Quantencomputer

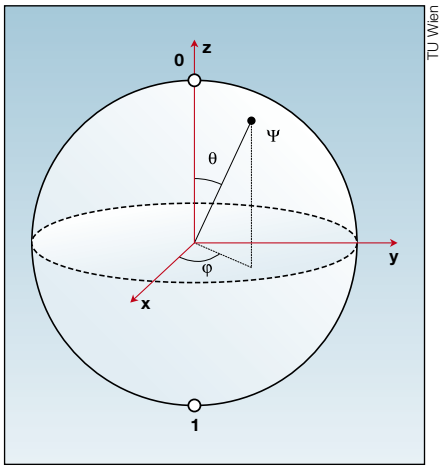
Wenn ein Bit gleichzeitig 0 und 1 ist

Je kleiner die Elektronik, desto grösser der Einfluss der Quantenphysik. Ein Bit ist dann nicht mehr nur eine 0 oder eine 1, sondern kann etwas dazwischen sein – eine Überlagerung der beiden Zustände. Einen klassischen Computer bringt dies durcheinander, die Forscher wollen die Quantengesetze nun aber gezielt nutzen, um leistungsfähige Quantencomputer zu entwickeln. Diese könnten Verschlüsselungen, die heute als sicher gelten, leicht knacken.

Johannes Majer

Die Computertechnologie ist in den letzten Jahren fast ungebremst gewachsen. Durch den Einsatz von Mikrotechnologie werden die Bauteile ständig verkleinert, sodass die Anzahl der Transistoren sich alle 18 Monate verdoppelt, was als Mooresches Gesetz bekannt ist. Dabei stellt sich die Frage unweigerlich, ob diese Entwicklung einfach so weitergehen kann. Spätestens wenn die Grösse eines Bauteils diejenige eines einzelnen Atoms erreicht hat, ist das Ende dieser Entwicklung erreicht.

Bei dieser rasanten Entwicklung und Begriffen wie «virtuelle Informationsverarbeitung» könnte man den Eindruck erhalten, dass die Informatik keine physikalischen Grenzen kennt. Indessen ist aber zu beachten, dass jeder Information ein physikalischer Zustand zugrunde liegt. Zum Beispiel entspricht die Information eines Bits in einem D-RAM-Speicher der Ladung auf einem Kondensator; oder auf einer Harddisk der Ausrichtung der Magnetisierung. Informationsverarbeitung ist daher immer ein physikalischer Prozess, seien die beteiligten Effekte noch so klein. Dieser Umstand wird sofort plausibel, wenn man die Abwärme beachtet, die durch ein modernes Rechenzentrum produziert wird. Unser tägliches Leben, aber auch die modernsten Computer werden bestimmt durch die Gesetze der klassischen Physik. Und die Grundlage der Physik bildet wiederum die Quantenmechanik. Daher stellt sich die Frage, ob es nicht möglich wäre, sich diese Effekte zunutze zu machen und einen qualitativ besseren Computer herzustellen, der auf den Gesetzen der Quantenmechanik basiert. Motiviert durch diese Perspektiven, sind grosse Aktivitäten in der Grundlagenforschung der Physik und der Informatik entstanden.



TU Wien

Bild 1 Blochsphäre.
Beschreibung des Zustands eines Qubits auf der Blochspäre. Nord- und Südpol stellen die klassischen Zustände 0 und 1 dar, während alle anderen Zustände durch Überlagerungen entstehen.

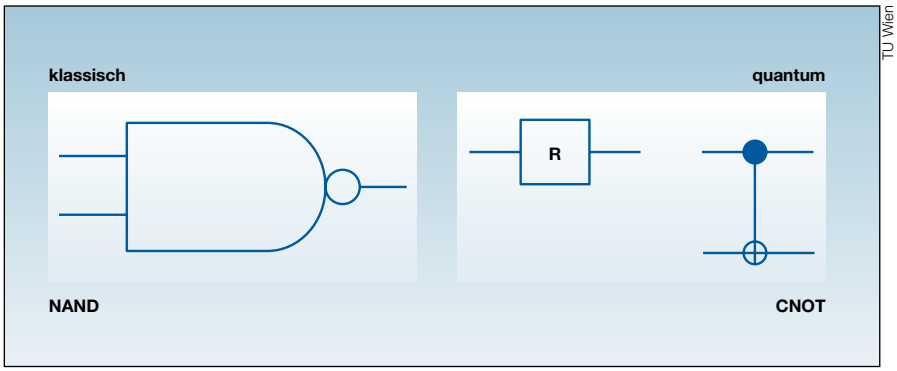
Quantenbits

Wie in der klassischen Informationsverarbeitung ist die Grundeinheit ein Bit, hier ein Quantenbit oder kurz: Qubit. Für ein klassisches Bit sind nur zwei Zustände möglich, 0 oder 1. Da die Quantenmechanik Zustände durch Wellen beschreibt, sind für ein Qubit auch Überlagerungen möglich. Das heisst, ein Qubit kann sowohl im Zustand 0 als auch im Zustand 1 sein. Quantenmechanisch kann der Zustand eines Qubits als Punkt auf einer Kugeloberfläche, genannt Blochsphäre, dargestellt werden (siehe Bild 1). Dabei entspricht der Nordpol dem klassischen Zustand 0 und der Südpol dem Zustand 1. Alle anderen Positionen sind Überlagerungen dieser zwei Zustände.

Mehrere Qubits können nun zu einem Quantenregister zusammengefügt werden. Die Annahme, dass der Zustand von zwei Qubits einfach durch zwei Kugeln beschrieben wird, ist jedoch falsch. Der Raum, der diese zwei Qubits beschreibt, hat schon 6 Dimensionen und wächst exponentiell mit der Anzahl Qubits. Während ein klassisches Register mit N Bits nur in einem Zustand zur selben Zeit ist, kann ein Quantenregister eine Überlagerung von allen 2^N Zuständen annehmen. Hätte man ein Register mit 500 Qubits, wäre die Zahl der Zustände grösser als die Zahl der Atome im Universum. Dies illustriert das Potenzial eines Quantenregisters – und das Ziel eines Quantencomputers ist, diese Leistungsfähigkeit auszunutzen.

Quantenalgorithmen

Ein Quantencomputer führt einen Algorithmus aus, indem er die Zustände eines Quantenregisters manipuliert. Da die Operationen der Quantenmechanik gehorchen, müssen sie unitär, das heisst reversibel sein. Wünschenswert wäre ein universeller Block, aus dem jede beliebige unitäre Operation aufgebaut werden kann. In der klassischen Boolschen Logik ist ein solcher Block bekannt, das NAND-Gatter (Bild 2). Jede beliebige Boolsche Operation lässt sich ausschliesslich aus einzelnen NAND-Gattern aufbauen. Leider ist das NAND-Gatter für einen Quantencomputer nicht geeignet, da es nicht reversibel ist, d.h., der Eingangszustand lässt sich nicht mehr aus dem Ausgangszustand herleiten. In der Quantenlogik ist bis jetzt noch kein einzelner universeller Block bekannt. Jedoch lässt sich jede unitäre Operation durch zwei universelle Blöcke bilden (Bild 2): Der erste sind einzelne Qubit-Rotationen, d.h. beliebige Bewegungen auf der Kugeloberfläche. Der zweite Block besteht aus zwei Qubit-Operationen, wobei das Ziel-Qubit invertiert wird, falls das Kontroll-Qubit im Zustand 1



TU Wien

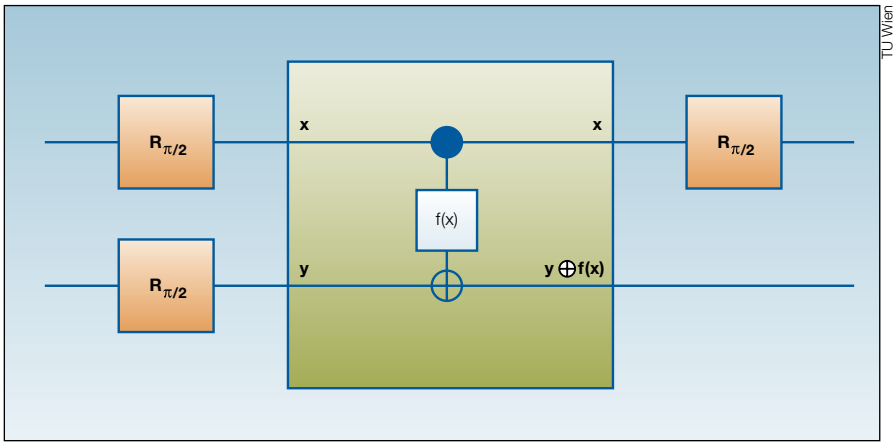
Bild 2 Universelle Gatter.
Aus einem NAND-Gatter kann jede Boolsche Logik eines klassischen Computers aufgebaut werden. Jeder Quantenalgorithmus kann gebildet werden durch einzelne Qubit-Rotationen und einen Controlled Not (CNOT).

ist – und nur dann. Diese Operation wird Controlled Not (CNOT) genannt. In der Boolschen Logik ist eine solche Operation als XOR bekannt. Diese zwei Blöcke erlauben es, jede beliebige Quantenoperation auszuführen.

Ein Quantenalgorithmus versucht nun, mit diesen universellen Blöcken ein Problem schneller zu lösen als ein klassischer Computer, indem Gebrauch gemacht wird vom Überlagerungsprinzip. Ein einfaches Beispiel ist der Deutsch-Josza-Algorithmus (Bild 3). Leider ist das Problem nicht sehr relevant und nur von akademischem Interesse, illustriert aber gut die Funktion eines Quantencomputers: Die Problemstellung lautet, festzustellen, ob eine Münze fair ist, sprich: ob sich auf einer Seite Kopf und auf der anderen eine Zahl befindet oder ob es sich um eine gefälschte Münze mit zwei Köpfen (resp. Zahlen) handelt. Während man klassisch alle Möglichkeiten prüfen, d.h. beide Seiten anschauen muss, nutzt ein Quantencomputer das Überlagerungsprinzip. Die Münze wird in eine Überlagerung der zwei Seiten gebracht und vom Quantencomputer überprüft, womit sie nur einmal angeschaut werden muss.

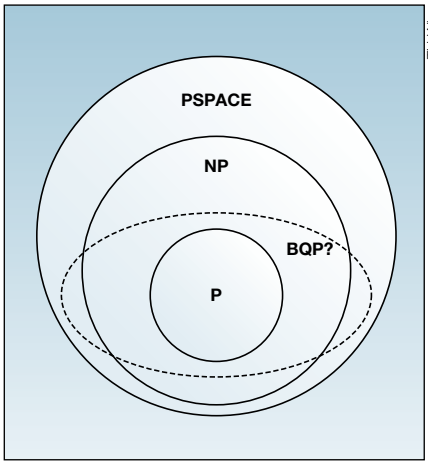
Ein viel relevanteres Problem versucht der Grover-Algorithmus zu lösen, nämlich die Suche in einer unstrukturierten Datenbank. Da die Daten nicht sortiert sind, bleibt einem klassischen Computer nichts anderes übrig, als alle Datensätze anzuschauen, bis der gewünschte Eintrag gefunden ist. Ein Quantencomputer nimmt das Überlagerungsprinzip zu Hilfe und kann massiv parallel suchen. Der Grover-Algorithmus findet den gesuchten Eintrag quadratisch schneller als ein klassischer Computer.

Der wohl berühmteste und interessanteste Quantenalgorithmus ist der Shors-Algorithmus zur Suche von Primfaktoren. Das Problem, das der Algorithmus zu lösen versucht, ist, zu einer grossen Zahl die Zerlegung in Primzahlen zu finden. Auf einem klassischen Computer steigt der Aufwand dazu exponentiell an. Das bedeutet, dass es zwar nicht unmöglich ist, die Primzahlen zu finden, dass man aber leicht die Zahl so gross machen kann, dass sämtliche Computer zusammen Jahre brauchen würden, um das Problem zu lösen. Auf diesem mathematischen Umstand basieren moderne Kryptografiealgorithmen wie der RSA-Algorithmus, der die sichere Kommunikation zwischen Banken und auf dem Internet garantiert. Peter Shor hat gezeigt, dass sein Algorithmus auf einem Quantencomputer das Problem in polynomialer Zeit lösen kann und somit ein Brechen der Codes möglich wäre.



TU Wien

Bild 3 Quantenlogik zur Implementierung des Deutsch-Josza-Algorithmus.
Zu beachten ist, dass im Gegensatz zu einem klassischen Computer die Linien nicht elektrische Leitungen sind, sondern die zeitliche Evolution eines Qubits darstellen.



TU Wien

Bild 4 Komplexitätsklassen.
Verhältnis zwischen klassischen und Quantum-Klassen. Ein Quantencomputer BQP löst sicher alle Probleme von P, und sicher keines, das sich nicht in PSPACE befindet. Wo sich aber BQP zwischen P, NP und PSPACE befindet, ist noch nicht bekannt.

Die Frage stellt sich natürlich, ob jedes Problem viel schneller mit einem Quantencomputer gelöst werden könnte. Diese Frage wurde noch nicht beantwortet und ist ein aktives Forschungsgebiet der Mathematik. Zur Charakterisierung werden die verschiedenen Probleme in Komplexitätsklassen eingeteilt (Bild 4). Die allgemeinste Klasse ist PSPACE, die alle Probleme umfasst, die polynomiale Grösse im Speicher beanspruchen. Das bedeutet, sie sind effektiv auf einem Computer programmierbar; es kann aber durchaus sein, dass die Lösung sehr lange dauert. Eine weitere Klasse ist NP, die Probleme beinhaltet, die effektiv, d.h. in polynomialer Zeit, überprüfbar sind. Die Primfaktorisierung ist genau ein solches Problem: Man kann sehr schnell überprüfen, ob die Primfaktoren in der Tat die Zahl ergeben, das Suchen der Primfaktoren ist hingegen eine sehr aufwendige Aufgabe. Eine weitere Klasse ist P, die Klasse der Probleme, die effektiv auf einem klassischen Computer gelöst werden können. Dazu gehört die Multiplikation von zwei Zahlen.

Die Klasse der Probleme, die effektiv auf einem Quantencomputer gelöst werden können, wird BQP genannt. Bis jetzt ist nur

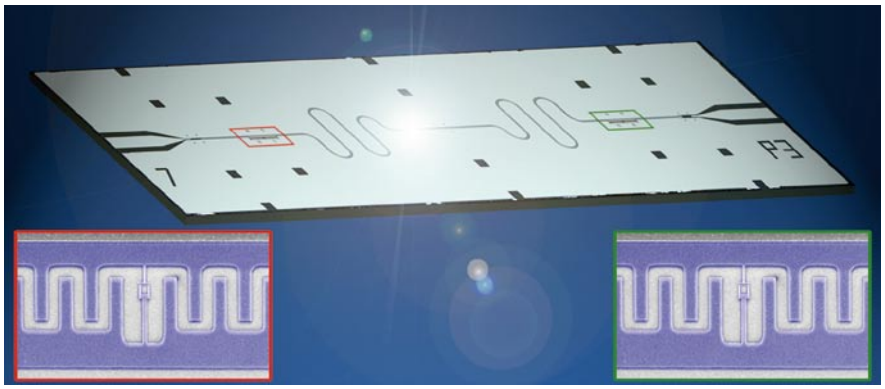


Bild 5 Supraleitender Chip.
Zwei supraleitende Qubits (roter und grüner Rahmen) koppeln durch einen supraleitenden Resonator. Die Qubits (blaue Flächen) bestehen aus Aluminium und der Resonator (grau glänzend) aus Niob. Sie werden auf einen Siliziumchip (7 × 2 mm) aufgedampft. (Quelle: Yale University)

bekannt, dass P sicher ein Teil von BQP ist, d.h., was ein klassischer Computer schnell löst, kann auch ein Quantencomputer schnell bearbeiten. Zudem kann ein Problem, das nicht zu PSPACE gehört, auch nicht von einem Quantencomputer gelöst werden: Ein Problem, das exponentiell viele Bits braucht, wird auch exponentiell viele Qubits brauchen. Wo aber BQP sich zwischen den Klassen befindet und welche Probleme zu welchen Klassen gehören, sind Fragen der aktuellen Forschung.

Technologische Realisierungen

Motiviert durch die theoretischen Möglichkeiten, versuchen heute experimentelle Forscher, den Quantencomputer zu realisieren; sie untersuchen die verschiedensten Systeme auf ihre Eignung als Qubit. Leider sind aber quantenmechanische Effekte extrem fragil. Zum Beispiel reicht für ein Qubit im optischen Bereich eine Energie von 10^{-19} Joule aus, um den Zustand zu zerstören. Der Prozess der Zerstörung des Quantenzustands wird als Dekohärenz bezeichnet, und die Kohärenzzeit misst die mittlere Zeit, in der ein Quantenzustand zerstört wird. Bei der Suche nach einem geeigneten Qubit ergeben sich leider widersprüchliche Anforderungen: Einerseits möchte man Qubits, die möglichst vom Rest der Welt entkoppelt sind und damit eine möglichst lange Kohärenzzeit aufweisen. Andererseits muss man die Qubits auch von aussen kontrollieren, um einen gewünschten Algorithmus auszuführen. Vor allem muss zum Schluss der Zustand der Qubits mit möglichst hoher Präzision gemessen werden.

Ein natürlicher Kandidat für ein Qubit ist der Kernspin eines Atoms. Im Magnetfeld hängt die Energie des Atomkerns davon ab, ob der Spin parallel oder antiparallel ausgerichtet ist. Diese zwei Zustände bilden jetzt die 0 oder die 1 eines Qubits. Durch Anlegen von Radiofrequenzfeldern kann der Zustand des Kerns kontrolliert werden. Diese Technologie wird auch in der Medizin benutzt und ist bekannt unter dem Namen Magnetic Resonance Imaging (MRI). Die verschiedenen Atomkerne eines Moleküls werden als Qubits verwendet und formen ein Quantenregister. Diese Technologie erzielt schon einige Erfolge; so wurde zum Beispiel der Shors-Algorithmus auf einem 7-Qubit-Register demonstriert. Leider stösst diese Technologie an ihre Grenzen bei der Ausdehnung auf mehr Qubits.

Eine vielversprechende Technologie sind die Ionenfallen. Ein Ion, d.h. ein geladenes Atom, kann durch elektromagnetische Felder im Vakuum gefangen werden und ist daher fast ganz entkoppelt von seiner Umgebung. Die Qubits werden in den elektronischen Zuständen der einzelnen Ionen gespeichert und können mit Laserstrahlen kontrolliert und gemessen werden. Durch die elektrostatische Wechselwirkung können die Qubits wiederum kontrolliert gekoppelt werden. Mit dieser Technologie wurde ein 8-Bit-Quantenregister demonstriert, und die Entwicklung spezieller Mikrofallen erlaubt den Ausbau zu mehr Qubits. Diese Ionenfallen-Technologie wird auch benutzt zum Bau von ultrapräzisen Atomuhren und sorgt damit für die Referenzzeit.

Eine ganz andere Technologie bilden supraleitende Schaltungen. Dabei werden mit lithografischen Methoden Schaltkreise auf einem Chip hergestellt (Bild 5) und bei tiefen Temperaturen (< 4 Kelvin) gemessen. Die Supraleitung, d.h. das Verschwinden des ohmschen Widerstands bei diesen Temperaturen, ist ein wichtiger Aspekt dieser Schaltkreise. Ohmsche Verluste und damit Dissipation bedeutet für die Qubits Dekohärenz und muss absolut vermieden werden. Der Vorteil dieser Technologie ist, dass mit Mikrotechnologie viele Qubits in einem Schritt gebaut werden können. Zudem werden die supraleitenden Qubits mit Mikrowellensignalen kontrolliert, was einfacher ist als mit Laserpulsen. Andererseits hat diese Technologie den Nachteil, dass die Kohärenzzeiten kurz sind, da die Schaltkreise aus einem Festkörper bestehen und an viele Freiheitsgrade koppeln.

Neben diesen Technologien werden weitere auf ihre Eignung als Qubits untersucht, wie Elektronenspins in Quantenpunkten, Fehlstellen in Diamanten, Atome in optischen Gittern und viele mehr. Einen vielversprechenden Ansatz bilden auch hybride Systeme, die versuchen, die Vorteile verschiedener Technologien zu kombinieren. Die aktuelle und die zukünftige Forschung werden zeigen, ob und mit welcher Technologie ein Quantencomputer gebaut werden kann.

Angaben zum Autor

Dr. *Johannes Majer* hat an der ETH Zürich Physik studiert. Nach Forschungsaufenthalten in Holland (TU Delft) und USA (Yale University) ist er jetzt wissenschaftlicher Assistent am Atominstitut der TU Wien.
TU Wien, A-1020 Wien, johannes@majer.ch, www.majer.ch/johannes

Résumé

Les ordinateurs quantiques

Quand un chiffre binaire est tant 0 que 1. Plus l'électronique est petite, plus l'influence de la physique quantique augmente. Un chiffre binaire n'est alors plus uniquement un 0 ou un 1, mais peut être quelque chose entre deux – une superposition des deux états. Sur un ordinateur classique, cela mène à la confusion, mais les chercheurs veulent maintenant exploiter les lois quantiques de manière ciblée en vue de développer des ordinateurs quantiques performants. Ceux-ci pourraient facilement déchiffrer les méthodes cryptographiques actuellement considérées comme sûres.