

Der digitale Zauberlehrling

Vor zwei Jahren ging eine Meldung durch die Medien: Ein Rechner hatte das knifflige Wissensquiz *Jeopardy* im US-amerikanischen Fernsehen gewonnen. Das wirft Fragen auf: Was können Computer wissen? Wie setzen sie dieses Wissen für Sprachverstehen und Dialoge mit Menschen ein? Und: Was lässt sich dagegen tun, wenn Maschinen über einen Nutzer Fakten sammeln, die nicht zu dessen Bestem sind?

TEXT GERHARD WEIKUM

Haben Computer das Potenzial, dem Menschen intellektuell ebenbürtig oder gar überlegen zu sein? Die Informatik und ihr Teilgebiet, die künstliche Intelligenz, verfolgen diese Frage, seit Alan Turing vor mehr als fünfzig Jahren einen Test vorgeschlagen hat: Kann ein Computer, der mit einem menschlichen Dialogpartner über eine Textschnittstelle kommuniziert, sich so verhalten, dass der Mensch selbst nach längerer Zeit nicht festzustellen vermag, ob hinter dem Gesprächspartner ein Mensch oder eine Maschine steckt?

.....

**Unser Wissen ist nahezu
lückenlos digitalisiert
und systematisch organisiert.**

Menschliches Wissen – in Büchern, Aufsätzen, Nachrichten und anderen Texten – ist heute nahezu lückenlos digitalisiert und systematisch organisiert. Das prominenteste Beispiel digitaler Wissenssammlungen ist die Online-Enzyklopädie *Wikipedia*. Für Computer ist *Wikipedia* allerdings zunächst nicht verständlich, da die Textinhalte für Menschen geschrieben sind.

Das hat sich in den vergangenen Jahren geändert: Umfassende maschinenlesbare Wissensbasen wie der von Google genutzte *Knowledge Graph* ermöglichen Computern ein Textverständnis, das darüber hinaus geht, nur die Begriffe etwa einer Suchanfrage in einem Text zu erkennen. Sie stellen vielmehr zwischen den Begriffen einen Bedeutungszusammenhang her und erlauben somit semantisches Suchen. Sie können also auch Fragen mit mehrdeutigen Begriffen richtig beantworten. Und dank des semantischen Verständnisses kennen Computer auch die Bedeutung von Texten, welche sich, wie die Artikel der *Wikipedia*, an Menschen richten.

Die Wissensbasen, die das tiefere Sprachverständnis ermöglichen, wurden weitgehend automatisch erstellt und werden ständig aktualisiert und erweitert. Der *Knowledge Graph* kennt mehr als zwanzig Millionen Personen, Orte, Filme, Arzneimittel, Sportereignisse und vieles mehr, dazu mehr als eine Milliarde Fakten über diese Einheiten und ihre Beziehungen untereinander. Google nutzt das gewaltige Wissen, um Suchanfragen besser zu verstehen, Suchresultate besser in Ranglisten zu ordnen, bessere Empfehlungen für Nutzer von Youtube und anderen Webportalen zu geben sowie für intelligente Vorschläge zu Restaurants, Konzerten und anderem.

Vor allem drei Projekte haben die Methoden zur automatischen Konstruktion derartig umfassender Wissensbasen entscheidend vorangebracht: *DBpedia*



an der FU Berlin und Uni Leipzig; *Freebase*, das von Google aufgekauft wurde und heute den Kern des *Knowledge Graph* bildet; und *Yago*, das wir seit dem Jahr 2005 am Max-Planck-Institut für Informatik entwickelt haben.

Eine wichtige erste Dimension digitalen Wissens besteht darin, Einheiten – Entitäten genannt – zu sammeln, eindeutig zu benennen und in semantische Klassen wie Personen, Orte, Organisationen oder Ereignisse einzuordnen. Das macht im großen Stil vor allem *Yago*, indem es mit cleveren Algorithmen Kategorienamen aus *Wikipedia* mit dem manuell erstellten Thesaurus *WordNet* verknüpft. Die resultierende Wissensbasis enthält nahezu zehn Millionen Entitäten und mehr als 300 000 feinkörnige und hierarchisch organisierte Klassen wie Politiker, Musiker, Bassisten, Rockballaden, Heavy-Metal-Songs, Benefizkonzerte oder Freiluftopern.

Die zweite Dimension einer Wissensbasis sind Fakten über Entitäten. Das sind zum einen Merkmale wie die Größe eines Fußballtorhüters oder die Anzahl seiner Länderspiele; zum anderen Beziehungen zwischen Entitäten, etwa der Geburtsort eines Torwarts, die Vereine, für die er gespielt hat, seine Ehefrau, die Hauptstadt eines Landes oder die Vorstandsmitglieder eines Unternehmens.

Sprache ist oft mehrdeutig. So lassen Namen und Phrasen mehrere Interpretationen zu.

Die dritte Dimension schließlich sind Regeln, die generelle Zusammenhänge ausdrücken – unabhängig von konkreten Entitäten. Dazu gehören Gesetzmäßigkeiten wie etwa die, dass jede Person genau einen Geburtsort hat und dass Hauptstädte von Ländern im jeweiligen Land liegen müssen. Solche Regeln können allerdings auch mit Unsicherheiten behaftet sein, müssen also nicht immer hundertprozentig zutreffen. Eine Person wohnt wahrscheinlich in derselben Stadt wie der Ehepartner oder in der Stadt, in der sie arbeitet.

Solches Allgemeinwissen brauchen Maschinen, um mehrere Fakten logisch zu verknüpfen. Hat man zum Beispiel keine Anhaltspunkte über den Wohnort von Angela Merkel, weiß man aber, dass ihr Ehemann an der Humboldt-Universität Berlin arbeitet, kann der Computer daraus schließen, dass die Kanzlerin in Berlin wohnt.

Sprache ist oft mehrdeutig. Das mag an der Satzstruktur liegen, viel häufiger aber lassen Namen und Phrasen mehrere Interpretationen zu. Um dies zu illustrieren, betrachten wir den Satz: „Page played Kashmir on his Gibson.“ Handelt es sich hier um den Google-Gründer Larry Page, der sich mit dem Schauspieler und Regisseur Mel Gibson am Rande des Himalaja trifft? Das macht offensichtlich keinen Sinn! Menschen erkennen dies aufgrund ihres Erfahrungsschatzes sofort, die Maschine jedoch muss das systematisch und algorithmisch analysieren. Tatsächlich ist hier die Rede von dem Led-Zeppelin-Gitarristen Jimmy Page, der den Song *Kashmir* auf einer Les-Paul-Gitarre der Firma Gibson spielt.

Um einen Satz aber wirklich zu verstehen, muss die Maschine auch die Beziehungen zwischen den beteiligten Entitäten erkennen und semantisch interpretieren. So kann sich das Verb „play“ auf Spiele, Sport, Musik, Trickserei und vieles mehr beziehen. Die Wahrscheinlichkeit, dass „play“ im Sinne der Relation *MusicianPerformsSong* verwendet wurde, ist eben sehr hoch, wenn die mehrdeutigen Namen „Page“ und „Kashmir“ auf einen Musiker und ein Musikstück hinweisen.

Umgekehrt spricht in einem Satz, der „play“ mit der genannten Bedeutung von *MusicianPerformsSong* verwendet, vieles dafür, dass der Satz auch einen Musiker und einen Song erwähnt. Diese wechselseitigen Abhängigkeiten in der Interpretation der Verbal- und Nominalphrasen werden mithilfe von Optimierungsalgorithmen gelöst.

Digitales Wissen in Kombination mit reichhaltiger Statistik und schlaun Algorithmen ermöglicht der Maschine also ein verblüffend tiefes Sprachverstehen. Und natürlich bleibt man nicht bei einzelnen Sätzen in Aussageform stehen, sondern betrachtet außerdem Fragen, ganze Absätze, lange Essays oder wissenschaftliche Publikationen und auch Dialoge mit dem Menschen.



Ein schwieriges Beispiel für einen Fragesatz ist etwa: „Who did scores for westerns?“ Da muss man analysieren, dass sich „scores“ auf Filmmusik bezieht, mit „westerns“ Westernfilme gemeint sind und die saloppe Formulierung „did“ im Sinne der Relation *ComposedMusic* zu interpretieren ist. Mit diesem Sprachverständnis kann der Computer direkt eine Antwort aus seiner Wissensbasis liefern – etwa Ennio Morricone, der zum Beispiel die Musik zum Film *Spiel mir das Lied vom Tod* komponiert hat.

Die Wissens- und Sprachtechnologie von Computern unterliegt heute noch massiven Grenzen. Oft steht und fällt alles mit dem Reichtum der zugrunde liegenden Statistiken oder dem Ausmaß an Training für Lernverfahren. Auch gibt es Sprachen wie Mandarin, die einer Syntaxanalyse schwer zugänglich sind und ein viel komplexeres Maß an Mehrdeutigkeit aufweisen als das Englische oder Deutsche. Bei manchen Sprachen wie Bambara oder Urdu existiert kein großer Korpus an digitalen Texten und damit auch keine umfassende Statistik.

Wenn wir jedoch den Fortschritt des vergangenen Jahrzehnts extrapolieren, kann man womöglich schon im Jahr 2020 mit Leistungen rechnen, die dem Bestehen des anfangs erwähnten Turing-Tests nahe kommen. Wir könnten dem Computer ein Schullehrbuch über Biologie „zum Lesen“ geben – und der Rechner würde anschließend Fragen auf dem Niveau einer mündlichen Abiturprüfung beantworten. Oder man denke an ein Spiel, in dem man gemeinsam mit anderen Onlinenutzern mit einer virtuellen Version des britischen Kochs Jamie Oliver Speisen zubereitet. Damit Jamie auf die Fehler seiner Lehrlinge bei der Zubereitung von Tiramisu richtig reagieren kann, muss der Computer die Gespräche und Gesten, die Mimik und visuellen Eindrücke analysieren und mit seinem Kochkunstwissen kombinieren.

Im Bereich der medizinischen Diagnose gab es vor dreißig Jahren den heute belächelten Versuch automatischer Expertensysteme. Dieses damals gescheiterte Unterfangen rückt heute in variiertem Form in Reichweite. Man stelle sich einen Arzt vor, der mit einem Patienten dessen Symptome und die Ergebnisse der ersten Labortests bespricht. Dabei hört der Computer zu und übernimmt die Rolle des beratenden Assistenten.

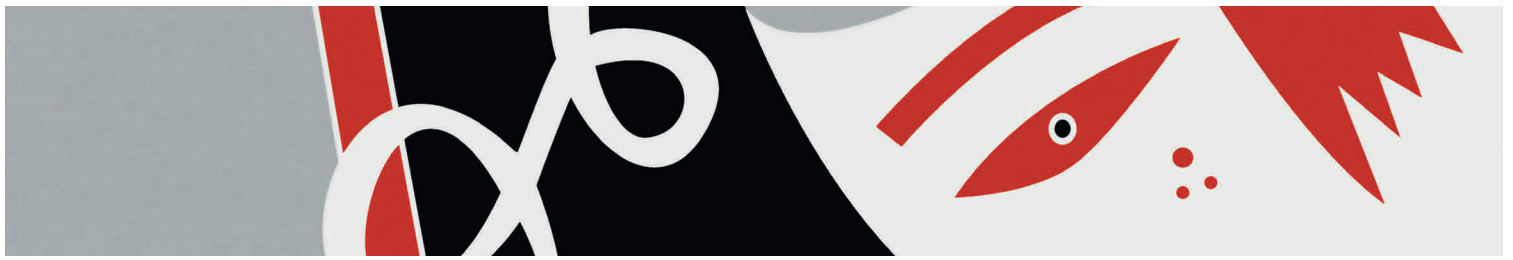
Mit seinem enzyklopädischen Fachwissen kann dieser digitale Assistent entscheidende Hinweise liefern auf Diagnosehypothesen, die sich ausschließen lassen, oder zusätzliche Untersuchungen empfehlen, die unterschiedliche Hypothesen spezifisch diskriminieren. Der Computer kann sich auch als Gesprächspartner einschalten, mit Fragen an den Arzt oder den Patienten. In diesem Zukunftsszenario hat die Maschine eine sehr wesentliche Rolle, überlässt aber Entscheidungen und Verantwortung dem menschlichen Experten.

**Wir werden potenziell zum
Spielball von Effekten, um die
wir nicht gebeten haben.**

Digitales Wissen und intelligentes Sprachverstehen machen nicht bei Nachrichten, prominenten Personen und Allgemeinwissen halt, sondern sind auch methodische Bausteine, um Wissen über uns alle und unsere Vorlieben zu sammeln und für smarte Empfehlungen und Mensch-Maschine-Interaktionen zu nutzen. Die Quelle dafür sind unsere vielfältigen Interaktionen mit dem Internet – sei es über unsere Mitgliedschaften in sozialen Netzen oder über unser Smartphone und alles, was wir mit ihm machen.

Damit werden wir potenziell auch zum Spielball von Benutzertracking, Werbung und anderen Effekten, um die wir nicht unbedingt gebeten haben. Im Jahr eins nach dem NSA-Skandal ist offensichtlich, wie stark unser aller Privatsphäre dadurch beeinträchtigt werden kann. Dabei spielt digitales Hintergrundwissen eine wesentliche Rolle, wie das folgende fiktive Szenario vor Augen führt.

Zoe, eine junge Frau aus Namibia, die in Europa studiert, stellt Fotos und anderes Material auf ihre Seite in einem sozialen Netzwerk. Dort empfiehlt sie ihren Freunden außerdem Filme und Musik, unter anderem die grönländische Indie-Rock-Sängerin Nive Nielsen. Zoe ist im Netzwerk unter ihrem richtigen Namen bekannt und verfügt über ein öffentliches Kurzprofil. >



Zoe hat Probleme mit ihrer Schilddrüse, nimmt das Medikament Synthroid und leidet unter Nebenwirkungen. Sie findet ein Onlineforum zu Gesundheitsthemen, wird unter einem Pseudonym Mitglied und beteiligt sich an Diskussionen. Zu guter Letzt benutzt Zoe auch Suchmaschinen, um nach alternativen Medikamenten zu recherchieren, etwa Levothroid, aber auch nach Filmen über Apartheid oder nach ihrer Lieblingsängerin Nive Nielsen. Die Suchmaschinen

Der Privacy Advisor verfügt über sehr persönliche Kenntnisse von Zoe.

erkennen Zoe nur als anonymen Nutzer, aber ein Internetbeobachter der Tracking- und Targeting-Branche kann ihre Such- und Clickhistorie über einen längeren Zeitraum sammeln.

Dieses vermeintlich harmlose Szenario hat es in sich. Ein Algorithmus mit Hintergrundwissen könnte Verknüpfungen zwischen Zoes drei Identitäten in der digitalen Welt herstellen. Der Angreifer könnte mithilfe einer Wissensbasis ermitteln, dass Synthroid und Levothroid Arzneien für dieselbe Art von Unterfunktion der Schilddrüse sind. Zusammen mit weiteren Hinweisen könnte er dann schließen, dass es sich im Gesundheitsforum und in der Suchhistorie um ein und dieselbe Person handelt.

Zudem gibt es eine extrem geringe statistische Wahrscheinlichkeit, dass sich zwei verschiedene junge Frauen aus Afrika für dieselbe grönländische Sängerin und andere Nicht-Mainstream-Themen interessieren. Der Angreifer kann somit die Suchhistorie mit Zoes Identität im sozialen Netzwerk verknüpfen. Schließlich folgt, dass Zoe dieselbe Person sein muss, die über ihre Schilddrüsenprobleme im Gesundheitsforum diskutiert. Das öffnet die Tür für unerwünschte Werbemails, mögliche Probleme mit der Krankenversicherung und andere – mehr als nur unangenehme – Konsequenzen.

Was wir hier skizziert haben, ist eine automatisierte Attacke auf Zoes Privatsphäre. Sie lebt von genau jener Wissens- und Sprachtechnologie des Computers, die wir zuvor als Segen und Hilfe für den Men-

schen angesehen haben. Eine systematische, nachhaltig wirkende Gegenmaßnahme könnte selbst auf digitalem Wissen und Sprachverstehen beruhen: ein persönliches Softwarewerkzeug, genannt Privacy Advisor. Es beobachtet kontinuierlich Zoes Verhalten im Internet, kennt ihre Aktivitäten und Vorlieben. Und es analysiert permanent das Risiko, inwieweit Zoe kritische Dinge von sich preisgibt, die ein mächtiger Angreifer ausnutzen könnte. Wenn das Werkzeug Alarm schlägt, sollte es Zoe die Lage erklären und vorschlagen, wie sie sich alternativ zu verhalten hat, um das Risiko zu verringern.

Der Privacy Advisor ist ein Konzept, das tatsächlich in hohem Maße auf maschinellem Wissen und Sprachverstehen basiert. Gegenüber potenziellen Angreifern besitzt es jedoch einen Vorteil: Es verfügt nicht nur über Welt- und Allgemeinwissen, sondern darüber hinaus auch über sehr persönliche Kenntnisse von Zoe. Damit Zoe dem Werkzeug vertrauen kann, muss es selbst als Open-Source-Software konzipiert und durch zahlreiche Programmierer überprüft sein. Seine Leistungsfähigkeit erhält es durch die an Zoe angepasste Konfiguration und die persönliche Wissensbasis.

An der Realisierung dieser Vision arbeiten Michael Backes (Universität des Saarlandes), Peter Druschel und Rupak Majumdar (Max-Planck-Institut für Softwaresysteme) sowie der Autor im Rahmen des durch einen ERC Synergy Grant geförderten Projekts IMPACT. Das Projekt zielt auf ein wissenschaftlich fundiertes Verständnis aller relevanten Dimensionen des sozialen Basars, zu dem sich das Internet entwickelt hat, und ihrer potenziellen Spannungen: Zusätzlich zur Privatsphäre (*Privacy*) sind die Verantwortlichkeit der Nutzer (*Accountability*), die Spezifikations-treue von Diensten (*Compliance*) und das Vertrauen in Information und Wissen (*Trust*) fundamentale Pfeiler, die ein künftiges Internet haben sollte.

Dieser Artikel hat beleuchtet, inwieweit der Computer Wissen und Sprache – intellektuelle Fähigkeiten, die dem Menschen vorbehalten zu sein scheinen – zu erwerben vermag. Dabei haben wir gesehen, dass Maschinen heute digitales Wissen in großem Umfang automatisch sammeln und organisieren und für ein immer besser werdendes Sprachverständnis nutzen. Die folgenden Thesen mögen zum weiteren Nachdenken und Diskutieren anregen:

Maschinen werden dem Menschen in nicht zu ferner Zukunft in vielen Anwendungssituationen haushoch überlegen sein, wie etwa beim Beantworten wissensintensiver Fragen oder der automatischen Zusammenfassung langer Texte oder ganzer Korpora und deren Aufbereitung für Analysen. Maschinen werden auch in der Lage sein, Abiturprüfungen zu bestehen. Dem Bestehen des Turing-Tests werden Maschinen damit sehr nahe kommen. Man kann dies als Simulation intelligenten Verhaltens ansehen, die auf Wissen, Statistik und Algorithmen beruht. Für den Effekt in Anwendungen ist es irrelevant, ob wir es mit „künstlicher“ oder „echter“ Intelligenz zu tun haben.

In Situationen, die Einfühlungsvermögen und kognitive Flexibilität erfordern, wird die Maschine dem Menschen nicht wirklich überlegen sein, sich aber als unverzichtbarer Assistent erweisen. Ein Beispiel dafür ist die Hilfe bei medizinischen Diagnosen, wo der Computer als nahezu vollwertiger Gesprächspartner für Arzt und Patient fungieren kann. Es wird aber auch immer Situationen geben, in denen uns die Maschine nicht zu imitieren vermag: Humor, Ironie, Flirten und andere Emotionen bleiben sicher noch lange dem Menschen vorbehalten.

**Wir können Computern beibringen,
uns zu warnen, wenn wir im Internet
zu viel preisgeben.**

Da Computer zunehmend die Bedeutung von Texten in sozialen Medien analysieren und Zusammenhänge zwischen Begriffen herstellen, eröffnen sich ihnen völlig neue Anwendungsmöglichkeiten – aber nicht nur zum Besten der Nutzer: Das semantische Verständnis befähigt die Maschinen auch, uns Menschen umfassender zu analysieren. Doch wir müssen uns dem nicht ausliefern: Schließlich können wir Computern beibringen, uns mit ihrem Sinn für Bedeutungen und Zusammenhänge zu warnen, wenn wir im Internet zu viele Informationen preisgeben, die Algorithmen zu detaillierten Persönlichkeitsprofilen verknüpfen könnten. ◀

DER AUTOR



Prof. Dr. Gerhard Weikum, Jahrgang 1957, studierte Informatik und promovierte an der TU Darmstadt. An dieser Hochschule arbeitete er 1987 als wissenschaftlicher Assistent. Weitere Stationen als Postdoc waren das MCC in Austin sowie die ETH Zürich, wo er zwischen 1990 und 1994 auch eine Professur innehatte. In dieser Funktion ging er danach an die Universität des Saarlandes in Saarbrücken. Seit 2003 ist er Direktor und wissenschaftliches Mitglied am Max-Planck-Institut für Informatik.