

Seltsamkeit auf die Tagesordnung setzen

Die Leistung von Quantencomputern bestimmen

Die Vorteile von Quantencomputing erkennen

Eine Bestandsaufnahme verschiedener
Quantencomputer-Typen vornehmen

Hindernisse für neue Möglichkeiten überwinden

Kapitel 1

Das Quantencomputing-Bootcamp

Stellen Sie sich vor, Sie werfen eine Münze in die Luft. Zeigt sie Kopf oder Zahl, während sie sich dreht? Während die Münze geworfen wird, haben Sie keine Antwort darauf. Erst wenn die Münze landet und am Boden liegt, zeigt sie ein eindeutiges Ergebnis.

Die Ungewissheit, die Sie erfahren, während sich die Münze dreht, entspricht der Ungewissheit, die wir beim Quantencomputing erfassen und nutzen. Wir versetzen viele Verarbeitungseinheiten – sogenannte *Qubits* – in einen Zustand der Unsicherheit (wir werfen die Münze also quasi in die Luft, damit sie anfängt sich zu drehen und wissen eben nicht, ob sie nun gerade eine 1, oder eine 0 zeigt oder etwas dazwischen). Dann programmieren wir die Qubits, führen das Programm aus und erfassen die Ergebnisse – genau wie bei der Münze.

Quantencomputing funktioniert anders als wir es von den eindeutig bestimmten 0en und 1en, Bits und Bytes, die in den heutigen Computern verwendet werden, gewohnt sind. Das Quantencomputing basiert auf der Quantenmechanik, einem Teilgebiet der Physik, das mitunter schwer zu verstehen ist. Aber die Art und Weise, wie Quantencomputing mit großen Unsicherheiten umgeht, ähnelt der Art und Weise, wie wir viele unserer Entscheidungen im täglichen Leben treffen.

Quantencomputing ist eine Ergänzung zum klassischen Computing, also der Art von Computing, wie wir es heute verwenden – und kein Ersatz dafür. Durch den Ansatz, mit Ungewissheit zu arbeiten, können wir einige der größten und komplexesten Probleme der Menschheit auf eine neue und vielversprechende Weise angehen. Quantencomputing wird

Probleme lösen, für die die heutige Technologie nicht ausreicht – Probleme in Bereichen wie der Klimamodellierung, der Medikamentenentwicklung, der Finanzoptimierung und der Frage, ob es ein guter Morgen ist, um eine Rakete zu starten.

Quantencomputing steht erst am Anfang; viele vergleichsweise leistungsstarke Quantencomputer laufen jeweils nur für den Bruchteil einer Sekunde. Aber es werden ständig Fortschritte gemacht. Und schon jetzt, in diesem frühen Stadium, inspiriert uns Quantencomputing dazu, »anders zu denken«, was die Art und Weise betrifft, wie wir vorhandene Rechenkapazität nutzen. In diesem Kapitel stellen wir die Leistungsfähigkeit und das Potenzial des Quantencomputing vor.



In diesem Kapitel werden viele Begriffe und Konzepte vorgestellt, die Ihnen vielleicht noch nicht geläufig sind. Keine Sorge, wir erklären sie alle in späteren Kapiteln ausführlich. (In Kapitel 3 beispielsweise wird die Quantenmechanik beschrieben und erklärt, wie Quantencomputing damit zusammenhängt.) Betrachten Sie dieses Kapitel als eine Art Bootcamp für den neuen Quantencomputingspezialisten, zu dem Sie sich nach der Lektüre dieses Buches entwickeln werden.

Verstehen, warum Quantencomputing so seltsam ist

Quantencomputer sind irgendwie seltsam – auf eine geradezu mystische Art und Weise. (Der Film »*Dr. Strange in the Multiverse of Madness*« aus dem Jahr 2022 fängt ein wenig von dem Gefühl ein, das die Menschen gegenüber der Quantenmechanik im Allgemeinen haben.) Warum ist das so?

Es gibt zwei Hauptgründe dafür. Der erste Grund ist das grundlegende Missverständnis der Menschen, was die Natur der Materie betrifft, die Gegenstand der Quantenmechanik ist. Der zweite Grund ist die unglaubliche Leistung, die Quantencomputing, wenn es irgendwann ausgereift sein wird, der Menschheit bringen wird.

Wie verändert die Quantenmechanik (beschrieben in Kapitel 3) die Weltanschauung der Menschen? Die Welt, in der wir leben, in der Steine nach unten fallen und Raketen aufwärts fliegen, scheint von fester Materie beherrscht zu sein, wobei Energie eine Macht ist, die zu verschiedensten Zeiten auf die Materie wirkt. Man könnte sich Materie jedoch auch einfach als erstarrte Energie vorstellen.

Der größte Teil der Masse der Protonen und Neutronen im Inneren eines Atomkerns beispielsweise ist lediglich eine zahlenbasierte Beschreibung der ungeheuer starken Energiefelder, die diese Teilchen an ihrem Platz halten. Eine der wichtigsten Arten von Teilchen im Quantencomputing, die Photonen, haben überhaupt keine Masse; sie bestehen aus reiner Energie.

Und es war Einstein selbst, der uns mit seiner berühmten Gleichung $E=mc^2$ mitteilte, dass Materie und Energie gleichwertig sind. Übersetzt bedeutet dies: Die in fester Materie enthaltene Energie ist gleich ihrer Masse multipliziert mit der Lichtgeschwindigkeit zum Quadrat.



Die Lichtgeschwindigkeit ist eine sehr große Zahl – sie beträgt circa 300.000 km/Sekunde. Quadriert man die Lichtgeschwindigkeit, erhält man eine noch viel größere Zahl. Setzt man diese sehr große Zahl in Einsteins berühmte Gleichung ein, sieht man, dass selbst in kleinen Mengen von Materie eine große Menge Energie stecken kann – wie Kernkraftwerke und Atomwaffen beweisen.

Der Punkt ist, dass in der Quantenmechanik Materie nur eine untergeordnete Rolle spielt. Teilchen verhalten sich weniger wie Massepunkte oder kleine Bälle, sondern eher wie Energiebündel. Quantencomputing macht sich die exotischen Eigenschaften dieser Teilchen – ionisierter Atome, Photonen, supraleitender Metalle und anderer Materie, die ein quantenmechanisches Verhalten zeigen – zunutze.

Der zweite Grund, warum Quantencomputer eine so starke emotionale Reaktion hervorrufen, ist ihre enorme Leistung. Die besten heute vorhandenen Quantencomputer, befinden sich noch im Anfangsstadium und sind deshalb, wenn überhaupt, nicht viel leistungsfähiger als ein herkömmlicher Supercomputer. Es wird jedoch erwartet, dass künftige Quantencomputer enorme Geschwindigkeitssteigerungen bei der Lösung nahezu aller Probleme liefern werden. Das bedeutet nicht nur, dass heute zu lösende Probleme schneller gelöst werden können – es bedeutet insbesondere, dass es möglich sein wird, Probleme, bei denen ein Computer heute so lange rechnen würde, dass sich die Rechnung nicht lohnt, lösbar sein werden.

Wir gehen davon aus, dass Quantencomputer in den nächsten zehn oder zwanzig Jahren im Hinblick auf die Probleme, die sie lösen können, Hunderte, Tausende oder sogar Millionen Male schneller sein werden als heutige Computer. Die Menschen können nicht wirklich vorhersagen oder sich auch nur ansatzweise vorstellen, wie es sein wird, wenn diese Art von Rechenleistung für einige der wichtigsten Herausforderungen der Menschheit zur Verfügung steht, wie in den Kapiteln 13 und 14 beschrieben wird. Diese Zukunft ist sehr aufregend, ja. Aber sie ist auch ein wenig »gespenstisch«, wie Einstein die Quantenmechanik beschrieb.

Die Macht des Quantencomputing verstehen

Um Ihnen den Einstieg in das Verständnis des Quantencomputing zu erleichtern, sollten Sie sich zunächst mit den folgenden fünf großen Konzepten vertraut machen:

- ✓ **Qubits:** *Qubits* sind die Quantencomputer-Variante von Bits – den 0en und 1en, die den Kern der klassischen Informatik bilden. Sie haben quantenmechanische Eigenschaften. Qubits sind der Ort, an dem die ganze Magie des Quantencomputing stattfindet.
- ✓ **Überlagerung oder Superposition:** Während Bits auf 0 oder 1 beschränkt sind, kann ein Qubit einen undefinierten Wert annehmen, der weder 0 noch 1 ist, bis der Wert des Qubit gemessen wird. Die Fähigkeit, mehrere Werte gleichzeitig anzunehmen, wird *Überlagerung* oder *Superposition* genannt.

- ✓ **Verschränkung oder Entanglement:** Beim klassischen Computing sind die Bits sorgfältig voneinander getrennt, sodass der Wert eines Bits den Wert der anderen nicht beeinflusst. Qubits dagegen können miteinander verschränkt sein. Wenn Änderungen an einem Teilchen sofortige Änderungen an einem anderen Teilchen bewirken und wenn die Messung des Wertes für ein Teilchen den entsprechenden Wert für ein anderes Teilchen ergibt, sind die Teilchen *miteinander verschränkt*.
- ✓ **Tunneling:** Ein quantenmechanisches Teilchen kann sich unmittelbar von einem Ort zu einem anderen bewegen, selbst wenn sich dazwischen eine Barriere befindet. (Das Quantencomputing nutzt diese Fähigkeit, um Barrieren zu umgehen und die bestmögliche Lösung zu finden.) Dieses Verhalten wird als *Tunneling bezeichnet*.
- ✓ **Kohärenz:** Ein Quanten-Teilchen, beispielsweise ein Elektron, das frei von äußeren Störungen ist, ist *kohärent*. Nur kohärente Teilchen können Superposition und Entanglement zeigen.

Wie hängen diese Begriffe zusammen? Hier ein Beispiel: Ein gutes Qubit lässt sich relativ leicht in einen kohärenten Zustand versetzen und in diesem Zustand halten, sodass es Superposition und Verschränkung aufweisen und daher tunneln kann. (Die Suche nach »guten Qubits« ist heute Gegenstand zahlreicher Arbeiten und Kontroversen. Dieses Thema wird in den Kapiteln 10 und 11 ausführlicher beschrieben.)

Diese fünf Begriffe bilden das Herzstück dessen, was sich Experten vom Quantencomputing versprechen und sind mit vielen der Herausforderungen verbunden, die eine vollständige Implementierung des Quantencomputing aktuell erschweren. In diesem Abschnitt beschreiben wir jedes dieser elementaren Konzepte genauer.



Das klassische Computing beschreibt die Computer, die wir täglich benutzen. Dazu gehören nicht nur Laptops und Desktop-Computer, sondern auch Smartphones, Webserver, Supercomputer und viele andere Arten von Geräten. Der Begriff »klassisches Computing« wird verwendet, weil klassische Computer für die Informationsverarbeitung die klassische Mechanik nutzen, also die Ursache-Wirkung-Regeln, die wir in unserem täglichen Leben sehen und anwenden. Quantencomputing verwendet anstatt der klassischen newtonschen Mechanik die Quantenmechanik – die tatsächlich nicht nur anders, kompliziert und sehr interessant, sondern auch sehr leistungsfähig ist – für die Informationsverarbeitung. Wir führen in diesem Kapitel einige quantenmechanische Prinzipien ein und gehen in Kapitel 2 dann noch einmal ausführlicher auf die Details ein.

Puff, Magie – oder kurz: Qubit?

Bits sind die Grundlage für klassisches Computing – also Laptops, Server, Smartphones und Supercomputer, die wir heute benutzen. *Bit* ist die Abkürzung für *Binary Digit*, also *Binärziffer*, wobei *Ziffer* für eine einzelne Zahl steht, und *binär* bedeutet, dass die Zahl nur einen von zwei Werten annehmen kann: 0 oder 1 – genau wie das Ergebnis eines Münzwurfs.

In einem Computer werden Bits in winzigen, billigen elektromechanischen Bauteilen gespeichert, die zuverlässig entweder eine 0 oder eine 1 aufnehmen, speichern und

zurückgeben – zumindest solange, bis der Strom abgeschaltet wird. Da ein einzelnes Bit nicht viel aussagt, werden Bits in Bytes (von dem jedes wiederum 8 Bits enthält) verpackt, wobei ein einzelnes Byte 256 Werte speichern kann. (2^8 – alle möglichen Kombinationen von 8 binären Ziffern, also 256).

Ein *Qubit* ist ein komplexes Gerät, dessen Kern Materie in einem quantenmechanischen Zustand bildet (beispielsweise ein Photon, ein Atom oder ein winziges Stück supraleitendes Metall). Das Qubit enthält eine Art Behälter, z. B. ein starkes Magnetfeld, das die Materie daran hindert, mit ihrer Umgebung in Wechselwirkung zu treten.

Ein Qubit ist viel komplexer und viel leistungsfähiger als ein Bit. Aber Qubits sind heute nicht sehr zuverlässig, und zwar aus zwei Gründen:

- ✓ Sie sind anfällig für Fehler, die durch Rauschen in ihrer Umgebung verursacht werden. Ein Ergebnis von 0 kann versehentlich in ein Ergebnis von 1 umgewandelt werden oder umgekehrt, und es gibt keine einfache Möglichkeit zu erkennen, dass überhaupt ein Fehler passiert ist.
- ✓ Es ist schwierig, Qubits kohärent zu halten, sodass sie überhaupt zur Überlagerung, Verschränkung und zum Tunneln fähig sind.

Die Situation mit den Qubits ist heute ein wenig wie der alte Witz über ein schlechtes Restaurant: »Das Essen ist schrecklich – und die Portionen sind klein!« Bei Qubits sind die Fehlerquoten hoch und die Kohärenzzeit ist kurz. Das bedeutet, dass den Geräten trotz hoher Fehlerquoten nur wenig Zeit für einzelne Rechenoperationen und die Lösung des Problems bleibt. Aber trotz dieser Probleme liefern Quantencomputer wertvolle und interessante Ergebnisse, wenn sie in Betrieb sind.

Qubits sind außerdem viel komplexer und teurer als Bits. Sie sind auch nicht so einfach zu handhaben – aber sie sind viel leistungsfähiger.

Abbildung 1.1 zeigt ein Quantencomputermodule von IBM, das am Boden einer Kühlung hängt, die die supraleitenden Qubits auf einer Temperatur nahe dem absoluten Nullpunkt hält.

Bis es gemessen wird, repräsentiert jedes Qubit einen unendlichen Bereich von Werten zwischen 0 und 1. Wie kann ein Qubit so viele Werte auf einmal repräsentieren? Der Kern des Qubits ist ein *Quantenteilchen* – ein winziges Stück Realität in Form eines Photons, eines Elektrons, eines ionisierten Atoms oder eines künstlichen Atoms aus einem supraleitenden Metall.

Für das Quantencomputing muss das Quantenteilchen im Kern des Qubits in einem *kohärenten Zustand* gehalten werden – unkontrolliert, wie die geworfene Münze, während sie sich in der Luft dreht. In einem kohärenten Zustand wissen wir nicht, ob der Wert des Qubits zu einem bestimmten Zeitpunkt 0 oder 1 ist. Wenn wir den Zustand des Qubits messen, wird die von uns gewünschte Berechnung ausgeführt, und das Qubit gibt 0 oder 1 als Ergebnis der Messung zurück.

Ein großer Teil der Leistungsfähigkeit von Qubits beruht auf der Tatsache, dass sie sich *probabilistisch* verhalten; ein bestimmtes Qubit, das dieselbe Berechnung mehrfach fehlerfrei

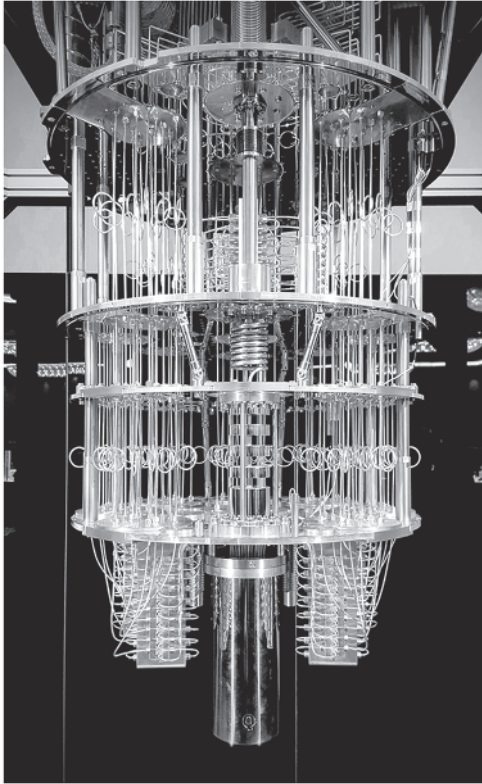


Abbildung 1.1: Ein Quantencomputer-Prozessor von IBM.
© Flickr/Lars Plougmann

durchführt, kann bei einigen Durchläufen eine 0 und bei anderen eine 1 ergeben. Das Endergebnis setzt sich aus der Anzahl der Fälle zusammen, in denen das entsprechende Qubit jeweils eine 0 oder eine 1 ausgegeben hat. Das Ergebnis der meisten Quantenberechnungen ist also eine Menge von Wahrscheinlichkeiten und kein einzelnes Ergebnis in Form einer einzelnen Zahl.

Qubits sind sowohl schwer zu erzeugen als auch in einem Zustand der Kohärenz zu halten; außerdem neigen sie dazu, mit benachbarten Qubits unkontrolliert zu interferieren. Die Zählung von Qubits ist eine der größten Herausforderungen bei der Entwicklung nützlicher Quantencomputer.

Ein beliebter Ansatz für den Bau von Quantencomputern ist die Verwendung supraleitender Qubits, die bei einer Temperatur nahe dem absoluten Nullpunkt gehalten werden müssen, um hitzebedingte Störungen zu minimieren und so seine quantenmechanischen Eigenschaften zu erhalten.

Klassische Computer sind so konzipiert, dass sie bei Raumtemperatur funktionieren, aber sie neigen dazu, Wärme zu erzeugen und bei zu stark ansteigender Temperatur nicht mehr richtig zu funktionieren. Die Notwendigkeit, die Wärme, die beim Betrieb der Computer

entsteht, abzuführen, hindert die Gerätehersteller daran, die Komponenten so dicht nebeneinander zu packen, wie sie es gerne hätten, ohne auf teure und umständliche Lösungen wie Wasserkühlung oder Kühlung der Komponenten zurückzugreifen.

Beim Quantencomputing steigert jedes zusätzliche Qubit die Leistung des Computers exponentiell. Da Qubits jedoch dazu neigen, sich gegenseitig zu stören, ist das Hinzufügen weiterer Bits schwierig.

IBM, ein führendes Unternehmen im Bereich Quantencomputing, hat einen Entwicklungsplan veröffentlicht, der zeigt, wie sich die Anzahl der Qubits, die in den aktuellen und künftigen Quantencomputern verbaut sind, in der Vergangenheit erhöht hat und in der Zukunft erhöhen wird. Eine vereinfachte Version dieses Plans ist in Abbildung 1.2 dargestellt. Einen Link zur aktuellen Version finden Sie unter <https://research.ibm.com/blog/ibm-quantum-roadmap-2025>.

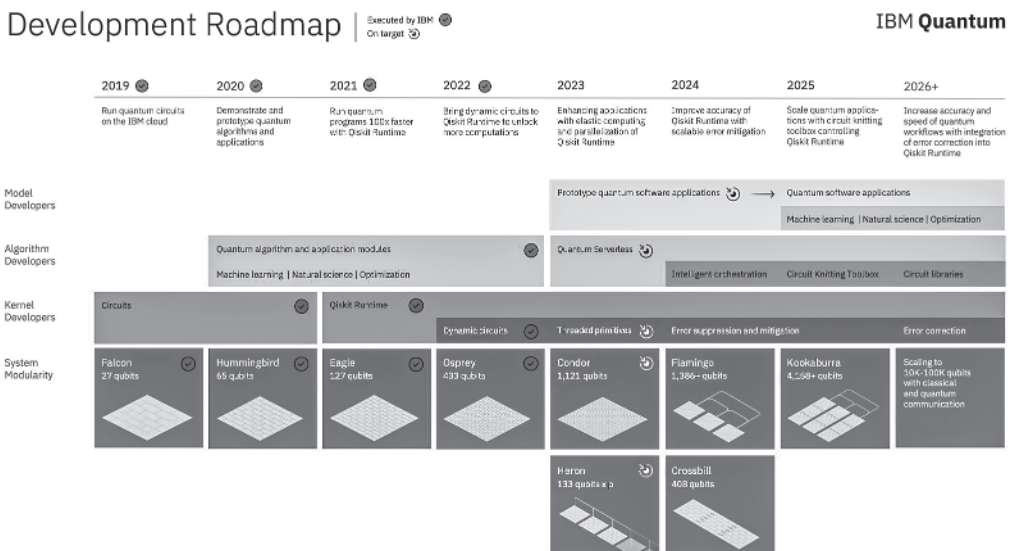


Abbildung 1.2: Die Roadmap für Quantencomputer von IBM zeigt das bisherige und das erwartete Wachstum der Anzahl der verfügbaren Qubits.

Superposition (Überlagerung) – die erste Quanten-Superkraft

Der Zustand der Möglichkeit, der den Qubits zur Verfügung steht, wird als *Superposition* (Überlagerung) bezeichnet, wobei *Super* für *viele* und *Position* für *Möglichkeiten* steht. Ein herkömmliches Bit kann entweder 0 oder 1 sein. Ein Qubit im Zustand der Überlagerung hat keinen definierten Wert, da es viele potenzielle Werte gleichzeitig transportiert. Aber wenn wir ein Qubit messen, erhalten wir einfach 0 oder 1 zurück – je nachdem, in welchen Wert die energetische Wellenfunktion des Qubits im Moment der Messung kollabiert.

Die Superposition ist der erste von zwei wichtigen Gründen für die Leistungsfähigkeit der Quanteninformatik. Der andere, das Entanglement, also die Verschränkung, wird im nächsten Abschnitt beschrieben.

In Kapitel 3 wird erklärt, wie die Schöpfer der Quantenmechanik die Superposition und andere Quantenprinzipien während einer außergewöhnlichen Periode wissenschaftlicher Kreativität zwischen etwa 1900 und 1930 entdeckten. (In diese Zeit fielen auch die Katastrophe des Ersten Weltkriegs und der Beginn der Weltwirtschaftskrise.)

DAS LEBEN, DAS MULTIVERSUM UND IHRE ERKLÄRUNG

Quantencomputer beruhen auf den Gesetzen der Quantenmechanik, die in Kapitel 3 in Grundzügen beschrieben werden. Quantenmechanische Prinzipien sind für den Betrieb von Quantencomputern unerlässlich.

Eine Möglichkeit, die Funktionsweise der Quantenmechanik zu verstehen, ist die Vorstellung, dass jeder mögliche Zustand eines quantenmechanischen Objekts wahr wird – in einem neuen Paralleluniversum, das entsteht, um diese Möglichkeit zu realisieren. In dem Moment, in dem unser Qubit also in unserer Welt in den Zustand 0 bei der Messung kollabiert, entsteht eine andere Welt, in der das Qubit in den Zustand 1 kollabiert. Diese Art, sich die Realität vorzustellen, ist die Grundlage für aktuelle Filme wie *Everything Everywhere All at Once* und *Quantumania*. Es gibt jedoch auch eine anhaltende Kontroverse darüber, ob multiple Universen real sind.

Wir müssen uns bei unserer täglichen Arbeit im Bereich des Quantencomputing nicht mit diesen Debatten aufhalten; wir können, wie man so schön sagt, »einfach die Klappe halten und programmieren«. Aber diese scheinbar wilden Ideen können uns helfen zu verstehen, wie ungewöhnlich und wunderbar die Quantenwelt ist. Sie können uns bei unserer täglichen Arbeit inspirieren, und sie können zu scheinbar science-fiction-artigen Errungenschaften wie Zeitreisen, Teleportation und Reisen »schneller als das Licht« führen – zumindest für Informationen, wenn auch nicht für Gegenstände oder Menschen.

Es ist kompliziert – das neue Must Have

George Washington warnte die Amerikaner einst, außenpolitische Verwicklungen zu vermeiden. Mit Qubits jedoch begrüßen wir genau solche komplizierten Abhängigkeiten – in unserem Kontext als Verschränkung oder Entanglement bezeichnet – als ein zusätzliches, leistungsfähiges Werkzeug in unserem Werkzeugkasten für Quantencomputing.

Die *Verschränkung* ist eine Art Verbindung zwischen zwei oder mehr Quantenteilchen. Wir können dafür verschiedenste Eigenschaften von Teilchen nutzen. Zum Beispiel haben Quantenteilchen eine Eigenschaft, die *Spin* genannt wird, und die wir entweder als abwärts oder aufwärts (0 oder 1) messen können. Wenn zwei Quantenteilchen verschränkt sind

und bei einem von ihnen ein Aufwärtsspin gemessen wird, wissen wir ohne Messung, dass das andere verschränkte Teilchen einen Abwärtsspin hat. Und wenn wir den Spin des ersten Quantenteilchens so beeinflussen, dass er bei der Messung nach oben wechselt, wissen wir ohne Messung, dass das andere Quantenteilchen nach unten wechseln wird. Einen Spin können Sie sich am besten mittels Wendeltreppen vorstellen. Auf Wendeltreppen gehen Sie scheinbar im Kreis, bewegen sich dabei jedoch trotzdem nach unten oder oben – ähnlich verhält sich der Spin von Teilchen.

Abbildung 1.3 zeigt die Verbindung zwischen zwei verschränkten Qubits, die entgegengesetzte Spins haben. Wenn man den Spin des einen Qubits misst, weiß man, dass der Spin des anderen entgegengesetzt ist; wenn man den Spin des einen Qubits in eine Richtung ändert, ändert sich der Spin des anderen in die entgegengesetzte Richtung.

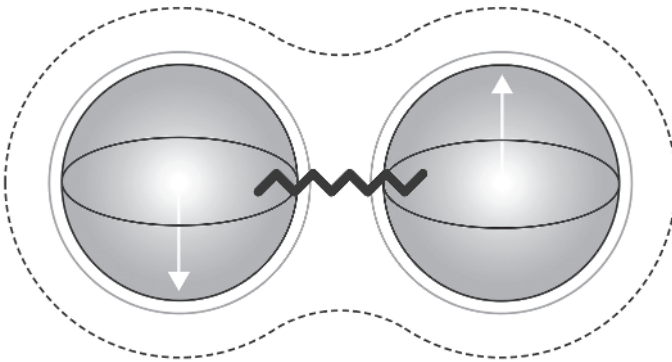


Abbildung 1.3: Verschränkte Qubits beeinflussen sich gegenseitig.

Wie bereits erwähnt, ist die Verschränkung die zweite Eigenschaft, auf der die Leistungsfähigkeit des Quantencomputing beruht. Bisher haben wir in unseren Beispielen immer von zwei Qubits gesprochen. Tatsächlich kann man theoretisch beliebig viele Qubits miteinander verschränken. Das führt dazu, dass bei Qubits die Beeinflussung eines einzelnen Qubits eine Auswirkung auf viele andere hat.

Entanglement und Superposition arbeiten zusammen. Wenn sich ein verschränktes Qubit im Zustand der Superposition befindet, befindet sich jedes mit ihm verschränkte Qubit ebenfalls im Zustand der Überlagerung. Diese kaskadierenden Ungewissheiten erhöhen die potenzielle Leistung von Quantencomputern exponentiell.

Um einen Quantencomputer zu programmieren und Berechnungen durchzuführen, muss die Verschränkung und Überlagerung der entsprechenden Qubits aufrechterhalten werden, indem man sie kohärent und frei von Rauschen hält. Dann messen wir die Qubits (wodurch sie dekohärent werden) und zeichnen die Ergebnisse auf, eine 0 oder 1 für jedes Qubit. Das führt dazu, dass man während der Berechnung gleichzeitig mit allen Werten rechnen kann, ohne jede Berechnung einmal für den Wert 1 und einmal für den Wert 0 durchzuführen.

SCHNELLER ALS DAS LICHT

Albert Einstein spielt in der Geschichte der Quantenmechanik zweierlei Rollen – die nicht unbedingt gut zueinander passen.

Die eine Rolle entstammt Einsteins Entdeckung der Relativitätstheorie, die 1905 veröffentlicht wurde. Relativität bedeutet dabei, dass die Geschwindigkeit in unserem Universum von der eigenen Bewegung relativ zu der Bewegung anderer Beobachter ist, dass aber die Lichtgeschwindigkeit – etwa 300.000 Kilometer pro Sekunde – für alle Beobachter immer gleich ist. Diese universelle Geschwindigkeitsgrenze wird als *Lokalität* bezeichnet.

Die andere Rolle hat mit Einsteins Entdeckung des Photons zu tun, ebenfalls im Jahr 1905. (Für diese Entdeckung, nicht etwa für die Relativitätstheorie, erhielt Einstein seinen einzigen Nobelpreis.) Die Entdeckung des Photons ist grundlegend für die Quantenmechanik.

Einsteins Problem besteht darin, dass Quantenphysiker später behaupteten, dass Quantenteilchen wie Photonen miteinander verschränkt sein können, sodass man durch Ablesen des Spins (zum Beispiel) des einen Photons den Spin des anderen ablesen kann. Und diese Beziehung gilt sofort, unabhängig von der Lichtgeschwindigkeit. Physiker nennen dies eine Behauptung der Nichtlokalität, was wiederum einen Widerspruch zur eben erläuterten Relativität darstellt.

Einstein hasste diesen Widerspruch und nannte diese Nichtlokalität »spukhafte Fernwirkung«. Er und seine Kollegen verbrachten viel Zeit damit, sie zu widerlegen, sogar als Einstein weitere bahnbrechende Quantenentdeckungen machte, wie beispielsweise die Identifizierung von Bose-Einstein-Kondensaten, supraleitenden Gasen, die zur Erzeugung von Qubits verwendet werden können.

Die heutigen herkömmlichen Computer unterliegen der klassischen Mechanik und sind durch die Lichtgeschwindigkeit begrenzt. Quantencomputer beruhen auf der Quantenmechanik und sind, da sie die Verschränkung nutzen, nicht durch die Lichtgeschwindigkeit begrenzt, wenn es um die Übermittlung von Informationen geht.

Der Nobelpreis für Physik im Jahr 2022 wurde Physikern verliehen, die bewiesen haben, dass Verschränkung jenseits von Lichtgeschwindigkeit existiert. Forscher im Bereich Quantencomputing, deren Forschung auf Entanglement angewiesen ist, können also ganz nach Galileo sagen: »Und er rechnet doch.« (Galileo, der vor Gericht stand, weil er – wie sich herausstellte zu Recht – behauptet hatte, dass die Erde nicht im Mittelpunkt des Universums steht, soll bekanntlich geflüstert haben: »Und sie bewegt sich doch.«)



Die Quantenkommunikation wird durch die Verwendung verschränkter Qubits für die Kommunikation zwischen entfernten Orten ermöglicht. Dies wird in Kapitel 3 näher erläutert.

Quantencomputing braucht Kohärenz

Qubits können nur dann für Quantencomputer verwendet werden, wenn sie in einem Zustand der *Kohärenz* gehalten werden, frei von Wechselwirkungen mit ihrer Umgebung. Um Quantencomputing zu betreiben, müssen Qubits den Regeln der Quantenmechanik folgen (wie in Kapitel 2 erläutert), und diese Regeln gelten nur für kohärente Qubits.



Quantenteilchen, die im Universum herumschwirren – zum Beispiel Photonen, die von der Sonne ausgesandt werden – befinden sich in einem Zustand der Kohärenz. Was führt dazu, dass sie dekohärent werden? Jede Wechselwirkung mit übermäßigen Störungen (wie Schwingungen oder einem starken Magnetfeld), einem festen Gegenstand oder einem Messgerät.

Es ist schwierig, Qubits kohärent zu halten. Durch Wärme werden sie dekohärent, also werden die Qubits kalt gehalten. Das Gleiche gilt für Erschütterungen (man denke an einen vorbeifahrenden Lastwagen auf einer Straße) und jede Kollision mit ihrer Umgebung. Um solche Kollisionen zu verhindern, verwenden Wissenschaftler häufig starke Magnetfelder oder gezielte Laserstrahlen, um zu verhindern, dass die Quantenteilchen in ihrem Inneren mit ihren technischen Behältern kollidieren.

Die Dekohärenz ist nicht die einzige Katastrophe, die Qubits treffen kann. Temperaturänderungen, Schwingungen oder physikalische Wechselwirkungen können den Wert eines Qubits unkontrolliert verändern, ohne dass es dekohärent wird. Dieses Rauschen führt zu Fehlern in den Ergebnissen von Quantenberechnungen. Die Minimierung des Rauschens und die Erkennung von Fehlern sind zwei der größten Herausforderungen für Quantencomputer.

Um ein Qubit zu manipulieren – um es zum Beispiel für das Quantencomputing zu programmieren –, muss es so gesteuert werden, dass sein Wert verändert wird, ohne dass es dekohärent wird. Magnetfelder und Laserstrahlen gehören zu den Mitteln, mit denen Qubits manipuliert werden können, ohne Dekohärenz zu verursachen.

Wenn wir den Wert eines Qubits messen, geschehen zwei Dinge:

- ✓ Das Qubit wird dekohärent und unterliegt damit den Regeln der klassischen Mechanik.
- ✓ Der Wert des Qubits kollabiert von irgendwo zwischen 0 und 1 auf entweder 0 oder 1.

Das Qubit muss reinitialisiert – in den Zustand der Kohärenz versetzt – werden, bevor es wieder zum Rechnen verwendet werden kann.



Manchmal wird argumentiert, dass das Potenzial von Quantencomputern sehr begrenzt ist – weil das für Quantencomputer erforderliche Maß an Kohärenz, um nützliche Ergebnisse zu erzielen, theoretisch und tatsächlich unmöglich ist. In der Extremform dieser Argumentation wird den führenden Vertretern des Quantencomputing vorgeworfen, bewusst zu betrügen, was bedeuten würde, dass es sich bei dem Ganzen einfach nur um eine massive Verschwörung handelt. Nur weitere Forschung und Entwicklung werden die Grenzen des Quantencomputing aufzeigen, sofern diese Grenzen existieren, aber die massiven Betrugsvorwürfe sind nur eine Verschwörungstheorie.

Die Leistung des Quantencomputing in Zahlen fassen

Es ist schwierig, die potenzielle Leistung von Quantencomputern im Vergleich zu klassischen Computern vollständig zu erfassen, da diese Leistung auf quantenmechanischen Prinzipien beruht und die Messung von Rechenleistungen, wie wir sie kennen, auf mechanischen. Aber wir können das Ganze mit ein paar mathematischen Überlegungen zusammenfassen.

Da die Bits beim klassischen Rechnen nur einen von zwei Werten – 0 oder 1 – gleichzeitig annehmen können, wird die Anzahl der Zustände, die ein klassischer Computer annehmen kann, durch die Anzahl der Bits, n , erhoben in die zweite Potenz, dargestellt: n^2 . Ein Satz verschränkter Qubits kann jedoch alle möglichen Werte der Qubits gleichzeitig annehmen. Aus diesem Grund wird die Anzahl der Zustände, die ein Quantencomputer speichern kann, durch 2, erhoben in die Potenz der Anzahl der Qubits, n , dargestellt: 2^n . Um beispielsweise eine Million möglicher Zustände darzustellen, wären 1.000 Bits erforderlich, aber nur 20 Qubits.

Heutige Computer enthalten Milliarden von Bits, aber wir müssen eine Menge davon für ein einziges komplexes Problem aufwenden, um auch nur ein näherungsweise gutes Ergebnis zu erhalten. Heutige Quantencomputer haben eine geringe Anzahl von Qubits – ein kürzlich vorgestellter Quantencomputer von IBM hatte 433 Qubits –, aber wir brauchen auch nur ein paar hundert Qubits, um sehr komplexe Probleme zu lösen.

Die Leistung der heutigen Quantencomputer ist durch Fehler und kurze Kohärenzzeiten begrenzt. Sobald wir jedoch eine Lösung für diese Probleme haben, werden die Ergebnisse wahrscheinlich großartig sein.

Was Quantencomputing für die Menschen bewirken kann

Man kann natürlich lang und breit über die Seltsamkeiten und die Macht des Quantencomputing diskutieren. Aber welchen Unterschied wird Quantencomputing für die Zukunft der Menschheit machen? Um die Antwort zu verstehen, müssen wir zunächst mit einem weit verbreiteten Missverständnis ausräumen. Die Menschen neigen heute dazu, sich Sorgen darüber zu machen, wie leistungsfähig die *heutigen* Computer sind: sie machen sich Gedanken über die Leistungsfähigkeit des Internets, der sozialen Medien, des maschinellen Lernens und der KI.

Aber es gibt auch ein anderes Problem, nämlich die *mangelnde* Leistungsfähigkeit der heutigen Computer: sie sind den großen rechnerischen Herausforderungen in vielen Bereichen einfach nicht gewachsen, wie beispielsweise der Entwicklung besserer Batterien zur Bekämpfung des Klimawandels, einer besseren Aerodynamik, einer besseren Streckenführung in komplexen Verkehrsnetzen oder auch der besseren und zielgerichteteren Entwicklung neuer Medikamente, um nur einige der wichtigsten Beispiele zu nennen, (In den Kapiteln 13 und 14 finden Sie weitere Informationen über die Herausforderungen, bei deren Bewältigung Quantencomputing helfen kann.)

Und genau bei diesen großen rechnerischen Herausforderungen erwarten wir, dass Quantencomputing den entscheidenden Unterschied machen wird. Künftige Quantencomputer werden in der Lage sein, Probleme zu lösen, an die wir heute nicht herankommen, und zwar viel schneller, kostengünstiger und mit weniger Energieaufwand als mit heutigen Computern.



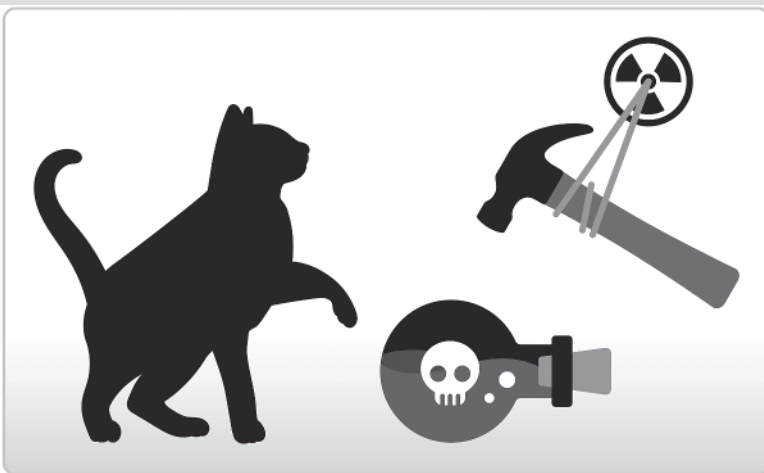
Quantencomputer können ihre Aufgabe nur in Zusammenarbeit mit Computern erfüllen, wie wir sie heute verwenden. Wenn Sie also Informationen darüber lesen, was Quantencomputer leisten können, sollten Sie sich darüber im Klaren sein, dass diese Leistungen auch eine ganze Menge konventioneller Rechenleistung erfordern.

GIBT ES SCHRÖDINGERS KATZE WIRKLICH?

Nein, Schrödingers Katze ist nicht real. Aber wir wollen diese Antwort noch etwas nuancieren. Die Quantenmechanik, also die Physik, die Quantencomputing zugrunde liegt, hat die Menschen seit der Veröffentlichung der wichtigsten theoretischen Arbeiten zwischen 1900 und 1930 zugleich fasziniert und verwirrt. (Weitere Informationen dazu finden Sie in Kapitel 3.) Und nichts symbolisiert diese Verwirrung besser als Schrödingers Katze.

Erwin Schrödinger, der brillante Physiker, der hinter dem Gedankenexperiment zu Schrödingers Katze steht, versuchte 1935 damit, Quantenmechanik zu *widerlegen*. Dennoch hat er das Geheimnis, das sich hinter den Quanten verbirgt, besser auf den Punkt gebracht als irgendein anderer.

Beim Gedankenexperiment mit Schrödingers Katze legt ein Wissenschaftler ein Fläschchen mit radioaktivem Gift, eine zerfallende radioaktive Masse und eine Katze in eine Kiste. Irgendwann wird der radioaktive Zerfall einen Hammer aktivieren, der das Fläschchen zerbricht und die Katze tötet, wie in der Abbildung dargestellt. Aber der radioaktive Zerfall ist zufällig, sodass niemand vorhersagen kann, wann der Hammer das Fläschchen zerbricht.



Der Wissenschaftler schließt also den Kasten, geht weg und wartet mehrere Stunden, bevor er zurückkommt. Während dieser Stunden stellt sich eine dringende Frage: Ist die Katze lebendig oder tot?

Die Quantenmechanik bietet nur eine gnomische Antwort: Ja und Nein. Keine Intelligenz der Welt kann mit Sicherheit sagen, ob der radioaktive Zerfall die Katze zu einem bestimmten Zeitpunkt töten wird oder nicht. Die Katze ist also sowohl tot als auch lebendig, bis der Wissenschaftler zurückkommt und die Kiste öffnet.

Diese scheinbar lächerliche Vermutung zeigt auf, *Superposition funktioniert*, bei der sich die Materie – in diesem Fall der Körper einer Katze – in zwei Zuständen gleichzeitig befindet. Die Existenz von Superposition, die für Quantencomputing von entscheidender Bedeutung ist, wurde seit Schrödingers Gedankenexperiment unzählige Male bewiesen. (Katzen sind eigentlich zu groß und zu sehr in unsere materielle Welt eingebettet, um sich in Superposition zu befinden, falls Sie sich Sorgen gemacht haben. Und noch einmal: ES WURDE KEINE KATZE VERLETZT. Miau.)

Ein verwandtes Prinzip, die *Verschränkung* – eine geheimnisvolle Verbindung zwischen beliebig weit entfernten Teilchen, wenn auch nicht Katzen –, wurde ebenfalls in einer Reihe von Experimenten nachgewiesen, die 2022 mit dem Nobelpreis für Physik ausgezeichnet wurden. Es war Einstein, der die Verschränkung im Besonderen und die Quantenmechanik im Allgemeinen als »spukhafte Fernwirkung« bezeichnete.

Schrödingers Katze – im Sinne von tatsächlichen Katzen, die in Lebensgefahr schweben – ist also nicht real. Aber die Prinzipien, die Schrödingers unsterbliches Gedankenexperiment beflügeln, sind sehr real, wie das Quantencomputing jeden Tag beweist.

Die verschiedenen Arten von Quantencomputern

Es gibt drei Möglichkeiten des Quantencomputing, die heute alle aktiv genutzt und untersucht werden. Sie werden in den Kapiteln 8 bis 11 ausführlich beschrieben. Hier gehen wir nur kurz darauf ein, um ein Gefühl für die verschiedenen Methoden und Architekturen von Quantencomputern zu bekommen.

Quanteninspiriertes Computing

Klassische Computer basieren auf sogenannten Logikgattern, die elektrische Ströme aufnehmen und eine binäre Logik auf sie anwenden, um entweder keinen Strom (eine 0) oder einen leicht messbaren Strom (eine 1) zu erzeugen. Bricht man ein beliebiges mathematisches oder logisches Problem auf eine ausreichend niedrige Ebene herunter und lässt es durch Logikgatter laufen, kann man eine Antwort finden. Ein Logikgatter ist quasi eine elektrische Schaltvorrichtung, die eine einfache logische Verknüpfung herstellt. Durch das Hintereinanderschalten von mehreren einfachen Gattern kann man insgesamt komplexe logische Operationen durchführen, indem man die Eingaben quasi durch einen Gatterparcours

laufen lässt. Die Notwendigkeit dieser sehr konkreten Vereinfachung des Problems, die zur Lösungsfindung notwendig ist, wird später noch wichtig, wenn es um die Vorteile geht, die Quantencomputer gegenüber klassischen Computern haben könnten.

Wenn Erkenntnisse aus dem Quantencomputing genutzt werden, um neue Algorithmen zu entwickeln, die auf klassischen Computern laufen, oder wenn Quantencomputer-Simulatoren auf klassischen Computern laufen, wird dies als *quanteninspiriertes Computing* bezeichnet, wie in Kapitel 8 beschrieben. Das quanteninspirierte Computing hat sich als produktiver Ansatz erwiesen, um in diesem frühen Stadium der Entwicklung des Quantencomputers neue Lösungen zu finden.

Quanten AnnealingIn der klassischen Datenverarbeitung gibt es einen Ansatz, der als *simuliertes Annealing* bezeichnet wird. Es ist vergleichbar mit dem Glühen in der Metallindustrie, bei dem ein Metall erhitzt wird, um seine innere Struktur zu schmelzen, und dann abgekühlt wird, um ein weicheres, leichter zu bearbeitendes Ergebnis zu erzielen. *Simuliertes Annealing* eignet sich gut für die Lösung von Optimierungsproblemen, beispielsweise für die Suche nach der günstigsten Route zum Besuch mehrerer Städte. Ein ähnliches Verfahren kann zur Lösung von Problemen verwendet werden, indem eine Reihe von Gleichungen durch eine Reihe von Transformationen geschickt wird, bis ein Ergebnis entsteht.

Die Quantencomputer-Version dieses Ansatzes wird als *Quanten-Annealing* (oder *Quantenglühen*) bezeichnet. Beim Quantenglühen wird kein gatterbasierter Quantencomputing-Ansatz verwendet, der zwar fortschrittlicher, aber schwieriger zu implementieren ist, wie in den Kapitel 10 und 11 beschrieben. Stattdessen werden beim Quantenglühen Qubits als Gruppe zur Lösung von Optimierungsproblemen verwendet, was weniger anspruchsvoll ist als die gezielte Nutzung, einzelner Qubits.

Quanten-Annealer lassen explizit Qubit-Fehler zu und liefern Ergebnisse, die zwar ungenau, aber in vielen Fällen dennoch nützlich sind. So könnte ein Quanten-Annealer beispielsweise einen sehr guten Weg für die Routenplanung einer Flotte von Lieferwagen ermitteln, statt die einzig mögliche Route zu liefern. Nur ein einziges großes Unternehmen, D-Wave, stellt Quantencomputer her, die den Ansatz des Quanten-Annealings verwenden, und es hat kürzlich Pläne angekündigt, auch Quantencomputer mit Logikgattern herzustellen.

Quanten-Annealer, wurden einst kritisiert, weil sie keine echten Quantencomputer sind, aber das ist nicht mehr der Fall. Die meiste Aufmerksamkeit, der meiste Forschungsaufwand und die meisten Investitionen entfallen jedoch auf gatterbasierte Quantencomputer.

Die Theorie besagt, dass das Quantenglühen schließlich durch eine Kombination aus besseren klassischen Rechenansätzen – die die Anwendungsfälle von »unten«, d. h. in Bezug auf die technische Raffinesse, übernehmen – und gatterbasiertem Quantencomputing – dass die Anwendungsfälle von »oben« übernimmt – ersetzt werden sollte. Wir werden sehen.

Gatterbasiertes Quantencomputing

Die meisten Quantencomputer verwenden Quantenschaltkreise, um die Logikgatter-Struktur von klassischen Computern nachzubilden. Diese Computer werden als *gatterbasierte Quantencomputer* bezeichnet. Gatterbasierte Quantencomputer verwenden Qubits

auf eine bestimmte Art und Weise und sind nicht tolerant gegenüber Fehlern im Betrieb der Qubits; die Quanten-Logikgatter funktionieren jedoch nicht zuverlässig, wenn die Qubits nicht fehlerfrei sind. Die heutigen Qubits sind nicht zuverlässig fehlerfrei, was den Nutzen der heutigen gatterbasierten Quantencomputer beeinträchtigt.



Das gatterbasierte Quantencomputing ist so schwer zu realisieren, dass wir noch nicht sicher sein können, ob es jemals sein volles Potenzial erreichen wird. Aber wenn es so weit ist, wird es wahrscheinlich sowohl das quanteninspirierte Computing als auch Quanten-Annealer überflüssig machen. Irgendwann dürfte das gatterbasierte Quantencomputing die beste Methode sein, um alle Arten von Quantencomputerproblemen zu lösen.

Bei dieser Art von Quantencomputern werden hauptsächlich vier Typen von Qubits verwendet, die auf verschiedenen physikalischen Objekten, die in einem kohärenten Zustand gehalten werden, um Quantencomputing durchzuführen:

- ✓ Supraleitende Metallschleifen
- ✓ Ionen (gespeichert in Ionenfallen)
- ✓ Photonen
- ✓ Neutrale Atome

Jede Art von Qubit hat ihre Vor- und Nachteile, die wir in den Kapiteln 10 und 11 beschreiben. Unterschiedliche Quantencomputerfirmen setzen auf unterschiedliche Arten von Qubits.

Es ist schwierig, die Qubits lange genug kohärent zu halten, um Logikgatter-Operationen mit ihnen durchführen zu können. Daher haben gatterbasierte Quantencomputer in der Regel nur relativ wenige Qubits – höchstens ein paar Hundert (zum Zeitpunkt an dem dieses Buch geschrieben wurde) – und führen Programme nur für den Bruchteil einer Sekunde aus, bevor sie dekohärieren.

DAS GROSSE GANZE IM AUGE BEHALTEN

Atome setzen sich aus drei Arten von Teilchen zusammen: Protonen, Neutronen und Elektronen. Protonen, die sich im Atomkern befinden, haben eine positive Ladung von 1. Neutronen, die sich ebenfalls im Kern befinden und in gleicher Anzahl wie Protonen vorhanden sind, haben eine Ladung von 0 – also effektiv keine Ladung. Die Anzahl der Protonen (und damit auch der Neutronen) im Kern bestimmt die Ordnungszahl des Atoms und welches Element das Atom darstellt. Wasserstoff hat beispielsweise nur ein Proton und ein Neutron, während Helium zwei davon hat.

Die Elektronen, die den Kern umkreisen, tragen eine negative Ladung, die genauso groß ist wie die positive Ladung eines Protons: eine Ladung von -1 . In den meisten Aggregatzuständen hält sich die Anzahl der Elektronen mit der Anzahl der Protonen die Waage, und das Atom als Ganzes hat eine neutrale elektrische Ladung, weil sich die

Ladungen der Protonen und der Elektronen gegenseitig ausgleichen. In einem ionisierten Atom werden Elektronen hinzugefügt oder entfernt. Wird ein zusätzliches Elektron vom Kern eingefangen, ist das Atom negativ geladen; flieht ein Elektron aus dem Kern, ist das Atom positiv geladen.

Was stoppt uns?

Im vorangegangenen Kapitel haben wir versucht, das Potenzial und die Leistungsfähigkeit vom Quantencomputing und die besonderen physikalischen Eigenschaften, auf denen diese zukunftsweisende Technologie basiert, darzustellen. Welche Herausforderungen muss das Quantencomputing bewältigen, damit all dieses Potenzial auch zu weiteren Ergebnissen führt?

Bei der Hardware müssen mehrere zusammenhängende Herausforderungen bewältigt werden:

- ✓ **Bessere Qubits:** Qubits mit niedrigeren Fehlerquoten werden weitaus bessere Ergebnisse liefern. Qubits und ihre Kontrollmechanismen müssen weniger Rauschen erzeugen, um kein Übersprechen (ungewollte Interferenzen zwischen benachbarten Qubits und der Umgebung) zu verursachen, und sie müssen besser isoliert werden, um ungewolltes Rauschen durch beispielsweise Hitze und Schwingungen zu vermeiden.
- ✓ **Mehr Qubits:** Sobald sich jedes Qubit besser kontrollieren lässt, können wir sie dichter und in größerer Zahl zusammenpacken. Wie beim klassischen Computing wird diese Entwicklung die Rechenleistung erheblich steigern und gleichzeitig die Kosten senken.
- ✓ **Kühlung und Superkühlung:** Supraleitende Qubits erfordern extrem niedrige Temperaturen, aber niedrigere Temperaturen sind auch besser für die Fehlerreduzierung bei allen anderen Arten von Qubits. Daher wird eine bessere, kostengünstigere und leichter herzustellende Kühlung und Superkühlung den anderen Hardware-Herausforderungen helfen.
- ✓ **Fehlerkorrektur:** Für die Fehlerkorrektur sind mehrere Lösungen erforderlich. Eine davon ist die Kombination mehrerer physikalischer Qubits zu einem einzigen, selbstkorrigierenden logischen Qubit. Kältere Temperaturen und bessere Kontrollmechanismen werden die Fehlerzahl verringern und die Fehlerkorrektur erleichtern.

Und hier die größten Herausforderungen im Bereich der Software:

- ✓ **Quantenalgorithmen:** An der Optimierung von Algorithmen für herkömmliche Computer wird schon seit Jahrzehnten gearbeitet, aber die Quantenalgorithmen stehen noch ganz am Anfang. Es sind sowohl theoretische Fortschritte als auch Optimierungen in der Praxis erforderlich. Bei vielen Algorithmen wissen wir heute nur theoretisch, wie wir sie auf einem Quantencomputer implementieren würden – die praktische Umsetzung, quasi das Rezept, fehlt, obwohl wir alle Zutaten haben. Bei anderen haben wir das Rezept, aber noch keine Ahnung, wie gut es am Ende schmeckt, weil wir die Geräte zur Umsetzung noch nicht haben.

- ✓ **Hybridform aus Quanten- und klassischem Computing:** Es sind Fortschritte sowohl bei der Software als auch bei der Hardware erforderlich, damit Quanten- und klassische Computer Probleme reibungslos und mit hoher Leistung gemeinsam zur Lösung von Problemen verwendet werden können.
- ✓ **Fehlervermeidung:** Software kann helfen, Fehler vorherzusagen und zu reduzieren, was die heutigen Quantencomputer nützlicher macht und die Belastung durch die Hardware-Fehlerkorrektur verringert.

Es mangelt jedoch auch an der Leistungsfähigkeit der Menschen:

- ✓ **Wissenschaftler und Forscher:** Es sind theoretische Arbeiten und Weiterentwicklungen notwendig, um das Gebiet voranzubringen, aber es gibt zu wenige qualifizierte Personen.
- ✓ **Software-Entwickler:** Nur eine kleine Zahl von Softwareentwicklern weiß, wie man Quantencomputersysteme nutzt und zu ihrer Weiterentwicklung beiträgt, auch wenn dieser Anteil langsam steigt.
- ✓ **Wirtschaftsanalysiker und Endnutzer:** Die Benutzergemeinschaft weiß noch nicht, welche Probleme sie mit Quantencomputersystemen angehen soll und wie sie nach notwendigen Verbesserungen fragen kann, die in naher Zukunft einen Nutzen bringen könnten.

Schließlich ist das Quantencomputing eine neue Art, Probleme zu betrachten – und oft führt diese neue Sichtweise zu besseren Lösungen beim Einsatz von klassischen Computern. Nur durch die Fortsetzung bisheriger Arbeit werden alle Beteiligten eine bessere Vorstellung davon bekommen, wie die verschiedenen Arten des Computings – und hybride Systeme, die beide Arten möglichst effizient nutzen – am besten eingesetzt werden können.

All dies lässt Sie vielleicht fragen, wo wir mit Quantencomputing heute stehen. Es befindet sich in einer schwierigen Lage: Es hat ein enormes Potenzial und zieht weltweit Investitionen in Milliardenhöhe an, ist aber bei wichtigen Problemen dem klassischen Rechnen noch nicht überlegen.

Bei Redaktionsschluss dieses Buches hat IBM jedoch Arbeiten angekündigt, die zeigen, was IBM als *Quantenvorteil* bezeichnet, nämlich die Fähigkeit von Quantencomputern, Ergebnisse zu erzielen, die mit klassischen Computern nicht oder aber schlechter lösbar sind. Für diese Arbeit verwendete IBM einen seiner neueren Quantencomputer mit 127 kontrollierten Qubits, um die Wechselwirkungen zwischen 127 Stabmagneten zu simulieren – ein subtiler, fraktaler Alptraum für klassische Computer. IBM ließ dasselbe Problem auf klassischen und Quantencomputersystemen lösen. Supercomputer (leistungsstarke klassische Computer) konnten mit dem IBM-Quantencomputer bis etwa 63 Qubits mithalten, also bis zur Hälfte seiner Kapazität. Darüber hinaus scheinen die Ergebnisse des Quantencomputers die Möglichkeiten von Supercomputern zu übersteigen.

Es gibt noch viel zu tun, um diesen offensichtlichen Durchbruch zu bestätigen oder zu dementieren – und er ist nur für diejenigen von unmittelbarem Nutzen, deren Produktplan genau 127 interagierende Stabmagnete beinhaltet. Aber als ernsthafte Absichtserklärung, den Ansatz weiterzuverfolgen, ist es vielversprechend.