Mit Quanten muss man rechnen

Eine geführte Reise in die faszinierende Computerwelt von morgen

Von Rainer Blatt

Quantencomputer verheißen ungeahnte Rechenleistungen. Erste Prototypen werden mit Hochdruck weiterentwickelt.

Rainer Blatt ist Professor für Experimentalphysik an der Universität Innsbruck und seit 2003 wissenschaftlicher Direktor am Institut für Quantenoptik und Quanteninformation der Österreichischen Akademie der Wissenschaften.

Seit einigen Jahren hören wir von Quantencomputern[160], die – so die oft zitierte Vision – eine gigantische Steigerung der Rechenleistung gegenüber klassischen Computern in Aussicht stellen. Was aber sind denn nun Quantencomputer? Wie funktionieren sie und was können sie wirklich? Klassische Computer stoßen schnell an ihre Grenzen, wenn es um Quantenphänomene geht, bei denen viele Teilchen eine Rolle spielen, etwa im Fall von schweren Atomen, Molekülen oder kondensierter Materie. Das Quantenverhalten dieser Teilchen kann nur mit großem Speicheraufwand berechnet werden, was mit ihren Welleneigenschaften zu tun hat (s. Kasten „Quantenphysik“). Schon in den 1980er-Jahren wies der Nobelpreisträger Richard Feynman darauf hin, dass es doch sehr viel zielführender sei, dafür Computer zu verwenden, die mit Quanteneigenschaften rechnen und somit das Quantenverhalten automatisch berücksichtigen – ohne dies auf einem klassischen Rechner kompliziert zu programmieren.

In einem klassischen Rechner ist die Informationseinheit das Bit, das heißt, eine Schalterstellung, die entweder EIN (1) oder AUS (0) ist. Klassische Computer arbeiten als schnelle Schalter, die Informationen als Zahlenreihen von Nullen und Einsen darstellen. Das Pendant in der Quantenwelt ist das Quantenbit (Qubit), ein System mit zwei Zuständen, das auch in einer Überlagerung vorkommen kann – also in einem Zustand, der sowohl in 1 als auch in 0 sein kann. Information über den Zustand sowohl eines Bits als auch eines Quantenbits erhält man durch Messen, also durch Auslesen oder Beobachten der Informationseinheit. Dabei findet man stets eine Null oder eine Eins, und Überlagerungen zeigen

sich, wenn bei gleich präparierter Information mal eine Null, mal eine Eins gefunden wird. Erst die statistische Auswertung vieler Messungen (wievielmal Null, wievielmal Eins) zeigt, mit welchen Anteilen die beiden Zustände 0 und 1 dazu beitragen.

Gibt es mehrere Qubits, beispielsweise in einem Rechenregister, kann auch eine Überlagerung all ihrer Zustände vorliegen. Man spricht dann von einer „Verschränkung“, wenn man den gesamten Zustand des Registers nicht durch die separate Beschreibung der einzelnen Qubits charakterisieren kann. Dies spiegelt das nichtlokale Wellenverhalten der Quantenbeschreibung wieder. Umgekehrt lässt sich bereits durch eine kleine Änderung an auch nur einem Qubit der Zustand des gesamten Systems verändern – und damit die (Quanten-) Information, die im System gespeichert ist. Das ermöglicht einem Quantencomputer die Verarbeitung von Information in nur wenigen Schritten; mit herkömmlichen Computern würde dieser Prozess sehr viele und komplexe Rechenoperationen erfordern.

Quantenphysik

Die Entwicklung der Quantenphysik ist eine der bedeutendsten intellektuellen Leistungen des 20. Jahrhunderts. Sie beschreibt die Welt der kleinsten Teilchen, etwa der Atome, Elementarteilchen und Lichtquanten. Ihre Grundaussage, dass Materieteilchen auch Welleneigenschaften und Wellen gleichermaßen Teilcheneigenschaften besitzen, ist vielfach getestet und als richtig und vorhersagekräftig befunden worden. Die Quantenphysik ist die Grundlage für revolutionäre technische Entwicklungen, darunter Lasertechnologie und medizinische Bildgebung, Halbleitertechniken und Navigationstechniken mittels GPS.

1995 haben Peter Zoller und Ignacio Cirac von der Universität Innsbruck zum ersten Mal theoretisch gezeigt, wie man mit in einer Fallenanordnung eingefangenen Ionen einen universellen Quantencomputer technisch realisieren kann. In meiner experimentellen Arbeitsgruppe haben wir dann diesen Vorschlag umgesetzt und 2002 die ersten Quantengatter mit zwei Qubits nach dem Vorschlag der Kollegen demonstriert. Bereits 2005 gelang uns die Realisierung eines ersten Quantenbytes, also einer Anordnung von acht Ionen als Quantenregister. Die gespeicherten Ionen (Abb. 1) können mit Lasern einzeln angesteuert werden, um Quantenoperationen ähnlich wie Gatterschaltungen in klassischen Computern vorzunehmen. Durch die Kombination verschiedener Quantengatteroperationen sind universelle Quantenrechnungen möglich.

Ausgehend vom Cirac-Zoller-Vorschlag wurden viele verschiedene

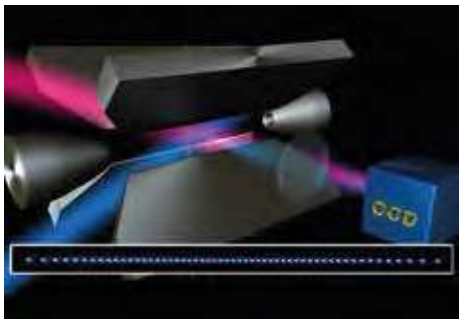

Abb. 1
Supraleitender-Quantencomputer: In einer Elektrodenanordnung halten elektrische Felder eine Kette von Ionen, die aufgrund ihrer Ladung voneinander Abstand wahren. Die unter einem Winkel applizierten Laserstrahlen dienen der Laserkühlung und der Fluoreszenzanregung. Das Bild einer CCD-Kamera zeigt die aufgenommene Fluoreszenz eines Quantenregisters von 54 Ca^+-Ionen, die hier als Qubits mit Laserstrahlen individuell angesteuert werden können.

© Rainer Blatt, Universität Innsbruck

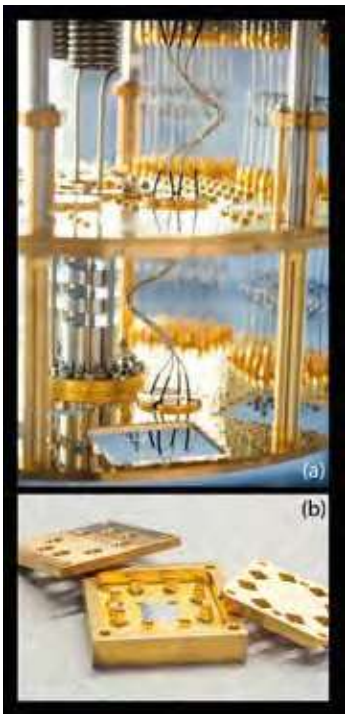

Abb. 2
Supraleitender Quantencomputer: Kryostataufbau (a) zur Kühlung und Ansteuerung der supraleitenden Schaltkreise, die auf einem Chip (b) integriert sind und einzelne Qubits enthalten.

© Kai Neunert, Bayerische Akademie der Wissenschaften und Technische Universität München.

Systeme vorgeschlagen, um Qubits zu realisieren. Als natürliche Systeme bieten sich dazu atomare Ionen oder Atome an, die man mit elektrischen oder Laserlicht-Feldern einfangen und einzeln fixieren kann. Dabei gilt es zu verhindern, dass die Atome sich zu sehr bewegen – man muss ihre Bewegung also ausfrieren, um ihre Quanteneigenschaften gezielt ausnützen zu können. Andere Konzepte setzen auf künstliche Atome bei tiefen Temperaturen, auf Fehlstellen in Diamantstrukturen oder auf durch Mikrostrukturierung erzeugte elektronische Schaltkreise, die Quanteneigenschaften aufweisen. Auch mit Photonen und komplexen Interferometern lassen sich so Quantenrechner darstellen[161]. Derzeit gibt es bereits eine Reihe von Quantencomputern, die mit einigen zehn Qubits arbeiten und rechnen können (s. Beispiele in Abb. 1–3).

In unseren Laboren haben wir den von uns entwickelten Quantencomputer auf der Basis von gespeicherten Ionen weiterentwickelt. Wir arbeiten heute routinemäßig mit 20 bis 50 Ionen als Qubits in einem Quantenregister für Quantenrechnungen in der Grundlagenforschung, für Quantensimulationen von Vielteilchensystemen und für Messtechniken, die mit Methoden der Quanteninformation verbessert werden – speziell für die Präzisionsspektroskopie.

Die potenzielle Leistungsfähigkeit solcher Quantencomputer lässt sich ermessen, wenn man versucht, ihre Funktionsweise komplett in einem klassischen Rechner nachzubilden. So erfordert die vollständige Darstellung von nur etwa 50 Qubits in einem klassischen Computer bereits mehr Speicher-Ressourcen als sie den besten Supercomputern zur Verfügung stehen. Im Prinzip sollte demnach ein Quantenrechner schon mit etwa 50 Qubits die Leistungsfähigkeit eines Supercomputers erreichen können. Das volle Potenzial auszuschöpfen setzt aber voraus, dass man die Quantenrechnungen beliebig lange fortsetzen kann und dass dabei keinerlei Fehler passieren.

Allerdings reagieren Quantensysteme, zumal wenn sie sich in Verschränkung befinden, sehr empfindlich auf äußere Störungen und Einflüsse. Daher werden die heutigen Quantenrechner auch als NISQ (Noisy Intermediate Scale Quantum)-Maschinen bezeichnet, die nur einige Hundert Rechenoperationen mit einigen zehn Qubits machen können, bevor die Rechenergebnisse unbrauchbar werden. Das genügt zwar, um viele Quantenprotokolle zu demonstrieren und Testprogramme zu entwickeln, reicht aber noch nicht aus, um mit klassischen Computern, insbesondere für kommerzielle Anwendungen, konkurrieren zu können.

Für eine zukünftige Nutzung von Quantencomputern ist es erforderlich, die bisherigen Ansätze zu skalieren. Wegen der inhärenten Empfindlichkeit der Quantenzustände muss man die Rechenoperationen fehlertolerant betreiben. Dazu ist zunächst eine Quantenfehlerkorrektur zu implementieren, für die man mehrere Qubits zu einem „logischen Qubit“

zusammenfasst, dessen Zustand sich beim Auftreten von Fehlern durch die damit vorhandene Redundanz wiederherstellen lässt.
In Innsbruck haben wir dazu bereits vor zehn Jahren zeigen können, dass man so durch Fehler oder Messprozesse gestörte Quanteninformation vollständig wiederherstellen kann. Schließlich gelang es uns, mit insgesamt sieben Ionen als physikalische Qubits ein logisches Qubit zu programmieren, darin auftretende Fehler zu erkennen und zu korrigieren. Zudem können wir damit bereits heute universelle Rechenoperationen auf einem logischen Qubit vornehmen. Darüber hinaus müssen alle Rechenoperationen in fehlertoleranter Weise kodiert werden, um zu verhindern, dass die Operationen Fehler propagieren, das heißt im Quantenregister ausbreiten.[162] Damit Quantencomputer vollständig fehlertolerant arbeiten, müssen daher auch mögliche Fehler im Verlauf der korrigierenden Quantenoperationen vermieden bzw. berichtigt werden. Das erfordert eine mehrlagige Kodierung und eine Mindestgüte der Quantengatteroperationen. Alle Schritte – wiederholte Fehlerkorrektur, fehlertolerante Codierung, Quantengatter zwischen logischen Qubits – sind bisher einzeln erfolgreich getestet und durchgeführt worden; die vollständige fehlertolerante Operation eines Quantencomputers ist Gegenstand der aktuellen Forschung.
Neben der Bereitstellung der Hardware ist die Weiterentwicklung der Software ein zentrales Thema, um Anwendungen zu ermöglichen, die die Vorteile eines Quantenrechners auch ausnützen können. Mögliche Anwendungen liegen im Bereich der Optimierung und überall dort, wo Quantenphänomene eine Rolle spielen, etwa bei Berechnungen in der Chemie oder für neue Materialien. Allerdings ist es noch ein weiter Weg zur praktischen Nutzung: Erste Abschätzungen zeigen, dass man für Quantenrechner, die komplexe Anwendungsprobleme bewältigen können, einige hunderttausend Qubits und Abermillionen von Rechenoperationen benötigen wird[163].
Die Fortschritte auf dem Gebiet der Quantentechnologien und der Quantencomputer in den vergangenen 25 Jahren sind enorm. Sie haben bereits großen Einfluss auf die Entwicklung von Quantensimulationen und neuen Quantenmethoden in der Metrologie sowie in der Kommunikation. Der weltweite Quantencomputer-Hype verleitet manche dazu, mehr zu versprechen als Wissenschaft und Technologie heute leisten können. Was man aber auch sagen muss: Derzeit ist kein physikalisches Gesetz bekannt, das eine Skalierung von Quantencomputern unmöglich machen würde und zweifellos wird es weitere Fortschritte geben. Für eine nachhaltige Entwicklung kompetitiver Quantencomputer wird es aber notwendig sein, Quantenphysik und Grundlagenforschung in der Quanteninformation weiter voranzutreiben. Vieles ist im Fluss, eines aber steht unstrittig fest: Mit Quanten muss man rechnen.

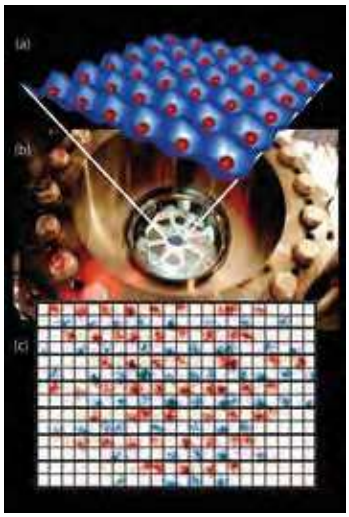

Abb. 3
Neutral-Atom-QC: Atome werden nach optischer Kühlung in einem optischen Gitterpotenzial eingefangen (a). Dieses wird erzeugt durch gekreuzte Laserstrahlen in einem optischen Resonator (b). Mithilfe eines Quantengasmikroskops kann das Fluoreszenzlicht der eingefangenen Atome beobachtet werden (c). Diese Atome lassen sich individuell adressieren und dienen als Qubits für einen atomaren Quantencomputer.

© Immanuel Bloch, Sebastian Blatt, Max-Planck-Institut für Quantenoptik, Garching.