Der Quantencomputer in der Schule

G. Pospiech u. B. Schorn

1 Einführung

In Medienberichten liest man immer wieder von Quantencomputern, denen große Rechenpower zugeschrieben wird [1, 2, 3, 4, 5]. Die Art der Berichte reicht von reißerisch bis hin zu nüchtern, von sauber recherchiert bis hin zu maßlos übertrieben. Dabei werden die merkwürdigen „Qu-Bits" erwähnt, es wird auf die „bizarre Quantenwelt" abgehoben und auf die extreme Verkürzung der Rechenzeit, meist im Zusammenhang mit Verschlüsselungsalgorithmen, eingegangen. Oft ist es schwer zu unterscheiden, welche Aspekte realistisch sind und welche „Wundertaten" keinesfalls realisiert werden können, weil sie prinzipiell unmöglich sind.

Eine wesentliche Schwierigkeit besteht darin, den Schülerinnen und Schülern die Fähigkeit zu vermitteln, entsprechende Medienberichte einzuordnen und kritisch zu bewerten. Dazu sollen sie lernen, was die Bestandteile eines Quantencomputers sind, nach welchen Prinzipien er funktioniert und was dies für die möglichen Algorithmen mittels eines solchen Rechners bedeutet.

Ein Kritikpunkt besteht bereits darin, dass der Begriff „Quantencomputer" nicht einheitlich verwendet wird. Quantencomputer im engeren Sinne beruhen auf der Verschränkung, einem zentralen Phänomen der Quantenphysik. Aber es gibt auch andere Quantencomputer, die Quanteneffekte wie den Tunneleffekt nutzen und schon von daher nur für eine bestimmte Klasse von Problemen geeignet sind. Ein Beispiel hierfür ist der oft zitierte Quantencomputer der Firma D-Wave. Bei diesem diskutieren die Experten, inwieweit er ein „echter" Quantencomputer ist und Probleme tatsächlich schneller lösen kann als ein klassischer Computer [6].

2 Forschung zu Quantencomputern

Eine schöne Übersicht über die zeitliche Entwicklung der Forschung zu Quantencomputern findet man auf der englischen Wikipediaseite „Timeline of quantum computing" [7] mit Verweisen auf zahlreiche Originalartikel, deren zukünftige Relevanz heute sicher nicht in jedem Fall abzuschätzen ist. Diese Seite verdeutlicht aber auch sehr gut, wie sich die Forschung in den letzten Jahren weiterentwickelt hat und wie vielfältig die Forschungsansätze und Themen sind. Bereits seit den 1970er Jahren, verstärkt seit den 1980er und 1990er Jahren, denkt man darüber nach, welche Eigenschaften der Materie man für das Rechnen nutzen kann, wenn die Herstellung „normaler" Chips an der atomaren Grenze angelangt ist (entsprechend dem Moore'schen Gesetz [8] werden etwa im Jahre 2020 die Basiselemente eines Computers von der Größe einzelner Atome sein). Einige Schlüsselereignisse auf dem Weg zum Quantencomputer sind der Vortrag „There's Plenty of Room at the Bottom" von *Feynman* 1959 [9], die erste Beschreibung eines universellen Quantencomputers durch *David Deutsch* 1985 [10] und die Entwicklung eines ideal für den Quantencomputer geeigneten Verfahrens zur Faktorisierung großer Zahlen von *Peter Shor* 1994 [11, 12]. Gerade diese letzte Demonstration, dass es in der Tat relevante Anwendungen für einen Quantencomputer geben könnte, in Verbindung mit gleichzeitigen deutlichen technologischen Fortschritten, beflügelte die Forschung auf diesem Gebiet. Bis heute viel zitierte Kriterien für geeignete Quantensysteme hat *David diVincenzo* 1997 veröffentlicht [13], eine „roadmap" wurde 2004 vom Quantum Information Science and Technology Roadmapping Project erstellt [14].

In die Forschung zu Quantencomputern gehen theoretische Aspekte, sowohl physikalischer Natur als auch aus der Informatik, ein und auch experimentelle Aspekte spielen eine zentrale Rolle (siehe Abb. 1). In der Theorie geht es um die Beschreibung und Eigenschaften von Quantensystemen, in der Informatik um den Aufbau eines Algorithmus aus möglichst einfachen logischen Gattern sowie um Strategien zur Fehlerkorrektur und im experimentellen Bereich um die Realisierung von Quantensystemen, mit denen man bestimmte Probleme effizient lösen kann.

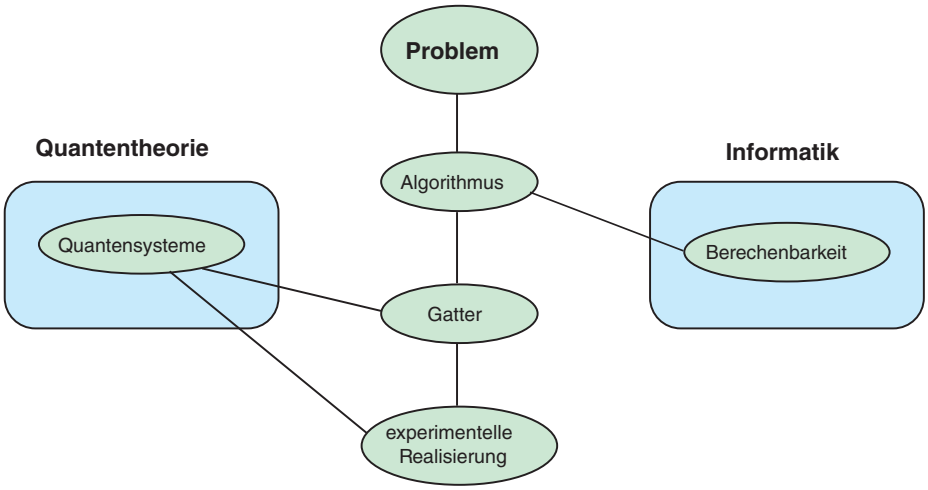

Abb. 1: Zusammenspiel von Quantentheorie und Informatik zur effizienten Lösung eines Problems

3 Perspektive der Quantenphysik

In diesem Abschnitt konzentrieren wir uns auf die spezifischen Merkmale der Quantentheorie, die für die Funktionsweise von Quantencomputern relevant sind. Aus diesen besonderen Merkmalen ergibt sich dann auch die Struktur der Probleme, die mit einem Quantencomputer besonders effizient lösbar sind.

3.1 Überlagerung in Quantensystemen

Die Zustände eines Quantenobjekts oder Quantensystems werden durch Vektoren in einem Hilbertraum beschrieben. Entsprechend ist die Schrödingergleichung, die die zeitliche Entwicklung eines Zustandes bestimmt, linear in der Zustandsfunktion. Diese Linearität hat zur Folge, dass (bis auf Normierung) die Überlagerung zweier oder mehrerer Quantenzustände wieder ein erlaubter Quantenzustand ist.

Eines der einfachsten Quantenobjekte ist ein Objekt, das man mithilfe von zwei Basiszuständen beschreiben kann. Symbo-

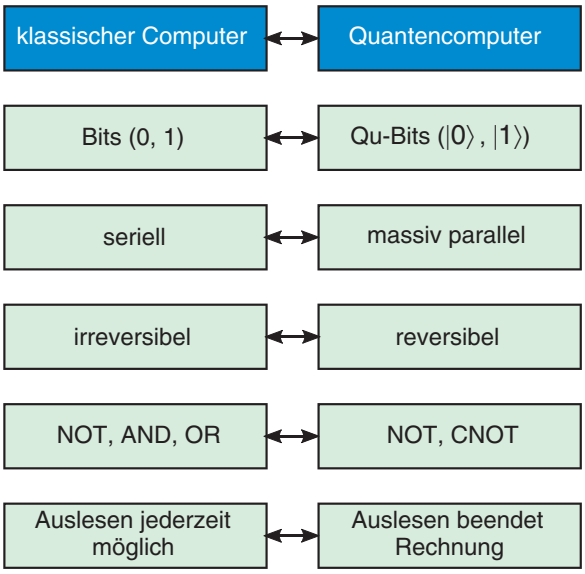

Abb. 2: Vergleich klassischer Computer und Quantencomputer

lisiert man die beiden Basiszustände mit $|0\rangle$ und $|1\rangle$, so ist auch jede Überlagerung $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ dieser Basiszustände mit $|\alpha|^2 + |\beta|^2 = 1$ ein möglicher Zustand dieses Quantensystems. Damit ist eine einheitliche mathematische Beschreibung sehr vielfältiger Systeme möglich: Polarisationszustände von Photonen (horizontal und vertikal polarisiert), Energiezustände von Atomen oder Ionen (Grundzustand und angeregter Zustand) usw.

Aus der Perspektive der Informatik gesehen lassen sich die Basiszustände $|0\rangle$ und $|1\rangle$ in Erweiterung der klassischen Bits (mit den Zuständen 0 und 1) als Zustände eines Quantenbits, kurz Qu-Bits, interpretieren. Diese Bezeichnung ist im Zusammenhang mit Quantencomputern die Kurzform für „Quantenobjekt mit genau zwei Basiszuständen". Damit ist der erste Baustein eines Quantencomputers identifiziert, das Qu-Bit. Die Regeln der Quantentheorie lassen erwarten, dass diese Qu-Bits anderen Regeln gehorchen als klassische Bits.

3.2 Verschränkung in Quantensystemen

Die Verschränkung ist eine Eigenschaft von Quantensystemen, die sie grundlegend von klassischen Systemen unterscheidet. Sie tritt zutage in Quantensystemen, die aus einzelnen Quantenobjekten zusammengesetzt sind, und ist eine Folge der Überlagerung von Quantenzuständen.

Beschränken wir uns zur Erläuterung auf Systeme aus Quantenobjekten mit zwei Basiszuständen: Fügt man zwei derartige Quantenobjekte zusammen, die beide die zwei Basiszustände $|0\rangle$ und $|1\rangle$ haben, so hat das entstehende Gesamtsystem eine Basis aus vier Produktzuständen, die sich aus allen möglichen Kombinationen der Basiszustände der einzelnen Objekte ergibt: $|0\rangle|0\rangle$, $|0\rangle|1\rangle$, $|1\rangle|0\rangle$ und $|1\rangle|1\rangle$. Diese vier Basiszustände können wiederum überlagert werden. Falls eine solche Überlagerung kein Produktzustand ist (d. h. sich nicht als ein Produkt schreiben lässt), so spricht man von einem verschränkten Zustand. Maximal verschränkte Zustände haben beispielsweise die Gestalt:

$$\frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle + |1\rangle|1\rangle\right) \text{ oder } \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle + |1\rangle|0\rangle\right).$$

Diese Verschränkung führt dazu, dass man beispielsweise bei bestimmten Messungen überzufällige Korrelationen zwischen den Ergebnissen finden wird.

Ein weiterer Effekt ist, dass jede Operation gleichzeitig auf beide miteinander verschränkte Quantenobjekte wirkt. Dies ist die Grundlage für den besonderen Quantenparallelismus, aufgrund dessen bestimmte Informationsverarbeitungen in hohem Maße parallel stattfinden können: Verschränkt man sehr viele Quantenobjekte bzw. Qu-Bits, so kann man mit einer einzigen Operation gleichzeitig auf allen verschränkten Quantenobjekten bzw. Qu-Bits rechnen.

3.3 Zeitliche Veränderung von Quantensystemen

Bei der zeitlichen Entwicklung von Quantensystemen treten ebenfalls ungewohnte Phänomene auf: Zum einen wird die Zeitentwicklung durch unitäre Operatoren (Matrizen) beschrieben und ist somit reversibel. Außerdem lassen sich alle unitären Operatoren auf einem einzelnen Qu-Bit mithilfe von vier Basisoperatoren (den Spinoperatoren) darstellen. Die Verknüpfung unitärer Operatoren ist wieder ein unitärer Operator. Damit ist eine beliebige Zeitentwicklung oder Veränderung eines Zustands reversibel. Das heißt, dass jeder Rechenvorgang eines Quantencomputers zwangsläufig reversibel sein muss.

Das Auslesen eines Ergebnisses geschieht in einem Messprozess. Wegen dessen statistischen Charakters ist daher das Ergebnis des Auslesens zufällig, man hat also kein vorhersagbares Rechenergebnis. Außerdem kann man keine Zwischenergebnisse auslesen, ohne den Rechenprozess irreversibel zu unterbrechen. Die Kunst, einen Quantencomputer zu programmieren, besteht also darin, die Wahrscheinlichkeit des gewünschten Ergebnisses so zu erhöhen, dass man die Rechnung nur wenige Male wiederholen muss, um sicher zu sein, in der Statistik der Messergebnisse das gesuchte Ergebnis zu erhalten.

4 Perspektive der Informatik

In diesem Abschnitt erläutern wir die Unterschiede in der Programmierung von Quanten- und klassischem Computer. Eine Übersicht über die Unterschiede ist in Abb. 2 dargestellt.

4.1. Klassische logische Gatter

In der klassischen Physik/ Informatik lassen sich alle logischen Operationen durch drei verschiedene logische Operationen (Gatter) darstellen:

- 1-Bit-Operation: NOT
- 2-Bit-Operationen: AND, OR

Betrachtet man die Wahrheitstafeln dieser Gatter (siehe Kasten 1), so fällt auf, dass das AND und das OR nicht reversibel sind, daher können diese keine möglichen Gatter für Quantencomputer sein. Die beiden klassischen nicht reversiblen 2-Bit-Operationen OR bzw. AND können jedoch durch die reversible 2-Bit-Operation CONTROLLED NOT (CNOT) bzw. 3-Bit-Operation CONTROLLED CONTROLLED NOT (CCNOT) dargestellt werden.

4.2. Quantengatter

Wegen der Reversibilität der Zeitentwicklung von Zuständen in der Quantenphysik müssen die Operationen beim Quantencomputer reversibel sein. Die entsprechenden drei reversiblen Gatter, mit denen sich alle logischen Operationen durchführen lassen, sind[1]:

- 1-Bit-Operation: NOT
- 2-Bit-Operation: CNOT

[1] *Zusätzlich zu den drei genannten reversiblen Gattern sind in manchen Fällen noch die unitären Rotationen (Phasenverschiebungen) als reversible Operationen notwendig.*

- 3-Bit-Operation: CCNOT

Da gemäß der Quantentheorie die zeitliche Entwicklung von Quantensystemen mit unitären Operatoren beschrieben wird, kann man zeigen, dass für die Implementierung jedes Algorithmus 1- und 2-Bit-Operationen ausreichen [15].

4.3 Unterschiede in der Realisierung der Computer

Beim klassischen Computer werden die Gatter, d. h. die logischen Schaltungen, in Hardware, z. B. mithilfe von Transistoren oder Dioden, realisiert, die dann entsprechend dem Algorithmus angesteuert werden. Die Bits 0 und 1 werden durch die Software, d. h. das Computerprogramm, vorgegeben und dann in den Schaltungen verarbeitet. Im Quantencomputer ist es gerade anders herum: Die Basiszustände $|0\rangle$ und $|1\rangle$ der Qu-Bits werden durch physikalische Objekte präsentiert (polarisierte Photonen oder Atome im Grund- bzw. angeregten Zustand) und die reversiblen logischen Gatter werden auf diese Qu-Bits angewendet, beispielsweise in Form von Laser- oder Radiopulsen.

4. 4. Identifizierung geeigneter Algorithmen

Es ist ferner eine interessante Frage, wie viel Rechenzeit man benötigt, um ein Problem zu lösen, das durch einen Input von n Bits gegeben ist. Dazu unterscheidet man zwischen Problemen, die mit polynomial in n wachsender Zahl von Rechenschritten gelöst werden können, und solchen, die eine exponentiell wachsende Zahl benötigen. Der oft zitierte Shor-Algorithmus zur Faktorisierung großer Zahlen zeigt, dass es Algorithmen gibt, die klassisch höchstwahrscheinlich nicht polynomial lösbar sind, auf einem Quantencomputer aber zur polynomialen Klasse gehören. Der Grund hierfür liegt darin, dass aufgrund der Verschränkung und dem daraus folgenden Quantenparallelismus viele „klassische" Rechenschritte durch einen „Quantenrechenschritt" ersetzt werden können. Dieses Prinzip kann man sehr gut an dem Deutsch-Algorithmus demonstrieren.

Der **Deutsch-Algorithmus** dient der effizienten Auswertung einer binären Funktion, ob diese konstant oder variierend ist. Dazu stelle man sich vor, man habe eine „Blackbox", die eine binäre Funktion

$$f: \{0, 1\} \to \{0, 1\}$$

berechnet, die also ein Bit x in ein einzelnes Bit $y := f(x)$ verwandelt. Da jeder der beiden Funktionswerte $f(0)$ und $f(1)$ einen der möglichen Werte 0 oder 1 annehmen kann, gibt es insgesamt vier Möglichkeiten für die Berechnung der Funktion und man möchte wissen, was die Box berechnet. Die Vorgänge in der Box sind jedoch so kompliziert, dass eine Berechnung 24 Stunden dauert. Man benötigt das Resultat, also ob die Funktion konstant (d. h. $f(0) = f(1)$) oder variierend (d. h. $f(0) \neq f(1)$) ist, nun aber auch in 24 Stunden, was mit einem klassischen Computer nicht möglich ist. Dieser müsste sowohl $f(0)$ als auch $f(1)$ berechnen und dann die Ergebnisse vergleichen, was insgesamt 48 Stunden dauern würde. Der Quantencomputer hingegen benötigt nur eine Messung, was also bedeutet, dass eine Berechnung ausreicht. Dies wird im Folgenden dargestellt: Angenommen, der Quantencomputer ist so programmiert, dass er auf den Produktbasiszuständen $|x\rangle\,|y\rangle$ mit $x, y \in \{0, 1\}$ die Operation

$$U(|x\rangle\,|y\rangle) = |x\rangle\,|y \oplus f(x)\rangle \text{ mit } x, y \in \{0, 1\}$$

ausführt[2] (siehe Abb. 3). Die Operation bedeutet in Worten, dass die Maschine das zweite Qu-Bit verändert, wenn f auf das erste Qu-Bit angewandt 1 ergibt, und dass die Maschine nichts macht, wenn f auf das erste Qu-Bit angewandt 0 ergibt.

Um die Reversibilität sicherzustellen, muss die Blackbox zwei Eingänge besitzen. Man kann sich vorstellen, dass das Qu-Bit $|x\rangle$ die Eingabe des Quantencomputers ist, während das zweite Qu-Bit $|y\rangle$ einen Funktionswert darstellt. Wenn man nun mit dieser Blackbox den Funktionswert $f(x)$ berechnen möchte, kann man z. B. die beiden Qu-Bits zunächst in dem Zustand $|x\rangle\,|y\rangle = |x\rangle\,|0\rangle$ präparieren. Dieser Zustand wird durch die Blackbox auf $|x\rangle\,|f(x)\rangle$ abgebildet und der Funktionswert kann nun durch Messung des zweiten Qu-Bits bestimmt werden.

Der Schlüssel zur Lösung von Deutschs Problem liegt darin, dass es die Quantenmechanik erlaubt, als Eingangszustand einen Überlagerungszustand der beiden Qu-Bits

$$|x\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \text{ und } |y\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

zu wählen, also

$$|\psi_{\text{in}}\rangle := |x\rangle|y\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right).$$

Hier wird schon das große Potential deutlich, das in den überlagerten Zuständen steckt: Wendet man die Blackbox auf $|\psi_{\text{in}}\rangle$ an, so rechnet man gleichzeitig für

NOT

a	a'
0	1
1	0

AND

a	b	a'
0	0	0
0	1	0
1	0	0
1	1	1

OR

a	b	a'
0	0	0
0	1	1
1	0	1
1	1	1

CONTROLLED NOT

a	b	a'	b'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

CONTROLLED CONTROLLED NOT

a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Kasten 1: Wahrheitstafeln

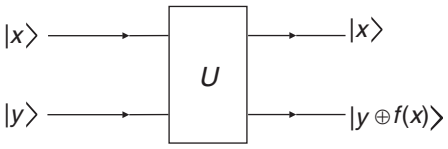

Abb. 3: Operation $U(|x\rangle\,|y\rangle) = |x\rangle\,|y \oplus f(x)\rangle$

[2] $\oplus$ *bezeichnet die binäre Addition (mod 2) – auch XOR –, d. h.*

$\oplus$	0	1
0	0	1
1	1	0

beide möglichen x-Werte, da beide in dem Zustand enthalten sind. Nach Anwendung der Operation U auf $|\psi_{in}\rangle$, erhält man

$$\begin{aligned}|\psi_{out}\rangle &:= U|\psi_{in}\rangle \\ &= \frac{1}{2}U\left(|0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle\right) \\ &= \frac{1}{2}\left(|0\rangle|0+f(0)\rangle - |0\rangle|1+f(0)\rangle \right. \\ &\quad \left. + |1\rangle|0+f(1)\rangle - |1\rangle|1+f(1)\rangle\right).\end{aligned}$$

Nun sei für $z \in \{0, 1\}$, $1 + z = \bar{z}$, wobei $\bar{1} = 0$ und $\bar{0} = 1$, dann erhält man für die binäre Addition mit

$\oplus$	$f(0)$	$f(1)$
0	$f(0)$	$\overline{f(1)}$
1	$\overline{f(0)}$	$\overline{f(1)}$

für den Ausgangszustand

$$\begin{aligned}|\psi_{out}\rangle &= \frac{1}{2}\left(|0\rangle|f(0)\rangle - |0\rangle|\overline{f(0)}\rangle + |1\rangle|f(1)\rangle - |1\rangle|\overline{f(1)}\rangle\right) \\ &= \frac{1}{\sqrt{2}}\left[|0\rangle\left(\frac{|f(0)\rangle - |\overline{f(0)}\rangle}{\sqrt{2}}\right) + |1\rangle\left(\frac{|f(1)\rangle - |\overline{f(1)}\rangle}{\sqrt{2}}\right)\right].\end{aligned}$$

Wie erwartet kommen in diesem Zustand die Funktionswerte sowohl für $x = 0$ als auch für $x = 1$ vor. Diese Eigenschaft wird als Quantenparallelismus bezeichnet.

Durch eine Messung kann man allerdings nicht beide Funktionswerte explizit bestimmen: Sobald man das erste Qu-Bit misst und dies z. B. den Wert 1 ergibt, enthält das zweite Qu-Bit nur noch Information über den Funktionswert $f(1)$. Die Frage nach der Konstanz der Funktion kann dennoch in einem Schritt beantwortet werden. Dazu betrachte man folgende Fallunterscheidung:

(1) f konstant $\Leftrightarrow f(0) = f(1)$

$$\Rightarrow |\psi_{out}\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|f(0)\rangle - |\overline{f(0)}\rangle}{\sqrt{2}}\right).$$

(2) f nicht konstant $\Leftrightarrow f(0) \neq f(1)$

$$\Leftrightarrow f(1) = \overline{f(0)},\ \overline{f(1)} = f(0)$$

$$\Rightarrow |\psi_{out}\rangle = \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{|f(0)\rangle - |\overline{f(0)}\rangle}{\sqrt{2}}\right).$$

Also gilt:

$$|\psi_{out}\rangle = \left(\frac{|0\rangle \pm |1\rangle}{\sqrt{2}}\right)\left(\frac{|f(0)\rangle - |\overline{f(0)}\rangle}{\sqrt{2}}\right).$$

Daran erkennt man, dass der Zustand des ersten Qu-Bits davon abhängt, ob die Funktion konstant ist („+“) oder nicht („–“). Folglich muss man nur noch messen, in welchem dieser beiden Zustände sich das erste Qu-Bit befindet, um die Frage nach der Konstanz der Funktion beantworten zu können, d. h., die Blackbox wird nur einmal durchlaufen.

Verallgemeinert lässt sich Folgendes festhalten: Mithilfe des Quantenparallelismus ist es zwar nicht möglich, alle Funktionswerte gleichzeitig auszuwerten, gewisse globale Eigenschaften der Funktion sind aber doch effektiver bestimmbar als mit klassischen Algorithmen.

5 Physikalische Realisierung – Stand der Forschung

5.1 Grundsätzliche Konstruktion

Um einen Quantencomputer zu bauen, sind folgende Schritte notwendig (siehe Abb. 4; s. a. [13]):

1. Schritt: Zunächst muss man sich für ein geeignetes Zwei-Zustandssystem entscheiden, d. h., man muss die Basiszustände $|0\rangle$ und $|1\rangle$ sowie ihre Überlagerungen herstellen können. Beispiele sind optische Systeme, die mit Polarisationszuständen von Photonen arbeiten, Ionen in Ionenfallen und Josephson-Kontakte, die den Stromfluss in einem Stromkreis steuern.

2.Schritt: Das System muss skalierbar sein, d. h., die Techniken müssen sich von Prototypen mit wenigen Qu-Bits auch auf Systeme mit vielen Qu-Bits übertragen lassen. Überlagerungen und Verschränkungen müssen gezielt herstellbar sein.

Schritt 1 und 2 beschreiben die Konstruktion der Hardware. Nun fehlt noch die Durchführung von Rechnungen. Dazu müssen die Quantensysteme ihre Zustände verändern. Dies wird durch unitäre Transformationen auf den Qu-Bits beschrieben.

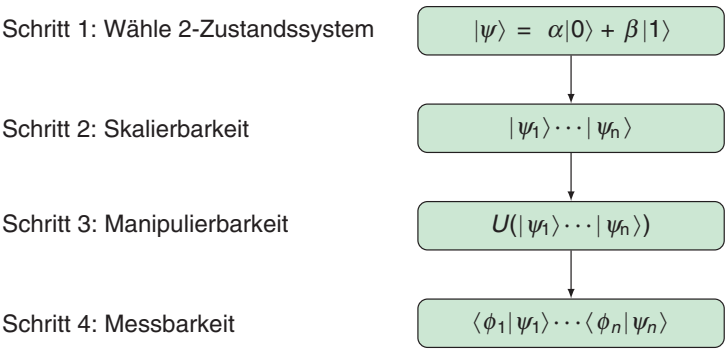

Abb. 4: Anforderungen an die Konstruktion eines Quantencomputers

3. Schritt: Das System muss gut manipulierbar sein, d. h., unitäre Transformationen müssen durchführbar sein, aus denen die logischen Gatter aufbaubar sind. Während der Durchführung dieser Operationen, die den Algorithmus implementieren, muss das System insgesamt dennoch möglichst gut von der Umgebung isoliert sein, damit keine Dekohärenz auftritt. Beispiele für Operationen sind z. B. der Halbaddierer, der Volladdierer oder Fehlerkorrekturen.

4. Schritt: Das System muss kontrollierte Messprozesse zulassen, die es erlauben, ein eindeutiges Ergebnis auszulesen.

Aus den Schritten 2 bis 4 ergeben sich zugleich die größten experimentellen Probleme, die der Realisierung eines Quantencomputers entgegenstehen: Die Skalierbarkeit, die Dekohärenz und kontrollierte Manipulierbarkeit.

Die Skalierbarkeit ergibt sich zum größten Teil aus der Wahl des Systems, seinen physikalischen Eigenschaften und den Techniken, die für die Manipulierbarkeit eingesetzt werden sollen.

Ein unausweichliches Problem ist jedoch die Dekohärenz, die umso stärker wird, je größer der Quantencomputer wird, d. h., je mehr Qu-Bits man kontrollieren muss. Hier geht die Forschung in die Richtung, dass man eher auf die Reparatur von Dekohärenz setzt, d. h. Implementierung von Fehlerkorrektur-Mechanismen, als die Dekohärenz vollkommen zu vermeiden. Fehlerkorrektur ist ohnehin notwendig, da man eine Quantenrechnung nicht unterbrechen kann, sondern erst das Endergebnis ausgelesen werden kann.

5.2 Aussichtsreiche Ansätze

Die aussichtsreichsten Ansätze scheinen im Moment die Ionenfallen zu sein oder Ansätze, die auf Festkörpertechniken beruhen. Zu Beginn der Forschung wurden die schnellsten Erfolge mit Kernspintechniken erzielt, die in geeigneten Flüssigkeiten durchgeführt wurden. Diese Methode ist allerdings praktisch nicht skalierbar. Daher ist man nun zur Nutzung von Kernspinresonanztechniken in Festkörpern, z. B. zum Implementieren von Fehlstellen in Diamantgittern, übergegangen [16].

Nahezu alle Festkörpersysteme haben den Vorteil, dass in der Festkörperphysik äußerst reichhaltige Experimentiertechniken und Experimentiererfahrungen genutzt werden können und die Skalierbarkeit in der Regel gut erreichbar zu sein scheint. Dies trifft auf Quantenpunkte ebenso zu wie auf Josephson-Kontakte.

6 Ein Vortrag für Schüler

Im Folgenden wird ein möglicher Vortrag bzw. eine kurze Unterrichtseinheit für Schülerinnen und Schüler skizziert (für weitere Hinweise oder Anregungen siehe auch [17, 18]).

6.1 Einleitung und Motivation

Zu Beginn sollte kurz dargelegt werden, welche Überlegungen die Entwicklung des Quantencomputers angestoßen haben:

1. Das Moore'sche Gesetz, das sich bislang empirisch bestätigt hat und vorhersagt, dass etwa im Jahr 2020 die Anzahl der Basiselemente von integrierten Schaltkreisen so groß ist, dass die Basiselemente eines Computers von der Größe einzelner Atome sind.
2. Überlegungen, wie man quantenmechanische Probleme am besten simulieren oder berechnen könnte.
3. Wie man die Eigenschaften der Quantenphysik für effiziente Berechnungen nutzen könnte, z. B. durch „eingebaute" Parallelität von Rechenschritten.

Ein Quantencomputer würde es erlauben, zum einen komplexere Probleme in Angriff zu nehmen, die bislang mit klassischen Computern nur ineffizient lösbar sind, und zum anderen auch durch die Reversibilität die Entropieerzeugung zu reduzieren.

6.2 Stärken eines Quantencomputers

Im Zusammenhang mit den Stärken eines Quantencomputers im Vergleich zum klassischen Computer können die folgenden Punkte diskutiert werden:

1. Aufgrund der Zufälligkeit von Messergebnissen kann ein Quantencomputer (genauer: bereits eine sehr einfache Implementierung mithilfe eines Zweizustandssystems) echte Zufallsfolgen erzeugen. Dies ist von großer Bedeutung für Verschlüsselungen und wird in der Quantenkryptographie genutzt.
2. Es wird dargestellt, dass Überlagerung und Verschränkung es erlauben, durch eine einzige Operation zahlreiche Rechenschritte gleichzeitig auszuführen (Quantenparallelismus).

Dabei ist hervorzuheben, dass diese Parallelität von einem grundsätzlich anderen Charakter ist, als die modernen Parallelrechner, die auf ihren Prozessoren entweder völlig unabhängige Prozesse verarbeiten oder aber untereinander ihren Rechenfortschritt kommunizieren müssen. Solche klassischen Parallelrechner hat mittlerweile wahrscheinlich jeder Jugendlicher in seinem Laptop oder Smartphone (nämlich einen Prozessor mit mehr als einem Kern).

Dadurch, dass in einem Quantencomputer die Notwendigkeit der Kommunikation zwischen parallel ablaufenden Berechnungen entfällt, lassen sich einige Probleme effizienter als mit einem klassischen Computer lösen, wie beispielsweise das mathematische Problem der Faktorisierung großer Zahlen mithilfe des Shor-Algorithmus. Auf der Schwierigkeit, mit klassischen Methoden große Zahlen in kurzer Zeit zu faktorisieren, beruht z. B. die Sicherheit von Verschlüsselungssystemen (beispielsweise der RSA- Algorithmus, der u. a. zur Verschlüsselung von Geheimzahlen im Bankwesen bzw. auch von E-Mails oder Mobilfunknetzen verwendet wird). Die Realisierung eines Quantencomputers würde also dazu führen, dass man auf dem Gebiet der Kryptographie ganz neue Algorithmen entwickeln muss.

6.3 Vergleich von klassischem Computer und Quantencomputer

Anschließend werden den Schülerinnen und Schülern Parallelen und Unterschiede zwischen klassischem Computer und Quantencomputer verdeutlicht. Beide Computer arbeiten mit Bits und mit logischen Verarbeitungsschritten (Gattern) auf diesen Bits. Der Unterschied liegt in Folgendem:

a) **Art der Bits:** Der klassische Computer arbeitet mit klassischen Bits, der Quantencomputer mit Quantenbits, sogenannten Qu-Bits. Beide Arten von Informationsträgern können jeweils zwei Zustände annehmen – jedes Bit einen der Zustände 0 oder 1 und jedes Qu-Bit einen der Zustände $|0\rangle$ oder $|1\rangle$. Das Besondere an den Qu-Bits ist, dass sie darüber hinaus auch einen Überlagerungszustand annehmen können.
Kombiniert man n (Qu-)Bits, so lassen sich jeweils 2^n verschiedene kombinierte Zustände darstellen. Während sich die Bits eines klassischen Computers in jeweils einem der 2^n (kombinierten) Zustände befinden und eine Berechnung auf der Grundlage *eines* Zustandes durchgeführt und ein Ergebnis erhalten wird, können die Qu-Bits auch einen überlagerten Zustand (Superposition) annehmen, sodass sich der Speicherbereich eines Quantencomputers also quasi gleichzeitig in *allen seinen möglichen* 2^n (kombinierten) Zuständen befindet und parallel mehrere, genauer gesagt 2^n Rechnungen durchgeführt respektive 2^n Werte berechnet werden können (Quantenparallelismus).
Insbesondere heißt das, dass sich mithilfe eines Quantencomputers einige Probleme (zeit-)effizienter als mit einem klassischen Computer lösen lassen, da mehrere Inputs eines Problems simultan in der Zeit berechnet werden können, in der eine klassische Berechnung durchgeführt wird.

b) **Auslesbarkeit:** In einem klassischen Computer können jederzeit z. B. Zwischenergebnisse ausgelesen werden, ohne den Rechenfortschritt substantiell zu stören. Ein solches Auslesen ist aber eigentlich eine Messung. Dies hat zur Folge, dass in einem Quantencomputer das Auslesen von Zwischenergebnissen nicht möglich ist, da die Messung den Ablauf der Rechnung irreversibel unterbrechen würde. Am Schluss der Rechnung, die daher „unsichtbar" verläuft und deren Endzeitpunkt man vorher genau bestimmen muss, kommt beim Auslesen des Rechenergebnisses der Zufälligkeitscharakter der Messung zum Tragen: Jede Messung in der Quantenphysik liefert nur einen aller möglichen Werte einer Rechnung, sodass die restlichen Ergebnisse unwiderruflich verloren gehen. Man muss also vorher den Ablauf der Rechnung so gestalten, dass die Wahrscheinlichkeit des gesuchten Ergebnisses möglichst hoch ist.
Bei einer Primfaktorzerlegung von 21 beispielsweise könnte der Rechner folgende Ergebnisse ausgeben: (1, 21) oder (21, 1) oder (3, 7) oder (7, 3). Die Ergebnisse (1, 21) und (21, 1) sind trivial und nicht zweckdienlich. Gegebenenfalls wird man also die Rechnung mehrfach durchführen müssen, ehe man das gesuchte und aussagekräftige Resultat erhält.

c) **Informationsverarbeitung:** Für beide Computer muss man ein Programm schreiben, das die Reihenfolge der Rechenschritte auf der Grundlage von logischen Verknüpfungen (Gatter) festlegt. Dabei können im Prinzip alle Programme eines klassischen Computers mithilfe von wenigen elementaren logischen Gattern wie das NOT-Gatter, AND-Gatter und OR-Gatter realisiert werden. Da ein Quantencomputer wegen der Reversibilität der quantenphysikalischen Zeitentwicklung der Zustandsfunktion ausschließlich reversibel arbeiten kann, können AND- oder OR-Gatter in der Quanteninformation nicht verwendet werden. Diese beiden Gatter können jedoch durch die reversiblen CNOT- und CCNOT-Gatter ersetzt werden. In der

Praxis genügen jedoch das NOT- und CNOT-Gatter.

An dieser Stelle kann auch der oben beschriebene Deutsch-Algorithmus im Detail besprochen werden.

6.4 Experimentelle Realisierung

Zum Schluss kann die Frage behandelt werden, wie sich Quantencomputer realisieren lassen. Dabei bewegt man sich im Spannungsfeld zwischen einem einerseits ungestört ablaufenden Rechenprozess, der zugleich erfordert, dass das Quantensystem von seiner Umgebung möglichst vollständig isoliert ist, um die Dekohärenz zu verhindern. Andererseits müssen die einzelnen Qu-Bits identifiziert, adressiert und ausgelesen werden können. Somit ist ein gezielt an- und ausschaltbarer Einfluss der Umgebung notwendig.

In allen bisherigen Ansätzen zu Realisierungen von Quantencomputern ist die Bedingung der Skalierbarkeit von wenigen auf viele Qu-Bits noch nicht erfüllt. In diesem Zusammenhang besteht die Schwierigkeit, dass eine Vergrößerung des Systems die Probleme die Adressierbarkeit und Dekohärenz betreffend nicht vervielfachen, sondern nur anteilig erhöhen sollten. Weitere Schwierigkeiten wie die Implementierung von Quantengattern und die effiziente Implementierung von Fehlerkorrekturen, hinsichtlich der in den letzten Jahren erhebliche Fortschritte gemacht wurden und die weiterhin intensiv im Fokus der Forschung stehen, werden an dieser Stelle nicht thematisiert.

Folgende Ansätze verdienen eine besondere Erwähnung:

1. Quantenoptische Quantencomputer
2. Quantencomputer auf Basis der Festkörperphysik (Fehlstellen in Diamant, spuraleitende Stromkreise, Quantenpunkte, ...)
3. Ionenfallen

7 Abschluss

Bei der experimentellen Realisierung eines Quantencomputers besteht das Hauptproblem darin, einen „universellen Quantencomputer“ zu konstruieren, der in der Lage ist, *alle* geeigneten Quantenalgorithmen abzuarbeiten. Die bisherigen Ansätze konzentrieren sich lediglich auf spezielle Klassen von Algorithmen.

Eine der ersten industriellen Realisierungen eines auf der Grundlage der Quantentheorie konstruierten Computers ist der „D-Wave Quantencomputer“. Es ist derzeit jedoch umstritten, ob der D-Wave Quantencomputer einen Quantencomputer im engeren Sinne darstellt, da seine Funktionsweise nicht in erster Linie auf dem Phänomen der Verschränkung, sondern auf dem quantenmechanischen Tunneleffekt beruht. Letzterer soll es ermöglichen, Optimierungsprobleme besonders effizient zu lösen. Damit ist der D-Wave Quantencomputer keinesfalls ein universeller Quantencomputer, sondern spezialisiert auf Optimierungsprobleme. Der Shor-Algorithmus zur Faktorisierung großer Zahlen beispielsweise ist auf dem D-Wave Quantencomputer nicht implementierbar. Die mit dem D-Wave Quantencomputer bisher erhaltenen Ergebnisse sind kompatibel sowohl mit einem klassischen als auch mit einem Quantencomputer, bei dem möglicherweise einige Bits miteinander verschränkt sind. Eine effizientere Lösung von Problemen mit dem D-Wave Quantencomputer im Vergleich zu einem klassischen Computer konnte bisher nicht erreicht werden. Dies könnte allerdings auch daran liegen, dass die mit dem D-Wave Computer untersuchten Probleme vergleichsweise einfach waren. ■

Literatur

[1] K. Schmeh, „US-Monsterrechner droht, die Welt ins Chaos zu stürzen”, Focus-Online vom 08.01.2014. http://www.focus.de/wissen/experten/schmeh/ quantencomputer-der-nsa-quantencomputer-koennten-die-welt-ins-chaos-stuerzen-3_id_3522157.html

[2] N. Lossau, „Was die neuen Superrechner alles können”, Die Welt vom 03.01.2014. http://www.welt.de/wissenschaft/article123501740/Was-die-neuen-Superrechner-alles-koennen.html

[3] R. Scharf, „Wenn man mit Photonen rechnet”, Frankfurter Allgemeine vom 31.01.2007. http://www.faz.net/aktuell/wissen/physik-chemie/quantencomputer-wenn-man-mit-photonen-rechnet-1407423.html

[4] C. Meier, „Was man von Quantencomputern erwarten darf (und was nicht)”, Neue Züricher Zeitung vom 13.11.2014. http://www.nzz.ch/wissenschaft/physik/was-man-von-quantencomputern-erwarten-darf-und-was-nicht-1.18422829

[5] P. Gotzner, „Quantencomputer: Physiker entwickeln neues Bauteil für Superrechner”, SPIEGEL ONLINE vom 10.04.2014. http://www.spiegel.de/wissenschaft/technik/quantencomputer-forscher-kombinieren-atom-und-photon-zu-neuem-bauteil-a-963608.html

[6] T. Albash, T. F. Rønnow, M. Troyer, und D. A. Lidar, „Reexamining classical and quantum models for the D-Wave One processor”, The European Physical Journal Special Topics, Vol. 224, Nr. 1, S. 111–129, 2015. http://link.springer.com/article/10.1140/epjst/e2015-02346-0

[7] Wikipedia, „Timeline of quantum computing”, https://en.wikipedia.org/wiki/Timeline_of_quantum_computing

[8] G. E. Moore, „Cramming more components onto integrated circuits”, Electronics, Vol. 38, Nr. 8, 1965. ftp://download.intel.com/sites/channel/museum/Moores_Law/Articles-Press_Releases/Gordon_Moore_1965_Article.pdf

[9] R. P. Feynman, „Viel Spielraum nach unten – Eine Einladung in ein neues Gebiet der Physik”, Kultur & Technik, 2000. http://www.deutsches-museum.de/fileadmin/Content/data/020_Dokumente/040_KuT_Artikel/2000/24-1-1.pdf

[10] D. Deutsch, „Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer”, Proc. Roy. Soc. Lond., Vol. A400, S. 97–117, 1985.

[11] P. W. Shor, „ Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer”, SIAM J. Sci. Statist. Comput., Vol. 26, S. 1484, 1997.

[12] P. W. Shor, „ Introduction to Quantum Algorithms”, eprint arXiv:quant-ph/0005003, Apr. 2000. http://arxiv.org/abs/quant-ph/0005003

[13] D. P. DiVincenzo, „Topics in quantum computers”, in: Mesoscopic electron transport. Springer, 1997, S. 657–677. http://link.springer.com/chapter/10.1007/978-94-015-8839-3_18

[14] Q. I. Science und T. E. Panel, „Quantum Computation Roadmap”. http://qist.lanl.gov/qcomp_map.shtml

[15] G. Benenti, G. Casati, und G. Strini, Principles of Quantum Computation and Information. New Jersey: World Scientific, 2004, Vol. Basic concepts, S. 118 ff.

[16] D. Lu, A. Brodutch, J. Park, H. Katiyar, T. Jochym-O'Connor, und R. Laflamme, „ NMR quantum information processing,” arXiv preprint arXiv:1501.01353, 2015. http://arxiv.org/abs/1501.01353

[17] G. Pospiech, „Quantencomputer – Was verbirgt sich dahinter?” Der mathematische-naturwissenschaftliche Unterricht, Vol. 53, Nr. 4, S. 195–202, 2000.

[18] B. Schorn, „Quantenphysik in der Schule. Eine Unterrichtskonzeption zur Einführung in die Quantenphysik für die 10. Jahrgangsstufe”, Dissertation, Technische Univerität Dresden, 2014.

Anschriften der Verfasserinnen

Prof. Dr. Gesche Pospiech, Technische Universität Dresden, Fakultät Mathematik und Naturwissenschaften, Fachrichtung Physik 01062 Dresden
E-Mail: gesche.pospiech@tu-dresden.de
Dr. Bernadette Schorn, I. Physikalisches Institut IA, RWTH Aachen, Sommerfeldstr. 14, 52074 Aachen
E-Mail: schorn@physik.rwth-aachen.de