FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Skript zur Vorlesung

Quanten Computing

Version 3.3

Georg Hoever

Fachbereich Elektrotechnik und
Informationstechnik
FH Aachen

Inhaltsverzeichnis

1 Qubits und Gatter

1.1 Qubits

Physikalische Realisierung:

Quantencomputer können auf Basis unterschiedlicher physikalischer Effekte gebaut werden:

Photonen,

Kernspinresonanz,

Ionenfallen,

Supraleitung.

Eine ganz andere Art von Quantencomputern sind die adiabatischen Quantencomputer (s. Abschnitt 5.3).

Im Weiteren wird nicht auf die physikalische Realisierung eingegangen.

Geschichtliches:

1900-1925: Entwicklung der Quantenmechanik

1980er Jahre: Der theoretische Physiker Richard Feynman (1918 – 1988) entwickelt die Idee eines auf Quanteneffekten beruhenden Computers.

1990er Jahre: Man beschäftigt sich mit dem theoretischen Konzept und entwickelt erste Algorithmen:

- 1985: Erste Version des Deutsch-Algorithmus
- 1992: Erste Version des Deutsch-Jozsa-Algorithmus
- 1993: Idee der Realisierung von Teleportation
- 1994: Shor-Algorithmus zur Faktorisierung von Zahlen
- 1996: Grover-Algorithmus

1997: Zeilinger u. Co realisieren eine Quantenteleportation über einen Meter.

1998: Erster Quantencomputer mit zwei Qubits

2001: Realisierung des Shor-Algorithmus auf einem Quantencomputer mit 7 Qubits zur Faktorisierung der Zahl 15

seitdem Quantencomputer mit immer mehr Qubits, z.B: 2019 von Google mit 53 Qubits und 2021 von IBM mit 127 Qubits und Ende 2023 mit mehr als 1000 Qubits .

Qubit:

Ein klassisches Bit ist entweder 0 oder 1.

Bei Qubits gibt es entsprechende Basiszustände, die in der sogenannten *Ket-* oder *Dirac*-Notation geschrieben werden als

$$|0\rangle \quad \text{bzw. } |1\rangle\,.$$

Ein allgemeines Qubit $|\Psi\rangle$ kann eine Überlagerung (Superposition) sein:

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

Beispiele:

$$|\Psi_1\rangle = \tfrac{1}{\sqrt{3}}\cdot|0\rangle + \sqrt{\tfrac{2}{3}}\cdot|1\rangle,$$
$$|\Psi_2\rangle = \tfrac{1}{\sqrt{3}}\cdot|0\rangle - \sqrt{\tfrac{2}{3}}\cdot|1\rangle,$$
$$|+\rangle := \tfrac{1}{\sqrt{2}}\cdot|0\rangle + \tfrac{1}{\sqrt{2}}\cdot|1\rangle = \tfrac{1}{\sqrt{2}}\cdot\big(|0\rangle+|1\rangle\big),$$
$$|-\rangle := \tfrac{1}{\sqrt{2}}\cdot|0\rangle - \tfrac{1}{\sqrt{2}}\cdot|1\rangle = \tfrac{1}{\sqrt{2}}\cdot\big(|0\rangle-|1\rangle\big).$$

Bemerkung:

Den Multiplikationspunkt lässt man oft weg:

$$\alpha\cdot|0\rangle+\beta\cdot|1\rangle \;=\; \alpha\,|0\rangle+\beta\,|1\rangle\,.$$

Messung von Qubits, globale Phase:

Misst man ein Qubit $|\Psi\rangle=\alpha\cdot|0\rangle+\beta\cdot|1\rangle$, so wird die Superposition zerstört, und man erhält $|0\rangle$ bzw. $|1\rangle$ mit der Wahrscheinlichkeit $|\alpha|^2$ bzw. $|\beta|^2$.

Beispiele:

Misst man $|\Psi_1\rangle = \frac{1}{\sqrt{3}}\cdot|0\rangle + \sqrt{\frac{2}{3}}\cdot|1\rangle$, so erhält man $|0\rangle$ mit der Wahrscheinlichkeit $\frac{1}{3}$ und $|1\rangle$ mit der Wahrscheinlichkeit $\frac{2}{3}$.

Misst man $|\Psi_2\rangle = \frac{1}{\sqrt{3}}\cdot|0\rangle - \sqrt{\frac{2}{3}}\cdot|1\rangle$, so erhält man ebenso wie bei $|\Psi_1\rangle$ die Ergebnisse $|0\rangle$ mit der Wahrscheinlichkeit $\frac{1}{3}$ und $|1\rangle$ mit der Wahrscheinlichkeit $\frac{2}{3}$.

Misst man $|+\rangle = \frac{1}{\sqrt{2}}\cdot|0\rangle + \frac{1}{\sqrt{2}}\cdot|1\rangle$, so erhält man $|0\rangle$ bzw. $|1\rangle$ jeweils mit der Wahrscheinlichkeit $\frac{1}{2}$.

Misst man $|\Psi_4\rangle = |0\rangle = 1\cdot|0\rangle + 0\cdot|1\rangle$, so erhält man garantiert $|0\rangle$.

Bemerkung:

Man kann auch in anderen Basen als der *Standard-Basis* $\{|0\rangle\,,|1\rangle\}$ messen. Mehr dazu in Abschnitt 8.1.1.

Da bei einer Messung nur die Betragsquadrate maßgebend sind, gibt es bzgl. der Messung keinen Unterschied zwischen $|\Psi_1\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ und z.B. $|\Psi_2\rangle = -\alpha\,|0\rangle + \beta\,|1\rangle$ oder $|\Psi_3\rangle = \alpha\,|0\rangle - \beta\,|1\rangle$ oder allg.

$$|\Psi\rangle \;=\; (\alpha \cdot \mathrm{e}^{\mathrm{j}\varphi_1}) \cdot |0\rangle + (\beta \cdot \mathrm{e}^{\mathrm{j}\varphi_2}) \cdot |1\rangle\,, \quad \varphi_1, \varphi_2 \in \mathbb{C}.$$

Allerdings gibt es bei Interaktionen mit anderen Qubits zum Teil unterschiedliches Verhalten zwischen z.B. $|\Psi_1\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ und $|\Psi_2\rangle = \alpha\,|0\rangle - \beta\,|1\rangle$ ($\beta \neq 0$).

In vielen Fällen ist aber eine *globale Phase* $\mathrm{e}^{\mathrm{j}\varphi}$ irrelevant, d. h. $|\Psi_3\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$ verhält sich wie

$$|\Psi\rangle \;=\; \mathrm{e}^{\mathrm{j}\varphi} \cdot \big(\alpha \cdot |0\rangle + \beta \cdot |1\rangle\big) \;=\; (\alpha \cdot \mathrm{e}^{\mathrm{j}\varphi}) \cdot |0\rangle + (\beta \cdot \mathrm{e}^{\mathrm{j}\varphi}) \cdot |1\rangle\,.$$

Man kann daher oft bei $\alpha \cdot |0\rangle + \beta \cdot |1\rangle$ ohne Beschränkung der Allgemeinheit α als reell und größer gleich Null annehmen.

Darstellung und Veranschaulichung von Qubits:

Für die Darstellung von Qubits gibt es zwei verschiedene Möglichkeiten, zwischen denen im Folgenden oft hin und her gewechselt wird:

Darstellung in der *Ket*-Notation: $|\Psi\rangle \;=\; \alpha \cdot |0\rangle + \beta \cdot |1\rangle$.

Vektorielle Darstellung:

Man identifiziert $|0\rangle$ mit dem Vektor $\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ und $|1\rangle$ mit dem Vektor $\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$. Dann ist

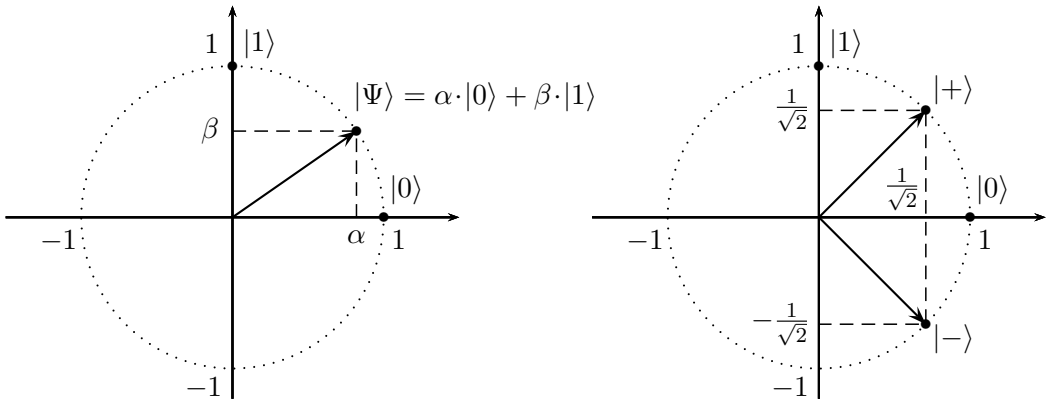
$$|\Psi\rangle \;=\; \alpha \cdot |0\rangle + \beta \cdot |1\rangle \;=\; \alpha \cdot \begin{pmatrix}1\\0\end{pmatrix} + \beta \cdot \begin{pmatrix}0\\1\end{pmatrix} \;=\; \begin{pmatrix}\alpha\\\beta\end{pmatrix}.$$

Dies ist ein Vektor im (komplexen) Vektorraum $\mathbb{C}^2$, ganz analog zum $\mathbb{R}^2$.

Für die Veranschaulichung von Qubits gibt es auch zwei häufig genutzte Möglichkeiten:

Kartesische Veranschaulichung:

Entsprechend der vektoriellen Darstellung kann man $|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \left(\begin{smallmatrix}\alpha\\\beta\end{smallmatrix}\right)$ bei reellem α und β in einem kartesischen Koordinatensystem darstellen:



Die Zustände $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ und $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ liegen beispielsweise in einem $\pm 45°$-Winkel zur waagerechten $|0\rangle$-Achse.

Veranschaulichung auf der Bloch-Kugel:

Auf der *Bloch-Kugel* kann man auch einen komplexen Phasenunterschied bei α und β darstellen. Dabei nutzt man die globale Phase, um bei $|\Psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$ ohne Beschränkung der Allgemeinheit α reell und größer oder gleich Null zu setzen. Damit kann man α darstellen als

$$\alpha \;=\; \cos\left(\tfrac{\vartheta}{2}\right) \quad \text{mit einem } \vartheta \in [0, \pi].$$

Wegen $|\alpha|^2 + |\beta|^2 = 1$ ist dann $|\beta| = \sin\left(\tfrac{\vartheta}{2}\right)$, so dass man

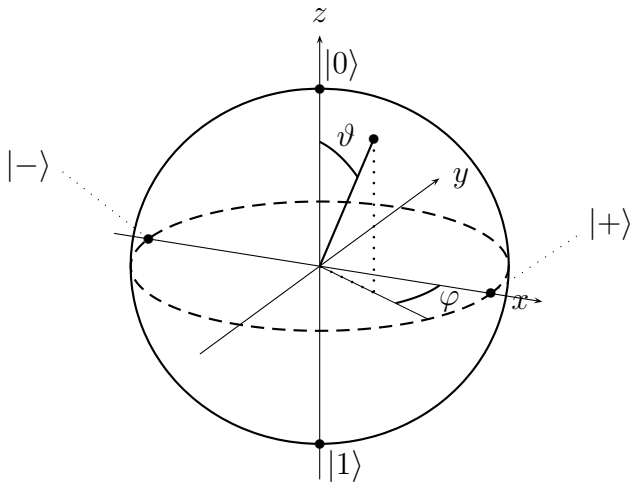
$$\beta \;=\; \mathrm{e}^{\mathrm{j}\varphi} \sin\left(\tfrac{\vartheta}{2}\right) \quad \text{mit } \varphi \in [0, 2\pi[$$

schreiben kann.

Man kann nun

$$|\Psi\rangle \;=\; \alpha \cdot |0\rangle + \beta \cdot |1\rangle \;=\; \cos\left(\tfrac{\vartheta}{2}\right) \cdot |0\rangle + \mathrm{e}^{\mathrm{j}\varphi} \sin\left(\tfrac{\vartheta}{2}\right) \cdot |1\rangle$$

wie in der Skizze als Punkt auf einer dreidimensionalen Kugel mit Radius 1 ansehen. Achtung: Das entspricht nicht der Darstellung einer Linearkombination der Basiszustände!



(Im Bild ist ein Zustand mit negativem φ eingezeichnet.)

Die Zustände $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ und $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ liegen auf dem Äquator gegenüberliegend dort, wo die x-Achse die Kugel durchstößt.

1.2 Modifikation von Qubits: Gatter

1.2.1 Ein bisschen Mathematik: komplexe Vektorräume und unitäre Matrizen

Skalarprodukt in komplexen Vektorräumen:

Das Skalarprodukt in $\mathbb{C}^n$ ist wie in $\mathbb{R}^n$ definiert, wobei der erste Faktor aber jeweils komplex konjugiert wird:

Definition:

Für $a, b \in \mathbb{C}^n$, $a = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$, $b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ ist das Skalarprodukt $\langle a, b \rangle$ definiert durch

$$\langle a, b \rangle \;=\; {a_1}^* \cdot b_1 + \ldots + {a_n}^* \cdot b_n.$$

Die Länge/Norm/Betrag von a ergibt sich durch

$$\|a\| \;=\; \sqrt{|a_1|^2 + \ldots + |a_n|^2} \;=\; \sqrt{\langle a, a \rangle}.$$

Beispiel:

Es ist

$$\begin{aligned} \langle \begin{pmatrix} \mathrm{j} \\ 1+2\mathrm{j} \end{pmatrix}, \begin{pmatrix} 3+2\mathrm{j} \\ \mathrm{j} \end{pmatrix} \rangle \;&= \mathrm{j}^* \cdot (3+2\mathrm{j}) \;+\; (1+2\mathrm{j})^* \cdot \mathrm{j} \\ &= -\mathrm{j} \cdot (3+2\mathrm{j}) \;+\; (1-2\mathrm{j}) \cdot \mathrm{j} \\ &= \quad -3\mathrm{j}+2 \quad + \quad \mathrm{j}+2 \\ &= 4-2\mathrm{j} \end{aligned}$$

und

$$\left\| \begin{pmatrix} \mathrm{j} \\ 1+2\mathrm{j} \end{pmatrix} \right\| \;=\; \sqrt{|\mathrm{j}|^2 + |1+2\mathrm{j}|^2} \;=\; \sqrt{1+(1+4)} \;=\; \sqrt{6}.$$

Adjungierte Matrizen:

Zu einer Matrix $A \in \mathbb{C}^{m \times n}$ ist die *adjungierte* Matrix $A^H \in \mathbb{C}^{n \times m}$, manchmal auch mit $A^\dagger$ bezeichnet, die Matrix, die aus A^T entsteht, indem man zusätlich die Einträge komplex konjugiert.

Beispiel:

Zu $A = \begin{pmatrix} \mathrm{j} & 2+3\mathrm{j} \\ 4 & 5 \end{pmatrix}$ ist $A^H = \begin{pmatrix} -\mathrm{j} & 4 \\ 2-3\mathrm{j} & 5 \end{pmatrix}$.

In $\mathbb{C}^{m \times n}$ gelten für adjungierte Matrizen die gleichen Rechengesetze, die man in $\mathbb{R}^{m \times n}$ für transponierte Matrizen kennt, z.B.

$$(A \cdot B)^H \;=\; B^H \cdot A^H.$$

Fasst man Vektoren als einspaltige Matrizen auf, und identifiziert man (1×1)-Matrizen mit Zahlen, so gilt für das Skalarprodukt

$$\langle a, b\rangle \;=\; a^H \cdot b.$$

Beispiel:

$$\begin{aligned}\langle\begin{pmatrix}\mathrm{j}\\ 1+2\mathrm{j}\end{pmatrix},\begin{pmatrix}3+2\mathrm{j}\\ \mathrm{j}\end{pmatrix}\rangle \;&=\; \begin{pmatrix}\mathrm{j}\\ 1+2\mathrm{j}\end{pmatrix}^H \cdot \begin{pmatrix}3+2\mathrm{j}\\ \mathrm{j}\end{pmatrix}\\ &=\; \begin{pmatrix}\mathrm{j}^* & (1+2\mathrm{j})^*\end{pmatrix} \cdot \begin{pmatrix}3+2\mathrm{j}\\ \mathrm{j}\end{pmatrix}\\ &=\; \begin{pmatrix}-\mathrm{j} & 1-2\mathrm{j}\end{pmatrix} \cdot \begin{pmatrix}3+2\mathrm{j}\\ \mathrm{j}\end{pmatrix}\\ &=\; -\mathrm{j}\cdot(3+2\mathrm{j}) + (1-2\mathrm{j})\cdot\mathrm{j} \;=\; 4-2\mathrm{j}.\end{aligned}$$

Unitäre Matrizen:

Definition:

Eine Matrix $U \in \mathbb{C}^{n\times n}$ heißt *unitär* $\quad\Leftrightarrow\quad U^{-1} = U^H$.

Bei rein reellen Einträgen sind die unitären Matrizen genau die orthogonalen Matrizen, also die, deren Zeilen und/oder Spalten paarweise orthogonal und normiert sind.

Unitäre Matrizen erhalten das Skalarprodukt.

$$\begin{aligned}\langle U\cdot a, U\cdot b\rangle \;&=\; (U\cdot a)^H\cdot(U\cdot b) \;=\; a^H\cdot U^H\cdot U\cdot b\\ &=\; a^H\cdot U^{-1}\cdot U\cdot b \;=\; a^H\cdot b \;=\; \langle a,b\rangle.\end{aligned}$$

Damit bleiben auch Längen unter unitären Transformationen erhalten:

$$\|Ua\| \;=\; \sqrt{\langle U\cdot a, U\cdot a\rangle} \;=\; \sqrt{\langle a,a\rangle} \;=\; \|a\|.$$

Entsprechendes gilt für Winkel, da man einen Winkel mit Hilfe des Skalarprodukts und von Beträgen berechnen kann.

1.2.2 Modifikation von Qubits

Eine (quantenmechanische) Modifikation von Qubits wird durch eine unitäre Matrix $A \in \mathbb{C}^{2\times 2}$ beschrieben. Dabei wird ein Qubit $|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \left(\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right)$ transformiert zu

$$A\,|\Psi\rangle \;=\; A\cdot\begin{pmatrix}\alpha\\ \beta\end{pmatrix}.$$

In dem Zusammenhang bezeichnet man A auch als *Gatter*.

Festlegung einer Transformation:

Eine Matrix $A \in \mathbb{C}^{2\times 2}$ ist durch die Bilder $A \cdot \binom{1}{0}$ und $A \cdot \binom{0}{1}$ eindeutig festglegt,denn dies sind genau die beiden Spalten von A.

Eine Transformation ist also durch die Wirkung auf $|0\rangle$ und $|1\rangle$ schon eindeutig festgelegt.

Dabei können die Bilder $A\,|0\rangle$ und $A\,|1\rangle$ nicht beliebig sein: Beide müssen die Länge 1 haben und „komplex“ senkrecht stehen: $\langle A\,|0\rangle\,, A\,|1\rangle\rangle = 0$.

1.2.3 Hadamard-Transformation

Definition:

Die *Hadamard*-Transformation, auch *Hadamard*-Gatter genannt, ist gegeben durch die *Hadamard*-Matrix H mit

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

Die Benennung ehrt den französischen Mathematiker Jacques Hadamard, 1865 bis 1963.

Die Hadamard-Matrix H ist unitär:

$$H^H \cdot H \;=\; \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \cdot \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \;=\; \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

also $H^{-1} = H^H$. Offensichtlich ist $H^H = H$, d.h., es gilt auch $H^{-1} = H$.

Bei einer Transformation mittels der Hadamard-Matrix

wird aus $|0\rangle = \binom{1}{0}$

$$H\,|0\rangle \;=\; H \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \;=\; \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} \;=\; \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \;=\; \tfrac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big) \;=\; |+\rangle\,,$$

wird aus $|1\rangle = \binom{0}{1}$

$$H\,|1\rangle \;=\; H \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \;=\; \begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix} \;=\; \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} \;=\; \tfrac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big) \;=\; |-\rangle\,.$$

Da $H^{-1} = H$ ist, gilt dann auch umgekehrt

$$H\,|+\rangle \;=\; |0\rangle \qquad \text{und} \qquad H\,|-\rangle \;=\; |1\rangle\,.$$

Dies kann man auch durch die Matrix-Vektor Multiplikation oder mittels der Linearität nachrechnen, z.B.

$$H\,|+\rangle \;=\; \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} \;=\; \begin{pmatrix} 1 \\ 0 \end{pmatrix} \;=\; |0\rangle$$

bzw.

$$\begin{aligned} H\,|+\rangle &= H\Big(\tfrac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big)\Big) \\ &= \tfrac{1}{\sqrt{2}}\Big(H\,|0\rangle + H\,|1\rangle\,\Big) \\ &= \tfrac{1}{\sqrt{2}}\Big(\tfrac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big) + \tfrac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big)\Big) \\ &= \tfrac{1}{\sqrt{2}} \cdot \tfrac{1}{\sqrt{2}} \cdot \big(\,|0\rangle + |0\rangle\,\big) \;=\; |0\rangle\,. \end{aligned}$$

Beispiel:

Aus dem überlagerten Zustand $|\Psi\rangle = -0.8\,|0\rangle + 0.6\,|1\rangle$ wird durch Anwendung der Hadamard-Transformation

$$H\,|\Psi\rangle \;=\; \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \cdot \begin{pmatrix} -0.8 \\ 0.6 \end{pmatrix} \;\approx\; \begin{pmatrix} -0.14 \\ -0.99 \end{pmatrix}.$$

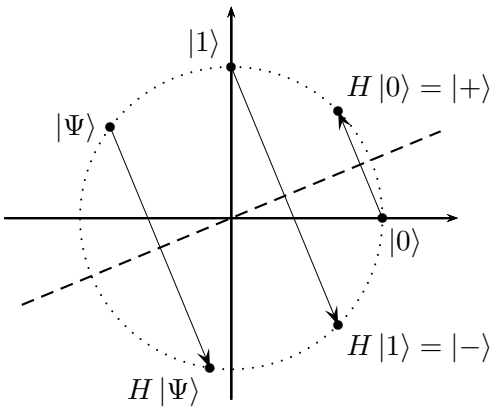
Wegen der Linearität der Matrix-Vektor-Multiplikation erhält man das Ergebnis auch durch

$$\begin{aligned} H\,|\Psi\rangle &= H\big(-0.8\,|0\rangle + 0.6\,|1\rangle\,\big) \\ &= -0.8 \cdot H\,|0\rangle + 0.6 \cdot H\,|1\rangle \\ &= -0.8 \cdot \tfrac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big) + 0.6 \cdot \tfrac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big) \\ &= \big(-0.8 \cdot \tfrac{1}{\sqrt{2}} + 0.6 \cdot \tfrac{1}{\sqrt{2}}\big)\,|0\rangle + \big(-0.8 \cdot \tfrac{1}{\sqrt{2}} - 0.6 \cdot \tfrac{1}{\sqrt{2}}\big)\,|1\rangle \\ &\approx \qquad -0.14 \cdot |0\rangle \qquad - \qquad 0.99 \cdot |1\rangle\,. \end{aligned}$$

Da $H^{-1} = H$ ist, also $H \cdot H = I$, erhält man aus der zweifachen Anwendung des Hadamard-Gatters wieder den Ursprungszustand zurück.

Veranschaulichung der Hadamard-Transformation:

Beschränkt man sich auf Qubits $\Psi = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$ mit $\alpha, \beta \in \mathbb{R}$, so kann man die Wirkung der Hadamard-Transformation interpretieren als Spiegelung an einer Achse, die um $22,5°$ gegenüber der x-Achse gedreht ist:



Auf der Bloch-Kugel beschreibt die Hadamard-Transformation eine 180°-Rotation um die Achse in Richtung $\left(\begin{smallmatrix}1\\0\\1\end{smallmatrix}\right)$, also die Hauptdiagonale der (x, z)-Ebene. Alternativ kann man das auch als Spiegelung an dieser Achse auffassen, d.h., zu einem Punkt bildet man die orthogonale Verbindung zu der Achse und spiegelt diese. Bei der Beschreibung in der Bloch-Kugel muss man allerdings beachten, dass globale Phasen ignoriert werden.

Als Spiegelung ist auch klar, dass die zweifache Ausführung wieder den Ursprungszustand ergibt.

1.2.4 Weitere Gatter

Pauli-Transformationen:

Die Benennung ehrt den Physiker Wolfgang Pauli, 1900 bis 1958.

Pauli-X-Transformation: $P_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

P_X vertauscht $|0\rangle$ und $|1\rangle$, wirkt also wie ein Bitflip:

$$P_X \cdot \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$$

bzw.

$$P_X\big(\alpha\,|0\rangle + \beta\,|1\rangle\big) = \alpha\,|1\rangle + \beta\,|0\rangle = \beta\,|0\rangle + \alpha\,|1\rangle\,.$$

Im $\mathbb{R}^2$ entspricht dies einer Spiegelung an der Hauptdiagonalen, auf der Bloch-Kugel einer 180°-Rotation um die x-Achse (bei Vernachlässigung einer globalen Phase).

Pauli-Z-Transformation: $P_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

P_Z invertiert das Vorzeichen von $|1\rangle$:

$$P_Z \cdot \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ -\beta \end{pmatrix}$$

bzw.

$$P_Z\big(\alpha \cdot |0\rangle + \beta \cdot |1\rangle\big) = \alpha\,|0\rangle - \beta\,|1\rangle\,.$$

Im $\mathbb{R}^2$ entspricht dies einer Spiegelung an der x-Achse, auf der Bloch-Kugel einer 180°-Rotation um die z-Achse (bei Vernachlässigung einer globalen Phase).

Pauli-Y-Transformation: $P_Y = \begin{pmatrix} 0 & -\mathrm{j} \\ \mathrm{j} & 0 \end{pmatrix}$.

Auf der Bloch-Kugel entspricht dies einer 180°-Rotation um die y-Achse (bei Vernachlässigung einer globalen Phase).

Dreh-Gatter RY:

Die Drehung (im $\mathbb{R}^2$) um den Winkel α wird auch als $\mathrm{RY}_{2\alpha}$-Gatter bezeichnet, als Transformationsmatrix:

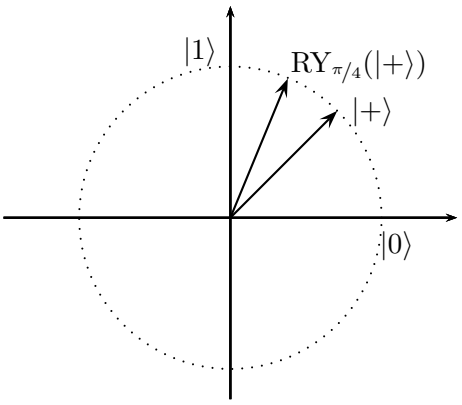
$$\mathrm{RY}_{2\alpha} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}.$$

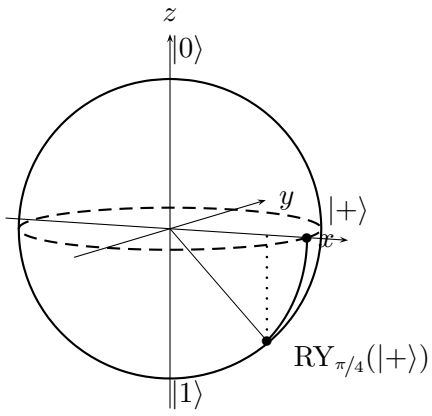
Das Argument „2α“ bei RY kommt von der Interpretation an Hand der Bloch-Kugel: Durch RY_θ wird ein Zustand in der Bloch-Kugel um den Winkel θ um die y-Achse rotiert (entsprechend der „rechten Faust“-Regel, wobei der ausgestreckte Daumen in die y-Richtung weist und die gekrümmten Finger dann die positive Drehrichtung anzeigen) .

Beispiel:

Betrachtet wird die Drehung um $22,5° = \frac{\pi}{8}$, also $\mathrm{RY}_{\pi/4}$, die in der Bloch-Kugel einer Rotation um die y-Achse um $45° = \frac{\pi}{4}$ entspricht.

Dargestellt ist jeweils $|+\rangle$ und $\mathrm{RY}_{\pi/4}(|+\rangle)$, links im $\mathbb{R}^2$, rechts in der Bloch-Kugel.

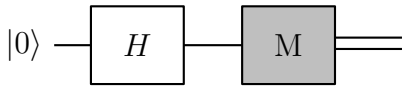




1.3 Ein erster Algorithmus: Zufallsgenerator

Quantenalgorithmen beschreibt man häufig durch Blockschaltbilder.

Durch den folgenden Algorithmus wird ein echter Zufallsgenerator erzeugt:



Analyse:

Der Algorithmus beginnt mit einem Qubit, das auf $|0\rangle$ initialisiert wird.

Anschließend wird eine Hadamard-Transformation darauf angewandt. Der Zustand ist nun also

$$H\,|0\rangle \;=\; |+\rangle \;=\; \tfrac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\big) \;=\; \tfrac{1}{\sqrt{2}}\,|0\rangle + \tfrac{1}{\sqrt{2}}\,|1\rangle\,.$$

Der anschließende M-Block bedeutet eine Messung. Dabei erhält man $|0\rangle$ und $|1\rangle$ jeweils mit der Wahrscheinlichkeit $\frac{1}{2}$.

Zur Darstellung:

Die doppelte Linie rechts des Mess-Blocks deutet an, dass man im Prinzip dort eine klassische Information/ein klassisches Bit (0 oder 1) hat.

2 Quantenregister

2.1 Zusammenfassung zweier Qubits und Tensorprodukt

2.1.1 Zusammenfassung zweier Qubits

Bei zwei Qubits hat man (ähnlich wie bei klassischen Bits) vier Basiszustände

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

Man schreibt diese auch als $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$.

Hat man zwei Qubits $|\Psi_1\rangle$ und $|\Psi_2\rangle$, die jeweils eine Überlagerung darstellen, also

$$\begin{aligned} |\Psi_1\rangle &= \alpha_1\,|0\rangle + \beta_1\,|1\rangle \quad \text{mit } \alpha_1, \beta_1 \in \mathbb{C},\ |\alpha_1|^2 + |\beta_1|^2 = 1, \\ |\Psi_2\rangle &= \alpha_2\,|0\rangle + \beta_2\,|1\rangle \quad \text{mit } \alpha_2, \beta_2 \in \mathbb{C},\ |\alpha_2|^2 + |\beta_2|^2 = 1, \end{aligned}$$

so schreibt man die Zusammenfassung als

$$|\Psi_1\rangle \otimes |\Psi_2\rangle \;=\; |\Psi_1\rangle\,|\Psi_2\rangle \;=\; |\Psi_1\Psi_2\rangle\,.$$

Man kann hier „Ausmultiplizieren“ und erhält eine Überlagerung der Basiszustände:

$$\begin{aligned} |\Psi_1\rangle \otimes |\Psi_2\rangle &= \big(\alpha_1\,|0\rangle + \beta_1\,|1\rangle\big) \otimes \big(\alpha_2\,|0\rangle + \beta_2\,|1\rangle\big) \\ &= \alpha_1\alpha_2\,|00\rangle + \alpha_1\beta_2\,|01\rangle + \beta_1\alpha_2\,|10\rangle + \beta_1\beta_2\,|11\rangle\,. \end{aligned}$$

Beispiele:

Mit

$$|\Psi_1\rangle \;=\; |+\rangle \;=\; \tfrac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big) \qquad \text{und} \qquad |\Psi_2\rangle \;=\; |-\rangle \;=\; \tfrac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big)$$

ist

$$\begin{aligned} |\Psi_1\rangle \otimes |\Psi_2\rangle &= \Big(\tfrac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big)\Big) \otimes \Big(\tfrac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big)\Big) \\ &= \Big(\tfrac{1}{\sqrt{2}}\,|0\rangle + \tfrac{1}{\sqrt{2}}\,|1\rangle\Big) \otimes \Big(\tfrac{1}{\sqrt{2}}\,|0\rangle - \tfrac{1}{\sqrt{2}}\,|1\rangle\Big) \\ &= \tfrac{1}{2}\,|00\rangle - \tfrac{1}{2}\,|01\rangle + \tfrac{1}{2}\,|10\rangle - \tfrac{1}{2}\,|11\rangle \\ &= \tfrac{1}{2}\big(\,|00\rangle - |01\rangle + |10\rangle - |11\rangle\,\big). \end{aligned}$$

Bei der Rechnung darf man auch intuitiv Konstanten vor das „Produkt“ ziehen:

$$\begin{aligned} |\Psi_1\rangle \otimes |\Psi_2\rangle &= \Big(\tfrac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big)\Big) \otimes \Big(\tfrac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big)\Big) \\ &= \tfrac{1}{\sqrt{2}} \cdot \tfrac{1}{\sqrt{2}} \cdot \Big(\big(\,|0\rangle + |1\rangle\,\big) \otimes \big(\,|0\rangle - |1\rangle\,\big)\Big) \\ &= \tfrac{1}{2}\big(\,|00\rangle - |01\rangle + |10\rangle - |11\rangle\,\big). \end{aligned}$$

Ferner ist beispielsweise

$$|\Psi_1\rangle \otimes |0\rangle \;=\; \Big(\tfrac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big)\Big) \otimes |0\rangle \;=\; \tfrac{1}{\sqrt{2}}\big(\,|00\rangle + |10\rangle\,\big).$$

Eigenschaft der Vorfaktoren:

Als Überlagerung der Basiszustände dargestellt gilt: Die Summe der Betragsquadrate der Vorfaktoren ist gleich 1:

$$\begin{aligned} & |\alpha_1\alpha_2|^2 + |\alpha_1\beta_2|^2 + |\beta_1\alpha_2|^2 + |\beta_1\beta_2|^2 \\ = \; & |\alpha_1|^2 \cdot \left(|\alpha_2|^2 + |\beta_2|^2\right) + |\beta_1|^2 \cdot \left(|\alpha_2|^2 + |\beta_2|^2\right) \\ = \; & |\alpha_1|^2 \cdot 1 + |\beta_1|^2 \cdot 1 \;=\; |\alpha_1|^2 + |\beta_1|^2 \;=\; 1. \end{aligned}$$

Vektorielle Darstellung:

Die vier Basiszuständen $|00\rangle$, $|01\rangle$, $|10\rangle$ und $|11\rangle$ kann man als Basisvektoren eines vierdimensionalen Vektorraums auffassen:

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

2.1.2 Ein bisschen Mathematik: Tensorprodukt von Vektoren

Definition:

Zu $v_1, v_2 \in \mathbb{C}^2$, $v_1 = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix}$, $v_2 = \begin{pmatrix} a_2 \\ b_2 \end{pmatrix}$ ist das *Tensorprodukt* $v_1 \otimes v_2 \in \mathbb{C}^4$ definiert durch

$$v_1 \otimes v_2 \;=\; \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \otimes \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} \;=\; \begin{pmatrix} a_1 \cdot \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} \\ b_1 \cdot \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} \end{pmatrix} \;=\; \begin{pmatrix} a_1 a_2 \\ a_1 b_2 \\ b_1 a_2 \\ b_1 b_2 \end{pmatrix}.$$

Dies ist konsistent zu den obigen Schreibweisen und Rechnungen. Beispielsweise ist

$$|01\rangle \;=\; |0\rangle \otimes |1\rangle \;=\; \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \;=\; \begin{pmatrix} 1 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} \;=\; \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

und bei $|\Psi_1\rangle = \alpha_1 |0\rangle + \beta_1 |1\rangle$, $|\Psi_2\rangle = \alpha_2 |0\rangle + \beta_2 |1\rangle$ ist

$$\begin{aligned} |\Psi_1\rangle \otimes |\Psi_2\rangle \;&=\; \left(\alpha_1 |0\rangle + \beta_1 |1\rangle\right) \otimes \left(\alpha_2 |0\rangle + \beta_2 |1\rangle\right) \\ &=\; \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} \otimes \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} \;=\; \begin{pmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{pmatrix} \\ &=\; \alpha_1\alpha_2 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \alpha_1\beta_2 \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \beta_1\alpha_2 \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \beta_1\beta_2 \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \\ &=\; \alpha_1\alpha_2 \cdot |00\rangle \;+\; \alpha_1\beta_2 \cdot |01\rangle \;+\; \beta_1\alpha_2 \cdot |10\rangle \;+\; \beta_1\beta_2 \cdot |11\rangle. \end{aligned}$$

Achtung: Das Tensorprodukt ist nicht kommutativ, d.h., im Allgemeinen ist $v_1 \otimes v_2 \neq v_2 \otimes v_1$, z.B.

$$|1\rangle \otimes |0\rangle \;=\; \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \;=\; \begin{pmatrix} 0 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 1 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} \;=\; \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \;\neq\; |0\rangle \otimes |1\rangle\,.$$

Tensorprodukt bei beliebigen Vektoren:

Definition:

Zu $v \in \mathbb{C}^n$, $w \in \mathbb{C}^m$, $v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$, $w = \begin{pmatrix} w_1 \\ \vdots \\ w_m \end{pmatrix}$ ist das *Tensorprodukt* $v \otimes w \in \mathbb{C}^{n \cdot m}$ definiert durch

$$v \otimes w \;=\; \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \otimes \begin{pmatrix} w_1 \\ \vdots \\ w_m \end{pmatrix} \;=\; \begin{pmatrix} v_1 \cdot \begin{pmatrix} w_1 \\ \vdots \\ w_m \end{pmatrix} \\ \vdots \\ v_n \cdot \begin{pmatrix} w_1 \\ \vdots \\ w_m \end{pmatrix} \end{pmatrix}.$$

Beispiel:

$$\begin{pmatrix} 1 \\ 2 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \;=\; \begin{pmatrix} 1 \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \\ 2 \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \end{pmatrix} \;=\; \begin{pmatrix} 1 \\ 2 \\ 3 \\ 2 \\ 4 \\ 6 \end{pmatrix}.$$

Rechenregeln:

Mit dem Tensorprodukt kann man bis auf die Kommutativität intuitiv umgehen:

a) $v \otimes (w_1 + w_2) \;=\; v \otimes w_1 + v \otimes w_2$ und $(v_1 + v_2) \otimes w \;=\; v_1 \otimes w + v_2 \otimes w$.

b) $(\lambda \cdot v) \otimes w \;=\; \lambda \cdot (v \otimes w) \;=\; v \otimes (\lambda \cdot w)$.

c) $(v_1 \otimes v_2) \otimes v_3 \;=\; v_1 \otimes (v_2 \otimes v_3)$.

Zu a): Es gilt „Punkt“-vor-Strich-Rechnung, also die Klammerkonvention

$$v \otimes w_1 + v \otimes w_1 = (v \otimes w_1) + (v \otimes w_1).$$

Zu b): Bei Betrachtung eines 2-Qubit-Systems kann man also eine globale Phase zwischen den beiden Qubits hin- und herschieben, entsprechend bei mehreren Qubits.

Zu c): Damit braucht man bei einem mehrfachen Tensorprodukt keine Klammern zu setzen.

2.2 Allgemeines 2-Qubit-Register

2.2.1 Definition

Definition:

Ein Zustand $|\Psi\rangle$ eines 2-Qubit-Registers wird beschrieben durch

$$|\Psi\rangle \;=\; \gamma_{00}\,|00\rangle + \gamma_{01}\,|01\rangle + \gamma_{10}\,|10\rangle + \gamma_{11}\,|11\rangle \;=\; \begin{pmatrix}\gamma_{00}\\ \gamma_{01}\\ \gamma_{10}\\ \gamma_{11}\end{pmatrix}$$

mit $\gamma_{00}, \gamma_{01}, \gamma_{10}, \gamma_{11} \in \mathbb{C}$ und $|\gamma_{00}|^2 + |\gamma_{01}|^2 + |\gamma_{10}|^2 + |\gamma_{11}|^2 = 1$.

Beispiel:

$$\Big(\tfrac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big)\Big) \otimes \Big(\tfrac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big)\Big) \;=\; \tfrac{1}{2}\big(\,|00\rangle - |01\rangle + |10\rangle - |11\rangle\,\big).$$

Nicht jeden Zustand $|\Psi\rangle$ eines 2-Qubit-Registers kann man als Tensorprodukt zweier Qubits schreiben.

Beispiel:

Betrachtet wird der sogenannte *Bell-Zustand*

$$|\Psi\rangle \;=\; \tfrac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big) \;=\; \tfrac{1}{\sqrt{2}}\cdot|00\rangle + 0\cdot|01\rangle + 0\cdot|10\rangle + \tfrac{1}{\sqrt{2}}\cdot|11\rangle\,.$$

Wäre $|\Psi\rangle$ das Tensorprodukt von $|\Psi_1\rangle = \alpha_1\,|0\rangle + \beta_1\,|1\rangle$ und $|\Psi_2\rangle = \alpha_2\,|0\rangle + \beta_2\,|1\rangle$, also

$$|\Psi\rangle \;=\; |\Psi_1\rangle \otimes |\Psi_2\rangle \;=\; \alpha_1\alpha_2\,|00\rangle + \alpha_1\beta_2\,|01\rangle + \beta_1\alpha_2\,|10\rangle + \beta_1\beta_2\,|11\rangle\,,$$

so müsste $\alpha_1\beta_2 = 0$ sein, also $\alpha_1 = 0$ oder $\beta_2 = 0$. Dann müsste aber auch der Vorfaktor von $|00\rangle$ oder $|11\rangle$ gleich 0 sein - Widerspruch!

2.2.2 Verschränktheit

Definition:

Man nennt den Zustand $|\Psi\rangle$ eines 2-Qubit-Registers *separabel* oder *unverschränkt*, wenn man $|\Psi\rangle$ als Tensorprodukt zweier Qubits $|\Psi_1\rangle$ und $|\Psi_2\rangle$ darstellen kann: $|\Psi\rangle = |\Psi_1\rangle \otimes |\Psi_2\rangle$.

Andernfalls heißt $|\Psi\rangle$ *verschränkt*.

Beispiel:

$\frac{1}{2}\big(\,|00\rangle - |01\rangle + |10\rangle - |11\rangle\,\big)$ ist ein separabler Zustand,

Der Bell-Zustand $\frac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big)$ ist verschränkt.

Separabilitätsbedingung:

Ein Zustand

$$|\Psi\rangle \;=\; \gamma_{00}\,|00\rangle + \gamma_{01}\,|01\rangle + \gamma_{10}\,|10\rangle + \gamma_{11}\,|11\rangle$$

eines 2-Qubit-Registers ist genau dann separabel, wenn

$$\gamma_{00}\cdot\gamma_{11} \;=\; \gamma_{01}\cdot\gamma_{10}.$$

Beweis:

„⇒“ Ist $|\Psi\rangle = |\Psi_1\rangle \otimes |\Psi_2\rangle$ mit $|\Psi_1\rangle = \alpha_1\,|0\rangle + \beta_1\,|1\rangle$ und $|\Psi_2\rangle = \alpha_2\,|0\rangle + \beta_2\,|1\rangle$, so gilt

$$|\Psi\rangle \;=\; |\Psi_1\rangle \otimes |\Psi_2\rangle \;=\; \alpha_1\alpha_2\,|00\rangle + \alpha_1\beta_2\,|01\rangle + \beta_1\alpha_2\,|10\rangle + \beta_1\beta_2\,|11\rangle\,.$$

Damit gilt

$$\gamma_{00}\cdot\gamma_{11} \;=\; \alpha_1\alpha_2\beta_1\beta_2 \;=\; \gamma_{01}\cdot\gamma_{10}.$$

„⇐“ Nun gelte für

$$|\Psi\rangle \;=\; \gamma_{00}\,|00\rangle + \gamma_{01}\,|01\rangle + \gamma_{10}\,|10\rangle + \gamma_{11}\,|11\rangle\,,$$

dass $\gamma_{00}\cdot\gamma_{11} = \gamma_{01}\cdot\gamma_{10}$ ist.

Ziel ist eine Darstellung $|\Psi\rangle = |\Psi_1\rangle \otimes |\Psi_2\rangle$ mit $|\Psi_1\rangle = \alpha_1\,|0\rangle + \beta_1\,|1\rangle$ und $|\Psi_2\rangle = \alpha_2\,|0\rangle + \beta_2\,|1\rangle$, also

$$|\Psi\rangle \;=\; |\Psi_1\rangle \otimes |\Psi_2\rangle \;=\; \alpha_1\alpha_2\,|00\rangle + \alpha_1\beta_2\,|01\rangle + \beta_1\alpha_2\,|10\rangle + \beta_1\beta_2\,|11\rangle\,,$$

also

$$\alpha_1\alpha_2 = \gamma_{00}, \quad \alpha_1\beta_2 = \gamma_{01}, \quad \beta_1\alpha_2 = \gamma_{10}, \quad \beta_1\beta_2 = \gamma_{11}.$$

Motivation: Wegen $|\alpha_2|^2 + |\beta_2|^2 = 1$ muss dann gelten

$$|\gamma_{00}|^2 + |\gamma_{01}|^2 \;=\; |\alpha_1\alpha_2|^2 + |\alpha_1\beta_2|^2 \;=\; |\alpha_1|^2\cdot\left(|\alpha_2|^2 + |\beta_2|^2\right) \;=\; |\alpha_1|^2.$$

Setzt man $\alpha_1 = \sqrt{|\gamma_{00}|^2 + |\gamma_{01}|^2}$, so erhält man bei $\gamma_{00} \neq 0$

- aus $\alpha_1\alpha_2 = \gamma_{00}$: $\alpha_2 = \frac{\gamma_{00}}{\alpha_1}$,
- aus $\alpha_1\beta_2 = \gamma_{01}$: $\beta_2 = \frac{\gamma_{01}}{\alpha_1}$,
- aus $\beta_1\alpha_2 = \gamma_{10}$: $\beta_1 = \frac{\gamma_{10}}{\alpha_2}$.

Man kann nachrechnen, dass dann auch $\beta_1\beta_2 = \gamma_{11}$ und die Normierungsbedingungen erfüllt sind.

Bei $\gamma_{00} = 0$ folgt wegen

$$\gamma_{01}\cdot\gamma_{10} \;=\; \gamma_{00}\cdot\gamma_{11} \;=\; 0\cdot\gamma_{11} \;=\; 0,$$

dass $\gamma_{01} = 0$ oder $\gamma_{10} = 0$ gelten muss; in beiden Fällen kann man $|\Psi\rangle$ leicht separieren.

Uneindeutigkeit der Zerlegung:

Bei der Konstruktion der Zerlegung im vorigen Beweis hätte man auch

$$\alpha_1 \;=\; -\sqrt{|\gamma_{00}|^2 + |\gamma_{01}|^2}$$

setzen können oder mit beliebigem $\varphi \in \mathbb{R}$ auch

$$\alpha_1 \;=\; \mathrm{e}^{\mathrm{j}\varphi} \cdot \sqrt{|\gamma_{00}|^2 + |\gamma_{01}|^2}.$$

Dies spiegelt die Beliebigkeit der globalen Phase wider; mehr Variabilität ist bei der Zerlegung nicht möglich.

Bezug zu Determinanten:

Die Separabilitätsbedingung $\gamma_{00} \cdot \gamma_{11} = \gamma_{01} \cdot \gamma_{10}$ des Zustands

$$|\Psi\rangle \;=\; \gamma_{00}\,|00\rangle + \gamma_{01}\,|01\rangle + \gamma_{10}\,|10\rangle + \gamma_{11}\,|11\rangle \;=\; \begin{pmatrix} \gamma_{00} \\ \gamma_{01} \\ \gamma_{10} \\ \gamma_{11} \end{pmatrix}$$

bedeutet, dass

$$\det \begin{pmatrix} \gamma_{00} & \gamma_{10} \\ \gamma_{01} & \gamma_{11} \end{pmatrix} \;=\; 0$$

ist. Also ist die Matrix nicht invertierbar, was äquivalent dazu ist, dass die Vektoren $\begin{pmatrix} \gamma_{00} \\ \gamma_{01} \end{pmatrix}$ und $\begin{pmatrix} \gamma_{10} \\ \gamma_{11} \end{pmatrix}$ linear abhängig sind.

Ist z.B. $\begin{pmatrix} \gamma_{00} \\ \gamma_{01} \end{pmatrix} = \lambda \cdot \begin{pmatrix} \gamma_{10} \\ \gamma_{11} \end{pmatrix}$, so ergibt sich in vektorieller Darstellung

$$|\Psi\rangle \;=\; \begin{pmatrix} \gamma_{00} \\ \gamma_{01} \\ \gamma_{10} \\ \gamma_{11} \end{pmatrix} \;=\; \begin{pmatrix} \lambda \cdot \begin{pmatrix} \gamma_{10} \\ \gamma_{11} \end{pmatrix} \\ \begin{pmatrix} \gamma_{10} \\ \gamma_{11} \end{pmatrix} \end{pmatrix} \;=\; \begin{pmatrix} \lambda \\ 1 \end{pmatrix} \otimes \begin{pmatrix} \gamma_{10} \\ \gamma_{11} \end{pmatrix}.$$

Durch geeignete Verschiebung eines Faktors so, dass beide Vektoren normiert sind, erhält man dann eine Zerlegung von $|\Psi\rangle$.

Beispiel:

Der Zustand

$$|\Psi\rangle \;=\; 0.3\,|00\rangle - 0.9\,|01\rangle + 0.1\,|10\rangle - 0.3\,|11\rangle$$

erfüllt die Separabilitätsbedingung $0.3 \cdot (-0.3) = -0.9 \cdot 0.1$.

Geht man für eine Zerlegung wie beim Beweis oben vor, so setzt man

$$\alpha_1 \;=\; \sqrt{0.3^2 + (-0.9)^2} \;=\; \sqrt{0.9} \;=\; \tfrac{3}{\sqrt{10}}.$$

Weiter ist dann

$$\alpha_2 = \frac{0.3}{\alpha_1} = \frac{1}{\sqrt{10}}, \quad \beta_2 = \frac{-0.9}{\alpha_1} = \frac{-3}{\sqrt{10}}, \quad \beta_1 = \frac{0.1}{\alpha_2} = \frac{1}{\sqrt{10}}.$$

Tatsächlich ist

$$|\Psi\rangle \;=\; \left(\tfrac{3}{\sqrt{10}}\,|0\rangle + \tfrac{1}{\sqrt{10}}\,|1\rangle\right) \otimes \left(\tfrac{1}{\sqrt{10}}\,|0\rangle - \tfrac{3}{\sqrt{10}}\,|1\rangle\right).$$

Vektoriell sieht man

$$|\Psi\rangle \;=\; \begin{pmatrix} 0.3 \\ -0.9 \\ 0.1 \\ -0.3 \end{pmatrix} \;=\; \begin{pmatrix} 3 \cdot \begin{pmatrix} 0.1 \\ -0.3 \end{pmatrix} \\ \begin{pmatrix} 0.1 \\ -0.3 \end{pmatrix} \end{pmatrix} \;=\; \begin{pmatrix} 3 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0.1 \\ -0.3 \end{pmatrix}.$$

Die beiden Vektoren sind nicht normiert. Verschiebt man aber einen Faktor $\sqrt{10}$ von dem ersten in den zweiten Vektor, erhält man

$$|\Psi\rangle \;=\; \left(\tfrac{1}{\sqrt{10}} \cdot \begin{pmatrix} 3 \\ 1 \end{pmatrix}\right) \otimes \left(\sqrt{10} \cdot \begin{pmatrix} 0.1 \\ -0.3 \end{pmatrix}\right) \;=\; \begin{pmatrix} \frac{3}{\sqrt{10}} \\ \frac{1}{\sqrt{10}} \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{\sqrt{10}} \\ -\frac{3}{\sqrt{10}} \end{pmatrix}$$

und damit die Zerlegung wie oben.

Eine andere Zerlegung erhält man durch

$$\begin{aligned} |\Psi\rangle \;&=\; \left(-\tfrac{3}{\sqrt{10}}\,|0\rangle - \tfrac{1}{\sqrt{10}}\,|1\rangle\right) \otimes \left(-\tfrac{1}{\sqrt{10}}\,|0\rangle + \tfrac{3}{\sqrt{10}}\,|1\rangle\right) \\ &=\; \begin{pmatrix} -\frac{3}{\sqrt{10}} \\ -\frac{1}{\sqrt{10}} \end{pmatrix} \otimes \begin{pmatrix} -\frac{1}{\sqrt{10}} \\ \frac{3}{\sqrt{10}} \end{pmatrix}. \end{aligned}$$

2.2.3 Verschränktheitsmaß

Ein Maß für die Verschränkung ist die *Concurrence*:

Definition:

Die *Concurrence* eines Zustands $|\Psi\rangle$ eines 2-Qubit-Registers,

$$|\Psi\rangle \;=\; \gamma_{00}\,|00\rangle + \gamma_{01}\,|01\rangle + \gamma_{10}\,|10\rangle + \gamma_{11}\,|11\rangle\,,$$

ist

$$C(|\Psi\rangle) \;=\; 2 \cdot |\gamma_{00} \cdot \gamma_{11} - \gamma_{01} \cdot \gamma_{10}|.$$

Aus der Separabilitätsbedingung folgt

$$|\Psi\rangle \text{ ist separabel} \quad \Leftrightarrow \quad C(|\Psi\rangle) = 0.$$

Man kann zeigen, dass aus der Zustandsnormierung folgt, dass $C(|\Psi\rangle) \leq 1$ ist.

Zustände $|\Psi\rangle$ mit $C(|\Psi\rangle) = 1$ sind also *maximal verschränkt*.

Beispiele:

Für den Bell-Zustand $|\Psi\rangle = \frac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big)$ ist $\gamma_{00} = \gamma_{11} = \frac{1}{\sqrt{2}}$ und $\gamma_{01} = \gamma_{10} = 0$, also

$$C(|\Psi\rangle) \;=\; 2 \cdot |\tfrac{1}{\sqrt{2}} \cdot \tfrac{1}{\sqrt{2}} - 0 \cdot 0| \;=\; 2 \cdot \tfrac{1}{2} \;=\; 1.$$

Der Zustand ist also maximal verschränkt.

Für $|\Psi_0\rangle = 0.8\,|00\rangle + 0.6\,|11\rangle$ ist

$$C(|\Psi_0\rangle) \;=\; 2 \cdot |0.8 \cdot 0.6 - 0 \cdot 0| \;=\; 0.96.$$

Für $|\Psi_1\rangle = 0.1\,|00\rangle + 0.7\,|01\rangle + 0.5\,|10\rangle + 0.5\,|11\rangle$ ist

$$C(|\Psi_1\rangle) \;=\; 2 \cdot |0.1 \cdot 0.5 - 0.7 \cdot 0.5| \;=\; 0.6.$$

Bemerkung:

Man kann zeigen, dass nach Anwendung einer unitären Transformation auf *ein* Qubit eines 2-Qubits-Registers sich die Concurrence nicht ändert; das gilt ebenso, wenn man auf die einzelnen Qubits *getrennte* unitäre Transformationen anwendet. Insbesondere bleiben maximal verschränkte Zustände weiterhin maximal verschränkt.

Beispiel:

Aus $|\Psi_1\rangle = 0.1\,|00\rangle + 0.7\,|01\rangle + 0.5\,|10\rangle + 0.5\,|11\rangle$ wird durch Anwendung von

$$U \;=\; \begin{pmatrix} 0.6 & -0.8 \\ 0.8 & 0.6 \end{pmatrix}$$

auf das erste Qubit der Zustand

$$\begin{aligned} |\Psi_2\rangle \;&=\; 0.1\big(0.6\,|0\rangle + 0.8\,|1\rangle\,\big) \otimes |0\rangle \;+\; 0.7\big(0.6\,|0\rangle + 0.8\,|1\rangle\,\big) \otimes |1\rangle \\ &\qquad + 0.5\big(-0.8\,|0\rangle + 0.6\,|1\rangle\,\big) \otimes |0\rangle \;+\; 0.5\big(-0.8\,|0\rangle + 0.6\,|1\rangle\,\big) \otimes |1\rangle \\ &=\; 0.06\,|00\rangle + 0.08\,|10\rangle \;+\; 0.42\,|01\rangle + 0.56\,|11\rangle \\ &\qquad - 0.4\,|00\rangle + 0.3\,|10\rangle \;+\; (-0.4)\,|01\rangle + 0.3\,|11\rangle \\ &=\; -0.34\,|00\rangle + 0.38\,|10\rangle + 0.02\,|01\rangle + 0.86\,|11\rangle\,. \end{aligned}$$

Es ist

$$C(|\Psi_2\rangle) \;=\; 2 \cdot |(-0.34) \cdot 0.86 - 0.38 \cdot 0.02| \;=\; 0.6 \;=\; C(|\Psi_1\rangle).$$

2.3 Messungen bei 2-Qubit-Registern

Messung beider Qubits:

Misst man bei einem Zustand

$$|\Psi\rangle \;=\; \gamma_{00}\,|00\rangle + \gamma_{01}\,|01\rangle + \gamma_{10}\,|10\rangle + \gamma_{11}\,|11\rangle$$

beide Qubits, so erhält man eines der vier Ergebnisse $|00\rangle$, $|01\rangle$, $|10\rangle$ bzw. $|11\rangle$ jeweils mit der Wahrscheinlichkeit $|\gamma_{00}|^2$, $|\gamma_{01}|^2$, $|\gamma_{10}|^2$ bzw. $|\gamma_{11}|^2$.

Beispiel:

Eine Messung beider Qubits bei

$$|\Psi\rangle \;=\; 0.3\,|00\rangle - 0.9\,|01\rangle + 0.1\,|10\rangle - 0.3\,|11\rangle$$

führt zu

$|00\rangle$ mit der Wahrscheinlichkeit $|0.3|^2 = 0.09$,

$|01\rangle$ mit der Wahrscheinlichkeit $|-0.9|^2 = 0.81$,

$|10\rangle$ mit der Wahrscheinlichkeit $|0.1|^2 = 0.01$,

$|11\rangle$ mit der Wahrscheinlichkeit $|-0.3|^2 = 0.09$.

Messung von einem Qubits:

Misst man bei einem Zustand

$$|\Psi\rangle \;=\; \gamma_{00}\,|00\rangle + \gamma_{01}\,|01\rangle + \gamma_{10}\,|10\rangle + \gamma_{11}\,|11\rangle$$

nur ein Qubit, so erhält man $|0\rangle$ oder $|1\rangle$, und je nach Messergebnis *kollabiert* der Zustand so, dass er nur noch eine Superposition zum entsprechend gemessenen Qubit ist, genauer:

Misst man das erste Qubit, so erhält man

$|0\rangle$ mit der Wahrscheinlichkeit $|\gamma_{00}|^2 + |\gamma_{01}|^2$;

der Zustand wird dann zu

$$|\Psi_0\rangle \;=\; \frac{\gamma_{00}}{\sqrt{|\gamma_{00}|^2 + |\gamma_{01}|^2}}\,|00\rangle + \frac{\gamma_{01}}{\sqrt{|\gamma_{00}|^2 + |\gamma_{01}|^2}}\,|01\rangle\,.$$

$|1\rangle$ mit der Wahrscheinlichkeit $|\gamma_{10}|^2 + |\gamma_{11}|^2$;

der Zustand wird dann zu

$$|\Psi_1\rangle \;=\; \frac{\gamma_{10}}{\sqrt{|\gamma_{10}|^2 + |\gamma_{11}|^2}}\,|10\rangle + \frac{\gamma_{11}}{\sqrt{|\gamma_{10}|^2 + |\gamma_{11}|^2}}\,|11\rangle\,.$$

Bei einem Messergebnis $|0\rangle$ sind also die Superpositionsanteile $|10\rangle$ und $|11\rangle$ verschwunden; die Vorfaktoren der Superpositionsanteile $|00\rangle$ und $|01\rangle$ werden so umskaliert, dass die Summe der Betragsquadrate wieder 1 ergibt.

Entsprechend ist es bei der Messung des zweiten Qubits.

Beispiel 1:

Betrachtet wird der separable Zustand

$$|\Psi\rangle \;=\; 0.3\,|00\rangle - 0.9\,|01\rangle + 0.1\,|10\rangle - 0.3\,|11\rangle\,.$$

Eine Messung des ersten Qubits führt zu

$|0\rangle$ mit der Wahrscheinlichkeit $|0.3|^2 + |-0.9|^2 = 0.9$;

der Zustand wird dann zu

$$|\Psi_0\rangle \;=\; \frac{0.3}{\sqrt{0.9}}\,|00\rangle - \frac{0.9}{\sqrt{0.9}}\,|01\rangle\,.$$

Wegen $\frac{1}{\sqrt{0.9}} = \frac{10}{\sqrt{90}} = \frac{10}{3\sqrt{10}}$, also $\frac{0.3}{\sqrt{0.9}} = \frac{1}{\sqrt{10}}$ und $\frac{0.9}{\sqrt{0.9}} = \frac{3}{\sqrt{10}}$ ist

$$|\Psi_0\rangle \;=\; \frac{1}{\sqrt{10}}\,|00\rangle - \frac{3}{\sqrt{10}}\,|01\rangle \;=\; |0\rangle \otimes \big(\frac{1}{\sqrt{10}}\,|0\rangle - \frac{3}{\sqrt{10}}\,|1\rangle\,\big).$$

$|1\rangle$ mit der Wahrscheinlichkeit $|0.1|^2 + |-0.3|^2 = 0.1$;

der Zustand wird dann zu

$$|\Psi_1\rangle \;=\; \frac{0.1}{\sqrt{0.1}}\,|10\rangle - \frac{0.3}{\sqrt{0.1}}\,|11\rangle\,.$$

Wegen $\frac{1}{\sqrt{0.1}} = \frac{10}{\sqrt{10}}$, also $\frac{0.1}{\sqrt{0.1}} = \frac{1}{\sqrt{10}}$ und $\frac{0.3}{\sqrt{0.1}} = \frac{3}{\sqrt{10}}$ ist

$$|\Psi_1\rangle \;=\; \frac{1}{\sqrt{10}}\,|10\rangle - \frac{3}{\sqrt{10}}\,|11\rangle \;=\; |1\rangle \otimes \big(\frac{1}{\sqrt{10}}\,|0\rangle - \frac{3}{\sqrt{10}}\,|1\rangle\,\big).$$

Dies ist konsistent mit der separierten Dartellung

$$|\Psi\rangle \;=\; \big(\tfrac{3}{\sqrt{10}}\,|0\rangle + \tfrac{1}{\sqrt{10}}\,|1\rangle\,\big) \otimes \big(\tfrac{1}{\sqrt{10}}\,|0\rangle - \tfrac{3}{\sqrt{10}}\,|1\rangle\,\big)\,:$$

Betrachtet man nur das erste Qubit $\frac{3}{\sqrt{10}}\,|0\rangle + \frac{1}{\sqrt{10}}\,|1\rangle$, so erhält man $|0\rangle$ mit der Wahrscheinlichkeit $|\frac{3}{\sqrt{10}}|^2 = \frac{9}{10} = 0.9$ und $|1\rangle$ mit der Wahrscheinlichkeit $|\frac{1}{\sqrt{10}}|^2 = \frac{1}{10} = 0.1$ wie oben. Das zweite Qubit entspricht dem zweiten Qubit des kollabierten Zustands.

Beispiel 2:

Betrachtet wird der verschränkte Zustand

$$|\Psi\rangle \;=\; 0.8\,|00\rangle + 0.4\,|01\rangle + 0.2\,|10\rangle - 0.4\,|11\rangle\,.$$

Eine Messung des *zweiten* Qubits führt zu

$|0\rangle$ mit der Wahrscheinlichkeit $|0.8|^2 + |0.2|^2 = 0.68$;

der Zustand wird dann zu

$$|\Psi_0\rangle \;=\; \frac{0.8}{\sqrt{0.68}}\,|00\rangle + \frac{0.2}{\sqrt{0.68}}\,|10\rangle \;\approx\; \big(0.97\cdot|0\rangle + 0.24\cdot|1\rangle\,\big)\otimes|0\rangle\,.$$

$|1\rangle$ mit der Wahrscheinlichkeit $|0.4|^2 + |-0.4|^2 = 0.32$;

der Zustand wird dann zu

$$|\Psi_1\rangle \;=\; \frac{0.4}{\sqrt{0.32}}\,|01\rangle - \frac{0.4}{\sqrt{0.32}}\,|11\rangle \;\approx\; \big(0.71\cdot|0\rangle - 0.71\cdot|1\rangle\,\big)\otimes|1\rangle\,.$$

Man sieht, dass je nach Messergebnis die jeweiligen ersten Qubit sehr verschieden sind.

Beispiel 3:

Misst man bei dem verschränkten Zustand

$$|\Psi\rangle \;=\; \tfrac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big)$$

das erste oder das zweite Qubit, so erhält man jeweils mit Wahrscheinlichkeit $\frac{1}{2}$ das Ergebnis $|0\rangle$ bzw. $|1\rangle$.

Das andere Qubit ist dann in dem gleichen Zustand, also $|0\rangle$ bzw. $|1\rangle$!

Weiteres zu Messungen bei diesem und ähnlichen Zuständen wird in Abschnitt 8.1.2 untersucht.

Messungen beider Qubits nacheinander:

Misst man bei einem Zustand

$$|\Psi\rangle \;=\; \gamma_{00}\,|00\rangle + \gamma_{01}\,|01\rangle + \gamma_{10}\,|10\rangle + \gamma_{11}\,|11\rangle$$

zunächst das eine und dann das andere Qubit, so erhält man die gleichen Wahrscheinlichkeiten wie bei gleichzeitiger Messung.

Beispielsweise ist die Wahrscheinlichkeit, bei der Messung des ersten Qubits $|0\rangle$ und dann bei der Messung des zweiten Qubits $|1\rangle$ zu erhalten gleich

$$\begin{aligned}
&\mathrm{P}(\text{bei der Messung des ersten Qubits } |0\rangle)\\
&\quad\cdot\,\mathrm{P}(\text{bei der anschließenden Messung des zweite Qubits } |1\rangle)\\
&= (|\gamma_{00}|^2 + |\gamma_{01}|^2)\cdot\left|\frac{\gamma_{01}}{\sqrt{|\gamma_{00}|^2 + |\gamma_{01}|^2}}\right|^2\\
&= (|\gamma_{00}|^2 + |\gamma_{01}|^2)\cdot\frac{|\gamma_{01}|^2}{|\gamma_{00}|^2 + |\gamma_{01}|^2} \;=\; |\gamma_{01}|^2.
\end{aligned}$$

2.4 n-Qubit-Register

Bei n Qubits gibt es 2^n Basiszustände:

$$|0\ldots00\rangle\,,\ |0\ldots01\rangle\,,\ldots,\ |1\ldots1\rangle\,.$$

Man nutzt hier auch eine alternative Schreibweise, indem man die Basiszustände als Binärzahl auffasst, z.B. bei drei Qubits

$$\begin{aligned}&|000\rangle = |0\rangle\,, \quad |001\rangle = |1\rangle\,, \quad |010\rangle = |2\rangle\,, \quad |011\rangle = |3\rangle\,,\\ &|100\rangle = |4\rangle\,, \quad |101\rangle = |5\rangle\,, \quad |110\rangle = |6\rangle\,, \quad |111\rangle = |7\rangle\,.\end{aligned}$$

Achtung:

Die Ausdrücke $|0\rangle$ und $|1\rangle$ sind nun doppeldeutig, und auch bei z.B. $|3\rangle$ ist ohne Weiteres unklar, wie groß das entsprechende Register ist.

Hier wird daher die Schreibweise $|\cdot\rangle_n$ genutzt, wenn der Ausdruck einen n-Qubit-Registerzustand beschreibt, also z.B. $|001\rangle = |1\rangle_3$.

Definition:

Ein Zustand $|\Psi\rangle$ eines n-Qubit-Registers wird beschrieben durch

$$|\Psi\rangle \;=\; \sum_{k=0}^{2^n-1} \gamma_k\,|k\rangle_n \quad \text{mit } \gamma_k \in \mathbb{C},\ k = 0,\ldots,2^n-1, \text{ und } \sum_{k=0}^{2^n-1} |\gamma_k|^2 = 1.$$

Man kann $|k\rangle_n$ auch als k-ten Einheitsvektor eines 2^n-dimensionalen Vektorraums auffassen; dann ist $|\Psi\rangle = \begin{pmatrix}\gamma_0\\ \vdots\\ \gamma_{2^n-1}\end{pmatrix}$.

Beispiel:

Ein Zustand $|\Psi\rangle$ eines 3-Qubit-Registers ist beispielsweise

$$\begin{aligned}&0.3\cdot|000\rangle + 0\cdot|001\rangle - 0.5\cdot|010\rangle + 0.3\cdot|011\rangle\\ &\quad + 0.4\cdot|100\rangle + 0.5\cdot|101\rangle + 0\cdot|110\rangle - 0.4\cdot|111\rangle\\ =\ &0.3\cdot|0\rangle_3 + 0\cdot|1\rangle_3 - 0.5\cdot|2\rangle_3 + 0.3\cdot|3\rangle_3\\ &\quad + 0.4\cdot|4\rangle_3 + 0.5\cdot|5\rangle_3 + 0\cdot|6\rangle_3 - 0.4\cdot|7\rangle_3\\ =\ &\begin{pmatrix}0.3\\0\\-0.5\\0.3\\0.4\\0.5\\0\\-0.4\end{pmatrix}.\end{aligned}$$

Durch das n-fache Tensorprodukt einfacher Qubits erhält man spezielle Zustände eines n-Qubit-Registers.

Beispiel:

Ein Zustand $|\Psi\rangle$ eines 3-Qubit-Registers ist beispielsweise

$$\begin{aligned}
&\big(0.8 \cdot |0\rangle + 0.6 \cdot |1\rangle\big) \otimes \big(0.6 \cdot |0\rangle - 0.8 \cdot |1\rangle\big) \otimes |1\rangle \\
&= 0.48 \cdot |001\rangle - 0.64 \cdot |011\rangle + 0.36 \cdot |101\rangle - 0.48 \cdot |111\rangle \\
&= 0.48 \cdot |1\rangle_3 - 0.64 \cdot |3\rangle_3 + 0.36 \cdot |5\rangle_3 - 0.48 \cdot |7\rangle_3 \\
&= \begin{pmatrix} 0 \\ 0.48 \\ 0 \\ -0.64 \\ 0 \\ 0.36 \\ 0 \\ -0.48 \end{pmatrix}.
\end{aligned}$$

Definition:

Man nennt den Zustand $|\Psi\rangle$ eines n-Qubit-Registers *separabel* oder *unverschränkt*, wenn man $|\Psi\rangle$ als Tensorprodukt von n Qubits $|\Psi_1\rangle, \ldots, |\Psi_n\rangle$ darstellen kann:

$$|\Psi\rangle \;=\; |\Psi_1\rangle \otimes \ldots \otimes |\Psi_n\rangle\,.$$

Andernfalls heißt $|\Psi\rangle$ *verschränkt*.

Bemerkung:

Eine notwendige Bedingung, dass ein Zustand unverschränkt ist, ist beispielsweise, dass in der vektoriellen Darstellung die obere und die untere Hälfte linear abhängig sind, da

$$\begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} \otimes |\Psi_2\rangle \otimes \ldots \otimes |\Psi_n\rangle \;=\; \begin{pmatrix} \alpha_1 \cdot \Phi \\ \beta_1 \cdot \Phi \end{pmatrix} \text{ mit } \Phi = |\Psi_2\rangle \otimes \ldots \otimes |\Psi_n\rangle.$$

Messung von einem Qubits:

Misst man bei einem Zustand $|\Psi\rangle$ eines n-Qubit-Registers das k-te Qubit, so erhält man $|0\rangle$ bzw. $|1\rangle$ mit Wahrscheinlichkeiten entsprechend der Summe der Betragsquadrate der Vorfaktoren zu den Basiszuständen, die an der k-ten Stelle eine 0 bzw. eine 1 haben.

Je nach Messergebnis *kollabiert* der Zustand so, dass er nur noch eine Superposition zum entsprechend gemessenen Qubit an der k-ten Stelle ist; die Vorfaktoren werden so umskaliert, dass die Summe der Betragsquadrate gleich 1 ist.

Beispiel 1:

Eine Messung des ersten Qubits beim Zustands $|\Psi\rangle$ eines 3-Qubit-Registers mit

$$\begin{aligned}
|\Psi\rangle \;&= 0.3 \cdot |000\rangle + 0 \cdot |001\rangle - 0.5 \cdot |010\rangle + 0.3 \cdot |011\rangle \\
&\quad + 0.4 \cdot |100\rangle + 0.5 \cdot |101\rangle + 0 \cdot |110\rangle - 0.4 \cdot |111\rangle
\end{aligned}$$

liefert beispielsweise das Ergebnis $|1\rangle$ mit der Wahrscheinlichkeit

$$|0.4|^2 + |0.5|^2 + |0|^2 + |-0.4|^2 \;=\; 0.57.$$

Der Zustand wird dabei zu

$$\tfrac{1}{\sqrt{0.57}} \cdot \big(0.4 \cdot |100\rangle + 0.5 \cdot |101\rangle + 0 \cdot |110\rangle - 0.4 \cdot |111\rangle\big).$$

Beispiel 2:

Eine Messung des zweiten Qubits beim unverschränkten Zustand $|\Psi\rangle$ eines 3-Qubit-Registers mit

$$\begin{aligned} |\Psi\rangle &= \big(0.8 \cdot |0\rangle + 0.6 \cdot |1\rangle\big) \otimes \big(0.6 \cdot |0\rangle - 0.8 \cdot |1\rangle\big) \otimes |1\rangle \\ &= 0.48 \cdot |001\rangle - 0.64 \cdot |011\rangle + 0.36 \cdot |101\rangle - 0.48 \cdot |111\rangle \end{aligned}$$

liefert beispielsweise das Ergebnis $|0\rangle$ mit der Wahrscheinlichkeit

$$|0.48|^2 + |0.36|^2 \;=\; 0.36.$$

Dies ist konsistent zum Vorfaktor 0.6 zu $|0\rangle$ beim zweiten Qubit.

Der Zustand wird nach einer Messung von $|0\rangle$ zu

$$\begin{aligned} &\tfrac{1}{\sqrt{0.36}} \cdot \big(0.48 \cdot |001\rangle + 0.36 \cdot |101\rangle\big) \\ =\; &\tfrac{0.48}{0.6} \cdot |001\rangle + \tfrac{0.36}{0.6} \cdot |101\rangle \\ =\; &\big(0.8 \cdot |0\rangle + 0.6 \cdot |1\rangle\big) \otimes |01\rangle\,, \end{aligned}$$

in Konsistenz mit der separierten Darstellung von $|\Psi\rangle$.

Entsprechendes gilt bei der Messung von mehreren Qubits eines Registers.

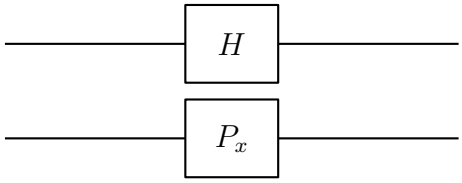
Die Messung mehrerer Qubits ergibt das Gleiche wie die Nacheinander-Ausführung von einzelnen Messungen.

3 Quantengatter

3.1 Modifikationen bei mehreren Qubits

3.1.1 Ein Beispiel

Bei einem 2-Qubit-Register soll auf das erste Qubit ein Hadamard-Gatter und auf das zweite ein Pauli-X-Gatter angewendet werden.



Die entsprechenden (2×2)-Transformationsmatrizen sind

$$H = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \quad \text{und} \quad P_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Aus einem Zustand

$$\begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} \otimes \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{pmatrix}$$

wird dann

$$\begin{aligned}
&\left(H \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix}\right) \otimes \left(P_x \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix}\right) \\
&= \left(\begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix}\right) \otimes \left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix}\right) \\
&= \begin{pmatrix} \frac{1}{\sqrt{2}}\alpha_1 + \frac{1}{\sqrt{2}}\beta_1 \\ \frac{1}{\sqrt{2}}\alpha_1 - \frac{1}{\sqrt{2}}\beta_1 \end{pmatrix} \otimes \begin{pmatrix} \beta_2 \\ \alpha_2 \end{pmatrix} = \begin{pmatrix} \left(\frac{1}{\sqrt{2}}\alpha_1 + \frac{1}{\sqrt{2}}\beta_1\right) \cdot \begin{pmatrix} \beta_2 \\ \alpha_2 \end{pmatrix} \\ \left(\frac{1}{\sqrt{2}}\alpha_1 - \frac{1}{\sqrt{2}}\beta_1\right) \cdot \begin{pmatrix} \beta_2 \\ \alpha_2 \end{pmatrix} \end{pmatrix} \\
&= \begin{pmatrix} \left(\frac{1}{\sqrt{2}}\alpha_1 + \frac{1}{\sqrt{2}}\beta_1\right) \cdot \beta_2 \\ \left(\frac{1}{\sqrt{2}}\alpha_1 + \frac{1}{\sqrt{2}}\beta_1\right) \cdot \alpha_2 \\ \left(\frac{1}{\sqrt{2}}\alpha_1 - \frac{1}{\sqrt{2}}\beta_1\right) \cdot \beta_2 \\ \left(\frac{1}{\sqrt{2}}\alpha_1 - \frac{1}{\sqrt{2}}\beta_1\right) \cdot \alpha_2 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}}\alpha_1\beta_2 + \frac{1}{\sqrt{2}}\beta_1\beta_2 \\ \frac{1}{\sqrt{2}}\alpha_1\alpha_2 + \frac{1}{\sqrt{2}}\beta_1\alpha_2 \\ \frac{1}{\sqrt{2}}\alpha_1\beta_2 - \frac{1}{\sqrt{2}}\beta_1\beta_2 \\ \frac{1}{\sqrt{2}}\alpha_1\alpha_2 - \frac{1}{\sqrt{2}}\beta_1\alpha_2 \end{pmatrix} \\
&= \begin{pmatrix} 0 & 1/\sqrt{2} & 0 & 1/\sqrt{2} \\ 1/\sqrt{2} & 0 & 1/\sqrt{2} & 0 \\ 0 & 1/\sqrt{2} & 0 & -1/\sqrt{2} \\ 1/\sqrt{2} & 0 & -1/\sqrt{2} & 0 \end{pmatrix} \cdot \begin{pmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{pmatrix}.
\end{aligned}$$

3.1.2 Ein bisschen Mathematik: Tensorprodukt von Matrizen

Man erkennt bei der Matrix U aus dem vorherigen Abschnitt eine Struktur, die man durch ein Tensorprodukt von Matrizen beschreiben kann:

$$\begin{aligned} U &= \begin{pmatrix} 0 & 1/\sqrt{2} & 0 & 1/\sqrt{2} \\ 1/\sqrt{2} & 0 & 1/\sqrt{2} & 0 \\ 0 & 1/\sqrt{2} & 0 & -1/\sqrt{2} \\ 1/\sqrt{2} & 0 & -1/\sqrt{2} & 0 \end{pmatrix} \\ &= \begin{pmatrix} \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & -\frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{pmatrix} \\ &= \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = H \otimes P_x. \end{aligned}$$

Definition:

Zu zwei Matrizen $A, S \in \mathbb{C}^{2\times 2}$ ist das Tensorprodukt $A \otimes S \in \mathbb{C}^{4\times 4}$ definiert durch

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} s & t \\ u & v \end{pmatrix} = \begin{pmatrix} a \cdot \begin{pmatrix} s & t \\ u & v \end{pmatrix} & b \cdot \begin{pmatrix} s & t \\ u & v \end{pmatrix} \\ c \cdot \begin{pmatrix} s & t \\ u & v \end{pmatrix} & d \cdot \begin{pmatrix} s & t \\ u & v \end{pmatrix} \end{pmatrix} = \begin{pmatrix} as & at & bs & bt \\ au & av & bu & bv \\ cs & ct & ds & dt \\ cu & cv & du & dv \end{pmatrix}.$$

Entsprechend definiert man das Tensorprodukt von $A \in \mathbb{C}^{m_A \times n_A}$ und $S \in \mathbb{C}^{m_S \times n_S}$ als $A \otimes S \in \mathbb{C}^{(m_A \cdot m_S)\times(n_A \cdot n_S)}$.

Beispiel 1:

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 & 0 & 3 & 0 \\ 0 & 1 & 0 & 2 & 0 & 3 \\ 4 & 0 & 5 & 0 & 6 & 0 \\ 0 & 4 & 0 & 5 & 0 & 6 \end{pmatrix}.$$

Beispiel 2:

Sind I_m bzw. I_n die m- bzw. n-dimensionale Einheitsmatrix, so ist $I_m \otimes I_n = I_{m\cdot n}$, z.B.

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

Bemerkungen:

1. Die Definition des Tensorprodukts von Matrizen umfasst offensichtlich das Tensorprodukt von Vektoren, wenn man Vektoren als einspaltige Matrizen auffasst.
2. Beim Tensorprodukt von Matrizen kann man offensichtlich intuitiv mit Konstanten umgehen.

   Beispiel:

$$H \otimes H = \left(\tfrac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\right) \otimes \left(\tfrac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\right)$$

$$= \frac{1}{2} \cdot \left(\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \otimes \begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\right) = \frac{1}{2}\begin{pmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{pmatrix}.$$

Verträglichkeit des Matrix-Vektor-Produkts mit dem Tensorprodukt:

Man kann (elementar aber etwas mühsam) nachrechnen, dass gilt:

Zu $a \in \mathbb{C}^{n_A}$, $A \in \mathbb{C}^{m_A \times n_A}$, $s \in \mathbb{C}^{n_S}$, und $S \in \mathbb{C}^{m_S \times n_S}$ gilt

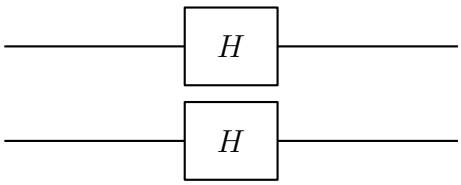
$$(A \cdot a) \otimes (S \cdot s) = (A \otimes S) \cdot (a \otimes s).$$

Interpretation für Qubit-Transformationen:

Einzel-Qubit-Transformationen, die durch A bzw. S beschrieben werden, kann man also zusammenfassen durch die Matrix-Vektor-Multiplikation von $A \otimes S$ auf den Gesamtzustand.

Beispiel:

Die Matrix $H \otimes H = \frac{1}{2}\begin{pmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{pmatrix}$ (vgl. oben) beschreibt die (gleichzeitige) Ausführung der Hadamard-Transformation auf die beiden Qubits eines 2-Qubit-Registers:



Die Verträglichkeit des Matrix-Vektor-Produkts mit dem Tensorprodukt ist ein Spezialfall (für einspaltige Matrizen B und T) des folgenden Satzes, den man (elementar aber etwas mühsam) nachrechnen kann.

Satz:

Sind A, B, S und T Matrizen, so dass man $A \cdot B$ und $S \cdot T$ bilden kann, so gilt

$$(A \cdot B) \otimes (S \cdot T) = (A \otimes S) \cdot (B \otimes T).$$

Bemerkung:

Es gilt

$$(A \otimes B)^H \;=\; A^H \otimes B^H.$$

Dies kann man sich an folgendem Beispiel illustrieren:

$$\left(\begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} \otimes U\right)^H \;=\; \begin{pmatrix} a \cdot U & b \cdot U & c \cdot U \\ d \cdot U & e \cdot U & f \cdot U \end{pmatrix}^H$$

$$= \begin{pmatrix} a^* \cdot U^H & d^* \cdot U^H \\ b^* \cdot U^H & e^* \cdot U^H \\ c^* \cdot U^H & f^* \cdot U^H \end{pmatrix} \;=\; \begin{pmatrix} a^* & d^* \\ b^* & e^* \\ c^* & f^* \end{pmatrix} \otimes U^H$$

$$= \begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix}^H \otimes U^H.$$

Tensorprodukt unitärer Matrizen ist wieder unitär:

Mit dem Satz und der Bemerkung oben kann man nachweisen, dass das Tensorprodukt $U \otimes V$ zweier unitärer Matrizen U und V wieder unitär ist:

Sind die Matrizen U und V unitär, so gilt $U^H \cdot U = I$ und $V^H \cdot V = I$ mit I als der Einheitsmatrix (gegebenenfalls zu unterschiedlichen Dimensionen). Damit gilt

$$\begin{aligned} & (U \otimes V)^H \cdot (U \otimes V) \\ \overset{\text{Bemerkung}}{=} \; & \left(U^H \otimes V^H\right) \cdot (U \otimes V) \\ \overset{\text{Satz}}{=} \; & \left(U^H \cdot U\right) \otimes \left(V^H \cdot V\right) \\ = \; & I \otimes I = I. \end{aligned}$$

Also ist $(U \otimes V)^H = (U \otimes V)^{-1}$ und damit $U \otimes V$ unitär.

3.1.3 Gatter bei n-Qubit-Registern

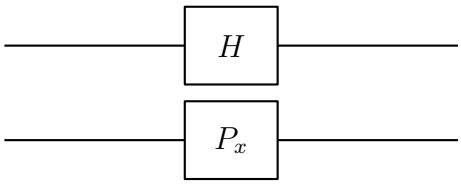
Modifikationen bei einem n-Qubit-Register werden beschrieben durch eine Matrix-Vektor-Multiplikation von einer unitären $\mathbb{C}^{2^n \times 2^n}$-Matrix U mit dem entsprechenden Zustand als Vektor im $\mathbb{C}^{2^n}$. In diesem Zusammenhang spricht man auch von *Gattern*.

Wirkt die Modifikation getrennt auf die einzelnen Qubits, so ergibt sich die Matrix U als Tensorprodukt der einzelnen Modifikationen. Dass das Tensorprodukt unitärer Matrizen tatsächlich wieder unitär ist, wurde oben nachgewiesen.

Es gibt aber auch Modifikationen, die auf mehrere Qubits gemeinsam wirken, und die man nicht als Tensorprodukt einzelner Modifikationen zerlegen kann. Beispiele dazu gibt es in Abschnitt 3.2.

Beispiel:

Der Schaltkreis



wird durch die Matrix

$$U \;=\; H \otimes P_x \;=\; \begin{pmatrix} 0 & 1/\sqrt{2} & 0 & 1/\sqrt{2} \\ 1/\sqrt{2} & 0 & 1/\sqrt{2} & 0 \\ 0 & 1/\sqrt{2} & 0 & -1/\sqrt{2} \\ 1/\sqrt{2} & 0 & -1/\sqrt{2} & 0 \end{pmatrix}$$

(s. Seite 30) beschrieben. Man kann leicht nachrechnen, dass U unitär ist.

Alternative Beschreibung eines Gatters:

Statt durch eine Matrix kann man ein Gatter bei einem n-Qubit-Register auch durch die Auswirkung auf die 2^n Basiszustände $|0\ldots00\rangle$, $|0\ldots01\rangle$, …, $|1\ldots11\rangle$ festlegen.

Beispiel:

Bei einem 2-Qubit-Register wird ein Gatter eindeutig festgelegt durch die Festlegung der Abbildungen

$$|00\rangle \mapsto \tfrac{1}{\sqrt{2}}\big(\,|01\rangle + |11\rangle\,\big), \qquad |01\rangle \mapsto \tfrac{1}{\sqrt{2}}\big(\,|00\rangle + |10\rangle\,\big)$$
$$|10\rangle \mapsto \tfrac{1}{\sqrt{2}}\big(\,|01\rangle - |11\rangle\,\big), \qquad |11\rangle \mapsto \tfrac{1}{\sqrt{2}}\big(\,|00\rangle - |10\rangle\,\big).$$

Dies entspricht der durch $H \otimes P_x$ beschriebenen Transformation.

Dies kann man einerseits durch Vergleich der Spalten der zu $H \otimes P_x$ gehörigen Matrix U (s. oben) mit der Zuordnungsvorschrift sehen.

Andererseits kann man umformen:

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

Genauso wie nicht durch beliebige Matrizen sondern nur durch unitäre Matrizen reguläre Gatter beschrieben werden, gehört auch nicht jede beliebige Zuordnung von Basiszuständen zu Zielzuständen zu einem regulären Gatter.

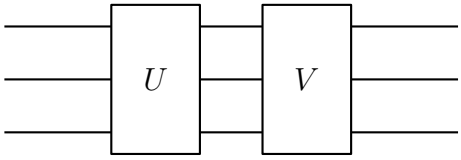
Mehrere Transformationen:

Führt man auf einem Quantenregister mehrere Transformationen nacheinander aus, z.B. zunächst eine Transformation U und dann eine Transformation V, so kann man

die Wirkung der gesamten Transformation T durch die Matrix

$$T \;=\; V \cdot U$$

beschreiben.



Man beachte die Reihenfolge: Das Bild liest man von links nach rechts. Da zuerst U und dann V ausgeführt wird, muss bei einer vektoriellen Berechnung auf einen Zustand $|\Psi\rangle$ zunächst $U \cdot |\Psi\rangle$ berechnet werden. Auf diesen Zustand wirkt dann V. Daher steht die Matrix V beim Produkt auf der linken Seite.

3.1.4 Hadamard-Transformation für jedes Qubit

Häufig beginnt ein Quantenalgorithmus auf einem n-Qubit-Register damit, dass man das Register mit $|0\rangle_n = |0\ldots0\rangle$ initialisiert und dann auf jedes Qubit eine Hadamard-Trasformation anwendet, also

$$H^{\otimes n} \;:=\; H \otimes H \otimes \ldots \otimes H.$$

Bei der Anwendung von $H^{\otimes n}$ auf $|0\rangle_n$ erhält man

$$\begin{aligned}
&\Big(\tfrac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big)\Big) \otimes \Big(\tfrac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big)\Big) \otimes \ldots \Big(\tfrac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big)\Big) \\
&= \frac{1}{2^{n/2}} \cdot \big(\,|0\rangle + |1\rangle\,\big) \otimes \big(\,|0\rangle + |1\rangle\,\big) \otimes \ldots \big(\,|0\rangle + |1\rangle\,\big).
\end{aligned}$$

Beim Ausmultiplizieren erhält man jede n-fache Kombination aus $|0\rangle$ und $|1\rangle$, also jedes $|k\rangle_n$, $k = 0, \ldots, 2^n - 1$. Also gilt:

$$H^{\otimes n}\,|0\rangle_n \;=\; \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} |k\rangle_n\,.$$

Wie wirkt $H^{\otimes n}$ auf einen Basiszustand $|x\rangle_n$ mit $x \in \{0, \ldots, 2^n - 1\}$?

Sei beispielhaft $n = 5$ und $x = 13$, also $|13\rangle_5 = |01101\rangle$:

$$\begin{aligned}
&H^{\otimes 5}\,|01101\rangle \\
&= \big(H\,|0\rangle\,\big) \otimes \big(H\,|1\rangle\,\big) \otimes \big(H\,|1\rangle\,\big) \otimes \big(H\,|0\rangle\,\big) \otimes \big(H\,|1\rangle\,\big) \\
&= \Big(\tfrac{1}{\sqrt{2}}\Big)^5 \cdot \big(\,|0\rangle + |1\rangle\,\big) \otimes \big(\,|0\rangle - |1\rangle\,\big) \otimes \big(\,|0\rangle - |1\rangle\,\big) \otimes \big(\,|0\rangle + |1\rangle\,\big) \otimes \big(\,|0\rangle - |1\rangle\,\big).
\end{aligned}$$

Beim Ausmultiplizieren erhält man wieder jede 5-fache Kombination aus $|0\rangle$ und $|1\rangle$, allerdings je nach dem mit einem $+$- oder einem $-$-Vorzeichen. Beispielsweise sind die Vorzeichen

von $|0\rangle_5 = |00000\rangle$: $+,+,+,+,+$, im Produkt also $+1$.

von $|31\rangle_5 = |11111\rangle$: $+,-,-,+,-$, im Produkt also -1.

von $|25\rangle_5 = |11001\rangle$: $+,-,+,+,-$, im Produkt also $+1$.

von $|19\rangle_5 = |10011\rangle$: $+,+,+,+,-$, im Produkt also -1.

Man sieht: Betrachtet man $|k\rangle_n$, so entsteht „$-$“ an der Stelle s genau dann, wenn sowohl das s-te Bit in der Binärdarstellung von $x = 13$ als auch bei k gleich 1 ist. Ist x_s bzw. k_s das entsprechende Bit, so erhält man „$-$“ also genau dann, wenn $x_s \cdot k_s = 1$ ist. Kommt dies für alle Bits gesehen ungerade-oft vor, so erhält man ein $-$-Vorzeichen, kommt es gerade-oft vor, so erhält man ein $+$-Vorzeichen.

Dies motiviert die folgende Definition:

Definition:

Seien $x = (x_{n-1} \dots x_1 x_0)_2$ und $k = (k_{n-1} \dots k_1 k_0)_2$ die Binärdarstellungen von $x, k \in \{0, \dots, 2^n - 1\}$. Dann sei

$$x \odot k \;:=\; x_{n-1} \cdot k_{n-1} \oplus \dots \oplus x_1 \cdot k_1 \oplus x_0 \cdot k_0.$$

Dabei ist „$\oplus$“ das übliche XOR von Bits.

Beispiel:

Zu $13 = (01101)_2$ und

$0 = (00000)_2$ erhält man: $13 \odot 0 = 0 \cdot 0 \oplus 1 \cdot 0 \oplus 1 \cdot 0 \oplus 0 \cdot 1 \oplus 1 \cdot 0 = 0$,

$31 = (11111)_2$ erhält man: $13 \odot 31 = 0 \cdot 1 \oplus 1 \cdot 1 \oplus 1 \cdot 1 \oplus 0 \cdot 1 \oplus 1 \cdot 1 = 1$,

$25 = (11001)_2$ erhält man: $13 \odot 25 = 0 \cdot 1 \oplus 1 \cdot 1 \oplus 1 \cdot 0 \oplus 0 \cdot 0 \oplus 1 \cdot 1 = 0$,

$19 = (10011)_2$ erhält man: $13 \odot 19 = 0 \cdot 1 \oplus 1 \cdot 0 \oplus 1 \cdot 0 \oplus 0 \cdot 1 \oplus 1 \cdot 1 = 1$.

Bei $x \in \{0, \dots, 2^n - 1\}$ ergibt sich durch $H^{\otimes n} |x\rangle_n$ eine Überlagerung aller Basiszustände $|k\rangle_n$, $k \in \{0, \dots, 2^n - 1\}$, wobei $|k\rangle_n$ ein $+$-Vorzeichen hat, wenn $x \odot k = 0$ ist, und ein $-$-Vorzeichen, wenn $x \odot k = 1$ ist. Dies kann man in jedem Fall durch $(-1)^{x \odot k}$ ausdrücken.

Insgesamt erhält man:

Satz:

Für $x \in \{0, \dots, 2^n - 1\}$ gilt

$$H^{\otimes n} |x\rangle_n \;=\; \frac{1}{2^{n/2}} \sum_{k=0}^{2^n - 1} (-1)^{x \odot k} |k\rangle_n .$$

3.2 Spezielle Gatter bei 2-Qubit-Registern

3.2.1 CNOT-Gatter

Ziel ist das Quanten-Computing-Pendant zum klassischen XOR-Operator.

Der klassische XOR-Operator hat am Eingang zwei klassische Bits x und y und am Ausgang die XOR-Verknüpfung $x \oplus y$ mit

$$0 \oplus 0 \;=\; 1 \oplus 1 \;=\; 0 \qquad \text{und} \qquad 0 \oplus 1 \;=\; 1 \oplus 0 \;=\; 1.$$

Quanten-Computing-Gatter werden durch unitäre Transformationen beschrieben. Insbesondere sind sie also umkehrbar und müssen daher genau so viele Eingabe- wie Ausgabe-Qubits besitzen. Dies kann man beispielsweise erreichen, indem ein Eingabe-Qubit mit zum Ausgang hin „durchgeschleift“ wird, also z.B. mit einer Abbidung

$$(x, y) \;\mapsto\; (x, x \oplus y).$$

Damit sind die Bilder der Basiszustände eines 2-Qubit-Registers festgelegt:

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

Man kann die Zuordnung auch folgendermaßen interpretieren:

Das zweite Bit wird negiert genau dann, wenn das erste gleich 1 ist.

Identifiziert man die Basiszustände wie üblich mit Einheitsvektoren, also

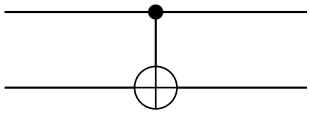
$$|00\rangle \;=\; \begin{pmatrix} 1\\0\\0\\0 \end{pmatrix}, \quad |01\rangle \;=\; \begin{pmatrix} 0\\1\\0\\0 \end{pmatrix}, \quad |10\rangle \;=\; \begin{pmatrix} 0\\0\\1\\0 \end{pmatrix}, \quad |11\rangle \;=\; \begin{pmatrix} 0\\0\\0\\1 \end{pmatrix},$$

so wird die Zuordnung durch die Matrix

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

beschrieben. Diese Matrix ist offensichtlich unitär und stellt damit ein Gatter für ein 2-Qubit-Register dar. Auf Grund der obigen Interpretationen wird es *controlled-NOT-Gatter* genannt.

Im Blockschaltbild wird das Kontroll-Qubit mit einem Punkt und das Ziel-Qubit mit einem $\oplus$-Symbol markiert:



Auf einen beliebigen Zustand $|\Psi\rangle$ eines 2-Qubit-Registers,

$$|\Psi\rangle \;=\; \gamma_{00}\,|00\rangle + \gamma_{01}\,|01\rangle + \gamma_{10}\,|10\rangle + \gamma_{11}\,|11\rangle$$

angewendet, liefert das CNOT-Gatter den Zustand

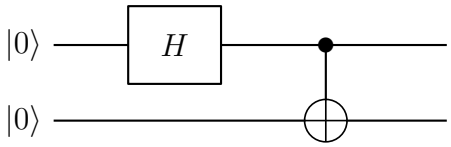
$$\gamma_{00}\,|00\rangle + \gamma_{01}\,|01\rangle + \gamma_{10}\,|11\rangle + \gamma_{11}\,|10\rangle \;=\; \gamma_{00}\,|00\rangle + \gamma_{01}\,|01\rangle + \gamma_{11}\,|10\rangle + \gamma_{10}\,|11\rangle\,.$$

Dies sieht man auch bei der vektoriellen Darstellung:

$$|\Psi\rangle = \begin{pmatrix}\gamma_{00}\\ \gamma_{01}\\ \gamma_{10}\\ \gamma_{11}\end{pmatrix} \;\mapsto\; \mathrm{CNOT}(|\Psi\rangle) \;=\; \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\cdot\begin{pmatrix}\gamma_{00}\\ \gamma_{01}\\ \gamma_{10}\\ \gamma_{11}\end{pmatrix} \;=\; \begin{pmatrix}\gamma_{00}\\ \gamma_{01}\\ \gamma_{11}\\ \gamma_{10}\end{pmatrix}.$$

Erzeugung des Bell-Zustands:

Welcher Zustand wird durch das folgende Blockschaltbild erzeugt?



Nach dem Hadamard-Gatter wird das erste Qubit zu $\frac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big)$. Der Gesamtzustand ist dann

$$\tfrac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big)\otimes|0\rangle \;=\; \tfrac{1}{\sqrt{2}}\big(\,|00\rangle + |10\rangle\,\big).$$

Durch die Anwendung des CNOT-Gatters wird dies zum Bell-Zustand

$$\tfrac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big).$$

Auf diese Weise erhält man also aus zwei unverschränkten Qubits einen verschränkten Zustand.

Matrix-Darstellung:

Da die Hadamard-Transformation nur auf das erste Qubit wirkt, kann man dies durch

$$H\otimes I \;=\; \tfrac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&1\end{pmatrix} \;=\; \tfrac{1}{\sqrt{2}}\begin{pmatrix}1&0&1&0\\0&1&0&1\\1&0&-1&0\\0&1&0&-1\end{pmatrix}$$

darstellen.

Die anschließende CNOT-Transformation wird durch die CNOT-Matrix beschrieben, die Gesamt-Transformation T also durch das Matrix-Produkt (beachte die Reihenfolge!)

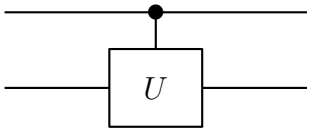
$$T := \mathrm{CNOT} \cdot (H \otimes I) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$$
$$= \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix}.$$

Die Wirkung auf $|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ ist dann

$$T \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

3.2.2 Allgemeine kontrollierte Gatter

Zu einer beliebigen Transformation U, die auf ein Qubit wirkt, kann man das entsprechend durch ein anderes Qubit kontrollierte Gatter betrachten:



Dies bedeutet für Basiszustände, dass das U-Gatter nur dann ausgeführt wird, wenn das Kontroll-Qubit gleich $|1\rangle$ ist, beim ersten Qubit als Kontroll-Qubit also

$$|00\rangle \mapsto |00\rangle, \quad |01\rangle \mapsto |01\rangle, \quad |10\rangle \mapsto \big(|1\rangle \otimes U|0\rangle\big), \quad |11\rangle \mapsto \big(|1\rangle \otimes U|1\rangle\big).$$

Die entsprechende Transformationsmatrix hat dann die Block-Struktur $\left(\begin{smallmatrix} I & 0 \\ 0 & U \end{smallmatrix}\right)$, also bei $U = \left(\begin{smallmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{smallmatrix}\right)$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{pmatrix}.$$

Beispiel:

Das Pauli-X-Gatter vertauscht die Basiszustände, $P_X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.

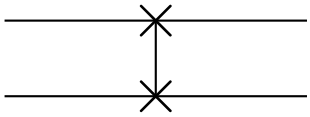
Das vom ersten Qubit kontrollierte Pauli-X-Gatter auf dem zweiten Qubit hat dann also die Transformationsmatrix

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

Dies entspricht genau der CNOT-Transformation, wie man sich auch durch die Abbildung der Basiszustände klar machen kann.

3.2.3 Swap Gatter

Das Swap-Gatter



vertauscht $|01\rangle$ und $|10\rangle$ und damit die beiden Qubits:

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

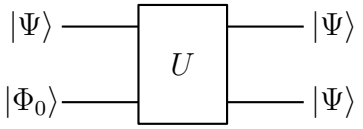
Die Abbildungsmatrix ist

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

3.3 No-cloning-Theorem

Kann es einen Quanten-Schaltkreis geben, der ein Qubit kopiert?

Da eine entsprechende Transformation unitär sein muss, und man am Ausgang zwei Qubits haben möchte (das originale und das kopierte), braucht man auch am Eingang zwei Qubits.



Ziel ist also eine Transformation U, die zwei Qubits $|\Psi\rangle$ und $|\Phi_0\rangle$ entgegennimmt und das eine kopiert, also

Für alle $|\Psi\rangle$ gilt: $U\big(|\Psi\rangle \otimes |\Phi_0\rangle\big) = |\Psi\rangle \otimes |\Psi\rangle\,.$

Bemerkung:

Es reicht dabei aus, wenn U nur bei einem bestimmten zweiten Qubit $|\Phi_0\rangle$ kopiert (man könnte hier auch o.B.d.A $|0\rangle$ nehmen); es braucht nicht bei allen $|\Phi\rangle$ zu kopieren; das wäre auch gar nicht möglich, denn dann wäre die Abbildung nicht invertierbar und damit auch nicht unitär, da z.B. sowohl $|00\rangle$ als auch $|01\rangle$ auf $|00\rangle$ abgebildet würden.

Es gilt also insbesondere

$$U\big(|0\rangle \otimes |\Phi_0\rangle\big) = |00\rangle \qquad \text{und} \qquad U\big(|1\rangle \otimes |\Phi_0\rangle\big) = |11\rangle\,.$$

Was ist dann $U\big(|\Psi\rangle \otimes |\Phi_0\rangle\big)$ mit $|\Psi\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)$?

Wegen der Kopier-Eigenschaft gilt einerseits

$$\begin{aligned} U\Big(\tfrac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \otimes |\Phi_0\rangle\Big) &= \tfrac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \otimes \tfrac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \\ &= \tfrac{1}{2}\big(|00\rangle + |01\rangle + |10\rangle + |11\rangle\big). \end{aligned}$$

Wegen der Linearität von U gilt andererseits

$$\begin{aligned} U\Big(\frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \otimes |\Phi_0\rangle\Big) &= U\Big(\tfrac{1}{\sqrt{2}}|0\rangle \otimes |\Phi_0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle \otimes |\Phi_0\rangle\Big) \\ &= \tfrac{1}{\sqrt{2}}U\Big(|0\rangle \otimes |\Phi_0\rangle\Big) + \tfrac{1}{\sqrt{2}}U\Big(|1\rangle \otimes |\Phi_0\rangle\Big) \\ &= \tfrac{1}{\sqrt{2}}|00\rangle + \tfrac{1}{\sqrt{2}}|11\rangle\,. \end{aligned}$$

Damit hat man einen Widerspruch! Eine solche Transformation kann es also nicht geben.

Es gilt allgemein:

No-cloning-Theorem:

Man kann ein Qubit nicht kopieren.

4 Deutsch- und Deutsch-Jozsa-Algorithmus

4.1 Deutsch–Algorithmus

Problemstellung:

Es soll untersucht werden, ob eine Münze zwei gleiche Seiten oder zwei verschiedene Seiten besitzt.

In der klassischen Welt muss man dazu die beiden Seiten der Münze betrachten, also zwei Blicke auf die Münze werfen.

Der Algorithmus von Deutsch (benannt nach David Deutsch) erlaubt, die Fragestellung mit *einem* „Blick“ auf die Münze zu beantworten.

Mathematische Formulierung:

Die beiden Seiten der Münze kann man mit 0 und 1 bezeichnen, und auch das, was auf der Münze steht kann man als 0 oder 1 auffassen, so dass man die Münze modellieren kann als Funktion

$$f : \{0,1\} \to \{0,1\}.$$

Die Frage ist dann,

ob $f(0) = f(1)$ (die beiden Seiten der Münze sind gleich) oder

ob $f(0) \neq f(1)$ (die beiden Seiten der Münze sind verschieden) gilt.

Klassisch muss man zur Beantwortung der Frage $f(0)$ und $f(1)$ berechnen, also die Funktion f zwei Mal auswerten. Der Algorithmus von Deutsch erlaubt, die Fragestellung mit *einer* Auswertung von f zu beantworten.

In dem Zusammenhang bezeichnet man die Funktion f auch als *Black-Box* oder als *Orakel*. Klassisch muss man das Orakel zwei Mal befragen, der Algorithmus von Deutsch kommt mit einer Befragung aus.

Quantenversion des Orakels:

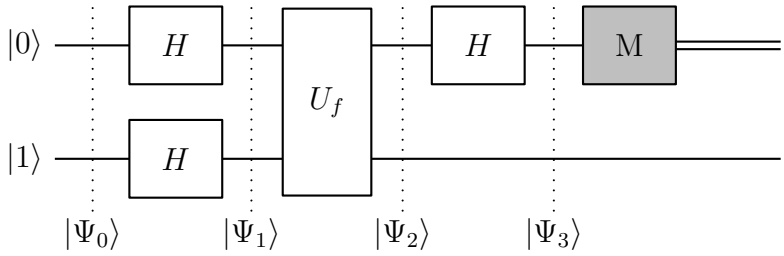
Für eine Quanten-Version des Orakels braucht man eine unitäre Transformation, in der f vorkommt. Dazu betrachtet man auf einem 2-Qubit-Register die Transformation U_f, die durch

$$U_f(|x\rangle \otimes |y\rangle) \;=\; |x\rangle \otimes |y \oplus f(x)\rangle \quad \text{für } x, y \in \{0,1\}$$

festgelegt ist. Dabei ist „$\oplus$“ das übliche XOR klassischer Zustände.

Man kann nachrechnen, dass U_f für jede beliebige Funktion $f : \{0,1\} \to \{0,1\}$ unitär ist.

Der Algorithmus:



Aus $|\Psi_0\rangle = |0\rangle \otimes |1\rangle$ wird zunächst

$$|\Psi_1\rangle \;=\; (H\,|0\rangle) \otimes (H\,|1\rangle) \;=\; \Big(\tfrac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big)\Big) \otimes \Big(\tfrac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big)\Big) \;=\; |+\rangle \otimes |-\rangle\,.$$

Betrachte nun zunächst die Wirkung von U_f auf $|x\rangle \otimes |-\rangle$ mit $x \in \{0,1\}$:

Wegen der Linearität von U_f gilt

$$\begin{aligned}
U_f\big(\,|x\rangle \otimes |-\rangle\,\big) &= U_f\Big(\,|x\rangle \otimes \tfrac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big)\Big) \\
&= U_f\Big(\tfrac{1}{\sqrt{2}}\big(\,|x\rangle \otimes |0\rangle - |x\rangle \otimes |1\rangle\,\big)\Big) \\
&= \tfrac{1}{\sqrt{2}}\Big(U_f\big(\,|x\rangle \otimes |0\rangle\,\big) - U_f\big(\,|x\rangle \otimes |1\rangle\,\big)\Big) \\
&= \tfrac{1}{\sqrt{2}}\Big(\,|x\rangle \otimes |0 \oplus f(x)\rangle - |x\rangle \otimes |1 \oplus f(x)\rangle\,\Big) \\
&= \tfrac{1}{\sqrt{2}}\,|x\rangle \otimes \big(\,|f(x)\rangle - |1 \oplus f(x)\rangle\,\big).
\end{aligned}$$

Für den hinteren Teil $|f(x)\rangle - |1 \oplus f(x)\rangle$ gilt,

falls $f(x) = 0$ ist:

$$|f(x)\rangle - |1 \oplus f(x)\rangle \;=\; |0\rangle - |1\rangle \;=\; (-1)^0 \cdot \big(\,|0\rangle - |1\rangle\,\big),$$

falls $f(x) = 1$ ist:

$$|f(x)\rangle - |1 \oplus f(x)\rangle \;=\; |1\rangle - |0\rangle \;=\; (-1)^1 \cdot \big(\,|0\rangle - |1\rangle\,\big).$$

Daher kann man in jedem Fall schreiben:

$$|f(x)\rangle - |1 \oplus f(x)\rangle \;=\; (-1)^{f(x)} \cdot \big(\,|0\rangle - |1\rangle\,\big).$$

Damit gilt weiter

$$\begin{aligned}
U_f\big(\,|x\rangle \otimes |-\rangle\,\big) &= \tfrac{1}{\sqrt{2}}\,|x\rangle \otimes \Big((-1)^{f(x)} \cdot \big(\,|0\rangle - |1\rangle\,\big)\Big) \\
&= (-1)^{f(x)} \cdot \big(\,|x\rangle \otimes |-\rangle\,\big).
\end{aligned}$$

Damit kann man nun $|\Psi_2\rangle$ berechnen:

$$\begin{aligned}
|\Psi_2\rangle &= U_f\Big(\big(\tfrac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big)\big) \otimes |-\rangle\Big) \\
&= U_f\Big(\tfrac{1}{\sqrt{2}}\big(\,|0\rangle \otimes |-\rangle + |1\rangle \otimes |-\rangle\,\big)\Big) \\
&= \tfrac{1}{\sqrt{2}}\Big(U_f\big(\,|0\rangle \otimes |-\rangle\,\big) + U_f\big(\,|1\rangle \otimes |-\rangle\,\big)\Big) \\
&= \tfrac{1}{\sqrt{2}}\Big((-1)^{f(0)} \cdot \big(\,|0\rangle \otimes |-\rangle\,\big) + (-1)^{f(1)} \cdot \big(\,|1\rangle \otimes |-\rangle\,\big)\Big) \\
&= \tfrac{1}{\sqrt{2}}\Big((-1)^{f(0)} \cdot |0\rangle + (-1)^{f(1)} \cdot |1\rangle\Big) \otimes |-\rangle\,.
\end{aligned}$$

1. Fall: $f(0) = f(1)$: Dann ist

$$\begin{aligned}
|\Psi_2\rangle &= \tfrac{1}{\sqrt{2}}\Big((-1)^{f(0)} \cdot |0\rangle + (-1)^{f(0)} \cdot |1\rangle\Big) \otimes |-\rangle \\
&= (-1)^{f(0)} \cdot \Big(\tfrac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big)\Big) \otimes |-\rangle \\
&= (-1)^{f(0)} \cdot \big(\,|+\rangle \otimes |-\rangle\,\big).
\end{aligned}$$

2. Fall: $f(0) \neq f(1)$: Dann ist $(-1)^{f(1)} = -(-1)^{f(0)}$ und damit

$$\begin{aligned}
|\Psi_2\rangle &= \tfrac{1}{\sqrt{2}}\Big((-1)^{f(0)} \cdot |0\rangle - (-1)^{f(0)} \cdot |1\rangle\Big) \otimes |-\rangle \\
&= (-1)^{f(0)} \cdot \Big(\tfrac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big)\Big) \otimes |-\rangle \\
&= (-1)^{f(0)} \cdot \big(\,|-\rangle \otimes |-\rangle\,\big).
\end{aligned}$$

Wegen $H\,|+\rangle = |0\rangle$ und $H\,|-\rangle = |1\rangle$ folgt dann

falls: $f(0) = f(1)$: $|\Psi_3\rangle = (-1)^{f(0)} \cdot \big(\,|0\rangle \otimes |-\rangle\,\big)$,

falls: $f(0) \neq f(1)$: $|\Psi_3\rangle = (-1)^{f(0)} \cdot \big(\,|1\rangle \otimes |-\rangle\,\big)$.

Die Messung des ersten Qubits gibt nun also Auskunft, welcher Fall vorliegt:

Liefert die Messung $|0\rangle$, so ist $f(0) = f(1)$,

liefert die Messung $|1\rangle$, so ist $f(0) \neq f(1)$.

4.2 Deutsch-Jozsa-Algorithmus

Der Deutsch-Jozsa-Algorithmus verallgemeinert den Deutsch-Algorithmus für eine Funktion $f : \{0,1\}^n \to \{0,1\}$. Als Argument werden n-stellige Bitstrings mit der entsprechend dargestellten Zahl $x \in \{0,\ldots,2^n-1\}$ identifiziert.

Problemstellung:

Vorgegeben ist eine Funktion $f : \{0,1\}^n \to \{0,1\}$, von der man weiß, dass sie entweder

konstant ist, also alle Funktionswerte sind gleich 0 oder alle Funktionswerte sind gleich 1, oder

balanciert ist, d.h. gleich oft 0 und 1 als Ergebnis liefert.

Es soll die Frage untersucht werden, welche der beiden Alternativen vorliegt.

Klassisch muss man dazu im worst-case die Funktion $\frac{1}{2}\cdot 2^n+1$ mal aufrufen, denn erhält man immer nur den gleichen Wert, so weiß man nach der Hälfte aller Argumente immer noch nicht mit Sicherheit, ob man bei einer balancierten Funktion zufällig genau die eine Hälfte der Argumente mit gleichem Funktionswert getestet hat. Erst die nächste Auswertung liefert Klarheit.

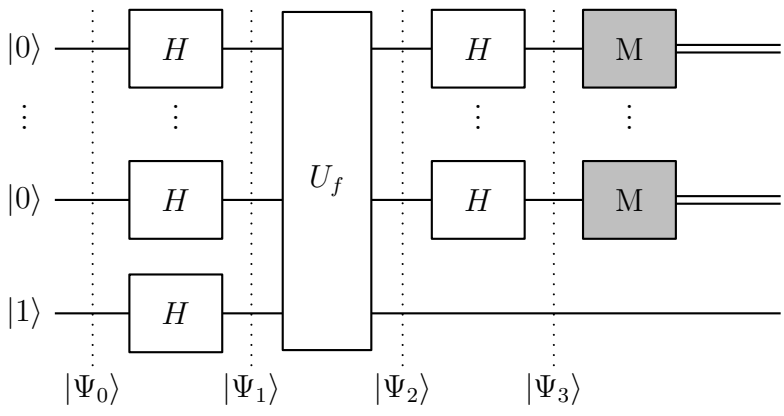
Der Algorithmus von Deutsch-Jozsa (benannt neben David Deutsch nach Richard Jozsa) erlaubt, die Fragestellung mit *einer* Funktionsauswertung zu beantworten.

In dem Zusammenhang bezeichnet man die Funktion f wieder als *Black-Box* oder als *Orakel* und braucht wieder eine Quanten-Version des Orakels, also eine unitäre Transformation, in der f vorkommt. Diese baut man ähnlich auf wie beim Deutsch-Algorithmus: Man betrachtet auf einem $(n+1)$-Qubit-Register die Transformation U_f, die durch

$$U_f(|x\rangle_n \otimes |y\rangle) \;=\; |x\rangle_n \otimes |y \oplus f(x)\rangle \quad \text{für } x \in \{0,1\}^n \text{ und } y \in \{0,1\}$$

festgelegt ist. Man kann nachrechnen, dass die Transformation U_f für jede beliebige Funktion $f : \{0,1\}^n \to \{0,1\}$ unitär ist.

Der Algorithmus:



Analyse:

Aus $|\Psi_0\rangle = |0\rangle_n \otimes |1\rangle$ wird zunächst

$$|\Psi_1\rangle \;=\; (H^{\otimes n}\,|0\rangle_n) \otimes (H\,|1\rangle).$$

Man kann sich überlegen (formal z.B. mittels vollständiger Induktion), dass die Transformationsmatrix zu $H^{\otimes n}$ bei einem Vorfaktor $\frac{1}{2^{n/2}}$ in der ersten Zeile und Spalte lauter Einsen enthält (an den anderen Stellen stehen $+1$ oder -1):

$$H^{\otimes n} \;=\; \frac{1}{2^{n/2}} \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 1 & * & \dots & * \end{pmatrix}. \qquad (*)$$

Damit ist

$$H^{\otimes n}\,|0\rangle_n \;=\; \frac{1}{2^{n/2}} \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 1 & * & \dots & * \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \;=\; \frac{1}{2^{n/2}} \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \;=\; \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n \,.$$

Wegen $H\,|1\rangle = |-\rangle$ ist also

$$|\Psi_1\rangle \;=\; (H^{\otimes n}\,|0\rangle_n) \otimes (H\,|1\rangle) \;=\; \Big(\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n\Big) \otimes |-\rangle\,.$$

Betrachtet man nun die Wirkung von U_f auf $|x\rangle_n \otimes |-\rangle$ mit $x \in \{0,1\}^n$, so erhält man genau wie beim Deutsch-Algorithmus

$$U_f\big(\,|x\rangle_n \otimes |-\rangle\,\big) \;=\; (-1)^{f(x)} \cdot \big(\,|x\rangle_n \otimes |-\rangle\,\big).$$

Damit erhält man

$$\begin{aligned} |\Psi_2\rangle \;&=\; U_f\,|\Psi_1\rangle \;=\; U_f\Big(\Big(\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n\Big) \otimes |-\rangle\Big) \\ &=\; \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} U_f\big(\,|x\rangle_n \otimes |-\rangle\,\big) \\ &=\; \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \cdot \big(\,|x\rangle_n \otimes |-\rangle\,\big). \\ &=\; \Big(\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \cdot |x\rangle_n\Big) \otimes |-\rangle\,. \\ &=\; \widetilde{|\Psi_2\rangle} \otimes |-\rangle \quad \text{mit} \quad \widetilde{|\Psi_2\rangle} = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \cdot |x\rangle_n\,. \end{aligned}$$

Für den letzten Teil des Algorithmus ist das $|-\rangle$ im letzten Qubit nicht mehr relevant sondern nur $\widetilde{|\Psi_2\rangle}$ und dann die Messung von $\widetilde{|\Psi_3\rangle} = H^{\otimes n}\widetilde{|\Psi_2\rangle}$.

1. Fall: f ist konstant, $f(x) = f(0)$ für alle $x \in \{0, \ldots, 2^n - 1\}$.

   Dann ist

   $$\widetilde{|\Psi_2\rangle} \;=\; (-1)^{f(0)} \cdot \Big(\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n\Big).$$

   Dies entspricht $(-1)^{f(0)} \cdot H^{\otimes n} |0\rangle_n$, und da $H^{\otimes n}$ zu sich selbst invers ist, erhält man

   $$\begin{aligned}\widetilde{|\Psi_3\rangle} \;&=\; H^{\otimes n}\widetilde{|\Psi_2\rangle} \;=\; H^{\otimes n}\big((-1)^{f(0)} \cdot H^{\otimes n} |0\rangle_n\big) \\ &= (-1)^{f(0)} \cdot H^{\otimes n}\big(H^{\otimes n} |0\rangle_n\big) \\ &= (-1)^{f(0)} \cdot |0\rangle_n .\end{aligned}$$

   Bei der abschließenden Messung erhält man also garantiert den 0-Zustand $|0\rangle_n$.

2. Fall: f ist balanciert.

   Behauptung:

   > Dann ist die Wahrscheinlichkeit, dass man bei der Messung von $\widetilde{|\Psi_3\rangle}$ den 0-Zustand $|0\rangle_n$ erhält, gleich 0.

   In Vektor-Schreibweise ist

   $$\widetilde{|\Psi_2\rangle} \;=\; \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \cdot |x\rangle_n \;=\; \frac{1}{2^{n/2}} \begin{pmatrix} (-1)^{f(0)} \\ \vdots \\ (-1)^{f(2^n-1)} \end{pmatrix}.$$

   Mit der Matrix-Darstellung $(*)$ von $H^{\otimes n}$ erhält man also

   $$\widetilde{|\Psi_3\rangle} \;=\; H^{\otimes n}\widetilde{|\Psi_2\rangle} \;=\; \frac{1}{2^{n/2}} \begin{pmatrix} 1 & 1 & \ldots & 1 \\ 1 & * & \ldots & * \\ \vdots & \vdots & \ddots & \vdots \\ 1 & * & \ldots & * \end{pmatrix} \cdot \frac{1}{2^{n/2}} \begin{pmatrix} (-1)^{f(0)} \\ \vdots \\ (-1)^{f(2^n-1)} \end{pmatrix}.$$

   Bei Darstellung von $\widetilde{|\Psi_3\rangle}$ als Linearkombination der Einheitsvektoren ist der Vorfaktor des ersten Einheitsvektors, also von $|0\rangle_n$, gleich der obersten Komponente dieses Matrix-Vektor-Produkts. Diese obersten Komponente ist gleich

   $$\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \;=\; 0,$$

   denn da f balanciert ist, gibt es in der Summe genau so viele $+1$ wie -1. Damit ist auch die Wahrscheinlichkeit, dass man bei der Messung von $\widetilde{|\Psi_3\rangle}$ den 0-Zustand $|0\rangle_n$ erhält, gleich 0.

Algorithmus von Bernstein-Vazirani:

Der Algorithmus von Bernstein-Vazirani ist von der Problemstellung eng verwandt bzw. vom Ablauf her identisch mit dem Deutsch-Jozsa-Algorithmus.

Problemstellung:

Vorgegeben ist eine Funktion $f : \{0,1\}^n \to \{0,1\}$, die durch ein binäres Skalarprodukt „$\odot$“ erzeugt wird, d.h. es gibt ein $a = (a_{n-1} \dots a_1 a_0)_2 \in \{0, \dots, 2^n - 1\}$, so dass für $x = (x_{n-1} \dots x_1 x_0)_2 \in \{0, \dots, 2^n - 1\}$ gilt

$$f(x) \;=\; a \odot x \;:=\; a_{n-1} \cdot x_{n-1} \oplus \dots \oplus a_1 \cdot x_1 \oplus a_0 \cdot x_0.$$

Gesucht ist das $a \in \{0, \dots, 2^n - 1\}$, das die Funktion f erzeugt.

Klassisch kann man a bestimmen, indem man f an 2er-Potenzen, also den Koordinaten-Vektoren mit einer 1 an der Stelle s und 0 an allen anderen Stellen, auswertet und so sukzessive die Werte a_s ermittelt. Dazu braucht man n Funktionsauswertungen.

Der Algorithmus von Bernstein-Vazirani erlaubt, die Fragestellung mit *einer* Funktionsauswertung zu beantworten.

Als Quanten-Version von f betrachtet man wie beim Deutsch-Jozsa-Algorithmus die Transformation U_f, die durch

$$U(|x\rangle_n \otimes |y\rangle) \;=\; |x\rangle_n \otimes |y \oplus f(x)\rangle \quad \text{für } x \in \{0,1\}^n \text{ und } y \in \{0,1\}$$

festgelegt ist.

Algorithmus:

Der Algorithmus ist nun genau gleich dem Deutsch-Jozsa-Algorithmus.

Man kann zeigen, dass bei einer durch a festgelegten Funktion gilt:

$$\widetilde{|\Psi_3\rangle} \;=\; |a\rangle_n \,.$$

Die Messung liefert also eindeutig a.

Begründung:

Dass die Messung tatsächlich eindeutig a liefert, kann man mit Hilfe der in Abschnitt 3.1.4 hergeleiteten Wirkung von $H^{\otimes n}$ nachrechnen:

Wie beim Deutsch-Jozsa-Algorithmus ist $\widetilde{|\Psi_3\rangle} = H^{\otimes n}\widetilde{|\Psi_2\rangle}$ mit

$$\widetilde{|\Psi_2\rangle} \;=\; \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \cdot |x\rangle_n \,,$$

hier mit der Funktion $f(x) = a \odot x$, also

$$\widetilde{|\Psi_3\rangle} \;=\; \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} (-1)^{a \odot x} \cdot H^{\otimes n} |x\rangle_n \,.$$

Nach Abschnitt 3.1.4 ist

$$H^{\otimes n} \left|x\right\rangle_n \;=\; \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} (-1)^{x \odot k} \left|k\right\rangle_n .$$

Damit erhält man durch Einsetzen und dann Vertauschung der Summationsreihenfolge

$$\begin{aligned} \widetilde{\left|\Psi_3\right\rangle} \;&=\; \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} (-1)^{a \odot x} \cdot \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} (-1)^{x \odot k} \left|k\right\rangle_n \\ &=\; \sum_{k=0}^{2^n-1} \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{a \odot x} \cdot (-1)^{x \odot k} \left|k\right\rangle_n . \end{aligned}$$

Der Vorfaktor von $\left|k\right\rangle_n$ ist also

$$\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{a \odot x} \cdot (-1)^{x \odot k} \;=\; \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{a \odot x + k \odot x} \qquad (*).$$

Ist $a = k$, so ist der Exponent von -1 immer gerade. In der Summe werden also 2^n Einsen addiert; mit dem Faktor $\frac{1}{2^n}$ erhält man also 1, d.h. der Vorfaktor von $\left|a\right\rangle_n$ ist 1. Wegen der Normierung müssen dann alle anderen Vorfaktoren gleich Null sein (man kann sich auch bei $(*)$ überlegen, dass bei $a \neq k$ genau so viele $+1$ wie -1 in der Summe entstehen, und diese daher gleich 0 ist), und eine Messung liefert eindeutig $\left|a\right\rangle_n$.

5 Was kann ein Quantencomputer?

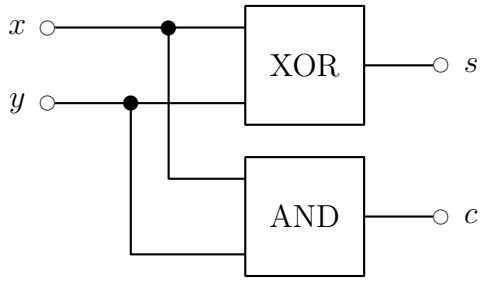
5.1 Schaltkreise

Fragestellung:

Operationen, die ein Quantencomputer durchführen kann, sind – abgesehen von Messungen – unitäre Transformationen. Kann man damit alles das programmieren, was man auch mit klassischen Computern programmieren kann?

Beispiel:

Der folgende Schaltkreis beschreibt einen klassischen Halbaddierer, d.h., der Output stellt in der Form cs die zweistellig binär dargestellte Summe von x und y, $x, y \in \{0, 1\}$, dar:



Bestandteile:

Ein klassicher Schaltkreis besteht aus den Basis-Verknüpfungen

NOT, XOR, AND und OR.

Ferner hat man in einem klassischen Schaltkreis Verzweigungen, also Stellen, an denen ein Bit kopiert wird.

Kann man diese auf Quantencomputern realisieren?

Hifs-Qubits:

Je nach Realisierung kann die gleiche Aufgabe klassisch durch mehr oder weniger Bits realisiert werden. Entsprechend sind für eine Quanten-Computing-Realisierung Hilfs-Qubits erlaubt.

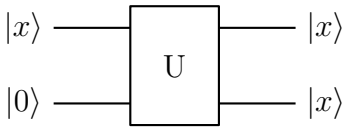
Hilfs-Qubits sind auch (unabhängig) für die Eingabe- und Ausgabe-Seite erlaubt. Ansonsten hätte man direkt ein Problem, denn bei einem klassischen Schaltkreis gibt es keine Restriktionen bzgl. der Anzahl der Eingabe- und Ausgabe-Bits – z.B. können drei Eingabe-Bits auf zwei Ausgabe-Bits abgebildet werden oder vier Eingabe-Bits auf sieben Ausgabe-Bits –, während man bei Qubits eine unitäre Transformation und damit insbesondere genausoviel Eingabe- wie Ausgabe-Qubits haben muss.

Kopieren von Bits:

Das No-Cloning-Theorem besagt, dass man Qubits nicht kopieren kann.

Hier geht es aber nur darum, den Fall klassischer Zustände betrachtet als Basiszustände nachzubilden.

Da der Ausgang eines Kopier-Vorgangs zwei Bits enthält, muss die Quanten-Computing-Realisierung auch am Eingang zwei Qubits entgegennehmen, also neben dem für die Basiszustände zu kopierenden Qubit noch ein zweites Qubit. Dabei reicht es, wenn nur für einen speziellen Wert, z.B. $|0\rangle$, des zweiten Qubits, die Kopier-Eigenschaft (bezogen nur auf Basiszustände des ersten Qubits) erfüllt ist.



für $x \in \{0, 1\}$.

Man sucht also eine unitäre Transformation U mit

$$U(|00\rangle) \;=\; |00\rangle \qquad \text{und} \qquad U(|10\rangle \;=\; |11\rangle\,;$$

die Wirkung auf $|x1\rangle$ ist nicht festgelegt.

Das CNOT-Gatter mit dem ersten Qubit als Kontroll- und dem zweiten als Ziel-Qubit erfüllt offensichtlich diese Eigenschaft.

Erste Überlegungen zu Verknüpfungen:

Die NOT-Operation ist die Abbildung von einem Bit auf ein Bit:

$$\mathrm{NOT}(0) \;=\; 1, \qquad \mathrm{NOT}(1) \;=\; 0.$$

Das Qubit-Pendant ist das P_X-Gatter:

$$P_X\,|0\rangle \;=\; \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \;=\; \begin{pmatrix} 0 \\ 1 \end{pmatrix} \;=\; |1\rangle\,,$$

$$P_X\,|1\rangle \;=\; \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \;=\; \begin{pmatrix} 1 \\ 0 \end{pmatrix} \;=\; |0\rangle\,.$$

Die anderen Operationen (XOR, AND und OR) bilden zwei (klassische) Bits auf ein (klassisches) Bit ab. Bei einer unitären Transformation hat man genausoviel Eingabe- wie Ausgabe-Qubits.

Für XOR wurde das schon in Abschnitt 3.2.1 betrachtet: Man dubliziert ein Eingabe-Qubit auf ein Ausgabe-Qubit; das andere Ausgabe-Qubit entspricht der XOR-Verknüpfung:

$$(x, y) \;\mapsto\; (x, x \text{ XOR } y).$$

Realisiert wird dies durch das CNOT-Gatter, das dem kontrollierten P_X-Gatter entspricht.

Allerdings ergibt eine ähnliche Konstruktion für AND bzw. OR keine unitäre Transformation, denn bei AND wäre dann beispielsweise

$$(0,0) \;\mapsto\; (0,0 \text{ AND } 0) = (0,0) \qquad \text{und} \qquad (0,1) \;\mapsto\; (0,0 \text{ AND } 1) = (0,0),$$

und bei OR wäre dann beispielsweise

$$(1,0) \;\mapsto\; (1,1 \text{ OR } 0) = (1,1) \qquad \text{und} \qquad (1,1) \;\mapsto\; (1,1 \text{ OR } 1) = (1,1);$$

die Abbildung wäre also nicht injektiv und damit nicht invertierbar.

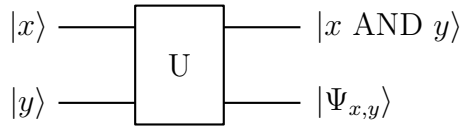
Keine 2-Qubit-Realisierung von AND und OR:

Behauptung:

Es gibt keine 2-Qubit-Realisierung von AND und OR, d.h. keine unitäre Transformation, die zwei Qubits entgegennimmt und am Ausgang in einem Qubit das Resultat einer AND- bzw. OR-Verknüpfung der Eingangs-Qubits enthält, falls diese in einem Basiszustand sind.

Begründung:

Angenommen, es gibt eine Realisierung von AND auf einem 2-Qubit-Register, also eine unitäre Transformation U, die zwei Qubits entgegennimmt und am Ausgang in einem Qubit – o.B.d.A. im ersten Qubit – das Resultat einer AND-Verknüpfung der Eingangs-Qubits enthält, falls diese in einem Basiszustand, also gleich $|0\rangle$ bzw. $|1\rangle$, sind. Das zweite Ausgangs-Qubit kann dabei irgendwie von den Eingangs-Qubits abhängen:



für $x, y \in \{0,1\}$.

Als Formel:

$$U(|x\rangle \otimes |y\rangle) \;=\; |x \text{ AND } y\rangle \otimes |\Psi_{x,y}\rangle \qquad \text{für } x, y \in \{0,1\}.$$

Dann gilt also insbesondere

$$U\,|00\rangle \;=\; |0\rangle \otimes |\Psi_{00}\rangle\,, \quad U\,|01\rangle \;=\; |0\rangle \otimes |\Psi_{01}\rangle\,, \quad U\,|10\rangle \;=\; |0\rangle \otimes |\Psi_{10}\rangle\,.$$

Betrachtet man dies vektoriell und setzt man $|\Psi_{xy}\rangle = \alpha_{xy}\,|0\rangle + \beta_{xy}\,|1\rangle = \binom{\alpha_{xy}}{\beta_{xy}}$, so erhält man als Bilder

$$\tbinom{1}{0} \otimes \tbinom{\alpha_{00}}{\beta_{00}} \;=\; \begin{pmatrix} \alpha_{00} \\ \beta_{00} \\ 0 \\ 0 \end{pmatrix}, \quad \tbinom{1}{0} \otimes \tbinom{\alpha_{01}}{\beta_{01}} \;=\; \begin{pmatrix} \alpha_{01} \\ \beta_{01} \\ 0 \\ 0 \end{pmatrix} \quad \text{und} \quad \tbinom{1}{0} \otimes \tbinom{\alpha_{10}}{\beta_{10}} \;=\; \begin{pmatrix} \alpha_{10} \\ \beta_{10} \\ 0 \\ 0 \end{pmatrix}.$$

Als Bilder der ersten drei Einheitsvektoren sind dies die ersten drei Spalten der Abbildungsmatrix zu U. Diese Matrix hat dann also die Gestalt

$$\begin{pmatrix} * & * & * & * \\ * & * & * & * \\ 0 & 0 & 0 & * \\ 0 & 0 & 0 & * \end{pmatrix},$$

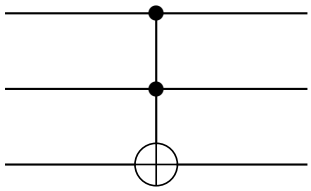
wobei $*$ für einen beliebigen Eintrag steht.

Da die letzten beiden Zeilen Vielfache voneinander sind, kann diese Matrix nicht invertierbar, also insbesondere nicht unitär sein - Widerspruch!

Ähnlich kann man für OR argumentieren.

Das Toffoli-Gatter:

Das Toffoli-Gatter T ist ein Gatter auf einem 3-Qubit-Register. Auf Basiszustände angewendet bewirkt es die Invertierung des dritten Qubits, falls die ersten beiden Qubits gleich $|1\rangle$ sind. Entsprechend kann man es als zweifach-kontrolliertes NOT (bzw. P_X-Gatter bzw. XOR) ansehen:



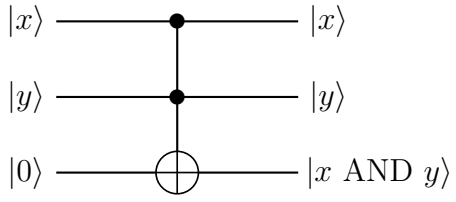
$$T(|1\rangle \otimes |1\rangle \otimes |z\rangle) = |1\rangle \otimes |1\rangle \otimes |\mathrm{NOT}(z)\rangle \qquad \text{für } z \in \{0,1\} \quad \text{und}$$

$$T(|x\rangle \otimes |y\rangle \otimes |z\rangle) = |x\rangle \otimes |y\rangle \otimes |z\rangle \qquad \text{für } x,y,z \in \{0,1\},\ (x,y) \neq (1,1).$$

Man kann sich überlegen, dass die Toffoli-Transformation unitär ist. Ferner ist sie offensichtlich zu sich selbst invers:

$$T(T(|xyz\rangle) = |xyz\rangle\,.$$

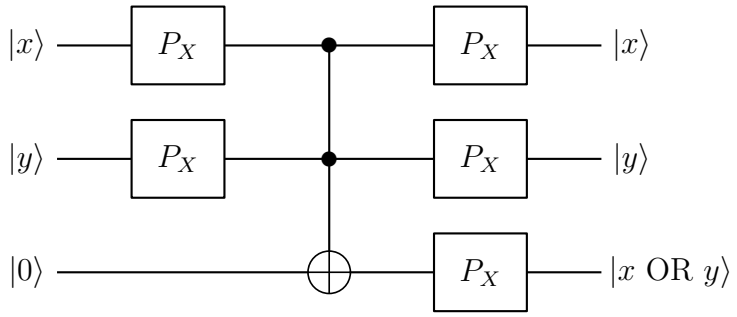
Mit dem Toffoli-Gatter kann man nun die AND-Verknüpfung realisieren, denn durch Betrachtung der vier unterschiedlichen Fälle für $x, y \in \{0,1\}$ sieht man:



Da man die OR-Verknüpfung durch Negation auf die AND-Verknüpfung zurückführen kann,

$$x \text{ OR } y \;=\; \text{NOT}\big(\text{NOT}(x) \text{ AND } \text{NOT}(y)\big),$$

kann man mit Hilfe von P_X-Gattern entsprechend die OR-Verknüpfung auf Qubits realisieren:



Bemerkung:

Man kann zeigen, dass das Toffoli-Gatter universell ist, d.h., dass sich allein damit alle Basis-Verknüpfungen darstellen lassen.

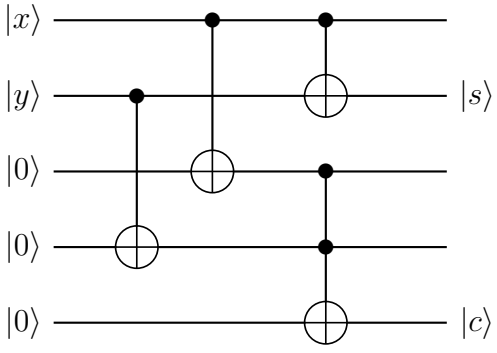
Fazit:

Mit einem Quantencomputer kann man klassische Schaltkreise nachbauen:

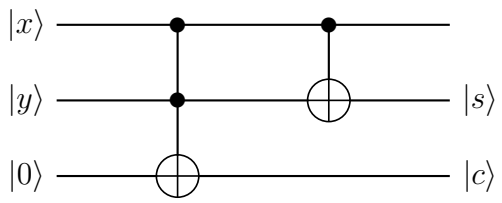
Mit ggf. linearem Mehraufwand kann man einen Quanten-Schaltkreis realisieren, der (ggf. bei entsprechender Initialisierung von Hilfs-Qubits) bzgl. der Basis-Zustände die gleiche Wirkung (ggf. auf ausgewählte Ausgabe-Qubits) hat wie der klassische Schaltkreis.

Beispiel:

Wendet man die vorgestellten Übertragungen von Kopieren und XOR- und AND-Verknüpfung auf den im Beispiel zu Beginn des Kapitels betrachteten Halbaddierer an, so erhält man folgende Quanten-Computing-Realisierung:



Man kann den Schaltkreis optimieren, indem man auf das explizite Kopieren verzichtet:



Durch Betrachtung der einzelnen Fälle kann man sich überzeugen, dass cs die zweistellig binär dargestellte Summe von x und y, $x, y \in \{0, 1\}$, darstellt.

5.2 Komplexitätsklassen

Disclaimer: Das folgende sind grob vereinfachte Darstellungen!

Betrachtet werden im Folgenden *Entscheidungsprobleme*, d.h. Probleme, die mit „ja“ oder „nein“ beantwortet werden können.

Beispiele:

1. Vorgegeben ist ein lineares Gleichungssystem. Hat das Gleichungssystem eine eindeutige Lösung?
2. Gibt es bei vorgegebenen Städten und Entfernungen zwischen diesen Städten eine Rundreise durch alle Städte, die eine gewisse vorgegebene Länge nicht überschreitet?
3. Man hat eine Urne, in der sich Kugeln befinden. Man weiß, dass entweder 2/3 der Kugeln schwarz und die anderen weiß sind oder umgekehrt. Ist die vorliegende Urne hauptsächlich mit schwarzen Kugeln gefüllt?

Definitionen:

- Ein Problem ist in der Klasse P (*polynomial*) genau dann, wenn man mit einem klassischen Computer das Problem in polynomieller Zeit lösen kann.

  Beispiel:

  Das erste Beispiel ist in P, da man ein lineares Gleichungssystem mit dem Gaußverfahren in polynomieller Zeit lösen und damit die Frage beantworten kann.

- Ein Problem ist in der Klasse NP (*non-deterministic polynomial*) genau dann, wenn man für den „ja“-Fall – falls einem ein „Orakel“ einen Beweis („Zertifikat“) für das „ja“ sagt – die Lösung in polynomieller Zeit mit einem klassischen Computer überprüfen kann.

  Beispiel:

  Das zweite Beispiel ist in NP, denn gibt es eine Rundreise kürzer als die vorgegebene Länge, und das Orakel verrät diese Rundreise, so kann man in polynomieller Zeit überprüfen, dass das stimmt.

- Ein Entscheidungsproblem ist in der Klasse BPP (*bounded error probabilistic polyno-*

mial) genau dann, wenn man in polynomieller Zeit mit einer festen Wahrscheinlichkeit größer $1/2$ die Entscheidung mit einem klassischen Computer richtig treffen kann.

Beispiel:

Das dritte Beispiel ist in BPP, denn durch die Ziehung einer Kugel hat man einen entsprechenden Hinweis für die Antwort. Durch mehrfache Ziehungen kann man die Sicherheit exponentiell erhöhen.

- Ein Entscheidungsproblem ist in der Klasse BQP (*bounded error quantum polynomial*) genau dann, wenn man in polynomieller Zeit mit einer festen Wahrscheinlichkeit größer $1/2$ die Entscheidung mit einem Quantencomputer richtig treffen kann.

Beziehungen zwischen den Komplexitätsklassen:

- $P \subseteq NP$,

  denn eine polynomielle Berechnung ist schon ein Zertifikat.

  Ob $P = NP$ oder $P \subsetneq NP$ gibt, ist eine der großen offenen Fragen in diesem Bereich.

- $P \subseteq BPP$,

  da eine sichere Entscheidung eine Entscheidung mit Wahrscheinlichkeit größer $1/2$ ist.

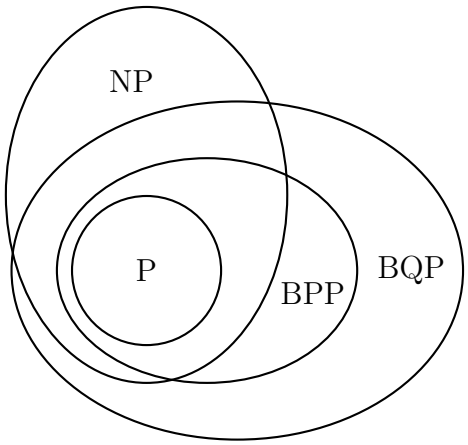
- $BPP \subseteq BQP$,

  wegen der Überlegungen aus Abschnitt 5.1.

- BPP und NP bzw. BQP und NP:

  bisher unbekannt.

Eine mögliche Lagebeziehung ist die folgende.



Es könnten aber auch Mengen-Gleichheiten gelten oder, dass NP ganz in BQP oder BPP liegt oder umgekehrt.

Beispiel:

Das Problem der Primfaktor-Zerlegung ist in NP, denn eine vom Orakel vorgegebene Faktorisierung kann man in polynomieller Zeit überprüfen. Bisher ist aber nicht bekannt, ob das Problem auch in P ist; zur Zeit ist kein polynomieller Algorithmus zur Berechnung einer Primfaktor-Zerlegung bekannt.

Der Shor-Algorithmus ist allerdings ein polynomieller Quanten-Algorithmus, der mit einer hohen Wahrscheinlichkeit die Primfaktor-Zerlegung berechnet, d.h., das Problem ist in BQP.

5.3 Adiabatischer Quantencomputer

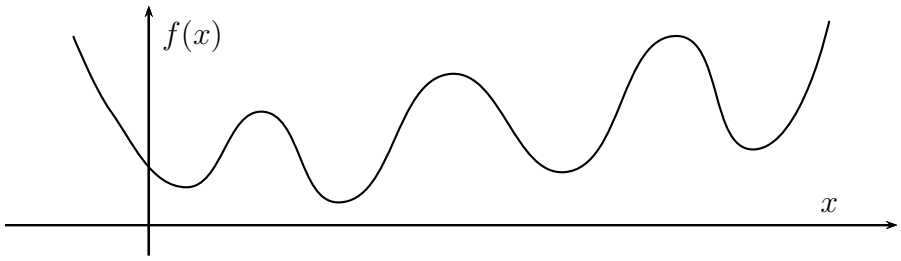
Die bisherigen Betrachtungen bezogen sich auf sogenannte Gitter-basierte-Quantencomputer. Entsprechend der obigen Ausführungen sind sie universell in dem Sinne, dass man prinzipiell alle Dinge, die man mit einem klassischen Computer berechnen kann, auch mit einem solchen Quantencomputer berechnen kann.

Adiabatische Quantencomputer, auch *Quanten-Annealer* genannt, arbeiten auf eine andere Weise und sind nicht universell. Sie übertragen das klassische Konzept des *simulated Annealing* auf Quanten.

Simulated Annealing:

Das *simulated Annealing* ist ein klassisches probabilistisches Optimierungsverfahren.

Es versucht, den Prozess des Abkühlens („annealing“) bei einer Kristallisation nachzubilden: Bei der Abkühlung von Substanzen kann es verschiedene lokale Energieminima geben, in die die Substanz überführt wird. Beim langsamen Abkühlen erhält man im Duchschnitt niedrigere Energieniveaus, da von Zeit zu Zeit durch Zufallsprozesse Energiebarrieren zwischen den lokalen Minima übersprungen werden.



Die Idee des *simulated Annealings* ist, Nachbarschafts-Strukturen in einem Definitionsgebiet D einer zu optimierenden Funktion $f : D \to \mathbb{R}$ auszunutzen. Man geht schrittweise vor (zufällig oder gezielt, z.B. mittels des Gradientenverfahrens) und akzeptiert einen Schritt, wenn man einen besseren Funktionswert hat. Bei einem schlechteren Funktionswert wird der Schritt mit einer im Laufe des Prozesses kleiner werdenden Wahrscheinlichkeit akzeptiert.

Quanten-Annealing:

Beim Quanten-Annealer nutzt man eine ähnliche Idee, allerdings direkt auf der quantenmechanischen Struktur. Man beginnt mit einer Konstellation, deren Grundzustand – also deren Energie-Minimum – man kennt und herstellen kann.

Ein quantenmechanisches Prinzip besagt nun, dass das System bei einer allmählichen Modifikation weiter im Energie-Minimum verbleibt. Dieses nutzt man aus, indem man die Konstellation mit einem bekannten und erreichten Grundzustand allmählich so modifiziert, bis man ein System erhält, bei dem der Grundzustand Rückschlüsse auf die Lösung des zu untersuchenden Optimierungsproblems gibt.

Stand der Technik:

Bei adiabatischen Quantencomputern kann man aktuell deutlich mehr Qubits handhaben als bei Gitter-basierten Quantencomputern.

Am Forschungszentrum Jülich wurde Anfang 2022 ein adiabatischen Quantencomputer mit 5000 Qubits von der Firma *D-Wave* in Betrieb genommen.

6 Algorithmus von Grover

6.1 Grundsätzlicher Ablauf

Fragestellung:

Gesucht ist ein bestimmtes Element in einer unsortierten Datenbank.

Konkreter: Gegeben ist eine Funktion $f : D \to \{0,1\}$, wobei bekannt ist, dass es genau ein $x_0 \in D$ gibt mit $f(x_0) = 1$; für alle anderen $x \in D$ ist $f(x) = 0$.

Klassisch muss man die Elemente aus D durchprobieren. Gibt es N verschiedene Elemente in D, so braucht man im worst-Case $N-1$ Auswertungen; im Durchschnitt sind es $N/2$.

Mit dem Algorithmus von Grover kann man schon nach ca. $\sqrt{N}$ Auswertungen das gesuchte Element mit hoher Wahrscheinlichkeit finden.

Quantenversion:

Für eine Quanten-Version betrachtet man $D = \{0,1\}^n$.

Zur Realisierung der Funktion f nutzt man wie beim Algorithmus von Deutsch-Jozsa eine unitäre Transformation U_f auf einem $(n+1)$-Qubit-Register, die durch

$$U_f(|x\rangle_n \otimes |y\rangle) \;=\; |x\rangle_n \otimes |y \oplus f(x)\rangle \quad \text{für } x \in \{0,1\}^n \text{ und } y \in \{0,1\}$$

festgelegt ist.

Idee des Algorithmus:

Die grundsätzliche Idee des Algorithmus ist eine sogenannte Amplituden-Verstärkung (*amplitude amplification*): Die Amplitude des gesuchten Elements wird (sukzessive) erhöht, die der anderen Elemente erniedrigt.

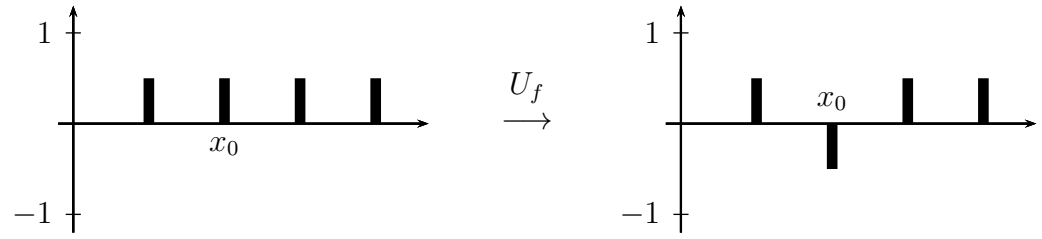
Genau wie beim Algorithmus von Deutsch bewirkt die Anwendung von U_f auf einen Zustand $|x\rangle_n \otimes |-\rangle$ mit $x \in \{0,1\}^n$

$$U_f\big(\,|x\rangle_n \otimes |-\rangle\,\big) \;=\; (-1)^{f(x)} \cdot \big(\,|x\rangle_n \otimes |-\rangle\,\big),$$

d.h., die Amplitude des gesuchten Elements x_0 wird invertiert, alle anderen Amplituden bleiben gleich.

Der Algorithmus von Grover startet mit einer gleichmäßigen Überlagerung aller Zustände $x \in \{0,1\}^n$. Durch Anwendung von U_f wird dann die Amplitude des gesuchten Elements invertiert.

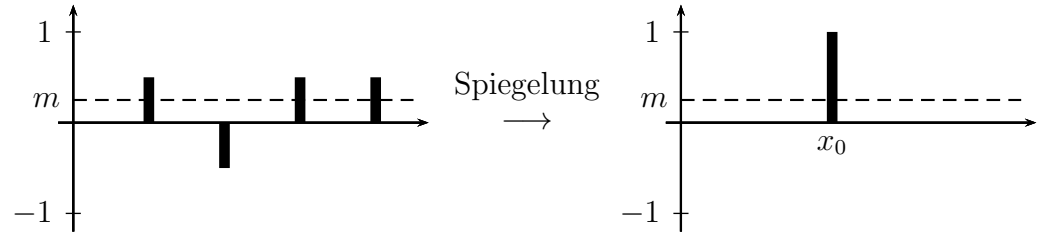
Das folgende Bild stellt die Amplituden für den Fall $n = 2$, also $N = 4$, dar, wobei das zweite Element das gesuchte ist. Die gleichmäßige Überlagerung liefert als Amplituden jeweils $\sqrt{\frac{1}{4}} = \frac{1}{2}$.



Bei einer Messung wären nun weiterhin alle Zustände gleich wahrscheinlich. Der Algorithmus spiegelt nun aber alle Amplituden am Mittelwert der Amplituden.

Im Beispiel $N = 4$ ist der Mittelwert m

$$m \;=\; \frac{1}{4}\cdot\left(\frac{1}{2}-\frac{1}{2}+\frac{1}{2}+\frac{1}{2}\right) \;=\; \frac{1}{4}.$$



Der gesuchte Zustand bekommt dadurch die Amplitude 1, alle anderen 0, so dass eine Messung den gesuchten Zustand sogar garantiert ermittelt.

Für größere Werte von N hat man eine kleinere Amplitudenverstärkung als bei $N = 4$. Daher wiederholt man die beiden Schritte (Anwendund von U_f und Spiegeln am Mittelwert), bis die Amplitude von x_0 signifikant groß ist.

Beispiel $N = 8$:

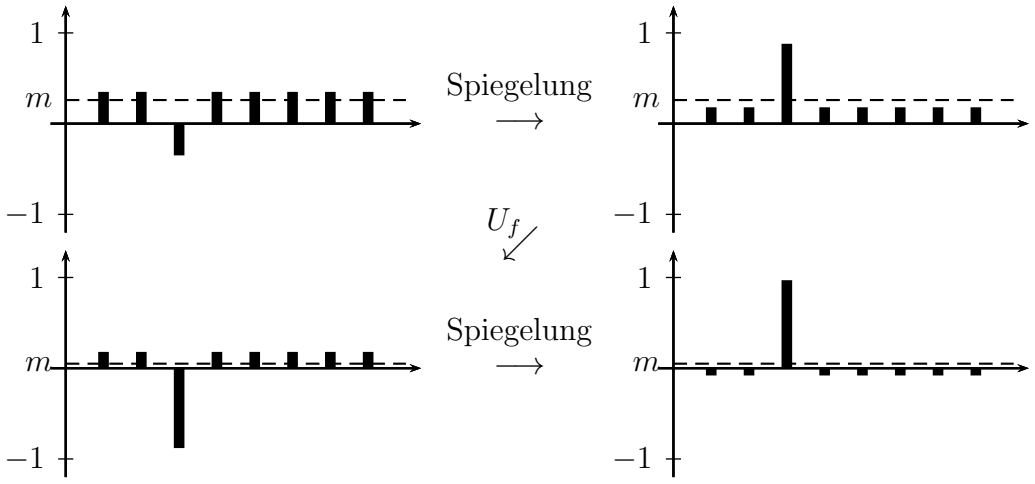
Für $N = 8$ haben zunächst alle Zustände die Amplitude $\sqrt{\frac{1}{N}} = \sqrt{\frac{1}{8}} \approx 0.35$. Nach Anwendung von U_f, also dem Invertieren der Amplitude des gesuchten Elements, ist der Mittelwert

$$m \;=\; \frac{1}{8}\cdot\left(-\sqrt{\frac{1}{8}}+7\cdot\sqrt{\frac{1}{8}}\right) \;\approx\; 0.26.$$

Nach dem Spiegeln erhält man ca. 0.88 als Amplitude des gesuchten Elements und ca. 0.18 für die übrigen Elemente.

Der Mittelwert nach erneutem Invertieren liegt bei ca. 0.04 und ein Spiegeln liefert ca. 0.97 als Amplitude des gesuchten Elements und ca. -0.09 für die übrigen Elemente.

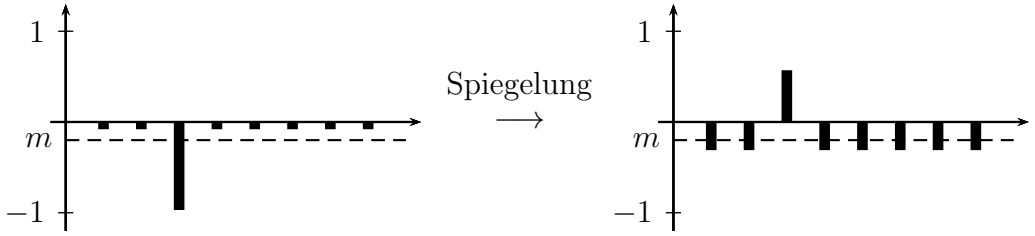
Die folgenden Bilder stellen die Amplituden beginnend nach der ersten Invertierung dar für den Fall, dass das dritte Element gesucht ist.



Man darf allerdings nicht zu viele Iterationen durchführen, da sich sonst die Amplitude von x_0 wieder verkleinert.

Beispiel $N = 8$:

Nach einer erneuten Invertierung im Beispiel oben für $N = 8$ ist der Mittelwert ca. -0.2 und ein Spiegeln liefert ca. 0.57 als Amplitude des gesuchten Elements und ca. -0.31 für die übrigen Elemente.



Details:

Start des Algorithmus:

Der Start des Algorithmus ist wie beim Deutsch-Jozsa-Algorithmus:

Neben den n Qubits, die die Zustände $x \in \{0,1\}^n$ repräsentieren, betrachtet man ein zusätzliches Hilfsqubit.

Ausgehend von $|\Psi_0\rangle = |0\rangle_n \otimes |1\rangle$ erhält man durch Anwendung von $H^{\otimes(n+1)} = H^{\otimes n} \otimes H$ die gleichmäßige Überlagerung in den ersten n Qubits und $|-\rangle$ im letzten:

$$(H^{\otimes n} |0\rangle_n) \otimes (H |1\rangle) \;=\; \Big(\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n\Big) \otimes |-\rangle\,.$$

Das Quanten-Orakel:

Wie oben schon erwähnt:

Zur Realisierung der Funktion f nutzt man wie beim Algorithmus von Deutsch-Jozsa eine unitäre Transformation U_f auf einem $(n+1)$-Qubit-Register, die durch

$$U_f(|x\rangle_n \otimes |y\rangle) \;=\; |x\rangle_n \otimes |y \oplus f(x)\rangle \quad \text{für } x \in \{0,1\}^n \text{ und } y \in \{0,1\}$$

festgelegt ist.

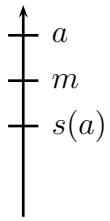
Genau wie beim Algorithmus von Deutsch bewirkt die Anwendung von U_f auf einen Zustand $|x\rangle_n \otimes |-\rangle$ mit $x \in \{0,1\}^n$

$$U_f\big(\,|x\rangle_n \otimes |-\rangle\,\big) \;=\; (-1)^{f(x)} \cdot \big(\,|x\rangle_n \otimes |-\rangle\,\big),$$

d.h., die Amplitude des gesuchten Elements x_0 wird invertiert, alle anderen Amplituden bleiben gleich.

Das Hilfsqubit dient zur Realisierung dieser Invertierung, ist aber ansonsten für die weiteren Betrachtungen nicht von Bedeutung.

Spiegeln an einem Wert:



Das Spiegeln einer Zahl a am Wert m wird durch die Funktion

$$s(a) \;=\; m - (a - m) \;=\; 2m - a$$

realisiert.

Spiegeln am Mittelwert:

Bei Amplituden α_k für Zustand $|k\rangle$, $k = 0, \ldots, N-1$, mit $N = 2^n$, ist der Mittelwert

$$m \;=\; \frac{1}{N} \sum_{k=0}^{N-1} \alpha_k.$$

Die Spiegelung von α_l am Mittelwert m ergibt also

$$s(\alpha_l) \;=\; 2 \cdot \left(\frac{1}{N} \sum_{k=0}^{N-1} \alpha_k \right) - \alpha_l \;=\; \Big(\frac{2}{N} - 1\Big)\alpha_l \;+\; \frac{2}{N} \sum_{\substack{k=0 \\ k \neq l}}^{N-1} \alpha_k.$$

Spiegelt man nun sämtliche Amplituden eines Zustands, den man als Vektor $\begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_{N-1} \end{pmatrix}$ betrachtet, so kann man das ansehen als Matrix-Vektor-Operation mit der Matrix

$$S \;=\; \begin{pmatrix} \frac{2}{N} - 1 & \frac{2}{N} & \ldots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} - 1 & \ldots & \frac{2}{N} \\ \vdots & & \ddots & \vdots \\ \frac{2}{N} & & \ldots & \frac{2}{N} - 1 \end{pmatrix}.$$

Behauptung:

Bei $N = 2^n$ gilt

$$S \;=\; -\,H^{\otimes n} \cdot D \cdot H^{\otimes n} \qquad \text{mit} \quad D = \begin{pmatrix} -1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

D ist also eine Diagonalmatrix mit -1 oben links und ansonsten 1 auf der Diagonalen. Zur Erinnerung: $H^{\otimes n}$ ist das n-fache Tensorprodukt der Hadamard-Matrix H.

Da bekanntlich $H^{\otimes n}$ und offensichtlich D unitär sind, und unitäre Matrizen bei Multiplikation mit -1 unitär bleiben, folgt damit insbesondere, dass S unitär ist.

Begründung:

Man kann D darstellen als

$$D \;=\; I - 2 \cdot E_{1,1} \quad \text{mit} \quad E_{1,1} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix},$$

d.h. $E_{1,1}$ besitzt außer Nullen nur oben links eine 1.

Damit gilt

$$\begin{aligned} & -\; H^{\otimes n} \cdot D \cdot H^{\otimes n} \\ = \; & -\; H^{\otimes n} \cdot (I - 2 \cdot E_{1,1}) \cdot H^{\otimes n} \\ = \; & -\; H^{\otimes n} \cdot H^{\otimes n} + 2 \cdot H^{\otimes n} \cdot E_{1,1} \cdot H^{\otimes n}. \end{aligned}$$

Da $H^{\otimes n}$ zu sich selbst invers ist, gilt $H^{\otimes n} \cdot H^{\otimes n} = I$ also

$$-\; H^{\otimes n} \cdot D \cdot H^{\otimes n} \;=\; -I \;+\; 2 \cdot H^{\otimes n} \cdot E_{1,1} \cdot H^{\otimes n}. \qquad (*)$$

Man kann sich leicht überlegen, dass $H^{\otimes n}$ in der ersten Zeile und in der ersten Spalte lauter Einsen enthält, wenn man den Faktor $\frac{1}{2^{n/2}}$ vor die Matrix zieht:

$$H^{\otimes n} \;=\; \frac{1}{2^{n/2}} \cdot \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & * & \dots & * \\ \vdots & & \ddots & \vdots \\ 1 & * & \dots & * \end{pmatrix}.$$

Das Matrix-Matrix-Produkt $E_{1,1} \cdot A$ mit einer beliebigen Matrix A ergibt eine Matrix, deren erste Zeile mit der ersten Zeile von A übereinstimmt und ansonsten Nullen enthält. Also gilt

$$E_{1,1} \cdot H^{\otimes n} \;=\; \frac{1}{2^{n/2}} \cdot \begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & 0 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}.$$

Multipliziert man eine beliebige Matrix A mit dieser Matrix, wird abgesehen vom Vorfaktor die erste Spalte von A in alle Spalten kopiert. Also gilt

$$\begin{aligned} & H^{\otimes n} \cdot E_{1,1} \cdot H^{\otimes n} \\ = \frac{1}{2^{n/2}} \cdot \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & * & \dots & * \\ \vdots & & \ddots & \vdots \\ 1 & * & \dots & * \end{pmatrix} \cdot \frac{1}{2^{n/2}} \cdot \begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & 0 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix} & = \frac{1}{2^n} \cdot \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 1 \\ \vdots & & \ddots & \vdots \\ 1 & 1 & \dots & 1 \end{pmatrix}. \end{aligned}$$

Wegen $\frac{1}{2^n} = \frac{1}{N}$ ergibt sich dann aus $(*)$ weiter:

$$\begin{aligned} - H^{\otimes n} \cdot D \cdot H^{\otimes n} &= - I + 2 \cdot H^{\otimes n} \cdot E_{1,1} \cdot H^{\otimes n} \\ &= \begin{pmatrix} -1 & 0 & \dots & 0 \\ 0 & -1 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & -1 \end{pmatrix} + \frac{2}{N} \cdot \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 1 \\ \vdots & & \ddots & \vdots \\ 1 & 1 & \dots & 1 \end{pmatrix} \end{aligned}$$

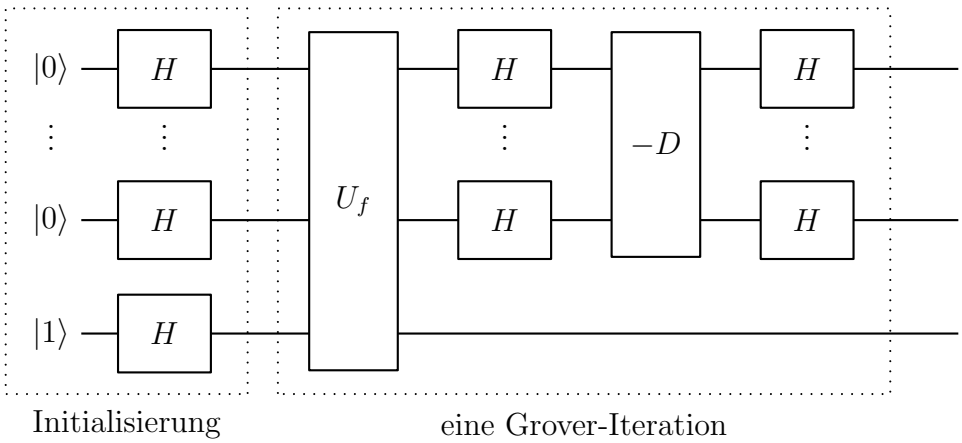
und damit die behauptete Gestalt von S.

Zusammenfassung:

Eine *Grover-Iteration* besteht aus der Invertierung der Amplitude des gesuchten Elements, also der Anwendung von U_f, und einer anschließenden Spiegelung am Mittelwert, also aus S, beziehungsweise – wenn man das Hilfsqubit von U_f mit berücksichtigt – aus $S \otimes I$. Wegen der Darstellung

$$S = H^{\otimes n} \cdot (-D) \cdot H^{\otimes n} \qquad \text{mit} \quad D = \begin{pmatrix} -1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

kann man den Start des Algorithmus und eine erste Iteration als Schaltkreis folgendermaßen darstellen:



6.2 Genauere Analyse

Berechnung der Amplituden:

Im Folgenden wird das für U_f nötige Hilfsqubit außer Acht gelassen.

Bei der Wirkung einer Grover-Iteration auf einen Zustand $|x\rangle_n$, $x \in \{0, \ldots, N-1\}$, gibt es zwei Fälle:

1. Fall: $|x\rangle_n$ ist nicht der gesuchte Zustand: $x \neq x_0$.
2. Fall: $|x\rangle_n$ ist der gesuchte Zustand: $x = x_0$.

Die Amplituden der nicht-gesuchten Zustände entwickeln sich alle gleich. Für die Analyse einer Iteration braucht man also nur zwei verschiedene Amplituden zu unterscheiden:

1. Sei α die Amplitude der nicht-gesuchten Zustände.
2. Sei α_0 die Amplitude des gesuchten Zustands.

Nach Anwendung von U_f hat man

$$\widetilde{\alpha} \;=\; \alpha \qquad \text{und} \qquad \widetilde{\alpha_0} \;=\; -\alpha_0.$$

Die neuen Werte α_{neu} und $\alpha_{0,\text{neu}}$ erhält man aus $\widetilde{\alpha}$ und $\widetilde{\alpha_0}$ durch Multiplikation des entsprechenden Zustandsvektors mit S. Wegen der Symmetrie kann man dabei o.B.d.A annehmen, dass der oberste Zustand der gesuchte ist. Dann ist

$$\begin{pmatrix} \alpha_{0,\text{neu}} \\ \alpha_{\text{neu}} \\ \vdots \\ \alpha_{\text{neu}} \end{pmatrix} = \begin{pmatrix} \frac{2}{N}-1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N}-1 & \cdots & \frac{2}{N} \\ \vdots & & \ddots & \vdots \\ \frac{2}{N} & & \cdots & \frac{2}{N}-1 \end{pmatrix} \cdot \begin{pmatrix} \widetilde{\alpha_0} \\ \widetilde{\alpha} \\ \vdots \\ \widetilde{\alpha} \end{pmatrix}.$$

Damit sieht man:

$$\begin{aligned} \alpha_{\text{neu}} &= \frac{2}{N} \cdot \widetilde{\alpha_0} + \Big(\frac{2}{N} - 1\Big) \cdot \widetilde{\alpha} + (N-2) \cdot \frac{2}{N} \cdot \widetilde{\alpha} \\ &= \frac{2}{N} \cdot (-\alpha_0) + \Big(\frac{2}{N} - 1 + 2 - \frac{4}{N}\Big) \cdot \alpha \\ &= -\frac{2}{N} \cdot \alpha_0 + \Big(1 - \frac{2}{N}\Big) \cdot \alpha, \\ \alpha_{0,\text{neu}} &= \Big(\frac{2}{N} - 1\Big) \cdot \widetilde{\alpha_0} + (N-1) \cdot \frac{2}{N} \cdot \widetilde{\alpha} \\ &= \Big(1 - \frac{2}{N}\Big) \cdot \alpha_0 + \frac{2(N-1)}{N} \cdot \alpha. \end{aligned}$$

Es bietet sich an, die Summe der nicht-gesuchten Zustände zusammenzufassen:

$$\begin{aligned}\sum_{\substack{x=0\\x\neq x_0}}^{N-1} \alpha\,|x\rangle_n &= \alpha\cdot\sum_{\substack{x=0\\x\neq x_0}}^{N-1}|x\rangle_n \\ &= \alpha\cdot\sqrt{N-1}\cdot|x_0\rangle_n^{\perp} \quad \text{mit} \quad |x_0\rangle_n^{\perp} := \frac{1}{\sqrt{N-1}}\sum_{\substack{x=0\\x\neq x_0}}^{N-1}|x\rangle_n\,.\end{aligned}$$

Der Faktor $\frac{1}{\sqrt{N-1}}$ dient dabei dazu, dass $|x_0\rangle_n^{\perp}$ die Länge 1 hat.

Bezeichnet man mit $\alpha_\perp$ die Amplitude von $|x_0\rangle_n^{\perp}$, also

$$\alpha_\perp \;=\; \alpha\cdot\sqrt{N-1} \qquad \text{bzw.} \qquad \alpha \;=\; \frac{1}{\sqrt{N-1}}\cdot\alpha_\perp,$$

so erhält man

$$\begin{aligned}\alpha_{\perp,\text{neu}} &= \alpha_{\text{neu}}\cdot\sqrt{N-1} \\ &= \left(-\frac{2}{N}\alpha_0 \;+\; \Big(1-\frac{2}{N}\Big)\alpha\right)\cdot\sqrt{N-1} \\ &= -\frac{2\sqrt{N-1}}{N}\alpha_0 \;+\; \Big(1-\frac{2}{N}\Big)\cdot\alpha_\perp, \\ \alpha_{0,\text{neu}} &= \Big(1-\frac{2}{N}\Big)\alpha_0 \;+\; \frac{2(N-1)}{N}\frac{1}{\sqrt{N-1}}\cdot\alpha_\perp \\ &= \Big(1-\frac{2}{N}\Big)\alpha_0 \;+\; \frac{2\sqrt{N-1}}{N}\cdot\alpha_\perp.\end{aligned}$$

Dies kann man interpretieren als eine Abbildung in der zweidimensionalen Ebene, die durch $|x_0\rangle_n$ und $|x_0\rangle_n^{\perp}$ aufgespannt wird. Dabei ist es üblich, $|x_0\rangle_n^{\perp}$ als ersten (waagerechten) Vektor anzusehen und $|x_0\rangle_n$ als zweiten (senkrechten) Vektor. Die Amplituden $\alpha_\perp$ bzw. α_0 von $|x_0\rangle_n^{\perp}$ bzw. $|x_0\rangle_n$ ändern sich gemäß

$$\begin{pmatrix}\alpha_{\perp,\text{neu}}\\ \\ \alpha_{0,\text{neu}}\end{pmatrix} \;=\; \begin{pmatrix}1-\frac{2}{N} & -\frac{2\sqrt{N-1}}{N}\\ \frac{2\sqrt{N-1}}{N} & 1-\frac{2}{N}\end{pmatrix}\cdot\begin{pmatrix}\alpha_\perp\\ \\ \alpha_0\end{pmatrix}.$$

Die Matrix ist eine orthogonale Matrix, denn offensichtlich stehen die Spalten senkrecht aufeinander, und für die Länge der Spalten erhält man

$$\begin{aligned}\left(1-\frac{2}{N}\right)^2+\left(\frac{2\sqrt{N-1}}{N}\right)^2 &= 1-2\cdot\frac{2}{N}+\frac{4}{N^2}+\frac{4(N-1)}{N^2} \\ &= 1-\frac{4}{N}+\frac{4}{N^2}+\frac{4}{N}-\frac{4}{N^2} \;=\; 1.\end{aligned}$$

Damit ist die Matrix eine zweidimensionalen Drehmatrix $\begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix}$ mit dem Drehwinkel β, falls $\cos\beta = 1 - \frac{2}{N}$, also $\beta = \arccos\left(1 - \frac{2}{N}\right)$ ist.

Beispiele:

Für $N = 4$ erhält man

$$\begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix},$$

was einer Drehmatrix zu $\beta = \arccos\left(\frac{1}{2}\right) = 60°$ entspricht.

Für $N = 8$ erhält man

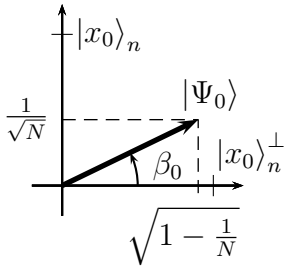
$$\begin{pmatrix} \frac{3}{4} & -\frac{\sqrt{7}}{4} \\ \frac{\sqrt{7}}{4} & \frac{3}{4} \end{pmatrix}.$$

was einer Drehmatrix zu $\beta = \arccos\left(\frac{3}{4}\right) \approx 41,4°$ entspricht.

Geometrische Interpretation:

Nach der Initialisierung hat man wegen $\frac{1}{2^{n/2}} = \frac{1}{\sqrt{N}}$ eine gleichmäßige Überlagerung

$$\begin{aligned} |\Psi_0\rangle &= \frac{1}{\sqrt{N}} \sum_{x=0}^{2^n-1} |x\rangle_n = \frac{1}{\sqrt{N}} |x_0\rangle_n + \frac{1}{\sqrt{N}} \sum_{\substack{x=0 \\ x\neq x_0}}^{2^n-1} |x\rangle_n \\ &= \frac{1}{\sqrt{N}} |x_0\rangle_n + \frac{1}{\sqrt{N}} \cdot \sqrt{N-1} \cdot |x_0\rangle_n^{\perp} \\ &= \frac{1}{\sqrt{N}} |x_0\rangle_n + \sqrt{1 - \frac{1}{N}} \cdot |x_0\rangle_n^{\perp}. \end{aligned}$$

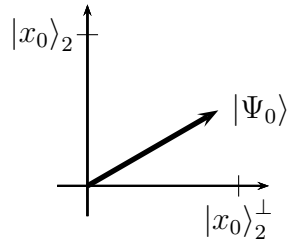


Dies entspricht einem Winkel β_0 gegenüber der $|x_0\rangle_n^{\perp}$-Achse, den man wegen der Länge 1 von $|\Psi_0\rangle$ berechnen kann durch $\beta_0 = \arccos\sqrt{1 - \frac{1}{N}}$.

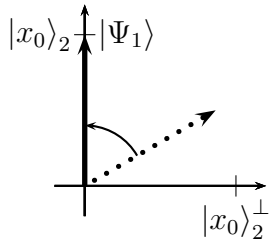
Mit jeder Iteration wird nun um den Winkel $\beta = \arccos\left(1 - \frac{2}{N}\right)$ gedreht.

Beispiele:

Für $N = 4$ startet man bei $\beta_0 = \arccos\sqrt{1 - \frac{1}{4}} = \arccos\frac{\sqrt{3}}{2} = 30°$ und dreht um $\beta = 60°$, so dass man nach einer Iteration bei 90° und damit im Zustand $|x_0\rangle_2$ ist.

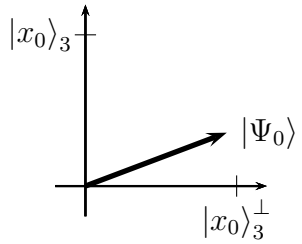


nach Initialisierung

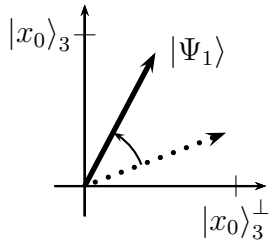


nach einer Grover-Iteration

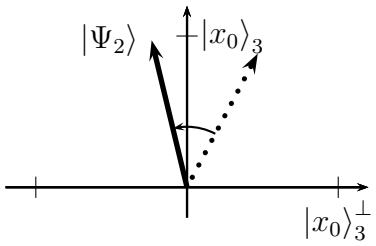
Für $N = 8$ startet man bei $\beta_0 = \arccos\sqrt{\frac{7}{8}} \approx 20,7°$ und dreht um $\beta \approx 41,4°$, so dass man nach einer Iteration bei ca. $62,1°$, nach zwei Iterationen bei ca. $103,5°$ und nach drei Iterationen bei ca. $144,9°$ ist.



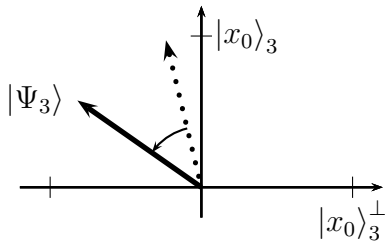
nach Initialisierung



nach einer Grover-Iteration



nach zwei Grover-Iterationen



nach drei Grover-Iterationen

Dies entspricht genau den Amplituden des gesuchten Elements im einführenden Beispiel:

$$\begin{aligned}
|\Psi_0\rangle &\approx 0.94 \cdot |x_0\rangle_3^\perp + 0.35 \cdot |x_0\rangle_3 , \\
|\Psi_1\rangle &\approx 0.47 \cdot |x_0\rangle_3^\perp + 0.88 \cdot |x_0\rangle_3 , \\
|\Psi_2\rangle &\approx -0.23 \cdot |x_0\rangle_3^\perp + 0.97 \cdot |x_0\rangle_3 , \\
|\Psi_3\rangle &\approx -0.82 \cdot |x_0\rangle_3^\perp + 0.57 \cdot |x_0\rangle_3 ,
\end{aligned}$$

Bemerkung:

In den Beispielen fällt auf, dass der Winkel β_0 nach der Initialisierung genau der Hälfte des Drehwinkels β entspricht. Tatsächlich kann man mittels Additionstheoremen zeigen, dass allgemein gilt:

$$\beta_0 = \arccos\sqrt{1 - \frac{1}{N}} \;=\; \frac{1}{2} \cdot \beta \qquad \text{mit} \qquad \beta = \arccos\left(1 - \frac{2}{N}\right).$$

Fazit:

Nach k Grover-Iterationen besitzt $|\Psi_k\rangle$ im $|x_0\rangle_n^\perp$-$|x_0\rangle_n$-Koordinatensystem einen Winkel

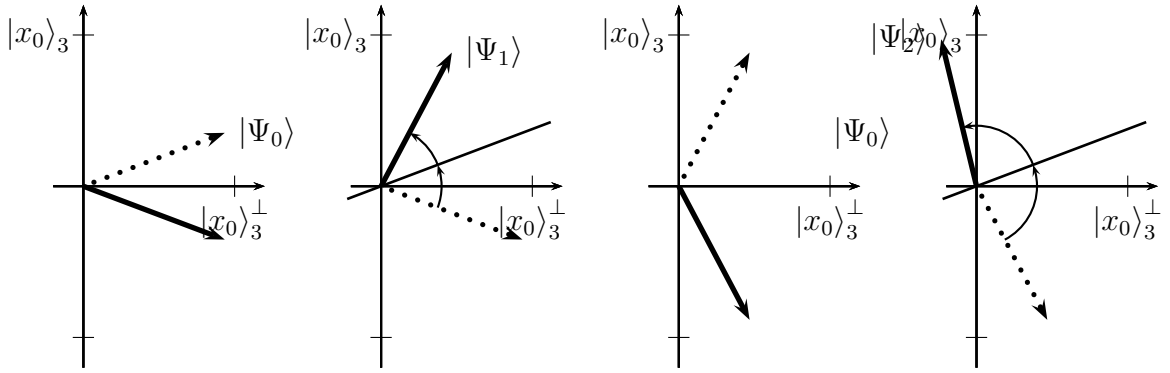
$$\beta_k \;=\; (k + \tfrac{1}{2}) \cdot \beta \qquad \text{mit} \qquad \beta = \arccos\left(1 - \frac{2}{N}\right), \quad N = 2^n$$

zur $|x_0\rangle_n^\perp$-Achse.

Alternative Interpretation:

Man kann eine Grover-Iteration im $|x_0\rangle_n^\perp$-$|x_0\rangle_n$-Koordinatensystem auch folgendermaßen deuten:

- Das Invertieren der Amplitude des gesuchten Elements bedeutet eine Spiegelung des Zustands $|\Psi_k\rangle$ an der $|x_0\rangle_n^\perp$-Achse.
- Die Spiegelung der Amplituden am Mittelwert bedeutet eine Spiegelung an einer Achse in Richtung des initialen (gleichmäßig überlagerten) Zustands $|\Psi_0\rangle$.



Invertierung Spiegelung Invertierung Spiegelung

Wieviel Iterationen braucht man?:

Die Anzahl k der Iterationen sollte so sein, dass man zu einem Zustand kommt, der (fast) in $|x_0\rangle_n$-Richtung liegt. Bei einem Drehwinkel β sollte also $(k+\frac{1}{2})\cdot\beta \approx \frac{\pi}{2}$ sein, also $k \approx \frac{\pi}{2\beta} - \frac{1}{2}$

Eine näherungsweise Abhängigkeit zwischen β und N erhält man durch den Beginn der Potenzreihenentwicklung des Cosinus:

$$1 - \frac{2}{N} \;=\; \cos\beta \;\approx\; 1 - \tfrac{1}{2}\beta^2, \qquad \text{also} \quad \beta^2 \approx \frac{4}{N} \quad \Leftrightarrow \quad \beta \approx \frac{2}{\sqrt{N}}.$$

Für die Anzahl der Iterationen erhält man

$$k \;\approx\; \frac{\pi}{2\cdot\frac{2}{\sqrt{N}}} - \tfrac{1}{2} \;=\; \frac{\pi}{4}\sqrt{N} - \tfrac{1}{2}.$$

Fazit:

Beim Grover-Algorithmus erhält man bei einer Messung nach ca. $\frac{\pi}{4}\sqrt{N} - \frac{1}{2}$ Iterationen mit hoher Wahrscheinlich den gesuchten Zustand $|x_0\rangle_n$.

Der Grover-Algorithmus kommt mit $O(\sqrt{N})$ Aufrufen der Funktion f aus.

6.3 Varianten und Ergänzungen

Mehrere mögliche Suchergebnisse:

Bisher wurde davon ausgegangen, dass man genau *ein* Element sucht.

Wie ist die Situation, wenn es genau r mögliche Treffer gibt?

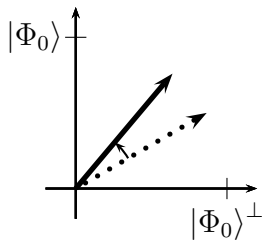
Statt bei *einem* Element werden dann die Amplituden bei r Elementen durch das Orakel invertiert.

Man kann nun eine genauere Analyse wie in Abschnitt 6.2 durchführen:

Weiterhin gilt: Alle gesuchten Elemente haben eine einheitliche Amplitude und alle nicht-gesuchten Elemente haben eine einheitliche Amplitude. Dies kann man wieder in einer zweidimensionalen Ebene betrachten, die einerseits von der gleichmäßigen Überlagerung $|\Phi_0\rangle$ der gesuchten Zustände (in Verallgemeinerung von $|x_0\rangle_n$) und andererseits von der gleichmäßigen Überlagerung $|\Phi_0\rangle^\perp$ der nicht-gesuchten Zustände (in Verallgemeinerung von $|x_0\rangle_n^\perp$) aufgespannt wird.

Mit entsprechender Rechnung erhält man, dass eine Grover-Iteration eine Drehung um den Winkel β bewirkt mit

$$\cos\beta \;=\; 1 - \frac{2r}{N},$$



und dass die Initialisierung zu einem Winkel $\beta_0 = \frac{1}{2}\beta$ führt, man nach k Iterationen also einen Winkel $(k + \frac{1}{2})\beta$ erhält.

Bei kleinem $\frac{r}{N}$, also großem N und verhältnismäßig kleinem r, erhält man mit der Potenzreihen-Näherung

$$\beta \;\approx\; \frac{2}{\sqrt{N/r}} \;=\; \frac{2\sqrt{r}}{\sqrt{N}}.$$

Für $k \approx \frac{\pi}{4} \cdot \sqrt{\frac{N}{r}} - \frac{1}{2}$ hat man also einen Gesamtwinkel von ca. $\frac{\pi}{2}$, so dass eine Messung ziemlich wahrscheinlich einen Zustand aus $|\Phi_0\rangle$, also einen gesuchten Zustand ergibt.

Fazit:

Gibt es r mögliche Suchergebnisse, erhält man beim Grover-Algorithmus bei einer Messung nach ca. $\frac{\pi}{4}\sqrt{\frac{N}{r}} - \frac{1}{2}$ Iterationen mit hoher Wahrscheinlich einen gesuchten Zustand.

Der Grover-Algorithmus kommt also auch dann mit $O(\sqrt{N})$ Aufrufen der Funktion f aus.

Unbekannte Anzahl von Suchergebnissen:

Ist die Anzahl der Suchergebnisse r nicht bekannt, so kann man eine zufällige Anzahl k_0 von Iterationen, $k_0 \in \{1, \ldots, \sqrt{N}\}$, wählen.

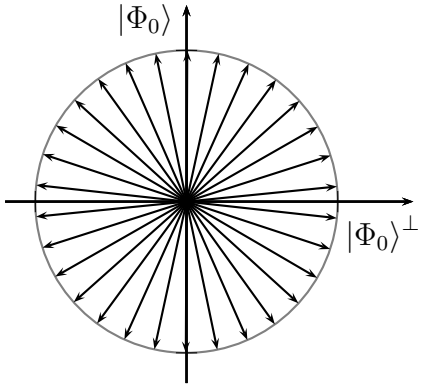
Die Wahrscheinlichkeit, bei einer Messung einen gesuchten Zustand zu erhalten, ist dann ungefähr 1/2. Dies kann man sich folgendermaßen plausibilisieren:

Betrachtet wird wieder die zweidimensionalen Ebene, die einerseits von der gleichmäßigen Überlagerung $|\Phi_0\rangle$ der gesuchten Zustände und andererseits von der gleichmäßigen Überlagerung $|\Phi_0\rangle^\perp$ der nicht-gesuchten Zustände aufgespannt wird.

Für $r = 1$ erhält man den kleinsten Drehwinkel; die Zustände nach k_0 Iterationen $k_0 \in \{1, \ldots, \sqrt{N}\}$ sind dann quasi gleichverteilt mit Winkeln zwischen 0 und 90°.

Bei größerem r sind die Zustände über größere Bereiche gleichverteilt.

Geht man davon aus, dass die Zustände über den ganzen Kreis gleichverteilt sind, so kann man den entsprechenden Winkel φ als gleichverteilt in $[0, 2\pi]$ ansehen.



Bei einem Winkel φ ist die Amplitude von $|\Phi_0\rangle$ gleich $\sin\varphi$, die Wahrscheinlichkeit, einen Zustand in $|\Phi_0\rangle$, also einen gesuchten Zustand, zu messen, also $\sin^2\varphi$. Die Gesamtwahrscheinlichkeit p bei einem in $[0, 2\pi]$ gleichverteilten Winkel φ ist also

$$p \;=\; \int_0^{2\pi} \frac{1}{2\pi} \cdot \sin^2\varphi \,\mathrm{d}\varphi \;=\; \frac{1}{2\pi} \cdot \frac{1}{2} \cdot 2\pi \;=\; \frac{1}{2}.$$

Fazit:

Bei einer unbekannten Anzahl möglicher Suchergebnisse, erhält man beim Grover-Algorithmus bei einer Messung nach einer zufälligen Anzahl k_0 von Iterationen, $k_0 \in \{1, \ldots, \sqrt{N}\}$, mit Wahrscheinlich ungefähr gleich 1/2 einen gesuchten Zustand.

Der Grover-Algorithmus kommt also auch dann mit $O(\sqrt{N})$ Aufrufen der Funktion f aus.

Aussagenlogische Funktion als Orakel:

Als Funktion, die dem Orakel zugrunde liegt, kann man beispielsweise eine aussagenlogische Funkion nehmen, z.B.

$$F(x_0, x_1, x_2, x_3) \;=\; (x_0 \vee x_1 \vee \overline{x_3}) \wedge (x_0 \vee \overline{x_2} \vee x_3) \wedge (\overline{x_1} \vee \overline{x_2} \vee x_3).$$

Der Grover-Algorithmus kann mit einem Aufwand $O(\sqrt{N})$ eine erfüllbare Belegung finden.

Durch Überprüfung der Funktion nach der Messung sieht man schnell, ob der gemessene Zustand tatsächlich eine Belegung ist, bei der die Formel erfüllt ist. Hat man nach hinreichend vielen Versuchen immer noch keine gültige Belegung, ist die Formel mit ziemlich hoher Wahrscheinlichkeit nicht erfüllbar.

Insbesondere lassen sich so *3-SAT*-Probleme behandeln. Dabei betrachtet man eine aussagenlogische Formel, die eine konjunktive Normalform mit höchstens 3 Literalen pro Klausel besitzt. Der Aufwand 2^n bei reinem Durchprobieren bei n Variablen wird durch den Grover-Algorithmus reduziert auf $O(\sqrt{2^n})$, was aber immer noch exponentieller Aufwand ist.

Bemerkung:

Man kann zeigen, dass der Grover-Algorithmus in der Hinsicht optimal ist, dass es keinen Quanten-Algorithmus gibt, der mit weniger als $O(\sqrt{N})$ Orakel-Aufrufen auskommt.

7 Teleportation und dichte Codierung

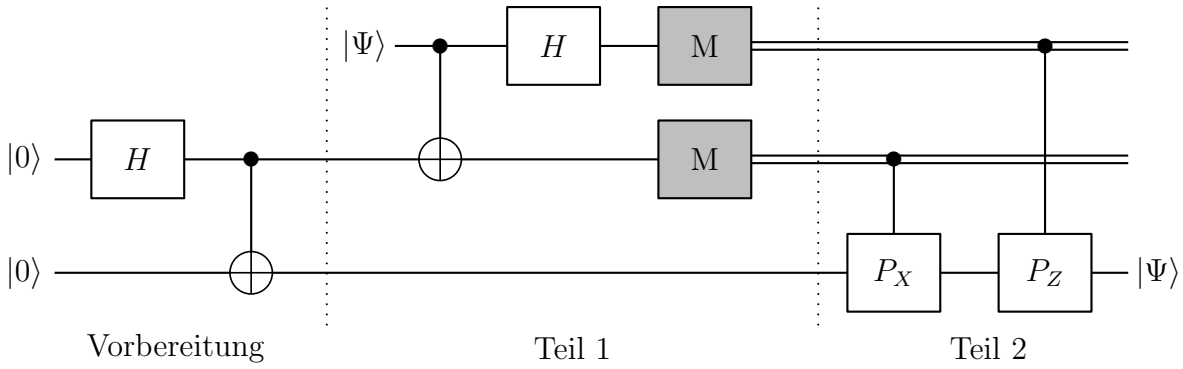
7.1 Teleportation

Ziel:

Bei der Teleportation soll ein Qubit $|\Psi\rangle$ von Alice zu Bob „teleportiert“ werden, ohne dass es einen Quantenkanal dafür zwischen Alice und Bob gibt. Allerdings teilen sich Alice und Bob die beiden verschränkten Qubits eines Bell-Zustands $\frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$ und können diese nutzen.

Die Verschränkung wird genutzt, um das Qubit $|\Psi\rangle$ von Alice zu Bob zu teleportieren.

Der Algorithmus:



Grobe Struktur:

Die Vorbereitung erzeugt ein Bell-Paar. Das unterste Qubit kommt zu Bob, das obere - im Teil 1 und 2 also das mittlere - kommt zu Alice.

Im Teil 1 führt Alice mit dem zu teleportierenden Qubit $|\Psi\rangle$ und ihrem Qubit des Bell-Paars die angegebenen Transformationen durch und misst dann beide Qubits. Durch die Verschränkung ändert die Messung auch etwas an dem untersten Qubit.

Die Information der Messung übermittelt Alice dann über einen klassischen Kanal an Bob.

Im Teil 2 führt Bob abhängig von den Messergebnissen, die er von Alice erhält, die beschriebenen Transformationen an seinem Qubit des Bell-Paares aus.

Behauptet wird, dass am Ende dieses Bit in einem Zustand ist, wie es $|\Psi\rangle$ zu Beginn war.

Bemerkung:

Statt des kontrollierten P_X-Gatters in Teil 2 könnte man auch ein CNOT-Gatter notieren; da allerdings in der Analyse der Gedanke des Vertauschens wichtig ist, ist das hier als als kontrollierten P_X-Gatter notiert.

Genaue Analyse:

Vorbereitung:

In der Vorbereitung wird ein Bell-Paar erzeugt:

Aus $|00\rangle$ wird durch die Hadamard-Transformation

$$\tfrac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big) \otimes |0\rangle \;=\; \tfrac{1}{\sqrt{2}}\big(\,|00\rangle + |10\rangle\,\big),$$

und durch das anschließende CNOT-Gatter wird daraus der Bell-Zustand

$$\tfrac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big).$$

Teil 1 - Alice:

Nun kommt das zu teleportierende Qubit $|\Psi\rangle$ hinzu. Dieses sei im Zustand $|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$. Die drei Qubits sind also im Zustand

$$\begin{aligned}&\big(\alpha\,|0\rangle + \beta\,|1\rangle\,\big) \otimes \Big(\tfrac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big)\Big)\\ =\; &\tfrac{\alpha}{\sqrt{2}}\,|000\rangle + \tfrac{\beta}{\sqrt{2}}\,|100\rangle + \tfrac{\alpha}{\sqrt{2}}\,|011\rangle + \tfrac{\beta}{\sqrt{2}}\,|111\rangle\,.\end{aligned}$$

Durch das CNOT-Gatter mit dem ersten Qubit als Kontroll-Qubit und dem zweiten als Ziel-Qubit wird dies zu

$$\tfrac{\alpha}{\sqrt{2}}\,|000\rangle + \tfrac{\beta}{\sqrt{2}}\,|110\rangle + \tfrac{\alpha}{\sqrt{2}}\,|011\rangle + \tfrac{\beta}{\sqrt{2}}\,|101\rangle\,.$$

Durch die Hadamard-Transformation angewendet auf das erste Bit wird dadurch

$$\begin{aligned}&\tfrac{\alpha}{\sqrt{2}} \cdot \tfrac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big) \otimes |00\rangle + \tfrac{\beta}{\sqrt{2}} \cdot \tfrac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big) \otimes |10\rangle\\ &\quad + \tfrac{\alpha}{\sqrt{2}} \cdot \tfrac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big) \otimes |11\rangle + \tfrac{\beta}{\sqrt{2}} \cdot \tfrac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big) \otimes |01\rangle\\ =\; &\tfrac{1}{2}\big(\alpha\,|000\rangle + \alpha\,|100\rangle + \beta\,|010\rangle - \beta\,|110\rangle\\ &\quad + \alpha\,|011\rangle + \alpha\,|111\rangle + \beta\,|001\rangle - \beta\,|101\rangle\,\big).\end{aligned}$$

Um zu sehen, was bei einer Messung der ersten beiden Qubits geschieht, ist es sinnvoll, den Ausdruck umzusortieren entsprechend der verschiedenen Fälle für die ersten beiden Qubits:

$$\begin{aligned}&\tfrac{1}{2}\big(\alpha\,|000\rangle + \alpha\,|100\rangle + \beta\,|010\rangle - \beta\,|110\rangle\\ &\quad + \alpha\,|011\rangle + \alpha\,|111\rangle + \beta\,|001\rangle - \beta\,|101\rangle\,\big)\\ =\; &\tfrac{1}{2}\big(\alpha\,|000\rangle + \beta\,|001\rangle + \beta\,|010\rangle + \alpha\,|011\rangle\\ &\quad + \alpha\,|100\rangle - \beta\,|101\rangle - \beta\,|110\rangle + \alpha\,|111\rangle\,\big)\\ =\; &\tfrac{1}{2}\Big(\,|00\rangle \otimes \big(\alpha\,|0\rangle + \beta\,|1\rangle\,\big) + |01\rangle \otimes \big(\beta\,|0\rangle + \alpha\,|1\rangle\,\big)\\ &\quad + |10\rangle \otimes \big(\alpha\,|0\rangle - \beta\,|1\rangle\,\big) + |11\rangle \otimes \big(-\beta\,|0\rangle + \alpha\,|1\rangle\,\big)\Big).\end{aligned}$$

Die Messung der ersten beiden Qubits ergibt also die Zustände $|00\rangle$, $|01\rangle$, $|10\rangle$ oder $|11\rangle$ mit jeweils gleichen Wahrscheinlichkeiten $\frac{1}{4}(|\alpha|^2 + |\beta|^2) = \frac{1}{4}$. Dabei kollabiert das dritte Qubit jeweils wie folgt:

1. Fall: Messung von $|00\rangle$: $\alpha|0\rangle + \beta|1\rangle$,
2. Fall: Messung von $|01\rangle$: $\beta|0\rangle + \alpha|1\rangle$,
3. Fall: Messung von $|10\rangle$: $\alpha|0\rangle - \beta|1\rangle$,
4. Fall: Messung von $|11\rangle$: $-\beta|0\rangle + \alpha|1\rangle$.

Teil 2 - Bob:

Je nach Messergebnis wird das dritte Qubit modifiziert:

Falls beim zweiten Qubit 1 gemessen wurde (2. und 4. Fall) wird ein P_X-Gatter angewendet. Dieses vertauscht die Amplituden von $|0\rangle$ und $|1\rangle$.

Falls beim ersten Qubit 1 gemessen wurde (3. und 4. Fall) wird ein P_Z-Gatter angewendet. Dieses multipliziert die Amplitude von $|1\rangle$ mit -1.

Danach ist das dritte Qubit in jedem Fall im Zustand $\alpha|0\rangle + \beta|1\rangle = |\Psi\rangle$.

Man beachte, dass dabei die Reihenfolge der kontrollierten P_X- und P_Z-Gatter wichtig ist. In anderer Reihenfolge ergibt sich ein anderes Ergebnis!

Geschichtliches:

1993: Idee der Teleportation

1997: Zeilinger u. Co realisieren eine Quantenteleportation über einen Meter.

2003: Gisin (Genf) führt eine Teleportation über Glasfaserkabel über 2km durch.

2004: Zeilinger führt eine Teleportation über 600m von einem Ufer der Donau zum anderen aus.

2010: Xian Min Lin (Shanghai): Teleportation über 16km

2012: Pan Jian Wei (chin. Akademie der Wissenschaften): Teleportation über 97km

2012: Zeilinger: Teleportation über 143km zwischen La Palma und Teneriffa

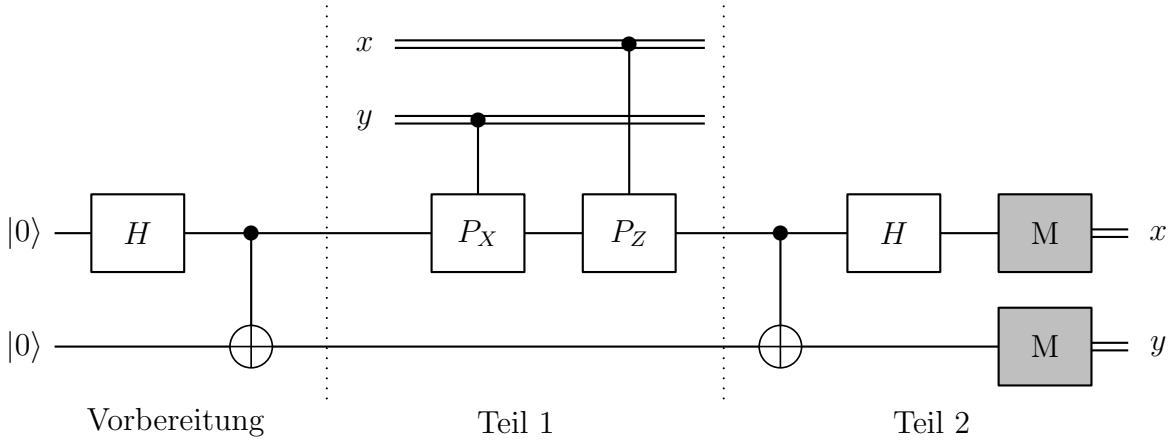
2017: Pan Jian Wei und Zeilinger: Teleportation über 1400km zwischen der Erde und einem Satelliten

7.2 Dichte Codierung

Ziel:

Bei der dichten Codierung soll Information mittels eines Qubits von Alice zu Bob transportiert werden. Wenn Alice und Bob sich die beiden verschränkten Qubits eines Bell-Zustands $\frac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big)$ teilen, kann man durch die Übertragung *eines* Qubits den Informationsgehalt von *zwei* klassischen Bits übertragen.

Der Algorithmus:



Grobe Struktur:

Die Vorbereitung erzeugt ein Bell-Paar. Das unterste Qubit kommt zu Bob, das andere kommt zu Alice.

Im Teil 1 sind x und y zwei klassische Bits mit möglichen Zuständen 0 und 1. Je nach Zustand wendet Alice das P_X- bzw. P_Z-Gatter auf ihr Qubit des Bell-Paars an.

Das Qubit von Alice wird dann an Bob übermittelt.

Im Teil 2 führt Bob die angegebenen Transformationen und Messungen auf den beiden Qubits aus.

Behauptet wird, dass er dadurch die Informationen x und y extrahieren kann.

Genaue Analyse:

Vorbereitung:

In der Vorbereitung wird wie bei der Teleportation ein Bell-Paar erzeugt:

Aus $|00\rangle$ wird durch die Hadamard-Transformation

$$\tfrac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big) \otimes |0\rangle \;=\; \tfrac{1}{\sqrt{2}}\big(\,|00\rangle + |10\rangle\,\big),$$

und durch das anschließende CNOT-Gatter wird daraus der Bell-Zustand

$$\tfrac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big).$$

Teil 1 - Alice:

In Abhängigkeit von den Zuständen von x und y gibt es folgende Fälle für die Transformation des oberen Qubits und damit des Bellpaares:

1. Fall: $x = 0$ und $y = 0$.

   Dann geschieht keine Transformation und am Ende von Teil 1 ist das Qubit-Paar im Zustand

   $$\tfrac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big).$$

2. Fall: $x = 0$ und $y = 1$.

   Dann wird P_X auf das erste Qubit angewendet; am Ende von Teil 1 ist das Qubit-Paar daher im Zustand

   $$\tfrac{1}{\sqrt{2}}\big(\,|10\rangle + |01\rangle\,\big).$$

3. Fall: $x = 1$ und $y = 0$.

   Dann wird P_Z auf das erste Qubit angewendet; am Ende von Teil 1 ist das Qubit-Paar daher im Zustand

   $$\tfrac{1}{\sqrt{2}}\big(\,|00\rangle - |11\rangle\,\big).$$

4. Fall: $x = 1$ und $y = 1$.

   Dann wird zunächst P_X auf das erste Qubit angewendet, so dass man den Zustand $\frac{1}{\sqrt{2}}\big(\,|10\rangle + |01\rangle\,\big)$ erhält. Anschließend wird P_Z auf das erste Qubit angewendet. Am Ende von Teil 1 ist das Qubit-Paar daher im Zustand

   $$\tfrac{1}{\sqrt{2}}\big(\,-|10\rangle + |01\rangle\,\big).$$

Teil 2 - Bob:

Man erhält folgende Fälle:

1. Fall: $x = 0$ und $y = 0$.

   Der Zustand $\frac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big)$ wird durch das CNOT-Gatter zu

   $$\tfrac{1}{\sqrt{2}}\big(\,|00\rangle + |10\rangle\,\big) \;=\; \tfrac{1}{\sqrt{2}}\big(\big(\,|0\rangle + |1\rangle\,\big) \otimes |0\rangle\,.$$

   Da $H\,|0\rangle = \frac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big)$ und H zu sich selbst invers ist, ergibt die anschließende Hadamard-Transformation auf das erste Qubit $|00\rangle$, so dass beide Messungen garantiert 0 ergeben.

2. Fall: $x = 0$ und $y = 1$.

   Der Zustand $\frac{1}{\sqrt{2}}\big(\,|10\rangle + |01\rangle\,\big)$ wird durch das CNOT-Gatter zu

   $$\tfrac{1}{\sqrt{2}}\big(\,|11\rangle + |01\rangle\,\big) \;=\; \tfrac{1}{\sqrt{2}}(\big(\,|0\rangle + |1\rangle\,\big) \otimes |1\rangle\,.$$

   Da $H\,|0\rangle = \frac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big)$ und H zu sich selbst invers ist, ergibt die anschließende Hadamard-Transformation auf das erste Qubit $|01\rangle$, so dass garantiert die obere Messung 0 und die untere 1 ergibt.

3. Fall: $x = 1$ und $y = 0$.

   Der Zustand $\frac{1}{\sqrt{2}}\big(\,|00\rangle - |11\rangle\,\big)$ wird durch das CNOT-Gatter zu

   $$\tfrac{1}{\sqrt{2}}\big(\,|00\rangle - |10\rangle\,\big) \;=\; \tfrac{1}{\sqrt{2}}(\big(\,|0\rangle - |1\rangle\,\big) \otimes |0\rangle\,.$$

   Da $H\,|1\rangle = \frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big)$ und H zu sich selbst invers ist, ergibt die anschließende Hadamard-Transformation auf das erste Qubit $|10\rangle$, so dass garantiert die obere Messung 1 und die untere 0 ergibt.

4. Fall: $x = 1$ und $y = 1$.

   Der Zustand $\frac{1}{\sqrt{2}}\big(\,-|10\rangle + |01\rangle\,\big)$ wird durch das CNOT-Gatter zu

   $$\tfrac{1}{\sqrt{2}}\big(\,-|11\rangle + |01\rangle\,\big) \;=\; \tfrac{1}{\sqrt{2}}(\big(\,|0\rangle - |1\rangle\,\big) \otimes |1\rangle\,.$$

   Da $H\,|1\rangle = \frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big)$ und H zu sich selbst invers ist, ergibt die anschließende Hadamard-Transformation auf das erste Qubit $|11\rangle$, so dass beide Messungen garantiert 1 ergeben.

Man sieht, dass die Messungen in jedem Fall x und y ergeben.

7.3 Optimalität von Teleportation und dichter Codierung

Kann man Teleportation und dichte Codierung verbessern, konkret:

1. Kann man mit weniger als zwei klassischen Bits den Informationsgehalt eines Qubits übertragen?

   Sei im Idealfall s_{opt} die Anzahl klassischer Bits, die nötig sind, den Informationsgehalt eines Qubits zu übertragen.

   Der Teleportations-Algorithmus realisiert $s = 2$, also $s_{\text{opt}} \leq 2$.

2. Kann man mit einem Qubit mehr als den Informationsgehalt zweier klassischer Bits übertragen?

   Sei im Idealfall t_{opt} die Anzahl klassicher Bits, deren Informationsgehalt mit einem Qubit übertragen werden kann.

   Die dichte Codierung realisiert $t = 2$, also $t_{\text{opt}} \geq 2$.

Also gilt

$$s_{\text{opt}} \;\leq\; 2 \;\leq\; t_{\text{opt}}. \qquad (*)$$

Überträgt man nun den Informationsgehalt von t_{opt} klassischen Bits mit einem Qubit entsprechend 2. und überträgt man dieses Qubit entsprechend 1. mit s_{opt} klassischen Bits, so muss zwangsläufig $s_{\text{opt}} \geq t_{\text{opt}}$ sein.

Damit und mit $(*)$ folgt also $s_{\text{opt}} = t_{\text{opt}}$, so dass die Realisierung mit $s = 2 = t$ optimal ist.

8 Quantenschlüsselaustausch

Vorbemerkung:

Im Folgenden werden zwei bekannte Protokolle vorgestellt, bei denen mit Hilfe eines Quanten-Kanals ein geheimer Schlüssel zwischen zwei beteiligten Personen (Alice und Bob) vereinbart wird. Tatsächlich „entsteht“ der Schlüssel erst während des Protokolls, daher wäre „Quantenschlüsselvereinbarung“ ein besserer Name, aber „Quantenschlüsselaustausch“ ist der geläufige Ausdruck.

Idee beim Quantenschlüsselaustausch:

Die grundsätzliche Idee beim Quantenschlüsselaustausch ist nicht, dass die Übertragung wirklich geheim ist, sondern dass Horcher entdeckt werden können. Die Grundlage dafür bietet das No-cloning-Theorem, das besagt, dass Qubits nicht kopiert werden können. Ein Horcher beeinflusst daher die übertragenen Quanten und kann dadurch erkannt werden.

8.1 Messungen in verschiedenen Basen

Bei den beiden Protokollen spielen Messungen in verschiedenen Basen eine wichtige Rolle, daher werden im Folgenden zunächst derartige Messungen genauer untersucht.

8.1.1 Messung eines Qubits

Bisher wurde gesagt, dass eine Messung eines Qubits $|\Psi\rangle$ die Werte $|0\rangle$ oder $|1\rangle$ ergibt. Nur wenn $|\Psi\rangle = |0\rangle$ bzw. $|\Psi\rangle = |1\rangle$ (bis auf eine Phase) ist, ist das Messergebnis eindeutig. Wenn man beispielsweise $|+\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)$ oder $|-\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)$ misst, erhält man $|0\rangle$ und $|1\rangle$ jeweils mit der Wahrscheinlichkeit $1/2$.

Eine solche Messung wird im folgenden als Messung *in der Standard-Basis* bezeichnet.

Misst man hingegen $H|\Psi\rangle$ (in der Standard-Basis), so ergibt $|\Psi\rangle = |0\rangle$ wegen $H|0\rangle = |+\rangle$ als Messergebnis $|0\rangle$ und $|1\rangle$ jeweils mit der Wahrscheinlichkeit $1/2$, entsprechend bei $|\Psi\rangle = |1\rangle$. Bei $|\Psi\rangle = |+\rangle$ erhält man wegen $H|+\rangle = |0\rangle$ mit Sicherheit $|0\rangle$ und bei $|\Psi\rangle = |-\rangle$ entsprechend mit Sicherheit $|1\rangle$.

Wenn man nur daran interessiert ist, dass die Messergebnisse unterscheidbar sind und man bei bestimmten Basiszuständen mit Sicherheit ein bestimmtes Messergebnis erhält, kann man die letztere Messung auch eine Messung *in der* $\{|+\rangle, |-\rangle\}$*-Basis* nennen. Das Messergebnis $|0\rangle$ wird dann mit $|+\rangle$ identifiziert, man sagt, man misst $|+\rangle$, entsprechend das Messergebnis $|1\rangle$ mit $|-\rangle$.

Dies kann man verallgemeinern:

Hat man zwei zueinander orthogonale Zustände $|\Phi_0\rangle$ und $|\Phi_1\rangle$, so kann man die unitäre Transformation U betrachten, die (eindeutig) definiert ist durch

$$U(|\Phi_0\rangle) \;=\; |0\rangle \qquad \text{und} \qquad U(|\Phi_1\rangle) \;=\; |1\rangle\,.$$

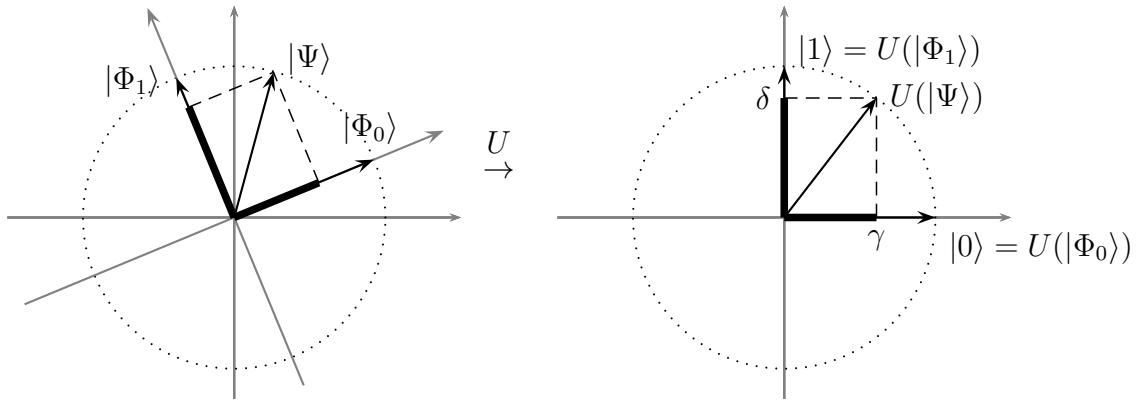
Misst man $U(|\Psi\rangle)$ (in der Standard-Basis), so erhält man bei $|\Psi\rangle = |\Phi_0\rangle$ mit Sicherheit $|0\rangle$ und bei $|\Psi\rangle = |\Phi_1\rangle$ mit Sicherheit $|1\rangle$. Das Messergebnis $|0\rangle$ bzw. $|1\rangle$ wird dann mit $|\Phi_0\rangle$ bzw. $|\Phi_1\rangle$ identifiziert, man sagt, man misst $|\Phi_0\rangle$ bzw. $|\Phi_1\rangle$.

Dies wird als Messung in der $\{|\Phi_0\rangle\,, |\Phi_1\rangle\}$-Basis bezeichnet.

Beispiel:

Betrachtet werden die bzgl. der Standard-Basis um $22.5° = \frac{\pi}{8}$ gedrehten Zustände $|\Phi_0\rangle$ und $|\Phi_1\rangle$, also

$$|\Phi_0\rangle \;=\; \begin{pmatrix} \cos\frac{\pi}{8} \\ \sin\frac{\pi}{8} \end{pmatrix} \qquad \text{und} \qquad |\Phi_1\rangle \;=\; \begin{pmatrix} -\sin\frac{\pi}{8} \\ \cos\frac{\pi}{8} \end{pmatrix}.$$



Die Transformation U, die $|\Phi_0\rangle$ auf $|0\rangle$ und $|\Phi_1\rangle$ auf $|1\rangle$ abbildet, ist dann die umgekehrte Drehung, also eine Drehung um $-\frac{\pi}{8}$.

Das Bild oben zeigt einen Zustand $|\Psi\rangle$ links, der entsprechend im rechten Bild gedreht ist. Sind γ und δ die projizierten Anteile von $U(|\Psi\rangle)$ auf $|0\rangle$ und $|1\rangle$, so sind $|\gamma|^2$ bzw. $|\delta|^2$ die Wahrscheinlichkeiten, bei einer Messung in der Standard-Basis $|0\rangle$ bzw. $|1\rangle$ zu erhalten, bei entsprechender Identifikation also die Messergebnisse $|\Phi_0\rangle$ bzw. $|\Phi_1\rangle$ zu erhalten.

Im Bild links sieht man, dass γ und δ auch direkt als projizierte Anteile von $|\Psi\rangle$ auf die Zustände $|\Phi_0\rangle$ und $|\Phi_1\rangle$ ermittelt werden können.

Wie im Beispiel gilt allgemein: Sind γ und δ die projizierten Anteile eines Zustands $|\Psi\rangle$ auf die (zueinander orthogonalen) Messbasen $|\Phi_0\rangle$ und $|\Phi_1\rangle$, also

$$|\Psi\rangle \;=\; \gamma \cdot |\Phi_0\rangle + \delta \cdot |\Phi_1\rangle\,,$$

so ist $|\gamma|^2$ bzw. $|\delta|^2$ die Wahrscheinlichkeit, bei einer Messung in der $\{|\Phi_0\rangle\,, |\Phi_1\rangle\}$-Basis $|\Phi_0\rangle$ bzw. $|\Phi_1\rangle$ zu messen.

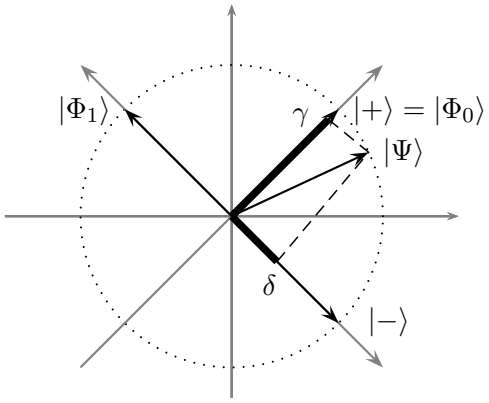
Bemerkung:

Da für die Wahrscheinlichkeiten wegen der Beträge Vorzeichen keine Rolle spielen, ist es unerheblich, ob man als Messbasen $|\Phi_0\rangle$ oder $-|\Phi_0\rangle$ bzw. $|\Phi_1\rangle$ oder $-|\Phi_1\rangle$ betrachtet.

Beispiel:

Die Messung in der $\{|+\rangle, |-\rangle\}$-Basis entspricht einer Messung in einer um $45° = \frac{\pi}{4}$ gedrehten Messbasis:

Bei einer Drehung der Standard-Basis um $45° = \frac{\pi}{4}$ entstehen die Messbasen $|\Phi_0\rangle = |+\rangle$ und $|\Phi_1\rangle = -|-\rangle$.



Einer Darstellung

$$|\Psi\rangle \;=\; \gamma \cdot |+\rangle + \delta \cdot |-\rangle$$

entspricht dann

$$|\Psi\rangle \;=\; \gamma \cdot |\Phi_0\rangle + (-\delta) \cdot |\Phi_1\rangle .$$

Eine Messung in der $\{|+\rangle, |-\rangle\}$-Basis ergibt die Wahrscheinlichkeiten

$$|\gamma|^2 \text{ für } |+\rangle \qquad \text{und} \qquad |\delta|^2 \text{ für } |-\rangle;$$

eine Messung in der $\{|\Phi_0\rangle, |\Phi_1\rangle\}$-Basis ergibt die Wahrscheinlichkeiten

$$|\gamma|^2 \text{ für } |\Phi_0\rangle \qquad \text{und} \qquad |-\delta| = |\delta|^2 \text{ für } |\Phi_1\rangle.$$

8.1.2 Messung verschränkter Qubits

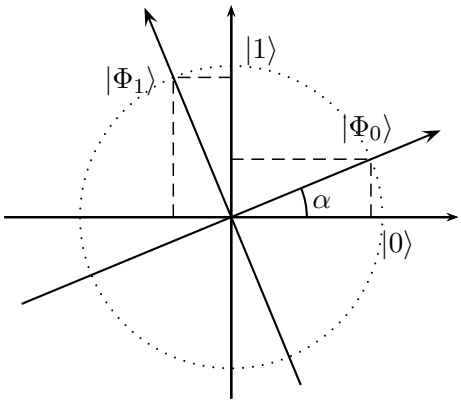
Das Bell-Paar $\frac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big)$:

Misst man eines der Qubits des (verschränkten) Bell-Paars $\frac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big)$ in der Standard-Basis, so erhält man $|0\rangle$ bzw. $|1\rangle$ jeweils mit der Wahrscheinlichkeit $1/2$; dabei kollabiert der Zustand zu $|00\rangle$ bzw. $|11\rangle$, so dass man, wenn man anschließend das andere Qubit in der Standardbasis misst, sicher das gleiche Ergebnis erhält.

Was passiert bei anderen Messbasen?

Eine um den Winkel α gedrehte Basis hat die Basiszustände

$$|\Phi_0\rangle \;=\; \cos\alpha\cdot|0\rangle + \sin\alpha\cdot|1\rangle \qquad \text{und} \qquad |\Phi_1\rangle \;=\; -\sin\alpha\cdot|0\rangle + \cos\alpha\cdot|1\rangle\,.$$



Nun gilt

$$\begin{aligned}
&\tfrac{1}{\sqrt{2}}\big(\,|\Phi_0\rangle\otimes|\Phi_0\rangle + |\Phi_1\rangle\otimes|\Phi_1\rangle\,\big)\\
&= \tfrac{1}{\sqrt{2}}\Big(\big(\cos\alpha\,|0\rangle + \sin\alpha\,|1\rangle\big)\otimes\big(\cos\alpha\,|0\rangle + \sin\alpha\,|1\rangle\big)\\
&\qquad + \big(-\sin\alpha\,|0\rangle + \cos\alpha\,|1\rangle\big)\otimes\big(-\sin\alpha\,|0\rangle + \cos\alpha\,|1\rangle\big)\Big)\\
&= \tfrac{1}{\sqrt{2}}\Big(\cos^2\alpha\,|00\rangle + \cos\alpha\sin\alpha\,|01\rangle + \sin\alpha\cos\alpha\,|10\rangle + \sin^2\alpha\,|11\rangle\\
&\qquad + \sin^2\alpha\,|00\rangle - \sin\alpha\cos\alpha\,|01\rangle - \cos\alpha\sin\alpha\,|10\rangle + \cos^2\alpha\,|11\rangle\Big)\\
&= \tfrac{1}{\sqrt{2}}\Big((\cos^2\alpha+\sin^2\alpha)\,|00\rangle + (\sin^2\alpha+\cos^2\alpha)\,|11\rangle\Big)\\
&= \tfrac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big).
\end{aligned}$$

Damit gilt in einer beliebigen Basis $\{|\Phi_0\rangle, |\Phi_1\rangle\}$:

Misst man eines der Qubits, so erhält man $|\Phi_0\rangle$ bzw. $|\Phi_1\rangle$ jeweils mit Wahrscheinlichkeit $1/2$. Dabei kollabiert der Zustand in der Art, dass man, wenn man anschließend das zweite Qubit in der gleichen Basis misst, sicher das gleiche Ergebnis erhält.

Man sagt, das Bell-Paar $\frac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big)$ ist perfekt korreliert in allen Basen.

Die anderen Bell-Paare:

1. Das Bell-Paar $\frac{1}{\sqrt{2}}\big(\,|01\rangle - |10\rangle\,\big)$.

   Misst man eines der Qubits in der Standard-Basis, so erhält man $|0\rangle$ bzw. $|1\rangle$ jeweils mit den Wahrscheinlichkeiten $1/2$; dabei kollabiert der Zustand so, dass man, wenn man anschließend das zweite Qubit in der Standardbasis misst, sicher das jeweils andere Ergebnis erhält. (Das negative Vorzeichen bei $|10\rangle$ ist für die Messung irrelevant.)

   Man kann zeigen, dass dies in jeder beliebigen Basis $\{|\Phi_0\rangle\,, |\Phi_1\rangle\}$ gilt:

   Misst man eines der Qubits, so erhält man $|\Phi_0\rangle$ bzw. $|\Phi_1\rangle$ jeweils mit Wahrscheinlichkeit $1/2$. Dabei kollabiert der Zustand in der Art, dass man, wenn man anschließend das zweite Qubit in der gleichen Basis misst, sicher das jeweils andere Ergebnis erhält.

   Das Bell-Paar $\frac{1}{\sqrt{2}}\big(\,|01\rangle - |10\rangle\,\big)$ ist perfekt antikorreliert in allen Basen.

2. Das Bell-Paar $\frac{1}{\sqrt{2}}\big(\,|01\rangle + |10\rangle\,\big)$.

   Wie beim Bell-Paar $\frac{1}{\sqrt{2}}\big(\,|01\rangle - |10\rangle\,\big)$ gilt: Bei einer Messung eines der beiden Qubits in der Standard-Basis erhält man offensichtlich die beiden Zustände $|0\rangle$ bzw. $|1\rangle$ jeweils mit Wahrscheinlichkeit $1/2$. Dabei kollabiert der Zustand in der Art, dass man, wenn man anschließend das zweite Qubit in der gleichen Basis misst, sicher das jeweils andere Ergebnis erhält.

   Das Bell-Paar ist also antikorreliert in der Standard-Basis.

   Man kann nachrechnen, dass gilt

   $$\tfrac{1}{\sqrt{2}}\big(\,|+\rangle\otimes|+\rangle \;-\; |-\rangle\otimes|-\rangle\,\big) \;=\; \tfrac{1}{\sqrt{2}}\big(\,|01\rangle + |10\rangle\,\big).$$

   Damit sieht man:

   Bei einer Messung eines der beiden Qubits in der $\{|+\rangle\,, |-\rangle\}$-Basis erhält man die beiden Zustände $|+\rangle$ bzw. $|-\rangle$ jeweils mit Wahrscheinlichkeit $1/2$. Dabei kollabiert der Zustand in der Art, dass man, wenn man anschließend das zweite Qubit in der gleichen Basis misst, sicher das *gleiche* Ergebnis erhält.

   In der $\{|+\rangle\,, |-\rangle\}$-Basis hat man also perfekte Korrelation.

   Man kann nachrechnen: Wenn man in anderen Messbasen eines der Qubits misst, so erhält man jeden der beiden Basiszustände mit gleicher Wahrscheinlichkeit $1/2$. Allerdings kollabiert der Zustand so, dass man über die Messung des anderen Qubits keine sichere Aussage machen kann; es herrscht nur teilweise Korrelation!

3. Das Bell-Paar $\frac{1}{\sqrt{2}}\big(\,|00\rangle - |11\rangle\,\big)$.

   Dieses Bell-Paar verhält sich ähnlich dem vorherigen; man kann nachrechnen:

   Misst man eines der Qubits in irgendeiner Basis, so erhält man jeden der beiden Basiszustände mit gleicher Wahrscheinlichkeit $1/2$.

In der Standard-Basis hat man perfekte Korrelation, d.h., bei Messung des anderen Qubits erhält man genau das gleiche Ergebnis; in der $\{|+\rangle, |-\rangle\}$-Basis hat man perfekte Antikorrelation, d.h., bei Messung des anderen Qubits erhält man genau das andere Ergebnis. In anderen Messbasen herrscht nur teilweise Korrelation.

8.2 BB84-Protokoll

Das BB84-Protokoll ist benannt nach Charles Bennett und Gilles Brassard, die das Verfahren 1984 veröffentlicht haben.

Notation:

Zur anschaulicheren Darstellung werden im Folgenden die folgenden Symbole (entsprechend der Darstellung in $\mathbb{R}^2$) für bestimmte Zustände genutzt:

$$— = |0\rangle, \quad | = |1\rangle, \quad ／ = |+\rangle, \quad ＼ = |-\rangle.$$

Die Standard-Basis wird entsprechend der —- und |-Symbole auch kurz +-Basis und die $\{|+\rangle, |-\rangle\}$-Basis entsprechend der ／- und ＼-Symbole ×-Basis genannt.

8.2.1 Ablauf

1. Alice und Bob vereinbaren, wie sie den Zuständen — und | sowie den Zuständen ／ und ＼ einen Bitwert zuordnen, z.B.

	0	1
+-Basis	—	|
×-Basis	／	＼

2. Alice erzeugt eine zufällige Folge von Bits sowie eine zufällige Folge von Basen (+- oder ×-Basis) und codiert die Bits entsprechend der Basis und der Vereinbarung aus 1..

   Sie erhält somit eine Folge von Zuständen —, |, ／ und ＼, die über einen Quantenkanal an Bob übertragen werden.

3. Bob wählt auch eine zufällige Folge von Basen (+- oder ×-Basis), misst die empfangenen Qubits in der gewählten Basis und übersetzt die gemessenen Ergebnisse entsprechend der Vereinbarung in Bits.

   Stimmen bei einem Qubit die von Alice und Bob gewählten Basen überein, so misst Bob den Zustand, den Alice gesendet hat und erhält das gleiche Bit wie Alice. Stimmen die Basen nicht überein, so erhält er zufällig 0 oder 1 jeweils mit der

Wahrscheinlichkeit 1/2, z.B. wenn ein ／ mit einer +-Basis gemessen wird: Bei der Messung erhält Bob — und | jeweils mit der Wahrscheinlichkeit 1/2.

4. Anschließend vergleichen Alice und Bob über einen klassischen (ggf. unsicheren) authentifizierten Kanal ihre Basen und verwerfen alle Bits, bei denen die Basen unterschiedlich waren.

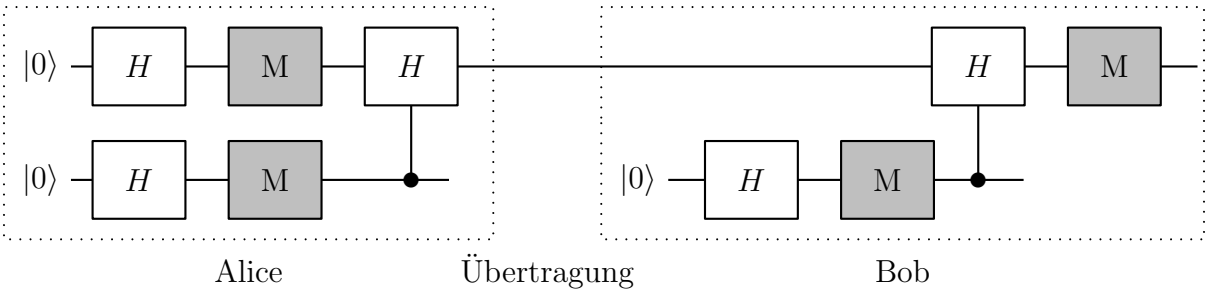
Beispiel:

Alice wählt zufällige Bits	1	0	1	0	1	1	0	1	0	1	0	0
Alice wählt zufällige Basen	×	+	+	×	×	+	×	×	+	+	×	+
Erzeugte Qubits	＼	—	|	／	＼	|	／	＼	—	|	／	—
Übertragung												
Bob wählt zufällige Basen	×	×	+	+	×	+	×	+	×	+	×	×
Gemessene Qubits	＼	＼	|	—	＼	|	／	—	／	|	／	＼
Übersetzt in Bits	1	1	1	0	1	1	0	0	0	1	0	1
Abgleich der Basen	✓	↯	✓	↯	✓	✓	✓	↯	↯	✓	✓	↯

Die ausgegrauten Bits werden verworfen; die gemeinsame Bitfolge ist 1111010.

5. Um Horcher zu entdecken (s. Abschnitt 8.2.2) vergleichen Alice und Bob noch einige der Bits mit gleichen Basen. Gibt es hier Unstimmigkeiten, kann man darauf schließen, dass es einen Horcher in der Leitung gibt.

Realisiert man die Zufalls-Entscheidungen auch quantenmechanisch, so kann man die Schritte 2 und 3 wie folgt als Schaltkreis darstellen:



8.2.2 Horcher

In diesem Abschnitt werden verschiedene Möglichkeiten eines Horchers, üblicherweise Eve genannt, („eavesdropping“=„horchen“) betrachtet.

Messen und Weiterleiten:

Eine Möglichkeit für Eve ist, das Qubit während der Übertragung in einer zufällig gewählten Basis zu messen und das Messergebnis dann an Bob weiterzuleiten.

Die Wahrscheinlichkeit, dass Eve die gleiche Messbasis gewählt hat wie Alice, ist 1/2.

Belauscht Eve auch den klassischen Kanal, über den Alice und Bob anschließend Ihre Basen vergleichen, hat sie in ca. 50% der Bits mit der richtigen Basis das richtige Bit gemessen. Wenn sie dieses an Bob weiterleitet und Bob auch die gleiche Basis gewählt hat, erhält auch Bob das gleiche Ergebnis.

Falls Eves Basis nicht mit der von Alice gewählten Basis übereinstimmt, erhält Eve ein zufälliges Ergebnis, z.B. wenn Alice die +-Basis gewählt, also — oder | gesendet hat, und Eve die ×-Basis gewählt hat. Gehört das Qubit zu einem anschließend von Alice und Bob nicht verworfenen Qubit, so hat Bob die gleiche Basis wie Alice gewählt, d.h., Bobs Basis ist eine andere als die von Eve gewählte. Das Qubit, das Eve sendet, passt also nicht zu Bobs Basis, so dass er ein zufälliges Ergebnis erhält. Mit Wahrscheinlichkeit ½ stimmt das Ergebnis mit dem überein, was Alice gesendet hat, aber mit Wahrscheinlichkeit ½ erhält er den anderen Zustand der Messbasis und interpretiert dies als ein anderes Bit als Alice ursprünglich hatte.

Bei den nicht-verworfenen Bits erhalten Alice und Bob also Unstimmigkeiten beim Vergleich der Bits in Schritt 5 mit der Wahrscheinlichkeit

$$P(\begin{smallmatrix}\text{Eve nutzt}\\ \text{anderen Filter}\end{smallmatrix}) \cdot P(\begin{smallmatrix}\text{Bei Bob wird es nicht}\\ \text{zufällig wieder richtig}\end{smallmatrix}) \;=\; \frac{1}{2}\cdot\frac{1}{2} \;=\; \frac{1}{4},$$

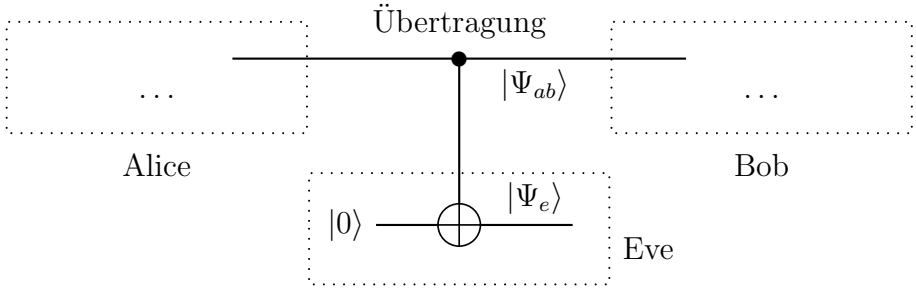
also eine 25%-ige Fehlerrate.

Beispiel:

Alice wählt zufällige Bits	1	0	1	0	1	1	0	1	0	1	0	0
Alice wählt zufällige Basen	×	+	+	×	×	+	×	×	+	+	×	+
Erzeugte Qubits	╲	—	|	╱	╲	|	╱	╲	—	|	╱	—
Übertragung												
Eves gewählte Basen	×	+	×	+	×	×	+	+	×	×	×	+
Gemessene Qubits	╲	—	╱	|	╲	╲	|	—	╲	╱	╱	—
Übertragung												
Bob wählt zufällige Basen	×	×	+	+	×	+	×	+	×	+	×	×
Gemessene Qubits	╲	╱	|	|	╲	—	╲	—	╱	|	╱	╲
Übersetzt in Bits	1	0	1	1	1	0	1	0	0	1	0	1
Abgleich der Basen	✓	↯	✓	↯	✓	✓	✓	↯	↯	✓	✓	↯
Vergleich einiger Bits	✓		✓		✓	↯	↯					

Verschränken:

Eve kann das übertragene Qubit mit einem eigenen Qubit verknüpfen, beispielsweise durch Initialisierung ihres eigenen Qubits mit $|0\rangle$ gefolgt von einem CNOT-Gatter mit dem übertragenen Qubit als Kontroll-Qubit und ihrem eigenen Qubit als Ziel-Qubit.



Belauscht Eve auch den klassischen Kanal, über den Alice und Bob anschließend Ihre Basen vergleichen, kann sie anschließend ihr Qubit in der entsprechenden Basis messen. Dabei gibt es unterschiedliche Fälle:

1. Fall: Alice sendet das Qubit in der +-Basis, also —= $|0\rangle$ oder | = $|1\rangle$.

   Die beiden Qubits $|\Psi_{ab}\rangle$ und $|\Psi_e\rangle$ sind dann in dem (unverschränkten) Zustand

   $$|00\rangle \qquad \text{oder} \qquad |11\rangle\,.$$

   Wird das Bit nach dem Basen-Abgleich nicht verworfen, hat Bob auch in der +-Basis gemessen, und Eve kann durch Messung in der +-Basis das Ergebnis reproduzieren.

2. Fall: Alice sendet das Qubit in der ×-Basis, also ／ = $|+\rangle$ oder ＼ = $|-\rangle$.

   Für den Fall von $|+\rangle = \frac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big)$ sind die beiden Qubits $|\Psi_{ab}\rangle$ und $|\Psi_e\rangle$ dann in dem verschränkten Zustand

   $$\tfrac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big).$$

   Wird das Bit nach dem Basen-Abgleich nicht verworfen, hat Bob auch in der ×-Basis gemessen.

   Entsprechend der Ausführungen in Abschnitt 8.1.2 ist der Zustand $\frac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big)$ in allen Basen perfekt korreliert, und bei einer Messung erhält Bob und damit dann auch Eve beide Basiszustände mit gleicher Wahrscheinlichkeit 1/2.

   In 50% der Fälle erhalten sie also ein anderes Bit als das von Alice gesendete.

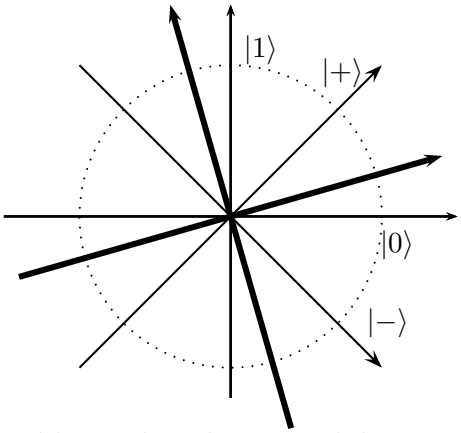
   Der Fall, dass Alice $|-\rangle = \frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big)$ sendet, ist entsprechend.

Beim Vergleich der Bits zwischen Alice und Bob in Schritt 5 erhält man also wieder eine Fehlerrate von 25% (mit Wahrscheinlichkeit 1/2 tritt der zweite Fall auf, in dem Bob mit Wahrscheinlichkeit 1/2 ein anderes Bit erhält, als Alice gesendet hat).

Andere Lauschstrategien:

Andere Messwinkel:

Eve könnte wie bei „Messen und Weiterleiten“ vorgehen, allerdings Ihre Messbasis in einem anderen Winkel als 0° (entspricht der +-Basis) oder 45° (entspricht der ×-Basis) einstellen.



Bei der ursprünglichen Wahl zwischen der +- und der ×-Basis hatte Eve eine 50%-Chance, die gleiche Basis wie Alice zu wählen und auf diese Weise sicher Alice's Bit zu messen; in den anderen 50% (andere Basis) hatte sie keine wirkliche Information über Alice's Bit bekommen, also eine Übereinstimmung mit Alice's Bit mit Wahrscheinlichkeit 1/2. Die Gesamtwahrscheinlichkeit einer Übereinstimmung ist also 3/4.

Bei einer anders gedrehten Messbasis hat Eve in jedem Fall eine Wahrscheinlichkeit größer als 1/2 das richtige Bit zu erhalten, allerdings in keinem Fall eine sichere Möglichkeit. Man kann nachrechnen, dass die Gesamtwahrscheinlichkeit, Alice's Bit zu erhalten, zwischen $\frac{3}{4}$ und $\frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.85$ liegt.

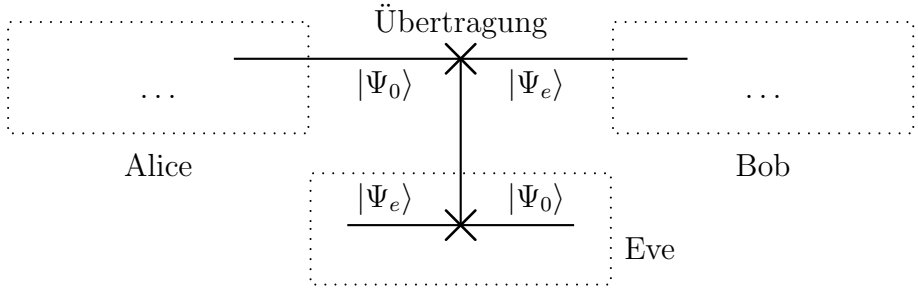
Ferner kann man nachrechnen, dass auch bei einer gedrehten Messbasis von Eve unter den Fällen, bei denen Bob die gleiche Messbasis nutzt wie Alice, die Wahrscheinlichkeit einer Verfälschung bei der Bitübertragung durch Eve gleich 1/4 ist.

Weniger Messungen:

Statt bei „Messen und Weiterleiten“ jedes Bit zu messen, könnte Eve nur einen Teil, z.B. jedes zweite Bit, messen. Dadurch wird die Fehlerrate, die Alice und Bob feststellen, verringert, allerdings verringert sich auch der Informationsgehalt, den Eve bekommt.

Das gesendete Qubit austauschen:

Bei den bisherigen Lauschangriffen gab es – abgesehen davon, dass Alice und Bob den Angriff mit einer gewissen Wahrscheinlichkeit bemerken – auch den Effekt, dass Eve nicht alle Bits von Alice sicher detektieren kann, sondern z.B. nur 75%. Will Eve jedes Bit sicher wissen, so kann Eve ein eigenes Qubit mit einem Swap-Gatter an das übertragene Qubit koppeln und so ihr eigenes Qubit mit dem übertragenen austauschen.



Belauscht Eve auch den klassischen Kanal, über den Alice und Bob anschließend Ihre Basen vergleichen, so kann sie anschließend ihr Qubit in der entsprechenden Basis messen und erhält mit Sicherheit Alice's Bit.

Allerdings bekommt Bob dann ein Bit, das mit Alice's Bit nichts zu tun hat, so dass die Fehlerrate bei einem Bit-Vergleich von Alice und Bob auf 50% steigt.

Allgemeiner Zielkonflikt:

Man kann zeigen, dass der Zielkonflikt von Eve, mölichst viel Information zu gewinnen, aber die Fehlerrate bei dem Bit-Vergleich von Alice und Bob möglichst klein zu halten, nicht gelöst werden kann: Je mehr Information Eve gewinnt, desto stärker wirkt sich das auf das Qubit von Bob aus und umso größer wird die Fehlerrate bei einem Bit-Vergleich von Alice und Bob.

8.3 E91-Protokoll

Das E91-Protokoll ist benannt nach Artur Ekert, der das Verfahren 1991 veröffentlicht hat.

8.3.1 Grobe Idee

Die Idee des E91-Protokolls ist sehr ähnlich der des BB84-Protokolls: Mittels Quantenmessungen in verschiedenen Basen vereinbaren Alice und Bob einen gemeinsamen Schlüssel. Würde die Quantenleitung abgehört, würde sich die Eigenschaft der Quanten ändern, was man bemerken kann.

Der Unterschied ist, dass beim E91-Protokoll verschränkte Quanten zum Einsatz kommen.

Statt dass Alice ein Qubit präpariert und an Bob schickt, erhalten Alice und Bob jeweils ein Qubit eines verschränkten Bell-Paares, z.B. von

$$\tfrac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big).$$

Alice wählt nun eine zufällige Basis, beispielsweise eine +-Basis oder eine ×-Basis und misst ihr Qubit. Damit kollabiert auch Bobs Qubit, und zwar in den gleichen Zustand wie Alice gemessen hat.

Gibt es einen Horcher, der eines der Qubits vorher misst, so wird die Verschränkung zerstört, was Alice und Bob durch Vergleich einiger Bits entdecken können. Auch andere Lauschangriffe können Alice und Bob bemerken, da die perfekte Korrelation gestört wird.

8.3.2 Einige Details

Verwendetes Bell-Paar:

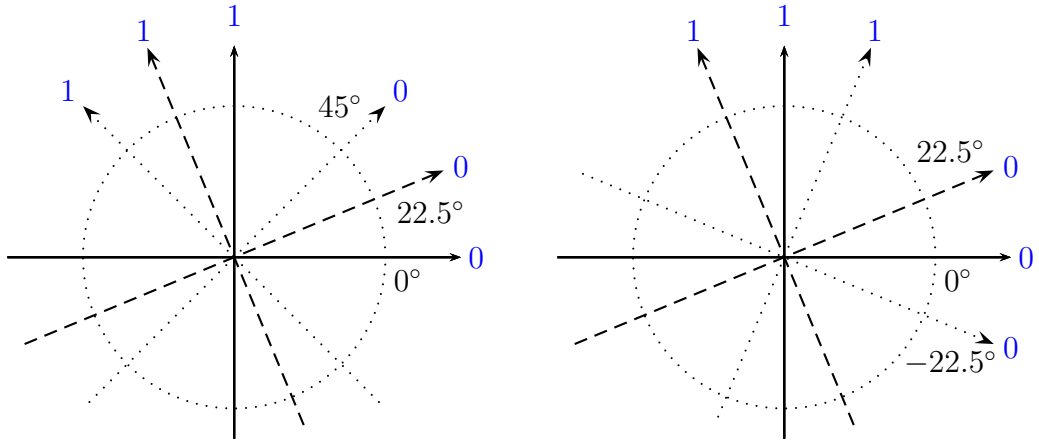
Häufig wird beim E91-Protokoll statt des Bell-Paares $\frac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big)$ das Bell-Paares $\frac{1}{\sqrt{2}}\big(\,|01\rangle - |10\rangle\,\big)$ genutzt, das in allen Basen perfekt antikorreliert ist, vgl. Abschnitt 8.1.2.

Herkunft der verschränkten Qubits:

Wo die verschränkten Qubits herkommen, ist egal. Alice könnte sie erzeugen und an Bob senden oder umgekehrt. Sie könnten auch von einer dritten Stelle erzeugt sein, die dann jeweils eines der Qubits an Alice und an Bob sendet. Dieser Stelle muss nicht vertraut werden, denn falls die erzeugende Stelle irgendwelche Informationen über die erzeugten Qubits bei sich behält, wirkt sie wie ein Horcher, so dass die versendeten Qubits nicht mehr perfekt (anti-)korreliert sind, was Alice und Bob durch entsprechenden Bit-Vergleich feststellen können.

Benutzte Basen:

Statt wie beim BB84-Protokoll nur die $\{|0\rangle, |1\rangle\}$- und $\{|+\rangle, |-\rangle\}$-Basis zu nutzen, kommen beim E91-Protokoll bei Alice und Bob jeweils drei Messbasen zum Einsatz, die jeweils um 22.5° gedreht sind, und von denen zwei bei Alice und Bob übereinstimmen. Dabei werden bei Alice die 0°-, 22.5°- und 45°-Achsen als Ergebnis 0 interpretiert, bei Bob die 0°- und ±22.5°-Achsen. Die entsprechend orthogonalen Achsen werden als 1 interpretiert

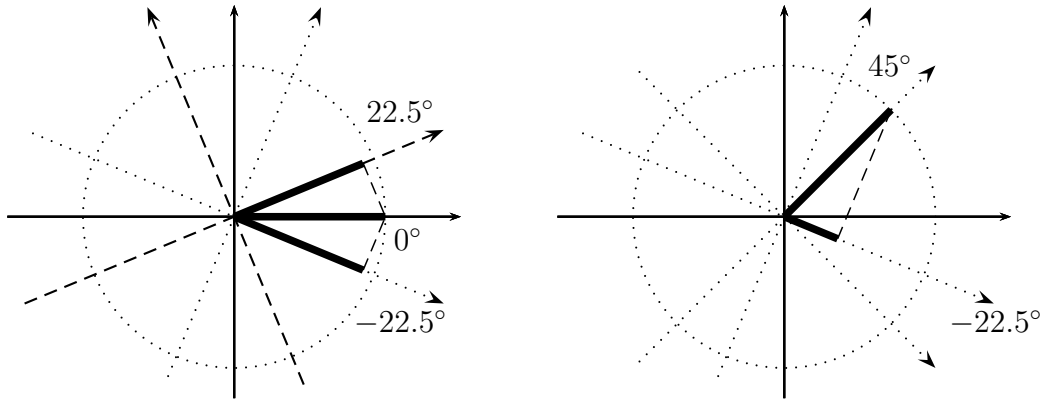


Messbasen und Ergebnisinterpretation (in blau) von Alice (links) und Bob (rechts)

Überprüfung auf Verschränktheit:

Tatsächlich werden beim E91-Protokoll nicht wie beim BB84-Protokoll Bits im Nachhinein verglichen, die mit *gleichen* Messbasen gemessen werden, sondern die mit speziellen *verschiedenen* Basen gemessen wurden, konkret bei Alice die 0°- oder 45°-Basis mit $\pm 22,5°$-Basen bei Bob:

Betrachtet wird im Folgenden der Fall, dass Alice und Bob jeweils ein Qubit eines Bell-Paars $\frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$ teilen. Misst Alice ihr Qubit, so kollabiert wegen der perfekten Korrelation des Bell-Paars in allen Basen das Qubit bei Bob in den gemessenen Zustand. Misst Bob nun mit einer um ±22.5° gegenüber Alice Basis gedrehten Basis, so erhält er mit der Wahrscheinlichkeit $\cos^2(22.5°)$ das gleiche Ergebnis, s. z.B. im Bild links.



Nutzt Alice die 45°-Basis und Bob die −22.5°-Basis (s. im Bild rechts), so erhält man das gleiche Ergebnis nur mit der Wahrscheinlichkeit $\cos^2(67.5°) = \sin^2(22.5°)$.

Bewerten Alice und Bob nun gleiche Ergebnisse mit +1 und ungleiche Ergebnisse mit −1, so kann man die Erwartungswerte dazu bei den verschiedenen Winkelkombinationen ermitteln:

		Bob	
		22.5°	−22.5°
Alice	0°	$\cos^2(22.5°) - \sin^2(22.5°)$	$\cos^2(22.5°) - \sin^2(22.5°)$
	45°	$\cos^2(22.5°) - \sin^2(22.5°)$	$\sin^2(22.5°) - \cos^2(22.5°)$

Wegen

$$\cos^2(22.5°) - \sin^2(22.5°) \;=\; \cos(2 \cdot 22.5°) \;=\; \cos(45°) \;=\; \tfrac{1}{\sqrt{2}}$$

sind die Einträge in der Tabelle gleich $\pm\frac{1}{\sqrt{2}}$:

		Bob	
		22.5°	−22.5°
Alice	0°	$\frac{1}{\sqrt{2}}$	$\frac{1}{\sqrt{2}}$
	45°	$\frac{1}{\sqrt{2}}$	$-\frac{1}{\sqrt{2}}$

Man betrachtet nun die Addition der ersten drei Erwartungswerte abzüglich des letzten:

$$\begin{aligned} S \;&:=\; \mathrm{E}(\text{A=0° und B=22.5°}) + \mathrm{E}(\text{A=0° und B=}-22.5°) \\ &\quad + \mathrm{E}(\text{A=45° und B=22.5°}) - \mathrm{E}(\text{A=45° und B=}-22.5°) \\ &=\; 3 \cdot \tfrac{1}{\sqrt{2}} - \big(-\tfrac{1}{\sqrt{2}}\big) \;=\; 4 \cdot \tfrac{1}{\sqrt{2}} \;=\; 2\sqrt{2} \;\approx\; 2.82. \end{aligned}$$

Für den Fall, dass die Qubits nicht verschränkt sind, besagt die sog. *Bell-Ungleichung* oder *CHSH-Ungleichung* (benannt nach John Clauser, Michael Horne, Abner Shimony und Richard Holt), dass eine entsprechende Kombination von Erwartungswerten betragsmäßig stets kleiner oder gleich 2 ist.

Indem Alice und Bob ihre Messergebnisse für die genannten Winkel-Kombinationen vergleichen und damit die beschriebenen Werte berechnen, können Sie testen, ob die CHSH-Ungleichung verletzt ist, und sich somit davon überzeugen dass ihre Qubits verschränkt sind.

8.4 Reale Umsetzung

8.4.1 Nachbearbeitung

Schwellwert für Fehlerrate:

Theoretisch kann man beim BB84-Protokoll bei Auftreten eines einzigen Fehlers von der Existenz eines Horchers ausgehen.

In der Praxis gibt es aber auch ohne Horcher eine gewisse Fehlerrate. Man nutzt daher üblicherweise einen gewissen Schwellwert, so dass man erst oberhalb davon einen Horcher annimmt. Ist die Fehlerrate unterhalb des Schwellwerts, kann man aber nicht ausschließen, ob vielleicht doch ein Horcher in der Leitung ist. Daher nutzt man zusätzlich *privacy Amplification*, s. unten.

Ähnlich ist die Situation beim E91-Protokoll.

Fehlerkorrektur:

In realen Systemen kommt es auch ohne Horcher zu Fehlern bei der Übertragung. Dies erfordert, dass man eine Fehlerkorrektur durchführt, um sicherzustellen, dass Alice und Bob am Ende tatsächlich den gleichen Schlüssel haben.

Ein Problem hier ist, dass viele (klassische) Verfahren der Fehlerkorrektur so vorgehen, dass der zu übertragenden Nachricht Prüfbits angehängt werden, die es erlauben, dass – wenn bei der Übertragung nicht zu viele Fehler entstehen – aufgetretene Fehler erkannt und korrigiert werden können. Dies ist hier nicht möglich, da erst nach Ende des Protokolls fest steht, welche Bits Alice und Bob gemeinsam haben (sollten).

Es gibt aber Verfahren, mit denen eine entsprechende Fehlerkorrektur möglich ist.

Beispiel:

Geht man davon aus, dass bei k Bits die Wahrscheinlichkeit von mehr als einem Fehler vernachlässigbar klein ist, können Alice und Bob die ausgetauschte Bitfolge in k-Bit-Blöcke zerteilen und jeweils die Parität (also die XOR-Verknüpfung über alle Bits des Blocks) über einen öffentlichen Kanal miteinander vergleichen und nur die Blöcke nutzen, bei denen die Parität übereinstimmt.

Oft geben Fehlerkorrekturverfahren durch einen Austausch über einen öffentlichen Kanal Informationen über die eigentlich geheimen Bits preis. Daher nutzt man zusätzlich *privacy Amplification*, s. unten.

Privacy Amplification:

Bei der *privacy Amplification* macht man aus einem teilweise geheimen Schlüssel einen geheimeren kürzeren Schlüssel.

Beispiel:

Alice und Bob gehen davon aus, dass Eve eines der beiden Bits b_1 und b_2 kennt, das andere aber nicht. Durch die XOR-Verknüpfung

$$b \;=\; b_1 \oplus b_2$$

entsteht ein Bit b, über das Eve keinerlei Kenntnis hat.

8.4.2 Angriffe

Einzelne Quanten:

Eine übliche Realisierung des BB84- oder E91-Protokolls geschieht mittels polarisierter Photonen. Allerdings ist es technisch schwierig, tatsächlich einzelne Photonen zu erzeugen. Werden allerdings z.B. beim BB84-Protokoll statt jeweils einem einzelnen polarisierten Photon mehrere Photonen in einem Slot gesendet, kann Eve einige davon abfangen und damit arbeiten, ohne dass Bob das bemerkt.

Man-in-the-middle-Angriff:

Sowohl beim BB84- als auch beim E91-Protokoll werden nach der Quantenmessung Daten über einen klassischen Kanal verglichen. Dieser Kanal muss nicht abhörsicher sein, aber er muss authentifiziert sein, d.h. Alice und Bob müssen sicher sein, mit der jeweils anderen Person zu kommunizieren. Ansonsten könnte sich Eve in die Quanten- und klassische Leitung einklinken und jeweils mit Alice und mit Bob einen eigenen Schlüssel vereinbaren.

8.4.3 Geschichtliches

1991: erster erfolgreicher Austausch eines Quantenschlüssels (32cm, BB84),

1999: Anton Zeilinger, Wien: Schlüsselaustausch mit verschränkten Photonen über 360m,

2002: Übertragung über 23.4km Luftlinie zwischen Berggipfeln (BB84),

2004: erste Geldüberweisung mit verschränkten Photonen über 1.5km Glasfaser,

2006: erfolgreiches Abhören eines Quantenkanals,

2016: Übertragung über 100km (Kilobit/s)

2017: Pan Jian Wei und Zeilinger: Übertragung verschränkter Photonen 1400km zwischen der Erde und einem Satelliten und über 2000 km Glasfaser.

immer wieder Verbesserungen der Verfahren, aber auch Ausnutzen von Schwächen in der praktischen Realisierung.

9 Fehler-Korrektur

In realen Systemen muss man mit Fehlern bedingt durch Umwelteinflüsse rechnen. Wie pflanzen sich Fehler fort? Wie können Verfahren zur Fehlerkorrektur aussehen?

9.1 Fehlerfortpflanzung

Störung eines Bits:

Klassische Bits sind recht robust gegenüber Störungen, da sie immer wieder auf 0 bzw. 1 gerundet werden können. Qubits haben hingegen einen kontinuierlichen Zustandsraum, so dass man nicht runden kann, um Störungen zu eliminieren.

Kann sich eine kleine Störung im Laufe weiterer Rechnungen zu einer großen Störung fortpflanzen?

Sei $|\Psi\rangle$ ein Zustand, der durch eine Störung zu $|\Psi'\rangle$ modifiziert wird. Die Störung kann man dann betragsmäßig vektoriell berechnen als

$$\varepsilon \;=\; \| \, |\Psi'\rangle - |\Psi\rangle \, \|.$$

Weitere Rechenschritte werden durch unitäre Transformationen beschrieben, die man auch zu einer unitären Transformation U zusammenfassen kann.

Unitäre Transformationen erhalten die Längen (s. S. 9). Daher gilt für die Störung nach den Transformationen wegen der Linearität von U:

$$\|U(|\Psi'\rangle) - U(|\Psi\rangle)\| \;=\; \|U(|\Psi'\rangle - |\Psi\rangle)\| \;=\; \| \, |\Psi'\rangle - |\Psi\rangle \, \| \;=\; \varepsilon.$$

Störungen werden also nicht verstärkt.

Gestörte Transformationen:

Wie kumulieren sich Störungen durch gestörte Transformationen?

Klassisch können sich Störungen exponentiell verstärken.

Beispiel:

Statt der identischen Abbildung $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x$ hat man die gestörte Abbildung $\tilde{f} : \mathbb{R} \to \mathbb{R}$, $\tilde{f}(x) = 1.1 \cdot x$.

Eine zehnfache Anwendung der Funktion f ist weiter die identische Abbildung.

Eine zehnfache Anwendung der Funktion $\tilde{f}$ bildet x auf $1.1^{10} \cdot x \approx 2.6 \cdot x$ ab.

Betrachtet werden zwei unitäre Transformationen U_1 und U_2, die nacheinander auf einen Zustand $|\Psi\rangle$ angewendet werden. Dies wird verglichen mit der Anwendung gestörter Transformationen U_1' und U_2'. Die maximale Störung sei dabei ε_1 bzw. ε_2,

also für $i = 1, 2$,

$$\varepsilon_i \;=\; \max_{|\Psi\rangle}\{\|U_i'(|\Psi\rangle) - U_i(|\Psi\rangle)\|\} \;=\; \max_{|\Psi\rangle}\{\|(U_i' - U_i)(|\Psi\rangle)\|\}.$$

Für die Abweichung bei der Hintereinander-Ausführung, also bei $U_2 \circ U_1$ bzw. $U_2' \circ U_1'$, erhält man durch geeignetes Abziehen und wieder Addieren, dann mit der Dreiecksungleichung für die Norm und dann wegen der Längenerhaltung von U_2'

$$\begin{aligned}
&\|U_2' \circ U_1'(|\Psi\rangle) - U_2 \circ U_1(|\Psi\rangle)\| \\
=\; &\|U_2' \circ U_1'(|\Psi\rangle) - U_2' \circ U_1(|\Psi\rangle) + U_2' \circ U_1(|\Psi\rangle) - U_2 \circ U_1(|\Psi\rangle)\| \\
=\; &\|U_2'\big(U_1'(|\Psi\rangle) - U_1(|\Psi\rangle)\big) + (U_2' - U_2)\big(U_1(|\Psi\rangle)\big)\| \\
\leq\; &\|U_2'\big(U_1'(|\Psi\rangle) - U_1(|\Psi\rangle)\big)\| + \|(U_2' - U_2)\big(U_1(|\Psi\rangle)\big)\| \\
=\; &\|U_1'(|\Psi\rangle) - U_1(|\Psi\rangle\,\| + \|(U_2' - U_2)\big(U_1(|\Psi\rangle)\big)\| \\
\leq\; &\qquad\quad \varepsilon_1 \qquad\quad + \qquad\quad \varepsilon_2.
\end{aligned}$$

Man sieht: Die Gesamtstörung ist beschränkt durch die Summe der einzelnen Störungen.

9.2 Bitflip-Korrektur

Um Bits bei Übertragungen gegen Verfälschung zu schützen werden klassisch fehlerkorrigierende Codes genutzt.

Beispiel zur klassischen Fehlerkorrektur:

Bei klassischen Bits kann man einen 3fach-Wiederholungscode nutzen, der jedes Nachrichten-Bit verdreifacht. Aus 00101 wird so beispielsweise

000 000 111 000 111.

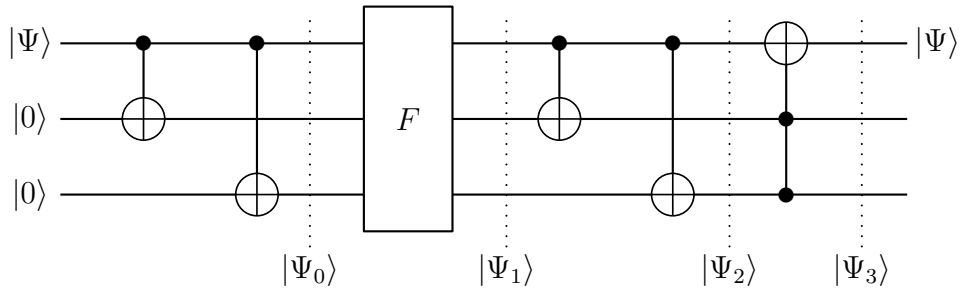
Kommt es innerhalb einer Dreier-Gruppe zu maximal einem Bitfehler, kann man durch Mehrheitsentscheid auf das richtige Nachrichtenbit schließen.

Derartige Verfahren kann man nicht unmittelbar auf Qubits anwenden, z.B., da Qubits nicht kopierbar sind. Es gibt aber andere Verfahren.

Beispielhaft wird hier eine mögliche Korrektur für den Fall eines Bitflips betrachtet, also für den Fall, dass ein Qubit $\alpha \cdot |0\rangle + \beta \cdot |1\rangle$ in den Zustand $\alpha \cdot |1\rangle + \beta \cdot |0\rangle$ übergeht. Dies entspricht der Anwendung eine Pauli-X-Gatters.

Mit zwei Hilfs-Qubits kann man das Auftreten *eines* Bitflips korrigieren:

In dem folgenden Schaltkreis bezeichnet F, dass maximal ein Bitflip auf einem der beteiligten Qubits geschieht; es könnte auch sein, dass kein Fehler passiert.



Behauptet wird, dass am Ende das oberste Bit in jedem Fall wieder den ursprünglichen Wert hat und mit den Hilfs-Qubits nicht verschränkt ist.

Dies kann man verifizieren, indem man alle möglichen Fälle betrachtet. Sei dazu

$$|\Psi\rangle \;=\; \alpha \cdot |0\rangle + \beta \cdot |1\rangle\,.$$

Dann ist

$$|\Psi_0\rangle \;=\; \alpha \cdot |000\rangle + \beta \cdot |111\rangle\,.$$

1. Fall: Es passiert kein Fehler. Dann ist

   $$|\Psi_1\rangle \;=\; |\Psi_0\rangle \;=\; \alpha \cdot |000\rangle + \beta \cdot |111\rangle$$

   und damit

   $$|\Psi_2\rangle \;=\; \alpha \cdot |000\rangle + \beta \cdot |100\rangle \;=\; \big(\alpha \cdot |0\rangle + \beta \cdot |1\rangle\big) \otimes |00\rangle \;=\; |\Psi\rangle \otimes |00\rangle\,.$$

   Die Anwendung des Toffoli-Gatters hat dann keine Auswirkung, und es ist

   $$|\Psi_3\rangle \;=\; |\Psi_2\rangle \;=\; |\Psi\rangle \otimes |00\rangle\,.$$

2. Fall: Es passiert ein Bitflip auf dem obersten Qubit. Dann ist

   $$|\Psi_1\rangle \;=\; \alpha \cdot |100\rangle + \beta \cdot |011\rangle$$

   und damit

   $$|\Psi_2\rangle \;=\; \alpha \cdot |111\rangle + \beta \cdot |011\rangle \;=\; \big(\alpha \cdot |1\rangle + \beta \cdot |0\rangle\big) \otimes |11\rangle\,.$$

   Die Anwendung des Toffoli-Gatters flipt dann das oberste Bit, und es ist

   $$|\Psi_3\rangle \;=\; \big(\alpha \cdot |0\rangle + \beta \cdot |1\rangle\big) \otimes |11\rangle \;=\; |\Psi\rangle \otimes |11\rangle\,.$$

3. Fall: Es passiert ein Bitflip auf dem mittleren Qubit. Dann ist

   $$|\Psi_1\rangle \;=\; \alpha \cdot |010\rangle + \beta \cdot |101\rangle$$

   und damit

   $$|\Psi_2\rangle \;=\; \alpha \cdot |010\rangle + \beta \cdot |110\rangle \;=\; \big(\alpha \cdot |0\rangle + \beta \cdot |1\rangle\big) \otimes |10\rangle \;=\; |\Psi\rangle \otimes |10\rangle\,.$$

   Die Anwendung des Toffoli-Gatters hat dann keine Auswirkung, und es ist

   $$|\Psi_3\rangle \;=\; |\Psi_2\rangle \;=\; |\Psi\rangle \otimes |10\rangle\,.$$

4. Fall: Es passiert ein Bitflip auf dem untersten Qubit. Dies ist ähnlich zum 3. Fall.

Phasenflip:

Man kann in ähnlicher Weise mit zwei Hilfs-Qubits einen Phasenflit korrigieren, d.h. die fehlerhafte Anwendung eines Pauli-Z-Gatters, das $\alpha \cdot |0\rangle + \beta \cdot |1\rangle$ auf $\alpha \cdot |0\rangle - \beta \cdot |1\rangle$ abbildet.

Ausblick:

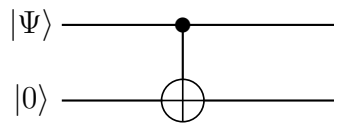
Die Bitflip- und Phasenflip-Korrektur kombiniert *Shors 9-Qubit-Code*, bei dem mit 8 Hilfs-Qubits eine Korrektur eines Bit- und/oder Phasenflips durchgeführt werden kann.

Es gibt weitere korrigierende Codes, die Störungen reduzieren können.

9.3 Verschränkung

9.3.1 Maximale Verschränkung

Mit einem CNOT-Gatter kann man Qubits verschränken.



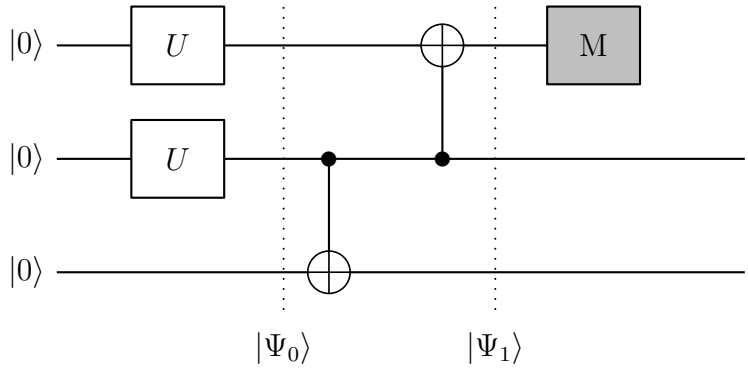
Ist beispielsweis $|\Psi\rangle = |+\rangle = H(|0\rangle)$, so erhält man am Ausgang das maximal verschränkte Qubit-Paar $\frac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big)$.

Hat man eine Transformation U, die angewendet auf $|0\rangle$ keine gleichmäßige Überlagerung von $|0\rangle$ und $|1\rangle$ erzeugt, sondern einen Zustand $U(|0\rangle) = \alpha\,|0\rangle + \beta\,|1\rangle$ mit $|\alpha| \neq |\beta|$, so ist der Zustand

$$\alpha\,|00\rangle + \beta\,|11\rangle$$

am Ausgang nicht maximal verschränkt.

Mit dem folgenden Schaltkreis kann man mit U aber einen maximal verschränkten Zustand produzieren:



Analyse:

Wegen $U(|0\rangle) = \alpha\,|0\rangle + \beta\,|1\rangle$ ist der gemeinsame Zustand nach Anwendung der U-Gatter

$$\begin{aligned} |\Psi_0\rangle &= \big(\alpha\,|0\rangle + \beta\,|1\rangle\big) \otimes \big(\alpha\,|0\rangle + \beta\,|1\rangle\big) \otimes |0\rangle \\ &= \alpha^2\,|000\rangle + \alpha\beta\,|010\rangle + \beta\alpha\,|100\rangle + \beta^2\,|110\rangle\,. \end{aligned}$$

Durch die CNOT-Gatter mit dem mittleren Qubit als Kontroll-Bit wird dies zu

$$|\Psi_1\rangle = \alpha^2\,|000\rangle + \alpha\beta\,|111\rangle + \beta\alpha\,|100\rangle + \beta^2\,|011\rangle\,.$$

Die Messung des ersten Qubits kann nun $|0\rangle$ oder $|1\rangle$ liefern:

Mit der Wahrscheinlichkeit $\alpha^4+\beta^4$ wird $|0\rangle$ gemessen. Die beiden unteren Zustände kollabieren dann bis auf einen Normierungsfaktor zu der Überlagerung $\alpha^2\,|00\rangle + \beta^2\,|11\rangle$, die noch weniger verschränkt ist als vorher.

Mit der Wahrscheinlichkeit $2\alpha^2\beta^2$ wird $|1\rangle$ gemessen. Dabei sind $|111\rangle$ und $|100\rangle$ gleich wahrscheinlich, so dass die unteren beiden Qubits in den maximal verschränkten Zustand

$$\tfrac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big)$$

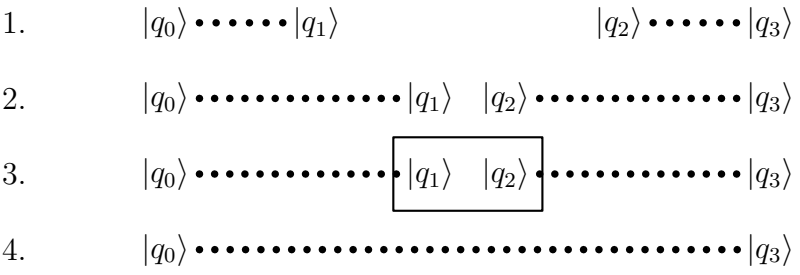
kollabieren.

9.3.2 Verschränkungs-Weitergabe (Entanglement Swapping)

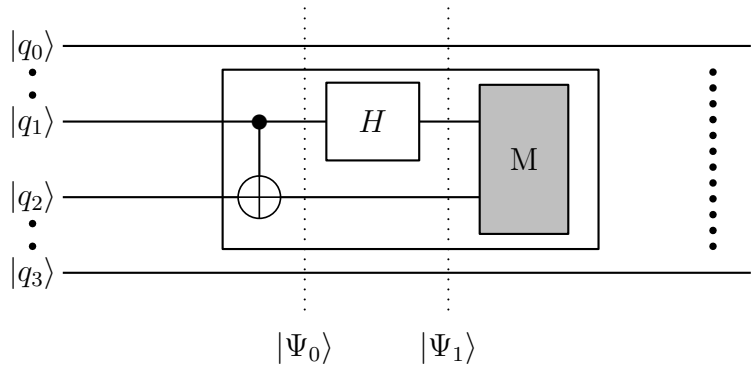
Bei der Übertragung klassischer Bits über lange Strecken kann man das Signal in regelmäßigen Abständen verstärken; bei Qubits ist das nicht möglich. Allerdings gibt es eine Möglichkeit, zwei Qubits miteinander zu verschränken, ohne dass sie sich räumlich treffen:

1. Man nutzt zwei verschränke Qubit-Paare.
2. Jeweils eines davon führt man zusammen.
3. Man führt den Schaltkreis unten mit anschließender Messung dadurch.
4. Anschließend sind die anderen beiden Qubits miteinander verschränkt.

Schematisch ist das also wie folgt, wobei eine Verschränkung durch eine gepunktete Linie dargestellt ist.



Der Schaltkreis ist der folgende



Analyse:

Betrachtet wird beispielhaft

$$|q_0q_1\rangle \;=\; \tfrac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big) \qquad \text{und} \qquad |q_2q_3\rangle \;=\; \tfrac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big).$$

Damit ist der Gesamtzustand

$$\begin{aligned} |\Psi\rangle \;&=\; |q_0q_1\rangle \otimes |q_2q_3\rangle \;=\; \tfrac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big) \otimes \tfrac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big) \\ &=\; \tfrac{1}{2}\big(\,|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle\,\big). \end{aligned}$$

Nach dem CNOT-Gatter wird dies zu

$$|\Psi_0\rangle \;=\; \tfrac{1}{2}\big(\,|0000\rangle + |0011\rangle + |1110\rangle + |1101\rangle\,\big).$$

Durch das Hadamard-Gatter wird dies zu

$$\begin{aligned} |\Psi_1\rangle \;&=\; \tfrac{1}{2}\Big(\,|0\rangle \otimes \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |00\rangle \quad + \quad |0\rangle \otimes \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |11\rangle \\ &\qquad + \quad |1\rangle \otimes \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |10\rangle \quad + \quad |1\rangle \otimes \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |01\rangle\,\Big) \\ &=\; \tfrac{1}{2\sqrt{2}}\big(\,|0000\rangle + |0100\rangle \quad + \quad |0011\rangle + |0111\rangle \\ &\qquad + \quad |1010\rangle - |1110\rangle \quad + \quad |1001\rangle - |1101\rangle\,\big). \end{aligned}$$

Bei der Messung von $|q_1q_2\rangle$ kommen alle Fälle $|00\rangle$, $|01\rangle$, $|10\rangle$ und $|11\rangle$ gleich wahrscheinlich vor. Für $|q_0q_3\rangle$ ergibt sich jeweils

falls $|00\rangle$ gemessen wird: $|q_0q_3\rangle = \tfrac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big)$,

falls $|01\rangle$ gemessen wird: $|q_0q_3\rangle = \tfrac{1}{\sqrt{2}}\big(\,|01\rangle + |10\rangle\,\big)$,

falls $|10\rangle$ gemessen wird: $|q_0q_3\rangle = \tfrac{1}{\sqrt{2}}\big(\,|00\rangle - |11\rangle\,\big)$,

falls $|11\rangle$ gemessen wird: $|q_0q_3\rangle = \tfrac{1}{\sqrt{2}}\big(\,|01\rangle - |10\rangle\,\big)$.

Man erhält also wieder verschränkte Zustände. Will man für $|q_0q_3\rangle$ den ursprünglichen Bell-Zustand $\tfrac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big)$ erreichen, kann man dies mit einer Nachbearbeitung abhängig vom Messergebnis – wie bei der Teleportation – erreichen.

Bemerkung:

Hier gibt es – anders als bei der Teleportation – keine einheitliche Nachbearbeitung:

Sind $|q_0q_1\rangle$ und $|q_2q_3\rangle$ in gleichen Bell-Zuständen, die nicht dem obigen entspricht, so braucht es andere Nachbearbeitungen.

Sind $|q_0q_1\rangle$ und $|q_2q_3\rangle$ in unterschiedlichen Bell-Zuständen, so ist das Ergebnis weiterhin verschränkt, aber eine Angleichung an die Eingangs-Verschränkung macht keinen Sinn.

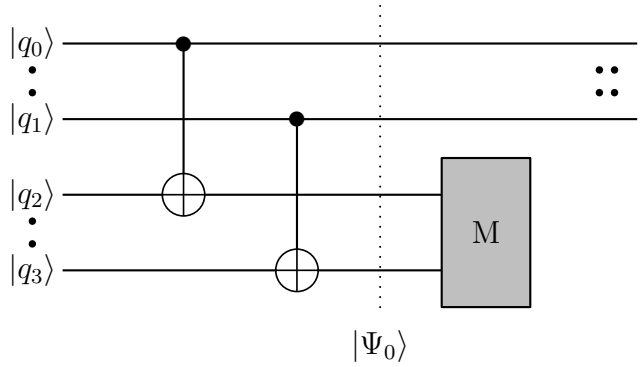
9.3.3 Verschränkungs-Verstärkung (Entanglement Distillation)

Um eine Verschränkung z.B. über größere Distanzen zu gewährleisten, kann man auch mehrer verschränkte Qubits transportieren. Lässt die Verschränkung nach, kann man sie durch Verknüpfung der teilweise verschränkten Qubits verstärken.

Konkret werden zwei in der folgenden Weise verschränkte Qubit-Paare betrachtet:

$$|q_0q_1\rangle \;=\; \alpha\,|00\rangle + \beta\,|11\rangle \qquad \text{und} \qquad |q_2q_3\rangle \;=\; \gamma\,|00\rangle + \delta\,|11\rangle\,.$$

Nun wird der folgende Schaltkreis ausgeführt:



Analyse:

Zu Beginn sind die vier Qubits im Zustand

$$\begin{aligned}|\Psi\rangle \;&=\; \big(\alpha\,|00\rangle + \beta\,|11\rangle\,\big) \otimes \big(\gamma\,|00\rangle + \delta\,|11\rangle\,\big)\\ &=\; \alpha\gamma\,|0000\rangle + \alpha\delta\,|0011\rangle + \beta\gamma\,|1100\rangle + \beta\delta\,|1111\rangle\,.\end{aligned}$$

Nach den CNOT-Gattern erhält man den Zustand

$$\begin{aligned}|\Psi_0\rangle \;&=\; \alpha\gamma\,|0000\rangle + \alpha\delta\,|0011\rangle + \beta\gamma\,|1111\rangle + \beta\delta\,|1100\rangle\\ &=\; \big(\alpha\gamma\,|00\rangle + \beta\delta\,|11\rangle\,\big) \otimes |00\rangle \;+\; \big(\alpha\delta\,|00\rangle + \beta\gamma\,|11\rangle\,\big) \otimes |11\rangle\,.\end{aligned}$$

Die Messung der unteren beiden Qubit liefert also $|00\rangle$ oder $|11\rangle$. In beiden Fällen erhält man verschränkte Zustände in den oberen beiden Qubits, falls $\alpha, \beta, \gamma, \delta \neq 0$:

Bei einem Messergebnis $|00\rangle$:

$$|q_0 q_1\rangle \;=\; \frac{1}{\sqrt{(\alpha\gamma)^2 + (\beta\delta)^2}}\big(\alpha\gamma\,|00\rangle + \beta\delta\,|11\rangle\,\big),$$

bei einem Messergebnis $|11\rangle$:

$$|q_0 q_1\rangle \;=\; \frac{1}{\sqrt{(\alpha\delta)^2 + (\beta\gamma)^2}}\big(\alpha\delta\,|00\rangle + \beta\gamma\,|11\rangle\,\big).$$

Bei $\alpha = \gamma$ und $\beta = \delta$ ist der Zustand beim Messergebnis $|11\rangle$

$$|q_0 q_1\rangle \;=\; \frac{1}{\sqrt{(\alpha\beta)^2 + (\beta\alpha)^2}}\big(\alpha\beta\,|00\rangle + \beta\alpha\,|11\rangle\,\big) \;=\; \frac{\alpha\beta}{\sqrt{2}|\alpha\beta|}\big(\,|00\rangle + |11\rangle\,\big),$$

also sogar maximal verschränkt. Der Zustand beim Messergebnis $|00\rangle$ ist dann allerdings weniger verschränkt.

Bemerkung:

Es kann auch passieren, dass man keinen Verschränkungsgewinn erhält, z.B., wenn ein Qubit-Paar schon stark verschränkt, das andere aber fast gar nicht verschränkt war.

10 Shor-Algorithmus und Quanten-Fourier-Transformation

Der vielleicht bekannteste Quanten-Algorithmus ist der Shor-Algorithmus zur Faktorisierung, den Peter Shor 1994 veröffentlicht hat.

Die Faktorisierung großer natürlicher Zahlen ist ein auf klassischen Rechnern (vermutlich) schwieriges Probelm, auf dem eine Vielzahl kryptografischer Anwendungen (RSA-Verfahren) basiert. Diese Verfahren werden unsicher, wenn es Quantencomputer gibt, die Shor's Algorithmus realisieren können.

In diesem Kapitel werden die Grundzüge des Shor-Algorithmus und dessen Kernelement, die Quanten-Fourier-Transformation beschrieben, ohne auf Details einzugehen.

10.1 Klassischer Teil des Shor-Algorithmus

Fragestellung:

Gegeben ist eine Zahl $m \in \mathbb{N}$, von der man weiß, dass sie das Produkt zweier großer verschiedener Primzahlen p und q ist, also $m = p \cdot q$.

Gesucht sind p und q. Natürlich reicht es, eine der beiden Zahlen zu bestimmen, denn die andere ergibt sich dann mittels Division von m durch diese Zahl.

Man kann die Fragestellung auch verallgemeinern, dass man zu einer nicht-Primzahl m einen echten Teiler sucht.

Modulo:

Zu $a, m \in \mathbb{N}$ bezeichnet $a \bmod m$ den Rest bei der Division von a durch m.

Beispiel:

$32 \bmod 6 = 2$, da $32 : 6 = 5$, Rest 2.

Die Modulo-Rechnung ist verträglich mit „+“ und „·“, d.h.

$$\begin{aligned} (a+b) \bmod m &= ((a \bmod m) + (b \bmod m)) \bmod m \qquad \text{und} \\ (a \cdot b) \bmod m &= ((a \bmod m) \cdot (b \bmod m)) \bmod m. \end{aligned}$$

Beispiel:

Es ist $17 + 15 = 32$. Einerseits ist $32 \bmod 6 = 2$, andererseits ist

$$\begin{aligned} (17+15) \bmod 6 &= ((17 \bmod 6) + (15 \bmod 6)) \bmod 6 \\ &= (5+3) \bmod 6 \\ &= 8 \bmod 6 = 2. \end{aligned}$$

Es ist $9 \cdot 7 = 63$. Einerseits ist $63 \bmod 6 = 3$, andererseits ist

$$\begin{aligned}(9 \cdot 7) \bmod 6 &= ((9 \bmod 6) \cdot (7 \bmod 6)) \bmod 6 \\ &= (3 \cdot 1) \bmod 6 = 3.\end{aligned}$$

Ordnung:

Sei $a \in \mathbb{N}$ mit $\text{ggt}(a, m) = 1$. Man kann zeigen, dass es dann ein $x_0 \in \mathbb{N}$ mit $a^{x_0} \bmod m = 1$ gibt.

Definition:

Sei $a \in \mathbb{N}$ mit $\text{ggt}(a, m) = 1$. Das kleinste $r \in \mathbb{N}$ mit $a^r \bmod m = 1$ heißt *Ordnung* von a modulo m.

Die Funktion

$$\mathbb{N} \to \mathbb{N},\ x \mapsto a^x \bmod m$$

ist dann r-periodisch.

Beispiel:

Zu $m = 35$ und $a = 4$ sind die Funktionswerte zu $f(x) = a^x \bmod m$, also $f(x) = 4^x \bmod 35$

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	...
4^x	4	16	29	11	9	1	4	16	29	11	9	1	4	16	...

Die Ordnung von 4 modulo 35 ist 6.

Zu $m = 35$ und $a = 3$ sind die Funktionswerte zu $f(x) = a^x \bmod m$, also $f(x) = 3^x \bmod 35$

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	...
3^x	3	9	27	11	33	29	17	16	13	4	12	1	3	9	...

Die Ordnung von 3 modulo 35 ist 12.

Faktorisierung mittels Ordnungsbestimmung:

Sei $a \in \mathbb{N}$ mit $\text{ggt}(a, m) = 1$ und r die Ordnung von m.

Falls r gerade ist, ist $\frac{r}{2} \in \mathbb{N}$. Es gilt dann, wenn man alles modulo m rechnet, entsprechend der dritten binomischen Formel:

$$0 = a^r - 1 = \left(a^{\frac{r}{2}}\right)^2 - 1 = (a^{\frac{r}{2}} - 1) \cdot (a^{\frac{r}{2}} + 1).$$

Also ist $(a^{\frac{r}{2}} - 1) \cdot (a^{\frac{r}{2}} + 1)$ ein Vielfaches von m, d.h., die Primfaktoren von m sind in den beiden Faktoren $(a^{\frac{r}{2}} - 1)$ und $(a^{\frac{r}{2}} + 1)$ enthalten.

Es kann nicht sein, dass alle Primfaktoren in $(a^{\frac{r}{2}} - 1)$ enthalten sind, denn dann wäre

$$(a^{\frac{r}{2}} - 1) \bmod m = 0 \quad \Leftrightarrow \quad a^{\frac{r}{2}} \bmod m = 1$$

im Widerspruch zur Eigenschaft der Ordnung r, das kleinste $x \in \mathbb{N}$ mit $a^x \bmod m = 1$ zu sein.

Falls nicht alle Primfaktoren von m in $(a^{\frac{r}{2}} + 1)$ enthalten sind, verteilen sich die Primfaktoren von m auf $(a^{\frac{r}{2}} - 1)$ und $(a^{\frac{r}{2}} + 1)$. Durch die Berechnung von $\text{ggt}(a^{\frac{r}{2}} - 1, m)$ erhält man so einen echten Teiler von m.

Beispiel:

Die Ordnung von 3 modulo 35 ist 12, also (alles modulo 35)

$$0 \;=\; 3^{12} - 1 \;=\; (3^6)^2 - 1 \;=\; (3^6 - 1) \cdot (3^6 + 1).$$

Es ist $3^6 - 1 \bmod 35 = 28$ und $3^6 + 1 \bmod 35 = 30$. Mit $\text{ggt}(28, 35) = 7$ erhält man einen echten Teiler von 35.

Bemerkung:

Bei großen Zahlen a und r ist $a^{\frac{r}{2}}$ so groß, dass die Zahl nicht mehr praktisch handhabbar ist; man kann alle auftretenden Werte aber immer modulo m betrachten, also z.B. $a^{\frac{r}{2}} - 1 \bmod m$ statt $a^{\frac{r}{2}} - 1$.

Auch für große Zahlen a, x und m ist $a^x \bmod m$ klassisch mit polynomiellem Aufwand berechenbar, z.B. mittels der *square-and-multiply*-Methode.

Auch für große Zahlen a und b ist $\text{ggt}(a, b)$ klassisch mit polynomiellem Aufwand berechenbar, z.B. mittels des *Euklidischen Algorithmus*.

Man kann zeigen, dass bei einem zufällig gezogenen a mit $\text{ggt}(a, m) = 1$ die obigen Annahmen, also r gerade und die Primfaktoren von m sind nicht alle in $(a^{\frac{r}{2}} + 1)$ enthalten, mit einer Wahrscheinlichkeit größer oder gleich $1/2$ eintreffen.

Damit hat man einen polynomiellen probabilistischen Faktorisierungsalgorithmus, falls man die Ordnung einer Zahl a modulo m effektiv berechnen kann. Bis heute ist allerdings kein polynomieller klassischer Algorithmus zur Periodenbestimmung bekannt.

10.2 Diskrete Fourier-Transformation

Die Fourier-Transformation zerlegt eine Funktion in Grund- und Oberschwingungen. Bei der diskreten Fourier-Transformation wird eine Funktion auf einem bestimmten Intervall betrachtet und an diskreten Punkten abgetastet. Die Fourier-Koeffizienten c_k geben dann die Gewichte der Grund- und Oberschwingungen an.

Definition:

Zu gegebenen f_k, $k = 0, \ldots, N-1$, bildet man die *Fourierkoeffizienten*

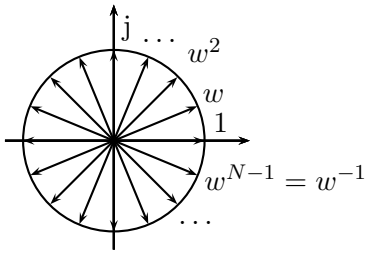
$$c_l \;=\; \frac{1}{\sqrt{N}} \cdot \sum_{k=0}^{N-1} f_k \cdot \mathrm{e}^{-\mathrm{j}\cdot\frac{2\pi kl}{N}}.$$

Mit der N-ten Einheitswurzeln

$$\omega \;=\; \mathrm{e}^{\mathrm{j}\cdot\frac{2\pi}{N}}$$

(ω erfüllt also $\omega^N = 1$) ist

$$\mathrm{e}^{-\mathrm{j}\cdot\frac{2\pi kl}{N}} \;=\; \left(\mathrm{e}^{\mathrm{j}\cdot\frac{2\pi}{N}}\right)^{-kl} \;=\; \omega^{-kl},$$



also

$$c_l \;=\; \frac{1}{\sqrt{N}} \cdot \sum_{k=0}^{N-1} f_k \cdot \omega^{-kl}.$$

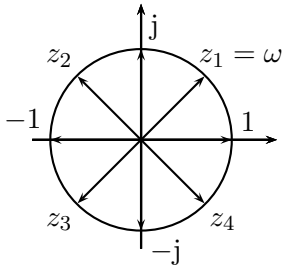
Man kann die Berechnung der Fourier-Koeffizienten c_0, …, c_{N-1} auch als Matrix-Vektor-Produkt schreiben:

$$\begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{N-1} \end{pmatrix} \;=\; \frac{1}{\sqrt{N}} \begin{pmatrix} \omega^{-0\cdot 0} & \omega^{-1\cdot 0} & \cdots & \omega^{-(N-1)\cdot 0} \\ \omega^{-0\cdot 1} & \omega^{-1\cdot 1} & \cdots & \omega^{-(N-1)\cdot 1} \\ \vdots & \vdots & \ddots & \vdots \\ \omega^{-0\cdot(N-1)} & \omega^{-1\cdot(N-1)} & \cdots & \omega^{-(N-1)\cdot(N-1)} \end{pmatrix} \cdot \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{N-1} \end{pmatrix}$$

Beispiel:

Für $N = 8$ ist $\omega = \mathrm{e}^{\mathrm{j}\cdot\frac{2\pi}{8}} = \mathrm{e}^{\mathrm{j}\cdot\frac{\pi}{4}}$.

Mit $z_1 = \omega$, $z_2 = \omega^3$, $z_3 = \omega^5$ und $z_4 = \omega^7$(s. Bild) ergibt sich konkret als Transformationsmatrix



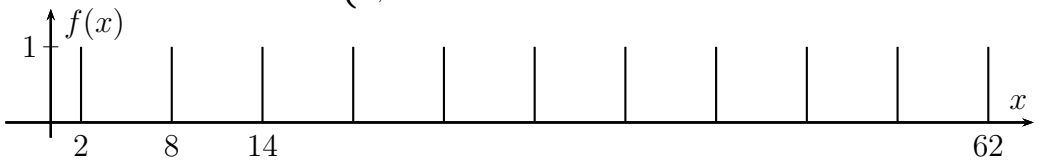
$$C \;=\; \frac{1}{\sqrt{8}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & z_4 & -\mathrm{j} & z_3 & -1 & z_2 & \mathrm{j} & z_1 \\ 1 & -\mathrm{j} & -1 & \mathrm{j} & 1 & -\mathrm{j} & -1 & \mathrm{j} \\ 1 & z_3 & \mathrm{j} & z_4 & -1 & z_1 & -\mathrm{j} & z_2 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & z_2 & -\mathrm{j} & z_1 & -1 & z_4 & \mathrm{j} & z_3 \\ 1 & \mathrm{j} & -1 & -\mathrm{j} & 1 & \mathrm{j} & -1 & -\mathrm{j} \\ 1 & z_1 & \mathrm{j} & z_2 & -1 & z_3 & -\mathrm{j} & z_4 \end{pmatrix}$$

Ist die Funktion bzw. sind die abgetasteten Werte f_k auf dem Intervall periodisch, so erkennt man das an den Fourier-Koeffizienten: Enthält das betrachtete Intervall genau k_0 Perioden, so sind nur die c_k von Null verschieden, für die k ein Vielfaches von k_0 ist.

Beispiel:

Betrachtet wird die 6-periodische Funktion

$$f : \mathbb{N} \to \mathbb{N},\ f(x) \ = \ \begin{cases} 1, \text{ falls } x = 2 + 6k,\ k \in \mathbb{N}, \\ 0, \text{ sonst.} \end{cases}$$



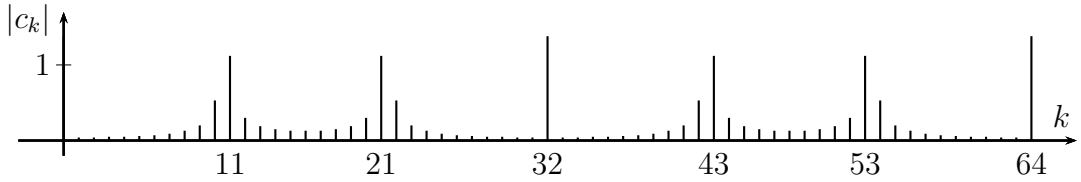
Die Fourierkoeffizienten bei einem Intervall $[0; 60[$ mit 60 Abtastungen ergibt:

Anders ausgedrückt: Ist f r-periodisch und $N = k_0 \cdot r$, so sind nur die c_k von Null verschieden, für die k ein Vielfaches von k_0, also von $\frac{N}{r}$ ist.

Ist f r-periodisch aber N kein genaues Vielfaches von r, so gilt weiterhin, dass nur die Fourierkoeffizienten mit Indizes nahe bei Vielfachen von $\frac{N}{r}$ wesentlich von Null verschieden sind.

Beispiel:

Betrachtet wird nun die 6-periodische Funktion f von oben aber betrachtet auf einem Intervall $[0; 64[$ mit 64 Abtastungen. Die Beträge der Fourierkoeffizienten ergeben folgendes Bild:



Man sieht deutlich die „Konzentration“ auf Fourier-Koeffizienten c_k, wobei k ein Vielfaches von $\frac{64}{6} \approx 10.7$ ist.

Bemerkung:

Eine naive Implementierung der diskreten Fourier-Transformation benötigt einen Aufwand von $O(N^2)$.

Ist N eine 2er-Potenz, so gibt es mit der *Fast-Fourier-Transformation* die Möglichkeit, die Koeffizienten mit einem Aufwand $O(N \cdot \log N)$ zu berechnen.

10.3 Quanten-Fourier-Transformation

Die Transformationsmatrix

$$C \;=\; \frac{1}{\sqrt{N}} \begin{pmatrix} \omega^{-0\cdot 0} & \omega^{-1\cdot 0} & \cdots & \omega^{-(N-1)\cdot 0} \\ \omega^{-0\cdot 1} & \omega^{-1\cdot 1} & \cdots & \omega^{-(N-1)\cdot 1} \\ \vdots & \vdots & \ddots & \vdots \\ \omega^{-0\cdot (N-1)} & \omega^{-1\cdot (N-1)} & \cdots & \omega^{-(N-1)\cdot (N-1)} \end{pmatrix}$$

der diskreten Fourier-Transformation ist unitär, ebenso dann auch die Transformationsmatrix der Rücktransformation $D = C^{-1} = C^H$. Wegen

$$\omega^* \;=\; \left(\mathrm{e}^{\mathrm{j}\cdot\frac{2\pi}{N}}\right)^* \;=\; \mathrm{e}^{-\mathrm{j}\cdot\frac{2\pi}{N}} \;=\; \left(\mathrm{e}^{\mathrm{j}\cdot\frac{2\pi}{N}}\right)^{-1} \;=\; \omega^{-1}$$

ist

$$D \;=\; \frac{1}{\sqrt{N}} \begin{pmatrix} \omega^{0\cdot 0} & \omega^{1\cdot 0} & \cdots & \omega^{(N-1)\cdot 0} \\ \omega^{0\cdot 1} & \omega^{1\cdot 1} & \cdots & \omega^{(N-1)\cdot 1} \\ \vdots & \vdots & \ddots & \vdots \\ \omega^{0\cdot (N-1)} & \omega^{1\cdot (N-1)} & \cdots & \omega^{(N-1)\cdot (N-1)} \end{pmatrix}.$$

Im Prinzip hat die Transformation mit D die gleichen Eigenschaften wie die diskrete Fouriertransformation.

Bei $N = 2^n$ kann man die Matrix D als Transformationsmatrix eines n-Qubit-Registers betrachten.

Beispiel:

Sei $N = 4$, also $n = 2$. Dann ist

$$\omega \;=\; \mathrm{e}^{\mathrm{j}\cdot\frac{2\pi}{4}} \;=\; \mathrm{e}^{\mathrm{j}\cdot\frac{\pi}{2}} \;=\; \mathrm{j}$$

und damit

$$D \;=\; \frac{1}{2}\cdot \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \mathrm{j} & -1 & -\mathrm{j} \\ 1 & -1 & 1 & -1 \\ 1 & -\mathrm{j} & -1 & \mathrm{j} \end{pmatrix}.$$

Definition:

Sei $N = 2^n$ und $\omega_N = \mathrm{e}^{\mathrm{j}\cdot\frac{2\pi}{N}}$. Die *Quanten-Fourier-Transformation* QFT_N der Ordnung N ist die Transformation auf einem n-Qubit-Register, die durch die Matrix D beschrieben wird.

Die Auswirkung auf den l-ten Basisvektor $|l\rangle_n$, $l = 0, \ldots, N-1$, ist also

$$\mathrm{QFT}_N(|l\rangle_n) \;=\; \frac{1}{\sqrt{N}} \cdot \sum_{k=0}^{N-1} {\omega_N}^{k\cdot l} \cdot |k\rangle_n \,.$$

Satz:

Sie $N = 2^n$ und $\omega_s = \mathrm{e}^{\mathrm{j}\cdot\frac{2\pi}{s}}$. Man kann zeigen, dass für den l-ten Basisvektor $|l\rangle_n$, $l = 0, \ldots, N-1$, gilt

$$\mathrm{QFT}_N(|l\rangle_n) \;=\; \frac{1}{\sqrt{N}} \cdot \big(\,|0\rangle + {\omega_2}^l\,|1\rangle\,\big) \otimes \big(\,|0\rangle + {\omega_4}^l\,|1\rangle\,\big) \otimes \ldots \otimes \big(\,|0\rangle + {\omega_N}^l\,|1\rangle\,\big).$$

Bemerkungen:

1. Das Tensorprodukt rechts besitzt also n Tensor-Faktoren. Wenn man den Vorfaktor $\frac{1}{\sqrt{N}} = \frac{1}{\sqrt{2^n}} = \big(\frac{1}{\sqrt{2}}\big)^n$ auf die einzelnen Tensor-Faktoren aufteilt, hat man also Tensor-Faktoren der Gestalt

   $$\tfrac{1}{\sqrt{2}}\big(\,|0\rangle + {\omega_{2^k}}^l\,|1\rangle\,\big).$$

2. Die Darstellung ist eng verwandt mit der Berechnung der klassischen diskreten Fourier-Transformation mittel der *Fast-Fourier-Transformation*.

Beispiel:

Sei $N = 4$, also $n = 2$. Wegen

$$\omega_2 = \mathrm{e}^{\mathrm{j}\cdot\frac{2\pi}{2}} = \mathrm{e}^{\mathrm{j}\cdot\pi} = -1 \qquad \text{und} \qquad \omega_4 = \mathrm{e}^{\mathrm{j}\cdot\frac{2\pi}{4}} = \mathrm{e}^{\mathrm{j}\cdot\frac{\pi}{2}} = \mathrm{j}$$

erhält man

$$\begin{aligned}
\mathrm{QFT}_4(|l\rangle_2) \;&=\; \frac{1}{\sqrt{4}} \cdot \big(\,|0\rangle + {\omega_2}^l\,|1\rangle\,\big) \otimes \big(\,|0\rangle + {\omega_4}^l\,|1\rangle\,\big) \\
&=\; \frac{1}{2} \cdot \big(\,|0\rangle + (-1)^l\,|1\rangle\,\big) \otimes \big(\,|0\rangle + \mathrm{j}^l\,|1\rangle\,\big) \\
&=\; \frac{1}{2} \cdot \big(\,|00\rangle + \mathrm{j}^l\,|01\rangle + (-1)^l\,|10\rangle + (-\mathrm{j})^l\,|11\rangle\,\big),
\end{aligned}$$

also

$$\begin{aligned}
\mathrm{QFT}_4(|0\rangle_2) \;&=\; \tfrac{1}{2} \cdot \big(\,|00\rangle + |01\rangle + |10\rangle + |11\rangle\,\big), \\
\mathrm{QFT}_4(|1\rangle_2) \;&=\; \tfrac{1}{2} \cdot \big(\,|00\rangle + \mathrm{j}\,|01\rangle - |10\rangle - \mathrm{j}\,|11\rangle\,\big), \\
\mathrm{QFT}_4(|2\rangle_2) \;&=\; \tfrac{1}{2} \cdot \big(\,|00\rangle - |01\rangle + |10\rangle - |11\rangle\,\big), \\
\mathrm{QFT}_4(|3\rangle_2) \;&=\; \tfrac{1}{2} \cdot \big(\,|00\rangle - \mathrm{j}\,|01\rangle - |10\rangle + \mathrm{j}\,|11\rangle\,\big).
\end{aligned}$$

Man erkennt die Transformationsmatrix D von oben.

Wie lassen sich die einzelnen Tensor-Faktoren in der Darstellung des Satzes oben, also z.B. $\frac{1}{\sqrt{2}}\big(\,|0\rangle + {\omega_2}^l\,|1\rangle\,\big)$ oder $\frac{1}{\sqrt{2}}\big(\,|0\rangle + {\omega_4}^l\,|1\rangle\,\big)$ erzeugen?

Betrachte beispielhaft QFT_8, also $n = 3$. Sei $l = (l_2 l_1 l_0)_2$ die Binärdarstellung von l, also

$$l \;=\; 2^2 \cdot l_2 + 2^1 \cdot l_1 + 2^0 \cdot l_0 \;=\; 4l_2 + 2l_1 + l_0.$$

Es ist $\omega_2 = -1$ und

$$\omega_2{}^l \;=\; (-1)^{4l_2+2l_1+l_0} \;=\; (-1)^{l_0}.$$

Der Wert von $\omega_2{}^l$ und damit von $\frac{1}{\sqrt{2}}\big(\,|0\rangle + \omega_2{}^l\,|1\rangle\,\big)$ hängt also nur von l_0 ab und ist gleich $\frac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big)$ bzw. $\frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big)$, je nachdem, ob $l_0 = 0$ oder $l_0 = 1$ ist.

Daher kann $\frac{1}{\sqrt{2}}\big(\,|0\rangle + \omega_2{}^l\,|1\rangle\,\big)$ durch eine Hadamard-Transformation angewendet auf das l_0-darstellende Qubit realisiert werden, da gilt

$$H\,|l_0\rangle \;=\; \tfrac{1}{\sqrt{2}}\big(\,|0\rangle + (-1)^{l_0}\,|1\rangle\,\big) \quad \text{für } l_0 \in \{0,1\}.$$

Es ist $\omega_4 = \mathrm{j}$ und

$$\omega_4{}^l \;=\; \mathrm{j}^{4l_2+2l_1+l_0} \;=\; (\mathrm{j}^4)^{l_2} \cdot (\mathrm{j}^2)^{l_1} \cdot \mathrm{j}^{l_0} \;=\; 1^{l_2} \cdot (-1)^{l_1} \cdot \mathrm{j}^{l_0} \;=\; (-1)^{l_1} \cdot \mathrm{j}^{l_0}.$$

Daher kann man $\frac{1}{\sqrt{2}}\big(\,|0\rangle + \omega_4{}^l\,|1\rangle\,\big)$ realisieren durch eine Hadamard-Transformation angewendet auf das l_1-darstellende Qubit, wobei bei $l_0 = 1$ der $|1\rangle$-Zustand noch mit j multipliziert wird. Eine entsprechend Multiplikation kann man mit dem *Phasengatter* R_d realisieren:

$$R_d \;=\; \begin{pmatrix} 1 & 0 \\ 0 & \omega_{2^d} \end{pmatrix}.$$

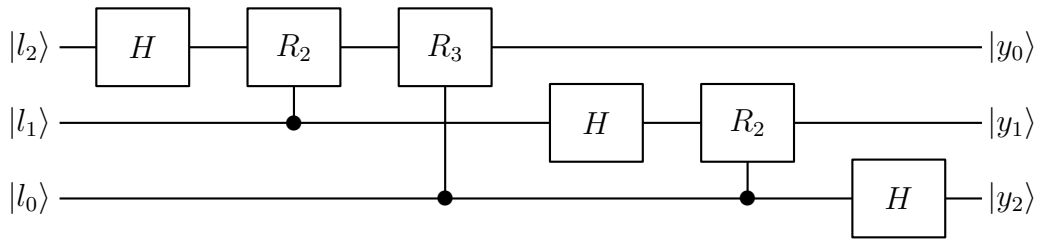
Bei $|1\rangle$ wird also die Amplitude mit ω_{2^d} multipliziert, d.h., die komplexe Phase wird um $\frac{2\pi}{2^d}$ gedreht. Eine Multiplikation des $|1\rangle$-Zustands mit j entspricht also einer Anwendung von R_2.

Bei den weiteren Tensor-Faktoren geht es ähnlich: $\frac{1}{\sqrt{2}}\big(\,|0\rangle + \omega_8{}^l\,|1\rangle\,\big)$ kann man wegen

$$\omega_8{}^l \;=\; \omega_8{}^{4l_2+2l_1+l_0} \;=\; (\omega_8{}^4)^{l_2} \cdot (\omega_8{}^2)^{l_1} \cdot \omega_8{}^{l_0} \;=\; (-1)^{l_2} \cdot \omega_4{}^{l_1} \cdot \omega_8{}^{l_0}$$

durch eine Hadamard-Transformation angewendet auf das l_2-darstellende Qubit gefolgt von l_1- bzw. l_0-bedingten Phasengatter R_2 bzw. R_3 realisieren.

Der folgende Schaltkreis zeigt die Berechnung von QFT_8:



Man beachte, dass beim Schaltkreis am Ausgang die Qubits in umgekehrter Reihenfolge stehen!

Für eine entsprechenden Realisierung einer Quanten-Fourier-Transformation bei n Qubits, also bei $N = 2^n$, benötigt man

$$n \ + \ (n-1) \ + \ \ldots \ + \ 1 \ = \ \tfrac{1}{2}n(n+1)$$

Gatter. Damit hat man einen Aufwand von $O(n^2) = O((\log N)^2)$ gegenüber $O(N \cdot \log N)$ bei der klassischen Fast-Fourier-Transformation.

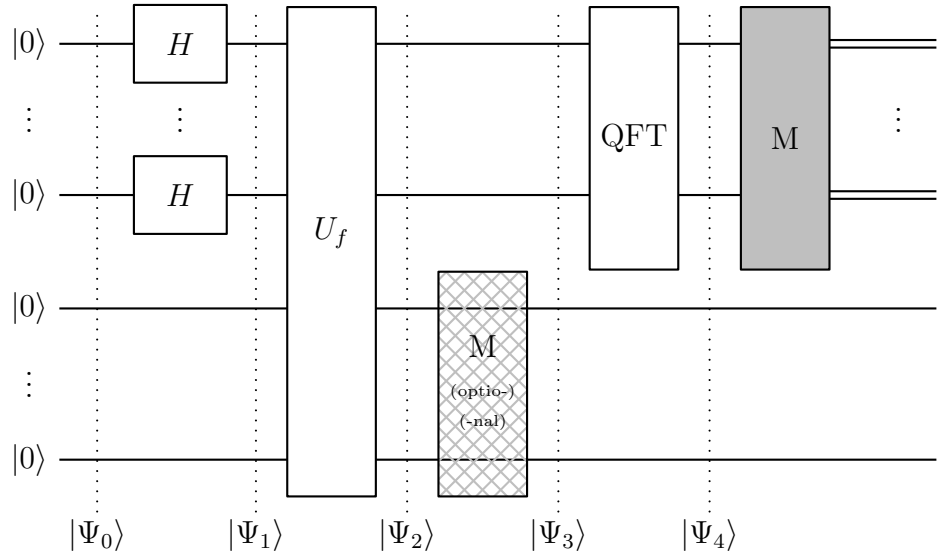
10.4 Der eigentliche Quanten-Algorithmus

Vorgegeben ist ein m, das das Produkt zweier (großer) verschiedener Primzahlen ist, und ein $a \in \{1, \ldots, m\}$ mit $\text{ggt}(a, m) = 1$.

Ziel ist die Bestimmung der Ordnung r von a modulo m.

Man wählt nun eine 2er-Potenz $N = 2^{n_x}$ in der Größenordnung von m^2, um mit hoher Wahrscheinlichkeit am Ende ein erfolgreiches Ergebnis zu haben, und ferner n_y (minimal), so dass $m < 2^{n_y}$ ist, damit man Zahlen modulo m mit n_y Bits darstellen kann.

Der Quanten-Algorithmus, der die Ordnungsbestimmung (probabilistisch) realisiert, ist im folgenden Schaltkreis dargestellt:



Analyse:

Man beginnt mit einem Zustand $|\Psi_0\rangle$ bestehend aus $n_x + n_y$ Qubits, die mit $|0\rangle$ initialisiert werden. Die oberen n_x Qubits werden im folgenden als x-Register bezeichnet, die unteren n_y Qubits als y-Register.

Durch die Hadamard-Transformationen werden die Qubits des x-Registers gleichmäßig überlagert (Zustand $|\Psi_1\rangle$).

Die Transformation U_f ist (ähnlich dem Deutsch-Josza- und Grover-Algorithmus) die Quanten-Version der Funktion

$$f(x) \;=\; a^x \bmod m,$$

die auf die x- und y-Register wirkt durch

$$U_f(|x\rangle_{n_x} \otimes |y\rangle_{n_y}) \;=\; |x\rangle_{n_x} \otimes |y \oplus f(x)\rangle_{n_y}\,.$$

Da nach Abschnitt 5.1 ein Quantencomputer alles das kann, was ein klassischer Computer kann, ist die Realisierung von U_f (ggf. mit Hilfs-Qubits) möglich.

Wegen der Initialisierung der Qubits des y-Registers mit $|0\rangle$ besteht der Zustand $|\Psi_2\rangle$ aus einer gleichmäßigen Überlagerung aller

$$|x\rangle_{n_x} \otimes |f(x)\rangle_{n_y}\,, \quad x = 0, \ldots, N-1.$$

Hier wird die Parallelität bei der Quanten-Berechnung ausgenutzt: Die Berechnung ist mit in n_x polynomiellem Aufwand möglich; klassisch braucht man $N = 2^{n_x}$ Funktionsauswertungen.

Beim Zustand $|\Psi_2\rangle$ kann man nun optional das y-Register messen. Dabei wird man einen der Funktionswerte $f(x)$ für ein spezielles x_0 erhalten. Wegen der r-Periodizität von f kann man sich o.B.d.A. $x_0 \in \{0, \ldots, r-1\}$ vorstellen.

Der Zustand kollabiert dann so, dass das x-Register aus der gleichmäßigen Überlagerung all der x-Werte besteht, die $f(x) = f(x_0)$ erfüllen, also aus

$$x_0, \quad , x_0 + r, \quad x_0 + 2r, \quad \ldots.$$

Beispiel:

Sei $m = 35$ und $a = 4$ (vgl. das Beispiel in Abschnitt 10.1) und $N = 64$.

Misst man beispielsweise $4^2 \bmod 35 = 16$, so erhält man wegen der 6-Periodizität von $4^x \bmod 35$ eine gleichmäßige Überlagerung von

$$|2\rangle_{n_x} \otimes |16\rangle_{n_y}\,, \quad |8\rangle_{n_x} \otimes |16\rangle_{n_y}\,, \quad |14\rangle_{n_x} \otimes |16\rangle_{n_y}\,, \quad \ldots \quad , |62\rangle_{n_x} \otimes |16\rangle_{n_y}$$

also bis auf einen Normierungsfaktor

$$\big(\,|2\rangle_{n_x} + |8\rangle_{n_x} + |14\rangle_{n_x} + \ldots + |62\rangle_{n_x}\,\big) \otimes |16\rangle_{n_y}\,.$$

Betrachtet man nun $|\Psi_3\rangle$ als einen solchen kollabierten Zustand nach einer Messung, so entsteht nach der QFT entsprechend der Ausführungen in Abschnitt 10.2 ein Zustand $|\Psi_4\rangle$, bei dem nur die Basiszustände $|x\rangle$ mit x nahe bei Vielfachen von $\frac{N}{r}$ Amplituden haben, die wesentlich von Null verschieden sind.

Dieses Verhalten hat man unabhängig von dem bei der Messung des y-Registers von $|\Psi_2\rangle$ beobachteten Funktionswert $f(x_0)$. Ohne Messung ist $|\Psi_3\rangle = |\Psi_2\rangle$ eine Überlagerung von diesen Zuständen zu unterschiedlichen Funktionswerten $f(x)$.

Beispiel:

Sie $m = 35$ und $a = 4$ (vgl. das Beispiel in Abschnitt 10.1) und $N = 64$.

Bis auf einen Normierungsfaktor ist $|\Psi_2\rangle$ gleich

$$\begin{aligned}
&\big(\,|0\rangle_{n_x} + |6\rangle_{n_x} + |12\rangle_{n_x} + \ldots + |60\rangle_{n_x}\,\big) \otimes |1\rangle_{n_y} \\
+&\big(\,|1\rangle_{n_x} + |7\rangle_{n_x} + |13\rangle_{n_x} + \ldots + |61\rangle_{n_x}\,\big) \otimes |4\rangle_{n_y} \\
+&\big(\,|2\rangle_{n_x} + |8\rangle_{n_x} + |14\rangle_{n_x} + \ldots + |62\rangle_{n_x}\,\big) \otimes |16\rangle_{n_y} \\
+&\quad \ldots \\
+&\big(\,|5\rangle_{n_x} + |11\rangle_{n_x} + |17\rangle_{n_x} + \ldots + |59\rangle_{n_x}\,\big) \otimes |9\rangle_{n_y}\,.
\end{aligned}$$

Da die QFT jeweils die gleiche Konzentration auf Basiszustände $|x\rangle$ mit x nahe bei Vielfachen von $\frac{N}{r}$ bewirkt, geschieht dies unabhängig davon, ob man das y-Register von $|\Psi_2\rangle$ misst oder nicht: In jedem Fall ist $|\Psi_4\rangle$ ein Zustand, bei dem nur die Basiszustände $|x\rangle$ mit x nahe bei Vielfachen von $\frac{N}{r}$ Amplituden haben, die wesentlich von Null verschieden sind.

Die abschließende Messung des x-Registers liefert also ein x, das nahe bei einem Vielfachen von $\frac{N}{r}$ liegt:

$$x \;\approx\; k \cdot \frac{N}{r} \quad \text{für ein } k \in \mathbb{N} \quad \Leftrightarrow \quad \frac{x}{N} \;\approx\; \frac{k}{r} \quad \text{für ein } k \in \mathbb{N}.$$

Klassische Nachbearbeitung:

Gesucht ist die Ordnung r, also der Nenner eines Näherungsbruchs $\frac{k}{r}$ zu $\frac{x}{N}$; dabei sind x und N bekannt, k und r unbekannt, wobei r klein ist im Vergleich zu N.

Es gibt klassische Verfahren (z.B. *Kettenbruch-Entwicklung*), um zu einem Bruch Näherungsbrüche mit kleinerem Nenner zu ermitteln. Diese Nenner $\tilde{r}$ sind dann Kandidaten für die Ordnung. Ob man wirklich die Ordnung gefunden hat, kann man nachprüfen, indem man prüft, ob $a^{\tilde{r}} \bmod m = 1$ ist.

Beispiel:

Betrachtet wird der Fall, dass bei einer 6-periodischen Funktion bei $N = 64$ der Wert 53 gemessen wird. Die Kettenbruch-Entwicklung ergibt dann

$$\begin{aligned}
\frac{53}{64} &= \frac{1}{\frac{64}{53}} = \frac{1}{1+\frac{11}{53}} = \frac{1}{1+\frac{1}{\frac{53}{11}}} = \frac{1}{1+\frac{1}{4+\frac{9}{11}}} \\
&= \frac{1}{1+\frac{1}{4+\frac{1}{\frac{11}{9}}}} = \frac{1}{1+\frac{1}{4+\frac{1}{1+\frac{2}{9}}}} = \frac{1}{1+\frac{1}{4+\frac{1}{1+\frac{1}{\frac{9}{2}}}}} = \frac{1}{1+\frac{1}{4+\frac{1}{1+\frac{1}{4+\frac{1}{2}}}}}.
\end{aligned}$$

Näherungsbrüche erhält man durch die abgeschnittenen Kettenbrüche, hier also

$$\frac{1}{1+\frac{1}{4}} \;=\; \frac{4}{5} \qquad \text{und} \qquad \frac{1}{1+\frac{1}{4+\frac{1}{1}}} \;=\; \frac{5}{6}.$$

Der zweite Näherungsbruch hat die gesuchte Periode als Nenner.

Bemerkung:

Wenn k und r gemeinsame Teiler haben, so wird man durch die Kettenbruch-Entwicklung nur gekürzte Darstellungen von $\frac{k}{r}$ finden. Man kann aber zeigen, dass mit hoher Wahrscheinlichkeit k und r teilerfremd sind.

Man kann zeigen, dass man so mit einer gewissen Wahrscheinlichkeit die Periode r bestimmen kann.

10.5 Diskrete Logarithmen

Einige Verfahren der asymmetrischen Kryptographie basieren nicht auf der (vermutlichen) Schwierigkeit des Faktorisierungsproblems sondern auf der (vermutlichen) Schwierigkeit des diskreten Logarithmus, z.B. der Diffie-Hellman-Schlüsselaustausch oder das Elgamal-Verschlüsselungsverfahren.

Definition:

Ist $p \in \mathbb{N}$ eine Primzahl und $a \in \{1, \ldots, p-1\}$ so gewählt, dass

$$\{a^x \bmod p \,|\, x \in \{1, \ldots, p-1\}\} \;=\; \{1, \ldots, p-1\},$$

so ist der *diskrete Logarithmus* von $A \in \{1, \ldots, p-1\}$ zur Basis a modulo p das (eindeutige) $x \in \{1, \ldots, p-1\}$ mit $A = a^x \bmod p$.

Man nimmt an, dass die Bestimmung des diskreten Logarithmus klassisch schwierig zu lösen ist.

Mit der Idee des Shor-Algorithmus – konkret der Periodenberechnung mittels der Quanten-Fourier-Transformation – ist das Problem effektiv lösbar. Dazu betrachtet man bei vorgegebenem p, a und A die Funktion

$$f : \mathbb{N} \times \mathbb{N} \to \mathbb{N},\; f(x,y) \;=\; a^x \cdot A^{-y} \bmod p.$$

Dabei ist A^{-y} das modulare Inverse zu A^y modulo p, also die Zahl z mit $z \cdot A^y \bmod p = 1$.

Ist $a^{x_0} = A$, also x_0 der diskrete Logarithmus von A zur Basis a modulo p, so gilt modulo p

$$\begin{aligned} f(x+x_0, y+1) \;&=\; a^{x+x_0} \cdot A^{-(y+1)} \;=\; a^x \cdot a^{x_0} \;\cdot\; A^{-y-1} \\ &=\; a^x \cdot A \;\cdot\; A^{-y} \cdot A^{-1} \;=\; a^x \cdot A^{-y} \;=\; f(x,y), \end{aligned}$$

d.h., die Funktion f ist $(x_0, 1)$-periodisch, und mit einer Periodenbestimmung kann man x_0 ermitteln.

Bemerkung:

In der Kryptographie werden auch diskrete Logarithmen auf der Gruppe der elliptischen Kurven genutzt. Auch hier gibt es eine Variante des Shor-Algorithmus, mit der derartige diskrete Logarithmen effektiv berechnet werden können.