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
$\frac{\alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle}{\sqrt{|\alpha_0\beta_0|^2+|\alpha_0\beta_1|^2}} = \frac{\alpha_0|0\rangle \otimes (\beta_0|0\rangle + \beta_1|1\rangle)}{\sqrt{|\alpha_0|^2(\underbrace{|\beta_0|^2 + |\beta_1|^2}_{=1})}} = \underbrace{\frac{\alpha_0}{\sqrt{|\alpha_0|^2}}|0\rangle}_{\text{äquivalent zu } |0\rangle} \otimes (\beta_0|0\rangle + \beta_1|1\rangle)$

Analog:
- Mit Ws. $|\alpha_1|^2$ Messung $|1\rangle$ im 1. Qubit. Nach messung: $|1\rangle \otimes (\beta_0|0\rangle + \beta_1|1\rangle)$
- Mit Ws. $|\beta_0|^2$ Messung $|0\rangle$ im 2. Qubit. Nach messung: $(\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes \beta_0|0\rangle)$
- Mit Ws. $|\beta_1|^2$ Messung $|1\rangle$ im 2. Qubit. Nach messung: $(\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes \beta_1|1\rangle)$

Man beachte: Bei separablen 2-Qubit Systemen können die einzelnen Qubits unabhängig voneinander betrachtet werden.

Beispiel (verschränkter Zustand): $|z\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Schreibe $|z\rangle = (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle)$

$$\Rightarrow \text{Gleichungssystem} \left| \begin{array}{c|l} \alpha_0\beta_0 = \frac{1}{\sqrt{2}} & \Rightarrow \alpha_0 \neq 0 \wedge \beta_0 \neq 0 \\ \alpha_0\beta_1 = 0 & \Rightarrow \alpha_1 = 0 \vee \beta_0 = 0 \\ \alpha_1\beta_0 = 0 & \Rightarrow \alpha_1 = 0 \vee \beta_0 = 0 \\ \alpha_1\beta_1 = \frac{1}{\sqrt{2}} & \Rightarrow \alpha_1 \neq 0 \wedge \beta_1 \neq 0 \end{array} \right. \lightning \text{ nicht erfüllbar.}$$

Bezeichnung (EPR Paar): Ein 2-Qubit System im Zustand $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$wird als EPR-Paar (Einstein, Podolsky, Rosen) bezeichnet.

Messung des 1. Qubits eines EPR-Paars liefert: $|0\rangle$ mit $Ws.\frac{1}{2}$, nachher im Zustand $\frac{\frac{1}{\sqrt{2}}|00\rangle}{\frac{1}{\sqrt{2}}} = |00\rangle$.

D.h. aber: Messung des 2. Qubits liefert ebenfalls Null! (Qubits sind abhängig).

Fakt: 2-Qubit Systeme entwickeln sich gemäß unitärer Abbildung $U \in \mathbb{C}^{4\times4}$

Beispiel (CNOT): $M_{\texttt{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{array}{lll} |00\rangle & \mapsto & |00\rangle \\ |01\rangle & \mapsto & |01\rangle \\ |10\rangle & \mapsto & |11\rangle \\ |11\rangle & \mapsto & |10\rangle \end{array}$

Controlled-Not: Das zweite Bit wird genau dann invertiert, wenn das 1. Bit (Kontrollbit) gesetzt ist. Man überprüfe, dass $M_{\texttt{CNOT}} \cdot (M^*_{\texttt{CNOT}})^T = I_2$

Definition: $U \in \mathbb{C}^{m\times m}$ heißt Permutationsmatrix $\Leftrightarrow U$ in jeder Zeile und Spalte genau eine Eins und sonst Nullen erhält.

Beispiel: $M_{\texttt{CNOT}}$ ist Permutationsmatrix.

Übung: Permutationsmatrizen sind unitär.

Bez.: Eine unitäre Abbildung, die nur auf einen Teil der Qubits agiert, heißt <u>lokal</u> unitär.
Sei $|z\rangle = (c_0|00\rangle + c_2|10\rangle + c_3|11\rangle)$ ein 2-Qubit und $A, B \in \mathbb{C}^{2\times2}$ unitär.
$c_0(A|0\rangle \otimes B|0\rangle) + c_1(A|0\rangle + B|1\rangle) + c_2(A|1\rangle + B|0\rangle) + c_3(A|1\rangle + B|1\rangle)$ heißt Anwendung von A auf das 1. Qubit und Anwendung von B auf das 2. Qubit.

Spezialfälle:
- $B = I_2$ liefert eine lokal unitäre Abb. auf dem 1. Qubit
- $A = I_2$ liefert eine lokal unitäre Abb. auf dem 2. Qubit

5.3 Tensorprodukt bzw. Kroneker-Produkt von Matrizen

Definition: Seien

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mm} \end{pmatrix} \in \mathbb{C}^{m\times m}, B = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix} \in \mathbb{C}^{n\times n}$$

Dann ist das Tensorprodukt von A und B definiert als:

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1m}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mm}B \end{pmatrix} \in \mathbb{C}^{mn\times mn}$$

Beispiel:

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}, A \otimes B = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix}$$

Satz: Seien $A, B \in \mathbb{C}^{2\times 2}$ unitär. Ferner sei $|z\rangle \in \mathbb{C}^4$ ein 2-Qubit System. Die Anwendung von A auf das 1. Qubit und B auf das 2. Qubit wird beschrieben durch: $(A \otimes B)|z\rangle$

Beweis: Für $|00\rangle$, andere Basiszustände folgen analog:

$$\begin{aligned}(A\otimes B)|00\rangle &= a_{11}b_{11}|00\rangle + a_{11}b_{21}|01\rangle + a_{21}b_{11}|10\rangle + a_{21}b_{21}|11\rangle\\ &= a_{11}|0\rangle \otimes (b_{11}|0\rangle + b_{21}|1\rangle) + a_{21}|1\rangle \otimes (b_{11}|0\rangle + b_{21}|1\rangle)\\ &= (a_{11}|0\rangle + a_{21}|1\rangle) \otimes (b_{11}|0\rangle + b_{21}|1\rangle)\\ &= A|0\rangle \otimes B|0\rangle\end{aligned}$$

Aus der Linearität von $A \otimes B$ folgt: Gilt obige Identität für alle Basiszustände, so gilt sie auch für alle Linearkombinationen von Basiszuständen.
$\Rightarrow$ Identität gilt für beliebiges $|z\rangle \in \mathbb{C}^4$

Man beachte: Lokal unitäre Abb. auf separablen Zuständen $|z\rangle = |x\rangle \otimes |y\rangle$ liefert stets einen separablen Zustand: $|z\rangle \overset{A\otimes B}{\longmapsto} A|x\rangle \otimes B|y\rangle$.
D.h. lokal unitäre Operationen allein können keine Verschränkung erzeugen.

Beispiel 1: Anwendung von W_2 auf das 1. Qubit: $W_2 \otimes I_2$

$W_2 = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}, I_2 = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$

$W_2 \otimes I_2 = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & -1 & 0\\ 0 & 1 & 0 & -1\end{pmatrix} \quad |00\rangle \mapsto \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) = \underbrace{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)}_{W_2} \otimes |0\rangle$

Beispiel 2: $W_4 = W_2 \otimes W_2$

$$W_4 = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{pmatrix}$$

Zustandsübergang für Basiszustand $|x_0x_1\rangle, x_0, x_1 \in \{0,1\}$:
$W_4|x_0x_1\rangle = \frac{1}{2}(|00\rangle + (-1)^{x_1}|01\rangle + (-1)^{x_0}|10\rangle + (-1)^{x_0+x_1}|11\rangle)$
$= \underbrace{\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_0}|1\rangle)}_{W_2|x_0\rangle} \otimes \underbrace{\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1}|1\rangle)}_{W_2|x_1\rangle}$

Wissen bereits: Nicht jeder 2-Qubit Zustand ist Tensorprodukt zweier 1-Qubit Zustände.
Analog gilt:

Satz: Nicht jede unitäre Abb. $U \in \mathbb{C}^{4\times 4}$ ist Tensorprodukt unitärer Matrizen $A, B \in \mathbb{C}^{2\times 2}$

Beweis: $M_{\texttt{CNOT}}$ ist unitär.

Annahme: $M_{\texttt{CNOT}}$ sei Tensorprodukt zweier unitärer Abbildungen, d.h. $M_{\texttt{CNOT}} = A \otimes B$.
Beachte: $|00\rangle \overset{W_2\otimes I_2}{\longmapsto} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \overset{A\otimes B}{\longmapsto} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
D.h. wir erhalten ein verschränktes EPR-Paar durch lokal unitäre Abbildungen auf dem separablen Zustand $|00\rangle$. $\lightning$ 5.3

5.4 No-Cloning Theorem

Definition (Quanten-Kopiermaschine): Sei $|x\rangle \in \mathbb{C}^2$ ein Qubit. Eine Quanten-Kopiermaschine ist eine unitäre Abbildung U mit: $U(|z\rangle \otimes |x\rangle) = |z\rangle \otimes |z\rangle$ für alle Qubits $|z\rangle \in \mathbb{C}^2$

Satz (No-Cloning Theorem): Es gibt keine Quantenkopiermaschine.

Beweis: Annahme: Es gibt Quanten-Kopiermaschine U. Seien $|0\rangle, |1\rangle$ Basiszustände. Aufgrund der Kopiereigenschaft gilt: $U(W_2|0\rangle \otimes |1\rangle = W_2|0\rangle \otimes W_2|0\rangle$ (ist seperabel).
Aufgrund der Linearität von U gilt aber ebenfalls:
$U(W_2|0\rangle \otimes |1\rangle) = U(\frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle) = \frac{1}{\sqrt{2}}(U|01\rangle + U|11\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ (ist verschränkt, (EPR-Paar)). $\lightning$

Man beachte: $M_{\texttt{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ ist Kopiermaschine für Basiszustände $|0\rangle, |1\rangle$,
denn $|00\rangle \mapsto |00\rangle, |10\rangle \mapsto |11\rangle$.
Allerdings gilt $(\alpha_0|0\rangle + \alpha_1|1\rangle)|0\rangle \overset{M_{\texttt{CNOT}}}{\longmapsto} \alpha_0|00\rangle + \alpha_1|11\rangle \neq (\alpha_0|0\rangle + \alpha_1|1\rangle)(\alpha_0|0\rangle + \alpha_1|1\rangle)$ für $\alpha_0, \alpha_1 \neq 0$.

6 n-Qubit Zustandssysteme (Register)

Sei $|0\rangle$, $|1\rangle$ eine orthonormale Basis des $\mathbb{C}^2$.
Gemäs Basis-Lemma (4.1): $|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle$ ist orthonormale Basis des $\mathbb{C}^4$. Erneute Anwendung des Lemmas liefert eine orthonormale Basis $|b_0 b_1 b_2\rangle, b_i \in \{0,1\}$ des $\mathbb{C}^{2^3}$.
Induktiv: $|b_0 \dots b_{n-1}\rangle, b_i \in \{0,1\}$ ist orthonormale Basis des $\mathbb{C}^{2^n}$.

Definition: Ein n-Qubit System ist ein Einheitsvektor im $\mathbb{C}^{2^n}$ der Form
$|z\rangle = \sum_{x \in \{0,1\}^n} c_x |x\rangle$ mit $c_x \in \mathbb{C}$, $\sum_{x \in \{0,1\}^n} |c_x|^2 = 1$.

Notation: Wir interpretieren $x = x_0 \dots x_{n-1}$ als Binärdarstellung der natürlichen Zahl $\sum_{i=0}^{n-1} x_i 2^{n-1-i}$.
Damit schreiben wir auch $|z\rangle = \sum_{i=0}^{2^n-1} c_i |i\rangle$.

Zustandsübergang:
- n-Qubit Systeme entwickelt sich gemäß unitärer Abb. $U : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$
- Lokal unitäre Abbildungen operieren auf einzelnen Qubits des Systems.

Beobachtung:
- n Qubits werden durch 2^n Amplituden beschrieben.
- Unitäre Matrizen $U \in \mathbb{C}^{2^n \otimes 2^n}$ haben Beschränkungsgröße 2^{2n}.

D.h. die Beschreibungsgröße ist exponentiell in der physikalischen Größe n.
Feyman: "Quantenrechner sollten nicht effizient auf klassischen Rechnern simulierbar sein."

Definition (Separabilität): Ein n-Qubit $|z\rangle \in \mathbb{C}^{2^n}$ heißt separabel gdw. $|z\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \dots \otimes |x_n\rangle$ für $|x_i\rangle \in \mathbb{C}^2$.
Nicht separable Zustände heißen verschränkt.

Beispiel: $|z\rangle = \frac{1}{\sqrt{3}}(|000\rangle - |001\rangle - |111\rangle)$ ist verschränkt.
Messung des 1. Qubits: $|0\rangle$ mit $Ws\frac{2}{3}$, $|0\rangle$ mit $Ws\frac{1}{3}$
Falls:
- $|0\rangle$ gemessen: Zustand $\frac{\frac{1}{\sqrt{3}}(|000\rangle - |001\rangle)}{\sqrt{\frac{2}{3}}} = \frac{1}{\sqrt{2}}(|000\rangle - |001\rangle)$
- $|1\rangle$ gemessen: Zustand $\frac{\frac{1}{\sqrt{3}}|111\rangle}{\sqrt{\frac{1}{3}}} = |111\rangle$.

7 Quanten-Protokolle

7.1 Quantenteleportation

Szenario:
- Alice besitzt Qubit $|z\rangle = c_0|0\rangle + c_1|1\rangle$. Amplituden c_0, c_1 sind Alice unbekannt.
- Alice kann über klassischen Kanal mit Bob kommunizieren (d.h. Bits, keine Qubits)