Wie man EINEN BRIEF frankiert

Im zweiten Teil der Serie geht es um Komplexität, hier um die Frage, wie effizient sich bestimmte kombinatorische Probleme lösen lassen. In der Komplexitätstheorie ist dies unter dem Kürzel »P = NP« bekannt (siehe »Info«). Für die Lösung bietet das Clay Institute ein Preisgeld von einer Million Dollar.

Von Ian Stewart

Eines Tages muss sich ein früher babylonischer Schreiber entschlossen haben, seinen Schülern Arithmetik beizubringen. Er stellte ihnen Probleme der Art »Ich fand einen Stein, habe ihn aber nicht gewogen ...«. Seitdem interessieren sich Mathematiker stets auch für die verborgenen Tiefen scheinbarer Alltagsprobleme: wie man Torten in Teile schneidet, Knoten knüpft oder Münzen rotieren lässt. Aber selbst die Fachleute waren davon überrascht, welch abgründiges Geheimnis hinter einer unschuldigen Frage zu Briefmarken steckt.

Angenommen, Ihr Postamt verkauft Ihnen Briefmarken nur in zwei Stückelungen: zwei Cent und fünf Cent. Kombiniert man diese Werte, dann lässt sich daraus fast jeder gewünschte Wert zusammensetzen. Wenn beispielsweise ein Brief neun Cent kostet, dann kann man eine Briefmarke mit fünf Cent und dazu zwei mit je zwei Cent daraufkleben. Nicht darstellen lassen sich ein Cent und drei Cent – und das sind die einzigen nicht darstellbaren Beträge. Jeden geraden Betrag erreicht man jedenfalls mit ausreichend vielen Zwei-Cent-Marken – zumindest, falls der Umschlag groß genug ist –, und jeder ungerade Betrag über fünf Cent ergibt sich mit Hilfe einer Fünf-Cent- und entsprechend vielen Zwei-Cent-Marken.

Dieses Beispiel ist typisch für das Stückelungsproblem. Eine unbegrenzte Zahl an Briefmarken (nicht an Markenwerten!) vorausgesetzt, existiert immer ein Schwellenwert, von dem ab sich jeder beliebige Betrag darstellen lässt, indem eine passende Kombination von Marken auf den Umschlag geklebt wird. Das gilt auch, wenn mehr als nur zwei Markenwerte zur Verfügung stehen.

Die Eine-Million-Dollar-Frage lautet aber: Gegeben seien Briefmarken mit n verschiedenen Stückelungen, wie groß ist dann dieser Schwellenwert? Der Erste, der sich mit einer allerdings einfacheren Variante dieses Problems befasst hat, war im Jahr 1883 James Joseph Sylvester (1814–1897). Genauer gesagt hat er sich mit Münzen beschäftigt, aber wir bleiben hier trotzdem bei Briefmarken. Dem englischen Mathematiker gelang es, eine einfache Formel zur Bestimmung dieses Schlüsselwerts für den Fall zweier Stückwerte anzugeben (siehe Kasten S. 77).

Effizient, einfach, polynomial

In seiner allgemeinen Form könnte die Lösung unseres Briefmarkenrätsels tatsächlich eine Million Dollar einbringen: Das Clay Mathematics Institute in Cambridge, Massachusetts, offeriert nämlich genau diese Summe demjenigen, dem es gelingt, ein Problem zu lösen, das logisch äquivalent zu unserer Frankierfrage ist. Gerade jetzt gibt es neue, aufregende Hinweise darauf, dass es – und damit vielleicht auch das damit verwandte Eine-Million-Dollar-Rätsel – möglicherweise doch nicht so einschüchternd ist, wie es scheint.

In Kürze

Womit beschäftigt sich die Komplexitätstheorie?

Es gibt Probleme, deren Lösung extrem schwierig ist, sich aber leicht überprüfen lässt. Hier Beispiele:

Das Sortierproblem: Sortiere eine gegebene Liste von Zahlen nach ihrer Größe.

Das Rucksackproblem: Aus einer Menge von Gegenständen mit verschiedenen Volumina und Werten wähle eine Teilmenge so aus, dass sie »in den Rucksack passt«, das heißt ein vorgegebenes Gesamtvolumen nicht überschreitet, und zugleich ihr Gesamtwert maximal wird.

Das Faktorisierungsproblem: Ist eine vorgegebene Zahl eine Produkt zweier Faktoren?

SERIE: DIE GRÖSSTEN RÄTSEL DER MATHEMATIK

Teil I:	Interview mit Gerd Faltings	SdW 09/2008
	Die riemannsche Vermutung	
Teil II:	Das Komplexitätsproblem P = NP	SdW 10/2008
	Ein Beispiel: Rekonstruktion von Gen-Inversionen (S. 80)	
Teil III:	Die goldbachsche Vermutung / Primzahlzwillinge	SdW 12/2008
Teil IV:	Die Vermutung von Birch und Swinnerton-Dyer	SdW 01/2009
Teil V:	Das abc-Problem	SdW 02/2009
Teil VI:	Das Yang-Mills-Problem	SdW 03/2009
Teil VII:	Das Navier-Stokes-Problem	SdW 04/2009

Von dem Mathematiker James Joseph Sylvester (1814 – 1897) stammt die erste, einfache Formulierung des Sortierproblems.

Darüber nachzudenken, wie wir unsere Briefe frankieren, könnte also zum Durchbruch bei einem der bedeutendsten mathematischen Rätsel des 21. Jahrhunderts führen.

Dieses Problem dreht sich um den Aufwand, der zur Lösung einer Aufgabe nötig ist – ausgedrückt nicht in Euro oder Cent, sondern in Rechenzeit. Als Maß für die Kompliziertheit einer Berechnung betrachtet man nämlich die Anzahl der einzelnen dazu nötigen Operationen: Um den Umfang eines bestimmten Problems abzuschätzen, fragt man, wie lange ein entsprechendes Lösungsverfahren »laufen« würde. Diese Laufzeit wird dann wiederum als Funktion der Problemgröße ausgedrückt. Das ist zum Beispiel die Anzahl der Ziffern, die zu berechnen sind. So vergleicht man etwa, wie viel länger die Berechnung einer Zahl mit 50 Stellen dauert, verglichen mit der für eine 25-stellige. Und wie steht es mit 100-stelligen Zahlen oder gar beliebig großen Zahlenmostern? Ich will dabei aber deutlich sagen, dass »Rechenzeit« hier im abstrakten Sinn zu verstehen ist. Sie hat zwar etwas mit der Zeit zu tun, die ein echter Computer für die gesamte Operation brauchen würde, ist aber nicht genau dasselbe.

Etwas unscharf ausgedrückt betrachtet man ein Rechenverfahren als »effizient« oder auch »einfach«, falls die benötigte Rechenzeit mit ei-

INFO

Wie komplex ist komplex?

Ein Maß für Komplexität ist die Zahl der maximal notwendigen Rechenschritte eines Computers für eine gegebene Eingabelänge n.

Für Probleme der Komplexitätsklasse »P« (polynomial) wächst die Rechenzeit proportional zu einer Potenz k von n, also n^k. Solche Probleme gelten als »praktisch lösbar«.

Andere Probleme gehören zur so genannten Klasse »NP« (nichtdeterministisch polynomial). Unklar ist, ob **die Klassen P und NP identisch** sind: ob also die schwersten NP-Probleme ebenso effizient gelöst werden können wie P-Probleme. Kurz: Ist P = NP?

ner bestimmten Potenz der Ziffernzahl wächst, die ein bestimmtes Problem charakterisiert. Ein Algorithmus, der etwa eine Zahl q daraufhin prüft, ob sie eine Primzahl ist, könnte eine Rechenzeit haben, die mit der sechsten Potenz der Stellenanzahl von q anwächst.

Im Jargon der Mathematiker zählen Algorithmen, deren Laufzeit sich so verhält, »zur Klasse P«. Dabei steht das »P« für »polynomial«. Algorithmen, die polynomiale Rechenzeit haben (im Primzahlbeispiel also proportional zu n^6), weisen eine besondere Eigenschaft auf: Sie erweisen sich als vergleichsweise stabil. Wird etwa die Größe des Eingabewertes geringfügig vergrößert, verlängert sich die Rechenzeit nicht allzu sehr. Im Gegensatz dazu sind so genannte »Nicht-P«-Algorithmen im Allgemeinen ineffizient. Selbst wenn die Eingabedaten nur etwas umfangreicher werden, droht die Rechenzeit ins Astronomische anzuwachsen.

Etwas genauer betrachtet ist die Angelegenheit leider doch nicht ganz so einfach. Einerseits können manche Nicht-P-Algorithmen nämlich ziemlich effizient sein, zumindest solange die Eingabe nicht allzu umfangreich wird; andererseits können die Parameter mancher P-Algorithmen so groß werden, dass die Laufzeit ein Menschenleben überträfe. Trotzdem scheint die Unterscheidung zwischen P- und Nicht-P-Algorithmen die grundlegendste und wichtigste für alle Fragen zu sein, die mit der Effizienz von Algorithmen zu tun haben. Sie bietet Mathematikern eine Möglichkeit, den intuitiven Unterschied zwischen »leicht zu berechnen« und »schwierig zu berechnen« formal zu erfassen.

Gibt es denn so etwas wie wirklich schwierige Probleme? Die Antwort lautet »Ja, sogar ganz verschiedene Sorten«. Die offensichtlichen dieser Fälle sind aus einem ganz schlichten Grund schwierig, etwa, weil die Ausgabe des Ergebnisses viel zu lange dauert. Ein Beispiel: »Drucke alle möglichen Kombinationen der nachfolgenden Liste von Symbolen!« Für die 52 Karten in einem Kartenspiel wären das nämlich schon 80 658 175 17 0 943 878 571 660 636 856 403 766 975 289 50 5 440 883 277 824 000 000 000 000, also rund $8 \cdot 10^{67}$ verschiedene Anordnungen, und sie alle wären – dem »Algorithmus« zufolge – auszudrucken.

Ist eine leicht überprüfbare Lösung auch leicht zu finden?

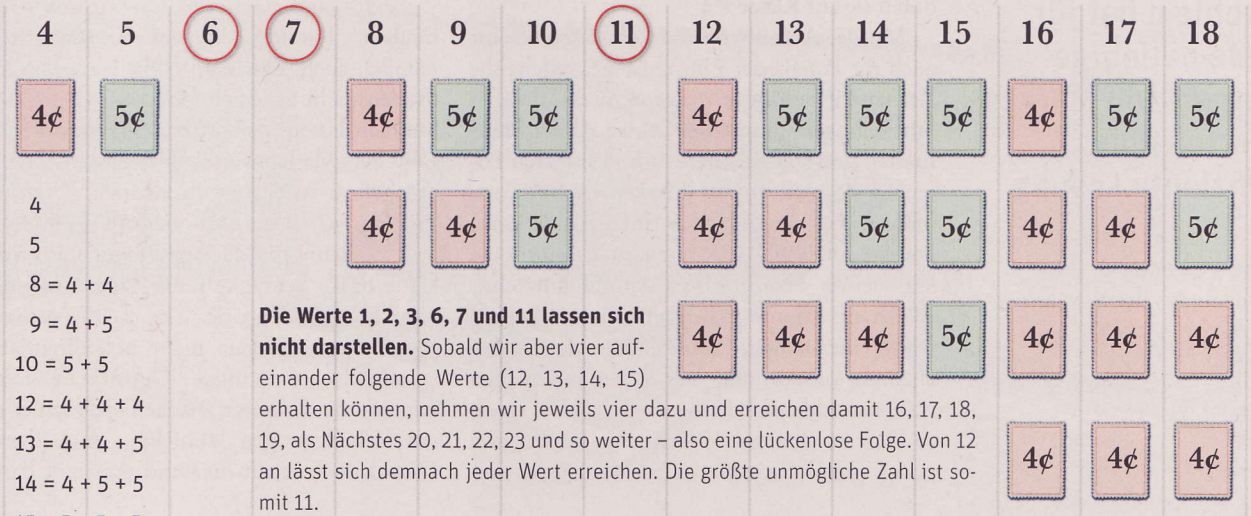
Probleme dieser simplen Art sollten ausgeschlossen werden. Wir erreichen das durch die Einführung einer neuen Klasse von Algorithmen, die im Fachjargon verwirrenderweise mit NP bezeichnet wird. Diese Abkürzung steht für eine »nichtdeterministisch polynomiale« Rechenzeit. Was heißt das? Die Definition lautet: Ein Problem gehört dann zur Klasse NP, wenn für jede vorgeschlagene Lösung in polynomialer – also akzeptabler – Zeit entschieden werden kann, ob sie richtig oder falsch ist. Eine grobe, aber dennoch hilfreiche Analogie liefern Puzzles. Es kann zwar sehr lange dauern, bis man alle Teile in einem Bild zusammengefügt hat – das wäre der nichtdeterministische Aspekt. Doch es genügt meist schon ein kurzer Blick, um festzustellen, ob das Ergebnis auch stimmt.

Diese Einteilung in die zwei Problemklassen P und NP hat zu einer fundamentalen Frage geführt, und wer sie beantwortet, der hat Anspruch auf den Clay-Preis: Ist NP gleich P, oder ist NP wirklich verschieden von P? Stark vereinfacht könnte man fragen, ob sich eine Frage, bei der sich leicht prüfen lässt, ob eine mögliche auch eine tatsächliche Lösung ist, nicht auch selbst einfach lösen lässt.

Kluge Köpfe behaupten, dass NP-Probleme nicht unbedingt zur Klasse P gehören müssen. Auch wenn es einfach ist, jede vorgeschlagene Lösung eines Problems auf ihre Korrektheit zu prüfen, lässt sich die Aufgabe selbst noch lange nicht dadurch effizient lösen, dass man immer wieder Lösungen rät und sie anschließend überprüft. Das übersteigt einfach alle Möglichkeiten. Stellen Sie sich zum Beispiel vor, Sie würden ein Zahlenschloss dadurch öffnen wollen, dass Sie nach-

Wie sich Briefmarken kombinieren lassen

Nehmen wir an, wir hätten zwei Sorten von Briefmarken zur Verfügung: zu 4 beziehungsweise 5 Cent. Welche Gesamtwerte lassen sich mit ihnen erreichen, und welches ist der größte, der nicht aus ihnen kombiniert werden kann? Offenbar sind folgende Werte möglich:



Die Werte 1, 2, 3, 6, 7 und 11 lassen sich nicht darstellen. Sobald wir aber vier aufeinander folgende Werte (12, 13, 14, 15) erhalten können, nehmen wir jeweils vier dazu und erreichen damit 16, 17, 18, 19, als Nächstes 20, 21, 22, 23 und so weiter – also eine lückenlose Folge. Von 12 an lässt sich demnach jeder Wert erreichen. Die größte unmögliche Zahl ist somit 11.

11 ist aber gleich $4 \cdot 5 - (4 + 5)$, und diese Formel erweist sich als universell. Haben die beiden Markenwerte x und y keinen gemeinsamen Faktor, dann ist der größte mit ihnen nicht erreichbare Wert $x \cdot y - (x + y)$. Mit den Briefmarkenwerten 99 Cent und 101 Cent lässt sich also jeder Wert kombinieren, der größer als $99 \cdot 101 - (99 + 101) = 9799$ Cent ist.

SPEKTRUM DER WISSENSCHAFT

einander alle Kombinationen ausprobieren. Natürlich verkündet irgendwann ein einfaches »Klick«, dass Sie die korrekte Lösung gefunden haben. Bei einem etwas komplizierteren Schloss jedoch könnten Sie Ihr ganzes Leben mit dem Durchprobieren aller möglichen Kombinationen verbringen, ohne jemals dieses Klick zu hören. Das Passwort eines Computers zu raten, bietet ein weiteres Beispiel für solch ein Problem.

Anlass zu Optimismus

Sogar ohne den Clay-Preis als Ansporn würden wohl die meisten Mathematiker ihr letztes Hemd verkaufen, wenn sie dadurch herausfinden könnten, ob NP tatsächlich verschieden von oder gleich P ist. Auch für die Fachleute ist diese Frage ebenso rätselhaft wie fundamental. Das wirklich Quälende daran ist eine Eigenschaft, die »NP-Vollständigkeit« genannt wird. NP-vollständige Probleme bilden eine spezielle Teilmenge aller NP-Probleme. NP-vollständig sind sie genau dann, wenn eine effiziente Lösung für eines von ihnen dazu dienen kann, auch jedes andere NP-Problem effizient zu lösen.

Anders ausgedrückt: Findet sich ein effizientes Verfahren zur Lösung irgendeines NP-vollständigen Problems, dann hat man bewiesen, dass alle NP-Probleme auch zur Klasse P gehören. Die Sache ist keineswegs rein exotisch: So hat sie beispielsweise Bedeutung für das Thema Sicherheit von Bankgeschäften – das ist schon ein guter Grund, nach einer Lösung zu suchen. Was uns wieder zu unserem Ausgangsthema bringt – den Briefmarken.

Im Jahr 1996 bewies Jorge Ramirez-Alfonsin von der Université Pierre et Marie Curie in Paris, dass die allgemeine Version des Briefmarkenproblems – mit einer unbeschränkten Zahl von Markenwerten – NP-vollständig ist. Falls also für die Frage der Briefmarkenstückelungen eine effiziente Lösungsmethode existiert, dann lässt sich auch jedes andere NP-Problem ebenso ökonomisch lösen.

Tja, gibt es denn nun dafür eine effiziente Methode? Bisher noch nicht, aber zumindest gibt es neuen Anlass zu Optimismus, wenigstens für eine vereinfachte Fassung des Problems. Dabei wird eine Schranke für die Anzahl der Markenwerte zugelassen – drei, vier, zehn, hundert oder irgendeine andere. Allerdings ist das Problem mit einer solchen Schranke, egal wie groß sie auch ist, nicht mehr NP-vollständig. Außerdem lassen sich für das Briefmarkenproblem keine so ein-

Das Briefmarkenproblem hat für jede beliebige Anzahl von Markenwerten eine effiziente Lösung

fachen Lösungsformeln angeben, wie sie Sylvester entdeckt hatte. Komplexere Algorithmen kann man jedoch auf diesen Problemtyp anwenden, und auch sie laufen, im Prinzip jedenfalls, mit polynomialer Rechenzeit. Betrachten wir also solche speziellen Beispiele für unser NP-vollständiges Problem, dann gehören sie zur Klasse P.

Mit der Anzahl von Markenwerten wächst auch die Potenz der Eingabelänge, welche die Rechenzeit bestimmt. Angenommen, für drei Stückelungen könnte man einen Algorithmus finden, dessen Rechenzeit mit der dritten Potenz der Stellenzahl der Markenwerte variiert; für vier Werte würde dies einen Algorithmus liefern, für den die Rechenzeit proportional zur vierten Potenz dieser Anzahl anwächst. Allgemein könnte man dann für n Markenwerte einen Algorithmus finden, dessen Rechenzeit proportional zur n-ten Potenz der Stellenanzahl anwächst.

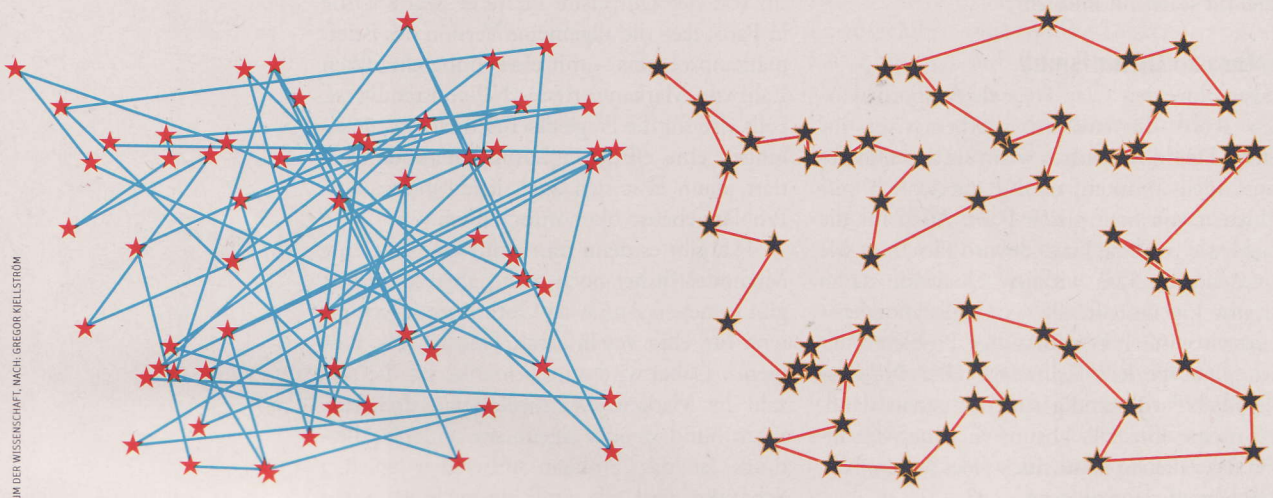
Das ist eine gute Nachricht: Denn grob gesagt gehört bei diesem Szenario jedes einzelne, also das Drei-Marken-, das Vier-Marken- oder auch das 1000-Marken-Problem, zur Klasse P. Tatsächlich hat Ravi Kannan, heute an der Yale University in New Haven, bereits 1992 gezeigt, dass eine effiziente Lösung für jede beliebige Anzahl von Markenwerten existiert.

Leider sind nicht alle Nachrichten so erfreulich. Ramirez-Alfonsins Theorem zeigt nämlich auch, dass sich all die einzelnen Methoden nicht zu einem einzigen Algorithmus bündeln lassen, der unabhängig von der Anzahl der Markenwerte effizient ist. Zusammengefasst zu einem allgemeinen n-Marken-Problem wären sie nicht mehr in der Klasse P, weil es dann für die auftretenden Potenzen keine obere Schranke mehr gäbe. Außerdem zeigt Kannans Theorie, dass ihr theoretischer Begriff von Effizienz nicht unbedingt auch »praktisch« sein muss: Gigantische Exponenten oder Faktoren machen viele seiner guten Überlegungen zunichte. Aus diesem Grund denkt auch niemand ernsthaft daran,

DIE HANDLUNGSREISE – EIN BESONDERS SCHWERES NP-PROBLEM?

Das Problem des Handlungsreisenden (englisch: *travelling salesman problem*) wurde bereits im 19. Jahrhundert diskutiert, in seiner allgemeinen Form aber erst in den 1930ern von dem aus Wien stammenden Mathematiker Karl Menger untersucht. Dabei wird eine Rundreise durch mehrere Orte gesucht mit der Eigenschaft, dass die gesamte Reisestrecke bis zur Rückkehr zum Ausgangsort möglichst kurz ist. Heute steht eine Vielzahl von heuristischen und exakten Methoden zur Verfügung, mit denen auch schwierige Fälle mit mehreren tausend Städten optimal gelöst wurden. Dieses Problem gilt als »NP-schwer«.

Einfach gesagt: Es ist mindestens so komplex (schwer) wie die schwersten Problem in der NP-Klasse. Forscher vermuten daher, dass die längste Laufzeit jedes deterministischen Algorithmus, der für dieses Problem stets optimale Lösungen liefert, im besten Fall »nur« exponentiell mit der Anzahl der Städte variiert. Schon für wenige Städte kann die benötigte Laufzeit eines solchen Algorithmus also unpraktikabel viel Zeit beanspruchen. Das Problem des Handlungsreisenden tritt in vielen praktischen Anwendungen auf, etwa beim Design von Mikrochips, bei der Verteilung von Waren, der Tourenplanung von Kunden- oder Pannendiensten und bei Genomsequenzierung.



SPEKTRUM DER WISSENSCHAFT, NACH: GREGOR KIELLSTRÖM

Eine Reise durch 60 Städte: links mit einem zufälligen, rechts mit einem optimierten Weg

Einige der Mathematiker, die das Sortierproblem vorantrieben (im Uhrzeigersinn): Stan Wagon, Jorge Ramirez-Alfonsin, Ravi Kannan sowie Bjarke Roune

Kannans Methode für ein konkretes Computerprogamm zu benutzen.

Die jüngste Wendung unserer Geschichte ist nun wieder ermutigender. Stan Wagon vom Macalester College in St. Paul, Minnesota, und seine Kollegen können jetzt das Vier-Marken-Problem für Zahlen mit 100 Stellen auf einem schnellen PC in etwa einer Sekunde lösen und das Zehn-Marken-Problem für Zahlen mit zehn Stellen in zwei Tagen. Noch erfolgreicher war Bjarke Roune an der Universität Aarhus. Dem jungen dänischen Computerwissenschaftler gelang es mit Methoden der algebraischen Geometrie auf seinem Rechner, das Vier-Marken-Problem mit 10 000-stelligen Zahlen in wenigen Sekunden und das 13-Marken-Problem für zehnstellige Zahlen in wenigen Tagen zu knacken.

Unsichere Kontodaten

Zwar bleibt das allgemeine *n*-Marken-Problem davon unberührt, aber diese Resultate zeigen zumindest, dass ein NP-vollständiges Problem in vielen konkreten Fällen gelöst werden kann. Man stelle sich einmal vor, eine einzige, »hässliche« Kombination der Markenwerte unter Billionen von Möglichkeiten würde eine ewige Rechenzeit verschlingen, während sich alle übrigen in wenigen Minuten erledigen ließen. Die Wahrscheinlichkeit, gerade auf einen dieser hässlichen Fälle zu stoßen, wäre vernachlässigbar. Obwohl also bei diesem Szenario das allgemeine Problem NP-vollständig ist, könnten sich die meisten konkreten Beispiele bei richtigem Vorgehen als viel einfacher entpuppen.

Dass so etwas passieren kann, zeigt das berühmte »Problem des Handlungsreisenden« (siehe Kasten links) – dabei geht es um die Berechnung des kürzesten Rundwegs durch *n* Städte, der genau einmal durch jede Stadt führt – sowie um andere Probleme aus der Wirtschaftsmathematik. Auch beim Briefmarkenproblem stellt sich heraus, dass konkrete Beispiele einfach lösbar sind. Und das könnte bei anderen NP-vollständigen Problemen ebenso passieren.

All das hat auch praktische Konsequenzen. Selbst wenn das Verfahren, das Ihre Bank einsetzt, um Kontodaten zu verschlüsseln, »im Allgemeinen« NP-vollständig ist – was mehr wäre, als gegenwärtig für die meisten der tatsächlich verwendeten Verschlüsselungsverfahren bewiesen werden kann –, könnte das konkret von Ihrer Bank eingesetzte Verfahren trotzdem unsicher sein. Vermutlich ist das noch kein Anlass, um gleich loszurennen und die Kontoauszüge zu prüfen. Es könnte aber dazu anregen, sich über das Thema »sichere Verschlüsselung« ein paar Gedanken zu machen.

Die neuesten Entwicklungen beim Briefmarkenproblem lassen hoffen, dass viele der Probleme, die bisher als unlösbar galten, dennoch lösbar sind. Schließt man nämlich die seltenen übelsten Szenarios aus und konzentriert man sich auf die Untersuchung der typischen und häufigsten Fälle, dann klappt es ja vielleicht. ◁

Ian Stewart ist Mathematiker, Buchautor und Wissenschaftsjournalist. Er unterrichtet als Professor an der University of Warwick in England. Sein letztes Buch schildert »Die wunderbare Welt der Mathematik« (Piper-Verlag, München 2007).

Clay Mathematics Institute siehe www.claymath.org/millennium/.

Zum Problem des Handlungsreisenden siehe http://de.wikipedia.org/wiki/Problem_des_Handlungsreisenden.

Zur Kompexitätstheorie siehe http://de.wikipedia.org/wiki/Komplexitätstheorie.

Weitere Weblinks zu diesem Thema finden Sie unter www.spektrum.de/artikel/965711.