Chapter 3

Register und Gatter

Das Herz des klassischen Computers (die ALU) besteht aus einer Reihe geeignet miteinander verschalteter logischer Gatter. Von einem abstrakt logischen Standpunkt aus geseheh, heißt Rechen die Manipulation von Bits, die in den Registern der ALU bzw. des Hauptspeichers zur Vefügung gehalten werden. Dieses Konstruktionsprinzip wiederholt sich auch bei der Realisierung eines QC mit zwei wesentlichen Variationen – einerseits haben die Bits eine allgemeinere Bedeutung und andererseits erfolgt ihre Verarbeitung auf reversible Weise. Wir wenden uns zunächst der Frage des reversiblen Computings zu, die auch schon auf klassische Weise realisiert werden kann. Danach stellen wir die quantenmechanische Verallgemeinerung des Bits (Quantenbit) und die Quantengatter dar.

3.1 Vektorielle Zustandsbeschreibung klassischer Register

3.1.1 Zustandsbeschreibung

Klasssich ist das Bit auf der abstrakten Ebene durch eine zweielementige Menge repräsentiert, beispielweise $\mathbf{B} = \{0, 1\}$ oder $\mathbf{B} = \{true, false\}$ und Worte aus n Bits durch das n–fache kartesiche Produkt $\mathbf{B}^n = \mathbf{B} \times \mathbf{B} \times \ldots \times \mathbf{B}$. Rechnen ist durch logische Operationen auf diesen Mengen realisiert. Das kann vollständig unabhängig von der hardware betrachtet werden. Für den QC steht mehr die physikalische Realisierung der Bits im Mittelpunkt. Wir betrachten zunächst den physikalischen Zustand des Speicherelements für ein einzelnes Bit. Klassisch ist dieser durch einen skalaren Wert (z.B. die Spannung oder Magentisierung des Speicherelements) gegeben und im definierten Speicherzustand kann dieser auf die Werte 0 und 1 abgebildet werden. Damit gibt es eine direkte Übersetzung der abstrakt–logischen in die physikalischen Zustände unseres Rechensystems.

Der Zustand eines quantenmechanischen Speicherelementes (Spin eines Elektrons) kann nicht mehr durch einen einzelnen Wert repräsentiert werden. Geeignet ist stattdessen ein zweikomponentiger Vektor. Es steht uns frei, auch schon im klassischen mit dieser Zustandsdarstellung zu arbeiten, d.h. wir betrachten jetzt statt $\mathbf{B} = \{0, 1\}$die Menge der Zustände die das Speicherelement einnehmen kann. Symbolisch führen wir (in Anlehnung an die Dirac–Schreibweise)

$$|Name\rangle$$

als Bezeichner für Zustände ein, wobei $Name$ ein geeignet gewählter Name ist. Wählen wir $Name = Bitwert$, dann ist die Menge der Zustände eines Bits

$$\mathbf{B} = \{|0\rangle, |1\rangle\}$$

Diese Zustände werden durch Vektoren repräsentiert (wir verwenden das Gleichheitszeichen, obwohl links ein abstrakter Zustand und rechts ein Vektor steht)

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

so dass wir auch

$$\mathbf{B} = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\} \tag{3.1}$$

schreiben können. Die Wörter aus 2 Bits sind durch die Elemente des kartesischen Mengenproduktes

$$\mathbf{B} \times \mathbf{B} = \{00, 01, 10, 11\}$$

gegeben. In der Darstellung (3.1) heißt das

$$\begin{aligned} \mathbf{B} \times \mathbf{B} &= \{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\} \\ &= \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \dots \right\} \end{aligned}$$

wobei $\otimes$ das direkte Produkt zwischen zwei Vektoren bezeichnet. Für zwei beliebige (2– d) Vektoren $\vec{a}, \vec{b}$ gilt

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 \vec{b} \\ a_2 \vec{b} \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ a_2 b_1 \\ a_2 b_2 \end{pmatrix}$$

Folglich:

$$\mathbf{B} \times \mathbf{B} = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\} \tag{3.2}$$

Abgekürzt schreiben wir

$$|q_1\rangle \otimes |q_2\rangle = |q_1 q_2\rangle$$

und schließlich in einer kompakten Schreibweise (Name des Zustandes gleich Zahlenwert des Registerinhaltes)

$$\mathbf{B} \times \mathbf{B} = \{|0\rangle_2, |1\rangle_2, |2\rangle_2, |3\rangle_2\}$$

wobei der Index die Zahl der Bits im Register angibt. Das ist erforderlich, um Verwechslungen z.B. zwischen dem 1 Bit Zustand $|0\rangle$ und dem Zwei-Bit Zustand $|0\rangle_2 = |00\rangle$ zu unterscheiden. Meist werden wir den Index aber weglassen, weil die Zahl der Bits des Registers klar ist. Die konkrete Darstellung durch Vektoren ist

$$\begin{aligned} |0\rangle_2 &= \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |1\rangle_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \\ |2\rangle_2 &= \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |3\rangle_2 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \end{aligned} \tag{3.3}$$

Die Verallgemeinerung der obigen Relationen auf n Bits ist

$$|q_1\rangle \otimes |q_2\rangle \ldots \otimes |q_n\rangle = |q_1 q_2 \ldots q_n\rangle$$

3.2 Klassische logische Gatter

3.2.1 Vorbetrachtung: Reversible und irreversible logische Gatter

Logische Gatter sind Realisierungen Boolscher Funktionen. Ein sehr einfaches Gatter ist durch die NOT–Funktion gegeben.

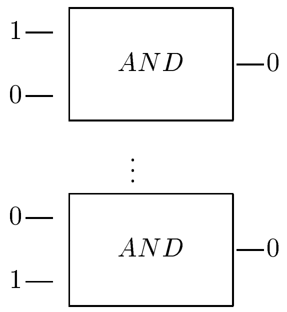
$$0 - \boxed{NOT} - 1 \tag{3.4}$$

$$1 - \boxed{NOT} - 0$$

Das ist ein reversibles Gatter, denn die Hintereinanderschatung von zwei Gattern ist die Identität

$$s - \boxed{NOT} - \boxed{NOT} - s, \qquad s \in \{0, 1\} \tag{3.5}$$

Die Berechnung (Ausführung der NOT–Funktion) ist umkehrbar, weil am Output sozusagen noch die volle Information zur Verfügung steht. Hingegen enspricht die AND Funktion einem irreversiblen Gatter, betr. z. B.



(3.6)

Offensichtlich kann aus dem Wert des Bits am Ausgang nicht auf die Bits am Eingang rückgeschlossen werden.

3.2.2 Unäre Operatoren

Wir habe oben eine neue Zustandsbeschreibung der Speicherelemente für die Bits eingeführt. Diese hat den Vorteil, dass sie auf die Quantenzustände erweiterbar ist. In dieser Darstellung werden Operationen auf den Zuständen durch Matrizen bewirkt, z. B. das logische NOT mit der Funktionalität ("Umschalten" eines Bits)

$$NOT\,|0\rangle = |1\rangle\,, \quad NOT\,|1\rangle = |0\rangle$$

was durch

$$NOT\;|x\rangle = |(x+1) \bmod 2\rangle$$

kompakter geschrieben werden kann, ist durch die Matrix

$$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

gegeben, weil ja

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

Diese Operation ist reversibel, weil $NOT\,NOT = \mathbf{1}$ mit $\mathbf{1}$ der Einheitsmatrix. Irreversibel ist hingegen die Operation $\mathcal{N}$, die ein Bit abschaltet

$$\mathcal{N}\,|0\rangle = \mathcal{N}\,|1\rangle = |0\rangle$$

was durch die Matrix

$$\mathcal{N} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

realisiert wird, denn wie man unmittelbar einsieht, ist

$$\mathcal{N}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \mathcal{N}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

3.2.3 Operationen auf zwei Bits

Operationen auf den Bits eines 2–Bit Registers sind durch 4×4 Matrizen dargestellt. Operationen, die Kombinationen aus 1– Bit Operationen sind, sind durch das direkte Produkt der 1–Bit Matrizen gegeben. Das direkte Produkt zwischen zwei beliebigen Matrizen A und B ist

$$\begin{aligned} A \otimes B &= \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \otimes \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} \\ &= \begin{pmatrix} A_{11}B & A_{12}B \\ A_{21}B & A_{22}B \end{pmatrix} \end{aligned}$$

und damit

$$A \otimes B = \begin{pmatrix} A_{11}B_{11} & A_{11}B_{12} & A_{12}B_{11} & A_{12}B_{12} \\ A_{11}B_{21} & A_{11}B_{22} & A_{12}B_{21} & A_{12}B_{22} \\ A_{21}B_{11} & A_{21}B_{12} & A_{22}B_{11} & A_{22}B_{12} \\ A_{21}B_{21} & A_{21}B_{22} & A_{22}B_{21} & A_{22}B_{22} \end{pmatrix}$$

Als Beispiel betrachten wir die Anwendung von NOT auf das zweite Bit (das erste bleibe unbeeinflußt)

$$NOT\,(2)\,|q_1 q_2\rangle = |q_1 q_2'\rangle$$

mit $q_2' = NOT\,q_2$ in der logischen Notation. In der Matrixdarstellung ist $NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ und

$$\begin{aligned} NOT\,(2) &= E \otimes NOT = \begin{pmatrix} 1\,NOT & 0\,NOT \\ 0\,NOT & 1\,NOT \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{aligned}$$

wobei E die 2×2 Einheitsmatrix ist.

In der Praxis ist es meist günstiger, in der kompakten Dirac Notation zu arbeiten. Rechnet man immer mod 2, dann gilt z. B.

$$NOT\, q = q + 1, \quad q \in \{0, 1\}$$

und etwa

$$NOT\,(2)\, |q_1\rangle \otimes |q_2\rangle = |q_1\rangle \otimes |q_2 + 1\rangle$$

3.2.4 Operationen auf Multibit–Registern

Es gilt in der Verallgemeinerung der obigen Relationen

$$|q_1\rangle \otimes |q_2\rangle \ldots \otimes |q_n\rangle = |q_1, q_2, \ldots q_n\rangle$$

wobei die Operationen sich meist aus der Kombination von 1 und 2–Bit Operationen zusammensetzen. Beispielsweise ist

$$NOT\,(k) = E \otimes E \otimes \ldots \otimes NOT \otimes \ldots \otimes E$$

oder auch

$$NOT\,(k)\, |q_1\rangle \otimes \ldots \otimes |q_k\rangle \otimes \ldots \otimes |q_n\rangle = |q_1\rangle \otimes \ldots \otimes |q_k + 1\rangle \otimes \ldots \otimes |q_n\rangle$$

3.3 Spezielle reversible Gatter

Von Benett[**?**] u. a. wurde schon in den siebziger Jahren gezeigt, dass jeder Rechenprozeß auch reversibel ausgeführt werden kann. Des weiteren konnte gezeigt werden, dass sich alle Rechnungen auf eine Sequenz von reversiblen Ein– und Zwei–Bit Operationen zurückführen lassen. Grundvoraussetzung des reversiblen Rechnens ist, dass kein Bit Information verloren gehen darf, d.h. am Ausgang eines jeden Gatters liegen genau so viele Bits an, wie am Eingang. Bei Operationen $\mathbf{B}^n \to \mathbf{B}^m$ mit $m < n$ wird das Ergebnis in m beliebig aber fest ausgewählten Bits zur Verfügung gestellt. Beispielsweise betrachten wir das logische XOR (*exclusive or*), also die Boolesch Funktion $f: \quad \mathbf{B}^2 \to \mathbf{B}$ mit

$$f\,(q_1, q_2) = (q_1 + q_2) \bmod 2$$

Als reversible Operation auf einem Zwei–Bit Register läßt es sich als

$$XOR\, |q_1\rangle \otimes |q_2\rangle = |q_1\rangle \otimes |q_1 + q_2\rangle\,, \qquad q_i \in \{0, 1\} \tag{3.7}$$

implementieren, wobei das Ergebnis im zweiten Bit erscheint. In der Dastellung des Registerzustandes durch die Vektoren gemäß (3.3) gilt

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

so dass

$$XOR\begin{pmatrix}1\\0\\0\\0\end{pmatrix}=\begin{pmatrix}1\\0\\0\\0\end{pmatrix},\ldots,\quad XOR\begin{pmatrix}0\\0\\0\\1\end{pmatrix}=\begin{pmatrix}0\\0\\1\\0\end{pmatrix} \tag{3.8}$$

wie es sein muss.

3.3.1 Das Toffoli-Landauer Gatter

Wie gezeigt werden konnte, können alle Rechenoperationen in reversibler Weise durch die Kombination von TL-Gattern und dem XOR ausgeführt werden. Das TL-Gatter realisiert eine Boolesche Funktion $f: \quad \mathbf{B}^3 \to \mathbf{B}$ wobei

$$f(q_1, q_2, q_3) = (q_3 + q_1 q_2) \mod 2, \qquad q_i \in \{0, 1\}$$

Als Operation auf einem Drei–Bit Gatter heißt sie $CCNOT$ oder ${}^{CC}NOT$ mit (wir rechnen mod 2)

$${}^{CC}NOT\,|q_1\rangle \otimes |q_2\rangle \otimes |q_3\rangle = |q_1\rangle \otimes |q_2\rangle \otimes |q_3 + q_1 q_2\rangle$$

Das bedeutet, dass die ersten zwei Bits immer unverändert bleiben und im dritten Bit die NOT Operation ausgeführt wird, falls die beiden ersten Bits gesetzt sind ($q_1 = q_2 = 1$), sonst bleibt dessen Wert ebenfalls erhalten. Die Operation auf dem dritten Bit wird also durch die ersten beiden Bits kontrolliert, daher der Name *controlled controlled NOT*.

3.3.2 Das Fredkin Gatter

Das Fredkin Gatter führt ebenfalls ein Operation auf drei Bits aus. Sei U_{Fred} die unitäre Matrix des Gatters, dann ist

$$U_{Fred}\,|q_1\rangle \otimes |q_2\rangle \otimes |q_3\rangle = \begin{cases} |q_1\rangle \otimes |q_2\rangle \otimes |q_3\rangle & falls \quad q_1 = 1 \\ \\ |q_1\rangle \otimes |q_3\rangle \otimes |q_2\rangle & falls \quad q_1 = 0 \end{cases}$$

wobei $q_i \in \{0, 1\}$. Das erste Bit (von links) wirkt also wie eine Art Kontrollinput, der den Austausch der beiden anderen Bitwerte steuert.

Übung: Gib die 4×4 Matrix U an, die auf einem 2–Bit Register die beiden Bit Werte vertauscht. Zeige die Unitarität.

3.4 Quantenregister

Bisher haben wir uns mit rein klassischen Gattern und Registern befasst, das besondere war nur die gewählte Art der Darstellung der Zustände der Speicherelemente. Wir betrachten nun die quantenmechanische Verallgemeinerung und dabei den speziellen Fall, daß die Bits der Register unseres Computers duch die Zustände der Spins geeigneter Teilchen realisiert sind. Der Spin werde bezüglich einer bestimmten Raumrichtung gemessen, so daß seine Projektion nur zwei Werte annehmen kann, nämlich längs dieser Richtung oder entgegengesetzt zu ihr. Abstrakt stellen wir diese beiden Zustände wie bisher durch

$$|0\rangle \quad \text{und} \quad |1\rangle$$

oder in mehr physikalisch orientierter Schreibweise al

$$|\uparrow\rangle \quad \text{und} \quad |\downarrow\rangle \tag{3.9}$$

dar. Konkret verwenden wir die oben eingeführten Vektoren. Es gilt also

$$|0\rangle = |\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle = |\downarrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{3.10}$$

Wenn wir ein Input– bzw. Outputregister mit K Bits realisieren wollen, so brauchen wir K Spins, die man sich alle nebeneinander angeordnet vorstellen kann, den gemeinsamen Zustand schreibt man als direktes Produkt der Einzelzustände, abstrakt z. B. (wir lassen das Symbol $\otimes$ für das direkte Produkt der Vektoren im folgenden weg)

$$|\downarrow\rangle\,|\downarrow\rangle \dots |\downarrow\rangle = |\downarrow\downarrow \dots \downarrow\rangle\,, \quad |\uparrow\rangle\,|\downarrow\rangle \dots |\downarrow\rangle = |\uparrow\downarrow \dots \downarrow\rangle\,, \quad \dots \tag{3.11}$$

Die Produktzustände können ebenfalls durch Vektoren dargestellt werden, für zwei Spins schreiben wir

$$|\uparrow\rangle\,|\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |\uparrow\rangle\,|\downarrow\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad |\downarrow\rangle\,|\uparrow\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |\downarrow\rangle\,|\downarrow\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix},, \tag{3.12}$$

In einer kompakten Schreibweise interpretieren wir den Spinzustand als die Binärkodierung einer Zahl a und schreiben $|a\rangle$ für den Zustand, z. B.

$$|\uparrow\uparrow \dots \uparrow\rangle = |0\rangle\,, |\uparrow\uparrow \dots \downarrow\rangle = |1\rangle\,, \dots, |\downarrow\downarrow \dots \downarrow\rangle = \left|2^K\right\rangle \tag{3.13}$$

bei K Bits.

Bisher verhalten sich die Spins nicht anders als die klassischen Bits in jedem herkömmlichen Computer. Das liegt daran, daß wir die Zustände der Spins immer erst nach einer Beobachtung (bezüglich der augewähllten Raumrichtung) betrachtet haben. Das besondere an der Quanenmechanik ist aber, daß unbeobachtet auch andere Zustände möglich sind, z. B. (zunächst wieder für einen Spin) die Überlagerung der zwei definierten Spinzustände.

$$\overline{|\cdot\rangle} = \frac{1}{\sqrt{2}}\left(|\downarrow\rangle + |\uparrow\rangle\right) \tag{3.14}$$

Die Schreibweise $\overline{|.\rangle}$ soll andeuten, daß sich der Spin nun nicht mehr in einem definierten Zustand befindet. Im Gegenteil, er befindet sich in einer Überlagerung seiner beiden ihm überhaupt zur Verfügung stehenden Möglichkeiten, eine Situation, die klassisch keine Entsprechung hat. Der Zustand des Spins (3.14) wird allgemein als das **Quantenbit** (im engeren Sinne) bezeichnet. Ganz allgemein ist jeder Vektor des 2–d Hilbertraumes, d.h. jede komplexe Überlagerung der beiden Basiszustände $|\downarrow\rangle$ und $|\uparrow\rangle$ ein möglicher Zustand des Spins (Superpositionsprinzip). Wir schreiben den allgemeinsten Zustand (das Quantenbit im allgemeinen Sinne) abstrakt als

$$|\psi\rangle = \alpha\ |\uparrow\rangle + \beta\ |\downarrow\rangle$$

oder

$$|\psi\rangle = \alpha\ |0\rangle + \beta\ |1\rangle$$

mit (Normierung)

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

und konkret als

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Bei der Messung des Spinzustandes – einer Operation, die dem Auslesen des Registerinhaltes entspricht – wird gleichwahrscheinlich immer genau eine der beiden Möglichkeiten realisiert, d. h. entweder

$$|\psi\rangle \;\text{——}\; \boxed{\text{Auslesen des Registers}} \;\text{——}\; |\downarrow\rangle \tag{3.15}$$

oder

$$|\psi\rangle \;\text{——}\; \boxed{\text{Auslesen des Registers}} \;\text{——}\; |\uparrow\rangle \tag{3.16}$$

Nach der Messung ist der Spin dann in dem durch das Ergebnis der Messung definierten Zustand $|\downarrow\rangle$ oder $|\uparrow\rangle$. Die Wahrscheinlichkeitsamplitude für die einzelnen Ereignisse ist, wie im Kapitel ”Grundlagen” besprochen, durch das Skalarprodukt des Zustandsvektors $|\psi\rangle$ mit dem Ergebnisvektor ($|\downarrow\rangle$ oder $|\uparrow\rangle$) gegeben. Das Skalarprodukt zweier Vektoren $|\psi\rangle$ und $|\phi\rangle$ des 2–d Hilbertraumes ist bekanntlich

$$< \psi|\phi >= \alpha^*\gamma + \beta^*\delta$$

wobei γ und δ die Komponenten des Vektors $|\phi\rangle$ sind.

3.5 Quantengatter

Der Zustand eines Spins und damit auch eines ganzen Registers kann durch physikalische Manipulationen verändert werden. Wir wollen die den Zustand eines Registers ändernden physikalischen Systeme Gatter nennen. In der Darstellung der Zustände durch Vektoren wird dir Funktion der Gatter durch Matrizen bewirkt. Grundlegend für die Funktion des QC ist, dass diese Matrizen unitär sind. Ist U eine solche Matrix und U^+ ihre Hermitesch konjugierte, dann ist U genau dann unitär wenn $U^+ = U^{-1}$ gilt, in Komponentenschreibweise ($*$ heißt konjugiert komplex)

$$U_{ij}^+ = (U_{ji})^* = \left(U^{-1}\right)_{ij} \tag{3.17}$$

Falls U unitär ist so sind die repräsentierten physikalischen Operationen reversibel. Die oben eingeführten Matrizen für NOT, XOR und auch die Matrix für ${}^{CC}NOT$ sind unitär. Sie sind deshalb für die Realisierung von Rechenoperationen des QC tauglich. Mit anderen Worten, sie sind schon Beispiele für Quantengatter. Weitere Gatter, die nut auf Quantenbits Sinn machen, werden im folgenden beschrieben.

3.5.1 Ein-Bit Quantengatter

Die Erweiterung der Zustände des Speicherelementes (Spin) auf den gesamten Hilbertraum macht schon für den Fall eines einzelnen Spins völlig neue Gatter möglich. In der Tat repräsentiert jede unitäre 2×2 Matrix ein möglilches Gatter bzw. eine mögliche Manipulation auf einem Quanten–Bit. Als eine Art Basis in der Gruppe der unitären Transformationen dienen die Paulimatrizen

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

wobei z.B. $\sigma_1 = NOT$. Wichtige Gatter sind (i) das Kohärenzgatter (Hadamard–Transformation) mit

$$\begin{aligned} \mathbf{h}\,|0\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \qquad (3.18) \\ \mathbf{h}\,|1\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \end{aligned}$$

zusammengefasst (rechne mod 2)

$$\mathbf{h}\,|x\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-)^x\,|1\rangle\right), \qquad x \in \{0,1\} \tag{3.19}$$

das aus einem Bit ein Quantenbit macht. Wie man leicht prüft, ist

$$\mathbf{h} = \frac{1}{\sqrt{2}}\left(\sigma_1 + \sigma_3\right)$$

Weiterhin (ii) der Phasenschieber

$$\mathbf{P}\left(\phi\right)\left|\psi\right\rangle = e^{i\phi}\left|\psi\right\rangle$$

mit $\mathbf{P}\left(\phi\right) = \exp\left(i\phi\sigma_3\right)$, der die Phase eines Zustandes um ϕ ändert. Meist wird allerdings stattdessen die Operation

$$\mathbf{P}_\varepsilon = \begin{pmatrix} 1 & 0 \\ 0 & \varepsilon \end{pmatrix}, \qquad |\varepsilon|^2 = 1$$

verwendet, die ebenfalls den Vektor im Hilbertraum rotiert, wobei aber der Zustand $\left|0\right\rangle$ unverändert bleibt. Es ist ja

$$\begin{pmatrix} 1 & 0 \\ 0 & \varepsilon \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ \varepsilon\beta \end{pmatrix}$$

Eine Vielzahl von Gattern kann durch die parametrisierte unitäre Matrix

$$U_\theta = \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \tag{3.20}$$

beschrieben werden.

$$\left|s\right\rangle \Rightarrow \boxed{\text{Gatter}} \Rightarrow U_\theta\left|s\right\rangle \tag{3.21}$$

(Der Zustand $\left|s\right\rangle$ wird durch das Gatter geschickt und ist danach $\left|s'\right\rangle = U_\theta\left|s\right\rangle$). Beispielweise gilt

$$U_\pi\left|\uparrow\right\rangle = -\left|\downarrow\right\rangle \tag{3.22}$$

$$U_\pi\left|\downarrow\right\rangle = \left|\uparrow\right\rangle$$

für den Parameter $\theta = \pi$ bewirkt das Gatter also gerade die Bit–Umkehr. Damit hat U_π bei der Anwendung auf einen Spin mit definierter Projektion die gleiche Wirkung wie das klassische NOT–Gatter

$$U_\pi \quad\Leftrightarrow\quad NOT \tag{3.23}$$

Mit $\theta = \pi/2$ ergibt sich das Kohärenzgatter und mit (3.23) und

$$U_{\frac{\pi}{2}}U_{\frac{\pi}{2}} = U_\pi \quad = \quad NOT$$

gilt

$$U_{\frac{\pi}{2}} = \sqrt{NOT}$$

Arbeitet man mit Quatenbits, so ergeben sich also interessante Verallgemeinerungen der Booleschen Funktionen.

3.5.2 Zwei- und Drei–Bit Gatter

Die Operationen auf zwei Bits können wie schon im klassischen Fall besprochen, aus Ein–Bit Operationen durch Bildung des direkten Produktes der Matrizen konstruiert werden. Ausserdem sind wie schon erwähnt die Gatter für XOR wie auch das TL Gatter reversibel, d.h. die Matrizen sind unitär und sind damit unverändert auf den Quantenfall übertragbar.

3.5.3 Kohärenzgatter auf n Bits

Die Funktion des $\sqrt{NOT}$–Gatters besteht gemäß (**??**) in der Überführung eines definierten Spinzustandes in die kohärente Überlagerung der beiden Alternativen. Dieses Gatter überführt also das Bit mit dem Wert 0 in ein Quantenbit. Wir nennen dieses Gatter das Kohärenzgatter, weil es einen kohärenten Quantenzustand herstellt.

$$|\uparrow\rangle \Rightarrow \boxed{\text{Kohärenzgatter}} \Rightarrow \overline{|.\rangle}$$

Wenden wir diese Operation auf alle Bits eines Registers an, so erhalten wir

$$|\uparrow\uparrow \ldots \uparrow\rangle \Rightarrow \boxed{\text{Kohärenzgatter}} \Rightarrow \left(\frac{1}{\sqrt{2}}\right)^K \left[\left(|\downarrow\rangle + |\uparrow\rangle\right)\left(|\downarrow\rangle + |\uparrow\rangle\right) \ldots \left(|\downarrow\rangle + |\uparrow\rangle\right)\right] \tag{3.24}$$

für K Bits (Spins). Nun ist

$$\begin{aligned} \left(|\downarrow\rangle + |\uparrow\rangle\right)\left(|\downarrow\rangle + |\uparrow\rangle\right) \ldots \left(|\downarrow\rangle + |\uparrow\rangle\right) &= |\downarrow\downarrow \ldots \downarrow\rangle + |\uparrow\downarrow \ldots \downarrow\rangle + \ldots + |\uparrow\uparrow \ldots \uparrow\rangle \\ &= \sum_{a=0}^{2^K-1} |a\rangle \end{aligned} \tag{3.25}$$

weil $|\downarrow\rangle\,|\downarrow\rangle \ldots |\downarrow\rangle = |\downarrow\downarrow \ldots \downarrow\rangle$, usw. Die Spinzustände sind wieder als die Binärkodierung der Zahlen a verstanden. Wir bezeichnen mit

$$\overline{|a\rangle} = \left(\frac{1}{\sqrt{2}}\right)^K \sum_{a=0}^{2^K-1} |a\rangle \tag{3.26}$$

den kohärenten Zustand, so daß zusammengefaßt die Funktion des Kohärenzgatters in der Umwandlung des definierten Zustandes $|0\rangle = |\uparrow\uparrow \ldots \uparrow\rangle$ in den kohärenten Zustand besteht

$$|\uparrow\uparrow \ldots \uparrow\rangle \Rightarrow \boxed{\text{Kohärenzgatter}} \Rightarrow \overline{|a\rangle}$$

3.6 Auslesen der Register

Eine etwas knifflige Besonderheit der Quantenmechanik besteht darin, daß sie den Meßprozeß der Eigenschaften eines Systems nicht beschreibt. Im Sinne der Quantenmechanik ist das Meßgerät ein makroskopisches Objekt, das durch einen Satz von zueinander orthogonalen Zuständen $|\theta_k\rangle$, $k = 0, 1, \ldots$ beschrieben wird, die ihrerseits die Eigenzustände des sog. Meßoperators darstellen, der notwendig ein Hermitescher Operator ist,

$$M\,|\theta_k\rangle = m_k\,|\theta_k\rangle \tag{3.27}$$

wobei die m_k die Meßwerte sind und

$$\langle\theta_k|\theta_l\rangle = \delta_{k,l} \tag{3.28}$$

Wird nun ein System im Zustand $|\psi\rangle$ durch das Meßgerät mit Meßoperator M gemessen, so entspricht das einer Wechselwirkung mit dem Gerät, die den Zustand $|\psi\rangle$ in irreduzibler Weise verändert. Das ist ein reines Zufallsgeschehen, wobei genau einer der möglichen Meßwerte $m_{k,} \quad k \in \{0, 1, \ldots\}$ gemessen wird und gleichzeitig $|\psi\rangle$ augenblicklich in den zugehörigen Eigenzustand $|\theta_k\rangle$ übergeht. Danach bleibt das System dauerhaft in diesem Zustand, wenn es nicht durch äußere Einwirkungen gestört wird.

3.6.1 Realisierungswahrscheinlichkeiten der Meßereignisse

Die Quantenmechanik kann diesen "Kollaps" der Zustandsfunktion nicht beschreiben, sie macht aber eine genaue Aussage über die Wahrscheinlichkeiten für das Eintreten dieser Ereignisse. Sei P_k die Wahrscheinlichkeit für das Eintreten des Ereignisses k (Messung von m_k und Übergang $|\psi\rangle \to |\theta_k\rangle$). Dann gilt

$$P_k = |\langle\theta_k|\psi\rangle|^2 \tag{3.29}$$

das heißt, die Wahrscheinlichkeitsamplitude für die Messung von m_k ist durch die Überlappung des Zustandes $|\psi\rangle$ mit dem Eigenzustand $|\theta_k\rangle$ gegeben.

Als Beispiele betrachten wir die Messung der Spinprojektion längs der z-Achse. Der zugehörige Meßoperator ist

$$\sigma_3 = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{3.30}$$

Die zugehörigen Eigenzustände sind durch die Eigenwertgleichung

$$\sigma_3\,|\theta_k\rangle = m_k\,|\theta_k\rangle \tag{3.31}$$

definiert. Es gilt offensichtlich

$$\sigma_3\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad \sigma_3\begin{pmatrix} 0 \\ 1 \end{pmatrix} = -\frac{1}{2}\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

oder in der Diracnotierung

$$\sigma_3 \left|0\right\rangle = \frac{1}{2} \left|0\right\rangle , \qquad \sigma_3 \left|1\right\rangle = -\frac{1}{2} \left|1\right\rangle \tag{3.32}$$

Die Eigenzustände des Meßoperators stimmen also mit den bisherigen Basiszuständen für die Register unseres Computers überein.

Wie sieht nun beispielsweise die Messung der Spinprojektion aus, wenn das System (der Spin) sich in einem allgemeinen Zustand

$$\left|\psi\right\rangle = \alpha_0 \left|0\right\rangle + \alpha_1 \left|1\right\rangle \tag{3.33}$$

befindet. Wegen $\langle 0|1\rangle = \langle 1|0\rangle = 0$ sind offensichtlich die Wahrscheinlichkeiten

$$\begin{aligned} P_0 &= \left|\langle 0|\psi\rangle\right|^2 = \left|\alpha_0\right|^2 \\ P_1 &= \left|\langle 1|\psi\rangle\right|^2 = \left|\alpha_1\right|^2 \end{aligned} \tag{3.34}$$

Das kann man offensichtlich aus Gl. (3.33) direkt ablesen, denn in ihr ist ja der Zustand $\left|\psi\right\rangle$ direkt in Termen der Eigenzustände des Meßoperators dargestellt, so daß die Wahrscheinlichkeitsamplituden direkt abgelesen werden können.

3.6.2 Der Spezialfall der sicheren Messung

Ein Spezialfall tritt ein, wenn das System sich schon in einem Eigenzustand zum Meßoperator befindet. Das ist immer dann der Fall, wenn vorher schon eine Messung mit diesem Meßgerät durchgeführt wurde und seitdem keine weitere Wechselwirkung mit einem makroskopischen Objekt stattgefunden hat. Sei also etwa das System im Zustand $\left|\theta_k\right\rangle$. Dann wird bei einer weiteren Messung mit dem gleichen Meßgerät mit Sicherheit der Meßwert m_k beobachtet und der Systemzustand bleibt durch die Messung unbeeinflußt. Man sagt in diesem Falle, daß der Zustand des Systems bzw. die Meßwerte "scharf" sind.

3.6.3 Messungen an verschränkten Quantenzuständen

In den Kombiregistern des QC liegt im allgemeinen nach der Kohärenzierung des Input–Registers und Anwendung des Funktionsgatters ein verschränkter Quantenzustand vor. Wir betrachten das Beispiel der NOT Funktion mit einem Quanten-Input Bit $\left|Q\right\rangle = \frac{1}{\sqrt{2}} \left(\left|0\right\rangle + \left|1\right\rangle\right)$

$$E \otimes NOT \left|Q\right\rangle \otimes \left|0\right\rangle = \frac{1}{\sqrt{2}} \left(\left|0\right\rangle \otimes \left|1\right\rangle + \left|1\right\rangle \otimes \left|0\right\rangle\right)$$

Lesen wir (durch eine Messung) das erste Bit aus, so wird dieses mit Wahrscheinlichkeit 1/2 im Zustand $\left|0\right\rangle$ oder $\left|1\right\rangle$ beobachtet. Die Verschränkung äußert sich nun so, dass das Output–Bit in Korrespondenz zum Ergebnis der Messung des Input–Bits entsprechend zu $\left|1\right\rangle$ oder $\left|0\right\rangle$ festgelegt wird.

3.6.4 **Messung komplementärer Eigenschaften

Eine wichtige Besonderheit der Quantenmechanik, die im wesentlichen die Unschärferelation widerspiegelt, ist die Tatsache, daß es immer Messungen (mit verschiedenen Meßgeräten und folglich verschiedenen Meßoperatoren) gibt, deren Meßwerte nicht gleichzeitig scharf sein können.

Formal äußert sich die Tatsache, daß zwei Messungen komplementär zueinander sind dadurch, daß die zugehörigen Operatoren nicht kommutieren. Beispielsweise ist der Meßoperator für die Messung der x-Projektion des Spins durch die Paulimatrix

$$\sigma_1 = \frac{1}{2}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{3.35}$$

gegeben. Diese kommutiert nicht mit dem Meßoperator σ_3 für die Messung der z-Projektion, denn $\sigma_1\sigma_3 \neq \sigma_3\sigma_1$. In der Tat ist der Kommutator

$$[\sigma_1, \sigma_3] = \sigma_1\sigma_3 - \sigma_3\sigma_1 = -i\sigma_2$$

mit

$$\sigma_2 = \frac{1}{2}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{3.36}$$

der Paulimatrix, die gleichzeitig den Meßoperator für die Messung des Spins in x-Richtung darstellt.

Die Eigenzustände $|\chi_0\rangle$ und $|\chi_1\rangle$ von σ_1 sind

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \qquad \frac{1}{\sqrt{2}}\begin{pmatrix} -1 \\ 1 \end{pmatrix} \tag{3.37}$$

zum Eigenwert $\frac{1}{2}$ bzw. $-\frac{1}{2}$. In Diracnotation ist das

$$\begin{aligned} |\chi_0\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \\ |\chi_1\rangle &= -\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \end{aligned}$$

Analog sind die Eigenzustände $|\phi_0\rangle$ und $|\phi_1\rangle$ von σ_2 durch

$$\begin{aligned} |\phi_0\rangle &= -\frac{i}{\sqrt{2}}\left(|0\rangle + i\,|1\rangle\right) \\ |\phi_1\rangle &= \frac{i}{\sqrt{2}}\left(|0\rangle - i\,|1\rangle\right) \end{aligned}$$

gegeben. Aus der Sicht der Messungen bezüglich der z-Achse stellen diese Eigenvektoren also gerade ideale Quantenbits (gleichwahrscheinliche Zustände $|0\rangle$ und $|1\rangle$) dar. Generell sehen wir also, daß die Wahrscheinlichkeit, einen bestimmten Wert ($+1/2$ oder $-1/2$) der Projektion des Spins auf eine Achse zu bekommen immer genau gleich $1/2$ ist, wenn der Spin vorher bezüglich einer der anderen Achsen gemessen wurde. Die vorhergehende komplementäre Messung macht den Spins also maximal unbestimmt.