GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN
Institute of Computer Science

Julian Kunkel, Sascha Safenreider
Carolina Ranfla Jimenez

KI-Methoden im akademischen Alltag: KI-Kompetenz

Agenda

1. Einführung: KI, Datenschutz und rechtliche Grundlagen
2. Verständnis von Art. 4 KI-VO ("KI-Kompetenz")
3. Funktionsweise und Grenzen von KI-Systemen
4. Verantwortungsvoller Umgang und praktische Beispiele

Lernziele

- Verständnis der rechtlichen Anforderungen und Zielsetzung von Art. 4 KI-VO
- Fähigkeit, grundlegende KI-Konzepte und -Risiken zu erklären
- Bewusstsein für einen sachkundigen und verantwortungsvollen KI-Einsatz

Art. 4, KI-VO ("KI-Kompetenz")

"Die Anbieter und Betreiber von KI-Systemen ergreifen Maßnahmen, um nach besten Kräften sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen, wobei ihre technischen Kenntnisse, ihre Erfahrung, ihre Ausbildung und Schulung und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, zu berücksichtigen sind."

W-Fragen

- Warum machen wir das/ist das wichtig?
  - Pflicht per Gesetz – Erfüllung von Art. 4, KI-VO ("KI-Kompetenz")
- Wer/was ist betroffen?
  - Unternehmen, welche KI-Dienste anbieten und betreiben
  - Personal/Mitarbeitende
- Worum geht es?
  - Grundverständnis aufbauen – was ist KI, wie funktioniert das
  - Ermöglicht sicheren und verantwortungsbewussten Umgang mit KI-Systemen
  - Gibt Anknüpfpunkte an das Recht
- Worum geht es NICHT?
  - Klärung von Rechtsfragen und Verfahrensfragen im Detail

Rechtlicher Hintergrund

- Verordnung über künstliche Intelligenz (Kurztitel)
  - "KI-Verordnung" (KI-VO), engl. "AI act"
  - Rechtsakt der EU zur Regulierung von Künstlicher Intelligenz (KI)
  - Seit 2019 ausgearbeitet, ab 01.08.2024 in Kraft
- ab Februar 2025 sind KI-Unternehmen verpflichtet, ihre Mitarbeitenden zu schulen
  - insbes. durch Art. 4

Titel: Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828

Implikationen aus Art. 4, KI-VO

- Schulungsangebot für Mitarbeitende und (externe) Nutzende der KI-Systeme schaffen:
  - Sachkundige, verantwortungsvolle Nutzung
  - Verständnis für Potenziale und Risiken
- Appell umfasst folgende Aspekte des Wissens und der Nutzung:
  - technische,
  - soziale,
  - ethische und
  - rechtliche

Wie wird KI definiert?

Ist das KI? Ja oder Nein?

oder

Frage 1:

Ein Roboter, der vordefinierte Bewegungen in einer Fabrik ausführt.

oder

Frage 1:

Ein Roboter, der vordefinierte Bewegungen in einer Fabrik ausführt.

oder

Das ist Automatisierung, aber keine KI, da der Roboter keine Entscheidungen trifft oder lernt.

Frage 2:

Ein Taschenrechner, der statistische Berechnungen durchführt.

oder

Frage 2:

Ein Taschenrechner, der statistische Berechnungen durchführt.

oder

Ein Taschenrechner führt nur programmierte Berechnungen durch und lernt nicht.

Frage 3:

Ein Algorithmus, der aus Daten lernt und Vorhersagen trifft.

Ja oder **Nein**

Frage 3:

Ein Algorithmus, der aus Daten lernt und Vorhersagen trifft.

oder

Das ist ein Beispiel für maschinelles Lernen, ein Teilbereich der KI.

Frage 4:

Ein Chatbot, der auf Spracheingaben reagiert.

oder

Frage 4:

Ein Chatbot, der auf Spracheingaben reagiert.

Ja oder **Nein**

Es kommt darauf an: KI-Sprachverarbeitung oder algorithmische Worterkennung?

Frage 5:

Ein Programm, das basierend auf festen Regeln Schach spielt.

Ja oder **Nein**

Frage 5:

Ein Programm, das basierend auf festen Regeln Schach spielt.

oder

Das ist ein Expertensystem, das keine Lernfähigkeit besitzt (“basierend auf festen Regeln”).

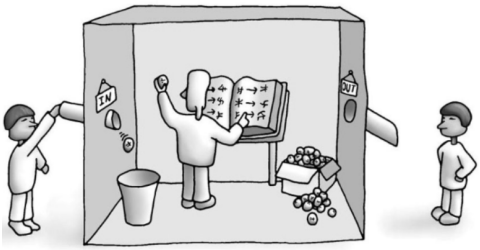
KI, ML und KNN

- 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)

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, ML und KNN

- Machine Learning (ML)
  - Teilgebiet der KI, das aus Daten lernt und Vorhersagen oder Entscheidungen trifft
  - z.B. Schriftzeichenerkennung, automatisierte Diagnoseverfahren

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

KI, ML und KNN

- Künstliche Neuronale Netze (KNN)
  - Spezielle Klasse vom ML, die aus miteinander verbundenen Neuronen besteht, ähnlich wie das biologische Gehirn
  - z.B. Deep Learning
- Betrachten wir KI einmal von Seiten der Informatik...

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

Algorithmen

- Ein Algorithmus ist eine Vorschrift zum Lösen eines Problems (festgelegte Aufgabe).
- Hierzu verarbeitet er Eingabe mittels vorgegebenen Verarbeitungsschritten und erzeugen eine Ausgabe
- Randbedingungen: endet immer, generiert für alle gültigen Eingaben die richtigen Ausgaben ...
- Meist deterministisch, d.h. nach derselben Eingabe kommt dieselbe Ausgabe Programmierende definieren die Verarbeitungsschritte (bspw. in Programmiersprache)

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 & KI

- KI lernt von Eingabe- und Ausgabedaten, wie die Verarbeitung stattfinden muss, sie ist datengetrieben
  - Das Erlernen selbst passiert mittels Algorithmen und ist deterministisch
  - Hierbei werden Inkonsistenzen (widersprüchliche Daten) zwischen Ein- und Ausgabe toleriert
  - Ein bestmöglicher Match zwischen Input und Output wird erstellt, aber enthält Fehler
- KI-Algorithmus erstellt quasi das "Programm" für die Verarbeitung als Annäherung an ein "perfektes" Programm

Algorithmen & KI

- Probleme:
  - Das "Programm" enthält Fehler von Input/Output
  - Die Annäherung ist fehlerbehaftet
  - Es ist nicht immer klar, woher die Ergebnisse kommen
    - Schwierigkeit, das Programm zu debuggen
- Dies ist sehr ähnlich zu den Heuristiken / Verallgemeinerungen des Menschen!
  - "Künstliche Intelligenz"

Und was ist generative KI?

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

Wie funktioniert generative KI?

- Generative Adversarial Networks (GANs)
  - Zwei neuronale Netze arbeiten gegeneinander. Eines erzeugt Inhalte (Generator), und das andere bewertet deren Echtheit (Diskriminator).
- Transformer
  - Text wird in Vektoren umgewandelt und von Kodierern/Dekodierern verarbeitet
  - GPT-Modelle (Generative Pre-trained Transformer), die auf großen Datenmengen trainiert werden, um umfassende Ergebnisse zu liefern.

(Durall et al. 2021; Xu et al. 2021)

Wie funktioniert generative KI?

- Hybride Ansätze
  - Hybride Ansätze kombinieren die Struktur von GANs, die aus einem Generator und einem Diskriminator besteht, mit Fähigkeiten von Transformern, um generative Aufgaben zu lösen.

(Durall et al. 2021; Xu et al. 2021)

Sprechen / LLMs

- Wie passiert das “Sprechen”?
- Was sind Large Language Models?
- Warum kann KI nicht denken und trotzdem mit mir sprechen?
  - KI imitiert menschliche Sprache durch statistische Modelle und Algorithmen
  - Das "Sprechen" ist lediglich das Ergebnis der Verarbeitung von Mustern – ohne Bewusstsein, Gedanken, Emotionen oder Intentionen.

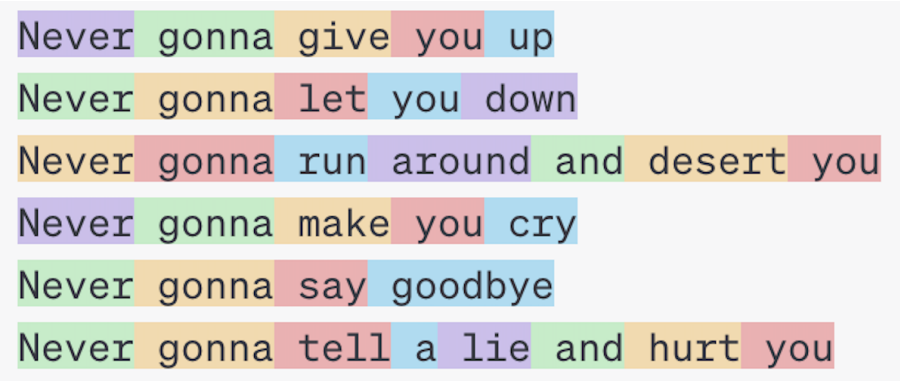
Was sind LLMs?

- Large Language Models (LLMs) sind transformative KI-Modelle (basierend auf KNN), die mithilfe von riesigen Datenmengen trainiert werden, um menschliche Sprache zu verarbeiten und generieren zu können.

Wie arbeiten LLMs?

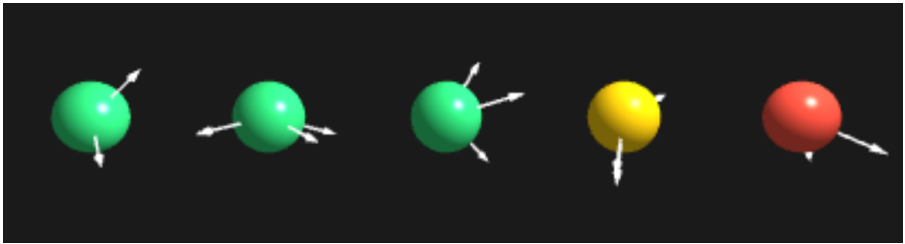
1. Schritt: Text zerlegen

Text wird in kleine Einheiten (Tokens) zerlegt.



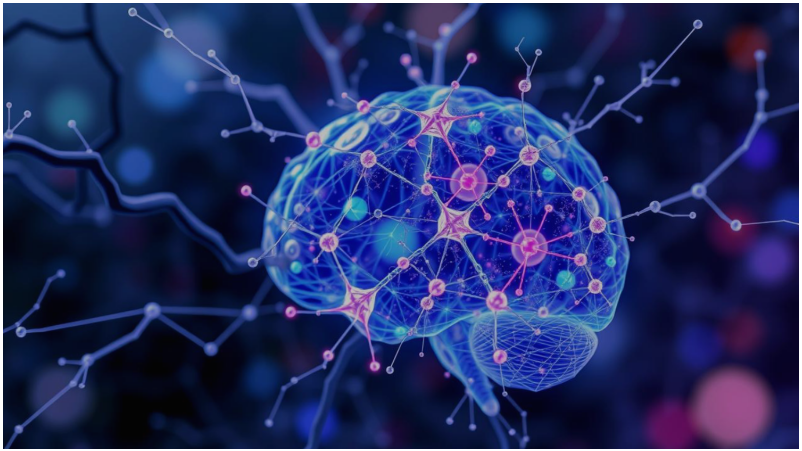
2. Schritt: Tokens in Zahlen umwandeln

Tokens werden als Zahlen bzw. Vektoren repräsentiert.



3. Schritt: Informationsverarbeitung

Das künstliche neuronale Netz (KNN) verarbeitet die Token.

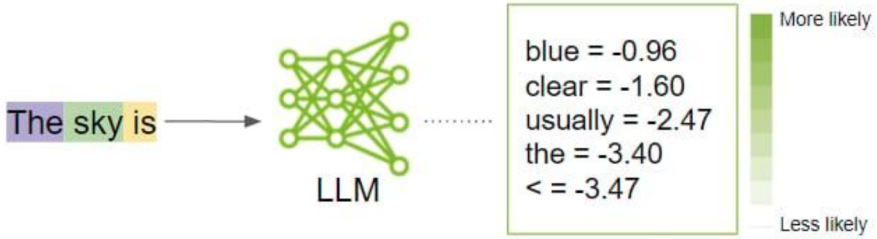


3. Schritt: Informationsverarbeitung

Beispiel Word2Vec

4. Schritt: Vorhersage

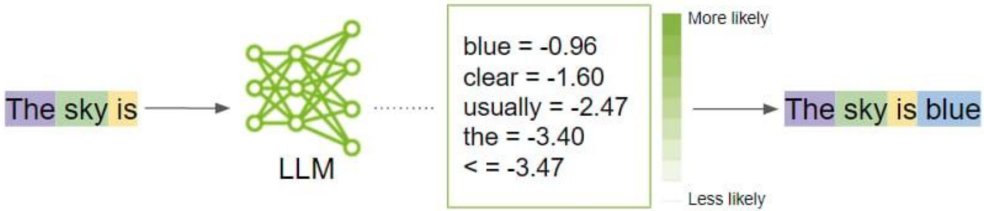
Basierend auf den Token berechnet das LLM das wahrscheinlich nächste Token.



Bildquelle: beehiiv.com

5. Schritt: Zahlen in Token umwandeln

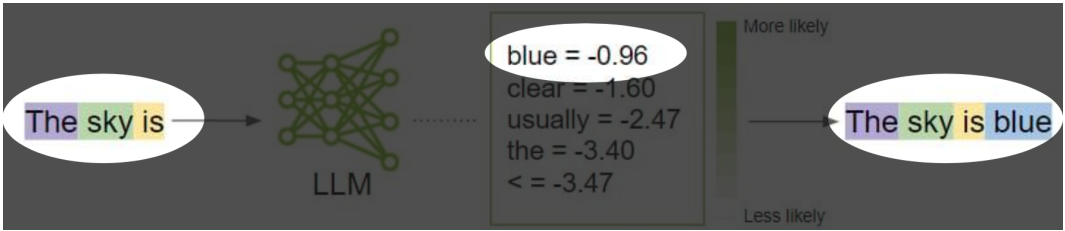
Das statistisch vorhergesagte Token wird wieder in lesbaren Text umgewandelt.



Bildquelle: beehiiv.com

5. Schritt: Zahlen in Token umwandeln

Das statistisch vorhergesagte Token wird wieder in lesbaren Text umgewandelt.



Bildquelle: beehiiv.com

Workshop: Heuristiken

- Welche Heuristken wendet ihr im Alltag an?

Workshop: KI Anwendungen

- Diskutiert bitte die folgenden Fragen:
  - Welche KI-Anwendungen habt ihr bereits genutzt?
    - Ist das wirklich KI? Könnte es auch ein "traditioneller" Algorithmus sein
    - Was leistet die Anwendung für euch?
    - Sind die Ergebnisse immer korrekt oder gab es Fehler?
  - Welche KI-Anwendungen würdet ihr gern häufiger oder anders nutzen (z. B. im Studium, Alltag, Forschung, Arbeit)?

Diskussion im Plenum

- Welche Heuristken kennt ihr / benutzt ihr?
- Wie unterscheiden sich „echte“ KI-Systeme von regelbasierten Tools?
- Warum ist das relevant für verantwortungsbewusste KI-Nutzung?

Take-Home-Message

- Heuristiken sind vereinfachte, oft nützliche Entscheidungsregeln, aber fehleranfällig.
- KI-Anwendungen bieten Effizienz und Unterstützung, aber keine Garantie für Richtigkeit.
- Viele genutzte Tools sind nicht automatisch KI, sondern beruhen auf vordefinierten Regeln oder Automatisierung.