Messungen in verschiedenen Basen

Messung am Qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ führt das Qubit über in ein klassisches, nicht quantenmechanisches Bit, mit Wahrscheinlichkeit $|\alpha|^2$ Zustand $|0\rangle$ oder Wahrsch. $|\beta|^2$ in Zustand $|1\rangle$. Wie erwartet kann man mit einer Messung α und β nicht bestimmen, aber Messung in verschiedenen Basen erlaubt etwas Flexibilität:

Basiswechsel
$$\left.\begin{aligned} |+\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \\ |-\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \end{aligned}\right\} \left\{\begin{aligned} |0\rangle &= \frac{1}{\sqrt{2}}\left(|+\rangle + |-\rangle\right) \\ |1\rangle &= \frac{1}{\sqrt{2}}\left(|+\rangle - |-\rangle\right) \end{aligned}\right. \qquad (35)$$

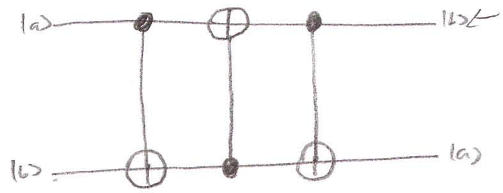
behandle nun $|\pm\rangle$ als neue Rechen bzw. Messbasis. Dabei gilt:
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha\frac{|+\rangle + |-\rangle}{\sqrt{2}} + \beta\frac{|+\rangle - |-\rangle}{\sqrt{2}} = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle \qquad (36)$$

d.h. Messung in der $|\pm\rangle$ Basis ergibt
$$\begin{aligned} &|+\rangle \text{ mit Wahrsch. } |\alpha+\beta|^2/2 \\ &|-\rangle \text{ mit Wahrsch. } |\alpha-\beta|^2/2 \end{aligned} \qquad (37)$$

mit den entsprechenden Zuständen nach Messung (post-measurement) $|+\rangle$ oder $|-\rangle$. Dies gilt allgemein für eine beliebige orthonormale Basis $|a\rangle, |b\rangle$, und analog auch für mehr als 1 Qubit. (möglich heisst aber nicht, dass es in Experimenten einfach durchzuführen ist.)

Quantenschaltkreise

Bsp.



← Linien repräsentieren Qubits, nicht Drähte

addition Modulo 2 (oder XOR)

„SWAP" gate $\quad |a,b\rangle \to |a, a\oplus b\rangle$

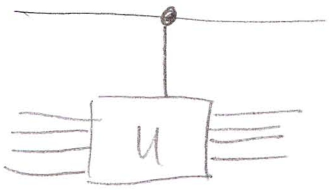
$a \oplus a = 0$ / $0 \oplus b = b$

d.h. Zustände werden vertauscht.
$$\begin{aligned} &\to |a\oplus(a\oplus b), a\oplus b\rangle = |b, a\oplus b\rangle \\ &\to |b, (a\oplus b)\oplus b\rangle = |b, a\rangle \end{aligned} \qquad (38)$$

Im Vergleich zu konventionellen Schaltkreisen sind beim Quantenrechner folgende Operationen nicht möglich:

- Loops / feedback.
- FANIN (Verbindung zweier Linien mit OR) → nicht reversibel
- FANOUT (Verdopplung einer Linie) mit QM das Kopieren eines Zustandes nicht erlaubt (siehe „no-cloning" Theorem weiter unten)

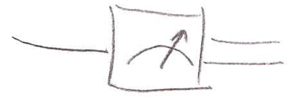
Wir werden im Kommenden weitere quanten Gates U (unitär) einführen wo nötig. Daraus lässt sich ein controlled-U definieren, was eine natürliche Erweiterung des controlled-NOT gates ist, mit einem control Qubit und n target qubits. Falls das control Qubit 0 ist passiert mit den andern Qubits nichts, andernfalls wird U angewandt.



z.B. CNOT:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad (39)$$

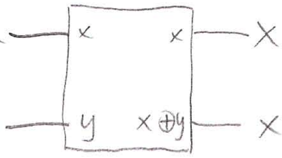
Messung:



Diese Quantenschaltkreise sind einerseits nützlich für die Veranschaulichung von Quantenrechnungen, andererseits aber auch für quantum communication, quantum noise und manchmal für das Verständnis von Experimenten

Kopieren eines Quantenmechanischen Zustandes

klassisch möglich, mit CNOT:



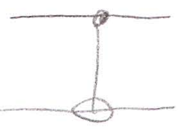
(40)

versuchen wir analoges quantenmechanisch:

allg. Überlagerungszustand

$|\psi\rangle = a|0\rangle + b|1\rangle$

$|0\rangle$



$a|00\rangle + b|11\rangle$ (41)

Eingangszustand: $\{a|0\rangle + b|1\rangle\}|0\rangle = a|00\rangle + b|10\rangle$

Ausgangszustand

Eine quan Kopie des Zustands $|\psi\rangle$ wäre aber $|\psi\rangle|\psi\rangle$

$$|\psi\rangle|\psi\rangle = a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle \qquad (42)$$

d.h. der Ausgangszustand (41) ist <u>keine</u> Kopie von $|\psi\rangle$. (als allg. Überlagerungszustand)

falls aber $|\psi\rangle = |0\rangle$ $(b=0)$ oder $|\psi\rangle = |1\rangle$ $(a=0)$ dann ist (41) eine Kopie.

(„<u>no-cloning</u>" Theorem)

nun zeigen wir allgemein, dass es <u>nicht</u> möglich ist, den quan Zustand $|\psi\rangle$ zu kopieren.

No cloning Theorem

quantum state cloning device:

$$|\psi\rangle \otimes |s\rangle \xrightarrow{U} U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle \qquad (43)$$

cloning Operation

wobei $|s\rangle$ ein „reines" Zustand ist (kein Überlagerungs Zustand).

Beh. Es ist unmöglich, $|\psi\rangle$ zu kopieren in $|\psi\rangle|\psi\rangle$. (cloning) (44)

Bew. Wir nehmen an, cloning sei möglich und führen ad absurdum.
Nehme zwei reine Zustände $|\psi\rangle$ und $|\varphi\rangle$ und klone:

$$|\psi\rangle \longrightarrow U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle \qquad (45)$$

$$|\varphi\rangle \longrightarrow \underbrace{U(|\varphi\rangle \otimes |s\rangle) = |\varphi\rangle \otimes |\varphi\rangle}_{} \qquad (46)$$

nehme das innere Produkt dieser Gleichungen.

linke Seite: $\langle s| \otimes \langle\psi| \underbrace{U^+ U}_{1} |\varphi\rangle \otimes |s\rangle = \langle\psi|\varphi\rangle\langle s|s\rangle = \langle\psi|\varphi\rangle$ (47)

rechte Seite: $(\langle\psi| \otimes \langle\psi|)(|\varphi\rangle \otimes |\varphi\rangle) = \langle\psi|\varphi\rangle\langle\psi|\varphi\rangle = (\langle\psi|\varphi\rangle)^2$

$LS = RS$: $\langle\psi|\varphi\rangle = (\langle\psi|\varphi\rangle)^2 \rightarrow x = x^2$ (48)

$\rightarrow x = 0$ oder $x = 1$

d.h. entweder $|\varphi\rangle$ und $|\psi\rangle$ orthogonal $(\langle\psi|\varphi\rangle = 0)$
oder $|\psi\rangle = |\varphi\rangle$ $(\langle\psi|\varphi\rangle = 1)$ (49)

$\Rightarrow$ diese „cloning" Maschine kann nur Zustände, die orthogonal sind, klonen, aber nicht beliebige, verschiedene Eingangszustände.

(z.B. können $|\psi\rangle = |0\rangle$ und $|\varphi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ nicht geklont werden)

Maschine soll aber für jedes beliebige $|\psi\rangle$ funktionieren $\rightarrow$ Widerspruch! ∎

D.h. mit einer unitären Operation kann man keinen bel. Quantenzustand klonen.
(wohl aber klassische Zustände, z.B. $|0\rangle$ oder $|1\rangle$)

Warum soll die klone Operation unitär sein? QM ist unitär, und selbst wenn nicht-unitäre Operationen zugelassen werden, können nicht-orthog Zustände nicht ohne Verluste kopiert werden!

Beispiel: Bellsche Zustände

Schauen wir uns eine etwas kompliziertere Operation an:

$|\beta_{xy}\rangle$ (50)

mit $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ Hadamard gate.

Bsp. $|00\rangle \xrightarrow{H} \underbrace{(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}|0\rangle}_{\text{Superpos.}} \xrightarrow{CNOT} (|00\rangle + |11\rangle)\frac{1}{\sqrt{2}}$

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

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \qquad (51)$$

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

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

Bellsche Zustände, erzeugt durch (53) aus reinen Zuständen

$$|\beta_{xy}\rangle = \frac{|0,y\rangle + (-1)^x |1,\bar{y}\rangle}{\sqrt{2}} \qquad (52)$$

Logiktabelle:

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

(53)

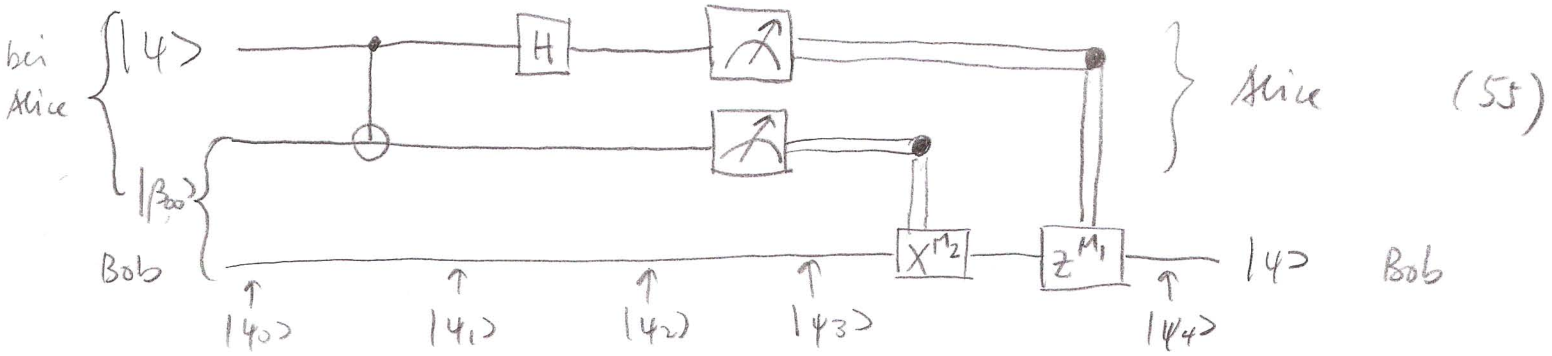
Quanten Teleportation

Zustände können zwar nicht kopiert werden, aber verschieben/übermitteln (mit Zerstörung des Originals) ist möglich.

Setup: Alice / Bob weit voneinander entfernt, haben aber je ein Teilchen eines EPR Paares. Alice's Aufgabe: sende $|\psi\rangle$ Zustand zu Bob, Alice kann aber nur klassische Information übermitteln. (54)

- Alice kennt $|\psi\rangle$ nicht
- kann somit $|\psi\rangle$ nicht bestimmen (hat nur $|\psi\rangle$ und kann nicht kopieren)
- selbst wenn Alice $|\psi\rangle$ genau kennen würde: ist unendlich viel Information, übermittlung klassisch dauert ∞ lange.

Lösung?



(55)

Sei $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ $\qquad \alpha, \beta$ unbekannt (56)

Zustand beim Input:
$$|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left\{\alpha\underset{\text{Alice}}{|0\rangle}\left(|0\overset{\text{Bob}}{0}\rangle + |11\rangle\right) + \beta|1\rangle\left(|00\rangle + |11\rangle\right)\right\} \tag{57}$$

nach CNOT:
$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left\{\alpha|0\rangle\left(|00\rangle + |11\rangle\right) + \beta|1\rangle\left(|10\rangle + |01\rangle\right)\right\} \tag{58}$$

nach Hadamard:
$$|\psi_2\rangle = \frac{1}{2}\left\{\alpha\left(|0\rangle+|1\rangle\right)\left(|00\rangle+|11\rangle\right) + \beta\left(|0\rangle-|1\rangle\right)\left(|10\rangle+|01\rangle\right)\right\} \tag{59}$$
$$= \frac{1}{2}\left\{|00\rangle\left(\alpha|0\rangle+\beta|1\rangle\right) + |01\rangle\left(\alpha|1\rangle+\beta|0\rangle\right) + |10\rangle\left(\alpha|0\rangle-\beta|1\rangle\right) + |11\rangle\left(\alpha|1\rangle-\beta|0\rangle\right)\right\}$$

Sind 4 Terme $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ (die beiden Qubits bei Alice.) Alice misst nun beide.

falls sie	$\lvert 00\rangle$ erhält:	Bob hat	$\alpha\lvert 0\rangle + \beta\lvert 1\rangle$, d.h. $\lvert\psi\rangle$
falls sie	$\lvert 01\rangle$ erhält:	Bob hat	$\alpha\lvert 1\rangle + \beta\lvert 0\rangle$
	$\lvert 10\rangle$:		$\alpha\lvert 0\rangle - \beta\lvert 1\rangle$
	$\lvert 11\rangle$		$\alpha\lvert 1\rangle - \beta\lvert 0\rangle$

(60)

Bob erhält einen dieser vier Zustände, abhängig davon, was Alice's Messung ergeben hat.

Alice teilt nun Bob das Resultat ihrer Messung über den klassischen Kanal mit. Bob „repariert" abhängig davon sein $|\psi\rangle$

Falls Messung ergab: $|00\rangle$ schon erledigt, Bob hat $|\psi\rangle$

$$\begin{aligned} |01\rangle &: \quad X\text{-gate} \quad \left(X=\begin{pmatrix}0&1\\1&0\end{pmatrix}\right) \text{ erzeugt } |\psi\rangle \\ |10\rangle &: \quad Z\text{-gate} \quad \left(Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}\right) \text{ erzeugt } |\psi\rangle \\ |11\rangle &: \quad ZX\text{-gate} \quad \text{"} \quad \text{"} \end{aligned} \tag{61}$$

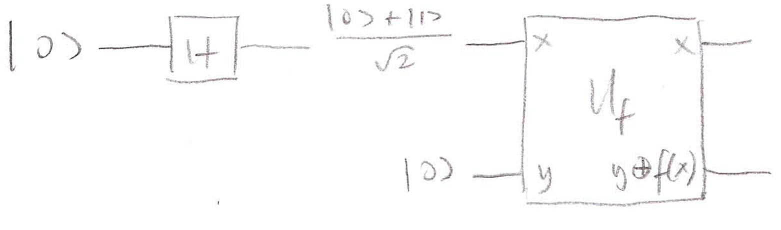
→ Zusammengefasst: Transformation $Z^{M_1} X^{M_2}$ erzeugt $|\psi\rangle$ DONE!

Beachte:

- klassische Komm. benötigt, d.h. $|\psi\rangle$ nicht schneller als Lichtgeschw. übermittelt. (man kann zeigen: ohne die klassische Komm. hier: überhaupt <u>keine</u> Information übermittelt)
- haben wir hier eine Kopie von $|\psi\rangle$ erzeugt? Nein, das Original ist durch Messung zerstört → kein Widerspruch zum no-cloning Theorem
- EPR Paar + klassischer Komm. Kanal ~ äquiv. Qubit. zeigt nochmals Mächtigkeit der verschränkten (EPR) Zustände auf.

<u>Quantenparallelismus</u>

Etwas vereinfacht kann man sagen: Quanten Parallelismus erlaubt es einem Quantencomputer, eine Funktion $f(x)$ <u>gleichzeitig</u> für verschiedene Werte x auszurechnen. Dies sei am folgenden Beispiel illustriert:

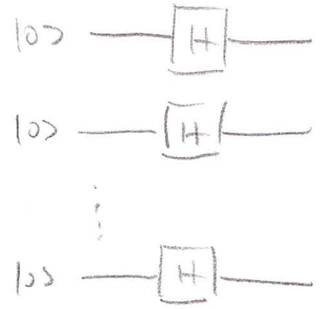


(62)

Sei $f(x): \{0,1\} \to \{0,1\}$ eine Funktion, die 1 Qubit auf ein Qubit abb. betrachte nun (62): $|x,y\rangle \xrightarrow{U_f} |x, y\oplus f(x)\rangle$. Man kann zeigen: U_f unitär. falls $y=0$ → 2. Qubit ist $f(x)$. Wendet man U_f auf einen Superpositionszustand $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ an (62), erhält man:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0, f(0)\rangle + |1, f(1)\rangle\right) \tag{63}$$

was bemerkenswerterweise sowohl $f(0)$ als auch $f(1)$ enthält, obwohl nur eine Operation U_f ausgeführt wurde. → „Quanten Parallelismus" dies lässt sich leicht auf n Qubits verallgemeinern:



$$= \frac{1}{\sqrt{2^n}} \sum_x |x\rangle \qquad (64)$$

Summe über alle 2^n Kombinationen von n 1 und 0.

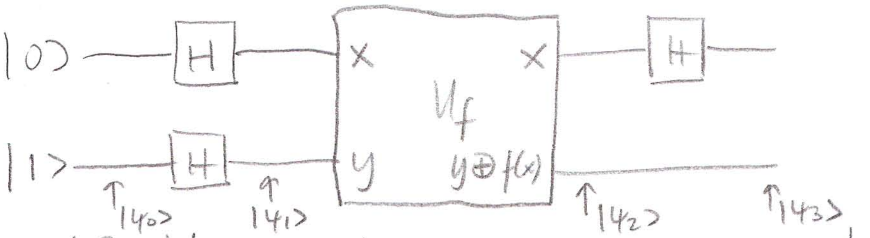
d.h. n parallele Hadamard Transformationen / Gates erzeugen eine Überlagerung (gleichmäßig) von $\underline{2^n}$ Zuständen. Sei nun $f(x)$ eine Funktion von n Qubits auf ein einziges Qubit. Präpariere den n+1 Qubit Zustand $|0\rangle^{\otimes n}|0\rangle = \underbrace{|0\rangle\dots|0\rangle}_{n}|0\rangle$, wende H wie in (64) auf die ersten n Qubits an, dann U_f (auf n+1 verallgemeinert) $\longrightarrow$

$$|\psi\rangle = \text{Output} = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle|f(x)\rangle \qquad (65)$$

d.h. eine einzige Operation U_f wertet gleichzeitig alle 2^n möglichen Werte $f(x)$ für x eine beliebige Kombination von n-stelligen 1/0. Natürlich: Messung ergibt (z.B. von (63)) nur entweder $|0, f(0)\rangle$ oder $|1, f(1)\rangle$, d.h. wir müssen es irgendwie geschickt anstellen, um gleichzeitig Information über mehrere/alle Werte $f(x)$ zu erhalten.

Deutsch's Algorithmus

Wir illustrieren die Effizienz eines Quantenrechners in einer leichten Modifikation von der Operation (64) und (65), nach D. Deutsch benannt. Diese Modifikation vereint Parallelismus mit Interferenz.



(66)

d.h. Eingang 2 ist nun $|1\rangle \to H|1\rangle = (|0\rangle - |1\rangle)\frac{1}{\sqrt{2}}$

$$|\psi_0\rangle = |0\rangle|1\rangle \qquad (67)$$

nach Hadamard gates:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{68}$$

Was ist $U_f|\psi_1\rangle$?

$$|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \xrightarrow{U_f} |x\rangle \underbrace{\left[\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \oplus f(x)\right]}$$

$$\begin{aligned}
&= (|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle)\tfrac{1}{\sqrt{2}} \\
&= (|f(x)\rangle - |\overline{f(x)}\rangle)\tfrac{1}{\sqrt{2}} \\
\text{falls } f(x)=0 \quad &= (|0\rangle - |1\rangle)\tfrac{1}{\sqrt{2}} \\
\text{falls } f(x)=1 \quad &= (|1\rangle - |0\rangle)\tfrac{1}{\sqrt{2}}
\end{aligned}\Bigg\} \; (-1)^{f(x)}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{69}$$

also:

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \xrightarrow{U_f} \frac{1}{\sqrt{2}}(-1)^{f(0)}|0\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{70}$$
$$+ \frac{1}{\sqrt{2}}(-1)^{f(1)}|1\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$f(0)=0$ (+), $f(0)=1$ (−)

$$|\psi_2\rangle = \begin{cases} = \pm\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \text{falls } f(0) = f(1) \quad (71) \\[2ex] = \pm\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \text{falls } f(0) \neq f(1) \quad (72) \end{cases}$$

nun noch das letzte Hadamard Gate auf Qubit eins:

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \text{falls } f(0)=f(1) \\[2ex] \pm|1\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \text{falls } f(0)\neq f(1) \end{cases} \tag{73}$$

nun benutzt man $f(0) \oplus f(1) = 0$ falls $f(0)=f(1)$, andernfalls $=1$

$$\Rightarrow \quad |\psi_3\rangle = \pm|f(0) \oplus f(1)\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \tag{74}$$

Durch Messung des ersten Qubits in $|\psi_3\rangle$ bestimmt man also $f(0)\oplus f(1)$, was eine „globale" Eigenschaft der Funktion $f(x)$ ist, mit nur einer einzigen Auswertung von f. Klassisch wären dazu 2 Auswertungen nötig, analoges gilt für n-Qubits, wo der Geschwindigkeitsgewinn 2^n sein kann!