> WISSEN

SIEBENMEILEN-STIEFEL FÜR COMPUTER

Wunder ist ein großes Wort, und ein sehr ungewöhnliches, wenn die Rede von Computern ist. Wenn aber eine neue Technikära dämmert, in der Rechner sicher geglaubte Verschlüsselungen knacken und schier unendlich komplexe Aufgaben im Handumdrehen lösen, liegen mystische Begriffe nahe. Auch wenn es die in Tausenden Experimenten bestätigte Quantenmechanik ist, die das Mirakel produziert.

Die neue Ära des „Wunderrechners", wie die Medien den Quantencomputer gerne nennen, ist nah. Zumindest macht das das Stakkato glauben, in dem Protagonisten der Branche neue Fortschritte melden. Google etwa will bald zum ersten Mal eine Anwendung demonstrieren, bei der ein Quantencomputer schneller ist als der größte Supercomputer des Planeten. „Sehr wahrscheinlich" noch dieses Jahr könne die sogenannte Quantenüberlegenheit („quantum supremacy") erreicht werden, glaubt John Martinis von der University of California in Santa Barbara, der für Google einen Quantenrechner entwickelt. Der IT-Riese IBM wiederum hat jüngst seinen ersten kommerziellen Quantencomputer vorgestellt, der die Quantenüberlegenheit aber noch nicht erreicht. Auch China will die Schwelle zum neuen Zeitalter möglichst bald überwinden. Es investiert gigantische zehn Milliarden US-Dollar in ein Forschungszentrum zum Thema. Der chinesische Online-Händler Alibaba bietet Zugriff auf seinen Quantenrechner über die Cloud. Die Europäische Union läutet zur Aufholjagd: Eine Milliarde Euro investiert sie in ein „Flaggschiff-Projekt" für Quantentechnologie, das Forschung und Industrie zusammenbringen soll. Eines der Ziele: zwei leistungsstarke Quantenrechner binnen drei Jahren zu bauen.

Auch die Abwehrfront gegen den Wundercomputer formiert sich, da dieser im Internet viel genutzte Verschlüsselungen oder digitale Signaturen bedroht. Kryptologen entwickeln daher neue Verschlüsselungsmethoden, die vor Angriffen aus dem Reich der Quanten schützen sollen. Sie empfehlen, diese schon jetzt beim Design neuer Software vorzusehen, um sie schnell gegen die alten Methoden eintauschen zu können. Auch die „Quantenkommunikation" sichert gegen einen Lauschangriff per Quantencomputer, da sie einzelne Lichtteilchen nutzt, die ein Lauscher zwangsläufig verändert. Armando Rastelli von der Universität Linz entwickelt dazu Quellen für einzelne Photonen.

Indessen: Nicht alle befeuern den Hype um die neue Computertechnik. Die europäische Industrie etwa zögert mit Investitionen. Zum Bau der Quantencomputer des „Quanten-Flaggschiffs" der EU trägt sie einige Geräte bei, aber kein Geld. Mancher Physiker, der am „Wunderrechner" bastelt, ärgert sich über allzu vollmundige Ankündigungen von US-amerikanischen Unternehmen. Sie fürchten, dass die Prophezeiung wundersamer Rechenpower zu Enttäuschungen und in der Folge gekürzten Forschungsbudgets führen könnte.

Und das, obwohl sie selbst um die unbegreiflichen Phänomene in der Welt der kleinsten Teilchen wissen. Übertragen auf den Alltag würde diese jedermann „unmöglich" nennen. Der österreichische Physiker Erwin Schrödinger hat dafür ein Gedankenexperiment ersonnen. „Schrödingers Katze" ist in einer Kiste gefangen, die einen tödlichen Mechanismus enthält: Ein radioaktives Atom löst die Freisetzung von Gift aus, sobald es zerfällt. Laut Quantenmechanik ist das Atom in einem Schwebezustand, solange die Kiste für einen Beobachter verschlossen bleibt. Es ist gleichzeitig zerfallen und intakt. Somit wäre die Katze simultan lebendig und tot. „Absurd", sagt der „gesunde Menschenverstand". Das Haustier könne nicht leben und nicht leben. Genau wie eine Tasse entweder hier oder dort steht und nicht an zwei Orten simultan.

Und doch bestätigen Experimente mit Quantenobjekten wie Molekülen, Atomen oder Elektronen immer wieder diese „Superposition" von Möglichkeiten, die sich eigentlich ausschließen. Die Superposition ist vielgestaltig: ein Elektron, das links und rechts herum rotiert, ein Lichtteilchen, dessen Polarisation in zwei Richtungen weist, oder elektrischer Strom, der durch eine supraleitende Schleife im und gegen den Uhrzeigersinn fließt.

Die Parallelexistenz lässt sich in die Sprache der Computer übersetzen. Die kleinste klassische Informationseinheit, das Bit, speichert entweder 0 oder 1. Dank der Superposition verkörpern Atome oder andere Teilchen ein Quantenbit, kurz Qubit. Dieses speichert 0 und 1 simultan. Interessant wird es durch das Hinzufügen weiterer Qubits: Jedes einzelne verdoppelt die Anzahl der simultan speicherbaren Werte.

FOTO: IBM/GRAHAM CARLOW (KÜHLSYSTEM DER QUANTENPROZESSOREN VON IBM)

Daher halten schon 300 Qubits mehr Zahlen vor, als es Teilchen im bekannten Universum gibt.

Ein weiteres „Wunder" der Quantenphysik macht aus dem astronomischen Speicher einen superschnellen Rechner: die sogenannte „Verschränkung". Zwei Teilchen, die einmal miteinander in Wechselwirkung standen, beispielsweise kollidiert sind, bilden fortan eine Einheit, ähnlich wie ein Paar Schuhe. Ihre Verbindung bleibt, auch wenn sie sich beliebig weit voneinander entfernen. Verändert man den Zustand des einen Partners, ändert sich der des anderen im selben Moment. Im Bild mit den Schuhen: Geht der eine von einer Superposition aus linkem und rechtem Schuh in den eindeutigen Zustand „linker Schuh" über, wechselt der andere Partner, und sei er Lichtjahre entfernt, zeitgleich in „rechter Schuh". Einstein nannte das ungläubig „spukhafte Fernwirkung". Doch der Spuk ist experimentell bewiesen: Chinesische Physiker demonstrierten die Verschränkung von Photonen über 1203 Kilometer hinweg. Magie ist indessen nicht im Spiel: Das Phänomen folgt klaren mathematischen Regeln und lässt sich exakt reproduzieren. Die Welt der Quanten ist materiell, sie tickt nur anders.

Durch die Verschränkung lassen sich einzelne Qubits miteinander verschalten. Die Schaltungen führen dann gemeinsam logische Operationen aus, ähnlich wie elektronische Schaltkreise heutiger Computer. Mit dem Unterschied, dass ein Quantenschaltkreis alle Aktionen, die dieser Schaltung möglich sind, simultan ausführt. Bildlich gesprochen wie ein Taschenrechner, der die Zahlen 3 und 7 mit einem Knopfdruck addiert, subtrahiert, multipliziert und dividiert. Gewissermaßen geht ein Quantenrechner alle Lösungswege parallel.

Dadurch ist es ihm theoretisch möglich, hochkomplexe Aufgaben zu knacken, indem er alle denkbaren Varianten durchprobiert. Er ermittelt etwa, aus welchen Primzahlen sich eine Zahl mit Hunderten von Dezimalstellen zusammensetzt. Dafür gibt es keine Formel, im Wesentlichen muss man alle Kandidaten durchprobieren. Und das sind mehr, als es Teilchen im Universum gibt. Ein klassischer Rechner bräuchte dafür Äonen. Wegen ihrer praktischen Unknackbarkeit beruhen Verschlüsselungen und digitale Signaturen im Internet auf dieser „Faktorisierung". Doch ein leistungsstarker Quantencomputer könnte sie binnen Minuten ausführen – und Codes knacken.

Laborprototypen von Quantenrechnern haben bislang jedoch nur sehr kleine Zahlen faktorisiert. Denn sie besitzen nur wenige Qubits. Der größte Quantenrechner, bei dem einzelne Qubits wahlweise miteinander verschränkt werden können, hat 20 Qubits aus Kalzium-Ionen, gebaut vom Team um Rainer Blatt von der Universität Innsbruck. Zwar hat John Martinis von Google einen Quantenrechner mit 72 Qubits und IBM einen mit 50 gebaut, jeweils bestehend aus supraleitenden Leiterschleifen. Doch lassen sich deren Qubits nicht so präzise kontrollieren wie die der Innsbrucker Maschine. Würden sie es, dann wäre die Quantenüberlegenheit bereits erreicht. Denn kein Supercomputer ist in der Lage, Moleküle mit mehr als 50 Atomen exakt zu simulieren, eine Anwendung, die die Wirkstoffsuche in der Pharmaindustrie beschleunigen würde. Der Quantenrechner könnte es – ohne Etagen voller Computerschränke. Das soll in den nächsten Jahren möglich sein. Doch es wäre erst ein bescheidener Anfang. Um klassische Rechner auch auf Gebieten wie der Mustererkennung, dem maschinellen Lernen oder der Optimierung von Verkehrsströmen zu schlagen, bräuchte es Quantenrechner mit Tausenden oder Hunderttausenden von Qubits.

Doch diese sind alles andere als leicht zu bauen. Das Problem ist, dass eine Katze entweder lebt oder tot ist, nie beides. Im Alltag sehen wir keine Superposition. Denn der Schwebezustand ist empfindlicher als jedes Soufflee. Sobald ein Quantenobjekt mit seiner Umwelt interagiert, wechselt es in die Eindeutigkeit. Schon ein Stoß mit einem Luftmolekül löst diesen Übergang aus, im Fachjargon „Dekohärenz" genannt. Je größer ein System, desto wahrscheinlicher werden solche Wechselwirkungen. Was Physiker mit dem Quantencomputer anstreben, ist daher etwas Unnatürliches: ein System aus Tausenden oder Millionen Qubits in Superposition zu halten. „Das ist etwa so, als würde man versuchen, den radioaktiven Zerfall eines Atoms zu stoppen", drückt es Ferdinand Schmidt-Kaler von der Universität Mainz aus, der einen Quantenrechner aus Kalzium-Ionen bauen will. Deshalb schützen Physiker ihre Qubits, etwa mit Vakuen, indem sie sie mit elektromagnetischen

Wie sehr der Quantencomputer die Welt verändert, wird davon abhängen, ob man trickreiche Algorithmen findet.

„Das wird bei vielen Aufgabenstellungen gelingen, bei vielen aber auch nicht."

Feldern in der Schwebe halten oder auf Temperaturen knapp über dem absoluten Nullpunkt abkühlen (siehe Bild). So gelingt es, den natürlichen Prozess der Dekohärenz zumindest hinauszuzögern. „Unsere Qubits leben bis zu zwei Sekunden", sagt Schmidt-Kaler. Da die „Kohärenzzeit" die Zahl der möglichen Rechenschritte eingrenzt, versuchen die Forscher, sie weiter zu erhöhen. Dazu geben sie den Qubits eine Art Selbstheilungskraft. Sie fügen den rechnenden Qubits weitere hinzu, die prüfen, ob sich Dekohärenz einschleicht, und, wenn ja, dies melden, woraufhin ein Steuerungslaser den sich anbahnenden Fehler ausgleicht. Unklar ist bislang, wie viele solche Selbstheilungs-Qubits es braucht. „Ein Quantencomputer könnte inklusive Fehlerkorrektur Millionen von Qubits benötigen", meint Schmidt-Kaler. Ein vielseitiger, wirklich mächtiger Quantenrechner wird daher noch mindestens ein Jahrzehnt auf sich warten lassen, meinen die meisten Physiker.

„Doch auch dieser wird den klassischen Rechner nicht überflüssig machen", ist sich Robert Wille von der Universität Linz sicher. Zwar ließe sich die neue Maschine frei programmieren, vom Textverarbeitungsprogramm bis zum maschinellen Lernen. Doch der „Wunderrechner" würde nicht per se alles schneller erledigen als ein normaler Computer. Zwar geht der Quantenrechner alle Lösungswege simultan. Er filtert aber den richtigen nicht automatisch heraus. „Dafür braucht man Quantentricks", sagt Wille. Die Crux: Jede Anwendung verlangt ihren eigenen Kniff. Bislang gelang das nur mit wenigen Quantenalgorithmen. Zum Beispiel mit dem Algorithmus von Grover, benannt nach dem indisch-amerikanischen Informatiker Lov Grover. Dieser findet in ein paar Schritten einen gesuchten Eintrag in einer ungeordneten Datensammlung. Die möglichen Lösungen kann man sich als eine Zahl vorstellen. Bei vier Einträgen in der Datenbank jeweils ein Viertel. Der Trick beim Grover-Algorithmus ist, dem gesuchten Eintrag zunächst ein negatives Vorzeichen zu verpassen, also minus ein Viertel. Und zweitens alle vier Zahlen an ihrem Mittelwert, also ein Achtel, zu spiegeln. Bei den drei positiven Werten kommt dabei null heraus. Bei dem negativen hingegen eins. Somit wurden alle falschen Lösungswege neutralisiert, nur der richtige bleibt übrig. Willes Team simuliert Algorithmen, die für künftige Quantencomputer geschrieben werden, auf klassischen Rechnern. Mit den Methoden der Linzer Forscher ist es möglich, Quantenalgorithmen schon heute zu testen, was bei der Suche nach solchen Quantentricks hilft. Im März letzten Jahres hat Willes Team dafür den mit 50.000 Euro dotierten Google-Award gewonnen.

Wie sehr der Quantencomputer die Welt verändert, wird davon abhängen, ob man trickreiche Algorithmen findet. „Das wird bei vielen Aufgabenstellungen gelingen, bei vielen aber auch nicht", schätzt Wille. Forscher glauben, dass es bei wichtigen Problemen im Bereich Big Data glücken kann, bei denen klassische Computer schnell an Grenzen stoßen. Dazu gehören Mustererkennung oder Optimierung, also das schnelle Finden der bestmöglichen Lösung unter gegebenen Bedingungen. Algorithmen in der künstlichen Intelligenz könnten rascher lernen. „Auch die Simulation des Klimas könnte schneller gehen", meint Robert Wille. Als erste Anwendung erwarten Experten indessen die Simulation von chemischen Verbindungen oder Festkörpern auf atomarer Ebene. Das würde viele Prozesse in der Chemie- oder Pharmaindustrie sowie in der Materialentwicklung beschleunigen. Als Heiliger Gral gilt Physikern ein Supraleiter, der Strom nicht nur bei sehr tiefen Minusgraden verlustfrei leitet, sondern auch bei Raumtemperatur. Denn die Supraleitung ist ein Quantenphänomen, das sich mit einem Quantenrechner leichter verstehen ließe, so die Hoffnung. Es gibt aber auch Beispiele, wo der Quantencomputer definitiv nicht schneller sein wird, was zeigt, dass er nicht jeder Form von Komplexität Herr werden, sprich: keine Wunder vollbringen wird.

Viele Experten glauben, dass es auf eine Art Hybrid-Computer hinauslaufen wird. Künftige Rechner enthalten demnach eine „Quantum Processing Unit", kurz: QPU, ähnlich wie heutige Computer Spezialchips haben, zum Beispiel eine Grafikkarte, um Spiele mit komplexer, rechenintensiver Computergrafik auf den Bildschirm zu bringen. Die QPU würde mit klassischen Chips zusammenarbeiten. Sie würde jene Aufgabenteile übernehmen, mit denen sich der herkömmliche Chip schwertut. Im Tabletcomputer sehen die meisten Experten die QPU indessen nicht. „Eher als Cloudservice", meint Wille. Das könnte den Clouddiensten ähneln, mit denen IBM oder Alibaba heute schon ihre prototypischen Quantenrechner der internationalen Forschergemeinde zur Verfügung stellen.

Bevor solche Visionen wahr werden, muss indessen etwas Entscheidendes passieren. Bislang forschen Physiker oft recht isoliert in ihren Laboren. Um den „Wunderrechner" in die Anwendung zu bringen, müssen sie nicht nur ihre Kräfte bündeln, sondern auch Ingenieure, Informatiker und andere Spezialisten einbinden. Das Vorhaben wird oft mit dem Kernforschungszentrum CERN bei Genf verglichen, wo Hunderte von Institutionen an einem Teilchendetektor basteln. Das Flaggschiff-Projekt der EU will das Schlagen solcher Brücken nun fördern.

Der Weg zum „Wunderrechner" ist also noch weit. Am Ende könnte etwas stehen, das diese Bezeichnung halbwegs verdient. Es wäre allerdings kein reiner Quantencomputer. ■

CHRISTIAN J. MEIER
50, ist freier Journalist und Autor aus der Nähe von Frankfurt. Der Physiker schreibt Artikel für Zeitungen oder Magazine, z.B. „NZZ" oder „bild der wissenschaft", und populärwissenschaftliche Sachbücher. Zum Thema hat er das Buch „Eine kurze Geschichte des Quantencomputers" verfasst.