Quanteninformation

# Mit Quanten ist zu rechnen

## Von der Quantenphysik zur Quanteninformation: eine Einführung

Dominik Janzing

**Die Quantentheorie hat unzweifelhaft Physik und Technik revolutioniert und ebenso tiefschürfende Fragen in der Mathematik und Philosophie aufgeworfen. Mit dem Konzept des Quantencomputers erhält nun auch die Informatik neue Impulse. Die quantenmechanischen Gesetze erlauben nämlich grundsätzlich neuartige Ansätze, um Probleme zu knacken, für die auf klassischen Computern bislang kein effizientes Lösungsverfahren bekannt ist.**


Selbst Albert Einstein, der sonst sicher nicht gerade davor zurückschreckte, gewohntes Denken über Bord zu werfen, glaubte bis zu einem Lebensende nicht daran, dass auf der untersten Ebene der Natur ein „absoluter Zufall“ existieren soll, der nicht auf unserer Unfähigkeit beruht, die zugrunde liegenden Gesetzmäßigkeiten zu erfassen. Aus dem Unbehagen gegenüber der Quantenmechanik heraus präsentierten Albert Einstein, Boris Podolsky und Nathan Rosen 1935 ein Gedankenexperiment, das später als EPR-Paradox bekannt wurde. Einstein und seine Koautoren wollten damit zeigen, welche „absurden“ Effekte die Quantenmechanik, speziell das Phänomen der quantenmechanischen *Verschränkung*, implizieren würde. Im Jahre 1964 gelang John Bell der mathematische Beweis dafür, dass sich der Zufall der Quantenmechanik in geeigneten Experimenten messbar von dem gewohnten Zufall, der durch unsere Unkenntnis erzeugt wird, unterscheiden sollte, da Quanten-Zufall zu einer veränderten Statistik führen würde (siehe Infokasten „Die Bellsche Ungleichung“). In wegweisenden Experimenten, unter anderem dem bekannten Versuch von Alain Aspect und seinen Mitarbeitern im Jahre 1981, wurde eine solche veränderte Statistik nachgewiesen.[1)]

Angesichts der Bedeutung der Quantentheorie für Physik, Mathematik und Philosophie erstaunt es, dass Implikationen von Quanteneffekten für Grundannahmen der Informatik erst im vergangenen Jahrzehnt klar wurden: So muss man, um den Rechenaufwand zur Lösung eines Problems abzuschätzen, Annahmen darüber zugrunde legen, über welche Grundoperationen der Rechner verfügt, d. h., was als *ein Rechenschritt* zu werten ist. Diese Annahmen bilden das so genannte abstrakte *Rechnermodell*. Damit hängen Abschätzungen darüber, wie aufwändig die Lösung eines Problems ist, natürlich von dem zugrundeliegenden Modell ab. Nun hat sich aber in der Informatik eine vergröberte Sichtweise bewährt, bei der der Rechenaufwand nicht aufgrund der genauen Anzahl der Rechenschritte beurteilt wird, sondern nur qualitativ untersucht wird, wie die Anzahl der Rechenschritte mit der Anzahl der Eingabebits wächst. So werden z. B. Probleme, deren Rechenaufwand nur wie ein Polynom wächst, in der Informatik als „gutartig“ betrachtet und als in der Regel mit vernünftigem Zeitaufwand lösbar. Diese vergröberte Sichtweise bei der Aufwandsabschätzung erwies sich als unglaublich unempfindlich gegenüber einer Veränderung des Rechnermodells. Daher darf Aufwandsabschätzungen trotz des rasanten Fortschritts in der Computertechnologie bis heute ein Rechnermodell zugrunde gelegt werden, das von Alan Turing bereits 1936 formuliert wurde, die so genannte *Turing-Maschine*. Es galt als ein Postulat der Informatik, dass sich jedes Problem, für das auf der Turing-Maschine kein Programm mit höchstens polynomialem Aufwand existiert, auch auf keinem anderem sinnvollem Rechnermodell „gutartig“ verhält.

Daher war es eine Sensation, als Peter Shor im Jahre 1994 einen „gutartigen“ Algorithmus zur Faktorisierung großer Zahlen in Primzahlen präsentierte, denn für die klassische Turing-Maschine ist kein Algorithmus bekannt, bei dem die Laufzeit nur polynomial wäre. Shor legte diesem Algorithmus ein Modell eines Rechners zugrunde, der quantenmechanische Überlagerungen

1) Da man prinzipiell jedoch gewisse bei der Auswertung der experimentellen Daten notwendige Annahmen anzweifeln kann, wurden auch später weitere Experimente durchgeführt, die diese Zweifel noch abschwächen konnten.

**Dr. Dominik Janzing, Institut für Algorithmen und Kognitive Systeme, Arbeitsgruppe Quantum Computing, Universität Karlsruhe, Am Fasanengarten 5, 76131 Karlsruhe**

 1617-9439/05/1111-25

zwischen verschiedenen Zuständen des Registers erlaubt. Mit einem solchen Quantenrechner könnten – so die Hoffnung – manche Probleme gutartig sein, für die ein klassischer Computer astronomische Laufzeiten benötigen würde.

## Eine neue Art der Information

Doch nicht nur das Rechnermodell der klassischen Informatik wird in neuerer Zeit in Frage gestellt, es wurde auch klar, dass Quantensuperpositionen eine neue Art von Information beinhalten. Bis dahin galt es als selbstverständlich, dass jede Information in Bit gemessen werden kann, unabhängig vom physikalischen Träger. Es war Shannons Verdienst, eine Hardware-unabhängige mathematische Theorie der Information zu formulieren. Erst in den 80er- und 90er-Jahren setzte sich die Ansicht durch, dass sich der Informationsgehalt eines Quantensystems nicht durch Bits ausdrücken lässt. Stattdessen wurde der Begriff Quantenbit („Qubit“) geschaffen, eine Einheit für eine Art von Information, welche sich prinzipiell nicht kopieren lässt, da sie bei jedem solchen Versuch zumindest teilweise zerstört würde[2)]. Diese Tatsache kann sich die Quantenkryptographie zunutze machen, bei der ein Spion entdeckt werden kann, weil er den Quantenzustand verändert, über den er Information gewinnt. Realisierungen quantenkryptographischer Protokolle liegen bereits vor, wie der Artikel von Dagmar Bruß und Harald Weinfurter detailiert beschreibt.

2) vgl. den Infokasten „No-Cloning-Theorem“ im Artikel von Dagmar Bruß und Harald Weinfurter.

Die Quanteninformationstheorie versucht nun (ebenso wie die klassische Informatik), Merkmale von Information und ihrer Verarbeitung aufzudecken, die unabhängig von dem betrachteten physikalischen System sind. Dabei entstanden Gedankenexperimente und mathematische Fragestellungen, die von ihrer Struktur her so erstaunlich einfach sind, dass es verwundert, dass sie erst ein knappes Jahrhundert nach der Entwicklung der Quantenmechanik aufkamen.

### Die Bellsche Ungleichung

Die Bellsche Ungleichung beschreibt ein Experiment, bei dem zwei räumlich voneinander getrennte Empfänger Alice und Bob je ein Qubit eines verschränkten Paares erhalten und jeder der beiden Empfänger eine beliebige Messung an seinem Qubit durchführt, deren Ergebnisse $\pm 1$ seien. Sei nun $C_{a,b}$ der Erwartungswert der Resultate von Alice und Bob, wenn $a$, $b$ die dazugehörigen Messrichtungen sind. Eine solche Messrichtung entspricht der Wahl zweier gegenüberliegender Punkte auf der Bloch-Kugel. Bell erkannte nun folgendes Merkmal klassischer Statistik: Angenommen, zu dem Zeitpunkt, zu dem der verschränkte Zustand präpariert wurde, würde eine verborgene physikalische Größe bereits festlegen, mit welchem Ergebnis Alice (unabhängig von Bobs Entscheidung) zu rechnen hätte, wenn sie eine Messung $a$ durchführte, und ebenso wäre das Ergebnis von Bob schon durch die verborgene Variable festgelegt. Dann wäre folgende Ungleichung erfüllt:

$$C(a_1,b_1) + C(a_1,b_2) + C(a_2,b_1) - C(a_2,b_2) \leq 2 \ ,$$

wobei $a_1, a_2$ und $b_1, b_2$ jeweils zwei mögliche Messrichtungen bezeichnen. Die Annahmen drücken aus, was man von einer klassisch-relativistischen physikalischen Theorie erwartet, falls Alice und Bob ihre Messungen so kurz hintereinander durchführen, dass kein Signal als Folge von Alices Messung das Resultat von Bob beeinflussen kann oder umgekehrt. Klassisch sollte dann nämlich gelten:

▶ 1) Die aktuellen Werte aller physikalischen Größen nach dem Zeitpunkt der Präparation legen den Ausgang jedes künftigen Experiments fest.

▶ 2) Damit Alices Experiment Bobs Resultat beinflussen könnte, müsste ein physikalisches Signal diese Wirkung übertragen, das sich jedoch höchstens mit Lichtgeschwindigkeit bewegt.

Bell erkannte, dass die nach ihm benannten Bell-Zustände nach der Quantentheorie für den obigen Ausdruck $2\sqrt{2}$ liefern müssten. Im Einklang damit haben inzwischen zahlreiche Experimente Werte größer als 2 geliefert.

## Das Qubit

Das Quantenbit (Qubit) ist die Abstraktion eines Quantensystems, das zwei voneinander unterscheidbare Zustände einnehmen kann. Diese werden durch $|0\rangle$ und $|1\rangle$ beschrieben und bilden eine Basis im Vektorraum $\mathbb{C}^2$. Sie können z. B. die Zustände „Spin up“ und „Spin down“ eines Spins sein oder zwei Energieniveaus eines Atoms. Nun sind aber auch beliebige Überlagerungen erlaubt, also komplexe Linearkombinationen

$$c_0|0\rangle + c_1|1\rangle ,$$

die einen Vektor der Länge eins ergeben. Vektoren, die nur durch Multiplikation mit einer komplexen Zahl auseinander hervorgehen, repräsentieren dabei physikalisch denselben Zustand. Aufgrund dieser Vieldeutigkeit charakterisiert man die gesamte Menge der Zustände des Qubits besser als Punkte auf einer dreidimensionalen Kugeloberfläche (der „Bloch-Kugel“), wobei Nordpol und Südpol die beiden logischen Zustände $|0\rangle$ und $|1\rangle$ darstellen. Drückt man die Lage eines Punktes durch den Längengrad $\theta$ zwischen –180° und 180° und den Winkel zum Nordpol $\phi$ aus, so entspricht dieser dem Zustand

$$\cos(\phi/2)\,|0\rangle + \sin(\phi/2)\,e^{i\theta}|1\rangle \ .$$

Beim Spin z. B. gibt die Lage des Punktes auf der Kugel gerade die Orientierung der „Magnetnadel“ (wenn man sich den Spin als solchen vorstellen will) im dreidimensionalen Raum an.

Das System weist also ein Kontinuum an möglichen Superpositionszuständen auf, aber nur jeweils zwei gegenüberliegende Punkte lassen sich mit Sicherheit unterscheiden, falls man die Vorabinformation hat, dass einer dieser beiden vorliegt. Dann lässt sich nämlich eine Messung wählen, die eben gerade diese beiden Alternativen unterscheidet. Wenn keine solche Vorabinformation vorhanden ist, lassen sich aus dem Messergebnis nur Wahrscheinlichkeitsaussagen über den Zustand vor der Messung ableiten. Liegt der wirkliche Zustand z. B. $\phi = 60^\circ$ vom Nordpol weg und führt man eine Messung durch, die dazu geeignet wäre, Nordpol und Südpol zu unterscheiden, so erhält man mit Wahrscheinlichkeit $\cos^2 30^\circ$ das Resultat „Nordpol“ und mit $\sin^2 30^\circ$ das Ergebnis „Südpol“. Nach der Messung liegt dann auch der entsprechende Zustand vor. Wendet man hingegen eine Messung, die zwei andere gegenüberliegende Punkte, z. B. auf dem Äquator, unterscheiden kann, auf ein System an, das sich am Nordpol oder am Südpol befindet, so liefert sie nicht nur keine sichere Information mehr über Nord oder Süd, sie zerstört darüber hinaus auch noch die anfangs vorliegende Information.

## Quantenregister

Obwohl sich der Zustand eines Qubits durch die Lage eines Punktes auf einer Kugel angeben lässt, kann man den Zustand von zwei Qubits nicht durch die Lage von zwei Punkten auf zwei Kugeln beschreiben. Das liegt daran, dass nicht nur jedes Qubit für sich Superpositionen von $|0\rangle$ und $|1\rangle$ zulässt, sondern auch Superpositionen von *Zustandskombinationen*. Zwei Qubits können auch gemeinsam in einer Überlagerung aus $|00\rangle$ und $|11\rangle$ sein, wobei der Zustand jedes einzelnen Qubits gar nicht definiert ist. Wäre jedes Qubit für sich in einer Überlagerung aus $|0\rangle$ und $|1\rangle$, so würde man bei Messungen beider Qubits alle vier Ergebnisse 00, 01, 10, 11 erhalten, wogegen bei der Superposition aus $|00\rangle$ und $|11\rangle$ eben nur diese beiden Binärstrings als Ergeb-

nis möglich sind. Solche Superpositionen aus Zwei-Bit-Kombinationen hat man z. B. bei den Bell-Zuständen

$$|\Phi^{\pm}\rangle := (1/\sqrt{2})\,(|00\rangle \pm |11\rangle)$$
$$|\Psi^{\pm}\rangle := (1/\sqrt{2})\,(|01\rangle \pm |10\rangle)\,.$$

Liest man in einem dieser Zustände nur das linke Qubit aus, so erhält man mit Wahrscheinlichkeit 1/2 jeweils 1 oder 0, kennt dann aber gleichzeitig auch den Wert des anderen Qubits. Dies ist zunächst kein Unterschied zu einem klassischen Zufallsexperiment, bei dem man einen Zufallsgenerator beispielsweise entscheiden lässt, ob sich das Register im Zustand 11 oder 00 befinden soll: Sobald man den Wert des einen Bits kennt, ist der des anderen ebenso klar. Wenn man aber dem Zustandsvektor (der „Wellenfunktion“) eine direkte physikalische Realität zuweist, anstatt ihn als ein mathematisches Objekt anzusehen, welches Wahrscheinlichkeiten potenzieller Messresultate repräsentiert, so erscheint es als „mysteriöse Fernwirkung“, wenn durch Messen des einen Qubits sich der Zustand des anderen ändert. Dies war eben gerade der Standpunkt, von dem aus das „EPR-Paradox“ erst zum Paradox wurde. Diese Paradoxie beeindruckt insbesondere dann, wenn man sich vorstellt, dass die beiden Qubits weit voneinander entfernt sind und die Messung an einem Qubit dann instantan den Zustand des anderen Qubits festlegt.

Allgemein kann ein Register aus $n$ Qubits in einer Superposition aller $2^n$ möglichen $n$-Bit-Strings $b$ sein,

$$\Sigma_b\, c_b |b\rangle\,,$$

wobei die $c_b$ komplexe Zahlen sind, deren Betragsquadrat in der Summe eins ergibt und $|b\rangle$ der Zustand zum Binärwort $b$ ist. Alle Zustandsvektoren dieses Systems, die sich nicht durch die Zustände ihrer $n$ Qubits beschreiben lassen, nennt man *verschränkte* Zustände. Mathematisch sind dies diejenigen Vektoren, die sich nicht als ein Tensorprodukt der Form

$$|\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle$$

schreiben lassen, wobei jedes $|\psi_j\rangle$ ein beliebiger Superpositionszustand eines Qubits ist.

## Quantengatter

In der klassischen Schaltungstechnik stellt man sich logische Gatter wie UND, ODER, NICHT, NOR, NAND in der Regel als *Bauteile* mit Eingabe- und Ausgabedrähten vor. Im Quantencomputing hingegen existieren logische Operationen nur als *Prozesse*, bei denen die Eingabe in die Ausgabe transformiert wird. Der Grund ist, grob gesagt, dass Eingabe und Ausgabe nicht gleichzeitig existieren können, da dies zumindest teilweise ein faktisches Kopieren der Information beinhalten würde.[3)] Quantengatter führen eine Superposition in eine andere über. Ein wichtiges Gatter, das auf zwei Qubits wirkt, ist das so genannte Controlled-NOT (CNOT), das den Wahrheitswert des eines Qubits invertiert, wenn das andere Qubit gesetzt ist. Eine andere wichtige Klasse von Gattern ist durch die Drehungen auf der Bloch-Kugel gegeben, die sog. Ein-Qubit-Gatter.

Es wurde bewiesen, dass sich jeder mögliche Prozess auf $n$ Qubits als Hintereinanderausführung von CNOT-Gattern und solchen Ein-Qubit-Gattern zusammensetzen lässt, wenn die CNOT-Gatter auf beliebige Qubit-Paare und die Ein-Qubit-Gatter auf beliebige Qubits wirken können. Dieses Zusammensetzen einer beliebigen $n$-Qubit-Transformation aus einfachen elementaren Gattern kann man sich in Analogie zur klassischen Schaltungstechnik vorstellen, in der sich jede Boolesche Funktion aus NOR- oder aus NAND-Bausteinen zusammensetzen lässt.

## Was ist eigentlich ein Quantenalgorithmus?

Ein Quantencomputer führt eine Überlagerung verschiedener Binärstrings als Eingaben in eine Überlagerung der entsprechenden Ausgaben über. Betrachten wir z. B. eine Boolesche Funktion $f$ mit einer $n$-stelligen Eingabe und einer $k$-stelligen Ausgabe, so kann man aus Quantengattern einen Prozess erzeugen, der auf einem Register aus $n+k$ Qubits den Zustand

$$|b, 0, \ldots\, 0\rangle$$

in den Zustand

$$|b, f(b)\rangle$$

überführt. Ein solcher Prozess würde aber auch den Überlagerungszustand

$$\Sigma_b\, c_b\, |b, 0, \ldots\, 0\rangle$$

auf den Zustand

$$|\psi\rangle := \Sigma_b\, c_b\, |b, f(b)\rangle$$

abbilden. Interessanterweise enthält nun, falls alle Koeffizienten $c_b$ ungleich null sind, der Quantenzustand $|\psi\rangle$ die Information über alle Funktionswerte $f(b)$. Es scheint so, als ob man sich daher mit einem Quantencomputer alle Ergebnisse mit demselben Rechenaufwand beschaffen könne, der sonst für die Berechnung eines einzigen Wertes nötig wäre. Wäre z. B. $f$ die Funktion mit einer einstelligen Ausgabe, die testet, ob eine Zahl eine Primzahl ist oder nicht, so enthielte der Überlagerungszustand die gesamte Information darüber, welche Zahl zwischen 0 und $2^n-1$ prim ist.

Die Frage ist aber, welchen Nutzen eine Überlagerung vieler Ausgaben tatsächlich hat, schließlich „entscheidet“ sich das Register beim Auslesen doch nur für einen bestimmten Binärstring. Ebenso wie man noch nicht einmal bei einem Qubit die Lage des Vektors auf der Kugeloberfläche bestimmen kann, sondern bei der üblichen Messung, die nur Nord- und Südpol (also $|0\rangle$ bzw. $|1\rangle$) unterscheidet, mit einer gewissen Wahrscheinlichkeit einen dieser Zustände erhält, liefert das Auslesen des Registers nur eine der möglichen Ausgaben, sodass man also im Endeffekt doch nur *einen* Funktionswert berechnet hätte. Das könnte man auch einfacher erreichen, indem man die Eingabe $b$ eines klassischen Rechners zufällig wählt und dann auch zufällig die Ausgabe $f(b)$ dazu erhält. Ein Quantenalgorithmus wird daher nicht damit enden, einfach einen Überlagerungszustand herzustellen, der Information über viele Funktionswerte gleichzeitig enthält. Er wird vielmehr weitere Transformationen auf eine solche Überlagerung anwenden, um die darin enthaltene Information auf subtilere Weise ins Endergebnis einfließen zu lassen.

Allerdings scheint es schwer, ein allen Quantenalgorithmen zugrunde liegendes gemeinsames Prinzip zu formulieren, das erklärt, warum diese effizienter sein können als klassische Algorithmen und warum Superpositionen verschiedener logischer Zustände tatsächlich nützen können. Hierüber ist noch recht wenig bekannt, da wohl noch zu wenige Beispiele für Algorithmen existieren. Wäre dieser Punkt wirklich verstanden, ließe sich sicher auch besser abschätzen, für welchen Typ von mathematischen Problemen noch leistungsfähige Quantenalgorithmen zu erwarten sind.

3) Etwas präziser gesagt würde ein Quantengatter, bei dem Eingabe- und Ausgabequbits gleichzeitig existieren, zu einer Verschränkung von Eingabe- und Ausgaberegister führen, bei der der quantenmechanische Zustand des Ausgaberegisters alleine nicht mehr definiert ist.

Dennoch kann eine Analogie helfen, das Besondere eines Quantenalgorithmus zu verstehen. Bei Interferenzexperimenten an einem Doppelspalt oder einem Gitter aus sehr vielen Spalten (sei es mit Schrödinger-Wellen oder mit klassischen Wellen) wird die Intensität der an einem bestimmten Punkt auf dem Schirm ankommenden Welle durch die Lage *aller* Spalte mitbestimmt, d. h. *alle möglichen Wege* gehen in das Interferenzmuster ein. Ähnlich kann beim Quantencomputer das Endergebnis durch viele potenzielle Zwischenergebnisse bestimmt werden, die für manche potenzielle Endergebnisse destruktiv und für manche konstruktiv interferieren. Im Quantencomputer können nun aber eine sehr große Zahl solcher Zwischenergebnisse interferieren, da die Anzahl der möglichen Basiszustände exponentiell in der Anzahl der Qubits wächst. Dies ist der entscheidende Unterschied zu einem Interferenzexperiment mit einer klassischen oder einer Schrödinger-Welle im dreidimensionalen Raum, bei der die Anzahl der potenziellen Pfade nicht exponentiell mit dem zur Verfügung stehenden Platz anwachsen kann. Die Leistungsfähigkeit des Quantencomputers besteht also gerade darin, dass seine Wellenfunktion nicht durch $n$ Wellenfunktionen seiner $n$ Qubits beschrieben werden kann ebenso wie der quantenmechanische Zustand von zwei Elektronen nicht durch *zwei* Wellenfunktionen im dreidimensionalen Raum, sondern durch *eine* Funktion im sechsdimensionalen Raum beschrieben wird. Dieses Verhalten von Quantensystemen bei der Zusammensetzung von Teilsystemen hat keine Entsprechung bei klassischen Wellenphänomenen.

## Dekohärenz und Fehlerkorrektur

Eine wichtige Eigenschaft einer quantenmechanischen Superposition ist die *Phase*. So ist z. B. bei einem Qubit jeder Vektor der Form

$$|\phi\rangle = (1/\sqrt{2})\,(|0\rangle + e^{i\phi}|1\rangle)$$

für jede Phase $\phi$ eine erlaubte Superposition und für Phasen mit Phasenbeziehung $\phi_2 = \phi_1 + 180^\circ$ erhält man wieder zwei mit Sicherheit unterscheidbare Zustände $|\phi_1\rangle$ und $|\phi_2\rangle$. Somit ist die Phase eine reale physikalische Eigenschaft. Wechselwirkungen eines Qubits mit seiner Umgebung führen oft unerwünschterweise dazu, dass die Phase auf unbekannte Art verändert wird. Dieses Phänomen heißt Dekohärenz. Nun verhält sich aber ein Zustand mit unbekannter Phase bezüglich jedes Experiments genauso, als ob man mit jeweils Wahrscheinlichkeit 1/2 einen der Zustände $|0\rangle$ und $|1\rangle$ vorliegen hätte. Dies ist z. B. auch der Fall, nachdem man gemessen hat, ob $|0\rangle$ oder $|1\rangle$ vorliegt. Paradoxerweise ist also ein Superpositionszustand mit unbekannter Phase gar kein Superpositionszustand mehr. Die Dekohärenz ist daher ein zentrales Problem für das Quantencomputing, und die große Herausforderung besteht demnach darin, Superpositionen aufrecht zu erhalten – zumindest auf der Zeitskala, in der die Implementierung der Gatter abläuft. Die vielen Vorschläge für die physikalische Umsetzung von Qubits konzentrieren sich deshalb darauf, diese durch recht gut isolierbare Quantensysteme zu repräsentieren. Darüber hinaus muss ein Quantensystem aber auch noch andere Bedingungen erfüllen, um für die Implementierung eines Quantencomputers in Betracht zu kommen (vgl. Infokasten „Die Kriterien von DiVincenzo“).

Um einen Quantencomputer unempfindlicher zu machen gegenüber solchen Störungen von außen, kann die Information eines Qubits so in mehreren physikalischen Systemen gemeinsam repräsentiert werden, dass sich der ursprüngliche Zustand wiederherstellen lässt, wenn eines der Systeme durch die Umgebung gestört wird. Dieser Ansatz unterscheidet sich zunächst nicht von klassischen Methoden des fehlertoleranten Rechnens. Nun muss man aber bei der Quantenfehlerkorrektur die Teilsysteme auf eine Weise überprüfen, die zwar Aufschluss darüber gibt, welche *Veränderung* der Fehler herbeigeführt hat, nicht aber darüber, in welchem logischen Zustand sich das Qubit befindet oder befand. Mitte der 90er-Jahre gelang es tatsächlich, Quantencodes anzugeben, bei denen gerade solche Messungen möglich sind.

## Die Bausteine für ein ehrgeiziges Fernziel

Das Ziel, einen Quantencomputer zu realisieren, hat vielfältige interdisziplinäre Forschungen losgetreten, die sich der Herausforderung widmen, geeignete Hardware zu finden. Ignacio Cirac und Peter Zoller, die selbst wichtige Grundlagen der Quanteninfomationsverarbeitung gelegt haben, behandeln in ihrem Artikel, wie sich Quantenrechnungen prinzipiell in quantenoptischen Systemen implementieren lassen. Sie stellen auch Konzepte für „Vorläufer“ von Quantencomputern vor, die interessante Anwendungen versprechen: Quantensysteme, die so flexibel kontrollierbar sind, dass sie zur Simulation anderer Quantensysteme geeignet sind, könnten bei der Erforschung komplexer Systeme hilfreich sein.

Zu den derzeit am intensivsten untersuchten Systemen gehören eingesperrte Atome oder Ionen. Welchen Stand die Versuche erreicht haben, um mit Ionen in Fallen die Bauteile des Quantencomputers zu realisieren, berichtet Rainer Blatt in seinem Artikel, während sich Gerhard Birkl den Versuchen mit neutralen Atomen widmet. Gerd Schön und Alexander Shnirman stellen Festkörpersysteme wie Josephson-Kontakte und Quantenpunkte als alternative Kandidaten für Qubits und Quantenregister vor.

Neben der experimentellen Implementierung stellt sich auch die Aufgabe, zu erforschen, welche anderen Modelle des Quantencomputers ebenso leistungsfähig wären wie das aus Ein-Qubit- und Zwei-Qubit-Gattern bestehende. Modelle mit völlig anderen Grundoperationen, z. B. mit Ein-Qubit-Messungen an einem verschränkten Zustand, wurden bereits vorgeschlagen.

Unabhängig davon, ob ein „richtiger“ Quantencomputer jemals gebaut werden kann, gilt sicher, dass die Modelle und Experimente des Quantencomputing zu einem tieferen Verständnis der Quantentheorie beigetragen haben und weiterhin beitragen werden.

### Die Kriterien von DiVincenzo

Nach David DiVincenzo kommt ein Quantensystem nur dann für die Implementierung eines Quantencomputers in Betracht, falls es die folgenden Bedingungen erfüllt:

- Das System muss aus vielen, wohldefinierten quantenmechanischen Zwei-Zustands-Systemen (Qubits) bestehen, die zu einer durch die geplante Anwendung bestimmten großen Anzahl $N$ „skalierbar“ sind.
- Die Qubits müssen sich in einem wohldefinierten Anfangszustand initialisieren lassen.
- Ein „universeller Satz“ an Ein-Qubit und Zwei-Qubit-Manipulationen muss kohärent durchgeführt werden können (z. B. alle Spin-Drehungen und Phasenverschiebungen sowie die Operation eines CNOT zwischen jeweils zwei Spins).
- Die quantenmechanische Phasenkohärenzzeit muss lang genug sein, um eine große Zahl von Manipulationen kohärent durchführen zu können.
- Schließlich muss der Quantenzustand der Qubits verlässlich ausgelesen werden.