Quanteninformationstheorie im Schulunterricht

Wolfgang Dür*

*Institut für Theoretische Physik, Universität Innsbruck, Technikerstrasse 25, A-6020 Innsbruck, Austria

Kurzfassung

Die Quanteninformationstheorie ist ein modernes interdisziplinäres Forschungsgebiet, welches Quantentheorie und Informationswissenschaften vereint. Dabei geht es einerseits um eine systematische Untersuchung und ein besseres Verständnis der seltsamen Quanteneigenschaften, allen voran der quantenmechanischen Verschränkung, andererseits um eine praktische Nutzung dieser Effekte im Sinne der Informationsverarbeitung. In den letzten Jahren hat es dabei sowohl auf konzeptioneller als auch auf experimenteller Ebene interessante Fortschritte gegeben, welche uns einer praktischen Nutzung von Quantenkommunikation, Quantenkryptographie und Quanteninformationsverarbeitung mit Quantencomputern näher bringen. In diesem Beitrag soll die Relevanz der Quanteninformationstheorie für den Schulunterricht -im Sinne eines alternativen Zugangs zur Quantenphysik- diskutiert und erste Ansätze für ein darauf basierendes Unterrichtskonzept vorgestellt werden.

1. Einleitung

Die Quantenmechanik ist eine der zentralen Theorien der modernen Physik, und noch heute ein vielbeachtetes und aktuelles Forschungsgebiet. Dabei spielen Themengebiete wie die Quantenoptik, Quantencomputer, Atom- und Festkörperphysik oder kondensierte Materie ebenso eine bedeutende Rolle wie die Untersuchung von grundlegenden Konzepten der Theorie und deren philosophische Konsequenzen. Kaum eine physikalische Theorie hat unser Bild der Welt derart geprägt und verändert wie die Quantentheorie, und aus den seltsam anmutenden Eigenschaften, die schon ihre Gründungsväter wie Einstein, Bohr, Heisenberg und Schrödinger in zahllose kontroverse Diskussionen gestürzt haben sind in den letzten Jahren praktische Anwendungen wie etwa der Laser entstanden, die aus der heutigen modernen Welt nur schwer wegzudenken sind. Gedankenexperimente von damals können heute in zahlreichen Labors weltweit durchgeführt werden, wobei die Manipulation und Kontrolle von Materie auf atomarem Niveau und bei Temperaturen praktisch am absoluten Nullpunkt möglich ist.

Dennoch spielt die Quantenphysik in der Schule nur eine untergeordnete Rolle und wird – wenn überhaupt - oft nur am Rande gestreift. Warum ist dies so? Ein Hauptgrund dürfte wohl die recht komplexe mathematische Struktur der Theorie sein, die eine fundierte Behandlung in der Schule erschwert. Aber auch konzeptuell ist die Quantenphysik schwierig zu behandeln, steht sie doch scheinbar im Widerspruch zur Alltagserfahrung und beruht auf Methoden und Konzepten, die selbst ihre Gründungsväter zu Aussagen hingerissen haben, dass niemand die Quantenmechanik wirklich verstanden hat. Tatsächlich sind noch heute Debatten über Deutungsfragen und Interpretation der Quantenmechanik im Gange, und obwohl unser Verständnis der grundlegenden Konzepte der Theorie besonders in den letzten Jahren stark zugenommen hat sind längst nicht alle Aspekte vollständig verstanden. Dies sollte aber keinesfalls aus Ausrede herangezogen werden, erst gar nichts über die Quantenmechanik im Allgemeinen und die Deutungsfrage im Besonderen zu erwähnen. Vielmehr stellt sich die Frage, wie man die Quantentheorie so aufbereiten kann, dass sie auch für Schüler interessant und vor allem verständlich präsentiert werden kann.

In den letzten Jahren hat es einige Ansätze gegeben, die grundlegenden Elemente der Quantenmechanik zu identifizieren und darauf aufbauend ein Kerncurriculum zu erstellen (siehe z.B. [1-7]). Im Vergleich zu anderen Gebieten der (klassischen) Physik (wie z.B. der Mechanik oder Elektrizitätslehre) ist eine solche Auswahl noch nicht so weit fortgeschritten bzw. etabliert, und trotz guter und interessanter Ansätze gibt es wohl noch Raum für Verbesserungsmöglichkeiten in der Erarbeitung eines allgemein akzeptierten, praktikablen Zugangs zur Quantenmechanik für den Schulunterricht. Ziel dieses Beitrags ist es, ein neues Element in diese Diskussion mit aufzunehmen und einen Ansatz vorzustellen, der auf einem modernen und aktuellen Forschungsgebiet – der Quanteninformationstheorie – beruht [8]. Im Mittelpunkt stehen dabei nicht die Eigenschaften und Beschreibung von (komplexen) Objekten wie Atomen oder Elektronen, sondern ein Zugang basierend auf elementaren Quantensystemen,

den sogenannten Qubits. Die Behandlung des einfachsten denkbaren Quantensystems soll helfen, begriffliche und mathematische Schwierigkeiten zu reduzieren und einige der zentralen Elemente der Theorie einzuführen und qualitativ und quantitativ zu diskutieren. Darüber hinaus erlaubt dieser Zugang die Behandlung von modernen Forschungsthemen wie Quantenkryptographie und Quantencomputer im Schulunterricht.

2. Klassische Informationsverarbeitung

Zuerst sollten aber wichtige Elemente der klassischen Informationsverarbeitung kurz angesprochen werden, nicht zuletzt um die Unterschiede zur Quanteninformationsverarbeitung zu illustrieren.

2.1 Bits, Bistrings und logische Gatter

Das einfachste klassische System ist ein 2-Niveau System, ein System mit einer charakteristischen Eigenschaft die nur zwei mögliche Werte – 0 oder 1 - annehmen kann. Man spricht dabei auch von einem Bit (binary digit), wobei ein Bit auch ein elementarerer Informationsträger bzw. die kleinste Einheit von Information ist. Ein Bit sollte dabei als abstraktes Objekt verstanden werden, und es ist nicht vorgegeben, welche charakteristische Eigenschaft bzw. welche physikalische Realisierung betrachtet wird. So kann es sich z.B. um einen Schalter mit 2 möglichen Stellungen, um eine Spannung die Werte *U=0V* oder *U=5V* annehmen kann, oder auch um den Ort eines Teilchens mit möglichen Werten x_0 und x_1 handeln (z.B. ein Ball, der in einem Schrank auf dem unteren oder oberen Regal liegt). In jedem Fall wird aber nur eine charakteristische Eigenschaft betrachtet, weitere Eigenschaften werden vernachlässigt bzw. als fixiert angesehen. Beim Ball sind dies z.B. dessen Größe, Gewicht, Geschwindigkeit, oder auch weitere mögliche Orte.

Ebenso kann man Systeme betrachten, die aus mehreren Bits bestehen. Dabei handelt es sich um eine Ansammlung von elementaren 2-Niveau Systemen, die jeweils eine unterschiedliche charakteristische Eigenschaft mit zwei möglichen Werten repräsentieren. Jedes Bit kann dabei wieder 2 mögliche Werte annehmen. Ein System von *n* Bits hat also insgesamt 2^n verschieden Einstellmöglichkeiten bzw. Werte. In diesem Zusammenhang spricht man auch von einem Bitstring $\boldsymbol{x} = x_1 x_2 \dots x_n$, wobei $x_j \epsilon \{0,1\}$ den Wert von Bit j bezeichnet.

Klassische Informationsverarbeitung geschieht nun durch Manipulation eines Bitstrings durch logische Gatter. Diese arbeiten nach einer einfachen Abbildungsvorschrift (Wertetabelle bzw. logische Verknüpfung). Elementare logische Gatter sind z.B. das NOT Gatter, das AND Gatter sowie das OR Gatter. Durch Anwendung von Sequenzen von elementaren logischen Gattern die jeweils auf einem bzw. 2 Bits wirken wird ein Bitstring $x_1 x_2 \dots x_n$ auf einen anderen Bitstring $y_1 y_2 \dots y_m = f(x_1 x_2 \dots x_n)$ abgebildet. Es wird also – abhängig von der Sequenz von Gattern - eine Funktion *f* berechnet, deren Wert dann ausgelesen werden kann. Auf diese Weise kann jede beliebige Funktion *f* realisiert werden. Um die Berechnung reversibel zu gestalten, kann der Funktionswert in ein 2.Register gespeichert werden und zusätzlich der Eingangswert (Bitstring $x_1 x_2 \dots x_n$) ausgegeben werden. Jede Berechnung am Computer funktioniert nach diesem Schema, wobei zu einem gegebenen Wert x der zugehörige Funktionswert $f(x)$ ermittelt werden soll.

2.2 Eigenschaften von klassischen Systemen

Die physikalische Realisierung von Bits erfolgt durch klassische Systeme, die deshalb auch durch die Gesetzte der klassischen Physik beschrieben werden. Daraus ergeben sich einige grundlegende Eigenschaften solcher Systeme, von denen wir hier einige ausgewählte zusammenfassen. Dies erfolgt bereits mit Hinblick darauf, welche dieser –aus Alltagssicht teilweise selbstverständlichen- Eigenschaften bei Quantenmechanischen Systemen in dieser Form nicht mehr gegeben sind.

Insbesondere erfüllen diese klassischen Systeme die Annahme einer „Realität“. Betrachten wir eine charakteristische Eigenschaft eines Objekts –z.B. den Ort-, so besitzt diese Eigenschaft einen bestimmten Wert – unabhängig davon, ob wir diesen Wert kennen bzw. gemessen haben oder nicht. Die Bestimmung des Wertes ist durch eine Messung bzw. Beobachtung möglich, und der Wert bleibt durch die Messung unverändert. Die Messung beeinflusst also den Zustand des Systems nicht. Interessieren wir uns für mehrere (unabhängige) Eigenschaften eines Objekts –z.B. den Ort und die Geschwindigkeit-, so haben diese Eigenschaften unabhängig voneinander bestimmte Werte, die unabhängig voneinander und ohne gegenseitige Beeinflussung bestimmt werden können. Daraus folgt auch, dass es möglich ist, Kopien eines Systems herzustellen – der Wert wird ausgelesen und daraufhin werden beliebig viele identische Systeme im entsprechenden Zustand präpariert. Man denke dabei etwa an die Speicherung von Computerdaten auf mehreren Datenträgern.

Sieht man sich die zugrundeliegenden Gleichungen zur Beschreibung von klassischen Systemen an – etwa die Bewegungsgleichungen der klassischen Mechanik oder die Maxwellgleichungen der Elektrodynamik – so handelt es sich dabei um deterministische Differentialgleichungen. Gibt man die Anfangsbedingungen vollständig vor, so erhält man eine eindeutige Lösung. Insbesondere bedeutet dies, dass diese Systeme ein deterministisches Verhalten zeigen und gewissen Lokalitätsgesetzen unterliegen. Bei einer vollständigen, genauen Kenntnis des An

fangszustandes ist der Zustand des Systems zu je-Verhalten des Systems ist deshalb im Prinzip für alle späteren Zeiten vorhersagbar [1].

3. Einfache Quantensysteme

Wir wenden uns nun Quantenmechanischen Systemen zu und betrachten die Beschreibung von Zuständen, Messungen und Operationen, sowie die daraus resultierenden Eigenschaften.

3.1. Quantenmechanisches 2-Niveau System – Qubit

Ganz analog zum klassischen Bit ist ein Quantenbit (Qubit) das einfachste quantenmechanische System. Auch hier handelt es sich um ein 2-Niveau System, wobei eine charakteristische Eigenschaft wieder zwei mögliche Werte annehmen kann. Wir bezeichnen diese nun mit $|0>$ und $|1>$. Dabei kann es sich z.B. um den Ort eines Teilchens (Ort x_1 oder x_2), um den Spin eines Elektrons (Spin ↑ oder Spin ↓), um die Polarisation eines Photons (Horizontal H oder Vertikal V) oder um zwei interne Zustände eines Atoms (entsprechend zweier möglicher Elektronenkonfigurationen) handeln. Die übrigen Freiheitsgrade des Teilchens werden dabei vernachlässigt bzw. als fixiert angenommen. Ein Qubit ist dabei als abstraktes Objekt zu verstehen, welches durch verschiedenartige physikalische Systeme realisiert werden kann.

Neu ist nun, dass auch *beliebige Überlagerungen* der beiden Zustände $|0>$ und $|1>$ möglich sind. Berücksichtigt man, dass Quantenzustände normiert sein müssen (also Vektoren der Länge 1 entsprechen) und eine globale Phase irrelevant für das physikalische Verhalten ist, so ist der Zustand eines Qubits durch zwei reelle Parameter ϑ, φ charakterisiert und kann in der Form

$$|\Psi> = \cos\vartheta/2\,|0> + e^{i\varphi}\sin\vartheta/2\,|1> \quad \{1\}$$

dargestellt werden. Die Winkel ϑ, φ können dabei mit Kugelkoordinaten assoziert werden (die sogenannte Bloch Kugel), wobei ϑ der Polarwinkel und φ der Azimutalwinkel ist. Somit kann der Quantenzustand eines Qubits durch einen Vektor im Raum der Länge 1 veranschaulicht werden. In diesem Bild sind senkrechte Zustände antiparallel, und der Zustand $|0>$ entspricht $\vartheta = 0$ und ist in $+z$-Richtung dem späteren Zeitpunkt eindeutig festgelegt. Das orientiert, während $|1>$ $\vartheta = \pi$ entspricht und in $-z$-Richtung orientiert ist. Der Überlagerungszustand $(|0> + |1>)/\sqrt{2}$ entspricht einem Vektor in $+x$-Richtung.

Führt man Zustände von Qubits in der Schule ein, ist es (zunächst) ausreichend, nur reelle Koeffizienten zu betrachten (Phase $e^{i\varphi} = 1$). Dadurch vermeidet man Probleme mit komplexen Vektoren und deren Skalarprodukten. Das Bild der Blochkugel reduziert sich damit auf den Einheitskreis, also Vektoren der Länge 1 in der Ebene, die durch den Winkel ϑ parametrisiert sind.

Der Zustand eines Qubits kann manipuliert werden bzw. sich mit der Zeit ändern. Dies entspricht dann einer Drehung des Zustandsvektors in der Bloch Kugel, und wird mathematisch beschrieben durch unitäre Operationen – in diesem Fall durch Multiplikation des Zustandsvektors mit einer (unitären) 2×2 Matrix U. Je nach physikalischem System geschieht dies durch unterschiedliche Mittel, z.B. durch Laserpulse oder externe Magnetfelder.

Neu ist nun auch das Verhalten des Quantensystems bei Messungen. Messungen können nur zwischen zwei möglichen Zuständen unterscheiden (also z.B. Zustand $|0>$ oder $|1>$ - man spricht auch von einer Messung in *z*-Richtung), und deshalb auch nur eines von zwei möglichen Ergebnissen liefern. Ist das Quantensystem vor der Messung in einem Überlagerungszustand $|\Psi> = \alpha|0> + \beta|0>$, so erhält man ein zufälliges, nicht vorhersagbares Ergebnis. Die Wahrscheinlichkeit für ein bestimmtes Meßergebnis ist dabei durch den Abstand des Zustandsvektors zum jeweiligen Meßergebnis (z.B. $|0>$) bestimmt. Es handelt sich also um eine strukturierte Form von Zufall: die Kenntnis des Zustands des Systems erlaubt keine Vorhersage für ein Einzelereignis, führt man allerdings viele Wiederholungen desselben Experiments durch, so kann man das statistische Verhalten, also die Meßwahrscheinlichkeiten, berechnen. Nach der Messung ist der Überlagerungszustand nicht mehr vorhanden, der Zustandsvektor nach der Messung schaut in Richtung des Meßvektors (also bei einer *z*-Messung in Richtung des Vektors $|0>$ falls das Meßergebnis „$|0>$“ gefunden wurde bzw. in Richtung des Vektors $|1>$ falls das Meßergebnis „$|1>$“ gefunden wurde).

Wir wollen hier auf eine mathematische Beschreibung verzichten, wenn diese auch nicht sonderlich kompliziert ist [2]. Stattdessen betrachten wir ein anschauliches Bild des Meßprozesses, bei dem wir eine Messung durch einen Schlitz in eine bestimmte Raumrichtung illustrieren. Der ursprüngliche Zu-

[1] Wie aus der Chaostheorie bekannt können aber selbst kleinste Abweichungen der Anfangsbedingungen zu einem vollständig unterschiedlichen Verhalten führen. Für den Fall dass keine vollständige Kenntnis der Anfangsbedingungen vorliegt muss in der Regel auf eine statistische Beschreibung z.B. im Rahmen der statistischen Mechanik zurückgegriffen werden – diesen Fall wollen wir hier aber nicht betrachten.

[2] Man benötigt lediglich Skalarprodukte von Vektoren zur Berechnung der Meßwahrscheinlichkeiten, sowie Projektionen, also Multiplikation eines Vektors mit einer Matrix, zur Berechnung des Zustands nach der Messung

standsvektor wird durch den Meßprozess in (positive oder negative) Richtung des Schlitzes geklappt (also durch den Schlitz „hindurchgepresst“). Dadurch ergeben sich zwei mögliche Meßergebnisse und auch die Änderung des ursprünglichen Zustands durch die Messung.

An dieser Stelle sollte noch bemerkt werden, dass Messungen in beliebige Richtungen möglich sind. So kann der Schlitz z.B. auch in Richtung der *x*-Achse orientiert sein, wobei die möglichen Meßergebnisse durch die Zustände $(|0> \pm |1>)/\sqrt{2}$ beschrieben werden. Diese unterschiedlichen Meßrichtungen entsprechen unterschiedlichen Eigenschaften des Systems, die abgefragt werden können. Betrachtet man etwa den Zustand $(|0> + |1>)/\sqrt{2}$, so hat dieser eine wohldefinierte Eigenschaft – er schaut in Richtung der positiven *x*-Achse. Eine entsprechende *x*-Messung bestätigt dies auch – die Messung liefert mit Wahrscheinlichkeit 1 das Ergebnis „$(|0> + |1>)/\sqrt{2}$“. Führt man allerdings am selben Zustand eine *z*-Messung durch, so liefert diese ein vollkommen zufälliges Ergebnis – mit Wahrscheinlichkeit ½ erhält man entweder das Ergebnis „$|0>$“ oder das Ergebnis „$|1>$“ (umklappen des Vektors in positive oder negative *z*-Richtung). Der Zustand besitzt diese „*z*-Eigenschaft“ also nicht, die beiden Eigenschaften sind komplementär. Nach der entsprechenden *z*-Messung hat sich allerdings der Zustand des Systems geändert – dieses besitzt nun eine definitive „*z*-Eigenschaft“, die „*x*-Eigenschaft“ ist nun aber unbestimmt.

3.2. Verschränkte Zustände

Ganz analog kann man nun komplexere Quantensysteme beschrieben, die aus mehreren Qubits zusammengesetzt sind. Ein System von zwei Qubits hat nun 4 Basiszustände $|0> |0> = |00>, |01>, |10>, |11>$, wobei wieder beliebige Überlagerungen möglich sind. Ein entsprechender Quantenzustand von zwei Qubits ist also durch einen 4-er Vektor mit insgesamt 4 komplexen Koeffizienten beschrieben.

Von besonderem Interesse sind dabei die sogenannten verschränkten Zustände, z.B. der Bell Zustand

$$|\Phi^+> = (|00> + |11>)/\sqrt{2}. \qquad \{2\}$$

Dabei ist das Gesamtsystem in einem wohldefinierten Zustand, nicht aber die einzelnen Qubits. Messungen der einzelnen Qubits liefern vollkommen zufällige Ergebnisse. Misst man aber beide Qubits unabhängig voneinander in derselben (reellen) Meßbasis, so sind die Ergebnisse der Messungen zwar zufällig, aber in beiden Fällen immer perfekt korreliert, d.h. die Meßergebnisse sind identisch. Dies ist unabhängig von der Entfernung der beiden Teilchen der Fall, und führt dazu, dass solche quantenmechanischen Zustände die Bell’sche Ungleichung verletzen. Die Quantenmechanik ist also eine Theorie, welche die gemeinsame Annahmen von „Lokalität“ und „Realität“ nicht erfüllt – und deshalb unser gewohntes Bild der Welt gehörig durcheinanderbringt. Diese quantenmechanische Verschränkung lässt sich aber auch als Ressource für Anwendungen im Bereich der Quanteninformationsverarbeitung verwenden – z.B. zur Teleportation oder für die Quantenkryptographie.

Ebenso wie einzelne Qubits können auch Systeme von mehreren Qubits manipuliert werden. Beschrieben wird dies wiederum durch unitäre Abbildungen bzw. Gatter, wobei gezeigt werden kann, dass jede solche Manipulation (=Quantenrechnung) auf *n* Qubits durch eine Sequenz von beliebigen 1-qubit Drehungen und einer speziellen 2-qubit Operation, dem sogenannten kontrollierten NOT Gatter (CNOT) realisiert werden kann.

Anhand der Betrachtung dieser einfachen Quantensysteme haben wir bereits drei der zentralen Eigenschaften der Quantentheorie kennen gelernt, und diese durch ein einfaches Bild – der Bloch Kugel- illustriert: die Möglichkeit von Überlagerungen und damit verbunden das Phänomen der Verschränkung, das zufällige Verhalten bei Messungen sowie die Änderung des Zustands durch eine Messung. Insbesondere zeigt sich, dass viele dieser Eigenschaften im direkten Widerspruch zu uns vertrauten und als selbstverständlich betrachteten Eigenschaften von klassischen Systemen stehen (vergleiche Kapitel 2.2).

3.3. Quanteninformationsverarbeitung - Anwendungen

Aus Sicht der Quanteninformationstheorie sind aber nicht nur die seltsamen Eigenschaften von Quantenteilchen von Interesse, sondern die Anwendung dieser Eigenschaften für eine (verbesserte) Informationsverarbeitung [9,10]. Diese Anwendungen eignen sich teilweise auch gut für eine Behandlung im Schulunterricht.

Betrachtet man nur ein einzelnes Qubit, so kann gezeigt werden, dass Quanteninformation nicht kopiert werden kann. Auch die Grundzüge von Komplementarität sowie der Heissenberg‘schen Unschärferelation können diskutiert werden, und die Funktionsweise von einfachen Quantenkryptographieprotokollen zur Durchführung von (beweisbar sicherer) Kommunikation kann erklärt werden. Im Wesentlichen basieren diese Protokolle auf der Tatsache, dass jeder Informationsgewinn auf Messungen beruht, und somit mit einer Störung des vorliegenden Quantenzustands verbunden ist.

Betrachtet man Systeme von 2 bzw. 3 Qubits, so taucht das Phänomen der Verschränkung auf, und es bietet sich an, anhand der Bell’schen Ungleichung über die Auswirkungen der Quantentheorie auf unser Weltbild zu sprechen. Ebenso können aber auch

Anwendungen von Verschränkung im Bereich der Kryptographie oder auch der Quantenkommunikation (Teleportation) behandelt werden. Bei der Teleportation dient ein verschränkter Zustand als Ressource, um (unbekannte) Quanteninformation zu übertragen.

Betrachtet man schließlich zusammengesetzte Systeme von *n* Qubits, kann die Quanteninformationsverarbeitung , also das Rechnen mit Quantenzuständen, behandelt werden. Im Rest dieses Beitrages wollen wir etwas genauer auf solche Quantencomputer eingehen.

4. Quantencomputer

Betrachtet man die historische Entwicklung von klassischen Computern, so fällt auf, dass ein (exponentielles) Wachstum der Rechenleistung mit einer immer zunehmenden Miniaturisierung einhergeht. Während frühe Röhrenrechner noch ganze Fabrikhallen füllten, ist ein moderner Mikroprozessor in der Lage, ein Vielfaches der Rechenleistung zur Verfügung zu stellen, und dabei trotzdem auf einem Fingernagel Platz zu finden.

Diese zunehmende Miniaturisierung führt aber dazu, dass immer weniger Atome ein einzelnes klassisches Bit repräsentieren. Setzt man die bisher beobachtete Entwicklung in die Zukunft fort, so wären bereits in wenigen Jahren nur mehr eine Handvoll Atome bzw. sogar einzelne Atome zur Speicherung eines einzelnen Bits notwendig. Allerdings wissen wir, dass auf mikroskopischem Niveau quantenmechanische Effekte eine wichtige Rolle spielen. Für klassische Informationsverarbeitung sind solche Effekte allerdings überwiegend unerwünscht und müssen unterdrückt werden – wir möchten ja, dass unser Computer immer genau das macht, was wir von ihm erwarten. Somit scheint sich eine natürliche Grenze für eine weitere Miniaturisierung aufzutun.

Der Ansatz der Quanteninformationsverarbeitung geht aber einen Schritt weiter: anstatt die Quanteneffekte zu unterdrücken, werden diese gezielt dazu verwendet, um eine verbesserte Informationsverarbeitung zu erzielen. Als Informationsträger dienen in der Tat einzelne Atome, einzelne Elektronen oder einzelne Photonen, welche gezielt manipuliert werden können. Es konnte gezeigt werden, dass solche Quantencomputer Probleme effizient lösen können, die für jeden klassischen Computer praktisch unmöglich zu lösen sind (da die benötigte Rechenzeit exponentiell mit der Problemgröße wächst).

4.1. Grundlagen & Quantenalgorithmen

Wir betrachten ein Quantenregister bestehend aus *n* Quantenbits, sowie ein 2. Register derselben Größe. Wir verwenden eine Binärnotation zur Beschreibung des Zustands der einzelnen Register, $|x>=|x_1>|x_2>\cdots|x_n>$. Ein Anfangszustand $|x>|0>$ wird durch Anwendung einer Sequenz von elementaren 1- und 2-qubit Gattern manipuliert, und dadurch wird ein gewünschter Funktionswert *f(x)* berechnet, wobei das Ergebnis dieser Berechnung in das 2.Register geschrieben wird [3]. Dies ist analog zur klassischen Informationsverarbeitung.

Neu ist allerdings, dass nun auch Überlagerungszustände als mögliche Eingangszustände erlaubt sind. Insbesondere kann man einen Zustand $|\Psi>=2^{-n/2}\sum_{x=0}^{2^n-1}|x>$ verwenden – dabei handelt es sich um eine Überlagerung aller möglichen Eingangswerte – dies entspricht dem Fall, dass jedes der Qubits des 1.Registers im Zustand $(|0>+|1>)/\sqrt{2}$ präpariert ist. Durch Anwendung der unitären Operation *U* erhält man nun auf Grund der Linearität der Quantenmechanik

$$\sum_{x=0}^{2^n-1}|x>|0>\rightarrow\sum_{x=0}^{2^n-1}|x>|f(x)>. \qquad \{3\}$$

Durch eine einzige Berechnung der Funktion *f* liegen also alle Funktionswerte *f(x)* vor. Allerdings kann bei einer Messung nicht mehr als ein Funktionswert ausgelesen werden. Interessiert man sich aber für eine globale Eigenschaft der Funktion *f* – etwa ihre Periode – so kann man (mit Hilfe einer diskreten Fouriertransformation) diese Information gezielt auslesen, wobei man ausnützt, dass alle Funktionswerte im Quantenzustand enthalten sind. Im Wesentlichen wird dabei wieder verwendet, dass die Quantenmechanik Überlagerungszustände zulässt – eine Eigenschaft, die (diskrete) klassische Systeme nicht aufweisen. Dieser „Quantenparallelismus“ erklärt im Prinzip bereits die potentielle Stärke eines Quantencomputers.

An dieser Stelle sei aber zur Vorsicht gemahnt: zur Zeit verfügen wir nur über ein unvollständiges Verständnis über die genauen Stärken eines Quantencomputers und der exakten Ursache für den Geschwindigkeitsgewinn gegenüber klassischen Computern. Einerseits sind eine Reihe von Quantenalgorithmen bekannt, die einen beweisbaren (exponentiellen) Geschwindigkeitsgewinn gegenüber jeglicher Form von klassischer Informationsverarbeitung erlauben. Andererseits gibt es aber ganz ähnlich aussehende „echte“ Quantenprozesse, die mit Hilfe eines klassischen Computers effizient simuliert werden können. Wo also die genaue Grenze zwi-

[3] Die Verwendung eines 2.Registers ist notwendig, da unitäre Operationen reversibel sind und ansonsten nur umkehrbare Funktionen berechnet werden könnten.

schen klassischen Computern und Quantencomputern liegt bedarf noch weiterer Forschungsarbeit – auch wenn schon jetzt die Nützlichkeit von Quantencomputern zweifelsfrei feststeht, sofern man in der Lage ist diese zu bauen.

Der wohl bekannteste Quantenalgorithmus ist der Shor Algorithmus zur Faktorisierung von (großen) Zahlen [11]. Dieser Algorithmus beruht im Wesentlichen auf dem oben angesprochenen Prinzip der Ermittlung der Periode einer Funktion unter Ausnutzung des Quantenparallelismus, und bietet einen exponentiellen Geschwindigkeitsgewinn gegenüber dem besten bekannten klassischen Algorithmus. Nachdem das in der Praxis häufig verwendete RSA-Verschlüsselungsverfahren aber darauf beruht, dass die Primfaktorzerlegung einer großen Zahl für jeden klassischen Computer ein schwieriges Problem ist, würde ein Quantencomputer die Entschlüsselung der derzeit verwendeten RSA Codes ermöglichen. Sichere Datenübertragung, etwa von Kreditkartendaten über das Internet, wäre mit diesem Verfahren dann unmöglich. Gut, dass es dann die Quantenkryptographie als Alternative gibt – die sogar eine *beweisbar* sichere Nachrichtenübermittlung ermöglicht.

In den letzten Jahren wurde eine Reihe weiterer Algorithmen –vorwiegend zur Lösung von bestimmten mathematischen oder physikalischen Problemen entwickelt. Nähere Informationen dazu findet man in [12].

4.2. Physikalische Realisierung

Zum Bau eines Quantencomputer benötigt man ein physikalisches System, das eine Reihe von Kriterien – die sogenannten DiVincenzo Kriterien - erfüllen muss. Einerseits sollte das System skalierbar sein und wohldefinierte Qubits enthalten, deren Zustand initialisiert und ausgelesen werden kann. Andererseits ist es notwendig, dass Qubits mit einem Satz von universellen Quantengattern – z.B: CNOT und allgemeine 1-Qubit Drehungen – manipuliert werden können, um dann beliebige unitäre Operationen (=Quantenrechnungen) durchzuführen. Schlussendlich ist es noch notwendig, dass die Lebensdauer der Qubits viel grösser ist als die Gatterzeit, also jene Zeit, die für die Durchführung eines Gatters benötigt wird.

Es gibt eine Reihe von Ansätzen zur experimentellen Realisierung eines Quantencomputers. Eine Übersicht über die verwendeten physikalischen Systeme und den derzeitigen Entwicklungsstand findet man in [13,14]. Besonders weit fortgeschritten sind Systeme basierend auf Ionenfallen [15] (siehe Abb. 1), bei denen Quanteninformation in internen Zuständen einzelner Ionen gespeichert und mittels Laser manipuliert werden kann. Man ist bereits in der Lage, entsprechende 1- und 2-qubit Quantengatter mit einer Güte von mehr als 99% zu realisieren, und auch die Information durch eine Messung mit ähnlicher Güte auszulesen. Auf diese Weise konnten für Systeme von einigen Qubits bereits einfache Sequenzen von Operationen demonstriert werden. Die derzeit verwendeten linearen Fallen weisen allerdings nur eine begrenzte Skalierbarkeit auf, es gibt aber auch Vorschläge bzw. erste Experimente basierend auf fragmentierten Fallen, welche Quanteninformationsverarbeitung mit einer größeren Anzahl von Qubits ermöglichen würden.

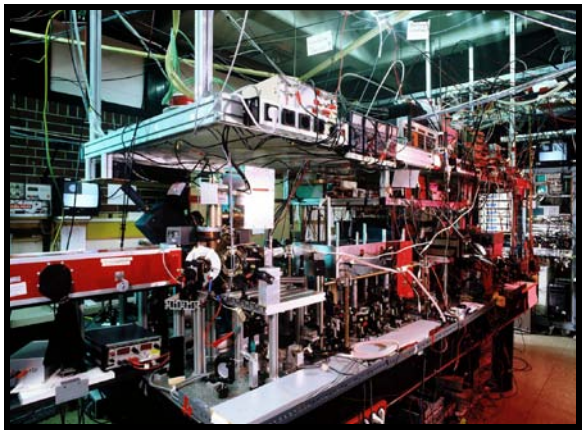

Abb.1: Foto des experimentellen Aufbaus eines Ionenfallen-Quantencomputers in der Gruppe von R. Blatt in Innsbruck (Foto: C. Lackner, IQOQI).

Andere Ansätze, insbesondere basierend auf Festkörpersystemen (Quantenpunkten), zeichnen sich durch ihre gute Skalierbarkeit aus, die Manipulation einzelner Qubits ist aber schwieriger als bei Ionen, und auch die erreichte Güte für Gatter bzw. Meßprozesse sind noch deutlich geringer. Es lässt sich aber aus heutiger Sicht nur schwer abschätzen, welches physikalische System für die Realisierung eines funktionstüchtigen Quantencomputers erfolgreich eingesetzt werden kann, bzw. bis wann es möglich sein wird, ein solches Gerät zu bauen. Es konnte zwar gezeigt werden, dass ein Quantencomputer auch unter realen Bedingungen (Rauschen) funktioniert, wenn Qubits codiert werden und Gatteroperationen mit einer Güte von mehr als 99.5% durchgeführt werden können. Dazu ist aber ein Mehraufwand notwendig, der schlussendlich dazu führt, dass für praktische Anwendungen im Bereich der Quantenalgorithmen Quantencomputer mit mehreren Zehntausend Qubits notwendig sind. Solch ein Gerät zu bauen stellt technologisch eine große Herausforderung dar.

4.3. Messungsbasierter Quantencomputer

Ein neuartiges Konzept zur Realisierung eines Quantencomputers stellen sogenannte messungsbasierte Quantencomputer [16] dar. Anders als im

Netzwerkmodell werden hier nicht Eingangszustände durch Sequenzen von logischen (unitären) Gattern manipuliert, sondern die Informationsverarbeitung findet ausschließlich durch Messungen statt. Dazu wird –ausgehend von einem hoch verschränkten Vielteilchenzustand, der als universelle Ressource dient- eine Sequenz von 1-qubit Messungen durchgeführt (siehe Abb. 2). Die Wahl des Meßmusters, also die Wahl der Meßrichtung (Meßbasis) der einzelnen Qubits sowie die Reihenfolge der Messung bestimmen den Zustand, in dem sich die nichtgemessenen Qubits danach befinden. Obwohl jede Messung ein zufälliges Ergebnis liefert, kann man zeigen, dass trotzdem jeder beliebe Endzustand $|\Psi>=U|0>$ (bis auf lokale Basisdrehungen) deterministisch auf diese Weise hergestellt werden kann, und dadurch ein universeller Quantencomputer realisierbar ist.

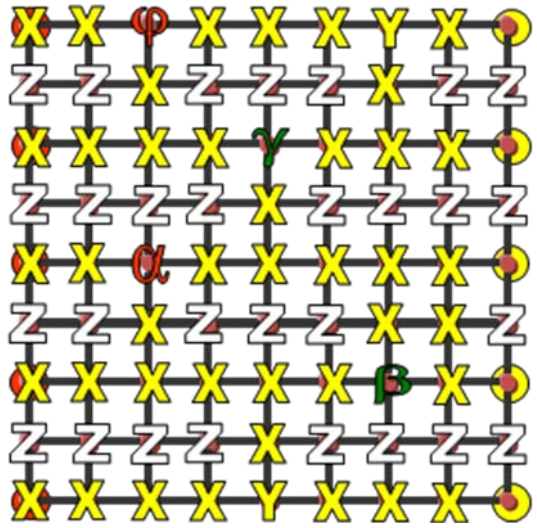

Abb.2: Ein hochverschränkter Vielqubit Zustand (ein 2D Clusterzustand) wird als Ressource verwendet. Durch Messungen der einzelnen Qubits in unterschiedlichen Basen werden die nicht gemessenen Qubits (bis auf eine lokale Drehung) in einem Zustand $|\Psi>=U|0>$ übergeführt, wobei die Auswahl des Meßmusters (also die Wahl der Meßbasen) eine Auswahl der unitären Operation *U* erlaubt.

Dadurch ergeben sich einerseits neue Einsichten in die fundamentale Struktur von Quantencomputern. Die Stärke eines messungsbasierten Quantencomputers ist unmittelbar mit den Verschränkungseigenschaften des Ressourcenzustands verknüpft, und die Grenze zwischen klassischer Informationsverarbeitung und Quanteninformationsverarbeitung kann dadurch näher untersucht werden [16]. Andererseits ergibt sich auch eine alternative Möglichkeit, Quantencomputer physikalisch zu realisieren. Dazu ist es lediglich notwendig, einen bestimmten hochverschränkten Quantenzustand herzustellen und diesen durch Messung von einzelnen Qubits zu manipulieren. Kohärente Gatter werden dazu nicht benötigt. Dieser Ansatz scheint insbesondere für Systeme basierend auf gefangenen neutralen Atomen in optischen Gittern, aber auch für Quantencomputer basierend auf Photonen als vielversprechende Alternative [16].

5. Zusammenfassung

In diesem Beitrag wurde skizziert, wie die Quanteninformationstheorie einen neuen, einfachen Zugang zur Quantenphysik ermöglicht, der vielleicht dazu dienen kann, die Quantenmechanik im Schulunterricht besser zu etablieren. Dabei können elementare Prinzipien der Quantenmechanik wie Überlagerungen von Zuständen, stochastisches Verhalten und Änderung des Zustands bei Messung, sowie Verschränkung anhand einfacher Systeme –den Qubits- behandelt und mit Hilfe einfacher Bilder illustriert werden. Insbesondere kann der Unterschied zu klassischen Systemen hervorgehoben werden.

Mit diesem Ansatz können auch moderne Anwendungen und Themen der aktuellen Forschung, etwa im Bereich der Quantenkryptographie oder der Quantencomputer behandelt werden. Die Grundzkonzepte eines Quantencomputers, einfache Quantenalgorithmen sowie mögliche physikalsische Realisierungen wurden dabei im zweiten Teil des Beitrags kurz angesprochen. Dort wurde auch das Konzept eines Messungsbasierten Quantencomputers vorgestellt. Eine detaillierte Darstellung –auch weiterer Anwendungen im Bereich der Quanteninformationsverarbeitung- findet sich in [8], und ein genaueres Unterrichtskonzept basierend auf einem Quanteninformationszugang zur Quantenphysik befindet sich derzeit in Ausarbeitung.

6. Literatur

[1] R. Müller, Quantenphysik in der Schule, Studien zum Physiklernen Band 26 (Logos Verlag Berlin 2003).
[2] J. Küblbeck und R. Müller, Die Wesenszüge der Quantenphysik, Praxis Schriftenreihe Physik, Band 60 (Aulis Verlag Deubner, Köln 2002).
[3] F. Bader, Eine Quantenwelt ohne Dualismus, Schroedel, Hannover (1996).
[4] H. Wiesner, Beiträge zur Didaktik des Unterrichts über Quantenphysik in der Oberstufe,Westarp Verlag, Essen (1989).
[5] A. Berg, H. Fischler, M. Lichtfeldt, M. Nitzsche, B. Richter, F.Walther, Einführung in die

Quantenphysik. Ein Unterrichtsvorschlag für Grund- und Leistungskurse, Pädagogisches Zentrum Berlin (1989).
[6] W. Salm, Zugänge zur Quantenphysik, Praxis Schriftenreihe Physik, Band 56 (Aulis Verlag Deubner, Köln 1999).
[7] H.Fischler (Hrsg.): Quantenphysik in der Schule, IPN Kiel, S. 6 (1992).
[8] W. Dür, Quanteninformation – Ein Thema für den Schulunterricht, Praxis der Naturwissenschaften: Physik in der Schule 6/58, 12-21 (2009).
[9] N. David Mermin, Gregg Jaeger, and Barbara Terhal, Quantum Computer Science: An Introduction and Quantum Information: An Overview, Phys. Today 61 March 54 (2008).
[10] M. Nielson and I. Chuang, Quantum Computation and Quantum Information (Cambridge Univ. Press, Cambridge, 2000).
[11] Artur Ekert and Richard Jozsa, Quantum computation and Shor's factoring algorithm, Rev. Mod. Phys. 68, 733 (1996).
[12] A. M. Childs and W. van Dam, Quantum algorithms for algebraic problems, Rev. Mod. Phys. 82, 1–52 (2010).
[13] Quantum Information Science and technology roadmap Project, Quantum Computation Roadmap http://qist.lanl.gov/qcomp_map.shtml (Stand April 2010)
[14] Zoller, P. et al. Quantum information processing and communication. Strategic report on current status, visions and goals for research in Europe. Eur. Phys. J. D 36, 203–228 (2005). http://qist.ect.it/ (Stand April 2010)
[15] H. Häffner, C.F. Roos and R. Blatt, Quantum computing with trapped ions, Physics Reports 469, 155 (2008).
[16] H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf, M. Van den Nest, Measurement-based quantum computation , Nature Physics 5, 19 (2009).