Computational Intelligence

Reihe herausgegeben von
W. Bibel, Technische Universität Darmstadt, Darmstadt, Deutschland
R. Kruse, Fakultät für Informatik, OVG Universität Magdeburg, Magdeburg, Deutschland
B. Nebel, Albert-Ludwigs-Universität Freiburg, Freiburg, Deutschland

Die Reihe „Computational Intelligence“ wird herausgegeben von Prof. Dr. Wolfgang Bibel, Prof. Dr. Rudolf Kruse und Prof. Dr. Bernhard Nebel.

Aus den Kinderschuhen der „Künstlichen Intelligenz“ entwachsen bietet die Reihe breitgefächertes Wissen von den Grundlagen bis in die Anwendung, herausgegeben von namhaften Vertretern ihres Faches.

Computational Intelligence hat das weitgesteckte Ziel, das Verständnis und die Realisierung intelligenten Verhaltens voranzutreiben. Die Bücher der Reihe behandeln Themen aus den Gebieten wie z.B. Künstliche Intelligenz, Softcomputing, Robotik, Neuro- und Kognitionswissenschaften. Es geht sowohl um die Grundlagen (in Verbindung mit Mathematik, Informatik, Ingenieurs- und Wirtschaftswissenschaften, Biologie und Psychologie) wie auch um Anwendungen (z.B. Hardware, Software, Webtechnologie, Marketing, Vertrieb, Entscheidungsfindung). Hierzu bietet die Reihe Lehrbücher, Handbücher und solche Werke, die maßgebliche Themengebiete kompetent, umfassend und aktuell repräsentieren.

Weitere Bände in der Reihe
http://www.springer.com/series/12572

Matthias Homeister

Quantum Computing verstehen

Grundlagen – Anwendungen – Perspektiven

5., aktualisierte und erweiterte Auflage

Springer Vieweg

Matthias Homeister
Informatik und Medien
Technische Hochschule Brandenburg
Brandenburg, Deutschland

Computational Intelligence
ISBN 978-3-658-22883-5 ISBN 978-3-658-22884-2 (eBook)
https://doi.org/10.1007/978-3-658-22884-2

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

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

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 113
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 174
7.3 Lauschstrategien 182
7.4 Quantenverschlüsselung mit Verschränkung 187

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 206
8.4 Die Quanten-Fouriertransformation 214
8.5 Simons Algorithmus 218
8.6 Shors Algorithmus 223
8.7 Jenseits von Shor 231

9 Fehler korrigieren 237
9.1 Dekohärenz und Fehler auf Quantenbits 237
9.2 Klassische Fehlerkorrektur 242
9.3 Herausforderungen bei der Korrektur von Quantenbits 242
9.4 Qubits gegen Fehler sichern 243
9.4.1 Bitflip-Code mit Syndrom: Korrektur des Codewords 243
9.4.2 Der Bitflip-Code: Korrektur des Datenbits 245
9.4.3 Korrektur von Phaseflips 246
9.5 Shors 9-Qubit-Code 247
9.6 Ausblick 250

10 Quantenhardware **253**
10.1 Anforderungen . . . 253
10.2 Photonen . . . 255
10.2.1 Mach-Zehnder-Interferometer . . . 255
10.2.2 Zufallszahlen . . . 258
10.2.3 Kryptographie . . . 259
10.3 Kernspinresonanz . . . 263
10.4 Ionenfallen . . . 265
10.5 Einwegberechnungen mit Clusterzuständen . . . 266
10.6 Supraleiter . . . 269
10.7 Adiabatische Quantencomputer . . . 271

11 Zur Geschichte der Quantenmechanik **277**
11.1 Max Planck: das Quantum der Wirkung . . . 277
11.2 Albert Einstein: Spukhafte Fernwirkung . . . 279
11.3 Niels Bohr: Kopenhagen . . . 280
11.4 Werner Heisenberg: Ein großes Quantenei . . . 283
11.5 Erwin Schrödinger: Katzen und Wellen . . . 285
11.6 Zur Geschichte des Quantencomputers . . . 286

A Mathematische Grundlagen **289**
A.1 Komplexe Zahlen . . . 289
A.2 Vektorräume . . . 291
A.2.1 Was sind Vektorräume? . . . 291
A.2.2 Basen und Unterräume . . . 293
A.2.3 Winkel und Abstände in einem Vektorraum . . . 294
A.2.4 Projektionen . . . 296
A.3 Matrizen . . . 297
A.4 Kombinatorik und Wahrscheinlichkeit . . . 299
A.5 Ganze Zahlen . . . 301
A.5.1 Teiler und Vielfache . . . 301
A.5.2 Modulares Rechnen . . . 301
A.5.3 Zur Division . . . 303

B Lösungen ausgewählter Übungsaufgaben **305**

Literatur **315**

Symbole und Abkürzungen **321**

Quantengatter **322**

Namen- und Sachwortverzeichnis **323**

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.

Noch lässt sich nicht genau sagen, wann Quantencomputer praxistauglich sein werden. Allerdings sind die Fortschritte gerade der letzten Jahre so

beeindruckend, dass es vielleicht nicht mehr lange dauern wird, bis Quantenrechner unseren herkömmlichen Computern praktisch überlegen sein werden. Auf jeden Fall scheinen wir gerade Zeugen einer neuen wissenschaftlichen und technologischen Revolution zu sein.

Am weitesten ist bisher die Umsetzung von Verschlüsselungsverfahren fortgeschritten. Verschiedene Firmen bieten seit vielen Jahren Quantenkryptographiesysteme an und China plant den Bau eines umfangreichen Quantennetzwerks. Und auch wenn zur Zeit Quantenrechner noch nicht praktisch eingesetzt werden, hat sich schon längst unsere Auffassung vom Rechnen selbst, von dem, was ein Computer prinzipiell leisten kann, 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 und sie können einige Probleme lösen, an denen herkömmliche Computer nach dem Stand der Wissenschaft scheitern müssen.

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 Quantenalgorithmen 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 Thema 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 mathematischen Grundkenntnissen. Der Leser wird so schnell wie möglich die Arbeitsweise von Quantenrechnern 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 5. Auflage: Für die aktuelle Auflage wurde das Buch erneut vollständig durchgesehen, aktualisiert und es wurden Verbesserungen der Darstellung vorgenommen. Neu hinzugekommen ist insbesondere das Thema *Fehlerkorrektur für Quantenbits*. Kein praktisch einsetzbarer Quantenrechner kann ohne solche Techniken auskommen; darum wird in Kapitel 9 die Bedeutung fehlerkorrigierender Codes erläutert und in dieses umfangreiche und anspruchsvolle Gebiet eingeführt.

Brandenburg an der Havel, 2018

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, Rolf Socher, Michael Syrjakow, 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.