

Prompt Engineering: Warum KI den Menschen braucht

Computer sind nicht länger nur Zuhörer. Dank Technologien wie neuronalen Netzen, großen Sprachmodellen (LLM), maschinellem Lernen (ML) und der Verarbeitung natürlicher Sprache (NLP) antworten sie auch. Sie werden zu Assistenten, Autoren, Analysten, Trainern, Beratern oder Programmierern.

Der Einsatz der Technologie birgt allerdings zahlreiche Risiken. Trainingsdaten sind immer nur so vollständig, wie sie zur Verfügung stehen. Sie enthalten Verzerrungen und unerwünschte Inhalte oder sind voreingenommen. Unklare Instruktionen oder die Verwendung falscher Modelle führen zu ungenauen, fehlerhaften Ergebnissen. Die Verwendung eines ungeeigneten Modells liefert vielleicht nicht die gewünschten Ergebnisse.

Das Wichtigste: Bei aller menschlichen Anmutung sind Computer nach wie vor nur Maschinen; KI ist nur Mathematik. Sowohl das Training als auch die Anwendung von KI sind in hohem Maße auf menschliche Mitarbeit angewiesen. Eindeutige und präzise Informationen sind kritisch für eine zufriedenstellende Erledigung einer Aufgabe. Je mehr Informationen (Kontext) der KI zur Verfügung stehen, desto besser ist das Resultat. Dabei ist Vorsicht geboten: sensible Informationen sollten vermieden werden. Auch das Ergebnis muss kritisch betrachtet werden. KI hat keine interkulturelle Kompetenz. Sowohl Ton als auch Stil müssen ggf. der Zielgruppe angepasst werden. Im Code können sich Fehler aus Trainingsdaten wiederholen. Hier sind ein paar weitere Herausforderungen:

- Korrelation ist nicht zwingend Kausalität.
- Je nach Trainingsdaten ist eine KI mehr oder weniger voreingenommen (biased).
- KI neigt zur Halluzination.
- Urheberrechte könnten verletzt werden.

Auch das Lizenzrecht spielt eine Rolle. Zwar sind viele Modelle inzwischen Open Weight. Das macht sie aber noch lange nicht zu Open Source. Last not least kann KI mit den falschen Instruktionen selbst zur Schwachstelle werden und vertrauliche Informationen dem falschen Publikum preisgeben.

Im Vortrag werden Grundlagen zur Funktionsweise großer Sprachmodelle, damit verbundene Herausforderungen, entsprechende Sicherheitsmaßnahmen und bewährte Strategien z. B. im Prompt-Engineering für präzisere und relevantere Ergebnisse vorgestellt.

Der Vortrag richtet sich sowohl an Verantwortliche in Unternehmen, die den Einsatz von KI planen, als auch Anwender, die mehr über Prompt Engineering erfahren und ihre Technik verbessern wollen.

Es sind keine besonderen Vorkenntnisse nötig.