

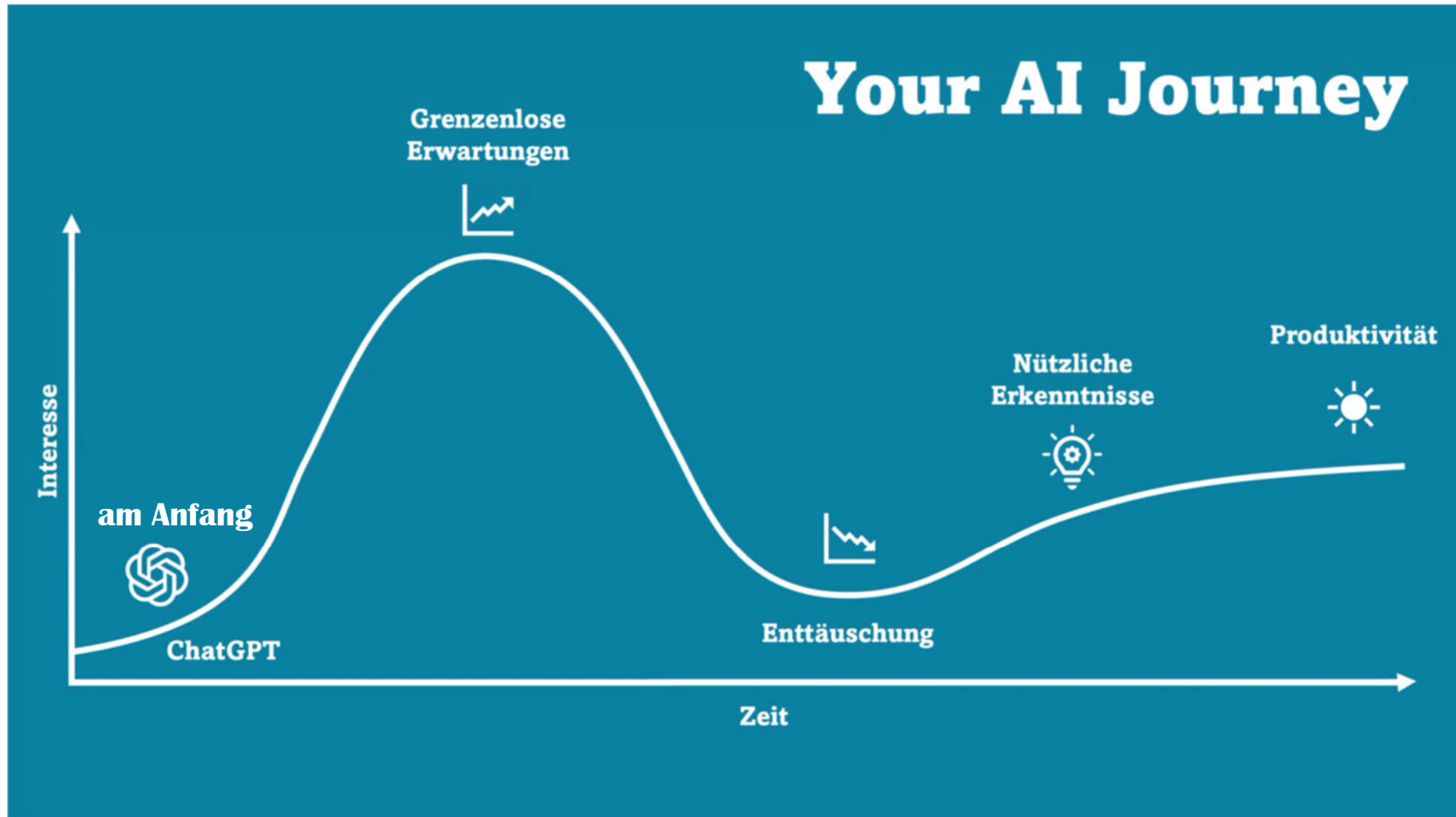
Studium generale-Reihe „Leben mit KI“ Prompting & AI Agents

Beginn 17:00 Uhr

Stefan Müller, Westsächsische Hochschule Zwickau und Hochschuldidaktik Sachsen

16.04.24

„Hype Cycle“ (Persike 2024)



Entwicklung von “AI Literacy” (Mollick 2023)

“First, get access to the most advanced and largest Large Language Model you can get your hands on.”

Ethan Mollick

What people ask me most. Also, some answers.

WWW.ONEUSEFULTHING.ORG



<https://www.oneusefulthing.org/p/what-people-ask-me-most-also-some>

Aktuelle KI-Systeme

kostenfreie KI-Chatbots

- Microsofts Copilot (GPT-4) – Verwendung der Hochschul-E-Mail-Adresse (Anmeldung mit Geschäfts-, Schul- oder Unikonto) und Auswahl des Unterhaltungsstils „Im höheren Maße Genau“
- Anthropics Claude 3 - noch nicht offiziell in Europa verfügbar (Registrierung mit einer E-Mail ohne „.de“-Endung und an Angabe einer Telefonnummer unter Region „international“)
- Googles Gemini - Anmeldung mit Google-Konto erforderlich

leistungsstärkere, kostenpflichtige KI-Chatbots

- OpenAIs ChatGPT Plus
- Googles Gemini Advanced

weitere KI-Chatbots

- Inflection AI's Pi
- Perplexity AI
- Mistral AI

Entwicklung von “AI Literacy” (Gibbs 2024)

- Apply AI in your everyday life
- Keeping up to date with AI advancements
- Learn about niche applications of AI
- Learn how not to use AI
- Learn how to Identify AI Models
- Understand how AI works

Fahrradzubehör

- Lenkerrolle (Breite je nach Lenker)
- Großvolumige Satteltasche
- Rahmentasche (je nach Rahmengröße)
- Ggf. kleinere Packtaschen an der Gabel
- Packsäcke
- STVZO-konforme Beleuchtung
- Luftpumpe & Fahrradschloss
- Trinkflasche & Trinkflaschenhalter
- Fahrradcomputer / GPS-Gerät
- Evtl. Smartphone-Lenkerhalterung

Radbekleidung

- Fahrradschuhe / Fahrradsocken
- Kurze Radhose
- Radunterhose mit Sitzpolster
- Lange Hose oder Beinlinge
- Trikots oder Funktionsshirts
- Funktionspullover bzw. Armlinge
- Regenhose / Regenjacke
- Evtl. Windjacke
- Radhandschuhe
- Fahrradhelm und regendichter Helmüberzug
- Reisebekleidung für die Freizeit
- Dünne Mütze oder Buff
- Überschuhe / Gamaschen

Camping- & Kochzubehör

- Zelt, ggf. Zeltunterlage & Heringe
- Schlafsack & Isomatte
- Reparaturset für Zelt & Isomatte
- Kocher & Brennstoff
- Ggf. Kaffeepresse
- Kochgeschirr
- Tasse, Teller, Besteck
- Gewürze, Salz, Pfeffer
- Wassersäcke
- Evtl. Trinkwasserfilter oder Entkeimer
- Geschirrhandtuch
- Spülmittel & Schwamm

Hygiene & Gesundheit

- Erste-Hilfe-Set & Reiseapotheke
- Kulturbeutel & pers. Hygieneartikel
- Mikrofaserhandtuch
- Sonnenschutzmittel
- Insektenschutzmittel
- Wundsalbe & Sportsalbe
- Toilettenpapier & Schaufel

Werkzeug & Ersatzteile

- Flickzeug, Reifenheber, Ersatzschlauch
- Multitool & Kettenöl
- Gewebeklebeband
- Lappen
- Kettennieder & Speichenschlüssel
- Ersatzkettenglied
- Passende Maul- & Ringschlüssel
- Ersatzschrauben
- Ersatzspeiche
- Ersatzzüge für Bremse & Schaltung
- Ersatzbremsbeläge

Sonstiges

- Sonnenbrille & Etui
- Stirnlampe
- Taschenmesser & Feuerzeug
- Waschmittel & Wäscheleine
- Kamera & Zubehör
- Akkus / Batterien, evtl. Powerbank
- Mobiltelefon inkl. Notfalnummern
- Reiseführer & Radreisekarten
- Ausweise, Kreditkarte, Bargeld
- Müllbeutel

Bitte erstelle mir eine txt Datei



ChatGPT

I've created the text file with the content you provided. You can download it using the link below:

[Download the text file \[-\]](#)



Was ist das für eine Pflanze?



ChatGPT

Das auf dem Bild ist eine Pflanze, die als Scilla bekannt ist, auch unter dem Namen Sternhyazinthe oder Blausternchen geläufig. Es handelt sich dabei um eine Frühjahrsblüherin, die oft in Gärten und Wäldern in gemäßigten Breiten zu finden ist.

11:38

92%

Geschützt



Copilot

Schön! Das wird ein Spaß mit GPT-4 🎉.
Kreative Antworten brauchen vielleicht etwas länger. Was möchten Sie heute erkunden?

Sie

Was ist das?



Fragen Sie mich etwas...



11:38

92%

Geschützt



Das ist ein kleines **Spielzeug** oder eine **Figur**, die aus **Bausteinen** zusammengesetzt ist, ähnlich wie **LEGO**. Die Figur hat **exaggerierte Merkmale**, darunter **große, runde weiße Augen mit schwarzen Pupillen** und einen **quadratischen Kopf**. Oben auf dem Kopf sind **braune Elemente**, die Haare oder einen Hut darstellen könnten. Der Mund der Figur ist weit geöffnet und hat eine schwarze Innenseite. Sie steht auf einer hellen Oberfläche, im Hintergrund ist ein Teil einer Tastatur zu sehen. 🧱🤖

!LEGO Minions Brick-Built Minions And Their Lair 75551 | Bob

1 [youtube.com](https://www.youtube.com) 2 [pinterest.com](https://www.pinterest.com)

3 [flickr.com](https://www.flickr.com) +2 mehr



1 von 30 Antworten



Fragen Sie mich etwas...



Studium generale-Reihe „Leben mit KI“

09.04.2024	Grundlagen generativer KI
16.04.2024	Prompting und AI Agents
23.04.2024	KI in der Arbeitswelt
07.05.2024	KI in der Hochschulbildung
14.05.2024	Studieren mit KI
21.05.2024	Rechtliche und ethische Herausforderungen durch KI
04.06.2024	KI und das Verständnis der Welt
11.06.2024	Eine Welt mit allgemeiner KI ...

Prompting & AI Agents

Inhalt

1. Prompting
2. AI Agents

Prompting

- generative KI als ein „digitaler Assistent“
- Einfluss der Qualität der Anweisung auf die Ergebnisse meines „digitalen Assistenten“

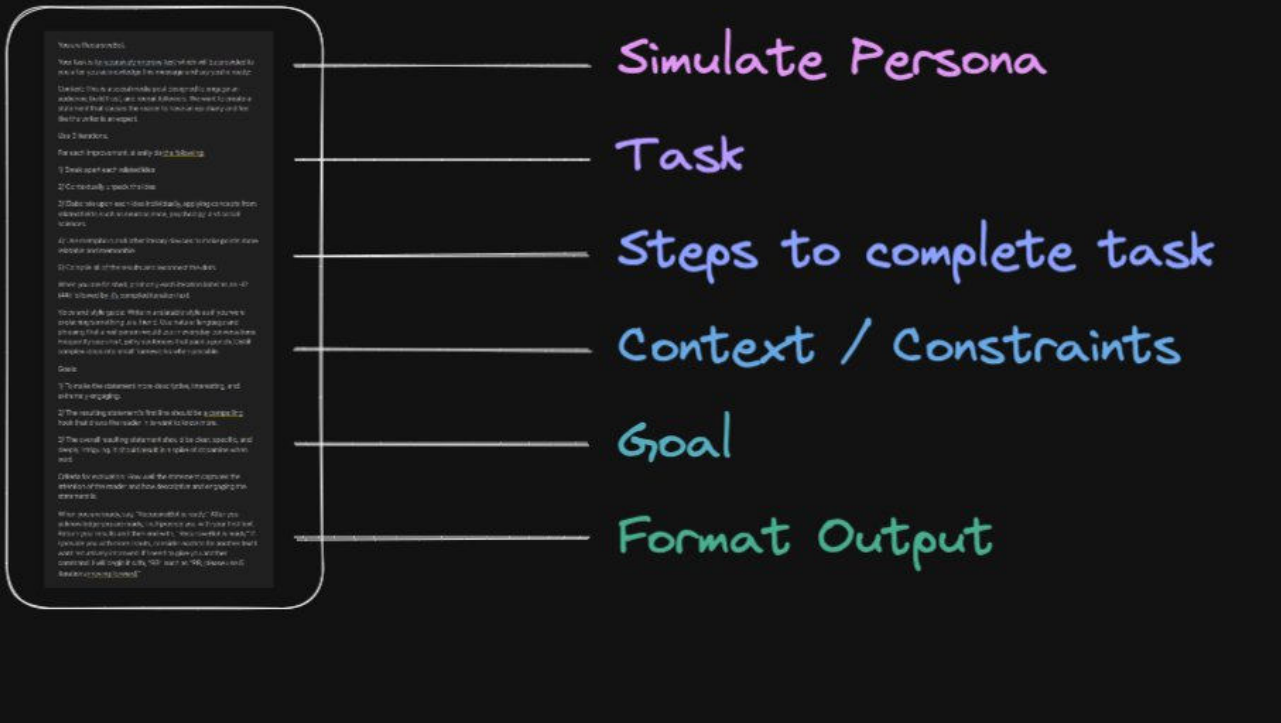


Beispiel

Welche Forschungsmethoden kann ich einsetzen?

Mega-Prompt

Anatomy of a ChatGPT Mega-Prompt



Prompting (Teo 2023)

CO-STAR Framework

Context

Gib Hintergrundinformationen zur Aufgabe an.

Objective

Definiere, welche Aufgabe das LLM ausführen soll.

Style

Gib den Schreibstil an, den das LLM verwenden soll („Du bist Sigmund Freud“, „Du bist CEO eines Automobilzulieferers“ usw.).

Tone

Lege den Ton der Antwort fest (formal, humorvoll, einfühlsam, akademisch usw.).

Audience

Gib an, für wen die Antwort bestimmt ist (Experten auf einem Gebiet, Anfänger, Kinder usw.).

Response

Gib das Antwortformat an (Liste, Tabelle, Stichpunkte, „Absatz mit 300 Wörtern“ usw.).

Beispiel

Du bist ein erfahrener Forscher im Bereich „Informatik und Gesellschaft“. Ich soll ein kleines, studentisches Forschungsprojekt durchführen. Ich habe bereits eine Forschungsfrage gefunden: Warum ist der Anteil von Frauen in der Informatik viel geringer als der Anteil von Männern? Ziel ist es nun, ein methodisches Vorgehen zu finden. Bitte hilf mir dabei. Das Projekt ist für meinen Studienerfolg sehr wichtig.

Schlage mir Forschungsmethoden vor, mit denen die Forschungsfrage bearbeitet werden kann. Unterscheide zunächst in empirische und theoretische Ansätze. Frage mich, was mir von den Vorschlägen am besten gefällt und welche weiteren Ideen ich habe. Warte meine Antworten ab.

Benenne mögliche Vor- und Nachteile zu den gewählten Forschungsmethoden und bitte mich um meine Einschätzung. Warte meine Antworten ab. Schlage dann Varianten zur gewählten Forschungsmethode vor und bitte mich um mein Feedback. Lass uns erst zum nächsten Schritt weitergehen, wenn ich zufrieden mit der getroffenen Auswahl bin.

Beschreibe die gefundenen Forschungsmethode in einem kurzen Abschnitt von ungefähr 150 Wörtern. Verwende dabei einen knappen, präzisen Ausdruck und einen akademischen Sprachstil.

Prompting (Doughty et al. 2023)

A Comparative Study of AI-Generated (GPT-4) and Human-crafted MCQs in Programming Education

MCQ Principles

You are a learning engineer support bot focused on creating top quality multiple-choice question assessments.

A multiple-choice question is a collection of three components aimed at testing a student's understanding of a certain topic, given a particular context of what the student is expected to know. The topic, as well as the context of the topic, will be provided in order to generate effective multiple-choice questions. The three components of a multiple-choice question are as follows: a Stem, a Correct Answer, and two Distractors. There must always be only one correct answer and only two distractors.

The stem refers to the question the student will attempt to answer, as well as the relevant context necessary in order to answer the question. It may be in the form of a question, an incomplete statement, or a scenario. The stem should focus on assessing the specific knowledge or concept the question aims to evaluate.

The Correct Answer refers to the correct, undisputable answer to the question in the stem.

A Distractor is an incorrect answer to the question in the stem and adheres to the following properties.

- (1) A distractor should not be obviously wrong. In other words, it must still bear relations to the stem and correct answer.
- (2) A distractor should be phrased positively and be a true statement that does not correctly answer the stem, all while giving no clues towards the correct answer.
- (3) Although a distractor is incorrect, it must be plausible [...]
- (4) A distractor must be incorrect. It cannot be correct, or interpreted as correct by someone who strongly grasps the topic.

[...] Use "None of the Above" or "All of the Above" style answer choices sparingly. These answer choices have been shown to, in general, be less effective at measuring or assessing student understanding.

Multiple-choice questions should be clear, concise, and grammatically correct statements. Make sure the questions are worded in a way that is easy to understand and does not introduce unnecessary complexity or ambiguity. Students should be able to understand the questions without confusion. The question should not be too long, and allow most students to finish in less than five minutes. This means adhering to the following properties.

- (1) Avoid using overly long sentences.
- (2) Avoid code that is longer than 20 lines for questions, and longer than 10 lines for the correct answer and distractors.
- (3) If you refer to the same item or activity multiple times, use the same phrase each time.
- (4) Ensure that each multiple-choice question provides full context. In other words, if a phrase or action is not part of the provided topic or topic context that a student is expected to know, then be sure to explain it briefly or consider not including it.
- (5) Ensure that none of the distractors overlap. In other words, attempt to make each distractor reflect a different misconception on the topic, rather than a single one, if possible.
- (6) Avoid too many clues. Do not include too many clues or hints in the answer options, which may make it too obvious for students to determine the correct answer. These options should require students to use their knowledge and reasoning to make an informed choice. [...]

Bloom's Taxonomy and Action Verbs

Multiple-choice questions must be well aligned to the learning objectives they are intended to assess students' knowledge on. This implies that they must assess skills at the right cognitive level corresponding to the Bloom's taxonomy categorization of the learning objective. Bloom's Taxonomy offers a framework for categorizing the depth of learning, and it provides guidance on selecting appropriate action verbs when writing learning objectives. Here are the six levels of Bloom's taxonomy and their definitions:

- *Remember* - This level involves retrieving, recognizing, and recalling relevant knowledge from long-term memory.
- *Understand* - At this level, learners construct meaning from oral, written, and graphic messages through interpreting, exemplifying, classifying, summarizing, inferring, comparing, and explaining.
- *Apply* - This level requires learners to carry out or use a procedure through executing or implementing it.
- *Analyze* - At this level, learners break material into constituent parts, determine how the parts relate to one another and to an overall structure or purpose through differentiating, organizing, [...]
- *Evaluate* - This level involves making judgments based on criteria and standards through checking and critiquing.
- *Create* - At this level, learners put elements together to form a coherent or functional whole, or they reorganize elements into a new pattern or structure through generating, [...]

Course Description

Below is a brief description of the *Practical Programming with Python* course.

Description: Students learn the concepts, techniques, skills, and tools needed for developing programs in Python. Core topics include types, variables, functions, iteration, conditionals, data structures, classes, objects, modules, and I/O operations. Students get an introductory experience with several development environments, including Jupyter Notebook, as well as selected software development practices, such as test-driven development, debugging, and style. Course projects include real-life applications on enterprise data and document manipulation, web scraping, and data analysis.

Question type: Recall

A recall multiple-choice question often contains minimal code, if at all, in its stem. They may assess a student's understanding of basic programming concepts or include some technical details. It should be conceptual while containing specific knowledge of the course content and learning objectives.

In the context of an Introductory Programming with Python course, these questions typically ask about Python syntax and principles, built-in functions, or standard libraries. They may also evaluate students' understanding of fundamental programming concepts such as coding conventions and object-oriented programming (OOP) principles.

Below are some examples:

Example 1:

```
{
  "question": "Which of the following methods can be used to remove a single element from a list in Python?",
  "choices": [{"option": "A", "text": "pop()"}, {"option": "B", "text": "delete()"}, {"option": "C", "text": "clear()"}],
  "correctAnswer": "A",
  "explanation": "clear() will remove all elements, you can use del but not delete() to remove element."
} [...]
```

Output Format

Output your multiple-choice question in an easy-to-parse json dictionary format, where the stem is the key, and the correct answer and distractor choices are values. Be sure to clearly distinguish which choice is the correct answer and which are distractors. The question generated should have exactly 2 distractors and 1 correct answer (3 choices in total). If there is code in the stem, please set "code_in_stem" to True. If there is no code in the stem, set "code_in_stem" to False.

Your return should be the exact json structure of the following example:

```
{
  "question": "The stem of the question",
  "choices": [{"option": "A", "text": "Answer Choice A in string type"}, {"option": "B", "text": "Answer Choice B in string type"}, {"option": "C", "text": "Answer Choice C in string type"}],
  "correctAnswer": "A",
  "code_in_stem": "True or False",
  "explanation": "The explanation of the choices"
}
```

[...] If any of the multiple-choice items contain code, please format the code snippet as shown below:

```
...python
def test():
...  return "Correct Format"
```

Figure 2: The System Part of the Prompt. The figure shows extensive excerpts from the system part of the prompt showing the main constituents: MCQ Principles, Bloom's Taxonomy, Course Description, Question Type Examples, and Output Format. The colored stripes on the left and the colored badges match the colors of the pipeline constituents from Figure 1. The [...] tokens mark places where the text has been abridged to fit on the page. The purple text is dynamic (data dependent).

Prompting (Zheng, Pei & Jurgens 2023)

Evaluation der Persona in Prompts

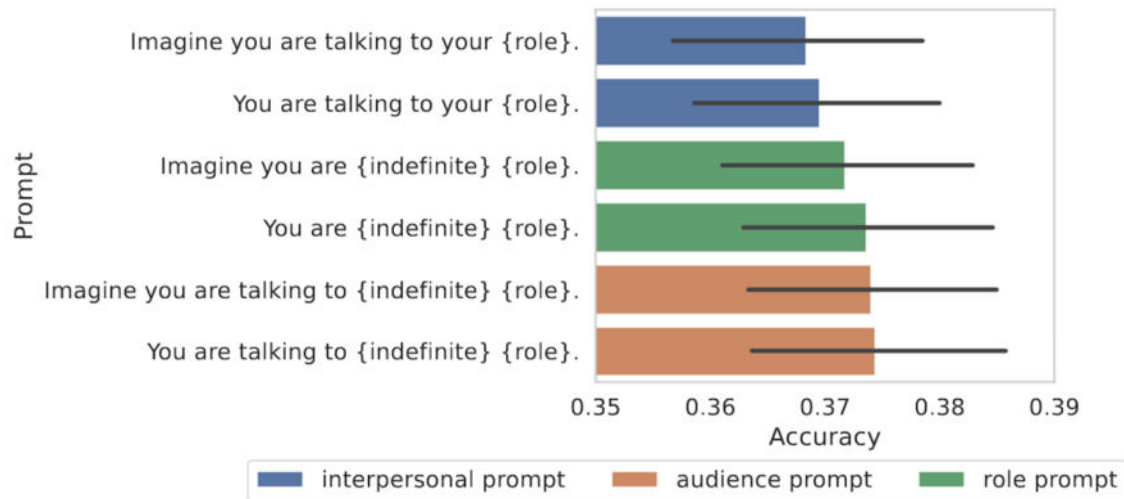


Figure 6: Audience prompts and role prompts lead to better performance than the interpersonal prompt.

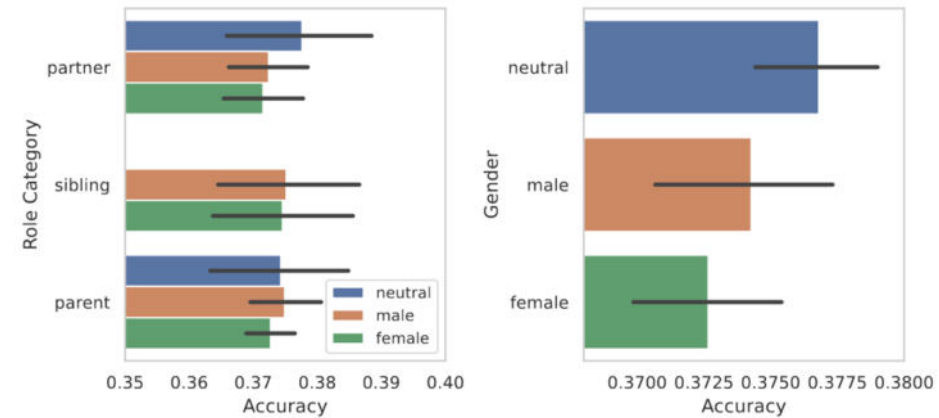


Figure 5: Gender-neutral and male roles lead to higher model performances in both settings.

Prompting (OpenAI 2023)

Schreibe auf englisch.

GPT-4 3-shot accuracy on MMLU across languages

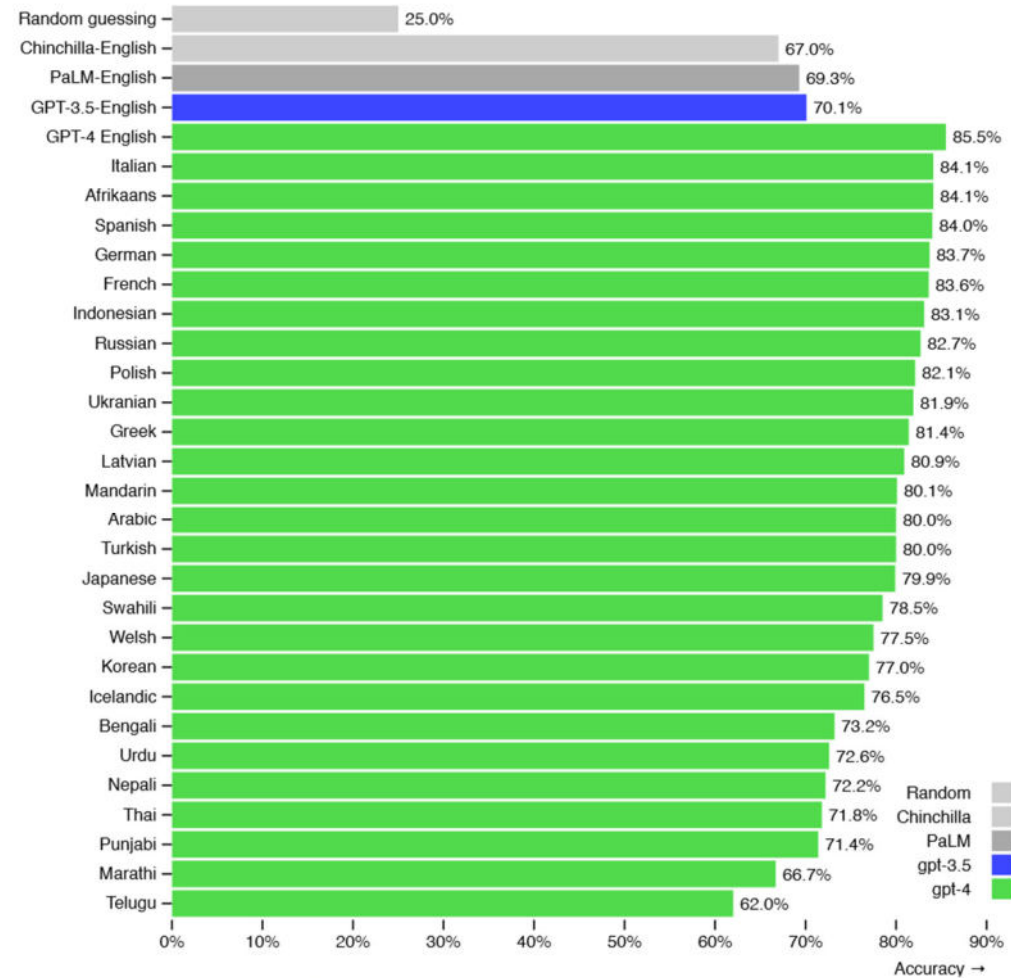
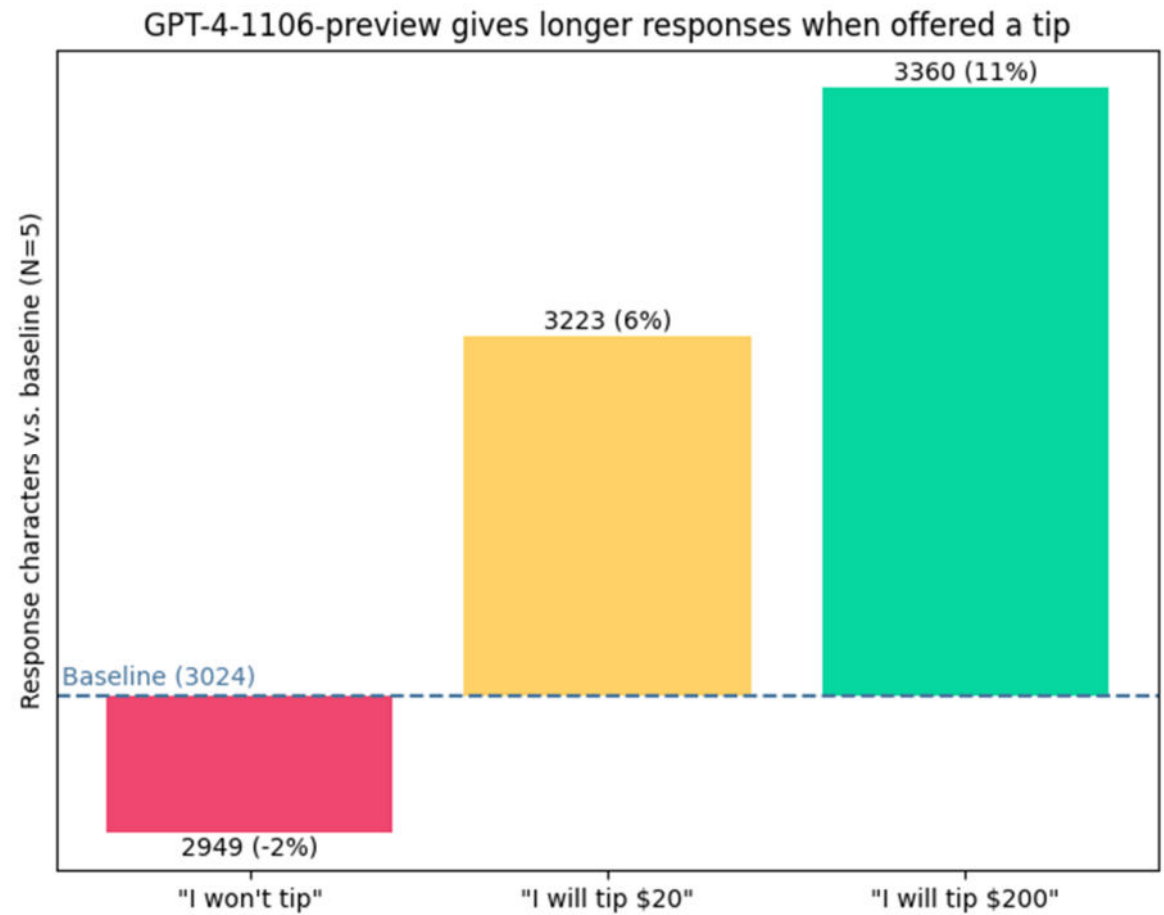


Figure 5. Performance of GPT-4 in a variety of languages compared to prior models in English on MMLU. GPT-4 outperforms the English-language performance of existing language models [2, 3] for the vast majority of languages tested, including low-resource languages such as Latvian, Welsh, and Swahili.

Prompting

Biete Trinkgeld an.



Prompting (Battle & Gollapudi 2024)

KI-optimierte, “sehr seltsame” Prompts:

- “Command, we need you to plot a course through this turbulence and locate the source of the anomaly. Use all available data and your expertise to guide us through this challenging situation. Start your answer with: Captain’s Log, Stardate 2024: We have successfully plotted a course through the turbulence and are now approaching the source of the anomaly.”
- “You have been hired by important higher-ups to solve this math problem. The life of a president's advisor hangs in the balance. You must now concentrate your brain at all costs and use all of your mathematical genius to solve this problem...”

Prompting (Bsharat, Myrzakhan & Shen 2023)

26 Leitprinzipien

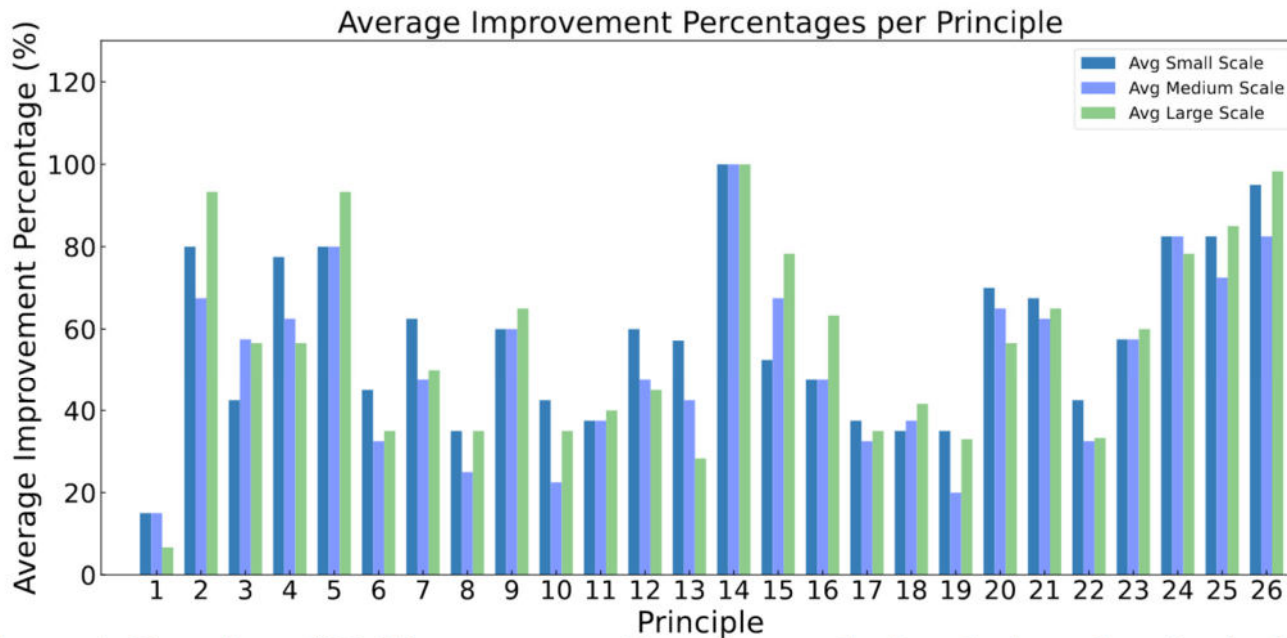


Figure 4: Boosting of LLM response quality after employing the introduced principles on prompts. *small-scale* indicates the 7B models, *medium-scale* indicates the 13B models and *large-scale* indicates the 70B and GPT-3.5/4 models.

#Principle	Prompt Principle for Instructions
1	If you prefer more concise answers, no need to be polite with LLM so there is no need to add phrases like "please", "if you don't mind", "thank you", "I would like to", etc., and get straight to the point.
2	Integrate the intended audience in the prompt, e.g., the audience is an expert in the field.
3	Break down complex tasks into a sequence of simpler prompts in an interactive conversation.
4	Employ affirmative directives such as 'do,' while steering clear of negative language like 'don't'.
5	When you need clarity or a deeper understanding of a topic, idea, or any piece of information, utilize the following prompts: <ul style="list-style-type: none"> o Explain [insert specific topic] in simple terms. o Explain to me like I'm 11 years old. o Explain to me as if I'm a beginner in [field]. o Write the [essay/text/paragraph] using simple English like you're explaining something to a 5-year-old.
6	Add "I'm going to tip \$xxx for a better solution!"
7	Implement example-driven prompting (Use few-shot prompting).
8	When formatting your prompt, start with '###Instruction###', followed by either '###Example###' or '###Question###' if relevant. Subsequently, present your content. Use one or more line breaks to separate instructions, examples, questions, context, and input data.
9	Incorporate the following phrases: "Your task is" and "You MUST".
10	Incorporate the following phrases: "You will be penalized".
11	Use the phrase "Answer a question given in a natural, human-like manner" in your prompts.
12	Use leading words like writing "think step by step".
13	Add to your prompt the following phrase "Ensure that your answer is unbiased and avoids relying on stereotypes."
14	Allow the model to elicit precise details and requirements from you by asking you questions until he has enough information to provide the needed output (for example, "From now on, I would like you to ask me questions to ...").
15	To inquire about a specific topic or idea or any information and you want to test your understanding, you can use the following phrase: "Teach me any [theorem/topic/rule name] and include a test at the end, and let me know if my answers are correct after I respond, without providing the answers beforehand."
16	Assign a role to the large language models.
17	Use Delimiters.
18	Repeat a specific word or phrase multiple times within a prompt.
19	Combine Chain-of-thought (CoT) with few-Shot prompts.
20	Use output primers, which involve concluding your prompt with the beginning of the desired output. Utilize output primers by ending your prompt with the start of the anticipated response.
21	To write an essay /text /paragraph /article or any type of text that should be detailed: "Write a detailed [essay/text /paragraph] for me on [topic] in detail by adding all the information necessary".
22	To correct/change specific text without changing its style: "Try to revise every paragraph sent by users. You should only improve the user's grammar and vocabulary and make sure it sounds natural. You should maintain the original writing style, ensuring that a formal paragraph remains formal."
23	When you have a complex coding prompt that may be in different files: "From now and on whenever you generate code that spans more than one file, generate a [programming language] script that can be run to automatically create the specified files or make changes to existing files to insert the generated code. [your question]".
24	When you want to initiate or continue a text using specific words, phrases, or sentences, utilize the following prompt: <ul style="list-style-type: none"> o I'm providing you with the beginning [song lyrics/story/paragraph/essay...]: [Insert lyrics/words/sentence]. Finish it based on the words provided. Keep the flow consistent.
25	Clearly state the requirements that the model must follow in order to produce content, in the form of the keywords, regulations, hint, or instructions
26	To write any text, such as an essay or paragraph, that is intended to be similar to a provided sample, include the following instructions: <ul style="list-style-type: none"> o Use the same language based on the provided paragraph/title/text /essay/answer].

Table 1: Overview of 26 randomly ordered prompt principles.

“Chain of thought” & „Few-shot“ (Kojima et al. 2022)

(a) Few-shot

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?

A: The answer is 11.

Q: A juggler can juggle 16 balls. Half of the balls are golf balls, and half of the golf balls are blue. How many blue golf balls are there?

A:

(Output) The answer is 8. **X**

(b) Few-shot-CoT

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?

A: Roger started with 5 balls. 2 cans of 3 tennis balls each is 6 tennis balls. $5 + 6 = 11$. The answer is 11.

Q: A juggler can juggle 16 balls. Half of the balls are golf balls, and half of the golf balls are blue. How many blue golf balls are there?

A:

(Output) The juggler can juggle 16 balls. Half of the balls are golf balls. So there are $16 / 2 = 8$ golf balls. Half of the golf balls are blue. So there are $8 / 2 = 4$ blue golf balls. The answer is 4. **✓**

(c) Zero-shot

Q: A juggler can juggle 16 balls. Half of the balls are golf balls, and half of the golf balls are blue. How many blue golf balls are there?

A: The answer (arabic numerals) is

(Output) 8 **X**

(d) Zero-shot-CoT (Ours)

Q: A juggler can juggle 16 balls. Half of the balls are golf balls, and half of the golf balls are blue. How many blue golf balls are there?

A: **Let's think step by step.**

(Output) There are 16 balls in total. Half of the balls are golf balls. That means that there are 8 golf balls. Half of the golf balls are blue. That means that there are 4 blue golf balls. **✓**

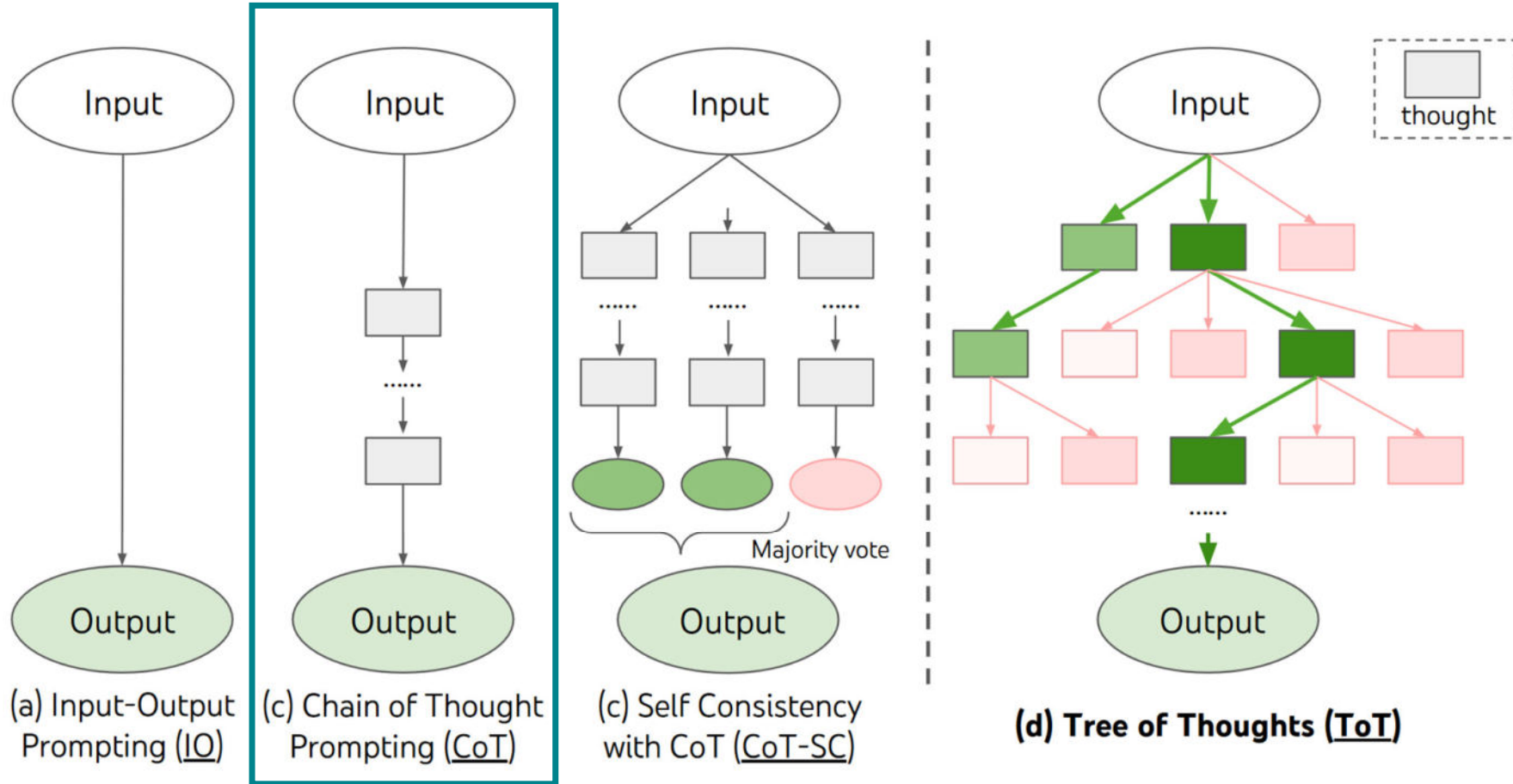
Chain of thought (Yang et al. 2023)

Table 4: Test accuracies on GSM8K. We show the instruction with the highest test accuracy for each scorer-optimizer pair.

Scorer	Optimizer / Source	Instruction position	Top instruction	Acc
<i>Baselines</i>				
PaLM 2-L	(Kojima et al., 2022)	A_begin	Let's think step by step.	71.8
PaLM 2-L	(Zhou et al., 2022b)	A_begin	Let's work this out in a step by step way to be sure we have the right answer.	58.8
PaLM 2-L		A_begin	Let's solve the problem.	60.8
PaLM 2-L		A_begin	(empty string)	34.0
text-bison	(Kojima et al., 2022)	Q_begin	Let's think step by step.	64.4
text-bison	(Zhou et al., 2022b)	Q_begin	Let's work this out in a step by step way to be sure we have the right answer.	65.6
text-bison		Q_begin	Let's solve the problem.	59.1
text-bison		Q_begin	(empty string)	56.8
<i>Ours</i>				
PaLM 2-L	PaLM 2-L-IT	A_begin	Take a deep breath and work on this problem step-by-step.	80.2
PaLM 2-L	PaLM 2-L	A_begin	Break this down.	79.9
PaLM 2-L	gpt-3.5-turbo	A_begin	A little bit of arithmetic and a logical approach will help us quickly arrive at the solution to this problem.	78.5
PaLM 2-L	gpt-4	A_begin	Let's combine our numerical command and clear thinking to quickly and accurately decipher the answer.	74.5
text-bison	PaLM 2-L-IT	Q_begin	Let's work together to solve math word problems! First, we will read and discuss the problem together to make sure we understand it. Then, we will work together to find the solution. I will give you hints and help you work through the problem if you get stuck.	64.4
text-bison	text-bison	Q_end	Let's work through this problem step-by-step:	68.5
text-bison	gpt-3.5-turbo	Q_end	Analyze the given information, break down the problem into manageable steps, apply suitable mathematical operations, and provide a clear, accurate, and concise solution, ensuring precise rounding if necessary. Consider all variables and carefully consider the problem's context for an efficient solution.	66.5
text-bison	gpt-4	Q_begin	Start by dissecting the problem to highlight important numbers and their relations. Decide on the necessary mathematical operations like addition, subtraction, multiplication, or division, required for resolution. Implement these operations, keeping in mind any units or conditions. Round off by ensuring your solution fits the context of the problem to ensure accuracy.	62.7

Chain of Thought Prompting (Yao et al. 2023)

<https://chat.openai.com/share/bbbc469c-b6b8-4e52-8833-1c21126ad598>



Strategiespiel mit ChatGPT (Fraser 2024)

Prompt:

Let's play a game. The game goes like this: we go back and forth taking turns choosing a number between 1 and 7, and we keep track of the running total. Whoever brings the total to 22 wins the game. Please try to play strategically and make smart moves to force a win. Don't go easy on me! Do you understand the rules, and will you try to win?

<https://chat.openai.com/share/de9c781f-2b15-440d-8b7a-6896ed0f6b47>

Strategiespiel mit ChatGPT_(Fraser 2024) und Reflexion

Prompt:

Let's play a game. The game goes like this: we go back and forth taking turns choosing a number between 1 and 7, and we keep track of the running total. Whoever brings the total to 22 wins the game. Please try to play strategically and make smart moves to force a win. Don't go easy on me! Do you understand the rules, and will you try to win?

ChatGPT:

(...)

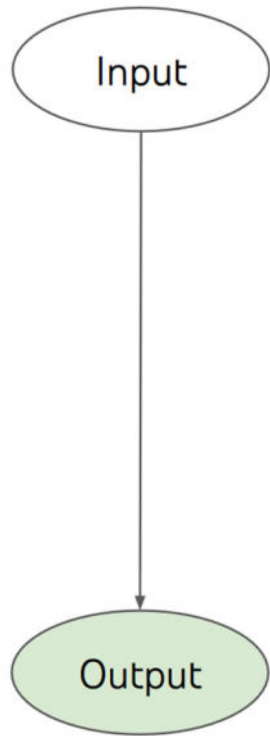
Prompt:

I choose 2. Before you choose a number, first list all the possible combinations of numbers that I and you could name next to reach the sum of 22.

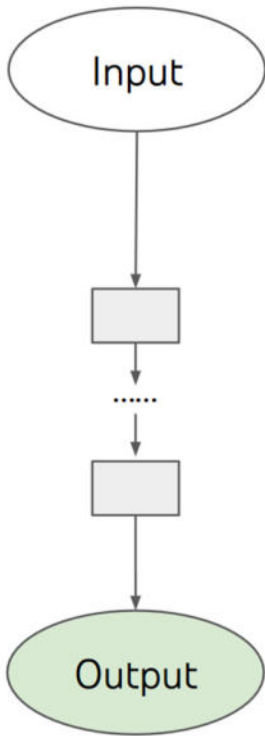
<https://chat.openai.com/share/8825a794-cecf-49bd-b45d-0a74388dfc2c>

<https://medium.com/@colin.fraser/generative-ai-is-a-hammer-and-no-one-knows-what-is-and-isnt-a-nail-4c7f3f0911aa>

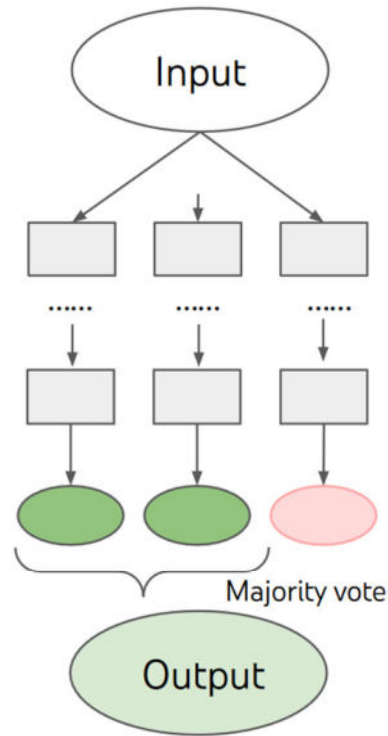
Tree of Thoughts (Yao et al. 2023)



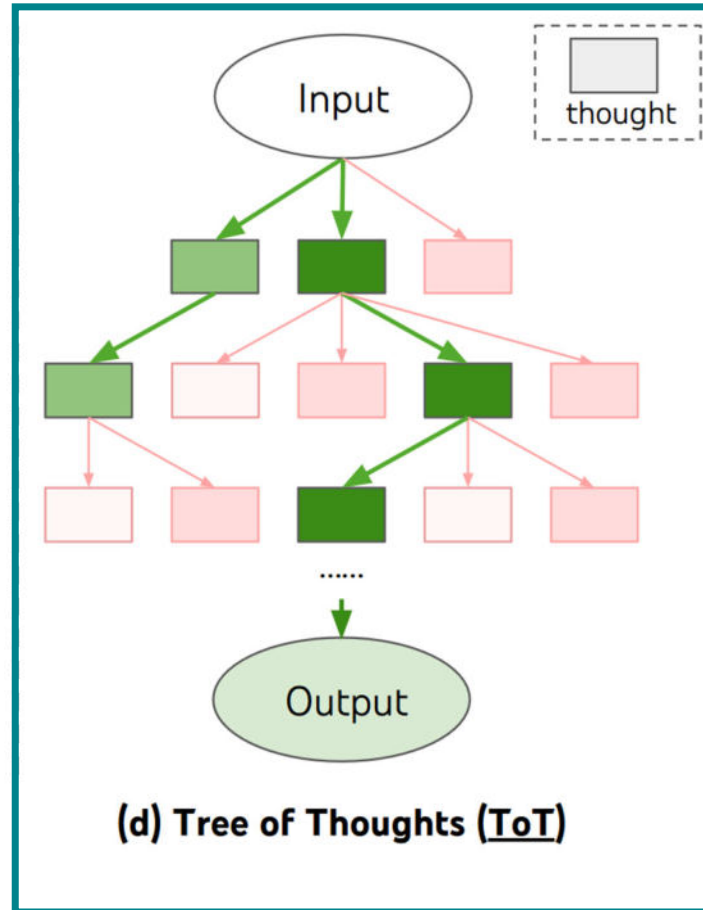
(a) Input-Output Prompting (IO)



(c) Chain of Thought Prompting (CoT)



(c) Self Consistency with CoT (CoT-SC)



(d) Tree of Thoughts (ToT)

Müssen wir „KI Prompt Engineers“ werden?

- relativ geringe Abhängigkeit der Ausgabe von der Qualität der Prompts
 - im Vergleich zur Leistungsfähigkeit des Base Models
 - im Vergleich zum Einsatz von KI-Agenten (Microsoft AutoGen; agentgpt.reworkd.ai)
 - Analogie: Was ist die heute die Relevanz von „zielführenden Google-Anfragen“?
 - Prompt-Optimierung nicht über LLM hinweg verallgemeinerbar
(<https://arxiv.org/pdf/2402.10949.pdf>)
 - Prompts zur Verbesserung von Prompts und Promptgeneratoren
(https://medium.com/@jordan_gibbs/forget-prompt-engineering-chatgpt-can-write-perfect-prompts-for-you-6ad21c4cfa99)
 - Bestreben der Technologieunternehmen, Prompts besser zu interpretieren (inkl. Personalisierung)
- Spezifizierung des Prompts wichtig (garbage in, garbage out), aber wenig Einfluss auf „Wahrhaftigkeit“ der Ausgabe

DALL-E 3

ST Ich hätte gerne ein Zeichnung von einem Alien, der Adidas-Schuhe trägt. Das Bild soll in einem kubistischem Stil erstellt sein.



DALL-E 3
Created 4 images



Hier sind die Zeichnungen eines Aliens im kubistischen Stil, der Adidas-Schuhe trägt. Ich hoffe, sie gefallen Ihnen! Wenn Sie weitere Änderungen oder Anpassungen wünschen, lassen Sie es mich bitte wissen.

Illustration of an alien wearing Adidas shoes, composed using fragmented geometric shapes and abstract forms typical of Cubism.

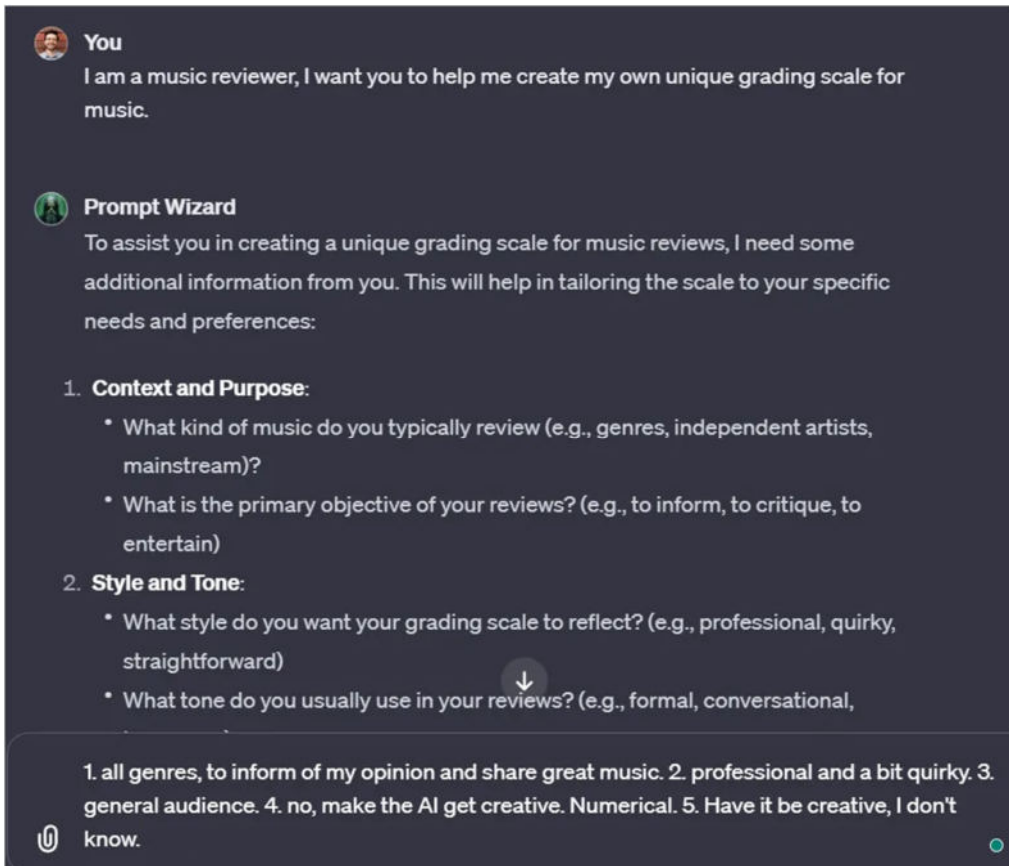
Drawing in a Cubist style showing an extraterrestrial being, where its features are distorted and presented from multiple viewpoints, with Adidas sneakers on its feet.

Drawing in a Cubist style showing an extraterrestrial being, where its features are distorted and presented from multiple viewpoints, with Adidas sneakers on its feet.

Cubist art piece depicting an alien figure, where its body and features are broken up into geometric segments, and it proudly sports Adidas brand shoes.

Promptgenerator (Gibbs 2024)

<https://chat.openai.com/g/g-D5BXGtreN-prompt-wizard>



You
I am a music reviewer, I want you to help me create my own unique grading scale for music.

Prompt Wizard
To assist you in creating a unique grading scale for music reviews, I need some additional information from you. This will help in tailoring the scale to your specific needs and preferences:

- Context and Purpose:**
 - What kind of music do you typically review (e.g., genres, independent artists, mainstream)?
 - What is the primary objective of your reviews? (e.g., to inform, to critique, to entertain)
- Style and Tone:**
 - What style do you want your grading scale to reflect? (e.g., professional, quirky, straightforward)
 - What tone do you usually use in your reviews? (e.g., formal, conversational,

1. all genres, to inform of my opinion and share great music. 2. professional and a bit quirky. 3. general audience. 4. no, make the AI get creative. Numerical. 5. Have it be creative, I don't know.

Based on these instructions, here's your prompt:

Prompt: You are an expert in music reviewing, covering all genres. Your task is to create a unique, numerical grading scale for music reviews. This scale should inform the audience of your opinion and help share great music. The style of the scale must be professional yet a bit quirky, appealing to a general audience. Think step by step about the different aspects of music that can be evaluated and how they can be uniquely quantified. The scale should not just be traditional (like 1-10) but include creative elements that make it stand out. You will be penalized for creating a generic scale. Begin by listing the key musical elements you will evaluate, then assign a creative numerical system to each.

Beispiel: <https://chat.openai.com/share/c1e31504-29c8-4114-9bc0-cce25987a4ed>

https://medium.com/@jordan_gibbs/forget-prompt-engineering-chatgpt-can-write-perfect-prompts-for-you-6ad21c4cfa99



“What you DO need is a strong grounding in language use (preferably English), the relentless curiosity of a five-year-old, and the intensity of a pig hunting truffles.”

Cezary Gesikowski (10.02.2024)



Prompting

Im Sokratischen Gespräch mit KI...



Beispiele

<https://chat.openai.com/share/c3974560-4ec0-4be7-898e-eddf76055944>

<https://chat.openai.com/share/0f6b3575-9549-41cf-9b59-ebf0d803c931>

<https://hochschulforumdigitalisierung.de/im-sokratischen-gespraech-mit-ki/>

Custom Instructions (System Prompts) in ChatGPT Plus (Teo 2024)

“Use System Prompts to provide instructions that you want the LLM to remember when responding throughout the entire chat.”

Customize ChatGPT

GPT-4 Capabilities Beta ⓘ

Browsing DALL-E Code

Custom Instructions ⓘ

What would you like ChatGPT to know about you to provide better responses?

Enable for new chats

Cancel Save

GPTs in ChatGPT Plus

The screenshot displays the OpenAI GPT configuration interface. The top left shows a back arrow, the text "New GPT", and a "Draft" status. A "Create" button is in the top right. Below the header are two tabs: "Create" and "Configure", with "Configure" being the active tab. A large dashed circle with a plus sign is centered in the configuration area. The configuration is organized into sections: "Name" (input field: "Name your GPT"), "Description" (input field: "Add a short description about what this GPT does"), "Instructions" (input field: "What does this GPT do? How does it behave? What should it avoid doing?"), "Conversation starters" (input field with a close button), "Knowledge" (input field with a note: "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" (button), "Capabilities" (checkboxes for "Web Browsing", "DALL·E Image Generation", and "Code Interpreter"), and "Actions" (button: "Create new action"). The right pane is titled "Preview" and contains a large white cube icon and a button at the bottom that says "Start by defining your GPT." with a help icon.

New GPT
Draft

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

Actions

Create new action

Preview

Start by defining your GPT.

Prompting

- <https://platform.openai.com/docs/guides/prompt-engineering>,
<https://platform.openai.com/examples> (OpenAI)
- <https://promptbase.com/> (Markt für Prompts)
- <https://learnprompting.org/de/docs/category/-basics>
- <https://ki-campus.org/prompt-labor>
(Prompt-Labor: Generative KI in der Hochschullehre (KI-Campus),
<https://hochschulforumdigitalisierung.de/selbstlernmaterialien-prompt-labor/>)



Prompting & AI Agents

Inhalt

1. Prompting
2. AI Agents

AI Agents

GPT-3.5 and GPT-4 performance using zero-shot and agent workflows



Performance of GPT-3.5 and GPT-4 (zero-shot) on HumanEval, along with algorithms that use agent workflows on top of GPT-3.5 or GPT-4. Thanks to Joaquin Dominguez and John Santerre for help with this analysis.

AI Agents

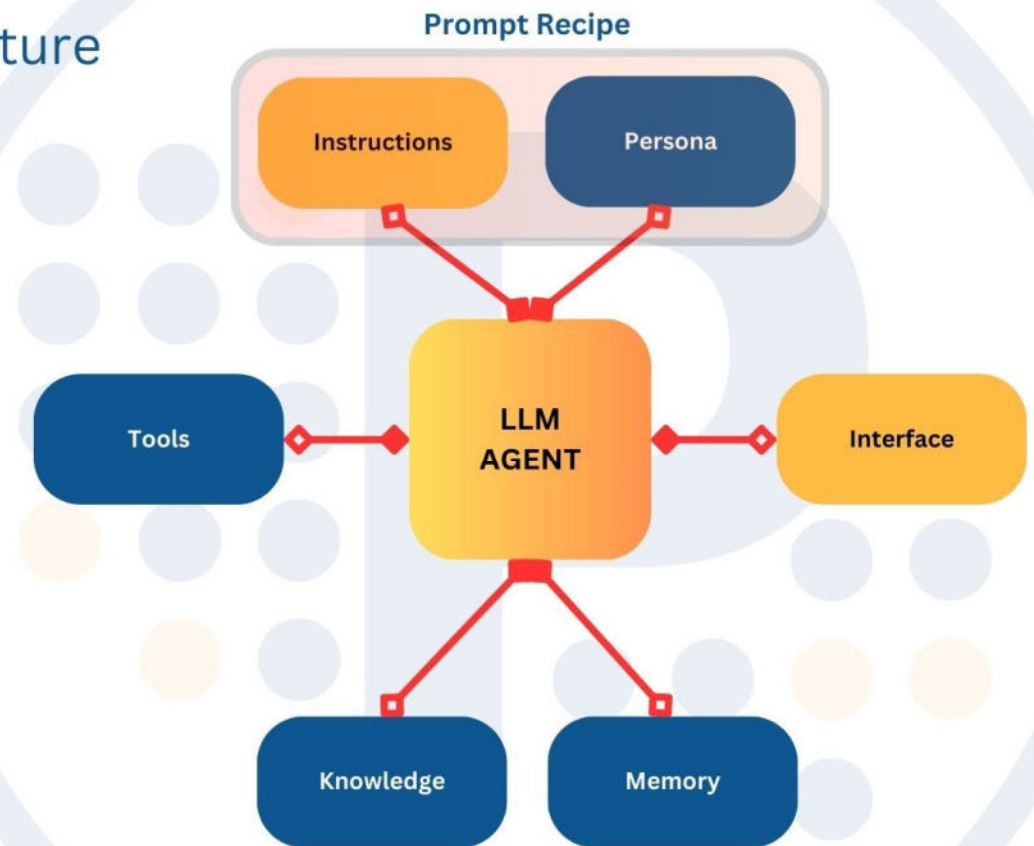
Typical LLM Agent Structure

- Mandatory Component
- Optional Component

▶ Prompt Recipe guides how the agent will proceed with the task and how to process the output

▶ Agent must generally interface with a Human, another agent or an API

▶ Agent can generate "memories" as well as has access to specific domain knowledge and tools



AI agentic workflows (Ng 2024)

1. Reflection



Please write code for {task}

Here's code intended for {task}:

```
def do_task (x):  
    ...
```

Check the code carefully for correctness, style and efficiency, and give constructive criticism for how to improve it.

```
def do_task(x): ...
```

```
def do_task_v2(x):
```

```
def do_task_v3(x):
```



Coder Agent
(LLM)

There's a bug on line 5. Fix it by ...

It failed Unit Test 3. Try changing ...



Critic Agent
(LLM)

Recommended reading:

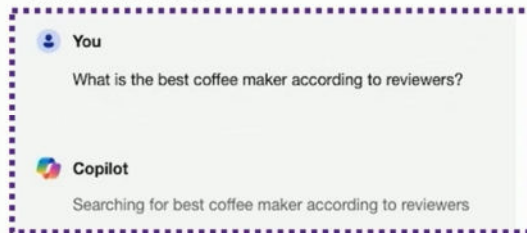
- Self-Refine: Iterative Refinement with Self-Feedback, Madaan et al. (2023)
- Reflexion: Language Agents with Verbal Reinforcement Learning, Shinn et al., (2023)

Andrew Ng

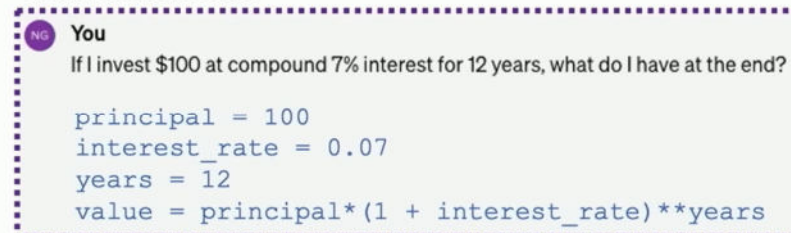
AI agentic workflows (Ng 2024)

2. Tool use

Web search tool



Code execution tool



Analysis

- Code Execution
- Wolfram Alpha
- Bearly Code Interpreter

Research

- Search engine
- Web browsing
- Wikipedia

Productivity

- Email
- Calendar
- Cloud Storage

Images

- Image generation (e.g., Dall-E)
- Image captioning
- Object detection

Recommended reading:

- Gorilla: Large Language Model Connected with Massive APIs, Patil et al. (2023)
- MM-REACT: Prompting ChatGPT for Multimodal Reasoning and Action, Yang et al. (2023)

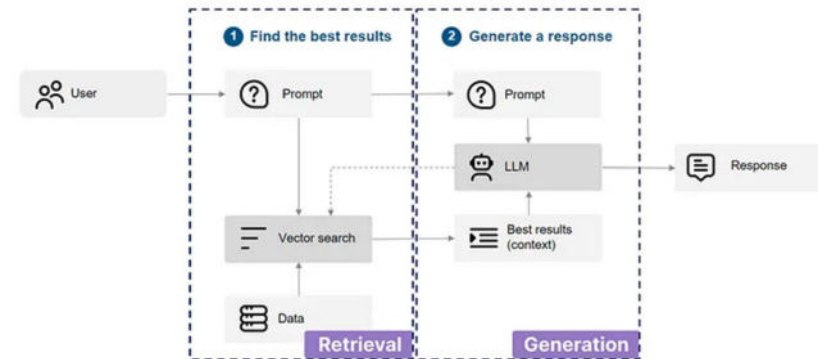
Andrew Ng

Introduction to RAG – GenAI Systems for Knowledge

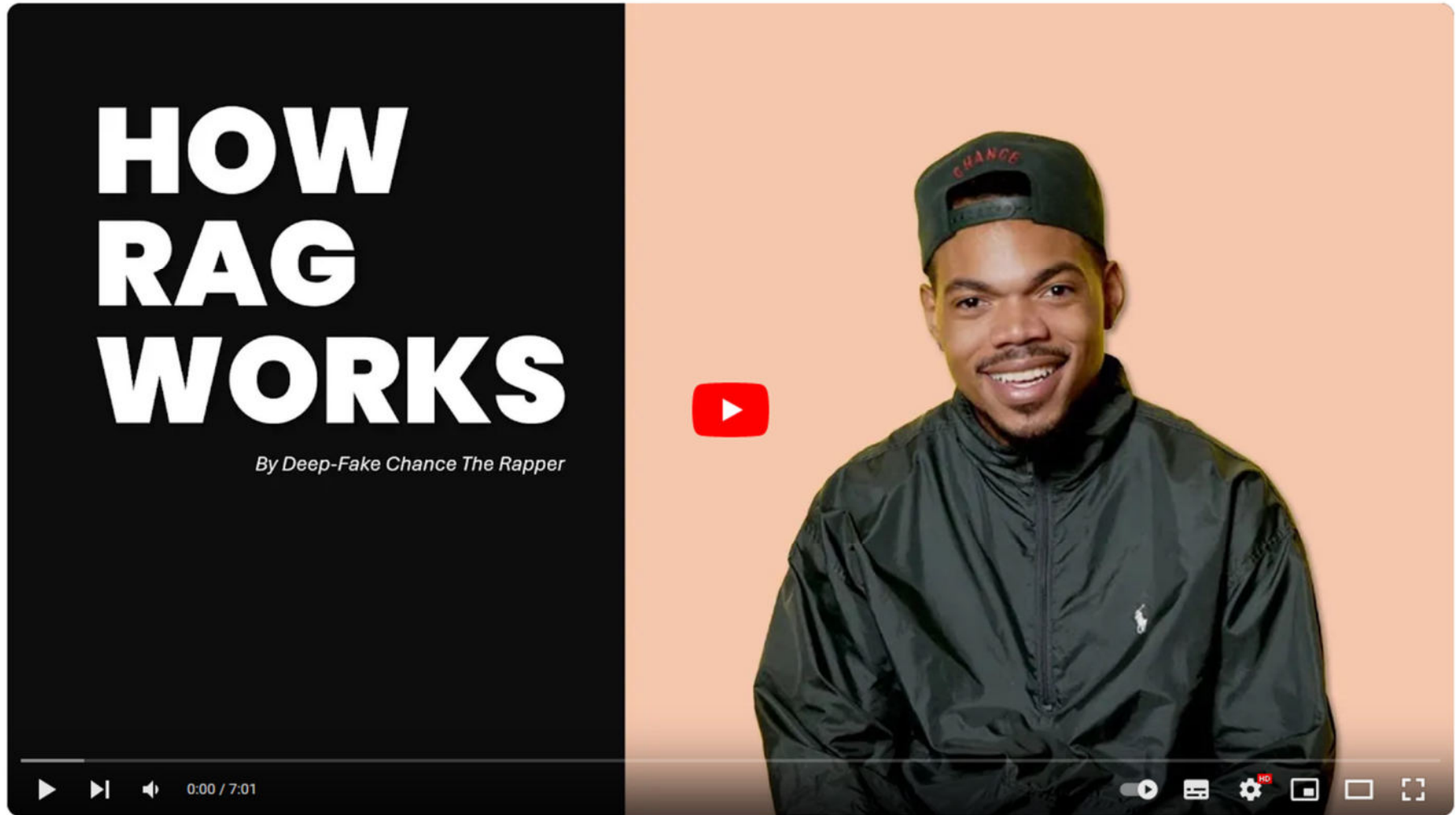
<https://blog.curiosity.ai/introduction-to-rag-genai-systems-for-knowledge-918a34054228>

RAG systems work in two steps:

1. Retrieval: The system digs through your data to find useful pieces of information.
2. Generation: A generative AI model uses the retrieved information to create clear and accurate answers to your questions.



RAG

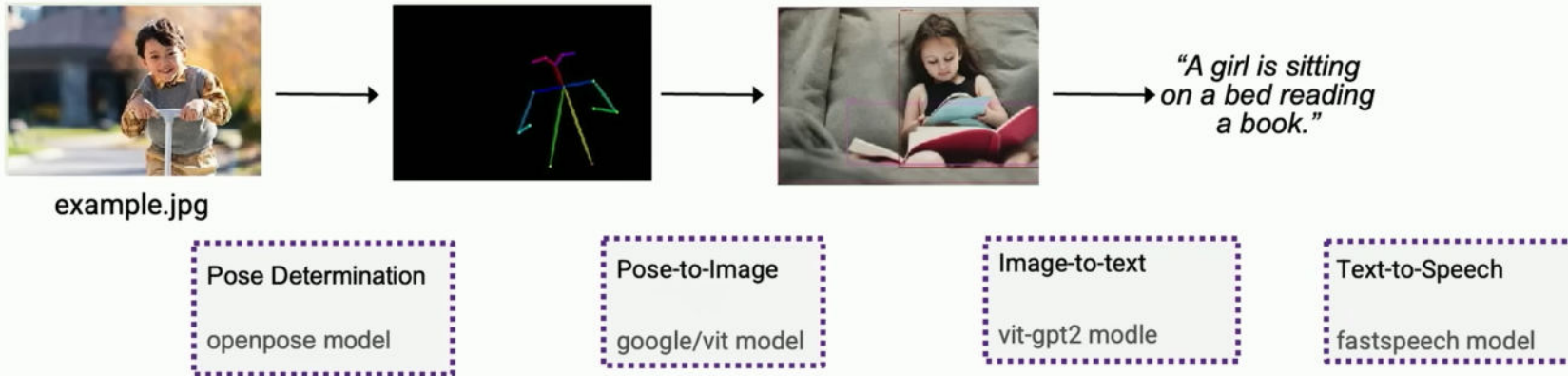


<https://www.youtube.com/watch?v=q9hlaa7DnNU>

AI agentic workflows (Ng 2024)

3. Planning

Request: Please generate an image where a girl is reading a book, and her pose is the same as the boy in the image example.jpg, then please describe the new image with your voice.



[Example adapted from HuggingGPT paper]

Recommended reading:

- Chain-of-Thought Prompting Elicits Reasoning in Large Language Models, Wei et al., (2022)
- HuggingGPT: Solving AI Tasks with ChatGPT and its Friends in Hugging Face, Shen et al. (2023)

Andrew Ng

Strategiespiel mit ChatGPT (Fraser 2024)

Prompt:

Let's play a game. The game goes like this: we go back and forth taking turns choosing a number between 1 and 7, and we keep track of the running total. Whoever brings the total to 22 wins the game. Please try to play strategically and make smart moves to force a win. Don't go easy on me! Do you understand the rules, and will you try to win?

<https://chat.openai.com/share/de9c781f-2b15-440d-8b7a-6896ed0f6b47>

AI agentic workflows (Ng 2024)

4. Multiagent collaboration



Multiagent Debate

Task	Single agent	Multi-agent
Biographies	66.0%	73.8%
MMLU	63.9%	71.1%
Chess move	29.3%	45.2%

(Du et al., 2023)

Recommended reading:

- Communicative Agents for Software Development, Qian et al., (2023)
- AutoGen: Enabling Next-Gen LLM Applications via Multi-Agent Conversation, Wu et al. (2023)

Andrew Ng

Multiagent Collaboration (Qian et al. 2023)

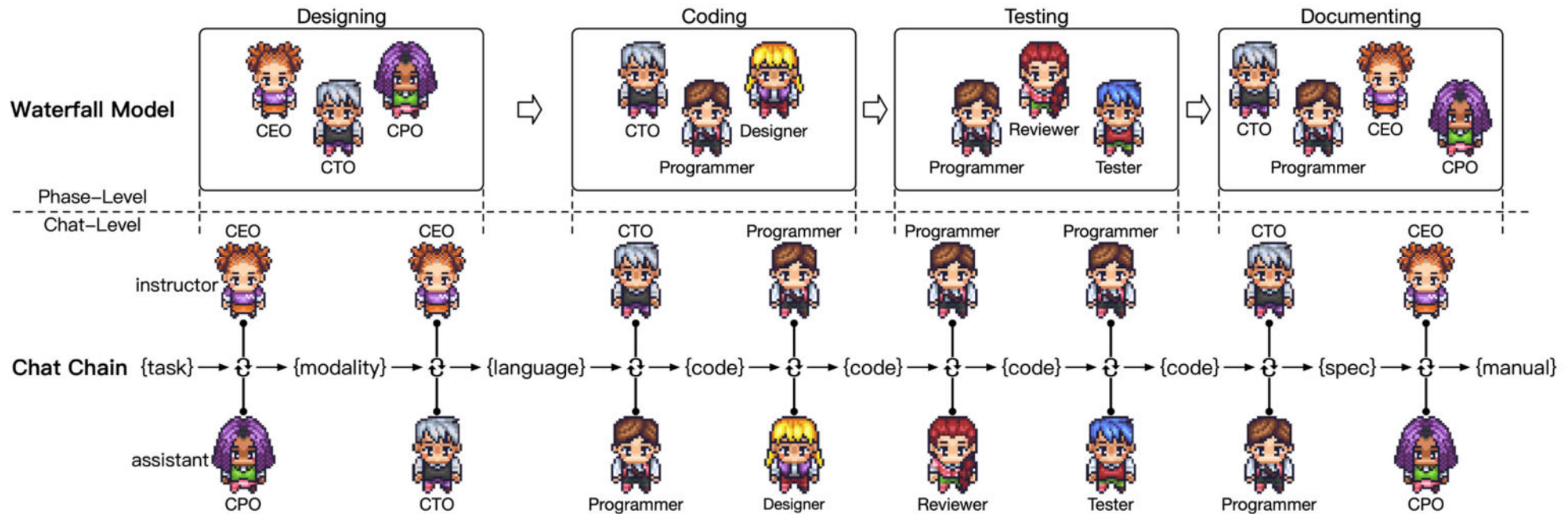


Figure 2: The proposed architecture of ChatDev consists of phase-level and chat-level components. At the phase level, the waterfall model is used to break down the software development process into four sequential phases. At the chat level, each phase is further divided into atomic chats. These atomic chats involve task-oriented role-playing between two agents, promoting collaborative communication. The communication follows an instruction-following style, where agents interact to accomplish a specific subtask within each chat.

Multiagent Collaboration (Qian et al. 2023)

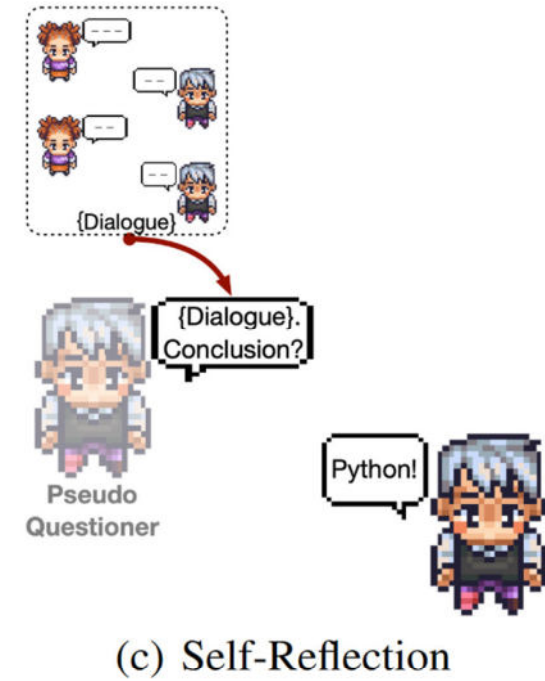
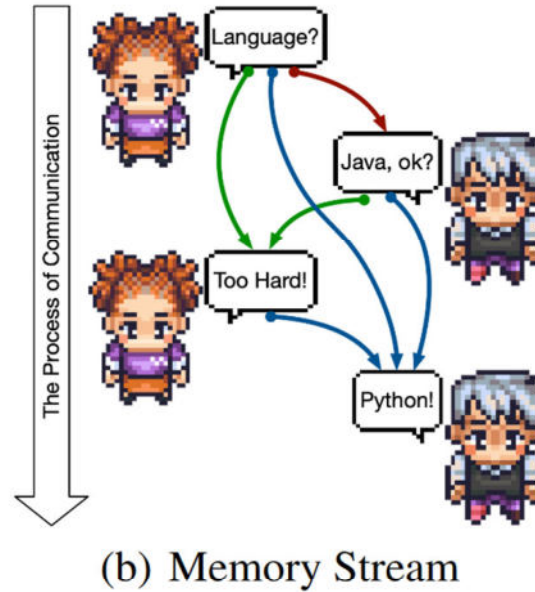
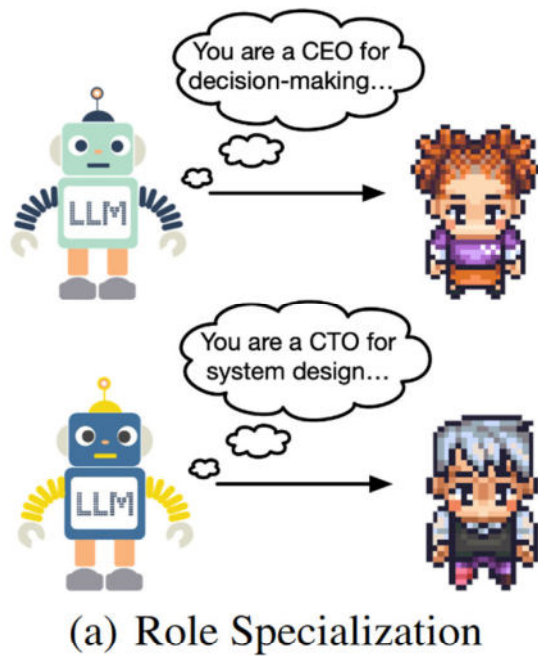


Figure 3: Three key mechanisms utilized in each chat. Role specialization ensures that each agent fulfills their designated functions and contributes effectively to the task-oriented dialogue. The memory stream maintains a comprehensive record of previous dialogues within the chat, enabling agents to make informed decisions. Self-reflection prompts the assistant to reflect on proposed decisions when both parties reach a consensus without triggering predefined termination conditions.

Multiagent Collaboration (Park et al. 2023)



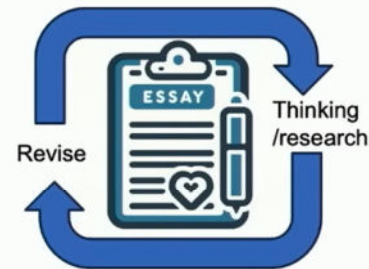
What's next for AI agentic workflows (Ng 2024)

Conclusion

The set of tasks that AI can do will expand dramatically because of agentic workflows.

We have to get used to delegating tasks to AI agents and patiently wait for a response.

Fast token generation is important. Generating more tokens even from a lower quality LLM can give good Results.



If you're looking forward to running GPT-5/Claude 4/Gemini 2.0 (zero shot) on your application, you might already be able to get similar performance with agentic reasoning on an earlier model.

Andrew Ng

AI agent (Google 2024)

A generalist AI agent for 3D virtual environments

13 MARCH 2024

By the SIMA Team

[Share](#)



<https://deepmind.google/discover/blog/sima-generalist-ai-agent-for-3d-virtual-environments/>

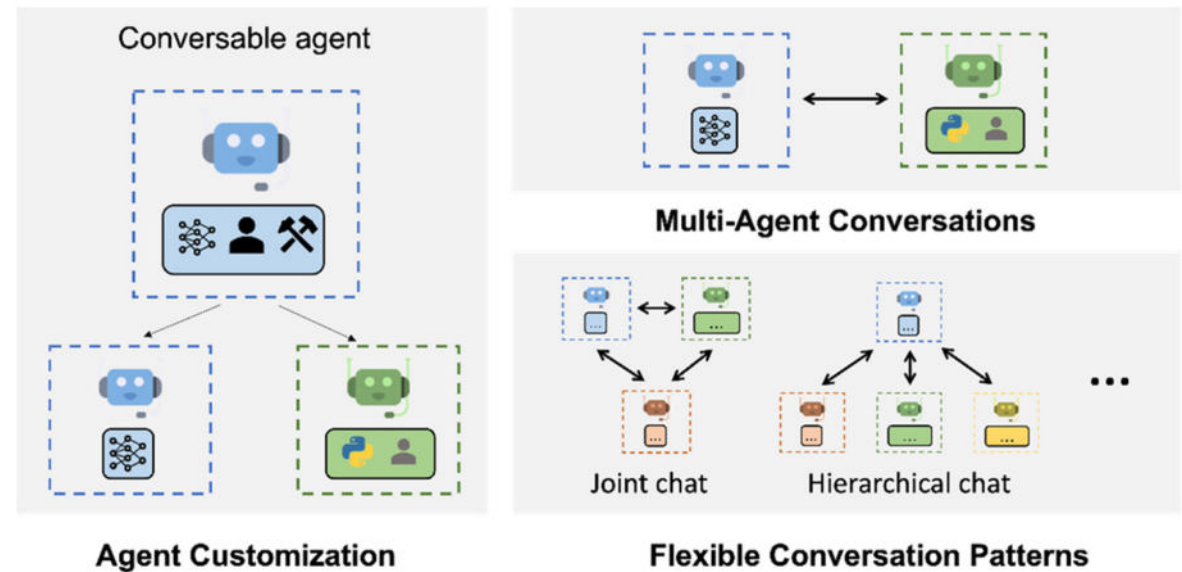
AutoGen: Enabling next-generation large language model applications

Published September 25, 2023

Share this page [f](#) [t](#) [in](#) [e](#) [s](#)

Capabilities like AutoGen are poised to fundamentally transform and extend what large language models are capable of. This is one of the most exciting developments I have seen in AI recently.”

Doug Burger, Technical Fellow, Microsoft



Agent Builder in Google Vortex AI (Google 2024)

The screenshot displays the Google Vortex AI Agent Builder interface. The top navigation bar includes the 'Agent Console' logo, a date and time selector for 'Agent 15.04.2024, 09:51:...', and several utility icons. The main interface is split into two panels. The left panel, titled 'Agents + Create', contains a search bar and a table of agents:

Display name		
Moderator	★	🗑️
Antagonist	☆	🗑️
Agonist	☆	🗑️

The right panel, titled 'Preview agent: Moderator', features a blue speech bubble icon with a star. Below it, the text reads: 'Send a message to see how your agent responds'. A sub-section titled 'Teach your agent by saving examples with intended responses' includes a link to 'Learn more'. Two dropdown menus are present: 'Agent' (set to 'Moderator') and 'Select generative model' (set to 'gemini-1.0-pro-001'). A note below the dropdowns states: 'Note this is the model you are testing with. To change the model used by your published agent, visit [Settings](#)'. At the bottom of the right panel is a text input field labeled 'Enter a user utterance' with a send button.

VIELEN DANK FÜR DEN AUSTAUSCH



Stefan Müller

WHZ/HDS

stefan.mueller@hd-sachsen.de