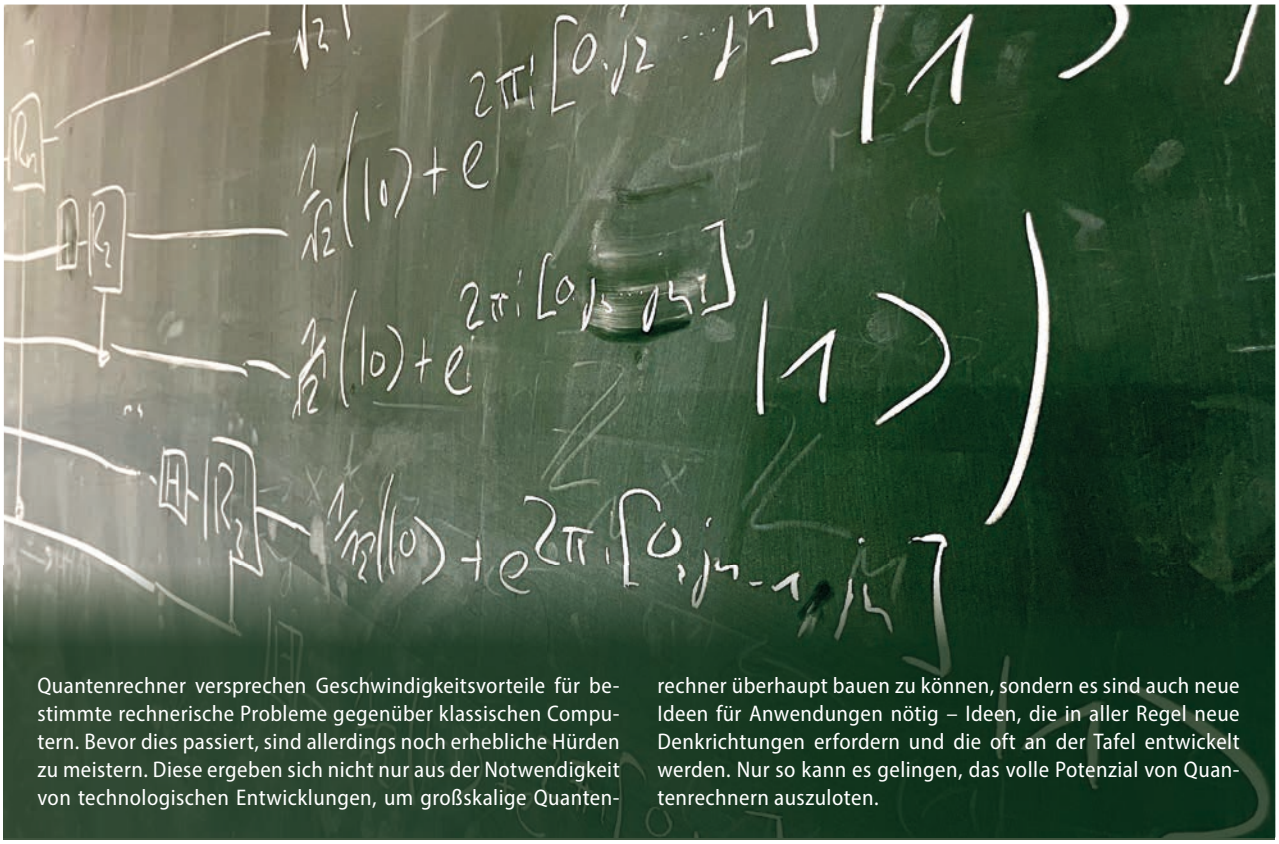

Quantenrechner versprechen Geschwindigkeitsvorteile für bestimmte rechnerische Probleme gegenüber klassischen Computern. Bevor dies passiert, sind allerdings noch erhebliche Hürden zu meistern. Diese ergeben sich nicht nur aus der Notwendigkeit von technologischen Entwicklungen, um großskalige Quantenrechner überhaupt bauen zu können, sondern es sind auch neue Ideen für Anwendungen nötig – Ideen, die in aller Regel neue Denkrichtungen erfordern und die oft an der Tafel entwickelt werden. Nur so kann es gelingen, das volle Potenzial von Quantenrechnern auszuloten.

QUANTENCOMPUTING

Eine kurze Geschichte des Quantenrechnens von gestern bis morgen

Die Anfänge des Quantencomputings reichen rund 30 Jahre zurück, aber um dessen volles Potenzial auszuschöpfen, sind noch etliche Forschungsanstrengungen notwendig.

Jens Eisert, Paul K. Fährmann und Matthias C. Caro

Durch den Mitte der 1990er-Jahre vorgestellten Shor-Algorithmus zur Primfaktorzerlegung erhielt das theoretische Feld des Quantenrechnens auch außerhalb der Wissenschaft Aufmerksamkeit. Dies führte zu einer kreativen Explosion des Forschungsfeldes. Etwa 30 Jahre später können erste Quantenchips simple Quantenalgorithmen ausführen. Um hierfür praktische Anwendungen zu finden, bedarf es weiterhin gründlicher Forschung. In diesem Artikel zeichnen wir die Entwicklungen dieses spannenden Feldes nach und zeigen vielversprechende Forschungsrichtungen auf.

Alan Turing schrieb Weltgeschichte als der erste Forscher, dem es gelang, mit „Turochamp“ ein Computerprogramm für Schach zu schreiben und gleichzeitig die Grundlagen der künstlichen Intelligenz zu schaffen. Sein Team war es auch, das die Enigma-Verschlüsselungsmaschine der Nationalsozialisten im zweiten Weltkrieg knackte, mit den bekannten, erheblichen Konsequenzen. Für die Informatik war Turing, nach dem heute das Nobelpreis-Äquivalent für Informatik benannt ist, eine wissenschaftliche Lichtgestalt als jener, der die Grundlagen für moderne Computer legte: Die A-Maschine, wie er sie nannte, war ein mit Papier und Bleistift konzipierter, einfachst möglicher Computer, der dennoch beliebige rechnerische Aufgaben bewältigen konnte. Diese Turing-Maschine war weniger eine echte Rechenmaschine, sondern eher ein paradigmatisches Gedankenmodell eines Computers: Sie umfasst einen verschiebbaren Schreib- und Lesekopf, ein Programm und einen Speicher, der durch ein Band

repräsentiert wird. Auch wenn dieses Modell einfach anmuten sollte: Das Rechnermodell selbst der modernsten klassischen Superrechner lässt sich auf solche Turing-Maschinen zurückführen.

Turing war in der Entwicklung seiner Maschine durch grundlegende Überlegungen motiviert. Letztlich wollte er Gedankenprozesse von Menschen beim Rechnen verstehen und diese nachbilden. So nutzt Turing in seiner bahnbrechenden Arbeit aus dem Jahr 1937 [1] zwar den uns heute geläufigen Begriff „Computer", jedoch schreibt er auch von dessen „state of mind". Dies legt nahe, dass der Computer in Turings Motivation tatsächlich ein Mensch ist, der etwas berechnet. Die Überlegung, dass sich die Berechnung von Funktionen so abbilden lässt, motivierte ihn, zusammen mit Alonzo Church die Church-Turing-These aufzustellen: „Die Klasse der auf einer Turing-Maschine berechenbaren Funktionen stimmt mit der Klasse der intuitiv berechenbaren Funktionen überein." Diese These ist bis heute unangefochten und für eine Vielzahl anderer Rechenmodelle sogar bewiesen. Die erweiterte Church-Turing-These geht noch einen Schritt weiter: Sie vermutet, dass jede Funktion, die sich effizient auf einem Computer berechnen lässt, auch effizient auf einer Turing-Maschine auszuwerten ist. Dies bedeutet, dass die Anzahl der Rechenschritte in einem Rechnermodell als Polynom der Schritte auf einem anderen modellierbar ist.

Unlösbare Probleme lösen

In den 1980er-Jahren gab es erste Überlegungen, ob diese These durch einen radikalen Schritt herauszufordern wäre. Lassen sich vielleicht Rechner bauen, die auf einer ganz anderen Grundlage basieren, ja auf anderen physikalischen Gesetzen? Würde vielleicht sogar die Quantenmechanik, eine der großen Entdeckungen der ersten Hälfte des 20. Jahrhunderts, neue Arten von Computern erlauben, indem man Eigenschaften wie Superposition und Verschränkung geschickt ausnutzt? Da diese Eigenschaften kein Gegenstück in der Welt klassischer Computer haben, könnten sie zu entscheidenden Unterschieden darin führen, wie Rechnungen in einem Computer vonstatten gehen. Es könnte sogar sein, so dachte man, dass sich auf solchen antizipierten Quantencomputern, wie sie bald genannt wurden, Probleme lösen lassen, die selbst auf klassischen Supercomputern praktisch unlösbar sind.

Richard Feynman war der erste, der diese Idee laut aussprach [2]. Dabei warf er nicht nur diese vage Konzeption in den Raum – auch wenn die publizierte Arbeit manchmal so zitiert wird. Stattdessen bemerkte er, dass es am Ende des Tages darum geht, wie der Aufwand zur Berechnung einer Funktion mit der Länge der Eingabe skaliert und skizzierte das, was in der Informatik als polynomielle Reduktion bezeichnet wird. Feynman war von der Idee fasziniert, dass Quantencomputer besser geeignet sein sollten, andere kompliziert zu beschreibende Quantensysteme in ihren Eigenschaften zu simulieren. Dadurch rückte die Idee des Quantensimulators in den Vordergrund. Auch heute ist dieser mögliche Einsatz von Quantencomputern, der großen Einfluss auf Chemie und Physik hätte, ein wichtiges Forschungsfeld und eine der vielversprechendsten Anwendungen solcher Computer.

Damit war auch die Idee geboren, dass die zugrundeliegende physikalische Theorie eine Rolle dabei spielen könnte, wie rechnerisch mächtig Computer sind. Ebenso in den frühen 80er-Jahren schlug Paul A. Benioff ein quantenmechanisches Modell einer Turing-Maschine vor [3]. David Deutsch griff diese Idee auf und entwickelte daraufhin eine Quanten-Turing-Maschine. Er ging davon aus, dass sie rechnerisch mächtiger als eine klassische Turing-Maschine wäre. In der Tat thematisiert seine 1985 veröffentlichte Arbeit die erweiterte Church-Turing-These [4]. Das bald eingeführte und weitaus geläufigere Schaltkreismodell von Quantenrechnern wurde kurz darauf als gleichbedeutend aufgezeigt. Hierbei beschreibt man einen Quantencomputer wie einen herkömmlichen Computer: Eine Rechnung wird in kleine Einheiten heruntergebrochen, die angelehnt an logische Gatter in klassischen Rechnern als Quantengatter bezeichnet werden. Während bei einem klassischen Computer das Ergebnis einer Rechnung am Ende einfach ablesbar ist, verlangt die Quantenmechanik hier einen zusätzlichen Schritt, nämlich eine Messung. Die probabilistische Natur der Quantenmechanik erfordert es, die gleiche Prozedur mehrfach zu wiederholen, weil – nach den Gesetzen der Quantenmechanik – nicht jedesmal das gleiche Ergebnis auftritt und die Wahrscheinlichkeiten, mit denen verschiedene Ergebnisse vorliegen, wichtige Informationen für die finale Auswertung der Rechnung enthalten.

David Deutsch war es, der in der gleichen Arbeit einen ersten, waschechten Quantenalgorithmus entwickelte: Dieser findet heraus, ob eine Funktion, die einen Bitwert, also eine Null oder eine Eins, auf einen anderen abbildet, balanciert oder konstant ist. Balanciert heißt hier, dass ein Bitwert auf Null abgebildet wird und der andere auf Eins, während eine konstante Funktion für beide Bitwerte dieselbe Ausgabe liefert. Dies ist in der Welt von Quantencomputern mit nur einem einzigen Funktionsaufruf möglich, wohingegen im klassischen Fall zwei Funktionsaufrufe nötig sind. Wichtig ist hier, dass der Quantencomputer die Funktion durch Anwenden eines Hadamard-Gatters in Superposition aufrufen kann, ähnlich der Situation in **Abb. 1**. Der klassische Rechner muss die Funktion zweimal hintereinander getrennt aufrufen. Diese Eigenschaft verschafft dem Quantencomputer in dieser Aufgabe einen kleinen Vorteil gegenüber einem klassischen Rechner.

Freilich kann hier noch nicht die Rede von einer echten effizienten Lösung eines Problems sein – immerhin ist nicht einmal die Länge der Eingabe frei wählbar. Dennoch ist die konzeptuelle Bedeutung der Arbeit kaum zu überschätzen. Sie klärte, was es heißt, ein Orakel – also eine Entität, die einen bestimmten Teil einer Rechnung als Black Box ausführen kann – in der Quantenmechanik aufzurufen. Zudem trat sie eine ungeheuer kreative Entwicklung los.

Schon 1992 wurde mit dem Deutsch-Jozsa-Algorithmus eine Variante des Deutsch-Algorithmus vorgeschlagen, die für eine beliebige Anzahl von Eingabe-Bits herausfinden kann, ob eine Funktion balanciert oder konstant ist [5]. Dies ist bei – etwas unrealistisch – exakter Funktionsweise auf einem Quantencomputer sogar mit einer exponentiell

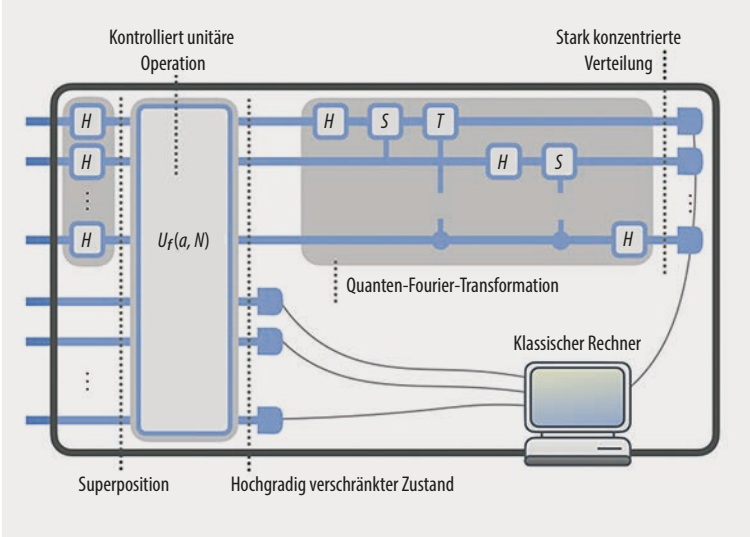

Abb. 1 Der Quantenteil des Shor-Algorithmus umfasst zwei Register: Eines wird in einer Superposition aller Basiszustände präpariert. Dann wird eine kontrolliert unitäre Operation durchgeführt, die mittels modularem Potenzieren den eigentlichen Funktionsaufruf realisiert. Im letzten Schritt wird eine Quanten-Fourier-Transformation durchgeführt, die auf Basisvektoren wie eine diskrete Fouriertransformation wirkt. Tatsächlich sind die Zustände im Verlaufe des Algorithmus stark verschränkt. Vor dem Auslesen liegt dann jedoch wenig Verschränkung vor und man erhält Wahrscheinlichkeitsverteilungen, die stark konzentriert sind.

kleineren Anzahl von Funktionsaufrufen möglich, als klassisch nötig wäre. Der ebenso 1992 vorgestellte Bernstein-Vazirani-Algorithmus [6] entwickelt diese Idee weiter und erlaubt das Lernen eines versteckten Bitstrings, der in einer Funktion enkodiert ist.

Vorteilhafter Quantenalgorithmus

Als echter Durchbruch gilt der Algorithmus von Daniel Simon [7] aus dem Jahr 1997: Dabei handelt es sich um den ersten Quantenalgorithmus, der einen exponentiellen Vorteil gegenüber einem probabilistisch arbeitenden klassischen Rechner – also einem klassischen Rechner, der nicht deterministisch arbeitet, sondern seine Schritte von den Ergebnissen fairer Münzwürfe abhängig machen kann – aufzeigt. Wichtiger vielleicht war noch die Rolle dieses Resultats als Blaupause für den ebenso 1997 veröffentlichten Shor-Algorithmus [8].

Letzterer teilt viele Merkmale mit dem Simon-Algorithmus. In der Tat können beide als Lösungen gelten, in denen eine verborgene Untergruppe auftritt. Allerdings war der Shor-Algorithmus der erste Algorithmus, der einen exponentiellen Vorteil gegenüber dem besten bekannten klassischen Algorithmus für ein praktisch relevantes und berüchtigtes Problem aufwies, nämlich das der Faktorisierung natürlicher Zahlen in ihre Primfaktoren. Der Algorithmus schlug ins Feld ein wie eine Bombe: Bis heute ist er der bekannteste und vielleicht auch mächtigste Algorithmus für Quantenrechner. Er hat das Forschungsfeld initiiert wie kein anderer. Es war über Nacht klar geworden, dass Quantenrechner praktisch relevante Probleme lösen können, die selbst für klassische Superrechner in sinnvoller Zeit nicht bewältigbar sind. Das enorme Interesse am Quantencomputer war geboren – freilich für viele Jahre erst nur als theoretisches Konzept in unseren Köpfen.

Der Shor-Algorithmus umfasst einen klassischen, zahlentheoretischen Teil und einen Quantenteil (**Abb. 1**). Letzterer basiert auf einer Quanten-Fourier-Transformation. Dabei ist es spannend zu sehen, wo der Quantenvorteil herkommt. Jeder einzelne Teil des Algorithmus ist nämlich für passende Eingaben klassisch effizient simulierbar. Erst im Zusammenspiel ergibt sich der mächtige Algorithmus, wie wir ihn kennen. Auch entsteht im Verlauf des Algorithmus viel Verschränkung – und das muss auch so sein: Denn wenn in der Rechnung zu wenig Verschränkung in einem präzisen Sinne auftritt, gibt es mächtige, klassische Simulationsalgorithmen für den Quantenrechner, und deren Vorteil verpufft. Am Ende, vor der Messung, ist diese Verschränkung allerdings wieder weitgehend eingedampft – und auch dies ist zwingend nötig [9].

Shors Algorithmus ist nicht nur ein wichtiger Algorithmus für ein praktisches Problem, oder eher für eine Klasse von Problemen, weil man ihn auf eine Reihe von Problemen mit verborgenen Untergruppen anwenden kann, sondern zeigt auch auf, was den Quantenrechner mächtiger machen kann als sein klassisches Analogon. So ist ein Quantenrechner – entgegen anderslautender Behauptungen, die man zuweilen liest – kein Wunderrechner, keine Maschine, die alles besser kann. Nur für bestimmte strukturierte Probleme ist ein Vorteil zu erwarten. Und schlimmer noch: Jedes dieser Probleme erfordert eine neue zündende Idee.

Einen weiteren einflussreichen Quantenalgorithmus entwickelte Lov Grover 1996 [10]. Sein Quanten-Suchalgorithmus zielt darauf ab, eine Datenbank nach einem spezifischen Eintrag zu durchsuchen. Dieses Problem ist allgegenwärtig, aber ein klassischer Rechner kann es im schlimmsten Fall nicht wirklich effizienter lösen, als sich jedes Element der Datenbank einzeln anzuschauen. Der Grover-Algorithmus macht sich den Quantenzugriff auf die Datenbank zunutze und kann das gesuchte Element so in einer Anzahl an Schritten finden, die mit der Wurzel der Größe der Datenbank skaliert. Das ist zwar kein exponentieller Vorteil, ist aber wegen der Relevanz des Problems dennoch beachtenswert. Vielleicht noch bemerkenswerter ist die fundamental quantenphysikalische Funktionsweise des Algorithmus. Sie basiert auf Rotationen und Spiegelungen im kontinuierlichen Raum der Quantenzustände. Variationen dieser Vorgehensweise kamen seither erfolgreich in einigen anderen Quantenalgorithmen zur Anwendung.

Von der Idee zur Anwendung

Ende der 90er-Jahre gab es also zwar noch keinen funktionierenden Quantencomputer, aber dessen Theorie hatte sich innerhalb von gerade einmal zwei Jahrzehnten von einer vagen, hoffnungsvollen Idee zu einer Handvoll relevanter und eindrucksvoller Quantenalgorithmen entwickelt. Doch diese Entwicklung geriet etwas ins Stocken. Selbst heute noch sind die Algorithmen von Shor und Grover zwei der meistgenannten Antworten auf die Frage nach den praktischen Anwendungen von Quantenrechnern.

Dennoch machte und macht das Feld weiter kontinuierlich Fortschritte [11]. Etwa wurden Algorithmen gefunden, die auf Random Walks, also Zufallsbewegungen, basieren, und bei denen Quantenrechner exponentielle Vorteile aufweisen können [12]. Wohl wichtiger noch ist der 2008 von Aram Harrow, Avinatan Hassidim und Seth Lloyd vorgeschlagene HHL-Algorithmus zum Lösen linearer Gleichungssysteme mit dünn besetzten Matrizen von niedrigem Rang [13]. Dieser kann als Startschuss für viele Arbeiten zu linearer Algebra auf Quantencomputern gelten. Diese tragfähige Idee zog eine Vielzahl von Varianten nach sich: Etwa wurden so auch Quantenalgorithmen gefunden, die konvexe Optimierungsprobleme (semi-definite Programme) besser lösen können. Ein verallgemeinernder moderner Rahmen, in den sich zahlreiche Quantenalgorithmen einbetten lassen, ist derjenige der Quanten-Singulärwertzerlegung [14], die den HHL-Algorithmus, den Grover-Algorithmus und viele andere in einer Art Vereinheitlichung umfasst.

Das Potenzial für einen Vorteil von Quantencomputern in einem fairen Vergleich mit klassischen Rechnern scheint seit 2019 dank Ewin Tang etwas eingeschränkt [15]. Ihre Einsichten nutzen Bausteine eines Quantenalgorithmus, um einen zumindest ebenbürtigen klassischen Algorithmus für dasselbe Problem zu erstellen. Jedoch führten eben diese Einsichten zu weiteren klassischen Algorithmen, die durch existierende Algorithmen motiviert wurden. In der Tat ist die Idee des Quantenrechners längst inspirierend und wichtig für Algorithmenentwicklung, bevor ein einziger Quantenrechner gebaut wurde. Auch in der Festkörperphysik sind Tensornetzwerkmethoden [16] mächtige und viel benutzte Werkzeuge für die Untersuchung stark korrelierter Systeme, die zwar auf herkömmlichen Rechnern arbeiten, die aber von quantenmechanischen Konzepten wie Verschränkung inspiriert sind.

Bei all den theoretischen Überlegungen und mathematisch konzipierten Algorithmen drängt sich natürlicherweise die folgende Frage auf: Sind Quantencomputer überhaupt mehr als mathematische Konstrukte, ja lassen sie sich überhaupt praktisch realisieren und nutzbar machen? Über lange Zeit war das trotz einiger Fortschritte nur bedingt der Fall. Erst in den jüngsten Jahren ist die Entwicklung experimenteller Realisierungen von Quantenrechnern explodiert – zum Teil getrieben von erheblichen Anstrengungen der Industrie. Verschiedene Forschungsgruppen haben, teils an Universitäten, vor allem aber auch in der freien Wirtschaft, erste Geräte gebaut, die einzelne für Quantencomputer wesentliche Operationen ausführen können [17, 18]. Diese Situation kommt einer kleinen Revolution gleich – etwa sind nun Quantenrechner mit 433 Quantenbits realisiert. Einen voll funktionstüchtigen Quantencomputer gibt es freilich noch nicht, jedoch haben diese experimentellen Fortschritte dem Feld einen wichtigen Impuls gegeben. Dabei liegt die Herausforderung weniger in der Systemgröße – wenngleich diese auch eine nichttriviale Hürde darstellt. Viel schwieriger ist es, die nötige extrem hohe Qualität der Gatteroperationen zu erreichen. Erst dann lassen sich Quantenrechner fehlerkorrigieren, sodass sie wirklich skalierbar sind – auch wenn dies wiederum mit einem Überhang an Ressourcen einhergeht.

Am lebenden Objekt

Dennoch ist diese Situation extrem motivierend: Während sich die Fortschritte der 90er- und 2000er-Jahre größtenteils in den Köpfen der Forscherinnen und Forscher abgespielt haben, lassen sich neue Ideen nun teilweise quasi am lebenden Objekt testen. Für paradigmatische Probleme, die bisher wenig anwendungsbezogen sind, sind bereits Quantenvorteile bekannt – eine Situation, in der Quantenrechner bestimmte Probleme schneller lösen als die schnellsten verfügbaren klassischen Superrechner [18, 19]: Dies sind artifizielle Probleme, in denen man von komplizierten Wahrscheinlichkeitsverteilungen Stichproben zieht. Daraus ergeben sich völlig neue Fragen.

Die derzeit verfügbaren Quantengeräte können leider nicht alles, was ein waschechter Quantencomputer kann. Was aber können sie bereits? Welche interessanten Probleme lassen sich mit den verfügbaren Quantengeräten lösen, oftmals im Zusammenspiel mit klassischen Rechnern? Dies ist eine wichtige und stimulierende Frage, welche dieser Tage die Köpfe umtreibt. Sie ist vor allem auch deshalb von großer Bedeutung, weil die benötigten Ressourcen zur Implementierung der oben genannten Algorithmen das derzeit mögliche massiv übersteigen. So wären zur Faktorisierung einer 2048-Bit-Zahl mittels Shor-Algorithmus mehrere Millionen Quantenbits nötig, die in der Lage sein müssten, diesen Algorithmus über mehrere Stunden am Laufen zu halten [19]. Somit klafft eine riesige Lücke zwischen den gewünschten Fähigkeiten eines Quantencomputers und den derzeitigen Quantenchips mit einigen hundert Quantenbits und kurzen Rechenzeiten.

Folglich sind die theoretisch vorhergesagten Quantenvorteile noch deutlich länger außer Reichweite als mancher Artikel einem das vielleicht nahelegen möchte. Um die verfügbare Technik trotzdem bereits für erste Benchmarks auf kleineren Probleminstanzen nutzen zu können und nach neuen Algorithmen zu suchen, hat sich das Feld der hybriden Quantenalgorithmen aufgetan [21, 22]. Diese nutzen einen fixen Quantenschaltkreis mit parameterabhängigen Quantengattern, welche durch einen klassischen Computer optimiert werden (**Abb. 2**). Solch variationelle Quantenalgorithmen kommen mit deutlich geringeren Quanten-Ressourcen aus, da sie anstatt beweisbar exakter Problemlösungen nur eine Approximation der Lösung generieren, die für einen Quantenvorteil ausreichen könnte. Der viel-

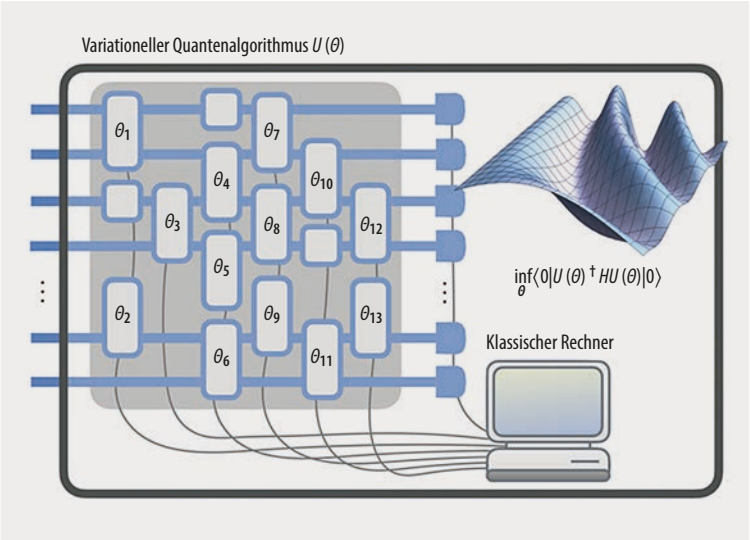

Abb. 2 Variationelle Quantenalgorithmen umfassen in ihrem Quantenteil parametrisierte Quantenschaltkreise, deren Parameter veränderbar sind. Ein klassischer Rechner liest Messergebnisse ein und ändert auf Basis dieser Daten die variationellen Parameter. Da sowohl der klassische als auch der Quantenteil eine integrale Rolle im Algorithmus spielt, sind solche Algorithmen auch als hybride Quantenalgorithmen bekannt. Sie finden Anwendungen in der Quantenchemie und in der approximativen Lösung von Optimierungsproblemen.

leicht bekannteste dieser Algorithmen ist der Quantum Approximate Optimization Algorithm von Edward Farhi, Jeffrey Goldstone und Sam Gutmann [23], der auf variationelle Art versucht, Lösungen klassischer Optimierungsprobleme besser zu approximieren.

Mehrere theoretische Arbeiten haben hier bereits Limitationen und deren potentielle Umgehung diskutiert, und es ist entgegen der bisher genannten Quantenalgorithmen auch noch nicht mathematisch solide nachgewiesen, dass diese Klasse von Algorithmen tatsächlich einen Vorteil gegenüber klassischen Computern erreichen kann. Dies hält Forschende aber nicht davon ab, wichtige Anwendungen systematisch auszuloten. Inspiriert von solch hybrider Zusammenarbeit von Quantenschaltkreisen unter klassischer Kontrolle und zusätzlichem klassischen Pre- und Postprocessing hat auch das Interesse an praktischen, industriell relevanten Problemen zugenommen. Man will Optimierungsprobleme geeigneter lösen – wie sie in der industriellen Produktion allgegenwärtig sind – oder deren Lösungen besser approximieren. Außerdem geht es darum, Algorithmen des maschinellen Lernens mithilfe von Quantenkomponenten zu verbessern.

Dies ergibt in der Tat Sinn: Während Quantencomputer in vielerlei Hinsicht noch Zukunftsmusik sind, beeinflusst das maschinelle Lernen viele Aspekte unserer modernen Welt bereits heute. Im Quanten-Maschinenlernen, einem sich insbesondere in den letzten zehn Jahren rapide entwickelnden Forschungsgebiet, fragt man nun: Wie lassen sich die Vorteile von maschinellem Lernen und Quantencomputern vereinen? Hier gibt es bereits vielversprechende theoretische Resultate. Zum einen sind Quantendaten, ebenso wie Quantencomputer, zwar längst nicht allmächtig, doch inzwischen kennen wir einige praktisch relevante Probleme, bei denen Daten in Quantenform das Lernen signifikant vereinfachen [24]. Zum anderen sind Techniken aus dem maschinellen Lernen heutzutage wichtige Werkzeuge, um Informationen über Quantenzustände und -prozesse zu sammeln [25]. Des Weiteren gibt es Lernprobleme mit klassischen Daten, bei deren Lösung Quantenlernmodelle einen Vorteil haben [26, 27]. Allerdings sind diese Probleme bisher nur praxisferne theoretische Konstrukte. Ob Quanten-Maschinenlernen also die bereits sehr ausgefeilten und mächtigen neuronalen Netze für Aufgaben in der realen Welt ersetzen wird, ist noch unklar und angesichts des atemberaubenden Fortschritts klassischer künstlicher Intelligenz wohl erst einmal unwahrscheinlich. Hinzu kommt die Schwierigkeit des Übersetzens klassischer Daten in Quantendaten, was noch einiger Forschung bedarf. Ansonsten besteht die Gefahr, mögliche Vorteile von Quantencomputern in der Datenverarbeitung bereits vor Verwendung der Algorithmen zunichte zu machen.

Diese Entwicklungen befeuern auch eine Denkrichtung, die weitere, potenziell industriell relevante Probleme auslotet. In ähnlicher Weise und sogar mit ähnlicher mathematischer Methodik gibt es substantiierte Hinweise, dass Quantenrechnen im kombinatorischen Optimieren Vorteile bieten kann, zumindest für viele Instanzen. Ausgehend von neuen Quantenalgorithmen, die nichtlineare Differenzialgleichungen lösen – welche tatsächlich mathematisch vom oben genannten Algorithmus zur Lösung von Gleichungssystemen inspiriert sind – hofft man auf Anwendungen etwa in der Strömungsmechanik oder der Modellierung von Finanzmärkten. Ob diese Anwendungen in der mittleren Zukunft erreichbar sind, steht in den Sternen, und häufig werden unrealistische Erwartungshaltungen geschürt. Viel wird davon abhängen, ob zumindest eine partielle Fehlerkorrektur erreichbar ist.

Feynmans Traum

Einiges spricht dafür, dass sich die ersten praktischen Anwendungen in der Quantensimulation von Materialien, anderen Systemen der kondensierten Materie und in der Quantenchemie erreichen lassen. Dies hat auch damit zu tun, dass derartige Anwendungen verhältnismäßig resilient gegen Fehlereinflüsse sind. So schließt sich der Bogen zum Traum, den Richard Feynman einst laut träumte: die Simulation von Quantensystemen mit Quantensystemen.

Wohin die Reise geht, weiß niemand. Die kommenden Jahre, vielleicht Jahrzehnte, werden entscheiden, wie nahe-

liegend praktische Quantenvorteile wirklich sind. So ergibt sich geradezu ein Krimi, eine Fahrt auf der Achterbahn zwischen neuen Durchbrüchen bei der Entwicklung von Quantenalgorithmen und Hardware sowie Rückschlägen und Aussagen darüber, wie schädlich Fehler von Quantencomputern sein können. Nach wie vor sind zündende und oft radikal neue Ideen nötig, um neue Algorithmen zu finden.

Es gibt auch immer wieder überraschende neue Anwendungen: Etwa wurden unlängst Quantenalgorithmen zur Lösung gekoppelter klassischer harmonischer Oszillatoren gefunden [28]. Für die Forschung ist dies eine ideale Situation, solange man eine realistische Erwartungshaltung pflegt und den Hype vermeidet. In jüngerer Vergangenheit fanden sich in einigen prominenten Wirtschaftsmagazinen Titelgeschichten über Quantencomputer, die angeblich alle rechnerischen Prozesse rasant beschleunigen würden. Dies ist nicht der Fall. Die Gemengelage im Feld ist aber insgesamt eher ermutigend als demotivierend: Über Quantenrechner zu reden ist sogar dann spannend, wenn man nur Dinge sagt, die wahr sind.

Literatur

[1] *A. M. Turing*, Proc. Lond. Math. Soc. **42**, 230 (1937)
[2] *R. P. Feynman*, Int. J. Theor. Phys **21**, 6/7 (1982)
[3] *P. Benioff*, J. Stat. Phys. **22**, 563 (1980)
[4] *D. Deutsch*, Proc. Royal Soc. Lond. A **400**, 97 (1985)
[5] *D. Deutsch* und *R. Jozsa*, Proc. R. Soc. Lond. A **439**, 553 (1992)
[6] *E. Bernstein* und *U. Vazirani*, SIAM J. Comp. **26**, 1411 (1997)
[7] *D. R. Simon*, SIAM J. Comp. **26**, 1474 (1997)
[8] *P. W. Shor*, SIAM J. Comp. **26**, 1484 (1997)
[9] *D. Gross*, *S. T. Flammia* und *J. Eisert*, Phys. Rev. Lett. **102**, 190501 (2009)
[10] *L. K. Grover*, In Proc. 28th Annual ACM Symp. Theory of Computing, pp. 212 (1996)
[11] *A. Montanaro*, npj Quant. Inf **2**, 15023 (2016)
[12] *A. Childs* et al., In Proc. 35th Annual ACM Symp. Theory of Computing, pp. 59 (2003)
[13] *A. W. Harrow*, *A. Hassidim* und *S. Lloyd*, Phys. Rev. Lett. **103**, 150502 (2009)
[14] *A. Gilyen* et al., In Proc. 51st Annual ACM Symp. Theory of Computing, pp. 193 (2019)
[15] *E. Tang*, In Proc. 51st Annual ACM Symp. Theory of Computing, pp. 217 (2019)
[16] *J. I. Cirac* et al., Rev. Mod. Phys. **93**, 045003 (2021)
[17] *A. Kandala* et al., Nature **549**, 7671 (2017)
[18] *F. Arute* et al., Nature **574**, 505 (2019)
[19] *D. Hangleiter* und *J. Eisert*, Rev. Mod. Phys. **95**, 035001 (2023)
[20] *C. Gidney* und *M. Ekerå*, Quantum **5**, 433 (2021)
[21] *M. Cerezo* et al., Nature Rev. Phys. **3**, 625 (2021)
[22] *K. Bharti* et al., Rev. Mod. Phys. **94**, 015004 (2022)
[23] *E. Farhi, J. Goldstone* und *S. Gutmann*, arXiv:1411.4028 (2014)
[24] *S. Arunachalam* und *R. de Wolf*, ACM Sigact News 48.2, pp. 41 (2017)
[25] *A. Elben* et al., Nature Rev. Phys. **5**, 9 (2023)
[26] *Y. Liu, S. Arunachalam* und *K. Temme*, Nature Phys. **17**, 1013 (2021)
[27] *R. Sweke, J.-P. Seifert, D. Hangleiter* und *J. Eisert*, Quantum **5**, 417 (2021)
[28] *R. Babbush* et al., arXiv:2303.13012 (2023)

Die Autoren

Jens Eisert (FV Quantenoptik und Photonik) leitet eine interdisziplinär arbeitende Forschungsgruppe in der theoretischen Physik an der FU Berlin, die an komplexen Quantensystemen und Quantentechnologien forscht. Zudem ist er mit der Fraunhofer-Gesellschaft und der Helmholtz-Gemeinschaft verbunden. Für seine Beiträge wurde er bereits mit zwei ERC Grants, einem EURYI Award und dem Google NISQ-Award ausgezeichnet.

Paul Fährmann (FV Theoretische u. Mathematische Grundlagen der Physik & Atomphysik) promoviert an der FU Berlin zu Quantenalgorithmen in der nahen und fernen Zukunft. Zuvor studierte er in Berlin und Kopenhagen Physik und wurde mit dem Studienpreis der Physikalischen Gesellschaft zu Berlin sowie dem Quantum Futur Award ausgezeichnet.

Matthias C. Caro (FV Quanteninformation & Theoretische u. Mathematische Grundl. der Physik) forscht als DAAD PRIME Postdoctoral Fellow an der FU Berlin und am California Institute of Technology zu Fragen an der Schnittstelle von Quantencomputern und maschinellem Lernen. Seine Promotion an der TU München wurde mit Preisen vom Freunde der TUM e.V., vom Munich Center for Quantum Science and Technology und vom TopMath Programm des Elitenetzwerks Bayern ausgezeichnet.

Prof. Dr. Jens Eisert, **Paul Fährmann** und **Dr. Matthias C. Caro**, Freie Universität Berlin, Arnimallee 14, 14195 Berlin