Physik und Didaktik in Schule und Hochschule
PhyDid 1/11 (2012) – S. 1-16

Was man vom einzelnen Qubit über Quantenphysik lernen kann

Wolfgang Dür*, Stefan Heusler[+]

* Institut für Theoretische Physik, Universität Innsbruck, Österreich, wolfgang.duer@uibk.ac.at
[+] Institut für Didaktik der Physik, Universität Münster, Deutschland, stefan.heusler@uni-muenster.de
(Eingegangen: 31.10.2011; Angenommen: 01.01.2012)

Kurzfassung

In diesem Artikel wird ein Zugang zur Quantenphysik vorgestellt, der auf dem einfachsten möglichen Quantensystem basiert – dem Qubit. Dabei wird demonstriert, wie viele der zentralen Prinzipien der Quantenphysik – insbesondere das Überlagerungsprinzip, das stochastische Verhalten, die Zustandsänderung bei Messungen, sowie die Heisenberg'sche Unschärferelation, mit Hilfe von Bildern und einfacher Mathematik den Schülern zugänglich gemacht werden können. Großer Wert wird dabei auf die Entwicklung von Visualisierungen gelegt, wobei neben den abstrakten Eigenschaften eines Qubits auch verschiedene physikalische Realisierungen des Qubits im Detail vorgestellt werden. Abschließend werden noch Anwendungen der vorgestellten Prinzipien, insbesondere im Bereich der Quantenkryptographie, diskutiert.

1. Einleitung

Die Quantenmechanik ist eine der zentralen Theorien der modernen Physik, und noch heute ein vielbeachtetes und aktuelles Forschungsgebiet. Die Entwicklung und Evaluation geeigneter Unterrichtskonzepte elementarer Quantenphysik für die Schule ist ein wichtiges Forschungsthema der Physikdidaktik [1, 2]. In diesem Beitrag wollen wir zeigen, dass viele der zentralen Konzepte der modernen Quantenphysik – allen voran das Superpositionsprinzip, das Verhalten von Systemen bei Messungen, aber auch die Heisenberg'sche Unschärferelation – anhand des einfachsten Quantensystems, dem sogenannten Qubit, erarbeitet und erklärt werden können [3]. Insbesondere ist dazu keine komplexe Mathematik notwendig. Die mathematischen Strukturen werden durch graphische Visualisierungen zugänglich gemacht. Die „Übersetzung" in Bilder eignet sich gut für eine direkte Umsetzung im Unterricht. Darüber hinaus können auf diese Weise auch Themen der modernen Forschung, wie etwa die Realisierung von Qubits mit einzelnen Atomen oder Photonen, sowie Anwendungen im Bereich der Quanteninformationsverarbeitung, insbesondere der Quantenkommunikation und der Quantenkryptographie, behandelt werden. Folgt man diesem Konzept weiter und betrachtet Systeme von mehreren Qubits, so hat man die Möglichkeit, Konzepte wie Verschränkung und Nichtlokalität und weitere moderne Anwendungen im Bereich der Quanteninformationsverarbeitung wie Teleportation oder Quantencomputer zu behandeln.

In diesem Beitrag wird zunächst das einfachste klassische System – das Bit – behandelt, und die Unterschiede zum einfachsten quantenmechanischen System – dem Qubit – herausgearbeitet. Dabei steht zunächst die (abstrakte) Beschreibung des Qubits durch die Bloch-Kugel im Mittelpunkt, mit deren Hilfe nicht nur Überlagerungszustände und Operationen beschrieben und illustriert werden, sondern auch ein anschauliches Bild vom quantenmechanischen Messprozess gewonnen wird. Es folgt die Diskussion einer Reihe von möglichen physikalischen Realisierungen eines Qubits, welche so unterschiedliche Objekte wie die Polarisationszustände eines Photons, den Spin eines Teilchens, den Ort eines einzelnen Atoms in einem Doppelmulden-Potentialtopf, sowie die internen elektronischen Zustände eines Atoms oder Ions beinhalten. Dabei werden Zustände, Operationen und Messprozesse für diese unterschiedlichen Systeme behandelt und die Vor- und Nachteile im Hinblick auf eine Diskussion in der abstrakten Bloch-Kugel-Darstellung im Unterricht herausgearbeitet. Es folgt eine kurze Auswahl von interessanten Anwendungen dieser Konzepte, insbesondere eine qualitative Erklärung der Heisenberg'schen Unschärferelation, das No-Cloning-Theorem für Quanteninformation und einfache Quantenkryptographieverfahren.

2. Klassische Systeme – das Bit

Das einfachste klassische System ist ein 2-Niveau-System, ein System mit einer charakteristischen Eigenschaft, die nur zwei mögliche Werte annehmen kann – 0 oder 1. Man spricht dabei auch von einem Bit (**bi**nary digi**t**), wobei ein Bit auch ein elementarer Informationsträger bzw. die kleinste Einheit von Information ist. Ein Bit sollte dabei als abstraktes Objekt verstanden werden; es ist nicht vorgegeben, welche charakteristische Eigenschaft bzw. welche physikalische Realisierung betrachtet wird.

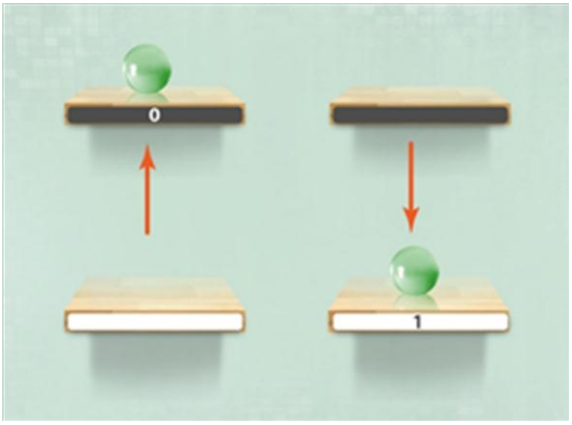

Abb. 1: Illustration eines klassischen Bits. Die zwei möglichen Zustände 0 und 1 des Bits sind in diesem Fall durch die Position eines Balls im oberen oder unteren Regal, bzw. durch die Orientierung eines Vektors (nach oben oder unten) gegeben.

So kann es sich z. B. um einen Schalter mit zwei möglichen Stellungen handeln, oder um eine Spannung, die die Werte $U = 0$ V oder $U = 5$ V annehmen kann, oder auch um den Ort eines Teilchens mit den möglichen Werten x_0 und x_1 (z. B. ein Ball, der in einem Schrank auf dem unteren oder oberen Regal liegt). In jedem Fall wird aber nur *eine* charakteristische Eigenschaft betrachtet, weitere Eigenschaften werden vernachlässigt bzw. als fixiert angesehen. Beim Ball sind dies z. B. dessen Größe, Gewicht oder Geschwindigkeit. Wir wollen im Folgenden die Darstellung eines Bits mit Hilfe eines „Zeigers“ bzw. Vektorpfeils verwenden. Dabei hat der Zeiger zwei mögliche Orientierungen, nach oben (Bitwert 0) bzw. nach unten (Bitwert 1), siehe Abb. 1. Im Rahmen der klassischen Informationsverarbeitung kann der Wert eines Bits durch Anwendung eines logischen Gatters manipuliert werden. Im Falle eines einzelnen Bits ist dabei nur das NOT-Gatter relevant, welches den Bitwert invertiert ($0 \rightarrow 1$, $1 \rightarrow 0$).

3. Quantenmechanische Systeme – das Qubit

Wir wenden uns nun quantenmechanischen Systemen zu, und betrachten die Beschreibung von Zuständen, Messungen und Operationen sowie die daraus resultierenden Eigenschaften.

3.1. Zustände

Ganz analog zum klassischen Bit ist ein Quantenbit (Qubit) das einfachste quantenmechanische System. Auch hier handelt es sich um ein Zwei-Niveau-System, wobei eine charakteristische Eigenschaft wieder zwei mögliche Werte annehmen kann. Im Folgenden werden parallel zueinander die mathematische und die bildliche Darstellung entwickelt. Im Unterricht reicht es aus, lediglich auf die Visualisierungen zurückzugreifen, und nur exemplarisch auf die zugrunde liegenden Rechnungen einzugehen. Wir bezeichnen die beiden Zustände mit

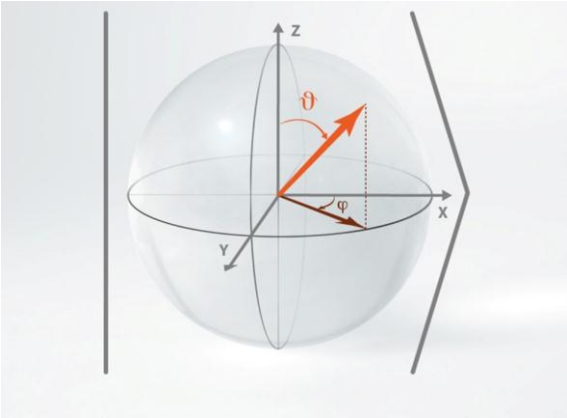

Abb. 2: Grafische Darstellung der Zustände eines Qubits mit Hilfe der Bloch-Kugel. Quantenmechanische Zustände entsprechen Vektoren der Länge 1 im 3-dimensionalen Raum. Diese Vektoren werden durch Angabe des Polarwinkels ϑ und des Azimutwinkels φ (Kugelkoordinaten) charakterisiert.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \qquad \{1\}$$

Die übrigen Freiheitsgrade des Teilchens werden dabei vernachlässigt bzw. als fixiert angenommen. Ein Qubit ist als abstraktes Objekt zu verstehen, welches durch verschiedenartige physikalische Systeme realisiert werden kann, worauf wir in Abschnitt 4 noch näher eingehen werden. Das Qubit ist das zentrale Element der Quanteninformationstheorie und die elementare Einheit der Quanteninformation.

Neu im Vergleich zum klassischen Bit ist nun, dass auch *beliebige Überlagerungen* der beiden Zustände $|0\rangle$ und $|1\rangle$ möglich sind. Mathematisch wird eine solche Überlagerung als Summe der beiden Zustände beschrieben, gewichtet mit zwei komplexen Amplituden α und β. Diese Überlagerung kann physikalisch als *Interferenz* der Zustände gedeutet werden. Der Zustand eines Qubits wird also beschrieben durch den Vektor

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}. \qquad \{2\}$$

Der zugehörige Vektorraum ist der Raum der Zweiervektoren mit komplexen Koeffizienten C^2. Bezeichnen wir mit $|\phi\rangle = \gamma|0\rangle + \delta|1\rangle$ einen zweiten (beliebigen) Vektor, so ist in diesem Vektorraum ein Skalarprodukt als $\langle\psi|\phi\rangle = \alpha^* \gamma + \beta^* \delta$ definiert, wobei * komplexe Konjugation bezeichnet. Für Quantenzustände gilt, dass diese normiert sein müssen ($|\alpha|^2 + |\beta|^2) = 1$), um eine sinnvolle Interpretation von Messungen im Sinne von Wahrscheinlichkeiten sicherzustellen, wie in Abschnitt 3.3 genauer beschrieben wird. Nur normierte Vektoren – also Vektoren der Länge 1 – beschreiben einen einzelnen Quantenzustand. Darüber hinaus stellt sich heraus, dass für das physikalische Verhalten, insbesondere für alle beobachtbaren Größen, die globale Phase

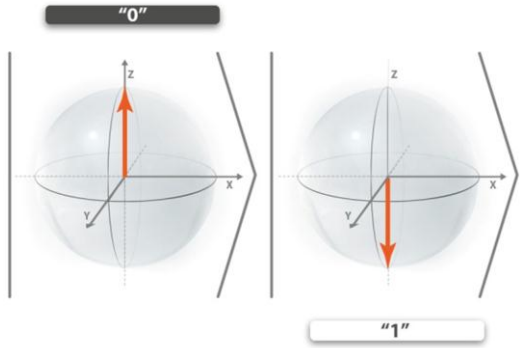

Abb. 3: Darstellung der Zustände $|0\rangle$ und $|1\rangle$ in der Bloch-Kugel. Es ist zu beachten, dass orthogonale Zustände in der Bloch-Kugel-Darstellung antiparallel sind.

des Zustands keine Rolle spielt. Dies wird später bei der Behandlung von Messungen klar werden. Dadurch kann α in Gleichung (1) reell gewählt werden. Der allgemeine Zustand eines Qubits kann durch zwei reelle Parameter ϑ und φ charakterisiert werden. Die Winkel ϑ und φ können dabei mit Kugelkoordinaten auf der sogenannten Bloch-Kugel assoziiert werden, wobei ϑ der Polarwinkel und φ der Azimutwinkel ist:

$$|\psi\rangle = \cos\tfrac{\vartheta}{2}\,|0\rangle + \sin\tfrac{\vartheta}{2}\,e^{i\varphi}\,|1\rangle. \qquad \{3\}$$

Wichtig ist hierbei, dass der Quantenzustand eines Qubits durch einen Vektor der Länge 1 auf der Bloch-Kugel veranschaulicht werden kann, siehe Abb. 2. Senkrechte Zustände sind auf der Bloch-Kugel antiparallel. Der Zustand $|0\rangle$ entspricht $\vartheta = 0$ und ist in $+z$-Richtung orientiert, während der Zustand $|1\rangle$ dem Winkel $\vartheta = \pi$ entspricht und in $-z$-Richtung orientiert ist, siehe Abb. 3.

Durch die Visualisierung des Qubits auf der Bloch-Kugel ist es einfach möglich, Überlagerungszustände darzustellen. Für $\vartheta = \pi/2$ und $\varphi = 0$ bzw. $\varphi = \pi$ erhält man Überlagerungszustände der Form:

$$|0_x\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad \{4\}$$

und

$$|1_x\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \qquad \{5\}$$

welche auf der Bloch-Kugel in ± x-Richtung orientiert sind, siehe Abb. 4. Wichtig ist festzuhalten, dass es diese Überlagerungszustände für klassische Systeme nicht gibt – und sie besitzen auch keine einfache, anschauliche Bedeutung. Während klassische Zustände einer Orientierung des Vektorpfeils nach oben bzw. unten entsprechen (das Teilchen befindet sich im oberen bzw. unteren Regal), befindet sich in diesem Bild das Teilchen zwischen den Regalen; es ist weder im oberen noch im unteren, sondern vielmehr in beiden gleichzeitig. Was das genau bedeutet, werden wir bei der Behandlung des Messprozesses näher erläutern.

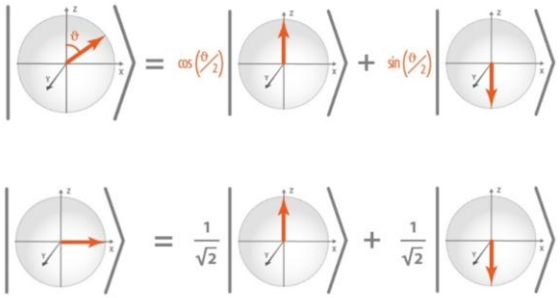

Abb. 4: Darstellung von verschiedenen Überlagerungszuständen auf der Bloch-Kugel.

Führt man Zustände von Qubits in der Schule ein, ist es ausreichend, nur reelle Koeffizienten zu betrachten (Phase $e^{i\varphi} = 1$), mit $\vartheta \in [0, 2\pi]$.

Dadurch vermeidet man Probleme mit komplexen Zahlen und dem Skalarprodukt in komplexen Vektorräumen. Das Bild der Bloch-Kugel reduziert sich damit auf den Einheitskreis, also Vektoren der Länge 1 in der Ebene, die durch den Winkel ϑ parametrisiert sind. Zu beachten ist in diesem Fall auch, dass in dem verwendeten Bild senkrechte Vektoren antiparallel sind, da wir als Argument $\vartheta/2$ verwenden – dies erweist sich später bei der Veranschaulichung von Messungen als hilfreich und kann hier als Konvention angesehen werden.

3.2. Operationen

Der Zustand eines Qubits kann manipuliert werden bzw. sich mit der Zeit ändern. Dies entspricht dann einer Drehung des Zustandsvektors in der Bloch-Kugel, und wird mathematisch durch unitäre Operationen beschrieben – in diesem Fall durch eine 2x2-Matrix U aus der Gruppe SU(2) mit der Eigenschaft $U^\dagger U = U\,U^\dagger = \mathbb{1}$, wobei † komplexe Konjugation und Transposition der Matrix bedeutet. Der Zustand nach der Operation ist durch $U\,|\psi\rangle$ gegeben.

Drehungen können dabei um eine beliebige Achse $\boldsymbol{a}$ im Raum erfolgen. Eine Drehung um die y-Achse um den Winkel $\vartheta = -2\gamma$ entspricht z. B. der Operation

$$U_y(\gamma) = \exp(i\gamma\sigma_y) = \begin{pmatrix} \cos\gamma & \sin\gamma \\ -\sin\gamma & \cos\gamma \end{pmatrix} \qquad \{6\}$$

und man erhält für den Ausgangszustand $|0\rangle$:

$$U_y(\gamma)\,|0\rangle = \cos\gamma\,|0\rangle - \sin\gamma\,|1\rangle. \qquad \{7\}$$

Drehungen des Zustandsvektors um eine beliebige Achse (normierter Vektor) $\boldsymbol{a} = (a_x, a_y, a_z)^T$ sind durch einen Drehoperator U beschrieben, wobei

$$U = \exp(i\gamma\sigma_{\mathbf{a}}) = \cos\gamma I + i\sin\gamma\sigma_{\mathbf{a}} \qquad \{8\}$$

mit

$$\sigma_{\mathbf{a}} = a\cdot\sigma = a_x\sigma_x + a_y\sigma_y + a_z\sigma_z. \qquad \{9\}$$

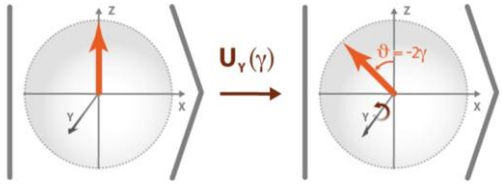

Abb. 5: Die unitäre Drehung eines Qubits entspricht der Rotation des Zustandsvektors um eine fixe Drehachse mit einem gegebenen Winkel. In diesem Beispiel ist die Wirkung der unitären Operation $U_y(\gamma)$ auf den Eingangszustand $|0\rangle$ dargestellt, was einer Rotation um den Winkel $\vartheta = -2\gamma$ um die *y*-Achse entspricht.

Dabei verwenden wir die Pauli-Matrizen

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \{10\}$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Für die Schule ist es ausreichend, sich Drehungen des Zeigers im Kreis als eine mögliche Manipulation des Qubits vorzustellen, siehe Abb. 5.

3.3. Messungen

Neu ist in der Quantenmechanik auch das Verhalten des Systems bei Messungen. Die Eigenschaften eines Zustands können im Gegensatz zu klassischen Bits nicht einfach vollständig ausgelesen werden. Es ist nur möglich, eine Eigenschaft mit zwei möglichen (Mess-)Werten abzufragen – z. B. ob sich das Quantensystem nach der Messung im Zustand $|0\rangle$ oder $|1\rangle$ befindet. Mathematisch entsprechen die möglichen Messergebnisse der Observablen σ_z den Eigenwerten +1 und –1, die zu den Eigenvektoren $|0_z\rangle = |0\rangle$ und $|1_z\rangle = |1\rangle$ gehören. In der Bloch-Kugel Darstellung befinden sich diese Zustände in Richtung der ± *z*-Achse. Dabei erhält man eines der beiden möglichen Ergebnisse, also ein Bit an Information. Die physikalische Interpretation der Eigenwerte +1 und –1 hängt vom betrachteten Zwei-Niveau-System ab und wird im Abschnitt 4 konkretisiert. Ist das Quantensystem vor der Messung im Zustand $|0\rangle$ bzw. $|1\rangle$, so wird die Messung auch immer dieses Ergebnis liefern. Ist das Qubit allerdings vor der Messung in einem Überlagerungszustand $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, so erhält man als *zufälliges, nicht vorhersagbares Ergebnis entweder „0“ oder „1“, wobei die Wahrscheinlichkeit durch*

$$p_0 = \langle\psi|0\rangle\langle 0|\psi\rangle = |\langle 0|\psi\rangle|^2 = |\alpha|^2 \qquad \{11\}$$

bzw.

$$p_1 = |\langle 1|\psi\rangle|^2 = |\beta|^2 \qquad \{12\}$$

gegeben ist. Nach der Messung ist dieser Überlagerungszustand nicht mehr vorhanden. Der Zustand

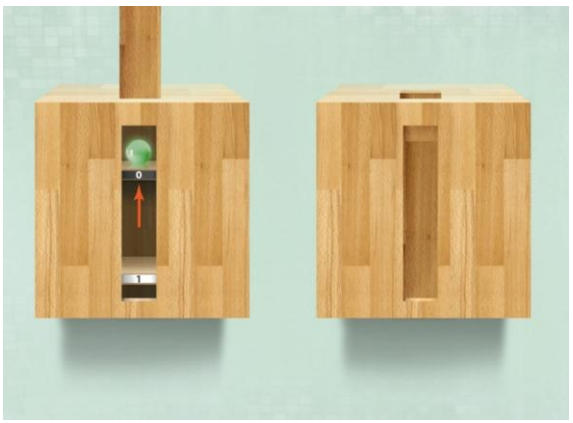

Abb. 6: Illustration einer Messung in *z*-Richtung (Observable σ_z). Dies entspricht der Orientierung eines Schlitzes in dieser Raumrichtung. Es wird abgefragt, ob der Zustandsvektor in positiver (Messergebnis „$|0\rangle$“) oder negativer (Messergebnis „$|1\rangle$“) Schlitzrichtung orientiert ist.

des Qubits hat sich also durch den Messprozess verändert. Erhält man als Messergebnis den Eigenwert +1, so ist der Zustand nach der Messung $|0\rangle$, für das Messergebnis[1] –1 ist der Zustand dann $|1\rangle$. Durch die Messung bricht die Superposition zwischen den Zuständen $|0\rangle$ und $|1\rangle$ zusammen. Wichtig ist dabei festzuhalten, dass es sich um eine strukturierte Form von Zufall handelt: Einerseits gibt es Zustände, für die Messungen deterministische Ergebnisse liefern – bei der Messung von σ_z sind das die Eigenzustände $|0\rangle$ und $|1\rangle$. Andererseits kann für eine häufige Wiederholung eines Experimentes (Präparation eines Systems in einem bestimmten Zustand mit nachfolgender Messung) eine Vorhersage über das *statistische Verhalten* gemacht werden. Und diese statistischen Aussagen über Erwartungswerte bei mehreren Experimenten ist es, was die Quantenmechanik im Allgemeinen liefern kann.

3.3.1. Darstellung des Messprozesses mit Hilfe der Bloch-Kugel

Verwendet man die Bloch-Kugel zur Illustration des Zustands eines Qubits (Abb. 3), so können Messungen mit „Schlitzen“ in einer bestimmten Raumrichtung assoziiert werden, siehe Abb. 6, Abb. 7 und Abb. 8.

Die Messung von σ_z (σ_x) entspricht z. B. einem Schlitz in Richtung der *z*-Achse (*x*-Achse). Der Messprozess bewirkt, dass der Zustandsvektor durch den Schlitz „gepresst“ wird, und deshalb nach der Messung entweder in positive oder negative Schlitzrichtung orientiert sein muss, siehe Abb. 7 (Abb. 8). Es kommt also zu einer Änderung des Zustands durch den Messprozess. Der Winkel zwischen Schlitz und Zustandsvektor bestimmt dabei die Wahrscheinlichkeit, ein entsprechendes Messergebnis zu erhalten. Ist der Zustandsvektor sehr nahe der

[1] Die Messergebnisse ±1 werden im Folgenden vereinfacht auch direkt mit den zugehörigen Eigenzuständen als „Messergebnis“ beschrieben.

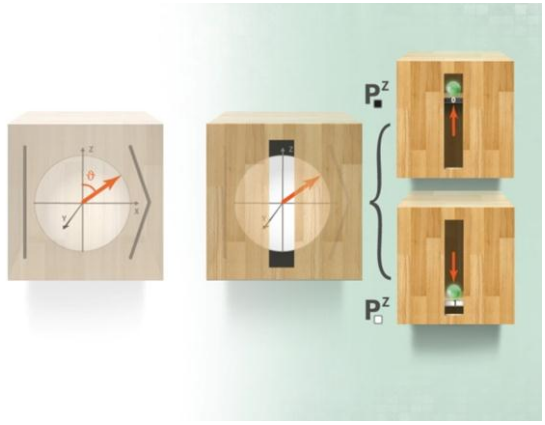

Abb. 7: Illustration einer Messung in *z*-Richtung (Observable σ_z) für ein Qubit im Zustand $|\psi\rangle = \cos\vartheta/2\,|0\rangle + \sin\vartheta/2\,|1\rangle$. Der Zustandsvektor ist nicht in Schlitzrichtung orientiert. Der Messprozess bewirkt ein Umklappen des Vektors in positive oder negative Schlitzrichtung. Dies führt zu einem zufälligen Messergebnis („$|0\rangle$“ oder „$|1\rangle$“ mit der Wahrscheinlichkeit $p_0 = \cos^2\vartheta/2$ bzw. $p_1 = \sin^2\vartheta/2$, und einer Änderung des Quantenzustands durch den Messprozess.

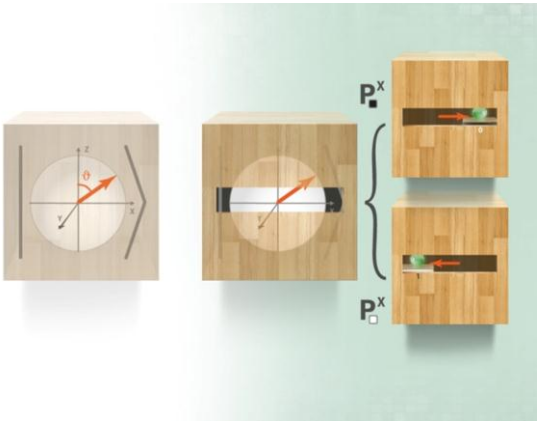

Abb. 8: Illustration einer Messung in *x*-Richtung (Observable σ_x) für ein Qubit im Zustand $|\psi\rangle = \cos\vartheta/2\,|0\rangle + \sin\vartheta/2\,|1\rangle$. Der Schlitz ist in *x*-Richtung orientiert. Der Messprozess bewirkt ein Umklappen des Zustandsvektors in positive oder negative Schlitzrichtung. Dies führt zufällig zum Messergebnis „$|0_x\rangle$“ oder „$|1_x\rangle$“ mit der Wahrscheinlichkeit $p_0 = ½ + \cos\vartheta/2\,\sin\vartheta/2$ bzw. $p_1 = ½ - \cos\vartheta/2\,\sin\vartheta/2$ und einer Änderung des Quantenzustands durch den Messprozess.

positiven *z*-Achse, so ist es sehr wahrscheinlich, das Messergebnis +1 bzw. den Zustand „$|0\rangle$“ zu erhalten – das vollständige Umklappen des Vektors in negative *z*-Richtung – was dem Zustand „$|1\rangle$“ bzw. dem Messergebnis –1 entspricht – ist unwahrscheinlich. Diese Visualisierung macht auch deutlich, dass es nicht möglich ist, durch eine einzelne Messung den gesamten Zustand des Qubits zu erfassen, der „Schlitz“ bzw. die Messachse schränkt den Blickwinkel auf eine bestimmte Richtung ein. Es wird weiterhin deutlich, wie das Wechselspiel zwischen „Zustand“ und „Beobachten“ zu verstehen ist: Ohne Definition der Messachse ist es nicht möglich, ein Messergebnis zu erhalten. Die Messung selbst führt zu einem Umklappen des Zustandsvektors in positive oder negative Schlitzrichtung, also zu einer Zustandsänderung. Wichtig ist festzuhalten, dass die „Schlitze“ lediglich als Hilfsobjekte zur Illustration des Messprozesses zu verstehen sind, und keine direkte physikalische Bedeutung haben.

3.3.2. Messungen in einer gedrehten Basis

Wie bereits erwähnt ist es möglich, eine alternative Eigenschaft des Systems abzufragen, z. B. ob es sich im Zustand

$$|0_x\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad \{13\}$$

oder

$$|1_x\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \qquad \{14\}$$

befindet. Die Messung der Observablen σ_x mit Eigenvektoren „$|0_x\rangle$“ und „$|1_x\rangle$ entspricht in der Bloch-Kugel-Darstellung einem „Schlitz“ in Richtung der ± *x*-Achse, siehe Abb. 8. Eine Messung kann in jeder beliebigen Basis durchgeführt werden. Die entsprechende Messrichtung ist dabei durch die Eigenzustände „$|0_a\rangle$, „$|1_a\rangle$ einer beliebigen Observablen *A* gegeben, also durch die Angabe von zwei aufeinander senkrecht stehenden Vektoren mit der Eigenschaft

$$A|0_a\rangle = (+1)\,|0_a\rangle\,, \qquad \{15\}$$

$$A|1_a\rangle = (-1)\,|1_a\rangle\,. \qquad \{16\}$$

In der Visualisierung entspricht dies einem Schlitz in einer beliebigen Richtung in der Bloch-Kugel-Darstellung. Die Wahrscheinlichkeit für die einzelnen Messergebnisse kann wieder mittels des Skalarprodukts mit dem Zustandsvektor $|\psi\rangle$ berechnet werden:

$$p_0 = |\langle 0_a\,|\,\psi\rangle|^2 \qquad \{17\}$$

bzw.

$$p_1 = |\langle 1_a\,|\,\psi\rangle|^2\,. \qquad \{18\}$$

Je kleiner der Winkel zwischen Zustandsvektor und Ergebnisvektor ist, desto größer ist die Wahrscheinlichkeit, dass dieses Messergebnis auch auftritt. Der Zustand nach der Messung ist – je nach Messergebnis – dann durch $|0_a\rangle$ oder $|1_a\rangle$ gegeben. Aus den Formeln zur Berechnung der Wahrscheinlichkeiten wird auch unmittelbar klar, dass Zustände der Form $e^{i\gamma}|\psi\rangle$ physikalisch äquivalent zu $|\psi\rangle$ sind, eine globale Phase γ also keine Rolle spielt.

Wir weisen nochmals darauf hin, dass durch die Messung der Zustand des Systems verändert wird. Nach einer Messung der Observablen σ_z ist das System in einem der Eigenzustände von σ_z also $|0\rangle$ oder $|1\rangle$, egal wie der Zustand vorher ausgesehen hat. Das Ergebnis einer nachfolgenden Messung der Observablen σ_x ist vollkommen zufällig. Daraus folgt auch, dass durch weitere Messungen keine zusätzliche Information mehr über den ursprünglichen Ausgangszustand gewonnen werden kann.

3.3.3. Klassische Gemische vs. reine Quantenzustände

Wir wollen nun auf den Unterschied zwischen einem klassischen Gemisch und einem quantenmechanischen Ensemble von Überlagerungszuständen eingehen. Auch klassische Systeme können sich bei Messungen zufällig verhalten. Dies hat aber eine andere Ursache als im quantenmechanischen Fall und ist mit diesem nicht vergleichbar. Betrachten wir dazu ein Ensemble von N klassischen Bits, wobei jedes dieser Bits einen zufälligen Wert 0 oder 1 besitzt. Beide Werte sollen dabei gleich häufig vorkommen. Es ist zu beachten, dass jedes der Bits einen fixen Wert besitzt. Allerdings betrachten wir eine Situation, in der wir davon ausgehen, dass wir diesen Wert nicht kennen – deshalb bezeichnen wir diese Bits als zufällig. Führen wir nun Messungen an den einzelnen Bits durch, so werden wir zufällige Ergebnisse erhalten. Betrachtet man die Statistik der einzelnen Messergebnisse, so werden die Ergebnisse 0 und 1 etwa in jeweils $N/2$ Fällen gefunden werden. Die allgemeine Beschreibung einer solchen Situation kann mit Hilfe einer Wahrscheinlichkeitsverteilung für die einzelnen Bitwerte erfolgen, welche unsere Unkenntnis über die vorliegende Situation ausdrückt. Eine solche Beschreibung findet man z. B. im Rahmen der klassischen statistischen Mechanik. Ein analoges Verhalten findet man, wenn man ein Ensemble von zufälligen Quantenbits betrachtet, die sich jeweils im Zustand $|0\rangle$ oder $|1\rangle$ befinden (Abb. 9, erste Zeile). Dabei spricht man von einem gemischten Zustand, der durch eine sogenannte Dichtematrix beschrieben wird. Anschaulich kann man eine solche Dichtematrix in der Bloch-Kugel durch einen Vektor beschreiben, dessen Länge ≤ 1 ist. In unserem Fall hätte der Vektor die Länge 0 und entspräche einem komplett gemischten Zustand. Dies bedeutet, dass Messungen *in jeder beliebigen Basis* ein vollkommen zufälliges Ergebnis liefern.

Betrachten wir nun im Vergleich dazu N Kopien des quantenmechanischen Überlagerungszustands

$$|0_x\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad \{19\}$$

(Abb. 9, zweite Zeile). Führt man an diesen Zuständen jeweils eine z-Messung durch, so wird man bei jeder einzelnen Messung jeweils mit 50 % Wahrscheinlichkeit den Wert $|0\rangle$ oder $|1\rangle$ finden. Im Schnitt erhält man also auch in etwa $N/2$ der Fälle das Ergebnis $|0\rangle$ bzw. $|1\rangle$ – ganz analog wie bei einem klassischen Gemisch bzw. dem Gemisch von Qubits.

In der Tat sind diese Ensembles durch z-Messungen nicht voneinander zu unterscheiden. Führt man allerdings eine x-Messung durch, so ist im Falle des Gemisches das Ergebnis dieser Messung wieder zufällig (Abb. 9, dritte Zeile). Aber für den reinen Zustand wird sich *immer* das Ergebnis $|0_x\rangle$ finden – es zeigt sich also kein zufälliges Verhalten. Im Fall eines klassischen Bits ist diese Messung gar nicht definiert, weil klassische Bits nicht interferenzfähig sind und somit kein Superpositionszustand $|0_x\rangle$ existiert.

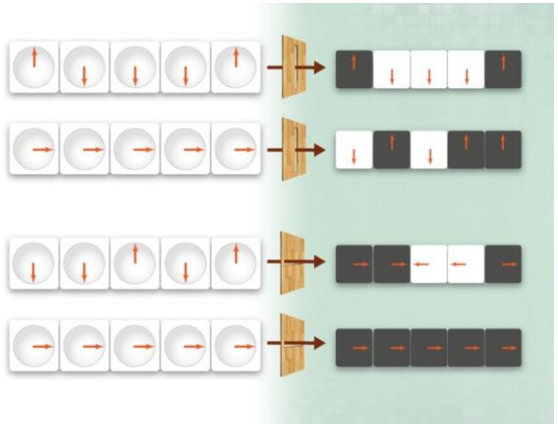

Abb. 9: Illustration des Unterschiedes zwischen einem gemischten Zustand (Ensemble aus zufälligen Qubits im Zustand $|0\rangle$ oder $|1\rangle$) und einem reinen Zustand (alle Qubits im gleichen Zustand $|0_x\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$. Durch eine z-Messung sind die beiden Situationen nicht unterscheidbar, man erhält zufällige Messergebnisse. Eine x-Messung führt jedoch für den gemischten Zustand auf zufällige Ergebnisse, während man für das reine Ensemble immer dasselbe, deterministische Messergebnis erhält.

Damit haben wir bereits drei der zentralen Elemente der Quantenmechanik kennen gelernt – die Möglichkeit von *Überlagerungen*, das *stochastische Verhalten* bei Messungen, sowie die *Veränderung des Zustands* des Systems durch die Messung. Zudem ist es leicht, das entsprechende Verhalten nicht nur qualitativ, sondern auch quantitativ zu beschreiben. Notwendig sind dazu lediglich Skalarprodukte zwischen Zweiervektoren. Auch ein anschauliches Bild – das der Bloch-Kugel – kann für solche einfachen Quantensysteme herangezogen werden, und hilft auch dabei, sich den Messprozess zu veranschaulichen.

4. Physikalische Realisierungen eines Qubits

Ein Qubit ist ein abstraktes Objekt, und als solches haben wir es bisher behandelt, um die quantenmechanischen Eigenschaften und die Unterschiede zu einem klassischen Bit hervorzuheben. Es gibt eine Reihe von möglichen physikalischen Realisierungen eines Qubits, und wir werden im Weiteren einige Beispiele dazu näher diskutieren. Bei der Behandlung in der Schule bietet es sich aus unserer Sicht an, mehrere dieser möglichen physikalischen Realisierungen vergleichend zu diskutieren und die (abstrakten) Eigenschaften eines Qubits dadurch zu illustrieren. Die verschiedenen Aspekte (Zustände, Messungen, Operationen) lassen sich mit den Beispielen unterschiedlich gut erläutern, wobei allerdings keines der Systeme frei von möglichen Fehlinterpretationen bzw. Anschauungsproblemen ist.

Es ist heute in vielen Labors weltweit möglich, mit einzelnen (oder auch mehreren verschränkten)

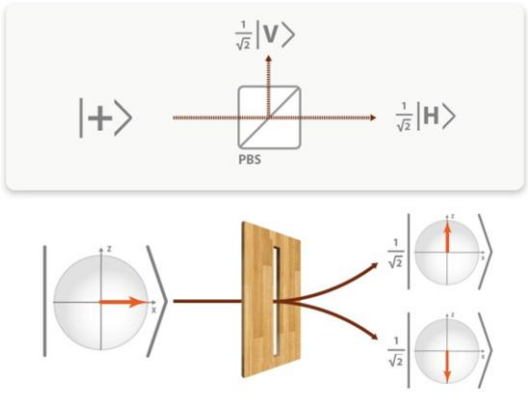

Abb. 10: Illustration einer Messung für den Polarisationsfreiheitsgrad von Photonen. Der polarisierende Strahlteiler bewirkt eine Transmission von horizontal polarisierten Photonen, währen vertikal polarisierte Photonen reflektiert werden. Der Nachweis erfolgt durch Photodetektoren an den beiden Ausgängen, wobei jeweils nur einer der beiden Detektoren ein Photon registriert. Dies entspricht einer *z*-Messung (Messung der Observablen σ_z).

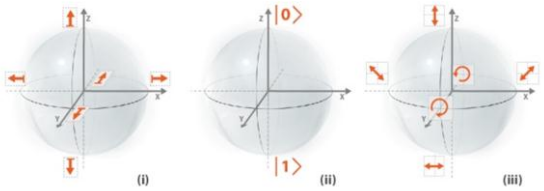

Abb. 11: Gegenüberstellung der Bloch-Kugel-Darstellung für Spin und Polarisation. Während die Orientierung des Spins genau der Orientierung des Bloch-Vektors entspricht, sind senkrechte Polarisationsrichtungen in dieser Darstellung antiparallel. Ein +45°- bzw. –45°-polarisiertes Photon entspricht der Orientierung des Bloch-Vektors in positive bzw. negative *x*-Richtung. In *y*-Richtung liegen die zirkular polarisierten Photonen.

Qubits zu experimentieren und die seltsamen quantenmechanischen Eigenschaften wie das Verhalten beim Messprozess zu verifizieren. Dabei wird für viele Systeme eine ganz außergewöhnliche Güte und Kontrollierbarkeit erreicht, wobei Experimente mit einzelnen Photonen, aber auch mit einzelnen Atomen oder Ionen möglich geworden sind.

4.1. Polarisationseigenschaften eines Photons

Eine Möglichkeit, ein Qubit zu realisieren, sind einzelne Photonen, wobei z. B. der Polarisationsfreiheitsgrad verwendet wird. Der Zustand $|0\rangle = |H\rangle$ ist dabei durch die horizontale Polarisation des Photons gegeben, der Zustand $|1\rangle = |V\rangle$ entspricht vertikaler Polarisation.

Der Überlagerungszustand

$$|0_x\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad \{20\}$$

entspricht einer Polarisation von 45°. Die Manipulation der Polarisation des Photons erfolgt durch doppelbrechende Kristalle mit unterschiedlicher Dicke, sogenannte Wellenplatten bzw. λ-Platten, wodurch Drehungen auf der Bloch-Kugel realisiert werden können. Messungen können mit Hilfe eines um 45° geneigten polarisierenden Strahlteilers durchgeführt werden, wobei ein horizontal polarisiertes Photon transmittiert wird, und ein vertikal polarisiertes Photon reflektiert und somit um 90° abgelenkt wird (siehe Abb. 10). Durch Einzel-Fotodetektoren an den beiden Ausgängen des polarisierenden Strahlteilers kann nun zwischen den beiden Zuständen $|H\rangle$ und $|V\rangle$ unterschieden werden, was einer *z*-Messung (Messung der Observablen σ_z) entspricht. Trifft ein in 45°-Richtung polarisiertes Photon

$$|0_x\rangle = \tfrac{1}{\sqrt{2}}(|H\rangle + |V\rangle) \qquad \{21\}$$

auf den polarisierenden Strahlteiler, so registriert nur jeweils einer der beiden Detektoren ein Photon – niemals beide. Das Photon wird mit einer Wahrscheinlichkeit von 50 % bei Detektor 1 registriert und somit transmittiert, und mit 50 % Wahrscheinlichkeit von Detektor 2 registriert und somit reflektiert. Wichtig ist aber festzuhalten, dass erst durch den Messprozess am Detektor der Überlagerungszustand zerstört wird. Dies lässt sich gut illustrieren, indem man die Anordnung durch zwei weitere Spiegel und einen zusätzlichen Strahlteiler ergänzt und ein Interferometer erhält, für dessen Funktion die Möglichkeit von Überlagerung und Interferenz eine zentrale Rolle spielen.

Die Verwendung der Polarisation greift ein Konzept auf, das bereits im Rahmen der klassischen Optik Anwendung findet und den Schülern bekannt ist. Dies ist einerseits für die Anschauung hilfreich, da nicht nur vertikale und horizontale Polarisation unmittelbar anschaulich sind, sondern auch Überlagerungszustände wie 45°-polarisiertes Licht bzw. ein in 45°-Richtung polarisiertes Photon:

$$|0_x\rangle = \tfrac{1}{\sqrt{2}}(|H\rangle + |V\rangle)\,. \qquad \{22\}$$

Auch die Manipulation des Quantenzustands und der Messprozess sind anschaulich und transparent.

Andererseits birgt diese unmittelbare Anschauung mit Hilfe des klassischen Konzepts der Polarisation von Lichtwellen aber auch die Gefahr, dass die neuen quantenmechanischen Eigenschaften nicht erkannt werden und als Eigenschaften gesehen werden, welche auch klassische Objekte (hier eine elektromagnetische Welle) besitzen. Im klassischen Fall ist aber von elektromagnetischen Wellen und nicht von einzelnen Photonen die Rede – und bei solchen klassischen Wellen tritt das typische quantenmechanische Verhalten bei Messungen bzw. die Quantisie-

rung des Polarisationsfreiheitsgrades nicht auf. Klassisch gesehen wird an einem polarisierenden Strahlteiler ein Teil der Welle transmittiert und ein Teil der Welle reflektiert, was lediglich zu einer Abschwächung der Amplitude der entsprechenden elektromagnetischen Welle führt. Erst durch die Quantisierung des Lichts und die Beschreibung durch einzelne Photonen ist es legitim von einem Quantenobjekt – einem Qubit – zu sprechen. Wir wollen auch darauf hinweisen, dass die Bloch-Kugel in diesem Fall nur bedingt zur anschaulichen Beschreibung geeignet ist bzw. leicht zu Verwirrung führen kann. In der Bloch-Kugel-Darstellung sind senkrechte Zustände antiparallel (z. B. entsprechen horizontal bzw. vertikal polarisierte Photonen einem Bloch-Vektor in positiver oder negativer *z*-Richtung), während Polarisationsvektoren, die orthogonalen Zuständen entsprechen – z. B. horizontale und vertikale Polarisation –, im Labor senkrecht aufeinander stehen. Dies hat seine Ursache in der Verwendung des Winkels $\vartheta/2$ in der abstrakten Bloch-Kugel-Darstellung. Die Bloch-Kugel beinhaltet nicht nur linear polarisierte Photonen, sondern alle möglichen Polarisationen des einzelnen Photons (siehe Abb. 11), z. B. auch zirkular polarisierte Photonen:

$$|0_y\rangle = \tfrac{1}{\sqrt{2}}(|H\rangle + i|V\rangle)\,. \qquad \{23\}$$

Experimente mit einzelnen Photonen sind sehr weit fortgeschritten, wobei die Manipulation, Übertragung und Messung von Einzelphotonenzuständen mit großer Güte realisiert werden kann. Für die Schule stehen gut ausgearbeitete Bildschirmexperimente zur Verfügung [4]. Im Bereich der Quantenkommunikation und Quantenkryptographie spielt die Realisierung von Qubits mit Hilfe von Photonen eine große Rolle, weil diese sich besonders gut für die Übertragung (mittels Glasfaserkabel oder im freien Raum) eignen. An dieser Stelle sei auch erwähnt, dass es noch eine Reihe weiterer Möglichkeiten gibt, einzelne Photonen zur Realisierung eines Qubits zu verwenden, bei denen nicht nur die Polarisation eine Rolle spielt. So z. B. eine Kodierung mit Hilfe einer Zeitverzögerung (Time-Bin-Photonen), aber auch die Verwendung von unterschiedlichen örtlichen Moden (ein Photon in Mode 1 – z. B. linker Pfad – entspricht dem Zustand $|0\rangle$, ein Photon in Mode 2 (rechter Pfad) entspricht dem Zustand $|1\rangle$).

4.2. Spin eines Teilchens

Der Spin eines Teilchens ist wohl das Lehrbuchbeispiel für ein diskretes quantenmechanisches System, und ist auch aus historischer Sicht besonders interessant. Der Spin ist eine quantenmechanische Eigenschaft, die kein direktes klassisches Analogon besitzt, und am ehesten als „Eigendrehimpuls“ eines Teilchens betrachtet werden kann. Ein Qubit wird dabei durch ein Spin-½-Teilchen realisiert, wobei die Zustände $|0\rangle = |\uparrow\rangle$ bzw. $|1\rangle = |\downarrow\rangle$ einer Orientierung des Spins in positive bzw. negative *z*-Richtung entsprechen. Überlagerungszustände entsprechen der

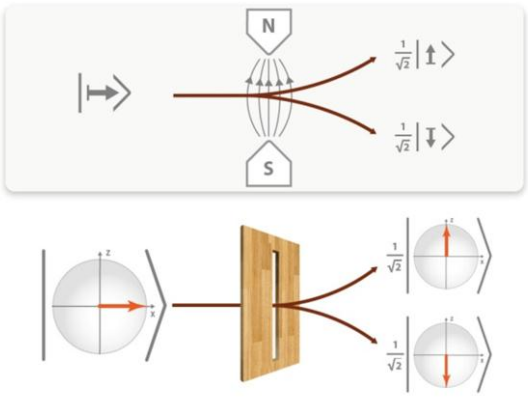

Abb. 12: Illustration des Messprozesses für Spins mit Hilfe des Stern-Gerlach-Apparates. Die Orientierung des inhomogenen Magnetfeldes bestimmt die Messrichtung (Schlitz), die hier gezeigte Anordnung entspricht einer Messung in *z*-Richtung. Durch die Kopplung des Spins an das inhomogene Magnetfeld erhält man eine diskrete Ablenkung des Teilchens, entsprechend der zwei möglichen Messergebnisse „Spin up“ und „Spin down“.

Orientierung des Spins in eine andere Raumrichtung, z. B. ergibt

$$|0_x\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad \{24\}$$

eine Orientierung in positive *x*-Richtung (siehe Abb. 11). Die Drehungen eines Spinzustandes erfolgt durch das Anlegen eines äußeren homogenen Magnetfeldes in eine bestimmte Raumrichtung. Der Spin (bzw. das zugehörige magnetische Moment) koppelt an das Magnetfeld und präzediert dadurch um die durch das Magnetfeld bestimmte Achse mit der sogenannten Larmor-Frequenz. Der gewünschte Rotationswinkel lässt sich durch die Dauer, für die das Magnetfeld angelegt wird, steuern. Die Messung eines Spins erfolgt mit Hilfe des bekannten Stern-Gerlach-Apparates, wobei das Teilchen ein *inhomogenes* Magnetfeld durchläuft, und abhängig von seinem Spin abgelenkt wird. Das Magnetfeld muss inhomogen sein, damit der Spin nicht nur mit konstanter Larmor-Frequenz präzediert, sondern tatsächlich in Richtung des Magnetfelds ausgerichtet wird. Dabei werden nur diskrete Ablenkungen beobachtet, da der Spin hierbei nur diskrete Werte annehmen kann (Abb. 12). Historisch wurde mit Hilfe eines solchen Experimentes – durchgeführt mit Silberatomen – erstmals die Quantisierung des Spins nachgewiesen. Die Messrichtung wird durch die Orientierung des inhomogenen Magnetfeldes bestimmt, wobei die *z*-Messung einer Orientierung des Magnetfeldes in *z*-Richtung entspricht. Für den Spin ist die Bloch-Kugel-Darstellung unmittelbar geeignet, da die tatsächliche räumliche Orientierung eines Spin-Eigenzustandes mit der Orientierung

$$\sigma_{\mathbf{a}} = a\cdot\sigma = a_x\sigma_x + a_y\sigma_y + a_z\sigma_z \qquad \{25\}$$

des Spins in der abstrakten Bloch-Kugel-Darstellung übereinstimmt.

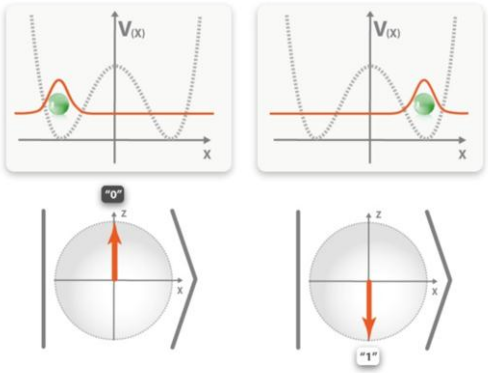

Abb. 13: Realisierung eines Qubits durch Ortsfreiheitsgrade eines einzelnen Atoms. Der Zustand $|0\rangle$ entspricht der Lokalisierung des Atoms im linken Topf eines Doppeltopfpotentials, während der Zustand $|1\rangle$ der Lokalisierung im rechten Topf entspricht.

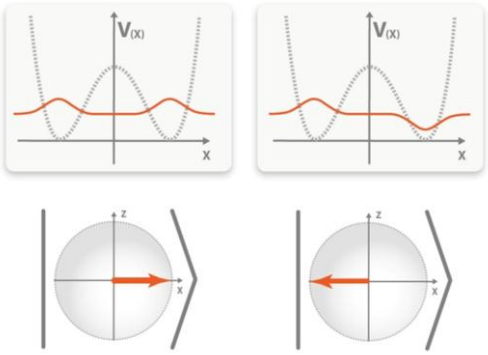

Abb. 14: Überlagerungszustände eines einzelnen Atoms im Doppeltopfpotential. Der Zustand $|0_x\rangle$ entspricht der symmetrischen Überlagerungszustand, während der Zustand $|1_x\rangle$ einem antisymmetrischen Überlagerungszustand entspricht.

Der Messprozess kann mit Hilfe des Stern-Gerlach-Apparates gut illustriert werden. Insbesondere sind auch Messungen in unterschiedlichen Richtungen einfach zu behandeln. Ein Problem für die Erklärung im Unterricht könnte aber die fehlende Anschauung für den Spin sein – es gibt kein direktes klassisches Analogon, sieht man von dem formalen Verhalten als Eigendrehimpuls ab, was aber für ein Punktteilchen aus klassischer Sicht widersprüchlich ist.

In Quantenpunkten (Quantum Dots) werden einzelne Elektronen mittels elektrischer Felder gespeichert und der Elektronenspin zur Realisierung eines Qubits verwendet. Basierend auf diesem Prinzip gibt es auch Vorschläge zur Realisierung von Quanteninformationsverarbeitung bzw. eines skalierbaren Quantencomputers [12]. Auch die Experimente in diese Richtung sind weit fortgeschritten, wenn auch die Qualität der einzelnen Operationen und Messungen, insbesondere im Vergleich zu Experimenten mit Ionen oder auch Photonen, noch deutlich geringer ist. Aufgrund der höheren Kohärenzzeiten wird auch über die Verwendung von Kernspins zur Speicherung von Quanteninformation nachgedacht.

4.3. Ortszustände eines Atoms

Eine weitere mögliche Realisierung eines Qubits ist durch die Verwendung des Ortsfreiheitsgrades von Atomen gegeben, wobei nur zwei Orte betrachtet werden. Im klassischen Bild entspricht dies einem Ball auf einem von zwei Regalen. Für das Atom bedeutet das nun, dass der Zustand $|0\rangle$ der Ortskoordinate x_0 entspricht, während der Zustand $|1\rangle$ der Ortskoordinate x_1 entspricht (Abb. 13) [5]. Überlagerungszustände sind in diesem Bild besonders schwer mit unserer klassischen Vorstellung zu vereinbaren, in der sich Teilchen ja nur an einem Ort befinden können – und nicht an beiden Orten gleichzeitig. Trotzdem lassen sich auch solche Qubits experimentell realisieren, wobei dabei ein einzelnes Atom in einem Doppeltopfpotential gefangen wird (Abb. 14). Durch Manipulation der Potentialbarriere zwischen den beiden Töpfen ermöglicht man einen kohärenten Tunnelprozess und somit die Manipulation des Quantenzustands. Die *z*-Messung entspricht einer Ortsmessung, d. h. der Beobachtung, in welchem der beiden Potentialtöpfe sich das Atom befindet. In diesem Bild wird es besonders deutlich, welche (seltsamen) Konsequenzen aus dem quantenmechanischen Superpositionsprinzip folgen – nämlich die Existenz von Überlagerungszuständen, bei denen sich ein Teilchen an zwei verschiedenen Orten befindet – oder genauer gesagt, bei dem die Ortseigenschaft nicht festgelegt ist. Dieses Prinzip liegt auch dem bekannten Beispiel von Schrödinger mit der sogenannten Schrödinger-Katze zugrunde – mit dem er gerade diese schwer vorstellbaren und mit unserer Alltagserfahrung im direkten Konflikt stehenden Eigenschaften der Quantenmechanik illustrieren wollte.

Dabei befindet sich ein makroskopisches Objekt – in diesem Fall eine Katze – im Produktzustand $1/\sqrt{2}$ ($|0\rangle$ |Katze lebt$\rangle$) + ($|1\rangle$ |Katze tot$\rangle$), wobei sowohl das Atom als auch die Katze sich in einer Überlagerung von zwei Quantenzuständen befinden. Im Gedankenexperiment von Schrödinger hängt der Zustand der Katze vom Zerfall eines einzelnen radioaktiven Atoms ab – hier symbolisiert durch die Zustände $|0\rangle$ und $|1\rangle$. Die Frage „ob die Katze nun tot ist oder noch lebt, so lange niemand hinsieht“ (bzw. eine Messung durchführt) ist unter Verwendung dieser klassischen Begriffe, die nur ein „entweder oder“, und kein „sowohl als auch“ zulassen, nicht zufriedenstellend möglich. Die Katze befindet sich in einem Überlagerungszustand, in der diese Eigenschaft nicht definiert bzw. festgelegt ist.

Erst bei einer Messung ändert sich der Zustand der Katze – und danach ist sie entweder tot oder lebendig. Aus didaktischer Sicht gibt es mehrere Probleme bei diesem Gedankenexperiment. Zum einen verlassen wir mit diesem Beispiel die Ein-Teilchen-Quantenphysik, betrachten also keine einzelnen

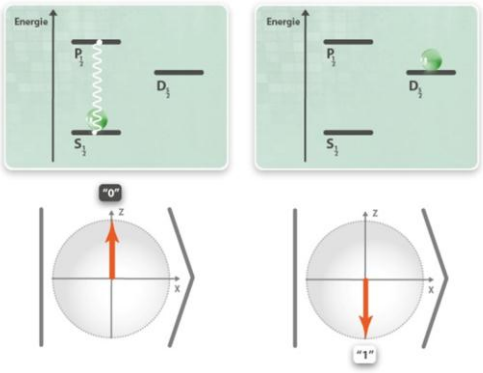

Abb. 15: Realisierung eines Qubits durch elektronische Zustände eines Atoms (Termschema). Der Zustand $|0\rangle$ entspricht der Besetzung des $S_{1/2}$-Niveaus, während der Zustand $|1\rangle$ der Besetzung des $D_{5/2}$-Niveaus entspricht. Eine z-Messung wird durch Streuung von Laserlicht am $S_{1/2}$-$P_{1/2}$-Übergang realisiert.

Qubits mehr, sondern Produktzustände, was eine zusätzliche Komplikation bedeutet. Weiterhin ist hierbei problematisch, dass der Begriff der „Beobachtung“ in der Alltagssprache an menschliche Sinne und an Bewusstsein geknüpft ist. In der Quantenphysik hat Beobachtung aber nichts mit Sinneseindrücken oder Bewusstsein zu tun, sondern lediglich mit der Wechselwirkung des Qubits mit der Umgebung bzw. dem Messapparat, durch die die Superposition zwischen zwei Überlagerungszuständen zerstört wird. In Abb. 7 und Abb. 8 wird diese Wechselwirkung des Qubits mit der Umgebung visualisiert. Für makroskopische Objekte ist eine kohärente Superposition schwierig, aber nicht unter allen Umständen unmöglich. Heutzutage ist man bestrebt, quantenmechanische Überlagerungszustände von makroskopischen Objekten, z. B. eines kleinen Spiegels oder einer großen Anzahl von Photonen oder Atomen im Labor herzustellen [6, 7]. Allerdings muss davor gewarnt werden, Begriffe der Quantenphysik mit Alltagsbegriffen, insbesondere zu Bewusstsein, Leben und Tod zu vermengen. Um diese Problematik zu vermeiden, ist es besser, von Überlagerungszustanden makroskopischer Objekte zu sprechen, in dem sich z. B. ein Objekt, bestehend aus einer großen Anzahl von Atomen, entweder am Ort x_0 oder am Ort x_1 befindet. Auch das strapaziert unsere Alltagsvorstellung bereits stark, und spiegelt die derzeit durchgeführten Experimente besser wieder. In diesem Zusammenhang sollte noch erwähnt werden, dass es eine Reihe weiterer Experimente gibt, welche Quanteneigenschaften bei mesoskopischen bzw. makroskopischen Objekten nachweisen, etwa die Beobachtung von Welleneigenschaften von Molekülstrukturen mit immer größerer Masse am Doppelspalt bzw. Gitter [8].

4.4. Elektronische Zustände eines Atoms oder Ions

Eine weitere Möglichkeit zur Realisierung eines Qubits durch einzelne Atome oder Ionen besteht in der Verwendung von zwei internen (elektronischen) Zuständen. Sämtliche anderen Freiheitsgrade des Atoms werden dabei eingefroren, insbesondere wird das Atom mittels Laserkühlung in den Bewegungsgrundzustand gekühlt. Ionen werden dabei in einer Paul-Falle gefangen, wobei ein rotierendes Sattelpotential für einen Einschluss in alle drei Raumrichtungen sorgt. Die Manipulation des Quantenzustands erfolgt durch Laserpulse von bestimmter Frequenz und Dauer, welche die beiden elektronischen Zustände entweder direkt oder mittels eines Raman-Übergangs koppeln. Der Messprozess findet mittels eines zusätzlichen metastabilen internen Hilfszustandes statt. Durch einen Laserpuls wird dabei einer der internen Zustände – z. B. $|0\rangle$ – mit dem Hilfsniveau gekoppelt, wobei dieser Hilfszustand dann unter Aussendung eines Photons wieder in den Zustand $|0\rangle$ zerfällt. Durch Detektion dieser Photonen erfolgt der Messprozess, genauer gesagt eine z-Messung, wobei eine fehlende Detektion von Photonen dem Messergebnis $|1\rangle$ entspricht.

Für die Anschauung ist es hilfreich, auf bekannte Atommodelle – etwa das von Rutherford – Bezug zu nehmen. Dabei kann der Zustand $|0\rangle$ einer Elektronwelle auf einer „Bahn“ mit kleinerem Radius entsprechen, während der Zustand $|1\rangle$ einem angeregten Zustand mit einem größeren Bahnradius entspricht. In der tatsächlichen experimentellen Realisierung werden unterschiedliche Atomniveaus verwendet – z. B. bei Experimenten mit $^{40}Ca^{+}$-Ionen das $S_{1/2}$ ($m = -1/2$)- und das $D_{5/2}$ ($m = -1/2$)-Niveau für die Zustände sowie das $P_{1/2}$-Niveau als Hilfsniveau für den Messprozess, wobei Licht am $S_{1/2}$-$P_{1/2}$-Übergang gestreut wird. Bei anderen Experimenten, etwa mit neutralen Atomen, werden auch Zustände der Hyperfeinstruktur verwendet. Die Experimente mit einzelnen Atomen, insbesondere aber mit einzelnen Ionen, sind sehr weit fortgeschritten [6, 9]. Dabei ist es möglich, einzelne Atome mit einer Güte von ca. 99.9 % kontrolliert zu manipulieren und auch zu messen. In der Tat sind ultrakalte Ionen und Atome eine sehr vielversprechende Basis für Quanteninformationsverarbeitung – auch von mehreren Qubits –, wobei z. B. verschränkte Zustände von bis zu 14 Ionen kontrolliert hergestellt wurden.

5. Anwendungen

Wir wollen nun noch einige Anwendungen der bisher besprochenen Prinzipien näher erläutern. Dabei steht das Verhalten eines quantenmechanischen Systems bei Messungen im Mittelpunkt. Wir wollen dabei sowohl grundsätzliche Aspekte betrachten, etwa die Möglichkeit, einen unbekannten Quantenzustand zu bestimmen bzw. zu kopieren, als auch eine qualitative Diskussion der Heisenberg‘schen Unschärferelation. Abschließend gehen wir noch auf anwendungsbezogene Aspekte im Zusammenhang mit der sicheren Übermittlung von geheimen Nachrichten im Rahmen der Quantenkryptographie ein.

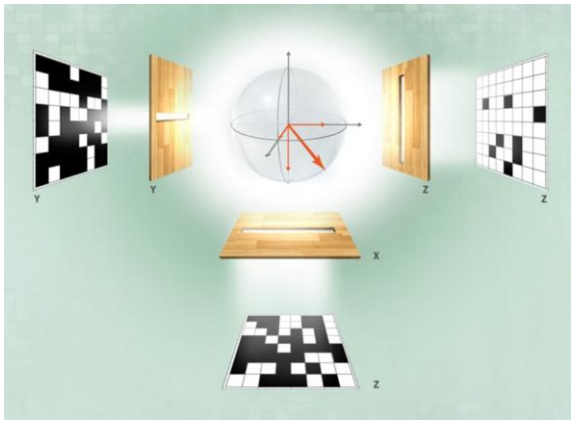

Abb. 16: Zur Bestimmung eines quantenmechanischen Zustands ist eine Zustandstomographie an einem großen Ensemble aus identisch präparierten Qubits notwendig. Messungen in x, y- bzw. z-Richtung liefern dabei die Erwartungswerte der Observablen σ_x, σ_y bzw. σ_z, was den Projektionen des Bloch-Vektors auf die x-, y- bzw. z-Achse entspricht.

5.1. Zustandstomographie

Aus dem Verhalten eines Qubits bei Messungen folgt, dass es nicht möglich ist, den Zustand eines einzelnen Qubits vollständig zu bestimmen. Eine Messung – egal in welcher Basis – liefert ein Bit an Information: die Antwort auf eine Ja/Nein-Frage. Da der Zustand des Systems durch diese Messung aber verändert wird, ist es nicht möglich, weitere Information über den ursprünglichen Zustand zu gewinnen. Betrachten wir dazu ein allgemeines Qubit im Zustand (Abb. 2)

$$|\psi\rangle = \cos\tfrac{\vartheta}{2}\,|0\rangle + \sin\tfrac{\vartheta}{2}\,e^{i\varphi}\,|1\rangle\,. \qquad \{26\}$$

Eine *z*-Messung liefert mit der Wahrscheinlichkeit

$$p_0 = \cos^2\tfrac{\vartheta}{2} \qquad \{27\}$$

das Ergebnis $|0\rangle$, und mit der Wahrscheinlichkeit

$$p_1 = \sin^2\tfrac{\vartheta}{2} \qquad \{28\}$$

das Ergebnis $|1\rangle$. Nach dieser Messung ist der Zustand des Qubits aber durch $|0\rangle$ oder $|1\rangle$ gegeben und enthält keine Information mehr über die Parameter ϑ bzw. φ (Abb. 7). Ebenso wenig hat uns das Ergebnis dieser Messung eine vollständige Information über diese Parameter verschafft. Uns liegt lediglich ein (zufälliges) Messergebnis vor, und wir können nur Vermutungen über den ursprünglichen Zustand machen.

Es ist aber möglich, den Zustand des Qubits mit gewünschter Genauigkeit zu bestimmen, wenn ein reines Ensemble von *N* identischen Kopien des (unbekannten) Quantenzustands $|\psi\rangle$ vorliegt. Führen wir nun an jeder der Kopien dieses Zustands unabhängig voneinander *z*-Messungen durch, so erhalten wir eine Sequenz von *N* zufälligen Messergebnissen. Wir können nun aus der Statistik der resultierenden Wahrscheinlichkeitsverteilung den Parameter ϑ bestimmen. Dazu muss lediglich die relative Häufigkeit der Messergebnisse berechnet werden, also

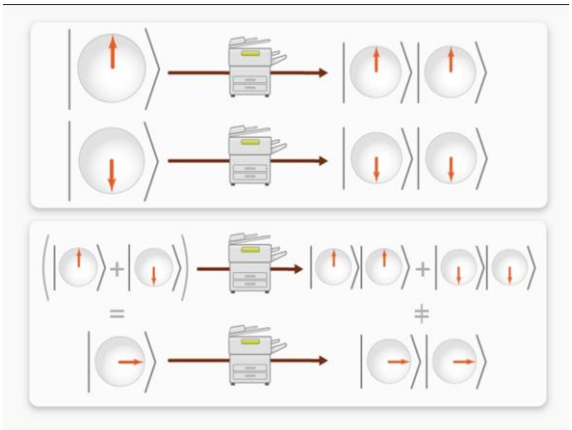

Abb. 17: Illustration des No-Cloning-Theorems. Wenn das Kopieren der Basiszustände $|0\rangle$ und $|1\rangle$ möglich wäre, würde die entsprechende Quantenkopiermaschine für einen Überlagerungszustand $|0\rangle + |1\rangle$ ein falsches Resultat liefern. Es kann also keinen Quantenkopierer geben.

$$(N_0(+1) + N_1(-1))/N\,, \qquad \{29\}$$

wobei die Messergebnisse durch die Eigenwerte +1 (für $|0\rangle$) bzw. –1 (für $|1\rangle$) gegeben sind. Für große *N* nähert sich die relative Häufigkeit dem Erwartungswert

$$\begin{aligned}\langle\sigma_z\rangle_{|\psi\rangle} &= p_0(+1) + p_1(-1)\\ &= \cos^2\tfrac{\vartheta}{2} - \sin^2\tfrac{\vartheta}{2} = \cos\vartheta\end{aligned}\,, \qquad \{30\}$$

wobei die Varianz und somit die Messgenauigkeit mit $1/\sqrt{N}$ skaliert. Dadurch kann nun der Parameter ϑ mit gewünschter Genauigkeit bestimmt werden. Allerdings liefern diese Messungen keinerlei Information über den Parameter φ. Dazu ist es notwendig, zusätzliche Messungen an weiteren Kopien des Zustands in einer anderen Messbasis, z. B. der *x*-Basis durchzuführen. Die Wahrscheinlichkeit, den Zustand $|0_x\rangle$ (bzw. das Messergebnis +1) zu finden, ist durch

$$p_0 = |\langle\psi\,|\,0_x\rangle|^2 = \tfrac{1}{2}\,|\cos\tfrac{\vartheta}{2} + \sin\tfrac{\vartheta}{2}\,e^{i\varphi}\,|^2 \qquad \{31\}$$

gegeben. Daraus ergibt sich als Erwartungswert für die Observable σ_x:

$$\langle\sigma_x\rangle_{|\psi\rangle} = p_0(+1) + p_1(-1) = \cos\varphi\sin\vartheta. \qquad \{32\}$$

Ist nun ϑ bereits durch die Sequenz von *z*-Messungen bekannt, so kann aus der relativen Häufigkeit der *x*-Messungen der Erwartungswert $\langle\sigma_x\rangle_{|\psi\rangle}$ und daraus φ bestimmt werden (allerdings nicht eindeutig). Für die vollständige Kenntnis von φ ist eine weitere Messsequenz notwendig, z. B. durch *y*-Messungen.

Betrachtet man das Problem der Bestimmung eines unbekannten Zustands in der Bloch-Kugel, so ist es notwendig, die Orientierung des Vektors im Raum zu bestimmen. Dazu benötigt man die Projektionen des Bloch-Vektors auf die *x*-, *y*- bzw. *z*-Achse.

Dies entspricht aber genau den Erwartungswerten der Observablen σ_x, σ_y bzw. σ_z. In Abb. 16 entspricht die experimentelle Bestimmung der Observablen σ_z der Messung durch den „*z*-Schlitz“, wobei das Ergebnis „0“ durch ■, das Ergebnis „1“ durch □ visualisiert wird [10]. Durch das Abzählen der schwarzen und weißen Kästchen lässt sich die Projektion der Länge des Zustandsvektors auf die *z*-Achse experimentell bestimmen. Entsprechendes gilt für die Observablen σ_x und σ_y.

5.2. No-Cloning-Theorem

Aus den vorgestellten Prinzipien ergibt sich, dass Quanteninformation nicht kopiert werden kann – was im sogenannten „No-Cloning-Theorem“ [11] ausgedrückt wird. Wie bereits im vorigen Abschnitt diskutiert, kann Quanteninformation nicht einfach durch Auslesen des Quantenzustands kopiert werden – es wäre notwendig, mehrere Kopien zur Verfügung zu haben, um durch Messungen die Erwartungswerte von verschiedenen Observablen zu ermitteln, um damit wiederum auf die Koeffizienten α und β zu schließen. Eine einzelne Messung liefert nur 1 Bit an Information über 2 reelle Zahlen. Theoretisch könnte man zwar fordern, dass eine unitäre Operation Kopien der Basiszustände $|0\rangle$ und $|1\rangle$ herstellt – damit ist die Wirkung der unitären Operation aber bereits fixiert:

$$|00\rangle \rightarrow |00\rangle \ , \ |10\rangle \rightarrow |11\rangle \, , \qquad \{33\}$$

und es lässt sich leicht zeigen, dass durch eine solche Operation der Überlagerungszustand

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad \{34\}$$

nicht korrekt kopiert wird, da

$$|\psi\rangle|0\rangle \xrightarrow{U} \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \neq |\psi\rangle|\psi\rangle \qquad \{35\}$$

Es lässt sich ganz allgemein zeigen, dass es keinen quantenmechanischen Prozess geben kann, der es erlaubt, den unbekannten Zustand eines Qubits zu kopieren. Es ist lediglich die Herstellung von zwei oder mehr imperfekten Kopien möglich, wobei die Quanteninformation auf mehrere Qubits verteilt, aber nicht kopiert wurde. Das No-Cloning-Theorem spiegelt eine zentrale Eigenschaft der Quantenwelt wieder, und führt auch zu interessanten Anwendungen, z. B. im Bereich der Quantenkryptographie.

5.3. Sequenz von Messungen

Wir wollen nun eine Sequenz von verschiedenen Messungen behandeln, und dabei die Wahrscheinlichkeiten betrachten, ein bestimmtes Messergebnis zu erhalten. Betrachten wir zunächst ein Qubit im Zustand $|0\rangle$, an dem eine *z*-Messung durchgeführt wird. Das Ergebnis der Messung wird immer „$|0\rangle$“ sein, und dementsprechend ist die Wahrscheinlichkeit, das Ergebnis „$|1\rangle$“ zu erhalten, gleich null. Betrachtet man den Messapparat als Filter, welcher Qubits mit der Eigenschaft „$|1\rangle$“ passieren lässt, so werden alle Teilchen geblockt. Bei einer physikalischen Realisierung des Messprozesses mittels eines Stern-Gerlach-Apparates entspricht dies dem Blocken eines der beiden Messzweige – ebenso bei der Messung von Photonen mit Hilfe eines polarisierenden Strahlteilers (siehe Abb. 18, 19 sowie die Abschnitte 4.1 und 4.2).

Wir betrachten nun einen zweiten Filter, der einer *x*-Messung (Messung der Observablen σ_x) entspricht. Dabei können nur jene Qubits passieren, welche die Eigenschaft

$$|1_x\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \qquad \{36\}$$

besitzen. Führt man nun eine solche *x*-Messung vor der *z*-Messung durch, so passiert Folgendes:

Mit der Wahrscheinlichkeit $p_0 = 0{,}5$ liefert die *x*-Messung am Eingangszustand $|1\rangle$ das Ergebnis $|0_x\rangle$. In diesem Fall hat sich der Zustand des Systems nach dieser Messung verändert und ist nun durch $|0_x\rangle$ gegeben. Eine nachfolgende *z*-Messung liefert mit der Wahrscheinlichkeit $p_0 = 0{,}5$ das Ergebnis $|0\rangle$. Insgesamt ist die Wahrscheinlichkeit, dass das Teilchen beide Filter passiert, $0{,}25$, d. h. im Schnitt passiert eines von 4 Teilchen beide Filter, während bei Vorhandsein nur des zweiten Filters (*z*-Messung) kein Teilchen den Filter passiert. Durch das Vorschalten eines zusätzlichen Filters wurde also die Wahrscheinlichkeit erhöht, dass Teilchen passieren können.

Das analoge Experiment mit Photonen lässt sich in der Schule mit folgender Anordnung von linearen Polarisationsfiltern einfach durchführen: Zwei orthogonale Polarisationsfilter lassen zunächst kein Licht mehr hindurch. Wird ein dritter Polarisationsfilter zwischen die beiden Filter gebracht, kann doch etwas Licht passieren, bei der 45°-Stellung ist das Transmissionsmaximum erreicht, mit genau ¼ der Ausgangsintensität. Im Bild einzelner Teilchen bzw. Photonen zeigt sich deutlich, dass eine „Messung“ bzw. Wechselwirkung mit dem Filter den Zustand verändert.

5.4. Heisenberg‘sche Unschärferelation

Wir wollen uns noch mit der Messung von unterschiedlichen Eigenschaften bzw. Observablen eines Qubits beschäftigen. Dabei ist zu beachten, dass Messungen in unterschiedlichen Basen “komplementär“ sind, da sie Bezug auf unterschiedliche Eigenschaften des Systems nehmen. Man muss sich für *eine* Eigenschaft, die gemessen werden soll, entscheiden. Ist ein System etwa im Zustand

$$|0_x\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \, , \qquad \{37\}$$

liefert eine Messung der Observablen σ_x ein deterministisches Ergebnis. Eine Messung der Observablen σ_z liefert hingegen ein vollkommen zufälliges Ergebnis – der Zustand $|0_x\rangle$ besitzt die Eigenschaft $|0\rangle$ oder $|1\rangle$ nicht.

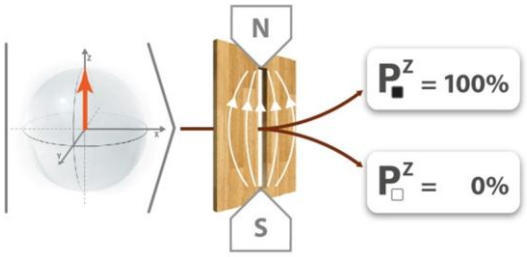

Abb. 18: Blockt man bei einem Stern-Gerlach-Versuch einen Zweig, so kann dies als „Filter“ gesehen werden. Ein in $|0\rangle$ präpariertes Qubit wird dementsprechend immer den oberen Zweig nehmen (Messergebnis +1 bzw. Zustand „$|0\rangle$“ mit Wahrscheinlichkeit 1). Wird der obere Zweig geblockt, kommt keines der Teilchen durch den Filter.

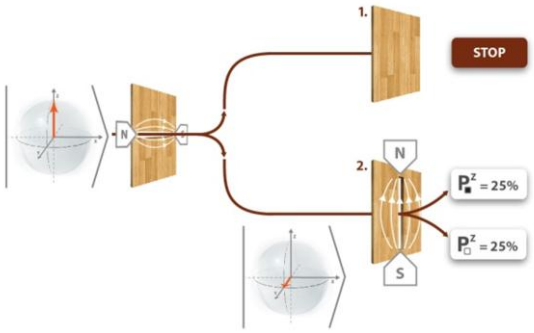

Abb. 19: Darstellung einer Sequenz von Messungen in unterschiedlichen Messbasen bzw. Messrichtungen. Schaltet man vor dem in Abb. 18 gezeigten Filter in *z*-Richtung einen weiteren, in *x*-Richtung orientierten Filter (nur Qubits im Zustand $|1_x\rangle$ können den Filter passieren), so kann nun ein Qubit im Zustand $|0\rangle$ die gesamte Anordnung mit der Wahrscheinlichkeit ¼ passieren, während dies ohne den zusätzlichen Filter nicht möglich ist.

Dies äußert sich auch formal dadurch, dass für diesen Zustand für Erwartungswert und Varianz gilt:

$$\langle \sigma_x \rangle_{|0_x\rangle} = +1\,, \qquad \{38\}$$

$$\langle \sigma_z \rangle_{|0_x\rangle} = 0\,, \qquad \{39\}$$

$$V(\sigma_x)_{|0_x\rangle} = 0\,, \qquad \{40\}$$

$$V(\sigma_z)_{|0_x\rangle} = 1\,. \qquad \{41\}$$

Dabei haben wir verwendet, dass

$$\begin{aligned} V(\sigma_{\mathbf{a}})_{|\psi\rangle} &= \langle (\sigma_{\mathbf{a}} - \langle \sigma_{\mathbf{a}} \rangle)^2 \rangle_{|\psi\rangle} \\ &= \langle \sigma^2{}_{\mathbf{a}} \rangle_{|\psi\rangle} - \langle \sigma_{\mathbf{a}} \rangle^2{}_{|\psi\rangle} \\ &= 1 - \langle \sigma_{\mathbf{a}} \rangle^2{}_{|\psi\rangle} \end{aligned} \quad . \qquad \{42\}$$

Die Varianz ist dabei ein Maß für die Größe der Fluktuationen um den Erwartungswert, wobei Varianz 0 bedeutet, dass keine Fluktuationen auftreten und man dieser Eigenschaft einen fixen Wert zuordnen kann. Dies bedeutet nun aber, dass wenn eine Observable einen festgelegten („scharfen“) Wert besitzt (also Varianz = 0, die Eigenschaft bezüglich dieser Observablen ist festgelegt), die Varianz der zweiten (komplementären) Observablen groß ist, deren Wert also nicht festgelegt ist. Dies gilt für die Observablen σ_z und σ_x nicht nur für den speziellen Zustand $|0_x\rangle$, sondern für jeden Zustand $|\psi\rangle$ – es existiert kein Zustand, bei dem die Varianz von σ_x und σ_z beide klein sein können. In diesem Sinne sind die Observablen σ_x und σ_z komplementär.

Dies entspricht derselben Situation, wie sie bei der Heisenberg‘schen Unschärferelation für die Varianzen von Ort und Impuls vorliegt – dort kann dies allerdings noch quantitativ gefasst werden durch $\Delta x\, \Delta p \geq \hbar/2$. Auch dort entsprechen Ort und Impuls unterschiedlichen Eigenschaften des Quantensystems – bzw. äquivalent dazu Messungen in unterschiedlichen Basen, der Ortsbasis und der Impulsbasis. Ortsbasis und Impulsbasis hängen dabei mittels Fourier-Transformation zusammen, und die Heisenberg‘sche Unschärferelation drückt in diesem Fall lediglich aus, dass Funktionen, die im Ortsraum stark lokalisiert sind, im Impulsraum (bzw. Frequenzraum) nicht lokalisiert sind und deshalb bei Messungen zu großen Varianzen bzw. Fluktuationen führen. Man kann einem Quantensystem nicht gleichzeitig eine Ortseigenschaft und eine Impulseigenschaft genau zuordnen. Interessant ist auch noch zu erwähnen, dass die *z*-Basis und *x*-Basis des Qubits auch über eine (diskrete) Fourier-Transformation zusammenhängen – die sich für ein einzelnes Qubit auf $U = |0\rangle\langle 0_x| + |1\rangle\langle 1_x|$ vereinfacht. Die Unschärferelation gilt auch für andere komplementäre Observablen, wobei in diesem Fall die Erklärung mittels Fourier-Transformation nicht ausreicht.

5.5. Zufallsgeneratoren

Die Erzeugung von „echten“ Zufallszahlen ist für viele technische Anwendungen, insbesondere im Bereich von numerischen Computersimulationen, von großer Bedeutung. Häufig werden dabei sogenannte Pseudo-Zufallszahlen verwendet, welche durch bestimmte Algorithmen erzeugt werden. Dies ist für manche Anwendungen aber nicht ausreichend. Die Messung eines einzelnen Qubits bietet die Möglichkeit, echte Zufallsbits und in weiterer Folge Zufallszahlen zu erzeugen. Dazu wird lediglich ein Qubit im Zustand $|0_x\rangle$ präpariert und eine Messung des Qubits in der *z*-Basis $|0\rangle$, $|1\rangle$ durchgeführt. Solche Quantenzufallsgeneratoren sind kommerziell zu erwerben [13].

5.6. Quantenkryptographie – das BB84-Protokoll

Wir wollen uns abschließend noch mit einer modernen praktischen Anwendung einzelner Qubits im

Rahmen der Quantenkryptographie beschäftigen [15]. Dabei geht es um die Übermittlung von geheimen Nachrichten von einem Sender (Alice) zu einem Empfänger (Bob). Genauer gesagt wird dabei die Übermittlung von einzelnen Qubits im Rahmen der Quantenkommunikation dazu benutzt, einen geheimen Schlüssel – also eine Sequenz von Zufallsbits, die nur Alice und Bob bekannt sind – zu erzeugen. Daraus lässt sich dann eine beliebige Nachricht gleicher Länge unter Verwendung des sogenannten One-time-pads abhörsicher übertragen, indem die Zufallsbits zuerst von Alice zur Nachricht addiert werden, und danach von Bob wieder subtrahiert werden. Durch die Addition der Zufallszahlen verliert die übermittelte Nachricht jede Struktur und kann ohne Kenntnis des Schlüssels nicht decodiert werden.

Für den Aufbau des Schlüssels gibt es mehrere Verfahren, deren Sicherheit auf den physikalischen Prinzipien der Quantenmechanik beruht. Wir wollen hier das sogenannte BB84-Protokoll – benannt nach dessen Erfindern C. Bennett und G. Brassard – näher behandeln. Die Sicherheit des Protokolls beruht darauf, dass jeder Versuch, Information über gesendete Quantenzustände zu gewinnen, eine Messung bedeutet und somit notwendigerweise zu einer Veränderung des Quantenzustands führt. Diese Veränderung kann detektiert werden, und dadurch ist es möglich, auf die Anwesenheit eines Lauschers zu schließen. Darüber hinaus ist es nicht möglich, einen unbekannten Quantenzustand zu kopieren bzw. den Quantenzustand vollständig zu bestimmen. Diese beiden Aspekte gemeinsam können dazu verwendet werden, ein Verfahren zu entwickeln, bei dem die Sicherheit des Schlüssels durch Naturgesetze – genauer durch das Verhalten von Quantensystemen bei Messungen – gewährleistet ist. Dies ist im Gegensatz zu klassischen Kryptographieverfahren wie z. B. der häufig verwendeten RSA-Verschlüsselung zu sehen, deren Sicherheit auf unbewiesenen Annahmen über die Komplexität bzw. Schwierigkeit von bestimmten Rechenoperationen beruhen – z. B. der Primfaktorzerlegung einer großen Zahl.

Beim BB84-Protokoll werden einzelne Qubits von Alice zu Bob geschickt und dort gemessen. Zu diesem Zweck wählt Alice zunächst zufällig einen Bitwert $j \in \{0,1\}$ aus, den sie übermitteln will. Ebenso wählt sie zufällig eine Basis $\alpha \in \{z,x\}$, in der das Qubit präpariert werden soll. Alice präpariert nun das Qubit im Zustand $|j_\alpha\rangle$, also einem der vier Zustände

$$|0\rangle, |1\rangle, |0_x\rangle, |1_x\rangle \qquad \{43\}$$

mit

$$|0_x\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad \{44\}$$

und

$$|1_x\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\,. \qquad \{45\}$$

Das Qubit wird jetzt an Bob gesendet, der selbst zufällig eine Messbasis $\beta \in \{z,x\}$ auswählt. Dabei erfolgt die Messung des Qubits entweder in der *z*-Basis (Messung der Observablen σ_z) oder in der *x*-Basis (Messung der Observablen σ_x). Stimmen die Präparationsbasis α und die Messbasis β überein, so erhält Bob bei seiner Messung ein deterministisches Ergebnis – nämlich den Zustand $|j_\alpha\rangle$ – und kann daraus den gesendeten Bitwert j ermitteln. Stimmen Messbasis und Präparationsbasis aber nicht überein, so liefert die Messung bei Bob ein vollkommen zufälliges Ergebnis. Zum Beispiel ist für $\alpha = x$ und $j = 0$ der gesendete Zustand

$$|0_x\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,. \qquad \{46\}$$

Eine Messung in der z-Basis ($\beta = z$) liefert das Ergebnis $|0\rangle$ bzw. $|1\rangle$ jeweils mit einer Wahrscheinlichkeit $p_0 = p_1 = 0{,}5$.

Es werden nun auf diese Weise N Qubits von Alice präpariert und von Bob gemessen, wobei für jedes Qubit unabhängig voneinander von Alice die Präparationsbasis α und der Bitwert j, und von Bob die Messbasis β zufällig festgelegt werden. Es erfolgt anschließend die Diskussion der verwendeten Basen über einen öffentlichen Kanal. Das heißt, Alice und Bob geben öffentlich bekannt, in welcher Basis das jeweilige Qubit präpariert bzw. gemessen wurde. Dies beinhaltet aber *nicht* die Information über den präparierten bzw. gemessenen Bitwert. Stimmen Präparationsbasis und Messbasis überein, also $\alpha = \beta$, so wissen wir aus den obigen Überlegungen, dass Bobs Messergebnis mit dem gesendeten Bitwert übereinstimmt. Alice und Bob besitzen also eine gemeinsame Sequenz von etwa $\tilde{N} \approx N/2$ korrelierten Zufallsbits. In einem abschließenden Kontrollschritt wählen Alice und Bob zufällig M ihrer Zufallsbits aus und vergleichen den Bitwert über einen öffentlichen Kanal. Stimmen alle dieser M Bits überein, so können Alice und Bob bei hinreichend großem M sicher sein, dass ein etwaiger Lauscher (Eavesdropper) keine Information über die zufällige Bitsequenz gewonnen hat. Die restlichen Zufallsbits können dann zur Übermittlung einer geheimen Nachricht verwendet werden. Für den Fall, dass viele der Kontrollbits nicht übereinstimmen, muss daraus geschlossen werden, dass möglicherweise ein Lauscher Information über die gesamte Bitsequenz gewonnen hat, und es ist keine sichere Datenübermittlung möglich.

Wir wollen nun noch die Sicherheit des vorgestellten Protokolls diskutieren. Dazu betrachten wir eine konkrete Abhörstrategie des Lauschers. Um Information über den Bitwert eines gesendeten Qubits zu erhalten, ist es notwendig, eine Messung durchzuführen. Da der Lauscher Eve die Basis der gesendeten Bits nicht kennt, wäre eine Möglichkeit, seine Messbasis $\gamma \in \{z,x\}$ zufällig zu wählen. Es ist notwendig, verschiedene Fälle zu unterscheiden, wobei wir uns auf erfolgreiche Übermittlungsversuche beschränken wollen, also auf jene Fälle, in denen

$\alpha = \beta$, d. h. die Präparationsbasis von Alice und die Messbasis von Bob überein stimmen. (i) Wir nehmen an, dass $\alpha = \gamma$, d. h. dass Eve die korrekte Basis errät. In diesem Fall lernt Eve durch die Messung den korrekten Bitwert, ohne den gesendeten Zustand zu verändern. So ist etwa für den Fall $\alpha = \gamma = x$ und $j = 0$ der gesendete Zustand $|0_x\rangle$. Die x-Messung von Eve liefert das Ergebnis $|0_x\rangle$ mit der Wahrscheinlichkeit 1, und der Zustand nach der Messung ist weiterhin durch $|0_x\rangle$ gegeben. Deshalb wird auch bei Bob eine x-Messung das Ergebnis $|0_x\rangle$ liefern – und es wird bei einer möglichen Kontrolle kein Fehler entdeckt. (ii) Wir nehmen nun an, dass $\alpha \neq \gamma$, d. h. dass Eve die Messung in der falschen Basis durchführt. In diesem Fall liefert die Messung von Eve ein zufälliges Ergebnis – und auch der Zustand des Qubits wird durch die Messung verändert. Dadurch erhält auch Bob ein zufälliges Ergebnis. Betrachten wir dazu wieder den Fall $\alpha = x$, $j = 0$ aber $\gamma = z$. Die z-Messung von Eve liefert das Ergebnis $|0\rangle$ oder $|1\rangle$ jeweils mit der Wahrscheinlichkeit $p_0 = p_1 = 0{,}5$. Der Zustand des Qubits nach der Messung ist ebenfalls durch $|0\rangle$ oder $|1\rangle$ gegeben. Bobs x-Messung an einem solchen Zustand liefert aber ein zufälliges Ergebnis, nämlich $|0_x\rangle$ oder $|1_x\rangle$, jeweils mit der Wahrscheinlichkeit ½. Eve erhält also nur in der Hälfte der Fälle den korrekten Bitwert. Darüber hinaus erhält jetzt auch Bob in der Hälfte der Fälle den falschen Bitwert – der Kontrollschritt wird in diesem Fall also zu einem Fehler führen. Nachdem die Fälle (i) und (ii) jeweils mit der Wahrscheinlichkeit ½ auftreten, können wir schließen, dass Eve den Bitwert mit der Wahrscheinlichkeit ¾ korrekt bestimmen kann – der gesamte Bitstring ist allerdings nur mit einer Wahrscheinlichkeit von $(3/4)^N$ korrekt bekannt. Darüber hinaus erhält Bob mit der Wahrscheinlichkeit $p_{\text{error}} = ¼$ den falschen Bitwert. Diese Situation ist vergleichbar mit der Sequenz von Messungen in Abb. 19. Werden nun M Qubits kontrolliert, so ist die Wahrscheinlichkeit, dass ein Fehler entdeckt wird, durch

$$1-(1-p_{\text{error}})^M = 1-(\tfrac{3}{4})^M \qquad \{47\}$$

gegeben. Für genügend großes M kann man also praktisch mit Sicherheit davon ausgehen, dass Eves Abhörversuch erkannt wird.

Eine weitere mögliche Abhörstrategie ist durch bloßes Raten von Eve gegeben – ohne Durchführung der Messungen. Dadurch wird jedes Bit mit der Wahrscheinlichkeit ½ korrekt erraten – ohne dass eine Störung detektiert wird. Allerdings ist die Wahrscheinlichkeit, den gesamten Bitstring korrekt zu erraten, mit $p = (0{,}5)^N$ exponentiell klein. Eine weitere extremale Strategie ist dadurch gegeben, dass Eve alle gesendeten Qubits abfängt und speichert, und dafür selbst zufällig ausgewählte Zustände an Bob weiterschickt. Eve führt dabei die Messung erst durch, nachdem Alice und Bob ihre Messbasen bekannt gegeben haben. Dadurch erhält Eve die vollständige Information über jedes einzelne Bit und somit über den gesamten Bitstring. Allerdings erhält Bob nun mit der Wahrscheinlichkeit ½ einen falschen Bitwert, und somit wird ein Fehler bei der Kontrolle von M Bits mit der Wahrscheinlichkeit $1 - (0{,}5)^M$ erkannt.

Dies gilt nicht nur für die oben diskutierten Strategien. Man kann vielmehr zeigen, dass für jede mögliche Abhörstrategie (inklusive Strategien, welche gemeinsame Messungen auf allen gesendeten Qubits und auch ein Speichern der Qubits durch Eve beinhalten) ein Informationsgewinn von Eve immer mit einem Fehler des gemessenen Bitwertes bei Bob und mit einer bestimmten Detektionswahrscheinlichkeit verbunden ist. Durch die Kontrolle einer genügend großen Anzahl von Bits kann diese Wahrscheinlichkeit exponentiell verstärkt werden, und es ist möglich, einen Lauscher zuverlässig zu entdecken. Im Gegenzug kann man sicher sein, dass bei keinem bzw. einer sehr geringen Anzahl von Fehlern ein Lauscher keine bzw. nur sehr geringe Information über den gesamten Bitstring haben kann – eine sichere Nachrichtenübermittlung ist deshalb möglich.

Es sollte darauf hingewiesen werden, dass wir hier ein idealisiertes Szenario betrachtet haben. Einerseits wird von perfekten Kanälen zur Quanteninformationsübertragung ausgegangen – in der Realität sind diese allerdings verrauscht, und Fehler durch Rauschen können nicht von Fehlern, die durch Lauschversuche von Eve verursacht werden, unterschieden werden. Es gibt aber Strategien – z. B. klassische „privacy amplification“ –, die es erlauben, die Übertragungssicherheit auch in diesem Fall zu gewährleisten, wenn das Kanalrauschen klein genug ist (ca. 10 %). Andererseits wird in den Sicherheitsbeweisen davon ausgegangen, dass tatsächlich Qubits vorliegen. In vielen experimentellen Realisierungen ist dies bisher jedoch nicht der Fall: Laserdioden erzeugen keine Einzelphotonenzustände, sondern mit gewisser Wahrscheinlichkeit auch Multiphotonenzustände (gemäß einer Poisson-Verteilung) – dies kann für sogenannte „Trojanische-Pferde-Attacken“ genutzt werden. Auch eine derzeitige technische Implementierung der Einzelphotonendetektoren erlauben Abhörstrategien, welche technische Effekte wie z. B. eine gewisse Detektortotzeit nach der Detektion eines Photons ausnützen [14]. Dabei handelt es sich aber um technologische Probleme, die im Prinzip gelöst werden können. Es sei jedenfalls darauf hingewiesen, dass Quantenkryptographiesysteme, die auf dem BB84-Protokoll basieren, bereits seit einiger Zeit kommerziell als PC-Steckkarten erhältlich sind, und auch in einigen Bereichen (z. B. bei Banken) bereits eingesetzt werden [13].

6. Zusammenfassung

In diesem Beitrag haben wir das einfachste quantenmechanische System – das Qubit – genauer behandelt. Dabei haben wir zu verdeutlichen versucht, dass sich anhand des Qubits viele der zentralen

quantenmechanischen Konzepte und Grundprinzipien illustrieren lassen. Es erscheint uns dabei von besonderer Bedeutung, dass keine komplexe mathematische Beschreibung – etwa der quantenmechanischen Wellenfunktion oder der Schrödinger-Gleichung – notwendig ist, sondern die Behandlung von Vektoren für eine quantitative Beschreibung ausreicht bzw. eine qualitative Beschreibung mit Hilfe von einfachen Bildern – basierend auf der Bloch-Kugel – möglich ist. Trotzdem kann das Superpositionsprinzip der Quantenmechanik, aber auch das seltsame Verhalten von Quantensystemen bei Messungen, detailliert untersucht und verstanden werden. Ebenso können die Unterschiede zur klassischen Physik hervorgehoben werden.

Wir haben uns dabei nicht auf die spezielle Realisierung eines Qubits mit Hilfe eines bestimmten physikalischen Systems beschränkt, sondern das Qubit zunächst abstrakt behandelt und erst dann verschiedene mögliche Realisierungen aufgezeigt. Dabei wurden einige Stärken und Schwächen diskutiert, insbesondere im Hinblick auf eine mögliche Behandlung im Unterricht. Die genaue Analyse der Eigenschaften eines Qubits erlaubt dabei nicht nur die Diskussion von fundamentalen Konzepten wie der Heisenberg'schen Unschärferelation, sondern auch von modernen Anwendungen im Bereich der Quanteninformationsverarbeitung, insbesondere der Quantenkryptographie. Wir hoffen, mit diesem Beitrag eine Möglichkeit aufgezeigt zu haben, wie die Grundprinzipien einer der zentralen Theorien der modernen Physik Schülern trotz fehlender Kenntnisse höherer Mathematik nähergebracht werden kann.

7. Danksagung

Wir bedanken uns bei Dipl.-Des. Michael Tewiele für die Realisierung der Bilder.

8. Literatur

[1] R. Müller, H. Wiesner, Teaching Quantum Mechanics on an Introductory Level, American Journal of Physics 70, 200 (2002); Münchener Internetprojekt zur Lehrerfortbildung in Quantenmechanik, http://milq.tu-bs.de/

[2] G. Pospiech, Teaching quantum theory – between the photoelectric effect and quantum information, Proceedings of the GIREP08 conference

[3] W. Dür, Quanteninformation – ein Thema für den Schulunterricht, PdN-PhiS 6/58 (2009)

[4] Quantum Lab, www.quantumlab.de, Universität Erlangen, Didaktik der Physik, AG J.P. Meyn

[5] J. Mompart, K. Eckert, W. Ertmer, G. Birkl, and M. Lewenstein, Phys. Rev. Lett. 90, 147901 (2003), Quantum Computing with Spatially Delocalized Qubits

[6] D. Leibfried *et al.*, Nature 438, 639 (2005); T. Monz *et al.*, Phys. Rev. Lett. 106, 130506 (2011)

[7] S. Gröblacher *et al*,, Nature Phys. 5, 485 (2009), D. *O'Conn*ell *et al*., Nature 464, 697 (2010); F. De Martini, F. *Scia*rrino and C. Vitelli, Phys. Rev. Lett. 100, *253*601 (2008); J. M. Raimond, M. Brune, and S. Haroche, Rev. Mod. Phys. 73, 565 (2001)

[8] Klaus Hornberger, Stefan Gerlich, Philipp Haslinger, Stefan Nimmrichter, Markus Arndt, Colloquium: Quantum interference of clusters and molecules, Rev. Mod. Phys 84, 157 (2012)

[9] H. Häffner, C.F. Roos and R. Blatt, Quantum computing with trapped ions, Physics Reports 469, 155 (2008)

[10] DVD-ROM „Quantendimensionen – Doppelspalt, Verschränkung, Quantencomputer", Klett Verlag & Sciencemotion (2010)

[11] W.K. Wootters and W.H. Zurek, A Single Quantum Cannot be Cloned, Nature 299, 802-803 (1982)

[12] J. M. Taylor, H.-A. Engel, W. Dür , A. Yacoby, C. M. Marcus, P. Zoller and M. D. Lukin, Nature Physics 1, 177 (2005)
"Fault-tolerant architecture for quantum computation using electrically controlled semiconductor spins"

[13] siehe z. B. www.idquantique.com bzw. www.magiqtech.com

[14] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nat. Photonics 4, 686 (2010); Valerio Scarani, Christian Kurtsiefer , The black paper of quantum cryptography: real implementation problems, arXiv:0906.4547

[15] N. Gisin & R. Thew, Quantum communication, Nature Photon, 1, 165-171 (2007); N. Gisin, G. Ribordy, W. Tittel & H. Zbinden, Quantum cryptography, Rev. Mod. Phys. 74, 145 (2002).