

Jürgen Audretsch

 WILEY-VCH

Verschränkte Systeme

Die Quantenphysik auf neuen Wegen



Jürgen Audretsch

Verschränkte Systeme

Die Quantenphysik auf neuen Wegen



WILEY-
VCH

WILEY-VCH Verlag GmbH & Co. KGaA

This Page Intentionally Left Blank

Jürgen Audretsch

Verschränkte Systeme

Die Quantenphysik auf neuen Wegen

Jürgen Audretsch

Verschränkte Systeme

Die Quantenphysik auf neuen Wegen



WILEY-
VCH

WILEY-VCH Verlag GmbH & Co. KGaA

Autor

Jürgen Audretsch

Universität Konstanz, Fachbereich Physik
e-mail: juergen.audretsch@uni-konstanz.de

Das vorliegende Werk wurde sorgfältig erarbeitet.
Dennoch übernehmen Autor und Verlag für die
Richtigkeit von Angaben, Hinweisen und Ratschlägen
sowie für eventuelle Druckfehler keine Haftung.

Umschlagbild

Itten, Johannes: Die Begegnung, 1916
© VG Bild-Kunst, Bonn 2004

Bibliografische Information

Der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

© 2005 WILEY-VCH Verlag GmbH & Co. KGaA,
Weinheim

Alle Rechte, insbesondere die der Übersetzung in andere Sprachen vorbehalten. Kein Teil dieses Buches darf ohne schriftliche Genehmigung des Verlages in irgendeiner Form – durch Photokopie, Mikroverfilmung oder irgendein anderes Verfahren – reproduziert oder in eine von Maschinen, insbesondere von Datenverarbeitungsmaschinen, verwendbare Sprache übertragen oder übersetzt werden.

Printed in the Federal Republic of Germany
Gedruckt auf säurefreiem Papier

Satz Uwe Krieg, Berlin
Druck Strauss GmbH, Mörlenbach
Bindung Litges & Dopf Buchbinderei GmbH,
Heppenheim

ISBN-13: 978-325-40452-0

ISBN-10: 3-527-40452-X

This Page Intentionally Left Blank

Inhaltsverzeichnis

Vorwort	XI
1 Der mathematische Rahmen	1
1.1 Hilbert-Raum der Vektoren	2
1.1.1 Skalarprodukt, Dirac-Schreibweise	2
1.1.2 Lineare Operatoren auf dem Hilbert-Raum	3
1.1.3 Normale Operatoren und spektrale Zerlegung	6
1.1.4 Hermitesche Operatoren	9
1.1.5 Unitäre Operatoren	11
1.1.6 Positive Operatoren und Projektionsoperatoren	11
1.2 Liouville-Raum der Operatoren	13
1.2.1 Skalarprodukt	13
1.2.2 Superoperatoren	15
1.3 Elemente der Wahrscheinlichkeitstheorie	15
1.3.1 Wahrscheinlichkeit zufälliger Ereignisse	16
1.3.2 Bedingte Wahrscheinlichkeit und Satz von Bayes	17
1.3.3 Zufallsgrößen	19
1.4 Ergänzende Themen und weiterführende Literatur	20
1.5 Übungsaufgaben	20
2 Grundkonzepte der Quantentheorie	23
2.1 Erste Fassung der Postulate (reine Zustände abgeschlossener Quantensysteme)	23
2.1.1 Das Szenario der Quantentheorie	23
2.1.2 Postulate für reine Zustände abgeschlossener Quantensysteme	29
2.1.3 Kommentare zu den Postulaten	35
2.2 Ausblick	36
2.3 Manipulation der Zustandsbewegung durch projektive Messungen	37
2.3.1 Quanten-Zeno-Effekt	37
2.3.2 Treiben eines Zustandsvektors durch eine Sequenz von Projektions- messungen	38
2.4 Die Struktur physikalischer Theorien*	39
2.4.1 Bauelemente einer physikalischen Theorie*	39
2.4.2 Theoretische Terme*	41

Die mit einem Stern * gekennzeichneten Kapitel können bei einem ersten Durchgang überschlagen werden.

2.5	Interpretationen der Quantentheorie und physikalische Wirklichkeit*	42
2.5.1	Minimalinterpretation*	42
2.5.2	Standardinterpretation*	42
2.6	Ergänzende Themen und weiterführende Literatur	43
3	Die einfachsten Quantensysteme: Qubits	45
3.1	Pauli-Operatoren	46
3.2	Veranschaulichung von Qubits auf der Bloch-Kugel	48
3.3	Veranschaulichung der Messdynamik und der unitären Dynamik	51
3.4	Quantengatter für einzelne Qubit-Systeme	55
3.5	Spin- $\frac{1}{2}$	57
3.6	Photonenpolarisationen	58
3.7	Einzelne Photonen im Strahlteiler und Interferometer	59
3.7.1	Strahlteiler	59
3.7.2	Interferometer	62
3.8	Ergänzende Themen und weiterführende Literatur	64
3.9	Übungsaufgaben	64
4	Gemischter Zustand und Dichteoperator	67
4.1	Dichteoperator zu gegebenem Ensemble (statistisches Gemisch)	67
4.1.1	Reiner Zustand	67
4.1.2	Die Physik der statistischen Gemische (Gemenge)	69
4.1.3	Definition und Eigenschaften des allgemeinen Dichteoperators	73
4.1.4	Inkohärente Überlagerung reiner Zustände	74
4.2	Der allgemeine Quantenzustand	76
4.3	Verschiedene Ensemblezerlegungen eines Dichteoperators und Ignoranzinterpretation	76
4.4	Dichteoperatoren von Qubits	79
4.5	Ergänzende Themen und weiterführende Literatur	80
4.6	Übungsaufgaben	80
5	Shannon-Entropie und klassische Information	83
5.1	Definition und Eigenschaften	83
5.2	Shannons Theorem	87
5.2.1	Typische Sequenzen	87
5.2.2	Klassische Datenkompression	89
5.3	Information	90
5.4	Klassische relative Entropie	91
5.5	Wechselseitige Information als Maß für die Korreliertheit zweier Botschaften	92
5.5.1	Wechselseitige Information	92
5.5.2	Bedingte Entropie	93
5.6	Ergänzende Themen und weiterführende Literatur	95
5.7	Übungsaufgaben	95

6	Von-Neumann-Entropie und Quanteninformation	97
6.1	Quantenkanal und Quantenentropie	97
6.2	Qubit als Einheit der Quanteninformation	100
6.3	Eigenschaften	102
6.4	Die Schnittstellen von Präparation und Messung	104
6.4.1	Entropie der projektiven Messung	104
6.4.2	Entropie der Präparation	106
6.5	Quanteninformation	106
6.6	Ergänzende Themen und weiterführende Literatur	107
6.7	Übungsaufgaben	107
7	Zusammengesetzte Systeme	109
7.1	Teilsysteme	109
7.2	Produktraum	110
7.2.1	Vektoren	111
7.2.2	Operatoren	112
7.3	Grundlagen der Physik zusammengesetzter Quantensysteme	114
7.3.1	Postulat für zusammengesetzte Systeme und Ausblick	114
7.3.2	Messungen an einem Teilsystem und reduzierter Dichteoperator	116
7.3.3	Zustand nach einer Messung an einem Teilsystem	117
7.3.4	Lokale Messungen an zwei Teilsystemen	119
7.3.5	Unitäre Dynamik zusammengesetzter Systeme	123
7.4	Quantengatter für mehrere Qubit-Systeme	123
7.4.1	Verschränkung durch das CNOT-Gatter	123
7.4.2	Toffoli-Gatter	126
7.5	Ergänzende Themen und weiterführende Literatur	126
7.6	Übungsaufgaben	127
8	Verschränkung	129
8.1	Korrelationen und Verschränkung	129
8.1.1	Klassisch korrelierte Quantenzustände und LOCC	129
8.1.2	Separabilität und Verschränkung	131
8.1.3	Das Separabilitätsproblem	132
8.2	Verschränkte reine Zustände	133
8.2.1	Schmidt-Zerlegung	133
8.2.2	Schmidt-Zahl und Verschränkung	135
8.2.3	Entropie der Teilsysteme als Maß für Verschränkung	136
8.2.4	Teilsysteme in reinen Zuständen sind total isoliert	137
8.3	Erzeugung verschränkter Zustände	139
8.4	Informationsübertragung mit Überlichtgeschwindigkeit und das No-cloning-Theorem	141
8.5	Zustandsmarkierung durch Verschränkung	143
8.5.1	Welcher-Weg-Markierung	143
8.5.2	Quantenradieren	146
8.5.3	Tatsächlich „delayed choice“?	147

8.6	Ergänzende Themen und weiterführende Literatur	149
8.7	Übungsaufgaben	150
9	Korrelationen und nicht-lokale Messungen	151
9.1	Entropien und Korreliertheit zusammengesetzter Quantensysteme	151
9.1.1	Wechselseitige Information als Maß für Korreliertheit	151
9.1.2	Dreiecksungleichung	152
9.1.3	Verschränkte versus klassische korrelierte Quantensysteme	153
9.2	Nicht-lokale Messungen	156
9.2.1	Bell-Zustände	156
9.2.2	Lokale und nicht-lokale Messungen	157
9.2.3	Nicht-lokal gespeicherte Information und Bell-Messungen	159
9.3	Ergänzende Themen und weiterführende Literatur	161
9.4	Übungsaufgaben	161
10	Es gibt keine (lokal-realistische) Alternative zur Quantentheorie	163
10.1	EPR-Experimente und ihre quantentheoretische Deutung	163
10.2	Korrelierte Handschuhe	166
10.3	Lokaler Realismus	167
10.4	Verborgene Parameter, Bellsche Ungleichungen und Konflikt mit dem Experiment	168
10.5	Separable Quantengemische erfüllen die Bellsche Ungleichung	171
10.6	Bell-Verletzung als Kriterium für Verschränkung bei reinen Zuständen	172
10.7	3-Teilchen-Verschränkung und Quantennichtlokalität	172
10.7.1	GHZ-Zustand	172
10.7.2	Lokaler Realismus und Quantentheorie im Konflikt	173
10.8	Ergänzende Themen und weiterführende Literatur	174
10.9	Übungsaufgaben	175
11	Verschränkung als Hilfsmittel	177
11.1	Quantenkryptographie	177
11.1.1	Die Vernam-Verschlüsselung	177
11.1.2	B92-Protokoll	178
11.1.3	Weitere 1-Qubit-Protokolle	179
11.1.4	EPR-Protokolle	180
11.1.5	Das Schema der Quantenkryptografie	181
11.2	Ein Qubit überträgt zwei Bit (dense coding)	182
11.3	Quantenteleportation	182
11.4	Verschränkungs austausch	184
11.5	Ergänzende Themen und weitere Literatur	185
11.6	Übungsaufgaben	186
12	Quantencomputer	187
12.1	Register und Netzwerke	187
12.2	Funktionsberechnung und Quantenparallelismus	189

12.3	Quantenparallelismus	192
12.4	Zwei einfache Quantenalgorithmen	194
12.4.1	Deutsch-Problem	194
12.4.2	Deutsch-Jozsa-Problem	195
12.5	Suchalgorithmus von Grover	197
12.6	Faktorisierungsalgorithmus von Shor	199
12.6.1	Rückführung von Faktorisierung auf Periodensuche	200
12.6.2	Quantenalgorithmus zur Periodenbestimmung	203
12.7	Quantenfehlerkorrektur mit Hilfe nicht-lokaler Messungen	207
12.7.1	Bit-Flip-Fehler	207
12.7.2	Phasen-Flip-Fehler	209
12.8	Ergänzende Themen und weiterführende Literatur	209
12.9	Übungsaufgaben	211
13	Verallgemeinerte Messungen, POVM	213
13.1	Aufgaben einer allgemeinen Dynamik offener Quantensysteme	213
13.1.1	Fragestellungen	213
13.1.2	Ein einfaches Beispiel	214
13.2	Das nicht-ideale Stern-Gerlach-Experiment als Beispiel für eine verallgemeinerte Messung	217
13.2.1	Der Versuchsaufbau	217
13.2.2	Beispiel einer verallgemeinerten Messung	219
13.2.3	Unschärfe und schwache Messungen	221
13.3	Verallgemeinerte Messungen	222
13.3.1	Was ist eine Quantenmessung?	222
13.3.2	Verallgemeinerte Messpostulate	223
13.3.3	Polare Zerlegung eines linearen Operators	224
13.3.4	Minimale Messungen	225
13.3.5	Realisierung einer verallgemeinerten Messung durch unitäre Transformation und Projektion	227
13.4	POVM-Messung	228
13.4.1	Messwahrscheinlichkeiten und positive Operatoren	228
13.4.2	Zusammengesetzte Messung als Beispiel einer POVM-Messung	229
13.4.3	Kann eine einzelne POVM-Messung zwei Zustände sicher unterscheiden?	230
13.4.4	Vorteil einer POVM-Messung bei der Zustandsermittlung	231
13.4.5	Informationell vollständiges POVM	232
13.4.6	Schätzung des Zustands vor der Messung	233
13.5	Ergänzende Themen und weiterführende Literatur	234
13.6	Übungsaufgaben	235
14	Allgemeine Entwicklung eines offenen Quantensystems und spezielle Quantenkanäle	237
14.1	Quantenoperationen und ihre Operatorsummenzerlegungen	237
14.1.1	Quantenoperationen	237

14.1.2	Operatorsummenzerlegung von Quantenoperationen	239
14.1.3	Quantenoperationen sind noch nicht die allgemeinsten Entwicklungen	240
14.1.4	Einfache Beispiele	241
14.1.5	Mehrdeutigkeit der Operatorsummenzerlegung	242
14.2	Völlig allgemeine Messung und POVM	242
14.3	Quantenkanäle	243
14.3.1	Depolarisierungskanal	243
14.3.2	Quantensprünge und Amplitudendämpfungskanal	245
14.4	Blick zurück: Das Szenario und die Regeln der Quantentheorie	245
14.5	Ergänzende Themen und weiterführende Literatur	248
14.6	Übungsaufgaben	248
15	Dekohärenz und Ansätze für die Beschreibung des Quantenmessprozesses	249
15.1	Dekohärenz erzeugende Kanäle	249
15.1.1	Phasendämpfungskanal	249
15.1.2	Streuung und Dekohärenz	251
15.1.3	Phasenflipkanal	252
15.2	Umgebungsinduzierte Dekohärenz	253
15.2.1	Die Herausbildung der klassischen Welt	253
15.2.2	Schrödingers Katze	255
15.3	Quantenmessprozess*	257
15.3.1	Das Forschungsprogramm*	257
15.3.2	Vormessung*	257
15.3.3	Verschränkung mit der Umgebung fixiert die Observable*	258
15.3.4	Verschränkung mit vielen Freiheitsgraden der Umgebung*	259
15.4	Ist das Messproblem gelöst?*	262
15.5	Die Viele-Welten-Interpretation*	263
15.6	Ergänzende Themen und weiterführende Literatur	264
15.7	Übungsaufgaben	264
16	Zwei Realisierungen von Quantenoperationen*	267
16.1	Operatorsummenzerlegung*	267
16.2	Unitäre Realisierung von Quantenoperationen*	270
16.3	Realisierung einer völlig allgemeinen Messung durch unitäre Transformation und Projektion*	271
16.4	Ergänzende Themen und Literatur	273
16.5	Übungsaufgaben	273
Literatur		275
	Literaturhinweise	275
	Literaturverzeichnis	276
Register		287

Vorwort

Dieses Buch ist ein

Lehrbuch der theoretischen Physik.

Es ist aus Vorlesungen und Seminaren entstanden, die ich in den letzten Jahren an der Universität Konstanz zum Thema

Quanteninformationstheorie und die Grundlagen der Quantentheorie

gehalten bzw. veranstaltet habe.

Die unrelativistische Quantenphysik hat in den letzten ein bis zwei Jahrzehnten eine stürmische Entwicklung durchgemacht. Quantencomputer, Quantenteleportation, Quantenkryptographie, Quanteninformation sind die typischen Schlagwörter, die über den Kreis der Physiker hinaus in populärwissenschaftlichen Artikeln und im Feuilleton mit dieser Entwicklung verbunden werden. Das Konzept der Verschränkung ist das zentrale theoretische Konzept auf diesen „neuen Wegen“ der Quantenphysik, die immer häufiger auch im Physikunterricht an den Schulen beschrieben werden. Die theoretischen Grundlagen der neuen Entwicklungen sind das Thema dieses Buches.

An wen wendet sich das Buch? Das Buch wendet sich in erster Linie an Studenten, aber darüber hinaus auch an alle, die an der Quantenphysik interessiert oder vielleicht sogar von ihr fasziniert sind. Es sollen aber nicht nur Physikstudenten und Physiker, sondern auch Studenten der Informatik, Chemie und anderer Naturwissenschaften, sowie Ingenieure und Lehrer angesprochen werden. Das Buch setzt voraus, dass der Leser schon durch eine Lehrveranstaltung oder durch Selbststudium erste Einblicke in die Quantentheorie hatte. Es fängt also nicht bei null an.

Allerdings werden alle mathematischen und physikalischen Grundkenntnisse, die für die Lektüre späterer Kapitel benötigt werden, als Einstieg in den Anfangskapiteln 1 und 2 wiederholt und aus einer für den Leser möglicherweise neuen Sicht aufgearbeitet. Dabei soll u.a. darauf vorbereitet werden, dass in der Quantentheorie die Konzepte Zustand und Zustandsentwicklung einschließlich Messung anders als in der klassischen Physik zu verstehen sind. Hierauf bauen die in den späteren Kapiteln beschriebenen Verallgemeinerungen auf. Das zweite Kapitel enthält auch ein wissenschaftstheoretisches Rüstzeug, mit dem die Frage diskutiert werden kann, auf welche Realität sich die Quantentheorie bezieht.

Anschließend steigen die Anforderungen an den Leser von Kapitel zu Kapitel an. Die Kapitel bauen aufeinander auf. Übungsaufgaben können zur Kontrolle dienen. Kursiv geschriebene Sätze fassen Ergebnisse zusammen. Fortgeschrittene Leser können mit ihrer Hilfe den Text schnell querlesen.

Zielsetzung Dieses Buch will dem Leser dabei helfen, die raschen Entwicklungen der Quanteninformationstheorie besser überblicken, einordnen und mit angemessenem Aufwand nachvollziehen zu können.

Beschränkung und Ergänzung Der Anspruch an mathematische Präzision entspricht dem der gebräuchlichen Lehrbücher der theoretischen Physik. Inhaltlich beschränke ich mich auf die theoretischen Aspekte. Die Beschreibung der entsprechenden Experimente und technischen Anwendungen würde noch einmal so viele Kapitel benötigen. Jedes Kapitel enthält aber ein Unterkapitel über ergänzende Themen und weiterführende Literatur. Dort wird auf Experimente hingewiesen.

Diese Unterkapitel weisen auch auf theoretische Übersichtsartikel und Bücher hin. Mit deren Hilfe kann der Leser das Dargestellte vervollständigen und vertiefen. Zusammenfassenden Darstellungen wurde gegenüber Originalartikeln der Vorzug gegeben. Es werden also nicht die für die Entwicklung wichtigen Arbeiten rückblickend historisch korrekt aufgelistet, vielmehr sollen in erster Linie für den Leser nützliche weiterführende Literaturhinweise gegeben werden.

Inhalt Im Anschluss an die beiden ersten Kapitel wird in Kap. 3 und 4 zunächst die Physik abgeschlossener Quantensysteme weiterentwickelt. Viele Beispiele und Anwendungen beziehen sich auf Qubits (2-Niveau-Systeme). Mit dem Dichteoperator wird das Konzept des Quantenzustands in Kap. 4 abschließend erweitert. Allgemeinere Zustände gibt es nicht. Kapitel 5 und 6 führen in das klassische bzw. quantentheoretische Entropie- und Informationskonzept ein.

Die Grundlagen der Physik zusammengesetzter Quantensysteme werden in Kap. 7 beschrieben. Dass sich Teilsysteme zusammen in einem verschränkten Zustand befinden können, hat eine Vielzahl von überraschenden Effekten zur Folge. Eine Einführung wird in Kap. 8 gegeben. Verschränkung bedingt Korreliertheit der Teilsysteme. Zur Nicht-Lokalität der Zustände treten noch die Möglichkeiten nicht-lokaler Messungen hinzu (Kap. 9).

Die experimentell nachgewiesenen spezifischen Quantenkorrelationen (EPR-Korrelationen) bestätigen die fundamentale Aussage, dass es keine klassische Alternative zur Quantentheorie gibt (Kap. 10). Diese EPR-Korrelationen können zur Grundlage einer im Prinzip völlig abhörsicheren Quantenkryptographie gemacht werden. Auch die Quantenteleportation beruht auf ihnen (Kap. 12). Für den Quantencomputer ist Verschränkung ein wesentliches Hilfsmittel. Die Ausnutzung der Quantenparallelität erlaubt es, sehr viele Funktionswerte in sehr wenigen Operationen zu berechnen. Das Problem ist dann das Auslesen der Ergebnisse (Kap. 12).

In Kap. 13 wenden wir uns der allgemeinen Dynamik offener Quantensysteme zu und diskutieren zunächst verallgemeinerte Messungen, die die projektiven Messungen als Spezialfall enthalten. Sie spielen zusammen mit den operatorwertigen Maßen (POVM) eine immer

größere Rolle in den aktuellen Publikationen. Die allgemeine Entwicklung von offenen Quantensystemen zwischen Präparation und Messung wird mit Hilfe der Quantenoperationen beschrieben. Verschiedene Quantenkanäle werden diskutiert (Kap. 14). Die Verallgemeinerung der projektiven Messungen und der unitären Transformationen führen auf ein neues Szenario der Quantenphysik.

Dekohärenz ist der Verlust der Interferenzfähigkeit und stellt daher ein Problem beim Quantencomputer dar. Umgekehrt spielt die umgebungsinduzierte Dekohärenz eine wichtige Rolle bei der Beantwortung der Frage warum es klassische Objekte gibt (Kap. 15). Es liegt nahe, diesen Ansatz auch bei der Begründung des Quantenmessprozesses zu versuchen. Mit dem Nachtrag einiger Beweise in Kap. 16 schließt das Buch ab.

Danksagungen An erster Stelle möchte ich mich bei meiner Frau für ihre Geduld bedanken. Die langjährige Zusammenarbeit mit Thomas Konrad hat sehr zum vertieften Verständnis des Stoffes beigetragen. Der „Montagsrunde“ mit Thomas Konrad, Michael Nock und Artur Scherer verdanke ich ebenfalls viele Hinweise, Anregungen und Korrekturen. Vor allen Dingen haben die vielen gemeinsamen Diskussionen dafür gesorgt, dass die Begeisterung für das Thema nicht nachgelassen hat. Joseph Demuth hat die Entstehung des Manuskripts mit Hinweisen und Kommentaren begleitet. Jan Nötzold und Marcus Kubitzki haben bei der Erstellung des Manuskripts geholfen, aber ohne das unermüdliche Engagement von Stefan Bretzel und insbesondere von Michael Nock wäre das Manuskript nicht termingerecht fertig geworden. Ihnen allen vielen Dank. Danken möchte ich schließlich noch dem Zentrum für angewandte Photonik (CAP) an der Universität Konstanz für seine Unterstützung.

Jürgen Audretsch

Konstanz, im Januar 2005

This Page Intentionally Left Blank

1 Der mathematische Rahmen

Es ist die Aufgabe der Quantentheorie – genau wie die jeder anderen physikalischen Theorie – das Ergebnis von Experimenten vorherzusagen und diese Prognose zu begründen. Dazu muss man den Zustand des physikalischen Systems zu Beginn eines Experiments beschreiben, man muss die Entwicklung des Systems während des Experiments formulieren und das Ergebnis einer Wechselwirkung mit dem Messapparat vorhersagen können. Der mathematische Rahmen, der sich für die Formulierung der Quantentheorie bewährt hat, ist die Theorie des Hilbert-Raums und die Wahrscheinlichkeitstheorie. Die fundamentale Verknüpfung zwischen mathematischen Größen und physikalischer Realität wird dabei über die folgenden Zuordnungen etabliert:

Quantensystem	\leftrightarrow	Hilbert-Raum
Quantenzustand	\leftrightarrow	Vektor im oder Operator auf dem Hilbert-Raum
Entwicklung des Quantenzustands	\leftrightarrow	Lineare Operatoren, die auf den Vektoren wirken bzw. lineare Operatoren, die auf den Raum der Operatoren (Liouville-Raum) wirken.
Prognosen	\leftrightarrow	Wahrscheinlichkeitstheoretische Aussagen.

Wir werden dieses Grundschemata der Quantentheorie noch im Einzelnen darstellen. In diesem Kapitel sollen zunächst die benötigten Definitionen und Sätze zusammengestellt werden. Dabei werden wir nicht alle mathematischen Sätze beweisen. Insbesondere werden wir voraussetzen, dass der Leser schon einmal Kontakt mit der Quantentheorie hatte, sodass die Darstellung knapp gehalten werden kann.

Da wir durchweg d -Niveau-Quantensysteme ($d = 2, 3, \dots$) untersuchen werden, wollen wir eine stark vereinfachende Einschränkung machen:

Mathematische Generalvoraussetzung: Wir betrachten Quantensysteme, die mit Hilfe eines endlich-dimensionalen Hilbert-Raums \mathcal{H}_d der Dimension $d = 2, 3, \dots$ beschrieben werden können.

Die Einschränkung ist gerechtfertigt, weil die wesentlichen begrifflichen Probleme sowie die neuen Konzepte und zentralen Methoden bereits mit Bezug auf einen endlich-dimensionalen Hilbert-Raum eingeführt werden können. Wir wollen den konzeptionellen physikalischen Problemen nicht noch mathematische Subtilitäten hinzufügen. Für die meisten physikalisch relevanten Fällen, die eine Beschreibung im unendlich-dimensionalen Hilbert-Raum erfordern, lassen sich die Ergebnisse für endlich-dimensionale Räume direkt übertragen.

Wie in der theoretischen Physik üblich, werden wir die *Dirac-Schreibweise* benutzen. In diesem Rahmen ist es günstig, die dyadische Zerlegung von Operatoren in den Mittelpunkt

der Behandlung zu stellen. Sie ist für praktische Anwendungen wichtig, da sie ein einfaches direktes Ablesen von Operatoreigenschaften und Operatorwirkungen erlaubt.

1.1 Hilbert-Raum der Vektoren

1.1.1 Skalarprodukt, Dirac-Schreibweise

Ein d -dimensionaler Hilbert-Raum \mathcal{H}_d , wie er in der Quantentheorie verwendet wird, ist ein linearer Vektorraum über dem Körper der komplexen Zahlen \mathbb{C} , auf dem ein Skalarprodukt definiert ist. Die Vektoren bezeichnen wir durch $|\varphi\rangle$, $|\psi\rangle$, $|u\rangle$, $|\Phi\rangle$ usw., $|\text{Null}\rangle$ ist der Nullvektor.

Addition, Multiplikation mit einer komplexen Zahl, lineare Unabhängigkeit, Basis und Dimension des Hilbert-Raums \mathcal{H}_d sind analog zu den Begriffen in reellen Vektorräumen definiert.

Je zwei Vektoren $|\varphi\rangle$ und $|\psi\rangle$ ist als *Skalarprodukt* (scalar product) oder *inneres Produkt* (inner product) eine komplexe Zahl zugeordnet, die wir in der Form $\langle\varphi|\psi\rangle$ schreiben. Als Grundlage für diese *Dirac-Schreibweise*¹ (Dirac notation) haben wir einen *Ket-Raum* mit den *Ket-Vektoren* $|\varphi\rangle, |\psi\rangle, \dots$ und den hierzu dualen Vektorraum der *Bra-Vektoren* $\langle\chi|, \langle\theta|, \dots$ eingeführt (Raum der linearen Funktionale). Es ist eine Korrespondenz zwischen den Vektoren des Ket- und des Bra-Raum erklärt (wir verwenden das gleiche Kernsymbol).

$$|\varphi\rangle \xleftrightarrow{d,K.} \langle\varphi|, \quad (1.1)$$

die *duale Korrespondenz* (dual correspondence) genannt wird. Dabei wird dem Ket-Vektor $|\varphi\rangle = c_1|\varphi_1\rangle + c_2|\varphi_2\rangle$ eineindeutig der Bra-Vektor $\langle\varphi| = c_1^*\langle\varphi_1| + c_2^*\langle\varphi_2|$ zugeordnet (* bedeutet konjugiert komplex). Die Reihenfolge im Produkt $\langle\varphi|\psi\rangle$ ist daher wichtig. Es gilt:

$$\begin{aligned} \langle\varphi|\psi\rangle &= \langle\psi|\varphi\rangle^* \\ \langle\varphi|c_1\psi_1 + c_2\psi_2\rangle &= c_1\langle\varphi|\psi_1\rangle + c_2\langle\varphi|\psi_2\rangle, \quad c_1, c_2 \in \mathbb{C} \\ \langle\varphi|\varphi\rangle &\geq 0 \quad \forall |\varphi\rangle \in \mathcal{H}_n, (\langle\phi|\phi\rangle = 0 \Leftrightarrow |\varphi\rangle = |\text{Null}\rangle). \end{aligned} \quad (1.2)$$

Daraus folgt

$$\langle c_1\varphi_1 + c_2\varphi_2|\psi\rangle = c_1^*\langle\varphi_1|\psi\rangle + c_2^*\langle\varphi_2|\psi\rangle. \quad (1.3)$$

Das Skalarprodukt ist linear im zweiten Argument und *antilinear* im ersten Argument. Falls $\langle\varphi|\psi\rangle = 0$ gilt, werden die Vektoren als zueinander *orthogonal* (orthogonal) bezeichnet.

Durch das Produkt wird auf dem Hilbert-Raum eine *Norm* (norm) gemäß

$$\|\varphi\| =: |||\varphi||| := \sqrt{\langle\varphi|\varphi\rangle} \quad (1.4)$$

induziert. Sie verschwindet genau dann, wenn $|\varphi\rangle$ der Nullvektor ist. Wir erwähnen ohne Beweis die *Schwarzsche Ungleichung*

$$|\langle\varphi|\psi\rangle| \leq \|\varphi\| \|\psi\| \quad (1.5)$$

¹Nach Dirac wird das Skalarprodukt $\langle\varphi|\psi\rangle$ geschrieben und „bracket“ genannt. Die Bestandteile „bra“ $\langle\varphi|$ und „ket“ $|\psi\rangle$ haben eine eigenständige Bedeutung

und die *Dreiecksungleichungen*

$$\|\varphi\| - \|\psi\| \leq \|\psi - \varphi\|, \quad \|\varphi + \psi\| \leq \|\varphi\| + \|\psi\|. \quad (1.6)$$

Durch Einsetzen bestätigt man

$$\langle \varphi | \psi \rangle = \frac{1}{4} \left(\|\varphi + \psi\|^2 - \|\varphi - \psi\|^2 + i \|\varphi - i\psi\|^2 - i \|\varphi + i\psi\|^2 \right) \quad (1.7)$$

sowie die *Parallelogrammgleichung*

$$\|\varphi + \psi\|^2 + \|\varphi - \psi\|^2 = 2\|\varphi\|^2 + 2\|\psi\|^2. \quad (1.8)$$

Für einen Satz $\{|\varphi_1\rangle, |\varphi_2\rangle, \dots, |\varphi_l\rangle\}$ von Vektoren aus \mathcal{H}_d wird durch $\text{span}(|\varphi_1\rangle, \dots, |\varphi_l\rangle)$ die Menge aller möglichen Linearkombinationen dieser Vektoren bezeichnet. Diese Menge bildet einen Unterraum von \mathcal{H}_d , der ebenfalls ein Hilbert-Raum ist. Wir bezeichnen eine *orthonormale Basis* (orthonormal basis) mit *ONB*. Für eine ONB $\{|i\rangle, i = 1, \dots, d\}$ gilt die Identität

$$|\varphi\rangle = \sum_{i=1}^d |i\rangle \langle i | \varphi \rangle \quad (1.9)$$

mit den *Komponenten* $\langle i | \varphi \rangle$ des Vektors $|\varphi\rangle$ bezüglich der ONB. Zu einem Unterraum $\hat{\mathcal{H}}$ von \mathcal{H} bildet die Menge aller Vektoren $|\psi\rangle$, die zu allen Vektoren $|\chi\rangle \in \hat{\mathcal{H}}$ orthogonal sind ($\langle \psi | \chi \rangle = 0$), einen weiteren Unterraum von \mathcal{H} , der das *orthogonale Komplement* (orthogonal complement) $\hat{\mathcal{H}}^\perp$ genannt wird. Die direkte Summe beider Unterräume ist wieder der Hilbert-Raum $\mathcal{H} = \hat{\mathcal{H}} \oplus \hat{\mathcal{H}}^\perp := \{\alpha|\chi\rangle + \beta|\psi\rangle \text{ mit } |\chi\rangle \in \hat{\mathcal{H}}, |\psi\rangle \in \hat{\mathcal{H}}^\perp \text{ und } \alpha, \beta \in \mathbb{C}\}$.

1.1.2 Lineare Operatoren auf dem Hilbert-Raum

Lineare Operatoren (linear operators) A, B, \dots bilden Ket-Vektoren in linearer Weise aufeinander ab

$A(\alpha \psi\rangle + \beta \phi\rangle) = \alpha A \psi\rangle + \beta A \phi\rangle$	Linearität
$(A + B) \psi\rangle = A \psi\rangle + B \psi\rangle$	Summe
$(AB) \psi\rangle = A(B \psi\rangle)$	Produkt
$A \psi_a\rangle = a \psi_a\rangle$	Eigenvektor (eigenvector) $ \psi_a\rangle$ von A
$\mathbb{1} \psi\rangle = \psi\rangle$	Eigenwert (eigenvalue) a von A
	Identitätsoperator, Einsoperator (identity operator).

($\alpha, \beta \in \mathbb{C}$). Für den Identitätsoperator $\mathbb{1}$ gilt $\mathbb{1}|\psi\rangle = |\psi\rangle$ für alle $|\psi\rangle$ aus \mathcal{H}_d . Der Definitionsbereich von A muss nicht der gesamte Hilbert-Raum sein und der Wertebereich muss nicht mit dem Definitionsbereich übereinstimmen. Wenn nötig, weisen wir darauf hin. Für den *inversen Operator* (invers operator) A^{-1} gilt $AA^{-1} = A^{-1}A = \mathbb{1}$.

Wir wollen die Dirac-Schreibweise weiter ausbauen und vereinbaren, dass Operatoren auf dem Bra-Raum von rechts auf die Bra-Vektoren wirken sollen:

$$\langle \varphi' | = \langle \varphi | B =: | B \varphi \rangle . \quad (1.11)$$

Die Operatoren auf dem Ket-Raum wirken entsprechend von links. Wir schreiben für den resultierenden Vektor

$$| \psi' \rangle = A | \psi \rangle =: | A \psi \rangle . \quad (1.12)$$

Dem Ket-Vektor $| \psi' \rangle$ entspricht über die duale Korrespondenz (1.1) ein Bra-Vektor $\langle \psi' |$

$$| \psi' \rangle \xleftrightarrow{d.K.} \langle \psi' | = \langle A \psi | . \quad (1.13)$$

Wir führen noch zusätzlich eine duale Korrespondenz für Operatoren ein. In der Dirac-Schreibweise wird der zum Ket-Operator A korrespondierende Bra-Operator ebenfalls mit demselben Symbol A bezeichnet und durch folgende Bedingung an die Skalarprodukte festgelegt (erste Gleichung):

$$(\langle \varphi | A) | \psi \rangle = \langle \varphi | (A | \psi \rangle) =: \langle \varphi | A | \psi \rangle . \quad (1.14)$$

Die zweite Gleichung ist eine für die Dirac-Schreibweise charakteristische geschickte Abkürzung.

Adjungierter Operator Die duale Korrespondenz für Vektoren ordnet dem Ket-Vektor $| \psi \rangle$ einen Bra-Vektor $\langle \psi |$ zu und dem Ket-Vektor $| \psi' \rangle$ einen Bra-Vektor $\langle \psi' |$:

$$\langle \psi | \xleftrightarrow{d.K.} | \psi \rangle \quad (1.15)$$

$$\langle \psi' | = \langle A \psi | \xleftrightarrow{d.K.} | \psi' \rangle = | A \psi \rangle . \quad (1.16)$$

Hiervon ausgehend definieren wir einen zu einem Operator A im Ket-Raum *adjungierten Operator* (adjoint operator) A^\dagger im Bra-Raum, der die linken Seiten der Gl. (1.15) und (1.16) verknüpft und $\langle \psi |$ auf $\langle \psi' |$ abbildet:

$$\langle \psi' | = \langle A \psi | =: \langle \psi | A^\dagger . \quad (1.17)$$

Bei der dualen Schreibweise von Operatoren wird sich diese Relation als nützlich erweisen.

Über die duale Korrespondenz der Operatoren ist damit aber wiederum ein Ket-Operator A^\dagger eingeführt. Wir werten $\langle \psi' | \varphi \rangle$ mit Gl. (1.17) und (1.14) aus.

$$\langle A \psi | \varphi \rangle = (\langle \psi | A^\dagger) | \varphi \rangle = \langle \psi | (A^\dagger | \varphi \rangle) = \langle \psi | A^\dagger \varphi \rangle = \langle \psi | A^\dagger | \varphi \rangle \quad (1.18)$$

und fassen zusammen

$$\langle A \psi | \varphi \rangle = \langle \psi | A^\dagger \varphi \rangle = \langle \psi | A^\dagger | \varphi \rangle . \quad (1.19)$$

Mit $\langle \varphi | \psi \rangle = \langle \psi | \varphi \rangle^*$ folgt aus Gl. (1.19)

$$\langle \psi | A^\dagger | \varphi \rangle = \langle \varphi | A \psi \rangle^* = \langle \varphi | A | \psi \rangle^* . \quad (1.20)$$

Zweifache Anwendung der Gl. (1.20) ergibt

$$\langle \psi | A | \psi \rangle = (\langle \varphi | A | \psi \rangle^*)^* = \langle \psi | A^\dagger | \varphi \rangle^* = \langle \varphi | (A^\dagger)^\dagger | \psi \rangle \quad (1.21)$$

für beliebige Vektoren $\langle \varphi |$ und $\langle \psi |$. Daher gilt

$$(A^\dagger)^\dagger = A \quad (1.22)$$

und wir erhalten die der Gl. (1.19) entsprechende Relation

$$\langle A^\dagger \psi | \varphi \rangle = \langle \psi | A \varphi \rangle = \langle \psi | A | \varphi \rangle . \quad (1.23)$$

In ähnlicher Weise überzeugt man sich leicht von der Gültigkeit der folgenden Operatorrelationen:

$$(A^{-1})^\dagger = (A^\dagger)^{-1} , \quad (cA)^\dagger = c^* A^\dagger \quad (1.24)$$

$$(A + B)^\dagger = A^\dagger + B^\dagger , \quad (AB)^\dagger = B^\dagger A^\dagger . \quad (1.25)$$

Neben der Definition (1.17) werden die Gleichungen (1.22) und (1.23) häufig verwendet.

Dyadische Zerlegung Aus zwei Vektoren $|u\rangle$ und $|v\rangle$ können wir das *dyadische Produkt* (outer product) oder die *Dyade* (dyad) $|u\rangle\langle v|$ bilden. Sie ist ein linearer Operator

$$|\varphi\rangle \rightarrow |\psi\rangle = |u\rangle\langle v|\varphi\rangle ,$$

der in einen Vektor parallel zu $|u\rangle$ überführt. Dabei gilt

$$(\alpha|u\rangle\langle v|)^\dagger = \alpha^*|v\rangle\langle u| . \quad (1.26)$$

Für Operatorprodukte finden wir

$$A|u\rangle\langle v| = |Au\rangle\langle v| , \quad |u\rangle\langle v|A = |u\rangle\langle A^\dagger v| . \quad (1.27)$$

Wir haben in Gl. (1.9) gesehen, dass sich mit Hilfe einer ONB $\{|i\rangle, i = 1, \dots, d\}$ des Hilbert-Raums der Identitätsoperator dyadisch darstellen lässt:

$$\mathbb{1} = \sum_i |i\rangle\langle i| . \quad (1.28)$$

Man nennt dies auch eine *Vollständigkeitsrelation* (completeness relation) oder die *dyadische Zerlegung des Identitätsoperators* (resolution of the identity). Es folgt unmittelbar, dass jeder lineare Operator eine *dyadische Zerlegung* (Äußere-Produkt-Darstellung)

$$A = \sum_{i,j} |i\rangle\langle i|A|j\rangle\langle j| = \sum_{i,j} \langle i|A|j\rangle|i\rangle\langle j| = \sum_{i,j} A_{ij}|i\rangle\langle j| \quad (1.29)$$

mit den *Matrixelementen* $A_{ij} := \langle i|A|j \rangle$ besitzt. Für den adjungierten Operator ergibt sich

$$A^\dagger = \sum_{i,j} A_{ij}^* |j\rangle \langle i|. \quad (1.30)$$

Über die *Supremumsnorm* $\|A\|$ kann man einem linearen Operator A eine positive Zahl zuordnen

$$\|A\| := \max_{\langle \varphi | \varphi \rangle = 1} |\langle \varphi | A | \varphi \rangle|. \quad (1.31)$$

Spur Die *Spur* (trace) ist eine sehr häufig gebrauchte komplexwertige Funktion eines linearen Operators:

$$\text{tr}[A] := \sum_i \langle i|A|i \rangle = \sum_i A_{ii}, \quad \{|i\rangle\} \text{ ONB}. \quad (1.32)$$

Die Spur eines Operators ist unabhängig von der Wahl der Basis. Der Beweis demonstriert die Nützlichkeit der dyadischen Zerlegung (1.28) des Identitätsoperators. Seien $\{|l_i\rangle\}$ und $\{|m_j\rangle\}$ beliebige ONB, dann gilt:

$$\begin{aligned} \text{tr}[A] &= \sum_i \langle l_i|A|l_i \rangle = \sum_{i,j,k} \langle l_i|m_j \rangle \langle m_j|A|m_k \rangle \langle m_k|l_i \rangle \\ &= \sum_{i,j,k} \langle m_k|l_i \rangle \langle l_i|m_j \rangle \langle m_j|A|m_k \rangle = \sum_{j,k} \langle m_k|m_j \rangle \langle m_j|A|m_k \rangle \\ &= \sum_j \langle m_j|A|m_j \rangle. \end{aligned} \quad (1.33)$$

In ähnlicher Weise beweist man mit Hilfe von Gl. (1.28) die folgenden Eigenschaften der Spur:

$\text{tr}[AB] = \text{tr}[BA]$	zyklische Vertauschung
$\text{tr}[A+B] = \text{tr}[A] + \text{tr}[B]$	Linearität
$\text{tr}[\alpha A] = \alpha \text{tr}[A]$	Linearität
$\text{tr}[A \psi\rangle\langle\psi] = \langle\psi A \psi\rangle$	Erwartungswert von A
$\text{tr}[\varphi\rangle\langle\psi] = \langle\varphi \psi\rangle$	Spur einer Dyade
$\text{tr}[A^\dagger] = (\text{tr}[A])^*$	adjungierter Operator

(1.34)

Die physikalische Bezeichnung *Erwartungswert* (expectation value) von A wird später gerechtfertigt.

1.1.3 Normale Operatoren und spektrale Zerlegung

Unter den linearen Operatoren auf \mathcal{H}_d spielen die diagonalisierbaren oder *normalen Operatoren* (normal operators) mathematisch und physikalisch eine herausragende Rolle. Ein Operator N heißt *diagonalisierbar*, wenn es eine ONB $\{|i\rangle\}$ von \mathcal{H}_d und komplexe Zahlen $\lambda_i \in \mathbb{C}$

gibt, so dass

$$N|i\rangle = \lambda_i|i\rangle \quad (1.35)$$

gilt. Dabei ist $\lambda_i = 0$ nicht ausgeschlossen. Als unmittelbare Folge ergibt sich, dass die Matrix von N in der ONB der Eigenvektoren diagonal ist

$$N_{ij} = \langle i|N|j\rangle = \lambda_i\delta_{ij} \quad (1.36)$$

und sich der Operator A in der Form der *spektralen Zerlegung* (spectral decomposition)

$$N = \sum_i \lambda_i |i\rangle\langle i| \quad (1.37)$$

schreiben lässt. Sie heißt auch *orthogonale Zerlegung* (orthogonal decomposition). Die ONB $\{|i\rangle\}$ von Gl. (1.35) wird auch *Eigenbasis* (eigenbasis) von N genannt. Umgekehrt folgt aus jeder dieser Relationen direkt die Erfüllung der Diagonalisierbarkeitsbedingung (1.35).

Gehören zu einem Eigenwert λ_i des Eigenwertproblems (1.35) $g \geq 2$ linear unabhängige Eigenvektoren, so heißt λ_i *g-fach entartet* (degenerate). Jede Linearkombination dieser Eigenvektoren

$$|\psi\rangle = \sum_{i=1}^g c_i |i\rangle \quad (1.38)$$

ist dann ebenfalls Eigenvektor zum Eigenwert a . Die Eigenvektoren spannen einen g -dimensionalen Unterraum $\mathcal{H}_{(a)}$ von \mathcal{H} auf. Der *Projektor*

$$P = \sum_{i=1}^g |i\rangle\langle i|; \quad P^\dagger = P; \quad P^2 = P \quad (1.39)$$

projiziert in den Unterraum $\mathcal{H}_{(a)}$. Der Projektor $Q = 1 - P$ projiziert in das orthogonale Komplement von $\mathcal{H}_{(a)}$.

Diagonalisierbarkeit ist keine trivialerweise vorliegende Eigenschaft. Bereits im zweidimensionalen Hilbert-Raum \mathcal{H}_2 gibt es vielfach gebrauchte Operatoren, die nicht diagonalisierbar sind. Ein Beispiel ist

$$A = |0\rangle\langle 1| \quad \text{mit} \quad \langle 0|1\rangle = 0 \quad \text{und} \quad \langle 0|0\rangle = \langle 1|1\rangle = 1 \quad (1.40)$$

wie mit dem nachfolgenden Satz gezeigt werden kann.

Um zu erkennen, ob ein gegebener Operator ein normaler Operator ist, ist der folgende zentrale Satz sehr nützlich: *Notwendig und hinreichend dafür, dass es für einen Operator N eine spektrale Zerlegung gibt – dass er also diagonalisierbar ist – ist das Verschwinden des Kommutators $[A, B]_- := AB - BA$ von N und N^\dagger :*

$$[N, N^\dagger]_- = 0. \quad (1.41)$$

Der Beweis kann als Anwendungsbeispiel für den bisher aufgebauten Formalismus dienen. Dass aus der Diagonalisierbarkeit die Gl. (1.41) folgt, ist offensichtlich. Die andere Richtung des Beweises zerlegen wir in zwei Schritte:

1. Schritt: Jeder Operator in \mathcal{H}_n hat zumindest einen Eigenwert λ und einen Eigenvektor $|1\rangle$, die sich mit Hilfe der Säkulargleichung ergeben.

$$N|1\rangle = \lambda|1\rangle, \quad \langle 1|N^\dagger = \lambda^*\langle 1|. \quad (1.42)$$

Daraus folgt

$$\langle 1|N|1\rangle = \lambda, \quad \langle 1|N^\dagger|1\rangle = \lambda^* \quad (1.43)$$

und damit

$$N^\dagger|1\rangle = \lambda^*|1\rangle + |a\rangle, \quad \langle 1|N = \lambda\langle 1| + \langle a| \quad (1.44)$$

mit $\langle 1|a\rangle = 0$. Mit Normalitätsbedingung $[N, N^\dagger]_- = 0$ ergibt sich nach Auswertung mit Gl. (1.42) und (1.44)

$$0 = \langle 1|[N, N^\dagger]_-|0\rangle = \langle a|a\rangle. \quad (1.45)$$

$|a\rangle$ ist somit der Nullvektor $|\text{Null}\rangle$ und (1.44) lässt sich folgendermaßen schreiben

$$N^\dagger|1\rangle = \lambda^*|1\rangle, \quad \langle 1|N = \lambda\langle 1|. \quad (1.46)$$

Wir kennen damit die Wirkung von N und N^\dagger auf $|1\rangle$.

2. Schritt: Wir ergänzen $|1\rangle$ zu einer ONB $\{|i\rangle\}$ und führen mit Hilfe der dualen Schreibweise von N

$$N = \sum_{ij} n_{ij} |i\rangle\langle j|, \quad n_{ij} := \langle i|N|j\rangle, \quad n_{1i} = n_{i1} = \lambda\delta_{i1} \quad (1.47)$$

den Operator M ein:

$$M := N - \lambda|1\rangle\langle 1|, \quad M = \sum_{i,j \neq 1} n_{ij} |i\rangle\langle j|. \quad (1.48)$$

M ist die Einschränkung von N auf das orthogonale Komplement von $|1\rangle$.

Mit Hilfe von Gl. (1.42) und (1.46) können wir zeigen, dass auch M ein normaler Operator ist ($[M, M^\dagger]_- = 0$). Für ihn lässt sich auf dem zu $|1\rangle$ senkrechten Unterraum das gleiche Verfahren anwenden. Auch M hat einen Eigenvektor, den wir $|2\rangle$ nennen. Wir ergänzen $|1\rangle$ und $|2\rangle$ zu einer ONB und wiederholen die Prozedur. So fahren wir fort bis der ganze Hilbert-Raum ausgeschöpft ist und $|1\rangle$ zu einer wohlbestimmten ONB ergänzt wurde. Zugleich wird dadurch N bezüglich dieser Basis spektral zerlegt. Das schließt den Beweis ab.

Das Diagramm in Abb. 1.1 demonstriert wie den verschiedenen Eigenschaften der Operatoren im Hilbert-Raum eine zunehmende Spezialisierung in der dyadischen Zerlegung entspricht. Wir werden im Folgenden im Diagramm Schritt für Schritt nach unten gehen.

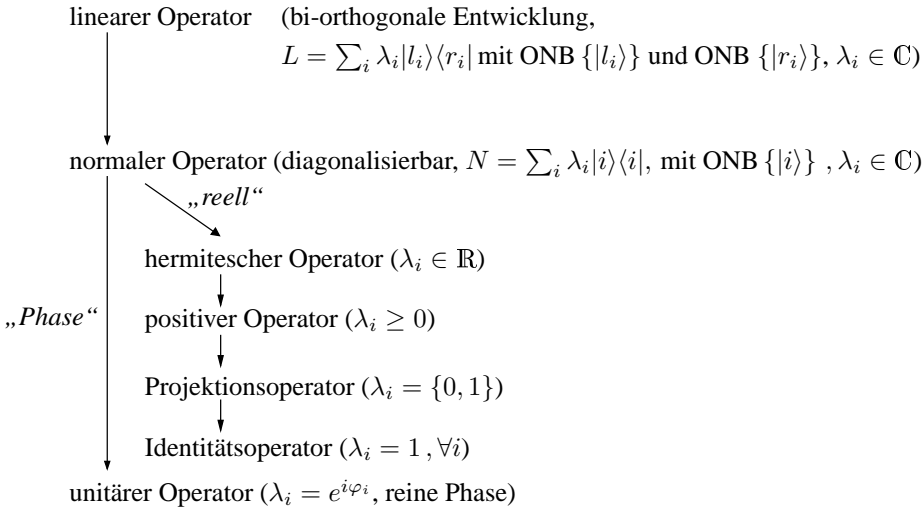


Abbildung 1.1: Operatorenhierarchie. Charakterisierung von Operatoren durch ihre dyadische Zerlegung. \rightarrow ist jeweils die Richtung einer Spezialisierung. In den Klammern () werden die Eigenwerte charakterisiert. Man beachte, dass mit $\lambda_i = \{1, -1\}$ spezielle hermitesche Operatoren auch unitär sein können und umgekehrt. Die bi-orthogonale Entwicklung eines linearen Operators wird in Abschn. 13.3.3 abgeleitet.

Funktionen von Operatoren Eine *Operatorfunktion* $f(N)$ ist durch ihre Entwicklung in eine Potenzreihe definiert. Für einen normalen Operator N lässt sie sich in der dyadischen Zerlegung in einfacher Weise auf die Funktionen der Eigenwerte zurückführen.

$$f(N) := \sum_i f(\lambda_i) |i\rangle \langle i| \rightarrow f(N) |i\rangle = f(\lambda_i) |i\rangle. \quad (1.49)$$

$f(N)$ hat die gleichen Eigenvektoren wie N . Wir geben ein Beispiel, das in der Matrixdarstellung bezüglich der Basis der Eigenvektoren formuliert ist:

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle \langle 0| - |1\rangle \langle 1| \quad (1.50)$$

$$e^{\varphi \sigma_z} = e^{\varphi} |0\rangle \langle 0| + e^{-\varphi} |1\rangle \langle 1| = \begin{pmatrix} e^{\varphi} & 0 \\ 0 & e^{-\varphi} \end{pmatrix}. \quad (1.51)$$

1.1.4 Hermitesche Operatoren

Wir folgen dem rechten Ast der Verzweigung in Abb. 1.1. Ein linearer Operator H heißt *hermitesch* (hermitian) oder *selbstadjungiert* (self-adjoint) auf \mathcal{H}_d , wenn für ihn $H^\dagger = H$ gilt. *Hermitesche Operatoren sind spezielle normale Operatoren.* Wegen der folgenden Eigenschaften spielen sie in der Quantentheorie eine wichtige Rolle: *Hermitesche Operatoren*

besitzen eine Spektralzerlegung mit einer ONB $\{|i\rangle\}$

$$H = \sum_i r_i |i\rangle\langle i|, \quad r_i \in \mathbb{R} \quad (1.52)$$

und reellen Eigenwerten r_i . Bei Entartung können die Eigenvektoren orthonormal gewählt werden, sodass $\{|i\rangle\}$ eine ONB bildet. Eigenvektoren zu verschiedenen Eigenwerten sind orthogonal. Dies wird oft als *Spektraltheorem* (spectral theorem) bezeichnet. Hermitesche Operatoren heißen auch *Observable* (observable). Der Grund für diese physikalische Bezeichnung wird später deutlich werden.

Aus Gl. (1.52) folgt unmittelbar, dass für einen beliebigen Vektor $|\varphi\rangle$ der Erwartungswert (expectation value) $\langle\varphi|H|\varphi\rangle$ reell ist. Es ist eine wichtige Kennzeichnung hermitescher Operatoren, dass auch die Umkehrung gilt: *Der Erwartungswert $\langle\varphi|A|\varphi\rangle$ ist genau dann für alle Vektoren reell, wenn A hermitesch ist.*

Für den Beweis der Umkehrung nehmen wir an, dass für einen Operator A der Mittelwert $\langle\chi|A|\chi\rangle$ für alle Vektoren $|\chi\rangle$ reell ist. Für irgend zwei Vektoren $|\varphi\rangle$ und $|\psi\rangle$ aus \mathcal{H} gilt die Identität

$$\begin{aligned} 4\langle\varphi|A|\psi\rangle = & \{(\langle\varphi| + \langle\psi|)A(|\varphi\rangle + |\psi\rangle) - (\langle\varphi| - \langle\psi|)A(|\varphi\rangle - |\psi\rangle)\} \\ & + i[(\langle\varphi| - i\langle\psi|)A(|\varphi\rangle - i|\psi\rangle) - (\langle\varphi| + i\langle\psi|)A(|\varphi\rangle + i|\psi\rangle)] \end{aligned} \quad (1.53)$$

Wenn wir in diesem Ausdruck $|\varphi\rangle$ und $|\psi\rangle$ vertauschen, dann geht der Teil $\{\dots\}$ in sich über und der Teil $[\dots]$ wird mit (-1) multipliziert. Berücksichtigen wir noch, dass alle Erwartungswerte reell sind, so folgt daraus $\langle\psi|A\varphi\rangle = \langle\varphi|A\psi\rangle^* = \langle A\psi|\varphi\rangle$. Der Operator A ist also hermitesch. Es ist bemerkenswert, dass in Gl. (1.53) rechts nur Erwartungswerte und links ein Übergangsmatrixelement stehen. *Wenn für einen hermiteschen Operator alle Erwartungswerte bekannt sind, sind auch alle Übergangsmatrixelemente bekannt.*

Kommutierende hermitesche Operatoren Für sie gilt der Satz (o.B.) über die simultane Diagonalisierbarkeit: *Zwei hermitesche Operatoren (Observablen) A und B sind genau dann vertauschbar ($[A, B]_- = 0$), wenn sie eine gemeinsame ONB $\{|i\rangle\}$ aus Eigenvektoren besitzen.*

Ist der Eigenwert a einer Observablen A entartet, so bilden die Eigenvektoren einen mindestens zweidimensionalen Unterraum. Mit Angabe von a ist daher kein zugehöriger Eigenvektor eindeutig charakterisiert. Wenn wir im Unterraum nur solche Eigenvektoren von A betrachten, die zugleich Eigenvektoren einer Observablen B zum Eigenwert b sind (Schnittmenge), könnte ein gemeinsamer Eigenvektor durch diese Zusatzforderung bereits eindeutig festgelegt sein. Wir bezeichnen ihn mit $|a, b\rangle$:

$$A|a, b\rangle = a|a, b\rangle, \quad B|a, b\rangle = b|a, b\rangle. \quad (1.54)$$

Sollte wiederum dadurch nur ein Unterraum festgelegt sein, dann werden wir fortfahren und verlangen, dass ein Eigenvektor von A und B zugleich Eigenvektor von einer mit A und B vertauschbaren Observablen C ist: $|a, b, c\rangle$. Das Verfahren muß bis zur Aufhebung aller Entartung fortgesetzt werden. Man nennt einen Satz von Observablen, die genau ein gemeinsames System von Eigenvektoren besitzen, ein *vollständiges System kommutierender Observabler*.

Durch Angabe der Eigenwerte zu allen Operatoren ist genau ein Vektor festgelegt. Wichtig ist, dass das oben beschriebene Verfahren auch tatsächlich abbricht. Dies garantiert der Satz: *Auf jedem Hilbert-Raum \mathcal{H} existiert eine endliche(!) vollständige Menge paarweise kommutierender Operatoren (Funktionen von Operatoren nicht berücksichtigt).* Zum Beweis verweisen wir auf die Literatur (vergl. Abschn. 1.4)

1.1.5 Unitäre Operatoren

Wir folgen zunächst dem linken Ast der Verzweigung der Operatorhierarchie in Abb. 1.1 und kehren danach zum rechten Ast zurück. Ein linearer Operator U heißt *unitär* (unitary), wenn $U^\dagger = U^{-1}$ gilt. *Unitäre Operatoren sind spezielle normale Operatoren. Sie besitzen daher eine Spektralzerlegung*

$$U = \sum_i e^{i\varphi_i} |i\rangle\langle i|, \quad \varphi_i \in \mathbb{R}, \quad (1.55)$$

mit einer ONB $\{|i\rangle\}$, wobei aufgrund der definierenden Gleichung die Eigenwerte reine „Phasenterme“ sind. Wie bei hermiteschen Operatoren spannen die Eigenvektoren den ganzen Raum auf. Eigenvektoren zu verschiedenen Eigenwerten sind orthogonal. Eigenvektoren zu entarteten Eigenwerten können orthogonal gewählt werden. Man zeigt leicht: Ein linearer Operator ist genau dann unitär, wenn jede seiner Matrixdarstellungen unitär ist.

Aus der Spektralzerlegung folgt unmittelbar die Unitarität von $U(t) = e^{iHt}$, $t \in \mathbb{R}$, falls H hermitesch ist. Weiterhin gilt in diesem Fall:

$$U(t=0) = \mathbb{1} \quad (1.56)$$

$$U(t_2)U(t_1) = U(t_2 + t_1). \quad (1.57)$$

Unitäräquivalenz und Normerhaltung Unter kombinierten unitären Transformationen von Vektoren und Operatoren gemäß

$$|\varphi'\rangle = U|\varphi\rangle \quad A' = UAU^{-1} \quad (1.58)$$

bleiben Skalarprodukte (speziell auch die Norm eines Vektors), Eigenwerte und Erwartungswerte unverändert. *Umgekehrt ist ein linearer Operator T , der bei Anwendung auf beliebige Vektoren aus \mathcal{H}_n die Norm erhält*

$$\|T\varphi\| = \|\varphi\| \quad (1.59)$$

ein unitärer Operator: $T^\dagger = T^{-1}$. Zum Beweis verwenden wir die Gl. (1.7) und formen mit Gl. (1.59) um. Für T gilt die Unitaritätsrelation

$$\langle T\varphi|T\psi\rangle = \langle\varphi|\psi\rangle. \quad (1.60)$$

1.1.6 Positive Operatoren und Projektionsoperatoren

Wir wollen noch Spezialfälle hermitescher Operatoren diskutieren. Ein *positiver Operator* ist dadurch definiert, dass für einen beliebigen Vektor $|\varphi\rangle$ die Ungleichung

$$\langle\varphi|A|\varphi\rangle \geq 0 \quad \forall |\varphi\rangle, \quad (1.61)$$

gilt, dass also sein Erwartungswert stets reell und nicht negativ ist. Wir schreiben dann

$$A \geq 0. \quad (1.62)$$

Weiterhin erklären wir

$$A \geq B \Leftrightarrow (A - B) \geq 0. \quad (1.63)$$

Aus der Positivität folgt für die Spektralzerlegung: *Jeder positive Operator A ist hermitesch $A^\dagger = A$. Er besitzt die Spektralzerlegung*

$$A = \sum_i a_i |i\rangle\langle i|, \quad a_i \geq 0. \quad (1.64)$$

mit nicht-negativen Eigenwerten.

Für einen beliebigen Operator A ist $A^\dagger A$ ein positiver Operator. Andererseits gibt es für jeden positiven Operator A einen linearen Operator B , so dass A sich in der Form

$$A = B^\dagger B \quad (1.65)$$

schreiben lässt. B ist nur bis auf unitäre Transformationen festgelegt ($B \rightarrow UB$). Wir finden B explizit über die Spektralzerlegung (1.64) von A und eine ONB $\{|\varphi_i\rangle\}$

$$B = \sum_i \sqrt{a_i} |\varphi_i\rangle\langle i|. \quad (1.66)$$

Einsetzen betätigt (1.65).

Ein linearer Operator P ist ein *Projektionsoperator* (projection operator) (genauer: orthogonaler Projektionsoperator), wenn er die folgenden Bedingungen erfüllt:

- (i) $P^2 = P$ idempotent.
- (ii) $P^\dagger = P$ hermitesch.

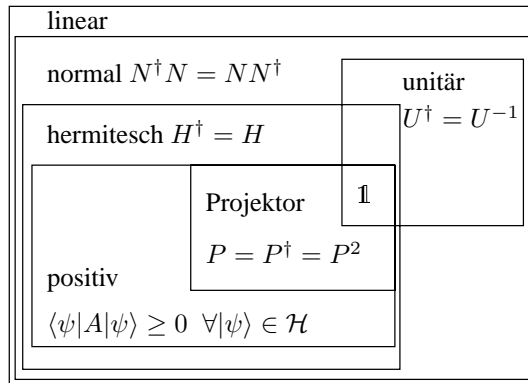


Abbildung 1.2: „Schnittmengen“ der Operatortypen

Aus dieser Eigenschaft folgt

$$\langle v|P|v\rangle = \langle v|PP|v\rangle = \langle v|P^\dagger P|v\rangle = \|P|v\rangle\|^2 \geq 0. \quad (1.67)$$

P ist daher ein positiver Operator und es gilt

$$P = \sum_i p_i |i\rangle\langle i|; \quad p_i \geq 0 \quad (1.68)$$

mit der ONB $\{|i\rangle\}$. Wegen der Idempotenz (i) haben wir weiterhin

$$P^2 = \sum_i p_i^2 |i\rangle\langle i|, \quad P = \sum_i p_i |i\rangle\langle i|, \quad (1.69)$$

und damit $p_i^2 = p_i$ beziehungsweise $p_i \in \{0, 1\}$. Der Projektionsoperator P nimmt deshalb die Form

$$P = \sum_{j \in I} |j\rangle\langle j|, \quad I \leftrightarrow \text{Untermenge der ONB} \quad (1.70)$$

an. P projiziert auf den durch $\{|j\rangle\}$ mit $j \in I$ aufgespannten Unterraum.

In Ergänzung zu Abb. 1.1 sind in Abb. 1.2 im Rückblick die „Schnittmengen“ der verschiedenen Operatortypen dargestellt.

1.2 Liouville-Raum der Operatoren

Wir werden in Kap. 2 sehen, dass sich im Spezialfall der reinen Zustände quantentheoretische Systeme durch normierte Vektoren $|\psi\rangle$ in einem Hilbert-Raum \mathcal{H} beschreiben lassen. Im allgemeinen Fall der gemischten Quantenzustände erfolgt die Beschreibung über den Dichteoperator (Kap. 4). Alle möglichen dynamischen Zustandsänderungen können als lineare Transformationen von Übergängen zwischen Dichteoperatoren beschrieben werden (Schrödinger Bild). Wir werden das ganz allgemein in Kap. 14 diskutieren. Im Hinblick darauf ist es zweckmäßig den Liouville-Raum \mathbb{L} als den Raum der auf dem Hilbert-Raum wirkenden linearen Operatoren einzuführen. Wir können die Darstellung knapp halten, da im Wesentlichen die Vorgehensweise aus Abschn. 1.1 wiederholt wird.

1.2.1 Skalarprodukt

Der *Liouville-Raum* \mathbb{L} ist ein linearer Vektorraum über dem Körper der komplexen Zahlen, dessen Elemente $|A\rangle, |B\rangle, \dots$ die linearen Operatoren A, B, \dots auf einem Hilbert-Raum sind. Man prüft leicht nach, dass diese linearen Operatoren tatsächlich die Axiome eines linearen Vektorraums erfüllen. Wir werden die Klammern $|\rangle$ später zur Vereinfachung der Schreibweise weglassen.

Die dyadische Zerlegung (1.29) eines Operators A nach der Basis $\{|i\rangle\}$ von \mathcal{H}_d hat in der neuen Schreibweise die Form

$$|A\rangle = \sum_{i,j=1}^d A_{ij} |i\rangle\langle j|. \quad (1.71)$$

Die d^2 Dyaden $|i\rangle\langle j|$ in \mathcal{H}_d bilden die d^2 Elemente $||i\rangle\langle j|$ einer Basis in \mathbb{L} . Für die Dimensionen der Räume gilt daher

$$\dim \mathbb{L} = (\dim \mathcal{H}_d)^2 . \quad (1.72)$$

Selbstverständlich gibt es neben den Dyaden andere Basen in \mathbb{L} . Wir können den Liouville-Raum \mathbb{L} mit einem Skalarprodukt $(A|B)$ ausstatten. Es hat formal dieselben Eigenschaften wie das Skalarprodukt im Hilbert-Raum \mathcal{H}_d (vergl. Abschn. 1.1.1). $(A|B)$ ist eine komplexe Zahl und es gilt

$$(A|B) = (B|A)^* , (A|c_1 B_1 + c_2 B_2) = c_1 (A|B_1) + c_2 (A|B_2) , (A|A) \geq 0 . \quad (1.73)$$

Operatorbasis Zwei Operatoren A und B heißen orthogonal, wenn

$$(A|B) = 0 \quad (1.74)$$

erfüllt ist, ohne dass einer der Operatoren der Nulloperator ist. Es gelten die Dreiecksungleichung (1.6) und die zur Parallelogrammungleichung (1.8) analogen Gleichungen. Jeder Operator $|A)$ lässt sich nach einer orthonormalen Basis $\{|Q_s), s = 1, \dots, d^2\}$ von \mathbb{L}

$$(Q_s|Q_t) = \delta_{st}, \quad \sum_{s=1}^{d^2} |Q_s)(Q_s| = \mathbb{1} \quad (1.75)$$

zerlegen:

$$|A) = \sum_{s=1}^{d^2} |Q_s)(Q_s|A) . \quad (1.76)$$

Skalarprodukt als Spur Skalarprodukte auf \mathbb{L} können in ganz verschiedener Weise realisiert werden. Wir werden das über die Spur in \mathcal{H}_d gebildete Skalarprodukt verwenden, da in diesem Fall die für die einfachsten Quantensysteme wichtigen Paulischen Spinoperatoren zu einer Basis ergänzt werden können (vergl. Abschn. 3.1)

$$(A|B) := \text{tr}[A^\dagger B] . \quad (1.77)$$

Die Zerlegung (1.76) nimmt dann bei weggelassenen Vektorklammern die Form

$$A = \sum_{s=1}^{n^2} Q_s \text{tr}[Q_s^\dagger A] \quad (1.78)$$

an. Die aus den Dyaden $|i\rangle\langle j|$, $i, j = 1, \dots, d$ gebildete Basis des Liouville-Raums ist bei Bezug auf das Spur-Skalarprodukt (1.77) orthonormal

$$\left(|i\rangle\langle j| \middle| |i'\rangle\langle j'|\right) = \delta_{ii'} \delta_{jj'} . \quad (1.79)$$

1.2.2 Superoperatoren

Wie zu vermuten ist, lassen sich auf einem Liouville-Raum selber wiederum *lineare* Operatoren definieren, die Elemente aufeinander abbilden:

$$|A\rangle \rightarrow |A\rangle = \mathcal{S}|A\rangle = |\mathcal{S}A\rangle . \quad (1.80)$$

Diese kursiv geschriebenen Operatoren heißen *Superoperatoren* (superoperators). Aus der Sicht des Hilbert-Raums \mathcal{H}_n bilden sie lineare Operatoren in linearer Weise aufeinander ab

$$A \rightarrow B = \mathcal{S}A . \quad (1.81)$$

Beispiele Wir geben zwei Beispiele für Superoperatoren an: Beim Superoperator \mathcal{A}

$$B \rightarrow \mathcal{A}B := ABA^{-1} \quad (1.82)$$

folgt die Linearität aus der Linearität von A . Man sieht leicht, dass

$$\mathcal{A}^{-1}B = A^{-1}BA \quad (1.83)$$

gilt. Ein für die Beschreibung der dynamischen Entwicklung von gemischten Zuständen wichtiger Superoperator (vergl. Kap. 4) ist der *Liouville-Operator* (Liouvillian) \mathcal{L}

$$A \rightarrow \mathcal{L}A := \frac{1}{\hbar} [H, A]_- . \quad (1.84)$$

($[H, A] := HA - AH$). In der physikalischen Anwendung ist H dabei der Hamilton-Operator. Die Potenz von \mathcal{L} schreibt sich

$$\mathcal{L}^2 A = \frac{1}{\hbar^2} [H, [H, A]_-]_- . \quad (1.85)$$

Vom Hilbert-Raum lassen sich direkt die Konzepte des adjungierten, hermiteschen, unitären und positiven Superoperators übertragen.

1.3 Elemente der Wahrscheinlichkeitstheorie

Die zentrale Aufgabe der Quantentheorie ist es, Vorhersagen über die Wahrscheinlichkeiten des Eintreffens von Messergebnissen zu machen. Dabei wird vorausgesetzt, dass Informationen über den Zustand des Quantenobjekts vorliegen, an dem gemessen wird. Im Hinblick auf diese Aufgabe ist es sinnvoll die Grundkonzepte der Wahrscheinlichkeitstheorie kurz darzustellen.

Vorhersagen sind ein Schluss von der Vergangenheit auf die Zukunft. In der klassischen Physik spielt die umgekehrte Schlussrichtung eine vergleichbar wichtige Rolle. Aus den Messergebnissen wird auf den Zustand des Objekts vor der Messung zurück geschlossen. In welchem Umfang ist das auch für Quantensysteme möglich? Bei der Diskussion dieser Frage spielt der Satz von Bayes eine wichtige Rolle. Wir skizzieren seinen Beweis nachdem wir Vorüberlegungen zur bedingten Wahrscheinlichkeit angestellt haben.

1.3.1 Wahrscheinlichkeit zufälliger Ereignisse

Bei der Wiederholung eines Zufallsexperiments liegt das Ergebnis nicht vorher fest. Es ist ein *zufälliges Ereignis* (random event). Solche Ereignisse können beim Werfen eines Würfels z. B. das Auftreten einer geraden (bzw. ungeraden) Augenzahl oder das Auftreten einer Augenzahl größer als 2 sein. Sei $\{A_i; i = 1, \dots, n\}$ die Menge der möglichen Ereignisse. Es werden folgende Bezeichnungen in Analogie zur Mengenlehre eingeführt:

$A_i \cap A_j \cap A_k$ ist das Ereignis das darin besteht, dass die Ereignisse A_i, A_j und A_k zusammen (gleichzeitig) auftreten. Beim Werfen eines Würfels kann A_1 z. B. das Ereignis „gerade Augenzahl“ und A_2 das Ereignis „Augenzahl > 4 “ sein, dann ist $A_1 \cap A_2$ das Ereignis „Es fällt die Sechs“. $p(A_1 \cap A_2)$ ist die Wahrscheinlichkeit, dass sowohl A_1 als auch A_2 eintritt (*Verbundwahrscheinlichkeit*, joint probability). Wir schreiben auch $p(A_1, A_2) := p(A_1 \cap A_2)$.

$A_i \cup A_j \cup A_k$ ist das Ereignis das im Auftreten wenigstens eines der Ereignisse A_i, A_j und A_k besteht. Für die Augenzahl Z möge $2 \leq Z \leq 4$ das Ereignis A_1 und $3 \leq Z \leq 5$ das Ereignis A_2 bedeuten. Dann ist $A_1 \cup A_2$ das Ereignis $2 \leq Z \leq 5$.

Das unmögliche Ereignis wird mit \emptyset und das sichere mit Ω bezeichnet. Zwei Ereignisse A_i und A_j heißen *unvereinbar* (exclusive events), wenn $A_i \cap A_j = \emptyset$ gilt. Sie können nicht gleichzeitig eintreten.

Axiomatik Jedem zufälligen Ereignis A wird eine reelle Zahl $p(A)$ mit $0 \leq p(A) \leq 1$ zugeordnet, die die *Wahrscheinlichkeit* (probability) von A genannt wird und eine Reihe von Axiomen erfüllt, die wir hier nicht aufführen wollen. Ein Beispiel ist die Kolmogorov-Axiomatik. Wir notieren nur das *Additivitätsaxiom*: Für paarweise unvereinbare zufällige Ereignisse A_1, A_2, \dots, A_n gilt

$$p(A_1 \cup A_2 \cup \dots \cup A_n) = p(A_1) + p(A_2) + \dots + p(A_n). \quad (1.86)$$

Wenn die Ereignisse A_1 und A_2 vereinbar sind, gilt

$$p(A_1 \cup A_2) = p(A_1) + p(A_2) - p(A_1 \cap A_2). \quad (1.87)$$

Das Mengendiagramm von Abb. 1.3 veranschaulicht diese Relation. Beim Würfeln möge $Z \leq 2$ das Ereignis A_1 und $Z \geq 4$ das Ereignis A_2 sein, dann ist die Wahrscheinlichkeit dafür, dass entweder A_1 oder A_2 eintritt $p(A_1 \cup A_2) = \frac{2}{6} + \frac{3}{6} = \frac{5}{6}$.

Häufigkeitsinterpretation Wir haben uns zur Veranschaulichung des Axioms auf das Werfen eines Würfels bezogen. Tatsächlich erfordert die Axiomatik wie jede mathematische Axiomatik keine physikalische Interpretation. $p(A)$ ist durch die Axiome selber festgelegt. Bei der Anwendung auf physikalische Ereignisse wird Wahrscheinlichkeit üblicherweise als Grenzwert der *relativen Häufigkeit* (relative frequency) interpretiert:

$$p(A) := \lim_{N \rightarrow \infty} \frac{N(A)}{N} \quad (1.88)$$

Dabei ist $N(A)$ die absolute Häufigkeit des Auftretens von A bei einer Gesamtzahl N von Versuchen. Diese physikalische Interpretation ist nicht unproblematisch. Für endliche große N kann sie als Schätzung von $p(A)$ aufgefasst werden.

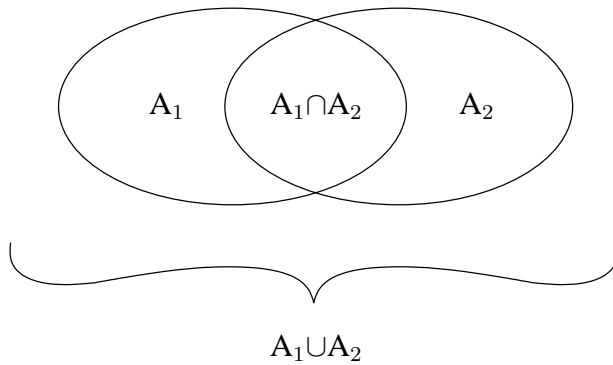


Abbildung 1.3: Mengendiagramm der Wahrscheinlichkeiten.

1.3.2 Bedingte Wahrscheinlichkeit und Satz von Bayes

Wir erweitern das Konzept der Wahrscheinlichkeit, Die *bedingte Wahrscheinlichkeit* (conditional probability) $p(A|B)$ eines Ereignisses A ist die Wahrscheinlichkeit des Eintretens von A unter der Bedingung, dass ein anderes Ereignis B , das selber die Wahrscheinlichkeit $p(B)$ hat, bereits eingetreten ist. Wir definieren:

$$p(A|B) := \frac{p(A \cap B)}{p(B)} . \quad (1.89)$$

Auflösung führt auf die plausible Gleichung für die Wahrscheinlichkeit $p(A \cap B)$ dafür, dass sowohl A als auch B eintritt:

$$p(A \cap B) = p(A|B) \cdot p(B) . \quad (1.90)$$

Wir schreiben in späteren Kapiteln

$$p(A, B) := p(A \cap B) . \quad (1.91)$$

Als Beispiel betrachten wir zwei Urnen. Die Urne U_1 enthält 3 weiße und 3 schwarze Kugeln, die Urne U_2 2 weiße und 4 schwarze Kugeln. In jede der Urnen wird mit gleicher Wahrscheinlichkeit $p(U_1) = p(U_2) = \frac{1}{2}$ gegriffen. Die Wahrscheinlichkeit gezogen zu werden ist für jede Kugel einheitlich $\frac{1}{12}$. Die Wahrscheinlichkeit sowohl in U_1 zu greifen als auch eine weiße Kugel zu ziehen ist $p(w \cap U_1) = \frac{3}{12} = \frac{1}{4}$. Die bedingte Wahrscheinlichkeit $p(w|U_1)$ nachdem man in eine Urne U_1 gegriffen hat eine weiße Kugel zu ziehen ist nach Gl. (1.89)

$$p(w|U_1) = \frac{p(w \cap U_1)}{p(U_1)} = \frac{2}{4} = \frac{1}{2} . \quad (1.92)$$

Das folgt auch anschaulich unmittelbar aus der Beschreibung der Zufallssituation. Analog findet man $p(w|U_2) = \frac{1}{3}$.

Unabhängigkeit Zwei zufällige Ereignisse A und B heißen voneinander *unabhängig*, wenn durch das Eintreten des einen das Eintreten des anderen nicht beeinflusst wird

$$p(A|B) = p(A) . \quad (1.93)$$

In diesem Fall faktorisiert $p(A \cap B)$

$$p(A \cap B) = p(A)p(B) . \quad (1.94)$$

Hiervon ist zu unterscheiden, dass die Ereignisse A und B unvereinbar (einander widersprechend) sind $A \cap B = \emptyset$. Dann gilt $p(A|B) = 0$.

Totale Wahrscheinlichkeit Das sichere Ereignis Ω möge sich als Summe von n paarweise unvereinbaren zufälligen Ereignissen A_i darstellen lassen ($A_i \cap A_j = \emptyset$, $\forall i \neq j$):

$$\Omega = A_1 \cup A_2 \cup \dots \cup A_n; \quad A_i \cap A_j = \emptyset, \quad \forall i \neq j . \quad (1.95)$$

Für ein beliebiges zufälliges Ereignis B gilt dann $B = (A_1 \cap B) \cup (A_2 \cap B) \cup \dots \cup (A_n \cap B)$. Mit dem Additivitätsaxiom (1.86) folgt daraus

$$p(B) = \sum_{i=1}^n p(B \cap A_i) \quad (1.96)$$

und mit Gl. (1.90) ergibt sich der *Satz von der totalen Wahrscheinlichkeit*

$$p(B) = \sum_{i=1}^n p(B|A_i)p(A_i) . \quad (1.97)$$

Wir geben ein Beispiel im nächsten Abschnitt.

Satz von Bayes Mit $p(A \cap B) = p(B \cap A)$ führt die Gl. (1.90) auf

$$p(A|B)p(B) = p(B|A)p(A) . \quad (1.98)$$

Unter der Voraussetzung, dass die paarweise Unvereinbarkeit und Vollständigkeit (1.95) erfüllt ist, gewinnen wir daraus mit Gl. (1.97) den fundamentalen Satz von Bayes (Bayes's theorem)

$$p(A_i|B) = \frac{p(B|A_i)p(A_i)}{\sum_{j=1}^n p(B|A_j)p(A_j)} . \quad (1.99)$$

Der Nenner garantiert die Normierung $\sum_i p(A_i|B) = 1$, die besagt, dass irgendeines der Ereignisse A_i eintreten muß.

Der Satz von Bayes hat folgende Bedeutung: Es seien in einer Situation die Wahrscheinlichkeit $p(A_i)$ und die bedingten Wahrscheinlichkeiten $p(B|A_i)$ bekannt. Dann erlaubt die Formel (1.99) die Berechnung der Wahrscheinlichkeit $p(A_i|B)$ dafür, dass in einem Zufallsexperiment unter der Voraussetzung „ B ist eingetreten“ die Bedingung A_i erfüllt war (bzw. ist).

Wir geben ein Beispiel an, dass sich wieder auf das Ziehen von Kugeln aus Urnen bezieht. Es mögen drei Urnen von Typ I mit jeweils 2 weißen und 6 schwarzen Kugeln vorliegen und eine Urne vom Typ II mit 1 weißen und 7 schwarzen Kugeln. Mit gleicher Wahrscheinlichkeit wird in eine der Urnen gegriffen und eine Kugel gezogen. Das Ereignis B ist das Ziehen einer weißen Kugel. Das Ereignis A_1 ist das Greifen in eine Urne vom Typ I (bzw. Typ II). Dann liegen die folgenden Wahrscheinlichkeiten vor: $p(A_1) = \frac{3}{4}, p(A_2) = \frac{1}{4}, p(B|A_1) = \frac{1}{4}, p(B|A_2) = \frac{1}{8}$. Die Wahrscheinlichkeit, dass die gezogene weiße Kugel aus einer Urne von Typ I stammt, ist nach dem Satz von Bayes $p(A_1|B) = \frac{6}{7} = 0,86$ und daher größer als $p(A_1)$. Aus der Urne vom Typ II stammt die weiße Kugel mit der Wahrscheinlichkeit $p(A_2|B) = \frac{1}{7} = 0,14$, die kleiner als $p(A_2)$ ist. Die Wahl eines Urnentyps erfolgt mit den a-priori-Wahrscheinlichkeiten $p(A_i)$. Wenn eine weiße Kugel gezogen wurde, kann man darauf rückschließen, in welche Urne gegriffen wurde. Für diesen Rückschluss gibt es i.a. wiederum nur eine Wahrscheinlichkeitsaussage, die durch $p(A_i|B)$ gegeben ist. Würde die Urne vom Typ II keine weiße Kugel enthalten, könnte mit Sicherheit ($p(A_1|B) = 1$) der Rückschluss gemacht werden, dass in eine Urne vom Typ I gegriffen wurde.

Annahme von Bayes Sie sollte nicht mit dem Satz von Bayes verwechselt werden. Wenn es keinen Anlass zur Vermutung gibt, dass ein Ereignis A_i durch die Situation ausgezeichnet ist, kann es sinnvoll sein, die *Bayessche Annahme* zu machen, dass alle a-priori-Wahrscheinlichkeiten übereinstimmen

$$p(A_1) = p(A_2) = \dots = p(A_n) . \quad (1.100)$$

Nach dem Eintreten von B wird dann diese Annahme durch die Wahrscheinlichkeiten $p(A_i|B)$ von Gl. (1.99) ersetzt. So lassen sich die Wahrscheinlichkeiten schätzen.

1.3.3 Zufallsgrößen

Eine *Zufallsgröße* X ist durch die Zuordnung von Zahlen x zu den zufälligen Ereignissen gegeben. Würfe eines Würfels sind ein Beispiel. Eine diskrete zufällige Größe X ist bestimmt durch die Werte x_1, x_2, \dots, x_n und die Wahrscheinlichkeiten $p(x_1), p(x_2), \dots, p(x_n)$, mit denen die Werte angenommen werden ($\sum_{i=1}^n p_i = 1$). Die Verallgemeinerung auf abzählbar unendlich viele Werte x_i und auf stetige x ist i.a. unproblematisch.

Wichtige Größen zur Charakterisierung einer Zufallsgröße X sind *Erwartungswert* (expectation value) oder *Mittelwert* (mean value)

$$\langle X \rangle := \sum_i p_i x_i \quad (1.101)$$

und die *Streuung* (dispersion) oder *mittlere quadratische Abweichung* (mean square deviation)

$$\text{var}(X) = (\Delta X)^2 := \langle X^2 \rangle - \langle X \rangle^2 = \langle (X - \langle X \rangle)^2 \rangle , \quad (1.102)$$

die auch *Varianz* (variance) genannt wird. Die *Standardabweichung* (standard deviation) $\Delta X = \sqrt{\text{var}(X)}$ gibt an, wie sehr eine Zufallsvariable um ihren Mittelwert streut. In der Quantentheorie wird $\Delta(X)$ auch als die *Unbestimmtheit* (uncertainty) von X bezeichnet.

1.4 Ergänzende Themen und weiterführende Literatur

- Die meisten Lehrbücher der Quantentheorie enthalten eine Darstellung der mathematischen Grundlagen. Auf folgende Bücher sei besonders hingewiesen: [Sak 85], [CDL 91], [Ish 95], [Bal 98], [Gri 02].
- Eine ausführliche Darstellung des Hilbert-Raums mit Bezug auf die Quantentheorie findet sich in [Jor 69].
- Bra-Raum als Vektorraum aller linearen stetigen Funktionale auf einem Vektorraum V (auch Dualraum V^* genannt): [FK 98, Kap. 2.8 und 4.2].
- Literatursammlung zu 1.3: [Per 93, z. B. 53], [Ish 95], [NC 00].

1.5 Übungsaufgaben

ÜA 1.1 [zu 1.1] Beweisen Sie die Relationen (1.5), (1.6), (1.7), (1.8), (1.24), (1.25), (1.59), (1.34).

ÜA 1.2 [zu 1.1] Geben Sie mehrere Beispiele für eine Basis im \mathcal{H}_3 an.

ÜA 1.3 [zu 1.1] $\{|i\rangle, i = 1, \dots, d\}$ sei eine ONB. Beweisen Sie, dass die Parsevalsche Identität

$$\|\varphi\|^2 = \sum_{i=1}^n |\langle \varphi | i \rangle|^2 \quad (1.103)$$

für alle Vektoren $|\varphi\rangle \in \mathcal{H}_2$ gilt.

ÜA 1.4 [zu 1.1] Zeigen Sie, dass die Matrix, die dem Operatorprodukt AB entspricht, gleich dem Produkt der Matrizen zu A und B ist.

ÜA 1.5 [zu 1.1] Zeigen Sie, dass die Determinante einer unitären Matrix ± 1 ist.

ÜA 1.6 [zu 1.1] Zeigen Sie, dass für zwei unitäre $n \times n$ Matrizen U_1 und U_2 auch die Matrix $\begin{pmatrix} U_1 & 0 \\ 0 & U_2 \end{pmatrix}$ unitär ist.

ÜA 1.7 [zu 1.1] Besitzt der Projektionsoperator $P = |u\rangle\langle u|$ ein Inverses?

ÜA 1.8 [zu 1.1]

- Der Operator A sei diagonalisierbar. Wie findet man seine Spektraldarstellung?
- Sind die Pauli-Operatoren $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$, $\sigma_y = -i|0\rangle\langle 1| + i|1\rangle\langle 0|$, $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$ diagonalisierbar? Finden Sie ihre Spektraldarstellung.

ÜA 1.9 [zu 1.2] Bestätigen Sie für den in Gl. (1.82) definierten Superoperator A die Relation

$$\mathrm{tr}[C(\mathcal{A}B)] = \mathrm{tr}[(\mathcal{A}^{-1}C)B] \quad (1.104)$$

gilt.

ÜA 1.10 [zu 1.2] H sei ein hermitescher Operator mit Eigenwertgleichung

$$H|e_i\rangle = E_i|e_i\rangle. \quad (1.105)$$

Bestimmen Sie Eigenvektoren und Eigenwerte des Liouville-Operators \mathcal{L} von Gl. (1.84).

ÜA 1.11 [zu 1.2] Zeigen Sie, dass der Liouville-Operator von Gl. (1.84) die Matrixdarstellung

$$\mathcal{L}_{ij,i'j'} = \frac{1}{\hbar}(H_{ij'}\delta_{i'j} - \delta_{ij'}H_{i'j}) \quad (1.106)$$

hat.

ÜA 1.12 [zu 1.2] Beweisen Sie mit Bezug auf die Definition des Liouville-Operators \mathcal{L} die Relation

$$e^{c\mathcal{L}}A = e^{\frac{c}{\hbar}H}Ae^{-\frac{c}{\hbar}H}. \quad (1.107)$$

ÜA 1.13 [zu 1.2] Geben Sie Situationen an, mit deren Hilfe die bedingte Wahrscheinlichkeit, der Satz von der totalen Wahrscheinlichkeit oder der Satz von Bayes veranschaulicht werden können.

This Page Intentionally Left Blank

2 Grundkonzepte der Quantentheorie

2.1 Erste Fassung der Postulate (reine Zustände abgeschlossener Quantensysteme)

2.1.1 Das Szenario der Quantentheorie

Wenn man die Quantentheorie auf konzeptionell weniger vertraute Situationen anwenden will, wie sie im Zusammenhang mit zusammengesetzten Systemen auftreten, dann ist es nützlich, sich zunächst noch einmal an die Grundstrukturen der Quantentheorie zu erinnern. Dazu soll das Kapitel 2 dienen.

*Wir machen die **physikalische Generalvoraussetzung**, dass wir nur Vorgänge untersuchen, die keine relativistische Beschreibung benötigen und die auf einem endlich-dimensionalen Hilbert-Raum formuliert werden können.*

Doppelspaltexperiment Die charakteristischen Züge der Quantenphysik werden deutlich, wenn man sie mit denen der klassischen Physik vergleicht. Hierzu betrachtet man zwei analoge physikalische Situationen. In einem Fall kann die Situation im Rahmen der klassischen Physik beschrieben werden, im anderen Fall ist eine quantentheoretische Beschreibung erforderlich. Das Doppelspaltexperiment ist hierfür ein gerne diskutiertes konkretes Beispiel, an dem man viele Elemente der Quantentheorie ablesen kann. Wir besprechen das Experiment daher ausführlich. Die Ergebnisse sollen die Einführung der Postulate in Abschn. 2.1.2 und der Konzepte in Kap. 4 vorbereiten. Verschränkung werden wir später an anderen Experimenten veranschaulichen und damit das Szenario der Quantentheorie noch erweitern.

Wir beschreiben zunächst die experimentelle Situation bei einem Doppelspalt mit den Spaltöffnungen 1 und 2. Vor dem Spalt, d. h. links in der Abb. 2.1a befindet sich ein Apparat für das Schießen von kleinen Kugeln, den wir durch den Wurf einer Münze steuern. Je nachdem wie die Münze fällt, schießt der Apparat durch Spalt 1 oder durch Spalt 2. Dabei soll über die jeweilige Spaltöffnung hin eine gleichmäßige Streuung der Durchschussorte gegeben sein. Hinter dem Doppelspalt wird ein Schirm aufgestellt, auf dem die Einschlagorte der Kugeln registriert werden. Wir diskutieren die Fälle, in denen nur einer der beiden Spalte offen ist (der andere ist abgedeckt), und den Fall, dass beide Spalte offen sind. Wir tragen in allen drei Fällen die relative Häufigkeit der Auftreffer auf dem Schirm als Funktion des Ortes auf. Je häufiger geschossen wird, umso klarer zeigen die relativen Häufigkeiten, wenn nur ein Spalt offen ist, die in Abb. 2.1a angegebene räumliche Verteilung. Sie gibt im Grenzfall vieler Schüsse die Wahrscheinlichkeit $P(x)$ für das Auftreffen der Kugeln wieder. Wenn Spalt 1 abgedeckt wird,

finden wir eine entsprechende Verteilung hinter Spalt 2. Es ist eine Alltagserfahrung, dass sich bei Öffnen beider Spalte die mit dem Faktor $\frac{1}{2}$ multiplizierten Auftreffwahrscheinlichkeiten der Einzelspalte addieren.

In dem analogen quantenphysikalischen Experiment wird der Schussapparat durch eine Apparatur ersetzt, die einen Atomofen enthält¹. Man findet geeignete Apparaturen und passend präparierte Schirme, so dass Folgendes gilt: Wenn man den Schirm, ohne dass ein Doppelspalt vorhanden ist, hinter der Apparatur aufbaut, dann werden nacheinander regellos über den Schirm verteilt einzelne Treffer registriert. Wenn man lange genug wartet, entsteht eine homogene Verteilung der Auftreffpunkte. Da die Treffer zeitlich getrennte Einzelereignisse sind, wollen wir damit die Vorstellung verbinden, dass ein einzelnes Objekt, das wir schon Atom genannt haben, den Ofen verlassen hat und auf dem Schirm aufgeschlagen ist. Über ein Atom zwischen Ofen und Schirm können wir keine Aussage machen. Sodann schieben wir einen geeignet dimensionierten Doppelspalt zwischen Ofen und Schirm ein und schließen wieder zum Beispiel Spalt 2. Dann messen wir im Grenzfall sehr vieler Aufschläge für die relative Häufigkeit (und damit für die Auftreffwahrscheinlichkeit $P(x)$) die räumliche Verteilung von Abb. 2.1b. Ihr Maximum liegt gegenüber der Spaltöffnung. Wenn Spalt 1 geschlossen ist, finden wir eine entsprechend verschobene Kurve gegenüber dem offenen Spalt. Wenn wir allerdings für Atome beide Spalte öffnen, ergibt sich die in Abb. 2.2 dargestellte Verteilung der relativen Häufigkeiten, die ihr Maximum gerade hinter dem Steg zwischen den beiden Spalten hat. Wieder ist der Grenzfall sehr vieler Aufschläge eingezeichnet. Wie bei den Kugeln ändert sich eine Wiederholung des Experimentes die Reihenfolge der Orte der einzelnen Einschläge *in völlig zufälliger Weise* (vergl. Abb. 2.3). Nur im Grenzfall sehr vieler Einschläge ergibt sich *in deterministischer Weise* immer dieselbe Häufigkeitsverteilung.

Als wesentliches Ergebnis halten wir fest: Für Atome erhalten wir die Wahrscheinlichkeitsverteilung beim Doppelspalt – anders als bei Kugeln – nicht durch Addition der Wahrscheinlichkeitsverteilungen der Einzelspalte. Es ist ein *Interferenzbild* entstanden, wie wir es von der Optik her kennen, das nicht dadurch erklärt werden kann, dass wir den Atomen Bahnen zuordnen, wie wir das für die einzelnen Kugeln tun konnten. Wegen der verblüffenden Analogie zur optischen Beugung können wir vermuten, dass die mathematische Berechnung der Wahrscheinlichkeitsverteilung beim Doppelspalt in ähnlicher Weise das Phänomen der Interferenz durch Überlagerung widerspiegeln wird.

Entweder-Oder versus Weder-Noch Im Hinblick auf später immer wieder verwendete Begriffe wollen wir die Experimente mit Kugeln bzw. Atomen noch etwas genauer charakterisieren. Wir fassen die durch die Münze gesteuerte Schießanlage für Kugeln und die jeweiligen Spalte davor als ein *Präparationsverfahren* auf. Präpariert wird der entsprechende Zustand der Kugeln. Wenn nur Spalt 1 (bzw. 2) geöffnet ist, wollen wir den Zustand Z_1 (bzw. Z_2) nennen. Für jeden Zustand liegen die Wahrscheinlichkeitsverteilungen der Auftreffer auf dem Schirm fest. Schießanlage und Doppelspalt präparieren einen weiteren Zustand, den wir $Z_g(1, 2)$ nennen wollen. Die zugehörige Wahrscheinlichkeitsverteilung ergibt sich durch Addition der Verteilungen zu den *klassischen Zuständen* Z_1 und Z_2 , die noch jeweils mit der Wahrscheinlichkeit $\frac{1}{2}$ multipliziert werden. Gemäß der Münzsteuerung der Schießanlage liegen jeweils mit

¹Das Doppelspaltexperiment wurde für Elektronen, Atome, van-der-Waals-Cluster, Fullerene und Biomoleküle mit Erfolg durchgeführt (vergl. Abschn. 15.6).

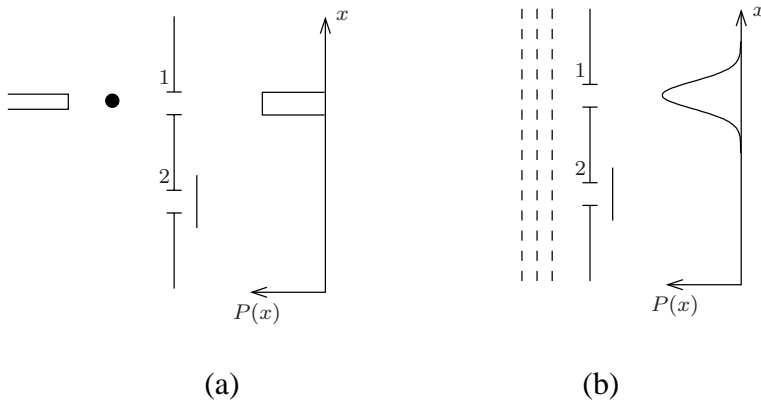


Abbildung 2.1: Schirm hinter einem Einzelspalt: Auftreffwahrscheinlichkeit $P(x)$ für klassische Objekte (a) und für Quantenobjekte (b).

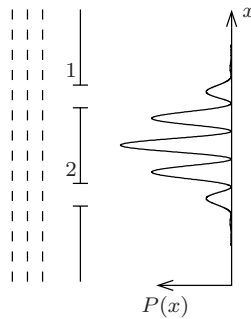


Abbildung 2.2: Schirm hinter einem Doppelspalt: Auftreffwahrscheinlichkeit $P(x)$ für Quantenobjekte.

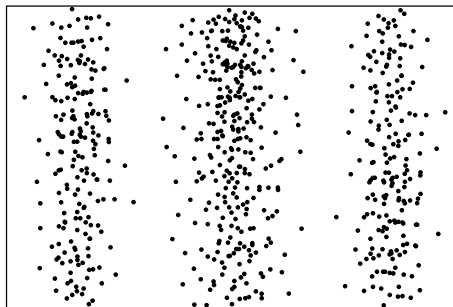


Abbildung 2.3: Es ist völlig zufällig, wo ein einzelnes Quantenobjekt auf dem Schirm auftrifft. Das Streifenbild aus vielen Auftreffpunkten ist hingegen wohlbestimmt.

der Wahrscheinlichkeit $\frac{1}{2}$ Kugeln im Zustand Z_1 und im Zustand Z_2 vor. Durch Mischen der Zustände Z_1 und Z_2 mit diesen Gewichten entsteht der Zustand $Z_g(1, 2)$. Wir nennen so entstandene Zustände *klassische Gemische* (classical mixtures). Für eine einzelne Kugel liegt immer entweder Z_1 oder Z_2 vor. Klassische Gemische sind in diesem Sinne *Entweder-Oder-Zustände*. Das klassische Gemisch enthält über die Würfe der Münze ein statistisches Element. Die Bahn einer einzelnen Kugel ist dagegen völlig determiniert.

Für Atome können wir ebenfalls durch Schließen eines der Spalte die *Quantenzustände* \hat{Z}_1 bzw. \hat{Z}_2 präparieren. Für viele Atome in diesen Zuständen finden wir eindeutig entweder die Wahrscheinlichkeitsverteilungen von Abb. 2.1a oder die verschobene Verteilung. Wenn wir jeweils mit der Wahrscheinlichkeit $\frac{1}{2}$ einen der Spalte abdecken, entsteht der Quantenzustand $\hat{Z}_g(1, 2)$. Die zugehörige Wahrscheinlichkeitsverteilung ergibt sich wie in der klassischen Physik durch Addition der mit dem Faktor $\frac{1}{2}$ gewichteten Wahrscheinlichkeitsverteilungen von \hat{Z}_1 und \hat{Z}_2 . Wieder haben wir nur gemischt. Das Ergebnis wird in der Quantenphysik *statistisches Gemisch* (statistical mixture) oder *Gemenge* genannt. Der Begriff *Quantengemisch* (quantum mixture), den wir in Kap. 4 diskutieren werden, ist allgemeiner und enthält das Gemenge als Spezialfall. Da immer nur einer der Spalte offen war, können wir in diesem Fall davon sprechen, dass das einzelne Atom entweder durch Spalt 1 oder durch Spalt 2 geflogen sein muss. Es liegt ein quantenphysikalischer Entweder-Oder-Zustand vor. Soweit existiert also eine Analogie zu den Zuständen der Kugel.

Für Atome gibt es aber noch einen weiteren Zustand $\hat{Z}_r(1, 2)$ mit einer Wahrscheinlichkeitsverteilung, die für Kugeln nicht auftreten kann. Er entsteht, wenn beide Spalte geöffnet sind (vergl. Abb. 2.2). Wichtig ist, dass diese Wahrscheinlichkeitsverteilung nicht durch Mischen präpariert werden kann. Wir nennen einen ungemischten Zustand einen *reinen Zustand* (pure state). $\hat{Z}_r(1, 2)$ ist ein Beispiel. Anders als bei Kugeln im Zustand $Z_g(1, 2)$ liegt hier ein einzelnes Atom hinter dem Doppelspalt weder im Zustand \hat{Z}_1 noch im Zustand \hat{Z}_2 vor. Der reine Zustand $\hat{Z}_r(1, 2)$ ist ein *Weder-Noch-Zustand*. Wir können dementsprechend auch vom Atom nicht sagen, es sei durch einen der Spalte gekommen. Diese an Kugeln orientierte klassische Vorstellung versagt bei Atomen. Wir erwähnen noch, dass die ungemischten Zustände \hat{Z}_1 und \hat{Z}_2 ebenfalls gemäß unserer Definition reine Zustände sind.

Selektive und nicht-selektive Messung Wir wollen durch Messung für die gemischten Zustände $Z_g(1, 2)$ und $\hat{Z}_g(1, 2)$ von Kugeln bzw. Atomen und für den reinen Zustand $\hat{Z}_r(1, 2)$ der Atome feststellen, hinter welchem Spalt eine einzelne Kugel oder ein einzelnes Atom anzutreffen ist. Die möglichen Messergebnisse sind daher „hinter dem ersten Spalt“ und „hinter dem zweiten Spalt“. Wir strahlen zur Messung Licht ein, das von den Kugeln, bzw. den Atomen gestreut werden kann. Dabei beobachten wir, dass ein Aufblitzen immer nur hinter einem der beiden Spalte stattfindet. Wir haben also die gewünschte Messung realisiert. Anschließend hinterlässt die Kugel bzw. das Atom wieder seinen Einschlagspunkt auf dem Schirm. Tatsächlich ist die experimentelle Realisierung komplizierter. Literaturangaben hierzu finden sich in Abschn. 8.6.

Welche Häufigkeitsverteilungen entstehen, wenn wir wieder sehr viele Einschläge abwarten? Die Antwort hängt nicht nur vom Zustand ab, an dem wir messen, sondern auch davon, wie wir die Messergebnisse auswerten (vergl. Tab. 2.1). Ein mögliches Verfahren besteht dar-

in, selektiv vorzugehen und immer nur die Einschlagspunkte zu markieren, die zum Beispiel zum Aufblitzen hinter Spalt 1 gehören. Wir nennen dies eine *selektive Messung* (selective measurement). Sie bestehen aus vielen Messungen mit anschließender Selektion je nach Messergebnis. Wir lesen an den resultierenden Häufigkeitsverteilungen folgendes ab: Das klassische Gemisch im Zustand $Z_g(1, 2)$ geht in den Zustand $Z(1)$ über. In analoger Weise geht das quantenphysikalische Gemenge $\hat{Z}_g(1, 2)$ in den Zustand $\hat{Z}(1)$ über. Beides ist nicht verwunderlich. Wir haben einfach durch selektive Messung die gemischten Zustände wieder entmischt.

Für Atome können wir darüber hinaus aber auch den reinen Zustand $\hat{Z}_r(1, 2)$ präparieren. Die selektive Messung, die zum Aufblitzen hinter Spalt 1 gehört, überführt diesen Zustand gemäß resultierender Häufigkeitsverteilung in den Zustand $\hat{Z}(1)$. Beim Doppelspalt überführt die selektive Messung also einen reinen Zustand in einen davon verschiedenen reinen Zustand. Die Messung greift ein und ändert ab. Wir können eine selektive Messung auch als eine *Umpräparation* auffassen. Das Resultat der Interferenz beim reinen Zustand wird aufgebrochen. In Spezialfällen wird nicht umpräpariert: Wenn der reine Zustand $\hat{Z}(1)$ vorliegt (Spalt 2 ist geschlossen), dann blitzt es immer hinter Spalt 1 auf. Darüber hinaus zeigt die registrierte Häufigkeitsverteilung der Atome, die geblitzt haben, dass der Zustand $\hat{Z}(1)$ nicht abgeändert wurde. In diesen Fällen bestätigt die Messung nur die Präparation.

Ein alternatives Auswertungsverfahren besteht darin, dass wir nicht selektiv messen, also zwar die Atome und die Kugeln anstrahlen, aber die Aufschlagpunkte unabhängig davon wo der Blitz aufgeleuchtet hat (und daher ohne Auswahl) auf dem Schirm zu einem einzigen Bild zusammenfassen (*nicht-selektive Messung*, non-selective measurement). An der resultierenden Wahrscheinlichkeitsverteilung können wir ablesen, dass für Kugeln wie für Atome gleichermaßen statistisches ein Gemisch (bzw. Gemenge) wieder in ein statistisches Gemisch (bzw. Gemenge) übergeht. Das ist plausibel. Da wir nicht selektieren, mischen wir die Zustände wieder. Für Atome können wir zusätzlich den reinen Zustand $\hat{Z}_r(1, 2)$ präparieren, der keine Entsprechung für Kugeln hat. Wenn wir an diesem Zustand nicht-selektiv messen, erhalten wir die Häufigkeitsverteilung, die zum Gemenge $\hat{Z}_g(1, 2)$ gehört. Wir haben die zu den beiden Messergebnissen gehörigen Zustände $\hat{Z}(1)$ und $\hat{Z}(2)$ gemischt. Im Bereich der Quantenphysik überführt eine nicht-selektive Messung einen reinen Zustand in ein Gemenge.

Schließlich wollen wir eine letzte Bemerkung zur Messung an Atomen machen. Wir hatten oben schon beschrieben, dass $\hat{Z}(1)$ durch eine Messung unverändert bleibt. Eine direkt nachfolgende Messung erfolgt daher wieder am Zustand $\hat{Z}(1)$, und wir registrieren erneut ein Aufblitzen hinter Spalt 1. Das ist der Grund dafür, dass man Atomen mit Aufblitzen zum Beispiel hinter dem ersten Spalt die *Eigenschaft* „hinter Spalt 1“ durchaus zuordnen kann.

Die Messung, die die Frage wiederholt „hinter welchem Spalt?“ führt bei diesen Atomen wieder auf die Antwort „hinter Spalt 1“.

Die typische experimentelle Situation Wir können noch in anderer Weise als durch eine Messung zwischen Doppelspalt und Schirm eingreifen. Wenn die Kugeln bzw. die Atome geladen sind, können wir zum Beispiel ein elektrisches Feld anlegen, dann wird sich das Bild der Auftreffwahrscheinlichkeiten verzerren. Je schwächer das Feld ist umso schwächer ist die Verzerrung. Das elektrische Feld bewirkt eine Änderung des Zustandes. Selbstverständlich ist das Anlegen des elektrischen Feldes nur ein Beispiel. Es gibt andere Eingriffsformen. Einheitlich

	<i>Klassische Physik</i>	<i>Quantenphysik</i>
Selektive Messung	Klassisches Gemisch → in einen der im Gemisch enthaltenen reinen Zustände	Gemenge → in einen reinen Zustand. (*) Reiner Zustand → in einen (im Allgemeinen verschiedenen) reinen Zustand
Nicht-selektive Messung	Klassisches Gemisch → in das gleiche klassische Gemisch	Gemenge → in ein möglicherweise anderes Gemenge Reiner Zustand → in ein Gemenge

Tabelle 2.1: Die Auswirkungen von Messungen in der klassischen Physik und der Quantenphysik. Der Pfeil „→“ besagt: „...“ wird durch Messung in „...“ überführt. Wir verwenden für Gemenge auch die Bezeichnung statistisches Gemisch. Wie wir später sehen werden, gilt (*) nur, wenn keine Entartung vorliegt.

werden wir sie als das Einwirken eines *Transformationsapparates* auffassen. Die ungestörte freie Entwicklung ist als Spezialfall enthalten.

Zusammenfassend lässt sich sagen, dass wir es in der Physik mit drei Typen von Apparaten zu tun haben: Präparationsapparate, Transformationsapparate und Messapparate. Bei einem Versuchsaufbau im Labor liegt jeweils ein spezieller Typ dieser Apparate vor. Das Experiment kann in drei unabhängige aufeinander folgende Phasen zerlegt werden: Präparation, Transformation und Messung (vergl. Abb. 2.4).

Anwendungsbereich der Quantentheorie Die Aufgabe einer physikalischen Theorie ist es, zu bekanntem Präparations- und Transformationsapparat die Messergebnisse, die der Messapparat anzeigt, zu prognostizieren und hierfür eine Begründung auf der Grundlage einer Theorie zu geben. Es zeigt sich bereits am Doppelspalt – insbesondere beim Zustand $\hat{Z}_r(1, 2)$, den wir als Ergebnis einer „Interferenz“ charakterisiert haben – dass es in gewissen Fällen keine Begründung im Rahmen der klassischen Physik gibt. Diese Experimente setzten dem Anwendungsbereich der klassischen Physik Grenzen. Sie liegen außerhalb im *Quantenbereich*. Ein *Quanteneffekt* liegt dann vor, wenn eine rein klassische Begründung des Verhaltens der drei Apparatetypen nicht möglich ist.

Die *Quantentheorie* begründet die Quanteneffekte. Ob und in welcher Weise sie auch eine Begründung für die Effekte der klassischen Physik geben kann, ob also die klassische Physik

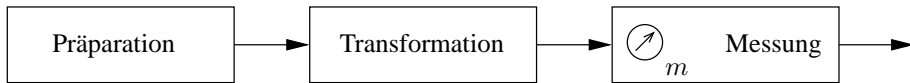


Abbildung 2.4: Die Einflüsse auf den Zustand eines physikalischen Systems.

als ein Grenzfall aus der Quantentheorie ableitbar ist, ist eine offene Frage. Sie ist Gegenstand aktueller Forschung und wir werden noch auf sie in Kap. 15 zurückkommen. Auch die umgekehrte Begründungsrichtung ist denkbar. Der Anwendungsbereich der Quantentheorie könnte leer sein. Kann man möglicherweise Quanteneffekte mit Hilfe der klassischen Physik beschreiben? Wir greifen die Frage in Kap. 10 wieder auf, wenn wir die „verborgenen Parameter“ diskutieren.

2.1.2 Postulate für reine Zustände abgeschlossener Quantensysteme

Wir wollen im Folgenden die theoretische Begründung der Phänomene im Quantenbereich auf einige wenige Grundannahmen zurückführen. Wir verallgemeinern hierzu die Erfahrungen, die wir im Experiment zur Atominterferometrie gemacht haben. Dabei streben wir allerdings nicht die mathematische und begriffliche Präzision einer Axiomatisierung der Quantentheorie an. Hierfür sei auf die Literatur verwiesen. Wir präzisieren zunächst den schon verwendeten Begriff des Quantenzustandes und stellen dann die Postulate vor, die die Quantenphänomene begründen können, die bei reinen Zuständen auftreten. In späteren Kapiteln dieses Buches werden wir die Postulate Schritt für Schritt allgemeiner fassen. Dabei wird sich zeigen, dass die Grundgliederung, die letztlich durch das Schema von Abb. 2.4 bestimmt ist, erhalten bleibt.

Quantensysteme Die Apparate in Abbildung 2.4 werden nacheinander von links nach rechts wirksam. Die Pfeile kennzeichnen dabei den Übergang eines Quantensystems von einem Apparat zum anderen. Mit *Quantensystem* (quantum system) bezeichnen wir etwas, das einen Präparationsvorgang durchlaufen hat und an dem Messungen vorgenommen werden können. Die Begründung dieser Messungen muss dabei in den Bereich der Quantentheorie fallen. Im oben diskutierten Beispiel ist ein einzelnes Atom ein solches Quantensystem. Auch die Spinorientierung eines Atoms oder die Polarisierung eines Photons kann präpariert und registriert werden. In der *Standardinterpretation* der Quantentheorie, die wir in diesem Kapitel anwenden wollen, wird dem einzelnen Quantensystem physikalische *Realität* zugesprochen. Seine Existenz wird behauptet, so wie wir das, ausgehend von den Einzelaufschlägen auf dem Schirm, für die Atome im Atominterferometer bereits getan haben. Wir kommen auf das Problem der Realität im Abschn. 2.5 noch einmal zurück. Wir werden sehen, dass Quantensysteme selber wieder aus Teilsystemen zusammengesetzt sein können. In diesem Fall spielen die verschränkten Zustände eine zentrale Rolle.

Quantenzustand und Messungen Quantensysteme, die in gleicher Weise präpariert wurden, können zu verschiedenen Messergebnissen führen. Beispielsweise können in unse-

rem Experiment die Atome an verschiedenen Orten des Schirms detektiert werden (vergl. Abb. 2.3). Eine bestimmte Präparation legt nur die Wahrscheinlichkeiten für die verschiedenen Messergebnisse fest. Damit die Wahrscheinlichkeitsverteilung experimentell bestimmt werden kann, müssen Messungen an sehr vielen gleich präparierten Systemen durchgeführt werden. *Der Zustand eines Quantensystems ist dem durchlaufenen speziellen Präparationsverfahren zugeordnet. Unter einem Quantenzustand (quantum state) verstehen wir dasjenige mathematische (!) Objekt, das es erlaubt, eindeutig die Wahrscheinlichkeiten für die Ergebnisse aller möglichen Messungen an Systemen zu berechnen, die das zugeordnete Präparationsverfahren durchlaufen haben.* Der Quantenzustand charakterisiert somit das Präparationsverfahren. Wir erwarten also nicht, dass der so eingeführte Quantenzustand eine Entsprechung in der Realität hat, die dem einzelnen Quantensystem zugeordnet werden kann. Für die Zustände von Objekten in der klassischen Physik ist das der Fall. Weiterhin können verschiedene Präparationsverfahren auf den gleichen Zustand führen. Diese Verfahren bilden in diesem Sinne eine Äquivalenzklasse von Zustandspräparationen. Die mathematische Beschreibung des Zustandes und die Berechnung der Wahrscheinlichkeiten werden wir weiter unten postulieren. Durch den Bezug auf Äquivalenzklassen werden auch die individuellen Strukturen der einzelnen Präparations- und Messapparate gleichen Typs eliminiert.

Es ist wichtig, auf diesem Hintergrund noch eine *Sprechweise* zu erklären, die sich eingebürgert hat und die wir auch verwenden wollen: Häufig sagt man, dass ein einzelnes Quantensystem sich in einem speziellen Zustand *befindet* oder einen Zustand *hat*. Gemeint ist damit, dass es die entsprechende Präparationsprozedur aus einer bestimmten Äquivalenzklasse von Präparationen durchlaufen hat. Nur in diesem Sinne ordnet man einem Einzelsystem einen Zustand zu. Wir sind also in diesem ersten Schritt hin zur Formulierung der Standardinterpretation der Quantentheorie sehr zurückhaltend mit Aussagen über Quantensysteme selber. Weitergehende Festlegungen über Existenz von Eigenschaften wie Energie, Ort usw. werden wir erst nach Formulierung der Postulate treffen.

Reine Zustände abgeschlossener Quantensysteme Wie für die Klassische Mechanik der „freie Massenpunkt“ so ist für den Aufbau der Quantentheorie das Konzept des *total isolierten* oder *freien Systems* fundamental. Es handelt sich dabei um eine Idealisierung, die tatsächlich nur näherungsweise realisiert werden kann. Ihr liegt die Vorstellung zugrunde, dass in gewissen Situationen Quantensysteme so vollständig vom Rest der Welt entkoppelt werden können, dass alle möglichen Vorgänge in diesem Rest den Zustand des Systems unverändert lassen. Insbesondere könnte der Rest ohne Einfluss auf das System völlig leer geräumt werden².

Freie Quantensysteme sind für Anwendungen uninteressant. Wir lassen daher zu, dass sich der Zustand des Systems zwischen der Zeit der Präparation und der Zeit der Messung ändern kann. Das äußert sich darin, dass Messungen zu den beiden Zeiten zu verschiedenen Wahrscheinlichkeitsverteilungen der Messwerte führen. Wie in der klassischen Mechanik wird für diese Abweichung vom freien Verhalten eine Ursache angegeben, die hier durch den Transformationsapparat repräsentiert wird. Er beschreibt eine innere Entwicklung des Systems bzw. äußere konstante oder zeitabhängige Einflüsse wie sie zum Beispiel durch elektromagnetische

²Wie wir in nachfolgenden Kapiteln sehen werden reicht für Quantensysteme die Abschirmung aller von außen angreifenden Wechselwirkungen nicht aus. Zur totalen Isolierung müssen zusätzlich alle EPR-Korrelationen mit der Außenwelt verhindert werden. Abschirmung hat so eine neue Qualität erhalten.

oder gravitative Felder verursacht werden. Wir setzen dabei aber voraus, dass es keine Rückwirkung auf das den Einfluss bewirkende äußere System geben soll. Das Quantensystem soll also für Rückwirkungen „nach außen hin“ abgeschlossen sein. Dies wird im Allgemeinen ebenfalls nur näherungsweise der Fall sein. Wir nennen diese Systeme *abgeschlossene Quantensysteme* (closed systems).

Unser Präparationsapparat kann selber aus anderen Präparationsapparaten aufgebaut sein, die mit wohlbestimmten Häufigkeiten tätig werden und entsprechend unterschiedliche Präparationen des Quantensystems durchführen. Auch in diesem Fall ist die Prognose der Wahrscheinlichkeiten aller Messergebnisse eindeutig möglich. Der alles zusammenfassenden Präparationsapparat präpariert einen Zustand, den man mit Blick auf die vielen beteiligten Präparationsprozeduren statistisches Gemisch oder Menge nennt. Der Zustand $\hat{Z}_g(1, 2)$ ist ein Beispiel. Wir werden so präparierte Zustände später noch im Einzelnen untersuchen. Sie sind spezielle Gemische. Für die erste Fassung der Postulate sollen solche Gemische ausgeschlossen sein. Wir beschränken uns auf Zustände, die in keiner Weise durch eine echte Mischungsprozedur erzeugt oder hinsichtlich der Wahrscheinlichkeitsaussage simuliert werden können und nennen sie *reine Zustände* (pure states). Neben der Abgeschlossenheit des Systems ist die Reinheit der Zustände die zweite starke Idealisierung. Wie in der klassischen Mechanik, die auf einem Postulat für die Messpunkte (Inertialsystem) aufbaut, werden wir schrittweise zur Beschreibung realistischer physikalischer Situationen übergehen.

Postulate Es stehen uns damit alle Konzepte zur Verfügung, um die *erste Fassung* der Postulate zu formulieren. Wir werden alle drei Postulate in späteren Kapiteln

Postulat 1 (reiner Zustand) *Ein abgeschlossenes Quantensystem, das sich in einem reinen Zustand befindet, wird durch seinen Zustandsvektor $|\psi\rangle$ beschrieben. Er ist ein normierter Vektor in einem dem System zugeordneten Hilbert-Raum \mathcal{H} .*

Wir vereinfachen zunächst unsere experimentelle Grundsituation und gehen direkt zu Messungen über. Wir denken uns daher den Transformationsapparat herausgenommen oder fassen ihn als Teil des Präparationsapparates auf. Auch für die Messgeräte soll an dieser Stelle zunächst nicht der allgemeinste Fall behandelt werden. Wir beschränken uns vielmehr auf Projektionsmessungen. Dies ist ein bestimmter fundamentaler Typ von Messungen, der aber auch bei den späteren Verallgemeinerungen immer wieder eine zentrale Rolle spielen wird.

Postulat 2 (Projektionsmessung, von Neumann-Messung)

- a) *Eine an einem Quantensystem durchgeführte Projektionsmessung einer physikalischen Größe (z. B. Energie, Drehimpuls, usw.) wird durch einen hermiteschen Operator beschrieben, der auf \mathcal{H} wirkt. Wir sprechen von einer Messung der Observablen A und bezeichnen den Operator mit dem selben Symbol A .*
- b) *Die möglichen Messergebnisse einer Messung der Observablen A sind die Eigenwerte a_n des zugehörigen Observablenoperators A . Wir setzen voraus, dass das Spektrum diskret ist:*

$$A|u_n^i\rangle = a_n|u_n^i\rangle, \quad i = 1, \dots, g_n \quad (2.1)$$

Die $|u_n^i\rangle$ bilden eine orthonormale Basis. g_n ist der Entartungsgrad degeneracy von a_n .

- c) Wenn die Messung der Observablen A an einem System mit normiertem Zustandsvektor $|\psi\rangle$ auf das Messergebnis a_n führt, dann ist der unnormierte Zustandsvektor $|\tilde{\psi}'_n\rangle$ unmittelbar nach der Messung durch die Projektion von $|\psi\rangle$

$$|\psi\rangle \rightarrow |\tilde{\psi}'_n\rangle = P_n|\psi\rangle \quad (2.2)$$

mit dem Projektionsoperator

$$P_n := \sum_{i=1}^{g_n} |u_n^i\rangle\langle u_n^i| \quad (2.3)$$

gegeben, der in den Raum der Eigenvektoren zu a_n projiziert.

- d) Wir bezeichnen mit $N(a_n)$ die Häufigkeit mit der sich der Messwert a_n ergibt, wenn die Messung an N gleich präparierten Systemen im Zustand $|\psi\rangle$ durchgeführt wird. Die relativen Häufigkeiten $\frac{N(a_n)}{N}$ gehen für alle solchen Ensemble im Grenzfall $N \rightarrow \infty$ einheitlich in die Wahrscheinlichkeit $p(a_n)$ als Grenzwert über:

$$\frac{N(a_n)}{N} \xrightarrow{N \rightarrow \infty} p(a_n) \quad (2.4)$$

- e) Die Wahrscheinlichkeit $p(a_n)$ den Messwert a_n zu erhalten, ist gleich dem Erwartungswert des Projektionsoperators P_n vor der Messung bzw. gleich dem Quadrat der Norm des Zustandsvektors $|\tilde{\psi}'_n\rangle$ nach der Messung:

$$p(a_n) = \langle \psi | P_n | \psi \rangle = \|\tilde{\psi}'_n\|^2. \quad (2.5)$$

Messungen, die durch dieses Postulat beschrieben werden, heißen *Projektionsmessungen* (projection measurements) oder *Von-Neumann-Messungen*. Da A ein hermitescher Operator ist, gilt $\sum_n P_n = \mathbb{1}$ und damit, wie für die Gesamtwahrscheinlichkeit zu erwarten ist,

$$\sum_n p(a_n) = \langle \psi | \psi \rangle = 1. \quad (2.6)$$

Wir beschreiben schließlich noch die Wirkung des Transformationsapparates für abgeschlossene Systeme:

Postulat 3 (dynamische Entwicklung zwischen Präparation und Messung)

- a) Die Zeitentwicklung eines abgeschlossenen Quantensystems zwischen zwei beliebigen Zeiten t_0 und t_1 wird durch einen unitären Zeitentwicklungsoperator (time development operator) $U(t_1, t_0)$ beschrieben:

$$U^\dagger(t_1, t_0) = U^{-1}(t_1, t_0). \quad (2.7)$$

Er erfüllt die Bedingungen $U(t_0, t_0) = \mathbb{1}$ und

$$U(t_2, t_1)U(t_1, t_0) = U(t_2, t_0) \quad (2.8)$$

für beliebige Zeiten t_0, t_1, t_2 .

- b) Aus den Bedingungen (2.7) und (2.8) ergibt sich (siehe unten) für $U(t, t_0)$ die Differentialgleichung

$$i\hbar \frac{\partial}{\partial t} U(t, t_0) = H(t)U(t, t_0) \quad (2.9)$$

mit einem hermiteschen Operator H , der explizit zeitabhängig sein kann. $\hbar = 1,0546 \times 10^{-34} \text{ Joule} \cdot \text{sec}$ ist die Plancksche Konstante. Es wird postuliert, dass $H(t)$ diejenige Observable ist, die zur Gesamtenergie des Systems gehört (Hamilton-Operator).

- c) Das Schrödinger-Bild (Schrödinger picture) ist eine der vielen möglichen Beschreibungen der Zeitentwicklung. In diesem Bild wird die dynamische Entwicklung in linearer Weise allein durch den Zustandsvektor gemäß

$$|\psi(t)\rangle = U(t, t_0)|\psi(t_0)\rangle \quad (2.10)$$

wiedergegeben. Observablen können nur explizit zeitabhängig sein.

Andere Bilder, wie z. B. das Heisenberg- und das Wechselwirkungsbild, ergeben sich mit Hilfe der Unitäritätsäquivalenz. Sie sorgt dafür, dass alle Aussagen über Messungen am Ende der Zeitentwicklung in allen Bildern gleich sind. Wir verwenden i.A. das Schrödinger-Bild.

Warum unitäre Zeitentwicklung? Infolge der Unitarität des Zeitentwicklungsoperators bleibt der Zustandsvektor $|\psi\rangle$ normiert und die Gesamtwahrscheinlichkeit irgendeiner der Messwerte zu messen ist gleich eins: $\sum_n p(a_n) = 1$. Wenn man umgekehrt die Erhaltung der Gesamtwahrscheinlichkeit während der dynamischen Entwicklung mit einem (noch nicht als unitär vorausgesetzten) Zeitentwicklungsoperator $T(t_1, t_0)$ fordert, so muss auch zum Zeitpunkt t_1

$$\sum_n p_{t_1}(a_n) = \langle T(t_1, t_0) \psi | T(t_1, t_0) \psi \rangle = 1 \quad (2.11)$$

für alle Zustände $|\psi\rangle$ gelten. Wie wir in Abschn. 1.1.5 gezeigt haben, folgt aus dieser Normerhaltung die Unitarität von T . Man könnte also das Postulat 3 umformulieren und die Forderung der Erhaltung der Gesamtwahrscheinlichkeit an die Spitze stellen.

Schrödinger-Gleichung Der inverse Operator U^{-1} ist wiederum unitär. Die zeitliche Entwicklung eines Quantensystems außerhalb des Messprozesses ist daher umkehrbar. Wählt man in Gl. (2.8) $t_2 = t_0$, dann sieht man, dass der inverse Operator durch

$$U^{-1}(t_1, t_0) = U(t_0, t_1) \quad (2.12)$$

gegeben ist. Gemäß Gl. (2.10) ist die infinitesimale Zeitentwicklung

$$|\psi(t_0 + dt)\rangle = U(t_0 + dt, t_0)|\psi(t_0)\rangle \quad (2.13)$$

durch den Operator $U(t_0 + dt, t_0)$ bestimmt. Seine Entwicklung nach der Zeit kann in der Form

$$U(t_0 + dt, t_0) = \mathbb{1} - \frac{i}{\hbar} H(t) dt \quad (2.14)$$

geschrieben werden, wobei H ein hermitescher Operator ($H^\dagger = H$) mit der Dimension Energie ist. H kann explizit zeitabhängig sein. Die Unitarität ergibt sich dann mit

$$U^\dagger(t_0 + dt, t_0)U(t_0 + dt, t_0) = \left(1 + \frac{i}{\hbar}H(t)dt\right)\left(1 - \frac{i}{\hbar}H(t)dt\right) \simeq \mathbb{1} \quad (2.15)$$

Durch Auswerten von

$$U(t_0 + dt_1 + dt_2, t_0) = U(t_0 + dt_1 + dt_2, t_0 + dt_0) U(t_0 + dt_1, t_0) \quad (2.16)$$

kann man leicht zeigen, dass der infinitesimale Zeitentwicklungsoperator von (2.14) auch die Relation (2.8) bis auf einen Term der Ordnung dt erfüllt.

Die Differentialgleichung für den Zeitentwicklungsoperator $U(t, t_0)$ erhalten wir mit Hilfe von (2.8) und (2.14). Aus

$$U(t + dt, t_0) = U(t + dt, t)U(t, t_0) = \left(1 - \frac{i}{\hbar}H(t)dt\right) U(t, t_0) \quad (2.17)$$

folgt

$$U(t + dt, t_0) - U(t, t_0) = -\frac{i}{\hbar}H(t)dt \quad (2.18)$$

und damit die Gl. (2.9)

$$i\hbar \frac{\partial}{\partial t} U(t, t_0) = H(t)U(t, t_0). \quad (2.19)$$

Im Schrödinger-Bild folgt daraus mit Gl. (2.10) für die Zeitentwicklung des Zustandsvektors die *Schrödinger-Gleichung*

$$i\hbar \frac{\partial}{\partial t} |\psi(t)\rangle = H(t)|\psi(t)\rangle. \quad (2.20)$$

Physikalische Eigenschaften Die Postulate ermöglichen es uns die bisherige Interpretation zu erweitern. Inwieweit können Quantensysteme bestimmte *physikalische Eigenschaften* (properties) haben, wie das in der Standardinterpretation üblicherweise angenommen wird? Wenn der Zustand ein Eigenvektor $|u_n\rangle$ zum Eigenwert a_n des Observablenoperators A ist, dann führt eine Messung von A mit Sicherheit auf das Messergebnis a_n . Wiederholen wir die Messung so ergibt sich immer wieder mit Sicherheit a_n . Dies ist wegen $P_n P_n = P_n$ die charakteristische Eigenschaft projektiver Messungen.

Es macht daher Sinn davon zu sprechen, dass das im Zustand $|u_n\rangle$ präparierte System die physikalische *Eigenschaft* a_n besitzt. Sie wird als real angenommen. Wenn A z. B. der Energie-Operator ist, dann hat das System die Energie a_n . Ergibt sich für einen allgemeinen Zustand $|\psi\rangle \neq |u_n\rangle$ bei Messung von A der Messwert a_n , so kann man allerdings nicht davon sprechen, dass das System die Eigenschaft a_n schon vorher hatte. Erst durch das Zusammenwirken von Quantensystem und Messapparat im Messprozess geht das System in den Zustand $|u_n\rangle$ über und der Messapparat zeigt a_n an. Wir kommen in Abschn. 2.4 auf die oben beschriebene Interpretation der Quantentheorie noch einmal zurück.

2.1.3 Kommentare zu den Postulaten

- Die Dimension des Hilbert-Raums eines Quantensystems ist physikalisch charakterisiert als die maximale Zahl von Zuständen, die in einer Einzelmessung verlässlich voneinander unterschieden werden können. Das wird deutlich, wenn man als Observablenoperator einen hermiteschen Operator nimmt, bei dem keiner der Eigenwerte entartet ist.
- Neben der Dimension des Hilbert-Raums gibt es weitere beobachterunabhängige Charakterisierungen von Quantensystemen, die keiner Wahrscheinlichkeitsaussage unterliegen. Dazu gehören die klassischen Variablen Masse, Ladung und Betrag des Spins eines Quantensystems. Obwohl diese Größen Messgrößen sind, tauchen sie in der unrelativistischen Quantentheorie nur als Parameter auf.
- Die Entwicklung des Systems gemäß Postulat 3 ist deterministisch und reversibel. Zeit ist in der Quantentheorie eine klassische Variable und keine Observable.
- Es wird angenommen, dass nicht nur jeder reine Zustand durch einen Zustandsvektor dargestellt wird, sondern, dass auch jeder Zustandsvektor einen möglichen reinen Zustand repräsentiert. Das zugehörige Präparationsverfahren lässt sich im Prinzip experimentell realisieren.
- Den reinen Zustand haben wir als einen Zustand eingeführt, der nicht gemischt ist. Diese negative Charakterisierung ist für praktische Anwendungen nur bedingt brauchbar. Wir haben aber mit Postulat 2.c ein Verfahren zur Auszeichnung eines reinen Zustandes kennen gelernt, das leichter operationalisierbar ist und auf das wir zurückgreifen können. Ein reiner Zustand entsteht als Ergebnis einer Messung, wenn der Messwert nicht entartet ist. Falls Entartung vorliegt muss ein vollständiger Satz paarweise kommutierender Observablen gemessen werden. Der Satz der zugehörigen Messwerte charakterisiert den resultierenden Zustandsvektor eindeutig.
- Ein dynamischer Prozess stellt einen beobachtbaren Wechsel in den Wahrscheinlichkeitsverteilungen dar. Die Postulate gehen davon aus, dass es im Quantenbereich zwei völlig verschiedene Typen dynamischer Prozesse gibt: den irreversiblen probabilistischen Messprozess (Postulat 2) und die reversible unitäre Zustandsentwicklung zwischen Präparation und Messung (Postulat 3).
- Das legt den Gedanken nahe, das Quantensystem um ein quantentheoretisch beschriebenes Messgerät zu einem größeren abgeschlossenen Quantensystem zu erweitern. Man könnte dann versuchen die gemeinsame Entwicklung im Sinne von Postulat 3 zu beschreiben. Das Postulat 2 würde überflüssig. Wir werden später solche Ansätze noch diskutieren (vergl. Kap. 15). Zunächst bleiben wir dabei, dass mit den Postulaten 2 und 3 zwei ganz verschiedene Dynamiken eingeführt sind: die *Messdynamik* und die *Transformationsdynamik*.
- Es ist das mathematische Zusammenwirken von Zustandsvektor und Observable, das das physikalische Zusammenwirken von Quantensystem und Messapparat im Laboratorium abbildet. Dabei geht – anders als in der klassischen Physik – nicht nur der Messapparat

in einen neuen Zustand über, sondern das Quantensystem ebenfalls. Es muss in der Regel mit einem neuen Zustandsvektor beschrieben werden.

- Es ist zugelassen, dass die Messung das Quantensystem zerstört. Dann entfällt Abschnitt c) von Postulat 2.
- Wir werden annehmen, dass sich zu jedem hermiteschen Operator ein Messapparat finden lässt, der durch den Operator beschrieben wird. Tatsächlich ist es in den meisten Fällen eine keineswegs einfache Aufgabe, eine solche experimentelle Realisierung anzugeben.

2.2 Ausblick

Wir haben bei der Formulierung der Postulate eine ganze Reihe von physikalischen Einschränkungen gemacht, die wir in den kommenden Kapiteln Schritt für Schritt aufgeben wollen, bis sich die ganz allgemeine Struktur der Quantentheorie ergibt.

- Wir haben uns auf reine Zustände beschränkt. Der allgemeine Quantenzustand ist ein Gemisch (Kap. 4).
- Quantensysteme können aus Untersystemen zusammengesetzt sein, die dann im Allgemeinen nicht mehr abgeschlossen sind. Die Quantentheorie solcher offenen Systeme ist zu entwickeln (Kap. 7 und 8). Bei zusammengesetzten Systemen werden wir zum ersten Mal den verschränkten Zuständen begegnen.
- Projektionsmessungen sind ein spezieller Typ von Quantenmessungen. Wir werden in Kap. 13 und Kap. 14 und Verallgemeinerungen einführen.
- Für offene Quantensysteme sind dynamische Entwicklungen möglich, die sich nicht mehr durch unitäre Zeitentwicklungsoperatoren beschreiben lassen. Wir werden sie mit Hilfe von Superoperatoren formulieren (Kap. 14).
- Was lässt sich erreichen, wenn man versucht, die Messdynamik von Postulat 2 auf die Dynamik von Postulat 3 zurückzuführen (vergl. Kap. 15)?

Alle diese Fortentwicklungen vertiefen nicht nur das Verständnis der unrelativistischen Quantentheorie. Sie führen auch auf neue physikalische Effekte und sind die Grundlage von Quanteninformationstheorie und von Quantencomputern.

Weitere Verallgemeinerungen, die wir aber nicht diskutieren wollen, ließen sich anschließen: Wir könnten Observablenoperatoren mit kontinuierlichem Eigenwertspektrum wie Ort und Impuls einbeziehen. Wenn die Zahl der Quantensysteme nicht fest oder wohlbestimmt ist, ist zur Beschreibung ein Fock-Raum nötig. In beiden Fällen sind weitere neue Effekte zu erwarten. Beim Übergang zu Hilbert-Räumen mit abzählbarer unendlicher Dimension können dagegen die bisherigen Ergebnisse in den physikalisch relevanten Fällen direkt übertragen werden.

Bevor wir die angekündigten Verallgemeinerungsschritte durchführen, wollen wir im Folgenden die Macht der Projektionsmessung kennen lernen und in den Abschnitten 2.4 und 2.5 von höherer Warte einen Blick auf den bisher beschriebenen Aufbau der Theorie werfen.

2.3 Manipulation der Zustandsbewegung durch projektive Messungen

Quantentheoretische Messungen greifen in die dynamische Entwicklung eines Quantensystems ein und ändern sie ab. Bei Projektionsmessungen ist dieser Eingriff besonders stark. Wir können durch eine Sequenz von Projektionsmessungen die Entwicklung völlig „einfrieren“ oder aber dem Zustand eine willkürliche Entwicklung aufprägen, ihn also durch Messungen „treiben“.

2.3.1 Quanten-Zeno-Effekt

Kurzzeitverhalten Wir betrachten folgende Situation: Der Zustand des Systems zur Zeit $t = 0$ ist ein Eigenvektor $|a\rangle$ einer Observablen A : $|\psi(t = 0)\rangle = |a\rangle$. A hat ein diskretes Spektrum. Die unitäre Entwicklung erfolgt mit dem zeitunabhängigen Hamilton-Operator H . Wir setzen $\hbar = 1$.

$$|\psi(t)\rangle = e^{-iHt}|a\rangle. \quad (2.21)$$

Nach der Zeit t messen wir die Observable A . Die Wahrscheinlichkeit des Systems nach dieser Messung wieder im Anfangszustand $|a\rangle$ zu finden ist

$$p(t) = |\langle a|e^{-iHt}|a\rangle|^2. \quad (2.22)$$

Für kleine Zeiten erhalten wir daraus

$$p(t) = 1 - (\Delta H)^2 t^2 + \mathcal{O}((\Delta H)^4 t^4) \quad (2.23)$$

mit der Energie-Unbestimmtheit ΔH

$$(\Delta H)^2 := \langle a|H^2|a\rangle - \langle a|H|a\rangle^2 =: \tau_z^{-2}. \quad (2.24)$$

Die Zeit τ_z heißt *Zeno-Zeit*. Sie ist umso größer, je ähnlicher $|a\rangle$ einem Energie-Eigenzustand ist. Im Grenzfall $\Delta H = 0$ ergibt sich $p(t) = 1$. Für $\Delta H \neq 0$ hängt $p(t)$ für kleine Zeiten $t \ll \tau_z$ quadratisch von t ab.

Quanten-Zeno-Effekt³ Wir führen nun über eine Zeit T hin N Messungen der gleichen Observablen A in gleichen Zeitintervallen

$$\tau := \frac{T}{N} \quad (2.25)$$

mit $\tau \ll \tau_z$ durch. Die bedingte Wahrscheinlichkeit $p^{(N)}(T)$ nach jeder einzelnen Messung in der Sequenz immer wieder den Anfangszustand $|a\rangle$ zu finden ist mit (2.23)

$$p^{(N)}(T) = [p(\tau)]^N = [p(T/N)]^N \approx \left(1 - \frac{1}{\tau_z^2} \left(\frac{T}{N}\right)^2\right)^N. \quad (2.26)$$

³Benannt nach dem Pfeil-Paradoxon des Zeno von Elea ca. 495-430 v.Chr.

Je mehr Messungen im Zeitintervall $[0, T]$ bei festem T stattfinden, d.h. je kleiner das Zeitintervall τ wird, desto größer ist die Wahrscheinlichkeit, dass das System im Anfangszustand $|a\rangle$ bleibt. Im Grenzfall $N \rightarrow \infty$ bzw. $\tau \rightarrow 0$ der kontinuierlichen projektiven Messung hat sich die Messdynamik völlig gegenüber der unitären Entwicklung durchgesetzt und das System wird im Anfangszustand „eingefroren“:

$$p^{(N)}(T) \xrightarrow{N \rightarrow \infty} 1. \quad (2.27)$$

Dies nennt man den *Quanten-Zeno-Effekt*. Anders als die Gl. (2.26) ist der Grenzübergang in Gl. (2.27) aber tatsächlich unphysikalisch: Der quantentheoretische Messprozess hat eine gewisse endliche Dauer.

2.3.2 Treiben eines Zustandsvektors durch eine Sequenz von Projektionsmessungen

Wir können durch Projektionsmessungen die Entwicklung eines Quantenzustandes nicht nur näherungsweise unterbinden, sondern auch ihren zeitlichen Verlauf bestimmen. Der Hilbert-Raum des Systems möge zweidimensional sein mit der ONB $\{|\uparrow\rangle, |\downarrow\rangle\}$. Der Anfangszustand zur Zeit $t = 0$ sei $|\uparrow\rangle$. Für eine Observable, die einen dagegen gedrehten Eigenzustand

$$|\alpha\rangle = \cos \alpha |\uparrow\rangle + \sin \alpha |\downarrow\rangle \quad (2.28)$$

hat, ist die Wahrscheinlichkeit das System nach der Messung im Zustand $|\alpha\rangle$ zu finden

$$p(\alpha) = \cos^2 \alpha. \quad (2.29)$$

Wir führen wieder N Messungen mit Zeitabstand $\tau = \frac{T}{N}$ im Zeitintervall $[0, T]$ durch. Aber in diesem Fall gehen wir dabei nacheinander jeweils zu neuen Observablenoperatoren über, die die Eigenzustände $|\alpha_n\rangle$ mit $\alpha_n = n\omega\tau$ und $n = 1, 2, 3, \dots$ besitzen. Wir nehmen an, dass es keine zusätzliche unitäre Entwicklung gibt. Dann ist die bedingte Wahrscheinlichkeit das System im Zustand $|\alpha_n\rangle$ zu finden, wenn es vorher im Zustand $|\alpha_{n-1}\rangle$ war

$$\tilde{p}(n) = |\langle \alpha_n | \alpha_{n-1} \rangle|^2 = \cos^2 \omega\tau. \quad (2.30)$$

Die Wahrscheinlichkeit das System nach jeder dieser Messungen im entsprechenden Eigenzustand $|\alpha_1\rangle, |\alpha_2\rangle, |\alpha_3\rangle \dots$ zu finden ist

$$\tilde{p}^{(N)}(n) = \left(\cos \omega \frac{T}{N} \right)^{2N} \xrightarrow{N \text{ groß}} 1 - \frac{\omega^2 T^2}{N^2} 2N \xrightarrow{N \rightarrow \infty} 1. \quad (2.31)$$

Im Grenzfall $N \rightarrow \infty$ bei festem t bzw. für den Zeitabstand $\tau \rightarrow 0$ stimmt der Systemzustand stets mit dem Zustand $|\alpha\rangle$ von Gl. (2.28) mit $\alpha = \omega t$ überein. Dem System ist eine vorgegebene Zustandsbewegung durch eine Sequenz angepasster projektiver Messungen aufgezwungen worden. Auch in diesem Fall ist der Grenzfall $\tau \rightarrow 0$ im strengen Sinne unphysikalisch wegen der endlichen Dauer des Messprozesses.

2.4 Die Struktur physikalischer Theorien*

Wir haben bisher immer nur von der Standardinterpretation gesprochen. Gibt es andere Interpretationen? Was versteht man unter der Interpretation einer physikalischen Theorie? Wir werden uns in den nächsten beiden Kapiteln diesen Fragen zuwenden. Beide Kapitel sind zum Verständnis der restlichen Kapitel nicht nötig und können daher auch überlesen werden. Andererseits spielen gerade die mit Interpretationsproblemen verknüpften naturphilosophischen⁴ und wissenschaftstheoretischen⁵ Fragen sowohl in Grundsatzdiskussionen als auch in populärwissenschaftlichen Darstellungen eine große Rolle. Gerade die Frage „Was sagt die Quantenphysik über die Wirklichkeit aus?“ übt offenbar auf viele Physiker und Nicht-Physiker eine große Faszination aus. Das rechtfertigt ein mit einem Stern versehene Anmerkungen dazu, wie solche Fragen einzuordnen sind. Sie können auch für den mehr „praktisch“ orientierten Leser nützlich sein, da dadurch manche Konfusion in der Diskussion quantentheoretische Probleme und der Interpretation von Aussagen vermieden werden kann.

2.4.1 Bauelemente einer physikalischen Theorie*

Vortheorien Wir schließen das Kapitel 2 über die Grundkonzepte der Quantentheorie mit einigen strukturellen Überlegungen ab. Dabei soll insbesondere nach der Wirklichkeit gefragt werden, auf die sich die Quantentheorie bezieht. Hierzu ist es nützlich sich zunächst klar zu machen wie physikalische Theorien aufgebaut sind. Wir machen hierzu einen Ausflug in die klassische Physik und betrachten die Elektrodynamik. Typische elementare Experimente bestehen darin, dass Kräfte gemessen werden, Drähte sich erwärmen und Ähnliches. Kraftmessung, Wärmemessung und andere Messungen beziehen sich dabei auf Theorien wie Mechanik, Thermodynamik usw., die bereits vor der Elektrodynamik und unabhängig von ihr formuliert werden. Sie sind für die Elektrodynamik *Vortheorien*. Neben Drähten und Massen werden wir auch Kraftfelder, Wärme usw. zur physikalischen Wirklichkeit zählen. Es sind die Elemente der Wirklichkeit, die mit Hilfe der Vortheorien bereits eingeführt wurden. Wenn wir die Elektrodynamik experimentell und theoretisch entwickeln, gehen wir davon aus, dass die auf den Vortheorien beruhenden Apparaturen und Messgeräte Teile der physikalischen Wirklichkeit sind.

Bauelemente Damit können wir bereits am Beispiel der Elektrodynamik mehrere Bauelemente einer physikalischen Theorie ablesen. Eine *physikalische Theorie* ist ein mathematisch-deduktives Schema, das die folgenden Mindestbestandteile enthält:

1. einen *mathematischen Teil* MT, der aus mathematischen Größen, Definitionen, Gleichungen, Umformungen, Lösungsprozeduren usw. besteht,
2. einen Teil der Natur, den man *Grundbereich* GB nennt und von dem angenommen wird, dass er existiert

*Die mit einem Stern gekennzeichneten Kapitel können bei einem ersten Durchgang überschlagen werden.

⁴Die *Naturphilosophie* untersucht die Begriffe, die erforderlich sind um zu verstehen, was die Naturwissenschaften über die Natur aussagen. Sie ist eine auf die Natur bezogene *Ontologie*, also eine Lehre vom Sein.

⁵*Wissenschaftstheorie* (Erkenntnistheorie) gibt eine logische Analyse wissenschaftlicher Theorien und vergleicht Theorien miteinander. Themen sind dabei u.a.: Konzepte der Wirklichkeit, Grenzen der Erkenntnis, physikalische Theorien als Handlungsanweisungen, Wirklichkeit als Konstruktion und vieles mehr.

3. und *Abbildungsprinzipien* AP, die man auch *Korrespondenzregeln* nennt, die den Grundbereich GB und Teile vom mathematischen Teil MT aufeinander beziehen.

Erst dadurch, dass die Abbildungen zu den mathematischen Relationen hinzukommen, entsteht eine physikalische Theorie. Typischerweise können die mathematischen Größen dann auch dimensionsbehaftet sein.

So wird z. B. in der Elektrodynamik der Buchstabe **F** im mathematischen Teil mit dem Wort „Kraft“ bezeichnet und eine Abbildung zu dem hergestellt, was man z. B. mit realen Federwaagen messen oder an der Bewegung von Massen ablesen kann. Es werden mit den Abbildungsprinzipien in den Grundbereich nur Abbildungen in den Wirklichkeitsbereich der Vorthorien hergestellt. Die Vorthorie ist in diesem Fall die Mechanik bzw. Thermodynamik. Zur Beschreibung und zur Vorhersage von Experimenten zur Elektrodynamik genügen diese Abbildungen aber völlig. Die Messgrößen entstammen diesem Bereich. Zwar gibt es im mathematischen Teil der Theorie z. B. auch das Symbol **j**, zu dem wir „elektrische Stromdichte“ sagen, es reicht aber für die experimentelle Aussage, dass wir der Theorie entnehmen können, dass ein Draht sich erwärmt. Wir können so Ströme messen. Es ist nicht nötig hierfür vorauszusetzen, dass es elektrische Ströme „in Wirklichkeit“ gibt und sie irgendwie durch Drähte „fließen“. Das Wort Strom dient zunächst dann nur dazu, sich über Teile der Theorie schneller verständigen zu können.

Interpretation Wir verstehen unter der *Interpretation* (interpretation) einer Theorie die Angabe der Abbildungsprinzipien, mit denen Symbole des mathematischen Teils MT der physikalischen Theorie durch Verknüpfung mit Teilen der Wirklichkeit *physikalisch interpretiert* werden. Es werden für einige mathematische Symbole physikalische Referenzen angegeben. In diesem Sinne ist eine physikalische Theorie ein teilweise interpretiertes formales System. Man sollte streng dazwischen unterscheiden, ob zu gleichem MT die Abbildungsprinzipien geändert oder erweitert werden, oder ob in einer *Alternativtheorie* auch der MT geändert und z. B. andere Feldgleichungen postuliert werden. Die bisher geschilderte Interpretation, die sich nur auf den Wirklichkeitsbereich der Vorthorie bezieht, wollen wir die *Minimalinterpretation* (minimal interpretation) nennen. Sie umfasst den Minimalbestand an Abbildungsprinzipien, die nötig sind, um für den mathematischen Teil den Anschluss an die Beobachtungsebene zu erreichen. Auf der Grundlage der Minimalinterpretation kann über die empirische Richtigkeit einer physikalischen Theorie entschieden werden. Darüber hinausgehende Elemente einer Interpretation können weder experimentell bestätigt noch widerlegt werden. Es sind viele solcher konsistenten Erweiterungen und damit viele Interpretationen denkbar. Sie sind weder richtig noch falsch. Es sind Fragen der Erklärungskraft und Verstehbarkeit, die dazu motivieren können über die Minimalinterpretation hinauszugehen. Von erweiterten Interpretationen können wertvolle Impulse für neue Forschungsprogramme ausgehen. Die Suche nach einer Theorie des Quantenmessprozesses ist ein Beispiel (vergl. Kap. 15). Wir machen noch darauf aufmerksam, dass der Begriff Minimalinterpretation in der Literatur unterschiedlich verwendet wird.

2.4.2 Theoretische Terme*

Schon das Beispiel Elektrodynamik zeigt, dass die meisten Physiker über die Minimalinterpretation hinausgehen. Im mathematischen Teil der Elektrodynamik tauchen neben Termen, die eine Abbildung in die Ausschläge von Messgeräten erlauben, weitere Terme wie z. B. das elektrische Feld \mathbf{E} oder der Strom \mathbf{j} auf, von denen ebenfalls eine Entsprechung in der Realität angenommen wird. Die hierzu gehörigen zusätzlichen Abbildungsprinzipien wollen wir *hypothetische Abbildungsprinzipien* hAP nennen. Der Bereich in den sie abbilden, heißt *erschlossener Wirklichkeitsbereich* eWB und die entsprechenden Terme der mathematischen Theorie nennt man *theoretische Terme* (vergl. Abb. 2.5). Üblicherweise herrscht Konsens darüber, dass man die hypothetischen Abbildungsprinzipien zur Theorie hinzunimmt und so zugleich die *physikalische Wirklichkeit* über den Grundbereich hinaus erweitert. Wir wollen das mit Blick auf die Quantentheorie die *Standardinterpretation* (standard interpretation) nennen. Auch diese Bezeichnungen werden in der Literatur unterschiedlich verwendet.

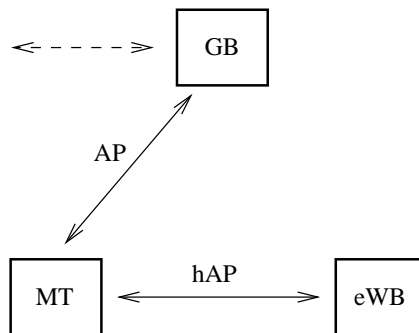


Abbildung 2.5: Die Abbildungsprinzipien AP beziehen den mathematischen Teil MT einer physikalischen Theorie und den Grundbereich GB der physikalischen Wirklichkeit aufeinander. Hypothetische Abbildungsprinzipien hAP verknüpfen mit einem erschlossenen Wirklichkeitsbereich eWB.

Es sollte aber deutlich geworden sein, dass die Festlegung eines erschlossenen Wirklichkeitsbereichs ein Element der Willkür enthält und dass mit ihm die Wirklichkeit zumindest in Teilen theorieabhängig wird. Noch aus einem anderen Grund entsteht die physikalische Welt mit Hilfe der Theorie. *Alternativtheorien*, die die gleichen Erfahrungen in anderer Weise begründen, können in diesem Sinne verschiedene Wirklichkeiten haben. Beispiele dafür sind eine speziell-relativistische Gravitationstheorie in der flachen Raum-Zeit, die mit dem Konzept des Gravitationsfeldes arbeitet und die Allgemeine Relativitätstheorie, in der das Gravitationsfeld völlig eliminiert und die Raum-Zeit gekrümmt ist. Die jeweilige Standardinterpretation beantwortet die Frage nach der Existenz eines Gravitationsfeldes unterschiedlich.

Die Elektrodynamik zeigt allerdings weiterhin, dass auch in der Standardinterpretation keineswegs zu allen Größen der mathematischen Theorie eine Entsprechung in der Wirklichkeit behauptet wird. So wird üblicherweise dem eichabhängigen Vektorpotential an einem Ort keine Realität zugesprochen. Vektorpotentiale werden nur als rechnerische Hilfsmittel aufgefasst. In der Coulomb-Eichung ändert sich das Vektorpotential instantan. Es wird damit aber kein realer Ausbreitungsvorgang mit Überlichtgeschwindigkeit verbunden.

2.5 Interpretationen der Quantentheorie und physikalische Wirklichkeit*

2.5.1 Minimalinterpretation*

Wie fügt sich die Quantentheorie in das im vorigen Kapitel beschriebene Schema ein? Die Minimalinterpretation der Quantentheorie schreibt nur den Präparations-, Transformations- und Messgeräten Realität zu. Es gibt nur deren Wirklichkeit und darüber hinaus keine hypothetischen Abbildungsprinzipien hAP und keine erschlossene Wirklichkeit eWB. Die Abbildung AP erfolgt in die klassisch beschreibbare Realität (z. B. Zeigerausschläge der Messgeräte). Das empirische Wissen in der Quantentheorie kann mit den Elementen der klassischen Physik formuliert werden. Alle anderen Bestandteile des mathematischen Teils MT der Quantentheorie sind nur rechnerische Hilfsmittel. Diese Einstellung lässt sich gut mit der zugespitzten Formulierung von Niels Bohr charakterisieren: „*There is no quantum world.*“⁶. Elektronen, Atome usw. gibt es nicht. Man wird diese Einstellung wissenschaftstheoretisch als *instrumentalistisch* und *pragmatisch* charakterisieren. Der Vorteil der Beschränkung auf die Minimalinterpretation liegt in der Vermeidung von scheinbaren Paradoxien. Das ist erkaufte um den Preis, dass keine Veranschaulichung und kaum physikalische Intuition angeregt wird.

Die einzige Aufgabe der Quantentheorie in dieser Interpretation ist es, präzise Vorhersagen über mögliche Ergebnisse von Messungen und die Wahrscheinlichkeiten ihres Eintretens zu machen. Weitere Aussagen sind überflüssig und werden nicht gemacht. Objektivität ist garantiert. Nach Abschluss der Messung kann ein Beobachter ein Messergebnis nur ablesen aber nicht mehr beeinflussen. Es ist Teil der klassischen Welt. Die so gewonnenen empirischen Aussagen (z. B. über Zeigerausschläge) lassen sich im Rahmen der klassischen Physik als der zugehörigen Vortheorie beschreiben. Sie können aber nicht im Rahmen der klassischen Physik erklärt, bzw. theoretisch begründet werden. Man braucht dazu den mathematischen Teil MT der Quantentheorie und einige wenige Abbildungsprinzipien. Es gibt in der Literatur keine einheitlichen Festlegungen darüber, was man unter der *Kopenhagener Interpretation* verstehen soll. Die Minimalinterpretation gibt aber sicher charakteristische Züge dieser Interpretation wieder.

2.5.2 Standardinterpretation*

Die unter Physikern allseits akzeptierte Standardinterpretation geht darüber hinaus. Man stellt fest, dass zu einzelnen Quantensystemen Eigenschaften gehören, die abtrennbar sind von Präparation und Registration, die also nicht Relationen zwischen dem System und dem Präparations- und Registrationsgeräten beschreiben. Die zugehörigen physikalischen Größen sind elektrische Ladung, Baryonenladung, Masse und Betrag des Spins eines Elementarteil-

⁶ „There is no quantum world. There is only an abstract quantum physical description. It is wrong to think, that the task of physics is to find out how nature is. Physics concerns with what we can say about nature.“ Nach [Pet 63, S. 12].

chens. Sie heißen auch *klassische Observable*⁷. Da sie sich zum Teil auf die Vortheorien zur Quantentheorie beziehen, ist es sinnvoll, auch diesen Eigenschaften eine objektive Realität zuzusprechen und damit zugleich auch dem zugehörigen Quantensystem. *Quantensysteme haben dann reale Träger in einer erschlossenen Wirklichkeit, die man Quantenobjekte (quantum objects) nennen kann.* Man kann von einzelnen Quantenobjekten wie Atomen, Elektronen usw. sprechen und verbindet damit in der Standardinterpretation folgende Vorstellung: Die makroskopischen Effekte der Messgeräte werden klassisch beschrieben, z. B. in der Form von Zeigerausschlägen. Sie stellen in dieser Interpretation gewissermaßen nur die „Oberfläche“ dar und lassen sich auf die Wirkungen real vorhandener Quantensysteme bzw. Quantenobjekte zurückfahren. *Es gibt eine Quantenwelt.* Es gibt keine physikalische Theorie ohne Interpretation. *Die Postulate spiegeln in ihrer Formulierung in Abschn. 2.1.2 bereits die Abbildungsprinzipien der Standardinterpretation wider.*

Wiederum wird aber nicht von allen Termen des mathematischen Teils MT behauptet, dass sie in Elemente der Wirklichkeit abgebildet werden können. *Anders als beim elektrischen Feld gibt es in der Quantentheorie für den durch ein Präparationsverfahren festgelegten Zustandsvektor (bzw. Dichteoperator) keine Entsprechung in der Wirklichkeit.* Er erlaubt nur im Zusammenwirken mit den Messoperatoren, die Berechnung von Wahrscheinlichkeitsverteilungen. Er ähnelt damit in seinem Status dem Vektorpotential in der Elektrodynamik. Was sich unter dem Einfluss eines Transformationsapparates deterministisch entwickelt, sind die vorhersagbaren Wahrscheinlichkeitsverteilungen von Messresultaten. Der Zeitentwicklungsoperator $U(t, t_0)$ repräsentiert diese Entwicklung.

Auch wenn das im Folgenden nicht immer explizit durchgeführt wird, kann es für das Verständnis nützlich sein sich klar zu machen, ob eine Aussage sich auf die volle Standardinterpretation bezieht oder mit weniger Interpretation auskommt.

Weitere Interpretationen Die Viele-Welten-Interpretation der Quantentheorie ist ein Beispiel für eine alternative Interpretation, die unter Beibehaltung des mathematischen Teils andere Aussagen über die Wirklichkeit macht. Wir werden sie in Abschn. 15.5 kurz besprechen.

2.6 Ergänzende Themen und weiterführende Literatur

- Wissenschaftstheorie: [Sch 64], [Mai 96], [Mit 96], [Bal 70], [Hom 97], [Bub 97], [Mai 96], [Stö 86], [Lal 01], [DG 71], [Esf 02a], [Mut 98].
- Zeno-Effekt: [NPN 97, S. 172], [Hom 97, Kap. 6].
- Hinweise auf Experimente zum Zeno-Effekt: [IHB 90], Literatur zur Diskussion über dieses Experiment und Vorschläge weiterer Experimente in [NPN 97, S. 177].
- Theoretische Terme und Abbildungsprinzipien: [Sch 90], [Sch 88].
- Interpretation der Quantentheorie: [FP 00], [Lud 55], [Lud 89] [Lud 90], [Omn 94], [Lud 96].

⁷Die Zustände von Quantenobjekten, die sich in diesen Eigenschaften unterscheiden, können nicht superponiert werden. Linearkombinationen solcher Zustände sind physikalisch nicht realisiert (*Superauswahlregeln*).

This Page Intentionally Left Blank

3 Die einfachsten Quantensysteme: Qubits

Alle Quantensysteme, die nicht mehr als zwei linear unabhängige Zustände besitzen, werden in einem zweidimensionalen Hilbert-Raum \mathcal{H}_2 beschrieben. Sie sind die einfachsten nicht trivialen Quantensysteme. Quantenzustände im \mathcal{H}_2 heißen mit Blick auf ihre spätere Rolle in der Quanteninformatiktheorie *Qubits*. Sie sind von der Form

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle, \quad |c_0|^2 + |c_1|^2 = 1 \quad (3.1)$$

mit der ONB $\{|0\rangle, |1\rangle\}$, die auch *Rechenbasis* oder *Standardbasis* genannt wird. Observablen besitzen zwei Messwerte.

Wichtige physikalische Realisierungen von *Qubit-Systemen* sind:

- 2-Niveau-Atom (auch Atome mit mehr Niveaus, wenn nur zwei Niveaus in einem Prozess eine Rolle spielen), Ionen mit zwei Energieniveaus
- Polarisation von Spin- $\frac{1}{2}$ -Teilchen
- Polarisation einzelner Photonen (horizontal \leftrightarrow vertikal oder linksdrehend \leftrightarrow rechtsdrehend)
- Strahlengänge in einem Zwei-Wege-Interferometer, in dem sich genau ein Photon befindet.
- Quantenpunkte
- Moden des elektromagnetischen Feldes in einer Kavität

Es gibt weitere Qubit-Systeme. Auch der Doppelspalt und das Stern-Gerlach-Experiment lassen sich vereinfacht so beschreiben.

Wir haben in Abschn. 1.2.1 die Operatorbasis der Übergangsoperatoren kennen gelernt. Für Rechnungen im \mathcal{H}_2 ist die Operatorbasis, die aus dem Einsoperator $\mathbb{1}$ und den σ -Operatoren (*Pauli-Operatoren*) besteht, ein wichtiges Hilfsmittel. Pauli-Operatoren werden üblicherweise im Zusammenhang mit dem Spin als innerem Drehimpuls eingeführt. Da sie aber bei anderen Qubit-Systemen im Allgemeinen physikalisch nicht mit einem Drehimpuls zusammenhängen, können wir von dieser Bedeutung zunächst absehen. Wir führen Pauli-Operatoren in Abschn. 3.1 ein und beschreiben in Abschn. 3.2 und Abschn. 3.3 eine sehr häufig verwendete Veranschaulichung von Quantenzuständen im \mathcal{H}_2 und ihrer Dynamik mit Hilfe der Bloch-Kugel.

Qubit-Systeme sind die Träger einer Einheit der Quanteninformation. Die Verarbeitung von Quanteninformation wird wie die Verarbeitung von klassischer Information mit Hilfe von

elementaren Operationen beschrieben, den sogenannten logischen Schaltungen oder *Gattern* (gates). *Quantengatter* (quantum gates) sind unitäre Transformationen oder Messungen auf dem \mathcal{H}_2 . Wir beschreiben unitäre Gatter, die auf nur einem Qubit wirken, in Abschn. 3.4.

Realisierungen von Qubit-Systemen und Quantengattern werden in Abschn. 3.5 bis 3.7 vorgestellt.

3.1 Pauli-Operatoren

Operatorbasis Wir führen im \mathcal{H}_2 drei hermitesche Operatoren σ_k mit $k = 1, 2, 3$ oder $k = x, y, z$ ein

$$\sigma_k^\dagger = \sigma_k, \quad (3.2)$$

für die wir

$$\sigma_k^2 = \mathbb{1} \quad (3.3)$$

fordern. Da $\sigma_k \neq \mathbb{1}$ sein soll und die Eigenwerte reell sind, folgt daraus und aus der Hermitezität, dass jeder Operator σ_k die Eigenwerte $(+1)$ und (-1) besitzt. Wie die Spektralzerlegung zeigt, sind die σ_k damit zugleich unitär

$$\sigma_k^\dagger = \sigma_k^{-1}. \quad (3.4)$$

und spurfrei

$$\text{tr}[\sigma_k] = 0. \quad (3.5)$$

Die Abb. 1.2 verdeutlicht, wie speziell die σ -Operatoren sind. Abbildung 1.2 zeigt auch, dass man die Forderungen Hermitezität, Unitarität und $\sigma \neq \mathbb{1}$ an die Spitze stellen könnte. Die Eigenwerte $+1$ und -1 sowie die Gl. (3.3) und (3.5) wären dann die Folge.

Wir wollen die σ_k durch eine Forderung, die sie untereinander verknüpft, zu einer Operatorbasis ausbauen (vergl. Abschn. 1.2.1). Das wird erreicht, wenn wir in Ergänzung zu Gl. (3.2) und (3.3) noch die Bedingung

$$\text{tr}[\sigma_i \sigma_j] = 2\delta_{ij} \quad (3.6)$$

erfüllen, indem wir vom Antikommutator $([A, B]_+ := AB + BA)$

$$[\sigma_i, \sigma_j]_+ = 2\delta_{ij}\mathbb{1} \quad (3.7)$$

verlangen. Die Operatoren $\{\frac{1}{\sqrt{2}}\mathbb{1}, \frac{1}{\sqrt{2}}\sigma_k\}$ bilden dann eine orthonormale Operatorbasis im Liouville-Raum. Jeder Operator A lässt sich in der Form

$$A = \frac{1}{2}\text{tr}[A]\mathbb{1} + \frac{1}{2}\sum_{k=1}^3 \text{tr}[A\sigma_k]\sigma_k \quad (3.8)$$

darstellen.

Drehimpulsoperatoren Die zweite wichtige Eigenschaft der σ_k ergibt sich durch die folgende Festlegung des Kommutators $([A, B]_- := AB - BA)$ durch die die Gl. (3.7) ergänzt wird:

$$[\sigma_i, \sigma_j]_- = 2i \sum_{k=1}^3 \epsilon_{ijk} \sigma_k. \quad (3.9)$$

ϵ_{ijk} ist der in allen Indizes total antisymmetrische Tensor mit $\epsilon_{123} = 1$. Hierdurch werden die σ_k formal proportional zu Drehimpulsoperatoren und können Observable des 2-Niveau-Systems *Spin* beschreiben. Zusammenfassend schreiben wir für Gl. (3.7) und (3.9)

$$\sigma_i \sigma_j = \delta_{ij} \mathbb{1} + i \sum_{k=1}^3 \epsilon_{ijk} \sigma_k. \quad (3.10)$$

Die hermiteschen Operatoren σ_k , die Gl. (3.10) erfüllen, heißen *Pauli-Operatoren* (Pauli operators) oder σ -Operatoren. Die Gleichungen zeigen, dass die Indizes völlig gleichberechtigt eingehen. Dies lässt sich in manchen Rechnungen ausnutzen.

Als Grundlage einer indexfreien Formulierung führen wir den vektoriellen Pauli-Operator $\boldsymbol{\sigma} := \sigma_x \mathbf{e}_x + \sigma_y \mathbf{e}_y + \sigma_z \mathbf{e}_z$ ein. Die Vektoren $\mathbf{e}_x, \mathbf{e}_y$ und \mathbf{e}_z sind dabei die kartesischen Basisvektoren des \mathbb{R}^3 . Mit Hilfe von Gl. (3.10) lässt sich für beliebige Vektoren $\mathbf{a}, \mathbf{b} \in \mathbb{R}^3$

$$(\boldsymbol{\sigma} \mathbf{a})(\boldsymbol{\sigma} \mathbf{b}) = (\mathbf{a} \mathbf{b}) \mathbb{1} + i \boldsymbol{\sigma} (\mathbf{a} \times \mathbf{b}) \quad (3.11)$$

ableiten. Diese Gleichung geht für beliebige normierte Vektoren \mathbf{e} in

$$(\boldsymbol{\sigma} \mathbf{e})(\boldsymbol{\sigma} \mathbf{e}) = \mathbb{1} \quad (3.12)$$

über. Damit erhalten wir mit Hilfe der Spektralzerlegung für die Entwicklung der Exponentialfunktion

$$\exp(i\theta \mathbf{e} \boldsymbol{\sigma}) = \mathbb{1} + i\theta \mathbf{e} \boldsymbol{\sigma} - \frac{1}{2} \theta^2 \underbrace{(\mathbf{e} \boldsymbol{\sigma})^2}_{=1} + \frac{i}{3!} \theta^3 \mathbf{e} \boldsymbol{\sigma} \pm \dots \quad (3.13)$$

und nach geeigneter Zusammenfassung die häufig benutzte Relation

$$\exp(i\theta \mathbf{e} \boldsymbol{\sigma}) = (\cos \theta) \mathbb{1} + i(\sin \theta) \mathbf{e} \boldsymbol{\sigma}. \quad (3.14)$$

Matrixdarstellung Wenn wir die ONB der Eigenvektoren $|0\rangle$ und $|1\rangle$ von σ_z mit den Eigenwerten $(+1)$ bzw. (-1)

$$\begin{aligned} \sigma_z |0\rangle &= +|0\rangle \\ \sigma_z |1\rangle &= -|1\rangle \end{aligned} \quad (3.15)$$

als Rechenbasis nehmen, dann ist die Matrixdarstellung von σ_z

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (3.16)$$

Mit Hilfe der Gl. (3.2) und (3.10) können die Matrixdarstellungen von σ_x und σ_y in der Rechenbasis im Einzelnen berechnet werden. Hier soll nur das Ergebnis angegeben werden. Wir bezeichnen diese *Pauli-Matrizen* ebenfalls mit dem gleichen Symbol wie den Operator und fügen die dyadische Darstellung direkt an:

$$\begin{aligned}\sigma_x &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0| \\ \sigma_y &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = -i(|0\rangle\langle 1| - |1\rangle\langle 0|) \\ \sigma_z &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|.\end{aligned}\tag{3.17}$$

Es ist nützlich, die Wirkung der σ -Operatoren auf die Vektoren der Rechenbasis zu notieren:

$$\begin{aligned}\sigma_x|0\rangle &= |1\rangle & \sigma_x \text{ vertauscht (bit flip)} \\ \sigma_x|1\rangle &= |0\rangle \\ \sigma_y|0\rangle &= i|1\rangle & \sigma_y \text{ vertauscht und fügt die relative Phase } \pm i \text{ ein} \\ \sigma_y|1\rangle &= -i|0\rangle \\ \sigma_z|0\rangle &= +|0\rangle & \sigma_z \text{ fügt die relative Phase } \pm 1 \text{ ein (phase flip).} \\ \sigma_z|1\rangle &= -|1\rangle.\end{aligned}\tag{3.18}$$

Damit lassen sich schließlich in der Rechenbasis die orthonormalen Eigenzustände von σ_x und σ_y direkt als

$$\begin{aligned}\sigma_x|0_x\rangle &= |0_x\rangle & \sigma_x|1_x\rangle &= -|1_x\rangle \\ |0_x\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) & |1_x\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\end{aligned}\tag{3.19}$$

und

$$\begin{aligned}\sigma_y|0_y\rangle &= |0_y\rangle & \sigma_y|1_y\rangle &= -|1_y\rangle \\ |0_y\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) & |1_y\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\end{aligned}\tag{3.20}$$

bestätigen.

3.2 Veranschaulichung von Qubits auf der Bloch-Kugel

Wir führen eine auf der Zerlegung nach der Operatorbasis beruhende mathematische Vorüberlegung durch, auf die wir uns später häufiger beziehen werden. Ein Operator ρ mit den

Eigenschaften $\rho^\dagger = \rho$ und $\text{tr}[\rho] = 1$ lässt sich mit Gl. (3.8) in der Form

$$\rho = \frac{1}{2}(\mathbb{1} + \mathbf{r}\boldsymbol{\sigma}) \quad (3.21)$$

mit reellem Vektor \mathbf{r}

$$\mathbf{r} := \text{tr}[\rho\boldsymbol{\sigma}] \quad (3.22)$$

schreiben. Mit Gl. (3.5) und (3.10) gewinnen wir daraus

$$\begin{aligned} \text{tr}[\rho^2] &= \frac{1}{4}\text{tr}[\mathbb{1} + 2\mathbf{r}\boldsymbol{\sigma} + \sum_{i,j} r_i r_j \sigma_i \sigma_j] \\ &= \frac{1}{2}(1 + |\mathbf{r}|^2). \end{aligned} \quad (3.23)$$

Wir betrachten als Spezialfall den mit einem beliebigen normierten Vektor $|\psi\rangle$ gebildeten Operator $\rho := |\psi\rangle\langle\psi|$. Für ihn gilt $\rho^2 = \rho$ sowie $\text{tr}[\rho^2] = \text{tr}[\rho] = 1$ und mit (3.23) folgt $|\mathbf{r}| = 1$. Einsetzen von ρ in (3.22) liefert als Interpretation von \mathbf{r} den Erwartungswert

$$\mathbf{r} = \langle\psi|\boldsymbol{\sigma}|\psi\rangle, \quad (3.24)$$

sowie $\langle\psi|\mathbf{r}\boldsymbol{\sigma}|\psi\rangle = \mathbf{r}\mathbf{r} = 1$ und damit als weiteres Resultat

$$\mathbf{r}\boldsymbol{\sigma}|\psi\rangle = |\psi\rangle. \quad (3.25)$$

Wir haben zwei Ergebnisse gefunden: Für einen beliebigen normierten Zustandsvektor $|\psi\rangle \in \mathcal{H}_2$ ist der Erwartungswert des vektoriellen Pauli-Operators $\boldsymbol{\sigma}$ ein reeller Vektor $\mathbf{r} \in \mathbb{R}^3$ vom Betrag 1. Zugleich ist $|\psi\rangle$ Eigenvektor des hiermit gebildeten Operators $\mathbf{r}\boldsymbol{\sigma}$ zum Eigenwert $(+1)$.

Bloch-Kugel Über den Erwartungswert von $\boldsymbol{\sigma}$ ist gemäß Gl. (3.24) jedem Qubit $|\psi\rangle$ eindeutig ein Vektor \mathbf{r} im \mathbb{R}^3 zugeordnet, der *Bloch-Vektor* genannt wird. Seine Spitze liegt auf der Oberfläche der Einheitskugel (*Bloch-Kugel*) (vergl. Abschn. 3.1). Wir nennen den damit bezeichneten Punkt den *Bloch-Punkt*. Mit Hilfe von \mathbf{r} können wir Zustandsvektoren $|\psi\rangle$ sowie die Auswirkungen der Messdynamik und der unitären Dynamik auf $|\psi\rangle$ einfach dreidimensional veranschaulichen. Darin liegt die Bedeutung der Bloch-Vektoren.

$\mathbf{r}\boldsymbol{\sigma}$ ist hermitesch, \mathbf{r} ist normiert und Gl. (3.12) gilt entsprechend. Wir können daher die Argumentation vom Anfang des Kapitels übertragen: Die Eigenwerte der vektoriellen Pauli-Operatoren $\mathbf{r}\boldsymbol{\sigma}$ sind $(+1)$ und (-1) . Der Eigenvektor zu $(+1)$ ist $|\psi\rangle$ mit Bloch-Vektor \mathbf{r} von Gl. (3.24). Der zweite Eigenvektor zu $\mathbf{r}\boldsymbol{\sigma}$ steht auf $|\psi\rangle$ senkrecht ($\langle\chi|\psi\rangle = 0$) und erfüllt

$$\mathbf{r}\boldsymbol{\sigma}|\chi\rangle = -|\chi\rangle. \quad (3.26)$$

Multiplikation mit $\langle\chi|$ führt mit $|\langle\chi|\boldsymbol{\sigma}|\chi\rangle| = -1$ (vergl. Gl. (3.24)) auf

$$\langle\chi|\boldsymbol{\sigma}|\chi\rangle = -\mathbf{r}. \quad (3.27)$$

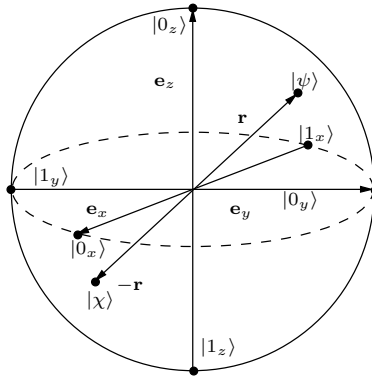


Abbildung 3.1: Bloch-Kugel mit den Bloch-Vektoren zu den Eigenzuständen der Pauli-Operatoren. Die Bloch-Vektoren \mathbf{r} und $-\mathbf{r}$ zu zwei beliebigen orthonormalen Qubits $|\psi\rangle$ und $|\chi\rangle$ liegen spiegelsymmetrisch zum Ursprung.

Der Bloch-Vektor zum Eigenwert (-1) entsteht durch Spiegelung von \mathbf{r} am Ursprung (vergl. Abschn. 3.1)

Allgemein gehören zu zwei orthogonalen Qubits am Ursprung gespiegelte Bloch-Vektoren. Der zugehörige vektorielle Pauli-Operator ergibt sich direkt über den Bloch-Vektor \mathbf{r} als $\mathbf{r}\sigma$. Speziell finden wir, dass die Bloch-Vektoren zu den Eigenzuständen der drei Pauli-Operatoren für die Eigenwerte $(+1)$ mit den Basisvektoren $\mathbf{e}_x, \mathbf{e}_y, \mathbf{e}_z$ übereinstimmen. Für die Eigenwerte (-1) liegen die Bloch-Vektoren in der jeweiligen Gegenrichtung. Dies ist in Abschn. 3.1 dargestellt. Wir wollten noch die Bloch-Punkte mit Hilfe von Polarkoordinaten durchparametrisieren. Ein beliebiges Qubit $|\psi\rangle$ (vergl. Gl. (3.1)) lässt sich stets mit Hilfe von 2 Parametern θ und φ in der Form

$$\begin{aligned} |\psi\rangle &= e^{-i\frac{\varphi}{2}} \cos\left(\frac{\theta}{2}\right) |0\rangle + e^{i\frac{\varphi}{2}} \sin\left(\frac{\theta}{2}\right) |1\rangle \\ &= e^{-i\frac{\varphi}{2}} \left\{ \cos\left(\frac{\theta}{2}\right) |0\rangle + e^{i\varphi} \sin\left(\frac{\theta}{2}\right) |1\rangle \right\} \end{aligned} \quad (3.28)$$

($0 \leq \varphi \leq 2\pi$, $0 \leq \theta \leq \pi$) darstellen. Mit Gl. (3.17) und (3.24) berechnen wir damit leicht für den zu $|\psi\rangle$ gehörigen Bloch-Vektor

$$\mathbf{r} = (\sin\theta \cos\varphi, \sin\theta \sin\varphi, \cos\theta). \quad (3.29)$$

Die Parameter θ und φ erhalten also bei der Veranschaulichung auf der Bloch-Kugel gerade die Bedeutung der Polarkoordinaten des Bloch-Punktes (Abb. 3.2). Charakteristisch ist das Auftreten der halben Polarwinkel beim zugehörigen Zustandsvektor von Gl. (3.28).

Das hat zur Folge, dass einerseits zu gegebenem Qubit $|\psi\rangle$ der Bloch-Vektor \mathbf{r} wohlbestimmt ist, dass aber andererseits ein Bloch-Vektor zwei verschiedenen Qubits zugeordnet ist. Wenn wir z. B. den Bloch-Vektor um die x -Achse in der y - z -Ebene drehen ($\varphi = \frac{\pi}{2}$), dann kehrt er nach einer 2π -Drehung ($\vartheta = 0 \rightarrow \vartheta = \pi \rightarrow \vartheta = 0$) wieder in seine Ausgangslage zurück. Gleichung (3.28) zeigt, dass dabei der zugehörige Zustandsvektor das Vorzeichen

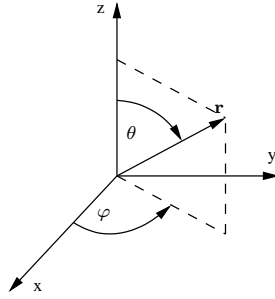


Abbildung 3.2: Polarkoordinaten veranschaulichen die Winkel θ und φ von Gl. 3.28.

wechselt $|\psi\rangle \rightarrow -|\psi\rangle$. Erst nach einer vollen 4π -Drehung des Blochvektors erreicht der Zustandsvektor wieder seine Ausgangsstellung $|\psi\rangle \rightarrow +|\psi\rangle$.

Es ist nützlich noch die Komponentendarstellungen des Operators $\mathbf{r}\sigma$ in der Rechenbasis zu notieren:

$$\mathbf{r}\sigma = \begin{pmatrix} \cos \theta & e^{-i\varphi} \sin \theta \\ e^{i\varphi} \sin \theta & -\cos \theta \end{pmatrix}. \quad (3.30)$$

Wir bezeichnen die Eigenvektoren von $\mathbf{r}\sigma$ mit $|0_{\mathbf{r}}\rangle$ und $|1_{\mathbf{r}}\rangle$. Der Eigenvektor $|0_{\mathbf{r}}\rangle = |\psi\rangle$ wurde schon in Gl. (3.28) angegeben. Wir ergänzen den Eigenvektor $|1_{\mathbf{r}}\rangle = |\chi\rangle$ zum Eigenwert -1 :

$$|0_{\mathbf{r}}\rangle = |\psi\rangle = \begin{pmatrix} e^{-i\varphi/2} \cos(\theta/2) \\ e^{i\varphi/2} \sin(\theta/2) \end{pmatrix}; \quad |1_{\mathbf{r}}\rangle = |\chi\rangle = \begin{pmatrix} -e^{-i\varphi/2} \sin(\theta/2) \\ e^{i\varphi/2} \cos(\theta/2) \end{pmatrix}. \quad (3.31)$$

3.3 Veranschaulichung der Messdynamik und der unitären Dynamik

Projektive Messung Wir haben in den Postulaten zwei Dynamiken eingeführt, die Messdynamik und die unitäre Dynamik. Die Messdynamik der projektiven Messung lässt sich einfach veranschaulichen. Ein Observablenoperator im zweidimensionalen Hilbert-Raum \mathcal{H}_2 der Qubits hat zwei orthogonale Eigenvektoren $|0\rangle$ und $|1\rangle$. Wir können sie immer als Eigenvektoren von σ_z auffassen. Auf der Bloch-Kugel legen wir hierzu die Richtung von \mathbf{e}_z in die Richtung des Bloch-Vektors von $|0\rangle$. Eine Messung dieser Observablen bewirkt dann einen sprunghaften Übergang von einem Ausgangszustand $|\psi\rangle$ in den Endzustand $|0\rangle$ oder $|1\rangle$ je nach Messergebnis (siehe Abb. 3.3).

Wenn wir $|\psi\rangle$ in der Form

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle \quad (3.32)$$

schreiben, dann sind die zugehörigen Wahrscheinlichkeiten $|c_0|^2$ bzw. $|c_1|^2$. Die Projektion r_z des Bloch-Vektors \mathbf{r} auf die z -Achse ist mit Gl. (3.29)

$$r_z = \cos \vartheta = \cos^2 \frac{\vartheta}{2} - \sin^2 \frac{\vartheta}{2} = |c_0|^2 - |c_1|^2. \quad (3.33)$$

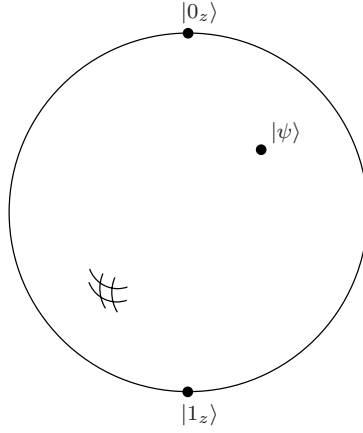


Abbildung 3.3: Bei einer Projektionsmessung eines Observablenoperators mit Eigenvektoren $|0_z\rangle$ und $|1_z\rangle$ wird der Zustandsvektor $|\psi\rangle$ sprunghaft je nach Messergebnis in $|0_z\rangle$ oder $|1_z\rangle$ überführt. Dargestellt sind die entsprechenden Bloch-Punkte auf der Bloch-Kugel.

Da $|c_0|^2 + |c_1|^2$ gilt, folgt daraus für die Wahrscheinlichkeit $|c_0|^2$

$$|c_0|^2 = \frac{r_z + 1}{2} . \quad (3.34)$$

Unitäre Transformation Wir wollen ergänzend die Wirkung der unitären Dynamik veranschaulichen, die mit einem unitären Operator U einen Ausgangszustand $|\psi\rangle$ gemäß

$$|\psi'\rangle = U|\psi\rangle \quad (3.35)$$

in den Endzustand $|\psi'\rangle$ überführt. Dazu gehen wir von einigen mathematischen Eigenschaften unitärer Transformationen und ihrer Matrixdarstellungen im \mathcal{H}_2 aus.

Sowohl die Zeilen als auch die Spalten einer unitären Matrix sind untereinander paarweise orthonormal ($\sum_j U_{ij}^* U_{kj} = \delta_{ik}$). Die Auswertung der entsprechenden Relationen, die wir hier nicht vorführen, zeigt, dass für eine unitäre Matrix U im \mathcal{H}_2 vier reelle Parameter α, β, γ und δ existieren, sodass U sich als Matrix

$$U = e^{i\kappa} \begin{pmatrix} e^{-i\lambda/2} \cos(\mu/2) e^{-i\nu/2} & -e^{-i\lambda/2} \sin(\mu/2) e^{i\nu/2} \\ e^{i\lambda/2} \sin(\mu/2) e^{-i\nu/2} & e^{i\lambda/2} \cos(\mu/2) e^{i\nu/2} \end{pmatrix} \quad (3.36)$$

oder als Operatorprodukt

$$U = \exp(i\kappa) \exp\left(-\frac{i}{2}\lambda\sigma_z\right) \exp\left(-\frac{i}{2}\mu\sigma_y\right) \exp\left(-\frac{i}{2}\nu\sigma_z\right) \quad (3.37)$$

schreiben lässt. Nur die Pauli-Operatoren σ_y und σ_z tauchen auf. Es ist geschickt noch den unitären Operator \hat{U} einzuführen

$$U =: e^{i\kappa} \hat{U}, \quad (3.38)$$

der mit U bis auf den globalen Phasenfaktor $e^{i\kappa}$ übereinstimmt. An Gl. (3.36) lesen wir direkt die folgenden Eigenschaften der Matrixdarstellung von \hat{U} ab:

$$\begin{aligned}\hat{U}_{00} &= \hat{U}_{11}^* \\ \hat{U}_{10} &= -\hat{U}_{01}^* \\ \hat{U}_{00}\hat{U}_{11} - \hat{U}_{01}\hat{U}_{10} &= 1 .\end{aligned}\tag{3.39}$$

Wir zerlegen \hat{U} nach der Operatorbasis $\{\frac{1}{\sqrt{2}}\mathbb{1}, \frac{1}{\sqrt{2}}\sigma_k\}$ gemäß Gl. (3.8)

$$\hat{U} = v_0\mathbb{1} - i\mathbf{v}\boldsymbol{\sigma} .\tag{3.40}$$

wobei v_0 und \mathbf{v} durch Spurbildungen bestimmt sind:

$$v_0 = \frac{1}{2}\text{tr}[\hat{U}] , \quad \mathbf{v} = \frac{i}{2}\text{tr}[\hat{U}\boldsymbol{\sigma}] .\tag{3.41}$$

Mit Hilfe der Relationen (3.39) lässt sich einfach zeigen, dass v_0 und \mathbf{v} reell sind. Die Unitaritätsrelation $\hat{U}^\dagger\hat{U} = \mathbb{1}$ ist mit Gl. (3.11) gleichbedeutend mit der Bedingung

$$v_0^2 + \mathbf{v}\mathbf{v} = 1 .\tag{3.42}$$

Sie bestätigt noch einmal, dass eine unitäre 2×2 -Matrix durch eine globale Phase und drei reelle Parameter bestimmt ist.

Da die Bedingung (3.42) erfüllt ist, hat die Gl. (3.40) die Struktur der Gl. (3.14). Für spätere Zwecke gehen wir wieder zum halben Winkel über und führen den Winkel ϕ und den Einheitsvektor \mathbf{e} gemäß

$$v_0 := \cos \frac{\phi}{2} , \quad \mathbf{v} = \left(\sin \frac{\phi}{2} \right) \mathbf{e}\tag{3.43}$$

ein. Zu gegebenem \hat{U} sind dabei ϕ und \mathbf{e} durch Gl. 3.41 festgelegt. Damit erhält die Gl. (3.40) die Gestalt

$$\hat{U} = \exp \left(-i\frac{\phi}{2}\mathbf{e}\boldsymbol{\sigma} \right) ,\tag{3.44}$$

wobei \mathbf{e} und ϕ durch die Gl. (3.41) und (3.43) gegeben sind. *Jede unitäre Transformation im \mathcal{H}_2 lässt sich bis auf einen Phasenfaktor $e^{i\alpha}$ eindeutig in die Form (3.44) bringen.*

Schließlich wollen wir die Wirkung von U auf der Bloch-Kugel veranschaulichen. Der Phasenfaktor $e^{i\alpha}$ hat keinen Einfluss auf den Bloch-Vektor. Wegen der Symmetrie der Darstellung können wir ohne Einschränkung \mathbf{e}_z in die Richtung von \mathbf{e} legen. Der Operator \hat{U} nimmt dann mit Gl. (3.44) die Form

$$\hat{U} = e^{-i\frac{\phi}{2}}|0\rangle\langle 0| - e^{+i\frac{\phi}{2}}|1\rangle\langle 1|\tag{3.45}$$

an (vergl. Gl. (1.52)). Mit Hilfe von Gl. (3.28) lesen wir direkt ab, dass $\hat{U}|\psi\rangle$ aus $|\psi\rangle$ durch die Substitution $\varphi \rightarrow \varphi + \phi$ hervorgeht. Daraus folgt eine einfache Interpretation der Wirkung von U auf der Bloch-Kugel: Wenn der Zustand $|\psi\rangle$ durch den Bloch-Vektor \mathbf{r} repräsentiert wird, dann entsteht der Bloch-Vektor \mathbf{r}' zum unitären transformierten Vektor

$$|\psi'\rangle = R_{\mathbf{e}}(\phi)|\psi\rangle, \quad R_{\mathbf{e}}(\phi) = \exp\left(-i\frac{\phi}{2}\mathbf{e}\sigma\right) \quad (3.46)$$

durch Rotation von \mathbf{r} um den Drehwinkel ϕ auf einem Kegel um die Achse \mathbf{e} (vergl. Abb. (3.4)). Die Größen \mathbf{e} und ϕ sind dabei über die Gl. (3.41) und (3.43) festgelegt. Die unitäre Transformation $\exp(-i\frac{\phi}{2}\sigma_z)$ (bzw. $\exp(-i\frac{\phi}{2}\sigma_x)$ oder $\exp(-i\frac{\phi}{2}\sigma_y)$) entspricht einer Drehung des Bloch-Vektors um die z -Achse (bzw. x -Achse oder y -Achse) um den Winkel ϕ .

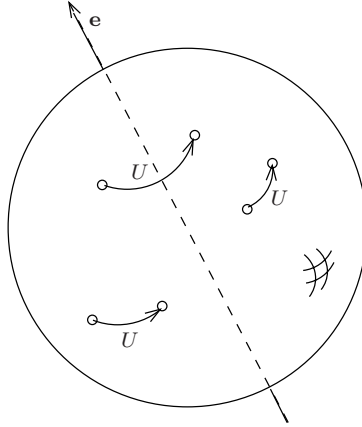


Abbildung 3.4: Wirkung der unitären Transformation U auf die Endpunkte der Bloch-Vektoren reiner Zustände. Der Vektor \mathbf{e} ist durch die Gl. (3.41) und (3.43) gegeben.

Beispiel: Rabi-Oszillationen Wir wollen eine physikalische Situation beschreiben, in der sich der Bloch-Vektor periodisch bewegt. In einer Kavität wechselwirkt ein einzelnes Photon mit einem einzelnen 2-Niveau-Atom mit den Energie-Niveaus $|0\rangle$ und $|1\rangle$. Der Einfachheit halber soll Resonanz vorliegen. Das heißt, die Energiedifferenz der Niveaus stimmt mit der Photonenenergie überein. Dann wird das Photon periodisch absorbiert und emittiert. Die Wahrscheinlichkeit $|c_0|^2$ das Atom im angeregten Zustand $|0\rangle$ zu finden oszilliert. Die entsprechende Frequenz wird *Rabi-Frequenz* Ω_R genannt, ihre Höhe ist ein Maß für die Stärke der Wechselwirkung zwischen Atom und quantisiertem Strahlungsfeld. Die quantenelektrodynamische Rechnung zeigt, dass der resultierende Einfluss auf den Zustandsvektor des Atoms durch die unitäre Transformation

$$U(t, t_0) = \exp\left[-i(t - t_0)\frac{\Omega_R}{2}\sigma_x\right] \quad (3.47)$$

beschrieben wird.

Wie wir gesehen haben, hat das zur Folge, dass sich der Bloch-Vektor \mathbf{r} mit der Frequenz Ω_R auf einem Kegel um die x -Achse dreht (vergl. Abb. 3.5). Im Grenzfall des völlig geöffneten Kegels dreht er sich in der y - z -Ebene. Die Wahrscheinlichkeit $|c_0|^2$ ergibt sich aus der Projektion $r_z(t) = r_z(t - \frac{2\pi}{\Omega_R})$ von \mathbf{r} auf die z -Achse gemäß

$$|c_0|^2 = \frac{r_z(t) + 1}{2}. \quad (3.48)$$

Der maximale Wert der Projektion $r_z(t)$ kann nur dann den maximal möglichen Wert 1 annehmen, wenn \mathbf{r} sich in der y - z -Ebene dreht. Hierzu reicht es, dass \mathbf{r} z. B. durch eine anfängliche Projektionsmessung parallel zu \mathbf{e}_z oder $-\mathbf{e}_z$ ausgerichtet wird. Dem entspricht der Zustand $|0\rangle$ oder $|1\rangle$. Im anderen Grenzfall wird das Atom im Eigenzustand $|0_x\rangle$ oder $|1_x\rangle$ von σ_x präpariert (vergl. Abb. 3.1). Dann stimmt der Bloch-Vektor mit \mathbf{e}_x bzw. $-\mathbf{e}_x$ überein und bleibt unter dem Einfluss der Wechselwirkung unverändert. Der Grund dafür ergibt sich aus der quantentheoretischen Rechnung. Der Hamilton-Operator des Gesamtsystems, der sich additiv aus den Hamilton-Operatoren für das freie Photon, das freie Atom und für die Wechselwirkung zusammensetzt, hat zwei Eigenzustände. Wenn sich das Gesamtsystem in einem dieser Zustände befindet, bleibt es in diesem Zustand. Die zugehörigen atomaren Zustände sind $|0_x\rangle$ und $|1_x\rangle$.

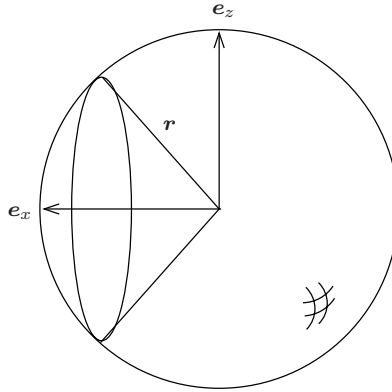


Abbildung 3.5: Rabi-Oszillationen des Bloch-Vektors \mathbf{r} .

3.4 Quantengatter für einzelne Qubit-Systeme

Wir wollen noch einmal die mathematisch und physikalisch besonders relevanten unitären Transformationen im \mathcal{H}_2 zusammenstellen. Wir haben im vorigen Kapitel gesehen, dass die Transformationen $\exp(i\phi\sigma_k)$ Drehungen des Bloch-Vektors um die Koordinatenachsen \mathbf{e}_k bewirken. Wesentlich ist, dass gemäß Gl. (3.37) jede beliebige unitäre Transformation durch mehrfache Anwendung dieser speziellen Transformationen gewonnen werden kann.

Phasengatter In der Quanteninformationstheorie spielen spezielle unitäre Operatoren eine besondere Rolle, die auch als *Quantengatter* (quantum gates) bezeichnet werden. Hierzu gehören die drei Pauli-Operatoren σ_k , deren Wirkung wir bereits beschrieben haben, und das *Phasengatter* (phase gate)

$$\phi(\alpha) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix} = |0\rangle\langle 0| + e^{i\alpha}|1\rangle\langle 1|, \quad (3.49)$$

das eine Phasenverschiebung der $|0\rangle$ -Komponente eines Vektors bewirkt (*Phasenschieber*). $\phi(\alpha)$ lässt sich auch in der Form

$$\phi(\alpha) = e^{i\frac{\alpha}{2}} e^{-i\frac{\alpha}{2}\sigma_z} \quad (3.50)$$

schreiben und stimmt daher bis auf einen globalen Phasenfaktor mit einer der einleitend erwähnten Drehungen überein.

Hadamard-Gatter Wir führen noch das unitäre und hermitesche *Hadamard-Gatter* H ein

$$H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z), \quad H^\dagger = H = H^{-1}, \quad (3.51)$$

das sich als Summe von Pauli-Operatoren schreiben lässt. H stimmt mit seinem Inversen überein und überführt die Vektoren der Rechenbasis in die Eigenvektoren von σ_x (vergl. Gl. (3.19)):

$$\begin{aligned} H|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ H|1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned} \quad (3.52)$$

Wir notieren noch die Beziehungen

$$H\sigma_x H = \sigma_z, \quad H\sigma_y H = -\sigma_y, \quad H\sigma_z H = \sigma_x, \quad (3.53)$$

die man z. B. durch Anwenden der Relation (3.7) erhält.

Um welche Achse \mathbf{e} und mit welchem Drehwinkel θ wird der Bloch-Vektor gedreht, wenn das Hadamard-Gatter auf einen Zustand wirkt? Wir verwenden die Ergebnisse aus Abschn. 3.4. Mit dem Phasenfaktor $e^{-i\kappa} = -i$ ergibt sich aus H ein unitärer Operator \hat{U} (vergl. Gl. (3.39)) mit der Wirkungsweise

$$\hat{U}|0\rangle = \frac{-i}{\sqrt{2}}(|0\rangle + |1\rangle), \quad \hat{U}|1\rangle = \frac{-i}{\sqrt{2}}(|0\rangle - |1\rangle). \quad (3.54)$$

Damit können wir mit Hilfe von Gl. (3.17) die Gl. (3.41) leicht auswerten mit dem Ergebnis: Das Hadamard-Gatter bewirkt eine Drehung mit dem Winkel


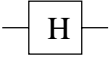
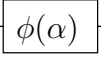
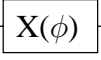
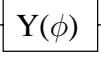
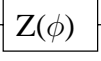
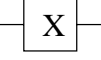
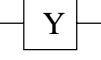
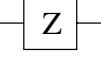
$$\theta = 180^\circ \quad (3.55)$$

um die Achse

$$\mathbf{e} = \frac{1}{\sqrt{2}}(e_x + e_z). \quad (3.56)$$

Weitere Gatter finden sich in Tab. (3.1).

Tabelle 3.1: Häufig benutzte Gatter für ein Qubit.

	Gatter	Operator- symbol	Operator	Matrix
NOT		NOT, σ_x	$ 0\rangle\langle 1 + 1\rangle\langle 0 $	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Hadamard		H	$\frac{1}{\sqrt{2}}(\sigma_x + \sigma_z)$ $= e^{-i\frac{\pi}{4}\sigma_y}\sigma_z$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
Phase		$\phi(\alpha)$	$ 0\rangle\langle 0 + e^{i\alpha} 1\rangle\langle 1 $	$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$
x-Rotation		$R_x(\phi)$	$e^{-i\frac{\phi}{2}\sigma_x}$	$\begin{pmatrix} \cos\frac{\phi}{2} & -i\sin\frac{\phi}{2} \\ -i\sin\frac{\phi}{2} & \cos\frac{\phi}{2} \end{pmatrix}$
y-Rotation		$R_y(\phi)$	$e^{-i\frac{\phi}{2}\sigma_y}$	$\begin{pmatrix} \cos\frac{\phi}{2} & -\sin\frac{\phi}{2} \\ \sin\frac{\phi}{2} & \cos\frac{\phi}{2} \end{pmatrix}$
z-Rotation		$R_z(\phi)$	$e^{-i\frac{\phi}{2}\sigma_z}$	$\begin{pmatrix} e^{-i\frac{\phi}{2}} & 0 \\ 0 & e^{i\frac{\phi}{2}} \end{pmatrix}$
σ_x -Operator		σ_x	σ_x	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
σ_y -Operator		σ_y	σ_y	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
σ_z -Operator		σ_z	σ_z	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

3.5 Spin- $\frac{1}{2}$

Eine besonders wichtige Realisierung eines *Qubit-Systems* ist der *Spin* mit der Quantenzahl $\frac{1}{2}$. Er ist ein innerer Freiheitsgrad von Elementarteilchen, wie z. B. den Elektronen, und wird in einem zweidimensionalen Hilbert-Raum \mathcal{H}_2 beschrieben (Spinraum). Die zugehörige Observable ist

$$\mathbf{S} = \frac{\hbar}{2} \boldsymbol{\sigma} . \quad (3.57)$$

Ihre Komponenten erfüllen gemäß Gl. (3.9) die Kommutatorrelationen für Drehimpulse

$$[S_i, S_j]_- = i\hbar\varepsilon_{ijk}S_k . \quad (3.58)$$

Mit dem Spin ist ein magnetisches Moment verbunden mit der Observablen

$$\mathbf{M} = \gamma \mathbf{S} . \quad (3.59)$$

Das gyromagnetische Verhältnis γ ist für Elektronen $\frac{e}{mc}$. In einem Magnetfeld \mathbf{B} führt die Wechselwirkung zwischen dem Magnetfeld und dem magnetischen Moment zu einem Hamilton-Operator

$$H = -\gamma \mathbf{B} \mathbf{S}. \quad (3.60)$$

Wir orientieren \mathbf{e}_z in Richtung von \mathbf{B} und führen $\omega := -\gamma B$ mit $B = |\mathbf{B}|$ ein. Dann hat der Hamilton-Operator die Form $H = \frac{\hbar\omega}{2}\sigma_z$ mit den beiden Eigenwerten $\pm \frac{\hbar\omega}{2}$ und den Eigenzuständen $|0_z\rangle$ und $|1_z\rangle$. Für ein Spin- $\frac{1}{2}$ -System kann die Observable σ_z bis auf einen Faktor je nach physikalischer Situation als Komponente des magnetischen Moments oder als Energie im Magnetfeld interpretiert werden (2-Niveau-System).

3.6 Photonenpolarisationen

Bei linearer Polarisation haben die elektrischen Wellenfelder die Form

$$E_H \sim \mathbf{e}_H \exp i(\mathbf{k}\mathbf{r} - \omega t); \quad E_V \sim \mathbf{e}_V \exp i(\mathbf{k}\mathbf{r} - \omega t); \quad (3.61)$$

mit dem Ausbreitungsvektor \mathbf{k} (siehe Abb. 3.6). Die Indizes H und V bezeichnen horizontale und vertikale Polarisation bzw. Schwingungsebene. Eine andere Basis ist

$$\mathbf{e}_{H'} = \mathbf{e}_{+45^\circ} = \frac{1}{\sqrt{2}}(\mathbf{e}_H + \mathbf{e}_V); \quad \mathbf{e}_{V'} = \mathbf{e}_{-45^\circ} = \frac{1}{\sqrt{2}}(\mathbf{e}_H - \mathbf{e}_V). \quad (3.62)$$

Sie entspricht einer Drehung der Schwingungsebenen um 45° . Die rechts- und linkszirkular polarisierten Wellen sind durch

$$E(R, L) \sim \mathbf{e}(R, L) \exp i(\mathbf{k}\mathbf{r} - \omega t) \quad (3.63)$$

mit

$$\mathbf{e}(R) = \frac{1}{\sqrt{2}}(\mathbf{e}_H + i\mathbf{e}_V); \quad \mathbf{e}(L) = \frac{1}{\sqrt{2}}(\mathbf{e}_H - i\mathbf{e}_V) \quad (3.64)$$

gegeben. Die diesen Polarisationen entsprechenden Zustandsvektoren des Quantensystems Photon sind Vektoren in einem Hilbert-Raum \mathcal{H}_2 und daher Qubits. Die Zuordnung lautet:

$$\mathbf{e}_H \leftrightarrow |H\rangle = |0\rangle, \quad \mathbf{e}_V \leftrightarrow |V\rangle = |1\rangle \quad (3.65)$$

$$\mathbf{e}_{H'} \leftrightarrow |H'\rangle = | + 45^\circ \rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) = |0_x\rangle$$

$$\mathbf{e}_{V'} \leftrightarrow |V'\rangle = | - 45^\circ \rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle) = |1_x\rangle \quad (3.66)$$

$$\mathbf{e}(R) \leftrightarrow |R\rangle = \frac{1}{\sqrt{2}}(|H\rangle + i|V\rangle) = |0_y\rangle$$

$$\mathbf{e}(L) \leftrightarrow |L\rangle = \frac{1}{\sqrt{2}}(|H\rangle - i|V\rangle) = |1_y\rangle \quad (3.67)$$

Den Zusammenhang zu den Eigenvektoren der Pauli-Operatoren haben wir für die drei Polarisationstypen angefügt.

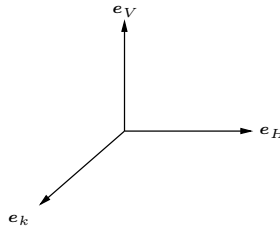


Abbildung 3.6: Polarisationsvektoren und Ausbreitungsvektor bei linear polarisierten Photonen

3.7 Einzelne Photonen im Strahlteiler und Interferometer

Wir wollen ein weiteres Qubit-System kennen lernen, das insbesondere für quantenoptische Experimente zur Quanteninformationstheorie von Bedeutung ist. Es handelt sich um ein einzelnes Photon auf das im Sinne von Abschn. 1.2 ein Transformationsapparat wirkt, der aus einer Abfolge von einzelnen Strahlteilern, Phasenschiebern und Spiegeln aufgebaut ist. Einfache Beispiele für ein solches photonisches Netzwerk zur Quanteninformationsverarbeitung sind Strahlteiler und Interferometer selber (vergl. Abb. 3.8).

Das Photon ist das Quant eines Strahlungsfeldes mit wohlbestimmten Modenfunktionen, die in diesem Falle durch den Wellenvektor charakterisiert sind. Die von uns betrachtete optische Anlage soll so einfach sein, dass nur zwei Lichtmoden oder Wege, ein 0-Weg und ein 1-Weg, durch sie hindurch gelegt werden können. Das Photon soll bei einer Messung vor, im Innern und hinter der Anlage immer nur auf genau einem der Wege registriert werden. Dann können wir das Photon in dieser Situation als Qubit beschreiben, wobei die Zustände $|0\rangle$ bzw. $|1\rangle$ den jeweiligen Wegen zugeordnet sind. Den normierten Photonenzustand beschreiben wir in der Form

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle. \quad (3.68)$$

mit $|c_0|^2 + |c_1|^2 = 1$. Wenn wir einen Detektor in den 0-Weg stellen (0-Detektor), dann spricht er mit der Wahrscheinlichkeit $|c_0|^2$ an. Entsprechendes gilt für den 1-Weg. Die verwendeten optischen Apparate haben zwei einlaufende und zwei auslaufende Wege und bewirken eine Abfolge unitärer Transformationen des Zustandsvektors $|\psi\rangle$. Sie ändern die Wahrscheinlichkeit das Photon auf einem bestimmten Weg zu registrieren, wobei die Gesamtwahrscheinlichkeit erhalten bleibt.

Phasenschieber haben wir schon beschrieben. Verlustfreie Spiegel bewirken allenfalls eine Phasenverschiebung. Strahlteiler werden wir im Anschluss beschreiben und danach die optischen Bauteile zu einem Interferometer zusammensetzen.

3.7.1 Strahlteiler

Strahlteiler allgemein Wir betrachten einen *verlustfreien Strahlteiler* (lossless beamsplitter) mit zwei einfallenden und zwei ausfallenden Strahlungsmoden wie er schematisch in

Abb. 3.7 dargestellt ist. Der einlaufende Photonenzustand $|\psi\rangle$ wie der auslaufende Photonenzustand $|\psi'\rangle$ sind von der Form (3.68). Die Zuordnung zu den Strahlungsmoden erfolgt gemäß Abb. 3.7.

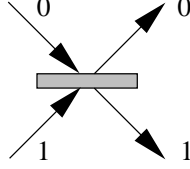


Abbildung 3.7: Wege beim Strahlteiler

Die Verlustfreiheit des Strahlteilers hat die Wahrscheinlichkeitserhaltung zur Folge. Mit einlaufendem Zustand $|\psi\rangle$ ist damit auch der auslaufende Zustand $|\psi'\rangle$ ein normierter Vektor und die Wirkung des Strahlteilers wird durch eine unitäre Transformation U wiedergegeben (vergl. Abschn. 1.1.5)

$$|\psi'\rangle = U|\psi\rangle. \quad (3.69)$$

Wir notieren U in der Form der Matrix (3.36) und führen neue Bezeichnungen für Amplituden und Phasen ein. ρ, τ und δ sind reell.

$$U = e^{i\kappa} \begin{pmatrix} \rho e^{i\delta_r} & -\tau e^{-i\delta_t} \\ \tau e^{i\delta_t} & \rho e^{-i\delta_r} \end{pmatrix}. \quad (3.70)$$

Die Wirkung von U lässt sich einfach beschreiben, wenn der einlaufende Photonenzustand nur aus einem Vektor der Rechenbasis besteht

$$|0\rangle \rightarrow U_{00}|0\rangle + U_{10}|1\rangle, \quad |1\rangle \rightarrow U_{01}|0\rangle + U_{11}|1\rangle. \quad (3.71)$$

Beim Einlaufen von $|0\rangle$ bewirkt der Strahlteiler in Reflexion eine Phasenverschiebung $\kappa + \delta_r$ und eine Multiplikation mit dem reellen *Reflexionsfaktor* ρ . Die Transmission ist entsprechend durch die Phasenverschiebung $\kappa + \delta_t$ und den *Transmissionsfaktor* τ bestimmt. Die Wirkung auf Superpositionen ist eine unmittelbare Folge.

Mit Gl. (3.36) erhalten wir als Ausdruck der Wahrscheinlichkeitserhaltung und damit der Unitarität

$$\rho^2 + \tau^2 = 1. \quad (3.72)$$

Wir führen noch die Phasendifferenz δ_0 zwischen reflektiertem und transmittiertem Zustand bei Einfall im Zustand $|0\rangle$ ein (δ_1 für den Zustand $|1\rangle$)

$$\delta_0 = \delta_r - \delta_t; \quad \delta_1 = -\delta_r + \delta_t \pm \pi. \quad (3.73)$$

Dann folgt aus Gl. (3.70) als eine stets erfüllte Beziehung

$$\delta_0 + \delta_1 = \pm \pi. \quad (3.74)$$

Spezielle Strahlteiler Zwei Typen von dielektrischen Strahlteilern werden in der Praxis häufig verwendet. Das ist einmal der Strahlteiler, der bei Reflexion eine Phasenverschiebung von $\frac{\pi}{2}$ und bei Transmission keine Phasenverschiebung bewirkt:

$$U_1 = \begin{pmatrix} i\rho & \tau \\ \tau & i\rho \end{pmatrix}. \quad (3.75)$$

Dem entspricht eine Festlegung $\delta_r = 0$, $\delta_t = -\frac{\pi}{2}$ und $\kappa = \frac{\pi}{2}$. Der Strahlteiler ist nicht zeitlich symmetrisch, da $U_1^{-1} \neq U_1$. Die räumlich symmetrische Version dieses Strahlteilers, bei der Reflexivität und Transmissivität übereinstimmen, ist durch $\rho = \tau = \frac{1}{\sqrt{2}}$ gegeben und bewirkt

$$U_1|0\rangle = \frac{1}{\sqrt{2}}(i|0\rangle + |1\rangle), \quad (3.76)$$

$$U_1|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle). \quad (3.77)$$

Für beide einfallenden Moden gilt, dass ein Photon mit der gleichen Wahrscheinlichkeit $\frac{1}{2}$ auf einer der auslaufenden Moden wieder ausläuft (50 : 50 beamsplitter). Wir schreiben Gl. (3.75) mit $\rho = \cos \theta$ und $\tau = \sin \theta$ um und erhalten die unitäre Transformation in der Form

$$U_1 = (\cos \theta)\mathbb{1} - i(\sin \theta)\sigma_x = \exp(-i\theta\sigma_x). \quad (3.78)$$

Ein globaler Phasenfaktor i ist weggelassen.

Der andere gebräuchliche Strahlteiler bewirkt einen Phasensprung um π bei der Reflexion an einer der Seiten:

$$U_2 = \begin{pmatrix} \rho & \tau \\ \tau & -\rho \end{pmatrix}. \quad (3.79)$$

Er entspricht der Wahl $\delta_r = \frac{\pi}{2}$, $\delta_t = \frac{\pi}{2}$ und $\kappa = -\frac{\pi}{2}$ und ist mit $U^{-1} = U$ zeitlich symmetrisch. Dafür ist er räumlich nicht symmetrisch, d. h. er wirkt unterschiedlich auf die in den Moden $|0\rangle$ bzw. $|1\rangle$ einlaufenden Photonen. Im symmetrischen Spezialfall $\rho = \tau = \frac{1}{\sqrt{2}}$ ergibt sich eine *optische Realisierung des Hadamard-Gatters* H von Gl. (3.51), dessen Wirkung in Gl. (3.52) beschrieben ist.

Wir schreiben $\rho = \cos \phi$ und $\tau = \sin \phi$ und bilden $\sigma_z U_2$. Explizites Ausrechnen der entsprechenden Matrizen zeigt dann mit Gl. (3.14)

$$\exp(i\phi\sigma_y) = \sigma_z U_2. \quad (3.80)$$

Da σ_z mit Phasenschiebern realisierbar ist, und Gl. (3.37) neben Phasenverschiebungen $\exp(-\frac{i}{2}\lambda\sigma_z)$ und $\exp(-\frac{i}{2}\nu\sigma_z)$ nur einen Operator der Form $\exp(i\mu\sigma_y)$ enthält, lässt sich jede unitäre Transformation (3.69) mit dem durch U_2 von Gl. (3.79) beschriebenen Strahlteiler (Hadamard-Gatter) und Phasenschiebern realisieren.

3.7.2 Interferometer

Ein *Mach-Zehnder-Interferometer* entsteht, wenn man zwischen zwei Hadamard-Strahlteilern einen Phasenschieber z. B. in den 1-Weg einbaut, durch den die $|1\rangle$ -Komponente des Photonzustands mit einem Phasenfaktor multipliziert wird (vergl. Abb. 3.8). Wir setzen den Phasenfaktor in der Form $\exp(-i\alpha)$ an. Die Strahlumlenkung durch zwei gleichartige ideale reflektierende Spiegel hat keinen Einfluss auf relative Phasen. Mit dem Phasengatter $\phi(\alpha)$ von

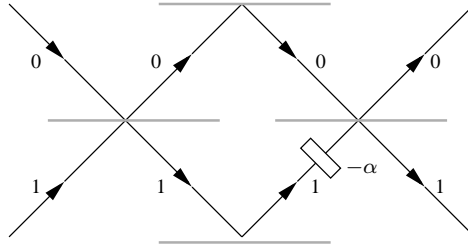


Abbildung 3.8: Mach-Zehnder Interferometer mit Phasenschieber

Gl. (3.49) können wir das Interferometer durch das Diagramm von Abb. 3.9 symbolisieren.

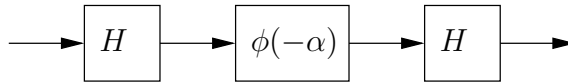


Abbildung 3.9: Schaltbild für das Mach-Zehnder-Interferometer.

Anweisungen für die Anwendung von *Gattern* (gates) in einer speziellen Reihenfolge heißen *Schaltungen* (circuits). Das Interferometer ist ein Beispiel eine einfache *Quantenschaltung* (quantum circuit).

Wenn ein Photon im Zustand $|0\rangle$ und damit in der 0-Mode einläuft, erfährt es nacheinander die Transformationen

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + e^{-i\alpha}|1\rangle) \rightarrow \frac{1}{2}[(1 + e^{-i\alpha})|0\rangle + (1 - e^{-i\alpha})|1\rangle] . \quad (3.81)$$

Die Wahrscheinlichkeit, dass danach ein Detektor das Photon im Zustand $|0\rangle$ detektiert (d. h., dass ein Detektor im 0-Ausgang anspricht) ist

$$p_0 = \frac{1}{2}(1 + \cos \alpha) . \quad (3.82)$$

Es entsteht in Abhängigkeit von der Phasenverschiebung α ein periodisch oszillierendes *Interferenzbild*.

Interferenzbild Gemäß Gl. (3.81) hat der erste Hadamard-Strahlteiler nur die Funktion einen einfachen in beiden Moden symmetrischen Zustandsvektor zu präparieren. Die Wahrscheinlichkeit, dass ein Detektor hinter dem Strahlteiler im 0-Weg oder im 1-Weg anspricht, ist dann jeweils $\frac{1}{2}$. Die Gl. (3.81) zeigt, dass die Wirkung des zweiten Strahlteilers darin besteht die komplexen Amplituden der $|0\rangle$ - und $|1\rangle$ -Komponenten des Zustandsvektors zur komplexen Amplitude des auslaufenden $|0\rangle$ -Vektors zu superponieren und so zur Interferenz zu bringen. Das Interferenzbild kann als Funktion von α von einem Detektor im 0-Weg hinter dem Interferometer registriert werden.

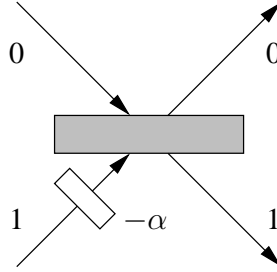


Abbildung 3.10: Strahlteiler mit Phasenschieber

Die *Interferenz* erzeugende Wirkung des zweiten Strahlteilers wollen wir für spätere Zwecke noch auf andere Weise beschreiben. Der in Phasenschieber und Strahlteiler der Anordnung von Abb. 3.10 einlaufende Zustand $|\psi^{\text{in}}\rangle$ wird durch die Wirkung von $\phi(\alpha)$ und H gemäß

$$|\psi^{\text{out}}\rangle = H(|0\rangle\langle 0| + e^{-i\alpha}|1\rangle\langle 1|)|\psi^{\text{in}}\rangle \quad (3.83)$$

in den auslaufenden Zustand $|\psi^{\text{out}}\rangle$ überführt. Die Wahrscheinlichkeit, das Photon im Zustand $|0\rangle$ zu finden ist

$$p_0(\alpha) = |\langle 0|\psi^{\text{out}}\rangle|^2. \quad (3.84)$$

Wir setzen $|\psi^{\text{out}}\rangle$ ein und lassen die Operatoren auf $|0\rangle$ wirken, dann folgt

$$p_0(\alpha) = |\langle \alpha|\psi^{\text{in}}\rangle|^2 \quad (3.85)$$

mit

$$|\alpha\rangle := (|0\rangle\langle 0| + e^{i\alpha}|1\rangle\langle 1|)H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\alpha}|1\rangle). \quad (3.86)$$

Die Messgröße $p(\alpha)$ lässt sich direkt als Mittelwert des Projektionsoperators $P_{|\alpha\rangle} := |\alpha\rangle\langle \alpha|$ im einlaufenden Zustand $|\psi^{\text{in}}\rangle$ schreiben:

$$p_0(\alpha) = \langle \psi^{\text{in}}|P_{|\alpha\rangle}|\psi^{\text{in}}\rangle. \quad (3.87)$$

Wählt man $|\alpha\rangle$ selber als einlaufenden Zustand, dann spricht wegen $p_0(\alpha) = 1$ nur der Detektor auf dem auslaufenden 0-Weg an. Gl. (3.87) kann man daher folgendermaßen

interpretieren: Die Wahrscheinlichkeit, dass der 0-Detektor anspricht, ist gleich der Wahrscheinlichkeit, dass der einlaufende Zustand $|\psi^{\text{in}}\rangle$ mit demjenigen Zustand $|\alpha\rangle$ übereinstimmt, der mit Sicherheit das Ansprechen des 0-Detektors bewirkt.

Für den allgemeinen einlaufenden Zustand,

$$|\psi^{\text{in}}\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\frac{\phi}{2}} \sin \frac{\theta}{2} |1\rangle, \quad (3.88)$$

der durch die Parameter θ und ϕ charakterisiert ist, lässt sich Gl. (3.85) leicht mit dem Ergebnis

$$p_0(\alpha) = \frac{1}{2} \left[1 + \sin \theta \cos \left(\alpha - \frac{\phi}{2} \right) \right] \quad (3.89)$$

auswerten. Bei Variation von α durch entsprechende Einstellung des Phasenschiebers entsteht ein periodisches Interferenzbild $p_0(\alpha)$ mit einem *Streifenkontrast*

$$\nu := \frac{p_{\max} - p_{\min}}{p_{\max} + p_{\min}} = \sin \theta. \quad (3.90)$$

Durch Ausmessen der Interferenzkurve können die Phasenverschiebung φ und der Streifenkontrast $\sin \theta$ ermittelt werden. *Damit haben wir ein interferometrisches Messverfahren zur Bestimmung des Zustands $|\psi^{\text{in}}\rangle$ gefunden.*

3.8 Ergänzende Themen und weiterführende Literatur

- Wechselwirkung zwischen Licht und einem 2-Niveau-Atom: [MW 95].
- Allgemeiner verlustfreier Strahlteiler: [CST 89], [MW 95]
- Systeme mit höherem Spin als $\frac{1}{2}$ werden im Hinblick auf ihre Rolle als Teilsysteme zusammengesetzter Quantensysteme ausführlich in [Zei 81], [PSM 87], [CST 89], [MW 95] untersucht.

3.9 Übungsaufgaben

ÜA 3.1 [zu 3.1 und 3.3] leiten Sie die Gl. (3.11), (3.17), (3.36), (3.37), (3.42), (3.53), (3.54) ab.

ÜA 3.2 [zu 3.1] Bestimmen Sie die Komponenten des Operators $\sigma_i \sigma_j$ in der Operatorbasis der σ -Operatoren.

ÜA 3.3 [zu 3.4] Berechnen Sie die Darstellungen der Operatoren in Tab. 3.1 soweit das nicht schon im Text geschehen ist.

ÜA 3.4 [zu 3.7.2] In ein Mach-Zehnder-Interferometer ist im 0-Strahlengang ein Phasenschieber mit der Wirkung $e^{i\alpha}$ und im 1-Strahlengang einer mit der Wirkung $e^{-i\alpha}$ eingebaut. Zeigen Sie, dass die resultierende Transformation von der Form

$$U = \begin{pmatrix} \cos \alpha & i \sin \alpha \\ i \sin \alpha & \cos \alpha \end{pmatrix} \quad (3.91)$$

ist. Durch Einbau zusätzlicher Phasenschieber in den ein- und auslaufenden Moden kann eine beliebige unitäre Transformation realisiert werden.

This Page Intentionally Left Blank

4 Gemischter Zustand und Dichteoperator

Wir haben schon im einleitenden Abschnitt 2.1.1 Gemische kennen gelernt und uns dann aber bei der Formulierung der Postulate auf reine Zustände beschränkt. Die reinen Zustände haben wir durch Vektoren im Hilbert-Raum beschrieben. Wir wollen nun zunächst eine andere Darstellung der reinen Zustände vorstellen, die direkt auf einen Zugang zur Beschreibung von statistischen Gemischen (Gemenge) und allgemeinen Gemischen mit Hilfe von Dichteoperatoren führt. Dichteoperatoren beschreiben den allgemeinen Quantenzustand. Die Postulate aus Abschn. 2.1.2 werden verallgemeinert.

4.1 Dichteoperator zu gegebenem Ensemble (statistisches Gemisch)

4.1.1 Reiner Zustand

Dem reinen Zustand, dem wir bisher den normierten Zustandsvektor $|\psi\rangle$ zugeordnet haben, können wir in eineindeutiger Weise den Operator

$$\rho := |\psi\rangle\langle\psi| \quad (4.1)$$

zuordnen. Er wird *Dichteoperator* (density operator) *eines reinen Zustands* und oft auch *Dichtematrix* genannt.

Die folgenden Eigenschaften von ρ lassen sich direkt ablesen:

- (i) ρ ist positiv: $\langle\varphi|\rho|\varphi\rangle \geq 0$, $\forall |\varphi\rangle \in \mathcal{H}_d$ (und damit hermitesch, $\rho^\dagger = \rho$)
- (ii) $\text{tr}\rho = 1$
- (iii) $\rho^2 = \rho$.

Eigenschaft (ii) ist eine Folge der Normiertheit von $|\psi\rangle$. Umgekehrt garantieren die drei Eigenschaften zusammen, dass die Spektralzerlegung von ρ die Form (4.1) hat und daher ρ eindeutig bis auf eine Phase einen Vektor $|\psi\rangle$ bestimmt. Mit Hilfe der Spektralzerlegung kann man auch zeigen, dass bei Gültigkeit von (i) und (ii) für einen Operator ρ die Eigenschaft (iii) gleichbedeutend ist mit

$$(\text{iii}^*) \text{tr}[\rho^2] = 1. \quad (4.2)$$

Eine Messung der Observablen A mit dem Messergebnis a_n und dem zugehörigen Projektionsoperator P_n von Gl. (2.3) überführt ρ gemäß Gl. (2.2) in den Dichteoperator ρ'_n

$$\rho \rightarrow \rho'_n = \frac{1}{p(a_n)} P_n \rho P_n . \quad (4.3)$$

Hierbei ist

$$p(a_n) = \text{tr}[P_n \rho] \quad (4.4)$$

entsprechend Gl. (2.5) die Wahrscheinlichkeit den Wert a_n als Messwert zu erhalten. Es kann günstig sein, den resultierenden Dichteoperator in der *unnormierten Form* $\tilde{\rho}'_n = |\tilde{\psi}'_n\rangle\langle\tilde{\psi}'_n|$ zu schreiben. In dieser Form muß die Spur nicht gleich Eins sein. Wie beim Zustandsvektor charakterisieren wir das durch eine Tilde:

$$\tilde{\rho}'_n = P_n \rho P_n . \quad (4.5)$$

Die Messwahrscheinlichkeit ist dann gleich der Spur des unnormierten resultierenden Dichteoperators nach der selektiven Messung.

$$p(a_n) = \text{tr}[\tilde{\rho}'_n] . \quad (4.6)$$

Den Erwartungswert $\langle A \rangle$ der Observablen A erhalten wir durch Einschieben des mit der ONB $\{|u_i\rangle\}$ gebildeten Identitätsoperators

$$\begin{aligned} \langle A \rangle &= \sum_{j,k=1}^d \langle \psi | u_j \rangle \langle u_j | A | u_k \rangle \langle u_k | \psi \rangle \\ &= \sum_{j,m} \langle u_k | \rho | u_j \rangle \langle u_j | A | u_k \rangle \\ &= \sum_k \langle u_k | \rho A | u_k \rangle \\ &= \text{tr}[\rho A] . \end{aligned} \quad (4.7)$$

Bleibt noch die Aufgabe, die unitäre Dynamik im Schrödinger-Bild für ρ umzuschreiben. Mit Gl. (2.14) finden wir

$$\rho(t) = U(t, t_0) \rho(t_0) U^{-1}(t, t_0) \quad (4.8)$$

und mit Gl. (2.9) ergibt sich die *von-Neumann-Gleichung*

$$\begin{aligned} i\hbar \dot{\rho}(t) &= i\hbar \dot{U}(t_0) U^{-1} + i\hbar U \rho(t_0) \dot{U}^{-1} \\ &= H U \rho(t_0) U^{-1} - U \rho(t_0) U^{-1} H \\ &= [H, \rho(t)] . \end{aligned} \quad (4.9)$$

Sie kann mit dem Liouville-Operator \mathcal{L} von Gl. (1.84) auch in der Form

$$i\hbar \dot{\rho} = \mathcal{L} \rho \quad (4.10)$$

geschrieben werden.

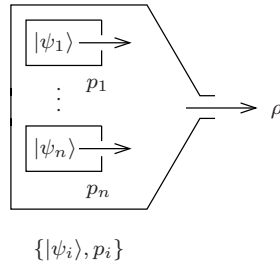


Abbildung 4.1: Das statistische Gemisch (Gemenge) zum Ensemble $\{|\psi_i\rangle, p_i\}$ entsteht indem immer einer der Präparationsapparate für $\{|\psi_i\rangle\}$ mit der Wahrscheinlichkeit p_i tätig wird.

Zusammenfassend stellen wir fest, dass die Physik abgeschlossener Quantensysteme in reinen Zuständen, die durch das mathematische Objekt Zustandsvektor $|\psi\rangle$ beschrieben wird, gleichwertig durch den Dichteoperator ρ von Gl. (4.1) beschrieben werden kann. In diesem Sinne kann man mit der gleichen operationalen Bedeutung wie bei $|\psi\rangle$ sagen: das System befindet sich im *Zustand* ρ . Im Gegensatz zur vektoriellen Formulierung können wir aber die Zustandsformulierung mit dem Dichteoperator unmittelbar auf eine allgemeinere Klasse von Quantenzuständen, die statistischen Gemische, übertragen. Wir beschreiben das im nächsten Kapitel im Einzelnen.

4.1.2 Die Physik der statistischen Gemische (Gemenge)

Präparation Wir betrachten die folgende experimentelle Situation: Es steht für ein abgeschlossenes Quantensystem eine beliebige aber endliche Anzahl unterschiedlicher Präparationsverfahren zur Verfügung, die mit dem Index i durchnummeriert sind ($i = 1, \dots, N$) und entsprechend in die reinen Zustände $|\psi_i\rangle$ überführen. Diese Zustände müssen weder orthogonal noch linear unabhängig sein. N kann größer sein als die Dimension d . Wir gehen zu einem neuen Typ von Präparationsverfahren über, der darin besteht, dass immer eines der Ausgangsverfahren mit einer gewissen *klassischen Wahrscheinlichkeit* p_i mit

$$\sum_{i=1}^N p_i = 1 \quad (4.11)$$

zum Einsatz kommt. Es wird also zur Präparation des betrachteten Quantensystems in zufälliger Weise immer genau einer der Präparationsapparate angeschaltet (vergl. Abb. 4.1). *Der entsprechende Zustand $|\psi_i\rangle$ liegt dann beim Einzelsystem tatsächlich vor.* Dabei wird aber eingehalten, dass der i -te Apparat mit der Wahrscheinlichkeit p_i tätig wird. Man sagt, dass durch „Mischen“ der reinen Zustände das *Ensemble* $\{|\psi_i\rangle, p_i\}$ realisiert wird. Bei Kenntnis der Zustände $|\psi_i\rangle$ und der Präparationswahrscheinlichkeiten p_i ist wieder für beliebige Messungen eine sichere Prognose der Wahrscheinlichkeit des Eintretens von Messergebnissen möglich. *Nach dem von uns verwendeten Konzept definiert dieses verallgemeinerte Präparationsver-*

fahren also einen Quantenzustand. Er wird *statistisches Gemisch*¹ (statistical mixture) oder *Gemenge* genannt und beinhaltet den reinen Zustand als Spezialfall.

Dichteoperator statistischer Gemische Wir zeigen, dass sich die Gleichung für die physikalischen Aussagen aus Abschnitt 4.1.1 übertragen, wenn das statistische Gemisch durch den Dichteoperator

$$\rho := \sum_{i=1}^N p_i |\psi_i\rangle\langle\psi_i| = \sum_{i=1}^N p_i \rho_i \quad (4.12)$$

mit $\rho_i := |\psi_i\rangle\langle\psi_i|$ beschrieben wird. Hierzu führen wir Aussagen über das Gemisch auf Aussagen über die Ensemblezustände ρ_i zurück.

So wird bei einer Messung der Observablen A mit der Wahrscheinlichkeit

$$p(a_n) = \sum_i p(a_n|i) p_i \quad (4.13)$$

der Wert a_n gemessen. Dabei ist $p(a_n|i)$ die *bedingte Wahrscheinlichkeit* (conditional probability), dass der Messwert a_n gemessen wird, wenn der Zustand ρ_i vorliegt. Mit (4.4) erhalten wir

$$p(a_n|i) = \text{tr}[P_n \rho_i] . \quad (4.14)$$

Das führt mit (4.12) und den Rechenregeln für die Spurbildung auf

$$p(a_n) = \text{tr}[P_n \rho] . \quad (4.15)$$

Gleichung (4.4) überträgt sich also. Auch die Gl. (4.7) überträgt sich für statistische Gemische mit dem Argument, dass sich Erwartungswerte zu den einzelnen Zuständen mit den Wahrscheinlichkeiten p_i zum Erwartungswert beitragen.

$$\langle A \rangle = \sum_i p_i \text{tr}[A \rho_i] = \text{tr}[A \rho] . \quad (4.16)$$

Wie Gl. (4.13) und (4.16) zeigen, treten bei der Berechnung von Messwahrscheinlichkeiten und Erwartungswerten Produkte aus klassischen und quantentheoretischen Wahrscheinlichkeiten auf.

Selektive und nicht-selektive Messungen Abzuleiten sind noch die Gleichungen für die beiden Formen des dynamischen Verhaltens. Wir beginnen mit der Messdynamik. Für jeden der einzelnen Zustände ρ_i des Ensembles ergibt sich mit Gl. (4.5) als Ergebnis einer *selektiven Messung* (selective measurement) mit Messwert a_n der unnormierte Zustand

$$\rho_i \rightarrow \tilde{\rho}'_{i,n} = P_n \rho_i P_n . \quad (4.17)$$

¹Durch den Zusatz „statistisch“ soll hervorgehoben werden, dass ein Ensemble präpariert wurde. In der englischsprachigen Literatur findet sich hierfür auch die Bezeichnung *proper mixture*. Wir werden auch andere Gemische kennen lernen.

Wir lassen ausdrücklich Entartung der Messwerte zu. Für den Dichteoperator ρ von Gl. (4.12) folgt aus Gl. (4.17)

$$\rho \rightarrow \rho'_n = \sum_i p_i \tilde{\rho}'_{i,n} = P_n \rho P_n . \quad (4.18)$$

Dies stimmt mit der Relation (4.5) überein. Mit Gl. (4.15) erhalten wir für den normierten Dichteoperator nach der selektiven Messung in Übereinstimmung mit Gl. (4.3)

$$\rho \rightarrow \rho'_n = \frac{1}{p(a_n)} P_n \rho P_n . \quad (4.19)$$

Eine Ableitung dieser Gleichung, die von der bestimmenden empirischen Größe, also vom Messergebnis a_n ausgeht, lässt sich auch mit Hilfe des Satzes von Bayes (vergl. Abschn. 1.3.2) gewinnen². Die Wahrscheinlichkeit $p(a_n)$ für den Messwert a_n kann gemäß Gl. (4.15) und (4.18) in Übereinstimmung mit Gl. (4.6) auch in der Form

$$p(a_n) = \text{tr}[\tilde{\rho}'_n] \quad (4.23)$$

geschrieben werden kann.

Wir erwähnen noch den Spezialfall, dass für den Messwert a_n keine Entartung vorliegt. Dann ist $P_n = |a_n\rangle\langle a_n|$ mit dem zum Eigenwert a_n gehörigen Eigenvektor $|a_n\rangle$. Damit wird Gl. (4.19)

$$\rho \rightarrow \rho'_n = |a_n\rangle\langle a_n| . \quad (4.24)$$

Wenn der Messwert nicht entartet ist, präpariert daher die zugehörige selektive Messung an einem statistischen Gemisch einen reinen Zustand. Das ist plausibel, denn jeder der Zustandsvektoren $|\psi_i\rangle$ des Ensembles wird in diesem Fall durch die Messungen in $|a_n\rangle$ überführt.

Bei einer *nicht-selektiven Messung* (nonselective measurement) der Observablen A wiederholt man die Messung sehr oft an Quantensystemen im gleichen Zustand, aber sortiert

²Die Messung der Observablen A möge auf das Ergebnis a_n führen. Falls dabei vor der Messung der Zustand ρ_i vorlag, dann befindet sich nach der Messung der normierte Zustand

$$\rho'_{i,n} = \frac{1}{p(a_n|i)} P_n \rho_i P_n \quad (4.20)$$

(vergl. Gl. (4.14) und (4.23)). Mit welcher Wahrscheinlichkeit $p(i|a_n)$ lag vor der Messung ρ_i vor, wenn a_n registriert wurde? Nach dem bereits in Abschn. 1.3.2 genauer diskutierten Satz von Bayes gilt (wir formen noch mit Gl. (4.13) um)

$$p(i|a_n) = \frac{p(a_n|i)p_i}{\sum_j p(a_n|j)p_j} = \frac{p(a_n|i)p_i}{p(a_n)} \quad (4.21)$$

mit $\sum_i p(i|a_n) = 1$. $p(i|a_n)$ stimmt also i.a. nicht etwa mit p_i überein. Insgesamt folgt, daß zum Messergebnis a_n der Übergang

$$\rho \rightarrow \rho'_n = \sum_i p(i|a_n) \rho'_{i,n} \quad (4.22)$$

gehört. Einsetzen von $\rho'_{i,n}$ führt direkt auf Gleichung (4.19).

nicht wie in der selektiven Messung die Zustände ρ'_n aus, die zu einem bestimmten Messergebnis a_n gehören. Als resultierender Zustand ρ' entsteht in diesem Fall das statistische Gemisch, das sich additiv aus den Zuständen ρ'_n zusammensetzt, die bei der Messung mit den Wahrscheinlichkeiten $p(a_n)$ erzeugt werden:

$$\rho \xrightarrow{n.s.} \rho' = \sum_n p(a_n) \frac{P_n \rho P_n}{\text{tr}[\rho P_n]} = \sum_n P_n \rho P_n, \quad \text{tr}[\rho'] = 1. \quad (4.25)$$

Wir haben dabei Gebrauch von Gl. (4.15) gemacht.

Unitäre Dynamik Zu ergänzen ist noch die unitäre Dynamik. Hierbei ändern sich die klassischen Zusammensetzungswahrscheinlichkeiten p_i nicht. Die Gl. (4.8) überträgt sich daher direkt für statistische Gemische:

$$\rho(t) = U(t, t_0) \rho(t_0) U^{-1}(t, t_0) \quad (4.26)$$

und es ergibt sich die von Neumann-Gleichung (4.9) bzw. (4.10).

Wo treten statistische Gemische auf? Das am Anfang des Kapitels beschriebene Präparationsverfahren mag etwas künstlich erscheinen. Wir haben aber gesehen, dass für abgeschlossene Quantensysteme statistische Gemische tatsächlich in sehr natürlicher Weise auftreten. Alle nicht-selektiven Messungen an reinen Zuständen und an statistischen Gemischen überführen in statistische Gemische und nicht in reine Zustände.

Auch selektive Messungen an statistischen Gemischen führen im Allgemeinen auf statistische Gemische, wenn der eingetretene Messwert ein entarteter Eigenwert des Observablenoperators ist. Entartung kann zu Mischung führen. Mit ρ von Gl. (4.12) ist ρ'_n von Gl. (4.19)

$$\rho'_n = \frac{1}{p(a_n)} \sum_i p_i P_n |\psi_i\rangle \langle \psi_i| P_n. \quad (4.27)$$

Projektionsoperatoren P_n zu entarteten Eigenwerten projizieren in Unterräume (vergl. Gl. (2.3)), daher werden die $P_n |\psi_i\rangle$ im Allgemeinen nicht übereinstimmen. Der resultierende Dichteoperator ist eine Summe von Dichteoperatoren reiner Zustände und kann damit selber nicht der Dichteoperator eines reinen Zustands sein. Wir führen das unten im Zusammenhang mit Konvexkombinationen näher aus. Das Gemisch wird bei Entartung durch eine selektive Messung nicht völlig entmischt.

Schließlich soll noch eine weitere Messsituation erwähnt werden, die auf statistische Gemische führt. Bei einem Messapparat mögen die Messwerte nicht entartet sein. Es soll aber eine Ungenauigkeit in der Anzeige vorliegen, so dass alle Messwerte aus dem Intervall $[a_n, a_{m>n}]$ tatsächlich vom Apparat als Messwert a_n angezeigt werden. Eine selektive Messung zum abgelesenen Messwert a_n präpariert dann nicht einen reinen Zustand, sondern ein statistisches Gemisch.

Wir haben bisher nur abgeschlossene Systeme behandelt. Es wird sich in Abschnitt 7.3 zeigen, dass die Teilsysteme verschränkter Systeme ebenfalls durch Dichteoperatoren beschrieben werden können. Dies führt zu einer wichtigen Erweiterung des Konzepts „Gemisch“ auf nicht-statistische Gemische, denen kein wohlbestimmtes Ensemble aus realisierten Zuständen entspricht.

4.1.3 Definition und Eigenschaften des allgemeinen Dichteoperators

Definition Wir haben noch zu prüfen, welche der für reine Zustände abgeleiteten Eigenschaften (i) bis (iii^(*)) aus Abschnitt 4.1.1 auch für den Dichteoperator eines statistischen Gemisches gelten. Mit Hilfe von Gl. (4.11) und (4.12) bestätigen wir (i) und (ii) unmittelbar. Zur Diskussion von (iii) betrachten wir die Spektralzerlegung von ρ

$$\rho = \sum_{j=1}^d \lambda_j |j\rangle\langle j| . \quad (4.28)$$

$\{|j\rangle\}$ ist eine ONB und in Folge von (i) und (ii) gilt $\lambda_j = \lambda_j^*$, $\lambda_j \geq 0$ und $\sum_j \lambda_j = 1$. Damit erhalten wir

$$0 \leq \lambda_j \leq 1 \quad (4.29)$$

und daher

$$\text{tr}[\rho^2] \leq 1 . \quad (4.30)$$

Durch das Gleichheitszeichen in Gl. (4.30) ist eineindeutig das Vorliegen eines reinen Zustands charakterisiert. Die Ungleichung gilt nur für ein echtes Gemisch (kein reiner Zustand).

Wir lösen uns von den bisherigen Realisierungen und nennen allgemein einen Operator einen *Dichteoperator*, wenn er die Bedingungen

(i) ρ ist positiv (und damit hermitesch, $\rho^\dagger = \rho$)

(ii) $\text{tr}[\rho] = 1$

erfüllt.

Gemischtheitsgrad Aus Gl. (4.28) ergibt sich für den kleinsten Wert von $\text{tr}[\rho^2]$ der Quotient $\frac{1}{d}$, wobei d die Dimension des Hilbert-Raums ist. Der Wert wird für $\lambda_j = \frac{1}{d}$ angenommen und gehört somit zu

$$\rho = \frac{1}{d} \mathbb{1} . \quad (4.31)$$

Dieser völlig strukturlose Dichteoperator heißt der *maximal gemischte Dichteoperator*.

Wie oben beschrieben entstehen statistische Gemische operational im Experiment durch „Mischen“ von Zuständen. Man kann über den Parameter

$$\Xi := 1 - \text{tr}[\rho^2] \quad (4.32)$$

den *Gemischtheitsgrad* (degree of mixture) beschreiben, der zwischen dem des reinen Zustands $\Xi = 0$ und dem der maximalen Mischung $\Xi = 1 - \frac{1}{d}$ variiert:

$$0 \leq \Xi \leq 1 - \frac{1}{d} . \quad (4.33)$$

Bei statistischen Gemischen nähert sich Ξ der 1 an, wenn die Dimension d des Hilbert-Raums zunimmt. Wir geben hierfür ein Beispiel: Für $\rho_1 = \frac{1}{3}|0\rangle\langle 0| + \frac{2}{3}|1\rangle\langle 1|$ ist $\text{tr}[\rho^2] = \frac{5}{9}$ und für $\rho_2 = \frac{1}{3}|0\rangle\langle 0| + \frac{1}{3}|1\rangle\langle 1| + \frac{1}{3}|2\rangle\langle 2|$ folgt $\text{tr}[\rho^2] = \frac{1}{3}$.

Konvexkombination Wir notieren eine einfache Folge der Definition des Dichteoperators. Wenn $\{\rho_l, l = 1, \dots, k\}$ Dichteoperatoren sind und $\{r_l\}$ positive Zahlen mit $\sum_l r_l = 1$, dann ist die *konvexe Summe* (convex sum)

$$\rho = \sum_{l=1}^k r_l \rho_l \quad (4.34)$$

wieder ein Dichteoperator.

Wir zeigen, dass der Dichteoperator ρ eines reinen Zustandes außer durch $\text{tr}[\rho^2] = 1$ noch in einer anderen Weise ausgezeichnet ist. *Anders als alle anderen Dichteoperatoren kann der Dichteoperator eines reinen Zustands nicht in eine konvexe Summe zerlegt werden.* Zum Beweis machen wir mit dem Dichteoperator

$$\rho = |\psi\rangle\langle\psi| \quad (4.35)$$

den Zerlegungsversuch

$$\rho = \lambda \rho_1 + (1 - \lambda) \rho_2, \quad 0 < \lambda < 1. \quad (4.36)$$

Für einen zu $|\psi\rangle$ orthogonalen Vektor $|\chi\rangle$ erhalten wir

$$\langle\chi|\rho|\chi\rangle = 0 = \lambda \langle\chi|\rho_1|\chi\rangle + (1 - \lambda) \langle\chi|\rho_2|\chi\rangle. \quad (4.37)$$

Da λ und $1 - \lambda$ positiv sind und die Operatoren ρ_1 und ρ_2 positive Operatoren sind, folgt daraus

$$\langle\chi|\rho_1|\chi\rangle = \langle\chi|\rho_2|\chi\rangle = 0. \quad (4.38)$$

Wir ergänzen $|\psi\rangle$ durch Hinzunahme von Vektoren zu einer ONB. Für diese Vektoren gilt jeweils Gl. (4.38). Wir bilden die Matrixelemente von ρ_1 und ρ_2 in dieser Basis und nutzen $\text{tr}[\rho_1] = \text{tr}[\rho_2] = 1$ aus. Dann finden wir als einzige nichtverschwindende Matrixelemente

$$\langle\psi|\rho_1|\psi\rangle = \langle\psi|\rho_2|\psi\rangle = 1. \quad (4.39)$$

Damit ist

$$\rho = \rho_1 = \rho_2. \quad (4.40)$$

Die Zerlegung (4.36) ist daher nicht möglich. *Durch Mischen reiner Zustände (oder Gemische) kann nicht wieder ein reiner Zustand entstehen.* Dies zeichnet reine Zustände sowohl mathematisch wie auch im Prinzip operational aus. Wir haben diese Eigenschaft zur Definition des reinen Zustands bei der Formulierung der Postulate in Abschnitt 2.1.2 verwendet.

4.1.4 Inkohärente Überlagerung reiner Zustände

Während einer unitären dynamischen Entwicklung gilt als Folge von Gl. (4.26) die Erhaltung der Positivität und der Spur von ρ

$$\text{tr}[\rho(t)] = \text{tr}[\rho(t_0)] \quad (4.41)$$

sowie der Spur von ρ^2

$$\mathrm{tr}[\rho^2(t)] = \mathrm{tr}[\rho^2(t_0)] . \quad (4.42)$$

Daher kann durch eine unitäre Dynamik weder ein reiner Zustand in ein Gemisch übergehen noch umgekehrt. Demgegenüber kann als Ergebnis einer selektiven Messung mit nicht entartetem Messwert aber sehr wohl ein echtes Gemisch in einen reinen Zustand übergehen, wie wir in Gl. (4.24) gesehen haben. Ist bei einer Messung, also der zweiten Form von Dynamik die durch die Postulate beschrieben wird, auch der umgekehrte Vorgang, den man *Dekohärenz* (decoherence) nennt, möglich? Wir werden diese Frage im Zusammenhang mit der Theorie der Messung in Kap. 15 präzisieren. Hier wollen wir zunächst veranschaulichen, warum die Bezeichnung Kohärenz bzw. Inkohärenz in diesem Zusammenhang sinnvoll ist.

An Gl. (4.16) können wir ablesen, dass bei der Bildung des Erwartungswertes $\langle A \rangle$ die Mittelung in den Erwartungswerten $\mathrm{tr}[A\rho_i]$ und nicht wie bei der Superposition in den Zuständen erfolgt. Es handelt sich beim statistischen Gemisch in diesem Sinne um eine *inkohärente Überlagerung* (incoherent superposition) reiner Zustände. Die beteiligten Zustände interferieren nicht miteinander. Ihre relative Phase ist experimentell nicht bestimmbar. Das ist bei dem in Abschn. 4.1.2 angegebenen Präparationsverfahren auch unmittelbar verständlich. Dieser Aussage kann man eine direkte operationale Veranschaulichung in einem Interferenzexperiment geben. Die Verhältnisse am Doppelspalt (vergl. Abschn. 2.1) sind ein weiteres Beispiel.

Wir haben in Abschn. 3.7.2 gesehen wie mit Hilfe eines Strahlteilers die 0-Komponente und die 1-Komponente eines Photonenzustands $|\psi^{\mathrm{in}}\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\frac{\phi}{2}}\sin\frac{\theta}{2}|1\rangle$ zur kohärenten Überlagerung gebracht werden kann. Der Phasenschieber bewirkt ein Interferenzbild, das von der Phase α abhängt. In den Spezialfällen $|\psi^{\mathrm{in}}\rangle = |0\rangle$ und $|\psi^{\mathrm{in}}\rangle = |1\rangle$ entsteht kein Interferenzbild. Für ein einlaufendes Gemisch ρ^{in} ist die Ansprechwahrscheinlichkeit des 0-Detektors in Abhängigkeit von der Phasenverschiebung α durch

$$p(\alpha) = \mathrm{tr}[P_{|\alpha\rangle}\rho^{\mathrm{in}}] \quad (4.43)$$

mit $P_{|\alpha\rangle} = |\alpha\rangle\langle\alpha|$ von Gl. (3.86) gegeben. Für $\rho^{\mathrm{in}} = |0\rangle\langle 0|$ und $\rho^{\mathrm{in}} = |1\rangle\langle 1|$ ist $p(\alpha) = \frac{1}{2}$.

Wenn wir die Zustände $|0\rangle$ und $|1\rangle$ nicht superponieren wie bei $|\psi^{\mathrm{in}}\rangle$, sondern mischen

$$\rho^{\mathrm{in}} = \lambda_0|0\rangle\langle 0| + \lambda_1|1\rangle\langle 1| \quad (4.44)$$

($\lambda_{0,1} \geq 0$, $\lambda_0 + \lambda_1 = 1$), erhalten wir für die Ansprechwahrscheinlichkeiten den von α unabhängigen Wert

$$p(\alpha) = \frac{1}{2}(\lambda_0 + \lambda_1) = \frac{1}{2} . \quad (4.45)$$

Das statistische Gemisch ρ^{in} ist eine inkohärente Überlagerung, bei der ebenfalls beim Interferometer mit den Wegen $|0\rangle$ und $|1\rangle$ keine Interferenz auftritt. Das wird plausibel, wenn man sich vorstellt, dass Objekte in den Zuständen $|0\rangle$ und $|1\rangle$ nacheinander einlaufen.

Bemerkenswerterweise ergibt sich aber das gleiche Resultat auch für statistische Gemische mit Ensemble $\{|\psi_i\rangle, p_i\}$, das nicht mit dem Ensemble $\{|0\rangle, |1\rangle, \lambda_0, \lambda_1\}$ übereinstimmt,

wenn nur der zugehörige Dichteoperator sich in der Form (4.44) schreiben lässt. Das ist möglich, wenn $|0\rangle$ und $|1\rangle$ eine Eigenbasis von ρ sind. Auch in diesen Fällen zeigt das aus vielen Messpunkten zusammengesetzte Interferenzbild keinen Streifenkontrast, obwohl möglicherweise die Zustände $|\psi_i\rangle$ einzeln sehr wohl zu Interferenz mit Streifenkontrast führen. Wir können die Beiträge im Interferenzbild nicht nach den Zuständen sortieren, in dem sich die einzelnen registrierten Objekte befunden haben. Wir werden im Zusammenhang mit dem Quantenradierer in Abschn. 8.5 auf diesen Punkt zurückkommen.

4.2 Der allgemeine Quantenzustand

Wir erinnern an die Definition des Zustands eines Quantensystems wie sie in Abschnitt 2.1.2 gegeben wurde. Der Zustand ist dasjenige mathematische Objekt, das es erlaubt, die Wahrscheinlichkeit der Ergebnisse aller möglichen Messungen am System zu berechnen. Er ist einem Projektionsverfahren zugeordnet. Wir verstehen unter Messungen weiterhin nur projektive Messungen.

Messpostulate Dichteoperatoren, also alle positiven (und damit hermiteschen) Operatoren ρ , die die Bedingung $\text{tr}[\rho] = 1$ erfüllen, sind offenbar solche mathematische Objekte, wenn man als Postulat fordert: Die Wahrscheinlichkeiten sind durch Gl. (4.15) gegeben. Der Messprozess überführt in die Zustände ρ'_n von Gl. (4.19) bzw. ρ' von Gl. (4.25). Dies verallgemeinert das Postulat 2 aus Abschn. 2.1.2. Man kann zeigen, dass es keine anderen mathematischen Objekte gibt, die die an einen Zustand gestellten Forderungen erfüllen (Theorem von Gleason, vergl. Abschn. 4.5).

Bisher haben wir nur statistische Gemische (d. h. Gemenge) als Quantenzustände kennen gelernt. Wir werden in Kap. 7 mit den reduzierten Dichteoperatoren der Teilsysteme von zusammengesetzten Systemen andere Realisierungen von Zuständen behandeln. Sie unterscheiden sich durch ihre Präparation von statistischen Gemischen. Das Postulat, das das Postulat 1 von Abschn. 2.1 verallgemeinert, lautet dann: *Quantenzustände werden durch Dichteoperatoren repräsentiert*. Sie werden allgemein *Gemische* (mixtures) genannt. Statistische Gemische sind ein physikalischer Spezialfall, der durch das Präparationsverfahren ausgezeichnet ist.

4.3 Verschiedene Ensemblezerlegungen eines Dichteoperators und Ignoranzinterpretation

Wir beginnen mit einer einfachen Beobachtung. Die Zerlegung von zwei Qubit-Zuständen $|a\rangle$ und $|b\rangle$ (die z. B. Spin- $\frac{1}{2}$ -Zustände beschreiben) nach der Rechenbasis möge

$$\begin{aligned} |a\rangle &= \sqrt{\frac{2}{3}}|0\rangle + \sqrt{\frac{1}{3}}|1\rangle \\ |b\rangle &= \sqrt{\frac{2}{3}}|0\rangle - \sqrt{\frac{1}{3}}|1\rangle \end{aligned} \tag{4.46}$$

sein. Dann lässt sich der Dichteoperator ρ , der zum Ensemble aus den Zuständen $|a\rangle$ und $|b\rangle$ mit den Wahrscheinlichkeiten $p_a = p_b = \frac{1}{2}$ gehört, in zweifacher Weise schreiben:

$$\rho = \frac{1}{2}|a\rangle\langle a| + \frac{1}{2}|b\rangle\langle b| = \frac{2}{3}|0\rangle\langle 0| + \frac{1}{3}|1\rangle\langle 1|. \quad (4.47)$$

Er ist also zugleich der Dichteoperator zum Ensemble mit den Zuständen $|0\rangle$ und $|1\rangle$ (z. B. Spinpolarisationen in z -Richtung) und den Wahrscheinlichkeiten $p_0 = \frac{2}{3}$ und $p_1 = \frac{1}{3}$.

Wir geben noch ein physikalisches Beispiel. In einer Versuchsanordnung werden mit gleicher Häufigkeit horizontal und vertikal polarisierte Photonen erzeugt. Das zugehörige Ensemble $\{|H\rangle, |V\rangle, p_H = p_V = \frac{1}{2}\}$ wird durch den Dichteoperator

$$\rho = \frac{1}{d}\mathbb{1} \quad (4.48)$$

beschrieben. In einer völlig anders aufgebauten Versuchsanordnung werden rechtszirkular und linkszirkular polarisierte Photonen mit gleicher Häufigkeit produziert. Das Ensemble $\{|R\rangle, |L\rangle, p_R = p_L = \frac{1}{2}\}$ hat den selben Dichteoperator ρ . Die Photonen befinden sich daher in dem selben Zustand. Durch kein mit den Photonen durchgeführtes Experiment kann man entscheiden, durch welches der beiden Verfahren die Photonen präpariert wurden. Aus der Kenntnis des Dichteoperators ρ lässt sich auch in diesem Fall nicht eindeutig darauf schließen, welches Ensemble vorliegt. Wir wollen beweisen, dass das für jeden Dichteoperator gilt und zugleich zeigen, wie die verschiedenen Ensembles auseinander hervorgehen. Im Folgenden wollen wir voraussetzen, dass der Dichteoperator keinen reinen Zustand beschreibt.

Ensemblezerlegungen Wir betrachten den Dichteoperator

$$\rho = \sum_a p_a |\psi_a\rangle\langle\psi_a| = \sum_a |\tilde{\psi}_a\rangle\langle\tilde{\psi}_a|, \quad |\tilde{\psi}_a\rangle := \sqrt{p_a}|\psi_a\rangle, \quad (4.49)$$

den wir mit unnormierten Vektoren formulieren, die durch eine Tilde gekennzeichnet sind. Wieder müssen die Vektoren $\{|\psi_a\rangle\}$ weder orthogonal noch linear unabhängig sein. Dass ein Dichteoperator ρ als Dichteoperator des Ensembles $\{|\psi_a\rangle, p_a\}$ aufgefasst und damit wie Gl. (4.49) geschrieben werden kann, nennen wir eine *Ensemblezerlegung* (ensemble decomposition) von ρ . Wir wollen annehmen, dass es eine weitere Ensemblezerlegung von ρ gibt:

$$\rho = \sum_i |\tilde{\varphi}_i\rangle\langle\tilde{\varphi}_i|. \quad (4.50)$$

Darüber hinaus existiert stets die Spektralzerlegung von ρ

$$\rho = \sum_{n=1}^d \lambda_n |n\rangle\langle n| = \sum_{n=1}^d |\tilde{n}\rangle\langle\tilde{n}| \quad (4.51)$$

mit der ONB $\{|n\rangle\}$, die ebenfalls eine Ensemblezerlegung von ρ darstellt. Die Laufbereiche der Indizes der Typen a, b, \dots und i, j, \dots sowie n, m, \dots müssen nicht übereinstimmen.

Wir beschränken uns auf Eigenwerte $\lambda_n \neq 0$ und schränken den Laufbereich von n, m, \dots entsprechend ein. Dann bilden die zugehörigen $\{|n\rangle\}$ nicht notwendig eine Basis des ganzen

Hilbert-Raums \mathcal{H} . Wir nehmen an, dass sie den Unterraum \mathcal{H}' aufspannen. Für $|\chi\rangle$ aus dem orthogonalen Komplement von \mathcal{H}' gilt

$$0 = \langle \chi | \rho | \chi \rangle = \sum_a \langle \chi | \tilde{\psi}_a \rangle \langle \tilde{\psi}_a | \chi \rangle = \sum_a |\langle \chi | \tilde{\psi}_a \rangle|^2 \quad (4.52)$$

und damit

$$\langle \chi | \tilde{\psi}_a \rangle = 0 \quad (4.53)$$

für alle $|\chi\rangle$ und alle Indizes a . Entsprechendes gilt für die Vektoren $|\tilde{\varphi}_i\rangle$. Somit liegen alle $|\tilde{\psi}_a\rangle$ und alle $|\tilde{\varphi}_i\rangle$ im Unterraum \mathcal{H}' und wir können sie nach der Basis $\{|n\rangle\}$ von \mathcal{H}' entwickeln:

$$|\tilde{\psi}_a\rangle = \sum_n c_{an} |\tilde{n}\rangle, \quad |\tilde{\varphi}_i\rangle = \sum_n d_{in} |\tilde{n}\rangle. \quad (4.54)$$

Einsetzen in Gl. (4.49) und Berücksichtigung von Gl. (4.51) führt auf

$$\rho = \sum_{a,n,m} c_{an} c_{am}^* |\tilde{n}\rangle \langle \tilde{m}| = \sum_n |\tilde{n}\rangle \langle \tilde{n}| \quad (4.55)$$

und damit auf

$$\sum_a c_{an} c_{am}^* = \delta_{nm}, \quad \sum_i d_{in} d_{im}^* = \delta_{nm}. \quad (4.56)$$

Die aus Gl. (4.50) folgende Beziehung haben wir ebenfalls aufgeführt. Wenn die Laufbereiche der Indizes übereinstimmen, besagen die Gl. (4.56), dass die Matrizen c_{an} und d_{in} unitär sind.

Wir finden mit Gl. (4.54) und (4.56)

$$\sum_a c_{am}^* |\tilde{\psi}_a\rangle = \sum_{a,n} c_{am}^* c_{an} |\tilde{n}\rangle = |\tilde{m}\rangle. \quad (4.57)$$

Da Gl. (4.57) für jeden Basisvektor von \mathcal{H}' gilt, kann die Zahl der Vektoren $|\psi_a\rangle$ und $|\varphi_i\rangle$ nicht geringer als die Dimension von \mathcal{H}' sein. Abschließend setzen wir Gl. (4.57) noch in Gl. (4.54) ein und erhalten

$$|\tilde{\varphi}_i\rangle = \sum_{n,a} d_{in} c_{an}^* |\tilde{\psi}_a\rangle. \quad (4.58)$$

Eine entsprechende Zerlegung lässt sich daraus mit Hilfe von Gl. (4.56) für $|\tilde{\psi}_a\rangle$ gewinnen.

Wir haben gezeigt: Für zwei Ensemblezerlegungen $\{|\tilde{\psi}_a\rangle\}$ und $\{|\tilde{\varphi}_i\rangle\}$ eines Dichteoperators lassen sich die Vektoren der einen Zerlegung gemäß Gl. (4.58) als Linearkombination der Vektoren der anderen Zerlegung schreiben, wobei Gl. (4.56) erfüllt ist. Umgekehrt zeigt man leicht, dass Vektoren $|\tilde{\varphi}_i\rangle$ und $|\tilde{\psi}_a\rangle$, die wie in Gl. (4.58) verknüpft sind, jeweils eine Ensemblezerlegung desselben Dichteoperators darstellen, wenn die Matrizen die Bedingungen (4.56) erfüllen. Offenbar gibt es beliebig viele solcher Matrizen und damit beliebig viele Ensemblezerlegungen eines Dichteoperators.

Das Beispiel von Gl. (4.47) und der Beweis haben deutlich gemacht, dass die Mehrdeutigkeit der Ensemblezerlegung eine für die Quantentheorie typische Ursache hat: Ein Zustandsvektor lässt sich in unendlich vielen verschiedenen Weisen als Linearkombination anderer Zustandsvektoren schreiben. Etwas Analoges gibt es für klassische Zustände nicht.

Ignoranzinterpretation Wir haben gesehen, dass ein Dichteoperator mathematisch verschiedenen Ensemblezerlegungen zulässt. Das sollte im Zusammenhang mit der Frage, was physikalisch tatsächlich vorliegt, nicht zu Verwirrungen führen. Wenn ein Quantensystem im Zustand ρ als ein statistisches Gemisch (bzw. Gemenge) mit Ensemble $\{|\psi_i\rangle, p_i\}$ nach dem Verfahren aus Abschnitt 4.1.2 präpariert wurde, dann kann man die über die Minimalinterpretation hinausgehende Annahme machen, dass es sich auch real und objektiv stets in einem der Zustände $|\psi_i\rangle$ befindet. Wir wissen nur subjektiv nicht in welchem. Im Prinzip kann es aber jemand wissen, wenn er z. B. die Möglichkeit hat festzustellen, welcher Präparationsapparat gerade tätig war. Man sagt dann, dass der Zustand ρ eine *Ignoranzinterpretation* (ignorance interpretation) zulässt. Selbstverständlich kann man auch eine minimale Interpretation der Quantentheorie bevorzugen, in der die oben gestellte Frage gar nicht erst auftritt.

4.4 Dichteoperatoren von Qubits

Der Dichteoperator ρ in \mathcal{H}_2 lässt sich wie in Abschn. 3.1 nach der Pauli-Operatorbasis zerlegen

$$\rho = \frac{1}{2}(\mathbb{1} + \mathbf{r}\boldsymbol{\sigma}) \quad (4.59)$$

mit dem Bloch-Vektor

$$\mathbf{r} = \text{tr}[\rho\boldsymbol{\sigma}] = \langle \boldsymbol{\sigma} \rangle, \quad \mathbf{r} \in \mathbb{R}. \quad (4.60)$$

Mit

$$\text{tr}[\rho^2] = \frac{1}{2}(1 + |\mathbf{r}|^2) \quad (4.61)$$

von Gl. (3.23) folgt aus

$$\frac{1}{2} \leq \text{tr}[\rho^2] \leq 1 \quad (4.62)$$

für den Bloch-Vektor

$$|\mathbf{r}|^2 \leq 1. \quad (4.63)$$

Der Gemischtheitsgrad wird unmittelbar durch den Betrag des Bloch-Vektors bestimmt:

$$\Xi = \frac{1}{2}(1 - |\mathbf{r}|^2). \quad (4.64)$$

Für ein echtes Gemisch liegt der Bloch-Vektor \mathbf{r} im Inneren der Bloch-Kugel. Der vollständig gemischte Zustand $\frac{1}{2}\mathbb{1}$ wird durch den Kugelmittelpunkt ($\mathbf{r} = \mathbf{0}$) repräsentiert.

Zustandsbestimmung Der Zusammenhang $\rho \leftrightarrow \mathbf{r}$ gemäß Gl. (4.59) und (4.60) ist, anders als die Beziehung $|\psi\rangle \leftrightarrow \mathbf{r}$, eine eindeutige Beziehung, da Phasenfaktoren durch ρ nicht wiedergegeben werden. Wir können den Zustand ρ durch Messung der Erwartungswerte $\langle \sigma \rangle$ der drei verschiedenen Observablen σ bestimmen. Beim Spin geschieht das durch Messung der Mittelwerte der Spinkomponenten in drei unabhängige Richtungen. Beim reinen Zustand reichen wegen der Normiertheit von \mathbf{r} zwei Richtungen.

Wir notieren noch die Matrixelemente als Funktionen der Komponenten des Bloch-Vektors:

$$\rho(\mathbf{r}) = \frac{1}{2} \begin{pmatrix} 1 + r_3 & r_1 - ir_2 \\ r_1 + ir_2 & 1 - r_3 \end{pmatrix} \quad (4.65)$$

$$(4.66)$$

mit

$$\begin{aligned} r_3 &= \rho_{00} - \rho_{11} \\ r_2 &= i(\rho_{01} - \rho_{10}) \\ r_1 &= \rho_{01} + \rho_{10} \end{aligned} \quad (4.67)$$

4.5 Ergänzende Themen und weiterführende Literatur

- Theorem von Gleason: Wir haben Quantenzustände zunächst durch Zustandsvektoren und dann durch Dichteoperatoren beschrieben. Gibt es andere mathematische Objekte, die sichere Wahrscheinlichkeitsaussagen ermöglichen? Das *Theorem von Gleason* [Gle 57] besagt, dass

$$\langle A \rangle = \text{tr}[A\rho] \quad (4.68)$$

die allgemeinste Formel für den Erwartungswert ist, die mit der Wahrscheinlichkeitsstruktur der Quantentheorie verträglich ist, wenn die Dimension des Hilbert-Raums größer als 2 ist. Die Zustandsbeschreibung mit positiven Operatoren der Spur 1 ist die allgemeinste quantentheoretische Zustandsbeschreibung. Das gilt auch dann, wenn Messungen durch ein POVM (vgl. Abschn. 13.4) beschreiben werden. Literatur: [Per 93, S. 190f], [BGL 95, S. 124f], [Aul 00, S. 199f]. In [Bus 99] wird das auch für die Dimension 2 bewiesen.

- Ergänzende Literatur zu Dichteoperatoren: [Fan 57].

4.6 Übungsaufgaben

ÜA 4.1 [zu 4.1 und 4.4] Der Zustand eines Quantensystems ist durch die Dichtematrix

$$\rho = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

mit $a, b \in \mathbb{R}$, $a \geq 0$, $b \geq 0$ und $a + b = 1$ gegeben.

- Wie groß ist die Wahrscheinlichkeit bei einer Messung von σ_x den Wert $+1$ bzw. -1 zu erhalten?
- Berechnen Sie ohne Bezug auf a) direkt den Erwartungswert bei einer σ_x -Messung.
- Berechnen Sie die entsprechenden Größen für σ_y statt σ_x .
- Bestimmen Sie den Bloch-Vektor und veranschaulichen Sie die Ergebnisse für die Erwartungswerte.

ÜA 4.2 Geben Sie für die Dichtematrix

$$\rho = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

eines Spinsystems verschiedene Ensemblezerlegungen an.

ÜA 4.3 [zu 4.4] Zeigen Sie, dass sich ein Dichteoperator bei Bezug auf die Eigenbasis sich einfach als Funktion des Betrages des Bloch-Vektors schreiben lässt:

$$\rho \leftrightarrow \begin{pmatrix} 1 - |\mathbf{r}|^2 & 0 \\ 0 & 1 + |\mathbf{r}|^2 \end{pmatrix}$$

(Hinweis: Bestimmen Sie die Eigenwerte von $\rho(\mathbf{r})$.)

ÜA 4.4 [zu 4.4] Die Observablen A , B und C besitzen die Darstellung

$$A = \begin{pmatrix} 3 & 0 \\ 0 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & -2i \\ 2i & 0 \end{pmatrix} \quad (4.69)$$

in der Rechenbasis. Messungen am Zustand mit dem Dichteoperator ρ führen auf die Erwartungswerte

$$\langle A \rangle = 2, \quad \langle B \rangle = \frac{1}{2}, \quad \langle C \rangle = 0. \quad (4.70)$$

Bestimmen Sie den Dichteoperator ρ .

This Page Intentionally Left Blank

5 Shannon-Entropie und klassische Information

Entropie ist ein Konzept, das im Rahmen der Thermodynamik entwickelt wurde. In der klassischen statistischen Mechanik und in der Quantenstatistik wird es zur Beschreibung statistischer Gemische herangezogen. Entropie dient dabei als Maß für Unordnung und für die fehlende Information über einen Zustand. Ausgehend von dieser Interpretation wurde Entropie zu einem Schlüsselkonzept der klassischen Informationstheorie (*Shannon-Entropie*) und der Quanteninformationstheorie (*von Neumann-Entropie*).

Die Quanteninformationstheorie beschreibt die Übertragung und Verarbeitung von Information mit Hilfe von Quantensystemen als Informationsträger. Dabei spielt die von Neumann-Entropie eine mehrfache Rolle:

- (i) Sie erlaubt Aussagen über den klassischen Informationsgehalt – denn nur den können wir „ablesen“ – der auf quantentheoretischen Trägern kodierten Information.
- (ii) Sie quantifiziert, welche quantentheoretischen Ressourcen mindestens benötigt werden, um eine vorgegebene Information zu speichern.
- (iii) Schließlich kommt noch eine Aufgabe hinzu, die kein klassisches Analogon hat: Mit Hilfe der von Neumann-Entropie lässt sich die Verschränktheit zusammengesetzter Systeme quantifizieren.

Zu diesen drei Aufgaben treten im Zusammenhang mit der Messtheorie, mit gestörten Quantenkanälen usw. noch weitere Aufgaben hinzu.

Wir beginnen mit dem ersten Punkt, der unmittelbar an die bisherigen Überlegungen zum statischen Gemisch anschließt, und stellen als Vorbereitung zunächst die klassische Shannon-Entropie vor. Anschließend werden wir den Informationstransport durch Quantenkanäle untersuchen, um der Quantenentropie eine operationale Veranschaulichung zu geben. Die Bedeutung des Entropie-Konzeptes für die Beschreibung verschränkter Systeme werden wir im übernächsten Kapitel skizzieren.

5.1 Definition und Eigenschaften

Problemstellung In einem einführenden Kapitel wollen wir das Konzept der Shannon-Entropie am Beispiel eines geschriebenen Textes (z. B. einer Zeitung) verdeutlichen, der eine

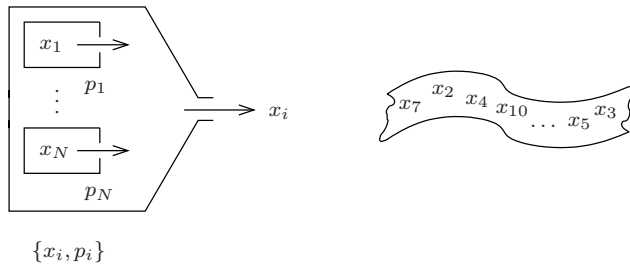


Abbildung 5.1: Eine Signalquelle mit Signalensemble $\{x_i, p_i\}$ erzeugt eine Zeichenfolge.

Information übermitteln soll. Der Text ist aus einer Reihe von n Buchstaben eines Alphabets gebildet.

Texte in einer Sprache sind für unsere Zwecke allerdings noch viel zu komplexe Gebilde. Sie bestehen z. B. aus deutschen Wörtern, d. h. es sind nicht alle Buchstabenkombinationen zugelassen. Weiterhin sind Buchstaben in ihrer Abfolge nicht unabhängig voneinander, denn es folgt im deutschen Text z. B. auf „sc“ mit hoher Wahrscheinlichkeit „h“. Von diesen Korrelationen zwischen Buchstaben wollen wir absehen und nur Texte betrachten, die von *Signalquellen* (signal source) *ohne Erinnerung* produziert werden, die einer Bedingung unterliegen: Ein Buchstabe x_i soll mit der a-priori-Wahrscheinlichkeit p_i mit $\sum_{i=1}^N p_i = 1$ erzeugt werden. N ist die Zahl der verschiedenen Buchstaben. Sie hängt von der Sprache ab. In einem deutschen Text kommt z. B. im Gegensatz zu einem englischen Text der Buchstabe y eher selten vor. Eine solche *stochastische erinnerungslose Signalquelle* ist allein durch das *Signalensemble* $\{x_i, p_i\}$ mit $i = 1, \dots, N$ charakterisiert. Es stellt eine Menge von unterscheidbaren Alternativen x_i zusammen mit ihren Wahrscheinlichkeiten p_i dar. Man bezeichnet das Signalensemble auch als *Zufallsvariable* (random variable) X .

Man kann sich als operationale Realisierung vorstellen, dass N Druckmaschinen vorliegen, die jeweils einen der Buchstaben x_i drucken können. Mit Hilfe dieser Druckmaschinen kann nun Alice als der Absender einen Text drucken. Diese *Botschaft* (message) besteht aus einer *Zeichenfolge* (string) oder *Sequenz* (sequence) aus n Buchstaben. Die Zahl der möglichen Botschaften ist dann N^n . Die Maschinen sind dabei aber so eingestellt, dass sie eine Nebenbedingung erfüllen. Wir betrachten sehr viele solcher Sequenzen, wie sie von der Anlage gedruckt werden. Die relative Häufigkeit mit der der Buchstabe x_i gedruckt wird, soll dann p_i sein. Im Spezialfall $p_1 = 1, p_{i \neq 1} = 0$ gibt es z. B. immer nur eine einzige Sequenz: $x_1 x_1 x_1 \dots x_1 \dots$. Aber auch für $p_1 \neq 1$ kann diese Sequenz vorkommen¹. Alle Maschinen zusammengefasst bilden eine große Druckanlage, die in unserer Veranschaulichung die Signalquelle darstellt (siehe Abb. 5.1 und vergleiche mit Abb. 4.1)

Der spezielle von Alice gedruckte Text wird Buchstabe für Buchstabe störungsfrei mit Hilfe eines mit klassischer Physik beschreibbaren Trägers (z. B. auf Papier) an den Empfänger Bob übermittelt. Bob weiß nicht welchen Buchstaben er als Nächsten empfangen wird, aber

¹Wir haben uns mit dem Bild von Druckmaschinen weitgehend von „Sprache“ gelöst, denn $yy \dots y$ wird ebenfalls von einer Druckanlage gedruckt, deren p_i mit den Buchstabenhäufigkeiten der deutschen Sprache übereinstimmen, allerdings geschieht das sehr selten.

er soll wissen, welche Druckanlage Alice verwendet. *Bob hat daher eine wichtige Vorinformation: Er kennt das Signalensemble $\{x_i, p_i\}$ und damit insbesondere die Wahrscheinlichkeiten $\{p_i\}$.* Dies ist sein Vorwissen (a-priori-Wissen). Wir suchen ein Maß für die verbliebene a-priori-Ungewissheit von Bob. Dies Maß kann zugleich als ein Maß für die *Information* (information) dienen, die diese *Ungewissheit* (uncertainty) beseitigt. Wir werden sehen, dass die Entropie ein solches Maß für die Information darstellt. Das wird bereits bei der jetzt folgenden heuristischen Einführung der Entropie deutlich. Eine genauere Quantifizierung und Operationalisierung diskutieren wir anschließend in Abschn. 5.2.

Shannon-Entropie² Alice druckt eine Zeichensequenz aus n Zeichen. Es gibt N^n solcher Sequenzen. Wenn n eine sehr große Zahl ist, dann ist es wahrscheinlich, dass viele dieser Sequenzen jeweils in sich bereits die relativen Häufigkeiten p_i widerspiegeln, dass also mit der Häufigkeit $n_i = np_i$ der Buchstabe x_i in der langen Sequenz irgendwo auftaucht. Sequenzen der Form $x_i x_i \dots x_i$ sind nicht ausgeschlossen aber unwahrscheinlich, wenn die p_i klein sind. Wenn n groß ist, darf Bob daher vermuten, dass er eine der Sequenzen erhalten hat, die die x_i mit den Häufigkeiten n_i enthält. Wie viele verschiedene Sequenzen von diesem Typ gibt es? Es gibt $n!$ Möglichkeiten n Buchstaben anzuordnen. Vertauschen derselben Buchstaben untereinander führt auf keinen neuen Text. Für x_i sind $n_i!$ Vertauschungen möglich. Daher handelt es sich um

$$Z_n = \frac{n!}{n_1! n_2! \dots n_N!} \quad (5.1)$$

Sequenzen mit $\sum_{i=1}^N n_i = n$.

Um zu den Wahrscheinlichkeiten p_i übergehen zu können, betrachten wir den Grenzfall unendlich langer Texte ($n \rightarrow \infty, n_i \rightarrow \infty$). Dann ist $p_i = \frac{n_i}{n}$ und es ergibt sich mit der Stirlingschen Formel $\log(n!) = n \log n - n + \mathcal{O}(\log n)$ für den Logarithmus der Anzahl Z_n

$$\begin{aligned} \log Z_n &\rightarrow n \log n - n - \sum_{i=1}^N (n_i \log n_i - n_i) \\ &= -n \sum_{i=1}^N p_i \log p_i. \end{aligned} \quad (5.2)$$

Wir verwenden $0 \log 0 = 0$.

Wenn wir den Logarithmus der Anzahl Z_n der Möglichkeiten durch n dividieren, ihn also als Mittelwert auf die einzelne Buchstabenstelle beziehen, entsteht die *Shannon-Entropie* oder *klassische Entropie* $H(\tilde{p})$ der *Wahrscheinlichkeitsverteilung* $\tilde{p} \leftrightarrow \{p_i, i = 1, \dots, N\}$, die folgendermaßen definiert ist:

$$H(\tilde{p}) := \lim_{n \rightarrow \infty} \frac{1}{n} \log Z_n = - \sum_{i=1}^N p_i \log p_i \geq 0. \quad (5.3)$$

Der Logarithmus wird dabei zur Basis 2 genommen. Auch die Bezeichnung $H(X)$ statt $H(\tilde{p})$ ist gebräuchlich. Die Zahl Z_n der möglichen Texte mit einer Anzahl n von Buchstaben ergibt

² [Sha 48], [Sha 49]

sich dann im Grenzfall als

$$Z_n = 2^{nH(\tilde{p})}. \quad (5.4)$$

Da viele (wenige) Möglichkeiten ein großes (kleines) Maß von a-priori-Ungewissheit von Bob widerspiegelt, ist $H(\tilde{p})$ von Gl. (5.3) ein Maß für die mittlere a-priori-Unbestimmtheit eines Buchstabens, den Bob empfängt. Damit ist H zugleich die mittlere Information, die Bob pro übermittelten Buchstaben erhält. Sie erlaubt es ihm unter den alternativ möglichen Sequenzen die Übermittelte zu identifizieren. H ist dimensionslos. Der Wert von H gibt die Information in der Einheit *Bit* an. Wir werden das in Abschn. 5.3 noch weiter präzisieren.

$H(\tilde{p})$ charakterisiert die Wahrscheinlichkeitsverteilung $\{p_i\}$ des Signalensembles. Ob das Signal dabei aus Buchstaben oder anderen Zeichen besteht, ist unwesentlich. Die x_i können irgendwelche Alternativen sein, die mit den zugehörigen Wahrscheinlichkeiten p_i vorliegen. Im Unterschied zu einer Signalübertragung mit Quantensystemen haben wir vorausgesetzt, dass die Zeichen (z. B. Buchstaben) klassische Zeichen sind. Sie können eindeutig voneinander unterschieden werden und werden im Prozess des Auslesens nicht verändert. Kommt x_i bei Bob an, dann liest Bob auch x_i . Dabei spielt es keine Rolle, mit welchem klassischen Träger (Papier, Töne usw.) die Information übermittelt wird.

Eigenschaften Wir wollen zunächst noch einige mathematische Eigenschaften der Entropie beweisen. *Der Maximalwert von $H(\tilde{p})$ ist $\log N$, wenn N die Zahl der Zeichen im Signalensemble ist. Er wird für die Gleichverteilung $p_1 = p_2 = \dots = p_n = N^{-1}$ angenommen.* Zum Beweis schreiben wir die Nebenbedingung $\sum_i p_i = 1$ in der Form $p_N = 1 - \sum_{i=1}^{N-1} p_i$ und betrachten die anderen $p_{i \neq N}$ als unabhängige Variablen. Die Ableitung von

$$H(\tilde{p}) = - \sum_{i=1}^{N-1} p_i \log p_i - p_N \log p_N \quad (5.5)$$

verschwindet dann wegen

$$\partial H / \partial p_l = -\log p_l + \log p_N \quad (5.6)$$

für $p_l = p_N = \frac{1}{N}$ mit

$$H^{\max}(\tilde{p}) = H(p_i = N^{-1}) = \log N. \quad (5.7)$$

Ein weiteres Extremum, beispielsweise am Rand, gibt es nicht. Wir notieren noch den *Minimalwert* von $H(\tilde{p})$:

$$H^{\min}(\tilde{p}) = 0 \quad \Leftrightarrow \quad p_l = 1, \quad p_{i \neq l} = 0 \quad (5.8)$$

Er liegt vor, wenn die Sprache nur einen einzigen Buchstaben besitzt.

Insgesamt gilt also

$$0 \leq H \leq \log N \quad (5.9)$$

und bei *binärer Kodierung* (binary coding) ($N = 2$):

$$0 \leq H \leq 1. \quad (5.10)$$

$H(\tilde{p})$ ist in diesem Fall ($p_1 = p, p_2 = 1 - p$) eine Funktion von p mit $0 \leq p \leq 1$.

$$H(p) = -p \log p - (1 - p) \log(1 - p) \quad (5.11)$$

die in Abb. 5.2 dargestellt ist. Ein klassisches System mit zwei Zuständen hat eine maximale Informationskapazität von $H(p = \frac{1}{2}) = 1$ Bit.

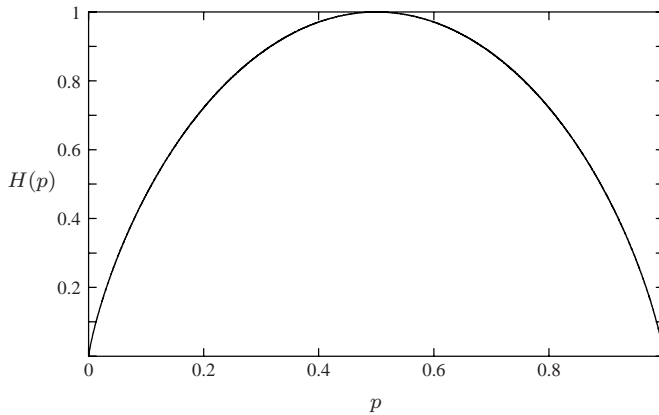


Abbildung 5.2: Shannon-Entropie $H(p)$ bei binärer Kodierung mit den Wahrscheinlichkeiten $p_1 = p$ und $p_2 = 1 - p$.

5.2 Shannons Theorem

5.2.1 Typische Sequenzen

Wir wollen zeigen, dass die Entropie $H(\tilde{p})$ ein gutes Maß für den Informationsgehalt pro Buchstabe darstellt, wenn ein langer Text ($n \rightarrow \infty$) aus einer Quelle mit Signalensemble $\{x_i, p_i\}$ kommt. Wie kann man Information operational genauer fassen? Nehmen wir an, Alice hat einen Text, den wir den *Ausgangstext* nennen wollen, und sie möchte ihn Bob mitteilen. Alice verwendet dabei nicht das Signalensemble selber, sondern das einfachste nicht-triviale Alphabet. Es besteht aus zwei Zeichen (z. B. aus den *Binärzahlen* (binary digits) 0 und 1), die mit gleicher Wahrscheinlichkeit auftreten sollen. Der neue Text ist dann eine *Bit-Sequenz* (bit sequence, binary string). Die Übertragung an Bob soll wieder störungsfrei sein. Immer wenn eines dieser Symbole von Bob empfangen wird, wollen wir sagen, dass er die Information 1 *Bit* erhalten hat. Die Antwort auf eine Ja-Nein-Frage („Liegt die Zahl 0 vor?“) enthält die Information 1 Bit. Wir bestimmen den Informationsgehalt des Ausgangstextes indem wir zählen wie viele Bits Alice bei geschicktestem Vorgehen senden muss, damit Bob erfährt, welcher aus der Menge der Texte der Länge n der Ausgangstext war. Da wir nur sehr lange Texte betrachten, reicht es, die mittlere Zahl notwendiger Bits pro Buchstabe des Ausgangsalphabets zu bestimmen. Wir werden zeigen, dass sie gleich der Shannon-Entropie $H(\tilde{p})$ ist. Die Information im Ausgangstext ist dann $nH(\tilde{p})$ bits. Zur Analyse des Vorgehens von Alice gehen wir vom Gesetz der großen Zahlen aus.

Grenzwertsatz Wir betrachten eine stochastische erinnerungslose Quelle, die keine Buchstaben, sondern reelle Zahlen y_i , $i = 1 \dots N$ mit den Wahrscheinlichkeiten p_i erzeugt. Eine Sequenz von n dieser Zahlen ist z. B.

$$y_4 y_1 y_{17} y_4 \dots y_1. \quad (5.12)$$

Wir nummerieren die Zahlen durch. Die reelle Zahl an der Stelle l nennen wir w_l mit $l = 1, \dots, n$. In (5.12) ist z. B. $w_2 = y_1$. Die Sequenz in (5.12) können wir dann auch in der durchnummerierten Form

$$w_1 w_2 w_3 \dots w_n \quad (5.13)$$

schreiben.

Wir wollen sehr lange Sequenzen betrachten. Dann gilt das *Gesetz der großen Zahlen* (law of large numbers). Es besagt, dass das arithmetische Mittel der Zahlen in der Sequenz gegen den mit den Wahrscheinlichkeiten p_i gebildeten Erwartungswert geht:

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{l=1}^n w_l = \sum_{i=1}^N p_i y_i =: \langle y \rangle . \quad (5.14)$$

Man kann den Grenzprozess noch etwas genauer formulieren: Zu gegebenem beliebig kleinen $\epsilon > 0$ und $\delta > 0$ gibt es bei endlicher Varianz der y_i eine große Sequenzlänge n , so dass die Wahrscheinlichkeit dafür, dass eine Sequenz mit $\left| \frac{1}{n} \sum_l w_l - \langle y \rangle \right| < \delta$ erzeugt wird größer als $1 - \epsilon$ ist.

Typische Sequenzen Wir gehen zu unseren Buchstaben bzw. Zeichen x_i aus dem Signalensemble $\{x_i, p_i\}$ über. Eine spezielle Sequenz der Länge n ist z. B.

$$x_4 x_1 x_{17} x_4 \dots x_1 . \quad (5.15)$$

Die Gesamtwahrscheinlichkeit $P(x_4 \dots x_1)$ für das Auftreten dieser Sequenz ist das Produkt

$$P(x_4 \dots x_1) = p_4 \cdot p_1 \cdot p_{17} \cdot p_4 \dots p_1 . \quad (5.16)$$

Wir bilden den negativen Logarithmus und dividieren durch n .

$$-\frac{1}{n} \log P(x_4, x_1, \dots, x_1) = \frac{1}{n} \{ -\log p_4 - \log p_1 \dots - \log p_1 \} . \quad (5.17)$$

Diese Summe hat die Struktur eines Mittelwertes. Die Summanden in der Klammer bilden eine Sequenz reeller Zahlen. Sie entspricht der Sequenz (5.12) mit $y_4 = -\log p_4$ usw. Im Anschluss an Gl. (5.13) können wir schreiben: $w_1 = -\log p_4, \dots, w_n = -\log p_1$. Die Wahrscheinlichkeit für das Auftreten von $-\log p_i$ auf der rechten Seite von Gl. (5.17) ist gleich der des Auftretens von x_i in der Sequenz (5.15) und damit gleich p_i . Mit Gl. (5.14) lässt sich das arithmetische Mittel wieder als Erwartungswert schreiben. Die Gl. (5.17) zusammen mit der Definition (5.3) führt dann auf:

$$\lim_{n \rightarrow \infty} \left\{ -\frac{1}{n} \log P \right\} = - \sum_{i=1}^N p_i \log p_i =: \langle -\log \tilde{p} \rangle =: H(\tilde{p}) . \quad (5.18)$$

Wieder wollen wir dieses Ergebnis durch Einführen von infinitesimalen Größen ϵ und δ präzisieren. Höhere Potenzen von ϵ und δ lassen wir weg. Die Wahrscheinlichkeit dafür, dass eine Sequenz mit $P(\dots)$ auftritt, die auf einen Wert von $-\frac{1}{n} \log P$ aus dem Intervall

$$H - \delta < -\frac{1}{n} \log P < H + \delta \quad (5.19)$$

führt, ist größer als $1 - \epsilon$. Es wird daher mit an Sicherheit grenzender Wahrscheinlichkeit eine Sequenz erzeugt, deren Gesamtwahrscheinlichkeit P von Gl. (5.16) die Bedingung (5.19) erfüllt. Oder wie oben formuliert: Zu vorgegebenem ϵ und δ gibt es eine Sequenzlänge n , sodass (5.19) mit der Wahrscheinlichkeit $1 - \epsilon$ erfüllt ist. Mit immer kleineren ϵ und δ wird n immer größer. Wir formen Gl. (5.19) um:

$$2^{-n(H+\delta)} \leq P \leq 2^{-n(H-\delta)} . \quad (5.20)$$

Gleichung (5.20) besagt, dass fast ausschließlich (nämlich mit Wahrscheinlichkeit $1 - \epsilon$) Sequenzen auftreten, deren gemäß Gl. (5.16) gebildete Wahrscheinlichkeiten P übereinstimmend alle gleich 2^{-nH} sind. Diese Sequenzen werden *typische Sequenzen* (typical sequences) genannt. *Für hinreichend große n zerfällt die Menge der Sequenzen der Länge n in zwei disjunkte Mengen: in die gleichwahrscheinlichen typischen Sequenzen und den Rest der untypischen Sequenzen.*

Wie groß ist die Anzahl $Z(n, \epsilon, \delta)$ dieser typischen Sequenzen? Die Summe der Wahrscheinlichkeiten aller typischen Sequenzen muss zwischen $1 - \epsilon$ und 1 liegen:

$$1 - \epsilon \leq Z(n, \epsilon, \delta)P \leq 1 \quad (5.21)$$

Wir dividieren durch P und beachten, dass P selber aus dem Intervall von Gl. (5.20) stammt. Dann folgt für die Anzahl typischer Sequenzen

$$(1 - \epsilon)2^{n(H-\delta)} \leq Z(n, \epsilon, \delta) \leq 2^{n(H+\delta)} \quad (5.22)$$

Dies präzisiert Gl. (5.4).

5.2.2 Klassische Datenkompression

Kodierung langer Blöcke und Datenkompression Die Ungleichungen (5.20) und (5.22) haben eine unmittelbare praktische Bedeutung. Mit wachsender Buchstabenanzahl n der Botschaft tauchen untypische Sequenzen so gut wie nicht mehr auf. Die Anzahl $Z(n, \epsilon, \delta)$ der typischen Sequenzen geht gegen 2^{nH}

$$Z(n, \epsilon, \delta) \xrightarrow{n \gg 1} 2^{nH} . \quad (5.23)$$

Weiterhin treten alle typischen Sequenzen mit der gleichen Wahrscheinlichkeit $P = 2^{-nH}$ auf (Gleichverteilung). Wir nummerieren die 2^{nH} verschiedenen typischen Sequenzen mit Zahlen in binärer Schreibweise durch. Wir kodieren somit ganze Sequenzen (*Block-Kodieren*, block coding) und betrachten nicht mehr individuelle Signale. Dann benötigen wir dazu Zahlen mit nH Stellen ($H \neq 0$ vorausgesetzt).

Die Zahl der insgesamt möglichen Sequenzen ist demgegenüber $N^n = 2^{n \log N}$. Wenn wir sie in binärer Schreibweise durchnummerieren, brauchen wir Zahlen mit $n \log N$ Stellen. Für eine Charakterisierung einer speziellen typischen Sequenz der Länge n reicht somit im Fall $H \neq H^{\max} = \log N$ ein binärer Text der kleineren Länge nH (vergl. Gl. (5.9)). Eine kürzere Kodierung mit weniger Bits ist allerdings nicht möglich, da alle typischen Sequenzen bereits gleichwahrscheinlich sind. Durch Umkodieren kann nichts gewonnen werden. Der Text

wird dem Empfänger übermittelt. Wenn die Durchnummerierung dem Empfänger bekannt ist, kann er die spezielle typische Sequenz eindeutig rekonstruieren. *Durch die Beschränkung auf die typischen Sequenzen – nur diese treten für große n als Botschaften auf – und binäres Durchnummerieren hat eine Datenkompression (data compression) stattgefunden. Eine darüber hinaus gehende Kompression ist nicht möglich.* Im Hinblick auf eine analoge Aussage über Quantensysteme als Informationsträger notieren wir noch: *Die Shannon-Entropie gibt die Anzahl der klassischen binären Informationsträger an, die mindestens nötig ist, um die Information in einer Botschaft zu übermitteln. Klassische binäre Informationsträger können z. B. Zettel sein, die entweder mit 0 oder mit 1 bedruckt sind, oder Töne, die nur in zwei Frequenzen ausgesendet werden.*

Shannons Theorem Wir formulieren das Ergebnis (5.22) noch einmal in einer anderen Weise und gehen dabei auch auf die Fehlerwahrscheinlichkeit ein. Die rechte Ungleichung (5.22) besagt, dass wir jede typische Sequenz eineindeutig in eine Sequenz von $n(H + \delta)$ binären Zahlenstellen abbilden können. Die verbliebenen wenig wahrscheinlichen untypischen Sequenzen bildet Alice „fehlerhaft“ alle auf eine einzige binäre Sequenz ab (z. B. 000...00). Dann ist es bei diesem Verfahren möglich, dass zwei ursprüngliche Botschaften durch dieselbe binäre Sequenz kodiert sind und es kann ein *Fehler* bei der Dekodierung auftreten. Wir schreiben die Fehlerwahrscheinlichkeit in der Form $1 - F$. F wird die *Treue (fidelity) des Kodierung-Dekodierung-Schemas* genannt. *Shannons Theorem³ der fehlerfreien Kodierung (Shannons noiseless coding theorem) fasst die obigen Überlegungen in folgender Form zusammen: Wenn $n(H + \delta)$ Bits für die Kodierung von Botschaften der (großen) Länge n zur Verfügung stehen, dann können die Botschaften mit einer Fehlerwahrscheinlichkeit $1 - F < \epsilon$ in den entsprechenden binären Sequenzen kodiert werden (Zu gegebenem ϵ und δ gibt es ein n sodass dieser Satz gilt). Stehen nur $H - \delta$ Bits zur Verfügung, dann ist die Fehlerwahrscheinlichkeit größer als $1 - \epsilon$.*

5.3 Information

Wir kommen auf unser am Anfang von Abschn. 5.1 formuliertes Ausgangsproblem zurück. Alice hat einen ihr bekannten Text mit n Buchstaben bzw. Zeichen aus einer erinnerungslosen Quelle mit Signalensemble $\{x_i, p_i\}$ vorliegen. Die zugeordnete Entropie ist $H(\tilde{p})$. Alice hat mit Bob, der das Signalensemble kennt, vorher vereinbart, wie die typischen Sequenzen digital mit Zahlen der Länge $nH(\tilde{p})$ durchnummeriert werden. Wie wir in Abschn. 5.2.2 gezeigt haben, muss Bob an Alice dann $nH(\tilde{p})$ Ja-Nein-Fragen stellen, um zu erfahren welches die Nummer des Ausgangstextes und damit welcher Text der Ausgangstext selber ist. Damit ergibt sich eine *operationale Interpretation der Entropie*: *Die Shannon-Entropie $H(\tilde{p})$ ist die mittlere Zahl der benötigten Ja-Nein-Fragen pro Buchstabe des Ausgangstextes.* Je kleiner die Shannon-Entropie $H(\tilde{p})$ ist, desto weniger Fragen muss Bob stellen. Es ist also sinnvoll $H(\tilde{p})$ als den *Informationsgehalt pro Buchstabe des Ausgangstextes* zu bezeichnen. Hat das Signalensemble $\{x_i, p_i\}$ mit $i = 1, \dots, N$ z. B. nur einen einzigen Buchstaben ($N = 1$), dann kennt Bob den Text bereits. Er muss gar keine Fragen mehr stellen. Dem entspricht $H(\tilde{p}) = 0$ (vgl.

³ [Sha 48], [Sha 49]

Gl. (5.7)). Wie Gl. (5.8) zeigt, muss Bob die meisten Fragen pro Buchstabe stellen – nämlich $\log N$ – wenn die Wahrscheinlichkeiten p_i gleich verteilt sind: $p_1 = p_2 = \dots = p_N = N^{-1}$.

5.4 Klassische relative Entropie

Gibbs-Ungleichung Es ist für viele Beweise nützlich für zwei Wahrscheinlichkeitsverteilungen $\{p_i\}$ und $\{q_i\}$ zum selben Alphabet $\{x_i\}$ als Hilfsmittel die *klassische relative Entropie* $H(\tilde{p}||\tilde{q})$ von $\{p_i\}$ relativ zu $\{q_i\}$ einzuführen und ihre Eigenschaften auszunutzen.

$$H(\tilde{p}||\tilde{q}) := \sum_{i=1}^N p_i \log \frac{p_i}{q_i} = -H(\tilde{p}) - \sum_{i=1}^N p_i \log q_i . \quad (5.24)$$

Mit Hilfe der die Logarithmen verknüpfenden fundamentalen Ungleichung für alle positiven x

$$\log x \ln 2 = \ln x \leq x - 1 \quad (5.25)$$

können wir $H(\tilde{p}||\tilde{q})$ abschätzen

$$\begin{aligned} H(\tilde{p}||\tilde{q}) &= - \sum_{i=1}^N p_i \log \frac{q_i}{p_i} \\ &\geq \frac{1}{\ln 2} \sum_{i=1}^N p_i \left(1 - \frac{q_i}{p_i}\right) \\ &= \frac{1}{\ln 2} \sum_{i=1}^N (p_i - q_i) = 0. \end{aligned} \quad (5.26)$$

Diese Ungleichung wird *Gibbs-Ungleichung* genannt. Die *relative Entropie* $H(\tilde{p}||\tilde{q})$ ist nicht negativ. Sie ist gleich Null genau dann wenn $p_i = q_i$ für alle i gilt (identische Verteilungen).

Konkavität Dass die Shannon-Entropie eine konkave Funktion ist, ist eine direkte Konsequenz der Gibbs-Ungleichung. Wenn \tilde{p}_1 und \tilde{p}_2 zwei Wahrscheinlichkeitsverteilungen mit Wahrscheinlichkeiten $\{p_{1i}\}$ und $\{p_{2i}\}$ sind, dann gilt für die Verteilung $\tilde{p} = \lambda \tilde{p}_1 + (1 - \lambda) \tilde{p}_2$ mit Wahrscheinlichkeiten $\{p_i = \lambda p_{1i} + (1 - \lambda) p_{2i}\}$ und $0 < \lambda < 1$

$$H(\lambda \tilde{p}_1 + (1 - \lambda) \tilde{p}_2) \geq \lambda H(\tilde{p}_1) + (1 - \lambda) H(\tilde{p}_2) . \quad (5.27)$$

Die Gleichheit gilt genau dann, wenn die Verteilungen \tilde{p}_1 und \tilde{p}_2 identisch sind. Das heißt, wenn man über zwei Wahrscheinlichkeitsverteilungen mittelt, dann erhöht sich die Entropie. Der Beweis folgt aus der Gibbs-Ungleichung (5.26) durch Ausschreiben der Terme mit Hilfe von Gl. (5.24):

$$0 \leq \lambda H(\tilde{p}_1||\tilde{p}) + (1 - \lambda) H(\tilde{p}_2||\tilde{p}) = H(\tilde{p}) - \lambda H(\tilde{p}_1) - (1 - \lambda) H(\tilde{p}_2) . \quad (5.28)$$

5.5 Wechselseitige Information als Maß für die Korreliertheit zweier Botschaften

Wir nehmen an, dass zwei Signalensemble $X \leftrightarrow \{x_i, p_i\}$ und $Y \leftrightarrow \{y_j, p_j\}$ vorliegen, deren Signale nicht unabhängig voneinander auftreten. Es sollen Korrelationen vorliegen. Wir wollen ein Maß für die Korreliertheit von Botschaften der beiden Signalensemble gewinnen. Zur Vereinfachung schreiben wir für die Ensemble $X \leftrightarrow \{x, p(x)\}$ und $Y \leftrightarrow \{y, p(y)\}$ sowie $\sum_i = \sum_y$ usw. Wir haben dann z. B. $H(\tilde{p}(x)) = H(X)$.

$p(y|x)$ ist die bedingte Wahrscheinlichkeit für das Auftreten von y , wenn x bereits aufgetreten ist. Wie wir in Abschn. 1.3 diskutiert haben gilt

$$p(y|x)p(x) = p(y, x) = p(x, y) . \quad (5.29)$$

$p(x, y)$ ist dabei die Wahrscheinlichkeit dafür, dass X und Y gemeinsam auftreten (joint probability). Die *mittlere Ungewissheit über das Auftreten eines Paares* (joint entropy) bei bekanntem Signalensemble $\{(x, y), p(x, y)\}$ der Paare ist

$$H(X, Y) := - \sum_{x, y} p(x, y) \log p(x, y) = H(Y, X) . \quad (5.30)$$

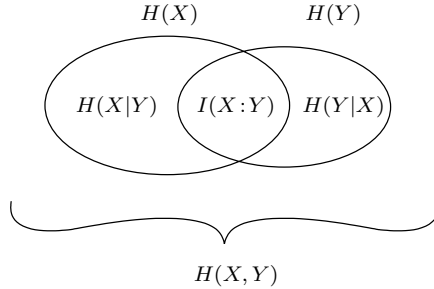


Abbildung 5.3: Mengentheoretische Veranschaulichung der verschiedenen Entropiearten.

5.5.1 Wechselseitige Information

Als *wechselseitige Information* (mutual information) führen wir die Größe

$$I(X:Y) := H(X) + H(Y) - H(X, Y) = I(Y:X) \quad (5.31)$$

ein mit den Entropien $H(X) := - \sum_x p(x) \log p(x)$ und $H(Y)$ der einzelnen Ensembles (vgl. Abb. 5.3). Wenn wir Gl. (5.31) nach $H(X, Y)$ auflösen

$$H(X, Y) = H(X) + H(Y) - I(X:Y) \quad (5.32)$$

sehen wir, dass $I(X:Y)$ angibt, um wie viel die Unbestimmtheit der Paare kleiner ist als die Summe der Unbestimmtheiten der beiden Ensembles. Dies ist ein sinnvolles Maß für die Korreliertheit der beiden Ensembles.

Wir geben ein Beispiel an. Alice besitzt nur Socken in grüner und blauer Farbe. Sie zieht aber immer Socken gleicher Farbe an. Bob weiß das und weiß noch darüber hinaus, dass Alice mit der Wahrscheinlichkeit $p(g) = \frac{1}{4}$ grüne und mit der Wahrscheinlichkeit $p(b) = \frac{3}{4}$ blaue Socken trägt. Die Ensemble $X \leftrightarrow L$ und $Y \leftrightarrow R$ beziehen sich auf den linken bzw. rechten Socken. Dann haben wir $p(g, g) = \frac{1}{4}$, $p(b, b) = \frac{3}{4}$, $p(g, b) = 0$, $p(b, g) = 0$ und damit

$$H(L, R) = H(L) = H(R) = -0,25 \log(0,25) - 0,75 \log(0,75) = 0,81 . \quad (5.33)$$

Bevor Bob z.B. auf den linken Socken schaut, ist seine Ungewissheit über die Farbe der rechten Socke gleich $H(R)$. Schaut er aber auf den linken Socken, dann ist diese Ungewissheit völlig beseitigt. Bob hat die Information

$$I(L : R) = H(R) \quad (5.34)$$

erhalten. Das wird gerade durch die Relation (5.31) zusammen mit Gl. (5.33) wiedergegeben. $I(L : R)$ wird am größten, nämlich $I(L : R) = 1$, für $p(g) = p(b) = \frac{1}{2}$. Die wechselseitige Information hängt wie alle Informationen vom Vorwissen ab. Wenn man sie als ein Maß für die Korreliertheit der beiden Signalensemble auffasst, sollte man das im Blick behalten.

Es ist instruktiv, sich die Interpretation von $I(X : Y)$ noch einmal auf andere Weise zu verdeutlichen.

5.5.2 Bedingte Entropie

Wir können die Entropie $H(X) = -\sum_x p(x) \log p(x)$ auch folgendermaßen interpretieren: $-\log p(x)$ ist die Ungewissheit für das Auftreten des Signals x . Gewichtung mit der Wahrscheinlichkeit $p(x)$ für das Auftreten und Summation über alle x führt zu $H(X)$ als mittlere Ungewissheit pro Signal. Mit der Wahrscheinlichkeit $p(x, y)$, dass sowohl x als auch y eintritt und der Ungewissheit $-\log p(x|y)$ des Auftretens von x , wenn y schon aufgetreten ist, bilden wir analog

$$H(X|Y) := -\sum_{x,y} p(x, y) \log p(x|y) \geq 0 . \quad (5.35)$$

Diese Größe ist, anders als bei $H(X, Y)$ von Gl. (5.30) bezogen auf die bedingte Wahrscheinlichkeit $p(x|y)$. $H(X|Y)$ heißt *bedingte Entropie* (conditional entropy). $H(X|Y)$ beschreibt wie unsicher wir (im Mittel) noch über den Wert von x sind, wenn wir y bereits kennen. Es handelt sich also um eine Restunsicherheit⁴

⁴Man kann die bedingte Entropie $H(X|Y)$ auch noch etwas anders einführen. Die verbliebene Entropie der Variablen X , wenn das spezielle Signal y empfangen wurde, ergibt sich im Mittel über die bedingte Wahrscheinlichkeit $p(x|y)$

$$H(X|y) = -\sum_x p(x|y) \log p(x|y) . \quad (5.36)$$

Mittelung über y führt mit (5.29) auf die bedingte Entropie $H(X|Y)$

$$H(X|Y) = -\sum_y p(y) \sum_x p(x|y) \log p(x|y) = -\sum_{x,y} p(x, y) \log p(x|y) . \quad (5.37)$$

Wir formen $H(X, Y)$ mit Gl. (5.29) um:

$$\begin{aligned}
 H(X, Y) &= - \sum_{x,y} p(x, y) \log p(x|y)p(y) \\
 &= - \sum_{x,y} p(x, y) \log p(y) - \sum_{x,y} p(x, y) \log p(x|y) \\
 &= - \sum_y p(y) \log p(y) + H(X|Y) .
 \end{aligned} \tag{5.38}$$

Damit ergibt sich

$$H(X|Y) = H(X, Y) - H(Y) \quad \text{und} \quad H(Y) \leq H(X, Y) . \tag{5.39}$$

Die Unsicherheit für Paare $H(X, Y)$ verringert sich zur Restunsicherheit $H(X|Y)$, wenn die Information $H(Y)$ über das y -Signal vorliegt. Analoge Relationen gelten bei Vorliegen des x -Signals. In unserem Sockenbeispiel ist die Restunsicherheit gleich Null. Die Abb. 5.3 gibt die Bezeichnungen der verschiedenen Entropiekonzepte in anschaulicher Weise geometrisch wieder.

Die Gleichungen (5.31) und (5.39) führen auf

$$H(X|Y) = H(X) - I(X : Y) . \tag{5.40}$$

Die Unsicherheit über x wenn y aufgetreten ist, verringert sich gegenüber der a-priori-Unsicherheit über das Auftreten von x , wenn Korrelationen zwischen den Ensembles X und Y vorliegen. Man kann $I(X : Y)$ auch als die mittlere Information interpretieren, die man über den Wert von X erhält, wenn der Wert von Y bekannt ist und umgekehrt ($I(X : Y) = I(Y : X)$). Die wechselseitige Information $I(X : Y)$ ist ein Maß für die Korreliertheit des Ensembles. Wir werden auf Korrelationen in Kap. 9 im Zusammenhang mit verschränkten Quantensystemen zurückkommen.

Subadditivität Abschließend erwähnen wir noch, dass man mit Hilfe der Konvexität der Logarithmus-Funktion die Ungleichung

$$H(X) \geq H(X|Y) \geq 0 \tag{5.41}$$

beweisen kann. Dann folgt mit Gl. (5.40), dass die wechselseitige Information nicht negativ sein kann

$$I(X : Y) \geq 0 . \tag{5.42}$$

Eine Information über Y kann das Wissen über X nicht verringern und umgekehrt. Gleichheit gilt genau dann, wenn X und Y unabhängig sind. Gl. (5.31) führt als unmittelbare Konsequenz auf die *Subadditivität* (subadditivity) der Entropie

$$H(X, Y) \leq H(X) + H(Y) . \tag{5.43}$$

5.6 Ergänzende Themen und weiterführende Literatur

Siehe auch Abschn. 6.6.

- Übersichtsartikel: [Ved 02], [Ste 98], [Weh 78].

5.7 Übungsaufgaben

ÜA 5.1 [zu 5.2] Notieren Sie die möglichen Botschaften der Länge $n = 4$ aus den Binärzahlen 0 und 1 (d. h. $N = 2$). Demonstrieren Sie wie bei Annäherung von p_0 an 1 und p_1 an 0 sich die Anzahl der typischen Sequenzen ändert. Wie verhält sich die Wahrscheinlichkeit der typischen Sequenzen? Was passiert für wachsende Länge n ?

ÜA 5.2 [zu 5.5.2] Beweisen Sie die Subadditivität (5.43) mit Hilfe der Gibbs-Ungleichung (5.26).

ÜA 5.3 [zu 5.5.2] Beweisen Sie die Ungleichungen

$$H(X) \geq H(X|Y) \geq 0 . \quad (5.44)$$

ÜA 5.4 [zu 5.5.2] Zeigen Sie, dass die wechselseitige Information $I(X : Y)$ genau dann verschwindet, wenn X und Y unabhängig sind, d. h. wenn $p(x, y) = p(x)p(y)$ gilt.

This Page Intentionally Left Blank

6 Von-Neumann-Entropie und Quanteninformation

6.1 Quantenkanal und Quantenentropie

Quantenkanal Wir betrachten die folgende physikalische Situation (vergl. Tab. 6.1):

Eine klassische Signalquelle erzeugt nacheinander die Buchstaben einer Zeichenfolge. Wie wir gesehen haben, kann diese Signalquelle durch ein Ensemble $\{x_i, p_i\}$ mit $i = 1, \dots, N$ beschrieben werden. Die Botschaft soll durch einen *Quantenkanal* übertragen werden. Dabei übernehmen gleichartige Quantenobjekte (z. B. Atome derselben Sorte mit Spin $\frac{1}{2}$ oder Photonen) die Rolle der Träger eines quantentheoretischen Signalalphabets. Dazu wird zu jedem Buchstaben x_i ein Präparationsgerät mit der Nummer i tätig, das ein einzelnes Exemplar des Quantensystems im *Signalzustand* $|\psi_i\rangle$ (signal state) erzeugt und abschickt (vergl. Abb. 4.1 mit Abb. 5.1). Der Zusammenhang zwischen Buchstabe x_i und Zustand $|\psi_i\rangle$ soll eindeutig sein. Die Gesamtanlage heißt *Quantensignalquelle* (quantum signal source). Durch Präparation wird so die klassische Information in reinen Quantenzuständen kodiert. An dieser ersten Schnittstelle wird ein statistisches Gemisch aus Signalzuständen mit Dichteoperator

$$\rho = \sum_{i=1}^N p_i |\psi_i\rangle \langle \psi_i| \quad (6.1)$$

auf einem Hilbert-Raum \mathcal{H}_d der Dimension d erzeugt. Der Dichteoperator ρ (auch Zustand ρ genannt) bezeichnet wieder ein Präparationsverfahren. Das zugehörige Ensemble ist das *Quantensignalensemble* $\{|\psi_i\rangle, p_i\}$. Wichtig ist, dass wir i. a. nicht verlangen, dass die normierten Zustandsvektoren $|\psi_i\rangle$ orthogonal sind. Weiterhin muss die Dimension d nicht mit N übereinstimmen, N kann z. B. größer sein. Der übertragende Quantenkanal soll störungsfrei und nach außen abgeschlossen sein. Das Quantensignalensemble soll also der Einfachheit halber im Kanal unverändert bleiben.

An einer zweiten Schnittstelle wird versucht durch projektive Messung die ursprünglich von der Signalquelle ausgesandte Information wieder auszulesen. Dazu wird am Gemisch ρ eine Detektorobservable D gemessen. Die orthonormalen Eigenzustände $\{|d_m\rangle, m = 1, \dots, d\}$ der Observablen D

$$D|d_m\rangle = d_m|d_m\rangle \quad (6.2)$$

bilden eine ONB von \mathcal{H}_d . Die zugehörigen Eigenwerte d_m sollen nicht entartet sein. Damit ist die Zuordnung zwischen Messwert d_m und Zustand $|d_m\rangle$ nach der Messung eineindeutig.

Tabelle 6.1: Klassische Information wird in Quanteninformation kodiert. Durch Messung entsteht wieder klassische Information.

<p>Signalensemble</p> $\{x_i, p_i\}, i = 1, \dots, N$	<p>1. Schnittstelle:</p> <p>klassischer Träger → Quantenträger</p>	<p>2. Schnittstelle:</p> <p>Quantenträger → klassischer Träger</p> <p>Messwert-Ensemble $\{d_m, p(d_m)\}, H(\tilde{p}(d))$</p>
<p>Entropie: $H(\tilde{p}(x))$</p>	<p>Kodieren in $\psi_i\rangle \in \mathcal{H}_d$</p> $\{x_i, p_i\} \rightarrow \{ \psi_i\rangle, p_i\}$ $\rho = \sum_{i=1}^N p_i \psi_i\rangle \langle \psi_i $ <p>Spektrale Zerlegung:</p> $\rho = \sum_{m=1}^d \lambda_m m\rangle \langle m $ $\langle l m\rangle = \delta_{lm}$	<p>Auslesen: Messen der Detektorobservablen D.</p> $D d_m\rangle = d_m d_m\rangle$ $m = 1, \dots, d$
		<p>Messwert d_m mit Wahrscheinlichkeit</p> $p(d_m) = \text{tr}[\rho d_m\rangle \langle d_m]$
		<p>Zustände $d_m\rangle \in \mathcal{H}_d$ nach der Messung: $\langle d_l d_m\rangle = \delta_{lm}$</p>
		<p>Nicht selektiv:</p> $\rho \xrightarrow{n.s.} \rho' = \sum_{m=1}^d p(d_m) d_m\rangle \langle d_m $
	<p>$H(\tilde{p}(x)) \geq S(\rho)$</p>	<p>$S(\rho') = H(\tilde{p}(d)), \quad S(\rho') \geq S(\rho)$</p>

Die Wahrscheinlichkeit, mit der der Messwert d_m bei einer Messung an ρ auftritt, nennen wir $p(d_m)$. Die Signalübertragung durch einen Quantenkanal spiegelt das Grundscheema der Quantentheorie wieder: Am Anfang steht eine Zustandspräparation und am Ende eine Messung. Eingegeben wird eine Sequenz klassischer Signale mit einer Shannon-Entropie $H(\tilde{p})$ und ausgelesen wird eine Sequenz von Messwerten mit Shannon-Entropie $H(\tilde{p}(d))$.

Zur Vervollständigung der Beschreibung notieren wir noch die spektrale Zerlegung des Dichteoperators ρ :

$$\rho = \sum_{m=1}^d \lambda_m |m\rangle \langle m|, \quad \langle m|m'\rangle = \delta_{mm'} \quad (6.3)$$

mit den Eigenvektoren $|m\rangle$ und den Eigenwerten λ_m . Auch die $\{|m\rangle, m = 1, \dots, d\}$ bilden eine ONB von \mathcal{H}_d , die auch die *Eigenbasis* von ρ genannt wird.

Von-Neumann-Entropie Wir betrachten zunächst eine spezielle Situation, in der die eingegebene klassische Information ohne Verlust wieder ausgelesen werden kann. Das Quantensystem wird hierfür so gewählt, dass die Dimension d von \mathcal{H}_d mit der Anzahl N der Buchstaben im klassischen Signalensemble übereinstimmt. An der ersten Schnittstelle werden durch geeignete Wahl des Präparationsverfahrens zu den Buchstaben x_i in eindeutiger Abbildung speziell die orthonormalen Eigenzustände der Detektorobservablen D erzeugt (d. h. $|\psi_i\rangle = |d_i\rangle$).

$$\rho = \sum_i^N p_i |d_i\rangle \langle d_i| = \sum_i^N \lambda_i |i\rangle \langle i|. \quad (6.4)$$

Wir haben in diesem Fall also $p_i = \lambda_i$ und $|d_i\rangle = |i\rangle$. Die Quantensignalquelle wird wegen der Unterscheidbarkeit der Signalzustände zu einer quasi-klassischen Quelle. Schließlich wird an der zweiten Schnittstelle die Observable D gemessen. Am Eintreten des Messwerts d_i kann dann wegen der Unterscheidbarkeit eindeutig auf das ursprüngliche Vorliegen des Signalbuchstabens x_i geschlossen werden. Alle beteiligten Wahrscheinlichkeitsverteilungen stimmen überein: $p(d_i) = p_i = \lambda_i$. Entsprechend erhalten wir für die Shannon-Entropie des Signalensembles und des Messwertensembles $H(\tilde{p}) = H(\tilde{p}(d))$.

Die in dieser speziellen quasi-klassischen Situation vorliegende eindeutige Beziehung zwischen den Ensembles $\{x_i, p_i\}$, $\{|\psi_i\rangle, p_i\}$ und $\{d_i, p(d_i)\}$ und entsprechend die Übereinstimmung der drei Wahrscheinlichkeitsverteilungen legen es nahe, dem statistischen Gemisch mit Dichteoperator ρ von Gl. (6.4) eine *Quantenentropie* $S(\tilde{\lambda})$ mit dem Wert der Shannon-Entropie zuzuordnen ($S(\tilde{\lambda}) = H(\tilde{p})$):

$$S(\tilde{\lambda}) = - \sum_{i=1}^d \lambda_i \log \lambda_i \geq 0. \quad (6.5)$$

Mit der Spektralzerlegung von ρ von Gl. (6.3) lässt $S(\tilde{\lambda})$ sich als Funktion des Dichteoperators ρ schreiben

$$S(\rho) := S(\tilde{\lambda}) = -\text{tr}[\rho \log \rho] \geq 0. \quad (6.6)$$

Die Quantenentropie $S(\rho)$ heißt auch die *von-Neumann-Entropie*¹ *des Gemisches mit Dichteoperator* ρ . Die Einheit dieser Entropie ist Quantenbit oder ein *Qubit*. Wir werden diese Bezeichnung im nächsten Kapitel begründen.

Da $S(\rho)$ bei Vorgabe von ρ eindeutig bestimmt ist, kann man sich von dem oben beschriebenen speziellen Schema einer Informationsübertragung lösen und auch in physikalischen Situationen, in denen gar keine Signalübertragung oder -verarbeitung vorliegt, jedem Dichteoperator ρ und damit jedem Quantenzustand seine von-Neumann-Entropie $S(\rho)$ gemäß Gl. (6.6) zuordnen. $S(\rho)$ charakterisiert einen Dichteoperator ρ unabhängig davon wie das zugehörige Gemisch physikalisch präpariert wurde. Ein Zustand ρ mit spektraler Zerlegung (6.3) kann hinsichtlich aller Wahrscheinlichkeitsaussagen nicht vom statistischen Gemisch der Zustände der Eigenbasis mit Ensemble $\{|m\rangle, \lambda_m\}$ unterschieden werden. Mit diesem statistischen Gemisch wird pro Signalfeld im Mittel die klassische Information $H(\tilde{\lambda}) = S(\rho)$ übertragen. Wir werden $S(\rho)$ allgemein als Informationsgehalt eines Zustands ρ auffassen.

Messung der von-Neumann-Entropie Es reicht hierfür, ρ zu bestimmen und die Eigenwerte abzulesen. Das wird besonders einfach wenn die Eigenzustände $\{|m\rangle\}$ von ρ bekannt sind. Messungen in der Eigenbasis von ρ sind besonders günstig. Sie führen auf die Wahrscheinlichkeiten

$$p(d_m) = \lambda_m, \quad (6.7)$$

mit denen sich die von-Neumann-Entropie von ρ bestimmen lässt:

$$S(\rho) = - \sum_{m=1}^d p(d_m) \log p(d_m) = H(\tilde{p}(d)). \quad (6.8)$$

6.2 Qubit als Einheit der Quanteninformation

Unter *Quanteninformation* (quantum information) wollen wir die Information verstehen, die durch den Zustand eines Quantensystems repräsentiert wird und mit Hilfe von Quantensystemen als Träger übermittelt wird. Dabei ist der Sender ein Präparationsgerät und der Empfänger ein Messgerät. Dies sind die Schnittstellen für die Übergänge klassische \rightarrow quantentheoretische bzw. quantentheoretische \rightarrow klassische Information. Nur die klassische Information ist eine Information, die wir direkt ablesen können.

Wir nehmen an, dass eine klassische Sequenz aus N Buchstaben des Signalensembles $\{x_i, p_i\}$ mit Entropie $H(\tilde{p})$ in N Quantenzustände aus dem Quantensignalensemble $\{|\psi_i\rangle, p_i\}$ mit Entropie $S(\rho) = H(\tilde{p})$ umkodiert wird. Die Ensemblezustände $\{|\psi_i\rangle\}$ sollen orthonormal sein. Die Ursprungssequenz kann durch Messen in der ONB $\{|\psi_i\rangle\}$ vollständig ausgelesen werden. Wie wir bereits gesehen haben, kann man die klassische Sequenz auch in nH Buchstaben eines binären Codes kodieren, die in einer Sequenz von nH quantentheoretischen 2-Niveau-Systemen (Qubit-Systemen) mit Zuständen $|0\rangle$ und $|1\rangle$ übermittelt und eindeutig ausgelesen werden können. Die übertragene Information pro Buchstabe ist H (gemessen in

¹ [vNe 68]

bits). Pro einzeltem übermitteltem Signalzustand $|\psi_i\rangle$ hätte man wegen $H(\tilde{p}) = S(\rho)$ im Mittel also auch eine Anzahl $S(\rho)$ von 2-Niveau-Systemen in wohlbestimmten Zuständen (z. B. $|0\rangle$ oder $|1\rangle$) übermitteln können. Die von-Neumann-Entropie $S(\rho)$ eines Ensembles orthogonaler Quantenzustände ist also gerade die mittlere Zahl von 2-Niveau-Systemen, die nötig ist, um die Zustände des Ensembles zu kodieren.

Die obige Aussage geht nicht über das Theorem von Shannon hinaus. Da die Zustände $\{|\psi_i\rangle\}$ orthogonal sind, hätte man nach Auslesen der Ursprungssequenz durch Messung an ρ die Information dem Empfänger auch klassisch übertragen können und der hätte mit dieser Information die Sequenz der Quantenzustände präparieren können. Im allgemeinen Fall sind die Signalzustände aber nicht orthogonal. Sie können durch Messung nicht eindeutig bestimmt werden. Die Informationsübermittlung über einen klassischen Kanal führt nicht zum Ziel. Die einfachste Lösung ist es in diesem Fall, die Signalzustände selber durch einen Quantenkanal zu übertragen, der die Zustände der Quantensysteme nicht beeinflusst. Dabei würde allerdings keine Datenkompression stattfinden.

Es ist die Aufgabe, eine Sequenz von Quantenzuständen $|\psi_1\rangle, \dots, |\psi_n\rangle$ aus einem gegebenen Signalensemble mit möglichst wenigen Quantensystemen zu übertragen. Man kann zeigen [Sch 95], dass sich eine solche Sequenz *ohne Bezug auf klassische Information* in unitärer Weise so komprimieren lässt, dass sie beim Empfänger mit asymptotisch perfekter Treue (Übereinstimmung mit dem Ausgangszustand) mit Hilfe einer unitären Transformation wieder zurückgewonnen werden kann. Hierzu werden Qubit-Systeme als quantentheoretische Trägersysteme verwendet. *Die mittlere Zahl der benötigten Qubit-Systeme pro Signalzustand bei optimaler Kompression stimmt mit der von-Neumann-Entropie des durch den Dichteoperator beschriebenen Signalensembles $\{|\psi_i\rangle, p_i\}$ überein.* Dieses Theorem ist das quantentheoretische Analogon zum Shannon-Theorem. Es ist von Schumacher in präziserer Form mit Hilfe von *Quantendatenkompression* (quantum data compression) abgeleitet worden und heißt auch *Schumachers quantum noiseless coding theorem*. Wir können die Aussage an dieser Stelle nicht beweisen, da im Beweis die Sequenz von Quantenzuständen als ein Produktzustand eines großen zusammengesetzten Systems aufgefasst wird. Solche Quantensysteme werden wir erst im nächsten Kapitel kennenlernen. Wir verweisen für den nicht ganz einfachen Beweis² auf die Literatur (vergl. Abschn. 6.6). Die Einheit der Quantenentropie $S(\rho)$ wird *Qubit* genannt. Ein Quantensystem mit zwei Niveaus (z. B. $|0\rangle$ und $|1\rangle$), durch das man gerade ein Qubit an Information kodieren kann, wird selber auch als Qubit (oder Qubit-System) bezeichnet.

Wir wollen die klassische Übertragung von Quanteninformation mit der quantentheoretischen vergleichen. Das Signalensemble möge aus den Zuständen

$$|\psi_0\rangle = |0\rangle, |\psi_1\rangle = |0_x\rangle \quad (6.9)$$

²Der Beweis ähnelt dem von Shannon in Abschn. 5.2, der auf der Idee der typischen Sequenzen beruht. Wenn wir uns auf Qubit-Systeme beschränken, dann sind die Signalzustände $|\psi_i\rangle$ Zustände in \mathcal{H}_2 , die nicht notwendig orthogonal sein müssen. Wir fassen die n Systeme einer langen Sequenz zu einem zusammengesetzten System mit einem Zustandsvektor im 2^n -dimensionalen Produktraum zusammen. Dann lässt sich Folgendes zeigen (vergl. Abschn. 6.6): Wenn das Signalensemble $\{|\psi_i\rangle, p_i\}$ eine von-Neumann-Entropie $S(\rho) < 1$ hat, dann ist die (mit n anwachsende) Wahrscheinlichkeit groß, dass der Zustandsvektor in einem vom Ensemble abhängigen *typischen Unterraum* (typical subspace) des Produktraums liegt. Dessen Dimension ist $2^{nS(\rho)}$. Es reichen daher Produktzustände aus $nS(\rho)$ Qubit-Zuständen aus, um solche Zustandsvektoren darzustellen. Entsprechend werden nur $nS(\rho)$ Qubit-Systeme als Träger zur Übermittlung benötigt. Aus ihrem Gesamtzustand kann die Ausgangssequenz durch eine unitäre Transformation rekonstruiert werden. Der Fehler nimmt dabei mit wachsendem n ab.

bestehen, die mit den Wahrscheinlichkeiten

$$p_1 = p_2 = \frac{1}{2} \quad (6.10)$$

auftauchen. Bei klassischer Übermittlung der Information ist wegen $H(p_1, p_2) = 1$ Bit keine Datenkompression möglich. Für eine Sequenz von n Quantenzuständen werden nach Umkodieren n klassische Träger für jeweils 1 Bit benötigt. Die von-Neumann-Entropie ergibt sich über den Dichteoperator

$$\rho = p_0 |\psi_0\rangle\langle\psi_0| + p_1 |\psi_1\rangle\langle\psi_1| = \begin{pmatrix} \frac{3}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} \end{pmatrix}. \quad (6.11)$$

Die Matrix bezieht sich auf die Rechenbasis. Die Eigenwerte lassen sich bestimmen ($\lambda_0 = \cos^2 \frac{\pi}{8} = 0,853$, $\lambda_1 = \sin^2 \frac{\pi}{8} = 0,146$) und führen mit Gleichung (6.5) auf $S(\rho) = 0,601$ Qubits (vergl. Abschn. 6.7). Zur Übermittlung einer Sequenz von Zuständen des Signalensembles benötigen wir daher nur 0,601 Qubit-Systeme pro Zustand. *Dies belegt, dass die Quantenkompression mit Quantenkodieren in Qubit-Systeme ein nützliches Hilfsmittel bei der Übertragung von Quanteninformation ist. Insbesondere erhält durch dieses Ergebnis die von-Neumann-Entropie eine operationale Interpretation, die keinen Bezug mehr auf die klassische Entropie enthält.* Das Qubit ist eine sinnvolle Einheit für Quanteninformation. Hervorzuheben ist noch, dass das Kompressionsverfahren von Schumacher zu gegebenem Signalensemble universell ist. Zu seiner Durchführung muss man den zu übermittelnden Zustand nicht kennen.

6.3 Eigenschaften

Mit Bezug auf Gl. (6.8) lässt sich in Analogie zur Shannon-Entropie direkt zeigen:

- (i) Ein reiner Zustand $\rho = |\psi\rangle\langle\psi|$ hat den Minimalwert der Entropie $S(\rho) = 0$.
- (ii) Für einen Dichteoperator mit d nicht verschwindenden Eigenwerten findet man

$$0 \leq S(\rho) \leq \log d. \quad (6.12)$$

Das Gleichheitszeichen gilt, wenn alle nicht verschwindenden Eigenwerte übereinstimmen. Der vollständig gemischte Zustand $\rho = \frac{1}{d}\mathbf{1}$ im Hilbert-Raum der Dimension d hat die maximale von-Neumann-Entropie $S(\rho) = \log d$.

- (iii) Als Folge der Konkavität der Shannon-Entropie gilt auch für die von Neumann-Entropie für $p_j > 0$ mit $\sum_j p_j = 1$ die Konkavitätsrelation

$$S(p_1\rho_1 + \dots + p_r\rho_r) \geq p_1S(\rho_1) + \dots + p_rS(\rho_r). \quad (6.13)$$

Zum Beweis geht man zur Spektralzerlegung der ρ_j über. $\sum_j p_j \rho_j$ ist der Zustand eines Quantensystems, das sich mit der Wahrscheinlichkeit p_j im unbekannten Zustand ρ_j befindet. Das Ergebnis ist plausibel. Es sind mehrere Ensembles zusammengeführt worden bzw. die zugehörigen Ensemblezerlegungen sind gemischt worden. Unser Unwissen über dieses Gemisch ist größer als das mittlere Unwissen über die Zustände ρ_j . Die Information darüber, von welchem Gemisch ein Zustand kommt, ist verloren gegangen. Die Entropie ist größer, weil wir weniger über die Präparation wissen. Mit (i) folgt speziell

$$S(\rho) > 0, \quad (6.14)$$

wenn ρ kein reiner Zustand ist.

Unitäre Dynamik Allgemein gilt bei einer unitären Transformation des Dichteoperators

$$S(U\rho U^\dagger) = S(\rho), \quad (6.15)$$

da S nur von den Eigenwerten von ρ abhängt. Die Entropie ist also – unabhängig davon welches Bild man für die unitäre dynamische Entwicklung wählt – immer zeitunabhängig:

$$\frac{dS}{dt} = 0. \quad (6.16)$$

Unsere Information über einen Zustand ändert sich während der unitären dynamischen Entwicklung nicht. Das ist anders in der Messdynamik.

Quantentheoretische relative Entropie und Kleinsche Ungleichung Sie wird uns in erster Linie als mathematische Hilfsgröße dienen. Wir betrachten zwei Dichteoperatoren ρ und σ und führen die *quantentheoretische relative Entropie* $S(\rho||\sigma)$ von ρ bezüglich σ ein:

$$S(\rho || \sigma) := \text{tr}[\rho \log \rho] - \text{tr}[\rho \log \sigma]. \quad (6.17)$$

Wie im analogen klassischen Fall wollen wir eine Abschätzung ableiten. Die orthogonalen Zerlegungen von ρ und σ seien durch Gl. (6.3) und

$$\rho = \sum_{m=1}^d \lambda_m |\phi_m\rangle \langle \phi_m|, \quad \sigma = \sum_{m=1}^d \kappa_m |\xi_m\rangle \langle \xi_m| \quad (6.18)$$

gegeben. Daraus folgt:

$$S(\rho||\sigma) = \sum_m \lambda_m \log \lambda_m - \sum_m \langle \phi_m | \rho \log \sigma | \phi_m \rangle. \quad (6.19)$$

Mit $\langle \phi_m | \rho = \lambda_m \langle \phi_m |$ schreiben wir den zweiten Term um

$$\langle \phi_m | \log \sigma | \phi_m \rangle = \langle \phi_m | \left(\sum_{m'} \log \kappa_{m'} |\xi_{m'}\rangle \langle \xi_{m'}| \right) | \phi_m \rangle = \sum_{m'} P_{mm'} \log \kappa_{m'}. \quad (6.20)$$

Hierbei haben wir

$$P_{mm'} := \langle \phi_m | \xi_{m'} \rangle \langle \xi_{m'} | \phi_m \rangle \quad (6.21)$$

mit den Eigenschaften $P_{mm'} \geq 0$, $\sum_m P_{mm'} = 1$ und $\sum_{m'} P_{mm'} = 1$ eingeführt. Wir schreiben Gl. (6.19) weiter um.

$$S(\rho\|\sigma) = \sum_m \lambda_m (\log \lambda_m - \sum_{m'} P_{mm'} \log \kappa_{m'}). \quad (6.22)$$

Der Logarithmus ist eine konkave Funktion, daher gilt $\sum_{m'} P_{mm'} \log \kappa_{m'} \leq \log \mu_m$ mit $\mu_m := \sum_{m'} P_{mm'} \kappa_{m'}$. Mit Gl. (6.22) überträgt sich diese Ungleichung

$$S(\rho\|\sigma) \geq \sum_m \lambda_m \log \frac{\lambda_m}{\mu_m}. \quad (6.23)$$

Die rechte Seite stimmt formal mit einer klassischen relativen Entropie überein. Das führt auf die *Kleinsche Ungleichung*:

$$S(\rho\|\sigma) \geq 0. \quad (6.24)$$

Die quantentheoretische relative Entropie ist nicht negativ. Sie verschwindet genau dann, wenn $\rho = \sigma$ (übereinstimmende Zustände). Wie sein klassisches Gegenstück werden wir diesen Satz in erster Linie als Hilfssatz verwenden.

6.4 Die Schnittstellen von Präparation und Messung

In Kapitel 6.1 haben wir ideal angepasst präpariert und ideal angepasst ausgelesen. Abweichungen hiervon führen zu Informationsverlust. Woran liegt das und wie kann man das quantitativ fassen?

Bei Transport und Verarbeitung quantentheoretische kodierter Information wirken sich drei charakteristische Züge der Quantentheorie besonders aus, die in der klassischen Physik nicht zu finden sind: Das ist einmal der Umstand, dass nicht-orthogonale reine Zustände durch eine Messung nicht perfekt unterschieden werden können. Selbst orthogonale Zustände können durch eine Messung nur dann unterschieden werden, wenn die Eigenzustände des Observablenoperators mit ihnen übereinstimmen. Hinzu kommt als zweites, dass eine Quantenmessung i.a. den Zustand abändert. Ein dritter Punkt ist die Mehrdeutigkeit der Ensemblezerlegung eines Dichteoperators. Das hat umgekehrt zur Folge, dass es viele klassische Ensembles mit unterschiedlichen Shannon-Entropien gibt, die nach der Kodierung an der ersten Schnittstelle auf den gleichen Dichteoperator führen und dann durch keine Messung mehr unterscheidbar sind. Die von-Neumann-Entropie des Zustands ρ ist aber über seine orthogonale Zerlegung bestimmt, die nur genau eins der klassischen Ensembles kodiert. Wir wollen die Konsequenzen näher diskutieren und beginnen mit der Messung, also mit der zweiten Schnittstelle von Tab. 6.1.

6.4.1 Entropie der projektiven Messung

Die Zustände im Quantenkanal werden durch den Dichteoperator ρ mit der von Neumann-Entropie $S(\rho)$ beschrieben. Die *nicht-selektive* Messung der Dekodierungsobservablen D führt auf eine Wahrscheinlichkeitsverteilung $\{p(d_m)\}$ der Messwerte d_m . Man kann die Messung als klassische stochastische Quelle mit dem Signalensemble $\{d_m, p(d_m)\}$ auffassen. Das

Signalensemble hat die Shannon-Entropie $H(\tilde{p}(d_m))$. Dabei ist $\{p(d_m)\}$ zugleich die Wahrscheinlichkeitsverteilung der Zustände $\{|d_m\rangle\}$, in die das System bei der nicht-selektiven Messung überführt wird. Als Ergebnis liegt ein Dichteoperator ρ' mit der orthogonalen Zerlegung

$$\rho' = \sum_{m=1}^d p(d_m) |d_m\rangle \langle d_m| = \sum_{m=1}^d P_m \rho P_m \quad (6.25)$$

vor. Für die Projektionsoperatoren gilt: $P_m^2 = P_m$ und $\sum_m P_m = 1$. Die Shannon-Entropie $H(\tilde{q})$ der Messwerte und die von-Neumann-Entropie $S(\rho')$ des Gemisches der Quantenzustände nach der Messung stimmen überein:

$$S(\rho') = H(\tilde{p}(d)) . \quad (6.26)$$

Die Kleinsche Ungleichung erlaubt es, die Quantenentropien $S(\rho)$ und $S(\rho')$ vor und nach der nicht-selektiven Messung zu vergleichen. Wir gehen von

$$0 \leq S(\rho \| \rho') = -S(\rho) - \text{tr}[\rho \log \rho'] \quad (6.27)$$

aus und betrachten den zweiten Term genauer:

$$\text{tr}[\rho \log \rho'] = \text{tr}\left[\left(\sum_m P_m\right) \rho \log \rho'\right] = \text{tr}\left[\sum_m P_m \rho \log(\rho') P_m\right] . \quad (6.28)$$

Wir haben $P_m^2 = P_m$ verwendet. Gl. (6.25) zeigt, dass $P_m \rho' = P_m \rho P_m = \rho' P_m$ gilt. Daher vertauscht P_m auch mit der Operatorfunktion $\log \rho'$ und wir finden

$$\begin{aligned} \text{tr}[\rho \log \rho'] &= \text{tr}\left[\sum_m P_m \rho P_m \log \rho'\right] \\ &= \text{tr}[\rho' \log \rho'] = -S(\rho') . \end{aligned} \quad (6.29)$$

Damit haben wir nach Einsetzen in Gl. (6.27) und mit Gl. (6.26) insgesamt das Ergebnis erhalten:

$$S(\rho') = H(\tilde{p}(d)) \geq S(\rho) . \quad (6.30)$$

Bei einer nicht-selektiven projektiven Messung stimmt die Quantenentropie des Zustandes ρ' nach der Messung nur dann mit der von-Neumann-Entropie des Zustandes ρ vor der Messung überein, wenn die Messung in der Eigenbasis von ρ erfolgt, sonst ist sie größer. Eine nicht-selektive Messung überführt daher i.a. in ein neues Signalensemble mit größerer Entropie und vernichtet auf diese Weise Information. Das gilt auch für eine selektive Messung. Man kann sich das an einem sehr einfachen Beispiel veranschaulichen. Der reine Zustand

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (6.31)$$

hat verschwindende Entropie. Nicht-selektive Messung in der Eigenbasis überführt in den total gemischten Zustand

$$\rho = \frac{1}{2} \mathbb{1} \quad (6.32)$$

mit maximaler Entropie $S(\rho) = 1$.

6.4.2 Entropie der Präparation

Bei der Quantenkodierung wird die klassische Signalquelle mit Ensemble $\{x_i, p_i\}$ in das Quantenensemble $\{|\psi_i\rangle, p_i\}$, beschrieben durch den Dichteoperator ρ von Gl. (6.1), umkodiert (vergl. Tab. 6.1). Wegen der fehlenden Eindeutigkeit der Ensemblezerlegung von ρ führen verschiedene klassische Ensembles mit vielen verschiedenen Entropiewerten H auf Quantenensembles mit demselben Dichteoperator ρ und damit auf dieselbe von-Neumann-Entropie $S(\rho)$. Der Maximalwert der Quantenentropie ist über Gl. (6.12) durch die Dimension des Hilbert-Raums des Quantensystems gegeben, in dessen Zuständen kodiert wird. Der Maximalwert der *Präparationsentropie* $H(\tilde{p})$ ist durch die Zahl N der Buchstaben im klassischen Alphabet x_i gegeben. Sie stimmt mit der Zahl der Zustandsvektoren $|\psi_i\rangle$ überein, die größer als die Zahl der Basisvektoren von H_d sein kann, da die $|\psi_i\rangle$ nicht orthogonal sein müssen. Wir werden eine Relation der Form

$$H(\tilde{p}) \geq S(\rho) \quad (6.33)$$

erwarten. Sie lässt sich tatsächlich in einem längeren Beweis bestätigen (vergl. [Weh 78, S. 238] oder [CD 94, S. 527]). In Gl. (6.33) besteht Gleichheit genau dann, wenn die Zustände $|\psi_i\rangle$ wechselseitig orthogonal sind. *Wenn die Signalzustände nicht orthogonal sind, können sie nicht unterschieden werden. Es gibt keine Dekodierungsobservable mit deren Hilfe der volle Informationsgehalt der kodierten klassischen Botschaft wieder ausgelesen werden könnte.* Durch ρ wird weniger Information übermittelt als das ursprüngliche klassische Signal enthält. Auch mit optimal angepasster anschließender Messung kann die Information nicht zurückgewonnen werden.

6.5 Quanteninformation

Wir fassen zusammen: In der klassischen Informationstheorie kann man davon absehen, wie der Träger der Information physikalisch realisiert ist. Gedruckte Buchstaben können z. B. ohne Fehler in die Laute gesprochener Buchstaben konvertiert werden und umgekehrt. Wie wir gesehen haben, kann Quanteninformation im Allgemeinen nicht verlustfrei in klassische Information und zurück übertragen werden. Die Ursache liegt unter anderem in der nicht-klassischen Struktur des Messprozesses. *Quanteninformation ist daher eine von der klassischen Information i.a. sehr verschiedene Art von Information, ähnlich wie ein Quantenzustand eine andere Art von Zustand ist als der Zustand eines klassischen Systems.*

Quanteninformation wird in Quantenzuständen gespeichert. Ihre Träger sind Quantensysteme. Ihre Übermittlung besteht darin, dass die Träger zwischen Präparations- und Messgerät propagieren. Die Verarbeitung von Quanteninformation besteht in der Manipulation von Quantenzuständen. Unitäre Transformationen sind hierfür ein Beispiel. Den beiden Informationstypen sind verschiedene Informationseinheiten zugeordnet: Bit bzw. Qubit. Die Quanteninformationstheorie gilt einheitlich für die unterschiedlichen Qubit-Systeme (Spin, Photonenpolarisation usw.).

Wie wir in den nachfolgenden Kapiteln noch im Einzelnen darstellen werden, unterscheidet sich die Speicherung und Verarbeitung von Quanteninformation wesentlich von der klassischen Information: (i) Die Zustände eines Qubits sind nicht auf 0 und 1 beschränkt. Sie werden durch die ganze Bloch-Kugel beschrieben. (ii) Der Zustand eines Quantensystems, das aus mehreren Qubit-Systemen zusammengesetzt ist, kann verschränkt sein. (iii) Klassisch gibt es nur Sprünge zwischen 0 und 1. Unitäre Transformationen und andere Operationen sind aber sehr viel allgemeiner und reichhaltiger. (iv) Allerdings kann man in einer Messung den quantentheoretischen Endzustand nicht so auslesen wie den klassischen Zustand.

6.6 Ergänzende Themen und weiterführende Literatur

Siehe auch Abschn. 5.6.

- Übersichtsartikel: [Weh 78], [CD 94], [CF 96], [Ste 98], [Joz 98], [Ved 02].
- Zum Konzept „Quanteninformation“: [Wer 01], [Wer 02].
- Zu Schumachers Theorem und zur Quantendatenkompression: [JS 94], [Sch 95], [Joz 98], [Ved 02], [Ben 95].

6.7 Übungsaufgaben

ÜA 6.1 [zu 6.1] Bestimmen Sie mit Bezug auf ein Ergebnis in Kap. 3 die Entropie eines Zustands ρ in \mathcal{H}_2 als Funktion des Bloch-Vektors.

ÜA 6.2 [zu 6.2] Bestimmen Sie den Bloch-Vektor \mathbf{r} zum Dichteoperator ρ von Gl. (6.11). Die Eigenvektoren von ρ und $\mathbf{r}\cdot\boldsymbol{\sigma}$ stimmen überein (warum?). Lesen Sie mit Bezug auf Abschn. 3.2 an $\mathbf{r}\cdot\boldsymbol{\sigma}$ die Darstellung der Eigenvektoren in der Rechenbasis ab und bestimmen Sie die Eigenwerte λ_0 und λ_1 . Berechnen Sie $S(\rho)$.

This Page Intentionally Left Blank

7 Zusammengesetzte Systeme

Wir gehen zu zusammengesetzten Systemen über und stellen zunächst wieder den mathematischen Rahmen zur Verfügung. Dann werden die Postulate verallgemeinert und der Spezialfall der Messungen an Teilsystemen ausführlich diskutiert. Die Konsequenzen von Verschränkung werden verdeutlicht. Die unitäre Dynamik kann wieder mit Hilfe von Liouville-Operatoren formuliert werden. Die Wirkung einfacher Quantengatter auf mehreren Qubit-Systemen wird vorgestellt.

7.1 Teilsysteme

Wir sind von der klassischen Physik her gewohnt, dass *zusammengesetzte Systeme* (composite systems, compound systems) in *Teilsysteme* oder Untersysteme (subsystems) zerlegt werden können und dass umgekehrt Systeme zu Gesamtsystemen zusammengesetzt werden können. Das klassische Gesamtsystem ist dabei vollständig durch die Zustände der Teilsysteme und ihre dynamischen Wechselwirkungen untereinander beschreibbar. Das Sonnensystem mit Sonne, Planeten und Gravitationsfeld ist ein Beispiel. In der Quantenphysik zeigt sich, dass zusammengesetzte Systeme darüber hinaus völlig andere und überraschende ganzheitliche Eigenschaften aufweisen können. Sie treten auf, wenn sich zusammengesetzte Quantensysteme in *verschränkten Zuständen* (entangled states) befinden. In diesen Fällen ist tatsächlich „das Ganze mehr als die Summe seiner Teile“. Wir werden zur Darstellung der Einzelheiten ähnlich wie in Abschn. 1.2 vorgehen und die Diskussion von Präparation und Messung an den Anfang stellen.

Was sind zusammengesetzte Systeme? Es gibt spezielle Quantensysteme, die eine innere Struktur aufweisen. Man kann bei ihnen zwei oder mehrere Teilsysteme unterscheiden, auf die man getrennt Zugriff hat. Damit ist gemeint, dass sich experimentell Teilsysteme finden lassen, an denen man jeweils einzeln (und in diesem Sinne lokal) Eingriffe durchführen kann. Diese Operationen werden *lokale Operationen* (local operations) genannt. Es können z. B. Messungen sein.

Wir geben einige *2-Teile-Systeme* (bi-partite-systems) an. Es können z. B. Quantensysteme präpariert werden, bei denen man an zwei verschiedenen Orten bei Messungen jeweils ein Photon registriert. Analoge Systeme gibt es für Elektronen. Es gibt Systeme, bei denen an einem Ort ein Photon und an einem anderen Ort ein Atom registriert wird. Teilsysteme werden allgemein als *lokal* bezeichnet, müssen aber tatsächlich nicht räumlich getrennt sein. Es kann

sich beim zusammengesetzten System z. B. auch um die Bahn (äußerer Freiheitsgrad) und die Polarisierung (innerer Freiheitsgrad) vom einzelnen Quantenobjekt handeln. Selbstverständlich kann man auch zwei getrennte Systeme, die völlig unabhängig voneinander sind, formal als ein Gesamtsystem auffassen.

Wesentlich ist, dass man z. B. bei einem 2-Photonen-System nicht davon ausgeht, dass die beteiligten Photonen unterscheidbar sind (was sie bekanntlich nicht sind). Unterscheidbar sind z. B. die Orte, an denen bei einer Messung eine Photonenpolarisation gemessen wird. Von Messungen wissen wir auch, dass immer zwei und nicht mehr Photonen zusammen präpariert werden und daher das Gesamtsystem ein 2-Teile-System ist. Die entsprechenden Teilsysteme S^A und S^B sind in diesem Fall den Orten A und B zugeordnet (Photon am Ort A bzw. am Ort B). Allgemein sind Geräte klassische Objekte und haben daher Individualität. Demgegenüber macht es wegen der Ununterscheidbarkeit der Photonen keinen Sinn zu fragen, welchem der beiden Photonen bei einer Messung z. B. am Ort A gemessen wurde.

Alice und Bob Um besonders deutlich zu machen, dass an verschiedenen Teilsystemen S^A und S^B des zusammengesetzten Systems S^{AB} gemessen oder manipuliert wird, werden häufig die Experimentatoren *Alice* und *Bob* eingeführt, die am Teilsystem S^A bzw. S^B (oft aber nicht notwendig an verschiedenen Orten) lokale Operationen ausführen. Mit dem Bezug auf Alice und Bob unterstreicht man auch nochmal, dass sehr viele quantentheoretische Aussagen *operational* (operational) oder *operativ* (d. h. als Handlungsanweisungen) zu verstehen sind z. B. von der Art: Wenn Alice am Teilsystem S^A dieses ausführt, wird Bob am Teilsystem S^B jenes messen.

Existenz Wir werden gemäß der Standardinterpretation aus Abschn. 1.2 wiederum annehmen, dass solche Teilsysteme keine gedanklichen Hilfskonstruktionen sind wie die Quantensysteme in der Minimalinterpretation, sondern tatsächlich existieren. Damit ist allerdings nicht gemeint, dass dem einzelnen Teilsystem ein vom Zustand der anderen Teilsysteme unabhängiger Zustand zugeschrieben werden kann. Bei verschränkten Gesamtsystemen liegt diese Unabhängigkeit gerade nicht vor. Dies ist die Ursache für viele verblüffende quantenphysikalische Effekte. Es ist darüber hinaus mit der Existenzaussage auch nicht unterstellt, dass gleichartige Elementarteilchen derselben Sorte, wie z. B. zwei Photonen, Individualität besitzen und daher unterscheidbar sind. So weit geht die Annahme, dass die Photonen existieren, nicht. Die einzelne Zugriffsmöglichkeit und nicht die Individualität von Quantenobjekten definiert das Teilsystem.

7.2 Produktraum

Wir wollen zunächst den mathematischen Formalismus bereitstellen, mit dessen Hilfe die Physik der zusammengesetzten Systeme formuliert werden kann. Wir benötigen hierzu den *Produkt-Hilbert-Raum*.

7.2.1 Vektoren

Das *Tensorprodukt* \mathcal{H}^{AB} aus zwei Hilbert-Räumen \mathcal{H}^A und \mathcal{H}^B , deren Dimensionen nicht übereinstimmen müssen

$$\mathcal{H}^{AB} = \mathcal{H}^A \otimes \mathcal{H}^B \quad (7.1)$$

ist wieder ein Hilbert-Raum. Wir nennen \mathcal{H}^A und \mathcal{H}^B die *Faktorräume*. Zu jedem Paar von Vektoren $|\varphi^A\rangle \in \mathcal{H}^A$ und $|\chi^B\rangle \in \mathcal{H}^B$ gehört ein *Produktvektor* (product vector) aus \mathcal{H}^{AB} , der unterschiedlich geschrieben werden kann

$$|\varphi^A\rangle \otimes |\chi^B\rangle =: |\varphi^A\rangle |\chi^B\rangle =: |\varphi^A, \chi^B\rangle =: |\varphi, \chi\rangle. \quad (7.2)$$

Er ist bezüglich der Multiplikation mit komplexen Zahlen in jedem Argument linear.

Mit $\lambda, \mu \in \mathbb{C}$

$$|\varphi^A\rangle \otimes (\lambda |\chi_1^B\rangle + \mu |\chi_2^B\rangle) = \lambda |\varphi^A\rangle \otimes |\chi_1^B\rangle + \mu |\varphi^A\rangle \otimes |\chi_2^B\rangle, \quad (7.3)$$

$$(\lambda |\varphi_1^A\rangle + \mu |\varphi_2^A\rangle) \otimes |\chi^B\rangle = \lambda |\varphi_1^A\rangle \otimes |\chi^B\rangle + \mu |\varphi_2^A\rangle \otimes |\chi^B\rangle. \quad (7.4)$$

Verschränkte Vektoren Wenn $\{|n^A\rangle\}$ eine Basis von \mathcal{H}^A und $\{|i^B\rangle\}$ eine Basis von \mathcal{H}^B ist, dann ist

$$\{|n^A\rangle \otimes |i^B\rangle\} \quad (7.5)$$

eine von \mathcal{H}^{AB} . Für die Dimension von \mathcal{H}^{AB} gilt $\dim \mathcal{H}^{AB} = (\dim \mathcal{H}^A) \cdot (\dim \mathcal{H}^B)$. Jeder Vektor $|\psi^{AB}\rangle$ aus \mathcal{H}^{AB} kann nach der Basis zerlegt werden

$$|\psi^{AB}\rangle = \sum_{n,i} \alpha_{ni} |n^A, i^B\rangle. \quad (7.6)$$

Alle Definitionen und Aussagen lassen sich direkt auf das Produkt einer endlichen Zahl von Hilbert-Räumen $\mathcal{H}^{AB\dots M} = \mathcal{H}^A \otimes \mathcal{H}^B \otimes \dots \otimes \mathcal{H}^M$ übertragen. Vektoren aus \mathcal{H}^{AB} , die keine Produktvektoren sind, werden *verschränkt* (entangled) genannt. Durch sie werden wir verschränkte reine Zustände repräsentieren, die im Folgenden eine wichtige Rolle spielen werden. An der Zerlegung (7.6) nach der Basis ist zumeist nicht direkt ablesbar, ob ein Vektor $|\psi^{AB}\rangle$ verschränkt ist. Wir werden hierzu später ein Kriterium entwickeln (Abschn. 8.2.1) und auch das Konzept der Verschränkung auf Dichteoperatoren erweitern (Abschn. 8.1.1).

Skalarprodukt Der Bra-Vektor zum Produktvektor $|\varphi^A\rangle \otimes |\chi^B\rangle$ hat die Form

$$(|\varphi^A\rangle \otimes |\chi^B\rangle)^\dagger = \langle \varphi^A | \otimes \langle \chi^B | =: \langle \varphi^A | \langle \chi^B | =: \langle \varphi^A, \chi^B | =: \langle \varphi, \chi |. \quad (7.7)$$

Daraus folgt für $|\psi^{AB}\rangle$ von Gl. (7.6)

$$(|\psi^{AB}\rangle)^\dagger = \langle \psi^{AB} | = \sum_{n,i} \alpha_{ni}^* \langle n^A, i^B |. \quad (7.8)$$

Das Skalarprodukt wird „raumweise“ gebildet:

$$\langle \varphi^A, \chi^B | \xi^A, \zeta^B \rangle = \langle \varphi^A | \xi^A \rangle \langle \chi^B | \zeta^B \rangle . \quad (7.9)$$

Eine Basis $\{|n^A, i^B\rangle\}$ von \mathcal{H}^{AB} ist orthonormal, wenn

$$\langle n^A, i^B | n'^A, i'^B \rangle = \delta_{nn'} \delta_{ii'} \quad (7.10)$$

gilt, d. h. wenn $\{|n^A\rangle\}$ und $\{|i^B\rangle\}$ ONB sind.

Bell-Basis¹ Wie man leicht nachprüfen kann bilden die folgenden vier Vektoren eine spezielle ONB im Raum $\mathcal{H}^{AB} = \mathcal{H}_2^A \otimes \mathcal{H}_2^B$ der 2-Qubit-Vektoren:

$$|\Phi_{\pm}\rangle := \frac{1}{\sqrt{2}}(|0, 0\rangle \pm |1, 1\rangle) , \quad |\Psi_{\pm}\rangle := \frac{1}{\sqrt{2}}(|0, 1\rangle \pm |1, 0\rangle) . \quad (7.11)$$

Diese Basis spielt bei vielen Untersuchungen eine besondere Rolle. Wir werden später zeigen, dass diese häufig verwendeten *Bell-Zustände* maximal verschränkt sind.

7.2.2 Operatoren

Produktoperatoren C^A sei ein linearer Operator auf \mathcal{H}^A und D^B ein linearer Operator auf \mathcal{H}^B . Das Tensorprodukt

$$C^A \otimes D^B =: C^A D^B \quad (7.12)$$

bezeichnet einen *Produktoperator*, der „raumweise“ wirkt

$$[C^A \otimes D^B]|\varphi^A, \chi^B\rangle = |C^A \varphi^A, D^B \chi^B\rangle . \quad (7.13)$$

Der Produktoperator ist ein linearer Operator auf \mathcal{H}^{AB} .

$$[C^A \otimes D^B] \sum_{n,i} \alpha_{ni} |n^A, i^B\rangle = \sum_{n,i} \alpha_{ni} |C^A n^A, D^B i^B\rangle . \quad (7.14)$$

Der aus den Produktvektoren $|\psi^{AB}\rangle = |\varphi^A, \chi^B\rangle$ und $|\theta^{AB}\rangle = |\xi^A, \zeta^B\rangle$ gebildete dyadische Operator $|\psi^{AB}\rangle \langle \theta^{AB}|$ ist ebenfalls ein Produktoperator.

$$|\psi^{AB}\rangle \langle \theta^{AB}| = |\varphi^A, \chi^B\rangle \langle \xi^A, \zeta^B| = (|\varphi^A\rangle \langle \xi^A|) \otimes (|\chi^B\rangle \langle \zeta^B|) . \quad (7.15)$$

Man kann die Klammern auch weglassen. Der Identitätsoperator auf \mathcal{H}^{AB} kann mit der Basis von Gl. (7.5) dyadisch zerlegt werden:

$$\mathbb{1}^{AB} = \sum_{n,i} |n^A, i^B\rangle \langle n^A, i^B| = \mathbb{1}^A \otimes \mathbb{1}^B . \quad (7.16)$$

¹ Benannt nach J.S. Bell (1928-1990)

Mit dem Identitätsoperator eines Faktorraums lassen sich spezielle Produktoperatoren bilden. Die durch ein Dach gekennzeichneten *erweiterten Operatoren* (*Teilsystem-Operatoren*)

$$\hat{C}^{AB} = C^A \otimes \mathbb{1}^B; \quad \hat{D}^{AB} = \mathbb{1}^A \otimes D^B \quad (7.17)$$

sind auf $\mathcal{H}^{AB} = \mathcal{H}^A \otimes \mathcal{H}^B$ definiert, wirken jedoch nur in den jeweiligen Faktor-Hilbert-Räumen in nicht-trivialer Weise. \hat{C}^{AB} und \hat{D}^{AB} kommutieren auf \mathcal{H}^{AB} und es gilt

$$\hat{C}^{AB} \otimes \hat{D}^{AB} = \hat{D}^{AB} \otimes \hat{C}^{AB} = C^A \otimes D^B. \quad (7.18)$$

Allgemeine Operatoren Mit Bezug auf die dyadische Zerlegung (7.16) von $\mathbb{1}^{AB}$ können wir den allgemeinen Operator Z^{AB} auf \mathcal{H}^{AB} in der Form

$$Z^{AB} = \mathbb{1}^{AB} Z^{AB} \mathbb{1}^{AB} = \sum_{n,m} \sum_{i,j} \langle n^A, i^B | Z^{AB} | m^A, j^B \rangle (|n^A\rangle \langle m^A| \otimes |i^B\rangle \langle j^B|) \quad (7.19)$$

schreiben. Er ist durch seine Matrixelemente in der orthonormalen Basis (7.5) bestimmt.

Spur und Teilspur Die *Spur* (trace) ist auch in \mathcal{H}^{AB} über eine orthonormale Basis in gewohnter Weise definiert

$$\mathrm{tr}_{AB}[Z^{AB}] :=: \mathrm{tr}[Z^{AB}] := \sum_{n,i} \langle n^A, i^B | Z^{AB} | n^A, i^B \rangle. \quad (7.20)$$

Für Produktoperatoren folgt daraus

$$\mathrm{tr}[C^A \otimes D^B] = \sum_{n,i} C_{nn}^A D_{ii}^B = \mathrm{tr}_A[C^A] \mathrm{tr}_B[D^B], \quad (7.21)$$

mit den Matrixelementen C_{nn}^A und D_{ii}^B . Die Spur wird „raumweise“ gebildet.

Die Bildung der *Teilspur* (partial trace) über einen der Faktorräume, beispielsweise den Raum \mathcal{H}^A , ist für die Physik besonders wichtig. Sie ist durch

$$\mathrm{tr}_A[Z^{AB}] := \sum_n \langle n^A | Z^{AB} | n^A \rangle \quad (7.22)$$

definiert. Wie man an Gl. (7.19) ablesen kann, entsteht dabei ein Operator auf \mathcal{H}^B . Für Produktoperatoren folgt

$$\mathrm{tr}_A[C^A \otimes D^B] = \mathrm{tr}_A[C^A] D^B. \quad (7.23)$$

Die Gesamtspur ergibt sich als Abfolge von Teilspuren

$$\mathrm{tr}[Z^{AB}] = \mathrm{tr}_B[\mathrm{tr}_A[Z^{AB}]] = \mathrm{tr}_A[\mathrm{tr}_B[Z^{AB}]]. \quad (7.24)$$

Dabei kommt es auf die Reihenfolge der Bildung der Teilspuren nicht an.

Operatorbasis Auch dieses Konzept, das wir in Abschn. 1.2 kennen gelernt haben, lässt sich direkt auf den Produktraum \mathcal{H}^{AB} übertragen. Wenn $\{Q_\alpha^A, \alpha = 1, \dots, (\dim \mathcal{H}^A)^2\}$ eine Operatorbasis auf \mathcal{H}^A und $\{R_\kappa^B, \kappa = 1, \dots, (\dim \mathcal{H}^B)^2\}$ eine Operatorbasis auf \mathcal{H}^B ist, dann bilden die Produktoperatoren

$$T_{\alpha\kappa}^{AB} := Q_\alpha^A \otimes R_\kappa^B \quad (7.25)$$

wegen

$$\text{tr}[T_{\alpha\kappa}^{AB\dagger} T_{\beta\lambda}^{AB}] = \delta_{\alpha\beta} \delta_{\kappa\lambda} \quad (7.26)$$

eine Operatorbasis des Produktraums \mathcal{H}^{AB} . Man kann jeden Operator Z^{AB} , der auf \mathcal{H}^{AB} wirkt, nach ihr entwickeln:

$$Z^{AB} = \sum_{\alpha, \kappa} T_{\alpha\kappa}^{AB} \text{tr}[T_{\alpha\kappa}^{AB\dagger} Z^{AB}] . \quad (7.27)$$

Es gibt Operatoren auf \mathcal{H}^{AB} , die nicht als Produkt von zwei Operatoren in der Form $C^A \otimes D^B$ geschrieben werden können. Aber alle Operatoren auf \mathcal{H}^{AB} können als Summe von Produktoperatoren geschrieben werden.

Produkt-Liouville-Raum Wir übertragen die Konzepte aus Abschn. 1.2 und bilden den *Produkt-Liouville-Raum*

$$\mathbb{L}^{AB} = \mathbb{L}^A \otimes \mathbb{L}^B . \quad (7.28)$$

Seine Elemente sind die Operatoren

$$C^{AB} = \sum_{\alpha, \beta} c_{\alpha\beta} Q_\alpha^A \otimes R_\beta^B . \quad (7.29)$$

auf \mathcal{H}^{AB} . Der *Liouville-Operator* wird in Verallgemeinerung von Gl. (1.84) mit dem Hamilton-Operator H^{AB} auf \mathcal{H}^{AB} definiert:

$$\mathcal{L}^{AB} Z^{AB} := \frac{1}{\hbar} [H^{AB}, Z^{AB}]_- . \quad (7.30)$$

7.3 Grundlagen der Physik zusammengesetzter Quantensysteme

7.3.1 Postulat für zusammengesetzte Systeme und Ausblick

Wir betrachten *zusammengesetzte Quantensysteme* (composite quantum systems), die selber abgeschlossen sein sollen. Daher können wir alle Postulate von Kap. 2 und 4 direkt übertragen. Insbesondere wird der Zustand des zusammengesetzten Systems durch einen Dichteoperator in einem Hilbert-Raum beschrieben. Die operationale Interpretation des Konzepts „Zustand“

eines Quantensystems als „das System hat ein bestimmtes Präparationsverfahren durchlaufen“ überträgt sich. Das zusammengesetzte System $S^{AB\dots}$ soll aus *Teilsystemen* (subsystems) S^A, S^B, \dots bestehen. Da wir Teilsysteme betrachten wollen, die selber Quantensysteme sind, liegt es nahe, ihnen zur Beschreibung jeweils einen Hilbert-Raum $\mathcal{H}^A, \mathcal{H}^B, \dots$ zuzuordnen. Dann bleibt zunächst noch die Frage offen, welche Struktur der Hilbert-Raum des Gesamtsystems hat, d. h. wie er sich aus den $\mathcal{H}^A, \mathcal{H}^B, \dots$ mathematisch zusammensetzt. Hier gibt es im Prinzip viele Möglichkeiten. Eine ist z. B. die direkte Summe $\mathcal{H}^{AB\dots} = \mathcal{H}^A \oplus \mathcal{H}^B \oplus \dots$. Tatsächlich postuliert man aber das Tensorprodukt, wie wir es in Abschn. 7.2.1 beschrieben haben, um Übereinstimmung mit den Experimenten zu erzielen. Diese Festlegung hat weitreichende Konsequenzen für alle physikalischen Aussagen über zusammengesetzte Quantensysteme, deren Teilsysteme nicht völlig voneinander isoliert sind. Wir sind im Folgenden gerade an diesen Aussagen interessiert.

Postulat Die Zustände eines aus den Teilsystemen S^A, S^B, \dots zusammengesetzten abgeschlossenen Gesamtsystems $S^{AB\dots}$ werden durch Dichteoperatoren $\rho^{AB\dots}$ im Produkt-Hilbert-Raum

$$\mathcal{H}^{AB\dots} = \mathcal{H}^A \otimes \mathcal{H}^B \otimes \dots \quad (7.31)$$

beschrieben. Die Postulate für abgeschlossene Systeme aus Abschn. 2.1 und Abschn. 4.2 übertragen sich auf das Gesamtsystem $S^{AB\dots}$.

Ausblick An dem Postulat kann man unmittelbar eine Reihe von Besonderheiten der Physik zusammengesetzter Systeme ablesen. Die mathematische Produktstruktur (7.31) gibt eine Gliederung vor. Wir stellen sie am Beispiel eines 2-Teile-Systems S^{AB} dar.

- (i) Zustände: Ein reiner Zustand kann ein Produktzustand $|\psi^{AB}\rangle = |\phi^A\rangle \otimes |\chi^B\rangle$ oder ein verschränkter Zustand $|\psi^{AB}\rangle \neq |\phi^A\rangle \otimes |\chi^B\rangle$ sein. Die ungewöhnlichen Eigenschaften verschränkter Zustände, insbesondere das Auftreten nicht-klassischer Korrelationen und ihre Nutzung, werden wir im Rest dieses Kapitels und in allen weiteren Kapiteln im Einzelnen diskutieren. Auf korrelierte Dichteoperatoren $\rho^{AB} \neq \rho^A \otimes \rho^B$ gehen wir in Abschn. 8.1 ein.
- (ii) Observablen: Es gibt den Spezialfall der erweiterten Observablenoperatoren, wie z. B. $\hat{C}^{AB} = C^A \otimes \mathbb{1}^B$, die mit einem Observablenoperator gebildet werden, der nur auf einem der Produkträume wirkt. Mit ihnen werden *lokale Messungen* (local measurements) beschrieben, die nur an einem der Teilsysteme durchgeführt werden (z. B. Messung der Observablen C^A am Teilsystem S^A). Es gibt aber auf \mathcal{H}^{AB} allgemeinere hermitesche Operatoren Z^{AB} , die nicht als erweiterte Operatoren schreibbar sind. Auch ihnen entsprechen Messungen physikalischer Observablen Z^{AB} . Diese Observablen werden *nicht-lokale Observablen* (non-local observables) oder *kollektive Observablen* (collective observables) genannt. Die entsprechenden Messungen sind *nicht-lokale Messungen* (non-local measurements), die i. a. nicht direkt als lokale Messungen an S^A und S^B durchgeführt werden können. Das gilt auch für den Spezialfall der Observablen, die Operatorprodukten entsprechen (z. B. $Z^{AB} = C^A \otimes D^B$). Nicht-lokale Messungen werden im Zusammenhang mit Quantenkorrelationen und der nicht-lokalen Speicherung von Information wichtig. Wir besprechen sie daher erst in Abschn. 9.2.

- (iii) Unitäre Entwicklungen: Auch die unitären Entwicklungen müssen nicht von der Struktur $U^{AB} = U^A \otimes U^B$ sein. Es kann z. B. eine Wechselwirkung zwischen den Systemen S^A und S^B existieren. Wir diskutieren das in Abschn. 7.3.5. Nicht-lokale unitäre Entwicklungen können verschränkend und entschränkend wirken. .

7.3.2 Messungen an einem Teilsystem und reduzierter Dichteoperator

Über das Postulat sind insbesondere die Einzelheiten der projektiven Messung einer Observablen des Gesamtsystems festgelegt. Diese Messung am Gesamtsystem wird durch einen hermiteschen Operator auf $\mathcal{H}^{AB\dots}$ beschrieben. Die Messung einer Observablen mit Observablenoperator C nur an einem Teilsystem, z. B. an S^A , ist als ein Spezialfall enthalten. Ihr ist ein Observablenoperator C^A zugeordnet, der auf \mathcal{H}^A wirkt. Dieser *lokalen Messung* (local measurement) entspricht in $\mathcal{H}^{AB\dots}$ ein *lokaler Observablenoperator* (local observable)

$$\hat{C}^{AB\dots E} = C^A \otimes \mathbb{1}^B \otimes \dots \otimes \mathbb{1}^E . \quad (7.32)$$

Wir wollen uns in diesem Kapitel auf Gesamtsysteme beschränken, die aus zwei Teilsystemen zusammengesetzt sind. Die Erweiterung auf mehr Teilsysteme ist trivial.

Wahrscheinlichkeitsaussagen Gemäß Postulat übertragen sich die Regeln für die Messdynamik auf die Zustände ρ^{AB} des zusammengesetzten Systems S^{AB} . Wir wollen die sich daraus ergebenden Konsequenzen für lokale Messungen untersuchen. Hierzu ist es nützlich jedem Teilsystem durch die Bildung der Teilspur über das andere Teilsystem einen *reduzierten Dichteoperator* (reduced density operator) zuzuordnen.

$$\rho^A := \text{tr}_B [\rho^{AB}] , \quad \rho^B := \text{tr}_A [\rho^{AB}] \quad (7.33)$$

Da ρ^{AB} ein Dichteoperator ist, erfüllen ρ^A und ρ^B ebenfalls die Bedingungen für einen Dichteoperator. Das Eigenwertproblem des Observablenoperators C^A

$$C^A |c_n^{(r)A}\rangle = c_n |c_n^{(r)A}\rangle, \quad r = 1, \dots, g_n \quad (7.34)$$

führt auf die ONB $\{|c_n^{(r)A}\rangle\}$ von \mathcal{H}^A und die Eigenwerte $\{c_n\}$ mit Entartung g_n . Die Wahrscheinlichkeit bei einer Messung von C am System S^A den Messwert c_n zu erhalten, ist dann mit dem *lokalen Projektionsoperator*

$$\hat{P}_n^A = P_n^A \otimes \mathbb{1}^B, \quad P_n^A := \sum_{r=1}^{g_n} |c_n^{(r)A}\rangle \langle c_n^{(r)A}| \quad (7.35)$$

durch

$$p(c_n) = \text{tr}[\hat{P}_n^A \rho^{AB}] = \text{tr}_A[\text{tr}_B\{\hat{P}_n^A \rho^{AB}\}] = \text{tr}_A[P_n^A \rho^A] \quad (7.36)$$

gegeben. In analoger Weise erhalten wir für den Erwartungswert der Observablen C

$$\langle \hat{C}^A \rangle = \text{tr}[\rho^{AB} \hat{C}^A] = \text{tr}_A[\rho^A C^A] . \quad (7.37)$$

Zusammenfassend stellen wir fest: *Alle Wahrscheinlichkeitsaussagen für lokale Messungen am Teilsystem S^A ergeben sich indem man dem System S^A den reduzierten Dichteoperator ρ^A von Gl. (7.33) zuordnet und die für die Dichteoperatoren abgeschlossener Systeme postulierte Regeln anwendet.*

Zustand eines Teilsystems Da alle Wahrscheinlichkeitsaussagen für Messungen an S^A durch den reduzierten Dichteoperator ρ^A eindeutig bestimmt sind, liegt es nahe davon zu sprechen, dass sich das Teilsystem S^A im Zustand ρ^A befindet. So hatten wir in Kap. 2 das Zustandskonzept eingeführt. Das Gesamtsystem S^{AB} durchläuft ein Präparationsverfahren, das auf den Zustand ρ^{AB} führt. Damit ist zugleich der Zustand $\rho^A = \text{tr}_B [\rho^{AB}]$ präpariert.

Gemische allgemein Bei einem Produktzustand $|\alpha_k^A, \beta_k^B\rangle$ des Gesamtzustands S^{AB} ist das Untersystem S^A im reinen Zustand $|\alpha_k^A\rangle$. Ist der Zustand von S^{AB} speziell ein statistisches Gemisch (Gemenge) aus solchen Produktzuständen präpariert worden (vergl. Kap. 4)

$$\rho^{AB} = \sum_s p_s |\alpha_s^A, \beta_s^B\rangle \langle \alpha_s^A, \beta_s^B|, \quad \sum_s p_s = 1, \quad (7.38)$$

dann befindet sich S^A ebenfalls in einem statistischen Gemisch

$$\rho^A = \text{tr}_B [\rho^{AB}] = \sum_k p_k |\alpha_k^A\rangle \langle \alpha_k^A| \quad (7.39)$$

aus den Zuständen $\{|\alpha_k^A\rangle\}$. Eine Ignoranzinterpretation (vergl. Abschn. 4.3) ist möglich (proper mixture). Im allgemeinen wird der Zustand S^A nach der Präparation von ρ^{AB} aber kein statistisches Gemisch reiner Zustände sein wie in Gl. (7.39). Dennoch wird er durch einen Dichteoperator ρ^A beschrieben. Man überträgt daher operational den Begriff *Gemisch* (mixture) auch auf diesen Zustand ρ^A von S^A , dem – wie schon in Abschn. 4.2 beschrieben – kein Mischen zugrunde liegt, und lässt zur Verdeutlichung den Zusatz „statistisches“ weg. Zur Kennzeichnung wird in diesem Fall auch von *improper mixture* im Gegensatz zur *proper mixture* gesprochen. Gemisch ist also der Überbegriff. Bei Teilsystemen können Gemische auftreten, die hinsichtlich ihrer Präparation keine statistischen Gemische sind und daher keine Ignoranzinterpretation zulassen. Für sie gibt es formal viele Ensemblezerlegungen. Es gibt daher viele statistische Gemische eines abgeschlossenen Systems S^A , durch die sie hinsichtlich aller Wahrscheinlichkeitsaussagen für lokale Messungen ununterscheidbar *simuliert* werden können. Dies rechtfertigt noch einmal die Übertragung des Begriffs Gemisch auf alle reduzierten Dichteoperatoren.

7.3.3 Zustand nach einer Messung an einem Teilsystem

Auch den Zustand ρ_n^A nach der selektiven Messung der Observablen C am System S^A mit Messwert c_n erhalten wir nach den für das Gesamtsystem gültigen Postulaten mit Hilfe des lokalen Projektionsoperators \hat{P}_n^A von Gl. (7.35) wie in Gl. (4.19)

$$\rho^A \rightarrow \rho_n^A = \frac{\text{tr}_B [\hat{P}_n^A \rho^{AB} \hat{P}_n^A]}{\text{tr}_A [\text{tr}_B \{\hat{P}_n^A \rho^{AB}\}]} \quad (7.40)$$

Mit Gl. (7.33) finden wir für diese selektive lokale Messung

$$\rho^A \rightarrow \rho_n^A = \frac{P_n^A \rho^A P_n^A}{\text{tr}_A [P_n^A \rho^A]} \quad (7.41)$$

Für die entsprechende nicht-selektive lokale Messung gilt mit Gl. (7.36) in Analogie zu Gl. (4.25)

$$\rho^A \xrightarrow{n.s.} \rho'^A = \text{tr}_B \left[\sum_n \hat{P}_n^A \rho^{AB} \hat{P}_n^A \right] = \sum_n P_n^A \rho^A P_n^A. \quad (7.42)$$

Wir können für lokale Messungen auch hinsichtlich der resultierenden Zustände die Regeln für Dichteoperatoren von Kap. 4 anwenden, wenn wir dabei dem Teilsystem S^A den reduzierten Dichteoperator ρ^A von Gl. (7.33) zuordnen. Entsprechendes gilt für das Teilsystem S^B . Die Messwahrscheinlichkeiten (7.36) lassen sich wieder mit dem unnormierten (Spur $\neq 1$) Dichteoperator $\tilde{\rho}_n^{A'} = P_n^A \rho^{AB} P_n^A$ nach der Messung schreiben:

$$p(c_n) = \text{tr}_A [\tilde{\rho}_n^{A'}] \quad (7.43)$$

Wir betrachten noch den Spezialfall, dass sich das Gesamtsystem S^{AB} vor der Messung in einem verschränkten reinen Zustand $|\psi^{AB}\rangle$ befindet. Nach Definition (vergl. Abschn. 7.2.1) ist ein verschränkter reiner Zustand nicht als Produktvektor schreibbar. Im Hinblick auf die Messung der Observablen C am Teilsystem S^A entwickeln wir $|\psi^{AB}\rangle$ nach der ONB von \mathcal{H}^{AB} , die die Eigenvektoren $\{|c_n^A\rangle\}$ von C^A enthält. Es möge keine Entartung vorliegen.

$$|\psi^{AB}\rangle = \sum_{n,i} \alpha_{ni} |c_n^A, d_i^B\rangle. \quad (7.44)$$

Wenn die Messung auf den Wert c_n führt, ergibt sich (Tilde kennzeichnet fehlende Normierung)

$$\begin{aligned} |\psi^{AB}\rangle &\rightarrow |\tilde{\psi}_n^{AB'}\rangle = P_n^A |\psi^{AB}\rangle = \\ &= |c_n^A\rangle \otimes \sum_i \alpha_{ni} |d_i^B\rangle = \\ &= |c_n^A, \tilde{w}_n^B\rangle \end{aligned} \quad (7.45)$$

mit

$$|\tilde{w}_n^B\rangle := \sum_i \alpha_{ni} |d_i^B\rangle. \quad (7.46)$$

Die Messung überführt somit in einen Produktzustand. Für einen verschränkten Zustand $|\psi^{AB}\rangle$ bricht die nicht entartete Messung an einem Teilsystem die Verschränkung. Es ist bemerkenswert, dass dabei das andere Teilsystem S^B in einen speziellen Zustand $|w_n^B\rangle$ übergeht, der über den Index n bei α_{ni} vom Ergebnis der Messung an S^A abhängt. Auch wenn die verschränkten Teilsysteme S^A und S^B räumlich weit voneinander getrennt sind, hat die lokale Messung an S^A instantan eine wohlbestimmte Zustandsänderung des Systems S^B zur Folge. Die Messung an einem Teilsystem S^A wirkt präparierend auf das andere Teilsystem S^B . Wenn für ein System im Bell-Zustand $|\Phi_+^{AB}\rangle$ die Messung von σ_z an einem Teilsystem in den Zustand $|0\rangle$ überführt, dann auch beim anderen und entsprechend mit dem Zustand $|1\rangle$ (vergl. den Neckerschen Würfel in Abb. 7.1). Dies ist Ausdruck der besonderen *Ganzheitlichkeit* des verschränkten Systems. Entsprechendes gilt für zusammengesetzte klassische Systeme nicht.

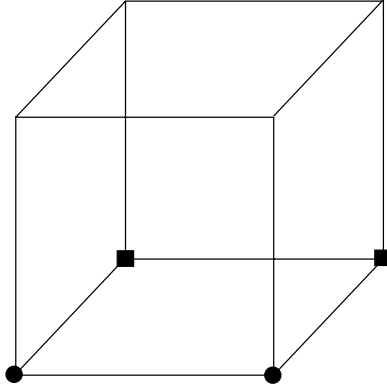


Abbildung 7.1: Der Neckersche Würfel und die Analogie zum verschränkten System. Die beiden linken unteren Eckpunkte (Kugel und Würfel) entsprechen den verschiedenen Zuständen von Teilsystem S^A , die rechten denen von Teilsystem S^B . Messen wird durch Hinsehen realisiert. Entweder sind als Ergebnis die beiden Kugelzustände vorn oder die beiden Würfelzustände sind vorn (Blick von oben oder von unten auf den Würfel). Immer wird bei Überführung des einen Teilsystems in einen Zustand auch das andere in den korrelierten Zustand überführt. Vor der Messung durch Hinsehen ist der Zustand des Neckerschen Würfels eine klassisch unmögliche „Superposition“.

7.3.4 Lokale Messungen an zwei Teilsystemen

Nachdem wir lokale Messungen an einem Teilsystem beschrieben haben, gehen wir zu lokalen Messungen an beiden Teilsystemen über. Wir betrachten wieder ein Quantensystem S^{AB} , das aus den Systemen S^A und S^B zusammengesetzt ist. Wir wollen am Teilsystem S^A die Observable C und am Teilsystem S^B die Observable D messen. Die zugehörigen Observablenoperatoren $\hat{C}^A = C^A \otimes \mathbb{1}^B$ und $\hat{D}^B = \mathbb{1}^A \otimes D^B$ kommutieren

$$[\hat{C}^A, \hat{D}^B]_- = 0. \quad (7.47)$$

Wir notieren noch die entsprechenden Eigenwertgleichungen

$$C^A |c_n^A\rangle = c_n |c_n^A\rangle, \quad D^B |d_i^B\rangle = d_i |d_i^B\rangle. \quad (7.48)$$

Die Vektoren $\{|c_n^A\rangle\}$ und $\{|d_i^B\rangle\}$ bilden ONB von \mathcal{H}^A bzw. \mathcal{H}^B . Die möglichen Messwerte $\{c_n\}$ und $\{d_i\}$ der lokalen Messungen sollen der Einfachheit halber nicht entartet sein.

Relativzustände Das Gesamtsystem S^{AB} soll sich vor den Messungen in einem reinen Zustand $|\psi^{AB}\rangle$ befinden, den wir nach der den Messungen angepassten Basis von \mathcal{H}^{AB} zerlegen

$$|\psi^{AB}\rangle = \sum_{n,i} \alpha_{ni} |c_n^A, d_i^B\rangle. \quad (7.49)$$

Es erweist sich als geschickt, im Hinblick auf das Ergebnis (7.45) die Doppelsumme in der Form

$$|\psi^{AB}\rangle = \sum_n |c_n^A, \tilde{w}_n^B\rangle \quad (7.50)$$

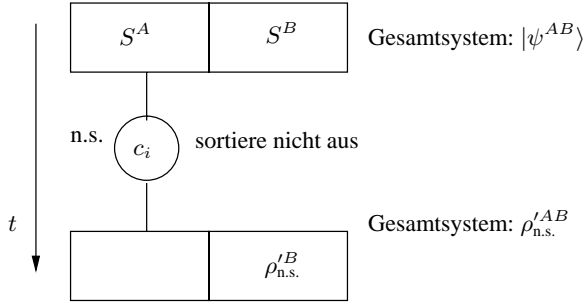


Abbildung 7.2: Nicht-selektive Messung am Teilsystem S^A .

aufzuspalten mit

$$|\tilde{w}_n^B\rangle := \sum_i \alpha_{ni} |d_i^B\rangle; \quad |w_n^B\rangle = \frac{|\tilde{w}_n^B\rangle}{\sqrt{\langle \tilde{w}_n^B | \tilde{w}_n^B \rangle}}. \quad (7.51)$$

Der Vektor $|w_n^B\rangle$ heißt der *relative Zustand* (relative state) zu $|c_n^A\rangle$. Unnormierte Zustände sind wieder durch eine Tilde gekennzeichnet. Die relativen Vektoren $\{|w_n^B\rangle\}$ bilden i.a. kein Orthonormalsystem. Ihre Anzahl muß auch nicht mit der Dimension des Hilbert-Raums \mathcal{H}^B übereinstimmen. $|\psi^{AB}\rangle$ lässt sich analog zu Gl. (7.50) auch bezüglich der zu $\{|d_i^B\rangle\}$ relativen Zustände $\{|\tilde{v}_i^A\rangle\}$ zerlegen.

$$|\psi^{AB}\rangle = \sum_i |\tilde{v}_i^A, d_i^B\rangle. \quad (7.52)$$

Nicht-selektive lokale Messung Wir führen eine Messung der Observablen C an S^A durch. Dabei soll sich der Messwert c_n ergeben. Dann geht das Gesamtsystem in den Produktvektor $|c_n^A, \tilde{w}_n^B\rangle$ bzw. den normierten Vektor $|c_n^A, w_n^B\rangle$ über. Die Wahrscheinlichkeit den Messwert c_n zu erhalten ist gemäß Gl. (7.36) durch das Quadrat der Norm des unnormierten relativen Zustandsvektors $|\tilde{w}_n^B\rangle$ gegeben

$$p(c_n) = \langle \psi^{AB} | (|c_n^A\rangle \langle c_n^A| \otimes \mathbf{1}^B) | \psi^{AB} \rangle = \langle \tilde{w}_n^B | \tilde{w}_n^B \rangle = ||\tilde{w}_n^B||^2. \quad (7.53)$$

Nach einer nicht-selektiven Messung an S^A befindet sich das Gesamtsystem S^{AB} in einem gemischten Zustand mit Dichteoperator

$$\rho'_{n.s.}^{AB} = \sum_n p(c_n) |c_n^A, w_n^B\rangle \langle c_n^A, w_n^B| = \sum_n |c_n^A, \tilde{w}_n^B\rangle \langle c_n^A, \tilde{w}_n^B|. \quad (7.54)$$

Dabei haben wir Gl. (7.53) verwendet. Die Superposition von Gl. (7.50) ist in das Gemisch von Gl. (7.54) zerlegt worden.

Alle Messungen am System S^B nach dieser nicht-selektiven Messung an S^A können durch den reduzierten Dichteoperator $\rho_{n.s.}^B$ beschrieben werden

$$\rho_{n.s.}^B = \text{tr}_A \rho'_{n.s.}^{AB} = \sum_n |\tilde{w}_n^B\rangle \langle \tilde{w}_n^B|, \quad (7.55)$$

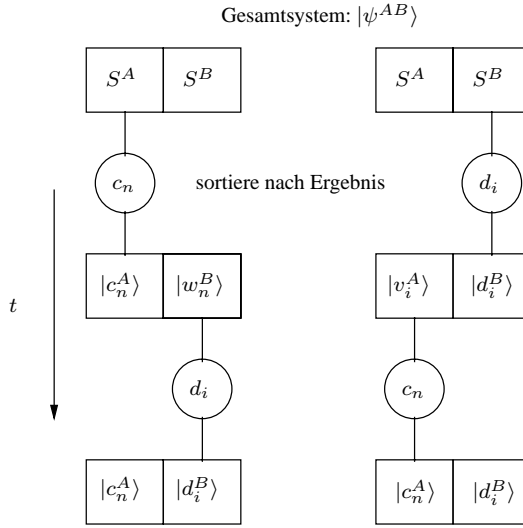


Abbildung 7.3: Selektive Messung an den Teilsystemen S^A und S^B . Links wird zuerst an S^A und dann an S^B gemessen, rechts in der anderen Reihenfolge. Es wird jeweils nach den Messwerten d_i und c_n selektiert. Die Wahrscheinlichkeit das Messwertepaar (c_n, d_i) zu erhalten und der entsprechende Endzustand $|c_n^A, d_i^B\rangle$ ist in beiden Fällen gleich.

der direkt durch den relativen Zustand $|\tilde{w}_i^B\rangle$ gegeben ist. Gl. (7.50) zeigt unmittelbar, dass er mit dem reduzierten Dichteoperator des Teilsystems S^B vor der Messung übereinstimmt.

$$\rho^B = \text{tr}_A[|\psi^{AB}\rangle\langle\psi^{AB}|] = \rho'_{n.s.}^B \quad (7.56)$$

Dies ist ein bemerkenswertes Ergebnis. Betrachten wir die Situation, dass das System S^A sich bei Alice befindet und das System S^B räumlich getrennt davon bei Bob. In einem Präparationsverfahren wird sehr oft ein 2-Teile-System im Zustand $|\psi^{AB}\rangle$ erzeugt. Alice ist es freigestellt, ob sie Messungen der Observablen C an ihrem System durchführt oder nicht. *Bob kann dann in keiner Weise durch Messungen welcher Observablen auch immer an seinem Teilsystem S^B feststellen, ob Alice Messungen durchgeführt hat oder nicht.* Das besagt gerade die Gl. (7.56). Da die Situation vollständig symmetrisch ist, gilt die Aussage entsprechend wenn Bob die ersten Messungen durchführt.

Nicht-selektiv bedeutet in diesem Zusammenhang, dass es Alice nicht erlaubt ist nach ihrer Messung z. B. die Zustände $|c_n^A, w_n^B\rangle$ des Gesamtsystems herauszusuchen, die zu ihrem Messergebnis c_n gehören und dafür zu sorgen, dass nur an Systemen in diesen Zuständen weitere Messungen durchgeführt werden. Das könnte sie offenbar nur erreichen, wenn Bob in gleicher Weise bei seinen Teilsystemen selektionieren würde. Dazu müsste Alice nach jeder ihrer Messungen Bob die Information übermitteln, ob er sein zugehöriges Teilsystem für anschließende Messungen weiter verwenden kann oder ob er es aussondern soll. Wenn Bob aber im Gegensatz dazu misst ohne vorher zu selektieren, kann er nicht feststellen, ob Ali-

ce gemessen hat oder nicht. Wenn er Anweisungen für eine Selektion bekommt, weiß er das trivialerweise.

Selektive lokale Messungen Wir gehen zu selektiven Messungen über und stellen sie zur Einübung in den Formalismus ausführlicher dar. Zunächst misst Alice und erhält mit der Wahrscheinlichkeit $p(c_n) = \langle \tilde{w}_n^B | \tilde{w}_n^B \rangle$ den Messwert c_n . Das System geht in den Gesamtzustand $|c_n^A, w_n^B\rangle$ über (vgl. Abb. 7.3). Wenn anschließend an diese Selektion Bob misst, erhält er den Messwert d_i mit der bedingten Wahrscheinlichkeit

$$p(d_i|c_n) = \frac{|\alpha_{ni}|^2}{p(c_n)}. \quad (7.57)$$

Dies kann man an den Gl. (7.51) ablesen. Das Gesamtsystem geht dabei in den Produktzustand $|c_n^A, d_i^B\rangle$ über. Wenn umgekehrt zuerst Bob und dann – nach Selektion nach dem Messwert d_i – Alice misst, erhalten wir analog (vgl. Abb. 7.3) den gleichen Endzustand für das Messwertepaar (c_n, d_i) . Für die Wahrscheinlichkeiten ergibt sich

$$p(c_n|d_i) = \frac{|\alpha_{ni}|^2}{p(d_i)}. \quad (7.58)$$

Die Wahrscheinlichkeit $p(c_n, d_i)$, mit der das Messwertepaar (c_n, d_i) erhalten wird, ist unabhängig von der Reihenfolge der Messungen:

$$p(c_n, d_i) = p(c_n|d_i)p(d_i) = p(d_i|c_n)p(c_n) = |\alpha_{ni}|^2 = \langle \psi^{AB} | P_{ni}^{AB} | \psi^{AB} \rangle \quad (7.59)$$

mit Projektionsoperator $P_{ni}^{AB} := |c_n^A, d_i^B\rangle\langle c_n^A, d_i^B|$. Da die Operatoren \hat{C}^A und \hat{D}^B kommutieren, war das auch nicht anders zu erwarten. Wir ergänzen noch, dass alle oben für den reinen Ausgangszustand $|\psi^{AB}\rangle$ gemachten Aussagen sich in bekannter Weise übertragen lassen, wenn der Ausgangszustand ein Gemisch mit Dichteoperator ρ^{AB} ist.

Erwartungswerte von Produktoperatoren Produktoperatoren repräsentieren spezielle nicht-lokale Observable. Für Anwendungen ist es wichtig, dass ihre Erwartungswerte durch lokale Messungen und klassische Kommunikation bestimmt werden können. Die dyadische Zerlegung des Operators $C^A \otimes D^B$ ist von der Form (vgl. Gl. (7.48))

$$C^A \otimes D^B = \sum_{n,i} c_n d_i |c_n^A, d_i^B\rangle\langle c_n^A, d_i^B|. \quad (7.60)$$

Für seinen Erwartungswert im Zustand ρ^{AB} gilt

$$\text{tr}[C^A \otimes D^B \rho^{AB}] = \sum_{n,i} \text{tr}[P_{ni}^A B \rho^{AB}] c_n d_i. \quad (7.61)$$

Die Spur auf der rechten Seite ist die Wahrscheinlichkeit dafür, dass bei lokalen Messungen an den Teilsystemen S^A und S^B das Messwertepaar (c_n^A, d_i^B) auftritt. *Der Erwartungswert eines Produktoperators stimmt mit dem Erwartungswert der Produkte korrelierter Messwerte überein.* Zu seiner Bestimmung messen Alice und Bob an einem Quantensystem im Zustand ρ^{AB}

an denen ihnen jeweils zugänglichen Teilsystemen, informieren sich über die Messergebnisse und bilden das Produkt der beiden korrelierten Messwerte. Das wiederholen sie an vielen Systemen im Zustand ρ^{AB} und berechnen schließlich den Mittelwert der Messwertprodukte. Wir kommen auf nicht-lokale Observable noch einmal in Abschn. 9.2 zurück.

7.3.5 Unitäre Dynamik zusammengesetzter Systeme

Die von-Neumann-Gleichung (4.9) bzw. (4.10) überträgt sich nach den Postulaten auf zusammengesetzte Systeme

$$i\hbar \frac{d\rho^{AB}}{dt} = [H^{AB}, \rho^{AB}(t)] - i \frac{d\rho^{AB}}{dt} = \mathcal{L}^{AB} \rho^{AB}(t) . \quad (7.62)$$

mit dem Liouville-Operator $\mathcal{L}^{AB} \in \mathbb{L}^A \otimes \mathbb{L}^B$. Wir verwenden das Schrödinger-Bild.

Wenn eine durch einen Hamilton-Operator $H_{\text{int}}^{AB} \neq 0$ beschriebene Wechselwirkung zwischen den Teilsystemen S^A und S^B vorliegt, sind die einzelnen Teilsysteme *offen* (open quantum systems). Der Gesamt-Hamilton-Operator hat dann die Form

$$H^{AB} = H^A \otimes \mathbb{1}^B + \mathbb{1}^A \otimes H^B + H_{\text{int}}^{AB} . \quad (7.63)$$

Der zugehörige Liouville-Operator ergibt sich als

$$\mathcal{L}^{AB} = \mathcal{L}^A + \mathcal{L}^B + \mathcal{L}_{\text{int}}^{AB} \quad (7.64)$$

und für die von-Neumann-Gleichung folgt:

$$i \frac{d\rho^{AB}}{dt} = (\mathcal{L}^A + \mathcal{L}^B + \mathcal{L}_{\text{int}}^{AB}) \rho^{AB}(t) . \quad (7.65)$$

Dies führt für den reduzierten Dichteoperator ρ^A auf die Differentialgleichung

$$i \frac{d\rho^A}{dt} = \mathcal{L}^A \rho^A(t) + \text{tr}_B[\mathcal{L}_{\text{int}}^{AB} \rho^{AB}(t)] \quad (7.66)$$

Zur Bestimmung von $\rho^A(t)$ muss man die volle Gl. (7.65) integrieren. Hierfür gibt es verschiedene Näherungsverfahren. Wir werden in Abschn. 13.1 und 14 einen In-Out-Zugang (in-out-approach) zur Dynamik offener Systeme kennenlernen, der nicht auf dem durch Gl. (7.66) beschriebenen differentiellen zeitlichen Verhalten von $\rho^A(t)$ beruht, sondern in phänomenologischer Weise durch einen Superoperator den Endzustand $\rho^A(t_{\text{out}})$ auf den Anfangszustand $\rho^A(t_{\text{in}})$ zurückführt.

7.4 Quantengatter für mehrere Qubit-Systeme

7.4.1 Verschränkung durch das CNOT-Gatter

Die Verarbeitung von Quanteninformation wird oft schematisch ohne Bezug auf eine experimentelle Realisierung durch *Quantenschaltungen* (quantum circuits) veranschaulicht. Die

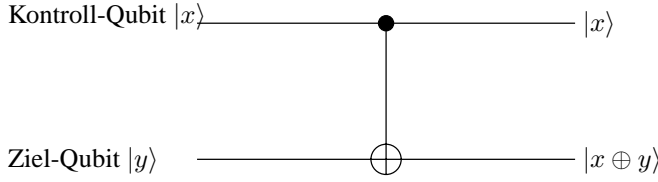


Abbildung 7.4: CNOT-Gatter.

wesentlichen Bauelemente, die dabei auftauchen, sind: *Quantendrähte* (quantum wires), dies sind spezielle Quantenkanäle durch die Quantensysteme unbeeinflusst propagieren, sowie *Quantengatter* (quantum gates), durch die unitäre Transformationen von Quantensystemen bewirkt werden. Die Systeme sind Multi-Qubits aus Räumen $\mathcal{H}_2 \otimes \mathcal{H}_2 \otimes \mathcal{H}_2 \dots \otimes \mathcal{H}_2$. *Messungen* dienen zum Auslesen von Information. Wegen der Unitarität repräsentieren Quantengatter umkehrbare Prozesse. Messungen sind demgegenüber irreversibel. *Quantencomputer* (quantum computers) sind ein Netzwerk von Quantengattern. Quantengatter für Quantensysteme aus \mathcal{H}_2 haben wir bereits in Abschn. 3.4 kennengelernt. Wir gehen jetzt zu Produkträumen über. In Kap. 12 werden wir Quantenschaltungen zu Quantencomputern zusammensetzen.

Verschränkung durch das CNOT-Gatter Ein einfaches Quantengatter, das einen Qubit-Produktzustand in einen verschränkten Zustand überführt, ist das *CNOT-Gatter* (CNOT gate, controlled NOT gate, XOR gate). Seine Wirkung auf der Rechenbasis von $\mathcal{H}_2^A \otimes \mathcal{H}_2^B$ ist durch

$$|x, y\rangle \rightarrow |x, y \oplus x\rangle \quad (7.67)$$

mit $x, y, \dots \in \{0, 1\}$ definiert. Damit liegt die Wirkung auf einen beliebigen Vektor aus $\mathcal{H}_2^A \otimes \mathcal{H}_2^B$ fest. \oplus bezeichnet die Addition modulo 2, d. h. es gilt $1 \oplus 1 = 0$. Im Einzelnen bedeutet das:

$$|0, 0\rangle \xrightarrow{\text{CNOT}} |0, 0\rangle \quad (7.68)$$

$$|0, 1\rangle \xrightarrow{\text{CNOT}} |0, 1\rangle \quad (7.69)$$

$$|1, 0\rangle \xrightarrow{\text{CNOT}} |1, 1\rangle \quad (7.70)$$

$$|1, 1\rangle \xrightarrow{\text{CNOT}} |1, 0\rangle. \quad (7.71)$$

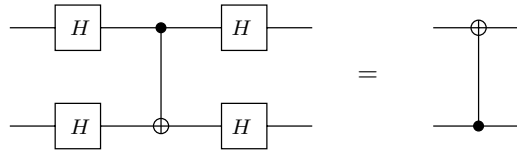
Daraus folgt

$$(\text{CNOT}) \cdot (\text{CNOT}) = \mathbb{1}. \quad (7.72)$$

Mit Hilfe der Matrixdarstellung in der Rechenbasis prüft man leicht die Unitarität nach

$$(\text{CNOT})^\dagger = (\text{CNOT})^{-1}. \quad (7.73)$$

Die Qubits des Systems A bzw. B werden *Kontroll-Qubit* (control qubit) bzw. *Ziel-Qubit* (target qubit) genannt (siehe Abb. 7.4). Ein einfaches Beispiel zeigt, dass das CNOT-Gatter

**Abbildung 7.5:** Zwei äquivalente Netzwerke.

Superpositionen im Kontroll-Qubit in Verschränkungen von Kontroll- und Ziel-Qubit überführt:

$$(\alpha|0^A\rangle \pm \beta|1\rangle)|0^B\rangle = \alpha|0^A, 0^B\rangle \pm \beta|1^A, 1^B\rangle, \quad (7.74)$$

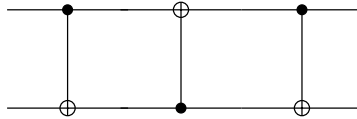
$$(\alpha|0^A\rangle \pm \beta|1^A\rangle)|1^B\rangle = \alpha|0^A, 1^B\rangle \pm |1^A, 0^B\rangle. \quad (7.75)$$

Für $\alpha = \beta = \frac{1}{\sqrt{2}}$ entstehen so die vier Bell-Zustände. Der reduzierte Dichteoperator vom Ziel-Qubit ist in diesem Fall $\rho^B = \frac{1}{2}\mathbb{1}^B$ (entsprechend beim Kontroll-Qubit). Die Messung in irgendeiner ONB von \mathcal{H}_2^B liefert die beiden Messwerte und Zustände in perfekter Zufälligkeit mit den Wahrscheinlichkeiten $\frac{1}{2}$.

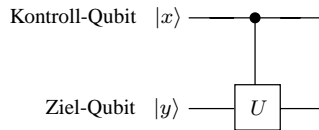
Ein CNOT-Gatter und vier Hadamard-Gatter lassen sich zum Inversen eines CNOT-Gatters zusammenbauen (siehe Abb. 7.5).

Die Schaltung von Abb. 7.6 aus drei CNOT vertauscht Kontroll- und Ziel-Qubit

$$|x, y\rangle \rightarrow |x, x \oplus y\rangle \rightarrow |y, x \oplus y\rangle \rightarrow |y, x\rangle. \quad (7.76)$$

**Abbildung 7.6:** Vertauschen von zwei Qubits.

Das CNOT-Gatter ist der Spezialfall eines *kontrollierten U-Gatters* (controlled U gate) (siehe Abb. 7.7). Es lässt $|0, 0\rangle$ und $|0, 1\rangle$ unverändert. $|1, y\rangle$ mit $y = 0, 1$ geht in $|1\rangle \otimes U|y\rangle$ über. CNOT ergibt sich mit $U = \sigma_x$.

**Abbildung 7.7:** Kontrolliertes U-Gatter.

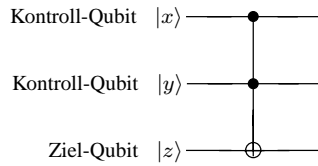


Abbildung 7.8: Toffoli-Gatter.

7.4.2 Toffoli-Gatter

Das *Toffoli-Gatter* (Toffoli gate) von Abb. 7.8 wird auch *CCNOT-Gatter* (controlled-controlled NOT) oder doppelt kontrolliertes NOT-Gatter genannt. Bei ihm wird das NOT-Gatter genau dann auf das Ziel-Qubit angewendet, wenn beide Kontroll-Qubits im Zustand $|1\rangle$ sind. Die Wirkung von CCNOT ist

$$|x, y, z\rangle \rightarrow |x, y, z \oplus xy\rangle. \quad (7.77)$$

Analog kann man ein doppelt kontrolliertes U-Gatter konstruieren (siehe Abb. 7.9)

Universelle Quantengatter (universal quantum gates) sind eine Menge von Quantengattern, mit denen man jede unitäre Transformation auf $\mathcal{H}_2 \otimes \mathcal{H}_2 \otimes \dots \otimes \mathcal{H}_2$ erzeugen kann. Es lässt sich zeigen, dass z. B. das *Deutsch-Gatter* (Deutsch gate) hierfür ausreicht. Bei diesem Gatter ist die unitäre Transformation U von Abb. 7.8

$$U = -i \exp\left(i \frac{\theta}{2} \sigma_x\right). \quad (7.78)$$

Es gibt weitere universelle Gatter (vergl. Abschn. 7.5).

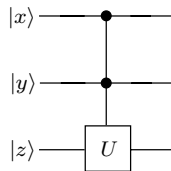


Abbildung 7.9: Doppelt kontrolliertes U-Gatter.

7.5 Ergänzende Themen und weiterführende Literatur

- Zu „proper mixture“ und „improper mixture“: [d’Es95], [d’Es99].
- Die Idee, dass das Ganze mehr ist als die Summe seiner Teile, wird in der Philosophie als *Holismus* (holism) oder *Ganzheitlichkeit* bezeichnet. Es gibt eine Reihe von philosophischen Analysen, in denen versucht wird, dieser Idee in ganz verschiedenen Gebieten von der Soziologie bis zur Physik eine präzise Bedeutung zu geben und ihre Konsequenzen

zu untersuchen. Für die naturphilosophische Frage, ob es Holismus in der Physik gibt, haben sich mit den nicht-separablen Zuständen zusammengesetzter Systeme ganz neue Aspekte ergeben. Zwei unterschiedliche darauf aufbauende Analysen werden in [Esf 04] und [See 04] vorgestellt (vergl. [Esf 02]). Dort ist auch weiterführende Literatur angegeben. Siehe auch [Hea 99].

- Das Deutsch-Gatter ist ein universelles Gatter: [Deu 89], [Pre 98, Kap. 6.2.3].
- Zu weiteren universellen Gattern: [Pre 98, Kap. 6.2.3], [NC 00, S. 188], [BBC 95].
- Lokale Messungen und die Forderung der Relativitätstheorie: [PT 04].
- Übersicht über Quantengatter für Qubits: [Bra 02], [DiV 98].

7.6 Übungsaufgaben

ÜA 7.1 [zu 7.3.2] Zeigen Sie, dass ρ^A und ρ^B von Gl. (7.33) die Eigenschaften eines Dichteoperators erfüllen.

ÜA 7.2 [zu 7.3.4] Bestätigen Sie die Ergebnisse von Abschn. 7.3.4 für den Fall, dass der Ausgangszustand kein reiner Zustand $|\psi^{AB}\rangle$, sondern ein Gemisch ρ^{AB} ist.

ÜA 7.3 [zu 7.4] Zeigen Sie jeweils die Äquivalenz der Netzwerke von Abb. 7.5 und Abb. 7.10.

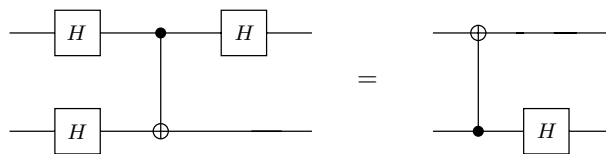


Abbildung 7.10: Zwei äquivalente Netzwerke.

ÜA 7.4 [zu 7.4] Zeigen Sie, dass das Netzwerk von Abb. 7.11 Paare von Bell-Zuständen in Paare von Bell-Zuständen überführt.

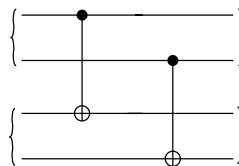


Abbildung 7.11: Abbildung von Bell-Zuständen auf Bell-Zustände.

This Page Intentionally Left Blank

8 Verschränkung

Das Konzept der EPR-Korrelationen wird in Abgrenzung zu klassischen Korrelationen, die es auch für Quantensysteme gibt, operational begründet und mit Verschränkung in Verbindung gebracht. Für reine Zustände kann das Vorliegen von Verschränkung über die Schmidt-Zerlegung festgestellt werden. Ein Maß für Verschränkung wird angegeben und ein Beispiel für die Erzeugung verschränkter Zustände vorgestellt. Es ist eine für Anwendungen wichtige Eigenschaft, dass Quantenzustände nicht kopiert werden können. Dass Zustände durch Verschränkung mit anderen Zuständen markiert werden können, führt auf den Quantenradierer und die Frage nach der verzögerten Wahl („delayed choice“).

8.1 Korrelationen und Verschränkung

Ein zusammengesetztes Spin-System mit zwei Teilsystemen kann sich z. B. in den Produktzuständen $|0^A, 0^B\rangle$ und $|1^A, 1^B\rangle$, aber auch in deren Superpositionen $\alpha|0^A, 0^B\rangle + \beta|1^A, 1^B\rangle$ befinden. Die Superposition $\alpha \neq 0, \beta \neq 0$ ist ein Beispiel für einen verschränkten Zustand. Verschränkte Zustände spielen eine fundamentale Rolle in der Quanteninformation. Sie sind das zentrale Hilfsmittel mit dem nicht-klassische Effekte bewirkt werden.

Zusammengesetzte Systeme in verschränkten Zuständen sind korreliert. Wenn beim obigen Zustand an den Teilsystemen jeweils die Observable σ_z gemessen wird, dann ergibt sich immer nur die Messwertekombination $(-1, -1)$ oder $(+1, +1)$. Im Gegensatz zu korrelierten klassischen Systemen sind aber in diesem Fall die Korrelationen von anderer Struktur. Mit ihrer Hilfe sind Prozesse möglich, die auf der Basis klassischer Korrelationen nicht möglich sind. Wir wollen im Folgenden die entsprechenden Konzepte näher erläutern.

8.1.1 Klassisch korrelierte Quantenzustände und LOCC

Korrelierte Quantenzustände Wir betrachten wieder ein zusammengesetztes System S^{AB} mit den Teilsystemen S^A und S^B . Zu irgend zwei (voneinander unabhängigen) Zuständen ρ^A und ρ^B gibt es immer einen Zustand $\hat{\rho}^{AB}$, so dass $\rho^A = \text{tr}_B[\hat{\rho}^{AB}]$ und $\rho^B = \text{tr}_A[\hat{\rho}^{AB}]$ gilt. Der Produktzustand $\hat{\rho}^{AB} = \rho^A \otimes \rho^B$ erfüllt diese Forderung. Nach Konstruktion liefern Messungen an den Teilsystemen stets voneinander unabhängige Messwerte. Umgekehrt wollen wir Zustände ρ^{AB} , die keine Produktzustände sind

$$\rho^{AB} \neq \rho^A \otimes \rho^B, \quad (8.1)$$

korreliert (correlated) nennen.

Diese mathematische Charakterisierung ist äquivalent zu einer operationalen Aussage über Messwerte, die im Prinzip durch Messungen an den Teilsystemen überprüft werden kann (vergl. Abschn. 7.3.3): Ein Zustand ρ^{AB} ist genau dann korreliert, wenn es Observablen C^A und D^B gibt, für die der Erwartungswert von $C^A \otimes D^B$ – gewonnen über die Produkte der zusammengehörigen Messergebnisse an S^A und S^B – sich nicht als Produkt der Erwartungswerte der reduzierten Dichteoperatoren ergibt. (vergl. Übungsaufgabe ÜA. 1 in Abschn. 8.7).

Klassisch korrelierte Quantenzustände Nach dieser allgemeinen Charakterisierung von Korreliertheit wollen wir einen speziellen Typ von Korrelationen beschreiben. Wir gehen dazu nicht wie oben von den Messwerten, sondern vom Präparationsverfahren aus.

Das Gesamtsystem S^{AB} wird von Alice und Bob durch lokale Operationen (das sind unitäre dynamische Entwicklung, Messungen und alle anderen Manipulationen mit lokalen Hilfsmitteln) und klassische Kommunikation präpariert werden. Man kürzt „local operations and classical communication“ mit *LOCC* ab. Hierzu präpariert Alice am System S^A den Zustand ρ_r^A und teilt das Bob über klassische Kommunikationskanäle mit, der seinerseits ρ_r^B präpariert. Dies wird häufig für unterschiedliche r in zufälliger Weise unter Einhaltung der relativen Häufigkeiten p_r wiederholt. Der präparierte Gesamtzustand ρ^{AB} ist dann nach Konstruktion eine Konvexkombination bzw. ein statistisches Gemisch (Gemenge) von Produktzuständen

$$\rho^{AB} = \sum_{r=1}^m p_r \rho_r^A \otimes \rho_r^B. \quad (8.2)$$

Die klassische Kommunikation wird dabei von Alice und Bob dazu verwendet, um ihre lokalen Aktionen zu korrelieren. Eine solche Prozedur könnte genauso mit klassischen Zuständen durchgeführt werden. Der Vergleich mit Gl. (8.1) zeigt, dass der resultierende Zustand ρ^{AB} korreliert ist, wenn sich die Summe nicht auf einen Term reduziert. Da die Korrelationen durch LOCC mit den Wahrscheinlichkeiten $\{p_r\}$ rein klassisch bewirkt werden, nennt man einen Quantenzustand ρ^{AB} , der sich in Form (8.2) schreiben lässt, *klassisch korreliert* (classically correlated). Wir notieren noch, dass man nach Einführung von Ensemblezerlegungen für alle ρ_r^A und ρ_r^B den Dichteoperator auch in der Form

$$\rho^{AB} = \sum_j \pi_j |a_j^A\rangle\langle a_j^A| \otimes |b_j^B\rangle\langle b_j^B| \quad (8.3)$$

mit $0 \leq \pi_j \leq 1$ und $\sum_j \pi_j = 1$ schreiben kann. Die beteiligten Zustände müssen dabei nicht orthogonal sein.

Wie beim Übergang von Gemenge zu Gemisch lösen wir uns wieder vom speziellen vom Präparationsverfahren. Ein Quantenzustand ρ^{AB} wird auch dann als klassisch korreliert bezeichnet, wenn er nicht in dem oben beschriebenen Präparationsverfahren erzeugt worden ist. Es reicht, dass er durch einen in dieser Weise präparierten Zustand in jeder Hinsicht simuliert werden kann, dass also seine statistischen Eigenschaften durch einen LOCC-Mechanismus reproduziert werden können. Mathematisch bedeutet das, dass ρ^{AB} sich in der Form (8.3) schreiben lässt.

Eine allerdings begrenzte Analogie zu korrelierten klassischen Systemen ist offensichtlich. Wir betrachten das Beispiel, dass in die Kisten von vielen Kistenpaaren mit der Wahrscheinlichkeit p_1 entweder je eine rote oder mit der Wahrscheinlichkeit p_2 je eine blaue Kugel gelegt

wird ($p_1 + p_2 = 1$). Wenn die Kisten geöffnet werden, stellt man eine Korrelation fest, die der Korrelation bei der Messung der Spinkomponenten in z -Richtung im klassisch korrelierten Quantenzustand

$$\begin{aligned}\rho^{AB} &= p_1 |0^A, 0^B\rangle\langle 0^A, 0^B| + p_2 |1^A, 1^B\rangle\langle 1^A, 1^B| \\ &= p_1 |0^A\rangle\langle 0^A| \otimes |0^B\rangle\langle 0^B| + p_2 |1^A\rangle\langle 1^A| \otimes |1^B\rangle\langle 1^B|\end{aligned}\quad (8.4)$$

entspricht. Wenn man beim klassisch korrelierten Zustand (8.4) am Teilsystem S^A eine Messung in der Rechenbasis durchführt, dann führt sie mit der Wahrscheinlichkeit p_1 auf den Zustand $|0^A\rangle$ und S^B befindet sich nach der Messung in dem zu $|0^A\rangle$ korrelierten Zustand $|0^B\rangle$.

Man sollte aber die Bezeichnung „klassisch korreliert“ für Quantensysteme nicht physikalisch überinterpretieren. Anders als in der klassischen Physik kann man in der Quantenphysik in gedrehten Basen messen. Eine Messung am Zustand ρ^{AB} von Gl. (8.4) mit $p_1 = p_2 = \frac{1}{2}$ in der Basis $\{|0_x^A\rangle, |1_x^A\rangle\}$ mit dem Endzustand $|0_x^A\rangle$ für S^A führt auf

$$\rho^{AB} \rightarrow \rho^{AB'} = |0_x^A\rangle\langle 0_x^A| \otimes \frac{1}{2} \mathbb{1}^B. \quad (8.5)$$

Der Zustand von S^B ist ein maximal gemischter Zustand. Die Zustände von S^A und S^B sind nach dieser Messung nicht korreliert. Dass ρ^{AB} von Gl. (8.4) klassisch korreliert ist, besagt nur, dass man ρ^{AB} durch LOCC präparieren kann, und dass man eine spezielle Messung finden kann (in diesem Fall die Messung in der Rechenbasis), nach der die Zustände der Teilsysteme korreliert sind.

8.1.2 Separabilität und Verschränkung

Es hat sich als sinnvoll erwiesen, die folgenden Begriffe einzuführen. Ein Zustand ρ^{AB} eines zusammengesetzten Systems S^{AB} heißt *separabel* (separable) genau dann, wenn er in der Form (8.2) einer Konvexkombination von Produktzuständen geschrieben werden kann. Ein separabler Zustand ist somit klassisch korreliert oder gar nicht korreliert ($m = 1$). Einen reinen oder gemischten Quantenzustand, der nicht separabel ist, nennen wir *verschränkt* (entangled). *Ein verschränkter Quantenzustand enthält daher nicht-klassische Korrelationen, die auch Quantenkorrelationen (quantum correlations) oder EPR-Korrelationen¹ (EPR correlations) genannt werden. Darin liegt seine große physikalische Bedeutung.*

Das Präparationsverfahren LOCC führt auf separable Zustände. *Verschränkte Zustände können nicht durch LOCC erzeugt werden.* Man kann diese Charakterisierung auch als eine äquivalente Definition von Verschränkung nehmen.

Es ist ein wichtiges Charakteristikum der Quantenphysik verglichen mit der klassischen Physik, dass nicht alle Korrelationen klassisch sein müssen. Das sieht man unmittelbar am Beispiel der reinen Zuständen in $\mathcal{H}^A \otimes \mathcal{H}^B$. Wir haben in Abschn. 4.1.3 gesehen, dass der Dichteoperator eines reinen Zustands $|\psi^{AB}\rangle$ nicht in eine konvexe Summe zerlegt werden

¹Das Akronym EPR kürzt die Namen A. Einstein, B. Podolsky und N. Rosen ab. Diese Personen haben in einer bedeutenden Arbeit [EPR 35] den Anstoß zu solchen Überlegungen gegeben, wie wir sie insbesondere in Kap. 10 durchführen wollen. Die Bezeichnung EPR hat sich allerdings in der Zwischenzeit weitgehend von dieser Arbeit gelöst und charakterisiert z. B. die Korrelationen, die an verschränkten Systemen gemessen werden, und die zugehörigen Experimente. EPR ist daher heute eine systematische Bezeichnung und kein historischer Verweis.

kann. Damit kann er nicht wie in Gl. (8.2) klassisch korreliert sein. *Wenn ein reiner Zustand kein Produktzustand ist*

$$|\psi^{AB}\rangle \neq |\phi^A\rangle \otimes |\chi^B\rangle \quad (8.6)$$

und somit die Bedingung (8.1) für Korreliertheit erfüllt, ist er verschränkt und damit nicht-klassisch korreliert. Das heißt, er muß einen neuen Typ von Korrelationen enthalten, der bei klassischen Systemen nicht auftritt. Wir werden die weitreichenden physikalischen Konsequenzen noch ausführlich diskutieren.

8.1.3 Das Separabilitätsproblem

Da Verschränkung als Hilfsmittel eine große Rolle spielt, ist es eine wichtige Aufgabe, Kriterien zu entwickeln, mit deren Hilfe abgelesen werden kann, ob ein gegebener Zustand verschränkt ist. Für reine Zustände von 2-Teile-Systemen ist das einfach. *Der Zustand $|\psi^{AB}\rangle$ ist genau dann separabel, wenn er von der Form $|\psi^{AB}\rangle = |\phi^A\rangle \otimes |\chi^B\rangle$ ist, d.h wenn jeder seiner beiden reduzierten Dichteoperatoren ein reiner Zustand ist.* Wir werden in Abschn. 8.2 mit der Schmidt-Zerlegung ein weiteres Kriterium kennenlernen, das auch auf ein Maß für Verschränkung führt. Mit Hilfe der Quantenentropie der Teilsysteme werden wir in Abschn. 8.2.3 das heute allgemein akzeptierte Maß für die Verschränkung reiner Zustände von 2-Teile-Systemen einführen.

Für gemischte Zustände ist die Situation schwieriger. Wir verdeutlichen das an einem Beispiel. Die Bell-Zustände von Gl. (7.11) sind verschränkte reine Zustände. Das kann man nach dem oben angegebenen Kriterium unmittelbar an den reduzierten Dichteoperatoren ablesen, die gleich $\frac{1}{2}\mathbb{1}$ sind. Durch Mischen der verschränkten (!) Zustände $|\Phi_+^{AB}\rangle$ und $|\Phi_-^{AB}\rangle$ mit gleichen Wahrscheinlichkeiten entsteht der Zustand

$$\rho^{AB} = \frac{1}{2}(|\Phi_+^{AB}\rangle\langle\Phi_+^{AB}| + |\Phi_-^{AB}\rangle\langle\Phi_-^{AB}|).$$

Wenn man die Definitionen der Bell-Zustände einsetzt, ergibt sich

$$\begin{aligned} \rho^{AB} &= \frac{1}{2}(|0^A, 0^B\rangle\langle 0^A, 0^B| + |1^A, 1^B\rangle\langle 1^A, 1^B|) \\ &= \frac{1}{\sqrt{2}}(|0^A\rangle\langle 0^A| \otimes |0^B\rangle\langle 0^B| + |1^A\rangle\langle 1^A| \otimes |1^B\rangle\langle 1^B|). \end{aligned} \quad (8.7)$$

Der Zustand ρ^{AB} ist vom Typ (8.2) und daher nicht verschränkt. Es ist möglich ihn alternativ auch allein durch LOCC zu präparieren.

Ein gegebener Dichteoperator hat unendlich viele Ensemblezerlegungen. Wenn eine darunter die Form (8.2) hat, ist der Zustand separabel, sonst ist er verschränkt. Eine Aussage hierüber, die sich ja auf alle möglichen Ensemblezerlegungen beziehen muß ist bis heute nicht befriedigend möglich. Das entsprechende Forschungsprogramm wird das *Separabilitätsproblem* (separability problem) genannt: Ist ein durch einen Dichteoperator gegebener Zustand eines zusammengesetzten Quantensystems separabel oder nicht? Allgemein anwendbare Maß für die Verschränkung von Gemischen existieren ebenfalls bisher nicht. Wenn ein System aus mehr als zwei Teilen besteht, ist die Situation noch komplizierter.

Eine andere Aufgabe ist es, ein Maß für die Korreliertheit von zwei Teilsystemen anzugeben. Wir werden den Korreliertheitsgrad in Kap. 6 mit Hilfe der von-Neumannschen wechselseitigen Entropie (bzw. Information) beschreiben. Dies ist ein weiterer Themenkreis, in dem Entropie eine wichtige Rolle spielt.

8.2 Verschränkte reine Zustände

8.2.1 Schmidt-Zerlegung

Für die Diskussion der Verschränkung reiner Zustände $|\psi^{AB}\rangle$ von 2-Teile-Systemen hat sich die *Schmidt-Zerlegung* (Schmidt decomposition) als besonders hilfreich erwiesen. Sie wird auch *bi-orthogonale oder polare Zerlegung* (bi-orthogonal or polar expansion) des Vektors $|\psi^{AB}\rangle$ genannt. Sie besagt das Folgende:

$|\psi^{AB}\rangle$ sei ein normierter Zustand des zusammengesetzten Systems S^{AB} im Produkt-Hilbert-Raum $\mathcal{H}^{AB} = \mathcal{H}^A \otimes \mathcal{H}^B$ mit $\dim \mathcal{H}^A = a$ und $\dim \mathcal{H}^B = b$. Mit $\rho^{AB} = |\psi^{AB}\rangle\langle\psi^{AB}|$ sind $\rho^A = \text{tr}_B[\rho^{AB}]$ und $\rho^B = \text{tr}_A[\rho^{AB}]$ die reduzierten Dichteoperatoren der Teilsysteme S^A und S^B . Dann gilt:

- (i) Der Vektor $|\psi^{AB}\rangle$ kann in Form der Schmidt-Zerlegung²

$$|\psi^{AB}\rangle = \sum_{n=1}^k \sqrt{p_n} |u_n^A, w_n^B\rangle \quad \text{mit } p_n > 0 \quad (8.8)$$

geschrieben werden, wobei $\{|u_n^A\rangle$ (bzw. $\{|w_n^B\rangle\}$) die orthonormierten Eigenvektoren von ρ^A in \mathcal{H}^A (bzw. ρ^B in \mathcal{H}^B) mit geeignet gewählten Phasen sind. Für paarweise verschiedene p_n sind die Vektoren $|u_n^A\rangle$ und $|w_n^B\rangle$ bis auf eine Phase eindeutig bestimmt. Daraus folgt:

- (ii) ρ^A und ρ^B haben dieselben nicht verschwindenden positiven Eigenwerte p_1, \dots, p_k mit $k \leq \min(a, b)$ (bei g -facher Entartung wird der entsprechende Eigenwert g -fach wiederholt).

Die Zahl k heißt der *Schmidt-Rang* (Schmidt rank) von $|\psi^{AB}\rangle$.

Zum Beweis zerlegen wir $|\psi^{AB}\rangle$ nach den ONB $\{|c_l^A\rangle\}$ bzw. $\{|d_i^B\rangle\}$ von \mathcal{H}^A bzw. \mathcal{H}^B

$$|\psi^{AB}\rangle = \sum_{l,i=1}^{a,b} a_{li} |c_l^A, d_i^B\rangle \quad (8.9)$$

und führen wieder die relativen Zustände

$$|\tilde{w}_l^B\rangle = \sum_{i=1}^b a_{li} |d_i^B\rangle \quad (8.10)$$

²E. Schmidt, Math. Ann. 63,433 (1906).

ein:

$$|\psi^{AB}\rangle = \sum_{l=1}^a |c_l^A, \tilde{w}_l^B\rangle. \quad (8.11)$$

Die relativen Zustände $|\tilde{w}_l^B\rangle$ sind i. a. weder orthogonal noch normiert. Wir zeigen wie die für Gl. (8.8) behauptete Orthogonalität erreicht werden kann.

Dazu wählen wir als ONB $\{|c_l^A\rangle\}$ in Gl. (8.9) speziell die orthonormalen Eigenvektoren $\{|u_n^A\rangle\}$ von ρ^A und zerlegen ρ^A

$$\rho^A = \sum_{n=1}^a p_n |u_n^A\rangle\langle u_n^A| \quad \text{mit } p_n \geq 0, \quad \sum_{n=1}^a p_n = 1. \quad (8.12)$$

Es sei $p_n > 0$ für $0 \leq n \leq k$ und $p_n = 0$ für $k+1 \leq n \leq a$. Die Vektoren $|u_n^A\rangle$ sind nur bis auf einen Phasenfaktor festgelegt. Andererseits gilt mit den zu $\{|u_n^A\rangle\}$ relativen Zustände $\{|\tilde{w}_n^B\rangle\}$

$$\begin{aligned} \rho^A &= \text{tr}_B[|\psi^{AB}\rangle\langle\psi^{AB}|] \\ &= \text{tr}_B\left[\sum_{l,n=1}^a |u_l^A\rangle\langle u_n^A| \otimes |\tilde{w}_l^B\rangle\langle\tilde{w}_n^B|\right] = \\ &= \sum_{l,n=1}^a |u_l^A\rangle\langle u_n^A| \text{tr}_B[|\tilde{w}_l^B\rangle\langle\tilde{w}_n^B|] = \\ &= \sum_{l,n=1}^a \langle\tilde{w}_n^B|\tilde{w}_l^B\rangle |u_l^A\rangle\langle u_n^A| \end{aligned} \quad (8.13)$$

wobei im letzten Schritt

$$\text{tr}_B[|\tilde{w}_l^B\rangle\langle\tilde{w}_n^B|] = \sum_{i=1}^b \langle d_i^B|\tilde{w}_l^B\rangle\langle\tilde{w}_n^B|d_i^B\rangle \quad (8.14)$$

$$= \sum_{i=1}^b \langle\tilde{w}_n^B|d_i^B\rangle\langle d_i^B|\tilde{w}_l^B\rangle = \langle\tilde{w}_n^B|\tilde{w}_l^B\rangle \quad (8.15)$$

eingesetzt wurde. Der Vergleich von (8.12) mit (8.13) führt auf die Orthogonalität:

$$\langle\tilde{w}_n^B|\tilde{w}_l^B\rangle = p_n \delta_{nl} \quad i, k = 1 \dots n \quad (8.16)$$

Für $n \geq k+1$ sind die $|\tilde{w}_n^B\rangle$ Nullvektoren. Damit ist die Behauptung von (i) bewiesen. (ii) ist eine direkte Folge.

Mit Gl. (8.16) reduziert sich die Summe in Gl. (8.13) auf

$$\rho^A = \sum_{i=1}^k p_n |u_n^A\rangle\langle u_n^A|. \quad (8.17)$$

Die $\{p_n\}$ heißen *Schmidt-Koeffizienten*. Wir ergänzen noch, dass auch der reduzierte Dichteoperator ρ^B die p_n als Eigenwerte hat

$$\rho^B = \sum_{n=1}^k p_n |w_n^B\rangle \langle w_n^B|. \quad (8.18)$$

Das hat unmittelbar zur Folge, dass jede Funktion eines Dichteoperators, die nur von seinen Eigenwerten abhängt, für beide reduzierten Dichteoperatoren denselben Wert hat. Die von-Neumann-Entropie, die wir in Kap. 6 eingeführt haben, ist ein Beispiel.

Ein Schmidt-Zerlegung bezieht sich immer auf einen bestimmten reinen Zustand eines zusammengesetzten Systems. Verschiedene Zustände haben verschiedene Schmidt-Zerlegungen. Im allgemeinen kann die Schmidt-Zerlegung nicht auf Systeme mit mehr als zwei Teilsystemen ausgedehnt werden. Etwas ähnliches wie die Schmidt-Zerlegung gibt es für Gemische nicht.

8.2.2 Schmidt-Zahl und Verschränkung

Wir wollen einige Beispiele für die Nützlichkeit der Schmidt-Zerlegung geben. $\{|u_n^A\rangle\}$ bzw. $\{|w_n^B\rangle\}$ mit $n = 1, \dots, k$ heißen *Schmidt-Basen* von \mathcal{H}^A bzw. \mathcal{H}^B . In ihnen sind die beiden reduzierten Dichteoperatoren diagonal. Die *Schmidt-Zahl* k ist die Zahl der nicht verschwindenden Schmidt-Koeffizienten. $|\psi^{AB}\rangle$ ist genau dann ein Produktzustand und damit nicht verschränkt, wenn die Schmidt-Zahl gleich Eins ist. ρ^A und ρ^B haben dann den Rang Eins. Das ist gleichbedeutend mit $\text{tr}[(\rho^A)^2] = \text{tr}[(\rho^B)^2] = 1$. Ob ein reiner Zustand $|\psi^{AB}\rangle$ verschränkt ist oder nicht, lässt sich somit direkt an dem reduzierten Dichteoperator eines Teilsystems ablesen. Die Schmidt-Zahl kann als ein Maß für die Verschränkung dienen. Darin liegt ihre hauptsächliche Bedeutung. Weiterhin können wir direkt ablesen: Wenn einer der reduzierten Dichteoperatoren einen reinen Zustand beschreibt, dann tut es auch der andere. Wenn sich das Gesamtsystem S^{AB} in einem reinen Zustand $|\psi^{AB}\rangle$ befindet ist es daher unmöglich, dass eines der Untersysteme sich in einem reinen Zustand befindet und das andere in einem echten Gemisch. Wir werden diese Aussage noch verallgemeinern.

Ähnlich finden wir: Wenn ein Qubit-System mit einem System mit m linear unabhängigen Zuständen verschränkt ist, dann besteht die Schmidt-Zerlegung nur aus zwei Termen. In Rechnungen ist es oft geschickt diese Schmidt-Basis einzuführen. Allgemein gilt der Satz: Wenn ein Teilsystem die Dimension d hat, dann kann es mit nicht mehr als d orthogonalen Zuständen eines anderen Systems verschränkt werden.

Wenn ρ^A und damit auch ρ^B als einzige entartete Eigenwerte allenfalls die Null haben, dann ist die Schmidt-Zerlegung durch ρ^A und ρ^B eindeutig festgelegt. Man bestimmt dazu die Eigenzustände von ρ^A und ρ^B und bildet das Produkt der Zustände zum gleichen Eigenwert wie in Gl. (8.8).

Wir geben ein Beispiel für Entartung an. Der Bell-Zustand

$$|\Psi_-^{AB}\rangle = \frac{1}{\sqrt{2}}(|0^A, 1^B\rangle - |1^A, 0^B\rangle) \quad (8.19)$$

ist wie alle anderen Bell-Zustände verschränkt. Die zugehörigen Basen in \mathcal{H}^A bzw. \mathcal{H}^B sind z. B. $\{|0^A\rangle, |1^A\rangle\}$ und $\{|1^B\rangle, -|0^B\rangle\}$. Der Zustand $|\Psi_-^{AB}\rangle$ weist eine sphärische Symmetrie

auf, denn man bestätigt leicht, dass

$$|\Psi_-^{AB}\rangle = \frac{1}{\sqrt{2}}(|0_r^A, 1_r^B\rangle - |1_r^A, 0_r^B\rangle) \quad (8.20)$$

gilt, wobei $|0_r\rangle$ und $|1_r\rangle$ die Eigenvektoren von $\mathbf{r}\sigma$ zu beliebigem Bloch-Vektor \mathbf{r} sind (vergl. Gl. (3.31)). Dies demonstriert, dass in diesem Fall die Schmidt-Zerlegung nicht eindeutig ist. Wenn mehrere p_n in Gl. (8.8) übereinstimmen, können die entsprechenden Vektoren $|u_n^A, w_n^B\rangle$ durch Linearkombinationen ersetzt werden. Dem entspricht es, dass für $|\Psi_-^{AB}\rangle$ die Eigenvektoren der reduzierten Dichteoperatoren

$$\rho^A = \rho^B = \frac{1}{2}\mathbb{1} \quad (8.21)$$

nicht festgelegt sind.

Purifizierung Der folgende Hilfssatz ist nützlich: *Für jedes System mit Dichteoperator ρ^A aus \mathcal{H}^A existiert ein reiner Zustand $|\phi^{AB}\rangle$ aus $\mathcal{H}^A \otimes \mathcal{H}^B$, so dass ρ^A der zugehörige reduzierte Dichteoperator ist:*

$$\rho^A = \text{tr}_B[|\phi^{AB}\rangle\langle\phi^{AB}|] . \quad (8.22)$$

Zum Beweis betrachten wir die ONB $\{|u_n^A\rangle\}$, in der ρ^A diagonal ist:

$$\rho^A = \sum_{n=1}^a p_n |u_n^A\rangle\langle u_n^A| . \quad (8.23)$$

Gemäß Schmidt-Zerlegung ist dann

$$|\phi^{AB}\rangle = \sum_{n=1}^a \sqrt{p_n} |u_n^A, w_n^B\rangle \quad (8.24)$$

mit irgendeiner ONB $\{|w_n^B\rangle\}$ eine mögliche Purifizierung. Andere Purifizierungen gehen durch unitäre Transformationen dieser Basis daraus hervor. Dies macht noch einmal deutlich, dass es zur Bildung der Teilspur keine eindeutige Umkehrung gibt. Es gibt unendlich viele Gesamtsysteme S^{AB} , die im Zustand S^A übereinstimmen.

8.2.3 Entropie der Teilsysteme als Maß für Verschränkung

Reine Zustände eines 2-Teile-Systems S^{AB} sind entweder in einem Produktzustand, dann sind die Teilsysteme nicht korreliert, oder sie sind verschränkt, dann sind sie EPR-korreliert. Korrelationen können in diesem Fall nur nicht-klassisch sein. Wir bezeichnen die Entropie des Gesamtsystems mit $S(AB)$ und die mit den reduzierten Dichteoperatoren $\rho^A = \text{tr}_B[\rho^{AB}]$ und $\rho^B = \text{tr}_A[\rho^{AB}]$ gebildeten Entropien der Teilsysteme mit $S(A)$ und $S(B)$. Da wir nur reine Zustände betrachten liegt stets die maximale Information über den Gesamtzustand vor.

$$S(AB) = 0 . \quad (8.25)$$

Bei einem Produktzustand liegt auch über den Zustand der Teilsysteme die maximale Information vor

$$S(A) = S(B) = 0 . \quad (8.26)$$

Demgegenüber sind z. B. die Dichteoperatoren der Bell-Zustände völlig strukturlos

$$\rho^A = \rho^B = \frac{1}{2} \mathbb{1} . \quad (8.27)$$

Die Teilsysteme sind in diesem Fall maximal gemischt und maximal unbestimmt

$$S(A) = S(B) = 1 . \quad (8.28)$$

Die Entropie (Unbestimmtheit des Zustands) der Teilsysteme ist ein Maß für die – verglichen mit dem reinen Zustand – fehlende Information. Wenn man nur die Teilsysteme betrachtet, verliert man umsomehr Information über den Gesamtzustand, je mehr Informationen in den Korrelationen zwischen den Teilzuständen enthalten ist. Je größer daher die Entropie der Zustände der Teilsysteme ist, umso stärker ist der reine Zustand des Gesamtsystems korreliert und damit verschränkt. *Wir nehmen daher bei einem reinen Zustand $|\psi^{AB}\rangle$ des Gesamtsystems den Wert $E(\psi)$ der Entropie der Teilsysteme*

$$0 \leq E(\psi) := S(A) = S(B) \leq 1 \quad (8.29)$$

als Maß für die Verschränktheit des Zustandes. $E(\psi)$ heißt auch *Entropie der Verschränkung* (entropy of entanglement). Diese Quantifizierung der Verschränkung gilt nur für reine Gesamtzustände. Für gemischte Zustände gibt es eine Reihe von Vorschlägen für Verschränkungsmaß, die im Spezialfall reiner Zustände von 2-Teile-Systemen mit $E(\psi)$ übereinstimmen (vergl. Abschn. 8.6).

Die Entropie der Verschränkung hängt nur von den Schmidt-Koeffizienten ab. Sie ist basisunabhängig und ändert sich nicht unter lokalen unitären Transformationen. Mit $|\psi^{AB}\rangle = U^A \otimes U^B |\psi^{AB}\rangle$ gilt $E(\psi') = E(\psi)$. Zustände in $\mathcal{H}_d \otimes \mathcal{H}_d$ für die $E(\psi) = \log d$ mit $d = \dim \mathcal{H}$ gilt, heißen *maximal verschränkt* (maximally entangled). Bell-Zustände sind hierfür ein Beispiel.

8.2.4 Teilsysteme in reinen Zuständen sind total isoliert

Wir beweisen einen Satz für Gemische, den wir für reine Zustände von S^{AB} oben schon erwähnt haben: *Wenn bei einem 2-Teile-System S^{AB} , das sich in einem gemischten Zustand ρ^{AB} befindet, der reduzierte Dichteoperator ρ^A eines Teilsystems S^A der eines reinen Zustands ist, dann ist ρ^{AB} separabel.* Da wir eine Aussage über Gemische anstreben, ist zum Beweis dieses Satzes ein Rückgriff auf die Schmidt-Zerlegung nicht möglich.

Wir diskutieren zunächst den Fall, dass ρ^A ein Gemisch ist. ρ^A ist ein positiver Operator. Er lässt sich nach seinen orthonormalen Eigenzuständen zerlegen, die wir zu einer ONB $|u_n^A\rangle$ ergänzen

$$\rho^A = \sum_n r_n |u_n^A\rangle \langle u_n^A|, \quad \sum_n r_n = 1, \quad r_n \geq 0 . \quad (8.30)$$

Entsprechendes gilt für ρ^{AB}

$$\rho^{AB} = \sum_q s_q |\psi_q^{AB}\rangle \langle \psi_q^{AB}|, \quad \sum_q s_q = 1, \quad s_q > 0. \quad (8.31)$$

Es ist rechentechnisch günstig, die Eigenvektoren $|\psi_q^{AB}\rangle$ mit Hilfe der jeweiligen Relativzustände $|\tilde{w}_n^{(q)B}\rangle$ zu $|u_n^A\rangle$ zu schreiben (vergl. Abschn. 7.3.5). Um die Rechnung übersichtlich zu gestalten, werden wir weitgehend auf die Indizes A und B sowie auf die Tilde verzichten. Wir erhalten

$$|\psi_q^{AB}\rangle = |\psi_q\rangle = \sum_n |u_n, w_n^{(q)}\rangle \quad (8.32)$$

und damit

$$\begin{aligned} \rho^{AB} &= \sum_{q,n,m} s_q |u_n, w_n^{(q)}\rangle \langle u_m, w_m^{(q)}| \\ &= \sum_{n,m} |u_n\rangle \langle u_m| \otimes \sum_q s_q |w_n^{(q)}\rangle \langle w_m^{(q)}|. \end{aligned} \quad (8.33)$$

Dies ist im allgemeinen kein separabler Zustand. Für den reduzierten Dichteoperator ρ^A des Teilsystems S^A folgt

$$\rho^A = \text{tr}_B[\rho^{AB}] = \sum_{n,m} |u_n\rangle \langle u_m| \sum_q s_q \langle w_m^{(q)} | w_n^{(q)} \rangle. \quad (8.34)$$

Bei der Spurbildung mit der ONB $\{|v_i\rangle\}$ von \mathcal{H}^B haben wir von der Relation

$$\sum_i \sum_q s_q \langle v_i | w_n^{(q)} \rangle \langle w_m^{(q)} | v_i \rangle = \sum_q s_q \langle w_n^{(q)} | w_m^{(q)} \rangle \quad (8.35)$$

Gebrauch gemacht.

Mit Gl. (8.30) und (8.34) ergeben sich die Matrixelemente von ρ^A als

$$\langle u_k | \rho^A | u_l \rangle = r_k \delta_{kl} = \sum_q s_q \langle w_l^{(q)} | w_k^{(q)} \rangle. \quad (8.36)$$

Wenn speziell $r_k = 0$ ist, dann gilt

$$\sum_q s_q ||w_k^{(q)}|| = 0 \quad (8.37)$$

und mit $s_q > 0$

$$||w_k^{(q)}|| = 0, \quad |w_k^{(q)}\rangle = 0 \quad (8.38)$$

für alle q .

Mit diesem Ergebnis kehren wir zum Ausgangsproblem zurück. ρ^A soll ein reiner Zustand sein. Ohne Einschränkung setzen wir

$$\rho^A = |u_1\rangle \langle u_1|. \quad (8.39)$$

Dann gilt $r_{n \neq 1} = 0$ und damit $|w_{n \neq 1}^{(q)}\rangle = 0$. Einsetzen in Gl. (8.33) führt auf

$$\rho^{AB} = |u_1\rangle\langle u_1| \otimes \sum_q s_q |w_1^{(q)}\rangle\langle w_1^{(q)}|. \quad (8.40)$$

Der Dichteoperator ρ^{AB} ist also separabel. Das ergibt das bemerkenswerte physikalische Ergebnis: *Wenn ein System in einem reinen Zustand ist, kann es nicht mit einem anderen System verschränkt sein.* Es existieren keine Korrelationen zwischen diesem System und irgendeinem anderen System. Es ist total isoliert.

Die Postulate aus Abschn. 2.1 beziehen sich auf reine Zustände. Die durch diese Postulate beschriebenen Systeme sind daher notwendigerweise auch gegen EPR-Korrelationen isoliert. Wir notieren noch eine weitere Folge: Eine Messung an einem Teilsystem mit nicht-entartetem Messwert überführt dieses Teilsystem in einen reinen Zustand. *Daher durchbricht diese projektive Messung die Verschränkung mit anderen Teilsystemen unabhängig davon, ob das Gesamtsystem vorher in einem gemischten oder in einem reinen Zustand war.* Wieder erwies sich eine projektive Messung als ein i.a. starker Eingriff.

8.3 Erzeugung verschränkter Zustände

Die Erzeugung von verschränkten Zuständen ist vom theoretischen Standpunkt aus sehr einfach. Ein zusammengesetztes System, das aus zwei Teilsystemen bestehen soll, möge sich zum Zeitpunkt t_0 in einem Produktzustand

$$|\psi^{AB}\rangle = |\phi^A\rangle \otimes |\chi^B\rangle \quad (8.41)$$

befinden. Wenn das System für $t > t_0$ eine dynamische Entwicklung mit einem unitären Operator U^{AB} erfährt, der kein Produktoperator ist

$$U^{AB} \neq U^A \otimes U^B, \quad (8.42)$$

– dies ist der Normalfall – dann geht es dabei in einen verschränkten Zustand über. In diesem Sinne ist Verschränktheit der „Normalzustand“. Tatsächlich erfordert die gezielte Produktion wohlbestimmter verschränkter Zustände (wie z. B. der Bell-Zustände) für vorgegebene Sorten von Quantenobjekten (wie z. B. Photonen) experimentellen Aufwand.

Kaskaden-Photonen Es gibt heute eine Reihe experimenteller Möglichkeiten, verschränkte Zustände im Labor zu erzeugen. Wir wollen exemplarisch ein Beispiel diskutieren. Für den Nachweis von Korrelationen sind die Polarisationen von Photonenpaaren besonders geeignet, da Photonen ohne Störung über Labordistanzen und noch größere Entfernungen propagieren. Wir schildern eine Quelle für Verschränkung, die im optischen Bereich arbeitet. Weitere Einzelheiten finden sich in den Literaturangaben in Abschn. 8.6.

Ein Atom geht in zwei aufeinander folgenden Übergängen in einer *Kaskade* (cascade) aus einem angeregten Zustand über einen Zwischenzustand in den Grundzustand über. Eine solche Kaskade kann z. B. mit Kalziumatomen realisiert werden (vgl. Abb. 8.1). Die beiden emittierten Photonen haben die Wellenlängen $\lambda_A = 551,3$ nm bzw. $\lambda_B = 422,7$ nm. Sie werden

i.a. nicht in entgegengesetzten Richtungen davonfliegen. Man beschränkt sich im Experiment aber auf Paare, bei denen z. B. das Photon mit Wellenlänge λ_A in positiver und das mit Wellenlänge λ_B in negativer z -Richtung fliegt. Da bei dem $J = 0 \rightarrow J = 1 \rightarrow J = 0$ Übergang sich der Gesamtdrehimpuls J nicht ändert, müssen diese Photonen zirkular polarisiert sein und entgegengesetzten Drehimpuls haben. Aus den Einzelheiten des atomaren Zerfalls folgt weiterhin, dass der Gesamtzustand der beiden Photonen gerade Parität haben muss. Diese beiden Bedingungen sind vom Zustand des 2-Photonen-Systems zu erfüllen.

Wir haben in Abschn. 3.6 gesehen, dass die rechts- und linkspolarisierten Zustände bei vorgegebener Ausbreitungsrichtung \mathbf{k} eine Basis im Hilbert-Raum \mathcal{H}_2 der Polarisationen bilden. Für das Photonenpaar sind also $|R^A, R^B\rangle, |R^A, L^B\rangle, |L^A, R^B\rangle, |L^A, L^B\rangle$ eine Basis des Produktraumes $\mathcal{H}^A \otimes \mathcal{H}^B$. Mit A und B bezeichnen wir dabei die positive bzw. negative z -Richtung in der die einzelnen Photonen fliegen. Der Wellenvektor \mathbf{k} ist also in einem Fall proportional zu \mathbf{e}_z und im anderen zu $-\mathbf{e}_z$. Wegen des verschwindenden Gesamtdrehimpulses kann der 2-Photonen-Zustand nur eine Linearkombination aus $|R^A, R^B\rangle$ und $|L^A, L^B\rangle$ sein (vergl. Abb. 8.2)

$$|\phi^{AB}\rangle = \alpha|R^A, R^B\rangle + \beta|L^A, L^B\rangle. \quad (8.43)$$

Aus der Physik des atomaren Übergangs kommt eine weitere Forderung hinzu: Der 2-Photonen-Zustand muß gerade Parität haben, Das heißt, wenn man Rechtshändigkeit mit Linkshändigkeit vertauscht, muß er in sich selbst übergehen. Das ist offenbar nur möglich für eine spezielle Wahl von α und β :

$$|\Phi_+^{AB}\rangle = \frac{1}{\sqrt{2}} (|R^A, R^B\rangle + |L^A, L^B\rangle). \quad (8.44)$$

Der 2-Photonen-Zustand ist daher auf Grund der Symmetrien des Erzeugungsprozesses, die er widerspiegeln muß, ein Bell-Zustand.

Die Verschränktheit wird plausibel, wenn man berücksichtigt, dass der intermediäre Zustand mit $J = 1$ entartet ist. Der Grundzustand kann daher über zwei verschiedene Zwischenzustände erreicht werden (vgl. Abb. 8.1). Beide „Wege“ sind möglich. In Analogie zu den „Wegen“ beim Doppelspalt interferieren die resultierenden Zustände. Dabei werden auf dem einen „Weg“ zwei rechtszirkular polarisierte Photonen emittiert und auf dem anderen zwei linkszirkulare. Diese Korrelation führt zusammen mit der Superposition auf Verschränkung.

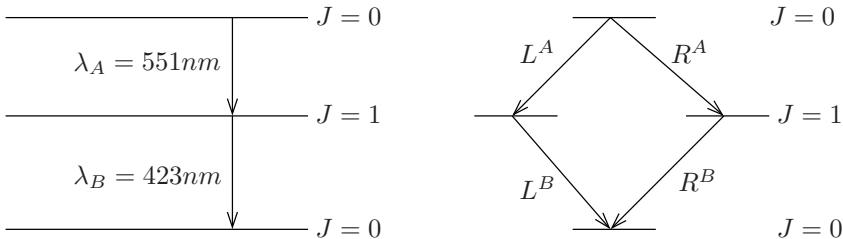
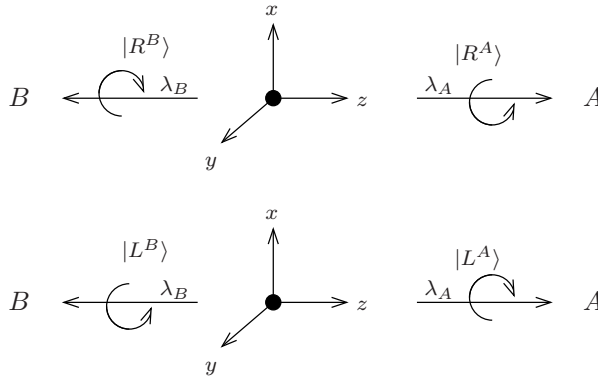


Abbildung 8.1: Übergangsschema der Kaskaden-Photonen.

**Abbildung 8.2:** Polarisationen der Kaskaden-Photonen

Der Bell-Zustand $|\Phi_+^{AB}\rangle$ von Gl. (8.44) gibt genau diese Entstehungssituation der Photonenpaare wieder.

Für spätere Zwecke rechnen wir noch auf die linearen Polarisierungen in x -Richtung und y -Richtung um. Wir können hierzu Gl. (3.63) und (3.64) benutzen, müssen dabei aber die Konvention von Abb. 8.2 bei der Ausbreitungsrichtung beachten. Wir finden

$$\begin{aligned}
 |R^A\rangle &= \frac{1}{\sqrt{2}}(|x^A\rangle + i|y^A\rangle) \\
 |L^A\rangle &= \frac{1}{\sqrt{2}}(|x^A\rangle - i|y^A\rangle) \\
 |R^B\rangle &= \frac{1}{\sqrt{2}}(|x^B\rangle - i|y^B\rangle) \\
 |L^B\rangle &= \frac{1}{\sqrt{2}}(|x^B\rangle + i|y^B\rangle)
 \end{aligned} \tag{8.45}$$

und damit für den verschränkten Zustand

$$|\Phi_+^{AB}\rangle = \frac{1}{\sqrt{2}}(|x^A, x^B\rangle + |y^A, y^B\rangle). \tag{8.46}$$

In unserer Rechnung war die Lage der x -Achse und der y -Achse nicht festgelegt. Gl. (8.46) gilt für beliebige Orientierungen. Der Zustand $|\Phi_+^{AB}\rangle$ ist rotationssymmetrisch bezüglich der z -Achse. Wir kommen auf diesen 2-Photonen-Zustand in Kap. 10 zurück.

8.4 Informationsübertragung mit Überlichtgeschwindigkeit und das No-cloning-Theorem

Wir haben gesehen, dass eine Messung am Teilsystem A das Teilsystem B instantan in einen wohlbestimmten Zustand überführt. Das Wort „instantan“ ist verführerisch. Stellen wir uns

vor, es ist ein verschränkter reiner Zustand erzeugt worden, dessen Teilsystem S^A sich bei Alice befindet und dessen anderes Teilsystem S^B sehr weit entfernt bei Bob befindet. Alice versucht an Bob eine Information mit einem Bit zu übermitteln, indem sie wahlweise eine von zwei nicht kommutierenden Observablen an ihrem Untersystem S^A misst. Falls es Bob gelingt durch Messung an seinem Untersystem S^B diese Information auszulesen, dann wäre sie mit Überlichtgeschwindigkeit übertragen worden und die Relativitätstheorie wäre widerlegt.

Wir beschreiben das vorgeschlagene Verfahren im Einzelnen. Alice und Bob haben jeweils Zugriff auf ein Photon eines polarisationsverschränkten Photonenpaars, das sich z. B. im Bell-Zustand

$$|\Psi_-\rangle = \frac{1}{\sqrt{2}}(|H, V\rangle - |V, H\rangle) = \frac{1}{\sqrt{2}}(|-45^\circ, 45^\circ\rangle + |45^\circ, -45^\circ\rangle) \quad (8.47)$$

befindet. Alice führt eine Messung entweder in der $\{|H\rangle, |V\rangle\}$ -Basis oder in der um 45° gedrehten Basis mit den Vektoren $|+45^\circ\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$ und $|-45^\circ\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$ durch. Diese beiden Basissysteme sind Bob bekannt. Die Wahl der einen oder der anderen Basis durch Alice ist die Information, die übertragen werden soll.

In dem Augenblick, in dem Alice durch Messung mit einem Observablenoperator zu einem der beiden Basissysteme ihr Photon in einen bestimmten Zustand (z. B. $|-45^\circ\rangle$) überführt, geht der Zustand des Photons bei Bob in den dazu senkrechten Zustand über (im Beispiel $|+45^\circ\rangle$). Wenn Bob die Polarisation seines Photons messen könnte, dann könnte er die Botschaft von Alice lesen. Bob kann aber zur Messung nur zufällig eine der beiden Basen wählen und es steht ihm zur Messung auch nur ein Photon zur Verfügung. Wenn Bobs Photon wie in unserem Beispiel im Zustand $|+45^\circ\rangle$ ist und er in der Basis $\{|H^B\rangle, |V^B\rangle\}$ misst kann entweder der Detektor zu H-Polarisation oder der Detektor zu V-Polarisation ansprechen. Eine einzige Messung reicht also nicht aus, um die $(+45^\circ)$ -Polarisation mit Sicherheit zu ermitteln. Bob kann daher die Information nicht auslesen. Wenn Bob aber eine Maschine hätte, die viele Kopien seines Photons herstellen kann, dann wäre eine Zustandsbestimmung und damit die Informationsübertragung möglich. Das führt auf die Frage, ob man Quantensysteme klonen kann.

No-cloning-Theorem Wir wollen beweisen, dass es keine Maschine gibt, die beliebige unbekannte reine Quantenzustände kopieren kann. Zunächst beschreiben wir eine andere Situation, in der Kopieren möglich ist. Wir zeigen, dass es für orthogonale Zustände $|0\rangle$ und $|1\rangle$ einen hierfür angepassten Kopierer gibt. Es ist das entsprechende CNOT-Gatter aus Abschn. 7.4.1. Wenn das Kontroll-Qubit die Form $|\psi^A\rangle = \alpha|0\rangle + \beta|1\rangle$ hat und $|0^B\rangle$ als Ziel-Qubit gewählt wird, dann besteht die Wirkung des CNOT-Gatters zur Basis $\{|0\rangle, |1\rangle\}$ in

$$|\psi^A, 0^B\rangle \rightarrow |\phi^{AB}\rangle = \alpha|0, 0\rangle + \beta|1, 1\rangle. \quad (8.48)$$

Die beiden orthogonale Zustände des Kontroll-Qubits $|0\rangle$ oder $|1\rangle$ (d. h. $\beta = 0$ oder $\alpha = 0$) werden daher durch das dieser Basis angepasste Gatter kopiert. Bis auf diese beiden Grenzfälle wird die Superposition $|\psi^A\rangle$ aber auf diese Weise nicht kopiert.

Wir wenden uns dem allgemeinen Fall zu. Ein Quantensystem S^A ist im Zustand $|\psi^A\rangle$. Dieser Zustand soll kopiert werden. Das heißt, ein zweites Quantensystem S^B , das sich zunächst im Zustand $|i^B\rangle$ befindet, soll in den Zustand $|\psi^B\rangle$ überführt werden. Dabei kann der

anfängliche Zustand $|i^C\rangle$ des Kopiersystems S^C in einer von $|\psi^B\rangle$ abhängigen Weise in einen neuen Zustand $|f(\psi)^C\rangle$ übergehen. Die Gesamtprozedur soll universell sein, d. h. für alle Zustände von S^A soll mit der gleichen unitären Transformation U eine Kopie erstellt werden.

$|\varphi^A\rangle$ ist ein zweiter zu kopierender Zustand. Dann lautet die Forderung:

$$|\psi^A\rangle|i^B\rangle|i^C\rangle \xrightarrow{U} |\psi^A\rangle|\psi^B\rangle|f(\psi)^C\rangle \quad (8.49)$$

$$|\varphi^A\rangle|i^B\rangle|i^C\rangle \xrightarrow{U} |\varphi^A\rangle|\varphi^B\rangle|f(\varphi)^C\rangle. \quad (8.50)$$

Die unitäre Transformation erhält das innere Produkt

$$\langle\psi^A|\varphi^A\rangle = \langle\psi^A|\varphi^A\rangle\langle\psi^B|\varphi^B\rangle\langle f(\psi)^C|f(\varphi)^C\rangle. \quad (8.51)$$

Wenn $|\psi^A\rangle$ und $|\varphi^A\rangle$ nicht orthogonal sind ($\langle\psi^A|\varphi^A\rangle \neq 0$) folgt

$$1 = \langle\psi^B|\varphi^B\rangle\langle f(\psi)^C|f(\varphi)^C\rangle. \quad (8.52)$$

Wir gehen zu Beträgen über. Da alle Zustände normiert sind mit $|\langle\psi^B|\varphi^B\rangle| \leq 1$ und $|\langle f(\psi)^C|f(\varphi)^C\rangle| \leq 1$, ist

$$|\langle\psi^B|\varphi^B\rangle| = 1 \quad \text{d. h. } |\psi^A\rangle = |\varphi^A\rangle \quad (8.53)$$

eine notwendige Bedingung für die Erfüllung von (8.52). Daher hat die Anlage keinen zweiten zu $|\psi^A\rangle$ nicht orthogonalen Zustand $|\varphi^A\rangle$ kopieren können. *Es gibt keinen universellen Kopierer für reine Quantenzustände (No-cloning-Theorem).*

Damit misslingt auch der oben beschriebene Versuch, einen Widerspruch zwischen Relativitätstheorie und Quantentheorie zu konstruieren. Die konfliktfreie Koexistenz beider Theorien ist bemerkenswert, da bei der Formulierung der Quantentheorie in der unrelativistischen Form, wie wir sie verwenden, die Forderungen der Relativitätstheorie nicht berücksichtigt wurden.

8.5 Zustandsmarkierung durch Verschränkung

8.5.1 Welcher-Weg-Markierung

2-Wege-Interferometer Wir erinnern zunächst an das in Abschn. 3.7 behandelte Mach-Zehnder-Interferometer (vgl. Abb. (3.8)), das von einem einzelnen Quantenobjekt durchlaufen wird. Der erste Strahlteiler dient dazu, eine symmetrische Superposition der den beiden Wegen zugeordneten Zustände $|0\rangle$ und $|1\rangle$ zu erreichen. Das Quantensystem in diesem Zustand trifft auf einen Strahlteiler mit Phasenschieber. Hierdurch werden die komplexen Amplituden des $|0\rangle$ - und des $|1\rangle$ -Vektors im 0-Ausgang hinter dem Strahlteiler superponiert. Ein Detektor im 0-Ausgang kann dann je nach Situation ein von der eingestellten Phasenverschiebung α abhängiges Interferenzbild registrieren. Genauer besagt das, dass seine Ansprechwahrscheinlichkeit $p(\alpha)$ eine Funktion von α sein kann. Gemäß Gl. (3.87) ergibt sie sich für einen beliebigen einfallenden Zustand ρ als

$$p_\rho(\alpha) = \text{tr}[\rho|\alpha\rangle\langle\alpha|] \quad (8.54)$$

mit

$$|\alpha\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\alpha}|1\rangle). \quad (8.55)$$

Für einen einlaufenden reinen Zustand $|\varphi\rangle$ sind Ansprechwahrscheinlichkeit und Streifenkontrast des Interferenzbildes in Abschn. 3.7.2 angegeben worden. Wir notieren diese Ergebnisse noch einmal.

Die Zuordnung eines einlaufenden Zustands $|\chi\rangle$ zu einem Weg ergibt sich indem man vor Phasenschieber und Strahlteiler einen Detektor entweder in Weg 0 oder Weg 1 einschiebt. Bei $|\chi\rangle = |0\rangle$ (bzw. $|\chi\rangle = |1\rangle$) spricht nur der Detektor auf Weg 0 (bzw. auf Weg 1) an. Das Quantenobjekt propagiert auf dem 0-Weg (bzw. dem 1-Weg). Bei der Interpretation des Gemischs

$$\rho = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2}\mathbb{1} \quad (8.56)$$

als Gemenge würde das Quantenobjekt entweder auf dem Weg 0 oder auf dem Weg 1 jeweils mit der relativen Häufigkeit $1/2$ einlaufen. In all diesen Fällen tritt keine α -Abhängigkeit und damit keine Interferenz auf:

$$p_{|0\rangle}(\alpha) = p_{|1\rangle}(\alpha) = p_{\rho}(\alpha) = \frac{1}{2} \quad (8.57)$$

Der Streifenkontrast ν ist

$$\nu_{|0\rangle} = \nu_{|1\rangle} = \nu_{\rho} = 0. \quad (8.58)$$

Einem reinen Zustand $|\chi\rangle$, der eine Superposition von $|0\rangle$ und $|1\rangle$ ist, kann man keinen Weg mehr zuordnen. Dementsprechend tritt Interferenz auf. Der allgemeine Qubit-Vektor $|\chi(\Theta, \varphi)\rangle$ und der dazu senkrechte Vektor $|\chi_{\perp}(\Theta, \varphi)\rangle$ haben die Form (vgl. Gl. (3.88))

$$|\chi(\Theta, \varphi)\rangle = \cos \frac{\Theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\Theta}{2} |1\rangle \quad (8.59)$$

$$\begin{aligned} |\chi_{\perp}(\Theta, \varphi)\rangle &= -\sin \frac{\Theta}{2} |0\rangle + e^{i\varphi} \cos \frac{\Theta}{2} |1\rangle \\ &= |\chi(\pi + \Theta, \varphi)\rangle. \end{aligned} \quad (8.60)$$

Sie bilden eine ONB. Mit $p(\alpha)$ von Gl. (3.87) folgt damit für die Ansprechwahrscheinlichkeit des Detektors als Funktion der Phasenverschiebung

$$p_{|\chi\rangle}(\alpha) = \frac{1}{2}[1 + \sin \Theta \cos(\alpha - \varphi)] \quad (8.61)$$

$$p_{|\chi_{\perp}\rangle}(\alpha) = \frac{1}{2}[1 - \sin \Theta \cos(\alpha - \varphi)]. \quad (8.62)$$

Für den Streifenkontrast ergibt sich

$$\nu_{|\chi\rangle} = \nu_{|\chi_{\perp}\rangle} = \sin \Theta. \quad (8.63)$$

Wenn nicht speziell der Zustand $|0\rangle$ oder $|1\rangle$ einläuft, entsteht mit variierendem α ein Interferenzbild.

Die Interferenzbilder zu $|\chi\rangle$ und $|\chi_\perp\rangle$ sind für $\varphi = -\frac{\pi}{2}$ in Abb. (8.3) dargestellt. Man sieht, dass sich bei Addition der Wahrscheinlichkeiten bzw. relativen Häufigkeiten die Abhängigkeiten der Kurven von der Phasenverschiebung α gerade aufheben. Die Interferenz verschwindet:

$$p_{|\chi\rangle} + p_{|\chi_\perp\rangle} = 1. \quad (8.64)$$

Diese Addition gibt die Situation wieder, die bei dem gleich gewichteten statistischen Gemisch

$$\rho = \frac{1}{2}(|\chi\rangle\langle\chi| + |\chi_\perp\rangle\langle\chi_\perp|) = \frac{1}{2}\mathbb{1} \quad (8.65)$$

aus den Basiszuständen $|\chi\rangle$ und $|\chi_\perp\rangle$ vorliegt. Wie in Gl. (8.57) erhalten wir $p_\rho = \frac{1}{2}$.

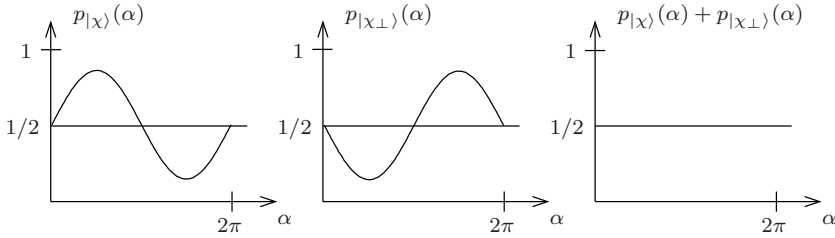


Abbildung 8.3: Die Interferenzbilder zum Zustand $|\chi\rangle$ und dem dazu senkrechten Zustand $|\chi_\perp\rangle$.

Verschränkung mit Markerzuständen Wir betrachten als Beispiel einzelne Atome im Atominterferometer. Die folgenden Überlegungen gelten aber allgemein. Das Atom im Qubit-Zustand mit maximalem Streifenkontrast

$$|\chi^A\rangle = c_0|0^A\rangle + c_1|1^A\rangle \quad (8.66)$$

soll im Interferometer mit einem weiteren Qubit-System S^M so in nicht-lokaler Weise wechselwirken, dass daraus der verschränkte Zustand

$$|\phi^{AM}\rangle = c_0|0^A, 0^M\rangle + c_1|1^A, 1^M\rangle \quad (8.67)$$

des Gesamtsystems S^{AM} entsteht. Die Atomzustände $\{|0^A\rangle, |1^A\rangle\}$ werden durch die zugehörigen *Markerzustände* $\{|0^M\rangle, |1^M\rangle\}$, die ebenfalls Eigenzustände zu σ_z sind, „markiert“. S^M heißt das *Markersystem*. Im vorliegenden Fall handelt es sich entsprechend der Bedeutung von $|0^M\rangle$ und $|1^M\rangle$ um *Welcher-Weg-Marker* (which-way marker). In anderen physikalischen Situationen können Marker auch innere Freiheitsgrade z. B. eines Atoms oder andere Quantenobjekte sein.

Die Wechselwirkung zwischen S^A und S^M , die die Markierung bewirkt, muss folgendes erreichen

$$(c_0|0^A\rangle + c_1|1^A\rangle) |i^M\rangle \rightarrow c_0|0^A, 0^M\rangle + c_1|1^A, 1^M\rangle. \quad (8.68)$$

Wenn man Fragen der physikalischen Realisierbarkeit außer Acht lässt, kann eine unitäre Transformation, die das leistet, leicht angegeben werden:

$$U^{AB} = |0^A\rangle\langle 0^A| \otimes |0^M\rangle\langle 0^M| + |1^A\rangle\langle 1^A| \otimes |1^M\rangle\langle 1^M|. \quad (8.69)$$

Als Ausgangszustand des Marker-Systems wählen wir $|i^M\rangle = \frac{1}{\sqrt{2}}(|0^M\rangle + |1^M\rangle)$. U^{AB} ist offenbar eine nicht-lokale Transformation. Im Spezialfall, dass das Atom auf dem Weg 0 kommt, wird der Marker in die „Position“ $|0^M\rangle$ gebracht und entsprechend in die Position $|1^M\rangle$ bei Weg 1. Nur wenn das Atom in einer Superposition einläuft, entsteht ein verschränkter Zustand.

Verlust der Interferenzfähigkeit Was besagt die Welcher-Weg-Markierung von Gl. (8.67) physikalisch? Wir messen am Marker-Qubit in der Rechenbasis $\{|0^M\rangle, |1^M\rangle\}$ oder anders gesagt, wir messen die *Markerobservable*. Beim Messergebnis $+1$, das zu $|0^M\rangle$ gehört, läuft das Atom auf dem 0-Weg weiter, bei -1 auf dem 1-Weg. *Messung der Markerobservablen bricht also die Interferenz auf und legt für das Atom einen Weg fest.*

Bemerkenswerter Weise ist es für den Verlust der Interferenzfähigkeit gar nicht nötig, dass am Markersystem gemessen wird. Nachdem durch Markieren der verschränkte Zustand $|\phi^{AM}\rangle$ von Gl. (8.67) mit reduziertem Dichteoperator

$$\rho^A = \text{tr}_M[\rho^{AM}] = |c_0|^2 |0^A\rangle\langle 0^A| + |c_1|^2 |1^A\rangle\langle 1^A| \quad (8.70)$$

entstanden ist, stimmt der reduzierte Dichteoperator des Atomsystems ρ^A hinsichtlich aller Wahrscheinlichkeitsaussagen mit Gemenge der Zustände $|0^A\rangle$ und $|1^A\rangle$ überein. Die Interferenz verschwindet. *Wenn man interferierende Zustände markiert, geht die Interferenzfähigkeit selbst dann verloren, wenn an den Markern gar nicht gemessen wird.*

Die Information, die vor der Markierung im reinen Zustand $|\chi^A\rangle$ des Atoms steckte und die das Interferenzbild bestimmt hat, ist nicht mehr im Zustand des Atoms gespeichert und kann durch Messungen am Atom nicht abgerufen werden. Tatsächlich ist sie bei der unitären Verschränkungsdynamik aber nicht verloren gegangen. Sie wurde als wechselseitige Information in den Korrelationen mit dem Markersystem deponiert. Wir wollen jetzt sehen, wie man sie dort wieder abrufen kann indem man Korrelationen misst.

8.5.2 Quantenradieren

Wir betrachten der Einfachheit halber den Spezialfall $c_1 = c_2 = \frac{1}{\sqrt{2}}$.

$$|\phi^{AM}\rangle = \frac{1}{\sqrt{2}} (|0^A, 0^M\rangle + |1^A, 1^M\rangle) \quad (8.71)$$

$$\rho^A = \frac{1}{2} \mathbb{1}^A. \quad (8.72)$$

Da der Interferenz zerstörende Einfluss der Markierung wieder beseitigt werden soll, spricht man vom *Quantenradieren* (quantum erasure). Die Überlegungen im vorigen Kapitel zu den Basiszuständen $|\chi(\Theta, \varphi)\rangle$ und $|\chi_\perp(\Theta, \varphi)\rangle$ mit $\Theta \neq 0, \pi$ geben einen Hinweis darauf, wie man aus dem vorliegenden Gemisch ρ^A Informationen gewinnen kann. ρ^A ist in unserem Fall

kein statistisches Gemisch (Gemege), sondern ein reduzierter Dichteoperator eines Teilsystems. Er ist aber im Hinblick auf alle denkbaren Aussagen über Messungen nicht von einem Gemenge zu unterscheiden, das durch Mischen der Zustände $|\chi^A\rangle$ und $|\chi_\perp^A\rangle$ entsteht. Wenn es nach der Markierung gelänge, erstens die Atome in die Zustände $|\chi^A\rangle$ oder $|\chi_\perp^A\rangle$ zu überführen und zweitens Atome im Zustand $|\chi^A\rangle$ von denen im Zustand $|\chi_\perp^A\rangle$ zu trennen, dann würden die zugehörigen atomaren Ensemble auf die Interferenzbilder von Abb. 8.3 führen. Sie stimmen mit den ursprünglichen Interferenzbildern zum Zustand $|\chi^A\rangle$ bzw. $|\chi_\perp^A\rangle$ bis auf eine Phasenverschiebung und möglicherweise geringeren Phasenkontrast überein. Da das Gesamtsystem ρ^{AM} in einem reinen Zustand $|\phi^{AM}\rangle$ vorliegt, können wir tatsächlich beide Forderungen durch geeignete Messung am Markersystem S^M erfüllen. Wir werden ein solches oder ein ähnliches Verfahren noch häufiger verwenden. Es besteht allgemein darin, dass ein System mit einem Hilfssystem verschränkt wird und dann am Hilfssystem gemessen wird, um den Zustand des Ausgangssystems in gewünschter Weise zu manipulieren.

Um im vorliegenden Fall Quantenradieren zu erreichen, gehen wir folgendermaßen vor: Der verschränkte Zustand $|\psi^{AM}\rangle$ von Gl. (8.67) lässt sich mit Hilfe „gedrehter“ Markerzustände (vergl. Bloch-Kugel)

$$|\Lambda^M(\Theta, \varphi)\rangle = \frac{1}{\sqrt{2}}(\cos \frac{\Theta}{2}|0^M\rangle + e^{-i\varphi} \sin \frac{\Theta}{2}|1^M\rangle) \quad (8.73)$$

$$|\Lambda_\perp^M(\Theta, \varphi)\rangle = \frac{1}{\sqrt{2}}(-\sin \frac{\Theta}{2}|0^M\rangle + e^{-i\varphi} \cos \frac{\Theta}{2}|1^M\rangle) \quad (8.74)$$

in der zu Gl. (8.71) völlig analogen Form

$$|\phi^{AM}\rangle = \frac{1}{\sqrt{2}}(|\chi^A, \Lambda^M\rangle + |\chi_\perp^A, \Lambda_\perp^M\rangle) \quad (8.75)$$

schreiben. Dadurch sind bei unverändertem Gesamtzustand $|\phi^{AM}\rangle$ die interferenzfähigen Zustände $|\chi^A\rangle$ und $|\chi_\perp^A\rangle$ statt der Zustände $|0^A\rangle$ und $|1^A\rangle$ mit den neuen Markerzuständen verschränkt. Eine Messung am Markersystem in der Basis $\{|\Lambda^M\rangle, |\Lambda_\perp^M\rangle\}$, die auf die Messwerte $1+$ und -1 führen soll, überführt den Atomzustand in $|\chi^A\rangle$, wenn der Messwert $+1$ eingetreten ist, bzw. in $|\chi_\perp^A\rangle$ beim Messwert -1 . Bei einer nicht-selektiven Messung führt das resultierende statistische Gemisch ρ^A von Gl. (8.65) aber noch immer nicht auf ein Interferenzbild.

Der entscheidende zweite Schritt besteht daher in einer Selektion, also in einer Entmischung des Gemisches. Betrachten wir nur die Beiträge derjenigen Atome zum Interferenzbild, die in der Messung mit dem Messergebnis $+$ präpariert wurden, dann erhalten wir das Interferenzbild von Abb. 8.3 zu $p_{|\chi\rangle}(\alpha)$ von Gl. (8.61). Entsprechend finden wir nach Selektion zum Messergebnis -1 die Interferenzkurve $p_{|\chi_\perp\rangle}(\alpha)$ von Gl. (8.62). *Durch selektive Messung in einer „gedrehten“ Markerbasis wird der die Interferenz zerstörende Einfluss aufgehoben. Die Interferenzkurve wird reproduziert.* Der Streifenkontrast $\nu = 1$ wird mit $\Theta = \frac{\pi}{2}$ erzielt. Für $\varphi = 0$ sind dann die Markerzustände die Eigenzustände zu σ_x .

8.5.3 Tatsächlich „delayed choice“?

Gedankenexperimente Die Experimente, die zur „Welcher-Weg“-Markierung vorgeschlagen oder durchgeführt wurden, sind quantenoptische bzw. atomoptische Experimente. Wir müssen uns hier mit Literaturhinweisen begnügen (vergl. Abschn. 8.6).

Ohne Anspruch auf einfache Realisierbarkeit können wir uns in Abwandlung vom oben beschriebenen Experiment in einem Gedankenexperiment folgenden Versuchsaufbau vorstellen: Ein Atom durchläuft ein Atominterferometer. Im Zustand $|0\rangle$ emittiert es ein Photon mit vertikaler Polarisation $|V^M\rangle$, im Zustand $|1\rangle$ mit horizontaler Polarisation $|H^M\rangle$. Das Photon dient als Markersystem M . Seine beiden Polarisationszustände sind die Markierzustände. Die von den einzelnen Atomen emittierten Photonen werden getrennt gespeichert. Es wird dafür gesorgt, dass z. B. durch Durchnummerieren eine eindeutige Zuordnung zwischen den einzelnen Photonen und Ereignissen am Atomdetektor besteht. Es wird dabei zunächst nicht an den Photonen gemessen, sondern erst die Messung an vielen Atomen abgewartet. Ist in dieser Situation, in der die Atome nicht mehr zur Verfügung stehen, noch Quantenradieren möglich? Wir kommen auf diese Frage noch zurück.

Die in Abschn. 3.7 beschriebene Situation des Strahlteilers mit Phasenschieber hat große Ähnlichkeit mit der physikalischen Situation hinter einem Doppelspalt, wie wir sie in Abschn. 2.1.1 diskutiert haben. Der Zustand $|0^A\rangle$ bzw. $|1^A\rangle$ steht in Analogie zu dem Zustand, der vorliegt, wenn nur der erste (bzw. nur der zweite) Spalt geöffnet ist. Diese Zustände superponieren. Das Resultat wird als unterschiedlich starke Schwärzung an Orten des Schirms beobachtet. Durch die Wegunterschiede interferieren die Zustände $|0\rangle$ und $|1\rangle$ dabei mit einer Phasenverschiebung α . Eine mögliche Markierung könnte dann im Prinzip darin bestehen, dass Atome hinter Spalt 1 dazu gebracht werden, vertikal polarisierte Photonen auszusenden und hinter Spalt 2 entsprechend horizontal polarisierte Photonen. Auch dieses Gedankenexperiment ist zu einfach, um direkt experimentell realisierbar zu sein. Wir erwähnen es, da in der „Welcher-Weg“-Diskussion gerne der Doppelspalt angeführt wird. Wiederum könnte man im Prinzip zunächst alle Atome registrieren und erst dann die Polarisation der zugehörigen Photonen bestimmen.

Interpretation Weil in Diskussionen zur „Welcher-Weg“-Markierung häufig Missverständnisse auftauchen, wollen wir uns kritisch fragen, wie die oben beschriebene Rechnung zu interpretieren ist. Die Markierung besteht darin, dass das Gesamtsystem S^{AM} aus einem Produktzustand in den verschränkten Zustand (8.67) überführt wird. Der Zustand $|\chi^A\rangle$ von Gl. (8.66), der ursprünglich vorlag, hat Interferenz gezeigt. Die darin enthaltene Information ist nach der Verschränkung in den Korrelationen gespeichert. Sie kann durch Messungen allein an S^A oder allein an S^M nicht abgerufen werden. Wir müssen an beiden Untersystemen messen und die Messergebnisse in Paaren zusammenfassen: am ersten Atom-Photon-Paar erhaltene Messergebnisse, am zweiten Atom-Photon-Paar ... usw.

Wir wollen in diesem Zusammenhang auf einen für die Interpretation wichtigen Punkt hinweisen. Wir hatten schon in Abschn. 7.3.4 gesehen, dass es für die Korrelationen zwischen den Messergebnissen nicht darauf ankommt, in welcher zeitlichen Reihenfolge an den Teilsystemen gemessen wird. Das ist auch hier so. Man muss also nicht, wie oben dargestellt, zunächst am Markersystem messen. Man kann mit gleichem Ergebnis auch erst Detektormessungen an einer großen Zahl nacheinander eintreffenden Atome machen und die Ergebnisse durchnummerieren. Die zugehörigen Photonen werden in diesem Gedankenexperiment ebenfalls jeweils durchnummeriert und ohne Messung getrennt abgespeichert. Erst in einer späteren Phase des Experiments werden dann die Photonen mit der „gedrehten“ Markerobservablen einzeln gemessen und die Ergebnisse durchnummeriert. Korreliert man schließlich

gemäß ihrer Nummer die Messergebnisse an Atomen und Photonen, dann ergibt sich nach Selektion das Interferenzbild. Die Ergebnisse der Messungen an den Atomen alleine und die der Messungen an den Photonen alleine enthalten keine Information.

Nachdem die Atome das Interferometer durchlaufen haben und bereits detektiert wurden, kann man somit durch Wahl der an den Photonen gemessenen Observablen bestimmen, ob ein Interferenzbild entsteht ($|\Lambda^M\rangle, |\Lambda_\perp^M\rangle$) oder nicht ($|0^M\rangle, |1^M\rangle$). Dies könnte man so verstehen, dass man zwischen den Alternativen (i) Atome kommen immer nur auf einem der Wege (Teilchenverhalten und daher keine Interferenz) und (ii) Atome kommen im Sinne einer Superposition „auf beiden Wegen“ (Wellenverhalten und daher Interferenz) wählen kann, wenn die Atome schon lange das Interferometer verlassen haben und an ihnen gemessen wurde. Diese *verzögerte Wahl* (delayed choice) scheint eine Beeinflussung des Geschehens in der Vergangenheit zu sein. Was ist falsch bei dieser Interpretation?

Falsch ist die Annahme, dass vom Ereignis „auf einem Weg“ überhaupt gesprochen werden kann. Das System S^A befindet sich vor der Messung im vollständig gemischten und daher völlig strukturlosen Zustand. Man kann Photonen auf den beiden Wegen 0 und 1 registrieren. Es ergibt sich bei Messung an S^A kein Interferenzbild ($p(\alpha) = \frac{1}{2}$). Das bleibt so bei anschließender Messung in der nicht gedrehten ONB $\{|0^M\rangle, |1^M\rangle\}$. Erst wenn man an den Photonen in der gedrehten ONB $\{|\Lambda^M\rangle, |\Lambda_\perp^M\rangle\}$ misst, z. B. die Messwerte herausucht, die zum Messergebnis +1 gehören und die relativen Häufigkeiten als Funktionen von α in eine Abbildung einträgt, entsteht für die Wahrscheinlichkeit der Kurvenverlauf $p_{|\chi\rangle}(\alpha)$ von Abb. 8.3, der Interferenz widerspiegelt. Die Alternativen (i) und (ii) realisieren sich daher erst in der Form (i) „keine Interferenz“ und (ii) „Interferenz“ mit der Wahl der entsprechenden Messung an den Photonen gefolgt von einer Selektion und nicht schon mit der Messung an den Atomen. Vorher hat nichts vorgelegen, was mit (i) oder (ii) verbunden werden könnte. *Es gibt also kein „delayed choice“-Paradoxon.*

8.6 Ergänzende Themen und weiterführende Literatur

- Kriterien für Separabilität für Systeme mit zwei und mehr Untersystemen, Verschränkungsmaß auch für Gemische: [Wer 89], [Key 02], [Bru 01], [DHR 02], [HHH 01], [Cir 02], [LBC 00], [Ter 01].
- Erzeugung von Verschränkung: [Aul 00], [BEZ 00], [NC 00], [BZ 02], [DM 02], [Hei 02], [SS 04].
- Zum Konzept der klassisch korrelierten Quantenzustände: [Wer 89].
- Experimente zu „delayed choice“: [Aul 00, Kap. 26], [DR 00].
- Der Anstoß zur „delayed choice“-Diskussion: [Weh 78].
- Welcher-Weg-Experimente: [DNR 98], [Rem 02], [Eng 99], [ESW 99], [DR 00].
- Quantenradierer: [Eng 99], [ESW 99].
- Verschränkung von gemischten Zuständen: [Cir 02], [HHH 01].

8.7 Übungsaufgaben

ÜA 8.1 [zu 8.1.1] Beweisen Sie die in Abschn. 8.1.1 im Anschluss an Gl. (8.1) aufgestellte Behauptung über die Charakterisierung korrelierter Zustände.

ÜA 8.2 [zu 8.1.2] Beweisen Sie, dass die Separabilitätsbedingung (8.2) gleichbedeutend ist mit der Forderung

$$\rho^{AB} = \sum_l q_l |\phi_l^A\rangle\langle\phi_l^A| \otimes |\chi_l^B\rangle\langle\chi_l^B| \quad (8.76)$$

mit $0 \leq q_l \leq 1$ und $\sum_l q_l = 1$. Der Vergleich mit dem allgemeinen Operator Z^{AB} von Gl. (7.19) zeigt, dass die Forderung (8.76) tatsächlich eine Einschränkung bedeutet.

ÜA 8.3 [zu 8.3] Bestätigen Sie die Gl. (8.45).

ÜA 8.4 [zu 8.5] Wie ändern sich die Überlegungen zum Quantenradieren, wenn man vom Zustand (8.67) statt vom Zustand (8.71) ausgeht.

ÜA 8.5 [zu 8.2] Zeigen Sie, dass es für den Zustand

$$|\phi^{ABC}\rangle = \frac{1}{\sqrt{2}}(|0^A\rangle(|0^B, 0^C\rangle + |1^B, 1^C\rangle)) \quad (8.77)$$

keine Schmidt-Zerlegung

$$|\phi^{ABC}\rangle = \sum_n \sqrt{p_n} |u_n^A\rangle |v_n^B\rangle |w_n^C\rangle \quad (8.78)$$

mit orthonormalen Schmidt-Basen $\{|u_n^A\rangle\}$, $\{|v_n^B\rangle\}$, $\{|w_n^C\rangle\}$ gibt.

This Page Intentionally Left Blank

9 Korrelationen und nicht-lokale Messungen

Quanteninformation kann in Korrelationen zwischen Teilsystemen stecken. Das soll im Einzelnen präzisiert werden. Bei zusammengesetzten Systemen sind über die Messungen an Teilsystemen hinaus auch nicht-lokale Messungen möglich, mit deren Hilfe u.a. nicht-lokal gespeicherte Information abgefragt werden kann.

9.1 Entropien und Korreliertheit zusammengesetzter Quantensysteme

9.1.1 Wechselseitige Information als Maß für Korreliertheit

Additivität Mit Hilfe der Definition der *Gesamtentropie* (joint entropy) für zusammengesetzte Systeme

$$S(AB) := S(A, B) := S(\rho^{AB}) := -\text{tr}_{AB}[\rho^{AB} \log \rho^{AB}] \quad (9.1)$$

prüft man sofort nach, dass sich für einen Produktzustand die Entropien der Teilsysteme addieren

$$S(\rho^A \otimes \rho^B) = S(\rho^A) + S(\rho^B). \quad (9.2)$$

Subadditivität Wenn ρ^{AB} kein Produktzustand ist, können wir statt Gl. (9.2) nur eine Abschätzung ableiten. Wir gehen dazu von der Kleinschen Ungleichung (6.24) aus, die wir jetzt im Produktraum $\mathcal{H}^A \otimes \mathcal{H}^B$ anwenden.

Wir ersetzen in Gl. (6.17) ρ durch ρ^{AB} und σ durch $\sigma^{AB} = \rho^A \otimes \rho^B$ mit den reduzierten Dichteoperatoren ρ^A und ρ^B von ρ^{AB} , die wir nach den Basen von \mathcal{H}^A und \mathcal{H}^B zerlegen

$$\begin{aligned} \rho^A &= \sum_n a_n |n^A\rangle \langle n^A|, \\ \rho^B &= \sum_j b_j |j^B\rangle \langle j^B|. \end{aligned} \quad (9.3)$$

Dann gilt

$$\begin{aligned} \log \sigma^{AB} = \log \rho^A \otimes \rho^B &= \sum_{n,j} \log(a_n b_j) |n^A, j^B\rangle \langle n^A, j^B| \\ &= (\log \rho^A) \mathbb{1}^B + \mathbb{1}^A (\log \rho^B). \end{aligned} \quad (9.4)$$

Damit folgt aus der Kleinschen Ungleichung (6.24)

$$\begin{aligned} S(\rho^{AB}) &\leq -\text{tr}_{AB}[\rho^{AB} \log \sigma^{AB}] \\ &= -\text{tr}_{AB}[\rho^{AB} (\log \rho^A) \mathbb{1}^B] - \text{tr}_{AB}[\rho^{AB} \mathbb{1}^A \log(\rho^B)] \\ &= -\text{tr}_A[\rho^A \log \rho^A] - \text{tr}_B[\rho^B \log \rho^B] = S(\rho^A) + S(\rho^B). \end{aligned} \quad (9.5)$$

Wir schreiben das Resultat in der Form

$$S(AB) \leq S(A) + S(B). \quad (9.6)$$

Diese Eigenschaft wird als *Subadditivität* (subadditivity) der Entropie zusammengesetzter Quantensysteme bezeichnet. Das Gleichheitszeichen gilt genau dann, wenn die Teilsysteme S^A und S^B unabhängig voneinander sind: $\rho^{AB} = \rho^A \otimes \rho^B$. Die analoge Gleichung für klassische Systeme ist Gl. (5.43). *Wenn die Teilsysteme nicht unabhängig voneinander sind, der Gesamtzustand ρ^{AB} also nicht separabel ist, dann enthält das Gesamtsystem mehr Information als insgesamt aus den Teilsystemen ausgelesen werden kann.* Wir werden das noch an einem Beispiel verdeutlichen.

Wechselseitige Information der Teilsysteme Im klassischen wie im quantentheoretischen Fall steckt die Zusatzinformation in den Korrelationen zwischen den Systemen. Um das für zusammengesetzte Quantensysteme quantitativ zu fassen, führen wir *als Maß für die Korreliertheit der Teilsysteme die wechselseitige Information* (mutual information) $S(A : B)$ der Teilsysteme in Analogie zur Gl. (5.31) ein:

$$S(A : B) := S(A) + S(B) - S(AB) \geq 0. \quad (9.7)$$

$S(A : B)$ gibt für einen Zustand ρ^{AB} an, wie viel die durch die Entropie ausgedrückte Unbestimmtheit des Gesamtsystems S^{AB} kleiner ist als die der Teilsysteme S^A und S^B zusammen, wenn diese Teilsysteme nicht verschränkt wären (vgl. Gl. (9.5)). Oder anders formuliert: $S(A : B)$ ist ein Maß dafür, wie viel mehr Information im Gesamtsystem als in den Teilsystemen steckt. $S(A : B)$ kann zugleich den Abstand des Zustands ρ^{AB} vom unverschränkten Zustand $\rho^A \otimes \rho^B$ charakterisieren.

9.1.2 Dreiecksungleichung

Das System S^{AB} möge sich in einem Zustand ρ^{AB} befinden. Wir hatten in Abschn. 8.2.2 gesehen, dass dieser Zustand immer purifiziert werden kann. Das besagt, dass man immer ein System S^C zu S^{AB} hinzufügen kann und dann im erweiterten Gesamtsystem S^{ABC} einen reinen Zustand finden kann, so dass der reduzierte Dichteoperator des Teilsystems S^{AB} gerade ρ^{AB} ist.

Wir wenden die Ungleichung für Subadditivität an:

$$S(C) + S(A) \geq S(AC). \quad (9.8)$$

Da das System S^{ABC} in einem reinen Zustand ist, stimmen die reduzierten Dichteoperatoren bei Zerlegung in zwei Teilsysteme überein. Das haben wir im Zusammenhang mit der Schmidt-Zerlegung gezeigt.

$$S(AC) = S(B), \quad S(C) = S(AB). \quad (9.9)$$

Einsetzen in Gl. (9.8) führt auf

$$S(AB) \geq S(B) - S(A). \quad (9.10)$$

Die Systeme S^A und S^B gehen symmetrisch in die Überlegung ein. Es gilt also auch

$$S(AB) \geq S(A) - S(B) \quad (9.11)$$

und damit

$$S(AB) \geq |S(A) - S(B)|. \quad (9.12)$$

Dies ist die *Dreiecksungleichung* (triangle inequality), die manchmal auch *Araki-Lieb-Ungleichung* genannt wird.

Wir haben in Gl. (5.39) gezeigt, dass für die Shannon-Entropie der klassischen Systeme immer

$$H(A, B) \geq \left\{ \begin{array}{l} H(A) \\ H(B) \end{array} \right\} \quad (9.13)$$

erfüllt ist. Die Unbestimmtheit des Gesamtsystems übertrifft die jedes Einzelsystems. Dass kann für Quantensysteme nicht gelten. Die Bell-Zustände, für die wir $S(AB) = 0$ und $S(A) = S(B) = 1$ gezeigt hatten, sind ein einfaches Gegenbeispiel.

9.1.3 Verschränkte versus klassische korrelierte Quantensysteme

Wir wollen am Beispiel eines 2-Teile-Systems S^{AB} in drei verschiedenen Zuständen die Entropie der Teilsysteme S^A und S^B , die in allen Fällen gleich eins sein soll, mit der Entropie des Gesamtsystems vergleichen. Die Teilsysteme sollen der Einfachheit halber Qubits sein. Unser Ziel ist es dabei, Korrelation und Verschränkung mit der Entropie und dabei insbesondere über die Gl. (9.7) mit der wechselseitigen Information $S(A : B)$ in Zusammenhang zu bringen. Die Verhältnisse sind graphisch in Abb. 9.1 dargestellt.

Beispiel I: Unabhängige Teilsysteme Im ersten Zustand sind die Teilsysteme völlig unabhängig voneinander, d. h. ρ^{AB} ist ein Produktzustand

$$\rho^{AB} = \frac{1}{4} \mathbb{1}^{AB} = \left(\frac{1}{2} \mathbb{1}^A \right) \otimes \left(\frac{1}{2} \mathbb{1}^B \right) = \rho^A \otimes \rho^B. \quad (9.14)$$

Es existieren keine Korrelationen zwischen den Teilsystemen. Die Quantenentropien ergeben sich unmittelbar als

$$S(AB) = \log 4 = 2, \quad (9.15)$$

$$S(A) = S(B) = \log 2 = 1 \quad (9.16)$$

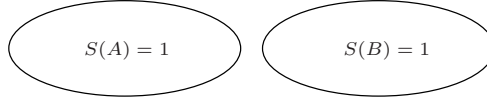
$$S(A : B) = 0. \quad (9.17)$$

Für einen späteren Vergleich notieren wir noch ρ^{AB} in der Rechenbasis von $\mathcal{H}^A \otimes \mathcal{H}^B$

$$\begin{aligned} \rho^{AB} = & \frac{1}{4} (|0^A, 0^B\rangle\langle 0^A, 0^B| + |0^A, 1^B\rangle\langle 0^A, 1^B| \\ & + |1^A, 0^B\rangle\langle 1^A, 0^B| + |1^A, 1^B\rangle\langle 1^A, 1^B|). \end{aligned} \quad (9.18)$$

Beispiel I

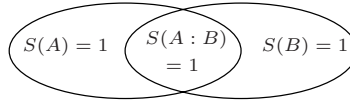
$$S(AB) = 2$$



völlig unabhängig

Beispiel II

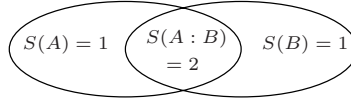
$$S(AB) = 1$$



klassisch korreliert

Beispiel III

$$S(AB) = 0$$



verschränkt

Abbildung 9.1: Wechselseitige Information $S(A : B)$ bei gleicher Entropie der Teilsysteme.

Beispiel II: Klassische korrelierte Teilsysteme Wir wollen Korrelationen etablieren, ohne dass dabei Verschränkung entsteht. Das können wir z. B. mit dem *separablen Gemisch*

$$\rho^{AB} = \frac{1}{2}(|0^A\rangle\langle 0^A| \otimes |0^B\rangle\langle 0^B| + |1^A\rangle\langle 1^A| \otimes |1^B\rangle\langle 1^B|) \quad (9.19)$$

$$= \frac{1}{2}(|0^A, 0^B\rangle\langle 0^A, 0^B| + |1^A, 1^B\rangle\langle 1^A, 1^B|) \quad (9.20)$$

aus reinen Produktzuständen erreichen. ρ^{AB} ist verglichen mit Gl. (9.18) eingeschränkt. In der Rechenbasis von $\mathcal{H}^A \otimes \mathcal{H}^B$ hat ρ^{AB} die Matrixdarstellung

$$\rho^{AB} = \text{diag}\left(\frac{1}{2}, 0, 0, \frac{1}{2}\right). \quad (9.21)$$

Es treten nur Diagonalterme auf. Damit ergibt sich die Entropie als

$$S(AB) = -2 \left[\frac{1}{2} \log \frac{1}{2} \right] = 1. \quad (9.22)$$

Die reduzierten Dichteoperatoren der Teilsysteme stimmen mit denen in den anderen Beispielen überein

$$\rho^A = \frac{1}{2} \mathbb{1}^A, \quad \rho^B = \frac{1}{2} \mathbb{1}^B. \quad (9.23)$$

Daraus folgt wieder

$$S(A) = S(B) = 1 \quad (9.24)$$

und in diesem Fall eine nicht verschwindende wechselseitige Information

$$S(A : B) = 1. \quad (9.25)$$

An Gl. (9.20) ist unmittelbar ablesbar, dass die Ergebnisse von Messungen in der Rechenbasis an den beiden Teilsystemen korreliert sind: Ergibt die Messung an S^A den zu $|0\rangle$ gehörigen Messwert, dann ergibt auch die Messung an S^B diesen Messwert. Entsprechendes gilt für $|1\rangle$. Die Teilsysteme heißen *klassisch korreliert*, weil sie durch LOCC entstanden sind und weil die Messung an einem Teilsystem den wohlbestimmten (korrelierten) reinen Zustand des anderen Teilsystems nicht abändert. Damit wird noch einmal mit anderen Worten ausgedrückt, dass der Zustand von S^{AB} ein separables Gemisch ist.

Beispiel III: Verschränkte Teilsysteme Hier nehmen wir als Beispiel den Bell-Zustand

$$|\Phi_+^{AB}\rangle = \frac{1}{\sqrt{2}}(|0^A, 0^B\rangle + |1^A, 1^B\rangle). \quad (9.26)$$

Da er ein reiner Zustand ist, haben wir

$$S(AB) = 0. \quad (9.27)$$

Wie in den beiden Beispielen vorher finden wir

$$\rho^A = \frac{1}{2} \mathbb{1}^A, \quad \rho^B = \frac{1}{2} \mathbb{1}^B \quad (9.28)$$

und damit

$$S(A) = S(B) = 1. \quad (9.29)$$

Für einen Bell-Zustand nimmt man die wechselseitige Information den größten möglichen Wert an

$$S(A : B) = 2. \quad (9.30)$$

Vergleich der drei Beispiele Dass bei Verschränkung die Ergebnisse von Messungen an den Teilsystemen korreliert sind, haben wir schon diskutiert. Im Zusammenhang mit der Bellschen Ungleichung werden wir in Kap. 10 explizit zeigen, dass sich die Korrelationen in Beispiel II und III quantitativ unterscheiden. Hier wollen wir den Unterschied mit Hilfe der Entropie beschreiben.

In allen drei Fällen liegt wegen $S(A) = S(B)$ die gleiche Unbestimmtheit der Zustände der Teilsysteme vor. Die Unbestimmtheit $S(AB)$ des Zustands des Gesamtsystems ist demgegenüber in jedem Fall verschieden (vergl. Abb. 9.1). Die *wechselseitige Information* (mutual information) $S(A : B)$ gibt wegen

$$S(AB) = S(A) + S(B) - S(A : B) \quad (9.31)$$

an, um wie viel die tatsächliche Entropie des Gesamtsystems kleiner ist als es die Gesamtentropie wäre, wenn die Teilsysteme mit Dichteoperatoren ρ^A und ρ^B völlig unabhängig wären. Geringere Entropie bedeutet geringere Unbestimmtheit des Zustands. In allen drei Beispielen sind die Zustände der Teilsysteme maximal unbestimmt. Dennoch ist im Beispiel III der verschränkte Gesamtzustand maximal bestimmt. Die Information, die hierfür noch gefehlt hat, steckt vollständig in den Korrelationen und wird durch $S(A : B)$ veranschaulicht. Im Beispiel II reichen die Korrelationen nicht zur völligen Festlegung des Zustandes von S^{AB} . Dementsprechend befindet sich das Gesamtsystem in einem Gemisch. $S(A : B)$ ist in diesem Fall kleiner. *Wie wir gesehen haben, bezieht sich die wechselseitige Quantenentropie $S(A : B)$ nicht auf Verschränkung alleine, sondern gibt auch die klassischen Korrelationen mit wieder.*

9.2 Nicht-lokale Messungen

9.2.1 Bell-Zustände

Die vier Bell-Zustände

$$|\Phi_{\pm}^{AB}\rangle = \frac{1}{\sqrt{2}}(|0^A, 0^B\rangle \pm |1^A, 1^B\rangle) \quad (9.32)$$

$$|\Psi_{\pm}^{AB}\rangle = \frac{1}{\sqrt{2}}(|0^A, 1^B\rangle \pm |1^A, 0^B\rangle) \quad (9.33)$$

bilden eine orthonormale Basis (*Bell-Basis*) des Produktraums $\mathcal{H}_2^A \otimes \mathcal{H}_2^B$. Sie sind maximal verschränkt. Die reduzierten Dichteoperatoren sind maximal gemischt. $\rho^A = \rho^B = \frac{1}{2}\mathbb{1}$. *Man kann durch Eingriff bei nur einem Teilsystem (also lokal ohne klassische Kommunikation) in unitärer Weise mit Hilfe der σ -Operatoren einen Bell-Zustand in jeden anderen überführen.* Wir geben ein Beispiel:

$$\text{Bit-Flip } \sigma_1^A : |\Psi_+^{AB}\rangle \rightarrow \frac{1}{\sqrt{2}}(|1^A, 1^B\rangle + |0^A, 0^B\rangle) = |\Phi_+^{AB}\rangle \quad (9.34)$$

$$\text{Phasen-Flip } \sigma_2^A : |\Psi_+^{AB}\rangle \rightarrow \frac{-i}{\sqrt{2}}(|0^A, 0^B\rangle - |1^A, 1^B\rangle) = -i|\Phi_-^{AB}\rangle. \quad (9.35)$$

$$\sigma_3^A : |\Psi_+^{AB}\rangle \rightarrow \frac{1}{\sqrt{2}}(|0^A, 1^B\rangle - |1^A, 0^B\rangle) = |\Psi_-^{AB}\rangle \quad (9.36)$$

Häufig treten in Rechnungen Produkte von Pauli-Operatoren auf, deren Matrixelemente in der Bell-Basis auszuwerten sind (z. B. $\langle \Phi_+^{AB} | \sigma_1^A \sigma_3^B | \Phi_+^{AB} \rangle$). In diesen Fällen ist es günstig, die Wirkung der Pauli-Operatoren in \mathcal{H}_2^B auf die in \mathcal{H}_2^A zurückzuführen, dann kann man alle in Abschn. 3.1 für Pauli-Operatoren abgeleitete Relationen (z. B. in Gl. (3.11)) direkt übernehmen. Wir geben ein Beispiel, auf das wir später zurückkommen werden:

$$\sigma_1^A : |\Phi_+^{AB}\rangle \longrightarrow |\Psi_+^{AB}\rangle, \quad \sigma_1^B : |\Phi_+^{AB}\rangle \longrightarrow |\Psi_+^{AB}\rangle \quad (9.37)$$

$$\sigma_2^A : |\Phi_+^{AB}\rangle \longrightarrow -i|\Psi_-^{AB}\rangle, \quad \sigma_2^B : |\Phi_+^{AB}\rangle \longrightarrow i|\Psi_-^{AB}\rangle \quad (9.38)$$

$$\sigma_3^A : |\Phi_+^{AB}\rangle \longrightarrow |\Phi_-^{AB}\rangle, \quad \sigma_3^B : |\Phi_+^{AB}\rangle \longrightarrow |\Phi_-^{AB}\rangle \quad (9.39)$$

Die Wirkung von σ_3^B auf $|\Phi_+^{AB}\rangle$ kann durch die Wirkung von σ_3^A ersetzt werden usw.. Es gibt entsprechende Relationen für alle Vektoren der Bell-Basis. Man bestätigt auf diese Weise z. B., dass

$$\begin{aligned} \langle \Phi_+^{AB} | \sigma_1^A \sigma_3^B | \Phi_+^{AB} \rangle &= \langle \Phi_+^{AB} | \sigma_1^A \sigma_3^A | \Phi_+^{AB} \rangle \\ &\sim \langle \Phi_+^{AB} | \sigma_2^A | \Phi_+^{AB} \rangle \sim \langle \Phi_+^{AB} | \Psi_-^{AB} \rangle = 0 \end{aligned} \quad (9.40)$$

gilt.

Wir notieren noch eine weitere mathematische Eigenschaft der Bell-Zustände. Sie sind Eigenvektoren zu Produkten der σ -Operatoren:

$$\sigma_1^A \sigma_1^B | \Phi_{\pm}^{AB} \rangle = (\pm 1) | \Phi_{\pm}^{AB} \rangle \quad (9.41)$$

$$\sigma_1^A \sigma_1^B | \Psi_{\pm}^{AB} \rangle = (\pm 1) | \Psi_{\pm}^{AB} \rangle \quad (9.42)$$

$$\sigma_3^A \sigma_3^B | \Phi_{\pm}^{AB} \rangle = | \Phi_{\pm}^{AB} \rangle. \quad (9.43)$$

$$\sigma_3^A \sigma_3^B | \Psi_{\pm}^{AB} \rangle = - | \Psi_{\pm}^{AB} \rangle. \quad (9.44)$$

9.2.2 Lokale und nicht-lokale Messungen

Wie wir in Abschn. 7.3.1 gesehen haben, kann Nicht-Lokalität in zweifacher Weise auftreten:

- (i) Zustände können nicht separabel sein.
- (ii) Messungen können zu Observablenoperatoren auf $\mathcal{H}^A \otimes \mathcal{H}^B \otimes \mathcal{H}^C \otimes \dots$ gehören, die nicht von der Form $C^A \otimes \mathbb{1}^B \otimes \mathbb{1}^C \dots$ oder $\mathbb{1}^A \otimes D^B \otimes \mathbb{1}^C \dots$ usw. sind (nicht-lokale Messungen). Sie stellen dann keine lokalen Messungen dar (Messungen an nur einem Teilsystem). Sie heißen *nicht-lokale Messungen* (non-local measurements) und messen *nicht-lokale Observablen* (non-local observables)

Wir betrachten speziell hermitesche Produktoperatoren $C^A D^B$ auf dem Raum $\mathcal{H}^A \otimes \mathcal{H}^B$. Sie beschreiben die nicht-lokale Messung der kollektiven physikalischen Größe $C^A D^B$ (als ein einziges Symbol zu lesen) an einem 2-Teile-System. Die Observable $\sigma_3^A \sigma_3^B$ eines 2-Spin-Systems ist ein Beispiel. Wie Gl. (9.43) und (9.44) zeigen sind die zugehörigen Messwerte $+1$ und -1 entartet. Als Ergebnis der Messung mit Messwert $+1$ wird der Zustand in den durch $|\Phi_+^{AB}\rangle$ und $|\Phi_-^{AB}\rangle$ aufgespannten Unterraum projiziert. Alle Bell-Zustände bleiben bei der Messung der Observablen $\sigma_3^A \sigma_3^B$ unverändert.

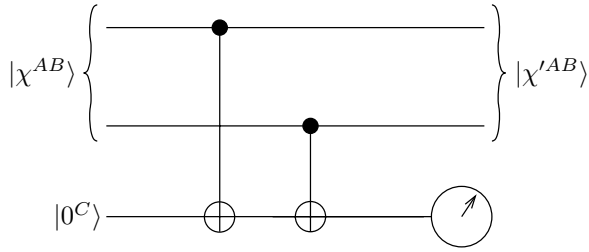


Abbildung 9.2: Nicht-lokale Messungen in der Rechenbasis am System S^{AB} durch projektive Messung am Hilfssystem S^C .

Misst Bob hingegen in lokaler Weise bei einem 2-Spin-System im Zustand $|\Phi_+^{AB}\rangle$ am Untersystem B die Observable σ_3^B (Spin in z -Richtung), so wird beim Messergebnis -1 das System in den Zustand $|1^A, 1^B\rangle$ überführt. Der Ausgangszustand $|\Phi_+^{AB}\rangle$ liegt nicht mehr vor. Die Verschränkung wurde durch die lokale Messung gebrochen. Eine nachfolgende Messung von σ_3^A durch Alice am Untersystem S^A ergibt den Messwert -1 und lässt den Zustand $|1^A, 1^B\rangle$ unverändert. Das Beispiel zeigt: Mathematisch entsteht die Wirkung des Operators $\sigma_3^A \sigma_3^B$ dadurch, dass die Operatoren σ_3^A und σ_3^B in \mathcal{H}_2^A bzw. \mathcal{H}_2^B wirken. Physikalisch stimmt aber die Messung der kollektiven Observablen $\sigma_3^A \sigma_3^B$ i.a. nicht mit zwei lokalen Spinmessungen durch Alice bzw. Bob überein. Das wird schon durch die unterschiedlichen Endzustände belegt. *Observablen, denen hermitesche Operatoren auf dem Produktraum entsprechen, benötigen zu ihrer Messung i.a. einen nicht-lokalen Messprozess.* Wie kann man nicht-lokale Messungen auf lokale Messungen zurückführen?

Wir betrachten ein einfaches Beispiel. Die Eigenwerte des Operators $\sigma_3^A \sigma_3^B$ sind $+1$ und -1 . Sie sind entartet. Das sieht man auch daran, dass neben $|\Phi_\pm^{AB}\rangle$ und Ψ_\pm^{AB} die Vektoren der Rechenbasis

$$\begin{aligned} \sigma_3^A \sigma_3^B |0, 0\rangle &= |0, 0\rangle, & \sigma_3^A \sigma_3^B |1, 1\rangle &= |1, 1\rangle \\ \sigma_3^A \sigma_3^B |0, 1\rangle &= -|0, 1\rangle, & \sigma_3^A \sigma_3^B |0, 1\rangle &= -|0, 1\rangle \end{aligned} \quad (9.45)$$

ebenfalls Eigenzustände zu $+1$ und -1 sind.

Die 2-Qubit-Observable $\sigma_3^A \sigma_3^B$ wird nicht-lokal durch eine kollektive Messung bestimmt. Sie kann mit Hilfe von zwei CNOT-Gattern und einem im Zustand $|0^C\rangle$ präparierten Hilfs-Qubit wie in Abb. 9.2 realisiert werden. Wir fügen also zu S^{AB} ein Hilfssystem S^C mit Zustand in \mathcal{H}_2^C hinzu. Ein beliebiger Zustand $|\chi^{AB}\rangle$ aus \mathcal{H}^{AB} lässt sich nach der Rechenbasis zerlegen

$$|\chi^{AB}\rangle = c_1|0^A, 0^B\rangle + c_2|1^A, 1^B\rangle + c_3|1^A, 0^B\rangle + c_4|0^A, 1^B\rangle \quad (9.46)$$

mit $\sum_i |c_i|^2 = 1$. Die Quantenschaltung überführt den Anfangszustand $|\chi^{AB}\rangle|0^C\rangle$ unitär in den Zustand

$$U|\chi^{AB}\rangle|0^C\rangle = c_1|0^A, 0^B, 0^C\rangle + c_2|1^A, 1^B, 0^C\rangle + c_3|1^A, 0^B, 1^C\rangle + c_4|0^A, 1^B, 1^C\rangle \quad (9.47)$$

Eine projektive Messung von σ_3^C auf dem Hilfssystem S^C ergibt die Messwerte $+1$ oder -1 mit den Wahrscheinlichkeiten $p(+1)$ und $p(-1)$. Zugleich überführt sie den Ausgangszustand

$|\chi^{AB}\rangle$ je nach Messergebnis in den Zustand χ'^{AB}_+ bzw. χ'^{AB}_- :

$$\begin{aligned} +1 : \quad |\tilde{\chi}'^{AB}_+\rangle &= c_1|0^A, 0^B\rangle + c_2|1^A, 1^B\rangle \\ p(+1) &= |c_1|^2 + |c_2|^2 \end{aligned} \quad (9.48)$$

$$\begin{aligned} -1 : \quad |\tilde{\chi}'^{AB}_-\rangle &= c_3|1^A, 0^B\rangle + c_4|0^A, 1^B\rangle \\ p(-1) &= |c_3|^2 + |c_4|^2. \end{aligned} \quad (9.49)$$

$|\tilde{\chi}'^{AB}_+\rangle$ ist die Projektion von $|\chi^{AB}\rangle$ in den von $|0^A, 0^B\rangle$ und $|1^A, 1^B\rangle$ aufgespannten Unterraum von \mathcal{H}^{AB} zum Eigenwert $+1$ von $\sigma_3^A \sigma_3^B$. Entsprechendes gilt für $|\tilde{\chi}'^{AB}_-\rangle$. Die Messungen am Hilfssystem haben auf die Messwerte und Wahrscheinlichkeiten der direkten Messung geführt. Die resultierenden Zustände von S^{AB} stimmen mit den Resultaten der Messungen von $\sigma_3^A \sigma_3^B$ überein.

Wir haben nach Verschränkung durch die unitäre Transformation U und projektive Messungen im Hilfsraum \mathcal{H}_2^C eine projektive nicht-lokale Messung am Zustand in \mathcal{H}^{AB} bewirkt. Die Messergebnisse und die Wahrscheinlichkeiten mit denen sie eintreten, konnten an der projektiven Messung in \mathcal{H}^C abgelesen werden. Dieses Beispiel für eine nicht-lokale Messung in \mathcal{H}^{AB} spiegelt eine ganz allgemeine Struktur von Quantenmessungen wieder. Wir werden solche verallgemeinerten Messungen noch ausführlich in Kap. 13 darstellen. Mit der beschriebenen 2-Qubit-Messung der Observablen $\sigma_3^A \sigma_3^B$ kann noch nicht zwischen zwei Zuständen zum gleichen Eigenwert $+1$ oder -1 unterschieden werden. Wir schildern im nächsten Kapitel, wie eine nicht-lokale Messung an der Bell-Basis auf zwei lokale Messungen zurückgeführt werden kann.

9.2.3 Nicht-lokal gespeicherte Information und Bell-Messungen

In der Rechenbasis von $\mathcal{H}_2^A \otimes \mathcal{H}_2^B$ lassen sich zwei Bit in Form der 4 Möglichkeiten $(0, 0)$, $(0, 1)$, $(1, 0)$, $(1, 1)$ speichern und durch zwei lokale Messungen mit $\sigma_3^A \otimes \mathbb{1}^B$ bzw. $\mathbb{1}^A \otimes \sigma_3^B$ wieder auslesen. Die zugehörigen Projektionsoperatoren sind:

$$P_{00} := |0^A, 0^B\rangle\langle 0^A, 0^B|, \quad P_{01} := |0^A, 1^B\rangle\langle 0^A, 1^B| \quad (9.50)$$

$$P_{10} := |1^A, 0^B\rangle\langle 1^A, 0^B|, \quad P_{11} := |1^A, 1^B\rangle\langle 1^A, 1^B|. \quad (9.51)$$

Die Information ist lokal gespeichert. In der Bell-Basis von $\mathcal{H}_2^A \otimes \mathcal{H}_2^B$ lassen sich ebenfalls zwei Bit speichern. Man spricht vom *Paritätsbit* (parity bit) Φ oder Ψ (d. h. parallele oder antiparallele „Spins“) und vom *Phasenbit* (phase bit) (Vorzeichen $+$ bzw. $-$). Wie wir schon gesehen haben, ist diese Information als wechselseitige Information in den Korrelationen und daher nicht-lokal gespeichert.

Wenn wir an einem System im Bell-Zustand $|\Phi_{\pm}^{AB}\rangle$ lokal die Observablen $\sigma_3^A \otimes \mathbb{1}^B$ und $\mathbb{1}^A \otimes \sigma_3^B$ messen und das Produkt der Messergebnisse bilden, so ergibt sich $+1$. Bei $|\Psi_{\pm}^{AB}\rangle$ ergibt sich entsprechend -1 . Damit ist lokal das Paritätsbit ausgemessen. Danach liegt aber nicht mehr der Ausgangszustand, sondern ein Zustand der Rechenbasis vor. Wir können daher lokal nur 1 bit auslesen. Entsprechendes gilt für die lokale Messung des Phasenbits durch $\sigma_1^A \otimes \mathbb{1}^B$ und $\mathbb{1}^A \otimes \sigma_1^B$. *Durch lokale Messungen kann nicht die volle in Bell-Zuständen gespeicherte Information ausgelesen werden.* Wir brauchen eine Projektionsmessung, die auf die Zustände der Bell-Basis statt auf die der Rechenbasis projiziert. Die beiden Basissysteme

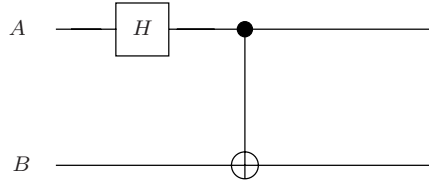


Abbildung 9.3: Quantenschaltung zur Erzeugung von Bell-Zuständen.

gehen durch eine unitäre Transformation im Raum $\mathcal{H}_2^A \otimes \mathcal{H}_2^B$ ineinander über. Das können wir ausnutzen.

Wir notieren die Wirkung einer Hadamard-Transformation gefolgt von einer CNOT-Transformation auf die Rechenbasis. Die *Quantenschaltung* (quantum circuit) hierzu findet sich in Abb. 9.3.

$$\begin{aligned} |0^A, 0^B\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}}(|0^A\rangle + |1^A\rangle)|0^B\rangle \\ &\xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(|0^A, 0^B\rangle + |1^A, 1^B\rangle) = |\Phi_+^{AB}\rangle \end{aligned} \quad (9.52)$$

$$|0^A, 1^B\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0^A\rangle + |1^A\rangle)|1^B\rangle \xrightarrow{\text{CNOT}} |\Psi_+^{AB}\rangle \quad (9.53)$$

$$|1^A, 0^B\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0^A\rangle - |1^A\rangle)|0^B\rangle \xrightarrow{\text{CNOT}} |\Phi_-^{AB}\rangle \quad (9.54)$$

$$|1^A, 1^B\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0^A\rangle - |1^A\rangle)|1^B\rangle \xrightarrow{\text{CNOT}} |\Psi_-^{AB}\rangle. \quad (9.55)$$

Wegen

$$H = H^\dagger, \quad H^2 = 1 \quad (9.56)$$

$$\text{CNOT} = (\text{CNOT})^\dagger, \quad (\text{CNOT})^2 = 1 \quad (9.57)$$

gilt insgesamt für die angewandte unitäre Transformation

$$U^{AB} := (\text{CNOT}) \cdot H, \quad (U^{AB})^{-1} = H \cdot (\text{CNOT}) \quad (9.58)$$

Wenn wir Bell-Zustände die Quantenschaltung in umgekehrter Richtung durchlaufen lassen, dann entstehen daraus durch Wirkung von $(U^{AB})^{-1}$ wieder die entsprechenden Zustände der Rechenbasis. Die Projektoren der Basissysteme sind über

$$|\phi_+^{AB}\rangle\langle\phi_+^{AB}| = U^{AB} P_{00}^{AB} (U^{AB})^{-1} \quad (9.59)$$

$$|\psi_+^{AB}\rangle\langle\psi_+^{AB}| = U^{AB} P_{01}^{AB} (U^{AB})^{-1} \quad (9.60)$$

$$|\phi_-^{AB}\rangle\langle\phi_-^{AB}| = U^{AB} P_{10}^{AB} (U^{AB})^{-1} \quad (9.61)$$

$$|\psi_-^{AB}\rangle\langle\psi_-^{AB}| = U^{AB} P_{11}^{AB} (U^{AB})^{-1} \quad (9.62)$$

verknüpft.

Eine *Bell-Messung* (Bell measurement) an einem Zustand $|\chi^{AB}\rangle$ besteht darin, ihn zunächst unitär und nicht-lokal mit $(U^{AB})^{-1} = H \cdot (\text{CNOT})$ zu transformieren und dann eine lokale Messung am resultierenden Zustand in der Rechenbasis durchzuführen. Dann wird z. B. mit der Wahrscheinlichkeit, die zum Projektionsoperator $|\Phi_+^{AB}\rangle\langle\Phi_+^{AB}|$ gehört,

$$p_{00} = \langle\chi^{AB}|\Phi_+^{AB}\rangle\langle\Phi_+^{AB}|\chi^{AB}\rangle \quad (9.63)$$

das Messwertepaar $(0, 0)$ erhalten. Entsprechend ergibt sich mit der Wahrscheinlichkeit $p_{01} = \langle\chi^{AB}|\Psi_+^{AB}\rangle\langle\Psi_+^{AB}|\chi^{AB}\rangle$ das Paar $(0, 1)$ usw. Dabei gilt $p_{00} + p_{01} + p_{10} + p_{11} = 1$. Im Spezialfall $|\chi^{AB}\rangle = |\Phi_+^{AB}\rangle$ ist $p_{00} = 1$. Entsprechendes gilt für die anderen Bell-Zustände. Kodiert man 2 Bit Information in Bell-Zuständen, dann kann diese Information eindeutig über die Bell-Messung ausgelesen werden mit den Entsprechungen $(0, 0) \leftrightarrow |\phi_+^{AB}\rangle$, $(0, 1) \leftrightarrow |\psi_+^{AB}\rangle$, $(1, 0) \leftrightarrow |\phi_-^{AB}\rangle$, $(1, 1) \leftrightarrow |\psi_-^{AB}\rangle$.

Um zu erreichen, dass die Bell-Messung auch in einen Bell-Zustand überführt, muss der in den lokalen Messungen erhaltene Zustand der Rechenbasis noch die Quantenschaltung (Anwendung von U^{AB}) rückwärts durchlaufen. Beim Messwertepaar $(0, 0)$ überführt sie dann z. B. in den zugehörigen Bell-Zustand $|\Phi_+^{AB}\rangle$.

9.3 Ergänzende Themen und weiterführende Literatur

Siehe Abschn. 5.6 und 6.6.

9.4 Übungsaufgaben

ÜA 9.1 [zu 9.2.2] Führen Sie hintereinander lokale Messungen von $\sigma_3^A \otimes \mathbb{1}^B$ und $\mathbb{1}^A \otimes \sigma_3^B$ an $|\chi^{AB}\rangle$ von Gl. (9.46) durch. Bestimmen Sie die resultierenden Zustände und die Wahrscheinlichkeiten für die verschiedenen Messwertepaare. Bilden Sie Messwerteprodukte und die zugehörigen Wahrscheinlichkeiten. Vergleichen Sie mit den Ergebnissen (9.48) und (9.49) sowie mit der Aussage über die Erwartungswerte aus Abschn. 7.3.4.

10 Es gibt keine (lokal-realistische) Alternative zur Quantentheorie

Wir haben im vorherigen Kapitel gesehen, dass bei verschränkten Zuständen, im Unterschied zu Zuständen klassischer Systeme, die Information nicht-lokal gespeichert ist. Im Folgenden soll ein Zugang beschrieben werden, der es erlaubt operational in direkter Weise zu demonstrieren, dass Verschränkung kein Gegenstück in der klassischen Physik hat. Wir wollen zeigen, dass Verschränkung eines der zentralen nicht-klassischen Strukturelemente der Quantentheorie ist. Hierzu geben wir exemplarisch zwei Experimente an, deren Ergebnisse klassisch nicht begründet werden können.

Von welchem Typ werden solche Experimente sein? Einen unmittelbaren experimentellen Zugriff auf zusammengesetzte Systeme haben wir über lokale Messungen an den Untersystemen. Wenn man die Paare der Messergebnisse vergleicht, zeigen sich charakteristische Unterschiede zwischen Systemen in verschränkten reinen Zuständen einerseits und nicht verschränkten sowie klassischen Systemen andererseits. Dies kann als eine weitere theoretische Charakterisierung von Verschränkung dienen. Von größerer Bedeutung ist aber in diesem Zusammenhang die Abgrenzung von Quantentheorie und klassischer Physik. Wenn sich klassische zusammengesetzte Systeme und verschränkte Quantensysteme in den Korrelationen unterscheiden und das Experiment die Existenz von Quantenkorrelationen bestätigt, dann gibt es ein Phänomen, das nicht klassisch begründet werden kann. Damit wäre gezeigt, dass die Quantentheorie nicht auf klassische Physik zurückführbar ist. Um dieses Programm durchzuführen, müssen wir typische Korrelationsexperimente beschreiben und sowohl quantentheoretisch wie auch klassisch durchrechnen. Dazu müssen wir aber zunächst die Frage „Was ist klassisch?“ beantworten und daraus experimentell prüfbare Konsequenzen ableiten.

10.1 EPR-Experimente und ihre quantentheoretische Deutung

Photonen Wir wollen ein Experiment mit den Kaskaden-Photonen beschreiben, die wir bereits in Abschn. 8.3 kennen gelernt haben. Eine Quelle emittiert paarweise Photonen mit verschiedenen Frequenzen ν_A und ν_B in entgegengesetzte Richtungen. Sie propagieren entlang der z -Achse zu den Beobachtern an den Orten A und B (vgl. Abb. 10.1). Die Abstände der Beobachter von der Quelle können sehr groß sein. Sie müssen nicht übereinstimmen. Die Photonenpaare sind polarisationsverschränkt. Sie befinden sich im rotationssymmetrischen

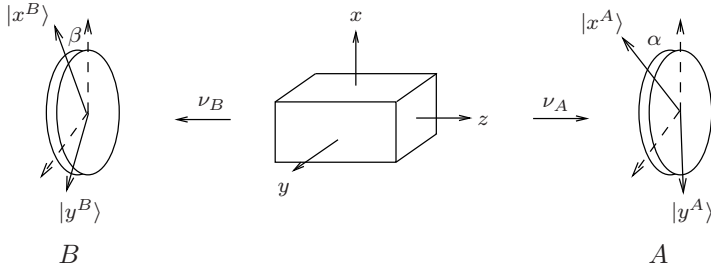


Abbildung 10.1: Polarisationsmessung an Photonenpaaren.

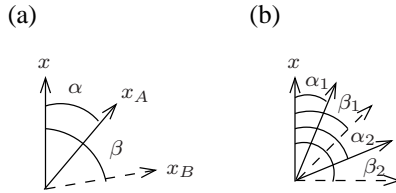


Abbildung 10.2: Orientierung der Analysatoren.

Bell-Zustand

$$|\Phi_+^{AB}\rangle = \frac{1}{\sqrt{2}}|x_0^A, x_0^B\rangle + |y_0^A, y_0^B\rangle. \quad (10.1)$$

$|x_0\rangle$ und $|y_0\rangle$ sind Zustände mit linearer Polarisation in x_0 - bzw. y_0 -Richtung.

Die Beobachter messen an den beiden Photonen die lineare Polarisation (vergl. Abb. 10.2a). Hierzu ist in A ein Analysator mit der Orientierung (x^A, y^A) aufgestellt. Er ist um einen Winkel α um die z -Achse gegen die durch die x - und y -Achse gegebene Orientierung gedreht. Hinter ihm befinden sich zwei Detektoren, die jeweils ansprechen, wenn die Polarisation $|x^A\rangle$ oder $|y^A\rangle$ gefunden wird. Der Polarisation $|x^A\rangle$ ordnen wir das Messergebnis $+1$ und der Polarisation $|y^A\rangle$ das Ergebnis -1 zu. Die Messung in B am zweiten Photon erfolgt in gleicher Weise. Wir wollen insbesondere zulassen, dass der B-Analysator um den Winkel $\beta \neq \alpha$ gegen die Ausgangsorientierung verdreht ist. Die entsprechenden Polarisationsrichtungen sind $|x^B\rangle$ bzw. $|y^B\rangle$. Ihnen sind wieder die Messwerte $+1$ bzw. -1 zugeordnet. Die Observablenoperatoren für die lokalen Messungen an den Photonen in A und B sind dementsprechend

$$E^A = |x^A\rangle\langle x^A| - |y^A\rangle\langle y^A| \quad (10.2)$$

$$E^B = |x^B\rangle\langle x^B| - |y^B\rangle\langle y^B|. \quad (10.3)$$

Wir betrachten zunächst Messungen nur am Photon in A bzw. nur am Photon in B. Die reduzierten Dichteoperatoren des Bell-Zustandes $|\Phi_+^{AB}\rangle$ sind jeweils maximal gemischt. Die Wahrscheinlichkeit in A das Resultat $+1$ oder -1 zu erhalten ist daher unabhängig von den Verdrehungen α und β jeweils $\frac{1}{2}$. Das gleiche gilt für die Messung am zweiten Photon in B.

Im nächsten Schritt untersuchen wir Korrelationen und bestimmen die Wahrscheinlichkeiten für das Auftreten von Messwertepaaren. Mit P_{+-} bezeichnen wir die Wahrscheinlichkeit, dass in A die x^A -Polarisation und in B die y^B -Polarisation gemessen wird. Das entspricht den lokalen Messwerten $+1$ und -1 und dem Messwerteprodukt -1 . Die Wahrscheinlichkeiten für die restlichen Kombinationen sind entsprechend bezeichnet. Für die vektoriellen Polarisationszustände haben wir

$$|x^A\rangle = \cos \alpha |x\rangle + \sin \alpha |y\rangle \quad (10.4)$$

$$|y^A\rangle = -\sin \alpha |x\rangle + \cos \alpha |y\rangle. \quad (10.5)$$

Analoge Relationen gelten für $|x^B\rangle$ und $|y^B\rangle$ mit dem Drehwinkel β . Damit ergibt sich für die Wahrscheinlichkeit P_{++}

$$P_{++} = \langle \Phi_+^{AB} | x^A, x^B \rangle \langle x^A, x^B | \Phi_+^{AB} \rangle = \frac{1}{2} \cos^2(\beta - \alpha). \quad (10.6)$$

und entsprechend für die anderen Wahrscheinlichkeiten

$$P_{--} = P_{++} = \frac{1}{2} \cos^2(\beta - \alpha) \quad (10.7)$$

$$P_{+-} = P_{-+} = \frac{1}{2} \sin^2(\beta - \alpha). \quad (10.8)$$

Dass nur die Differenz der Drehwinkel α und β auftaucht, spiegelt die Rotationssymmetrie des Ausgangszustands $|\Phi_+^{AB}\rangle$ wieder.

EPR-Korrelationen verschränkter Photonen Im Spezialfall der parallelen Ausrichtung der Polarisatoren ($\alpha = \beta$) finden wir eine vollständige Korrelation der Messergebnisse: Wenn in A die $|x^A\rangle$ -Polarisation gefunden wird, dann wird in B mit Sicherheit ebenfalls die $|x^B\rangle$ -Polarisation gefunden ($P_{++} = 1$). Gleiches gilt für die y-Polarisationen ($P_{--} = 1$). Die beiden Polarisationsrichtungen treten dabei in A und B in völlig zufälliger Weise jeweils mit der Wahrscheinlichkeit $\frac{1}{2}$ auf. Unterschiedliche Polarisierungen werden nie registriert ($P_{+-} = P_{-+} = 0$).

Um die Korrelationen der Messergebnisse bei nicht-paralleler Ausrichtung der Analysatoren zu erfassen, führen wir den *Korrelationskoeffizienten* (correlation coefficient) ϵ^{AB} ein. Er ist definiert als der Erwartungswert des Produktes der lokalen Messwerte in A und B. Wie wir in Abschn. 9.2.2 gesehen haben, lässt er sich als Erwartungswert des Produktoperators $E^A \otimes E^B$ berechnen:

$$\epsilon^{AB} := \langle \Phi_+^{AB} | E^A \otimes E^B | \Phi_+^{AB} \rangle. \quad (10.9)$$

Die explizite Auswertung mit Gl. (10.2) und Gl. (10.3) führt auf die Wahrscheinlichkeiten von Gl. (10.7) und (10.8) (vergl. Gl. (10.6)).

$$\epsilon^{AB} = P_{++} + P_{--} - P_{+-} - P_{-+}. \quad (10.10)$$

Die Gleichung (10.10) kann auch direkt abgelesen werden. Sie enthält die Messwerteprodukte $+1$ und -1 multipliziert mit den Wahrscheinlichkeiten ihres Auftretens. Gl. (10.10) wird mit Gl. (10.7) und (10.8) ausgewertet und führt auf das Ergebnis

$$\epsilon^{AB} = \cos 2(\beta - \alpha). \quad (10.11)$$

Im Spezialfall parallel orientierter Analysatoren ($\alpha = \beta$) ergibt sich die perfekte Korrelation $\epsilon^{AB} = 1$.

Objekte mit Spin- $\frac{1}{2}$ Für Polarisationsmessungen an zwei Objekten mit Spin- $\frac{1}{2}$ können wir ganz analog vorgehen. Es wird zu einer gegebenen \mathbf{e}_3 -Richtung der Bell-Zustand

$$|\Phi_+^{AB}\rangle = \frac{1}{\sqrt{2}}(|0^A, 0^B\rangle + |1^A, 1^B\rangle) \quad (10.12)$$

durch eine Quelle präpariert. $|0\rangle$ und $|1\rangle$ sind die Eigenzustände zu σ_3 . In A und B werden die Polarisierungen in Richtung \mathbf{a} bzw. \mathbf{b} gemessen. Um die Rechnung zu vereinfachen nehmen wir an, dass \mathbf{a} und \mathbf{b} senkrecht auf \mathbf{e}_2 stehen

$$\mathbf{a} = (\sin \alpha, 0, \cos \alpha), \quad \mathbf{b} = (\sin \beta, 0, \cos \beta). \quad (10.13)$$

Die entsprechenden Observablen sind

$$E^A = \boldsymbol{\sigma}^A \mathbf{a}, \quad E^B = \boldsymbol{\sigma}^B \mathbf{b}. \quad (10.14)$$

Den Korrelationskoeffizienten E^{AB} von Gl. (10.9) können wir mit Rückgriff auf einige schon abgeleitete Hilfsrelationen einfach bestimmen. Wir wenden zunächst Gl. (9.37) und (9.39) an und berücksichtigen dabei $a_2 = b_2 = 0$. Dann greifen wir auf Gl. (3.11) zurück, verwenden $\mathbf{a} \times \mathbf{b} \sim \mathbf{e}_2$ sowie die Gl. (9.38) und die Orthonormalität der Bell-Vektoren. Nacheinander finden wir so für den Korrelationskoeffizienten ϵ^{AB} :

$$\begin{aligned} \epsilon^{AB} &= \langle \Phi_+^{AB} | (\boldsymbol{\sigma}^A \mathbf{a}) (\boldsymbol{\sigma}^B \mathbf{b}) | \Phi_+^{AB} \rangle = \Phi_+^{AB} | (\boldsymbol{\sigma}^A \mathbf{a}) (\boldsymbol{\sigma}^B \mathbf{b}) | \Phi_+^{AB} \rangle \\ &= \langle \Phi_+^{AB} | (ab) \mathbb{1}^A | \Phi_+^{AB} \rangle + i \langle \Phi_+^{AB} | \boldsymbol{\sigma}^A (\mathbf{a} \times \mathbf{b}) | \Phi_+^{AB} \rangle \\ &= ab = \cos \alpha \cos \beta + \sin \alpha \sin \beta = \cos(\beta - \alpha). \end{aligned} \quad (10.15)$$

Verglichen mit ϵ^{AB} für Photonen taucht bei Spinoren typischerweise wieder der halbe Winkel auf.

10.2 Korrelierte Handschuhe

Wir haben gesehen, dass bei paralleler Ausrichtung der Analysatoren in A und B vollständige Korrelation herrscht. Wenn an einem Photon am Ort A die x-Polarisation gemessen wird, dann wird mit Sicherheit auch am Photon in B die parallele x-Polarisation registriert und umgekehrt. Entsprechendes finden wir für die y-Polarisation. Es kommt dabei nicht darauf an, ob zuerst in A oder zuerst in B gemessen wird. Weiterhin kann der Abstand zwischen A und B beliebig groß sein (ideale Übertragung der Photonen vorausgesetzt). Ist das ein Resultat, das man nur für Quantenobjekte findet?

Handschuhpaar Wir wollen unter einem Handschuhpaar einen linken und einen rechten Handschuh verstehen. Jeder der Handschuhe wird in einen Kasten getan. Ein Kasten wird nach A und der andere nach B transportiert. Die dortigen Beobachter wissen, dass es sich um ein Handschuhpaar handelt. Wird dann nach Öffnen des Kastens in A ein rechter (bzw.

ein linker) Handschuh gefunden, dann kann der Beobachter in A im selben Augenblick mit Sicherheit sagen, dass in B ein linker (bzw. ein rechter) Handschuh schon gefunden wurde oder noch gefunden wird. Eine entsprechende Aussage kann der Beobachter in B machen, wenn er seinen Kasten geöffnet hat.

Selbstverständlich lag der jeweilige Handschuhtyp *real* schon vor der Öffnung der Kästen in A und B fest. Die Handschuhe sind klassisch korreliert. Ermittlung des Handschuhtyps in A hat weder auf den Handschuh in A selber noch auf den in B einen Einfluss gehabt (Entsprechendes gilt für B). Die physikalische Realität am Ort eines Beobachters wird nicht durch ein entferntes Experiment des Partners abgeändert. Es gibt für Handschuhe nur *lokale* Vorgänge. Obwohl eine vollständige Information über den anderen Handschuh gewonnen wird, hat keine Informationsübertragung stattgefunden. Die vollständige Korrelation geht einfach darauf zurück, dass das 2-Handschuhe-System am Anfang als ein Handschuhpaar *präpariert* wurde.

Wir haben bei den Handschuhen eine Situation der klassischen Physik beschrieben, die – soweit es die Messergebnisse betrifft – genau der Situation beim Photonenpaar bei paralleler Analysatorausrichtung entspricht. Lässt sich daher möglicherweise auch das 2-Photonen-Experiment im Rahmen einer rein klassischen Theorie, d. h. ohne Bezug auf die Quantentheorie, beschreiben? Um eine möglichst allgemein gültige Antwort zu geben, wollen wir zunächst am Beispiel der Handschuhe ablesen, welche Prinzipien für eine klassische Theorie gelten.

10.3 Lokaler Realismus

Wir orientieren uns begrifflich an dem Artikel von A. Einstein, B. Podolsky und N. Rosen [EPR 35] und charakterisieren die klassische Physik durch die zwei Prinzipien des *lokalen Realismus* (local realism), die wir am Handschuhpaar ablesen können:

Physikalische Realität¹ Eigenschaften (z. B. Energie) physikalischer Systeme sind diejenigen physikalischen Größen, deren Wert man mit Sicherheit vor der entsprechenden Messung (z. B. Energiemessung) vorhersagen kann. Diese Eigenschaften liegen real bereits vor der Messung vor. Das System „hat sie“. Sie sind *Elemente der physikalischen Realität* (elements of physical reality). Ihr Wert ist unabhängig davon, ob er gemessen wird oder nicht. Wir nennen dieses klassische Realitätskonzept *Einstein-Realität*.

Lokalität² Die physikalische Realität kann in *lokaler* Weise beschrieben werden. Das heißt, dass jedes System seine Eigenschaften unabhängig von allen anderen Systemen hat. Insbesondere bleibt das Resultat einer Messung an einem System unbeeinflusst von Einwirkungen auf davon räumlich getrennte andere Systeme. Dieses Lokalitätskonzept der klassischen Physik heißt *Einstein-Lokalität*.

¹Elemente der Realität: „If without in any way disturbing a system, we can predict with certainty the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity. This means that this physical quantity has a value independent of whether we measure it or not.“ [EPR 35]

²Lokalität: „The real factual situation of system A is independent of what is done with system B, which is spatially separated from the former.“. [EPR 35].

Verborgene Parameter Wir gehen – wie die EPR-Autoren auch – davon aus, dass die experimentellen Aussagen der Quantentheorie korrekt sind. Wenn man dann annimmt, dass Einstein-Realität und Einstein-Lokalität zutreffende Beschreibungen physikalischer Systeme sind, dann ist die Quantentheorie zwar nicht falsch aber *unvollständig* (incomplete).³ Es gibt Elemente der Realität, die nicht in der Theorie wiedergegeben werden. Sie tauchen dort nicht auf und sind daher *verborgene Parameter* (hidden variables).

Unter einer *klassischen Theorie* (classical theory) wollen wir eine Theorie verstehen, die – anders als die Quantentheorie – die beiden Forderungen des lokalen Realismus erfüllt. Wir werden versuchen, die bisher verborgenen Parameter explizit einzuführen, um eine lokal-realistische und somit klassische *Alternativtheorie* zur Quantentheorie zu konstruieren, die alle experimentellen Phänomene im Quantenbereich begründen kann. Verkürzt gesagt: *Es gibt nur klassische Physik*. Wir wollen diesem Programm folgen und versuchen Photonen und Spin-1/2 Objekte so zu beschreiben, wie man Handschuhe beschreibt. Es wird sich zeigen, dass dieser Versuch misslingt.

10.4 Verborgene Parameter, Bellsche Ungleichungen und Konflikt mit dem Experiment

Stochastische lokal-realistische Theorie Wir berechnen die Ergebnisse des Polarisationsexperiments aus Abschn. 10.1 im Rahmen einer ganz allgemein angesetzten lokal-realistischen Theorie. Ein im Symbol λ zusammengefasster Satz von verborgenen Parametern repräsentiert die „Elemente der Realität“, die im Zusammenhang mit der Polarisation eines nunmehr klassisch beschriebenen einzelnen Photons oder Spin-1/2-Teilchens auftauchen. λ ist variabel. Die Eigenschaften eines einzelnen Teilchens ist durch einen bestimmten Parameter λ charakterisiert. Wir formulieren eine stochastische lokal-realistische Theorie. Teilchen mit Parameter λ werden von der Quelle mit der Wahrscheinlichkeitsdichte $\rho(\lambda)$ produziert, für die

$$\int \rho(\lambda) d\lambda = 1, \quad \rho(\lambda) \geq 0 \quad (10.16)$$

gilt.

Für ein durch λ charakterisiertes Photon in A und den Drehwinkel δ_1 des Analysators in A liegt fest, ob die Polarisationsrichtung x^A oder y^A gemessen wird. Wir ordnen wie in Abschn. 10.2 dem Messergebnis den Messwert $+1$ bzw. -1 zu. Dann gibt es dementsprechend eine eindeutige Funktion $S_B^\lambda(\delta_1)$ von λ und δ_1 mit den Werten $+1$ bzw. -1 . Analog gibt es eine möglicherweise davon verschiedene Funktion $S_A^\lambda(\delta_2)$, die zu gegebenem λ und gegebener Verdrehung δ_2 in B eindeutig den dortigen Messwert $+1$ oder -1 bestimmt.

$$S_A^\lambda(\delta_1) = \begin{Bmatrix} +1 \\ -1 \end{Bmatrix}, \quad S_B^\lambda(\delta_2) = \begin{Bmatrix} +1 \\ -1 \end{Bmatrix} \quad (10.17)$$

Der klassische Korrelationskoeffizient ist

$$\epsilon^{kl}(\delta_1, \delta_2) = \int \rho(\lambda) S_A^\lambda(\delta_1) S_B^\lambda(\delta_2) d\lambda. \quad (10.18)$$

³ Vollständigkeit: „In a complete theory there is an element corresponding to each element of reality“. [EPR 35]

Dass das Produkt der beiden Funktionen auftaucht, drückt die Lokalität aus. Durch die Formulierung mit verborgenen Parametern λ ist eine lokal-realistische Theorie für den Korrelationskoeffizienten entstanden.

Bellsche Ungleichung In einem ersten Schritt passen wir die bisher noch sehr allgemein formulierte Theorie an die zu reproduzierenden quantentheoretischen Messergebnisse an. Im Spezialfall gleicher Ausrichtung soll die gut bestätigte vollständige Korrelation

$$\epsilon^{kl}(\delta, \delta) = \int \rho(\lambda) S_A^\lambda(\delta) S_B^\lambda(\delta) d\lambda = 1 \quad (10.19)$$

gelten. Mit Gl. (10.16), (10.17) und (10.18) folgt daraus

$$S_A^\lambda(\delta) = S_B^\lambda(\delta) =: S^\lambda(\delta). \quad (10.20)$$

Die beiden Observablen haben die gleiche funktionale Abhängigkeit von der verborgenen Variablen λ und dem Winkel δ .

Wir gehen zu einer allgemeineren Situation über und betrachten drei Orientierungen δ_1, δ_2 und δ_3 . Es werden Messungen durchgeführt mit folgenden Einstellungen der Analysatoren in A und B: (δ_1, δ_2) , (δ_2, δ_3) und (δ_1, δ_3) . Für die Observablen gilt dann wegen Gl. (10.17)

$$S^\lambda(\delta_1) S^\lambda(\delta_2) - S^\lambda(\delta_1) S^\lambda(\delta_3) = \underbrace{S^\lambda(\delta_1) S^\lambda(\delta_2)}_{=\pm 1} \underbrace{[1 - S^\lambda(\delta_2) S^\lambda(\delta_3)]}_{\geq 0}. \quad (10.21)$$

Integration führt hiermit und mit Gl. (10.16) und (10.17) auf

$$\begin{aligned} & \left| \int \rho(\lambda) \{ S^\lambda(\delta_1) S^\lambda(\delta_2) - S^\lambda(\delta_1) S^\lambda(\delta_3) \} d\lambda \right| \\ &= \left| \int \rho(\lambda) S^\lambda(\delta_1) S^\lambda(\delta_2) [1 - S^\lambda(\delta_2) S^\lambda(\delta_3)] d\lambda \right| \\ &\leq \int \rho(\lambda) \underbrace{[1 - S^\lambda(\delta_2) S^\lambda(\delta_3)]}_{\geq 0} d\lambda = 1 - \int \rho(\lambda) S^\lambda(\delta_2) S^\lambda(\delta_3) d\lambda. \end{aligned} \quad (10.22)$$

Gl. (10.22) bedeutet für die klassischen Korrelationsfunktionen

$$|\epsilon^{kl}(\delta_1, \delta_2) - \epsilon^{kl}(\delta_1, \delta_3)| \leq 1 - \epsilon^{kl}(\delta_2, \delta_3). \quad (10.23)$$

Dies ist die *Bellsche Ungleichung* (Bell inequality).

Konflikt mit der Quantentheorie Auf welches Ergebnis führt demgegenüber die Quantentheorie? Wir untersuchen Spin-1/2-Teilchen im Zustand $|\Phi_+^{AB}\rangle$ und wählen als Einstellungen für die Analysatoren: $\delta_1 = 60^\circ$, $\delta_2 = 120^\circ$, $\delta_3 = 180^\circ$. Dann erhalten wir für die Korrelationskoeffizienten

$$\epsilon^{AB}(\delta_1, \delta_2) = \frac{1}{2}, \quad \epsilon^{AB}(\delta_1, \delta_3) = -\frac{1}{2}, \quad \epsilon^{AB}(\delta_2, \delta_3) = \frac{1}{2}. \quad (10.24)$$

Einsetzen in Gl. (10.23) führt auf

$$1 \leq \frac{1}{2}, \quad (10.25)$$

d. h. die *Bellsche Ungleichung ist verletzt*. *Quantentheorie und lokal-realistische Theorien führen auf unterschiedliche Aussagen*. Für Photonen wählt man einen Winkel von 30° statt von 60° und stellt ebenfalls eine Verletzung der Bellschen Ungleichung fest.

CHSH-Ungleichung Wir diskutieren noch eine andere Kombination von Drehwinkeln. Ein Bezug auf das Experiment, wie wir ihn in Gl. (10.20) eingebaut haben, ist dabei nicht nötig. In A wird mit den Einstellungen α_1 und α_2 und in B mit β_1 und β_2 gemessen. Wir betrachten die folgende Kombination von Observablenfunktionen und notieren die verschiedenen Werte, die in Folge von $S_{A,B}^\lambda = \pm 1$ angenommen werden können:

$$\begin{array}{ccc} \{S_A^\lambda(\alpha_2) \underbrace{[S_B^\lambda(\beta_1) + S_B^\lambda(\beta_2)]}_{\pm 2} + S_A^\lambda(\alpha_1) \underbrace{[S_B^\lambda(\beta_1) - S_B^\lambda(\beta_2)]}_{0} & =: & \{\dots\} \\ & \begin{array}{ccc} \xleftarrow{\hspace{1.5cm}} & & \xrightarrow{\hspace{1.5cm}} \\ 0 & & \pm 2 \end{array} & (10.26) \end{array}$$

Es gilt somit

$$|\{\dots\}| = 2 \quad (10.27)$$

und daher mit Gl. (10.16)

$$\left| \int \rho(\lambda) \{\dots\} d\lambda \right| \leq \int \rho(\lambda) |\{\dots\}| d\lambda = 2 \int \rho(\lambda) d\lambda = 2. \quad (10.28)$$

Für die klassischen Korrelationskoeffizienten bei den Messungen mit den verschiedenen Winkeleinstellungen bedeutet das

$$S^{VP} := |\epsilon^{kl}(\alpha_2, \beta_1) + \epsilon^{kl}(\alpha_2, \beta_2) + E^{kl}(\alpha_1, \beta_1) - \epsilon^{kl}(\alpha_1, \beta_2)| \leq 2. \quad (10.29)$$

Dies ist die nach J. F. Clauser, M. A. Horne, A. Shimony und R. A. Hold [CHS 69] benannte *CHSH-Ungleichung* (CHSH inequality).

Alle Ungleichungen für die Korrelationskoeffizienten in stochastischen Theorien mit verborgenen Parametern (stochastische lokal-realistische Theorien) werden üblicherweise einheitlich *Bellsche Ungleichungen* (Bell inequalities) genannt. *Sie sind Gleichungen der klassischen Physik.* Ihre Bedeutung für die Quantentheorie wird erst deutlich, wenn man Prognosen aufgrund der Bell-Ungleichungen den quantentheoretischen Prognosen gegenüberstellt (wie in Gl. (10.25)) und beide mit den tatsächlichen experimentellen Ergebnissen vergleicht.

Konflikt mit der Quantentheorie Für die entsprechende Messung an korrelierten Photonen im Zustand $|\Phi_+^{AB}\rangle$ wählt man Winkel, die sich um $22,5^\circ$ unterscheiden (vergl. Abb. 10.2b): $\alpha_1 = 22,5^\circ$, $\beta_1 = 45^\circ$, $\alpha_2 = 67,5^\circ$, und $\beta_2 = 90^\circ$. Das führt mit Gl. (10.11) auf:

$$\epsilon^{AB}(\alpha_1, \beta_1) = \epsilon^{AB}(\alpha_2, \beta_1) = \epsilon^{AB}(\alpha_2, \beta_2) = \cos \frac{\pi}{4} = \frac{1}{\sqrt{2}} \quad (10.30)$$

$$\epsilon^{AB}(\alpha_1, \beta_2) = \cos \frac{3\pi}{4} = -\frac{1}{\sqrt{2}}. \quad (10.31)$$

(Für Spin- $\frac{1}{2}$ -Teilchen doppelte Winkel einstellen.) Die quantentheoretische Berechnung der Korrelationskoeffizienten in Gl. (10.29) liefert

$$S^{QM} = 2\sqrt{2}. \quad (10.32)$$

Vergleich mit der CHSH-Ungleichung führt zu dem Ergebnis: *Die Quantentheorie verletzt die CHSH-Ungleichung.*

Experimentum crucis⁴ Wir haben zwei experimentelle Anordnungen beschrieben, für die Quantentheorie einerseits und Theorien mit verborgenen Parametern andererseits auf sich widersprechende Prognosen führen. In einer solchen Situation können Experimente eine Entscheidung herbeiführen. Die Experimente bestätigen die quantentheoretischen Prognosen (vergl. Abschn. 10.8). *Die lokal-realistischen Alternativtheorien zur Quantentheorie sind damit widerlegt.* Die Ursache ist darin zu suchen, dass die EPR-Korrelationen im verschränkten Bell-Zustand nicht durch Einführung verborgener lokaler Parameter simuliert werden können. Sie sind echte Quantenkorrelationen.

10.5 Separable Quantengemische erfüllen die Bellsche Ungleichung

Wir betrachten separable d. h. nicht verschränkte Gemische von 2-Teilchen-Zuständen

$$\rho^{AB} = \sum_i \lambda_i \rho_i^A \otimes \rho_i^B, \quad 0 \leq \lambda_i \leq 1, \quad \sum_i \lambda_i = 1 \quad (10.33)$$

und bilden wieder den quantentheoretischen Korrelationskoeffizienten (vergl. Gl. (10.9))

$$\begin{aligned} E^{AB}(\alpha, \beta) &= \text{tr}_{AB}[\rho^{AB} E^A(\alpha) \otimes E^B(\beta)] \\ &= \sum_i \lambda_i A_i(\alpha) B_i(\beta) \end{aligned} \quad (10.34)$$

mit

$$A_i(\alpha) := \text{tr}_A[\rho_i^A E^A(\alpha)], \quad B_i(\beta) := \text{tr}_B[\rho_i^B E^B(\beta)]. \quad (10.35)$$

Die Beträge der Erwartungswerte von Operatoren mit Eigenwerten ± 1 können 1 nicht übersteigen, daher haben wir

$$|A_i(\alpha)| \leq 1, \quad |B_i(\beta)| \leq 1. \quad (10.36)$$

Die Auswertung der CHSH-Ungleichung führt auf

$$\begin{aligned} &|E^{AB}(\alpha_2, \beta_1) + E^{AB}(\alpha_2, \beta_2) + E^{AB}(\alpha_1, \beta_1) - E^{AB}(\alpha_1, \beta_2)| \\ &= \left| \sum_i \lambda_i \{A_i(\alpha_2)B_i(\beta_1) + A_i(\alpha_2)B_i(\beta_2) + A_i(\alpha_1)B_i(\beta_1) - A_i(\alpha_1)B_i(\beta_2)\} \right| \\ &\leq \sum_i \lambda_i \{|A_i(\alpha_2)B_i(\beta_1) + A_i(\alpha_2)B_i(\beta_2)| + |A_i(\alpha_1)B_i(\beta_1) - A_i(\alpha_1)B_i(\beta_2)|\}. \end{aligned} \quad (10.37)$$

Als Folge der Separabilität treten nur Produkte auf. Wir schätzen den Inhalt der geschweiften Klammer $\{\dots\}$ mit Gl. (10.36) ab

$$\{\dots\} \leq |B_i(\beta_1) + B_i(\beta_2)| + |B_i(\beta_1) - B_i(\beta_2)| \leq 2 \quad (10.38)$$

⁴Ein Experiment, das es gestattet, unter mehreren Theorien eine zu bestätigen und die übrigen zu widerlegen, nennt man ein *experimentum crucis*.

und erhalten mit Gl. (10.33) für die rechte Seite der Ungleichung (10.37)

$$\sum_i \lambda_i \{ \dots \} \leq 2. \quad (10.39)$$

Einsetzen in Gl. (10.37) und Vergleich mit der CHSH-Ungleichung (10.29) zeigt, dass für 2-Teile-Systeme ein separables Gemisch von Quantenzuständen (und damit auch jeder reine Produktzustand) die Bellsche Ungleichung erfüllt. Die Erfüllung der CHSH-Ungleichung ist daher nur eine notwendige Bedingung für das Vorliegen einer lokalen Theorie mit verborgenen Parametern und keine hinreichende Bedingung.

10.6 Bell-Verletzung als Kriterium für Verschränkung bei reinen Zuständen

Für separable Zustände erfüllt sowohl die nicht-realistische Quantentheorie mit den Besonderheiten ihres nicht-klassischen Messprozesses wie auch jede realistische Theorie (vergl. Abschn. 10.5) die Bellsche Ungleichung. Wir haben gesehen, dass das Durchbrechen der Ungleichung beim maximal verschränkten Zustand $|\Phi_+^{AB}\rangle$ eine Folge der fehlenden Separabilität, d. h. eine Folge seiner Verschränktheit ist. Diese Aussage lässt sich verallgemeinern. Man kann ausgehend von der Schmidt-Zerlegung aus Abschn. 8.2.1 zeigen, dass sich für alle verschränkten reinen Zustände von 2-Teile-Systemen, also auch für nicht maximal verschränkte Zustände, Observablen finden lassen, sodass die Bell-Ungleichung durch die korrelierten Messergebnisse verletzt wird. [Hom 97, S. 206], [HS 91, Kap. 2.1.4].

Zusammenfassend können wir daher feststellen: Für reine Zustände von 2-Teile-Systemen ist Verschränkung äquivalent mit Verletzung der Bell-Ungleichung. Wir haben damit für diese Zustände ein operationales, d. h. im Prinzip experimentell realisierbares Verfahren gefunden, um Verschränkung festzustellen. Eine entsprechende Aussage für Gemische oder Zustände von Systemen mit mehr als zwei Teilen gibt es zur Zeit noch nicht.

10.7 3-Teilchen-Verschränkung und Quantennichtlokalität

10.7.1 GHZ-Zustand

D. M. Greenberger, M. A. Horne und A. Zeilinger (GHZ) haben in einer vom Bell-Zugang unabhängigen nicht-statistischen Weise gezeigt, dass Quantentheorie und lokaler Realismus nicht miteinander verträglich sind. ([GHZ 89], [GHZ 90]). Wir geben hier ihre Argumentation mit Bezug auf die Spins von 3 Quantenobjekten wieder, die sich voneinander getrennt an den Orten A, B und C befinden sollen. Sie sind miteinander verschränkt. Ihr Gesamtzustand liegt in $\mathcal{H}_2^A \otimes \mathcal{H}_2^B \otimes \mathcal{H}_2^C$ und soll durch

$$|\psi^{ABC}\rangle = \frac{1}{\sqrt{2}}(|0^A, 0^B, 0^C\rangle + |1^A, 1^B, 1^C\rangle) \quad (10.40)$$

gegeben sein. $|0\rangle$ bzw. $|1\rangle$ sind wieder die Eigenvektoren von σ_z mit den Eigenwerten $+1$ und -1 . Der Zustand (10.40) des 3-Teile-Systems heißt *GHZ-Zustand* (GHZ state). Er ist symmetrisch gegenüber einer Vertauschung der Bezeichnungen A, B und C.

10.7.2 Lokaler Realismus und Quantentheorie im Konflikt

Wir bestimmen zunächst das Ergebnis von lokalen quantentheoretischen Spinmessungen an den drei Teilsystemen. Dabei werden verschiedene Polarisationsrichtungen gewählt. In der yyx -Messung zum Beispiel werden jeweils die Observablen σ_y^A, σ_y^B und σ_x^C gemessen. Die Reihenfolge der Messungen ist unwichtig. Zur Bestimmung des Messergebnisses ist es geschickt, in den Räumen $\mathcal{H}_2^A, \mathcal{H}_2^B$ und \mathcal{H}_2^C die Eigenvektoren der jeweiligen Observablen als Basis einzuführen und den Zustandsvektor $|\psi^{ABC}\rangle$ hiernach zu zerlegen. Dann ergibt sich

$$|\psi^{ABC}\rangle = \frac{1}{2}(|0_y^A, 1_y^B, 0_x^C\rangle + |1_y^A, 0_y^B, 0_x^C\rangle + |0_y^A, 0_y^B, 1_x^C\rangle + |1_y^A, 1_y^B, 1_x^C\rangle). \quad (10.41)$$

Die Messwerte bezeichnen wir mit s_x und s_y . Sie sind stets $+1$ oder -1 . Wie man an Gl. (10.41) ablesen kann, erfüllen die möglichen Kombinationen der korrelierten Messwerte für jedes einzelne 3-Teile-System die Relation

$$s_y^A s_y^B s_x^C = -1. \quad (10.42)$$

Symmetrie unter Vertauschung der Bezeichnungen der Teilsysteme führt auf

$$s_x^A s_y^B s_y^C = -1, \quad s_y^A s_x^B s_y^C = -1. \quad (10.43)$$

Für eine xxx -Messung der Observablen σ_x^A, σ_x^B und σ_x^C zerlegen wir $|\psi^{ABC}\rangle$ nach den Eigenvektoren von σ_x

$$|\psi^{ABC}\rangle = \frac{1}{2}(|0_x, 0_x, 0_x\rangle + |0_x, 1_x, 1_x\rangle + |1_x, 0_x, 1_x\rangle + |1_x, 1_x, 0_x\rangle) \quad (10.44)$$

und finden

$$s_x^A s_x^B s_x^C \stackrel{qu}{=} +1. \quad (10.45)$$

An den Gl. (10.42) und (10.43) lässt sich die folgende Eigenschaft des Systems im GHZ-Zustand ablesen: Das Resultat der σ_x -Messung an einem der Teilsysteme kann mit Sicherheit vorhergesagt werden, wenn die Ergebnisse der σ_y -Messungen an den beiden anderen Teilsystemen bekannt sind. Um z. B. das Ergebnis s_x^A der σ_x^A -Messung zu bestimmen, muß man nur an den Systemen die Observablen σ_x^B und σ_y^C messen. Analog kann man das Resultat einer σ_y -Messung vorhersagen, wenn man an den beiden anderen Systemen eine σ_x - und eine σ_y -Messung vornimmt. Dies sind die Aussagen der Quantentheorie, die durch das Experiment bestätigt werden.

Wir wollen jetzt diese Prognosen der Quantentheorie (bzw. die experimentellen Aussagen) vom Standpunkt des lokalen Realismus interpretieren. Um die durch die Gl. (10.42) bis (10.44) wiedergegebenen Korrelationen im Rahmen dieses Zugangs zu begründen, müssen wir annehmen: Die in den σ -Messungen ermittelten individuellen Eigenschaften der einzelnen Teilsysteme liegen schon vor der Messung fest. Sie sind daher auch unabhängig davon, welchen Typ von σ -Messung wir für die drei Teilsysteme wählen. Der Ausgang einer jeden Messung ist z. B. über verborgene Parameter vorherbestimmt. Wenn das so ist, dann sind bei einem der 3-Teile-Objekte die individuellen Werte $s_{x,y}^{A,B,C}$ in allen drei Gleichungen (10.42)

und (10.43) dieselben. Wir multiplizieren die linken Seiten der Gl. (10.42)-(10.43) miteinander und erhalten mit $s_y^A s_y^A = s_y^B s_y^B = s_y^C s_y^C = 1$ im Gegensatz zu Gl. (10.45)

$$s_x^A s_x^B s_x^C \stackrel{l.r.}{=} -1. \quad (10.46)$$

Dies ist in der lokal-realistischen Theorie das Ergebnis einer xxx -Messung. Die x -Polarisationen müssen bereits vor der Messung so beschaffen sein, dass Gl. (10.46) gilt. In der quantentheoretischen Beschreibung der Messergebnisse liegen beim nicht separablen GHZ-Zustand vor der Messung keine Polarisationen fest. Eine xxx -Messung führt auf Messwerte, die Gl. (10.45) erfüllen. Damit besteht ein klarer Widerspruch zwischen der Aussage lokal-realistischer Theorien und der Quantentheorie. Wenn die Experimente die quantentheoretische Gleichung (10.45) bestätigen – was tatsächlich der Fall ist (vergl. Abschn. 10.8) – dann ist der lokale Realismus widerlegt.

Warum kann man in der Quantentheorie nicht in gleicher Weise aus den Gl. (10.42) und (10.43) eine Relation (10.45) ableiten? Gleichung (10.41) zeigt, dass die quantentheoretischen Messergebnisse korreliert sind. Wenn die lokalen Messungen z. B. $s_y^A = +1$ und $s_y^B = -1$ ergeben, dann findet man $s_x^C = +1$. Für $s_y^A = +1$ und $s_y^B = +1$ findet man entsprechend $s_x^C = -1$ usw. Das Ergebnis s_x^C liegt nicht vorher fest und stimmt i. a. in den Gl. (10.42) und (10.43) nicht überein.

Wir haben folgendes gezeigt: *Drei Objekte werden in einem Präparationsverfahren so präpariert, dass der resultierende Zustand im Rahmen der Quantentheorie der GHZ-Zustand (10.40) ist. Wenn sich dann für die oben beschriebenen Polarisationsmessungen die quantentheoretischen Vorhersagen als richtig erweisen, dann ist jede lokal-realistische Theorie für diese Systeme widerlegt.* Die Quantentheorie kann daher durch solche Theorien nicht ersetzt werden.

Wir haben in Abschn. 3.6 gesehen, dass die beiden linearen Polarisationen und die zirkuläre Polarisation im \mathcal{H}_2 in enger Analogie zum Spin formuliert werden können. Für photonische GHZ-Zustände lässt sich in gleicher Weise ein Widerspruch ableiten. Für Photonen bestätigen die experimentellen Resultate die quantentheoretischen Vorhersagen und widerlegen so den lokal-realistischen Ansatz. Eine Übersicht über die Experimente findet sich z. B. in [PZ 02].

Wir weisen abschließend noch auf Unterschiede zur Bell-Argumentation hin. Die CHSH-Ungleichung macht Aussagen über klassische Erwartungswerte und ist eine direkte Folge des lokalen Realismus. Sie macht eine Aussage über die klassische Physik ohne Bezug auf die Quantentheorie. Das GHZ-Argument basiert demgegenüber auf dem Versuch einer lokal-realistischen Interpretation von quantentheoretischen Resultaten (10.42) und (10.43), von denen angenommen wird, dass sie experimentell bestätigt sind. Der Widerspruch zur Quantentheorie ist nicht probabilistisch sondern direkt. In beiden Fällen bestätigen die Experimente die Quantentheorie.

10.8 Ergänzende Themen und weiterführende Literatur

- Die Klassiker : [EPR 35], [Bel 64], [CHS 69], [Boh 51], [GHZ 89], [GHZ 90].
- Übersichtsartikel: [Aul 00, Kap. IX], [HS 91], [Hom 97, Kap. 4], [Per 93, Kap. 6], [HS 91], [WW 01].

- Das Argument von Hardy: In einer vom Bell- und vom GHZ-Zugang unabhängigen Weise hat Hardy gezeigt, dass lokaler Realismus und Quantentheorie nicht kompatibel sind. Eine Darstellung des verblüffenden Theorems mit Hinweisen auf weitere Literatur findet sich z. B. in [Hom 97, Kap. 4.2.2.1] und [Aul 00, Kap. 36.6].
- Bücher mit Übersichtsartikeln zur Bellschen Ungleichung und Experimenten dazu: [BZ 02], [Asp 02].
- Zur Einsteinschen Kritik an der Quantentheorie: [Hom 97, Kap. 8].

10.9 Übungsaufgaben

ÜA 10.1 [zu 10.1] Geben Sie einen alternativen (direkten) Beweis für Gl. (10.15) an.

ÜA 10.2 [zu 10.4] Beweisen Sie Gl. (10.20).

ÜA 10.3 [zu 10.4] An einem linear polarisierten Photon im Zustand $|\varphi^A\rangle$ werden Messungen mit einem Analysator A mit den Richtungen x^A und y^A durchgeführt. Formulieren Sie für diese Situation ein Modell mit verborgenen Parametern, d. h. geben Sie λ , $\rho(\lambda)$ und S_A^λ so an, dass die Messergebnisse richtig wiedergegeben werden.

ÜA 10.4 [zu 10.7] Geben Sie eine Quantenschaltung an, die den Zustand $|0^A, 0^B, 0^C\rangle$ in den GHZ-Zustand überführt.

This Page Intentionally Left Blank

11 Verschränkung als Hilfsmittel

Verschränkung ist die Grundlage für neue Effekte und deren technische Anwendung. Wir diskutieren einige Beispiele.

11.1 Quantenkryptographie

11.1.1 Die Vernam-Verschlüsselung

Alice möchte an Bob eine verschlüsselte Botschaft schicken, die perfekt geheim bleiben soll. Niemand außer Bob soll sie entschlüsseln können. In dem von Vernam 1926 vorgeschlagenen Verfahren [Ver 26] wird ein *Quellentext* (source text), der bereits digital als (0,1)-Folge der Länge n vorliegen soll, mit Hilfe eines *Schlüssels* (key) verschlüsselt. Es entsteht das *Kryptogramm* (cryptogram). Der Schlüssel selber besteht aus einer (0,1)-Zufallsfolge, die ebenfalls die Länge n hat. Zur Verschlüsselung werden die Zahlen von Quelltext und Schlüssel gliedweise modulo 2 addiert. Wir machen ein Beispiel:

Quellentext	01101100
Schlüssel	10000110
Kryptogramm	11101010

Das Kryptogramm wird an Bob geschickt. Bob soll im Besitz des Schlüssels sein. Die Entschlüsselung besteht darin, dass Bob den Schlüssel zu der verschlüsselten Nachricht gliedweise modulo 2 addiert. Wegen $x + 0 + 0 = x + 0 = x$ und $x + 1 + 1 = x + 0 = x$ entsteht dann wieder der Quelltext:

Kryptogramm	11101010
Schlüssel	10000110
Quellentext	01101100

Da der Schlüssel aus einer Zufallsfolge besteht, wird der verschlüsselte Text vom Quelltext völlig unabhängig. Er kann offen von Alice an Bob geschickt werden. Für einen Lauscher, der nicht den Schlüssel besitzt, enthält das Kryptogramm keinerlei Information. Entscheidend ist, dass der Schlüssel nur Alice und Bob bekannt ist, dass er tatsächlich eine echte Zufallsfolge ist, dass er so lang wie der Quelltext ist und insbesondere, dass er nur einmal verwendet wird (one-time pad system). Unter diesen Voraussetzungen kann der Vernam-Kode nicht gebrochen werden [Sha 49].

Das Problem bei dem Verfahren besteht darin, dass Bob und Alice immer wieder für jede Botschaft in den Besitz eines neuen Schlüssels kommen müssen und dass bei diesem Prozess sicher gestellt sein muß, dass der Schlüssel nicht von einem Lauscher gelesen wurde.

Wir wollen zeigen, dass eine solche Schlüsselübermittlung mit Hilfe von Quantensystemen möglich ist. Es gibt eine ganze Reihe von quantenkryptographischen Verfahren (vergl. Abschn. 11.5). Wir diskutieren hier nur zwei Typen von Verfahren. Die einen Verfahren nutzen die Besonderheiten des quantenphysikalischen Messprozesses aus, die anderen verwenden die nicht-lokalen EPR-Korrelationen. Die Abfolge von Handlungsanweisungen zur Durchführung eines kryptographischen Schemas nennt man *Protokoll* (protocol).

11.1.2 B92-Protokoll

Das nach der Arbeit [Ben 92] von C.H. Bennett aus dem Jahre 1992 benannte B92-Protokoll verwendet zur Schlüsselübertragung zwei nicht-orthogonale Quantenzustände und nutzt die folgenden für Quantensysteme charakteristischen Eigenschaften aus: (i) Es gibt keine Messung mit der zwischen den beiden Zuständen unterschieden werden kann. (ii) Die Zustände können nicht durch einen Quantenkopierer geklont werden. (iii) Eine Messung ändert i.a. einen Quantenzustand ab.

Der Ablauf der Schlüsselübermittlung Wir wollen Photonen für die Durchführung des B92-Protokolls verwenden. Alice hat zwei Filter, die Photonen vertikal im Zustand $|V\rangle$ oder unter der Neigung -45° , d. h. im Zustand $|V'\rangle$ linear polarisieren können (vergl. Abschn. 3.6). Es gilt $\langle V|V'\rangle|^2 = \frac{1}{2}$. Alice verwendet eine binäre Zufallsfolge, z. B. 1, 0, 0, 1, 1, 0, \dots , und erzeugt bei Vorliegen der 0 ein Photon mit der Polarisation $|V\rangle$ und bei 1 mit der Polarisation $|V'\rangle$. Die Photonen fliegen störungsfrei zu Bob.

Bob hat ein Messgerät in Form eines Detektors, der hinter einem Polarisationsfilter steht. Er kann für den Filter zwei Orientierungen wählen: horizontale Polarisation $|H\rangle$, ihr entspricht der Projektionsoperator $P_1 = \mathbb{1} - |V\rangle\langle V| = |H\rangle\langle H|$, und um -45° gedrehte Polarisation, ihr entspricht der Projektionsoperator $P_0 = \mathbb{1} - |V'\rangle\langle V'| = |H'\rangle\langle H'|$. Bob hat ebenfalls eine binäre Zufallsfolge zur Verfügung, die unabhängig von der Folge ist, die Alice benutzt, z. B. 0, 0, 1, 0, 1, 0, \dots . Die Zahlen 0 und 1 kommen in beiden Fällen gleich häufig vor. Die i -te Zahl von Bobs Folge bestimmt die Art der Messung am i -ten von Alice präparierten Photon. Wenn bei Bob die Zahl 0 vorliegt, stellt er die Analysatorrichtung $|H'\rangle$ (entspricht P_0) ein und bei der 1 die Richtung $|H\rangle$ (entspricht P_1). In jedem Fall registriert er, ob sein Detektor anspricht oder nicht.

Wegen der Orthogonalität der Vektoren gilt $P_0|V'\rangle = 0$ und $P_1|V\rangle = 0$. Wenn Alice und Bob verschiedene Zahlen vorliegen haben, spricht daher der Detektor bei Bob nicht an. Haben Alice und Bob gleiche Zahlen vorliegen, dann spricht der Detektor wegen $\langle V|P_0|V\rangle = \langle V'|P_1|V'\rangle = \frac{1}{2}$ mit der Wahrscheinlichkeit $\frac{1}{2}$, also in der Hälfte der Fälle an. Ein Beispiel ist in Tabelle 11.1 dargestellt. „ja/nein“ besagt, dass bei der Versuchsanordnung das Ergebnis ja oder nein jeweils mit der Wahrscheinlichkeit $\frac{1}{2}$ möglich ist. Der tatsächlich eingetretene Fall ist unterstrichen.

Im nächsten Schritt teilt Bob über einen öffentlichen Kanal Alice mit, bei welchen Photonen sein Detektor angesprochen hat. Die zugehörige Orientierung teilt er nicht mit. In dem in der Tabelle dargestellten Beispiel sind das die Photonen mit den Nummern 2 und 6. Damit besitzen Alice und Bob eine übereinstimmende Zahlenfolge 0, 0, \dots , die nur ihnen beiden bekannt ist und die sie als Schlüssel verwenden können. Es ist wie gewünscht eine Zufallsfolge der Zahlen 0 und 1, besteht aber nur im Mittel noch aus 25% der Zahlen der ursprünglichen Folge.

Tabelle 11.1: B92-Protokoll zur Quantenkryptografie.

Photonennummer	1	2	3	4	5	6
Zahlenfolge Alice	1	0	0	1	1	0
erzeugte Polarisation	$ V'\rangle$	$ V\rangle$	$ V\rangle$	$ V'\rangle$	$ V'\rangle$	$ V\rangle$
Zahlenfolge Bob	0	0	1	0	1	0
Analysatorstellung	$ H'\rangle$	$ H'\rangle$	$ H\rangle$	$ H'\rangle$	$ H\rangle$	$ H'\rangle$
Ansprechen	nein	<u>ja</u> /nein	nein	nein	ja/ <u>nein</u>	<u>ja</u> /nein

Abwehr von Lauschangriffen Wir wollen kurz auf die Sicherheit bei dieser Erzeugung eines gemeinsamen Schlüssels eingehen. Nehmen wir an, eine dritte Person mit Namen *Eve*¹ versucht in einem *Lauschangriff* (eavesdropping) durch Abfangen und Polarisationsmessungen an den Photonen in den Besitz des Schlüssels zu kommen, dann hat sie die oben mit (i) bis (iii) aufgeführten Probleme. Sie kann den Polarisationszustand eines einzelnen Photons in einer Messung nicht sicher bestimmen. Sie kann den Zustand auch nicht auf viele Photonen kopieren, ein Photon weiterlaufen lassen und an den Kopien Messungen durchzuführen. Schließlich wird sie durch eine Messung den Zustand des anschließend zu Bob geschickten Photons abändern. Es ist dieser Umstand, der es Alice und Bob ermöglicht festzustellen, ob ein Lauscher tätig war. Durch die Zustandsänderung wird Bob hin und wieder ein Ansprechen seines Analysators feststellen, obwohl bei ihm und Alice nicht die gleichen Zahlen vorliegen. Das können beide feststellen, indem sie einen zufällig ausgewählten Teil ihres Schlüssels öffentlich austauschen und vergleichen. Liegt Lauschen vor, dann wird der ganze Schlüssel nicht verwendet und ein neuer Versuch einer Schlüsselerzeugung begonnen. Ein Test auf Lauschen besteht zusätzlich in der Prüfung, ob 25% der Photonen zum Schlüssel beitragen.

Verbesserung der Sicherheit Tatsächlich ist der Transport der Quantenobjekte von Alice zu Bob, auch dann wenn nicht abgehört wird, anfällig für Störungen. Der Quantenkanal ist im Allgemeinen verrauscht. Damit in der Praxis überhaupt ein Schlüssel erzeugt wird, müssen Alice und Bob ein gewisses Ausmaß an Fehlern akzeptieren, von denen sie nicht wissen, ob sie nicht doch auf den Einfluss von Eve zurückgehen. Diese Situation taucht in allen quantentheoretischen Kryptographieverfahren auf. Im letzten Schritt des entsprechenden Protokolls werden daher klassische Algorithmen eingesetzt um zunächst Fehler zu korrigieren. In einem Protokoll (error correction protocol) wird versucht einen kürzeren Schlüssel zu gewinnen. daran schließt sich ein Verfahren an, in dem Eves Information auf ein Minimum reduziert wird (private amplification algorithm). Für Übersichtsartikel siehe Abschn. 11.5.

11.1.3 Weitere 1-Qubit-Protokolle

Das auf zwei nicht-orthogonalen Zuständen beruhende B92-Protokoll ist anfällig gegenüber POVM-Messungen. Diese nicht projektiven Messungen werden wir in Kap. 13 vorstellen. Daher ist es Standard geworden, wie beim BB84-Protokoll vier Zustände zu verwenden. Ein weiterer Ansatz ist der folgende: Die Symmetrie der Bloch-Kugel legt es nahe, die Eigenzustände von σ_x , σ_y und σ_z zu verwenden. Das entsprechende 6-Zustände-Protokoll erlaubt eine vereinfachte Sicherheitsanalyse (vergl. Abschn. 11.5).

¹Von eavesdropper, das ist der Lauscher

11.1.4 EPR-Protokolle

Quantenkryptographie unter Verwendung des Bellschen Theorems Das in Abschn. 10.4 beschriebene Experiment mit Photonenpaaren zum Test der CHSH-Ungleichung kann auch zur Schlüsselübermittlung verwendet werden. Das Protokoll sieht die folgenden Schritte vor, die entweder öffentlich erfolgen oder von Alice (in A) und Bob (in B) jeweils im Geheimen durchgeführt werden.

Öffentlich

In A und B einheitliche Festlegung der vier Messrichtungen $\alpha_1 = 22,5^\circ, \beta_1 = 45^\circ, \alpha_2 = 67,5^\circ, \beta_2 = 90^\circ$ im Raum (wie in Abschn. 10.4, vergl. Abb. 10.1)

Es wird öffentlich ausgetauscht, welche Polarisationsrichtungen in A und B bei den einzelnen Photonenpaaren jeweils gewählt wurden.

Die Messergebnisse zu *ungleicher* Orientierung werden zusammen mit der Nummer der Photonenpaare öffentlich ausgetauscht. Hiermit prüft jede Seite nach, ob der quantentheoretische Wert $S^{QM} = 2\sqrt{2}$ von Gl. (10.32) für die Korrelationen erreicht wurde. Wenn nicht, wird die Übertragungsreihe verworfen, da abgehört wurde. Wird S^{QM} erreicht,

Jeweils in A und B geheim

Die Quelle erzeugt Paare verschränkter Photonen im Bell-Zustand $|\Phi_+^{AB}\rangle$. In A und B werden unabhängig voneinander in völlig zufälliger Reihenfolge die Analysatoren in eine der 4 Richtungen gedreht. In A werden wie in Abschn. 10.1 die Polarisationszustände $|x^A\rangle$ (Messwert +1) bzw. $|y^A\rangle$ (Messwert -1) gemessen und in B entsprechend $|x^B\rangle$ (Messwert +1) bzw. $|y^B\rangle$ (Messwert -1).

In A und B wurden jeweils die Messergebnisse danach sortiert, ob gleiche oder ungleiche Analysatorrichtungen vorlagen.

dann sind die nicht ausgetauschten Ergebnisse zu *gleicher Orientierung* perfekt korreliert (vergl. Abschn. 10.1). Sie stellen eine völlig zufällige Abfolge der Zahlen 0 und 1 dar, die von Alice und Bob als Schlüssel verwendet werden kann.

Für die Schlüsselerzeugung mit Spin- $\frac{1}{2}$ -Teilchen werden Orientierungen mit den doppelten Winkeln eingestellt.

Die einzelnen Teilsysteme bei Alice und Bob befinden sich in den maximal gemischten Zuständen $\rho^A = \rho^B = \frac{1}{2}\mathbb{1}$. An ihnen kann keinerlei Information abgelesen werden. Wie wir schon in Kap. 9 gesehen haben, steckt Information allein in den Korrelationen. Wenn ein Lauscher eine Messung z. B. an den zu Alice fliegenden Objekten durchführt, dann überführt er dieses Untersystem in einen reinen Zustand. Wir haben in Abschn. 8.2.4 gezeigt, dass damit die Verschränkung durchbrochen wird und ein separabler Zustand entsteht. Gemäß Abschn. 10.5 erfüllen separable Zustände die CHSH-Ungleichung, d. h. es gilt $|S| \leq 2$. Die explizite Rechnung führt sogar auf $|S| \leq \sqrt{2}$ (vergl. [ÜA 11.3]). Dieser Wert unterscheidet sich deutlich vom quantentheoretischen Wert $S^{QM} = 2\sqrt{2}$.

BBM92-Protokoll² Es gibt ein sehr einfaches Protokoll, das auf EPR-Korrelationen beruht und keinen Bezug auf eine Bellsche Ungleichung benötigt. Wir verwenden wieder Photonenpaare im drehsymmetrischen Bell-Zustand $|\Phi_+^{AB}\rangle$, den wir mit Bezug auf die linearen Polarisationen $|H\rangle, |V\rangle$ und $|H'\rangle, |V'\rangle$ aus Abschn. 3.6 in der Form

$$|\Phi_+^{AB}\rangle = \frac{1}{\sqrt{2}}(|H^A, H^A\rangle + |V^A, V^A\rangle) = \frac{1}{\sqrt{2}}(|H'^A, H'^A\rangle + |V'^A, V'^A\rangle) \quad (11.1)$$

schreiben. Alice und Bob messen unabhängig voneinander in völlig zufälliger Weise entweder die Polarisationen $|H\rangle$ und $|V\rangle$ oder die um -45° dagegen gedrehten Polarisationen $|H'\rangle$ und $|V'\rangle$.

Nach einer Reihe von Messungen an Photonenpaaren tauschen Alice und Bob aus, welche Richtung sie bei den einzelnen Paaren eingestellt hatten. Die Ergebnisse, die zu verschiedenen Richtungen gehören, und diejenigen, bei denen ein Photon verloren gegangen ist, werden eliminiert. Die verbleibenden Messergebnisse müssen perfekt korreliert sein, wenn nicht gelauscht wurde. Um das zu prüfen, vergleichen Alice und Bob wieder eine hinreichend große Untermenge dieser Messungen über einen öffentlichen Kanal. Im positiven Fall liefert die für beide gleiche Sequenz der verbliebenen Messergebnisse den gewünschten Schlüssel.

11.1.5 Das Schema der Quantenkryptografie

Die Grundidee besteht darin, Bob und Alice mit Hilfe von Quantensystemen als Träger in den Besitz des selben Schlüssels kommen zu lassen. Die Botschaft selber wird nach ihrer Verschlüsselung in einem allgemein zugänglichen Kanal übertragen. Das Protokoll muss so gestaltet werden, dass Alice und Bob jeder für sich feststellen kann, ob bei der Schlüsselübertragung ein Lauscher tätig war. Hierfür nutzen sie aus, dass eine Quantenmessung durch den Lauscher den Zustand abändert, wenn er nicht gerade ein Eigenzustand der gemessenen Observablen ist.

Wenn die Präparationen von Alice und die Ergebnisse der zugehörigen Messungen von Bob mit der theoretischen Prognose übereinstimmen, ist kein Messeingriff erfolgt und es gibt

²Benannt nach der Arbeit [BBM 92].

keinen Informationsgewinn für einen Lauscher. Alice und Bob tauschen einen Teil ihrer Ergebnisse öffentlich aus und prüfen so die Übereinstimmung. Wenn sie nicht vorliegt, wird die Schlüsselübermittlung verworfen und das Protokoll neu durchlaufen. Im anderen Fall haben Alice und Bob einen geheimen Schlüssel erhalten, der darüber hinaus eine perfekte Zufallsverteilung darstellt, da er auf Quantenprozessen beruht.

11.2 Ein Qubit überträgt zwei Bit (dense coding)

In Kap. 6 haben wir gesehen, dass man ein Bit in einem Qubit kodieren und wieder auslesen kann. Kann man mehr klassische Information mit einem einzigen Qubit übertragen? Wir wollen zeigen, dass *dichtes Quantenkodieren* (quantum dense coding) die Übertragung von zwei Bits durch ein Qubit ermöglicht. Der Trick ist dabei, dass vor der Übertragung bereits ein verschränktes 2-Qubit-System mit Teilsystemen bei Alice und Bob etabliert wurde. Zum Beispiel hat Alice ein Qubit-System (z. B. ein Photon eines Photonenpaares) an Bob geschickt und den damit verschränkten Partner bei sich behalten. Der Zustand des Gesamtsystems sei z. B. $|\Phi_+^{AB}\rangle$. Bob erhält dadurch keine Information. Weiterhin wurde vorher zwischen Alice und Bob abgesprochen, wie Sie zwei Bits den vier Bellzuständen $|\Phi_+^{AB}\rangle$, $|\Phi_-^{AB}\rangle$, $|\Psi_+^{AB}\rangle$ und $|\Psi_-^{AB}\rangle$ zuordnen.

Wir haben in Abschn. 9.2.1 darauf hingewiesen, dass man lokal mit Hilfe der σ -Operatoren in unitärer Weise einen Bell-Zustand in jeden anderen Bell-Zustand transformieren kann. Alice soll die Transformationen $\mathbb{1}^A$ (trivial), σ_1^A , σ_2^A und σ_3^A an ihrem Qubit ausführen können. Zur Übertragung der zwei Bit Information überführt sie so den verschränkten Zustand $|\Phi_+^{AB}\rangle$ in den entsprechenden Bell-Zustand und schickt ihr Qubit-System an Bob. Damit kann Bob auf beide Teilsysteme zugreifen und durch Messung feststellen, welcher Bell-Zustand vorliegt. Durch Übermittlung eines Qubits sind an ihn zwei Bits übertragen worden.

Dichtes Kodieren lässt sich nur schwer implementieren. Wenn der verwendete verschränkte reine Zustand nicht maximal verschränkt ist, nimmt die Menge der übertragenen Information ab und wird im Grenzfall ein Bit. Eine wichtige Eigenschaft des Verfahrens ist die Abhörsicherheit. Es kann im günstigsten Fall an dem Qubit-System das Alice an Bob schickt, ein Bit ausgelesen werden. Dichtes kodieren demonstriert noch einmal die Bedeutung von Verschränkung als Hilfsmittel bei der Informationsübertragung.

11.3 Quantenteleportation

Alice besitzt ein ihr unbekanntes klassisches Objekt, z. B. eine Eisenkugel, die in einem Kasten eingeschlossen ist. Bob hätte gerne ein gleiches Objekt. Dazu muss Alice den Kasten aufmachen und optische Messungen an der Kugel durchführen. Sie übermittelt über einen klassischen Kanal die Informationen an Bob und der kann sich aus einem Eisenblock eine Kugel im gleichen Zustand herstellen. Kann ein analoges Verfahren auch bei Quantenobjekten zum Erfolg führen?

Eine einzige Messung an einem Quantenobjekt in einem unbekannten Zustand reicht nicht zur Zustandsbestimmung. Selbst wenn Alice der Quantenzustand bekannt wäre, weil sie die Präparationsanlage kennt, müsste sie an Bob unendlich viele Bits übertragen. Das sieht man

bereits am Beispiel von Qubit-Systemen. Das Qubit-System das Alice besitzt, möge in einem Eigenzustand von σ_r sein. Um den Vektor r zu beschreiben, braucht man eine binäre Zahl mit unendlich vielen Stellen. Nur bei vollständiger Kenntnis von r könnte Bob das Präparationsverfahren exakt wiederholen. Alice muss daher einen anderen Zugang wählen.

Mit Blick auf das Vorgehen bei dichtem Kodieren liegt es nahe, wieder eine verschränkungsunterstützte Informationsübertragung zu versuchen. Tatsächlich führt das folgende Protokoll der *Quantenteleportation* (quantum teleportation) zum Erfolg (vergl. Abb. 11.1): Alice und Bob teilen sich wieder den Bell-Zustand $|\Phi_+^{AB}\rangle$. Die Teilsysteme sind die Quantensysteme S^A und S^B , die sich bei Alice bzw. Bob befinden. Bei Alice befindet sich ein weiteres Quantensystem S^C in einem ihr unbekannten reinen Zustand

$$|\varphi^C\rangle = a|0^C\rangle + b|1^C\rangle \quad (11.2)$$

mit $|a|^2 + |b|^2 = 1$.

Dieser Zustand $|\varphi\rangle$, nicht das Quantensystem S^C selber, soll zu Bob teleportiert werden, das heißt, dass das sich bei Bob befindliche Teilsystem S^B in den reinen Zustand $|\varphi^B\rangle$ übergehen soll. S^B ist dann notwendigerweise mit keinem anderen System mehr verschränkt. Insgesamt liegt ein 3-Teile-System vor. An seinem Zustand in $\mathcal{H}_2^C \otimes \mathcal{H}_2^A \otimes \mathcal{H}_2^B$ führen wir einige algebraische Umformungen durch. Dazu verwenden wir die Definition der Bell-Zustände sowie die Eigenschaften der Pauli-Operatoren und führen in einem Zwischenschritt in $\mathcal{H}_2^C \otimes \mathcal{H}_2^A$ eine Bell-Basis ein.

$$\begin{aligned} |\varphi^C\rangle|\Phi_+^{AB}\rangle &= \frac{1}{\sqrt{2}} (a|0^C\rangle + b|1^C\rangle) (|0^A\rangle|0^B\rangle + |1^A\rangle|1^B\rangle) \\ &= \frac{1}{\sqrt{2}} (a|0^C\rangle|0^A\rangle|0^B\rangle + a|0^C\rangle|1^A\rangle|1^B\rangle \\ &\quad + b|1^C\rangle|0^A\rangle|0^B\rangle + b|1^C\rangle|1^A\rangle|1^B\rangle) \\ &= \frac{1}{2} \left\{ a(|\Phi_+^{CA}\rangle + |\Phi_-^{CA}\rangle)|0^B\rangle + a(|\Psi_+^{CA}\rangle + |\Psi_-^{CA}\rangle)|1^B\rangle \right. \\ &\quad \left. + b(|\Psi_+^{CA}\rangle - |\Psi_-^{CA}\rangle)|0^B\rangle + b(|\Phi_+^{CA}\rangle - |\Phi_-^{CA}\rangle)|1^B\rangle \right\} \quad (11.3) \\ &= \frac{1}{2} \left\{ |\Phi_+^{CA}\rangle(a|0^B\rangle + b|1^B\rangle) + |\Psi_+^{CA}\rangle(a|1^B\rangle + b|0^B\rangle) \right. \\ &\quad \left. + |\Psi_-^{CA}\rangle(a|1^B\rangle - b|0^B\rangle) + |\Phi_-^{CA}\rangle(a|0^B\rangle - b|1^B\rangle) \right\} \\ &= \frac{1}{2} \left\{ |\Phi_+^{CA}\rangle|\varphi^B\rangle + |\Psi_+^{CA}\rangle\sigma_1^B|\varphi^B\rangle + \right. \\ &\quad \left. + |\Psi_-^{CA}\rangle(-i\sigma_2^B)|\varphi^B\rangle + |\Phi_-^{CA}\rangle\sigma_3^B|\varphi^B\rangle \right\}. \end{aligned}$$

Bisher haben wir den Ausgangszustand nur mathematisch nach einer Bell-Basis in dem Alice zugänglichen Raum $\mathcal{H}_2^C \otimes \mathcal{H}_2^A$ entwickelt. Dabei ist in \mathcal{H}_2^B bis auf Transformationen mit den Pauli-Operatoren der Zustand $|\varphi^B\rangle$ entstanden. Bob muß diese Transformation noch durch einen Eingriff kompensieren. Dazu wird zunächst Alice tätig. Sie führt an den Teilsystemen S^C und S^A eine Bell-Messung durch, beispielsweise so wie wir das in Abschn. 9.2.3 beschrieben haben. Damit überführt sie das Gesamtsystem in einen der vier Summanden in der

letzten Gleichung (11.3). Welcher Summand nach der Messung vorliegt, kann sie dem Messergebnis entnehmen. Die entsprechenden zwei Bits an klassischer Information – mehr Bits werden nicht benötigt – überträgt Alice z. B. telefonisch an Bob. Der kennt damit ebenfalls den Zustand des Gesamtsystems und kann durch Transformationen mit einem der Operatoren ($\mathbb{1}^B, \sigma_k^B$) wegen $\sigma_k^B \sigma_k^B = \mathbb{1}^B$ sein System S^B in den Zustand $|\varphi^B\rangle$ überführen. Damit ist die Teleportation gelungen.

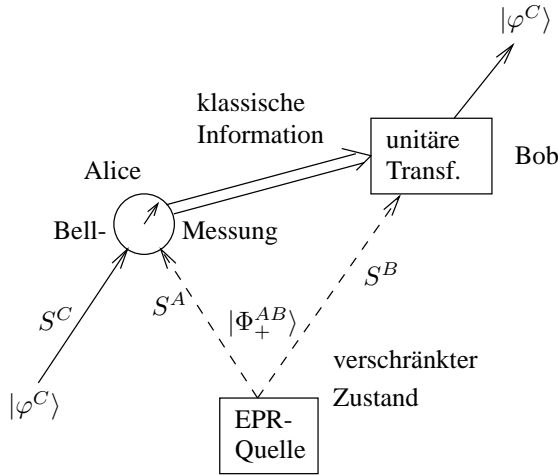


Abbildung 11.1: Quantenteleportation.

Am Ende der Zustandsübertragung befindet sich keines der Systeme S^C und S^A im Zustand $|\varphi\rangle$. Das spiegelt das Kopierverbot wieder. Die anfängliche Verschränktheit von S^A und S^B wurde auf S^C und S^A übertragen. Jedes der Ergebnisse der Bell-Messung von Alice tritt mit der gleichen Wahrscheinlichkeit $\frac{1}{4}$ auf. Aus dieser Messung kann weder Alice noch Bob eine Information über den teleportierten Zustand $|\varphi\rangle$ gewinnen. Wenn der Zustand $|\varphi\rangle$ vorher unbekannt ist, taucht er als unbekannter Zustand am System S^B wieder auf. Die Relativitätstheorie ist nicht verletzt, da eine klassische Informationsübermittlung verwendet wurde. Der Zustand der Teilsysteme S^C und S^A bei Alice ist am Ende der Übertragung der vollständig gemischte Zustand $\frac{1}{4}\mathbb{1}^{AB}$.

11.4 Verschränkungs austausch

Wir haben die Produktion verschränkter Qubit-Paare in Abschn. 8.3 beschrieben. Tatsächlich ist es für die Verschränkung von zwei Qubits nicht nötig, dass der Zustand in einem einzigen Gesamtprozess mit Hilfe unitärer Dynamik erzeugt wird. Durch *Verschränkungs austausch* (entanglement swapping) können zwei Quantensysteme an getrennten Orten ohne Wechselwirkung untereinander in einen vom Rest isolierten verschränkten Gesamtzustand versetzt werden. Wir diskutieren ein Beispiel.

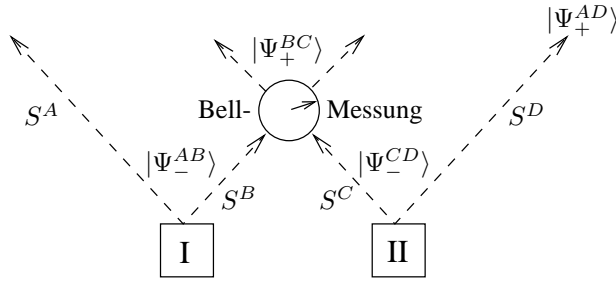


Abbildung 11.2: Austausch von Verschränkung von den Systemen S^{AB} und S^{CD} auf die Systeme S^{AD} und S^{BC} .

Zwei EPR-Quellen I und II erzeugen simultan jeweils ein 2-Teile-System S^{AB} und S^{CD} im Bell-Zustand $|\Psi_-^{AB}\rangle$ bzw. $|\Psi_-^{CD}\rangle$ (siehe Abb. 11.2. Insgesamt liegt daher der Produktzustand

$$|\Psi_-^{AB}\rangle|\Psi_-^{CD}\rangle = \frac{1}{2} (|0^A, 1^B\rangle - |1^A, 0^B\rangle) (|0^C, 1^D\rangle - |1^C, 0^D\rangle) \quad (11.4)$$

aus $\mathcal{H}_2^A \otimes \mathcal{H}_2^B \otimes \mathcal{H}_2^C \otimes \mathcal{H}_2^D$ vor. Wir führen in den Räumen $\mathcal{H}_2^A \otimes \mathcal{H}_2^D$ und $\mathcal{H}_2^B \otimes \mathcal{H}_2^C$ Bell-Basen ein. Dann können wir den Zustand umschreiben:

$$|\Psi_-^{AB}\rangle|\Psi_-^{CD}\rangle = \frac{1}{2} (|\Psi_+^{AD}\rangle|\Psi_+^{BC}\rangle - |\Psi_-^{AD}\rangle|\Psi_-^{BC}\rangle - |\Phi_+^{AD}\rangle|\Phi_+^{BC}\rangle + |\Phi_-^{AD}\rangle|\Phi_-^{BC}\rangle) \quad (11.5)$$

Man sieht unmittelbar, dass eine Bell-Messung an den Teilsystemen S^B und S^C die vorher unverschränkten Teilsysteme S^A und S^D in einen Bell-Zustand überführen. Projektion z. B. auf $|\Psi_+^{BC}\rangle$ erzeugt $|\Psi_+^{AD}\rangle$. Die Bell-Zustände der verschränkten Untersysteme S^{AD} und S^{BC} stimmen jeweils überein. Bei diesem Prozess handelt es sich nicht um die Teleportation vom Zuständen, sondern eher um die *Übertragung von Verschränkung*.

11.5 Ergänzende Themen und weitere Literatur

- Weiterführende Literatur zur Abwehr von Lauschangriffen: [GRT 02], [Lom 02a], [Lom 02a], [Gru 99], [HN 99].
- Protokolle mit mehr als zwei Zuständen: [GRT 02], [Lom 02a].
- B92-Protokoll: [HAD 95], [Lom 02a], [Gru 99].
- Experimentelle Quantenkryptographie: [HAD 95], [EGH 00], [HN 99], [Zbi 98], [BD 00], [GM 02], [GRT 02].
- BBM92: [BBM 92], [GM 02, S. 369].

- Übersicht: [Wer 01].
- Experimente zum dichten Kodieren: [BHL 02], [BEZ 00, S. 62], [BD 00].
- Teleportation von höherdimensionalen Zuständen und Gemischen [Wer 01, S. 53], [Key 02, S. 474], [vLo 02, 1232].
- Experimente zur Teleportation: [BHL 02], [BD 00], [BEZ 00], [GM 02, S. 363].

11.6 Übungsaufgaben

ÜA 11.1 Fälschungssichere Banknoten.

Nehmen Sie an, dass es technisch möglich ist, auf einer Banknote Photonen in einzelnen Zellen über längere Zeit zu speichern. Wie kann man so fälschungssichere Banknoten drucken?

ÜA 11.2 [zu 11.3] Was ändert sich an den Überlagerungen in Abschn. 11.3, wenn der Zustand $|\Psi_{-}^{AB}\rangle = \frac{1}{\sqrt{2}}(|0, 1\rangle - |1, 0\rangle)$ statt $|\Phi_{+}^{AB}\rangle$ verwendet wird?

ÜA 11.3 [zu 11.1] Nehmen Sie an, dass der Lauscher an den beiden Photonen (Spin- $\frac{1}{2}$ -Teilchen) jeweils eine Polarisationsmessung durchführt und die Photonen anschließend an Alice bzw. Bob weiterlaufen lässt. Der Lauscher präpariert also mit einer Wahrscheinlichkeit $p(\theta^A, \theta^B)$ Photonenpaare mit Photonen in den Zuständen $|\theta^A\rangle$ und $|\theta^B\rangle$. Die beiden Polarisationsrichtungen werden durch die Winkel θ^A und θ^B beschrieben. Bestimmen Sie explizit die Korrelationskoeffizienten und zeigen Sie, dass $|S| \leq \sqrt{2}$ gilt. Alice und Bob würden daher diesen Eingriff feststellen können.

ÜA 11.4 [Zu 11.3] In vorangegangenen Kapiteln wurde der Begriff des Quantenzustands näher präzisiert. Prüfen Sie, ob in diesem Sinne in Abschn. 11.3 von der Teleportation eines Quantenzustands gesprochen werden kann.

12 Quantencomputer

Wir wollen in diesem Kapitel zeigen, wie man mit Quantensystemen Rechnungen durchführen kann und worin sich die Durchführung von denen mit einem klassischen Computer unterscheiden. Dabei soll deutlich gemacht werden, bei welchen Fragestellungen Quantencomputer überlegen sind. Eine solche Überlegenheit wird auf die typischen nicht-klassischen Strukturen der Quantentheorie wie Superposition und Verschränkung zurückgehen.

12.1 Register und Netzwerke

Register Eine Reihe von n Qubit-Systemen stellt ein *Quantenregister* (quantum register) dar. Der Zustand dieses zusammengesetzten Systems wird durch einen Vektor $|\psi^{\text{in}}\rangle$ im Hilbert-Raum $\mathcal{H}_2^{(n)} = \mathcal{H}_2 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_2$ mit n Faktorräumen \mathcal{H}_2 beschrieben. Wir arbeiten in allen Hilbert-Räumen in der Rechenbasis $\{|0\rangle, |1\rangle\}$. In den Registern wird die Information in binärer Form gespeichert. Der natürlichen Zahl a wird der Registerzustand

$$|a\rangle = |a_{n-1}\rangle |a_{n-2}\rangle \cdots |a_0\rangle \quad , a_i \in \{0, 1\} \quad (12.1)$$

aus $\mathcal{H}_2^{(n)}$ zugeordnet. Wir beziehen uns dabei auf die binäre Schreibweise von a

$$a = a_{n-1}2^{n-1} + a_{n-2}2^{n-2} + \cdots + a_02^0 \leftrightarrow (a_{n-1}, a_{n-2}, \dots, a_0) . \quad (12.2)$$

Es gibt $d := 2^n$ Zustände dieser Art. Sie bilden die Rechenbasis von $\mathcal{H}_2^{(n)}$. Die natürlichen Zahlen $a = 0$ bis $a = d - 1$ nummerieren die Basiszustände durch. Mit $a \in \{0, 1\}^n$ kennzeichnet man, dass der Zustand $|a\rangle$ ein Element der Rechenbasis zu einem Register der Länge n ist. Zum Beispiel ist $6 \in \{0, 1\}^3$ und der zugehörige Zustand hat die Form $|6\rangle = |1, 1, 0\rangle$.

Es ist eine wichtige Eigenschaft eines Quantenregisters, dass in ihm durch Superposition mehrere Zahlen gleichzeitig in orthogonalen und damit unterscheidbaren Zuständen gespeichert werden können. Ein Beispiel ist

$$\frac{1}{\sqrt{2}} (|0, 1, 1\rangle + |1, 1, 1\rangle) = \frac{1}{\sqrt{2}} (|3\rangle + |7\rangle) . \quad (12.3)$$

Der allgemeine Zustand eines Registers der Länge n ist

$$|\psi\rangle = \sum_{a=0}^{d-1} c_a |a\rangle , \quad \sum_a |c_a|^2 = 1 . \quad (12.4)$$

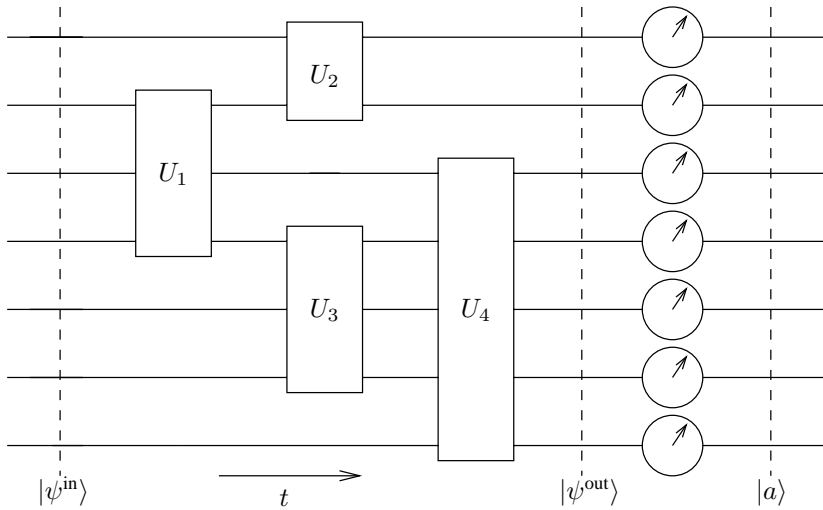


Abbildung 12.1: Schema eines Quantennetzwerks mit Bit-für-Bit-Messung.

Die Anzahl d der zugleich speicherbaren Basiszustände wächst exponentiell mit der Registerlänge n an. Für $n = 200$ ist ihre Zahl bereits größer als die geschätzte Zahl der Atome im Universum. In dieser Speicher- und Verarbeitungskapazität liegt eine der Stärken des Quantencomputers.

Bei ungeschicktem Vorgehen kann diese Stärke allerdings durch die Eigenart der Quantenmessung wieder kompensiert werden. Zu beachten ist, dass Messungen in der Rechenbasis am auslaufenden Zustand $|\psi^{\text{out}}\rangle$, die nacheinander oder simultan an den Registerstellen durchgeführt werden, immer in einen der beteiligten Basiszustände überführen. Sie erlauben es nur, eine einzige Zahl a auszulesen. Bei der Messung am Zustand (12.3) ist das die Zahl 3 oder 7. Solche Messungen in der Rechenbasis heißen *Bit-für-Bit-Messungen* (bit by bit measurements). Eine nachfolgende Messung am resultierenden Zustand ergibt keine weitere Information.

Netzwerke Die Manipulationen der Registerzustände durch den Quantencomputer erfolgt mit Hilfe von unitären Transformationen auf $\mathcal{H}_2^{(n)}$. Ein *Quantengatter* (quantum gate) führt eine wohlbestimmte unitäre Transformation durch, die meist eine Analogie zu einem logischen Gatter der klassischen Computer hat. Ein *Quantennetzwerk* (quantum network) oder eine *Quantenschaltung* (quantum circuit) besteht aus mehreren Quantengattern, die in zeitlich geordneter Weise gleichzeitig oder nacheinander auf den Zustand einwirken (vergl. Abb. 12.1). Die Gatter sind dabei durch *Quantendrähte* (quantum wires) verbunden, die einen der Teilräume \mathcal{H}_2 von $\mathcal{H}_2^{(n)}$ und damit einem der Quantensysteme zugeordnet sind. Ideale Drähte beeinflussen den Zustand nicht. Reale Drähte sind zumeist Quellen für Fehler. Wir haben bereits in Kap. 3 und 7 solche Gatter und Netzwerke kennen gelernt.

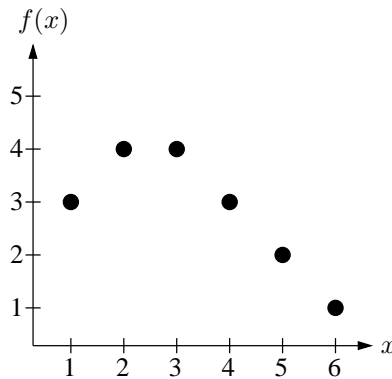


Abbildung 12.2: Nicht eindeutig umkehrbare Funktion.

Ein *Quantencomputer* (quantum computer) ist ein Quantennetzwerk, das eine *Quantenberechnung* (quantum computation) durchführt, indem er den Eingangszustand $|\psi^{\text{in}}\rangle$ in unitärer Weise in einen Ausgangszustand $|\psi^{\text{out}}\rangle$ überführt. Messungen werden in der Regel projektiv und Bit-für-Bit an einigen oder allen Qubits (Registerstellen) des Ausgangszustands durchgeführt. Im ganz allgemeinen Fall kann auch die unitäre Entwicklung durch Messungen in einem oder mehreren Faktorräumen \mathcal{H}_2 unterbrochen werden.

Für die experimentelle Realisierung von Quantennetzwerken ist es wichtig, dass auf einzelnen Faktorräumen oder auf Produkten von Faktorräumen getrennt (lokal) wohlbestimmte unitäre Transformationen in kontrollierter Weise induziert werden können. Diese unitären Transformationen der Teilsysteme durch die Quantengatter entstehen durch einen äußeren Eingriff auf die Qubit-Systeme oder durch Wechselwirkung mit Nachbarqubits. Sie stellen eine der Herausforderungen beim Bau von Quantencomputern dar.

12.2 Funktionsberechnung und Quantenparallelismus

Zur Berechnung einer *Booleschen Funktion* (boolean function) $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ mit Hilfe des Quantencomputers wird ein Register der Länge n benötigt, in dem im Anfangszustand $|\psi^{\text{in}}\rangle$ eingegeben wird, und ein zweites Register der Länge m , in dem im Ausgangszustand der Funktionswert $f(x)$ gespeichert wird. Beide Register haben endliche Längen. Die Rechnung wird daher nach den Regeln der *modularen Arithmetik* (modular arithmetic) durchgeführt. Sie beschreibt das Rechnen mit *Resten* (remainder). Unter $a \bmod n$ versteht man den Rest, der bei der Division der natürlichen Zahl a durch die natürliche Zahl n entsteht¹. Es gilt daher $a = qn + r$ mit $q \in \mathbb{N}$. Gleichungen, die auf der rechten Seite durch $(\bmod n)$ gekennzeichnet werden, beschreiben die Gleichheit der Reste (z. B. $1 = 9 = 25 \pmod{n}$).

¹Ganze Zahlen (integers) \mathbb{Z} : $\{\dots, -2, -1, 0, +1, +2, \dots\}$. Natürliche Zahlen (natural numbers) \mathbb{N} : $\{0, 1, 2, \dots\}$. Sie werden auch positive ganze Zahlen (positive integers) oder nicht-negative ganze Zahlen (non-negative integers) genannt.

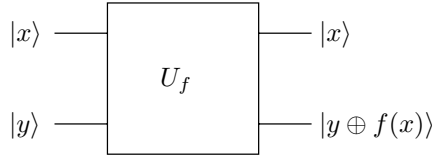


Abbildung 12.3: Funktionsberechnung als unitäre Transformation.

Wir werden beim Rechnen mit Resten in erster Linie die Addition benötigen. Für sie gilt

$$(a + b) \bmod n = (a \bmod n) \pm (b \bmod n) \pmod{n}. \quad (12.5)$$

Man lässt bei der Addition häufig den Zusatz $\bmod n$ weg und schreibt

$$(a + b) \bmod n =: a \oplus b. \quad (12.6)$$

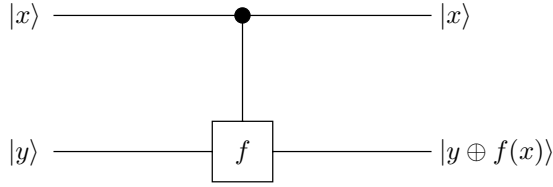
Quantencomputer basieren auf unitären und daher umkehrbaren Zustandsentwicklungen. Funktionen f , die keine ein-eindeutige Abbildung darstellen (für die also $f(x) = f(y)$ für Argumente $x \neq y$ gilt) können nicht direkt durch unitäre Operationen berechnet werden (vergl. Abb. 12.2). Dieses Problem wird dadurch gelöst, dass man das Argument x in einem ersten Register unverändert mitführt. Daher besteht die Notwendigkeit von zwei Registern, einem ersten Register (x -Register) der Länge n und einem zweiten Register (y -Register) der Länge m . Die unitäre Transformation zur Bestimmung von $f(x)$ wirkt dann auf einen Zustand aus $\mathcal{H}_2^{(n)} \otimes \mathcal{H}_2^{(m)}$ in folgender Weise:

$$|x, y\rangle \xrightarrow{U_f} |x, (y + f(x)) \bmod 2^n\rangle = |x, y \oplus f(x)\rangle. \quad (12.7)$$

Schematisch ist das in Abb. 12.3 dargestellt. U_f ist eine kontrollierte Operation, da das was mit dem Inhalt des zweiten Registers durchgeführt wird, vom Inhalt des ersten Registers abhängt. Das CNOT-Gatter, das wir in Abschn. 7.4 beschrieben haben, ist ein Spezialfall mit $m = n = 1$ und $f(x) = x$. Die graphische Darstellungsweise wird von dort übertragen. U_f von Gl. (12.7) wird durch das Schaltbild von Abb. 12.4 wiedergegeben.

Wir geben ein Beispiel zur Veranschaulichung von Gl. (12.7) an. Die Quantenregister sollen die Länge $n = 2$ und $m = 3$ haben. Die Boolesche Funktion f ist dann von der Form $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$. Wir betrachten speziell die Berechnung von $f(x) = x^2$

$$|x, 0\rangle \xrightarrow{U_f} |x, x^2 \bmod 2^3\rangle. \quad (12.8)$$

**Abbildung 12.4:** Funktionsberechnung als kontrollierte Operation.

Die unitäre Transformation U_f muß dann Folgendes leisten:

$$\begin{aligned}
 |0, 0\rangle|0, 0, 0\rangle &\rightarrow |0, 0\rangle|0, 0, 0\rangle \\
 |0, 1\rangle|0, 0, 0\rangle &\rightarrow |0, 1\rangle|0, 0, 1\rangle \\
 |1, 0\rangle|0, 0, 0\rangle &\rightarrow |1, 0\rangle|1, 0, 0\rangle \\
 |1, 1\rangle|0, 0, 0\rangle &\rightarrow |1, 1\rangle|0, 0, 1\rangle .
 \end{aligned} \tag{12.9}$$

Wir haben dabei $9 \bmod 2^3 = 1$ verwendet.

Bleibt noch die Frage zu beantworten, ob eine solche unitäre Transformation U_f immer mit Hilfe von Gattern implementiert werden kann. Es lässt sich zeigen, dass für jede Boolesche Funktion $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ das Quantennetzwerk, das die Transformation U_f und damit die Berechnung einer jeden Funktion f auf dem Quantencomputer bewirkt, allein aus Toffoli-Gattern aufgebaut werden kann. Damit ist zugleich die Unitarität von U_f gewährleistet. Das Toffoli-Gatter ist in diesem Sinn ein universelles reversibles Gatter. Für den Beweis verweisen wir auf die Literatur (vergl. Abschn. 8.6).

Unitarität Wir wollen einen einfachen Spezialfall von Gl. (12.7) untersuchen und zeigen, dass für jede Funktion $f : \{0, 1\} \rightarrow \{0, 1\}$ die Transformation U_f eine unitäre Transformation auf $\mathcal{H}_2 \otimes \mathcal{H}_2$ ist. Sie kann daher durch eine Kombination einfacher Quantengatter implementiert werden. Wir haben

$$U_f U_f |x, y\rangle = U_f |x, y \oplus f(x)\rangle = |x, y \oplus f(x) \oplus f(x)\rangle = |x, y\rangle \tag{12.10}$$

und damit $U_f U_f = \mathbb{1}$.

Zu zeigen ist noch, dass $U_f^\dagger = U_f$ gilt. Es gibt vier Funktionen f_i :

$$\begin{aligned}
 f_1(0) &= 0 & , & & f_1(1) &= 0 \\
 f_2(0) &= 1 & , & & f_2(1) &= 1 \\
 f_3(0) &= 0 & , & & f_3(1) &= 1 \\
 f_4(0) &= 1 & , & & f_4(1) &= 0 .
 \end{aligned} \tag{12.11}$$

Wir untersuchen die mit Bezug auf die Rechenbasis gebildete Matrix U_f . Für f_1 haben wir $U_f |x, y\rangle = U_f |x, y \oplus 0\rangle = |x, y\rangle$ und damit $U_f = \mathbb{1} = U_f^\dagger$. Für f_2 gilt $U_f |0, 0\rangle = |0, 0\rangle$, $U_f |0, 1\rangle = |0, 1\rangle$, $U_f |1, 0\rangle = |1, 1\rangle$ und $U_f |1, 1\rangle = |1, 0\rangle$. Für die Matrixdarstellung von U_f

können wir daraus

$$U_f = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = U_f^\dagger \quad (12.12)$$

ablesen. Die Unitarität von U_f für f_3 und f_4 zeigt man in analoger Weise.

Kick-back Wir betrachten eine Funktion $f : \{0, 1\}^n \rightarrow \{0, 1\}$, d. h. den Fall $m = 1$, und stellen im zweiten Register im Anfangszustand die Superposition $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ her. Die Wirkung von U_f besteht dann in

$$\begin{aligned} |x\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) &\xrightarrow{U_f} |x\rangle \frac{1}{\sqrt{2}} (|f(x)\rangle - |1 \oplus f(x)\rangle) \\ &= |x\rangle (-1)^{f(x)} \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) . \end{aligned} \quad (12.13)$$

Basisvektoren $|x\rangle$, für die $f(x) = 1$ gilt, werden mit -1 multipliziert. Das Argument x kontrolliert daher einen Vorzeichenflip. Obwohl die Funktionsberechnung und die Addition im zweiten Register erfolgt, bleibt der Zustand im zweiten Register unverändert $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ und nur im ersten Register treten abhängig von $f(x)$ Vorzeichenänderungen auf. Man nennt diesen Vorgang, den wir noch mehrfach nutzen werden, einen *Kick-back* (kick back).

12.3 Quantenparallelismus

Durch parallele Anwendung von Hadamard-Gattern auf den Registerzustand $|0, 0, \dots, 0\rangle$ des ersten Registers der Länge n

$$\begin{aligned} |\Omega\rangle &= H \otimes H \otimes \dots \otimes H |0, 0, \dots, 0\rangle \\ &= \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \dots \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \\ &= \frac{1}{\sqrt{d}} \sum_{x=0}^{d-1} |x\rangle \end{aligned} \quad (12.14)$$

($d := 2^n$) entsteht eine gleichgewichtete Superposition der d Basisvektoren von $\mathcal{H}_2^{(n)}$. Wir können den Zustand $|\Omega\rangle$ als die „Superposition“ der Zahlen $0 \leq x \leq d$ auffassen. Wenn wir das zweite Register der Länge m mit Zustand $|0\rangle$ hinzufügen und die unitäre Transformation

wirken lassen, überführt sie in den Zustand

$$\begin{aligned}
 |\psi\rangle &= U_f \left(\frac{1}{\sqrt{d}} \sum_{x=0}^{d-1} |x, 0\rangle \right) \\
 &= \frac{1}{\sqrt{d}} \sum_{x=0}^{d-1} U_f(|x, 0\rangle) \\
 &= \frac{1}{\sqrt{d}} \sum_{x=0}^{d-1} |x, f(x) \bmod n\rangle.
 \end{aligned} \tag{12.15}$$

Als Folge der Linearität von U_f und der Superposition (12.14) im Zustand $|\Omega\rangle$ im ersten Register wird nach einmaligem Durchlaufen des Netzwerks simultan der Wert $f(x)$ für $d = 2^n$ Argumente berechnet. Diese Parallelverarbeitung von Information wird als *Quantenparallelismus* (quantum parallelism) bezeichnet. d steigt mit der Registerlänge n exponentiell an. Abgesehen von Trivialfällen ist der resultierende Zustand $|\psi\rangle$ verschränkt.

Wenn wir bei dem Zustand $|\psi\rangle$ von Gl. (12.15) die ersten n Qubits (d. h. das x -Register) mit Bezug auf die Standardbasis ausmessen, erhalten wir mit einheitlicher Wahrscheinlichkeit $\frac{1}{d}$ einen der Zustände $|x\rangle$. Wenn z. B. $|x_0\rangle$ gemessen wird, wird der Gesamtzustand in $|x_0, f(x_0)\rangle$ überführt. Eine Messung am zweiten Register liefert $f(x_0)$. Aussagen über andere x -Werte können nicht mehr gewonnen werden. Bei dieser Berechnung von $f(x)$ Argument nach Argument ist der Quantencomputer schlechter als der klassische Computer, da beim klassischen Computer der Wert x_0 nach Belieben vorgegeben werden kann. Beim Quantencomputer ist x_0 ein Zufallsergebnis. Die Überlegenheit der Quantencomputer wird sich bei anderen Fragestellungen zeigen.

Quantenalgorithmen Die Überlegenheit von *Quantenalgorithmen* (quantum algorithms) gegenüber klassischen Algorithmen beruht in erster Linie auf der Ausnutzung von Superposition und Verschränkung für ganz spezifische Fragestellungen. In erster Linie werden die folgenden beiden Techniken verfolgt:

- (i) Aufsuchen von globalen Eigenschaften einer Funktion $f(x)$, wie z. B. der Periode. Hierzu werden nicht wie beim klassischen Computer zunächst Funktionswerte berechnet und anschließend miteinander verglichen, sondern direkt Korrelationen zwischen den Zuständen des Ausgangsregisters untersucht. Wir werden das beim Deutsch-Problem, beim Deutsch-Jozsa-Problem und beim Shor-Algorithmus kennenlernen.
- (ii) *Amplitudenverstärkung* (amplitude amplification) in zumeist iterativer Weise. Dabei wird die Superposition so transformiert, dass der Zustand mit dem gesuchten Resultat eine besonders große Amplitude erhält und daher mit großer Wahrscheinlichkeit gemessen wird. Als ein Beispiel hierfür behandeln wir den Grover-Algorithmus.

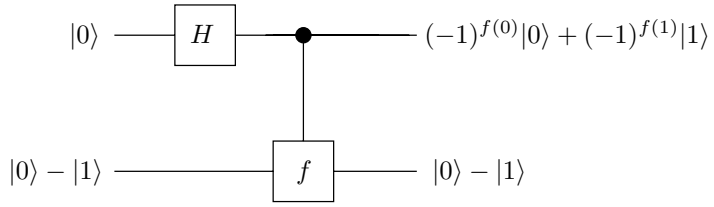


Abbildung 12.5: Erzeugung eines Kick-back im ersten Register.

12.4 Zwei einfache Quantenalgorithmen

12.4.1 Deutsch-Problem

Wir diskutieren die Situation, dass eine Funktion $f : \{0, 1\} \rightarrow \{0, 1\}$ als *Blackbox* (black box) bzw. als *Orakel* (oracle) gegeben ist. Die Blackbox kann den Funktionswert $f(x)$ zu jedem eingegebenen Argument x berechnen, liefert aber keine darüber hinaus gehende Informationen über $f(x)$. Man kann wie bei einem Orakel eine *Anfrage* (query) stellen und erhält jeweils eine Antwort. Die Aufgabe besteht darin, bestimmte Eigenschaften von $f(x)$ mit einer minimalen Zahl von Anfragen zu bestimmen. Wir vergleichen dabei eine klassische Blackbox mit einer quantentheoretischen Blackbox, in der $f(x)$ als Quantenalgorithmus implementiert ist.

Es gibt vier Funktionen $f(x)$, die in Gl. (12.11) aufgelistet sind. Die Funktionen $f_1(x)$ und $f_2(x)$ heißen konstant. Die Funktionen $f_3(x)$ und $f_4(x)$ heißen ausgeglichen, da gleich viele Werte 0 und 1 angenommen werden. Beides sind globale Eigenschaften der Funktionen. Es soll festgestellt werden, ob die Funktion $f(x)$ der Blackbox konstant oder ausgeglichen ist. Hierzu muß im klassischen Fall die Berechnung mit den Werten $x = 0$ und $x = 1$ laufen. Das Orakel muss also zweimal befragt werden.

Beim Quantencomputer verwenden wir den Deutsch-Algorithmus² und fragen nicht „Welcher Funktionswert?“ sondern „Welche Funktion?“. Wir nutzen den Kick-back von Gl. (12.13) aus und verwenden im x -Register den Zustand $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Das kann man erreichen, indem man dort $|0\rangle$ einlaufen lässt und eine Hadamard-Transformation anschließt (vergl. Abb. 12.5). Nach der Anwendung von U_f gemäß Gl. (12.13) liegt der Gesamtzustand

$$\frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \xrightarrow{U_f} \frac{1}{2} \left[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle \right] (|0\rangle - |1\rangle) \quad (12.16)$$

vor. Das zweite Register wird nicht mehr betrachtet. Wenn $f(x)$ konstant ist, enthält das erste Register den Zustand

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \Leftrightarrow \text{konstant} . \quad (12.17)$$

Im ausgeglichenen Fall liegt der Zustand

$$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \Leftrightarrow \text{ausgeglichen} \quad (12.18)$$

²D. Deutsch, 1985, [Deu85].

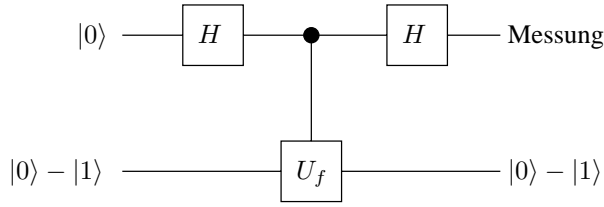


Abbildung 12.6: Quantenschaltung für den Deutsch-Algorithmus.

vor. Zur Ausmessung führen wir wie in Abb. 12.6 eine zweite Hadamard-Transformation H durch, die auf

$$|0\rangle \Leftrightarrow \text{konstant}, \quad |1\rangle \Leftrightarrow \text{ausgeglichen} \quad (12.19)$$

führt. Eine einzige Messung in der Rechenbasis liefert dann bereits mit Sicherheit die gewünschte Antwort.

12.4.2 Deutsch-Jozsa-Problem

Es werden Funktionen $f : \{0, 1\}^n \rightarrow \{0, 1\}$ betrachtet, die auf $d = 2^n$ Werten für x erklärt sind. $f(x)$ soll entweder konstant oder ausgeglichen sein. Ausgeglichen bedeutet, dass die Hälfte aller Funktionswerte null und die andere Hälfte eins ist. Die Aufgabe besteht wieder darin zu ermitteln, welcher Typ von Funktion in einer Blackbox vorliegt.

Der Quantenalgorithmus von Deutsch und Jozsa³ entsteht durch Erweiterung des Deutsch-Algorithmus. Wir betrachten das in Abb. 12.7 dargestellte Schaltbild. Die Hadamard-Gatter $H^{(n)} = H \otimes H \otimes \dots \otimes H$ haben auf den Zuständen des x -Registers die in Gl. (12.14) beschriebene Wirkung.

$$|0, 0, \dots, 0\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \xrightarrow{H^{(n)}} |\psi\rangle = \frac{1}{\sqrt{d}} \sum_{x=0}^{d-1} |x\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) . \quad (12.20)$$

Nach der simultanen Funktionsberechnung entsteht daraus wie in Gl. (12.13)

$$|\psi\rangle \xrightarrow{U_f} |\psi'\rangle = \frac{1}{\sqrt{d}} \sum_{x=0}^{d-1} (-1)^{f(x)} |x\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) . \quad (12.21)$$

Wir schließen eine weitere Transformation des x -Registers mit Hadamard-Gattern an. Die Wirkung von $H^{(n)} = H \otimes H \otimes \dots \otimes H$ wollen wir an dieser Stellen nicht im Einzelnen ausrechnen. Die folgende Überlegung reicht für unsere Zwecke aus. Die Wirkung des einzelnen Hadamard-Gatters ist $|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$ bzw. $|1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$. Der Zustand $|x\rangle$ des x -Registers ist wie in Gl. (12.2) „binär geschrieben“. Mit $H^{(n)}$ entsteht

$$|x\rangle \xrightarrow{H^{(n)}} \frac{1}{\sqrt{2}} (|0\rangle|0\rangle \dots |0\rangle + \text{Rest}), \quad \text{Rest} \neq |0\rangle|0\rangle \dots |0\rangle . \quad (12.22)$$

³D. Deutsch und R. Jozsa, 1992, [DJ 92].

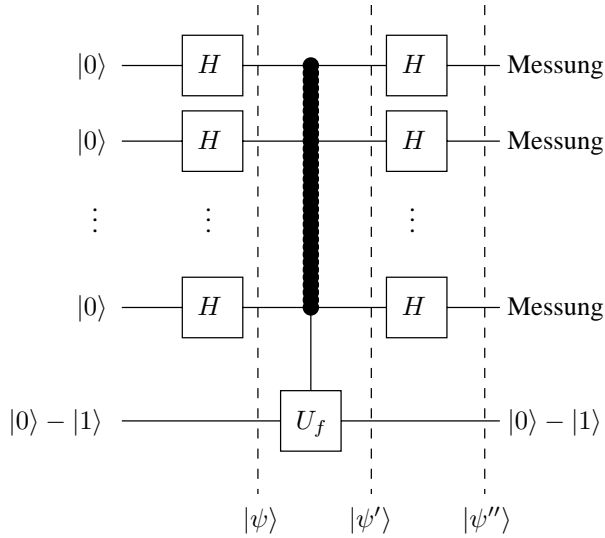


Abbildung 12.7: Quantenschaltung für den Deutsch-Jozsa-Algorithmus.

Als Zustand beider Register erhalten wir daher durch Auswerten von Gl. (12.21)

$$|\psi'\rangle \xrightarrow{H^{(n)}} |\psi''\rangle = \frac{1}{\sqrt{d}} \left(\sum_{x=0}^{d-1} (-1)^{f(x)} \right) \{ |0\rangle|0\rangle \dots |0\rangle + \text{Rest} \} \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) . \quad (12.23)$$

Schließlich messen wir die einzelnen Stellen des x -Registers in der Rechenbasis. Die Wahrscheinlichkeit das Messergebnis $(0, 0, \dots, 0)$ zu erhalten ist

$$p(0, 0, \dots, 0) = \frac{1}{d} \left| \sum_{x=0}^{d-1} (-1)^{f(x)} \right|^2 . \quad (12.24)$$

Daraus folgt

$$\begin{aligned} p(0, 0, \dots, 0) &= 1 \quad \Leftrightarrow \quad f(x) \text{ konstant} \\ p(0, 0, \dots, 0) &= 0 \quad \Leftrightarrow \quad f(x) \text{ ausgeglichen} \end{aligned} \quad (12.25)$$

Wir messen daher nur einmal das x -Register. Wenn dabei das Resultat $0, 0, \dots, 0$ eintritt, ist $f(x)$ konstant. Wenn irgendein anderes Messresultat eintritt, kann $f(x)$ nicht konstant sein, d. h. $f(x)$ muss ausgeglichen sein.

Für beliebige Registerlänge n reicht beim Quantennetzwerk bereits eine Anfrage an das Orakel aus. Beim klassischen Netzwerk fragt man nacheinander den Wert $f(x)$ zu den N möglichen x -Werten ab. Sobald man für zwei Eingaben verschiedene Werte für $f(x)$ erhält, ist die Funktion nicht konstant und also ausgeglichen. Um sicher zu wissen, dass $f(x)$ konstant ist, muss sich derselbe Wert in mehr als der Hälfte aller Fälle, als mindestens in $2^{n-1} + 1$ Fällen, ergeben. Die Zahl der klassisch nötigen Anfragen wächst daher exponentiell mit n an.

12.5 Suchalgorithmus von Grover

Telefonbuchproblem Das *Telefonbuchproblem* (phone book problem) besteht darin, in einem Telefonbuch zu gegebener Telefonnummer (z. B. 7581) den zugehörigen Namen zu finden.

x = Name	Nummer
Müller	4892
Meier	1739
...	...
Schmidt	7581
...	...

Die Verteilung der Nummern soll zufällig sein. Das Telefonbuch ist im Orakel gespeichert. Beim klassischen Algorithmus lautet die Frage „Hat Müller die Nummer 7581?“ Das Orakel antwortet in diesem Fall mit „nein“. So werden die Namen nacheinander abgefragt, bis „Schmidt“ gefunden ist. Die Nutzung des Quantenparallelismus im *Grover-Algorithmus*⁴ (Grover’s algorithm) erlaubt es wieder, alle Fragen gleichzeitig zu stellen. Das Auslesen erfolgt in diesem Fall mit Hilfe von Amplitudenverstärkung (vergl. Abschn. 12.3).

Das Telefonbuch – oder allgemeiner eine nicht strukturierte Datenbank, in der ein Eintrag gesucht werden soll – entspricht einer Funktion $f(x)$, $x = 0, 1, \dots, d-1$ mit den Werten

$$f(x) = 0 \text{ für } x \neq l, \quad f(x) = 1 \text{ für } x = l. \quad (12.26)$$

Das Quantenorakel erlaubt die Berechnung von $f : \{0, 1\}^n \rightarrow \{0, 1\}$ wie in Gl. (12.21) mit $d = 2^n$. Das zweite Register soll wieder aus nur einem Qubit bestehen. Wir lassen dort den Zustand $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ einlaufen und nutzen den Kick-back aus. Der Zustand $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ läuft wieder aus. Wir geben im Folgenden nur die Transformationen des ersten Registers an. Dann wird die Wirkung der quantentheoretischen Funktionsberechnung durch den unitären Operator U_l

$$|x\rangle \xrightarrow{U_l} (-1)^{f(x)} |x\rangle \quad (12.27)$$

beschrieben. U_l flippt den Zustand $|l\rangle$ in $-|l\rangle$ und lässt alle anderen Zustände unverändert. Man kann diesen Operator daher auch in der Form

$$U_l = \mathbb{1} - 2|l\rangle\langle l| \quad (12.28)$$

schreiben.

Wir nutzen wieder den Quantenparallelismus aus. Durch Anwendung des Produkts $H^{(n)} = H \otimes H \otimes H \cdots \otimes H$ erzeugen wir wie in Gl. (12.14) aus den Zustand $|0\rangle|0\rangle \cdots |0\rangle$ die gleichgewichtete Superposition aller Zustände der Rechenbasis von $H_2^{(n)}$

$$|\Omega\rangle = \frac{1}{\sqrt{d}} \sum_{x=0}^{d-1} |x\rangle. \quad (12.29)$$

⁴L.K. Grover, 1996 [Gro 96].

Der unitäre Operator

$$U_S := 2|\Omega\rangle\langle\Omega| - \mathbb{1} \quad (12.30)$$

bewirkt eine „Spiegelung“ an $|\Omega\rangle$. Er erhält $|\Omega\rangle$ und flippt das Vorzeichen von jedem Vektor orthogonal zu $|\Omega\rangle$. Mit Gl. (12.14) lässt sich U_S mit Hadamard-Transformationen in der Form

$$U_S = H^{(n)}(2|0\rangle\langle 0| - \mathbb{1})H^{(n)} \quad (12.31)$$

mit $|0\rangle = |0, 0, \dots, 0\rangle$ schreiben.

Wir wollen die Wirkung der Spiegelung auf einen allgemeinen Zustand

$$|\psi\rangle = \sum_x a_x |x\rangle, \quad a_x \in \mathbb{R} \quad (12.32)$$

angeben. Die Projektion auf $|\Omega\rangle$ führt auf

$$\langle\Omega|\psi\rangle = \frac{1}{\sqrt{d}} \sum_x a_x = \sqrt{d} \bar{a} \quad (12.33)$$

mit dem Mittelwert der Amplituden

$$\bar{a} := \frac{1}{d} \sum_x a_x. \quad (12.34)$$

Damit ergibt sich als Resultat der Anwendung von U_S auf $|\psi\rangle$ mit Gl. (12.30) und (12.32)

$$U_S|\psi\rangle = (2|\Omega\rangle\langle\Omega| - \mathbb{1})|\psi\rangle = 2 \left(\sum_x |x\rangle \right) \bar{a} - \sum_x a_x |x\rangle = \sum_x (2\bar{a} - a_x) |x\rangle. \quad (12.35)$$

Die Amplituden a_x von $|\psi\rangle$ werden wie $a_x \rightarrow 2\bar{a} - a_x$ transformiert. Das entspricht einer Spiegelung von a_x am Mittelwert \bar{a} .

Der Algorithmus besteht nun darin, in einem ersten Iterationsschritt $U_S U_l$ auf $|\Omega\rangle$ anzuwenden

$$|\Omega_1\rangle = U_S U_l |\Omega\rangle. \quad (12.36)$$

In Abb. 12.8 sind die Amplituden a_x über x aufgetragen. Für $|\Omega\rangle$ haben sie einheitlich den Wert $\frac{1}{\sqrt{d}}$. Anwendung von U_l flippt a_l in $-a_l$ und lässt die anderen Amplituden unverändert. Der Mittelwert \bar{a} verschiebt sich dabei nach unten. Die nachfolgende Transformation U_S spiegelt die Werte a_x am neuen Mittelwert und bewirkt eine Verstärkung der Amplitude a_l im Zustand $|\Omega_1\rangle$. Dies ist ein erster Durchgang. Auf $|\Omega_1\rangle$ wird dann wieder $U_S U_l$ angewendet usw. Schließlich wird das x -Register Bit-für-Bit ausgemessen. Dann ist die Wahrscheinlichkeit am größten, den Zustand $|l\rangle$ und damit das Messergebnis l in dualer Schreibweise zu finden.

Der Grover-Algorithmus beschreibt eine Situation, in der der Quantencomputer das gewünschte Resultat nicht mit Sicherheit, sondern nur mit großer Wahrscheinlichkeit liefert.

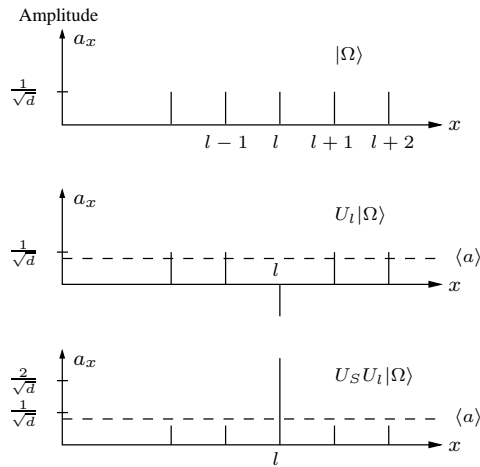


Abbildung 12.8: Amplitudenverstärkung beim Grover-Algorithmus.

Dafür ist er offenbar in Folge des Quantenparallelismus wesentlich schneller als eine wiederholte Befragung des klassischen Orakels.

Eine unitäre Transformation ist eine Rotation im komplexen Raum. Wiederholte Anwendungen können einen Zustand immer näher an einen gewünschten Zustand heranrotieren. Es kann aber auch passieren, dass die Rotation über den gewünschten Zustand hinausgeht und bei Wiederholung der Rotation sich mehr und mehr von ihm entfernt. Es ist daher beim Grover-Algorithmus wichtig zu wissen, wann das Iterationsverfahren abzubrechen ist (vergl. Abschn. 12.8).

Die systematische klassische Durchsuchung der Datenbank benötigt eine Anzahl von Fragen in der Größenordnung 2^n . Sie steigt exponentiell mit n an. Um mit dem Grover-Algorithmus mit großer Wahrscheinlichkeit den richtigen Eintrag zu finden, reichen $\sqrt{2^n}$ Anfragen (vergl. Abschn. 12.8).

12.6 Faktorisierungsalgorithmus von Shor

In schnell wachsendem Umfang beruht die Kommunikation im militärischen und nicht-militärischen Bereich auf einer sicheren Kryptographie für die öffentliche Übertragung von Schlüsseln und Signaturen. Bis heute beruht das Verschlüsselungsverfahren auf der Annahme, dass es keine effektive Faktorisierung großer Zahlen gibt. Der Quantenalgorithmus von Shor⁵ erlaubt eine, verglichen mit klassischen Methoden, sehr viel schnellere Faktorisierung. Wenn sich ein effektiver Quantenprozessor für diesen Algorithmus technisch realisieren lassen ließe, hätte das eine große Auswirkung auf die Sicherheit von geheimer Datenübertragung und Datenspeicherung. Dies ist einer der Gründe für das schnell wachsende Interesse an Quantenalgorithmen und an der Realisierung von Quantencomputern. Wir wollen den

⁵P. Shor, 1994 [Sho 94] und 1997 [Sho 97].

quantentheoretischen Faktorisierungsalgorithmus hier vorstellen. Er besteht aus einem klassischen Algorithmus, der stochastische Elemente (Zufallselemente) enthält, und dem eigentlichen Quantenalgorithmus zum Auffinden der Periode einer Funktion. Wir beginnen mit dem klassischen Teil.

12.6.1 Rückführung von Faktorisierung auf Periodensuche

Der größte gemeinsame Teiler als Hilfsgröße Das Fundamentaltheorem der Arithmetik besagt: Für jede natürliche Zahl $a > 1$ gibt es eine eindeutige *Primfaktorzerlegung* (prime factorization)

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n} \quad (12.37)$$

mit verschiedenen Primzahlen p_1, \dots, p_n und nicht verschwindenden natürlichen Zahlen a_1, \dots, a_n . Unser Ziel ist die Angabe eines schnellen Algorithmus zur Primzahlzerlegung. Wir machen dabei davon Gebrauch, dass es effiziente Methoden zur Bestimmung des *größten gemeinsamen Teilers* $\text{ggT}(a, b)$ (greatest common divisor) von zwei natürlichen Zahlen a und b gibt (vergl. 12.8). $\text{ggT}(a, b)$ ist die größte ganze Zahl, die sowohl Teiler von a wie von b ist.

$$\begin{aligned} 12 : & \text{ Teiler } 1, 2, 3, 4, 6, 12 . \\ 18 : & \text{ Teiler } 1, 2, 3, 6, 9, 18 . \\ \Rightarrow & \text{ ggT}(12, 18) = 6 \end{aligned} \quad (12.38)$$

N sei ungerade und keine Primzahl. Zur Primzahlzerlegung von N ermitteln wir einen nicht-trivialen Teiler von N und wenden das Verfahren sukzessive wieder auf die gefundenen Faktoren von N an. Hierzu reicht es, eine natürliche Zahl b zu finden, die mit N mindestens einen Teiler $\neq 1$ gemeinsam hat, dann haben wir mit $\text{ggT}(b, N)$ insbesondere auch einen Teiler von N gefunden. Eine solche Situation liegt vor, wenn es natürliche *nicht durch N teilbare* Zahlen $c > N$ und $d > N$ gibt, sodass die Gleichung

$$\frac{cd}{N} = m \quad (12.39)$$

für eine natürliche Zahl m erfüllt ist. Dann muss es möglich sein, alle Faktoren der Primzahlzerlegung von N gegen einige oder alle Faktoren von c und d zu kürzen. Es gibt also einen $\text{ggT}(c, N)$ und einen $\text{ggT}(d, N)$. Wir berechnen beide mit dem ggT -Algorithmus und haben damit zugleich Faktoren von N gefunden.

Die Rolle der Periodenbestimmung Wie gewinnen wir zu vorgegebenem N eine solche Relation (12.39)? Hierzu stellen wir eine Vorüberlegung an. a sei eine natürliche Zahl mit $2 \leq a \leq N - 1$. Wir setzen voraus, dass

$$\text{ggT}(a, N) = 1 \quad (12.40)$$

erfüllt ist, sonst wäre bereits ein Teiler von N gefunden, und bilden die Funktion

$$f(x) := a^x \pmod{N} . \quad (12.41)$$

Man kann zeigen (vergl. Abschn. 12.8), dass die Funktion $f(x)$ eine Periode r hat. Darunter verstehen wir die kleinste natürliche Zahl, für die

$$f(x+r) = f(x) \pmod{N} \quad (12.42)$$

gilt. Die Periode r hängt von a ab. Aus

$$a^{x+r} = a^x a^r = a^x \pmod{N} \quad (12.43)$$

folgt der Zusammenhang

$$a^r = 1 \pmod{N}. \quad (12.44)$$

Wir machen ein einfaches Beispiel und berechnen modular

$$(x, f(x) = 2^x \pmod{3}) : (1, 2), (2, 1), (3, 2), (4, 1), \dots \quad (12.45)$$

Die Periode ist $r = 2$ und es gilt

$$a^r = 2^2 = 1 \pmod{3}. \quad (12.46)$$

Nehmen wir an, zu gegebenem a sei die Periode r in einem geeigneten Verfahren bereits bestimmt worden. Und nehmen wir weiter an, dass die folgenden beiden Bedingungen erfüllt sind:

$$r \text{ ist gerade,} \quad (12.47)$$

$$a^{\frac{r}{2}} + 1 \not\equiv 0 \pmod{N}. \quad (12.48)$$

Dann können wir wegen Bedingung (12.47) die Gl. (12.44) umformen

$$a^r - 1 = (a^{\frac{r}{2}} + 1)(a^{\frac{r}{2}} - 1) = 0 \pmod{N}. \quad (12.49)$$

Die linke Seite der Gl. (12.49) muss ein Vielfaches von N sein. Es gibt daher eine natürliche Zahl $m > 0$, sodass wir

$$\frac{(a^{\frac{r}{2}} + 1)(a^{\frac{r}{2}} - 1)}{N} = m \quad (12.50)$$

schreiben können.

Gleichung (12.48) besagt, dass $a^{\frac{r}{2}} + 1$ kein Vielfaches von N ist. Da r die kleinste Zahl mit der Eigenschaft (12.42) ist, muss weiterhin

$$a^{\frac{r}{2}} - 1 \not\equiv 0 \pmod{N} \quad (12.51)$$

gelten, denn sonst wäre wegen Gl. (12.44) bereits $\frac{r}{2}$ die Periode. Daher ist auch $a^{\frac{r}{2}} - 1$ kein Vielfaches von N . Andererseits besagt Gl. (12.50), dass wir auf ihrer linken Seite nach einer Primzahlzerlegung alle Faktoren von N gegen Faktoren im Zähler wegkürzen können. Das Kürzen muss dabei in $(a^{\frac{r}{2}} + 1)$ und in $(a^{\frac{r}{2}} - 1)$ erfolgen, denn sonst wäre einer dieser Terme

ein Vielfaches von N und im Widerspruch zu Gl. (12.48) und (12.51). Beide Terme haben daher mit N gemeinsame Teiler. Darunter gibt es jeweils GröÙte mit

$$\text{ggT}(a^{\frac{r}{2}} + 1, N) \neq \binom{N}{1}, \quad \text{ggT}(a^{\frac{r}{2}} - 1, N) \neq \binom{N}{1}. \quad (12.52)$$

Diese Existenzaussage ist unser Ergebnis. Wenn wir schließlich den Algorithmus zur ggT-Bestimmung anwenden, haben wir einen oder zwei Faktoren von N gewonnen.

Wir sind nur dann erfolgreich, wenn wir zu vorgegebenem N ein a finden, sodass die Bedingungen (12.47) und (12.48) erfüllt sind. Die Suche erfolgt, indem Zufallswerte für a eingegeben werden und so lange der Algorithmus immer wieder durchlaufen wird, bis sich ein a findet, das die Bedingungen erfüllt. Es handelt sich daher um einen *Zufallsalgorithmus* (randomized algorithm). Die gewonnenen Faktoren von N werden in gleicher Weise weiter bearbeitet, bis die Faktorzerlegung erreicht ist.

Flussdiagramm Das oben beschriebene Schema des Faktorisierungsalgorithmus ist in Abb. 12.9 dargestellt. Nur für den doppelt gerahmten Teil der Periodensuche wird ein Quantenalgorithmus eingesetzt.

Das Beispiel $N = 15$ Die Zahl 15 ist die kleinste ungerade Zahl, die keine Primzahl ist. 15 ist daher die kleinste Zahl, die mit der beschriebenen Methode faktorisiert werden kann. Mit $N = 15$ haben wir $2 \leq a \leq 14$. Da Gl. (12.40) zu erfüllen ist, gibt es für die Wahl von a die folgenden Möglichkeiten:

$$a \in \{2, 4, 7, 8, 11, 13, 14\}. \quad (12.53)$$

Wir wählen z. B. $a = 11$ und suchen die Periode r von $f(x)$ von Gl. (12.41).

$$\begin{aligned} x = 0 & : 11^0 = 1 \pmod{15} \\ x = 1 & : 11^1 = 11 \pmod{15} \\ x = 2 & : 11^2 = 121 = 8 \cdot 15 + 1 = 1 \pmod{15} \\ x = 3 & : 11^3 = 1331 = 88 \cdot 15 + 11 = 11 \pmod{15}. \end{aligned} \quad (12.54)$$

Wir haben die Periode $r = 2$ erhalten und damit

$$\text{ggT}(11 + 1, 15) = 3, \quad \text{ggT}(11 - 1, 15) = 5. \quad (12.55)$$

Die Zahlen 3 und 5 sind Teiler von 15. Die Primzahlzerlegung von 15 lautet $15 = 3 \cdot 5$.

Wenn die zufällige Festlegung von a auf $a = 14$ führt, erhalten wir:

$$\begin{aligned} x = 0 & : 14^0 = 1 \pmod{15} \\ x = 1 & : 14^1 = 14 \pmod{15} \\ x = 2 & : 14^2 = 196 = 13 \cdot 15 + 1 = 1 \pmod{15} \\ x = 3 & : 14^3 = 2744 = 182 \cdot 15 + 14 = 14 \pmod{15}. \end{aligned} \quad (12.56)$$

Die Periode ist wieder $r = 2$. Wir bilden

$$\text{ggT}(14 + 1, 15) = 15, \quad \text{ggT}(14 - 1, 15) = 1. \quad (12.57)$$

Damit ist die Bedingung (12.52) verletzt. In Abb. 12.9 (Flussdiagramm) führt die Schleife zurück. Es muss ein neuer Wert für a gewählt werden.

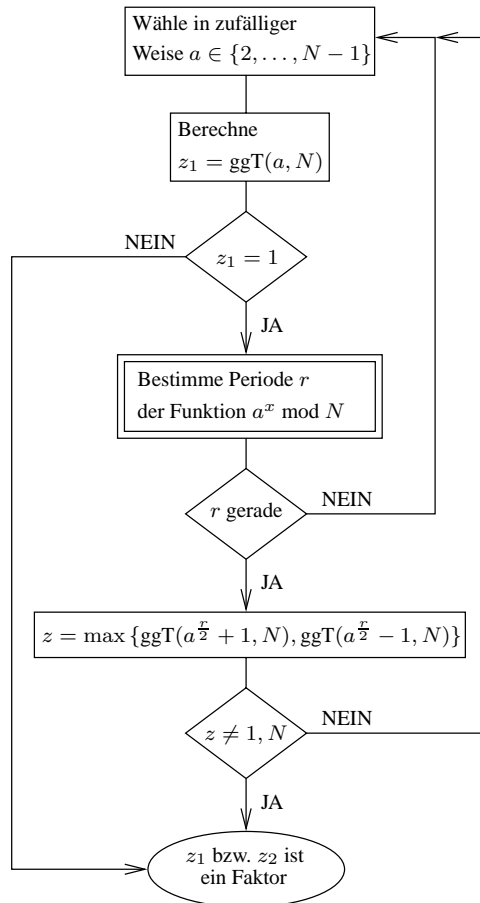


Abbildung 12.9: Schema des Faktorisierungsalgorithmus. Nur der doppelt gerahmte Teil wird auf dem Quantencomputer durchgeführt.

12.6.2 Quantenalgorithmus zur Periodenbestimmung

Die verbliebene Aufgabe besteht in der Bestimmung der Periode der Funktion $f(x) = a^x \pmod{N}$. Wir verwenden wieder zwei Register der Länge n und m . Im ersten Register können die $d = 2^n$ Basisvektoren $|x\rangle$ von $\mathcal{H}_2^{(n)}$ sowie jede Superposition $|\phi\rangle \in \mathcal{H}_2^{(n)}$ eingegeben werden. Im zweiten Register wird $f(x) \pmod{N}$ abgelegt. Die Länge m ist so zu wählen, dass die Dimension $2^m \geq N$ ist. Zustände in diesem Register bezeichnen wir mit $|\chi\rangle \in \mathcal{H}_2^{(m)}$. Ein Gesamtzustand aller Register ist von der Form $|\psi\rangle = |\phi\rangle|\chi\rangle \in \mathcal{H}_2^{(n)} \otimes \mathcal{H}_2^{(m)}$.

1.Schritt: Initialisierung Als Ausgangspunkt für die Nutzung des Quantenparallelismus wird im ersten Schritt der Zustand $|\psi\rangle$ in bekannter Weise in die gleichgewichtige Superposi-

tion der Basiszustände von $\mathcal{H}_2^{(n)}$ gebracht

$$|\psi_1\rangle = \frac{1}{\sqrt{d}} \sum_{x=0}^{d-1} |x\rangle|0\rangle. \quad (12.58)$$

Beispiel $N = 15$:

1. Register: $n=3$ Qubits für die Zahlen 0 bis 7. Damit ist $d = 8$.

2. Register: $m = 4$ Qubits für die Zahlen 0 bis $N = 15$.

Wähle $a = 11$.

$$|\psi_1\rangle = \frac{1}{\sqrt{8}} (|0\rangle + |1\rangle + \dots + |7\rangle) |0\rangle$$

2. Schritt: Berechnung von $f(x)$ im zweiten Register Das Ergebnis der unitären Transformation ist der verschränkte Zustand

$$|\psi_2\rangle = \frac{1}{\sqrt{d}} \sum_{x=0}^{d-1} |x\rangle|a^x\rangle \pmod{N} \quad (12.59)$$

Beispiel $N = 15$:

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{\sqrt{8}} (|0\rangle|1\rangle + |1\rangle|11\rangle + |2\rangle|1\rangle + |3\rangle|11\rangle \\ &\quad + \dots + |7\rangle|11\rangle) \end{aligned} \quad (12.60)$$

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{\sqrt{8}} \{ (|0\rangle + |2\rangle + |4\rangle + |6\rangle) |1\rangle \\ &\quad + (|1\rangle + |3\rangle + |5\rangle + |7\rangle) |11\rangle \} . \end{aligned} \quad (12.61)$$

Periodizität kann man an der Folge der x -Werte ablesen, für die die Funktionswerte sich wiederholen. Die Periode ist eine globale Eigenschaft der Funktion. Sie ist nach einem einzigen Rechenschritt bereits in den Zuständen repräsentiert. In Gl. (12.61) ist nach den Funktionswerten im zweiten Register zusammengefasst worden. Die Periode (hier $r = 2$) ist in den verschiedenen Zuständen des ersten Registers gespeichert, die sich bei der Zusammenfassung ergeben. Die Zerlegungen dieser Zustände nach Basiszuständen können in den Nummern der Basiszustände Verschiebungen um $l \in \mathbb{N}$ gegenüber 0 aufweisen, die auch *Offset* genannt werden. In Gl. (12.61) haben wir als Nummern der Basisvektoren (0, 2, 4, 6) und (1, 3, 5, 7). Der Offset ist $l = 0$ bzw. $l = 1$.

Die Periode ist damit bereits im Prinzip ablesbar. Wir messen in der Rechenbasis des zweiten Registers und überführen dabei das erste Register je nach Offset in den Zustand

$$|\phi'_2(l)\rangle = \sqrt{\left[\frac{r}{q}\right]} \sum_{j=0}^{\left[\frac{q}{r}\right]-1} |l + jr\rangle. \quad (12.62)$$

$\left[\frac{q}{r}\right]$ ist dabei die größte natürliche Zahl kleiner oder gleich $\frac{q}{r}$. Im Beispiel ist $\left[\frac{q}{r}\right] = 4$. Diese Messung wiederholen wir sehr oft und selektieren nach dem Messergebnis (also nach dem Offset l). $|\phi'_2(l)\rangle$ wird dann in der Rechenbasis gemessen. Im Beispiel würde $l = 1$ die Messergebnisse (0, 2, 4, 6) liefern und die Perioden $r = 2$ ist ablesbar. Dies wird allerdings mit wachsendem N immer aufwendiger. Man verwendet daher ein anderes Verfahren.

3. Schritt: Diskrete Fourier-Transformation Ein schnelleres Verfahren besteht darin, mit Hilfe einer Fourier-Transformation den Offset in einen für die quantentheoretische Messung irrelevanten Phasenfaktor zu verschieben. Der unitäre Operator zur diskreten Fourier-Transformation bewirkt

$$U_{DFT}|x\rangle = \frac{1}{\sqrt{d}} \sum_{z=0}^{d-1} \exp\left(2\pi i \frac{xz}{d}\right) |z\rangle \quad (12.63)$$

mit $z \in \mathbb{N}$. Die Zustände im ersten Register sind in (12.62) angegeben. Wir diskutieren zunächst den Spezialfall

$$\frac{d}{r} \in \mathbb{N}. \quad (12.64)$$

Dann ist

$$|\phi_2(l)\rangle = \sqrt{\frac{r}{d}} \sum_{j=0}^{d/r-1} |l + jr\rangle \quad (12.65)$$

und

$$U_{DFT}|\phi_2(l)\rangle = \sum_{z=0}^{d-1} \tilde{f}(z) |z\rangle \quad (12.66)$$

und

$$\begin{aligned} \tilde{f}(z) &= \frac{\sqrt{r}}{d} \sum_{j=0}^{\frac{d}{r}-1} \exp\left(2\pi i \frac{(l + jr)z}{d}\right) \\ &= \frac{\sqrt{r}}{d} \left[\sum_{j=0}^{\frac{d}{r}-1} \exp\left(2\pi i j \frac{rz}{d}\right) \right] \exp\left(2\pi i \frac{lz}{d}\right). \end{aligned} \quad (12.67)$$

Wir untersuchen den Faktor [...] weiter. Wenn z ein Vielfaches (einschließlich der Null) von $\frac{d}{r}$ ist, dann liegt eine geometrische Reihe vor

$$[\dots] = \frac{\exp\left(2\pi i \frac{rz}{d} \cdot \frac{d}{r}\right) - 1}{\exp\left(2\pi i \frac{rz}{d}\right) - 1} = 0, \quad (12.68)$$

da $z \in \mathbb{N}$. Wir müssen also nur $z = k \frac{d}{r}$ betrachten.

Der neue Laufbereich von z zieht sich auf die Zustände $|z\rangle$ durch. Das führt auf

$$U_{DFT}|\phi_2(l)\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left(2\pi i \frac{lk}{r}\right) \left|k \frac{d}{r}\right\rangle. \quad (12.69)$$

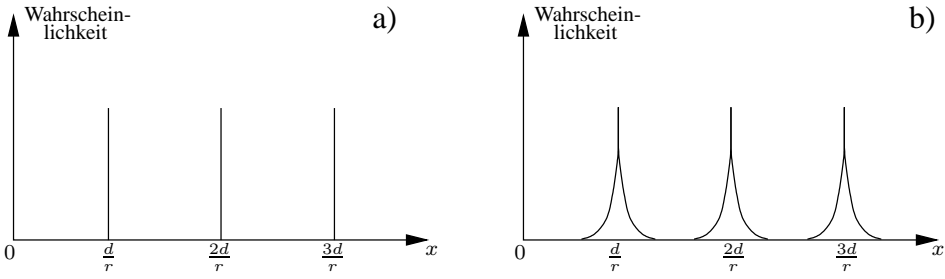


Abbildung 12.10: Wahrscheinlichkeitsverteilung der Messergebnisse x im ersten Register beim Shor-Algorithmus.

Der Offset l steht jetzt in der Phase. Die Periode r steht in den Bezeichnungen der Zustände ($k\frac{d}{r} \in \mathbb{N}$). Der Gesamtzustand ist

$$|\psi_3(l)\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |k\frac{d}{r}\rangle |\xi_l\rangle. \quad (12.70)$$

Den Zustand des zweiten Registers müssen wir nicht explizit hinschreiben. Insgesamt sind bisher erst zwei unitäre Transformationen erfolgt.

3. Schritt: Messung am ersten Register Wir messen in der Rechenbasis und wiederholen die ganze Prozedur mehrfach. Nur die Messergebnisse $x_k = k\frac{d}{r}$ mit $k = 0 \dots, r-1$ werden mit nicht verschwindender konstanter Wahrscheinlichkeit angezeigt (vergl. Abb. 12.10a). Daraus lässt sich $\frac{d}{r}$ ablesen. Da d bekannt ist, ist so die Periode r bestimmt.

Beispiel $N = 15$:

Wir haben $d = 8$.

Die Summanden in Gl. (12.61) haben den Offset $l = 0$ und $l = 1$. Die unitäre Transformation U_{DFT} überführt in

$$|\psi_3\rangle = \frac{1}{\sqrt{4}} \{ (|0\rangle + |4\rangle)|1\rangle + (|0\rangle + e^{i\pi}|4\rangle)|11\rangle \} \quad (12.71)$$

Mit der Wahrscheinlichkeit $\frac{1}{2}$ wird am ersten Register das Ergebnis 0 gemessen. Das enthält keine Information. Wenn der zu $k = 1$ gehörige Wert 4 gemessen wird, folgt aus $4 = k\frac{d}{r}$ für die Periode $r = 2$. Das beendet die Periodenbestimmung.

Wir ergänzen noch, dass man bei nur einer Messung mit dem Messwert x' mit einer gewissen Wahrscheinlichkeit auf ein k' trifft, dass mit r keinen gemeinsamen Teiler hat. ($\text{ggT}(k', r) = 1$).

$$\frac{x'}{d} = \frac{k'}{r} \quad (12.72)$$

Dann kürzt man x'/d so lange, bis ein irreduzibler Bruch entsteht und liest r ab. Mit einer gewissen Wahrscheinlichkeit reicht daher schon eine einzige Messung zur Periodenbestimmung.

Allgemeiner Fall Wenn r kein Teiler von d ist und damit die Annahme (12.64) nicht erfüllt ist, werden wir trotzdem erwarten, dass sich die Wahrscheinlichkeitsverteilung um die Werte von x konzentriert ist, die „fast“ ein Vielfaches von $\frac{d}{r}$ sind (vergl. Abb. 12.10b). Das lässt sich auch beweisen. Ein passendes Auswertungsverfahren kann angegeben werden (vergl. Abschn. 12.8). Die Zeit zur Durchführung der Quanten-Fourier-Transformation in einem d -dimensionalen Raum ist von der Größenordnung $(\log d)^2$. Die klassische schnelle Fourier-Transformation ist von der Ordnung $d \log d$. Daraus ergibt sich ihre Unterlegenheit (vergl. Abschn. 12.8).

12.7 Quantenfehlerkorrektur mit Hilfe nicht-lokaler Messungen

Wie in klassischen Computern, so treten auch in realen Quantencomputern Fehler auf. Wie wir in Kap. 15 im Einzelnen sehen werden, führt die Wechselwirkung mit der Umgebung zu Dekohärenz. Die reinen Zustände, auf denen die Berechnung beruht, werden in Gemische überführt. Eine andere Störung besteht darin, dass die Quantengatter, aus denen der Quantencomputer aufgebaut ist, nicht völlig perfekt arbeiten und möglicherweise gestörte unitäre Transformationen durchführen. Besonders drastische Störungen entstehen, wenn Zustände in Registerstellen umspringen (z. B. $|0\rangle \rightarrow |1\rangle$) oder eine Phasenänderung erfahren (z. B. $|0\rangle \rightarrow -|0\rangle$). Sowohl im Computer wie auch bei der Übertragung in Kanälen muß Quanteninformation gegen Verlust geschützt werden indem man Fehler aufspürt (Diagnose) und beseitigt (Therapie).

Die üblichen Verfahren zur Fehlerkorrektur bei klassisch verarbeiteter Information sind nicht übertragbar, da sie auf dem Kopieren von Zuständen und auf lokalen Messungen beruhen. Es gibt aber keine universellen Kopierer für Quantenzustände und lokale Messungen zerstören die Verschränkung. Man benötigt Quantenverfahren zur Fehlerkorrektur. Wir geben einige an.

Die *quantentheoretischen fehlerkorrigierenden Codes* (quantum error-correcting codes, QECC) sind ein Beispiel für die Verwendung von Verschränkung und von nicht-lokalen Messungen als Hilfsmittel. Die Grundidee besteht darin, Information redundant zu speichern. Es entstehen verschränkte Zustände. Im einfachsten Fall treten einzelnen Fehler lokal, d. h. in Untersystemen und einzelnen Registern auf. Dann können diese Fehler durch nicht-lokale Messungen (vergl. Abschn. 9.2) aufgespürt werden und die lokal-verborgene Information kann wieder hergestellt werden. Wir wollen das an einigen Beispielen demonstrieren.

12.7.1 Bit-Flip-Fehler

Ein *Bit-Flip-Fehler* (bit flip error) $|0\rangle \rightarrow |1\rangle, |1\rangle \rightarrow |0\rangle$ tritt lokal an einer einzelnen Registerstelle auf. Man kann sich dagegen schützen, indem man ein einzelnes Qubit durch drei Qubits in der folgenden Weise redundant kodiert:

$$|0\rangle \rightarrow |\bar{0}\rangle := |0, 0, 0\rangle \quad |1\rangle \rightarrow |\bar{1}\rangle := |1, 1, 1\rangle . \quad (12.73)$$

Damit wird aus dem Zustand $|\varphi\rangle$ der verschränkte Zustand $|\phi\rangle$

$$|\varphi\rangle := c_0|0\rangle + c_1|1\rangle \quad \rightarrow \quad |\phi\rangle := c_0|0, 0, 0\rangle + c_1|1, 1, 1\rangle . \quad (12.74)$$

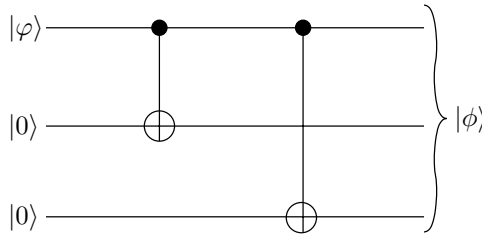


Abbildung 12.11: Erzeugung einer redundanten Kodierung.

Die entsprechende Quantenschaltung lässt sich mit Hilfe von zwei CNOT-Gattern wie in Abb. 12.11 aufbauen.

Wir bezeichnen die Produkt-Hilbert-Räume nicht mehr mit großen Buchstaben, sondern nummerieren sie durch: $\mathcal{H}^{(1)} \otimes \mathcal{H}^{(2)} \otimes \dots$. Die Zustände $|\bar{0}\rangle$ und $|\bar{1}\rangle$ sind beide Eigenzustände von $\sigma_z^{(1)} \sigma_z^{(2)}$ und $\sigma_z^{(2)} \sigma_z^{(3)}$ zum Eigenwert $+1$. Die entsprechenden nicht-lokalen Messungen in der Rechenbasis ergeben den Messwert $+1$ (vergl. Abschn. 9.2).

Ein Bit-Flip an einer Registerstelle führt z. B. auf den Zustand

$$|\phi'\rangle := c_0|1, 0, 0\rangle + c_1|0, 1, 1\rangle. \quad (12.75)$$

Die Messung der Observablen $\sigma_z^{(1)} \sigma_z^{(2)}$ ergibt nun den Messwert -1 , die der Observablen $\sigma_z^{(2)} \sigma_z^{(3)}$ den Messwert $+1$. Daraus kann eindeutig geschlossen werden, dass der Bit-Flip im ersten Register stattgefunden hat. Wichtig ist, dass bei der nicht-lokalen Messung der Zustand $|\phi'\rangle$ nicht abgeändert wurde. Daher führt eine unitäre Transformation $\sigma_x^{(1)} \otimes \mathbb{1}^{(2)} \otimes \mathbb{1}^{(3)}$, die einen Bit-Flip beim ersten Registerzustand bewirkt, dort wieder auf den Zustand $|\phi\rangle$ zurück. Die Messwertepaare, die bei der Messung von $\sigma_z^{(1)} \sigma_z^{(2)}$ und $\sigma_z^{(2)} \sigma_z^{(3)}$ erhalten werden, sind: $(+1, +1)$, $(-1, +1)$, $(-1, -1)$, $(+1, -1)$. Sie entsprechen der Reihe nach: kein Flip, Flip in der ersten, der zweiten oder der dritten Registerstelle. Der Bit-Flip wird wieder durch einen weiteren Bit-Flip an derselben Stelle rückgängig gemacht.

Unitäre Transformationen können nahe an der Identität sein. Dann findet nur selten ein Bit-Flip statt. Wir betrachten das Beispiel ($|\epsilon| \ll 1$)

$$\begin{aligned} |\phi\rangle \rightarrow |\phi''\rangle &= c_0 (|0, 0, 0\rangle + \epsilon|1, 0, 0\rangle) \\ &\quad + c_1 (|1, 1, 1\rangle + \epsilon|0, 1, 1\rangle) \end{aligned} \quad (12.76)$$

Durch Messung von $\sigma_z^{(1)} \sigma_z^{(2)}$ und $\sigma_z^{(2)} \sigma_z^{(3)}$ wird mit der Wahrscheinlichkeit $1 - |\epsilon|^2$ das Messergebnis $(0, 0)$ erhalten und auf den Zustand $|\phi\rangle$ zurück projiziert. Mit der Wahrscheinlichkeit $|\epsilon|^2$ findet man das Ergebnis $(-1, +1)$ und die Messung überführt in $|\phi'\rangle$. Aus dem Messergebnis kann auf den Endzustand geschlossen werden und, wenn nötig, der Fehler korrigiert werden.

12.7.2 Phasen-Flip-Fehler

Es wird ein Qubit in folgender Weise in 9 Qubits kodiert, die zu Clustern von 3 Qubits zusammengefasst sind:

$$\begin{aligned} |0\rangle &\rightarrow |\bar{0}\rangle = \frac{1}{2^{3/2}} (|0, 0, 0\rangle + |1, 1, 1\rangle) (|0, 0, 0\rangle + |1, 1, 1\rangle) (|0, 0, 0\rangle + |1, 1, 1\rangle) \\ |1\rangle &\rightarrow |\bar{1}\rangle = \frac{1}{2^{3/2}} (|0, 0, 0\rangle - |1, 1, 1\rangle) (|0, 0, 0\rangle - |1, 1, 1\rangle) (|0, 0, 0\rangle - |1, 1, 1\rangle) \end{aligned} \quad (12.77)$$

Jeder Cluster hat eine redundante Bit-Kodierung. Ein einzelner Bit-Flip kann wie in Abschn. 12.7.1 ermittelt und behoben werden. Ein *Phasen-Flip-Fehler* (phase flip error), der an einer der 9 Registerstellen stattfindet, kann folgendermaßen festgestellt werden: Man misst die zwei nicht-lokalen 6-Qubit-Observablen

$$\begin{aligned} &\sigma_x^{(1)} \sigma_x^{(2)} \sigma_x^{(3)} \sigma_x^{(4)} \sigma_x^{(5)} \sigma_x^{(6)} \\ &\sigma_x^{(4)} \sigma_x^{(5)} \sigma_x^{(6)} \sigma_x^{(7)} \sigma_x^{(8)} \sigma_x^{(9)} \end{aligned} \quad (12.78)$$

die mit σ_x gebildet werden. Die Zustände $|\bar{0}\rangle$ und $|\bar{1}\rangle$ sind Eigenzustände zum Eigenwert $+1$.

Wenn ein Phasenflip (Vorzeichenwechsel) in einem der Register stattfindet, dann ändert sich für diesen Cluster der Messwert der $\sigma_x \sigma_x \sigma_x$ -Messung um den Faktor -1 . Durch Messung der Operatoren (12.78) kann man ähnlich wie beim Bit-Flip-Fehler ermitteln, in welchem Cluster der Phasen-Flip stattgefunden hat. Die Fehlerkorrektur besteht dann darin, dass in diesem Cluster an irgendeiner Registerstelle eine σ_z -Transformation durchgeführt wird. Dadurch wird der Ausgangszustand wieder hergestellt.

Fehler bei allen Registerstellen Wir lassen zu, dass an allen Registerstellen ein Fehler auftreten kann, verlangen aber, dass das bei jeder einzelnen Registerstelle nur selten geschieht. Auf das einzelne Qubit kann dann die unitäre Transformation $U = \mathbb{1} + O(\epsilon)$ mit $\epsilon \ll 1$ wirken. Sie hat ganz allgemein die Struktur

$$U = \mathbb{1} + i\epsilon_x \sigma_x + i\epsilon_y \sigma_y + i\epsilon_z \sigma_z. \quad (12.79)$$

Die einzelnen Terme bewirken Bit-Flip, Phasen-Flip oder beides zusammen. Wir betrachten die Kodierung (12.77). Man führt wieder die Diagnose für Phasen-Flip und Bit-Flip durch und erreicht damit bereits, dass mit großer Wahrscheinlichkeit auf den ungestörten Zustand zurück projiziert wird. Mit einer geringen Wahrscheinlichkeit $|\epsilon|^2$ hat ein Bit-Flip oder Phasen-Flip in einem Register stattgefunden. Dieser Fehler wird erkannt und kann auf bekannte Weise behoben werden. Bei Fehlern an zwei oder mehr Stellen ist das so nicht möglich. Diese Situation tritt allerdings auch nur mit einer Wahrscheinlichkeit $|\epsilon|^4$ oder kleiner auf.

12.8 Ergänzende Themen und weiterführende Literatur

- Das Toffoli-Gatter ist ein universelles reversibles Gatter. Jede unitäre Transformation lässt sich durch Kombination von Toffoli-Gattern realisieren: [Pre 98, Kap. 6], [Gru 99, Kap. 1.7.1 und 3.1], [Hir 01, Kap. 2.3.2].

- Rechenzeiten für klassische und quantentheoretische Fourier-Transformation: [Pre 98, Kap. 6].
- Diskrete Fourier-Transformation, wenn Gl. (12.64) nicht erfüllt ist: [EJ 96], [Pre 98, Kap. 6.9.1].
- Dekohärenz durch Kopplung an die Umgebung zerstört die unitäre Entwicklung im Quantencomputer und ist daher eine wichtige Fehlerquelle: [Bar 96], [PSE 96].
- Dekohärenzfreie Unterräume und Systeme gelten als eine der erfolgversprechenden Lösungen des Dekohärenzproblems beim Quantencomputing: [LW 03].
- Wissen über Computational Complexity ermöglicht die Einschätzung von Vorteilen und Grenzen von Quantencomputern: [Mer 02].
- Fehlerkorrigierende Quantenkodes: [Pre 98, Kap. 7], [Pre 98 a], [Gru 99, Kap. 7], [Pre 99].
- Anzahl der nötigen Anfragen beim Grover-Algorithmus: [Pre 98, Kap. 6], [EHI 01].
- Beschreibung weiterer Such-Algorithmen: [Gru 99, Kap. 3].
- Optimale Zahl der Wiederholungen beim Grover-Algorithmus: [BBH 98], [EHI 01].
- Übersichtsartikel zum Shor-Algorithmus: [EJ 96].
- Übersichtsartikel zum Quantencomputing: [Ben 95], [Bar 96], [PVK 96], [Bar 98], [CEM 98], [DE 98], [Pre 98, Kap. 6], [Ste 98], [VP 98], [Bra 99a], [Joz 00], [NC 00, Part II], [RP 00], [EHI 01], [CB 02], [GM 02], [Lom 02a], [Wer 02].
- Euklidischer Algorithmus zur Bestimmung des größten gemeinsamen Teilers: [NC 00, Appendix 4].
- Wenn die Bedingung (12.40) erfüllt ist, hat die Funktion $f(x)$ von Gl. (12.42) eine Periode. Beweis mit Hilfe des Satzes von Euler und Fermat: [HW 79].
- Bücher über Quantencomputing: [BDM 98], [WC 98], [Bra 99], [Bro 99], [Gru 99], [Pit 00], [CP 01], [Hir 01], [DM 02], [KSV 02], [LB 02], [Lom 02], [SS 04].
- Bücher oder Übersichtsartikel zur experimentellen Realisierung von Quantencomputern: [Pel 98], [Gru 99, Kap. 7.6], [BEZ 00], [CLK 00], [DiV 00], [NC 00, Part II], [DM 02], [SS 04].
- Bücher mit Übersichtsartikeln zur experimentellen Realisierung von Quantencomputern: [LSP 98], [Bra 99], [BEZ 00], [DM 02], [Hei 02].
- Buch mit einer Gesamtdarstellung der Ansätze zur experimentellen Realisierung von Quantencomputern: [SS 04].
- Bücher mit Übersichtsartikeln zur Theorie der Quantencomputer: [LSP 98], [Bra 99], [CB 02], [GM 02], [Hei 02], [Lom 02].

12.9 Übungsaufgaben

ÜA 12.1 [Zu 12.4.2]

- (i) Zeigen Sie, dass die Wirkung der Hadamard-Transformation von n Qubits $H^{(n)} = H \otimes H \otimes \cdots \otimes H$ auf $|x\rangle$ die Form

$$|x\rangle \xrightarrow{H^{(n)}} \frac{1}{\sqrt{d}} \sum_{y=0}^d (-1)^{(x \cdot y)} |y\rangle \quad (12.80)$$

hat. Es entsteht eine gleichgewichtete Superposition der Basisvektoren von $\mathcal{H}_2^{(2)}$ mit Vorzeichen $+1$ und -1 . Dabei ist $(x \cdot y)$ das „vektorielle innere Produkt“ der Registerzustände

$$(x \cdot y) = x_{n-1}y_{n-1} + x_{n-2}y_{n-2} + \cdots + x_0y_0. \quad (12.81)$$

- (ii) Geben Sie $|\psi''\rangle$ von Gl. (12.23) vollständig an.
 (iii) Eine Blackbox berechnet die Funktion $f_a : \{0, 1\}^n \rightarrow \{0, 1\}$ definiert durch

$$f_a(x) = (a \cdot x). \quad (12.82)$$

Geben Sie einen Quantenalgorithmus an, der in der Lage ist, durch einmalige Berechnung von f_a und Messung des x -Registers die 2^n Funktionen f_a zu unterscheiden (Bernstein-Vazirani-Problem). Gehen Sie hierzu von dem in der Teilaufgabe (ii) gewonnenen Ausdruck für $|\psi''\rangle$ aus.

ÜA 12.2 [Zu 12.5] Für welchen Wert von N ist beim Grover-Algorithmus der gesuchte Zustand $|l\rangle$ bereits nach einem Durchgang mit Sicherheit bestimmt?

This Page Intentionally Left Blank

13 Verallgemeinerte Messungen, POVM

In der Quantentheorie sind nicht nur projektive Messungen möglich. Verallgemeinerte Messungen beschreiben komplexe Messsituationen und eröffnen neue Messmöglichkeiten. Wir führen am Beispiel des nicht-idealen Stern-Gerlach-Experiments in diese Messungen und in die POVM-Messungen ein.

13.1 Aufgaben einer allgemeinen Dynamik offener Quantensysteme

13.1.1 Fragestellungen

Wir haben schon bisher ein Quantensystem S^A um ein weiteres System S^B zu einem 2-Teile-System S^{AB} erweitert. Wechselwirkungen und Verschränkungen zwischen den beiden Teilsystemen sind erlaubt. Dadurch wird S^A zu einem *offenen System* (open system). Das Gesamtsystem S^{AB} soll aber wieder ein geschlossenes System sein. Es kann wie alle geschlossenen Systeme eine unitäre dynamische Entwicklung durchlaufen (unitäre Dynamik) und man kann an ihm projektive Messungen durchführen (Messdynamik). Die Regeln für beide Formen von Dynamik haben wir im vorangegangenen Kapitel 7.3.1 in den Postulaten formuliert. Wir wollen in den nächsten Kapiteln eine andere Betrachtungsweise vorstellen und dabei die Offenheit des Systems S^A in den Mittelpunkt stellen.

Die folgenden Fragestellungen sollen behandelt werden:

- (i) Welche Form hat die Dynamik von S^A in der speziellen Situation, in der S^A Teilsystem eines abgeschlossenen Systems S^{AB} ist, das eine unitäre Entwicklung durchläuft?
- (ii) Welche Struktur hat die allgemeinste physikalische Dynamik eines offenen Systems S^A ? Diese Frage soll weitgehend ohne einen Bezug auf ein zweites System (also auf S^B) beantwortet werden.
- (iii) Kann man diese – nicht mehr notwendig unitäre – verallgemeinerte Dynamik von S^A immer als Folge einer unitären Dynamik eines um S^B erweiterten Gesamtsystems S^{AB} auffassen? Wenn das möglich ist, wäre zugleich ein Verfahren für die experimentelle Realisierung der verallgemeinerten Dynamik von S^A angegeben.

Bisher haben wir die unitäre Dynamik verallgemeinert. Analog kann man die projektive Messdynamik verallgemeinern. Zunächst gehen wir wieder vom verschränkten Gesamtsystem S^{AB} aus.

- (i) Eine projektive Messung am zweiten System S^B überführt ein damit verschränktes System S^A mit gewissen Wahrscheinlichkeiten in entsprechende neue Zustände.
- (ii) Wenn wir von der möglichen Existenz eines zweiten Systems S^B absehen und nur S^A betrachten, welches ist die allgemeinste physikalische Struktur einer Messung an einem System S^A ?
- (iii) Kann man diese – nicht mehr notwendig projektive – verallgemeinerte Messung an S^A immer als Folge einer projektiven Messung an einem mit S^A verschränkten System S^B auffassen? Geeignete Verschränkung mit einem Hilfssystem S^B wäre dann die Grundlage für die Realisierung einer verallgemeinerten Messung an S^A .

Wir werden zunächst an einem einfachen Beispiel ablesen, welche Antworten auf die beiden Fragen (i) zu erwarten sind. Danach wenden wir uns den verallgemeinerten Messungen und den POV-Maßen zu. In Kap. 14 betrachten wir Quantenoperationen als Verallgemeinerung der unitären Dynamik und ergänzen in Kap. 16 noch fehlende Beweise.

13.1.2 Ein einfaches Beispiel

Verallgemeinerte Dynamik Um uns mit den zu erwartenden Strukturen vertraut zu machen, diskutieren wir zunächst ein mathematisch einfaches Beispiel. Wir beginnen mit einer unitären Dynamik des Gesamtsystems S^{AB} . Der Anfangszustand in $\mathcal{H}_2^A \otimes \mathcal{H}_2^B$ sei der Produktzustand

$$\rho^{AB} = \rho^A \otimes |0^B\rangle\langle 0^B|. \quad (13.1)$$

Er wird durch die unitäre Transformation

$$U^{AB} = \frac{1}{\sqrt{2}} (\sigma_x^A \otimes \mathbb{1}^B + \sigma_y^A \otimes \sigma_x^B) \quad (13.2)$$

in den verschränkten Zustand

$$\begin{aligned} \rho'^{AB} &= U^{AB} \rho^{AB} U^{AB\dagger} \\ &= \frac{1}{2} \left\{ \sigma_x^A \rho^A \sigma_x^A \otimes |0^B\rangle\langle 0^B| + \sigma_y^A \rho^A \sigma_y^A \otimes |1^B\rangle\langle 1^B| \right. \\ &\quad \left. + \sigma_x^A \rho^A \sigma_y^A \otimes |0^B\rangle\langle 1^B| + \sigma_y^A \rho^A \sigma_x^A \otimes |1^B\rangle\langle 0^B| \right\} \end{aligned} \quad (13.3)$$

überführt. Das System S^A geht dabei in den Zustand

$$\rho^A \rightarrow \rho'^A = \text{tr}_B[\rho'^{AB}] = \frac{1}{2} \{ \sigma_x^A \rho^A \sigma_x^A + \sigma_y^A \rho^A \sigma_y^A \} \quad (13.4)$$

über.

Die unitäre Entwicklung des Gesamtsystems bewirkt daher am Teilsystem S^A eine nicht-unitäre spurerhaltende Entwicklung, die mit Hilfe eines Superoperators \mathcal{E}^A in der Form einer *Operatorsummenzerlegung* (operator-sum decomposition)

$$\rho'^A = \mathcal{E}(\rho^A) = \sum_{i=1}^2 K_i^A \rho^A K_i^{A\dagger} \quad (13.5)$$

geschrieben werden kann. Dabei ist

$$K_1^A := \frac{1}{\sqrt{2}}\sigma_x^A, \quad K_2^A := \frac{1}{\sqrt{2}}\sigma_y^A. \quad (13.6)$$

Die K_i^A heißen *Kraus-Operatoren* (Kraus operators) (oder *Operationselemente* (operation elements) bzw. *Zerlegungsoperatoren* (decomposition operators)). Sie erfüllen die Vollständigkeitsrelation

$$\sum_{i=1}^2 K_i^{A\dagger} K_i^A = \mathbb{1}. \quad (13.7)$$

Im Vorgriff auf einen noch zu führenden Beweis stellen wir fest: *Die Dynamik des offenen Systems S^A lässt sich mit einem Superoperator \mathcal{E}^A beschreiben, der nur auf den Zustand von S^A wirkt. Für \mathcal{E}^A gibt es eine Operatorsummen-Darstellung.*

Man kann sich die Entwicklung (13.4) auch dadurch nicht-unitär erzeugt denken, dass mit den Wahrscheinlichkeiten $\frac{1}{2}$ die unitären Operatoren auf σ_x^A und σ_y^A auf S^A angewendet werden. Das wäre physikalisch ein ganz anderer Vorgang als der durch U^{AB} von Gl. (13.2) beschriebene. Die nicht-unitäre Entwicklung von S^A lässt sich durch die unitäre Entwicklung des erweiterten Systems S^{AE} realisieren. Beide stimmen in ihrer Auswirkung auf S^A überein. Wir werden zeigen, dass zu vorgegebener Entwicklung $\rho^A \rightarrow \rho'^A$ auch die Operatorsummen-Zerlegung nicht eindeutig festgelegt ist. Viele Einwirkungen auf S^A können zum selben Endzustand führen.

Verallgemeinerte Messung Wir schließen eine spezielle projektive Messung am zweiten Teilsystem S^B an. Hierfür wählen wir die Projektoren zur Rechenbasis von \mathcal{H}_2^B

$$P_+^B = |0^B\rangle\langle 0^B|, \quad P_-^B = |1^B\rangle\langle 1^B|. \quad (13.8)$$

Die Wahrscheinlichkeiten für das Auftreten der Messergebnisse $+$ und $-$ sind

$$p_{+,-} = \text{tr}_B [P_{+,-}^B \rho'^B P_{+,-}^B]. \quad (13.9)$$

$\rho'^B = \text{tr}_A [\rho'^{AB}]$ ist dabei der reduzierte Dichteoperator der Umgebung S^B nach der unitären Entwicklung. Wir können $p_{+,-}$ auch mit Blick auf das Teilsystem S^A interpretieren. $p_{+,-}$ sind zugleich die Wahrscheinlichkeiten dafür, dass sich das System S^A nach der Messung in einem der Zustände

$$\tilde{\mu}_{+,-}^A = \text{tr}_B [P_{+,-}^B \rho'^{AB} P_{+,-}^B] = \frac{1}{2} \sigma_{x,y}^A \rho^A \sigma_{x,y}^A \quad (13.10)$$

befindet. Wir haben zur Ableitung die Gl. (13.3) verwendet. Mit der Tilde kennzeichnen wir wieder, dass der Zustand noch nicht normiert ist. Der Normierungsfaktor wäre 2. Die Gesamtentwicklung von S^A ist also $\rho^A \rightarrow \rho'^A \rightarrow \mu_{+,-}^A$.

Die Zustände $\tilde{\mu}_{+,-}^A$ des Untersystems S^A nach der Messung an S^B wurden nicht durch Projektionen des Ausgangszustandes ρ^A gewonnen. Wie sind die Superoperatoren auf \mathcal{H}_2^A

aufgebaut, die den Anfangszustand ρ^A in diese beiden Zustände überführen? Zur Beantwortung schreiben wir die erste Gl. (13.10) für den Index $+$ unter Verwendung der Gl. (13.1) und (13.3) aus:

$$\begin{aligned}\tilde{\mu}'_+{}^A &= \text{tr}_B [(\mathbb{1}^A \otimes |0^B\rangle\langle 0^B| U^{AB} (\rho^A \otimes |0^B\rangle\langle 0^B|) U^{AB} (\mathbb{1}^A \otimes |0^B\rangle\langle 0^B|)] \\ &= \text{tr}_B [\langle 0^B| U^{AB} |0^B\rangle \rho^A \langle 0^B| U^{AB} |0^B\rangle \otimes |0^B\rangle\langle 0^B|] .\end{aligned}\quad (13.11)$$

Wir führen noch

$$M_+^A := \langle 0^B| U^{AB} |0^B\rangle = \frac{1}{\sqrt{2}} \sigma_x^A \quad (13.12)$$

ein und finden

$$\tilde{\mu}'_+{}^A = M_+^A \rho^A M_+^{A\dagger} . \quad (13.13)$$

Entsprechend ergibt sich für das Messergebnis $-$

$$\tilde{\mu}'_-{}^A = M_-^A \rho^A M_-^{A\dagger} \quad (13.14)$$

mit

$$M_-^A := \langle 1^B| U^{AB} |0^B\rangle = \frac{1}{\sqrt{2}} \sigma_y^A . \quad (13.15)$$

Die *Messoperatoren* (measurement operators) $M_{+,-}^A$ auf \mathcal{H}_2^A genügen der Vollständigkeitsrelation

$$M_+^{A\dagger} M_+^A + M_-^{A\dagger} M_-^A = \mathbb{1} . \quad (13.16)$$

Mit einer ähnlichen Umformung von Gl. (13.9) bestätigt man leicht, dass sich auch die Messwahrscheinlichkeiten, die ja zu Messungen an S^B gehören, mit Hilfe der Messoperatoren schreiben lassen (tr_B und tr_A vertauschen)

$$p_+ = \text{tr}_A [M_+^{A\dagger} M_+^A \rho^A] \quad (13.17)$$

entsprechend für p_- . Es gilt $p_+ + p_- = 1$.

Wir haben die Systeme S^A und S^B durch eine unitäre Entwicklung verschränkt. Eine anschließende projektive Messung am zweiten Teilsystem S^B führt mit den Wahrscheinlichkeiten p_+ bzw. p_- auf die Messergebnisse $+$ oder $-$. Abhängig vom Messergebnis geht dabei zugleich das Ausgangssystem S^A in einen von zwei wohlbestimmten Zuständen (13.10) über. Wir können diesen nicht-projektiven Eingriff an S^A als eine *verallgemeinerte selektive Messung* (generalized selective measurement) an S^A interpretieren. Zu ihr gehören die Messergebnisse $+$ oder $-$ mit den Wahrscheinlichkeiten p_+ bzw. p_- und den Endzuständen $\tilde{\mu}'_+{}^A$ bzw. $\tilde{\mu}'_-{}^A$. Wir kommen darauf noch genauer in Abschn. 13.3 zurück. Diese Messung lässt sich mit Hilfe der Messoperatoren $M_{+,-}^A$ formulieren, die nur auf den Zustand ρ^A von S^A vor der Messung wirken.

Das spezielle Beispiel zeigt, dass verallgemeinerte Messungen Situationen beschreiben können, die sich deutlich von den am Projektionsformalismus orientierten traditionellen Vorstellungen von einer Quantenmessung unterscheiden. Mit den Messoperatoren von Gl. (13.12) und (13.15) finden wir

$$p_+ = p_- = \frac{1}{2}. \quad (13.18)$$

Die Wahrscheinlichkeiten für die beiden Messergebnisse hängen daher gar nicht vom Zustand ρ^A ab, an dem gemessen wird. Bei den physikalisch relevanten verallgemeinerten Messungen ist das allerdings i.a. nicht so. Nachdem wir zur Verdeutlichung gewissermaßen einen „Extremfall“ vorgestellt haben, wollen wir im nächsten Kapitel ein physikalisches Beispiel diskutieren, in dem sich die Beschreibung als verallgemeinerte Messung in natürlicher Weise ergibt. Die allgemeine Struktur behandeln wir danach in Abschn. 13.3.

13.2 Das nicht-ideale Stern-Gerlach-Experiment als Beispiel für eine verallgemeinerte Messung

13.2.1 Der Versuchsaufbau

Der Versuchsaufbau Im *Stern-Gerlach-Experiment* (S-G-Experiment) werden in einer Quelle Spin- $\frac{1}{2}$ -Objekte erzeugt, die nach Austritt in y -Richtung durch ein inhomogenes Magnetfeld \mathbf{B} fliegen. Der Magnetfeldvektor liegt näherungsweise in z -Richtung (vergl. Abb. 13.1) sein Betrag ist eine Funktion von z . Das magnetische Moment der Objekte verursacht eine Wechselwirkung mit dem Magnetfeld, die eine polarisationsabhängige Kraft auf die Objekte bewirkt. Sie führt dazu, dass Objekte im Zustand $|\uparrow\rangle (= |0_z\rangle)$ in positiver z -Richtung und Objekte im Zustand $|\downarrow\rangle (= |1_z\rangle)$ in negativer z -Richtung abgelenkt werden. Für unsere Überlegungen brauchen wir nur diese sehr idealisierte Beschreibung. Einzelheiten der Bahnberechnung finden sich in den Lehrbüchern der Quantentheorie. Die abgelenkten Objekte treffen auf einen detektierenden Schirm in der x - z -Ebene, auf dem sie Schwärzungspunkte erzeugen.

Das ideale Stern-Gerlach-Experiment Beim idealen S-G-Experiment ist die Schrödinger-Funktion $|\psi_+(\mathbf{r})\rangle$, die das Ortsverhalten bei der Polarisation $|\uparrow\rangle$ beschreibt, in einem engen Bereich um die obere Bahn in Abb. 13.1 lokalisiert und die Schwärzungspunkte liegen ausschließlich in der oberen Halbebene ($z > 0$) des Schirms. Objekte mit Spin $|\downarrow\rangle$ haben eine um die untere Bahn in Abb. 13.1) lokalisierte Zustandsfunktion $|\psi_-(\mathbf{r})\rangle$ im Ortsraum und treffen entsprechend nur auf der unteren Halbebene ($z < 0$) des Schirms auf. Die Wahrscheinlichkeitsverteilungen für diese beiden Fälle sind in Abb. 13.2a dargestellt. Beim idealen S-G-Experiment überlappen sie nicht.

Vereinfachte Beschreibung Wir wollen jedes Auftreffen bei $z > 0$ einheitlich als Messergebnis $+1$ und bei $z < 0$ als Messergebnis -1 auffassen. Die Objekte werden durch Zustände in einem Produkt-Hilbert-Raum beschrieben. Er setzt sich zusammen aus dem Spin-Raum

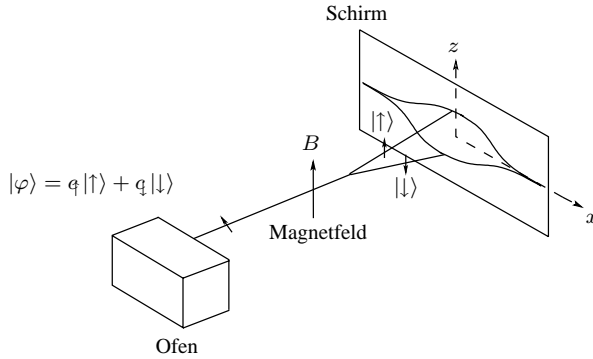


Abbildung 13.1: Stern-Gerlach-Experiment. Zeichnung nach [BGL 95].

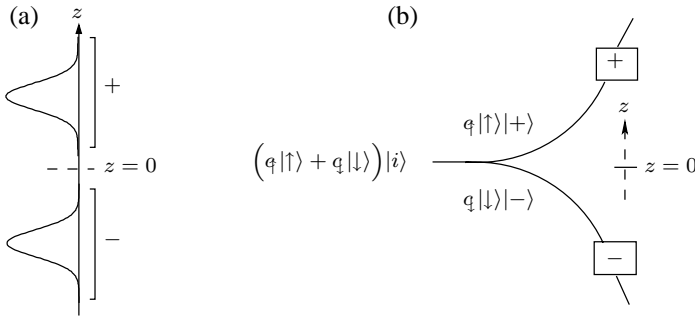


Abbildung 13.2: Ideales Stern-Gerlach-Experiment. Auftreffwahrscheinlichkeiten (a) und schematische Darstellung (b). Die Detektoren + und – sprechen bei Auftreffen auf der oberen bzw. unteren Halbebene an.

\mathcal{H}_2^S des inneren Spinfreiheitsgrads und dem Raum der äußeren Bahnfreiheitsgrade. Im idealen S-G-Experiment werden die Spinpolarisationen in z -Richtung und damit die Observable σ_z gemessen.

Um die Rechnungen übersichtlicher zu gestalten, vereinfachen wir die Beschreibung und führen statt des Bahnraums einen Raum \mathcal{H}_2^B mit der ONB $\{|+\rangle, |-\rangle\}$ ein. Die Observable $O = |+\rangle\langle+| - |-\rangle\langle-|$ mit den Messwerten $+1$ und -1 gibt das Ansprechen auf den Halbebenen $z > 0$ bzw. $z < 0$ wieder. Wir repräsentieren das durch das Ansprechen eines projektiv wirkenden (+)-Detektors bzw. (–)-Detektors wie in Abb. 13.2b. Der komplexe Ablenkungsprozess ist dadurch auf zwei „Bahnen“ reduziert worden. Anders als der Schirm, sollen die Detektoren keine zerstörenden Messungen durchführen. Es macht daher Sinn vom Zustand des Objekts nach der Messung zu sprechen.

Das nicht optimale Stern-Gerlach-Experiment Im nicht optimal realisierten S-G-Experiment sind die Schrödinger-Funktionen $\psi_{\pm}(\mathbf{r})$ nicht streng auf einer Halbebene

lokalisiert. Die Funktion $\psi_+(\mathbf{r})$ verschwindet nicht für $z < 0$ (vergl. Abb. 13.3a und 13.3b). Das hat zur Folge, dass für Objekte mit Spin $|\uparrow\rangle$ mit einer gewissen Wahrscheinlichkeit auch der $(-)$ -Detektor anspricht und für Spin $|\downarrow\rangle$ der $(+)$ -Detektor anspricht. Aus dem Ansprechen eines Detektors kann daher nicht mehr sicher auf das Vorliegen einer Spinpolarisation geschlossen werden. Im Folgenden diskutieren wir die bisher nur qualitativ beschriebenen verschiedenen physikalischen Situationen im Einzelnen.

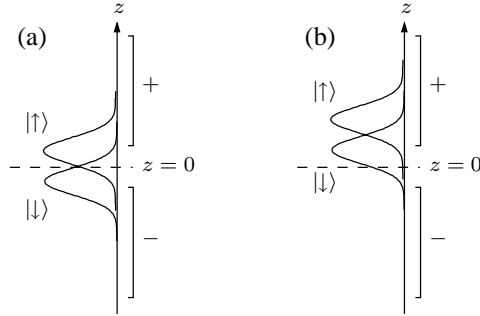


Abbildung 13.3: Nicht-optimales Stern-Gerlach-Experiment. Aus dem Ansprechen eines Detektors kann nicht eindeutig auf die Spinpolarisation geschlossen werden.

13.2.2 Beispiel einer verallgemeinerten Messung

Vor Durchlaufen des Magnetfelds liegen der Spinzustand

$$|\varphi\rangle = c_\uparrow|\uparrow\rangle + c_\downarrow|\downarrow\rangle, \quad |c_\uparrow|^2 + |c_\downarrow|^2 = 1 \quad (13.19)$$

und der Bahnzustand $|i\rangle$ vor. Der Gesamtzustand aus $\mathcal{H}_2^S \otimes \mathcal{H}_2^B$ ist der einlaufende Produktzustand

$$|\chi\rangle = |\varphi\rangle|i\rangle. \quad (13.20)$$

Die Wechselwirkung korreliert die Zustände $|\uparrow\rangle$ und $|+\rangle$ sowie die Zustände $|\downarrow\rangle$ und $|-\rangle$ miteinander. Das führt auf Verschränkung. Im idealen S-G-Experiment geht dabei $|\chi\rangle$ unitär in den verschränkten Zustand

$$|\chi\rangle \rightarrow |\chi'\rangle = c_\uparrow|\uparrow\rangle|+\rangle + c_\downarrow|\downarrow\rangle|-\rangle \quad (13.21)$$

über. Bei einer projektiven Messung in der Rechenbasis spricht der $(+)$ -Detektor mit der Wahrscheinlichkeit p_+ an und das Spinsystem wird in den Zustand $|\uparrow\rangle$ überführt. Entsprechendes gilt für den $(-)$ -Detektor.

$$\text{„+“} : |\varphi\rangle \rightarrow |\uparrow\rangle, \quad p_+ = |c_\uparrow|^2; \quad \text{„-“} : |\varphi\rangle \rightarrow |\downarrow\rangle, \quad p_- = |c_\downarrow|^2. \quad (13.22)$$

Beim idealen Stern-Gerlach-Experiment führt die durch die Detektoren bewirkte projektive Messung im Bahnraum \mathcal{H}_2^B auf eine indirekte projektive Messung der Observablen σ_z im Spinraum. Das ist schematisch in Abb. 13.2b dargestellt.

Im realen S-G-Experiment liegen demgegenüber die beiden Wahrscheinlichkeitsverteilungen nicht mehr symmetrisch zu $z = 0$, sondern sind unsymmetrisch verschoben und ragen jeweils über $z = 0$ hinaus (siehe Abb. 13.3). Der Anfangszustand mit Spinzustand $|\uparrow\rangle|i\rangle$ wird entsprechend durch die Wechselwirkung in

$$|\uparrow\rangle|i\rangle \rightarrow |\uparrow\rangle(\sqrt{1-p_0}|+\rangle + \sqrt{p_0}|-\rangle) \quad (13.23)$$

mit $0 \leq p_0 \leq 1$ überführt. Analoges gilt für $|\downarrow\rangle$

$$|\downarrow\rangle|i\rangle \rightarrow |\downarrow\rangle(\sqrt{p_1}|+\rangle + \sqrt{1-p_1}|-\rangle) \quad (13.24)$$

mit $0 \leq p_1 \leq 1$. Die Parameter p_0 und p_1 geben die Verschiebungen der Wahrscheinlichkeitsverteilungen wieder. Für die oben beschriebene indirekte Projektionsmessung gilt $p_0 = 0$ und $p_1 = 0$. Die Normierung der Zustandsvektoren erzwingt die Form der Vorfaktoren in Gl. (13.23) und (13.24).

Mit den Gl. (13.23) und (13.24) liegt zugleich fest, wie der allgemeine einlaufende Zustand $|\chi\rangle = |\varphi\rangle|i\rangle$ durch die Wechselwirkung verschränkt wird:

$$|\chi\rangle \rightarrow |\chi'\rangle = \{\sqrt{1-p_0} c_\uparrow |\uparrow\rangle + \sqrt{p_1} c_\downarrow |\downarrow\rangle\}|+\rangle + \{\sqrt{p_0} c_\uparrow |\uparrow\rangle + \sqrt{1-p_1} c_\downarrow |\downarrow\rangle\}|-\rangle. \quad (13.25)$$

Eine Messung besteht wieder im Ansprechen des (+) - Detektors oder (−) - Detektors. Wir führen die Messoperatoren

$$M_+ := \sqrt{1-p_0} |\uparrow\rangle\langle\uparrow| + \sqrt{p_1} |\downarrow\rangle\langle\downarrow|, M_- := \sqrt{p_0} |\uparrow\rangle\langle\uparrow| + \sqrt{1-p_1} |\downarrow\rangle\langle\downarrow| \quad (13.26)$$

ein. Sie erfüllen die Vollständigkeitsrelation

$$M_+^\dagger M_+ + M_-^\dagger M_- = \mathbb{1}. \quad (13.27)$$

Als Verallgemeinerung von Gl. (13.22) finden wir dann (vergl. Abb. 13.4a)

$$\begin{aligned} \text{„+“: } |\varphi\rangle \rightarrow |\varphi_+\rangle &= \{\sqrt{1-p_0} c_\uparrow |\uparrow\rangle + \sqrt{p_1} c_\downarrow |\downarrow\rangle\} \cdot \frac{1}{\text{Norm}} \\ &= M_+ |\varphi\rangle \cdot \frac{1}{\text{Norm}}, \end{aligned} \quad (13.28)$$

$$p_+ = (1-p_0)|c_\uparrow|^2 + p_1|c_\downarrow|^2 = \langle\varphi|M_+|\varphi\rangle, \quad (13.29)$$

$$\begin{aligned} \text{„−“: } |\varphi\rangle \rightarrow |\varphi_-\rangle &= \{\sqrt{p_0} c_\uparrow |\uparrow\rangle + \sqrt{1-p_1} c_\downarrow |\downarrow\rangle\} \cdot \frac{1}{\text{Norm}}, \\ &= M_- |\varphi\rangle \cdot \frac{1}{\text{Norm}} \end{aligned} \quad (13.30)$$

$$p_- = p_0|c_\uparrow|^2 + (1-p_1)|c_\downarrow|^2 = \langle\varphi|M_-|\varphi\rangle. \quad (13.31)$$

Das nicht-optimale Stern-Gerlach-Experiment stellt ebenfalls eine verallgemeinerte Messung dar. Die Analogie zu den Gl. (13.12)–(13.17) ist offensichtlich.

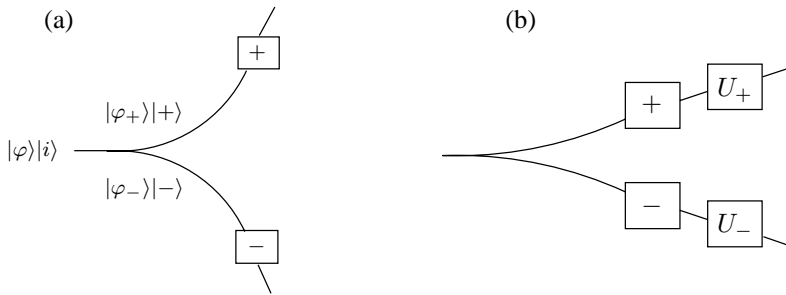


Abbildung 13.4: (a) Schematische Darstellung des nicht-optimalen Stern-Gerlach-Experiments. (b) Erweiterung durch unitäre Einwirkungen zu einer nicht-minimalen Messung.

13.2.3 Unscharfe und schwache Messungen

Beim nicht optimalen S-G-Experiment führt die projektive Messung im Bahnraum \mathcal{H}_2^B nicht mehr auf eine Projektion im Spinraum. Aus den Wahrscheinlichkeiten p_+ und p_- kann nicht mehr auf $|c_\uparrow|^2$ und $|c_\downarrow|^2$ geschlossen werden. *Die verallgemeinerte Messung ist in diesem Sinne eine unscharfe Messung der Spinpolarisation.* Es gibt zwei Grenzfälle:

- (i) $p_0 = p_1 = 0$: Der Zustand $|\chi'\rangle$ zeigt zu vorgegebenem Spinzustand $|\varphi\rangle$ die größte mögliche Verschränkung die Messung ist eine *scharfe (oder exakte) Messung* (sharp measurement), da aus den Messergebnissen direkt auf $|c_\uparrow|^2$ und $|c_\downarrow|^2$ geschlossen werden kann. Das S-G-Gerät ist perfekt eingestellt. Der Informationsgewinn ist in diesem Fall am größten. Der Ausgangszustand wird andererseits am stärksten durch die Messung abgeändert.
- (ii) $p_0 = p_1 = \frac{1}{2}$: Der Zustand $|\chi'\rangle$ ist gar nicht verschränkt ($|\chi'\rangle = \frac{1}{\sqrt{2}}|\varphi\rangle \otimes \{|+\rangle + |-\rangle\}$). Die Messung ist völlig *unscharf (oder unexakt)* (unsharp measurement). Wegen $p_+ = p_- = \frac{1}{2}$ erlauben die Messungen keinen Schluss auf $|c_\uparrow|^2$ oder $|c_\downarrow|^2$. Die S-G-Anlage ist für die Bestimmung dieser Größe völlig unbrauchbar. Ein Informationsgewinn liegt nicht vor. Der Ausgangszustand wird andererseits durch die Messung nicht verändert. Wir erwähnen noch, dass diese Parameterwahl der Situation entspricht, in der in Abb. 13.3 die beiden Kurven übereinander liegen und einen zu $z = 0$ spiegelsymmetrischen Verlauf haben.

Wenn die Werte der Parameter p_0 und p_1 in der Nähe von $\frac{1}{2}$ liegen ist die Abänderung des Spinzustands gering. Wir nennen diesen Eingriff eine *schwache Messung* (weak measurement). Entsprechend ist auch der Informationsgewinn durch die Messung gering. Die Messung ist unscharf.

Wir kehren noch einmal zum System S^A und dem Hilfssystem S^B von Abschn. 13.1.2 zurück. Das nicht-ideale S-G-Experiment ist ein Beispiel dafür, wie durch Wahl von S^B (hier das Bahnsystem) und geeignete Anpassung der unitär erzeugten Verschränkung mit S^A (hier mit dem Spinsystem) ein kontinuierliches Spektrum von verallgemeinerten Messungen von S^A bewirkt werden kann. Hierzu wird an S^B projektiv gemessen. Kann man auf diese Weise

an jedem System S^A eine beliebig vorgegebene nicht-projektive Messung realisieren? Wir kommen auf die Frage in Abschn. 13.3.5, 13.4 und in Abschn. 16.3 zurück.

13.3 Verallgemeinerte Messungen

13.3.1 Was ist eine Quantenmessung?

In Kap. 2 wurden die unitäre Dynamik und die Messdynamik eingeführt. Beide Typen von Entwicklungen werden durch *Eingriffe* (interventions) bewirkt. Wir haben in den vorangegangenen Kapiteln 13.1 und 13.2 gesehen, dass es allgemeinere Entwicklungen zwischen zwei Messungen gibt und dass man nicht-projektive Messungen durchführen kann. Wir wollen beide Eingriffe genauer beschreiben und beginnen dabei mit den Messungen.

Eine *allgemeine Messung* (general measurement) ist ein Eingriff besonderen Typs an einem einzelnen Quantensystem bei dem (von trivialen Spezialfällen abgesehen) eine *Verzweigung* (branching) in der Entwicklung des Quantensystems stattfindet. Diese Verzweigung ist mit einer wohlbestimmten Änderung eines klassischen Systems verbunden, die die Ablesung einer reellen Zahl (Messergebnis, z. B. Zeigerstellung) aus einem für den Eingriff spezifischen Wertebereich erlaubt. Die Wahrscheinlichkeiten für das Eintreten der verschiedenen Verzweigungsäste und der zugeordneten Messergebnisse liegen fest, wenn der Messeingriff spezifiziert ist und der Zustand des Systems vor der Messung fixiert ist. Die projektive Messung einer Observablen ist ein Spezialfall. Wir haben das am Beispiel des Stern-Gerlach-Experiments veranschaulicht.

Auch im allgemeinen Fall überführt eine selektive Messung des Quantensystems abhängig vom Messergebnis in einen bestimmten Zustand und wirkt daher präparierend. Üblicherweise laufen dabei irreversible Prozesse ab, so dass das Messergebnis fixiert ist (z. B.: der Zeiger bewegt sich nicht mehr über der Skala). Unmittelbare Wiederholung derselben Messung (d. h. des gleichen Eingriffs) muss aber nicht wieder auf dasselbe Messergebnis führen. Anders als bei einer projektiven Messung kann bei einer allgemeinen Messung i. a. nicht von der Messung einer physikalischen Größe (Observablen) wie Energie, Spinpolarisation usw. gesprochen werden.

In der Quantentheorie kann die Bezeichnung „Messung“ leicht ebenso missverstanden werden wie die Bezeichnung „Zustand“, da Assoziationen mit den Bedeutungen dieser Begriffe in der klassischen Physik geweckt werden. Es gibt für Quantensysteme i. a. keine Eigenschaften, die vor der Messung festliegen und die wir durch die Messung ermitteln. Messen heißt nur, einen speziellen Eingriff durchführen, bei dem in Gestalt der Messwerte eine Information abgelesen werden kann, die sich primär auf den auslaufenden Zustand bezieht. Wir werden Beispiele diskutieren, wie man diese Information ausnutzen kann. Bei gewissen Fragestellungen können allgemeine Messungen den projektiven Messungen überlegen sein. Auch hierfür geben wir Beispiele. Wir betrachten in diesem Kapitel zunächst noch die einfachste Verallgemeinerung der projektiven Messung und diskutieren die völlig allgemeinen Messungen in Abschn. 14.2.

13.3.2 Verallgemeinerte Messpostulate

Eine *verallgemeinerte Messung* (generalized measurement) wird durch einen Satz $\{M_m\}$ von linearen *Messoperatoren* (measurement operators) beschrieben. Zu jedem ablesbaren reellen *Messwert* m (measurement outcome) ist genau ein Messoperator M_m erklärt. Der Einfachheit halber setzen wir die Messwerte wieder als diskret voraus. Durch den Messeingriff wird der Zustand $|\psi\rangle$ des Quantensystems in den Zustand

$$|\psi\rangle \rightarrow |\psi'_m\rangle = \frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} \quad (13.32)$$

überführt. Diese Überführung und der zugehörige Messwert m treten mit der Wahrscheinlichkeit

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle \quad (13.33)$$

auf. Da $M_m^\dagger M_m$ ein positiver Operator ist, ist die Bedingung $p(m) \geq 0$ erfüllt. Wir müssen zur Erhaltung der Wahrscheinlichkeitsinterpretation ($\sum_m p(m) = 1$) noch zusätzlich von den Messoperatoren die Vollständigkeitsrelation

$$\sum_m M_m^\dagger M_m = \mathbb{1} \quad (13.34)$$

fordern. (vergl. das Beispiel in Abschn. 13.1.2)

Die Verallgemeinerung auf Dichteoperatoren als Zustände ergibt sich mit den gleichen Begründungen wie in Kap. 4:

$$\rho \rightarrow \rho'_m = M_m \rho M_m^\dagger \quad (13.35)$$

$$p(m) = \text{tr}[M_m^\dagger M_m \rho] = \text{tr}[\tilde{\rho}'_m], \quad \rho'_m = \frac{1}{p(m)} \tilde{\rho}'_m. \quad (13.36)$$

Bei einer nicht-selektiven Messung haben wir

$$\rho \xrightarrow{\text{n.s.}} \rho' = \sum_m M_m \rho M_m^\dagger. \quad (13.37)$$

Von den Operatoren M_m wird nur Linearität verlangt. Dadurch ist garantiert, dass sich die Relationen von Kap. 4 für Gemische und insbesondere die physikalisch unmittelbar plausible Gl. (4.13) übertragen. Die Operatoren M_m müssen nicht hermitesch sein. Sie sind keine Observablenoperatoren. Es wird i.a.

$$M_m M_{m'} \neq \delta_{m,m'} M_m \quad (13.38)$$

sein. Insbesondere kann die Anzahl der Messoperatoren auch größer als die Dimension des Hilbert-Raums sein. Die M_m sind also nur im Spezialfall der projektiven Messungen ($M_m = P_m$) orthogonale Projektoren. An den Gl. (13.32) und (13.38) lässt sich ablesen, dass bei der Wiederholung einer Messung sich die Wahrscheinlichkeitsverteilung der Messwerte ändert. Mit einem Satz $\{M_m\}$ wird i.a. nicht die Messung einer Eigenschaft verknüpft. Wir werden in Abschn. 14.2 sehen, dass die hier beschriebenen verallgemeinerten Messungen (zu einem Messwert gehört nur ein Messoperator) noch nicht die allgemeinsten Messungen sind.

13.3.3 Polare Zerlegung eines linearen Operators

Wir stellen zunächst einige mathematische Vorüberlegungen an, die wir dann bei der Interpretation der verallgemeinerten Messungen anwenden.

Bi-orthogonale Entwicklung eines unitären Operators U sei ein unitärer Operator und $\{|v_i\rangle\}$ eine ONB des Hilbert-Raums. Dann entsteht durch die unitäre Transformation

$$|w_i\rangle = U|v_i\rangle \quad (13.39)$$

wieder eine ONB $\{|w_i\rangle\}$. Ein beliebiger unitärer Operator U lässt sich daher bei Vorgabe einer ONB $\{|v_i\rangle\}$ stets in der Form

$$U = \sum_i |w_i\rangle\langle v_i| \quad (13.40)$$

mit einer ONB $\{|v_i\rangle\}$ schreiben.

Polare Zerlegung und bi-orthogonale Entwicklung eines linearen Operators L sei ein linearer Operator. Dann sind $L^\dagger L$, LL^\dagger , $\sqrt{L^\dagger L}$ und $\sqrt{LL^\dagger}$ positive Operatoren. Wir gehen von der spektralen Zerlegung

$$L^\dagger L = \sum_i \lambda_i |r_i\rangle\langle r_i|, \quad \lambda_i \geq 0 \quad (13.41)$$

aus. $\{|r_i\rangle\}$ ist eine ONB. Die Wirkung von L führt auf die Vektoren

$$|m_i\rangle := L|r_i\rangle, \quad (13.42)$$

für die

$$\langle m_i | m_i \rangle = \langle r_i | L^\dagger L | r_i \rangle = \lambda_i \quad (13.43)$$

gilt. Für die Indexwerte i , für die $\lambda_i \neq 0$ ist, können wir die Vektoren $|m_i\rangle$ normieren:

$$|l_i\rangle := \frac{1}{\sqrt{\lambda_i}} |m_i\rangle. \quad (13.44)$$

Diese $|l_i\rangle$ sind orthonormal

$$\langle l_i | l_j \rangle = \frac{1}{\sqrt{\lambda_i} \sqrt{\lambda_j}} \langle r_i | L^\dagger L | r_j \rangle = \delta_{i,j}. \quad (13.45)$$

Wir ergänzen diese Vektoren $|l_i\rangle$ zu einer ONB.

Mit Hilfe der ONB $\{|r_i\rangle\}$ und $\{|l_i\rangle\}$ führen wir den unitären Operator

$$U := \sum_i |l_i\rangle\langle r_i| \quad (13.46)$$

ein. Für U ergibt sich mit Gl. (13.41)

$$U\sqrt{L^\dagger L} = \sum_i \sqrt{\lambda_i} |l_i\rangle \langle r_i| . \quad (13.47)$$

Andererseits folgt aus Gl. (13.42) und (13.44)

$$L|r_i\rangle = \sqrt{\lambda_i} |l_i\rangle . \quad (13.48)$$

Da die Wirkung von $U\sqrt{L^\dagger L}$ und L auf der Basis $\{|r_i\rangle\}$ übereinstimmt, gilt

$$L = U\sqrt{L^\dagger L} . \quad (13.49)$$

U ist eindeutig durch L bestimmt, wenn $\lambda_i \neq 0$ für alle i . Die Relation (13.49) wird die *links-polare Zerlegung* (left polar decomposition) des linearen Operators L genannt. Damit soll an die Analogie zur Zerlegung $c = e^{i\phi}|c|$ einer komplexen Zahl c in Betrag und Phase erinnert werden.

Wir schreiben Gl. (13.49) noch mit Hilfe der Gl. (13.41) und (13.46) um

$$L = \sum_i \sqrt{\lambda_i} |l_i\rangle \langle r_i|, \quad \lambda_i \geq 0 . \quad (13.50)$$

Für jeden linearen Operator L gibt es eine bi-orthogonale Zerlegung (13.50) (*bi-orthogonal decomposition*) bezüglich zweier ONB $\{|l_i\rangle\}$ und $\{|r_i\rangle\}$, deren Konstruktion oben angegeben ist. Wir ergänzen noch ohne Beweis die *rechts-polare Zerlegung* (right-polar decomposition)

$$L = \sqrt{LL^\dagger} U \quad (13.51)$$

Man beachte die andere Reihenfolge der Operatoren unter der Wurzel. $L^\dagger L$ und LL^\dagger haben dieselben Eigenwerte λ_i (vergl. Gl. (13.41))

$$LL^\dagger = \sum_i \lambda_i |l_i\rangle \langle l_i| . \quad (13.52)$$

13.3.4 Minimale Messungen

Die Messoperatoren M_m einer verallgemeinerten Messung kann man immer polar zerlegen

$$M_m = U_m \sqrt{E_m} \quad (13.53)$$

mit

$$E_m := M_m^\dagger M_m . \quad (13.54)$$

Die E_m erfüllen als Folge von Gl. (13.34) die Bedingung

$$\sum_m E_m = \mathbb{1} . \quad (13.55)$$

Die positiven Operatoren E_m bilden ein *POVM* (positive operator valued measure). Sie heißen Effektoroperatoren (*effect operators*) oder *POVM-Elemente* (*POVM elements*). Wir kommen auf die *POVM-Messung* in Abschn. 13.3.5 zurück. Der unzerlegte Messoperator M_m bewirkt gemäß Gl. (13.32) bzw. (13.35) den Übergang zum neuen Zustand, der zum angezeigten Messwert m gehört. Der gleiche Endzustand wird erreicht, wenn man den Ausgangszustand zunächst mit dem positiven Operator $\sqrt{E_m}$ transformiert und die unitäre Entwicklung U_m anschließt. Die Wahrscheinlichkeit $p(m)$ von Gl. (13.42) für das Auftreten des Messwertes m ist nur eine Funktion von E_m

$$p(m) = \text{tr}[\rho E_m] . \quad (13.56)$$

Die unitäre Entwicklung hat keinen Einfluss auf die durch $p(m)$ gewonnene Information. Wir können uns daher eine verallgemeinerte Messung mit Messwert m formal zerlegt denken in eine durch $\sqrt{E_m}$ repräsentierte Messdynamik, die mit der Wahrscheinlichkeit $p(m)$ korreliert ist, und einer unitären Dynamik U_m , die keinen Einfluss auf $p(m)$ hat, wohl aber den ausgehenden Zustand ρ'_m mit bestimmt. *Es gibt zu einem POVM beliebig viele Operatoren U_m , die auf die gleiche Wahrscheinlichkeitsverteilung $p(m)$ führen.* Verallgemeinerte Messungen mit $U_m = \mathbb{1}$, bei denen also der unitäre Einfluss auf den Zustand nicht vorhanden ist, werden *minimale Messungen* (minimal measurements) genannt. Projektive Messungen sind minimal.

Minimale Messungen an Qubits Wir wollen wie im Stern-Gerlach-Experiment voraussetzen, dass nur zwei Messergebnisse $+$ und $-$ möglich sind. Wegen der Bedingung (13.55) gilt dann

$$E_+ = \mathbb{1} - E_- \quad (13.57)$$

und die *POVM-Operatoren* vertauschen

$$[E_+, E_-] = 0 . \quad (13.58)$$

Da die Operatoren positiv sind, sind sie auch hermitesch und es gibt eine orthonormale Basis $\{|0\rangle, |1\rangle\}$ bezüglich derer beide orthogonal sind:

$$E_+ = a|0\rangle\langle 0| + p_1|1\rangle\langle 1| , \quad (13.59)$$

$$E_- = p_0|0\rangle\langle 0| + b|1\rangle\langle 1| . \quad (13.60)$$

Die Bedingung (13.58) wird durch $a = 1 - p_0$ und $b = 1 - p_1$ erfüllt. Die Positivität der Operatoren bedingt dann $0 \leq p_0 \leq 1$ und $0 \leq p_1 \leq 1$. Die Messoperatoren für die zugehörigen minimale Messung ergeben sich ganz allgemein in der Form

$$M_+ = \sqrt{1 - p_0}|0\rangle\langle 0| + \sqrt{p_1}|1\rangle\langle 1| , \quad (13.61)$$

$$M_- = \sqrt{p_0}|0\rangle\langle 0| + \sqrt{1 - p_1}|1\rangle\langle 1| . \quad (13.62)$$

Wie die Gl. (13.28) und (13.30) zeigen, beruht das in Abschn. 13.2 beschriebene Stern-Gerlach-Experiment auf diesen Messoperatoren. Es stellt eine minimale Messung dar. Eine nicht-minimale Messung ergibt sich, wenn man wie in Abb. 13.4b hinter den Detektoren jeweils noch eine zusätzliche unitäre Dynamik anschließt.

13.3.5 Realisierung einer verallgemeinerten Messung durch unitäre Transformation und Projektion

Wir haben in Abschn. 13.1.2 gesehen, dass man eine verallgemeinerte Messung bewirken kann, indem man das System S^A um ein Hilfssystem S^B erweitert, auf $\mathcal{H}^A \otimes \mathcal{H}^B$ eine unitäre Transformation durchführt und am System S^B projektiv misst. Wir wollen jetzt zeigen, dass jede verallgemeinerte Messung so realisiert werden kann.

Wir erweitern das System S^A um das *Hilfssystem* (ancilla) S^B . Die Dimension von \mathcal{H}^A ist beliebig. Die Dimension von \mathcal{H}^B soll gleich der Anzahl der Messoperatoren sein. In \mathcal{H}^B wählen wir eine ONB $\{|m^B\rangle\}$ und einen beliebigen aber festen Zustand $|0^B\rangle$. Wir definieren auf einem Unterraum von $\mathcal{H}^A \otimes \mathcal{H}^B$ den linearen Operator \hat{U}^{AB} durch

$$\hat{U}^{AB}|\phi^A, 0^B\rangle = \sum_m M_m^A |\phi^A\rangle \otimes |m^B\rangle \quad (13.63)$$

für beliebige $|\phi^A\rangle$ aus \mathcal{H}^A . Die Messoperatoren $|M_m^A\rangle$ und die Basis $\{|m^B\rangle\}$ legen \hat{U}^{AB} fest. Für irgend zwei Vektoren $|\phi_1^A, 0^B\rangle$ und $|\phi_2^A, 0^B\rangle$ aus diesem Unterraum erhält der Operator \hat{U}^{AB} das innere Produkt.

$$\begin{aligned} \langle \phi_1^A, 0^B | \hat{U}^{AB\dagger} \hat{U}^{AB} | \phi_2^A, 0^B \rangle &= \sum_{m, m'} \langle \phi_1^A | M_m^{A\dagger} M_m^A | \phi_2^A \rangle \langle m^B | m'^B \rangle \\ &= \sum_m \langle \phi_1^A | M_m^{A\dagger} M_m^A | \phi_2^A \rangle \\ &= \langle \phi_1^A | \phi_2^A \rangle = \langle \phi_1^A, 0^B | \phi_2^A, 0^B \rangle. \end{aligned} \quad (13.64)$$

Daher können wir einen mathematischen Satz anwenden, der besagt, dass in diesem Fall eine unitäre Erweiterung U^{AB} von \hat{U}^{AB} auf den ganzen Raum $\mathcal{H}^A \otimes \mathcal{H}^B$ existiert. Das ist deshalb wichtig, weil man davon ausgehen kann, dass U^{AB} eine physikalisch realisierbare dynamische Entwicklung des Gesamtsystems S^{AB} darstellt, die durch einen geeigneten Hamilton-Operator auf $\mathcal{H}^A \otimes \mathcal{H}^B$ beschrieben werden kann. Die Wirkung des unitären Operators U^{AB} auf den Vektoren des Unterraums reduziert sich auf die von \hat{U}^{AB} .

Wenn man nach der unitären Entwicklung mit U^{AB} eine projektive Messung in \mathcal{H}^B mit den Projektionsoperatoren

$$P_m^B := \mathbf{1}^A \otimes |m^B\rangle\langle m^B| \quad (13.65)$$

durchführt, geht das Gesamtsystem in den Zustand

$$P_m^B U^{AB} |\phi^A, 0^B\rangle \cdot \frac{1}{\text{Norm}} = \frac{M_m^A |\phi^A\rangle |m^B\rangle}{\sqrt{\langle \phi^A | M_m^{A\dagger} M_m^A | \phi^A \rangle}} \quad (13.66)$$

mit der Wahrscheinlichkeit

$$p(m) = \langle \phi^A, 0^B | U^{AB\dagger} P_m^B U^{AB} | \phi^A, 0^B \rangle = \langle \phi^A | M_m^{A\dagger} M_m^A | \phi^A \rangle \quad (13.67)$$

über. Im letzten Schritt haben wir $P_m^B = P_m^{B\dagger} P_m^B$ und Gl. (13.66) verwendet. Damit haben wir gezeigt: *Jede verallgemeinerte Messung lässt sich dadurch physikalisch realisieren, dass das System S^A um ein Hilfssystem S^B ergänzt wird. Durch eine geeignete unitäre Transformation des Gesamtsystems S^{AB} , deren dynamische Realisierbarkeit wir voraussetzen wollen, wird S^{AB} in einen verschränkten Zustand überführt. Projektionsmessungen am Hilfssystem S^B führen schließlich auf die verallgemeinerte Messung an S^A .* Die Operatoren sind in den Gl. (13.63) und (13.65) angegeben.

13.4 POVM-Messung

13.4.1 Messwahrscheinlichkeiten und positive Operatoren

Wir diskutieren Messungen in einer reduzierten und dadurch völlig allgemeinen Betrachtungsweise: Von einem Messeingriff sollen nur die Messwerte m und die Wahrscheinlichkeiten $p(m)$ ihres Auftretens bekannt sein. Da der Messeingriff sich auf den Zustand linear auswirken soll, gibt es die den jeweiligen Messergebnissen zugeordnete lineare Operatoren E_m , mit denen sich die Wahrscheinlichkeiten $p(m)$ in der Form

$$p(m) = \langle \psi | E_m | \psi \rangle \quad (13.68)$$

$$p(m) = \text{tr}[\rho E_m] \quad (13.69)$$

schreiben lassen. Wegen $p(m) \geq 0$ müssen die E_m positive Operatoren sein, die wegen $\sum_m p(m) = 1$ zusätzlich der Bedingung

$$\sum_m E_m = \mathbb{1} \quad (13.70)$$

genügen müssen. Die Operatoren E_m sind die Elemente einer Zerlegung des Einsoperators in positive Operatoren. Wie wir schon in Abschn. 13.3.4 festgestellt haben, heißt eine solche Zerlegung der Eins *positiv-operatorwertiges Maß POVM* (Akronym für positive operator-valued measure). Die Operatoren E_m werden *POVM-Elemente* (POVM elements) genannt.

Bei der Einführung eines POVM wird nicht vorausgesetzt, dass die Messung in der in Abschn. 13.3.2 beschriebenen Weise durch Messoperatoren beschrieben werden kann. Das POVM-Schema gilt auch in allgemeineren Messsituationen, die wir in Abschn. 14.2 besprechen werden. Für viele Fragestellungen kann man sich mit Aussagen über die Wahrscheinlichkeitsverteilung $p(m)$ begnügen. Man spricht dann von einer *POVM-Messung* (POVM measurement). Im Spezialfall verallgemeinerter Messungen ist

$$E_m = M_m^\dagger M_m. \quad (13.71)$$

Für die physikalische Realisierung eines vorgegebenen POVM genügt es, den Messoperator $M_m = \sqrt{E_m}$ wie in Abschn. 13.3.5 zu realisieren. Die Projektionsoperatoren P_n einer projektiven Messung sind der Spezialfall eines POVM. Sie werden *projektionswertiges Maß PVM* (projection valued measure) genannt. Anders als im PVM kann aber die Anzahl der POVM-Elemente größer als die Dimension des Zustandsraums sein.

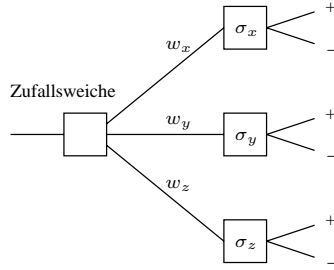


Abbildung 13.5: Zusammengesetzte Messung

13.4.2 Zusammengesetzte Messung als Beispiel einer POVM-Messung

Wir betrachten einen Versuchsaufbau (vergl. Abb. 13.5), bei dem eine klassische Zufallsweiche die im Zustand $|\psi\rangle$ eintreffenden Spin- $\frac{1}{2}$ -Objekte mit den Wahrscheinlichkeiten w_x , w_y und w_z auf Messgeräte für die Observablen σ_x , σ_y und σ_z lenkt ($w_x + w_y + w_z = 1$). Die drei Messgeräte zeigen als Messwerte jeweils $+1$ oder -1 an. Die Geräte messen projektiv. Die zugehörigen Projektionsoperatoren sind $P_i(+) = |0_i\rangle\langle 0_i|$ und $P_i(-) = |1_i\rangle\langle 1_i|$ mit $i = x, y, z$. Insgesamt gibt es sechs mögliche Messergebnisse (i, \pm) . Die entsprechenden Messwahrscheinlichkeiten sind

$$p(i, \pm) = w_i \langle \psi | P_i(\pm) | \psi \rangle = \langle \psi | E_i(\pm) | \psi \rangle \quad (13.72)$$

mit den sechs POVM-Operatoren

$$E_i(\pm) = w_i P_i(\pm), \quad (13.73)$$

die die Vollständigkeitsrelation

$$\sum_i E_i(+)+\sum_i E_i(-)=\sum_i w_i \mathbb{1}=\mathbb{1} \quad (13.74)$$

erfüllen. Durch die vorgeschaltete Zufallsweichen geht der Projektorcharakter verloren. Wir erwähnen noch, dass die Anlage eine *informationell vollständige Messung* (informationally complete measurement) darstellt. Die durch die Messwahrscheinlichkeiten $p(i, \pm)$ wiedergegebene Statistik erlaubt auch für Gemische die eindeutige Bestimmung des Anfangszustands (vergl. ÜA 13.5). Wir diskutieren informationell vollständige Messungen in Abschn. 13.4.5.

Wir erweitern die Anlage zu einer zusammenfassenden Messung indem wir nicht mehr zwischen den drei Messgeräten unterscheiden. Registriert wird nur der Messwert unabhängig davon welches Gerät ihn angezeigt hat. Dann finden wir für die verbliebenen zwei Wahrscheinlichkeiten

$$p(\pm) = \sum_i p(i, \pm) = \langle \psi | E(\pm) | \psi \rangle \quad (13.75)$$

mit den Operatoren

$$E(\pm) = \sum_i w_i P_i(\pm) \quad , \quad \sum_{+,-} E(\pm) = \mathbb{1} . \quad (13.76)$$

Es ist wieder eine POVM-Messung entstanden.

13.4.3 Kann eine einzelne POVM-Messung zwei Zustände sicher unterscheiden?

Mathematische Vorüberlegungen Ein Operator E sei positiv. Dann hat er eine Spektraldarstellung

$$E = \sum_i \lambda_i |i\rangle\langle i| ; \quad \lambda_i \in \mathbb{R} , \quad 0 \leq \lambda_i \leq 1 \quad (13.77)$$

mit einer ONB $|i\rangle$. Die Wirkung von E auf einen beliebigen normierten Vektor $|\phi\rangle$ ist

$$E|\phi\rangle = \sum_i \lambda_i \langle i|\phi\rangle |i\rangle = \sum_i \lambda_i c_i |i\rangle \quad (13.78)$$

mit

$$c_i := \langle i|\phi\rangle , \quad \sum_i |c_i|^2 = 1 . \quad (13.79)$$

Damit wird

$$\langle \phi|E|\phi\rangle = \sum_i \lambda_i |c_i|^2 . \quad (13.80)$$

Ein spezieller Zustand $|\phi\rangle$ möge die Eigenschaft

$$\langle \phi|E|\phi\rangle = \sum_i \lambda_i |c_i|^2 = 1 \quad (13.81)$$

haben. Die nicht verschwindenden c_i haben dabei Indizes i aus einer Indexmenge I . Für diese Indizes folgt aus der Gl. (13.81) und $0 \leq \lambda_i \leq 1$

$$\lambda_{i \in I} = 1 . \quad (13.82)$$

Einsetzen in Gl. (13.78) führt auf das Ergebnis

$$\langle \phi|E|\phi\rangle = 1 \quad \Longleftrightarrow \quad E|\phi\rangle = |\phi\rangle . \quad (13.83)$$

Die Richtung \Leftarrow ist trivial. Auf ähnliche Weise zeigt man

$$\langle \phi|E|\phi\rangle = 0 \quad \Longleftrightarrow \quad E|\phi\rangle = 0 . \quad (13.84)$$

Unmöglichkeit einen Zustand durch eine einzige POVM-Messung zu bestimmen Wir nehmen an, dass wir durch eine einzige Messung entscheiden können, ob ein einzelnes Quantenobjekt in einen Zustand $|\chi\rangle$ ist. Dann muß es eine Messung mit POVM-Operatoren E_m geben, bei der ein spezielles Messergebnis \hat{m} mit Sicherheit eintritt, wenn $|\chi\rangle$ vorliegt, und mit Sicherheit nicht eintritt, wenn ein beliebiger anderer Zustand $|\Theta\rangle \neq |\chi\rangle$ aus dem Hilbert-Raum vorliegt:

$$p_\chi(\hat{m}) = \langle \chi|E_{\hat{m}}|\chi\rangle = 1 \quad (13.85)$$

$$p_\Theta(\hat{m}) = \langle \Theta|E_{\hat{m}}|\Theta\rangle = 0 . \quad (13.86)$$

Wir haben also mit Gl. (13.83) und (13.84)

$$E_{\hat{m}}|\chi\rangle = |\chi\rangle \quad , \quad E_{\hat{m}}|\Theta\rangle = 0 \quad . \quad (13.87)$$

Damit erhalten wir

$$\langle\chi|\Theta\rangle = \langle E_{\hat{m}}|\Theta\rangle = \langle\chi|E_{\hat{m}}\rangle = 0 \quad . \quad (13.88)$$

Das heißt, alle anderen Vektoren $|\Theta\rangle$ des Hilbert-Raums müssen senkrecht auf $|\chi\rangle$ stehen. Das ist unmöglich. *Es ist daher nicht möglich mit einer einzigen POVM-Messung den Zustand eines Quantenobjekts vor der Messung zu bestimmen. Weiterhin zeigt das Ergebnis, dass es keine POVM-Messung gibt, die es erlaubt eindeutig zwischen zwei nicht orthogonalen Zuständen zu unterscheiden.* Diese wichtige Aussage, auf der viele heuristische Überlegungen basieren, gilt also nicht nur für Projektionsmessungen, sondern für beliebige Messungen.

13.4.4 Vorteil einer POVM-Messung bei der Zustandsermittlung

Für eine etwas modifizierte Fragestellung ist die Verwendung von POVM-Messungen hingegen günstiger als die projektiver Messungen. Es soll uns (oder einem Lauscher) bekannt sein, dass ein Quantensystem mit gleicher Wahrscheinlichkeit entweder in einem Zustand $|1\rangle$ oder in einem dazu nicht orthogonalen Zustand $|2\rangle$ präpariert wird. Wir wollen nach einer einzigen Messung entweder keine Aussage machen („weiß nicht“) oder mit Sicherheit sagen können: „in $|1\rangle$ “ oder „in $|2\rangle$ “. Es müssen daher mindestens drei Messergebnisse möglich sein. Die POVM-Operatoren sind E_1, E_2, E_3 . Wir konstruieren sie so, dass Folgendes erreicht wird: Wenn Zustand $|1\rangle$ vorliegt, tritt das Messergebnis 2 nie ein (d.h. $\langle 1|E_2|1\rangle = 0$), aber Ergebnisse 1 und 3 können eintreten. Beim Zustand $|2\rangle$ tritt das Messergebnis 1 nie ein (d.h. $\langle 2|E_1|2\rangle = 0$), aber Ergebnisse 2 und 3 sind möglich. Wir können daher aus einer einzigen Messung die folgenden Schlüsse ziehen: Wenn sich das Messergebnis 1 ergibt, dann lag der Zustand $|1\rangle$ vor. Beim Messergebnis 2 lag $|2\rangle$ vor. Aus Messergebnis 3 kann nichts gefolgert werden. Für POVM-Operatoren bedeutet das

$$E_1 = a_2(\mathbb{1} - |2\rangle\langle 2|) \quad , \quad (13.89)$$

$$E_2 = a_1(\mathbb{1} - |1\rangle\langle 1|) \quad (13.90)$$

und

$$E_3 = \mathbb{1} - E_1 - E_2 \quad . \quad (13.91)$$

Es ist sicher sinnvoll, die Messung zu optimieren. Dazu müssen die Parameter a_1 und a_2 so gewählt werden, dass die Wahrscheinlichkeit p dafür, dass ein sicherer Schluss möglich ist, maximiert wird. Sichere Schlüsse kann man nur aus den Messergebnissen 1 und 2 ziehen. Die Wahrscheinlichkeit dafür, dass diese Messergebnisse eintreten, ist nach Voraussetzung

$$p = \frac{1}{2}\langle 1|E_1|1\rangle + \frac{1}{2}\langle 2|E_2|2\rangle \quad (13.92)$$

$$= \frac{1}{2}(a_1 + a_2)(1 - |\langle 1|2\rangle|^2) \quad (13.93)$$

In [Bus 97] wird gezeigt, dass p unter Beachtung der Positivität von E_3 , durch die die Parameter a_1 und a_2 verknüpft werden, den maximalen Wert

$$p_{\max} = 1 - |\langle 1|2 \rangle| \quad (13.94)$$

für die Parameterwahl

$$a_1 = a_2 = \frac{1}{1 - |\langle 1|2 \rangle|} \quad (13.95)$$

annimmt. Gl. (13.95) zeigt, dass die Wahrscheinlichkeit, sichere Aussagen durch eine Messung zu treffen, immer geringer wird, je mehr die Zustände $|1\rangle$ und $|2\rangle$ sich einander annähern. Eine Auflösung der Zustände durch die POVM-Messung wird dann immer schwieriger. Für orthogonale Zustände $\langle \phi | \chi \rangle = 0$ ist $p_{\max} = 1$.

13.4.5 Informationell vollständiges POVM

Ein POVM heißt *informationell vollständig* (informationally complete), wenn für einen beliebigen Zustand die Kenntnis der Wahrscheinlichkeiten aller möglichen Messergebnisse einer Messung ausreicht, um den Zustand zu bestimmen. Es wird also nur ein einziges Messgerät (nur ein POVM) verwendet. Welche Bedingungen muss ein informationell vollständiges POVM zur Bestimmung von Qubit-Zuständen erfüllen?

Wir haben in Abschn. 3.1 gesehen, dass die Pauli-Operatoren durch $\mathbb{1}$ zu einer Operatorbasis auf \mathcal{H}_2 ergänzt werden können. Jedes POVM-Element lässt sich in der Form

$$E_m = a_m \mathbb{1} + b_m \mathbf{n}_m \boldsymbol{\sigma} \quad (13.96)$$

schreiben. \mathbf{n}_m ist dabei ein Einheitsvektor im \mathbb{R}^3 und a_m und b_m sollen nicht-negative reelle Zahlen sein, damit E_m und $\mathbb{1} - E_m$ positive Operatoren sind. Die Vollständigkeitsbedingung (13.70) führt auf die Bedingungen

$$\sum_m a_m = 1, \quad (13.97)$$

$$\sum_m b_m \mathbf{n}_m = 0. \quad (13.98)$$

Wie wir in Abschn. 4.4 gezeigt haben, kann jeder Dichteoperator ρ auf \mathcal{H}_2 in der Form

$$\rho = \frac{1}{2}(\mathbb{1} + \mathbf{r} \boldsymbol{\sigma}) \quad (13.99)$$

mit dem Bloch-Vektor \mathbf{r} geschrieben werden. Die Wahrscheinlichkeiten für die Messergebnisse der POVM-Messung sind daher

$$p(m) = \text{tr}[\rho E_m] = a_m + b_m \mathbf{n}_m \mathbf{r}. \quad (13.100)$$

Man sieht daran, dass zur Bestimmung von \mathbf{r} die nicht verschwindenden Vektoren $b_m \mathbf{n}_m$ den \mathbb{R}^3 aufspannen müssen. Daraus folgt zusammen mit der linearen Abhängigkeit (13.98),

dass es mindestens vier Vektoren \mathbf{n}_m geben muß ($m = 1, 2, 3, 4$) und dass andererseits vier Vektoren, die die Gl. (13.98) erfüllen, ausreichen.

Wir geben ein Beispiel das Gl. (13.97) und (13.98) erfüllt: $a_m = b_m = \frac{1}{4}$ und

$$\mathbf{n}_1 = (0, 0, 1), \quad (13.101)$$

$$\mathbf{n}_2 = \left(\frac{2\sqrt{2}}{3}, 0, -\frac{1}{3} \right), \quad (13.102)$$

$$\mathbf{n}_3 = \left(-\frac{\sqrt{2}}{3}, \sqrt{\frac{2}{3}}, -\frac{1}{3} \right), \quad (13.103)$$

$$\mathbf{n}_4 = \left(-\frac{\sqrt{2}}{3}, -\sqrt{\frac{2}{3}}, -\frac{1}{3} \right). \quad (13.104)$$

Einsetzen in Gl. (13.96) führt auf das informationell vollständig POVM für Qubit-Zustände.

Wir haben in Abschn. 4.4 gesehen, dass durch die Messung der Erwartungswerte der drei verschiedenen Observablen σ_x, σ_y und σ_z der Bloch-Vektor \mathbf{r} und damit der Zustand ρ bestimmt werden kann. Hier haben wir gezeigt, dass der Qubit-Zustand ρ auch durch Messung der Wahrscheinlichkeiten $p(m)$ einer einzigen POVM-Messung (nur ein Messgerät) mit vier Messwerten m ermittelt werden kann.

13.4.6 Schätzung des Zustands vor der Messung

In der klassischen Physik wird durch die Messung der Zustand vor der Messung bestimmt. Bei einer einzelnen Quantenmessung kann demgegenüber bei fehlender Entartung aus einem Messergebnis m nur auf den Zustand nach der Messung geschlossen werden. Wir wollen zeigen, dass auf der Grundlage der Annahme von Bayes zumindest geschätzt werden kann, welcher Zustand vor der Messung vorlag. Die Messung soll durch das POVM $\{E_m\}$ beschrieben sein.

Wir kehren zunächst zum Satz von Bayes von Gl. (1.99) zurück und machen die Bayessche Annahme (1.100), dass alle Ausgangswahrscheinlichkeiten $p(A_i)$ übereinstimmen. Um den Bayesschen Satz zu veranschaulichen, betrachten wir den Fall, dass die bedingte Wahrscheinlichkeit $p(B|A_i)$ dafür, dass B eintritt, für ein spezielles Ereignis A_j besonders groß ist: $p(B|A_j) \gg p(B|A_{i \neq j})$. Das Ereignis B möge tatsächlich eintreten. Dann hat in diesem Fall mit besonders großer Wahrscheinlichkeit vorher A_j vorgelegen: $p(A_j|B) \gg p(A_{i \neq j}|B)$. Dasjenige Ereignis A_j , auf das mit der größten Wahrscheinlichkeit B folgt, ist auch dasjenige, das mit der größten Wahrscheinlichkeit $p(A_j|B)$ vorher vorgelegen hat, wenn B eintritt. Dies ist die plausible Aussage des Satzes von Bayes.

Wir übertragen die Aussage auf die quantentheoretische Messsituation. Es wird an einem einzelnen Quantensystem eine Präparation in einem reinen Zustand durchgeführt. Die Messung an diesem System mit einem durch ein POVM beschriebenen Messapparat liefert den Messwert m . Unter der Bayesschen Annahme ist der Zustand $|\chi_{pre}\rangle$, der mit der größten Wahrscheinlichkeit vor der Messung vorlag, dadurch gegeben, dass für ihn $p(m)$ am größten ist¹.

¹Eine mathematisch exakte Formulierung muss berücksichtigen, dass die möglichen Zustände ein Kontinuum bilden (vergl. Abschn. 13.5)

Die POVM-Elemente sind positive Operatoren mit der Spektralzerlegung

$$E_m = \sum_i a_i^{(m)} |r_i^{(m)}\rangle \langle r_i^{(m)}|. \quad (13.105)$$

Die Eigenvektoren sollen nicht entartet sein. Für $p(m)$ erhalten wir

$$p(m) = \langle \psi | E_m | \psi \rangle = \sum_i a_i^{(m)} |\langle \psi | r_i^{(m)} \rangle|^2 \quad (13.106)$$

mit $|\langle \psi | r_i^{(m)} \rangle| \leq 1$ und $\sum_i |\langle \psi | r_i^{(m)} \rangle| = 1$. Wir können daher $p(m)$ abschätzen:

$$p(m) \leq a_{\max}^{(m)} \quad (13.107)$$

mit $a_{\max}^{(m)} = \max\{a_i^{(m)}\}$. Der Maximalwert von $p(m)$ wird in Gl. (13.106) für den zu $a_{\max}^{(m)}$ gehörigen Eigenvektor $|\chi_{pre}\rangle = |r_{\max}^{(m)}\rangle$ von E_m angenommen. *Wenn keine weitere Information vorliegt, ist die beste Schätzung für den Zustand vor einer Messung mit dem Messergebnis m der Eigenvektor $|r_{\max}^{(m)}\rangle$ zum größten Eigenwert $a_{\max}^{(m)}$ des POVM-Elements E_m .* Bei einer projektiven Messung ($P_m = |r^{(m)}\rangle \langle r^{(m)}|$) ist daher der auslaufende Zustand $|r^{(m)}\rangle$ die beste Schätzung für den einlaufenden Zustand.

13.5 Ergänzende Themen und weiterführende Literatur

- Weiterführende Literatur zu informationell vollständiger Messung: [BGL 95], [Aul 00].
- Zur Unmöglichkeit, individuelle Quantenzustände zu bestimmen, sowie zur optimalen Zustandsunterscheidung: [Bus 97] (dort auch weitere Literatur).
- Das Theorem von Neumark beschreibt die Realisierung einer Quantenmessung durch eine Projektionsmessung auf dem *zusammengesetzten* System aus Ursprungssystem und Umgebung: [Per 90].
- Ausführliche Darstellung von Quantenmessungen und POVM: [BGL 95], [Kon 03], [Fle 00].
- Detaillierte Behandlung des Stern-Gerlach-Experiments: [BGL 95, Kap VII].
- Bücher zu den Grundlagen der Theorie der Quantenoperationen und der nicht-projektiven Messungen: [Kra 83], [BGL 95].
- Dynamik offener Systeme: [MW 98], [Dav 76], [Hol 01], [BP 02].
- Eine Bestätigung des Ergebnisses aus Abschn. 13.4.6, die nicht auf dem Bayesschen Satz und der Bayesschen Annahme beruht, findet sich in [ADK 03].
- Die Nützlichkeit von schwachen Messungen zeigt sich, wenn man versucht die Zeitentwicklung $|\psi(t)\rangle$ eines Zustands messend zu verfolgen: [AKK 04].

13.6 Übungsaufgaben

ÜA 13.1 [zu 13.1] Bestätigen Sie Gl. (13.17).

ÜA 13.2 [zu 13.2] Bestimmen Sie für das reale Stern-Gerlach-Experiment im Spezialfall $p_0 = p_1$ über die Entropie die Verschränkung des Zustandes $|\chi'\rangle$ von Gl. (13.25) und den Informationsgewinn durch die Messung.

ÜA 13.3 [zu 13.2] Entwerfen Sie unter Verwendung der verschränkenden Wirkung des CNOT-Gatters ein Schaltbild zur Erzeugung von $|\chi'\rangle$ von Gl. (13.25) im Spezialfall $p_0 = p_1$. Welche Zustände müssen einlaufen.

ÜA 13.4 [zu 13.3] Zeigen Sie, dass die Hintereinanderausführung von zwei Messungen wieder eine Messung ist. Geben Sie die Messoperatoren an.

ÜA 13.5 [zu 13.3.3] Beweisen Sie die rechts-polare Zerlegung.

ÜA 13.6 [zu 13.3.3] Zeigen Sie ausgehend von der bi-orthogonalen Zerlegung (13.50) des linearen Operators L , dass L sich stets in der Form

$$L = VDW \quad (13.108)$$

schreiben lässt. V und W sind dabei unitäre Operatoren. D ist ein positiver Operator mit den Eigenwerten λ_i . Hinweis: Schreiben Sie die Zerlegung durch Einführung einer ONB $\{|a_i\rangle\}$ um.

ÜA 13.7 [zu 13.3.5] Die mit einer ONB $\{|n^A\rangle\}$ von \mathcal{H}^A gebildeten Vektoren $\{|n^A, 0^A\rangle\}$ sind die ONB eines Unterraums von $\mathcal{H}^A \otimes \mathcal{H}^B$. \hat{U}^{AB} sei ein auf dem Unterraum definierter linearer Operator, der auf $\mathcal{H}^A \otimes \mathcal{H}^B$ abbildet und dabei innere Produkte erhält. Dann existiert eine Erweiterung U^{AB} von \hat{U}^{AB} , die auf dem ganzen Raum als unitärer Operator wirkt und auf dem Unterraum mit \hat{U}^{AB} übereinstimmt. Es könnte geschickt sein, die dyadische Darstellung und die Ergebnisse aus Abschn. 13.3.3 zu verwenden.

ÜA 13.8 [zu 13.4] Zeigen Sie, dass jede Messung, bei der die Messoperatoren M_m und die POVM-Elemente E_m übereinstimmen, eine projektive Messung ist.

ÜA 13.9 [zu 13.4.2] Zeigen Sie, dass die zusammengesetzte Messung aus Abschn. 13.4.2 informationell vollständig ist.

ÜA 13.10 [zu 13.4.3] Beweisen Sie die Behauptung (13.84).

ÜA 13.11 [zu 13.4.3] Beweisen Sie Ergebnisse (13.94) und (13.95).

ÜA 13.12 [zu 13.4.5] Zeigen Sie, dass die in Abschn. 13.4.2 beschriebene POVM-Messung informationell vollständig ist.

ÜA 13.13 [zu 13.4.6] Ein durch Messoperatoren $\{M_m\}$ beschriebener Messapparat führt eine Messung an einem Quantenobjekt durch, dass sich in einem reinen Zustand befindet. Das Messergebnis ist m . Eine weitere Information ist nicht gegeben. Schätzen Sie den Zustand nach der Messung. Beachten Sie dabei, dass mit dem Zustand vor der Messung auch der Zustand nach der Messung eindeutig festliegt. Betrachten Sie auch den Spezialfall einer minimalen Messung.

14 Allgemeine Entwicklung eines offenen Quantensystems und spezielle Quantenkanäle

Teilsysteme machen i.a. keine unitären Entwicklungen mehr durch. Quantenoperationen sind der angemessene Zugang zu einer In-Out-Formulierung der dynamischen Entwicklung offener Systeme. Wir veranschaulichen sie am Beispiel von Quantenkanälen. Auch die Zustandsänderungen bei Messungen sind im allgemeinsten Fall Quantenoperationen. Aus dieser Sicht lassen sich das Szenario und die Regeln der Quantentheorie noch einmal neu formulieren.

14.1 Quantenoperationen und ihre Operatorsummenzerlegungen

14.1.1 Quantenoperationen

Dynamische Entwicklung als Quantenoperation Im Zusammenhang mit Quantenkanälen, Teleportation, Kryptographie, Quantencomputern und Quantenmessungen treten zeitliche Entwicklungen von Quantenzuständen auf, die allgemeiner sind als unitäre Entwicklungen, die mit Projektionen kombiniert wurden. Beispiele für allgemeine Zustandsänderungen, die auftreten wenn das System mit der Umgebung gekoppelt ist, haben wir in Kap. 13 kennen gelernt. Wir wollen allgemeine Entwicklungen im Folgenden vom offenen System aus beschreiben und nicht bereits spezielle Ansätze für eventuell vorhandene weitere Systeme machen, mit denen das betrachtete System verschränkt ist oder dynamisch wechselwirkt.

Wir denken bei einer Entwicklung immer an einen spezifischen äußeren Eingriff und beschreiben seine Auswirkung auf einen beliebigen Dichteoperator. Der Eingriff kann z. B. darin bestehen, dass Quantenobjekte einen wohlbestimmten verrauschten Kanal passieren oder dass an ihnen eine spezielle unscharfe Messung durchgeführt wird. Welche mathematische Struktur hat die Beschreibung der allgemeinen Zustandsentwicklung offener Systeme?

Die Entwicklung wird im Schrödinger-Bild durch eine für sie spezifische Abbildung des Anfangszustands ρ (mit $\text{tr}[\rho] = 1$) in einen als Dichteoperator formulierten Endzustand $\tilde{\rho}'$ im Liouville Raum beschrieben (*In-out-Schema*):

$$\rho \rightarrow \tilde{\rho}' = \mathcal{E}(\rho) . \quad (14.1)$$

Durch die Tilde wird gekennzeichnet, dass auch unnormierte Zustände ($\text{Spur} \neq 1$) zugelassen sind. Wenn wir an Gemenge denken, ist es plausibel zu fordern, dass die Wirkung von \mathcal{E} auf den einzelnen Zuständen eines Ensembles mit der auf dem Dichteoperator übereinstimmt.

\mathcal{E} ist daher ein positiver Superoperator. Superoperatoren sind nach Abschn. 1.2 gemäß Definition linear.

Wir werden allerdings nicht fordern, dass \mathcal{E} die Spur des Dichteoperators erhält, sonst hätten wir bereits die Projektionen, die im Rahmen der projektiven Messung einer Observablen auftreten, ausgeschlossen. Wenn man die verallgemeinerte Messung aus Abschn. 13.3 als Wirkung eines Superoperators schreibt, dann hat sie die Form

$$\rho \rightarrow \tilde{\rho}' = \mathcal{E}(\rho) = M_m \rho M_m^\dagger \quad (14.2)$$

und mit $\text{tr}[\rho] = 1$ ist $\text{tr}[\tilde{\rho}] < 1$ (vergl. Abschn. 13.3.2 und insbesondere Gl. (13.33)). Wir fordern daher nur, dass die Spur des Dichteoperators nicht vergrößert wird:

$$\text{tr}[\mathcal{E}(\rho)] \leq 1 \quad \text{bei } \text{tr}[\rho] = 1. \quad (14.3)$$

Als Drittes tritt die Forderung der *vollständigen Positivität* (complete positivity) von \mathcal{E} hinzu. Durch sie wird verlangt, dass bei der Abbildung (14.1) nicht nur die Positivität des Dichteoperators erhalten bleibt, sondern darüber hinaus Folgendes gilt: Wenn man zum betrachteten System S^A ein beliebiges weiteres System S^B mit Hilbert-Raum \mathcal{H}^B hinzunimmt und den Superoperator \mathcal{E}^A der Entwicklung von S^A trivial in der Form $\mathcal{E}^A \otimes \mathbb{1}^B$ zum Entwicklungsoperator des zusammengesetzten Systems S^{AB} erweitert, dann soll auch $\mathcal{E}^A \otimes \mathbb{1}^B$ wieder ein positiver Superoperator auf $\mathcal{H}^A \otimes \mathcal{H}^B$ sein. Physikalische bedeutet das: Wenn nur S^A eine dynamische Entwicklung durchläuft, dann soll garantiert sein, dass dabei der Dichteoperator des Zustands eines Gesamtsystems S^{AB} wieder (eventuell nach Normierung) in einen Dichteoperator übergeht. Das ist zu fordern, da nicht ausgeschlossen werden soll, dass das betrachtete System S^A offen und damit ein Teilsystem eines größeren Systems ist. In diesem Fall könnte durch die Einwirkung \mathcal{E}^A auf S^A z. B. über eine Wechselwirkung oder eine Verschränkung das Gesamtsystem S^{AB} beeinflusst werden. Alle diese Einflüsse sollen wieder vom erlaubten Typ sein.

Wir fassen zusammen: *Die allgemeinen Entwicklungen eines Quantensystems, die im Schrödinger-Bild Anfangszustände ρ in Endzustände $\tilde{\rho}'$ überführen, sind Quantenoperationen \mathcal{E} .* Eine *Quantenoperation* (quantum operation) ist eine durch einen Superoperator \mathcal{E} beschriebene

- (i) lineare,
- (ii) die Spur nicht erhöhende,
- (iii) vollständig positive Abbildung

$$\rho \rightarrow \tilde{\rho}' = \mathcal{E}(\rho). \quad (14.4)$$

Der Endzustand ρ' ergibt sich, wenn nötig, durch Normierung

$$\rho' = \frac{\mathcal{E}(\rho)}{\text{tr}[\mathcal{E}(\rho)]}. \quad (14.5)$$

Wir wollen vom Ausgangszustand $\text{tr}[\rho] = 1$ annehmen, sodass Bedingung (ii) $\text{tr}[\mathcal{E}(\rho)] \leq 1$ besagt.

14.1.2 Operatorsummenzerlegung von Quantenoperationen

Wir formulieren hier ein Theorem über Quantenoperationen an, das wir in Kap. 16 beweisen werden. Es ist der *Satz von der Operatorsummenzerlegung (operator-sum decomposition)*: Eine Abbildung $\rho \rightarrow \rho' = \mathcal{E}(\rho)$ ist genau dann eine Quantenoperation, wenn es für sie eine Zerlegung (bzw. Darstellung)

$$\mathcal{E}(\rho) = \sum_i K_i \rho K_i^\dagger \quad (14.6)$$

mit linearen Operatoren K_i gibt, die die Bedingung

$$\sum_i K_i^\dagger K_i \leq \mathbb{1} \quad (14.7)$$

erfüllen und den Eingangs-Hilbert-Raum in den Ausgangs-Hilbert-Raum abbilden. Für

$$\sum_i K_i^\dagger K_i = \mathbb{1} \quad (14.8)$$

ist die Operation spurerhaltend. Die Zerlegung (14.6) ist nicht eindeutig. Der Satz heißt auch der *Satz (oder das Darstellungstheorem) von Kraus*. Die Operatoren K_i werden *Kraus-Operatoren* (Kraus operators) oder *Operationselemente* (operation elements) aber auch *Zerlegungsoperatoren* (decomposition operators) genannt. Wir haben ein Beispiel für eine Operatorsummenzerlegung in Abschn. 13.1.2 und 13.2 kennen gelernt.

Wir betrachten den einfachen Fall, dass ein zusammengesetztes System S^{AB} eine unitäre Entwicklung mit U^{AB} durchläuft. Um die zu U^{AB} gehörige Operatorsummenzerlegung für die Quantenoperation auf S^A zu erhalten, gehen wir von der Wirkung von U^{AB} auf den Zustand $\rho^{AB} = \rho^A \otimes |i^B\rangle\langle i^B|$ aus. Er wird in

$$\rho'^{AB} = U^{AB} |i^B\rangle\langle i^B| \rho^A \langle i^B| U^{AB\dagger} \quad (14.9)$$

überführt. Für den Zustand von S^A bedeutet das

$$\rho'^A = \text{tr}_B[\rho'^{AB}] = \sum_n \langle e_n^B | U^{AB} | i^B \rangle \rho^A \langle i^B | U^{AB\dagger} | e_n^B \rangle. \quad (14.10)$$

$\{|e_n^B\rangle\}$ ist dabei eine ONB von \mathcal{H}^B . Aus der Unitarität von U^{AB} folgt für

$$K_i := \langle e_i^B | U^{AB} | i^B \rangle \quad (14.11)$$

die Vollständigkeitsrelation

$$\sum_i K_i - i^\dagger K_i = \mathbb{1}. \quad (14.12)$$

Die Abbildung

$$\rho^A \rightarrow \rho'^A = \mathcal{E}(\rho^A) = \sum_i K_i \rho K_i^\dagger \quad (14.13)$$

ist eine Quantenoperation mit Kraus-Operatoren (14.11). Es folgt unmittelbar, dass zu gegebenem U^{AB} die Operatorsummenzerlegung nicht eindeutig ist. Wir werden in Kap. 16 zeigen, dass auch folgende Umkehrung gilt: *Zu jeder Quantenoperation \mathcal{E}^A auf S^A lässt sich nach Erweiterung zum System S^{AB} eine unitäre Transformation U^{AB} auf \mathcal{H}^{AB} finden, die für das Teilsystem S^A die Operation \mathcal{E}^A bewirkt.*

14.1.3 Quantenoperationen sind noch nicht die allgemeinsten Entwicklungen

Nicht alle positiven Abbildungen sind vollständig positiv. Ein Beispiel hierfür ist die *Transposition* (transposition) T^A in \mathcal{H}^A .

Mit Bezug auf die Rechenbasis $\{|n^A\rangle\}$ von \mathcal{H}^A ist sie als die Abbildung definiert, die $\rho^A = \sum_{n,m} \rho_{nm} |n^A\rangle\langle m^A|$ in

$$T^A(\rho^A) = (\rho^A)^{TA} := \sum_{n,m} \rho_{nm} |m^A\rangle\langle n^A| \quad (14.14)$$

überführt. Dies ist eine lineare und positive Abbildung. Aber ist sie auch vollständig positiv? Mit Bezug auf die Matrixdarstellung mit den Basen $\{|n^A\rangle\}$ und $\{|\mu^B\rangle\}$ von \mathcal{H}^A bzw. \mathcal{H}^B ist die *Teil-Transposition* in \mathcal{H}^A (partial transposition) $(T^A \otimes \mathbb{1}^B)\rho^{AB} =: (\rho^{AB})^{TA}$ durch die Abbildung von ρ^{AB}

$$\rho^{AB} \leftrightarrow \rho_{m\mu, n\nu} = \langle m^A, \mu^B | \rho^{AB} | n^A, \nu^B \rangle \quad (14.15)$$

in

$$(\rho^{AB})^{TA} \leftrightarrow \rho_{m\mu, n\nu}^{TA} = \rho_{n\mu, m\nu} \quad (14.16)$$

gegeben. Diese Teil-Transposition ist trivialerweise positiv auf allen separablen Dichteoperatoren

$$T^A \otimes \mathbb{1}^B (\rho^A \otimes \sigma^B) = (\rho^A)^{TA} \otimes \sigma^B. \quad (14.17)$$

Zu prüfen bleibt daher, ob das auch für verschränkte Zustände gilt.

Wir betrachten hierzu den Bell-Zustand

$$|\Phi_+^{AB}\rangle = \frac{1}{\sqrt{2}}(|0^A, 0^B\rangle + |1^A, 1^B\rangle) \quad (14.18)$$

und nummerieren die Rechenbasis in $\mathcal{H}^A \otimes \mathcal{H}^B$ durch:

$$\begin{aligned} |0^A, 0^B\rangle &\leftrightarrow 1, \\ |0^A, 1^B\rangle &\leftrightarrow 2, \\ |1^A, 0^B\rangle &\leftrightarrow 3 \\ |1^A, 1^B\rangle &\leftrightarrow 4. \end{aligned} \quad (14.19)$$

Dann ergibt sich als Matrixdarstellung

$$|\Phi_+^{AB}\rangle\langle\Phi_+^{AB}| \leftrightarrow \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}. \quad (14.20)$$

Darauf wenden wir die Vorschrift (14.16) an und erhalten in Matrixschreibweise

$$(\rho^{AB})^{T_A} \leftrightarrow \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \quad (14.21)$$

Man prüft leicht nach, dass diese Matrix die Eigenzustände $\frac{1}{2}$, $\frac{1}{2}$, $\frac{1}{2}$ und $-\frac{1}{2}$ hat. $(\rho^{AB})^{T_A}$ ist daher nicht positiv. *Die Transposition ist eine lineare positive Abbildung, die nicht vollständig positiv ist.* Das liegt in dem Beispiel daran, dass wir $T^A \otimes \mathbb{1}^B$ auf einen verschränkten Zustand angewendet haben.

Das führt auf die folgende Frage: Ist fehlende Positivität nach Anwendung von $T^A \otimes \mathbb{1}^B$ möglicherweise ein Kriterium, mit dem man die Nicht-Separabilität eines Zustands feststellen kann? Ein Theorem mit dieser Aussage gibt es tatsächlich für niedrige Dimensionen $\mathcal{H}_2^A \otimes \mathcal{H}_2^B$ und $\mathcal{H}_2^A \otimes \mathcal{H}_3^B$ (vergl. Abschn. 14.5). Mit seiner Hilfe kann festgestellt werden, ob Dichteoperatoren ρ^{AB} separabel sind.

14.1.4 Einfache Beispiele

Eine Projektion P_m , wie sie z.B. bei einer Messung auftritt, ist eine Quantenoperation $K = P_m$ mit $K^\dagger K < \mathbb{1}$. Sie erhält die Spur nicht. Eine unitäre Transformation U ist eine spurerhaltende Operation mit $K = U$. Wenn man unitäre Transformationen U_i mit der Wahrscheinlichkeit p_i auf ein System wirken lässt, entsteht wegen $\sum_i p_i = 1$ wieder eine Quantenoperation

$$\mathcal{E}(\rho) = \sum_i p_i U_i \rho U_i^\dagger. \quad (14.22)$$

Auch die Bildung der Teilspur ist eine Quantenoperation. Um das zu sehen, bilden wir den Operator K_i^{AB} , der von $\mathcal{H}^A \otimes \mathcal{H}^B$ auf \mathcal{H}^A in der folgenden Weise abbilden soll

$$K_i^{AB}(\psi^{AB}) = K_i^{AB} \left(\sum_j \alpha_j |a_j^A\rangle |e_j^B\rangle \right) = \alpha_i |a_i^A\rangle \quad (14.23)$$

$\{|e_j^B\rangle\}$ ist eine ONB von \mathcal{H}^B . Durch Wirkung auf die Basisvektoren von $\mathcal{H}^A \otimes \mathcal{H}^B$ überzeugt man sich von

$$\sum_i K_i^{AB\dagger} K_i^{AB} = \mathbb{1}^{AB}. \quad (14.24)$$

Damit ist

$$\mathcal{E}(\rho^{AB}) = \sum_i K_i^{AB} \rho^{AB} K_i^{AB\dagger} \quad (14.25)$$

eine Quantenoperation. Wir zerlegen ρ^{AB} dual nach der ONB $\{|l_n^A\rangle|e_i^B\rangle\}$ von \mathcal{H}^{AB} , wobei $\{|l_n^A\rangle\}$ eine ONB von \mathcal{H}^A ist. Die Wirkung von K_i^{AB} besteht dann gemäß Gl. (14.23) in

$$\mathcal{E}(\rho^{AB}) = \sum_j \langle e_j^B | \rho^{AB} | e_j^B \rangle. \quad (14.26)$$

14.1.5 Mehrdeutigkeit der Operatorsummenzerlegung

Wir lassen in \mathcal{H}_2 die folgenden zwei Quantenoperationen auf ein Qubit wirken:

$$\mathcal{E}_i(\rho) := \frac{1}{2}\rho + \frac{1}{2}\sigma_i\rho\sigma_i, \quad i = x, y, z \quad (14.27)$$

$$\hat{\mathcal{E}}_i(\rho) := \langle 0_i | \rho | 0_i \rangle | 0_i \rangle \langle 0_i | + \langle 1_i | \rho | 1_i \rangle | 1_i \rangle \langle 1_i |. \quad (14.28)$$

Mit $|0_i\rangle\langle 0_i| = (\mathbb{1} + \sigma_i)/2$ und $|1_i\rangle\langle 1_i| = (\mathbb{1} - \sigma_i)/2$ finden wir nach kurzer Umformung

$$\hat{\mathcal{E}}_i(\rho) = \mathcal{E}_i(\rho). \quad (14.29)$$

Die Wirkung beider Quantenoperationen ist gleich, obwohl die physikalischen Interpretationen von Gl. (14.27) und (14.28) völlig verschieden sind: In Gl. (14.27) werden auf ρ jeweils mit der Wahrscheinlichkeit $\frac{1}{2}$ entweder die unitären Transformationen $\mathbb{1}$ (d. h. keine Änderung) oder σ_i angewandt. Gl. (14.28) entspricht der nicht-selektiven Messung in der Rechenbasis $\{|0_i\rangle, |1_i\rangle\}$. Der Bloch-Vektor \mathbf{r} von ρ' liegt dementsprechend parallel zur i -Achse. Das kann man mit Gl. (14.28) und den Relationen von Kap. 3 leicht nachprüfen. Was passiert mit dem Bloch-Vektor, wenn alle drei Pauli-Operatoren σ_x, σ_y und σ_z statt nur einem Pauli-Operator σ_i wie in $\mathcal{E}_i(\rho)$ mit gleicher Wahrscheinlichkeit wirken? Wir kommen auf diese Frage in Abschn. 14.3.1 zurück.

14.2 Völlig allgemeine Messung und POVM

Messoperationen statt Messoperatoren In Abschn. 13.3 haben wir gesehen, dass verallgemeinerte Messungen jeweils durch einen Satz $\{M_m\}$ von Messoperatoren gegeben sind. Jeder zu einem einzelnen Messwert m gehörige dynamische Vorgang ist eine Quantenoperation

$$\rho \rightarrow \rho' = \mathcal{M}_m(\rho) = M_m \rho M_m^\dagger \quad (14.30)$$

mit nur einem Kraus-Operator M_m . Die Gl. (13.35) zeigt, dass

$$p(m) = \text{tr}[\mathcal{M}_m(\rho)] \quad (14.31)$$

die Wahrscheinlichkeit dafür ist, dass die Durchführung der Operation \mathcal{E}_m eintritt. Bei nicht-trivialen verallgemeinerten Messungen ($p_m < 1$) verkleinert daher die Operation zu einem Messwert m die Spur. Für den Zerlegungsoperator gilt:

$$M_m^\dagger M_m < \mathbb{1}. \quad (14.32)$$

Diese Überlegungen zu verallgemeinerten Messungen zeigen bereits, dass es einen noch allgemeineren Typ von Messungen geben muß, bei dem die Operatorsummenzerlegung der Messoperationen \mathcal{M}_m mehr als einen Summanden enthält. In Verallgemeinerung der Gl. (14.30) und (14.31) ergibt sich dann der der Zustand $\tilde{\rho}'_m$ nach der Messung als Ergebnis einer Quantenoperation mit einem Superoperator \mathcal{M}_m

$$\rho \rightarrow \tilde{\rho}'_m = \mathcal{M}_m(\rho) = \sum_i M_{m,i} \rho M_{m,i}^\dagger . \quad (14.33)$$

Der Laufbereich von i kann dabei vom Messwert m abhängen. Die Wahrscheinlichkeit für das Eintreten des Messwerts ist wieder

$$p(m) = \text{tr}[\mathcal{M}_m(\rho)] . \quad (14.34)$$

Aus $\sum_m p(m) = 1$ ergibt sich als Bedingung an die Zerlegungsoperatoren

$$\sum_{m,i} M_{m,i}^\dagger M_{m,i} = \mathbb{1} . \quad (14.35)$$

$\sum_m \mathcal{M}_m$ ist spurerhaltend.

POVM Es zeigt sich, dass die in Abschn. 13.4 vorgestellte POVM-Messung von vorneherein den Grad an Allgemeinheit hat, den wir für Messungen erst mit Einführung der Quantenoperationen in Gl. (14.33) und (14.34) erreicht haben. Jeder völlig allgemeinen Messung ist ein POVM $\{E_m\}$ über die positiven Operatoren

$$E_m := \sum_i M_{m,i}^\dagger M_{m,i} , \quad (14.36)$$

zugeordnet, die mit Gl. (14.35) die Vollständigkeitsrelation

$$\sum_m E_m = \mathbb{1} \quad (14.37)$$

erfüllen. Die Messwahrscheinlichkeit ergibt sich mit (14.34) in der Form

$$p(m) = \text{tr}[E_m \rho] . \quad (14.38)$$

14.3 Quantenkanäle

14.3.1 Depolarisierungskanal

Zur Beantwortung der am Ende von Abschn. 14.1.5 gestellten Frage führen wir in Erweiterung von Gl. (14.27) zusätzlich zu $K_0 = \sqrt{1-p} \mathbb{1}$ noch die drei Zerlegungsoperatoren

$$K_i = \sqrt{\frac{p}{3}} \sigma_i , \quad i = 1, 2, 3 \quad (14.39)$$

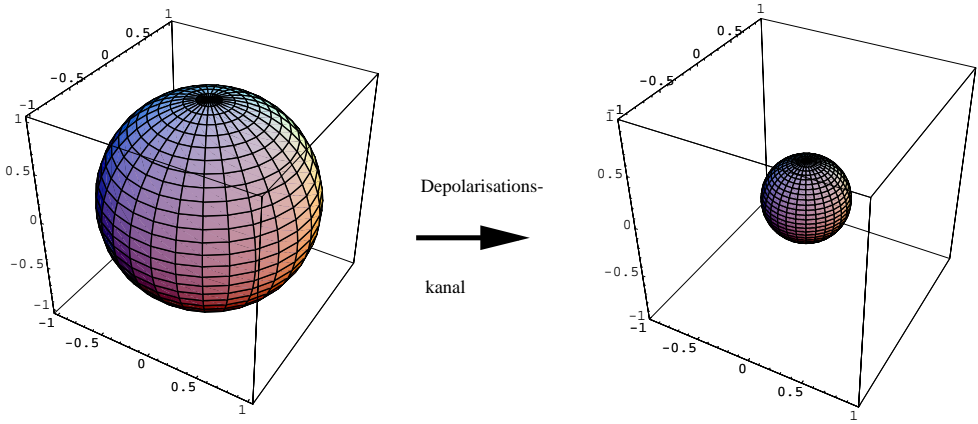


Abbildung 14.1: Auswirkung des Depolarisierungskanals auf die Bloch-Kugel.

ein mit $0 \leq p \leq 1$. $\mathcal{E}(\rho)$ ist dann

$$\mathcal{E}(\rho) = (1 - p)\rho + \frac{p}{3}(\sigma_1\rho\sigma_1 + \sigma_2\rho\sigma_2 + \sigma_3\rho\sigma_3). \quad (14.40)$$

Wir wollen die Wirkung von \mathcal{E} auf den Bloch-Vektor \mathbf{r} von ρ

$$\rho = \frac{1}{2}(\mathbb{1} + \mathbf{r}\boldsymbol{\sigma}) \quad (14.41)$$

beschreiben. Hierzu wählen wir die Koordinatenachsen so, dass $\mathbf{r} = r_3\mathbf{e}_3$ ist und erhalten

$$\rho = \frac{1}{2}(\mathbb{1} + r_3\sigma_3). \quad (14.42)$$

Mit $\sigma_3\sigma_3\sigma_3 = \sigma_3$, $\sigma_1\sigma_3\sigma_1 = -\sigma_3$ und $\sigma_2\sigma_3\sigma_2 = -\sigma_3$ können wir $\mathcal{E}(\rho)$ wieder in der Form (14.42) schreiben:

$$\mathcal{E}(\rho) = \frac{1}{2}(\mathbb{1} + r'_3\sigma_3), \quad r'_3 = \left(1 - \frac{4}{3}p\right)r_3. \quad (14.43)$$

Die Spinpolarisation $\mathbf{r} = \text{tr}[\rho\boldsymbol{\sigma}]$ wird reduziert. Man nennt das *Depolarisierung* (depolarization). In zentralsymmetrischer Weise werden alle Bloch-Vektoren einheitlich mit dem Faktor $(1 - \frac{4}{3}p)$ multipliziert (vergl. Abb. 14.1). Insbesondere werden dadurch reine Zustände zu Gemischen. Eliminieren von $r_3\sigma_3$ mit Hilfe von Gl. (14.42) überführt Gl. (14.43) in

$$\mathcal{E}(\rho) = \frac{4}{3}p\frac{\mathbb{1}}{2} + \left(1 - \frac{4}{3}p\right)\rho \quad (14.44)$$

Mit wachsendem p wächst der strukturlose Anteil $\frac{1}{2}\mathbb{1}$.

14.3.2 Quantensprünge und Amplitudendämpfungskanal

Ein 2-Niveau-Atom S^A mit Grundzustand $|0^A\rangle$ und angeregtem Zustand $|1^A\rangle$ emittiert mit der Wahrscheinlichkeit p ein Photon (spontane Emission in den Zustand $|1^B\rangle$). Wenn kein Photon emittiert wird, ist das Photonensystem S^B im Zustand $|0^B\rangle$. Wir betrachten nur den Quantensprung, bei dem am Anfang kein Photon vorliegt ($|i^B\rangle = |0^B\rangle$). Absorption findet nicht statt. Dann lassen sich die Kraus-Operatoren wie in Abschn. 14.1.2 ablesen:

$$\begin{aligned} K_0 &= \langle 0^B | U^{AB} | 0^B \rangle = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{pmatrix} \\ K_1 &= \langle 1^B | U^{AB} | 0^B \rangle = \begin{pmatrix} 0 & \sqrt{p} \\ 0 & 0 \end{pmatrix}. \end{aligned} \quad (14.45)$$

Sie erfüllen

$$K_0^\dagger K_0 + K_1^\dagger K_1 = \mathbb{1}. \quad (14.46)$$

Der Superoperator hat damit die Wirkung

$$\begin{aligned} \mathcal{E}(\rho^A) &= K_0 \rho^A K_0^\dagger + K_1 \rho^A K_1^\dagger \\ &= \begin{pmatrix} \rho_{00} + p\rho_{11} & \sqrt{1-p} \rho_{01} \\ \sqrt{1-p} \rho_{10} & (1-p)\rho_{11} \end{pmatrix} \end{aligned} \quad (14.47)$$

Die Matrixelemente von ρ^A werden gedämpft.

Für viele Atome kann der Prozess häufig stattfinden. Es ist immer wieder \mathcal{E} auf den jeweils resultierenden Zustand ρ'^A anzuwenden. Die Wahrscheinlichkeit, alle Atome im Grundzustand zu finden, wächst an. Das Gemisch geht in den reinen Zustand $|0^A\rangle\langle 0^A|$ über. Da die Komponente $\langle 1 | \rho^A | 1 \rangle$ weggedämpft wird, heißt der Kanal *Amplitudendämpfungskanal* (amplitude damping channel). Für die Auswirkung auf die Bloch-Kugel vergl. Abb. 14.2.

14.4 Blick zurück: Das Szenario und die Regeln der Quantentheorie

Szenario Wir haben einleitend in Abschn. 2.1.1 das Szenario der Quantentheorie beschrieben. Wir kommen im Rückblick noch einmal darauf zurück. Jedes Experiment in der Quantenphysik hat genauso wie jedes Experiment in der klassischen Physik den folgenden Aufbau: Ein physikalisches System unterliegt drei Typen von Einwirkungen, die von drei Typen von Geräten verursacht werden (vergl. Abb. 14.3):

1. Ein *Präparationsgerät* (preparation apparatus) präpariert das System in einem bestimmten Zustand.
2. Ein *Transformationsapparat* (transformation apparatus) wirkt auf das System ein und ändert den Zustand ab (z. B. Einfluss eines äußeren Potentials, Wechselwirkung mit einem anderen System, Wechselwirkung unter Teilsystemen. Es können mehrere Transformationen „durchlaufen“ werden. Es kann auch gar kein Transformationsapparat vorhanden sein.

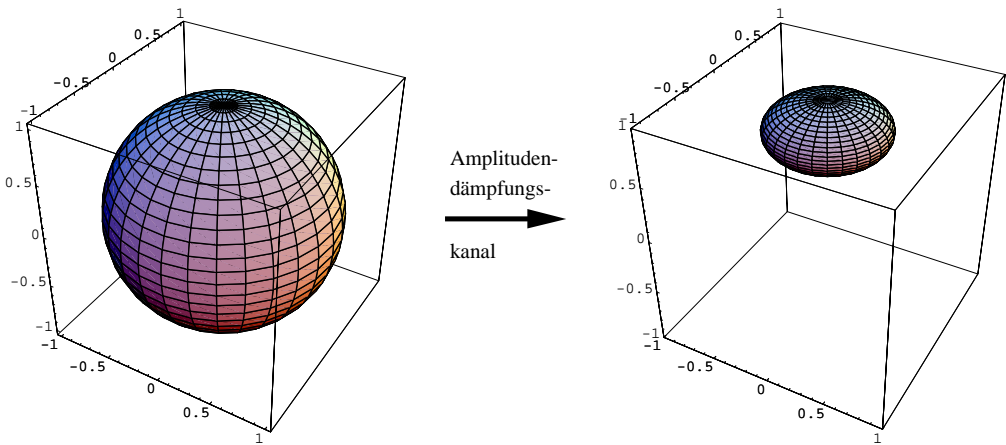


Abbildung 14.2: Auswirkung des Amplitudendämpfungs Kanals auf die Bloch-Kugel.

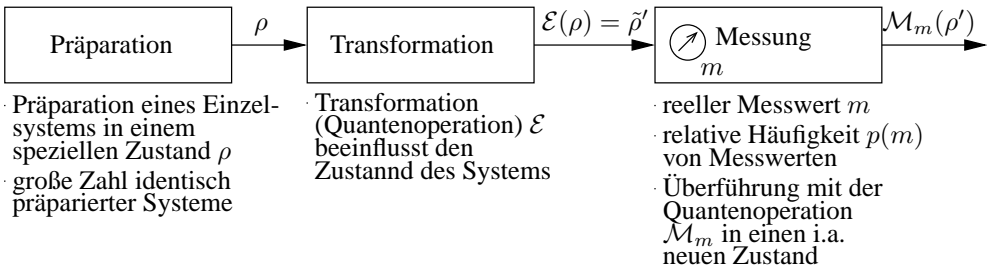


Abbildung 14.3: Das Szenario der Quantentheorie im Schrödinger-Bild.

3. Abschließend erfolgt im *Messgerät* eine Einwirkung, die dazu führt, dass an ihrem Ende am Messgerät ein *Messergebnis* (measurement outcome) in Form einer reellen Zahl abgelesen werden kann. Es ist möglich, dass das System durch die Messung nicht zerstört wird, sondern auch danach noch vorliegt. Dann wirkt das Messgerät auf den einlaufenden Zustand des Systems wie ein Transformationsapparat, das abhängig vom Messergebnis verschiedene Transformationen durchführt und in entsprechende Zustände überführt.

Regeln Zur Vereinfachung der Beschreibung haben wir dabei interpretierend schon vorausgesetzt, dass es stets einzelne physikalische Systeme gibt. In vielen Fällen misslingt der Versuch, die experimentellen Resultate mit Hilfe der Theorien der klassischen Physik zu erklären, und die Verwendung der (unrelativistischen) Quantentheorie ist erfolgreich. Dann werden die folgenden Regeln angewendet:

- Jedem Präparationsverfahren wird ein Zustand zugeordnet. Der Zustand ist dasjenige mathematische Objekt, das erlaubt die Wahrscheinlichkeiten des Eintretens der verschiedenen Messergebnisse für alle Arten von Messungen zu prognostizieren, die an den ent-

sprechend präparierten Quantensystem durchgeführt werden können. Wahrscheinlichkeit wird dabei üblicherweise als Grenzwert der relativen Häufigkeit aufgefasst. Zustände sind Dichteoperatoren ρ auf einem Hilbert-Raum.

- Die Transformation ist eine Quantenoperation. Sie wird im Schrödinger-Bild durch einen linearen vollständig positiven Superoperator \mathcal{E} beschrieben

$$\rho \rightarrow \tilde{\rho}' = \mathcal{E}(\rho), \quad (14.48)$$

der die Spur von ρ nicht erhöht. Durch die Transformation ändern sich die Prognosen für die Messergebnisse.

- Ein durch einen Messapparat durchgeführter Messeingriff wird durch die Messwerte m und ein POVM $\{E_m\}$ repräsentiert

$$\sum_m E_m = \mathbb{1}. \quad (14.49)$$

Die Wahrscheinlichkeit bei Vorliegen des Zustands ρ das Messergebnis m zu erhalten, ist

$$p_m = \text{tr}[E_m \rho]. \quad (14.50)$$

- Wenn das Quantensystem beim Messeingriff nicht zerstört wird, geht es abhängig vom Messergebnis m in den unnormierten Zustand

$$\rho \rightarrow \tilde{\rho}'_m = \mathcal{M}_m(\rho) \quad (14.51)$$

über. Normierung führt auf den neuen Dichteoperator ρ'_m mit $\text{tr}[\rho'_m] = 1$. Diese Messoperationen werden durch lineare, vollständig positive Superoperatoren (Quantenoperationen) \mathcal{M}_m dargestellt, die die Spur verringern. Ihre Form ist für die jeweilige Messung spezifisch. Die Wahrscheinlichkeit für das Auftreten des Messwerts m ist

$$p_m = \text{tr}[\tilde{\rho}'_m], \quad \sum_m p_m = 1. \quad (14.52)$$

Die Operatorsummenzerlegung der Superoperatoren \mathcal{M}_m

$$\mathcal{M}_m(\rho) = \sum_i M_{m,i} \rho M_{m,i}^\dagger \quad (14.53)$$

führt auf den Zusammenhang

$$E_m = \sum_i M_{m,i}^\dagger M_{m,i} \quad (14.54)$$

mit dem POVM $\{E_m\}$. Die Bedingung (14.49) schränkt die linearen Operatoren $M_{m,i}$ ein. Eine selektive Messung (Aussondern nach dem Messergebnis) stellt wieder ein Präparationsverfahren dar.

14.5 Ergänzende Themen und weiterführende Literatur

- Siehe auch Abschn. 13.5.
- Quantenoperationen, Operatorsummenzerlegungen: [HK 69], [HK 70], [Kra 83], [Sch 96].
- Mit Hilfe der teilweisen Transposition $T^A \otimes \mathbb{1}^B$ (partial transposition) kann man feststellen, ob ein Dichteoperator ρ^{AB} separabel ist. Es gilt der Satz: *Ein Zustand ρ^{AB} in $\mathcal{H}_2^A \otimes \mathcal{H}_2^B$ oder $\mathcal{H}_2^A \otimes \mathcal{H}_3^B$ ist genau dann separabel, wenn die Teiltransposition auf einen positiven Operator führt.* Dieses Theorem ist ein wichtiger Ausgangspunkt für die Beantwortung der Frage, wie man bei Gemischen Verschränkung (Nicht-Separabilität) feststellen kann [HHH 01].
- Eine Axiomatik der Quantentheorie, die von dem in Abschn. 14.4 beschriebenen Szenario ausgeht, findet sich in [Har 01a], [Har 01b].
- Man beachte auch die Literaturangaben zu Kap. 13.

14.6 Übungsaufgaben

ÜA 14.1 [zu 14.1.2] Zeigen Sie, dass sich eine Quantenoperation \mathcal{E} , die auf den Dichteoperator eines Qubits wirkt, in der Form

$$\mathcal{E}(\rho) = \sum_{i,j=1}^3 a_{ij} \sigma_i \rho \sigma_j \quad (14.55)$$

mit $a_{ij} = a_{ij}^*$ schreiben lässt.

ÜA 14.2 [zu 14.1.5] Zeigen Sie in expliziter Rechnung, dass der Bloch-Vektor von ρ' von Gl. (14.29) parallel zur i-Achse liegt.

ÜA 14.3 [zu 14.3] Berechnen Sie die Wirkung des Amplitudendämpfungskanals auf den Dichteoperator

$$\rho = \frac{1}{2}(\mathbb{1} + \mathbf{r}\boldsymbol{\sigma}) . \quad (14.56)$$

Wie ändert sich der Bloch-Vektor \mathbf{r} ?

15 Dekohärenz und Ansätze für die Beschreibung des Quantenmessprozesses

Dekohärenz ist für Anwendungen ein Störeffekt, für das Verständnis des Quantenmessprozesses aber ein wichtiger Ansatz. Die durch Streuung bewirkte Dekohärenz gibt den Hinweis darauf, dass umgebungsinduzierte Dekohärenz der wesentliche Effekt beim Messprozess sein könnte. Das Herausbilden der klassischen Welt und das klassische Verhalten von Schrödingers Katze sind weitere Beispiele. Die Frage, ob das Quantenmessproblem heute bereits gelöst ist, wird anschließend behandelt.

15.1 Dekohärenz erzeugende Kanäle

15.1.1 Phasendämpfungskanal

Streuung als einfache Realisierung Wir betrachten ein Qubit-System S^A an dem ein Quantensystem S^B gestreut wird. Wir wollen die Streuung für unsere Beschreibung stark vereinfachen (vergl. Abb. 15.1). Wir nehmen dazu an, dass es zwei orthonormale Zustände $|0^A\rangle$ und $|1^A\rangle$ des Systems S^A gibt, die bei der Streuung keine Änderung erfahren (stabile Zustände). Das System S^B fällt im Zustand $|i^B\rangle$ ein. Bei der Streuung am Zustand $|0^A\rangle$ (bzw. $|1^A\rangle$) soll das gestreute System S^B in der räumlichen Asymptotik in den Zustand $|0^B\rangle$ (bzw. $|1^B\rangle$) übergehen. Diese Zustände von S^B sollen ein ONB in \mathcal{H}_3^B bilden. Wir wollen noch zulassen, dass mit der Wahrscheinlichkeit $1 - p$ das System S^B gar nicht gestreut wird und daher im Zustand $|i^B\rangle$ bleibt. Man kann sich unter $|0^A\rangle$ und $|1^A\rangle$ z. B. zwei Energieniveaus vorstellen und unter $|i^B\rangle$, $|0^B\rangle$ und $|1^B\rangle$ drei Impulszustände („Bahnen“).

Die Streuung ist ein unitärer Prozess des Gesamtsystems S^{AB} . Der Operator, der die Zustände in der Einlaufregion in die der Auslaufregion überführt, hat die Eigenschaften

$$\hat{U}^{AB}|0^A, i^B\rangle = \sqrt{1-p}|0^A, i^B\rangle + \sqrt{p}|0^A, 0^B\rangle \quad (15.1)$$

$$\hat{U}^{AB}|1^A, i^B\rangle = \sqrt{1-p}|1^A, i^B\rangle + \sqrt{p}|1^A, 1^B\rangle. \quad (15.2)$$

Wir kennen daher seine Wirkung auf Teilen der ONB von $\mathcal{H}_2^A \otimes \mathcal{H}_3^B$ und können den Operator zu einem unitären Operator auf $\mathcal{H}_2^A \otimes \mathcal{H}_3^B$ ergänzen.

$$\begin{aligned} U^{AB} = & \left(\sqrt{1-p}|0^A, i^B\rangle + \sqrt{p}|0^A, 0^B\rangle \right) \langle 0^A, i^B| \\ & + \left(\sqrt{1-p}|1^A, i^B\rangle + \sqrt{p}|1^A, 1^B\rangle \right) \langle 1^A, i^B| + \text{Rest}. \end{aligned} \quad (15.3)$$

Weitere duale Bildungen mit $\langle 0^A, i^B|$ oder $\langle 1^A, i^B|$ kommen im Rest nicht vor.

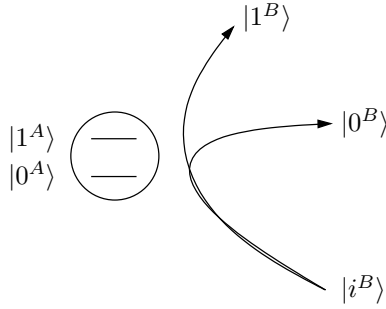


Abbildung 15.1: Streuung an einem 2-Niveau-System.

Die Kraus-Operatoren, die zu der auf dem Untersystem S^A wirkenden Quantenoperation gehören, lassen sich gemäß Gl. (14.11) direkt ablesen:

$$K_i = \langle i^B | U^{AB} | i^B \rangle = \sqrt{1-p} \mathbb{1}^A = \sqrt{1-p} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad (15.4)$$

$$K_0 = \langle 0^B | U^{AB} | i^B \rangle = \sqrt{p} |0^A\rangle \langle 0^A| = \sqrt{p} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad (15.5)$$

$$K_1 = \langle 1^B | U^{AB} | i^B \rangle = \sqrt{p} |1^A\rangle \langle 1^A| = \sqrt{p} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \quad (15.6)$$

Die Bedingung

$$K_i^\dagger K_i + K_0^\dagger K_0 + K_1^\dagger K_1 = \mathbb{1} \quad (15.7)$$

für Kraus-Operatoren ist erfüllt. Die Quantenoperation, die die Änderung des Systems S^A beschreibt, wenn es sich vor der Streuung im Zustand ρ befindet, ist durch

$$\rho \rightarrow \rho' = \mathcal{E}(\rho) = K_i \rho K_i + K_0 \rho K_0 + K_1 \rho K_1 \quad (15.8)$$

gegeben (der Index A ist weggelassen). In der Rechenbasis hat sie die Form

$$\rho' = \mathcal{E}(\rho) = \begin{pmatrix} \rho_{00} & (1-p)\rho_{01} \\ (1-p)\rho_{10} & \rho_{11} \end{pmatrix}. \quad (15.9)$$

Wenn Streuung mit Sicherheit stattfindet ($p = 1$), verschwinden in der Rechenbasis die Außerdiagonalelemente der Dichtematrix von S^A . Für $0 \leq p < 1$ werden mit jedem weiteren einzelnen Quantensystem S^E , das an S^A gestreut wird, die Außerdiagonalelemente um den Faktor $(1-p)$ kleiner. Streuung bewirkt Dekohärenz.

Phasendämpfungs kanal Im Grenzfall $p = 1$ (perfekte Streuung) wird durch eine Streuung eine Markierung mit orthogonalen Markerzuständen $|0^B\rangle$ und $|1^B\rangle$ durchgeführt. Ein reiner Zustand geht in einen verschränkten Zustand über

$$(c_0 |0^A\rangle + c_1 |1^A\rangle) |i^B\rangle \rightarrow c_0 |0^A, 0^B\rangle + c_1 |1^A, 1^B\rangle. \quad (15.10)$$

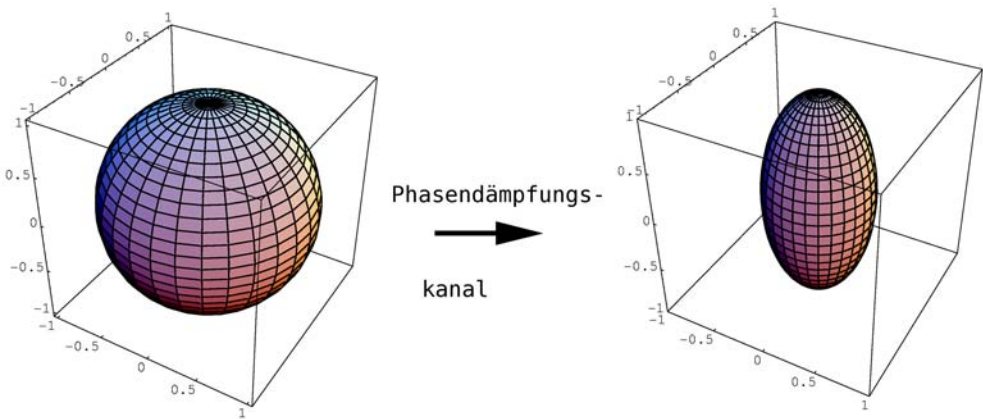


Abbildung 15.2: Auswirkung des Phasendämpfungskanals auf die Bloch-Kugel.

Der reine Zustand des Untersystems S^A geht in ein Gemisch über. Die Phasenbeziehung zwischen den Summanden des reinen Zustands und damit die Kohärenz, d. h. die Interferenzfähigkeit gehen verloren. Dies ist die Dekohärenz durch Markieren, die wir bereits in Abschn. 8.5 diskutiert haben. Das System S^A durchläuft für $0 \leq p \leq 1$ während der Streuung einen Quantenkanal, der *Phasendämpfungs kanal* (phase-damping channel) genannt wird. Die Auswirkung des Kanals auf beliebige Gemische kann man am einfachsten an der Bloch-Kugel demonstrieren. Man kann zeigen, dass die Bloch-Vektoren auf der z -Achse unverändert bleiben. Alle anderen Punkte bewegen sich für $p \neq 1$ bei vielen Streuungen auf die z -Achse zu unter Beibehaltung der Rotationssymmetrie um die z -Achse (vergl. Abb. 15.2).

15.1.2 Streuung und Dekohärenz

Charakteristische Eigenschaften Wir wollen Eigenschaften des oben beschriebenen Streuprozesses herausstellen, die wir in allgemeineren Situationen in denen Dekohärenz eine Rolle spielt, teilweise wiederfinden werden.

- Zunächst einmal muß festgehalten werden, dass der zu Grunde liegende Prozess, den das Gesamtsystem durchläuft, eine unitäre Entwicklung U^{AE} ist, die auf die spezielle Dynamik der Wechselwirkung zurückgeht. Ein reiner Zustand von S^{AB} geht in einen reinen Zustand von S^{AB} über. Information geht dabei nicht verloren.
- Dieser Streuprozess ist infolge der Unitarität reversibel. Wenn S^A am Anfang in einem reinen Zustand war, kann durch geeignete „Spiegelung“ (Umkehrung von Bewegung und Dynamik) der Streuprodukte wieder der reine Zustand erzeugt und die Dekohärenz von S^A vollständig rückgängig gemacht werden. Wie wir schon in Abschn. 9.1 gesehen haben, haben wir beim Übergang (15.10) Information in die Korrelationen transferiert, die dort im Prinzip wieder abgerufen werden kann. Dazu ist ein nicht-lokaler Prozess nötig, der bei Streuung praktisch nicht realisierbar ist.

- c) Wesentlich ist, dass durch die Wechselwirkung eine Basis $\{|0^A\rangle, |1^A\rangle\}$ aus stabilen Zuständen ausgezeichnet ist, die durch den dynamischen Einfluss nicht geändert werden (vergl. Gl. (15.9)).

$$\mathcal{E}(|0\rangle\langle 0|) = |0\rangle\langle 0|, \quad \mathcal{E}(|1\rangle\langle 1|) = |1\rangle\langle 1|. \quad (15.11)$$

- d) Diese Eigenzustände von σ_z zeichnen die Lage der z -Achse aus, auf die sich die Bloch-Kugel zusammenzieht (vergl. Abb. 15.2). Verglichen mit der Charakterisierung der Dekohärenz über das Verschwinden der Außendiagonalelemente des Dichteoperators, ist dies eine basisunabhängige Charakterisierung.
- e) Von c) her lässt sich schon vermuten, dass wir eine elastische Streuung beschrieben haben. Wenn die Zustände $|0\rangle$ und $|1\rangle$ zu Energieniveaus E_0 und E_1 gehören, dann kann man mit dem Hamilton-Operator

$$H = E_0|0\rangle\langle 0| + E_1|1\rangle\langle 1| \quad (15.12)$$

leicht zeigen, dass der Erwartungswert \bar{E} der Energie unverändert bleibt

$$\bar{E} = \text{tr}[\rho H] = \text{tr}[\rho' H] = \bar{E}'. \quad (15.13)$$

Es findet keine Dissipation statt.

- f) Wenn die Streuung nicht perfekt ist ($p \neq 1$), führt die vielfache Wiederholung mit immer neuen einfallenden Teilchen zu einer sich schrittweise verstärkenden Dekohärenz, die die Bloch-Vektoren orthogonal auf die z -Achse zutreibt.

15.1.3 Phasenflipkanal

Wir hatten bereits gesehen, dass es zu einer Quantenoperation viele Operatorsummenzerlegungen gibt. Physikalisch bedeutet das, dass bei gleichem Anfangszustand verschiedene dynamische Prozesse zu demselben Endzustand führen können. Wir können die Quantenoperation $\mathcal{E}(\rho)$ von Abschn. 15.1.1 und damit Dekohärenz auch durch einen *Phasenflipkanal* (phase-flip channel) erreichen, der ebenfalls geordnete Phasenbeziehungen zerstört. In ihm wirkt mit der Wahrscheinlichkeit w auf den Ausgangszustand ρ eine Dynamik ein, die eine unitäre Transformation σ_z und damit einen Phasenflip bewirkt. Die Quantenoperation hat daher die zwei Kraus-Operatoren

$$K_+ = \sqrt{w} \sigma_z, \quad K_- = \sqrt{1-w} \mathbb{1} \quad (15.14)$$

mit

$$K_+^\dagger K_+ + K_-^\dagger K_- = \mathbb{1}. \quad (15.15)$$

Die Operation ist in der Eigenbasis von σ_z durch

$$\begin{aligned} \rho \rightarrow \rho' &= w \begin{pmatrix} \rho_{11} & -\rho_{12} \\ -\rho_{21} & +\rho_{22} \end{pmatrix} + (1-w) \begin{pmatrix} \rho_{11} & \rho_{12} \\ \rho_{21} & \rho_{22} \end{pmatrix} \\ &= \begin{pmatrix} \rho_{11} & (1-2w)\rho_{12} \\ (1-2w)\rho_{21} & \rho_{22} \end{pmatrix} \end{aligned} \quad (15.16)$$

gegeben. Für $w = \frac{1}{2}$ tritt totale Dekohärenz auf. *Ein Kanal mit zufälligem Phasenflip ist in seiner Wirkung einem Phasendämpfungskanal äquivalent.*

15.2 Umgebungsinduzierte Dekohärenz

15.2.1 Die Herausbildung der klassischen Welt

Das Programm Wir haben in Abschn. 2.1.1 das Verhältnis am Doppelspalt einmal für Kugeln (also für klassische Objekte) und einmal für Atome (also für Quantenobjekte) beschrieben und die Unterschiede in den experimentellen Ergebnissen herausgestellt. Die theoretische Begründung wurde im einen Fall ganz im Rahmen der klassischen Physik gegeben und im anderen Fall ganz im Rahmen der Quantentheorie in der Fassung, wie sie noch einmal in Abschn. 14.4 zusammenfassend dargestellt wurde. Die Experimente am Doppelspalt legen folgende Fragen nahe: Was beobachtet man, wenn man ausgehend von Elektronen und Atomen über Moleküle und Viren zu immer makroskopischeren Objekten übergeht (vergl. Abschn. 15.6) um schließlich bei Tennisbällen zu enden? Kann in den unterschiedlichen Bereichen einschließlich der Ballexperimente eine unveränderte Quantentheorie zur Begründung herangezogen werden? Dann wäre letztlich die klassische Physik aus der Quantenphysik ohne Zusätze ableitbar. Oder tritt in einem Zwischenbereich eine ganz neue Physik auf, die auch eine neue Theorie erfordert?

Die Frage wie die klassische Physik aus der Quantentheorie hervorgeht, lässt sich wohl auch in naher Zukunft nicht völlig befriedigend beantworten. Es macht aber Sinn, Ansätze zur Lösung von Teilproblemen zu diskutieren. So kann ein Gefühl dafür entstehen, was die Quantentheorie in der bisher dargestellten Form zu begründen vermag und was nicht. Während wir in Kap. 10 mit Hilfe der verborgenen Parameter vergeblich versucht haben, Quantenphänomene aus der klassischen Physik heraus zu verstehen, drehen wir jetzt die Beweisrichtung um und versuchen die klassische Physik aus der Quantentheorie heraus zu verstehen.

Das Problem Eine für klassische mechanische Objekte charakteristische Eigenschaft ist die, dass sie nie in einer Superposition von zwei Zuständen beobachtet werden. Ein klassisches Objekt ist z. B. immer entweder an einem Ort 1 oder an einem Ort 2, aber nie in einer Superposition der beiden Ortszustände. Für den Doppelspalt bedeutet das, dass bei Experimenten mit klassischen Objekten keine Interferenz auftreten kann¹. Die für Quantenobjekte mögliche Superposition und damit die Kohärenz der Zustände ist bei klassischen Objekten unmöglich. Wenn wir daher versuchen, auch klassische Objekte mit Hilfe der Quantentheorie zu beschreiben, taucht das Problem auf, wie wir, ohne den Rahmen dieser Theorie zu verlassen, die Dekohärenz klassischer Zustände begründen können. Wir wollen die typisch klassische Eigenschaft, dass Zustände klassischer Objekte nicht superponieren, als eine *emergente Eigenschaft* (emergent property) ableiten. Der Phasendämpfungskanal zeigt, dass Verschränkung mit der Umgebung in Form von Streuung dabei eine Rolle spielen kann.

¹Für die Interferometrie mit Makromolekülen vergl. Abschn. 15.6.

Ein Beispiel Wir betrachten eine Kugel oder einen anderen makroskopischen Körper. Seine quantentheoretisch beschriebenen Ortszustände sollen $|0^A\rangle$ und $|1^A\rangle$ sein. Man kann sich darunter z. B. die Zustände hinter den einzelnen Spalten eines Doppelspalts vorstellen. Quantentheoretisch ist dann auch der Zustand

$$|\varphi^A\rangle = c_0|0^A\rangle + c_1|1^A\rangle \quad (15.17)$$

erlaubt, der auf ein Interferenzbild führen würde. Wir müssen berücksichtigen, dass die Kugel ein offenes System ist. Sie wechselwirkt ständig mit der Umgebung z. B. durch Streuung von Photonen. Selbst im Dunkeln bleibt die kosmische Hintergrundstrahlung präsent. $|0^A\rangle$ und $|1^A\rangle$ bleiben als klassische Zustände bei dieser Streuung unverändert (stabile Zustände). Damit haben wir eine Situation, die analog ist zu der bei der Streuung in Abschn. 15.1. Wenn die Kugel im Zustand $|0^A\rangle$ ist, wird das Photon mit der Nummer 1 in den Zustand $|0_1^E\rangle$ gestreut, entsprechend bei $|1^A\rangle$ in $|1_1^E\rangle$. Wie wir in Abschn. 15.1 gesehen haben, wird der Kugelzustand durch den reduzierten Dichteoperator

$$\rho^A = \begin{pmatrix} |c_0|^2 & c_0 c_1^* \langle 1_1^E | 0_1^E \rangle \\ c_0^* c_1 \langle 0_1^E | 1_1^E \rangle & |c_1|^2 \end{pmatrix} \quad (15.18)$$

beschrieben. Im Vergleich zu Gl. (15.9) haben wir $p = 1$ gesetzt, aber nicht die Orthogonalität der Streuzustände gefordert.

Es wird nicht nur ein Photon, sondern es werden ständig viele Photonen gestreut. Dementsprechend muss die Umgebung durch einen Produktraum $\mathcal{H}^E = \mathcal{H}_1^E \otimes \mathcal{H}_2^E \otimes \dots$ mit vielen Faktorräumen beschreiben werden. Die Umgebung hat viele Freiheitsgrade. Der verschränkte Zustand $|\psi^{AE'}\rangle$ des Gesamtsystems nach der Streuung ist

$$|\psi^{AE'}\rangle = c_1|0^A\rangle|0_1^E, 0_2^E, \dots\rangle + c_2|1^A\rangle|1_1^E, 1_2^E, \dots\rangle. \quad (15.19)$$

Der Zustand der Kugel ist durch den reduzierten Dichteoperator

$$\rho'^A = \begin{pmatrix} |c_0|^2 & c_0 c_1^* \langle 1_1^E | 0_1^E \rangle \langle 1_2^E | 0_2^E \rangle \dots \\ c_0^* c_1 \langle 0_1^E | 1_1^E \rangle \langle 0_2^E | 1_2^E \rangle \dots & |c_1|^2 \end{pmatrix} \quad (15.20)$$

gegeben. Die Kugeln an den verschiedenen Orten streuen Photonen in unterschiedlicher Weise, sonst würden wir sie ja auch gar nicht optisch unterscheiden können. Die Zustände $|0_j^E\rangle$ und $|1_j^E\rangle$ mit $j = 1, 2, 3, \dots$ sind daher alle sehr verschieden und es gilt $|\langle 0_j^E | 1_j^E \rangle| \ll 1$. Da sehr viele Photonen gestreut werden, tauchen in den Außerdiagonalelementen von ρ'^A in Gl. (15.20) sehr viele dieser dem Wert nach sehr kleinen inneren Produkte auf. Durch die Verschränkung mit den gestreuten Photonen geht der Zustand der Kugel in ein nicht mehr interferenzfähiges Gemisch über

$$\rho'^A \rightarrow |c_0|^2 |0^A\rangle \langle 0^A| + |c_1|^2 |1^A\rangle \langle 1^A|. \quad (15.21)$$

Dieser Dichteoperator stimmt mit dem eines Gemenges überein, bei dem die Kugel *entweder* mit der Wahrscheinlichkeit $|c_0|^2$ im Zustand $|0^A\rangle$ *oder* mit der Wahrscheinlichkeit $|c_1|^2$ im

Zustand $|1^A\rangle$ vorgefunden wird. Alle statistischen Aussagen über nachfolgende Messungen stimmen überein. Wir kommen im Zusammenhang mit dem Quantenmessproblem auf die Bedeutung dieser Aussage zurück.

Was wir hier für Kugeln gezeigt haben, gilt entsprechend für alle Systeme S^A , die (i) einer verschränkenden Wechselwirkung mit einem (Umgebungs-) System S^E unterliegen. Die Wechselwirkung soll (ii) gewisse Zustände von S^A unverändert lassen (stabile Zustände) und (iii) sie jeweils mit Zuständen von S^E verschränken, die sehr unterschiedlich (nahezu orthogonal) sind. *Die dann eintretende umgebungsinduzierte Dekohärenz (environment induced decoherence) ist umso größer, je mehr Freiheitsgrade das Umgebungssystem hat. Sie überführt in ein Gemisch aus den stabilen Zuständen. Dies sind die klassischen Zustände (classical states), da jede Superposition dieser Zustände – falls sie jemals auftreten sollte – sehr schnell durch Dekohärenz zerfällt.* Das „Umgebungs“-System S^E kann auch aus den inneren Freiheitsgraden eines makroskopischen Körpers bestehen.

15.2.2 Schrödingers Katze

Das Experiment E. Schrödinger [Sch 35] hat folgendes Experiment beschrieben (vergl. Abb. 15.3): Eine Katze ist zusammen mit einem radioaktiven Präparat in einen abgeschlossenen undurchsichtigen Kasten gesperrt. Innerhalb von einer Stunde soll mit einer Wahrscheinlichkeit $\frac{1}{2}$ ein einzelner Zerfall stattfinden. Der Zerfall bewirkt, dass ein Fläschchen Blausäure zertrümmert und die Katze getötet wird. Wenn man sich darauf beschränkt die Erfahrungen zu beschreiben, die ein Experimentalphysiker bei diesem Experiment macht, tritt keinerlei Problem auf: Der Versuch mit der Katze im Kasten wird mit vielen Katzen und Kästen durchgeführt. Jeweils wird nach einer Stunde nachgeschaut bzw. gemessen, ob die Katze lebt oder tot ist. Man stellt fest, dass sie in der Hälfte der Fälle tot und in der anderen Hälfte lebendig ist.

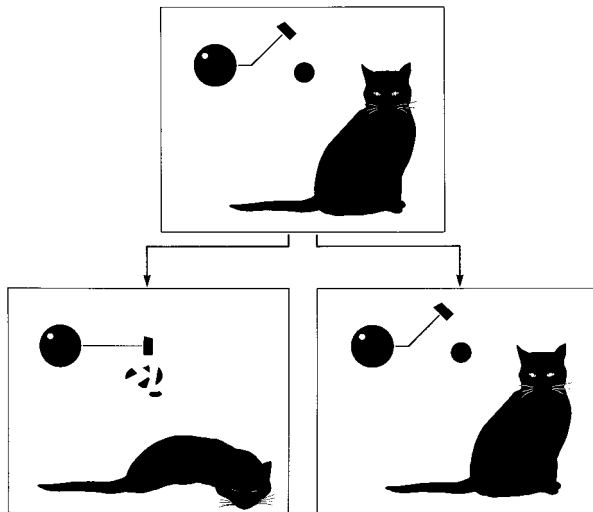


Abbildung 15.3: Nach Öffnen des Kastens findet man Schrödingers Katze mit der Wahrscheinlichkeit $1/2$ entweder lebend oder tot. (Aus: Audretsch/Mainzer: *Wieviele Leben hat Schrödingers Katze?* 1990 ©Elsevier GmbH, Spektrum Akademischer Verlag, Heidelberg.)

Tote Katzen zum Leben erwecken Wenn man die Quantentheorie auch auf die Katze anwendet und ihr einen Quantenzustand $|\text{lebt}\rangle$ bzw. $|\text{tot}\rangle$ zuordnet, entsteht zunächst noch kein Problem. Die Katze befindet sich vor der Messung, also bevor jemand den Kasten öffnet und nachschaut, in einer Superposition aus „lebendig“ und „tot“ mit Markierung (vergl. Abb. 15.4)

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\text{lebt}\rangle|\text{nicht zerfallen}\rangle + e^{i\phi}|\text{tot}\rangle|\text{zerfallen}\rangle) . \quad (15.22)$$

Das mag ungewohnt erscheinen, aber das oben geschilderte Experiment, bei dem am Ende an der Katze „lebendig“ oder „tot“ gemessen wird, wird völlig korrekt beschrieben.

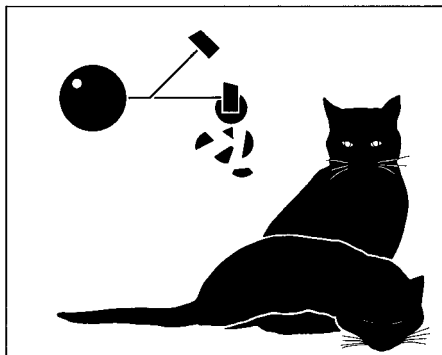


Abbildung 15.4: Liegt vor Öffnen des Kastens eine Superposition der Quantenzustände mit lebender und toter Katze vor? (Aus: Audretsch/Mainzer: Wieviele Leben hat Schrödingers Katze? 1990 ©Elsevier GmbH, Spektrum Akademischer Verlag, Heidelberg.

Wesentlich ist, dass sich Katze und Präparat im Zustand (15.22) in einer kohärenten Superposition befinden. Superposition kann auf Interferenz führen, wie wir das bei der Welcher-Weg-Markierung und dem Quantenradieren gesehen haben. Es ist also nicht ausgeschlossen, dass es eine andere Messung als „lebendig“ oder „tot“ gibt, bei der eine Interferenz zwischen lebender und toter Katze registriert wird. Eine solche Interferenz hat man weder bei Kugeln noch bei Katzen jemals gesehen.

Schlimmer noch. Wenn es Katzenzustände $|\varphi\rangle = \frac{1}{\sqrt{2}}(|\text{lebt}\rangle + |\text{tot}\rangle)$ gäbe, wäre Folgendes möglich: Man nimmt ein Ensemble von Katzen im Zustand $|\text{tot}\rangle$ und führt eine Projektionsmessung mit der Observablen $|\varphi\rangle\langle\varphi| - |\varphi_{\perp}\rangle\langle\varphi_{\perp}|$ mit $|\varphi_{\perp}\rangle = \frac{1}{\sqrt{2}}(|\text{lebt}\rangle - |\text{tot}\rangle)$ durch. Diese Observable gäbe es dann ebenfalls. Durch eine anschließende Messung der Observablen $|\text{lebt}\rangle\langle\text{lebt}| - |\text{tot}\rangle\langle\text{tot}|$ wird in 50% der Fälle die Katze in den Zustand $|\text{lebt}\rangle$ überführt. Man könnte also tote Katzen zum Leben erwecken. Bei Zuständen von Katzen ist daher eine Superposition nicht möglich. Wir hatten schon in Abschn. 15.2.1 gesehen, dass die umgebungsinduzierte Dekohärenz das verhindert. Sie überführt in ein Gemisch aus den stabilen Zuständen $|\text{lebt}\rangle|\text{nicht zerfallen}\rangle$ und $|\text{tot}\rangle|\text{zerfallen}\rangle$.

15.3 Quantenmessprozess*

15.3.1 Das Forschungsprogramm*

Seit ihren Anfängen ist die Quantentheorie nach einem dualistischen dynamischen Schema aufgebaut: Es gibt einerseits die Quantenoperationen, die das Verhalten des Systems zwischen Präparation und Messung beschreiben, und andererseits die Quantenoperationen der Messung. Im einfachsten Fall sind das unitäre Transformationen bzw. Projektionen. Von vielen wird es für unbefriedigend gehalten, zwei verschiedene Dynamiken zu postulieren. Daraus ist das Forschungsprogramm entstanden, die bisher als Postulat eingeführte Messdynamik so weitgehend wie möglich oder vielleicht sogar vollständig auf die unitäre Dynamik der Wechselwirkung zwischen System und Messapparat zurückzuführen. Die folgenden Forderungen sind dabei zu erfüllen:

- (i) Zu verschiedenen Observablen wie Energie, Spin usw. gehören verschiedene Messgeräte und verschiedene Einwirkungen auf das System. Es muss aus der dynamischen Entwicklung hervorgehen, welche Observable durch den Apparat gemessen wird.
- (ii) Der Zeigerzustand, der sich als Ergebnis einer Messung eingestellt hat, darf sich zeitlich nicht mehr verändern.
- (iii) Zeiger sind klassische Systeme. Es muss sich ergeben, dass sie nie in der Superposition verschiedener Stellungen auftreten.
- (iv) Die Rechnung muss wiedergeben, dass bei einer Einzelmessung immer genau eine Zeigerstellung von vielen möglichen realisiert ist, denn diese Aussage ist auch in den Messpostulaten enthalten. Das Ergebnis der Messung soll angezeigt werden. Es wird allerdings keine deterministische Begründung dafür verlangt, welche der Zeigerstellungen eintritt.

15.3.2 Vormessung*

Wir betrachten der Einfachheit halber als System S^A , an dem die Messung durchgeführt werden soll, ein Qubit-System und einen quantentheoretisch beschriebenen Messapparat S^M , dessen Hilbert-Raum \mathcal{H}^M ebenfalls die Dimension zwei hat. Die unitäre Messwechselwirkung auf $\mathcal{H}^A \otimes \mathcal{H}^M$, die zur Messung mit den Eigenzuständen $|0^A\rangle$ und $|1^A\rangle$ von S^A gehört, soll markierende Wirkung haben (vergl. Abschn. 8.5). Bei Vorliegen von $|0^A\rangle$ (bzw. $|1^A\rangle$) soll der Messapparat in den Zustand $|0^M\rangle$ (bzw. $|1^M\rangle$) übergehen. Für den allgemeinen Zustand $|\varphi^A\rangle = c_0|0^A\rangle + c_1|1^A\rangle$ von S^A bedeutet das die Verschränkung mit den Zuständen des Messapparats:

$$|\phi^{AM}\rangle = |\varphi^A\rangle|i^M\rangle = (c_0|0^A\rangle + c_1|1^A\rangle)|i^M\rangle \quad (15.23)$$

$$\rightarrow |\phi'^{AM}\rangle = c_0|0^A\rangle|0^M\rangle + c_1|1^A\rangle|1^M\rangle. \quad (15.24)$$

$|i^M\rangle$ ist ein Anfangszustand von S^M . Diese dynamische Entwicklung wird oft als *Vormessung* (pre-measurement) bezeichnet.

*Die mit einem Stern gekennzeichneten Kapitel können bei einem ersten Durchgang überschlagen werden.

Die Zerlegung des resultierenden Zustands $|\phi'^{AM}\rangle$ nach einer Basis von $\mathcal{H}^A \otimes \mathcal{H}^M$ ist nicht eindeutig. Für $c_0 = c_1 = \frac{1}{\sqrt{2}}$ liegt der Bell-Zustand $|\Phi_+^{AM}\rangle$ vor, den wir auch in der Form

$$|\phi'^{AM}\rangle = |\Phi_+^{AM}\rangle = \frac{1}{\sqrt{2}} (|0_x^A\rangle|0_x^M\rangle + |1_x^A\rangle|1_x^M\rangle) \quad (15.25)$$

schreiben können. Es gibt beliebig viele weitere Kombinationen von dieser Struktur. Wenn $|\phi'^{AM}\rangle$ der Zustand sein soll, bei dem der Messapparat die Observable

$$Z^A = z_0|0^A\rangle\langle 0^A| + z_1|1^A\rangle\langle 1^A| \quad (15.26)$$

gemessen hat, dann kann man den Apparat auch ebenso als einen Apparat zur Messung der Observablen $X^A = x_0|0_x^A\rangle\langle 0_x^A| + x_1|1_x^A\rangle\langle 1_x^A|$ ansehen. Es liegt also bisher gar nicht fest, welche Observable bei der unitären Entwicklung (15.23) letztlich gemessen wird. Oder anders betrachtet: Wenn $|0^A\rangle$ und $|1^A\rangle$ die klassischen Zeigerzustände sind, dann ist nicht ausgeschlossen, dass als Ergebnis der Vormessung die Markierung mit den Superpositionen von Zeigerzuständen erfolgt. Die Forderung (i) ist bisher nicht erfüllt. Mit Blick auf Abschn. 15.2.1 liegt die Vermutung nahe, dass durch Berücksichtigung der Umgebung dieses Problem gelöst werden kann.

Auch die restlichen Forderungen werden durch die Vormessung nicht erfüllt. Wir demonstrieren das am Beispiel der Forderung (ii). Unitäre Entwicklungen sind umkehrbar. Andererseits ist der Messprozess aber irreversibel. Wir wollen das am Beispiel der einfachen unitären Entwicklung $U = e^{-iHt}$ mit dem Hamilton-Operator

$$H^{AM} = g \sigma_z^A \otimes \sigma_y^M \quad (15.27)$$

auf $\mathcal{H}^A \otimes \mathcal{H}^M$ untersuchen. Der Anfangszustand sei der Produktzustand

$$|\phi^{AM}(t=0)\rangle = (c_0|0^A\rangle + c_1|1^A\rangle) |0_x^M\rangle \quad (15.28)$$

mit $|c_0|^2 + |c_1|^2 = 1$. Eine Zwischenrechnung, die wir nicht wiedergeben (vergl. ÜA 15.1), führt auf

$$\begin{aligned} |\phi^{AM}(t)\rangle &= c_0|0^A\rangle \left\{ \sin\left(\frac{\pi}{4} + gt\right) |0^M\rangle + \cos\left(\frac{\pi}{4} + gt\right) |1^M\rangle \right\} \\ &+ c_1|1^A\rangle \left\{ \sin\left(\frac{\pi}{4} - gt\right) |0^M\rangle + \cos\left(\frac{\pi}{4} - gt\right) |1^M\rangle \right\}. \end{aligned} \quad (15.29)$$

Wir erhalten eine zeitabhängige Verschränkung, die zum Zeitpunkt $t = \frac{\pi}{4}g$ auf den gewünschten Zustand $|\phi'^{AM}\rangle$ von Gl. (15.23) führt. Zum Zeitpunkt $t = \frac{2\pi}{g}$ ist allerdings wieder der unverschränkte Anfangszustand $|\phi^{AM}(t=0)\rangle$ erreicht. Die Vormessung führt somit auf keine zeitlich stabile Markierung des Gesamtsystems.

15.3.3 Verschränkung mit der Umgebung fixiert die Observable*

Ein erster Schritt zur Lösung der Probleme besteht darin, die Systeme S^A und S^M um die Umgebung S^E zu erweitern, die zunächst aus einem einzigen Qubit-System bestehen soll.

Der Zustand des Gesamtsystems S^{AME} liegt in $\mathcal{H}^A \otimes \mathcal{H}^M \otimes \mathcal{H}^E$. Wir koppeln S^M an S^E über eine Dynamik mit einem Hamilton-Operator H^{ME} , der nur auf $\mathcal{H}^M \otimes \mathcal{H}^E$ wirkt und daher den Zustand von S^A nach der Vormessung unverändert lässt.

$$H^{ME} = g \mathbb{1}^A \otimes \sigma_z^M \otimes \sigma_z^E. \quad (15.30)$$

Die Zustände $|0^E\rangle$ und $|1^E\rangle$ bilden ein ONB von \mathcal{H}^E .

Der Anfangszustand zur Zeit $t = 0$ nach der Vormessung ist mit $|\phi'^{AM}\rangle$ von Gl. (15.23)

$$|\psi(t=0)\rangle = \{c_0|0^A\rangle|0^M\rangle + c_1|1^A\rangle|1^M\rangle\} (\alpha|0^E\rangle + \beta|1^E\rangle). \quad (15.31)$$

Die anschließend durch H^{ME} bewirkte unitäre Entwicklung führt auf eine zeitabhängige Verschränkung mit der Umgebung (vergl. ÜA 15.2)).

$$|\psi(t)\rangle = c_0|0^A\rangle|0^M\rangle|\omega_0^E(t)\rangle + c_1|1^A\rangle|1^M\rangle|\omega_1^E(t)\rangle \quad (15.32)$$

mit

$$|\omega_0^E(t)\rangle = \alpha \exp(igt)|0^E\rangle + \beta \exp(-igt)|1^E\rangle = |\omega_1^E(-t)\rangle. \quad (15.33)$$

Ist auch jetzt noch unbestimmt, welcher Zustand beim System S^A und beim Messapparat S^M vorliegt? Die Umformung von Gl. (15.23) in Gl. (15.25) für $c_0 = c_1 = \frac{1}{\sqrt{2}}$ ist nur dann möglich, wenn die Summanden keine unterschiedlichen Faktoren enthalten. Die Zustände $|\omega_0^E\rangle$ und $|\omega_1^E\rangle$ in Gl. (15.32) sind solche unterschiedlichen „Faktoren“. Die Verschränkung mit der nur aus einem Qubit bestehenden Umgebung hat bereits bewirkt, dass nur noch eine Korrelation zwischen den Eigenzuständen von σ_z^A und σ_z^M , aber nicht mehr zwischen denen von σ_x^A und σ_x^M besteht². Der Apparat mit der Messdynamik H^{ME} ist damit der Observablen Z^A zugeordnet. Die Forderung (i) ist erfüllt. Allerdings wird nach wie vor periodisch verschränkt und entschärft. Zur Zeit $t = \frac{2\pi}{g}$ liegt wieder der Ausgangszustand $|\psi(t=0)\rangle$ vor.

15.3.4 Verschränkung mit vielen Freiheitsgraden der Umgebung*

Kollaps und Wiederkehr Realistische Umgebungen haben sehr viele Freiheitsgrade. Es liegt also ein Gesamtsystem in einem Hilbert-Raum $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^M \otimes \mathcal{H}_{(1)}^E \otimes \dots \otimes \mathcal{H}_{(N)}^E$ vor. N ist dabei eine große Zahl. Wir diskutieren den einfachen Fall, dass alle Hilbert-Räume zweidimensional sind, und gehen wieder wie im vorigen Kapitel vor.

Vor Anschalten der Wechselwirkung zwischen Messapparat und Umgebung liegt der Zustand

$$|\psi(t=0)\rangle = \{c_0|0^A\rangle|0^M\rangle + c_1|1^A\rangle|1^M\rangle\} \otimes \left\{ \prod_{k=1}^N (\alpha_k|0_{(k)}^E\rangle + \beta_k|1_{(k)}^E\rangle) \right\} \quad (15.34)$$

²Mit Hilfe des folgenden Theorems lässt sich der Beweis noch präzisieren [Bub 97, Kap. 5.5]: Eine Darstellung eines Zustands $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}' \otimes \mathcal{H}''$ als *triorthogonale Zerlegung* (triorthogonal decomposition)

$$|\psi\rangle = \sum_i c_i |u_i\rangle |v_i\rangle |w_i\rangle$$

mit Basisvektoren $\{|u_i\rangle\} \in \mathcal{H}$, $\{|v_i\rangle\} \in \mathcal{H}'$ und $\{|w_i\rangle\} \in \mathcal{H}''$ existiert nicht immer. Aber wenn sie existiert, ist sie eindeutig.

mit $|\alpha_k|^2 + |\beta_k|^2 = 1$ vor. Die Wechselwirkung soll durch den einfachen Hamilton-Operator

$$H^{ME} = \sum_{k=1}^N H_k^{ME} \quad (15.35)$$

mit

$$H_k^{ME} := g_k \mathbb{1}^A \otimes \sigma_z^M \otimes \sigma_{z(k)}^E \otimes \prod_{j \neq k} \mathbb{1}_{(j)}^E \quad (15.36)$$

gegeben sein. Der Zustand $|\psi(t)\rangle$ des Gesamtsystems zur Zeit t erhalten wir über die zu \mathcal{H}^{ME} gehörige unitäre Transformation nach einer Zwischenrechnung (vergl. ÜA 15.2), bei der wir unmittelbar das Resultat (15.32) verwenden, als

$$|\psi(t)\rangle = c_0 |0^A\rangle |0^M\rangle |\Omega_0^E(t)\rangle + c_1 |1^A\rangle |1^M\rangle |\Omega_1^E(t)\rangle \quad (15.37)$$

mit

$$|\Omega_0^E(t)\rangle := \prod_{k=1}^N (\alpha_k \exp(ig_k t) |0_{(k)}^E\rangle + \beta_k \exp(-ig_k t) |1_{(k)}^E\rangle) =: |\Omega_1^E(-t)\rangle. \quad (15.38)$$

Die Umgebungszustände sind normiert $\langle \Omega_0^E(t) | \Omega_0^E(t) \rangle = 1$, $\langle \Omega_1^E(t) | \Omega_1^E(t) \rangle = 1$, aber i.a. nicht zu allen Zeiten orthogonal

$$r(t) := \langle \Omega_0^E(t) | \Omega_1^E(t) \rangle. \quad (15.39)$$

Zur Beschreibung der Auswirkung der Messung am System S^A durch das Messgerät S^M müssen wir durch Abspuren über die Freiheitsgrade der Umgebung zum reduzierten Dichteoperator des Systems S^{AM} übergehen.

$$\rho^{AM} = \text{tr}_E[|\psi(t)\rangle\langle\psi(t)|] = |c_0|^2 |0^A\rangle\langle 0^A| \otimes |0^M\rangle\langle 0^M| \quad (15.40)$$

$$\begin{aligned} &+ |c_1|^2 |1^A\rangle\langle 1^A| \otimes |1^M\rangle\langle 1^M| \\ &+ r(t) c_0 c_1^* |0^A\rangle\langle 1^A| \otimes |0^M\rangle\langle 1^M| \\ &+ r^*(t) c_0^* c_1 |1^A\rangle\langle 0^A| \otimes |1^M\rangle\langle 0^M|. \end{aligned} \quad (15.41)$$

Man findet leicht (vergl. ÜA 15.2) als explizite Zeitabhängigkeit von $r(t)$

$$r(t) = \prod_{k=1}^N \{ \cos 2g_k t + i(|\alpha_k|^2 - |\beta_k|^2) \sin 2g_k t \}. \quad (15.42)$$

Nach Konstruktion ist $r(t=0) = 1$ und $|r(t)|^2 \leq 1$.

Wichtig ist im Hinblick auf die Forderung (ii) das Verhalten von $r(t)$ für große Zeiten. Wie Gl. (15.42) zeigt, ist $r(t)$ aufgebaut aus periodischen Funktionen mit vielen verschiedenen Frequenzen $2g_k$. Es ist aus der statistischen Mechanik, aus der Quantenoptik und aus anderen Gebieten der theoretischen Physik bekannt, dass so zusammengesetzte Funktionen *Kollaps und Wiederkehr* (collapse and revival) zeigen. Beginnend bei $t = 0$ mit $r = 1$ fällt

$|r(t)|$ zunächst ab und nähert sich dem Wert Null, kann dann aber nach längerer Zeit wieder ansteigen, wieder auf Null abfallen, wieder ansteigen usw. $|r(t)|$ kann beliebig nahe an $|r(t)| = 1$ zurückkehren³. Mit wachsendem N wird diese *Rekohärenz* (recoherence) aber zu immer größeren Zeiten hin verschoben (vergl. Abb. 15.5).

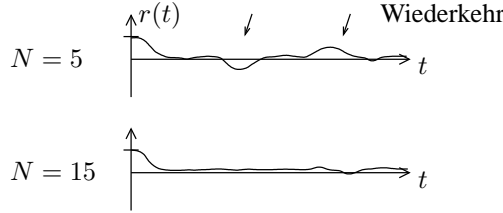


Abbildung 15.5: Kollaps und Wiederkehr (spezielle Parameterwahl).

$r(t)$ erreicht sehr schnell einen Wert proportional zu 2^{-N} (vergl. Abschn. 15.6). Wie Gl. (15.41) zeigt, entspricht dem ein sehr schneller Dekohärenzvorgang in den Basen $\{|0^A\rangle, |1^A\rangle\}$ und $\{|0^M\rangle, |1^M\rangle\}$. S^{AM} geht aus einem reinen Zustand in ein Gemisch ρ^{AB} über. Insbesondere die Markerzustände $|0^M\rangle$ und $|1^M\rangle$ können nicht mehr miteinander interferieren. Es sind klassische Zustände geworden, die man *Zeigerzustände* (pointer states) nennt. Damit ist auch die Forderung (iii) erfüllt.

Der von der Umgebung S^E induzierte Dekohärenzprozess hat beim reduzierten Dichteoperator ρ^{AM} die Basis der Zeigerzustände ausgezeichnet. Das Ergebnis ist für das Teilsystem S^{AM} der reduzierte Dichteoperator

$$\rho^{AM} = |c_0|^2 |0^A, 0^M\rangle \langle 0^A, 0^M| + |c_1|^2 |1^A, 1^M\rangle \langle 1^A, 1^M|. \quad (15.43)$$

Ein Gemenge aus den Zuständen $|0^A, 0^M\rangle$ und $|1^A, 1^M\rangle$ aus $\mathcal{H}^A \otimes \mathcal{H}^M$ mit den Wahrscheinlichkeiten $p_0 = |c_0|^2$ und $p_1 = |c_1|^2$ wird ebenfalls durch den Dichteoperator ρ^{AM} beschrieben. Ein solches Gemenge entspricht gemäß Messpostulat genau dem Ergebnis einer nicht-selektiven Messung der Observablen Z^A . Sind damit alle Anforderungen aus Abschn. 15.3.1 erfüllt?

Welche Zeigerzustände? Mit dieser nur auf S^{AB} bezogenen reduzierten Betrachtungsweise, die von der Umgebung S^E absieht, ist die Argumentation allerdings noch unvollständig, denn wir haben dadurch wieder ein Problem mit Forderung (i) bekommen. Denn ρ^{AM} ist der reduzierte Dichteoperator eines verschränkten Teilsystems und damit nicht das Ergebnis eines Präparationsprozesses, der auf ein Gemenge führt. Eine Ignoranzinterpretation (vergl. Abschn. 4.3) ist nicht möglich. Das Gesamtsystem befindet sich in einem reinen Zustand. Der Dichteoperator ρ^{AM} hat beliebig viele Ensemblezerlegungen z. B. auch

$$\rho^{AM} = p_u |u^A, u^M\rangle \langle u^A, u^M| + p_v |v^A, v^M\rangle \langle v^A, v^M|. \quad (15.44)$$

³Wiederkehr kann man genauer fassen: \mathcal{H} sei ein endlich-dimensionaler Hilbert-Raum und U ein unitärer Operator. Dann gibt es zu jedem $\varepsilon > 0$ eine natürliche Zahl q , sodass $\sup\{\|U^q - \mathbb{1}|\varphi\rangle\| : |\varphi\rangle \in \mathcal{H}, \|\varphi\| = 1\} < \varepsilon$. Wenn man die Anwendung von U häufig genug wiederholt, kommt man dem Ausgangszustand wieder beliebig nahe. [SSS 04]

Ist daher möglicherweise eine ganz andere Observable $U^A = u|u^A\rangle\langle u^A| + v|v^A\rangle\langle v^A|$ mit Zeigerzuständen $|u^M\rangle$ und $|v^M\rangle$ gemessen worden.

Wir dürfen von der Umgebung nicht absehen. Wir wissen, dass beim Messprozess die Zeigerstellung stabil ist. Die Wechselwirkung mit der Umgebung ist ständig vorhanden. Wenn sie wie oben von der Form

$$H^{ME} = Z^M \otimes H^E \quad (15.45)$$

mit einem hermiteschen Operator H^E ist, dann vertauscht H^{ME} mit der *Zählerobservablen* (pointer observable) Z^M

$$[H^{ME}, Z^M]_- = 0. \quad (15.46)$$

Die Zustände $|0^M\rangle$ und $|1^M\rangle$ und damit auch die Korrelationen mit den Zuständen $|0^A\rangle$ und $|1^A\rangle$ bleiben unter dem Einfluss der Umgebung unverändert. Die Stabilität dieser Korrelationen zeichnet die Zeigerbasis $\{|0^M\rangle, |1^M\rangle\}$ vor anderen Basen aus.

Die Diagonalisierung von ρ^{AB} durch umgebungsinduzierte Dekohärenz und die Stabilität der Korrelationen zwischen S^A und S^M unter fortdauerndem Einfluss der Umgebung führt auf die Festlegung der zeitlich unveränderlichen klassischen Zeigerzustände. Z^A liegt als gemessene Observable ebenfalls fest. Damit sind die Forderungen (i) bis (iii) an eine dynamische begründende Theorie des Messprozesses für die nicht-selektive Messung in diesem sehr einfachen Modell durch die Ankopplung an die Umgebung weitgehend erfüllt. Die Verschränkung mit der Umgebung S^E ist allerdings nicht durchbrochen wie die Möglichkeit der „Wiederkehr“ in sehr ferner Zukunft zeigt. Durch ρ^{AM} wird kein Gemenge beschrieben. Eine Ignoranzinterpretation (vergl. Abschn. 4.3) ist nicht möglich. Das Urteil darüber, ob das als ein gravierender Mangel des Erklärungsmodelles anzusehen ist, bleibt dem Leser überlassen.

15.4 Ist das Messproblem gelöst?*

Ein weiterer damit zusammenhängender gravierender Mangel liegt in jedem Fall vor: Die Forderung (iv) von Abschn. 15.3.1 ist nicht erfüllt. Umgebungsinduzierte Dekohärenz kann nicht erklären, warum in jedem Einzelexperiment immer nur eine von vielen möglichen Zeigerstellungen eines Messapparats realisiert ist. Das ist aber gerade die elementarste Erfahrung, die ein messender Experimentator noch vor allen anderen Erfahrungen macht. Sie ist Teil der Messpostulate. *Das Messproblem ist daher (in der Standardinterpretation) nicht gelöst.*

Verlangt ist allerdings keine deterministische Begründung dafür welche Zeigerstellung eintritt. Das würde auf die verborgenen Parameter zurückführen. Die Erklärungslücke betrifft typischerweise einen Einzelprozess und damit als Konsequenz die selektive Messung überhaupt, da sie auf Einzelmessungen aufbaut. Mit dem Zustand ρ^{AM} des vorigen Kapitels haben wir ein Gemisch erhalten, Wenn man das als Ergebnis einer nicht-selektiven Messung und also als ein Gemenge interpretiert, hat man bereits vorausgesetzt, dass die Forderung (iv) erfüllt werden konnte.

Es ist offenbar so, dass man die in den Messpostulaten enthaltene Forderung (iv) im Rahmen der vorliegenden Quantentheorie einschließlich der Standardinterpretation dynamisch nicht begründen kann. Wenn das so ist, hat man zwei Möglichkeiten: Man kann einmal die

Quantentheorie abändern, indem man z. B. andere dynamische Gleichungen postuliert (vergl. Abschn. 15.6). Die zweite Möglichkeit besteht darin, die Theorie in der bestehenden mathematischen Formulierung unverändert zu lassen und zu einer anderen Interpretation für sie überzugehen. Wir wollen ein Beispiel hierfür sehr kurz skizzieren.

15.5 Die Viele-Welten-Interpretation*

Die *Viele-Welten-Interpretation* (many-worlds interpretation), die auch *Everett*⁴-*Interpretation* (Everett interpretation) genannt wird, bezieht den Beobachter als System mit ein. Er entspricht formal dem System S^M aus Abschn. 15.3.2. Wir wollen im Folgenden S^M so verstehen. Wie in der Vormessung entwickelt sich der Zustand von S^{AM} , wenn S^A ein Qubit ist, in den Zustand (15.24). Die Zustände $|0^M\rangle$ und $|1^M\rangle$ sind die in diesem Zusammenhang *Erinnerungszustände* (memory states) des Beobachters. Dies beschreibt bereits den Messprozess. Der Zustand $|\phi^{AM}\rangle$ geht nicht noch anschließend in einen der Zustände (also z. B. $|0^A\rangle|0^M\rangle$) über, sondern beide *Zweige* (branches) $|0^A\rangle|0^M\rangle$ und $|1^A\rangle|1^M\rangle$ sind realisiert. Die Realisierung manifestiert sich allerdings in verschiedenen realen Welten, die nicht miteinander wechselwirken. Da die Zustände $|0^M\rangle$ und $|1^M\rangle$ Erinnerungszustände sein sollen, kann sich ein Beobachter mit wohlbestimmter Erinnerung, z. B. $|1^M\rangle$, nur an das zu $|1^A\rangle$ gehörige Messergebnis erinnern und er findet entsprechend System S^A auch im Zustand $|1^A\rangle$ und nicht im Zustand $|0^A\rangle$. Die Vorhersagen über das, was im nächsten Experiment zu dem hinzukommen wird, an was sich ein Beobachter erinnern kann, sind Wahrscheinlichkeitsaussagen. Auch in diesem nachfolgenden Experiment wird wieder alles realisiert was potentiell möglich ist. Die Welt spaltet immer wieder in jeder Messung auf.

Es ist das Wesen einer Interpretation, dass sie nicht empirisch widerlegt werden kann. Das gilt auch für die Viele-Welten-Interpretation. Weiterhin ist jeder frei darin, diejenige Interpretation zu wählen, die er aus guten (metaphysikalischen) Gründen für die Geeignetere hält. Wir haben das in Abschn. 2.5 analysiert. Die Viele-Welten-Interpretation ist bizarr, aber sie hat neben vielen Unklarheiten (vergl. Abschn. 15.6) und nicht befriedigend ausgearbeiteten Details auch Vorteile: Die Forderung (iv) an die Theorie des Messprozesses ist erfüllt. Weiterhin ist der Beobachter mit in das System einbezogen. Es wird „alles“ beschrieben. Es gibt nur ein einziges abgeschlossenes System, das das ganze kosmologische Universum repräsentiert. Das könnte das Verständnis der Quantenphysik des extremen Frühzustands des Universums erleichtern. Andererseits lassen sich auch Probleme erkennen. Wir geben ein Beispiel: Wie bei der Vormessung in Abschn. 15.3.2 muss man sich fragen, warum die Aufspaltung in die Welten nicht nach der Gl. (15.25) folgt. Wird der Beobachter S^M sich an eine Messung der Observablen Z^A oder der Observablen X^A erinnern? Es liegt nahe, zur Lösung dieses Problems (welches das Problem (i) aus Abschn. 15.3.1 ist) wieder die Dekohärenz durch die Umgebung heranzuziehen.

Wir wollen im nächsten Kapitel, dem Schlusskapitel, noch einmal zu „hartem“ theoretischem Stoff zurückkehren und einige Beweise nachliefern.

⁴ [Eve 57]

15.6 Ergänzende Themen und weiterführende Literatur

- Alle Aspekte des Themas Dekohärenz werden in dem Sammelband [GJK 96] behandelt.
- Übersichtsartikel zur Dekohärenz: [Joo 96], [Zeh 96], [Bub 97, Kap. 5.4], [Zeh 00], [Joo 02], [PZ 02], [Leg 02], [Zur 02], [Zur 03].
- Übersichtsartikel und Bücher zur Viele-Welten-Interpretation: [DG 73], [Deu 96], [Bar 00], [Vai 01].
- Kurze Darstellungen der Viele-Welten-Interpretation: [Pri 81, Kap. 3.6], [d’Es95, Kap. 12], [Bub 97, Kap.8.2], [Hom 97, Kap. 2] [Mit 98, Kap. 3.2], [Aul 00, Kap. 15].
- Übersichtsartikel und Bücher zur Theorie des Quantenmessprozesses: [Zur 82], [Zur 91], [BLM 91], [Bub 97, Kap. 8], [Mit 98], [Aul 00, Kap. IV], [PZ 02], [Leg 02].
- Eine Reihe von gut lesbaren Aufsätzen zu Schrödingers Katze, zum Verhältnis von Mikro- zu Makrophysik und zum Erscheinen der klassischen Welt findet sich in [AM 96].
- Vergleich von Dekohärenzraten und Relaxationsraten, Zeitskalen der Dekohärenz: [Joo 96], [PZ 02].
- Zeitlicher Ablauf des Verschwindens der Dekohärenz zwischen räumlich getrennten Komponenten einer Wellenfunktion (Lokalisierungsrate): [Joo 96].
- Übersichtsartikel zur Beschreibung des Messprozesses mit abgeänderter Schrödinger- und von-Neumann-Gleichungen (Zustandsreduktion als dynamischer Prozess): [Sta 96], [Lal 01].
- Wir haben nur ein besonders einfaches Modell für umgebungsinduzierte Dekohärenz studiert. Man sollte vorsichtig sein mit der Verallgemeinerung der Ergebnisse: [PZ 02].
- Interferometrie mit Makromolekülen und Dekohärenz: [ANZ 02], [HUH 03].
- Superposition makroskopischer Systeme in einem SQID: [FPC 00]. [VdW 00].
- Experimente zu Verschränkung, Dekohärenz und Katzenzuständen in Kavitäten: [HRB 02], [RBH 01].

15.7 Übungsaufgaben

ÜA 15.1 [zu 15.1] Berechnen Sie die Wirkung des Phasendämpfungskanal auf den Dichteoperator

$$\rho = \frac{1}{2}(\mathbb{1} + \mathbf{r}\boldsymbol{\sigma}) . \quad (15.47)$$

Wie ändert sich der Bloch-Vektor \mathbf{r} ?

ÜA 15.2 [zu 15.3] Leiten Sie die Gl. (15.29), (15.32) und (15.37) ab. Berechnen Sie hierzu zunächst die dyadische Zerlegung der Operatoren $\exp(\sigma_z^A \otimes \sigma_y^M)$ und $\exp(\sigma_z^A \otimes \sigma_z^M)$ in geeigneten Basen von $\mathcal{H}^A \otimes \mathcal{H}^M$.

ÜA 15.3 [zu 15.3] Leiten Sie Gl. (15.41) ab.

This Page Intentionally Left Blank

16 Zwei Realisierungen von Quantenoperationen*

16.1 Operatorsummenzerlegung*

Relative Zustände und Indexzustände Wir betrachten ein 2-Teile-System S^{AB} mit Hilbert-Raum $\mathcal{H}^A \otimes \mathcal{H}^B$ und setzen der Einfachheit halber $\dim \mathcal{H}^A = \dim \mathcal{H}^B = d$ voraus. In \mathcal{H}^A und \mathcal{H}^B führen wir ONB $\{|a_n^A\rangle\}$ und $\{|e_n^B\rangle\}$ ein und bilden daraus einen maximal verschränkten unnormierten Zustand

$$|\tilde{\psi}^{AB}\rangle = \sum_{n=1}^d |a_n^A, e_n^B\rangle \quad (16.1)$$

für den

$$|a_n^A\rangle = \langle e_n^B | \tilde{\psi}^{AB} \rangle \quad (16.2)$$

gilt. Wir können $|e_n^B\rangle$ als einen Markerzustand für $|a_n^A\rangle$ auffassen.

Diese Idee wird verallgemeinert. Wir können einen beliebigen Zustand $|\phi^A\rangle$

$$|\phi^A\rangle = \sum_n c_n |a_n^A\rangle \quad (16.3)$$

aus \mathcal{H}^A durch Projektion in \mathcal{H}^B gewinnen. Dazu bilden wir in \mathcal{H}^B den zu $|\phi^A\rangle$ gehörigen *Indexzustand* (index state)

$$|\phi^{*B}\rangle := \sum_n c_n^* |e_n^B\rangle. \quad (16.4)$$

Dann finden wir mit Gl. (16.1)

$$|\phi^A\rangle = \langle \phi^{*B} | \tilde{\psi}^{AB} \rangle \quad (16.5)$$

und ebenso

$$|\phi^{*B}\rangle = \langle \phi^A | \tilde{\psi}^{AB} \rangle. \quad (16.6)$$

$|\phi^A\rangle$ heißt *relativer Zustand* (relative state). Über den nur von den beiden ONB abhängigen maximal verschränkten Hilfszustand $|\tilde{\psi}^{AB}\rangle$ wird zwischen einem beliebigen Zustand

*Die mit einem Stern gekennzeichneten Kapitel können bei einem ersten Durchgang überschlagen werden.

$|\phi^A\rangle \in \mathcal{H}^A$ und seinem Indexzustand $|\phi^{*B}\rangle$ in \mathcal{H}^B ein einfacher Zusammenhang hergestellt. $|\tilde{\psi}^{AB}\rangle$ etabliert eine eindeutige Abbildung

$$|\phi^A\rangle \leftrightarrow |\phi^{*B}\rangle, \quad (16.7)$$

die *konjugiert linear* (conjugate linear) ist. Es gilt

$$|\phi^A\rangle = a_1|\phi_1^A\rangle + a_2|\phi_2^A\rangle, \quad |\phi^{*B}\rangle = a_1^*|\phi_1^{*A}\rangle + a_2^*|\phi_2^{*A}\rangle. \quad (16.8)$$

Der Beweis ergibt sich durch Zerlegung nach den Basisvektoren.

Beweis des Theorems Wir wollen den folgenden in Abschn. 14.1.2 bereits behaupteten Satz beweisen: *Eine Abbildung $\rho \rightarrow \tilde{\rho}' = \mathcal{E}(\rho)$ ist genau dann eine Quantenoperation, wenn es eine Operatorsummenzerlegung*

$$\mathcal{E}(\rho) = \sum_i K_i \rho K_i^\dagger \quad (16.9)$$

mit linearen Operatoren K_i gibt, die die Bedingung

$$\sum_i K_i^\dagger K_i \leq \mathbb{1} \quad (16.10)$$

erfüllen und den Eingangs-Hilbert-Raum auf den Ausgangs-Hilbert-Raum abbilden. Die Bedingung (16.10) ist gleichbedeutend damit, dass die Spur nicht erhöht wird

$$\text{tr}[\mathcal{E}(\rho)] \leq \mathbb{1} \quad (16.11)$$

($\text{tr}[\rho] = 1$). $\tilde{\rho}'$ ist wieder ein Dichteoperator.

Wir zeigen zunächst, dass $\mathcal{E}^A \otimes \mathbb{1}^B$ einen positiven Operator π^{AB} aus $\mathcal{H}^A \otimes \mathcal{H}^B$ in einen positiven Operator überführt. $|\psi^{AB}\rangle$ sei ein beliebiger Vektor aus $\mathcal{H}^A \otimes \mathcal{H}^B$. Wir greifen einen Index i heraus und bilden

$$|\phi_i^{AB}\rangle := (K_i^{A\dagger} \otimes \mathbb{1}^B)|\psi^{AB}\rangle. \quad (16.12)$$

Dann ist $K_i^A \otimes \mathbb{1}^B$ wegen

$$\langle \psi^{AB} | (K_i^A \otimes \mathbb{1}^B) \pi^{AB} (K_i^{A\dagger} \otimes \mathbb{1}^B) | \psi^{AB} \rangle = \langle \phi_i^{AB} | \pi^{AB} | \phi_i^{AB} \rangle \geq 0 \quad (16.13)$$

ein positiver Operator auf $\mathcal{H}^A \otimes \mathcal{H}^B$. Das gilt auch für die Summe über i . \mathcal{E}^A ist nicht nur positiv, sondern auch vollständig positiv.

Für die umgekehrte Beweisrichtung gehen wir im ersten Schritt von dem maximal verschränkten Zustand $|\tilde{\psi}^{AB}\rangle \langle \tilde{\psi}^{AB}|$ von Gl. (16.1) aus. Da \mathcal{E}^A nach Voraussetzung eine Quantenoperation ist, führt die Anwendung von $\mathcal{E}^A \otimes \mathbb{1}^B$

$$(\mathcal{E}^A \otimes \mathbb{1}^B) |\tilde{\psi}^{AB}\rangle \langle \tilde{\psi}^{AB}| =: C^{AB} \quad (16.14)$$

auf einen positiven Operator C^{AB} .

Im zweiten Schritt schreiben wir C^{AB} mit Gl. (16.1) unter Ausnutzung der Linearität von \mathcal{E}^A aus

$$\begin{aligned} C^{AE} &= (\mathcal{E}^A \otimes \mathbb{1}^B) \left(\sum_n |a_n^A, e_n^B\rangle \right) \left(\sum_{n'} \langle a_{n'}^A, e_{n'}^B| \right) \\ &= \sum_{n, n'} \mathcal{E}^A (|a_n^A\rangle \langle a_{n'}^A|) \otimes (|e_n^B\rangle \langle e_{n'}^B|) \end{aligned} \quad (16.15)$$

und bilden mit Gl. (16.3) und (16.4) den Erwartungszustand mit dem Indexzustand $|\phi^{*B}\rangle$.

$$\langle \phi^{*B} | C^{AB} | \phi^{*B} \rangle = \sum_{n, n'} c_n c_n^* \mathcal{E}^A (|a_n^A\rangle \langle a_{n'}^A|) = \mathcal{E} (|\phi^A\rangle \langle \phi^A|). \quad (16.16)$$

Dabei haben wir wieder die Linearität von \mathcal{E}^A ausgenutzt. Die Gl. (16.16) zeigt, dass im Operator C^{AB} die volle Information über die Wirkung des Superoperators \mathcal{E}^A auf der Basis des Liouville-Raums \mathbb{L}^A steckt.

Im dritten Schritt wählen wir eine Ensemblezerlegung von C^{AB} aus

$$C^{AB} = \sum_i |\tilde{c}_i^{AB}\rangle \langle \tilde{c}_i^{AB}| \quad (16.17)$$

und formen die linke Seite der Gl. (16.16) um.

$$\mathcal{E}^A (|\phi^A\rangle \langle \phi^A|) = \sum_i \langle \phi^{*B} | \tilde{c}_i^{AB} \rangle \langle \tilde{c}_i^{AB} | \phi^{*B} \rangle. \quad (16.18)$$

Wir führen Operatoren K_i^A durch ihre Wirkung auf $|\phi^A\rangle$ ein

$$\langle \phi^{*B} | \tilde{c}_i^{AB} \rangle =: K_i^A |\phi^A\rangle \quad (16.19)$$

und erhalten aus Gl. (16.18)

$$\mathcal{E}^A (|\phi^A\rangle \langle \phi^A|) = \sum_i K_i^A |\phi^A\rangle \langle \phi^A| K_i^{A\dagger}. \quad (16.20)$$

Wegen der Linearität von \mathcal{E}^A gilt damit für alle Dichteoperatoren ρ^A auf \mathcal{H}^A :

$$\mathcal{E}^A (\rho^A) = \sum_i K_i^A \rho^A K_i^{A\dagger}. \quad (16.21)$$

Da die Abbildung $|\phi^A\rangle \leftrightarrow |\phi^{*B}\rangle$ konjugiert linear ist, sind mit Gl. (16.19) auch die Operatoren K_i^A lineare Operatoren. Da weiterhin die Quantenoperation $\mathcal{E}^A(\rho^A)$ von Gl. (16.21) für alle ρ^A die Spur nicht erhält, ergibt sich die Bedingung (16.10). Damit ist der Satz über die Operatorsummenzerlegung in beiden Richtungen bewiesen.

Die Wahl der beiden Orthonormalbasen $\{|a_n^A\rangle\}$ und $\{|e_n^B\rangle\}$ war ebenso wie die Ensemblezerlegung (16.17) willkürlich. Das zeigt noch einmal, dass die Operationselemente K_i^A bei vorgegebenem Superoperator \mathcal{E}^A nicht eindeutig festgelegt sind.

16.2 Unitäre Realisierung von Quantenoperationen*

Spurerhaltende Quantenoperationen Eine spurerhaltende Quantenoperation \mathcal{E}^A auf dem System S^A

$$\mathrm{tr}[\mathcal{E}^A(\rho^A)] = \mathrm{tr}[\rho^A] = 1 \quad (16.22)$$

heißt auch *vollständige Quantenoperation* (complete quantum operation). Die zugehörigen Zerlegungsoperatoren erfüllen die Vollständigkeitsrelation

$$\sum_i K_i^{A\dagger} K_i^A = \mathbb{1} . \quad (16.23)$$

Für eine unitäre Realisierung der Quantenoperation ergänzen wir wieder das System S^A um ein Hilfssystem S^B . Die Dimension von \mathcal{H}^B soll mit der Zahl der Zerlegungsoperatoren übereinstimmen.

In \mathcal{H}^B wählen wir eine Basis $\{|i^B\rangle\}$. S^B sei am Anfang im Zustand $|0^B\rangle$ und das Gesamtsystem im Produktzustand $|\psi^A\rangle|0^B\rangle$. Wir definieren mit Hilfe der K_i^A einen Operator \hat{U}^{AB} durch seine Wirkung auf Zustände $|\psi^A\rangle|0^B\rangle$

$$\hat{U}^{AB}|\psi^A\rangle|0^B\rangle := \sum_i K_i^A |\psi^A\rangle|i^B\rangle . \quad (16.24)$$

Für beliebige Zustände $|\psi^A\rangle$ und $|\phi^A\rangle$ gilt dann mit der Vollständigkeitsrelation (16.23)

$$\begin{aligned} \langle\psi^A| \langle 0^B| \hat{U}^{AB\dagger} \hat{U}^{AB} |\phi^A\rangle |0^B\rangle &= \sum_i \langle\psi^A, 0^B| K_i^{A\dagger} K_i^A |\phi^A, 0^B\rangle \\ &= \langle\psi^A, 0^E| \phi^A, 0^E\rangle . \end{aligned} \quad (16.25)$$

Auf Zuständen der Form $|\psi^A, 0^B\rangle$ erhält \hat{U}^{AB} die inneren Produkte. Mit dem schon in Abschn. 13.3.5 verwendeten Hilfssatz kann daher \hat{U}^{AB} zu einem unitären Operator U^{AB} erweitert werden, der auf ganz $\mathcal{H}^A \otimes \mathcal{H}^B$ wirkt. Von solchen Operatoren nehmen wir an, dass sie sich physikalisch realisieren lassen.

Das Untersystem S^A wird durch die unitäre Transformation des Gesamtsystems in den Zustand

$$\begin{aligned} \mathrm{tr}_B[U^{AB}(|\psi^A\rangle\langle\psi^A| \otimes |0^B\rangle\langle 0^B|)U^{AB\dagger}] \\ &= \mathrm{tr}_B\left[\sum_{i,i'} K_i^A |\psi^A\rangle\langle\psi^A| K_{i'}^{A\dagger} \otimes |i^B\rangle\langle i'^B|\right] \\ &= \sum_i K_i^A |\psi^A\rangle\langle\psi^A| K_i^{A\dagger} \\ &= \mathcal{E}^A(|\psi^A\rangle\langle\psi^A|) \end{aligned} \quad (16.26)$$

überführt in den es auch die Quantenoperation \mathcal{E}^A überführt. Jede vollständige Quantenoperation auf \mathcal{H}^A hat daher eine *unitäre Realisierung* auf $\mathcal{H}^A \otimes \mathcal{H}^B$ in der Form

$$\mathcal{E}^A(\rho^A) = \mathrm{tr}_B[U^{AB}(\rho^A \otimes |0^B\rangle\langle 0^B|)U^{AB\dagger}] . \quad (16.27)$$

In jeder vollständigen Quantenoperation \mathcal{E}^A eines Systems S^A lässt sich ein Gesamtsystem S^{AB} mit Hilbert-Raum $\mathcal{H}^A \otimes \mathcal{H}^B$ und eine unitäre Transformation U^{AB} auf \mathcal{H}^{AB} finden, so dass das Teilsystem die Entwicklung mit \mathcal{E}^A durchmacht. U^{AB} ist die Erweiterung des in Gl. (16.24) definierten Operators \hat{U}^{AB} .

Quantenoperationen, die die Spur nicht erhalten Bei unvollständigen Quantenoperationen ($\sum_i K_i^{A\dagger} K_i^A < \mathbb{1}$) ergänzen wir die Menge der Operatoren K_i^A um einen Operator K_* , so dass ein vollständiger Satz

$$\sum_i K_i^{A\dagger} K_i^A + K_*^\dagger K_* = \mathbb{1} \quad (16.28)$$

entsteht.

Den Raum \mathcal{H}^B ersetzen wir durch den Raum $\mathcal{H}^{B'}$, dessen Dimension um eins erhöht ist. Ein Operator $U^{AB'}$ wird wie oben gebildet. Nach der Entwicklung mit $U^{AB'}$ wird durch den Projektor P^B eine Projektion auf \mathcal{H}^B durchgeführt. Wir ersetzen also in der Rechnung oben U^{AB} durch $P^B U^{AB'}$. Dann verschwindet in der zu Gl. (16.24) analogen Gleichung gerade der Operator K_*^A . Auch in der Operatorsummendarstellung (16.26) taucht er nicht mehr auf.

16.3 Realisierung einer völlig allgemeinen Messung durch unitäre Transformation und Projektion*

Wir wollen *völlig allgemeine Messungen* (most general measurements) physikalisch realisieren. Bei diesen Eingriffen geht der Zustand ρ^A bei Eintreten des Messwerts m in den Zustand $\tilde{\rho}_m'^A$ über, der durch eine Quantenoperation \mathcal{M}_m^A gegeben ist.

$$\rho^A \rightarrow \tilde{\rho}_m'^A = \mathcal{M}_m^A(\rho^A). \quad (16.29)$$

Die in Abschn. 13.3 diskutierte verallgemeinerte Messung ist der Spezialfall $\mathcal{M}_m^A(\rho) = M_{m,i}^A \rho^A M_{m,i}^{A\dagger}$.

Die Anzeige des Messwerts m soll mit der Wahrscheinlichkeit

$$p(m) = \text{tr}_A[\tilde{\rho}_m'^A] = \text{tr}_A[\mathcal{M}_m^A(\rho)] \quad (16.30)$$

erfolgen. Es ist also für beliebige ρ^A

$$\text{tr}_A\left[\sum_m \mathcal{M}_m^A(\rho^A)\right] = \sum_m p(m) = 1. \quad (16.31)$$

Die Superoperatoren \mathcal{M}_m^A haben eine Operatorsummenzerlegung

$$\mathcal{M}_m^A(\rho) = \sum_i M_{m,i}^A \rho^A M_{m,i}^{A\dagger}. \quad (16.32)$$

Der Laufbereich von i kann von m abhängen. Als Folge von Gl. (16.31) müssen die Zerlegungsooperatoren die Vollständigkeitsrelation

$$\sum_{m,i} M_{m,i}^{A\dagger} M_{m,i}^A = \mathbb{1} \quad (16.33)$$

erfüllen.

Es kann auch in diesem Fall eine im Prinzip durchführbare physikalische Realisierung für diese ganz allgemeine Messung am System S^A gefunden werden, indem ein Hilffsystem S^B hinzugenommen wird. Das Gesamtsystem S^{AB} wird wieder geeignet unitär entwickelt und schließlich wird in S^B eine projektive Messung durchgeführt.

Wir führen ein Hilffsystem S^B mit einer ONB $\{|m, i^B\rangle\} \in \mathcal{H}^B$ ein (d. h. $\langle m, i | m', i' \rangle = \delta_{mm'} \delta_{ii'}$), deren Vektoren den Zerlegungsoperatoren zugeordnet sind $M_{m,i}^A \leftrightarrow |m, i^B\rangle$. Dann können wir Schritt für Schritt dem Vorgehen in Abschn. 16.2 folgen. Der Anfangszustand des Gesamtsystems sei $|\psi^A, 0^B\rangle$. Es wird ein Operator \hat{U}^{AB} mit der Wirkung

$$\hat{U}^{AB} |\psi^A, 0^B\rangle := \sum_{m,i} M_{m,i}^A |\psi^A\rangle |m, i^B\rangle \quad (16.34)$$

definiert. Er lässt sich wieder zu einem unitären Operator U^{AB} auf ganz $\mathcal{H}^A \otimes \mathcal{H}^B$ erweitern.

Wir führen orthogonale Projektionsoperatoren P_m^B auf dem Hilffsystem S^B zu den Messwerten m ein:

$$P_m^B := \sum_i |m, i^B\rangle \langle m, i^B|, \quad \sum_m P_m^B = \mathbb{1}^B. \quad (16.35)$$

Die unitäre Gesamttransformation mit nachfolgender Projektion P_m^B auf dem Hilffsystem S^B ergibt

$$\begin{aligned} P_m^B U^{AB} |\psi^A\rangle |0^B\rangle &= \left(\sum_{i'} |m, i'^B\rangle \langle m, i'^B| \right) \left(\sum_{n,i} M_{n,i}^A |\psi^A\rangle |n, i^B\rangle \right) \\ &= \sum_i M_{m,i}^A |\psi^A\rangle |m, i^B\rangle. \end{aligned} \quad (16.36)$$

Zur Bestimmung des reduzierten Dichteoperators des Ausgangssystems S^A gehen wir wie in Gl. (16.26) vor und erhalten mit Gl. (16.32) die gewünschte Relation (16.29)

$$\tilde{\rho}_m^A = \sum_i M_{m,i}^A |\psi^A\rangle \langle \psi^A| M_{m,i}^{A\dagger} = \mathcal{M}_m^A(|\psi^A\rangle \langle \psi^A|). \quad (16.37)$$

Die Wahrscheinlichkeit $p(m)$, mit der bei der projektiven Messung auf S^B der Messwert m auftritt, ist durch den reduzierten Dichteoperator ρ^B von S^B nach der unitären Entwicklung gegeben. Durch Bilden der Teilspur tr_A bei Gl. (16.36) gewinnen wir zunächst nach einer Zwischenrechnung ρ^B und daraus $p(m)$

$$p(m) = \text{tr}_B [P_m^B \rho^B P_m^B]. \quad (16.38)$$

Man liest dann an den expliziten Ausdrücken in der hier nicht dargestellten Zwischenrechnung mit Hilfe von Gl. (16.37) die angestrebte Endrelation (vergl. Gl. (16.30))

$$p(m) = \text{tr}_A [\mathcal{M}_m^A(|\psi^A\rangle \langle \psi^A|)] \quad (16.39)$$

ab. Die Rechnung überträgt sich infolge der Linearität der Superoperatoren auf Dichteoperatoren.

Wir haben folgendes Ergebnis erhalten: *Eine völlig allgemeine Messung am System S^A mit Messergebnis m ist als unitäre Entwicklung U^{AB} des um S^B erweiterten Gesamtsystems S^{AB} mit anschließend projektiver Messung an S^B mit Projektor P_m^B realisierbar. U^{AB} und P_m^B sind dabei durch die Gl. (16.34) und (16.35) gegeben. Es findet eine Rückführung auf projektive Messungen statt, die physikalisch nicht weiter reduziert werden kann.*

16.4 Ergänzende Themen und Literatur

- Zu den Beweisen: [Sch 96].

16.5 Übungsaufgaben

ÜA 16.1 [zu 16.1] Beweisen Sie Gl. (16.8).

ÜA 16.2 [zu 16.3] Ergänzen Sie die Zwischenrechnung, die auf Gl. (16.38) führt.

This Page Intentionally Left Blank

Literatur

Literaturhinweise

- Mit diesen Arbeiten fing es an: [EPR 35], [Sch 35].
- Der Klassiker: [vNe 68].
- Auswahl von allgemeinen Lehrbüchern der theoretischen Physik: [Pri 81], [Sak 85], [CDL 91], [Ish 95], [Bal 98].
- Bücher mit Gesamtdarstellungen des Gebiets (teilweise einschließlich der experimentellen Aspekte): [Per 93], [d'Es95], [Pre 98], [d'Es99], [Aul 00], [NC 00], [Bru 03], [SS 04].
- Bücher, in denen Teilgebiete ausführlich dargestellt werden: [Jor 69], [Kra 83], [BLM 91], [BGL 95], [Bub 97], [Hom 97], [Mit 98], [MW 98], [WC 98], [Bro 99], [Gru 99], [Pit 00], [CP 01], [Hir 01], [Hol 01], [Gri 02], [SS 04].
- Sammlungen von Übersichtsartikeln: [GJK 96], [LSP 98], [Bra 99], [BEZ 00], [BGJ 00], [ABH 01], [BZ 02], [DM 02], [CB 02], [Hei 02], [Lom 02], [LB 02].
- Übersichtsartikel in Zeitschriften mit Gesamtdarstellungen des Gebiets: [Ben 95], [Joz 98], [PV 98], [Ste 98], [BD 00], [Lal 01], [Key 02], [KLB 04].
- Übersichtsartikel in Zeitschriften, in denen ein Teilgebiet ausführlich dargestellt wird: [DiV 98], [Ste 98], [WW 01], [GM 02], [GRT 02], [Ved 02], [Zur 03], [PT 04].
- Übersichtsartikel zu Experimente zur Quanteninformationstheorie und Sammlungen, die solche Artikel enthalten: [LSP 98], [Bra 99], [BEZ 00] [ABH 01], [BZ 02], [DM 02], [GRT 02], [Hei 02].
- Sammlungen von elementarisierten Übersichtsartikeln: [AM 96], [Aud 02].
- Aufarbeitung des Themenbereichs für die Schule: [KM 02].
- Sehr umfangreiche gegliederte Bibliographie zu allen Teilgebieten: [Cab 04].

Literaturverzeichnis

- [ABH 01] Alber, G., Beth, T., Horodecki, M., Horodecki, P., Horodecki, R., Rötteler, M., Weinfurter, H., Werner, R. und Zeilinger, A.: *Quantum Information – An Introduction to Basic Theoretical Concepts and Experiments*, Springer-Verlag, Berlin 2001.
- [ADK 03] Audretsch, J., Diósi, L. und Konrad, T.: *Estimating the postmeasurement state*, Phys. Rev. **A68**, 034302 (2003).
- [AKK 04] Audretsch, J., Klee, F. E. und Konrad, T.: *Monitoring Quantum Oscillations with very small Disturbance*, quant-ph/0408107 (2004).
- [AM 88] Audretsch, J. und Mainzer, K. (Hrsg.): *Philosophie und Physik der Raum-Zeit*, BI-Wiss.-Verl., Mannheim 1988.
- [AM 96] Audretsch, J. und Mainzer, K. (Hrsg.): *Wieviele Leben hat Schrödingers Katze? – Zur Physik und Philosophie der Quantenmechanik*, Spektrum Akad. Verlag, Heidelberg 1996.
- [ANZ 02] Arndt, M., Nairz, O. und Zeilinger, A.: *Interferometry with Macromolecules and the Mesoscopic World*, in [BZ 02], S. 334–350, 2002.
- [Asp 02] Aspect, A.: *Bell's Theorem: The Naive View of an Experimentalist*, in [BZ 02], 119–153 (2002).
- [Aud 02] Audretsch, J. (Hrsg.): *Verschränkte Welt – Faszination der Quanten*, Wiley-VCH, Weinheim, 2002.
- [Aul 00] Auletta, G.: *Foundations and Interpretations of quantum mechanics*, World Scientific, Singapore 2000.
- [Bal 70] Ballentine, L. E.: *The Statistical Interpretation of Quantum Mechanics*, Rev. Mod. Phys. **42**, 358–381, (1970).
- [Bal 98] Ballentine, L. E.: *Quantum mechanics – a modern development*, World Scientific, Singapore 1998.
- [Bar 96] Barenco, A.: *Quantum physics and computers*, Contemp. Phys. **37**, 375–389 (1996).
- [Bar 98] Barenco, A.: *Quantum computation: an introduction*, in [LSP 98], S. 143–183 (1998).
- [Bar 00] Barrett, J.: *Everett's Relative-State formulation of Quantum Mechanics*, Stanford Encyclopedia of Philosophy, <http://plato.stanford.edu/entries/qm-everett>, 2000.
- [BBC 95] Barenco, A., Bennet, C. H., Cleve, R., DiVincenzo, D. P., Margolus, N., Shor, P. W., Sleator, T., Smolin, J. A. und Weinfurter, H.: *Elementary gates for quantum computation*, Phys. Rev. **A 52**, 3457–3467 (1995); quant-ph/9503016.
- [BBH 98] Boyer, M., Brassard, G., Høyer, P. und Tapp, A.: *Tight bounds on quantum searching*, Fortschr. Phys. **46**, 493–505 (1998); quant-ph/9605034.
- [BBM 92] Bennett, C. H., Brassard, G. und Mermin, N. D.: *Quantum Cryptography without Bell's Theorem*, Phys. Rev. Lett. **68**, 557–559 (1992).
- [BD 00] Bennett, Ch. H. und DiVincenzo, D. P.: *Quantum information and computation*, Nature **404**, 247–255 (2000).
- [BDM 98] Berman, G. P., Doolen, G. D., Mainieri, R. und Tsifrinovich, V. I.: *Introduction to quantum computers*, World Scientific, Singapore, 1998.

- [Bel 64] J. S. Bell *On the Einstein-Podolsky-Rosen paradox*, Physics **1**, 195–200 (1964). Nachdruck in J. S. Bell *Speakable and Unspeakable in Quantum Mechanics*, Cambridge University Press, Cambridge, 1987.
- [Ben 92] Bennett, C. H.: *Quantum cryptography using any two nonorthogonal states*, Phys. Rev. Lett., **68**, 3121–3124 (1992).
- [Ben 95] Bennett, C. H.: *Quantum Information and Computation*, Physics Today, October 24–30 (1995).
- [BEZ 00] Bouwmeester, D., Ekert, A. und Zeilinger, A. (Hrsg.): *The physics of quantum information – quantum cryptography, quantum teleportation, quantum computation*, Springer-Verlag, Berlin 2000.
- [BGJ 00] Blanchard, Ph., Giulini, D., Joos, E., Kiefer, C. und Stamatescu, J.-O. (Hrsg.): *Decoherence: Theoretical, Experimental, and Conceptual Problems*, Springer, Berlin, 2000.
- [BGL 95] Busch, P., Grabowski, M. und Lahti, P. J.: *Operational quantum mechanics*, Springer-Verlag, Berlin 1995.
- [BHL 02] Bouwmeester, D., Howell, J. C. und Lamas-Linares, A.: *Quantum Information Science Using Photons*, in [Hei 02], S. 149–197 (2002)
- [BLM 91] Busch, P., Lahti, P. J. und Mittelstaedt, P.: *The Quantum Theory of Measurement*, Springer-Verlag, Berlin 1991.
- [Boh 51] Bohm, D.: *Quantum Physics* Prentice Hall, New York 1951.
- [BP 02] Breuer, H.-P. und Petruccione, F.: *The Theory of Open Quantum Systems*, Oxford University Press, Oxford 2002.
- [Bra 99] Braunstein, P. (Hrsg.): *Quantum computing: Where do we want to go tomorrow*, Wiley-VCH, Weinheim 1999.
- [Bra 99a] Braunstein, S.: *Quantum Computation*, in [Bra 99], 1–21.
- [Bra 02] Brandt, H. E.: *Qubit Devices* in [Lom 02], S. 67–139 (2002).
- [Bro 99] Brooks, M. (Hrsg.): *Quantum computing and communications*, Springer-Verlag, Berlin, 1999.
- [Bru 01] Bruß, D.: *Characterizing Entanglement*, quant-ph/0110078, (2001).
- [Bru 03] Bruß, D.: *Quanteninformation*, Fischer Verlag, Frankfurt a.M. 2003.
- [Bub 97] Bub, J.: *Interpreting the Quantum World*, Cambridge University Press, Cambridge 1997.
- [Bus 97] Busch, P.: *Is the quantum state (an) observable?* in: R.S. Cohen et. Al. (Hrsg.) *Potentiality and Passion -at-a- Distance*, S. 61–70, Kluwer Acad. Publ. 1997.
- [Bus 99] Busch, P.: *Quantum States as Effect Valuations: Giving Operational Content to von Neumann's No-Hidden-Variable Theorem*, quant-ph/9909073 *Multiparticle generalization of entanglement swapping*, Phys. Review **A 57**, 822–829 (1997), quant-ph/9708004.
- [BZ 02] Bertelmann, R. A. und Zeilinger, A. (Hrsg.): *Quantum [un]speakables – From Bell to quantum information*, Springer-Verlag, Berlin 2002
- [Cab 04] Cabello, A.: *Bibliographic guide to the foundations of quantum mechanics and quantum information*, quant-ph/0012089v11 (2004).
- [CB 02] Chen, G. und Brylinski, R.K. (Hrsg.): *Mathematics of Quantum Computation*, Chapman and Hall/CRC, Boca Raton 2002.

- [CD 94] Caves, C. M. und Drummond, P.D.: *Quantum limits on bosonic communication rates*, Rev. Mod. Phys. **66**, 481–537 (1994).
- [CDL 91] Cohen-Tannoudji, C., Diu, B. und Laloë, F.: *Quantum Mechanics, Vol. 1*, John Wiley, New York 1991.
- [CEM 98] Cleve, R., Ekert, A., Macchiavello, C. und Mosca, M.: *Quantum algorithms revisited*, Proc. R. Soc. London, **A454**, 339–354 (1998).
- [CF 96] Caves, C. M. und Fuchs, Ch. A.: *Quantum Information: How much Information in a State Vektor?* quant-ph/9601025
- [CHS 69] Clauser, J. F., Horne, M. A., Shimony, A. und Holt, R. A.: *Proposed experiment to test local hidden-variable theories*, Phys. Rev. Lett., 23, 880–884 (1969).
- [Cir 02] Cirac, J. I.: *Quantum Information: Entanglement, Purification, Error Correction and Quantum Optical Implication*, in [Hei 02], S. 199–239.
- [CLK 00] Cory, D. G., Laflamme, R., Knill, E., Viola, L., Havel, T. F., Boulant, N., Boutis, G., Fortunato, E., Lloyd, S., Martinez, R., Negrevergne, C., Pravia, M., Sharf, Y., Teklemariam, G., Weinstein, Y. S. und Zurek, W. H.: *NMR based quantum information processing: Achievements and prospects*, Fortschr. Phys. **48**, 9–11 (Special issue: Experimental proposals for quantum computation), 875–907 (2000); quant-ph/0004104.
- [CP 01] Calude, C. S. und Paun, G.: *Computing with Cells and Atoms – An Introduction to quantum, DNA and membrane computing*, Taylor and Francis, London 2001.
- [CST 89] Campos, R. A., Saleh, B. E. A. und Teich, M. C.: *Quantum-mechanical lossless beam splitter: SU(2) symmetry and photon statistics*, Phys. Rev. **A 40**, 1371–1384 (1989).
- [d'Es95] D'Espagnat, B.: *Veiled reality – an analysis of present-day quantum mechanical concepts*, Addison-Wesley, Reading (Mass.) 1995.
- [d'Es99] D'Espagnat, B.: *Conceptual foundations of quantum mechanics*, Perseus Books, Reading 1999.
- [Dav 76] Davies, E. B.: *Quantum Theory of open systems*, Academic Press, London 1976.
- [DE 98] Deutsch, D. und Ekert, A. K.: *Quantum computation*, Phys. World **11**, 3, 53–57 (1998).
- [Deu85] : Deutsch D.: *Quantum theory, the Church-Turing principle and the universal quantum computer*, Proc. R. Soc. Lond. **A 400**, 1818, 97–117 (1985).
- [Deu 89] Deutsch, D.: *Quantum computational networks*, Proc. R. Soc. Lond., **A 425**, S. 73–90 (1989).
- [Deu 96] Deutsch, D.: *Comment on The many minds interpretation of quantum mechanics*, Brit. J. Philos. Sci. **47**, 2, S. 222, (1996).
- [DG 71] DeWitt, B. S. und Graham, R. N.: *Resource Letter IQM-1 on the Interpretation of Quantum Mechanics*, Am. J. Phys. **39**, 724–738 (1971).
- [DG 73] DeWitt, B. S. und Graham, R. N. (Hrsg.): *The many-worlds interpretation of quantum mechanics*, Princeton University Press, Princeton, New Jersey, 1973.
- [DHR 02] Donald, M. J., Horodecki, M. und Rudolph, O.: *The uniqueness theorem for entanglement measures*, quant-ph/0105017 v2, (2002).
- [DiV 98] DiVincenzo, D. P.: *Quantum gates and circuits*, Proc. R. Soc. London, **A 454**, 261–276 (1998).

- [DiV 00] DiVincenzo, D. P.: *The physical implementation of quantum computation*, Fortschr. Phys. **48**, 9–11 (Special issue: Experimental proposals for quantum computation), 771–783 (2000); quant-ph/0002077.
- [DJ 92] Deutsch D., Jozsa R.: *Rapid solution of problems by quantum computation*, Proc. R. Soc. Lond. **A 439**, 1907, 553–558 (1992).
- [DM 02] DeMartini, F. und Monroe, C.: *Experimental Quantum Computation and Information*, „Enrico Fermi“ Course CXLVIII, IOS Press, Amsterdam 2002.
- [DNR 98] Dürr, S., Nonn, T. und Rempe, G.: *Fringe visibility and which-way information in an atom interferometer*, Phys. Rev. Lett. **81**, 5705–5709 (1998).
- [DR 00] Dürr, S. und Rempe, G.: *Wave-Particle Duality in an Atom Interferometer*, Advances Atomic, Molecular and Optical Physics, **45**, 29–71 (2000).
- [EGH 00] Ekert, A., Gisin, N., Huttner, B., Inamori, H. und Weinfurter, H.: *Quantum Cryptography*, in [BEZ 00], S. 15–48 (2000).
- [EHI 01] Ekert, A., Hayden, P. M. und Inamori, H.: *Basic concepts in quantum computation*, in Les Houches, Session LXXII *Coherent atomic matter waves*, Kaiser, R., Westbrook, C. and David, F. (Hrsg.), S. 661–701, Springer, Berlin 2001.
- [EJ 96] Ekert, A. und Jozsa, R.: *Quantum computation and Shor's factoring algorithm*, Rev. Mod. Phys. **68**, 733–753 (1996).
- [Eng 99] Engler, B.-G.: *Remarks on some basic issues in quantum mechanics*, Zeitschrift f. Naturforschung **54**, 11–32 (1999).
- [EPR 35] A. Einstein, B. Podolsky und H. Rosen *Can quantum-mechanical description of reality be considered complete?*, Phys. Rev. **47**, 777–780 (1935).
- [Esf 02] Esfeld, M.: *Quantentheorie: Herausforderung an die Philosophie!* in [Aud 02] S. 136–217, 2002.
- [Esf 02a] Esfeld, M.: *Einführung in die Naturphilosophie*, Wissenschaftliche Buchgesellschaft, Darmstadt 2002.
- [Esf 04] Esfeld, M.: *Quantum entanglement and a metaphysics of relations*, Studies in History and Philosophy of Science Part B, Vol. **35**, Issue 4, 625–641 (2004).
- [ESW 99] Englert, B.-G., Scully, M. O. und Walther, H.: *Quantum erasure in double-slit interferometers with which-way detectors* Am. J. Phys. **67**, 325–329 (1999)
- [Eve 57] Everett, H.: *Relative state formulation of quantum mechanics*, Rev. Mod. Phys. **29**, 3, S. 454–462, (1957).
- [Fan 57] Fano, U.: *Description of States in Quantum Mechanics by Density Matrix and Operator Techniques*, Rev. Mod. Phys. **29**, 74–93 (1957)
- [FK 98] Fischer, H. und Kaul, H.: *Mathematik für Physiker Bd. 2: Gewöhnliche und partielle Differentialgleichungen, mathematische Grundlagen der Quantenmechanik*, Teubner, Stuttgart, 1998.
- [Fle 00] Fleming, G. N.: *Operational Quantum Physics*, Stud. Hist. Phil. Mod. Phys. **31**, 117–125 (2000).
- [FP 00] Fuchs, C. A. und Peres, A.: *Quantum theory needs no interpretation*, Physics Today, March 2000, 70–71 sowie Sept. 2000, 11–14, 1990.

- [FPC 00] Friedman, J. R., Patel, V., Chen, W., Tolpygo, S. K. und Lukens, J. E.: *Quantum superposition of distinct macroscopic states*, Nature **406**, 43–46 (2000). quant-ph/0105039v1 (2001).
- [GHZ 89] Greenberger, D. M., Horne, M. A. und Zeilinger, A.: *Going Beyond Bell's Theorem* in M. Kafatos (Hrsg.) *Bell Theorem, Quantum Theory and Conceptions of the Universe*, S. 69–72, Kluwer, Dordrecht, 1989.
- [GHZ 90] Greenberger, D. M., Horne, M. A., Shimony, A. und Zeilinger, A.: *Bell's Theorem without inequalities*, Am. J. Phys., **58**, 1131–1143 (1990)
- [GJK 96] Giulini, D., Joos, E., Kiefer, C., Kupsch, J., Stamatescu, I.-O. und Zeh, D. H.: *Decoherence and the appearance of the classical world in quantum theory*, Springer-Verlag, Berlin 1996.
- [Gle 57] Gleason, A. M.: *Measures on the Closed Subspaces of a Hilbert Space*, J. Math. Mech. **6**, 885–894 (1957)
- [GM 02] Galindo, A. und Martín-Delgado, M. A.: *Information and computation: Classical and quantum aspects*, Reviews of Modern Optics **74**, 347–423 (2002), quant-ph/0112105.
- [Gri 02] Griffiths, R. B.: *Consistent Quantum Theory*, Cambridge University Press, Cambridge UK 2002.
- [Gro 96] Grover, L. K.: *A fast quantum mechanical algorithm for database search* in *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, p. 212–219, Philadelphia 1996.
- [GRT 02] Gisin, N., Rikordy, G., Tittel, W. und Zbinden, H.: *Quantum cryptography*, Rev. Mod. Phys. **74**, 145 – 195 (2002).
- [Gru 99] J. Gruska *Quantum Computing*, McGraw-Hill, London, 1999.
- [HAD 95] Hughes, R. J., Alde, D. M., Dyer, P., Luther, G. G., Morgan, G. L. und Schauer, M.: *Quantum Cryptography*, Contemp. Phys. **36**, 149–163 (1995), quant-ph/9504002.
- [Har 01a] Hardy, L.: *Why Quantum Theory?*, 2001. quant-ph/011068v1
- [Har 01b] Hardy, L.: *Quantum Theory from five reasonable Axioms*, 2001. quant-ph/0101012v4
- [Hea 99] Healey, R.: *Holism and Nonseparability in Physics*, in *Stanford Encyclopedia of Physics*, <http://plato.stanford.edu/entries/physics-holism>
- [Hei 02] Heiss, D. (Hrsg.): *Fundamentals of Quantum Information*, Springer-Verlag, Berlin 2002
- [HHH 01] Horodecki, M., Horodecki, P. und Horodecki, R.: *Mixed State entanglement and Quantum Communication*, in [ABH 01], S. 151–195, 2001.
- [Hir 01] Hirsensvalo, M.: *Quantum computing*, Springer-Verlag, Berlin 2001.
- [HK 69] Hellwig, H.-E. und Kraus, K.: *Pure operations and measurements*, Comm. math. Phys. **11**, 214–220 (1969).
- [HK 70] Hellwig, H.-E. und Kraus, K.: *Operations and measurements*, Comm. math. Phys. **16**, 142–147 (1970).
- [HN 99] Hughes, R. und Nordholdt, J.: *Quantum cryptography takes to the air*, Physics Word, May 1999, 31–35.

- [Hol 01] Holevo, A. S.: *Statistical Structure of Quantum Theory*, Springer-Verlag, Berlin 2001.
- [Hom 97] Home, D.: *Conceptual foundations of quantum physics – an overview from modern perspective*, Plenum Press, New York 1977.
- [HRB 02] Haroche, S., Raimond, J. M. und Brune, M.: *Entanglement, complementarity and decoherence in cavity QED experiments*, in [DM 02], S. 3–36, 2002.
- [HS 91] Home, D. und Selleri, F.: *Bell's Theorem and the EPR Paradox*, Riv. Nuov. Cim. **14**, n9. 1–95 (1991).
- [HUH 03] Hackermüller, L., Uttenthaler, S., Hornberger, K., Reiger, E., Brezger, B., Zeilinger, A. und Arndt, M.: *Wave Nature of Biomolecules and Fluorofullerenes*, Phys. Rev. Lett. **91**, 090408-1 bis 09048-4 (2003).
- [HW 79] Hardy, G. und Wright, E.: *An Introduction to the Theory of Numbers*, Clarendon Press, Oxford, 1979.
- [IHB 90] Itano, W. H., Heinzen, D. J., Bollinger, J. J., und Wineland, D. J.: *Quantum Zeno Effect*, Phys. Rev. **A41**, 2295–2300, (1990).
- [Ish 95] Isham, C.: *Lectures on quantum theory – mathematical and structural foundations*, Imperial College Press, distributed by World Scientific, Singapore 1995.
- [Joo 96] Joos, E.: *Decoherence Through Interaction with the Environment*, in [GJK 96], S. 35–136, 1996.
- [Joo 02] Joos, E.: *Dekohärenz und der Übergang von der Quantenphysik zur klassischen Physik*, in [Aud 02], S. 169–195, 2002.
- [Jor 69] Jordan, Th. F.: *Linear Operators for Quantum Mechanics*, Wiley, New York 1969.
- [Joz 98] Jozsa, R.: *Quantum Information and its Properties*, in [LSP 98], S. 49–75, (1998).
- [Joz 00] Jozsa, R.: *Quantum Algorithms*, in *The Physics of Quantum Information*, in [BEZ 00], S. 104–126, 2000.
- [JS 94] Jozsa, R. und Schumacher, B.: *A new proof of the quantum noiseless coding theorem*, Journal of Modern Optics **41**, 2343–2349, (1994).
- [Key 02] Keyl, M.: *Fundamentals of quantum information theory*, Physics Reports **369**, 431–548 (2002).
- [KLB 04] Knill, E., Laflamme, R., Barnum, D., Dalvit, D., Dziarmaga, J., Gubernatis, L., Gurvits, L., Ortiz, G., Viola, L. und Zurek, W. H.: *Introduction to quantum Information Processing*, quant-ph/0207171 v1, 2002.
- [KM 02] Küblbeck, J. K. und Müller, R.: *Die Wesenszüge der Quantenphysik – Modelle, Bilder, Experimente*, Aulis Verlag Deubner, Köln, 2002.
- [Kon 03] Konrad, Th.: *On the theory and application of weak and unsharp measurements in Quantum Mechanics*, Doctoral thesis, University of Konstanz 2003, <http://www.ub.uni-konstanz.de/kops/volltexte/2003/1050/>
- [Kra 83] Kraus, K.: *States, Effects and Operations*, Springer-Verlag, Berlin 1983.
- [KSV 02] Kitaev, A. Y., Shen, A. H. und Vyalys, M. N.: *Classical and Quantum Computation*, Amer. Math. Society, Providence 2002.
- [Lal 01] Laloë, F.: *Do we really understand quantum mechanics? Strange correlations, paradoxes and theorems*, Am. J. Phys. **69**, 655–701 (2001).

- [LB 02] Lomonaco, S. J. und Brandt, H. E. (Hrsg.): *Quantum computation and information*, American Mathematical Society, Providence, Rhode Island, 2002.
- [LB 03] Leuchs, G. und Beth, T. (Hrsg.): *Quantum Information Processing*, Wiley-VCH, Weinheim 2003.
- [LBC 00] Lewenstein, M., Bruß, D., Cirac, J. I., Kraus, B., Kuś, M., Samsonowicz, J., Sanpera, A. und Tarrach, R.: *Separability and distillability in composite quantum systems – a primer*, quant-ph/0006064 v2, (2000).
- [Leg 02] Leggett, A. J.: *Qubits, Cbits, Decoherence, Quantum Measurement and Environment*, in [Hei 02], S. 3–45, 2002.
- [Lom 02] Lomonaco, S. J., (Hrsg.): *Quantum computation: A Grand mathematical challenge for the twenty-first century and the millenium*, American Mathematical Society, Providence, Rhode Island, 2002.
- [Lom 02a] Lomonaco, S. J.: *Rosetta stone for Quantum Mechanics with an Introduction to Quantum Computation Version 1.5*, in [Lom 02], S. 3–65, 2002, quant-ph/0007045v1
- [LSP 98] Lo, H.-K., Spiller, T. und Popescu, S. (Hrsg.): *Introduction to Quantum Computing and Information*, World Scientific, Singapore 1998.
- [Lud 55] Ludwig, G.: *Zur Deutung der Beobachtung in der Quantenmechanik*, Phys. Bl. 11, 489–494 (1955).
- [Lud 89] Ludwig, G.: *Atoms: Are they real or are they objects*, Foundations of Physics 19, 971–983 (1989).
- [Lud 90] Ludwig, G.: *Concepts of States in Physics*, Found. of Phys. 20, 621–633 (1990).
- [Lud 96] Ludwig, G.: *Die Katze ist tot in* [AM 96], S. 183–208, 1996.
- [LW 03] Lidar, D. A. und Whaley, K. B.: *Decoherence-Free Subspaces and Subsystems in Irreversible Quantum Dynamics*, Benatti, F. und Floreanini (Hrsg.), S. 83–120, Springer, Berlin, 2003; quant-ph/0301032.
- [Mai 96] Mainzer, K.: *Naturphilosophie und Quantenmechanik* in [AM 96], S. 245–299, 1996.
- [Mer 02] Mertens, S.: *Computational Complexity for Physicists*, Computing in Science and Engineering 4, 31–47 (2002); cond-mat/0012185v2.
- [Mit 96] Mittelstaedt, P.: *Objektivität und Realität in der Quantenphysik*, in [AM 96]. S. 125–155, 1996.
- [Mit 98] Mittelstaedt, P.: *The interpretation of quantum mechanics and the measurement process*, Cambridge University Press, Cambridge 1998.
- [Mut 98] Mutschler, H.-D.: *Die Welt als Konstruktion* in Magerl, G. und Komarek, K. (Hrsg.) *Virtualität und Realität: Bild und Wirklichkeit der Naturwissenschaften*, Wien 1998.
- [MW 95] Mandel, L. und Wolf, E.: *Optical coherence and quantum optics*, Cambridge University Press, Cambridge 1995.
- [MW 98] Mahler, G. und Weberruß, V. A.: *Quantum networks – dynamics of open nanostructures*, 2 ed., Springer-Verlag, Berlin 1998.
- [NC 00] Nielsen, M. A. und Chuang, I. L.: *Quantum Computation and quantum information*, Cambridge University Press, Cambridge 2000.
- [NPN 97] Namiki, M., Pascasio, S. und Nakazato, H.: *Decoherence and quantum measurements*, World Scientific, Singapore, 1997.

- [Omn 94] Omnès, R.: *The Interpretation of Quantum Mechanics*, Princeton University Press, Princeton, 1994.
- [Pel 98] Pellizzari, T.: *Quantum computers, error-correction and networking: Quantum optical approaches*, in [LSP 98], S. 270–310, 1998.
- [Per 90] Peres, A.: *Neumark's Theorem on Quantum Inseparability*, Found. Phys. 20, 1441–1453 (1990).
- [Per 93] Peres, A.: *Quantum theory – concepts and methods*, Kluwer, Dordrecht 1993.
- [Pet 63] Petersen, A.: *The Philosophy of Nils Bohr*, Bull. Of the Atomic Scientists, **19** (Heft 7), 8–14 (1963).
- [Pit 00] Pittenger, A. O.: *An Introduction to Quantum Computing Algorithms*, Birkhäuser, Basel 2000.
- [Pre 98] Preskill, J.: *Course Informations for Physics 219/Computer Science 219 Quantum Computation (Formerly Physics 229)*, California Institute of Technology, 1998, <http://www.theory.caltech.edu/preskill/ph229>.
- [Pre 98 a] Preskill, J.: *Fault-tolerant quantum computation*, in [LSP 98], S. 213–269, 1998; quant-ph/9712048.
- [Pre 99] Preskill, J.: *Battling decoherence: The fault-tolerant quantum computer*, Phys. Today **52**, 6, 24, 30 (1999).
- [Pri 81] Primas, H.: *Chemistry, Quantum Mechanics and Reductionism*, Springer-Verlag, Berlin 1981.
- [PSE 96] Palma, G. M., Suominen, K. und Ekert, A. K.: *Quantum computers and dissipation*, Proc. R. Soc. Lond. **A 452**, 567–584 (1996).
- [PSM 87] Prasad, S., Scully, M. O. und Martienssen, W.: *A Quantum Description of the Beam Splitter*, Optics Communications **62**, 139–145, (1987).
- [PT 04] Peres, A. und Terno, D. R.: *Quantum information and relativity theory*, Rev. Mod. Phys. **76**, 93–123 (2004).
- [PV 98] Plenio, M. B. und Vedral V.: *Teleportation, entanglement and thermodynamics in the quantum world*, Contemporary Physics **39**, 431–446, (1998).
- [PVK 96] Plenio, M. B., Vedral, V. und Knight, P. L.: *Computers and communication in the quantum world*, Phys. World **9**, 10, 19–20 (1996).
- [PZ 02] Paz, J. P. und Zurek, W. H.: *Environment-Induced Decoherence and the Transition from Quantum to Classical* in [Hei 02], S. 77–148, 1902.
- [RBH 01] Raimond, J.M., Brune, M. und Haroche, S.: *Manipulating quantum entanglement with atoms and photons*, Rev. Mod. Phys. **73**, 565–582 (2001).
- [Rem 02] Rempe, G.: *Verschränkte Quantensysteme: Vom Welle-Teilchen-Formalismus zur Einzel-Photon-Lichtquelle*, in [Aud 02], S. 95–118, 2002.
- [RP 00] Rieffel, E. und Polak, W.: *An Introduction to Quantum Computing for Non-Physicists*, quant-ph/98090 v2, (2002).
- [Sak 85] Sakurai, Jun John: *Modern Quantum Mechanics*, Addison-Wesley, New York 1985.
- [Sch 35] Schrödinger, E.: *Die gegenwärtige Situation in der Quantenmechanik*, Naturwissenschaften **23**, S. 807–812, S. 823–828, S. 844–849 (1935).
- [Sch 64] Scheibe, E.: *Die kontingenten Aussagen in der Physik. Axiomatische Untersuchungen zur Ontologie der klassischen Physik und der Quantentheorie* Frankfurt 1964.

- [Sch 88] Schröter, J.: *Zur Axiomatik der Raum-Zeit-Theorie*, in [AM 88], S. 121–144 (1988).
- [Sch 90] Schröter, J.: *Das L-Konzept physikalischer Theorien*, Praxis der Naturwissenschaften – Physik 39, Heft 2, 20–27 (1990).
- [Sch 95] Schumacher, B.: *Quantum coding*, Phys. Rev. **A51**, 2738–2747 (1995)
- [Sch 96] Schumacher, B.: *Sending entanglement through noisy channels*, Phys. Rev. **A 54**, 2614–2628 (1996).
- [See 04] Seevinck, M. P.: *Holism, physical theories and quantum mechanics*, Studies in History and Philosophy of Science Part B, Vol. **35**, Issue 4, 693–712 (2004).
- [Sha 48] Shannon, C. E.: *A mathematical theory of communication*, Bell System Tech. J. **27**, 379–423, 623–656 (1948)
- [Sha 49] Shannon, C. E.: *Communication theory of secrecystems*, Bell Systems Technical Journal **28**, 656–715 (1949).
- [Sho 94] Shor, P. W.: *Algorithms for quantum computation: Discrete logarithms and factoring*, in Goldwasser, S. (Hrsg.): *Proc. of the 35th Annual Symp. on the Foundations of Computer Science (Santa Fe, New Mexico, 1994)*, IEEE Computer Science Society Press, Los Alamitos, California, 1994, pp. 124–134.
- [Sho 97] : Shor, P.W.: *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, Soc. Ind. Appl. Math. J. Comp. **26**, 1484–1509 (1997); quant-ph/9508027.
- [SS 04] Stolze, J. und Suter, D.: *Quantum Computing – A Short Course from Theory to Experiment*, Wiley-VCH, Weinheim 2004.
- [SSS 04] Scherer, A., Soklakov, A. N. und Schack, R.: *A simple necessary decoherence condition for a set of histories*, Phys. Lett. **A 326**, 307–314 (2004).
- [Sta 96] Stamatescu, I.-O.: *Stochastic Collapse Modells*, in [GJK 96], S. 249–267 (1996).
- [Ste 98] Steane, A. M.: *Quantum computing*, Rep. Prog. Phys. **61**, 117–173 (1998); quant-ph/9708022.
- [Stö 86] Stöckler, M.: *Philosophen in der Mikrowelt – ratlos?* Zeitschrift für allg. Wissenschaftstheorie **XVII/1**, 68–95, 1986.
- [Ter 01] Terhal, B. M.: *Detecting Quantum Entanglement*, quant-ph/0101032 v1, (2001) und Journal of Theoretical Computer Science **287**, 313–335 (2002).
- [Vai 01] Vaidman, L.: *The Many-Worlds Interpretation of Quantum Mechanics*, Stanford Encyclopedia of Physics, <http://plato.stanford.edu/entries>, 2001.
- [VdW 00] van der Wal, C. H., ter Haar, A. C. J., Wilhelm, F. K., Schouten, R. N., Harmans, C. J. P. M., Orlando, T. P., Lloyd, S. und Mooij, J. E.: *Quantum superposition of macroscopic persistent-current states*, Science **290**, 5492, S. 773–777 (2000).
- [Ved 02] Vedral, V. M.: *The role of relative entropy in quantum information theory*, Rev. Mod. Phys. **74**, 197–234 (2002)
- [Ver 26] Vernam, G. S.: *Cipher printing telegraph systems for secret wire and radio telegraphic communication*, J. Am. Just. Electr. Eng. **45**, 109–115 (1926).
- [vLo 02] Van Loock, P.: *Quantum Communication with Continuous Variables*, Fortschr. Phys. **50**, 1177–1372 (2002).
- [vNe 68] von Neumann, J.: *Mathematische Grundlagen der Quantenmechanik*, Springer-Verlag, Berlin 1968.

- [VP 98] Vedral, V. und Plenio, M. B.: *Basics of quantum computation* ; quant-ph/9802065.
- [VRP 97] Vedral, V., Rippin, M. A. und Plenio, M. B., *Quantum correlations, local interactions and error correction*, J. of Mod. Optics **44**, 2185–2205 (1997).
- [VV 00] Vojta, G. und Vojta, M.: *Teubner Taschenbuch der statistischen Physik*, Teubner, Stuttgart 2000.
- [WC 98] Williams, C. P. und Clearwater, S. H.: *Explorations in quantum computing*, Springer-Verlag, New York, 1998.
- [Weh 78] Wehrl, A.: *General properties of entropy*, Rev. Mod. Phys. **50**, 221–260, (1978).
- [Wer 89] Werner, R. F.: *Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model*, Phys. Review A **40**, 4277–4281 (1989).
- [Wer 01] Werner, R. F.: *Quantum Information Theory – an Invitation*, in [ABH 01], 14–57.
- [Wer 02] Werner, R. F.: *Quantenrechner – eine neue Generation von Supercomputern?* in [Aud 02], 141–168.
- [Wie 83] Wiesner, S.: *Conjugate coding*, Sigact news, 15 (1), 78–88 (1982).
- [WW 01] Werner, R. F. und Wolf, M. M.: *Bell Inequalities and Entanglement*, Quantum Information and Computation , **1**, 1–25 (2001).
- [Zbi 98] Zbinden, H.: *Experimental Quantum Cryptography*, in [LSP 98], S. 120–142, (1998).
- [Zeh 96] Zeh, H. D.: *The Program of Decoherence: Ideas and Concepts*, in [GJK 96], S. 5–34 (1996).
- [Zeh 00] Zeh, H. D.: *The Meaning of Decoherence*, in [BGJ 00] S. 19–42, (2000).
- [Zei 81] Zeilinger, A.: *General properties of lossless beam splitters in interferometry*, Am. J. Phys. **49**, 882, (1981).
- [Zur 82] Zurek, W. H.: *Environment-induced superselection rules*, Phys. Rev. D **26**, 1862–1880 (1982).
- [Zur 91] Zurek, W. H.: *Decoherence and the transition from quantum to classical*, Phys. Today **44**, 10, 36–44 (1991).
- [Zur 02] Zurek, W. H.: *Decoherence and the Transition from Quantum to Classical-Revisited*, Los Alamos Science, Nr. **27**, 2–25 (2002).
- [Zur 03] Zurek, W. H.: *Decoherence, einselection, and the quantum origins of the classical*, Rev. Mod. Phys. **75**, 715–775 (2003).

This Page Intentionally Left Blank

Register

- 50 : 50 beamsplitter **61**
 2-Teile-System **109**
- Abbildungsprinzipien **40**
 hypothetische **41**
 abgeschlossene Quantensysteme **31**
 Abweichung, mittlere quadratische **19**
 Additivitätsaxiom **16**
 adjoint operator, *siehe* Operator, adjungierter
 Äußere-Produkt-Darstellung, *siehe* dyadische
 Zerlegung
 Alice **110**
 allgemeine Messung **222**
 Alternativtheorie **40, 41, 168, 171**
 amplitude amplification, *siehe* Amplituden-
 verstärkung
 amplitude damping channel, *siehe* Amplitu-
 dendämpfungskanal
 Amplitudendämpfungskanal **245**
 Amplitudenverstärkung **193**
 ancilla, *siehe* Hilfssystem
 Anfrage **194**
 antilinear **2**
 Araki-Lieb-Ungleichung **153**
 Arithmetik, modulare **189**
 Ausgangstext **87**
- B92-Protokoll **178**
 Basis **111**
 orthonormale **3**
 Bayes's theorem, *siehe* Satz von Bayes
 Bayessche Annahme **19, 233**
 BB84-Protokoll **179**
 BBM92-Protokoll **181**
 bedingte Entropie **93**
 bedingte Wahrscheinlichkeit **17**
 Bell inequality, *siehe* Bellsche Ungleichung
 Bell measurement, *siehe* Bell-Messung
 Bell-Basis **156**
 Bell-Messung **161, 185**
 Bell-Zustand **112, 140, 159, 164, 182, 183,**
 185
 Bellsche Ungleichung **169, 170, 181**
 Bellsches Theorem **180**
 bi-orthogonal decomposition, *siehe* bi-
 orthogonale Zerlegung
 bi-orthogonal expansion, *siehe* bi-orthogonale
 Zerlegung
 bi-orthogonale Zerlegung **133, 225**
 bi-partite-system, *siehe* 2-Teile-System
 binäre Kodierung **86**
 Binärzahlen **87**
 binary coding, *siehe* binäre Kodierung
 binary digits, *siehe* Binärzahlen
 binary string, *siehe* Bit-Sequenz
 Bit **86, 87**
 bit by bit measurement, *siehe* Bit-für-Bit-
 Messung
 bit flip **48**
 bit flip error, *siehe* Bit-Flip-Fehler
 bit sequence, *siehe* Bit-Sequenz
 Bit-für-Bit-Messung **188**
 Bit-Flip-Fehler **207**
 Bit-Sequenz **87**
 black box, *siehe* Blackbox
 Blackbox **194**
 Bloch
 -Kugel **49, 244, 245, 251**
 -Punkt **49**
 -Vektor **49, 79**
 block coding, *siehe* Block-Kodieren
 Block-Kodieren **89**
 Bob **110**
 boolean function, *siehe* Funktion, Boolesche

- Botschaft **84**
 Bra-Raum **2**
 Bra-Vektor **2**, 111
 branch, *siehe* Zweig
 branching, *siehe* Verzweigung

 cascade, *siehe* Kaskade
 CCNOT-Gatter **126**
 CHSH-Ungleichung **170**, 181
 circuit, *siehe* Schaltung
 classical mixture, *siehe* klassisches Gemisch
 classical state, *siehe* klassischer Zustand
 classical theory, *siehe* klassische Theorie
 closed systems, *siehe* abgeschlossene Quantensysteme
 CNOT gate, *siehe* CNOT-Gatter
 CNOT-Gatter **124**, 158, 208
 CNOT-Transformation **160**
 collapse and revival, *siehe* Kollaps und Wiederkehr
 collective observable, *siehe* kollektive Observable
 complete positivity, *siehe* vollständige Positivität
 complete quantum operation, *siehe* vollständige Quantenoperation
 completeness relation, *siehe* Vollständigkeitsrelation
 composite quantum system, *siehe* zusammengesetztes Quantensystem
 composite system, *siehe* zusammengesetztes System
 compound system, *siehe* zusammengesetztes System
 computational complexity 210
 conditional entropy, *siehe* bedingte Entropie
 conditional probability, *siehe* bedingte Wahrscheinlichkeit
 conjugate linear, *siehe* konjugiert linear
 control qubit, *siehe* Kontroll-Qubit
 controlled NOT gate, *siehe* CNOT-Gatter
 controlled U gate, *siehe* kontrolliertes U-Gatter
 controlled-controlled NOT **126**
 convex sum, *siehe* konvexe Summe
 correlation coefficient, *siehe* Korrelationskoeffizient
 cryptogram, *siehe* Kryptogramm

 data compression, *siehe* Datenkompression
 Datenkompression **90**, 101
 decoherence, *siehe* Dekohärenz
 decomposition operators, *siehe* Zerlegungsoperatoren
 degeneracy, *siehe* Entartungsgrad
 degenerate, *siehe* entartet
 degree of mixture, *siehe* Gemischtheitsgrad
 Dekohärenz **75**, 207, 210, 250–252
 umgebungsinduzierte **253**, 255, 256
 delayed choice, *siehe* verzögerte Wahl
 density operator, *siehe* Dichteoperator
 Depolarisierung **244**
 depolarization, *siehe* Depolarisierung
 Deutsch gate, *siehe* Deutsch-Gatter
 Deutsch-Gatter **126**
 Deutsch-Jozsa-Problem **193**
 Deutsch-Problem **193**
 Dichtematrix **67**
 Dichteoperator **67**, 70, 73
 maximal gemischter **73**
 reduzierter 76, 116, **116**
 dichtes Quantenkodieren 182
 Dimension, des Hilbert-Raumes **35**
 Dirac-Schreibweise **2**
 dispersion, *siehe* Streuung
 Doppelspaltexperiment **23**
 Drehimpulsoperatoren **47**
 Dreiecks-Ungleichung **3**
 Dreiecksungleichung 153
 dual correspondence, *siehe* duale Korrespondenz
 duale Korrespondenz **2**
 dyad, *siehe* Dyade
 Dyade **5**
 dyadische Zerlegung **5**
 dyadisches Produkt **5**
 Dynamik
 unitäre **32**, 51, 52, 75, 103, 123, 213, 222

 eavesdropping, *siehe* Lauschangriff
 effect operator, *siehe* Effektoroperator
 Effektoroperator **226**
 Eigenbasis **7**, 99
 eigenbasis, *siehe* Eigenbasis
 Eigenschaft
 emergente **253**
 physikalische **34**

- eigenvalue, *siehe* Eigenwert
- eigenvector, *siehe* Eigenvektor
- Eigenvektor **3**
- Eigenwert **3**
- Eingriff **222**
- Einstein
 - Lokalität **167**
 - Realität **167**
- Elemente der physikalischen Realität **167**
- elements of physical reality, *siehe* Elemente der physikalischen Realität
- emergent property, *siehe* emergente Eigenschaft
- emergente Eigenschaft **253**
- Ensemble **69**
- ensemble decomposition, *siehe* Ensemblezerlegung
- Ensemblezerlegung **77, 104**
- entangled pure state, *siehe* verschränkter reiner Zustand
- entangled quantum state, *siehe* verschränkter Quantenzustand
- entangled state, *siehe* verschränkter Zustand
- entangled, *siehe* verschränkt
- entanglement swapping, *siehe* Verschränkungsaustausch
- entartet **7**
- Entartung **35**
- Entartungsgrad **31**
- Entropie
 - bedingte **93**
 - der Verschränkung **137**
 - klassische **85**
 - operationale Interpretation **90**
 - relative **91**
 - theoretische relative **103**
- entropy of entanglement, *siehe* Entropie der Verschränkung
- Entweder-Oder-Zustände **26**
- Entwicklung
 - bi-orthogonale **9**
- environment induced decoherence, *siehe* umgebungsinduzierte Dekohärenz
- EPR **131**
- EPR correlations, *siehe* EPR-Korrelationen
- EPR-Korrelationen **131, 165**
- Ereignis
 - unabhängiges **18**
 - zufälliges **16**
- Ereignisse
 - unvereinbare **16**
- Erinnerungszustand **263**
- error correction protocol **179**
- Erwartungswert **6**
- Euklidischer Algorithmus **210**
- Eve **179**
- Everett-Interpretation **263**
- exclusive events, *siehe* unvereinbare Ereignisse
- expectation value, *siehe* Erwartungswert
- experimentum crucis **171**
- Faktor-Raum **111**
- Fehler **90**
- fidelity, *siehe* Treue
- Form, unnormiert **68**
- Funktion, Boolesche **189**
- ganze Zahl **189**
- geheim **180**
- Gemenge **26, 31, 70, 261**
- Gemisch **76, 117**
 - klassisches **26**
 - separables **154**
 - statistisches **26, 31, 70**
- Gemischtheitsgrad **73, 79**
- general measurement, *siehe* allgemeine Messung
- generalized selective measurement, *siehe* verallgemeinerte selektive Messung
- Generalvoraussetzung **23**
- Gesamtentropie **151**
- Gesetz der großen Zahlen **88**
- ggT **200**
- GHZ state, *siehe* GHZ-Zustand
- GHZ-Zustand **172**
- Gleasons Theorem **80**
- greatest common divisor, *siehe* größter gemeinsamer Teiler
- größter gemeinsamer Teiler **200**
- Grover-Algorithmus **193**
- Grundbereich **39**
- Häufigkeit, relative **16**
- Hadamard
 - Gatter **56, 195**
 - Strahlteiler **62**
 - Transformation **160**

- Hamilton-Operator **33**
- hidden variables, *siehe* verborgene Parameter
- Hilbert-Raum, endlich-dimensionaler **1**
- Hilfs-Qubit **158**
- Hilfssystem **159**, 227, 270
- idempotent **12**
- Identitätsoperator **3**
- identity operator, *siehe* Identitätsoperator
- ignorance interpretation, *siehe* Ignoranzinterpretation
- Ignoranzinterpretation **79**, 261
- improper mixture **117**
- In-Out-Zugang **123**, 237
- incoherent superposition, *siehe* inkohärente Überlagerung
- incomplete, *siehe* unvollständig
- index state, *siehe* Indexzustand
- Indexzustand **267**
- Individualität **110**
- Information, wechselseitige **92**, 152, 156
- informationally complete measurement, *siehe* informationell vollständige Messung
- informationally complete, *siehe* informationell vollständig
- informationell vollständig **232**
- Informationsgehalt **90**
- inkohärente Überlagerung **75**
- inner product, *siehe* inneres Produkt
- inneres Produkt **2**
- integer, *siehe* ganze Zahl
- Interferenz **63**, 75
- Interferenzbild **24**, 62
- Interpretation **40**
- intervention, *siehe* Eingriff
- inverse operator, *siehe* inverser Operator
- inverser Operator **3**
- joint entropy, *siehe* Gesamtentropie
- joint probability **16**, **92**
- Kaskade **139**
- Ket-Raum **2**
- Ket-Vektor **2**
- key, *siehe* Schlüssel
- kick back, *siehe* Kick-back
- Kick-back **192**
- klassisch korreliert **155**
- klassische Physik **253**
- klassische Theorie **168**
- klassischer Zustand **255**
- klassisches Gemisch **26**
- Kode, quantentheoretisch fehlerkorrigierender **207**
- Kodierung, binäre **86**
- Kollaps und Wiederkehr **260**
- Komplement, orthogonales **3**
- Komponente **3**
- konjugiert linear **268**
- Kontroll-Qubit **124**
- konvexe Summe **74**
- Kopenhagener Interpretation **42**
- Kopie **179**
- Korrelationskoeffizient **165**
- Korreliertheit **92**, 94, 152
- Korrespondenz, duale **2**
- Korrespondenzregeln **40**
- Kraus operator, *siehe* Kraus-Operator
- Kraus-Operator **215**, 239, 245, 250
- Kryptogramm **177**
- Lauschangriff **179**
- law of large numbers, *siehe* Gesetz der großen Zahlen
- left polar decomposition, *siehe* links-polare Zerlegung
- linear operator, *siehe* linearer Operator
- linearer Operator **3**
- Liouville
 - Operator **15**, 68, 123
 - Raum **13**
- Liouvillian, *siehe* Liouville-Operator
- local measurement, *siehe* lokale Messung
- local operation, *siehe* lokale Operation
- local realism, *siehe* lokaler Realismus
- LOCC **130**
- lokal **109**, 167
- lokale Messung **116**
- lokale Operation **109**
- lokaler Realismus **167**
- lossless beamsplitter, *siehe* verlustfreier Strahlteiler
- Maß, projektionswertiges **228**
- Mach-Zehnder-Interferometer **62**, 143
- many-worlds interpretation, *siehe* Viele-Welten-Interpretation

Marker

- System **145**
- observable **146**
- zustand **145**, 267

Markierung **250**Matrizelement **6**

maximal verschränkter Zustand 137

maximally entangled state, *siehe* maximal verschränkter Zustand

mean square deviation, *siehe* mittlere quadratische Abweichung

mean value, *siehe* Mittelwert

measurement operator, *siehe* Messoperator

measurement outcome, *siehe* Messwert, *siehe* Messergebnis

memory state, *siehe* Erinnerungszustand

message, *siehe* Botschaft

Messdynamik 51, **213**, 222

Messergebnis **31**, 246

Messgerät **246**

Messoperator **216**, **223**

Messung **99**

- allgemeine **222**
- informationell vollständige **229**
- kollektive **158**
- lokale 115, **116**, 118, 157
- minimale 226, **226**
- nicht-lokale 157, **157**, 207, 208
- nicht-selektive 27, **71**, 104, 262
- nicht-selektive lokale 120
- projektive, *siehe* Projektionsmessung
- scharfe **221**
- schwache **221**
- selektive 27, **70**, 262
- selektive lokale **117**, 122
- unscharfe **221**
- völlig allgemeine **271**
- verallgemeinerte 159, **223**, 228
- selektive **216**

Messwert 223

Messwerte, korrelierte **122**

minimal measurement, *siehe* minimale Messung

minimale Messung 226

Minimalinterpretation 40, **42**, 79

Mittelwert **19**

mittlere quadratische Abweichung 19

mixture, *siehe* Gemisch

modular arithmetic, *siehe* modulare Arithmetik

modulare Arithmetik 189

most general measurements, *siehe* völlig allgemeine Messung

mutual information, *siehe* wechselseitige Information

natürliche Zahl 189

natural number, *siehe* natürliche Zahl

Naturphilosophie **39**

No-cloning-Theorem **143**

non-local measurement, *siehe* nicht-lokale Messung

non-local observable, *siehe* nicht-lokale Observable

non-negative integer, *siehe* natürliche Zahl

non-selective measurement, *siehe* nicht-selektive Messung

Norm **2**

norm, *siehe* Norm

normal operator, *siehe* normaler Operator

normaler Operator 6

Normerhaltung **11**

Observabelenoperator **31**

Observable **10**, 31

klassische **43**

kollektive **115**

nicht-lokale **115**, 122, 157

observable, *siehe* Observable

offene Quantensysteme 123

offenes System 213

ONB **3**

Ontologie **39**

open quantum system, *siehe* offene Quantensysteme

open system, *siehe* offenes System

operation element, *siehe* Operationselement

Operation, lokale **109**

operational **110**

Operationselement **215**, 239

operativ **110**

Operator

σ , *siehe* Pauli-Operator

-funktion **9**

adjungierter **4**

diagonalisierbarer **6**

erweiterter **113**

- hermitescher **9**
- inverser **3**
- linearer **3**
- lokaler Observablen- **116**
- normaler **6**
- unitärer **11**
- Operator, adjungierter **4**
- operator-sum decomposition, *siehe* Operator-summenzerlegung
- Operatorbasis **46**
- Operatorsummenzerlegung **214, 239**
- oracle, *siehe* Orakel
- Orakel **194**
- orthogonal **2**
- orthogonal decomposition, *siehe* orthogonale Zerlegung
- orthogonale Zerlegung **7**
- outer product, *siehe* dyadisches Produkt
- Parallelogrammgleichung **3**
- Parameter, verborgene **168**
- Paritätsbit **159**
- parity bit, *siehe* Paritätsbit
- partial trace, *siehe* Teilspur
- partial transposition, *siehe* Teil-Transposition
- Pauli
 - Matrix **48**
 - Operator **45, 47, 157**
- phase bit, *siehe* Phasenbit
- phase flip **48**
- phase flip error, *siehe* Phasen-Flip-Fehler
- phase gate **56**
- phase-damping channel, *siehe* Phasendämpfungskanal
- phase-flip channel, *siehe* Phasenflipkanal
- Phasen-Flip-Fehler **209**
- Phasenbit **159**
- Phasendämpfungskanal **251**
- Phasenflipkanal **252**
- Phasengatter **56**
- Phasenschieber **56, 75**
- Photon **178, 182**
- Photonenpolarisation **58**
- physikalische Eigenschaft **34**
- pointer observable, *siehe* Zählerobservable
- pointer state, *siehe* Zeigerzustand
- polar expansion, *siehe* polare Zerlegung
- polare Zerlegung **133**
- positive integer, *siehe* natürliche Zahl
- positive operator valued measure, *siehe* POVM
- positive operator, *siehe* positiver Operator
- positiver Operator **11**
- Positivität, vollständige **238**
- Postulat **31, 76, 115**
- POVM **226, 228**
 - Element **226, 228**
 - Messung **228, 230, 231, 243**
- POVM element, *siehe* POVM-Element
- POVM measurement, *siehe* POVM Messung
- POVM Messung **228**
- Präparationsentropie **106**
- Präparationsgerät **245**
- Präparationsverfahren **24, 30, 35**
- pre-measurement, *siehe* Vormessung
- preparation apparatus, *siehe* Präparationsgerät
- prime factorization, *siehe* Primfaktorzerlegung
- Primfaktorzerlegung **200**
- private amplification protocol **179**
- probability, *siehe* Wahrscheinlichkeit
- product vector, *siehe* Produktvektor
- Produkt
 - Hilbert-Raum **110**
 - operator **112**
 - vektor **111**
 - dyadisches **5**
 - inneres **2**
- Produktvektor **111**
- projection measurement, *siehe* Projektionsmessung
- projection operator, *siehe* Projektionsoperator
- projection valued measure, *siehe* projektionswertiges Maß, PVM
- Projektionsmessung **31, 32, 37, 51**
- Projektionsoperator **12**
 - lokaler **116**
- Projektor **7**
- proper mixture **117**
- properties, *siehe* physikalische Eigenschaft
- protocol, *siehe* Protokoll
- Protokoll **178**
- pure state, *siehe* reiner Zustand
- Purifizierung **136**
- PVM **228**
- Quanten-Zeno-Effekt **38**
- Quantenalgorithmus **193**

- Quantenberechnung **189**
Quantenbereich **28**
Quantencomputer **124, 189**
Quantendatenkompression **101**
Quantendraht **124, 188**
Quanteneffekt **28**
Quantenentropie **99**
Quantengatter **46, 56, 124, 188**
 universelle **126**
Quantengemisch **26**
Quanteninformation **100, 106**
Quanteninformationstheorie **83**
Quantenkanal **97**
Quantencode, fehlerkorrigierender **210**
Quantenkodieren, dichtes **182**
Quantenkorrelationen **131**
Quantenmessprozess **40**
Quantennetzwerk **188**
Quantenobjekte **43**
Quantenoperation **238, 239, 250, 271**
 vollständige **270**
Quantenparallelismus **193, 197**
Quantenradieren **146**
Quantenregister **187**
Quantenschaltung **123, 160, 188**
Quantensignalensemble **97**
Quantensignalquelle **97**
Quantensprünge **245**
Quantensystem **29**
 abgeschlossenes **31**
 offenes **123**
 zusammengesetztes **114**
Quantenteleportation **183**
quantentheoretisch fehlerkorrigierender Kode
 207
Quantentheorie **28**
Quantenzustand **26, 30, 76**
 klassisch korreliert **130**
 verschränkter **131**
quantum algorithm, *siehe* Quantenalgorith-
 mus
quantum circuit, *siehe* Quantenschaltung
quantum computation, *siehe* Quantenberech-
 nung
quantum computer, *siehe* Quantencomputer
quantum correlations, *siehe* Quantenkorrela-
 tionen
quantum data compression, *siehe* Quantenda-
 tenkompression
quantum dense coding, *siehe* dichtes Quan-
 tenkodieren
quantum erasure, *siehe* Quantenradieren
quantum error-correcting code, *siehe* quan-
 tentheoretisch fehlerkorrigierender
 Kode
quantum gate, *siehe* Quantengatter
quantum information, *siehe* Quanteninforma-
 tion
quantum mixture, *siehe* Quantengemisch
quantum network, *siehe* Quantennetzwerk
quantum objects, *siehe* Quantenobjekte
quantum operation, *siehe* Quantenoperation
quantum parallelism, *siehe* Quantenparallelis-
 mus
quantum register, *siehe* Quantenregister
quantum signal source, *siehe* Quantensignal-
 quelle
quantum state, *siehe* Quantenzustand
quantum system, *siehe* Quantensystem
quantum teleportation, *siehe* Quantentelepor-
 tation
quantum wire, *siehe* Quantendraht
Qubit **45, 100**
 -System **45, 57**
Quellentext **177**
query, *siehe* Anfrage

Rabi
 -Frequenz **54**
 -Oszillation **54**
random event, *siehe* zufälliges Ereignis
random variable, *siehe* Zufallsvariable
randomized algorithm, *siehe* Zufallsalgorith-
 mus
real **167**
Realisierung des Hadamardgatters
 optische **61**
Realismus, lokaler **167, 168**
Realität **29, 43**
Rechenbasis **45**
recoherence, *siehe* Rekohärenz
reduced density operator, *siehe* reduzierter
 Dichteoperator
reduzierter Dichteoperator **116**
Reflexionsfaktor **60**
reiner Zustand **31**
Rekohärenz **261**
relative frequency, *siehe* relative Häufigkeit

- relative Häufigkeit 16
- remainder, *siehe* Rest
- resolution of the identity, *siehe* dyadische Zerlegung des Identitätsoperators
- Rest **189**
- Restunsicherheit **93**
- right polar decomposition, *siehe* rechts-polare Zerlegung
- Satz
 - von Bayes **18**, 71, 233
 - von der Operatorsummenzerlegung **239**
 - von der totalen Wahrscheinlichkeit **18**
- scalar product, *siehe* Skalarprodukt
- Schaltung **62**
 - Quanten- **62**
- scharfe Messung 221
- Schlüssel **177**, 178
- Schmidt
 - Basen **135**
 - Koeffizienten **135**
 - Zahl **135**
 - Zerlegung **133**
 - decomposition, *siehe* Schmidt-Zerlegung
- Schrödinger
 - Bild **33**, 123, 238
 - Gleichung **33**, 34
- Schrödinger picture, *siehe* Schrödinger-Bild
- Schrödingers Katze **255**
- Schumachers quantum noiseless coding theorem **101**
- schwache Messung 221
- selbstadjungiert **9**
- selective measurement, *siehe* selektive Messung
- self-adjoint, *siehe* selbstadjungiert
- separabel **157**
- Separabilitätsproblem **132**
- separability problem, *siehe* Separabilitätsproblem
- separable state, *siehe* separabler Zustand
- separabler Zustand 131
- sequence, *siehe* Sequenz
- Sequenz **84**
 - typische **89**
- Shannon-Entropie 83, **85**, 90, 99, 105
- Shannons noiseless coding theorem, *siehe* Shannons Theorem
- Shannons Theorem **90**
- sharp measurement, *siehe* scharfe Messung
- signal source, *siehe* Signalquelle
- Signalensemble **84**
- Signalquelle **84**
 - stochastisch erinnerungslose **84**
- Signalzustand **97**
- Simulation **117**
- Skalarprodukt **2**, 112
- source text, *siehe* Quellentext
- spectral decomposition, *siehe* spektrale Zerlegung
- spectral theorem, *siehe* Spektraltheorem
- spektrale Zerlegung 7
- Spektraltheorem **10**
- Spin **47**, **57**
- Spin- $\frac{1}{2}$ -Teilchen 57, **181**
- Spur **6**, 113
- standard deviation, *siehe* Standardabweichung
- Standardabweichung **19**
- Standardbasis **45**
- Standardinterpretation **29**, 41–43, 262
- state, correlated **129**
- statistical mixture, *siehe* statistisches Gemisch
- statistisches Gemisch 70
- Stern-Gerlach-Experiment **217**
 - ideales **219**
 - nicht-optimales **218**
- Strahlteiler, verlustfreier **59**
- Streifenkontrast **64**
- Streuung **19**
- string, *siehe* Zeichenfolge
- Subadditivität **94**, 152
- subadditivity, *siehe* Subadditivität
- subsystem, *siehe* Untersystem
- Summe, konvexe **74**
- Superauswahlregeln **43**
- Superoperator **15**, 243
- superoperator, *siehe* Superoperator
- Supremumsnorm **6**
- System
 - freies **30**
 - offenes **213**
 - total isoliertes **30**
 - zusammengesetztes 76, **109**
- Szenario der Quantentheorie **23**, 245
- target qubit, *siehe* Ziel-Qubit

- Teil-Transposition **240**
- Teiler, größter gemeinsamer **200**
- Teilspur **113**
- Teilsystem **109, 115**
- Teilsystem-Operator **113**
- Tensorprodukt **111, 115**
- Terme, theoretische **41**
- Theorie
 - klassische **168**
 - physikalische **39**
 - stochastische lokal-realistische **168**
- time development operator, *siehe* Zeitentwicklungsoperator
- Toffoli gate, *siehe* Toffoli-Gatter
- Toffoli-Gatter **126**
- trace, *siehe* Spur
- transformation apparatus, *siehe* Transformationsgerät
- Transformationsapparat **28, 245**
- Transformationsgerät **245**
- Transmissionsfaktor **60**
- Transposition **240**
- transposition, *siehe* Transposition
- Treue **90**
- triangle inequality, *siehe* Dreiecksungleichung
- triorthogonal decomposition, *siehe* triorthogonale Zerlegung
- triorthogonale Zerlegung **259**
- typical sequence, *siehe* typische Sequenz
- typical subspace, *siehe* typischer Unterraum
- typische Sequenz **89**
- typischer Unterraum **101**
- Überlagerung, inkohärente **75**
- Übertragung von Verschränkung **185**
- U-Gatter, kontrolliertes **125**
- Umpräparation **27**
- Unbestimmtheit **19**
- uncertainty, *siehe* Unbestimmtheit, *siehe* Ungewissheit
- Ungewissheit **85**
- Ungleichung
 - Dreiecks- **153**
 - Gibbs- **91**
 - Kleinsche **104**
 - Schwarzsche **2**
- unitär **11**
- Unitäräquivalenz **11**
- unitary, *siehe* unitär
- universal quantum gates, *siehe* universelle Quantengatter
- universelle Quantengatter **126**
- unscharfe Messung **221**
- unsharp measurement, *siehe* unscharfe Messung
- Unterräume
 - dekohärenzfreie **210**
 - typische **101**
- Untersystem **109**
- Ununterscheidbarkeit **110**
- unvereinbare Ereignisse **16**
- unvollständig **168**
- Variable, klassische **35**
- variance, *siehe* Varianz
- Varianz **19**
- verborgene Parameter **168**
- verlustfreier Strahlteiler **59**
- verschränkt **111, 193, 213**
- verschränkter Quantenzustand **131**
- verschränkter reiner Zustand **118**
- verschränkter Zustand **109**
- Verschränkung **110, 129, 136, 153, 172, 219, 238**
- Verschränkungs austausch **184**
- Verschränkungsmaß **136**
- verzögerte Wahl **147, 149**
- Verzweigung **222**
- Viele-Welten-Interpretation **43, 263**
- völlig allgemeine Messung **271**
- vollständige Positivität **238**
- vollständige Quantenoperation **270**
- vollständiges System kommutierender Observabler **10**
- Vollständigkeitsrelation **5**
- von-Neumann
 - Entropie **83, 106**
 - Gleichung **68, 123**
 - Messung **32**
- Vormessung **257**
- Vorthorie **39**
- Wahl, verzögerte **149**
- Wahrscheinlichkeit **16, 32, 116**
 - bedingte **17, 70, 92**
 - klassische **69**
- weak measurement, *siehe* schwache Messung

- wechselseitige Information 92
- Weder-Noch-Zustand **26**
- Welcher-Weg-Marker **145**
- which-way-marker, *siehe* Welcher-Weg-Marker
- Wirklichkeit **39**
 - physikalische **41**
- Wirklichkeitsbereich, erschlossener **41**
- Wissenschaftstheorie **39**
- XOR gate, *siehe* CNOT-gatter
- Zählerobservable 262
- Zahl
 - ganze **189**
 - natürliche **189**
- Zeichenfolge **84**
- Zeigerzustand 257, **261**
- Zeit **35**
- Zeitentwicklungsoperator **32, 34**
- Zeno
 - Effekt **37**
 - Zeit **37**
- Zerlegung
 - bi-orthogonale **133, 225**
 - dyadische **5**
 - des Identitätsoperators **5**
 - links-polare **225**
 - orthogonale **7**
 - polare **133**
 - rechts-polare **225**
 - spektrale **7**
 - triorthogonale 259
- Zerlegungsoperator 215, **239**
- Ziel-Qubit **124**
- Zufallsalgorithmus **202**
- Zufallsgröße **19**
- Zufallsvariable **84**
- zusammengesetztes Quantensystem 114
- zusammengesetztes System 109
- Zustand 24, **69, 117, 193**
 - klassischer **24, 255**
 - korrelierter **129**
 - maximal verschränkter **137**
 - reiner **26, 31, 67, 73, 74, 139**
 - relativer **120, 267**
 - separabler **131**
 - verschränkter **109**
 - reiner **118**
- Zustandsbestimmung **80**
- Zustandspräparation **99**
- Zustandsschätzung **233**
- Zustandsvektor **31, 35**
- Zweig **263**