Was ist Machine Learning?

von Clarissa Kupfermann

Clarissa studiert Jura an der Universität zu Köln und ist als studentische Hilfskraft am Institut für Straf- und Strafprozessrecht tätig.

Künstliche Intelligenz (KI) ist ein aktuell viel diskutiertes Thema. Technische Entwicklungen schreiten stetig voran und KI spielt dabei eine immer bedeutendere Rolle. In diesem Zusammenhang taucht häufig der Begriff „Machine Learning", zu Deutsch „Maschinelles Lernen", auf. Der folgende Beitrag soll grundlegend erklären, was unter Machine Learning zu verstehen ist und anhand von kurzen Beispielen seine Anwendungsfelder aufzeigen. Hier soll ein erster Überblick über die Funktionsweise von Verfahren des maschinellen Lernens gegeben werden.

A. Definitionsansatz

In Literatur und Wissenschaft findet man vielfältige Definitionsansätze für den Begriff Machine Learning. Weitreichende Einigkeit besteht darüber, dass Machine Learning einen Teilbereich von KI[1] darstellt. Es gilt als Schlüsseltechnologie für KI-Systeme. Das Gabler Wirtschaftslexikon definiert Machine Learning als „Anwendung und Erforschung von Verfahren, durch die Computersysteme befähigt werden, selbstständig Wissen aufzunehmen und zu erweitern, um ein gegebenes Problem besser lösen zu können als vorher (Learning)". Im Kern geht es somit um selbstständiges Lernen auf Grundlage von großen Datenmengen. Dies geschieht durch Algorithmen,[2] die eigenständig Muster erkennen und nutzbar machen.

1 *Lihotzky*, CTRL 2021, S. 4 ff.

2 Vgl. zum Begriff Algorithmus: https://wirtschaftslexikon.gabler.de/definition/algorithmus-27106/version-250769 (zuletzt abgerufen am 9.1.2021).

B. Wofür kann Machine Learning eingesetzt werden?
Maschinelles Lernen dient der Bewältigung von Fragestellungen, die zu umfassend oder variabel sind, als dass ein Mensch sie erfassen könnte. Es geht darum, „Wissen" aus „Erfahrung" zu generieren. Ein IT-System soll auf Basis vorhandener Daten Muster und Gesetzmäßigkeiten erkennen. Mithilfe der gewonnenen Erkenntnisse können in der Folge neue Problemlösungen entwickelt oder unbekannte Daten analysiert werden.

In der sogenannten Trainingsphase, die der Anwendung vorausgehen muss, soll das System eigenständig eine Lösung für ein spezifisches Problem erarbeiten. Der Programmierer legt im Vorfeld nur die Lernregeln fest. Damit das funktionieren kann, benötigt der Lernalgorithmus Trainingsdaten, auf Grundlage derer er komplexe Wissensmodelle entwickeln kann. Jene erlernten Modelle kann er anschließend auf neue, unbekannte Daten anwenden, um eine Prognose zu treffen, eine Empfehlung abzugeben oder eine Entscheidung zu generieren.
Die Zuverlässigkeit des vom Lernalgorithmus errechneten Modells hängt dabei entscheidend von der Qualität und Quantität der zugrundeliegenden Trainingsdaten ab. Je größer und repräsentativer der Beispiel-Datensatz ist, der dem System zur Verfügung gestellt worden ist, desto zuverlässiger sind auch die vom Lernalgorithmus getroffenen Voraussagen.

C. Formen des Machine Learnings
Grundprinzip des maschinellen Lernens ist das Erkennen von Mustern aufgrund eines Datenpools. Nach Abschluss der Kalibrierung kann das System Vorhersagen treffen. Dabei lassen sich beim Machine Learning unterschiedliche Lernstile, Lernaufgaben, Lernverfahren oder -modelle unterscheiden.
Bei der Unterscheidung nach Lernstilen wird typischerweise zwischen dem überwachten und unüberwachten Lernen unterschieden.

I. Überwachtes Lernen (Supervised Learning)
Beim überwachten Lernen muss das System in der Trainingsphase mit ausreichend Trainingsdaten gespeist werden. Bei den Trainingsdaten muss es sich um sogenannte gelabelte Daten handeln. Das bedeutet, dass die Trainingsdaten immer aus Input-Output-Paaren bestehen müssen, sodass die zu erlernenden Antworten auf die jeweilige Fragestellung dem System während des Trainings von Anfang an bekannt sind.
Die Lernaufgabe des Systems besteht im Erkennen und Abbilden von Beziehungen und Zusammenhängen zwischen der Input- und der Output-Größe. Durch überwachte Lernverfahren soll ein Modell entstehen, das den Zusammenhang zwischen Input und Output verallgemeinert, sodass für einen unbekannten Input ein sinnvoller Output vorhergesagt werden kann.

Am Beispiel der Erkennung und Unterscheidung von Verkehrsschildern auf Bildern bedeutet das, dass dem System zu Beginn zahlreiche Bilder von Verkehrsschildern (etwa Stoppschilder, Parkverbotsschilder, Einbahnstraßenschilder, etc.) mit ihren korrekten Bezeichnungen zur Verfügung gestellt werden müssen.

Das System muss dann während des Trainingsprozesses eigenständig Kriterien entwickeln, anhand derer es die einzelnen Schilder voneinander unterscheiden kann, um dann bei unbekannten Bildern zukünftig bestimmen zu können, welches Verkehrsschild abgebildet ist.

II. Unüberwachtes Lernen (Unsupervised Learning)
Im Gegensatz zum überwachten Lernen ist das unüberwachte Lernen dadurch gekennzeichnet, dass dem Lernalgorithmus anstelle von Input-Output-Datenpaaren nur Input-Daten zur Verfügung stehen.

Der Algorithmus soll dann allein aus jenen Daten Erkenntnisse gewinnen. Allerdings kann auf diese Weise kein Zusammenhang zwischen Input und Output ermittelt werden. Stattdessen können die Daten beispielsweise strukturiert werden. Je nach Art des Problems, kann das System die Daten auf verschiedene Weisen strukturieren.

Beim sogenannten Clustering, einer Form unüberwachten Lernens, geht es darum, die gegebenen Daten in eine sinnvolle Struktur in Form von Clustern zu bringen. Während des Lernprozesses erstellt das System mehrere Cluster. Durch die Anwendung des Modells könnte dann ein neuer Input einem Cluster zugeordnet werden.
Ein derartiges Lernverfahren eignet sich beson-

ders zur Anomalieerkennung. Wenn die Input-Daten das Normalverhalten eines Systems abbilden, kann das Modell anschließend für aufgezeichnetes Verhalten abnormale Abweichungen im Verhältnis zu den Trainingsdaten ermitteln. Anwendungsbeispiele sind etwa Vorhersagemodelle zur Wartung von Maschinen oder zur Prognose von Zielobjekten von Einbrüchen.

D. Künstliche neuronale Netze und Deep Learning

Machine Learning kann auch durch den Einsatz künstlicher neuronaler Netze realisiert werden. Dies funktioniert sowohl mit überwachten als auch mit unüberwachten Verfahren.

Künstliche neuronale Netze werden nach dem Vorbild der Neurophysiologie menschlicher Gehirne entworfen. Die einzelnen Bestandteile künstlicher neuronaler Netze werden Neuronen genannt, stellen Rechenknoten dar und werden durch mathematische Funktionen nachgebildet. Zwischen den Neuronen bestehen gewichtete Verbindungen (sogenannte Synapsen), das heißt, dass der Input, der an ein Neuron gegeben wird, unterschiedlich gewichtet wird. Im Neuron wird der Input aufsummiert. Sobald ein definierter Grenzwert erreicht ist, wird das Neuron aktiviert und gibt eine Ausgabe an das nächste Neuron.

Regelmäßig werden die Neuronen in unterschiedlichen Schichten zusammengefasst.
Es gibt eine Input-Schicht, eine Output-Schicht und dazwischen befinden sich eine oder mehrere versteckte Schichten (Hidden Layers).
Bei Netzwerken mit besonders vielen Hidden Layers spricht man von tiefen neuronalen Netzwerken.

Der Lernprozess wird Deep Learning genannt. Die Hidden Layers spielen eine große Rolle für das Erlernen von Wissenszuständen und Zusammenhängen, weswegen sich tiefe neuronale Netze besonders für sehr komplexe Aufgabenstellungen eignen, bei denen viele Einflussfaktoren eine Rolle spielen.

Beispielsweise könnte man Deep Learning zum Errechnen von Grundstückspreisen anhand der Lage, der Grundfläche und anhand der Preise umliegender Grundstücke sowie vieler weiterer Faktoren einsetzen, die eine Berechnung ansonsten sehr zeitaufwendig machen würden.
Ein überwacht lernendes neuronales Netz hat in der Trainingsphase die Aufgabe, Zusammenhänge und Korrelationen zwischen den In- und Output-Daten zu ermitteln. Die Stärke, mit der ein Neuron auf eine Input-Information reagiert oder sie weiterleitet, lässt sich durch die oben erwähnten Gewichte der Verbindungen und die Festsetzung der Grenzwerte bestimmen. Man startet mit einer zufälligen Gewichtung. Das System kann dann während des Lernprozesses selbstständig Veränderungen vornehmen. Es errechnet entsprechend der gewählten Gewichtung den Output und vergleicht das errechnete Ergebnis mit dem vorgegebenen Output. Durch Anpassung der Gewichtungen während des Prozesses erreicht das System, dass vorgegebener Output und errechneter Output übereinstimmen.

Auch künstliche neuronale Netze können zur Bilderkennung angewendet werden.
Ein bekanntes Beispiel ist das Erkennen von Katzen in Fotos. Hierzu wird das neuronale Netz während der Trainingsphase mit Pixeln eines Katzenfotos gespeist. Diese Daten werden in den Neuronen verrechnet und weitergeleitet. Das System gibt dann am Ende aus, mit welcher Wahrscheinlichkeit sich auf dem gezeigten Bild eine Katze befindet. Anhand der Ergebnisse wird die Gewichtung der Neuronen so lange angepasst, bis das neuronale Netz eine Vielzahl von Katzenbildern sicher erkennt.

E. Ausblick

Machine Learning wird hauptsächlich dann angewendet, wenn die verfügbaren Datenmengen zu groß sind, als dass einzelne Menschen sie analysieren könnten. Es hat über die genannten Beispiele hinaus ein weites Anwendungsfeld und spielt insbesondere im Kontext von Gesichtserkennung, Spracherkennung und -verarbeitung, automatisiertem Fahren und Empfehlungsdiensten (Recommendation-Engines) eine bedeutende Rolle. Allerdings stellen sich Probleme, die unter anderem mit der Qualität, Verfügbarkeit und Repräsentativität von Trainingsdatensätzen zusammenhängen. Auch Nachvollziehbarkeit und Transparenz von Machine-Learning-Anwendungen sind viel diskutierte Themen. Welche weiteren technischen Neuerungen Machine Learning ermöglichen wird, bleibt abzuwarten.

Weiterführend:

Um das Verständnis von Machine Learning, seinen Potentialen und Risiken zu vertiefen, bieten sich unter anderem die folgenden Beiträge an, die auch die Grundlage dieses Beitrags bilden.

https://www.bigdata.fraunhofer.de/content/dam/bigdata/de/documents/Publikationen/Fraunhofer_Studie_ML_201809.pdf, zuletzt abgerufen am 9.1.2021

https://blogs.nvidia.com/blog/2018/08/02/supervised-unsupervised-learning/, zuletzt abgerufen am 9.1.2021

https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/kuenstliche-intelligenz/kuenstliche_intelligenz_node.html, zuletzt abgerufen am 9.1.2021

https://medium.com/@yasminehamdi/the-story-of-machine-learning-7ac3e8a5eaf9, zuletzt abgerufen am 9.1.2021

https://wirtschaftslexikon.gabler.de/definition/maschinelles-lernen-38193/version-261619, zuletzt abgerufen am 9.1.2021

Bilski/Schmid, NJOZ 2019, S. 657 ff., „Verantwortungsfindung beim Einsatz maschinell lernender Systeme“

von Bünau, Paul, Künstliche Intelligenz, in: Rechtshandbuch Legal Tech, hrsg. von Stephan Breidenbach u. Florian Glatz, 2018, Kap. 3, S. 47-59

Burgstaller/Hermann/Lampesberger, Künstliche Intelligenz - rechtliches und technisches Grundwissen, 2019

Zech, ZfPW 2019, S. 198 ff. (200 f.), „Künstliche Intelligenz und Haftungsfragen“

Talking Legal Tech - Folge 25
„künstliche Intelligenz- was ist das eigentlich, manuela lenzen?“