Man beachte: $U_{cnot} = \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{pmatrix}$ ist Kopiermaschine für Basiszustände $|0\rangle, |1\rangle$, denn

$|00\rangle \mapsto |00\rangle$
$|10\rangle \mapsto |11\rangle$

Allerdings gilt $(\alpha_0|0\rangle + \alpha_1|1\rangle)|0\rangle \xrightarrow{U_{cnot}} \alpha_0|00\rangle + \alpha_1|11\rangle \neq (\alpha_0|0\rangle + \alpha_1|1\rangle)(\alpha_0|0\rangle + \alpha_1|1\rangle)$

für $\alpha_0, \alpha_1 \neq 0$

n-Qubit Zustandssysteme (Register)

Sei $|0\rangle, |1\rangle$ eine orthonormale Basis des $\mathbb{C}^2$.

Gemäß Basis-Lemma (S.6): $|0\rangle\otimes|0\rangle, |0\rangle\otimes|1\rangle, |1\rangle\otimes|0\rangle, |1\rangle\otimes|1\rangle$ 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 $\mathbb{C}^{2^n}$.

Def.: Ein n-Qubit System ist ein Einheitsvektor im $\mathbb{C}^{2^n}$ der Form

$$|z\rangle = \sum_{x \in \{0,1\}^n} c_x |x\rangle \quad \text{mit } c_x \in \mathbb{C}, \ \sum_{x \in \{0,1\}^n} |c_x|^2 = 1$$

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

Zustandsübergang:
- n-Qubit Systeme entwickeln 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 $U \in \mathbb{C}^{2^n \times 2^n}$ haben Beschreibungsgröße 2^{2n}.

D.h. die Beschreibungsgröße ist exponentiell in der physikalischen Größe n.

Feynman: „Quantenrechner sollten nicht effizient auf klassischen Rechnern simulierbar sein"

Def. (Separabilität): Ein n-Qubit $|z\rangle \in \mathbb{C}^{2^n}$ heißt separabel gdw.

$$|z\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \dots \otimes |x_n\rangle \quad \text{für } |x_i\rangle \in \mathbb{C}^2.$$

Nicht separable Zustände heißen verschränkt.

Bsp.: $|z\rangle = \frac{1}{\sqrt{3}}(|000\rangle - |001\rangle - |111\rangle)$ ist verschränkt.

Messung des 1. Qubits: $|0\rangle$ mit Ws $\frac{2}{3}$

$|1\rangle$ 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 $\frac{\frac{1}{\sqrt{3}}|111\rangle}{\sqrt{\frac{1}{3}}} = |111\rangle$

Quanten Teleportation

Szenario: • Alice besitzt Qubit $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$. Amplituden c_0, c_1 sind Alice unbekannt.

• Alice kann über klassischen Kanal mit Bob kommunizieren (d.h. Bits, keine Qubits)

• Alice und Bob teilen sich EPR-Paar $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$; 1. Bit ist Alice, 2. Bit gehört Bob.

Ziel: Alice sendet $|\psi\rangle$ an Bob.

Probleme: • Alice kennt Amplituden nicht.

• Messung zerstört Wellenfunktion.

• Alice kann keine Kopien von $|\psi\rangle$ erzeugen, um Amplituden durch hinreichend viele Messungen zu approximieren. Würde auch nur $|c_0|^2, |c_1|^2$ liefern, nicht c_0, c_1.

• Gibt es einen Algorithmus zur Rekonstruktion von Quantenbits aus klassischer Information, so existiert ein Quanten-Kopierer. ↯ (No Cloning-Theorem)

Lösung: Nutze Verschränkung zur Übertragung.

Zusammengesetzter Zustand von $|\psi\rangle$ und $|e\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$:

$$|\psi\rangle \otimes |e\rangle = (c_0|0\rangle + c_1|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$= \frac{1}{\sqrt{2}}(c_0|000\rangle + c_0|011\rangle + c_1|100\rangle + c_1|111\rangle)$$

Man beachte: Alice hat Zugriff auf die ersten beiden Qubits, Bob auf das 3. Qubit.

Protokoll für die Teleportation von $|\psi\rangle$

1. Alice wendet CNOT auf das 2. Qubit mit dem 1. Qubit als Kontrollbit an:

$$|\psi e\rangle \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}(c_0|000\rangle + c_0|011\rangle + c_1|110\rangle + c_1|101\rangle)$$

2. Alice wendet nun auf das 1. Qubit die Hadamard-Walsh Transformation W_2 an:

$$\frac{1}{\sqrt{2}}\left(\frac{c_0}{\sqrt{2}}(|0\rangle + |1\rangle)|00\rangle + \frac{c_0}{\sqrt{2}}(|0\rangle + |1\rangle)|11\rangle + \frac{c_1}{\sqrt{2}}(|0\rangle - |1\rangle)|10\rangle + \frac{c_1}{\sqrt{2}}(|0\rangle + |1\rangle)|01\rangle\right)$$

$$= \frac{1}{2}\left(c_0|000\rangle + c_0|100\rangle + c_0|011\rangle + c_0|111\rangle + c_1|010\rangle - c_1|110\rangle + c_1|001\rangle - c_1|101\rangle\right)$$

$$= \frac{1}{2}\left(|00\rangle(c_0|0\rangle + c_1|1\rangle) + |01\rangle(c_0|1\rangle + c_1|0\rangle) + |10\rangle(c_0|0\rangle - c_1|1\rangle) + |11\rangle(c_0|1\rangle - c_1|0\rangle)\right)$$

3. Alice misst die ersten beiden Qubits. Sie erhält jeweils mit Ws. $\frac{1}{4}$

Qubit	Zustand nach Messung
$\|00\rangle$	$\|00\rangle(c_0\|0\rangle + c_1\|1\rangle)$
$\|01\rangle$	$\|01\rangle(c_0\|1\rangle + c_1\|0\rangle)$
$\|10\rangle$	$\|10\rangle(c_0\|0\rangle - c_1\|1\rangle)$
$\|11\rangle$	$\|11\rangle(c_0\|1\rangle - c_1\|0\rangle)$

Alice sendet Messergebnis 00, 01, 10 oder 11 zu Bob.

4 Abhängig vom Messergebnis führt Bob folgende Operation aus.

Für $|00\rangle$: Bobs Qubit ist bereits im gewünschten Zustand.

$|01\rangle$: NOT Operation $c_0|1\rangle + c_1|0\rangle \xmapsto{\text{NOT}} c_0|0\rangle + c_1|1\rangle$

$|10\rangle$: Flip Operation $c_0|0\rangle - c_1|1\rangle \xmapsto{\text{Flip}} |c_0|0\rangle + c_1|1\rangle$

$|11\rangle$: Flip ∘ NOT $c_0|1\rangle - c_1|0\rangle \xmapsto{\text{Flip}\circ\text{NOT}} |c_0|0\rangle + c_1|1\rangle$

Beobachtung: · Alices Zustand $|\psi\rangle$ wird übertragen, nicht kopiert.
· Es wird nur der Zustand übertragen, kein physikalisches Qubit.
· Bob benötigt Alices Messung, um $|\psi\rangle$ zu erhalten.

Superdense Coding (Bennett, Wiesner 1992)

Szenario: · Alice und Bob teilen sich ein EPR $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
· Alice & Bob besitzen einen Quantenkanal zum Übertragen von Qubits.

Ziel: Übertrage zwei klassische Bits b_0, b_1 mit Hilfe eines einzelnen Qubits.

Protokoll Superdense Coding

1. Abhängig von b_0, b_1 berechnet Alice:
Falls $b_0 = 1$: Flip auf 1. Qubit
Falls $b_1 = 1$: NOT auf 1. Qubit

b_0	b_1	Zustand
0	0	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$
0	1	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$
1	0	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$
1	1	$\frac{1}{\sqrt{2}}(\|10\rangle - \|01\rangle)$

Alice sendet $|\psi\rangle$ an Bob.