

HELMHOLTZ AI

ChatGPT in Action: Enhancing Your Workflow

Isra Mekki

HELMHOLTZ AI

Consultants teams



WHAT IS OUR MISSION?

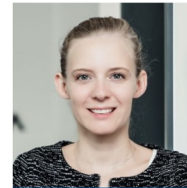


Maximise research impact by
democratising access to AI

HOW DO WE DO THAT?

- Short to mid-term scientific
collaboration (2 weeks – 6 months)
- Free of charge
- Easy application

TEAM MEMBERS



Marie Piraud



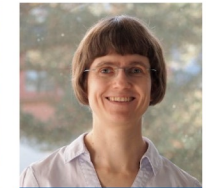
Lisa Barros de
Andrade e Sousa



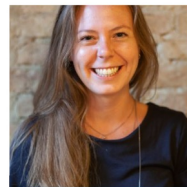
Christina Bukas



Donatella Cea



Elisabeth Georgii



Theresa Willem



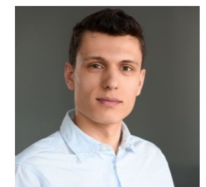
Isra Mekki



Erinc Merdivan



Helena Pelin



Francesco
Campi

Reach out to us at
consultant-helmholtz.ai@helmholtz-munich.de

DISCLAIMERS

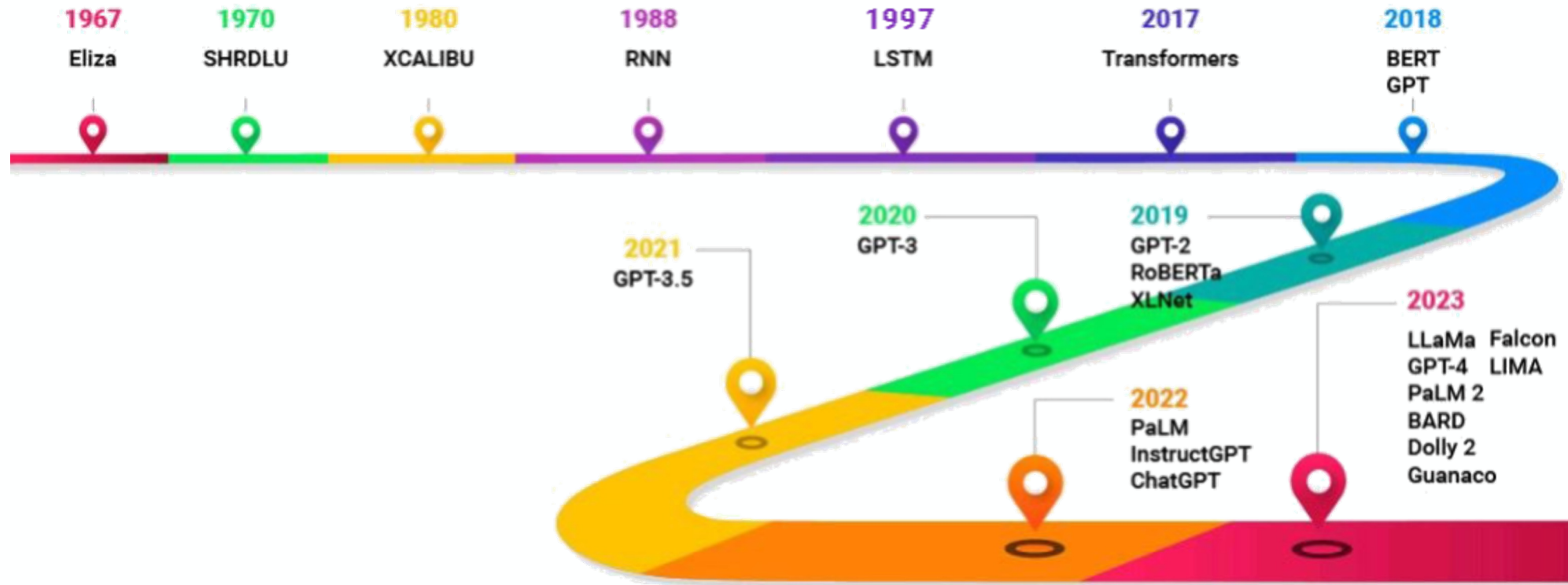
- I am not a certified expert in the field. The goal of this lecture is to share insights gathered by our team.
- While the primary focus will be on ChatGPT, the concepts discussed often apply to other large language models (LLMs) as well.
- My practical experience is primarily with ChatGPT. I have limited hands-on experience with other tools like Gemini, Claude, etc.

AGENDA

1. Introduction
2. Modern Applications
3. General Recommendations
4. Blablador: A Privacy-Focused Alternative, No Data Stored
5. Conclusions and open questions

INTRODUCTION

Evolution of Large Language Models (LLMs)



<https://cdn.analyticsvidhya.com/wp-content/uploads/2023/07/roadmap-1.jpg>

INTRODUCTION

Evolution of Large Language Models (LLMs)

```
=====
EEEEEEEE L      IIIIII ZZZZZZZ AAA
E         L      I      Z      A  A
E         L      I      Z      A  A
EEEEEE   L      I      Z      A  A
E         L      I      Z      A  A
E         L      I      Z      A  A
EEEEEEEE LLLLLLL IIIIII ZZZZZZ A  A

=====
ELIZA > (PLEASE TYPE IN ALL CAPS) WHAT'S YOUR NAME DEAR ?
AMIT
ELIZA > HI, I'M ELIZA. WHAT DO YOU WANT TO TALK ABOUT ?
AMIT > CAN I TALK ABOUT MY PROBLEM ?
ELIZA > SURE... !
AMIT > DUE TO ON GOING EXAMS IN COLLEGE, I HAVE A LOT OF STRESS.
ELIZA > PLEASE RELAX A LITTLE. SLEEP WELL.
AMIT > THANKS FOR YOUR ADVICE.
ELIZA > NO MENTION.
AMIT > BYE
ELIZA > BYE AND KEEP IN TOUCH...

=====
```

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

EVENTUALLY THE WEB WILL BE ONLY CHATBOTS —

After ChatGPT disruption, Stack Overflow lays off 28 percent of staff

The popular developer forum is still hunting for a "path to profitability." [Amadeo, 2023](#)

The Washington Post
Democracy Dies in Darkness

ChatGPT took their jobs. Now they walk dogs and fix air conditioners.

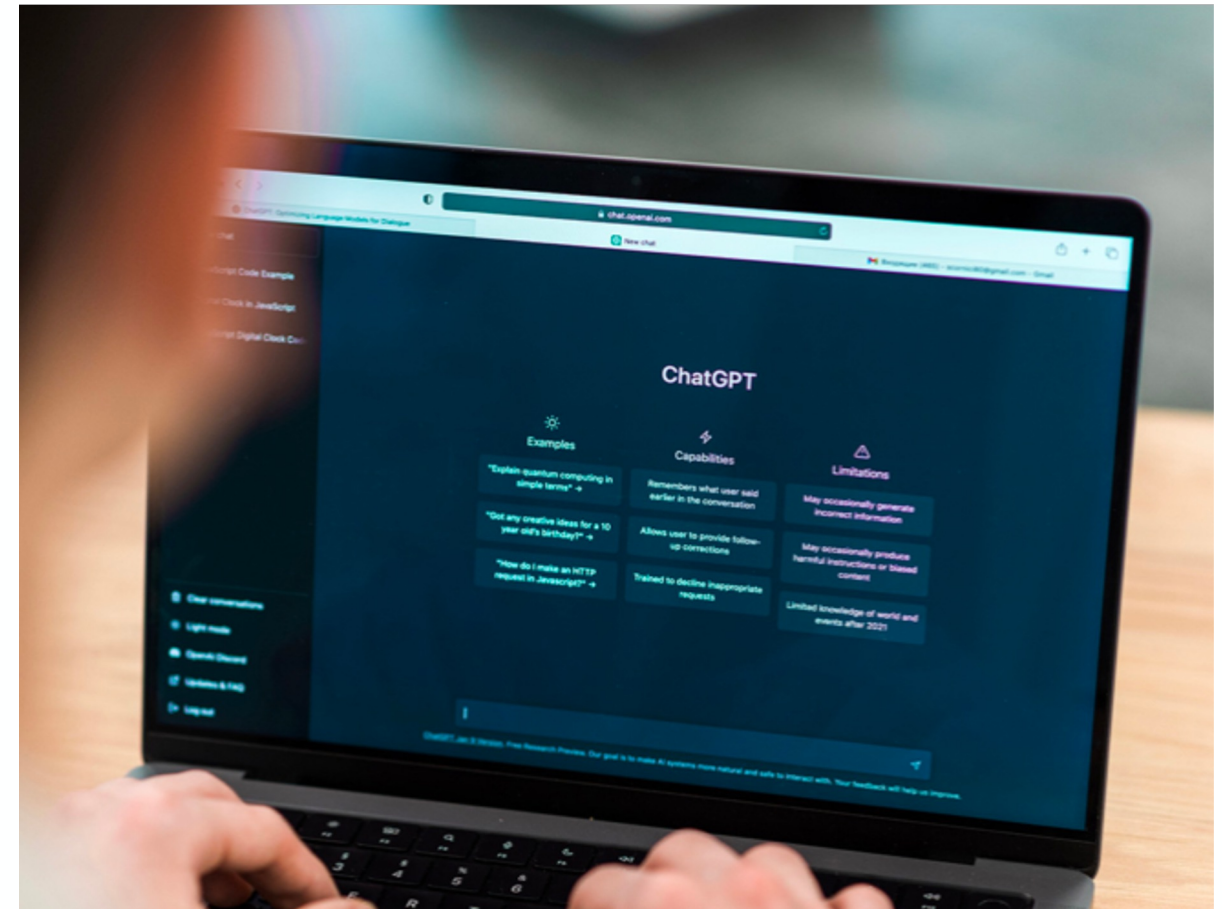
Technology used to automate dirty and repetitive jobs. Now, artificial intelligence chatbots are coming after high-paid ones.

[Verma & De Vynck, 2023](#)

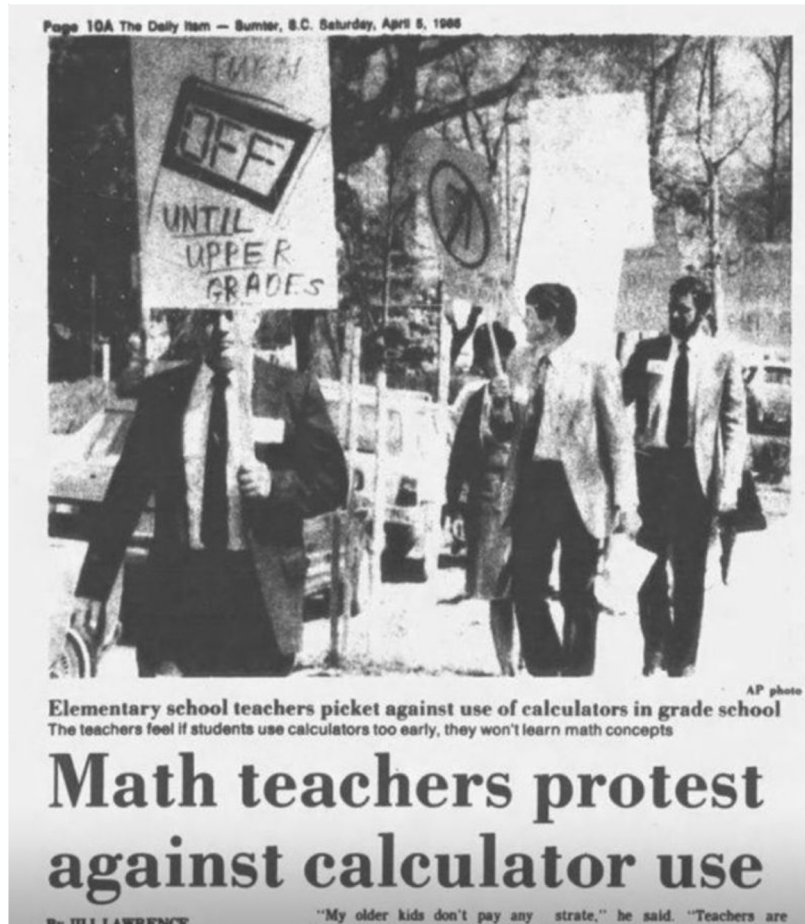
WILL LLMS TAKE OUR JOBS?

No.

You will lose your job to a person using AI and LLMs



WILL LLMS AFFECT THE WAY WE LEARN?



- *“We’ve heard people say things like they think this is going to make students stupid, that they’re not going to learn how to write or learn the basics of language. In some ways it’s similar to arguments we heard about the introduction of calculators back when I was a kid.”*
 - Sarah Elaine Eaton, University of Calgary
- *“Generative text is something we all need to adapt to, we adapted to calculators and changed what we tested for in math class, I imagine. This is a more extreme version of that, no doubt, but also the benefits of it are more extreme, as well.”*
 - Sam Altman, CEO OpenAI

OPEN ISSUES

- ❑ Robustness
- ❑ Hallucinations
- ❑ Transparency
- ❑ Bias
- ❑ Privacy violations (Lomas, 2019)
- ❑ Data Reliability

"AI is probably the most important thing humanity has ever worked on. I think of it as something more profound than electricity or fire." — Sundar Pichai (CEO of Alphabet Inc.)

We need to be aware of its strengths and pitfalls, so let's talk, discuss and educate.

NLP AND LLMS

- ❑ Natural Language Processing (NLP) is the technology to handle human language using computers.
- ❑ A Language Model assigns a probability to a piece of text
 - ❑ Compute the probability of a sentence or a sequence of words: $P(w) = P(w_1, w_2, w_3, w_4, w_5 \dots w_n)$
 - ❑ Probability of an upcoming word:
 $P(w_5 | w_1, w_2, w_3, w_4)$
- ❑ When the model had much more parameters and training data we call it **Large Language Model (LLM)**

Example	Probability
The cat sat on the mat	0.95
The cat sad on the mat	0.20

High wind tonight	0.97
Large wind tonight	0.31

The cat

ALWAYS KEEP IN MIND!

LLMs are language models,
not knowledge models!

PROMPTING

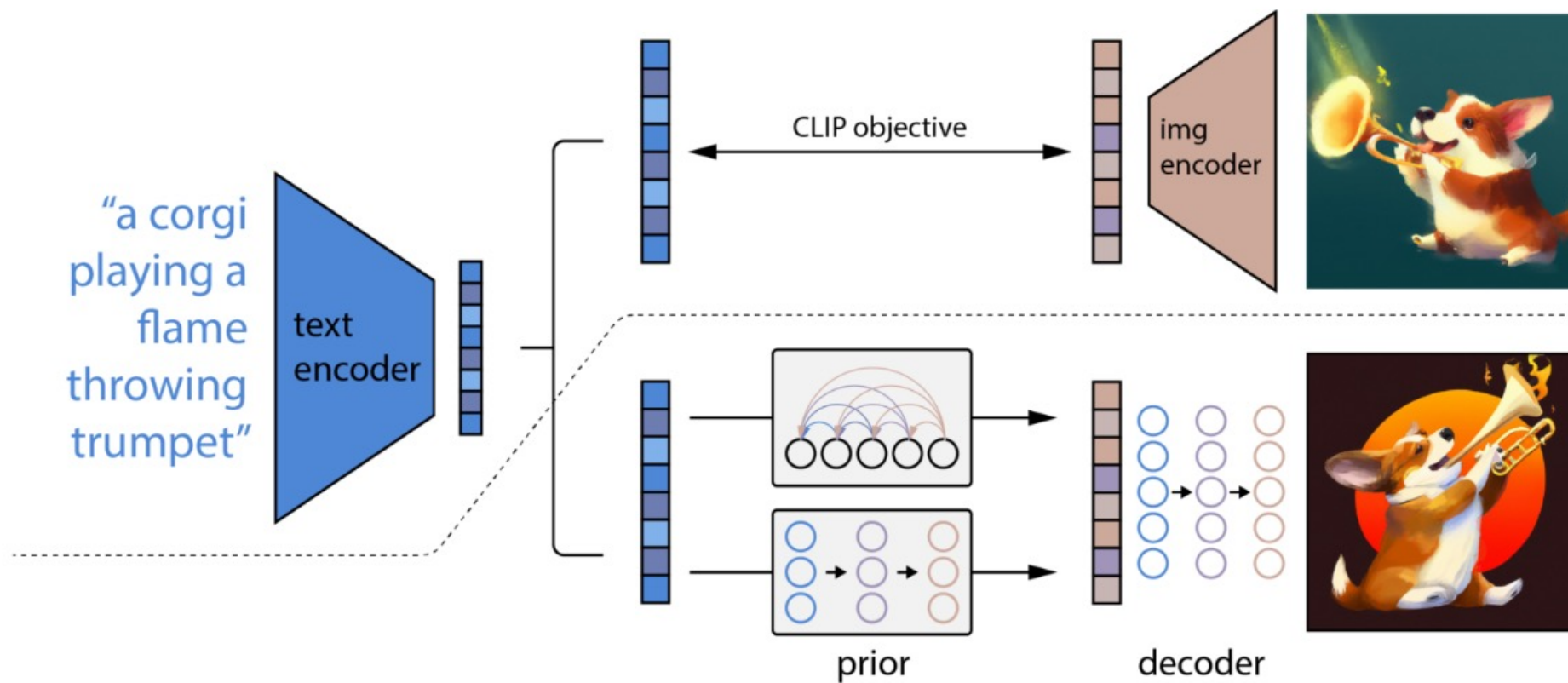
Introduction

- In the context of LLMs, **prompting** refers to the act of providing specific instructions or input to guide the generation of text or responses.
- When interacting with a language model, users can provide a prompt that sets the context or specifies the desired output.
- Examples:
 - What is the best itinerary for a trip in the south of Mexico?
 - Give me a recipe for a cake with no eggs
 - The sky is blue and today I...

AGENDA

1. Introduction
2. Modern Applications
3. General Recommendations
4. Blablador: A Privacy-Focused Alternative, No Data Stored
5. Conclusions and open questions

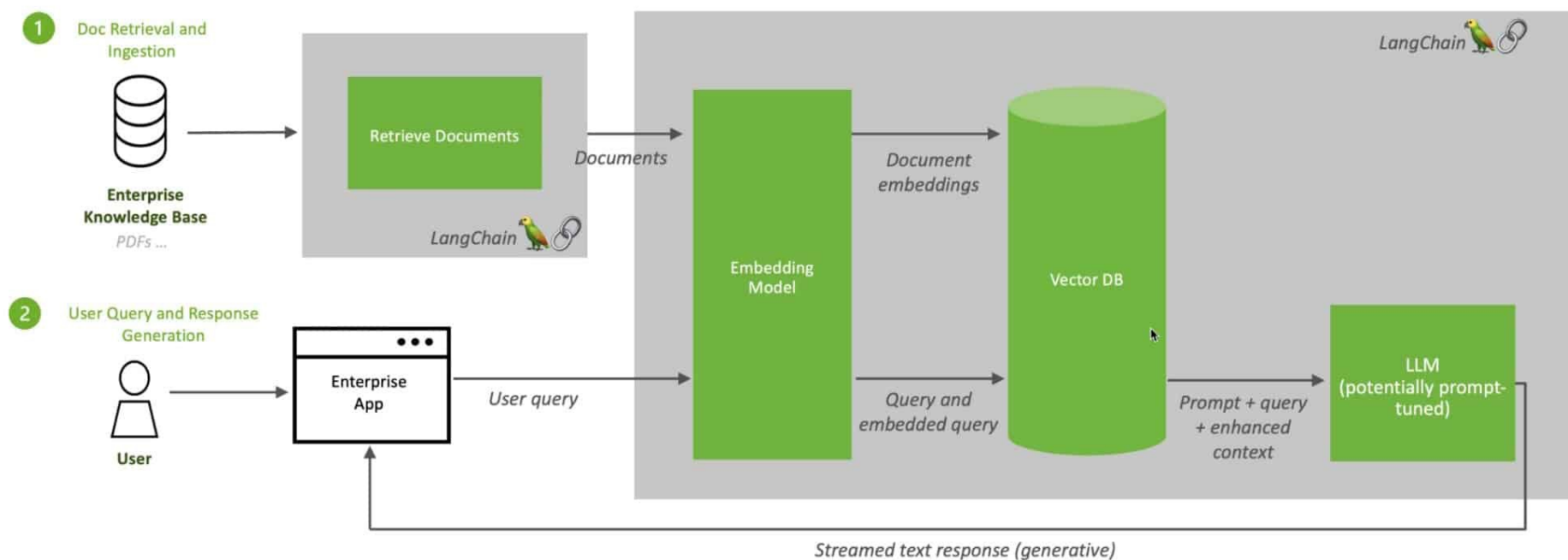
DALL-E



RETRIEVAL AUGMENTED GENERATION

RAG

Retrieval Augmented Generation (RAG) Sequence Diagram



<https://blogs.nvidia.com/wp-content/uploads/2023/11/NVIDIA-RAG-diagram-scaled.jpg>

MUSIC GENERATION

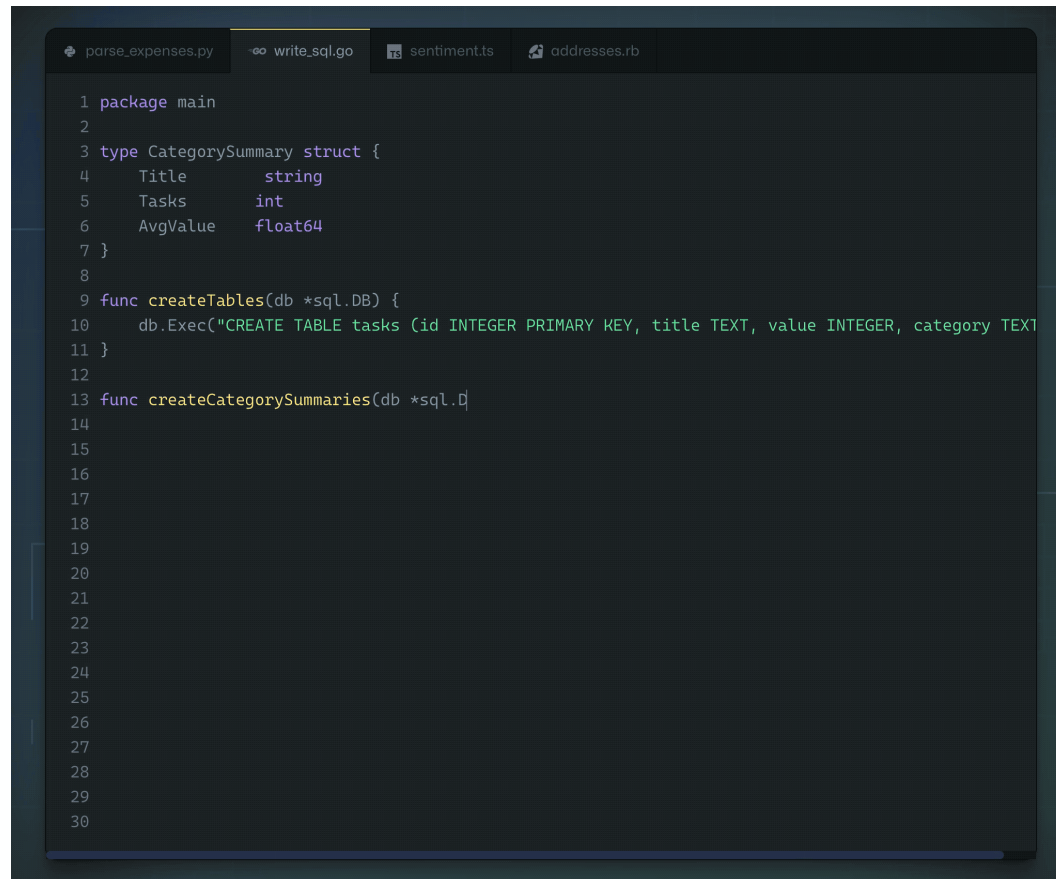
Suno

- Writes lyrics from a description
- Takes an indication on the style of the music
- Generates a song from the lyrics



CODING

Github copilot

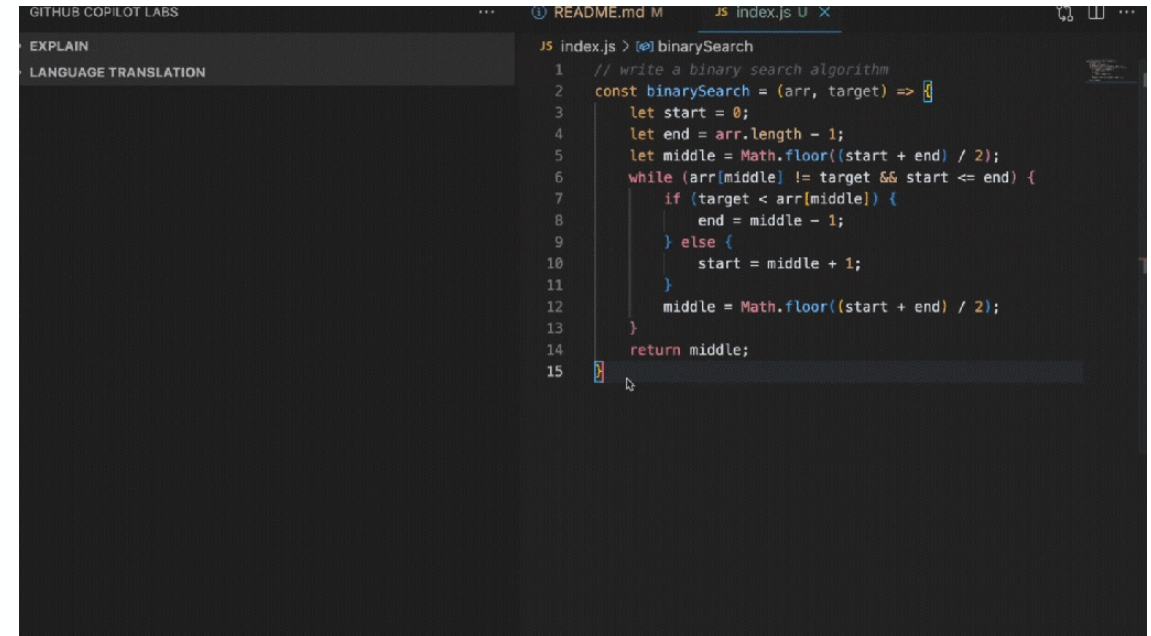


```

1 package main
2
3 type CategorySummary struct {
4     Title      string
5     Tasks      int
6     AvgValue    float64
7 }
8
9 func createTables(db *sql.DB) {
10     db.Exec("CREATE TABLE tasks (id INTEGER PRIMARY KEY, title TEXT, value INTEGER, category TEXT)")
11 }
12
13 func createCategorySummaries(db *sql.DB) {
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30

```

<https://techcrunch.com/wp-content/uploads/2021/06/GitHub-Copilot-2.gif>



```













1 // write a binary search algorithm
2 const binarySearch = (arr, target) => {
3     let start = 0;
4     let end = arr.length - 1;
5     let middle = Math.floor((start + end) / 2);
6     while (arr[middle] !== target && start <= end) {
7         if (target < arr[middle]) {
8             end = middle - 1;
9         } else {
10             start = middle + 1;
11         }
12         middle = Math.floor((start + end) / 2);
13     }
14     return middle;
15 }

```

<https://github.blog/wp-content/uploads/2022/09/unexpectedcopilot7.gif?w=1024&resize=1024%2C576>

https://education.github.com/discount_requests/application

CUSTOM GPTS

 Tech Support Advisor From setting up a printer to troubleshooting a device, I'm here to help you step-by-step.	By ChatGPT	 Data Analysis Drop in any files and I can help analyze and visualize your data
 Coloring Book Hero Take any idea and turn it into whimsical coloring book pages	By ChatGPT	 ChatGPT Classic The latest version of GPT-4 with no additional capabilities
 Laundry Buddy Ask me anything about stains, settings, sorting and everything laundry.	By ChatGPT	 Game Time I can quickly explain board games or card games to players of any age. Let the games begin!
 Sous Chef I'll give you recipes based on the foods you love and ingredients you have.	By ChatGPT	 The Negotiator I'll help you advocate for yourself and get better outcomes. Become a great negotiator.
 Sticker Whiz I'll help turn your wildest dreams into die-cut stickers, shipped right to your door.	By ChatGPT	 Creative Writing Coach I'm eager to read your work and give you feedback to improve your skills.
 Math Mentor I help parents help their kids with math. Need a 9pm refresher on geometry proofs? I'm here for you.	By ChatGPT	 Cosmic Dream Visionary painter of digital wonder

CUSTOM GPTS

Setting up

Create

Configure

Name

Name your GPT

Description

Add a short description about what this GPT does

Instructions

What does this GPT do? How does it behave? What should it avoid doing?

Conversation starters

Knowledge

If you upload files under Knowledge, conversations with your GPT may include file contents. Files can be downloaded when Code Interpreter is enabled

Upload files

Capabilities

☒ Web Browsing

☒ DALL-E Image Generation

☐ Code Interpreter & Data Analysis

Actions

Create new action

<

Add actions

Let your GPT retrieve information or take actions outside of ChatGPT.

Learn more.

None

Schema

Import from URL

Examples

Taken from https://github.com/OAI/OpenAPI-Specification/blob/main/examples/v3.0/petstore.yaml

```
openapi: "3.0.0"
info:
  version: 1.0.0
  title: Swagger Petstore
  license:
    name: MIT
servers:
  - url: https://petstore.swagger.io/v1
paths:
  /pets:
    get:
      summary: List all pets
      operationId: listPets
      tags:
        - pets
      parameters:
        - name: limit
          in: query
          description: How many items to return at one time (max 100)
          required: false
          schema:
            type: integer
```

Format

Available actions

Name	Method	Path	
listPets	GET	/pets	Test
createPets	POST	/pets	Test

CUSTOM GPTS

Consensus

- Send the query directly to Consensus
- Consensus is an academic search engine, powered by AI, but grounded in scientific research.
- They use their own LLM and perform a search against a database of scientific papers
- <https://consensus.app/home/blog/welcome-to-consensus/>

CUSTOM GPTS

VEED

- Step1: Script creation (ChatGPT)
 - The model is instructed to ask specific questions
- Step 2: Send the script to VEED and a "male" or "female" parameter for the voice
- VEED:
 - Text to speech
 - "Smart" retrieval of images and videos for the script
 - The user can edit the video



CUSTOM GPTS

Data Analyst

- Chat with Excel sheets
- Impressive, it also cross-references data from multiple sheets
- Can suggest interesting statistics and plots
- Uses Python in the backend
- You can (and have to) review the Python code to verify the accuracy of the output



OPEN-SOURCE PROJECTS

- Online demos
 - <https://huggingface.co/spaces>
 - <https://build.nvidia.com/explore/discover>
 - Open source LLMs
 - <https://github.com/Hannibal046/Awesome-LLM>
- 😊 They can be deployed locally; you decide what happens to the processed data
- 😞 ChatGPT (or similar) has a better model, which is continuously updated its model

LLMS AS APIS

Example: a company that has a bunch of customer reviews, and wants to do something with this data

☐ Classical approach

- ☐ Get a general idea about comments
- ☐ Redirect reviews to the relevant department
- ☐ Detect spams
- ☐ ...

☐ LLM approach

- ☐ One single model
- ☐ Several prompts

AGENDA

1. Introduction
2. Modern Applications
3. General Recommendations
4. Blablador: A Privacy-Focused Alternative, No Data Stored
5. Conclusions and open questions

GENERAL RECOMMENDATIONS

Technical recommendations

PROMPTING

Elements of a prompt

A prompt contains any of the following elements:

- ❑ **Instruction** a specific task or instruction you want the model to perform.
- ❑ **Context** external information or additional context that can steer the model to better responses.
- ❑ **Input Data** the input or question that we are interested to find a response for.
- ❑ **Output Indicator** the type or format of the output.

You do not need all the four elements for a prompt and the format depends on the task at hand.

PROMPT DESIGN

General tips (1/4)

1. Write Clear Instructions:

- ❑ Use clear and specific commands to instruct the model (e.g., Write, Classify, Summarize)
- ❑ Include details in your query to get more relevant answers
- ❑ Ask the model to adopt a persona
- ❑ Use delimiters to clearly indicate distinct parts of the input (e.g. use "###" to separate the instruction from context)
- ❑ Specify the steps required to complete a task
- ❑ Provide examples
- ❑ Specify the desired format and length of the output

PROMPT DESIGN

General tips (2/4)

Explain the concept prompt engineering. Keep the explanation short, only a few sentences, and don't be too descriptive.



Use 2–3 sentences to explain the concept of prompt engineering to a high school student.



D You
 ### Instruction###
 Translate the text below into Spanish

Text ###
 "Hello!"
 < 2 / 2 >

ChatGPT
Text
 ¡Hola!

D You
 Question: what are the pro and cons of using ChatGPT
 Instruction: answer with a table containing three pros and three cons

ChatGPT

Pros	Cons
1. Versatility	1. Lack of real-world knowledge
2. User-friendly interface	2. Potential for biased or inappropriate responses
3. Continuous learning	3. Dependency on input phrasing and biases



D You
 Context: You are an expert astrophysicist who wants to explain the concept of Gamma-Ray Burst to an 12-year old.
 Instruction: Give the explanation in 3 bullet point

ChatGPT

- **Gamma-Ray Bursts (GRBs) are powerful cosmic explosions:**
 - They're like super-bright flashes of gamma rays, which are really energetic rays of light.
- **Originating from faraway places in space:**
 - GRBs happen in distant galaxies and are caused by events like collapsing stars or the merging of compact objects.
- **Scientists use special tools to study them:**
 - We have telescopes and satellites that help us observe and understand these bursts, unlocking the mysteries of the universe.



PROMPT DESIGN

General tips (3/4)

2. Give the model time to "think"

- ❑ Instruct the model to work out its own solution before rushing to a conclusion
- ❑ Use inner monologue or a sequence of queries to guide the model's reasoning process
- ❑ Ask the model if it missed anything on previous passes

Standard Prompting	Chain-of-Thought Prompting
<p>Model Input</p> <p>Q: Roger has 5 tennis balls. He buys 2 more cans of tennis balls. Each can has 3 tennis balls. How many tennis balls does he have now?</p> <p>A: The answer is 11.</p> <p>Q: The cafeteria had 23 apples. If they used 20 to make lunch and bought 6 more, how many apples do they have?</p>	<p>Model Input</p> <p>Q: Roger has 5 tennis balls. He buys 2 more cans of tennis balls. Each can has 3 tennis balls. How many tennis balls does he have now?</p> <p>A: Roger started with 5 balls. 2 cans of 3 tennis balls each is 6 tennis balls. $5 + 6 = 11$. The answer is 11.</p> <p>Q: The cafeteria had 23 apples. If they used 20 to make lunch and bought 6 more, how many apples do they have?</p>
<p>Model Output</p> <p>A: The answer is 27. ❌</p>	<p>Model Output</p> <p>A: The cafeteria had 23 apples originally. They used 20 to make lunch. So they had $23 - 20 = 3$. They bought 6 more apples, so they have $3 + 6 = 9$. The answer is 9. ✅</p>

PROMPT DESIGN

General tips (4/4)

3. Provide reference text

- ❑ Instruct the model to answer using a reference text
- ❑ Instruct the model to answer with citations from a reference text

4. Split complex tasks into simpler subtasks

- ❑ Use intent classification to identify the most relevant instructions for a user query
- ❑ For dialogue applications that require very long conversations, summarize or filter previous dialogue
- ❑ Summarize long documents piecewise and construct a full summary recursively

PROMPT DESIGN

Prompt design patterns

From Vanderbilt University [Full paper](#), [Course on coursera](#)

- ❑ **Persona and audience persona pattern**
 - ❑ Act as a nutritionist, I am going to tell you what I am eating and you will tell me about my eating choices.
 - ❑ Explain large language models to me. Assume that I am a 13 year old who is passionate about star wars.
- ❑ **Flipped interaction pattern**
 - ❑ I would like you to ask me questions to help me diagnose a problem with my Internet. Ask me questions until you have enough information to identify the two most likely causes. Ask me one question at a time. Ask me the first question.

PROMPT DESIGN

Prompt design patterns

- ❑ **Question refinement pattern**

- ❑ From now on, whenever I ask a question, suggest a better version of the question and ask me if I would like to use it instead

- ❑ **Fact check list pattern**

- ❑ Whenever you output text, generate a set of facts that are contained in the output. The set of facts should be inserted at the end of the output. The set of facts should be the fundamental facts that could undermine the veracity of the output if any of them are incorrect.

- ❑ **Alternative approaches pattern**

- ❑ If there are alternative ways to accomplish a task X that I give you, list the best alternate approaches. Compare/contrast the pros and cons of each approach

PROMPT DESIGN

Prompt design patterns

☐ Semantic filter pattern

- ☐ Filter this text to remove any personally identifying information.

☐ Few shot prompting

- ☐ This is awesome! // Negative
This is bad! // Positive
Wow that movie was rad! // Positive
What a horrible show! //

☐ Cognitive verifier pattern

- ☐ When you are asked a question, follow these rules. Generate a number of additional questions that would help you more accurately answer the question. Combine the answers to the individual questions to produce the final answer to the overall question.

PROMPT DESIGN

Prompt design patterns

❑ Outline expansion pattern

- ❑ Act as an outline expander. Generate a bullet point outline based on the input that I give you and then ask me for which bullet point you should expand on. Create a new outline for the bullet point that I select. At the end, ask me for what bullet point to expand next. Ask me for what to outline.

❑ Tail generation pattern

- ❑ From now on, at the end of your output, add the disclaimer "This output was generated by a large language model and may contain errors or inaccurate statements. All statements should be fact checked." Ask me for the first thing to write about.

PROMPT DESIGN

Prompt design patterns

❑ Template pattern

- ❑ Create a random strength workout for me today with complementary exercises. I am going to provide a template for your output . CAPITALIZED WORDS are my placeholders for content. Try to fit the output into one or more of the placeholders that I list. Please preserve the formatting and overall template that I provide. This is the template: NAME, REPS @ SETS, MUSCLE GROUPS WORKED, DIFFICULTY SCALE 1-5, FORM NOTES

❑ Game play pattern

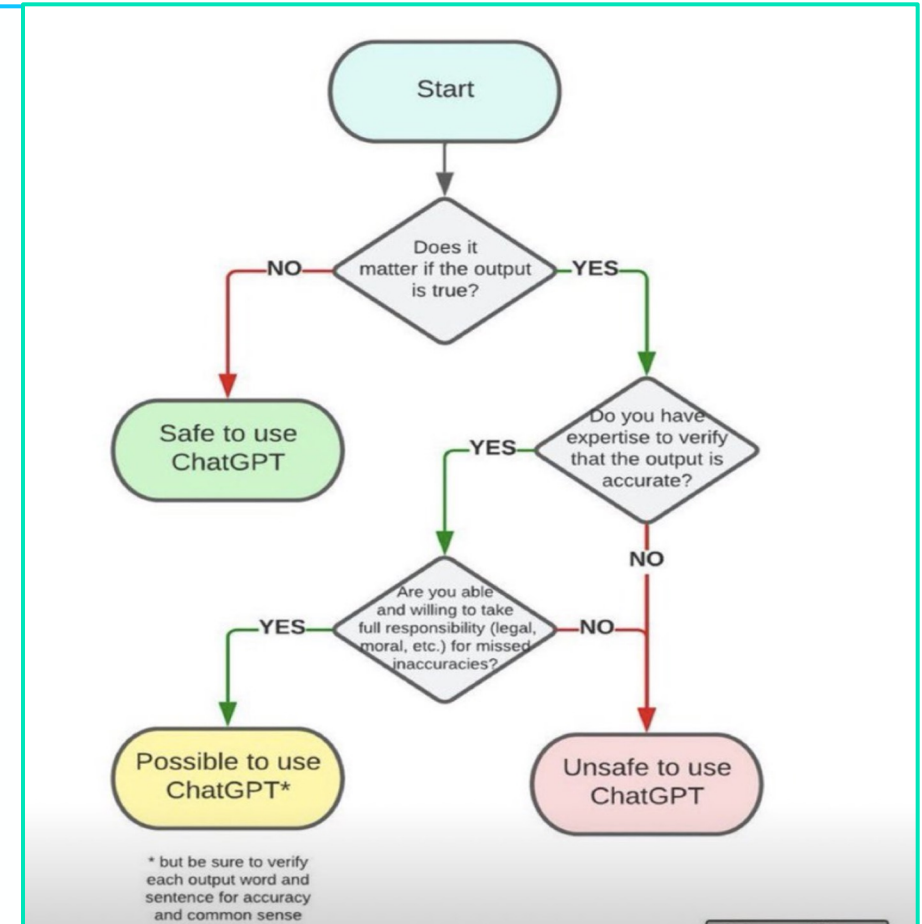
- ❑ Create a cave exploration game for me to discover a lost language. Describe where I am in the cave and what I can do. I should discover new words and symbols for the lost civilization in each area of the cave I visit. Each area should also have part of a story that uses the language. I should have to collect all the words and symbols to be able to understand the story. Tell me about the first area and then ask me what action to take.

GENERAL RECOMMENDATIONS

“Usage” recommendation

GENERAL RECOMMENDATIONS

- ❑ **Verify Accuracy:** Always cross-check critical information when using LLMs
- ❑ **Use Ethically:** Avoid malicious activities and misrepresentation, as this will have serious consequences on tremendous users
- ❑ **Protect Privacy:** Refrain from sharing sensitive personal data



"Is it safe to use ChatGPT for your task?" by Aleksander Tiulkanov

OFFICIAL GUIDELINES FOR WRITING WITH LLMS

(1/3)

- ❑ [DFG Press Release No. 30, September 2023](#)
 - ❑ Researchers can use generative models in their research work but must disclose the use of generative models.
 - ❑ Generative models can be included in funding proposals submitted to the DFG.
 - ❑ Documents provided for review are confidential and cannot be used as input for generative models.
- ❑ [Intellectual property in ChatGPT, European Commission, February 2023](#)
 - ❑ Content generated may be copyrighted, but ChatGPT, as an AI, cannot own it (current laws do not recognize AI as having legal personality)
 - ❑ OpenAI's terms: **Users own their input and output**, though the output generated may not be unique.

OFFICIAL GUIDELINES FOR WRITING WITH LLMS

(2/3)

- ❑ [Conferences: example AISTATS 2024](#)
 - ❑ LLMs can't be used to generate text longer than one page, but can be used for text polishing without restrictions.
 - ❑ It is still the authors responsibility to ensure their submissions' quality, correctness, and originality.
 - ❑ The use of LLM-generated content must be disclosed, and doubtful submissions will undergo checks for misconduct

Make sure that you are up to date with potential new regulations

OFFICIAL GUIDELINES FOR WRITING WITH LLMS

(3/3)

- ❑ Researchers should disclose the tools and algorithms they used and clearly identify the contributions of machines and humans.
- ❑ Researchers remain responsible for the accuracy of the data and the conclusions they draw from it, even if they have used AI analysis tools.
- ❑ AI-generated data must be labeled so that it cannot be confused with real-world data and observations.
- ❑ Experts must ensure that their findings are scientifically sound and do no harm. For example, the risk of the AI being "biased" by the training data used must be kept to a minimum.
- ❑ Finally, researchers, together with policymakers, civil society and business, should monitor the impact of AI and adapt methods and rules as necessary.

<https://www.tum.de/en/news-and-events/all-news/press-releases/details/guidelines-for-the-use-of-ai-in-science>

<https://www.pnas.org/doi/epdf/10.1073/pnas.2407886121>

AGENDA

1. Introduction
2. Modern Applications
3. General Recommendations
4. Blablador: A Privacy-Focused Alternative, No Data Stored
5. Conclusion and reflexion



BLABLADOR

Homemade solution

HELMHOLTZAI | ARTIFICIAL INTELLIGENCE COOPERATION UNIT

This is *BLABLADOR*, our experimental large language model server! 🐶

Different models might be available at Alex Strube's whim. These are the models currently running:

Mistral-7B-Instruct-v0.2

🗨 This is what I have to say.... Remember: I am a BLABLADOR! Not all I say is true or even real

BLA!

Click and press ENTER

Send

🔄 Regenerate

🗑 Clear history

Parameters

AGENDA

1. Introduction
2. Modern Applications
3. General Recommendations
4. Blablador: A Privacy-Focused Alternative, No Data Stored
5. Conclusion and reflexion

CONCLUSION

Main takeaway

Applications of LLMs are crazy impressive, but it's more important than ever to be careful with your input and output!

REFLECTION

Shift in researchers' skills

Important skills in the era of LLMs ([Fecher et al., 2023](#))

- ❑ Prompt engineering
- ❑ Critical thinking
- ❑ Problem solving
- ❑ Ethical decision making
- ❑ Creativity

"A good researcher will be able to read and interpret, more than writing" [Tuebner et al., 2023](#)

REFLECTION

Should we stop encouraging kids to code?



<https://www.youtube.com/watch?v=6Lcy2N3Ycls>

“Over the last 10-15 years, almost everybody who sits on a stage like this would tell you that it is vital that your children learn computer science, everybody should learn how to program. And in fact, it's almost exactly the opposite.

It is our job to create computing technology such that nobody has to program, and that the programming language is human. Everybody in the world is now a programmer. This is the miracle of AI”.

Jensen Huang, NVIDIA CEO

SOME OTHER TOOLS AND RESOURCES

- ❑ [Prompt examples](#): conversational search engine, answers with verifiable sources
- ❑ [Perplexity.ai](#): a conversational search engine, answering questions with verifiable sources
- ❑ [ExplainPaper](#): upload a research paper and ask for explanations for complex text passages and equations, break down information in simple words
- ❑ [NVIDIA Chat with RTX](#)
- ❑ [Gemini](#): chatbot from Google
- ❑ [Claude.ai](#)
- ❑ [ChatGPT failures](#): LLM failure archive (ChatGPT and beyond)
- ❑ [Our prompt engineering and LLM repo](#) Practical examples for coding and writing

- **Please note that this list might not be exhaustive, but it is a collection of tools we have tried out in our team.*