

Agentic AI

Vom Chatbot zum autonomen System

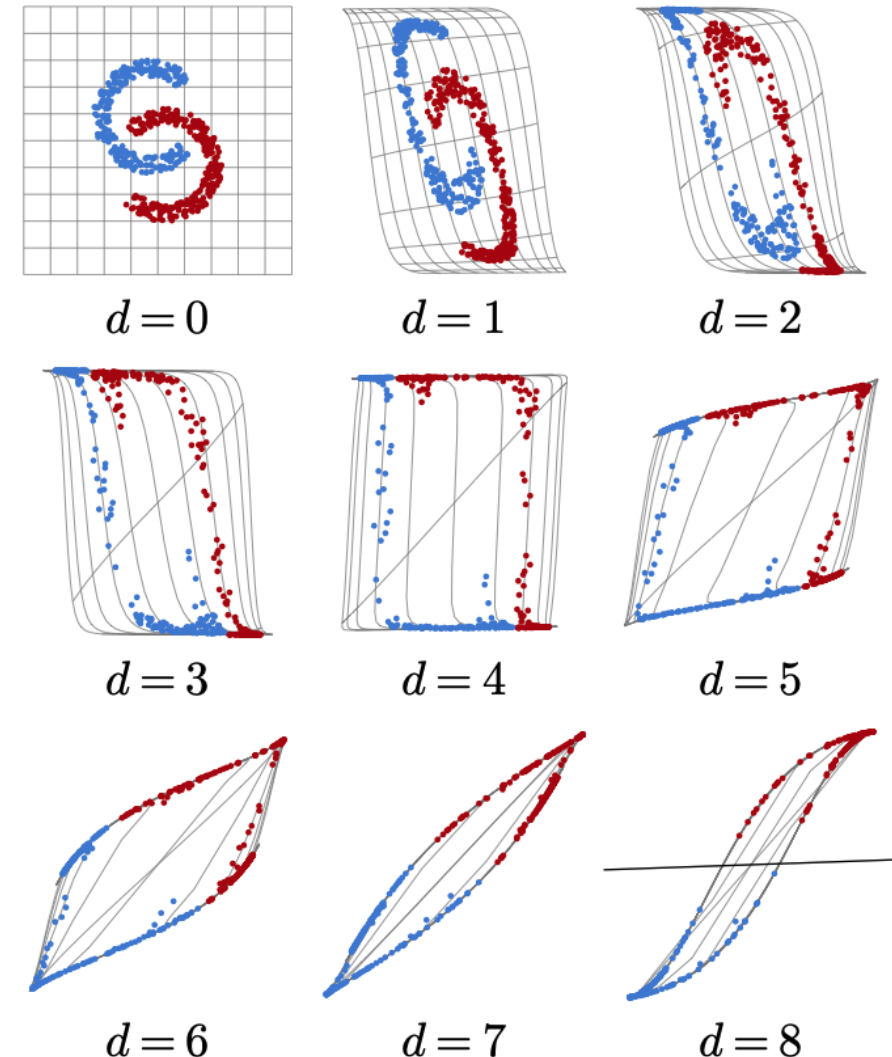
Von klassischem ML zu Deep Learning

Früher: **Feature Engineering**

- manuelle Merkmalsextraktion
- stark domänenspezifisch
- hoher Expertenaufwand

Deep Learning: **Feature Learning**

- Modelle lernen Repräsentationen selbst
- bessere Generalisierung



Von Single-Task-KI zu Foundation Models

Vom Spezialmodell zum universellen Modell

Früher:



Spamfilter



Übersetzung



Bildererkennung



Sprachverarbeitung



Heute:

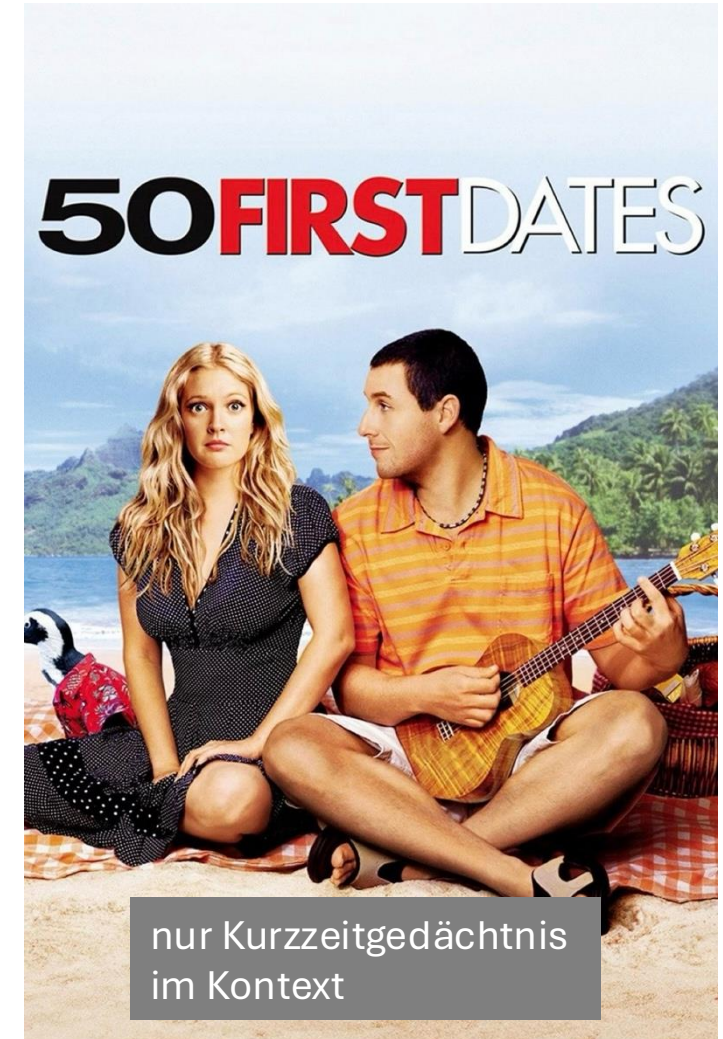


- Ein Modell
- Viele Aufgaben
- Prompting statt Retraining

Große Sprachmodelle werden zur universellen KI-Schnittstelle.



LLM: *Simulation eines Gelehrten mit kognitiven Einschränkungen*



von Karpathy

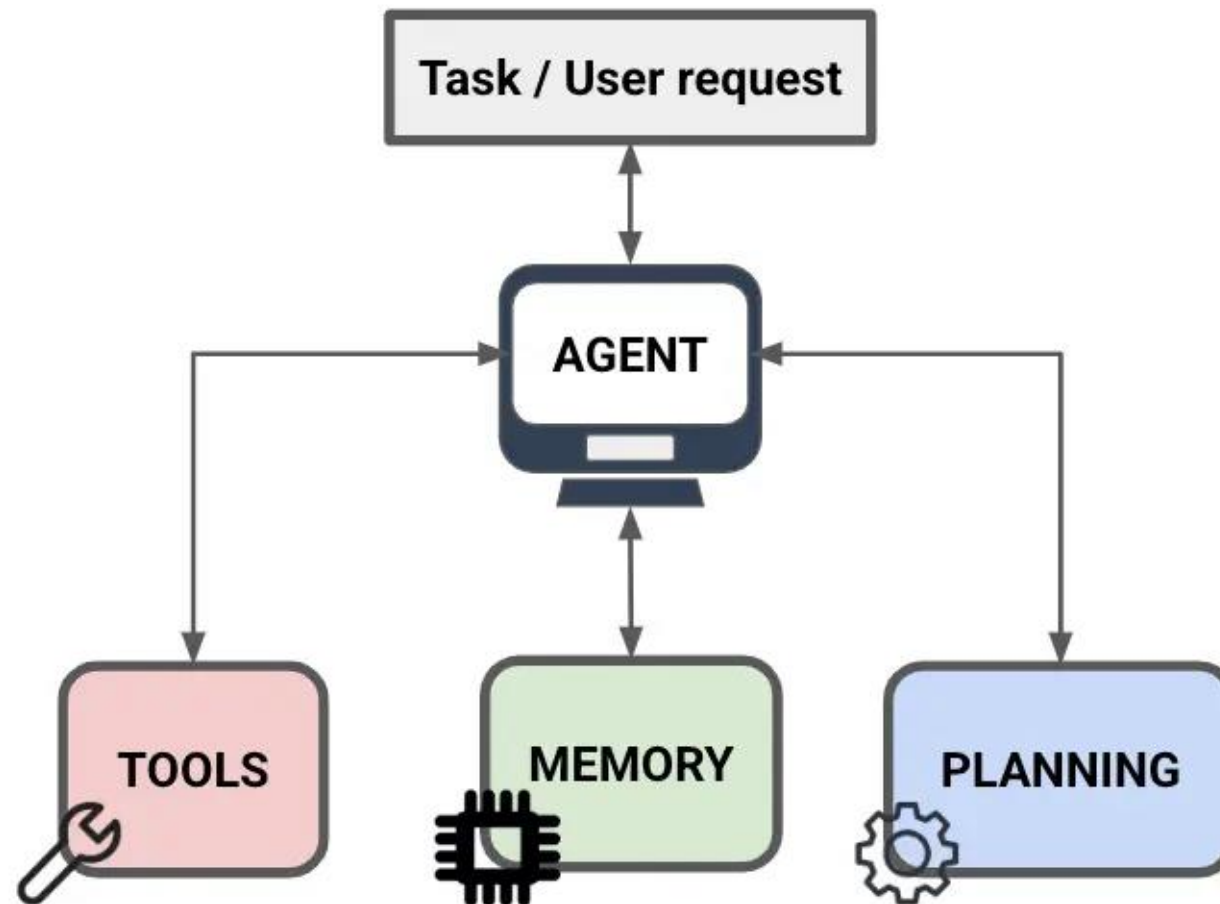
Warum reicht ein LLM allein nicht aus?

Ein LLM kann antworten, erklären und Inhalte erzeugen.

Ein LLM kann aber nicht handeln, planen und persistent arbeiten.

Intelligenz $\neq$ Autonomie

Agentic AI: Vom Denken zum Handeln



mittels Orchestrierung
von LLMs

Tools

Agenten können externe Systeme nutzen.

Beispiele:

- APIs
- Datenbanken
- Codeausführung
- Unternehmenssoftware

Anwendungen:

- SQL-Abfragen
- CRM aktualisieren
- E-Mails versenden
- Reports erzeugen

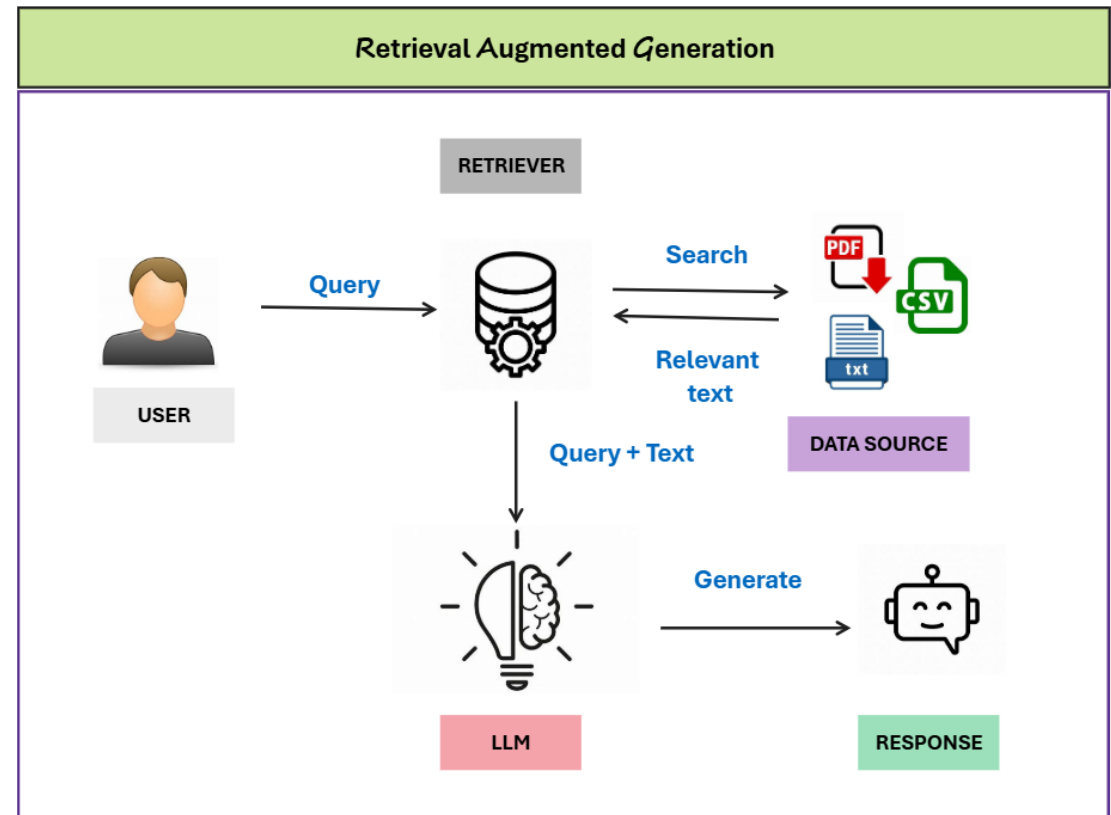
Memory

Modelle benötigen zusätzlichen Kontext:

- Unternehmenswissen
- aktuelle Daten
- Dokumente
- Nutzerinformationen

RAG ermöglicht:

- Wissenszugriff
- kontextbezogene Antworten
- erweiterte Informationsbasis



Planning

Agenten zerlegen Ziele in Arbeitsschritte.

„Erstelle eine Marktanalyse.“

1. Recherche
2. Datensammlung
3. Analyse
4. Visualisierung, Bericht

Eigenschaften:

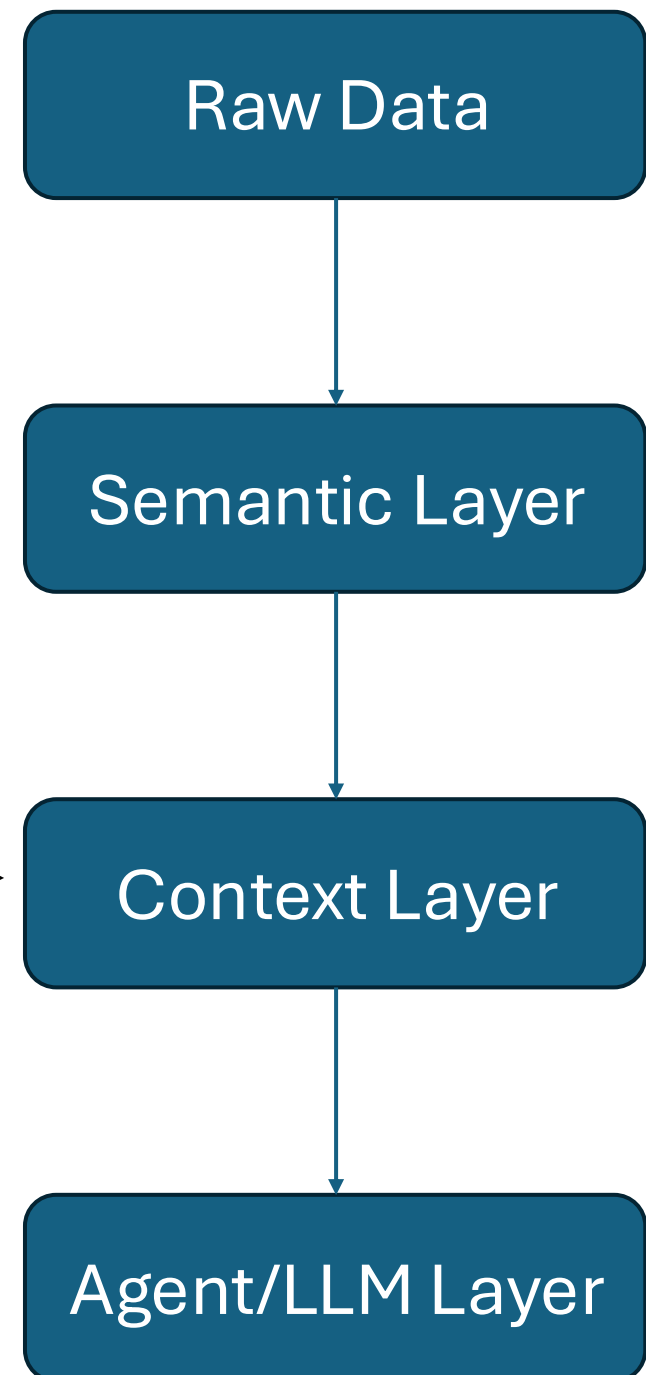
- mehrstufiges Denken
- Zielorientierung
- Aufgabenzerlegung

Nächste Evolutionsstufen

Computer Use: Agenten bedienen Benutzeroberflächen direkt.

Langzeitkontext und Personalisierung →

Selbstverbesserung



Automatisierung von Wissensarbeit

Softwareentwicklung

- Coding Assistants
- Debugging
- längere Entwicklungsprozesse

Forschung & Analyse

- Dokumentenauswertung
- Wettbewerbsanalyse
- Berichterstellung

Unternehmensprozesse

- Einkauf
- Operations
- Finanzprozesse

Kundenservice

- Ticketbearbeitung
- Prozessinitiierung
- wiederkehrende Interaktionen

Grenzen heutiger Agentensysteme

- keine robuste Langzeitkonsistenz
- Halluzinationen in komplexen Abläufen
- schwierige Tool-Orchestrierung
- hoher Ressourcenbedarf
- Governance und Kontrolle

Fazit

Sprachmodelle beantworten Fragen. Agenten verfolgen Ziele.

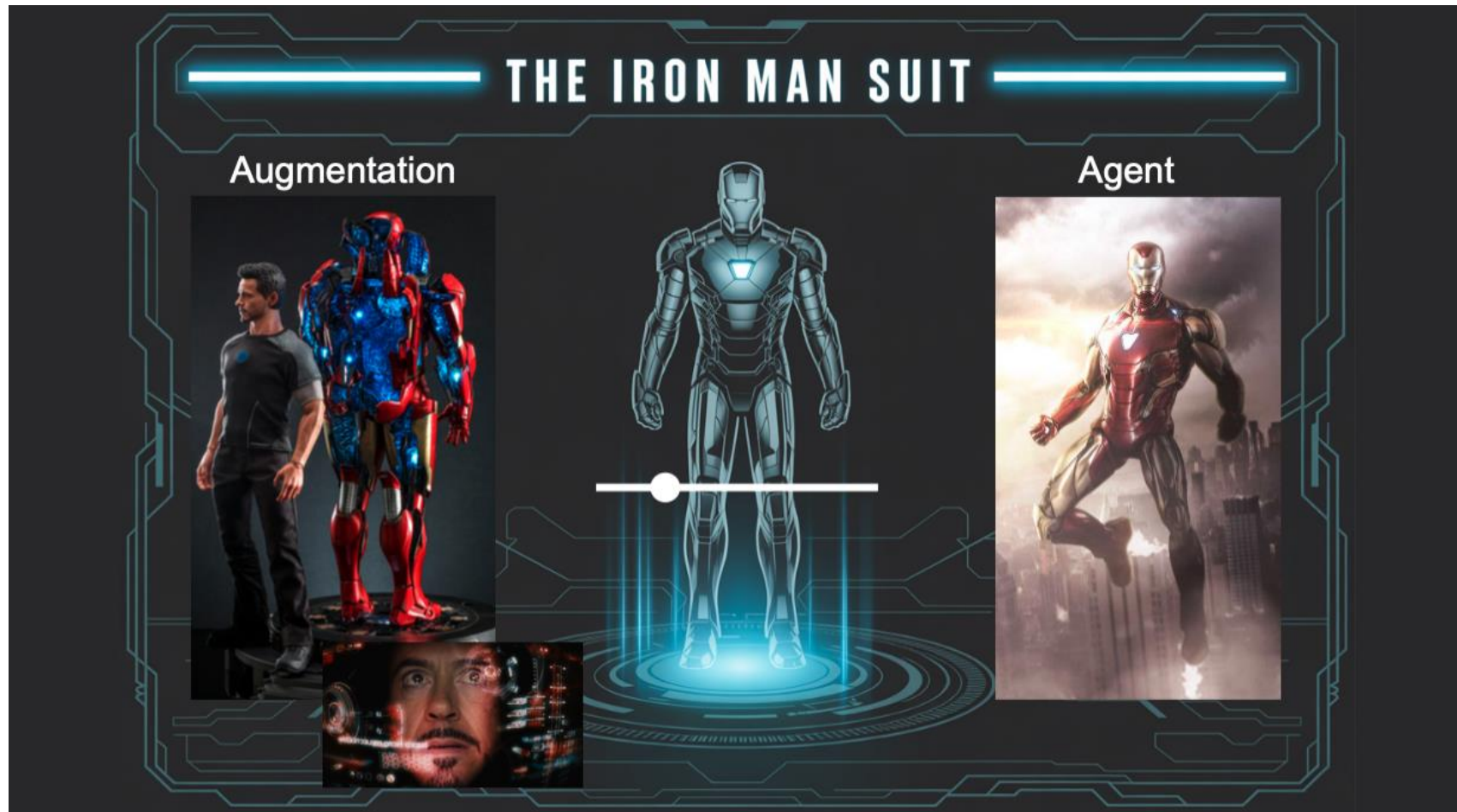
Heute bereits real nutzbar

Aber: noch teuer, fragil und nicht vollständig autonom

Trotzdem enormes Automatisierungspotenzial für Wissensarbeit

Wie viel Verantwortung geben wir der KI?

Autonomy Slider:



Quiz

Was ist ein LLM-Agent?

1. Eine individuelle Instanz eines Sprachmodells
2. Ein orchestriertes LLM mit Speicher, Tools und Planung