merkwürdige Quantenzustand, die Superposition, *zerstört*. Mit einer gewissen Wahrscheinlichkeit, die von α und β abhängt, nimmt das Teilchen eine der beiden Richtungen an; diese ist unser Messergebnis.

Messen stellt eine Wechselwirkung mit der Außenwelt dar: Der Zustand von Schrödingers Katze ist nur so lange unbestimmt, wie sie in der Kiste von der Außenwelt abgeschottet ist. Wollen wir Schrödingers Katze anschauen, muss Licht in die Kiste dringen. Die *splendid isolation* ist beendet, die Wechselwirkung mit den Lichtteilchen kann die Superposition zerstören. Einer der Zustände *tot* oder *lebendig* wird realisiert. Wir selbst gehören stets zur Außenwelt eines Quantenteilchens. Versuchen wir etwas darüber herauszufinden, beeinflussen wir es. In diesem Sinne ist die Kiste ein entscheidender Teil des Gedankenexperiments.

Auf diesen Überlegungen baut die Hauptdefinition des nächsten Abschnittes auf. Ein Quantenbit kann gleichzeitig den Wert 0 und den Wert 1 annehmen. Wollen wir etwas über dieses Bit erfahren, bleibt uns nichts anderes übrig, als es zu *messen*. Die Eigenschaft, gleichzeitig in zwei Zuständen zu sein, geht verloren. Wir erhalten den Wert 0 mit einer Wahrscheinlichkeit p und den Wert 1 mit der Wahrscheinlichkeit $1-p$.

2.2 Das Quantenbit

Ein klassisches Bit ist entweder 0 oder 1. Ein Quantenbit kann beides zugleich sein. Wie das zu verstehen ist, wird in diesem Abschnitt erläutert.

Dirac-Notation

In der Quantenmechanik ist es üblich, Zustände in Klammern der Form $|\cdot\rangle$ zu setzen. Die Werte eines klassischen Bits werden damit zu $|0\rangle$ und $|1\rangle$. Es ist dies die *ket-Notation* oder auch *Dirac-Notation*, die auf den britischen Physiker Paul Dirac (1902-1984) zurückgeht, der 1933 zusammen mit Schrödinger den Nobelpreis erhielt.

Definition Quantenbit

Ein *Quantenbit*, kurz *Qubit*, nimmt Zustände der folgenden Form an:

$$\alpha \cdot |0\rangle + \beta \cdot |1\rangle. \tag{2.1}$$

α und β heißen *Amplituden* und sind komplexe Zahlen mit

$$|\alpha|^2 + |\beta|^2 = 1.$$

Superposition, Überlagerung

Ein Quantenbit kann sich also in zwei klassischen Zuständen gleichzeitig befinden; die komplexen Zahlen drücken deren jeweiligen Anteil aus. Man spricht von *Superposition* oder *Überlagerung* der klassischen Zustände $|0\rangle$ und $|1\rangle$. Die Bedingung $|\alpha|^2 + |\beta|^2 = 1$ schränkt die möglichen Werte der Amplituden ein, zulässige Beispiele sind $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ und $0 \cdot |0\rangle + 1 \cdot |1\rangle = |1\rangle$. Trotz dieser Einschränkung sind unendlich viele verschiedene Zustände möglich.

Ein klassisches Bit kann man lesen und seinen genauen Zustand feststellen. Das ist bei einem Quantenbit in dieser Form nicht möglich: Möchte man auf ein Quantenbit lesend zugreifen, muss man es *messen*. Das Messergebnis hängt von den Amplituden α und β ab.

Messen eines Quantenbits

Messen wir ein Quantenbit im Zustand $\alpha \cdot |0\rangle + \beta \cdot |1\rangle$, wird die Superposition zerstört. Anschließend ist es mit Wahrscheinlichkeit $|\alpha|^2$ im Zustand $|0\rangle$ und mit Wahrscheinlichkeit $|\beta|^2$ im Zustand $|1\rangle$. Diesen Zustand nach dem Messen können wir beobachten.

Beispiel 2.1: Die Superposition $\frac{1}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle$ ist ein zulässiger Zustand eines Quantenbits. Denn es gilt

$$(\frac{1}{\sqrt{3}})^2 + (\sqrt{\frac{2}{3}})^2 = \frac{1}{3} + \frac{2}{3} = 1.$$

Messen wir ein Bit in diesem Zustand, ist das Ergebnis mit Wahrscheinlichkeit $1/3$ der Zustand $|0\rangle$ und mit Wahrscheinlichkeit $2/3$ $|1\rangle$.

Messen wir ein Bit im Zustand $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, sind die Ergebnisse $|0\rangle$ und $|1\rangle$ gleichwahrscheinlich. ◇

Dazu eine Erläuterung: Werfen wir einen sechsseitigen Würfel, ist das Ergebnis eine der Zahlen $1, 2, \ldots, 6$. Sehen wir von Unregelmäßigkeiten des Würfels ab, erhalten wir jede Zahl mit Wahrscheinlichkeit $1/6$; werfen wir den Würfel sehr oft, erwarten wir, dass wir zum Beispiel die 1 in einem Sechstel der Fälle beobachten. Aber was ist Wahrscheinlichkeit? Man kann wie folgt argumentieren: hätten wir exakte Informationen über den Würfelwurf und die Beschaffenheit der Oberfläche, auf der er auftritt, könnten wir den genauen Bewegungsablauf berechnen, wie wir die Bewegung der Planeten berechnen können. Uns fehlen nur diese exakten Informationen!

Das ist in der Quantenwelt nicht so. Messen wir ein Bit im Zustand $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, ist der Ausgang tatsächlich unbestimmt und keine Folge unserer Unwissenheit oder der Grobheit der Messinstrumente. Gibt es auch Quantenzustände, bei denen das Ergebnis feststeht? Messen wir $0 \cdot |0\rangle + 1 \cdot |1\rangle = |1\rangle$, so erhalten wir mit Sicherheit den Wert $|1\rangle$ als Ergebnis. Dieser Zustand verhält sich wie ein klassisches Bit, das 1 gesetzt ist. Wir bezeichnen $|0\rangle$ und $|1\rangle$ als *nicht-überlagerte Zustände*, da sie den Zuständen eines klassischen Bits entsprechen.

Aufgabe 2.3: 100 Quantenbits befinden sich im Zustand $\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$. Sie messen alle. Welches Ergebnis erwarten Sie?

Phase

Das Ergebnis der Messung hängt nur von dem Betrag der Amplitude ab. Messungen der Zustände $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ und $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ ergeben jeweils $|0\rangle$ und $|1\rangle$ mit Wahrscheinlichkeit $1/2$. Zwei reelle Zahlen haben denselben Betrag, wenn sie sich nur im Vorzeichen unterscheiden. Komplexe Zahlen z haben denselben Betrag, wenn sie sich nur bezüglich der Phase unterscheiden, siehe Seite 295.

Zustände als Vektoren

Was nun folgt ist wesentlich, um die Arbeitsweise des Quantencomputers zu verstehen. Den Zustand eines Quantenbits werden wir ab jetzt als Vektor in einem zweidimensionalen Vektorraum über den komplexen Zahlen betrachten; Vektorräume sind immer dann nützlich, wenn eine Beschreibung von mehreren unabhängigen Komponenten abhängt. Auf die folgenden Überlegungen geht auch Abschnitt A.2 im Anhang über Vektorräume ein.

In unserem Fall sind die Komponenten die Amplituden, und die Superposition $\alpha|0\rangle + \beta|1\rangle$ wird zu dem Vektor aus Abbildung 2.11. Der zugehörige *Zustandsvektor* ist

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

Diesen Vektor können wir als Linearkombination der zweidimensionalen Standardbasisvektoren angeben:

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

Die Basis unseres Vektorraumes besteht damit aus den beiden nicht überlagerten Zuständen $\{|0\rangle, |1\rangle\}$. Die Superposition $\alpha|0\rangle + \beta|1\rangle$ wird zu einer *Linearkombination* dieser Basiselemente. Natürlich sind nicht alle Vektoren unseres zweidimensionalen Vektorraums mögliche Zustände eines Quantenbits. Wegen der Bedingung $|\alpha|^2 + |\beta|^2 = 1$ sind es gerade diejenigen der Länge 1.

Aus Abbildung 2.11 kann man nicht ersehen, dass α und β komplexe Zahlen sind. Wir stellen uns den Vektorraum einfach so vor, als wäre er über den reellen Zahlen definiert, und rechnen gemäß den Regeln für komplexe Zahlen.

Realisierung

Wie kann man ein Quantenbit bauen, um damit konkret zu rechnen? Dazu muss ein Teilchen von seiner Umwelt strikt abgeschottet werden. Wir erinnern uns an die Kiste, in der Schrödingers Katze steckte. Ohne diese Abschottung würde die Umwelt mit dem Teilchen wechselwirken, und die Superposition würde zerstört werden; ähnlich wie durch eine Messung. Das Stichwort hierzu lautet *Dekohärenz*, siehe Abschnitt 9.1.

Nun nimmt man eine messbare und beeinflussbare Eigenschaft des abgeschotteten Teilchens her, zum Beispiel die Drehrichtung um eine festgelegte Achse oder zwei Energieniveaus. Wir wählen zwei Zustände dieser Eigenschaft, die sich in der klassischen Welt ausschließen: diese bezeichnen wir mit $|0\rangle$ und $|1\rangle$. Fertig. Dieser Zugang ist aus praktischer Sicht unverantwortlich hemdsärmelig. Wir sollten uns jedoch auf genau diesen Standpunkt stellen.

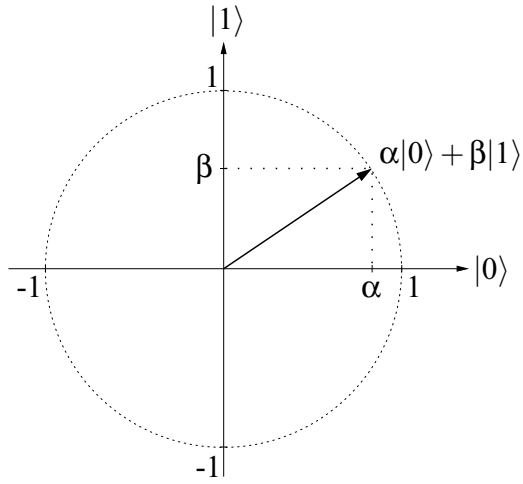

Abbildung 2.11: Die Superposition als Vektor

Quantenbits sind realisierbar; das haben Experimentalphysiker bewiesen. Wir stellen uns im weiteren die Frage, was sich damit anfangen lässt.

Unsere aktuelle Frage lautet: Wie können wir mit Quantenbits rechnen? Oder anders ausgedrückt, was für Rechenschritte können wir ausführen, wie gehen zwei Zustände eines Quantenbits ineinander über?

2.3 Rechenschritte auf einem Quantenbit

Wir wissen bereits, was ein Quantenbit ist, aber noch nicht, was man damit machen kann. In Abschnitt 2.1 haben wir festgestellt, dass eine Berechnung eine Folge von Zuständen des Rechners ist. Ein Rechenschritt überführt dabei den aktuellen Zustand in den Folgezustand. Bei klassischen Rechnern gibt es keine weiteren Einschränkungen. Hat das Bit etwa den Wert 0, kann es im nächsten Rechenschritt 1 gesetzt werden oder den Wert 0 behalten. Ein Quantenbit hingegen kann unendlich viele verschiedene Zustände annehmen. Der Übergang zwischen den Zuständen unterliegt dabei besonderen Bedingungen.

Die möglichen Rechenschritte auf einem Quantenbit werden durch quadratische Matrizen beschrieben, genauer durch 2×2-Matrizen, die *unitär* sind. Unitäre Matrizen beschreiben mathematisch, wie sich ein abgeschottetes Quantensystem ändert. Matrizen beschreiben Abbildungen, siehe dazu den Anhang. Aus einer unitären Matrix lässt sich besonders einfach die inverse Matrix beziehungsweise die Umkehrabbildung ableiten.

Dazu benötigen wir folgenden Begriff: Hat eine Matrix $A = (a_{ij})$ komplexe Einträge, kommen wir zu A^*, der *komplex konjugierten* von A, indem wir a_{ij} durch a_{ij}^* ersetzen (zu komplexen Zahlen siehe Abschnitt A.1 und zu Matrizen und der verwendeten Notation Abschnitt A.3 im Anhang). Mit $A^\dagger$ bezeichnen wir die komplex konjugierte und transponierte Matrix $(A^*)^T$. $A^\dagger$ heißt zu A *adjungierte* Matrix und entsteht aus A, indem a_{ij} durch a_{ji}^* ersetzt wird. Leider gibt es keine einheitliche Notation: in der deutschsprachigen Literatur wird die komplex konjugierte Matrix meistens mit $\overline{A}$ bezeichnet und die adjungierte mit A^*. Unsere Schreibweise hat den Vorteil, den Einstieg in die Originalliteratur zu erleichtern.

Definition unitäre Matrix

Sei A eine $n \times n$-Matrix, deren Einträge komplexe Zahlen sind.
A heißt *unitär*, falls $A^\dagger$ zu A invers ist:

$$A^\dagger = A^{-1}.$$

Eine unitäre Matrix beschreibt eine unitäre Transformation.

Eine Matrix A mit rellen Einträgen ist genau dann unitär, wenn wir durch Transposition zur Inversen gelangen: $A^{-1} = A^T$. Die beiden folgenden Matrizen sind unitär:

Beispiel 2.2: Die zweidimensionale Einheitsmatrix

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

ist unitär. Denn es gilt $I_2^\dagger = I_2 = I_2^{-1}$.

Hadamard-Matrix

Die Matrix

$$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

ist unitär. Sie heißt Hadamard-Matrix und wird eine wichtige Rolle für uns spielen.

Benannt ist die Matrix H nach dem französischen Mathematiker Jacques Hadamard (1865-1963).

Aufgabe 2.4: Beweisen Sie, dass die Matrix H unitär ist.

Entwicklung eines Qubits

Nun beschreiben wir, wie eine solche Matrix eine Zustandsveränderung eines Quantenbits bewirkt. Auf einem Quantenbit im Zustand $\alpha|0\rangle + \beta|1\rangle$ soll ein

Rechenschritt ausgeführt werden, der durch eine zweidimensionale (unitäre) Matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

beschrieben wird. Wir erhalten den Folgezustand $\alpha'|0\rangle + \beta'|1\rangle$, indem wir den Zustandsvektor mit der Matrix multiplizieren.

$$\begin{pmatrix} \alpha' \\ \beta' \end{pmatrix} = A \cdot \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} a \cdot \alpha + b \cdot \beta \\ c \cdot \alpha + d \cdot \beta \end{pmatrix}.$$

Man nennt die zu einer unitären Matrix gehörende Abbildung zwischen Vektoren eine *unitäre Transformation*. In der Folge unterscheiden wir jedoch nicht allzu streng zwischen diesen Begriffen.

Beispiel 2.3: Wir wenden die Matrix H aus Beispiel 2.2 auf die Basiszustände an:

$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.
$|1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Wenden wir H nun noch einmal an, ergibt sich:

$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \xrightarrow{H} |0\rangle$ und
$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \xrightarrow{H} |1\rangle$.

H ist zu sich selbst invers: $H^{-1} = H$ oder $HH = I$. Da sogar $H^\dagger = H$ gilt, folgt daraus, dass H unitär ist, siehe Aufgabe 2.4.

Aufgabe 2.5: Konstruieren Sie alle unitären Transformationen eines Bits, die den Zustand $|0\rangle$ auf $\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$ abbilden.

Realisierung

Seit Ende des letzten Abschnitts stellen wir uns ein Quantenbit als von seiner Umwelt abgeschottetes Teilchen vor. Der Zustand gewisser Teilchenarten lässt sich mit Hilfe von Laserstrahlen oder Magnetfeldern ändern. Mit diesen oder ähnlichen Verfahren könnte man beispielsweise eine Superposition zweier Energieniveaus in eine andere Superposition übergehen lassen und so eine *unitäre Transformation* auf dem Quantenbit realisieren. Eine wichtige Möglichkeit, Quantenbits zu konstruieren, stellen polarisierte Photonen oder Lichtquanten dar. Der Zustand so konstruierter Quantenbits lässt sich mit optischen Geräten wie lichtbrechenden Kristallen manipulieren – mehr dazu findet sich in Kapitel 10.2.

Zusammenfassung

Der Zustand eines Quantenbits wird durch einen Vektor der Länge 1 in einem zweidimensionalen komplexen Vektorraum beschrieben. Wir führen einen Rechenschritt aus, ändern den Zustand des Quantenbits, indem wir eine

unitäre Transformation anwenden beziehungsweise den Zustandsvektor mit einer unitären Matrix multiplizieren. Messen wir ein Quantenbit im Zustand $\alpha|0\rangle + \beta|1\rangle$, beobachten wir $|0\rangle$ mit Wahrscheinlichkeit $|\alpha|^2$ und $|1\rangle$ mit Wahrscheinlichkeit $1 - |\alpha|^2 = |\beta|^2$. Nach der Messung ist die vorhergehende Superposition zerstört. Insbesondere kann man nie feststellen, welchen Wert die Amplituden α und β haben.

2.4 Der erste Algorithmus: Ein Zufallsgenerator

Bisher stehen uns nur sehr bescheidene Mittel zur Verfügung. Wir können ein Quantenbit manipulieren und messen. Dies genügt jedoch, um einen Quantenalgorithmus für ein Problem zu beschreiben, das für einen klassischen Rechner unmöglich ist: das Erzeugen von Zufallszahlen. Zufallszahlen sind für viele Anwendungen nötig, wovon zwei in diesem Buch behandelt werden. In Abschnitt 4.2 geht es um randomisierte Algorithmen, ein sehr mächtiges Werkzeug. Eine Anwendung aus der Kryptographie lernen wir in Abschnitt 7.1 kennen. Weiter spielen Zufallszahlen für die Vorhersage von Börsenkursen oder anderen wirtschaftlichen Indizes eine große Rolle. Auch für Simulationen, etwa der Klimaentwicklung oder anderer Naturprozesse, werden Zufallszahlen benötigt. Solche Prozesse sind so komplex, dass sie nicht absolut korrekt berechnet werden können. Man kann die Prozesse aber annähern, sie approximieren; dabei kommt der Zufall ins Spiel.

Klassische Computer erzeugen für jede Eingabe eine exakt festgelegte Ausgabe. Mehr noch, jeder Rechenschritt ist durch den aktuellen Zustand determiniert, wie wir an den Berechnungsmodellen in Abschnitt 2.1 gesehen haben. Das Beste, was solche Rechner herstellen können, sind sogenannte *Pseudozufallszahlen*. Das sind Folgen von Zahlen, die mit Mitteln der Statistik nicht von tatsächlichen Zufallszahlen zu unterscheiden sind. Aber der Statistik sind bei solchen Fragen Grenzen gesetzt. Es sind keine echten Zufallszahlen und für Anwendungen äußerst problematisch.

Der folgende Algorithmus erzeugt ein zufälliges Bit. Da die möglichen Ergebnisse beide mit derselben Wahrscheinlichkeit erzeugt werden, verhält er sich wie ein Münzwurf. Die Notation wird in der anschließenden Analyse erklärt.

Algorithmus Münzwurf

Spezifikation: Wir verwenden ein Quantenbit $|x\rangle$. Nach Ablauf des Algorithmus ist es mit Wahrscheinlichkeit $1/2$ auf $|0\rangle$ gesetzt und mit Wahrscheinlichkeit $1/2$ auf $|1\rangle$.

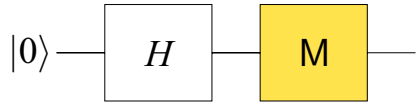

Abbildung 2.12: Schaltkreis für den Algorithmus Münzwurf

1. $|x\rangle \leftarrow |0\rangle$
2. $|x\rangle \leftarrow H\,|x\rangle$
3. Miss $|x\rangle$

Die verwendete Notation wird durch die Analyse erklärt.

Analyse:

In Schritt 1 wird das Quantenbit $|x\rangle$ in den Anfangszustand $|0\rangle$ versetzt. In Schritt 2 wird die Hadamard-Transformation auf dieses Bit angewendet, danach ist es also im Zustand $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Messen wir es, so erhalten wir das in der Spezifikation beschriebene Ergebnis.

Aufgabe 2.6: Was ist das Ergebnis des Algorithmus, wenn wir im ersten Schritt das Bit $|x\rangle$ auf $|1\rangle$ setzen?

Aufgabe 2.7: Was ist das Ergebnis des Algorithmus, wenn wir $|x\rangle$ im ersten Schritt in einen beliebigen Ausgangszustand $\alpha|0\rangle + \beta|1\rangle, |\alpha|^2 + |\beta|^2 = 1$, versetzen?

Alle unsere Algorithmen werden von ungefähr dieser Form sein. Man versetzt zunächst einige Quantenbits in einen Ausgangszustand. Dann wendet man eine Reihe von unitären Transformationen an und misst am Ende. Wie angekündigt, ist das grundlegende Berechnungsmodell dieses Buches der Quantenschaltkreis. Ein Gatter eines solchen Schaltkreises führt eine unitäre Transformation aus. Im Abschnitt 3.3 werden wir Quantenschaltkreise näher untersuchen. Der Begriff ist aber so anschaulich, dass wir in Abbildung 2.12 den Schaltkreis angeben, der unserem Algorithmus für den Münzwurf entspricht.

Realisierung

Wir haben bereits eine gewisse Vorstellung davon, was eine Quantenberechnung ist. Folgendermaßen ließe sich der Zufallsgenerator realisieren: man isoliert ein Teilchen, überführt dieses bezüglich seiner Drehrichtung in die Superposition $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ und misst anschließend die Drehrichtung. Das ist alles. Zufälligkeit ist schließlich eines der Charakteristika der Quantenmechanik. Quantenzufallsgeneratoren werden seit längerem produziert und eingesetzt, siehe dazu auch Abschnitt 10.2.2.