
Mathematik der Quanteninformatik

Wolfgang Scherer

Mathematik der Quanteninformatik

Eine Einführung

 Springer Spektrum

Wolfgang Scherer
Kingston Upon Thames, Großbritannien

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

ISBN 978-3-662-49080-8 (eBook)

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

© Springer-Verlag Berlin Heidelberg 2016

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.

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 $1, 2, 3, \dots$
\mathbb{P}	die Menge der Primzahlen $\{2, 3, 5, 7, 11, \dots\} \subset \mathbb{N}$
\mathbb{N}_0	die Menge der natürlichen Zahlen inklusive der Null $0, 1, 2, 3, \dots$
\mathbb{Z}	die Menge der ganzen Zahlen $0, \pm 1, \pm 2, \pm 3, \dots$
\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 $a + ib$ mit $a, b \in \mathbb{R}$ und $i^2 = -1$
$ z $	Betrag der komplexen Zahl $z = a + ib$ mit $a, b \in \mathbb{R}$, d. h. $ z = \sqrt{z\bar{z}} = \sqrt{a^2 + b^2}$
\bar{z}	die komplexkonjugierte der komplexen Zahl $z = a + ib$ mit $a, b \in \mathbb{R}$, d. h. $\bar{z} = a - ib$
\mathbf{a}	Vektor in \mathbb{R}^n , meist für den Fall $n = 3$
$\mathbf{a} \cdot \mathbf{b}$	Skalarprodukt der Vektoren $\mathbf{a}, \mathbf{b} \in \mathbb{R}^n$
$ \mathbf{a} $	Norm des Vektors $\mathbf{a} \in \mathbb{R}^n$, d. h. $ \mathbf{a} = \sqrt{\mathbf{a} \cdot \mathbf{a}}$
\mathbb{H}	Hilbert-Raum, d. h. ein komplexer Vektorraum mit einem Skalarprodukt, das die Norm induziert
${}^{\mathbb{H}}\mathbb{H}$	Qbit-Hilbert-Raum, d. h. der Hilbert-Raum ${}^{\mathbb{H}}\mathbb{H} \simeq \mathbb{C}^2$
$ \psi\rangle$	„Ket“-Schreibweise für einen Vektor in einem Hilbert-Raum
$\langle\psi $	„Bra“-Schreibweise für einen Vektor im Dualraum zu einem Hilbert-Raum
$\langle\varphi \psi\rangle$	Skalarprodukt der Vektoren $ \varphi\rangle, \psi\rangle \in \mathbb{H}$
$\ \psi\ $	Norm des Vektors $ \psi\rangle \in \mathbb{H}$, d. h. $\ \psi\ = \sqrt{\langle\psi \psi\rangle}$
δ_{xy}	Kronecker-Delta

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

- 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 $\mathbb{H} = {}^{\mathbb{H}}\mathbb{H}^{\otimes n}$ 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
- ${}^{\mathbb{H}}\mathbb{H}^{\otimes n}$ n -faches Tensorprodukt des Qbit-Hilbert-Raums ${}^{\mathbb{H}}\mathbb{H}$
- $B_{\mathbb{V}}^r$ 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 $B_{\mathbb{R}^3}^1$ die Einheitsvektoren im \mathbb{R}^3
- $|x\rangle$ Element der Rechenbasis in ${}^{\mathbb{H}}\mathbb{H}^{\otimes n}$; 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

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

- $\neg A$ 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 $a \overset{2}{\oplus} b := a + b \bmod 2$
- \oplus faktorweise Binäraddition; für Vektoren der Rechenbasis $|x\rangle, |y\rangle \in {}^{\mathbb{H}}\mathbb{H}^{\otimes n}$ definiert durch

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

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

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

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

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

$\mathbb{P}(n)$ 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 $a \in \mathbb{Z} \setminus \{0\}$ definieren wir die Primfaktorzerlegung für $|a| \in \mathbb{N}$ und setzen $a = \text{sign}(a) \prod_{p \in \mathbb{P}(|a|)} p^{\nu_p}$
 $\phi(n)$ Euler-Funktion

$$\phi : \mathbb{N} \longrightarrow \mathbb{N}$$

$$n \longmapsto \phi(n) := \text{Anzahl aller } r \in \mathbb{N}, 1 \leq r < n, \text{ die mit } n \text{ teilerfremd sind, d. h. } \text{ggT}(n, r) = 1 \text{ erfüllen}$$

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

$$\text{ord}_N(b) := \min\{n \in \mathbb{N} \mid b^n \pmod{N} = 1\}$$

$a \mid b$ 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. $\text{id}_A : A \rightarrow A$ mit $\text{id}_A(a) = a$
 $o(\cdot)$ das kleine Landau-Symbol, definiert hier für Funktionen auf \mathbb{N} im Limit $n \rightarrow \infty$ als

$$f(n) \in o(g(n)) \text{ für } (n \rightarrow \infty)$$

$$:\Leftrightarrow \forall \varepsilon \in \mathbb{R}_+, \exists M \in \mathbb{N} : \forall n > M : |f(n)| \leq \varepsilon |g(n)|$$

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

$$f(n) \in O(g(n)) \text{ für } (n \rightarrow \infty)$$

$$:\Leftrightarrow \exists C \in \mathbb{R}, M \in \mathbb{N} \forall n > M : |f(n)| \leq C |g(n)|$$

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 angeführt 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

1	Einführung	1
1.1	Historisches	1
1.2	Motivation und Inhalt	4
1.3	Was in diesem Buch nicht behandelt wird	7
1.4	Anmerkungen zur Notation und Literatur	8
2	Grundbegriffe der Quantenmechanik	9
2.1	Allgemeines	9
2.2	Mathematisches: Hilbert-Raum und Operatoren	11
2.3	Physikalisches: Zustände und Observable	20
2.3.1	Reine Zustände	20
2.3.2	Gemischte Zustände	31
2.4	Qbits	40
2.5	Operatoren auf Qbits	46
3	Zusammengesetzte Systeme und Tensorprodukte	57
3.1	Auf dem Weg zum Qbyte	57
3.2	Tensorprodukte von Hilbert-Räumen	58
3.2.1	Definition	58
3.2.2	Die Rechenbasis	63
3.3	Zustände und Observable für zusammengesetzte Systeme	67
3.4	Schmidt-Zerlegung	76
4	Verschränkung	79
4.1	Allgemeines	79
4.2	Definition und Charakterisierung	81
4.3	Erzeugung verschränkter Zustände ohne Wechselwirkung	84
4.4	Das Einstein-Podolsky-Rosen-Paradoxon	86
4.5	Bell'sche Ungleichungen	91
4.5.1	Die ursprüngliche Bell'sche Ungleichung	91
4.5.2	Die CHSH-Verallgemeinerung der Bell'schen Ungleichung	97

4.6	Zwei unmögliche Apparate	104
4.6.1	Bell'sches Telefon	104
4.6.2	Der perfekte Quantenkopierer	107
5	Quantengatter und Schaltkreise für elementare Rechenoperationen	111
5.1	Klassische Gatter	111
5.2	Quantengatter	116
5.2.1	Unäre Quantengatter	117
5.2.2	Binäre Quantengatter	122
5.2.3	Allgemeine Quantengatter	123
5.3	Zum Ablauf von Quantenalgorithmen	147
5.3.1	Vorbereitung des Input- und Nutzung des Arbeitsregisters	148
5.3.2	Implementierung von Funktionen und Quantenparallelismus	151
5.3.3	Auslesen des Outputregisters	155
5.4	Schaltkreise für elementare Rechenoperationen	156
5.4.1	Quantenaddierer	156
5.4.2	Quantenaddierer modulo N	168
5.4.3	Quantenmultiplikator modulo N	172
5.4.4	Quantenschaltkreis für Exponentiation modulo N	176
5.4.5	Quanten-Fourier-Transformation	180
6	Vom Nutzen der Verschränkung	189
6.1	Dichte Quantenkodierung	189
6.2	Teleportation	191
6.3	Quantenkryptografie	193
6.3.1	Allgemeines zur Kryptografie	193
6.3.2	Schlüsselverteilung ohne Verschränkung	195
6.3.3	Schlüsselverteilung mit verschränkten Zuständen	198
6.3.4	Öffentliche Schlüsselverteilung nach RSA	201
6.4	Shors Algorithmus zur Faktorisierung großer Zahlen	206
6.4.1	Allgemeines	206
6.4.2	Der Algorithmus	207
6.4.3	Schritt 1: Auswahl von b und Berechnung von $ggT(b, N)$	210
6.4.4	Schritt 2: Periodenbestimmung mit Quantencomputern	211
6.4.5	Schritt 3: Wahrscheinlichkeit der Auswahl eines geeigneten b	224
6.4.6	Bilanzierung der Schritte	230
6.5	Grovers Suchalgorithmus	235
6.5.1	Suchalgorithmus bei bekannter Anzahl von gesuchten Objekten	235
6.5.2	Suchalgorithmus bei unbekannter Anzahl von gesuchten Objekten	246
7	Nachwort	253

8	Anhang A – Elementare Wahrscheinlichkeitstheorie	255
9	Anhang B – Elementare Rechenoperationen	259
10	Anhang C – Landau-Symbole	267
11	Anhang D – Modulare Arithmetik	269
12	Anhang E – Kettenbrüche	297
13	Anhang F – Lösungen	309
	13.1 Lösungen zu Übungen aus Kap. 2	309
	13.2 Lösungen zu Übungen aus Kap. 3	322
	13.3 Lösungen zu Übungen aus Kap. 4	324
	13.4 Lösungen zu Übungen aus Kap. 5	329
	13.5 Lösungen zu Übungen aus Kap. 6	335
	13.6 Lösungen zu Übungen aus Kap. 9	341
	13.7 Lösungen zu Übungen aus Kap. 10	341
	13.8 Lösungen zu Übungen aus Kap. 11	342
	Literatur	345
	Sachverzeichnis	349

Abbildungsverzeichnis

Abb. 4.1	CHSH-Spinnmessrichtungen	99
Abb. 4.2	EPR-Experiment	100
Abb. 5.1	Generische klassische Gatter	112
Abb. 5.2	Klassische Gatter	114
Abb. 5.3	Generisches Quantengatter	117
Abb. 5.4	Unäre Quantengatter	118
Abb. 5.5	Binäre Quantengatter 1	120
Abb. 5.6	Binäre Quantengatter 2	121
Abb. 5.7	Kontrolliertes V -Gatter	126
Abb. 5.8	Kontrolliertes n_a, n_b -Gatter	129
Abb. 5.9	Binäradditionsoperator	152
Abb. 5.10	Implementierung f	154
Abb. 5.11	Binärsumme	157
Abb. 5.12	Additionsübertrag	158
Abb. 5.13	Quantenaddierer	161
Abb. 5.14	Teil 1 des Quantenaddierers	163
Abb. 5.15	Teil 2 des Quantenaddierers	163
Abb. 5.16	Teil 3 des Quantenaddierers	164
Abb. 5.17	Teil 1 des Quantensubtrahierers	166
Abb. 5.18	Teil 2 des Quantensubtrahierers	167
Abb. 5.19	Teil 3 des Quantensubtrahierers	167
Abb. 5.20	Quantenaddierer modulo N	170
Abb. 5.21	Quantenmultiplikator modulo N	173
Abb. 5.22	Exponentiation modulo N	177
Abb. 5.23	Quanten-Fourier-Transformation	188

Abb. 6.1	Dichte Quantenkodierung	191
Abb. 6.2	Teleportation	193
Abb. 6.3	Auswahl l	220
Abb. 6.4	Shor-Beobachtungswahrscheinlichkeit	234
Abb. 6.5	Grover-Iteration	242
Abb. 13.1	Orthogonaler Vektor	310
Abb. 13.2	Spiegelung an Vektor	340