



Licht und Schatten. Mit dem Prototyp eines Quantencomputers im Labor konnten chinesische Forschende die Überlegenheit gegenüber herkömmlichen Computern aufzeigen.

Sensibel in der Babyphase

Mythenumrankt, leistungsstark und empfindlich: Jens Eisert erklärt, wie Quantencomputer funktionieren und wie weit fortgeschritten ihre Entwicklung ist

VON ROLAND WENGENMAYR

Quantencomputer sind heute fast schon ein moderner Mythos. Im Internet finden sich wahre Wunder, zu denen diese Maschinen eines Tages fähig sein sollen. Und tatsächlich investieren große Unternehmen wie Google und Staaten wie China und die USA gewaltige Summen in die Entwicklung der Quanteninformationstechnologien. Auch Deutschland ist dabei, die Bundesregierung fördert diese Technologien mit zwei Milliarden Euro, und Bayern steckt 300 Millionen Euro in das Munich Quantum Valley. Doch was werden Quantencomputer wirklich können, wenn die Technologie ausgereift ist? Und was nicht? Was ist Hype und was realistisch? Mit solchen Fragen beschäftigt sich Jens Eisert, der am Dahlem Center for Complex Quantum Systems der Freien Universität Berlin forscht und international bestens vernetzt ist.

„Noch sind Quantencomputer in der Babyphase“, betont der Physikprofessor. „Grundsätzlich sind sie erst einmal Computer, sie können also Aufgaben wie herkömmliche Rechner lösen“, sagt er. „Allerdings funktionieren sie radikal anders!“ Herkömmliche Rechner zerlegen die Aufgaben, mit denen sie gefüttert werden, in Ja-Nein-Entscheidungen als logische Grundvokabeln, also die berühmten Einsen und Nullen der Bits. Die Qubits der Quantencomputer, kurz Qubits, kennen ebenfalls zwei Zustände, die man Eins und Null nennen kann. Doch nun kommen die Gesetze der Quantenmechanik ins Spiel. „Das ist immerhin die Theorie, die die Natur am genaues-

ten beschreibt, aber auf der Skala der Atome, Lichtquanten, eben der elementaren physikalischen Teilchen“, sagt Eisert. Da wir jedoch in einer Welt der großen Dinge leben, sind unser Verstand und unsere Wahrnehmung nicht auf die Eigenheiten der Quantenwelt trainiert. Deshalb kommen uns gerade jene besonders sensiblen Quanteneffekte, die den allgegenwärtigen Störungen der Makrowelt zum Opfer fallen, äußerst fremd vor. Besonders merkwürdig erscheint das Phänomen der Verschränkung: Quantenteilchen können im Prinzip über beliebige Entfernungen eine Einheit im Hinblick auf eine Quanteneigenschaft bilden, und sobald eines der Teilchen verändert wird, „merkt“ dies der entfernte Partner sofort.



Physikprofessor. Jens Eisert forscht am Dahlem Center for Complex Quantum Systems.

Genau solche Eigenschaften der Quantenwelt nutzen Quantencomputer. Das beginnt damit, dass die beiden Quantenzustände Null und Eins eines Qubits überlagert werden können, was ihren Quanteninformationsgehalt enorm steigert. Zudem können die Zustände mehrerer Qubits überlagert und miteinander ver-

schränkt werden. Schon mit wenigen Qubits ergibt dies theoretisch eine ungeheure Rechenmacht. Deshalb werden Quantencomputer im Prinzip bestimmte Typen von Aufgaben lösen können, an denen selbst heutige Supercomputer scheitern müssen. Es sind Aufgaben, die die Rechenzeit und den Speicherbedarf bei klassischen Computern exponentiell explodieren lassen würden, sozusagen die Pandemie im Reich der Rechenaufgaben. Unter diesem Typus von Problemen finden sich einige, die technisch hochinteressant sind und die Quantencomputer elegant mit wenigen Qubits in praktikabler Zeit lösen könnten – so die Hoffnung. „Für bestimmte paradigmatische Probleme ist dies tatsächlich bereits gezeigt“, betont Jens Eisert.

Um das zu illustrieren, bringt er ein konkretes Beispiel: das Multiplizieren von Zahlen. „Das ist einfach, $3 \times 5 = 15$ kann auch meine siebenjährige Tochter ausrechnen“, sagt er. „Selbst wenn die Zahlen groß werden, kann ich das mit der Technik, die ich in der Schule lerne, auf dem Papier lösen.“ Will man aber umgekehrt bei einer Zahl herausfinden, wie diese als Produkt aus miteinander multiplizierten Primzahlen zusammengesetzt ist, wird es überraschend kompliziert. Dieses „Primzahl-Faktorisieren“ überfordert bei größeren Zahlen sehr schnell auch einen Supercomputer. Genau das wird bei heute gängigen Verschlüsselungen ausgenutzt. Sie sind sicher, weil selbst die besten Computer einen solchen Schlüssel nicht innerhalb einer Zeit knacken können, die für die Geheimhaltung entscheidend ist.

Quantencomputer allerdings würden genau das mit einer überschaubaren Anzahl von Qubits schaffen, eben wegen ih-

rer exponentiellen Rechenmacht. Das hat der US-amerikanische Informatiker Peter Shor bereits 1994 theoretisch bewiesen: Sein Shor-Algorithmus ist einer der ersten Quantenalgorithmen, deren Überlegenheit über die klassische Computerwelt gesichert ist. Im Grunde funktioniert das Programmieren von Quantenrechnern ziemlich analog zu klassischen Computern. „Man bricht auch hier komplexere Funktionen in elementare herunter“, erklärt Physiker Eisert. „Bei herkömmlichen Computern sind das logische Entscheidungen, Gatter genannt, analog gibt es Quantengatter bei Quantencomputern“.

Das eigentliche „Rechenwerk“ funktioniert bei Quantencomputern aber radikal anders. Anstatt die Rechenschritte Schritt für Schritt hintereinander abzuwickeln, geschieht im Ensemble der überlagerten Qubits alles zugleich, sobald die Quantengatter programmiert sind. Diese Eigenschaft wird auch Quantenparallelität genannt. Vor allem müssen die miteinander verschränkten Qubits während ihres Werkens perfekt isoliert sein und in Ruhe gelassen werden. Auf keinen Fall darf man zu früh „nachschaun“, denn das würde den Rechenprozess sofort stoppen. Ein bisschen kann man sich das wie Kochen mit einem Schnellkochtopf vorstellen, in den man die Zutaten hineingibt und ihn erst wieder öffnet, wenn der Eintopf – hoffentlich – fertig gegart ist.

Allerdings verfügt ein Schnellkochtopf über einen Druckanzeiger, der über den Garprozess informiert, und das wäre bei einem Quantencomputer schon verboten. Denn eine Messung hat in der Quantenwelt als Eingriff die unangenehme Eigenschaft, das gemessene Objekt zu verändern. „Das wäre so, als würde man die

Länge eines Tisches messen, und durch die Messung würde er länger oder kürzer werden“, sagt Jens Eisert. In unserer makroskopischen Welt machen wir keine vergleichbar absurd erscheinenden Erfahrungen, weil eben die Umwelt mit ihren vielfältigen Störungen solcherlei Quanteneffekte ausschaltet.

Diese extreme Empfindlichkeit gegen kleinste Störungen ist die Achillesferse der Quantencomputer. Die Physik hat zwar faszinierende Techniken hervorgebracht, mit der sich zum Beispiel einzelne

Große Anfälligkeit gegen kleinste Störungen

Atome mit Laserstrahlen einfangen und als Qubits manipulieren lassen. Elektrisch geladene Atome, sogenannte Ionen, lassen sich wochenlang isoliert in elektromagnetischen Fallen gefangen halten. Das erlaubt bereits einfache, grundlegende Quantenrechenoperationen. Auch mit winzigen supraleitenden Schaltkreisen als Qubits funktioniert das ansatzweise; darauf setzen zum Beispiel die Unternehmen Google und IBM. Doch bislang gelang es nicht, die Qubits so gut von ihrer störenden Umwelt zu isolieren, dass größere Quantencomputer mit Hunderten, Tausenden, Zehntausenden von Qubits realisierbar sind. Solche „fehlerfrei“ arbeitenden Quantencomputer sind noch Zukunftsmusik – ob und wann sie zur Verfügung stehen werden, weiß niemand voraussagen.

Immerhin, betont Jens Eisert, stünden schon die kleinen, „schmutzigen“ Quantencomputer zur Verfügung. Mit „schmutzig“

meint er Störungen, die in Form von Rauschen die Lebenszeit der Quanteninformation begrenzen und eine Quantenrechnung mit der Zeit immer stärker durch Fehler „verschmutzen“. „Diese kleinen schmutzigen Quantencomputer sind aber sehr wertvoll“, betont der Physiker, denn damit lässt sich ausloten, was bereits funktionieren könnte. An speziell angepassten Quantenalgorithmen als „Software“ arbeitet die Forschung derzeit intensiv. Für die Hardware verfolgen Forscher wie Eisert die Idee, Aufgaben aufzuteilen in einen Teil, den ein herkömmlicher Computer bearbeiten kann, und einen Teil, der Quantencomputer erfordert. Das führt zu „hybriden“ Rechnerarchitekturen, erklärt der Wissenschaftler: „Wir setzen dabei unseren kleinen Quantencomputer in einen großen klassischen Computer als Umgebung hinein.“

Bei den möglichen Anwendungen kommt der Forscher auf die Deutsche Bahn. Die hat zuweilen Probleme mit der Einhaltung ihrer Fahrpläne und möchte das auch mithilfe neuer Informationstechnologien verbessern. „Die Fahrplannerstellung ist ein hochkomplexes Optimierungsproblem“, sagt Jens Eisert. Das bekannteste ist das eng verwandte Problem des Handlungsreisenden: Der Reisende will eine Reihe von Städten besuchen, die über die Landkarte verteilt sind, und dafür den kürzesten Weg ermitteln. Mit wachsender Zahl der Städte gerät er schnell an die Grenzen der Berechenbarkeit des Problems. Auch hier könnten Quantencomputer helfen, und dafür steht Jens Eiserts Team in Kontakt mit der Deutschen Bahn.

„Es ist ein Krimi“, schildert der Physiker begeistert sein Forschungsfeld. Denn niemand kann vorhersehen, welche Ideen es noch hervorbringen wird.