Algorithmen

was ist das?

Immer öfters sind Schlagzeilen wie „Algorithmen – die heimliche Weltmacht“ oder „Beherrschen Algorithmen unseren Alltag?“ zu lesen, insbesondere im Zusammenhang mit Big Data. In diesem Dossier erklären wir, was Algorithmen eigentlich sind, wie sie funktionieren und was für Anwendungen sie haben. Außerdem gehen wir auf die ethischen Bedenken ein.

Ein Algorithmus ist eine eindeutige, logische Anweisung oder Regel, wie ein Problem zu lösen ist und besteht aus Einzelschritten, die nacheinander oder gleichzeitig ausgeführt werden. Eine bestimmte Eingabe führt (bei den allermeisten Algorithmen) immer zu der gleichen Ausgabe. Algorithmen sind meistens in der Form von Computerprogrammen umgesetzt, können aber auch in menschlicher Sprache formuliert werden. Das einfachste Beispiel für einen Algorithmus im Alltag ist ein Kochrezept.

Woher stammt der Name?

Der Name Algorithmus leitet sich vom Namen des choresmischen Gelehrten und Mathematiker Abu Dscha'far Muhammad ibn Musa al-Chwarizmi ab, der aus dem Gebiet des heutigen Irans stammte und den größten Teil seines Lebens in Bagdad lebte. Er verfasste im Jahr 825 ein Lehrbuch „Über die indischen Ziffern“ und erklärte darin auch die Funktionsweisen von Algorithmen. Das Buch, das die Ziffern behandelte, die wir heute als „arabische Ziffern“ kennen, wurde im 12. Jahrhundert auf Latein übersetzt. Dabei wurde der letzte Teil seines Namens (al-Chwarizmi) zu „Algorismi“. Die Anfangsworte lauteten „*Dixit Algorismi*“ (Algorismi hat gesagt), woraus schließlich der Begriff Algorithmus wurde.

Eigenschaften eines Algorithmus

Alle Algorithmen teilen bestimmte Eigenschaften, die sie ausmachen.

Eindeutigkeit: Jeder Algorithmus muss eindeutig sein, das heißt er darf keine Anweisungen haben, die sich widersprechen

Ausführbarkeit: jeder einzelne Schritt muss ausführbar sein (also darf z.B. keine Division durch Null enthalten sein)

Endlichkeit: der Algorithmus muss ein definiertes Ende haben, also nicht unendlich weiterlaufen.

Terminierung: nach endlich vielen Schritten muss der Algorithmus enden und ein Ergebnis liefern

Determiniertheit: bei den gleichen Inputs muss der Algorithmus stets den gleichen Output, also das gleiche Ergebnis liefern

Determinismus: Jeder Folgeschritt ist eindeutig bestimmt, es besteht also nach jedem Schritt nur eine eine Möglichkeit, was der nächste Schritt ist.

Zur computergestützten Lösung von Problemen gibt es jedoch nicht nur Algorithmen. Mittlerweile gibt es auch andere Werkzeuge, die jedoch immer in irgendeiner Form auf Algorithmen basieren.

Heuristiken

Obwohl wir heute über gewaltige Rechenpower verfügen, können manche Aufgaben nicht in zufriedenstellender Zeit von Algorithmen gelöst werden. Ein Beispiel wäre die optimale Route für einen Lieferdienst, der Pakete mehrere Kunden in einem Gebiet zustellen soll. Für solch ein Problem existiert zwar eine perfekte, optimale Lösung – die zu finden ist jedoch sehr zeitaufwändig.

Eine Heuristik wird dann angewandt, wenn ein einfacher Algorithmus zu langsam wäre. Eine Heuristik basiert oft auf Zufallsvariablen. Der „Greedy-Algorithmus" ist eine Heuristik, die in jedem Schritt jene Alternative auswählt, die am erfolgversprechendsten aussieht. Dadurch findet diese Heuristik sehr schnell eine Lösung, diese ist aber oft nicht die optimale Lösung. Heuristiken sind schneller als Algorithmen, aber auch fehleranfälliger.

Künstliche Intelligenz

Künstliche Intelligenz wird auch Artifizielle Intelligenz (englisch *artificial intelligence)* genannt und als KI oder AI abgekürzt. Mithilfe von Programmen soll intelligentes Verhalten simuliert werden. Der Begriff ist problematisch, weil es keine genaue Definition von „Intelligenz" gibt. Grundsätzlich wird versucht, menschenähnliche Intelligenz nachzubauen – der Computer soll eigenständig Probleme bearbeiten können. Ein wichtiges Forschungsgeld, das sich im Bereich der KI in den letzten Jahren aufgetan hat, sind sogenannte „künstliche neuronale Netzwerke", die auf ein Modell der Nervenzellen des menschlichen Gehirns aufbauen. Eng verknüpft damit sind auch die Begriffe „Deep Learning" bzw. „Machine Learning".

Infobox: Turing-Test

Wie bestimmt man, ob eine Maschine als intelligent gilt? Für diese Aufgabe hat der britische Mathematiker Alan Turing den nach ihm benannten Turing-Test entwickelt. Ohne Sicht- und Hörkontakt (etwa in einem Chat) unterhält sich dabei ein menschlicher Fragesteller mit zwei Personen, einem Menschen und einer Maschine. Beide sollen versuchen, den Tester davon zu überzeugen, dass sie menschlich sind.

Wenn der Tester nicht mit Sicherheit sagen kann, welche der beiden Gesprächspartner ein Mensch ist, hat die Maschine den Test bestanden. Bisher ist es noch keiner KI gelungen, den Turing-Test zu bestehen – in letzter Zeit gab es allerdings Fortschritte. So hat die University of Chicago im August 2017 eine KI vorgestellt, die Rezensionen (etwa von Restaurants) schreiben konnte, die nicht von jenen unterschieden werden konnten, die von Menschen geschrieben waren.

Machine Learning

Machine Learning, auf Deutsch auch manchmal „Maschinelles Lernen" genannt, bezeichnet eine spezielle Art der KI: Ein System lernt aus Beispielen kann am Ende einer Lernphase diese Beispiele verallgemeinern. Das System erkennt Muster und Regelmäßigkeiten aus den Lerndaten und kann diese (im besten Fall) auf neue Daten anwenden. Maschinelles Lernen ist ein selbstadaptiver Algorithmus – die Maschine verbessert sich (wenn alles so läuft wie geplant) also selbst.

Eine der Methoden, die zur Umsetzung der Lernphase angewandt werden, nennt sich „Deep Learning" (tiefgehendes Lernen). Hierbei werden künstliche neuronale Netze verwendet, die viele Zwischenschichten, die „hidden Layers" genannt werden, zwischen Input und Output haben. Diese Schichten sind – grob gesagt – wie die Neuronen im menschlichen Gehirn organisiert. In jeder Schicht werden die Informationen aus der Eingabeschicht abstrahiert und verallgemeinert. Dadurch ist es möglich, dass ein Computer komplizierte Konzepte „lernt", indem er sie aus einfacheren

zusammensetzt. Während es sehr schwierig wäre, das benötigte Wissen (z.B. Handschrifterkennung) manuell zu programmieren, kann dies mit Machine Learning bewältigt werden, ohne dass ein Mensch die Informationen formalisieren muss. Beispiele für Anwendungen, die mit Machine Learning realisiert werden können, sind automatisierte medizinische Diagnoseverfahren, Erkennung von Kreditkartenbetrug, Aktienmarktanalysen, DNA-Analyse, Sprach-, Schrift- und Texterkennung sowie autonome Systeme wie selbstfahrende Autos.

Data-Mining

Data-Mining bedeutet übersetzt „Daten fördern“ (wie in einem Bergwerk, einer Mine). Der Begriff ist etwas irreführend, denn es geht nicht darum, neue Daten zu fördern, sondern aus dem vorhandenen „Datenberg“ neue Querverbindungen, Trends und Verknüpfungen herauszufiltern. Data-Mining ist eng verwandt mit Machine Learning und es kommen oft die gleichen Algorithmen zu Anwendung. Das Ziel ist jedoch, *neue* Muster und Gesetzmäßigkeiten zu finden, während beim Machine Learning der Computer die gegebenen Muster erkennen soll. Dabei kommen oft statistische Methoden und Algorithmen zur Anwendung. So werden bei der Ausreißer-Analyse jene Daten gefunden, die nicht zum Rest des Datenberges passen – dies ist zum Beispiel dann hilfreich, wenn Kreditkartenbetrug erkannt werden soll.
Andere Methoden des Data-Minings fassen Daten in bestimmte Gruppen zusammen (bspw. bei der Cluster- und der Klassifikationsanalyse) oder suchen nach Zusammenhängen zwischen Daten (wie bspw. die Regressions- und Assoziationsanalyse). So entstehen zum Beispiel die bekannten „Kunden, die dieses Produkt gekauft haben, kauften auch …“-Anzeigen in Onlineshops.

Infobox: Algorithmen to go: Wer steckt hinter Machine Learning-Anwendungen?

Aktuell gibt es einen regelrechten Hype um Machine Learning – viele Firmen und Webseitenanbieter versuchen, ihre Daten mit diesen neuen Methoden auszuwerten. Aber nur wenige haben selbst das Know-How und die Rechenpower, um eigene Machine Learning-Anwendungen zu entwickeln. Wie so viele Dienstleistungen werden auch Machine Learning-Applikationen in der Cloud angeboten. Dabei gibt es aktuell vier große Anbieter, die keine Unbekannten sind: Microsoft mit Microsoft Azure, IBM mit IBM Watson Machine Learning, Google mit seiner Google Cloud Platform und Amazon mit Amazon Machine Learning. Je nach Anbieter sind unterschiedliche Vorkenntnisse nötig bzw. unterschiedliche Einblicke in die Prozesse möglich. Der Machine Learning-Service von Amazon ist extrem nutzerfreundlich und benötigt wenig Kenntnisse, funktioniert allerdings als „black box“ – es ist also als Außenstehender von Amazon nicht möglich, genau zu sehen und zu verstehen, welche Algorithmen am Werk sind.

Anwendungen

Algorithmen sind, wie weiter oben schon erwähnt, hunderte Jahre alt. Dementsprechend sind sie schon lange Zeit in unserem Leben und fallen uns oft gar nicht auf, denn auch z.B. Kochrezepte und Gesetze sind eigentlich Algorithmen. Dennoch haben wir eine (natürlich unvollständige) Liste mit Beispielen zusammengestellt, wo die oben erwähnten Techniken zum Einsatz kommen:

Finanzsektor: Zur Erkennen von Betrugsversuchen und beim Credit-Scoring, um einschätzen zu können, welchen Kunden mit welchem Risiko ein Kredit gewährt werden kann.

Marketing: Auswahl von Zielgruppen („Wie muss Werbung gestaltet werden, damit sie unsere Kunden erreicht?“), Warenkorbanalyse („Welche Produkte werden gemeinsam gekauft?“ – nach diesen Erkenntnissen werden Supermärkte gestaltet), Kundenprofile („Was kauft dieser Kunde? Woran könnte er noch interessiert sein?“)

Medizin: neue Wirkstoffe für Arzneimittel analysieren, Überwachung von Nebenwirkungen

Industrie: automatisierte Prozesse sind durch Algorithmen gesteuert, aber durch Data Mining und Machine Learning lassen sie sich kontinuierlich verbessern, zum Beispiel in der chemischen Industrie und der Kunststoffverarbeitung

Internet: gerade im Netz spielen Algorithmen, KI, Machine Learning und Data Mining eine große Rolle. So gibt es zum Beispiel folgende Anwendungen:

- IT-Sicherheit: Angriffserkennung (intelligente Firewall)
- Nutzererlebnis in sozialen Medien: basiert zum Großteil auf Netzwerkanalysen in sozialen Netzwerken, ermöglicht z.B. die Empfehlung von neuen Freunden auf Facebook
- Analyse des Nutzerverhaltens: bspw. mithilfe von Logfiles, Cookies und anderen Daten, die Nutzer auf Webseiten hinterlassen
- Empfehlungsdienste für Produkte, Musik oder Filme, z.B. beim Streaming-Dienst Netflix.

Sicherheitstechnik: Gesichtserkennung und Erkennen von „verdächtigem Verhalten“ bei Videoüberwachung, Terrorverdacht

Es gibt kaum Grenzen für die Anwendungsgebiete, in denen komplexe Algorithmen und Techniken wie Machine Learning zum Einsatz kommen. Die Firma hudl gibt zum Beispiel an, dass sie mit Hilfe von Videoanalyse und Machine Learning Sportlern hilft, sich auf Wettkämpfe vorzubereiten, während das Start-Up „Upserve“ Restaurants helfen will, die Gästezahlen vorherzusagen – und sogar, welche Speisen Gäste dazu veranlassen, das Lokal ein weiteres Mal zu besuchen.

Ethische Bedenken und Probleme

Seit einiger Zeit werden immer wieder Bedenken über Algorithmen geäußert. Schlagzeilen wie „Algorithmen – die heimliche Weltmacht“ oder auch „Zwei Chatbots haben eine eigene Sprache entwickelt“ könnten einen glauben lassen, Algorithmen an sich wären „böse“ - dabei sind sie lediglich Werkzeuge. Welche Probleme und ethischen Bedenken sich ergeben, hängt davon ab, wozu, wie und von wem sie programmiert werden – und natürlich, wie und zu welchem Zweck sie eingesetzt werden.

Aufgaben, die die meisten Menschen ohne Probleme meistern können – zum Beispiel, ein Gesicht zu erkennen oder ein Tier oder ein Objekt auf einem Foto zu bestimmen, stellen Computer vor große Schwierigkeiten – oft auch dann, wenn die Algorithmen durch einen sogenannten "DeepLearning"-Prozess gegangen sind und dabei an tausenden von Bildern trainiert wurden, Objekte auf Fotos zu erkennen. In einem Test von Googles neuralem Netzwerk entdeckte die Informatikerin Julia Evans zum Beispiel, dass die KI dachte, die englische Queen würde eine Badehaube (statt einer Krone) tragen.

Die Informatikerin entwickelte eine Methode, Bilder so zu verändern, dass sie für Menschen gleich aussehen, die KI jedoch komplett andere Dinge darin „sehen“ – zum Beispiel einen Geier statt einem Panda oder ein Handtuch statt einer Katze. Sie musste dazu nur einzelne Pixel verändern. Allerdings gelang es ihr nicht, die KI mit manipulierten Hundebildern hinters Licht zu führen – die Fotos wurden immer als Hunde erkannt. Das lag wahrscheinlich daran, dass die KI mit sehr vielen Hundebildern trainiert wurde und dementsprechend gut darin war, Hunde zu erkennen. Bei Pandas und Kronen war das jedoch nicht so.

Leider gibt es auch viele Beispiele, die nicht so lustig sind. Joy Buolamwini, Doktorandin am MIT Media Lab berichtet davon, dass sie immer wieder auf ein Problem stieß: Software, auf Gesichtserkennung beruhte, funktionierte bei ihr nicht. Joy Buolamwini ist schwarz. Sie stellte bald fest, dass die Software zwar eine weiße Maske als „Gesicht“ erkannte, an ihrem Gesicht jedoch scheiterte. Googles Bilderkennung klassifizierte Menschen mit schwarzer Hautfarbe mal als Gorillas, während Nikon eine Kamera baute, die Menschen mit asiatischen Gesichtszügen fragte, ob sie geblinzelt hätten – um noch ein Foto ohne den „Schönheitsfehler“ aufnehmen.

Sind die Algorithmen etwa rassistisch?

Joy Buolamwini nennt dieses Phänomen „algorithmic bias“ (algorithmische Vorurteile bzw. Verzerrung). Die Algorithmen übernehmen die (oft unbewussten bzw. systemischen) Denkweisen bzw. Vorurteile ihrer Entwickler_innen. Im Falle der Gesichtserkennung zum Beispiel deswegen, weil nicht genügend "nicht-weiße People Of Color" in den Trainingsdaten waren. Und weil Informatik ein Feld ist, in dem vor allem weiße Männer arbeiten, sei dies auch „zufällig“ vorher niemandem aufgefallen.

Gesichter oder Objekte in Fotos richtig erkennen ist eine Sache, bei anderen (möglichen) Anwendungen von Algorithmen kann die Lage aber noch kritischer werden: Wenn Algorithmen, die die Kreditwürdigkeit bestimmen sollen, ebenfalls einen (rassistischen) Bias haben, können Menschen diskriminiert werden, ohne es zu merken. Das gleiche gilt für KIs, die Bewerbungen für Arbeitsstellen oder Unis einordnen sollen. Auch bei Videoüberwachung, die „intelligent“ vermeintliches verdächtiges Verhalten erkennen soll, könnte es – unbeabsichtigt – zu sogenanntem „racial profiling“ kommen, also dazu, dass Aktionen von People of Color eher „verdächtig“ sind als jene von weißen Menschen.

Grundsätzlich stellt sich bei jedem Algorithmus, der wichtige Entscheidungen trifft die Frage der Transparenz. Wer überprüft, ob sich Fehler oder eben ein „algorithmic bias“ in den Code eingeschleust hat? Wie kann sichergestellt werden, dass die Daten, mit denen ein MachineLearning-Algorithmus gefüttert wird, möglichst repräsentativ sind?

Lösungsansätze

Eine mögliche Lösung ist, dass Code als quelloffen, also als sogenannter Open Source-Code veröffentlicht wird. Viele bekannte Projekte sind so organisiert, zum Beispiel der Firefox-Browser oder das Betriebsystem Linux. Nicht nur die Programme sind frei, sondern auch der darunterliegende Code wird veröffentlicht und alle Interessierten sind eingeladen, sich an der Weiterentwicklung zu beteiligen. Das hat den Vorteil, dass eventuelle Bugs und Schwachstellen schneller gefunden werden und behoben werden können. Gewisse Probleme von Algorithmen könnten so behoben werden – Freiwillige oder auch NGOs könnten den Code untersuchen und Schwachstellen, die zu ethischen Problemen führen, ausbessern. Bei Algorithmen, die auf Deep Learning basieren, würde dies allerdings nur dann helfen, wenn auch die Trainingsdaten (also z.B. die Fotos, mit denen Gesichtserkennung trainiert wird) öffentlich sind und ergänzt werden können.

Wenn wir versuchen würden, ethische Probleme von Algorithmen durch sogenanntes Crowdsourcing – also den Einsatz vieler Freiwillger, die nach Fehlern suchen – zu beheben, würde das vorausetzen, dass viel mehr von uns in der Lage sind, Code zu lesen und zu verstehen. Diese Fähigkeit wird also immer wichtiger – ein Grund mehr, um beispielsweise schon in der Schule programmieren und algorithmische Zusammenhänge zu verstehen zu lernen.

Ein weiterer Lösungsansatz wäre die Möglichkeit, ein unabhängiges Audit für Algorithmen, die in sensible Bereiche des Lebens eingreifen, einzuführen. Bevor ein Algorithmus z.B. für die Einstufung von Kreditwürdigkeit eingesetzt werden dürfte, müsste er von einer unabhängiger Stelle überprüft werden – ähnlich wie zum Beispiel die Abgaswerte bei Fahrzeugen.

Algorithmen sind oft kompliziert – und die ethischen Probleme, die ihr Einsatz mit sich bringt, sind es ebenfalls. Ebensowenig, wie es möglich ist, Zahnpasta wieder in die Tube zu drücken, ist es auch unmöglich, den technischen Fortschritt aufzuhalten. Wichtig ist allerdings, dass wir eine gesellschaftliche Debatte über alle Vor- und Nachteile führen und den Fortschritt gestalten. Umso wichtiger ist, informiert zu sein und die Fakten zu kennen.

Bei Fragen bezüglich des Internetbetrugs
oder der Nutzung des Internet im Allgemeinen,
wenden Sie sich bitte an die BEE SECURE Helpline:

BEE SECURE HELPLINE
BERATUNG
Tel: 8002 1234

Herausgeber: BEE SECURE · B.P. 707 · L-2017 Luxemburg
Tel.: (+(+352) 247-86427 · Fax.: Fax: (+ 352) 46 41 86
bee-secure@snj.luwww.bee-secure.lu

THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG
Co-financed by the European Union
Connecting Europe Facility