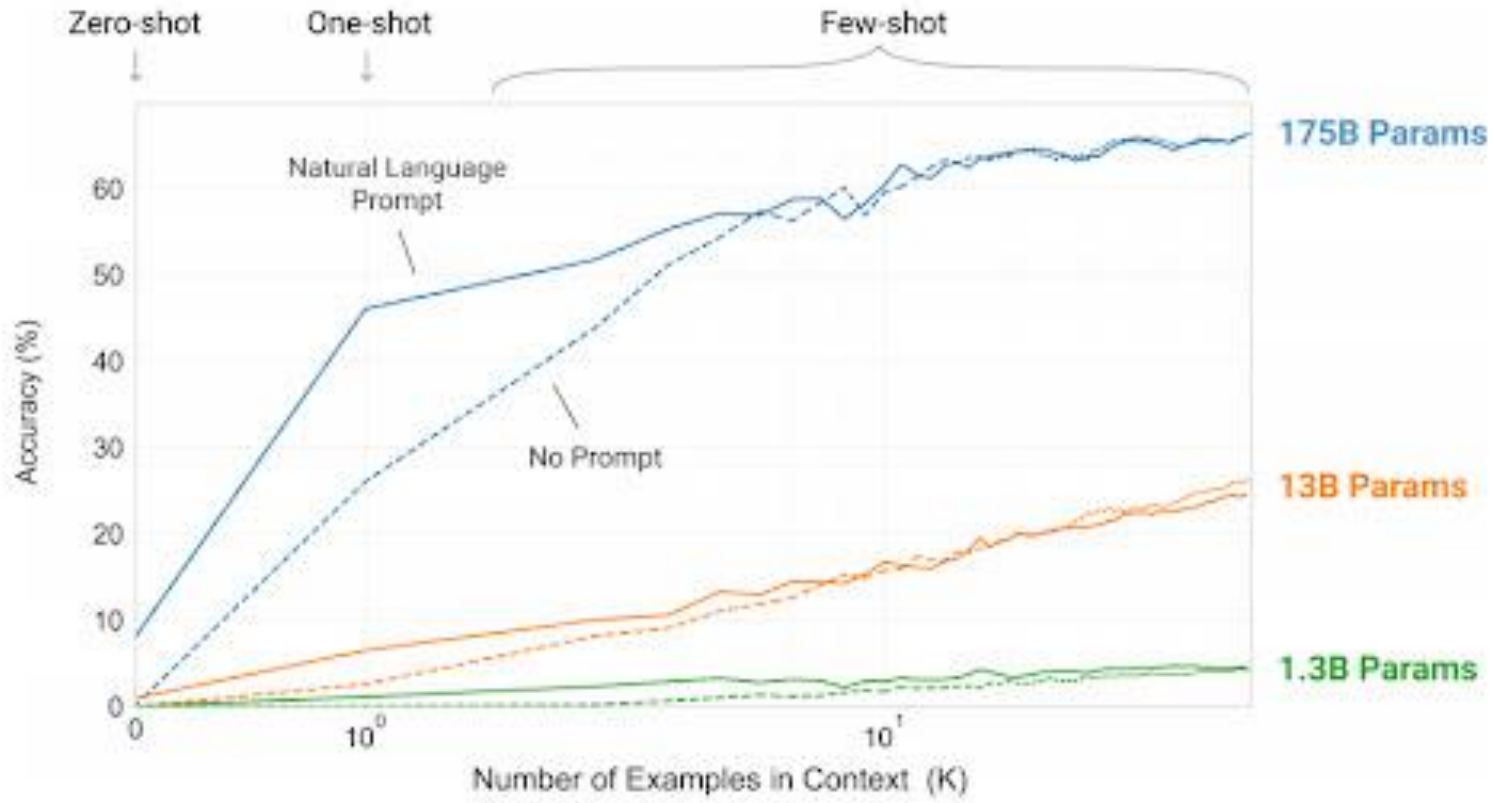
- Ask further what can be explicitly be improved.
- Tell Copilot to implement some/all of the recommendations.

- Review what has been created and build yourself an opinion.

Techniques
Introduction

- Many prompting techniques have been designed to improve performance on complex tasks.
  - Zero-shot prompts
  - One-shot prompts
  - Few-shot prompts
  - Prompt-Chaining
  - Chain-of-thought (CoT) prompting
  - Ask before Answering
  - Activate Creativity
  - Using Different Perspectives
  - Constructive Critic Prompting
  - Self-Consistency
  - Knowledge Generation Prompting
  - Directional Stimulus Prompting
  - …

Basics
Context and Accuracy



- As more context you provide in the input, as better the transformer can derive the context.
- As more „shots“/prompts you provide, as more accurate the result will be.

Techniques
Chain-of-Thought (CoT) Prompting

- Technique to guide the LLM to explain its answers in a step-by-step manner.
- Helps to gain transparency of the answering process.

- Prompt Formula
  - *[Your question]*. Let's think step by step.
- Examples
  - What is the diameter of the sun? Let's think step by step.
  - What is the weight of an oxygen molecule? Let's think step by step.

Basics
Chain of Thought

Before

What is the annual water demand of a single-family household containing four people who are at home an average of 200 days per year and use an average of 100 liters of water per day?

The annual water demand of a single-family household containing four people who are at home an average of 200 days per year and use an average of 100 liters of water per day is 8,000,000 liters per year.

After

What is the annual water demand of a single-family household containing four people who are at home an average of 200 days per year and use an average of 100 liters of water per day?

Let's think step by step and explain the calculation step by step.

Step 1: Calculate the total number of days in a year:
There are 365 days in a year.

Step 2: Calculate the total number of days the family is at home:
The family is at home an average of 200 days per year.

Step 3: Calculate the total water demand of the family:
The family uses an average of 100 liters of water per day. Therefore, the total water demand of the family is 100 liters x 200 days = 20,000 liters per year.

Step 4: Calculate the annual water demand of the single-family household:
The annual water demand of the single-family household is 20,000 liters per year.

Lab

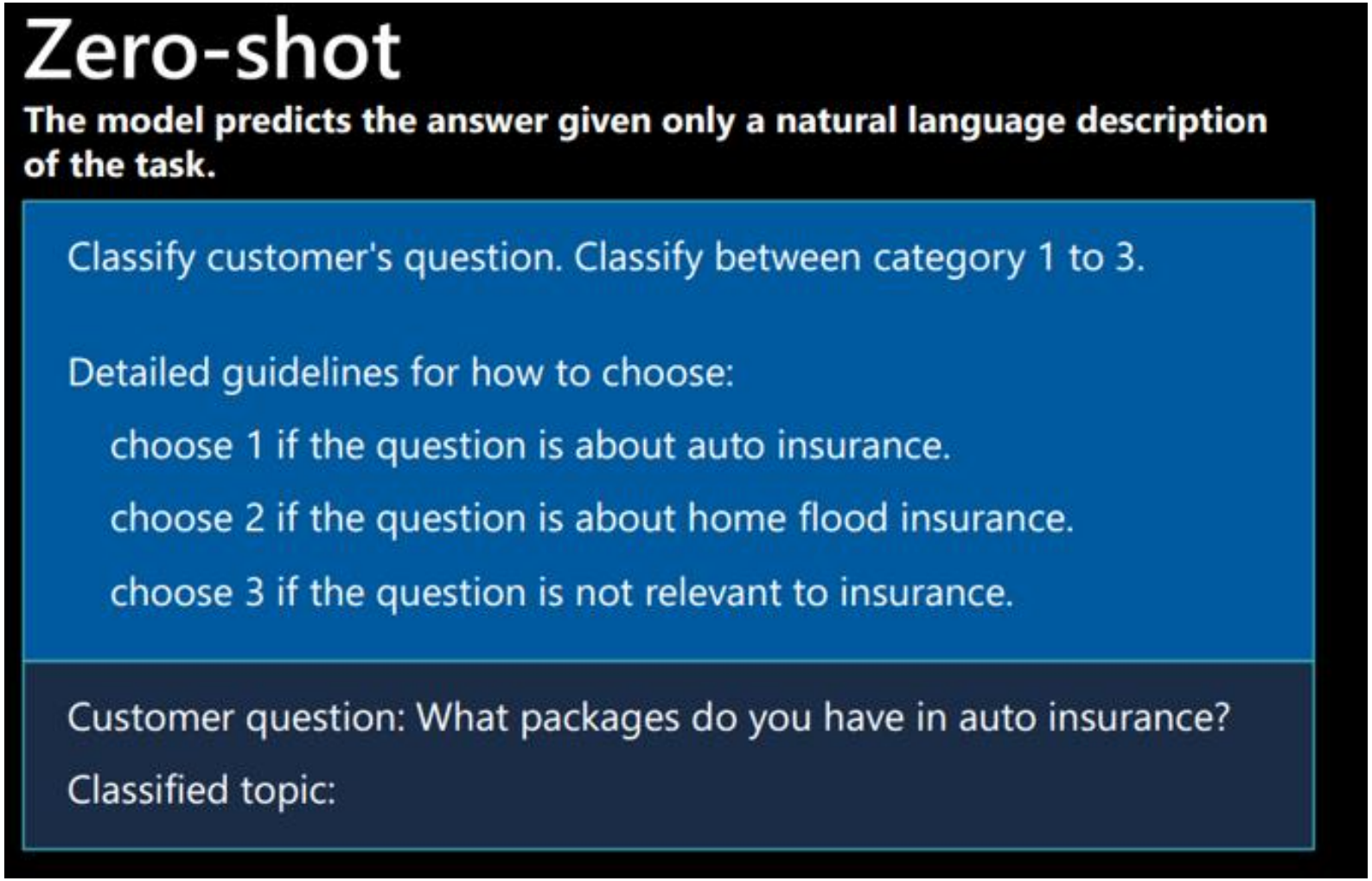
- Tell Copilot to identify edge cases for the “Credit Card” page of the reference application

  hosted here.

  1. Ask for summarizing what the content and goal of that page is (reuse technique from before and modify/re-ask if required.
  2. Ask Copilot to create a plan of how to perform the task of identifying the edge cases and adjust.
  3. Ask Copilot to create a detailed implementation plan and adjust.
  4. Tell Copilot to implement the detailed plan and adjust.

Techniques
Zero-shot Prompts

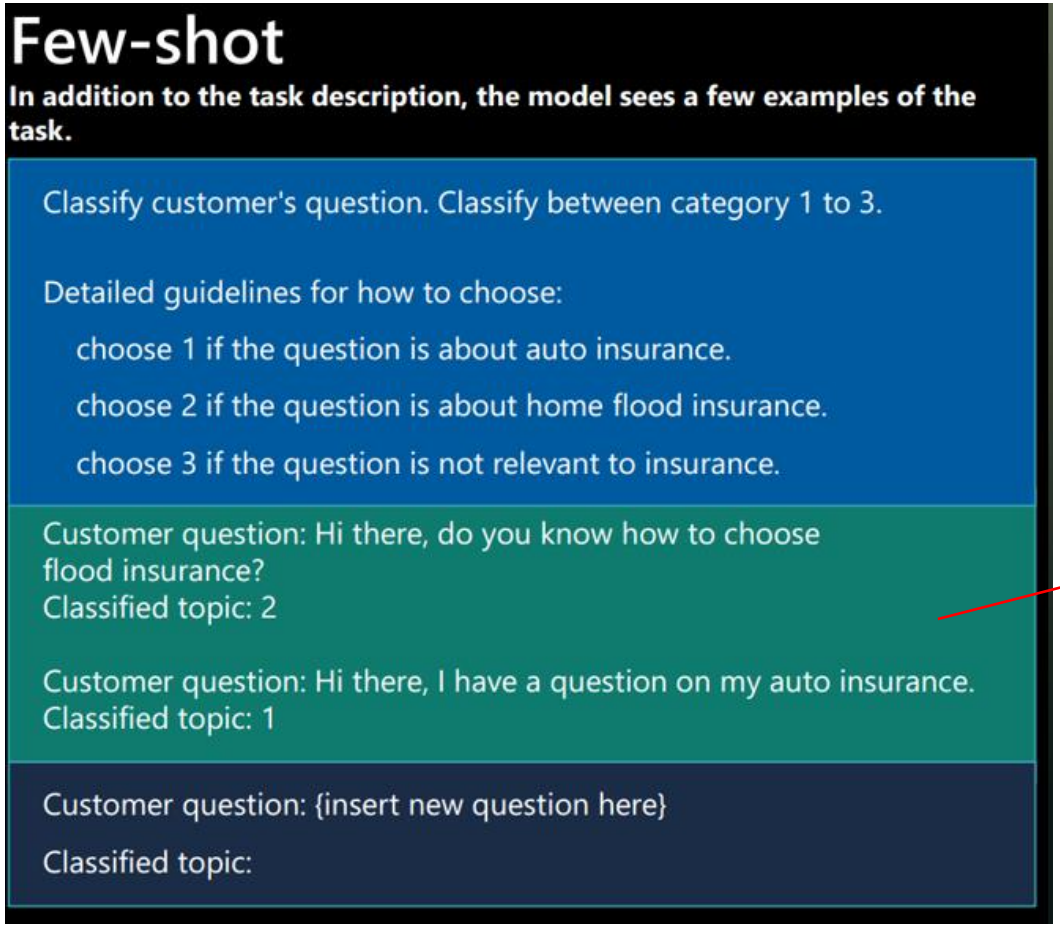
- No previous data or guidelines given before completing request.



Techniques
Few-shot Prompts

- **One Shot**: One piece of data or guideline given before completing request.

- **Few Shot**: Multiple pieces of data or guidelines given before completing request.



Lab

- Tell Copilot to write further tests by using *few-shot prompting* for the “Credit Card” page of the reference application hosted here.
    1. Use the same chat window as in the lab before.
    2. Tell Copilot to identify further edge cases and provide it as table output format.
    3. Tell Copilot to create a plan to implement one of the further edge cases.
    4. Use existing tests from before as template and copy and paste it into the chat window. In the same window tell Copilot to implement the further edge case similar to the reference test you have copied into the chat before.

Techniques
Ask before Answering

- Guide the LLM to ask for clarification before giving an answer.
- Helps ensuring that the model's answers are as accurate and specific as possible.

- **Prompt Formula**
  1. You are an expert in the field of *[industry]*. I'm going to ask you to complete some specific tasks, but before you answer, I want you to do the following: If you have any questions about my task or uncertainty about delivering the best answer possible, always ask bullet point questions for clarification before generating your answer. Is that understood?
  2. Great, my question is *[question]*. Your task is to *[task]*. Please ask any questions you have so that I can improve my prompt before you complete your task.

Techniques
Activate Creativity

- Guide the LLM to bring in creativity.
- Can help you generate new ideas.

- **Prompt Formula**
  - *[Your content]*. Do you have more ideas to this topic?
  - *[Your content]*. What do you think about it?
  - *[Your content]*. Did I miss important aspects?

- Example
  - I want to invest in stocks from VW. What do you think about that?
  - I have the following application *[text]* to the job description *[description]*. Did I miss important aspects?

Techniques
Using Different Perspectives

- You can direct the LLM to write from a single or multiple perspective.

- Prompt Formula
  - **Singular Perspective**: Please write about *[topic]* from the perspective of *[view point]*.
  - **Multiple Perspectives**: Please write an argument *[for/against]* the topic of *[topic]* from multiple diverse perspectives. Include the names and points of view of the different perspectives, such as *[view points]*.

- **Examples**:
  - *Singular Perspective*: Please write about improving as a kickboxer from the perspective of a kickboxing coach.
  - *Singular Perspective*: Please write about improving as a kickboxer from the perspective of a human anatomy expert.
  - *Multiple Perspectives*: Please write an argument against genetically modified organisms (GMOs) that considers multiple perspectives. Include the names and points of view of the different perspectives, such as a farmer, a consumer, and a geneticist.

Lab

- Tell Copilot to identify *functional* and *non-functional* test cases for the “Credit Card” page of the reference application hosted here.
  - Follow the procedure from the lab before before.

Techniques
Constructive Critic

- Provide objective and expert feedback on your writing.
- Highlighting areas for improvement and offering constructive criticism to help you refine and enhance your work.

- **Prompt Formula**
  - I want you to act as an expert and critic in the subject of *[industry]*. Criticize my content pasted below, convince me why it's bad, and give me constructive criticism on how it should be improved. For some context, my *[product or service]* is for *[details, demographic, etc]*. The purpose of my *[product or service]* is to *[your content goal]*. Let's think step by step and I want you to address each piece of content individually. Here is my content to critique, *[your content]*.

Lab

- Ask Copilot to judge about the existing test cases for the *entire* reference application.

  Extend it by identifying critical paths which are not covered enough.
- Repeat the steps from before the get an understand how to guide Copilot to implement

  the recommendations.