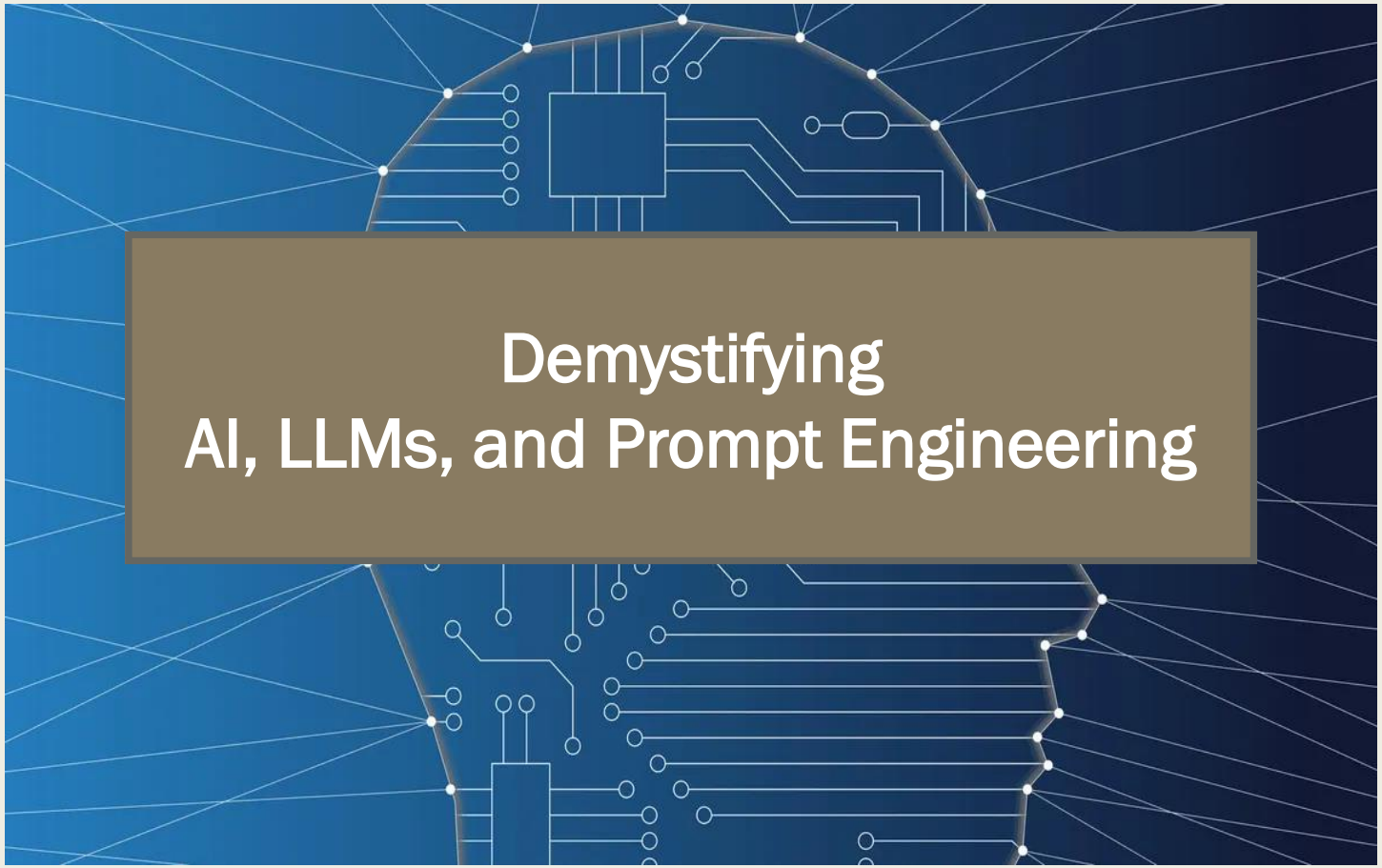
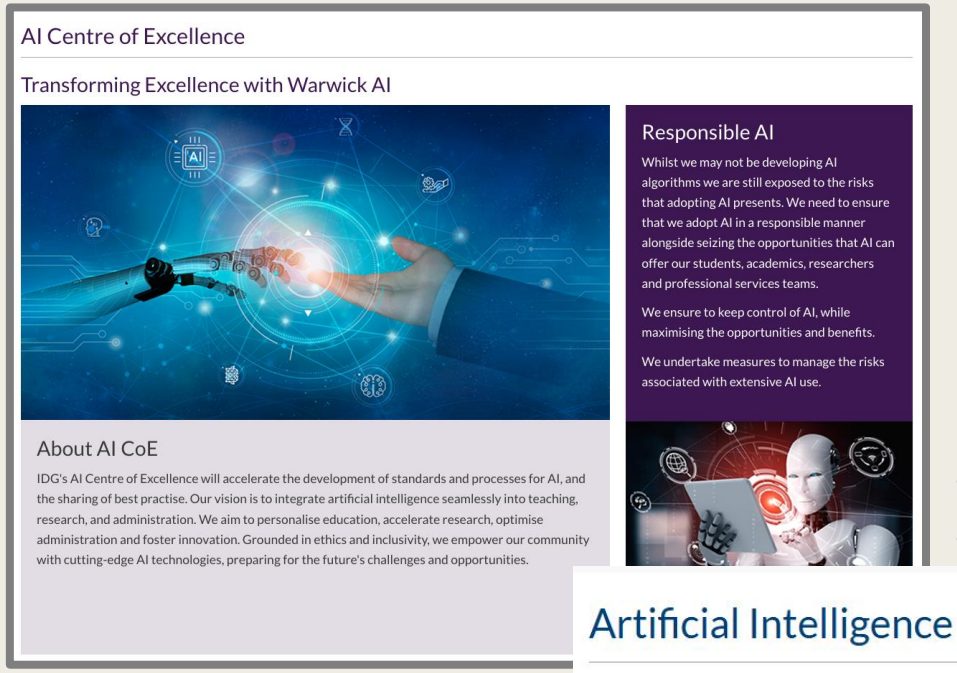


Demystifying AI, LLMs, and Prompt Engineering

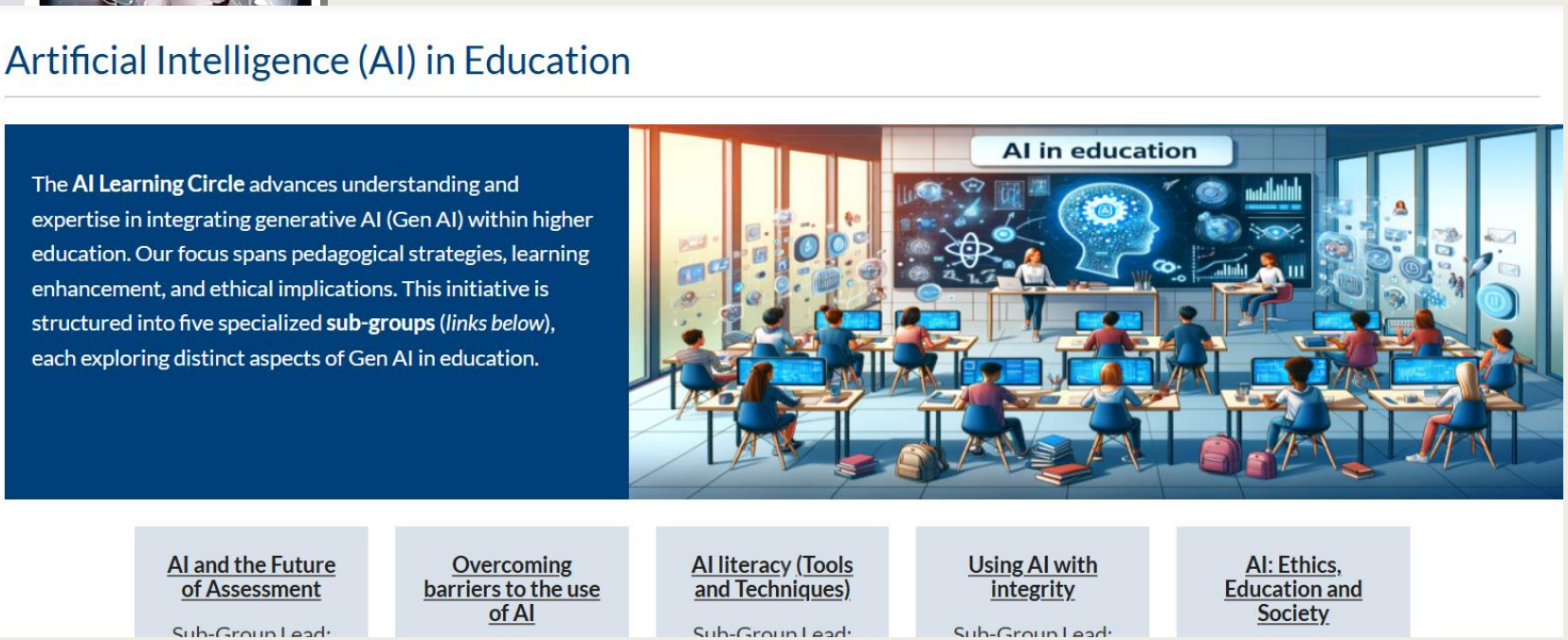
Dr. Neha Gupta,
Asst. Professor, WBS
Dr. Alex Dixon,
Asst. Professor, Dept. of Computer Science

9th December 2024



IDC + WIHEA

https://warwick.ac.uk/fac/cross_fac/academy/activities/learningcircles/ai_in_education/



https://warwick.ac.uk/services/idg/about/technology-office/ai/

WHAT IS A “GPT”?
WHAT IS AN “LLM”?

Artificial Intelligence Models

Expert Systems (since 1960s)

Voicemail systems

Video game characters

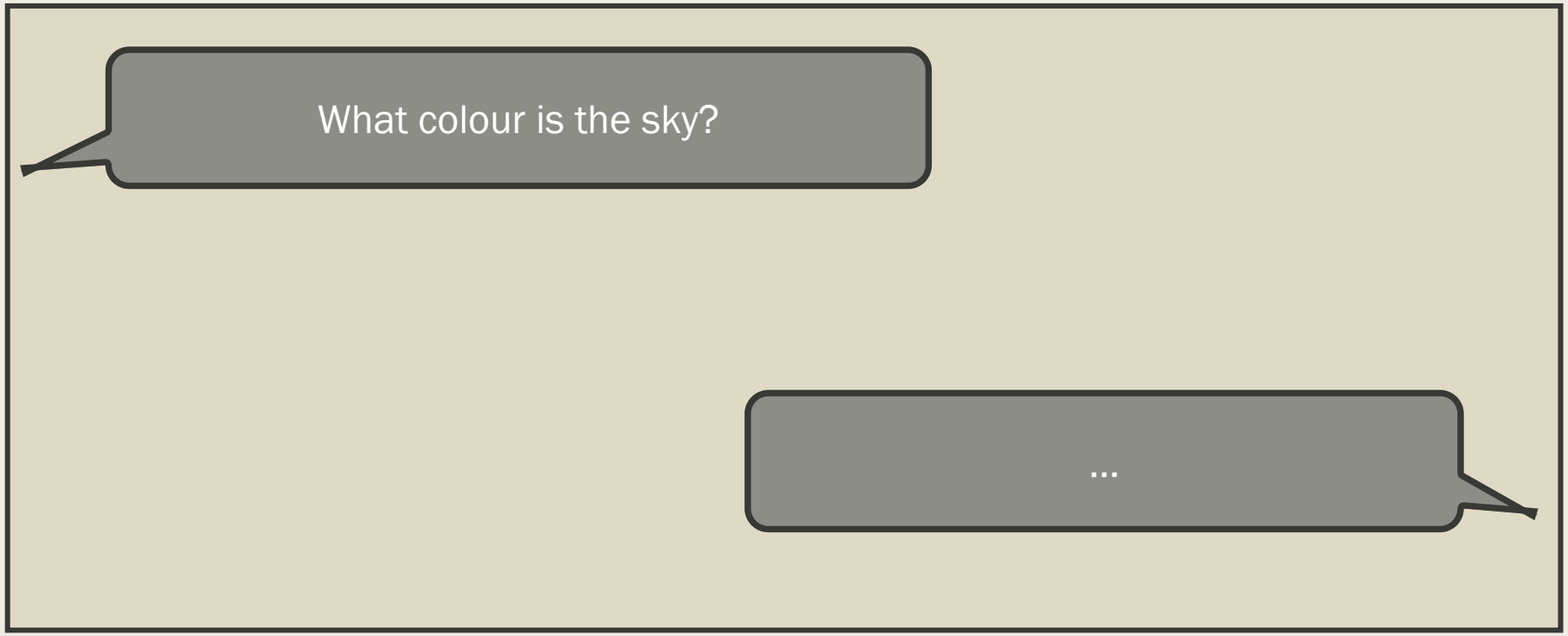
Simple “chatbots”

“General” AI (since 2018)

- **Large language models**, including GPTs like ChatGPT

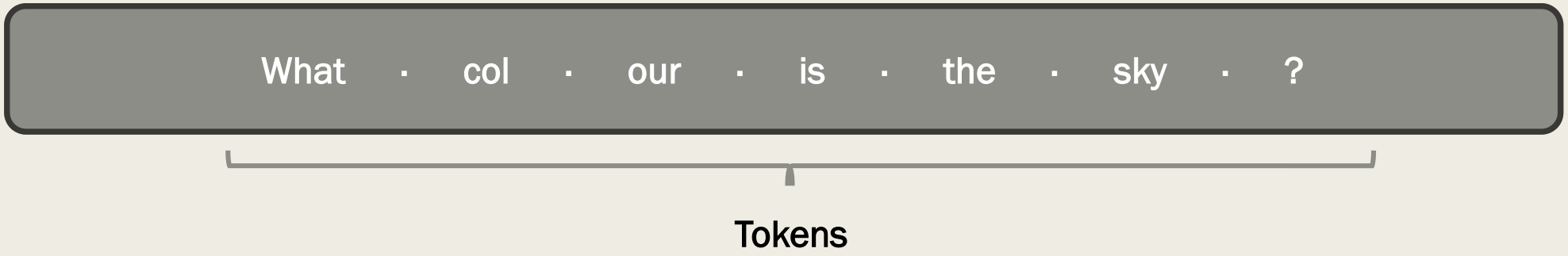
How does a language model “think”?

- LLMs work by **tokenizing inputs** and then **predicting outputs.**



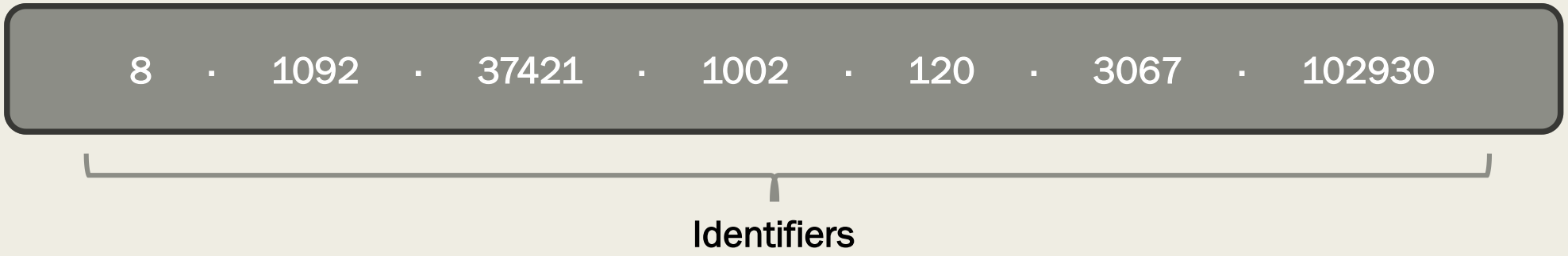
How does a language model “think”?

- LLMs work by **tokenizing inputs** and then **predicting outputs.**



How does a language model “think”?

- Each token is assigned a number.



How does a language model “think”?

- Then the model “predicts” what the next numbers in the sequence will be, based on what it has seen before.

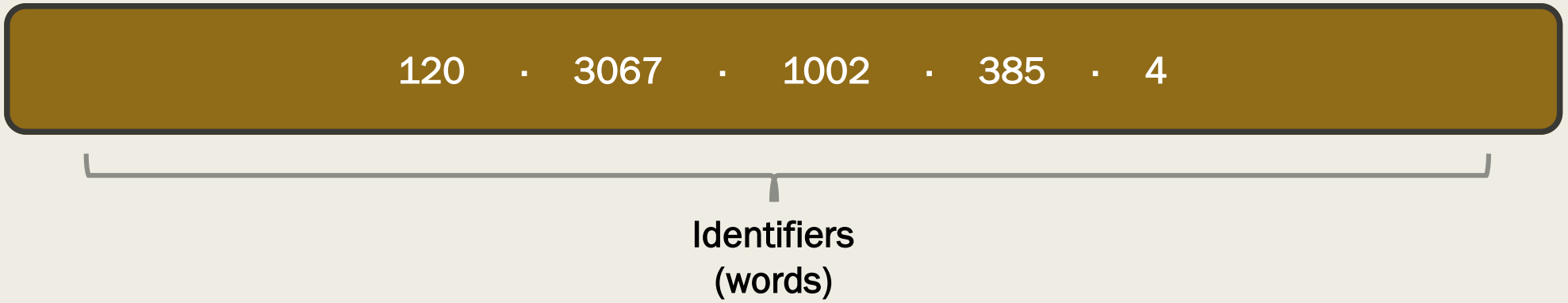
8, 1092, 37421, 1002, 120, 3067, 102930, ….?

The most likely next numbers would be

… 120, 3067, 1002, 385, 4, …

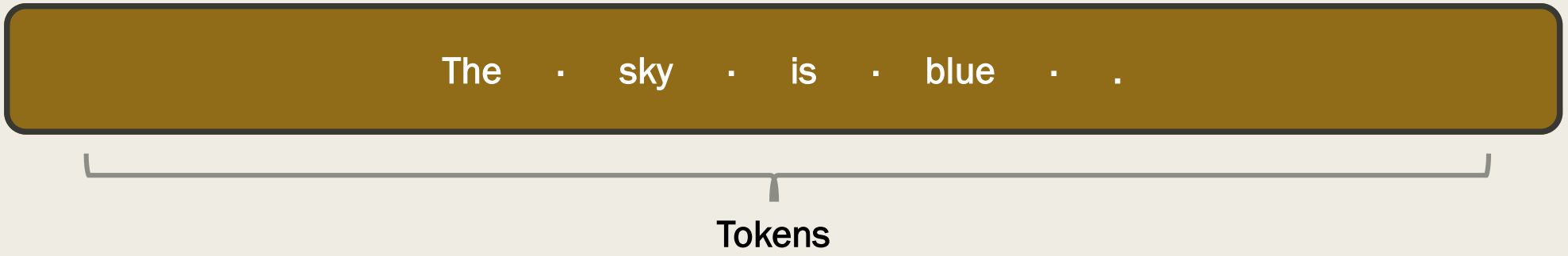
How does a language model “think”?

- Then the model “predicts” what the next numbers in the sequence will be, based on what it has seen before.



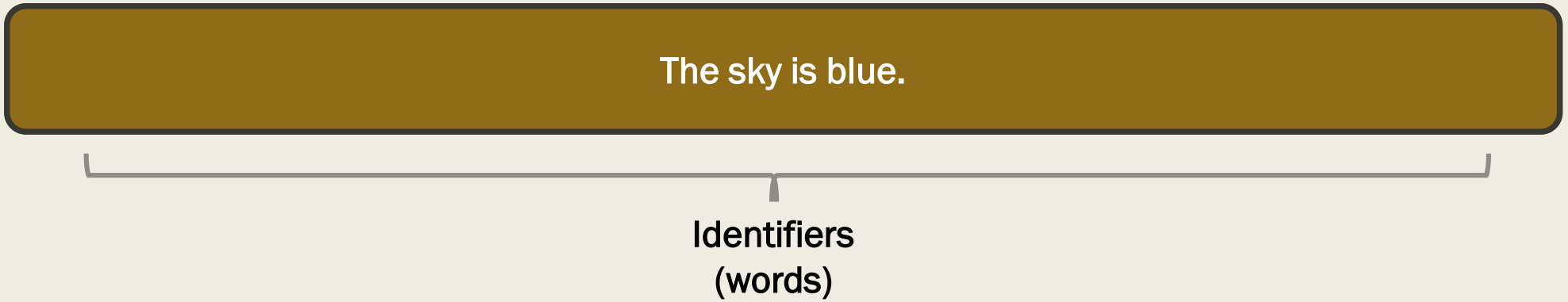
How does a language model “think”?

- Then the model “predicts” what the next numbers in the sequence will be, based on what it has seen before.



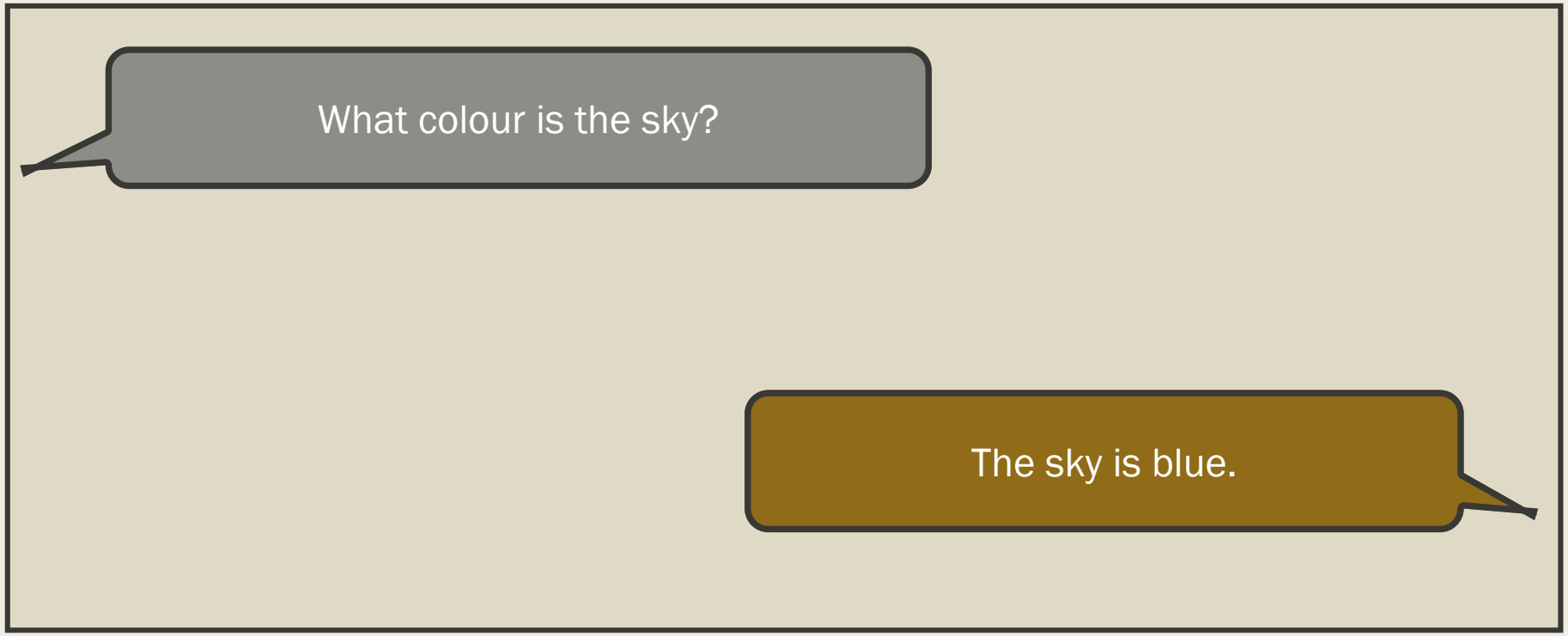
How does a language model “think”?

- Then the model “predicts” what the next numbers in the sequence will be, based on what it has seen before.



How does a language model “think”?

- LLMs work by **tokenizing inputs** and then **predicting outputs.**



How does a language model “think”?

- Despite the name, language models don’t “think” in words. They think only about sequences of tokens.
- **Exercise:** You can play around with tokens with this interesting tool: https://platform.openai.com/tokenizer
- So **why** does the output of ChatGPT look so much like human thought?

LLMs and Training

- To create these prediction machines, the creators feed in text, which is then **tokenized** and stored as **sequences** of tokens.

A very simple data set
”What colour is the sky?” ”The sky is blue.”
”What colour is the sky?” ”The sky is blue.”
”What colour is the sky?” ”The sky is blue.”
”What colour is the sky?” ”The sky is blue.”
”What colour is the sky?” ”The sky is blue.”

LLMs and Training

- Sometimes models will always output the most common response in their data set.
- Sometimes they apply some **randomness**.

A very simple data set
”What colour is the sky?” ”The sky is blue.”
”What colour is the sky?” ”The sky is blue.”
”What colour is the sky?” ”The sky is blue.”
”What colour is the sky?” ”The sky is red.”
”What colour is the sky?” ”The sky is red.”

LLMs and Training

- For large language models, this data set is **big**. It includes
  - *A large portion of the internet, including everything on Wikipedia*
  - *Every book ever written*
  - *Basically, every piece of text ever*
  - *OpenAI's latest data set is approx. 1 TRILLION tokens.*

- Once you start including more data, the model starts to learn about the **relationships** between different tokens (words). This means that more complex ideas can emerge that **combine** different sources.

LLMs and Training

- For large language models, this data set is **big**. It includes
  - *A large portion of the internet, including everything on Wikipedia*
  - *Every book ever written*
  - *Basically, every piece of text ever*
  - *OpenAI's latest data set is approx. 1 TRILLION tokens.*
  - *A worrying trend:* ***other AI generated results online…!***

- Once you start including more data, the model starts to learn about the **relationships** between different tokens (words). This means that more complex ideas can emerge that **combine** different sources.

What is a GPT?

- GPT stands for Generative Pretrained Transformer.

- **Generative**: It produces something (usually text)
- **Pretrained**: It has gone through the process we just described
- **Transformer**: It transforms the input into tokens

Each of these words alone refers to a different type of AI.

Together they refer to the sort of model used by ChatGPT and Copilot.

GPT AT WARWICK

ChatGPT

- ChatGPT is run by OpenAI, who first developed GPT models.
- It is the most widely used interface for LLMs.
- ChatGPT runs at a **significant financial loss.**
- Inputs to ChatGPT are **retained by OpenAI** to train future models.
- Conclusion: It **cannot be trusted** with sensitive information!

Microsoft Copilot

- https://copilot.cloud.microsoft/
- OpenAI partnered* with Microsoft in 2023.
- Copilot uses the same models as ChatGPT under the hood.
- Warwick has a site-wide license for Copilot.
- Copilot is **not trained** on data uploaded.
- It can be trusted with commercially sensitive data, just like MS Word and Excel.
- ALWAYS use Copilot rather than ChatGPT.

WHAT IS “PROMPT ENGINEERING”?

Prompt Engineering:

- Developing and optimizing **prompts** (text commands) to efficiently use language models (LMs) for a wide variety of applications and research topics.

- Prompt engineering skills help to better understand the capabilities and limitations of **large** language models (LLMs).

- Prompt Design vs. *Prompt Engineering*:
  - Terminology ambiguity
  - Use them synonymously
  - ‘Prompt engineering’ is the most established term

What is a Prompt?

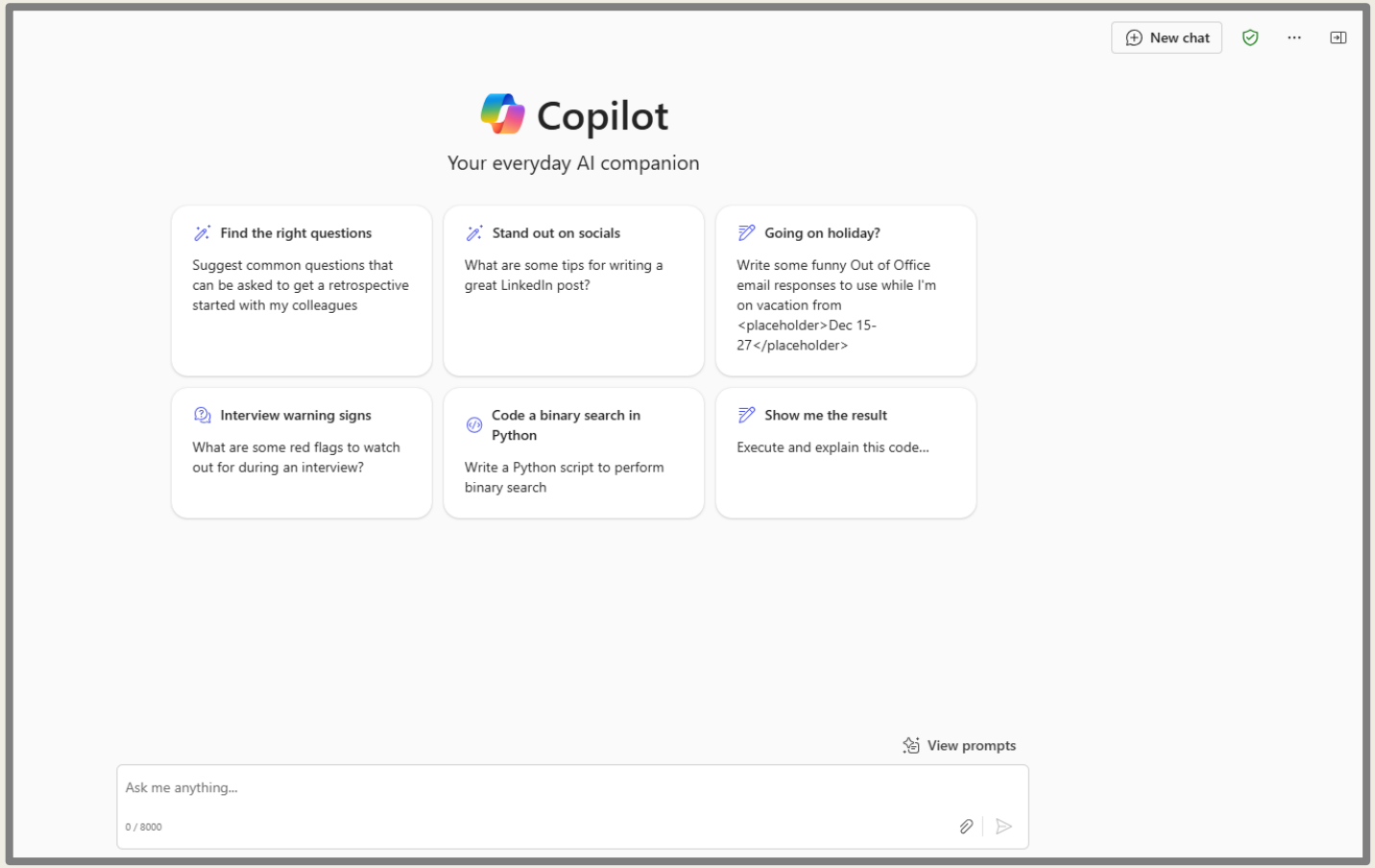
- **Input** to an AI model in Natural language
- Via a text interface, API,….or microphone
- Sequence of Prompts : *Prompt Chains!*

Benefits	Limitations
Describe Task precisely and creatively	Limited no. words per prompt
No expert skills required (code, “Boolean” logic, …)	Limited prompt per chain
Multi-lingual inputs	Lack of transparency
Can be used as a black box	Lack of repeatability

Lets Try Prompting Now:

Open Microsoft co-pilot using your university ID in your browser

https://copilot.cloud.microsoft/



Lets Try Prompting Now:

Exercise 1:

Imagine you are teaching a module to postgraduate students.

Can you **write a prompt in Simple English** which asks Co-pilot to redesign/expand a module from 6 weeks to 15 weeks assuming that you will upload your learning outcomes, reading list and assessment activities.

The ultimate goal is to refresh your module with **latest research outputs**.

Exercise Resource:

AI Literacy-9thDec-Prompts

Imagine you are creating a course handbook for any undergraduate courses in your department. Write a prompt that ensures AI generates a structured and relevant handbook.

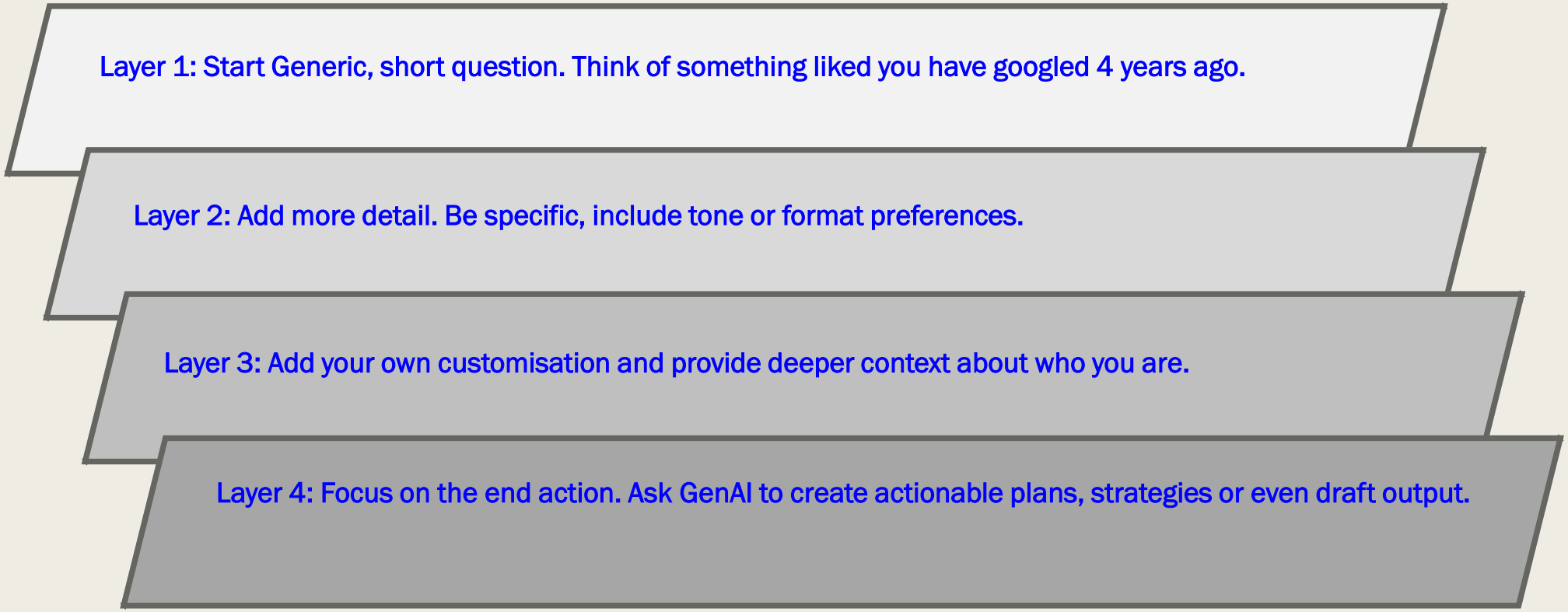
https://tinyurl.com/mabfe4xd

Prompting: CRAFT Technique
(with reference to Exercise 1)

- **CONTEXT** – Higher Education Russell Group University
- **ROLE** (Persona) – Professor
- **ACTION** – Recreate content
- **FORMAT** – Table
- **TARGET** – Students

Prompting - generic understanding

- Look at it as a layered approach:



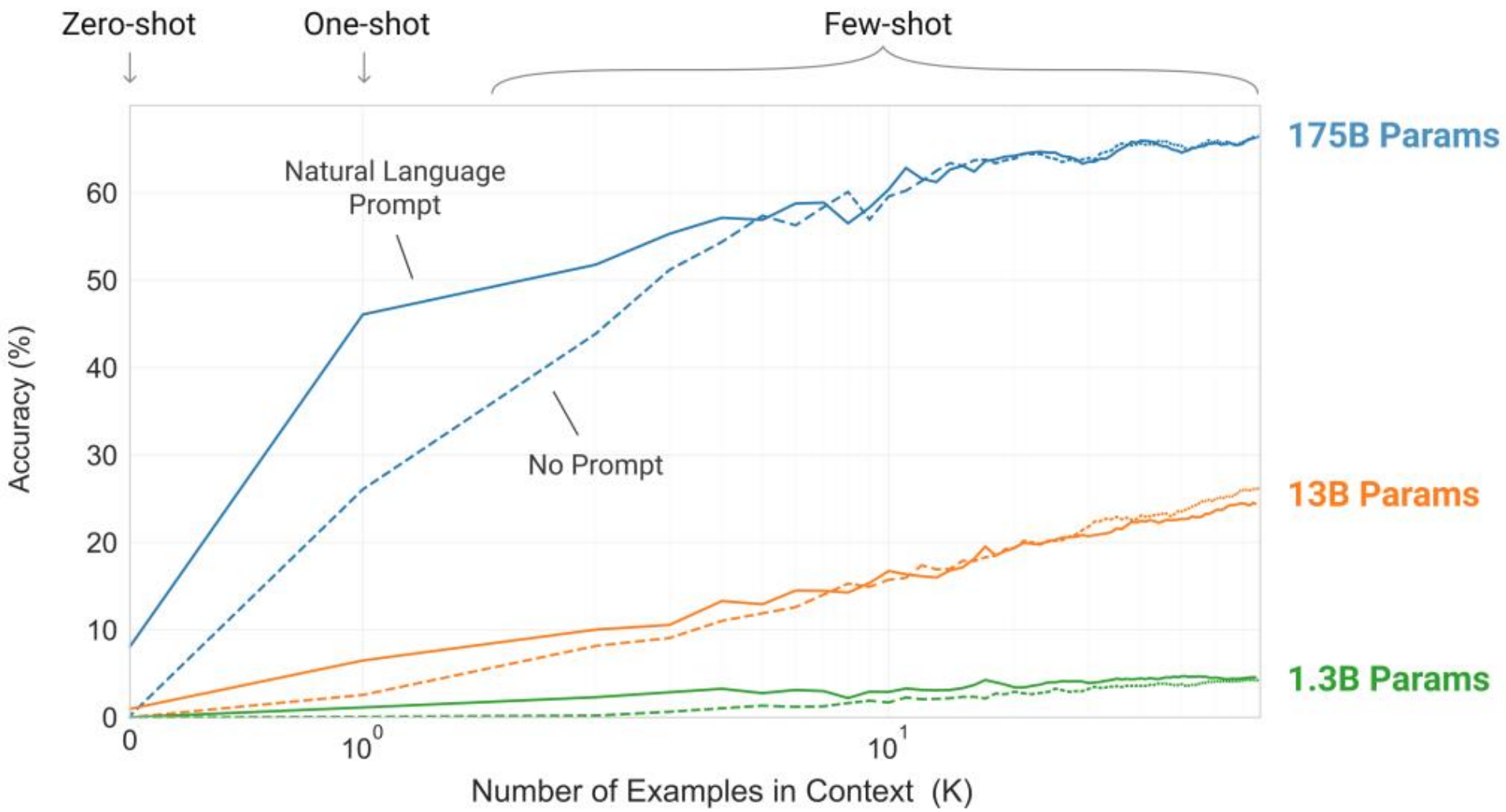
Prompt Engineering Techniques – Giving Examples

- **Zero-shot prompting** : Prompting without examples
- **Few shot prompting**: enable in-context learning where we provide demonstrations in the prompt to steer the model to better performance. The *examples* serve as conditioning for subsequent examples where we would like the model to generate a response.
- **Chain-of-thought (CoT) prompting**: CoT prompts guide the model to break down a complex question into manageable steps, akin to how a human might solve the problem. CoT embeds reasoning steps within the prompt.

  CoT "Prompt: Conduct a cultural analysis of the 1960s American Civil Rights Movement. Step 1: Describe the social and political context. Step 2: Discuss key figures and events. Step 3: Analyze its impact on contemporary society."

- And many more…. (*for another session*)

https://www.promptingguide.ai/techniques
https://platform.openai.com/docs/guides/prompt-engineering



https://arxiv.org/pdf/2005.14165

Prompt Engineering Techniques – Using Personas

- Role play: Use personas and scenarios
- '*Program*' the AI model through pretend roles & scenarios
- It can be seen as a shortcut to manually fine-tuning tone, depth, style

> *"I am a university student, preparing for a very busy exam season. I have access to a GenAI chatbot. You will be my instructor, who is open-minded on teaching methods and new technology, but firm on academic integrity.*
>
> *You are aware of a recent spike in student breach of academic integrity standards through unauthorized GenAI tool use. What advice would you give me on the usage of those tools, that will convince me not to use them?"*

Prompt Engineering Techniques–multimodal CoT

- ‘Multimodal prompts are a type of prompts for large language models (LLMs) that combine **multiple input** type formats.
- Enhances the model’s ability to handle complex inputs and outputs that require understanding beyond plain text.

“describe the image with as many details as possible, then write a poem for my picture.”

[then attach/upload a picture/image]

[Image of a crowded city street] + “*Describe the traffic conditions shown in this image and suggest improvements for better flow*.”

https://www.medrxiv.org/content/10.1101/2024.10.30.24316434v1.full.pdf+html

Lets Try Prompting *again* Now:

Exercise 2: Look at the example of **Analyze the grant proposal** in the shared document.

Can you think of other ways this prompt can be further improved?

https://docs.anthropic.com/en/prompt-library/library
https://platform.openai.com/docs/examples

Reflections and Q&A