



Julian Kunkel
Lorenz Glißmann und Sascha Safenreider

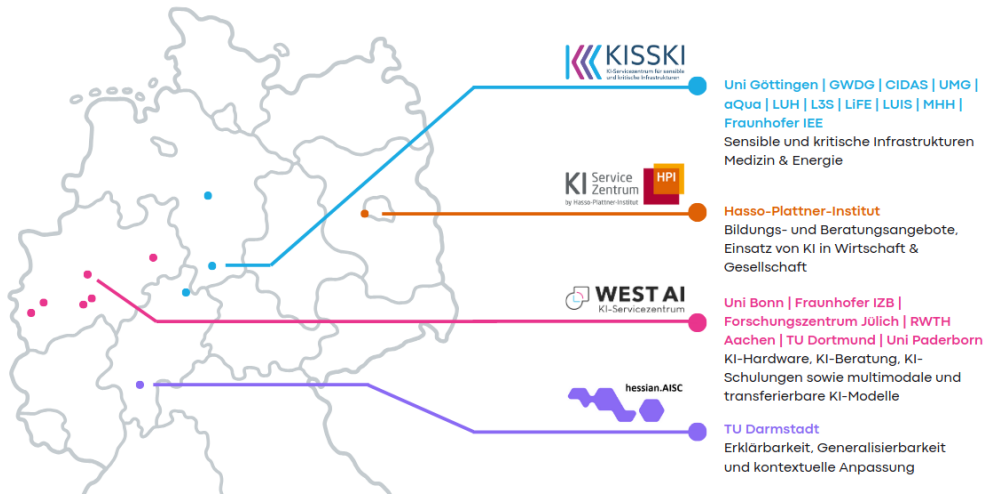
KI - Chancen für alle - Gemeinsam Potentiale entfalten an der Universität Göttingen

Über Mich – Prof. Dr. Julian Kunkel

- Stellvertretender Leiter der GWDG
im Bereich Hochleistungsrechnen
 - ▶ Die GWDG ist das Rechenzentrum der Universität und
Max-Planck Gesellschaft
- Professor am Institut für Informatik
- Koordinator des KI-Servicezentrums KISSKI
- Forschungsfragen (vereinfacht)
 - ▶ Wie können wir größte Datenmengen verarbeiten
 - ▶ Wie können wir 1000 Computer für Wissenschaftliche
Fragestellungen nutzen



KISSKI - Eines der nationalen BMFTR-geförderten KI-Servicezentren



KI-Servicezentrum KISSKI

... für Sensiblen und Kritischen Infrastrukturen

- Erfüllung **Anforderungen** kritischer Infrastrukturen:
Sicherheit, Datenschutz, Zuverlässigkeit
- über 1000 Hilfestellungen zu Projekten und Beratungen
- gefördert mit 23 Mio € - bis 12/2027
 - KI-Dienste über GWDG zertifiziert gemäß **ISO 27001**
(Informationssicherheit) - **C5 Testat** in Arbeit
 - Dienstleistungen für Pilotprojekte in ganz Deutschland
 - ▶ Beratung, Training, von Infrastruktur bis Endnutzerdienste
 - **Forschung** zur weiteren Verbesserung der Dienstleistungen
 - Fokus auf die Branchen Medizin und Energiewirtschaft ABER branchenoffen



<https://kisski.de>

KISSKI Leistungsspektrum

- Ganzheitliches Angebot rund um KI
- KI Lösungen im Browser und via API
- Hardwareressourcen
 - ▶ Trainingsplattform (Nvidia H100, A100)
 - ▶ Future Technology Plattform (Intel Habana Gaudi 2, NVIDIA Grace Hopper, GraphCore, Esperanto.ai, SpiNNaker)
- Schulungsangebot HPC und KI
 - ▶ GWDG Academy
 - ▶ KISSKI Schulungsangebot
 - ▶ Individuelle Kurse auf Anfrage



Veranstaltung heute

■ Session 1h: Einführung in KI

- ▶ Abfrage: Kenntnisstand KI, Interessen der Teilnehmenden
- ▶ Vortrag: Crashkurs – KI-Kompetenzen (insbesondere LLM), inkl. Motivation
- ▶ Diskussion in Kleingruppen über KI-Kompetenz
- ▶ Plenardiskussion

■ Pause (15 min) ☕

■ Session 45 min: Potentiale von KI erkennen

- ▶ Vortrag: Dienste der GWDG/KISSKI
- ▶ Vortrag: Use Cases und Beispiele von administrativen Tätigkeiten
- ▶ Methodische Herangehensweise zur Erarbeitung von Use Cases

■ Session 45 min: Anwendung von KI im eigenen Einsatzbereich

- ▶ Gruppenarbeit: Diskussion möglicher Einsatzgebiete und Priorisierung
- ▶ Diskussion eines Use Cases mit Solution Architekt zur Machbarkeit

■ Pause (15 min) ☕

■ Session 1h: Konsolidierung der Ergebnisse

Interaktivität



- Gruppenarbeit
- Alle Fragen erlaubt
- Stellt auch kritische Fragen

Eigene Erfahrungen und Erwartungen

Denkanstöße

- *Welche Erwartungen verbinden Sie mit dem Einsatz von KI in Ihrem Arbeitsumfeld?*
- *Wo sehen Sie das größte Potenzial – und wo mögliche Risiken?*
- *Welche Fragen oder Bedenken würden Sie gern im Workshop besprechen?*



Table of contents

- 1 Was ist KI?
- 2 Was hat KI mit Algorithmen zu tun?
- 3 Wie spricht KI?
- 4 Was ist ein ChatBot?
- 5 Rechtliches, Copyright und Datenschutz

Agenda



Was ist KI?

Wie wird KI definiert?

KI und ML

■ Künstliche Intelligenz (KI)

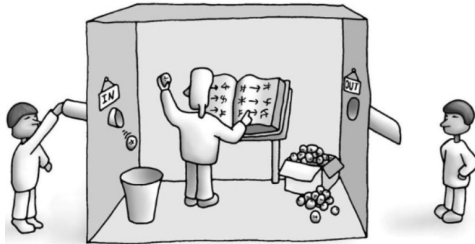
- ▶ Überbegriff für Systeme, welche Aufgaben ausführen, die normalerweise menschliche Intelligenz erfordern
- ▶ z.B. Sprachverarbeitung, Bilderkennung, Entscheidungsfindung

(Dukino et al. 2020; Kufel et al. 2023)

- Maschinelles Lernen
- Generative KI

KI und ML

Ist eine KI “intelligent”? Gedankenexperiment: Das Chinesische Zimmer (Searle 1980)



- ▶ Eine Person sitzt in einem Raum
- ▶ Spricht kein Chinesisch, hat aber ein Regelbuch (ein Algorithmus)
- ▶ Von außen kommen Fragen auf Chinesisch rein, die Person verarbeitet diese nach Anweisung und gibt passende Antworten aus
- ▶ Für Außenstehende wirkt es, als ob die Person Chinesisch versteht – tatsächlich folgt sie nur syntaktischen Regeln
- ▶ Kein Bewusstsein, also keine Intelligenz

KI und ML

■ Machine Learning (ML)

- ▶ Teilgebiet der KI, das aus Daten lernt
- ▶ Und Vorhersagen oder Entscheidungen trifft
- ▶ z.B. Schriftzeichenerkennung, automatisierte Diagnoseverfahren

■ Betrachten wir KI einmal von Seiten der Informatik...

(Dukino et al. 2020; Kufel et al. 2023)

Was hat KI mit Algorithmen zu tun?

Algorithmen

- Algorithmus: Vorschrift zum Lösen eines Problems (festgelegte Aufgabe)
- Verarbeitet Eingabe mit vorgegebenen Verarbeitungsschritten → Ausgabe
- Randbedingungen
 - ▶ endet immer, generiert für alle gültigen Eingaben die richtige Ausgaben
- Meist deterministisch, dieselben Eingabe → dieselbe Ausgabe
- Programmierende definieren die Verarbeitungsschritte

Algorithmen & Approximation

 **Heuristik:** Ist eine vereinfachte Lösungsmethode für eine Aufgabe.

- ▶ Ergebnis nicht immer korrekt
- ▶ Aber häufig gut genug, um sinnvoll zu sein

Algorithmen & Approximation

 **Heuristik:** Ist eine vereinfachte Lösungsmethode für eine Aufgabe.

- ▶ Ergebnis nicht immer korrekt
- ▶ Aber häufig gut genug, um sinnvoll zu sein

 Heuristiken werden durch Beobachtungen und Erfahrungen erstellt.

- ▶ Datengesteuert

Algorithmen & Approximation

 **Heuristik:** Ist eine vereinfachte Lösungsmethode für eine Aufgabe.

- ▶ Ergebnis nicht immer korrekt
- ▶ Aber häufig gut genug, um sinnvoll zu sein

 Heuristiken werden durch Beobachtungen und Erfahrungen erstellt.

- ▶ Datengesteuert

 Das menschliche Gehirn verallgemeinert automatisch, erkennt Zusammenhänge und erstellt „Heuristiken“.

- ▶ So lernen und abstrahieren wir
- ▶ Verallgemeinerungen können auch falsch sein

Algorithmen & Approximation

 **Heuristik:** Ist eine vereinfachte Lösungsmethode für eine Aufgabe.

- ▶ Ergebnis nicht immer korrekt
- ▶ Aber häufig gut genug, um sinnvoll zu sein

 Heuristiken werden durch Beobachtungen und Erfahrungen erstellt.

- ▶ Datengesteuert

 Das menschliche Gehirn verallgemeinert automatisch, erkennt Zusammenhänge und erstellt „Heuristiken“.

- ▶ So lernen und abstrahieren wir
- ▶ Verallgemeinerungen können auch falsch sein

 **5-Minuten-Aufgaben:**

- ▶ Welche Heuristiken kennen Sie und nutzen Sie?
- ▶ Welche falschen Annahmen sind Ihnen im Zusammenleben schon aufgefallen?

Algorithmen & Approximation

5-Minuten-Aufgaben:

- ▶ Welche Heuristiken kennen Sie und nutzen Sie?
- ▶ Welche falschen Annahmen sind Ihnen im Zusammenleben schon aufgefallen?

Welche Heuristiken kennt und nutzt ihr?

- ▶ Wetterbericht, "im Sommer ist es wärmer als im Winter"
- ▶ Merkgeregeln

Welche falschen Annahmen sind euch im Zusammenleben schon aufgefallen?

- ▶ Vorurteile, Bias, falsche Vorbilder

Probleme:

- ▶ Heuristiken enthalten die Fehler der Beobachtungen.
- ▶ Die Annahme selbst ist fehlerbehaftet.
- ▶ Es ist nicht immer klar, woher unsere Annahmen kommen.

Typische Algorithmen vs. KI-Modelle

Typischer Algorithmus

- **Regelbasiert:** Programm mit festen Schritten
- **Deterministisch:** Gleiche Eingabe → gleiche Ausgabe.
- **Gut geeignet, wenn das Problem klar definiert ist.**

KI-Modell

- **Lernt aus Daten:** Extrahiert Muster aus Beispielen
- **Probabilistisch:** Gleiche Eingabe kann leicht unterschiedliche Ergebnisse liefern („wahrscheinlichste“ Vorhersage).
- **Gut für komplexe, unscharfe Probleme:**
Sprache, Bilder, Texte.

Algorithmen & KI



KI-Systeme lernen von Eingabe- und Ausgabedaten

- ▶ Lernen ist datengetrieben, passiert algorithmisch
- ▶ Ziel: KI bekommt Eingabedaten und "schätzt" dazu gute Ausgaben
- ▶ Mechanismus: Muster in Daten verallgemeinern und reproduzieren
- ▶ Intuition: Annäherung an ein "perfektes Programm"



Probleme:

- ▶ Trainingsdaten sind inkonsistent, fehlerhaft und/oder verzerrt
- ▶ Nachvollziehbarkeit, Fehlersuche, -behebung sind schwierig



Sehr ähnlich zu den menschlichen Heuristiken / Verallgemeinerungen!

- ▶ "Künstliche Intelligenz"

Gruppenarbeit

- a) Bilden Sie bitte Gruppen 
- b) Diskutieren Sie bitte für 10 Minuten in der Gruppe! 
- Fragestellungen:
 - ▶ a) Welche KI-Anwendungen haben Sie bereits genutzt?
 - Ist das wirklich KI? Könnte es auch ein "traditioneller" Algorithmus sein
 - Was leistet sie für Sie?
 - Sind die Ergebnisse immer korrekt?
 - ▶ b) Welche Anwendungen würden Sie gern mehr nutzen?
 - Welche Tätigkeit ist besonders zeitaufwändig oder fehleranfällig und sollte durch KI unterstützt werden?

Und was ist generative KI?

Generative KI erstellt Inhalte, die i.d.R. kreativ von Menschen erzeugt werden:



Texte



Bilder



Audios



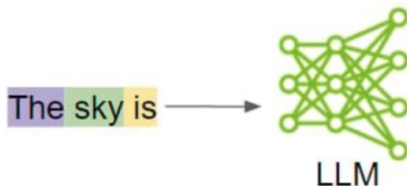
Videos

Wie spricht KI?

Was sind Large Language Models?

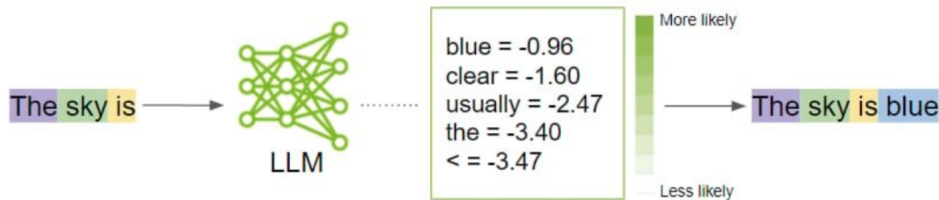
Wie arbeiten LLMs? Vereinfacht!

- LLM = Large Language Model = Großes Sprachmodell
- Vorhersage
 - ▶ LLM bekommt den bisherigen Text
 - ▶ Rät/Schätzt das "nächste Wort"
 - ▶ Statt ganzen Wörtern: Wortfragmente (Tokens)

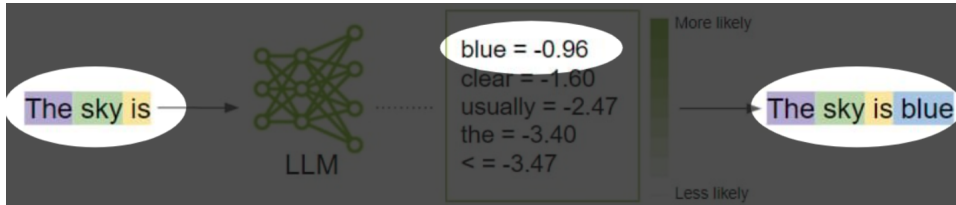


Wie arbeiten LLMs?

- Im LLM wird mit Zahlen als Repräsentationen gearbeitet
- Zahlen werden wieder in Tokens/Wörter umgewandelt



Wie arbeiten LLMs?



Was ist ein Chatbot?



Der digitale Freund, der hilft

- Versteht Sprache und antwortet sofort
- Merkt sich Kontext, der Zeit spart
- Erklärt, plant, erledigt Routine uvm.
- 24/7 verfügbar

LLM-basierter Chatbot: Was er kann / wo seine Grenzen liegen

Leistungen

- **Generierung von Texten** – z.B. E-Mails, Zusammenfassungen, Code-Snippets, Formatvorlagen.
- **Allgemeinwissen** – Fakten, Konzepte und Abläufe aus dem Trainings-Corpus.

Beispiel

„Schreibe meine Steuererklärung vom letzten Jahr.“

*→ Der Chatbot erzeugt ein Dokument, das optisch einer Steuererklärung entspricht, **aber** die Zahlen, Belege und persönlichen Angaben werden erfunden.*

Grenzen

- **Halluzinationen** – erzeugt plausible, aber falsche Fakten.
- **Kein Zugriff auf persönliche/unternehmensspezifische Daten** – kann keine individuellen Werte (z.B. Steuer-IDs) einbinden.

Halluzinationen



Halluzinationen



Here's your hidden-object challenge! Try to find the small antique key in this cluttered vintage study room. Let me know if you need a hint! 🔑

Rechtliches, Copyright und Datenschutz

Was darf ich und was darf ich nicht?

Welche Probleme gibt es mit Eingabedaten?

- Viele Nutzende übergeben Daten in KI-Systeme
- Falsche Nutzung kann ein Verstoß gegen Datenschutz darstellen!
 - ▶ Personenbezogener Daten
 - ▶ Als “vertraulich” klassifizierte Information
 - ▶ Ähnlich zur Situation, Daten in einen “ominösen” Cloudspeicher hochzuladen
- Wir haben keine Kontrolle, was die Anbieter mit den Daten machen
 - ▶ Viele “kostenlose” KI-Tools speichern Daten, um zu lernen!
 - ▶ Passwörter oder Namen von Personen im Trainingsdatensatz sind ein Problem
 - ▶ Industriespionage mancher Staaten
- Es obliegt der Verantwortung der Nutzenden!
- Betriebliche Rahmenbedingungen (**KI-Nutzungsrichtlinien**) beachten!

Welche Nutzung von KI-Systemen ist gefahrlos im Sinne des Datenschutzes möglich?

**Allgemein nur bei Anonymisierung und Schutz von Eingabe-Daten!
Oder nur öffentliche Input-Daten verwenden**



Text-, Tabellenkalkulations-
und Präsentationserstellung



Grafik- und
Videoerstellung

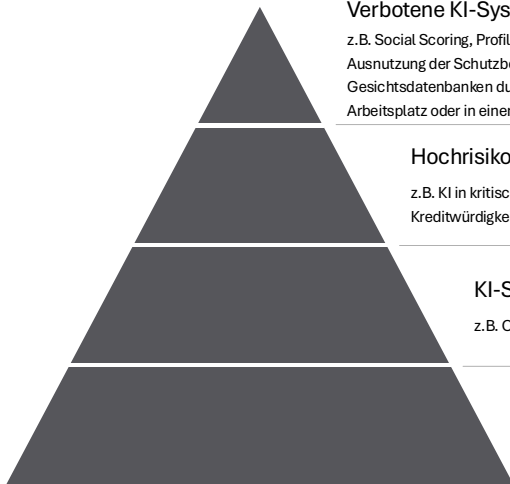


Erstellung von
Code



Vorhersagen
und Analysen

Welche Nutzung ist nach KI-VO Art. 5 reguliert?



Verbotene KI-Systeme (unannehmbares Risiko)

z.B. Social Scoring, Profiling zur Vorhersage von Straftaten, Unterschwellige Beeinflussung von Personen, Ausnutzung der Schutzbedürftigkeit von Personen (Alter, Behinderung, soziale oder wirtschaftliche Situation), Gesichtsdatenbanken durch ungezieltes Auslesen von Bildern aus dem Internet, Emotionserkennung am Arbeitsplatz oder in einer Bildungseinrichtung (außer aus medizinischen oder Sicherheitsgründen)

Hochrisiko-KI-Systeme

z.B. KI in kritischen Infrastrukturen (Energie, Verkehr, Gesundheit, ...), Personalmanagement, Kreditwürdigkeitsprüfung, Diagnosen zur Behandlung von Patienten

KI-Systeme mit begrenztem Risiko

z.B. Chatbots, Empfehlungssysteme

KI-Systeme mit minimalen oder keinem Risiko

z.B. KI in Videospielen, Spamfilter

Diskussion

KI-Kompetenz

Diskutieren Sie bitte für **10 Minuten.** ⌚

- Welche Ihrer Anwendungen von KI bisher würden Sie jetzt noch einmal hinterfragen?
 - ▶ Im Bezug zur KI-VO / AI Act
 - ▶ Im Bezug auf Datenschutz
- Können Sie jetzt andere sensibilisieren?



15 Min