

Rätselhafte Triebfeder für Quantencomputer

Forscher debattieren über die Notwendigkeit von Verschränkungen für das parallele Rechnen

Die Verschränkung von Teilchen gilt als Voraussetzung, um mit einem Quantencomputer parallel rechnen zu können. Manche Forscher bezweifeln das. Sie glauben, auch einfacher ans Ziel gelangen zu können.

Christian Meier

Ein Quantencomputer ähnelt einem fiktiven Schachspieler, der alle denkbaren Reaktionen seines Gegners parallel in seinem Kopf durchprobieren kann. Er testet alle möglichen Lösungswege im gleichen Moment und filtert den richtigen heraus. Dank diesem Auf-einen-Blick-Erfassen könnten künftige Quantenrechner beispielsweise grosse Datenbanken viel schneller durchsuchen als heutige Rechner; oder sie könnten grosse Zahlen in Windeseile in ihre Primfaktoren zerlegen. Doch das ist noch Zukunftsmusik: Die ersten Quantenrechner lösen nur kleine Problemchen zu Demonstrationszwecken. Vor allem aber arbeiten sie nur in der extrem kontrollierten Umgebung einiger Physikalabors. Denn jeder Umwelteinfluss – und sei es nur die Kollision mit einem einzigen Luftmolekül – zerstört die fragile Beziehung zwischen den Quantenobjekten, auf der die Parallelität eines Quantencomputers beruht.

Mysteriöse Fernwirkung

Manche Physiker glauben indes, dass Quantencomputer auch mit einem gehörigen Mass an Unordnung in ihren logischen Schaltkreisen herkömmliche Rechner überflügeln können. Vor gut drei Jahren behauptete Animesh Datta von der University of Oxford, dies sei

dank einem rätselhaften Quantenphänomen namens Discord möglich. Sollte er recht haben, könnten Quantenrechner viel schneller in den Alltag eindringen, als dies angesichts der schleppenden Fortschritte in dem Gebiet bisher angenommen wurde. Diese Aussicht hat Physiker auf der ganzen Welt veranlasst, sich intensiv mit dem Discord zu beschäftigen.

Was Quantencomputer nach heutigem Verständnis so schlagkräftig macht, ist eine bestimmte Art der Fernwirkung zwischen Atomen oder anderen Quantenobjekten: die sogenannte Verschränkung. Verschränkte Teilchen bilden auf unheimliche Weise eine Einheit: Misst man etwa die Polarisationsrichtung eines Photons, das mit einem zweiten verschränkt ist, wird im selben Moment die Polarisationsrichtung des anderen festgelegt, selbst dann, wenn dieses Lichtjahre entfernt ist.

Die Verschränkung von Atomen, Photonen oder anderen Quantenobjekten macht es möglich, mit einem Quantencomputer parallel zu rechnen und viele Lösungswege gleichzeitig auszuprobieren. Denn durch die Verschränkung potenziert sich die Zahl der Zustände, in die man einen Quantencomputer gleichzeitig versetzen kann. Sind es mit einem einzelnen Teilchen zwei Zustände (0 und 1), können zwei verschränkte Teilchen bereits vier Zustände parallel einnehmen (00, 01, 10 und 11). Vierzehn miteinander verschränkte Kalzium-Ionen – der derzeitige Rekord im Verschränken, gehalten von Physikern der Universität Innsbruck – nehmen 16 384 Zustände synchron ein. Dank dieser Parallelität wächst die Rechenzeit für bestimmte Aufgaben relativ langsam mit der Grösse der Eingabe, also etwa der Zahl der Einträge in einer Datenbank. Experten

sprechen daher von einem «exponentiellen Geschwindigkeitsgewinn».

Der Haken: Die Verschränkung ist eine Mimose. Die kleinste Störung von aussen zerstört die Innigkeit zwischen den Partikeln. Dies geschieht binnen Sekundenbruchteilen, weshalb selbst die geschützten Quantenrechner in heutigen Labors extrem fehleranfällig sind. Die Verschränkung halten viele Physiker aber für die unabdingbare Quelle der Schnelligkeit von Quantenrechnern. Sie tüfteln daher an Verfahren, um die Fehler effizient zu korrigieren.

Es geht auch ohne

Datta zweifelt jedoch an der Notwendigkeit der Verschränkung. Auch in einem Teilchensystem, das mit der Umwelt in Verbindung stehe, gebe es Quantenkorrelationen, mit denen sich parallel rechnen lasse, sagt er. Datta meint damit Korrelationen zwischen Teilchen, die unter dem Einfluss der Umwelt zumindest teilweise in einen gemischten Zustand übergegangen sind. Zwar können solche Teilchen nicht mehr miteinander verschränkt werden. Trotzdem kann es zwischen ihnen noch gespenstische Fernwirkungen geben, die man in makroskopischen Systemen vergebens sucht. Formal lässt sich das durch den sogenannten Discord zum Ausdruck bringen. Diese Grösse ist ein Mass für die Quantenkorrelationen in einem System und kann auch ohne Verschränkung grösser als null sein. Nach Ansicht von Datta sollte das für einen Quantencomputer genügen.

Die Aussicht, ohne den üblichen Aufwand einen Quantencomputer zu betreiben, hat Andrew White von der University of Queensland motiviert, Dattas These experimentell zu prüfen. Er verwendete dazu zwei Photonen, mit

denen er eine bestimmte Rechenaufgabe löste. Das Teilchensystem wurde kaum von der Umwelt abgeschirmt, und es lag keine Verschränkung vor. Dennoch habe der einfache Computer das Problem exponentiell schneller gelöst als ein klassischer Rechner, sagt White.

Wie White durch Messungen feststellte, war der Discord grösser als null. Also gab es tatsächlich eine irgendwie geartete Fernwirkung zwischen den Quanten – einen unempfindlichen Bruder der Verschränkung. «Der Discord lässt sich als Triebkraft für Quantenrechner nutzen», ist Datta überzeugt. Als Vorteile sieht er nicht nur den geringeren Aufwand. «So ein Rechner wäre wesentlich fehlertoleranter.» Er wäre darüber hinaus leichter zu skalieren – die Leistungsfähigkeit lasse sich also ohne überproportionalen Aufwand steigern.

Forscher fragen sich allerdings, ob mit dem Discord die gleiche Parallelität, also der gleiche Geschwindigkeitsgewinn, erreichbar ist wie mit der Verschränkung. Der Discord sei eine schwächere Triebkraft als die Verschränkung, räumt Datta ein. Ein Discord-basierter Quantencomputer stelle einen Mittelweg dar zwischen dem, was wünschenswert, und dem, was machbar sei. Für viele praxisrelevante Aufgaben sei ein exponentieller Geschwindigkeitsgewinn möglich, sagt Datta. Beispielsweise bei der Simulation von magnetischen Materialien, was die Entwicklung neuer Werkstoffe voranbringen könne.

Fehlendes Verständnis

Doch bis es so weit ist, gibt es noch viel zu erforschen. Derzeit versuchen Physiker herauszufinden, wie der Discord Quantenrechner antreibt. Letztes Jahr zeigte Bryan Eastin vom National Insti-

tute of Standards and Technology in Boulder, Colorado, dass sich während jeder Rechnung in einem Quantencomputer Discord aufbaut. Dass dieser aber eine tragende Rolle spielt, ist damit nicht bewiesen, geschweige denn, welche. Eine genaue Analyse der Mechanismen, die hinter dem Discord stecken, ist nötig, um Discord-basierte Quantencomputer für Praxisaufgaben programmieren zu können.

Doch das könnte dauern, denn laut Tommaso Calarco von der Universität Ulm fehlt ein entscheidendes Forschungswerkzeug: ein Quantenrechner, der diesen Namen verdient. Die jetzigen Maschinen sind eher Spielzeuge, die sich zu einem praktisch nutzbaren Quantencomputer etwa so verhalten wie eine mechanische Additionsmaschine zu einem PC. «Wir verstehen nur für bestimmte Fälle, wie die Verschränkung Rechnungen antreibt», sagt Calarco. Man tue sich schwer, Neues auszuprobieren. «Wir haben keinen Rechner, den wir Ingenieuren in die Hand geben könnten, damit sie damit kreativ spielen», sagt der Physiker. Also könne kein allgemeines Verständnis der Verschränkung entstehen. Dattas und Whites Discord betrachtet Calarco als eine noch unverstandene Form der Verschränkung.

Das passt zu einem Vorschlag brasilianischer Physiker vom Februar dieses Jahres. Demnach wirken verschiedene Teile eines Discord-basierten Quantenrechners indirekt aufeinander ein: Jeder von ihnen baut eine Verschränkung mit der Umwelt auf, die somit zu einer Art Brücke zwischen den Teilen wird.

Die Debatte um den Discord offenbart vor allem eines: Die Wissenslücken klaffen noch zu weit, als dass in absehbarer Zeit ein praxistauglicher Quantencomputer den Kalkulationen Flügel verleihen könnte.

Ein Quantenprozessor der anderen Art

Die kanadische Firma D-Wave stellt beim Rechnen mit Quantenbits das vorherrschende Dogma in Frage

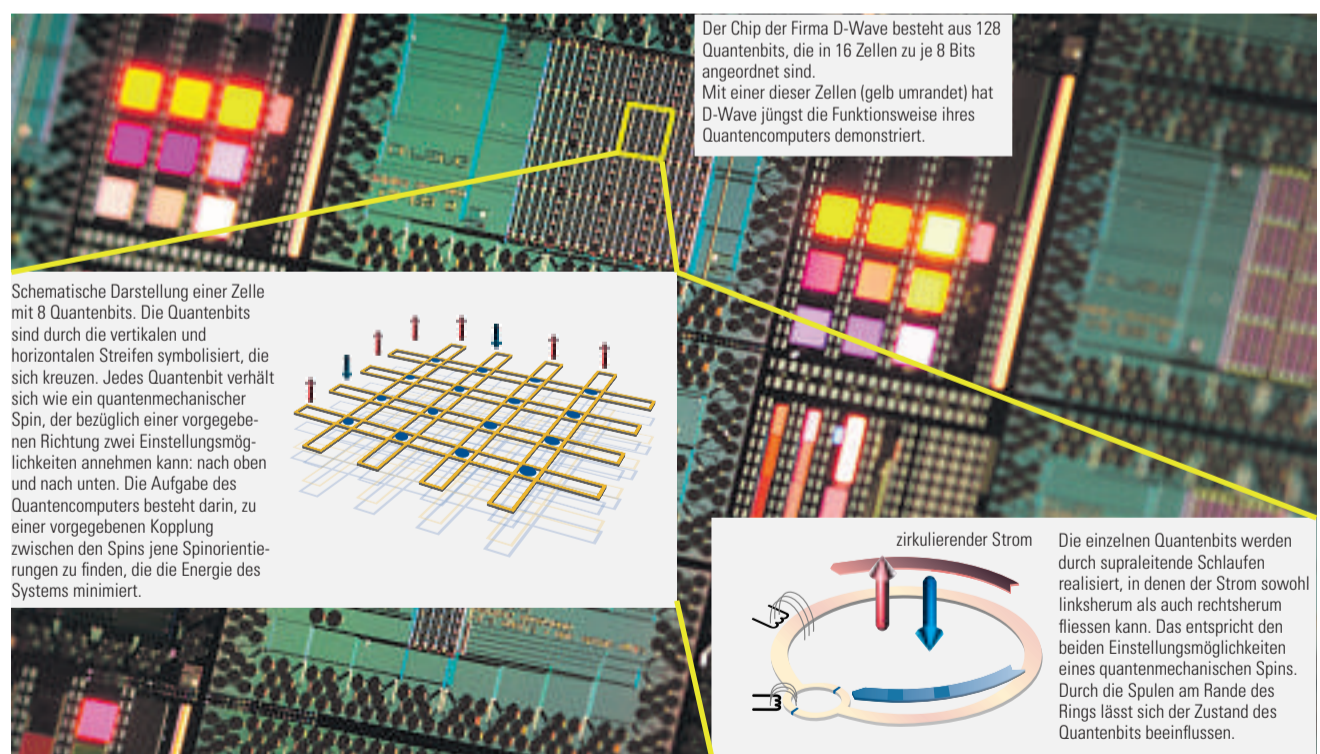
Christian Speicher · Ende Mai gab die kanadische Firma D-Wave bekannt, sie habe einen Quantencomputer mit 128 Quantenbits an den amerikanischen Rüstungskonzern Lockheed Martin verkauft. Lockheed Martin plane, den Prozessor für die Lösung besonders anspruchsvoller Computerprobleme einzusetzen. Die Meldung liess aufhorchen. Wenn man sich vor Augen hält, dass Quantencomputer noch im Laborstadium stecken und bestenfalls mit wenigen Quantenbits «rechnen» können, schien diese Ankündigung zu schön, um wahr zu sein. Anders als im Jahr 2007, als D-Wave einen Sudoku-Rätsel lösenden Quantencomputer präsentiert hatte, hielt sich die Forschungsgemeinschaft jedoch mit negativen Kommentaren zurück. Denn mit einer Publikation in der Fachzeitschrift «Nature» hatte sich D-Wave kurz zuvor erstmals in die Karten blicken lassen.

Suche nach dem Optimum

Unter einem Quantencomputer verstehen Forscher in der Regel eine Rechenmaschine, in der logische Schaltungen die in den Quantenbits gespeicherten Informationen nach einem vorgegebenen Algorithmus bearbeiten. Der Quantencomputer der Firma D-Wave ist anders. Zwar werden die Informationen auch hier in Quantenbits gespeichert. Die eigentliche Berechnung erfolgt jedoch nicht durch logische Schaltkreise, sondern durch einen Prozess, der gewisse Ähnlichkeiten mit dem Ausglühen von Metallen hat. Wenn man ein Metall erhitzt und es danach langsam wieder abkühlt, so kann man auf diese Weise Defekte im Kristallgitter zum Verschwinden bringen. Das Metall geht durch das Ausglühen von einem metastabilen Zustand idealerweise in den Zustand niedrigster Energie über.

Was das mit dem Lösen von mathematischen Problemen zu tun hat, ist auf den ersten Blick nicht ersichtlich. Tat-

Ein Zoom in den Quantencomputer der Firma D-Wave



QUELLE: D-WAVE

NZZ-INFOGRAFIK/cke.

sächlich lassen sich jedoch viele mathematische Optimierungsprobleme eins zu eins auf das physikalische Problem übertragen, den Grundzustand eines Systems aus wechselwirkenden Spins zu finden. Wenn jeder der Spins bezüglich einer vorgegebenen Richtung nur nach oben oder nach unten zeigen kann, gilt es also, unter den vielen Kombinationsmöglichkeiten jene zu finden, die die Gesamtenergie des Systems minimiert. Die Hoffnung ist, dass Optimierungsprobleme, die mit einem herkömmlichen Computer wegen der grossen Zahl der möglichen Lösungen nicht in vertretbarer Zeit gelöst werden können, mit einem Quantencomputer sehr viel schneller geknackt werden können.

Die Voraussetzung dafür ist, dass sich die Quantenbits des Quantencomputers wie Spins verhalten und dass sich die Wechselwirkung zwischen ihnen variieren lässt. Die Idee ist die folgende: Man startet mit einer möglichst einfachen Situation, für die der Grundzustand leicht zu finden ist. Anschliessend verändert man die Wechselwirkungen zwischen den Spins so lange, bis sie dem komplizierten Optimierungsproblem entsprechen, das man lösen will. Geschieht diese Transformation adiabatisch, also so sanft, dass das System während der gesamten Entwicklung im jeweiligen Grundzustand bleibt, so muss man die Lösung am Ende nur noch ablesen.

Der Vorteil gegenüber einem auf logischen Schaltungen basierenden Quantencomputer liegt auf der Hand. Während dieser mit angeregten und damit fragilen Zuständen rechnet, verharret ein adiabatischer Quantencomputer idealerweise stets im Grundzustand. Die Quantenbits können also durch äussere Störungen nicht in einen noch tieferen Energiezustand befördert werden. Das macht sie relativ robust.

Als die Firma D-Wave 2007 den ersten Prototyp ihres Quantencomputers präsentierte, waren viele Forscher skeptisch. Sie bezweifelten, dass dieser überhaupt Quanteneffekte nutzt. Diese Zweifel hat D-Wave mit der Publikation in «Nature» ausgeräumt. Zwar wurde

dort nicht der gesamte Chip getestet. Anhand einer Zelle aus 8 Spins konnten die Forscher aber zeigen, dass es tatsächlich Quanteneffekte sind, die das System seinen Grundzustand finden lassen.

Das Problem der Skalierung

Die «Nature»-Publikation habe dazu beigetragen, dass viele Forscher den Anstrengungen von D-Wave nun aufgeschlossener gegenüberstünden, sagt Edward Farhi vom Massachusetts Institute of Technology, der vor über zehn Jahren die ersten Überlegungen zum adiabatischen Quantencomputer angestellt hatte. Zwar könne man mit 8 Quantenbits noch keine ernsthaften Probleme lösen. Wenn man aber davon ausgehe, dass D-Wave mit den 128 Quantenbits auf dem Chip in gleicher Weise rechnen könne, werde es langsam interessant.

Selbstverständlich ist das nicht. Zwar sind die Zustände, mit denen ein adiabatischer Quantencomputer rechnet, relativ robust. Mit zunehmender Anzahl von Quantenbits wächst aber auch die Zahl der möglichen Energiezustände des Systems. Man muss daher damit rechnen, dass die Energielücke zwischen dem Grundzustand und dem ersten angeregten Zustand während einer Berechnung sehr klein wird. Dadurch besteht eine gewisse Wahrscheinlichkeit, dass das System der Spins am Ende im falschen Zustand landet.

Um das zu verhindern, muss man das System langsam durch den «Engpass» manövrieren – und zwar umso langsamer, je kleiner die Energielücke ist. Das geht auf Kosten der Rechengeschwindigkeit. Ob ein adiabatischer Quantencomputer komplizierte Optimierungsprobleme deutlich schneller lösen kann als ein herkömmlicher Rechner, hängt also davon ab, ob man Rechenpfade findet, die die übelsten Engpässe umgehen. Ob es solche Pfade gibt, ist bis heute unbewiesen.