
Computational Intelligence

Herausgegeben von

Prof. Dr. Wolfgang Bibel, Scheidegg

Prof. Dr. Rudolf Kruse, Otto-von Guericke-Universität Magdeburg

Prof. Dr. Bernhard Nebel, Albert-Ludwigs-Universität Freiburg

Matthias Homeister

Quantum Computing verstehen

Grundlagen – Anwendungen –
Perspektiven

4. Auflage

Matthias Homeister
Brandenburg an der Havel
Deutschland

Computational Intelligence
ISBN 978-3-658-10454-2 ISBN 978-3-658-10455-9 (eBook)
DOI 10.1007/978-3-658-10455-9

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

Springer Vieweg

© Springer Fachmedien Wiesbaden 2005, 2008, 2013, 2015

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften. Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen.

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Fachmedien Wiesbaden ist Teil der Fachverlagsgruppe Springer Science+Business Media
(www.springer.com)

Inhaltsverzeichnis

Vorwort	IX
1 Einleitung	1
1.1 Eine neue Art des Rechnens	1
1.2 Über dieses Buch	8
2 Vom Bit zum Quantenregister	9
2.1 Was ist eine Berechnung?	10
2.1.1 Die Turingmaschine	13
2.1.2 Schaltkreise	14
2.1.3 Der Sprung in die Quantenwelt: Schrödingers Katze	17
2.2 Das Quantenbit	20
2.3 Rechenschritte auf einem Quantenbit	23
2.4 Der erste Algorithmus: Ein Zufallsgenerator	26
2.5 Quantenregister	28
2.6 Der zweite Algorithmus: Das Problem von Deutsch	33
2.7 Die Rolle des Tensorprodukts	37
2.8 Das Messen von Quantenregistern	44
2.9 Noch einmal das Problem von Deutsch	50
2.10 Bestandsaufnahme: Die drei Prinzipien des Quantum Computing	51
2.11 Verschränkung	53
2.12 Die Hadamard-Transformation und mehrere Bits	59
2.13 Der Algorithmus von Deutsch-Jozsa	62
3 Vom Quantenregister zum Quantenschaltkreis	67
3.1 Laufzeit	68
3.2 Klassische Schaltkreise und Komplexität	75
3.3 Quantengatter und Quantenschaltkreise	76
3.4 Quantenbits kopieren: Das No-Cloning-Theorem	81
3.5 Umkehrbare Berechnungen	84
3.6 Unterscheidbare Zustände	93
3.7 Gestörte Berechnungen	95
4 Hilfsmittel aus der Theoretischen Informatik	101
4.1 Komplexitätsklassen	101
4.2 Randomisierte Algorithmen	106
4.2.1 Mit dem Zufall rechnen	106

4.2.2	Ein Primzahltest	107
4.2.3	Probabilistische Komplexitätsklassen	110
4.3	Unlösbare Probleme? NP-Vollständigkeit	114
4.4	Quantenkomplexitätstheorie	118
4.5	Die Churchsche These	121
5	Teleportation und dichte Kodierung	125
5.1	Quantenteleportation	127
5.2	Dichte Kodierung	131
5.3	Verschränkte Bits	133
6	Suchen	137
6.1	Die Nadel im Heuhaufen	138
6.2	Die Grover-Iteration	140
6.3	Eine geometrische Veranschaulichung	146
6.4	Varianten der Quantensuche	153
6.4.1	Suche nach einer von mehreren Lösungen	153
6.4.2	Suche bei unbekannt vielen Lösungen	155
6.4.3	Die Suche nach dem Minimum	156
6.4.4	Zählen	159
6.5	Anwendungen von Grovers Algorithmus	159
6.6	Grovers Algorithmus ist von optimaler Größenordnung	161
6.7	Folgen für die Fähigkeiten von Quantencomputern	166
7	Geheime Botschaften	169
7.1	Alice, Bob und Eve	170
7.2	Quantenverschlüsselung: das BB84-Protokoll	175
7.3	Lauschstrategien	183
7.4	Quantenverschlüsselung mit Verschränkung	188
8	Klassische Verschlüsselungen knacken: Primfaktorzerlegung	193
8.1	Faktorisierung und Verschlüsselung: RSA-Kryptographie	194
8.2	Die Suche nach Perioden	199
8.3	Die schnelle Fouriertransformation	207
8.4	Die Quanten-Fouriertransformation	214
8.5	Simons Algorithmus	218
8.6	Shors Algorithmus	223
8.7	Jenseits von Shor	231
9	Quantenhardware	237
9.1	Anforderungen	237
9.2	Dekohärenz	238
9.3	Photonen	241
9.3.1	Mach-Zehnder-Interferometer	241
9.3.2	Zufallszahlen	244
9.3.3	Kryptographie	245
9.4	Kernspinresonanz	249
9.5	Ionenfallen	251

9.6	Einwegberechnungen mit Clusterzuständen	252
9.7	Supraleiter	255
9.8	Adiabatische Quantencomputer	257
10	Zur Geschichte der Quantenmechanik	263
10.1	Max Planck: das Quantum der Wirkung	263
10.2	Albert Einstein: Spukhafte Fernwirkung	265
10.3	Niels Bohr: Kopenhagen	266
10.4	Werner Heisenberg: Ein großes Quantenei	269
10.5	Erwin Schrödinger: Katzen und Wellen	271
10.6	Zur Geschichte des Quantencomputers	272
A	Mathematische Grundlagen	275
A.1	Komplexe Zahlen	275
A.2	Vektorräume	277
A.2.1	Was sind Vektorräume?	277
A.2.2	Basen und Unterräume	279
A.2.3	Winkel und Abstände in einem Vektorraum	280
A.2.4	Projektionen	282
A.3	Matrizen	283
A.4	Kombinatorik und Wahrscheinlichkeit	285
A.5	Ganze Zahlen	287
A.5.1	Teiler und Vielfache	287
A.5.2	Modulares Rechnen	287
A.5.3	Zur Division	289
B	Lösungen ausgewählter Übungsaufgaben	291
	Literatur	299
	Symbole und Abkürzungen	305
	Quantengatter	306
	Namen- und Sachwortverzeichnis	307

Vorwort

Zwei wissenschaftliche Revolutionen prägten die erste Hälfte des 20. Jahrhunderts. Zum einen legten Pioniere wie Konrad Zuse, Alan Turing und John von Neumann die Grundlagen für den Bau der ersten praktikablen Rechenmaschinen. Zum anderen stürzte das klassische Weltbild der Physik, seit den Tagen Newtons erweitert, aber kaum verändert, in sich zusammen. Um den Aufbau der Materie zu verstehen, wurde eine radikal neue Theorie geschaffen. Die Quantenmechanik veränderte unsere Auffassung von der Realität so sehr, dass auch viele ihrer Schöpfer vor den Konsequenzen zurückschreckten.

Diese wissenschaftlichen Revolutionen zogen sehr schnell technische nach sich. Wie sehr der Computer unsere heutige Gesellschaft, unser Welt- und Menschenbild prägt, steht jedem vor Augen. Weniger bewusst ist vielen, dass die Quantenmechanik unseren Alltag ebenso beeinflusst. Erst die quantenmechanische Beschreibung des Atoms machte es möglich, Halbleiter und den Laser zu entwickeln; das Transistorradio, der CD-Spieler und moderne Computerhardware sind Folgen der Quantenmechanik.

In den letzten Jahrzehnten wurden diese beiden Wissenschaften zusammengeführt, es entstand ein neuer interdisziplinärer Zweig namens *Quantum Computing*. Das Ziel ist, Quantencomputer zu bauen, Quantenalgorithmen zu entwickeln und zu untersuchen, welche Konsequenzen die Quantenmechanik für die Informationsübertragung hat. Es gibt verschiedene Auslöser für diese Entwicklung, am wichtigsten sind die beiden folgenden:

1. Die grundlegenden Bauteile unserer Rechner werden immer kleiner. Wenn diese Entwicklung im aktuellen Tempo fortschreitet, wird es in nicht allzu ferner Zeit Bauteile von der Größe eines einzelnen Atoms geben. Für Hardwarekomponenten dieser Größenordnung gelten die Gesetze der klassischen Physik nicht mehr, und man muss sich auf die Quantenmechanik einlassen.
2. Computer, welche die Gesetze der Quantenmechanik für sich ausnutzen, können Aufgaben erledigen, die für herkömmliche Rechner unmöglich sind. Dazu gehören absolut abhörsichere Nachrichtenübertragung, die Teleportation von Information, das Erzeugen echter Zufallszahlen und das Knacken von Verschlüsselungsmethoden, die zurzeit als sicher gelten. Dabei geht es um Probleme, die herkömmliche Rechner grundsätzlich nicht lösen können, egal wie sich ihre Leistungsfähigkeit steigern wird.

Es lässt sich schwer absehen, welche Konsequenzen diese Entwicklung haben wird, da noch ungewiss ist, wie die künftigen Quantencomputer aussehen werden und wie aufwändig ihre Herstellung und ihr Betrieb sein wird. Vieles

deutet darauf hin, dass wir gerade Zeugen einer neuen wissenschaftlichen Revolution sind. Unter Laborbedingungen sind Quantencomputer längst Realität, und die Medien berichten regelmäßig über neue Erfolge bei der Suche nach praktikabler Quantenhardware. Firmen wie Amazon und insbesondere Google engagieren sich, und zuletzt war die Debatte um die kommerziellen Quantenrechner der Firma D-Wave Systems in der Wissenschaftspresse sehr präsent. Die Enthüllung von Edward Snowden, dass auch die NSA die Entwicklung von Quantencomputern mit vielen Millionen Dollar vorantreibt, konnte Kenner der Materie nur wenig überraschen.

Am weitesten ist bisher die Umsetzung von Verschlüsselungsverfahren fortgeschritten. Verschiedene Firmen bieten seit langem Quantenkryptographiesysteme an und China kündigte vor kurzem den Bau eines umfangreichen Quantennetzwerkes an. Der erste praktisch einsetzbare Quantencomputer hingegen wird noch einige Jahre auf sich warten lassen, aber unsere Auffassung vom Rechnen selbst, von dem, was ein Computer leisten kann, hat sich bereits verändert. Jeder Informatikstudent lernt im ersten Semester die Churchsche These kennen. Ihre moderne Fassung lautet: Lässt sich ein Problem von irgendeiner physikalisch realisierbaren Rechenmaschine effizient berechnen, so lässt es sich von einer (randomisierten) Turingmaschine effizient berechnen. Das stimmt so nicht mehr. Quantencomputer sind physikalisch realisierbar, wenn sie auch bisher nur mit wenigen Bits und unter Laborbedingungen rechnen. Und sie können Probleme lösen, an denen herkömmliche Computer nach dem Stand der Wissenschaft scheitern.

Aber auch für das Verständnis der physikalischen Realität werden Informationsprozesse immer wichtiger. Die Forschung rund um den Quantencomputer hat nicht nur das Potential, eine neue Technologie hervorzubringen, sondern auch unser Weltbild zu verändern. Information könnte ein grundlegenderes Prinzip sein als die klassischen physikalischen Begriffe Materie oder Energie.

Wir sind also Zeugen der Entstehung einer neuen Wissenschaft, der eine rasante Entwicklung bevorsteht. Kenntnisse in einigen ihrer Bereiche haben dadurch eine geringe Halbwertszeit. Was ein Quantencomputer ist und was er kann, wird in diesem Buch an Hand von Quantenalgorithmien erläutert, also an konkreten Rechenverfahren. Dieser theoretische Zugang bereitet den Leser auch auf künftige Entwicklungen vor. Man denke daran, dass die Ideen Zuses, Turings und von Neumanns heute nichts von ihrer Gültigkeit verloren haben und aus der Antike stammende Algorithmen noch immer praktisch eingesetzt werden.

Leider trauen sich viele Interessierte nicht zu, sich mit diesem neuen Gebiet näher auseinander zu setzen. Quantenmechanik ist ein voraussetzungsreiches Gebiet, in das man sich nicht mal eben so einarbeitet. Um jedoch zu verstehen, wie Quantencomputer rechnen, genügen zunächst wenige quantenmechanische Prinzipien. Es sind einfache Prinzipien, auch wenn sie naturgemäß unanschaulich sind. Dieses Buch stellt sie so anwendungsorientiert wie möglich dar und ist für Leser ohne besondere Vorkenntnisse geschrieben.

Ein typischer Leser dieses Buches könnte ein Informatikstudent nach den Grundvorlesungen sein, aber genauso jede andere Person mit mathemati-

schen Grundkenntnissen. Der Leser wird so schnell wie möglich die Arbeitsweise von Quantenrechtern verstehen können und die wichtigen Algorithmen kennen lernen. Die fortgeschrittenen Kapitel vermitteln vertieftes Wissen und bereiten auf die Forschungsliteratur vor. Um dieses Buch für Leser ohne Informatikkenntnisse lesbar zu machen, werden wichtige Begriffe, wie Berechnung oder Algorithmus, umfassend eingeführt. Lesern, deren Mathematikkenntnisse aus Schule oder Studium verblasst sind, hilft ein Abschnitt im Anhang, der Themen wie komplexe Zahlen, Vektorräume und Matrizen behandelt.

Zur 4. Auflage: Für die aktuelle Auflage wurde das Buch vollständig durchgesehen, grundlegend aktualisiert und es wurden Verbesserungen der Darstellung vorgenommen. Neu hinzugekommen sind unter anderem Abschnitte zu den Themen *Supraleiter* und *Adiabatische Quantencomputer*. Dort wird auch kurz auf die Debatte um die Quantenrechner der Firma D-Wave Systems eingegangen, die zuletzt in der Wissenschaftspresse sehr präsent war.

Brandenburg an der Havel, Juli 2015

Matthias Homeister

Danksagung

Viele Menschen halfen bei der Entstehung dieses Buches, ich möchte mich an dieser Stelle für alle Hinweise bedanken. Namentlich danke ich Dagmar Bruß, Carsten Damm, Christoph Dürr, Martin Gorbahn, Maike Tech, Philip Walther, Harald Weinfurter, Stephan Waack und insbesondere Hecke Schrobsdorff, dessen unermüdliche Unterstützung als Korrektor und Gesprächspartner für das Gelingen dieses Buches wesentlich war. Cornelia Caspary danke ich für die wunderbaren Illustrationen. Für viele Hinweise und eine sehr engagierte Zusammenarbeit danke ich dem Herausgeber Prof. Dr. Wolfgang Bibel, Dr. Reinald Klockenbusch vom Vieweg Verlag sowie Herrn Bernd Hansemann und Frau Sybille Thelen von Springer-Vieweg.