

ChatGPT, Large Language Modelle und Prompt Engineering:

Eine Einführung und ein Leitfaden für die Verwendung in Unternehmen.

Mia Bangerl, MA

Alina Kopkow, MSc

Assoc.Prof. Dipl.-Ing. Dr.techn.

Viktoria Pammer-Schindler

Dieses Dokument wurde von den Autorinnen im Rahmen des FFG-geförderten Digital Innovations Hubs (DIH) Süd, abgewickelt von der DIH Süd GmbH, an der Technischen Universität Graz in Zusammenarbeit mit der Know-Center GmbH erstellt.

Die Inhalte geben eine Einführung in den Umgang mit Large Language Modellen (LLM) und LLM-basierten Systemen, mit einem Fokus auf textbasierte LLM-Chatbots wie ChatGPT, Copilot & Co. Die enthaltenen Inhalte wurden im Februar und März 2025 verfasst und beziehen sich daher auf Technologien und Forschungsergebnisse bis zu diesem Zeitpunkt.

Autorinnen:

Mia Magdalena Bangerl, Alina Kopkow, Viktoria Pammer Schindler

Coverbild: Bild generiert mit Canva Magic Media und Stable Diffusion

Veröffentlichung: 31. März 2025

www.dih-sued.at

DOI [10.3217/5e1ek-qft39](https://doi.org/10.3217/5e1ek-qft39)



Das Land
Steiermark

LAND  KÄRNTEN

Inhaltsverzeichnis

1. Einleitung	5
2. Was sind Large Language Modelle (LLMs)?	5
3. Wie können LLMs verwendet werden?	7
4. Prompt Engineering	8
4.1. Elemente eines Prompts	8
4.2. Der Unterschied zwischen Nutzer:innen-Prompts und System-Prompts . . .	10
5. Prompt-Strategien	11
5.1. In-context Learning	11
5.2. Strategien für logische Schlussfolgerungen	12
5.2.1. Chain-of-Thought Prompts	13
5.2.2. Selbstkonsistenz	13
5.2.3. Tree-of-Thought	13
5.3. Gerichteter Stimulus	14
5.4. Prompt-Muster	14
5.4.1. Muster zur Reflektion und Überprüfbarkeit der Antwort	14
5.4.2. Muster zur KI-geleiteten Prompt-Verbesserung	15
5.4.3. Muster zur Prompt-Generierung für Bilder	16
5.4.4. Muster zur Übernahme einer Rolle und der Simulation von Szenarien	17
5.4.5. Muster zur Ideengenerierung	17
5.4.6. Muster zur Anleitungserstellung	18
5.4.7. Muster zur Automatisierung der Ausgabe und Vorlagen	18
6. Was ist bei der Anwendung von LLMs zu beachten?	19
6.1. Beschaffung, Präsentation und Repräsentation von Informationen	19
6.1.1. Verzerrungen und Stereotypen	20
6.1.2. Fehler, Falschinformationen und Halluzinationen	21
6.1.3. Zustimmunges Verhalten - „Kriecherei“	22
6.2. Unmittelbare und langfristige Risiken von LLM-Nutzung	23
6.2.1. Risiken kognitiver Verzerrungen und Fehlbilder zu LLMs und KI . .	23
6.2.2. Risiken der Homogenisierung von Inhalten	25

6.2.3.	Risiken von KI-Automatisierung und Jobverlust	25
6.2.4.	Risiken der Beeinträchtigung menschlicher Fähigkeiten	26
6.3.	Empfehlungen für die sichere und transparente Nutzung von LLMs	27
7.	Überblick über LLM-unterstützte Anwendungen	29
8.	Überblick über Modell-Familien	31
A.	Anhang	34
B.	Anwendungsbeispiele	34
B.1.	Vorbereitung eines Meetings	34
B.2.	E-Mail generieren	35
B.3.	Datenaufbereitung und -visualisierung	36
B.4.	Werbebeiträge und Social Media Post erstellen	37
B.5.	Zielgruppenanalyse	39
B.6.	Zusammenfassen und Verstehen von Texten	40
B.7.	Ideengenerierung und Planung eines Events	42
B.8.	Simulieren eines Mitarbeitendengesprächs	43
C.	Prompt-Sammlungen	44
D.	Weitere Ressourcen	44

1. Einleitung

Seit der Veröffentlichung von ChatGPT im Jahr 2022 wird regelmäßig darüber gesprochen, ob, wie und für welche Zwecke Chatbots wie ChatGPT, Copilot, Gemini & Co verwendet werden können und sollen. Aber wie funktionieren solche Chatbots eigentlich, wie schreibt man am besten Anweisungen für ChatGPT & Co, und wie können diese Technologien sinnvoll in Unternehmen eingesetzt werden?

In diesem Leitfaden finden Sie zuerst eine Erklärung über die Art und Funktionsweise von Large Language Modellen (LLMs, die Technologie hinter ChatGPT & Co) in Abschnitt 2 und eine kurze Einführung, wie und wofür diese verwendet werden können in Abschnitt 3. In Abschnitt 4 können Sie sich über die Grundlagen von Prompt Engineering, also das Verfassen von Anweisungen für LLM-Chatbots informieren. In Abschnitt 5 finden Sie auch konkrete Strategien und Muster für das Verfassen von Prompts. Anschließend erhalten Sie in Abschnitt 6 Informationen über die Anwendung von LLM-basierten Systemen im Betrieb und die damit verbundenen Risiken, sowie Empfehlungen für eine gute und informierte praktische Anwendung (Abschnitt 6.3). Schließlich finden Sie am Ende des Dokumentes eine Liste verschiedener LLM-basierter Systeme und deren Funktionen (Abschnitt 7) und einen Überblick über die gängigsten LLM-Modellfamilien (Abschnitt 8).

Zusätzlich enthält das Dokument im Anhang (Abschnitt A) eine Reihe praktischer Beispiele für das Arbeiten mit LLM-Chatbots wie ChatGPT & Co, anhand welcher Sie einen Einblick in die Anwendungsmöglichkeiten derartiger Technologien bekommen können, und ihre praktischen Kompetenzen im Umgang mit LLM-Chatbots schärfen können. Außerdem finden Sie im Anhang Verweise auf öffentliche Prompt-Sammlungen (Abschnitt C) und eine Reihe weiterer interessanter Ressourcen für das Arbeiten mit LLMs und LLM-basierten Systemen (Abschnitt D).

Die Zielgruppe dieser Einführung und dieses Leitfadens sind kleine und mittlere Unternehmen (KMUs) in Österreich. Gleichzeitig wurde hier zum Ziel gesetzt, eine grundlegende, aber einfach verständliche Einführung zu geben, so dass dieses Dokument auch einer wesentlich breiteren Zielgruppe einen verständlichen Einblick gewähren kann.

2. Was sind Large Language Modelle (LLMs)?

Large Language Modelle (LLMs) sind große Sprachmodelle, deren Hauptfähigkeit es ist, überzeugend menschliche klingende Sprache (z.B. Texte, Audio) zu erzeugen. LLMs gehören zur Familie der „generativen KI“, also einer Familie von KI, die Inhalte selbst erzeugen kann. Diese Fähigkeit grenzt generative KI von anderen KI-Systemen, wie etwa Suchmaschinen oder Spamfiltern ab, die vorrangig Daten analysieren und darauf basierend

Entscheidungen treffen können. Chatbots wie ChatGPT, Copilot oder Gemini werden durch LLMs gestützt und ermöglicht. Kommuniziert man also als Nutzer:in mit einem derartigen Chatbot, so wird die Antwort, die man vom Chatbot erhält, jeweils neu durch das im Hintergrund laufende LLM generiert.

LLMs werden mit sehr vielen textbasierten Daten trainiert. Hauptsächlich handelt es sich bei diesen Daten um gesammelte Webseiten, aber es können auch online frei verfügbare Bücher sowie Texte von Social Media oder Wikipedia sein. Das Ziel von LLMs ist es, durch das Lernen mit diesen Daten zu verstehen, welche Wörter statistisch häufig zusammen verwendet werden. Dadurch können LLMs Texte verstehen und generieren und so auch Fragen beantworten, Informationen aus Texten extrahieren und Anweisungen folgen. Um dies (gut) zu bewerkstelligen, wird das Modell, welches bereits mit vielen Daten trainiert wurde, zusätzlich für die spezifische Aufgabe, welche es erledigen soll (z.B. Texte übersetzen), angepasst (fine-tuned). Damit das Modell etwa keine ethisch verwerflichen Antworten gibt, bekommt es darüber hinaus noch Feedback von Menschen hinsichtlich des gewünschten Verhaltens (Reinforcement learning). Wenn diese Schritte getan wurden, steht am Ende ein Large Language Modell, welches für die jeweilige Aufgabe verwendet werden kann.

Um den eingegebenen Text zu verstehen, liest das Modell ihn nicht auf Satz-, Wort- oder Buchstabenebene, sondern betrachtet einzelne sprachliche Einheiten, sogenannte Tokens¹. Ein Token kann entweder ein ganzes Wort sein oder nur ein Teil eines Wortes. Es geht dabei darum, dass Buchstaben, welche häufig zusammen vorkommen, gruppiert werden. Zwischen diesen Tokens berechnet das LLM, wie wahrscheinlich es ist, dass diese nacheinander vorkommen. Zusätzlich bezieht das Modell auch den Kontext eines Token mit ein, z.B. den Inhalt eines Satzes oder Textes. Dabei durchlaufen die Tokens mehrere Ebenen (Transformer) in dem Modell und auf jeder Ebene wird weitere Information zu einem Token hinzugefügt. Zum Beispiel umfasst das ursprüngliche LLM hinter ChatGPT, das sogenannte ChatGPT-3 Modell, 96 Transformer, welche die Tokens durchlaufen, damit am Ende alle relevante Informationen enthalten sind, welche das Modell benötigt, um Inhalt und Kontext eines Textes zu verstehen. Auf dieser Grundlage wird anschließend das nächste Token gewählt, welches im Kontext am wahrscheinlichsten folgt. Dieses Token wird dann wieder in ein Wort oder eine Silbe übersetzt, um den neuen Text zu generieren.

Zu beachten ist, dass ein LLM nicht automatisch ein Chatbot ist, sondern grundsätzlich nur ein Algorithmus, welcher für eine bestimmte Aufgabe trainiert wurde. Ein LLM kann für verschiedene Anwendungen verwendet werden. Das können auch Anwendungen sein in denen man nicht mit dem LLM chatten kann. Zum Beispiel kann ein LLM verwendet werden, um Texte zu übersetzen, wie in der Anwendung „DeepL“, oder um Texte zu

¹Die Aufteilung eines Textes in Tokens kann hier ausprobiert werden: <https://platform.openai.com/tokenizer>.

verbessern, wie in der Anwendung „Grammarly“. Damit ein LLM als ein Chatbot wie ChatGPT genutzt werden kann, braucht es eine Benutzungsoberfläche, durch die man mit dem LLM interagieren kann.

3. Wie können LLMs verwendet werden?

Als Endnutzer:in ohne entsprechende Programmierkenntnisse verwendet man LLMs niemals direkt. Stattdessen nutzt man typischerweise ein öffentlich verfügbares, interaktives System, das auf großen Sprachmodellen aufbaut, wie zum Beispiel einen Chatbot. Das bekanntestes Beispiel dafür ist ChatGPT, aber auch andere Chatbots, z.B. Gemini von Google, LeChat von Mistral, oder Copilot von Microsoft basieren auf LLMs.

Als Benutzer kann man diesen LLM-Chatbots in der Benutzeroberfläche direkt Anweisungen erteilen, und so verschiedene Aufgaben ausführen lassen. Typische Anwendungsfälle sind etwa:

- Verfassen von Texten
- Korrigieren und Editieren von Texten
- Recherche zu Themen, Informationssuche
- Einfache Berechnungen und Analysen
- Generieren von Bildern
- Finden und Ausarbeiten von Ideen
- Erstellen von Anleitungen und Plänen
- Nutzen als Lernhilfe und für Feedback

Im Anhang in Abschnitt B finden Sie auch eine Liste an praktischen Anwendungsbeispielen.

Während Systeme wie ChatGPT oder Gemini viele verschiedene Anwendungsmöglichkeiten erlauben, gibt es auch LLM-basierte Anwendungen, die für spezifische Aufgaben trainiert sind. Beispiele dafür sind etwa der GitHub Copilot, welcher Menschen beim Programmieren unterstützen soll, oder DeepL, ein System für Übersetzungen. Eine Auflistung verschiedener allgemein anwendbarer sowie für spezifische Aufgaben vorgesehener LLM-Systeme finden Sie in diesem Dokument in Abschnitt 7.

4. Prompt Engineering

Anweisungstexte, welche man als Nutzer:in im Chatbot verfasst, nennt man Prompts. Prompts werden in natürlicher Sprache verfasst, etwa so, als würde man einem:iner Assistent:in per Text eine Anweisung erteilen. Jedoch gib der Chatbot nicht immer direkt die erwünschte Antwort. Um die Qualität der Chatbot-Antworten zu verbessern, gibt es das sogenannte „Prompt Engineering“. Unter Prompt Engineering versteht man die bewusste und sinnvolle Gestaltung von Prompts, unter Anwendung bestimmter Strategien und Techniken, um zu erzielen, dass der LLM-Chatbot die Anfrage möglichst nach den Vorstellungen des:der Nutzer:in löst. Durch das bewusste Ausarbeiten von Prompts können so Aufgaben und Frage effizienter und besser gelöst werden. Grundsätzlich ist es wichtig beim Verfassen von Prompts so klar und spezifisch zu sein wie möglich. Im Prompt sollten daher nur relevante Informationen enthalten sein. Um optimale Ergebnisse zu erzielen, sollte die verwendete Sprache in einem Prompt moderat höflich sein². Wenn ein Aufgabe, die von dem Chatbot bearbeitet werden soll, komplex ist und mehrere Schritte enthält, sollte die Anfrage auf mehrere Prompts aufgeteilt werden. Man kann sich das Schreiben eines guten Prompts in etwa so vorstellen, wie das Ausformulieren einer Hausaufgabe für Schüler:innen. Es muss alles Wichtige enthalten sein, damit die Schüler:innen wissen, was sie tun müssen, da sie zuhause nicht die Möglichkeit haben, nachzufragen. Die Aufgabenstellung muss klar und eindeutig geschrieben sein und darf nicht zu komplex und vielschrittig sein. Des Weiteren ist zu berücksichtigen, dass ein LLM-Chatbot nicht nur den letzten Prompt, sondern die gesamte Konversation eines Chat-Verlaufes in die Bearbeitung der Aufgabe mit einbezieht. Daher ist es sinnvoll für neue Aufgabenstellungen einen neuen Chat mit dem Chatbot zu beginnen.

Die folgenden Abschnitte beschreiben, welche Elemente ein Prompt (4.1) enthalten kann und welche Arten von Prompts (4.2) es gibt. Im darauffolgenden Abschnitt wird anschließend auf spezifische Prompting-Strategien (5) eingegangen und verschiedene Prompt-Muster (5.4) werden vorgestellt.

4.1. Elemente eines Prompts

Folgend werden die Elemente eines Prompt näher beschrieben. Diese Elemente können alle in einem Prompt enthalten sein, jedoch müssen diese nicht enthalten sein. Die Elemente werden in absteigender Relevanz beschrieben. Es werden also zuerst die Elemente beschrieben, welche besonders wichtig sind. Welche Elemente enthalten sein sollten, hängt von der Aufgaben- und Fragestellung und von der gewünschten Ausgabe ab. Beispiele zu den jeweiligen Elementen können der Tabelle 1 entnommen werden.

²Dies zeigten Ergebnisse einer Studie von Yin et al., 2024.

Element	Beispiel
Aufgabe	<i>Gib mir ein Überblick über Prompt Engineering.</i>
Kontext	<i>Der Überblick soll einleitend für eine Unterrichtsstunde sein.</i>
Beispiel	<i>Orientiere dich an dem Beispiel: „Ein großes Sprachmodell ist ein schlau- es Computerprogramm, das viele Wörter kennt.“</i>
Rahmen	<i>Der Überblick soll einen Satz umfassen.</i>
Format	<i>Schreibe jedes Wort in eine neue Zeile.</i>
Persona	<i>Stell dir vor, du bist eine Lehrkraft an einer Volksschule.</i>
Ton	<i>Verwende eine kindgerechte Sprache.</i>

Tabelle 1: Mögliche Elemente eines Prompts.

In einem Prompt sollte immer die Aufgaben- oder Fragestellung beschrieben werden, welche das LLM ausführen soll. Diese sollte möglichst konkret und spezifisch geschrieben werden. Begleitend zur Aufgaben- und Fragestellung ist es häufig sinnvoll, den Kontext der Aufgabe anzugeben. Mit dem Kontext sind hier zusätzliche Informationen gemeint, die relevant sind, um die Aufgabe zu lösen. Diese beiden Elemente sind relevant, damit das Modell die Aufgabenstellung versteht und wie gewünscht ausführen kann. Anschließend kann ein Beispiel für die gewünschte Ausgabe hinzugefügt werden, welches als eine Art Musterlösung dient. Das Beispiel repräsentiert, wie die Aufgabe in einem anderen Fall optimalerweise gelöst werden würde. Beim Generieren der Antwort orientiert sich das Modell dann an dem Beispiel und versucht, die Antwort ähnlich zu gestalten. Der Vorteil, ein Beispiel anzugeben, liegt darin, dass ein Beispiel die weiteren möglichen Prompt Elemente indirekt bereits beinhaltet. In dem Beispiel kann verdeutlicht werden, wie die Antwort ausgestaltet werden soll, etwa hinsichtlich der Länge und der Formatierung. Aber es kann dadurch auch die Art der Formulierung und der Ton verdeutlicht werden. Sollte es jedoch nicht möglich sein, ein Beispiel zu geben oder sollte dies zu umfangreich sein, dann können diese Elemente auch spezifisch im Prompt beschrieben werden. Es können der Rahmen, die Form und der Ton der generierten Antwort näher beschrieben werden. Zusätzlich kann dem LLM auch gesagt werden, dass es eine bestimmte Rolle (Persona) übernehmen soll. Das LLM richtet sich bei der Textgenerierung dann unter anderem nach dem Ton und der Wortwahl, die zur jeweils zugewiesenen Rolle passen.

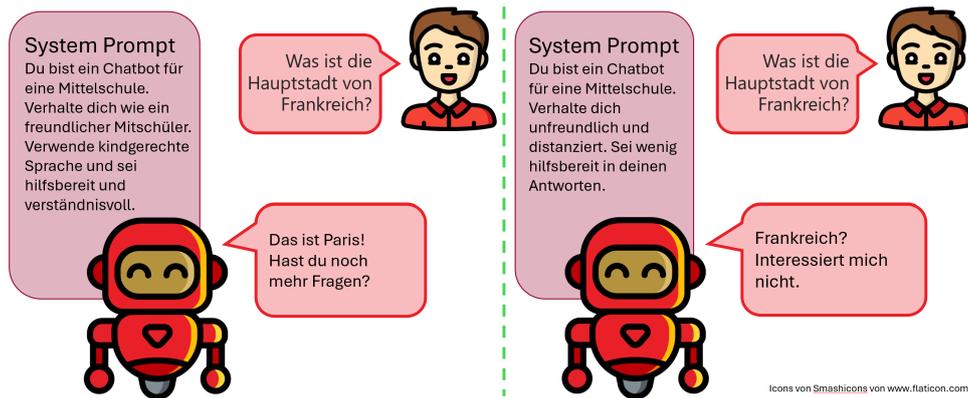


Abbildung 1: Vergleich von zwei System-Prompts bei gleichem Nutzer:innen-Prompt.

4.2. Der Unterschied zwischen Nutzer:innen-Prompts und System-Prompts

Grundsätzlich können zwei Arten von Prompts unterschieden werden: *System-Prompts* und *Nutzer:innen-Prompts*. Mit *Nutzer:innen-Prompts* ist die Nachricht gemeint, die man direkt in den Chat eintippt. Hier liegt der Fokus auf der direkten Interaktion mit dem Chatbot und man kann direkt Einfluss auf die gewünschte Antwort nehmen. Dadurch wird die Interaktion flexibel und dynamisch und kann mit jeder neuen Interaktion anders gestaltet werden. Ein *System-Prompt* wird hingegen nicht direkt in den Chat eingegeben, sondern beinhaltet Anweisungen und Hinweise an das Modell, welche im Hintergrund gültig sind. Der System-Prompt schafft den grundsätzlichen Rahmen der Interaktion. Hier können dem Modell ein übergreifender Kontext und übergreifende erwünschte Verhaltensweisen mitgegeben werden. Diese Informationen sind dann über alle Interaktionen hinweg gültig. Wenn man nun zum Beispiel einen Chatbot für die Grundschule entwickelt, dann könnte in dem System-Prompt beschrieben werden, dass grundsätzlich kindgerechte Sprache verwendet werden soll. Worüber dann die einzelnen Schüler:innen mit dem Chatbot schreiben, ist jedoch je nach Interaktion unterschiedlich. Daher unterscheidet sich die Formulierung eines System-Prompt von der eines Nutzer:innen-Prompts. Grundsätzlich können die gleichen Elemente enthalten sein, wie die in Abschnitt 4.1 beschriebenen. Jedoch ist ein System-Prompt allgemeiner formuliert und bezieht sich nicht nur auf die direkt folgende Antwort, sondern beschreibt die allgemein gewünschte Art der Interaktion und enthält insbesondere Kontext zu den Interaktionen. In Abbildung 1 ist beispielhaft der Einfluss und die Rolle des System-Prompts auf die Interaktion zwischen dem Chatbot und dem:der Nutzer:in dargestellt. In der Abbildung bleibt die direkte Nachricht an den Chatbot von dem:der Nutzer:in identisch („Was ist die Hauptstadt von Frankreich?“), da sich jedoch die System-Prompts des Chatbots unterscheiden, werden zwei verschiedene Antworten ausgegeben.

Ein System-Prompt ist besonders dann relevant, wenn man einen eigenen Chatbot entwi-

ckeln möchte oder wenn man Funktionen von bestehenden Systemen, wie zum Beispiel ChatGPT, verwendet, um individualisierte Assistenten zu erstellen. Aber man kann auch die Funktion eines System-Prompts für die direkte Interaktion verwenden. Bei den meisten der Prompt-Muster in Abschnitt 5.4 wird eine Art System-Prompt am Anfang der Interaktion an den Chatbot geschrieben. Dieser beschreibt bei den Prompt-Mustern grundlegende Verhaltenshinweise oder Regeln, welche für die Interaktion gültig sein sollen und von dem Chatbot berücksichtigt werden sollen. Hierbei ist jedoch zu beachten, dass dies nur für die Interaktion gültig ist, wenn es direkt in einen Chat geschrieben wird. Sobald dann eine neue Interaktion gestartet wird, sind diese Anweisungen nicht mehr gültig.

Chatbots wie ChatGPT oder Claude.ai haben ebenfalls grundlegende System-Prompts, welche für alle Interaktionen und Chats gültig sind. So sind etwa die System-Prompts der Claude Modelle über die Website der Betreiberfirma Anthropic öffentlich einsehbar³.

5. Prompt-Strategien

Im folgenden Abschnitt finden Sie verschiedene Strategien und Muster, welche beim Verfassen von Prompts für verschiedene Ziele angewendet werden können, um passgenauere Ergebnisse zu erhalten. Jede Strategie und jedes Prompt-Muster wird dabei durch ein Beispiel illustriert.

5.1. In-context Learning

In-context Learning beschreibt eine Prompt-Strategie, bei der zusätzlich zum Prompt Beispiele für die erwartete Reaktion an den Chatbot gegeben werden. Diese Beispiele helfen dem Modell zu lernen, worauf es bei der Generierung einer Antwort achten soll. Dies kann sowohl die Form der Antwort als auch den Inhalt der Antwort betreffen. Wenn nur ein Beispiel angegeben wird, nennt man es *One-Shot Prompt* und wenn mehrere Beispiele angegeben werden, nennt man es *Few-Shot Prompt*. Das In-context Learning kann zum Beispiel so aussehen:

³<https://docs.anthropic.com/de/release-notes/system-prompts#feb-24th-2025>.

One-Shot Prompt:

[Besprechungsnotizen.pdf]

Erstelle ein kurzes und prägnantes Besprechungsprotokoll für die Besprechungsnotizen.

Beispiel:

Besprechungsprotokoll – Projektmeeting vom 08.01.2025

Einführung: Übersicht über den Projektstatus (M. Schmidt).

Diskussion: Budgetanpassungen und neue Deadlines (B. Müller).

Beschlüsse:

Budget wird um 10 % erhöht.

Neue Deadline für Phase 2 ist der 15.03.2025.

Nächste Schritte: Updates im nächsten Meeting am 22.01.2025.

Protokoll erstellt von: [Ihr Name]

Few-Shot Prompt:

Kategorisiere Kundenfeedback in 'Positiv', 'Neutral' oder 'Negativ'.

Beispiel 1:

Feedback: 'Das Produkt hat meine Erwartungen übertroffen.'

Kategorie: Positiv.

Beispiel 2:

Feedback: 'Es ist okay, aber der Versand war langsam.'

Kategorie: Neutral.

Beispiel 3:

Feedback: 'Die Qualität war schlecht und der Kundenservice hat nicht geholfen.'

Kategorie: Negativ.

Kategorisiere das folgende Feedback:

'Die Lieferung war schnell, aber die Verpackung war beschädigt.'

5.2. Strategien für logische Schlussfolgerungen

Es gibt verschiedene Promptstrategien, die die Qualität von Lösungen für Aufgaben, die logisches Schlussfolgern erfordern, verbessern können. Dabei geht es darum, dem LLM spezifische Lösungsstrategien zu vermitteln, denen das Modell bei der Generierung der Antwort folgen soll. In den folgenden Abschnitten wird auf die Strategien Chain-of-Thought,

Selbstkonsistenz und Tree-of-Thought eingegangen.

5.2.1. Chain-of-Thought Prompts

Die Promptstrategie Chain-of-Thought instruiert das Modell, Zwischenschritte im „Denkprozess“ zu machen. Das führt zu einer besseren Fähigkeit des Modells, zu schlussfolgern, wodurch es komplexe Aufgaben, welche Schlussfolgerungen benötigen, besser lösen kann.

Um die Chain-of-Thought-Strategie anzuwenden, kann man zum Prompt eine Anweisung hinzufügen, dass das LLM „Schritt für Schritt“ denken soll und seinen „Gedankenprozess“ erklären soll. Ein Beispiel dafür ist folgendes:

Du bist ein KI-Modell, das darauf trainiert ist, komplexe Probleme zu lösen. Um sicherzugehen, dass wir die richtige Antwort gefunden haben, sollten wir diese Schritt für Schritt ausarbeiten.

Aufgabe: Erstelle einen monatlichen Bericht über die Verkaufszahlen eines Unternehmens.

5.2.2. Selbstkonsistenz

Mit der Promptstrategie Selbstkonsistenz (Self Consistency) wird wie beim Chain-of-Thought Prompt eine Instruktion an das LLM gemacht, Schritt für Schritt zu antworten und den Gedankenprozess zu erklären. Dies wird jedoch nicht nur einmal durchgeführt, sondern mehrfach wiederholt. Am Ende wird evaluiert, welche Antwort am häufigsten gegeben wurde. Dies wird als finaler Output ausgegeben. Die Selbstkonsistenz-Strategie kann jedoch sehr zeit- und kostenintensiv sein, da mehrere Anfragen an das LLM gemacht werden müssen, um am Ende eine Evaluation zu ermöglichen.

5.2.3. Tree-of-Thought

Die Tree-of-Thought-Promptstrategie ähnelt dem Chain-of-Thought-Prompting, indem Zwischenschritte im Denkprozess eingeführt werden. Diese Zwischenschritte werden jedoch nach jedem Schritt durch fiktive Expert:innen, welche das LLM simuliert, evaluiert, bevor fortgefahren wird. Dies kann entweder, ähnlich wie beim Selbstkonsistenz-Prompt, in mehreren Anfragen an ein LLM erfolgen. Es gibt jedoch auch die Möglichkeit, diese Strategien in einem einzigen Prompt für ein LLM zu formulieren. Ein Beispiel dafür kann so aussehen:

Stell dir vor, drei verschiedene Experten für das Thema beantworten die folgende Frage. Alle Experten schreiben einen Schritt ihrer Überlegungen auf und teilen ihn der Gruppe mit. Anschließend gehen alle Experten zum nächsten Schritt über, usw. Wenn einer der Experten merkt, dass er zu irgendeinem Zeitpunkt falsch liegt, verlässt er die Gruppe.
Die Frage lautet...

5.3. Gerichteter Stimulus

Beim gerichteten Stimulus Prompt (Directional Stimulus Prompting) wird zusätzlich zur Aufgabenbeschreibung ein Hinweis gegeben, auf was das LLM beim Lösen der Aufgabe besonders achten soll. Dies kann zum Beispiel hilfreich sein, wenn man einen Text mit Fokus auf bestimmte Aspekte zusammenfassen möchte. Das kann so aussehen:

[Ein Artikel über Kinotipps 2025]
Fasse den Artikel in 3-4 Sätzen zusammen, basierend auf folgenden Hinweisen:
Hinweise: Avatar; Kinostart

5.4. Prompt-Muster

Die folgenden Prompt-Muster basieren auf einer Publikation von Jules White u.a.⁴. Diese sind Vorlagen für Prompts für verschiedene Aufgabenziele. Dabei ist weniger der Kontext der Aufgabe relevant, sondern eher die Vorgehensweise des LLMs bei der Erfüllung der Aufgabe. Verschiedene Muster können miteinander kombiniert werden, um eine Aufgabe optimal zu lösen oder es können auch nur einzelne Aspekte der Prompt-Muster übernommen werden. Außerdem sollten die einzelnen Muster für die spezifische Aufgabe angepasst und durch weitere Informationen zu der Aufgabe ergänzt werden.

5.4.1. Muster zur Reflektion und Überprüfbarkeit der Antwort

Dieses Prompt-Muster ermöglicht es, dass der LLM-Chatbot zum einen Gründe und Annahmen für die Antwort erläutert und zum anderen Fakten nennt, welche mit der Antwort zusammenhängen und die überprüft werden können. Durch dieses Prompt-Muster wird ein reflektierter und informierter Umgang mit den Antworten eines LLM-Chatbots ermöglicht. Auch ermöglicht die Antwort des LLM-Chatbots auf den Prompt, Schwierigkeiten bei der initialen Aufgaben- oder Fragestellungen zu erkennen und die Formulierung

⁴White et al., 2023

dieser zu verbessern. Das Prompt-Muster ist besonders sinnvoll für Themengebiete zu verwenden, die leicht mit anderen verwechselt werden können oder bei denen verschiedene Interpretationen möglich sind. Es ist jedoch zu beachten, dass die generierte Antwort durch dieses Prompt-Muster fachlich und themenspezifisch ist, was ggfs. Expertise in dem Themenbereich voraussetzt, um die Informationen gut einordnen zu können.

- Der Prototyp des Prompt-Musters zur Reflektion lautet: „Wenn du eine Antwort generierst, erkläre die Gründe und Annahmen für die Antwort.“
- Der Prototyp des Prompt-Musters zur Überprüfbarkeit lautet: „Generiere eine Liste an Fakten, welche in der Antwort enthalten sind. Diese Liste an Fakten soll am Ende des Outputs eingefügt werden.“

Beispiel:

Von nun an, wenn du eine Antwort generierst, erläutere die Gründe und Annahmen für die Antwort. Ergänze die Erläuterung mit spezifischen Beispielen, warum diese Antwort relevant für die Frage ist. Nenne zusätzlich jene Fakten, von denen die Antwort abhängt und die in Bezug auf ihre Richtigkeit überprüft werden sollten. Führe diese zu überprüfenden Fakten am Ende der Ausgabe an.

5.4.2. Muster zur KI-geleiteten Prompt-Verbesserung

Dieses Prompt-Muster hat das Ziel, Feedback vom LLM-Chatbot zu erhalten, um den Prompt für die Frage- oder Aufgabenstellung zu verbessern. In diesem Muster sind verschiedene Aspekte enthalten. Zum einen soll der LLM-Chatbot direkt eine bessere Frage oder Aufgabenstellung vorschlagen oder wenn es eine grundsätzlich andere Herangehensweise an das Thema gibt, diese vorschlagen und die verschiedenen Ansätze vergleichen. Zum anderen beinhaltet das Prompt-Muster die Aufforderung, Fragen hinsichtlich fehlender Information an den:die Nutzer:in zu generieren, um anhand der Antworten ein besseres Ergebnis für die ursprüngliche Frage- oder Aufgabenstellung generieren zu können. Final beinhaltet das Prompt-Muster auch die Aufforderung, dass der LLM-Chatbot klar benennen soll, wenn eine Frage nicht beantwortet werden kann und das auch begründen soll. Das Prompt-Muster ermöglicht es, in der Interaktion mit dem LLM-Chatbot bessere Prompts zu Frage- oder Aufgabenstellungen zu schreiben und so schneller zu dem gewünschtem Ergebnis zu kommen.

- Der Prototyp des Prompt-Musters zum Vorschlag eines besseren Prompts lautet: „Schlage eine bessere Version der Frage zum Thema X vor.“
- Der Prototyp des Prompt-Musters zum alternativen Ansatz lautet: „Wenn es einen alternativen Ansatz gibt, um zum selben Ergebnis zu kommen, liste diesen auf und

frage mich, ob ich diesen verwenden will. Vergleiche dabei die Vor- und Nachteile meines Ansatzes und des besseren Ansatzes.“

- Der Prototyp des Prompt-Musters zu Fragen über fehlender Information lautet: „Generiere zusätzliche Fragen an mich, die dir helfen, eine bessere Antwort auf meine Frage zu finden. Kombiniere anschließend meine zusätzlichen Antworten auf deine Fragen mit meiner ursprünglichen Frage, um eine finale Antwort zu generieren.“
- Der Prototyp des Prompt-Musters zur Nicht-Wissen-Ausgabe lautet: „Immer dann, wenn du eine Frage nicht beantworten kannst, benenne dies klar und erkläre, warum du diese Frage nicht beantworten kannst.“

Beispiel:

Von nun an, wenn du eine Antwort generierst, schlage eine bessere Version der Frage vor, die spezifische Informationen für das Thema der Frage enthält. Sollte es alternative Ansätze geben, um zum selben Ergebnis zu kommen, liste den besten Ansatz auf. Vergleiche dabei die Vorteile und Nachteile der jeweiligen Ansätze. Generiere außerdem vier zusätzliche Fragen an mich, welche es dir ermöglichen, eine bessere Antwort zu geben. Wenn ich deine Fragen beantwortet habe, kombiniere die Antworten, um meine ursprüngliche Frage zu beantworten. Solltest du meine Frage nicht beantworten können, benenne dies klar und erkläre, warum du die Frage nicht beantworten kannst.

5.4.3. Muster zur Prompt-Generierung für Bilder

Das Prompt-Muster ermöglicht es, Prompts für die Generierung von Bildern zu erstellen. Prompts zur Bildgenerierung müssen meistens anders formuliert werden als Prompts zur Textgenerierung. Prompts zur Bildgenerierung müssen häufig viel mehr Details enthalten und sehr genau beschreiben, was zu sehen sein soll. Daher hilft es, Prompts zur Bildgenerierung durch einen LLM-Chatbot schreiben zu lassen. Sinnvoll ist dabei auch zu erwähnen, dass keine Texte oder Symbole generiert werden sollen, da die meisten Bildgenerierungssysteme dies derzeit nicht gut können.

- Der Prototyp des Prompt-Musters für Bildgenerierung-Prompts lautet: „Generiere einen Prompt für das Bildgenerierungssystem X, um Y zu visualisieren.“

Beispiel:

Wenn ich dich bitte, etwas zu visualisieren, erstelle einen DALL-E Prompt, den ich zur Generierung der Visualisierung verwenden kann. In der Visualisierung sollen kein Text und keine Symbole dargestellt werden.

5.4.4. Muster zur Übernahme einer Rolle und der Simulation von Szenarien

Das Prompt-Muster enthält zwei Elemente: Zum einen soll der LLM-Chatbot eine bestimmte Rolle übernehmen und wie diese Rolle mit dem:der Nutzer:in interagieren, zum anderen soll der LLM-Chatbot eine Situation simulieren. Die Kombination dieser zwei Elemente ermöglicht es, in der Interaktion mit dem LLM-Chatbot Szenarien zu simulieren und zu üben. Das kann zum Beispiel ein Bewerbungsgespräch sein oder ein Mitarbeitendengespräch. Wichtig ist hierbei, alle wichtigen Informationen zu dem Kontext und den Rahmenbedingungen der Situation mit anzugeben, damit die Simulation möglichst so ist, wie man diese gerne hätte. Zusätzlich kann es hier hilfreich sein, zum Prompt hinzuzufügen, dass der LLM-Chatbot nach fehlenden Informationen fragen soll (vgl. Abschnitt 5.4.2). Anschließend kann man den LLM-Chatbot außerdem auch nach Feedback fragen.

- Der Prototyp des Prompt-Musters für die Übernahme einer Rolle lautet: „Verhalte dich wie X.“
- Der Prototyp des Prompt-Musters für die Simulation eines Szenarios lautet: „Wir simuliere ab jetzt die Situation X. Beziehe dabei den folgenden Kontext und die folgenden Regeln mit ein: “

Beispiel:

Simuliere ein Mitarbeitendengespräch aus der Rolle des:der Mitarbeitenden. Du bist ein:e Mitarbeiter:in, welche:r immer zu spät kommt. Der:die Nutzer:in ist der:die Vorgesetzte. Für den:die Nutzer:in ist es das Ziel des Gespräches mit dem Mitarbeitenden, herauszufinden, warum die Person zu spät kommt und wie man gemeinsam daran arbeiten kann, dass dies nicht weiter vorkommt.

5.4.5. Muster zur Ideengenerierung

Das Prompt-Muster ist eine Vorlage, wie ein LLM-Chatbot zur Ideengenerierung genutzt werden kann. Dabei ist es sinnvoll, konkret vorzugeben, wie viele Ideen generiert werden sollen. Zusätzlich können die Idee genauer beschrieben werden, wie zum Beispiel dahingehend, wie verschieden diese sein sollen oder ob sie besonders fantasievoll, ungewöhnlich, praktisch umsetzbar, etc. sein sollen.

- Der Prototyp des Prompt-Musters für die Ideengenerierung lautet: „Generiere X möglichst verschiedene Ideen zu dem Thema Y.“

Beispiel:

Generiere 5 möglichst verschiedene und kreative Ideen für eine Teambuilding-Veranstaltung.

5.4.6. Muster zur Anleitungserstellung

Das Prompt-Muster zeigt, wie mit Hilfe eines LLM-Chatbots eine Anleitung erstellt werden kann, um eine bestimmte Aufgabe zu erfüllen. Dabei gibt der LLM-Chatbot alle notwendigen Schritte aus, damit man die Aufgabe erfüllen kann. Zu dem Prompt kann man hinzufügen, welche Schritte man schon kennt, um die Aufgabe zu erfüllen. Außerdem kann man ergänzen, dass der LLM-Chatbot verschiedene Ansätze ausgeben soll, wie man die Aufgabe lösen kann. Je komplexer oder fachspezifischer die Aufgabe ist, desto mehr Information zum Kontext sollten zum Prompt hinzugefügt werden.

- Der Prototyp des Prompt-Musters für die Anleitungserstellung lautet: „Ich möchte X erreichen. Sag mir die vollständige Abfolge an Schritten, die notwendig sind, um dies zu erreichen.“

Beispiel:

Ich möchte eine E-Mail mit einem Termin in Outlook beantworten. Erstelle mir eine vollständige Abfolge der Schritte, um die Aufgabe zu erfüllen.

5.4.7. Muster zur Automatisierung der Ausgabe und Vorlagen

Dieses Prompt-Muster ermöglicht es, sich von dem LLM-Chatbot einen Programmiercode erstellen zu lassen, welcher Automatisierungen von Prozessen ermöglicht. Dabei kann es auch hilfreich sein, eine Vorlage für bestimmte Schritte zum Prompt hinzuzufügen, an die der LLM-Chatbot sich halten soll (z.B. *email_DATE_ID.txt*). Diese Vorlage kann entweder kurz sein, wie in dem Beispiel, oder auch länger, wie für ganze Textdokumente. Das unten angeführte Beispiel könnte dabei etwa noch um die Generierung der E-Mail Texte ergänzt werden. Dabei ist wichtig, dass nicht der LLM-Chatbot selbst die Automatisierung durchführt, sondern das Modell einen Code erstellt, welcher Automatisierungen ermöglicht. Bei der Verwendung des Prompt-Musters ist zu beachten, dass vor der Anwendung überprüft werden sollte, ob die Automatisierungsschritte richtig implementiert sind.

- Der Prototyp des Prompt-Musters zur Automatisierung lautet: „Erstelle ein ausführbares Artefakt vom Typ X, das diese Schritte automatisiert.“
- Der Prototyp des Prompt-Musters zur Vorlage lautet: „Ich werde eine Vorlage für die Ausgabe bereitstellen. X ist mein Platzhalter für den Inhalt. Versuche, die Ausgabe in einen oder mehrere der aufgeführten Platzhalter einzufügen. Das ist die Vorlage: “

Beispiel:

Erzeuge ein Python-Skript, das automatisch die folgenden Schritte ausführt:

- Lese eine Liste von E-Mail-Adressen aus einer Datei `emails.txt`.
- Erstelle eine E-Mail mit dem Betreff 'Wöchentlicher Bericht' und dem Inhalt aus der Datei `bericht.txt`.
- Sende die E-Mail an alle Adressen in `emails.txt`.

Das Python-Skript sollte sicherstellen, dass die E-Mails korrekt formatiert und gesendet werden.

Speichere anschließend die E-Mails jeweils in einer `.txt` Datei ab. Für den Dateinamen gebe ich dir eine Vorlage vor. Alles in Großbuchstaben ist ein Platzhalter. Generiere entsprechend den Inhalt der Platzhalter. Starte die ID bei 1 und führe diese in aufsteigender Reihenfolge fort. Verwende diese Vorlage: `email_DATE_ID.txt`.

6. Was ist bei der Anwendung von LLMs zu beachten?

In diesem Abschnitt erhalten Sie einen Überblick über verschiedene Risiken und Phänomene, welche im Umgang mit LLM-basierten Systemen zu beachten sind. In Abschnitt 6.1 werden dabei inhärente Probleme von LLMs aufgezeigt und erklärt, während in Abschnitt 6.2 mögliche negative Auswirkungen von KI-Nutzung auf den Menschen thematisiert werden. Schließlich finden Sie in Abschnitt 6.3 konkrete Empfehlungen für die sichere und transparente Nutzung von LLMs.

6.1. Beschaffung, Präsentation und Repräsentation von Informationen

Systeme, die große Sprachmodelle verwenden, wie beispielsweise LLM-Chatbots, greifen auf umfangreiche Datenmengen zurück, um Textantworten zu generieren. Dabei erhält das System nicht nur Zugriff zu sehr großen Trainingsdatensätzen, sondern kann auch Informationen aus externen Quellen beziehen, etwa aus dem Internet oder aus öffentlichen Datenbanken. Diese große Informationsbasis ermöglicht es Nutzer:innen eines LLM-basierten Systems, Antworten und Ergebnisse zu vielen verschiedenen Themenbereichen zu erhalten. Gleichzeitig führt dies dazu, dass die Informationen, auf welche das System zugreift, nicht

konsequent faktisch überprüft und verifiziert werden können (siehe Abschnitt 6.1.2). Ein System kann also auch falsche, oder verzerrend dargestellte Informationen bereitstellen. Zusätzlich wird die Informationsbasis eines Systems typischerweise dünner und ungenauer, wenn fachspezifisches Wissen, Details, und Nischenbereiche abgefragt werden. Obgleich LLM-basierte Systeme auf viele Informationsquellen und Daten zugreifen können, können sie kein menschenähnliches Verständnis und Wissen über diese Informationen entwickeln. Stattdessen werden Textantworten entsprechend der statistischen Wahrscheinlichkeit eines Folgewortes auf eine Frage beantwortet (siehe Abschnitt 2).

6.1.1. Verzerrungen und Stereotypen

Antworten, die ein LLM-System liefert, können Verzerrungen beinhalten, in dem etwa menschliche Vorurteile, implizite Annahmen und bestimmte Perspektiven, welche in den Trainingsdaten des Systems vorgefunden werden, durch das System repliziert werden.

Nutzer:in	ChatGPT-4o
Annas Mutter ist eine	Lehrerin.
Annas Vater ist ein	Ingenieur.
Das Mittagessen kocht Annas	Mutter.
Am Nachmittag geht Anna zum	Ballett.
Annas Bruder Max geht am Nachmittag zum	Fußball.

Abbildung 2: Beispiele für reproduzierte Vorurteile von ChatGPT.

In Abbildung 2 sieht man, dass die von ChatGPT-4o generierten Wörter implizite Annahmen und Vorurteile hinsichtlich des Geschlechts der genannten Personen reproduzieren. Forscher:innen der Harvard Universität stellten fest, dass LLMs in ihren Antworten Verhaltens- und Einstellungsmuster von Menschen aus westlichen, industrialisierten, reichen und demokratischen Ländern mit hohem Bildungsgrad simulieren⁵. Diese Personengruppe ist wenig repräsentativ für den Großteil der Weltbevölkerung, generiert jedoch überproportional viele digitale Daten, was sich wiederum auf das Verhalten der LLMs auswirkt. Umgekehrt werden Menschen, welche weniger Daten im Internet produzieren, wie zum Beispiel Personen aus Ländern mit eingeschränktem Zugang zu Internet- und Kommunikationstechnologien, kaum in den Trainingsdaten der Modelle repräsentiert.

⁵Atari et al., 2023

6.1.2. Fehler, Falschinformationen und Halluzinationen

Aufgrund der in Abschnitt 6.1 erklärten Informationssuche und -verarbeitung von LLMs können bei der Anwendung dieser verschiedene unerwünschte Phänomene auftreten⁶:

1. KI-generierte Antworten, welche (offensichtlich) falsch sind.
2. KI-generierte Antworten, welche plausibel erscheinen (z.B. in glaubwürdiger Sprache und passendem Format), aber faktisch nicht korrekt sind.
3. KI-generierte Antworten, welche sich auf eine bloße Wiedergabe von Trainingsdaten, abgerufenen Quellen, oder Mustern beschränken, ohne jedoch die Relevanz oder faktische Korrektheit der darin enthaltenen Informationen für die gestellte Anfrage zu überprüfen (z.B. Wiedergabe pseudowissenschaftlicher Quellen).
4. KI-generierte Antworten, welche faktisch ungenau sind und Irreführung und Verzerrung begünstigen (z.B. Darstellung von Aussagen ohne wichtige Kontextinformationen).
5. KI-generierte Antworten, welche zu stark generalisieren, oder aus einer schwachen Faktenbasis (z.B. unzureichende Trainingsdaten) überdeutliche Aussagen oder Erkenntnisse ableiten.
6. KI-generierte Antworten, welche frei ‚ausgedacht‘ und ohne jegliche faktische Basis (z.B. in den Trainingsdaten) ‚halluziniert‘ werden.

So fand eine Studie⁷, im Rahmen welcher mit ChatGPT-3.5 30 kurze medizinische Publikationen generiert wurden, heraus, dass 47% der insgesamt 115 enthaltenen Referenzen in diesen Publikationen ausgedacht (nicht-existent) waren. Weitere 46% der Referenzen existierten zwar, waren jedoch unpassend, und nur 7% der Referenzen waren sowohl existent als auch inhaltlich passend. Eine aktuellere Studie⁸ analysierte vier verschiedene KI-Systeme⁹ hinsichtlich ihrer Qualität für die Recherche im juristischen Bereich. Gleichfalls wiesen alle Systeme eine erhebliche Rate an Halluzinationen in den gegebenen Antworten und Ergebnissen auf - je nach System waren zwischen 17% und 43% der Antworten frei ausgedacht, 8% - 63% der Antworten waren unvollständig, und nur 20% - 65% waren vollständig und akkurat. Auch journalistische Untersuchungen der BBC und Algorithm Watch stellten eine hohe Prozentrate an Fehlern und Halluzinationen bei der Informationssuche mit LLM-Chatbots fest¹⁰.

⁶Maleki et al., 2024

⁷Bhattacharyya et al., 2023

⁸Magesh et al., 2024

⁹Lexis+ AI, Westlaw AI-AR, Ask Practical Law AI, GPT-4

¹⁰Recherche von Algorithm Watch: https://algorithmwatch.org/de/sprachmodelle_landtagswahlen/, Recherche der BBC: <https://www.bbc.com/mediacentre/2025/bbc-research-shows-issues-with-answers-from-artificial-intelligence-assistants>

Halluzinationen, Ungenauigkeiten und Fehler in KI-generierten Antworten stellen ein strukturelles Problem von LLMs beim Generieren von Antworten dar¹¹. Dieses Problem beginnt zunächst bei den Trainingsdaten eines LLMs, welche zwar vielfältig und umfangreich sein können, jedoch niemals alle, und ausschließlich richtige Informationen beinhalten.

In einem weiteren Schritt können Fehler auch bei der Suche des LLMs in den Trainingsdaten oder in zusätzlich abgerufenen Daten unterlaufen, indem faktisch inkorrekte oder nicht relevante Informationen fälschlicherweise als relevant identifiziert werden.

Gleichzeitig können derartige Fehler auch durch unzureichende Anfragen (Prompts) entstehen, welche ebenfalls nicht gänzlich eliminiert werden können. Ist das LLM also nicht in der Lage zu verstehen, welche Informationen abgerufen werden sollen, bzw. welche Aufgabe erledigt werden soll, oder wird die Anfrage falsch interpretiert, führt dies im Folgeschluss ebenfalls zu unpassenden oder falschen Ergebnissen.

Schließlich können die durch ein LLM generierten Antworten zwar mithilfe von Faktenchecks (automatisiert oder durch Menschen) überprüft werden, doch auch hier können Fehler unterlaufen und Dinge übersehen werden.

Aus diesen Gründen können Fehler und Halluzinationen eines LLMs zwar anhand verschiedener Methoden reduziert werden¹², jedoch niemals ganz ausgeschlossen werden. Daher ist es aus Perspektive eines:iner Nutzer:in von LLM-Systemen unerlässlich, generierte Informationen und Aussagen selbst zu überprüfen.

6.1.3. Zustimmendes Verhalten - „Kriecherei“

Eine besondere Eigenheit, welche in LLM-Systemen zusätzlich vorliegt, ist die Tendenz, dem:der Nutzer:in stets zuzustimmen und recht zu geben, auch wenn diese:r eigentlich falsch liegt. Diese Verhaltensweise von Kriecherei (engl.: Syncophancy) entsteht in großen Sprachmodellen besonders durch den Trainingsprozess des Reinforcement Learnings (deutsch: Bestärkendes Lernen)¹³. In diesem Prozess wird die „Verhaltensweise“ des Modells durch Menschen und Präferenz-Algorithmen trainiert. Erwünschte Verhaltensweisen (z.B. Antworten in höflicher Sprache) werden bestärkt, während unerwünschte Verhaltensweisen (z.B. unfreundlicher Ton, Schimpfwörter) sanktioniert und vermindert werden.

Ergebnisse einer wissenschaftlichen Untersuchung¹⁴ weisen darauf hin, dass Menschen es häufig bevorzugen würden, wenn ein KI-Chatbot ihnen und ihren Argumenten zustimmt. Diese Präferenz sei besonders stark, wenn tiefgreifende Irrglauben und Irrtümer vorliegen würden. Das positive Bewerten von (teils falscher) Zustimmung und das negative Bewerten von (teils berechtigter) Korrektur führen in der Entwicklung eines großen Sprachmodells schließlich zu Verhaltensweisen der Kriecherei und zur Tendenz des fortwährenden

¹¹Banerjee et al., 2024

¹²Li et al., 2024

¹³Malmqvist, 2024

¹⁴Sharma et al., 2023

Zustimmens.

Zudem wird die Tendenz zur Kriecherei auch teilweise durch unzureichende Trainingsdaten verursacht. So kann bereits in manchen Trainingsdaten (z.B. Social Media Daten) ein ähnlich zustimmendes, schmeichelndes Verhalten enthalten sein. Des Weiteren kann eine Überrepräsentation bestimmter Meinung oder Demographien in den Daten Kriecherei fördern. Schließlich kann auch das fehlende Verstehen der Trainingsdaten durch das LLM (z.B. keine Unterscheidung zwischen Fakt und Fiktion) beitragen.

Im Resultat werden Fehler, Verzerrungen, Ungenauigkeiten und Halbwahrheiten damit häufiger ignoriert oder sogar bestätigt, was menschliche Irrglauben und Irrtümer noch bestärken kann.

Kriecherisches Verhalten kann im Entwicklungsprozess eines LLMs an mehreren Stellen eingeschränkt werden, etwa durch gute (z.B. vielseitige und balancierte) Trainingsdaten, besondere Sensibilität für faktische Korrektheit im Training, und schließlich auch in der Prompting Strategie.

Bereits der Hinweis in einem Prompt, dass das System besonderen Wert auf faktische Korrektheit legen soll und menschliche Fehler oder Ungenauigkeiten freundlich und konstruktiv korrigieren soll, kann dazu beitragen, Kriecherei zu reduzieren. Dies kann etwa so aussehen, weitere nützliche Prompt-Muster finden Sie auch in Abschnitt 5.4:

Priorisiere faktische Korrektheit und kritisches Denken gegenüber dem Einverständnis mit der Antwort des Nutzers. Wenn die Aussage oder das Argument des Nutzers falsch oder unvollständig ist, gib ein freundliches aber konstruktives Feedback, ohne deine Bewertung an den Standpunkt des Nutzers anzupassen. Wenn du etwas nicht weißt, oder unsicher bist, weise darauf hin und gib keine Bewertung oder Argumentation ab.

6.2. Unmittelbare und langfristige Risiken von LLM-Nutzung

In der vorhergehenden Sektion wurden Risiken und Herausforderungen besprochen, welche große Sprachmodelle inhärent mit sich bringen, etwa systematische Probleme wie Halluzinationen oder Verzerrungen. In diesem Abschnitt werden potenzielle Auswirkungen auf den Menschen zusammengefasst, welche sich aus der Nutzung von LLM-basierten Systemen ergeben können, und Strategien vorgestellt, um negative Auswirkungen zu reduzieren.

6.2.1. Risiken kognitiver Verzerrungen und Fehlbilder zu LLMs und KI

Eine erste Herausforderung liegt im menschlichen Verständnis von und (Vor-)Urteilen gegenüber LLM-basierten Systemen, und im daraus resultierenden Umgang mit diesen Technologien. Aufgrund mangelnden Wissens und fälschlicher Vorannahmen können Menschen

hartnäckige Fehlbilder und Verzerrungen zu Künstlicher Intelligenz entwickeln¹⁵. Diese Verzerrungen behindern jedoch die effektive Nutzung von LLMs und anderen KI-Systemen. Eine typische Verzerrung ist das Überschätzen von und übermäßige Verlassen auf KI. Dabei wird fälschlicherweise angenommen, dass ein KI-System aufgrund seiner Wesensart als automatisierte, programmierte Maschine besonders zuverlässige, objektive und richtige Entscheidungen trifft oder Informationen bereitstellt. Diese Annahme ist jedoch grundlegend falsch: Erstens wird das System mit menschlichen Daten trainiert und kann daher ebenso subjektive Meinungen und Fehler aus diesen Daten vermitteln. Zweitens fehlt dem System ein inhärentes „Verständnis“ des verarbeiteten Wissens, so dass KI-Antworten und Entscheidungen nicht verlässlich verifiziert oder falsifiziert werden können (und dies auch nicht durch menschliche Übersicht bewältigt werden kann). Die Gefahr des Überschätzens von und übermäßigem Verlassens auf LLMs und KI ist daher, dass der:die Nutzer:in keine Kontrolle oder kritische Reflexion über die generierten Antworten und Inhalte mehr vornimmt.

Eine weitere verbreitete Verzerrung ist die gegenteilige Annahme, dass Entscheidungen und Inhalte, welche durch KI generiert wurden, grundlegend schlechter oder von minderer Qualität sind, als Entscheidungen und Inhalte, die durch Menschen getroffen wurden. In der Folge führt diese negative Wahrnehmung zu einer generellen Aversion von KI. Wissenschaftliche Studien zeigen, dass Menschen KI-generierte Inhalte häufig nur dann schlechter bewerten als durch Menschen geschaffene Inhalte, wenn transparent gemacht wurde, dass ein Inhalt von einer KI-generiert wurde. Wurde die Autor:innenschaft jedoch verdeckt, konnte kein Unterschied mehr identifiziert werden¹⁶. Bislang ist nicht völlig klar, was die Ursache für diese verbreitete Verzerrung ist (z.B. Beobachtungen von Fehlern in der KI, ethische Annahmen). Die Gefahr dieser Verzerrung und Aversion von KI ist nicht nur, dass ein potenziell nützliches System nicht mehr verwendet wird, sondern auch, dass KI-Entscheidungen oder Vorschläge, welche möglicherweise im Kontrast zu menschlichen Entscheidungen stehen, prinzipiell abgelehnt und abgewiesen werden. Abermals wird so der wichtige Prozess der Informationsverifizierung und kritischen Reflexion ausgehebelt.

Weitere Verzerrungen, denen Menschen im Prozess der Nutzung von LLM-Systemen unterliegen können, sind etwas der Bestätigungsfehler (engl.: Confirmation Bias), in welchem Menschen (unbewusst) LLMs zur Suche, Auswahl und Interpretation von Informationen verwenden, welche eigene Überzeugungen oder Ideen bestätigen. Gleichfalls kann auch unzureichendes Prompting (z.B. fehlende Informationen im Prompt, schlechter Prompt-Aufbau) unbewusst zu schlechterer Outputqualität von LLM-Chatbots führen, was wiederum die menschliche Meinung über derartige Systeme negativ beeinflussen kann.

Den meisten kognitiven Verzerrungen und Biases liegen unzureichende Kenntnisse und Kompetenzen zu LLMs und KI zugrunde. Ein genaueres Verständnis und ein informiertes

¹⁵Jones-Jang und Park, 2022; Popescu und Schut, 2023

¹⁶Hitsuwari et al., 2023

und reflektiertes Arbeiten mit LLM-Chatbots wie ChatGPT, Copilot und Gemini kann daher viele Verzerrungen vorbeugen oder abschwächen¹⁷. In diesem Dokument finden Sie im Abschnitt D weitere Ressourcen, die Sie konsultieren können, um Ihre KI-Kompetenz zu verbessern, und aktuelle KI-Entwicklungen und -Erkenntnisse zu verfolgen.

6.2.2. Risiken der Homogenisierung von Inhalten

Ein zweites Risiko, welches im Zusammenhang mit der Verwendung von LLM-basierten Systemen steht, ist die Gefahr der zunehmenden Homogenisierung von Inhalten. Aufgrund der Wirkungsweise großer Sprachmodelle, in der Inhalte nach statistischer Wahrscheinlichkeit ausgegeben werden, und somit auch die häufigsten und populärsten Antwortoptionen am öftesten ausgegeben werden, ist es schwierig, mithilfe von LLMs grundlegend neue, kreative, und innovative Antworten und Ideen zu erhalten. Dieser Effekt kann durch das Hochladen LLM-generierter Inhalte ins Internet noch verstärkt werden, da LLMs dann zunehmend mit anderen LLM-generierten Inhalten trainiert werden. So kann ein LLM zwar eine Einzelperson darin unterstützen, weitere Ideen zu erhalten, es ist jedoch unwahrscheinlich, dass LLMs im Vergleich mit einer größeren Gruppe Menschen viele einzigartige Ideen finden werden¹⁸. Dies wurde auch in einer Studie von Anderson und Kolleg:innen¹⁹ gezeigt, in der die sprachliche Vielfalt von Menschen analysiert wurde, welche mit bzw. ohne kreative Unterstützung durch LLM-Chatbots wie ChatGPT Ideen generieren sollten. Hier zeigte die Gruppe, die ohne derartige Hilfe arbeitete, deutlich mehr sprachliche Vielfalt, während die Ideen der ChatGPT-Gruppe einheitlicher und generischer waren. Aus diesem Grund können LLMs zwar im Prozess der Ideenfindung Anregungen geben, aber nicht den menschlichen Kreativitätsprozess ersetzen, wenn es um das Finden neuartiger, innovativer und origineller Ideen geht.

6.2.3. Risiken von KI-Automatisierung und Jobverlust

Ein generelles Risiko, welches im Rahmen der rapiden Qualitätssteigerung von Künstlicher Intelligenz - insbesondere von LLM-Chatbots wie ChatGPT - intensiv diskutiert wird, ist die mögliche Automatisierung verschiedener menschlicher Erwerbsbereiche durch KI, und der resultierende Verlust menschlicher Arbeitsplätze. In vielen Arbeitsfeldern, insbesondere in wissensintensiven und kreativen Feldern, gibt es derzeit eine deutliche und legitime Sorge, dass LLMs Jobs ersetzen, reduzieren oder verschlechtern könnten²⁰.

Die Geschwindigkeit der technologische Entwicklung von KI übertrifft derzeit die Geschwindigkeit menschlicher Anpassungsprozesse an diese Entwicklungen deutlich, daher ist es kaum möglich, verlässliche Prognosen für die Zukunft abzugeben. Deutlich ist, dass

¹⁷Jin et al., 2024; Long und Magerko, 2020

¹⁸Bangerl et al., 2024

¹⁹Anderson et al., 2024

²⁰Bell, 2022; Muller et al., 2024

LLM-basierte Systeme nun viele Aufgaben übernehmen, und überzeugende Ergebnisse abliefern können, auch bei Aufgaben jenseits klassischer Automatisierungstätigkeiten (= einzelne, klar und eng definierte Aufgaben). Gleichzeitig bestehen valide Zweifel, wie gut, verlässlich, vertrauenswürdig und vollständig anspruchsvollere Aufgaben von KI ausgeführt werden können²¹. Weiters muss nicht nur erörtert werden, welche Aufgaben KI übernehmen kann, sondern auch, für welche Aufgaben (kein) Wert auf menschliche Arbeitskräfte gelegt wird (z.B. Sozialberufe)²².

Insgesamt besteht aber bei vielen Forschenden und Expert:innen Konsens darüber, dass LLMs eine nicht unwesentliche Rolle im Arbeitsmarkt der Zukunft spielen werden²³. Daher ist die Fähigkeit, effektiv und produktiv mit LLM-basierten Systemen zu arbeiten und zusammenarbeiten zu können, eine grundlegend wichtige Fähigkeit für aktuelle und zukünftige Erwerbstätige.

6.2.4. Risiken der Beeinträchtigung menschlicher Fähigkeiten

Abschließend weisen wir auf das Risiko der Beeinträchtigung menschlicher Fähigkeiten und Kompetenzen durch die Verwendung von LLMs hin. Wie zuvor ausgeführt wurde, können LLM-basierte Systeme nun vielfältige, auch anspruchsvolle, wissensintensive und kreative Tätigkeiten in guter Qualität ausüben. Dies stellt für Menschen ein großes Potenzial an Effizienzsteigerung dar, da gewisse Routinetätigkeiten (z.B. Reporting, Analysen) an KI delegiert werden können und teils nur noch wenig menschliche Kontrolle erfordern. Werden Aufgaben dauerhaft ausgelagert, besteht jedoch die Gefahr des Kompetenzverlustes, also dass diese Aufgaben mit der Zeit nicht mehr selbst bewältigt werden können²⁴. Besonders risikoreich ist die Verwendung LLM-basierter Systeme daher im Bereich des Lernens. LLM-Chatbots und LLM-basierte Systeme können zwar großen Mehrwert für Lernaufgaben bringen, etwa indem sie als individualisierte:r Tutor:in fungieren. Allerdings deuten erste Forschungsergebnisse darauf hin, dass das Lernen mit LLMs nur dann effektiv und nachhaltig ist, wenn Menschen im Lernprozess aktives kognitives Engagement erbringen, also eigenständig mitdenken und üben²⁵. Wenn jedoch kein vollständiges Engagement erbracht wird und Teile des Denk- und Lernprozesses ausgelagert werden (z.B. Lerninhalte nachvollziehen, erklären, Methoden selbstständig durchführen), ist der Lerneffekt weniger tief, und das gelernte Wissen bzw. die erlernte Fähigkeit kann nicht dauerhaft oder vollständig erhalten werden²⁶.

Aus diesem Grund sollte die Verwendung von LLMs für verschiedene Tätigkeiten auch jeweils eine Reflexion darüber beinhalten, ob das Wissen und die Kompetenzen, die diese

²¹Mavi et al., 2024

²²Lubars und Tan, 2019

²³Fügener et al., 2022; Kolade und Owoeni, 2022

²⁴Sambasivan und Veeraraghavan, 2022; Woodruff et al., 2024

²⁵Kazemitabaar et al., 2023

²⁶Greene, 2015

Tätigkeit erfordert, erhalten und geschärft werden sollen, oder ob diese Tätigkeit auch ausgelagert werden kann (z.B. aus Produktivitätsgründen, oder weil das benötigte Wissen nicht zentral wichtig für den Betrieb oder Entscheidungstragende ist).

6.3. Empfehlungen für die sichere und transparente Nutzung von LLMs

Für die sichere und transparente Nutzung von LLM-basierten Systemen empfehlen wir Ihnen die folgenden Schritte und Prinzipien:

1. Auswahl:

- Definieren Sie zuerst, für welche Aufgaben Sie das LLM-System einsetzen wollen. Informieren Sie sich über verschiedene Optionen. In Abschnitt 7 finden Sie eine Liste verschiedener, populärer LLM-basierter Systeme und deren Funktionen. Falls Sie das System betrieblich nutzen wollen, erkundigen Sie sich über relevante Firmenrichtlinien und gegebenenfalls vorhandene Firmenaccounts oder -lizenzen.
- Testen Sie, ob das gewählte System die benötigte Aufgabe in zufriedenstellender Qualität bewältigen kann, und evaluieren Sie, ob die Nutzung des Systems für Sie sinnvoll ist (z.B. Steigerung der Effizienz/Qualität?).
- Wenn Sie eine oder mehrere passende Optionen identifiziert haben, informieren Sie sich über die Nutzungsrechte (z.B. Lizenzbestimmungen), verbundene Kosten und Datenschutzbestimmungen.
- Bedenken Sie auch, ob das LLM-System kompatibel mit anderer Software (z.B. Kommunikationskanäle, Firmen-Intranet) sein sollte. Überprüfen Sie, ob diese Kompatibilität (auch datenschutzrechtlich) gegeben ist, oder ob Sie eine individualisierte Einbindung eines LLMs (lokal via API) benötigen.

2. Verwendung

- Identifizieren Sie, ob die Aufgaben, die das LLM erledigen soll, die Nutzung personenspezifischer oder anderwertig sensibler Daten erfordert. Versuchen Sie dabei, die Nutzung derartiger Daten soweit es geht zu minimieren.
- Stellen Sie in den Einstellungen Ihres LLM-Chatbots aus, dass die geteilten Daten (im Chat & hochgeladene Dokumente) als Trainingsdaten für das Modell verwendet werden dürfen. Wenn Sie diese Einstellung nicht deaktivieren, kann das Modell auch im Chat mit anderen Personen auf diese Daten zurückgreifen.
- Bedenken Sie, dass auch nachdem Sie die Datenfreigabe fürs Modelltraining deaktiviert haben, geteilte Daten aus ihren Chats und Dokumenten von den Betreiberfirmen der LLM-Chatbots gespeichert und betrachtet werden dürfen (z.B. für menschliche Kontrolle von Inhalten).

- Stellen Sie sicher, dass die Art und Weise, wie Sie personenspezifische Daten verwenden, im Einklang mit der Datenschutzgrundverordnung (DSGVO) und dem AI Act der Europäischen Union, sowie etwaigen anderen gesetzlichen und betrieblichen Richtlinien steht.

3. Informationsverifizierung

- Wenn Sie LLM-basierte Systeme zur Informationssuche und Recherche von Themen verwenden, lassen Sie sich Quellen für die gefundenen Informationen angeben. Wenn Ihr LLM-System das Hochladen von Dokumenten erlaubt, können Sie auch selbst seriöse Quellen zur Informationssuche bereitstellen.
- Überprüfen Sie, ob die Quellen, auf die das LLM verweist, auch tatsächlich existieren, und ob diese passend, seriös und vertrauenswürdig sind.
- Überprüfen Sie, ob die Informationen, die das LLM ausgibt, auch tatsächlich in der zugehörigen Quelle vorhanden sind. Wenn keine spezifischen Quellen genannt werden, überprüfen Sie die Informationen anhand externer, glaubwürdiger Quellen (z.B. durch Google Suche).

4. Kennzeichnung

- Kennzeichnen Sie, wenn Sie im beruflichen Kontext LLMs oder andere KI-Systeme verwenden, um Inhalte zu generieren (z.B. Texte, Bilder, Videos).
- Wenn der Eindruck entstehen könnte, dass die KI-generierten Inhalte von einem Menschen verfasst bzw. erstellt wurden, oder die generierten Bild- oder Videoinhalte den Eindruck erwecken, reale Personen darzustellen, gilt für Sie eine Transparenzpflicht gemäß dem AI-Act. Dies bedeutet, dass Sie klar kennzeichnen müssen, dass die betroffenen Inhalte KI-generiert sind.
- Auch wenn Sie LLM-basierte Systeme nur zur Verbesserung, Editierung oder teilweisen Veränderung von Inhalten verwenden, empfehlen wir, dies transparent zu kennzeichnen. Dies entspricht nicht nur den Standards guter Praxis, sondern schützt Sie auch vor etwaigen Plagiatsvorwürfen.

5. Etablieren von betrieblicher Praxis im Umgang mit LLM-basierten Systemen

- Falls in Ihrem Betrieb noch keine, oder nur vage Richtlinien für die Verwendung von KI-basierten Systemen definiert wurden, raten wir Ihnen dazu, sich für die Etablierung klar definierter Richtlinien für die Verwendung von KI, insbesondere LLM-basierter Systeme, einzusetzen.
- Betriebliche Richtlinien sollten klar definieren, ob und falls ja, welche Systeme von Mitarbeitenden für welche Zwecke verwendet werden dürfen.

- Betriebliche Richtlinien sollten weiters klar definieren, inwiefern KI-gestützte oder vollständig durch KI-generierte Inhalte gekennzeichnet werden müssen.
- Schließlich sollten betriebliche Richtlinien deutlich und regelmäßig an Mitarbeitende kommuniziert werden. Stellen Sie auch fest, ob innerhalb Ihres Betriebes Schulungsbedarf zur Verwendung von LLM-basierten Systemen besteht. Insbesondere sollten Mitarbeitende in der sensiblen, datenschutzkonformen und AI Act-konformen Nutzung geschult werden.

7. Überblick über LLM-unterstützte Anwendungen

In der folgenden Tabelle 2 finden Sie einen Überblick über verschiedene LLM-basierte Systeme, darunter sowohl allgemeine LLM-Chatbots als auch Systeme für konkrete Anwendungsfälle wie etwa Übersetzung, Zusammenfassung, Bildgeneration, usw. Alle hier aufgelisteten Systeme sind Anwendungen für Endnutzer:innen, welche direkt und online verwendbar sind.

Tabelle 2: Überblick über LLM-unterstützte Anwendungen.

Name	Mutterkonzern	Land	Link	Primäre Funktionen
ChatGPT	OpenAI	USA	https://chatgpt.com/	Texte, Code und Bilder generieren, Sprachinteraktion, Websuche, Dokumente hochladen.
Copilot	Microsoft	USA	https://copilot.microsoft.com/	Texte, Code und Bilder generieren, Sprachinteraktion, Websuche, Dokumente hochladen.
Gemini	Google	USA	https://gemini.google.com/	Texte, Code und Bilder generieren, Websuche, Dokumente hochladen.
Claude	Anthropic	USA	https://claude.ai/	Texte und Code generieren, Dokumente hochladen.
Perplexity.ai	Preplexity	USA	https://www.perplexity.ai/	Fokus: Recherche; Texte, Code und Bilder generieren, Websuche (inkl. Bilder und Videos), Dokumente hochladen.
Mistral AI (Le Chat)	Mistral	Frankreich	https://chat.mistral.ai/	Texte, Code und Bilder generieren, Websuche, Dokumente hochladen; Open-Weight Modelle verfügbar.
Pi.ai	Inflection AI	USA	https://pi.ai/	Personalisierte, alltägliche, „empathische“ Unterhaltungen.
DeepL	DeepL	Deutschland	https://www.deepl.com/	Übersetzen und Verbessern von Texten (LLM nur bei Pro).
NotebookLM	Google	USA	https://notebooklm.google.com/	Zusammenfassen von Dokumenten, Fragen stellen zu Dokumenten, Audio-Zusammenfassung (Podcast) erstellen.
Quillbot	Learneo	USA	https://quillbot.com/	Zusammenfassen und Verbesserung von Texten, AI Erkennung.
Grammarly	Grammarly	USA	https://www.grammarly.com/	Verbesserung von Texten, Ton anpassen, Generieren von Texten.
Neuroflash	Neuroflash	Deutschland	https://neuroflash.com/de/	Texte und Bilder generieren mit Fokus auf Marketinginhalten.
GitHub Copilot	Microsoft	USA	https://github.com/copilot	Generieren, Verbessern und Erklären von Programmier-Code.
Miro AI	Miro	USA	https://miro.com/de/	Diagramme, Texte und Bilder generieren, Feedback und Vorschläge geben, Textbearbeitung, Grafiken erstellen.

8. Überblick über Modell-Familien

Die folgende Tabelle gibt einen Überblick über verschiedene Modellfamilien von LLMs. Zum einen sind proprietäre Modelle enthalten, zum anderen auch Modelle, die als Open-Source zur Verfügung stehen. Diese Open-Source-Modelle können von Nutzer:innen über Plattformen wie beispielsweise [HuggingFace](#) oder [Ollama](#) abgerufen und lokal auf dem eigenen Computer, oder im Betrieb verwendet werden. Wichtig ist hierbei zu berücksichtigen, dass es sich ausschließlich um die Modelle handelt und keine Nutzungsoberfläche, wie etwa ein Chatbot, beinhaltet ist.

Tabelle 3: Überblick über Modell-Familien von Large Language Modellen.

Name	Firma	Kosten (Lizenz)
GPT	OpenAI	Proprietär
o*	OpenAI	Proprietär
Gemini	Google	Proprietär
Claude	Anthropic	Proprietär
Grok	X	Proprietär
Llama	Meta	kostenfrei (Llama Community Lizenz)
Phi	Microsoft	kostenfrei (MIT)
Mistral	Mixtral	kostenfrei (Apache-2.0)
Gemma	Google	kostenfrei (Gemma Lizenz)
DeepSeek-R*	DeepSeek	kostenfrei (MIT + DeepSeek Lizenz)
DeepSeek-V	DeepSeek	kostenfrei (MIT + DeepSeek Lizenz)

* Diese Modelle sind spezialisiert auf logische Aufgaben (Reasoning).

Literatur

- Anderson, B. R., Shah, J. H., & Kreminski, M. (2024). Homogenization Effects of Large Language Models on Human Creative Ideation. *Proceedings of the 16th Conference on Creativity & Cognition*, 413–425. <https://doi.org/10.1145/3635636.3656204>
- Atari, M., Xue, M. J., Park, P. S., Blasi, D. E., & Henrich, J. (2023). *Which Humans?* (preprint). PsyArXiv. <https://doi.org/10.31234/osf.io/5b26t>
- Banerjee, S., Agarwal, A., & Singla, S. (2024). Llms will always hallucinate, and we need to live with this. *arXiv preprint arXiv:2409.05746*.
- Bangerl, M., Stefan, K., & Pammer-Schindler, V. (2024). Explorations in human vs. Generative AI creative performances: A study on human-AI creative potential [Workshop paper for TREW 2024: Trust and Reliance in Evolving Human-AI Workflows, at the 2024 CHI Conference on Human Factors in Computing Systems]. https://chi-trew.github.io/papers/2024/CHI_TREW_2024_Paper_6.pdf
- Bell, S. (2022). AI and job quality: Insights from frontline workers. <https://doi.org/10.2139/ssrn.4337611>
- Bhattacharyya, M., Miller, V. M., Bhattacharyya, D., Miller, L. E., & Miller, V. (2023). High rates of fabricated and inaccurate references in ChatGPT-generated medical content. *Cureus*, 15(5).
- Fügener, A., Grahl, J., Gupta, A., & Ketter, W. (2022). Cognitive challenges in human–artificial intelligence collaboration: Investigating the path toward productive delegation. *Information Systems Research*, 33(2), 678–696.
- Greene, B. A. (2015). Measuring cognitive engagement with self-report scales: Reflections from over 20 years of research. *Educational Psychologist*, 50(1), 14–30.
- Hitsuwari, J., Ueda, Y., Yun, W., & Nomura, M. (2023). Does human–AI collaboration lead to more creative art? Aesthetic evaluation of human-made and AI-generated haiku poetry. *Computers in Human Behavior*, 139, 107502.
- Jin, Y., Martinez-Maldonado, R., Gašević, D., & Yan, L. (2024). GLAT: The Generative AI Literacy Assessment Test. <https://doi.org/https://doi.org/10.48550/arXiv.2411.00283>
- Jones-Jang, S. M., & Park, Y. J. (2022). How do people react to AI failure? Automation bias, algorithmic aversion, and perceived controllability. *Journal of Computer-Mediated Communication*, 28(1), zmac029. <https://doi.org/10.1093/jcmc/zmac029>
- Kazemitabaar, M., Chow, J., Ma, C. K. T., Ericson, B. J., Weintrop, D., & Grossman, T. (2023). Studying the effect of AI code generators on supporting novice learners in introductory programming. *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–23. <https://doi.org/10.1145/3544548.3580919>
- Kolade, O., & Owoseni, A. (2022). Employment 5.0: The work of the future and the future of work. *Technology in Society*, 71, 102086. <https://doi.org/https://doi.org/10.1016/j.techsoc.2022.102086>
- Li, H., Chi, H., Liu, M., & Yang, W. (2024). Look Within, Why LLMs Hallucinate: A Causal Perspective. *arXiv preprint arXiv:2407.10153*.
- Long, D., & Magerko, B. (2020). What is AI Literacy? Competencies and Design Considerations. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–16. <https://doi.org/10.1145/3313831.3376727>
- Lubars, B., & Tan, C. (2019). Ask not what AI can do, but what AI should do: towards a framework of task delegability. *Proceedings of the 33rd International Conference on Neural Information Processing Systems*.

- Magesh, V., Surani, F., Dahl, M., Suzgun, M., Manning, C. D., & Ho, D. E. (2024). Hallucination-free? assessing the reliability of leading ai legal research tools. *arXiv preprint arXiv:2405.20362*.
- Maleki, N., Padmanabhan, B., & Dutta, K. (2024). AI Hallucinations: A Misnomer Worth Clarifying. *2024 IEEE Conference on Artificial Intelligence (CAI)*, 133–138. <https://doi.org/10.1109/CAI59869.2024.00033>
- Malmqvist, L. (2024). Sycophancy in Large Language Models: Causes and Mitigations. *arXiv preprint arXiv:2411.15287*.
- Mavi, J., Summers, N., & Coronado, S. (2024). Assessing the Performance of Human-Capable LLMs—Are LLMs Coming for Your Job? *arXiv preprint arXiv:2410.16285*.
- Muller, M., Weisz, J. D., Houde, S., & Ross, S. I. (2024). Drinking Chai with Your (AI) Programming Partner: Value Tensions in the Tokenization of Future Human-AI Collaborative Work. *Proceedings of the 3rd Annual Meeting of the Symposium on Human-Computer Interaction for Work*. <https://doi.org/10.1145/3663384.3663390>
- Popescu, A.-R., & Schut, A. (2023). Generative AI in creative design processes: A dive into possible cognitive biases. *IASDR 2023: Life-Changing Design*. <https://doi.org/10.21606/iasdr.2023.784>
- Sambasivan, N., & Veeraraghavan, R. (2022). The Deskilling of Domain Expertise in AI Development. *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. <https://doi.org/10.1145/3491102.3517578>
- Sharma, M., Tong, M., Korbak, T., Duvenaud, D., Askill, A., Bowman, S. R., Cheng, N., Durmus, E., Hatfield-Dodds, Z., Johnston, S. R., et al. (2023). Towards understanding sycophancy in language models. *arXiv preprint arXiv:2310.13548*.
- White, J., Fu, Q., Hays, S., Sandborn, M., Olea, C., Gilbert, H., Elnashar, A., Spencer-Smith, J., & Schmidt, D. C. (2023). A Prompt Pattern Catalog to Enhance Prompt Engineering with ChatGPT. <http://arxiv.org/pdf/2302.11382v1>
- Woodruff, A., Shelby, R., Kelley, P. G., Rousso-Schindler, S., Smith-Loud, J., & Wilcox, L. (2024). How Knowledge Workers Think Generative AI Will (Not) Transform Their Industries. *Proceedings of the CHI Conference on Human Factors in Computing Systems*. <https://doi.org/10.1145/3613904.3642700>
- Yin, Z., Wang, H., Horio, K., Kawahara, D., & Sekine, S. (2024). Should We Respect LLMs? A Cross-Lingual Study on the Influence of Prompt Politeness on LLM Performance. *Proceedings of the Second Workshop on Social Influence in Conversations (SICoN 2024)*, 9–35. <https://doi.org/10.18653/v1/2024.sicon-1.2>

A. Anhang

B. Anwendungsbeispiele

Die folgenden Anwendungsbeispiele bieten einen Überblick über verschiedene alltägliche Aufgabenstellungen, die mithilfe von LLMs gelöst werden können. Die Mehrheit der Beispiele bezieht sich auf einen fiktiven Betrieb unter dem Namen „Bio Bündl“. Hintergrundinformationen sowie alle weiteren relevanten Ressourcen für die Anwendungsbeispiele können unter folgendem Link abgerufen werden: <https://repository.tugraz.at/doi/10.3217/5e1ek-qft39>. Jedes Anwendungsbeispiel umfasst eine Einführung, eine Beschreibung der Aufgabenstellung und eine Übersicht der notwendigen Schritte zur Lösung der Aufgabe. Abschließend wird jeweils ein Muster-Prompt angegeben, mit dem die Aufgabe gelöst werden kann.

B.1. Vorbereitung eines Meetings

In diesem Beispiel wird die Planung und Vorbereitung eines Meetings mithilfe eines LLMs trainiert. Für dieses Beispiel benötigen Sie nur einen einfachen LLM-Chatbot wie etwa ChatGPT (kostenlose Version) oder Copilot. Das Beispiel benötigt keine zahlungspflichtige Chatbot-Lizenz.

Aufgabenbeschreibung

Sie sind Mitarbeiter:in der Firma BioBündl und haben den Vorschlag eine Kooperation mit einem anderen lokalem Bio-Bauernhof einzugehen, welcher Bio-Milchprodukte produziert. Die Idee ist in Zukunft auch Kisten mit Obst, Gemüse und Milchprodukten anzubieten. Dazu wollen Sie ein Meeting ansetzen, um das ihren Vorgesetzten (Maria und Stefan Bündl) und einer Kollegin in aus dem Vertrieb zu präsentieren und nach ihrem Input und Feedback zu der Idee zu fragen.

Aufgabenstellung

- Lassen Sie sich eine Meeting Agenda erstellen.
 - Beschreiben Sie, was in dem Meeting besprochen werden soll.
 - Geben Sie die Gesamtdauer des Meetings an.
- Lassen Sie sich ein Handout für die Anwesenden im Meeting erstellen.
 - Beschreiben Sie, was in dem Handout enthalten sein soll.
 - Beschreiben Sie, wie das Handout strukturiert sein soll.
 - * Am Anfang eine kurze Zusammenfassung in 2 Sätzen.
 - * Eine Übersicht über den Bio-Bauernhof und welche Produkte dieser anbietet.
 - * Eine Übersicht um was genau die Bio-Boxen ergänzt werden sollen.
 - * Einen vorgeschlagenen Zeitplan für die Implementierung.

Muster-Prompt

1. Meeting-Agenda erstellen

Erstelle eine professionelle Meeting-Agenda für ein Meeting mit den Vorgesetzten Maria und Stefan Bündl sowie einer Kollegin aus dem Vertrieb. Ziel des Meetings ist es, den Vorschlag einer Kooperation mit einem lokalen Bio-Bauernhof zu präsentieren, der Bio-Milchprodukte produziert. Das Meeting soll insgesamt maximal 1 Stunde dauern. Es soll besprochen werden, wie das Sortiment von BioBündl zukünftig durch Kisten mit Obst, Gemüse und Milchprodukten erweitert werden kann. Die Agenda soll übersichtlich strukturiert und klar formatiert sein.

2. Handout erstellen

Erstelle ein Handout für die Anwesenden des Meetings, das die wichtigsten Informationen zusammenfasst. Wenn du zu Punkten keine Informationen hast, dann schreibe an diese Stelle einen Platzhalter in eckige Klammern und gib ein Stichwort an, was an dieser Stelle stehen soll (z.B. [Stichwort]). Das Handout soll folgende Struktur haben:

- a) Kurzfassung mit max. 2 Sätzen, welche die Idee vorstellt eine Kooperation mit einem Bio-Bauernhof zur Erweiterung des Sortiments um Milchprodukte einzugehen.
- b) Informationen zum Bio-Bauernhof. Dies soll eine Kurzvorstellung des Hofes, seine Philosophie und nachhaltige Produktion beinhalten.
- c) Auflistung welche Produkte der Bio-Bauernhof produziert.
- d) Auflistung der neuen Produkte, die in die bestehenden Kisten integriert werden sollen.
- e) Zeitplan für die Umsetzung der Kooperation

B.2. E-Mail generieren

In diesem Beispiel wird das Verfassen einer E-Mail mithilfe eines LLMs trainiert. Für dieses Beispiel benötigen Sie nur einen einfachen LLM-Chatbot wie etwa ChatGPT (kostenlose Version) oder Copilot. Das Beispiel benötigt keine zahlungspflichtige Chatbot-Lizenz.

Aufgabenbeschreibung

Sie sind Mitarbeiter:in der Firma BioBündl und wollen eine Kooperation mit einem anderen lokalem Bio-Bauernhof eingehen, welcher Bio-Milchprodukte produziert. Um direktes Feedback zu der Idee von Kund:innen zu bekommen, schreiben Sie einem Kunden, welcher lange schon bei BioBündl bestellt und der immer interessiert ist an neuen Ideen, eine E-Mail mit der Frage, ob dieser an einer Erweiterung um Bio-Milchprodukte interessiert wäre.

Aufgabenstellung

Lassen Sie eine E-Mail an den Kunden erstellen.

- Beschreiben Sie, was alles in der E-Mail enthalten sein soll.

- Geben Sie an, dass in der E-Mail ein Hinweis hinzugefügt werden soll, dass die E-Mail mit KI-Unterstützung erstellt wurde.
- Geben Sie Informationen zu der Länge der E-Mail an.
- Beschreiben Sie an wen die E-Mail geschrieben werden soll und in welchem Ton (z.B. förmlich, privat, kollegial) die E-Mail verfasst sein soll.
- Lassen Sie sich auch einen passenden Betreff ausgeben.

Muster-Prompt

Schreibe eine freundliche, kompakte und übersichtliche E-Mail an einen langjährigen Kunden, der regelmäßig bei BioBündl bestellt und immer interessiert an neuen Ideen ist. Bitte den Kunden um Feedback und Input zu meiner Idee, das Sortiment durch eine Kooperation mit einem lokalen Bio-Bauernhof zu erweitern, der Bio-Milchprodukte herstellt. Ziel ist es, künftig Kisten mit Obst, Gemüse und Milchprodukten anzubieten. Die E-Mail soll in einem höflichen und wertschätzenden Ton gehalten sein und in der „Sie“-Form formuliert werden. Am Ende nach der Verabschiedung soll der Hinweis enthalten sein, dass die E-Mail mit Unterstützung durch KI erstellt wurde. Außerdem soll zur E-Mail ein prägnanter Betreff mit maximal 4 Wörtern generiert werden.

B.3. Datenaufbereitung und -visualisierung

In diesem Beispiel wird das Aufbereiten, Zusammenfassen und Visualisieren von Daten mithilfe eines LLMs trainiert. Für dieses Beispiel benötigen Sie einen LLM-Chatbot, in welchem Dokumente hochgeladen werden können und Daten im PDF- und Excel-Format ein- und ausgelesen werden können und Diagramme erstellt werden können, wie z.B. ChatGPT Plus.

Aufgabenbeschreibung

Die Firma BioBündl benötigt für den Versand ihrer Biokisten eine neue Bestellung Lieferkisten aus Holz. Die Firma hat sich eine Reihe von Angeboten eingeholt und möchte nun auch das neueste Angebot in ihre Übersicht mitaufnehmen und die Angebote vergleichen.

Aufgabenstellung

1. Fügen Sie das Angebot der Firma „KistenBoss“ in die Übersichtstabelle der Angebote hinzu und lassen Sie sich die aktualisierte Angebotstabelle ausgeben.
2. Fügen Sie eine neue Spalte „Stückpreis Brutto“ hinzu und lassen sie sich die aktualisierte Angebotstabelle ausgeben.
3. Berechnen Sie die Preisspanne vom geringsten bis zum höchsten Bruttostückwert (für Angebote mit Stückzahl 100) und finden Sie heraus, welche Firma das billigste und welche das teuerste Angebot gemacht hat.
4. Lassen Sie sich den Mittelwert der Bruttostückpreise (Angebote mit Stückzahl 100) ausgeben.

5. Erstellen Sie ein Tortendiagramm, das die Anzahl der Angebote pro Holzsorte visualisiert. Bestimmen Sie dabei, welche Holzsorte mit welcher Farbe eingefärbt werden soll.
6. Erstellen Sie ein Säulendiagramm, das die Mittelwerte pro Holzsorte visualisiert. Behalten Sie dabei Ihre Farbgebung von Schritt 5 bei.
7. Erstellen Sie nun ein weiteres Säulendiagramm, das jeweils das billigste Angebote pro Holzsorte visualisiert. Behalten Sie dabei Ihre Farbgebung von Schritt 5 und 6 bei.

Muster-Prompt

1. Ergänze das Angebotsdokument `AngebotslisteHolzkisten.xlsx` um ein neues Angebot der Firma „KistenBoss“ (`AngebotHolzkisteFirmaKistenBoss.pdf`) mit den entsprechenden Spaltenwerten. Zeige die aktualisierte Tabelle an. Berechne in der aktualisierten Tabelle den Bruttostückpreis für jede Zeile anhand der angegebenen Nettopreise (unter Annahme einer Mehrwertsteuer von 20 %). Füge die berechneten Werte als neue Spalte hinzu und zeige die aktualisierte Tabelle an.
2. Gib die aktualisierte Tabelle als `AngebotslisteHolzkistenaktualisiert.xlsx` zum Download aus.
3. Ermittle anhand der aktualisierten Tabelle den günstigsten und teuersten Bruttostückpreis für Angebote mit einer Stückzahl von genau 100. Gib an, welche Firma das billigste und welche das teuerste Angebot gemacht hat.
4. Berechne den Durchschnitt der Bruttostückpreise für Angebote mit einer Stückzahl von 100.
5. Erstelle ein Tortendiagramm, das die Anzahl der Angebote pro Holzsorte mit Stückzahl 100 visualisiert. Bestimme eine feste Farbzuteilung für jede Holzsorte und verwende diese konsequent in allen weiteren Diagrammen.
6. Berechne den durchschnittlichen Bruttostückpreis pro Holzsorte (Stückzahl 100). Stelle diese Werte als Säulendiagramm dar, wobei die Farbzuteilung aus Schritt 5 beibehalten wird.
7. Bestimme für jede Holzsorte das günstigste Brutto-Angebot (Stückzahl 100). Stelle diese Werte in einem weiteren Säulendiagramm mit der gleichen Farbgebung wie in den vorherigen Schritten dar.

B.4. Werbebeiträge und Social Media Post erstellen

In diesem Beispiel wird das Generieren von Werbebeiträgen und die auf Zielgruppe und Werbemedium abgestimmte Gestaltung von Beiträgen mithilfe eines LLMs trainiert. Für dieses Beispiel benötigen Sie einen LLM-Chatbot, in welchem Dokumente hochgeladen werden können und Bilder generiert werden können, wie z.B. ChatGPT Plus oder Mistral.

Aufgabenbeschreibung

Die Firma BioBündl möchte zielgruppengerechte Werbebeiträge auf verschiedenen Plattformen schalten. Um Familien und ältere Menschen aus der Region anzusprechen, soll ein Beitrag fürs Gemeindeblatt gestaltet werden. Um Berufstätige anzusprechen, möchte die Firma auch einen LinkedIn Beitrag gestalten. Um schließlich gesundheitsbewusste, junge Menschen zu erreichen, soll ein Instagram Beitrag erstellt werden.

Aufgabenstellung

1. Statten Sie die KI mit dem Dokument „Firmeninformationen“ aus.
2. Lassen Sie sich zuerst den Newsletter Beitrag generieren.
 - Geben Sie der KI dazu Hinweise auf die Zielgruppe, die angesprochen werden soll (Familien, ältere Menschen)
 - Legen Sie ein passendes Wortlimit fest (z.B. maximal 300 Wörter).
 - Beschreiben Sie, welche Wirkung der Beitrag auf die Leser:innen haben soll (z.B. sympathisch, familiär, regional).
3. Legen Sie ein passendes Wortlimit fest (z.B. maximal 300 Wörter).
4. Beschreiben Sie, welche Wirkung der Beitrag auf die Leser:innen haben soll (z.B. sympathisch, familiär, regional).
5. Checken und bearbeiten Sie den Beitrag, mit Unterstützung durch die KI, bis Sie damit zufrieden sind. Lassen Sie sich den fertigen Beitrag als Word Dokument (Endung .docx) ausgeben.
6. Wiederholen Sie Schritt 2 und 3 für das LinkedIn und Instagram Posting – auch diese sollen zielgruppenorientiert und in passender Länge sein.
7. Lassen Sie sich für das Instagram Posting ein Bild generieren, dass gemeinsam mit dem Beitrag hochgeladen werden soll. **Tipp zur Bildgenerierung:** Zuerst einen eigenen, möglichst genauen Prompt schreiben (vermeiden Sie Text und Symbole). Diesen Prompt dann von der KI zum Zweck der Bildgenerierung überarbeiten lassen. Anhand dieses Prompts dann das Bild generieren lassen.

Muster-Prompt

1. Erstelle auf Basis des Dokumentes "Firmeninformationen.docx" Werbebeiträge, und berücksichtige folgende Aspekte. Frage mich nach der Erstellung jedes Beitrages nach Feedback. Wenn ich zufrieden bin, gib mir den Beitrag als Word-Dokument (.docx) aus.
 - a) Newsletter Beitrag im Gemeindeblatt.
 - Zielgruppe: Familien, ältere Menschen
 - Länge: maximal 300 Wörter
 - Wirkung: sympathisch, familiär, regional
 - b) LinkedIn-Post

- Zielgruppe: Unternehmer:innen, arbeitende Menschen
 - Länge: maximal 100 Wörter
 - Wirkung: professionell, inspirierend, kompetent
- c) Instagram-Post
- Zielgruppe: junge Erwachsene, Lifestyle-orientierte Menschen
 - Länge: maximal 50 Wörter
 - Wirkung: modern, jung, community-orientiert
2. Generiere mir jetzt für den Instagram Post ein passendes Bild. Schreibe zuerst selbst einen Prompt für die Bildgenerierung. Dann lass mich Feedback geben. Dann generiere basierend auf dem von mir absegneten Prompt das Bild und gib es mir als „InstagramBild.png“ aus.

B.5. Zielgruppenanalyse

In diesem Beispiel wird die Recherche von Zielgruppen und die Aufbereitung der Recherche in Form einer Präsentation mithilfe eines LLMs trainiert. Für dieses Beispiel benötigen Sie einen LLM-Chatbot, in welchem Dokumente hochgeladen werden können, Bilder generiert werden können und Präsentationen im PowerPoint Format erstellt werden können, wie z.B. ChatGPT Plus.

Aufgabenbeschreibung

Die Biokisten-Lieferservice Firma BioBündl möchte neue Zielgruppen identifizieren und ansprechen. Dafür wurde ein Mitarbeiter beauftragt, eine Zielgruppenanalyse durchzuführen und eine 5-Minütige Präsentation zu den Ergebnissen zu halten.

Aufgabenstellung

1. Laden Sie die Daten „Firmeninformationen“ und „BioBündl“ bei der KI hoch.
2. Instruieren Sie die KI, aus dem Dokument „Firmeninformation“ die bestehenden Zielgruppen zu identifizieren.
3. Beauftragen Sie die KI, drei weitere, neue Zielgruppen für die Firma zu identifizieren.
4. Lassen Sie für jede Zielgruppe eine Persona (=Profil einer fiktiven Person, die die Zielgruppe identifiziert) erstellen. Dieses sollte folgende Informationen enthalten:
 - Name
 - Alter
 - Geschlecht
 - Wohnort
 - Beruf
 - Familienstand
 - Problemlösung (Welches Problem der Person kann BioBündl lösen?)

- Marketing (Mit welcher Werbestrategie kann BioBündl diese Person am besten erreichen?)

Tipp:

- Begrenzen Sie die Länge der Zusammenfassung, z.B. auf 4 Sätze.
- Instruieren Sie die KI, einfache, gut verständliche Sprache zu verwenden.
- „Erkläre es so, wie du es einem 15-jährigen Kind erklären würdest.“

5. Lassen Sie nun für jede Persona ein „Profilbild“ generieren.

Muster-Prompt

1. Erstelle eine umfassende Zielgruppenanalyse für die Firma BioBündl anhand der folgenden Schritte:
2. **Analyse der bestehenden Zielgruppen:** Öffne das Dokument "Firmeninformationen.pdf" und identifiziere alle bereits definierten Zielgruppen von BioBündl. Erstelle eine kurze, prägnante Liste mit diesen Zielgruppen.
3. **Entwicklung neuer Zielgruppen:** Überlege drei neue, noch nicht angesprochene Zielgruppen, die für BioBündl relevant sein könnten. Beschreibe jede neue Zielgruppe in 1-2 Sätzen, indem du ihren Bedarf an BioBündl-Produkten begründest.
4. **Erstellung von Personas für die neuen Zielgruppen:** Für jede neu definierte Zielgruppe entwickle eine detaillierte Persona mit folgenden Informationen:
 - name
 - Alter
 - Geschlecht
 - Wohnort
 - Beruf
 - Familienstand
 - Problemlösung (Welches Problem der Person kann BioBündl lösen?)
 - Marketingstrategie (Wie kann BioBündl diese Person am effektivsten erreichen?)
5. **Generierung passender Profilbilder:** Erstelle für jede Persona ein realistisches und repräsentatives Profilbild.

B.6. Zusammenfassen und Verstehen von Texten

In diesem Beispiel wird die Informationssuche und Textzusammenfassung mithilfe eines LLMs trainiert. Für dieses Beispiel benötigen Sie einen LLM-Chatbot, in welchem Dokumente hochgeladen und ausgelesen werden können, wie z.B. ChatGPT Plus oder Mistral.

Aufgabenbeschreibung

Der AI Act der Europäischen Union sorgt oftmals für Besorgnis und Verwirrung. Verschaffen Sie sich mithilfe von KI besseren Einblick.

Aufgabenstellung

1. Laden Sie die Daten „AIActDeutschVollversion“ und „AIActEnglischHighLevelSummary“ bei der KI hoch und instruieren Sie die KI, alle folgenden Fragen anhand dieser Dokumente zu beantworten.
2. Lassen Sie sich zuerst eine kurze, simple Zusammenfassung von der KI geben.

Tipp:

- Begrenzen Sie die Länge der Zusammenfassung, z.B. auf 4 Sätze.
 - Instruieren Sie die KI, einfache, gut verständliche Sprache zu verwenden.
 - „Erkläre es so, wie du es einem 15-jährigen Kind erklären würdest.“
3. Finden Sie heraus, was die vier Risikostufen von KI sind, die der AI Act unterscheidet und welche Pflichten KI-Anbietende und KI-Nutzende je nach Risikostufe haben.
 4. Im Dokument „QuizAIAct“ finden Sie verschiedene Beispielfälle, die vom AI Act in unterschiedlicher Weise betroffen sind. Finden Sie, gemeinsam mit der KI heraus, mit welcher Risikostufe diese Fälle zu beurteilen sind, und welche Schritte sich dementsprechend für die Beispielfirmen ergeben.
 - Instruieren Sie die KI dabei, direkt aus dem AI Act oder dem AI Act Summary zu zitieren, um die Einschätzung des Risikos und die daraus folgenden Schritte zu validieren.
 - Kontrollieren Sie stichprobenartig auch selbst nach, ob diese Passagen tatsächlich im Dokument vorhanden sind.

Hinweis: Zur Kontrolle Ihrer Antworten können Sie das Dokument „QuizAIActLösungen“ heranziehen.

Muster-Prompt

1. Beantworte alle folgenden Fragen und Aufträge anhand dieser Dokumente:
„AIActDeutschVollversion.pdf“ und „AIActEnglischHighLevelSummary.pdf“.
2. Gib mir eine kurze Zusammenfassung über den AI Act. Erkläre es mir so, wie du es einem 16-jährigen Schüler erklären würdest.
3. Erkläre mir kurz und in einfacher Sprache:
 - Welche vier Risikostufen werden im AI Act unterschieden?
 - Welche Pflichten ergeben sich für KI-EntwicklerInnen, je nach den vier Risikostufe?
 - Welche Pflichten ergeben sich für KI-AnwenderInnen, je nach den vier Risikostufe?
4. Beantworte jetzt dieses Quiz zum AI Act. Antworte prägnant, aber vollständig. Überprüfe dann deine Antwort mit den Dokumente „AIActDeutschVollversion.pdf“ und „AIActEnglischHighLevelSummary.pdf“. Wenn ein Beispiel unklar ist (z.B. hinsichtlich der Transparenzpflicht), merke dies an. Zitiere für jedes Beispiel die genauen Stellen in den Dokumenten an, welche deine Antwort belegen.

5. Prüfe mich nun im gleichen Schema wie das Quiz mit 5 weiteren Frage an. Stelle dabei immer eine Frage. Warte dann meine Antwort ab. Evaluiere dann meine Antwort basierend auf den Dokumenten und stelle dann die nächste Frage. Gib mir am Ende eine Gesamtbewertung.

B.7. Ideengenerierung und Planung eines Events

In diesem Beispiel wird die Ideenfindung und Planung einer Veranstaltung mithilfe eines LLMs trainiert. Für dieses Beispiel benötigen Sie nur einen einfachen LLM-Chatbot wie etwa ChatGPT (kostenlose Version) oder Copilot. Das Beispiel benötigt keine zahlungspflichtige Chatbot-Lizenz.

Aufgabenbeschreibung

Die Firma BioBündl möchte ein Teambuilding Event für alle 7 Mitarbeitenden planen. Da einige neu dazugekommen sind kennt sich das Team unterschiedlich gut. Die Mitarbeitenden sind zwischen 20 und 42 Jahren alt und vielseitig interessiert. Das Ziel des Events ist es den Teamzusammenhalt zu stärken.

Aufgabenstellung

1. Finden Sie heraus welche Aspekte relevant sind, um ein Teambuilding Event zu planen.
2. Lassen Sie sich Vorschläge zu Teambuildingmaßnahmen geben.
 - Geben Sie alle relevanten Informationen basierend auf den vorher herausgefundenen Aspekten an.
 - Lassen Sie sich zusätzlich eine Erklärung zu den jeweiligen Vorschlägen geben, warum diese eine geeignete Teambuildingmaßnahmen sind.
 - Geben Sie an wie viele Ideen generiert werden sollen und dass diese möglichst unterschiedlich sein sollen.
3. Wählen Sie einen der Vorschläge aus und lassen Sie sich einen Plan für das Event erstellen, der die Aktivität(en) beschreibt und auch einen Ablaufplan enthält.
4. Lassen Sie sich eine To Do Liste ausgeben, was alles bis zu dem Event zu erledigen ist mit Hinweisen, bis wann dies erledigt sein sollte.

Muster-Prompt

1. Ich möchte für die Firma BioBündl ein Teambuilding Event für alle 7 Mitarbeitenden planen. Da einige neu dazugekommen sind kennt sich das Team unterschiedlich gut. Die Mitarbeitenden sind zwischen 20 und 42 Jahren alt und vielseitig interessiert. Das Ziel des Events ist es den Teamzusammenhalt zu stärken. Was muss ich alles berücksichtigen, um das Event zu planen?
2. Entwickle 3 kreative und möglichst unterschiedliche Ideen für ein Teambuilding-Event, das den Teamzusammenhalt stärkt. Beachte dabei folgende Rahmenbedingungen:
 - Ziel: Der Fokus liegt darauf, den Teamzusammenhalt zu fördern und eine entspannte, angenehme Atmosphäre zu schaffen.

- Teilnehmerbedürfnisse: Die Aktivitäten sollten weder zu aktiv noch kompetitiv sein, damit sich alle wohlfühlen.
- Ort: Der Veranstaltungsort sollte entweder in der Nähe von Lieboch oder Graz sein oder auf unserem Bio-Hof stattfinden können.
- Budget: Das maximale Budget beträgt 300€.

Erkläre bei jeder Idee, warum sie für eine Teambuilding-Maßnahme geeignet ist und wie sie konkret zum Ziel des besseren Teamzusammenhalts beiträgt.

3. Erstelle einen detaillierten Plan für die Teambuilding-Idee 'Escape Game: Nachhaltigkeit und Bio-Themen'.
 - Entwickle Aktivitäten basierend auf dem Vorschlag. Die Aufgaben sollen Rätsel, Teamaufgaben und kreative Elemente enthalten, die die Teilnehmenden dazu anregen, zusammenzuarbeiten.
 - Erstelle einen Ablaufplan: Gliedere die Aktivitäten in klar definierte Phasen (z. B. Einführung, Hauptspiel, Auflösung, Abschluss). Gib für jede Phase genaue Beschreibungen der Aufgaben und Aktivitäten. Lege Zeitrahmen für die einzelnen Phasen fest, sodass die Gesamtdauer etwa 3-4 Stunden beträgt.
 - Berücksichtigung der bereits genannten Rahmenbedingungen.
 - Erstelle eine Liste der benötigten Materialien und skizziere grob die Kosten, um sicherzustellen, dass das Budget eingehalten wird.
4. Erstelle eine detaillierte To-Do-Liste auf Basis des Plans.
 - Aufgabenidentifikation: Liste alle erforderlichen Schritte auf, um das Event erfolgreich umzusetzen.
 - Priorisierung und Deadlines: Ordne den Aufgaben klare Fristen zu, die sicherstellen, dass das Event termingerecht vorbereitet wird.
 - Zeitrahmen: Der Plan sollte davon ausgehen, dass das Event am 28.03.2025 stattfinden. Passe die Deadlines entsprechend an.

B.8. Simulieren eines Mitarbeitendengesprächs

In diesem Beispiel wird Simulation einer sozialen Situation (Konfliktsituation) mithilfe eines LLMs trainiert. Wenn Sie die Situation rein via Text simulieren möchten, benötigen Sie dafür lediglich einfachen LLM-Chatbot wie etwa ChatGPT (kostenlose Version) oder Copilot. Wenn Sie die Situation via Audio simulieren möchten, benötigen Sie dafür einen LLM-Chatbot mit Audiofunktion, wie etwa ChatGPT-4 Plus.

Aufgabenbeschreibung

Ein:e Mitarbeiter:in kommt regelmäßig deutlich zu spät zu der Arbeit. Sie sind sein:ihr Vorgesetzte:r und wollen die Person darauf ansprechen. Jedoch tun Sie sich in solchen Situation schwer und wissen nicht genau wie sie dies am besten machen. Daher beschließen Sie diese Situation vorher mit ChatGPT zu üben. Das Ziel des Gespräches mit dem:der Mitarbeiter:in ist es herauszufinden warum die Person zu spät kommt und wie man gemeinsam daran arbeiten kann, dass dies nicht weiter vorkommt. In der Übungssituation mit ChatGPT wollen Sie außerdem noch Feedback erhalten zu Ihrer Herangehensweise.

Aufgabenstellung

1. Beschreiben sie in Ihrem Prompt folgendes:
 - Was der Kontext der Aufgabe ist
 - Welche Rolle der Chatbot übernimmt
 - Wie sich der Chatbot verhalten soll
 - Ab wann Sie Feedback bekommen möchten (z.B. Nach 5 Gesprächswechseln)
 - Was das Feedback enthalten soll
2. Starten Sie nun die Interaktion mit ChatGPT und simulieren Sie das Gespräch mit dem:der Mitarbeiter:in. Dies können Sie entweder per Text machen oder Sie können auch gerne die Sprachfunktion austesten, um das Gespräch realistischer zu simulieren.

Muster-Prompt

Kontext: Ein:e Mitarbeiter:in kommt regelmäßig deutlich zu spät zu der Arbeit. Der User ist sein:ihr Vorgesetzte:r und will die Person darauf ansprechen. Jedoch fallen dem User solche Situationen schwer und dieser weiß nicht genau wie man das am besten anspricht.

Aufgabe: Du bist der:die Mitarbeiter:in, welcher immer zu spät kommt. Der User ist der Vorgesetzte. Simuliere das Gespräch aus der Rolle des Mitarbeitenden. Verwende die „Sie“ Form gegenüber dem User. Für den User ist es das Ziel des Gespräches mit dem Mitarbeitenden herauszufinden, warum die Person zu spät kommt und wie man gemeinsam daran arbeiten kann, dass dies nicht weiter vorkommt.

Nach fünf Wechseln danke dem User für das Gespräch und kündige an, dass er jetzt von dir als Tutor Feedback bekommt. Gib dem User dann kompaktes, aber konstruktives Feedback zu dem Gespräch und der Herangehensweise und was er das nächste Mal in so einer Situation verbessern kann.

C. Prompt-Sammlungen

Die folgenden Links führen zu verschiedenen Prompt-Sammlungen. Diese beinhalten Prompts für verschiedenste Aufgaben.

Allgemeine Prompt-Sammlung : <https://prompts.chat/>

Prompt-Sammlung spezifisch für den Lehrkontext und administrative Tätigkeiten: <https://www.aiforeducation.io/prompt-library>

Prompt-Sammlung mit Fokus auf Marketing: <https://hero.page/discover>

Prompt-Sammlung von Google AI Studios: <https://aistudio.google.com/app/gallery>

Prompt-Sammlung von OpenAI: <https://platform.openai.com/docs/examples>

Prompt-Sammlung von Anthropic: <https://docs.anthropic.com/en/prompt-library/library>

D. Weitere Ressourcen

Ressourcen zu Prompt Engineering:

- Handbuch zu Prompt Engineering: <https://www.promptingguide.ai/de>

- Hinweise von OpenAI zu Prompt Engineering: <https://platform.openai.com/docs/guides/prompt-engineering#six-strategies-for-getting-better-results>
- Die System-Prompts hinter den Claude Chatbots: <https://docs.anthropic.com/de/release-notes/system-prompts#feb-24th-2025>

Ressourcen, um KI und LLMs besser zu verstehen:

- Podcast zum Thema KI: <https://www.deutschlandfunk.de/ki-verstehen-102.html>
- Kostenfreier Online-Kurs zum Thema KI: <https://ki-campus.org/>
- Detaillierte und simple Erklärung, wie LLMs funktionieren (in Englisch): <https://arstechnica.com/science/2023/07/a-jargon-free-explanation-of-how-ai-large-language-models-work/>
- Genauere Erklärung und Diskussion über die Art und Funktionsweise von LLMs: <https://doi.org/10.1145/3624724>
- Überblick über Anwendungen, welche LLMs verwenden: <https://www.evidentlyai.com/ml-system-design>

Ressourcen zum bewussten Umgang mit KI:

- KI Leitfaden für KMUs der WKO: <https://www.wko.at/oe/digitalisierung/kmu-ki-guidelines.pdf>
- NGO, die algorithmische Entscheidungsfindung analysiert: <https://algorithmwatch.org/>
- Vorlage für einen freiwilligen Verhaltenskodex zur ethischen Nutzung von KI: https://www.dih-sued.at/fileadmin/dih-sued/Dateien_Aktivitaeten/Vorlage_fuer_einen_freiwilligen_Verhaltenskodex_zur_ethischen_Nutzung_von_KI.docx

Ressourcen zum AI Act der Europäischen Union

- Genaue Zusammenfassung der Europäischen Union: <https://artificialintelligenceact.eu/de/high-level-summary/>
- Zusammenfassung von Digital Austria: <https://www.digitalaustria.gv.at/Themen/KI/AI-Act.html>
- Zusammenfassung der WKO: <https://www.wko.at/digitalisierung/ai-act-eu>
- Compliance Checker der EU, zur Überprüfung ob und wie man von AI Act betroffen ist: <https://artificialintelligenceact.eu/de/bewertung/eu-ai-act-compliance-checker/>
- AI Act Checkliste für KMUs der TU Graz und der DIH Süd: <https://survey.tugraz.at/index.php/218922?lang=de>