Letzte Frage der Informatik: Dieses Problem beschäftigt Forscher seit über 50 Jahren

Ein über 50 Jahre altes Problem der theoretischen Informatik – bekannt als P vs. NP – entzieht sich noch immer einer Lösung. Die könnte die IT-Geschichte ändern.

Von MIT Technology Review Online
05.06.2025, 18:30 Uhr • 12 Min.

Das „Problem des Handlungsreisenden“ (Travelling Salesman) besteht darin, den kürzesten Weg zwischen n Städten zu finden und dabei keinen Weg zweimal zu benutzen.

Montag, der 19. Juli 2021, war wieder einer dieser Tage. Ein Tag, mitten im zweiten Pandemie-Sommer, an dem anscheinend alles schiefgeht. Jedenfalls liest sich der Tweet eines führenden Informatikers so, der eigentlich auf dem Gebiet der Komplexitätstheorie forscht, sich nun aber heftig über den administrativen Schlamassel bei einer führenden Fachzeitschrift beklagt – und seinen Tweet mit einem sehr geladenen „Happy Monday“ beendet. Dabei hätte dieser Tag vielleicht tatsächlich ein glücklicher Montag sein können – in irgendeinem Paralleluniversum. Denn an diesem Tag erschien in der Online-Ausgabe der angesehenen Fachzeitschrift „ACM Transactions on Computational Theory“, die sich mit „herausragender Forschung zu den Grenzen machbarer Berechnungen“ befasst, ein Paper, in dem angeblich eine Lösung für das Problem aller Probleme stand – dem Heiligen Gral der theoretischen Informatik.

> Dieser Text ist zuerst in der Ausgabe 2/2022 von MIT Technology Review erschienen. Hier könnt ihr die TR als Print- oder pdf-Heft bestellen.

Dieses Problem – bekannt als „P versus NP“ – gilt als das wichtigste Problem der theoretischen Informatik. Für seine Lösung ist eine Prämie von einer Million US-Dollar ausgesetzt. Es befasst sich mit zentralen Fragen zu den Verheißungen, Grenzen und Ambitionen der Computertechnik: Welche Probleme können Computer realistischerweise lösen? Wie viel Zeit werden sie dafür

benötigen? Und warum sind manche Probleme schwieriger als andere? Was heißt eigentlich „schwierig“?

„P“ steht dabei für Probleme, die ein Computer leicht lösen kann

Die Angabe einer absoluten Zeit für Berechnungen ist wenig sinnvoll. Denn natürlich hängt die Geschwindigkeit einer Berechnung von der Rechenpower des Computers ab, zum anderen aber auch von der Größe des Problems selbst: Es dauert länger, eine Liste mit 1.000 Elementen zu sortieren als eine Liste mit 100 Elementen. Informatiker teilen Berechnungen also danach ein, wie die Rechenzeit mit der Anzahl der zu berechnenden Variablen ansteigt. „P“ steht dabei für Probleme, die ein Computer leicht lösen kann. Präziser ausgedrückt steht P für „Polynomial“. Das heißt, die Abhängigkeit der Berechnungszeit lässt sich als ein Polynom – die Summe von Potenzen – der Variablenzahl beschreiben. „NP“ steht für „Nichtdeterministisch Polynomial“. Das sind Probleme, die schwer zu lösen sind, bei den die Rechenzeit zum Beispiel exponentiell ansteigt. Gleichzeitig ist deren Lösung relativ einfach zu überprüfen: Solche Berechnungen funktionieren wie Falltüren oder Zahnräder mit Sperrhaken: In eine Richtung lassen sie sich leicht bewegen, in die andere nur gegen einen extremen Widerstand. Man nimmt eine mögliche Lösung und rechnet nach, ob sie wirklich funktioniert – wie bei Puzzles oder Sudoku-Rätseln.

Das klingt sehr abstrakt, aber viele NP-Probleme sind technisch und wissenschaftlich sehr relevant – wie die Frage, in welche Primfaktoren sich eine Zahl zerlegen lässt. Auf der Tatsache, dass der Rechenaufwand für dieses Problem mit der Größe dieser Zahl exponentiell anwächst, beruhen große Teile der Verschlüsselung im Internet. Die Millionen-Dollar-Frage, die sich bei P vs. NP stellt, ist folgende: Sind diese beiden Klassen von Problemen ein und dasselbe? Das heißt, könnten die Probleme, die so schwierig erscheinen, tatsächlich mit einem Algorithmus in einer vernünftigen Zeitspanne gelöst werden – zumindest im Prinzip? Wenn nur der richtige, teuflisch schnelle Algorithmus gefunden werden könnte?

Gigantische Chancen, wenn P=NP

Wäre P=NP, könnte früher oder später jemand eine Lösung für die Primzahlzerlegung finden, und damit die gesamte Kryptosphäre auseinanderreißen – ganz ohne Quantencomputer. Aber es gäbe auch gigantische Chancen: Die Proteinfaltung, eine 50 Jahre alte große Herausforderung in der Biologie, würde leichter zu bewältigen sein und damit völlig neue Möglichkeiten zur Entwicklung von Medikamenten zur Heilung oder Behandlung von Krankheiten und zur Entdeckung von Enzymen für den Abbau von Industrieabfällen eröffnen. Das würde auch bedeuten, dass man optimale Lösungen für schwierige Alltagsprobleme finden könnte, wie zum Beispiel die Planung einer Autoreise, um alle Ziele mit möglichst wenig Fahrzeit zu erreichen, oder die Sitzordnung für Hochzeitsgäste, sodass nur Freunde am selben Tisch sitzen.

Mit seiner Forschung hat der Informatiker Stephen Cook die Grundlagen der Komplexitätstheorie gelegt. Jetzt soll sein Sohn die Arbeit weiterführen

Seit das P-vs.-NP-Problem vor rund 50 Jahren zum ersten Mal formuliert wurde, haben Forscher auf der ganzen Welt versucht, eine Lösung zu finden. Doch selbst Stephen Cook von der University of Toronto, der mit einer bahnbrechenden Arbeit im Jahr 1971 den Grundstein für das Gebiet der Computerkomplexität legte, war mit seiner Suche überfordert. Für seine Arbeit erhielt er zwar den Turing Award, das Äquivalent zum Nobelpreis in der Informatik. Aber auch Cook gesteht ein, er habe nie eine gute Idee gehabt, wie man das Problem knacken könnte – „es ist einfach zu schwierig".

„Es ist peinlich, dass wir die Antwort noch nicht kennen"

Die meisten Forschenden, die sich mit dieser Materie beschäftigen, glauben mittlerweile, dass P nicht gleich NP ist. Sie lassen nur einen Funken Hoffnung zu, dass sich das Gegenteil bewahrheiten wird. „Ich würde die Wahrscheinlichkeit, dass P gleich NP ist, auf zwei bis drei Prozent schätzen", sagt der Mathematiker Scott Aaronson von der University of Texas, der seit nunmehr rund 20 Jahren über Komplexitätstheorie und die Grenzen von Quantencomputern nachdenkt. „Das sind die Wettchancen, die ich annehmen würde."

Doch das im Juli 2021 veröffentlichte Ergebnis schien ein Beweis für genau diese Unwahrscheinlichkeit zu sein. Aber das Paper war nur der jüngste in einer langen Tradition von Beweisen, die nur scheinbar funktionierten, weil sie logische Fehler enthalten. Tatsächlich handelte es sich um die jüngste Version einer Arbeit, die der Autor in den letzten zehn Jahren mehr als 60-mal auf dem Preprint-Server „arXiv" veröffentlicht hatte. Einen Tag nach der Veröffentlichung wurde die Arbeit aus der Online-Zeitschrift entfernt; dann schien sie kurz wieder aufzutauchen, bevor sie endgültig verschwand – in einer Monty-Python-würdigen Aktion. Der Chefredakteur der Zeitschrift erklärte auf Twitter, dass das Ergebnis abgelehnt worden war, aber durch einen menschlichen Fehler hatte sich der Status des Papers irgendwie von „ablehnen" in „annehmen" geändert, und der Beweis hatte seinen Weg zur Veröffentlichung gefunden.

Eines der sieben ungelösten „Millenium-Probleme“

Als ich Steve Cook Anfang August in seinem Büro auf dem Campus traf, hatte er von diesem jüngsten P-gegen-NP-Beweis-Chaos weder etwas gesehen noch gehört. Der 81-Jährige hatte sich erst vor kurzem zur Ruhe gesetzt, da sein Gedächtnis nachließ. „Deshalb haben wir James hier“, sagte er – sein Sohn James, 36, ebenfalls Informatiker, hatte sich für meinen Besuch zu uns gesellt. Steve war gerade dabei, sein Büro zu entrümpeln. In der Mitte des Raums stand ein riesiger Papierkorb, der sich mit alten, vergilbten Ausgaben des Journal of Symbolic Logic füllte. Gleich daneben lag ein Stapel fetter Telefonbücher aus Toronto.

Im Laufe der Jahre hat Cook viele Beweise gesehen, die vorgeben, das P-vs.-NP-Problem zu lösen. Nachdem das Clay Mathematics Institute das Problem im Jahr 2000 zu einem der sieben ungelösten „Millennium-Probleme“ ernannt hatte (deren Lösung jeweils mit einer Million Dollar dotiert ist), wurde er mit Nachrichten von Leuten überschwemmt, die glaubten, sie hätten den Sieg errungen. Etwa die Hälfte behauptete, bewiesen zu haben, dass P gleich NP ist; die andere Hälfte ging in die entgegengesetzte Richtung. Vor nicht allzu langer Zeit behauptete eine Person, beides bewiesen zu haben. Aber alle Ergebnisse waren falsch, wenn nicht sogar schlichtweg gefälscht. Cook war der Erste, der in einem Aufsatz von 1971 die Vermutung aufstellte, dass P nicht gleich NP sein könnte (er formulierte es mit einer anderen, damals üblichen Terminologie). Seitdem hat der Forscher eine beträchtliche Menge an Zeit investiert, um seine Vermutung zu beweisen. Erfolg hatte er damit jedoch nicht. Jetzt will sein Sohn James sich der Sache annehmen.

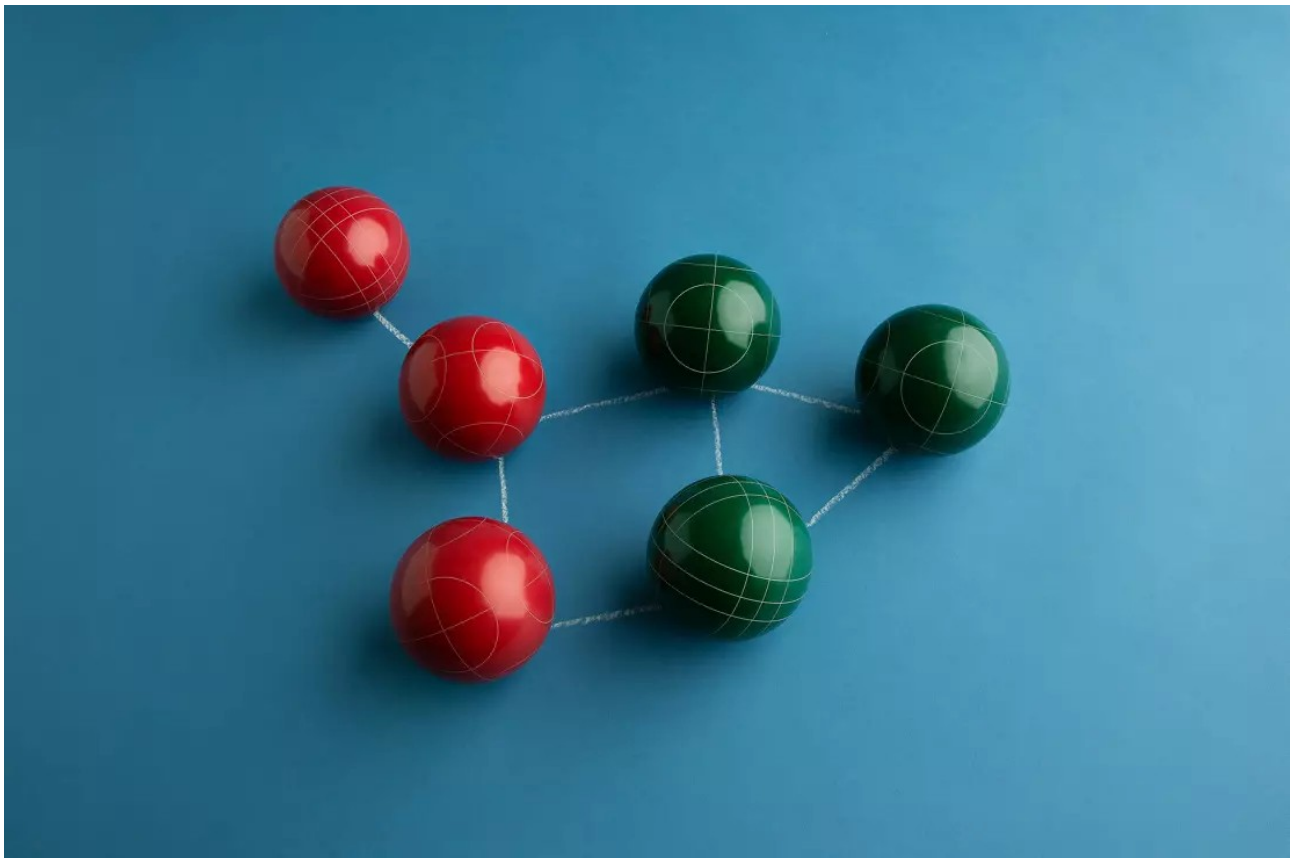
Schon früh interessierte sich James für Mathematik und Computer – im Alter von neun Jahren drängte er seinen Vater, ihm Boolesche Algebra und Logik beizubringen. Vor ein paar Jahren, nachdem er in Berkeley promoviert und bei Google gearbeitet hatte, machte er sich als unabhängiger Forscher selbstständig und konzentrierte sich auf verschiedene Projekte, von denen einige indirekt mit P vs. NP zu tun hatten. Und trotz dieser Erfolgsbilanz ist James, der seinem Vater verblüffend ähnlich sieht, nicht entmutigt, weil er eine so scheinbar endlose Aufgabe geerbt hat. Er betrachtet es wie jedes andere mathematische Unterfangen: Es ist ein lustiges Rätsel. „Es muss doch eine Antwort auf diese Fragen geben“, sagt er. „Irgendjemand muss sie doch lösen. Lasst uns das einfach herausfinden. Es hat lange gedauert. Es ist peinlich, dass wir die Antwort noch nicht kennen.“

Der fehlende Fortschritt hat die hartnäckige Gemeinschaft der Forschenden nicht davon abgehalten, das 50-jährige Bestehen der Komplexitätstheorie zu feiern. Die Feierlichkeiten begannen 2019, als sich ihre Anhänger aus der ganzen Welt am Fields Institute for Research in Mathematical Sciences an der University of Toronto zu einem Symposium zu Cooks Ehren versammelten. Christos Papadimitriou, ein Informatiker an der Columbia University, der einen Großteil seiner Karriere mit der Erforschung von P vs. NP verbracht hat, eröffnete die Veranstaltung mit einem öffentlichen Vortrag.

Auch Turings Maschine liefert keinen Wahrheitsbeweis

Schon Alan Turing, erklärte Papadimitrious, der britische Mathematiker, der 1936 in seiner Schrift „On Computable Numbers“ die Begriffe „Algorithmus“ und „Berechnung“ formalisiert hatte, legte die wissenschaftlichen Grundlagen. Denn Turing ersann zwar eine hypothetische universelle Rechenmaschine. Er bewies in dieser Arbeit aber auch mathematisch, dass es keinen „mechanischen“ (das heißt von einer Maschine durchführbaren) Weg gibt, die Wahrheit oder

Falschheit mathematischer Aussagen zu beweisen; keinen systematischen Weg, das Beweisbare vom Unbeweisbaren zu unterscheiden.



Beim Cliquenproblem geht es um die Frage, wie viele Untergruppen von miteinander verbundenen Punkten einer vorgegebenen Größe man in einem Netz von Knotenpunkten finden kann.

Turings Arbeit sei daher nicht nur Geburtsurkunde der Informatik. „Die Geburtsurkunde besagt auch, dass die Informatik mit einem klaren Verständnis ihrer eigenen Grenzen geboren wurde.“ Damit sei die Informatik der einzige bekannte Bereich des wissenschaftlichen Diskurses, der mit einem solchen Bewusstsein geboren wurde – „im Gegensatz zu anderen Wissenschaften, die ihre eigenen Grenzen wie wir alle erst im späten mittleren Alter erkennen“.

„Seiner Meinung nach ist P gleich NP.“

Es dauerte nicht lange, nachdem Turings Ideen – und ähnliche Konzepte anderer Forscher – in den ersten Computern ihren Niederschlag gefunden hatten, bis sich die Wissenschaftler mit Fragen zu den inhärenten Fähigkeiten und Grenzen dieser Maschinen auseinandersetzten. Bereits in den frühen 1950er-Jahren prahlte John von Neumann, der ungarisch-amerikanische Pionier des modernen Computers, damit, dass ein von ihm entwickelter Algorithmus polynomial sei, „verglichen mit dem exponentiellen Amtsinhaber“, wie sich Papadimitriou erinnert – er hatte einen langsamen Algorithmus mit einem schnellen überlistet. Dies war der Beginn einer neuen Theorie: der Theorie der rechnerischen Komplexität. Denn nur polynomiale Algorithmen galten in irgendeiner Weise als gut oder praktisch verwertbar, während ein exponentieller Algorithmus, so Papadimitriou, „das algorithmische Äquivalent des Todes ist“.

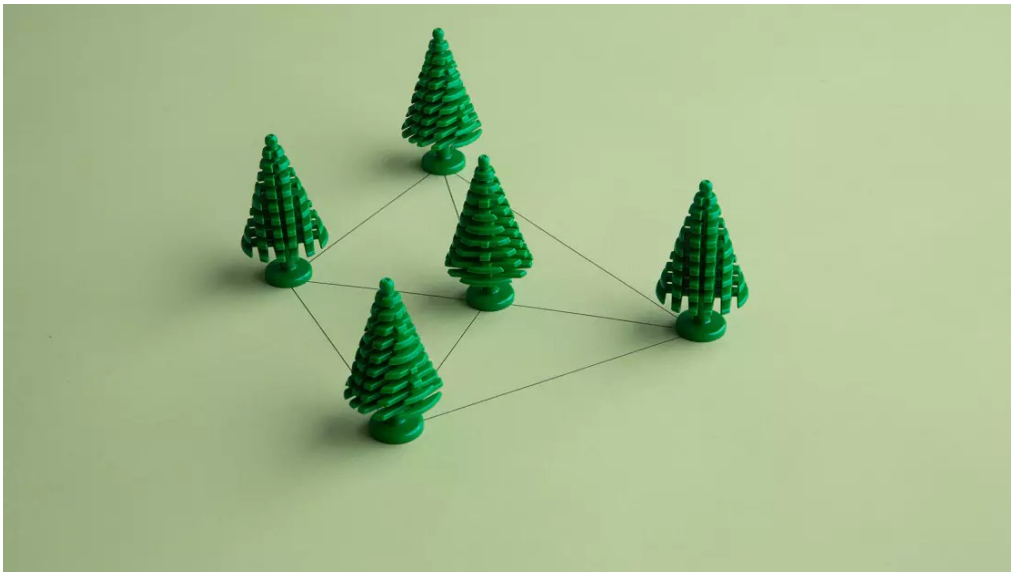
Auf der Suche nach dem Generalschlüssel

Cook begann Mitte der 1960er-Jahre, über Komplexität nachzudenken. 1967, während eines Postdoc-Aufenthalts in Berkeley, notierte er erste Ideen, die den Keim seines großen Ergebnisses

enthielten. Er hatte eine Formulierung der Komplexitätsklassen ausgearbeitet, die später als P und NP bekannt wurden, und er stellte die Frage, ob P gleich NP sei. Etwa zur gleichen Zeit beschäftigten sich andere, darunter der Informatiker Jack Edmonds, der inzwischen an der University of Waterloo im Ruhestand ist, mit denselben Ideen.

Aber das Gebiet der Informatik war gerade erst im Entstehen begriffen, und für die meisten Wissenschaftler und Mathematiker waren solche Ideen geradezu fremdartig. Nach vier Jahren an der mathematischen Fakultät von Berkeley wurde Cook zwar für eine Festanstellung in Betracht gezogen, aber ihm wurde keine Stelle angeboten. 1970 wechselte Cook daher an die University of Toronto. Im folgenden Jahr veröffentlichte er seinen Durchbruch. Das Paper, das er im Mai auf einem Symposium der ACM in Shaker Heights, Ohio, vorlegte, schärfte das Konzept der Komplexität noch einmal und ermöglichte erstmals, die schwierigsten Probleme zu charakterisieren. Denn Cook bewies, dass das „Erfüllbarkeitsproblem der Aussagenlogik“ (SAT, von englisch „satisfiability“ = „Erfüllbarkeit“) im Sinne der Theorie das schwierigste Problem in NP ist und sich alle anderen NP-Probleme darauf reduzieren lassen (das SAT beschäftigt sich mit der Frage, ob es für eine gegebene aussagenlogische Formel F einen Satz logischer Variablen gibt, für die F logisch wahr ist). Dies war ein entscheidendes Theorem, denn es bedeutet andererseits: Wenn es einen Algorithmus gäbe, der das Erfüllbarkeitsproblem in Polynomialzeit löst, würde dieser Algorithmus als Generalschlüssel dienen, der die Lösungen für alle Probleme in NP aufschließt. Und wenn es eine Polynomialzeitlösung für alle Probleme in NP gibt, dann ist P = NP.

1972 wies Dick Karp, Informatiker der University of California in Berkeley, nach der Lektüre von Cooks esoterischem Aufsatz nach, dass viele der klassischen Rechenprobleme, mit denen er bestens vertraut war – im Grunde jedes Problem aus den Bereichen mathematische Programmierung, Operations Research, Graphentheorie, Kombinatorik und Computerlogik, von dem er nicht wusste, wie es zu lösen war – dieselbe Umwandlungseigenschaft besaßen, die Cook beim Erfüllbarkeitsproblem gefunden hatte. Insgesamt fand Karp 21 Probleme, darunter das Knapsack-Problem (die Suche nach dem optimalen Weg, einen begrenzten Raum mit den wertvollsten Gegenständen zu füllen), das Travelling-Salesman-Problem (die Suche nach der kürzest möglichen Route, die jede Stadt einmal besucht und zur Ausgangsstadt zurückführt) und das Steinerbaumproblem (die Suche nach der optimalen Verbindung einer Menge von Punkten mit Liniensegmenten von minimaler Gesamtlänge).



Das Steinerbaumproblem beschäftigt sich mit der Frage, wie man einen vorgegebenen Satz von Punkten mit Linien verbinden kann, deren Länge minimal ist.

Ein Rätsel, „konkret und doch universell“

Karp zeigte, dass diese speziellen Probleme alle gleichwertig waren, was wiederum darauf hinwies, dass das von Cook identifizierte Muster kein isoliertes Phänomen war, sondern vielmehr eine Klassifizierungsmethode von überraschender Stärke und Reichweite. Es war eine Art Lackmustest, der die Klasse der sogenannten „NP-vollständigen“ Probleme identifizierte: Eine Lösung für eines dieser Probleme würde sie alle knacken. Wie es der wissenschaftliche Zufall wollte, kam ein sowjetischer Mathematiker, Leonid Levin, mehr oder weniger zur gleichen Zeit zu einem Ergebnis, das dem von Cook entsprach. Levin, der heute an der Universität Boston lehrt, führte seine Arbeit hinter dem Eisernen Vorhang aus. Nachdem es größere Aufmerksamkeit erlangte (er emigrierte 1978 nach Amerika), wurde das Ergebnis als Cook-Levin-Theorem bekannt.

Probleme in der Komplexitätstheorie, stellt James Cook fest, verhalten sich manchmal wie Dominosteine – wenn es in einer kritischen Ecke einen Beweis gibt, dann fallen auch alle anderen Dominosteine um. Die bahnbrechenden Erfolge sind das Ergebnis einer langen Reihe von Arbeiten vieler verschiedener Leute. Sie machen schrittweise Fortschritte und stellen Verbindungen zwischen verschiedenen Fragen her, bis schließlich ein großes Ergebnis herauskommt.

Widerlegung könnte eine große Enttäuschung sein

Doch auch wenn es gelänge, das Theorem seines Vaters zu widerlegen – ein wirklich teuflisch schneller P = NP-Algorithmus also existieren würde – könnte das Ergebnis eine große Enttäuschung sein: Denn es könnte sich herausstellen, dass ein P-Algorithmus, der in der Lage ist, das NP-komplette Problem zu lösen, auf einer Zeitskala von, sagen wir, n_{100} liegt. „Technisch gesehen fällt das unter P: Es ist ein Polynom“, sagt James. „Aber n_{100} ist immer noch sehr unpraktisch“ – es würde bedeuten, dass jedes größere Problem in menschlicher Zeit unlösbar wäre. Natürlich nur, wenn wir den Algorithmus überhaupt finden können. Donald Knuth, mittlerweile emeritierter Informatik-Professor der Stanford University und Autor des Standardlehrbuchs „The Art of Computer Programming“, hat in den letzten Jahren seine Meinung zu dieser Frage geändert – das „Bit umgedreht“, wie er sagt. Seiner Meinung nach ist P tatsächlich gleich NP, aber wir werden diese Tatsache praktisch nie nutzen können, weil wir keinen der Algorithmen kennen, die tatsächlich funktionieren. Es gäbe eine unvorstellbar große Anzahl von Algorithmen, erklärt er, aber die meisten von ihnen seien für uns nicht zugänglich, weil der Suchraum schlicht zu groß sei. Während also einige Forscher darauf bestehen, dass es keinen P = NP-Algorithmus gibt, behauptet Knuth, dass „es wahrscheinlicher ist, dass kein Polynomialzeit-Algorithmus jemals von Normalsterblichen verkörpert, das heißt tatsächlich als Programm niedergeschrieben wird“.

Für Papadimitriou würde jede Antwort eine lebenslange Besessenheit stillen. Seiner Meinung nach gehört das P-vs.-NP-Problem in den Bereich grundlegender wissenschaftlicher Rätsel wie der Suche nach dem Ursprung des Lebens oder der Theorie, die alle vier Grundkräfte der Natur auf eine einheitliche Wechselwirkung zurückführt. Es ist die Art von tiefgründigem, folgenreichem Rätsel, „konkret und doch universell“, sagt er, „das nicht nur der Wissenschaft, sondern auch dem menschlichen Leben selbst einen Sinn verleiht“. „Stellen Sie sich vor, dass wir Glück haben und es uns gelingt, trotz aller Widrigkeiten und trotz aller Ungereimtheiten noch ein paar tausend Jahre aus diesem Planeten herauszuquetschen“, sagt er. „Und wir lösen diese Probleme nicht. Was hätte das für einen Sinn?!“ (Dieser Artikel stammt von der Wissenschaftsjournalistin Siobhan Roberts.