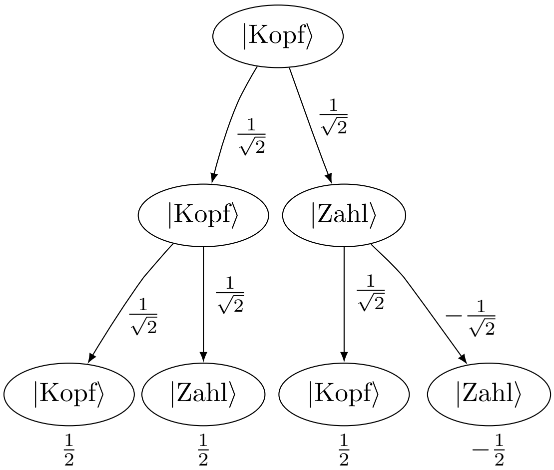
Allgemein: Seien $|x_1\rangle, \dots, |x_n\rangle$ eine orthonormale Basis des $\mathbb{C}^n$ (auch H_n für Hilbertraum).
Zustand eines Quantensystems: $\alpha_1|x_1\rangle + \alpha_2|x_2\rangle + \cdots + \alpha_n|x_n\rangle$ mit $|\alpha_1|^2 + \cdots + |\alpha_n|^2 = 1$
Messung: x_i mit $WS|\alpha_i|^2$

Bezeichnung:
- Basisvektoren $|x_i\rangle$ werden Basiszustände genannt.
- α_i heißen Amplituden
- Allg. Zustand ist Superposition der Basiszustände (Überlagerung)
- $\psi(x_i) = \alpha_i$ heist Wellenfunktion.
- $|x >= e^{i\varphi}|y > \Leftrightarrow$ Zustände $|x\rangle$ und $|y\rangle$ heißen äquivalent

Vergleich : Wahrscheinlichkeitsverteilung $P_1[x_1] + \cdots + p_n[x_n]$ $\sum i = 1^n p_i = 1$
Superposition $\alpha_1|x_1\rangle + \cdots + \alpha_n|x_n\rangle$ $\sum\limits_{i=1}^{n} |\alpha_i|^2 = 1$, d.h. $|\alpha_i|^2 WS-$Verteilung. Trotzdem fundamental verschieden!

Beispiel: Quanten-Münzwurf:
$|Kopf\rangle \mapsto \frac{1}{\sqrt{2}}|Kopf\rangle + \frac{1}{\sqrt{2}}|Zahl\rangle$
$|Zahl\rangle \mapsto \frac{1}{\sqrt{2}}|Kopf\rangle - \frac{1}{\sqrt{2}}|Zahl\rangle$
Einfacher Münzwurf liefert Kopf oder Zahl mit WS jeweils $\frac{1}{2}$
Zweifacher Münzwurf:



- Amplituden von $|Kopf\rangle$ summieren sich zu 1 $\rightarrow$ positive Interferenz
- Amplituden von $|Zahl\rangle$ summieren sich zu 0 $\rightarrow$ negative Interferenz

Strategie: Statt die Ws. unerwünschter Konfiguration klein zu halten, kann man auch deren Amplituden gegenseitig auslöschen.

Man beachte: Superposition $\alpha_1|x_1\rangle + \cdots + \alpha_n|x_n\rangle$ liefert x_i mit $Ws|\alpha_i|^2$
Wechsel zu anderer orthonormaler Basis $|x_1'\rangle, \dots, |x_n'\rangle$ mit $|x_1'\rangle = \alpha_1|x_1\rangle + \cdots + \alpha_n|x_n\rangle$ liefert x_1' mit $Ws1$.

3.1 Zustandsübergänge

Da Quantenzustände stets Einheitsvektoren sind: längenerhaltene Abbildung
Aus den Gesetzen der Quantenphysik: lineare Abbildung, reversibel

Definition (unitäre Abb.): eine lineare Abb. $U : \mathbb{C}^n \rightarrow \mathbb{C}^n$ heißt unitär, falls für alle $|x\rangle \in \mathbb{C}^n$ gilt: $||x\rangle| = \sqrt{\langle x|x\rangle} = \sqrt{\langle U||x\rangle|U|x\rangle >} = |U||x\rangle|$
Eine Matrix heißt unitär falls $(U^*)^T = U^{-1}$

Satz: Sei $U \in \mathbb{C}^{m\times m}$ eine unitäre Matrix. Dann gilt für alle $|x\rangle \in \mathbb{C}^m : |U|x\rangle| = ||x\rangle|$. D.h. U beschreibt eine unitäre Abbildung.

Beweis: Lineare Algebra: Für jedes $A \in \mathbb{C}^{m\times m}, |x\rangle, |y\rangle \in \mathbb{C}^m$ gilt: $\langle x|A|y\rangle = \langle (A^*)^T|x\rangle||y\rangle\rangle$

$\Rightarrow |U|x\rangle| = \sqrt{\langle U|x\rangle|U|x\rangle\rangle} = \sqrt{< \underbrace{(U^*)^T}_{U^{-1}} U|x\rangle||x\rangle\rangle} = \sqrt{\langle x|x\rangle} = ||x\rangle|$

Beispiel: Hadamard-Walsh-Matrix $W_2 = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$

Übung: $W_2(W_2^*)^T = I$

Anmerkung: W_2 Beschreibt "Quanten-Münzwurf"

3.2 Entwicklung eines Quantenbits

Sei $|0\rangle = (1,0)^T, |1\rangle = (0,1)^T, U = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$

$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} = a\begin{pmatrix} 1 \\ 0 \end{pmatrix} + b\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, d.h.$|0\rangle \overset{U}{\longmapsto} a|0\rangle + b|1\rangle$

$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} c \\ d \end{pmatrix} = c\begin{pmatrix} 1 \\ 0 \end{pmatrix} + d\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, d.h.$|1\rangle \overset{U}{\longmapsto} c|0\rangle + d|1\rangle$

3.3 Beispiele unitärer Abbildungen

Beispiel 1 (Quanten-Not): $M_\neg = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$M_\neg$ ist unitär, $(M_\neg^*)^T = M_\neg, M_\neg^2 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

$\begin{matrix} (1,0) \mapsto (0,1) \\ (0,1) \mapsto (1,0) \end{matrix}$ d.h. $\begin{matrix} |0\rangle \mapsto |1\rangle \\ |1\rangle \mapsto |0\rangle \end{matrix}$

Beispiel 2 (Wurzel des Not): $\sqrt{M_\neg} = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix}$

$$\begin{aligned} |0\rangle \overset{\sqrt{M_\neg}}{\longmapsto} \frac{1+i}{2}|0\rangle + \frac{1-i}{2}|1\rangle \overset{\sqrt{M_\neg}}{\longmapsto} &\frac{1+i}{2}(\frac{1+i}{2}|0\rangle + \frac{1-i}{2}|1\rangle) + \frac{1-i}{2}(\frac{1-i}{2}|0\rangle + \frac{1+i}{2}|1\rangle) \\ &= ((\frac{1+i}{2})^2 + (\frac{1-i}{2})^2)|0\rangle + 2\frac{1-i^2}{4}|1\rangle \\ &= \frac{1+2i+i^2+1-2i+i^2}{4}|0\rangle + \frac{4}{4}|1\rangle = |1\rangle \end{aligned}$$

Äqivalent $|1\rangle \overset{\sqrt{M_\neg}}{\longmapsto} \frac{1-i}{2}|0\rangle + \frac{1+i}{2}|1\rangle \overset{\sqrt{M_\neg}}{\longmapsto} |0\rangle$ wegen $\left|\frac{1+i}{2}\right|^2 = \left|\frac{1-i}{2}\right|^2 = \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$

Übung: $\sqrt{M_\neg}$ ist unitär, $(\sqrt{M_\neg})^2 = M_\neg$.

Beispiel 3 (Haddamard-Walsh Matrix $W_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$$\begin{aligned} |0\rangle \overset{W_2}{\longmapsto} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \overset{W_2}{\longmapsto} &\frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) + \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) \\ &= \left(\frac{1}{2} + \frac{1}{2}\right)|0\rangle + \left(\frac{1}{2} - \frac{1}{2}\right)|1\rangle = |0\rangle \end{aligned}$$

Beispiel 4 (Flip) $F = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$|0\rangle \mapsto |0\rangle, |1\rangle \mapsto -|1\rangle$

Allgemein: $F_\Theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\Theta} \end{pmatrix}$

$|0\rangle \mapsto |0\rangle, |1\rangle \mapsto e^{i\Theta}|1\rangle$, Man beachte: $F_\pi = F$

Definition (Äquivalenz von Zuständen) Zwei Zustände $|x\rangle, |y\rangle \in \mathbb{C}^n$ heißen genau dann äquivalent, wenn gilt: $|x\rangle = e^{i\Theta}|y\rangle$

Flip transformiert $|1\rangle$ in einen äquivalenten Zustand. Messung von $|1\rangle$ mit selber Ws.

Übung: $U = \begin{pmatrix} i\cos\Theta & -i\sin\Theta \\ i\sin\Theta & i\cos\Theta \end{pmatrix}$ ist unitär

Der Zustand eines 2-Qbit-Systems ist ein Einheitsvektor im $\mathbb{C}^4$

4 Exkurs über Tensorprodukte

Definition (Tensorprodukt) Seien $|x\rangle = (x_1, \dots, x_n) \in \mathbb{C}^n, |y\rangle = (y_1, \dots, y_m) \in \mathbb{C}^m$. Das Tensorprodukt von $|x\rangle$ und $|y\rangle$ ist definiert als:
$|x\rangle \otimes |y\rangle = (x_1y_1, x_1y_2, \dots, x_1y_m, x_2y_1, \dots, x_2y_m, \dots, x_ny_1, \dots, x_ny_m) \in \mathbb{C}^{nm}$

Beispiel:

- $|0\rangle = (1,0)^T, |1\rangle = (0,1)^T$
  $|0\rangle \otimes |1\rangle = (0,1,0,0)^T$
- $|x\rangle = \frac{1}{\sqrt{2}}(1,-1)^T, |y\rangle = \frac{1}{\sqrt{2}}(1,1)^T$
  $|x\rangle \otimes |y\rangle = \frac{1}{2}(1,1,-1,-1)^T$

Man beobachte: $|x\rangle \otimes |y\rangle \neq |y\rangle \otimes |x\rangle$

4.1 Rechenregeln für das Tensorprodukt

- Distributivität:
  $\forall\ |x\rangle \in \mathbb{C}^n, |y\rangle, |z\rangle \in \mathbb{C}^m, |x\rangle \otimes (|y\rangle + |z\rangle) = |x\rangle \otimes |y\rangle + |x\rangle \otimes |z\rangle$
  $\forall\ |x\rangle, |y\rangle \in \mathbb{C}^n, |z\rangle \in \mathbb{C}^m, (|x\rangle + |y\rangle) \otimes |z\rangle = |x\rangle \otimes |z\rangle + |y\rangle \otimes |z\rangle$
- Skalare Multiplikation:
  $\forall\ |x\rangle \in \mathbb{C}^n, |y\rangle, \in \mathbb{C}^m, c \in \mathbb{C} : (c|x\rangle) \otimes |y\rangle = c(|x\rangle \otimes |y\rangle) = |x\rangle \otimes (c|y >)$
- Skalarprodukt:
  $\forall\ |v\rangle, |x\rangle \in \mathbb{C}^n, |y\rangle, |z\rangle \in \mathbb{C}^m, \langle |v\rangle \otimes |y\rangle || x\rangle \otimes |z\rangle\rangle = \langle v|x\rangle \cdot \langle y|z\rangle$
- Norm des Tensorprodukts:
  $\forall\ |x\rangle \in \mathbb{C}^n, |y\rangle \in \mathbb{C}^m : ||x\rangle \otimes |y\rangle|^2 = ||x\rangle|^2 \cdot ||y\rangle|^2$

Lemma: Sei $|x_1\rangle, \dots, |x_n\rangle \in \mathbb{C}^n$ eine orthonormale Basis des $\mathbb{C}^n$ und $|y_1\rangle, \dots, |y_m\rangle \in \mathbb{C}^m$ eine orthonormale Basis des $\mathbb{C}^m$. Dann ist
$|x_1\rangle \otimes |y_1\rangle, |x_1\rangle \otimes |y_2\rangle, \dots, |x_1\rangle \otimes |y_m\rangle, |x_2\rangle \otimes |y_1\rangle, \dots, |x_n\rangle \otimes |y_m\rangle \in \mathbb{C}^{mn}$ eine orthonormale Basis des $\mathbb{C}^{nm}$

Beweis: Für $|x_i\rangle, |y_j\rangle$ gilt:
$||x_i\rangle \otimes |y_j\rangle| = ||x_i\rangle| \cdot ||y_j\rangle| = 1 \cdot 1 = 1$
Weiterhin sind die Vektoren paarweise orthogonal:
$\langle |x_i\rangle \otimes |y_j\rangle || x_k\rangle \otimes |y_l\rangle\rangle = \langle x_i||x_k\rangle \cdot \langle y_j||y_l\rangle = 0\ \forall\ i \neq k$ oder $j \neq l$.

Beispiel:

$$\begin{aligned} |0\rangle = (1,0)^T, |1\rangle &= (0,1)^T & |x\rangle &= \frac{1}{\sqrt{2}}(1,-1)^T, |y\rangle = \frac{1}{\sqrt{2}}(1,1)^T \\ |0\rangle \otimes |0\rangle &= (1,0,0,0)^T & |x\rangle \otimes |x\rangle &= \frac{1}{2}(1,-1,-1,1)^T \\ |0\rangle \otimes |1\rangle &= (0,1,0,0)^T & |x\rangle \otimes |y\rangle &= \frac{1}{2}(1,1,-1,-1)^T \\ |1\rangle \otimes |0\rangle &= (0,0,1,0)^T & |y\rangle \otimes |x\rangle &= \frac{1}{2}(1,-1,1,-1)^T \\ |1\rangle \otimes |1\rangle &= (0,0,0,1)^T & |y\rangle \otimes |y\rangle &= \frac{1}{2}(1,1,1,1)^T \end{aligned}$$

Notation: Seien $|x\rangle \in \mathbb{C}^n, |y\rangle \in \mathbb{C}^m$. Wir bezeichnen $|x\rangle \otimes |y\rangle$ abkürzend als $|xy\rangle$.
Insbesondere gilt: $|0\rangle \otimes |0\rangle = |00\rangle, |0\rangle \otimes |1\rangle = |01\rangle$, usw.

5 2-Quantum Register

Bezeichne $|00\rangle = (1,0,0,0)^T, |01\rangle = (0,1,0,0)^T, |10\rangle = (0,0,1,0)^T, |11\rangle = (0,0,0,1)^T$ eine orthonormale Basis dez $\mathbb{C}^4$.

5.1 Zustand eines 2-Qubit Systems

Ein Zustand eines 2-Qubit Systems ist ein Einheitsvektor
$|v\rangle = c_0|00\rangle + c_1|10\rangle + c_2|10\rangle + c_3|11\rangle \in \mathbb{C}^4$ mit $c_0, c_1, c_2, c_3 \in \mathbb{C}$
Es gilt: $|v\rangle$ ist ein Einheitsvektor $\Leftrightarrow |c_0|^2 + |c_1|^2 + |c_2|^2 + |c_3|^2 = 1$
D.h. die Amplitudenquadrate liefern eine Ws-Verteilung.

Messung eines 2-Qubit Systems: Messung von $|v\rangle$ liefert:

- Basiszustand $|00\rangle$ mit $Ws.|c_0|^2$
- Basiszustand $|01\rangle$ mit $Ws.|c_1|^2$
- Basiszustand $|10\rangle$ mit $Ws.|c_2|^2$
- Basiszustand $|11\rangle$ mit $Ws.|c_3|^2$

Nach Messung befindet sich das 2-Qubit System im gemessenen Basiszustand. (Kollaps der Wellenfunktion, irreversibel)

Messung eines einzelnen Qubits eines 2-Qubit Systems: Messung des 1. Qubits von $|1\rangle$ liefert:

- $|0\rangle$ mit $Ws.|c_0|^2 + |c_1|^2$
- $|1\rangle$ mit $Ws.|c_2|^2 + |c_3|^2$

Nach der Messung befindet sich das System im Zustand:

- $\frac{c_0|00\rangle + c_1|01\rangle}{\sqrt{|c_0|^2+|c_1|^2}}$ falls $|0\rangle$ im ersten Qubit gemessen wurde
- $\frac{c_2|10\rangle + c_3|11\rangle}{\sqrt{|c_2|^2+|c_3|^2}}$ falls $|1\rangle$ im ersten Qubit gemessen wurde

Man beachte: $\left|\frac{c_0|00\rangle + c_1|01\rangle}{\sqrt{|c_0|^2+|c_1|^2}}\right| = \frac{1}{\sqrt{|c_0|^2+|c_1|^2}} \cdot |c_0|00\rangle + c_1|01\rangle = \frac{1}{\sqrt{|c_0|^2+|c_1|^2}} \cdot \sqrt{|c_0|^2 + |c_1|^2} = 1$
D.h. der neue Zustand ist wieder ein Einheitsvektor im $\mathbb{C}^4$

5.2 Separabel/Verschränkt

Definition: Wir nennen den Zustand $|z\rangle \in \mathbb{C}^4$ eines 2-Qubit Systems separabel, falls $|z\rangle = |x\rangle \otimes |y\rangle$ für $|x\rangle, |y\rangle \in \mathbb{C}^2$.
Ein Zustand, der nicht separabel ist, heißt verschränkt.

Beispiel (separabler Zustand): $|z\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$ ist separabel
Gesucht: $\alpha_0, \alpha_1, \beta_0, \beta_1 \in \mathbb{C}$ mit $|z\rangle = (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle) = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle$.

Gleichungssystem $\left|\begin{array}{l} \alpha_0\beta_0 = \frac{1}{2} \\ \alpha_0\beta_1 = \frac{1}{2} \\ \alpha_1\beta_0 = \frac{1}{2} \\ \alpha_1\beta_1 = \frac{1}{2} \end{array}\right|$ erfüllt für $\alpha_0 = \beta_0 = \alpha_1 = \beta_1 = \frac{1}{\sqrt{2}}$ (ebenso z.B. für $-\frac{1}{\sqrt{2}}$).

Frage: Wie groß ist die Ws., $|0\rangle$ im 1. Qubit zu messen?
$|z\rangle = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle$

Messung von $|0\rangle$ im 1. Qubit mit Ws.: $|\alpha_0\beta_0|^2 + |\alpha_0\beta_1|^2 = |\alpha_0|^2(\underbrace{|\beta_0|^2 + |\beta_1|^2}_{=1}) = |\alpha_0|^2$

Nach Messung von $|0\rangle$ befindet sich das 2-Qubit System im Zustand
$\frac{\alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle}{\sqrt{|\alpha_0\beta_0|^2+|\alpha_0\beta_1|^2}} = \frac{\alpha_0|0\rangle \otimes (\beta_0|0\rangle + \beta_1|1\rangle)}{\sqrt{|\alpha_0|^2(\underbrace{|\beta_0|^2 + |\beta_1|^2}_{=1})}} = \underbrace{\frac{\alpha_0}{\sqrt{|\alpha_0|^2}}|0\rangle}_{\text{äquivalent zu } |0\rangle} \otimes(\beta_0|0\rangle + \beta_1|1\rangle)$