



FOTO: ADOBE STOCK/BARTEK WRÓBLEWSKI

Cooler Computer: Das finnisch-deutsche Unternehmen IQM entwickelt Quantenrechner, die mit supraleitenden Schaltkreisen, sogenannten SQDS, rechnen. Diese werden mit einem solchen Kryostaten auf Temperaturen nahe dem absoluten Nullpunkt von minus 273,15 Grad Celsius gekühlt.

QUANTENRECHNER AUF DEM SPRUNG

TEXT: ROLAND WENGENMAYR

Sie sollen Probleme lösen, an denen heute sogar die besten Computer scheitern. Mit dieser Erwartung investieren Regierungen, aber auch private Geldgeber massiv in die Entwicklung von Quantencomputern. Was die Rechner in den kommenden Jahren tatsächlich leisten können, erforscht das Team von Ignacio Cirac, Direktor am Max-Planck-Institut für Quantenoptik in Garching. Demnach werden sich wohl nicht alle Hoffnungen so bald erfüllen.

Eigentlich sollte Ignacio Cirac Grund zu Enthusiasmus haben. Der Direktor am Max-Planck-Institut für Quantenoptik in Garching bei München ist ein Pionier der Entwicklung von Quantencomputern. Solche Rechner sollen mithilfe der Quantenphysik manche Aufgaben etwa in der Logistik oder bei der Entwicklung neuer Medikamente und Werkstoffe wesentlich schneller bewältigen als heutige Computer. In dieser Hoffnung überbieten sich staatliche Institutionen geradezu bei der Förderung der Quantentechnologie, vor allem des Quan-

tencomputers: Die deutsche Bundesregierung hat von 2021 bis 2025 zwei Milliarden Euro für das Gebiet zur Verfügung gestellt, die US-Regierung gibt ebenfalls für vier Jahre rund eine Milliarde Dollar, und die EU-Kommission hat in einem über zehn Jahre laufenden Flaggschiffprogramm etwa genauso viel ausgelobt. Doch China übertrifft alle anderen mit gleich zehn Milliarden Euro für ein Institut für Quanteninformationswissenschaft. Dazu kommt: Neben zahlreichen Start-ups beteiligen sich auch große Unternehmen wie Google und IBM am Rennen zu den ersten Quantenrechnern – und sie begleiten jeden Fortschritt mit einigem medialen Tamtam. Hunderte Millionen Euro investieren die Firmen und ihre Kapitalgeber in die Entwicklung von Quantencomputern.

Das Forschungsfeld von Ignacio Cirac boomt also augenscheinlich. Doch das führt bei dem Physiker nicht nur

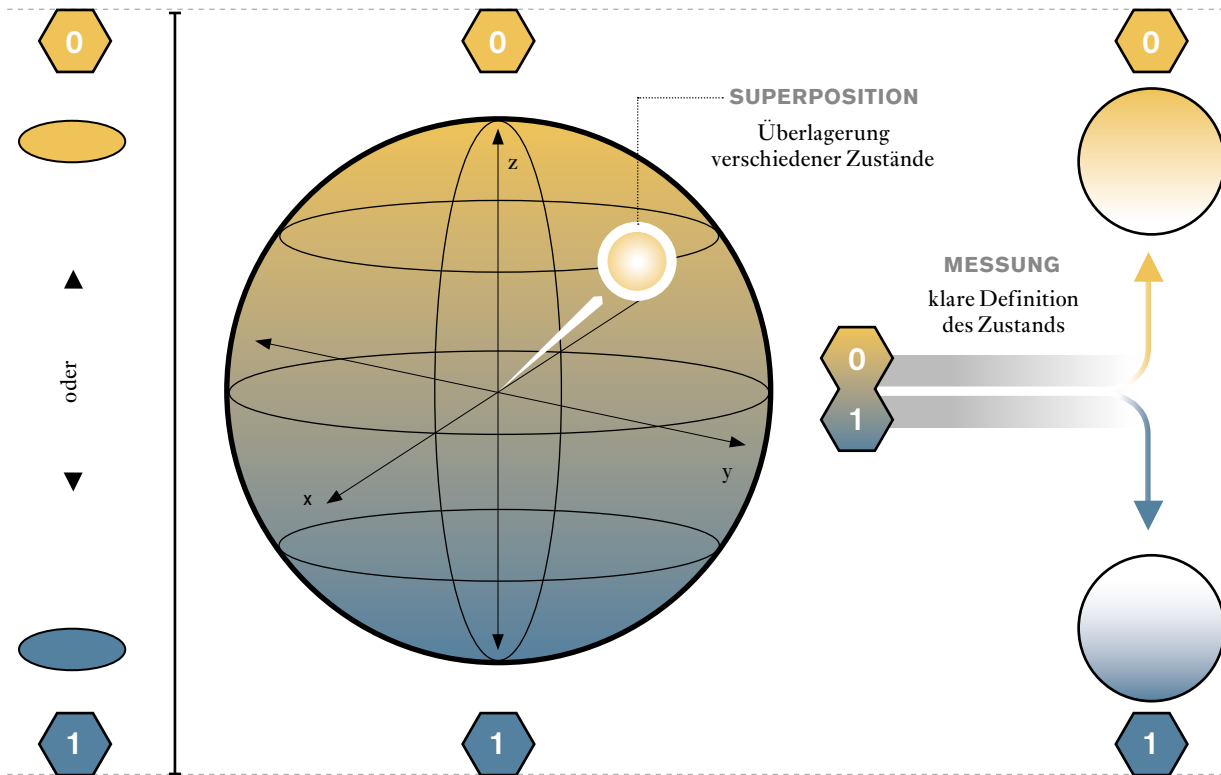
zu Begeisterung, sondern auch zu Beunruhigung. Wie viele seiner Kollegen, die sich auf dem Gebiet der Quanteninformation gut auskennen, fürchtet er, dieser Hype um Quanteninformationstechnologien könnte bei Misserfolgen bald ins Gegenteil umschlagen. „Wir werden jetzt nicht mehr nur durch die Forschung angetrieben, sondern auch durch Investoren“, sagt Cirac. Die aber könnten zu ungeduldig sein. Angesichts der enormen technischen Herausforderungen erwartet Cirac nämlich, dass es mindestens noch zehn Jahre, vielleicht sogar zwanzig bis dreißig Jahre dauern könnte, bis es wirklich anwendungsreife universelle Quantencomputer geben wird. „So lange wird aber kein Hype andauern“, betont er, „und am Ende werden wir Wissenschaftler als die Schuldigen ausgemacht, wenn der Quantencomputer noch nicht so weit ist.“ Die große Zukunftsvision sind universelle, das heißt frei programmierbare Quantencomputer. Sie sind

73

→

KLASSISCHES BIT
binäres System

QUANTENBIT (QUBIT)
willkürlich manipulierbares Quantensystem



74

GRAFIK: GCO NACH VOLKSWAGEN AKTIENGESELLSCHAFT 2019

Vieldeutiges Bit: Anders als ein klassisches Bit kann ein Quantenbit auch Überlagerungen der Zustände 0 und 1 annehmen, die sich mit den Koordinaten x, y und z auf einer Kugel darstellen lassen und bei einer Messung mit einer gewissen Wahrscheinlichkeit auftreten. Da Quantencomputer so verschiedene Lösungen parallel testen können, dürften sie manche Aufgaben schneller bewältigen als klassische Rechner.

das Gegenstück zu den digitalen Computern: Analog zu den digitalen Bits rechnen sie mit Quantenbits, kurz Qubits. Ihre Rechenmacht, wenn es um bestimmte Aufgaben geht, beziehen sie aus den Regeln der Quantenwelt: Anders als ein digitales Bit kann ein Qubit nicht allein die Zustände 0 und 1 annehmen, sondern sich auch in einer Überlagerung beider Zustände befinden. Darüber hinaus können mehrere Qubits miteinander überlagert werden. Diese Verschränkung bildet das Rechenwerk eines Quantencomputers.

Ein universeller Quantencomputer könnte vielfältige Anwendungen finden. „Ein typisches Beispiel ist das Problem des Handlungsreisenden“, sagt Cirac. Der Handlungsreisende soll eine gewisse Anzahl von Städten besuchen und will dafür die kürzeste Strecke errechnen. „Wie wächst nun mit der Anzahl der Städte die dafür auf einem digitalen Computer benötigte Rechenzeit?“, fragt der Physiker und antwortet gleich selbst: „Sie wächst exponentiell!“ Das sei typisch für derartige kombinatorische Probleme, und die lauern vielfältig dar-

auf, zum Beispiel in der Technik, Rechenzeiten auf herkömmlichen Computern explodieren zu lassen. Und nicht nur das: Auch der für das Rechnen benötigte Speicherplatz kann lawinenartig anwachsen.

Die Sache mit der exponentiellen Explosion kennen wir alle seit Beginn der Coronapandemie. Die Legende von der Erfindung des Schachspiels kann sie veranschaulichen. Der von dem neuen Spiel begeisterte König will dem Erfinder eine Belohnung zukommen lassen, die dieser sich aus-

suchen darf. Der im Gegensatz zum König mathematisch versierte Erfinder überlegt und wünscht sich dann Reis, nach folgender Regel: für das erste Feld des Schachbretts ein Reiskorn, für das zweite zwei Körner und dann für jedes nächste Feld immer die doppelte Anzahl. Mathematisch ergibt dies bei 64 Spielfeldern die Zahl $2^{64} - 1$, die in dieser Form als Potenz harmlos aussieht, aber gigantisch groß ist. Der König müsste dem Erfinder des Schachspiels so viel Reis geben, dass die Menge umgerechnet jener von rund zweitausend heutigen Weltjahresproduktionen entspräche.

Eine solche exponentielle Explosion erschwert auch die Lösung von Aufgaben aus der Physik und Chemie, die Quantencomputer schon recht bald bearbeiten könnten. Zum Beispiel wenn es darum geht, gezielt neue medizinische Wirkstoffe oder neue Werkstoffe zu entwickeln – etwa praxistaugliche Materialien, die Strom ohne Widerstand leiten. Denn wer die Eigenschaften von chemischen Reaktionen, von Molekülen und Materialien möglichst exakt berechnen will, muss unweigerlich Quanteneigenschaften berücksichtigen, genauer gesagt: das komplexe Zusammenspiel von Elektronen. Das Verhalten eines solchen Quantenvielteilchensystems kann selbst ein heutiger Supercomputer nicht berechnen. Daher hantieren Programme etwa für die Materialentwicklung mit stark vereinfachten Näherungsmodellen. Entsprechend unterentwickelt ist deren Vorhersagekraft. Quantencomputer können im Prinzip ein viel präziseres Materialdesign ermöglichen. Die Grundidee geht auf den amerikanischen Physik-Nobelpreisträger Richard Feynman zurück. Sie lautet: Will man ein Quantensystem exakt berechnen, so nehme man ein angepasstes zweites Quantensystem, welches sich als adäquates Ersatzteam eignet. Doch anders als das schwer zugängliche Untersuchungsobjekt, etwa das Elektronenkollektiv in einem Supraleiter, muss dieses zweite Quantensystem wie ein Rechenwerk gut von außen

steuerbar sein. Genau dadurch zeichnet sich ein Quantencomputer aus, und zwar in der Rolle eines Quantensimulators.

Simulatoren für die physikalische Forschung

Vergleicht man das mit der Geschichte der klassischen Computer, dann sind Quantensimulatoren das Pendant zu Analogrechnern. Das waren hochspezialisierte Computer, die zum Beispiel die aerodynamischen Eigenschaften eines zu entwickelnden Flugzeugs simulierten. Anders als digitale Computer, welche Information portionsweise als Bits verarbeiten, bildeten Analogcomputer ein bestimmtes System kontinuierlich nach, etwa mechanisch oder elektronisch. Analogcomputer hatten ihre große Zeit, als digitale Computer noch nicht so leistungsfähig waren. Heute, in der Frühphase der Quantencomputer, ist es ähnlich. Quantensimulatoren werden bereits zunehmend interessant, um zumindest Fragen der physikalischen Grundlagenforschung anzupacken. Daran forscht zum Beispiel die Gruppe von Immanuel Bloch, ebenfalls Direktor am Max-Planck-Institut für Quantenoptik, mit der Ciracs Team auch zusammenarbeitet.

Von dem universell programmierbaren Quantencomputer trennt einen Quantensimulator, der heute oder zumindest in naher Zukunft verfügbar ist, etwa so viel wie einen alten Analogrechner vom heutigen PC. Ciracs Team verfolgt daher eine doppelte Strategie. Ein Teil der von den Garcingern entwickelten Algorithmen wird erst in fernerer Zukunft auf leistungsfähigen, fehlerkorrigierten universellen Quantencomputern laufen können. Der andere Teil soll schon möglichst bald auf den bereits verfügbaren Quantenrechnern mit relativ wenigen Qubits einsetzbar sein und besonders in der Quantensimulation erste Vorteile demonstrieren. „Wir wollen zeigen, dass man schon jetzt

auf Quantencomputern etwas Nützlich machen kann, das auf klassischen Computern nicht mehr geht“, sagt Cirac, „zum Beispiel die Eigenschaften von einigen neuen Materialien vorherzusagen.“ Dazu kooperiert er auch mit Google Research, der Forschungsabteilung von Google.

Für die Hardware von Quantencomputern sind verschiedene physikalische Systeme im Wettrennen. Immanuel Blochs Gruppe etwa setzt auf ultrakalte Atome als Qubits, die in einem räumlichen Gitter aus Laserstrahlen gefangen sind und über Laserlicht angesteuert werden. Google hingegen entwickelt Chips, die winzige supraleitende Schaltkreise als Quantenbits nutzen. Mit einem solchen Quantenprozessor namens Sycamore, der 53 funktionierende Qubits enthielt, konnte die Google-Forschung 2019 erstmals demonstrieren, dass ein Quantencomputer in der Berechnung einer Aufgabe den leistungsfähigsten konventionellen Supercomputer schlagen kann. „Allerdings war das eine rein akademische Aufgabe ohne sinnvolle Anwendung“, kommentiert Cirac diesen gefeierten Durchbruch. Und Markus Hoffmann von Google Research in München vergleicht es mit dem ersten Motorflug-Hüpfer der Gebrüder Wright: „Mit diesem Flug sind wir auf einer ersten Insel gelandet, die klassisch nicht erreichbar ist – aber diese ist noch unfruchtbar.“ Er betont auch, dass Google Research das technische Entwicklungsniveau von Quantencomputern realistisch einschätzt. Zugleich gibt er sich optimistisch. So erwartet Google, dass die nächsten Meilensteine hundert supraleitende Qubits sind, danach tausend und schließlich – etwa in einer Dekade – eine Million.

75

Die Grenzen von Quantencomputern

Schon mit hundert Qubits ließe sich in der Materialentwicklung etwas anfangen. Will man nämlich die Eigen-



schaften eines mikroskopisch kleinen Supraleiterstückchens exakt berechnen, die von hundert stark miteinander wechselwirkenden Elektronen bestimmt werden, landet man bei einem Problem mit 2^{100} Unbekannten. Das ist weit mehr, als das Universum Sterne hat, und überfordert absehbar alle herkömmlichen Großcomputer. Ein Quantencomputer würde hingegen nur hundert verschränkte Qubits benötigen, um die Aufgabe zu lösen. Aber wie macht er das?

Mari Carmen Bañuls, leitende Forscherin in Ciracs Abteilung, versucht, die Prozedur zu erklären: „Man schreibt seine Instruktionen in die Quantenbits hinein und präpariert sie so in einem bestimmten Quantenzustand.“ Die zu berechnende Aufgabe, die einen bestimmten Quantenalgorithmus nutzt, steckt dabei in der Art, wie die Quantenbits anfänglich verschränkt sind. „Dann lässt man das System sich eine gewisse Zeit entwickeln“, erklärt die Physikerin, „und macht dann eine Messung, um das Ergebnis zu bekommen.“ Das ist in gewisser Weise mit dem Kochen in einem Schnellkochtopf vergleichbar: Man gibt die Zutaten hinein, verschließt den Topf und startet den Kochvorgang. Nach einer vom Rezept festgelegten Zeit schaut man nach, ob der Eintopf gelungen ist. Während des Kochens hat man nur den Druckanzeiger als Information über die Vorgänge im Topf – aber immerhin.

In der Quantenwelt ist nicht einmal eine solche Anzeige erlaubt, solange die verschränkten Qubits vor sich hin werkeln. Denn hier kommt eine weitere Eigenheit ins Spiel: Quanteninformation ist ein extremes Sensibelchen. Selbst ein minimaler Eingriff entspricht einer Messung, welche die Verschränkung sofort kollabieren lässt. Also darf man erst nach Ablauf der im Quantenrezept festgelegten Zeit nachschauen, sprich: eine Messung machen, und bekommt dann das erwünschte Resultat – vielleicht. Denn es gibt noch eine Besonderheit der Quantenmechanik. Sie beschreibt nur Wahrscheinlichkeiten, mit denen

sich bestimmte Quantenzustände einstellen. Ein Quantencomputer würde also nicht $1 + 1 = 2$ liefern, sondern das Resultat 2 nur mit einer gewissen, allerdings exakt berechenbaren Wahrscheinlichkeit ausgeben. Auch das ist ein Hinweis darauf, dass der Einsatz von Quantencomputern nur für spezielle Aufgaben sinnvoll sein wird, für die solch eine Unsicherheit tolerabel ist oder es keine Alternative

AUF DEN PUNKT GEBRACHT

Regierungen und Unternehmen investieren derzeit massiv in die Entwicklung eines Quantencomputers, der manche Aufgaben viel schneller lösen könnte als die besten heute verfügbaren Rechner.

Es wird vielleicht noch Jahrzehnte dauern, bis es einen universell programmierbaren Quantencomputer gibt, vor allem weil Rechnungen mit ihm sehr fehleranfällig sind und Quanteninformation sehr empfindlich ist. Forschende unter anderem des Max-Planck-Instituts für Quantenoptik arbeiten deshalb an der Fehlerkorrektur und der Validierung von Quantenrechnungen.

Quantensimulatoren lassen sich heute bereits für Untersuchungen in der physikalischen Grundlagenforschung nutzen. In naher Zukunft könnten sie auch die Entwicklung neuer Werkstoffe und Medikamente erleichtern.

gibt. Welche Aufgaben das sein könnten, das erforscht Ciracs Team ebenfalls. Denn hier ist trotz kühner Zukunftsvisionen noch sehr vieles offen: „Wir untersuchen auch, was Quantencomputer *nicht* können“, betont Cirac. Dies soll verhindern, dass wertvolle Ressourcen auf nicht erreichbare Ziele verschwendet werden.

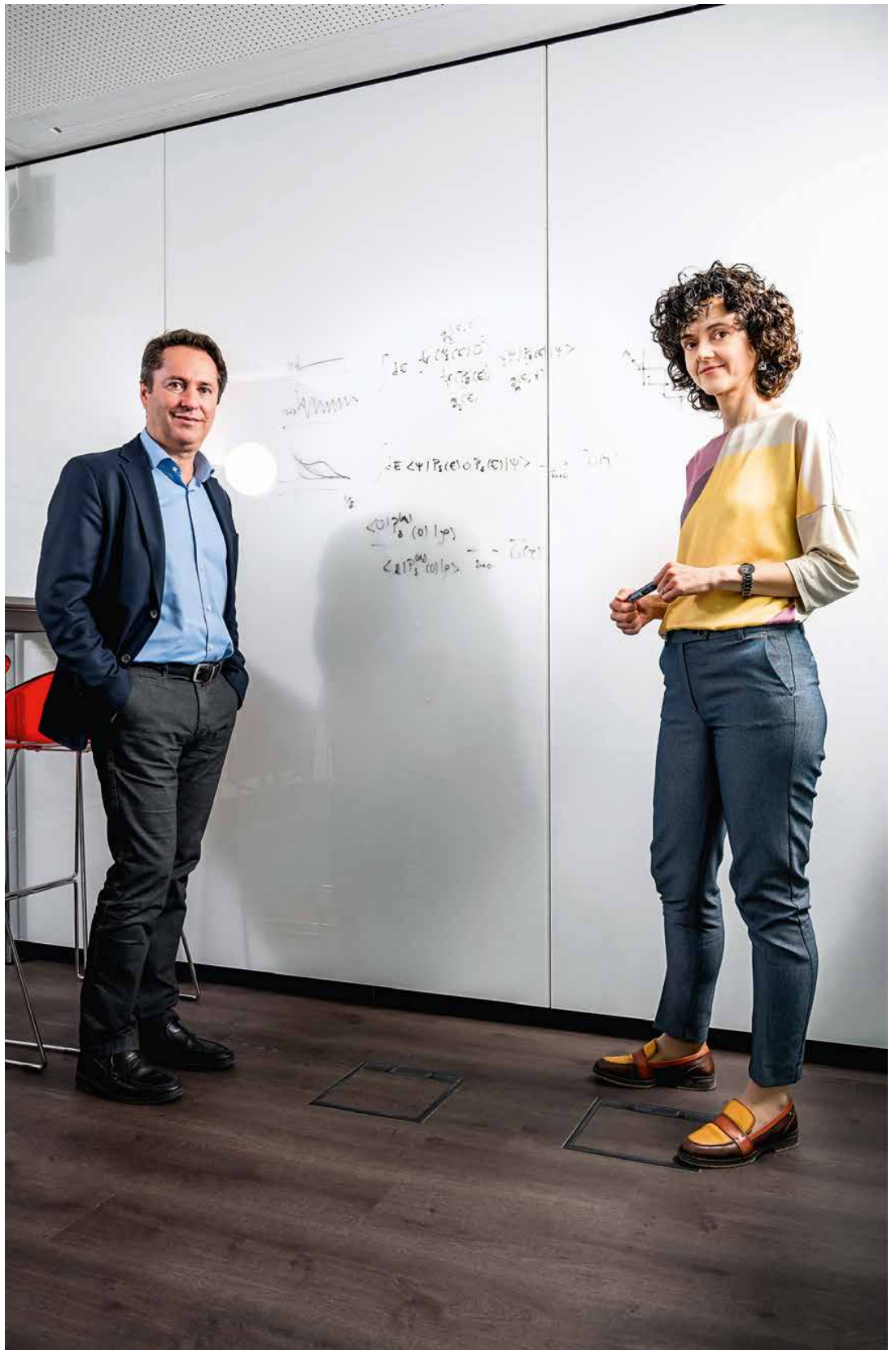
Auch ein universell programmierbarer Quantencomputer kann also nicht beliebige Probleme lösen. Und um die Hoffnungen überhaupt zu erfüllen, die auf ihn gesetzt werden, reichen selbst die von Google in rund zehn Jahren angepeilten eine Million Qubits nicht. Das liegt nicht zuletzt am Unterschied zwischen physikalischen und logischen Qubits, wie Google-Forscher Markus Hoffmann erklärt. Ein physikalisches Quantenbit ist eben zum Beispiel ein in einem Lichtgitter schwebendes Atom oder ein mikroskopischer supraleitender Kreisstrom. Doch weil diese physikalischen Bits so anfällig gegenüber Störungen aus der Umwelt sind, gibt es den Plan, mehrere physikalische Qubits zu einem logischen Qubit zusammenzuschalten, um darin die Quanteninformation wesentlich stabiler zu speichern. Bei der supraleitenden Technik, wie Google sie erforscht, würde ein logisches Qubit aus tausend synchronisierten physikalischen Qubits bestehen.

Bei einem universellen Quantencomputer werden viele zwischen den und rund um die logischen Qubits verteilte Hilfsquantenbits hinzukommen. Sie sollen als zusätzliche Sensoren Störungen messen. All das ist der Herausforderung geschuldet, dass die eigentlich rechnenden logischen Qubits während ihrer Arbeit nicht auf Fehler geprüft werden dürfen, was ein herkömmlicher Computer täte. Eine Prüfung wäre ja eine verbotene Messung. Aber auf Basis der Informationen von den Hilfsqubits und der Ergebnisse der logischen Qubits kann der Algorithmus eine sinnvolle Fehlerkorrektur machen.

Solche Konzepte für einen universellen, fehlerkorrigierten Quantencomputer haben Schätzungen zufolge einen hohen Preis. „Das läuft auf vielleicht hundert Millionen physikalische Qubits hinaus“, sagt Cirac: „Ein solcher Quantencomputer würde mit seinen Vakuum- und Kühlvorrichtungen unser ganzes Institut füllen!“ Mit der heutigen Technik sind diese Anforderungen also „crazy“, wie

→

FOTO: BETHEL FATH FÜR MPG



Forschen mit kurz- und mit langfristiger Perspektive: Ignacio Cirac und Mari Carmen Bañuls untersuchen, wie Quantenrechner bereits mit relativ wenigen Qubits nützliche Erkenntnisse liefern können. Darüber hinaus entwickeln sie Algorithmen für universell programmierbare Systeme mit etwa einer Million Qubits.

Cirac betont, und genau deshalb macht ihm der gegenwärtige Hype Sorgen. Aus seiner Sicht sind auch noch grundlegende technische Herausforderungen nicht gemeistert.

Neue Ideen aus ersten Anwendungen

Erstaunlich gelassen ist hingegen Thomas Monz von der Universität Innsbruck. Er gehört zu einem Team um Rainer Blatt, das eine andere Technik vorantreibt. Die Forschenden nutzen elektrisch geladene Calciumatome, die – wie Perlen aufgereiht – in einer elektromagnetischen Falle, der sogenannten Paul-Falle, schweben. Angesteuert werden sie mit Laserstrahlen. Der Vorteil dieser Calciumionen besteht darin, dass sie wegen ihrer elektrischen Abstoßung sehr stark miteinander wechselwirken. Dies lässt sich

für eine sehr kräftige Verschränkung nutzen. Bereits 24 Qubits konnten in diesem Ionen-Quantencomputer verschränkt werden.

„Das klingt nach wenig, aber diese Verschränkung ist sehr stabil“, sagt Monz. Er ist auch Geschäftsführer des Startups Alpine Quantum Technologies (AQT), das bereits Ionen-Quantencomputer kommerziell verkauft. Seine Gruppe an der Universität Innsbruck, unterstützt durch AQT, hat in Zusammenarbeit mit dem Forschungszentrum Jülich kürzlich erstmals eine erfolgreiche Quantenfehlerkorrektur demonstriert. „Dazu haben wir je sieben physikalische Qubits zu logischen Qubits zusammengeschaltet“, sagt Monz. Die Idee ist einfach: Nach einer gewissen Rechenzeit weichen gewöhnlich Zustände einiger physikalischer Qubits, die ein logisches Qubit formen, wegen Fehlern voneinander ab; dann zeigt die Mehr-

GLOSSAR

QUANTENCOMPUTER
rechnen mit Quantenbits, die – anders als digitale Bits – auch Überlagerungen der Zustände 0 und 1 annehmen können. Überdies können die Zustände mehrere solcher Qubits miteinander verschränkt werden. Damit können sie verschiedene Lösungen einer Rechenaufgabe parallel bearbeiten und kommen bei manchen Problemen deutlich schneller zu Lösungen als herkömmliche Rechner.

QUANTENSIMULATOR
wird ein spezialisierter Quantencomputer genannt, der mit wesentlich weniger Qubits auskommt als ein frei programmierbarer Quantencomputer und spezielle Aufgaben, etwa in der Materialwissenschaft, lösen kann.

heit der Qubits, die im Zustand übereinstimmen, wahrscheinlich das korrekte Ergebnis an. „Bei der Quantenfehlerkorrektur geht es ja einfach um Redundanz“, sagt Monz.

Um mit der Fehleranfälligkeit von Quantenrechnungen besser umgehen zu können, haben Cirac und sein Team ein Projekt gestartet: „Wir arbeiten an der Verifikation von Rechenergebnissen“, sagt er: „Ich denke, das ist eine wichtige Fragestellung.“ Denn es soll sichergestellt sein, dass Quantencomputer verlässliche Ergebnisse produzieren. Solch ein Debugging muss auch die etablierte Computertechnik immer wieder vornehmen.

Trotz aller Einschränkungen, trotz der Hindernisse, die Quantencomputer noch nehmen müssen, ehe sie für breitere Anwendungen nutzbar sind, ist Cirac überzeugt: Gibt es sie erst einmal, werden sie zu unerwarteten Ideen führen. Der inspirierende Effekt der fortschreitenden Entwicklung motiviert ihn auch, schnell zu ersten, kleineren Anwendungen zu kommen. Er ist sicher: „Falls wir in fünfzehn Jahren wieder ein Interview führen, werden die wichtigsten Anwendungen der Quantenphysik nicht die sein, über die wir heute gesprochen haben!“

Modell eines Quantensystems:
Gekreuzte Laserstrahlen formen ein Gitter, das einem Eierkarton ähnelt. In dessen Kuhlen lassen sich Atome fangen, die Quantenphänomene simulieren können. Solche Systeme sind aber auch Kandidaten für universelle Quantencomputer.

