Kryptographie

Studienbrief 8

universität wien

Quantum Computing

Gerald und Susanne Teschl

Druckfehler/Feedback bitte an:
gerald.teschl@univie.ac.at

SS 23

Version:
2023-06-30

Studienbrief 8

Quantum Computing

Inhalt

Ende des 17. Jahrhunderts legte Isaac Newton (1643–1727) den Grundstein für die Formulierung der Gesetze der klassischen Mechanik, welche die Bewegung von festen, flüssigen oder gasförmigen Körpern unter dem Einfluss von Kräften beschreiben. Gemäß diesen Gesetzen wird die Bewegung eines (punktförmigen) Körpers alleine durch die Angabe seines Ortes und seiner Geschwindigkeit zu einem beliebigen Anfangszeitpunkt und die auf ihn wirkenden äußeren Kräfte beschrieben. Sind diese Daten bekannt, so kann sein Ort (und seine Geschwindigkeit) zu allen zukünftigen, und auch zu allen vergangenen, Zeiten eindeutig berechnet werden. Der Zustand wird also vollkommen durch Anfangsort und Anfangsgeschwindigkeit beschrieben.

Um die Jahrhundertwende geriet jedoch das bisherige physikalische Weltbild ins Wanken und es traten immer mehr Phänomene auf, die sich nicht mit den Gesetzen

der klassischen Physik erklären ließen. Das führte am Beginn des 20. Jahrhunderts zur Entdeckung der **Relativitätstheorie** durch Albert Einstein (1879–1955) und etwas später der **Quantenmechanik**. Zunächst in der Form von mathematischen *Kunstgriffen* bis sie schlussendlich unabhängig durch Werner Heisenberg (1901–1976) und Erwin Schrödinger (1887–1961) auf solide mathematische Beine gestellt wurden (mit unterschiedlichen Zugängen, die aber später als äquivalent nachgewiesen wurden). Paul Dirac (1902–1984) gelang es schließlich Quantenmechanik und Relativitätstheorie zu verbinden.

Das Revolutionäre an der Quantenmechanik ist, dass der Zustand eines Teilchens nicht mehr alleine durch die Angabe seines Ortes und seiner Geschwindigkeit, sondern durch eine Funktion, die so genannte **Wellenfunktion**, gegeben ist. Das Betragsquadrat dieser Funktion entspricht einer Aufenthaltsdichte des Teilchens, die beschreibt, mit welcher Wahrscheinlichkeit das Teilchen an den verschiedenen Orten anzutreffen ist. Im Gegensatz zur klassischen Physik lässt sich nun auch die Frage nach dem Ort des Teilchens an einem zukünftigen Zeitpunkt in dieser Form nicht mehr beantworten. Man kann nur noch sagen, dass es mit einer bestimmten Wahrscheinlichkeit dort und mit einer bestimmten Wahrscheinlichkeit da sein wird. Es ist ein bisschen wie bei einer Welle, deren Amplitude an verschiedenen Orten verschieden hoch ist und die in einem gewissen Sinn auch verteilt über einen ganzen Bereich ist. Wenn man versucht, den Ort des Teilchens zu bestimmen, also zu messen, dann entscheidet sich das Teilchen, entsprechend der vorgegebenen Wahrscheinlichkeiten, da zu sein oder eben dort zu sein. Hat es sich aufgrund einer Messung einmal entschieden, dann bleibt das auch so und es ist zu 100% dort, wo es gemessen wurde (es wechselt also durch die Messung zu einem Zustand, der mit dem Messergebnis kompatibel ist) und nicht mehr über den Raum verteilt wie eine Welle.

Gerade diese zufällige Komponente der Quantenmechanik wurde anfänglich von vielen Wissenschaftlern abgelehnt und von Einstein mit dem berühmten Satz „Gott würfelt nicht" zusammengefasst. Wir sind hier nicht in der Lage weiter auf diese Dinge einzugehen und werden nur ein sehr vereinfachtes Modell betrachten, das ausreicht, um ein mathematisches Modell eines Quantencomputers zu erstellen.

8.1 Mathematische Grundlagen der Quantenmechanik in Kürze

Der Zustand eines quantenmechanischen Systems wird durch einen (nichttrivialen) Vektor ψ in einem komplexen Vektorraum $\mathfrak{H}$ beschrieben. Aufgrund der eingangs erwähnten wahrscheinlichkeitstheoretischen Interpretation wird die Länge des Vektors auf 1 normiert und alle Vielfachen $\{\alpha\psi \,|\, \alpha \in \mathbb{C}\backslash\{0\}\}$ eines Vektors ψ beschreiben denselben physikalischen Zustand. Ein Zustand ist also technisch gesehen eine Äquivalenzklasse von Vektoren, obwohl das meistens unterschlagen

wird und man einfach vom Zustand ψ spricht. Es muss aber klar sein, dass, auch wenn ψ ein Einheitsvektor ist, die Vektoren $-\psi$, $\mathrm{i}\psi$, $\frac{1+\mathrm{i}}{\sqrt{2}}\psi$ etc. denselben Zustand beschreiben.

Da wir bereits den Begriff Länge in den Mund genommen haben, ist auch ersichtlich, dass dieser Begriff in unserem Vektorraum Sinn machen muss. Mehr noch, in der Quantenmechanik wird gefordert, dass der Längenbegriff durch ein Skalarprodukt erzeugt wird, unser Vektorraum also ein **Hilbertraum** ist.

In der Quantenmechanik ist dieser Hilbertraum typischerweise unendlichdimensional, wodurch sich weitere technische Finessen ergeben, auf die wir hier nicht eingehen können. Wir werden aber nur den Fall eines endlichdimensionalen Hilbertraums benötigen, unser Hilbertraum wird also immer der $\mathbb{C}^n$ sein.

Ist der Anfangszustand ψ_a bekannt, so kann man (bei Kenntnis aller auf das System wirkenden Kräfte) daraus den Zustand zu einem späteren Zeitpunkt t berechnen:

$$\psi(t) = U(t)\psi_a.$$

Dies geschieht durch Lösen einer linearen Differentialgleichung, der **Schrödingergleichung** $\mathrm{i}\hbar\frac{d}{dt}\psi(t) = H\psi(t)$, wobei H eine symmetrische Matrix ist, die die Kräfte, die auf das System wirken, beschreibt (die Hamilton-Funktion des Systems). Die Zahl $\hbar = 1.054\ldots10^{-34}Js$ ist das reduzierte Planck'sche Wirkungsquantum (auch Dirac'sche Konstante), benannt nach Max Planck (1858–1947). Plank hat es ursprünglich als Kunstgriff eingeführt (das h steht für Hilfsgröße) um das Strahlungsspektrum eines schwarzen Körpers mathematisch herleiten zu können. Seine Annahme, dass sich die Schwingungsenergie nur in ganzzahligen Vielfachen des Schwingungsquants $\hbar\omega$ ändern kann (mit ω die Kreisfrequenz der Schwingung), kann als Geburtsstunde der Quantenmechanik betrachtet werden. Ursprünglich hat niemand wirklich an diese Theorie geglaubt (auch Plank selbst nicht) und Einstein war einer der wenigen der die Bedeutung von Planks Arbeit erkannte und zeigte, dass mithilfe des Schwingungsquants auch der photoelektrische Effekt erklärt werden kann.

Die Quantenmechanik besagt, dass diese Zuordnung von einem Anfangszustand auf einen späteren Zustand eine lineare Abbildung (lineare Transformation) ist. Da diese Abbildung $U(t)$ die Normierung des Zustandes erhalten muss, muss sie für jeden Vektor die Norm erhalten. Man kann in diesem Fall zeigen, dass $U(t)$ sogar das Skalarprodukt (also die Winkel zwischen Vektoren) erhalten muss und solche Abbildungen nennt man **orthogonale** oder auch **unitäre Transformationen**.

Erinnern Sie sich daran, dass eine Matrix genau dann unitär ist, wenn sie invertierbar ist und die Inverse gleich der Adjungierten ist: $U^{-1} = U^*$ (die adjungierte Matrix ist die konjugiert komplexe der transponierten Matrix und wird in der Physik meist mit $U^\dagger$ bezeichnet). Eine Matrix mit $A = A^*$ nennt man symmetrisch bzw. selbstadjungiert (in der Physik auch oft hermitisch).

Wir werden hier nicht darauf eingehen, wie die Transformation U aus den physikalischen Gesetzen der Quantenmechanik zu berechnen ist, sondern begnügen uns mit der Tatsache, dass, wenn ein Quantencomputer aus einem Anfangszustand einen Endzustand macht, dies nur mithilfe einer unitären Transformation geschehen kann. Ob und wie man physikalisch eine konkrete Transformation realisieren

kann, soll nicht unsere Sorge sein. In der binären Logik rechnen wir auch mit logischen Gattern (NOT, AND, OR, XOR, etc.) und machen uns in dem Moment keine Gedanken darüber, wie diese elektronisch umgesetzt werden.

Wenn wir unser System also eine Reihe von Quantengattern durchlaufen lassen, so wird jedes einzelne durch eine unitäre Transformation beschrieben. Der Endzustand nach Durchlaufen aller Gatter entspricht dem Produkt der einzelnen Transformationen (Hintereinanderausführung der Abbildungen) und ist damit selbst natürlich auch wieder eine unitäre Transformation U.

Haben wir den Anfangszustand ψ_a nun in den gewünschten Endzustand $U\psi_a$ gebracht, so müssen wir noch das Ergebnis unserer Berechnung vom Endzustand ablesen. Wir müssen also den Endzustand vermessen. Wie schon in der Einleitung angedeutet, ist es leider nicht möglich, den Endzustand genau festzustellen. Man kann dem System nur bestimmte Fragen stellen, die es dann mit bestimmten Wahrscheinlichkeiten beantwortet. Ein typische Frage ist, ob sich das System in einem bestimmten vorgegeben Zustand, nennen wir ihn ϕ, befindet. Dann würde das System diese Frage mit Wahrscheinlichkeit $|\langle\phi, U\psi_a\rangle|^2$ mit "Ja" und mit der Gegenwahrscheinlichkeit $1 - |\langle\phi, U\psi_a\rangle|^2$ mit "Nein" beantworten. Das klingt im ersten Moment ziemlich unbefriedigend, aber wenn man die Berechnung genügend oft wiederholt, so kann man die Wahrscheinlichkeit mit beliebiger Genauigkeit bestimmen. Natürlich bleibt die Möglichkeit eines statistischen Ausreißers, aber auch bei einem klassischen Computer kann die Möglichkeit eines Rechenfehlers (z.B. aufgrund von kurzzeitigen Spannungsschwankungen) nicht 100%ig ausgeschlossen werden.

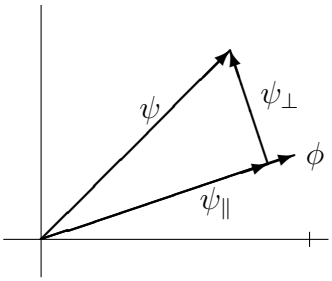


Abbildung 8.1: Orthogonale Projektion

Mathematisch gesehen entspricht die Messung einer orthogonalen Projektion.

Eine Projektion ist eine lineare Abbildung P mit der Eigenschaft $P^2 = P$. Eine orthogonale Projektion ist zusätzlich symmetrisch, $P^* = P$. Mithilfe einer Projektion kann man jeden Vektor ψ in zwei Komponenten zerlegen:t $\psi = P\psi + (\mathbb{I} - P)\psi$ (dabei ist $\mathbb{I}$ die Abbildung von ψ auf sich selbst). Bei einer orthogonalen Projektion sind die beiden Komponenten orthogonal: $\langle P\psi, (\mathbb{I} - P)\psi\rangle = \langle\psi, P^*(\mathbb{I} - P)\psi\rangle = \langle\psi, (P - P^2)\psi\rangle = 0$. Die orthogonale Projektion auf einen Einheitsvektor ϕ ist gegeben durch $P\psi = \langle\phi, \psi\rangle\phi$.

Der Endzustand $U\psi_a$ wird in eine Komponente $\psi_\parallel = \langle\phi, U\psi_a\rangle\phi$ parallel zu ϕ und eine Komponente $\psi_\perp = 1 - \psi_\parallel$ orthogonal zu ϕ zerlegt (vgl. Abbildung 8.1).

Entscheidet sich das System für ϕ, so ist es fortan im Zustand ϕ. Entscheidet es sich dagegen, so ist es fortan im Zustand $\frac{\psi_\perp}{\|\psi_\perp\|}$.

Fassen wir zusammen:

Definition 8.1 (Vereinfachte) Axiome der Quantenmechanik

- Der Zustand des Systems wird durch einen normierten Vektor ψ in einem Hilbertraum $\mathfrak{H}$ beschrieben. Alle (nichttrivialen) komplexen Vielfachen des Vektors beschreiben den gleichen Zustand.
- Der Übergang eines Zustands in einen neuen Zustand durch Wechselwirkung mit der Umgebung wird durch eine unitäre Transformation U beschrieben.
- Bei der Messung, ob sich das durch ψ beschriebene System in einem vorgegebenen Zustand ϕ befindet, entscheidet sich das System gemäß der Wahrscheinlichkeiten, die durch das Quadrat der Länge der entsprechenden Projektionen von ψ (parallel bzw. orthogonal zu ϕ) gegeben sind. Nach der Messung ist der neue Zustand durch die dem Ergebnis entsprechenden (normierten) Projektion gegeben.

Mehr Hintergrund zur Quantenmechanik findet man z.B. in [Tha00; Tha05].

8.2 Ein Qubit

Werden wir nun etwas konkreter. Das einfachste nichttriviale System wird durch einen zweidimensionalen Hilbertraum beschrieben und ist als **Qubit** bekannt.

Ein Qubit ist in der Regel ein Teilaspekt eines größeren Systems. Insbesondere ist ein Qubit (so wie ein Bit) ein mathematisches Modell und es gibt verschiedene Möglichkeiten dieses praktisch umzusetzen (Z.B.: Spin eines Elektrons, Polarisierung eines Photons, etc.).

Unser Hilbertraum ist also $\mathfrak{H} = \mathbb{C}^2$ und ein Zustand ist ein Einheitsvektor

$$\psi = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}, \qquad |\alpha_0|^2 + |\alpha_1|^2 = 1.$$

Jeder Vektor in unserem zweidimensionalen Vektorraum kann als Linearkombination von zwei Basisvektoren $\psi_0 = (1, 0)$ und $\psi_1 = (0, 1)$ geschrieben werden:

$$\psi = \alpha_0\psi_0 + \alpha_1\psi_1.$$

Dieses mathematisch wenig spektakuläre Resultat würde man physikalisch so interpretieren, dass unser System gleichzeitig in beiden Zuständen ψ_0 und ψ_1 ist, und zwar mit Wahrscheinlichkeit $|\alpha_0|^2$ im Zustand ψ_0 und mit Wahrscheinlichkeit $|\alpha_1|^2$ im Zustand ψ_1. Man spricht auch von einem **Überlagerungszustand**. Würden

wir es also im Rahmen einer Messung zur Rede stellen, so würden wir mit Wahrscheinlichkeit $|\alpha_0|^2$ die Antwort ψ_0 und mit Wahrscheinlichkeit $|\alpha_1|^2$ die Antwort ψ_1 erhalten.

Achtung: Auf den ersten Blick scheint es naheliegend zu vermuten, dass diese Wahrscheinlichkeitsinterpretation dadurch erklärt werden kann, dass man den Zustand des Systems eben einfach nicht genau genug kennt. So wie man das Ergebnis eines Münzwurfs nicht vorhersagen kann, weil man den exakten Abwurfwinkel und die exakte Abwurfgeschwindigkeit nicht kennt. Dem ist aber nicht so. Man kann zeigen, dass eine Erklärung der Quantenmechanik durch sogenannte versteckte Parameter, die man eben noch nicht kennt, nicht möglich ist. Wir müssen uns also damit abfinden, dass unser System in zwei Zuständen gleichzeitig sein kann.

Nachdem wir diese erste Hürde genommen haben, kommt gleich die nächste, die Notation. Zunächst halten wir fest, dass wir zur Beschreibung unseres Systems natürlich auch jede andere Orthonormalbasis nehmen hätten können. Und auch wie wir die Vektoren in unserer Orthonormalbasis bezeichnen, spielt natürlich keine Rolle. In der Physik kann ein Qubit z.B. durch den Spin (der innere Drehimpuls) eines Elektrons realisiert werden. Für diesen gibt es zwei mögliche Werte *Spin-Up* $\psi_\uparrow$ und *Spin-Down* $\psi_\downarrow$ und ein allgemeiner Zustand wird durch

$$\psi = \alpha_0\psi_\uparrow + \alpha_1\psi_\downarrow$$

beschrieben. Außer ein paar Umbenennungen ist noch nichts passiert, nun kommen wir aber zur angekündigten neuen Notation. Quantenphysiker lieben die auf Dirac zurückgehende **Bra-Ket-Notation** (auch **Dirac-Notation**). Hier werden Vektoren als Ket's $|\psi\rangle$, $|\phi\rangle$, etc. geschrieben und ein Bra $\langle\psi|$, $\langle\phi|$, etc. beschreibt den zugehörigen *dualen* Vektor, der mithilfe des Skalarprodukts ein Ket in eine komplexe Zahl umwandelt, also $\langle\psi|\,|\phi\rangle = \langle\psi|\phi\rangle = \langle\psi,\phi\rangle$.

Achtung: Es gilt zwar $|\alpha_0\psi_0 + \alpha_1\psi_1\rangle = \alpha_0\,|\psi_0\rangle + \alpha_1\,|\psi_1\rangle$, aber $\langle\alpha_0\psi_0 + \alpha_1\psi_1| = \alpha_0^*\,\langle\psi_0| + \alpha_1^*\,\langle\psi_1|$, da das Skalarprodukt im komplexen Fall konjugiert linear im ersten Argument ist. Fasst man $|\psi\rangle$ als Spaltenvektor auf, so ist $|\psi\rangle^* = \langle\psi|$ der zugehörige konjugierte Zeilenvektor.

Die Messung, ob das System im Zustand ϕ ist, wird dann oft mit $|\phi\rangle\,\langle\phi|$ beschrieben, was der Projektion auf die Komponente $|\phi\rangle\langle\phi|\,|\psi\rangle = \langle\phi,\psi\rangle\,|\phi\rangle$ parallel zu ϕ entspricht.

Um Tinte zu sparen schreibt man dann statt $|\psi_\uparrow\rangle$ nur kurz $|\uparrow\rangle$, etc. In diesem Sinn würde man für die Basisvektoren ψ_0 und ψ_1 in der Dirac-Notation $\psi_0 = |\psi_0\rangle = |0\rangle$ bzw. $\psi_1 = |\psi_1\rangle = |1\rangle$ schreiben. Gerade die letzte Schreibweise ist in der Informatik recht beliebt, da die zwei Basiszustände $|0\rangle$ und $|1\rangle$ des Qubits uns an die wohlvertrauten zwei möglichen Zustände 0 und 1 eines klassischen Bits erinnern.

Genau in dieser Vertrautheit liegt aber auch die größte Gefahr: Nämlich, dass man darauf vergisst, wofür die Symbole eigentlich stehen! Ein klassisches Bit kann eben wirklich nur die beiden Zustände 0 und 1 annehmen, während für ein Qubit auch alle Zustände $\alpha_0\,|0\rangle + \alpha_1\,|1\rangle$ dazwischen erlaubt sind! Und genau darin liegt wiederum seine Stärke!

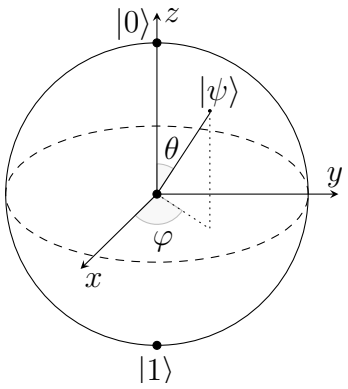


Abbildung 8.2: Bloch-Kugel zur Veranschaulichung eines Qubits

Wollen wir uns ein Qubit veranschaulichen, so haben wir zunächst das Problem, dass wir für jede komplexe Zahl zwei reelle Dimensionen brauchen (eine für den Real- und eine für den Imaginärteil), insgesamt hier also $2 \cdot 2 = 4$, was leider die Vorstellungskraft der meisten Menschen sprengt. Zum Glück beschreibt aber jedes (komplexe) Vielfache den gleichen Zustand, wodurch wieder 2 Dimensionen wegfallen und eine Darstellung als Punkt auf der Einheitskugel im $\mathbb{R}^3$ möglich wird: Es sei also $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ und wir wählen das Vielfache so, dass $|\psi\rangle$ normiert und der erste Koeffizient positiv ist. Es gilt also $\alpha_0 \geq 0$ und $\alpha_0^2 + |\alpha_1|^2 = 1$ und wir können $\alpha_0 = \cos(\frac{\theta}{2})$, $\alpha_1 = \sin(\frac{\theta}{2})\mathrm{e}^{\mathrm{i}\varphi}$ mit $0 \leq \theta \leq \pi$, $0 \leq \varphi < 2\pi$ schreiben. Identifiziert man $|\psi\rangle$ mit dem Einheitsvektor $(\sin(\theta)\cos(\varphi), \sin(\theta)\sin(\varphi), \cos(\theta))$ mit den sphärischen Koordinaten θ und φ, so erhält man die **Bloch-Kugel** aus Abbildung 8.2. Beachten Sie, dass der Nordpol $|\psi\rangle = |0\rangle$ und der Südpol $|\psi\rangle = |1\rangle$ entspricht.

Nachdem wir uns also mit dem Qubit vertraut gemacht haben, wollen wir nun damit rechnen.

Beispiel 8.2 Das **NOT-Gatter** oder **X-Gatter** wird durch die unitäre Matrix

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

beschrieben. Weisen Sie nach, dass es sich in der Tat um eine unitäre Transformation handelt. Zeigen Sie, dass sich ein System nach zweimaligem Durchlaufen des X-Gatters wieder im Ausgangszustand befindet.

Lösung zu 8.2 Es gilt $U_X^* = U_X$, und wir rechnen

$$U_X U_X^* = U_X^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

nach. Wegen $U_X^2 \psi = \psi$ befindet sich das System wieder im Ausgangszustand. ■

Das X-Gatter tauscht die beiden Basiszustände $|0\rangle$ und $|1\rangle$ aus. Das X in der Notation erklärt sich dadurch, dass es sich um eine der drei **Pauli-Matrizen**

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

handelt (oft findet man auch die Notation σ_1, σ_2, σ_3). Sie sind benannt nach dem Physiker Wolfgang Pauli (1900–1958). Die zugehörigen anderen beiden Gatter werden, wie nicht schwer zu erraten, mit U_Y und U_Z bezeichnet. Die Pauli-Matrizen sind nicht nur unitär, sondern auch symmetrisch und insbesondere ergibt das Quadrat jeder Pauli-Matrix die Einheitsmatrix. Es gilt sogar, dass die Pauli-Matrizen bei Multiplikation (bis auf ein Vielfaches) immer unter sich bleiben (vgl. Aufgabe 12).

Beispiel 8.3 Das **Hadamard-Gatter** wird durch die unitäre Matrix

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

beschrieben. Weisen Sie nach, dass es sich in der Tat um eine unitäre Transformation handelt. In welchem Zustand befindet sich ein System, nachdem es zwei Hadamard-Gatter durchlaufen hat?

Lösung zu 8.3 Wieder gilt $H^* = H$ und wir rechnen

$$HH^* = H^2 = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

nach. Wegen $H^2 = \mathbb{I}_2$ befindet sich das System wieder im Ausgangszustand. ■

Das Hadamard-Gatter transformiert die beiden Basiszustände $|0\rangle$ und $|1\rangle$ auf die neue Orthonormalbasis

$$|+\rangle = \frac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big), \quad |-\rangle = \frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big).$$

Es entspricht übrigens genau der diskreten Kosinustransformation in zwei Dimensionen.

Wir können die Gatter U im Prinzip in einer beliebigen Orthonormalbasis beschreiben, dabei ändert sich aber natürlich die Matrixdarstellung. Z.B. kann man leicht $U_X\,|\pm\rangle = \pm\,|\pm\rangle$ nachrechnen und die Matrixdarstellung von U_X in dieser Basis ist genau σ_z. Wir werden hier aber immer bei der Standardbasis $|0\rangle$, $|1\rangle$ bleiben.

Weitere wichtige Gatter sind die Phasengatter

$$U_S = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{i} \end{pmatrix}, \quad U_S^* = \begin{pmatrix} 1 & 0 \\ 0 & -\mathrm{i} \end{pmatrix}$$

und

$$U_T = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1+\mathrm{i}}{\sqrt{2}} \end{pmatrix}, \quad U_T^* = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1-\mathrm{i}}{\sqrt{2}} \end{pmatrix}.$$

Es gilt übrigens $U_S^2 = U_Z$ und $U_T^2 = U_S$.

Mit den bisher erwähnten Gattern kann man nicht alle denkbaren Gatter realisieren. Hätte man zum Beispiel nur die Pauli-Gatter zur Verfügung, so würde man durch Verknüpfung dieser irgendwann nicht mehr weiterkommen, da diese eine endliche Gruppe (die Pauli-Gruppe, vgl. Aufgabe 12) bilden. Deshalb muss man noch weitere Gatter, wie die Phasengatter, hinzunehmen (vgl. auch [Bar+95]). Allerdings benötigt man in jedem Fall unendlich viele Gatter. Eine mögliche Wahl sind

$$R_x(\theta) = \begin{pmatrix} \cos(\theta/2) & -\mathrm{i}\sin(\theta/2) \\ -\mathrm{i}\sin(\theta/2) & \cos(\theta/2) \end{pmatrix}, \qquad R_y(\theta) = \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix},$$
$$R_z(\theta) = \begin{pmatrix} \mathrm{e}^{-\mathrm{i}\theta/2} & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\theta/2} \end{pmatrix}, \qquad P(\varphi) = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\varphi} \end{pmatrix},$$

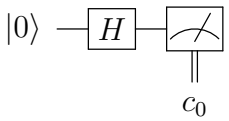
für alle $\theta, \varphi \in [0, 2\pi)$. Wegen $R_x(\theta)^* = R_x(\theta)^{-1} = R_x(-\theta)$ (und analog für R_y, R_z und P) sind diese Gatter unitär. Ausserdem gilt $U_Z = P(\pi)$, $U_S = P(\pi/2)$, $U_T = P(\pi/4)$ (beachte $\frac{1\pm\mathrm{i}}{\sqrt{2}} = \mathrm{e}^{\pm\mathrm{i}\pi/4}$) und $R_x(\theta) = R_z(-\pi/2)R_y(\theta)R_z(\pi/2)$.

Damit kann eine beliebige unitäre Transformation U wie folgt darstellen: Der erste Spaltenvektor muss normiert sein und kann daher in der Form $(\mathrm{e}^{\mathrm{i}\varphi_1}\cos(\theta), \mathrm{e}^{\mathrm{i}\varphi_2}\sin(\theta))$ geschrieben werden. Der zweite Spaltenvektor muss ebenfalls normiert und zum ersten orthogonal sein, daher muss er von der Form $\mathrm{e}^{\mathrm{i}\varphi_3}(-\mathrm{e}^{-\mathrm{i}\varphi_2}\sin(\theta), \mathrm{e}^{-\mathrm{i}\varphi_1}\cos(\theta))$ sein. Insgesamt ist also jede unitäre Matrix von der Form

$$U = \begin{pmatrix} \mathrm{e}^{\mathrm{i}\varphi_1}\cos(\theta) & -\mathrm{e}^{\mathrm{i}(\varphi_3-\varphi_2)}\sin(\theta) \\ \mathrm{e}^{\mathrm{i}\varphi_2}\sin(\theta) & \mathrm{e}^{\mathrm{i}(\varphi_3-\varphi_1)}\cos(\theta) \end{pmatrix} = R_z(-\varphi_1+\varphi_2)R_x(2\theta)R_z(-\varphi_1-\varphi_2)P(\varphi_3).$$

Beispiel 8.4 (Erzeugung von Zufallsbits) Präpariere das System im Anfangszustand $|0\rangle$. Durchlaufe das Hadamard-Gatter: $H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. Nun messen wir, ob das System im Zustand $|0\rangle$ ist. Wir erhalten mit Wahrscheinlichkeit $\frac{1}{2}$ das Ergebnis "Ja" und mit $\frac{1}{2}$ das Ergebnis "Nein".

Die zugehörige Schaltung kann wie folgt veranschaulicht werden:



Die Ausgabe ist das klassische Bit c_0, das auf 0 gesetzt wird, wenn das Qubit im Zustand $|0\rangle$ gefunden wird, und auf 1, wenn es im Zustand $|1\rangle$ gefunden wird.

Um ein Qubit im Zustand $|0\rangle$ zu erhalten, können wir zum Beispiel mit einem beliebigen Qubit starten und messen, ob es im Zustand $|0\rangle$ ist. Wenn ja, sind wir fertig. Wenn nein, ist es nun im Zustand $|1\rangle$ und wir müssen es nur noch durch ein NOT-Gatter schicken.

Die drei Pauli-Gatter werden in Schaltkreisen mit —[X]—, —[Y]—, —[Z]— bezeichnet. Für das X-Gatter verwendet man auch —⊕—. Einfache Linien entsprechen Qubits, während doppelte Linien klassischen Bits entsprechen. Eine Messung wird durch —[⌒]═ symbolisiert (wenn nicht anders angegeben, wird gemessen, ob das Qubit im Zustand $|0\rangle$ ist).

Beachten Sie in diesem Zusammenhang, dass ein Quantencomputer in der Praxis typischerweise von einem klassischen Computer gesteuert wird. Ein Quantencomputer ist also kein *Supercomputer* der einfach alles schneller kann, sondern eine Art Koprozessor, an den der klassische Computer bestimmte Berechnungen auslagert, die ein Quantencomputer effizienter ausführen kann.

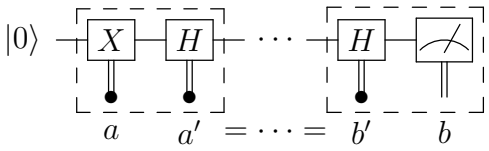
Anwendung: Abhörsicherer Schlüsseltausch mit BB84

Den Schaltkreis zur Erzeugung von Zufallsbits kann man noch etwas weiter ausbauen um einen Algorithmus für einen sicheren Schlüsseltausch zu erhalten. Er stammt von Bennett and Brassard [BB84]. Die zugrundeligende Idee ist es, auszunutzen, dass Eve einen Zustand nicht kopieren kann, und daher verändern muss, wenn sie Informationen über den Zustand erhalten möchte. Dass Zustände nicht kopiert werden können besagt das No-Cloning-Theorem, das wir im nächsten Abschnitt besprechen werden.

Nehmen wir an, Alice präpariert Zustände zufällig als $|0\rangle$ oder $|1\rangle$ und schickt sie an Bob. Dieser misst die Qubits und am Ende haben beide die gleiche Folge von Bits. In diesem Fall ist es natürlich für Eve einfach, jedes Qubit zu messen und danach an Bob weiterzuleiten.

Wenn nun aber Alice den zufälligen Zustand auch noch gegebenfalls zufällig durch ein Hadamard-Gatter schickt, so hat Eve ein Problem, da sie nicht weiß, ob das Qubit das Hadamard-Gatter durchlaufen hat oder nicht. Erhält Eve also das Ergebnis $|0\rangle$, so weiß Eve nicht ob Alice $|0\rangle$ geschickt hat oder ob Alice $\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ geschickt hat und sich das Qubit bei der Messung zufällig für $|0\rangle$ entschieden hat. Mehr noch, Eve hat durch ihre Messung den Zustand verändert und kann nur noch den veränderten Zustand an Bob weiterleiten.

Das gleiche Problem hat aber auch Bob und daher wird zusätzlich ein klassischer Kanal benötigt, über den diese Information ausgetauscht wird:



Der schwarze Punkt im Schaltreis signalisiert hier, dass das Gatter über das angegebene klassische Bit gesteuert wird. D.h., das Gatter ist nur aktiv wenn das klassische Bit gleich 1 ist.

Der Ablauf ist nun wie folgt: Alice erzeugt die Zufallsbits a, a' und präpariert das Qubit, das dann an Bob geschickt wird. Bob erzeugt ebenfalls ein Zufallsbit b' und misst dementsprechend mit bzw. ohne Hadamard-Gatter. Danach werden a' und b' über den klassichen Kanal verglichen. Stimmen Sie überein, so wird das übertragene Bit $a = b$ behalten, ansonsten verworfen.

In der Praxis wird dieses Verfahren mit Photonen (Lichtquanten) realisiert, da diese leicht über weite Distanzen geschickt werden können. Die beiden möglichen Zustände auf die man sich dabei beschränkt sind die lineare Polarisierung des Photons.

Warum ist dieses Verfahren abhörsicher? Angenommen, Eve kann Qubits abfangen und auch den klassichen Kanal abhören. Eve fängt also die Qubits ab und misst sie. Nun muss Eve raten ob Alice das Hadamardgatter verwendet hat oder nicht. Rät Eve richtig, so erhält Eve das korrekte Bit und kann auch den korrekten Zustand an Bob weiterleiten. Liegt Eve aber falsch, so erhält Eve nur mit Wahrscheinlichkeit $\frac{1}{2}$ das korrekte Bit und leitet auch einen falschen Zustand an Bob weiter. In Folge erhält auch Bob nur mit Wahrscheinlichkeit $\frac{1}{2}$ das korrekte Bit. Insgesamt hat also mit Wahrscheinlichkeit $\frac{3}{4}$ Eve das gleiche Bit wie Alice und das Gleiche gilt für Bob (wobei die Bits von Eve und Bob nicht gleich sondern ebenfalls mit Wahrscheinlichkeit $\frac{3}{4}$ verschieden sind).

Die Sicherheit beruht also auf der Tatsache, dass die Messung von Eve (das Abhöhren) den Zustand verändert. Man könnte meinen, Eve könnte das verhindern indem sie nicht das Original, sondern eine Kopie für die Messung verwendet. Aber die Spielregeln der Quantenmachanik erlauben es nicht den Zustand eines Qubits zu kopieren. Das ist die Aussage des No-Cloning-Theorems (Satz 8.8), zu dem wir später noch kommen werden.

Der Eingriff von Eve würde also ziemlich schnell auffliegen! Aber es geht noch besser. Alice und Bob können den Eingriff von Eve sofort erkennen, indem sie einen Teil der ausgetauschten Bits nach dem Austausch vergleichen (das muss über den unsicheren klassischen Kanal geschehen und diese Bits sind somit verloren). Vergleicht man n Bits, so ist die Wahrscheinlichkeit, dass Eve unentdeckt bleibt, gleich $(\frac{3}{4})^n$, was beliebig klein gemacht werden kann.

Hat Eve auch die Möglichkeit, den klassischen Kanal zu verändern, so steht ihr ein Man-in-the-Middle Angriff offen, gegen den auch dieses Verfahren nicht schützt. Außerdem sind natürlich auch Implementierungsangriffe weiterhin möglich (siehe z.B. [Lyd+10]).

8.3 Noch mehr Qubits

Auch wenn ein Quantencomputer mit einem Qubit schon um einiges spannender als ein klassischer Rechner mit einem Bit ist, so zählt auch in der Quantenwelt die Regel “Mehr ist besser”.

Im Prinzip könnte man natürlich einfach ein beliebiges System mit mehr als zwei Freiheitsgraden betrachten, man beschränkt sich bei einem Quantencomputer aber auf Systeme, die aus mehreren Qubits aufgebaut sind.

Deshalb betrachten wir nun Systeme die aus mehreren Qubits aufgebaut sind. Man spricht auch von einem **Register**.

In der Quantenmechanik wird ein System, das aus zwei Teilsystemen besteht, durch das **Tensorprodukt** beschrieben. Beschreibt $\mathfrak{H}_1$ das erste und $\mathfrak{H}_2$ das zweite System, so wird das Gesamtsystem durch das Tensorprodukt $\mathfrak{H}_1 \otimes \mathfrak{H}_2$ beschrieben, das aus der Menge der Linearkombinationen aller formalen Produkte

$$\psi_1 \otimes \psi_2, \qquad \psi_1 \in \mathfrak{H}_1,\ \psi_2 \in \mathfrak{H}_2$$

besteht so, dass folgende Rechenregeln gelten:

$$(\psi_1 + \phi_1) \otimes \psi_2 = \psi_1 \otimes \psi_2 + \phi_1 \otimes \psi_2,$$
$$\psi_1 \otimes (\psi_2 + \phi_2) = \psi_1 \otimes \psi_2 + \psi_1 \otimes \phi_2,$$
$$(\alpha_1\psi_1) \otimes (\alpha_2\psi_2) = (\alpha_1\alpha_2)\psi_1 \otimes \psi_2.$$

Achtung: Das Tensorprodukt ist nicht kommutativ (also $\psi_1 \otimes \psi_2 \neq \psi_2 \otimes \psi_1$)! Ansonsten sind das die üblichen Rechenregeln, die uns vom Produkt zweier Zahlen vertraut sind.

Das Skalarprodukt ist über

$$\langle \psi_1 \otimes \psi_2, \phi_1 \otimes \phi_2 \rangle = \langle \psi_1, \phi_1 \rangle \langle \psi_2, \phi_2 \rangle$$

definiert. Am einfachsten kann man das Tensorprodukt verstehen, indem man zwei Orthonormalbasen für $\mathfrak{H}_1$ und $\mathfrak{H}_2$ nimmt. Dann ist die Menge aller Tensorprodukte der Basisvektoren eine Orthonormalbasis für $\mathfrak{H}_1 \otimes \mathfrak{H}_2$. Da es für diese Produkte genau $\dim(\mathfrak{H}_1) \cdot \dim(\mathfrak{H}_2)$ Möglichkeiten gibt, gilt $\dim(\mathfrak{H}_1 \otimes \mathfrak{H}_2) = \dim(\mathfrak{H}_1)\dim(\mathfrak{H}_2)$.

Konkret ist der Hilbertraum für ein System aus zwei Qubits also $2 \cdot 2 = 4$-dimensional und die Vektoren

$$|0\rangle \otimes |0\rangle, \quad |0\rangle \otimes |1\rangle, \quad |1\rangle \otimes |0\rangle, \quad |1\rangle \otimes |1\rangle$$

bilden eine Orthonormalbasis. Wir schreiben dafür kurz auch einfach

$$|00\rangle, \quad |01\rangle, \quad |10\rangle, \quad |11\rangle.$$

Es geht sogar noch kürzer, indem man die Folge aus Nullen und Einsen als Binärdarstellung auffasst und dann

$$|0\rangle, \quad |1\rangle, \quad |2\rangle, \quad |3\rangle$$

schreibt. Hier lauert dann aber schon einer der vielen Fallstricke der Dirac-Notation: Ist $|0\rangle$ ein einzelnes Qubit oder sind das zwei Qubits im Zustand $|00\rangle$? In diesem Fall muss dann aus dem Kontext klar sein, aus wie vielen Qubits das System besteht!

Ist also das erste Qubit im Zustand $\alpha_0 |0\rangle + \beta_0 |1\rangle$ und das zweite Qubit im Zustand $\alpha_1 |0\rangle + \beta_1 |1\rangle$, so ist das Gesamtsystem im Zustand

$$(\alpha_0 |0\rangle + \beta_0 |1\rangle) \otimes (\alpha_1 |0\rangle + \beta_1 |1\rangle) = \alpha_0\alpha_1 |00\rangle + \alpha_0\beta_1 |01\rangle + \beta_0\alpha_1 |10\rangle + \beta_0\beta_1 |11\rangle.$$

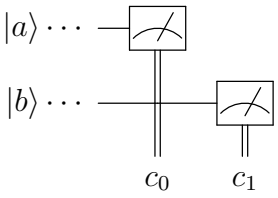
Dass das Tensorprodukt die korrekte Beschreibung ist, kann als weiteres Axiom der Quantenmechanik betrachtet werden. Anschaulich kann es dadurch motiviert werden, dass im obigen Fall die Wahrscheinlichkeiten durch die zugehörigen Produktwahrscheinlichkeiten gegeben sind. D.h. die Wahrscheinlichkeit (z.B.) beide Qubits im Zustand $|0\rangle$ zu finden ist $|\alpha_0\alpha_1|^2$, also die Wahrscheinlichkeit $|\alpha_0|^2$, dass

das erste im Zustand $|0\rangle$ ist, mal der Wahrscheinlichkeit $|\alpha_1|^2$, dass das zweite im Zustand $|0\rangle$ ist.

Der allgemeine Zustand eines Registers aus zwei Qubits ist also durch

$$\psi = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle$$

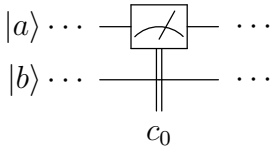
gegeben. Bei einer Messung beider Qubits



erhalten wir das Ergebnis $c_0c_1 = 00$ mit Wahrscheinlichkeit $|\alpha_{00}|^2$, das Ergebnis $c_0c_1 = 01$ mit Wahrscheinlichkeit $|\alpha_{01}|^2$, etc. Der neue Zustand ist je nach Ergebnis der Messung $|00\rangle$, $|01\rangle$, etc.

Es müssen aber nicht beide, sondern es kann auch nur eines der beiden Qubits gemessen werden. Um den neuen Zustand nach der Messung zu erhalten, sind alle Komponenten, die mit dem Ergebnis der Messung unvereinbar sind, zu entfernen und der resultierende Vektor ist neu zu normieren.

Wollen wir (z.B.) nur das erste Qubit messen,



so schreiben wir den Zustand etwas um

$$\psi = |0\rangle \otimes \big(\alpha_{00}\,|0\rangle + \alpha_{01}\,|1\rangle\,\big) + |1\rangle \otimes \big(\alpha_{10}\,|0\rangle + \alpha_{11}\,|1\rangle\,\big).$$

Daraus ersehen wir, dass wir das Ergebnis $c_0 = 0$ mit Wahrscheinlichkeit $\|\alpha_{00}\,|0\rangle + \alpha_{01}\,|1\rangle\,\|^2 = |\alpha_{00}|^2 + |\alpha_{01}|^2$ und das Ergebnis $c_0 = 1$ mit Wahrscheinlichkeit $\|\alpha_{10}\,|0\rangle + \alpha_{11}\,|1\rangle\,\|^2 = |\alpha_{10}|^2 + |\alpha_{11}|^2$ erhalten. Im z.B. ersten Fall $c_0 = 0$ ist der neue Zustand nach der Messung durch

$$\frac{1}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}\,|0\rangle \otimes \big(\alpha_{00}\,|0\rangle + \alpha_{01}\,|1\rangle\,\big) = \frac{\alpha_{00}}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}\,|00\rangle + \frac{\alpha_{01}}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}\,|01\rangle$$

gegeben.

Ist U_1 eine unitäre Matrix auf $\mathfrak{H}_1$ und U_2 eine unitäre Matrix auf $\mathfrak{H}_2$, so ist

$$(U_1 \otimes U_2)(\psi_1 \otimes \psi_2) = (U_1\psi_1) \otimes (U_2\psi_2)$$

eine unitäre Matrix auf $\mathfrak{H}_1 \otimes \mathfrak{H}_2$ (wir erinnern uns daran, dass eine Matrix durch ihre Wirkung auf die Basisvektoren eindeutig bestimmt ist). Das Tensorprodukt $U_1 \otimes U_2$ der beiden Matrizen ist auch als **Kronecker-Produkt** bekannt — nach Leopold Kronecker (1823–1891). Adjungieren bzw. Invertieren des Kroneckerprodukts erfolgt offensichtlich indem man die entsprechenden Operationen auf die Einzelteile anwendet:

$$(U_1 \otimes U_2)^* = U_1^* \otimes U_2^*, \qquad (U_1 \otimes U_2)^{-1} = U_1^{-1} \otimes U_2^{-1}.$$

Beispiel 8.5 Beschreiben Sie die Wirkung von $H \otimes H$ auf $|0\rangle \otimes |0\rangle$.

Lösung zu 8.5 Eine einfache Rechnung zeigt

$$\begin{aligned}(H \otimes H)\,|0\rangle \otimes |0\rangle &= (H\,|0\rangle) \otimes (H\,|0\rangle) = \frac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big) \otimes \frac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big) \\ &= \frac{1}{2}\big(\,|00\rangle + |01\rangle + |10\rangle + |11\rangle\,\big).\end{aligned}$$

Das Resultat ist also gleichmäßig über alle 4 möglichen Zustände verteilt. ■

Identifizieren wir die Basisvektoren mit

$$|00\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \quad |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \quad |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \quad |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix},$$

so können wir jede unitäre Transformation wieder als Matrix schreiben. Indem wir das letzte Beispiel vervollständigen und die Bilder der drei fehlenden Basisvektoren ausrechnen, erhalten wir zum Beispiel

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

Das Kronecker-Produkt transformiert aber beide Systeme unabhängig voneinander und vermischt sie nicht! Spannend wird es, wenn wir für U eine beliebige unitäre Matrix auf $\mathfrak{H}_1 \otimes \mathfrak{H}_2$ betrachten.

Beispiel 8.6 (SWAP) Eine unitäre Abbildung ist eindeutig durch ihre Wirkung auf die Basisvektoren bestimmt und insbesondere ist eine Umordnung der Basisvektoren unitär. Die Abbildung

$$|00\rangle \mapsto |00\rangle\,, \quad |01\rangle \mapsto |10\rangle\,, \quad |10\rangle \mapsto |01\rangle\,, \quad |11\rangle \mapsto |11\rangle$$

vertauscht beide Qubits und ist als SWAP bekannt. Etwas kompakter können wir die Abbildungsvorschrift als

$$\mathrm{SWAP}\,|a,b\rangle = |b,a\rangle$$

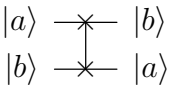
schreiben (wobei wir zur deutlicheren Kennzeichnung Beistriche zwischen die Ziffern der Basisvektoren geschrieben haben). Die zugehörige Matrix ist gegeben durch

$$U_{\mathrm{SWAP}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

und es gilt

$$\mathrm{SWAP}^* = \mathrm{SWAP}^{-1} = \mathrm{SWAP}.$$

In Schaltkreisen wird die SWAP Operation durch



symbolisiert.

Beispiel 8.7 (CNOT) Eine weitere unitäre Abbildung, die einer Umordnung der Basisvektoren entspricht, ist

$$|00\rangle \mapsto |00\rangle\,, \quad |01\rangle \mapsto |01\rangle\,, \quad |10\rangle \mapsto |11\rangle\,, \quad |11\rangle \mapsto |10\rangle$$

und als CNOT (für controlled not, gesteuerte Negation, auch CX) bekannt: Das zweite Qubit wird invertiert, wenn das erste im Zustand $|1\rangle$ ist, und ansonsten unverändert gelassen. Das erste Qubit wird auch als Steuerqubit (control) und das zweite als Zielqubit (target) bezeichnet. Kompakt können wir die Abbildungsvorschrift als

$$\mathrm{CNOT}\,|a,b\rangle = |a, a \oplus b\rangle$$

schreiben ($\oplus$ ist hier als Addition modulo 2 zu verstehen) und die zugehörige Matrix ist

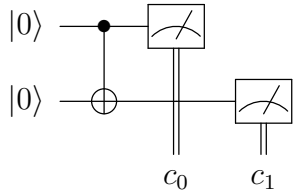
$$U_{\mathrm{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

und es gilt

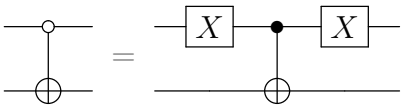
$$\mathrm{CNOT}^* = \mathrm{CNOT}^{-1} = \mathrm{CNOT}.$$

Ein kleiner Schaltkreis, der das Ergebnis des CNOT-Gatters veranschaulicht, sieht

wie folgt aus:



Wenn Sie den Wert der Eingangsqubits von $|0\rangle$ auf $|1\rangle$ ändern wollen, können Sie einfach ein X-Gatter davorsetzen. Wenn das zweite Qubit invertiert werden soll, wenn das erste im Zustand $|0\rangle$ ist, so kann man



verwenden.

Kommen wir nun zu einem weiteren fundamentalen Begriff: Ein Zustand, der als (Tensor-)Produkt zweier Einzelzustände geschrieben werden kann, wird als **unverschränkt** bezeichnet, also zum Beispiel die Zustände

$$|00\rangle = |0\rangle \otimes |0\rangle\,, \quad |0\rangle \otimes \big(\frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\,\big) = \frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|01\rangle\,.$$

In diesem Fall ist jedes der beiden Qubits unabhängig vom anderen in seinem eigenen Zustand. Wenn man also zum Beispiel Messungen an beiden Qubits durchführen würde, so würden sich diese Messungen gegenseitig nicht beeinflussen (das Ergebnis der einen Messung liefert keine Informationen über den Ausgang der anderen Messung).

Umgekehrt kann zum Beispiel der **Bell-Zustand**

$$\frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|11\rangle$$

nicht als Produkt zweier Einzelzustände geschrieben werden und wird deshalb als **verschränkt** bezeichnet.

Angenommen, der Bell-Zustand könnte als Produkt zweier Einzelzustände geschrieben werden, also

$$\begin{aligned}\frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|11\rangle &= (\alpha_0\,|0\rangle + \alpha_1\,|1\rangle) \otimes (\beta_0\,|0\rangle + \beta_1\,|1\rangle) \\ &= \alpha_0\beta_0\,|00\rangle + \alpha_0\beta_1\,|01\rangle + \alpha_1\beta_0\,|10\rangle + \alpha_1\beta_1\,|11\rangle\,.\end{aligned}$$

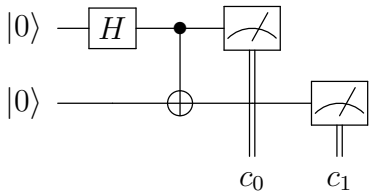
Durch Koeffizientenvergleich folgt z.B. $\alpha_0\beta_1 = 0$. Also $\alpha_0 = 0$ oder $\beta_1 = 0$. Aber der erste Fall ist unmöglich, da ja auch $\frac{1}{\sqrt{2}} = \alpha_0\beta_0$ gelten muss und analog widerspricht der zweite Fall $\frac{1}{\sqrt{2}} = \alpha_1\beta_1$.

Sind die zwei Qubits also im Bell-Zustand, und stellen wir durch eine Messung am ersten Qubit fest, dass es im Zustand $|0\rangle$ ist, so muss eine Messung am zweiten

Qubit ebenfalls $|0\rangle$ ergeben, denn die Wahrscheinlichkeit für den Zustand $|01\rangle$ ist ja Null! Sobald man also das erste Qubit misst, muss eine Messung am zweiten Qubit genau dasselbe Ergebnis liefern!

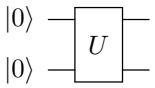
Und das auch, wenn man die beiden Qubits vorher räumlich getrennt hat. Diese (in Einstein's Worten) *spukhafte Fernwirkung* wurde zuerst von Albert Einstein, Boris Podolsky und Nathan Rosen beschrieben, allerdings ursprünglich als *Beweis*, dass die Quantenmechanik so nicht richtig sein kann. Es ist als **EPR-Paradoxon** bekannt.

Durch Anwendung eines einzelnen Gatters auf ein Qubit kann man keinen verschränkten Zustand erzeugen, mit dem CNOT-Gatter ist das aber möglich! Zum Beispiel erzeugt

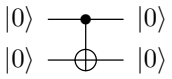


den Bell-Zustand.

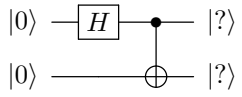
Achtung: Wenn man das Bild eines Quantenschaltkreises



betrachtet, könnte man meinen, dass man links zwei unabhängige Qubits hineinschickt und rechts zwei unabhängige Qubits herauskommen. Dem ist aber nicht so: Während die Notation zwar bedeutet, dass der Eingangszustand $|0\rangle \otimes |0\rangle = |00\rangle$ ist, ist der Ausgangszustand im Allgemeinen verschränkt und kann somit nicht als Produkt zweier Einzelzustände geschrieben werden! Auf der rechten Seite des Schaltkreises wieder zwei Einzelzustände zu schreiben macht also nur Sinn, wenn die Eingabe sicher zu einer unverschränkten Ausgabe führt. Wir können also



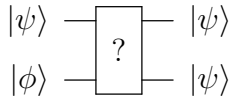
schreiben, aber



macht keinen Sinn, weil das Ergebnis $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ nicht als Produkt von Einzelzuständen geschrieben werden kann. Auch wenn sich unsere Qubits scheinbar auf unabhängigen Bahnen durch den Schaltkreis bewegen, so sind sie doch verbunden! Ziemlich spukhaft, nicht wahr? (Genaugenommen ist die Vorstellung, dass sich Qubits durch Schaltkreise bewegen unangebracht, denn die Qubits bleiben in der Regel an Ort und Stelle und ihr Zustand wird durch äußere Kräfte (z.B. ein Magnetfeld, das für eine bestimmte Zeit eingeschalten wird) verändert.)

Soweit ist ja alles ganz gut gelaufen, aber es stellt sich heraus, dass uns die Quantenmechanik auch neue Grenzen setzt. Dazu wollen wir der Frage nachgehen, ob es möglich ist, den Zustand eines Qubits auf ein anderes zu übertragen? Da ein Quantengatter keine Qubits erzeugen kann, sondern nur den Zustand der vorhandenen Qubits verändern, würden wir ein Quantengatter mit der folgenden Funktion

benötigen:



Es stellt sich heraus, dass das unmöglich ist.

Satz 8.8 (No-Cloning-Theorem) Es ist unmöglich, den Zustand eines beliebigen Qubits auf ein anderes zu kopieren.

Angenommen wir hätten so ein Gatter U, das einen beliebigen Zustand $|\psi\rangle$ eines Qubits zusammen mit einem weiteren Qubit $|\phi\rangle$ entgegennimmt und zwei identische Kopien des ersten Zustands am Ausgang zur Verfügung stellt: $U(|\psi\rangle \otimes |\phi\rangle) = |\psi\rangle \otimes |\psi\rangle$ für alle $|\psi\rangle \in \mathbb{C}^2$ und zumindest ein festes $|\phi\rangle$. Speziell für zwei Zustände $|\psi_0\rangle$, $|\psi_1\rangle$ erhalten wir wegen der Unitarität von U

$$\langle |\psi_0\rangle \otimes |\phi\rangle \, , |\psi_1\rangle \otimes |\phi\rangle \rangle = \langle U(|\psi_0\rangle \otimes |\phi\rangle), U(|\psi_1\rangle \otimes |\phi\rangle) \rangle = \langle |\psi_0\rangle \otimes |\psi_0\rangle \, , |\psi_1\rangle \otimes |\psi_1\rangle \rangle.$$

Nach Definition des Skalarprodukts im Tensorprodukt folgt

$$\langle \psi_0, \psi_1 \rangle \langle \phi, \phi \rangle = \langle \psi_0, \psi_1 \rangle^2$$

und da $\langle \phi, \phi \rangle = 1$, muss entweder $\langle \psi_0, \psi_1 \rangle = 1$ oder $\langle \psi_0, \psi_1 \rangle = 0$ gelten. Ist U also in der Lage, ψ_0 zu kopieren, so kann es einen weiteren Zustand ψ_1 nur dann kopieren, wenn dieser entweder parallel ist (also den gleichen Zustand beschreibt) oder orthogonal ist. Für alle Zustände dazwischen ist ein Kopieren unmöglich!

Dieses Theorem hat weitreichende Konsequenzen: Zunächst sind Qubits anfälliger für (in der Praxis unvermeidliche) Störungen von Außen (man spricht von **Dekoheränz**), da sie im Gegensatz zu klassischen Bits nicht nur zwei voneinander wohl getrennte Zustände einnehmen können. Deshalb benötigt man Fehlerkorrektur. Klassische fehlerkorrigierende Codes beruhen aber auf dem Kopieren von Information und sind daher für Quantencomputer ungeeignet, man muss sich also auch hier etwas Neues einfallen lassen. Außerdem bedeutet das, dass man einen quantenmechanischen Informationskanal nicht unbemerkt belauschen kann. Durch das Belauschen (=Messen) wird ja der Zustand verändert und das No-Cloning-Theorem besagt, dass man den Originalzustand messen muss, da man keine Kopie davon machen kann. Das haben wir bereits beim BB84 Protokoll verwendet.

Die Erweiterung auf n Qubits ist nun klar und ein solches System wird durch die 2^n Basisvektoren

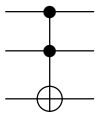
$$|0\rangle \otimes \cdots \otimes |0\rangle = |0 \cdots 0\rangle \, , \quad \ldots , \quad |1\rangle \otimes \cdots \otimes |1\rangle = |1 \cdots 1\rangle$$

beschrieben.

Mit dem bisher Gelernten sind wir bereits in der Lage unseren eigenen Quantencomputer-Simulator zu schreiben. Alles, was wir in einer Programmiersprache unserer Wahl implementieren müssen, sind Klassen für komplexe Zahlen, Vektoren und Matrizen inklusive der zugehörigen

Rechenoperationen (Skalarprodukt, Matrixmultiplikation). Schon ist unser eigener Quantencomputer fertig. Das erste Problem ist der Speicher: Wenn wir für eine komplexe Zahl (Real- und Imaginärteil) $2 \cdot 4 = 8$ Bytes benötigen (hier könnte man ev. noch den Exponenten einsparen, da die Koeffizienten aufgrund der Normierung immer kleiner als 1 sind), dann brauchen wir für n Qubits also 2^{n+3} Bytes. Nur 30 Qubits schlagen also schon mit fast 16GB RAM zu Buche und für jedes weitere Qubit muss der Speicher verdoppelt werden! Das zweite Problem ist die Anzahl der Rechenoperationen um die Matrixmultiplikationen durchzuführen benötigen wir (in der effizientesten Variante) $O(n4^n)$ Operationen. Deshalb ist die Simulation eines Quantencomputers auf einem klassischen Rechner zwar prinzipiell möglich, aber eben nicht effektiv. Bei einem Rekord aus 2018 waren es 60 Qubits die die Zahl 961307 mit dem Shor-Algorithmus auf einem Supercomputer (mit 5184 Prozessorkernen und knapp 40TB Speicher) in 8 Stunden faktorisieren konnten [DHH19].

Am Ende erwähnen wir noch, dass das CNOT-Gatter erweitert werden kann, indem man mehrere Steuerqubits verwendet. Der Fall von zwei Steuerqubits ist als **Toffoli-Gatter** (auch CCNOT oder CCX)



bekannt. Die Wirkung ist dadurch definiert, dass das X-Gatter nur dann auf das Zielqubit angewendet wird, falls beide Steuerqubits eins sind. Also

$$|11\rangle \otimes |\psi\rangle \mapsto |11\rangle \otimes |U_X \psi\rangle$$

und

$$|00\rangle \otimes |\psi\rangle \mapsto |00\rangle \otimes |\psi\rangle\,,\ |01\rangle \otimes |\psi\rangle \mapsto |01\rangle \otimes |\psi\rangle\,,\ |10\rangle \otimes |\psi\rangle \mapsto |10\rangle \otimes |\psi\rangle\,.$$

Etwas kompakter können wir die Abbildungsvorschrift als

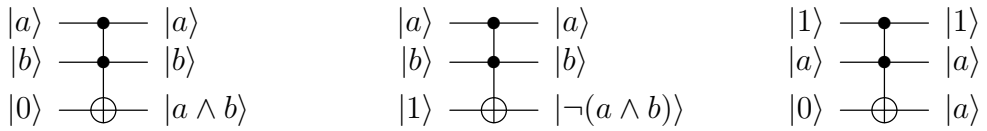
$$\mathrm{TOF}\,|a,b,c\rangle = |a,b,(a \wedge b) \oplus c\rangle$$

schreiben bzw. als Matrix

$$U_{\mathrm{TOF}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Wiederum gilt $\mathrm{TOF}^* = \mathrm{TOF}^{-1} = \mathrm{TOF}$.

Mit dem Toffoli-Gatter kann man insbesondere reversible Varianten von AND, NAND und eines Fan-Out-Gatters realisieren:

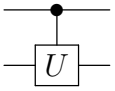


Da man mit diesen Verknüpfungen beliebige klassische Schaltkreise aufbauen kann folgt:

Satz 8.9 Ein Quantencomputer kann beliebige klassische Schaltkreise realisieren und somit auch alle Berechnungen die auf einem klassischen Computer möglich sind durchführen.

Allerdings sehen wir, dass aufgrund der Reversibilität in der Regel mehr Qubits als klassische Bits notwendig sind. Diese zusätzlichen Qubits werden auch als **Ancilla-Qubits** (oder Hilfs-Qubits) bezeichnet.

Man kann das X-Gatter im CNOT-Gatter auch durch ein anderes Gatter ersetzen und



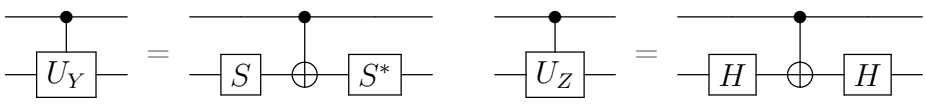
durch

$$|0\rangle \otimes |\psi\rangle \mapsto |0\rangle \otimes |\psi\rangle\,, \quad |1\rangle \otimes |\psi\rangle \mapsto |1\rangle \otimes |U\psi\rangle$$

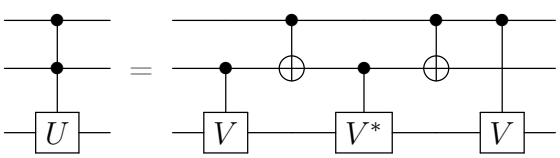
definieren. Die zugehörige Matrix ist

$$U_{\mathrm{CU}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{11} & U_{12} \\ 0 & 0 & U_{21} & U_{22} \end{pmatrix}.$$

Zum Beispiel kann man gesteuerte Pauli-Gatter aus dem CNOT-Gatter erzeugen, indem man $U_Y = U_S U_X U_S^*$ bzw. $U_Z = H U_X H$ verwendet:



Analog werden U-Gatter mit mehreren Steuerqubits definiert. Diesen Fall kann man übrigens auf den einfachen Fall zurückführen, indem man



mit $V^2 = U$ verwendet. Basierend auf dieser Idee kann man z.B. das Toffoli-Gatter mit unseren bisherigen Gattern via

$$\sqrt{U_X} = HU_SH = \begin{pmatrix} \frac{1+\mathrm{i}}{2} & \frac{1-\mathrm{i}}{2} \\ \frac{1-\mathrm{i}}{2} & \frac{1+\mathrm{i}}{2} \end{pmatrix}.$$

realisieren.

Falls Sie sich fragen wie man Funktionen, wie z.B. $V = \sqrt{U}$, einer unitären Matrix berechnet (so, dass $V^2 = U$ gilt), dann müssen Sie sich daran erinnern, dass man jede unitäre Matrix mithilfe einer Orthogonalbasis aus Eigenfunktionen auf Diagonalform bringen kann (wobei die Einträge auf der Diagonale genau die Eigenwerte sind, die alle Betrag 1 haben müssen). Für eine Diagonalmatrix erhält man die Wurzel aber einfach indem man die Wurzel aus jedem Eintrag zieht. Da die Wurzel aus einer Zahl vom Betrag 1 wieder Betrag 1 hat ($\sqrt{\mathrm{e}^{\mathrm{i}\varphi}} = \mathrm{e}^{\mathrm{i}\varphi/2}$), ist die neue Matrix wieder unitär.

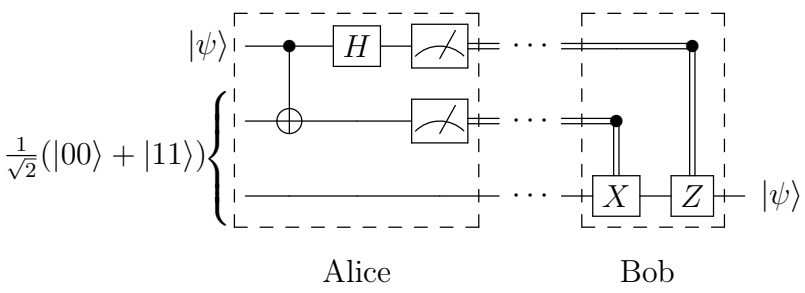
Das ist aber nur die Spitze des Eisberges, das CNOT-Gatter hat die universelle Eigenschaft, dass ein beliebiges Gatter für n-Qubits durch eine Zusammensetzung aus Gattern für die einzelnen Qubits und CNOT-Gattern erhalten werden kann (vgl. auch [Bar+95]).

8.3.1 Anwendung: Quantenteleportation

Als kleine Anwendung des Bell-Zustands wollen wir nun zeigen, wie es möglich ist, den Zustand eines Quantenbits zu *teleportieren*. Besitzen Alice und Bob je ein von zwei verschränkten Qubits, so kann Alice durch das Übertragen zweier klassischer Bits den Zustand eines beliebigen Qubits übertragen.

Das erscheint auf den ersten Blick wenig spektakulär, da man als Voraussetzung für die Teleportation des Zustands ja zunächst das eine Qubit eines verschränkten Zustands übertragen muss. Da hätte man ja gleich den ursprünglichen Zustand übertragen können. Der Vorteil hier ist, dass man das verschränkte Qubit schon vorher übertragen kann und danach keinen Quantenkanal mehr benötigt. Die beiden verschränkten Qubits könnten auch von einer unabhängigen Stelle an Alice und Bob verteilt werden.

Beispiel 8.10 (Quantenteleportation) Mit dem folgenden Schaltkreis ist es möglich, den Zustand $|\psi\rangle$ zu übertragen:



Alice erzeugt einen verschränkten Bell-Zustand. Ein Qubit davon wird mit $|\psi\rangle$ verknüpft und danach werden beide vermessen. Die beiden klassischen Ergebnisbits werden zusammen mit dem anderen der beiden verschränkten Qubits an

Bob übertragen. Abhängig von den übertragenen klassischen Bits wendet Bob noch U_X, U_Z auf das erhaltene Qubit an. Zeigen Sie, dass das Ergebnis $|\psi\rangle$ ist.

Lösung zu 8.10 Setzen wir $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$, so ist der Zustand nach CNOT und dem Hadamard-Gatter gleich

$$\begin{aligned}
&\frac{\alpha_0}{2}\big(|000\rangle + |011\rangle + |100\rangle + |111\rangle\big) + \frac{\alpha_1}{2}\big(|010\rangle + |001\rangle + |110\rangle + |101\rangle\big) \\
&\quad = \frac{1}{2}\big(|00\rangle \otimes (\alpha_0 |0\rangle + \alpha_1 |1\rangle) + |01\rangle \otimes (\alpha_0 |1\rangle + \alpha_1 |0\rangle) \\
&\qquad + |10\rangle \otimes (\alpha_0 |0\rangle - \alpha_1 |1\rangle) + |11\rangle \otimes (\alpha_0 |1\rangle - \alpha_1 |0\rangle)\big).
\end{aligned}$$

Wird also $|00\rangle$ gemessen, so hat Bob $\alpha_0 |0\rangle + \alpha_1 |1\rangle = |\psi\rangle$ und es ist nichts zu tun. Wird $|01\rangle$ gemessen, so hat Bob $\alpha_0 |1\rangle + \alpha_1 |0\rangle = U_X |\psi\rangle$ und Bob muss noch U_X anwenden, um $|\psi\rangle$ zu erhalten. Etc. ■

8.3.2 Ausblick: Fehlererkennung-/korrektur

Die Idee der Fehlererkennung bzw. Fehlerkorrektur ist wie folgt: Möchte man klassisch einen Fehler erkennen, so verwendet man zwei Bits die im gleichen Ausgangszusand starten und die gleichen Operationen durchlaufen. Sind irgendwann beide verschieden, so ist irgendwo ein Fehler passiert.

Analog startet man mit zwei Qubits im Zustand $|00\rangle$ und wenn beide die gleichen Gatter durchlaufen, dann sollte im Endzustand

$$|\psi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle$$

mit $\alpha_{01} = \alpha_{10} = 0$ sein. Um das zu überprüfen nehmen wir ein Hilfsqubit im Zustand $|0\rangle$ und führen folgende Operation aus: an:

$$\mathrm{CNOT}_{2,3} \circ \mathrm{CNOT}_{1,3} |\psi\rangle \otimes |0\rangle = \alpha_{00} |000\rangle + \alpha_{01} |101\rangle + \alpha_{10} |111\rangle + \alpha_{11} |110\rangle ,$$

wobei $\mathrm{CNOT}_{j,k}$ bedeutet, dass das CNOT-Gatter zwischen dem $j$ten (*control*) und dem $k$ten (*target*) Qubit anzuwenden ist.

Nun messen wir das dritte Qubit. Ist das Ergebnis 0, so ist es unwahrscheinlich, dass ein Fehler aufgetreten ist und das System ist im Zustand

$$\left(\frac{\alpha_{00}}{(|\alpha_{00}|^2 + |\alpha_{11}|^2)^{1/2}} |00\rangle + \frac{\alpha_{11}}{(|\alpha_{00}|^2 + |\alpha_{11}|^2)^{1/2}} |11\rangle\right) \otimes |0\rangle$$

mit dem wir weiterrechnen können. Ist das Ergebnis 1, so ist ein Fehler aufgetreten und es muss abgebrochen werden.

Möchte man den Fehler korrigieren, so muss man drei Qubits zusammenfassen und benötigt zwei Hilfsqubits, die man misst und anhand des Ergebnis der Messung den Zustand korrigiert [Won22].

8.4 Quantenalgorithmen

Wir haben nun ein grundlegendes Verständnis, wie man einen Quantencomputer programmieren kann, wir haben uns aber noch nicht damit auseinandergesetzt, was die praktischen Vorteile eines Quantencomputers sind. Die liegen vor allem darin, dass es eine Reihe von Problemen gibt, die auf einem Quantencomputer wesentlich effizienter gelöst werden können als auf einem klassischen. Zum Beispiel kann die diskrete Fouriertransformation auf einem Quantencomputer mit n Qubits in $O(n^2)$ Schritten berechnet werden während ein klassischer Computer mithilfe der schnellen Fouriertansformation (FFT) $O(n2^n)$ Schritte benötigt. Insbesondere für die Kryptographie von Bedeutung ist die Tatsache, dass es effektive Quantenalgorithmen für die Suche (Grover-Algorithmus) und für die Primfaktorzerlegung bzw. das DLP (Shor-Algorithmus) gibt.

8.4.1 Quantenorakel

Bei einem Quantenalgorithmus möchte man in der Regel ein klassisches Objekt mithilfe eines Quantencomputers untersuchen. Das erste Problem mit dem man dabei konfrontiert ist, ist die Frage wie man dem Quantencomputer die Informationen über das klassische Objekt zukommen lässt.

Beim Grover-Algorithmus hat man z.B. eine Datenbank mit (maximal) N Datensätzen die durchsucht werden soll. In unserem Fall entsprechen die Datensätze z.B. den 2^{128} möglichen Schlüssel beim AES. Wir gehen davon aus, dass wir ein Geheim-Klartextpaar (x_0, y_0) gegeben haben und wir suchen einen Schlüssel k_0 mit der Eigenschaft $\mathrm{AES}_{k_0}(x_0) = y_0$. Auf einem klassischen Computer würde wir die Funktion $k \mapsto \mathrm{AES}_k(x_0)$ implementieren und mit einem kleinen Test koppeln:

$$f : \mathbb{Z}_2^{128} \to \mathbb{Z}_2, \qquad k \mapsto f(k) = \begin{cases} 1, & \mathrm{AES}_{k_0}(x_0) = y_0, \\ 0, & \mathrm{AES}_{k_0}(x_0) \neq y_0. \end{cases}$$

Da x_0, y_0 konstant sind, haben wir die Abhängigkeit von f von diesen Variablen nicht explizit angeführt. Die Schlüsselsuche erfolgt nun indem wir f der Reihe nach für alle Schlüssel k aufrufen, bis wir einen passenden gefunden haben.

Auf einem Quantencomputer sieht die Situation wie folgt aus: Zuerst müssen wir $\mathrm{AES}_k(x_0)$ und damit dann f implementieren. Die Funktion f kann mit einem klassichen Schaltkreis realisiert werden und damit auch als reversibel Variante (Satz 8.9). Dazu identifizieren wir die $N = 2^n$ möglichen Schlüssel mit den N möglichen Basiszuständen eines Registers aus n Qubits. In diesem Zusammenhang ist es praktisch die Basiszustände durchzunummerieren:

$$|0\rangle, \ldots, |N-1\rangle .$$

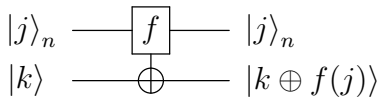
Wir wählen also $|j\rangle = |j_0 j_2 \cdots j_{n-1}\rangle$ wobei $j_{n-1} j_{n-1} \cdots j_0$ die Dualdarstellung von $j = j_0 + 2j_1 + \ldots + 2^{n-1} j_{n-1}$ ist. Z.B. für zwei Qubits schreiben wir

$$|0\rangle = |00\rangle , \quad |1\rangle = |01\rangle , \quad |2\rangle = |10\rangle , \quad |3\rangle = |11\rangle .$$

Wenn wir dabei betonen möchten aus wie vielen Qubits das Register besteht, schreiben wir das als Index dazu: $|0\rangle_2 = |00\rangle$, etc. Dann nehmen wir noch ein weiteres Hilfsqubit und implementieren f als **Quantenorakel**

$$U_f \, |j\rangle_n \otimes |k\rangle_1 = |j\rangle_n \otimes |k \oplus f(j)\rangle_1 \, .$$

Hier ist $\oplus$ wieder als Addition modulo 2 zu verstehen und da U_f durch eine Permutation der Basiszustände gegeben ist, entspricht es einer unitären Transformation. Als Schaltkreis:



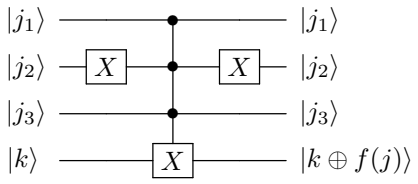
Wie wir bei Satz 8.9 gesehen haben, brauchen wir für die reversible Realisierung klassischer Schaltkreise im Allgemeinen weitere Qubits (sogenannte **Ancilla-Qubits**), deren Zustand am Ende nicht benötigt werden (vgl. auch Aufgabe 10). Das Quantenorakel wird also im Allgemeinen folgende Struktur haben:

$$U_f \, |j\rangle_n \otimes |k\rangle_1 \otimes |l\rangle_n = |j\rangle_m \otimes |k \oplus f(j)\rangle_1 \otimes |\tilde{l}\rangle_m.$$

Ein Quantencomputer wird daher, abhängig von der Komplexität des Quantenorakels, wesentlich mehr Qubits benötigen als nur die für den Algorithmus notwendigen. Die Hilfsqubits werden in der Regel nicht extra angeführt.

Es mag auf den ersten Blick sinnlos erscheinen, den ganzen AES auf unserem Quantencomputer mühsamst von Grund auf zu implementieren, wenn wir den AES ja schon (effektiv und schnell) auf unserem klassischen Computer implementiert haben. Der entscheidende Unterschied ist, dass während wir f immer nur mit einem Schlüssel aufrufen können, können wir U_f auch mit einer Überlagerung von beliebig vielen Schlüssel aufrufen. Und nur dann kann unser Quantencomputer seine Stärke ausspielen.

Oft findet man für das Quantenorakel einen kleinen Schaltreis wie z.B.



der das Quantenorakel im Falle $n = 3$ mit gesuchtem Datensatz $5 = (101)_2$ implementiert (vg. auch Aufgabe 15). Das ist aber irreführend, da die Implementierung in dieser Form bereits die Kenntnis des gesuchten Datensatz voraussetzt. Diese Form ist nur als Test, ob der eigene Algorithmus auch funktioniert, nützlich.

Ähnlich verhält es sich beim Shor-Algorithmus, wo die Periode einer Funktion $f : \mathbb{Z}_N \to \mathbb{Z}_M$ gefunden werden muss. Wiederum muss diese als Quantenorakel

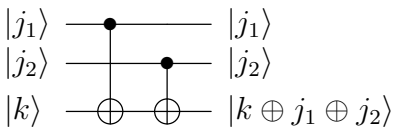
$$U_f \, |j\rangle_n \otimes |k\rangle_m = |j\rangle_n \otimes |k \oplus f(j)\rangle_m$$

implementiert werden.

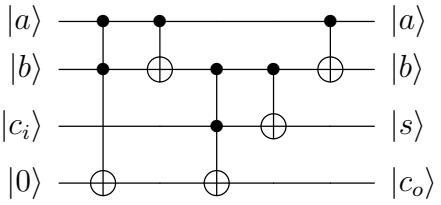
Diese Implementierung kann sehr aufwendig sein; unter Umständen sogar aufwendiger als der Algorithmus selbst! Um uns das klar zu machen, überlegen wir uns wie die Funktion $f : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2$, $(j_1, j_2) \mapsto j_1 \oplus j_2$ implementiert werden kann. Wir brauchen also ein Register aus drei Qubits und es muss

$$U_f \left|j_1, j_2, k\right\rangle = \left|j_1, j_2, k \oplus j_1 \oplus j_2\right\rangle$$

gelten. Betrachten wir dazu zunächst die einfachere Operation $\left|j_1, k\right\rangle \mapsto \left|j_1, k \oplus j_1\right\rangle$, dann entspricht das genau einem CNOT und die ursprünglich gewünschte Operation erhalten wir durch Komposition:



Ein Volladdierer ist z.B. durch folgenden Schaltkreis gegeben:



Dabei sind a, b die zu addierenden Bits, c_i der Übertrag aus einem vorherigen Schritt, s die Summe und c_o der Übertrag. Weitere Schaltkreise für klassische Rechenopertaionen sind in [Sch16] zu finden.

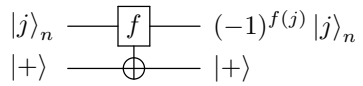
8.4.2 Grover-Suche

Der **Grover-Algorithmus** [Gro96] findet einen bestimmten Datensatz unter 2^n gegebenen unstrukturierten (also nicht sortierten) Datensätzen. Wir identifizieren die 2^n möglichen Datensätze mit den 2^n möglichen Basiszuständen eines Registers aus n Qubits und wir gehen davon aus, dass wir den gewünschten Zustand mithilfe einer Logikfunktion $f : \mathbb{Z}^n \to \mathbb{Z}_2$ identifizieren können, die 1 für den gesuchten Datensatz und 0 sonst liefert. Weiters gehen wir davon aus, dass wir f bereits als **Phasenorakel** in der Form

$$U_f \left|a\right\rangle_n = (-1)^{f(a)} \left|a\right\rangle_n$$

implementiert haben. Der gesuchten Basiszustand $\left|a_0 a_1 \cdots a_n\right\rangle$ wird also von U_f auf $U_f \left|a_0 a_1 \cdots a_n\right\rangle = -\left|a_0 a_1 \cdots a_n\right\rangle$ abgebildet und alle anderen Basiszustände bleiben unverändert.

Das weicht von der vorherigen Form $V_f \left|a\right\rangle_n \otimes \left|b\right\rangle = \left|a\right\rangle_n \left|b \oplus f(a)\right\rangle$ ab. Man kann aber leicht U_f aus V_f erhalten indem man $V_f(\left|a\right\rangle_n \otimes H\left|1\right\rangle) = (-1)^{f(a)}\left|a\right\rangle_n \otimes H\left|1\right\rangle$ verwendet:



Umgekehrt kann man $V_f(\left|a\right\rangle_n \otimes H\left|0\right\rangle) = \left|a\right\rangle_n \otimes H\left|0\right\rangle$ verwenden und erhält V_f aus einer gesteuerten Variante von U_f plus zwei Hadamard-Gattern.

Wir beginnen mit dem einfachsten Fall von $n = 2$ Qubits, um die Operationen zu veranschaulichen. Erinnern wir uns daran, dass wir, wenn wir das Hadamard-Gatter auf alle Qubits anwenden, einen gleichverteilten Zustand

$$\left|\psi_0\right\rangle = H \otimes H\left|00\right\rangle = \frac{1}{\sqrt{4}}\big(\left|00\right\rangle + \left|01\right\rangle + \left|10\right\rangle + \left|11\right\rangle\big)$$

erhalten, in dem alle Basiszustände die gleiche Wahrscheinlichkeit $\frac{1}{4}$ haben. Das entspricht unserer Ausgangssituation, bei der wir noch keinerlei Information darüber haben, wo der gesuchte Zustand ist. Für unser Beispiel sei $\left|10\right\rangle$ dieser gesuchte Zustand.

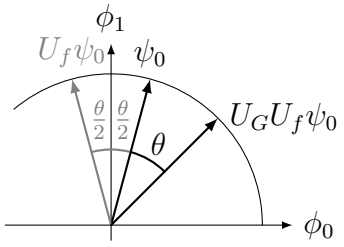
Die Idee ist es nun, den Ausgangszustand $\left|\psi_0\right\rangle$ so zu transformieren, dass die Wahrscheinlichkeit, das System im gesuchten Zustand zu finden, steigt (die Wahrscheinlichkeiten für die anderen Zustände müssen demnach sinken).

Zuerst wenden wir das Orakel U_f an,

$$U_f\left|\psi_0\right\rangle = \frac{1}{\sqrt{4}}\big(\left|00\right\rangle + \left|01\right\rangle - \left|10\right\rangle + \left|11\right\rangle\big),$$

um den gesuchten Zustand in die andere Richtung zu klappen. Unser Zustand kennt also bereits die Lösung, wir können diese aber durch eine Messung der einzelnen Qubits (noch) nicht sichtbar machen, da die Quadrate der einzelnen Amplituden unverändert sind. Unser Ziel muss es also sein durch weitere Transformationen das geänderte Vorzeichen in eine veränderte Amplitude zu verwandeln

Geometrisch entspricht die Anwendung von U_f einer Spiegelung an der zum gesuchten Zustand normalen Hyperebene. Man kann es sich auch leicht in 2 Dimensionen veranschaulichen. Nennen wir unseren gesuchten Zustand $\left|\phi_0\right\rangle = (0, 0, 1, 0)$ und sei $\left|\phi_1\right\rangle = \frac{1}{\sqrt{3}}(1, 1, 0, 1)$ der dazu orthogonale Zustand, sodass $\left|\psi_0\right\rangle = \frac{1}{2}\left|\phi_0\right\rangle + \frac{\sqrt{3}}{2}\left|\phi_1\right\rangle$ gilt. Im von diesen beiden Vektoren aufgespannten Unterraum entspricht U_f also der Spiegelung an der zweiten Achse. Und jetzt kommt der Trick: Wir spiegeln nochmals, diesmal aber an der Geraden, die von $\left|\psi_0\right\rangle$ aufgespannt wird. Dadurch wird unser Vektor wieder zurück in den ersten Quadranten gespiegelt und ist nun näher an den gesuchten Vektor $\left|\phi_0\right\rangle$ gedreht worden:



Der Endvektor $U_G U_f |\psi_0\rangle$ ist also um den Winkel θ in Richtung von $|\phi_0\rangle$ gedreht worden, wobei $\frac{\theta}{2}$ der Winkel zwischen $|\phi_1\rangle$ und $|\psi_0\rangle$ ist ($\cos(\frac{\theta}{2}) = \langle\phi_1, \psi_0\rangle$). In unserem Fall ist der Winkel $\theta = \frac{\pi}{3}$ und der Winkel des Endzustands (von $|\phi_1\rangle$ aus gerechnet) ist $\frac{\pi}{6} + \frac{\pi}{3} = \frac{\pi}{2}$. Wir sind also bei dem gesuchten Zustand $|\phi_0\rangle$ angekommen und brauchen nur noch alle Qubits zu messen um herauszufinden, wo wir gelandet sind.

Im allgemeinen Fall mit n Qubits müssen wir diese Operation mehrmals ausführen, um möglichst nahe an $|\phi_0\rangle$ zu kommen. Schreiben wir wieder

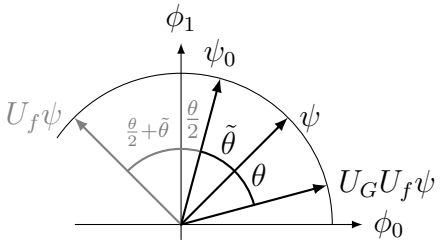
$$|\psi_0\rangle = \sin(\frac{\theta}{2})\,|\phi_0\rangle + \cos(\frac{\theta}{2})\,|\phi_1\rangle\,,$$

wobei $|\phi_1\rangle$ die Orthogonalkomponente von $|\psi_0\rangle$ bezüglich $|\phi_0\rangle$ ist. Haben wir den Vektor

$$|\psi\rangle = \sin(\frac{\theta}{2} + \tilde{\theta})\,|\phi_0\rangle + \cos(\frac{\theta}{2} + \tilde{\theta})\,|\phi_1\rangle\,,$$

so wird dieser durch Anwendung von $U_G U_f$ um den Winkel θ weitergedreht:

$$U_G U_f\,|\psi\rangle = \sin(\frac{\theta}{2} + \tilde{\theta} + \theta)\,|\phi_0\rangle + \cos(\frac{\theta}{2} + \tilde{\theta} + \theta)\,|\phi_1\rangle\,.$$

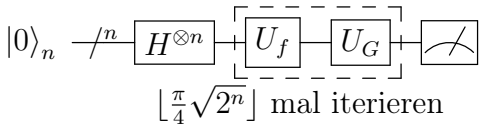


Nach k Iterationen haben wir also

$$(U_G U_f)^k\,|\psi_0\rangle = \sin(\frac{2k+1}{2}\theta)\,|\phi_0\rangle + \cos(\frac{2k+1}{2}\theta)\,|\phi_1\rangle$$

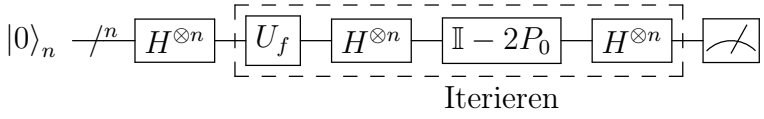
und nach $\lfloor\frac{\pi}{2\theta}\rfloor$ Schritten sind wir so nahe wie möglich bei $|\phi_0\rangle$ (wenn wir weiter drehen, so bewegen wir uns wieder weg von $|\phi_0\rangle$). Den Winkel θ erhalten wir leicht aus $\sin(\frac{\theta}{2}) = \langle\phi_0, \psi_0\rangle = \frac{1}{\sqrt{N}}$, also $\theta = 2\arcsin(1/\sqrt{N})$. Für großes N können wir

$\theta \approx 2/\sqrt{N}$ setzten (Taylorreihe: $\arcsin(x) = x + O(x^3)$) und sollten also ca. $\lfloor \frac{\pi}{4}\sqrt{N} \rfloor$ mal iterieren:

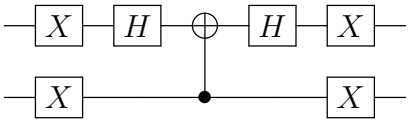


Das $/^n$ im obigen Schaltkreis signalisiert, dass es sich um n Leitungen handelt.

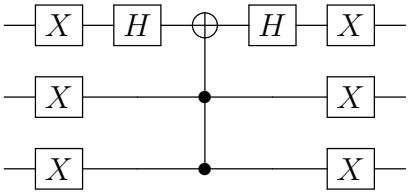
Es bleibt noch die Frage, wie die Spiegelung U_G zu implementieren ist. Eine Spiegelung um eine Ebene ist als Householder-Transformation bekannt und kann wie folgt erhalten werden: Es sei $P = |\psi_0\rangle\langle\psi_0|$ die orthogonale Projektion auf $|\psi_0\rangle$. Dann ist die Orthogonalzerlegung eines beliebigen Vektors $|\psi\rangle$ gegeben durch $|\psi\rangle = P|\psi\rangle + (\mathbb{I} - P)|\psi\rangle$ und die Spiegelung ändert das Vorzeichen der Orthogonalkomponente: $U_G|\psi\rangle = P|\psi\rangle - (\mathbb{I} - P)|\psi\rangle = (2P - \mathbb{I})|\psi\rangle$. Verwenden wir noch, dass $H^{\otimes n}|0\rangle_n = |\psi_0\rangle$, so können wir noch einen Basiswechsel machen: $U_G = H^{\otimes n}(2P_0 - \mathbb{I})H^{\otimes n}$ mit P_0 der Projektion auf $|0\rangle_n$.



Hier haben wir noch U_G durch $-U_G$ ersetzt, da ein Gesamtvorzeichen ja keine Rolle spielt. Die Operation $\mathbb{I} - 2P_0$ entspricht einer Diagonalmatrix mit -1 in der obersten Ecke und alle anderen Einträge sind $+1$. Das entspricht einem gesteuerten Gatter mit $-U_Z$ als Ziel und die restlichen $n-1$ Qubits als Steuerqubits. Also für 2 Qubits



und für 3 Qubits



etc.

Der Algorithmus funktioniert übrigens unverändert, wenn f mehr als einen Zustand markiert. In diesem Fall ist ϕ_0 die Summe über die Basisvektoren mit $f(j) = 1$ und ϕ_1 die Summe über die Basisvektoren mit $f(j) = 0$ (entsprechend normiert). Der Startwinkel ist in diesem Fall $\theta = 2\arcsin(k/\sqrt{N})$, wobei k die Anzahl der Basisvektoren mit $f(j) = 1$ ist und die Messung am Ende liefert (mit hoher Wahrscheinlichkeit) einen dieser Zustände.

Auf der Webseite [QISKIT] können Sie übrigens selbst Quantenalgorithmen ausprobieren. Dort finden Sie auch eine Implementierung des Grover-Algorithmus für zwei Qubits. Mehr zum Thema finden Sie zum Beispiel in [Hom15; NC10;

Sch16]. Man kann zeigen [Ben+97], dass die Ordnung des Grover-Algorithmus nicht verbessert werden kann. Also sind auch einem Quantencomputer Grenzen gesetzt.

8.4.3 Quanten-Fouriertransformation

Ein zentrale Operation auf einem Register aus n Qubits ist die sogenannte **Quanten-Fouriertransformation**. Um sie zu beschreiben sei

$$\omega = \mathrm{e}^{\frac{2\pi \mathrm{i}}{N}} = \cos(\frac{2\pi}{N}) + \mathrm{i}\sin(\frac{2\pi}{N})$$

die N-te Einheitswurzel. Wir benötigen, dass

$$\sum_{j=0}^{N-1} \omega^{jk} = \begin{cases} N, & k \text{ ist Vielfaches von } N, \\ 0, & \text{sonst}, \end{cases}$$

gilt.

Warum? — Falls $k = lN$ ein Vielfaches von N ist, so gilt $\omega^k = (\omega^N)^l = 1^l = 1$, also auch $\omega^{jk} = (\omega^k)^j = 1$ und somit ist $\sum_{j=0}^{N-1} \omega^{jk} = \sum_{j=0}^{N-1} 1 = N$. Anderenfalls ist $\omega^k \neq 1$ und aus der Formel für die Teilsummen der geometrischen Reihe erhalten wir

$$\sum_{j=0}^{N-1} \omega^{jk} = \frac{1-\omega^{kN}}{1-\omega^k} = 0,$$

da $\omega^{kN} = (\omega^N)^k = 1^k = 1$.

Dann lautet die zugehörige Matrix

$$U = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{N-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \cdots & \omega^{(N-1)(N-1)} \end{pmatrix}$$

(also $(U)_{jk} = \frac{1}{\sqrt{N}} \omega^{(j-1)(k-1)}$) und man kann überprüfen, dass U unitär in $\mathbb{C}^N$ ist.

Warum? — Wir müssen $U^*U = \mathbb{I}_n$ zeigen. Dazu berechnen wir ($\overline{\omega} = \omega^{-1}$)

$$(U^*U)_{jk} = \sum_{l=1}^{N} (U^*)_{jl}(U)_{lk} = \frac{1}{N} \sum_{l=1}^{N} \omega^{-(j-1)(l-1)} \omega^{(l-1)(k-1)} = \frac{1}{N} \sum_{l=0}^{N-1} \omega^{(k-j)l}.$$

Um die Summe zu berechnen müssen wir zwei Fälle unterscheiden: Im Fall $j = k$ gilt $\omega^{(k-j)l} = \omega^0 = 1$ und im Fall $j \neq k$ gilt $\omega^{(k-j)l} \neq 1$. Die Behauptung folgt also aus obiger Formel für die Einheitswurzel.

Im Fall von n Qubits wählen wir $N = 2^n$ und bezeichnen wie zuvor mit

$$|0\rangle, \ldots, |N-1\rangle$$

die N Basiszustände. Mit dieser Notation können wir nun die Quanten-Fouriertransformation wie folgt definieren:

$$\mathrm{QFT}_n |k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega_n^{jk} |j\rangle , \qquad \omega_n = \mathrm{e}^{\frac{2\pi \mathrm{i}}{2^n}}.$$

Die erste Frage, die man sich nun stellen muss ist, wie wir diese Transformation mit den bisherigen Gattern realisieren können.

Im Fall eines Qubits erhalten wir wegen $\omega_1 = -1$

$$|k_0\rangle \; \text{—}\boxed{H}\text{—} \; \tfrac{1}{\sqrt{2}}(|0\rangle + \omega_1^{k_0} |1\rangle)$$

also $\mathrm{QFT}_1 = H$.

Im Fall von zwei Qubits beginnen wir mit der Beobachtung (da $\omega_n^2 = \omega_{n-1}$):

$$\begin{aligned}\sum_{j=0}^{3} \omega_2^{jk} |j\rangle &= \sum_{j_0\in\{0,1\}} \sum_{j_1\in\{0,1\}} \omega_2^{(j_0+2j_1)k} |j_1 j_0\rangle = \sum_{j_0\in\{0,1\}} \omega_2^{j_0 k} \sum_{j_1\in\{0,1\}} \omega_1^{j_1 k} |j_1\rangle \otimes |j_0\rangle \\ &= \sum_{j_0\in\{0,1\}} \omega_2^{j_0 k} (|0\rangle + \omega_1^k |1\rangle) \otimes |j_0\rangle = (|0\rangle + \omega_1^k |1\rangle) \otimes (|0\rangle + \omega_2^k |1\rangle).\end{aligned}$$

Wegen $\omega_1^k = \omega_1^{k_0+2k_1} = \omega_1^{k_0}$ und $\omega_2^k = \omega_2^{k_0+2k_1} = \omega_2^{k_0}\omega_1^{k_1}$ erhalten wir die Darstellung

$$\begin{aligned}\mathrm{QFT}_2 |k\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + \omega_1^k |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + \omega_2^k |1\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle + \omega_1^{k_0} |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + \omega_1^{k_1}\omega_2^{k_0} |1\rangle)\end{aligned}$$

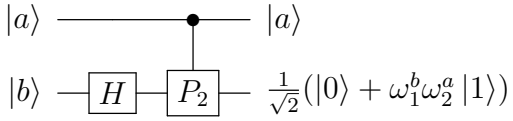
und daraus erkennen wir, dass wir für die Muliplikation mit ω_2 das Phasengatter $P_n = P(\frac{2\pi}{2^n})$ mit

$$P_n |0\rangle = |0\rangle , \qquad P_n |1\rangle = \omega_n |1\rangle .$$

benötigen. Und um die Multiplikation mit ω_n^a zu erhalten benötigen wir die gesteuerte Variante

$$CP_n |0, b\rangle = |0\rangle \otimes |b\rangle , \qquad CP_n |1, b\rangle = |1\rangle \otimes P_n |b\rangle$$

mit der wir



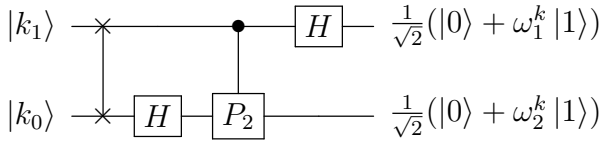
erhalten. Wenn wir beim ersten Qubit am Ende noch ein Hadamardgatter ergänzen, dann ist das praktisch die gesuchte Fouriertransformation, bis auf die Tatsache, dass wir am Eingang die Qubits in der umgekehrten Reihenfolge benötigen:

$$\mathrm{QFT}_2 = (H \otimes \mathbb{I}) \circ CP_2 \circ (\mathbb{I} \otimes H) \circ \mathrm{SWAP}.$$

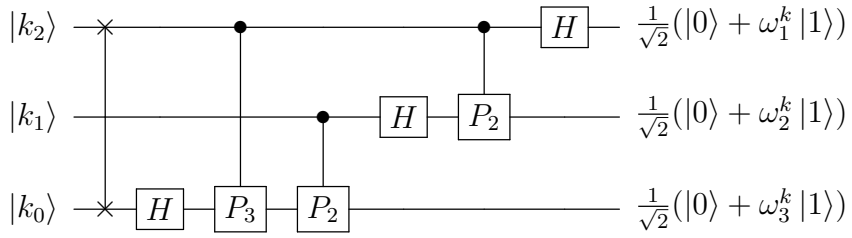
In der Tat gilt

$$\begin{aligned}
|k\rangle = |k_1\rangle \otimes |k_0\rangle &\overset{\text{SWAP}}{\to} |k_0\rangle \otimes |k_1\rangle \overset{\mathbb{I}\otimes \text{H}}{\to} |k_0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + \omega_1^{k_1} |1\rangle) \\
&\overset{\text{CP}_2}{\to} |k_0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + \omega_2^{k_0}\omega_1^{k_1} |1\rangle) \\
&\overset{\text{H}\otimes\mathbb{I}}{\to} \frac{1}{\sqrt{2}}(|0\rangle + \omega_1^{k_0} |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + \omega_2^{k_0}\omega_1^{k_1} |1\rangle) \\
&= \frac{1}{2}(|0\rangle + \omega_1^{k} |1\rangle) \otimes (|0\rangle + \omega_2^{k} |1\rangle)
\end{aligned}$$

Als Schaltkreis:



Für drei Qubits führt eine analoge Rechnung auf



Allgemein erhält man

$$\text{QFT}_n |k\rangle = \frac{1}{\sqrt{N}}(|0\rangle + \omega_1^k |1\rangle) \otimes \cdots \otimes (|0\rangle + \omega_n^k |1\rangle)$$

und das kann man mit einem Quantenschaltkreis aus $O(n^2)$ Gattern ($\lceil \frac{n}{2} \rceil$ mal SWAP, $\frac{n(n-1)}{2}$ mal CP_k und n mal H) realisieren.

8.4.4 Shor-Algorithmus

Ziel des **Shor-Algorithmus** [Sho97] ist es Perioden zu finden. In Abschnit 5.5 haben wir gesehen, dass es möglich ist, einen Faktor von m zu finden, wenn man in der Lage ist die Ordnung k von $a \in \mathbb{Z}_m^*$ zu ermitteln. Also das kleinste $k \in \mathbb{N}$ für das $a^k = 1 \pmod m$ gilt. Äquivalent dazu ist es, die Periode der Funktion $f(j) = a^j \pmod m$ zu finden. Letzteres kann mithilfe der Quanten-Fouriertransformation bewerkstelligt werden.

Um die Idee zu illustrieren betrachten wir ein einfaches Bespiel und versuchen die Zahl $m = 15$ zu faktorisieren. Dazu wählen wir $N = 2^n > m$, z.B. $N = 16$.

Wir beginnen mit zwei Quantenregistern zu jeweils $n = 4$ Qubits

$$|j\rangle \otimes |l\rangle$$

und gehen davon aus, dass wir die Funktion $f(j) = a^j \pmod m$ als Quantenorakel in der Form

$$U_f : |j\rangle \otimes |l\rangle \mapsto |j\rangle \otimes |l \oplus f(j)\rangle$$

implementiert haben. Dieser Schritt ist in der Praxis sehr aufwendig, da das Potenzieren implementiert werden muss.

Nun kommen wir zum eigentlichen Algorithmus: Wir initialisieren unsere Register und wenden auf das erste eine Hadamard-Transforation an

$$(H^{\otimes n} |0\rangle) \otimes |0\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle \otimes |0\rangle .$$

Nun wenden wir U_f an und erhalten

$$\frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle \otimes |f(j)\rangle .$$

Wählen wir in unserem Beispiel z.B. $a = 7$ so gilt:

j	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$f(j)$	1	7	4	13	1	7	4	13	1	7	4	13	1	7	4	13

Insbesondere sehen wir unmittelbar, dass die Periode $k = 4$ ist. Wir müssen diese Information aber noch unserem Quantenzustand

$$\frac{1}{4}(|0\rangle + |4\rangle + |8\rangle + |12\rangle) \otimes |1\rangle + \frac{1}{4}(|1\rangle + |5\rangle + |9\rangle + |13\rangle) \otimes |7\rangle +$$
$$\frac{1}{4}(|2\rangle + |6\rangle + |10\rangle + |14\rangle) \otimes |4\rangle + \frac{1}{4}(|3\rangle + |7\rangle + |11\rangle + |15\rangle) \otimes |13\rangle$$

entlocken. Da alle vier Summanden analoge Informationen enthalten, messen wir das zweite Register und erhalten einen der vier Summanden als Ergebnis. Z.B. könnte das Ergebnis der Messung 7 lauten und unser Quantencomputer wäre nun im Zustand

$$\frac{1}{2}(|1\rangle + |5\rangle + |9\rangle + |13\rangle) \otimes |7\rangle .$$

Nun wenden wir die Quanten-Fouriertransform auf das erste Register an und erhalten

$$\frac{1}{2}(|0\rangle + \mathrm{i}\,|4\rangle + |8\rangle + \mathrm{i}\,|12\rangle) \otimes |7\rangle .$$

Wir erhalten also genau die Zustände, die Information über die gesuchte Periode enthalten. Und das ist kein Zufall, sondern eine charakteristische Eigenschaft der Fouriertransformation! Bei der Darstellung des Eingangsvektors durch die Basisvektoren der Fouriertransformation werden nur jene Basisvektoren benötigt, die die gleiche Periode wie der Eingangsvektor besitzen. Eine Verschiebung des $k$ten

Basisvektors um eine Periode p entspricht einer Multiplikation mit ω_n^{kp} und es muss daher kp ein Vielfaches von N sein. In unserem Beispiel muss also $k \in \{j\frac{N}{p} | j = 0, \ldots, p-1\} = \{j\frac{16}{4} | j = 0, \ldots, 3\} = \{0, 4, 8, 12\}$ sein.

Führen wir also abschließend eine Messung des ersten Registers durch, so erhalten wir ein Ergebnis k, dass die Gleichung

$$\frac{j}{p} = \frac{k}{N}$$

erfüllt. Wir müssen also nur den Bruch k/N kürzen und erhalten p falls nicht gerade $k = 0$ ist. In diesem Fall muss die Rechnung wiederholt werden und man muss auf mehr Glück im nächsten Anlauf hoffen.

Das ist die wesentliche Idee des Shor-Algorithmus. Allerdings ist unser Beispiel etwas irreführend, denn im Allgemeinen wird die gesuchte Periode p kein Teiler von $N = 2^n$ sein. Deshalb muss N deutlich größer als m gewählt werden (konkret $N \approx m^2$) und dann kann man zeigen, dass das Ergebnis der Messung mit hoher Wahrscheinlichkeit eine Zahl nahe bei einem Vielfachen von N/p liefert. Die Periode kann dann durch eine Kettenbruchzerlegung von k/N ermittelt werden. Für weitere Details siehe [Mer07].

8.5 Kontrollfragen

Fragen zu Abschnitt 8.1: Mathematische Grundlagen der Quantenmechanik

Erklären Sie folgende Begriffe: Hilbertraum, Projektion, unitäre Matrix

1. Wie hängen in einem Hilbertraum Länge und Skalarprodukt miteinander zusammen?

   (Lösung zu Kontrollfrage 1)

2. Richtig oder falsch: Eine unitäre Matrix bildet Orthonormalsysteme auf Orthonormalsysteme ab.

   (Lösung zu Kontrollfrage 2)

3. Was ist die Projektion von $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ in die Richtung von $(1, 0)$?

   (Lösung zu Kontrollfrage 3)

4. Welche Vektoren beschreiben den gleichen Zustand?
   a) ψ und $-\psi$ b) $\frac{1}{\sqrt{2}}\psi_0 + \frac{1}{\sqrt{2}}\psi_1$ und $\frac{1}{\sqrt{2}}\psi_0 - \frac{1}{\sqrt{2}}\psi_1$

   (Lösung zu Kontrollfrage 4)

Fragen zu Abschnitt 8.2: Ein Qubit

Erklären Sie folgende Begriffe: Qubit, Bloch-Kugel, X-Gatter, Hadamard-Gatter

1. Was ist die Wahrscheinlichkeit, bei einer Messung den Zustand $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ im Zustand $(1, 0)$ zu finden?

   (Lösung zu Kontrollfrage 1)

2. Was erhält man nach zweimaliger Anwendung des Hadamard-Gatters?

   (Lösung zu Kontrollfrage 2)

Fragen zu Abschnitt 8.3: Noch mehr Qubits

Erklären Sie folgende Begriffe: Tensorprodukt, Verschränkung, CNOT-Gatter, No-Cloning-Theorem, Toffoli-Gatter

1. Ein Register aus 2 Qubits ist im Zustand $\alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 |10\rangle + \alpha_3 |11\rangle$. Mit welcher Wahrscheinlichkeit erhält man bei einer Messung, dass das erste Qubit im Zustand $|0\rangle$ ist?

   (Lösung zu Kontrollfrage 1)

2. Ein Register aus 2 Qubits ist im Zustand $\alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 |10\rangle + \alpha_3 |11\rangle$. Bei einer Messung hat sich das erste Qubit entschieden, im Zustand $|0\rangle$ zu sein. In welchem Zustand ist das Register nach der Messung?

   (Lösung zu Kontrollfrage 2)

3. Welche Vektoren sind verschränkt?
   a) $|00\rangle$ b) $\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$ c) $\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |01\rangle$

   (Lösung zu Kontrollfrage 3)

4. Ist es möglich ein Qubit zu kopieren?

   (Lösung zu Kontrollfrage 4)

5. Kann ein Quantencomputer beliebige klassische Logikschaltkreise simulieren?

   (Lösung zu Kontrollfrage 5)

Fragen zu Abschnitt 8.4: Quantenalgorithmen

Erklären Sie folgende Begriffe: Quantenorakel, Grover-Algorithmus, Quanten-Fourier-transformation, Shor-Algorithmus

1. Der Grover-Algoritmus kann AES in subexponentieller Zeit brechen.

   (Lösung zu Kontrollfrage 1)

2. Ist es sinnvoll beim Grover-Algoritmus die Anzahl der Iterationen zu erhöhen?

   (Lösung zu Kontrollfrage 2)

3. Was ergibt $\mathrm{QFT}_n |0\rangle$

   (Lösung zu Kontrollfrage 3)

4. Ist der Shor-Algoritmus immer erfolgreich? Wenn nein, was kann man in einem solchen Fall tun?

   (Lösung zu Kontrollfrage 4)

Lösungen zu den Kontrollfragen

Lösungen zu Abschnitt 8.1

1. $\|\psi\|^2 = \langle\psi, \psi\rangle$
2. Richtig
3. $(\frac{1}{\sqrt{2}}, 0)$
4. a) Ja. b) Nein.

Lösungen zu Abschnitt 8.2

1. $|\langle(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}), (1, 0)\rangle|^2 = \frac{1}{2}$
2. Den Ausgangszustand.

Lösungen zu Abschnitt 8.3

1. $|\alpha_0|^2 + |\alpha_1|^2$
2. Im Zustand $\frac{\alpha_0}{|\alpha_0|^2+|\alpha_1|^2} |00\rangle + \frac{\alpha_1}{|\alpha_0|^2+|\alpha_1|^2} |01\rangle$.
3. a) Nein. b) Ja. c) Nein
4. Nein, das besagt gerade das No-Cloning-Theorem.
5. Ja, mit dem Toffoli-Gatter.

Lösungen zu Abschnitt 8.4

1. Falsch. Er halbiert das Sicherheitsniveau.
2. Nein, das Ergebnis verschlechtert sich dadurch sogar.
3. Einen gleichverteilten Zustand: $\mathrm{QFT}_n |0\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle$.
4. Nein, das Ergebnis könnte gleich 0 sein und in diesem Fall kann die Periode nicht abgelesen werden. Der Algorithmus muss in diesem Fall wiederholt werden.

8.6 Übungen

Aufwärmübungen

1. Geben Sie einen Zustand an, bei dem $|0\rangle$ mit Wahrscheinlichkeit $\frac{2}{9}$ und $|1\rangle$ mit Wahrscheinlichkeit $\frac{7}{9}$ gemessen wird. Gibt es genau einen oder mehrere?
2. Welchen Aussagen sind wahr? Begründen Sie!
   Zur Erinnerung: Hadamard-Matrix: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
   a) Wenn man auf $|1\rangle$ die Hadamard-Matrix zweimal hintereinander anwendet, erhält man wieder $|1\rangle$.
   b) Wenn man auf $|1\rangle$ die Hadamard-Matrix anwendet, erhält man $|0\rangle$.
   c) Die Matrix $\frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$ ist unitär.
   d) $|0\rangle + |1\rangle$ ist ein zulässiger Zustand eines Qubits.
3. Für welche(s) $a \in \mathbb{C}$ wird die Matrix
   $$U = \begin{pmatrix} -a & 1 \\ 1 & -a \end{pmatrix}$$
   unitär? Begründen Sie!
   a) $a = 1$
   b) $a = \mathrm{i}$
   c) $a = 0$
   d) Für kein $a \in \mathbb{C}$
4. Welche Aussagen sind wahr? Begründen Sie!

a) Man geht davon aus, dass aufgrund des Algorithmus von Shor Public Key Verfahren wie z.B. RSA praktisch nicht mehr sicher sind, sobald es leistungsstarke Quantencomputer geben wird.

b) Man geht davon aus, dass aufgrund des Algorithmus von Grover Public Key Verfahren wie z.B. RSA praktisch nicht mehr sicher sind, sobald es leistungsstarke Quantencomputer geben wird.

c) Wenn man den Zustand $\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle$ bezüglich der Basis $|+\rangle, |-\rangle$ misst, so findet man das Qubit mit Wahrscheinlichkeit $\frac{1}{2}$ im Zustand $|0\rangle$ vor.

d) $\psi_1 = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ und $\psi_2 = -\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ bezeichnen denselben Zustand eines Qubit.

5. Zeigen Sie, dass die Pauli-Matrix

$$\sigma_y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}$$

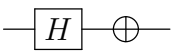
unitär ist.

6. a) Geben Sie alle unitären Transformationen U an, die den Vektor $|0\rangle$ auf $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ abbilden.
b) Wie lauten speziell die *reellen* Transformationen, die $|0\rangle$ wie gewünscht abbilden?

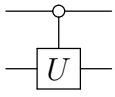
7. Berechnen Sie $H(\alpha\,|0\rangle + \beta\,|1\rangle)$, wobei H die Hadamard-Matrix ist. Stellen Sie das Ergebnis als Überlagerung von $|0\rangle$ und $|1\rangle$ dar.

8. Berechnen Sie $H\,|+\rangle$ und $H\,|-\rangle$, wobei H die Hadamard-Matrix ist und $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ bzw. $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

9. Durch welche Matrix wird der folgende Schaltkreis beschrieben?



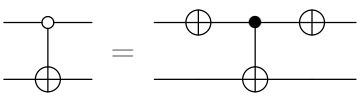
10. Durch welche Matrix wird das invers gesteuerte U-Gatter beschrieben?



11. Beschreiben Sie die Wirkung des Schaltkreises

der durch die Matrix $U_X \otimes \mathbb{I}_2$ beschrieben wird. Berechnen Sie den Zustand von $\frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|11\rangle$ nach Durchlaufen dieses Schaltkreises.

12. Beweisen Sie die Äquivalenz folgender beider Schaltkreise:

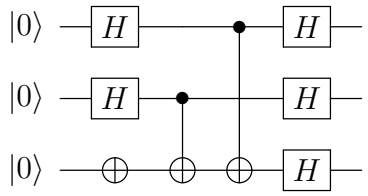


13. Finden Sie einen Schaltkreis, der den Bell-Zustand

$$\frac{1}{\sqrt{2}}\,|00\rangle - \frac{1}{\sqrt{2}}\,|11\rangle$$

erzeugt.

14. Welchen Zustand erzeugt der folgende Schaltkreis?



Weiterführende Aufgaben

1. Zeigen Sie, dass die Matrix

$$U_T = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1+\mathrm{i}}{\sqrt{2}} \end{pmatrix}$$

unitär ist.

2. Welchem Zustand entspricht der Punkt $(0, \frac{\sqrt{3}}{2}, \frac{1}{2})$ auf der Blochkugel?

3. a) Geben Sie alle unitären Transformationen U an, die den Zustand $|1\rangle$ auf $\frac{\sqrt{3}}{2}\,|0\rangle + \frac{1}{2}\,|1\rangle$ abbilden.
b) Wie lauten speziell alle *reellen* Transformationen, die $|1\rangle$ wie gewünscht abbilden?

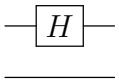
4. Berechnen Sie $H(\alpha\,|0\rangle - \beta\,|1\rangle)$, wobei H die Hadamard-Matrix ist. Stellen Sie das Ergebnis als Überlagerung von $|0\rangle$ und $|1\rangle$ dar.

5. Wir betrachten die Zustände: $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ und $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.
a) Zeigen Sie, dass $|+\rangle$ und $|-\rangle$ eine Orthonormalbasis des $\mathbb{C}^2$ bilden.
b) Stellen Sie $|0\rangle$ als Linearkombination von $|+\rangle$ und $|-\rangle$ dar.
c) Wenn ein Qubit im Zustand $|0\rangle$ ist und wir bezüglich der Basis $|+\rangle$, $|-\rangle$ messen, was ist dann als Messergebnis zu erwarten?

6. a) Was ist das Ergebnis das Algorithmus „Erzeugung eines Zufallsbits“ (Zufallszahlengenerator), wenn man als Anfangszustand nicht $|0\rangle$, sondern $|1\rangle$ wählt?
   b) Und was ist das Ergebnis, wenn man den Anfangszustand $|+\rangle$ wählt?

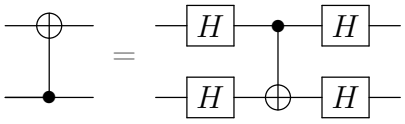
7. Zeigen Sie, dass zwei antipodale Zustände auf der Blochkugel orthogonal sind. (Zwei Punkte auf einer Kugel sind antipodal, wenn sie auf einer Geraden durch den Mittelpunkt liegen. Die Kugelkoordinaten zweier antipodaler Punkte sind (φ, θ) und $(\varphi + \pi, \pi - \theta)$.)

8. Berechnen Sie den Zustand von $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ nach Durchlaufen des Schaltkreises,

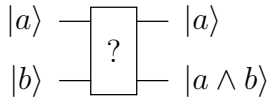
   

   der durch die Matrix $H \otimes \mathbb{I}_2$ beschrieben wird.

9. Zeigen Sie dass das umgedrehte CNOT-Gatter wie folgt realisiert werden kann:

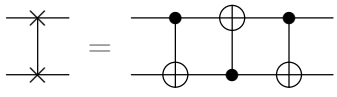
   

10. Kann man mit einem Quantengatter eine logische UND Verknüpfung in der folgenden Form realisieren?

    Wenn nein, wie könnte man das machen? Wie sieht es mit der OR Verknüpfung aus?

11. Zeigen Sie, dass das SWAP-Gatter mit zwei CNOT- und einem umgedrehten CNOT-Gatter realisieren werden kann:

12. Zeigen Sie, dass für die Pauli-Matrizen

    $$\sigma_a \sigma_b = \mathrm{i}\sigma_c$$

    für $abc \in \{xyz, zxy, yzx\}$ gilt. Zeigen Sie weiter

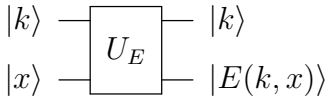
    $$\sigma_a \sigma_b = \begin{cases} \mathbb{I}_2, & a = b, \\ -\sigma_b \sigma_a, & a \neq b. \end{cases}$$

Die 16 Matrizen

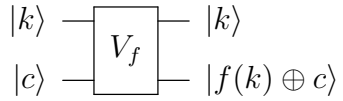
$$\{\pm\mathbb{I}_2, \pm\mathrm{i}\mathbb{I}_2, \pm\sigma_x, \pm\mathrm{i}\sigma_x, \pm\sigma_y, \pm\mathrm{i}\sigma_y, \pm\sigma_z, \pm\mathrm{i}\sigma_z\}$$

bilden also eine Gruppe, die **Pauli-Gruppe**.

13. Angenommen Sie haben bereits den Verschlüsselungsalgorithms $y = E(k, x)$ als Quantenorakel



implementiert (etwaige Ancilla-Qubits sind hier nicht mehr explizit angeführt). Nun hat ihre Auslandsabteilung das Klar-/Geheimtextpaar $x = 0$, $y = 1$ ausgespäht. Implementieren Sie ein Quantenorakel von der Form



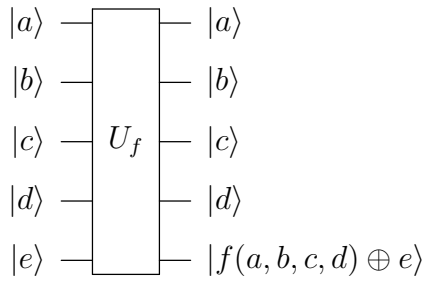
mit $f(k) = 1$ für $1 = E(k, 0)$ und $f(k) = 0$ sonst. Wie erhalten Sie daraus ein Phasenorakel

$$U_f \left|k\right\rangle = (-1)^{f(k)} \left|k\right\rangle ,$$

wie sie es für den Grover-Algorithmus brauchen? Sie sollten mit CNOT, X und H auskommen.

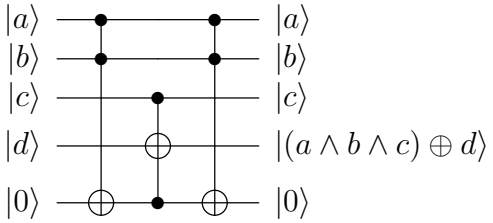
Optional: Testen Sie ihren Code mit einem Simulator (z.B. `qiskit.org`).

14. Entwerfen Sie ein Quantenorakel



mit $f(a, b, c, d) = 1$ falls $a = b$, $c = d$ und $f(a, b, c, d) = 0$ sonst.

15. Zeigen Sie, dass ein CCCNOT-Gatter mit drei Toffoli-Gatter und einem Hilfsqubit wie folgt realisiert werden kann:



Lösungen zu den Aufwärmübungen

1. Es gibt mehrere, z.B. $\frac{\sqrt{2}}{3}|0\rangle + \frac{\sqrt{7}}{3}|1\rangle$ oder $\frac{\sqrt{2}}{3}|0\rangle - \frac{\sqrt{7}}{3}|1\rangle$. Der allgemeinste Zustand ist $\mathrm{e}^{\mathrm{i}\alpha}\frac{\sqrt{2}}{3}|0\rangle + \mathrm{e}^{\mathrm{i}\beta}\frac{\sqrt{7}}{3}|1\rangle$ mit $\alpha, \beta \in [0, 2\pi)$. Wir können sogar $\alpha = 0$ wählen, da Vektoren, die sich um ein Vielfaches vom Betrag eins (also einen Faktor $\mathrm{e}^{\mathrm{i}\gamma}$) unterscheiden, den gleichen Zustand beschreiben.

2. a), c) sind richtig

3. $a = 0$ denn in diesem Fall ist $UU^* = \mathbb{I}$ (bzw. alternativ: die Spalten / Zeilen bilden eine ONB)

4. a) wahr
   b) falsch (siehe a))
   c) falsch; es wäre richtig, wenn bzlg. der Basis $|0\rangle, |1\rangle$ gemessen wird
   d) wahr, weil ψ_1 und ψ_2 sich um einen Faktor mit Betrag 1 unterscheiden

5. Es ist zu zeigen, dass $\sigma_y^*\sigma_y = \mathbb{I}_2$ ist. Es gilt: $\sigma_y^* = \overline{\sigma_y}^T = \sigma_y$, somit

$$\sigma_y^*\sigma_y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}\begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

6. a) Wir setzen U an in der Form

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad \text{mit } a, b, c, d \in \mathbb{C}.$$

   Aus der Bedingung

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

   folgt bereits die erste Spalte von U:

$$U = \begin{pmatrix} \frac{1}{\sqrt{2}} & b \\ \frac{1}{\sqrt{2}} & d \end{pmatrix}$$

   Weiters muss U unitär sein. Das bedeutet, dass die Spalten $\mathbf{u}_1 = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$ und $\mathbf{u}_2 = \begin{pmatrix} b \\ d \end{pmatrix}$ von U eine Orthonormalbasis des $\mathbb{C}^2$ bilden, es muss also gelten:

   - Die Spalten sind orthogonal: $\langle \mathbf{u}_1, \mathbf{u}_2 \rangle = 0$, d.h. $\frac{1}{\sqrt{2}}b + \frac{1}{\sqrt{2}}d = 0$, also $b + d = 0$ bzw.

$$d = -b \tag{1}$$

- Die Spalten sind normiert: Die erste Spalte ist bereits normiert, die zweite muss erfüllen
$$|b|^2 + |d|^2 = 1 \tag{2}$$

Wenn wir $U^*U = \mathbb{I}_2$ fordern (Definition einer unitären Matrix), kommen wir auf dieselben Bedingungen an b und d.

Wenn wir nun Bedingung (1) in Bedingung (2) einsetzen, ergibt sich: $2|b|^2 = 1$, also $|b| = \frac{1}{\sqrt{2}}$. Somit ist b eine komplexe Zahl mit Betrag $\frac{1}{\sqrt{2}}$, kann also in Exponentialform angegeben werden als

$$b = \frac{1}{\sqrt{2}} \mathrm{e}^{\mathrm{i}\alpha} \qquad \text{mit } \alpha \in [0, 2\pi).$$

Dann folgt mit Bedingung (1)

$$d = -b = -\frac{1}{\sqrt{2}} \mathrm{e}^{\mathrm{i}\alpha}$$

Insgesamt:

$$U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & \mathrm{e}^{\mathrm{i}\alpha} \\ 1 & -\mathrm{e}^{\mathrm{i}\alpha} \end{pmatrix} \quad \text{mit } \alpha \in [0, 2\pi).$$

Äquivalent zum obigen Weg ist die Forderung, dass die *Zeilen* von

$$U = \begin{pmatrix} \frac{1}{\sqrt{2}} & b \\ \frac{1}{\sqrt{2}} & d \end{pmatrix}$$

eine ONB bilden, bzw. dass $UU^* = \mathbb{I}_2$ (im Gegensatz zu $U^*U = \mathbb{I}_2$). Das führt auf die Gleichungen $\frac{1}{2} + |b|^2 = 1$, $\frac{1}{2} + |d|^2 = 1$, $\frac{1}{2} + \overline{b}d = 0$, die natürlich dieselbe Lösung wie oben ergeben.

b) Wir setzen U an in der Form

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad \text{mit } a, b, c, d \in \mathbb{R}.$$

Aus der Bedingung

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

folgt die erste Spalte von U:

$$U = \begin{pmatrix} \frac{1}{\sqrt{2}} & b \\ \frac{1}{\sqrt{2}} & d \end{pmatrix}$$

Damit U unitär ist, die Spalten also eine Orthonormalbasis (Spalten normiert und orthogonal zueinander) von $\mathbb{R}^2$ bilden, gibt es nur zwei Möglichkeiten:

$$U_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \text{ oder } U_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

7.

$$\begin{aligned} H(\alpha\,|0\rangle + \beta\,|1\rangle) &= \alpha H\,|0\rangle + \beta H\,|1\rangle = \alpha\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \beta\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \\ &= \frac{1}{\sqrt{2}}(\alpha+\beta)\,|0\rangle + \frac{1}{\sqrt{2}}(\alpha-\beta)\,|1\rangle \end{aligned}$$

8.

$$H\,|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}2\\0\end{pmatrix} = |0\rangle$$

und analog:

$$H\,|-\rangle = |1\rangle$$

9. Wir müssen das Produkt der entsprechenden Matrizen bilden:

$$U = U_X H = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}.$$

10.

$$\begin{pmatrix}U_{11} & U_{12} & 0 & 0\\ U_{21} & U_{22} & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{pmatrix}$$

11. Da das X-Gatter $|0\rangle \mapsto |1\rangle$ und $|1\rangle \mapsto |0\rangle$ bewirkt, gilt $U_X \otimes \mathbb{I}_2(|0\rangle \otimes |0\rangle) = (U_X\,|0\rangle) \otimes |0\rangle = |1\rangle \otimes |0\rangle$, etc. Insgesamt erhalten wir

$$U_X \otimes \mathbb{I}_2: \quad |00\rangle \mapsto |10\rangle\,,\ |01\rangle \mapsto |11\rangle\,,\ |10\rangle \mapsto |00\rangle\,,\ |11\rangle \mapsto |01\rangle$$

oder als Matrix

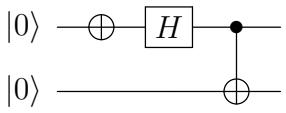
$$\begin{pmatrix}0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\\ 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\end{pmatrix}.$$

Im konkreten Fall ist der Endzustand durch $\frac{1}{\sqrt{2}}\,|10\rangle + \frac{1}{\sqrt{2}}\,|01\rangle$ gegeben.

12. Wir können das zum Beispiel durch Multiplizieren der zugehörigen Matrizen nachweisen:

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

13. Zum Beispiel



Denn $HU_X\,|0\rangle = H\,|1\rangle = \frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle$ und das CNOT-Gatter bewirkt $\big(\frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle\big) \otimes |0\rangle = \frac{1}{\sqrt{2}}\,|00\rangle - \frac{1}{\sqrt{2}}\,|10\rangle \mapsto \frac{1}{\sqrt{2}}\,|00\rangle - \frac{1}{\sqrt{2}}\,|11\rangle$.

14. Der Zustand vor dem ersten CNOT-Gatter ist

$$\begin{aligned}
|++1\rangle &= |+\rangle \otimes |+\rangle \otimes |1\rangle \\
&= \big(\frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\big) \otimes \big(\frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\big) \otimes |1\rangle \\
&= \big(\frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\big) \otimes \big(\frac{1}{\sqrt{2}}\,|01\rangle + \frac{1}{\sqrt{2}}\,|11\rangle\big) \\
&= \frac{1}{2}\big(\,|001\rangle + |101\rangle + |011\rangle + |111\rangle\,\big);
\end{aligned}$$

nach dem ersten

$$\begin{aligned}
&\big(\frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\big) \otimes \big(\frac{1}{\sqrt{2}}\,|01\rangle + \frac{1}{\sqrt{2}}\,|10\rangle\big) \\
&\qquad = \frac{1}{2}\big(\,|001\rangle + |101\rangle + |011\rangle + |110\rangle\,\big);
\end{aligned}$$

und nach dem zweiten

$$\frac{1}{2}\big(\,|001\rangle + |100\rangle + |011\rangle + |111\rangle\,\big) = \frac{1}{\sqrt{2}}\big(\,|+01\rangle + |+11\rangle\,\big).$$

Wenden wir nun Hadamard auf das erste

$$\frac{1}{\sqrt{2}}\big(\,|001\rangle + |011\rangle\,\big) = |0+1\rangle\,,$$

das zweite

$$|001\rangle\,,$$

und zuletzt auf das dritte Qubit an

$$|00+\rangle = \frac{1}{\sqrt{2}}\big(\,|000\rangle + |111\rangle\,\big).$$

Dieser Zustand ist als **GHZ-Zustand** bekannt.

Lösungen zu ausgewählten Aufgaben

1. Es ist zu zeigen, dass $U_T^* U_T = \mathbb{I}_2$ ist.
2. $\frac{\sqrt{3}}{2}|0\rangle + \frac{\mathrm{i}}{2}|1\rangle$
3. a)
$$U = \frac{1}{2}\begin{pmatrix} \mathrm{e}^{\mathrm{i}\alpha} & \sqrt{3} \\ -\sqrt{3}\mathrm{e}^{\mathrm{i}\alpha} & 1 \end{pmatrix} \quad \text{mit } \alpha \in [0, 2\pi).$$
b)
$$U_1 = \frac{1}{2}\begin{pmatrix} 1 & \sqrt{3} \\ -\sqrt{3} & 1 \end{pmatrix} \text{ oder } U_2 = \frac{1}{2}\begin{pmatrix} -1 & \sqrt{3} \\ \sqrt{3} & 1 \end{pmatrix}$$
4. $H(\alpha|0\rangle - \beta|1\rangle) = \frac{1}{\sqrt{2}}(\alpha - \beta)|0\rangle + \frac{1}{\sqrt{2}}(\alpha + \beta)|1\rangle$
5. a) ...
b) $|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$
c) Wir erhalten $|+\rangle$ mit Wahrscheinlichkeit $\frac{1}{2}$, ebenso $|-\rangle$.
6. a) Das Ergebnis ist unverändert. b) Das Ergebnis ist immer $|1\rangle$.
7. —
8. $\frac{1}{2}\big(|00\rangle + |01\rangle + |10\rangle - |11\rangle\big)$
9. Wir können das zum Beispiel durch Multiplizieren der zugehörigen Matrizen nachweisen:
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$
10. Nein. Mit einem Toffoli Gatter. Analog für OR.
11. Z.B. durch Multiplizieren der zugehörigen Matrizen.
12. —
13. Hinweis: $f(k) = \neg(E(k, x) \oplus y)$
14. Hinweis: $f(a, b, c, d) = (\neg(a \oplus b)) \wedge (\neg(c \oplus d))$
15. –

Literatur

[Bar+95] A. Barenco u. a. „Elementary gates for quantum computation“. In: *Phys. Rev. A* 52 (5 1995), S. 3457–3467. DOI: 10.1103/PhysRevA.52.3457.

[BB84] C. H. Bennett und G. Brassard. „Quantum cryptography: Public key distribution and coin tossing“. In: *International Conference on Computers, Systems and Signal Processing* 175 (1984), S. 175–179. URL: http://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf.

[Ben+97] C. H. Bennett u. a. „Strengths and weaknesses of quantum computing“. In: *SIAM J. Comput.* 26.5 (1997), S. 1510–1523. DOI: 10.1137/S0097539796300933.

[DHH19] A. Dang, C. D. Hill und L. C. L. Hollenberg. „Optimising matrix product state simulations of Shor's algorithm“. In: *Quantum* 3 (2019), S. 116. DOI: 10.22331/q-2019-01-25-116.

[Gro96] L. K. Grover. „A fast quantum mechanical algorithm for database search“. In: *STOC '96: Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing* (Juni 1996), S. 212–219. DOI: 10.1145/237814.237866.

[Hom15] M. Homeister. *Quantum Computing Verstehen*. 4. Aufl. Springer, 2015.

[Lyd+10] L. Lydersen u. a. „Hacking commercial quantum cryptography systems by tailored bright illumination“. In: *Nature Photonics* 4.10 (Aug. 2010), S. 686–689. DOI: 10.1038/nphoton.2010.214.

[Mer07] N. D. Mermin. *Quantum Computer Science; An Introduction*. Cambridge, 2007.

[NC10] M. A. Nielsen und I. L. Chuang. *Quantum Computation and Quantum Information*. 2. Aufl. Cambridge, 2010.

[QISKIT] *Qiskit*. URL: https://qiskit.org (besucht am 20. 11. 2022).

[Sch16] W. Scherer. *Mathematik der Quanteninformatik*. Springer, 2016.

[Sho97] P. W. Shor. „Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer“. In: *SIAM J. Comput.* 26.5 (1997), S. 1484–1509. DOI: 10.1137/S0097539795293172.

[Tha00] B. Thaller. *Visual Quantum Mechanics*. New York: Springer, 2000.

[Tha05] B. Thaller. *Advanced Visual Quantum Mechanics*. New York: Springer, 2005.

[Won22] T. G. Wong. *Introduction to Classical and Quantum Computing*. Rooted Grove, 2022.