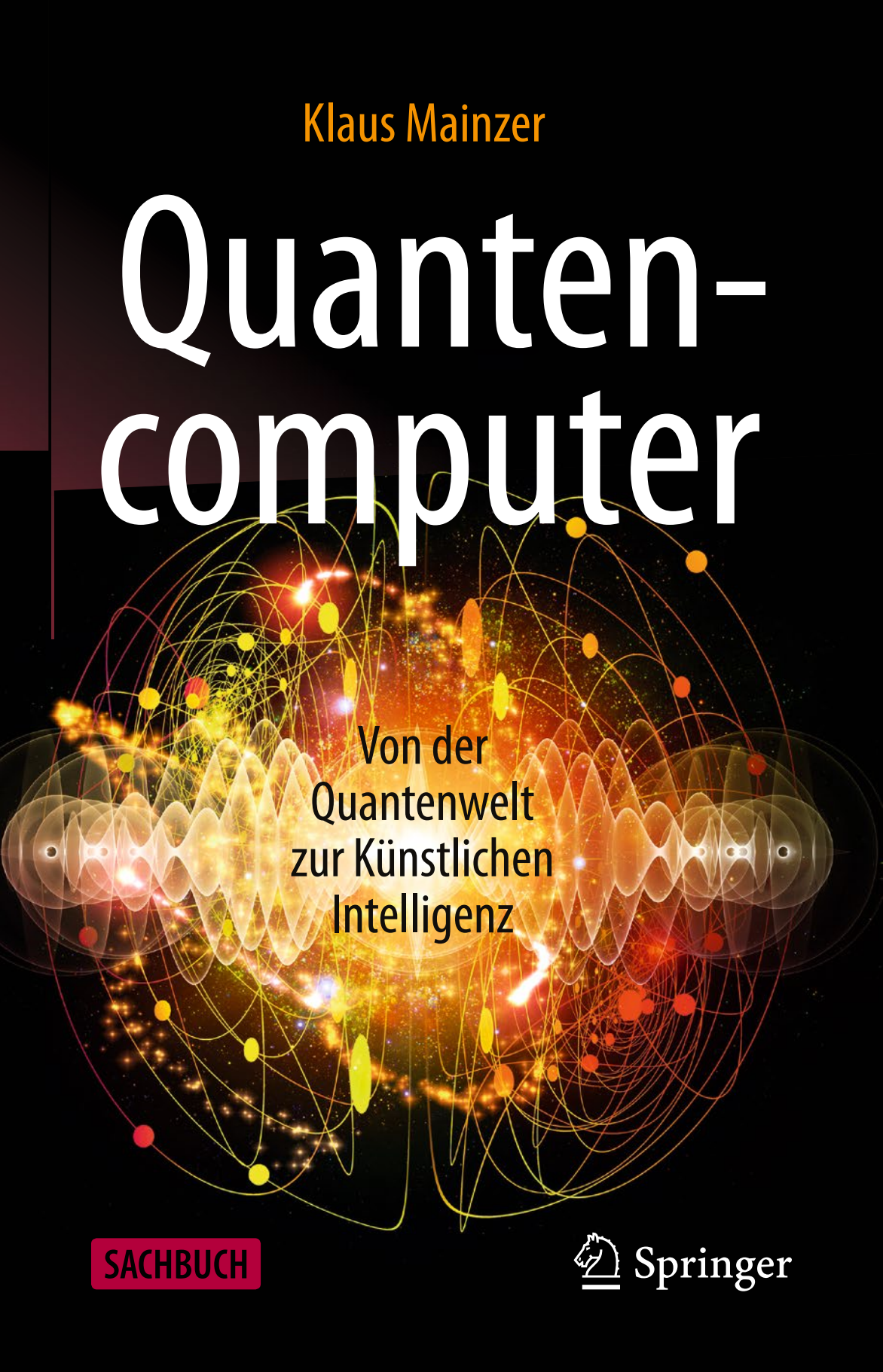
Klaus Mainzer

Quanten-computer



Von der Quantenwelt zur Künstlichen Intelligenz

SACHBUCH

Springer

Quantencomputer

Klaus Mainzer

Quantencomputer

Von der Quantenwelt zur Künstlichen Intelligenz

Springer

Klaus Mainzer
TUM Senior Excellence Faculty
Technische Universität München
Carl Friedrich von Weizsäcker Center
Eberhard Karls Universität Tübingen
München, Deutschland

ISBN 978-3-662-61997-1 ISBN 978-3-662-61998-8 (eBook)
https://doi.org/10.1007/978-3-662-61998-8

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer

Springer ist ein Imprint der eingetragenen Gesellschaft Springer-Verlag GmbH, DE und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

Vorwort

Die Quantenwelt ist längst im Alltag angekommen, ohne dass es vielen bewusst ist. Dazu gehören Transistoren, Dioden und Laser, die aus Alltagsgeräten nicht mehr fortzudenken sind und wie selbstverständlich in der Mess- und Kommunikationstechnik, industriellen Fertigung, Medizintechnik, Unterhaltungselektronik und 3D-Druck angewendet werden. Den Quantentechnologien dieser ersten Generation ist gemeinsam, dass Quanteneffekte nur indirekt genutzt werden.

Wir leben derzeit in der zweiten Generation der Quantentechnologie, in der Grundprinzipien der Quantenmechanik gezielt in quantenmechanischen Geräten umgesetzt werden. Dazu gehören erste Prototypen von Quantencomputern, klassische Supercomputer mit Quantensimulation, Quantenkryptografie und Quantenkommunikation, Quantensensorik und Quantenmesstechnik. Zur Lösung einer speziellen Aufgabe konnte 2019 ein spezieller Quantencomputer von Google erstmals die Überlegenheit eines Quantencomputers über einen klassischen Supercomputer beweisen. Im selben Jahr war bereits vorher mit IBM Q ein Quantencomputer vorgestellt worden, dem wenigstens im Prinzip die Architektur eines Mehrzweck-Computers zugrunde liegt.

Dennoch wird die Quantenwelt in der Öffentlichkeit häufig noch immer als rätselhaft wahrgenommen. Was Einstein 1935 als spukhafter Effekt vorkam, ist längst Grundlage umwälzender Quantenkommunikation in Glasfasernetzen und Satellitentechnik, die ein zukünftiges Quanteninternet ankündigt. Quantencomputer als Mehrzweckrechengeräte sind nur die Spitze des Eisbergs mit einer Technologie, die sich schrittweise als Netzwerk unserer Zivilisation ausbreitet. Deshalb ist es auch irreführend, von „disruptiver“ Technik zu sprechen, die unvermittelt plötzlich da ist. Das erscheint nur denjenigen so, für die diese Technologie unverständlich ist.

Umso dringender ist es, die Grundlagen der Quantenwelt als Hintergrund dieser Technologie zu verstehen. Grundlagen und Zusammenhänge begreifen, setzt auch ein Verständnis der mathematischen Sprache voraus. Sie ist letztlich Ausdruck des „gesunden Menschenverstandes“, der sich begrifflich präzise Instrumente schafft, um Experimente zu berechnen und Technik zu ermöglichen. Rechenverfahren werden in Algorithmen und Computerprogramme umgesetzt.

Die Quantenwelt mit ihrer Mathematik ermöglicht Algorithmen und Verfahren, die ungleich reichhaltiger, schneller und effektiver als klassische Computer sind. Ein Quantenbit enthält nicht nur zwei alternative Informationszustände der Bits 0 und 1, sondern alle zwischen 0 und 1 liegenden Zustände. Solche „Überlagerungen" (Superpositionen) von Zuständen führen in der Technik zum Quantenparallelismus, der eine gleichzeitige Berechnung aller Zustände ermöglicht und damit erhebliche Beschleunigung gegenüber nacheinander ausgeführten Rechenschritten in klassischen Computern. Quantenmechanische „Verschränkungen" entfernter Ort ermöglichen augenblickliche Quantenkommunikation. Verteilte Wahrscheinlichkeiten eröffnen in der Quantenwelt das „Durchtunneln" von Hindernissen, vermeiden klassische Umwege und beschleunigen damit Rechenverfahren erheblich.

Im Quanten Computing wachsen also Physik, Informatik, Logik und Mathematik zusammen. Ob nun die Welt selbst ein Computer ist (Leibniz) oder wenigstens durch einen Computer simulierbar ist (Feynman), wie ein roter Faden zieht sich diese Vision durch die Ideengeschichte der Neuzeit. Auf dem Hintergrund meiner bisherigen Buchpublikationen war das auch meine persönliche Faszination, die mich zum Schreiben dieses Buchs motivierte, das die Interessen für Physik, Informatik, Logik und Mathematik zusammenführt.

All das ist kein Hexeneinmaleins, sondern ergibt sich schrittweise aus den Grundlagen der Quantenwelt. Sie ist, wie Richard Feynman als Pionier des Quantencomputers richtig feststellte, die eigentliche und umfassende physikalische Wirklichkeit. Die klassische Physik beschreibt nur approximativ den Ausschnitt der makroskopischen Welt. In diesem Sinn ist die Quantenphysik ein natürlicher Zugang zur Welt und keine Frage von Zauberkunststücken wie „Schrödingers Katze" mit ihren wunderlichen Leben. Zudem entspricht das Denken in Statistik und Wahrscheinlichkeiten durchaus der Alltagserfahrung, die keineswegs wie klassische Mechanik determiniert ist.

Quantentechnologie und Quantencomputer werden zunehmend unser Alltag sein. Nach Elektrifizierung und Digitalisierung im 20. Jahrhundert steht nun die Quantisierung der Kommunikations- und Versorgungsnetzwerke an. Das geschieht schrittweise und nicht „disruptiv". Auch der universelle Quantencomputer wird nicht „disruptiv" die klassische Rechnertechnologie ablösen, sondern zunehmend in klassische Rechnerstrukturen eingebettet und neue Aufgaben lösen, die mit klassischen Verfahren ausgeschlossen waren. Man spricht bereits von „ökologischen" Rechnernetzwerken, die sich schrittweise über die Welt ausbreiten.

Diese Rechnernetzwerke sind der Hintergrund einer weltweiten Automatisierung durch Künstliche Intelligenz. In meinem Buch „Künstliche Intelligenz. Wann übernehmen die Maschinen?" (Springer 2. Aufl. 2019) wird Machine learning herausgestellt, das Automatisierung in Robotik, Industrie- und Arbeitswelt verwirklicht. In Zukunft werden enorme Rechnerkapazitäten notwendig sein, um die gewaltigen Datenmengen dieser Zivilisation zu bewältigen. Die Komplexität des Lebens, seine unverstandenen Zusammenhänge, seine Empfindlichkeit und Gefährdung, die sich in Krankheiten wie Krebs ebenso zeigt wie in viralen Pandemien, erfordert neue Tools in Life Sciences und Medizin. Hier wird Bioinformatik zunehmend auf Machine Learning und geeignete Rechner- und Speicherkapazitäten

zurückgreifen müssen. Das gleiche gilt zur Bewältigung weltweiter Finanz- und Wirtschaftskrisen, die Frühwarnsysteme erfordern. So wachsen Quantentechnologie und Quantencomputer mit dem großen anderen HighTech Hype, der Künstlichen Intelligenz, zusammen. Insofern kann dieses Buch als Fortsetzung meines Springer-Buchs über Künstliche Intelligenz gelesen werden, ohne es vorauszusetzen.

Mit Quantentechnologie, Quantencomputer und künstlicher Intelligenz zeichnet sich aber nicht nur eine Potenzierung neuer Möglichkeiten ab, sondern auch von Gefährdungen. Neben einer absolut sicheren Quantenkryptografie könnte Quantenkommunikation auch militärisch z. B. für eine weltweite Drohnensteuerung genutzt werden. Quantencomputer, die klassische Supercomputer schlagen, ermöglichen ungleich mehr und effektivere Kontrolle und Manipulation weltweit. Daher erhebt sich die Forderung nach frühzeitiger Technikgestaltung, die ich bereits in meinem KI-Buch gestellt hatte, noch einmal verstärkt. Damit wird aber auch klar, dass unter dem Eindruck weltweiter Krisen die Forderung nach einer nachhaltigen Technik unverzichtbar ist. Am Ende braucht es eine zukünftige Politik, in der die zentrale Rolle von nachhaltiger Wissenschaft und Technik im 21. Jahrhundert verstanden und zur Grundlage politischer Urteilsfindung und Entscheidung gemacht wird.

München Klaus Mainzer
Mai 2020

Inhaltsverzeichnis

1
Einführung

Unsere Welt wird zunehmend durch schnelle Algorithmen gesteuert, die ohne enorme Rechenleistungen von Computern nicht möglich wären. In Zivilisationen mit Milliarden von Menschen lassen sich Logistik und Mobilität, Versorgungs- und Verwaltungsprobleme, Industrie- und Arbeitswelt ohne ihren Einsatz nicht bewältigen. Aber auch um nachhaltige Zukunftsstrategien für Klima, Umwelt, Gesundheit und Medizin zu entwickeln, müssen gewaltige Datenmengen berücksichtigt werden, die ohne die Rechenleistung von Algorithmen und Computer nicht erfasst und bewertet werden können. Die ersten Anwendungen von Algorithmen der Künstlichen Intelligenz sind erst seit einigen Jahren aufgrund der nun erreichten Rechenleistung von Computern möglich.

Bereits Ende der 1960er-Jahre hatte der Physiker Gordon Moore, Mitbegründer des Chipherstellers Intel im Silicon Valley, vorausgesagt, dass sich die Computerleistung in einem Zeitraum von ca. 18 Monaten verdoppelt bei gleichzeitiger Verkleinerung und Verbilligung von Computerchips. Dieses „Mooresche Gesetz“ hat sich bis vor kurzem mehr oder weniger bestätigt. Tatsächlich bildet es das Rückgrat der gesamten bisherigen Digitalisierung von den Superrechnern bis zu immer leistungsfähigeren Smartphones und Robotern. Elementarteilchenbeschleuniger, Klimaprognosen und soziale Netzwerke, um nur einige Beispiele zu nennen, wären ohne das Mooresche Gesetz nicht möglich gewesen.

2008 erreichte der IBM-Superrechner Roadrunner die Marke von Petaflops, d. h. 10^{15} Rechenschritten pro Sekunde. Etwa ab diesem Zeitraum stieg die Rechenleistung nicht mehr so rasant wie in den vorherigen Jahrzehnten und lag im Zeitraum von 2018 bis 2019 bei den führenden Superrechnern weltweit nur noch bei ca. zehn Prozent. Die Frage drängt sich auf: Immer kleiner – und was dann? Wird die Rechnertechnologie in den 2020er-Jahren an ihre Grenzen gelangen?

Der Grund ist: Das jahrelange Wachstum der Computerleistung des „immer schneller durch immer kleiner“ stößt nun an fundamentale Grenzen der Miniaturisierung, die mit den Naturgesetzen der Physik eng zusammenhängen. Bei Chips in atomarer Größe gelten nicht länger die Gesetze der klassischen Physik, nach denen

K. Mainzer, *Quantencomputer*, https://doi.org/10.1007/978-3-662-61998-8_1

herkömmliche Computer funktionieren. Damit betreten wir die Quantenwelt, deren Gesetze Anfang des 20. Jahrhunderts die Physik revolutionierten.

Wer nur unsere Alltagswelt kennt, mag zunächst über die merkwürdigen Eigenschaften der Quantenwelt erstaunt sein. Albert Einstein selber sprach von „spukhaften Fernwirkungen“ zwischen Quantenobjekten an verschiedenen Orten, die Quantenphysiker als „verschränkt“ bezeichnen. Ein staunendes Publikum nahm zur Kenntnis, dass Quantenobjekte wie z. B. Elementarteilchen zugleich Welle und Teilchen sein können. Quantenobjekte können sogar zugleich in mehreren Zuständen sein, was Erwin Schrödinger, einer der Begründer der Quantenmechanik, im Bild einer Katze veranschaulichte, die in einem geschlossenen Kasten zugleich tot als lebendig sein könne. Erst nach Öffnen des Kastens wissen wir, ob ein miteingeschlossenes tödliches Gas zufällig freigesetzt wurde oder nicht. Nach Schrödinger zerfällt dann die „Überlagerung“ (Superposition) der Zustände in eine der beiden möglichen Zustände „tot“ oder „lebendig“.

Mittlerweile liegt ein höchst effizienter mathematischer Formalismus vor, der diese Phänomene erfasst und der modernen Quantentechnologie zugrunde liegt. Generationen von Studierenden haben diesen Formalismus gelernt und wenden ihn tagtäglich an. Viele Geräte des Alltags beruhen bereits auf den Gesetzen der Quantenmechanik, ohne dass sich die Verbraucher dessen bewusst wären. Die ersten Schritte waren schon seit den 1950er-Jahren Atomuhr und Laser. Heute kommen Quantenoptik, Atomoptik, Quantenelektronik und Quantennanomechanik hinzu. Die Frage liegt nahe: Lässt sich Quantentechnologie auch nutzen, um auf dieser Grundlage neuartige Rechner zu bauen – „Quantencomputer“, die noch effizienter als herkömmliche Supercomputer sind und ein neues Zeitalter jenseits des Mooreschen Gesetzes eröffnen?

Theoretisch tauchte die Forderung nach einem Quantencomputer erstmals in einer Arbeit des berühmten Nobelpreisträgers Richard Feynman 1982 auf. Tatsächlich ist die Theorie auf diesem Gebiet der Technik seit dieser Zeit weit voraus. Bereits in den 1980er- und 1990er-Jahren wurden Algorithmen entwickelt, die den mathematischen Formalismus der Quantenmechanik theoretisch nutzen, um Probleme wesentlich schneller als herkömmliche Algorithmen zu lösen. So wären mit dem Shor-Algorithmus Verschlüsselungsprobleme, die als praktisch unlösbar gelten und damit bis heute Sicherheit garantieren, mit schneller Rechenzeit lösbar.

Ziel dieses Algorithmus ist es, die Teiler einer ganzen Zahl zu bestimmen, die als Kode einer Information verstanden wird. Dekodierung des Zahlenschlüssels entspricht seiner Zerlegung in Teiler. Die Kodierung als Nachweis, dass diese Teiler multipliziert den Zahlenkode ergeben, ist einfach. Aber die Umkehrung der Dekodierung ist ein aufwendiger Suchprozess: Bei einem konventionellen Suchprozess der Teiler führen größer werdende Zahlenkodes zu einer exponentiellen Wachstumsexplosion von Möglichkeiten. Daher macht sich dieser Algorithmus die quantenmechanische Eigenschaft der „Überlagerung“ (Superposition) von Quantenständen zu Nutze, um viele Teilaufgaben (im Beispiel die Suche eines Teilers) quasi in einem Streich zu erledigen. Man spricht dann vom Quantenparallelismus.

Die Grundidee lässt sich wieder im Bild von Schrödingers Katze erläutern: Statt der alternativen Zustände „tot“ oder „lebendig“ haben wir es in der klassischen Welt

der Digitalisierung mit den alternativen Bitzuständen „0“ oder „1“ zu tun, mit deren Sequenzen sich jede Art der digitalen Information darstellen lässt. Überlagerung bzw. Superposition bedeutet, dass ein Quantensystem (z. B. Elektron oder Photon) in einem Quantenzustand mit einer bestimmten Wahrscheinlichkeit im Teilzustand „0“ und mit der Restwahrscheinlichkeit im Teilzustand „1“ ist. Dieser Gesamtzustand aus den beiden statistisch verteilten Teilzuständen heißt Quantenbit (Abkürzung: Qubit). Bei einer Messung des Quantensystems (in Schrödingers Gedankenexperiment das Öffnen des Kastens) kollabiert der Gesamtzustand in einen der beiden Teilzustände entweder „0“ oder „1“. Im Quantenparallelismus lassen sich beliebig viele Qubits verbinden, um beliebig viele Bitsequenzen „auf einmal“ (parallel) zu berechnen.

Was in der mathematischen Theorie funktioniert, erweist sich in der technischen Praxis als große Herausforderung. Ein Überlagerungszustand von Quantenzuständen muss zunächst technisch präpariert werden und ist dann äußerst empfindlich gegen Umwelteinflüsse wie z. B. Temperaturschwankungen. Bei geringsten Störungen kollabiert der Überlagerungszustand und löst damit Fehler in der Rechnung aus. Dieser Vorgang wird Dekohärenz genannt. Kohärenz bezeichnet den Zusammenhang der Quantenzustände, den es technisch so lange als möglich aufrecht zu erhalten gilt. Die Dekohärenz der Quantenzustände ist daher eine große technische Hürde, die von einem Quantencomputer zu nehmen ist. Unter dieser Voraussetzung muss er dann Probleme wesentlich schneller lösen als konventionelle Supercomputer. Diese Herausforderung wird „Supremacy“ (Überlegenheit) genannt.

In den vergangenen Jahren wurden bereits verschiedene Quantentechnologien zur Lösung dieser Aufgaben vorgeschlagen, die experimentell mit wenigen Qubits erprobt wurden, ohne allerdings die Überlegenheit von Quantencomputern über konventionelle Supercomputer demonstrieren zu können. Erinnert sei an NMR (Nuclear Magnetic Resonance)-Quantenprozessoren, mit denen sich einfache Beispiele von Quantenalgorithmen realisieren ließen. Für den Shor-Algorithmus gelang als einfaches Beispiel die Faktorisierung der Zahl 15 in ihre Teiler. Als Hardware diente eine Flüssigkeit mit einer großen Anzahl von Molekülen (ca. 10^{18}) eines bestimmten Typs in einem starken statischen magnetischen Feld.

Ein Qubit wird in diesem Fall durch den Spin eines molekularen Kerns dargestellt, der quantenphysikalisch als alternativer Zustand „up“ (0) oder „down“ (1) gegeben ist. Klassisch-physikalisch lässt sich ein Spin-Zustand als eine Art Drehimpuls vorstellen, der allerdings in der Quantenwelt für die hier betrachteten Teilchen nur in zwei alternativen Zuständen gegeben ist. Die Moleküle wurden im thermischen Gleichgewicht auf Zimmertemperatur präpariert. Zur Faktorisierung der Zahl 15 war ein sieben-Qubit Molekül notwendig. Leider ist diese Technologie nicht skalierbar, da das gemessene Signal mit der Anzahl der Qubits in einem Molekül exponentiell fällt.

Ein anderes Beispiel sind optische Systeme. Hier wird ein Qubit durch die alternativen Polarisationszustände „horizontal“ und „vertikal“ eines einzelnen Photons realisiert. Die Cavity (Hohlraum) – Quantum Electrodynamics (QED) Technik geht von einem Hohlraum-Resonator aus, in dem genau ein Atom eingesperrt ist, das mit dem elektromagnetischen Feld in dem Hohlraum interagiert. Die zwei Teilzustände

eines Qubits können durch die Polarisationszustände eines einzelnen Photons oder zwei erregte Zustände eines Atoms realisiert werden. Auch hier erweist sich die Skalierbarkeit für eine große Anzahl von Operationen als schwierig.

Erprobt wurden auch sogenannte „Ionen-Fallen“, bei denen die Hardware aus einer Kette von Ionen (also positiv geladenen Atomen) besteht, die in einer linearen „Falle“ von statischen und oszillierenden elektrischen Feldern kombiniert sind. Ein Qubit ist ein einzelnes Ion mit zwei langlebigen Zuständen. Eine Kette (Array) dieser Ionen lässt sich als Register von Qubits auffassen, die mit bestimmten Laserpulsen adressiert werden können. Diese Technologie wurde frühzeitig als skalierbar eingestuft.

Das gilt auch für Quantentechnologie, die auf Eigenschaften der Festkörperphysik beruht. Das verwundert deshalb nicht, da die Festkörperphysik in den vergangenen Jahren eine Reihe neuartiger Materialien und künstlicher Strukturen in Nanoskalierung ermöglicht hat, mit denen sich die zentralen Eigenschaften des Quanten Computing wie Superpositionen und Verschränkungen realisieren lassen. Dazu gehören insbesondere supraleitende Quantenchips. Supraleiter sind Materialien, deren elektrischer Widerstand beim Unterschreiten der sogenannten Sprungtemperatur auf Null fällt. Daher wird bei supraleitenden Quantenchips die Tieftemperaturphysik zum Schlüssel, um die Kohärenz von Superpositionen im Quantenparallelismus zu garantieren. Der technische Übergang von der derzeitigen Mikroelektronik der klassischen Computer zum Quantencomputer auf der Grundlage der Festkörperphysik bietet sich an.

Das Jahr 2019 begann mit der Ankündigung von IBM, den ersten kommerziellen Quantencomputer mit 20 Qubits hergestellt zu haben. Das Gerät lässt sich zwar nicht kaufen, kann aber über eine Cloud genutzt werden. Ein Vorgängermodell arbeitete noch mit 5 und 16 Qubits. 20 Qubits galt als Schwelle zu einem arbeitsfähigen Quantencomputer. Ab 50 Qubits sollte ein Quantencomputer einem klassischen Supercomputer überlegen sein. IBM setzte auf elektrische Schaltkreise, die in supraleitenden Mikrochips integriert sind. Die Quantenprozessoren müssen mit flüssigem Helium tiefgekühlt werden, um die supraleitenden Eigenschaften zu erreichen, die stabile Kohärenz ermöglichen. Der technische Vorteil besteht darin, dass an die bewährten Verfahren der Halbleitertechnik angeschlossen werden kann.

Eine zentrale Leistung von IBM bestand darin, dass mögliche Störquellen wie Wärmeeinfluss, elektrische Streuungen oder Erschütterungen weitgehend kontrollierbar sind. Immerhin konnten die 20 Quantenbits 75 Mikrosekunden in einem ungestörten kohärenten Zustand stabilisiert werden. Praktisch ist der IBM-Q insofern bereits ein universeller Quantencomputer, da (mit der Einschränkung von 20 Qubits) verschiedenartige Probleme in Angriff genommen werden könnten. Dazu gehören komplexe Optimierungsprobleme ebenso wie Modellierungen von Vielteilchensystemen wie Festkörper, Flüssigkeiten oder Gase. Damit eröffnen sich Anwendungsperspektiven in der Materialforschung, Chemie und Pharmakologie.

Mit IBM-Q war das Wettrennen der IT-Giganten eröffnet und die Antwort von Google ließ nicht lange auf sich warten. Der supraleitende Prozessor Sycamore löste ein spezielles mathematische Problem schneller als der führende klassische Supercomputer Summit von IBM im Jahr 2019. Sycamore benötigte für dieses

Problem nur 200 Sekunden, während Summit nach eigenen Angaben von IBM mehr als zwei Tage benötigte. Damit war die Überlegenheit des Quanten Computing erstmals wenigstens für diese spezielle Aufgabe bewiesen. Grundlage waren 53 supraleitende Qubits, also etwa die Anzahl, die auch für „Supremacy" veranschlagt wurde.

Der Vergleich des Quanten Computing mit der Rechnung auf einem klassischen Computer wird durch Simulation möglich. Dafür wird ein enormer Speicherplatz im klassischen Computer benötigt. Während die Simulation von Sycamore mit 53 Qubits mehr als zwei Tage mit einer 80 Petabyte Festplatte benötigte, wären für 73 Qubits bereits 10.000 Jahre mit einer 80 Zetabyte (Zeta = 10^{21}) Festplatte notwendig. Bei der Simulation müssen entsprechend der Architektur eines klassischen Computers gewaltige Datenmengen zwischen Speicher und Prozessoren hin- und hergeschoben werden. Dabei zeigt sich ein gravierender Vorteil des Quantencomputers: Er verbraucht deutlich weniger Energie als ein konventioneller Computer und ist in diesem Sinn umweltfreundlicher.

Festgehalten werden muss allerdings auch, dass Sycamore nur eine spezielle Aufgabe lösen kann und daher noch kein Computer ist, der für verschiedene Probleme universell programmierbar ist. Es steht auch nicht fest, ob die fragilen Quantenzustände eines supraleitenden Qubits die technische Zukunft sind. Weiterhin geforscht wird daher z. B. mit gespeicherten Ionen. Jedenfalls gibt es nun bereits Quantenrechner, die für spezielle Anwendungen von Quantenalgorithmen einsetzbar sind. Das erinnert in der Geschichte der Computer an die 1930er- und 1940er-Jahre, bevor Konrad Zuse (1943) und John von Neumann (1945) ihre ersten universell programmierbaren elektronischen Computer bauten. Damals gab es auch bereits spezielle Rechner, die z. B. bestimmte Differenzialgleichungen lösen konnten. Ein Beispiel für Quanten Computing bietet die Firma Volkswagen (VW), die Quantenalgorithmen einsetzt, um bei Verkehrsstaus Alternativstrecken für jedes Fahrzeug schneller und individuell zu berechnen. Dabei werden Quantenrechner des kanadischen Unternehmens D-Waves eingesetzt.

In der Entwicklung des klassischen Computers war die Entstehung des Internets und die Digitalisierung der Gesellschaft eine nicht vorhergesehene Revolution. Anfang der 1950er-Jahre dachten führende Computerexperten wie John von Neumann noch, dass sich die Computerentwicklung auf wenige Großrechner weltweit beschränken würde. Daher wird heute bereits darüber nachgedacht, wie sich Quantencomputer weltweit vernetzen lassen. Auch hier ist die Grundlage durch eine eigentümliche Eigenschaft der Quantenwelt gelegt. Gemeint sind die eingangs erwähnten „Verschränkungen" von Quantensystemen an entfernten Orten, die Einstein als „spukhafte Fernwirkungen" bezeichnet hatte. Sie können zwar nicht zur direkten Informationsübertragung im Sinn der klassischen Elektrotechnik verwendet werden, eröffnen aber neue Möglichkeiten quantenmechanischer Messmethoden. Man spricht bereits von Quantenkommunikation, die im Quanteninternet über Glasfaserkabel und in der Satellitenkommunikation erprobt wird.

Bemerkenswert ist, wie sich weltweit Länder, Firmen und Forschungsorganisationen in Stellung bringen, um sich im globalen Wettbewerb in dem sich anbahnenden Boom der Quantencomputer und Quantenkommunikation ihre Anteile zu

sichern. In Europa beginnen sich kleinere Forschungsgruppen in der Initiative „Quantum Technology Flagship“ zu koordinieren. Beim Thema „Quantencomputer“ sind derzeit allerdings Firmen wie Google und IBM eindeutig in Führung. China beeindruckt mit ersten technischen Realisationen der Quantenkommunikation über große Entfernungen seiner Städte und in der Satellitenkommunikation. Die dabei führenden chinesischen Wissenschaftler kooperierten seit ihrer Ausbildung mit der Forschergruppe um Anton Zeilinger, der maßgebend an ersten Experimenten mit verschränkten Quantenzuständen beteiligt war.

Die Situation des Quanten Computing heute erinnert an die Entwicklung der Künstlichen Intelligenz, bevor der Boom mit dem Machine Learning einsetzte. In meinem Buch „Künstliche Intelligenz. Wann übernehmen die Maschinen?“ (Springer 2. Aufl. 2019) wird gezeigt, wie die theoretischen Grundlagen des Machine Learning und der neuronalen Netze bereits in den 1970er- und 1980er-Jahren bewiesen vorlagen, aber erst Anfang der 2010er-Jahre sich die Rechenpower abzeichnete, um diese Algorithmen in Technik, Industrie, Wirtschaft und Gesellschaft einzusetzen. Im Fall des Quantencomputers liegt der mathematische Formalismus bereits seit der ersten Hälfte des 20. Jahrhunderts vor. Die entscheidenden Eigenschaften der „Superposition“ und „Verschränkung“ sind seit dieser Zeit fundamentale Züge der Quantenwelt, die Grundlagendiskussionen in Physik, Philosophie und Erkenntnistheorie auslösten. Seit den 1980er-Jahren sind sie auch experimentell gesichert und lösten erste Schritte technischer Realisation aus.

Ziel dieses Buchs ist es wie Fall meines KI-Buchs von 2019 [1], die Grundlagendiskussion der Forschung mit ihren Anwendungen und gesellschaftlichen Auswirkungen zu verbinden. Wir sollten vorbereitet sein, Mut zur Innovation haben und die Zusammenhänge begreifen, um auf diesem Hintergrund Verantwortung für die Zukunft übernehmen zu können. Wer aber nur über gesellschaftliche Folgen plaudert, schwebt in den Wolken und hat keine Bodenhaftung. Grundlagen und Zusammenhänge begreifen, setzt auch ein Verständnis der mathematischen Sprache voraus. Mathematik ist letztlich Ausdruck des „gesunden Menschenverstandes“, der sich begrifflich präzise Instrumente schafft, um Erkenntnis und Technik zu ermöglichen.

Das zeigen die Anfänge des mathematischen Denkens bis heute: Zahlen entstehen aus Mengenvergleichen, die wir bereits aus einem frühen Entwicklungsstadium des Menschen kennen. Dasselbe gilt für die Abstraktion von geometrischen Formen als Anfängen der Geometrie. Punkte repräsentieren Körper, Pfeile ihre Bewegungsrichtung in der Vektorgeometrie. Bei Quantensystemen wie z. B. Photonen und Elektronen lassen sich aber Ort und Impuls nicht mehr unabhängig voneinander mit beliebiger Genauigkeit messen (Heisenbergs Unschärferelation), wie in der klassischen Physik angenommen wurde. Der Hilbertraum zur Beschreibung von Quantensystemen ist nichts anderes als ein Vektorraum, der diese Eigenschaften von Quantensystemen berücksichtigt.

Mit diesen theoretischen Instrumenten können wir erst in einen Mikrokosmos vorstoßen, der uns mit unserer Umgangssprache verschlossen bliebe. Deshalb werden in diesem Buch auch die physikalischen Grundbegriffe der Quantenwelt und ihre mathematische Darstellung anschaulich erklärt. Ähnlich wie im Fall der KI,

müssen wir dazu in den Maschinenraum der Innovationen klettern. Erst dann wird klar, dass es sich nicht um Hexeneinmaleins handelt, das wir fürchten müssen. Nur wer verstanden hat, was die Maschinen leisten und was sie nicht leisten, kann auch, um im Bild eines Schiffs zu bleiben, auf der Brücke mitreden. Hier ist der Ort, wo Verantwortung zu übernehmen ist. Noch einmal: Am Ende sollten wir vorbereitet sein, wenn sich die Potenziale von Quantencomputern mit Künstlicher Intelligenz verbinden.

In 2. Kapitel werden zunächst die Grundlagen eines klassischen Computers erklärt. Was heißt maschinelle Berechenbarkeit und Entscheidbarkeit? Wie leistungsfähig sind Algorithmen? Nach diesen Kriterien lassen sich Komplexitätsklassen von Problemen einführen. Auf dieser Grundlage baut der klassische Informationsbegriff auf. Neben den logisch-mathematischen Grundlagen geht es aber auch um die physikalischen Grundlagen eines klassischen Computers nach den Gesetzen der klassischen Physik. Im 3. Kapitel werden die physikalischen Grundlagen der Quantenmechanik erklärt. Was ist ein Quantensystem? Wie entwickeln sich zeitabhängig Quantenzustände eines Quantensystems? Erklärt wird der Welle-Teilchen Dualismus ebenso wie Superposition und Verschränkung von Quantensystemen. Erkenntnistheoretisch sind diese Begriffe mit fundamentalen Eigenschaften unseres Realitätsverständnisses verbunden. Auch diese philosophischen Probleme der Quantenmechanik werden diskutiert.

Auf der Grundlage der beiden vorausgehenden Kapitel werden in Kap. 4 die Grundlagen eines Quantencomputers erklärt. Was ist ein Quantenbit im Unterschied zu einem klassischen Bit als Informationseinheit? Ein Quantencomputer wird als Quanteninformation verarbeitende Maschine eingeführt. Analog zu einem universellen klassischen Computer lässt sich ein universeller Quantencomputer wenigstens theoretisch definieren. Die Superposition von Quantenzuständen liegt dem Quantenparallelismus als zentralem Rechenvorteil eines Quantencomputers zugrunde. Dabei ist die Dekohärenz eine technische Herausforderung. In Kap. 5 werden die Grundlagen einzelner Quantenalgorithmen erklärt. Dazu gehören als Beispiele der Deutsch-Algorithmus, die Quanten-Fourier-Transformation, der Grover-Algorithmus, deren praktische Auswirkungen gravierend sind. In Kap. 6 werden zunächst die Grundlagen der klassischen Kryptografie von der Vernam-Kodierung, dem Problem des öffentlichen Schlüssels bis zu den heutigen RSA-Protokollen erläutert. Wären Quanten-Fourier Transformation und Shor-Algorithmus technisch mit Quantencomputern realisierbar, würde quasi über Nacht die Sicherheit aller bisherigen Verschlüsselungen in Banken und öffentlichen Einrichtungen, im Militär und Zivilleben zusammenbrechen. Die gute Nachricht ist, dass Quantenkryptografie (wenigstens theoretisch) vollständig sichere Kodierung mit verschränkten Quantensystemen anbietet. Kap. 7 behandelt die Grundlagen der Quantenkommunikation. Theoretisch beruht sie auf der Quantenmechanik verschränkter Quantensysteme mit Quantenteleportation. Mittlerweile liegt eine eigene Quanteninformationstheorie vor, die sich grundlegend von der klassischen Shannonschen Informationstheorie und der algorithmischen Informationstheorie nach Andrei N. Kolmogorov unterscheidet.

Die Zukunft des Quanten Computing wird eng mit der Zukunft der Künstlichen Intelligenz (KI) verbunden sein. Quantenalgorithmen können KI-Programme unterstützen und neue Anwendungsmöglichkeiten erschließen. Dieses Buch wir daher die Zukunft der Künstlichen Intelligenz mit Quanten Computing herausstellen. Dazu werden zunächst in Kap. 8 die Grundlagen der klassischen Künstlichen Intelligenz nach der klassischen Algorithmentheorie im Anschluss an mein Buch über Künstliche Intelligenz von 2019 [1] zusammengestellt. Darauf aufbauend geht es in Kap. 9 um die Grundlagen der Quanten-KI. Eine zentrale Rolle können leistungsstarke Quantenalgorithmen z. B. bei der Mustererkennung spielen, die eine zentrale Anwendung des Machine Learning ist. Quantenmechanische Superpositionen und Verschränkungen wurden auch im Zusammenhang mit der natürlichen Intelligenz auf der Grundlage der Gehirnforschung diskutiert. Daher schließt dieses Kapitel mit einem Ausblick auf die Frage, ob eine starke Künstliche Intelligenz mit technischen Quantensystemen zu erwarten ist, die natürliche Intelligenz überflügelt. Damit ist auch eine gravierende philosophisch-erkenntnistheoretische Frage durch Quantencomputer aufgeworfen.

Quantenkommunikation wird bereits über Landverbindungen mit Glasfasernetzen und durch Übertragungen im freien Raum mit Satellitentechnik verwirklicht. Damit eröffnen sich Perspektiven eines globalen Quanteninternets, die in Kap. 10 erörtert werden. Die Übertragungen mit Satellitentechnik lassen ahnen, wie einmal Quantenkommunikation in der zukünftigen Erforschung und Erschließung des Weltraums eingesetzt werden könnte.

Quanteninformationstheorie eröffnet aber auch eine grundlegende Perspektive auf unser Verständnis des Universums. Wenn das Universum nach den Gesetzen der Quantenphysik funktioniert, dann geht es um die Interaktion von Quantensystemen und die dabei stattfindende Transformation von Quantenzuständen und Quanteninformation. Bereits der Lehrer von Richard Feynman, der amerikanische Physiker Archibald Wheeler, stellte die von ihm selbst als fundamental bezeichnete Frage: „It from Bit?“ Am Anfang wäre danach das Quantenbit als kleinste Informationseinheit. Dann wäre aber das Universum selbst ein gewaltiger sich entwickelnder Quantencomputer. Dieses Bild erinnert an das Zeitalter der Mechanik im 17. und 18. Jahrhundert, als man sich die Welt nach dem Vorbild der damals am höchsten entwickelten Technik als gewaltiges mechanisches Uhrwerk vorstellte.

Wie lassen sich aber Quantenalgorithmen und Quanten-Schaltkreise technisch realisieren? Kap. 11 behandelt die verschiedenen technischen Ansätze, die bisher als Hardware für Quantencomputer vorgeschlagen wurden. Ihre jeweiligen Vor- und Nachteile, Chance auf zukünftige Skalierbarkeit und Anschluss an bereits erfolgreiche Quantentechnologie entscheiden über die Frage, welche Hardware am Ende das Rennen macht und in die Rechnerarchitektur eines effizienten Quantencomputers eingebaut wird.

Wie immer diese technische Perspektive des Quantencomputers aussehen mag, seine gesellschaftlichen Folgewirkungen werden uns alle auf diesem Planeten betreffen. Darum geht es im letzten Kap. 12. Quantencomputer und Quanteninformation werden zu einer bis dahin nicht gekannten Beschleunigung von Problemlösungen führen. Gleichzeitig lässt sich abschätzen, dass mit dieser Technologie weniger

Energie bei größerer Effizienz verbraucht würde. Sie eröffnet neue Formen der Kommunikation. Verbunden mit den heute bereits existierenden Möglichkeiten der Künstlichen Intelligenz zeichnet sich aber auch eine Beschleunigung von Potenzialen ab, die geradezu nach einer Technikgestaltung unter Beachtung sowohl ökonomischer als auch ökologischer und ethischer Kriterien verlangt. Dieses Buch zielt darauf ab, die Grundlagenforschung dieser neuen Technologie mit den Herausforderungen ihrer Technikgestaltung zu verbinden.

Wie schon erwähnt, werden in den folgenden Kapiteln die Grundlagenbegriffe des Quanten Computing erklärt. Dabei wird in der Regel auch auf die technischen und formalen Darstellungen Bezug genommen. Hintergrundwissen über mathematische Begriffe, Beweise und technische Verfahren, aber auch über historische Zusammenhänge, sind mit * bezeichnet und in kleinerer Schrift gesetzt. Zentrale Definitionen und Sätze sind hervorgehoben.

Literatur

1. Mainzer K (2019) Künstliche Intelligenz – Wann übernehmen die Maschinen? Springer, Heidelberg 2. Aufl.

2
Was kann ein klassischer Computer?

Wie arbeitet ein Computer? Bei einem Standardcomputer (z. B. Laptop, PC oder Smartphone) ist die technische Hardware für den Benutzer unter vielen Schichten von Bedienungssoftware verborgen. Der Standardaufbau eines Computers orientiert sich an einer nach dem Computerpionier John von Neumann benannten Architektur:

Auf der untersten Schicht gibt es einen Zentralprozessor (CPU) aus Registern, in denen Zahlen als Spannungszustände gespeichert und verarbeitet werden. Maschinelle Datenverarbeitung setzt voraus, dass Daten in physikalische Zustände eines Computers übersetzt werden. Im Prozessor werden dazu zwei Impulse mit verschiedener Spannung unterschieden. Der einzelne Impuls wird durch ein Bit dargestellt. Ziffern, Buchstaben und Sonderzeichen, wie wir sie von der Tastatur eines PCs kennen, werden automatisch in einen Binärkode aus den Symbolen 0 und 1 übersetzt, dem eine Bitfolge der beiden Stromimpulse als den physikalischen Zuständen der Maschine entspricht. Ein Zentralprozessor besteht aus einem Rechenwerk, das die Rechenoperationen durchführt, einigen Registern, in denen Daten und das Ergebnis aufgenommen werden, einem Steuerwerk bzw. Befehlsregister, das den jeweils anstehenden Befehl enthält, und einem Befehlszähler mit der Adresse des Befehls aus dem Steuerwerk. Hinzu kommt ein Arbeitsspeicher, der aus Speicherzellen für Daten und Befehle besteht. Ein Maschinenprogramm setzt sich aus einer Folge von Befehlen zusammen, die aus den Registern abgerufen, dekodiert und ausgeführt werden.

Um den mathematischen Begriff der Berechenbarkeit definieren zu können, wird von diesen technisch-physikalischen Details eines realen Computers nach Marvin Minsky abgesehen:

K. Mainzer, *Quantencomputer*, https://doi.org/10.1007/978-3-662-61998-8_2

Definition einer Registermaschine [1] Eine ideale Registermaschine besteht aus einer beliebigen, aber endlichen Anzahl von Registern, in denen jede der Zahlen 0, 1, 2, … (oder entsprechende Kodes) gespeichert werden kann.

Das Programm einer idealen Registermaschine verfügt über nur zwei Elementaroperationen, und zwar die beiden Befehle, den Inhalt eines Registers um 1 zu erhöhen oder um 1 zu vermindern. Wenn ein Register bereits leer ist (also 0 enthält), soll die Subtraktion von 1 wieder 0 ergeben.

Diese Elementaroperationen können durch Verkettung oder Iteration zu komplexen Programmen zusammengesetzt werden. Unter Verkettung wird die Hintereinanderausführung zweier Programme verstanden. Bei der Iteration wird die Wiederholung eines Programms davon abhängig gemacht, ob ein Kontrollregister leer ist.

Eine mathematische Funktion (z. B. die Addition $f(x, y) = x + y$) wird durch das Programm einer Registermaschine berechnet, indem die Maschine das Programm für beliebige Inputwerte (z. B. x und y bei der Addition) in ihren Registern ausführt, bis sie nach endlich vielen Schritten stoppt und im Ergebnisregister der Funktionswert (z. B. $x + y$ bei der Addition) steht.

Definition der Registermaschinen-Berechenbarkeit Eine Funktion heißt durch eine Registermaschine berechenbar, wenn es ein Programm einer Registermaschine zur Berechnung der Funktion gibt.

Die Anzahl der Elementaroperationen, die ein Programm zur Berechnung benötigt, ist durch das Programm eindeutig festgelegt und hängt von den Inputwerten ab. Nun könnte eine Funktion durch verschiedene Programme berechnet werden. Die Komplexität einer Funktion wird daher durch das beste Programm bestimmt, das die Funktion mit der kleinsten Anzahl von Rechenschritten berechnet.

Ein älteres, aber gleichwertiges Konzept einer idealen mathematischen Rechenmaschine stammt von Alan Turing. Eine Turingmaschine soll ebenfalls jedes effektive Verfahren symbolischer Datenverarbeitung ausführen können. Anschaulich erinnert ihre Architektur eher an das technische Modell einer Schreibmaschine, bei der ein Schreibmaschinenkopf einen Papierstreifen bedruckt. Für den mathematischen Begriff der Berechenbarkeit spielen diese technisch-physikalischen Details aber keine Rolle.

Definition einer Turingmaschine Eine Turingmaschine besteht aus einem Prozessor und einem (potenziell) unbegrenztem Band, das in Felder unterteilt ist. Die Elementaroperationen eines Turing-Programms besagen, dass der Prozessor das Band im Arbeitsfeld nacheinander mit endlich vielen Symbolen bedrucken, löschen, nach links und rechts um ein Feld verschieben oder stoppen kann.

Sowohl Turing- als auch Registermaschinen sind ideale mathematische Maschinen, da sie unbegrenzt steigerbare Speicherkapazitäten voraussetzen – sei es als unbegrenzt verlängerbares Rechenband bei der Turingmaschine oder als unbegrenzt vergrößerbare Registeranzahl. Jedenfalls kann bewiesen werden, dass jede durch eine

Turingmaschine berechenbare Funktion auch durch eine Registermaschine berechnet werden kann und umgekehrt.

Diese mathematischen Maschinenkonzepte mögen auf den ersten Blick sehr einfach erscheinen. Vom logischen Standpunkt aus ist aber jeder programmkontrollierte Allzweckcomputer, auf dem verschiedene Programme laufen können, nichts anderes als eine technische Realisation einer universellen Turingmaschine, die jedes mögliche Turing-Programm ausführen kann. Auch eine universelle Turingmaschine ist ein logisch idealisiertes Konzept, da ein technischer Allzweckcomputer wie z. B. ein Laptop nur endlich viele Programme anwendet. Analog dazu lässt sich eine universelle Registermaschine definieren, die jedes Registermaschinenprogramm ausführen kann.

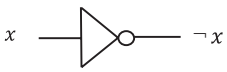
Eine Registermaschine ist immer noch sehr abstrakt mit Blick auf die Architektur und Arbeitsweise eines technischen Computers. Daher soll noch das dazu äquivalente Schaltkreismodell eines Rechners betrachtet werden, das auch als Vorlage für die Definition eines Quantencomputers in Kap. 3 dienen wird. In einem Computer wird Informationsverarbeitung auf Rechenschritte mit Bits 0 und 1 als Grundeinheiten klassischer Information zurückgeführt. Die Rechenschritte werden durch Rechenoperationen wie Addition und Multiplikation für die binäre Zahlen 0 und 1 ausgeführt. Die folgende Tabelle zeigt die binäre Addition $s = x \bigoplus y$ (Addition modulo 2) für zwei Bits x und y und den Übertrag c (englisch: carry):

x	y	s	c
0	0	0	0
0	1	1	0
1	0	0	0
1	1	0	1

Diese Idee geht historisch auf Leibniz zurück, weil er der Auffassung war, dass Rechnen mit 0 und 1 weniger Rechenregeln benötigt und deshalb einfacher sei als mit Dezimalzahlen. Technisch lassen sich 0 und 1 als alternative Spannungszustände darstellen und eröffneten damit die Technologie von elektronischen Rechnern seit den 1940er-Jahren. Im Schaltkreismodell werden die Operationen der Rechenschritte durch Gatter mit Input- und Output-Leitungen realisiert. Ein Schaltkreis besteht aus Gattern, die durch Leitungen verbunden werden. Hier kommen einige Beispiele von klassischen Gattern mit ihren Tabellen für Input- und Output-Zuständen und ihrem Gattersymbol im Schaltkreismodell [2]:

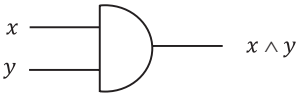
NOT-Gatter

x	$\neg x$
0	1
1	0



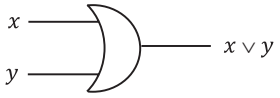
***AND*-Gatter**

x	y	$x \wedge y$
0	0	0
0	1	0
1	0	0
1	1	1



***OR*-Gatter**

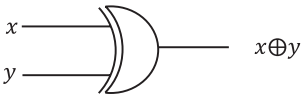
x	y	$x \vee y$
0	0	0
0	1	1
1	0	1
1	1	1



Das *XOR*-Gatter entspricht dem logischen Entweder-Oder (mit X für „exclusive“), während *NAND*-Gatter und *NOR*-Gatter jeweils das *AND*-Gatter und *OR*-Gatter verneinen (mit *N* für „not“):

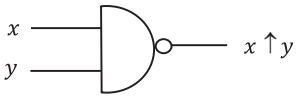
***XOR*-Gatter**

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0



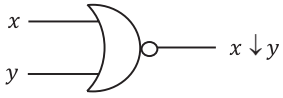
***NAND*-Gatter**

x	y	$x \uparrow y$
0	0	1
0	1	1
1	0	1
1	1	0



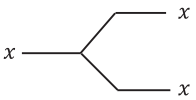
***NOR*-Gatter**

x	y	$x \downarrow y$
0	0	1
0	1	0
1	0	0
1	1	0

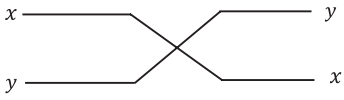


Ein weiteres Beispiel, das noch im Rahmen der Quantencomputer wichtig wird, ist das *FANOUT* bzw. *COPY*-Gatter, das einen Input x mit der Regel $COPY : x \longmapsto (x,x)$ dupliziert. Demgegenüber vertauscht das *CROSSOVER* - bzw. *SWAP*-Gatter zwei Inputs:

***COPY*-Gatter**



***SWAP*-Gatter**



Ein einfaches Beispiel eines Schaltkreises ist der Halbaddierer HA, der aus einem *XOR*- und *AND*-Gatter zusammengesetzt ist. Verzweigungen in Leitungen werden durch Punkte angezeigt. Die beiden Inputbits x_1 und x_2 führen zu einem Outputbit y für die Summe y der beiden Inputbits und einem Übertragungsbit c (englisch: carry) (Abb. 2.1).

Im Schaltkreismodell bedeutet universelle Berechenbarkeit, dass sich jeder Schaltkreis auf eine Verschaltung bestimmter Gatter zurückführen lässt. Die Menge dieser Gatter wird universell genannt. Es lässt sich beweisen, dass die Menge aus *AND*-, *OR*-, *NOT*- und *COPY*-Gattern universell ist.

Neben Turing-, Registermaschinen und Schaltkreisen wurden verschiedene andere mathematisch äquivalente Verfahren zur Definition berechenbarer Funktionen entwickelt. Ein Beispiel sind rekursive Funktionen. Dazu gehören elementare Funktionen wie z. B. die Zählfunktion $n(x) = x + 1$, die ausgehend von 0 jede Zahl x im nachfolgenden Schritt $x + 1$ um die Einheit 1 erhöht und so die Zahlen 0, 1, 2, … sukzessive erzeugt. Diese Funktion entspricht offenbar einer rekursiven Iterationsschleife, die ausgehend von 0 auf vorher gebildete Werte x immer wieder dasselbe Schema $n(x)$ anwendet und so iterierte Werte 0, $n(0)$, $n(n(0))$, … erzeugt. Hinzu kommen Ersetzungs- und Iterationsschemata für rekursive Funktionen, die Verkettungen und Iterationen von Maschinenprogrammen entsprechen. Schließlich führt der Suchprozess einer Lösung mit rekursiven Mitteln zum Ergebnis, wenn die Existenz einer Lösung gesichert ist.

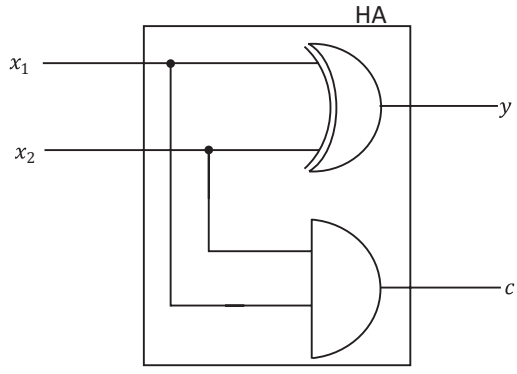
Jedes dieser verschiedenen mathematischen Berechenbarkeitskonzepte ist in einem anschaulichen Sinn berechenbar. So macht es uns z. B. keine Schwierigkeiten, die Nachfolgerfunktion bzw. das Hinzufügen einer Einheit (also den Zählprozess) als berechenbar zu akzeptieren. Eine endliche Iteration oder Verkettung von berechenbaren Prozessen wird berechenbar bleiben und nicht zu unberechenbaren Prozessen führen. Zudem lässt sich beweisen, dass alle bekannten Definitionen von Berechenbarkeit mit Turingmaschinen, Registermaschinen, rekursiven Funktionen etc. mathematisch äquivalent sind.

Daher stellte Alonzo Church in einer nach ihm benannten These fest, dass der Begriff der Berechenbarkeit durch jede einzelne dieser mathematisch äquivalenten Definitionen (z. B. der Turing-Berechenbarkeit) vollständig erfasst sei.

Churchsche These

Jede berechenbare Funktion ist auf einer Turingmaschine berechenbar.

Die Churchsche These kann natürlich nicht bewiesen werden, da sie mathematisch präzise Begriffe wie z. B. Turingmaschinen, Registermaschinen oder rekursive Funktionen mit intuitiven Vorstellungen von Berechenbarkeit vergleicht. Sie wird



x_1	x_2	y	c
0	0	0	0
1	0	1	0
0	1	1	0
1	1	0	1

Abb. 2.1 Klassischer Schaltkreis eines Halbaddierers

allerdings insofern gestützt, als verschiedene Definitionen, die jeweils bloß im intuitiven Sinn berechenbare Verfahren präzisieren, tatsächlich mathematisch äquivalent sind. Daher können wir von Berechenbarkeit überhaupt sprechen, ohne auf ein besonderes Verfahren zurückzugreifen.

Berechenbarkeitsverfahren heißen auch Algorithmen, und zwar nach dem persischen Mathematiker Muhammad al-Chwarismi, der um ca. 800 n. Chr. Lösungsverfahren für einfache algebraische Gleichungen suchte. Nach Churchs These können wir sagen, dass jedes berechenbare Verfahren (Algorithmus) durch eine Turingmaschine ausgeführt werden kann. Da für jede berechenbare Funktion ein Maschinenprogramm existiert, kann sie immer auf einem universellen programmkontrollierten Computer berechnet werden.

Im Rahmen seines Forschungsprogramms „mathesis universalis“ hatte Gottfried Wilhelm Leibniz bereits eine „Kunst der Entscheidung“ (ars iudicandi) gefordert, um Probleme durch Rechnen zu entscheiden [3]. Wir beschränken uns zunächst auf die Entscheidbarkeit arithmetischer Eigenschaften, z. B. auf die Frage, ob eine natürliche Zahl x gerade ist oder nicht. Wir können dazu auch fragen, ob x zur Menge der geraden natürlichen Zahlen gehört oder nicht. Diese Frage lässt sich immer in endlich vielen Schritten entscheiden, indem wir für eine vorgelegte Zahl x nachprüfen, ob sie durch 2 teilbar ist oder nicht. Das wiederum lässt sich z. B. mit einem einfachen Programm einer Turingmaschine nachrechnen.

Definition der effektiven Entscheidbarkeit

- Für eine Teilmenge M der natürlichen Zahlen (z. B. die Menge der geraden Zahlen) lässt sich eine charakteristische Funktion f_M mit $f_M(x) = 1$ definieren, falls x Element von M ist, und $f_M(x) = 0$, falls x nicht Element von M ist.
- Die Teilmenge M bzw. die dadurch definierte Eigenschaft heißt effektiv entscheidbar, wenn ihre charakteristische Funktion (wonach eine Zahl zu M gehört oder nicht) effektiv berechenbar ist.

Im Sinn der Churchschen These ist so der Begriff der effektiven Entscheidbarkeit überhaupt definiert. Darüber hinaus haben wir damit ein Entscheidbarkeitskonzept für alle Eigenschaften und Probleme, die sich arithmetisieren, also durch zahlentheoretische Funktionen darstellen lassen.

Es reicht aber nicht aus, auf Probleme ein vorgegebenes Entscheidungsverfahren anwenden zu können. Häufig kommt es darauf an, Lösungsverfahren zu finden. Daher fordert Leibniz eine „Kunst der Problemlösungsfindung“ (ars inveniendi), mit der eine Problemlösung automatisch zu finden ist. Konkret stellen wir uns ein Maschinenprogramm vor, das systematisch alle Zahlen aufzählt, die ein Problem lösen bzw. eine Eigenschaft erfüllen. Allgemein heißt eine arithmetische Eigenschaft dann effektiv aufzählbar, wenn ihre zutreffenden Zahlen durch ein effektiv berechenbares Verfahren (Algorithmus) aufgezählt (gefunden) werden können. Eine arithmetische Eigenschaft können wir auch mit der Menge M der Zahlen identifizieren, die diese Eigenschaft erfüllen.

Definition der effektiven Aufzählbarkeit Eine Zahlenmenge M heißt effektiv aufzählbar, wenn es eine berechenbare Funktion f gibt, mit der ihre Elemente nacheinander erzeugt werden können, d. h. formal $f(1) = x_1$, $f(2) = x_2$, … für alle Elemente x_1, x_2, … aus M.

Als einfaches Beispiel betrachten wir die Menge der geraden Zahlen 2, 4, 6, …. Die berechenbare Funktion, mit der sich diese Menge effektiv aufzählen lässt, lautet $f(n) = 2n$ mit $f(1) = 2, f(2) = 4, f(3) = 6$, … für $n = 1, 2, 3, \ldots$.

Um für eine beliebig vorgelegte Zahl zu entscheiden, ob sie gerade ist, reicht es allerdings nicht aus, alle geraden Zahlen nacheinander effektiv aufzuzählen, um dann festzustellen, ob die gesuchte Zahl dabei ist. Wir müssen ebenso alle nichtgeraden (ungeraden) Zahlen effektiv aufzählen können, um überprüfen zu können, ob die gesuchte Zahl zu der Menge derjenigen Zahlen gehört, die die geforderte Eigenschaft nicht erfüllen. Allgemein sprechen wir dann von der Komplementärmenge $\bar{M}$ von M. Im Fall der ungeraden Zahlen kann die Komplementärmenge durch die berechenbare Funktion $f(n) = 2n - 1$ mit $f(1) = 1, f(2) = 3, f(3) = 5$, … für $n = 1, 2, 3, \ldots$ aufgezählt werden.

Satz von Post (effektive Aufzählbarkeit)
Eine Menge ist effektiv entscheidbar, wenn sie selbst und ihre Komplementärmenge effektiv aufzählbar sind.

Der Beweis ergibt sich aus den Definitionen der effektiven Entscheidbarkeit und Aufzählbarkeit. Daraus folgt, dass jede effektiv entscheidbare Menge auch effektiv aufzählbar ist. Es gibt aber effektiv aufzählbare Mengen, die nicht entscheidbar sind. Leibnizens optimistisches Forschungsprogramm war ursprünglich noch von der Existenz universeller Entscheidungsalgorithmen ausgegangen.

Ein Beispiel für nicht effektiv entscheidbare Probleme betrifft die Turing- bzw. Registermaschine selbst:

Die Unentscheidbarkeit des Stopp-Problems
Es gibt prinzipiell kein allgemeines Entscheidungsverfahren für die Frage, ob eine beliebige Registermaschine (analog eine Turingmaschine) mit einem entsprechenden Maschinenprogramm bei einem beliebigen Input nach endlich vielen Schritten stoppt oder nicht [4].

Turing begann seinen Nachweis der Unentscheidbarkeit des Stopp-Problems mit der Frage, ob alle reellen Zahlen berechenbar seien. Eine reelle Zahl wie $\pi = 3,1415926\ldots$ besteht aus einer unendlichen Anzahl von Ziffern hinter dem Dezimalpunkt, die zufällig verteilt scheinen. Dennoch gibt es ein endliches Verfahren bzw. Programm zur schrittweisen Berechnung jeder Ziffer mit wachsender Genauigkeit von π. Daher ist π eine berechenbare reelle Zahl. In einem ersten Schritt definiert Turing eine nachweislich nicht-berechenbare reelle Zahl.

Ein Turing-Programm besteht aus einer endlichen Liste von Symbolen und Operationsanweisungen, die wir durch Zahlenkodes verschlüsseln können. Tatsächlich geschieht das auch im Maschinenprogramm eines Computers. Auf diesem Weg

lässt sich jedes Maschinenprogramm eindeutig durch einen Zahlenkode (Maschinenkode) charakterisieren. Diese Zahl nennen wir Kode- bzw. Programmnummer eines Maschinenprogramms. Wir stellen uns nun eine Liste von allen möglichen Programmnummern vor, die in der Reihenfolge p_1, p_2, p_3, … mit zunehmender Größe geordnet sei. Falls ein Programm eine reelle Zahl mit unendlicher Anzahl von Werten hinter dem Dezimalkomma (wie z. B. π) berechnet (wobei die Ziffern vor dem Komma vernachlässigt sind), dann wird sie in der Liste hinter der entsprechenden Programmnummer notiert. Andernfalls bleibt die Zeile hinter einer Programmnummer leer [5]:

$$p_1 \; -, \underline{z_{11}} z_{12} z_{13} z_{14} z_{15} z_{16} z_{17} \cdots$$

$$p_2 \; -, z_{21} \underline{z_{22}} z_{23} z_{24} z_{25} z_{26} z_{27} \cdots$$

$$p_3 \; -, z_{31} z_{32} \underline{z_{33}} z_{34} z_{35} z_{36} z_{37} \cdots$$

$$p_4$$

$$p_5 \; -, z_{51} z_{52} z_{53} z_{54} \underline{z_{44}} z_{56} z_{57} \cdots$$

Definition einer nicht-berechenbaren reellen Zahl Zur Definition seiner nicht-berechenbaren Zahl wählt Turing die unterstrichenen Werte auf der Diagonale der Liste, ändert sie um (z. B. durch Addition von 1) und setzt diese veränderten Werte (mit $\neq$ für ungleich) mit einem Dezimalkomma am Anfang zu einer neuen reellen Zahl zusammen:

$$-, \neq z_{11} \neq z_{22} \neq z_{33} \neq z_{44} \neq z_{55} \cdots$$

Diese neue Zahl kann nicht in unserer Liste vorkommen, da sie sich in der ersten Ziffer von der ersten Zahl hinter p_1 unterscheidet, in der zweiten Ziffer von der zweiten Zahl hinter p_2, etc. für alle ihre Ziffern hinter dem Dezimalpunkt. Daher ist die so definiert reelle Zahl nicht-berechenbar.

Mit dieser Zahl beweist Turing im nächsten Schritt die Nicht-Entscheidbarkeit des Stopp-Problems. Wäre nämlich das Stopp-Problem entscheidbar, dann könnten wir entscheiden, ob das n-te Computerprogramm (mit $n = 1, 2, \ldots$) eine n-te Ziffer hinter dem Dezimalkomma nach endlich vielen Schritten berechnet, stoppt und ausdruckt. Wir könnten also eine reelle Zahl berechnen, die nach ihrer Definition nicht in der Liste aller berechenbaren reellen Zahlen vorkommen kann.

Hilberts Forschungsprogramm des Formalismus [6]
Mit der Nicht-Entscheidbarkeit des Stopp-Problems wird Leibnizens Optimismus einer universellen Entscheidbarkeit (ars iudicandi) für alle Probleme prinzipiell eingeschränkt. Der große Göttinger Mathematiker David Hilbert hatte Leibnizens Ent-