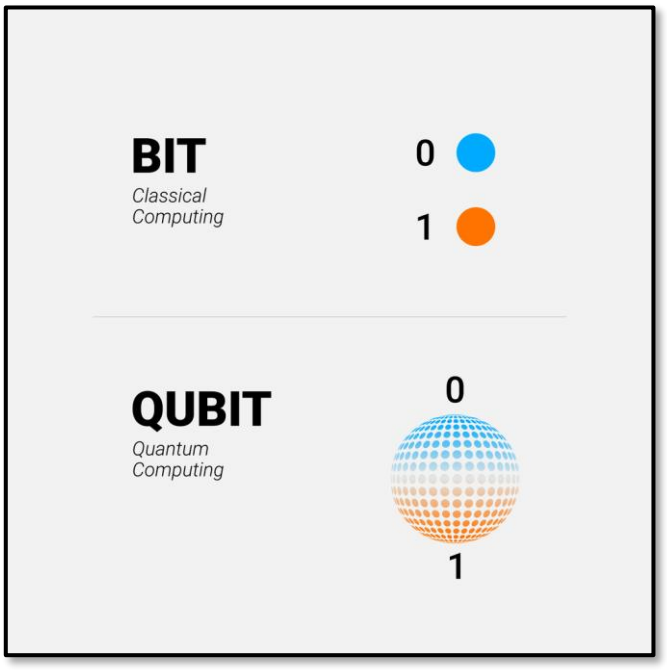
Quantencomputer

Technologie, Anwendungen und Anlagepotential



EXPOSE

Ein universell einsatzbarer Quantencomputer vermag Probleme in vielen Bereichen zu lösen, die bisher selbst mit einem Supercomputer nicht in endlicher Zeit gelöst werden können. Anwendungsbeispiele finden sich besonders in der Logistik und der Entwicklung von Medikamenten. Auch die Simulation von besseren Werkstoffen, beispielsweise bei der Batterieforschung. Technische Hürden bei der Entwicklung des Quantencomputers werden abgebaut, aber es gibt noch viele Herausforderungen, auch bei der Software, die speziell für den Quantencomputer entwickelt werden muss.

Von: Jürgen Brückner
FV Frankfurter Vermögen AG

Inhalt

Motivation und Einsatz des Quantencomputers

Der Quantencomputer findet abseits der Spezialliteratur seit kurzer Zeit auch in den Medien breite Erwähnung, da es technologische Erfolge gab und einer breiteren Öffentlichkeit zunehmend bewusst wird, dass der Quantencomputer bisher unlösbare Probleme zu lösen vermag.

Trotz des Fortschritts der Rechenleistung der heutigen Generation von Computern und sogar des Einsatzes von sehr leistungsfähigen Supercomputern oder sogar des Zusammenschlusses mehrerer Supercomputer gibt es eine Vielzahl von Aufgaben, die auch mit den besten Computern der Welt nicht in einer endlichen Zeit gelöst werden können. Hierbei handelt es sich keineswegs um Probleme, die nur Wissenschaftlern vorbehalten sind, sondern um praktische Anwendungen beispielsweise in der Medizin und der Logistik. Beim Quantencomputer handelt es sich um einen völlig anderen technologischen Ansatz als den herkömmlichen Computern, da er auf die Grundlagen der Quantenphysik zurückgreift. Die Quantenphysik selbst war zunächst lange Zeit umstritten, da sich ihre Ergebnisse der Intuition widersetzen. Nachdem jedoch die Quantenphysik als Erklärung wichtiger Phänomene der Welt anerkannt wurde und auch viele Produkte auf ihnen beruhen, richtete sich das Augenmerk auf eine revolutionäre Anwendung im Bereich des Computers.

Dieser Text richtet sich an Leser, die sich neben den Anwendungen auch in einem überschaubaren Rahmen mit den mathematischen und technologischen Grundlagen des Quantencomputers vertraut machen wollen. Er dient damit auch als Hilfestellung für einen tieferen Einstieg in einige der Besonderheiten des Quantencomputers. Ein tiefergehendes Verständnis dieser Grundlagen hilft bei der Einschätzung der Schwierigkeiten und zukünftigen Anwendungen. Dabei wird vor allem erläutert, wie im Quantencomputer die quantenmechanischen Eigenschaften der Materie genutzt werden:

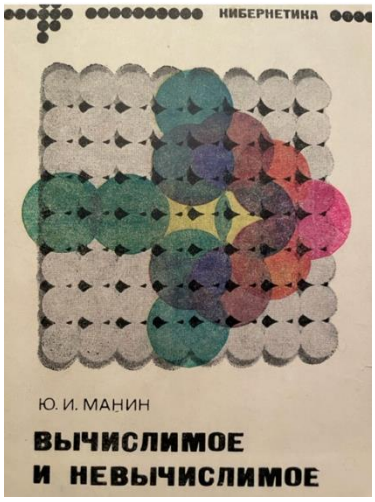
- Überlagerung (Superposition)
- Verschränkung
- Interferenz

Hilfreich für das Verständnis ist auch ein kleiner Abriss der historischen Entwicklung.

Wie kam es zur Entwicklung des Quantencomputers?

Die erste Erwähnung der Notwendigkeit der Entwicklung eines Quantencomputers wird allgemein auf den amerikanischen Nobelpreisträger Richard P. Feynman zurückgeführt, der 1982 in einer Fachzeitschrift mit dem Titel „Simulating Physics with Computers“ das folgende bekannte Zitat machte: “Nature isn't classical, dammit, and if you want to make a simulation of Nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy“. Kaum bekannt ist jedoch, dass bereits zwei Jahre zuvor der russische Mathematiker Yuri Manin in einem wissenschaftlichen Werk auf die Notwendigkeit der Entwicklung eines Quantencomputers hingewiesen hatte (s. Bild unten des Buchumschlags). In diesem Werk weist der Mathematiker genau auf den entscheidenden Vorteil

des Quantencomputers hin, nämlich die Möglichkeit 2^n Zustände in einem



Quantencomputer mit n Teilchen darzustellen.

Nachdem inzwischen fast genau 40 Jahre nach Erscheinen des Werks von Manin[1] vergangen sind, wird deutlich, dass die Entwicklung des Quantencomputers mit enormen Schwierigkeiten verbunden ist, denn erst 2019 konnte ein Durchbruch bei einer Rechnung mit einem Quantencomputer verzeichnet werden. Google berichtete, dass mit einem Quantencomputer erstmals eine Rechnung wesentlich schneller als mit einem Supercomputer durchgeführt werden konnte. Dieses Ergebnis macht deutlich, dass der Quantencomputer für die Menschheit von überragender Bedeutung sein wird. Anwendungen werden vor allem in der Klimaforschung, der Logistik, der Material- und Medikamentenentwicklung und der Verkehrslenkung stattfinden. Auch in der Kryptographie wird der Quantencomputer ein Umdenken erfordern. [2]Ob der Quantencomputer auch das Ende der Kryptowährungen einleiten wird, ist unter Experten umstritten.

Nachdem Google mit der Entwicklung eines 53 Qubit Quantencomputer einen wichtigen Meilenstein setzte, erwarten Experten frühestens zur Mitte des Jahrzehnts deutliche Erfolge bei der kommerziellen Anwendung. Zwar sind die USA und Kanada führend bei der Entwicklung des Quantencomputers, aber Europa ist bei einem anderen technologischen Ansatz (den sogenannten Ionenfallen) führend. Ionenfallen sind im Gegensatz zu der auf Supraleitung beruhenden Technologie der USA weniger leistungsstark, liefern aber dafür sicherere Ergebnisse.

Anwendungsbereiche und potenzielle Märkte

Der Einsatz des Quantencomputers eignet sich insbesondere für diejenigen Gebiete, wo eine sehr hohe Rechenleistung gefragt ist. Hierzu eine Auswahl möglicher Anwendungsbereiche:

- Kryptografie
- Chemie
- Materialwissenschaft
- KI
- Optimierung
- Simulation

[1] Prof. Dr. Yuri Ivanovich Manin ist emeritierter Professor an der Universität Bonn

[2] Seit der Publikation von Shors Algorithmus (1994) existieren Quantenalgorithmen zur Faktorisierung (Primfaktorzerlegung) von sogenannten RSA-Moduln, die die Grundlage der heutigen Verschlüsselungstechnik bilden. Während konventionelle Rechner für die Faktorisierung von RSA-Moduln eine lange Zeit bräuchten, könnte ein Quantencomputer diese Faktorisierung in Sekundenschnelle vornehmen. Die NSA arbeitet daher bereits seit 2015 an der Entwicklung von Quantencomputer-resistenten Verfahren.

Von der Vielzahl der Anwendungsbereiche seien im Folgenden nur einige Beispiele genannt. Kommerzielle Anwendungen stehen noch am Anfang, aber die Entwicklung schreitet schnell fort. Für die Menschheit von großem Nutzen wird insbesondere die Möglichkeit sein, die chemischen und biologischen Strukturen von Molekülen zu simulieren, um schneller wirksame Medikamente zu entwickeln. Quantencomputer können in diesem Zusammenhang genutzt werden, um die Wechselwirkungen von Molekülen mit potenziellen Therapeutika schnell und präzise zu simulieren. Dies kann dabei helfen, bessere Medikamente zu entwickeln, indem es möglich ist, die Wirksamkeit und die möglichen Nebenwirkungen von Medikamenten in einer virtuellen Umgebung zu testen, bevor sie an lebenden Organismen oder Menschen getestet werden müssen.

In der Chemie können Quantencomputer bei der Simulation komplexer chemischer Reaktionen und Prozesse verwendet werden, um zu einem besseren Verständnis der chemischen Grundlagen von Materialien zu gelangen. Im Bereich der Materialwissenschaft nutzen beispielsweise Mercedes-Benz (Partner IBM Quantum) und Hyundai (Partner IonQ) schon jetzt den Quantencomputer, um in der Batterieforschung die enorme Anzahl von Wechselwirkungen der Elektronen in einer Batterie auf Molekülebene und die chemischen Reaktionen zu simulieren.

In der Logistik gibt es eine Reihe von sehr rechenintensiven Optimierungsverfahren, wo der Quantencomputer ebenfalls sinnvoll eingesetzt werden kann. Die Komplexität optimale Routen für Lieferungen zu finden ist gut dokumentiert durch das sogenannte „Travelling Salesman Problem (TSP)“, wobei es darum geht, eine optimale Tour durch eine gegebene Anzahl von Städten zu finden, bei der jede Stadt genau einmal besucht wird und man am Ende wieder zur Ausgangsstadt zurückkehrt. Bei nur 15 Städten gibt es mehr als 43 Mrd. mögliche Wege, die durchlaufen werden müssen, um den optimalen Weg zu finden.

Das TSP ist ein sogenanntes NP-vollständiges[3] Problem, was bedeutet, dass es für große Probleme keine bekannte effiziente Lösung gibt. Trotzdem ist es ein wichtiges Problem, das in einer Reihe von Anwendungsbereichen relevant ist, einschließlich Logistik, Transportwesen, Produktion und Planung von Routen für Lastwagen, Flugzeuge oder andere Fahrzeuge.

Quantencomputer können auch in der Finanzindustrie eingesetzt werden, insbesondere bei Verfahren, die auf Simulationen basieren. Ein Beispiel dafür ist die Generierung von Zufallszahlen. Mit herkömmlichen Methoden ist es unmöglich, beliebig viele Zufallszahlen zu generieren. Der Zufall ist jedoch das Wesen des Quantencomputers. Durch die Verwendung von Qubits können Quantencomputer eine größere Anzahl von Zufallszahlen generieren als herkömmliche Computer, was für bestimmte Anwendungen in der Finanzindustrie von großem Nutzen sein kann. Da die Wirkungsweise des Quantencomputers auf Quanteneffekten beruht ist es

[3] Ein NP-vollständiges Problem ist ein Problem in der Informatik, das schwierig zu lösen ist. Es bedeutet, dass es sehr lange dauern kann, eine Lösung für dieses Problem zu finden. Außerdem gibt es keine bekannte Methode, die das Problem effizient lösen kann.

folgerichtig den Quantencomputer auch bei der Simulation von quantenphysikalischen Systemen einzusetzen um z.B. Phänomene wie Supraleitung besser zu verstehen. Hier schließt sich auch der Kreis zu Feynman, der genau diese Aufgabe zur Erklärung von Naturphänomenen in seinem eingangs erwähnten Text fordert.

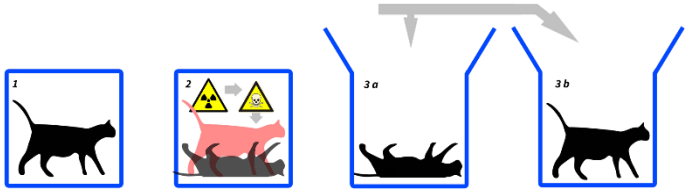
Ein Quantencomputer spielt auch eine zentrale Rolle in einem zukünftigen Quantennetz. In einem solchen Netzwerk kommunizieren Geräte miteinander durch Übertragung von quantenphysikalischen Zuständen wie Polarisation oder Spin. Der Quantencomputer ist besonders wichtig in einem Quantennetz, da er kryptographische Schlüssel generieren und verwalten kann, die für eine sichere Übertragung von Informationen im Netzwerk notwendig sind.

Die Grundlage eines Quantennetzes ist das später im Text beschriebene Phänomen der Verschränkung, welches auch eine zentrale Bedeutung für die Teleportation bildet. Der Begriff der Teleportation ist bekannt durch Science Fiction, aber im Gegensatz zum dort bekannten Phänomen der Teleportation von realen Gegenständen werden in der Quantenmechanik nur quanten-physikalische Zustände - keine realen Teilchen - zwischen entfernten Geräten übertragen. Der österreichische Physiker Zeilinger erhielt im vergangenen Jahr den Nobelpreis für Physik für grundlegende Arbeiten im Zusammenhang mit praktischen Aspekten der Teleportation, insbesondere für seine Entdeckung des "entanglement swapping", welches die Übertragung von Quantenzuständen über weite Entfernungen ermöglicht.

Wie funktioniert ein Quantencomputer?

Worin liegen die technologischen Schwierigkeiten bei der Entwicklung des Quantencomputers? Immerhin sind seit seiner erstmaligen Erwähnung mehr als vier Jahrzehnte vergangen und die Notwendigkeit eines Quantencomputers für die Simulation bestimmter Prozesse wurde bereits damals eindrücklich formuliert. Um die Herausforderungen des Baus eines Quantencomputers zu verstehen ist es notwendig, die Grundlagen der Funktionsweise eines Quantencomputers zu verstehen. Für ein tieferes Verständnis muss man sich idealerweise mit den Besonderheiten der Quantenmathematik beschäftigen, denn der Quantencomputer stellt nicht nur die Ingenieure vor besondere Herausforderungen, sondern auch die Mathematiker. Eine sinnvolle Anwendung eines Quantencomputers ist in der Tat nur möglich, wenn ebenfalls anwendungsrelevante Quantenalgorithmen entwickelt bzw. entdeckt werden. Quantenalgorithmen sind Algorithmen, die die Eigenschaften von Quantensystemen nutzen, um bestimmte Aufgaben schneller und effizienter zu lösen als herkömmliche Computer. Ohne die Entwicklung besonderer Quantenalgorithmen zur Lösung spezifischer Probleme wäre allein die technische Umsetzung des Quantencomputers nur von geringem Nutzen.
Worin liegt die Besonderheit und was sind die Voraussetzungen des Quantencomputers, um eine dramatische Erhöhung der Rechenzeit zu ermöglichen? Ganz generell kann man sagen, dass ein Quantencomputer bestimmte Eigenschaften der Quantenmechanik nutzt. Die Gesetze der Quantenmechanik selbst sind

oftmals schwer zu vermitteln, da sie nicht intuitiv sind und unseren Alltagserwartungen zuwiderlaufen. Eines der wichtigsten Merkmale der Quantenwelt ist die Möglichkeit, dass ein Teilchen gleichzeitig zwei Zustände einnehmen kann oder auch gleichzeitig an zwei verschiedenen Orten vorhanden sein kann. Ein gutes Beispiel zur Veranschaulichung des Konzepts der Quantenphysik ist das berühmte Beispiel von Schrödingers Katze. Das Gedankenexperiment von Schrödingers Katze geht auf den österreichischen Physiker und Nobelpreisträger Erwin Schrödinger zurück, der es 1935 beschrieb.



Bei Schrödingers Katze geht es um eine Katze, die in einem geschlossenen Behälter eingeschlossen ist. In dem Behälter befindet sich auch eine Substanz, die tödlich ist, wenn sie freigesetzt wird. Ein Zufallsgenerator entscheidet, ob die Substanz freigesetzt wird oder nicht.

Solange niemand nachschaut, ob die Substanz freigesetzt wurde oder nicht, befindet sich die Katze in einem Zustand der Unschärfe, in dem sie sowohl tot als auch lebendig sein kann. Dies ist ein wichtiger Aspekt der Quantenphysik, bei dem ein Objekt mehrere mögliche Zustände hat, bis es beobachtet wird. Mit seinem Gedankenexperiment schlägt Schrödinger auch die Brücke von den Elementarteilchen zur Makrowelt, denn man kann das Experiment so konstruieren, dass die tödliche Substanz durch einen Mechanismus freigesetzt wird, der den Gesetzen der Quantenmechanik gehorcht, z.B. ein radioaktives Präparat, welches mit einer bestimmten Wahrscheinlichkeit zufällig freigesetzt wird. Das Experiment verdeutlicht außerdem, dass in der Quantenwelt die Realität erst durch die Beobachtung definiert wird.

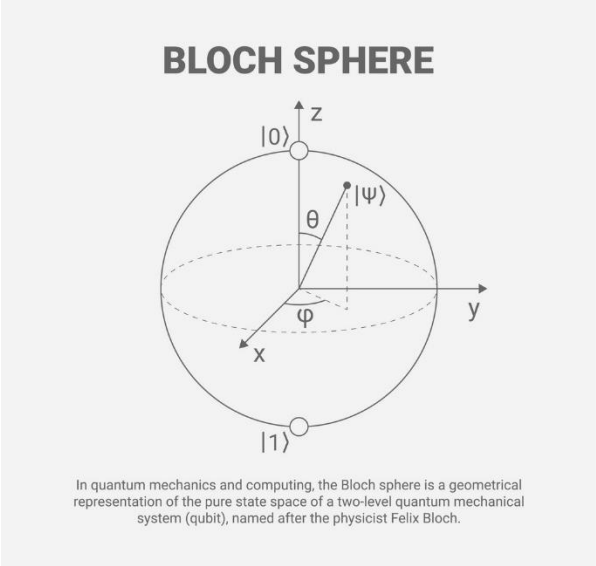
Was hat nun Schrödingers Katze mit dem Quantencomputer zu tun? Das Gedankenexperiment veranschaulicht die Überlagerung von zwei Zuständen, die zugleich auftreten. Wie Schrödingers Katze, die zugleich tot als auch lebendig sein kann, kann ein Quantenbit (abgekürzt Qubit) in einem Computer zugleich die Zustände 0 und 1 einnehmen, in quantenmechanischer Terminologie mit $|0\rangle$ und $|1\rangle$ bezeichnet. Bei einem klassischen Computer nimmt der Computer entweder 0 oder 1 ein. In quantenmechanischer Terminologie beschreibt man die Überlagerung der Zustände in einem Qubit mit einer Formel, die den Zustand mit der Wahrscheinlichkeit für das Auftreten eines Zustands verknüpft:

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle$$

Wesentlich ist, dass a und b, oft auch als Amplituden bezeichnet, komplexe Zahlen sind. Die Wahrscheinlichkeit wird nicht durch die Amplitude, sondern durch das Quadrat der Amplitude bestimmt. Sie gibt an, mit welcher Wahrscheinlichkeit das Qubit nach einer Messung im Zustand $|0\rangle$ oder $|1\rangle$ gefunden wird (s. für eine nähere Erklärung der Wahrscheinlichkeit auch den Anhang).

Physikalisch können die Zustände in einem Quantencomputer beispielsweise durch die niedrigste und höchste Energieebene eines elektronischen Systems oder die beiden

Polarisationen eines Photons repräsentiert werden. Der Quantencomputer macht sich genau diese Eigenschaft des Qubits zunutze, dass Qubits eine Überlagerung von zwei Zuständen aufzuweisen können. Welcher von zwei möglichen Zuständen eintritt wird erst bei Beobachtung bzw. Messung bekannt. Die Wahrscheinlichkeit für das Eintreten eines Zustands muss nicht notwendigerweise 50% sein, sondern kann jede beliebige Zahl annehmen, die jedoch vorher nicht bestimmbar ist. Durch die Möglichkeit beliebiger Kombinationen von Wahrscheinlichkeiten (die sich immer zu eins addieren müssen) ergibt sich eine Vielzahl von möglichen Zuständen. Diese Möglichkeit der Vielzahl von Zuständen kann man sich am besten anhand der Bloch-Kugel veranschaulichen (s. Grafik). Bevor wir auf die Bloch-Kugel kurz eingehen, wollen wir uns jedoch vergegenwärtigen, wie es möglich ist, dass eine Linearkombination von zwei Zahlen zu einer Beschreibung im Raum führen kann. Handelte es sich bei den Amplituden nur um reelle Zahlen, so könnten wir die Zustände des Qubits nur in der Ebene darstellen und wir hätten einen sehr viel kleineren Rechenraum. Tatsächlich sind die Amplituden (deren Quadrat die Wahrscheinlichkeit ist) jedoch komplexe Zahlen. Der Verdienst des Nobelpreisträgers Felix Bloch (nach dem die Kugel benannt ist) liegt darin, dass er einen Weg fand, durch eine mathematische Umformung das Qubit nicht als Linearkombination von zwei komplexen Zahlen zu schreiben, sondern von zwei Winkeln, ein Winkel, der die Bewegung in der Ebene beschreibt und ein Winkel, der die Bewegung im Raum beschreibt. Auf



diese Weise ist eine räumliche Ansicht möglich und ein Qubit kann durch einen Punkt auf einer Kugeloberfläche repräsentiert werden. Ein Qubit, das den Zustand Null hat, wird durch den Nordpol der Kugel dargestellt und ein Qubit, das den Zustand Eins hat, wird durch den Südpol dargestellt. Jeder Punkt auf der Kugeloberfläche kann als ein überlagerter Zustand aus Null und Eins interpretiert werden.

In der Bloch-Kugel kann also durch unterschiedliche Kombinationen von Null und Eins jeder Punkt auf der Oberfläche der Kugel erreicht werden. Hierdurch wird die enorme Vielfalt der möglichen Zustände eines Qubits und der ungeheuer große Rechenraum veranschaulicht. Die Bloch-Kugel eignet sich auch zur Veranschaulichung der Wirkung eines Quantengatters[4] auf ein Qubit: Die Änderung der Zustände eines Qubits wird in der Quantenmechanik durch sogenannte Quantengatter realisiert, die auf der Bloch-Kugel als Bewegung des Punktes von einem Ort auf der Kugel zu einem anderen Ort dargestellt werden.

[4] Ein Quantengatter ist eine Schaltung, die ähnlich wie ein logisches Gatter in einem klassischen Computer logische Operationen ermöglicht, wie zum Beispiel die Addition.

Der enorme Geschwindigkeitsvorteil gegenüber klassischen Computern ergibt sich u.a. daraus, dass der Computer gleichzeitig nicht nur auf n Qubits zurückgreifen kann, sondern gleichzeitig auf 2^n mögliche Zustände des Qubits. Jedes Qubit kann sich zur selben Zeit in einem Zustand von Null und Eins befinden, was bedeutet, dass ein n-Qubit-Quantencomputer in der Lage ist, 2^n Zustände gleichzeitig zu verarbeiten und mit ihnen gleichzeitig rechnen kann. Man kann sich das ungefähr verdeutlichen am Beispiel einer Münze, die in die Luft geworfen wird und die, solange sie sich in der Luft befindet, ebenfalls gleichzeitig zwei Zustände aufweist: Kopf und Zahl.

Stellen Sie sich also vor, Sie werfen eine Münze in die Luft und beobachten, ob sie auf Kopf oder Zahl landet. Mit einer klassischen Computerperspektive könnte man sagen, dass die Münze entweder auf Kopf oder Zahl landen wird, aber nicht beides gleichzeitig. Aus einer Quantencomputerperspektive kann man jedoch sagen, dass die Münze gleichzeitig in beiden Zuständen, also Kopf und Zahl, existieren kann, bis man sie beobachtet und durch die Beobachtung der Zustand kollabiert. Entscheidend ist, dass eine Rechnung nur solange stattfinden kann, wie die Überlagerung der Zustände anhält (um bei dem Münzbeispiel zu bleiben also solange wie sich die Münzen in der Luft befinden). Für die Verdeutlichung des parallelen Zugriffs auf 2^n Zustände kann man das Münzbeispiel auf eine größere Anzahl von Münzen ausdehnen:

Wenn man beispielsweise zwei Münzen gleichzeitig wirft, gibt es 4 mögliche Kombinationen: Kopf-Kopf, Kopf-Zahl, Zahl-Kopf, Zahl-Zahl. In einem klassischen Computer müsste man diese 4 Kombinationen nacheinander berechnen, was Zeit benötigt. In einem Quantencomputer hingegen kann man auf die 4 Kombinationen gleichzeitig einwirken. Dies ermöglicht eine signifikante Beschleunigung der Berechnungen, da der Quantencomputer parallel auf alle 2^n Zustände zugreifen kann und mit ihnen rechnen kann. Da der gleichzeitige Zugriff auf 2^n Zustände einer der Gründe für den Geschwindigkeitsvorteil ist, stellt sich natürlich die Frage, wie es überhaupt möglich ist, parallel auf Zustände einzuwirken, die sich in einer Überlagerung befinden und nicht direkt beobachtbar sind. Man kann sich das etwa so vorstellen, dass eine quantenmechanische Operation (Anwendung eines Quantengatters) die Überlagerung verändert, so dass die Wahrscheinlichkeit, dass das erste Qubit "0" ist, gesteigert wird, während die Wahrscheinlichkeit, dass das zweite Qubit "1" ist, gesenkt wird. Es ist wichtig zu beachten, dass die Anwendung eines Quantengatters keine Messung darstellt, bei der bereits einer der möglichen Zustände ausgewählt wird, sondern das Zugreifen auf die Qubits findet während der Überlagerung statt (bildlich auf das Münzbeispiel übertragen: während die Münze in der Luft ist). Eine der Kennzahlen von Quantencomputern ist daher auch die Zeit, die vergeht, bis die Zustände kollabieren (in der Fachsprache „dekohärieren“ genannt). Diese quantenmechanische Operation (eines oder mehrerer Quantengatter) kann parallel auf mehrere Qubits während der Überlagerung einwirken. Technisch kann die quantenmechanische Operation über verschiedene Arten erfolgen: In Quantensystemen, die auf elektrischen Ladungen basieren, kann sie beispielsweise durch die Verwendung von elektrischen Puls-Sequenzen implementiert werden. Hier werden spezifische Muster von elektrischen

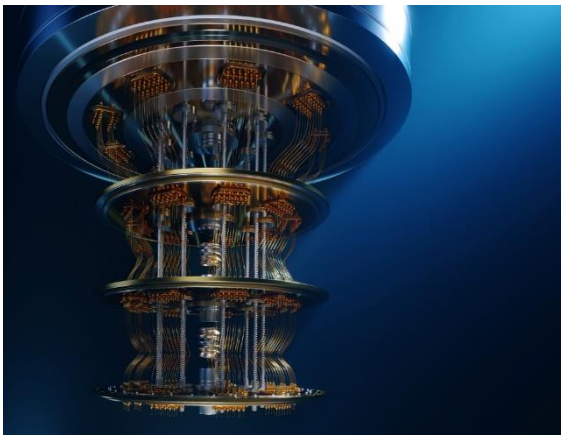
Pulsen auf die Ladungen angewendet, um ihre Zustände zu ändern.

Da die Anzahl der möglichen Informationen, die ein Quantencomputer speichern bzw. berechnen kann sich mit 2^n bestimmt, verdoppelt sich mit jedem weiteren Qubit die Menge. Der eingangs beschriebene Quantencomputer von Google mit 53 Qubits kann daher potentiell 2^53 = 9.007.199.254.740.990 Informationen verarbeiten bzw. Daten speichern. Eines der Probleme der Hinzufügung neuer Qubits besteht darin, dass bei steigender Anzahl die Fehlerhäufigkeit zunimmt, was ein wichtiger Faktor bei der Skalierbarkeit von Quantensystemen ist und spezielle Verfahren zur Reduzierung vorgenommen werden müssen. Um diese Fehler zu reduzieren, werden verschiedene Verfahren eingesetzt, wie z.B. Fehlerkorrekturcodes oder Technologien zur Steigerung der Stabilität von Qubits.

Eine weitere Besonderheit von Quantensystemen wird mit dem Begriff „Verschränkung“ (engl. Entanglement), bezeichnet, der in Quantensystemen mit mehr als einem Qubit eine besondere Wirkung entfaltet. In der Tat resultiert der Geschwindigkeitsvorteil des Quantencomputers nicht nur aus der Überlagerung, sondern auch aus der Verschränkung. Das Phänomen der Verschränkung beschreibt eine Verknüpfung bzw. Wechselwirkung von Teilchen, die in Quantensystemen auftaucht, die aber nicht in klassischen Systemen möglich ist. Wären die 2^n möglichen Quantenzustände losgelöst und unabhängig voneinander, so könnte man mit ihnen nicht rechnen, denn zur Verarbeitung der enormen Fülle von Informationen reicht es nicht aus, sie nur zu repräsentieren, sondern sie müssen miteinander verschränkt sein.

Das Phänomen der Verschränkung wurde zuerst von Schrödinger nachgewiesen und beschrieben. Schrödinger erkannte bereits 1935, dass das Phänomen der Verschränkung eine vollkommen neue Betrachtungsweise der Welt erfordert und als *das* Charakteristikum der Quantenmechanik angesehen werden kann. In seinen Worten: *„I would not call that one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought.“*

Ganz allgemein geht es bei der Verschränkung darum, dass die Quantenzustände von zwei Partikeln, die getrennt wurden, nicht unabhängig voneinander beschrieben werden können. In der Quantenmechanik entsteht eine Verschränkung zweier Elementarteilchen z.B. dann, wenn sie getrennt werden, so wie bei einem radioaktiven Zerfall oder nach einer Kollision zweier Partikel.



Der "Kronleuchter" in einem Quantencomputer soll seinen Verarbeitungschip auf eine Temperatur kühlen, die niedriger ist als -270°C.

Die Verschränkung ermöglicht es, dass die Zustände von mehreren Qubits miteinander verknüpft sind, was bedeutet, dass eine Zustandsänderung

in einem Qubit unmittelbar Auswirkungen auf die Zustände anderer Qubits hat, vollkommen unabhängig davon, wie weit diese Qubits voneinander entfernt sind. Dies macht es möglich, gleichzeitig mit allen möglichen Zuständen eines Systems aus mehreren Qubits zu arbeiten, was neben der Überlagerung ebenfalls zu einem enormen Geschwindigkeitsvorteil gegenüber klassischen Computern führt. Das Prinzip der Verschränkung bildet auch die Grundlage für wichtige Quantenalgorithmen.

Aktueller Stand der verschiedenen Technologien des Quantencomputers

Worin liegen nun aber die technologischen Schwierigkeiten des Quantencomputers und warum hat die Entwicklung seit der erstmaligen Erwähnung vor rund 40 Jahren so lange gedauert? Das Hauptproblem liegt darin, dass Qubits im Überlagerungszustand nur eine sehr geringe Lebensdauer haben und sehr schnell dekohärieren (kollabieren), wie es in der Fachsprache genannt wird, d.h. ein Qubit im Überlagerungszustand „0“ oder „1“ fällt in einen der beiden Grundzustände „0“ oder „1“ zurück, wenn auch nur der geringste Umwelteinfluss auf es einwirkt. Um diese Umwelteinflüsse weitgehend auszuschalten, setzt die erste Generation der Quantencomputer (so auch Sycomore von Google) darauf, die Qubits mittels Supraleitung[5] nahe dem absoluten Nullpunkt zu kühlen.

Eine anderer Ansatz beruht auf einer Technologie, die unter dem Namen

Technologie	Unternehmen	Land
Supraleitung Quantum Annealer	D-Wave	
Photonic Quantum Computing	Xanadu	
	Psi Quantum	
Supraleitung	IBM/Google/Rigetti	
	IQM	
Ionenfallen	EleQtron/AQT	
	IonQ/Quantinuum (Honeywell)	
Cäsiumatomfallen	ColdQuanta	

Ionenfallen bekannt ist. Das Prinzip der Ionenfallen beruht darauf, dass Ionen (Atome mit einer elektrischen Ladung) in einer gefangenen Umgebung eingeschlossen werden. Diese gefangene Umgebung kann eine Kombination aus elektrischen und magnetischen Feldern sein, die die Bewegung der Ionen kontrollieren und begrenzen. Um die Qubits zu kontrollieren und zu messen, werden Laserstrahlen verwendet, die auf die Ionen gerichtet werden. Diese Laserstrahlen können die quantenmechanischen Eigenschaften der Ionen beeinflussen und ändern, was es ermöglicht, Berechnungen durchzuführen.

Die Ergebnisse von Ionenfallen gelten als stabiler als die Berechnungen des Quantencomputers auf Basis der Supraleitung. Ein Vorteil von Ionenfallen besteht beispielsweise darin, dass ein Ion mit allen anderen Ionen interagieren kann, wohingegen supraleitende Qbits jeweils nur mit ihrem nächsten Nachbarn interagieren. Ein weiterer Vorteil besteht darin, dass die Ionen alle vollkommen identisch und rein sind. Als Vorteil der Technologie der Supraleitung wird hingegen gesehen, dass man hier auf bestehende bekannte Herstellungsverfahren zurückgreifen kann.

Die Technologie der Ionenfallen wird in der EU stark gefördert und wird auch von

[5] Wird ein Material auf Supraleitung, d.h. nahe dem absoluten Nullpunkt gekühlt, so verschwindet sein elektrischer Widerstand.

einigen amerikanischen Unternehmen wie Honeywell und IonQ eingesetzt. Die nachstehende Tabelle gibt eine Übersicht über die verschiedenen Technologien und einige ihrer Vertreter.

Wie kann ich Quantencomputer beurteilen?

Bei der Entwicklung des Quantencomputers ist neben der Hardware und den Quantenalgorithmen ebenfalls zu beachten, dass parallel speziell für den Quantencomputer geeignete Programmiersprachen entwickelt werden (beispielsweise Qiskit von IBM und Cirq von Google). Honeywell stellt heraus, dass das Software Tool TKET als open source – Softwareentwicklern ermöglicht unabhängig von der Hardware mit verschiedenen Plattformen zu arbeiten.

Es gibt noch keinen einheitlichen Standard, um die Güte und Leistungsfähigkeit eines Quantencomputers zu messen. Eine häufig verwendete Metrik ist das sogenannte „quantum volume“, welches sowohl die Anzahl der Qubits als auch die Schaltungstiefe („circuit depth“) betrachtet. Sie ist ein Maß für die Komplexität von Schaltungen und gibt an, wie viele Schichten (oder Ebenen) von Gattern in einer Schaltung benötigt werden, um eine bestimmte Berechnung durchzuführen. Jede Schicht arbeitet auf dem Ausgang der vorherigen Schicht, um die Eingabe in die Ausgabe zu transformieren. Die Tiefe einer Schaltung ist dann die Anzahl der Schichten, die benötigt werden, um die gesamte Berechnung durchzuführen. Eine Schaltung mit geringer Tiefe kann Berechnungen schneller durchführen als eine Schaltung mit höherer Tiefe, da weniger Schritte erforderlich sind, um die Eingabe in die Ausgabe zu transformieren. Neben dem „quantum volume“ spielt die Dekohärenzzeit der Qubits eine wichtige Rolle sowie die Güte der Gatter.

Neben den technologischen Hürden müssen auch mathematische Schwierigkeiten bewältigt werden. Um den Quantencomputers effektiv nutzen zu können, müssen Quantenalgorithmen entwickelt werden, die speziell für bestimmte Aufgaben ausgelegt sind. Quantenalgorithmen fallen jedoch nicht vom Himmel und ihre Entdeckung wird auch deshalb erschwert, weil das Arbeiten mit der Quantenmathematik eine ganz besondere Logik erfordert, die sich nicht an unserer Anschauung orientiert. Der bekannteste Quantenalgorithmus wurde 1994 von Peter Shor entwickelt, der die Primfaktorzerlegung großer Zahlen exponentiell schneller berechnet als jeder bekannte klassische Algorithmus.

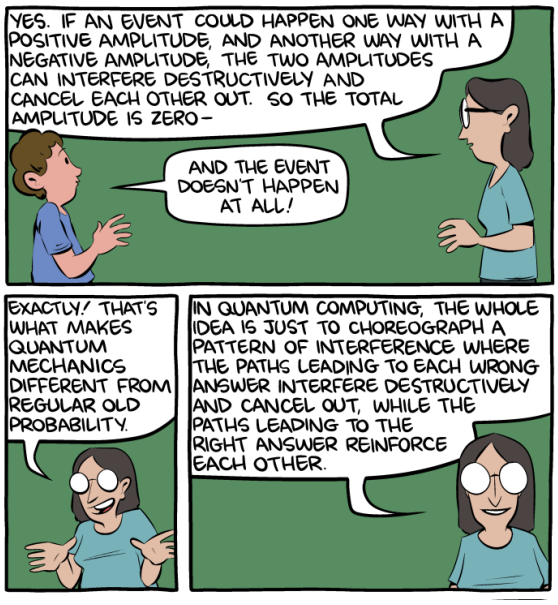
Wir haben zuvor gesehen, dass man zwar auf 2^n Zustände mehrerer Qubits während der Überlagerung zugreifen und daher rechnen kann (d.h. alle möglichen Lösungen eines Problems gleichzeitig betrachtet), dass aber bei Beobachtung bzw. Messung diese Zustände dekohärieren[6]. Der Quantenzustand repräsentiert daher nur so lange alle möglichen Lösungen, bis er durch Beobachtung oder Messung gestört wird. Eine der Herausforderungen bei der Entwicklung von Quantenalgorithmen besteht daher darin, vor der Dekohärierung der Qubits

[6] "Dekohärieren" bezieht sich auf den Prozess des Übergangs eines Quantensystems von einem überlagerten Zustand zu einem klassischen Zustand durch Messung bzw. Beobachtung. Eine solche „Beobachtung“ kann auch ein Umwelteinfluss sein.

sinnvolle Informationen aus dem Quantensystem zu gewinnen. Die Wissenschaftler machen sich hierbei zunutze, dass die Amplituden mehrerer Qubits sich überlagern oder auslöschen können, ähnlich wie zwei Wasserwellen, deren Wellenberge sich bei Aufeinandertreffen der Wellen ebenfalls überlagern[7]. Neben der Überlagerung und Verschränkung bildet daher die Interferenz das dritte Standbein des Quantencomputers, obwohl das Phänomen der Interferenz keine spezifische Eigenschaft der Quantenmechanik ist.

Durch ein ausgeklügeltes Design der Schaltung von Quantengattern können Wissenschaftler die Wahrscheinlichkeit für bestimmte Ergebnisse erhöhen, bevor das Quantensystem durch die Messung dekohäriert. Ziel eines Quantenalgorithmus ist es daher die Wahrscheinlichkeit für die korrekte Lösung zu vergrößern und die Wahrscheinlichkeit für alle anderen Lösungen zu verkleinern. Gerade im komplexen Design dieser Schaltungen liegt eine der Schwierigkeiten bei der Entdeckung von Quantenalgorithmen.

Für Leser, die eine humorvolle prägnante Erklärung der Anwendung der Interferenz im Quantencomputer bevorzugen, eignet sich der folgende Auszug aus einem Comic des Quantenmathematikers Scott Aaronson. Der gesamte Text ist übrigens hier erhältlich: Saturday Morning Breakfast Cereal - The Talk (smbc-comics.com)



Anlagemöglichkeiten

Das enorme Wachstumspotential des Marktes für Quantencomputer ist auch an den Investoren nicht vorbeigegangen. Zu den bekanntesten reinen „pure plays“, die in den letzten Jahren an die Börse gingen – teilweise über den Weg eines SPACs – gehören D-Wave, Rigetti und IonQ. Daneben gibt es weltweit viele kleinere Start-Ups (Quantum Computing Report zählt weltweit insgesamt 284 Unternehmen auf). Das schwierige wirtschaftliche Umfeld hat jedoch die Risikobereitschaft vieler Investoren und Anwender eingeschränkt und die Aktienkurse der genannten Unternehmen sind nach dem Börsengang stark eingebrochen. Die Aktienkurse von D-Wave, Rigetti und Quantum Computing sind außerdem nahe an der kritischen 1 $ - Marke und es droht diesen Aktien ein „delisting“. Trotz dieser schwierigen Situation darf nicht übersehen werden, dass neben privaten Mitteln für Start-Ups (in 2023 wurden in den ersten Wochen bereits insgesamt 11 neue Unternehmen verzeichnet) auch

[7] Dieses Phänomen wird Interferenz genannt.

beträchtliche öffentliche Mittel in den Sektor fließen.

Mit ca. USD 100 Mio konnten in den letzten Monaten vor allem Coldquanta und Xanada größere Mittel erhalten. Die Mittel von USD 6,1 Mio für das deutsche Start-Up EleQtron (ein Spin-Off der Universität Siegen) von Earlybird Venture Capital nehmen sich damit sehr bescheiden aus.

Fazit

Laut einer Studie von International Data Corporation vom 29. November 2021 werden die Kundenausgaben für Quantum Computing in den nächsten sechs Jahren stark ansteigen. Im Jahr 2020 betrugen sie 412 Millionen US-Dollar, bis 2027 werden sie jedoch auf 8,6 Milliarden US-Dollar anwachsen, was einer jährlichen Wachstumsrate von 50,9 % entspricht. Den wahrscheinlich besten Einblick in das Umsatzpotential des Quantum Computing bietet jedoch eine neuere Umfrage von Hyperion Research von Ende 2022, zitiert in Quantum Computing Report: Dieser Umfrage zufolge unter 145 Teilnehmern aus 18 Ländern sollten die Umsätze in 2022 US-Dollar 614 Mio. betragen haben. Es wird erwartet, dass sie bis 2025 mit einer Wachstumsrate von 25,3 % auf US-Dollar 1,2 Mrd. ansteigen werden.

Obwohl die Branche ein rasantes Wachstum verzeichnet, warnen einige Experten vor einem möglichen "Quantum Winter", ähnlich dem "KI Winter", in dem die Künstliche Intelligenz über einen längeren Zeitraum keine Fortschritte erzielte. Die eingangs zitierten Wachstumszahlen deuten jedoch darauf hin, dass ein „Quantum Winter“ vermieden werden kann.

Derzeit ist noch unklar, welche Technologien sich am Ende durchsetzen werden, aber es besteht kein Zweifel daran, dass der Sektor aufgrund der Bedeutung und Vielzahl von Anwendungsbereichen ein rasches Wachstum erfahren kann. Mit der Weiterentwicklung des neuromorphen Computings könnte sogar ein völlig neues Gebiet entstehen, das vom deutschen Mathematiker Prof. Klaus Mainzer als "hybrides Computing" bezeichnet wurde. Ziel sei es „to accelerate problem solving with increasing complexity in our civilization“.

Nicht nur die Unternehmen, sondern auch die Staaten haben die Bedeutung des Quantencomputers erkannt. Im Jahr 2021 hat China die Entwicklung von Quantentechnologien zu einer hohen Priorität in seinem Fünfjahresplan gemacht. Die chinesische Regierung investiert erhebliche Ressourcen in die Forschung und Entwicklung von Quantencomputern, Quantenkommunikation und anderen Quantentechnologien, um ihre wirtschaftliche und technologische Führungsposition in der Welt zu stärken. Die USA haben ebenfalls eine nationale Initiative namens "National Quantum Initiative" ins Leben gerufen, die darauf abzielt, die Entwicklung von Quantentechnologien voranzutreiben. Obwohl einige Stimmen die Initiative als nicht ambitioniert genug betrachten und den Fokus auf Cryptoverfahren bemängeln, ist die Initiative ein wichtiger Schritt in Richtung der Förderung von Forschung und Entwicklung von Quantentechnologien in den USA. Die kanadische Regierung hat seit 2012 CAD 1 Mrd. in F&E für Quantentechnologien investiert und im Januar 2023 verkündet, dass im Rahmen der Canadian Quantum Strategy weitere CAD 360 Mio investiert werden. Europa plant mit dem

„Quantum Flagship“ über den Zeitraum von 10 Jahren 1 Md. Euro in Quantentechnologien zu investieren. Ziel sei es „ein Quantennetz aufzubauen: Quantencomputer, Simulatoren und Sensoren, die über Quantennetze miteinander verbunden sind und Informationen und Quantenressourcen wie Kohärenz und Verschränkung verteilen.“

Investoren, die sich intensiver mit dem Anlagepotential von Unternehmen befassen wollen, ist zu raten, dass sie sich zumindest ansatzweise mit den unterschiedlichen Technologien vertraut machen. Hilfreich ist auch, zeitnah die Berichte der börsennotierten Unternehmen zu lesen. Es ist davon auszugehen, dass einige der bisher in Privatbesitz befindlichen Start-Ups ebenfalls den Weg an die Börse finden, wenn sich das Umfeld wieder verbessert. Hierbei werden folgende vier Geschäftsfelder unterschieden:

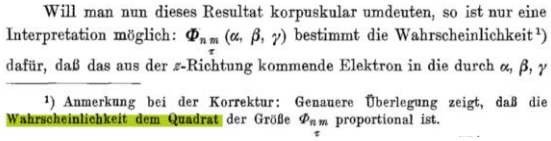
- Hardware
- Software
- Communications
- Consulting

Die in der Tabelle genannten nicht-börsennotierten Unternehmen könnten einen ersten Hinweis geben auf mögliche Kandidaten. Derzeit gibt es keine kollektiven Investmentprodukte, da das Anlageuniversum noch zu klein ist.

Anhang

Wahrscheinlichkeit in der Quantenmathematik

Viele gute Lehrbücher über Quantenmathematik weisen lediglich daraufhin, dass die Quadrate der Amplituden von 0 und 1 den Charakter einer Wahrscheinlichkeit haben, ohne jedoch eine Erklärung zu geben, warum es sich um Wahrscheinlichkeiten handelt. In der Tat lässt sich der Wahrscheinlichkeitscharakter der Komponenten nicht einfach ableiten. Bis heute ist es Wissenschaftlern nicht gelungen, einen Beweis für diese Eigenschaft zu finden. Die Entdeckung bzw. Vermutung, dass es sich bei den Quadraten der Amplituden a und b um Wahrscheinlichkeiten handelt geht auf den deutschen Physiker Max Born zurück, der 1926 in seinem Text „Zur Quantenmechanik der Stoßvorgänge“ in einer Fußnote auf diesen Zusammenhang hinwies. Die Eigenschaft einer Wahrscheinlichkeit der Komponenten wird auch als Born’sche Regel bezeichnet. Aufgrund der historischen Bedeutung der Entdeckung von Born haben wir die Fußnote als Faksimile nachstehend abgebildet und den entscheidenden Satzteil grün unterlegt.



Will man nun dieses Resultat korpuskular umdeuten, so ist nur eine Interpretation möglich: $\Phi_{n\,m}(\alpha, \beta, \gamma)$ bestimmt die Wahrscheinlichkeit[1]) dafür, daß das aus der z-Richtung kommende Elektron in die durch α, β, γ

[1]) Anmerkung bei der Korrektur: Genauere Überlegung zeigt, daß die Wahrscheinlichkeit dem Quadrat der Größe $\Phi_{n\,m}$ proportional ist.

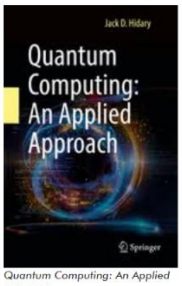
Wir möchten deshalb ausführlicher auf das Konzept der Wahrscheinlichkeit eingehen, weil die Bornsche Regel von erheblicher Bedeutung für die Quantenmechanik ist. Selbst wer sich nicht näher mit der Quantenmechanik befasst, hat oftmals doch eine Vorstellung davon, dass die Gesetze der Quantenmechanik auf der Ebene der Elementarteilchen keine

deterministischen Aussagen über einige Eigenschaften der Elementarteilchen machen können, sondern nur Wahrscheinlichkeitsaussagen. Zu Beginn der Forschung über die Quantenmechanik Anfang des letzten Jahrhunderts (der Begriff wurde übrigens das erste Mal als Überschrift in einem Artikel von Born benutzt) war es zunächst keineswegs klar, dass die quantenmechanischen Phänomene einen statistischen Charakter haben. Insbesondere Einstein weigerte sich bis zuletzt zu glauben, dass Messergebnisse in der Quantenmechanik letztendlich unbestimmt sind und einen statistischen Charakter haben. Einen guten Eindruck der Zweifel, die Einstein im Bezug auf den statistischen Charakter der Quantenmechanik hatte erhält man aus seinen Briefen an Born. In seinem berühmten Brief vom 29. April 1924 drückt er seine Überzeugung aus, dass Elektronen keinen freien Willen haben: „Der Gedanke, daß ein einem Strahl ausgesetztes Elektron aus freiem Entschluß den Augenblick und die Richtung wählt, in der es fortspringen will, ist mir unerträglich. Wenn schon, dann möchte ich lieber Schuster oder gar Angestellter einer Spielbank sein als Physiker.“ Mehr als zwei Jahre später (Brief vom 4. Dezember 1926 an Max Born) münden seine Zweifel in dem berühmten Spruch, dass Gott nicht würfelt: „Die Quantenmechanik ist sehr achtunggebietend. Aber eine innere Stimme sagt mir, daß das noch nicht der wahre Jakob ist. Die Theorie liefert viel, aber dem Geheimnis des Alten bringt sie uns kaum näher. Jedenfalls bin ich überzeugt, daß der nicht würfelt.“

Lektüre

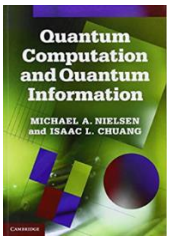
Es gibt eine Vielzahl guter Bücher zur Quantenmathematik. Hier eine Auswahl:

Das Buch von Jack Hidary bietet eine gut lesbare Einführung der mathematischen Grundlagen des Quantencomputers und kann auch für die Auffrischung einiger mathematischer Kenntnisse dienen.



Quantum Computing: An Applied Approach

Das Buch von Michael Nielsen gilt als Standardwerk und wird oft zitiert. Es ist sehr umfangreich, aber anspruchsvoll und als Einstiegslektüre nicht geeignet, eher als Nachschlagewerk.



Außer Lehrbüchern gibt es exzellente Online-Kurse auf Youtube bzw. Lehrbücher im Internet:

Sehr empfehlenswert ist der 126 Videos umfassende Kurs von Berkeley Professor Umesh Vazrani (ebenfalls im Advisory Board von IonQ), der auch auf Youtube verfügbar ist. Hier der Link:

Quantum Mechanics & Quantum Computation - Umesh Vazirani - YouTube (für ein tieferes Verständnis der Bloch-Kugel s. Video Nr. 15).

Empfehlenswert als Einstieg ebenfalls der Kurs von Michael Nielsen auf Youtube:

The qubit - YouTube