Vorwort des Herausgebers

Der November 2015 stand im Zeichen des 100. Geburtstags der Allgemeinen Relativitätstheorie Albert Einsteins. Dabei stellte ich fest, dass auch zwei andere Jubiläen zu feiern waren: die spezielle Relativitätstheorie wurde im Jahr 1905 veröffentlicht, und den grundlegenden Durchbruch zur Quantenmechanik publizierte Werner Heisenberg im Juli 1925. Über diese drei Wunderjahre der Physik berichte ich im letzten Kapitel dieses Buches.

Auch zwei Briefe, die Heisenberg mit dem Manuskript dieser Arbeit im Juli 1925 an Wolfgang Pauli, seinen engen Studien-und Forscherfreund schickte, drucken wir hier ab, ebenso wie den Vorschlag Paulis an das Nobelkomitee, der zusammen mit weiteren 28 Vorschlägen von Fermi, Perrin, Planck, Bohr, Wentzel, Klein, Einstein, Joos, Franck u.a. zur Verleihung des Nobelpreises 1932 an Heisenberg führte.

Die beiden ersten Kapitel sind den Vorträgen bei der Mitgliederversammlung im Oktober 2015 gewidmet. Rainer Blatt

(Innsbruck) beschreibt den Weg zum Quantencomputer, und Peter Schmüser (Hamburg) schildert, wie unser heutiges Leben von den Anwendungen der Quantenmechanik bestimmt wird.

Im Februar 2016

KONRAD KLEINKNECHT
VORSITZENDER DER HEISENBERG-GESELLSCHAFT

RAINER BLATT

Quantencomputer – Rechenkunst nach Heisenberg

Neue Rechentechniken sind seit Jahrtausenden die Grundlage für den technischen Fortschritt und haben in den meisten Fällen große technologische Umwälzungen zur Folge. Mit zunehmender Komplexität der zu bewältigenden Probleme wurden Algorithmen, Rechenhilfen und Rechenmaschinen entwickelt, mit denen immer aufwändigere Routineaufgaben bearbeitet werden konnten. Trotz visionärer Ideen war die technische Realisierung von maschinellen Rechnern in einigen Fällen für viele Jahre nicht möglich, weil ausgereifte Technologien nicht zur Verfügung standen. So hat zum Beispiel Charles Babbage (1791–1871) um 1830 eine Differenzenmaschine entworfen, mit deren Hilfe mechanisch multipliziert und dividiert werden kann. Deren technische Ausführung hätte aber mehrere Tonnen Materialien benötigt und wäre mit der damals verfügbaren Technologie kaum möglich gewesen, so dass ihre Konstruktion schließlich nach Jahren eingestellt wurde. Die grundlegenden Ideen von Charles Babbage zur Konstruktion dieser

und der nachfolgenden Maschinen waren aber wegweisend für die Entwicklung mechanischer Rechenmaschinen. Den ersten mechanischen, frei programmierbaren Computer der Welt hat schließlich Konrad Zuse (1910–1995) mit seiner Z1 im Jahre 1937 im Wohnzimmer seiner Eltern konstruiert und betrieben. Danach setzte die Entwicklung elektrischer bzw. elektronischer Rechner in großem Stil ein. Im Jahre 1947 arbeitete der ENIAC (Electronic Numerical Integrator And Computer) an der University of Pennsylvania mit mehr als 18.000 Vakuumröhren, wog etwa 30 Tonnen und hatte die Ausmaße eines kleinen Saales. Erst die Entwicklung des Transistors und die daraus resultierende Entwicklung der integrierten Schaltkreise hat die Rechnertechnologie der vergangenen Jahrzehnte ermöglicht.

Computertechnologie – Gestern und Heute

Den rasanten Fortschritt der Computertechnologie, wie wir ihn seit ca. 50 Jahren kennen, hat Gordon E. Moore (*1929), einer der Gründerväter der Firma Intel, mit dem nach ihm benannten *Moore'schen Gesetz* beschrieben. Nach diesem, in den 60er Jahren zunächst empirisch formuliertem Gesetz, verdoppelt sich etwa alle 18 Monate die Computerleistung. Bestimmt wird diese Leistungsfähigkeit meist mit der Anzahl der Transistoren, die man pro Computerchip unterbringen kann[1]. Dies geht in der Regel einher mit einer entsprechenden Verkleinerung der einzelnen Halbleiterbausteine und einer demzufolge schnelleren Schaltzeit. Die beobachtete Leistungssteigerung wurde dann die Grundlage für die so genannten *roadmaps* der Halbleiterindustrie, nach denen die jeweils neuen Werkzeuge rechtzeitig entwickelt und bereitgestellt wurden, um den entsprechenden Zuwachs der Computerleistung auch tatsächlich erzielen zu können. In einer etwas anderen Darstellung hat R. W. Keyes (1921–2010) bereits 1988 aufgetragen, wie viele Atome zur Darstellung eines klassischen Bits benötigt werden. Auch diese Kurve zeigt die Zunahme der Computerleistung durch stets

kleiner werdende Bauelemente. Wenn man diesen Darstellungen folgt und sie extrapoliert, stellt man sehr schnell fest, dass bereits in den kommenden Jahren die Grenze erreicht werden sollte, bei der ein einzelnes Atom zur Darstellung eines einzelnen Bits genügt. Die mikroskopische Welt der Atome und deren Wechselwirkung mit Ladungen und Licht kann aber nicht mehr mit den Mitteln der klassischen Physik beschrieben werden und spätestens an dieser Stelle wird klar, dass die Quantenphysik bei der Informationsverarbeitung nicht mehr ignoriert werden kann. Daher sei hier zunächst kurz zusammengefasst, was die von Heisenberg begründete Quantenphysik von der klassischen Physik so sehr unterscheidet.

Was sind Quanten, was ist Quantenphysik?

Der Begriff des *Quants* wird in der Physik seit Beginn des 20. Jahrhunderts verstanden als ein elementares Paket, d.h. als ein nicht weiter teilbares Paket der Materie oder der Energie, das deren jeweilige charakteristische Eigenschaften besitzt. Die Quanten der Materie sind demnach die Atome, die Quanten der Elektrizität sind die Elektronen und die Quanten des elektromagnetischen Feldes sind die Lichtquanten, oder wie sie modern heißen, die Photonen. Die Gründerväter der Quantenphysik fanden in den ersten Jahrzehnten des 20. Jahrhunderts sehr schnell heraus, dass es Phänomene gibt, die sich mit der klassischen Physik nicht mehr erklären lassen. Insbesondere gilt, dass ein beobachtetes, d.h. ein einer Messung unterworfenes Quantensystem anders reagiert als ein nicht beobachtetes Quantensystem. Jede Messung (Beobachtung) eines Quantensystems ändert das Quantensystem selbst, was auch als Rückwirkung der Messung bezeichnet wird. Wie Werner Heisenberg als erster erkannt hat, sind bei einer Messung etwa Ort und Geschwindigkeit eines Quants nicht gleichzeitig scharf messbar und Quantensysteme zeigen Welleneigenschaften, die sich beispielsweise in Interferenzphänomenen beobachten lassen. Diese im Expe-

riment überprüfbaren Eigenschaften begründen den Welle-Teilchen-Dualismus: Je nach Experiment und Fragestellung zeigen Teilchen Welleneigenschaften und Wellen zeigen Teilcheneigenschaften. Solche Experimente in der Quantenphysik befassen sich etwa mit dem Verhalten einzelner Quanten, z.B. bei der Wechselwirkung von Licht mit Atomen oder gar von einzelnen Photonen mit einzelnen Atomen. Über Jahrzehnte hinweg wurden solche Quantenphänomene ausgiebig untersucht und die mathematische Beschreibung der Quantenphysik, die sowohl die Wellen- als auch die Teilcheneigenschaften richtig wiedergibt, hat sich bisher in allen Details glänzend bewährt. Damit können quantenphysikalische Phänomene und Eigenschaften berechnet und vorhergesagt werden und für viele Anwendungen seit Jahrzehnten genutzt werden.

Daher hat die Quantenphysik schon seit langer Zeit einen zunehmend großen Einfluss auf technische Anwendungen und ein erheblicher Anteil der Bruttosozialprodukte der Industriestaaten wird mit Hilfe der Quantenphysik erwirtschaftet. Als Beispiele dafür seien nur die Halbleiterindustrie, die Lasertechniken, die medizinischen bildgebenden Verfahren und die gesamte Telekommunikation genannt, die ohne Quantentechniken heute nicht mehr denkbar sind.

Nach der technischen Revolution des 19. Jahrhunderts, die auf mechanischen und thermodynamischen Erkenntnissen beruhte, führte die Entwicklung und industrielle Nutzung der Elektrodynamik im 20. Jahrhundert u.a. zur modernen Elektronik und Computerindustrie. Aufgrund der vielen, heute weithin oft noch unbemerkten Anwendungen der Quantenphysik ist bereits abzusehen, dass moderne quantenphysikalische Methoden, vor allem zusammen mit den Informationswissenschaften die Basis für die Technologien des 21. Jahrhunderts sein werden. Als Paradebeispiel für die Entwicklung solcher Quantentechnologien wird oft der Quantencomputer genannt; er steht aber nur stellvertretend für viele weitere quantenphysikalische

Anwendungen, deren Entwicklung mit großer Wahrscheinlichkeit zu einer weiteren technischen Revolution führen wird.

Warum Quantencomputer?

Neben der schon besprochenen Verwendung von Quantentechnologien für viele technische Anwendungen insbesondere für die Optik, Elektronik und die Kommunikation stellt sich die Frage, inwieweit die Quantenphysik selbst zur Informationsverarbeitung herangezogen werden kann.

Solche Ideen wurden in den 80er Jahren des letzten Jahrhunderts von Richard Feynman (1918–1988) diskutiert. Er hatte erkannt, dass größere quantenmechanische Rechnungen nicht mehr auf klassischen Computern gemacht werden können[2] und er schlug die Verwendung von Quantencomputern vor. Im Jahr 1982 waren das visionäre Ideen, die aber mangels geeigneter Plattformen als exotisch und nicht realisierbar empfunden wurden. Erst Mitte der 90er Jahre wurden Konzepte und Ideen entwickelt, wie Quantenrechner tatsächlich gebaut werden können. Auslöser dieser erneuten Beschäftigung mit den quantenmechanischen Möglichkeiten zur effizienten Berechnung war die Erkenntnis, wie mit Hilfe eines Quantencomputers ein mathematisch schwieriges Problem, nämlich die Faktorisierung großer Zahlen, viel schneller gelöst werden kann als dies mit klassischen Computern möglich ist.

Die faktische Unmöglichkeit, mit klassischen Computern eine große Zahl in vertretbarer Zeit in ihre Primfaktoren zu zerlegen, ist die Grundlage für die Verschlüsselung von Daten und Nachrichten, wie zum Beispiel mit dem RSA-Algorithmus. Der Rechenaufwand, eine Zahl mit L Stellen zu faktorisieren, steigt exponentiell mit der Länge L der Zahl an. Hätte man dagegen einen Quantencomputer für die Berechnungen zur Verfügung, so zeigte P. Shor 1994 mit dem nach ihm benannten Shor-Algorithmus[3], dass der Rechenaufwand nur polynomial in L anwächst. So sind sicherheitsrelevante Informationen und Nachrichten-

übertragungen möglicherweise für Unbefugte einsehbar. Damit begann die ernsthafte Suche nach einer physikalischen Lösung zur Konstruktion eines Quantencomputers. Im Jahr 1997 stellte Lov Grover (*1960) einen Algorithmus vor, der mit Hilfe eines Quantencomputers in der Lage ist, eine unsortierte Datenbank sehr viel schneller zu durchsuchen, als dies mit klassischen Methoden möglich ist[4]. Mit klassischen Rechnern muss man im Mittel die Hälfte aller Einträge durchsuchen, mit einem Quantencomputer und unter Verwendung des Grover-Algorithmus genügt bereits die Wurzel aus der Anzahl der Einträge, um den gesuchten Datensatz zu finden. Die Vision von R. Feynman, Quantensysteme mit Hilfe von quantenmechanischen Systemen zu berechnen oder zumindest zu simulieren wurde in den darauffolgenden Jahren erneut aufgegriffen und stellt heute einen großen Forschungszweig der Quanteninformationsverarbeitung dar.

Darüber hinaus ist aus messtechnischer Sicht eine universell programmierbare Quantenmaschine von großem Interesse, denn für die Anwendung von quantenphysikalischen Methoden lassen sich mit einem (universellen) Quantencomputer beliebige Quantenzustände per Knopfdruck programmieren und zur Verfügung stellen. Dies ist besonders wichtig für Anwendungen in der Präzisionsmesstechnik (Metrologie), die mit Hilfe von Quantentechnologien empfindlicher, schneller und in programmierbarer (d.h. auf die jeweilige Problemstellung abgestimmter) Weise messen kann[5].

Angestoßen vom Shor- und Grover-Algorithmus und motiviert von den absehbaren Möglichkeiten für quantentechnologische Anwendungen hat die Suche nach einem realisierbaren Quantencomputer in der Mitte der 90er Jahre begonnen und das Gebiet der Quanteninformationsverarbeitung hat seither eine stürmische Entwicklung erfahren.

Wie baut man einen Quantencomputer?

Bevor wir diese Entwicklung nachvollziehen können, sollen an dieser Stelle zuerst die Grundbausteine für Rechenmaschinen besprochen werden. Abbildung 1 zeigt die für einen klassischen Rechner notwendigen Grundelemente. Man benötigt für einen Rechenvorgang zunächst eine Anfangsinformation, d.h.

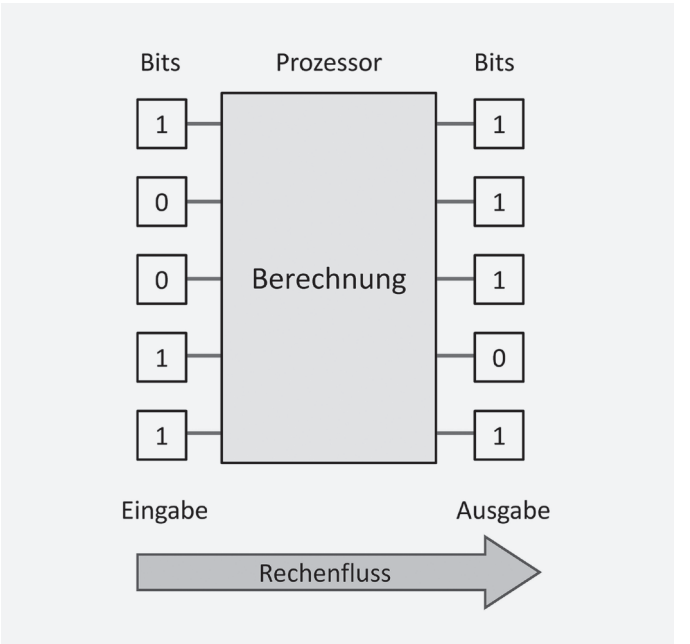

Abb. 1: In einem klassischen Rechner wird die Information in Form von Bits als Eingabe dargestellt. Abhängig davon, wie die Bits als physikalische Objekte implementiert werden, erfolgt deren Verarbeitung im mit dazu passenden physikalischen Prozessen und die Darstellung der Ausgabe erfolgt ebenfalls in den mit physikalischen Objekten repräsentierten Bits. Der Rechenfluss verläuft in diesem Schema von der Eingabe zur Ausgabe, hier von links nach rechts.

eine Eingabe, die im Rechner als physikalisches Objekt in Form von Bits *x,* wobei *x* den Wert 0 oder 1 einnehmen kann, d.h. ($x \in \{0,1\}$).

Die Informationsverarbeitung erfolgt dann nach einem vorgegebenen Programm in einem Prozessor, d.h. es läuft ein physikalischer Prozess ab, der die eingegebenen Bits so verändert, dass das Ergebnis schließlich in Form von Bits (die wiederum als physikalische Objekte repräsentiert sind) am Ausgang vorliegt. Je nach Bauform können die Bits als verschiedene physikalische Objekte implementiert werden, etwa als mechanische Objekte in einem Abakus oder aber als Ströme oder Spannungen in einem elektronischen Computer. Die physikalischen Prozesse während der Berechnung müssen mit diesen physikalischen Objekten arbeiten und schließlich die Ausgangsinformation darstellen. In klassischen Computern sind dies klassische Objekte und klassisch ablaufende Prozesse, wie etwa das mechanische Verschieben von Objekten im Abakus oder aber Schaltprozesse mit elektronischen Transistoren in herkömmlichen Rechnern. In Quantencomputern dagegen sind die Objekte Quantensysteme, Träger der Information sind also einzelne Quanten, und die Prozesse sind quantenmechanisch zu beschreibende Prozesse, die gemäß den Gesetzen der Quantenphysik das Wellenverhalten der quantenmechanischen Objekte verarbeiten müssen.

(a) Quantenbits

Das klassische Bit x, ($x \in \{0,1\}$) entspricht der Information eines Schalters mit genau zwei Stellungen, nämlich *An = 1* und *Aus = 0,* während für ein Bit, das Quanteneigenschaften trägt wegen des Wellenverhaltens auch Überlagerungen möglich sein müssen. Das quanten-mechanische Analogon zum Bit wird als *Quantenbit (Qubit)* bezeichnet und wir betrachten dazu ein quantenmechanisches System mit genau zwei Zuständen $|0\rangle$, $|1\rangle$, ein sogenanntes Zwei-Niveau-System. Eine Überlagerung $|\psi\rangle$ der beiden Zustände wird in der folgenden Form notiert