No-Cloning Theorem

Eine "Klonungsmaschine" wäre

für beliebiges $|\psi\rangle$

mit $\hat{K}$ = unitärer Operator. Es gibt $\hat{K}$'s, die bestimmte Zustände klonen, z.B $|\psi\rangle = |0\rangle$ könnte mit $\hat{K} = \hat{1}$ geklont werden.

Aber man kann zeigen, dass ein Operator $\hat{K}$, der ein bestimmtes $|\psi_0\rangle$ klonen kann, keine Zustände $|\phi\rangle \neq |\psi_0\rangle$ klonen kann, die nicht orthogonal zu $|\psi_0\rangle$ sind (also solche für die $\langle\phi|\psi_0\rangle \neq 0$).

Beweis:
$$\hat{K}|\psi_0 0\rangle = |\psi_0\psi_0\rangle$$
$$\hat{K}|\phi 0\rangle = |\phi\phi\rangle$$

Inneres Produkt (unter Ausnutzung von $\hat{K}^\dagger\hat{K} = \hat{1}$)

$$\langle\phi 0|\psi_0 0\rangle = \langle\phi\phi|\psi_0\psi_0\rangle$$
$$\langle\phi|\psi_0\rangle = \left(\langle\phi|\psi_0\rangle\right)^2 \qquad (\text{weil } \langle 0|0\rangle = 1)$$

$\Rightarrow$ entweder $\langle\phi|\psi_0\rangle = 0$ oder $\langle\phi|\psi_0\rangle = 1$

↳ $|\phi\rangle \perp |\psi_0\rangle$ ↳ $|\phi\rangle = |\psi_0\rangle$

□

Bem.: Wenn der Zustand $|\psi\rangle$ bekannt ist, dann kann man ihn natürlich ein zweites mal herstellen, aber das ist kein Klonen. Beim No-cloning Theorem geht es um <u>unbekannte</u> Zustände

Aber: Einen unbekannten Zustand kann man zwar nicht klonen, aber man kann ihn <u>teleportieren</u>.

Quantenteleportation

Alice habe ein Qubit (z.B. ein Spin-$\frac{1}{2}$-Teilchen) im (unbekannten) Zustand $|\psi\rangle$. Bob habe auch ein Qubit und möchte seinen in denselben Zustand $|\psi\rangle$ versetzen. Was dabei mit Alices Qubit passiert ist den beiden egal. (Er kann sicherlich nicht im Zustand $|\psi\rangle$ verbleiben, denn das widerspräche dem No-Cloning-Theorem.)

Lösung: Alices Qubit $|\psi\rangle = a|0\rangle + b|1\rangle$

Alice und Bob haben zusätzlich noch ein verschränktes Qubit-Paar $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$

Gesamtsystem: $|\psi_{tot}\rangle = |\psi\rangle|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle\right)$

Wende kontrolliertes-Nicht auf das mittlere Qubit an mit dem ersten Qubit als Kontrollbit:

$$|\psi_{tot}\rangle' = \text{CNOT}\,|\psi_{tot}\rangle$$

$$= \frac{1}{\sqrt{2}}\left(a|000\rangle + a|011\rangle + b|110\rangle + b|101\rangle\right)$$

Wende Hadamard auf das erste Qubit an

$$|\psi_{tot}\rangle'' = H\,|\psi_{tot}\rangle'$$

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

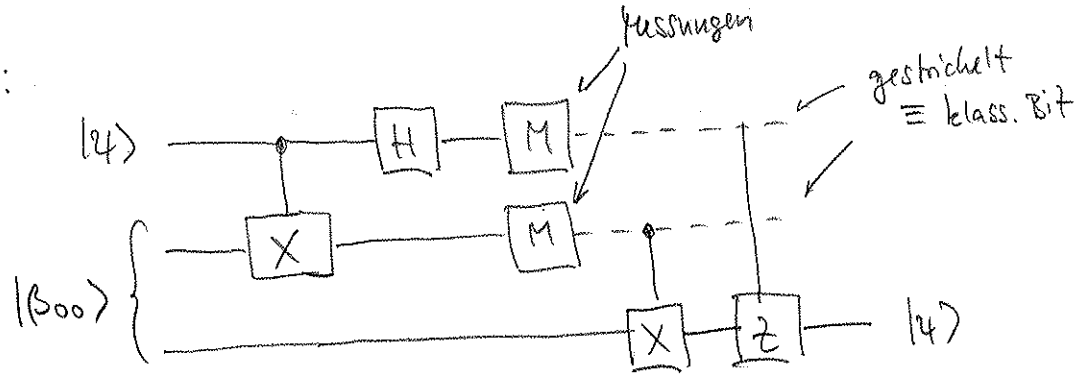
Dies läßt sich schreiben als

$$|\Psi_{tot}\rangle'' = \frac{1}{2}\Big[|00\rangle\big(a|0\rangle + b|1\rangle\big) + |01\rangle\big(a|1\rangle + b|0\rangle\big) + |10\rangle\big(a|0\rangle - b|1\rangle\big) + |11\rangle\big(a|1\rangle - b|0\rangle\big)\Big]$$

Nun misst Alice die ersten zwei Qubits (quasi $\hat{S}_{1,z}\hat{S}_{2,z}$)

Falls sie 00 misst, sagt sie zu Bob: „Mache nichts"
01 „Wende X an"
10 „Wende Z an"
11 „Wende XZ an"

Insgesamt:



Dieses Protokoll erfordert die Übertragung von 2 klassischen Bits Information, um ein Qubit zu teleportieren. Diese Tatsache bedeutet u.a., dass die Kausalität bewahrt bleibt. (Keine instantane Teleportation möglich.)

Theoretische Idee: 1993 Bennett, Brassard, Crépeau, Jozsa, Peres und Wootters

Erste Umsetzung: 1997 in Innsbruck, Zeilinger et al, ≈ 1m weit (Photonen)

2004 600m über die Donau

Rekord: 2012 143 km zu den kanarischen Inseln La Palma & Tenerife.

Bell-Zustände

Verschränkte Zustände spielen in der Quanteninformatik eine zentrale Rolle. Wir kennen schon zwei Basen für den Hilbertraum zweier Spins $\hat{=}$ Qubits:

Produktbasis $\{ |00\rangle, |01\rangle, |10\rangle, |11\rangle \}$ — 0 = up, 1 = down

Gesamtspinbasis $\{ |0,0\rangle, |1,1\rangle, |1,0\rangle, |1,-1\rangle \}$ — $|l,m\rangle$

Nun führen wir eine Basis aus verschränkten Zuständen ein:

Bell-Basis $\{ |\beta_{00}\rangle, |\beta_{01}\rangle, |\beta_{10}\rangle, |\beta_{11}\rangle \}$

mit
$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$
$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle)$$
$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle)$$
$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle)$$

Alle drei Basen sind gleichwertig zur Beschreibung der Zustände in $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ und können durch unitäre Transformationen aufeinander abgebildet werden. Die Bell-Basis ist aber in der Hinsicht besonders, dass man jeden der Basis-Zustände in jeden anderen überführen kann durch eine Transformation, die nur auf $\mathcal{H}_1$ wirkt (oder nur auf $\mathcal{H}_2$). Diese Eigenschaft macht man sich in der "dichten Kodierung" zunutze $\Rightarrow$ siehe Übungsblatt 8.

Deutsch-Algorithmus

(David Deutsch, * 1953 Israel, jetzt England)

Eine Münze hat zwei Seiten.
Gültige Münze: eine Seite 0 (Kopf), eine Seite 1 (Zahl)
Ungültige Münze: beide Seiten 0 oder beide Seiten 1.

Eine Münze kann durch eine Funktion $f: \{0,1\} \longrightarrow \{0,1\}$ repräsentiert werden.

Vorderseite, Rückseite, Kopf, Zahl

Es gibt 4 Typen von Münzen / Funktionen

	Vorderseite	Rückseite	
M_1	Kopf	Kopf	ungültig
M_2	Kopf	Zahl	gültig
M_3	Zahl	Kopf	gültig
M_4	Zahl	Zahl	ungültig

$\Longleftrightarrow$

	0	1	
f_1	0	0	konstant
f_2	0	1	balanciert
f_3	1	0	balanciert
f_4	1	1	konstant

bedeutet: gleich oft 0 wie 1

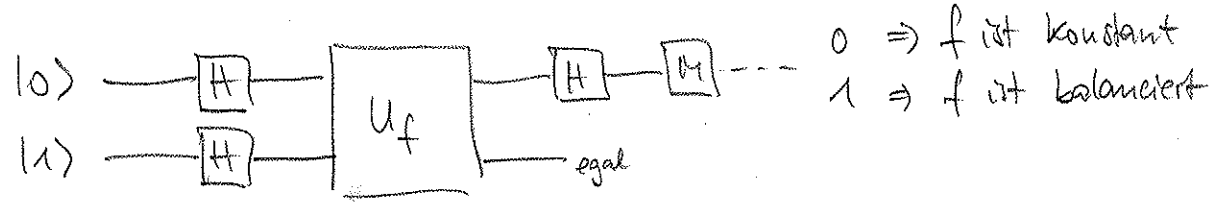
Zu bestimmen, ob eine Münze gültig ist, ist äquivalent dazu, zu bestimmen, ob eine Funktion $f: \{0,1\} \longrightarrow \{0,1\}$ balanciert ist. Klassisch muss man sich beide Seiten der Münze anschauen bzw. f <u>zweimal</u> aufrufen, um die Antwort zu finden. Der Deutsch-Algorithmus ist ein Protokoll für einen Quantenalgorithmus, der die Antwort mit nur <u>einem</u> Funktionsaufruf findet.

Zunächst bauen wir uns aus der Funktion f eine unitäre Transformation, die wir auf Qubits loslassen können. (Die Funktion f kann nur auf klassische Bits wirken. Man bedenke beispielsweise, dass ein konstantes f nicht umkehrbar ist.) Sei nun

$$U_f(x,y) := |x, y \oplus f(x)\rangle$$

$\oplus$ steht für XOR, bzw für "$+ \bmod 2$".

Der Algorithmus ist folgender



Beachte: U_f wird nur 1x aufgerufen!

Warum funktioniert's? Sei $|\psi_0\rangle = |01\rangle$ der Anfangszustand.

Dann

$$|\psi_1\rangle = (H \otimes H)|\psi_0\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$$

$$= \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

$$|\psi_2\rangle = U_f(|\psi_1\rangle) = \frac{1}{2}\Big[|0, \underbrace{0\oplus f(0)}_{f(0)}\rangle - |0, 1\oplus f(0)\rangle + |1, \underbrace{0\oplus f(1)}_{f(1)}\rangle - |1, 1\oplus f(1)\rangle\Big]$$

$$= \frac{1}{2}\Big[|0\rangle\underbrace{(|f(0)\rangle - |1\oplus f(0)\rangle)}_{\text{haben die Form } |f(x)\rangle - |1\oplus f(x)\rangle} + |1\rangle\underbrace{(|f(1)\rangle - |1\oplus f(1)\rangle)}_{\text{haben die Form } |f(x)\rangle - |1\oplus f(x)\rangle}\Big]$$

Nun gilt aber falls $|f(x)\rangle = |0\rangle$, dann $|1 \oplus f(x)\rangle = |1\rangle$

falls $|f(x)\rangle = |1\rangle$, dann $|1 \oplus f(x)\rangle = |0\rangle$

Das heißt $|f(x)\rangle - |1 \oplus f(x)\rangle$ ist in jedem Fall proportional zur Differenz aus $|0\rangle$ und $|1\rangle$, und nur das globale Vorzeichen hängt von $f(x)$ ab.

$$|f(x)\rangle - |1 \oplus f(x)\rangle = (-1)^{f(x)} \left[|0\rangle - |1\rangle \right]$$

Damit haben wir

$$|\psi_2\rangle = \frac{1}{2} \left[(-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle \right] \left[|0\rangle - |1\rangle \right]$$

Würden wir jetzt das erste Qubit messen, dann bekämen wir für egal welches f 50% $|0\rangle$ und 50% $|1\rangle$ ohne dabei irgendetwas über f gelernt zu haben. Ganz anders ist die Situation, wenn wir vorher ein Hadamard-Gatter auf das erste Qubit, also auf $|\psi_2\rangle_1 := \frac{1}{\sqrt{2}} \left((-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle \right)$, anwenden.

$$\begin{aligned} H |\psi_2\rangle_1 &= \frac{1}{2} \left[(-1)^{f(0)} \left(|0\rangle + |1\rangle \right) + (-1)^{f(1)} \left(|0\rangle - |1\rangle \right) \right] \\ &= \frac{1}{2} \left[\left((-1)^{f(0)} + (-1)^{f(1)} \right) |0\rangle + \left((-1)^{f(0)} - (-1)^{f(1)} \right) |1\rangle \right] \\ &= \begin{cases} \pm |0\rangle & \text{für } f(0) = f(1) \quad \text{(konstant)} \\ \pm |1\rangle & \text{für } f(0) \neq f(1) \quad \text{(balanciert)} \end{cases} \end{aligned}$$

Wenn wir <u>jetzt</u> das erste Qubit messen, dann können wir schließen

$|0\rangle \Rightarrow$ f ist konstant (Münze ungültig)

$|1\rangle \Rightarrow$ f ist balanciert (Münze gültig)

□

Komplexität

Die Schwierigkeit von Problemen wird definiert als die Laufzeit von Algorithmen (Programmen), die diese Probleme lösen. Schritte, die nur eine konstante Anzahl Male durchlaufen werden müssen, sind dabei nicht so relevant. Ins Gewicht fallen Schleifen und Rekursionen. (vgl. klassische Fünfte 2x hinschauen, Deutsch-Algorithmus 1x hinschauen.)

Jedes Problem hat eine Eingabe. Sei die Größe der Eingabe charakterisiert durch die Anzahl Bits/Qubits N, die man benötigt um die Eingabe anzugeben. Dann interessieren wir uns für das asymptotische Wachstum der Laufzeit als Funktion von N.

* Suche in einer unsortierten Liste mit $M \sim 2^N$ Einträgen
  - klassisch $\sim e^N \sim M$
  - Quantenalgorithmus nach Grover $\sim e^{N/2} \sim \sqrt{M}$

* Faktorisierung von Zahlen der Größe $n \sim 2^N$
  - klassisch (naiv) $\sim \sqrt{n} \sim e^{N/2}$
  - Quantenalgorithmus nach Shor $\sim N^3$

Literatur: Matthias Homeister: Quanten Computing verstehen.