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 <u>Basiszustände</u> $|0\rangle, |1\rangle$,
denn $|00\rangle \mapsto |00\rangle, |10\rangle \mapsto |11\rangle$.
Allerdings gilt $(\alpha_0|0\rangle + \alpha_1|1\rangle)|0\rangle \xmapsto{M_{\texttt{CNOT}}} \alpha_0|00\rangle + \alpha_1|11\rangle \neq (\alpha_0|0\rangle + \alpha_1|1\rangle)(\alpha_0|0\rangle + \alpha_1|1\rangle)$ für $\alpha_0, \alpha_1 \neq 0$.

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
$|z\rangle = \sum\limits_{x \in \{0,1\}^n} c_x|x\rangle$ mit $c_x \in \mathbb{C}$, $\sum\limits_{x \in \{0,1\}^n} |c_x|^2 = 1$.

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

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. $|z\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle$ 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: $\begin{matrix} |0\rangle \text{ mit } Ws\frac{2}{3} \\ |0\rangle \text{ mit } Ws\frac{1}{3} \end{matrix}$
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)

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

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

Probleme:
- Alice kennt Amplituden nicht.
- Messung zerstört Wellenfunktion.
- Alice kann keine Kopien von $|z\rangle$ 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 Rekonstrutkion von Quantenbits aus klassischer Information, so existiert ein Quanten-Kopierer. $\lightning$ (No-Cloning-Theorem (5.4))

Lösung: Nutze Verschränkung zur Übertragung.
Zusammengesetzter Zustand von $|z\rangle$ und $|e\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$:

$$\begin{aligned}|z\rangle \otimes |e\rangle &= (c_0|0\rangle + c_1|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\\ &= \frac{1}{\sqrt{2}}(c_0|000\rangle + c_0|011\rangle + c_1|100\rangle + c_1|111\rangle)\end{aligned}$$

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

Protokoll für die Teleportation von $|z\rangle$:

1. Alice wendet CNOT auf das 2. Qubit mit dem 1. Qubit als Kontrollbit an:
   $|ze\rangle \overset{\texttt{CNOT}}{\longmapsto} \frac{1}{\sqrt{2}}(c_0|000\rangle + c_0|011\rangle + c_1|110\rangle + c_1|101\rangle)$
2. Alice wendet nun auf das 1. Qubit die Hadamard-Walsh Transformation W_2 an:
   $\frac{1}{\sqrt{2}}(\frac{c_0}{\sqrt{2}}(|0\rangle + |1\rangle)|00\rangle + \frac{c_0}{\sqrt{2}}(|0\rangle + |1\rangle)|11\rangle + \frac{c_1}{\sqrt{2}}(|0\rangle - |1\rangle)|10\rangle + \frac{c_1}{\sqrt{2}}(|0\rangle - |1\rangle)|01\rangle)$
   $= \frac{1}{2}(c_0|000\rangle + c_0|100\rangle + c_0|011\rangle + c_0|111\rangle + c_1|010\rangle - c_1|110\rangle + c_1|001\rangle - c_1|101\rangle)$
   $= \frac{1}{2}(|00\rangle(c_0|0\rangle + c_1|1\rangle) + |01\rangle(c_0|1\rangle + c_1|0\rangle) + |10\rangle(c_0|0\rangle - c_1|1\rangle) + |11\rangle(c_0|1\rangle - c_1|0\rangle))$
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 an Bob.
4. Abhängig von Messergebnis führt Bob folgende Operation aus:
   Für $|00\rangle$: Bobs Qubit ist bereits im gewünschten Zustand.
   $|01\rangle$ NOT Operation $c_0|1\rangle + c_1|0\rangle \overset{\texttt{NOT}}{\longmapsto} c_0|0\rangle + c_1|1\rangle$
   $|10\rangle$ Flip Operation: $c_0|0\rangle - c_1|1\rangle \overset{\texttt{Flip}}{\longmapsto} c_0|0\rangle + c_1|1\rangle$
   $|11\rangle$ Flip $\circ$ NOT $c_0|1\rangle - c_1|0\rangle \overset{\texttt{Flip} \circ \texttt{NOT}}{\longmapsto} c_0|0\rangle + c_1|1\rangle$

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

7.2 Superdense Coding (Bennet, Wiesner 1992)

Szenario:
- Alice und Bob teilen sich ein EPR-Paar $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- 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 Codding:

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	$\frac{1}{\sqrt{2}}(\lvert 00\rangle + \lvert 11\rangle)$
0	1	$\frac{1}{\sqrt{2}}(\lvert 10\rangle + \lvert 01\rangle)$
1	0	$\frac{1}{\sqrt{2}}(\lvert 00\rangle - \lvert 11\rangle$
1	1	$\frac{1}{\sqrt{2}}(\lvert 10\rangle - \lvert 01\rangle$

   Alice sendet $|z\rangle$ an Bob.
2. Bob wendet die folgende unitäre Matrix U auf $|z\rangle$ an.
   $$U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \end{pmatrix}$$
   $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \xmapsto{U} \frac{1}{2}(|00\rangle + |10\rangle + |00\rangle - |10\rangle) = |00\rangle$ Interpretation: $(b_0, b_1) = (0, 0)$
   $\frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \xmapsto{U} \frac{1}{2}(|00\rangle + |10\rangle - |00\rangle + |10\rangle) = |01\rangle$ Interpretation: $(b_0, b_1) = (0, 1)$
   $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \xmapsto{U} \frac{1}{2}(|00\rangle + |10\rangle - |00\rangle + |10\rangle) = |10\rangle$ Interpretation: $(b_0, b_1) = (1, 0)$
   $\frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \xmapsto{U} \frac{1}{2}(-|01\rangle + |11\rangle + |01\rangle + |11\rangle) = |11\rangle$ Interpretation: $(b_0, b_1) = (1, 1)$

7.3 Quanten Schlüsselaustausch

One-Time Pad für n-Bit Nachricht $m = m_1 m_2 \dots m_n \in \{0,1\}^n$

$$\boxed{\text{Alice } (SK = k_1 \dots k_n \in \{0,1\}^n)} \xrightarrow{E_{SK}(m) = m \oplus SK} \boxed{\text{Bob } (SK = k_1 \dots k_n \in \{0,1\}^n)}$$

$D_{SK}(E_{SK}(m)) = E_{sk}(m) \oplus SK = m \oplus SK \oplus SK = m$

Szenario:
- Alice und Bob besitzen Quantenkanal
- Alice und Bob besitzen authentisierten klassischen Kanal
- Kanäle werden belauscht und manipuliert durch Eve.

Ziel: Austausch von n klassischen Bits, so dass

- Eve durch Belauschen keine Information erhält
- Manipulation von Eve entdeckt wird

Einfache Lösung: falls Alice und Bob n EPR-Paare $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$teilen:
Messen in derselben Basis $|0\rangle$, $|1\rangle$ liefert n identische Zufallsbits.

Definition(Z und X-Basis): Wir nennen $|0\rangle$, $|1\rangle$ die Z-Basis des $\mathbb{C}^2$
Die Basis $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, die durch Anwendung von W_2 auf die Basisvektoren der Z-Basis entsteht, bezeichnen wir als X-Basis.

Beobachtung:
- Messung von $\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ in Z-Basis liefert $|0\rangle$, $|1\rangle$ jeweils mit $Ws. \frac{1}{2}$.
- Messung von $|0\rangle$ oder $|1\rangle$ in X-Basis liefert $\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ jeweils mit $Ws. \frac{1}{2}$.