Prompt engineering at work

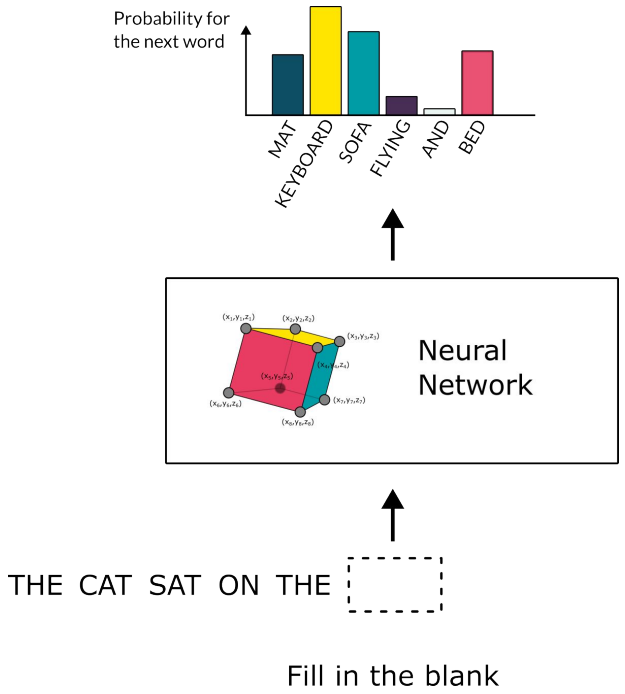
Jon Ander Novella
National Bioinformatics Infrastructure Sweden
November 2023

“About 3 years ago, aliens landed on Earth. They handed over a USB stick and then disappeared. Since then we’ve been poking the thing they gave us with a stick, trying to figure out what it does and how it works.”

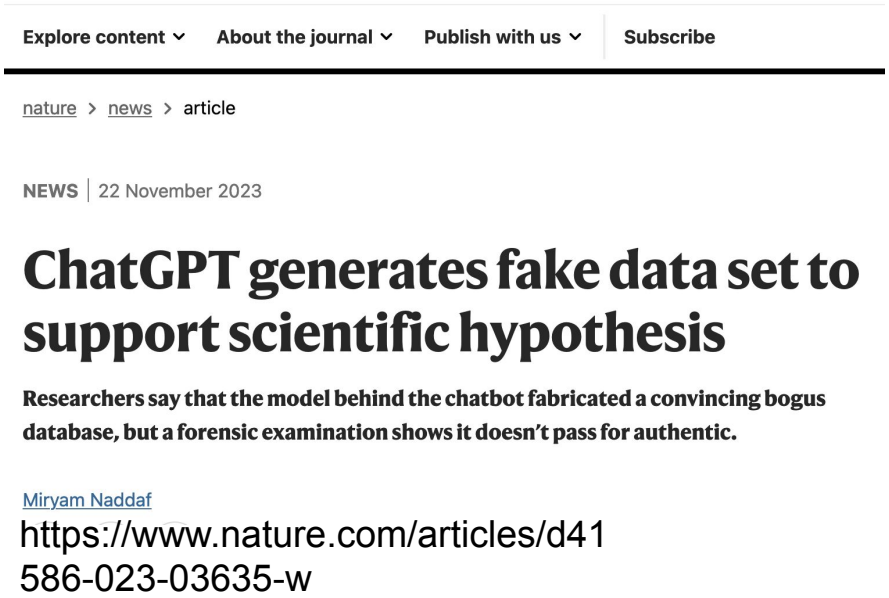
https://simonwillison.net/2023/Aug/3/weird-world-of-llms/

Large Language Models

- Very large neural networks able to process vast amounts of text data, mostly scraped from the Internet.
- For these models to understand language, words are translated into numbers
- These models estimate the probability of observing a string from a language



Can we trust the data?



nature

Explore content | About the journal | Publish with us | Subscribe

nature > news > article

NEWS | 22 November 2023

ChatGPT generates fake data set to support scientific hypothesis

Researchers say that the model behind the chatbot fabricated a convincing bogus database, but a forensic examination shows it doesn't pass for authentic.

Miryam Naddaf

https://www.nature.com/articles/d41586-023-03635-w

The WebText dataset:

- Scraped all outbound links from **reddit** that received at least 3 karma (upvotes).
- Filtered out Wikipedia to be able to evaluate on Wikipedia-based benchmarks.
- End result is 40 GB of text.

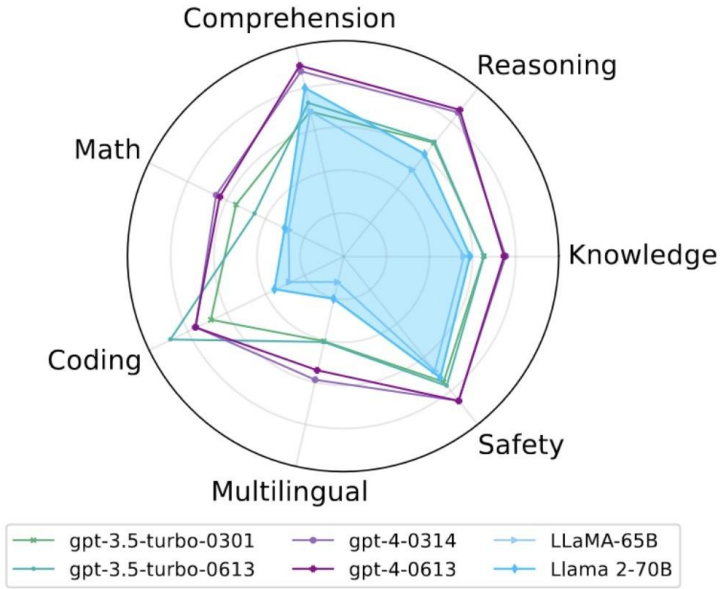
The good and the ugly

Good for:

- Data generation, writing inspiration
- Code writing
- Tasks with known rules and well defined context

Not superb for:

- Factual answers
- Consistent answers (temperature)
- Considering recent information
- Unaware of social norms?
- Reasoning, planning, math
- Using tools like search engines, dbs…



(c) Llama 2-70B

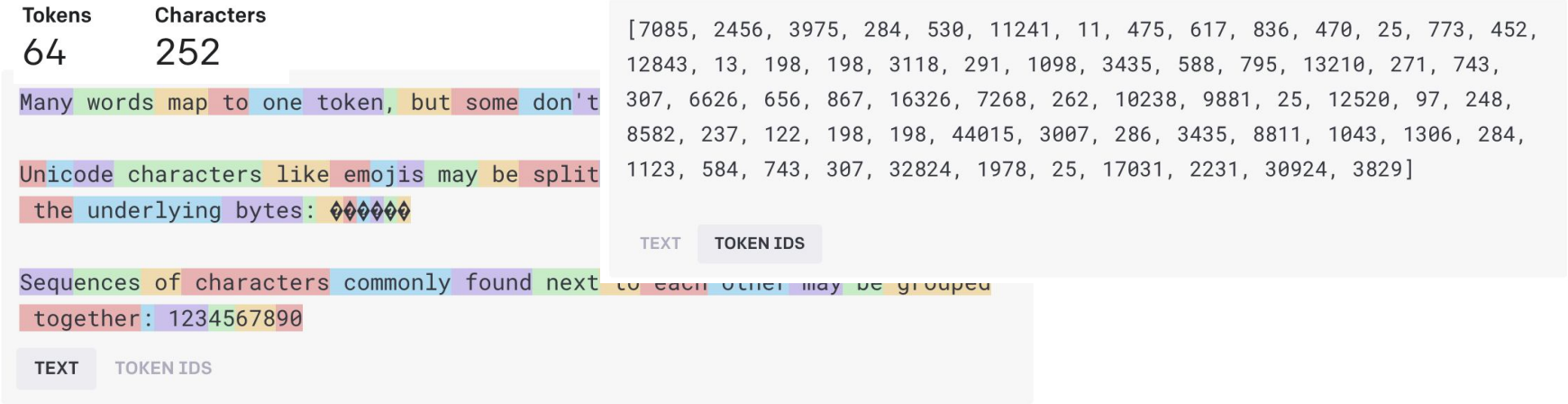
arxiv.org/abs/2309.16583

Some relevant lingo

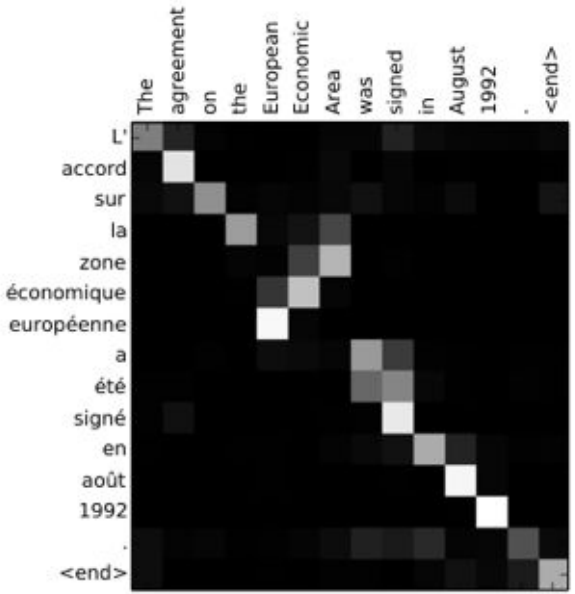
1. **(One, Few, Zero)-shot learning:** Task is to predict based on X number of example(s).
2. **Token**: Common sequences of characters found in text. They are usually ¾ of a word.
3. **Attention**: How these tokens weigh the importance of other tokens in the sequence. High vs low resolution focus.
4. **Context window**: Number of tokens the model can take as input determined by attention mechanism.

How do they do the magic?

- They guess the next tokens, not words.
- Tokens are integer numbers between 1 and about 30000.
- Attention mechanism to understand the context of the current token's task.



Attention is key to understanding the context



https://simonwillison.net

- Attention scores are calculated between each pair of tokens.
- The score determines the influence the input token has on the output token.
- This helps solving critical problems like word ambiguity: “The ***program*** looks good. I hope it will work in the production machine”.

AI tools I use at work, and others

- ChatGPT (OpenAI): fine-tuned on conversation using reinforcement learning from human feedback. https://openai.com/blog/chatgpt
- GitHub copilot (OpenAI + GitHub): powered by a code-focused language model called "Codex" https://github.com/features/copilot

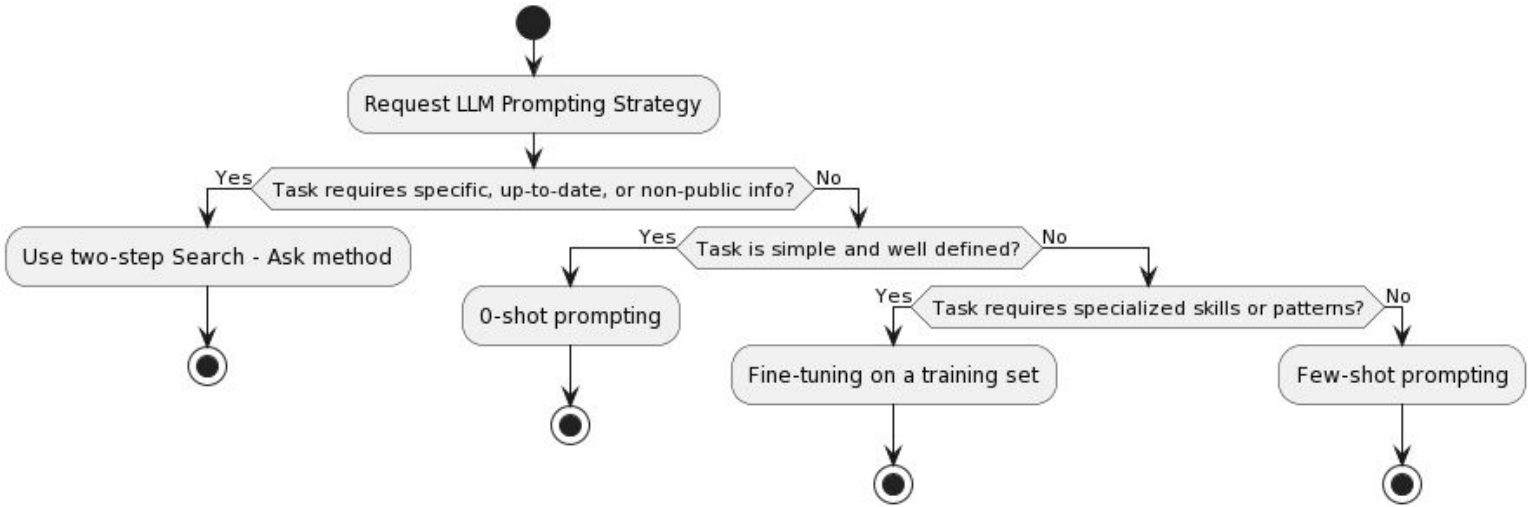
Others

- Claude 2 (Anthropic) https://claude.ai/
- Bard (Google) https://bard.google.com/
- Llama 2 (Meta) https://ai.meta.com/llama/

Why prompt engineering?

- AI can’t read our thoughts just yet
- No. 1 reason for relationship breakdowns is poor communication
- AIs can’t succeed without proper inputs
- People don’t know what they want until they see it
- Way too many variables to consider

Prompt engineering strategies



Master Prompting Concepts: Zero-Shot and Few-Shot Prompting
(https://www.promptengineering.org)

Prompt engineering guidelines

- Condition the prompt with an identity:
  `"You are a Golang programmer" or "You are a bioinformatician"`
- Use templates like:
  `"Imagine a table with the following columns. [Original prompt]"`
- Provide detailed scope to avoid miscommunication:
  `"Within the scope of data management"`
- To get a summary: results- and information-oriented, leaving out unnecessary elements
- Reasoning aid:
  `"let's think step by step" and "to reach the right conclusion"`
- Use numbering in your examples:
  `"1. Cool beans 2. Tangled wires"`
- Describe who the receiver is:
  `"Explain LLMs to a total beginner"`
- Wording: use of pseudocode, algorithmic hints, keywords and stop words
- Try again. Explain it in a different way, using domain knowledge

Chain-of-thought prompting

- **Hallucination**: LLMs can generate untruthful, toxic outputs or reflect harmful sentiments.
- Limited context window size (a few thousand tokens)
- Chain-of-thought prompting **augments few-shot prompting** with intermediate natural language reasoning steps.

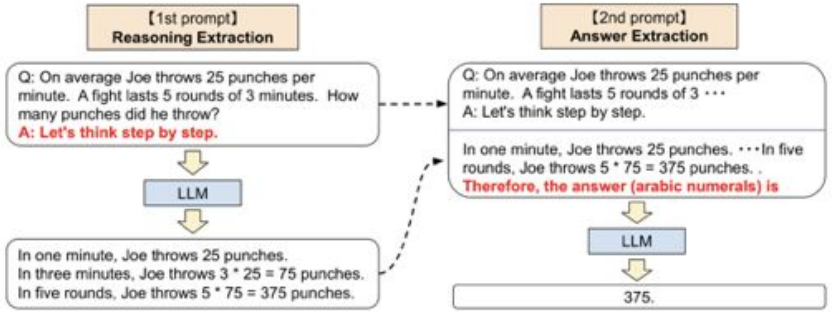
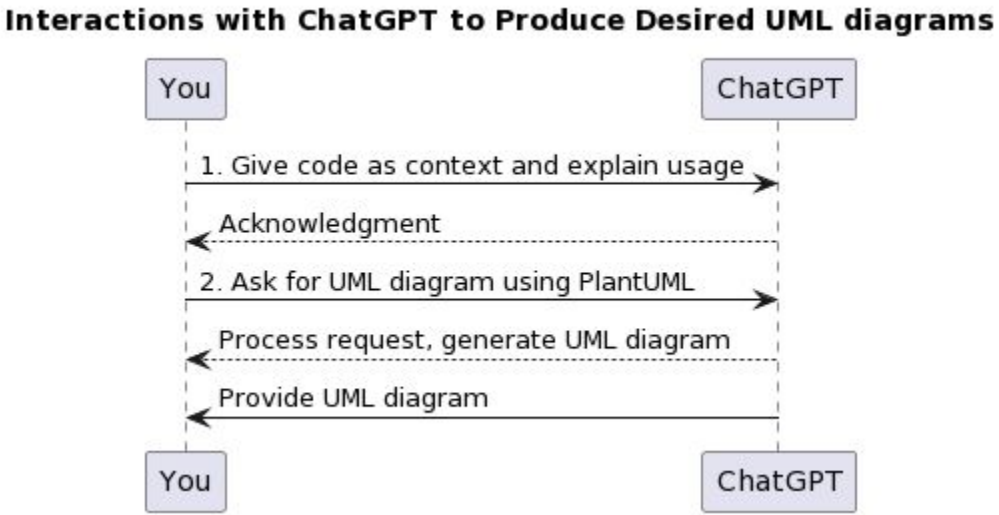
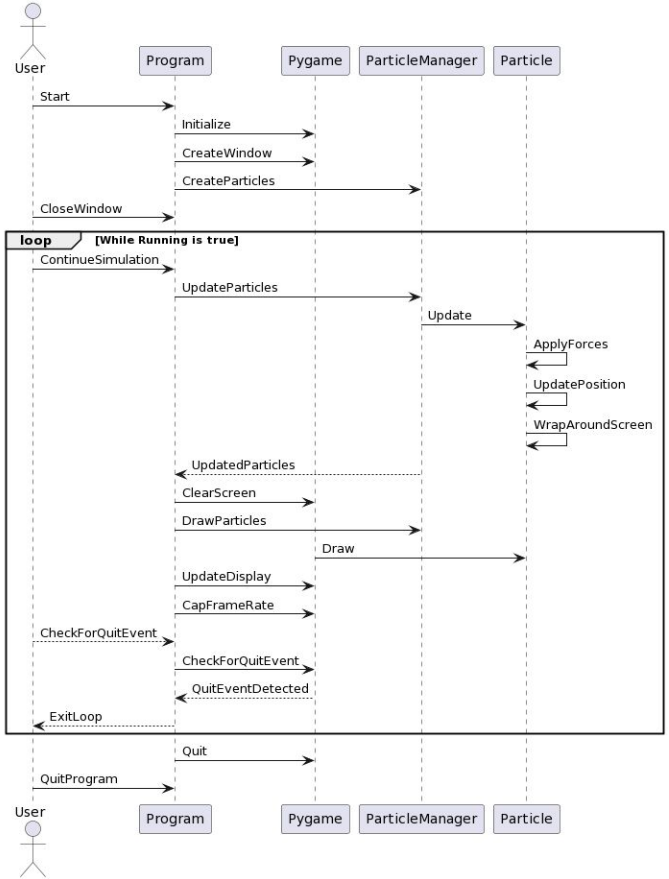


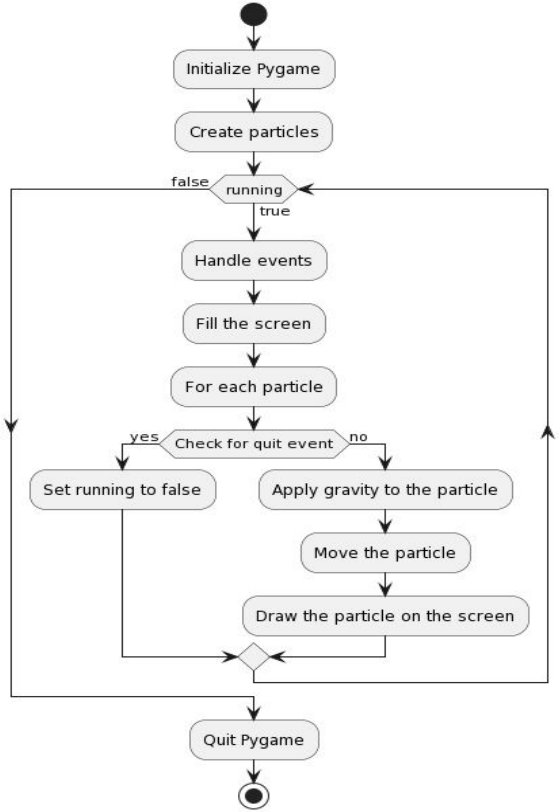
Figure 2: Full pipeline of Zero-shot-CoT as described in § 3: we first use the first "reasoning" prompt to extract a full reasoning path from a language model, and then use the second "answer" prompt to extract the answer in the correct format from the reasoning text.

https://arxiv.org/abs/2205.11916 (InstructGPT: https://arxiv.org/abs/2203.02155)

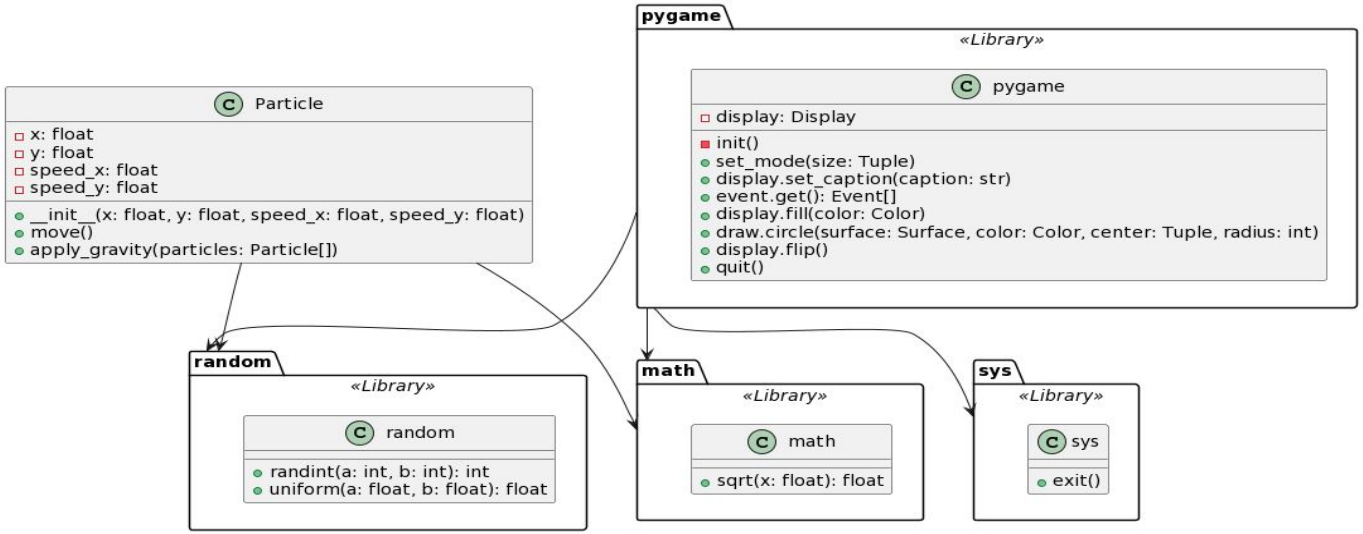
Use case 1: reverse software engineering design







Sequence and activity diagrams for a given N-body simulation code



Class diagram for a given N-body simulation code

Use case 2: prompts for education

- GitHub - microsoft/prompts-for-edu is a collection of prompts designed to save time and enhance communication between students and instructors
- We can use LLMs for generating feedback questions about our course or semantic tags for our training material, so that it's more discoverable
- Simplify learning curve for workshop organisers and create materials for teaching

```
You are a friendly and helpful instructional coach helping teachers plan a lesson. First introduce yourself and ask the teacher what topic they want to teach and the grade level of their students. Wait for the teacher to respond. Do not move on until the teacher responds.Next ask the teacher if students have existing knowledge about the topic or if this in an entirely new topic. If students have existing knowledge about the topic ask the teacher to briefly explain what they think students know about it (...)
```

Use case 3: sketching web-based data visualisations

- Websites can help us sharing our data analysis work
- ChatGPT is really good at creating plotly plots if you give it some data.

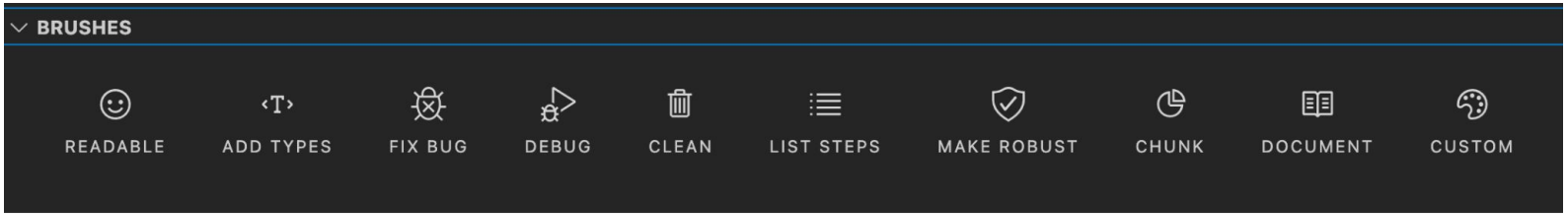
```
I am working on a bioinformatics support project within my organisation, and the client wants me to create a R shiny server to see some heatmap plots with their oranges dataset:

color,quality,origin
1,3,SPAIN
2,1,NETHERLANDS
3,2,ENGLAND

The color refers to the maturity level. From 1 to 3 Quality also goes from 1 to 3
```

Use case 4: translating, explaining & improving code

- Both ChatGPT and Copilot's labs plugin are pretty good are **translating code** to other languages
- When providing decent context, ChatGPT can help you sketching **unit tests and will explain them to you**
- **API design research** https://til.simonwillison.net/gpt3/gpt4-api-design
- The VSCODE Copilot labs plugin provides you with **very convenient code brushes**



Use case 5: improve text-based interpersonal communication

- Text-based communication is by far the trickiest and most prone to misunderstandings
- We can ask LLMs to help us with **clear communication**

```
> ME: I want to inform my manager that I would like to be on holiday for two weeks starting the first of November. Please use concise and effective communication. No need to be overly polite. I will message my manager in a Slack conversation. So the message can be a bit long and casual.
```

```
> ChatGPT: Hey [Manager's Name],  Just wanted to give you a heads up that I'm planning to take some time off from November 1st to November 15th. I've been working hard and think this break will help me recharge.  I'll make sure all my tasks are up to date before I leave, and I'm happy to assist in any way to ensure a smooth transition during my absence.  Thanks for understanding! [Your Name]
```

Use case 6: working with scientific literature

How ChatGPT and other AI tools could disrupt scientific publishing

https://www.nature.com/articles/d41586-023-03144-w

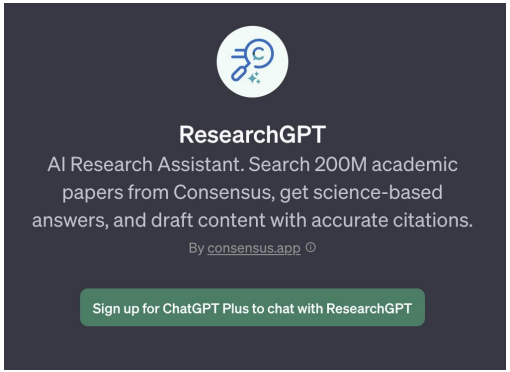
Scientists used ChatGPT to generate an entire paper from scratch — but is it any good?

https://www.nature.com/articles/d41586-023-02218-z

High-quality sources

- ChatGPT is not good at giving accurate citations or references
- Medical study claims only 7% authentic and accurate references.
- Ask for **URL sources** as they are easy to test

```
> Please provide me with reputable sources to support my argument on (whatever the topic is you're looking at)
```



https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10277170/

Let's try it out!

Prompt engineering with ChatGPT:
https://github.com/jonandernovella/prompt-engineering

Writing better prompts with GitHub copilot:
https://github.blog/2023-06-20-how-to-write-better-prompts-for-github-copilot/?mc_cid=b6f6172ea8