Mathematik der Quanteninformatik

Wolfgang Scherer

Mathematik der Quanteninformatik

Eine Einführung

Springer Spektrum

Wolfgang Scherer
Kingston Upon Thames, Großbritannien

ISBN 978-3-662-49079-2 ISBN 978-3-662-49080-8 (eBook)
DOI 10.1007/978-3-662-49080-8

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

Springer Spektrum

Planung: Margit Maly

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.

Springer-Verlag GmbH Berlin Heidelberg ist Teil der Fachverlagsgruppe Springer Science+Business Media
(www.springer.com)

In memoriam
Elisabeth et Heinz-Werner Scherer,
qui dixit: Scio me nihil scire.

Y para Negri, Matthias y Sebastian

Vorwort

Die Vorgeschichte dieses Buches begann mit einer Einführungsvorlesung zur Quanteninformatik im Jahre 1998 an der TU Clausthal. Seitdem hat die Digitalisierung unseres täglichen Lebens weiter rapide Fahrt aufgenommen und ist auf dem besten Weg allumfassend zu werden. Enorme Datenmengen und deren Verarbeitung erfordern immer neuere Technologien mit immer größeren Speicherkapazitäten und immer effizienteren Algorithmen. Dabei schreitet die Miniaturisierung der Speicherträger stetig voran. Folglich begann man sich bereits in den 80er-Jahren des vergangenen Jahrhunderts zu fragen, wie Information mit atomaren Bausteinen gespeichert und verarbeitet werden kann. Solcherart Bausteine folgen den Gesetzen der Quantenmechanik, und die Quanteninformatik entstand als ein Forschungszweig, in dem Grundlagenfragen ganz nahe bei potenziell revolutionären Anwendungen stehen.

In den darauf folgenden Dekaden wurde die diesbezügliche Theorie entwickelt. Es zeigte sich, dass die Speicherung und Bearbeitung von Information nach den Regeln der Quantenmechanik in der Tat neuartige und effizientere Methoden als die bisherigen verspricht. Mithilfe des massiven Quantenparallelismus könnten Faktorisierungs- und Suchalgorithmen mit einem Quantencomputer erheblich beschleunigt werden. Außerdem erlauben quantenmechanische Phänomene neuartige Kryptografieprotokolle, deren Abhörsicherheit durch die Naturgesetze der Quantenmechanik garantiert wird.

Die Theorie der Quanteninformatik hat mittlerweile einen fortgeschrittenen Reifegrad erreicht. Dabei wird von einer Vielzahl mathematischer Resultate hauptsächlich aus Linearer Algebra und Zahlentheorie Gebrauch gemacht. Dennoch gibt es kaum umfassende Darstellungen, die die Quanteninformatik durch eine streng mathematisch geprägte Brille betrachten. Dieses Buch möchte da etwas Abhilfe schaffen. Ausgehend von den physikalischen Grundlagen wird hier alle für die Quanteninformatik erforderliche Mathematik eingeführt und erklärt. Die wesentlichen Aspekte der Quanteninformatik werden mathematisch formuliert. Alle gemachten Aussagen werden auch im Buch bewiesen. Insofern kann der mathematisch geneigte Leser hier einen umfassenden Einblick in die Mathematik der Quanteninformatik bekommen, ohne das Buch aus der Hand zu legen.

Derzeit wird mit Nachdruck an verschiedenen möglichen physikalischen Realisierungen eines Quantencomputers gearbeitet. Nach der Lektüre dieses Buches sollten die Leserinnen und Leser auf eine erfolgreiche physikalische Implementierung eines Quantencomputers bestens vorbereitet sein. Aber vielleicht können sie ja als Folge der Lektüre selbst auch noch zur Theorie beitragen.

Danksagungen Auf dem Weg hierher haben mich viele Menschen und etliche Institutionen in meiner wissenschaftlichen Leidenschaft und Neugier begleitet, ermuntert und gefördert. Ihnen allen gilt mein aufrichtiger Dank.

Ganz herzlich danke ich auch dem Team vom Springer-Verlag, das mich im letzten Jahr des Projekts geduldig und hilfreich unterstützt hat.

Am allermeisten danke ich meiner Familie, Maria-Eugenia, Matthias und Sebastian, die über all die Jahre meine oft gedankliche und physische Abwesenheit hingenommen haben, aber dennoch immerzu den nötigen Rückhalt geboten und den Enthusiasmus mit mir geteilt haben. Ein besonderer Dank gebührt dabei Sebastian für sein akribisches Korrekturlesen des Manuskripts. Seine Durchsicht hat viele Fehler behoben, und seine Vorschläge haben an etlichen Stellen die Darstellung genauer, stringenter und klarer gemacht. Die Diskussionen mit ihm waren nicht nur sehr hilfreich, sondern haben auch viel Spaß gemacht. Aber selbst sein detailliertes Redigieren wird sicher nicht alle Unzulänglichkeiten des Manuskripts ausgebügelt haben. Diese sind natürlich immer noch vom Autor verursacht.

Kingston Upon Thames, im November 2015 Wolfgang Scherer

Symbolverzeichnis

$:=$	definierende Gleichheit, d. h. in $a := b$ wird a durch b definiert
$\mathbb{N}$	die Menge der natürlichen Zahlen $1, 2, 3, \ldots$
$\mathbb{P}$	die Menge der Primzahlen $\{2, 3, 5, 7, 11, \ldots\} \subset \mathbb{N}$
$\mathbb{N}_0$	die Menge der natürlichen Zahlen inklusive der Null $0, 1, 2, 3, \ldots$
$\mathbb{Z}$	die Menge der ganzen Zahlen $0, \pm 1, \pm 2, \pm 3, \ldots$
$\mathbb{Q}$	die Menge der rationalen Zahlen $\frac{q}{p}$ mit $q \in \mathbb{Z}, p \in \mathbb{N}$; $\mathbb{Q}_+$ bezeichnet die positiven rationalen Zahlen
$\mathbb{R}$	die Menge der reellen Zahlen; $\mathbb{R}_+$ bezeichnet die positiven reellen Zahlen
$\mathbb{C}$	die Menge der komplexen Zahlen $a + \mathrm{i}b$ mit $a, b \in \mathbb{R}$ und $\mathrm{i}^2 = -1$
$\lvert z \rvert$	Betrag der komplexen Zahl $z = a + \mathrm{i}b$ mit $a, b \in \mathbb{R}$, d. h. $\lvert z \rvert = \sqrt{z\overline{z}} = \sqrt{a^2 + b^2}$
$\overline{z}$	die komplexkonjugierte der komplexen Zahl $z = a + \mathrm{i}b$ mit $a, b \in \mathbb{R}$, d. h. $\overline{z} = a - \mathrm{i}b$
$\mathbf{a}$	Vektor in $\mathbb{R}^n$, meist für den Fall $n = 3$
$\mathbf{a} \cdot \mathbf{b}$	Skalarprodukt der Vektoren $\mathbf{a}, \mathbf{b} \in \mathbb{R}^n$
$\lvert \mathbf{a} \rvert$	Norm des Vektors $\mathbf{a} \in \mathbb{R}^n$, d. h. $\lvert \mathbf{a} \rvert = \sqrt{\mathbf{a} \cdot \mathbf{a}}$
$\mathbb{H}$	Hilbert-Raum, d. h. ein komplexer Vektorraum mit einem Skalarprodukt, das die Norm induziert
$^1\mathbb{H}$	Qbit-Hilbert-Raum, d. h. der Hilbert-Raum $^1\mathbb{H} \simeq \mathbb{C}^2$
$\lvert \psi \rangle$	„Ket“-Schreibweise für einen Vektor in einem Hilbert-Raum
$\langle \psi \rvert$	„Bra“-Schreibweise für einen Vektor im Dualraum zu einem Hilbert-Raum
$\langle \varphi \lvert \psi \rangle$	Skalarprodukt der Vektoren $\lvert \varphi \rangle, \lvert \psi \rangle \in \mathbb{H}$
$\lvert\lvert \psi \rvert\rvert$	Norm des Vektors $\lvert \psi \rangle \in \mathbb{H}$, d. h. $\lvert\lvert \psi \rvert\rvert = \sqrt{\langle \psi \lvert \psi \rangle}$
δ_{xy}	Kronecker-Delta

$$\delta_{xy} = \begin{cases} 1, & \text{falls } x = y \\ 0, & \text{sonst} \end{cases}$$

$\mathbf{1}$ der Identitätsoperator oder Einheitsmatrix, d. h. $\mathbf{1}\psi = \psi$ für alle $\psi \in \mathbb{H}$. Für speziell ausgezeichnete $\mathbb{H}^A$ schreiben wir zur Verdeutlichung für den Identitätsoperator auch $\mathbf{1}^A$, und für $\mathbb{H} = {}^{¶}\mathbb{H}^{\otimes n}$ schreiben wir für den Identitätsoperator auch $\mathbf{1}^{\otimes n}$

A^* der zu A adjungierte Operator, d. h. $\langle\varphi|A\psi\rangle = \langle A^*\varphi|\psi\rangle$ für alle $\varphi, \psi \in \mathbb{H}$

$[A, B]$ der Kommutator der Operatoren A, B, d. h. $[A, B] := AB - BA$

$|\varphi\rangle \otimes |\psi\rangle$ Tensorprodukt zweier Vektoren

${}^{¶}\mathbb{H}^{\otimes n}$ n-faches Tensorprodukt des Qbit-Hilbert-Raums ${}^{¶}\mathbb{H}$

$B^r_{\mathbb{V}}$ die Menge der Vektoren $\mathbf{v} \in \mathbb{V}$ mit $||\mathbf{v}|| = r$, d. h. die „Kugel mit Radius r“ im normierten Vektorraum $\mathbb{V}$. Zum Beispiel bezeichnet $B^1_{\mathbb{R}^3}$ die Einheitsvektoren im $\mathbb{R}^3$

$|x\rangle$ Element der Rechenbasis in ${}^{¶}\mathbb{H}^{\otimes n}$; für jedes $x \in \mathbb{N}_0$ mit $x = \sum_{j=0}^{n-1} x_j 2^j < 2^n$ und $x_j \in \{0, 1\}$ gegeben durch

$$|x\rangle := |x\rangle^n := \overset{0}{\bigotimes_{j=n-1}} |x_j\rangle = |x_{n-1}\rangle \otimes \cdots \otimes |x_0\rangle = |x_{n-1} \ldots x_0\rangle$$

$\neg A$ Verneinung der Aussage A

$\lfloor u \rfloor$ der ganze Anteil einer Zahl $u \in \mathbb{R}$, d. h.

$$\lfloor u \rfloor := \max\{z \in \mathbb{Z} | z \leq u\}$$

$a \bmod n$ der Rest von $a \in \mathbb{Z}$ nach der Division durch $n \in \mathbb{N}$, d. h.

$$a \bmod n := a - \left\lfloor \frac{a}{n} \right\rfloor n$$

$\overset{2}{\oplus}$ binäre Addition $a \overset{2}{\oplus} b := a + b \mod 2$

$\oplus$ faktorweise Binäraddition; für Vektoren der Rechenbasis $|x\rangle, |y\rangle \in {}^{¶}\mathbb{H}^{\otimes n}$ definiert durch

$$|x \oplus y\rangle := \overset{0}{\bigotimes_{j=n-1}} \left| x_j \overset{2}{\oplus} y_j \right\rangle$$

$ggT(a_1, \ldots, a_n)$ der größte gemeinsame Teiler für $a_i \in \mathbb{Z}, i = 1, \ldots, n$ mit $\sum_{i=1}^n |a_i| \neq 0$, d. h.

$$ggT(a_1, \ldots, a_n) := \max\{k \in \mathbb{N} | \forall a_i \exists b_i \in \mathbb{Z} : a_i = k b_i\}$$

$kgV(a_1, \ldots, a_n)$ das kleinste gemeinsame Vielfache für $a_i \in \mathbb{Z}, i = 1, \ldots, n$ mit $\prod_{i=1}^n |a_i| \neq 0$, d. h.

$$kgV(a_1, \ldots, a_n) := \min\{k \in \mathbb{N} | \, \forall a_i : a_i \,|\, k\}$$

$\mathbb{P}(n)$ die Menge der Primzahlen in der Primfaktorzerlegung von n

$n = \prod_{p\in\mathbb{P}} p^{\nu_p}$ die Primfaktorzerlegung von $n \in \mathbb{N}$, wobei die Exponenten von Primzahlen $p \in \mathbb{P}$, die kein Primfaktor sind, gleich null gesetzt werden, d. h. etwa $\nu_p = 0$, falls $p \notin \mathbb{P}(n)$. Für $a \in \mathbb{Z}\backslash\{0\}$ definieren wir die Primfaktorzerlegung für $|a| \in \mathbb{N}$ und setzen $a = sign(a) \prod_{p\in\mathbb{P}(|a|)} p^{|a|_p}$

$\phi(n)$ Euler-Funktion

$$\begin{aligned} \phi : \mathbb{N} &\longrightarrow \mathbb{N} \\ n &\longmapsto \phi(n) := \text{Anzahl aller } r \in \mathbb{N},\ 1 \le r < n, \\ &\qquad\qquad \text{die mit } n \text{ teilerfremd sind, d. h.} \\ &\qquad\qquad ggT(n, r) = 1 \text{ erfüllen} \end{aligned}$$

$ord_N(b)$ die *Ordnung von b modulo N* definiert für $b, N \in \mathbb{N}$ mit der Eigenschaft $ggT(b, N) = 1$ als

$$ord_N(b) := \min\{n \in \mathbb{N} | b^n \mod N = 1\}$$

$a \mid b$ a teilt b, d. h. es gibt ein $z \in \mathbb{Z}$ für das gilt $b = az$

$a \nmid b$ a teilt b nicht, d. h. für alle $z \in \mathbb{Z}$ gilt $b \neq za$

id_A die Identitätsabbildung auf der Menge A, d. h. $id_A : A \to A$ mit $id_A(a) = a$

$o(\cdot)$ das kleine Landau-Symbol, definiert hier für Funktionen auf $\mathbb{N}$ im Limit $n \to \infty$ als

$$\begin{aligned} & f(n) \in o(g(n)) \text{ für } (n \to \infty) \\ :\Leftrightarrow\quad & \forall \varepsilon \in \mathbb{R}_+, \exists M \in \mathbb{N} : \forall n > M : |f(n)| \le \varepsilon\, |g(n)| \end{aligned}$$

$O(\cdot)$ das große Landau-Symbol, definiert hier für Funktionen auf $\mathbb{N}$ im Limit $n \to \infty$ als

$$\begin{aligned} & f(n) \in O(g(n)) \text{ für } (n \to \infty) \\ :\Leftrightarrow\quad & \exists C \in \mathbb{R}, M \in \mathbb{N}\ \forall n > M : |f(n)| \le C\, |g(n)| \end{aligned}$$

Abkürzungsverzeichnis

ONB steht als Abkürzung für Orthonormalbasis, die maximale Menge linear unabhängiger Einheitsvektoren in einem Vektorraum mit Skalarprodukt, die paarweise orthogonal sind.

EPR Einstein-Podolsky-Rosen, drei Autoren eines Artikels [1] aus dem Jahre 1935, in dem kontraintuitive Effekte der Quantenmechanik als Argument für die Unvollständigkeit derselben angführt werden.

CHSH Clauser-Horne-Shimony-Holt, vier Autoren einer in [2] gezeigten Verallgemeinerung der Bell'schen Ungleichung.

RSA steht als Abkürzung für ein von Rivest, Shamir und Adleman in 1978 entwickeltes Chiffrierverfahren, das mit *öffentlichem Schlüsselaustausch* funktioniert.

BB84 ist die Abkürzung für eine quantenmechanische Methode der kryptografischen Schlüsselverteilung, die 1984 von Bennett und Brassard in [3] vorgeschlagen wurde.

EK91 ist die Abkürzung für ein von Artur Ekert in 1991 in [4] vorgeschlagenes Protokoll zur kryptografischen Schlüsselverteilung, welches die CHSH-Version der Bell'schen Ungleichung ausnutzt, um Lauschangriffe festzustellen.

oBdA steht für ohne Beschränkung der Allgemeinheit.

Inhaltsverzeichnis

Abbildungsverzeichnis