ChatGPT

Mit KI in ein neues Zeitalter

» Hier geht's direkt zum Buch

DIE LESEPROBE

1 KI und Machine Learning: Entwicklung und Technologien

1.1 Natürliche Intelligenz und ihre künstliche Schwester

Wer sich mit künstlicher Intelligenz (KI oder engl. AI für *artificial intelligence*) beschäftigt, muss zuerst klären, was natürliche Intelligenz eigentlich ist. *Intelligenz* ist ein ziemlich schwer zu definierendes Konzept. Wissenschaftliche Erklärungsversuche kommen aus der Psychologie und Philosophie, der Neurologie und weiteren Disziplinen, die basierend auf ihrem Forschungsgegenstand jeweils andere Aspekte in den Vordergrund stellen. Eine zusammenhängende Erklärung oder ein tiefgehendes Verständnis, warum unser Gehirn zu wirklich außerordentlichen Leistungen fähig ist, gibt es noch nicht.

Versucht man sich an einer allgemeingültigen Definition, die quer durch alle Fachrichtungen wenigstens ein Kopfnicken hervorrufen soll, könnte man Intelligenz als die Fähigkeit bezeichnen, Wissen zu erwerben und dieses Wissen anzuwenden, um damit beliebige Probleme zu lösen. In einem weiteren Schritt entsteht daraus idealerweise neues Wissen und es können neue Erkenntnisse und Konzepte formuliert werden. Intelligenz ist untrennbar mit dem Begriff des *Transfers* verbunden. Es geht dabei um Anpassungsfähigkeit, das Lernen aus Erfahrungen und das Anwenden von erworbenem Wissen in stetig variierenden Kontexten. Die Entwicklung von Intelligenztests zur Bewertung und Messung menschlicher Intelligenz war von Anfang an ein fragwürdiges Unterfangen, das nicht zu einem besseren Verständnis des Phänomens geführt hat.

Künstliche Intelligenz war und ist ganz allgemein gesprochen der Versuch, menschliche Intelligenz in Maschinenform nachzubilden und irgendwann sogar zu übertreffen. Maschinen im Allgemeinen und Computer im Besonderen sollten so gestaltet werden, dass sie menschenähnliche Fähigkeiten erhalten, um Aufgaben auszuführen, die normalerweise menschliche Intelligenz erfordern. Künstliche Intelligenz als umfassender Ansatz wurde in viele einzelne Teilbereiche zer-

legt, von Computer Vision (Bilder und Videos interpretieren, um daraus Informationen zu gewinnen) bis zur Robotik (Entwicklung von Maschinen, die eine Vielzahl von Aufgaben autonom ausführen können). Die natürliche Sprachverarbeitung (Natural Language Processing, NLP), also das Verstehen und aktive Verwenden menschlicher Sprache für Anwendungen wie Chatbots, Übersetzungsdienste und Sprachassistenten, entwickelte sich schnell zu einem der anspruchsvollsten Forschungszweige in der Informatik.

Künstliche Intelligenz ist bis heute keine Nachbildung *allgemeiner* menschlicher Intelligenz in Maschinenform. Die Entwicklung konkreter Anwendungen konzentriert sich immer auf eine *spezialisierte* Intelligenz für ganz bestimmte Aufgaben. Ein Schachcomputer kann die besten Spieler der Welt auf dem Schachbrett mattsetzen, kann außerhalb des Spielfeldes aber kein einfaches Gespräch führen und eine Maus nicht von einem Elefanten unterscheiden.

Heute ist die künstliche Repräsentation menschlicher Intelligenz ein ziemlich buntes und multidisziplinäres Unterfangen, das ständig wächst und sich in alle Richtungen in rasendem Tempo weiterentwickelt: Chatbots sprechen wie Menschen mit uns, Computerprogramme erkennen den Inhalt von Bildern, produzieren auf Wunsch auch neue Bilder oder Videos in täuschend echter Qualität, sie erkennen und bewerten komplexe Verkehrssituationen in Echtzeit und können Fahrzeuge autonom steuern. Diesen wirklich beeindruckenden Fortschritten in vielen Bereichen, die menschliche Fähigkeiten teilweise um ein Vielfaches überschreiten, stehen andere Aspekte menschlicher Intelligenz gegenüber, die auf der Maschine offenbar schwer zu replizieren sind: Emotion, Empathie und interdisziplinäres Denken.

1.2 Ursprünge der KI und historische Entwicklung

Die Geschichte der künstlichen Intelligenz ist ebenso lang wie faszinierend. Erste Konzepte und Visionen stammen von Heron von Alexandria, einem griechischen Mathematiker und Ingenieur, der unter dem Titel *Automata* das erste *Buch der Maschinen* veröffentlichte und einen Weihwasserautomaten entwickelte. Die Jahrtausende alte Idee, künstliches Leben zu erschaffen, griff ein französischer Ingenieur und Erfinder namens Jacques de Vaucanson auf und entwickelte 1738 die *Mechani-*

sche Ente und weitere Automaten. Aber erst das 20. Jahrhundert gilt als Geburtsstunde der modernen KI. Pionier in den 1930er- und 1940er-Jahren war Alan Turing mit seiner *Turing-Maschine*, die kein physisches Gerät, sondern ein theoretisches Konzept zur Theorie der Berechenbarkeit darstellte. Sie hat zur Entwicklung von Programmiersprachen, zur Theorie der Automaten und zur Erkenntnis der Grenzen der Computermathematik beigetragen und Grundlagen für das Verständnis algorithmischer Prozesse gelegt. Von ihm stammt auch der bekannte *Turing-Test*, der ab 1950 zu einem zentralen Diskussionsthema im Bereich KI wurde: Ein Computer besteht den Turing-Test, wenn ein menschlicher *Richter* nicht in der Lage ist zu entscheiden, ob er mit einem Menschen oder einem Computer kommuniziert, basierend allein auf den gegebenen Antworten.

Der Begriff *künstliche Intelligenz* wurde 1955 von John McCarthy geprägt und im Rahmen des Dartmouth Meetings im Jahr 1956 vorgestellt. Dieser Kongress gilt als die Geburtsstunde der KI als eigenständige Teildisziplin der Informatik. Die ersten KI-Programme wurden mit großer Euphorie entwickelt, darunter das Schachprogramm von Claude Shannon und das Programm *Logic Theorist* von Allen Newell und Herbert A. Simon. In den 1960ern und 1970ern gab es einen großen Optimismus in der KI-Forschung, mit respektablen Fortschritten in Bereichen wie maschinellem Lernen und der Sprachverarbeitung. »ELIZA« wurde in den 1960er-Jahren von Joseph Weizenbaum am Massachusetts Institute of Technology (MIT) entwickelt und war eines der ersten Computerprogramme, das in der Lage war, textbasierte Konversationen mit Menschen zu führen. Auf Grundlage des DOCTOR-Skripts ahmte es die Gesprächsführung eines Therapeuten nach. ELIZA verwendet Muster und Schlüsselwörter, um die Eingabe eines Benutzers zu analysieren und passende vordefinierte Antworten auszuwählen. Viele Benutzer hatten das Gefühl, mit einem menschlichen Therapeuten und nicht mit einem Computer zu sprechen.

Allerdings traten in den späten 1970ern auch die Grenzen der KI-Techniken zutage und führten zum ersten *KI-Winter.* In dieser Periode erlahmte das allgemeine Interesse am Forschungsgebiet und die Finanzierung wurde stark zurückgefahren. In den 1980ern kamen die sogenannten *Expertensysteme* auf den Markt und sorgten für eine Wiederbelebung der KI. Diese waren darauf ausgelegt, menschliches Fachwissen in einem spezifischen, stark eingegrenzten Bereich zu sammeln und

das Wissen vieler Experten darin zu bündeln, um Beratung und Entscheidungsunterstützung anzubieten. Ein prominentes Beispiel eines Expertensystems ist *MYCIN*, ein System, das Ärzte bei der Diagnose von bakteriellen Infektionen unterstützt und Therapieempfehlungen für Antibiotika gibt. Weitere Systeme wie *PUFF* halfen Medizinern bei der Interpretation von Lungenfunktionsdaten, ein anderes unterstütze Ingenieure bei der Entwicklung von Schaltungen (*CADET*: Computer Aided Design of Electric Circuits). Alle diese Systeme markierten einen signifikanten Fortschritt in der KI-Forschung und schufen überaus nützliche Anwendungen für eng abgegrenzte Bereiche. Obwohl ihre Fähigkeiten im Vergleich zu heutigen KI-Systemen sehr begrenzt waren, legten sie den Grundstein für viele heutige KI-Anwendungen und maschinelle Lernsysteme.

Auf den ersten KI-Winter folgte der zweite, als gegen Ende des Jahrzehnts die anfängliche Begeisterung wieder verflogen war. Ein Rückgang des allgemeinen Interesses an einem Forschungsgebiet führt immer zu einer Reduzierung der finanziellen Mittel und diese Ausdünnung der Forschungsgelder führte unweigerlich zum zweiten (und letzten) KI-Winter. Die Grundlagenforschung in den 1990ern fokussierte sich immer weiter auf datengetriebene, statistische Ansätze, besonders in der Sprachverarbeitung und beim maschinellen Lernen. In den 2000ern beschleunigten sich die Entwicklungen dann weiter. Die Verfügbarkeit von immer leistungsstärkerer Hardware und die exponentielle Zunahme an verfügbaren Daten läuteten nun das Zeitalter von *Big Data* ein und sorgten für große Fortschritte im Bereich des maschinellen Lernens.

Das 21. Jahrhundert bedeutet für die KI also gleichermaßen Renaissance wie endgültiger Durchbruch. Deep Learning sowie neuronale Netzwerke mit vielen Schichten und tiefen Architekturen revolutionierten Bereiche wie Bild- und Spracherkennung. KI-Systeme wie IBMs *Watson* und *AlphaGo* von DeepMind zeigten beeindruckende Fähigkeiten in der Lösung immer komplexerer Aufgaben. Bis heute hat die KI-Forschung eine beeindruckende Reise hinter sich, von ersten Visionen über die theoretischen Anfänge bis hin zu realen Anwendungen, die unsere moderne Welt immer tiefer prägen. Noch immer gibt es zahlreiche ungelöste Fragen und Herausforderungen, aber die Fortschritte der letzten Jahrzehnte sind erstaunlich.

1.3 KI-Sprachassistenten und Gründung von OpenAI

Ich erinnere mich an eine Szene aus der Serie *Raumschiff Enterprise*, die mich als Kind sehr beeindruckt hat: Ein Außerirdischer erhält Zugriff auf den Bordcomputer des Raumschiffes und eröffnet seine Befehlseingabe ganz selbstverständlich mit »Hallo Computer«. Ein etwas verdutzter, aber hilfsbereiter Mr. Spock händigt ihm daraufhin eine Tastatur aus, die der andere mit verächtlicher Miene entgegennimmt und mit »Wie rückständig!« kommentiert. Was in den 1970ern noch reine Utopie war, ist heute längst Realität: Siri, Alexa und ähnliche Sprachassistenten gehören auf dem Smartphone zum Alltag und sind dort längst keine Sensation mehr. Vor der Einführung von Siri im Jahre 2011 als Teil des iPhone 4S waren KI-Interaktionen mit gesprochener Sprache für den durchschnittlichen Verbraucher auf Science-Fiction-Filme beschränkt. Auf Apples Siri folgte Amazons Alexa und der Google Assistant. Die Sprachassistenten brachten KI in die Taschen und Wohnzimmer von zahllosen Menschen. Aus dem ehrgeizigen Konzept wurde im Handumdrehen ein ganz alltägliches Werkzeug.

Die Sprachassistenten der großen Internet-Konzerne führten mit der Kommerzialisierung zu erheblichen Investitionen in Forschung und Entwicklung von Spracherkennungstechnologien. Fortschritte in der Spracherkennung haben die Popularität von Sprachassistenten noch weiter gesteigert und die anfängliche Fehlerquote in der Erkennung natürlicher gesprochener Sprache ist in den letzten Jahren drastisch gesunken. Hinzu kommen Fortschritte im Natural Language Processing (NLP), weil Assistenten auch den Kontext und die Bedeutung der Anfragen verstehen müssen. Dieses konkrete kommerzielle Interesse hat die Entwicklung in den Bereichen NLP und Natural Language Understanding (NLU) enorm vorangetrieben.

Ein Meilenstein in der Entwicklung der KI war die Gründung von OpenAI im Dezember 2015. Die Organisation wollte sich der Forschung im Bereich künstlicher Intelligenz widmen. Der im ursprünglichen Gründungsbrief dargelegte Hauptzweck formulierte, dass künstliche allgemeine Intelligenz (Artificial General Intelligence, AGI) der gesamten Menschheit zugutekommen sollte. OpenAI wollte selbst Anwendungen entwickeln und damit sicherstellen, dass KI auch von anderen auf eine Weise entwickelt wird, die der Menschheit nützt. Zu den

Gründern von OpenAI gehörten Tech-Unternehmer und -Investoren wie Elon Musk und Sam Altman, der später CEO wurde. OpenAI hatte sich von Beginn an darauf festgelegt, seine Forschung öffentlich zugänglich zu machen, später wurde diese vollständige Offenheit wegen Sicherheits- und Wettbewerbsbedenken aber immer weiter einschränkt.

Elon Musk war einer der Hauptunterstützer von OpenAI, hatte aber keine Kontrolle über die Aktivitäten der Organisation, die als unabhängige Einheit agierte. Musk war natürlich Vorstandsmitglied und wollte der Nachrichtenwebsite Semafor zufolge im Jahr 2018 die Kontrolle von OpenAI übernehmen. CEO Sam Altman und andere Gründer hätten seine Ambitionen aber abgelehnt, was zum Ausstieg von Musk wegen angeblicher Interessenkonflikte führte. Die Gründung von OpenAI war neben gemeinnützigen und geschäftlichen Interessen nicht zuletzt auch Ausdruck einer wachsenden Besorgnis in der Tech-Gemeinschaft über die potenziellen Risiken von KI und insbesondere von AGI. Durch ihre Bemühungen und Forschungen hoffte die Organisation damals, den Weg für eine sichere und für alle vorteilhafte Entwicklung von fortschrittlichen KI-Technologien zu ebnen.

1.4 Machine Learning (ML) und Deep Learning (DL)

Machine Learning oder maschinelles Lernen ist ganz allgemein gesprochen der Ansatz, Maschinen so zu programmieren, dass sie, statt vorgegebene Anweisungen zu befolgen, aus Daten lernen können, ähnlich wie Menschen aus ihren Erfahrungen lernen. Ziel ist, dass die Maschinen ihre Leistung bei der Lösung bestimmter Aufgaben über die Zeit hinweg durch Erfahrung (also weiteres Lernen) immer weiter verbessern.

Machine Learning (ML) und Deep Learning (DL) sind Teilgebiete der künstlichen Intelligenz, die sich aber in Konzept, Architektur und Anwendung stark unterscheiden. Machine Learning beschreibt den konzeptuellen Ansatz, bei dem Computer die Fähigkeit erlernen, Aufgaben ohne explizite Programmierung auszuführen. ML-Algorithmen nutzen vorgegebene Daten, um Vorhersagen oder Entscheidungen zu treffen, ohne explizite Programmanweisungen, wie diese Entscheidungen getroffen werden sollen. Wenn ein KI-Programm Bilder von Stühlen und Sesseln unterscheiden soll, werden im Algorithmus keine Kriterien für

Stühle oder Sessel hinterlegt. Stattdessen werden dem Programm gelabelte Trainingsdaten vorgelegt, also Bilder von Stühlen und Sesseln gezeigt, und für jedes Bild wird der korrekte Typ genannt. Der ML-Algorithmen muss (und kann) nun selbstständig geeignete Kriterien zur Unterscheidung finden und gewichten. Nach den Trainingsdaten kommen weitere, bisher unbekannte Testdaten, mit denen geprüft wird, ob das System bereits praxistauglich ist oder weiteres Training benötigt.

Deep Learning (DL) ist ein Teilbereich von ML, der meistens tief verschachtelte neuronale Netzwerkarchitekturen verwendet. Diese *tiefen* Modelle können aus sehr vielen Schichten bestehen, weshalb man sie als *Deep Learning* bezeichnet. DL-Modelle sind komplexe Netzwerke, die sehr große Mengen an Daten benötigen, um angemessen trainiert zu werden. ML-Modelle können mit deutlich weniger Daten auskommen als DL-Modelle. Wegen der Datenmenge und der höheren Komplexität der Netzwerke erfordern DL-Modelle häufig spezialisierte Hardware wie Grafikprozessoreinheiten (GPUs) oder Tensor Processing Units (TPUs) für das Training, was enorm rechen- und kostenintensiv ist. Einfache ML-Modelle sind deutlich anspruchsloser und erfordern keine besondere Hardware.

Deep-Learning-Modelle, die auf großen Datenmengen beruhen, sind zwar sehr leistungsfähig, weil es aber schwierig bis unmöglich ist, die genaue Funktionsweise der einzelnen Neuronenschichten nachzuvollziehen, sind die Ergebnisse wenig bis gar nicht interpretierbar und werden oft als *Black Boxes* empfunden. Machine Learning wird in eher einfachen Anwendungen der Vorhersageanalyse, für Empfehlungssysteme bis hin zur Mustererkennung eingesetzt. Deep Learning hingegen ist bei sehr großen Mengen unstrukturierter Daten im Vorteil und entwickelt das volle Potenzial bei Aufgaben wie der Bild- und Spracherkennung. ML nutzt eine Vielzahl von Algorithmen wie lineare Regression, Entscheidungsbäume und Support Vector Machines, DL konzentriert sich hauptsächlich auf neuronale Netzwerkarchitekturen und Transformer, wie sie auch bei ChatGPT zum Einsatz kommen.

Deep Learning ist also so etwas wie das Sahnehäubchen und die Weiterentwicklung von Machine Learning. Es setzt auf komplexe neuronale Netzwerke und deren tief verschachtelte Architekturen. Praktisch alle neueren Leuchtturm-Anwendungen der KI basieren auf Deep-Learning-Algorithmen und profitieren von der großen Menge an verfügbaren Daten und einer immer leistungsfähigeren Hardware mit

exponentiell wachsender Rechenleistung. Wussten Sie das schon? Nach heutigen Standards betrachtet, hat ein aktuelles Smartphone schon deutlich mehr Rechenleistung als die Computer der ersten Apollo-Mission!

1.5 Schlüsseltechnologien und Methoden des Machine Learnings

Künstliche Intelligenz umfasst eine Reihe von Schlüsseltechnologien für spezifische Anwendungen, die je nach Problem und Art der vorliegenden Daten eingesetzt werden. Beim Machine Learning werden vor allem drei unterschiedliche Formen des Lernens eingesetzt: das Supervised Learning, das Unsupervised Learning und das Reinforcement Learning.

Man kann ein Modell anhand von gelabelten Daten trainieren, in unserem Beispiel Bilder von Stühlen und Sesseln, die vorher *gelabelt*, also gekennzeichnet und der jeweiligen Klasse zugeordnet wurden. Das Verfahren zum Training des Modells nennt sich überwachtes Lernen oder **Supervised Learning**. Typische Anwendungen von überwachtem Lernen sind E-Mail-Spam-Filter: Ein Modell wird trainiert, um zu erkennen, ob eine E-Mail Spam ist oder nicht. Das Training erfolgt auf einem Datensatz, in dem vorhandene E-Mails bereits als *Spam* oder *Nicht-Spam* gekennzeichnet sind. Systemanalytiker bezeichnen dieses Verfahren als *Klassifikation*. Im Gegensatz dazu eröffnen sich mit der sogenannten *Regression* weitere Möglichkeiten, wie sie z.B. in der Vorhersage von Immobilienpreisen durch eine KI verwendet werden: Ein Modell wird trainiert, um den Verkaufspreis von Häusern, basierend auf verschiedenen Merkmalen wie Größe, Lage und Anzahl der Zimmer, vorherzusagen. Der Trainingsdatensatz enthält historische Daten von verkauften Häusern mit allen Merkmalen und den tatsächlich erzielten Verkaufspreisen.

Wenn die Daten zum Trainieren von Modellen ohne Labels auskommen müssen, sprechen wir vom unüberwachten Lernen bzw. **Unsupervised Learning**. Das kommt immer dann zum Einsatz, wenn es zu viele Parameter gibt und gleichzeitig die Relevanz einzelner Parameter noch nicht eingeschätzt werden kann. Dass man auf die Intelligenz eines Menschen eher über dessen Schulnoten als über die Schuhgröße

rückschließen kann, steht sicherlich außer Frage. Aber an welchen Parametern erkennt der Online-Händler die Besucher seiner Website mit dem größten Umsatz-Potenzial?

Beim unüberwachten Lernen werden Modelle anhand von nicht gelabelten Daten trainiert. Das Hauptziel besteht darin, Muster, Strukturen oder Zusammenhänge in den Daten zu entdecken, ohne dass vorher festgelegte Labels oder Kategorien vorhanden sind. An konkreten Beispielen wird das deutlicher: Ein Handelsunternehmen möchte seine Kunden basierend auf ihrem Kaufverhalten in verschiedene Gruppen einteilen, ohne vorher zu wissen, welche Kategorien dafür eigentlich relevant sind. Ein **Clustering-Algorithmus** wie *k-Means* kann verwendet werden, um die Kunden in verschiedene Gruppen bzw. Cluster zu unterteilen, ohne dass vorher Kategorien für die Einteilung festgelegt wurden. Clustering ist für alle Arten von Segmentierungen ein sinnvolles Verfahren.

Für die Analyse des Warenkorbes werden **Assoziationsregeln** verwendet: Ein Einzelhändler möchte herausfinden, welche Produkte häufig zusammen gekauft werden, um effektive Produktbündel oder Werbeaktionen zu erstellen. Ein Algorithmus wie *Apriori* kann verwendet werden, um solche Assoziationsregeln in vorliegenden Transaktionsdaten zu finden. Bei diesen Beispielen zum Clustering und Assoziationsregel-Lernen gibt es keine vorgegebenen Labels oder Kategorien. Das Modell versucht stattdessen, die zugrunde liegende Struktur der Daten zu erkennen und daraus Erkenntnisse zu gewinnen.

Die dritte Form des Lernens ist das sogenannte **Reinforcement Learning** oder verstärkendes Lernen. Modelle lernen durch Belohnungen, basierend auf den getroffenen Entscheidungen. Das Konzept des verstärkenden Lernens hat Parallelen zur positiven und negativen Verstärkung in der Verhaltenspsychologie, die auch in Erziehungskontexten angewendet wird. Tatsächlich stammen viele Prinzipien des verstärkenden Lernens in der KI aus der Verhaltenspsychologie. In der Erziehung von Kindern bedeutet Verstärkung, dass bestimmte Reaktionen oder Verhaltensweisen des Kindes durch Belohnungen (positive Verstärkung) oder unangenehme Reize (negative Verstärkung) gestärkt werden, um das gewünschte Verhalten zu fördern. Maschinelles verstärkendes Lernen wird oft in der Robotik und in der Spiele-KI eingesetzt.