

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

„Mit Qubits zur Quantenphysik:
Ein quanteninformationstheoretischer Zugang
für den Schulunterricht“

verfasst von / submitted by

David Schaubmair, BEd

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of
Master of Education (MEd)

Wien, 2021 / Vienna 2021

Studienkennzahl lt. Studienblatt /
degree programme code as it appears on
the student record sheet:

UA 199 520 523 02

Studienrichtung lt. Studienblatt /
degree programme as it appears on
the student record sheet:

Master Lehramt UF Mathematik und Physik

Betreut von / Supervisor:

Mag. Dr. Beatrix Hiesmayr, Privatdoz.

Ein Zitat aus der Serie *The Big Bang Theory*, das ich zu Beginn meines Studiums in keinsten Weise nachvollziehen konnte, und nun ein bisschen besser verstehe:

„Quantum physics makes me so happy. It’s like looking at the universe naked.“

- Sheldon Cooper

Abstract

Deutsch

Diese Arbeit befasst sich mit quanteninformationstheoretischen Aspekten der Quantenphysik und gliedert sich in einen fachlichen und einen didaktischen Teil. Der erste Teil richtet sich inhaltlich an Studierende und interessierte Lehrpersonen, hierfür wird auf Grundkenntnisse zur Quantenphysik aufgebaut, um grundlegende Inhalte der Quanteninformationstheorie mit einem Fokus auf Quantencomputer darzustellen. Hierdurch soll eine kompakte Zusammenfassung zu physikalischen Grundlagen mit besonderem Augenmerk auf Verschränkung geboten werden, welche um eine theoretische Betrachtung der Funktionsweise von Quantencomputern und eine Diskussion des derzeitigen Entwicklungsstands erweitert wird. In einem zweiten Teil wird ein Zugang zur Quantenphysik im Schulunterricht vorgestellt, welcher auf die Thematisierung von Qubits aufbaut und die zuvor genannten Inhalte auf Schulniveau herunterbrechen und damit in den Unterricht bringen soll. Durch diesen inhaltlichen Aufbau auf Zwei-Level-Systeme werden grundlegende Charakteristika der Quantenmechanik an diskreten Systemen erarbeitet, wodurch eine spätere Ausweitung auf kontinuierliche Systeme und deren Behandlung unter diesen Gesichtspunkten ermöglicht werden soll.

English

This thesis deals with quantum information theory aspects of quantum physics and consists of a technical and a didactical part. In terms of content, the first part is aimed at students and interested teachers. For this purpose, knowledge of quantum physics is built upon in order to present fundamental contents of quantum information theory with a focus on quantum computers. Hereby a compact summary of physical basics with special emphasis on entanglement is offered, which is extended by a theoretical consideration of the functioning of quantum computers and a discussion of the current state of development. In a second part, an approach to teaching quantum physics in secondary education is presented, which builds on the topic of qubits and thus brings the aforementioned content into the classroom by breaking it down to school level. In this approach basic characteristics of quantum mechanics are worked out on discrete systems by using this content structure that is based on two-level systems, whereby a later extension to continuous systems and their treatment under these points of view is to be made possible.

Anmerkung: Aus Gründen der besseren Lesbarkeit wurde in der vorliegenden Arbeit das *Gendersternchen* für geschlechtergerechten Sprachgebrauch durch den *Gender-Doppelpunkt* ersetzt.

Danksagung

Zuallererst möchte ich Mag.^a Dr.ⁱⁿ Beatrix Hiesmayr meinen Dank aussprechen, die mir durch eine breite Auswahl an Möglichkeiten in der Themenfindung meiner Masterarbeit geholfen hat und mir bei der Konzeption der Arbeit freie Hand gelassen hat, sodass es mir möglich war, mich in jede beliebige Richtung hin weiterzuentwickeln.

Zudem möchte ich meiner Partnerin Katharina Heß danken, die nicht nur diese Arbeit zur Korrektur gelesen hat, sondern über die gesamte Studienzeit hinweg für mich eine wichtige Stütze in jeder erdenklichen und wünschenswerten Weise war.

Zu guter Letzt möchte ich meinen Eltern, Josef und Elisabeth Schaubmair, dafür danken, dass sie mich sowohl finanziell als auch moralisch stets in all meinen Entscheidungen unterstützt haben.

Inhaltsverzeichnis

1	Vorwort	1
I	Theorie	3
2	Physikalische Grundlagen	5
2.1	Quanteninformationstheorie	6
2.2	Postulate und mathematische Grundlagen	8
2.3	Reine und gemischte Zustände	13
2.4	Mehrteilchensysteme	20
2.5	Entropie	23
2.6	Verschränkung	26
2.7	Anwendungen von Verschränkung	34
2.8	Dekohärenz	37
3	Quantencomputer	41
3.1	Quantenschaltkreise und unitäre Transformationen	42
3.2	Universelle Quantencomputer	46
3.3	Parallelismus und prinzipielle Wirkungsweise	53
3.4	Shor und Grover	56
3.5	Quantum Hardware	64
3.6	Quantenkanäle und Dekohärenz	70
3.7	Zusammenfassung und Ausblick	74
II	Didaktik	77
4	Allgemeine didaktische Aspekte	79
4.1	Lernendenvorstellungen	80
4.2	Konzepte für Unterricht zur Quantenphysik	82
4.3	Kerninhalte der Quantenphysik	86
4.4	Aussichten für einen Ansatz mit Qubits	89
5	Unterrichtssequenz	95
5.0	Rahmenbedingungen und Vorbemerkungen	96
5.1	Einheit I - Spin	99
5.2	Einheit II - Superposition und Messung	102
5.3	Einheit III - Qubits und Realisierungen	105
5.4	Einheit IV - Zustände in der Blochkugel	108
5.5	Einheit V - Mehrere Qubits	111
5.6	Einheit VI - Quantencomputer	114
5.7	Einheit VII - Dekohärenz	117
5.8	Einheit VIII - Verschränkung: Phänomen	120
5.9	Einheit IX - Verschränkung: Anwendung	123
6	Ausblick	127
	Quellen	129
	Anhang	133

1 Vorwort

Ein Einstieg zur Quantenphysik erfolgt im Schulunterricht oftmals durch einen historischen Kontext, in vielen didaktischen Konzepten steht dabei die Behandlung des Doppelspalts und infolgedessen auch der Welle-Teilchen-Dualismus an oberster Stelle.

Aus quanteninformationstheoretischer Sicht scheint gerade letzteres Konzept nicht mehr unbedingt zeitgemäß, da dieses Phänomen lediglich eine Folgerung aus den Postulaten der Quantenmechanik darstellt, welche die Besonderheiten der Quantenphysik viel grundsätzlicher repräsentieren. Ebendiese Postulate, welche die vielen bekannten quantenphysikalischen Phänomene erst nach sich ziehen, könnten aber auch am einfachsten quantenmechanischen System besprochen und demonstriert werden - dem Qubit.

Eine einführende Behandlung der Besonderheiten der Quantenwelt am Qubit, die eine anschließende Thematisierung von quantenmechanischen Phänomenen, wie das Verhalten von Partikeln am Doppelspalt oder der Heisenberg'schen Unbestimmtheitsrelation, durch kontinuierliche Erweiterung immer noch ermöglicht, wäre aus folgenden Gründen ein zeitgemäßer Schritt:

Zum einen rücken *Quantencomputer* durch neuerliche Errungenschaften von Google [1] oder Erfolge aus China [2] auch im öffentlichen Interesse in den Mittelpunkt. Der Begriff „Quantencomputer“ wird dabei (nach persönlichem Empfinden) im Allgemeinen zwar als neuartig und technisch revolutionär eingestuft, eine ungefähre Funktionsweise bzw. auf welche Weise sich dieser vom klassischen Computer abhebt, bleibt dabei aber oft unerwähnt; zudem ist ein allgemein anerkannter Beweis bezüglich der tatsächlichen Vorzüge eines Quantencomputers noch nicht erbracht worden. Die Relevanz des Quantencomputers nimmt stetig zu, als technische Neuheit liegt eine Behandlung dessen wohl auch im Interesse von Schüler:innen, und diese lässt sich am besten mit Qubits denken.

Zum anderen ist das Themenfeld der Quantenphysik ein weit gestecktes, in einem Vergleich von Curricula aus 15 Nationen [3] werden dabei 17 verschiedene Themen herausgestrichen, die in diesem Themengebiet zu verorten sind. Da es aus zeitlichen Gründen unrealistisch ist, all diese Themen zu behandeln, muss eine Auswahl aus diesen erfolgen. Im Sinne einer *Scientific Literacy* gilt es also, abzuwägen, welche Kompetenzen und Kenntnisse zu einer wissenschaftlichen und physikalischen Grundbildung gehören. Wiederum einer persönlichen Auffassung und Beobachtung entspricht hier, dass besonders in Bezug zur Quantenphysik oftmals Begriffe wie *Verschränkung* und *Superposition* fehlerhaft gedeutet oder auf makroskopische Objekte übertragen werden und vermehrt in manch pseudowissenschaftlichen Argumenten Verwendung finden. Einer Unsicherheit in der Verwendung dieser Begriffe könnte abermals eine Behandlung an Qubits vorbeugen, zudem insbesondere die Verschränkung, ähnlich dem Quantencomputer, durch gelegentliche Thematisierung in der Tagespresse auch einer breiteren Gesellschaft grundsätzlich ein Begriff ist.

Ziel dieser Masterarbeit ist es, eine Unterrichtssequenz zu entwerfen und bereitzustellen, die einen alternativen Zugang zur Quantenphysik im Schulunterricht durch Einsatz und Thematisierung von Qubits ermöglicht und sich damit dem derzeitigen Wissensstand und aktuellen technischen Möglichkeiten annähert.

Hierfür erfolgt im ersten Teil der Arbeit eine Zusammenfassung der relevanten Inhalte, die das notwendige fachliche Hintergrundwissen für Lehrpersonen darstellt. Diese erstreckt sich von Kenntnissen, welche im Studium abgedeckt wurden, bis hin zur weiteren Vertiefung in Verschränkung und Grundlagen zu Quantencomputern. Zudem wird ein aktueller Einblick in die Technologie von Quantencomputern und deren Realisierungsmöglichkeiten gegeben.

Im zweiten Teil der Arbeit werden zunächst allgemeine fachdidaktische Aspekte des Themas zusammengefasst. Im Anschluss daran wird eine Sequenz von Unterrichtseinheiten dargestellt, welche durch benötigte Materialien, Erläuterungen zur Durchführung und didaktische Bemerkungen zu den einzelnen Einheiten ergänzt wird.

Teil I

Theorie

2 Physikalische Grundlagen

Zu einer konkreten Behandlung des Quantencomputers bedarf es nicht nur einiger Grundkenntnisse aus der Informationstheorie, sondern auch der Auffrischung und Erweiterung der physikalischen Grundlagen und der wesentlichen Konzepte aus der Quantentheorie.

Hierfür soll zunächst ein kleiner Einblick in die Entstehung der *Quanteninformationstheorie* gegeben werden, bevor der mathematische Formalismus der Quantenphysik nochmals kurz erläutert wird: Die Postulate der Quantenmechanik und der Umgang mit reinen und gemischten Zuständen (Kapitel 2.2 und 2.3) sollen anfangs zusammengefasst und erläutert werden, zusammen mit dem Umgang mit Mehrteilchensystemen soll damit das mathematische Fundament für weitere Behandlungen gelegt werden.

Die Idee der *Entropie* stellt sowohl in der klassischen Informationstheorie, als auch in physikalischen Systemen ein bedeutendes Instrument dar, um im Anschluss auch das Phänomen der *Verschränkung* eingehend zu behandeln und diese zu quantifizieren. Verschränkung ist ein zentrales und für die Funktion des Quantencomputers wesentliches Konzept, im hierfür vorgesehenen Kapitel werden Inhalte aus dem Studium mathematisch nochmals in Kürze wiedergegeben und um weiterführende Konzepte, wie etwa Separabilitätskriterien, Schmidt-Zerlegung und einen kurzen Ausblick auf die Herausforderungen der Verschränkungsmaße erweitert. Zudem werden einige bedeutende Anwendungen der Verschränkung, wie die Teleportation von Zuständen oder abhörsichere Kommunikation, dargelegt. Zuletzt soll aufgrund praktischer Relevanz beim Quantencomputer die *Dekohärenz* an einem einfachen Beispiel thematisiert werden, wobei Verbindungen zur Verschränkung dargelegt werden.

An dieser Stelle sei zudem angemerkt, dass den folgenden Ausführungen weitgehend die *Kopenhagener Deutung* als Interpretation der Quantenmechanik zugrunde liegt, da diese in der Unterrichtssequenz in Kapitel 5 aus Gründen der einfacheren Verständlichkeit im Kontext des Quantencomputers gewählt wurde, diese Interpretation soll sich aufgrunddessen einheitlich durch die vorliegende Arbeit ziehen.

Insgesamt lehnt sich die inhaltliche Gliederung im folgenden Kapitel stark an die Vorlesung *Quanteninformation* von Mag. Dr. Nicolai Friis aus dem Sommersemester 2020 an.

2.1 Quanteninformationstheorie

Seidem die Grundsteine für die Quantenphysik durch die Erklärung des Photoeffekts mittels Teilchenhypothese durch Albert Einstein, die Beschreibung der Schwarzkörperstrahlung mithilfe des Planck'schen Wirkungsquantums durch Max Planck und die erfolgreiche Anwendung der Schrödingergleichung zur Erklärung des Wasserstoff-Spektrums durch Erwin Schrödinger gelegt wurden, hat sich die Quantentheorie in vielfacher Weise weiterentwickelt, wodurch auch Wege zu zahlreichen interdisziplinären Fachrichtungen eingeschlagen wurden.

So verzweigt sich die Quantentheorie nicht nur in Gebiete wie *Quantenoptik*, *Quantenelektrodynamik*, *Quantenthermodynamik* etc., sondern findet auch zunehmend Anwendungen in der Verknüpfung mit Chemie, Biologie oder Informationswissenschaften. Die Verbindung zu letzterem Gebiet soll hier die *Quanteninformationstheorie* darstellen, welche sich wiederum in zahlreiche weitere Themengebiete gliedert. Insofern stellen die in den nächsten Abschnitten folgenden Erkenntnisse nur einige Grundlagen dar, die für das Verständnis des Quantencomputers notwendig sind, aber für sich gesehen noch weit ausgebaut werden könnten.

Als historisch relevanter Bezug und einer der frühesten Anstöße für die Quanteninformationstheorie erweist sich hier die Diskussion zwischen Einstein, Podolski & Rosen (EPR) und Niels Bohr über die vermeintliche Unvollständigkeit der Quantenmechanik (vgl. [4]). Dieser Diskurs, weiterbehandelt durch John Stewart Bell (vgl. [5]) und die experimentellen Darlegungen sind geschichtsträchtige und inhaltliche Ankerpunkte der hier behandelten Theorie, die in Kapitel 2.6 näher erläutert werden.

Eine nähere Beschreibung der Quanteninformationstheorie aus heutiger Sicht kann dabei vorerst durch die Abgrenzung von der klassischen Informationstheorie erfolgen. Letztere beschäftigt sich mit Informationsverarbeitung in klassischen Systemen mithilfe des *klassischen Bits*, das die Werte 0 und 1 annehmen kann. Das quantenphysikalische Analogon des klassischen Bits stellt das *Qubit* (*quantum bit*) dar, welches nicht nur die klassischen Zustände $|0\rangle$ und $|1\rangle$ zulässt (hier bereits in Dirac-Notation, diese wird 2.2 nochmals aufgegriffen); vielmehr lässt sich durch *Superposition* jede Kombination dieser *Basiszustände* denken, die wie folgt aussieht:

$$|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle \quad \text{mit} \quad \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$$

Letztere Bedingung stellt lediglich sicher, dass die Addition jener Wahrscheinlichkeiten, das System bei entsprechender Messung in der Basis $\{|0\rangle, |1\rangle\}$ im Zustand $|0\rangle$ oder $|1\rangle$ vorzufinden, den Wert 1 ergibt. Drückt man α und β mit der Polardarstellung einer komplexen Zahl in Form von $c_j e^{i\varphi_j}$ aus, ergibt sich

$$|\Psi\rangle = c_0 e^{i\varphi_0} |0\rangle + c_1 e^{i\varphi_1} |1\rangle = e^{i\varphi_0} (c_0 |0\rangle + c_1 e^{i(\varphi_1 - \varphi_0)} |1\rangle)$$

Der Ausdruck $(\varphi_1 - \varphi_0)$ bezeichnet eine *relative Phase*, der Faktor $e^{i\varphi_0}$ entspricht einer globalen

Phase, welche nicht gemessen werden kann und damit auch für die weiteren physikalischen Aussagen über das System keine Bedeutung hat.

An dieser Stelle lässt sich bereits anmerken, dass also nur Zustände mit *zwei Eigenzuständen* betrachtet werden, so wie z.B. der Spin eines Fermions bei Messung mittels eines *Stern-Gerlach-Apparates* nur zwei Messergebnisse zulässt. Andere Realisierungen, wie die beiden niedrigsten möglichen Energiezustände eines Elektrons, die Polarisation eines Photons oder die räumlichen Moden eines Photons (also welche Wege das Photon beispielsweise in einem *Mach-Zehnder-Interferometer* nehmen kann) lassen sich dabei ebenso bedenken, um allerdings einen möglichst allgemeinen Zugang zur Quanteninformationstheorie zu gewähren, wird zur Verallgemeinerung lediglich von Qubits gesprochen und nur an geeigneten Stellen auf ein physikalisches System hingedeutet; konkrete technische Anwendungen und Realisierungen werden in Kapitel 3.5 behandelt. Ebenso möglich wären physikalische Systeme mit mehreren Eigenzuständen, die sich in Superposition befinden, diese werden *qutrits* (drei Eigenzustände) oder *qudits* (d Eigenzustände) genannt, werden allerdings im Folgenden nicht behandelt.

Bevor die *Blochkugel* formal in Kapitel 2.2 thematisiert wird, soll sie schon an diesem Punkt als Visualisierung für den Unterschied zwischen klassischen Bits und Qubits dienen:

Demnach kann jedes Zweizustands-System mithilfe eines *Blochvektors* in der Blochkugel visualisiert werden, wie in Abb. 1 gezeigt. Den klassischen Bits entsprechen die Zustände $|0\rangle$ und $|1\rangle$, diese sind demnach entlang der vertikalen Achse zu finden. Qubits hingegen können jeden Zustand, der auf der Sphäre liegt, einnehmen und stellen gewissermaßen eine Verallgemeinerung eines klassischen Bits dar, erst durch entsprechende Messung wird der Zustand auf einen der beiden Basiszustände reduziert.

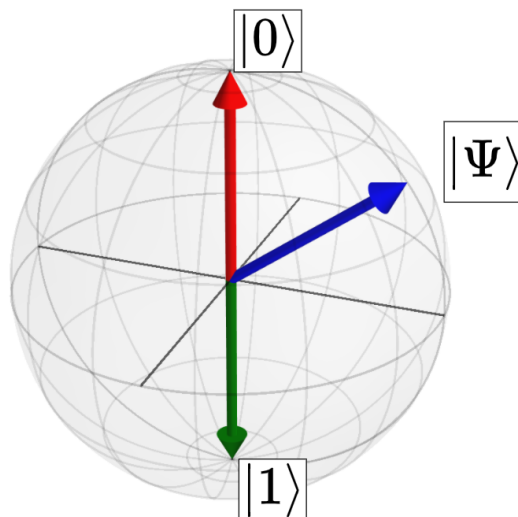


Abbildung 1: Beliebiger Qubit-Zustand und klassische Bitzustände

Zu erwähnen ist an diesem Punkt, dass das Qubit nicht in jeglicher Hinsicht eine Verallgemeinerung eines klassischen Bits ist. Letztere lassen sich für gewöhnlich kopieren, löschen oder ohne weitere Beeinflussung des Zustands messen. Für Qubits gelten diese Eigenschaften im Allgemeinen nicht, für den praktischen Umgang bei Berechnungen mit Quantencomputern sind diese allerdings nicht zwingend notwendig und können zum Teil umgangen werden (vgl. Kapitel 3.2).

2.2 Postulate und mathematische Grundlagen

Die mathematische Behandlung von Zuständen erfolgt nach dem quantenmechanischen Formalismus und wird von den Postulaten der Quantenmechanik geleitet. Diese sind Teil des Lehramtsstudiums und sollen im Folgenden nochmals zusammengefasst und entsprechende mathematische Grundlagen dargestellt werden. Hierfür werden die Inhalte auf diskrete Quantenmechanik beschränkt, da diese für die anschließenden Ausführungen relevant ist.

Zustände und Postulat I

Der Zustand eines physikalischen Systems kann als Sammlung aller verfügbaren Informationen über das System aufgefasst werden, diese Beschreibung kann z.B. in Form eines Vektors formuliert werden, diese Zustandsvektoren sind Elemente eines *Hilbert-Raumes* $\mathcal{H}$. Hilbert-Räume werden anschaulich von allen möglichen Quantenzuständen der Theorie aufgespannt, wobei für die konkrete Betrachtung eines Problems oftmals nur jener Teilraum betrachtet wird, der für das momentane Problem vonnöten ist. Hierbei spielt die Dimension des Hilbert-Raumes eine große Rolle: Für Qubits werden Hilbert-Räume der Dimension $d = 2$ betrachtet, an manchen Stellen wird hierfür die Notation $\mathcal{H}_2$ verwendet, um dies zu verdeutlichen. Durch die Beschreibung von Qubits mithilfe zweier komplexer Zahlen kann für die vorliegenden Ausführungen damit $\mathcal{H}_2 = \mathbb{C}^2$ gesetzt werden. (Betrachtet man allerdings z.B. die Ortsmessung eines Teilchens und eine Beschreibung dessen, werden aufgrund der kontinuierlichen Charakteristik der Ortsvariable unendlichdimensionale Hilbert-Räume betrachtet, wodurch es sinnvoll ist, für eine mathematische Beschreibung die Wellenfunktion heranzuziehen.)

Das erste Postulat der Quantenmechanik, das die Beschreibung durch Zustände betrifft, lässt sich wie folgt formulieren:

Postulat I - Zustandsvektoren: Jedem (isolierten/abgeschlossenen) physikalischen System ist ein komplexer vollständiger Vektorraum mit einem Inneren Produkt zugeordnet, der auch Zustandsraum des physikalischen Systems oder Hilbert-Raum $\mathcal{H}_2 = \mathbb{C}^2$ genannt wird. Das physikalische System ist vollständig durch einen normierten Zustandsvektor aus diesem Hilbert-Raum beschrieben.

Zum weiteren Umgang mit Zustandsvektoren soll im Folgenden auf mathematisch relevante Grundlagen und Formulierungen eingegangen werden. Zustandsvektoren werden in der bereits verwendeten Dirac-Notation geschrieben: $|\psi\rangle \in \mathcal{H}$.

Diese Vektoren werden *ket-Vektoren* genannt und lassen sich anschaulich als Spaltenvektoren interpretieren, z.B. kann eine Zuordnung in der *Rechenbasis* $|0\rangle, |1\rangle$ wie folgt aussehen:

$$|0\rangle \longleftrightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle \longleftrightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Um einen *bra-Vektor* aus dem dualen Hilbert-Raum $\langle\psi| \in \mathcal{H}^*$ aus einem ket-Vektor zu gewinnen, wird der ket-Vektor transponiert und komplex konjugiert, z.B. gilt für $|\psi\rangle \in \mathcal{H}_2$:

$$|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} \Rightarrow \langle\psi| = |\psi\rangle^\dagger = \frac{1}{\sqrt{2}}(1, -i) \quad (2.1)$$

Hilbert-Räume sind vollständig und mit einem inneren Produkt ausgestattet, welches eine Norm induziert durch $\|\psi\| = \sqrt{\langle\psi|\psi\rangle}$.

Im Folgenden sind einige Rechenregeln für $|\psi\rangle \in \mathcal{H}$, $\langle\phi| \in \mathcal{H}^*$ und $c_1, c_2 \in \mathbb{C}$ dargestellt:

$$\begin{aligned} \langle\phi|\psi\rangle &= \langle\psi|\phi\rangle^* \\ \langle\phi|c_1\psi_1 + c_2\psi_2\rangle &= c_1 \langle\phi|\psi_1\rangle + c_2 \langle\phi|\psi_2\rangle \\ \langle c_1\phi_1 + c_2\phi_2|\psi\rangle &= c_1^* \langle\phi_1|\psi\rangle + c_2^* \langle\phi_2|\psi\rangle \\ \langle\psi|\psi\rangle &= 0 \Leftrightarrow \|\psi\| = 0 \\ \langle\psi|\psi\rangle &> 0 \quad \forall \|\psi\| \neq 0 \end{aligned}$$

Anschaulich gesprochen erfolgt für $|\phi\rangle, |\chi\rangle \in \mathcal{H}_2$ durch die Bildung des inneren Produkts $\langle\phi|\chi\rangle$ die Projektion eines Zustandsvektors auf den anderen. Die im Postulat erwähnte Normierung erfolgt durch die Bedingung $\|\psi\| = |\langle\psi|\psi\rangle| = 1$, welche für Qubits der in Kapitel 2.1 erwähnten Forderung $|\alpha|^2 + |\beta|^2 = 1$ entspricht.

Hierbei soll erwähnt werden, dass die Darstellung von Zustandsvektoren in Form eines Spalten- oder Zeilenvektors zwar anschaulich und leichter verständlich wirkt als eine Darstellung mit ket- und bra-Vektoren, allerdings muss durch die Angabe eines Zeilenvektors auch stets angegeben werden, welche Basisvektoren den einzelnen Komponenten entsprechen. Durch die Dirac-Notation erfolgt allerdings eine allgemeinere und *basisunabhängige* Beschreibung von Zuständen, weswegen nur in konkreten Beispielen auf Vektoren zurückgegriffen wird, während allgemeine Aussagen stets in Dirac-Notation erfolgen.

Operatoren und Postulat II

Der Zustand eines physikalischen Systems verändert sich unter anderem durch äußere Einwirkungen, wie z.B. jenem der Messung. Diese Wirkung auf einen Zustand lässt sich mathematisch mit *linearen Operatoren* beschreiben, ein solcher bildet einen Zustand $|\psi\rangle$ auf einen neuen Zustand $|\psi'\rangle \in \mathcal{H}$ ab.

Unter einem Operator kann man sich eine Matrix vorstellen, wodurch es leichter fällt, eine Zerlegung eines Operators A in seine Matrixelemente $A_{ij} \in \mathbb{C}$ zu motivieren:

$$A = \sum_{i,j} A_{ij} |i\rangle \langle j|$$

Die Objekte $|i\rangle \langle j|$ stellen wiederum anschaulich ein (Tensor- bzw. Matrix-)Produkt eines Spalten- mit einem Zeilenvektor dar, wodurch eine Matrix entsteht, wobei $|i\rangle$ und $\langle j|$ jeweils eine (beliebige) Basis der Hilbert-Räume $\mathcal{H}$ und $\mathcal{H}^*$ darstellen. Eine ausführlichere Behandlung des Tensorprodukts und dessen Wirkungsweise erfolgt in Kapitel 2.4.

Durch die Zerlegung wird die Wirkungsweise eines solchen Operators auf einen beliebigen Zustand $|\psi\rangle \in \mathcal{H}$ ersichtlich:

$$A|\psi\rangle = \left(\sum_{i,j} A_{i,j} |i\rangle \langle j|\right) |\psi\rangle = \sum_{i,j} A_{i,j} |i\rangle \langle j|\psi\rangle = \sum_{i,j} \langle j|\psi\rangle A_{i,j} |i\rangle$$

Da $\langle j|\psi\rangle$ komplexe Zahlen ergeben, welche als Projektion von $|\psi\rangle$ auf den j -ten Basisvektor des dualen Hilbert-Raumes $\mathcal{H}^*$ aufgefasst werden können, ergibt sich dadurch eine Linearkombination der Basisvektoren des Hilbert-Raumes $\mathcal{H}$, somit liegt auch der neue Zustandsvektor tatsächlich in diesem. Eine Umkehrung ergibt sich dabei durch den *adjungierten Operator* $A^\dagger$, welcher wiederum komplex konjugiert und transponiert wird.

Im Folgenden soll eine Übersicht von speziellen Klassen von Operatoren und deren Eigenschaften gezeigt werden, da diese im Zuge der weiteren Postulate zu tragen kommen:

- *hermitesche Operatoren*: $A = A^\dagger$

Die Eigenwerte eines hermiteschen Operators sind stets reell.

- *Projektion*: $P = P^2$

Eine Projektion ist ein spezieller hermitescher Operator mit Eigenwerten $\lambda_i \in \{0, 1\}$. Eine mehrmalige Anwendung einer Projektion verändert den Zustandsvektor nach einmaliger Anwendung nicht mehr.

- *unitäre Operatoren*: $UU^\dagger = U^\dagger U = \mathbb{1}$

Unitäre Transformationen besitzen Eigenwerte mit $|\lambda_i| = 1$ und zeichnen sich beispielsweise dadurch aus, dass sie die Norm eines Vektors nicht verändern (und damit die Gesamtwahrscheinlichkeit erhalten).

Für hermitesche Operatoren gibt es Spektralzerlegungen, also eine Basis $\{|i\rangle\}$ des entsprechenden Hilbert-Raumes, in welcher der Operator wie folgt geschrieben werden kann (siehe z.B. [6, S.9-10]):

$$A = \sum_i \lambda_i |i\rangle \langle i|$$

Wendet man den Operator in dieser Form auf einen beliebigen Basisvektor $|j\rangle \in \{|i\rangle\}$ an, ergibt sich

$$A|j\rangle = \sum_i \lambda_i |i\rangle \langle i|j\rangle = \sum_i \langle i|j\rangle \lambda_i |i\rangle = \sum_i \delta_{ij} \lambda_i |i\rangle = \lambda_j |j\rangle$$

Hier wurde das *Kronecker-Delta* verwendet, womit sämtliche Terme mit $i \neq j$ wegfallen, da die zugehörigen Basisvektoren orthogonal sind. Betrachtet man das Ergebnis, erkennt man, dass es sich bei λ_i um Eigenwerte des Operators A mit den zugehörigen Eigenvektoren $|i\rangle$ handelt.

Mithilfe dieser Betrachtung lässt sich ein zweites Postulat formulieren:

Postulat II - Projektive Messung: Messungen einer Observablen $\mathcal{A}$ werden durch einen hermiteschen Operator A beschrieben mit der Spektralzerlegung

$$A = \sum_i \lambda_i P_i \quad \text{mit} \quad P_i = |i\rangle \langle i|,$$

wobei P_i Projektoren sind.

Diese Operatoren wirken auf dem Zustandsraum, mit dem das System beschrieben wird. Die möglichen Messwerte werden durch λ_i dargestellt. Die Wahrscheinlichkeit, den Messwert λ_i zu erhalten, ist durch die Wahrscheinlichkeit

$$p(\lambda_i) = \langle \psi | P_i^\dagger P_i | \psi \rangle = \langle \psi | P_i | \psi \rangle = \langle \psi | i \rangle \langle i | \psi \rangle = |\langle \psi | i \rangle|^2$$

gegeben und das System befindet sich nach der Messung in einem Eigenzustand des Operators A, welcher beschrieben wird durch

$$\frac{P_i |\psi\rangle}{\sqrt{\langle \psi | P_i | \psi \rangle}}$$

Aufgrund der Wahrscheinlichkeitserhaltung muss zudem $\sum_i P_i = \mathbb{1}$ gelten.

Hier gilt zu betonen, dass es sich lediglich um eine spezielle Art von Messungen - die projektiven

Messungen - handelt, für welche es eine Verallgemeinerung gibt, auf die allerdings hier nicht näher eingegangen wird; im Rahmen dieser Arbeit soll es genügen, projektive Messungen zu betrachten. Nicht unerwähnt soll zudem der Erwartungswert bei der Messung einer Observablen A an einem Zustand $|\psi\rangle$ bleiben, dieser lässt sich mit den Eigenwerten und Wahrscheinlichkeiten für entsprechende Messergebnisse wie folgt ausdrücken:

$$\langle A \rangle_{|\psi\rangle} = \sum_i \lambda_i p(\lambda_i) = \sum_i \lambda_i \langle \psi | i \rangle \langle i | \psi \rangle = \langle \psi | \left(\sum_i \lambda_i |i\rangle \langle i| \right) | \psi \rangle = \langle \psi | A | \psi \rangle$$

Um das Prozedere zu verdeutlichen, wird im Folgenden noch ein Beispiel einer Spinmessung betrachtet, wobei sowohl die Matrix- als auch die Dirac-Darstellung benutzt wird:

Sei der zu betrachtende Zustand durch $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ gegeben, an dem eine Spinmessung in z-Richtung mithilfe des Operators $\hat{S}_z = \frac{\hbar}{2}\sigma_z$ mit $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$ durchgeführt wird. Es ergibt sich unter Beachtung von $\langle 0|0\rangle = \langle 1|1\rangle = 1$ und $\langle 1|0\rangle = \langle 0|1\rangle = 0$:

Matrix-Notation	Dirac-Notation
$\hat{S}_z = \frac{\hbar}{2} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	$\hat{S}_z = \frac{\hbar}{2} (0\rangle\langle 0 - 1\rangle\langle 1),$
Eigenwerte hier an Diagonale ablesbar: $\lambda_{1/2} = \pm \frac{\hbar}{2}$	$\hat{S}_z$ in Spektraldarstellung mit $\lambda_{1/2} = \pm \frac{\hbar}{2}$
Eigenvektoren: $ v_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, v_2\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$	Eigenvektoren: $ v_1\rangle = 0\rangle$ und $ v_2\rangle = 1\rangle$
Projektoren: $P_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, P_2 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$	Projektoren: $P_1 = 0\rangle\langle 0 , P_2 = 1\rangle\langle 1 $
$ \psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \langle \psi = \frac{1}{\sqrt{2}}(1, 1)$	$ \psi\rangle = \frac{1}{\sqrt{2}}(0\rangle + 1\rangle), \langle \psi = \frac{1}{\sqrt{2}}(\langle 0 + \langle 1)$
$p(\lambda_1) = \langle \psi v_1 \rangle ^2 = \left \frac{1}{\sqrt{2}}(1, 1) \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right ^2 = \frac{1}{2}$	$p(\lambda_1) = \langle \psi v_1 \rangle ^2 = \left \frac{1}{\sqrt{2}}(\langle 0 + \langle 1) 0\rangle \right ^2 = \frac{1}{2}$
$\langle A \rangle_{ \psi\rangle} = \frac{\hbar}{4}(1, 1) \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 0$	$\langle A \rangle_{ \psi\rangle} = \frac{\hbar}{4}(\langle 0 + \langle 1)(0\rangle\langle 0 - 1\rangle\langle 1)(0\rangle + 1\rangle) = 0$

Tabelle 1: Vergleich einer Berechnung mit Matrix- und Dirac-Notation

Schrödingergleichung und Postulat III

Unitären Operatoren wird eine besondere Bedeutung beigemessen, die sich mit der Zeitentwicklung eines abgeschlossenen Systems, das keine Wechselwirkungen mit der Umgebung erfährt, beschäftigt. Diese Entwicklung wird durch folgendes Postulat beschrieben:

Postulat III - Zeitentwicklung: Die Entwicklung eines geschlossenen Quantensystems wird mit einer unitären Transformation beschrieben. D.h. ist das System zu einem bestimmten Zeitpunkt t_1 im Zustand $|\psi\rangle$, dann hängt der Zustand zu einem späteren Zeitpunkt $t_2 > t_1$ durch einen unitären Operator zusammen:

$$|\psi(t_2)\rangle = U |\psi(t_1)\rangle$$

Hier kann eine Verbindung zur Schrödingergleichung gezogen werden:

$$i\hbar \frac{d}{dt} |\psi(\vec{x}, t)\rangle = \hat{H} |\psi(\vec{x}, t)\rangle$$

Zunächst wählt man, wie für zeitunabhängige Potentiale üblich, einen Separationsansatz und teilt den Zustand in einen orts- und einen zeitabhängigen Teil $\chi(\vec{x})$ und $\phi(t)$. Der Hamiltonian $\hat{H}$ ist ein hermitescher Operator, also gibt es auch hierfür eine Spektralzerlegung: $\hat{H} = \sum_i E_i |E_i\rangle \langle E_i|$ mit den stationären Energiezuständen $|E_i\rangle$.

Dadurch ergibt sich im weiteren Verlauf die stationäre Schrödingergleichung $\hat{H} |\chi(\vec{x})\rangle = E |\chi(\vec{x})\rangle$, wobei der zeitabhängige Teil der Gleichung

$$i\hbar \frac{d}{dt} \phi(t) = E \phi(t)$$

unterliegt. Eine Lösung hierfür kann durch $\phi(t) = e^{-\frac{i}{\hbar} E t}$ angegeben werden, rückerinsetzen ergibt dann:

$$|\psi(\vec{x}, t)\rangle = e^{-\frac{i}{\hbar} \hat{H} t} |\psi(\vec{x}, 0)\rangle$$

Der Operator $\exp(-\frac{i}{\hbar} \hat{H} t)$ wird *Zeitentwicklungsoperator* genannt und ist unitär, womit dieser dem im Postulat definierten unitären Operator U entspricht.

2.3 Reine und gemischte Zustände

Reine und gemischte Zustände

Qubit-Zustände wie $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ können beispielsweise die Superposition von horizontal und vertikal polarisierten Photonen ($|H\rangle$ und $|V\rangle$) oder aber die Superposition von Spin-Zuständen eines Fermions ($|\uparrow\rangle$ und $|\downarrow\rangle$) beschreiben.

Betrachtet man nun eine Quelle, die mit jeweils einer Wahrscheinlichkeit von 50% Teilchen in den Zuständen $|0\rangle$ und $(\frac{1}{\sqrt{2}} |0\rangle + |1\rangle)$ aussendet, lässt sich dieses System nicht mehr mit einem Zustandsvektor beschreiben.

Es handelt sich um ein *Zustandsgemisch* bzw. einen *gemischten Zustand*, während Systeme, die

sich (wie der Zustand $|\psi\rangle$) mit einem Zustandsvektor beschreiben lassen, als *reine Zustände* bezeichnet werden. Für gemischte Zustände wirkt dabei eine *Ensemble-Interpretation* im ersten Moment anschaulicher als die Kopenhagener Deutung, da man hiermit eine Menge an entsprechend präparierten Systemen statt eines einzelnen Systems deuten kann, was sich für ein statistisches Gemisch anbietet.

Für die Charakterisierung solcher Systeme wird als Verallgemeinerung der *Dichteoperator* ρ herangezogen, der sowohl reine, als auch gemischte Zustände beschreiben kann und sich anschaulich als Matrix interpretieren lässt. Dichteoperatoren sind damit in ihrer mathematischen Struktur nicht Elemente desselben Hilbert-Raums wie die entsprechenden Zustandsvektoren, sondern eigentlich Elemente eines *Hilbert-Schmidt-Raums*; häufig werden diese der Einfachheit halber aber trotzdem mit $\mathcal{H}$ bezeichnet und Hilbert-Raum genannt, was auch für die folgenden Ausführungen übernommen wird.

Für einen reinen Zustand $|\psi\rangle$ lässt sich der Dichteoperator durch $\rho = |\psi\rangle \langle\psi|$ bilden, für ein Qubit bedeutet dies beispielsweise:

$$\rho = (\alpha|0\rangle + \beta|1\rangle)(\alpha^* \langle 0| + \beta^* \langle 1|) = |\alpha|^2 |0\rangle \langle 0| + \alpha\beta^* |0\rangle \langle 1| + \alpha^*\beta |1\rangle \langle 0| + |\beta|^2 |1\rangle \langle 1| = \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{bmatrix}$$

Gemischte Zustände, die sich als eine Mischung von reinen Zuständen beschreiben lassen, können als *konvexe Summe* von reinen Zuständen formuliert werden, also in Form von:

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i| \quad \text{mit} \quad \sum_i p_i = 1$$

Die Elemente in den Hauptdiagonalen lassen sich demzufolge als die Wahrscheinlichkeiten interpretieren, das System bei einer Messung in der Messbasis $\{|0\rangle, |1\rangle\}$ (Also mit Projektionsoperatoren $P_0 = |0\rangle \langle 0|$, $P_1 = |1\rangle \langle 1|$) im Zustand $|0\rangle$ bzw. $|1\rangle$ vorzufinden.

Mit diesen Überlegung können folgende allgemeine Eigenschaften für einen Dichteoperatoren festgelegt werden:

Dichteoperatoren sind...

- *...normiert*: $\text{Tr}(\rho) = 1$ - Dies entspricht der *Spurbildung (Trace)* (also der Summe über die Diagonalelemente) und der Bedingung, dass die Gesamtwahrscheinlichkeit erhalten bleibt
- *...hermitesch*: $\rho = \rho^\dagger$ - Dadurch sind alle Eigenwerte reell, was für Wahrscheinlichkeiten natürlich gegeben sein muss
- *...positiv semidefinit*: $\langle\phi|\rho|\phi\rangle \geq 0 \quad \forall |\phi\rangle$ - Durch diese Bedingung wird zudem sichergestellt, dass alle Wahrscheinlichkeiten tatsächlich nur Werte ≥ 0 annehmen können.

Bei einer gegebenen Matrix lässt sich anhand dieser Bedingungen also überprüfen, ob es sich tatsächlich um einen Dichteoperator und damit um eine geeignete Beschreibung für ein physikalisches System handelt.

Ebenso lässt sich überprüfen, ob es sich um einen reinen oder gemischten Zustand handelt, indem beispielsweise überprüft wird, ob alle Eigenwerte λ_i entweder den Wert 0 oder 1 annehmen. Dies lässt sich wie folgt interpretieren: Handelt es sich um einen reinen Zustand, lässt sich auch eine Basis finden, in der mit Sicherheit ein bestimmtes Messergebnis festgestellt werden kann (beispielsweise durch entsprechende Rotation des Messapparates bei Polarisationsmessungen oder Spinmessungen). Liegt jedoch ein gemischter Zustand vor, lässt sich eine solche Stellung des Messapparates nicht finden, und an der Hauptdiagonale bleibt stets mehr als ein positiver Wert, das Messergebnis lässt sich also nie mit Sicherheit vorhersagen.

Eine weitere Anmerkung zur Unterscheidung von reinen und gemischten Zuständen soll an dieser Stelle folgen:

Bei reinen Zuständen handelt es sich um *kohärente Überlagerungen* in Form von Superposition von Zuständen, das bedeutet, man kann also nicht sagen, das System befindet sich dem einen *oder* dem anderen Zustand. Für einen gemischten Zustand handelt es sich aber um ein statistisches Gemisch, also könnte man tatsächlich sagen, dass der eine oder andere Zustand vorliegt, die entsprechenden Wahrscheinlichkeiten sind klassisch erklärbar und nicht zwingend eine Folge der Superposition, man spricht von *inkohärenten Überlagerungen*. Der Dichteoperator lässt sich damit in eine gewichtete Summe von Dichteoperatoren reiner Zustände zerlegen, wobei es im Allgemeinen unendlich viele Möglichkeiten gibt, eine solche Zerlegung für einen gegebenen gemischten Zustand anzugeben.

Eine Folge von kohärenten Überlagerungen ist dabei die Fähigkeit zur *Interferenz* und dem Auftreten diverser Interferenzerscheinungen bei Messungen, so liegt z.B. beim Doppelspalt ohne Messung am Spalt eine kohärente Überlagerung vor und Interferenz tritt in Erscheinung. Stellt man allerdings durch eine Messung fest, durch welchen Spalt die beobachteten Teilchen gewandert sind, verliert man diese Interferenzfähigkeit, es ergibt sich ein klassisches Bild und eine inkohärente Überlagerung, also ein gemischter Zustand (*entweder* Spalt 1 *oder* Spalt 2).

Der Verlust von Interferenzfähigkeit und damit der Kohärenz (also der Übergang von reinen Zuständen und der Superposition von Basiszuständen zu gemischten Zuständen und klassischen Unterscheidungen) wird unter dem Begriff *Dekohärenz* zusammengefasst, dieser wird in Kapitel 2.8 näher beleuchtet.

Blochvektor und Blochkugel

Die Messung des Spins von Fermionen kann in der Quantenmechanik durch den Drehimpulsoperator

$$\hat{S}_i = \frac{\hbar}{2} \sigma_i \quad \text{mit} \quad i \in \{0, 1, 2, 3\}$$

dargestellt werden. Die hier vorkommenden *Pauli-Operatoren* sind nicht nur für die Messung von Spin-Zuständen, sondern auch die Darstellung von Qubits im Allgemeinen relevant, da sie mathematisch eine Basis für den Vektorraum der 2x2-Matrizen darstellen. Die vier Operatoren

lassen sich wie folgt (in Matrixdarstellung und Dirac-Notation) darstellen:

$$\begin{aligned}\sigma_0 &= |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & \sigma_1 &= |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ \sigma_2 &= i(|1\rangle\langle 0| - |0\rangle\langle 1|) = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} & \sigma_3 &= |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\end{aligned}$$

Die Pauli-Operatoren sind zudem *unitär*, *hermitesch*, *spurlos* (also $\text{Tr}(\sigma_i) = 0$) und besitzen Eigenwerte ± 1 .

Bildet man die Erwartungswerte der einzelnen Pauli-Operatoren (bis auf σ_0 , welcher der Einheitsmatrix $\mathbb{1}$ entspricht) für einen beliebigen Zustand $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, erhält man folgende Ergebnisse (wobei die Indizes ab diesem Punkt gegen die üblichen Bezeichnungen ausgetauscht werden, also $\sigma_1 = \sigma_x$, $\sigma_2 = \sigma_y$, $\sigma_3 = \sigma_z$):

$$\begin{aligned}a_x &= \langle\psi|\sigma_x|\psi\rangle = \alpha^*\beta + \alpha\beta^* \\ a_y &= \langle\psi|\sigma_y|\psi\rangle = -i\alpha^*\beta + i\alpha\beta^* \\ a_z &= \langle\psi|\sigma_z|\psi\rangle = |\alpha|^2 - |\beta|^2\end{aligned}$$

Fasst man diese Erwartungswerte als Vektorkomponenten eines dreidimensionalen Vektors $\vec{a} \in \mathbb{R}$, der *Blochvektor* genannt wird, auf, ergibt sich die Norm des Vektors zu

$$|\vec{a}| = \sqrt{a_x^2 + a_y^2 + a_z^2} = 1$$

wobei auf einen ausführlichen Rechengang verzichtet wurde. Bedeutsam ist hier, dass man also mithilfe der Pauli-Operatoren jedem reinen Zustand einen Vektor der Länge 1 zuordnen kann. Eine allgemeinere Darstellung dessen lässt sich mit der *Bloch-Zerlegung für einzelne Qubits* ausdrücken, die besagt, dass jeder Dichteoperator eines Qubit-Zustands in Form von

$$\rho = \frac{1}{2}(\mathbb{1} + \sum_i a_i \sigma_i) \tag{2.2}$$

repräsentiert werden kann, wobei mit a_i die Komponenten des Blochvektors, also Erwartungswerte der Pauli-Operatoren, gemeint sind. In Kurzform wird diese Zerlegung dabei oft als $\rho = \frac{1}{2}(\mathbb{1} + \vec{a}\vec{\sigma})$ geschrieben, wobei mit $\vec{\sigma}$ ein dreidimensionaler Vektor mit den Pauli-Operatoren als Komponenten gemeint ist.

Wie bereits erwähnt, lässt sich reinen Zuständen ein normierter Blochvektor zuordnen; fasst man einen gemischten Zustand nun wieder als konvexe Summe von reinen Zuständen auf, ergibt sich damit:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| = \frac{1}{2}(\mathbb{1} + \vec{a}\vec{\sigma}) = \frac{1}{2}(\mathbb{1} + \sum_i p_i \vec{a}_i \vec{\sigma}) = \frac{1}{2}(\mathbb{1} + \vec{r}\vec{\sigma})$$

Hier wurde der Vektor $\vec{r} = \sum_i p_i \vec{a}_i$ verwendet, wodurch zum einen gezeigt werden kann, dass auch gemischten Zuständen ein dreidimensionaler Blochvektor zugeordnet werden kann, zum anderen folgt aus $\sum_i p_i = 1$ und $|\vec{a}| = 1$ unter Anwendung der Dreiecksungleichung, dass $|\vec{r}| \leq 1$ gelten muss. Durch die Betrachtung der Länge eines Blochvektors ergibt sich damit eine zusätzliche Möglichkeit, bei einem gegebenen Zustand festzustellen, ob dieser rein oder gemischt ist. Jedem Zweizustandssystem kann somit ein Blochvektor zugeordnet werden, dies lässt sich besonders anschaulich mithilfe der *Blochkugel* darstellen, wie dies z.B. in Abb. 2 der Fall ist. Die hier dargestellten Zustände sind

$$\rho_1 = \frac{1}{2} \begin{bmatrix} 1 & -i \\ i & 1 \end{bmatrix}, \quad \rho_2 = \frac{1}{2} \begin{bmatrix} 1 & \frac{1}{2}(1 - \frac{i}{2}) \\ \frac{1}{2}(1 + \frac{i}{2}) & 1 \end{bmatrix}, \quad \rho_3 = \frac{1}{2} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

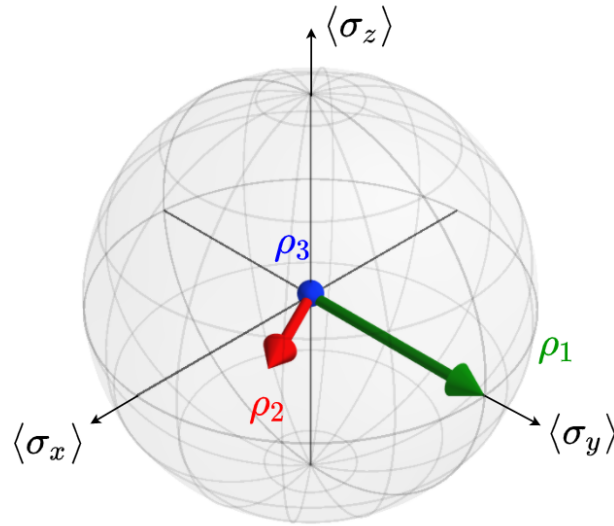


Abbildung 2: Beispiele für Blochvektoren für drei vorgegebene Dichteoperatoren

Der letzte Zustand ist dabei nicht als Vektor ersichtlich, sondern als blauer Punkt eingezeichnet, da dieser sich im Ursprung der Blochkugel befindet. Hierbei handelt es sich um den *maximal gemischten Zustand* $\rho_{mix} = \frac{1}{2}\mathbf{1}$. Die Tatsache, dass es keinen Zustand gibt, der „noch gemischter“ sein könnte, lässt sich daran ableiten, dass sämtliche Erwartungswerte der Pauli-Operatoren, welche ja die Komponenten des Blochvektors bilden, verschwinden. Jede erdenkliche Messung in Form von Pauli-Matrizen würden also keinen besonderen Aufschluss über das System geben. Konkret kann man den *Gemischtheitsgrad* (*degree of mixture*) folgendermaßen definieren [6, S.73]:

$$\Xi(\rho) := 1 - \text{Tr}(\rho^2) \quad (2.3)$$

Für einen reinen Zustand ergibt die Größe $Tr(\rho^2)$ den Wert 1 (und stellt damit eine weitere Überprüfungsmöglichkeit für die Zuordnung zu reinen/gemischten Zuständen dar), für einen maximal gemischten Zustand erreicht sie ein Minimum mit $Tr(\rho_{mix}^2) = \frac{1}{2}$, wodurch der Gemischtheitsgrad den maximalen Wert von $\Xi(\rho_{mix}) = \frac{1}{2}$ erreicht.

Nochmals Postulate

Dass es für physikalische Systeme eine allgemeinere Beschreibung als jene mit Zustandsvektoren gibt, kann als Erweiterung für das zuvor geschilderte Postulat I gesehen werden. Im Folgenden sollen der Vollständigkeit halber nochmals die Postulate II und III der Quantenmechanik dargestellt werden, in diesem Fall allgemeiner für Dichteoperatoren verfasst. Durch Einsetzen eines reinen Zustands und für den Dichteoperator und unter Ausnutzung der Invarianz der Spur bei zyklischem Vertauschen ($Tr(ABC) = Tr(BCA) = Tr(CAB)$) kann man sich leicht von der Äquivalenz überzeugen:

Postulat II - Projektive Messung:

Die Wahrscheinlichkeit den Messwert λ_i zu erhalten, ist durch die Wahrscheinlichkeit

$$p(\lambda_i) = Tr(P_i \rho)$$

gegeben und das System befindet sich nach der Messung im Zustand

$$\frac{P_i \rho P_i^\dagger}{\sqrt{Tr(P_i \rho)}}.$$

Zu ergänzen ist hier, dass sich der Erwartungswert bei Messung einer Observablen A nun durch $\langle A \rangle_\rho = Tr(A\rho)$ bestimmen lässt, demzufolge sind auch die Komponenten des Blochvektors durch $a_i = Tr(\sigma_i \rho)$ gegeben.

Bezüglich der Blochkugel lassen sich hier noch zwei nützliche Interpretationen anmerken, welche in Abb. 3 dargestellt sind:

Zum einen kann man sich Messungen in einer beliebigen Basis als eine Achse durch die Blochkugel vorstellen, die räumliche Orientierung hängt dabei von der gewählten Messung und damit der Messbasis ab, für eine Spin-Messung entspricht sie der Richtung des inhomogenen Magnetfelds eines Stern-Gerlach-Apparates. Führt man eine Messung durch, werden in der Folge nur Zustände in Richtung der Achse erzeugt.

Zum anderen kann der Erwartungswert einer beliebigen Messung damit visualisiert werden: Wird die Messung an einem Zustand ρ angewandt, lässt sich diese durch die Projektion des Blochvektors auf die Achse der Messung visualisieren.

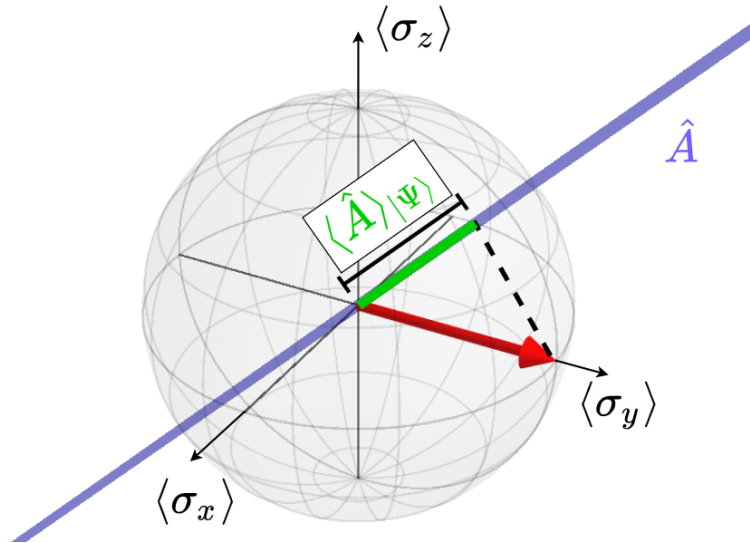


Abbildung 3: Visualisierung einer Messung und deren Erwartungswert in der Blochkugel

Postulat III - Zeitentwicklung:

Ist der Zustand zu einem bestimmten Zeitpunkt t_1 im Zustand $|\psi\rangle$, dann hängt der Zustand zu einem späteren Zeitpunkt $t_2 > t_1$ durch einen unitären Operator mit diesem zusammen:

$$\rho(t_2) = U\rho(t_1)U^\dagger$$

Die Schrödingergleichung lässt sich wie folgt für Dichteoperatoren verallgemeinern:

Für bra-Vektoren lässt sich die Schrödingergleichung durch $-i\hbar \frac{d}{dt} \langle \psi| = \langle \psi| \hat{H}$ formulieren. Gemäß Produktregel und mit $\rho = |\psi\rangle \langle \psi|$ gilt dann:

$$\frac{d}{dt} \rho = \frac{d}{dt} |\psi\rangle \langle \psi| = \left(\frac{d}{dt} |\psi\rangle \right) \langle \psi| + |\psi\rangle \left(\frac{d}{dt} \langle \psi| \right) = -\frac{i}{\hbar} \hat{H} \rho + \frac{i}{\hbar} \rho \hat{H}$$

Durch Umformung ergibt sich eine äquivalente Formulierung der Schrödingergleichung, diese wird **von-Neumann-Gleichung** genannt (siehe [6, S.68]), wobei die eckigen Klammern hier den *Kommutator* andeuten, für den $[A, B] = AB - BA$ gilt:

$$i\hbar \frac{d}{dt} \rho = [\hat{H}, \rho]$$

2.4 Mehrteilchensysteme

Von einem Qubit zu mehreren Qubits: Erweiterung durch Tensorprodukt

Da Qubits im Allgemeinen durch zwei komplexe Zahlen beschrieben werden können, kann der Hilbertraum, wie bereits beschrieben, mit $\mathcal{H} = \mathbb{C}^2$ identifiziert werden. In praktischen Anwendungsfällen, und insbesondere in Hinsicht auf die spätere Behandlung des Quantencomputers, ist es von Interesse, nicht nur ein Qubit, sondern eine Vielzahl von Qubits zu betrachten. Für die Beschreibung wird hier üblicherweise das *Tensorprodukts* $\otimes$ angewendet, die Verwendung dessen stellt dabei ein weiteres Postulat der Quantenmechanik dar. Damit kann beispielsweise der Hilbertraum für zwei Qubits (Systeme A und B) mit $\mathcal{H}^{AB} = \mathcal{H}^A \otimes \mathcal{H}^B = \mathbb{C}^2 \otimes \mathbb{C}^2$ mit der Dimension $\dim(\mathcal{H}) = 4$ angegeben werden.

Für N Qubits ergibt sich damit $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2 = (\mathbb{C}^2)^{\otimes N}$.

Durch das Tensorprodukt lassen sich natürlich nicht nur zugehörige Hilberträume, sondern auch konkrete Zustände beschreiben. Soll beispielsweise ein System von zwei Zuständen $|\phi\rangle, |\psi\rangle \in \mathcal{H}_2$ beschrieben werden, wird dies häufig wie folgt notiert:

$$|\phi\rangle \otimes |\psi\rangle = |\phi\rangle |\psi\rangle = |\phi, \psi\rangle = |\phi\psi\rangle$$

Eine solche Verkürzung wurde im Wesentlichen schon bei der Darstellung einer Matrix benutzt, beispielsweise bei der Spektralzerlegung und den Ausdrücken $|i\rangle \langle i|$, welche eigentlich ebenso ein Tensorprodukt in Form von $|i\rangle \otimes \langle i|$ darstellen. Handelt es sich um Basiszustände der Rechenbasis, z.B. $|0\rangle$ und $|1\rangle$, lässt sich dies mit $|0, 1\rangle$, oder durch Weglassen des Beistrichs, mit $|01\rangle$ ausdrücken. Für eine Aneinanderreihung von mehreren Qubits ergibt sich dadurch ein *Register* an Qubits, welches stark an klassische Bitfolgen erinnert, beispielsweise $|0101011101\rangle$.

Der konkrete Umgang mit dem Tensorprodukt sei an folgenden Beispielen mit Vektoren und Matrizen verdeutlicht:

$$\text{sei } |\psi\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |\phi\rangle = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \Rightarrow |\phi\rangle |\psi\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 1 \cdot \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \\ 0 \cdot \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \\ 0 \\ 0 \end{pmatrix}$$

$$\text{sei } \rho^A = \frac{1}{2} \begin{bmatrix} 1 & -i \\ i & 1 \end{bmatrix}, \rho^B = \frac{1}{2} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \Rightarrow \rho^A \otimes \rho^B = \frac{1}{2} \begin{bmatrix} 1 \cdot \rho^B & -i \cdot \rho^B \\ i \cdot \rho^B & 1 \cdot \rho^B \end{bmatrix} = \frac{1}{4} \begin{bmatrix} 1 & 0 & -i & 0 \\ 0 & 1 & 0 & -i \\ i & 0 & 1 & 0 \\ 0 & i & 0 & 1 \end{bmatrix} \quad (2.4)$$

$$\text{sei } |\chi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \Rightarrow |\chi\rangle \langle\chi| = \frac{1}{2} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \otimes (1, 0, 0, 1) = \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \quad (2.5)$$

Im Folgenden sollen allgemeine Rechenregeln zum Distributivgesetz und der Multiplikation mit einem Skalar festgehalten werden, für $|\psi\rangle, |\phi_1\rangle, |\phi_2\rangle \in \mathcal{H}$, $c \in \mathbb{C}$ (wobei selbiges für bra-Vektoren formuliert werden kann) gilt:

$$\begin{aligned} |\psi\rangle \otimes (|\phi_1\rangle + |\phi_2\rangle) &= |\psi\rangle \otimes |\phi_1\rangle + |\psi\rangle \otimes |\phi_2\rangle \\ (|\phi_1\rangle + |\phi_2\rangle) \otimes |\psi\rangle &= |\phi_1\rangle \otimes |\psi\rangle + |\phi_2\rangle \otimes |\psi\rangle \\ c(|\psi\rangle \otimes |\phi\rangle) &= (c|\psi\rangle) \otimes |\phi\rangle = |\psi\rangle \otimes (c|\phi\rangle) \end{aligned}$$

Besonders hervorzuheben ist das innere Produkt, welches für $|\psi\rangle, |\phi\rangle \in \mathcal{H}$, $\langle\chi|, \langle\omega| \in \mathcal{H}^*$ folgendermaßen gebildet wird:

$$(\langle\psi| \otimes \langle\phi|)(|\chi\rangle \otimes |\omega\rangle) = \langle\psi|\chi\rangle \otimes \langle\phi|\omega\rangle = \langle\psi|\chi\rangle \langle\phi|\omega\rangle$$

Im letzten Schritt wurde das Tensorprodukt wiederum weggelassen, da es sich hier lediglich um die Multiplikation zweier komplexer Zahlen handelt. Für Operatoren lassen sich die oben erwähnten Regeln gleichermaßen anwenden, beispielsweise für die Beschreibung von zwei Systemen durch Dichteoperatoren ($\rho^{AB} = \rho^A \otimes \rho^B$), oder für eine Hintereinanderausführung von Operatoren (z.B. im Zuge zweier Messungen) an zwei Systemen (z.B. $(X \otimes Y)(X' \otimes Y') = XX' \otimes YY'$).

Besonders relevant ist an dieser Stelle die Ausführung von Operatoren an zusammengesetzten Zuständen: Wendet man einen Operator X am ersten System $|\phi\rangle \in \mathcal{H}^A$ und einen Operator Y am zweiten System $|\psi\rangle \in \mathcal{H}^B$ an, lässt sich dies durch

$$(X^A \otimes Y^B)(|\phi\rangle^A \otimes |\psi\rangle^B) = X^A |\phi\rangle^A \otimes Y^B |\psi\rangle^B$$

ausdrücken. Hierbei wurden zur Übersicht Indizes eingeführt, um die Zugehörigkeiten zu den Systemen A und B zu verdeutlichen. Möchte man dabei nur einen Operator ausführen und das zweite System belassen, kann man dies durch $(X^A \otimes \mathbf{1}^B)$ ausdrücken, hierdurch bleibt also der zweite Zustand unverändert.

Von mehreren Qubits zu einem Qubit: Reduzierung durch Teilspur

Die Spur eines Operators wurde schon im vorigen Kapitel benutzt, für Matrizen wird diese durch die Summe der Diagonalelemente gebildet. Die quantenmechanische Formulierung unter Verwendung der Dirac-Notation (und Verzicht einer konkreten Matrixdarstellung) lässt sich wie folgt formulieren:

$$\text{Tr}(\rho) = \sum_{i=1}^d \langle n_i | \rho | n_i \rangle \quad \text{mit } d = \dim(\mathcal{H})$$

Die Vektoren $|n_i\rangle$ müssen hierbei eine Basis des entsprechenden Hilbertraums darstellen, diese ist allerdings frei wählbar. So könnte man für Qubits z.B.

$$|n_1\rangle = |0\rangle, |n_2\rangle = |1\rangle \quad \text{oder } |n_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |n_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

wählen, die konkrete Auswahl hängt dabei vom betrachteten Problem ab. Handelt es sich beispielsweise um einen reinen Zustand $\rho = |\psi\rangle\langle\psi|$, würde eine günstige Wahl mit $|n_1\rangle = |\psi\rangle$ und dem dazu orthogonalen Vektor $|n_2\rangle = |\psi^\perp\rangle$ erfolgen, da auch diese eine Basis bilden:

$$\text{Tr}(\rho) = \langle\psi|\psi\rangle\langle\psi|\psi\rangle + \langle\psi^\perp|\psi\rangle\langle\psi|\psi^\perp\rangle = 1 + 0 = 1$$

Möchte man nun ein Teilsystem eines physikalischen Systems beschreiben, beispielsweise ein einzelnes Qubit eines zusammengesetzten Systems ρ_{ges} , müssen die übrigen Systeme „ausgespart“ werden, hierfür wird eine *Teilspur* (*partial trace*) über das System gebildet. Anschaulich kann man sich die Wirkung einer Teilspur anhand einer 4x4-Matrix verdeutlichen, wofür eine Matrix aus einem vorhergehenden Beispiel verwendet werden soll. Die Teilspur fällt dabei auf zwei verschiedene Arten aus, je nachdem, welches System ausgespart werden soll (angedeutet durch einen Index bei der Spur), die daraus entstehenden Zustände werden *reduzierte Zustände* genannt. Konkret gestaltet sich das Anwenden der Teilspur an einer 4x4-Matrix wie folgt:

$$\begin{aligned} \text{sei } \rho^{AB} &= \frac{1}{4} \begin{bmatrix} 1 & 0 & -i & 0 \\ 0 & 1 & 0 & -i \\ i & 0 & 1 & 0 \\ 0 & i & 0 & 1 \end{bmatrix} \\ \text{Tr}_B(\rho^{AB}) &= \frac{1}{4} \text{Tr}_B \left(\begin{bmatrix} \boxed{1} & \boxed{0} & \boxed{-i} & \boxed{0} \\ \boxed{0} & \boxed{1} & \boxed{0} & \boxed{-i} \\ \boxed{i} & \boxed{0} & \boxed{1} & \boxed{0} \\ \boxed{0} & \boxed{i} & \boxed{0} & \boxed{1} \end{bmatrix} \right) = \frac{1}{4} \begin{bmatrix} \boxed{1+1} & \boxed{-i-i} \\ \boxed{i+i} & \boxed{1+1} \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & -i \\ i & 1 \end{bmatrix} \\ \text{Tr}_A(\rho^{AB}) &= \frac{1}{4} \text{Tr}_A \left(\begin{bmatrix} \boxed{1} & \boxed{0} & -i & 0 \\ \boxed{0} & \boxed{1} & 0 & -i \\ i & 0 & \boxed{1} & \boxed{0} \\ 0 & i & \boxed{0} & \boxed{1} \end{bmatrix} \right) = \frac{1}{4} \begin{bmatrix} \boxed{1+1} & \boxed{0+0} \\ \boxed{0+0} & \boxed{1+1} \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{aligned}$$

Hierbei fällt auf, dass die reduzierten Zustände den ursprünglichen Zuständen ρ^A, ρ^B aus dem obigen Beispiel in Gl. 2.4 entsprechen, durch das Aussparen konnten also die Einzelsysteme „wiederhergestellt“ werden. Eine Begründung hierfür wird im Folgenden angeführt:

Wiederum unter Verwendung der Dirac-Notation lassen sich die reduzierten Zustände $\rho^{A'}$, $\rho^{B'}$ für ein zusammengesetztes System $\rho^{AB} = \rho^A \otimes \rho^B$ mithilfe der Teilspur wie folgt definieren und anwenden:

$$\begin{aligned}
\rho^{A'} &= Tr_B(\rho^{AB}) := \left(\sum_i (\mathbb{1}^A \otimes \langle n_i|^B) \rho^{AB} (\mathbb{1}^A \otimes |n_i\rangle^B) \right) = \\
&= \sum_i \rho^A \otimes \langle n_i|\rho^B|n_i\rangle = \rho^A \otimes \left(\sum_i \langle n_i|\rho^B|n_i\rangle \right) = \rho^A \otimes 1 = \rho^A \\
\rho^{B'} &= Tr_A(\rho^{AB}) := \left(\sum_i (\langle n_i|^A \otimes \mathbb{1}^B) \rho^{AB} (|n_i\rangle^A \otimes \mathbb{1}^B) \right) = \\
&= \sum_i \langle n_i|\rho^A|n_i\rangle \otimes \rho^B = \left(\sum_i \langle n_i|\rho^A|n_i\rangle \right) \otimes \rho^B = 1 \otimes \rho^B = \rho^B
\end{aligned}$$

Für einen *Produktzustand*, also einen Zustand, der sich durch ein Tensorprodukt von Zuständen darstellen lässt, kann man im Allgemeinen den Zustand des einzelnen Systems durch die Teilspur wiedergewinnen!

Ein Beispiel für einen Zustand, der sich nicht als Produktzustand beschreiben lässt, sieht wie folgt aus:

$$\begin{aligned}
|\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \\
|\Phi^+\rangle\langle\Phi^+| &= \frac{1}{2}(|0\rangle|0\rangle + |1\rangle|1\rangle)(\langle 0|\langle 0| + \langle 1|\langle 1|) = \\
&= \frac{1}{2}(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 1| \otimes |0\rangle\langle 1| + |1\rangle\langle 0| \otimes |1\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|) \\
\Rightarrow \rho^{A'} &= Tr_B(|\Phi^+\rangle\langle\Phi^+|) = \frac{1}{2}(|0\rangle\langle 0| \otimes 1 + |0\rangle\langle 1| \otimes 0 + |1\rangle\langle 0| \otimes 0 + |1\rangle\langle 1| \otimes 1) = \\
&= \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2}\mathbb{1}_2 = \rho_{mix} = Tr_A(|\Phi^+\rangle\langle\Phi^+|) = \rho^{B'}
\end{aligned}$$

Das hier vorliegende Beispiel wurde in Form der Dirac-Notation bearbeitet, hätte aber auch durch Anwenden der Teilspur in der Matrix $|\chi\rangle\langle\chi|$ im obigen Beispiel aus Gl.2.5 dargestellt werden können, da der Zustand $|\Phi^+\rangle$ dem oben verwendeten Spaltenvektor zugeordnet werden kann.

Bemerkenswert ist, dass das Gesamtsystem durch einen reinen Zustand beschrieben werden kann, während die reduzierten Zustände maximal gemischt sind. Dieses Ergebnis soll in Kapitel 2.5 wieder aufgegriffen werden.

2.5 Entropie

Zur Quantifizierung von Information bzw. der Ungewissheit und Unkenntnis über ein System wird in der Regel die *Entropie* herangezogen, die die verschiedenen Möglichkeiten, in denen das System vorgefunden werden kann, mithilfe deren Auftretswahrscheinlichkeiten bemisst. Das

verallgemeinerte Prinzip dahinter bilden die sogenannten *Renyi-Entropien* (vgl. [7, S.148]), die sich mit einer Wahrscheinlichkeitsdistribution $(p_1, p_2, \dots, p_n)$ (mit der Wahrscheinlichkeit p_i für das Antreffen der i -ten Möglichkeit) und einer Ordnung $\alpha \neq 1$ folgendermaßen bilden lassen:

$$H_\alpha = \frac{1}{1-\alpha} \log \sum_{i=1}^n p_i^\alpha$$

Für den Grenzfall $\alpha \rightarrow 1$ ergibt sich nach der *Regel von de L'Hospital*:

$$\lim_{\alpha \rightarrow 1} \left(\frac{1}{1-\alpha} \log \sum_{i=1}^n p_i^\alpha \right) = - \sum_{i=1}^n p_i \log p_i$$

Diese Form der Entropie und damit der Bemessung von Informationsgehalt findet sich in vielen konkreten Anwendungsgebieten wieder, von denen einige im Folgenden aufgeführt werden.

Entropie in klassischer Informationstheorie

In der klassischen Informationstheorie wird oftmals die Shannon-Entropie verwendet, diese hat prinzipiell keine physikalische Bedeutung und lautet:

$$H = - \sum_i p_i \log_2 p_i$$

Der Logarithmus zur Basis 2 wird hier bereits in Anlehnung an Bits verwendet. Die Shannon-Entropie kann z.B. beim Versenden von Nachrichten mit einem Alphabet mit einzelnen Buchstaben (und entsprechender Basis des Logarithmus) und relativen Häufigkeiten derer betrachtet werden. Sie gilt dann als durchschnittlicher Informationsgehalt eines Buchstaben, den der Empfänger der Nachricht entnehmen kann, denn je „unsicherer“ der Inhalt eines Zeichens ist, desto mehr Information bringt das Empfangen und Lesen dieses im Anschluss.

Die Shannon-Entropie stimmt damit zudem der Form nach mit der Renyi-Entropie der Ordnung $\alpha = 1$ überein, durch eine davon abweichende Ordnung kann das Auftreten von Zeichen mit hoher Wahrscheinlichkeit je nach Wahl stärker oder schwächer gewichtet werden.

Entropie in statistischer Physik

In der Thermodynamik spielt die *Entropie* eine maßgebliche Rolle, so besagt das zweite Postulat der Thermodynamik, dass in einem abgeschlossenen System die Entropie nur zunehmen kann. Wichtige Begriffe sind hier Makrozustände, die das System mithilfe makroskopischer Größen wie der Gesamtenergie beschreiben, und Mikrozustände, die die möglichen Realisierungen des Makrozustands darstellen. Die Entropie eines Makrozustands ergibt sich durch

$$S = -k_B \sum_i p_i \ln p_i$$

wobei p_i die Wahrscheinlichkeiten für die einzelnen Mikrozustände bezeichnen und k_B für die Boltzmann-Konstante steht. Betrachtet man ein mikrokanonisches Ensemble (in dem die Gesamtenergie fixiert ist), sind im Gleichgewichtszustand alle Mikrozustände gleichwahrscheinlich, sei zudem Ω die Anzahl dieser Mikrozustände, dann ergibt sich laut Fundamentalpostulat der statistischen Physik mit $p_i = \frac{1}{\Omega}$:

$$S = -k_B \sum_i \frac{1}{\Omega} \ln \frac{1}{\Omega} = -k_B \frac{1}{\Omega} \sum_i \ln \frac{1}{\Omega} = k_B \frac{1}{\Omega} \sum_i \ln \Omega = k_B \frac{1}{\Omega} \Omega \ln \Omega = k_B \ln \Omega$$

Dieses Ergebnis entspricht der Boltzmannformel für die Entropie eines Systems im Gleichgewichtszustand.

Der oben beschriebene Zustand lässt sich zudem durch den Dichteoperator $\rho = \frac{1}{\Omega} \sum_i |\psi_i\rangle \langle \psi_i|$ beschreiben, wobei $|\psi_i\rangle$ einen möglichen Mikrozustand beschreibt. Dieser Zustand lässt sich als Diagonalmatrix mit den Diagonaleinträgen $\frac{1}{\Omega}$ interpretieren, es handelt sich also um einen maximal gemischten Zustand (alle Eigenwerte sind $p_i = \frac{1}{\Omega}$).

Die Entropie lässt sich dabei als Mangel an Information über den Mikrozustand des Systems beschreiben: Je mehr Mikrozustände theoretisch möglich sind, desto größer ist die Unkenntnis darüber.

Entropie in Quanteninformationstheorie

Für die Entropie eines Quantenzustands wird die *von-Neumann-Entropie* [6, S.99-100] verwendet:

$$S(\rho) = -\text{Tr}(\rho \ln \rho) = -\sum_i p_i \ln p_i$$

In letzterer Formulierung bezeichnen p_i die Eigenwerte des Dichteoperators. Wendet man diese Formel auf das zuvor erwähnte mikrokanonische Ensemble mit Eigenwerten $p_i = \frac{1}{\Omega}$ an, ergibt sich dadurch erneut (bis auf die Konstante k_B) die zuvor erwähnte Entropie.

Im Folgenden sollen einige nützliche Eigenschaften der von-Neumann-Entropie aufgelistet werden:

- *untere Schranke:* $S(\rho) \geq 0$ und $S(\rho) = 0 \Leftrightarrow \rho = |\psi\rangle \langle \psi|$

Die Entropie verschwindet nur bei reinen Zuständen, leicht nachzuvollziehen durch Einsetzen der Eigenwerte 0 und 1. Dies lässt sich auch wie folgt interpretieren: Liegt ein reiner Zustand vor, lässt sich dieser mit einem Zustandsvektor vollständig charakterisieren, es liegt kein Mangel an Information vor.

- *obere Schranke:* $S(\rho) \leq \ln(d)$ mit $d = \dim(\mathcal{H})$, S ist maximal für $\rho = \rho_{\text{mix}} = \frac{1}{d} \mathbb{1}_d$

Der Maximalwert der Entropie ist $\ln(d)$, wobei dieser nur beim maximal gemischten Zustand erreicht wird. Stellt man sich hierunter beispielsweise wieder eine Quelle vor, welche mit jeweils einer Wahrscheinlichkeit von 50% zwischen zwei reinen Zuständen wählt und aussendet, lässt sich dies als Mangel an Information und Unkenntnis über das vorliegende System interpretieren.

- *Invarianz bei unitären Transformationen:* $S(U\rho U^\dagger) = S(\rho)$

Die Entropie eines Systems ändert sich durch unitäre Transformationen, also z.B. bei der Zeitentwicklung eines abgeschlossenen Systems, nicht. Dies kann dadurch begründet werden, dass unitäre Transformationen die Eigenwerte einer Matrix nicht verändern, womit auch die Entropie erhalten bleibt.

- *konkav:* $S(\sum_i p_i \rho_i) \geq \sum_i p_i S(\rho_i)$

In Worten: Die Entropie eines Zustandsgemisches ist höher als die entsprechende anteilige Summe der Einzelentropien. Beim Mischen von Zuständen Addieren sich also Entropien nicht nur, die Entropie und damit der Mangel an Information über das System wird dadurch noch größer.

- *Subadditivität:* $S(\rho_{AB}) \leq S(\rho^A) + S(\rho^B)$ und $S(\rho^{AB}) = S(\rho^A) + S(\rho^B) \Leftrightarrow \rho^{AB} = \rho^A \otimes \rho^B$

In Worten: Die Entropie des Gesamtsystems ist also kleinergleich der Summe der Entropien der reduzierten Zustände, Gleichheit gilt nur bei einem Produktzustand. Falls kein Produktzustand vorliegt, ist also der Mangel an Information und die Unkenntnis bei Betrachtung der einzelnen Systeme höher als bei Betrachtung des Gesamtsystems. Salopp gesagt enthält das Gesamtsystem mehr Information als die Summe der Teilsysteme.

Ein Beispiel für die letzte Aussage wurde schon im vorherigen Kapitel betrachtet: Der Zustand $|\Phi^+\rangle$ ist ein reiner Zustand (denn sonst könnte er nicht als Zustandsvektor dargestellt werden), die Entropie beträgt somit $S(|\Phi^+\rangle) = 0$.

Beide reduzierten Zustände sind jedoch maximal gemischt, damit ergibt sich

$S(\rho^{A'}) = S(\rho^{B'}) = -\ln \frac{1}{2} = \ln 2$. Gemäß obiger Interpretation ist damit der Mangel an Information in den beiden Teilsystemen maximal, während bei Betrachtung des Gesamtsystems sämtliche Information zugänglich ist. Diese Aussagen werden im Kapitel 2.6 weiter behandelt und verallgemeinert.

2.6 Verschränkung

Bell-Zustände

Das Phänomen der Verschränkung soll zunächst an einem konkreten Beispiel diskutiert werden, hierfür wird der Zustand $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ betrachtet, der von zwei Experimentator:innen gemessen wird, die im Folgenden *Alice* und *Bob* genannt werden.

Als erstes soll angenommen werden, Alice und Bob teilen sich das System und messen in der Basis $\{|0\rangle, |1\rangle\}$ (z.B. die Messung der Polarisation von zwei Photonen in der Basis $\{|H\rangle, |V\rangle\}$), die Messergebnisse sollen mit $x \in \{0, 1\}$ (bei Alice) und $y \in \{0, 1\}$ (bei Bob) kodiert werden. Nun sollen die Wahrscheinlichkeiten dafür ausgedrückt werden, dass Alice ein bestimmtes Messergebnis feststellt, wenn Bob bereits ein bestimmtes Messergebnis hat; damit sind die bedingten Wahrscheinlichkeiten

$$p(x|y) = \frac{p(x \wedge y)}{p(y)}$$

gefragt. Der reduzierte Zustand $\rho^{B'}$, der für die Wahrscheinlichkeitsaussage von Bobs Einzelsystem gebraucht wird, ist der maximal gemischte Zustand $\rho_{mix} = \frac{1}{2}\mathbb{1}_2$, dadurch ergibt sich:

$$p(y=0) = \text{Tr}(|0\rangle\langle 0| \rho^{B'}) \text{Tr}(|0\rangle\langle 0| \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)) = \text{Tr}[\frac{1}{2}|0\rangle\langle 0|] = \frac{1}{2} = p(y=1)$$

Das Messergebnis bei Bob ist also prinzipiell zufällig und lässt sich nicht vorhersagen. Nun soll ein Blick auf die Wahrscheinlichkeit gerichtet werden, dass Alice und Bob gleiche Messergebnisse erhalten:

$$p(x=0, y=0) = \text{Tr}(|0\rangle\langle 0| \otimes |0\rangle\langle 0| |\Phi^+\rangle\langle \Phi^+|) = |\langle 00|\Phi^+\rangle|^2 = \frac{1}{2} = p(x=1, y=1)$$

Somit verschwinden die Wahrscheinlichkeiten für unterschiedliche Messergebnisse: $p(x=1, y=0) = p(x=0, y=1) = 0$. Damit ergeben sich für die bedingten Wahrscheinlichkeiten:

$$p(x=0|y=0) = p(x=1|y=1) = 1$$

Wenn Bob also bereits gemessen hat (und dabei ein völlig zufälliges Ereignis stattgefunden hat), bekommt Alice mit Sicherheit ein bestimmtes Messergebnis (in diesem Fall das selbe wie Bob), damit sind die Messergebnisse perfekt korreliert. Hier lässt sich bereits anmerken, dass sich dadurch *keine* überlichtschnelle Kommunikation betreiben lässt: Zwar können Alice und Bob gleichzeitig selbe Messergebnisse erhalten, aber niemand kann kontrollieren, *welches* Messergebnis denn stattfinden soll: Für Bob, der in diesem Beispiel als erstes messen konnte, gab es keine Möglichkeit, ein bestimmtes Messergebnis zu erzwingen und damit zu kontrollieren, welchen Zustand Alice im Nachhinein erhalten sollte. Für Bob gab es keine Möglichkeit, auf diese Weise Information an Alice zu übermitteln.

Teilen sich Alice und Bob den selben Zustand nochmals, beschließen nun aber, in der Basis $\{|+\rangle, |-\rangle\}$ (mit $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$) zu messen (z.B. durch drehen der Polarisationsfilter um 45°), ergibt sich folgendes Szenario: Man könnte nun die Berechnungen von zuvor wiederholen, indem man lediglich die Projektionsoperatoren durch $|+\rangle\langle +|$ und $|-\rangle\langle -|$ bzw. $|++\rangle\langle ++|$ und $|--\rangle\langle --|$ austauscht und sämtliche Berechnungen einheitlich entweder in der Basis $\{|+\rangle, |-\rangle\}$ oder $\{|0\rangle, |1\rangle\}$ ausdrückt. Vereinfachen lässt sich dies, indem man lediglich den Zustand $|\Phi^+\rangle$ anders ausdrückt:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{2\sqrt{2}}((|+\rangle + |-\rangle)(|+\rangle + |-\rangle) + (|+\rangle - |-\rangle)(|+\rangle - |-\rangle)) = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)$$

Die Struktur des Zustands bleibt also in dieser Basis völlig gleich, womit sich durch Austausch der Basis auch in den weiteren Berechnungen an den Ergebnissen nichts verändert: Es lässt sich

erneut eine perfekte Korrelation beobachten.

In der Tat lässt sich zeigen, dass es für den Zustand $|\Phi^+\rangle$ unendlich viele Kombinationen von Messbasen gibt, für die sich eine solche Korrelation einstellt. Hierin liegt die Stärke von *verschränkten Zuständen* (eine genauere Definition soll später noch folgen), denn beispielsweise könnte man auch für den Zustand $\rho = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$ solche perfekten Korrelationen feststellen, allerdings tauchen diese hier nur bei der Basiswahl $\{|0\rangle, |1\rangle\}$ auf. Zudem kann hier erwähnt werden, dass der hier betrachteten Verschränkung und den entsprechenden Korrelationen, wie sie experimentell unter anderem von Aspect im Jahr 1981 [8] beobachtet wurden, eigentlich nichts „Spukhaftes“ oder in mathematischem Sinne Neues innewohnt, sondern diese lediglich auf natürliche Weise aus dem zuvor festgelegten mathematischen Formalismus für die Quantenmechanik folgt.

Der bisher so oft behandelte Zustand ist einer der vier *Bell-Zustände*

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \quad |\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (2.6)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \quad (2.7)$$

Diese Zustände zeichnen sich durch einige besondere Eigenschaften aus, alle bisher festgestellten Eigenschaften für $|\Phi^+\rangle$ gelten auch für die anderen Bell-Zustände: Die Zustände sind rein, während ihre reduzierten Zustände maximal gemischt sind, und es gibt unendlich viele Kombinationen von Messbasen, für die sich perfekte Korrelationen in Messergebnissen zeigen. Zudem gilt zu erwähnen, dass diese vier Zustände eine Basis des Hilbert-Raumes $\mathcal{H}_2 \otimes \mathcal{H}_2$ bilden, somit lässt sich jeder reine 2-Qubit-Zustand durch Linearkombination dieser Zustände ausdrücken.

EPR-Paradoxon und CHSH-Ungleichung

Die Argumentation von Einstein, Podolski und Rosen gegen die Quantenmechanik als vollständige Theorie schlug hohe Wellen in der wissenschaftlichen Gemeinschaft, nach deren Überzeugung musste eine physikalische Theorie die folgenden Kriterien erfüllen (vgl.[4, S.777]):

- *Realität*: „If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.“
- *Komplettheit*: „Every element of the physical reality must have a counterpart in the physical theory “

Zusammen mit der Annahme der *Lokalität*, welche die Verhinderung von instantanen Effekten von Systemen, die räumlich getrennt sind, durch die spezielle Relativitätstheorie betrifft, ergeben sich dadurch die Standbeine der Argumentationen.

Erst durch John Stewart Bell und dessen Ausführungen (siehe [5]) konnte eine Möglichkeit aufgezeigt werden, diese Annahmen konkret zu überprüfen. Nach der Annahme einer Theorie

mit lokal-realistischen *versteckten Variablen* (also Variablen, die vielleicht nicht unmittelbar zugänglich sind, aber das Verhalten von Systemen bestimmen und lokal vorhanden sind), welche dann verträglich mit der EPR-Argumentation wäre, wurde eine Möglichkeit angegeben, diese einer experimentellen Überprüfung zu unterziehen. Diese wurde in Form einer Ungleichung angegeben, die Erwartungswerte bei konkreten Messungen miteinander in Beziehung setzt und in einer lokal-realistischen Theorie erfüllt werden müsste.

Die hierfür oft verwendete Form ist die *CHSH-Ungleichung* (Clauser, Horne, Shimony, Holt, siehe [9]). Auf eine genauere Ausführung der Herleitung soll hier verzichtet werden (für nähere Informationen siehe [10, S.111-117]), die Ungleichung sei an dieser Stelle allerdings erwähnt:

$$S_{CHSH} = |E(\vec{a}, \vec{b}) - E(\vec{a}, \vec{b}')| + |E(\vec{a}', \vec{b}) + E(\vec{a}', \vec{b}')| \leq 2$$

Die hier auftretenden Erwartungswerte beziehen sich auf ein Experiment, bei dem Alice und Bob zufällig aus verschiedenen Messbasen wählen, wobei Alice bei jeder Messung eines Systems zwischen den Messrichtungen $\vec{a}$ und $\vec{a}'$ sowie Bob zwischen $\vec{b}$ und $\vec{b}'$ wählt.

Anschaulich lässt sich z.B. wieder die Messung der Polarisation von Photonen und jeweils zwei unterschiedlichen Messrichtungen verstehen. In einem konkret gewählten Szenario würde eine quantenmechanisch ausgearbeitete Lösung mithilfe eines Bell-Zustands diese Ungleichung allerdings verletzen und einen Wert von $S_{QM} = 2\sqrt{2} > 2$ für ein Experiment vorhersagen, welcher mit einer Theorie von versteckten Variablen nicht möglich wäre. An diesem Punkt kommt dabei die Verschränkung ins Spiel, die durch die entsprechenden Korrelationen von Messwerten auch klassisch nicht erklärbare Erwartungswerte produziert, die wiederum in die CHSH-Ungleichung eingehen.

Zudem gilt zu erwähnen, dass nur verschränkte Zustände diese Ungleichung verletzen können, somit kann ein Experiment dieser Art beispielsweise dazu dienen, Verschränkung an einem Zustand überhaupt zu detektieren. Tatsächlich ist der Wert von $2\sqrt{2}$ die größtmögliche Verletzung der CHSH-Ungleichung und wird nur von Bell-Zuständen erreicht, diese obere Schranke wird *Tsirelson-Schranke* (*Tsirelson's Bound*) genannt (siehe [11]).

Diese Grenze der Ungleichung wurde 1972 von Clauser und Freedman (siehe [12]) sowie 1982 von Aspect (siehe [8]) (allerdings in anderen Realisierungen als zuvor angedeutet) überschritten, womit gezeigt werden konnte, dass die physikalische Realität entweder gegen die Annahme der Realität oder jener der Lokalität verstoßen müsste.

Verschränkung für reine und gemischte Zustände

Da im bisherigen Kapitel bereits mehrmals über Verschränkung gesprochen wurde, ohne diese formal zu definieren, sollen nun einige Definitionen und Interpretationen dafür folgen:

Definition 2.1. Ein reiner Zustand $|\Psi\rangle^{AB}$, für den es eine Zerlegung in Form von $|\Psi\rangle^{AB} = |\psi\rangle^A |\phi\rangle^B$ gibt, wird *separabel* genannt.

Definition 2.2. Ein reiner Zustand, der nicht separabel ist, wird **verschränkt** genannt:

$$|\Psi\rangle^{AB} \neq |\psi\rangle^A |\phi\rangle^B$$

Diese Definitionen können nun folgendermaßen interpretiert werden:

Sei $|\Psi\rangle^{AB}$ ein separabler Zustand, also $|\Psi\rangle^{AB} = |\psi\rangle^A |\phi\rangle^B$, dann kann der entsprechende Dichteoperator durch $\rho^{AB} = (|\psi\rangle^A \otimes |\phi\rangle^B)(\langle\psi|^A \otimes \langle\phi|^B) = |\psi\rangle^A \langle\psi|^A |\phi\rangle^B \langle\phi|^B = \rho^A \otimes \rho^B$ gebildet werden. Bildet man hieraus die reduzierten Zustände mit der Teilspur, ergibt sich für diese lediglich $\rho^A = \rho^A = |\phi\rangle^A \langle\phi|^A$ und $\rho^B = \rho^B = |\psi\rangle^B \langle\psi|^B$, die reduzierten Zustände sind also reine Zustände. Die Information ist demnach vollständig in den einzelnen Systemen enthalten und die Unkenntnis über diese Zustände minimal, das Gesamtsystem kann vollständig durch Kenntnis über beide Einzelsysteme charakterisiert werden.

Zieht man hingegen das Beispiel des Bell-Zustands $|\Phi^+\rangle$ wieder zur Betrachtung heran, lässt sich keine solche Zerlegung finden, die reduzierten Zustände sind maximal gemischt und damit ist auch die Unkenntnis durch alleinige Betrachtung der Einzelsysteme maximal. Das System lässt sich nicht durch alleinige Kenntnis der Einzelsysteme beschreiben und muss korrekterweise ganzheitlich beschrieben werden.

Aus obiger Überlegung folgt: Wenn die reduzierten Zustände eines reinen Zustands gemischt sind, ist das System verschränkt. Auch die Umkehrung gilt (welche später bei der *Schmidt-Zerlegung* erläutert wird), sodass sich folgende Äquivalenz ergibt:

$$\text{Ein reiner Zustand } |\Psi\rangle^{AB} \text{ ist verschränkt} \Leftrightarrow \text{reduzierte Zustände } \rho^A, \rho^B \text{ sind gemischt} \quad (2.8)$$

Die Definition für Separabilität und Verschränkung kann fast analog auf gemischte Zustände übertragen werden:

Definition 2.3. Ein gemischter Zustand ρ^{AB} , für den es eine Zerlegung in Form von $\rho^{AB} = \sum_i p_i \rho_i^A \otimes \rho_i^B$ gibt, wobei ρ_i^A, ρ_i^B Dichteoperatoren und p_i Elemente einer Wahrscheinlichkeitsverteilung sind, wird **separabel** genannt.

Definition 2.4. Ein gemischter Zustand, der nicht separabel ist, wird **verschränkt** genannt: $\rho^{AB} \neq \sum_i p_i \rho_i^A \otimes \rho_i^B$

Eine solche Zerlegung bei gegebenem Zustand zu finden bzw. zu entscheiden, ob ein Zustand überhaupt separabel ist, ist allerdings nicht trivial und in höheren Dimensionen im Allgemeinen ein ungelöstes Problem, lediglich für den Fall von zwei Qubits lässt sich dies eindeutig herausfinden (darauf wird später bei *Separabilitätskriterien* eingegangen).

Ein weiteres offenes Problem findet sich beim Quantifizieren und Auffinden von geeigneten Maßen von Verschränkung. Die Bell-Zustände sind Zustände mit perfekten Korrelationen in unendlich vielen Paaren von Messbasen, allerdings kann es bei höherdimensionalen Systemen sein, dass Korrelationen nur in einer eingeschränkten Menge von Basen oder nur Teile der

Ergebnisse korrelieren. Im Allgemeinen ist es daher von Interesse, Verschränkung mithilfe von *Verschränkungsmaßen* zu quantifizieren, wobei gleich erwähnt werden soll, dass es hierfür kein ausgezeichnetes Maß gibt, das in allen denkbaren Fällen alle gewünschten Eigenschaften aufweist. Dies bedeutet, dass es mehrere Verschränkungsmaße gibt, die in unterschiedlichen Situationen dienlich sein können.

Ein solches Maß für reine Zustände wurde dabei bereits eingeführt, ohne es als solches zu benennen: die *Verschränkungsentropie* (*entropy of entanglement*), welche die Entropie der reduzierten Zustände angibt:

$$\mathcal{E}(|\Psi\rangle^{AB}) = S(\rho^{A'}) = S(\rho^{B'})$$

Für gemischte Zustände sei an dieser Stelle lediglich erwähnt, dass dieser Ansatz nicht einfach übertragen werden kann. Ein Verschränkungsmaß muss im Allgemeinen bestimmte Eigenschaften erfüllen:

Definition 2.5. Ein **Verschränkungsmaß** $E(\rho)$ ist eine Abbildung von Dichteoperatoren auf die nichtnegativen reellen Zahlen $\mathbb{R}_{\geq 0}$, sodass

- (1) es für separable Zustände verschwindet: ρ ist separabel $\Leftrightarrow E(\rho) = 0$
- (2) es unter Anwendung von LOCC nicht erhöht werden kann
- (3) es sich für reine Zustände auf die Verschränkungsentropie reduziert: $E(|\Psi\rangle\langle\Psi|) = \mathcal{E}(|\Psi\rangle) \quad \forall |\Psi\rangle$

Unter LOCC (Abkürzung für *local operations and classical communication*) versteht man hierbei eine Klasse von Operationen, die lokale Manipulationen und Messungen, begleitet von Austausch klassischer Information, inkludieren. Durch diese Forderung wird sichergestellt, dass die Verschränkung nicht „zunimmt“, wenn man lediglich ein Teilsystem in Besitz hat und nur dieses manipuliert, da man ansonsten Verschränkung erzeugen könnte, ohne beide Verschränkungspartner in Besitz zu haben (mehr dazu in Kapitel 2.7).

An dieser Stelle sei lediglich erwähnt, dass es mehrere Möglichkeiten gibt, Zuständen ein Maß für die Verschränkung zuzuordnen. Je nach Anwendungsfall können bestimmte Maße bevorzugt eingesetzt werden, wobei allerdings eine Berechnung in vielen Fällen nicht analytisch erfolgen kann; ein universelles Maß kann (noch) nicht angegeben werden.

Separabilitätskriterien

Ob ein gemischter Zustand separabel oder verschränkt ist, lässt sich im Allgemeinen nicht mit freiem Auge erkennen. Eine erste Herangehensweise könnte darin bestehen, die reduzierten Zustände zu betrachten und die Entropien zu vergleichen, denn gemäß der Eigenschaft der Subadditivität gilt $S(\rho^{AB}) = S(\rho^A) + S(\rho^B) \Leftrightarrow \rho^{AB} = \rho^A \otimes \rho^B$.

Wenn die Summe der Entropien der reduzierten Zustände also gleich jener des Gesamtsystems ist, liegt mit Sicherheit ein Produktzustand vor und Verschränkung kann ausgeschlossen werden. Besteht hier ein Ungleichgewicht, lässt dies allerdings nicht unbedingt auf Verschränkung schließen. Problematisch ist hier, dass gemäß Def.2.3 auch entsprechend gewichtete *Summen von*

Produktzuständen definitionsgemäß separabel sind, und diese könnten durch Entropievergleich nicht detektiert werden.

Abhilfe schafft jedoch z.B. das *PPT-Kriterium* (*positive partial transpose criterion*), auch *Peres-Horodecki-Kriterium* genannt [13].

Zu Beginn gilt hier zu erwähnen, dass jeder Dichteoperator, den man transponiert, wieder ein gültiger Dichteoperator ist, denn es gilt: $\rho^T = (\rho^\dagger)^T = (\rho^T)^\dagger$, die Diagonalelemente werden nicht vertauscht, womit die Spur erhalten und normiert bleibt, und zudem wird auch die Determinante nicht verändert, was einer Erhaltung der Eigenwerte und der Definitheit entspricht.

Angenommen, ein gegebener Zustand sei nun separabel, also $\rho^{AB} = \sum_i p_i \rho_i^A \otimes \rho_i^B$. Wenn man nur bei den Dichteoperatoren ρ_i^B eine Transponierung durchführt, also nur einen Teil des Gesamtzustands transponiert (*partial transpose*), müsste sich durch

$$\rho^{T_B} := \sum_i p_i \rho_i^A \otimes (\rho_i^B)^T$$

ebenso ein gültiger Zustand ergeben, da ja auch die $(\rho_i^B)^T$ gültige Dichteoperatoren darstellen. Führt man diese Operation nun an einem konkreten Dichteoperator in Form einer Matrix, wie das folgende Beispiel zeigt, aus, müsste also die neue Matrix erneut einen Dichteoperator ergeben, der alle Eigenschaften eines solchen erfüllt. Das PPT-Kriterium soll hier am Bell-Zustand $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ getestet werden:

$$|\Psi^-\rangle \langle \Psi^-| = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ \hline 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \Rightarrow (|\Psi^-\rangle \langle \Psi^-|)^{T_B} = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix}$$

Die Transponierung des Systems B entspricht dabei der Transponierung der Teilmatrizen, die durch die strichlierten Linien angedeutet werden.

Die Eigenwerte der Matrix am Ende der Berechnung sind $\lambda_i = \pm \frac{1}{2}$, die Eigenwerte sind damit nicht mehr länger alle positiv und die entstandene Matrix ist damit kein Dichteoperator. Somit war die Grundannahme, es handle sich um einen Produktzustand, also falsch, und der Zustand ist verschränkt.

Aus $\rho_B^T \not\geq 0$ folgt also, dass ρ verschränkt ist, die Umkehrung gilt im Allgemeinen aber nicht, sodass die Positivität von ρ_B^T nicht unbedingt auf Separabilität hinweist. Im Falle von zwei Qubits gilt allerdings Äquivalenz dieser beiden Aussagen (siehe [13]).

Schmidt-Zerlegung und Purifizierung

Bipartite Systeme, also Systeme, die sich in zwei Teilsysteme „zerlegen“ lassen, lassen sich durch die *Schmidt-Zerlegung* besonders leicht und aussagekräftig analysieren, die folgende Definition ist sinngemäß [6, S.133] entnommen:

Theorem 2.6. Sei $|\Psi\rangle^{AB}$ ein normierter Zustand 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 $\rho^{AB} = |\Psi\rangle^{AB} \langle \Psi|^{AB}$ seien $\rho^{A'} = \text{Tr}_B(\rho^{AB})$ und $\rho^{B'} = \text{Tr}_A(\rho^{AB})$ die reduzierten Dichteoperatoren der Teilsysteme. Dann gilt:

(1) Der Zustand $|\Psi\rangle^{AB}$ kann in Form der **Schmidt-Zerlegung**

$$|\Psi\rangle^{AB} = \sum_{i=1}^k \sqrt{p_i} |u_i\rangle^A |w_i\rangle^B \quad \text{mit } p_i > 0$$

geschrieben werden, wobei $\{|u_i\rangle^A\}$ bzw. $\{|w_i\rangle^B\}$ die orthonormierten Eigenvektoren von $\rho^{A'}$ in $\mathcal{H}^A$ bzw. $\rho^{B'}$ in $\mathcal{H}^B$ sind. Für paarweise verschiedene p_i sind die Vektoren $|w_i\rangle^A$ bzw. $|u_i\rangle^B$ (bis auf eine Phase) eindeutig bestimmt. Daraus folgt:

(2) $\rho^{A'}$ und $\rho^{B'}$ haben dieselben nicht verschwindenden positiven Eigenwerte $p_1, \dots, p_k$ mit $k \leq \min(a, b)$, die Zahl k heißt der **Schmidt-Rang (Schmidt rank)** von $|\Psi\rangle^{AB}$, die $\{p_i\}$ heißen **Schmidt-Koeffizienten**.

Ein Beweis für die Aussage soll an dieser Stelle ausbleiben, hierfür wird auf [14, S.133] verwiesen. Allerdings sollen die Folgen der Aussagen, besonders im Hinblick auf Verschränkung bei reinen Zuständen, besprochen werden:

Die Koeffizienten p_i finden sich in Form von Eigenwerten in den reduzierten Zuständen $\rho^{A'}$ und $\rho^{B'}$ wieder. Ist nun $|\Psi\rangle^{AB}$ separabel, ist dies gleichbedeutend mit der Aussage, dass die Schmidt-Zerlegung nur einen Summanden besitzt, und damit gilt auch $p_1 = 1$. Dies bedeutet nach vorhergehender Aussage zudem, dass die reduzierten Zustände in diesem Fall rein sind.

Ist $|\Psi\rangle^{AB}$ nun nicht separabel, also verschränkt, ist dies verbunden mit der Tatsache, dass die Schmidt-Zerlegung mehr als einen Summanden besitzt. Damit gibt es bei den reduzierten Zuständen allerdings auch mehrere Eigenwerte $p_i > 0$, und damit liegt ein gemischter Zustand vor, womit die Äquivalenz in Gl.2.8 begründet werden kann.

Als Beispiele für die Schmidt-Zerlegung können wiederum die Bell-Zustände in 2.6 genannt werden, die allesamt aus zwei Summanden mit den Schmidt-Koeffizienten $p_1 = p_2 = \frac{1}{2}$ bestehen, welche sich als Eigenwerte in den maximal gemischten reduzierten Dichteoperatoren wiederfinden.

Eine interessante Folgerung aus der Schmidt-Zerlegung stellt zudem die *Purifizierung* dar (siehe [6, S.136]):

Theorem 2.7. Für jedes System mit Dichteoperator ρ^A aus $\mathcal{H}^A$ existiert ein reiner Zustand $|\Psi\rangle^{AB}$ aus $\mathcal{H}^A \otimes \mathcal{H}^B$, sodass ρ^A der zugehörige reduzierte Dichteoperator ist:

$$\rho^A = \text{Tr}_B(|\Psi\rangle^{AB} \langle \Psi|^{AB})$$

Laut dieser Aussage ist es also umgekehrt für jeden gemischten Zustand möglich, einen reinen Zustand in einem höherdimensionalen Hilbert-Raum so zu konstruieren, dass ρ^A sich als dessen reduzierter Zustand in einem Teilsystem ergibt. Jeder gemischte Zustand lässt sich also (zumindest theoretisch) als Teil eines „größeren“ reinen und verschränkten Zustands denken.

2.7 Anwendungen von Verschränkung

Erzeugung verschränkter Zustände

„Entanglement is a uniquely quantum mechanical resource that plays a key role in many of the most interesting applications of quantum computation and quantum information; entanglement is iron to the classical world’s bronze age.“[10, S.11]

Mit diesen Worten weisen Nielsen und Chuang bereits in der Einleitung auf die (zukünftige) Relevanz von Verschränkung hin, welche hier als Ressource betrachtet wird. Verschränkung lässt sich, wie zuvor bereits erwähnt, durch bestimmte Operationen, den LOCC, nicht „erhöhen“ (siehe *majorization* in [10, S.573-577]) und schon gar nicht erzeugen; möchte man also zwei Systeme verschränken, ist dies nicht möglich, wenn man nur auf eines davon zugreifen kann. Konkret lassen sich verschränkte Zustände, z.B. in Form zweier Qubits, mit einigen unitären Transformationen erzeugen, hierauf wird in Kapitel 3.2 noch eingegangen.

Von besonderer praktischer Relevanz ist beispielsweise die Erzeugung von verschränkten Photonenpaaren: Wenn man Photonen durch Beta-Bariumborat, einen optisch nicht-linearen Kristall, schickt, „kann dieses in zwei Photonen mit halbiertem Energiegehalt übergehen.[...]Tritt das oben beschriebene Photonenpaar in einem bestimmten Bereich des Kristalls aus, ist es maximal verschränkt; die Polarisationen sind antikorreliert, der Bell-Zustand $|\Phi^-\rangle$ entsteht.“[14, S.261]

Teleportation

Eine der wohl bekanntesten Anwendungen für verschränkte Zustände betrifft die Teleportation eines Zustands eines Systems auf ein System in räumlicher Entfernung. Im Folgenden soll die Funktionsweise davon thematisiert werden, die Ausgangssituation umfasst den zu teleportierenden Zustand $|\phi\rangle^{A'}$, sowie den Bell-Zustand $|\Phi^+\rangle^{AB}$ (in Abbildung 4 links zu erkennen).

Die weitere Vorgehensweise kann in drei Schritte gegliedert werden, wobei diese auch in Abb. 4 entsprechend gekennzeichnet sind:

(1): Der Zustand $|\phi\rangle^{A'} = \alpha|0\rangle^{A'} + \beta|1\rangle^{A'}$ befindet sich im Besitz von Alice, den Bell-Zustand $|\Phi^+\rangle^{AB}$ teilen sich Alice und Bob. Der gemeinsame Zustand kann unter Verwendung des Tensorprodukts zur Beschreibung von Mehrteilchensystemen wie folgt formuliert werden:

$$|\phi\rangle^{A'} |\Phi^+\rangle^{AB} = \frac{1}{\sqrt{2}} (\alpha |00\rangle^{A'A} |0\rangle^B + \alpha |01\rangle^{A'A} |1\rangle^B + \beta |10\rangle^{A'A} |0\rangle^B + \beta |11\rangle^{A'A} |1\rangle^B)$$

Hier wurden zur Übersicht jene Zustände, die sich im Besitz von Alice befinden, bereits gesondert in einem ket-Vektor zusammengefasst. Wie bereits in Kapitel 2.6 erwähnt, bilden die Bell-Zustände eine Basis des Hilbert-Raums $\mathcal{H}^2 \otimes \mathcal{H}^2$, somit lassen sich jene Zustände bei Alice auch durch die

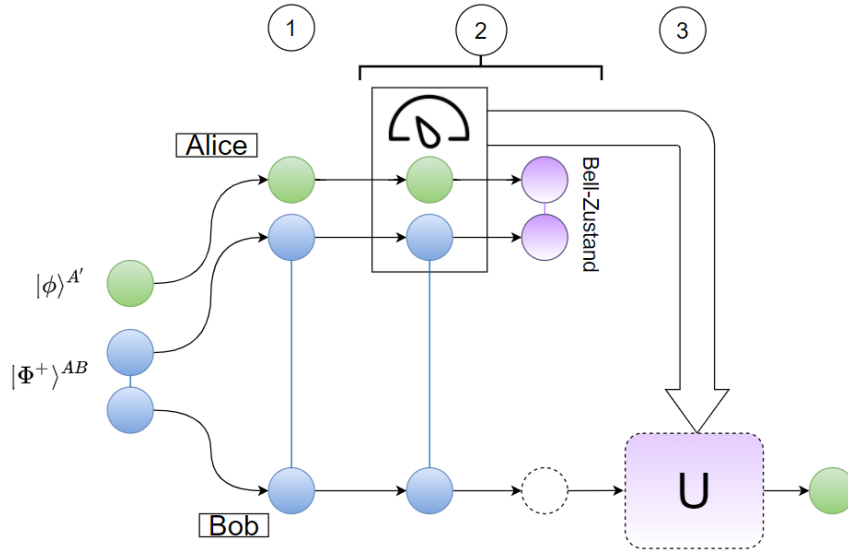


Abbildung 4: Schema der Teleportation eines beliebigen Zustands $|\phi\rangle$

Bell-Zustände ausdrücken, indem man folgendermaßen ersetzt:

$$\begin{aligned} |00\rangle &= \frac{1}{\sqrt{2}}(|\Phi^+\rangle + |\Phi^-\rangle) & |01\rangle &= \frac{1}{\sqrt{2}}(|\Psi^+\rangle + |\Psi^-\rangle) \\ |11\rangle &= \frac{1}{\sqrt{2}}(|\Phi^+\rangle - |\Phi^-\rangle) & |10\rangle &= \frac{1}{\sqrt{2}}(|\Psi^+\rangle - |\Psi^-\rangle) \end{aligned}$$

Setzt man diese nun oben ein, ergibt sich:

$$\begin{aligned} |\phi\rangle^{A'} |\Phi^+\rangle^{AB} &= \frac{1}{2} [\alpha(|\Phi^+\rangle + |\Phi^-\rangle)^{A'A} |0\rangle^B + \alpha(|\Psi^+\rangle + |\Psi^-\rangle)^{A'A} |1\rangle^B + \\ &\quad + \beta(|\Psi^+\rangle - |\Psi^-\rangle)^{A'A} |0\rangle^B + \beta(|\Phi^+\rangle - |\Phi^-\rangle)^{A'A} |1\rangle^B] \\ &= \frac{1}{2} [|\Phi^+\rangle^{A'A} (\alpha|0\rangle^B + \beta|1\rangle^B) + |\Phi^-\rangle^{A'A} (\alpha|0\rangle^B - \beta|1\rangle^B) + \\ &\quad + |\Psi^+\rangle^{A'A} (\alpha|1\rangle^B + \beta|0\rangle^B) + |\Psi^-\rangle^{A'A} (\alpha|1\rangle^B - \beta|0\rangle^B)] \end{aligned}$$

(2): Alice ist nun in der Lage, an ihrem Zustand eine *Bell-Messung* auszuführen, also eine Messung in der Bell-Basis. Dies hat zur Folge, dass nach ihrer Messung ein Bell-Zustand vorliegt, und ihr Messergebnis zudem verrät, um welchen der Bell-Zustände es sich handelt. Konkret kann dies erfolgen, indem sie auf ihr Paar an Zuständen eine unitäre Transformation anwendet, jedes einzelne System in der üblichen Basis $\{|0\rangle, |1\rangle\}$ misst, und anschließend wieder rücktransformiert (für eine genauere Behandlung siehe [6, S.159-161]).

Damit hat Alice zweierlei bewirkt: Zum einen ist sie nun in Besitz eines verschränkten Zustands, und zum anderen reduziert sie durch die Messung den obigen Gesamtzustand auf jenen Teil

Zustand nach Messung bei Alice	$\Rightarrow$ Zustand nach Messung bei Bob
$ \Phi^+\rangle^{A'A}$	$\alpha 0\rangle^B + \beta 1\rangle^B = \phi\rangle^B$
$ \Phi^-\rangle^{A'A}$	$\alpha 0\rangle^B - \beta 1\rangle^B = \sigma_z \phi\rangle^B$
$ \Psi^+\rangle^{A'A}$	$\alpha 1\rangle^B + \beta 0\rangle^B = \sigma_x \phi\rangle^B$
$ \Psi^-\rangle^{A'A}$	$\alpha 1\rangle^B - \beta 0\rangle^B = \sigma_x \sigma_z \phi\rangle^B$

Tabelle 2: Messergebnisse bei Alice und Bob nach der Bell-Messung

mit demjenigen Bell-Zustand, den sie soeben durch ihre Messung erzeugt hat. Eine Übersicht über Messergebnisse und die daraus folgenden Zustände bei Bobs System ist in Tabelle 2 zusammengefasst:

Die letzte Formulierung des Zustands von Bobs System gibt den entstandenen Zustandsvektor in Bezug zum ursprünglichen zu teleportierenden Zustand an, der Zustand bei Bob ist also lediglich eine unitäre Transformation des Zustands $|\phi\rangle$ (wobei im ersten Fall der Zustand sogar schon unverändert vorliegt).

(3): Alice kennt das Ergebnis ihrer Bell-Messung, also muss sie Bob nur noch auf klassischem Wege mitteilen, welchen der Bell-Zustände sie durch ihre Messung hergestellt hat. Entsprechend dieser Information kann Bob sein System rücktransformieren und damit den zu teleportierenden Zustand $|\phi\rangle^B$ erhalten.

Kryptographie mit Ekert-Protokoll

Für die Kryptographie, bei der es darum geht, einen Schlüssel zum Chiffrieren und anschließenden Dechiffrieren von verschlüsselten Nachrichten zu erstellen, der nicht von möglichen Lauschangriffen abgefangen werden kann und damit nur für Empfänger und Sender zugänglich ist, gibt es verschiedene Möglichkeiten, die Besonderheiten der Quantenmechanik sinnvoll einzusetzen.

Konkret gibt es unterschiedliche Protokolle, die befolgt werden können, um einen solchen Schlüssel zu erstellen. Da für das *Ekert-Protokoll* (siehe [15]) die Verschränkung maßgeblich ist, soll es an dieser Stelle noch thematisiert werden. Die folgenden Schritte sind für die Erstellung eines sicheren Schlüssels zu befolgen:

- (1):** Der Zustand $|\Psi^-\rangle^{AB} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ wird zunächst zwischen Alice und Bob aufgeteilt.
- (2):** Alice und Bob stehen nun jeweils drei Messbasen zur Verfügung, zwischen denen sie kurz vor der Messung zufällig wählen. Diese drei Messbasen sind allerdings nicht völlig gleich, Alice und Bob haben jeweils eine Basis zur Auswahl, die im jeweils anderen Labor nicht zur Verfügung steht (beispielsweise kann man sich Polarisationsfilter für Photonen vorstellen, bei denen Alice aus den Stellungen $\{0^\circ, 45^\circ, 90^\circ\}$ wählen kann, während Bob aus $\{45^\circ, 90^\circ, 135^\circ\}$ auswählt, siehe Abb. 5). Diese Messung wird für viele Photonenpaare wiederholt.
- (3):** Sobald die Messungen durchgeführt wurden, geben Alice und Bob öffentlich bekannt, welche Basen sie in den einzelnen Messungen benutzt haben. Damit besitzen beide eine Übersicht darüber, wann welche Basen gewählt wurde und insbesondere, wann die gleiche Basis gewählt wurde (was

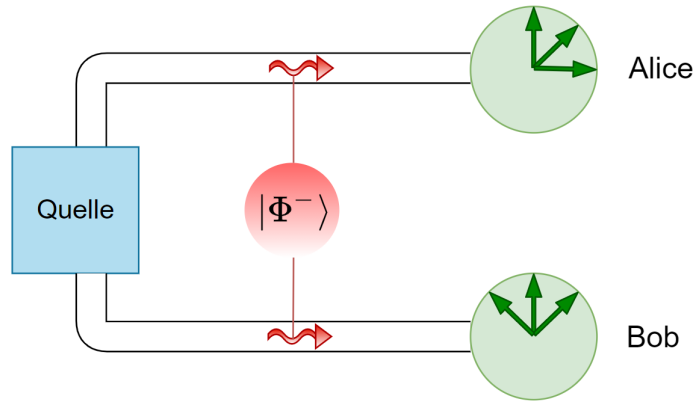


Abbildung 5: Anwendung des Ekert-Protokolls mit unterschiedlichen Messbasen bei Alice und Bob

im Durchschnitt in $\frac{2}{9}$ der Messungen der Fall ist, da es 3×3 mögliche Stellungen gibt). Da es sich um einen Bell-Zustand handelte, zeigen sich in den Ergebnissen in diesen Fällen entsprechende Korrelationen, wodurch den Ergebnissen $|0\rangle$ bei Alice und $|1\rangle$ bei Bob der Bitwert 0 sowie $|1\rangle$ bei Alice und $|0\rangle$ bei Bob der Bitwert 1 zugeordnet werden kann.

(4): Für den Rest der Ergebnisse (bei unterschiedlichen Wahlen der Messbasis) können anschließend die Messergebnisse öffentlich bekanntgegeben werden, damit die Chance besteht, mit diesen die Verletzung der CHSH-Ungleichung zu überprüfen. Wäre bei dem Prozedere ein Lauschangriff erfolgt, wären die verschränkten Zustände und damit auch die weiteren Messungen beeinflusst worden, womit die Ungleichung nicht mehr oder nur in ungenügendem Maße verletzt wäre. Liegt der Wert S_{CHSH} signifikant unter der Tsirelson-Schranke, wird der erzeugte Schlüssel verworfen und das Protokoll wiederholt.

2.8 Dekohärenz

Quantencomputer benutzen die namensgebenden Quanteneffekte von Qubits; diese Eigenschaften zu behalten, stellt allerdings in realen Systemen eine Herausforderung dar. Die *Dekohärenz* thematisiert diese Neigung, die quantenmechanischen Eigenschaften bei ungenügender Abschottung des Systems von der Umwelt zu verlieren und steht dabei in engem Zusammenhang mit der Verschränkung. Dies soll zunächst an einem einfachen Beispiel demonstriert werden, um anschließend qualitativ zu diskutieren, wie dieses Beispiel gedanklich ausgedehnt werden kann.

Ein vereinfachtes Beispiel

Die folgende vereinfachte Darstellung zur Behandlung der Dekohärenz orientiert sich stark an [16] und [14, S. 238–241]:

Hierfür wird ein (makroskopisches) Objekt (System A) betrachtet, welches in Abb. 6 als blaue

Kugel dargestellt ist. Dieses soll sich zu Beginn in Überlagerung der Zustände $|L\rangle^A$ und $|R\rangle^A$ befinden, welche die Position des Objekts charakterisieren. Zudem befindet sich ein Photon (System B) im Anflug, die Richtung der Bewegung wird zu Beginn mit dem Zustandsvektor $|\uparrow\rangle^B$ beschrieben.

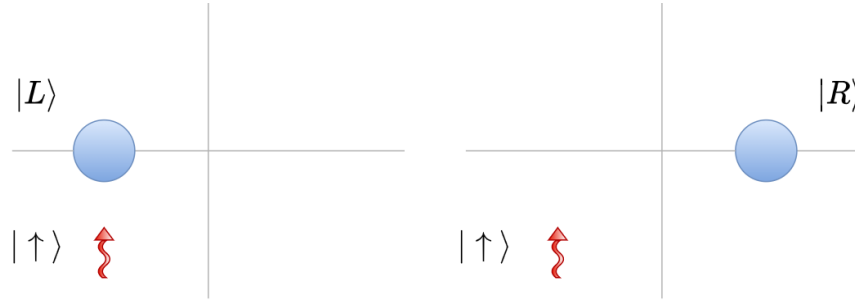


Abbildung 6: Zustände vor der möglichen Wechselwirkung zwischen Objekt (in blau) und Photon (rot)

Die Situation *vor* einem möglichen Zusammenstoß kann daher insgesamt durch den folgenden Zustand beschrieben werden:

$$|\Psi\rangle_{vor} = \frac{1}{\sqrt{2}}(|L\rangle^A + |R\rangle^A) |\uparrow\rangle^B \quad (2.9)$$

Demnach handelt es sich um einen separablen Zustand.

Die Situation nach einem möglichen Zusammenstoß (in Abb. 7 skizziert), bei dem zur Vereinfachung angenommen wird, dass das Photon gestreut wurde und der Vorgang das Objekt nicht beeinflusst hat, lässt sich dann als Überlagerung der Zustände $|R\rangle^A |\uparrow\rangle^B$ und $|L\rangle^A |\downarrow\rangle^B$ beschreiben:

$$|\Psi\rangle_{nach} = \frac{1}{\sqrt{2}}(|R\rangle^A |\uparrow\rangle^B + |L\rangle^A |\downarrow\rangle^B) \quad (2.10)$$

Dabei fällt auf, dass es sich nicht länger um einen separablen Zustand handelt, $|\Psi\rangle_{nach}$ ist demnach ein verschränkter Zustand und entspricht der Struktur nach dem Bell-Zustand $|\Phi^+\rangle$ mit entsprechender Zuordnung der Zustände $|0\rangle^{A,B}$, $|1\rangle^{A,B}$ zu den hier vorliegenden.

Betrachtet man anschließend nur das Objekt, also das System A, gelingt dies durch ausspuren des Systems B, und nach früherer Betrachtung ist bereits bekannt, dass es sich dabei um einen (maximal) gemischten Zustand handelt:

$$|\Psi\rangle_{nach}^A = Tr_B(|\Psi\rangle_{nach} \langle\Psi|_{nach}) = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix} \quad (2.11)$$

Demnach handelt es sich nicht mehr um eine kohärente Überlagerung, wie in 2.3 geschildert, sondern um eine inkohärente Überlagerung und damit ein klassisches Gemisch, das durch Inter-

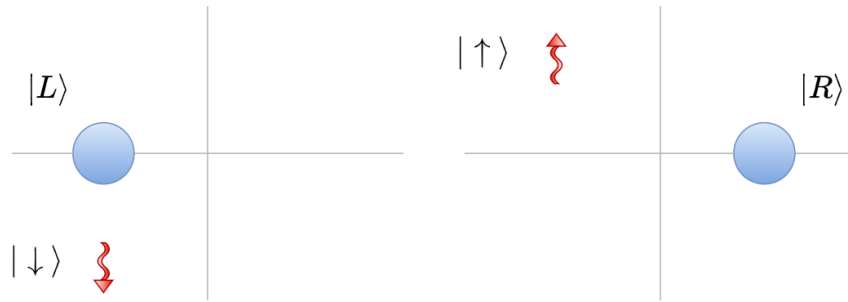


Abbildung 7: Zustände nach der möglichen Wechselwirkung zwischen Objekt (in blau) und Photon (rot)

aktion mit dem Photon seine Interferenzfähigkeit verloren hat und nicht länger mithilfe einer Superposition von Zuständen beschrieben werden kann. Die Wirkung der Dekohärenz ähnelt damit jener einer Messung (vgl. [14, S.242]).

Übergang zur klassischen Welt

Im obigen Beispiel wurden viele starke Vereinfachungen getroffen, wie z.B. der Einbezug der Umgebung mit nur einem Freiheitsgrad. Diese Betrachtung ist natürlich nicht realistisch und weicht von der Realität umso weiter ab, je größer das zu betrachtende Objekt ist, denn mit steigender Größe ergeben sich mehr Freiheitsgrade und mögliche Wechselwirkungen mit der Umgebung. Nichtsdestotrotz zeigt diese Simplifizierung bereits in Grundprinzipien auf, warum makroskopische Objekte gewohnt klassisch erscheinen und welche Rolle Verschränkung damit im Alltag spielt. Hierzu kann zusammengefasst werden:

„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.“[6, S.255]

Auf eine detailliertere mathematische Behandlung wird an dieser Stelle verzichtet, eine solche lässt sich aber beispielsweise in [6, S.259] unter „Verschränkung mit vielen Freiheitsgraden der Umgebung - Kollaps und Wiederkehr“ finden.

Für die Realisierung eines Quantencomputers und das Ausschöpfen dessen Möglichkeiten ist es deswegen äußerst wichtig, die Qubits im System von der Umgebung weitgehend abzuschotten, um die kohärente Überlagerung zu bewahren. Dies bringt einige technologische Herausforderungen mit sich, zudem hängt auch die Wahl der Realisierung der Qubits von der *Dekohärenzzeit* des Systems ab, da diese Zeit eine ungefähre obere Schranke für die Bearbeitung von Rechenschritten an den Qubits vorgibt, bevor Dekohärenz eintritt (siehe Kapitel 3.5).

3 Quantencomputer

Nach dem *Moore'schen Gesetz* verdoppelt sich die Rechenleistung von Computern bei gleichbleibenden Kosten alle zweieinhalb Jahre, und seit der Vorhersage durch den namensgebenden *Gordon Moore* im Jahr 1965 hat dieses Modell die tatsächliche Entwicklung erstaunlich akkurat prognostiziert. Dass dem allerdings eine Grenze gesetzt ist, bemerken auch Nielsen & Chuang in ihrer Einleitung:

„Amazingly enough, Moore’s law has approximately held true in the decades since the 1960s. Nevertheless, most observers expect that this dream run will end some time during the first two decades of the twenty-first century. Conventional approaches to the fabrication of computer technology are beginning to run up against fundamental difficulties of size. Quantum effects are beginning to interfere in the functioning of electronic devices as they are made smaller and smaller. “[10, S.4]

Nicht zuletzt aufgrund einiger Argumente und Ideen seitens *Richard P. Feynman* erhielt die Idee eines Quantencomputers Aufwind. Er plädierte dafür, dass es zur Beschreibung und Simulation von quantenmechanischen Effekten auch einen Computer, der nach quantenmechanischen Prinzipien arbeite, benötige:

„Can a quantum system be probabilistically simulated by a classical (probabilistic, I’d assume) universal computer? [...] If you take the computer to be the classical kind I’ve described so far [...] the answer is certainly, No! “[17]

Vorangetrieben wurde die Idee unter anderem durch Beiträge von *Peter Shor* und *Lov Grover*, welche den tatsächlichen Nutzen und die Überlegenheit des Quantencomputers in einzelnen Einsatzgebieten aufzeigten.

In diesem Kapitel sollen zunächst einige Analogien und Unterschiede von Quantencomputer und klassischem Computer sowie die theoretische Realisierung eines *universellen Quantencomputers* behandelt werden. Anhand des *Deutsch-Algorithmus* soll ein anschauliches Beispiel für die Stärken des Quantencomputers gegeben werden, bevor im Anschluss der *Grover-Algorithmus* und der *Shor-Algorithmus* diskutiert werden.

Zum Abschluss soll ein Überblick, der sich auch an aktuellen Ereignissen orientieren soll, über konkrete Realisierungsmöglichkeiten und eventuelle Hürden erfolgen sowie ein kurzer Ausblick dargelegt werden.

3.1 Quantenschaltkreise und unitäre Transformationen

Klassischer Computer und Quantencomputer

Die Wirkungsweise eines klassischen Computers lässt sich anhand eines Schaltkreises und der Verwendung von logischen *Gattern* (*Gates*) veranschaulichen. Zwei Beispiele für Gates, die dabei zum Einsatz kommen, sind das AND-Gate und das OR-Gate (siehe Abb. 8). Für zwei Bits, deren Signale mit diesen Gates bearbeitet werden, können Wahrheitstabellen erstellt werden, an denen das Ausgangssignal für alle möglichen Kombinationen von Eingangssignalen verdeutlicht wird.

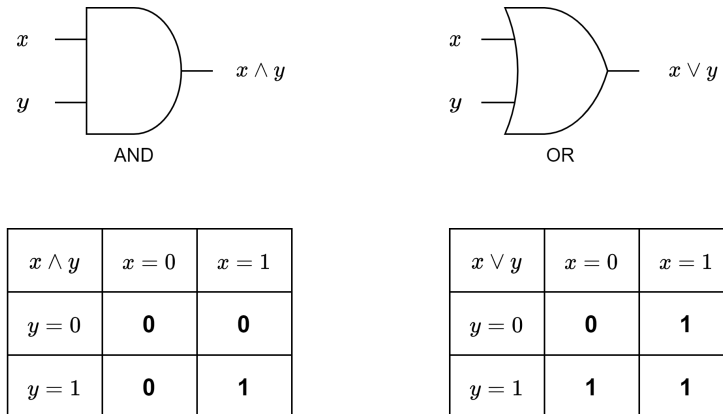


Abbildung 8: AND- und OR-Gates mit Wahrheitstabelle für klassische Bits

Durch entsprechende Anordnung und Verknüpfung von logischen Gattern kann ein Schaltkreis entstehen, um z.B. ein bestimmtes Problem zu lösen und eine Berechnung an einem Register von Bits auszuführen.

Das entsprechende Analogon im Quantencomputer bilden die *Quantenschaltkreise* (*quantum circuits*), anhand derer die Wirkungsweise eines Quantencomputers auf ein *Quantenregister*, welches durch Qubit-Zustände repräsentiert wird, dargestellt wird. Diese Wirkung wird dabei in Form einer unitären Transformation (siehe *Schrödingergleichung und Postulat III* in Kapitel 2.2) auf die Qubits angewendet, grundsätzlich kann man sich in diesem Modell einen Quantenschaltkreis also als Anwendung einer unitären Transformation auf einen Zustand $|\Psi\rangle$ vorstellen, wie in Abb.9, wobei der Zustand $U|\Psi\rangle$ einem Ergebnis der Berechnung entspricht. An dieser Stelle soll erwähnt werden, dass die Ausführung von unitären Transformationen zur Durchführung einer bestimmten Berechnung nicht die einzige Variante zur Konzipierung eines Quantencomputers darstellt. Ebenso sind beispielsweise *Einweg-Quantencomputer* denkbar, bei denen Berechnungen durch Kombinationen von Messungen und unitären Operationen (welche wiederum abhängig von vorangegangenen Messergebnissen sind) an verschränkten Zuständen ausgeführt werden (vgl. [14, S.266-269]).

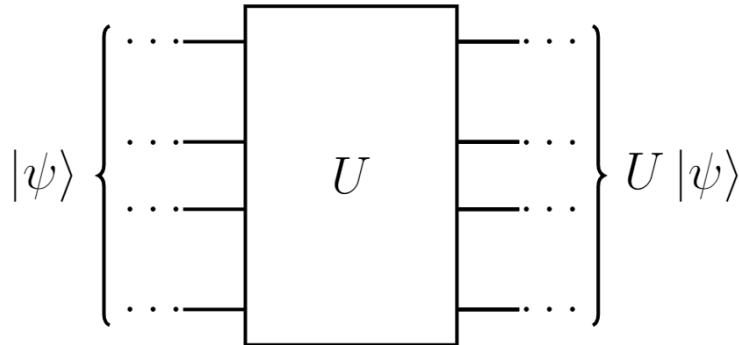


Abbildung 9: Schema eines Quantencomputers mit unitärer Transformation U

Da unitäre Transformationen prinzipiell *reversibel* sind, sind damit auch die damit realisierten Berechnungsvorgänge in einem Quantencomputer (im Gegensatz zum klassischen Computer) prinzipiell umkehrbar.

Diese unitäre Transformation lässt sich dabei, ähnlich der Berechnung eines klassischen Computers, in einzelne Schritte zerlegen, die sich durch Anordnung von *Quantengattern* (*quantum gates*) bilden lassen. Die Signalverarbeitung geschieht dabei durch entsprechende Operationen auf Qubits, welche in einem Quantenschaltkreis ähnlich der klassischen Variante (wie auch in Abb. 9 angedeutet) als Linien skizziert werden. In klassischen Schaltkreisen kann man sich dabei vorstellen, dass Elektronen durch den Schaltkreis „wandern“ und sie verschiedene Gatter nacheinander ansteuern; in diesem Fall ist es allerdings treffender, sich unter dem Verlauf eines Quantenschaltkreises eine rein zeitliche Abfolge von Operationen vorzustellen, die auf die (ruhenden) Qubits angewendet werden.

Wie bereits angedeutet, ergeben sich durchaus grundlegende Unterschiede in der Arbeitsweise von Quantencomputern und klassischen Computern durch die Umkehrbarkeit von Berechnungen. Neben der Tatsache, dass sich beliebige Qubits z.B. nicht einfach kopieren lassen (siehe *No-Cloning-Theorem* in Kapitel. 3.2), lassen sich Qubits auch nicht ohne weiteres Löschen. Dies ist auch an der Beobachtung ersichtlich, dass klassische Gatter wie das AND-Gatter zwei Eingangsbits und ein Ausgangsbit haben, eine solche Wirkung ist allerdings mit unitären Operationen nicht möglich.

So kann man bestimmte Operationen, die man mit klassischen Computern bedenkenlos ausführen kann, mit einem Quantencomputer zunächst nicht völlig analog übernehmen. Die Gestaltung beliebiger Berechnungen eines klassischen Computers ist in Quantenschaltkreisen durch entsprechende Konstruktion allerdings trotzdem möglich, ein kurzer Ausblick darauf soll in Kapitel 3.2 folgen.

Während klassische Gates also zumeist zwei oder mehrere Bits verarbeiten und für einzelne Bits nur die Möglichkeit eines Bit-Flips in Form einer Negation bleibt, soll in Tab.3 zunächst

eine Übersicht für *Single-Qubit-Gates* erfolgen, die nur auf einzelne Qubits wirken und häufig Verwendung finden.

Tabelle 3: Single-Qubit-Gates und Wirkungsweise auf Qubits

Schaltzeichen	Matrixdarstellung	Beschreibung
	$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$	Hadamard-Gate - Basiswechsel: $H 0\rangle = +\rangle, \quad H 1\rangle = -\rangle$ $H +\rangle = 0\rangle, \quad H -\rangle = 1\rangle$
	$R_x(\Phi) = \begin{bmatrix} \cos \frac{\Phi}{2} & -i \sin \frac{\Phi}{2} \\ -i \sin \frac{\Phi}{2} & \cos \frac{\Phi}{2} \end{bmatrix}$	Rotation des Blochvektors um x-Achse
	$X = \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	Pauli-X-Gate - vertauscht Basisvektoren ("bit flip")
	$R_y(\Phi) = \begin{bmatrix} \cos \frac{\Phi}{2} & -\sin \frac{\Phi}{2} \\ \sin \frac{\Phi}{2} & \cos \frac{\Phi}{2} \end{bmatrix}$	Rotation des Blochvektors um y-Achse
	$Y = \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$	Pauli-Y-Gate
	$R_z(\Phi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\Phi} \end{bmatrix}$	Rotation des Blochvektors um z-Achse Verändert die relative Phase zwischen Basisvektoren
	$Z = \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = R_z(\pi)$	Pauli-Z-Gate - ändert die relative Phase um π ("phase flip")
	$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} = R_z\left(\frac{\pi}{2}\right)$	Phase Gate - ändert die relative Phase um $\pi/2$
	$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix} = R_z\left(\frac{\pi}{4}\right)$	Verändert die relative Phase um $\pi/4$

Grundprinzipien des Quantencomputers

Als Grundlagen, nach denen ein Quantencomputer arbeitet, und die bei der Erstellung und Bearbeitung eines Algorithmus zu beachten sind, können nach vorhergehenden Überlegungen folgende drei *Prinzipien des Quantum Computing* genannt werden (vgl. [14, S.52-53]):

- **Registerzustände:** „Ein Quantenregister aus n Quantenbits wird durch einen $2n$ -dimensionalen Vektorraum über den komplexen Zahlen beschrieben. Die Standardbasis bildet die Menge der durch n klassische Bits darstellbaren Zahlen $\{|0\rangle, |1\rangle, |2\rangle, \dots, |2^n - 1\rangle\}$

oder die entsprechenden Binärdarstellungen $|00..00\rangle, |00..01\rangle, |00..10\rangle, \dots, |11..11\rangle$.“

(Anmerkung: Im Falle von zwei Qubits entspricht dies der Zuordnung $|00\rangle \mapsto |0\rangle, |01\rangle \mapsto |1\rangle, |10\rangle \mapsto |2\rangle, |11\rangle \mapsto |3\rangle$, für drei Qubits würde dies $|000\rangle \mapsto |0\rangle, |001\rangle \mapsto |1\rangle, \dots, |111\rangle \mapsto |8\rangle$ bedeuten.)

- **Rechenschritte:** „Mögliche Veränderungen an Quantenregistern werden durch unitäre Transformationen beschrieben. Dadurch ist jeder Rechenschritt auf einem Quantencomputer umkehrbar. Die möglichen Rechenschritte sind lokal: sie lassen sich in unitäre Operationen zerlegen, an denen höchstens zwei der Qubits beteiligt sind. Die Zerlegung geschieht gemäß dem Tensorprodukt.“

(Anmerkung: die hier angesprochene Zerlegung, die ein weiteres Postulat der Quantenmechanik darstellt, wird in Kapitel. 3.2 thematisiert.)

- **Messungen:** „Misst man ein Quantenregister im Zustand $R = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$ bezüglich der Standardbasis $\{|i\rangle\}$, $i \in \{0, 1, \dots, 2^n - 1\}$, erhält man mit Wahrscheinlichkeit $|\alpha_i|^2$ das Ergebnis $|i\rangle$. Misst man bezüglich einer Orthonormalbasis $\{|b_i\rangle\}$, $i \in \{0, 1, \dots, 2^n - 1\}$, und hat der Registerzustand gemäß dieser Basis die Form $R = \sum_{i=0}^{2^n-1} \beta_i |b_i\rangle$, so erhält man mit Wahrscheinlichkeit $|\beta_i|^2$ das Ergebnis $|b_i\rangle$.“

(Anmerkung: Dies folgt im Wesentlichen aus den Postulaten der Quantenmechanik, soll an dieser Stelle der Vollständigkeit halber aber nicht fehlen.)

Ein echter Zufallsgenerator

Als erstes illustratives Beispiel sei hier ein Zufallsgenerator gewählt, da hierfür nur ein Single-Qubit-Gate erforderlich ist. Konkrete Relevanz besteht hier darin, dass klassische Computer nur „Pseudozufallszahlen“ erzeugen, da die Berechnung und Ausgabe dabei streng deterministisch erfolgt, somit handelt es sich dabei nicht um echte Zufallszahlen (vgl. [14, S.26]).

Für dieses Problem kann daher ein System, das mit Qubits arbeitet, aufgrund des inhärenten Zufalls in der Quantenmechanik eingesetzt werden. Die Erzeugung eines Zufallsbits ist in Abb. 10 links zu sehen:

Am Qubit im Startzustand $|0\rangle$ wird mithilfe des *Hadamard-Gatters* eine gleichgewichtete Superposition von $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ erzeugt, welches anschließend gemessen wird und dabei mit einer Wahrscheinlichkeit von je 50% der Wert 0 oder 1 festgestellt wird.

Die Ausweitung auf eine n-Bit-Zufallszahl gestaltet sich lediglich durch Erweitern um $n - 1$ Qubits und Durchführen der gleichen Schritte (Abb. 10, rechts), wodurch eine Zufallszahl $0 \leq x \leq 2^n - 1$ erzeugt werden kann. Hier sei zudem auf die kompaktere Darstellung der n Qubits durch die Bezeichnung $|0\rangle^{\otimes n}$ bzw. das Zeichen $/^n$ sowie die n -fache Ausführung des Hadamard-Gatters durch $H^{\otimes n}$ hingewiesen. An dieser Stelle wird zudem deutlich, dass der Messprozess am Ende des Algorithmus einen integralen Bestandteil eines Quantenalgorithmus darstellt, wie bereits in obiger Aufzählung der Grundprinzipien angedeutet.

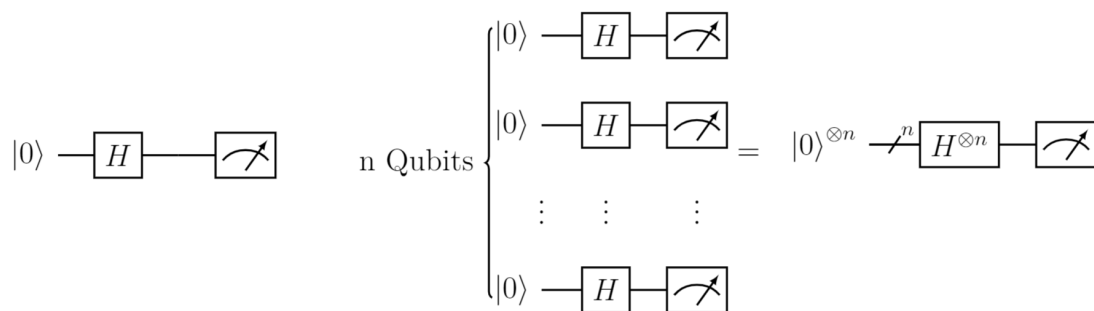


Abbildung 10: Schaltkreis für 1-Bit- (links) und n -Bit-Zufallsgenerator (rechts). Die Notation $/^n$ dient dazu, mehrere Qubits zusammenzufassen.

3.2 Universelle Quantencomputer

Für den klassischen Computer existiert die Vorstellung der *Turingmaschine*, die auf Alan Turing zurückgeht und Berechnungen eines Computers als das (Um)schreiben einer Zahlenreihe mit den Ziffern 0 und 1 auf einem Papierband deutet. Je nachdem, welche Ziffer der *Schreib-Lese-Kopf* an einer bestimmten Stelle am Papierband wahrnimmt und welcher Algorithmus der Maschine zur Ausführung übergeben wurde, tauscht die Maschine Ziffern am Papierband aus oder belässt es beim momentanen Stand. Das Ergebnis einer Berechnung kann man ablesen, sobald die Maschine alle Schritte ausgeführt hat (vgl. [14, S.13-14]).

So wie es also für eine Turingmaschine und klassische Computer wünschenswert ist, dass sie verschiedene Probleme lösen können (je nachdem, welchen Algorithmus man der Turingmaschine übergibt, führt sie andere Berechnungen am Papierband durch) und damit *universell* sind, wird diese Forderung auch an den Quantencomputer gestellt. Zum Beispiel lässt sich jede Funktion eines klassischen Computers prinzipiell vollständig aus einer Anordnung von NAND-Gattern (NOT AND) aufbauen, diese Eigenschaft wird *functional completeness* genannt. Die Frage, wie man einen *universellen Quantencomputer* durch Aneinanderreihung von Quantengattern konzipieren kann, wird im Folgenden beantwortet.

CNOT-Gate

Ein elementares Gatter zur Konzipierung eines universellen Quantencomputers stellt das *CNOT-Gate* (*controlled NOT*) dar, welches auf zwei Qubits wirkt und in Abb. 11 schematisch skizziert ist (siehe [10, S.20]). Die Qubits werden dabei üblicherweise als *Kontroll-Qubit* und *Ziel-Qubit* bezeichnet, da der Zustand des Kontroll-Qubits für die Änderung des Ziel-Qubits zuständig ist. Durch das CNOT-Gate erfolgt dabei eine Abbildung $|x, y\rangle \mapsto |x, x \oplus y\rangle$, wobei $\oplus$ einer binären Addition entspricht. Dadurch erfolgt also konkret diese Zuordnung:

$$\begin{aligned} |0, 0\rangle &\mapsto |0, 0\rangle & |1, 0\rangle &\mapsto |1, 1\rangle \\ |0, 1\rangle &\mapsto |0, 1\rangle & |1, 1\rangle &\mapsto |1, 0\rangle \end{aligned}$$

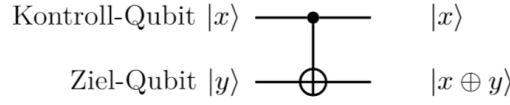


Abbildung 11: Schaltzeichen eines CNOT-Gates

Quantenmechanisch formuliert entspricht dies einer unitären Operation

$$U_{CNOT} = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \sigma_x.$$

Beispielhaft lässt sich die Wirkung desselben mithilfe eines Anfangszustands $|00\rangle$ untersuchen: Führt man z.B. vor Anwendung des CNOT-Gates am Kontroll-Qubit eine Hadamard-Transformation durch (und erzeugt damit in diesem Fall eine gleichgewichtete Superposition von Basiszuständen), lässt sich dies wie folgt ausdrücken:

$$\begin{aligned} U_{CNOT}(H \otimes \mathbb{1})|0\rangle|0\rangle &= (|0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \sigma_x) \left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle \right] = \\ &= \frac{1}{\sqrt{2}}(|0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \sigma_x)[|0\rangle|0\rangle + |1\rangle|0\rangle] = \\ &= \frac{1}{\sqrt{2}}[|0\rangle|0\rangle + |1\rangle|1\rangle] = |\Phi^+\rangle \end{aligned}$$

Dadurch erkennt man: mit dem CNOT-Gate lässt sich Verschränkung erzeugen.

No-Cloning-Theorem

An dieser Stelle soll das *No-Cloning-Theorem* (vgl. [14, S.81-84]) vorgestellt werden, wonach es im Allgemeinen nicht möglich ist, einen beliebigen Zustand zu kopieren:

Theorem 3.1. *Es gibt keine unitäre Transformation U , sodass für alle $|\psi\rangle$ und einen bestimmten Zustand $|0\rangle$ gilt: $U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$*

Dies soll durch Widerspruch gezeigt werden:

Angenommen, es gäbe eine solche unitäre Transformation die zwei beliebige Zustände $|\psi\rangle, |\phi\rangle$ auf diese Art kopieren kann, also sodass gilt:

$$U|\psi\rangle^A|0\rangle^B = |\psi\rangle^A|\psi\rangle^B \quad \text{und} \quad U|\phi\rangle^A|0\rangle^B = |\phi\rangle^A|\phi\rangle^B$$

Das innere Produkt der beiden Vektoren müsste in beiden Darstellungen zum gleichen Ergebnis führen, also:

$$\begin{aligned}
(\langle \psi|^A \langle 0|^B U^\dagger)(U |\phi\rangle^A |0\rangle^B) &= (\langle \psi|^A \langle \psi|^B)(|\phi\rangle^A |\phi\rangle^B) \\
U^\dagger U = \mathbb{1} \Rightarrow \langle \psi|\phi\rangle^A \langle 0|0\rangle^B &= \langle \psi|\phi\rangle^A \langle \psi|\phi\rangle^B \\
\Rightarrow \langle \psi|\phi\rangle &= \langle \psi|\phi\rangle^2 \Rightarrow \langle \psi|\phi\rangle \in \{0, 1\}
\end{aligned}$$

Damit gilt, dass die beiden Zustandsvektoren $|\psi\rangle$ und $|\phi\rangle$ entweder gleich oder orthogonal sein müssten, und die Aussage damit nicht für beliebige Zustandsvektoren gelten kann.

Damit wird allerdings auch ausgesagt, dass sich *bestimmte* Zustände sehr wohl mit einer unitären Transformation kopieren lassen, nämlich wenn sie die genannte Bedingung erfüllen. Eine solche unitäre Transformation wurde zuvor schon erwähnt: Das CNOT-Gate kann, wie man den zuvorgehenden Ausführungen entnehmen kann, die orthogonalen Zustände $|0\rangle$ und $|1\rangle$ auf das Ziel-Qubit übertragen, wenn dieses im Zustand $|0\rangle$ vorliegt.

Kontrollierte Operationen für zwei Qubits

Bisher wurden lediglich Single-Qubit-Gates und das CNOT-Gate genannt, wobei letzteres auf zwei Qubits wirkt. Als eine Verallgemeinerung des CNOT-Gates kann eine *kontrollierte unitäre Operation* (*controlled unitary*) betrachtet werden, welche schematisch in Abb. 12, links dargestellt ist.

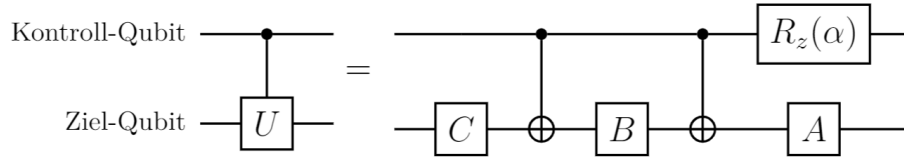


Abbildung 12: Schaltzeichen einer kontrollierten unitären Operation und Zerlegung in Single-Qubit-Gates und CNOT-Gates

Dass eine solche beliebige kontrollierte Operation mit den bisherigen Gates möglich ist, soll nun thematisiert werden, wobei für ausführliche Beweise und Darlegungen auf [10, S.175-176] verwiesen wird.

Hierfür sind folgende zwei Aussagen notwendig:

Korollar 3.2. *Sei U eine unitäre Operation auf einem Qubit, dann existieren $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ sodass:*

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta) \quad (3.1)$$

Bei den Operatoren R_y, R_z handelt es sich um Rotationen eines Blochvektors in der Blochkugel um die y - und z -Achse. Die Aussage lässt sich derart interpretieren, als dass man sich eine unitäre Operation an einem Qubit anhand des Blochvektors vorstellen kann: da es sich um eine unitäre Operation handelt, ist sie normerhaltend, damit ergibt sich auch danach ein Blochvektor

gleicher Länge, und die Operation resultiert in einer Drehung des Blochvektors um eine durch die Operation festgelegte Achse. Jede beliebige Rotation lässt sich allerdings zerlegen in drei aufeinanderfolgende Rotationen um zwei feste Achsen, also eine Rotation um die z-Achse mit dem Winkel δ , gefolgt von einer Rotation um die y-Achse mit dem Winkel γ und einer abschließenden Rotation um die z-Achse mit dem Winkel β ; bei α handelt es sich um eine Phase.

Diese Aussage lässt sich nun folgendermaßen weiterverwenden:

Korollar 3.3. *Sei U eine unitäre Operation auf einem Qubit, dann existieren unitäre Operationen A, B, C , sodass*

$$U = e^{i\alpha} A \sigma_x B \sigma_x C \quad \text{und} \quad ABC = \mathbb{1}$$

Von der Äquivalenz dieser Aussagen kann man sich durch geeignete Wahl von A, B, C mit $A = R_z(\beta)R_y(\frac{\gamma}{2})$, $B = R_y(-\frac{\gamma}{2})R_z(-\frac{\delta+\beta}{2})$ und $C = R_z(\frac{\delta-\beta}{2})$ überzeugen. Diese Zerlegung ist jene, die in Abb. 12, (rechts) in Form eines Quantenschaltkreises realisiert ist. Spielt man nun für das Kontroll-Qubit $|x\rangle$ zwei Szenarien durch, lässt sich folgendes feststellen:

- $|x\rangle = |0\rangle$: Die CNOT-Gates bewirken keine Änderung am Ziel-Qubit $|y\rangle$, es werden nur die Transformationen A, B und C (in umgekehrter Reihenfolge) darauf angewendet, und da $ABC = \mathbb{1}$ gilt, liegt auch insgesamt keine Änderung vor. Da $R_\alpha |0\rangle = |0\rangle$, verändert auch diese Operation nichts am Zustand.
- $|x\rangle = |1\rangle$: Auf das Ziel-Qubit $|y\rangle$ wirken die Operatoren derart, dass die Transformation $A\sigma_x B\sigma_x C |y\rangle$ durchgeführt wird. Die noch fehlende Phase wird nun in Form einer Rotation am Kontroll-Qubit vorgesehen, was äquivalent zur Ausführung der Operation $e^{i\alpha}$ am Ziel-Qubit ist (hierfür siehe [10, S.180]), womit insgesamt die gewünschte unitäre Transformation U ausgeführt wird.

Mit der geschilderten Zerlegung ist es damit gelungen, kontrollierte unitäre Operationen an einem Qubits, gesteuert durch ein anderes Qubit, mithilfe von Single-Qubit-Gates und zweier CNOT-Gates durchzuführen. Kontrollierte unitäre Operationen werden im Allgemeinen mit $C^n(U)$ bezeichnet, wobei n die Anzahl der Kontroll-Qubits angibt. Im vorliegenden Fall handelte es sich um $C(U)$ -Operationen, im Folgenden werden $C^2(U)$ und Möglichkeiten zur allgemeinen Erweiterung dargelegt.

Kontrollierte Operationen für drei Qubits und Toffoli-Gate

Um eine unitäre Operation an einem Ziel-Qubit mit zwei Kontroll-Qubits zu steuern, wie in Abbildung 13 (links) angedeutet, kann folgende Überlegung angestellt werden:

Unitäre Operatoren sind diagonalisierbar, also lässt sich auch ein Operator denken, der einer Wurzel des Operators U entspricht: $V := \sqrt{U}$ (bzw. $V^2 = U$), wobei V wieder unitär ist, also mit vorhergehenden Erkenntnissen auch in Form einer kontrollierten Operation $C(U)$ an einem Ziel-Qubit vorgesehen werden kann.

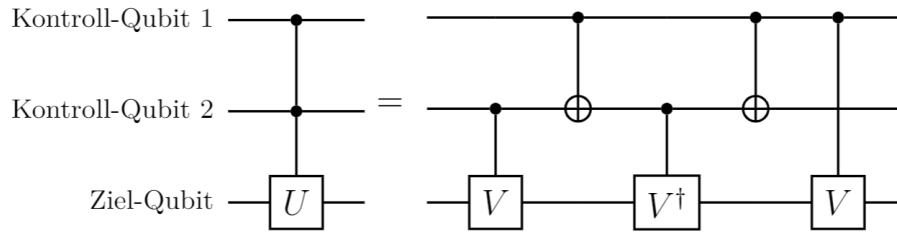


Abbildung 13: Schaltzeichen einer $C^2(U)$ -Operation und deren Zerlegung in CNOT-Gates und $C(U)$ -Operationen

Sieht man nun eine Schaltung wie in Abbildung 13 (rechts) vor, ergeben sich bei Analyse der möglichen Zustände der Kontroll-Qubits folgende Szenarien:

- $|x_1, x_2\rangle = |00\rangle$: Weder die CNOT-Gates, noch die unitären Operationen V oder $V^\dagger$ verändern etwas am Zustand des Ziel-Qubits.
- $|x_1, x_2\rangle = |10\rangle$ oder $|x_1, x_2\rangle = |01\rangle$: Je nach Reihenfolge der Kontroll-Qubits erfährt das Ziel-Qubit $|y\rangle$ entweder die Operation $VV^\dagger|y\rangle$ oder $V^\dagger V|y\rangle$, und da V unitär ist, gilt $V^\dagger V = VV^\dagger = \mathbf{1}$, womit erneut keine Änderung am Ziel-Qubit bewerkstelligt wird.
- $|x_1, x_2\rangle = |11\rangle$: Am Ziel-Qubit wirken nur die beiden unitären Transformationen V , da jenes Kontroll-Qubit, das die Transformation $V^\dagger$ auslösen würde, kurzzeitig von den CNOT-Gates auf $|0\rangle$ geändert wird. Somit ergibt sich für das Ziel-Qubit der Zustand $V^2|y\rangle = U|y\rangle$

So wie zuvor eine kontrollierte unitäre Operation $C(U)$ als Verallgemeinerung eines CNOT-Gates (mit $U = \sigma_x$) betrachtet wurde, lässt sich auch hier durch entsprechendes Einsetzen des Pauli-X-Gates ein Spezialfall konstruieren: das sogenannte *Toffoli-Gate* (siehe Abb. 14, links)

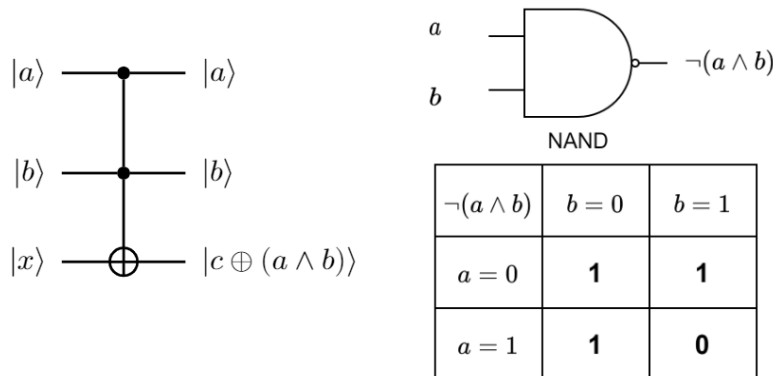


Abbildung 14: Schaltzeichen eines Toffoli-Gates (links) und eines klassischen NAND-Gates mit Wahrheitstabelle (rechts)

Durch die Möglichkeit, ein Toffoli-Gate zu konstruieren, ergibt sich eine interessante Folgerung: Wie zu Beginn erwähnt, ergeben sich für Quantencomputer insofern andere Spielregeln, als dass Qubits z.B. nicht gelöscht werden können. So besitzt z.B. das NAND-Gate, zu sehen in Abb. 14 (rechts), zwei Eingänge und nur einen Ausgang, was für ein Quantengatter prinzipiell nicht denkbar ist. Dieses Problem kann man aber lösen, indem man jene Qubits, die für die Berechnung eines Ergebnisses einer Operation verwendet wurden, einfach weiterhin mitführt und damit die Eingangs-Qubits gewissermaßen speichert.

Wie in Abbildung 14 (links) angedeutet, kann nun die Wirkung des Toffoli-Gates als eine Zuordnung $|x_1, x_2, y\rangle \mapsto |x_1, x_2, y \oplus (x_1 \wedge x_2)\rangle$ (vgl. [14, S.87]) aufgefasst werden, wobei die Operation $\wedge$ der klassischen AND-Operation entspricht und $\oplus$ wieder die binäre Addition darstellt.

Dass die Qubit-Zustände $|x_1\rangle$ und $|x_2\rangle$ auch im Ergebniszustand wieder unverändert vorliegen, lässt sich dabei als „Speichern“ von Eingangszuständen deuten, während man den Zustand $|y\rangle$ als Ergebnis der Berechnung deuten kann. Wählt man nun $|y\rangle = |1\rangle$ entspricht dies durch die binäre Addition einer *Negation des Ergebnisses der AND-Verknüpfung*, somit kann das Toffoli-Gatter als umkehrbares Analogon für das klassische NAND-Gatter verwendet werden. Da, wie zuvor erwähnt, klassische Computer theoretisch nur aus NAND-Gattern aufgebaut werden können, ist mit dem Toffoli-Gatter eine Möglichkeit geboten, alle klassischen Algorithmen auch auf einem Quantencomputer auszuführen. Der Unterschied besteht darin, dass die Eingangsbits „gespeichert“ werden und damit jede klassische Operation in eine reversible Variante übergeführt werden kann, was wiederum für die Anwendung in Form von unitären Operationen zwingend erfüllt sein muss.

Ganz allgemein gilt sogar: Man kann „jedes Gatter für eine klassische logische Operation mit zwei Eingabebits und einem Ausgabebit durch konstant [bzw. endlich] viele Toffoli-Gatter ersetzen“ [14, S.88].

Beliebige unitäre Operationen

Das Toffoli-Gate lässt sich nun wiederum weiterverwenden, um unitäre Transformationen durch beliebig viele Kontroll-Qubits, also $C^n(U)$ -Operationen zu ermöglichen. Als Beispiel ist in Abb. 15 die Realisierung einer $C^3(U)$ -Operation, also einer unitären Operation, die von drei Kontroll-Qubits gesteuert wird, dargestellt. Um dies zu realisieren, sind in diesem Fall zwei Hilfs-Qubits notwendig, das Prinzip kann für beliebige $C^n(U)$ -Operationen unter Verwendung zusätzlicher Hilfs-Qubits erweitert werden.

Zu guter Letzt gilt noch darauf hinzuweisen, welche Rolle $C^n(U)$ -Operationen nun für einen Quantencomputer spielen:

Wie zu Beginn erwähnt, kann die Wirkung der Berechnung eines Quantencomputers auf den Eingangszustand als eine übergreifende unitäre Transformation dargestellt werden (siehe Abb. 9). An dieser Stelle lässt sich anmerken, dass jede beliebige unitäre Transformation in ein Produkt von unitären Transformationen zerlegt werden kann, welche nur auf einen zweidimensionalen

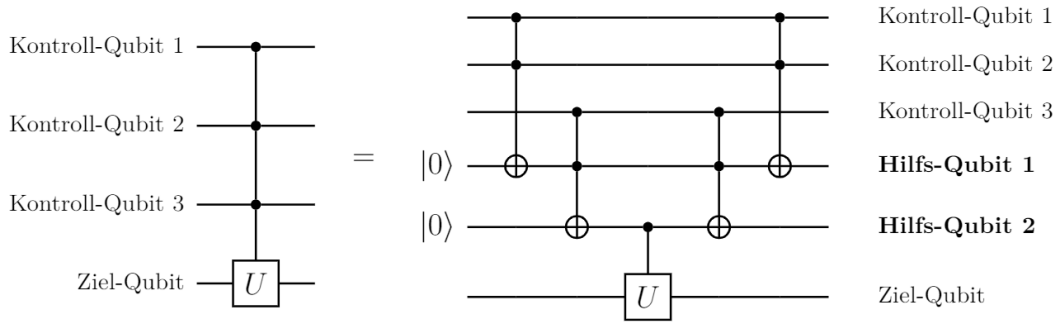


Abbildung 15: Schaltzeichen einer $C^3(U)$ -Operation und deren Zerlegung in Toffoli-Gates und einer $C(U)$ -Operation

Unterraum des gesamten Hilbert-Raums wirken (siehe [10, S.188]). Dies bedeutet anschaulich, dass jede denkbare unitäre Transformation in eine Nacheinanderausführung von (kontrollierten) unitären Operationen auf einzelne zwei-Level-Systeme, also z.B. Qubits, zerlegbar ist, und diese sind wiederum mithilfe der zuvor geschilderten Schritte in Form von $C^n(U)$ -Operationen durchführbar. (Für die konkrete Verwendung zum Einsatz in einem bestimmten Unterraum ist zudem die Anwendung von *Gray-Codes* notwendig, an dieser Stelle soll lediglich auf die Behandlung in [10, S.191-194] verwiesen werden.)

Zusammenfassung

Die zuvor erfolgte Betrachtung ist in umgekehrter Reihenfolge nochmal in Abb. 16 veranschaulicht, um damit zu verdeutlichen, welche Operationen für einen Quantencomputer durchführbar sein müssen.

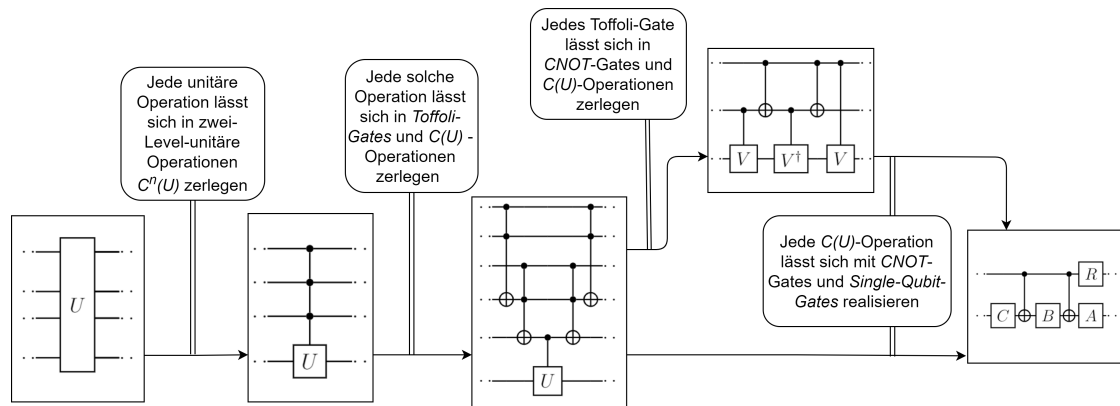


Abbildung 16: Zusammenfassung der Erkenntnisse in umgekehrter Reihenfolge

Aus dieser Abbildung ist erkennbar, dass für beliebige unitäre Operationen auf einem Eingangszu-

stand lediglich die Durchführung von CNOT-Gates und Single-Qubit-Gates möglich sein muss. Bis zu diesem Punkt wurden dabei nur CNOT-Gates als Kopplung zweier Qubits betrachtet, allerdings lassen sich CNOT-Gates auch mit anderen Kopplungen, wie dem *SWAP-Gate* (Vertauschung der Qubits) oder dem *CZ-Gate* (Controlled Z) konstruieren.

Zuletzt soll noch angemerkt werden, dass die Single-Qubit-Gates prinzipiell *beliebige* unitäre Transformationen, wie in Form von Rotationen, darstellen können. Diese lassen sich jedoch durch ein *diskretes Set* an Operationen approximieren, beispielsweise können hierfür Kombinationen der H -, S - und T -Gates verwendet werden um damit beliebige Gates in ungefährender Weise „nachzubauen“. Dadurch ergibt sich die Möglichkeit, jede unitäre Transformation lediglich unter Verwendung der vier Gates $\{CNOT, H, S, T\}$ näherungsweise durchzuführen (siehe [10, S.194-197]).

3.3 Parallelismus und prinzipielle Wirkungsweise

Nach der theoretischen Betrachtung von unitären Transformationen soll nun anhand eines konkreten Algorithmus der Nutzen und die Wirkungsweise eines Quantencomputers verdeutlicht werden.

Parallelismus durch Qubits

Ein entscheidender Vorteil und wesentliches Charakteristikum eines Quantencomputers ist der *Quantenparallelismus*. Zwar können klassische Computer, die mit mehreren Prozessoren ausgestattet sind, ebenso mehrere Befehle parallel ausführen; mit dem Quantenparallelismus ist jedoch gemeint, dass die *Eingabe selbst* die Superposition aller möglichen Bitkombinationen darstellen und dadurch wesentliche Vorteile verschaffen kann, denn „ein Quantenalgorithmus kann in einem einzelnen Rechengang auf allen möglichen Eingaben gleichzeitig rechnen, und wir erhalten eine Superposition aller Ergebnisse“ [14, S.2].

Diese Superposition aller möglichen Kombinationen kann man sich mathematisch näher führen, indem man mit einem n -Qubit-Register $|00\dots00\rangle$ (also n -mal dem Zustand $|0\rangle$) beginnt und an jedem Qubit eine Hadamard-Transformation angewendet wird:

$$\begin{aligned} (H \otimes H \otimes \dots \otimes H)(|0\rangle|0\rangle\dots|0\rangle) &= \bigotimes_{i=1}^n H|0\rangle = \frac{1}{\sqrt{2}^n}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)\dots(|0\rangle + |1\rangle) = \\ &= \frac{1}{\sqrt{2}^n}(|00\dots00\rangle + |00\dots01\rangle + \dots + |11\dots10\rangle + |11\dots11\rangle) \end{aligned}$$

Im letzten Schritt wurde lediglich ausmultipliziert und die Ergebnisse in einzelnen ket-Vektoren zusammengefasst, wodurch ersichtlich wird, dass es sich tatsächlich um eine Superposition aller klassischen Bitkombinationen handelt.

Deutsch-Algorithmus

Mithilfe des *Deutsch-Algorithmus*, benannt nach *David Deutsch*, lässt sich ein leicht verständliches Beispiel für einen Quantenalgorithmus geben, das auch erste Vorteile eines Quantencomputers erahnen lässt:

Motivieren kann man das Beispiel dabei anhand einer Analogie, wie sie in [14, S.33] beschrieben wird: Betrachtet wird eine Münze, von der in Erfahrung gebracht werden soll, ob sie echt (Kopf und Zahl) oder gefälscht (zweimal Kopf oder zweimal Zahl) ist. Bei einer klassischen Münze müsste man die Münze zweimal prüfen, also beide Seiten betrachten, um ein Ergebnis hierfür zu bekommen.

Hinsichtlich des nun folgenden Beispiels kann man dies in mathematischer Weise wie folgt formulieren: Man kodiert die Vorderseite mit dem Wert 0 und die Hinterseite mit dem Wert 1. Die Betrachtung einer beliebigen Seite spielt die Rolle einer Funktion, die den Wert 0 bei dem Ergebnis „Kopf“ und den Wert 1 bei dem Ergebnis „Zahl“ ausgibt. Das Betrachten der Münze ist somit eine Funktion $f : \{0, 1\} \rightarrow \{0, 1\}$. Möchte man nun wissen, ob es sich um eine echte oder falsche Münze handelt, muss die Funktion zweimal aufgerufen werden ($f(0)$ und $f(1)$ müssen ermittelt werden); liefern beide Aufrufe dasselbe Ergebnis, handelt es sich um eine falsche Münze, andernfalls ist sie echt.

Es gilt nun also, über die Funktion f herauszufinden, ob sie *konstant* (beide Funktionsaufrufe liefern gleichen Wert, $f(0) = f(1)$) oder *balanciert* (beide Funktionsaufrufe liefern verschiedene Werte, $f(0) \neq f(1)$) ist. Es wird also angenommen, dass eine solche Funktion gegeben ist, über die eine bestimmte Eigenschaft in Erfahrung zu bringen ist; die Funktion wird dabei oft als *Black Box*, oder wie im Folgenden, als *Orakel* bezeichnet (siehe [14, S.33]).

Wird das Orakel nun in einen Quantenschaltkreis integriert, lässt sich dies wie in Abbildung 17 mithilfe einer unitären Transformation U_f darstellen. Der erste Ausgang dient zunächst zur Speicherung der Eingabe x , während der Funktionswert $f(x)$ dieser Eingabe am zweiten Ausgang binär zu y addiert wird. Das zweite Qubit dient damit der Ausgabe des Ergebnisses der Funktion. Es gilt nun, die oben erwähnte Eigenschaft über $f(x)$ bzw. U_f in Erfahrung zu bringen.

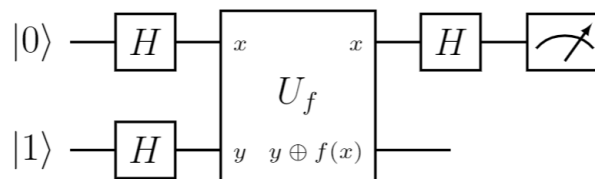


Abbildung 17: Schaltkreis des Deutsch-Algorithmus

Im Schaltkreis wird zunächst durch Hadamard-Gatter der Zustand $|\Phi_1\rangle := (H \otimes H)|0\rangle|1\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$ erzeugt, erneut lässt sich dies als Superposition aller möglichen Bitkombinationen deuten, an denen das Orakel nun in einem einzigen Durchlauf angewendet wird. Die unitäre Operation U_f bewirkt die Zuordnung $|x, y\rangle \mapsto |x, y \oplus f(x)\rangle$, damit ergibt sich:

$$\begin{aligned}
U_f |\Phi_1\rangle &= U_f \left[\frac{1}{2} (|00\rangle - |01\rangle + |10\rangle - |11\rangle) \right] = \\
&= \frac{1}{2} (|0\rangle |0 \oplus f(0)\rangle - |0\rangle |1 \oplus f(0)\rangle + |1\rangle |0 \oplus f(1)\rangle - |1\rangle |1 \oplus f(1)\rangle) = \\
&= \frac{1}{2} [|0\rangle (|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle) + |1\rangle (|0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle)] =: |\Phi_2\rangle
\end{aligned}$$

Um nun eine aufwendige Fallunterscheidung in vier Fälle bei der letzten Hadamard-Transformation für die einzelnen Möglichkeiten der Funktionswerte $f(x)$ zu vermeiden, soll die letzte Formulierung des Zustands $|\Phi_2\rangle$ betrachtet werden: In beiden Summanden kommt der Ausdruck $(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle)$ mit $x \in \{0, 1\}$ vor. Dieser wird nun wie folgt umformuliert, wobei man sich von der Äquivalenz durch Einsetzen überzeugen kann:

$$|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle = (-1)^{f(x)} (|0\rangle - |1\rangle) \quad (3.2)$$

Damit lässt sich der Zustand $|\Phi_2\rangle$ folgendermaßen schreiben:

$$\begin{aligned}
|\Phi_2\rangle &= \frac{1}{2} (|0\rangle (-1)^{f(0)} (|0\rangle - |1\rangle) + |1\rangle (-1)^{f(1)} (|0\rangle - |1\rangle)) = \\
&= \frac{1}{2} [(-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle] (|0\rangle - |1\rangle)
\end{aligned}$$

Interessant ist hier, dass der Funktionswert nun in der Beschreibung des ersten Register-Qubits zu finden ist. Das Umdeuten der Auswirkung der Funktion, welche eigentlich das zweite Register-Qubit „umschreibt“, auf den Zustand des ersten Qubits in Form eines eventuellen Vorzeichenwechsels wird dabei im Allgemeinen *Kick-back* genannt und in vielen Quantenalgorithmen angewendet (vgl [6, S.192]).

Nun kann nach zwei Fällen unterschieden werden:

- *$f(x)$ ist konstant:* Dann gilt $f(0) = f(1)$ und damit $|\Phi_2\rangle = (-1)^{f(0)} \frac{1}{2} (|0\rangle + |1\rangle) (|0\rangle - |1\rangle)$, wobei der Faktor $(-1)^{f(0)}$ einer globalen Phase entspricht und deswegen im weiteren Verlauf keine Bedeutung hat. Damit lässt sich allerdings der Gesamtzustand als $|\Phi_2\rangle = |+\rangle |-\rangle$ beschreiben, und die Hadamard-Transformation bringt

$$|\Phi_3\rangle = (H \otimes \mathbb{1}) |+\rangle |-\rangle = |0\rangle |-\rangle$$

- *$f(x)$ ist balanciert:* Dann gilt $f(0) \neq f(1) \Rightarrow (-1)^{f(1)} = -(-1)^{f(0)}$ und damit $|\Phi_2\rangle = (-1)^{f(0)} \frac{1}{2} (|0\rangle - |1\rangle) (|0\rangle - |1\rangle)$, wobei wiederum der Faktor $(-1)^{f(0)}$ entfallen kann. Der

Gesamtzustand ist damit $|\Phi_2\rangle = |-\rangle|-\rangle$, und die Hadamard-Transformation ergibt

$$|\Phi_3\rangle = (H \otimes \mathbb{1}) |-\rangle|-\rangle = |1\rangle|-\rangle$$

Damit liegt je nach Art der Funktion am Ende entweder der Zustand $|0\rangle|-\rangle$ oder $|1\rangle|-\rangle$ vor, und durch die Formulierung mithilfe des Kick-back muss lediglich das erste Register-Qubit gemessen werden um herauszufinden, ob es sich um eine konstante oder balancierte Funktion handelt.

Zusammengefasst gilt also: Dank der Superposition aller Bitzustände war nur ein Orakelaufruf notwendig, um die gefragte Eigenschaft mittels einer einzelnen abschließenden Messung zu ermitteln, während ein klassischer Computer zwei Aufrufe benötigt hätte. Hierin lässt sich erahnen, dass die Ermittlung *globaler Eigenschaften* einer Funktion bzw. eines Orakels zu den besonderen Stärken eines Quantenalgorithmus gehören. Die konkreten Stärken und Anwendungsgebiete sollen in Kapitel 3.4 näher besprochen werden.

Deutsch-Jozsa-Algorithmus

Das Deutsch-Problem kann als Spezialfall des *Deutsch-Jozsa-Problems* gesehen werden, welches ähnlich formuliert werden kann: Untersucht wird eine Funktion $f : \{0,1\}^n \rightarrow \{0,1\}$, von der bekannt ist, dass sie entweder konstant (alle möglichen Eingaben werden auf denselben Wert abgebildet) oder balanciert (die Hälfte der möglichen Eingaben wird auf den Funktionswert 0, die andere Hälfte auf den Wert 1 abgebildet) ist. Wieder soll in einem Orakelaufruf und mit anschließender Messung entschieden werden, welche Eigenschaft die Funktion hat.

Die konkrete Ausführung ist beispielsweise in [14, S.62-65] zu finden, an dieser Stelle soll lediglich durch Abb. 18 veranschaulicht werden, dass das Grundprinzip beim Vorgang gleich bleibt und eine Ähnlichkeit zum Schaltkreis des Deutsch-Algorithmus vorliegt.

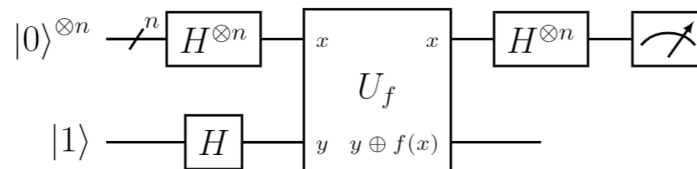


Abbildung 18: Schaltkreis des Deutsch-Jozsa-Algorithmus

3.4 Shor und Grover

Um zu analysieren und einzugrenzen, für welche Probleme ein Quantencomputer einem klassischen Computer überlegen ist, erfolgt häufig eine *Laufzeitanalyse*. Dabei wird konkret betrachtet, wie lange die Durchführung eines bestimmten Algorithmus im Durchschnitt (*average case*) oder im schlimmsten Fall (*worst case*) dauert.

Die Laufzeit hängt dabei von der Anzahl an Operationen ab, die man auf der Menge der Bits

oder Qubits durchführt, beispielsweise lässt sich dies durch die Anzahl an Single-Qubit-Gates und CNOT-Gates charakterisieren. Für einen gegebenen Algorithmus lässt sich dann die Laufzeit $t(n)$ mit der *Ordnung* $\mathcal{O}(f(n))$ ausdrücken, wobei n die *Eingabegröße* bezeichnet (also wieviele Bits/Qubits daran beteiligt sind), und die $\mathcal{O}$ -Notation angibt, wie schnell die Laufzeit mit steigender Eingabegröße wächst.

Man sagt, die Laufzeit „ $t(n) = \mathcal{O}(f(n))$ “, wenn $t(n)$ asymptotisch nicht schneller wächst als $f(n)$ “ [14, S.70]. Damit ist gemeint, dass es eine Konstante c und eine Schwelle n_0 gibt, sodass für alle $n \geq n_0$: $t(n) \leq c \cdot f(n)$ gilt. In Worten sagt dies aus, dass ab dieser Schwelle die Laufzeit $t(n)$ stets unter $c \cdot f(n)$ verläuft und damit durch die Angabe von $f(n)$ eine Art obere Schranke angegeben werden kann. Ist die Anzahl der Schritte beispielsweise ein beliebiges quadratisches Polynom in n , wird eine Laufzeit mit $\mathcal{O}(n^2)$ angegeben, da man ein c angeben kann, sodass ab einer bestimmten Schwelle sicher $t(n) \leq c \cdot f(n)$ gilt und $t(n)$ asymptotisch nicht schneller wächst als n^2 . Es also geht darum, $f(n)$ zu charakterisieren, um das Verhalten der Laufzeit für steigende Eingabegrößen abschätzen zu können.

Im Folgenden wird ein Blick auf zwei Algorithmen geworfen, welche beispielhaft für die Vorteile eines Quantencomputers in konkreten Anwendungen sind. Die mathematischen Ausführungen werden dabei aufgrund des Umfangs nicht im Detail dargestellt, hierfür wird an entsprechenden Stellen auf die Literatur verwiesen.

Shor-Algorithmus

Bei der Verschlüsselung von Nachrichten kommt es darauf an, Nachrichten zunächst mit einem Schlüssel zu chiffrieren, und sie beim Empfänger wieder zu dechiffrieren. *Public Key Kryptographie* beschäftigt sich damit, für das Chiffrieren einen *Public Key* zu erzeugen und diesen damit öffentlich bereitzustellen, während der Empfänger in Besitz eines dazu passenden *Private Key* ist und diesen zum Dechiffrieren benutzt [14, S.194]. Ein solches Beispiel ist die *RSA-Kryptographie*, welche in zahlreichen Anwendungsgebieten zum Einsatz kommt.

Das Verfahren setzt also darauf, dass es leicht ist, Nachrichten mit Kenntnis des Public Key zu verschlüsseln, während die Entschlüsselung mit dem Private Key wesentlich schwieriger ist, da sich dieser nicht so leicht aus Ersterem Ermitteln lässt. Das Prinzip basiert dabei auf Primfaktorzerlegung: Es ist einfach, bei Kenntnis von zwei Primzahlen diese zu multiplizieren und das Ergebnis festzustellen. Es ist allerdings ungemein schwieriger, eine Zahl in ihre Primfaktoren zu zerlegen. Die konkrete Anwendung des RSA-Verfahrens gestaltet sich etwas umfangreicher, folgt im Kern jedoch diesem Gedankengang. Eine RSA-Verschlüsselung zu knacken erfordert daher hohen Rechenaufwand, die Vorgangsweise lässt sich allerdings unter Anwendung einiger Kenntnisse aus der Zahlentheorie auf ein einzelnes Problem reduzieren:

Eine Zahl n lässt sich faktorisieren, „wenn wir zu einer Zahl $a < n$ die Periode der Funktion $f(x) = a^x \bmod n$ bestimmen können“, wobei $\bmod n$ den *modulo* n , also den Rest bei Division durch n , bezeichnet [14, S.223].

Mit dem Auffinden der Periode einer Funktion ist damit allgemein gemeint, ein p zu finden,

für welches $f(x) = f(x + p)$ gilt. Für dieses Beispiel soll also eine Zahl p gefunden, für welche $a^x \bmod n = a^{(x+p)} \bmod n$ gilt, p wird dabei auch „Ordnung modulo n von a “ genannt (siehe [14, S.202]).

Eine detailliertere Ausführung über das Vorgehen bei der RSA-Verschlüsselung sowie die zahlen-theoretische Begründung für die Reduktion auf dieses Problem sind in [14, S.195-206] ausführlich dargestellt.

Insgesamt geht es also darum, die Periode einer Funktion zu finden, wobei an dieser Stelle schon angemerkt sein soll, dass es sich also (wie schon beim Deutsch-Algorithmus) um das Auffinden einer globalen Funktionseigenschaft handelt.

Der Shor-Algorithmus (1994 von *Peter Shor* veröffentlicht, siehe [18]), der dabei angewendet wird, ist in Abb. 19 dargestellt und soll im Folgenden überblicksmäßig diskutiert werden.

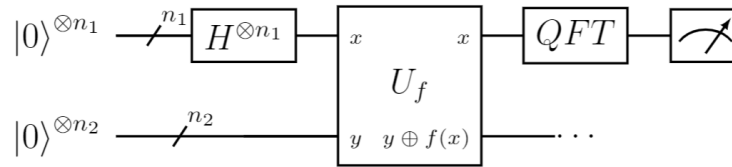


Abbildung 19: Shor-Algorithmus zum Auffinden der Periode einer Funktion

Der Algorithmus wurde im Jahr 2000 bereits erprobt und dadurch die Zahl 15 faktorisiert [19], weswegen diese Zahl (analog zu [14, S.225-227]) als demonstratives Beispiel dienen soll:

Damit gilt $n = 15$, a wird (zufällig) mit $a = 7$ gewählt, und es gilt, die Periode der Funktion $f(x) = 7^x \bmod 15$ zu finden.

Die konkrete Anwendung der Funktion erfolgt dabei wieder in Form einer unitären Operation, wobei das Qubit-Register hier (wie in Abb. 19 zu erkennen) in zwei Teile $|x\rangle|y\rangle$ geteilt wird, und durch das Orakel die Funktion $f : |x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$ durchgeführt wird. Die Bezeichnungen x und y können dabei das binäre Register oder die entsprechende Dezimalzahl repräsentieren, in letzterer Schreibweise beginnt der Algorithmus also mit dem Zustand $|0\rangle|0\rangle$.

Wie schon zuvor wird im ersten Teilregister durch die Anwendung der Hadamard-Transformation erneut eine Superposition der möglichen Bitkombinationen erzeugt, im vorliegenden Fall genügt es beispielsweise, hierfür $n_1 = 4$ Qubits vorzusehen, womit nach der Transformation der Zustand

$$|\Phi_1\rangle = \frac{1}{4}(|0\rangle|0\rangle + |1\rangle|0\rangle + \dots + |15\rangle|0\rangle)$$

vorliegt. Der Zustand des zweiten Teilregisters, der hier ebenso mit $n_2 = 4$ Qubits beschrieben werden soll, wird also nach wie vor mit $|0\rangle$ beschrieben, wozu aber nun durch Anwendung des Orakels der Funktionswert aus dem jeweiligen Zustand des ersten Registers addiert wird:

$$|\Phi_2\rangle = U_f |\Phi_1\rangle = \sum_{i=0}^{2^k-1} \frac{1}{4} |i\rangle |f(i)\rangle = \quad (3.3)$$

$$= \frac{1}{4} (|0\rangle |0\rangle + |1\rangle |7\rangle + |2\rangle |4\rangle + |3\rangle |13\rangle + |4\rangle |0\rangle + |5\rangle |7\rangle + \dots + |15\rangle |13\rangle) \quad (3.4)$$

An dieser Formulierung ist in diesem Beispiel bereits mit freiem Auge ersichtlich, dass in jedem vierten ket-Vektor der gleiche Funktionswert auftaucht und damit die Periode $p = 4$ ist.

Man beachte zudem, dass es sich hier um einen *verschränkten* Zustand handelt, da dieser nicht in Form eines Produktzustands formuliert werden kann. Für die weitere Vorgangsweise soll der Zustand aus Gl. 3.3 in folgende Form gebracht werden (analog zu [14, S.226]):

$$\begin{aligned} |\Phi_2\rangle = \frac{1}{4} [& (|0\rangle + |4\rangle + |8\rangle + |12\rangle) |1\rangle + (|1\rangle + |5\rangle + |9\rangle + |13\rangle) |7\rangle + \\ & + (|2\rangle + |6\rangle + |10\rangle + |14\rangle) |4\rangle + (|3\rangle + |7\rangle + |11\rangle + |15\rangle) |13\rangle] \end{aligned}$$

Für die folgende gedankliche Ausführung soll zunächst angenommen werden, dass (entgegen der Darstellung in Abb. 19) eine Messung am zweiten Teilregister erfolgt. Der Vorteil dieser Darstellung liegt darin, dass erkennbar wird, welche Zustände nach einer Messung des zweiten Teilregisters möglich wären. Für eine solche Messung gäbe es also vier Messergebnisse $\in \{1, 4, 7, 13\}$, und je nach Messergebnis würde sich der Zustand des ersten Teilregisters auf eine Superposition von vier Zuständen reduzieren, man nutzt hierbei also die Verschränkung des Zustands aus. Für die weitere Behandlung soll vorerst angenommen werden, dass im zweiten Register nun gemessen und der Zustand $|4\rangle$ festgestellt wurde, damit reduziert sich jener des ersten Teilregisters zu

$$|\Phi_3\rangle = \frac{1}{2} (|2\rangle + |6\rangle + |10\rangle + |14\rangle),$$

wobei damit das zweite Teilregister nun weggelassen wird. Auch an diesen Zuständen ist (in diesem Beispiel) die Periode grundsätzlich schon ablesbar, und könnte man immer nach dem Orakelaufruf garantieren, dass nach einer solchen Messung stets *dieser* Zustand $|\Phi_3\rangle$ vorliegt, könnte man durch mehrmaligen Durchlauf dieses Prozederes und wiederholten Messungen im nun vorliegenden Teilregister die Periode feststellen, da die Messergebnisse nur in der Menge $\in \{2, 6, 10, 14\}$ liegen, woraus man die Periode entnehmen könnte. Da aber diese erste Teilmessung selbst ein Zufallsergebnis ist, liegt nach dieser nicht immer der obige Zustand vor und eine Messung an dieser Stelle würde keinen Vorteil bringen. An diesem Punkt kommt die *Quantenfouriertransformation* ins Spiel, die in Abb. 19 mit QFT gekennzeichnet wird.

Die Quantenfouriertransformation würde für sich genommen ein ganzes Kapitel beanspruchen, für eine genaue Wirkungsweise wird auf [14, S.214-218] verwiesen. Für dieses Beispiel soll nur die Wirkung der QFT auf den vorliegenden Zustand gezeigt werden:

$$QFT \left[\frac{1}{2}(|2\rangle + |6\rangle + |10\rangle + |14\rangle) \right] = \frac{1}{2}(|0\rangle - |4\rangle + |8\rangle - |12\rangle)$$

Die QFT bringt dabei für dieses Beispiel *alle* möglichen Zustände $|\Phi_3\rangle$ auf eine Form $\frac{1}{2}(|0\rangle + \alpha|4\rangle + \beta|8\rangle + \gamma|12\rangle)$ mit $|\alpha|^2 = |\beta|^2 = |\gamma|^2 = 1$, somit wird durch die QFT stets eine Superposition der Zustände $|0\rangle, |4\rangle, |8\rangle, |12\rangle$ erzeugt, und dafür ist auch keine zuvorgehende Messung am zweiten Teilregister notwendig. Setzt man im letzten Schritt nun am ersten Teilregister eine Messung an und wiederholt den ganzen Vorgang einige Male, werden lediglich Messergebnisse aus $\{0, 4, 8, 12\}$ auftreten, woran man nun endgültig die Periode ablesen kann. Erst durch Anwendung der QFT kann also eine aussagekräftige Messung erfolgen, die einen Schluss auf die Periode der Funktion zulässt.

Zuletzt soll noch erwähnt werden, dass die Bestimmung der Periode auf diese Weise nicht *immer* zur Lösung des Problems der Faktorisierung führen muss. Tatsächlich hängt dies von der Wahl von a ab, welche hier recht willkürlich mit $a = 7$ festgelegt wurde. Es gibt im Allgemeinen auch Möglichkeiten für die Wahl von a , die zu keinem zufriedenstellenden Ergebnis führen. Dies stellt allerdings kein großes Problem dar, da das Ergebnis einer Faktorisierung recht einfach durch Multiplikation kontrolliert werden kann; ist das Ergebnis nicht das gewünschte, wird der Algorithmus durch andere Wahl von a und damit Veränderung des Orakels erneut durchgeführt, bis das Ergebnis nachweislich das Problem löst.

Fasst man alle notwendigen Schritte und Operationen zusammen, ergibt sich für den Shor-Algorithmus eine Laufzeit von $\mathcal{O}((\log n)^3)$. Die Laufzeit verhält sich also *polynomial* in $\log n$ (in diesem Fall ein Polynom dritten Grades). Die Überlegenheit dieses Algorithmus im Vergleich zu klassischen Algorithmen wird im Zuge der *Komplexitätsklassen* noch kurz diskutiert.

Grover-Algorithmus

Ein zweites bedeutendes Anwendungsgebiet für Quantenalgorithmen stellen *Suchalgorithmen* und damit verbunden *Optimierungsprobleme*, welche als Suche nach einer optimalen Lösung aufgefasst werden können, dar. Ein hierfür oft verwendetes Beispiel ist die Suche nach einer Person in einem Telefonbuch, wenn die Telefonnummer bekannt ist. Dank alphabetischer Ordnung fällt die Suche nach einer Nummer bei bekanntem Namen in der Regel kurz aus, die umgekehrte Suche erfordert allerdings wesentlich mehr Aufwand und im schlimmsten Fall müssen hierfür alle Einträge der Datenbank durchsucht werden. Das vorliegende Problem lässt sich mithilfe des Grover-Algorithmus (1996 von *Lov Grover* veröffentlicht, siehe [20]) äußerst effizient lösen, der zugehörige Schaltkreis bzw. ein Ausschnitt dessen ist in Abb. 20 zu erkennen. Der umrahmte Teil wird *Grover-Iteration* genannt (siehe [14, S.143]) und dabei mehrfach durchgeführt.

Die Notwendigkeit einer mehrfachen Durchführung der Grover-Iteration soll durch Analyse des Schaltkreises verdeutlicht werden:

Wie zuvor wird zunächst eine Superposition über alle N möglichen Zustände $|0\rangle, |1\rangle, \dots, |N-1\rangle$ der n Qubits durch die Hadamard-Transformation gebildet, unter all diesen Zuständen befindet

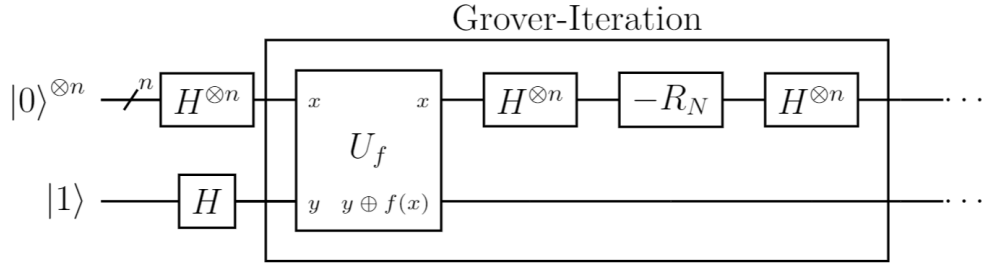


Abbildung 20: Grover-Algorithmus zur Datenbanksuche - der umrahmte Teil wird mehrmals ausgeführt, bevor die Messung (hier nicht dargestellt) erfolgt

sich nun ein einzelner, der das gewünschte Ergebnis darstellt. Dieser Zustand soll nun durch die Grover-Iteration „herausgefiltert“ werden. Würde man an dieser Stelle eine Messung vorsehen, würde jede Bitkombination mit gleicher Wahrscheinlichkeit als Messergebnis auftreten. Ziel der Grover-Iteration ist es, die Amplitude desjenigen Zustands, der das Suchergebnis darstellt, so sehr zu vergrößern, dass eine Messung mit sehr hoher Wahrscheinlichkeit dieses eine Ergebnis hervorbringt.

Zur Anwendung des Orakels wird zudem ein zusätzliches Qubit im Zustand $|1\rangle$ zur „Funktionsausgabe“ benutzt, auf welches die Hadamard-Transformation in Form von $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ wirkt. Durch das Orakel wird dann die Zuordnung $f : |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$ vorgenommen, wobei $f(x)$ nur für den gesuchten Eintrag den Wert 1, in allen anderen Fällen den Wert 0 liefert. Dafür lässt sich nun erneut, wie bereits beim Deutsch-Algorithmus, der *Kick-back* nutzen und der Zustand nach dem Orakel kann durch

$$|\Phi_1\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} (-1)^{f(x)} |x\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

beschrieben werden (siehe [14, S.141]). Diese Schreibweise verdeutlicht den Effekt des Orakels auf den Eingangszustand: Nur die Amplitude des gesuchten Ergebnisses bekommt ein negatives Vorzeichen, während die restlichen Amplituden erhalten bleiben. Dieser Vorgang ist der erste von zwei Schritten der Grover-Iteration, welcher in Abb. 21 mit U_f gekennzeichnet ist. In dieser Übersicht ist eine Auswahl der Amplituden der Zustände $|i\rangle \in \{|0\rangle, \dots, |N-1\rangle\}$, deren Superposition den Gesamtzustand $|x\rangle$ ergibt, ersichtlich, wobei der gesuchte Zustand mit $|j\rangle$ bezeichnet wird.

Der zweite Schritt der Iteration ist in Abb. 21 mit dem Schritt D_N zu erkennen: in der mittleren Grafik, die den Ausgangszustand für diesen Schritt darstellt, ist eine horizontale strichlierte Linie eingezeichnet, diese repräsentiert den Mittelwert der Amplituden zu diesem Zeitpunkt. Durch die Durchführung der Operation werden nun sämtliche Amplituden um ebendiesen Mittelwert gespiegelt. An der Abbildung wird dabei der Effekt dessen sichtbar: Der Mittelwert ist knapp unter dem Niveau der Amplituden jener Zustände, die nicht durch das Orakel gekippt wurden,

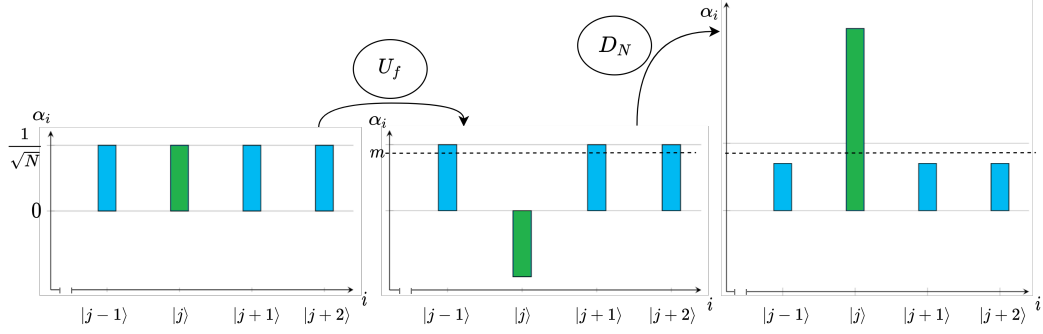


Abbildung 21: Wirkung der Grover-Iteration auf Amplituden

somit werden all diese Amplituden „nach unten korrigiert“. Die Amplitude des gesuchten Zustands befindet sich als einzige unter diesem Niveau, somit wird diese über das Niveau der anderen Amplituden erhöht.

Der Operation D_N kann man sich konkret folgendermaßen annähern: Die einzelnen Amplituden α_i werden abgebildet auf $2 \cdot m - \alpha_i$, wobei m den Mittelwert der Amplituden darstellt (siehe [14, S.142]). Damit soll eine Zuordnung

$$\alpha_i |i\rangle \mapsto \left(2 \cdot \sum_{j=0}^{N-1} \frac{\alpha_j}{N} - \alpha_i\right) |i\rangle$$

erfolgen. Dies kann besonders anschaulich nachvollzogen werden, wenn man D in Form einer Matrix angibt:

$$D_N = \begin{bmatrix} \frac{2}{N} - 1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} - 1 & \ddots & \frac{2}{N} \\ \vdots & \ddots & \ddots & \vdots \\ \frac{2}{N} & \cdots & \frac{2}{N} & \frac{2}{N} - 1 \end{bmatrix}$$

Diese Matrix kann dabei folgendermaßen zerlegt werden, wobei $H^{\otimes n}$ die Anwendung der Hadamard-Transformation auf die n Qubits, die für die Darstellung der $N = 2^n - 1$ Zahlen benötigt werden, kennzeichnet [14, S.144]:

$$D_N = -H^{\otimes n} R_N H^{\otimes n} \quad \text{mit} \quad R_N = \begin{bmatrix} -1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 \end{bmatrix} \quad (3.5)$$

Damit ergibt sich durch Ausführung des zweiten Schrittes die gesamte Grover-Iteration durch

$$|\Phi_2\rangle = D_N U_f |\Phi_1\rangle = H^{\otimes n} (-R_N) H^{\otimes n} U_f \left[|x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right]$$

Wird nach einmaliger Anwendung gemessen, wird somit mit erhöhter Wahrscheinlichkeit das gesuchte Ergebnis gemessen. Um diese Wahrscheinlichkeit zu erhöhen, kann die Grover-Iterationen mehrere Male durchgeführt werden.

Die Grover-Iteration kann dabei auch geometrisch durch das Drehen eines Vektors um eine entsprechende Achse und in Richtung eines gewünschten Vektors interpretiert werden (vgl. [14, S.146-153]). Dadurch kann beispielsweise verdeutlicht werden, dass bei zu oftmaliger Anwendung der Vektor „überdreht“ werden kann, wodurch sich die Wahrscheinlichkeit, das gewünschte Ergebnis zu messen, wieder verringert. Es kann allerdings eine optimale Anzahl $G(N)$ Iterationen angegeben werden, welche zudem für eine Laufzeitanalyse wesentlich ist (siehe [14, S.145]).

Insgesamt kommt der Groveraufruf damit mit $\mathcal{O}(\sqrt{N})$ Orakelaufrufen aus, das „entspricht einer quadratischen Beschleunigung gegenüber der klassischen Datenbanksuche im mittleren Fall“ [14, S.153], womit der Gebrauch von Quantencomputern für dieses Problem einen erheblichen Vorteil bringt.

Komplexitätsklassen

Bei der Behandlung von Algorithmen werden die zugehörigen Probleme in *Komplexitätsklassen* eingeteilt: Ein Problem gehört der Klasse P an, wenn sich das Problem in *polynomieller Laufzeit* lösen lässt, die Laufzeit also mit $\mathcal{O}(n^k)$ für konstantes k angegeben werden kann. Man sagt, das Problem lässt sich *effizient* lösen (vgl. [14, S.74]).

Die Klasse der Probleme, die sich *effizient verifizieren* lassen, gehören der Klasse NP an. Hierzu gehört z.B. die Frage, ob eine Zahl eine Primzahl ist, oder ob sie aus mehreren Zahlen zusammengesetzt ist: Das Herausfinden gestaltet sich zwar mitunter schwierig, aber die Überprüfung, ob zwei Zahlen zusammengesetzt die fragliche Zahl ergeben, fällt leicht. Mögliche Lösungen lassen sich also in Polynomialzeit verifizieren (vgl. [14, S.104]).

Ob $P=NP$ gilt, also ob jedes effizient verifizierbare Problem auch prinzipiell effizient lösbar ist, ist Inhalt gegenwärtiger Diskussionen und gilt zum Zeitpunkt des Schreibens vorliegender Arbeit als nicht beantwortet.

Von besonderem Interesse ist zudem die Klasse der *NP-vollständigen Probleme*, hierunter kann man die „am schwersten lösbaren“ Probleme aus der Klasse NP verorten. Die Angabe eines effizienten Algorithmus für eines dieser Probleme würde nämlich bedeuten, dass auch der Rest der Klasse NP effizient lösbar wäre. Ein Beispiel für ein NP-vollständiges Problem stellt das *Problem des Handlungsreisenden* (*Travelling Salesman Problem*, *TSP*) dar, welches z.B. nach dem minimalen Weg fragt, um n vorgegebene Orte je einmal zu besuchen und am Ende wieder am Ausgangsort anzugelangen. Im Prinzip gibt es bei n Städten $(n-1) \cdot (n-2) \cdot \dots \cdot 2 \cdot 1 = (n-1)!$ mögliche Rundreisen, die Laufzeit kann also mit $\mathcal{O}(n^n)$ angegeben werden.

Für Quantencomputer wäre es daher von Interesse, Algorithmen zu finden, die NP-vollständige Probleme effizient lösen können. Das TSP gilt als Optimierungsproblem, bei dem also die optimale Lösung gesucht werden soll. Wie schon zuvor erwähnt, kann der Grover-Algorithmus die Suche einem Element oder einer Lösung quadratisch beschleunigen. Da n in der Laufzeit eines klassischen Algorithmus aber im Exponenten aufzufinden ist, lässt sich das Problem mit dem Grover-Algorithmus nicht effizient lösen (siehe [14, S.166]).

Um eine effiziente Lösung des TSP zu erreichen, wäre damit eine *exponentielle Beschleunigung* notwendig. Eine solche Beschleunigung im Vergleich zu klassischen Algorithmen ist beispielsweise durch den Shor-Algorithmus zur Auffindung der Periode einer Funktion möglich, wodurch prinzipiell die Frage aufgeworfen werden könnte, ob eine solche Beschleunigung nicht auch für einen Suchalgorithmus erreicht werden könnte. Tatsächlich lässt sich jedoch zeigen, dass der Grover-Algorithmus von *optimaler Größenordnung* ist, das heißt, dass jeder Quantenalgorithmus mindestens $= \mathcal{O}(\sqrt{n})$ Orakelaufufe benötigen würde (siehe [14, S.161-166]).

Im Allgemeinen kann eine exponentielle Beschleunigung zwar durch Quantenalgorithmen erreicht werden, dies ist aber nur für Probleme möglich, welche die Bestimmung einer Funktionseigenschaft beinhalten: Man weiß also z.B., dass die Funktion eine bestimmte (globale) Eigenschaft hat (z.B. *konstant* oder *balanciert* (Deutsch-Algorithmus), Periodizität (Shor-Algorithmus)), und stellt die Frage nach einer Konkretisierung dieser Eigenschaft (vgl. [10, S.243]).

Jene Probleme, die durch Quantenalgorithmen effizient gelöst werden können, werden mit der Klasse *BPQ* beschrieben; eine Verortung dieser in Relation zu anderen Klassen ist ebenso ein offenes Problem (siehe [14, S.166-167]).

Für eine allgemeine detaillierte Behandlung der Komplexitätsklassen wird auf [14, S.101-125] verwiesen.

3.5 Quantum Hardware

Nachdem die theoretischen Grundlagen für die Realisierung eines Quantencomputers bereits thematisiert und auch relevante Algorithmen dargestellt wurden, soll sich dieses Kapitel der konkreten Machbarkeit und durchgeführten Experimenten widmen.

Allgemeine Kriterien zur Realisierung

In [14, S.254] werden vier Kriterien angegeben, die ein System erfüllen muss, um Quantenalgorithmen durchführen zu können und damit als Quantencomputer Verwendung zu finden:

„Ein Quantencomputer besteht aus einer Reihe von Quantenbits,

- die in einen Anfangszustand versetzt werden können,
- die Information robust speichern,
- auf die (universelle) Quantengatter anwendbar sind und
- die gemessen werden können. “

Der zweite Punkt birgt die Probleme der *Dekohärenz* in sich, auf die Möglichkeiten zur Modellierung dieser wird in Kapitel 3.6 noch weiter eingegangen.

Die Möglichkeiten, unitäre Transformationen (und darunter insbesondere die Ausführung von Single-Qubit-Gates und CNOT-Gate) auszuführen, sind ebenso vom jeweiligen physikalischen System abhängig. Gemäß der Schrödingergleichung kann eine unitäre Transformation (wie in Kapitel 2.2 beschrieben) durch den *Zeitentwicklungsoperator* $U = e^{-\frac{i}{\hbar}\hat{H}t}$ erfolgen, damit ist eine unitäre Entwicklung also prinzipiell durch Einflussnahme auf den Hamiltonian $\hat{H}$ steuerbar.

Im folgenden soll eine kurze Aufzählung von drei Realisierungsmöglichkeiten eines Quantencomputers dargestellt werden, die Diskussion erfolgt dabei hauptsächlich qualitativ, um einen groben Überblick zu geben. Hier gilt anzumerken, dass diese Liste keineswegs vollständig ist und viele Möglichkeiten zum Bau eines Quantencomputers denkbar sind. Vielmehr soll gezeigt werden, wie vielfältig die Zugänge hierzu sind.

Beispiel I: Photonen

Photonen lassen sich nicht nur in Form ihrer Polarisierung, sondern auch in Form von *räumlichen Moden* als Qubits verwenden, darunter kann man sich beispielsweise zwei verschiedene Wege in einem *Mach-Zehnder-Interferometer* vorstellen [10, S.287-288]. Die notwendigen Bauteile, um die einzelnen Gates zu realisieren, sind:

- *Phase shifter*: Hiermit wird lediglich eine relative Phase an einer räumlichen Mode hinzugefügt, wobei ausgenutzt wird, dass Licht in einem Medium langsamer propagiert. Damit kann die Wirkung durch $P|0\rangle = |0\rangle$ und $P|1\rangle = e^{i\Phi}|1\rangle$ beschrieben werden, was einem R_Φ -Gate (und damit einer Rotation des Blochvektors um die Z-Achse in der Blochkugel) entspricht. [10, S.290].
- *Beam splitter*: Dieser entspricht der Wirkung nach einer Rotation des Blochvektors um die y-Achse in der Blochkugel [10, S.292], und nach Gl.3.1 lässt sich aus Rotationen um z- und y-Achse jede beliebige unitäre Operation an einem einzelnen Qubit zusammenstellen. Damit gilt: Durch die Anwendung von Phase Shifter und Beam Splitter lassen sich beliebige Single-Qubit-Gates realisieren.
- *nichtlineares Medium*: Der *Kerr-Effekt* beschreibt die Abhängigkeit der Brechzahl eines nichtlinearen Mediums von der Gesamtintensität des einfallenden Lichts durch $n(I) = n + n_2 I$, beispielsweise treten solche Effekte in sehr schwacher Ausprägung bereits in Glas oder Zuckerwasser auf [10, S.290].

Makroskopisch beschrieben würde das bedeuten: Würden nun beispielsweise zwei räumlich getrennte Lichtstrahlen das Medium durchqueren, hängt die Brechzahl für einen Strahl nicht nur von der „eigenen“ Intensität, sondern auch von der des zweiten Lichtstrahls ab. Quantenmechanisch bedeutet dies, dass durch ein *Kerr-Medium* eine Kopplung zwischen Photonen hergestellt werden kann, was für die Ausführung von beispielsweise CNOT-Gates

notwendig ist. Konkret kann ein CNOT-Gate in Kombination mit einem Beam Splitter vorgesehen werden (siehe [10, S.294]).

Mit diesen drei Bauteilen lässt sich somit eine beliebige unitäre Entwicklung realisieren, zudem stellt die Erzeugung und Messung einzelner Photonen kein großes Hindernis dar. Dennoch lässt sich für diese Ausführung als Nachteil nennen, dass der Effekt verfügbarer nichtlinearer Kerr-Medien sehr schwach ist, und zudem der Absorptionskoeffizient in Relation viel zu hoch ist, um eine praktikable Anwendung zu gewährleisten [10, S.296].

Beispiel II: Ionenfalle

Ein weiteres Beispiel dafür, Qubits zu realisieren, bieten die zwei niedrigsten Energieniveaus eines Atoms bei Betrachtung der Hyperfeinstruktur, welche aus der Kopplung von Kernspin und Spin des Elektrons resultiert.

Die Kontrolle und Messung dieser beiden Energieniveaus fällt üblicherweise äußerst schwer, da die Energiedifferenz in der Regel viel kleiner ausfällt als z.B. allein die kinetische Energie der Atome bei Raumtemperatur ausmacht. Indem man Atome allerdings isoliert und entsprechend kühlt, werden diese Zustände zur Nutzung in Form von Qubits zugänglich (vgl. [10, S.309]).

Eine Präparation von Atomen kann dabei in Form von Ionen in einer *Ionenfalle* erfolgen, wobei diese in einer Reihe angeordnet werden und durch die Wechselwirkung mit Elektroden in Position gehalten werden. Eine solche Anordnung ist schematisch in Abb. 22 dargestellt.

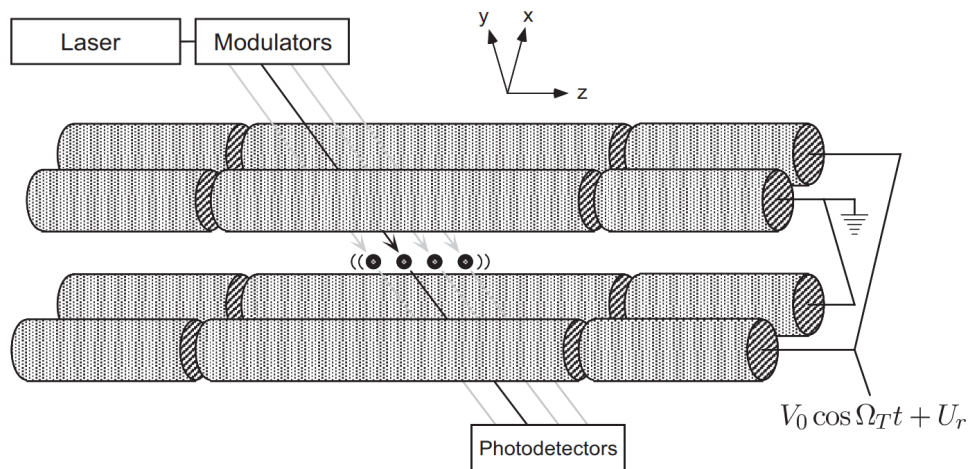


Abbildung 22: Schema einer Ionenfalle mit vier Ionen. Das Potential der Elektroden ist oszillierend, um die Ionen in Position zu halten; die Messung erfolgt durch Laser und Photodetektoren (Quelle: [10, S.311])

Qubits können dabei nicht nur durch die Spin-abhängigen Energiezustände realisiert werden, eine weitere Möglichkeit besteht zudem in der *Schwingungsmode* der gesamten Kette, dies lässt sich mit dem Zustand eines *Phonons* beschreiben. Hierdurch lassen sich beispielsweise schon durch ein

einzelnes Ion zwei Qubits realisieren.

Die anfängliche Präparation erfolgt dabei durch Laserkühlung, wodurch der Schwingungs- und hyperfeine Grundzustand hergestellt wird. Die Single-Qubit-Gates werden durch Laserpulse an den einzelnen Qubits durchgeführt, die Kopplung verschiedener Qubits (und damit in weiterer Folge die Ausführung eines CNOT-Gates) geschieht über die Schwingungsmode, welche ebenfalls über Laser angeregt wird. [10, S.324]). Die Behandlung erfolgt dadurch über weite Teile mithilfe von Laserpulsen, durch Anpassung der Frequenz lässt sich die Wechselwirkung und damit die unitäre Transformation kontrollieren, zudem erfolgt auch die Messung durch Anregung mittels Laser: Die eventuelle Aussendung von Photonen bei einem Übergang in den Grundzustand wird dann entsprechend von Photodetektoren registriert und als Zustand $|0\rangle$ gedeutet, das Ausbleiben einer Detektion entspricht dem Zustand $|1\rangle$.

Vorteile bietet dieser Zugang zudem in der einfachen Skalierbarkeit; so ist es besonders einfach, die Anzahl der Qubits zu erhöhen, indem zusätzliche Qubits der Länge nach aufgereiht werden und die Kette damit verlängert wird. Nachteile dieser Realisierung stellen beispielweise die fehlende Langlebigkeit der Phonon-Zustände und die vergleichsweise aufwendige Präparation des Grundzustands dar (vgl. [14, S.324]).

Beispiel III: Supraleitung

Eine weitere Möglichkeit, Qubits zu realisieren, besteht in Form von supraleitenden Ringleitern. Nach der *BCS-Theorie* binden sich bei tiefen Temperaturen je zwei Elektronen in einem Leiter unter einer Phonon-Wechselwirkung zu *Cooper-Paaren* [10, S.344]. In einem Kreis „bilden alle Cooper-Paare eine kohärente – quasi gemeinsame – Wellenfunktion aus. Das heißt, sie verhalten sich wie ein Teilchen, es gibt keine gegenseitigen Beeinflussungen“ [14, S.270].

In einem Ringleiter lassen sich dann *Josephson-Kontakte* vorsehen, welche durch Trennung von zwei Supraleitern mithilfe eines dünnen Isolators realisiert werden können; diese stellen damit für Cooper-Paare ein Hindernis dar, das allerdings durchtunnelt werden kann [14, S.270].

Mit diesem Ansatz sind grundsätzlich verschiedene Realisierungen eines Qubits möglich, beispielsweise kann die Richtung des Ringstroms (in und gegen Uhrzeigersinn) als solches realisiert werden (*Flux-Qubit*). Ebenso kann eine elektrostatische Variante gedacht werden, bei dem die beiden Zustände durch An- oder Abwesenheit in einer *Insel* im Ringleiter realisiert werden; das Qubit wird *charge-qubit* oder *Cooper-pair box* genannt [21]. Zu sehen ist eine solche Anordnung in Abb. 23, der Josephson-Kontakt ist mit der Kapazität C_j gekennzeichnet, der die beiden Supraleiter S trennt. Die Insel, die für die Charakterisierung der Qubit-Zustände relevant ist, ist mit einer strichlierten Linie umrahmt.

Die Einflussnahme und Realisierung der Single-Qubit-Gates geschieht durch die Kapazität C_g und die Regulierung der Spannung U . Eine Kopplung verschiedener Qubits kann durch gegenseitige Anbindung mittels weiterer Josephson-Kontakte, welche durch externe Magnetfelder reguliert werden können, vorgesehen werden, eine Messung kann durch Feststellen der elektrischen Ladung in der Insel realisiert werden [10, S.344].

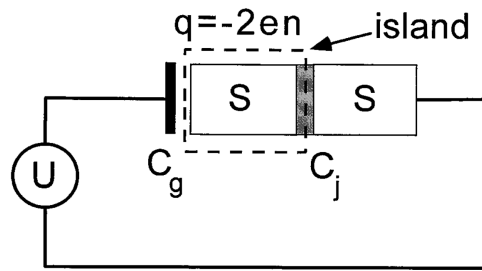


Abbildung 23: Schema einer Cooper-Box (Quelle: [21, S.165])

Besonders hervorzuheben ist die Langlebigkeit und robuste Repräsentation der Qubit-Zustände [10, S.344], zudem ist ein solcher Quantencomputer leicht skalierbar durch entsprechende Anordnung auf einer Platine [14, S.271].

Aktuelle Errungenschaften

Zur Einordnung des Entwicklungsstands in jenem Zeitraum, in dem vorliegende Arbeit verfasst wurde, sollen zwei Ansätze geschildert werden, welche zuvor bereits breite Aufmerksamkeit erfahren haben:

Googles Demonstration eines *Quantenvorteils* (*quantum advantage*) im Oktober 2019 durch Arute et al. [1] erfuhr auch außerhalb der Fachwelt viel Beachtung. Mit *Transmon*-Qubits, welche als eine robustere Variante von Charge-Qubits verstanden werden können, erfolgten Berechnungen in einem Zeitraum von etwa 200 Sekunden, für welche ein moderner Supercomputer nach eigenen Angaben 10 000 Jahre benötigen würde. Kritik bezüglich der Überlegenheit gegenüber klassischen Computern kam jedoch kurz darauf seitens *IBM*, wonach ein klassischer Algorithmus lediglich 2,5 Tage benötigen würde [22].

Hierzu wurden 53 Qubits verwendet, womit Berechnungen in einem 2^{53} -dimensionalen Hilbert-Raum durchgeführt werden konnten. Die Qubits wurden in einem zweidimensionalen Array angeordnet, wie in Abb. 24 dargestellt. Ursprünglich war die Verwendung von 54 Qubits angedacht, eines davon erwies sich jedoch als nicht funktionsfähig (in der Abbildung als weißes Kreuz zu erkennen).

Konkret wurden mit dieser Anordnung, dem *Sycamore-Prozessor*, Zufallszahlen erzeugt, indem zufällige Quantenschaltkreise ausgeführt wurden. Ein Beispiel für den Ausschnitt eines solchen zufälligen Schaltkreises ist in Abb. 25 zu sehen. Zur Beschreibung der tatsächlich durchgeführten Kopplungen von Qubits wird hier angemerkt:

„One can compose, for example, controlled-NOT (CNOT) gates from 1-qubit gates and two of the unique 2-qubit gates of any given pair. The implementation of high-fidelity ‘textbook gates’ natively, such as CZ or iSWAP, is work in progress“ [1, S.507].

Die Verteilung der damit erzeugten Zufallszahlen konnte aufgrund der langen Berechnungsdauern

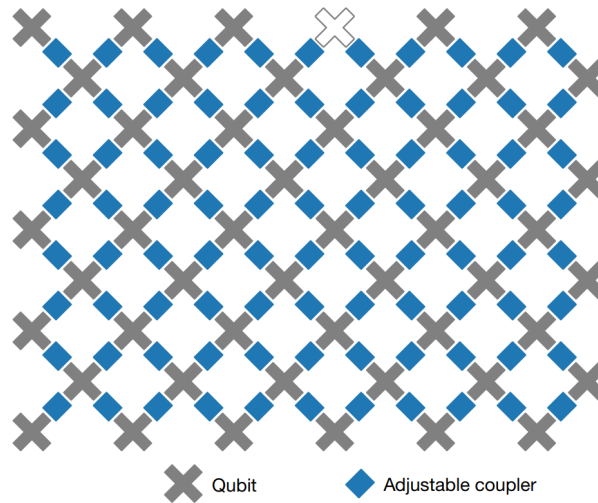


Abbildung 24: Array der 54 Qubits (in Form von Kreuzen) und deren Kopplungen (Quelle: [1, S.506])

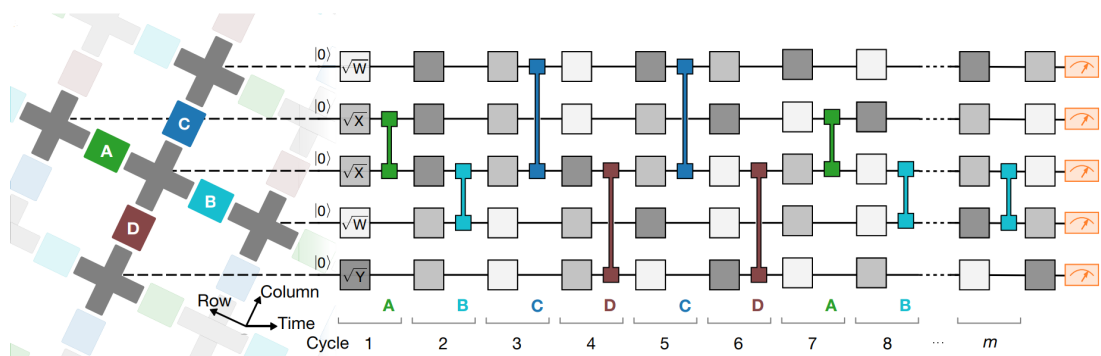


Abbildung 25: Ausschnitt eines zufälligen Quantenschaltkreises mit fünf Qubits (Quelle: [1, S.508])

mit klassischen Computern nicht simuliert werden, die Güte lässt sich dennoch durch eine globale Betrachtung der Verteilung und entsprechenden Näherungen beurteilen (siehe *cross-entropy-benchmarking*, siehe [1, S.506]). Für die zukünftigen Aussichten werden fehlertolerante Systeme angesprochen, die eine Ausführung von Shor- und Grover-Algorithmus möglich machen sollen; langfristig sollen dadurch Anwendungen für Optimierungsprobleme, in Materialwissenschaften und im Machine Learning möglich werden.

Einen fundamental anderen Zugang haben Zhong et al. (siehe [2]) im Dezember 2020 gewählt, und um diesen nachvollziehen zu können, soll zunächst das dabei relevante *Boson-sampling* dargelegt werden:

Möchte man beispielsweise mehrere *Fermionen* mit einer Wellenfunktion beschreiben, ist für

die mathematische Betrachtung mitsamt der gegenseitigen Wechselwirkungen die sogenannte *Slater-Determinante* notwendig. Das bosonische Analogon zur Beschreibung des Zusammenspiels mehrerer *Bosonen* ist die *Permanente* einer Matrix. Die Permanente ist ein Polynom in den Einträgen der Matrix und der Determinante einer Matrix sehr ähnlich. Während man bei letzterer allerdings einen Vorzeichenwechsel bei einzelnen Summanden berücksichtigt, fällt dieser bei der Permanente weg. Eine Permanente zu berechnen stellt im Allgemeinen ein äußerst aufwendiges Problem dar, das mit diesem Zugang gelöst werden soll.

Die Entwicklung mehrerer Photonen in Form einer unitären Transformation kann durch eine Matrix beschrieben werden. Schickt man nun mehrere Photonen durch einen Quantenschaltkreis (in Form mehrerer Beam Splitter und Spiegel), der damit eine entsprechende Matrixdarstellung besitzt, und betrachtet man das Ergebnis durch Messung am Ende der Prozedur, kann man umgekehrt auf die dabei relevante Permanente schließen. Das Boson-Sampling-Problem wird in diesem Ansatz also direkt mithilfe von Photonen und Rückschluss auf eine Permanente, deren Berechnung mit klassischen Algorithmen zu aufwendig wäre, bearbeitet.

Während der Prozess in diesem Fall 200 Sekunden dauerte, würde eine entsprechende klassische Berechnung mit dem chinesischen Supercomputer *TaihuLight* nach eigenen Angaben 2.5 Milliarden Jahre dauern (siehe [2, S.4]).

Während hierdurch ein beeindruckender Quantenvorteil erreicht wurde, ist allerdings anzumerken, dass diese Herangehensweise keinen Ansatz für einen universellen Quantencomputer darstellt. Zwar ist eine Anwendung in kombinatorischen Problemen und damit verbundenen Anwendungen in Graphentheorie und Machine Learning denkbar, beliebige Quantenalgorithmen lassen sich hierdurch allerdings nicht ausführen.

3.6 Quantenkanäle und Dekohärenz

Nachdem in Kapitel 2.8 bereits ein einfaches Beispiel zur Dekohärenz geschildert wurde, soll nun eine etwas allgemeinere Beschreibung, wie sie in der Quanteninformationstheorie üblich ist, nachfolgen.

Offene Systeme und Quantenkanäle

Systeme, die für die Realisierung eines Quantencomputers in Frage kommen, müssen „beeinflussbar“ sein, um bestimmte unitäre Operationen und somit Berechnungen damit zu tätigen. Gleichzeitig stellt diese fehlende Abgeschlossenheit eines Systems eine Herausforderung dar, wenn es darum geht, nur jene Operationen darauf wirken zu lassen, die tatsächlich beabsichtigt sind. Die Beschreibung offener Systeme kann dabei durch *Quantenkanäle* erfolgen, die das System nicht unverändert lassen, sondern je nach Wechselwirkung mit der Umgebung einen Einfluss auf dieses haben. Um das Prinzip dahinter zu veranschaulichen, soll folgendes Beispiel betrachtet werden:

Ein beliebiger Zustand

$$\rho = \begin{bmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{bmatrix} = \rho_{00} |0\rangle \langle 0| + \rho_{01} |0\rangle \langle 1| + \rho_{10} |1\rangle \langle 0| + \rho_{11} |1\rangle \langle 1|$$

soll als Kontroll-Qubit für ein CNOT-Gate verwendet werden, der Zustand $|0\rangle$ soll das Ziel-Qubit darstellen. Nach dem CNOT-Gate soll das Ziel-Qubit allerdings nicht weiter betrachtet werden, nur der Zustand des Kontroll-Qubits soll beschrieben werden. Die Darstellung dieses Vorgangs ist in Abb. 26 (links) mit einer verkürzten Darstellung (rechts) zu sehen. Hierdurch wurde ein *Kanal* modelliert, dessen Ergebnis mit $C[\rho]$ beschrieben wird.

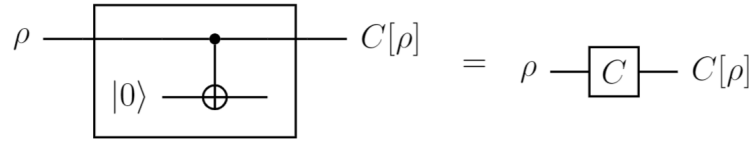


Abbildung 26: Modellierung eines Quantenkanals mittels CNOT-Gatter

Der Zustand vor Anwendung des CNOT-Gates kann damit durch $\rho \otimes |0\rangle \langle 0|$ beschrieben werden, die Wirkung dessen mit $U = |0\rangle \langle 0| \otimes \mathbb{1} + |1\rangle \langle 1| \otimes \sigma_x$ (siehe Kapitel 3.2) erfolgt dann durch

$$\begin{aligned} U(\rho \otimes |0\rangle \langle 0|)U^\dagger &= \rho_{00}U(|0\rangle \langle 0| \otimes |0\rangle \langle 0|)U^\dagger + \rho_{01}U(|0\rangle \langle 1| \otimes |0\rangle \langle 0|)U^\dagger + \\ &\quad + \rho_{10}U(|1\rangle \langle 0| \otimes |0\rangle \langle 0|)U^\dagger + \rho_{11}U(|1\rangle \langle 1| \otimes |0\rangle \langle 0|)U^\dagger \\ &= \rho_{00} |0\rangle \langle 0| \otimes |0\rangle \langle 0| + \rho_{01} |0\rangle \langle 1| \otimes |0\rangle \langle 1| + \rho_{10} |1\rangle \langle 0| \otimes |1\rangle \langle 0| + \rho_{11} |1\rangle \langle 1| \otimes |1\rangle \langle 1| \end{aligned}$$

Durch Ausspuren des zweiten Systems ergibt sich dann der Endzustand:

$$C[\rho] = \text{Tr}_2[U(\rho \otimes |0\rangle \langle 0|)U^\dagger] = \rho_{00} |0\rangle \langle 0| + \rho_{11} |1\rangle \langle 1| = \begin{bmatrix} \rho_{00} & 0 \\ 0 & \rho_{11} \end{bmatrix} \quad (3.6)$$

Damit entspricht dieses Ergebnis für $0 < \rho_{00} < 1$ einem gemischten Zustand, während der ursprüngliche Zustand ρ beliebig (und demnach möglicherweise rein) war. $C[\rho]$ lässt sich zudem der Form nach mit Gl. 2.11 vergleichen, womit sich eine erste Verbindung zur Dekohärenz feststellen lässt.

Das Beispiel soll verdeutlichen, dass die Entwicklung des Zustands ρ zu $C[\rho]$ nicht als unitäre Operation auf diesem alleinigen System aufgefasst werden kann. Dessen kann man sich überzeugen, indem man die Eigenwerte der beiden Zustände vergleicht: während $C[\rho]$ die Eigenwerte ρ_{00}, ρ_{11} besitzt, ist dies für ρ im Allgemeinen nicht der Fall. Da unitäre Transformationen die Eigenwerte allerdings nicht verändern, gibt es keine unitäre Operation U , mit der sich $C[\rho]$ als Ergebnis von $U\rho U^\dagger$ deuten lässt.

Vielmehr kann man die Entwicklung in Quantenkanälen als unitäre Operationen deuten, die auf

einem umfassenderen System wirken. Der Zustand $C[\rho]$ lässt sich dann durch Ausspuren gewinnen, damit lässt sich eine allgemeinere Formulierung für die Entwicklung in einem Quantenkanal mit $|\omega\rangle^B$ als „Umgebungszustand“ angeben:

$$C[\rho^A] = \text{Tr}_B[U(\rho^A \otimes |\omega\rangle\langle\omega|^B)U^\dagger] \quad (3.7)$$

Die Wirkung auf den Zustand ρ lässt sich allerdings in kompakterer Form mithilfe der *Kraus-Operatoren* K_i angeben: Jeder Quantenkanal lässt sich mithilfe dieser Operatoren durch

$$C[\rho^A] = \sum_i K_i \rho^A K_i^\dagger \quad (3.8)$$

mit $\sum_i K_i^\dagger K_i = \mathbb{1}$ beschreiben (vgl. [6, S.239]).

Diese Entwicklung lässt sich damit als eine allgemeinere Dynamik von Zuständen begreifen, wonach für ein offenes System nicht nur unitäre Operationen auf diesem System, sondern auch welche auf einem umfassenderen System möglich sind, wobei sich die konkrete Entwicklung des reduzierten betrachteten Systems mithilfe der Kraus-Operatoren beschreiben lässt.

Eine ähnliche Verallgemeinerung lässt sich im Übrigen auch für Messungen denken: So lässt sich eine allgemeinere Form von Messungen (siehe Kapitel 2.3) denken, wenn man Messungen an einem umfassenderen System zulässt, welche dann auf das eigentlich betrachtete System eine andere Wirkung haben als projektive Messungen. Auch diese Wirkung kann dabei mit einem Satz von Operatoren beschrieben werden, diese Klasse von Messungen wird *POVM* (*positive operator valued measure*) genannt und enthält projektive Messungen als Spezialfall (siehe [6, S.222-234]).

Phasendämpfungskanal und Dekohärenz

Ein bedeutsames und gelegenes Beispiel ist der *Phasendämpfungskanal* (*phase damping channel*) [6, S.249], der mit den Kraus-Operatoren

$$\begin{aligned} K_i &= \sqrt{1-p}(|0\rangle\langle 0|^A + |1\rangle\langle 1|^A) \\ K_0 &= \sqrt{p}|0\rangle\langle 0|^A \\ K_1 &= \sqrt{p}|1\rangle\langle 1|^A \end{aligned}$$

und einem Parameter $0 \leq p \leq 1$ beschrieben wird. Damit ergibt sich für die Wirkung auf einen beliebigen Zustand $\rho = \begin{bmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{bmatrix}$ durch Anwendung der Kraus-Operatoren [6, S.250]:

$$C[\rho] = K_i \rho K_i^\dagger + K_0 \rho K_0^\dagger + K_1 \rho K_1^\dagger = \begin{bmatrix} \rho_{00} & (1-p)\rho_{01} \\ (1-p)\rho_{10} & \rho_{11} \end{bmatrix}$$

Wiederum für den Grenzfall von $p = 1$ würde dies das Ergebnis von Gl. 3.6 reproduzieren, dies lässt sich also als eine Verallgemeinerung des zuvor gezeigten Kanals auffassen.

Für einen reinen Zustand ρ lässt sich dies nun wie folgt interpretieren: „Der reine Zustand des Untersystems A geht in ein Gemisch über. Die Phasenbeziehung zwischen den Summanden des reinen Zustands und damit die Kohärenz, d. h. die Interferenzfähigkeit gehen verloren“ [6, S.251]. Hier kann erneut eine Verbindung zum Beispiel der Dekohärenz in Kapitel 2.8 gezogen werden: Die dort geschilderte Situation des Objekts A entspricht einem reinen Zustand mit den anfänglichen Diagonaleinträgen $\rho_{00} = \rho_{11} = \frac{1}{2}$ (und $\rho_{01}, \rho_{10} \neq 0!$), welcher in Folge des Streuprozesses mit einem Photon zu einem gemischten Zustand mit gleichen Diagonaleinträgen, aber verschwindenden Nebendiagonaleinträgen übergeht. Auch dieser Vorgang lässt sich als Spezialfall des Phasendämpfungskanal mit $p = 1$ auffassen, wobei p in diesem Fall nun als Wahrscheinlichkeit für einen Streuvorgang interpretiert werden kann. Dass es nämlich überhaupt zu einer sicheren Streuung kommt, wurde in Kapitel 2.8 von vornherein angenommen. Falls dies aber nicht sicher eintritt, lässt sich dies mit dem Phasendämpfungskanal beschreiben, das einführende Beispiel zur Dekohärenz kann also als Grenzfall dessen betrachtet werden.

Eine nützliche Darstellung hierfür kann anhand der Blochkugel erfolgen: Betrachtet man diese als Raum aller möglichen Zustände ρ , lässt sich der Zustandsraum des Ergebnisses darstellen, indem man $C[\rho]$ mithilfe der Blochzerlegung aus Gl.2.2 einen entsprechenden Blochvektor zuweist und die möglichen Ergebnisse visualisiert. Zu sehen ist das Ergebnis für den Phasendämpfungskanal in Abb. 27 für $p=0,3$.

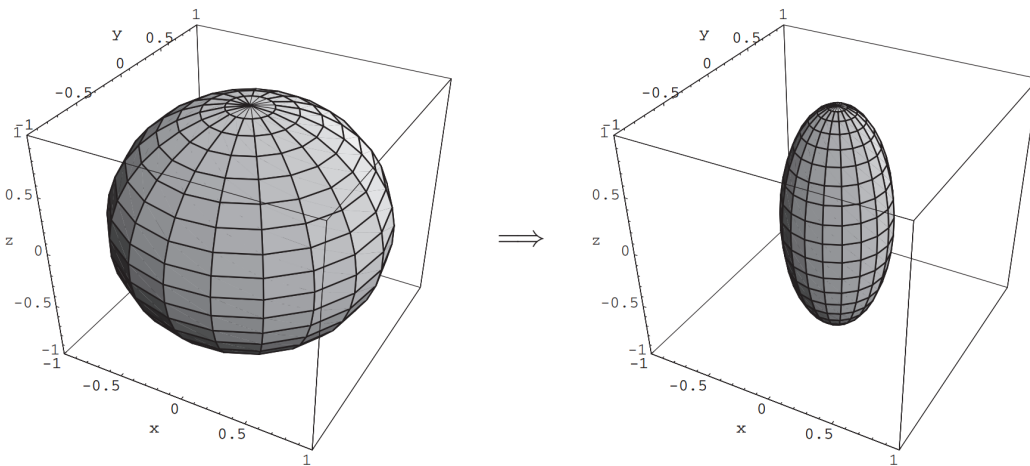


Abbildung 27: Auswirkung des Phasendämpfungskanal auf die Blochkugel für $p=0,3$ (Quelle: [10, S.377])

Für den Grenzfall von $p = 1$ ergibt sich damit visuell eine Reduzierung auf die z -Achse: Damit sind nur mehr die beiden Zustände $|0\rangle$ und $|1\rangle$ als Ergebnis möglich, was wiederum dem Vorgang der Dekohärenz entspricht.

Je nach Wechselwirkung mit der Umgebung gibt es allerdings weitere Kanäle mit unterschiedlichen Wirkungen auf die Blochkugel, im Allgemeinen wird dabei von *(Quantum) Noise*, also einem

Rauschen gesprochen, welches die Informationsverarbeitung stört. Zu erwähnen sind beispielsweise der *Depolarisierungskanal* (*depolarizing channel*) [10, S.378], oder der *Amplitudendämpfungskanal* (*amplitude damping channel*), welcher Energieverlust des Systems beschreiben kann [10, S.380]. Verglichen dazu beschreibt der Phasendämpfungskanal den Verlust von Information bei Energieerhaltung [10, S.383].

Was die Wirkung des Phasendämpfungskanals in Bezug zur Dekohärenz angeht, halten Nielsen & Chuang allerdings fest: „...phase damping has a unique role in the transition from quantum to classical physics; for certain environmental couplings, it occurs on a time scale which is much faster than any amplitude damping process, and can therefore be much more important in determining the loss of quantum coherence. The major point of these studies has been this emergence of classicality due to environmental interactions“ [10, S.398].

Quantenfehlerkorrektur

Fehler, die bei klassischen Computern passieren, lassen sich üblicherweise durch Messung oder Kopieren von Bits und entsprechende Vorkehrungen dafür wieder bereinigen. Da Qubits aber nicht kopiert werden können (vgl. 3.2) und auch nicht ohne weiteres gemessen werden können, ohne den Zustand dadurch zu verändern, müssen spezielle Strategien im Umgang mit Quantum Noise und daraus folgendem Verlust von Quanteninformation gefunden werden. Grundsätzlich bestehen diese Strategien darin, Quanteninformation in mehreren Qubits statt nur einem zu speichern, und durch geschickte Messungen von verschränkten Zuständen Fehler aufzuspüren oder wieder zu korrigieren (siehe [6, S.207]). Hierzu sollen zwei Beispiele genannt werden:

- Der *Bit-Flip-Fehler* (*bit flip error*) behandelt fälschliche Vertauschung der Zustände $|0\rangle$ und $|1\rangle$, also $|0\rangle \mapsto |1\rangle$ und $|1\rangle \mapsto |0\rangle$. Der Fehler lässt sich durch Kodierung mit *drei Qubits* aufspüren und korrigieren (siehe [6, S.207-208]).
- Der *Phase-Flip-Fehler* (*phase flip error*) betrifft eine Phasenänderung, also beispielsweise die fehlerhafte Zuordnung $|0\rangle \mapsto -|0\rangle$. Der Fehler kann durch Kodierung in *neun Qubits* und entsprechende Messungen aufgehoben werden (siehe [6, S.207-209]).

Hervorzuheben ist zudem der *Shor-Code*, der vor jedem beliebigen Fehler eines einzelnen Qubits schützt. Der Code ist eine Kombination von je drei Bit-Flip-Codes und Phase-Flip-Codes und wird beispielsweise in [10, S.432-434] dargestellt.

3.7 Zusammenfassung und Ausblick

Die Erkenntnisse auf dem Gebiet der Quanteninformationstheorie schreiten mit beachtlichem Tempo voran, die jüngsten Beispiele für das Erreichen eines Quantenvorteils wurden in Kapitel 3.5 geschildert. Der momentane Entwicklungsstand wird dabei geläufig als Beginn der *NISQ-era* bezeichnet, der Begriff ist eine Abkürzung für *Noisy Intermediate Scale Quantum technology* und wurde von John Preskill geprägt (siehe [23]).

Gemeint ist mit dieser Ära jene Phase, in denen Quantencomputer mit etwa 50 bis 100 Qubits (*Intermediate Scale*) Aufgaben erfüllen können, die klassische Algorithmen übertreffen. Die noch unkontrollierbaren und ungewünschten Effekte aus Wechselwirkungen mit der Umgebung (*Noisy*) stellen allerdings noch eine Herausforderung dar, weswegen die tatsächlichen Ausführungen von Quantenschaltkreisen noch limitiert sind. Die Beschreibung scheint dabei auch auf Googles *Sycamore*-Prozessor mit 53 Qubits zuzutreffen.

Im Allgemeinen fallen die Zugänge äußerst unterschiedlich aus; während Arute et. al. die Aussicht auf *universelle Quantencomputer* verfolgen, lassen sich mit Ausführungen wie von Zhong et al. bestimmte Aufgaben in beeindruckender Laufzeit erledigen. Was die zukünftige Entwicklung betrifft, sind letztere durchaus bedeutsam, da es oft einzelne Probleme sind, in denen Quantencomputer den entscheidenden Vorteil bringen können. So sind beispielsweise Hybridlösungen denkbar, in denen nur Teile eines Algorithmus von einem Quantencomputer ausgeführt werden, während andere Teile von klassischen Computern bewältigbar sind.

Mit voranschreitender Entwicklung treten auch immer mehr Anwendungsfelder in Erscheinung; anfangs von Feynman zur Simulation von quantenmechanischen Systemen ins Spiel gebracht, sind abseits von Materialwissenschaften und Anwendungen in Chemie auch rein mathematische Problemlösungen (wie die Permanente einer Matrix) und damit verbundene Probleme in das Anwendungsfeld gerückt, durch Grover- und Shor-Algorithmen sind zudem relevante informationstechnologische Anwendungen gegeben. Besonders im Bereich des *Machine Learning* zeigen sich dabei zunehmend Anwendungsgebiete aufgrund der äußerst aufwendigen Algorithmen, wodurch sich in Form von *Quantum Machine Learning (QML)* ein spannendes und modernes Anwendungsgebiet eröffnet.

Teil II

Didaktik

4 Allgemeine didaktische Aspekte

Die Inhalte der Quantenphysik umfassen eine Reihe an verschiedenen Phänomenen und Besonderheiten, weswegen eine Konkretisierung der Themenbereiche für den Schulunterricht mitunter schwer fallen kann. Die Vorgabe des österreichischen Lehrplans lässt hier viele Freiheiten, so wird der Unterricht zu Quantenphysik im 6. Semester der Oberstufe verortet, wobei eine Unterscheidung nach Anzahl der Wochenstunden fällt. Demnach gilt an Schulen mit bis zu sieben Wochenstunden Physik, die „Besonderheiten der Quantenwelt“ zu thematisieren und „Einblicke in die Theorieentwicklung und das Weltbild der modernen Physik“ zu ermöglichen. Für Schulen mit mehr als sieben Wochenstunden gibt es eine etwas genauere Vorgabe, hier werden konkret „Doppelspaltexperiment, Heisenberg’sche Unschärferelation [und] statistische Deutung“ [24] zusätzlich erwähnt.

Besonders in der Quantenphysik scheint es schwierig, den Unterricht auf einige wenige Themenbereiche zu fokussieren und damit zwangsweise andere Themen zu vernachlässigen. Im Zuge einer *Scientific Literacy* kann jedoch die Frage gestellt werden, welche Inhalte allen Schüler:innen in der Sekundarstufe II im Sinne einer wissenschaftlichen Grundbildung mitgegeben werden sollten. Besonders die Quantenphysik bringt durch ihren hohen Grad an Komplexität und die schwierig zu interpretierenden Ergebnisse viele Herausforderungen mit sich, das gesamte Thema ist damit sehr anfällig für Fehldeutungen und problematische Interpretationen.

So zählt beispielsweise Florian Freistetter in einem Blog-Beitrag in der Tageszeitung *der Standard* einige solcher Interpretationen und pseudowissenschaftlichen Argumente auf und meint dazu: „Aber gerade die enorme Komplexität und scheinbare Absurdität der Quantenmechanik hat sie zu einem idealen Spielplatz für Pseudowissenschaftler und Esoteriker aller Art gemacht“ [25]. Besonders die Verschränkung wird hier als ein Konzept erwähnt, das für fragwürdige Argumente mitunter auf makroskopische Objekte ausgeweitet und angewendet wird.

Zudem rücken Verschränkung und Quantencomputer auch durch diverse Berichterstattungen in der Tagespresse in den Fokus der Gesellschaft, eine Thematisierung moderner Konzepte der Quantentheorie und der Anwendungen und Grenzen dieser könnte also, mit entsprechenden Konzepten vermittelt, einen wichtigen Beitrag zu einer wissenschaftlichen Grundbildung leisten.

Im Folgenden soll eine allgemeine didaktische Analyse zum Thema Quantenphysik erfolgen, wofür zunächst klassische Lernendenvorstellungen beim Unterrichten von Quantenphysik diskutiert und berücksichtigt werden. Anschließend werden bewährte Konzepte aufgezählt und wesentliche Rahmenpunkte vorgestellt, darauf aufbauend soll eine Analyse der darin behandelten Inhalte dargestellt werden und ein internationaler Vergleich von Themenbereichen, die zur Quantenphysik unterrichtet werden, folgen. Zum Abschluss wird die Möglichkeit für einen alternativen Zugang zur Quantenphysik mittels Qubits näher beleuchtet und begründet. Dieses Kapitel stellt damit eine didaktische Aufbereitung des Themas dar, bevor in Kapitel 5 eine konkrete Unterrichtssequenz vorgestellt wird.

4.1 Lernendenvorstellungen

Bevor auf konkrete Konzepte eingegangen wird, soll eine Übersicht von Lernendenvorstellungen aus der Quantenphysik geboten werden.

Vorstellungen zum Atomaufbau

Vorstellungen von Atomen werden meist vom Bohr'schen Atommodell geleitet, dieses ist äußerst einprägsam und „die eindeutig dominante Schülervorstellung zu Atomen“ [26, S.211]. Dieses Bild von Elektronen auf Kreisbahnen entspricht nicht einer quantenmechanischen Beschreibung, bleibt aber selbst nach Thematisierung von anderen Modellen im Denken der Schüler:innen persistent (vgl. [26, S.212]).

Demnach werden im weiteren Verlauf Modelle wie die Vorstellung von verschmierten Ladungswolken um den Atomkern, das Schalenmodell oder das Orbitalmodell aufgenommen, diese koexistieren im weiteren Verlauf und fügen sich zu Mischvorstellungen vom Aufbau des Atoms (vgl. [26, S.212]). Eng mit dem Bohr'schen Atommodell ist demnach die Vorstellung von einem definierten Ort eines Elektrons verknüpft, die Wahrscheinlichkeitsaussagen aus der Quantenmechanik werden dementsprechend als Unkenntnis oder Schwierigkeit, den „wahren Ort“ wirklich zu messen, interpretiert (vgl. [26, S.213]).

Vorstellungen für Quantenobjekte

Für Quantenobjekte existieren verschiedene Vorstellungen, mit denen Schüler:innen arbeiten und die teilweise, je nach Fragestellung, bevorzugt Verwendung finden:

- *Quantenobjekte als Kügelchen:* Diese Vorstellung, welche einem Bild von Teilchen entspricht, wird besonders dadurch gefestigt, dass beispielsweise Elektronen häufig als Kügelchen oder Punkte skizziert werden. Diese gilt zwar als besonders anschaulich, bringt aber den Nachteil mit sich, dass Interferenzerscheinungen dadurch nicht zu Genüge erklärt werden können. So bemerken auch Kircher et al., dass viele Schüler:innen mit einer solchen Vorstellung von Elektronen in den Unterricht kommen, dies „sieht man z.B. auch daran, dass die Interferenzringe bei der Beugung an Graft für diese Schüler[:innen] überraschend sind“ [27, S.486].
- *Quantenobjekte als Wellen:* Die Vorstellung von Wellen erleichtert zwar das Erklären von Interferenzerscheinungen, bringt aber ihrerseits andere Probleme mit, wie etwa die Messung eines Ortes für einzelne Wellenpakete und den damit verbundenen Kollaps der Wellenfunktion; ebenso lässt sich nicht erklären, warum sich beispielsweise am Doppelspalt kein Interferenzmuster ergibt, wenn man den Durchgang am Spalt mit einer Messung des Ortes versieht.

Die beiden Vorstellungen miteinander in Einklang zu bringen, bereitet dabei viele Schwierigkeiten. Nach Kircher et al. ist an Hochschulen die Denkart „Beim Durchgang durch einen

Doppelspalt stellt man sich das Elektron als Welle vor, bei der Detektion am Schirm ist es wie ein kleines Kügelchen“ [27, S.486] weit verbreitet, lässt sich aber an Schulen nicht so leicht etablieren, da diese von einem konkreten mathematischen Formalismus begleitet werden kann, welcher den Schüler:innen nicht geläufig ist. Zur schwierigen Vereinbarkeit meinen auch Müller und Schecker in [26, S.216], dass Schüler:innen „die Teilchenvorstellung des Lichts bereitwillig akzeptieren. Die Wellenvorstellung wird nur bei intensivem Nachfragen reaktiviert,“ zudem wird auch der Versuch einer Vorstellung bei Elektronen im Atom angesprochen, dieser „führt bei einigen Schülerinnen und Schülern zur Vorstellung eines Elektrons, das auf einer Welle sitzt und mit ihr auf- und abschwingt.“

- *Quantenobjekte als verteiltes Stoffliches*: Gemäß dieser Vorstellung sind z.B. Elektronen nicht punktförmig, sondern *verschmiert*, die Dichte dieses Stoffes an einem Ort ist dabei proportional zur Wahrscheinlichkeit, das Elektron an diesem Ort zu aufzufinden (vgl. [27, S.488]). Problematisch bei dieser Vorstellung ist beispielsweise die Ortsmessung: Demnach müsste sich der Stoff bei einer Messung rasant auf einen Punkt zusammenziehen, wobei die Ladung in der Verteilung beschleunigt wird und ferner elektromagnetische Strahlung emittieren müsste (vgl.[27, S.489]).

Wahrscheinlichkeitsdeutung

Der Umgang mit der Wahrscheinlichkeit in der Quantenmechanik und die fundamentale Unterscheidung zur Wahrscheinlichkeit eines Würfelwurfs (und dessen prinzipiell deterministischer Beschreibung) fällt vielen Schüler:innen nicht leicht, oft wird diese dann als Unkenntnis der wahren Situation gedeutet. Eng damit verbunden ist zudem die Wahl der zugrunde liegenden Interpretation, also ob Aussagen auf ein *Ensemble* bezogen werden (*Ensemble-Interpretation*) oder diese Wahrscheinlichkeitsaussagen sich auf einzelne Quantenobjekte beziehen (wie in der *Kopenhagener Deutung*).

Müller und Schlecker erwähnen hierzu drei Kategorien, in denen Antworten und Haltungen von Schüler:innen verortet werden können (vgl. [26, S.215]):

- Wahrscheinlichkeit als Instrument, um Probleme kalkülhaft bearbeiten zu können
- Unzufriedenheit mit Erklärung durch Wahrscheinlichkeiten und Forderung nach kausaler Erklärung für Verteilungen
- Wahrscheinlichkeit als Ungenauigkeit

Zwar wird demnach die kalkülhafte Haltung durchaus von vielen Schüler:innen bevorzugt, jedoch zeigt sich bei manchen die Unzufriedenheit mit den Aussagen der Quantenmechanik: „Die mit dem Wahrscheinlichkeitsbegriff verbundene Vorstellung von Ungenauigkeit spiegelt in den Augen mancher Schülerinnen und Schüler die nach ihrer Ansicht unzureichenden Möglichkeiten zur Beschreibung von quantenphysikalischen Phänomenen wider“ [26, S.215].

Besonders zu letzterem Punkt ergibt sich zudem eine häufig anzutreffende Deutung der Unbestimmtheitsrelation als Unkenntnis, wie im folgenden Abschnitt dargelegt.

Unbestimmtheitsrelation

Dass Ort und Impuls nach der Heisenberg'schen Unbestimmtheitsrelation nur nicht genau gemessen werden können, ist eine häufig anzutreffende Vorstellung von einem wahren Wert zu Ort und Impuls und der Unfähigkeit, diese genau genug zu messen. Müller und Schlecker erwähnen hierzu: „Zur Fehlinterpretationen trägt auch die Bezeichnung ‚Heisenberg'sche Unschärferelation‘ bei, die man häufig antrifft und die so etwas wie einen ‚verschmierten Ort‘ eines Elektrons nahelegt“ [26, S.217].

Besonders betont werden hier die Schwierigkeiten bei der Deutung der Größen Δx und Δp , welche mitunter als *Ortsänderung*, *Abstand von wahren und gemessenem Wert*, *Maß für die Ungenauigkeit der Messung* etc. interpretiert werden (vgl. [26, S.218]). Für die Größen gibt es demnach viele Deutungen abseits einer Standardabweichung bei Messung eines Ensembles von gleich präparierten Quantenobjekten. Gerade letztere Deutung in Form einer Ensemble-Interpretation ist dabei jene, die sich weitläufig durchgesetzt hat und sich wie folgt ohne direkten Bezug auf einzelne Quantenobjekte formulieren lässt: „Die Aussage der Heisenberg'schen Unbestimmtheitsrelation ist dann, dass es nicht möglich ist, ein Ensemble von Quantenobjekten so zu präparieren, dass das Produkt von Δx und Δp_x den Wert $\frac{h}{4\pi}$ unterschreitet“ [26, S.218].

4.2 Konzepte für Unterricht zur Quantenphysik

Zunächst sollen einige gängige und erprobte Konzepte vorgestellt werden, um einen Überblick über momentane Zugänge und Motivationen zu bieten und basierend darauf zu analysieren, welche Gemeinsamkeiten und Unterschiede sich in der Menge an Konzeptionen zeigt.

Konzept nach Brachner und Fichtner

Das Konzept von Brachner und Fichtner [28] bildete in den 70er-Jahren den ersten ausgearbeiteten Kurs zur Quantenphysik und richtet sich in seinen Grundzügen nach den Vorlesungen von Feynman (vgl. [29]).

Inhaltlich wird eine große Fülle an Themengebieten abgedeckt, so wird mit Elektronen und Photonen am Doppelspalt begonnen, bei letzteren wird auch Photo- und Compton-Effekt sowie eine Bestimmung des Planck'schen Wirkungsquantums h angedacht. Nach einer Behandlung von Spin und Polarisation und der Energiequantisierung folgt eine allgemeine Betrachtung von Wahrscheinlichkeiten und Wahrscheinlichkeitsamplituden. Die Schrödingergleichung, Potentialtopf, Tunnel-Effekt und die Heisenberg'sche Unbestimmtheitsrelation schließen dabei den ersten Teil der Sequenz ab.

Die beiden letzten Teile des Kurses handeln von einer Ausweitung auf Atomphysik und Vielteilchensystemen.

Zentral ist in diesem Konzept, angelehnt an die Ausführungen von Feynman, das quantenmechanische Fundamentalprinzip:

„Gibt es verschiedene Möglichkeiten (Wege) für das Eintreten eines bestimmten Ereignisses und wird durch die Versuchsanordnung nicht festgelegt, dass ausschließlich eine bestimmte Möglichkeit gewählt wurde, so tritt immer Interferenz auf. Hinterlässt dagegen jedes Ereignis an der Versuchsanordnung eindeutig ein bestimmtes Merkmal, durch das entschieden werden kann, welche der verschiedenen Möglichkeiten gewählt wurde, dann tritt nie Interferenz auf.“ [29]

Das Berliner Konzept

Die „Einführung in die Quantenphysik“ von H. Fischler und M. Lichtfeldt [30] stützt sich in hohem Maße auf die gängigen Schwierigkeiten, die Schüler:innen im Umgang mit Quantenphysik haben und wurde speziell unter diesem Blickpunkt entwickelt. Die zentralen Punkte, die dabei berücksichtigt wurden, umfassen unter anderem [29]:

- „Die enge Verknüpfung von Photonen mit der Teilchenvorstellung “
- „Das Festhalten der Schülerinnen und Schüler am Bohr’schen Atommodell “
- „Die in den meisten Kursen unzureichende Darstellung der Welle-Teilchen-Problematik “

Charakteristisch für diesen an Lernendenvorstellungen orientierten Zugang ist, dass bestimmte problematische Vorstellungen durch Minderung von Rückgriffen auf klassische Begriffe vermieden werden sollen, sodass „quantenphysikalischen Phänomene von Anfang an durch die Brille der modernen Physik betrachtet werden“[30].

Inhaltlich gestaltet sich das Berliner Konzept wie folgt:

Zu Beginn wird, anders als in vielen Kursen üblich, bewusst nicht auf Photonen zurückgegriffen, um etwaige Deutungsschwierigkeiten mit dem „Welle-Teilchen-Dualismus“ zu vermeiden. Stattdessen wird mit einer eingehenden Behandlung von Experimenten mit Elektronen inklusive des Doppelspaltversuchs mit diesen begonnen. Dadurch wird eine alternative Beschreibung von Elektronen gefordert, welche zuvor nicht bereits mit einem „Wellencharakter“ gesehen wurden. In diesem Bild wird zudem auf die Kopenhagener Deutung verzichtet und auf die Ensemble-Interpretation zurückgegriffen.

Im weiteren Verlauf wird früh auf die Heisenberg’sche Unbestimmtheitsrelation zurückgegriffen, um dann auf die Energiequantelung im Atom überzugehen. Diese wird mit ein- und dreidimensionalem Potentialtopf behandelt, das Bohr’sche Atommodell wird dabei bewusst nicht thematisiert, um wiederum Bezüge zur klassischen Physik zu vermeiden.

Erst später sollen auch Photonen inklusive Photo- und Compton-Effekt behandelt werden, womit auf Parallelen und Unterschiede zum Verhalten von Elektronen zurückgegriffen werden kann. Deutungsfragen finden sich in dieser Konzeption erst am Ende, auf diese Weise können Schüler:innen auf bereits erlangtes Wissen im Zuge der vorangegangenen Behandlung zurückgreifen.

Durch diese inhaltliche Neuordnung der relevanten Themen, die sich auch in anderen Konzepten in unterschiedlicher Reihung finden, soll so ein Zugang geboten werden, der die angesprochenen Lernendenvorstellungen umgeht und entsprechende Deutungsschwierigkeiten vermeidet.

Konzepte mit Zeigerformalismus

Der *Zeigerformalismus* geht auf Richard P. Feynman zurück und wurde in seinem Buch *QED - Die seltsame Theorie des Lichts und der Materie* verwendet. Dazu beschrieb er anschaulich Phänomene der Quantenphysik durch Teilchen, die alle möglichen Bahnen „gleichzeitig“ gehen und sich diese Möglichkeiten dann überlagern. Möchte man sich z.B. im Zuge eines Doppelspaltversuchs unterschiedliche Bahnen zu einem bestimmten Punkt auf einem Schirm ansehen und herausfinden, was aus der Überlagerung der möglichen Wege resultiert, verwendet man für jede Bahn einen Zeiger, der mit fortschreitendem Weg rotiert und eine komplexe Amplitude repräsentiert. Die Amplituden verschiedener Wege lassen sich sodann (vektorartig) addieren, und aus dem Betragsquadrat dessen ergibt sich an unterschiedlichen Stellen am Schirm die Intensität der Verteilung.

Der Doppelspalt lässt sich mit dieser Möglichkeit wie folgt erklären: Kontrolliert man am Doppelspalt, welchen Weg ein Teilchen genommen hat, äußert sich dies im Formalismus dadurch, dass sich zwei Wahrscheinlichkeiten addieren, die aus zwei einzelnen resultierenden Zeigern gewonnen wurden. Erfolgt keine Kontrolle am Spalt, addiert man zunächst die Amplituden der beiden Wege und bildet erst dann den Betrag daraus; durch gegenseitiges Auslöschen der Amplituden entsteht dann die Möglichkeit, dass die Intensität an manchen Stellen verschwindet und so ein Interferenzmuster entsteht (siehe Fundamentalprinzip bei Brachner & Fichtner). Ein solches Vorgehen für drei verschiedene Punkte an einem Schirm inklusive einer grafischen Darstellung der Bildung des Amplitudenquadrats ist in Abb. 28 zu sehen. Das hier geschilderte Vorgehen ist dabei eine Vereinfachung der Bildung von *Pfadintegralen* (vgl. [31]).

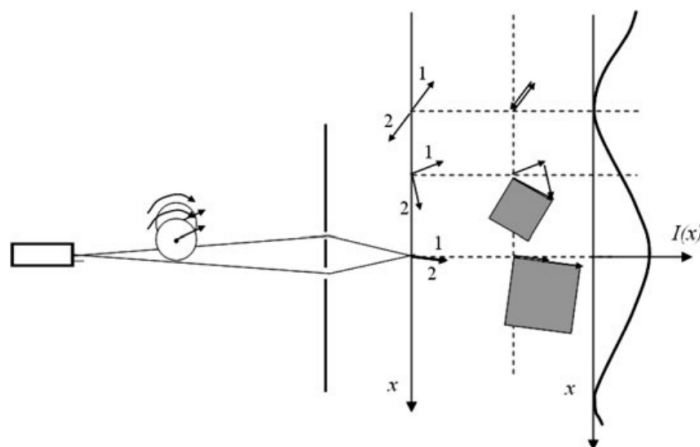


Abbildung 28: Zeigerformalismus für drei ausgewählte Punkt am Schirm (Quelle: [27, S.495])

Es gibt mehrere Konzepte, die sich auf diesen Formalismus berufen, zwei davon seien an dieser Stelle genannt:

- *Zeigerformalismus nach Küblbeck*: Es erfolgt zunächst der „traditionelle“ Weg über Doppelspaltexperimente mit Photonen und Elektronen sowie die Thematisierung der Unbestimmtheitsrelation, die ungenügsame Beschreibung durch Wellen und Teilchen wird als Anlass zur Modellbildung genommen, wodurch der Zeigerformalismus eingeführt und an bekannten Situationen erprobt wird (vgl. [32]).
- *Zeigerformalismus nach Bader*: Hier wird für die Anwendung des Zeigerformalismus mit Computern gearbeitet, das Modell wird bereits zu Beginn im Anschluss an die Wellenoptik eingeführt. Anschließend wird mit Photonen und Elektronen gearbeitet, Materiewellen und die Heisenberg'sche Unbestimmtheitsrelation werden thematisiert und zum Ende rücken die Energiequantisierung und -niveaus in den Fokus, wobei auch die Schrödingergleichung und Eigenwerte angesprochen werden. Besonders wichtig ist hier die Betonung darauf, dass die Zeiger nur ein Modell sind, das für die Berechnung von Wahrscheinlichkeiten zwar hilfreich ist, die Zeiger aber keine Entsprechung in der Wirklichkeit haben (vgl. [33]).

Das Münchener Unterrichtskonzept zur Quantenmechanik

Das von Rainer Müller entwickelte Konzept zur Einführung in die Quantenmechanik (vgl. [34]) nennt als Ziele unter anderem, dass insbesondere das Neue an der Quantenphysik thematisiert werden soll, da speziell die Grenzen des Vorstellbaren für viele Schüler:innen von Interesse sind; zudem sollen klare Begriffe zur Verfügung gestellt werden, die ein qualitatives Verständnis ermöglichen.

Hierzu gibt es einige Grundprinzipien, die sich durch die Anwendung des Konzepts ziehen:

- Das Herausstreichen der *Wahrscheinlichkeit* als durchgängiges Prinzip soll bereits von Anfang an etabliert und stets wieder aufgegriffen werden.
- Ein weiterer bedeutender Begriff ist jener der *Präparation*, hierzu wird im Allgemeinen auf die Ensemble-Interpretation zurückgegriffen.
- Dass Teilchen bestimmte Eigenschaften wie Ort, Impuls, Energie etc. nicht *haben*, sondern eine komplexere Beschreibung notwendig ist, soll sich ebenso durch die Behandlung ziehen.
- Der Vorgang des *Messens* soll als besonderes Ereignis herausgestellt werden, in diesem Sinne wird auch die Zustandsreduktion besprochen.

Zudem wird auf Schwierigkeiten im Verständnis der Quantenphysik Bezug genommen, besondere Beachtung erfahren demnach:

- Die Vorstellung von lokalisierten Elektronen, also Elektronen, die einen Ort *haben*, sowie eng damit verbunden die Vorstellung des Bohr'schen Atommodells, nach welcher sich diese Elektronen zudem auf bestimmten Bahnen bewegen.
- Selbst nach einiger Kenntnis in der Quantenphysik ist zudem die Vorstellung weit verbreitet, dass sich die Wahrscheinlichkeitsaussagen lediglich auf die Unkenntnis der Experimentator:innen bezieht, in Wahrheit Teilchen jedoch sehr wohl einen *wahren Ort* besitzen.
- Eng mit vorherigem Punkt verbunden ist eine fälschliche Deutung der Heisenberg'schen Unbestimmtheitsrelation als „Unschärfe der Messung“ und einer Deutung der Größen Δx , Δp als Ungenauigkeiten dieser.

Inhaltlich gliedert sich die Durchführung in zwei separate Teile, wobei der erste Teil einen qualitativen Basiskurs darstellt, während der zweite Teil einen quantitativen Aufbaukurs bildet.

Der erste Teil beginnt mit der Behandlung des Photoeffekts und geht dann zu optischen Instrumenten und der Eigenschaft der Polarisation über. Photonen bleiben dann Gegenstand des Interesses in Form eines Interferometers, anschließend wird der Doppelspaltversuch thematisiert. In all diesen Bereichen bleiben die oben genannten Prinzipien präsent.

Im Anschluss daran rücken Elektronen mit Beugung und Doppelspalt in den Fokus, daran anschließend wird besonderes Augenmerk auf den Messvorgang gerichtet. Der erste Teil wird dann durch eine ausgiebige Auseinandersetzung mit der Heisenberg'schen Unbestimmtheitsrelation abgeschlossen.

Der zweite Teil beinhaltet wesentlich mehr mathematische Ausführungen, so werden Operatoren, Eigenwertgleichungen und die Schrödingergleichung zum Thema gemacht, darauf folgt eine Behandlung von Atomen inklusive einer Erklärung der diskreten Spektren und ein konkretes Beispiel in Form des Wasserstoffatoms.

Insgesamt erfolgt damit eine äußerst inhaltsreiche Thematisierung der Quantenphysik mit zahlreichen Details und experimentellen Bezügen.

4.3 Kerninhalte der Quantenphysik

Vergleich der dargestellten Konzepte

Um die Inhalte, die im Quantenphysikunterricht vorkommen sollen, zu präzisieren, soll zunächst ein Überblick über Themen erfolgen, die in bekannten Konzepten bevorzugt behandelt werden. Dabei können folgende Beobachtungen gemacht werden:

- Der Doppelspaltversuch wird in allen Konzepten vorgesehen, zumeist wird er eher zu Beginn thematisiert und häufig wird er zuerst mit Photonen durchgeführt.

- Der Großteil der Konzepte setzt dabei allgemein die Behandlung von Photonen an den Anfang, teilweise wird mit dem Photoeffekt begonnen.
- Um zu zeigen, dass nicht nur Photonen Quanteneigenschaften besitzen, wird zumeist auf Elektronen zurückgegriffen, mit welchen Beugungs- und Doppelspaltversuche besprochen werden.
- In den meisten Vorschlägen wird auch die Heisenberg'sche Unbestimmtheitsrelation ausgiebig thematisiert, die Behandlung dieser erfolgt dabei oft nach den Betrachtungen von Photonen und Elektronen.
- Auch die Energieniveaus in Atomen und Spektralanalysen werden häufig behandelt, diese Themen erfolgen eher am Schluss einer Sequenz.
- Allgemein werden viele Themen entlang historischer Entwicklungen in der Physik des 20. Jahrhunderts gesetzt. Dies deckt sich mit dem zu Beginn angesprochenen Punkt im Lehrplan, welcher „Einblicke in die Theorieentwicklung und das Weltbild der modernen Physik“ vorsieht.

Inhaltlich gibt es damit grundsätzlich viele Überschneidungen, wenn es um Photonen, Elektronen, Unbestimmtheitsrelation und Energieniveaus geht. Die Reihenfolgen dieser unterscheiden sich je nach Zugang und dahinterliegender Intention.

Inhalte im internationalen Vergleich

In einer Analyse von Stadermann et al.[3] wurden Curricula aus 15 Ländern (inklusive Österreich) untersucht und dabei verglichen, welche Themen aus dem Bereich der Quantenphysik in der Sekundarstufe laut entsprechendem Curriculum vorgesehen sind.

Darin werden verschiedene Aspekte untersucht und Vergleiche gezogen, im Folgenden soll nur ein Teil der Ergebnisse dargestellt werden. Tabelle 4 enthält 17 Themenbereiche, denen die Inhalte aus den betrachteten Curricula zugeordnet wurden, kodiert mit Q1 bis Q17. Zu jedem Bereich wird dabei angegeben, in wievielen Ländern dieser im entsprechenden Curriculum erwähnt wird. Die ersten beiden genannten Zahlen befinden sich dabei in Klammern, da eine eindeutige Zuordnung zum Bereich Quantenphysik nicht im Curriculum gegeben war, der Inhalt jedoch in einem anderen Bereich oder Fach explizite Erwähnung fand (z.B. *Blackbody radiation* im Bereich *Astrophysik* oder *Bohr atomic model* im Fach *Chemie*, siehe [3, S.8]).

Wie auch in den bereits vorgestellten Konzepten finden sich Diskussion von Licht und Materie, Energieniveaus und Unbestimmtheitsrelation unter jenen mit den meisten Nennungen. Themen wie Tunnel-Effekt, Potentialtopf oder Schrödingergleichung finden sich zwar teilweise in den Konzepten, werden allerdings in Curricula selten erwähnt.

Tabelle 4: Häufigkeit der Themen in Curricula der 15 betrachteten Länder (Quelle: [3, S.11])

Content item mentioned in the curriculum document		Countries/15
Q1	Blackbody radiation	(9)
Q2	Bohr atomic model	(13)
Q3	Discrete energy levels (line spectra)	15
Q4	Interactions between light and matter	13
Q5	Wave-particle duality or complementarity	15
Q6	Matter waves, quantitative (de Broglie)	12
Q7	Technical applications	13
Q8	Heisenberg's uncertainty principle	9
Q9	Probabilistic or statistical predictions	8
Q10	Philosophical consequences or interpretations	5
Q11	One-dimensional model or potential well	3
Q12	Tunneling	4
Q13	Atomic orbital model	1
Q14	Exclusion principle or periodic table	2
Q15	Entanglement	2
Q16	Schrödinger equation	2
Q17	Calculations of detection probability	1

Auffällig ist zudem, dass die Verschränkung nur in zwei Ländern (in Norwegen und in Teilen Deutschlands) eine Erwähnung findet. Hierzu wird zudem folgendes erwähnt:

„Quantum entanglement has far-reaching philosophical consequences which [...] have the potential to motivate students. Many authors argue that understanding QP concepts could become much easier for students if we would introduce the concepts with entanglement experiments of two-level systems.“ [3]

Basierend auf diesen Nennungen wurde in der Studie ein *Core Quantum Curriculum* definiert, welches in Abb. 29 dargestellt ist und die Themenbereiche Q3 bis Q9 umfasst, während Bereiche mit weniger Nennungen, wie in diesem Beispiel Q10 bis Q12, dieses ergänzen können und zu einem *Extended Quantum Curriculum* erweitern.

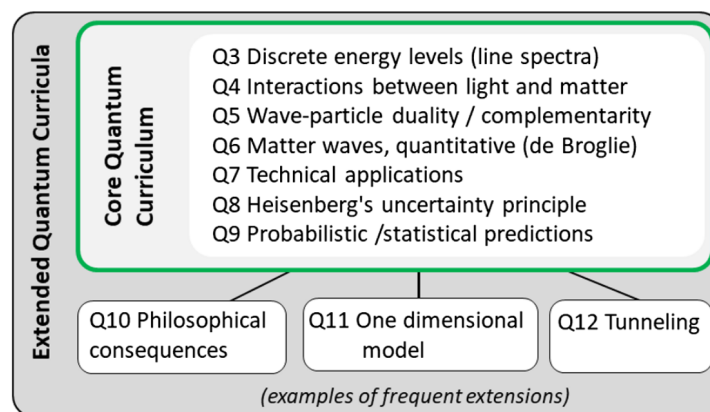


Abbildung 29: Core Quantum Curriculum (Q3-Q9) und mögliche Ergänzungen (Quelle: [3, S.11])

Technische Applikationen (Q7) finden demnach oft Eingang in den Unterricht und gehören dem hier definierten Kerncurriculum an, erwähnt werden hier explizit LED, Laser und Elektronenmikroskope. Auch die Thematisierung eines Quantencomputers und dessen Wirkungsweise könnte demnach hier verortet werden.

Die Möglichkeit eines Zugangs zur Quantenphysik, der von bisher geschilderten Konzepten abweicht und in weiterer Folge auch Quantencomputer zum Inhalt im Physikunterricht machen könnte, soll im nächsten Kapitel thematisiert werden.

4.4 Aussichten für einen Ansatz mit Qubits

Da Inhalte aus der Quanteninformationstheorie im Schulunterricht nur selten vorkommen, sollen hier einige Möglichkeiten und Vorzüge eines solchen Ansatzes vorgestellt werden. Hier soll in besonderem Maße auf Artikel von Wolfgang Dür und Stefan Heusler ([35],[36],[37]) Bezug genommen werden, in denen viele Anreize zum Unterrichten dieser Themen gegeben werden.

Didaktische Aspekte zu Qubits

Dass Quantenphysik in der Schule oftmals nur gestreift wird, macht Dür am komplexen mathematischen Formalismus und dem scheinbaren Widerspruch zu Erfahrungen aus dem Alltag fest, womit sich vermehrt die Frage stellt, „wie man die Quantentheorie so aufbereiten kann, dass sie auch für Schüler[:innen] interessant und vor allem verständlich präsentiert werden kann“ [35, S.1]. Aufgrunddessen soll zur Einführung gerade das einfachste denkbare Quantensystem dienen, um mathematische Schwierigkeiten zu umgehen und die zentralen Themen anhand dieses Systems einzuführen und verständlich zu machen (siehe [35, S.2]).

Dabei kann besonders zu Beginn die Vereinfachung von reellen Koeffizienten der Basiszustände getroffen werden, was den Umgang mit komplexen Zahlen damit vorerst beiseite lässt und in der Blochkugel damit nur Zustände auf einem Einheitskreis betrachtet werden (siehe [35, S.3]). Anhand der Darstellung in der Blochkugel können dann beispielsweise die Postulate aus Kapitel 2.2 verdeutlicht werden; so können Superpositionen, Manipulationen am System in Form von Drehungen eines Vektors (wie in Abb. 30) und Messungen mit der Blochkugel demonstriert und visualisiert werden.

So wie beispielsweise in Kapitel 2.3 eine Messung durch eine Achse durch den Ursprung visualisiert wurde, lässt sich hier vereinfacht eine Messung in Form eines „Schlitzes“ in einer bestimmten Raumrichtung veranschaulichen, wodurch der Messprozess sich in Form eines Umklappens des zugehörigen Blochvektors gestaltet, um durch den Schlitz „hindurchzupassen“. Hier kann bereits der stochastische Charakter besprochen werden und auf eine Ausdehnung auf relative Häufigkeiten bei vielen Durchführungen des Experiments hingewiesen werden, da schlussendlich nur über diese eine Aussage gemacht werden kann (siehe [35, S.3-4]).

Eine solche Visualisierung ist in Abb. 31 zu sehen, wobei in diesem Beispiel eine Spin-Messung mit einem Stern-Gerlach-Apparat als Vergleich herangezogen wird.

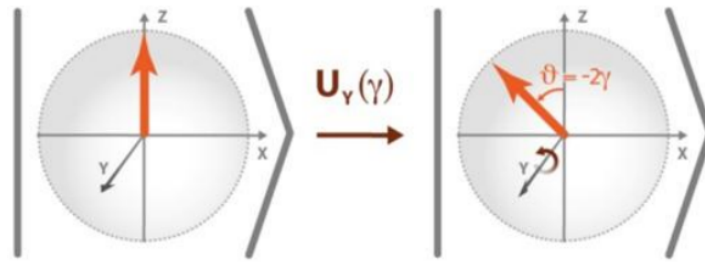


Abbildung 30: Visualisierung einer Manipulation am System in Form einer unitären Transformation durch Drehung des Blochvektors (Quelle: [36, S.4])

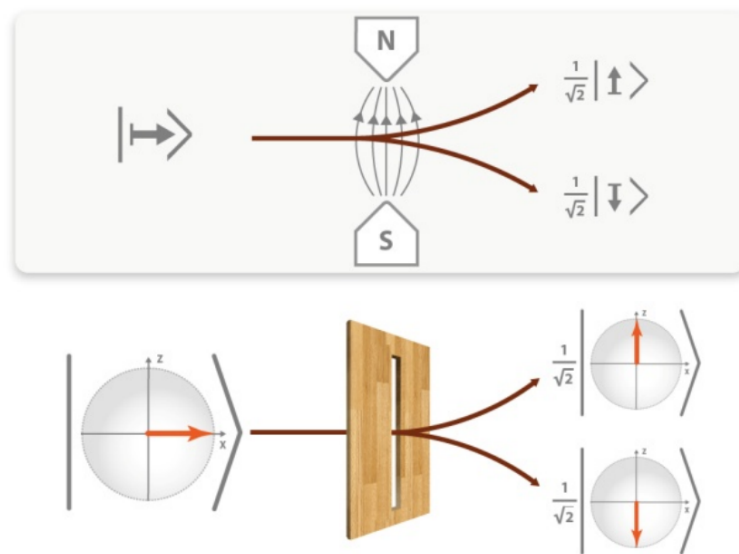


Abbildung 31: Visualisierung einer Spinnmessung in Form eines Schlitzes (Quelle: [36, S.8])

Zur Visualisierung der Messung führen Dür und Heusler weiter aus, dass durch eine einzelne Messung der Zustand des Qubits nicht erfasst werden kann, da der Zustand durch die Messung und die Wahl dieser verändert wird. Dabei gilt auch darauf hinzuweisen, dass der hier dargestellte Schlitz keine reale Entsprechung besitzt, sondern nur als Hilfsmittel herangezogen wird (siehe [36, S.5]).

Die Tatsache, dass eine Messung den Zustand auch tatsächlich verändert, kann z.B. mithilfe dreier Polarisationsfilter und einer Lichtquelle verdeutlicht werden, so wird dabei das folgende, leicht auszuführende Experiment beschrieben: Legt man zwei Polarisationsfilter orthogonal aufeinander, lassen diese kein Licht mehr hindurch. Legt man allerdings einen dritten Polarisationsfilter zwischen diese beiden, kann durchaus wieder Licht durchgelassen werden (mit einem Maximum bei einer 45°-Stellung). „Im Bild einzelner Teilchen bzw. Photonen zeigt sich deutlich, dass eine ‚Messung‘ bzw. Wechselwirkung mit dem Filter den Zustand verändert“ [36, S.12].

Für die konkrete Realisierung von Qubits zählen Dür und Heusler dabei folgende physikalische Systeme mit Vor- und Nachteilen der Ausführungen auf:

- *Polarisation von Photonen*: Durch Identifizieren der Basiszustände mit $|0\rangle = |H\rangle$ und $|1\rangle = |V\rangle$ können Superpositionen anschaulich dargestellt werden, zudem können Manipulationen mit Kristallen und Messungen mittels polarisierender Strahlteiler thematisiert werden. Die Anschaulichkeit rührt dabei von Kenntnissen aus der klassischen Optik her, was allerdings wiederum die Gefahr birgt, dass das quantenmechanische Besondere hier nicht erkannt wird. Hier muss darauf hingewiesen werden, dass es sich um einzelne Photonen handelt, aus denen sich dann das klassische Verhalten überhaupt erst ergibt. Zudem wird darauf hingewiesen, dass die Zuordnung von Polarisationen zu den Blochvektoren in Richtung der einzelnen Achsen für Verwirrung sorgen kann, da die Vektoren entlang der x-Achse die Zustände $|+\rangle$ und $|-\rangle$ repräsentieren, während es sich bei den Vektoren entlang der y-Achse um zirkular polarisierte Photonen handelt, wie in Abb. 32 (links) ersichtlich (siehe [36, S.7-8], siehe auch Kapitel 3.5).
- *Spin eines Teilchens*: Durch den Spin eines Teilchens und der Zuordnung $|0\rangle = |\uparrow\rangle$ und $|1\rangle = |\downarrow\rangle$ erfolgt eine intuitiv leichter nachvollziehbare Zuordnung zu den entsprechenden Blochvektoren, da diese mit der räumlichen Ausrichtung identifiziert werden kann (siehe Abb. 32, rechts). Manipulationen können mithilfe eines homogenen Magnetfelds erfolgen, während Messungen mit einem inhomogenen Magnetfeld in Form eines Stern-Gerlach-Apparates und einer Ablenkung abhängig vom Spin (wie in Abb. 31 angedeutet) durchgeführt werden können. Als Nachteile können hier die Notwendigkeit, den Spin vermutlich hierfür erst einführen zu müssen, und eine fehlende klassische Entsprechung des Spins angeführt werden, da die Interpretation eines Eigendrehimpulses durchaus problematisch ist (siehe [36, S.8-9]).
- *Ort eines Atoms*: Auch der Ort eines Atoms lässt sich hier prinzipiell erwähnen, wobei darauf hingewiesen wird, dass die Vorstellung einer Superposition hier schon deutlich schwieriger fällt als in anderen Beispielen. Durch Fangen eines Atoms in einem Doppelpotential lassen sich die Zustände $|0\rangle$ und $|1\rangle$ mit den beiden Orten in Abb. 33 identifizieren, Manipulationen können über Änderung des Potentials erfolgen und Messungen sind konkrete Ortsmessungen (siehe [36, S.9]).
- *Elektronische Zustände von Atomen/Ionen*: Die Nutzung von Zuständen der Elektronen in einer Ionenfalle wurde im Wesentlichen bereits in Kapitel 3.5 thematisiert, für den Unterricht kann dabei auch Bezug zu bereits bekannten Atommodellen und Energieniveaus genommen werden (siehe [36, S.10]).

I Bezug zur Thematisierung von verschiedenen physikalischen Systemen wird zudem erwähnt, dass sich für die Behandlung im Schulunterricht durchaus anbietet, mehrere Realisierungen vergleichend zu diskutieren, da es kein System gibt, das frei von Anschauungsproblemen ist (siehe

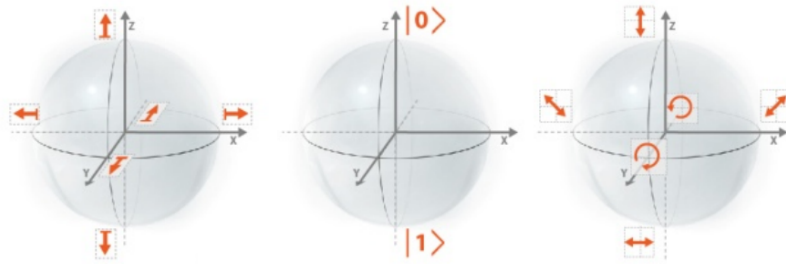


Abbildung 32: Entsprechungen von Blochvektoren für Polarisation von Photonen (links), Spin eines Teilchens (rechts) und ein allgemeines Qubit (Mitte) (Quelle: [36, S.7])

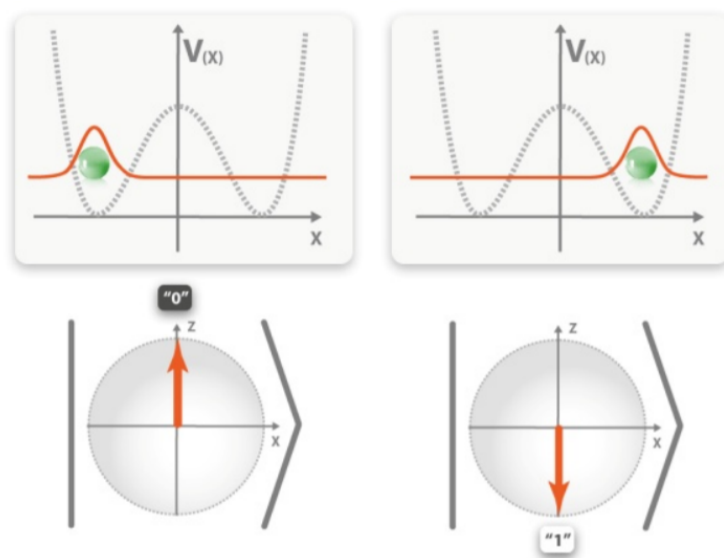


Abbildung 33: Der Ort eines Atoms im Doppelpotential als Qubit (Quelle: [36, S.9])

[36, S.6]).

Dem Spin bei einer Einführung der Quantenmechanik Vorzug zu geben, verfolgt auch der Ansatz von Manogue et al. in [38], der zu Beginn auf Simulationen von Spin-Messungen mit Stern-Gerlach-Apparaten setzt. Der *spin-first-approach* wird hier genutzt, um verschiedene Repräsentationen des quantenmechanischen Formalismus darzustellen (sowohl Matrix- als auch Dirac-Notation), und darauf aufbauend die Wellenfunktion zu thematisieren (vgl. [38, S.1-3]).

Zum Einsatz von Simulationen sei zudem die Arbeit von Kohnle et al. erwähnt, die in Form von *QuVis - The Quantum Mechanics Visualisation Project* zahlreiche Simulationen zur Quantenphysik auf einer Website zur Verfügung stellt (siehe [39]). In einer Arbeit zur Thematisierung von Zwei-Level-Systemen werden dabei Simulationen für Mach-Zehnder-Interferometer und Stern-Gerlach-Apparate behandelt, welche von Schüler:innen benutzt und darauf basierend evaluiert

wurden (vgl. [40]).

Eine Arbeit von Dür und Heusler zur Betrachtung von Systemen mit zwei Qubits (vgl. [37]) ist zwar nicht direkt zur Anwendung im Schulunterricht gedacht, soll an dieser Stelle allerdings erwähnt werden, da sie interessante Einblicke in Verschränkung, Vergleiche von klassischen Korrelationen und Quantenkorrelationen sowie Möglichkeiten zur Darstellung von verschränkten Zuständen liefert.

Ausblick auf weitere Themen aus der Quantenphysik

Zur weiteren Behandlung weisen Dür und Heusler darauf hin, dass auch die Heisenberg'sche Unbestimmtheitsrelation mit Qubits und deren Messungen behandelt werden kann, so können beispielsweise Messungen in x- und z-Richtung als komplementäres Paar thematisiert werden (siehe [36, S.12-13]).

Dies kann dabei bereits an einzelnen Teilchen mit Spin-Messungen qualitativ besprochen und auf ein Ensemble an Teilchen ausgeweitet werden.

Durch die frühe Demonstration der Postulate und der Vorstellung von Superposition aller möglichen Messergebnisse kann zudem im weiteren Verlauf schrittweise eine qualitative Ausweitung auf höherdimensionale und schließlich kontinuierliche Variablen, wie Ort und Impuls, erfolgen (siehe z.B. [38]).

5 Unterrichtssequenz

Die entworfene Sammlung an Unterrichtseinheiten, die sich durchgehend auf die Thematisierung von Qubits und das Behandeln quantenphysikalischer Prinzipien an diesen stützt und orientiert, umfasst insgesamt *neun Unterrichtseinheiten*.

Inhaltlich erfolgt dabei zunächst in Form von *vier Einheiten* eine Einführung in die Postulate der Quantenmechanik, die an Qubits und verschiedenen Realisierungen dieser demonstriert werden. Eine Betrachtung von mehreren Qubits und der Relevanz dieser für den Quantencomputer folgt im Anschluss daran, welche um die qualitative Diskussion von makroskopischen Systemen (mit Bezug zum Quantencomputer und dem darin enthaltenen Problem der Dekohärenz) erweitert wird und damit weitere *drei Einheiten* umfasst.

Abschließend wird in Form von *zwei Einheiten* das Phänomen der Verschränkung und eine Anwendung dieser in Form von abhörsicherer Kommunikation bearbeitet, da auch hier wiederum die Betrachtung von Qubits dienlich sein kann.

Bevor im Folgenden die einzelnen Einheiten mit entsprechenden Anmerkungen und Hinweisen dargelegt werden, soll zuvor noch eine Sammlung an Aspekten geboten werden, die bei der Durchführung allgemein zu beachten sind und das Vorgehen dabei begründen sollen.

5.0 Rahmenbedingungen und Vorbemerkungen

Vorwissen der Schüler:innen

Zur Bearbeitung von verschiedenen physikalischen Systemen, die das Prinzip der Superposition beinhalten, sind unter anderem Kenntnisse aus der Optik und Elektrodynamik relevant.

Besonders bedeutsam ist hier der Photoeffekt, der vor der Unterrichtssequenz thematisiert werden oder im Lehrplan auch im vorangehenden Semester an die Wellenoptik angeschlossen werden kann, um an dieser Stelle bereits anzudeuten, dass es durchaus noch weiterer Untersuchungen zur Natur des Lichts bedarf. Zudem wird häufig auf die Polarisierung von elektromagnetischen Wellen Bezug genommen, welche ebenso im Zuge der Wellenoptik angesprochen werden kann.

Im Bereich der Elektrodynamik ist zudem die Wirkung des elektrischen Stroms im Sinne eines Magnetfelds für die Behandlung von supraleitenden Ringleitern erforderlich, das Konzept der Supraleitung wird im Laufe der Einheiten kurz angesprochen.

Jenes Semester, in dem die Quantenphysik behandelt wird, enthält zudem auch die Atomphysik. Auf eine Behandlung dieser, in der wiederum Photonen eine wichtige Rolle spielen, wird in weiterer Folge ebenso aufgebaut, da auch verschiedene Energieniveaus eine mögliche Realisierung eines Qubits darstellen.

Der Spin von Teilchen spielt zudem aufgrund der Anschaulichkeit der Zustände in der Blochkugel eine große Rolle, aufgrund seltenen Vorkommens im Schulunterricht wird auf diesem Konzept jedoch nicht aufgebaut. Stattdessen widmet sich die erste Einheit vollständig dieser Eigenschaft, hierfür wird allerdings auf das Verhalten von Magneten in äußeren Magnetfeldern Bezug genommen.

Mathematische Vereinfachungen

Da quantenphysikalische Inhalte in hohem Maße auf mathematische Konzepte aufbauen können, auf die zum Zeitpunkt der Thematisierung im Schulunterricht kaum zurückgegriffen werden kann, wird die mathematische Herangehensweise im Zuge dieser Sequenz nur gestreift. Lediglich die Superposition von Zuständen wird hier für einzelne Qubits und eine Beschreibung zweier Qubits mathematisch behandelt.

Da auch der vertraute Umgang mit komplexen Zahlen nicht vorausgesetzt werden kann, wird darauf nur optional und nebenbei eingegangen. Vielmehr werden hauptsächlich Zustände behandelt, die sich in der Blochkugel in der x-z-Ebene befinden, um eine Beschreibung mit reellen Koeffizienten zu ermöglichen.

Im Zuge der Nutzung der Blochkugel als „Schaubild“ für Zustände werden diese zu jenem Zeitpunkt bewusst nicht als *Zustandsvektoren* eingeführt, um Verwirrungen um den Begriff *Vektor* zunächst zu vermeiden; Zustände werden hier vorerst als neuartige Objekte eingeführt. Auf eine Zuordnung zu entsprechenden orthogonalen Vektoren kann an geeigneten Stellen eingegangen werden, diese ist allerdings in der folgenden Sequenz nicht enthalten und könnte beispielsweise in einer daran anschließenden Behandlung höherdimensionaler Systeme und der Überleitung zur kontinuierlichen

Ortsvariable als Schreibweise für Zustände zum Einsatz kommen.

Methodische und inhaltliche Anmerkungen

Die Planung der Unterrichtseinheiten richtet sich nach dem 5E-Modell nach Bybee (siehe [41]), wonach die einzelnen Phasen der Unterrichtseinheiten den Bereichen *Engage*, *Explore*, *Explain*, *Elaborate* und *Evaluate* zugeordnet werden. Da die Durchführung von Realexperimenten in hohem Maße von aufwendigen Versuchsaufbauten und preisintensivem Equipment abhängt, baut die Sequenz hauptsächlich auf Gedankenexperimente, Analogien und Computersimulationen auf, um auf diesem Wege trotzdem Möglichkeiten zu selbstständigem Lernen bereitzustellen.

Um zu verdeutlichen, dass unterschiedliche physikalische Systeme zur Superposition von Zuständen fähig sind, werden durchgängig verschiedene Systeme thematisiert; aufgrund der Anschaulichkeit wird allerdings zumeist auf Spin von subatomaren Teilchen und Polarisierung von Photonen Bezug genommen. Der Doppelspalt, der auch eine Möglichkeit zur Realisierung zweier Messergebnisse darstellt, wird hier bewusst noch nicht thematisiert, um diese Möglichkeit für eine anschließende Behandlung von Photonen und Elektronen am Doppelspalt und einer darauf aufbauenden Ausdehnung auf die Ortseigenschaft aufzusparen. Dieser Themenblock wird hier ausgegliedert, um inhaltlich konsistent zu bleiben und durch diese Themenordnung möglichst wenig Verwirrung zu stiften. Auf eine mögliche anschließende Vorgangsweise hinsichtlich weiterführender Themen wird in Kapitel 6 noch eingegangen.

Materialien zur Durchführung

Die Materialien sind gesammelt im Anhang zu finden, eine bearbeitbare Version dieser wird unter [42] zum Download zur Verfügung gestellt. Die Materialien enthalten unter anderem eine Präsentation, die die Einheiten begleiten soll und ist mit diversen Grafiken, die die Durchführung dieser erleichtern sollen, versehen. Zudem dient die Präsentation zur Führung durch die einzelnen Einheiten, da Anweisungen, Ergebnisse zu Aufgabenstellungen und etwaige Merktex te enthalten sind. Besondere Symbole darin dienen zudem zur Orientierung für Lehrperson und Schüler:innen (ψ - Start einer neuen Einheit, $?$ - Fragestellungen an Schüler:innen, $!$ - Arbeitsphase mithilfe von Arbeitsblättern, $\star$ - besonders wichtige Ergebnisse).

Grafiken und Merktex te sind in dieser Form gesammelt, um die Lernzeit zu maximieren und aufwendige Erstellung von Skizzen und das handschriftliche Kopieren von Texten zu vermeiden, diese können aber wahlweise ausgegliedert und zur Mitschrift in Heften der Schüler:innen angedacht werden. Denkbar ist andernfalls auch, die Präsentation (in beliebiger Ausführung) Schüler:innen auf diversen Plattformen zur Verfügung zu stellen.

Ebenfalls inkludiert sind Arbeitsblätter, die Schüler:innen durch die Arbeitsphasen leiten und Aufgaben zum Ergründen der Inhalte oder Anwenden der erlernten Konzepte enthalten.

Um zudem Vorstellungen von Zuständen in der Blochkugel und Operationen damit zu vereinfachen, ist die Verwendung einer „Blochscheibe“ angedacht, die wiederholt zum Einsatz kommt und

Material zum Anfassen bieten soll. Diese kann entsprechend der Anleitung, die sich mit den Einzelteilen der Blochscheibe im Anhang befindet, ausgedruckt und zusammengefügt werden.

5.1 Einheit I - Spin

Tabelle 5: Planungsmatrix zur Einheit I - Spin

Key Ideas: Teilchen kann die Eigenschaft „Spin“ zugeordnet werden. Dieser kann mit einem Stern-Gerlach-Apparat gemessen werden.				
Kompetenzen: Schüler:innen können... ... Spin als Eigenschaft von Teilchen nennen, die mit Magnetfeldern wechselwirkt. ... erklären, wie man den Spin von Teilchen messen kann.				
Materialienliste: • Präsentation: S. 1 - 16 • Kärtchen in zwei Farben – grün & orange/rot				
Zeit	Phase	Lehrer:innen-Tätigkeit	Schüler:innen-Tätigkeit	Materialien
5‘	Engage	Erfragen von Vorstellungen von Quantenphysik, Rückschau: offene Punkte in Atomphysik und Optik, Konfrontation mit Zitaten von Bohr und Feynman	Vorstellungen und Vorerfahrungen einbringen	Präsentation
25‘	Explore	Quiz zur Einführung von Spin, Fragen zu Neutronen in Magnetfeld	Vermutungen zu Versuchen und Ergebnissen mit Kärtchen äußern	Präsentation, Kärtchen
10‘	Explain	Zusammenfassung, Herkunft des Begriffes Spin andeuten, Spin in makroskopischen Objekten ansprechen	Vermutung zu makroskopischen Objekten äußern	Präsentation
10‘	Elaborate	Versuch mit mehreren Neutronen und resultierende Verteilung besprechen, andeuten von <i>Quanten</i>	Vermutung zum Versuchsausgang äußern	Präsentation

Erläuterung

In der *Engage-Phase* sollen die Schüler:innen zunächst erläutern, was sie bereits von Quantenphysik gehört haben oder was sie sich darunter vorstellen. Zudem sollen sie daran erinnert werden, dass es in der Atomphysik (Energieniveaus) und Optik (Beschreibung von Licht als Welle oder Teilchen) durchaus noch offene Fragen gibt. Mit zwei Zitaten von Niels Bohr und Richard Feynman als Beginn der Präsentation werden die Schüler:innen darauf eingestimmt, dass das Folgende sehr abstrakt wirken kann und es daher in Ordnung ist, wenn an bestimmten Punkten Verwirrung auftaucht und es manchmal Modelle braucht, deren Ursprung merkwürdig erscheint, welche sich aber später als hilfreich und aussagekräftig erweisen werden.

Die *Explore-Phase* gestaltet sich methodisch durch ein Quiz, indem in der Präsentation verschiedene Situationen geschildert werden und die Schüler:innen zwischen zwei Antwortmöglichkeiten wählen können. Diese Antworten können sie im geeigneten Moment in Form von farbigen Kärtchen ausdrücken, woraufhin verschiedene Ideen gesammelt und die Lösung besprochen werden kann. Inhaltlich sollen zunächst Erkenntnisse aus dem Magnetismus reaktiviert werden, in dem die Wirkung von externen Magnetfeldern auf Magneten in homogenen und inhomogenen Magnetfeldern thematisiert wird. Dies dient auch zur Vorbereitung auf eine spätere Behandlung von Manipulationen eines Qubits in Form eines homogenen Magnetfelds. Hiermit soll zudem ein Anknüpfungspunkt zu bereits Erlerntem hergestellt werden, um nicht abrupt mit neuen und unbekannten Eigenschaften zu beginnen.

In weiterer Folge wird Spin als Eigenschaft eines Teilchens genannt, wodurch sich diese in Magnetfeldern wie Magneten verhalten. Der Name suggeriert dabei eine Drehung des Teilchens, auf die Namensherkunft soll jedoch erst später Bezug genommen werden. Mit einigen Beispielen sollen Orientierungen von Spin und inhomogenen Magnetfeldern zueinander und die Folgen daraus thematisiert werden: Die Kraft, die das Teilchen erfährt, ist also von der Orientierung des Spins relativ zum Magnetfeld abhängig, und damit sollten verschiedene Ablenkungen stattfinden. Aufgrund einer einfacheren Vorstellung werden zu diesem Punkt parallel kleine Magneten als Modelle für den Spin betrachtet, welche in weiterer Folge weggelassen werden.

In der *Explain-Phase* werden die Erkenntnisse zusammengefasst, wobei die gezeigte Vorrichtung mit Stern-Gerlach-Apparat bezeichnet und klargestellt wird, dass auch Protonen und Elektronen eine solche Eigenschaft aufweisen. Zudem wird kurz die Namensherkunft des Spin als Drehung bei Elektronen angedeutet, wobei wieder Bezug auf bereits bekannte Verbindungen von Elektrodynamik und Magnetismus genommen und dabei auch kurz das Problem der Vorstellung besprochen werden kann. Weiters soll auch angedeutet werden, warum ein solcher Spin in makroskopischen Objekten nicht feststellbar ist.

Zuletzt soll dieses Konzept in der *Elaborate-Phase* angewendet werden, indem eine Vorhersage eines Versuchs mit vielen Neutronen und zufälligen Spin-Ausrichtungen bemüht wird und eine Aussage

über die erwartete Verteilung erfolgen soll. Hierfür sollen Schüler:innen zunächst gegenseitig beratschlagen, welches Ergebnis (klassisch) zu erwarten wäre, zum Ende soll die Lehrperson auflösen, welches Ergebnis ein echter Versuch bringen würde. Hierfür kann zudem ein Video dienen, dessen Link in der Präsentation vermerkt ist.

Bemerkungen

Zu Beginn soll offen thematisiert werden, dass Quantenphysik schwer begreifbar ist und das Ungewöhnliche daran hervorgehoben werden. Hier gilt es, das Merkwürdige und Unverständliche an der Quantenphysik allerdings auch nicht zu sehr überzustrapazieren, um nicht von vornherein eine Ablehnung der Quantenphysik zu beschwören.

Zur Einführung von Qubits wird zunächst das Konzept des Spins eingeführt, da mit diesem eine einfache Vorstellung von Zuständen in der Blochkugel, welche in späteren Einheiten relevant wird, möglich wird. Zudem lassen sich auf diese Weise anschaulich Versuche mit einfachen Systemen simulieren, die die Untersuchung und Begründung zweier quantenmechanischer Postulate in der darauffolgenden Einheit ermöglicht. Der Spin von Teilchen soll in dieser Einheit als eine Größe, die mit einem Magnetfeld wechselwirkt, eingeführt werden. Hierbei soll auf etwaige Deutungsfragen nicht explizit eingegangen werden, es soll der Eindruck einer Eigenschaft von Teilchen vermittelt werden, die man messen kann. Um dabei keine Verbindung zu elektrischen Ladungen entstehen zu lassen, werden hierfür Neutronen als Versuchsobjekte gewählt.

Das unerwartete Ergebnis zum Ende der Einheit soll als erstes „merkwürdiges“ Ergebnis dargestellt werden und als Anknüpfungspunkt für die weitere Beschäftigung mit dem Spin von Teilchen dienen. An diesem Punkt kann zudem bereits auf die Namensherkunft von „Quantenphysik“ hingedeutet werden, da der Spin *quantisiert* ist, also (ähnlich wie Energieniveaus) offensichtlich nur bestimmte Werte annehmen kann.

5.2 Einheit II - Superposition und Messung

Tabelle 6: Planungsmatrix zur Einheit II - Superposition und Messung

Key Idea: Der Spin eines Teilchens kann vor einer Messung als Überlagerung der möglichen Messergebnisse beschrieben werden. Eine Messung verändert den Zustand.				
Kompetenzen: Schüler:innen können... ...beschreiben, welche Zustände nach einer Spin-Messung vorliegen können. ...das Konzept der Überlagerung von Zuständen erklären und begründen.				
Materialienliste: • Präsentation: S. 17 - 28 • Arbeitsblatt: „Superposition & Messung“				
Zeit	Phase	Lehrer:innen-Tätigkeit	Schüler:innen-Tätigkeit	Materialien
5‘	Engage	Einleitung mit Schrödingers Katze und Kenntnisse davon, außerdem: Bezug zum offenen Ergebnis aus letzter Stunde	Schildern der Vorstellungen und Kenntnisse über Vergleiche mit Schrödingers Katze	Präsentation
25‘	Explore	Einleitende Erklärung von Bezeichnungen und Skizzen, Umgang mit Simulation	Durchführen der Aufgaben mit Simulation, Interpretieren der Ergebnisse	Arbeitsblatt: „Superposition & Messung“
15‘	Explain	Erklärung und Zusammenfassung: Überlagerung von Zuständen als Modell für Zustand vor der Messung Abschluss: nochmals Schrödingers Katze	Ergebnisse notieren, an Diskussion teilnehmen	Präsentation, Arbeitsblatt

Erläuterung

Da in der Einheit zuvor das unerwartete Messergebnis einer Spin-Messung behandelt wurde, soll in dieser Einheit daran angeknüpft werden und im Fokus stehen, welcher Zustand bei den Neutronen vor der Messung vorhanden war und was eine Messung bewirkt.

In der *Engage-Phase* soll dafür die bekannte Metapher von Schrödingers Katze thematisiert werden, wobei Schüler:innen berichten sollen, was sie davon vielleicht schon einmal gehört haben. Weiters soll auf den Inhalt der folgenden Stunde vorbereitet werden, indem nochmals das Bild der erwarteten und tatsächlichen Verteilung bei einer Spin-Messung wiederholt wird. Hier soll besonders betont werden, dass das Ergebnis stark von der Vermutung abweicht und deswegen in dieser Einheit genauer untersucht werden soll, wie dieses begründet werden kann.

Die *Explore-Phase* stellt den Kern der Unterrichtseinheit dar. Hier soll an das Ergebnis angeschlossen werden und zum ersten Mal die Bezeichnung eines Zustands mit einem ket-Vektor erfolgen. Dies soll hier vorerst nur Symbolcharakter besitzen und als „Schreibweise für Zustände von Teilchen“ dienen, ohne genauer darauf einzugehen. Daraufhin werden Teilchen mit dem Zustand „Spin-up“ weitergeführt und nochmals gemessen, wobei in der zweiten Messung ein um 90° gedrehter Stern-Gerlach-Apparat zum Einsatz kommt. Wiederum sollen Schüler:innen zunächst überlegen, was klassisch zu erwarten wäre, bevor aufgelöst wird, dass auch hier zwei Ergebnisse am Schirm detektiert werden können. Dadurch soll verdeutlicht werden, dass eine Messung im Allgemeinen etwas am Zustand verändert. Dies soll am Arbeitsblatt einleitend in der entsprechenden Box vermerkt werden. Im zweiten Teil sollen Schüler:innen selbstständig eine Simulation bedienen (siehe [43]), diese kann unter folgendem Link abgerufen werden:

<https://physics.weber.edu/schroeder/software/Spins.html>

Dafür soll zunächst die Handhabung von der Lehrperson demonstriert und relevante „Bausteine“, wie Quelle, Analyzer (Stern-Gerlach-Apparate) und Counter, erklärt werden. Durch die beiden Aufgaben sollen Schüler:innen erkennen, dass die Zustände in einem Kanal nach einer Messung in z-Richtung in beide Zustände nach einer Messung in x-Richtung „zerlegt“ werden können, und gleiches in umgekehrter Reihenfolge beobachtet werden kann. Damit kann man die Zustände als Überlagerung der beiden möglichen Messergebnisse deuten, wobei für einzelne Teilchen eine Zuordnung völlig zufällig erfolgt. Die eingerahmten Textstellen sollen dabei vorerst noch freigelassen werden, Schüler:innen können sich aber überlegen, was hier eingefüllt werden könnte.

In der *Explain-Phase* sollen die Ergebnisse zusammengefasst und die eingerahmten Teile ausgefüllt werden (siehe Präsentation). Zudem soll besonders betont werden, dass einzelne Ergebnisse völlig zufällig erfolgen, man aber die Gesamtverteilung durchaus vorhersagen kann. Hier kann eine Analogie zum klassischen Münzwurf gezogen werden. Zudem soll abschließend die Analogie mit

Schrödingers Katze nochmals hergestellt werden. Hier soll außerdem auch schon angedeutet werden, dass Superposition für makroskopische Objekte im Alltag nicht beobachtet werden kann und daher für Katzen eigentlich ungeeignet erscheint, eine Begründung dafür soll auf eine spätere Einheit verschoben werden.

Bemerkungen

Zu Beginn dieser Einheit soll der Umstand, dass das Prinzip von Schrödingers Katze zunehmend Eingang in die Popkultur gefunden hat, dafür genutzt werden, die Konzepte der Superposition und Messung zu etablieren und zugänglich zu machen. An diesem Punkt soll eine vereinfachte Version dessen thematisiert werden, die ohne den Zerfall eines Atomkerns auskommt. Diese soll in einer späteren Einheit erneut diskutiert werden.

Die Darstellung von Zuständen in Form eines ket-Vektors, ohne diesen allerdings so zu benennen, wurde bewusst gewählt, um Schüler:innen prinzipiell an die Schreibweise heranzuführen und nicht sofort Assoziationen mit Spaltenvektoren herzustellen. Dies kann an einem späteren Punkt nachgeholt werden, indem Spaltenvektoren als eine Form dargestellt werden, in der Zustände geschrieben werden können. Hier sollen Zustände zunächst als eigenständige Objekte eingeführt werden, mit denen später auch gerechnet werden kann.

Durch die Hintereinanderausführung von Messungen in z- und x-Richtung sollen Schüler:innen eine Idee davon bekommen, dass sämtliche Zustände immer als Überlagerung ihrer Messergebnisse gesehen werden können. Da diese konkrete Denkweise nicht dem klassischen Denken entspricht, wird hier nicht verlangt, dass Schüler:innen diese selbstständig erschließen; allerdings sollen sie in der *Explore-Phase* jene Ergebnisse bekommen, die später für die Formulierung dessen dienen können.

5.3 Einheit III - Qubits und Realisierungen

Tabelle 7: Planungsmatrix zur Einheit III - Qubits und Realisierungen

Key Idea: Zustände mit zwei Möglichkeiten von Messergebnissen werden Qubits genannt. Es gibt verschiedene physikalische Realisierungen von Qubits. Kompetenzen: Schüler:innen können... ... verschiedene Systeme mit zwei Messergebnissen nennen. ... erklären, was man unter einem Qubit versteht. Materialienliste: • Präsentation: S. 29 - 32 • 3 × Polarisationsfilter • Texte: „Nur zwei Möglichkeiten: Supraleiter/Energieniveaus/Photonen“ • Smartphones oder Computer				
Zeit	Phase	Lehrer:innen-Tätigkeit	Schüler:innen-Tätigkeit	Materialien
5‘	Engage	Versuch mit Polarisationsfiltern, um Einfluss von Messung an einem anderen System zu demonstrieren	Vermutung zum Versuchsausgang äußern, Ergebnis deuten	Polarisationsfilter
30‘	Explore/ Elaborate	Austeilen von drei verschiedenen Texten, Anweisungen zum Modus und Hilfestellungen	Recherche über physikalische Systeme mit zwei Messergebnissen, gegenseitiges Erklären von Erkenntnissen	Präsentation, Texte, Smartphones/Computer
15‘	Explain	Nochmals Polarisationsfilter, Verallgemeinerung: Qubit, erste Darstellung mit Blochkugel	Neuerliche Deutung des Experiments mit drei Polarisationsfiltern	Polarisationsfilter, Präsentation

Erläuterung

In der *Engage-Phase* soll anhand dreier Polarisationsfilter erneut demonstriert werden, dass eine Messung den Zustand von Objekten verändert, ohne dies an jenem Punkt explizit zu erwähnen. Dadurch soll den Schüler:innen bewusst gemacht werden, dass sich die nun folgende Einheit nicht mit Spin beschäftigen wird, und trotzdem Erkenntnisse aus der vorherigen Einheit wieder auftauchen werden. Hier ist anzumerken, dass Kenntnisse zur Polarisation von Licht und einer Messung dieser mithilfe von Polarisationsfiltern erforderlich sind. Dazu werden zwei Polarisationsfilter orthogonal übereinander gelegt. Die Schüler:innen sollen hier erklären, warum unter diesen Bedingungen kein Licht durchgelassen werden kann. Im nächsten Schritt soll ein dritter Polarisationsfilter zwischen die beiden in einem Winkel von etwa 45° gelegt werden, die Schüler:innen sollen zunächst Vermutungen darüber anstellen, was hierdurch passieren könnte und ob dies etwas verändern würde. Intuitiv sollte in diesem Beispiel durch Hinzufügen eines weiteren Bauteils nicht mehr Licht durchdringen dürfen, durch den Messvorgang und die entsprechende Änderung des Zustands ist dies allerdings möglich. Diese Erklärung soll allerdings erst zum Ende der Einheit nachfolgen, wenn Schüler:innen bereits Wissen um Photonen und Polarisation als Systeme mit zwei möglichen Messergebnissen erlangt haben. Schüler:innen können hier z.B. gefragt werden, ob sie glauben, dass dies etwas mit Quantenphysik oder den bisherigen Konzepten zu tun hat. Hier soll erwähnt werden, dass es durchaus eine Verbindung zur vorherigen Einheit gibt, diese aber erst zu einem späteren Zeitpunkt ersichtlich wird.

In der zweiten Phase soll Schüler:innen mit vorbereiteten Texten Zeit gegeben werden, sich eigenständig mit verschiedenen physikalischen Systemen mit zwei Messergebnissen auseinanderzusetzen. Dafür sollen drei Systeme dienen (Supraleitung, Photonen, Energieniveaus), wobei jeder:r Schüler:in einen entsprechenden Text behandelt. Die hier dargestellten Inhalte sollen dabei an das Niveau der Schüler:innen angepasst und vereinfacht dargestellt werden, zudem soll ihnen (beispielsweise mit Smartphones) die Möglichkeit gegeben werden, weitere Recherchen zu Kernbegriffen anzustellen. Nach der Einzelbeschäftigung und dem Herausfiltern der wichtigen Inhalte sollen Schüler:innen mit verschiedenen Texten in Form von Gruppenpuzzles in Gruppen eingeteilt werden. Dies soll dazu führen, dass sich zunächst Schüler:innen mit gleichen Texten in Kleingruppen austauschen und über die neuen Informationen sprechen können, um anschließend in einer zweiten Gruppenphase Schüler:innen jeweils anderer Texte zu erklären, was sie in Erfahrung gebracht haben.

Dies dient gleichzeitig als *Explore-Phase*, da die Schüler:innen neue Inhalte erarbeiten, aber auch als *Elaborate-Phase*, da die Aspekte der Superposition und Messung auch hier wieder auftauchen.

Abschließend wird, nach einer Erklärung für das Experiment der drei Polarisationsfilter, in einer *Explain-Phase* zusammengefasst, dass es verschiedene Arten von sogenannten Zwei-Level-Systemen gibt, und diese mit Qubits bezeichnet werden. Hierfür kann der Wortstamm in den Vordergrund gerückt werden und eine erste Verbindung zu klassischen Bits gezogen werden. Zudem soll offen

thematisiert werden, dass von Schüler:innen nicht erwartet wird, die einzelnen Systeme in Details zu verstehen, da hierfür eine viel genauere Betrachtung notwendig wäre. Mit der Begründung, dass solche Qubits allgemein und für Quantencomputer von Interesse sein werden, wird zudem die Blochkugel zur Veranschaulichung herangezogen, wobei hervorgehoben werden soll, dass dies nur zur Darstellung von Zuständen dient, und die Pfeile darin im Allgemeinen keine reale Entsprechung haben.

Bemerkungen

Methodisch soll diese Einheit großteils auf Kommunikation und Eigenrecherche ausgelegt sein, um eine Abwechslung zu den Einheiten zu schaffen, die auf fachlich-inhaltliches Verständnis Wert legen.

Um an die Konzepte der zuvor erfolgten Einheit anzuknüpfen und die allgemeingültige Relevanz der behandelten Themen (Einfluss von Messung und Superposition) zu verdeutlichen, sollen Schüler:innen in dieser Einheit weitere Beispiele für Zwei-Level-Systeme kennenlernen. In der Erarbeitung der verschiedenen Realisierungen von Zwei-Level-Systemen geht es nicht um quantitatives oder detailliertes Verständnis zu den behandelten Gebieten, Schüler:innen sollen hier den Eindruck davon bekommen, dass diese Denkweise der Superposition in vielen Gebieten stattfindet (Optik, Elektromagnetismus, Atomphysik) und daher allgemeine Relevanz besitzt, und nicht nur bei der Betrachtung von Spin eine Rolle spielt. Dies soll den Umgang mit dem Gedanken von Überlagerung möglicher Messergebnisse festigen.

Der Versuch mit drei Polarisationsfiltern stellt dabei im ersten Moment keine schlüssige Verbindung zu den zuvor behandelten Konzepten dar, und dies soll auch offen mit Schüler:innen kommuniziert werden. Das Experiment wird dabei mit der Begründung durchgeführt, dass die Regeln der Quantenphysik bis jetzt wie etwas wirkten, das nur im mikroskopischen Bereich stattfindet; dadurch soll angedeutet werden, dass dies auch in anderen Bereichen Anwendung findet und dabei auch makroskopisch beobachtbare Effekte haben kann.

Der Begriff der Blochkugel soll hier vorerst nur mithilfe eines ersten Bildes angedeutet werden, um in der nächsten Einheit darauf zurückgreifen zu können und das Begriffsverständnis auszubauen und zu präzisieren.

5.4 Einheit IV - Zustände in der Blochkugel

Tabelle 8: Planungsmatrix zur Einheit IV - Zustände in der Blochkugel

Key Idea: Qubits und die Konzepte der Superposition, Messung und Manipulation an diesen können an einer Blochkugel demonstriert werden.				
Kompetenzen: Schüler:innen können... ... Superposition, Manipulation und Messung an einer Blochkugel demonstrieren.				
Materialienliste: • Präsentation: S. 33 – 43 • Blochscheibe • Arbeitsblatt: „Zustände in Blochkugeln“ • Arbeitsblatt: „Mehr zur Blochkugel“				
Zeit	Phase	Lehrer:innen-Tätigkeit	Schüler:innen-Tätigkeit	Materialien
10‘	Engage	Daumen-hoch/Daumen-runter Analogie für Superposition, Manipulation und Messung	Bewertung eines Films o.Ä. mit Daumen-hoch/Daumen-runter, zeigen und interpretieren der Anweisungen der Lehrperson	Präsentation
20‘	Evaluate	Arbeitsblatt und Blochscheibe bereitstellen, Hilfestellungen	Bearbeiten des Arbeitsblatts unter Zuhilfenahme von vorherigen Kenntnissen und der Blochscheibe, Erstellung einer Zusammenfassung von Qubits	Blochscheibe, Arbeitsblatt „Zustände in Blochkugeln“
20‘	Elaborate	Aufgabenblatt bereitstellen, gemeinsame Besprechung der Lösung	Zusätzliche Aufgaben bearbeiten	Arbeitsblatt „Mehr zur Blochkugel“

Erläuterung

In der *Engage-Phase* soll zunächst eine Analogie zum nun zu behandelnden Thema hergestellt werden: Die Schüler:innen werden gefragt, was sie von einem bestimmten Thema halten, und dies mit Daumen nach oben/unten oder einer Zwischenstufe zu deuten. Hierbei soll auch das Wort Zustand Verwendung finden, in dem Sinne, dass die Schüler:innen einen solchen einnehmen. Die Schüler:innen sollen anschließend nachdenken, was es von außen zu bedeuten hat, wenn ein Daumen beispielsweise eine Schräglage hat: Es gibt sowohl Pro-, als auch Kontra-Argumente, und je nach der Richtung überwiegt das eine oder andere. Von der Lehrperson wird betont, dass also sowohl positive, als auch negative Haltung vorzufinden ist. Als zweites soll die Lehrperson anbieten, irgendetwas am gefragten Thema für alle zu verbessern, also die Meinungen gleichermaßen in eine bestimmte Richtung zu verändern. Die Lehrperson betont hier, dass man sagen könnte, sie beeinflusst oder manipuliert die Meinungen, was sich in einer Zeigerdrehung äußert. Als drittes sollen sich Schüler:innen vorstellen, alle eine neutrale Lage einzunehmen, um z.B. das Stimmungsbild einer neutral gestimmten Bevölkerung zu demonstrieren. Die Lehrperson stellt die Frage, was wohl passieren würde, würde man diesen Teil der Bevölkerung lediglich fragen, ob sie etwas gut oder schlecht finden, also nur zwei Möglichkeiten zulässt. Das gleiche wird für einen eher positiv und einen eher negativ gestimmten Teil ($+45^\circ/-45^\circ$ -Stellung) wiederholt und gefragt, ob sie wissen, was dieser Teil der Befragung nun wohl repräsentieren sollte.

Bevor die Schüler:innen in Form einer *Evaluate-Phase* eigenständig zu arbeiten beginnen, soll die Darstellung eines Zustands mithilfe eines Zeigers in einer Blochkugel nochmal angeführt werden, welcher sich ähnlich verhält, wie das Anzeigen mit einem Daumen. Zudem soll nochmals an den Beispielen Spin und Polarisierung geklärt werden, welche Zustände in der Blochkugel den Vektoren in x- und z-Richtung entsprechen. Um dies alles in physikalischer Ausdrucksweise zusammenzufassen, wird den Schüler:innen Zeit gegeben, dies in einem Arbeitsblatt (und mit häufigem Bezug zu Spin und Polarisierung von Photonen) festzuhalten, zudem bekommen die Schüler:innen eine „Blochscheibe“ zur Verfügung gestellt, welche aus wenigen Bauteilen gebastelt werden kann und zur Demonstration und als Hilfestellung dienen soll. Bei Unsicherheiten sollen die Schüler:innen zunächst anhand der Daumenanalogie und von Spin-Messungen überlegen, zur Kontrolle können beispielsweise ausgefüllte Lösungen im Klassenraum bereitgestellt werden. Damit sollen Schüler:innen motiviert werden, zunächst selbst eine Lösung zu finden, aber trotzdem eine Kontrollmöglichkeit bekommen.

Nach Fertigstellung sollen Schüler:innen in der *Elaborate-Phase* noch Aufgaben besprechen, die weitgehend verbal beantwortet können, und sich vor allem untereinander dazu austauschen. Dabei geht es um die Messung eines unbekannten Zustands und eines Zustandsgemisches, weiters geht es um eine Andeutung zur mathematischen Formulierung sowie die Erweiterung der Blochscheibe zur eigentlichen Blochkugel.

Bemerkungen

Mithilfe der Daumen-Analogie soll ein Mittel bereitgestellt werden, das im weiteren Verlauf als Bezug dienen kann und anschaulich demonstriert, wie die bisherigen Konzepte in der Blochkugel angewendet werden können. Im weiteren Verlauf sollen Schüler:innen also bereits Bekanntes eigenständig in die Sprache der Blochvektoren „übersetzen“, da diese in den folgenden Einheiten noch häufiger auftauchen wird. Insgesamt sollen Schüler:innen auf diese Weise eine eigene Zusammenfassung der relevanten Punkte erstellen. Im Zuge dessen werden dabei nicht nur Neutronen, sondern auch Elektronen und Protonen angesprochen, um erneut einfließen zu lassen, dass alle genannten Teilchen über die Eigenschaft „Spin“ verfügen.

Die abschließenden Fragen sind weitgehend kurz zu beantworten, es handelt sich um Verständnisfragen, für die Schüler:innen sich untereinander austauschen können. Zwei der Aufgaben besitzen dabei besondere Relevanz:

Die mathematische Beschreibung aus Aufgabe 3) kommt in dieser Form in der darauf folgenden Einheit wieder vor, um die Vorgangsweise einer Zustandsbeschreibung für mehrere Qubits anzudeuten. Zudem soll dies als Basis für mögliche Erweiterungen zur Beschreibung von kontinuierlichen Variablen dienen, welche beispielsweise an die vorgestellte Sequenz anschließen kann.

Weiters ist eine Behandlung von Aufgabe 2) vorteilhaft, um auf den Begriff und die Möglichkeit eines Zustandsgemisches zurückzugreifen, wenn Schüler:innen sich in einer späteren Einheit mit dem Phänomen der Verschränkung auseinandersetzen (siehe Kapitel 5.8).

5.5 Einheit V - Mehrere Qubits

Tabelle 9: Planungsmatrix zur Einheit V - Mehrere Qubits

Key Idea: Die Zustände mehrerer Qubits lassen sich als Überlagerung aller möglichen Bitkombinationen begreifen.				
Kompetenzen: Schüler:innen können... ... beschreiben, aus wie vielen und welchen Zuständen ein System von n Qubits besteht. ... erklären, wie ein quantenphysikalischer Zufallsgenerator funktioniert.				
Materialienliste: • Präsentation: S. 44 - 49 • Münzen • Arbeitsblatt: „Zufallsgenerator“ • Evtl. Smartphones/Computer				
Zeit	Phase	Lehrer:innen-Tätigkeit	Schüler:innen-Tätigkeit	Materialien
10'	Engage	Einstieg und Begründung für Quantencomputer mit Moore'schem Gesetz	Vorkenntnisse zu Computern und Rechenleistungen einbringen	Präsentation
10'	Explore	Aufgabenstellung: Überlegungen mit Münzen zur Beschreibung mehrerer Qubits	Beschreibung mehrerer Qubits und Anzahl der möglichen Messergebnisse	Münzen
15'	Explain	Zusammenfassung, Einführung der 0/1-Schreibweise, mathematisch: zwei Qubits	Ergebnisse beisteuern, mathematische Schreibweise nachvollziehen	-
10'	Elaborate	Arbeitsblatt zu Zufallsgenerator, Zusammenfassung	Bearbeiten der Aufgabe	Arbeitsblatt, evtl. Smartphones/Computer

Erläuterung:

Die Schüler:innen sollen in der *Engage-Phase* auf die anstehende Behandlung eines Quantencomputers eingestimmt werden, indem sie mit einer Grafik des Moore'schen Gesetzes konfrontiert werden und versuchen müssen, daraus etwas abzulesen. Im Laufe der Diskussion soll dabei herausgestrichen werden, dass der sichtbare Verlauf aufgrund immer kleiner werdender Größenverhältnisse nicht beliebig lange fortgesetzt werden kann, und daher Alternativen für klassische Computer und deren Berechnungsweise gefragt sind. Dies soll als Motivation dafür dienen, nun Systeme mit mehreren Qubits zu betrachten.

In der *Explore-Phase* bekommen die Schüler:innen die Aufgabe, zu überlegen, wieviele Möglichkeiten von Messergebnissen es gibt, wenn zwei Qubits betrachtet werden, die jeweils in gleichgewichteter Superposition vorliegen. Diese Aufgabe kann dabei mit einer Analogie mit Münzen gestellt werden, wobei eine sich drehende Münze als Superposition aufgefasst werden kann, während Messergebnisse durch die Münzseiten abgebildet werden. Weiterhin sollen sie überlegen, wie dies für 3, 4 und n Qubits verallgemeinert werden kann.

In der *Explain-Phase* wird dann in der Blochkugel in Anlehnung an klassische Bits die allgemeine Schreibweise für Zustände entlang der z-Achse mit $|0\rangle$ und $|1\rangle$ eingeführt.

Die mathematische Formulierung soll hier nur angedeutet werden, damit Schüler:innen sehen, dass dies auf diese Weise möglich ist und anhand des Koeffizienten wiederum die Wahrscheinlichkeit, ein bestimmtes Messergebnis zu erhalten, bestimmt ist und mit einem intuitiven Wert von jeweils $(\frac{1}{2})^2 = \frac{1}{4}$ übereinstimmt.

Die *Elaborate-Phase* soll mit einer ersten Begründung zur Relevanz des behandelten Konzepts abgeschlossen werden, indem Schüler:innen sich eigenständig mit Zufallsgeneratoren beschäftigen. Hierfür soll zunächst recherchiert werden, wie ein „üblicher“ Zufallsgenerator funktioniert, und mit geeigneten Fragestellungen zur Funktionsweise eines quantenphysikalischen Zufallsgenerators übergeleitet werden.

Bemerkungen

Die anfängliche Betrachtung der Grafik zum Moore'schen Gesetz soll dazu dienen, Schüler:innen selbstständig Informationen aus der Grafik entnehmen zu lassen. Die Diskussion kann dabei beliebig vertieft werden.

Die Analogie mithilfe von Münzen bei der Betrachtung mehrerer Qubits kann abermals zur Erleichterung der Vorstellung von mehreren Qubits dienen, hier kann seitens der Lehrperson noch betont werden, dass die Münzen zwar eine gute Analogie dafür darstellen, in der Art des Zufalls aber ein Unterschied liegt, da die Drehung und der Fall von Münzen prinzipiell vorhersagbar sind, während dies für die Messung von Qubits nicht zutrifft. Eine weitere Behandlung der Natur des

Zufalls erfolgt allerdings ohnedies in einer späteren Einheit (siehe Kapitel 5.7).

Die mathematische Ausführung eines Zustands von zwei Qubits in gleichgewichteter Superposition soll hier dazu dienen, zu demonstrieren, dass Zustände auch als „Rechenobjekte“ aufgefasst werden können, mit denen wie mit „üblichen“ Variablen gerechnet werden kann. Auf dieses Ergebnis wird zudem später im Zuge der Verschränkung nochmal zurückgegriffen (siehe Kapitel 5.8).

Die Aufgabe zum Zufallsgenerator dient einerseits dazu, an einem ersten Modell die Relevanz des Behandelten zu verdeutlichen, andererseits soll zudem bereits ein Fundament für eine Vorstellung davon gelegt werden, was ein Quantencomputer eigentlich macht. An diesem einfachen Beispiel ist bereits ersichtlich, dass mehrere Qubits, die Superposition sowie die Messung dieser eine große Rolle spielen. Dies kann bereits an dieser Stelle zusammengefasst werden, alternativ kann in der darauf folgenden Einheit zum Funktionsprinzip des Quantencomputers auch eine Rückschau auf dieses Beispiel und die prinzipielle Vorgangsweise erfolgen.

Zudem besteht die Möglichkeit, an diesem Punkt auf eine konkrete technische Realisierung in Form eines Smartphones hinzuweisen (siehe beispielsweise [44]), um die Relevanz des Zufallsgenerators an einem echten Beispiel zu verdeutlichen.

5.6 Einheit VI - Quantencomputer

Tabelle 10: Planungsmatrix zur Einheit VI - Quantencomputer

Key Idea: Mit Quantencomputern lassen sich bestimmte Probleme schneller lösen. Quantencomputer nutzen dafür Qubits und die Superposition von Zuständen.				
Kompetenzen: Schüler:innen können... ... Anwendungsgebiete eines Quantencomputers nennen. ... Superposition der Eingaben als einen entscheidenden Unterschied zu klassischen Computern nennen.				
Materialienliste: • Präsentation: S. 50 - 59 • Arbeitsblatt „Lösungssuche“				
Zeit	Phase	Lehrer:innen-Tätigkeit	Schüler:innen-Tätigkeit	Materialien
10'	Engage	Suchaufgaben in Liste von Telefonnummern	Suchen eines bestimmten Namen und einer bestimmten Nummer	Präsentation
15'	Explore	Arbeitsblatt bereitstellen	Arbeitsblatt mit mathematischen Problemen bearbeiten	Arbeitsblatt
25'	Explain	Lösung und Vorgangsweise bei der Suche danach ansprechen, Funktionsweise von klassischen und Quantencomputern verdeutlichen, Anwendungsgebiete klären, Bilder und Funktionsweise zu Sycamore-Prozessor	Probleme und Lösungsstrategie bei Aufgaben besprechen, Wirkungsweise des Quantencomputers nachvollziehen	Präsentation

Erläuterung

Um die Schüler:innen auf eine allgemeine Tätigkeit eines Computers aufmerksam zu machen, wird ihnen in der *Engage-Phase* die Aufgabe gestellt, in einer fiktiven Liste von Telefonnummern möglichst schnell einen bestimmten Namen zu suchen und die zugehörige Nummer aufzusagen, sowie im nächsten Schritt eine bestimmte Nummer zu suchen und den zugehörigen Namen zu nennen. Dabei soll offensichtlich werden, dass die zweite Suchaufgabe mit freiem Auge wesentlich schwieriger ist, und von einem Computer nicht „mit freiem Auge“ angegangen wird, sondern eine schrittweise Abfrage verschiedener Namen und Nummern erfolgen muss.

Darüber hinaus sollen Schüler:innen in der *Explore-Phase* mit zwei weiteren Aufgaben, die das Problem des Handlungsreisenden und die Primfaktorzerlegung beinhalten, exemplarisch daran herangeführt werden, dass es Probleme gibt, die mit steigender Eingabegröße sehr schwierig zu lösen sind. Hier geht es nicht zwingend um die korrekte Lösung des Problems, sondern darum, dass Schüler:innen realisieren, dass solche Beispiele nicht einfach zu lösen sind und viele Versuche benötigen.

In der *Explain-Phase* sollen Ergebnisse gesammelt werden und auch Strategien besprochen werden, wobei hier mit einer Trial-and-Error-Strategie zu rechnen ist. Hier soll bewusst gemacht werden, dass vielfach probiert wird, ähnlich der Suche in der Nummernliste; zudem soll angesprochen werden, dass auch ein herkömmlicher Computer Probleme durch einen solchen Zugang löst, dies in diesem Fall aber mit Bits bzw. Registern von Bits passiert.

Im weiteren Verlauf sollen sich Schüler:innen in der *Explain-Phase* der generellen Wirkungsweise eines Quantencomputers bewusst werden und verstehen, dass einzelne Eingaben nicht nacheinander bearbeitet werden, sondern vielmehr eine Superposition über alle Bitkombinationen erfolgt und daher alle Eingaben gleichzeitig behandelt werden. Da eine Behandlung, die über diesen Grundgedanken hinausgeht, vieles an Mathematik und Übung im Umgang mit Zustandsvektoren verlangt, werden darüberhinausgehende Inhalte lediglich qualitativ angesprochen. In dieser wird zunächst kurz zusammengefasst, dass Suchprobleme oder jene Probleme, die gerade behandelt wurden, zu jenen Problemen gehören, die ein Quantencomputer schneller lösen kann als klassische Computer. Dazu soll auch das Schema eines Schaltkreises besprochen werden, welches den allgemeinen Vorgang und die dabei auftauchenden Konzepte schildern soll.

Zuletzt soll mithilfe von Bildern von Googles Sycamore-Prozessor ein Gefühl dafür gegeben werden, wie ein Quantencomputer aussehen kann. Ebenso kann, falls genügend Zeit bleibt, beispielsweise die Kopplung von Qubits kurz angesprochen werden und darauf hingewiesen werden, dass diese notwendig ist, um beliebige Berechnungen durchzuführen.

Bemerkungen

Die Probleme zur Berechnung sollen rein mathematische Probleme sein, um den physikalischen Inhalt hier etwas aufzulockern, zudem kann ein starker Bezug zur Informatik durch die Arbeitsweise eines klassischen Computers hergestellt werden. Dadurch soll verdeutlicht werden, dass in diesen vordergründig mathematischen Problemen die eben ergründeten physikalischen Prinzipien einen Vorteil verschaffen können.

Die dargestellten Schaltkreise für klassische Computer und Quantencomputer sind zur schematischen Darstellung ohne realen Bezug oder konkreten Algorithmus gedacht, sollen allerdings die Arbeitsweise und die wesentlichen Unterschiede verdeutlichen. Zudem kann beim Funktionsprinzip des Quantencomputers erneut auf den Zufallsgenerator aus der zuvorgehenden Einheit verwiesen werden (siehe Kapitel 5.5).

Die abschließende Behandlung des Quantencomputers in Form von Bildern von Googles Sycamore-Prozessor kann je nach Interesse der Schüler:innen beliebig erweitert werden, so können weitere aktuelle Errungenschaften daran geknüpft oder der tatsächlich realisierte Aufbau näher besprochen werden.

5.7 Einheit VII - Dekohärenz

Tabelle 11: Planungsmatrix zur Einheit VII - Dekohärenz

Key Idea: Superposition lässt sich an makroskopischen Objekten aufgrund ständiger Wechselwirkungen nicht beobachten, dieses Phänomen wird Dekohärenz genannt. Die Vermeidung von Dekohärenz spielt beim Quantencomputer eine große Rolle. Kompetenzen: Schüler:innen können... ... erklären, was unter dem Begriff Dekohärenz verstanden wird. ... erklären, warum Superposition nicht bei makroskopischen Objekten beobachtet werden kann. Materialienliste: • Präsentation: S. 60 – 71 • Evtl. Münzen				
Zeit	Phase	Lehrer:innen-Tätigkeit	Schüler:innen-Tätigkeit	Materialien
10'	Engage	Frage zur Art des Zufalls in der Quantenphysik	Vermutungen anstellen zum Zufall in der Quantenphysik	Präsentation, evtl. Münzen
15'	Explore	Bereitstellen von drei Fragestellungen	Diskussion in Partner- oder Gruppenarbeit	Präsentation
10'	Explain	Zusammenfassung, Hinweis auf Notwendigkeit bei Quantencomputer	Ergebnisse sammeln, Vermutungen anstellen, inwiefern dies für Quantencomputer von Bedeutung ist	Präsentation
15'	Elaborate	Zitat von Erwin Schrödinger einblenden, Fragestellung zur Beurteilung des Zitats	Befassen mit Originaltext zu Schrödingers Katze, Beurteilen der Situation	Präsentation

Erläuterung:

Diese Einheit soll einen Kommunikationsschwerpunkt besitzen und insofern auf einige historische Anmerkungen zur Quantentheorie Bezug nehmen, als dass Kommentare von Albert Einstein und Erwin Schrödinger zur Diskussion stehen und hier angemerkt werden kann, dass es im 20. Jahrhundert viel Diskussion um die Folgen der Quantentheorie gab.

Dazu soll auf den Unterschied von makro- und mikroskopischen Systemen hingewiesen werden, indem in der *Engage-Phase* der Unterschied von Münzwurf und Teilcheneigenschaften thematisiert wird. Hier soll bereits eine Diskussion über die Art des Zufalls und eine mögliche deterministische Beschreibung eines Münzwurfs, die für den quantenmechanischen Zufall nicht existiert, angeregt werden.

In der *Explore-Phase* werden Schüler:innen mit Fragen und Aussagen zum Thema Messung, Superposition und klassischer Welt konfrontiert, die sie wahlweise zu zweit oder in Gruppen diskutieren können. Die Ergebnisse werden nach jeder Frage im Plenum gesammelt:

- Was passiert (z.B. mikroskopisch) eigentlich allgemein bei einer Messung? Versuche, möglichst allgemein zu formulieren!
- „Sie werden doch nicht behaupten wollen, dass der Mond nicht da oben ist, wenn niemand hinsieht?“ -*Albert Einstein* zu *Niels Bohr*
- Warum können wir Gegenstände im Alltag nicht in Superposition beobachten?

In der *Explain-Phase* wird nochmals zusammengefasst und besonders auf zwei Punkte Wert gelegt:

Zum einen soll verdeutlicht werden, dass in der Natur andauernd „Messungen“ bzw. Wechselwirkungen mit der Umgebung stattfinden, und diese auch vom inneren Aufbau von Objekten herrühren. Zum anderen soll klar ausgesprochen werden, dass es dafür keine Beobachtung von Menschen benötigt und damit ein Bewusstsein keine Rolle dafür spielt. Die Erkenntnisse werden in der Präsentation festgehalten und der Begriff Dekohärenz wird genannt.

Ebenso kann allgemein angesprochen werden, dass im mikroskopischen Bereich Superposition existiert, aber keine genaue „Grenze“ dafür angegeben werden kann, wann Wechselwirkungen zu Dekohärenz führen.

Abschließend soll der Einfluss von Wärme thematisiert werden, indem das Konzept der Teilchenbewegung reaktiviert wird. Dadurch soll gemeinsam mit Schüler:innen begründet werden, warum eine niedrige Temperatur (sowie Vakuum) für Superposition bedeutsam und deshalb für den Betrieb eines Quantencomputers notwendig ist. Zudem soll hiermit der Aufbau hinsichtlich der kühler werdenden Etagen des Quantencomputers begründet werden.

In der *Elaborate-Phase* werden Schüler:innen mit dem Originalzitat von Erwin Schrödinger betreffend des Paradoxons mit Schrödingers Katze konfrontiert, die Aufgabe besteht für Schüler:innen darin, zu begründen, warum die Situation so nicht stattfinden kann.

Bemerkungen

Die Einheit dreht sich insgesamt gesehen inhaltlich um eine Unterscheidung zwischen makroskopischen und mikroskopischen Systemen, sowohl was die Art des Zufalls (zu Beginn der Einheit) als auch das „Fehlen“ der Superposition betrifft. Dies wird von einigen Zitaten bekannter Stimmen aus dem 20. Jahrhundert untermauert, die veranschaulichen sollen, dass die Konzepte der Quantenphysik durchaus umstritten waren und sich Interpretationsfragen über den Ursprung des Zufalls teilweise bis heute durchziehen. Hierzu kann bereits zu Beginn offen thematisiert werden, dass der quantenphysikalische Zufall bis jetzt einfach so hingenommen wurde, ohne aber einen möglichen Ursprung dessen auszumachen.

Zur Superposition von Teilchen und Dekohärenz ist an diesem Punkt keine genauere Betrachtung von experimentellen Durchführungen angedacht, allerdings kann erwähnt werden, dass diese nicht nur für einzelne Teilchen, sondern auch für Moleküle nachgewiesen werden kann. Hier kann angemerkt werden, dass eine genauere Behandlung auf später verschoben wird. Dies kann im Anschluss an die hier vorgestellte Unterrichtssequenz erfolgen, indem zunächst beispielsweise der Doppelspalt behandelt wird und über Experimente mit Molekülen zum Nachweis von Interferenz gesprochen wird.

5.8 Einheit VIII - Verschränkung: Phänomen

Tabelle 12: Planungsmatrix zur Einheit VIII - Verschränkung: Phänomen

Key Idea: Zwei Teilchen sind verschränkt, wenn sich deren Zustand nur gemeinsam beschreiben lässt. Mit Verschränkung lässt sich nicht überlichtschnell kommunizieren.				
Kompetenzen: Schüler:innen können... ... eine experimentelle Anordnung zum Erzeugen verschränkter Zustände skizzieren. ... erklären, wie sich verschränkte Zustände bei gleichen Messungen verhalten. ... erklären, warum mit Verschränkung nicht überlichtschnell kommuniziert werden kann.				
Materialienliste: • Präsentation: S. 72 - 82 • Evtl. Münzen • Arbeitsblatt: „Alice & Bob“ • Blochscheibe				
Zeit	Phase	Lehrer:innen-Tätigkeit	Schüler:innen-Tätigkeit	Materialien
5'	Engage	Frage nach Begriff der Verschränkung, Wiederholung des Münzexperiment	Vorstellungen zu Verschränkung äußern, Münzexperiment gedanklich wiederholen	Evtl. Münzen, Präsentation
15'	Explore	Bereitstellen von Arbeitsblatt und Blochscheiben	Bearbeiten des Arbeitsblattes, Interpretation	Arbeitsblatt, Blochscheibe
20'	Explain	Zusammenfassung, Aufbau mit Kristall und Beispiel mit Messungen in anderer Basis, Definition Verschränkung	Ergebnisse beisteuern, Vorstellungen von Versuchsausgang mit anderer Basis	Präsentation
10'	Elaborate	Zusatzaufgabe zur überlichtschnellen Kommunikation	Zusatzaufgabe bearbeiten	Präsentation

Erläuterung

Zu Beginn der Einheit werden Schüler:innen in der *Engage-Phase* gefragt, ob sie bereits etwas von Verschränkung gehört haben oder eine Vorstellung haben, worum es sich dabei handeln könnte. Hier soll mittels eines Zitats von Albert Einstein Interesse geweckt werden, mit der Vorausschau, die Phrase „spooky action at a distance“ im Verlauf der Einheit zu klären. Da für die folgende Erarbeitung der Inhalte das Betrachten der Ergebnisse zweier Münzwürfe hilfreich sein kann, werden die Schüler:innen gebeten, dieses gedanklich nochmals zu wiederholen.

In der *Explore-Phase* sollen sich Schüler:innen mit einem konkreten Experiment und den Ergebnissen der beiden Experimentator:innen Alice und Bob befassen, um zu realisieren, dass diese Zustände nicht wie bisher mit einem Blochvektor in einer Blochkugel dargestellt werden können. Dies spielt dabei auf gemischte Zustände an, wird aber in diesem Kontext nicht explizit erwähnt. Ein weiteres Ziel ist eine mathematische Formulierung dieses Zustands, welcher sich nun nicht mehr aus allen möglichen Bitkombinationen zusammensetzt.

In der *Explain-Phase* soll anhand von Bildern der experimentellen Anordnung der Umstand verdeutlicht werden. Dabei soll besonders darauf Wertgelegt werden, die Möglichkeit zu besprechen, dass die Polarisierungen im interessierenden Bereich bereits vor der Messung bestimmt sind und die Zustände H/V bereits vor der Messung vorliegen. Beim Besprechen dieser Annahme kann dies als „Zustandsgemisch“ bezeichnet werden, wobei an eine Aufgabe zur 4. Einheit (siehe Kapitel 5.4) erinnert werden soll, bei der zu einem solchen kein Blochvektor bestimmt werden konnte. Dass diese Annahme allerdings nicht mit den Messergebnissen vereinbar ist, soll anhand eines Wechsels der Messrichtungen verdeutlicht werden.

Insgesamt soll dabei der Eindruck bleiben, dass eine Beschreibung der Situation mit einzelnen Blochkugeln nicht mehr ausreicht, um das Phänomen zu veranschaulichen. Zudem kann mathematisch angedeutet werden, dass sich dieser Zustand nicht in ein Produkt zweier Zustände trennen lässt, was sich erneut als „Verbundenheit“ oder „Untrennbarkeit“ in einzelne Systeme interpretieren lässt. Hierzu kann mit der mathematischen Formulierung eines Produktzustands aus zwei Qubits (siehe Kapitel 5.5) verglichen werden.

Zudem soll im Zuge dessen zusammengefasst werden, welche Folgen dies nun hat, und was sich über verschränkte Zustände vor und nach einer Messung wirklich sagen lässt. Hier kann wiederum ein Vergleich mit zwei Münzen gezogen werden, um die Folgerungen anschaulich darzustellen. Hier soll auch die anfangs erwähnte Beschreibung „spooky action at a distance“ geklärt werden.

Abschließend soll in der *Elaborate-Phase* die oftmalige Vorstellung, durch Verschränkung lasse sich überlichtschnell kommunizieren, mithilfe einer zusätzlichen Fragestellung angesprochen werden, die Schüler:innen eigenständig diskutieren sollen.

Bemerkungen:

Zum Einstieg in die Einheit kann erneut mit zwei Münzen argumentiert werden, an diesem Punkt kann bewusst angesprochen und nochmals wiederholt werden, dass Münzwürfe nur bedingt gute Vergleiche für Quantenobjekte sind.

In der Erarbeitung der Beschreibung von verschränkten Systemen geht es insgesamt darum, dass Schüler:innen realisieren, dass für solche Systeme die Beschreibung durch einzelne Qubits mit einem Blochvektor mit Einheitslänge nicht mehr angemessen ist, der Situation kann kein solcher Blochvektor zugeordnet werden. Vielmehr soll versucht werden, das gesamte System anhand der möglichen Messergebnisse zu beschreiben. Der letzte Punkt, der die entsprechende mathematische Formulierung enthält, ist dabei als Zusatz markiert, um zu verdeutlichen, dass diese Aufgabenstellung nicht zwingend bearbeitet werden muss, aber eine gedankliche Vorsortierung erfolgen kann.

Zur Sammlung der Ergebnisse soll dabei bewusst angesprochen werden, dass ein Zustandsgemisch erklären könnte, warum kein Blochvektor dafür angegeben werden kann. Schüler:innen könnten dies anhand der Abbildung selbst realisieren, da es anhand dieser Anordnung naheliegend ist, ein solches Gemisch anzunehmen. Hier soll bei verschiedenen Messrichtungen Schritt für Schritt besprochen werden, was bei entsprechenden Annahmen zu erwarten wäre und herausgestrichen werden, dass ein im einzelnen beschreibbarer Zustand offensichtlich nicht schon vorher vorliegen kann.

Die Fragestellung zur überlichtschnellen Kommunikation zum Ende der Einheit ist bewusst offen gestellt, dies soll Schüler:innen dazu anregen, anhand des Gelernten diese oftmals vorkommende Vorstellung von Verschränkung zu beurteilen.

5.9 Einheit IX - Verschränkung: Anwendung

Tabelle 13: Planungsmatrix zur Einheit IX - Verschränkung: Anwendung

Key Idea: Wählt man unterschiedliche Messungen an verschränkten Zuständen, lassen sich nicht mehr die entsprechenden (Anti-)Korrelationen feststellen. Verschränkte Zustände lassen sich zur abhörsicheren Kommunikation verwenden.				
Kompetenzen: Schüler:innen können... ... beschreiben, welche Messergebnisse bei verschränkten Zuständen bei gleicher und unterschiedlicher Wahl von Messungen möglich sind. ... erklären, wie und warum Verschränkung für abhörsichere Kommunikation nützlich sein kann.				
Materialienliste: • Präsentation: S. 83 - 92 • Computer • Arbeitsblatt: „Ein sicherer Schlüssel“				
Zeit	Phase	Lehrer:innen-Tätigkeit	Schüler:innen-Tätigkeit	Materialien
10'	Engage	Quiz mit drei Aussagen zu Verschränkung	Vermutungen und Vorstellungen äußern	Präsentation
10'	Explore	Aufgabe: Auswirkung verschiedener Messungen bei Alice & Bob	Prüfung der Korrelationen mit Simulation (QuVis)	Computer
10'	Explain	Zusammenfassung und Deutung der Ergebnisse, Einführung zum Vorgang der Verschlüsselung von Nachrichten	Ergebnisse berichten, Verschlüsselung nachvollziehen	Präsentation
20'	Elaborate	Aufgabe und Anleitung für Simulation bereitstellen	Bearbeiten der Aufgabe und Schluss auf abhörsichere Kommunikation	Arbeitsblatt, Computer

Erläuterung

In der *Engage-Phase* werden Schüler:innen mit drei Aussagen konfrontiert, die auf oftmalige Missverständnisse von Verschränkung abzielen. Diese können dabei, ähnlich wie in der ersten Einheit, in Form eines Quiz mit entsprechenden Karten, die Zustimmung oder Ablehnung symbolisieren, behandelt werden. Dabei kommen die Konzepte aus den vergangenen beiden Einheiten zum Tragen, da sowohl Verschränkung, als auch Dekohärenz hierbei eine Rolle spielen, womit diese Phase als Wiederholung dienen kann.

Mit dieser Abgrenzung von Dingen, die die Verschränkung nicht leisten kann, kann zur *Explore-Phase* übergeleitet werden, indem nun bearbeitet wird, welchen konkreten Vorteil man aus der Verschränkung ziehen kann. Hierfür sollen Schüler:innen zunächst mit einer Simulation (siehe [39]) herausfinden, was passiert, wenn Alice und Bob unterschiedliche Messungen durchführen. Die Simulation ist unter folgendem Link zu finden:

<https://www.st-andrews.ac.uk/physics/quvis/>

In dieser Simulation sollen zunächst nur die Wahl der Basis und die Single-pair Messung gezeigt werden, da nur diese hier von Bedeutung sind.

In der *Explain-Phase* soll zum einen eine kurze Zusammenfassung der Ergebnisse inklusive der Folgerung, dass die Wahl von unterschiedlichen Messungen nicht mehr die Korrelationen aus der vorherigen Einheit erkennen lässt, dargestellt werden. Zum anderen soll eine kurze qualitative Diskussion zur Verschlüsselung von Nachrichten erfolgen, wobei bereits angedeutet werden kann, dass hier ein Einsatzgebiet von Verschränkung liegt.

Die genauere Untersuchung und den wesentlichen Vorteil einer solchen Verschlüsselung sollen Schüler:innen dann in der *Elaborate-Phase* wiederum mithilfe der Simulation untersuchen. Diese Aufgabe wird dabei von einem Arbeitsblatt angeleitet, da es innerhalb der Simulation viele Auswahlmöglichkeiten gibt und sich damit für manche Schüler:innen zu unübersichtlich gestalten könnte. Zum Ende soll der entscheidende Vorteil nochmals zusammengefasst und herausgestrichen werden.

Bemerkung

Die Verschränkung soll mit einem konkreten Anwendungsgebiet abgeschlossen werden, damit dem Konzept Sinn beigemessen wird und damit exemplarisch gezeigt wird, dass sich diese auch nutzen lässt.

Für die Nutzung der Simulation empfiehlt sich, darauf hinzuweisen, dass viele Einstellungsmöglichkeiten bestehen, die aber hier nicht gebraucht werden und mit denen experimentiert werden

kann, falls Schüler:innen vereinzelt Zeit dafür finden. Für die Behandlung in der *Explore-Phase* werden dabei nur wenige Einstellungen benötigt, für die *Elaborate-Phase* werden die notwendigen Vorkehrungen im Arbeitsblatt geschildert.

In der *Explore-Phase* ist zudem vorgesehen, dass die Schüler:innen zunächst von Hand eine Liste der Ergebnisse erstellen. Zwar gäbe es eine automatisch erzeugte Liste, allerdings werden in dieser bereits Einträge vermerkt, die zu diesem Zeitpunkt der Einheit nicht relevant sind und daher für Verwirrung sorgen könnten. Zudem kann auf diese Weise die später automatisch erstellte Liste und die Vorgangsweise bei der Erstellung dieser leichter nachvollzogen werden.

Die Verschlüsselung von Nachrichten in der Explain-Phase ist hier nur oberflächlich vorgesehen, da eine quantitative Betrachtung wesentlich aufwendiger wäre. Hierbei geht es nur darum, den Grundgedanken der Schlüsselerzeugung und -verteilung in Form einer Kombination von Bits anzudeuten.

6 Ausblick

Die vorgestellte Sequenz soll nur als Grundlage für eine weitere Vertiefung in die Quantenphysik dienen und soll die Behandlung von Quantenphysik nicht vollständig darstellen. Die bis zu diesem Punkt vorgestellten Einheiten beinhalten nur in geringem Maße die angesprochenen Kerninhalte aus Kapitel 4.3, allerdings soll damit ein Fundament für eine weitere Behandlung gelegt werden. Indem wesentliche Konzepte wie Superposition, Messung und Manipulation bereits an Qubits erarbeitet wurden, kann auf diese im späteren Verlauf erneut zurückgegriffen werden. Im Folgenden soll eine Übersicht erfolgen, wie die Sequenz inhaltlich weitergeführt werden kann, um die „üblichen“ Inhalte der Quantenphysik zu behandeln:

- **Photonen am Doppelspalt** können ebenso als System mit zwei Möglichkeiten aufgefasst werden, erneut können die Konzepte von Messung und Superposition zum Tragen kommen und Folgen daraus diskutiert werden.
- **Elektronen am Doppelspalt** können nach der Behandlung von Photonen thematisiert werden, hier kann durch die auftretende Interferenz eine Welleneigenschaft von Materie erkenntlich gemacht werden. Zudem kann ein Bezug zu Dekohärenz durch Experimente mit Molekülen am Doppelspalt hergestellt werden, da die Interferenzeigenschaft von der Aufrechterhaltung der Superposition abhängt.
- Vom Doppelspalt und möglichen Wegen kann zu einer **kontinuierlichen Beschreibung der Orts- und Impulsvariable** übergegangen werden, durch Andeuten einer Schreibweise ähnlich der Zustandsbeschreibung eines Qubits und dessen Erweiterung kann somit die Beschreibung in Form einer kontinuierlichen Funktion motiviert werden.
- Durch Weiterführung der kontinuierlichen Beschreibung von Ort und Impuls lässt sich in weiterer Folge die Verknüpfung dieser beiden durch die **Heisenberg'sche Unbestimmtheitsrelation** thematisieren.
- Da die Heisenberg'sche Unbestimmtheitsrelation häufig Schwierigkeiten im Sinne der Interpretation mit sich bringt, kann an dieser exemplarisch über **Interpretationsmöglichkeiten** der Quantenphysik allgemein diskutiert werden, die Kopenhagener Deutung und die Ensemble-Interpretation bieten sich in diesem Kontext an.
- Ausgehend von der klassischen Beschreibung der Energie und einer Adjustierung für eine quantenmechanische Beschreibung kann die **Schrödingergleichung** motiviert werden, die Folgen können in Form einer qualitativen Beschreibung für ein Teilchen im Potentialtopf visualisiert werden, wodurch eine Verbindung zu den Energieniveaus des H-Atom hergestellt werden kann.
- Zur Vertiefung und Thematisierung der Folgen dieser Beschreibung in Form von Wellen kann der **Tunneleffekt** und etwaige Anwendungen und Vorkommnisse besprochen werden.

Mit dieser Erweiterung könnte eine gesamte Behandlung der Quantenphysik im Schulunterricht im Rahmen von 16 Einheiten erfolgen, womit auch Inhalte aus bewährten Konzepten, wie in Kapitel 4.2 geschildert, ihren Platz im Unterricht finden würden.

Für die Anwendung in einer Schule mit mehr als 7 Wochenstunden Physikunterricht in der gesamten Oberstufe ist außer Quantenphysik auch die Behandlung von Atomphysik vorgesehen, welche vor der vorgestellten Sequenz unterrichtet werden kann. Rechnet man mit 18 Schulwochen pro Semester und 2 Wochenstunden in der 7.Klasse, ergibt dies eine Gesamtanzahl von 36 Physikeinheiten. Geht man dann von einer „Ausbeute“ von zwei Drittel reiner Unterrichtszeit aus, entspricht dies insgesamt 24 Unterrichtseinheiten, demnach würde dies einer Aufteilung von einem Drittel Atomphysik und zwei Drittel Quantenphysik entsprechen.

Eine Erprobung und Evaluierung dieses Zugangs stünde noch aus, um darauf aufbauend weitere Erfahrungen mit den Materialien zu sammeln, diese eventuell an Bedürfnisse von Schüler:innen anzupassen und herauszufinden, in welcher Weise dieser Zugang das Verständnis von weiterführenden quantenphysikalischen Inhalten beeinflusst.

Durch die vorgestellte Sammlung an Einheiten und deren Ausmaß, sowie eine Darlegung des fachlichen Hintergrunds im ersten Teil dieser Arbeit, soll hiermit ein Paket zur Verfügung gestellt werden, mit dem die vorgestellte Sequenz realistisch anwendbar und in der dargestellten Reihenfolge durchführbar ist. Die anfängliche Behandlung der einfachsten quantenmechanischen Systeme im Schulunterricht soll auf diese Weise die Entstehung eines konsistenten Gedankengebäudes von Quantenphysik in den Köpfen der Schüler:innen erleichtern.

Quellen

- [1] Frank Arute u. a. „Quantum supremacy using a programmable superconducting processor“. eng. In: *Nature (London)* 574.7779 (2019), S. 505–510.
- [2] Han-Sen Zhong u. a. „Quantum computational advantage using photons“. eng. In: *Science (American Association for the Advancement of Science)* 370.6523 (2020), S. 1460–1463.
- [3] H. K. E Stadermann, E van den Berg und M. J Goedhart. „Analysis of secondary school quantum physics curricula of 15 different countries: Different perspectives on a challenging topic“. eng. In: *Physical review. Physics education research* 15.1 (2019), S. 1–25.
- [4] A. Einstein, B. Podolsky und N. Rosen. „Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?“ In: *Phys. Rev.* 47 (10 Mai 1935), S. 777–780. URL: <https://link.aps.org/doi/10.1103/PhysRev.47.777>.
- [5] J. S. Bell. „On the Einstein Podolsky Rosen paradox“. In: *Physics Physique Fizika* 1 (3 Nov. 1964), S. 195–200. URL: <https://link.aps.org/doi/10.1103/PhysicsPhysiqueFizika.1.195>.
- [6] Jürgen Audretsch. *Verschränkte Systeme : die Quantenphysik auf neuen Wegen*. ger. [Lehrbuch Physik]. Weinheim : Wiley-VCH, 2005.
- [7] J. Aczél und Z. Daróczy. *On Measures of Information and Their Characterizations*. eng. Bd. 115. Mathematics in science and engineering. Oxford: Elsevier Science & Technology, 1975.
- [8] Alain Aspect, Philippe Grangier und Gérard Roger. „Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell’s Inequalities“. In: *Phys. Rev. Lett.* 49 (2 Juli 1982), S. 91–94. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.49.91>.
- [9] John F. Clauser u. a. „Proposed Experiment to Test Local Hidden-Variable Theories“. In: *Phys. Rev. Lett.* 23 (15 Okt. 1969), S. 880–884. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.23.880>.
- [10] Michael A Nielsen. *Quantum computation and quantum information*. eng. 10th anniversary ed.. Cambridge [u.a.]: Cambridge Univ. Press, 2010.
- [11] B. S. Cirel’son. „Quantum generalizations of Bell’s inequality“. In: *Letters in Mathematical Physics* 4.2 (März 1980), S. 93–100.
- [12] John F. Clauser und Michael A. Horne. „Experimental consequences of objective local theories“. In: *Phys. Rev. D* 10 (2 Juli 1974), S. 526–535. URL: <https://link.aps.org/doi/10.1103/PhysRevD.10.526>.
- [13] Michał Horodecki, Paweł Horodecki und Ryszard Horodecki. „Separability of mixed states: necessary and sufficient conditions“. In: *Physics Letters A* 223.1 (1996), S. 1–8. URL: <https://www.sciencedirect.com/science/article/pii/S0375960196007062>.

- [14] Matthias Homeister. *Quantum Computing verstehen : Grundlagen - Anwendungen - Perspektiven*. ger. 5., aktualisierte und erweiterte Auflage. Computational Intelligence. Wiesbaden: Springer Vieweg, 2018.
- [15] Artur K. Ekert. „Quantum cryptography based on Bell’s theorem“. In: *Phys. Rev. Lett.* 67 (6 Aug. 1991), S. 661–663. URL: <https://link.aps.org/doi/10.1103/PhysRevLett.67.661>.
- [16] Franz Embacher. *Grundidee der Dekohärenz - Wieso sieht die Welt so klassisch aus?* URL: <https://homepage.univie.ac.at/franz.embacher/Quantentheorie/Dekohaerenz/> (besucht am 02.05.2021).
- [17] Richard P. Feynman. „Simulating physics with computers“. In: *International Journal of Theoretical Physics* 21.6 (Juni 1982), S. 467–488. URL: <https://doi.org/10.1007/BF02650179>.
- [18] P. W. Shor. „Algorithms for quantum computation: discrete logarithms and factoring“. In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, S. 124–134.
- [19] Lieven M. K. Vandersypen u. a. „Experimental Realization of an Order-Finding Algorithm with an NMR Quantum Computer“. In: *Physical Review Letters* 85.25 (Dez. 2000), S. 5452–5455. URL: <http://dx.doi.org/10.1103/PhysRevLett.85.5452>.
- [20] Lov K. Grover. „A Fast Quantum Mechanical Algorithm for Database Search“. In: *Annual ACM Symposium on Theory of Computing*. ACM, 1996, S. 212–219.
- [21] V Bouchiat u. a. „Quantum coherence with a single Cooper pair“. eng. In: *Physica scripta* 1998.1 (1998), S. 165.
- [22] IBM Research Blog. *On “Quantum Supremacy”*. URL: <https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/> (besucht am 02.05.2021).
- [23] John Preskill. „Quantum Computing in the NISQ era and beyond“. In: *Quantum* 2 (Aug. 2018), S. 79. URL: <https://doi.org/10.22331/q-2018-08-06-79>.
- [24] Bundesministerium für Bildung, Wissenschaft und Forschung (BMBWF). *Gesamte Rechtsvorschrift für Lehrpläne—allgemeinbildende höhere Schulen, Fassung vom 12.02.2021*. URL: <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10008568> (besucht am 02.05.2021).
- [25] F. Freistetter. *Quantenheilung hilft, denn alles ist Schwingung und Energie*. URL: https://www.derstandard.at/story/2000017159015/quantenheilung-hilft-denn-alles-ist-schwingung-und-energie?_blogGroup=1&ref=rec (besucht am 02.05.2021).
- [26] H. Schecker u. a. *Schülervorstellungen und Physikunterricht: Ein Lehrbuch für Studium, Referendariat und Unterrichtspraxis*. ger. Berlin, Heidelberg: Springer Berlin Heidelberg.
- [27] H. Schecker u. a. *Kircher, E. and Girwidz, R. and Häußler, P.* ger. 3. Aufl. 2015. Springer-Lehrbuch. Berlin, Heidelberg: Springer Berlin Heidelberg.

- [28] A. Brachner und R. Fichtner. „Quantenmechanik. Aus der Serie: Materialien für die Sekundarstufe II, Physik, H. Schroedel Verlag KG, Hannover 1980, 16,- DM“. ger. In: *Physik in unserer Zeit* 12.6 (1981), S. 194–194.
- [29] MILQ – Münchener Internetprojekt zur Lehrerfortbildung in Quantenmechanik. *Didaktische Konzepte - Übersicht über die Unterrichtsentwürfe aus der fachdidaktischen Literatur*. URL: <https://www.milq.info/spezialgebiete/didaktische-konzepte/> (besucht am 02.05.2021).
- [30] H. Fischler und M. Lichtfeldt. „Ein Unterrichtskonzept zur Einführung in die Quantenphysik“. In: *Physik in der Schule* 32 (1994), S. 276–280.
- [31] Richard P Feynman. *QED : die seltsame Theorie des Lichts und der Materie*. ger. Ungekürzte Taschenbuchausg., 3. Aufl.. Serie Piper 1562. München [u.a.]: Piper, 1997.
- [32] J. Küblbeck. „Modellbildung in der Physik, hrsg. v. Landesinstitut für Erziehung und Unterricht Stuttgart“. In: (1997).
- [33] Franz Bader. *Eine Quantenwelt - ohne Dualismus*. ger. 2. Dr.. Naturwissenschaftlicher Unterricht heute : Physik Sekundarbereich II. Hannover: Schroedel, 2000.
- [34] R. Müller und H. Wiesner. „Das Münchener Unterrichtskonzept zur Quantenmechanik“. In: *Physik in der Schule* 38 (2000), S. 126–134.
- [35] Wolfgang Dür. „Quanteninformationstheorie im Schulunterricht“. ger. In: *PhyDid B - Didaktik der Physik, DD 13.01* (2010).
- [36] Wolfgang Dür und Stefan Heusler. „Was man vom einzelnen Qubit über Quantenphysik lernen kann“. ger. In: *PhyDid A, Physik und Didaktik in Schule und Hochschule* 11.1 (2012), S. 1–16.
- [37] Wolfgang Dür und Stefan Heusler. „Was man von zwei Qubits über Quantenphysik lernen kann: Verschränkung und Quantenkorrelationen“. ger. In: *PhyDid A, Physik und Didaktik in Schule und Hochschule* 13.1 (2014), S. 11–34.
- [38] Corinne Manogue u. a. „Representations for a spins-first approach to quantum mechanics“. eng. In: *AIP Conference Proceedings*. Bd. 1413. 2012, S. 55–58.
- [39] A. Kohnle. *The Quantum Mechanics Visualisation Project*. URL: <https://www.st-andrews.ac.uk/physics/quvis/> (besucht am 02.05.2021).
- [40] A Kohnle u. a. „Enhancing student learning of two-level quantum systems with interactive simulations“. eng. In: *American journal of physics* 83.6 (2015), S. 560–566.
- [41] Rodger Bybee. *The BSCS 5E Instructional Model: Creating Teachable Moments*. eng. Arlington, VA: National Science Teachers Association, 2015.
- [42] D. Schaubmair. *Unterrichtsmaterialien: Mit Qubits zur Quantenphysik*. URL: https://drive.google.com/drive/folders/1EjSI_uYy6b5vvDP0gq4Fo07EiHc3KjYc?usp=sharing (besucht am 02.05.2021).

- [43] Daniel V. Schroeder und Thomas A. Moore. „A computer-simulated Stern–Gerlach laboratory“. In: *American Journal of Physics* 61.9 (Sep. 1993), S. 798–805. URL: <http://dx.doi.org/10.1119/1.17172>.
- [44] C. Simondi. *ID Quantique and SK Telecom announce the world’s first 5G smartphone equipped with a Quantum Random Number Generator (QRNG) chipset*. URL: <https://www.idquantique.com/id-quantique-and-sk-telecom-announce-the-worlds-first-5g-smartphone-equipped-with-a-quantum-random-number-generator-qrng-chipset/> (besucht am 02.05.2021).

Anhang

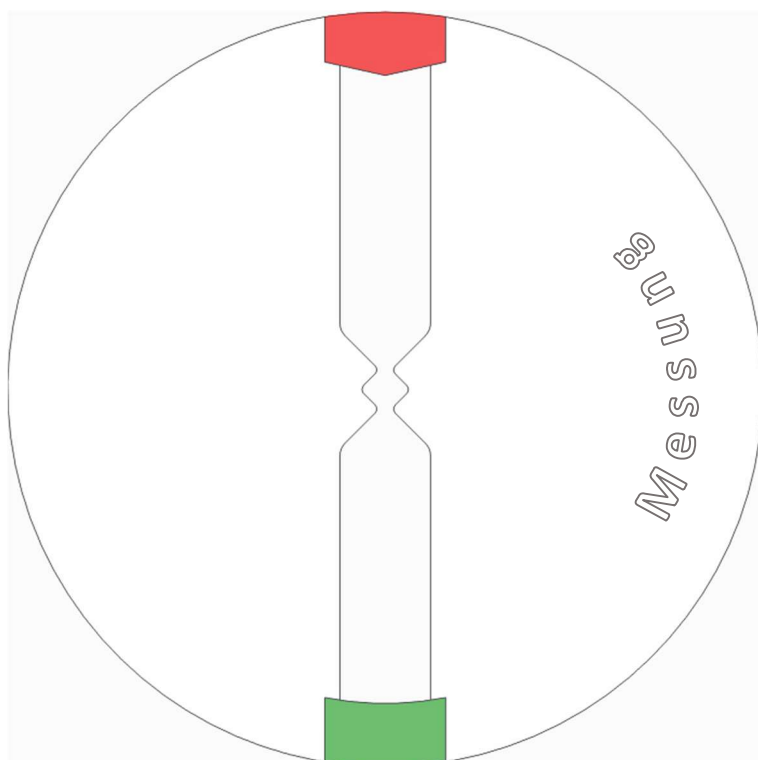
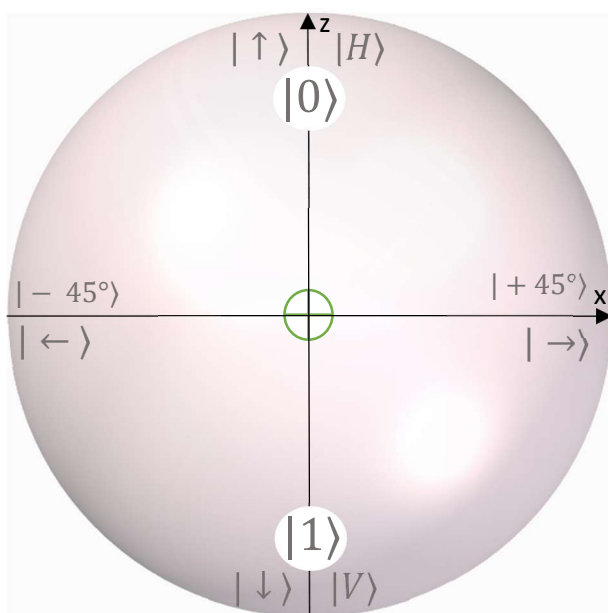
Blochscheibe

Um Darstellungen und Operationen an Qubits handgreiflicher zu gestalten, kann Schüler:innen eine *Blochscheibe* zur Verfügung gestellt werden. Diese besteht aus einer Blochkugel, deren x-z-Ebene betrachtet wird, und einem Zeiger, der einen beliebigen Zustand darin darstellen kann. Die Blochkugel enthält zudem Beschriftungen für Zustände, die Polarisation oder Spin beschreiben sowie die verallgemeinerten Bezeichnungen $|0\rangle$ und $|1\rangle$.

In untenstehender Kugel und im Zeiger sind Kreise angedeutet, die zur jeweiligen Befestigung dienen sollen, beispielsweise können handelsübliche Musterklammern bzw. Rundkopfkammern hierfür verwendet werden.

Ebenso ist eine Visualisierung des Messvorgangs in Form eines Schlitzes enthalten, wobei sich im Zentrum eine Positionierungshilfe befindet. Die roten und grünen Enden sollen dabei zur visuellen Hilfe einen Stern-Gerlach-Apparat andeuten, aber ohne eine konkretere Bezeichnung mit Nord- und Südpol auskommen, um eine verallgemeinerte Messung unabhängig der physikalischen Realisierung eines Qubits darstellen zu können.

Zum Ausdrucken wird empfohlen, festes Papier zu verwenden oder die ausgedruckten Exemplare zu laminieren, um eine höhere Stabilität zu gewährleisten.



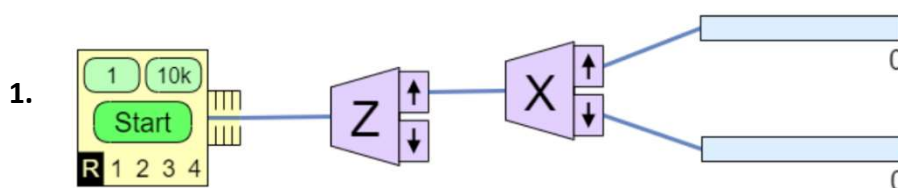


Superposition & Messung



Eine **Messung** _____

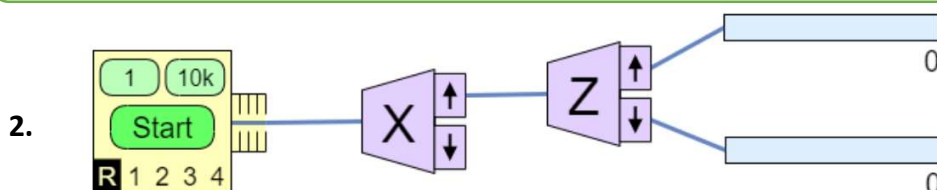
**Nutze die Simulation und baue folgende Anordnungen nach.
Beschrifte an den Ausgängen der Apparate die Zustände!**



→ Kann man für einzelne Teilchen vorhersagen, welches Messergebnis eintritt?

→ Was kann man über die gesamte Verteilung aussagen?

Der Zustand $|\uparrow\rangle$ „besteht“ ...



→ Was fällt im Vergleich zur vorherigen Anordnung auf?

Der Zustand $|\rightarrow\rangle$ „besteht“ ...

Man sagt, vor einer Messung _____



Nur zwei Möglichkeiten: Supraleiter



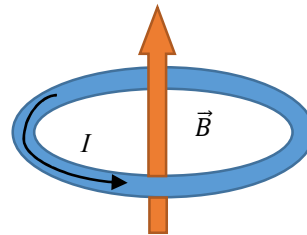
Üblicherweise besitzen elektrische Leitungen einen Widerstand, sodass elektrischer Strom nicht völlig verlustfrei fließen kann. *Supraleiter* besitzen jedoch die Eigenschaft, dass sie bei sehr tiefen Temperaturen ihren Widerstand verlieren und elektrischer Strom damit auch keine Verluste erfährt.

Supraleiter

Betrachtet man einen supraleitenden Ringleiter, kann durch ein äußeres Magnetfeld *Strom induziert* werden. Durch die verlustfreie Leitung ist nur eine kurze Beeinflussung notwendig, um einen kontinuierlichen Stromfluss zu gewährleisten.

Induktion

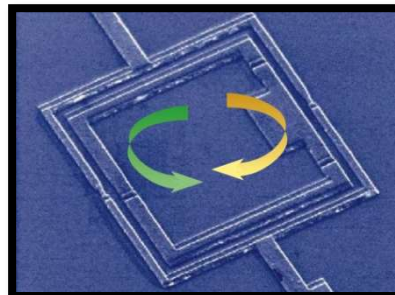
Da bewegte Ladungen ihrerseits ein Magnetfeld erzeugen, entsteht durch den kontinuierlichen Stromfluss im Ring ein Magnetfeld, dessen Richtung von jener des Stromflusses abhängt (im Uhrzeigersinn oder gegen den Uhrzeigersinn).



bewegte
Ladungen

Durch geschickte Manipulation mit einem äußeren Magnetfeld ist es jedoch möglich, eine Superposition von Stromrichtungen, und damit auch eine Superposition von Magnetfeldern zu erzeugen.

Dies kann sich in Messungen zeigen: Präpariert man mehrere solcher Ringleiter auf dieselbe Art und Weise, zeigen Messungen mit einer Wahrscheinlichkeit von je 50% ein Magnetfeld in die eine oder andere Richtung.



Da das hier auftretende Magnetfeld äußerst schwach ist, braucht es sensible Messgeräte dafür. Dies lässt sich mit einem sogenannten *SQUID* (*superconducting quantum interference device*) bewerkstelligen. Diese Technologie wird benutzt, um beispielsweise bei Untersuchungen von Hirnströmen äußerst schwache Magnetfelder zu untersuchen. Dabei wird durch das zu messende Magnetfeld Strom im Messgerät induziert, und abhängig davon kann auf das vorliegende Magnetfeld und damit auf die Richtung des Stromflusses im Ringleiter geschlossen werden.

SQUID

Notiere dir folgende Kernpunkte:

- Wovon existiert eine Superposition?
- Wie stellt man einen Anfangszustand her?
- Wie wird der Zustand beeinflusst?
- Was/wie wird gemessen?

Wenn du Zeit hast, suche dir zu den Begriffen am Rand weitere Informationen!



Nur zwei Möglichkeiten: Energieniveaus



Die Elektronen in Atomen können verschiedene *Energieniveaus* einnehmen, dies kann man sich beispielsweise anhand des Bohr'schen Atommodells mit verschiedenen Kreisbahnen um den Atomkern, oder im Orbitalmodell mit unterschiedlichen Orbitalen vorstellen.

Energie-
niveaus

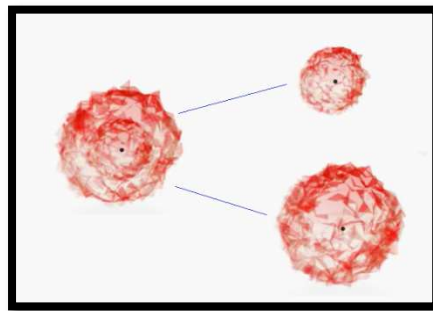
Einzelne Atome kann man z.B. in Form von Ionen in einer sogenannten *Paul-Falle* stabilisieren und untersuchen. Dabei werden die Ionen durch äußere elektrische Felder von passend platzierten Elektroden an einem Ort gehalten. Um ein Ion nicht nur an einem Platz zu halten, sondern auch dessen Bewegungsenergie (in Form von Schwingungen) zu verringern, kann man diese mithilfe von Lasern in einen möglichst ruhigen Bewegungszustand versetzen, dies nennt man *Laserkühlung*.

Paul-Falle

Laserkühlung

Infolgedessen werden zwei Energiezustände von Elektronen betrachtet: Mittels eines Lasers können Elektronen in ein höheres Niveau gehoben werden und unter Aussendung eines Photons wieder in den Grundzustand zurückkehren.

Durch Anregungen mit einem Laser (nun mit anderer Frequenz als bei der Kühlung) kann eine Superposition des Grundzustands und des angeregten Zustands erzeugt werden, welcher bei einer Messung mit einer Wahrscheinlichkeit von je 50% einen der beiden Zustände annimmt.



Auch die Messung geschieht durch einen Laserpuls, wobei man sich hierunter vorstellen kann, dass ein Photon mit bestimmter Frequenz ausgesendet wird. Bis zur Wechselwirkung von diesem Photon und dem zu messenden Ion befindet sich das Letztere in Superposition, erst durch die Interaktion mit dem Photon geht es in einen von beiden Zuständen über:

Wenn es dabei in den Grundzustand übergeht, wird das Photon vom Ion absorbiert, ein Elektron geht in den erhöhten Zustand über und emittiert wieder ein Photon, womit es wieder in den Grundzustand übergeht. Wird dieses emittierte Photon mit einem Photodetektor an geeigneter Stelle detektiert, bedeutet dies, dass es zu Beginn im Grundzustand vorlag. Wird ein solches Photon aber nicht detektiert, weiß man umgekehrt, dass das Ion im erhöhten Zustand vorlag.

Absorption &
Emission

Notiere dir folgende Kernpunkte:

- Wovon existiert eine Superposition?
- Wie stellt man einen Anfangszustand her?
- Wie wird der Zustand beeinflusst?
- Was/wie wird gemessen?

Wenn du Zeit hast, suche dir zu den Begriffen am Rand weitere Informationen!

Abbildungen aus: Quantum Made Simple – State Superposition and Decoherence,
<http://toutestquantique.fr/en/superposition/>



Nur zwei Möglichkeiten: Photonen



Die Polarisation von Licht beschreibt die Richtung der elektromagnetischen Schwingung. Licht kann z.B. linear oder zirkular polarisiert sein, wobei hier nur linear polarisiertes Licht betrachtet wird, bei welchem die Schwingung in einer Ebene stattfindet.

linear
polarisiert

Man kann Licht eine anfängliche Polarisation vorgeben, indem man beispielsweise einen Polarisationsfilter in vertikaler Richtung verwendet: In der Vorstellung von Photonen sind nach dem Filter nur noch Photonen mit vertikaler Polarisation vorhanden, man spricht vom Zustand $|V\rangle$. Der dazu „gegenteilige“ Zustand wird mit $|H\rangle$ bezeichnet, was für „horizontal“ steht.

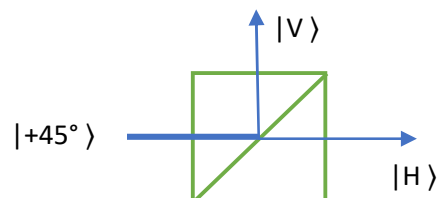
Polarisa-
tionsfilter

Beim Durchgang von linear polarisiertem Licht durch ein optisch aktives Medium (z.B. Kristalle) lässt sich die Polarisation verändern, womit eine Superposition der beiden Zustände erreicht werden kann. Dies lässt sich anschaulich durch eine Drehung der Polarisationsebene deuten. Dreht man die Ebene um 45° , lässt sich eine gleichgewichtete Superposition der Zustände $|V\rangle$ und $|H\rangle$ erzeugen.

Optisch
aktives
Medium

Mit einem Strahlteiler kann man dann eine Messung vornehmen: Photonen sind unteilbar, weswegen diese am Strahlteiler nicht in ihre $|V\rangle$ - und $|H\rangle$ -Anteile zerlegt werden können, wie man dies vielleicht von klassischer Wellenoptik gewohnt ist. Vielmehr erfolgt für jedes Photon am Strahlteiler eine Entscheidung, und mit je einer Wahrscheinlichkeit von 50% wird in diesem Fall dabei entweder ein vertikal oder horizontal polarisiertes Photon gemessen.

Strahlteiler



Wiederholt man dies für viele Photonen, ergibt sich das gewohnte Bild einer Aufteilung von Strahlen und Intensitäten.

Polarisationsfilter können dabei ebenso als Messgerät interpretiert werden: Entweder gelangt das Photon hindurch und besitzt den Zustand, der von der Messrichtung abhängt, oder es wird im anderen Fall *absorbiert* (im Gegensatz zum Strahlteiler, der im anderen Fall *reflektiert*).

Notiere dir folgende Kernpunkte:

- Wovon existiert eine Superposition?
- Wie stellt man einen Anfangszustand her?
- Wie wird der Zustand beeinflusst?
- Was/wie wird gemessen?

Wenn du Zeit hast, suche dir zu den Begriffen am Rand weitere Informationen!

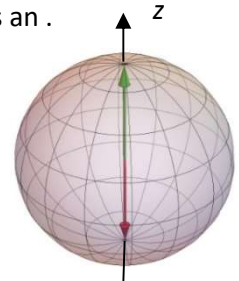


Zustände in Blochkugeln



In einer **Blochkugel** können Systeme veranschaulicht werden, die bei einer Messung zwei Ergebnisse haben können. Der **Blochvektor** in der Kugel zeigt dann den Zustand dieses Systems an.

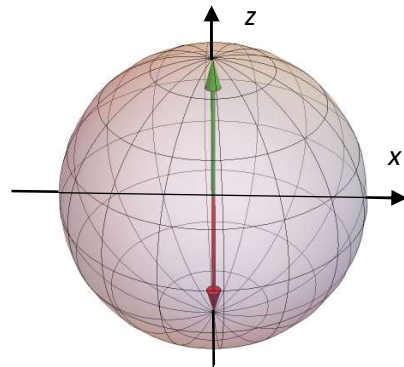
Die Zustände entlang der z-Achse sind „gegensätzliche“ Ergebnisse einer entsprechenden Messung, für *Spin-Messungen* (von beispielsweise Neutronen) könnten dies _____ und _____ sein, geht es um die Messung der *Polarisation von Photonen*, könnten diese mit _____ und _____ beschriftet werden.



- **Superposition**

Wie sieht eine gleichgewichtete Superposition der Zustände entlang der z-Achse aus? Wie sieht eine beliebige andere Superposition aus?

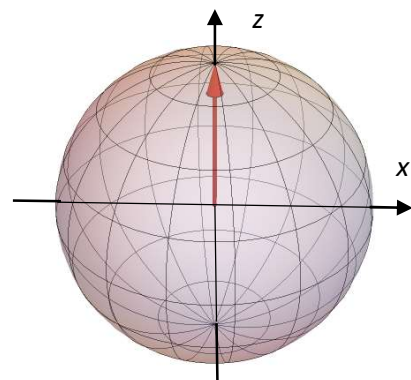
Was entspricht Zuständen entlang der x-Achse für Spin eines Elektrons oder der Polarisation von Photonen?



- **Manipulation**

Was entspricht einer Manipulation eines Zustands in der Blochkugel? Erkläre und zeichne ein!

Wie kann man solche Manipulationen am Spin eines Protons und der Polarisation eines Photons durchführen?

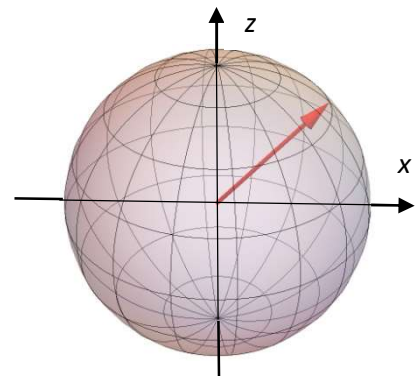


- **Messung**

Wie sehen mögliche Zustände nach einer Messung in der z-Achse für folgenden Zustand aus?

Welches Ergebnis tritt öfter auf?

Wie würde sich dies bei einer Messung in der x-Achse verhalten? (z.B. bei einer Spin-Messung eines Neutrons)





Mehr zur Blochkugel



Aufgabe 1

Stell dir vor, du bekommst viele Teilchen aus einer Quelle, die hinsichtlich einer Eigenschaft als Qubits beschrieben werden können, und alle gleich präpariert sind, also alle im selben Zustand vorliegen. Angenommen, der Zustand ist unbekannt: Wie kann man ihn herausfinden?

Aufgabe 2

Stell dir nun vor, die Quelle liefert nicht alle Teilchen im gleichen Zustand, sondern zwei verschiedene Zustände. Die Quelle „wählt“ dabei zufällig aus zwei verschiedenen Zuständen, die beobachtende Person weiß aber nicht, wann sie Zustand 1 oder Zustand 2 aussendet.
Kann man die beiden Zustände herausfinden?

Aufgabe 3

Mathematisch kann man die Superposition von Zuständen (hier für die Beschreibung von Spin) folgendermaßen angeben:

$$|\psi\rangle = \alpha \cdot |\uparrow\rangle + \beta \cdot |\downarrow\rangle$$

Die beiden Zahlen α und β geben dabei die „Art“ der Überlagerung an, so kann man die Wahrscheinlichkeit, bei der Messung den Zustand $|\uparrow\rangle$ zu erhalten, mit $|\alpha|^2$ ermitteln, der Zustand $|\downarrow\rangle$ wird mit der Wahrscheinlichkeit $|\beta|^2$ festgestellt.

In welchen Bereichen der Blochkugel ist α betragsmäßig größer als β ?

Was muss $|\alpha|^2 + |\beta|^2$ ergeben?

Aufgabe 4

Bis zu diesem Punkt wurde eigentlich nur ein Querschnitt der Blochkugel verwendet: die Ebene, die von x- und z-Achse aufgespannt wird.

Tatsächlich lassen sich die bisherigen Regeln auf Blochvektoren der gesamten Kugel ausweiten –
überlege, was sich daran ändert/gleich bleiben könnte!

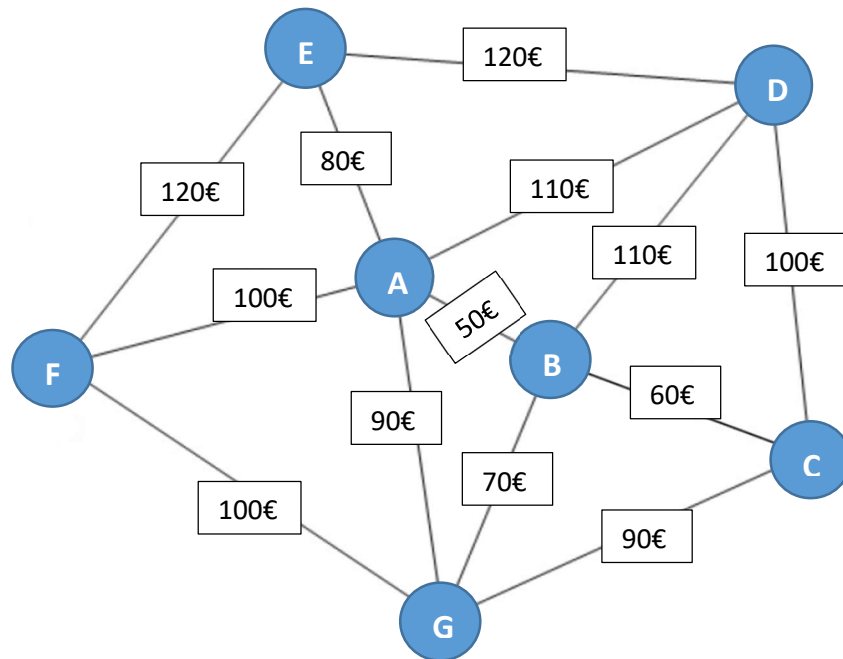
(Übrigens: wenn man die x-z-Ebene verlässt, werden für α und β *komplexe Zahlen* verwendet.)



Lösungssuche



1. Eine Person möchte eine **Rundreise** mit dem Zug durch **sieben Städte** planen, die Preise für die verschiedenen Strecken fallen dabei unterschiedlich aus.



In welcher **Reihenfolge** sollten die Städte besucht werden, wenn **möglichst wenig Geld** dafür ausgegeben werden soll und **jede Stadt nur einmal** besucht werden darf??
(Der Startpunkt ist beliebig, aber die Reise muss wieder an diesem Punkt enden.)

2. Zerlege die Zahlen **15**, **91**, **391** und **1073** in Primfaktoren!

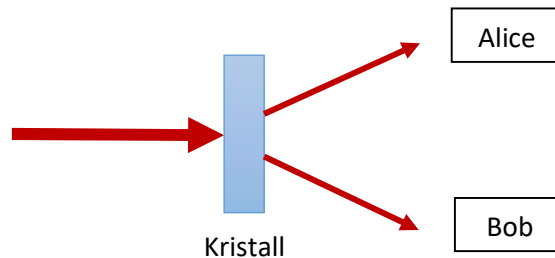


Alice & Bob



Schickt man ein Photon durch einen Kristall, können dadurch Photonenpaare (mit je halber Energie des ursprünglichen Photons) entstehen. Von besonderem Interesse sind nun Photonenpaare, die in einem bestimmten Bereich aus dem Kristall austreten (dazu später mehr).

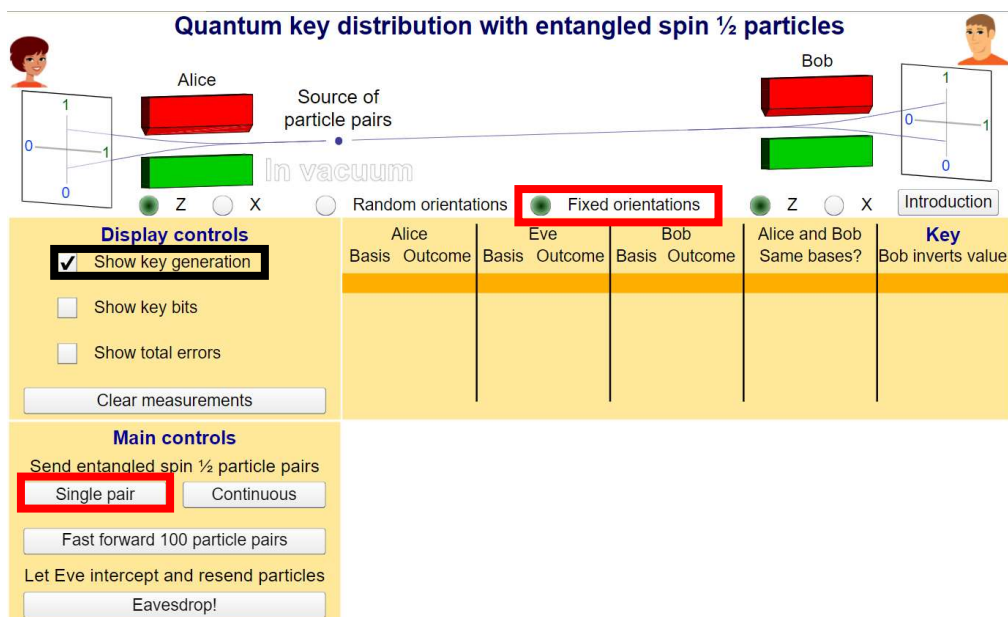
Zwei Experimentator:innen, genannt Alice und Bob, untersuchen nun diese Photonenpaare.



1. Wenn man beide Photonen in Form von Qubits beschreibt, deren Polarisation Alice und Bob (in horizontaler/vertikaler Richtung) messen würden, wie viele Möglichkeiten für einen Versuchsausgang gibt es insgesamt?
2. Es stellt sich heraus, dass Alice zu einer Wahrscheinlichkeit von je 50% entweder horizontal oder vertikal polarisierte Photonen misst, ebenso sieht es bei Bob aus. Wie könnten diese Zustände in der Blochkugel aussehen?
3. Alice und Bob beschließen nun, einige Messungen in anderen, aber stets gleichen Messrichtungen zu unternehmen (z.B. $\pm 45^\circ$). Jedes Mal zeigt sich eine 50/50-Verteilung. Kann dieser Zustand mit einem Blochvektor, wie wir sie bisher behandelt haben, dargestellt werden?
4. Alice und Bob führen viele solcher Messungen in der ursprünglichen Richtung (H/V) durch und beschließen, ihre Ergebnisse in einer Liste festzuhalten und zu vergleichen. Dabei bemerken sie, dass nur jeweils *gegengleiche Paarungen von Messergebnissen* auftreten. Welche Zustände bzw. Paare von Zuständen werden also gemessen?
5. **Zusatz:** Der Zustand von zwei Qubits in gleichgewichteter Superposition wurde bereits in einer vorhergehenden Einheit mathematisch formuliert. Anhand der möglichen Messergebnisse bei Alice und Bob, wie könnte dieser Zustand nun mathematisch formuliert werden?

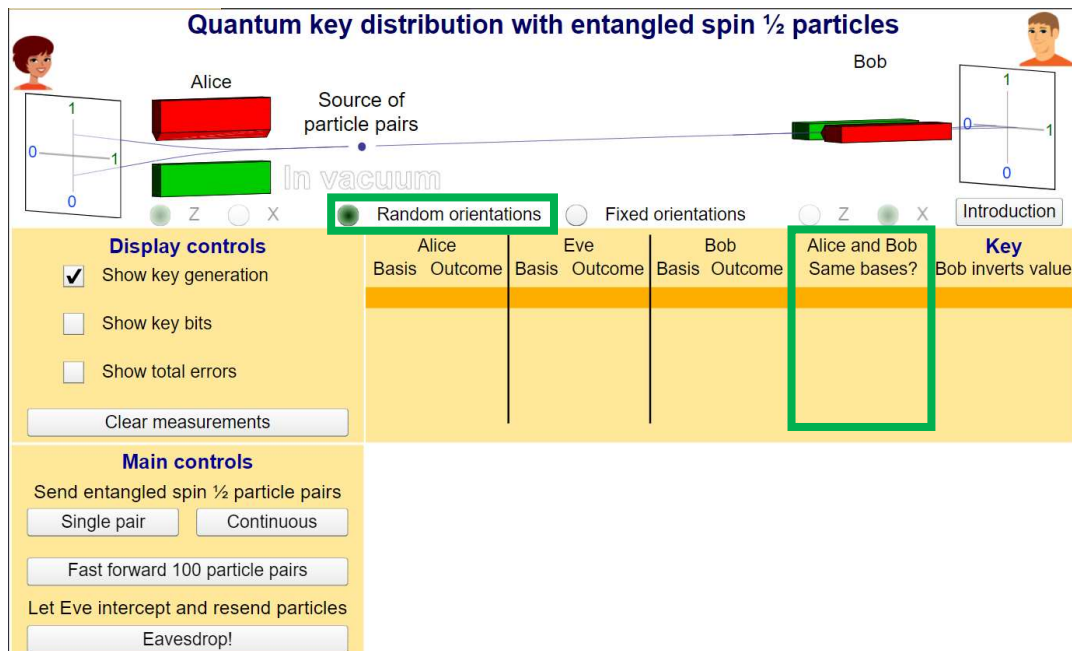
Für die folgenden Aufgaben setze in der Simulation zunächst ein Häkchen bei **Show key generation**, um die einzelnen Messergebnisse mitzuverfolgen, die restlichen Anzeigemöglichkeiten brauchst du hier nicht. Mit *Clear measurements* kannst du Ergebnisse aus durchgeführten Versuchen später wieder löschen.

1. Wähle, wie im Bild zu erkennen, **Fixed Orientations** aus. Dadurch kannst du selbst steuern, ob bei Alice und Bob Messungen in z- oder x-Richtung durchgeführt werden. Mit dem Befehl **Single pair** kannst du nun einzelne verschränkte Paare messen. Wie kann durch viele solcher Paare ein Schlüssel erzeugt werden, den nur Alice und Bob besitzen?



2. Mit dem Button **Eavesdrop!** (*belausche!*) schaltet sich nun – ohne dass Alice und Bob davon etwas mitbekommen – Eve dazwischen, um die beiden zu belauschen und unbemerkt den Schlüssel herauszufinden. Kontrolliere: Gelingt ihr Vorhaben wirklich?

3. Alice und Bob beschließen, ihre Strategie zu ändern und wechseln ihre Messungen zufällig. Wähle dafür **Random orientations** in der Simulation, und drücke außerdem erneut **Eavesdrop!**, um Eve wieder kurzzeitig aus dem Spiel zu nehmen. Nun führen Alice und Bob nicht immer die gleichen Messungen durch und bekommen dadurch auch nicht immer die entsprechenden gegengleichen Ergebnisse. Allerdings können sie nach der Messung besprechen, welche der Richtungen sie gewählt haben, und immer wenn sie zufälligerweise die gleiche Messung durchgeführt haben (siehe Spalte **Alice and Bob same bases?**), können sie ein Bit für den Schlüssel notieren. Führe einige Messungen in der Simulation durch und kontrolliere anhand der Spalten!



4. Schalte nun erneut **Eve** dazu und beobachte, was passiert:
- Kann Eve noch immer ohne weiteres belauschen und den Schlüssel herausfinden? Was bewirkt ihre (ebenfalls zufällige) Wahl einer Messung?
 - Für den Schlüssel von Bedeutung sind ohnehin nur jene Messungen, in denen Alice und Bob zufällig gleiche Richtungen gewählt haben. Erhalten Alice und Bob noch immer einen gültigen Schlüssel bei gleicher Wahl?
 - Wie könnten Alice und Bob einem möglichen Lauschangriff auf die Schliche kommen?



Spin

1

1

Zur Quantenphysik...

„Denn wenn man nicht zunächst über die Quantentheorie entsetzt ist, kann man sie doch unmöglich verstanden haben.“ - *Niels Bohr*

„Es gab eine Zeit, als Zeitungen sagten, nur zwölf Menschen verstanden die Relativitätstheorie. Ich glaube nicht, dass es jemals eine solche Zeit gab. Auf der anderen Seite denke ich, es ist sicher zu sagen, niemand versteht Quantenmechanik.“ - *Richard Feynman*

2

2

Neutronenquelle

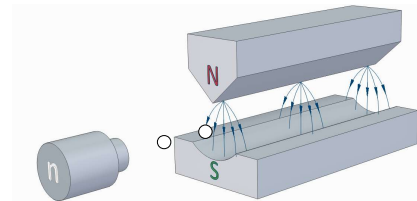


- Neutronen:
- keine elektrische Ladung
- als Produkt bei Kernzerfällen

3

3

Neutronen in einem Magnetfeld



- Neutronen werden von einem Magnetfeld...

...beeinflusst

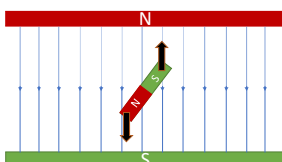
...nicht beeinflusst

Auflösung folgt!

4

4

Magnet in homogenem Magnetfeld



Der Magnet bleibt am selben Ort, aber er dreht sich!

- Der Magnet im **homogenen** Magnetfeld...

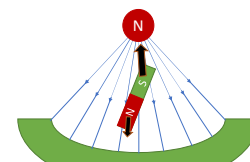
...wandert zu einem der Pole

...bleibt am selben Ort

5

5

Magnet in inhomogenem Magnetfeld



Die beiden Kräfte heben sich nicht auf, auf den Magneten wirkt eine **Gesamtkraft**: Er wandert zu einem der Pole!

- Der Magnet im **inhomogenen** Magnetfeld...

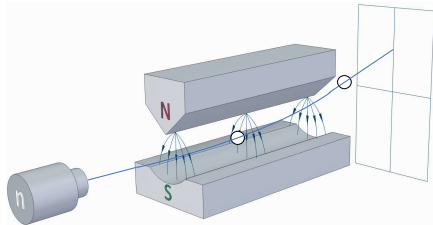
...wandert zu einem der Pole

...bleibt am selben Ort

6

6

Auflösung: Neutronen im inhomogenen Magnetfeld



7

7

Neutronen und Spin

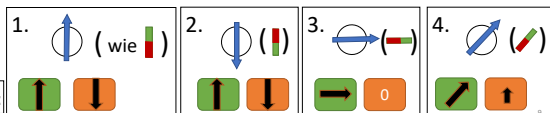
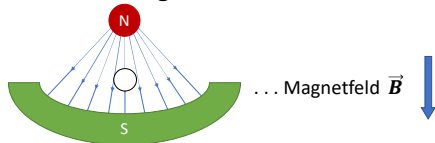


- **Spin** ist eine Eigenschaft von Teilchen, die eine Wechselwirkung mit Magnetfeldern ermöglicht

8

8

Beispiele: Welche Ablenkung wäre zu erwarten?



9

9

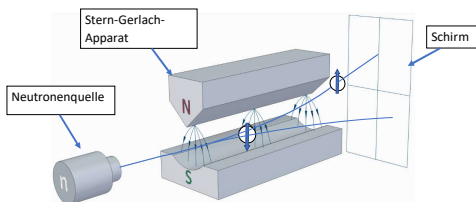
Spin – Zusammenfassung:

- **Spin** ist eine Eigenschaft von Teilchen, die eine Wechselwirkung mit Magnetfeldern ermöglicht.
- Spin kann mit einem **Stern-Gerlach-Apparat** gemessen werden, da Teilchen in einem inhomogenen Magnetfeld abgelenkt werden. Die Ablenkung findet dabei nur in Richtung des Magnetfelds statt! Der Auftreffpunkt gibt Auskunft über den Spin.
- Nicht nur Neutronen, auch Elektronen und Protonen kann ein Spin zugeordnet werden.

10

10

Stern-Gerlach-Apparat



- Teilchen werden nur in Richtung des Magnetfelds abgelenkt!

11

11

Spin ist keine Drehung

- Historisch:
Vorstellung einer Drehung von Elektronen in Form von Kugeln
- Stellt man sich die Ladung an der Oberfläche verteilt vor, würde durch den Ringstrom ein magnetisches Moment entstehen (ähnlich wie ein Elektromagnet)
- ABER: Ladung am Umfang müsste sich überlichtschnell bewegen!!



12

12

Spin in alltäglichen Objekten?

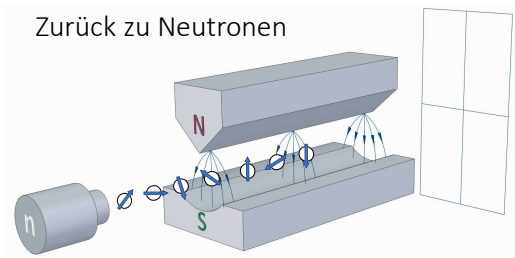


- Gegenseitige Aufhebung von Spin in makroskopischen Objekten

13

13

Zurück zu Neutronen



- Wenn der Spin der Neutronen völlig zufällig orientiert ist: Welche Verteilung könnte sich am hinteren Schirm ergeben?

14

14

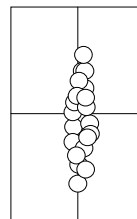
<https://www.youtube.com/watch?v=rg4Fnag4V-E>

15

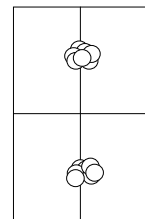
15

Verteilung bei Spin-Messung von Neutronen

Klassische Erwartung



Tatsächliche Messung



16

16

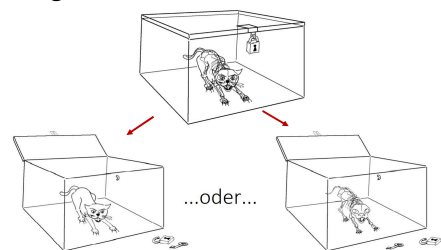
Superposition & Messung



17

17

Schrödingers Katze

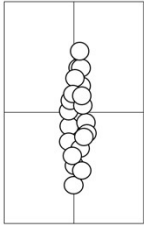


18

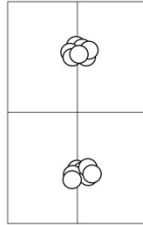
18

Vom letzten Mal...

Klassische Erwartung



Tatsächliche Messung

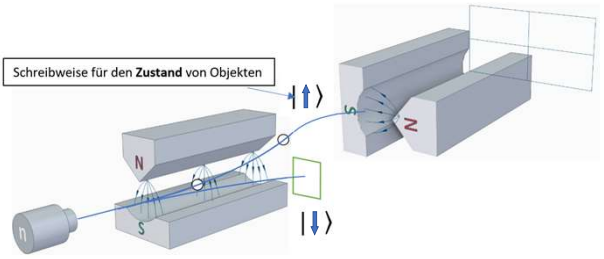


19

19

Nun:

Schreibweise für den Zustand von Objekten



20

20

<https://physics.weber.edu/schroeder/software/Spins.html>

21

21

Arbeitsblatt: Superposition & Messung

22

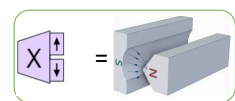
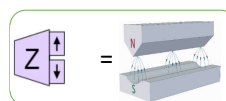
22

Eine **Messung** verändert den Zustand von Teilchen. Dadurch kann man nicht auf den Zustand eines Teilchens vor der Messung rückschließen.

23

23

Bearbeite die Aufgaben am Arbeitsblatt mithilfe der Simulation



24

24

Erkenntnisse

- Das Messergebnis bei einem einzelnen Teilchen lässt sich nicht vorhersagen
- Aber: Die Gesamtverteilung lässt sich vorhersagen (Vergleiche: Münzwurf)

25

25



Der Zustand $|\uparrow\rangle$ „besteht“ zu gleichen Teilen aus den Zuständen $|\rightarrow\rangle$ und $|\leftarrow\rangle$.

Der Zustand $|\rightarrow\rangle$ „besteht“ zu gleichen Teilen aus den Zuständen $|\uparrow\rangle$ und $|\downarrow\rangle$.

26

26

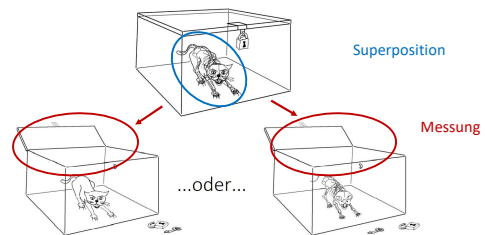
Man sagt, vor einer Messung befinden sich Teilchen in einer Überlagerung bzw. **Superposition** jener Zustände, die gemessen werden können.

27

27



Superposition & Messung



28

28



Qubits & Realisierungen

29

29



Auftrag: Nur zwei Möglichkeiten

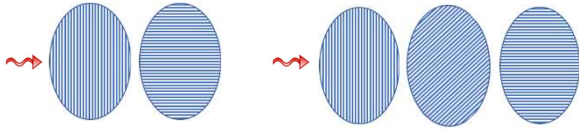
- Lies den dir zugeteilten Text, **beantworte die Fragen** und informiere dich über **Begriffe am Rand** weiter.
- Besprecht in **Gruppen mit dem gleichen Text** (je zu dritt), was ihr herausgefunden habt und vergleicht.
- Besprecht in **Gruppen mit unterschiedlichen Texten** (je zu dritt) und erklärt gegenseitig, was ihr herausgefunden habt.



30

30

Polarisationsfilter - Messung



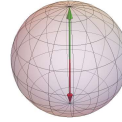
Zur Erinnerung:
Eine Messung verändert den Zustand eines Objekts

31

31

Zwei-Level-Systeme

- Bezeichnung: **Qubits** (*quantum bits*)
- Darstellungsmöglichkeit mit **Blochkugel** und **Blochvektoren**



Vektoren in entgegengesetzte Richtungen kennzeichnen verschiedene Ergebnisse einer Messung, z.B. $|\uparrow\rangle$ und $|\downarrow\rangle$ (wenn es um Spin geht) oder $|H\rangle$ und $|V\rangle$ (wenn es um Polarisationen geht) usw...

- **Achtung:**
Nur zu Anschauungszwecken, Pfeile haben keine „reale Entsprechung“

32

32

Ψ

Zustände in der Blochkugel

33

33

Daumen hoch/runter

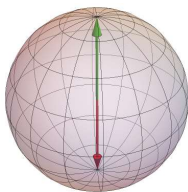
- Meinung zu ...
- Meinung positiv beeinflussen
- Empfehlung abgeben: ja oder nein?



34

34

Erarbeite: Zustände in Blochkugeln



35

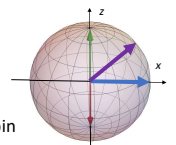
35

Superposition

Wie sieht eine gleichgewichtete Superposition der Zustände entlang der z-Achse aus?
Wie sieht eine beliebige andere Superposition aus?

Was entspricht Zuständen entlang der x-Achse für Spin eines Elektrons oder der Polarisation von Photonen?

Polarisation: $|+45^\circ\rangle$ und $|-45^\circ\rangle$
Spin: $|\rightarrow\rangle$ und $|\leftarrow\rangle$



36

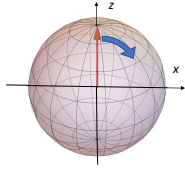
36

Manipulation

Was entspricht einer Manipulation eines Zustands in der Blochkugel?
Erkläre und zeichne ein!

Wie kann man solche Manipulationen am Spin eines Protons und der Polarisation eines Photons durchführen?

Polarisation: optisch aktives Medium
Spin: homogenes Magnetfeld



37

37

Messung

Wie sehen mögliche Zustände nach einer Messung in der z-Achse für folgenden Zustand aus?

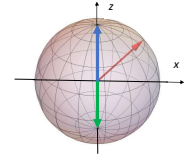
Welches Ergebnis tritt öfter auf?

$|1\rangle$ tritt öfter auf als $|1\rangle$

Wie würde sich dies bei einer Messung in der x-Achse verhalten?

(z.B. bei einer Spin-Messung eines Neutrons)

$| \rightarrow \rangle$ tritt öfter auf als $| \leftarrow \rangle$



38

38

Aufgabenblatt: Mehr zur Blochkugel

39

39

Aufgabe 1

Stell dir vor, du bekommst viele Teilchen aus einer Quelle, die hinsichtlich einer Eigenschaft als Qubits beschrieben werden können, und alle gleich präpariert sind, also alle im selben Zustand vorliegen. Angenommen, der Zustand ist unbekannt: Wie kann man ihn herausfinden?

→ Durch geeignete Wahl von Messungen kann der Zustand gefunden werden. Hat man z.B. eine Messrichtung gefunden, für welche 100% der Messergebnisse einen einzigen „Wert“ liefern, ist der Zustand gefunden!

40

40

Aufgabe 2

Stell dir nun vor, die Quelle liefert nicht alle Teilchen im gleichen Zustand, sondern zwei verschiedene Zustände. Die Quelle „wählt“ dabei zufällig aus zwei verschiedenen Zuständen, die beobachtende Person weiß aber nicht, wann sie Zustand 1 oder Zustand 2 aussendet.

Kann man die beiden Zustände herausfinden?

→ Nein, eine Messung wie beim vorherigen Beispiel lässt sich für verschiedene Zustände nicht finden!
→ „Zustandsgemisch“

41

41

Aufgabe 3

Mathematisch kann man die Superposition von Zuständen (hier für die Beschreibung von Spin) folgendermaßen angeben:

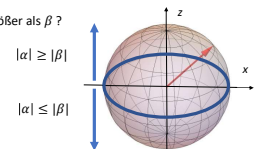
$$|\psi\rangle = \alpha \cdot |1\rangle + \beta \cdot |1\rangle$$

Die beiden Zahlen α und β geben dabei die „Art“ der Überlagerung an, so kann man die Wahrscheinlichkeit, bei der Messung den Zustand $|1\rangle$ zu erhalten, mit $|\alpha|^2$ ermitteln, der Zustand $|1\rangle$ wird mit der Wahrscheinlichkeit $|\beta|^2$ festgestellt.

In welchen Bereichen der Blochkugel ist α betragsmäßig größer als β ?

Was muss $|\alpha|^2 + |\beta|^2$ ergeben?

$$\rightarrow |\alpha|^2 + |\beta|^2 = 1$$



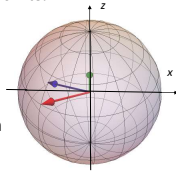
42

42

Aufgabe 4

Bis zu diesem Punkt wurde eigentlich nur ein Querschnitt der Blochkugel verwendet: die Ebene, die von x- und z-Achse aufgespannt wird. Tatsächlich lassen sich die bisherigen Regeln auf Zeiger der gesamten Kugel ausweiten – überlege, was sich daran ändert/gleich bleiben könnte!
(Übrigens: wenn man die x-z-Ebene verlässt, werden für α und β komplexe Zahlen verwendet.)

- Manipulationen sind Drehungen im Raum
- Messungen in beliebiger Raumrichtung möglich

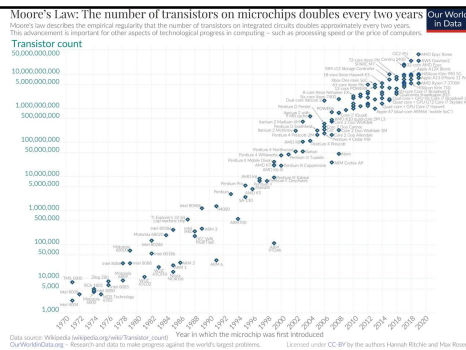


43



Mehrere Qubits

44



45

Aufgabe: viele Qubits

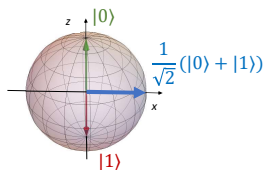
- Wieviele mögliche Messergebnisse gibt es bei 2 Qubits?
- Wieviele Ergebnisse gibt es bei 3, 4 und n Qubits?
- Wie hoch ist jeweils die Wahrscheinlichkeit, ein bestimmtes Gesamtergebnis (z.B. $|\uparrow\rangle|\downarrow\rangle$) bei der Messung zweier Qubits, hier mit Spin) zu erhalten, wenn bei den einzelnen Qubits beide Ergebnisse gleichwahrscheinlich sind?

(Hinweis: Überlege anhand von Münzen!)

46

Zusammenfassung:

Allgemeine Schreibweise:



Anzahl der Qubits	Mögliche Zustände nach Messung	Anzahl möglicher Messergebnisse
1	$ 0\rangle, 1\rangle$	2
2	$ 00\rangle, 01\rangle, 10\rangle, 11\rangle$	4
3	$ 000\rangle, 001\rangle, \dots, 111\rangle$	$8=2^3$
4	$ 0000\rangle, 0001\rangle, \dots, 1111\rangle$	$2^4=16$
n	...	2^n

47

Mathematisch: Beispiel für 2 Qubits

$$\begin{aligned}
 |\psi\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \cdot \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
 &= \frac{1}{2}(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle)
 \end{aligned}$$

Kurzschreibweise: $|00\rangle$

48

Aufgabe: Zufallsgenerator

1. Finde heraus, was man mit „Pseudozufallszahlen“ meint.
2. Mit **zwei Qubits** lassen sich **vier Zahlen (0,1,2,3)** darstellen.
Wieviele Zahlen lassen sich mit 3, 4 und n Qubits darstellen?
3. Erkläre, wie man mit Qubits einen *echten* Zufallsgenerator betreiben kann!
Wieviele Qubits bräuchte man für das Erzeugen einer Zufallszahl im Intervall $[0;100]$?

49



Quantencomputer

50

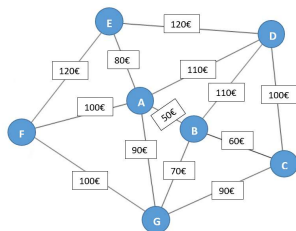
Telefonliste

Pos.	Name	Telefonnummer	Pos.	Name	Telefonnummer	Pos.	Name	Telefonnummer
01	Albus	06605472833	15	Gandalf	06809011892	29	Melisandre	06645897870
02	Aragorn	06647363694	16	Gimli	06766903543	30	Neville	06602311067
03	Arya	06645998462	17	Gollum	06649918201	31	Petyr	06768991018
04	Bilbo	06768334998	18	Harry	06604494833	32	R2-D2	06644786992
05	Boromir	06605639018	19	Hagrid	06601229910	33	Ron	06804967745
06	Bran	06604746839	20	Hermine	06646683780	34	Rubeus	06608223091
07	Brienne	06809011928	21	Hodor	06605229083	35	Samweiss	06649772855
08	C-3PO	06769373287	22	Jaime	06769018902	36	Samwell	06644787634
09	Cersei	06648109081	23	Joffrey	06803425771	37	Sansa	06604476623
10	Chewbacca	06604393380	24	Jon	06649895535	38	Severus	06769476878
11	Dany	06604311984	25	Legolas	06607876122	39	Theon	06604332452
12	Draco	06640198190	26	Leia	06805768575	40	Tyrian	06808416678
13	Eddard	06604380112	27	Luke	06601278244	41	Vader	06642833647
14	Frodo	06769124109	28	Margaery	06645669057	42	Yoda	06764595090

51

Aufgabenblatt: Lösungssuche

52



Lösung: A-E-D-C-B-G-F-A (630€)

- $15 = 3 \cdot 5$
- $91 = 7 \cdot 13$
- $391 = 17 \cdot 23$
- $1073 = 29 \cdot 37$

53

Vorgangsweise:

- Wie bist du prinzipiell bei der Lösung vorgegangen?
- Wie „denkt“ und rechnet ein klassischer Computer?
- Was können Qubits, was klassische Qubits nicht können?

54

★

Bei Problemen dieser Art und der Suche in einer Datenbank kommen Quantencomputer schneller zu einem Ergebnis als klassische Computer!

Der Vorteil besteht in der Superposition:

Während klassische Computer eine Eingabe nach der anderen behandeln, werden in einem Quantencomputer alle Bitkombinationen quasi gleichzeitig bearbeitet!

55

55

Klassischer Computer

Aufgabe: suche Eintrag zu 06642349875

Bildarstellung für Namen: $b_1b_2b_3\dots b_{n-1}b_nb_{n+1}$	Nummer	Ausgabe von f
10.....011	06991234567	0
11.....101	06800987654	0
...	...	...
10.....110	06642349875	1

Schema für Datenbanksuche bei klassischen Computern

56

56

Quantencomputer

★

57

57

Sycamore

58

58

Sycamore

59

59

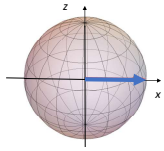
Dekohärenz

Der Unterschied zwischen mikro- und makroskopischer Welt

60

60

Was ist der Unterschied zwischen...



...und...



61

„Die Quantenmechanik ist sehr achtunggebietend. Aber eine innere Stimme sagt mir, daß das noch nicht der wahre Jakob ist. Die Theorie liefert viel, aber dem Geheimnis des Alten bringt sie uns kaum näher. Jedenfalls bin ich überzeugt, daß *der* nicht würfelt.“

- *Albert Einstein* an *Max Born*

62

Frage 1

Was passiert (z.B. mikroskopisch) eigentlich bei einer Messung?
Versuche, möglichst allgemein zu formulieren!



63

Frage 2

"Sie werden doch nicht behaupten wollen, dass der Mond nicht da oben ist, wenn niemand hinsieht?"
- *Albert Einstein* zu *Niels Bohr*



64

Frage 3

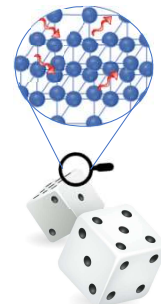
Warum können wir Gegenstände im Alltag
nicht in Superposition beobachten?



65

Prinzip 1: Messung in Natur

- In alltäglichen Objekten gibt es ständig Wechselwirkungen mit der Umgebung
- Auch die Teilchen, aus denen Objekte bestehen, wechselwirken miteinander
- → In der Natur wird ständig „gemessen“
- → Der Verlust von Superposition wird **Dekohärenz** genannt.



66

Prinzip 2: Beobachtung

- Diese Messung geschieht auch ohne die Beobachtung eines Menschen
- → Der Verlust von Superposition hängt **nicht** vom menschlichen Bewusstsein ab



67

67

Offene Probleme

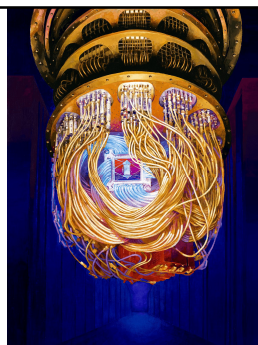
- Superposition bei einzelnen subatomaren Teilchen 
- Grenze?
- Superposition bei alltäglichen Gegenständen 
- Damit verbunden: Ab wann ist eine Wechselwirkung genug, um Superposition zu verhindern?
Was passiert genau bei einer Messung?

68

68

Zur Abschirmung der Qubits notwendig:

- Vakuum
- Niedrige Temperaturen
 - Hier: 15 mK



69

69

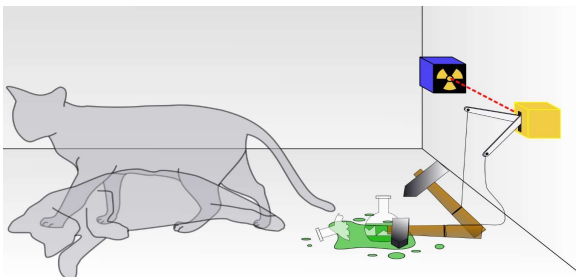
„Man kann auch ganz burleske Fälle konstruieren. Eine Katze wird in eine Stahlkammer gesperrt, zusammen mit folgender Höllenmaschine (die man gegen den direkten Zugriff der Katze sichern muß): in einem Geigerschen Zählrohr befindet sich eine winzige Menge radioaktiver Substanz, so wenig, daß im Laufe einer Stunde vielleicht eines von den Atomen zerfällt, ebenso wahrscheinlich aber auch keines; geschieht es, so spricht das Zählrohr an und betätigt über ein Relais ein Hämmerchen, das ein Kölbchen mit Blausäure zertrümmert. Hat man dieses ganze System eine Stunde lang sich selbst überlassen, so wird man sich sagen, daß die Katze noch lebt, wenn inzwischen kein Atom zerfallen ist. Der erste Atomzerfall würde sie vergiften haben. Die Psi-Funktion des ganzen Systems würde das so zum Ausdruck bringen, daß in ihr die lebende und die tote Katze zu gleichen Teilen gemischt oder verschmiert sind. Das Typische an solchen Fällen ist, daß eine ursprünglich auf den Atombereich beschränkte Unbestimmtheit sich in grobsinnliche Unbestimmtheit umsetzt, die sich dann durch direkte Beobachtung entscheiden läßt. Das hindert uns, in so naiver Weise ein „verwaschenes Modell“ als Abbild der Wirklichkeit gelten zu lassen. An sich enthielte es nichts Unklares oder Widerspruchsvolles. Es ist ein Unterschied zwischen einer verwackelten oder unscharf eingestellten Photographie und einer Aufnahme von Wolken und Nebelschwaden.“

- Erwin Schrödinger

70

70

Schrödingers Katze



71

71



Verschränkung: Phänomen

72

72

Veschränkung

"I cannot seriously believe in it because the theory cannot be reconciled with the idea that physics should represent a reality in time and space, free from **spooky action at a distance**"

-Albert Einstein an Max Born

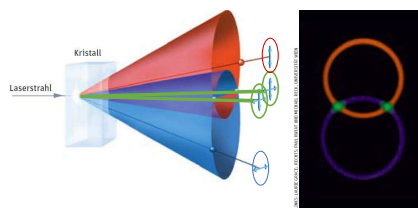
73

Aufgabe: Alice & Bob



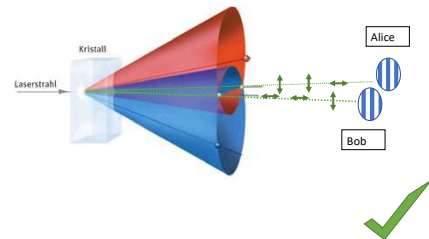
74

Experiment



75

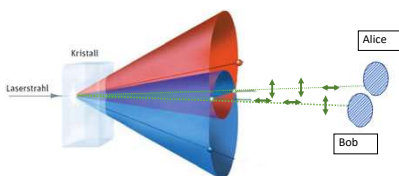
Annahme: entweder $\updownarrow$ oder $\leftrightarrow$



Erwartetes Messergebnis: Alice	Erwartetes Messergebnis: Bob
H	V
V	H
V	H
H	V
...	...
Tatsächliches Messergebnis: Alice	Tatsächliches Messergebnis: Bob
H	V
V	H
V	H
H	V
...	...

76

Messung in 45° - Stellung



Erwartetes Messergebnis: Alice	Erwartetes Messergebnis: Bob
+	+
+	-
-	-
-	+
...	...
Tatsächliches Messergebnis: Alice	Tatsächliches Messergebnis: Bob
+	-
+	-
-	+
-	+
...	...

77

Mit Spin:

https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/entanglement/entanglement.html

78



Die Beschreibung der Gesamtsituation ist nicht mehr mit zwei einzelnen Blochkugeln möglich – die Teilchen sind „verschränkt“

79

79

Verschränkung: mathematisch

- **Zum Vergleich:** Zwei Qubits in gleichgewichteter Superposition:

$$|\Psi\rangle = \underbrace{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)}_{1. \text{ Qubit}} \cdot \underbrace{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)}_{2. \text{ Qubit}} = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \quad \dots \text{„separabel“}$$

- **Verschränkter Zustand:**

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

Nicht separabel, also nicht in einzelne Qubits zerlegbar → Beschreibung nur gemeinsam möglich!

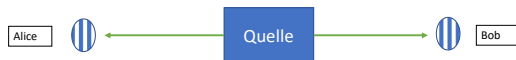
80

80



Gleichzeitige Messung

- **Vor der Messung:**
 - beide Messergebnisse gleichwahrscheinlich
 - Ergebnis völlig ungewiss



- **Nach der Messung:**
 - Bei beiden liegt nun einer der beiden möglichen Zustände vor: keine Verschränkung mehr!
 - Bei gleicher Wahl der Messung: **sofortige** Gewissheit, was der/die jeweils andere misst/messen wird!
 - „spooky action at a distance“

81

81



Kommunikation

Heißt das, dass durch Verschränkung *überlichtschnelle Kommunikation* möglich ist?

82

82



Verschränkung: Anwendung

83

83



Aussage 1

„Wenn Alice und Bob verschränkte Teilchen messen, kann Alice sofort eine Nachricht von Bob empfangen, weil Alice bei der Messung sofort weiß, was Bob gemessen hat.“

Richtig oder Falsch?

84

84

Aussage 2



„Die Verschränkung von zwei Teilchen kann man aufheben, indem man sie räumlich weit genug trennt.“

Richtig oder Falsch?

85

85

Aussage 3



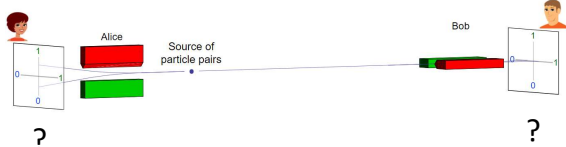
„Zwei Menschen können miteinander verschränkt sein, wenn ihr Zustand voneinander abhängig ist.“

Richtig oder Falsch?

86

86

Alice & Bob: verschiedene Messungen



→ Erstelle mit der Simulation eine Liste von Ergebnissen bei Alice und Bob – Gibt es auch hier ein „Muster“?

87

87

https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/simulations/cryptography/Quantum_Cryptography.html

88

88

Zusammenfassung



- Führen Alice und Bob an einem verschränkten Paar dieselbe Messung durch, stellen sie immer gegengleiche Ergebnisse fest.
- Führen Alice und Bob an einem verschränkten Paar unterschiedliche Messungen durch, ist dies nicht mehr der Fall!

89

89

Verschlüsselung von Nachrichten

- Nachricht von Alice: **H a l l o W e l t**
- Schlüssel: **A s d f g h j k l**
- Verschlüsselte Nachricht: **l t p r v E o x f**

- Bob erhält die verschlüsselte Nachricht.
- Zum Entschlüsseln benötigt er den **Schlüssel**, welcher als eine **Kombination von Nullen und Einsen** dargestellt werden kann
- Aber: auch der Schlüssel muss üblicherweise gesendet werden!

90

90



Aufgabe: Ein sicherer Schlüssel

91

91



Mit verschränkten Zuständen
kann man abhörsicher
kommunizieren.

92

92