Maschinelles Lernen 2022

Aktuelle Trends und deren Relevanz

www.bitkom.org

bitkom

Herausgeber

Bitkom
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin
T 030 27576-0
bitkom@bitkom.org
www.bitkom.org

Autoren

Claudia Pohlink | Deutsche Bahn AG
Andreas Klug | ITyX AG
Jörg Besier | Curaluna GmbH
Jörg Niestroj | omni:us GmbH
Nicole Ofenloch-Wendel | IBM Deutschland GmbH
Mathis Börner | SAP SE

Projektleitung

Merle Uhl | Bitkom e. V.

Satz & Layout

Katrin Krause | Bitkom e. V.

Titelbild

© Daniel van den Berg | unsplash.com

1 Vorwort

Für viele Branchen und Unternehmen ist Machine Learning (ML) eine wichtige Schlüsseltechnologie geworden. So gibt es mittlerweile einige Use Cases für Machine Learning-Technologien, in denen diese produktiv eingesetzt werden können und werden. Im Gartner Hype Cycle, einer Methodik zur Abschätzung der Entwicklung von Technologien, ist Machine Learning damit über den Punkt des »Gipfel der überzogenen Erwartungen« weit hinaus – aber auch über das »Tal der Enttäuschungen« hinweg.

»Zwei Drittel der Unternehmen halten KI für die wichtigste Zukunftstechnologie.[1]«

Anfang des letzten Jahres hat der Bitkom einige der **↗Innovationsthemen und Trends für 2021** vorgestellt. Ein Jahr später soll nun eine kurze Rückblende der beleuchteten Trends durchgeführt sowie ein neuer Ausblick für die Machine Learning-Trends 2022 gewagt werden.

Der Trend in Richtung »Robust AI«, also störunanfälligere Künstliche Intelligenz (KI), ist ungebrochen. Das Risiko des Missbrauchs wird weiterhin als hoch angesehen, aber entsprechende Lösungen stecken immer noch in den Kinderschuhen.

In der Praxis längst angekommen sind dagegen Lösungen für das Feld der »Explainable AI«, wo es schon für viele der genutzten Machine Learning-Methoden Möglichkeiten im Produktiveinsatz gibt. Aber auch hier gibt es noch viel Forschungs- und Weiterentwicklungspotenzial.

Im Bereich Quantum ML gibt es Fortschritte in der Hardware, wo IBM im letzten Herbst mit einem 127 Qubits Quantumprozessor die 100-Qubit Schallmauer durchbrochen hat und am Forschungszentrum in Jülich der erste Quantencomputer mit mehr als 5000 außerhalb Nordamerikas anlief. Das zeigt, dass gerade der Standort Europa immer wichtiger wird. Aber auch in der Software für Machine Learning-Anwendungen für Quantencomputer gibt es mit Weiterentwicklungen wie z.B. Tensorflow und dem Release 0.5 für verteiltes Rechnen Mitte 2021 weitere Fortschritte.

Eine schnelle Weiterentwicklung gibt es auch im Bereich Auto ML: Selbstlernende Systeme sind durch immer größere Datenmengen, die von Menschen nicht mehr verarbeitbar sind, nach wie vor als ein wichtiger Pfeiler für weitere Fortschritte in der KI angesehen.

Für Emotion AI war Covid-19 und die durch Corona ausgelöste Digitalisierungswelle ein Booster. Um die Gefühlslage von Menschen in Mails, Videocalls und Chats zu kennen und zu verstehen, ist Emotion AI ein gutes Instrument.

Dass es bis zum »Plateau der Produktivität« im Gartner Hype Cycle aber noch weiteres Innovations- und Wachstumspotential gibt, zeigt sich an den vielen Forschungsthemen im Bereich Machine Learning. Der Bitkom hat aus dem breiten Spektrum der Themen einige Trends identifiziert, die die Weiterentwicklung von Machine Learning weiter prägen werden.

»Der Anteil von Unternehmen, die KI einsetzen, steigt, liegt 2021 aber immer noch erst bei 8 Prozent.[1] Das Thema des Arbeitskreises AI für 2022 ist daher ›AI beyond the Hype: The Path from Innovation to Production‹«

1 Dies ergibt sich auch einer **↗Studie**, die 2021 von Bitkom Research im Auftrag des Digitalverbands Bitkom durchgeführt wurde

2 Data-Centric AI

In den letzten Jahren haben neue Modelle und neue Architekturen für große Schlagzeilen und Durchbrüche in der Forschung gesorgt. Wenn man schaut, wie viele dieser Entwicklungen in der Praxis angekommen sind, fällt das Fazit in den meisten Fällen momentan aber noch eher ernüchternd aus. Auch bei Befragungen von Anwendenden zeigt sich immer wieder, dass die Probleme von KI in der Praxis nicht bei den Modellen bzw. Modellarchitekturen liegen, sondern überwiegend in den Daten.

In der Praxis hat man es bei nahezu jeder Anwendung immer wieder mit komplett neuen Daten zu tun. In dieser Tatsache liegt die Ursache für viele Probleme, aber auch das große Potenzial, den Umgang mit Daten ins Zentrum der KI-Entwicklungsprozesse zu stellen. Bessere Werkzeuge für den Umgang mit Daten versprechen hohe Zeit- und Kostenersparnis bei der Entwicklung und können durch Verbesserung der Datenqualität neue Anwendungen ermöglichen. Das macht sie zu einem notwendigen Baustein für die weitere Industrialisierung von KI-Anwendungen.

Unter dem Schlagwort Data-Centric AI wird also der Fokus weniger auf die Modellierung, sondern vielmehr auf die Daten selbst gelegt. Eine Gruppe von Forschenden und Unternehmerinnen und Unternehmern rund um Andrew Ng (Mitgründer von Google Brain und Coursera) hat den Begriff geprägt und veranstaltet Workshops und Challenges zu dem Thema. Ziel ist es, Techniken und Werkzeuge für den Umgang mit Daten zu erforschen und zu entwickeln, mit denen die Datenqualität über den gesamten Lebenszyklus einer KI-Anwendung verbessert werden kann.

Dabei sollen alle Prozesse, angefangen bei der Datenerfassung, über das Labeln der Daten bis zu Datenaufbereitung, in den Fokus genommen und verbessert werden.

3 ML Ops

Mit ML Ops (der Kombination von Machine Learning und Dev Ops) fasst man alle Prozesse zusammen, die dafür sorgen, dass ein KI-Modell dauerhaft betrieben und weiterentwickelt werden kann. Um dies zu erreichen wird bei ML Ops der gesamte Lebenszyklus eines Modells begleitet. Der Fokus liegt dabei auf dem Management von Modelliterationen (Versionierung), dem Monitoring des Betriebs, der Governance und der Sicherheit der Modelle.

Mit jedem Modell, das die Prototypenphase verlässt, steigt der Bedarf an ML Ops. Folglich hat das Thema in den letzten beiden Jahren immer mehr Beachtung gefunden und an Fahrt aufgenommen. Schätzungen gehen davon aus, dass bereits im Jahr 2025 der Markt für ML Ops 4 Milliarden US-Dollar stark sein wird. Aktuell ist der Markt geprägt von Startups. Der Wettbewerb sorgt für rasante Entwicklungen, die sich auch im Jahr 2022 nicht verlangsamen werden.

Prozesse des Modell-Managements sind dabei stets eng verzahnt mit dem Datenmanagement. Auch deshalb wird ML Ops häufig im Zusammenhang mit Data-Centric AI genannt. ML Ops ist

»60 Prozent der Unternehmen wünschen sich mehr Austausch mit Firmen, die bei KI bereits weiter sind. Im AK ›Artficial Intelligence‹ versuchen wir mit Schwerpunkten wie ML Ops den Dialog hierzu zu ermöglichen.[2]«

2 Dies ergibt sich auch einer ↗**Studie**, die 2021 von Bitkom Research im Auftrag des Digitalverbands Bitkom durchgeführt wurde

ein weiterer entscheidender Baustein für die Industrialisierung von KI-Anwendungen, ohne den ein langfristiger und rentabler Betrieb von KI-Anwendungen nicht möglich sein wird.

4 AI Ethics

Neben der moralischen Verpflichtung, bei KI-Anwendungen ethische Prinzipien zu berücksichtigen, wird es durch Regulierungen wie den EU AI Act auch bald gesetzliche Verpflichtungen geben. In dem risikobasierten Ansatz des AI Acts werden selbst für komplett risikoarme Anwendungen ein Code of Conduct und das Bekenntnis zu grundlegenden Prinzipien gefordert. Sobald eine Anwendung risikobehaftet ist, ziehen sich die daraus folgenden Aufgaben durch den gesamten Entwicklungs- und Lebenszyklus der Anwendung. Entsprechend wichtig ist, dass alle Beteiligten das Risiko ihrer Anwendung früh erkennen. Dabei wird es beim Thema KI-Ethik ähnlich sein wie im Alltag: Diejenigen, die über ein gefestigtes Fundament verfügen und in der Auseinandersetzung mit ethischen Fragestellungen geübt sind, haben weniger Probleme, potentielle Konflikte zu erkennen und können sie angehen, bevor Schaden entsteht.

*»In einer **↗Arbeitskreis-Sitzung des AK ›Artficial Intelligence‹** zur Operationalisierung von KI-Ethik betrachten wir den Schritt von Grundsätzen hin zur Praxis.«*

Neben der Entwicklung von ethischen Grundsätzen bedarf es auch praktischer Strategien zur Erkennung von Problemen und zum Umgang mit konkreten Fragestellungen.

Auf dem Gebiet der KI-Ethik wird schon seit einigen Jahren geforscht und viele Firmen haben angefangen, Schulungen und Grundsätze zu entwickeln. Jedoch zeigen Umfragen und Studien immer wieder, dass diese Bemühungen oft wenig Auswirkungen auf die Praxis haben. Währenddessen nehmen die Erwartungen der Nutzerinnen und Nutzer und der Politik mit jeder neuen KI-Anwendung zu. Ohne die Auseinandersetzung mit ethischen Fragestellungen und ohne die Etablierung von darauf basierenden Strategien werden die Entwicklung und der Betrieb von KI-Anwendungen in absehbarer Zukunft nicht mehr möglich sein.

5 Sustainable AI

Bei der Entwicklung von KI-Systemen gewinnt Sustainable AI immer mehr an Bedeutung. Dabei spielen die drei Dimensionen der Nachhaltigkeit – Ökonomie, Ökologie und der soziale Kontext – eine zentrale Rolle.

»30 Prozent der Unternehmen erwarten einen geringeren Ressourcenverbrauch durch KI – auch solche Entwicklungen spielen für Sustainable AI eine Rolle.[3]«

Sustainable AI beschäftigt sich damit, wie es gelingen kann, die Umweltkosten von Künstlicher Intelligenz zu messen und politische Entscheidungstragende bei der Erstellung von Richtlinien zu unterstützen.

Für Unternehmen kann die Nichteinhaltung dieser Standards künftig zu einem erheblichen Nachteil führen. Es ist jedoch möglich, einen praktischen Ansatz für das Design, die Entwicklung und den Einsatz von nachhaltigen KI-Systemen zu verfolgen, der sowohl wirtschaftliche als auch menschliche Werte und Prinzipien berücksichtigt.

3 Dies ergibt sich auch einer **↗Studie**, die 2021 von Bitkom Research im Auftrag des Digitalverbands Bitkom durchgeführt wurde

Um Unternehmen bei der Erreichung dieses Ziels zu unterstützen, bietet sich ein sogenanntes Sustainable Artificial Intelligence Framework an, das als Leitfaden für die Entwicklung und den Einsatz von KI-Systemen dienen kann. Dabei wird sich auf die Bereiche konzentriert, die sich auf die sozioökonomischen und politischen Auswirkungen von KI beziehen. So wird ein Umfeld erzeugt, in dem eine Organisation lernt, ihre Risiken und ihre Anfälligkeit für unerwünschte Folgen von KI zu verstehen. Gleichzeitig ergibt sich das Potenzial kurz-, mittel- und langfristig Werte zu schaffen.

Sustainable AI stellt sicher, dass AI abgestimmt ist mit den Anforderungen aus Security, Data Privacy und Fairness.

6 Differential Privacy

»Beim ↗#BAS22 betrachten wir unter ›Trust-Enhancing Technologies‹ Möglichkeiten, Privacy zu gewährleisten.«

Mit Zunahme der Datenmengen wächst für die Unternehmen auch die Notwendigkeit, die sensiblen Daten während der Verarbeitung zu schützen und dennoch so viele Erkenntnisse bzw. Nutzungsmuster wie möglich daraus zu ziehen. Bekannte Verfahren wie Anonymisierung und Pseudonymisierung sind nicht sicher genug, wie das **↗Netflix/IMDB Beispiel** von 2007 bereits zeigte.

Seither beschäftigt sich die Forschung damit, welche weiteren Methoden möglich sind, den Rückschluss auf einzelne Personen bei der Verarbeitung und Auswertung zu verhindern.

Den Grundstein für Differential Privacy legten Cynthia Dwork, Frank McSherry, Kobbi Nissim und Adam Smith bereits vor 14 Jahren in ihrem Paper »Calibrating Noise to Sensitivity in Private Data Analysis«.

Den Datensätzen wird ein »mathematisches« Rauschen hinzugefügt, indem einem ursprünglichen Datensatz zufällige bzw. künstliche Daten hinzugefügt werden. Wird das Rauschen zu groß, können die Ergebnisse auch unbrauchbar werden. Daher ist es nötig, den Verlust der Privatsphäre und die Genauigkeit der Ergebnisse mit einem Parameter Epsilon ε abzuwägen. Je höher der Wert von Epsilon, desto präziser werden die Ergebnisse – aber die Anonymität leidet darunter.

Apple verwendet dieses Verfahren bereits seit 2016, um lokal häufig verwendete Emojis vorzuschlagen. Google nutzt es bei Mobilitätsstatistiken und der US-Zensus bei der aktuellen Volkszählung.

Viele Wissenschaftlerinnen und Wissenschaftler fordern inzwischen mehr Transparenz von den Unternehmen, ihre Privacy-Parameter (Epsilon) offenzulegen, damit von »echter« Differential Privacy gesprochen werden kann.

Bitkom vertritt mehr als 2.000 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom