Kein Nachdruck, keine Veröffentlichung im Internet oder einem Intranet ohne Genehmigung des Verlags und der GDNÄ

GDNÄ
Die Wissensgesellschaft
Gesellschaft Deutscher Naturforscher und Ärzte
German Association for the Advancement of Science and Medicine

Frank K. Wilhelm-Mauch, Saarbrücken

Quantencomputer

Anwendungen – Zeitskala – Plattformen

Quantencomputer sind derzeit in aller Munde. Nach einer langen Geschichte wissenschaftlicher Vorarbeiten erleben wir in den letzten Jahren den Wechsel von der grundlegenden in die angewandte Forschung: Sowohl die Europäische Union als auch die Bundesregierung haben große Forschungsprogramme für Quantentechnologien aufgelegt (zu denen neben dem Quantencomputing auch die Quantensensorik, -kommunikation und -simulation gehören). Die anwendungsorientierten außeruniversitären Forschungsaktivitäten auf diesem Gebiet steigen, wie das Engagement von Industrieunternehmen verschiedener Größen – vom Startup bis zum Weltkonzern – zeigt. Für das Gebiet völlig neue Personenkreise nehmen sich des Themas an, insbesondere entstehen neue mögliche Anwendungen. Es gibt Analysen zur Technikfolgenabschätzung z.B. des Bundesamts für Sicherheit in der Informationstechnik (BSI) und eine Anhörung im Bundestag. Auch das Medienecho ist entsprechend groß.

Was tut sich auf diesem Gebiet, was ist Hype, was ist realistisch? Dieser Artikel versucht, eine Momentaufnahme zum Jahresanfang 2019 zu geben – wissend, dass diese sehr bald veraltet sein kann.

Quantencomputing ist im Augenblick im Kontext des Höchstleistungsrechnens zu sehen, also im Zusammenhang mit anspruchsvollen und aufwendigen Rechenaufgaben von Wissenschaft und Technik, für die eigens Rechenzentren betrieben werden. Alle dort eingesetzten Supercomputer basieren bislang noch auf klassischen (also nicht quantenphysikalischer) Parallelrechnern, was sich allmählich zu ändern beginnt, zumal es für die Nutzung der wenigen bereits in Erprobung befindlichen Quantenrechner Cloud-Lösungen gibt. An einen Einsatz als PC ist aber auf absehbare Zeit überhaupt nicht zu denken – einerseits aufgrund der anspruchsvollen Hardware, andererseits aufgrund der spezialisierten Einsatzgebiete.

Potential der Quantentechnologie 2.0

Quantenphysik ist eine Schlüsseltheorie des 20. Jahrhunderts. Ihre Ergebnisse und Aussagen sind – formuliert in mathematischer Sprache – wohlverstanden und mit teilweise spektakulärer Genauigkeit verifiziert. Für physikalische Phänomene (mit Ausnahme der Gravitation) darf die Quantenphysik als bestätigt angesehen werden.

Quantenphysik ist schon seit längerem ein Technologietreiber. So beruhen unter anderem Laser, Transistor und Halbleiterelektronik, Spinresonanz- und Kerntechnik auf der gezielten technologischen Nutzung der Quantenphysik. Diese sind aber im heutigen Sprachgebrauch „Quantentechnologien 1.0“ (Abb. 1.): Sie nutzen zwar intern gezielt quantenphysikalische Gesetze, interagieren aber bereits mit dem nächsten Bauelement nach den Gesetzen der klassischen Physik. In diesem Sinn wird in den üblichen Transistoren auf unseren Computerchips die Information klassisch verarbeitet.

Die modernen Quantentechnologien 2.0 nutzen die Gesetze der Quantenphysik auch auf einer größeren Skala. Dies kann viele Formen annehmen, die zu verschiedenen Anwendungen führen:

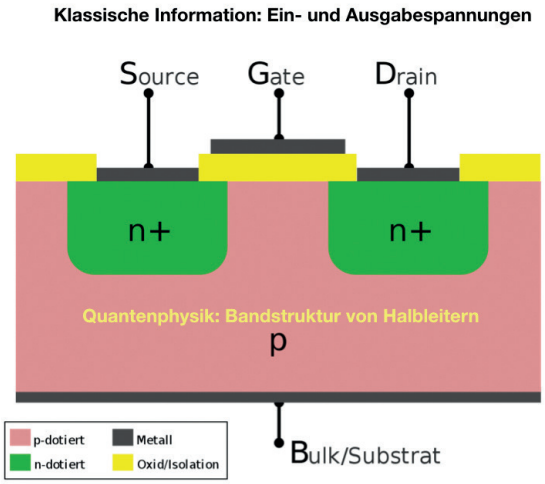

Abb. 1. Diagramm eines klassischen Feldeffekttransistors als Quantentechnologie 1.0: Die Materialeigenschaften nutzen die Quantenphysik, die verarbeitete Information ist klassisch.

©Wissenschaftliche Verlagsgesellschaft Stuttgart

Kein Nachdruck, keine Veröffentlichung im Internet oder einem Intranet ohne Genehmigung des Verlags und der GDNÄ

• In der *Quantensensorik* werden Techniken entwickelt, die Messungen mit einer Genauigkeit liefern, die nur noch durch die Heisenbergsche Unschärferelation begrenzt sind. Diese Grenze kann beliebig klein sein: Die Unschärferelation beschränkt das Produkt der Genauigkeiten zweier komplementärer Größen wie Ort und Geschwindigkeit – wenn man eine dieser Größen möglichst genau messen möchte, muss man gezielt Ungenauigkeiten der anderen Größe erlauben (sog. „Squeezing“).

• In der *Quantenkommunikation* nutzt man das quantenmechanische Gesetz, dass jede Messung i.A. den Quantenzustand verändert, zur Erzeugung von Informationssicherheit: Kryptographische Schlüssel werden so erzeugt, dass Lauscher sofort bemerkt werden.

• In der *Quantensimulation* nutzt man steuerbare Quantensysteme zum Studium von wissenschaftlich interessanten Quantensystemen.

• Im *Quantencomputing* nutzt man die Fähigkeit von Quantensystemen, mehrere Zustände (hier: Datenwerte) parallel zu durchlaufen, für massive Parallelverarbeitung.

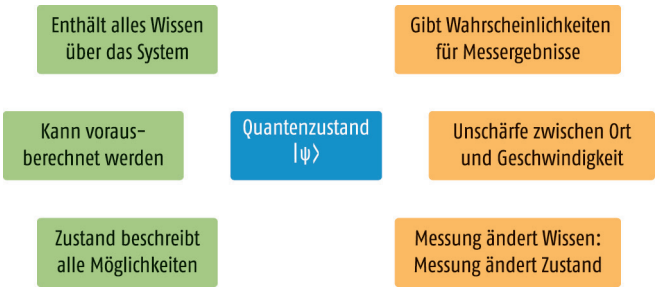

Abb. 2. Berechenbarkeit und Zufall in der Quantenphysik – der Zustand eines Systems kann zwar vorausberechnet werden, bestimmt aber nicht alle Messungen mit Sicherheit. Daraus ergibt sich die Unschärferelation, aber auch die Invasivität der Messung: Eine Messung, die Gewissheit herstellt, verändert den Zustand.

Quantencomputer als ultimativer Parallelrechner

Der letzte Punkt, Quantencomputing, soll hier vertieft werden. Was verspricht man sich von Quantencomputern? Dazu lohnt es sich, zunächst einmal die aktuellen Entwicklungen im Hochleistungsrechnen zu betrachten. Die wichtigste Technik in diesem Bereich ist die *Parallelisierung*. Die einzelnen Elemente und Prozessoren solcher Supercomputer sind durchaus vergleichbar mit denen von normalen PCs oder Spielekonsolen. Der Leistungssprung entsteht dadurch, dass eine Vielzahl dieser Prozessoren bzw. Prozessorkerne Daten parallel verarbeiten und dass die so entstehenden Prozess-Stränge untereinander kommunizieren. Diese Fokussierung auf Parallelrechner ist in Teilen den Gesetzen der Physik geschuldet, die z.B. eine weitere Erhöhung der Taktfrequenz, also der Geschwindigkeit jedes einzelnen Prozessorkerns, erschwert.

Vorweg einige grundlegende Bemerkungen: In der Quantentheorie kommt dem *Quantenzustand* Ψ als abstraktes mathematisches Objekt eine zentrale Bedeutung zu. Dieser kann (im Prinzip) vorausberechnet werden – was die Grundlage jeglicher technologischen Nutzung der Quantenphysik ist. Andererseits legt der Zustand, auch wenn er komplett bekannt ist, die messbaren Größen nicht mit Sicherheit fest (Abb. 2). Stattdessen kann er Überlagerungen beschreiben, dargestellt durch Wahrscheinlichkeitsamplituden, die der Physik von Wellen folgen. Gemäß der Heisenbergschen Unschärferelation wird z.B. der Ort eines Teilchens durch den Zustand im Allgemeinen nicht genau festgelegt.

Ein Quantencomputer basiert nun darauf, mit wohldefinierten Quantenzuständen zu arbeiten. Die klassische Bit-Werte 0 und 1, mit denen konventionelle Computern operieren, haben hier die Funktion von Basiswerten des Raums der Quantenbits (oder kurz Qubits). Anders als klassische Bits können Qubits aber auch quantenmechanische Überlagerungszustände einnehmen. Trotz ihres binären Charakters können sie aufgrund dieser Überlagerung Anteile beider Basiswerte simultan innehaben (Abb. 3,4). Dies macht den entscheidenden Unterschied zum klassischen Computer aus und ist verantwortlich für die *Quantenbeschleunigung*. Diese Quantenbeschleunigung bezieht sich nicht auf eine schnellere Taktfrequenz oder andere Leistungsmerkmale klassischer Computer, sondern darauf, dass der Quantencomputer Arbeiten leistet, an denen konventionelle Rechner scheitern, weil für sie der Arbeitsaufwand mit wachsender Aufgabengröße prohibitiv (z.B. exponentiell) anwächst.

In anderen Worten: Während beim konventionellen Computer Register und Speicher zu jedem Zeitpunkt einen einzigen Wert haben, können diese in einem Quantencomputer mehrere Werte gleichzeitig in Überlagerung enthalten und mit einem Quantenalgorithmus bearbeitet werden, der sich dann auf alle diese Werte auswirkt (Abb. 4).

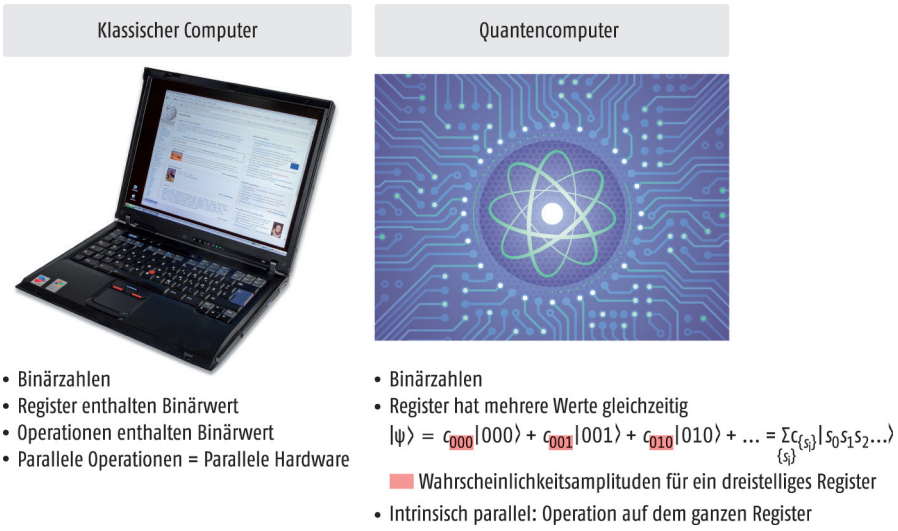

Abb. 3. Gegenüberstellung der binären Informationsspeicherung in klassischen und Quantencomputern – der Quantencomputer ist binär, gibt aber die Möglichkeit, mehrere Rechnungen zu überlagern.

©Wissenschaftliche Verlagsgesellschaft Stuttgart

Quantenbit = Qubit: Quantenzustände von 0 und 1

2-Qubit-Register $|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$ ← **Alle Werte kommen vor**

Wahrscheinlichkeitsamplitude $0 \le |c_{ij}| \le 1$

Wahrscheinlichkeit für ij $p_{ij} = |c_{ij}|^2$

$|\psi\rangle =$	Allgemeine Notation für einen Quantenzustand
$|\psi_0\rangle = |0\rangle$	Notation, wenn 100 % Wahrscheinlichkeit für Messergebnis „0“ bzw. „1“
$|\psi_1\rangle = |1\rangle$	(Vgl. Blochkugel rechts)

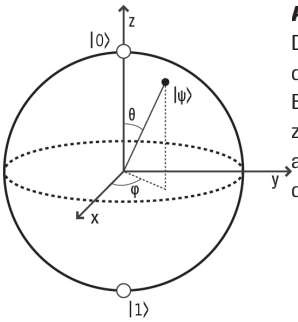

Abb. 4. Komplexität eines Quantenzustands: Der Zustand eines einzelnen Qubits kann durch Punkte auf einer Kugeloberfläche, der Blochkugel (links), dargestellt werden. Ein zwei-Qubit Register kann eine Überlagerung aller klassischer Werte einnehmen und wird durch vier komplexe Zahlen beschrieben.

Ein Quantencomputer arbeitet also ähnlich einem modernen Parallelcomputer, aber ohne dass mehrere Exemplare der Quantenhardware gebaut werden müssen – und die Parallelität kann im Prinzip den gesamten Datenraum erfassen – es können alle darstellbaren Eingabewerte verarbeitet werden. Man spricht auch vom massiven Quantenparallelismus.

Dieser Vorteil ist aber untrennbar mit einer zentralen Herausforderung verbunden: Am Ende der Rechnung soll ein eindeutiges, richtiges Ergebnis stehen – dies steht scheinbar im Widerspruch zur probabilistischen Natur der Quantenphysik, ausgedrückt in den schon erwähnten Wahrscheinlichkeitsamplituden. Der erwähnte Überlagerungscharakter und mithin die Parallelität der Quantenrechnung müssen also wieder aufgehoben werden (sog. „uncomputing“). Dies ist die Kernherausforderung bei der Entwicklung von Quantenalgorithmen, die den Quantenparallelismus nutzbar machen.

Trotz dieser Herausforderung ist es aber gelungen, Quantenalgorithmen mit potentiell disruptiven Anwendungen zu finden, die genau dies leisten: Nutzung der Quantenbeschleunigung bei nutzbarer Ein- und Ausgabe.

Deshalb eröffnen sich bereits heute neue Möglichkeiten der Optimierung bei der Datenbanksuche, dem Maschinellen Lernen, der Kryptanalyse, der ultraschnellen Fouriertransformation sowie der Simulation von Quantensystemen. Einige Beispiele sollen die Bedeutung der Quantenbeschleunigung verdeutlichen.

- **Quantenbeschleunigung der Datenbanksuche**

Mit einer Überlagerung von Testwerten kann nur eine einzige Abfrage die gesamte Datenbank durchmustern. Nach dem ersten parallelen Blick auf die Datenbank ist das gesuchte Ergebnis zwar im Quantenzustand markiert, ist aber leider noch nicht eindeutig abfragbar. Der Schritt muss deshalb wiederholt werden, um das richtige Ergebnis zu verstärken. Nach einer Zahl von Schritten, die der Wurzel der Anzahl der Einträge in der Datenbank entspricht, ist das richtige Ergebnis gefunden. Diese Technik heißt *Amplitudenverstärkung*. Mit einem klassischen Computer müsste man etwa die Hälfte der Einträge abfragen. Dagegen müsste man zum Auffinden eines Objekts in einer Million Datensätzen mit einem Quantencomputer statt etwa eine halbe Million nur tausend Abfragen durchführen.

Die Datenbanksuche ist aber nicht mehr die wichtigste Anwendung der Amplitudenverstärkung – insbesondere da sie erfordert, dass die Datenbank im Quantenspeicher auf eine sehr spezielle Art abgelegt ist. Zunehmend kommt sie vielmehr zur Beschleunigung von testbasierten Monte-Carlo-Algorithmen z.B. in der Finanzmarktmodellierung zum Einsatz.

- **Quantenbeschleunigung von Optimierung**

Optimierungsalgorithmen sind ein wesentlicher Antrieb der modernen Informatik. Auch beim Maschinellen Lernen ist es am Ende oft die Optimierung, die die meiste Rechenzeit erfordert. Optimierungsaufgaben sind dann schwierig, wenn die zu minimierende Funktion sehr viele lokale Minima erhält – also Stellen, an denen die Veränderung weniger Bits das Ergebnis vergrößert, die Änderung vieler Bits dieses aber wieder verkleinern kann.

Quantencomputer – sowohl die hier diskutierten als auch die unten erwähnten adiabatischen Quantencomputer – können bestimmte Optimierungsaufgaben beschleunigt lösen. Auf klassischen Computern ist eine Schwierigkeit von harten Optimierungsaufgaben, dass diese gerne in lokalen Minima stecken bleiben – also bei Lösungen, die sich bei geringen Veränderungen zwar stets verschlechtern, aber dennoch nicht das globale Optimum sind. Das Ausschließen solcher „falschen Optima“ ist auf klassischen Computern sehr zeitaufwendig. Auch hier erlaubt es die breite Überlagerung von Testwerten, den Optimierungsraum schnell zu erfassen. Hinzu kommt der *quantenmechanische Tunneleffekt* für die Information. Der Tunneleffekt ist eine Konsequenz des Wellencharakters der Quanten und erlaubt es, unvorteilhafte Bereiche der klassischen Optimierungslandschaft zu durchdringen und sich so aus den oben erwähnten lokalen Minima effizient zu befreien.

Wie effektiv diese Quantenbeschleunigung wirklich ist, ist Gegenstand der aktuellen Forschung. Man geht davon aus, dass viele dieser klassisch harten Optimierungsprobleme beschleunigt gelöst werden können, aber nicht alle.

- **Quantenbeschleunigung der Kryptanalyse**

Der aktuelle Standard für Kryptographie im Internet, RSA (benannt nach den drei Mathematikern, die den Standard 1976 entwickelten), basiert auf Komplexität. Entzifferung ist im Prinzip möglich, aber rechnerisch prohibitiv aufwendig. Vergrößerung des Schlüssels (einer langen zur Entschlüsselung benötigten Ganzzahl) um wenige Stellen erhöht den Computeraufwand beim Entschlüsseln immens. Selbst wenn moderne Rechner in die Nähe der Fähigkeit kommen, einen solchen Schlüssel zu brechen, kann dies vom Verschlüsseler durch die Verwendung eines längeren Schlüssels kompensiert werden – den Wettstreit beider Seiten gewinnt die Verschlüsselung.

Kein Nachdruck, keine Veröffentlichung im Internet oder einem Intranet ohne Genehmigung des Verlags und der GDNÄ

©Wissenschaftliche Verlagsgesellschaft Stuttgart

Kein Nachdruck, keine Veröffentlichung im Internet oder einem Intranet ohne Genehmigung des Verlags und der GDNÄ

RSA beruht auf der großen Komplexität des Findens der Primfaktoren von Ganzzahlen. Diese kann in der Zahlentheorie auf das Finden der Periode einer Funktion zurückgeführt werden. Da Quantensysteme sich auf natürliche Weise periodisch verhalten und quasi selbständig Fourieranalysen durchführen, wundert es nicht, dass mit ihnen diese Aufgabe erheblich beschleunigt erledigt werden kann. Damit wäre RSA von einem Quantencomputer zu knacken.

Bei oberflächlicher Betrachtung mag dies wie eine kryptographische Apokalypse aussehen und wird von den zuständigen Stellen auch mit dem nötigen Ernst behandelt. Folgende Fakten und Überlegungen mögen für eine realistische Einschätzung hilfreich sein:

- Die Algorithmen für Quantensysteme sind lang und störungsanfällig. Sie benötigen eine Quantenfehlerkorrektur (s.u.), weshalb sie auf absehbare Zeit nicht zur Verfügung stehen werden.
- Selbst wenn es im Rahmen eines Großprojektes gelänge, einen geeigneten Quantencomputer zu entwickeln, so wäre es mit kurzem Anlauf möglich, neue kryptographische Verfahren zu etablieren, für deren Entschlüsselung noch kein Quantenalgorithmus bekannt ist („Post-Quanten-Kryptographie“).
- Die Kryptographie kann aber auf ganz andere Weise, die nicht auf Komplexität beruht, mit Hilfe von Quantensystemen sicher gemacht werden: Sie besteht in der Nutzung der Quantenkommunikation zur Übertragung des Schlüssels. Jedes Abhören führt zur Veränderung der Quantenzustände und wird damit sofort entdeckt.
- Nicht zuletzt bleibt festzustellen, dass bislang keiner der bekannten Skandale in der Datensicherheit auf fehler- und mangelhafter Anwendung mathematischer oder physikalischer Prinzipien beruht, sondern auf Nachlässigkeiten auf politischer Ebene oder schlichtweg auf menschlichem Verhalten.

- **Simulation von Molekülen und Materialien**

Eine naheliegende und bereits von Richard P. Feynman bei seinen ersten Überlegungen zu einem Quantencomputer ins Auge gefasste Anwendung ist die Simulation der Eigenschaften von Molekülen und Materialien. Diese sind selbst Quantensysteme, und die Umsetzung von Simulationsaufgaben auf ein anderes, nun gesteuertes Quantensystem – eben auf einen programmierbaren Quantencomputer – ist vergleichsweise geradlinig. Mehr noch – diese Aufgaben sind von klassischen Rechnern oft kaum zu lösen. Anders als bei der Kryptanalyse sind sie meistens speicher- und nicht zeitlimitiert. Die Quantencomputer der ersten Generation, auf die wir nun zu sprechen kommen, haben dagegen ein zur Lösung dieser Aufgabe passendes Leistungsprofil (Abb. 5). Natürlich hat die klassische computergestützte Chemie hier großartige Fortschritte in Form von Näherungsverfahren erzielt, die es oft erlauben, das Speichern des ganzen Molekülzustands zu vermeiden – dies funktioniert bei all den Molekülen, die nicht stark elektronisch korreliert sind. Der Quantencomputer kann helfen, diese Einschränkung zu überwinden.

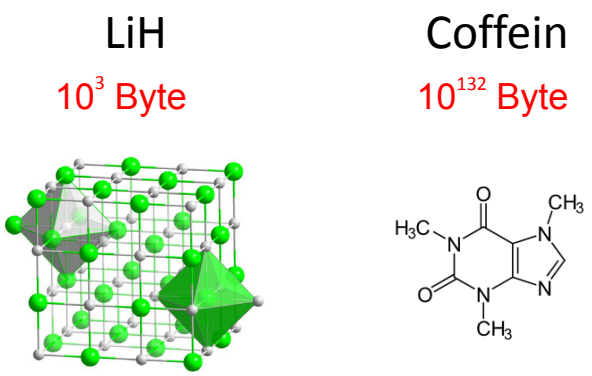

Abb. 5. Beispiel des anwachsenden Speicherbedarfs für die Erfassung molekularer Zustände vom zweiatomigen Lithium-Hydrid bis zum Coffein.

Die Eigenschaften von Molekülen, die hier zugängig werden, sind die Energetik und damit die Vorhersage der molekularen Struktur. Sie sind für die Modellierung katalytischer Prozesse von großem Interesse. Ein höchst wichtiges und sehr anspruchsvolles Ziel ist es, die biologische Luftstickstofffixierung – die Reduktion des molekularen Luftstickstoffs zu Ammoniak durch Mikroorganismen – technisch nachahmen zu können. Die durch die Nitrogenase (einen Enzymkomplex) katalysierte Reaktion läuft bei Zimmertemperatur ab, während wir Menschen dafür den energieaufwendigen Haber-Bosch-Prozess benötigen. Ein tieferes Verständnis der katalytisch wirksamen Eisenkomplexe der Nitrogenase könnte dazu beitragen, den anthropogenen CO_2-Ausstoß bei der Düngemittelherstellung erheblich zu reduzieren.

Entwicklungslinien

Die Arbeit an der Realisierung von Quantencomputern mit ihren algorithmischen Versprechen wird weltweit mit höchstem Einsatz betrieben. Auf dem Weg vom Konzept zur Umsetzung lassen sich große Entwicklungslinien identifizieren, auf die hier eingegangen werden soll.

- **Direktes, gatterbasiertes Quantencomputing**

Die direkteste Möglichkeit, das Konzept vom Quantencomputer in die Realität umzusetzen ist das Gattermodell. Dieses ähnelt der Funktionsweise eines klassischen Computers (und benötigt diesen zur Steuerung): In einem (klassischen) Programmspeicher sind die elementaren Befehle (Logikgatter) des Quantencomputers abgelegt. Die Quantenbits (Qubits) werden initialisiert und die Quantengatter werden in zeitlicher Abfolge auf sie angewandt. Der Unterschied zum klassischen Computer besteht in der Mächtigkeit der Operationen, die jetzt die volle Funktionalität des Quantencomputers enthalten und die Quantenparallelität ausschöpfen können.

Das Gattermodell ist der im Augenblick meistverfolgte Ansatz. Bislang sind im Labor damit Computer mit 20 Qubits realisiert und der Nutzung von außen zugänglich gemacht worden – diese kann man mit Fug und Recht als Quantencomputer der ersten Generation bezeichnen.

Ziel der Forschung ist das Erreichen der Quantenüberlegenheit: Die Schaffung eines Quantencomputers, der in zumindest einer Aufgabe den größten aktuell existierenden Hochleistungsrechner übertrifft. Im Prinzip ist dieser Punkt bei 50 Qubits erreicht (siehe Vortrag R. Blatt). Diese Zahl mutet

©Wissenschaftliche Verlagsgesellschaft Stuttgart

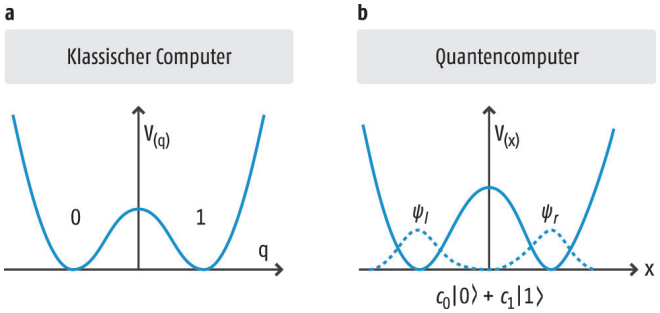

Abb. 6. Fehlerempfindlichkeit von klassischen Computern und Quantencomputern: **– a.** Bei klassischen Computern kommt es nur auf die Position analoger Spannungswerte relativ zu einer Trennlinie an, **– b.** bei Quantencomputern sind die analogen Vorfaktoren einer Überlagerung wichtig. V= Potentielle Energie, q, x stehen für abstrakte Koordinaten, im Falle eines Transistors wäre es die elektrische Spannung.

im Zeitalter der Terabytes absurd niedrig an – doch muss man sich vor Auge führen, dass zur Abspeicherung eines allgemeinen Quantenzustands mit N Qubits 2^N komplexe Zahlen benötigt werden.

Nach Erreichen dieses Punktes hofft man dann, diese Leistung auch zur Lösung nicht nur akademischer Probleme nutzen zu können. Wie oben beschrieben geht man davon aus, dass dies zunächst im Bereich der Simulation von Molekülen der Fall sein wird.

Ab diesem Augenblick hätte man die Situation, dass man im Alltag zwar immer noch nicht unbedingt mit Quantencomputern umgeht, aber deren Ergebnisse nutzt. Dies wäre vergleichbar der Zeit in den 1940er Jahren, als Computer noch nicht gängig waren, die Entschlüsselung der Enigma durch Alan Turing und Kollegen aber durchaus zur Verkürzung des Zweiten Weltkrieges beigetragen haben dürfte.

Die große Herausforderung ist aber nicht die Zahl der Qubits, sondern deren Qualität. Quanteninformation ist enorm anfällig für Störungen, die sich dann in Fehlern des Quantencomputers niederschlägt. Dies liegt am teilweise nicht-digitalen (analogen) Charakter der Quanteninformation und an ihrer Komplexität. Der klassische Computer ist in dieser Hinsicht viel robuster: Wenn alles in 0 und 1 codiert ist, kann man im Inneren der Hardware (also in den Transistoren) erlauben, dass z.B. die elektrischen Spannungen in einem gut bemessenen Intervall liegen, um sie als 0 oder 1 zu identifizieren (Abb. 6a). Man kann selbstkorrigierende Schaltungen entwickeln, die die Spannungen immer dort zentrieren – nur große Sprünge führen zu Fehlern. Fehler der Hardware werden in klassischen Computern daher nur in Hochsicherheitsanwendungen abgefangen (Fehlerkorrektur spielt aber eine große Rolle in der Kommunikation). Dieses Prinzip greift im Quantencomputer nicht – dort kommt es auf die nicht-digitalen Wahrscheinlichkeitsamplituden an (Abb. 6b).

Praktisch ist somit die Länge des Algorithmus durch die inverse Fehlerwahrscheinlichkeit begrenzt und daher nicht besonders groß. Ein in diesem Zusammenhang oft benutztes Schlagwort ist darum „Noisy Intermediate Scale Quantum technologies“ (NISQ) – in etwa „Fehlerbehaftete mittelgroße Quantentechnologien“.

- **Fehlertolerantes Quantencomputing**

Erfreulicherweise ist es unter bestimmten Voraussetzungen möglich, diese Fehler zu korrigieren. Die Methoden der Quantenfehlerkorrektur sind dabei eine Weiterentwicklung der Fehlerkorrektur klassischer Kommunikationssysteme. Grundidee ist das Vorhalten redundanter Information und die Lokalisierung von Fehlern durch Vergleich der verschiedenen Kopien dieser Information. Wenn Fehler selten genug und unkorreliert sind (d.h. unabhängig voneinander auftreten), lassen sie sich durch diesen Vergleich lokalisieren und korrigieren.

Die Gesetze der Quantenphysik erschweren diesen Zugang, er ist aber möglich. Die Schwierigkeit besteht in der Natur der Quantenmessung: Diese beeinflusst den Zustand und nimmt ihm gerade die Unsicherheit, die wir ja für den Quantenparallelismus nutzen wollen. Es wäre also falsch, während der Rechnung die redundanten Register immer mal wieder auszulesen und zu vergleichen, das würde die Quanteninformation

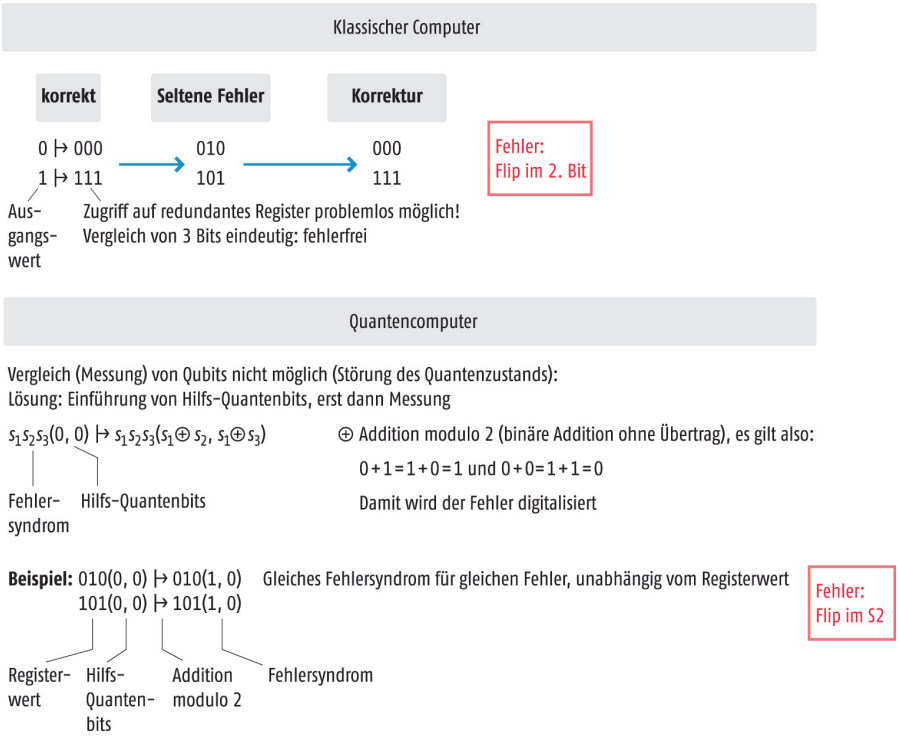

Abb. 7. Prinzip der Fehlerkorrektur durch Redundanz. Oben: Seltene Fehler können bei einem konventionellen Computer durch Vergleichsmessungen zwischen drei Bits lokalisiert werden. Unten: Bei einem Quantencomputer darf man nicht das Register auslesen (was die Quanteninformation zerstören würde). Um den Fehler zu lokalisieren, müssen Hilfs-Quantenbits eingeführt werden.

Kein Nachdruck, keine Veröffentlichung im Internet oder einem Intranet ohne Genehmigung des Verlags und der GDNÄ

©Wissenschaftliche Verlagsgesellschaft Stuttgart

Kein Nachdruck, keine Veröffentlichung im Internet oder einem Intranet ohne Genehmigung des Verlags und der GDNÄ

zerstören. Es ist aber möglich, nur die Information über den Fehler (und nicht den Wert des Registers) innerhalb des Quantencomputerprogramms auf ein Hilfs-Quantenbit zu schreiben, und dann dieses Hilfs-Quantenbit auszulesen – dies gibt dann Information über den Fehler, aber nicht über den Registerinhalt (Abb. 7). Damit wird aus der invasiven Messung während der Anwendung des Algorithmus sogar ein Vorteil: Während der Fehler vor der Messung analogen Charakter hat, z.B. in Form einer leichten Veränderung der Wahrscheinlichkeitsamplituden, ist er nach der Messung digitalisiert und damit deutlich einfacher weiter zu verarbeiten – der den Quantencomputer steuernde klassische Computer kann jetzt mit digitalen Operationen den Fehler beheben.

Die Problematik der Quantenfehlerkorrektur liegt darin, dass sie nur funktioniert, wenn der Hardwarefehler bereits klein ist – deutlich unter 1% Fehlerwahrscheinlichkeit. Und je größer die Fehlerwahrscheinlichkeit und je länger der fehlertolerant abzuarbeitende Algorithmus ist, desto mehr zusätzliche Bauelemente (Overhead) werden benötigt. Das bedeutet, dass für ein *logisches Qubit*, das in einem Algorithmus vorkommt, sehr viele (Hunderte bis Tausende) *physikalische Qubits* für Prüfzwecke benötigt werden, um die nötige Redundanz herzustellen und die Fehlersyndrome zu lokalisieren.

Dies macht das fehlertolerante Quantencomputing zu einem aufwendigen Fernziel. Nichtsdestotrotz wurden die Realisierbarkeit des Grundprinzips – Reduktion des Fehlers durch aktive Fehlerkorrektur – bereits experimentell bestätigt.

- **Adiabatisches Quantencomputing**

Das adiabatische Quantencomputing oder Quantenannealing ist ein alternativer Ansatz zum Gattermodell. Er ist darauf konzentriert, schwierige Optimierungsaufgaben zu lösen. Das Optimum einer Rechengröße wird in diesem Fall mit dem Minimum der Energie eines Quantensystems identifiziert, in dessen innerer Struktur die Optimierungsaufgabe angelegt ist. Wenn man Optima auf klassischem Weg finden möchte, gerät man bei komplexen Aufgaben sehr leicht in ein lokales Minimum, also in einen Zustand, der in einer abstrakt gefassten Umgebung optimal ist. Dies bedeutet, dass das Ändern weniger Bits die Energie immer weiter ansteigen lässt. Dennoch muss dieser Zustand nicht das Optimum sein – es kann viele Bitänderungen davon entfernt ein deutlich besseres Minimum geben.

Eine Analogie aus der klassischen Physik ist, dass ein System bei sehr tiefer Temperatur seinen Grundzustand einnimmt. Wenn man ein solches System einfach abkühlt (real oder simuliert), so kann es leicht in einem der erwähnten lokalen Minima gefangen werden. Durch aufwendiges Erwärmen und erneutes Kühlen kann man dies zwar vermeiden, doch erhöht dies den Zeitaufwand immens.

In einem adiabatischen Quantencomputer wird nun der Grundzustand durch quantenmechanische Überlagerungen geschützt. Statt der Anwendung einer schnellen Sequenz von Gattern wird er nur langsam verändert und ist (basierend auf dem adiabatischen Theorem der Quantenmechanik) in diesem Sinne adiabatisch. Er durchläuft eine Sequenz von Gleichgewichtszuständen – hier Grundzuständen –, jegliche Energieänderung kommt von einer äußeren Kraft.

Anders gesagt: Ähnlich wie Moleküle aufgrund quantenphysikalischer Effekte durch gemeinsame Elektronenorbitale zusammengehalten werden, können sich Datensätze zu einem „Datenmolekül“ verknüpfen, indem sie die programmierten logischen Verknüpfungen erfüllen und sind energetisch von den (im Sinn der Optimierung) schlechten Datensätzen abgesetzt. Es lässt sich zeigen, dass dieser Schutz es ermöglicht, den gesuchten Grundzustand aus dem Grundzustand eines einfacheren Problems zeitlich effizient zu entwickeln.

Rein mathematisch lässt sich beweisen, dass adiabatische Rechner genauso leistungsfähig sind wie gatterbasierte Rechner. Sie sind potentiell etwas einfacher zu bauen als diese, da sie keine schnelle komplexe Steuerung benötigen. Dieser Ansatz ist durch Aktivitäten einer kanadischen Firma berühmt geworden; gerade diese Produkte gerieten allerdings in Fachkreisen auch in Verruf. Denn die mit bis zu 2000 Qubits angebotenen adiabatischen Quantencomputer enthalten nur einen Teil der Zutaten, die man für eine echte Quantenbeschleunigung braucht. Ihr Anwendungspotential ist daher sehr fragwürdig, sollte aber nicht den adiabatischen Ansatz insgesamt entwerten.

- **Physikalische Realisierungen der Hardware**

Ansätze zur Realisierung von Hardware für Quantencomputer folgen grob zwei Grundphilosophien.

Quantenphysik ist die Physik kleiner Skalen, und quantenphysikalische Effekte wurden zuerst an Atomen und Photonen nachgewiesen. Es ist also naheliegend, Atome oder andere mikroskopische Systeme als Träger der Quanteninformation zu nutzen. Hier sind Quanteneffekte im Prinzip gut zugänglich. Die kleine Skala bedeutet eine große Herausforderung, diese Systeme tatsächlich zu skalierbaren und programmierbaren Quantenrechnern zusammenzusetzen. Der prominenteste und im Augenblick erfolgreichste Kandidat in diesem Bereich sind in elektrischen Feldern gefangene Ionen, die mit Lasern oder Mikrowellen gesteuert werden (Abb. 8). Diese Fallentechnologie ermöglicht die Realisierung von Quantencomputern mit 20 und mehr Qubits bereits heute und macht den Meilenstein von 50 Qubits greifbar (vgl. Vortrag Blatt). Das wäre dann ein NISQ-Computer mit Quantenüberlegenheit.

Der komplementäre Ansatz startet mit skalierbarer Technologie und integrierten Schaltkreisen und versucht, diese durch Miniaturisierung und sorgfältige Gestaltung zu Quantenobjekten mit geringer Fehlerrate zu machen (Abb. 9). Gewöhnliche Halbleitertransistoren sind bereits so klein, dass man im

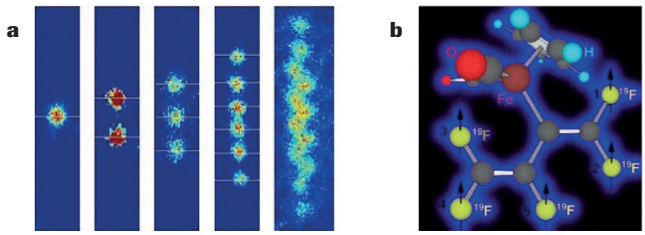

Abb. 8. Beispiele mikroskopischer bzw. atomarer Plattformen für Quantencomputing: **– a.** Ketten gefangener Ionen leuchten im Laserfeld auf. **– b.** Die Spins von Atomkernen können als natürliche Qubits verwendet werden.

©Wissenschaftliche Verlagsgesellschaft Stuttgart

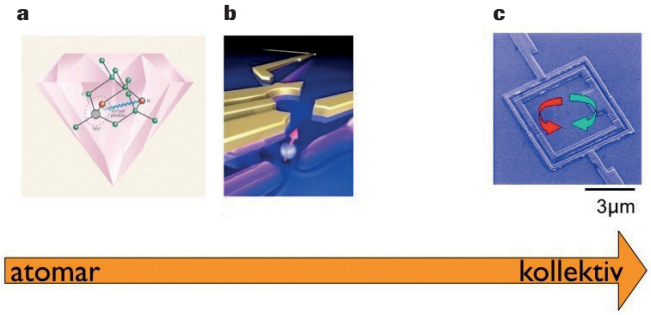

Abb. 9. Beispiele von Festkörper-Qubits: **– a.** Fehlstellen in Diamanten, **– b.** einzelne Elektronen in Halbleiter-Quantenpunkten, **– c.** Stromzustände in supraleitenden Schaltkreisen.

Schaltkreisdesign von klassischen Computern darauf achten muss, die dann unerwünschten Quanteneffekte zu vermeiden. In den letzten Jahren ist es dennoch gelungen, erste Prototypen von Qubits aus Silicium zu realisieren.

Der im Augenblick wesentlich weiter entwickelte Ansatz für Quantencomputer als integrierte Schaltkreise kann durch den Einsatz von Supraleitern erreicht werden. Hierbei nutzt man die Tatsache, dass Supraleitung – die Eigenschaft mancher Materialien, den elektrischen Strom bei tiefen Temperaturen verlustfrei zu leiten und das Magnetfeld perfekt zu verdrängen – selbst ein makroskopischer Quanteneffekt ist. Ein in der Metrologie etabliertes System sind die supraleitenden Josephson-Kontakte. Sie haben eine handhabbare Größe und gute Quanteneigenschaften. Auch mit ihnen wurden Rechner mit 20 Qubits realisiert, und man ist dabei, solche mit mehr als 50 Qubits zu bauen.

Beiden Plattformen ist gemein, dass sie metrologische Technologien anwenden, die bereits zur genauen Definition von Standards und Messungen genutzt werden. Bei der Ionenfalle ist es die Atomuhr und bei Josephson-Kontakten der Spannungsstandard. Dies ist kein Zufall, denn wie oben ausgeführt hat Quantencomputing hohe Genauigkeitsanforderungen, genau wie die Metrologie.

Auch wenn die beiden genannten Plattformen im Augenblick führend sind und sich untereinander wenig nehmen – je nach Parametersatz und Priorität kann mal die eine oder andere vorne sein – ist die Suche nach dem endgültigen Kandidaten noch lange nicht abgeschlossen. Die Lektüre dieser Zeilen mag in einigen Jahrzehnten merkwürdig antiquiert wirken, wie die früheren Diskussionen über die Entscheidung zwischen Relais und Röhren bei klassischen Computern.

Status 2018/19

Wo stehen wir? Die Erfolge des Quantencomputing und die insgesamt gute Entwicklung haben ein großes Interesse hervorgerufen. Große Forschungsprogramme werden weltweit aufgelegt, darunter das milliardenschwere Quantentechnologie-Flaggschiffprogramm der Europäischen Union. Auf industrieller Seite steigen IT-Firmen ein, und immer mehr potentielle Nutzer analysieren, bei welchem Entwicklungsstand sich der Einsatz von Quantencomputern lohnt.

Besonders wichtig ist die Möglichkeit, Quantencomputer bereits heute über Cloud-Dienste kennenzulernen und zu nutzen, wobei es sich sowohl um simulierte Quantencomputer als auch um einfache Prototypen handelt. Hierdurch ergibt sich ein völlig neuer Zugang zu den Konzepten der Quantenphysik, der zu einer größeren Vertrautheit und zu einem Verständnis der Quantentheorie beiträgt.

Dieser Nebeneffekt ist nicht zu unterschätzen, denn technologische Quantenrevolution braucht Wissen auf vielen Ebenen: Quanteningenieurinnen und -ingenieure, die die Quantenmaschinen der Zukunft bauen können und neben einem Verständnis der Physik auch ein Verständnis der Technologie mitbringen, aber auch eine Öffentlichkeit, die mit den Möglichkeiten der Quantenphysik verantwortungsbewusst und informiert umgeht.

Literaturhinweise

- Bundesamt für Sicherheit in der Informationstechnik: Entwicklungsstand Quantencomputer. Deutsche Zusammenfassung. BSI Projektnummer 283. Bonn 2018.
- N. David Mermin: Quantum Computer Science: An Introduction. Cambridge University Press. Cambridge 2007.
- A. Acin, I. Bloch, H. Buhrman et al.: The European Quantum Technologies Roadmap. New J. Phys. **20** (2018) 080201 [https://arxiv.org/ftp/arxiv/papers/1712/1712.03773.pdf]

Prof. Dr. **Frank Wilhelm-Mauch**, Jahrgang 1971, studierte in Karlsruhe Physik und promovierte dort über die Theorie supraleitender Nanostrukturen. Er war Stipendiat der Studienstiftung des deutschen Volkes. 1999 bis 2001 ging er als Postdoktorand an die TU Delft. Dort arbeitete er in der Frühzeit des Quantencomputing als Theoretiker in einer experimentellen Arbeitsgruppe. 2001wechselte er als wissenschaftlicher Assistent an die LMU München, wo er sich 2004 habilitierte und zum Privatdozenten ernannt wurde. Dort war er an der Gründung eines frühen Sonderforschungsbereichs im Gebiet Quantencomputing beteiligt. 2006 wurde Wilhelm-Mauch Associate Professor am Institute for Quantum Computing und dem Department of Physics and Astronomy an der University of Waterloo in Kanada. In diesem interdisziplinären Umfeld etablierte er ein Forschungsprofil, das die verschiedenen Ebenen des Quantencomputing, Hard- und Software, Einzelstrukturen und Systeme sowie Physik und Anwendungen miteinander verknüpft. Von dort folgte er 2011 einem Ruf auf eine W3-Professur an die Universität des Saarlandes. Er war Generalsekretär der virtuellen Einrichtung für Quantenkontrolle über ihre gesamte Existenz und engagiert sich an vielen Stellen beim Aufbau des europäischen Flaggschiffprogramms für Quantencomputing. Er berät in Fragen seines Arbeitsgebiets Unternehmen, Behörden und die Öffentlichkeit.

Universität des Saarlandes, Fachrichtung Physik, Campus E2.6, 66123 Saarbrücken

Kein Nachdruck, keine Veröffentlichung im Internet oder einem Intranet ohne Genehmigung des Verlags und der GDNÄ

©Wissenschaftliche Verlagsgesellschaft Stuttgart