

*Der Gast aus der Wissenschaft*

## Von Einstein zum Quantencomputer

### Philosophische Debatte legte den Grundstein zu einer neuen Informationstechnologie

Von Anton Zeilinger

Der Streit um die philosophischen Konsequenzen der Quantentheorie ist so alt wie die Theorie selbst. Experimente, die sich damals nur in Gedanken durchspielen liessen, sind heute jedoch im Labor durchführbar. Dadurch hat man nicht nur das Wesen und die Eigenarten der Quantentheorie besser verstanden, gleichzeitig wurde auch der Grundstein zu einer neuen Informationstechnologie gelegt.

«Raffiniert ist der Herrgott, aber boshaft ist er nicht!» Mit diesen Worten charakterisierte Albert Einstein seine Kritik an der Quantenphysik oder vielmehr sein ungläubiges Staunen, wie seltsam die philosophischen Konsequenzen dieser Theorie sind. Er selbst hatte im Jahre 1905 den photoelektrischen Effekt als ein Quantenphänomen erklärt und dafür 1922 den Physik-Nobelpreis erhalten. Wenn Einstein also die Quantentheorie kritisierte, dann nicht etwa, weil sie falsch wäre in ihrer Beschreibung der Naturphänomene. Er nennt sie sogar die erfolgreichste physikalische Theorie unserer Zeit. Vielmehr waren für ihn die philosophischen Ansatzpunkte dieser Theorie nicht akzeptabel.

#### Subjektiver und objektiver Zufall

Einsteins Kritik setzt hauptsächlich an zwei Punkten an. Zum einen wollte er nicht akzeptieren, dass das quantenmechanische Einzelereignis rein zufällig ist. Er hat dies in dem berühmten Satz: «Gott würfeln nicht!» ausgedrückt. Der quantenmechanische Zufall ist von anderer Natur als der Zufall im täglichen Leben. Wenn wir einen Würfel zur Hand nehmen, so wird die erhaltene Zahlenfolge rein zufällig sein, wenn wir fair würfeln. Wir erhalten die 1 im Durchschnitt gleich oft wie die 6 und wissen im Vorhinein bei einem Wurf nicht, was die nächste Zahl sein wird. Wir können uns aber vorstellen, dass es im Prinzip für jeden einzelnen Wurf eine genaue Erklärung gäbe, wenn wir nur alle Details genau genug kennen würden, wenn wir also wüssten, in welcher Weise sich die Hand beim Wurf bewegt, wie gross der Luftwiderstand für den Würfel ist oder wie die Oberfläche des Tisches genau beschaffen ist.

In der Praxis gelingt eine solche Vorhersage jedoch nicht, da wir im allgemeinen nicht alle das Experiment beeinflussenden Parameter genau genug kennen. Man spricht hier von einem subjektiven Zufall, da es nur subjektiv unbekannt ist, was genau abläuft. Objektiv gesehen gibt es jedoch für das Ergebnis eines jeden Wurfs einen Grund, auch wenn wir diesen nicht kennen.

Anders in der Quantenphysik. Stellen wir uns etwa ein einziges radioaktives Atom vor. Von diesem Atom wissen wir, dass es irgendwann zerfallen wird, und wir können die Wahrscheinlichkeit angeben, mit der es beispielsweise innerhalb der nächsten zehn Minuten zerfällt. Der konkrete Zerfall wird jedoch zu einem bestimmten Zeitpunkt auftreten, und wir haben keinerlei Möglichkeit, diesen Zerfall vorauszusagen. Die Quantenphysik sagt, dass es für den Zeitpunkt des einzelnen Zerfalls keinerlei Grund gibt, nicht einmal einen verborgenen. Man spricht hier von objektivem Zufall. Der Zufall tritt nicht nur deshalb auf, weil wir nicht genug wissen, sondern weil kein objektiver Grund vorhanden ist. Dieser objektive Zufall ist wahrscheinlich eine der tiefsten Entdeckungen der Naturwissenschaften in unserem Jahrhundert.

#### Verschränkte Objekte

Ein zweiter Kritikpunkt Einsteins war das Verhalten sogenannter verschränkter Quantensysteme. Ein einfaches Beispiel für ein verschränktes Quantensystem sind zwei Photonen, die immer orthogonal zueinander polarisiert sind, deren elektrisches Feld also senkrecht zueinander schwingt. Wenn ein Photon horizontal polarisiert ist, dann ist das zweite immer vertikal polarisiert und umgekehrt. Die natürlichste Annahme wäre, dass die orthogonale Polarisation der beiden Photonen einfach deshalb zustande kommt, weil sie von der Lichtquelle weg bereits diese Polarisation tragen oder zumindest irgendeine Eigenschaft, die bestimmt, welche Polarisation sie bei einer Messung zeigen werden. Dies wäre etwa so zu verstehen wie die Tatsache, dass zwei identische Zwillinge deshalb dieselbe Haarfarbe haben, weil sie die gleichen Gene tragen.

Das Interessante ist nun, dass die Korrelationen zwischen unseren beiden Photonen nicht auf diese Weise verstanden werden können. Die Polarisation von keinem der beiden Photonen ist von Anfang an festgelegt: das Messergebnis für jedes der beiden ist vollkommen zufällig im Sinne des objektiven Zufalls. Wird jedoch die Polarisation des einen Photons gemessen und zeigt sich dabei zufällig ein bestimmtes Resultat, so ist damit der Zustand des anderen Photons so festgelegt, dass seine Polarisation genau das dazu orthogonale Resultat zeigen wird. Einstein hat dies als «spukhafte Fernwirkung» bezeichnet.

In den letzten beiden Jahrzehnten gab es in diesen Fragen interessante Neuentwicklungen. Experimente, die lange Zeit nur als Gedankenexperimente diskutiert werden konnten, lassen sich heute im Detail im Labor durchführen. Dadurch ist nicht nur sehr schön bestätigt worden, dass die Quantenmechanik sich anders verhält, als Einstein es gerne gesehen hätte, es wurden auch die Tore zu einer neuen Technologie aufgestossen, in der gerade die beiden von Einstein kritisierten Punkte - der objektive Zufall und die Quantenverschränkung - eine zentrale Rolle spielen. - Das im Entstehen begriffene Gebiet der Quanteninformatik beruht auf der Grundidee, Information in einzelnen Quantensystemen zu speichern. Die Gesetze der Quantenphysik ermöglichen dann neue Methoden der Informationsverarbeitung und Informationsübertragung. Die wohl faszinierendste Idee ist die der Quantenteleportation. Die Teleportation ist ein Konzept aus der Science-fiction. Dort spricht man auch vom «Beamen». Ursprünglich ging es Gene Roddenberry, dem Schöpfer der Serie «Star Trek», darum, bei seinen Filmen Produktionskosten zu sparen. Das Problem war, dass bei der Landung und dem Start auf fremden Planeten komplizierte und teure Filmaufbauten und Tricks notwendig gewesen wären. Beim filmtechnisch sehr einfachen Beamen wird auf eine nicht näher erklärte Weise das zu transportierende Objekt gescannt, so dass seine gesamte Information vorliegt. Diese Information wird dann übertragen, um das Objekt an einem anderen Ort wieder zusammenzusetzen.

Die Schöpfer von «Star Trek» hatten erkannt, dass es dabei ein grundsätzliches, durch die Quantenphysik gegebenes Problem gibt. Es ist nämlich nicht möglich, die gesamte in einem Objekt vorhandene Information durch Messung abzutasten. Dies verbietet die Heisenbergsche Unschärferelation, der gemäss es nicht möglich ist, sowohl Ort als auch Geschwindigkeit eines Teilchens gleichzeitig zu kennen. Man erfand daher den «Heisenberg-Kompensator», dessen nähere Funktion uns nicht verraten wird. Einen solchen Kompensator kann es auch nicht geben, da er den Gesetzen der Quantenphysik widerspricht.

Das Interessante an dem in meiner Arbeitsgruppe durchgeführten Experiment zur Quantenteleportation ist, dass es dieses Problem umgeht. Durch die Verwendung von verschränkten Quantenzuständen ist es möglich, Information direkt zu übertragen, ohne diese Information vorher auszulesen, ohne sie also zu scannen (siehe Kasten Quantenteleportation).

#### Rechnen mit überlagerten Zuständen

Die Quantenteleportation ist nicht nur ein faszinierendes fundamentales Konzept, sie wird auch als einer der Mechanismen diskutiert, mit dem künftige Quantencomputer Informationen austauschen, also miteinander sprechen könnten. Bei diesen Quantencomputern ist nicht mehr das klassische Bit mit seinen Werten 0 oder 1 der Träger der Information. Das zentrale Element in einem Quantencomputer ist vielmehr das Quantenbit, auch Qubit genannt. Das Qubit wird durch ein physikalisches System repräsentiert, das sich in zwei Zuständen (0 oder 1) befinden kann. Zusätzlich - und das ist das wesentlich Neue an Quantencomputern - kann ein Qubit auch in der Überlagerung beider Möglichkeiten existieren. Dies bedeutet letztlich, dass man einen Quantencomputer mit einer Überlagerung von verschiedenen Eingabedaten füttern kann. Während ein gewöhnlicher Computer die Eingabedaten der Reihe nach bearbeitet, rechnet ein Quantencomputer mit den überlagerten Daten. Gewissermassen bearbeitet er alle Eingabedaten zugleich. Die Entdeckung zweier Algorithmen, die auf einem Quantencomputer sehr viel schneller ablaufen würden als auf einem klassischen Computer, hat dazu beigetragen, dass die Quanteninformatik in den letzten Jahren enorm an Schwung gewonnen hat.

Der erste Algorithmus wurde von dem Mathematiker Bruce Shor entdeckt. Es geht hier um die Zerlegung grosser Zahlen in ihre Primfaktoren. Ein einfaches Beispiel ist die Zerlegung der Zahl 6 in die Zahlen 2 und 3. Versucht man Probleme dieser Art auf einem herkömmlichen Computer zu lösen, wächst der Rechenaufwand exponentiell mit der Grösse der Zahl, die man in ihre Primfaktoren zerlegen möchte. Dies macht man sich heute in der Kryptographie zunutze, indem man zur Verschlüsselung einer geheimen Nachricht eine sehr grosse Zahl verwendet. Nur wer die

Primfaktoren dieser Zahl kennt, kann die Nachricht entschlüsseln. Die Zahlen sind so gross, dass kein existierender Computer das Problem in vernünftiger Zeit lösen kann, womit die Verschlüsselung de facto sicher ist.

Shor konnte nun zeigen, dass in einem Quantencomputer die Rechendauer zwar nach wie vor mit der Grösse der zu faktorisierenden Zahl steigt, jedoch sehr viel langsamer als mit einem klassischen Computer - womit das Problem auch für grosse Zahlen handhabbar wird. Sollte also ein Quantencomputer je verwirklicht werden, wären viele Verschlüsselungssysteme sofort obsolet. Der zweite Algorithmus wurde von Lov Grover von den Bell-Laboratorien entdeckt. Hier geht es darum, aus einem grossen Datensatz jene Elemente herauszusuchen, die eine bestimmte, einmalige Eigenschaft tragen. Dies ist etwa bei der Suche in Bibliotheksverzeichnissen notwendig. Ein klassischer Computer arbeitet die Einträge der Reihe nach ab. Ein Quantencomputer kann dagegen eine Überlagerung aller Elemente gleichzeitig untersuchen und kommt so viel schneller ans Ziel.

Wie weit steht es nun mit der Entwicklung des Quantencomputers? Es gibt hier mehrere hochinteressante Vorschläge. So können beispielsweise einzelne Ionen Träger der Quanteninformation sein. Diese Ionen werden in geeigneten elektrischen und magnetischen Feldern eingefangen. Sie können miteinander «sprechen», da sie sich elektrisch abtasten und die Bewegung eines Ions sich auf Nachbarionen übertragen kann. Durch winzige Laser, die jeweils ein einzelnes Ion adressieren, lassen sich von aussen Informationen auf die Qubits übertragen. Die experimentelle Entwicklung hinkt hier aber weit hinter den theoretischen Ideen her. Man kann zwar Ionen in Fallen einfangen. Jedoch ist es noch niemandem gelungen, mehrere Ionen in einen verschränkten Quantenzustand zu bringen. Das aber wäre nötig, wenn man tatsächlich mit den Ionen rechnen wollte.

Weiter fortgeschritten sind die Versuche, einen

rudimentären Quantencomputer mit den Methoden der Kernresonanzspektroskopie zu realisieren. Hier treten die einzelnen Atomkerne von grösseren Molekülen als Träger der Qubits auf. Von aussen kommuniziert man mit diesen Atomkernen, indem man sie hochfrequenten elektromagnetischen Feldern aussetzt. Die in einem Molekül befindlichen benachbarten Atomkerne können untereinander wechselwirken und damit Quanteninformation austauschen. Mit Hilfe solcher Methoden gelang es verschiedenen Forschergruppen, einfache Modelle eines Quantencomputers mit drei oder vier Qubits zu realisieren und ihre Funktionsweise zu demonstrieren. Diese Erfolge dürfen aber nicht darüber hinwegtäuschen, dass man sich beim Quantencomputer immer noch auf der elementarsten Stufe befindet.

Langfristig wird es wohl bedeutsam sein, ob es gelingen wird, Quantencomputer im Festkörper zu realisieren, womit der Quantencomputer auf einer ähnlichen Technologie basieren würde wie unsere derzeitigen Computer, nämlich auf der Basis von Chips. Hier gibt es zahlreiche Vorschläge, z. B. den des Australiers Bruce Kane, der als Qubits einzelne Phosphoratomkerne nimmt, die an ganz bestimmte Stellen in hochreinem Silizium implantiert werden. Diese Phosphoratomkerne entsprechen im Prinzip den Ionen in Ionenfallen. Andere Forscher geben sogenannten Quantenpunkten den Vorzug. Das sind kleine Halbleiterbereiche, in denen der Bewegungsspielraum von Elektronen räumlich so beschränkt ist, dass sie Quanteneigenschaften annehmen. Auch die Möglichkeit, mit sogenannten Josephson-Kontakten in Supraleitern zu rechnen, wird in Betracht gezogen.

#### Hürden zum Quantencomputer

Eine wesentliche Frage bei der Realisierung von Quantencomputern wird sein, ob es gelingt, das Problem der sogenannten Dekohärenz in den

Griff zu bekommen. Jedes Quantensystem ist nämlich ausserordentlich empfindlich gegenüber Störungen durch die Umgebung, wodurch es sehr leicht seine Quanteneigenschaften verliert. An Wechselwirkung mit der Umgebung reicht oft schon die Temperatur des Systems. Man muss einen Quantencomputer voraussichtlich bei tiefen Temperaturen betreiben und sehr gut gegenüber den elektrischen und magnetischen Störfeldern der Umgebung abschirmen. Dies ist um so aufwendiger, je mehr Qubits verwendet werden.

Während es heute vollkommen offen ist, ob diese Probleme überwunden werden können, hat sich in den letzten zwei bis drei Jahren ein intensiver Wettbewerb auf diesem Gebiet entwickelt, wobei gerade die USA imstande sind, Summen zu investieren, mit denen Europa nicht mithalten kann oder nicht mithalten will. Die Europäische Kommission hat kürzlich ein entsprechendes Programm gestartet, wobei das zur Verfügung gestellte Geld im Vergleich zu den amerikanischen Investitionen nur als ein «Tropfen auf den heissen Stein» angesehen werden kann. Es ist zu befürchten, dass in Europa zwar einige wesentliche Grundgedanken einer neuen Technologie entwickelt wurden, der Gewinn aber woanders gemacht wird.

Es ist meine persönliche Überzeugung, dass dieses Gebiet der Quanteninformatik zu revolutionär neuen Methoden der Informationsverarbeitung und Informationsübertragung führen wird, wobei wahrscheinlich die heutigen Konzepte noch zu konservativ sind, das heisst noch zu sehr angelehnt sind an die uns bekannten Ideen, was «computation» bedeutet. Die wirklich neuen Ideen, die die Eigenschaften der Quantenphysik voll ausnützen und damit auch beträchtlich über Einstein hinaus gehen werden, stehen uns wahrscheinlich noch bevor.

### *Teleportation von Quanten*

A. Z. Die beiden Mitspieler bei der Teleportation heissen Alice und Bob, nach den ersten beiden Buchstaben des Alphabets. Alice besitzt ein Photon (C), dessen Polarisation sie nicht kennt. Sie möchte, dass Bob ein Photon in genau demselben Quantenzustand erhält. Die Übertragung der unbekanntenen Information erfolgt unter Zuhilfenahme eines verschränkten Photonenpaares. Das eine der beiden Photonen (A) befindet sich im Besitz von Alice, das andere (B) im Besitz von Bob. Wie es der Natur eines verschränkten Zustandes entspricht, ist vor einer Messung keine der beiden Polarisationen festgelegt. Alice unterzieht nun das zu teleportierende Photon C und das Photon A einer gemeinsamen Messung, bei der nun auch diese beiden Photonen miteinander verschränkt werden. In einem von vier Fällen ist die Verschränkung derart, dass die beiden Photonen orthogonal zueinander polarisiert sind. Alice teilt Bob über das Telefon oder andere Informationskanäle mit, wann dies der Fall ist. Da nun das Photon B orthogonal zum Photon A und das Photon A orthogonal zum Photon C polarisiert ist, hat man automatisch erreicht, dass Bobs Photon B identisch mit dem vernichteten Original C ist. Da weder Alice noch Bob irgendeine Information über den genauen Zustand, also die genauen Eigenschaften der Photonen erhalten haben, lässt sich das Problem mit der Heisenbergschen Unschärferelation umgehen.

**Der Autor**

zz. Anton Zeilinger, geboren 1945 in Oberösterreich, studierte an der Universität Wien und promovierte 1971 mit einer Arbeit über festkörperphysikalische Untersuchungen mit Neutronen. Als Assistent am Atominstitut der österreichischen Universitäten interessierte er sich bald für das dort unter Helmut Rauch entwickelte Neutroneninterferometer und die damit möglichen fundamentalen Experimente zur Quantenmechanik. Nach seiner Habilitation an der Technischen Universität Wien war Zeilinger von 1981 bis 1983 Associate Professor am Massachusetts Institute of Technology, dann ausserordentlicher Professor an der Technischen Universität Wien. 1990 wurde er ordentlicher Professor an der Universität Innsbruck. Neun Jahre später kehrte er an das Institut für Experimentalphysik an der Universität Wien zurück. Seine Forschungstätigkeit konzentriert sich auf Experimente mit Photonen, Neutronen, Atomen und - seit kurzem - grossen Molekülen. Ziel dieser Experimente ist es, die Grundlagen der Quantenphysik zu verstehen. Für weltweites Aufsehen sorgte die erste Realisierung der Quantenteleportation.