Skript Quantencomputing

Prof. Andreas Goerdt

TU Chemnitz

October 14, 2013

1 Deutsches Algorithmus

David Deutsch (1986) - Ein einfaches Problem:

$f : \{0,1\} \to \{0,1\}$ ist gegeben.

Gesucht $f(0) \oplus f(1)$. (etwa durch exklusives $\vee$. ein Programm!).

Deterministisch: $f(0), f(1), f(0), f(0) \oplus f(1)$.

2-mal f aufrufen.

Randomisiert (zum Beispiel) $x_0 := f(0)$ oder $f(1)$ mit $\frac{1}{2}$

Im Falle $f(0) = f(1) = 0$, haben wir für x_0 die Verteilung $1 \cdot |0\rangle + 0|1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

Im Falle $f(0) = f(1) = 1$ $0|0\rangle + 1|1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

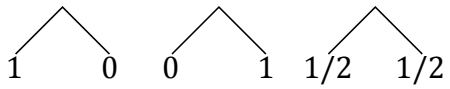
Im Falle $f(0) \neq f(1)$ haben wir

$$\frac{1}{2} \cdot |0\rangle + \frac{1}{2} \cdot |1\rangle = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}$$

Haben Matrix für f:

$$\begin{pmatrix} 1 & \\ & 1 \end{pmatrix} \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$$
$$\begin{pmatrix} 1 & 1 \\ & \end{pmatrix} \begin{pmatrix} & \\ 1 & 1 \end{pmatrix}$$

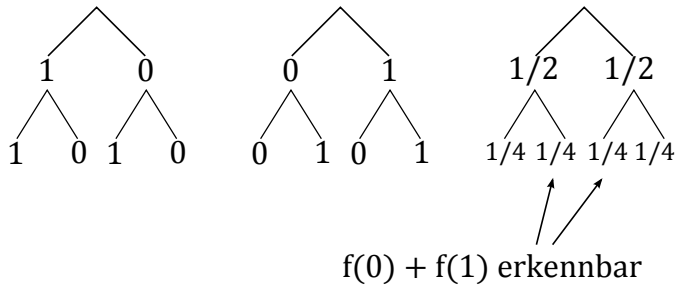
Als Baum:



Fehlerwahrscheinlichkeit bis hin zu 1.

2-maliges Lesen.

Bei $f(0) \neq f(1)$ richtig mit $\frac{1}{2}$. Bei $f(0) = f(1)$ richtig mit Wahrscheinlichkeit von 1.
Besser deterministisch.



Will f im Quatntenprogramm aufrufen. Dazu muss f als orthogonale Matrix gegeben sein, insbesondere bijektiv.

Klassisch: f ist eine Transformation des Zustandraums.

Dazu wird f durch $f_\oplus$ dargestellt: $f_\oplus : \{0,1\}^2 \to \{0,1\}^2$ mit $|x_1 x_2\rangle |x_1 \left(x_0 \oplus f(x_1)\right)$

Man behält das Argument bei (siehe jeweils x_1)

$$|x_1 0\rangle \to x_1 f\left(x_1\right)$$
$$|x_1 1\rangle \to x_1 \neg f\left(x_1\right)$$

Offensichtlich bijektiv.

Mögliche Matrizen für $f_\oplus$:

	00	01	10	11
00	01			
01		01		
10			01	
11				01

Sei 01 eine von diesen Matrizen. Startwert $|00\rangle$, zum Beispiel.

Was kann man damit anfangen?

01 anwendbar. $M|00\rangle = |0f(0)\rangle$. Mit einem Wort kann man gar nichts anfangen.

Also zuerst $H_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ auf das erste Qbit anwenden. Dann haben wir die Matrix:

$$\frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 1 & & \\ & 1 & & 1 \\ 1 & -1 & & \\ & 1 & & -1 \end{pmatrix} \begin{matrix} 00 \\ 01 \\ 10 \\ 11 \end{matrix}$$
$$00\ 01\ 10\ 11$$

Also

$$|00\rangle \xrightarrow{H_2 \text{ auf 1. Qbit}} \frac{1}{\sqrt{2}} \left(|00\rangle + |10\rangle\right)$$

$$\xrightarrow{M} \frac{1}{\sqrt{2}} \left(|0f(0)\rangle + |1f(1)\rangle\right)$$

4 Möglichkeiten:

$$\begin{matrix} 00 \\ 01 \\ 10 \\ 11 \end{matrix} \underbrace{\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}}_{\text{Ziel etwa } |0-\rangle}, \underbrace{\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}}_{\text{Ziel etwa } |1-\rangle} \quad \left(\frac{1}{\sqrt{2}}\right) \text{ als Ergebnis}$$

Messen ergäbe den Unterschied.

Wie wäre es, wenn wir die Vekroten hätten:

$$\underbrace{\begin{pmatrix}1\\-1\\1\\1\end{pmatrix},\begin{pmatrix}-1\\1\\-1\\1\end{pmatrix}}_{\longmapsto|0-\rangle},\underbrace{\begin{pmatrix}1\\-1\\-1\\1\end{pmatrix},\begin{pmatrix}-1\\1\\1\\-1\end{pmatrix}}_{\longmapsto|1-\rangle}\begin{pmatrix}\frac{1}{2}\end{pmatrix} \tag{1}$$

$H_2 = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$ auf das erste Qbit. Das bedeuted bei Matrix

$$\begin{array}{c} \quad 00\ 01\ 10\ 11 \\ \frac{1}{\sqrt{2}}\cdot\begin{pmatrix}1 & 1 & & \\ & 1 & & 1\\ 1 & & -1 & \\ & 1 & & -1\end{pmatrix}\begin{matrix}00\\01\\10\\11\end{matrix}\end{array}$$

$$\begin{pmatrix}1\\-1\\1\\-1\end{pmatrix}\cdot\tfrac{1}{2} = \tfrac{1}{2}\left(|00\rangle + |10\rangle - (|01\rangle + |11\rangle)\right)$$

$$\mapsto \tfrac{1}{\sqrt{2}}\cdot\tfrac{1}{2}\left(|00\rangle + |10\rangle + |00\rangle - |10\rangle\right)$$

Wegheben - "Negative Wahrscheinlichkeit"

$$|01\rangle \qquad |11\rangle$$

$$-\left(|01\rangle + |11\rangle + |01\rangle - |11\rangle\right)$$

$$= \tfrac{1}{\sqrt{2}}\cdot\left(|00\rangle - |01\rangle\right)$$

$$\begin{pmatrix} -1 \\ 1 \\ -1 \\ 1 \end{pmatrix} \cdot \frac{1}{2} = - \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} \cdot \frac{1}{2}$$

$$\mapsto \frac{1}{\sqrt{2}} \left(-|00\rangle + |01\rangle \right)$$

$$\begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix} \cdot \frac{1}{2} \mapsto \frac{1}{\sqrt{2}} \left(|10\rangle - |11\rangle \right)$$

$$\begin{pmatrix} -1 \\ 1 \\ 1 \\ -1 \end{pmatrix} \cdot \frac{1}{2} \mapsto \frac{1}{\sqrt{2}} \left(-|10\rangle + |11\rangle \right)$$

Beobachten und dann erstes Qbit setzen ergibt das Ergebnis.

Die Frage ist: Wie bekommt man die Ausgangsvektoren?

$\phi(0) = \phi(1) = 0$ gibt die Matrix für $f_\oplus$

$$M = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}$$

Dort soll $\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} \cdot \frac{1}{2}$ rauskommen.

Es gilt: $\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} \cdot \frac{1}{2} \Longleftrightarrow \frac{1}{2}\left(|00\rangle - |01\rangle + |10\rangle - |11\rangle\right)$

Also brauchen das als Anfangsvektor. Wie bekommt man das aus dem Startvektor $|00\rangle$?

Zuerst Negation $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ auf das 2. Qbit.

$$|00\rangle \mapsto |01\rangle$$

Dann H_2 auf das 2. Qbit

$$|01\rangle \mapsto \frac{1}{\sqrt{2}}\left(|00\rangle - |01\rangle\right) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix}$$

Dann H_2 auf das erste Qbit

$$|00\rangle \mapsto \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right)$$

$$|01\rangle \mapsto \frac{1}{\sqrt{2}}\left(|01\rangle + |11\rangle\right)$$

$$\frac{1}{\sqrt{2}}\left(|00\rangle - |01\rangle\right) \mapsto \frac{1}{2}\left(|00\rangle - |01\rangle + |10\rangle - |11\rangle\right) = \frac{1}{2}\sum_{b_1,b_2}(-1)^{b_2}|b_1 b_2\rangle.$$

Wenden wir auf diesen Vektor das M für $f_\oplus$ an, so bekommen wir:

$$\frac{1}{2}\sum_{b_1,b_2}(-1)^{b_2}|b_1 b_2\rangle \mapsto \sum_{b_1,b_2}(-1)^{\phi(b_2)}|b_1 b_2\rangle$$

Das sind dann gerade die Vektoren aus 1.

Qbit1	Qbit2	Qbit1	Qbit2
0	0		
	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$		M
		H_2	
H_2	H_2	Messen	

Sinn der Sache: Ein Aufruf von $f(d, k, M)$ gibt gewünschtes Ergebnis.

2 Teleportation

Betrachten wir 2 Qbits x_1, x_2 und nehmen nur an, sie sind in dem Zustand

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Vorstellung: x_1 oszilliert zwischen 0 und 1, x_2 ebenso, das stehts ist $x_1 = x_2$. Eine weitere Neuigkeit: x_1, x_2 bleiben 2 unabhängige Bits. D.h. wir können x_1 Benutzer A(lice) setzen und x_2 Benutzer B(ob). Für obrigen Zustand gilt: $x_1 = x_2$, egal wie weit sie auseinander sind. *("'Rätselhafte Fernwirkung"' (Einstein))*

A und B können auf ihren Qbits wie bekannt weiterarbeiten.

Wendet A etwa die Negation $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ auf x_1 an, so bekommen wir den Zustand $\frac{1}{\sqrt{2}}(||01\rangle + |01\rangle)$.

Wendet A $H_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ an, so

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

Was geschiet, wenn A im Zustand

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$\uparrow\uparrow \qquad \uparrow\uparrow$$
$x_1 x_2$ $\quad$ $x_1 x_2$ sein Qbit x_1 misst?

$x_1 = 0$ mit $\frac{1}{2}$, Folgezustand $|00\rangle$

$x_1 = 1$ mit $\frac{1}{2}$, Folgezustand $|11\rangle$

Was hat B?

B hat $|0\rangle$ oder $|1\rangle$ jeden Wert mit Wahrscheinlichkeit $\frac{1}{2}$. Also ein klassiches Zufallsbit. (nicht irgendetwas der Art $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.)

Was passiert, wenn für x_1, x_2 der gemeinsame Zustand $\frac{1}{2}(|00\rangle + |10\rangle + |01\rangle - |11\rangle)$ vorliegt?

A misst $|0\rangle$ in einem Qbit

$\Longleftrightarrow$

Die Messung trifft auf $|00\rangle$ oder $|01\rangle$.

Also Wahrscheinlichkeit $\frac{1}{4} + \frac{1}{4} = \frac{1}{2}$.

Wenn A $|0\rangle$ gemessen hat, was ist der Folgezustand?

Der Folgezustand muss sich ergeben aus $\frac{1}{2}(|00\rangle + |01\rangle)$.

Dieser muss nur auf L_2-Norm 1 normiert werden.

Teilen durch L_2-Norm ergibt $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$.

Also: Wahrscheinlichkeit $= (L_2\text{-Norm})^2$

Dann: Normieren, in dem wir durch L_2-Norm teilen.

Erinnerung: Betrachten $\sum a_i|i\rangle$.

L_2-Norm $= \sqrt{\sum a_i^2}$ (Pythagoras)

$(L_2\text{-Norm})^2 = \sum a_i^2$

$\frac{1}{\sqrt{\sum a_i^2}} \cdot \sum a_i|i\rangle$ hat L_2-Norm = 1, denn $\sum \frac{a_i^2}{\sum a_i^2} = \frac{\sum a_i^2}{\sum a_i^2} = 1$.

In dem Zustand (2) und von A $|1\rangle$ gemessen mit

- Wahrscheinlichkeit $\frac{1}{4} + \frac{1}{4} = \frac{1}{2}$
- Folgezustand $\frac{\frac{1}{2}(|10\rangle - |11\rangle)}{\frac{1}{\sqrt{2}}} = \frac{1}{\sqrt{2}}(|10\rangle - |11\rangle)$

Also, wenn A sein Qbit gemessen hat, so haben wir danach folgende Verteilung von Zuständen von x_1, x_2:

$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$ mit Wahrscheinlichkeit $\frac{1}{2}$

$\frac{1}{\sqrt{2}}(|10\rangle + |11\rangle)$ mit Wahrscheinlichkeit $\frac{1}{2}$

$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$ bedeutet auf jeden Fall, $x_1 = |0\rangle$. Lassen wir jetzt x_1 weg, so belibt übrig (bei B) $\frac{1}{\sqrt{2}(|0\rangle+|1\rangle)}$

Bei $\frac{1}{\sqrt{2}}(|10\rangle - |11\rangle)$ bekommen wir $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Wollen wir dagegen in $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$ das Qbit x_1 weglassen, wie soll das gehen? Es ist verschränkt *(entangled)* mit x_2. Können es nur messen und dann wegwerfen.

$\rightsquigarrow$ Verteilung von Qbits.

A hat Zustand $|\Phi\rangle = a_0|0\rangle + a_1|1\rangle$ (a_0, a_1 nicht explizit bekannt) eines Qbits. A soll $|H\rangle$ zu B senden. A und B haben vorher eine verschränktes Paar von Qbits x_1, x_2 bekommen. Als Zustand von x_1, x_2 ist

$$\begin{array}{ll} \frac{1}{\sqrt{2}} \cdot (|00\rangle + |11\rangle) & \\ \uparrow\uparrow \qquad \uparrow\uparrow & \text{EPR-Paar} \\ x_1 x_2 \quad x_1 x_2 & \text{Einstein, Podolski, Rosen} \end{array}$$

x_1 ist bei A, x_2 ist bei B. Des Weiteren haben A und B nur einen klassichen Kommunikationskanal. Sei $|\Phi\rangle$ Zustand von Qbit x_0 bei A. x_0 unabhängig (nicht entangled mit dem Rest). Damit ist der Gesamtzustand von x_0, x_1, x_2.

$$|x_0, x_1\rangle$$

$$|\Phi_0\rangle = a_0(|000\rangle + |011\rangle) + a_1 \frac{1}{\sqrt{2}}(|100\rangle + |111\rangle)$$

x_0, x_1 bei A, x_2 bei B.

A hat folgende Operationen zur Verfügung:

$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & & 1 \\ & & 1 & \end{pmatrix} \begin{matrix} |00\rangle \mapsto |00\rangle \\ |01\rangle \mapsto |01\rangle \\ |10\rangle \mapsto |11\rangle \\ |11\rangle \mapsto |10\rangle \end{matrix}$$

Kontrollierte Negation: Ist das 1-Qbit $= 1$, wird das 2-Qbit negiert, sonst nicht.

A wendet die kontrollierte Negation auf x_0, x_1 an. Das ergibt als Gesamtzustand

$$|\Phi_1\rangle = a_0 \frac{1}{\sqrt{2}} (|000\rangle + |001\rangle)$$

$$+ a_1 \tfrac{1}{\sqrt{2}} (|110\rangle + |101\rangle)$$
$$\uparrow \quad \uparrow$$
Negation

A sendet das 1. Qbit, x_0 durch ein H_2.

Dann $|\Phi_2\rangle = a_1 \frac{1}{2} \cdot (|000\rangle + |100\rangle + |011\rangle + |11\rangle) + a_1 \frac{1}{2} (|010\rangle - |110\rangle + |001\rangle + |101\rangle)$

H_2 damit nur die gleichen Anfänge (ersten 2 Qbit bekommen)

Übung

Was geschieht, wenn $|x_0\rangle$ noch mal einen anderern Qbit irgendwo verschränkt ist. Das heißt, wir haben einen Zustand der Art

weiteres Qbit x_0

$\searrow \quad \swarrow$

$|\Phi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$?

Oder sogar: $|\Phi\rangle = \sum_{b_{01-},b_m} a_{b_0-b_m}|b_0 \dots b_m\rangle$ *)

x_0 weitere Qbits

Übung

Seien x_0, x_1 2 Qbits, nicht verschränkt.

Auf x_0 stehe $|\Phi\rangle = a_0|0\rangle + a_1|1\rangle$

auf x_1 $|\Phi\rangle = b_0|0\rangle + b_1|1\rangle$

Wie sieht der gesamte Zustand aus?

$$
\begin{aligned}
&= a_0\frac{1}{2}|000\rangle + a_1\frac{1}{2}|001\rangle \\
&+ a_0\frac{1}{2}|011\rangle + a_1\frac{1}{2}|010\rangle \\
&+ a_0\frac{1}{2}|100\rangle + a_1\frac{1}{2}|101\rangle \\
&+ a_0\frac{1}{2}|111\rangle + a_1\frac{1}{2}|110\rangle
\end{aligned}
$$

Was bedeutet das?

$$
\begin{array}{lllll}
\text{"`Hat"'} A\ |00\rangle, & \text{so } B(!) & |(\Phi)\rangle & = a_0|0 + a_1|1\rangle \\
A \quad\ |01\rangle, & \text{so } B & |(\Phi')\rangle & = a_0|1 + a_1|0\rangle \\
|00\rangle, & \text{so } B & |(\Phi'')\rangle & = a_0|0 + a_1|1\rangle \\
|00\rangle, & \text{so } B & |(\Phi''')\rangle & = a_0|1 + a_1|0\rangle
\end{array}
$$

Also: A misst x_0, x_1. Jede Möglichkeit hat Wahrscheinlichkeit $\frac{1}{4}$.

Die $|\Phi\rangle$, $|\Phi'\rangle$, ... ergeben sich durch Teilen durch $\sqrt{\frac{1}{4}} = \frac{1}{2}$.

Nun sendet A sein Messergebnis (2 klassische Bits) zu B. Was macht B?

Nachricht

00	B macht nichts mit x_2.
01	B wendet $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ an.
10	B wendet $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ an.
11	B wendet erst $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, dann $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ an.

Dann ist

(b_0 Kontrollbit, 00 kontrollierte Negation)

$$
\begin{aligned}
|\Phi_0\rangle &= \sum a_{b_0-b_m} \cdot \frac{1}{\sqrt{2}} \left(|b_0 - b_m 00\rangle + |b_0 - b_m 11\rangle\right) \\
|\Phi_1\rangle &= \sum_{b_0=0} a_{b_0-b_m} \cdot \frac{1}{\sqrt{2}} \left(|0b_1 - b_m 00\rangle + |0b_0 - b_m 11\rangle\right) \\
&\quad + \sum_{b_0=1} a_{b_0-b_m} \cdot \frac{1}{\sqrt{2}} \left(|1b_1 - b_m 10\rangle + |1b_0 - b_m 01\rangle\right) \\
|\Phi_2\rangle &= \sum a_{0_{b_1-b_m}} \cdot \frac{1}{2} \left(|0b_1 - b_m 00\rangle + |1b_1 - b_m 00\rangle + |0b_1 - b_m 11\rangle |1b_1 - b_m 01\right) \\
&\quad + \sum_{b_1-b_2} a_{1_{b_1-b_m}} \cdot \frac{1}{2} \left(|0b_1 - b_m 10\rangle - |1b_1 - b_{m10}\rangle + |0b_1 - b_m 01\rangle - |1b_1 - b_m 01\rangle\right)
\end{aligned}
$$

A misst 00 mit $\sum (a_{b_0-b_m})^2 \cdot \frac{1}{4} = \frac{1}{4}$.

Es bleibt tatsächlich $\sum_{b_1-b_m} a_{0_{b_1-b_m}} |b_1 - b_m 0\rangle + \sum_{b_1-b_m} a_{1_{b_1-b_m}} |b_1 - b_m 1\rangle$

3 Superdense Coding

Wieder

$$\frac{1}{\sqrt{2}} \cdot (|00\rangle + |11\rangle)$$
$$\uparrow\uparrow \qquad \uparrow\uparrow \ \nwarrow EPR - Paar$$
$$x_1 x_2 \quad x_1 x_2$$

x_1 ist bei A, x_2 bei B.

A will 2 klassiche Bits zu B senden, soll aber nur 1 Qbit übertragen.

$Nachricht$	
00	A schickt Qbit x_1 zu B.
01	A wendet $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ auf x_1 an. Sendet x_1 zu B.
10	A wendet $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ auf $x_1$an. Sendet x_1.
11	A wendet $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ an. und schickt x_1

Was hat B in x_1, x_2?

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

Vektoren $\left(\frac{1}{\sqrt{2}}\right) \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}$. Diese sind alle orthogonal.

Anwendung von

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \end{pmatrix}$$

dann Messen ergibt das Bit.

Übung

Basistransformation, Matrizen, orthogonale Basen

Einschub: Lecture 3: Superdense coding, quantum circuits, and partial measurements (CPSC 519/619: Quantum Computation, J. Watrous, Unversity of Calgary, Janury 24 2006)

4 No-cloning Satz

Können **Qbits kopiert** werden? - Im Allgemeinen: **Nein**.

Wie sieht das im klassischen Fall aus?

Mit assignment $x_1 := x_0$ ✓

Ohne assignment: $x_1 = 0$ oder 1, $x_0 = 0$

dann kontrollierte Negation auf x_1 und x_0.

Randomisiert

$$\begin{array}{c} \begin{pmatrix} 1 & & & \\ & & 1 & \\ & 1 & & \\ & & & 1 \end{pmatrix} \begin{matrix} 00 \\ 01 \\ 10 \\ 11 \end{matrix} \\ 00\ 01\ 10\ 11 \\ x_0x_1 \end{array}$$

$x_1 = p_0|0\rangle + \pi_1|1\rangle$, $x_0 = 1 \cdot |0\rangle$

Startzustand von x_0x_1

x_0x_1

$|\Phi_0\rangle = p_0|00\rangle + p_1|01\rangle$.

Kontrollierte Neg.: 1

$|\Phi_1\rangle = p_0|00\rangle + p_1|11\rangle$.

Lassen wir jetzt x_1 weg, so haben wir geschätzt folgendes $|00\rangle$ mit p_0, $|11\rangle$ mit p_1.

Also bleibt $p_0|0 + p_1|1$ auf x_0

Aber: keine unabhängigen Kopien.

Das Analoge im Quantenfall: $|\Phi_0 = a_0|00\rangle + a_1|01$

Kontrollierte Negation ergibt $|\Phi_1 = a_0|00\rangle + a_1|01$

Lassen nun x_1 weg. Messen: $|00\rangle$ mit $|a_0|^2$ $|11\rangle$ mit $|a_1|^2$

Auf x_0 $\frac{a_0}{|a_0|}|0$ mit $|a_0|^2$ $\frac{a_1}{|a_1|}|1\rangle$ mit $|a_1|^2$

Keine Kopie! (globaler Faktor *global phase* unwichtig.)

Will haben: Unabhängige Kopien.

Also zuerst $p_0|0\rangle + p_1|1\rangle$ auf x_1 und auf x_0 eine feste andere Verteilung,

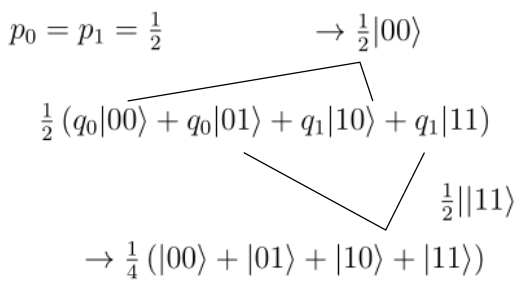
etwa $q_0|0\rangle + q_0|0\rangle$.

Dann also $|\Phi_0\rangle = q_0p_0|00\rangle + q_0p_1|01\rangle + q_1p_0|10\rangle + q_1p_1|11\rangle$

Und $|\Phi_1\rangle = p_0^2|00\rangle + p_0p_1|01\rangle + p_1p_0|10\rangle + p_1^2|11\rangle$

$p_0 = 1$, $p_1 = 0$, dann $q_0|00\rangle + q_1|10\rangle \to 1|00\rangle$

$p_0 = 0$, $p_1 = 1$, dann $q_0|01\rangle + q_1|11\rangle \to 1|11\rangle$



Also nach vorheriger Rechnung dürfte wegen Linearität nur rauskommen

$$\frac{1}{2}|00\rangle + \frac{1}{2}|11\rangle.$$

Kopieren i.a. nicht möglich.

Übung

Das geht bei $p_0 = q_0$ oder $p_0 = q_1$

Quantenrechnen

$a_0|0\rangle + a_1|1\rangle$ auf x_1,

$b_0|0\rangle + b_1|1\rangle$ auf x_0, fest.

$$|\Phi_0\rangle = a_0 b_0|00\rangle + a_0 b_1|01\rangle + a_1 b_0|10\rangle + a_1 b_1|11\rangle$$
$$|\Phi_1\rangle = a_0^2|00\rangle + a_0 a_1|01\rangle + a_1 a_0|10\rangle + a_1^2|11\rangle$$

Probe: Zweites Qbit wegwerfen.

$a_0^2|00\rangle + a_1 a_0|10\rangle$ Wahrscheinlichekit $|a_0|^4 + |a_1 a_0|^2$

$a_0 a_1|01\rangle + a_1^2|11\rangle$ Wahrscheinlichekit $|a_1|^4 + |a_1 a_0|^2$

Also übrig bleibt auf x_1

$$\begin{aligned} a_0|0\rangle + a_1 a_0|1\rangle \cdot \frac{1}{\sqrt{|a_0|^4 + |a_1 a_0|^2}} &= \frac{a_0}{|a_0|} \cdot (a_0|0\rangle + a_1|1\rangle) \\ &= |a_0| \cdot \sqrt{|a_0|^2 + |a_1|^2} \\ &= |a_0| \end{aligned}$$

Nebenrechnung: $\sqrt{|a_0|^2 + |a_1|^2} = 1$

oder

$$(a_1|11\rangle + a_0 a_1|01\rangle) \cdot \frac{1}{\sqrt{|a_1|^4 + |a_1 a_0|^2}} = \frac{a_1}{|a_1|}|a_0|0\rangle + a_1|1\rangle$$

Ebenso das 1. Qbit wegwerfen **+,-1** - globaler Faktor (global phase) egal!

Für eine Kopiermatrix k gilt also: $|\Phi_0\rangle \to K|\Phi_0\rangle = |\Phi_1\rangle$

Betrachten wir einen 2. Zustand auf x_1 etwa $c_0|0\rangle + c_1|1\rangle$

$$|\Psi_0\rangle = c_0 b_0|00\rangle + c_0 b_1|01\rangle + c_1 b_0|10\rangle + c_1 b_1|11\rangle$$
$$|\Psi\rangle = c_0^2 = c_0^2|00\rangle + c_0 c_1 + c_1 c_0|10\rangle + c_1^2|11\rangle$$

Dann $|\Psi_0\rangle \to K|\Psi_0\rangle = |\Psi_1\rangle$
Da K orthogonale Matrix ist, gilt immer

$$|\Psi_0 \cdot |\Phi\rangle = (K|\Psi\rangle) \cdot (K|\Phi)$$

Inneres Produkt Inneres Produkt - Orthogonalität

Es ist

$$|\Psi_0\rangle \cdot |\Phi_0\rangle = a_0 c_0 b_0^2 + a_0 c_0 b_1^2 + a_1 c_1 b_0^2 + a_1 c_1 b_1^2 = a_0 c_0 + a_1 c_1$$
$$|\Psi_1\rangle \cdot |\Phi_1\rangle = a_0^2 c_0 + a_0 a_1 c_0 c_1 + a_0 a_1 c_0 c_1 + a_1^2 c_1^2 = (a_0 c_0 + a_1 c_1)^2$$

Also

$$a_0 c_0 + a_1 c_1 = (a_0 c_0 + a_1 c_1 = 0)^2$$
$$a_0 c_0 + a_1 c_1 = 1 \text{ oder } a_0 c_0 + a_1 c_1 = 0$$

Im zweiten Fall sind die Zustände orthogonal, im ersten Fall gleich. (Inneres Produkt bei L_2-Norm 1 ist Cosinus!) **(No-cloning-Satz)**

Übung

$a_0|0\rangle + a_1|1\rangle$, $c_0|0\rangle + c_1|1\rangle$ orthogonal. Suche Matrix, die

$$a_0|00\rangle + a_1|10\rangle \to a_0^2|00\rangle + a_0 a_1|01\rangle + \ldots$$
$$c_0|00\rangle + c_1|10\rangle \to c_0^2|00\rangle + c_0 c_1|01\rangle + \ldots$$

5 Das Tensorprodukt

Zu einem Qbit gehört der Vektorraum $\mathbb{R}^2$, Wahrscheinlihchkeit eines Qbits ist

$a_0|0\rangle + a_1|1\rangle = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$ und $a_0^2 + a_1^2 = 1$.

Zu 2 Qbits gehört der $\mathbb{R}^4$, Wahrscheinlichkeit

$$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix},$$

$$\alpha_{00}^2 + \alpha_{01}^2 + \alpha_{10}^2 + \alpha_{11}^2 = 1.$$

Zusätzlich zum $\mathbb{R}^4$ können wir aber auch über das 1. oder 2. Qbit reden. Der Raum für 2 Qbits ist der $\mathbb{R}^4$ mit einer zusätzlich Struktur. Der Raum ist das **Tensorprodukt** von $\mathbb{R}^2$ mit $\mathbb{R}^2$, $\mathbb{R}^2 \otimes \mathbb{R}^2$ ein vierdimensionaler Vektorraum.

Fangen wir noch einem mit dem klassischen Fall an.

Wahrscheinlichkeit von 2 Bits ist $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$,

wobei $\alpha_{b_1 b_2} \geq 0$, $\alpha_{00} + \alpha_{01} + \alpha_{10} + \alpha_{11} = 1$.

Ist x_1 und Zustand $\frac{1}{4}|0\rangle + \frac{3}{4}|1\rangle$ und x_0 in $\frac{3}{4}|0\rangle + \frac{1}{4}|1\rangle$, so ist der Gesamtzustand von x_1, x_0

$$\frac{3}{16}|00\rangle + \frac{1}{16}|01\rangle + \frac{9}{16}|10\rangle + \frac{3}{16}|11\rangle.$$

Das schreibt man auch als Tensorprodukt der Vektoren:

$$\left(\frac{1}{4}|0\rangle + \frac{3}{4}|1\rangle\right) \otimes \left(\frac{3}{4}|0\rangle + \frac{1}{4}|1\rangle\right)$$

Das lässt sich auch schreiben als

$$\begin{aligned}
&\frac{1}{4}|0\rangle \otimes \left(\frac{3}{4}|0\rangle + \frac{1}{4}|1\rangle\right) + \frac{3}{4}|1\rangle \otimes \left(\frac{3}{4}|0\rangle + \frac{1}{4}|1\rangle\right) \\
&= |0\rangle \otimes \frac{1}{4}\left(\frac{3}{4}|0\rangle + \frac{1}{4}|1\rangle\right) + |1\rangle \otimes \frac{3}{4}\left(\frac{3}{4}|0\rangle + \frac{1}{4}|1\rangle\right) \\
&\quad \text{(Vorstellung: An } |0\rangle \text{ hängt } \frac{1}{4} \cdot \frac{3}{4}|0\rangle + \frac{1}{4}|1\rangle) \\
&= \frac{3}{4}\left(\frac{1}{4}|0\rangle + \frac{3}{4}|1\rangle\right) \otimes |0\rangle + \frac{1}{4} \cdot \left(\frac{1}{4}|0\rangle + \frac{3}{4}|1\rangle\right) \otimes |1\rangle
\end{aligned}$$

Definition

V	Vektorraum mit orthogonaler Basis $v_1, \ldots, v_n$
W	Vektorraum mit orthogonaler Basis $w_1, \ldots, w_n$
$V \otimes W$	Vektorraum mit orthogonaler Basis $v_1 \otimes w_1, \ldots, v_1 \otimes w_m, \ldots, v_n \otimes w_1, \ldots, v_n \otimes w_m$ auch geschrieben als $\lvert v_1, w_1\rangle, \ldots, \lvert v_n, w_m\rangle$

Es folgen einige Beobachtungen zu $V \otimes W$.

1. Jeder Vektor aus $V \otimes W$ hat die Form

$$\sum_{i=1,\ldots,n \; j=1,\ldots,m} a_{i,j}|v_i w_j\rangle = \begin{pmatrix} a_{11} \\ \vdots \\ a_{1m} \\ \vdots \\ a_{n1} \\ \vdots \\ a_{nm} \end{pmatrix} \begin{matrix} |v_1, w_1\rangle \\ \vdots \\ |v_1, w_m\rangle \\ \vdots \\ |v_n, w_1\rangle \\ \vdots \\ |v_n w_m\rangle \end{matrix}$$

v_i, w_j ist der Basisvektor von $V \otimes W$.
Dimension $V \otimes W$ = (Dimension von V) $\cdot$ (Dimension von W)

2. Bsp. $V = W = \mathbb{R}^2 \cdot \mathbb{R}^2$ hat Basis $|0\rangle, |1\rangle$. $\mathbb{R}^2 \cdot \mathbb{R}^2$ hat Basis $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$.
3. Wichtig ist der Bezug von V, W zu $V \otimes W$.
   Dazu definieren wir die Abbildung $\otimes$
   $\otimes : V \times W \to V \otimes W$
   mit für $v = \sum a_i v_i \in V$, $w = \sum c_j w_j \in W$ ist
   $\otimes(v, w) := v \otimes w := \sum a_i c_j |v_i w_j\rangle$
   $v \oplus w =$ der Tensor von v und w.

   Es ist

$$v \otimes w = \begin{pmatrix} a_1 c_1 \\ \vdots \\ a_1 c_m \\ a_2 c_1 \\ \vdots \\ a_2 c_m \\ \vdots \\ a_n c_1 \\ \vdots \\ a_n c_m \end{pmatrix} \begin{matrix} |v_1, w_1\rangle \\ \vdots \\ |v_1, w_m\rangle \end{matrix}$$

   Oder auch an v_1 hängt $a_1 w_1 \ldots a_1 w_m$, an v_2 $a_2 w_1 \ldots a_2 w_m$ usw.
   Vorstellung: an $a_1 v_1$ hängt w_j, an $a_2 v_2$ hängt w, $\ldots$ an $a_n v_n$ hängt w.
   Die Abbildung $\otimes : (v, w) \to v \otimes w$ ist bilinear. Das bedeutet

$$\begin{aligned} v \otimes (w + u) &= (v \otimes w) + (v \otimes u) \\ (v + x) \otimes w &= (v \otimes w) + (x \otimes w) \\ (a \cdot v) \otimes w &= a \cdot (v \otimes w), a \in \mathbb{R} \\ v \otimes a \cdot w &= a \cdot (v \otimes w), a \in \mathbb{R} \end{aligned}$$

Das alles rechnet man leicht aus der Definition nach.

Es ist

$$v_i \otimes w_j = |v_i w_j\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \begin{matrix} \leftarrow \text{Stelle } 1 \\ \\ v_i w_j \leftarrow \text{Stelle } i,j \end{matrix}$$

Beachte: Nicht jeder Vektor aus $V \otimes W$ ist von der Form $v \otimes w$! (Die meisten nicht.)

Bsp.: $V = W = \mathbb{R}^2$, dann $|00\rangle + |11\rangle \neq v \otimes w$ für alle v, w.

Für $w = \sum c_j w_j$, $v = \sum a_i v_i$ ist $v \otimes w = \sum v_i \otimes (a_i \cdot w) = \sum c_{ji} v \otimes w_j$

Allgemein ein Vektor aus $V \otimes W$ eindeutig darstellbar als $\sum v_i \otimes x_i$ für $x_i \in W$.

An jedem v_i hängt $a_i \cdot w$. Oder an $a_i v$ hängt das w.

An jedem Basisvektor hängt ein Vielfaches von w bzw. v.

Je nachdem wie herum man zerlegt. Nachrechnen wegen der Bilinerarität.

Was ist mit dem Nullvektor 0?

$$0 \otimes w = v \otimes 0 = 0_{v \otimes w}.$$

Bilinearität

$$0 = 0 \cdot v = 0 \cdot w = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Definition

Skalarprodukt auf $V \otimes W$

$$\left(\sum a_{ij} |v_i w_j\rangle, \sum c_{ij} |v_i w_j\rangle \right) = \sum a_{ij} \cdot c_{ij}$$

Es folgen weitere Beobachtungen

1. a_i c_i d_i e_i

$(v \otimes w, x \otimes y) \leftarrow$ Skalarprodukt von $v \otimes w$ und $x \otimes y$

$$= \sum_{i,j} a_i \cdot c_j \cdot d_i \cdot e_j = \sum_{i,j} a_i \cdot d_i \cdot c_j \cdot e_j = \sum_i a_i d_i \cdot \sum_j c_j e_j = (v, x) \cdot (w, y)$$

(Skalarprodukt)

2. $v \otimes w$ orthogonal zu $x \otimes y$ (Skalarprodukt = 0) $\Leftrightarrow$ v orthogonal zu x oder (!) w zu y.
   $|v_i w_j\rangle$ orthogonal zu $|v_i, w_{j'}\rangle$ $j' \neq i$, da w_j orthogonale Basis.
3. v und w L_2-Norm 1, dann auch $v \otimes w$, da L_2-Norm $= \sqrt{(v, v)}$ ((v, v) Skalarprodukt) und $v \otimes w = (v, v) \cdot (w, w)$
   Ebenso L_1-Norm von $v = \sum a_i v_i$ ist $\sum a_i$
   $y \otimes w \Leftarrow$ Unabhängigkeit von 1. und 2. Qbit

   Ein interessanter Zusammenhang:
   $V \otimes W \widehat{=}$ Lineare Abbildung von W nach V

$$\sum a_{ij} |v_i w_j\rangle = \begin{pmatrix} a_{11} \\ a_{12} \\ \vdots \\ a_{m1} \\ \vdots \\ a_{mn} \end{pmatrix}$$

   $a_{11} \ldots a_{1n}$ - 1. Zeile der Matrix.
   Lineare Abbildung der Matrix

$$\begin{pmatrix} a_{11} & a_{12} & a_{1m} \\ a_{21} & & a_{2n} \\ \vdots & & \\ a_{n1} & a_{n1} & a_{nn} \end{pmatrix} \begin{matrix} v_1 \\ \vdots \\ \\ v_n \end{matrix}$$
$$w_1 \; w_2 \ldots w_m$$

   Die Abbildung gibt sich als

$$w \to \sum_{j,j} |y_i\rangle \cdot (w_j, w)$$

(w_j, w) Skalarprodukt

$w = \sum a_j w_j$ dann $(w_j, w) = c_j$

Matrix zu

$$|00\rangle + |11\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \begin{matrix} \rceil \text{ 1. Zeile} \\ \\ \rceil \text{ 2. Zeile} \end{matrix}$$

Matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ Identität

$$|x\rangle \to |0\rangle \cdot (|0\rangle, |x\rangle) + |1\rangle \cdot (|1\rangle, |x\rangle)$$
$$= \begin{pmatrix} x_0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ x_1 \end{pmatrix}$$
$$= \begin{pmatrix} x_0 \\ x_1 \end{pmatrix}$$
$$= x$$

$$\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|00\rangle + |01\rangle = |0\rangle \otimes (|0\rangle + |1\rangle)$$

Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$. Rang 1.

$$|V\rangle = \sum a_i |v_i\rangle = \sum a_i cdot c_i |v_i w_j\rangle$$
$$|w\rangle = \sum c_j |w_j\rangle$$

Tensorvektoren $|v\otimes\rangle|w\rangle$ sind Abbildungen von Rang 1.

Das Bild hat die Basis x (alle Spalten der Matrix sind Vielfache von v). Matrix ist

$$\begin{pmatrix} a_1c_1 & a_1c_2 & \cdots & a_1c_m \\ a_2c_1 & a_2c_2 & \cdots & a_2c_m \\ \vdots & \vdots & \ddots & \vdots \\ a_nc_1 & a_nc_2 & \cdots & a_nc_m \end{pmatrix}$$

Wie arbeitet man mit $V \otimes W$?

Ist M eine Matrix über V und will man diese Matrix auf das V von $V \otimes W$ anwenden, so sollte es so aussehen

$|v_i w_j\rangle \to (M|v_i) \otimes w_j$ (w_j bleibt unberührt)

$= v_i \otimes w_j$, Basisvektor von $V \otimes W$.

$$\begin{pmatrix} * & & & \\ 0 & * & & \\ & & * & \\ & & & \\ * & & & \\ & * & & \\ 0 & & * & \end{pmatrix} \begin{matrix} v_1w_1 \\ \\ v_nw_m \\ \\ \\ \\ \end{matrix}$$
$$v_1w_1 \; v_1w_m \cdots \; v_nw_1 \cdots \; v_nw_m$$

Das selbe mit $M|v_2$ Hier $M|v_n$

Es steht nur an den Einträgen der Art $(v_i w_j, v_{i'} w_j)$ $(w_j = w_j)$ ein Wert $\neq 0$.

Kroneckerprodukt von Matrizen. Die obige Matrix ist

$$M \otimes I_m = \begin{pmatrix} a_{11} \cdot I_m & \\ \vdots & \\ a_{m1} \cdot I_m & \end{pmatrix}$$

$M \ldots M$ auf V

$I_m \ldots$ Identität auf W

$$M = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mm} \end{pmatrix}$$

Es gilt: M orthogonal $\Leftrightarrow$ $M \otimes I$ orthogonal.

Analog

$$I_n \otimes N = \begin{pmatrix} N & 0 & 0 \\ 0 & N & 0 \\ 0 & 0 & N \end{pmatrix}$$

$N \ldots$ auf W

Ebenso (nicht mehr so leicht zu schätzen):

M auf Faktoren $i_1, i_2, \ldots, i_k$ von $V_1 \otimes V_2 \ldots \otimes V_n$

Wie jetzt bei $V \otimes W$ M auf V danach N auf W.

Sollte setzen $M \otimes N \leftarrow$ Kroneckerprodukt

$$= \begin{pmatrix} a_{11} \cdot N & a_{12} \cdot N & \cdots \\ \vdots & & \\ & & \\ & & \end{pmatrix}$$

$$M = \begin{pmatrix} a_1 1 & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_m 1 & \cdots & a_{mm} \end{pmatrix}$$

$|v_i w_j\rangle \to M|v_i\rangle \otimes N|w_j\rangle$ (Spalte i von M_i) $\otimes$ (Spalte j von N)

Übung

$M \otimes N = (M \otimes Id) \cdot (Id \otimes N)$

Allgemein sollte sein:

$M \cdot M' \otimes N \cdot N' = (M \otimes N) \cdot (M' \otimes N')$

6 Deutsch's Algorithmus

Folgendes Problem wurde von David Deutsch um 1980 eingeführt.

Gegeben ist eine Funktion $f : \{0,1\} \to \{0,1\}$.

Gefragt ist, ob f die konstante Funktion ist oder nicht.

Ein deterministischer Algorithmus muss $f\,(0)$ und $f\,(1)$ kennen, also f zweimal aufrufen, um das Problem richtig zu lösen.

Wir stellen f durch $f_\oplus$ dar:

$$f_\oplus : \{0,1\}^2 \longrightarrow \{0,1\}^2 \;\; (a,b) \longmapsto (a, b \oplus f(a))\,.$$

Also $f(a,0) = (a, f(a))$. Halten wir $f(a)$ fest, so ist bei $f(a) = 0$, $b \oplus f(a) = b$ für $b = 0, 1$. Bei $f(a) = 1$ ist $b \oplus f(a) = \neg b$ für $b = 0, 1$.

Wir nehmen an, wir haben ein Quantenprogramm U für $f_\oplus$ gegeben.

Ist $f(a) = a$ die Identität, so ist

$$U = |0\rangle\langle 0| \otimes I_2 + |1\rangle\langle 1| \otimes X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Ist $f(a) = 1$, so ist

$$U = I_2 \otimes X = |0\rangle\langle 0| \otimes X + |1\rangle\langle 1| \otimes X = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Und die übrigen 2 Fälle gehen ebenso. Die Aufgabe ist es also zu unterscheiden, ob

$$U = |0\rangle\langle 0| \otimes I_2 + |1\rangle\langle 1| \otimes X \text{ oder } |0\rangle\langle 0| \otimes X + |1\rangle\langle 1| \otimes I_2$$

oder aber ob

$$U = |0\rangle\langle 0| \otimes I_2 + |1\rangle\langle 1| \otimes I_2 = I_2 \otimes I_2 \text{ oder } |0\rangle\langle 0| \otimes X + |1\rangle\langle 1| \otimes X = I_2 \otimes X$$

Wir betrachten also ein Register von 2 QBits und der Startzustand ist $|A\rangle_0\rangle = |00\rangle$. Führen wir jetzt U aus, so bekommen wir den Zustand $|0f(0)\rangle$. Damit können wir kaum etwas anfangen. Wenden wir vorher noch X auf das 1. QBit an, so bekommen wir $|1, f(1)\rangle$ Also H_2 auf des erste QBit. Wir bekommen *beide* Eingaben in einem Zustand:

$$|A_1\rangle = \frac{1}{\sqrt{2}} \cdot (|0\rangle + |1\rangle \otimes |0\rangle) = \frac{1}{\sqrt{2}} \cdot (|00\rangle + |10\rangle)\,.$$

Wir wenden U an und bekommen

$$|A_2\rangle = \frac{1}{\sqrt{2}} \cdot (|0f(0)\rangle + |1f(1)\rangle)\,.$$

Wir haben mit $|A_2\rangle$ einen Zustand, der $f(0)$ und $f(1)$ enthält – und das obwohl wir U nur einmal aufgerufen haben. Wir müssen aber herausbekommen, ob $f(0) = f(1)$ oder nicht. Wir könnten messen, bekommen dann aber nur $f(0)$ oder $f(1)$ heraus. Hier sieht man eines der Hauptprobleme des Quantencomputing: Wie bekommt man aus einem Zustand die dort enthaltene Information heraus? Ein Zustand kann nicht einfach durchgelesen werden.

Wir haben bis jetzt das Programm:

Programm 1

Nehmen wir einmal an, dass $f(0) = f(1) = c$ ist. Dann $|A_2\rangle = \frac{1}{\sqrt{2}} \cdot (|0\rangle + |1\rangle) \otimes |c\rangle$. Wir wenden H_2 auf das erste QBit an und bekommen $|c\rangle$. Interessant ist hier, dass wir auf der Eingabe, dem 1. QBit, weiterrechnen. Da das Ergebnis in den beiden Fällen das Gleiche ist, überlagern sich die Rechnungen auf den beiden Werten des 1. QBits, $H_2|0\rangle + H_2|1\rangle = \frac{2}{\sqrt{2}} \cdot |0\rangle$ und die Amplitude des Zustands $|1\rangle$ summiert sich zu 0.

Was passiert, wenn $f(0) = 1$ und $f(1) = 0$ ist? Dann ist $|A_2\rangle = \frac{1}{\sqrt{2}} \cdot (|01\rangle + |10\rangle)$. Die Anwendung von H_2 auf das erste QBit ergibt

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

Wir brauchen auch Fall, dass $f(0) \neq f(1)$ Überlagerung ist. Die Idee ist, mit dem 2. QBit in den Zustand $|B\rangle = \frac{1}{\sqrt{2}} \cdot (|0\rangle - |1\rangle)$ zu versetzen, bevor U angewandt wird. Dann ist $U(|1\rangle \otimes |B\rangle) = |a\rangle \otimes |B\rangle)|a\rangle \otimes (|0\rangle - |1\rangle) - |B\rangle)$. Das 2. QBit bleibt in B und es findet immer Überlagerung statt.

6.1 Deutsch-Josza

7 Eigenwertermittlung (phase estimation)

Ist U unitär, so wissen wir

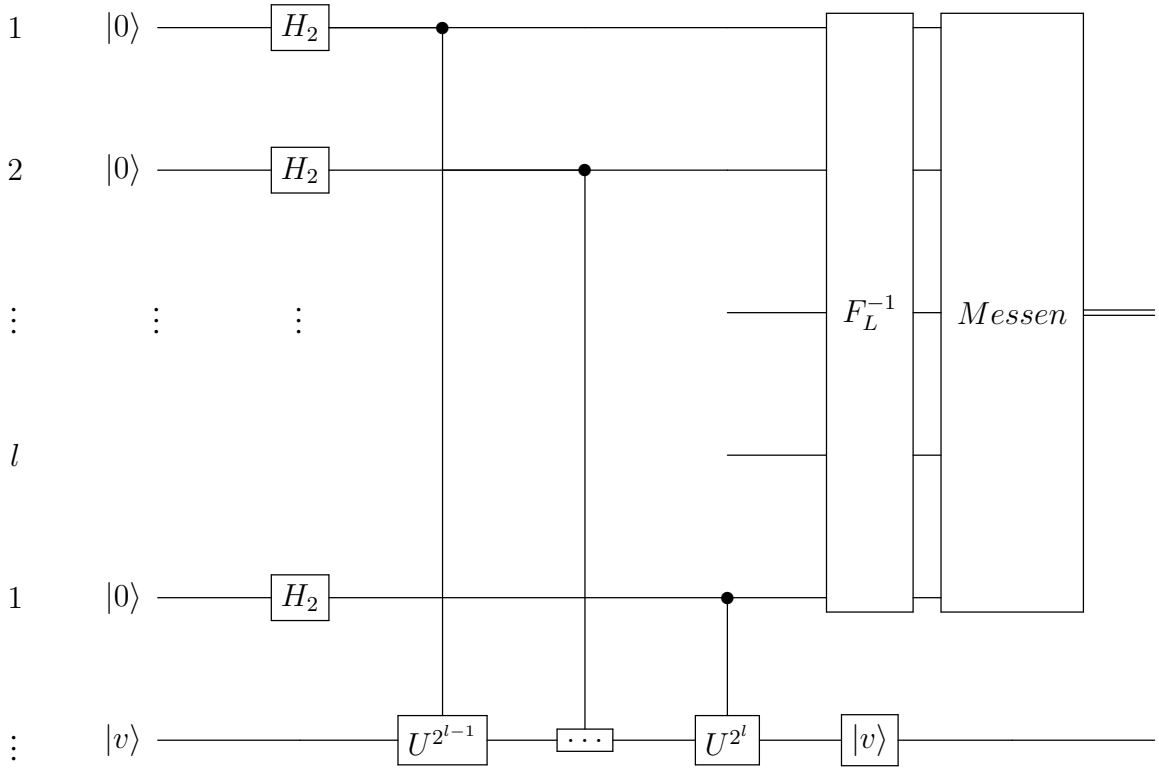
$$U = \exp(2\pi i \cdot \phi_0) \cdot |v_0\rangle\langle v_0| + \cdots + \exp(2\pi i \cdot \phi_{N-1}) \cdot |v_{N-1}\rangle\langle v_{N-1}|,$$

dabei sind die $|v_j\rangle$ orthogonale Eigenvektoren von U und $0 \leq \phi_j < 1$ sind reelle Zahlen.

Wir stellen folgende Aufgabe: Wir haben ein Register von n QBits, $N = 2^n$ und betrachten die unitäre $N \times N$-Matrix U auf dem Register. Wir haben Quantenprogramme für $U, U^2, U^{2^2} \ldots, U^{2^l}$ und auch für die durch ein weiteres QBit kontrollierten Versionen zur Verfügung. Außerdem haben wir einen Eigenvektor $|v\rangle = |v_j\rangle$ von U als Zustand

des Registers gegeben. Wir wollen den zugehörigen Eigenwert, also das $\phi = \phi_j$ ermitteln. Dazu verwenden wir ein weiteres Register von l QBits und betrachten Programm 1. Immer ist $L = 2^l$. Die oberen l QBits bezeichnen wir als das 1. Register, die unteren n sind das 2.

Programm 2



Abgesehen von den kontrollierten U^m hat das Programm eine Komplexität von $O(l^2)$: Es besteht aus l-mal H_2 und $O(l^2)$ vielen elementaren Matrizen für das F_L^{-1}. Das Messen zählen wir mit $O(l)$. Wir werden sehen, dass wir bei $l = O(n)$ das ϕ bis auf einen additiven Fehler vom Betrag $\leq \frac{1}{2^{n+1}}$ ermitteln können. Das läßt insofern hoffen, da das klassische Verfahren, die Gleichung $U|v\rangle = z \cdot |v\rangle$ nach z zu lösen, N Schritte erfordert.

Wir verwenden folgende Notation für die Binärdarstellung: Für $a_j \in \{0,1\}$ ist

$$(a_1 \dots a_k)_2 = \sum_{j=1}^{k} a_j \cdot 2^{k-j} \text{ und } (0.a_1 \dots a_k)_2 = \sum_{j=1}^{k} \frac{a_j}{2^j} = \frac{(a_1 \dots a_k)_2}{2^k}.$$

Für das Messergebnis $a_1 \dots a_l$ von Programm 2 gilt:

1. Ist ϕ als Binärbruch mit l Nachkommastellen darstellbar, so ist immer (Wahrscheinlichkeit 1) $\phi = (0.a_1 \dots a_l)_2$.

2. Für beliebiges ϕ gilt: Mit Wahrscheinlichkeit $\geq \frac{4}{\pi^2} = 0.405\dots$ ist $(0.a_1 \dots a_l)_2$ die beste l-Bit Approximation von ϕ.

Der Vorteil von Eigenvektoren ist: Die Multiplikation einer Matrix mit einem ihrer Eigenvektoren ist die einfache Multiplikation mit einem Skalar. Da für jede Matrix M und Skalar z gilt $M \cdot z|x\rangle = z \cdot M|x\rangle$ überträgt sich das auf die Potenzen der Matrix. Also

$$U|v\rangle = \exp(2\pi i \cdot \phi) \cdot |v\rangle \text{ und } U^m|v\rangle = \exp(2\pi i \cdot \phi \cdot m) \cdot |v\rangle \text{ für } m \in Z.$$

Beweis von 1. Wir nehmen an, dass $\phi = (0, a_1 a_2 \dots a_t)_2$, $t \leq l$ (l aus Programm 2). Wir geben einen Zustand $|B\rangle$ von l QBits, aus dem wir das ϕ ermitteln können. Wir sehen später, wie wir $|B\rangle$ aus dem Eigenvektor $|v\rangle$ mit Hilfe der U^m erzeugen können, ohne ϕ explizit zu kennen.

$$|B\rangle = \frac{1}{\sqrt{2^l}} \sum_{h_j=0,1} \exp(2\pi i \cdot \phi \cdot (h_1 \dots h_l)_2) \, |h_1 \dots h_l\rangle$$

$|B\rangle$ ist die Spalte $a_1 \dots a_t 0 \dots 0$ ($l-t$ Nullen angehängt) der $L \times L-$ Fouriermatrix, $L = 2^l$. Das folgt, da wir schreiben können $\phi = \frac{(a_1 \dots a_t 0 \dots 0)_2}{2^l}$ also

$$\exp(2\pi i \cdot \phi \cdot (h_1 \dots h_l)_2) = \exp\left(\frac{2\pi i}{2^l} \cdot (h_1 \dots h_l)_2 \cdot (a_1 \dots a_t 0 \dots 0)_2\right).$$

Wenden wir F_L^{-1} auf $|B\rangle$ an, so bekommen wir den Zustand $|a_1 \dots a_t 0 \dots 0\rangle$ und haben ϕ. Da wir $a_1 \dots a_t$ auf l Stellen auffüllen müssen um auf eine Spalte der $L \times L$-Fouriermatrix zu bekommen, muss $l \geq t$ sein.

Wie bekommen wir $|B\rangle$? Nach unserer Annahme ist $\exp(2\pi i \cdot \phi)$ Eigenwert zum Eigenvektor $|v\rangle$ von U. Damit ist

$$U^{(h_1 \ldots h_l)_2}|v\rangle = \exp(2\pi \cdot \phi \cdot (h_1 \ldots h_l)_2) \cdot |v\rangle.$$

Jetzt betrachten wir folgenden Zustand $|C\rangle$ des 1. Register mit l und des 2. Registers mit n QBits: Wir verschränken jedes $|h_1 \ldots h_l\rangle$ des ersten Registers mit $U^{(h_1 \ldots h_l)_2}|v\rangle$ des zweiten Registers.

$$\begin{aligned}
|C\rangle &= \frac{1}{\sqrt{2^l}} \sum_{h_j=0,1} |h_1 \ldots h_l\rangle \otimes U^{(h_1 \ldots h_l)_2}|v\rangle \\
&= \frac{1}{\sqrt{2^l}} \sum_{h_j=0,1} |h_1 \ldots h_l\rangle \otimes \exp(2\pi i \cdot \phi \cdot (h_1 \ldots h_l)_2)\,|v\rangle \\
&= \frac{1}{\sqrt{2^l}} \sum_{h_j=0,1} \exp(2\pi i \cdot \phi \cdot (h_1 \ldots h_l)_2) \cdot |h_1 \ldots h_l\rangle \otimes |v\rangle = |B\rangle \otimes |v\rangle.
\end{aligned}$$

Der letzte Schritt ist der entscheidende Umformungsschritt:

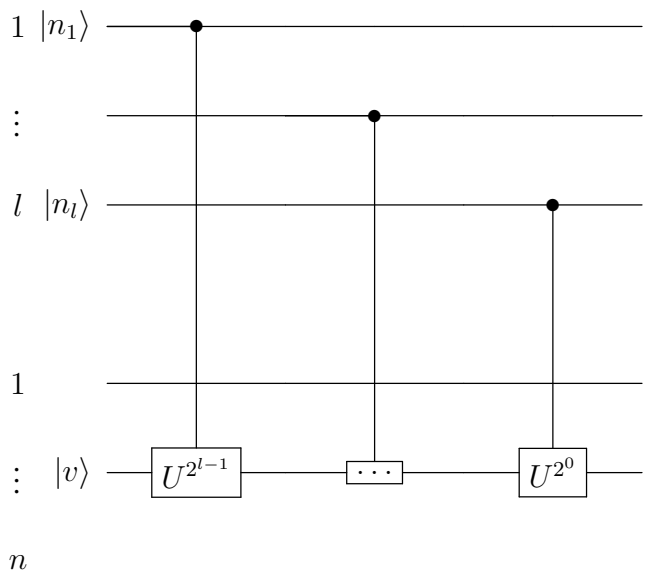
Der Eigenwert $\exp(2\pi i \cdot \phi \cdot (h_1 \ldots h_l)_2)$ von $U^{(h_1 \ldots h_l)_2}$ wird als skalarer Faktor von $|h_1 \ldots h_l\rangle$ dargestellt, und wir bekommen $|B\rangle$ im 1. Register; und das 1. Register ist nicht verschränkt mit dem 2. – das ist wichtig! (Man nennt diesen letzten Umformungsschritt gerne *Eigenvalue kick-back*.) Wenden wir F_L^{-1} auf das erste Register an ($F_L^{-1} \otimes Id_N$ auf beide Register), so ergibt sich $|a_1 \ldots a_t 0 \ldots 0\rangle \otimes |v\rangle$.

Wie bekommen wir $|C\rangle$? Es ist

$$U^{(h_1 \ldots h_l)_2} = U^{h_1 \cdot 2^{l-1}} \cdot U^{h_2 \cdot 2^{l-2}} \cdot \ldots \cdot U^{h_{l-1} \cdot 2^1} \cdot U^{h_l \cdot 2^0}$$

$U^{h \cdot m}$ für $h = 0, 1$ ist die kontrollierte Version von U^m mit h im Kontrollbit. Programm 3 liefert den Summanden $|h_1 \ldots h_l\rangle \otimes U^{(h_a \ldots h_l)_2}|v\rangle$ von $|C\rangle$. $|C\rangle$ selbst bekommen wir mit Eingabezustand $\frac{1}{\sqrt{2^l}} \sum_{h_i} |h_1 \ldots h_l\rangle$ im ersten Register.

Programm 3



$|n_1 - n_l \otimes |v\rangle\rangle$ $\qquad\qquad$ $|n_1 - n_l\rangle \otimes U^{(n_1-n_l)_2}|v\rangle$

Für Programm 2 mit Eingabezustand $|A_0> = \ |0\ldots0> \ \otimes |v>$ gilt:

$$
\begin{aligned}
|A_1\rangle &= \frac{1}{\sqrt{2^l}}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes \cdots \otimes (|0\rangle + |1\rangle) \otimes |v\rangle \\
&= \frac{1}{\sqrt{2^l}} \sum_{h_j=0,1} |h_1 \ldots h_l\rangle \otimes |v\rangle \\
|A_2\rangle &= |C\rangle \qquad \text{(Programm 3)} \\
|A_3\rangle &= |a_1 \ldots a_t 0 \ldots 0\rangle \otimes |v\rangle \quad (|A_2\rangle = |B\rangle \otimes |v\rangle).
\end{aligned}
$$

Da $\phi = (0.a_1 \ldots a_t)_2$, ist Aussage **1** gezeigt.

Beweis von 2. Im Beweis von **1** ist wichtig, dass ϕ ein endlicher Binärbruch ist (damit $|B\rangle$ gleich einer Spalte der Fouriermatrix ist). Schon bei $\phi = \frac{1}{3} = (0.010101...)_2$ funktioniert die Analyse nicht mehr. (Beachte, es ist

$$\phi = \frac{1}{4} + \frac{1}{4^2} + \frac{1}{4^3} + \cdots = \sum_{j \geq 1} \left(\frac{1}{4}\right)^j = \frac{1}{4} \cdot \frac{1}{1 - \frac{1}{4}} = \frac{1}{3}$$

mit der geometrischen Reihe $\sum_{j \geq 0} x^j = \frac{1}{1-x}$, für $|x| < 1$, der zusätzliche Faktor von $\frac{1}{4}$, da wir mit $j = 1$ anfangen.) Im Allgemeinen können wir ϕ nur noch näherungsweise ermitteln. Der Eigenwert $\exp(2\pi i \cdot \phi)$ liegt in der Gausschen Zahlenebene auf dem Einheitskreis (Radius 1, Umfang 2π). Wir stellen ϕ selbst auf dem Kreis mit Radius $\frac{1}{2\pi}$ und Umfang 1 dar.

Die Binärbrüche $(0.a_1 \ldots a_l)_2$ durchlaufen alle $\frac{k}{2^l}$, $0 \leq k \leq 2^l - 1$. Für $k \geq 1$ sagen wir $\frac{k}{2^l}$ ist beste l-Bit Approximation von ψ, Bezeichnung $A_l(\psi)$, genau dann, wenn $\frac{k}{2^l} - \frac{1}{2^{l+1}} \leq \psi \leq \frac{k}{2^l} + \frac{1}{2^{l+1}}$. Für $k = 0$ haben wir für $1 - \frac{1}{2^{l+1}} \leq \psi \leq \frac{1}{2^{l+1}}$. Man bekommt $A_l(\psi)$ durch Runden des $l+1$'ten Nachkommabits (und falls nötig Weglassen der 1).

Lemma 1. *(a) Für* $0 \leq \psi \leq 1 - \frac{1}{2^{l+1}}$ *ist* $\frac{-1}{2^{l+1}} \leq \psi - A_l(\psi) \leq \frac{1}{2^{l+1}}$.
(b) Für $1 > \psi \geq 1 - \frac{1}{2^{l+1}}$ *ist* $0 > \psi - A_l(\psi) \geq 1 - \frac{1}{2^{l+1}}$.

Bei allgemeinem ϕ betrachten wir $|B\rangle$ wie im Beweis von **1**.

$$|B\rangle = \frac{1}{\sqrt{2^l}} \sum_{h_j = 0,1} \exp(2\pi i \cdot \phi \cdot (h_1 \ldots h_l)_2) \, |h_1 \ldots h_l\rangle$$

Um zu sehen, was F_L^{-1} auf $|B\rangle$ bewirkt, schauen wir uns jeden Summanden von $|B\rangle$ einzeln an:

$$\exp(2\pi i \cdot \phi \cdot (h_1 \ldots h_l)_2) \, |h_1 \ldots h_l\rangle \longmapsto$$
$$\frac{1}{\sqrt{2^l}} \sum_{k_j = 0,1} \exp(2\pi i \cdot \phi \cdot (h_1 \ldots h_l)_2) \cdot \exp\left(-\frac{2\pi i}{2^l} \cdot (k_1 \ldots k_l)_2 \cdot (h_1 \ldots h_l)_2\right) |k_1 \ldots k_l\rangle =$$
$$\frac{1}{\sqrt{2^l}} \sum_{k_j = 0,1} \exp\left(2\pi i \cdot \left(\phi \frac{(k_1 \ldots k_l)_2}{2^l}\right) \cdot (h_1 \ldots h_l)_2\right) |k_1 \ldots k_l\rangle$$

$|D\rangle = F_L^{-1}|B\rangle$ bekommen wir, indem der vorherige Zustand über die h_i summiert und mit $\frac{1}{\sqrt{2^l}}$ multipliziert wird (wir haben noch die Summationsreihenfolge vertauscht):

$$|D\rangle = \frac{1}{2^l} \sum_{k_j=0,1} \sum_{h_i=0,1} \exp\left(2\pi i \cdot \left(\phi - \frac{(k_1 \dots k_l)_2}{2^l}\right) \cdot (h_1 \dots h_l)_2\right) |k_1 \dots k_l\rangle$$

Wir kürzen die Amplitude von $|k_1 \dots k_l\rangle$ ab,

$$\alpha(k_1, \dots, k_l) := \sum_{h_i=0,1} \exp\left(2\pi i \cdot \left(\phi - \frac{(k_1 \dots k_l)_2}{2^l}\right) \cdot (h_1 \dots h_l)_2\right).$$

Damit ist $|D\rangle = \frac{1}{2^l} \cdot \sum_{k_j} \alpha(k_1, \dots, k_l) \cdot |k_1 \dots k_l\rangle$.

Ist $\phi = (0.a_1 \dots a_l)_2$ ein Binärbruch mit l Nachkommastellen, dann ist $|D\rangle = |a_1 \dots a_l\rangle$. Das folgt direkt aus der geometrischen Reihe, da
$\exp\left(2\pi i \cdot \frac{(a_1 \dots a_l)_2 - (k_1 \dots k_l)_2}{2^l}\right)$ eine 2^l-te Einheitwurzel ist. Für den Fall, dass ϕ nicht als Binärbruch mit l Nachkommastellen darstellbar ist, benötigen wir das $A_l(\phi)$. Folgendes Lemma besagt: Messen wir $|D\rangle$, so sehen wir $A_l(\phi)$ mit einer Wahrscheinlichkeit von mindestens $\frac{4}{\pi^2}$.

Lemma 2. *Sei $A_l(\phi) = (0.a_1 \dots a_l)_2$, dann ist*

$$\left(\frac{1}{2^l} \cdot |\alpha(a_1, \dots, a_l)|\right)^2 \geq \frac{4}{\pi^2} \approx 0.405\dots$$

Beweis: Wir kürzen ab $\delta := \phi - A_l(\phi)$ und

$$\alpha := \alpha(a_1, \dots, a_l) = \sum_{h_i} \exp\left(2\pi i \cdot \delta \cdot (h_1 \dots h_l)_2\right).$$

Nach Lemma 1 ist $\frac{-1}{2^{l+1}} \leq \delta \leq \frac{1}{2^{l+1}}$ oder $0 > \delta \geq 1 - 2^{l+1}$

Zunächst etwas zur Intuition: Nehmen wir einmal an $\delta = \frac{1}{2^{l+1}}$. α ist die Summe von 2^l Summanden, der 2^{l+1}'ten Einheitswurzeln zwischen 1 für $h_1 = \dots = h_l = 0$ und fast -1 für $h_1 = \dots = h_l = 1$. Diese Summanden liegen alle auf der oberen Hälfte des Einheitskreises der Gausschen Zahlenebene. Der Realteil dieser Summe ist nur 1 da jeder Realteil außer der zum Winkel 0 einmal positiv und einmal negativ auftritt. (Realteil = Kosinus). Aber die Imginärteile haben alle positives Vorzeichen und addieren sich auf. Für die 2^{l-1} Winkel zwischen $\frac{\pi}{4}$ und $\frac{3\pi}{4}$ ist der Sinus $\geq \sin\left(\frac{\pi}{4}\right) = \frac{1}{\sqrt{2}} \approx 0.7$. Damit wird

der Imaginärteil von $\alpha \geq 2^{l-1} \cdot 0.7$, also $|\alpha|^2 \geq 2^{2l} \cdot 0.49/4$. Für kleinere $\delta > 0$ geht es ähnlich, $|\alpha|$ wird nur größer. Für $\delta = 0$ ist $\alpha = 2^l$.

Der eigentliche Beweis. Wir beschränken uns auf $\frac{1}{2^{l+1}} \geq \delta > 0$ (die anderen Fälle gehen analog). Die geometrische Reihe ergibt

$$\alpha = \frac{1 - \exp\left(2\pi i \cdot \delta \cdot 2^l\right)}{1 - \exp(2\pi i \cdot \delta)} \text{ und } |\alpha| = \frac{\left|1 - \exp\left(2\pi i \cdot \delta \cdot 2^l\right)\right|}{|1 - \exp(2\pi i \cdot \delta)|}$$

Der Betrag einer komplexen Zahl ist die Länge in der Gaussschen Zahlenebene und damit geometrischen Argumenten zugänglich. Wir schätzen den Nenner von $|\alpha|$ nach oben ab (sieht man direkt am Einheitskreis, $1 - \exp(2\pi i \cdot \delta)$ ist die Vektorsubtraktion):

$$|1 - \exp(2\pi i \cdot \delta)| \leq 2\pi \cdot \delta.$$

Den Zähler Z schätzen wir nach unten ab: $Z := \left|1 - \exp\left(2\pi i \cdot d \cdot 2^l\right)\right|$ ist die Länge der Sehne des Einheitskreises, die die Punkte mit Winkel 0 und $2\pi \cdot \delta \cdot 2^l$ verbindet. Es ist $2\pi \cdot \delta \cdot 2^l \leq \pi$, hier ist wichtig, dass $\delta \leq 2^{l+1}$, (gilt da $A_l(\phi)$ die *beste* l-Bit Approximation ist). Wir schlagen einen Kreis Γ mit Radius $\frac{Z}{2}$ um den Mittelpunkt dieser Sehne. Da der Punkt mit Winkel $2\pi \cdot \delta \cdot 2^l$ auf der oberen Hälfte des Einheitskreises liegt, liegt die obere Hälfte von Γ über dem Einheitskreis. Daraus ergibt sich, dass die Hälfte des Umfangs von Γ mindestens so groß ist, wie der Bogen zwischen 0 und $2\pi \cdot \delta \cdot 2^l$ auf dem Einheitskreis, also $\pi \cdot \frac{Z}{2} \geq 2\pi \cdot \delta \cdot 2^l$, damit ist $Z \geq 4 \cdot \delta \cdot 2^l$. Insgesamt bekommen wir:

$$|\alpha| = \frac{\left|1 - \exp\left(2\pi i \cdot \delta \cdot 2^l\right)\right|}{|1 - \exp(2\pi i \cdot \delta)|} \geq \frac{4 \cdot \delta \cdot 2^l}{2\pi \cdot \delta} = 2^l \cdot \frac{2}{\pi}$$

und die Behauptung gilt. □

Damit gilt **2**, da $|A_2\rangle = |B\rangle \otimes |v\rangle$ wie im Beweis von **1** und $|A_3\rangle = |D\rangle \times |v\rangle$.

8 Zyklen in Permutationen

8.1 Permutationsmatrizen, Eigenwerte und Eigenvektoren

Als Beispiel betrachten wir die Permutation:

$$U = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 0 & 1 \end{pmatrix} \quad \text{also } 0 \longmapsto 2, 1 \longmapsto 4 \ldots$$

Eine Permutation läßt sich in disjunkte Zyklen zerlegen:

$$U = \begin{pmatrix} 1 & 4 \\ 4 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 2 & 3 \\ 2 & 3 & 0 \end{pmatrix}$$

Eine Permutation läßt sich durch eine Permutationsmatrix (pro Zeile und Spalte genau eine 1, sonst 0'en) darstellen:

$$U = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Die Matrix U realisiert $|0\rangle \longmapsto |2\rangle$, $|1\rangle \longmapsto |4\rangle, \ldots$ Die Zyklen der Permutation induzieren eine Zerlegung in disjunkte Teilräume, die von der Permutationsmatrix auf sich selbst abgebildet werden. Permutationsmatrizen sind unitär. Also existiert also eine Zerlegung

$$U = \exp(2\pi i \cdot \phi_0) \cdot |v_0\rangle\langle v_0| + \cdots + \exp(2\pi i \cdot \phi_4) \cdot |v_4\rangle\langle v_4|$$

wobei die $|v_j\rangle$ orthogonale Eigenvektoren und die $\exp(2\pi i \cdot \phi_j)$ die zugehörigen Eigenwerte sind. Wir können die Eigenvektoren so wählen, dass sie zu den durch die Zyklen auf sich selbst abgebildeten Teilräumen gehören.

Für $\begin{pmatrix} 1 & 4 \\ 4 & 1 \end{pmatrix}$ bekommen wir als Eigenvektoren:

$$|v_0\rangle = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \text{ mit Eigenwert } 1, \; |v_1\rangle = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ -1 \end{pmatrix} \text{ mit Eigenwert } -1$$

Ein Zyklus der Länge 2 hat die beiden zweiten Einheitswurzeln $1, -1$ als Eigenwert. Wir betrachten $\begin{pmatrix} 0 & 2 & 3 \\ 2 & 3 & 0 \end{pmatrix}$.

$$\text{Für } |v\rangle = \begin{pmatrix} a_0 \\ 0 \\ a_2 \\ a_3 \\ 0 \end{pmatrix} \text{ ist } U|v\rangle = \begin{pmatrix} a_3 \\ 0 \\ a_0 \\ a_2 \\ 0 \end{pmatrix} \text{ und außerdem } U^3|v\rangle = |v\rangle.$$

Wir nehmen an, dass $|v\rangle$ ein Eigenvektor mit Eigenwert $\exp(2\pi i \cdot \phi)$ von U ist. Dann ist

$$|v\rangle = U^3|v\rangle = \exp(2\pi i \cdot \phi \cdot 3) \cdot |v\rangle$$

Also muss der Eigenwert $\exp(2\pi i \cdot \phi)$ eine dritte Einheitwurzel sein. Wir konstruieren zu jeder dritten Einheitwurzel einen zugehörigen Eigenvektor. Wir haben

$$|v_2\rangle = \frac{1}{\sqrt{3}} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \text{ mit Eigenwert } 1.$$

Wir konstruieren einen Eigenvektor $|v\rangle$ zum Eigenwert $\exp\left(2\pi \frac{i}{3}\right)$. Dazu setzen $a_0 = 1$. In $U|v\rangle$ ist die 1 von Position 0 auf Position 2 gerutscht. Damit $\exp\left(2\pi \frac{i}{3}\right)$ Eigenwert von $|v\rangle$ ist, muss in $|v\rangle$ an der Position 2 das Inverse des Eigenwerts stehen, $a_2 =$

$\exp\left(-2\pi\frac{i}{3}\right)$. So geht es weiter: An Position 3 muss das Inverse zum Quadrat stehen $a_3 = \exp\left(-2\pi\frac{i}{3}\cdot 2\right)$. Gehen wir den Zyklus von 0 aus in die umgekehrte Richtung, so stehen dort die Potenzen des Eigenwerts selbst $\exp\left(2\pi\frac{i}{3}\right) = \exp\left(-2\pi\frac{i}{3}\cdot 2\right)$.

Fassen wir zusammen: Eigenwerte und Eigenvektoren einer Permutationsmatrix lassen sich aus den Zyklen der Permutation bestimmen. Ein Zyklus der Länge R führt zu den R'ten Einheitswurzeln als Eigenwerten. Um einen Eigenvektor $|v\rangle$ mit Eigenwert $\omega = \exp\left(2\pi\frac{i}{R}\cdot j\right)$, $0 \le j \le R-1$, zu bekommen, gehen wir so vor:

Wir wählen ein festes Element a des Zyklus.

- Die Position zu a von $|v\rangle$ setzen wir auf 1.
- Nehmen wir an, die Permutation realisiere $a \longmapsto b$, so wird bei Anwendung der Permutation auf $|v\rangle$ die 1 von Position a auf Position b gesetzt. Damit $|v\rangle$ Eigenwert ω haben kann, muss an Position b von $|v\rangle$ das ω^{-1} stehen. So geht es weiter, bei $b \longmapsto c$ bekommt die Position von c den Wert $\omega^{-2}\ldots$. Dieser Prozess endet an der Position d mit $d \longmapsto a$. d bekommt den Wert $\omega^{-(R-1)} = \omega$. Man bekommt dasselbe $|v\rangle$, wenn man Position e mit $e \longmapsto d$ auf ω^2 setzt $\ldots$.
- Schließlich wird der noch mit $\frac{1}{\sqrt{R}}$ multipliziert, um $|v\rangle$ zu normieren.

Lemma 3. *Wir betrachten den Zyklus zu a der Länge R. Sei $|v_j\rangle$ der wie oben konstruierte Eigenvektor mit Eigenwert* $\exp\left(2\pi\frac{i}{R}\cdot j\right)$, $0 \le j \le R-1$.

(a) Die Eigenvektoren $|v_0\rangle, \ldots, |v_{R-1}\rangle$ sind orthogonal.

(b) Es ist

$$\sum_{j=0}^{R-1} |v_j\rangle = \sqrt{R}\cdot|a\rangle$$

Beweis:

(a) Die Vektoren haben an den Positionen, die zum Zyklus von a gehören eine R-te Einheitswurzel $\left(\text{multipliziert mit } \frac{1}{\sqrt{R}}\right)$ und 0 auf den übrigen Postionen stehen. Wir betrachten $|v_j\rangle$ und $|v_h\rangle$. Für $h = j$ ist (Konjugieren nicht vergessen)

$$\langle v_j|v_j\rangle = \frac{1}{R}\cdot\sum_{r=0}^{R-1}\exp\left(\frac{2\pi i}{R}\cdot j\cdot r\right)\cdot\exp\left(-\left(\left(\frac{2\pi i}{R}\right)\cdot j\right)\cdot r\right) = 1.$$

Für $h \neq j$ ist

$$\langle v_h | v_j \rangle = \frac{1}{R} \cdot \sum_{r=0}^{R-1} \exp\left(\frac{2\pi i}{R} \cdot (h-j) \cdot r\right) = 0$$

mit der geometrischen Reihe. Man beachte, dass im letzten Fall immer $h - j \neq 0 \mod R$ ist.

(b) Wir kürzen ab $|v\rangle = \sum_{j=0}^{R-1} |v_j\rangle$. Jeder Summand von $|v\rangle$ hat an der Position von a den Wert $|1\rangle\sqrt{R} \cdot 1$ stehen also hat $|v\rangle$ den Wert $\sqrt{R}$ an dieser Position stehen. Sei b die Position, auf die a mit $1 \leq r \leq R-1$ Schritten der Permutation abgebildet wird. Der Eintrag von $|v_j\rangle$ an Position b ist $\exp\left(-\left(\frac{2\pi i}{R}\right) \cdot j \cdot r\right)$ multipliziert mit $\frac{1}{\sqrt{R}}$. Summieren wir diese Einträge über j so ergibt sich $\sum_{j=0}^{R-1} \exp\left(-\left(\frac{2\pi i}{R} \cdot j\right) \cdot r\right) = 0$ mit der geometrischen Reihe. □

Zu Aussage (b) des Lemmas: Da die $|v_j\rangle$ orthogonal, also linear unabhängig sind, ist es nicht überraschend, dass sich $|a\rangle$ als Linearkombination der $|v_j\rangle$ darstellen lässt. Dass die Darstellung so einfach ist, ist interessant.

8.2 Ermittlung der Zyklenlänge

Wir stellen uns folgende Aufgabe: U ist eine Permutationsmatrix auf n QBits, gesucht ist die Länge des Zyklus von $a = \alpha_1 \dots \alpha_n$. Programm 3 ist Programm 1 mit $|a\rangle$ als Startzustand des 2. Registers.

$|A_0\rangle$ $|A_1\rangle$ $|A_2\rangle$ $|A_3\rangle$

Programm 4

Wir bezeichnen mit R die gesuchte Länge des Zyklus. Ist $a_1 \dots a_l$ das Messergebnis von Programm 3, dann gelten folgende Aussagen:

1. Ist $R = 2^m$ eine Zweierpotenz, dann ist immer $a_{m+1} = \cdots = a_l = 0$ und die Wahrscheinlichkeit von $a_1 \dots a_l$ ist $\frac{1}{2^m}$

2. Für beliebiges R gilt: Sei $0 \leq j \leq R-1$, dann ist $(0.a_1 \dots a_l)_2$ die beste l-Bit Approximation von $\frac{j}{R}$ mit Wahrscheinlichkeit $\geq \frac{1}{R} \cdot \frac{4}{\pi^2} = \frac{1}{R} \cdot 0.405\dots$

Wir bezeichnen mit $a = b_0 \longmapsto b_1 \longmapsto b_2 \cdots \longmapsto b_{R-2} \longmapsto b_{R-1} \longmapsto b_0 = a$ den Zyklus von a. Das 2. Register hat nur die Zustände $|b_r\rangle$ mit Amplitude $\neq 0$. Es ist

$$|A_2\rangle = \frac{1}{\sqrt{2^l}} \cdot \sum_{h_i} |h_1 \dots h_l\rangle \otimes U^{(h_1 \dots h_l)_2} |b_0\rangle.$$

Für $(h_1 \dots h_l)_2 = r \mod R$, $0 \leq r \leq R-1$ ist $U^{(h_1 \dots h_l)_2}|b_0\rangle = |b_r\rangle$. Wir zerlegen das 2. Register nach den $|b_r\rangle$.

$$\begin{aligned} |A_2\rangle = \tfrac{1}{\sqrt{2^l}} \cdot \Big(& \sum_{(h_1 \dots h_l)_2 = 0 \mod R} |h_1 \dots h_l\rangle \otimes |b_0\rangle \\ + & \sum_{(h_1 \dots h_l)_2 = 1 \mod R} |h_1 \dots h_l\rangle \otimes |b_1\rangle \quad + \\ & \cdots \\ & \cdots \\ & \cdots \\ + & \sum_{(h_1 \dots h_l)_2 = R-1 \mod R} |h_1 \dots h_l\rangle \otimes |b_{R-1}\rangle \Big) \end{aligned}$$

Beweis von 1. Auf das erste Register von $|A_2\rangle$ wirkt die inverse Fouriertransformation. Die $|b_r\rangle$ sind unterschiedliche Basiszustände, und die Fouriertransformation arbeitet ohne weitere Überlagerung auf dem zu $|b_r\rangle$ gehörenden Zustand des 1. Registers. Sie bildet $\sum_{(h_1 \dots h_l)_2 = r \mod R} |h_1 \dots h_l\rangle$ auf folgenden Vektor ab $\big(L = 2^l\big)$:

$$\sum_{(h_1 \dots h_l)_2 = r \mod R} \frac{1}{\sqrt{L}} \sum_{k_j} \exp\left(-\frac{2\pi i}{L} \cdot (k_1 \dots k_l)_2 \cdot (h_1 \dots h_l)_2\right) \cdot |k_1 \dots k_l\rangle.$$

Die Spalten zu $h_1 \dots h_l$ mit $(h_1 \dots h_l)_2 = r \mod R$ von F_L^{-1} werden einfach addiert. Eine überlegung was im Falle $R = 2$ passiert, ist hilfreich für $R = 2^m$.

Nach Annahme ist $R = 2^m$. Damit gilt für $0 \leq r \leq R-1$ mit Binärdarstellung $r = (b_1 \dots b_m)_2$

$$(h_1 \dots h_l)_2 = r \mod R \Longleftrightarrow h_1 \dots h_l = h_1 \dots h_{l-m} b_1 \dots b_m.$$

Das heißt $h_1 \dots h_l$ hat auf den letzten m Stellen die Binärdarstellung von r. Der skalare Faktor zu $|k_1 \dots k_l\rangle$ in obigem Vektor ist damit:

$$\begin{aligned}
&\frac{1}{\sqrt{L}} \cdot \sum_{h_1,\dots,h_{l-m}} \exp\left(-\frac{2\pi i}{L}\,(k_1 \dots k_l)_2 \cdot ((h_1 \dots h_{l-m})_2 \cdot 2^m + (b_1 \dots b_m)_2)\right) \\
&= \frac{1}{\sqrt{L}} \cdot \sum_{h_1,\dots,h_{l-m}} \exp\left(-\frac{2\pi i}{2^{l-m}}(k_1 \dots k_l)_2 \cdot (h_1 \dots h_{l-m})_2\right) \cdot \exp\left(-\frac{2\pi i}{L}(k_1 \dots k_l)_2 \cdot r\right) \\
&= \frac{2^{l-m}}{\sqrt{L}} \cdot \exp\left(-\frac{2\pi i}{L}(k_1 \dots k_l)_2 \cdot r\right) \quad \text{wenn } (k_1 \dots k_l)_2 = 0 \mod 2^{l-m}
\end{aligned}$$

und 0 sonst, wegen der geometrischen Reihe.

Damit haben wir insgesamt

$$|A_3\rangle = \frac{2^{l-m}}{2^l} \cdot \sum_{r=0}^{R-1} \sum_{(k_1 \dots k_l)_2 = 0 \mod 2^{l-m}} \exp\left(-\frac{2\pi i}{L}\,(k_1 \dots k_l)_2 \cdot r\right) |k_1 \dots k_l\rangle \otimes |b_r\rangle$$

Für das Messergebnis $k_1 \dots k_l = k_1 \dots k_m 0 \dots 0$ ist die Amplitude von $|k_1 \dots k_l\rangle \otimes |b_r\rangle$ gleich $\frac{1}{2^m} \cdot \exp\left(-\frac{2\pi i}{L}\,(k_1 \dots k_l)_2 \cdot r\right)$. Damit wird jedes solche $k_1 \dots k_l$ mit Wahrscheinlichkeit $\frac{1}{2^{2m}} \cdot 2^m = \frac{1}{2^m}$ gemessen. Der Faktor $R = 2^m$ kommt von der Summation über r, und $\exp\left(-\frac{2\pi i}{L} \cdot (k_1 \dots k_l)_2 \cdot r\right)$ spielt bei der Wahrscheinlichkeit keine Rolle (konjugieren). Wir haben die uniforme Verteilung auf den $k_1 \dots k_l = k_1 \dots k_m 0 \dots 0$. Damit ist Aussage **1** bewiesen.

Beweis von 2. Bei allgemeinem R lassen sich die Summen im 1. Register von $|A_2\rangle$ nicht mehr so ohne weiteres ausrechnen. Schon bei $l = 3$ und $R = 3$ scheint die Situation ziemlich verworren.

2. Register	Summantionsindices für das 1. Register
$\|a_0\rangle$	$000, 011, 110$
$\|a_1\rangle$	$001, 100, 111$
$\|a_2\rangle$	$010, 101$

Hier kommen Lemma 3 und die Eigenwertermittlung zu Hilfe. Seien also $|v_j\rangle, 0 \leq j \leq R-1$ die Eigenvektoren mit Eigenwerten $\exp\left(\frac{2\pi i}{R} \cdot j\right)$ wie wir sie vor Lemma 3 konstruiert haben. Nach Lemma 3 (b) ist

$$|A_0\rangle = |0 \ldots 0\rangle \otimes |a\rangle = \sum_{j=0}^{R-1} \frac{1}{\sqrt{R}} \cdot |0 \ldots 0\rangle \otimes |v_j.$$

Wir zerlegen also das 2. Register nach den $|v_j\rangle$ anstelle der $|b_r\rangle$ im vorhergehenden Fall. Das heißt keineswegs, dass die $|v_j\rangle$ in irgendeinem Sinne vom Quantenprogramm erzeugt werden, sie dienen uns nur als Rechenhilfe. Programm 4 ist, abgesehen von der Eingabe Programm 2. Also betrachten wir Programm 1 auf den einzelnen Summanden $|0 \ldots 0\rangle \otimes |v_j\rangle$. Sei $|A_{3,j}\rangle$ der Zustand den Programm 2 mit Startzustand $|v_j\rangle$ im zweiten Register (anstelle von $|A_3\rangle$ und Eingabe $|v\rangle$) erzeugt. Wegen der Linearität ist bei Programm 4 $|A_3\rangle = \frac{1}{\sqrt{R}} \cdot \sum_j |A_{3,j}\rangle$. Wir zerlegen $A_{3,j}$ weiter als $|A_{3,j}\rangle = |D_j\rangle \otimes |v_j\rangle$. Programm 2 mit Eingabe $|v_j\rangle$ hat das Messergebnis $k_1 \ldots k_l$ mit Wahrscheinlichkeit $|\alpha_j (k_1 \ldots k_l)|^2$, wobei $\alpha_j (k_1 \ldots k_l)$ die Amplitude von $|k_1 \ldots k_l\rangle$ in D_j ist.

In der Regel addieren sich Wahrscheinlichkeiten von Messergebnissen nicht ohne weiteres, aber da die $|v_j\rangle$ orthogonal sind, ist folgendes Lemma zu erwarten. Wir beweisen es hier nicht; es lässt sich auf den verallgemeinerten Satz von Pythargoras zurückführen: Sind die $|x_1\rangle, \ldots, |x_m\rangle$ paarweise orthogonal, so ist

$$(\langle x_1| + \cdots + \langle x_m|) (|x_1\rangle + \cdots + |x_m\rangle) = \langle x_1|x_1\rangle + \cdots + \langle x_m|x_m\rangle,$$

die Länge zum Quadrat einer Summe ist gleich der Summe der einzelnen Längen zum Quadrat.

Lemma 4. *Die Wahrscheinlichkeit in* $|A_3\rangle = \frac{1}{\sqrt{R}} \cdot \sum_j |A_{3,j}\rangle$ *das Messergebnis* $k_1 \dots k_l$ *zu bekommen ist gleich* $\frac{1}{R} \cdot \sum_j |\alpha_j(k_1, \dots k_l)|^2$.

Damit ist **2** bewiesen, denn für $(0.a_1 \dots a_l) = A_l\left(\frac{j}{R}\right)$ ist wegen **2** von Programm 2 schon $|\alpha_j(a_1 \dots a_l)|^2 \geq \frac{4}{\pi^2}$. Es kommt dann höchstens noch etwas von den anderen $D_k, k \neq j$ zu der Wahrscheinlichkeit hinzu.

Wie kommen wir an die Länge des Zyklus R?

Es ist auf jeden Fall $1 \leq R \leq N, N = 2^n$. Nehmen wir an, wir wissen das dass $R = 2^m$, Zweierpotenz ist, es ist $m \leq n$ Wir wählen $l = n$. Mit Aussage **1** zu Programm 4 können wir R mit Wahrscheinlichkeit von $\frac{1}{2}$ an dem Messergebnis erkennen.

Für den allgemeinen Fall wählen wir $l = 2n$. Gegeben das Messergebnis $a_1 \dots a_l$ und wir nehmen an, es gibt ein $0 \leq j \leq R-1$ dass $(0.a_1 \dots a_l)_2 = A_l\left(\frac{j}{R}\right)$ (vgl. Aussage **2** von Programm 4). Mit Wahrscheinlichkeit $\geq R \cdot \frac{1}{R} \cdot \frac{4}{\pi^2} = \frac{4}{\pi^2}$ hat ein Messergebnis diese Eigenschaft. Die erste Aufgabe ist es, das $\frac{j}{R}$ selbst zu finden.

Die Menge der Kandidaten für $\frac{j}{R}$ ist die Menge aller Brüche $\frac{t}{T}$ mit $1 \leq T \leq N$ und $0 \leq t \leq T-1$. Das sind $\mathcal{O}(N^2)$ viele Kandidaten. Einige Kandidaten: Die kleinsten sind $0, \frac{1}{N}, \frac{1}{N-1}, \frac{1}{N-2}$, die größten $\frac{N-2}{N-1} = 1 - \frac{1}{N-1}, \frac{N-1}{N} = 1 - \frac{1}{N}$, und um $\frac{1}{2}$ herum haben wir $\frac{\frac{N}{2}}{N+1}, \frac{\frac{N}{2}}{N} = \frac{1}{2}, \frac{\frac{N}{2}}{N-1}$.

Folgendes Lemma erhellt unsere Wahl $l = 2n$.

Lemma 5. *Ist* $l \geq 2n$*, dann gibt es zu jedem Binärbruch* $(0.a_1 \dots a_l)_2$ *höchstens einen Kandidaten mit* $A_l\left(\frac{t}{T}\right) = (0.a_1 \dots a_l)_2$.

Beweis: Es ist $\left|\left(A_l\frac{t}{T}\right) - \frac{t}{T}\right| \leq \frac{1}{2^{l+1}} = \frac{1}{2N^2}$. Der einzige Kandidat mit $A_l\left(\frac{t}{T}\right) = 0$ ist $\frac{t}{T} = 0$. Insbesondere gibt es kein $0 > \frac{t}{T} \geq 1 - \frac{1}{2^{l+1}}$.

Für zwei Kandidaten $\frac{t}{T} \neq \frac{t'}{T'}$ gilt $\left|\frac{t}{T} - \frac{t'}{T'}\right| > N^2$, denn ist $T = T' = N$ so ist $\left|\frac{t}{T} - \frac{t'}{T'}\right| > \frac{1}{N}$ ist T oder $T' < N$ so ist $\left|\frac{t}{T} - \frac{t'}{T'}\right| \geq \frac{1}{T \cdot T'} > \frac{1}{N^2}$. Da $\left|\left(A_l\frac{t}{T}\right) - \frac{t}{T}\right| \leq \frac{1}{2N^2}$ folgt die Behauptung. □

Zwei Kandidaten $\frac{t}{T}, \frac{t'}{T'}$ haben den gleichen Wert genau dann wenn es eine natürliche Zahl $m \geq 1$ gibt so dass $t' = mT$ und $T' = mT'$, das heißt, sie gehen durch Erweitern

oder Kürzen auseinander vor. Wir beschränken uns jetzt auf Kandidaten mit ggt$(t, T) = 1$, dadurch gehen keine Werte verloren.

Kehren wir zurück zu unserer Aufgabe aus dem gegebenen $A_l(\frac{j}{R})$ das $\frac{j}{R}$ zu ermitteln. Wir testen für jeden Kandidaten $\frac{t}{T}$, ob $\left|A_l\left(\frac{j}{R}\right) - \frac{t}{T}\right| \leq \frac{1}{2N^2}$. Nach dem Lemma gilt das für genau einen Kandidaten $\frac{t}{T}$. Damit kennen wir den *Wert* von $\frac{j}{R}$ und wissen, es gibt ein $m \geq 1$, sodass $j = mt$ und $R = mT$.

Wenn ggT$(j, R) = 1$, dann ist $m = 1$ und wir haben das R. Nun sind solche j relativ rar, besser ist es folgendes Lemma zu verwenden.

Lemma 6. *Seien $A_l\left(\frac{j_1}{R}\right), \ldots, A_l\left(\frac{j_k}{R}\right)$ gegeben und seien $\frac{t_1}{T_1}, \ldots, \frac{t_k}{T_k}$ die zugehörigen Kandidaten (mit ggT$(t_i, T_i) = 1$). Falls ggT$(j_1, \ldots, j_k) = 1$, dann ist $R =$ kgV$(T_1, \ldots, T_k)$*

Beweis: Es ist $R = m_1 \cdot T_1 = \cdots = m_k \cdot T_k$ ein gemeinsames Vielfaches von $T_1, \ldots, T_k$. Da $j_1 = m_1 \cdot t_1, \ldots, j_k = m_k \cdot T_k$ und nach Voraussetzung ggT$(j_1, \ldots j_k) = 1$, ist erst recht ggT$(m_1 \ldots m_k) = 1$. Mit dem nächsten Lemma ist der Beweis abgeschlossen. □

Lemma 7. *Sei $R \geq 1$ ein gemeinsames Vielfaches von $T_1, \ldots, T_k \geq 1$, $R = m_i \cdot T_i$ $m_i \geq 1$ natürliche Zahlen. Es gilt*

$$ggT(m_1, \ldots, m_k) = 1 \Longleftrightarrow R = kgV(T_1 \ldots T_k).$$

Beweis: Wir denken an die Primfaktorzerlegung:

Die Primfaktorzerlegung von $kgV(T_1 \ldots T_k)$ hat den Faktor p^α genau dann wenn α der maximale Exponent ist, mit dem p in den T_i vorkommt. Sei $R >$ kgV$(T_1 \ldots T_k)$. Es gibt eine Primzahl p, so dass p^β in der Primfaktorzerlegung von R auftritt und für alle i tritt p in der Primfaktorzerlegung von T_i mit Exponenten höchstens $\beta - 1$ auf. Also muss p als Faktor in jedem m_i auftreten und ggT$(m_1 \ldots m_k) \geq p$.

Ist andererseits ggT$(m_1, \ldots, m_k) > 1$, dann muss $R >$ kgV$(T_1 \ldots T_k)$. □

Lemma 8. *Sei $R \geq 2, k \geq 2$, dann ist*

$$\#\{(j_1, \ldots, j_k) \,|1 \leq j_i \leq R - 1, ggT(j_1 \ldots j_k) = 1\} \geq 1 - 3 \cdot \left(\frac{1}{2}\right)^k.$$

Beweis: Wir beschränken $\#\{(j_1,\ldots,j_k)|1 \le j_i \le R-1, \text{ggT}\,(j_1\ldots j_k) \ge 2\}$.

Für $l \ge 1$ ist

$$\#\{j|1 \le j \le R-1, l \text{ teilt } j\} \le \frac{R}{l}$$
$$\#\{(j_1,\ldots,j_k)\,|1 \le j_i \le R-1, l \text{ teilt } j_1\ldots j_k\} \le \left(\frac{R}{l}\right)^k$$
$$\#\{(j_1,\ldots,j_k)\,|1 \le j_i \le R-1, \text{ggT}\,(j_1\ldots j_k) \ge 2\} \le \left(\frac{R}{2}\right)^k + \left(\frac{R}{3}\right)^k + \left(\frac{R}{4}\right)^k + \cdots$$

Es ist

$$\sum_{j\ge 2}\left(\frac{1}{j}\right)^k = \left(\frac{1}{2}\right)^k + \sum_{j\ge 3}\left(\frac{1}{j}\right)^k$$
$$\sum_{j\ge 3}\left(\frac{1}{j}\right)^k \le \int_{x=2}^{\infty}\left(\frac{1}{x}\right)^k dx = -\frac{1}{k-1}\cdot\left(\frac{1}{x}\right)^{k-1}\Bigg|_2^{\infty} = \frac{1}{k-1}\cdot\left(\frac{1}{2}\right)^{k-1}$$

Insgesamt haben wir $\left(\frac{1}{2}\right)^k + \frac{1}{(k-1)}\left(\frac{1}{2}\right)^{k-1} \le 3\cdot\left(\frac{1}{2}\right)^k$. □

Jetzt ist klar, was zu machen ist: Wir lassen Programm 4 zweimal laufen. Wir lesen die beiden Messergebnisse als Binärbruch und suchen die zugehörigen Kandidaten. Wir ermitteln das kleinste gemeinsame Vielfache der Nenner der Kandidaten und geben es als Vorschlag für R aus.

Für gegebenes j ist die Wahrscheinlichkeit, dass ein Messergebnis $A_l\left(\frac{j}{R}\right)$ liefert $\ge \left(\frac{1}{R}\right)\cdot\frac{4}{\pi^2}$. Die Wahrscheinlichkeit, dass wir bei zwei Messergnissen das geordnete Paar $(A_l\,(j_1R)\,, A_l\,(j_2R))$ bekommen, ist $\ge \left(\left(\frac{1}{R}\right)\cdot\frac{4}{\pi^2}\right)^2$. Mit Lemma bekommen wir ein Paar $\left(A_l\left(\frac{j_1}{R}\right), A_l\left(\frac{j_2}{R}\right)\right)$ mit ggT$(j_1,j_2) = 1$ mit Wahrscheinlichkeit $\ge \frac{1}{4}\cdot\left(\frac{4}{\pi^2}\right)^2 = \frac{4}{\pi^4} = 0.041\ldots$. Hier addieren sich die Wahrscheinlichkeiten auf!

9 Effizientes Finden des Kandidaten

Kettenbrüche

10 Faktorisieren und Ordnung

Die Addition ganzer Zahlen $\leq M$ braucht eine Zeit von $\mathcal{O}(\log M)$, die Multiplikation und ganzzahlige Division eine Zeit von $\mathcal{O}(\log M)^2$. Wir betrachten $Z_M = \{0, \ldots, M-1\}$. Zu Z_M gehören die modularen Operationen $a + b = (a + b) \mod M$, $-b = M - b$ und $(a - b) = (a - b) \mod M$ in Zeit $\mathcal{O}(\log M)$ und $a \cdot b = (a \cdot b) \mod M$ in Zeit $\mathcal{O}(\log M)^2$.

Das Finden des größten gemeinsamen Teilers von zwei Zahlen $M \geq N$ wird durch den Euklidischen Algorithmus in Zeit $\mathcal{O}(\log M)^3$ realisiert. Die Laufzeit ergibt sich aus $\mathcal{O}(\log M)$ ganzzahligen Divisionen, jede Division dauert $\mathcal{O}(\log M)^2$. Man kann sich ggT(M, N) gut mit der Primfaktorzerlegung von M, N vorstellen: In der Primfaktorzerlegung von ggT(M, N) kommt p^α vor genau dann, wenn die Primzahlpotenz p^α in der Primfaktorzerlegung M *und* N vorkommt.

Während es zu $m \in Z_M$ ein m' gibt mit $m + m' = 0$, $m' = -m$, gilt Analoges für die Multiplikation und die 1 nicht immer. Deshalb

$$Z_M^* = \{a \in Z_M | \text{ggT}(a, M) = 1\} = \{a \in Z_M | \text{es gibt} a^{-1} \text{ mit } a^{-1} \cdot a = 1\}$$

das heißt $a \in Z_M^*$ genau dann, wenn a und M teilerfremd sind, das heißt a hat ein multiplikatives Inverses. Es sind Z_M mit der Addition und Z_M^* mit der Multiplikation kommutative Gruppen, und man kann dort wie üblich rechnen. Wir betrachten $a \in Z_M^*$ und die Potenzen von a, $a_1 = a$, $a_2 = a^2 \mod M$, $a_3 = a^3 \mod M, \ldots$. Da Z_M^* endlich ist, gibt es ein $j > k$, sodass $a^k = a^j = a^{k+(j-k)}$, also $a^{j-k} = 1 \mod M$. Die Ordnung von a ist das kleinste $l \geq 1$, sodass $a^l = 1 \mod M$ Bezeichnung: $\text{Ord}_{M(a)}$. Kennen wir die Ordnung , so kennen wir die Potenzen von a in folgendem Sinne: $a \neq 1, a^2 \neq 1, a^3 \neq 1, \ldots, a^l = 1, a^{l+1} = a \ldots$. Man rechnet auf den Potenzen von a mit der Multiplikation wie in Z_l mit der Addition: Mit der Abbildung $a^k \longmapsto k \mod l$ haben wir $a^{k+m} = a^{(k+m) \mod l} \longmapsto (k + m) \mod l$. Insbesondere wissen wir $a^k = 1$ genau dann wenn $k = 0 \mod l$. Für a^k ist die Ordnung von a^k das kleinste $m > 0$, sodass $\left(a^k\right)^m = a^{km} = 1$ also $\text{Ord}_M\left(a^k\right) = \frac{l}{\text{ggT}(k,l)}$.

Es ist für $M, N \neq 0$ $M \cdot \frac{N}{\text{ggT}(M,N)} = \text{kgV}\,(M, N)$, das kleinste geminsame Vielfache von M und N. In der Primfaktorzerlegung von kgV (M, N) kommt p^α vor genau dann, wenn die Primzahlpotenz p^α in der Primfaktorzerlegungen von M *oder* N vorkommt. Also oben ist der Gesamtexponent von a um von a^k auf die 1 zu kommen $k \cdot \frac{l}{\text{ggT}(k,l)} = \text{kgV}\,(k, l)$.

10.1 Ordnung in $\mathbb{Z}_M^*$

Wir stellen uns folgende Aufgabe: Gegeben ist M und $a \in \mathbb{Z}_M^*$, und es soll $\text{Ord}_M(a)$ ermittelt werden. Ermitteln wir die Potenzen von a nacheinander, so dauert das im Worstcase $\mathcal{O}\,(M \cdot \log M)^2$, also exponentiell in der #Bits von M. Mit dem Quantenalgorithmus für die Zyklenlänge brauchen wir $\mathcal{O}\,(\log M)^3$.

Zunächst beobachten wir, dass die Multiplikation mit a eine Permutation auf ganz Z_M (nicht nur Z_M^*) ist. Das folgt, denn für $m \in Z_M$ ist $m \cdot a \cdot a^{-1} = m \cdot 1 = m$. Sei $N \leq 2M$ eine Zweierpotenz und $n = \log_2 N$. Die Permutation $U = U_a$ ist die Multiplikation mit a ergänzt durch die Identität auf den Elementen $\geq M$:

$$U = \begin{pmatrix} 0 & 1 & 2 & \dots & M-1 & M & \dots & N-1 \\ 0 \cdot a & 1 \cdot a & 2 \cdot a & \dots & (M-1) \cdot a & M & \dots & N-1 \end{pmatrix}$$

Der Zyklus von a besteht gerade aus den Potenzen von a und $\text{Ord}_M(a)$ ist gleich der Länge dieses Zyklus. Da 1 zu dem Zyklus gehört, ist die Länge des Zyklus von 1 auch gleich $\text{Ord}_M(a)$.

Da ein klassischer Algorithmus durch einen Quantenalgorithmus simuliert werden kann, haben wir für die Permutationsmatrix $U = U_a$ einen Quantenalgorithmus der Komplexität $\mathcal{O}(\log M)^2$. Es ist $U^2 = U_{a^2 \mod M}$ was ebenfalls zu einem Quantenalgorithmus der Komplexität $\mathcal{O}(\log M)^2$ führt. Ebenso für $U^k = U_{a^k \mod M}$. Wir betrachten folgendes

Programm:

Programm 5

Lassen wir Programm 5 zweimal laufen, so bekommen wir mit Wahrscheinlichkeit $\geq 0.041\ldots$ die Ordnung von a.

10.2 Teiler und Ordnung

In folgendem Satz betrachten wir Zahlen M, die ungerade sind, das heißt 2 kommt nicht in ihrer Primfaktorzerlegung vor und die mindestens 2 verschiedene Primteiler haben. Der Satz wird in diesem Abschnitt bewiesen. Man beachte, dass (b) uns einen Teiler $\neq 1, M$ von M gibt und dass $1 - \frac{1}{2^{k-1}} \geq \frac{1}{2}$ ist.

Satz 1 *Sei die Primfaktorzerlegung von $M = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_k^{\alpha_k}$, alle $p_i \geq 3$ und $k \geq 2$. Für mindestens $\left(1 - \frac{1}{2^{k-1}}\right) \cdot \#\mathbb{Z}_M^*$ aller $a \in \mathbb{Z}_M^*$ gelten (a) und (b):*

(a) $R = Ord_M(a)$ ist gerade.
(b) Es gilt $ggT\left(a^{\frac{R}{2}} - 1, M\right) \neq 1$ und $\neq M$.

Der chinesische Restsatz erhellt die Struktur von $\mathbb{Z}_M^*$.

Satz 2 *Sei $m = r \cdot s$ und r und s seien teilerfremd. Wir betrachten die Abbildung*

$$f : Z_m \longrightarrow Z_r \times Z_s, a \longmapsto (a \mod r, a \mod s)\,.$$

(a) Die Abbildung ist bijektiv.

(b) Es gilt

$$f\left((a+b) \mod m\right) = f(a) + f(b), f\left((a \cdot b) \mod m\right) = f(a) \cdot f(b)$$

Dabei ist $f(a) + f(b)$ und $f(a) \cdot f(b)$ definiert durch Rechnen auf den Koordinaten, das heißt,

$$(w,x) + (y,z) = ((w+y) \mod r, (x+z) \mod s)$$
$$(w,w) \cdot (y,z) = ((w \cdot y) \mod r, (x \cdot z) \mod s).$$

Beweis: (a) Zunächst einmal ist $\#\mathbb{Z}_m = r \cdot s = \#\mathbb{Z}_r \times \mathbb{Z}_s$. Also für die Bijektivität reicht es zu zeigen, dass die Abbildung injektiv ist, das heißt, aus $f(a) = f(b)$ folgt $a = b$ für alle $a, b \in \mathbb{Z}_m$. Zunächst, aus $f(a) = f(b)$ folgt $a \mod r = b \mod r$ und $a \mod s = b \mod s$. Also ist $a - b = 0 \mod r$ und $a - b = 0 \mod s$. Das gilt, denn wenn die Reste gleich sind, heben sie sich bei Subtraktion einfach zu 0 auf. Also ist $a - b$ ein Vielfaches von r und auch ein Vielfaches von s. Da r und s teilerfremd sind (!), ist $a - b$ ein Vielfaches von $r \cdot s = m$. Das kann man sich durch die Primfaktorzerlegungen von r und s verdeutlichen, die keine gemeinsame Primzahl haben. Also ist $a - b = 0 \mod m$ also $a \mod m = b \mod m$. □

Man sagt $\mathbb{Z}_m$ ist isomorph zu $\mathbb{Z}_r \times Z_s$, dass heißt, ob in $\mathbb{Z}_m$ oder in $\mathbb{Z}_r \times \mathbb{Z}_s$ gerechnet wird, ist gleich, man kann mit der Abbildung f und der Umkehrabbildung f^{-1} hin- und hergehen. Die Abbildung f heißt dann Isomorphismus. Als Nächstes einige Beobachtungen und Folgerungen aus der Isomorphie.

Folgerung 1 *(a) $f(1) = (1,1)$, $f(0) = (0,0)$, $f(-1) = (-1,-1)$.*

(b) $a \in Z_m^*$ genau dann, wenn $f(a) \in \mathbb{Z}_r^* \times \mathbb{Z}_s^*$. Insbesondere ist $\#\mathbb{Z}_m^* = \#\mathbb{Z}_r^* \times \mathbb{Z}_s^*$.

(c) Ist $a \in \mathbb{Z}_m^*$, $f(a) = (b,c)$ und sei $M = Ord_m(a), R = Ord_r(b), S = Ord_s(b)$, dann ist $M = kgV(R,S)$

(d) Ist $f(a) = (0,b)$ und $b \mod s \neq 0$ so ist $ggT(a,m) \neq 1$ und $\neq m$

Beweis:

(a) Es ist $(0,0) = f(1+(-1)) = f(1) + f(-1)$ also $f(-1) = (-1,-1)$. Beachte, dass immer $-1 = l - 1 \mod l$ ist.

(b) Es läßt sich dem Inversen argumentieren, da für $f(a) = (b,c)$ gilt $f(a^{-1}) = (b^{-1} \mod r, c^{-1} \mod s)$.

(c) Zunächst gilt wegen der Isomorphie, dass $f\left(a^k \mod m\right) = (a \mod r, a \mod s)^k$ (koordinatenweises Potenzieren). Ist k ein Vielfaches von R und S, dann muss $a^k = 1 \mod m$ sein. Ist k kein Vielfaches von R, so ist $a^k \mod r \neq$ und $a^k \mod m$ kann nicht gleich 1 sein.

(d) Die Voraussetzung an b bedeutet, dass a kein Vielfaches von s also von m ist. Aber es ist $a \mod r = 0$, also ist a Vielfaches von r.

Durch direkte Induktion über k lässt sich folgende Verallgemeinerung mit analogen Folgerungen wie oben, des chinesischen Restsatzes beweisen:

Satz 3 *Sei $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_k^{\alpha_k}$ die Primfaktorzerlegung von m, wir bezeichnen $q_i = p_i^{\alpha_i}$. Die Abbildung*

$$f : \mathbb{Z}_m \longrightarrow \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \mathbb{Z}_{q_k}, m \longmapsto (m \mod q_1, m \mod q_2, \ldots, m \mod q_k)$$

ist ein Isomorphismus.

Wir betrachten eine endliche Gruppe G mit m Elementen. G ist zyklisch genau dann, wenn es ein $g \in G$ gibt, sodass $G = \{g, g^2, \ldots, g^m\}$. Das Element g ist ein erzeugendes Element der Gruppe. Zum Beispiel ist $\mathbb{Z}_m$ mit der Addition zyklisch, $\mathbb{Z}_m = \{1, 1+1, \ldots 1+1+\cdots+1\}$. Mittels der Abbildung $g^k \longmapsto k \mod m$ ist G mit der Multiplikation isomorph zu $\mathbb{Z}_m$ mit der Addition. Es ist $g^m = 1$ und es ist $g^l = 1$ genau dann, wenn $l = 0 \mod m$. Wir definieren für a in G die Ordnung von a, $\text{Ord}_G(a)$ als das kleinste $l \geq 1$, sodass $a^l = 1$. Wie oben bei $a \in \mathbb{Z}_m^*$ ist $\text{Ord}_G\left(g^k\right) = \frac{m}{\text{ggT}(k,m)}$. Einge weitere Eigenschaften von G folgen: Aussage (b) besagt, dass die Anzahl der Elemente, deren Ordnung eine feste Zweierpotenz in ihrer Primfaktorzerlegung hat, höchstens die Hälfte aller Elemente ist.

Lemma 9. *Sei m gerade.*

(a) Es gibt genau 2 Lösungen der Gleichung $x \cdot x = 1$. Diese sind $x = g^m = 1$ und $x = g^{\frac{m}{2}}$.

(b) Für $u \geq 0$ ist $\#\{a \in G | Ord_G(a) = 2^u \cdot v, v \text{ ungerade}\} \leq \frac{1}{2} \cdot m$.

Beweis:

(a) Man sieht das, indem man die Elemente g^k einzeln durchgeht und bedenkt, dass $g^l = 1$ genau dann, wenn $l = 0 \mod m$.

(b) Sei die Primfaktorzerlegung von $m = 2^v \cdot w, v \geq 1, w$ ungerade. Wir zeigen, dass genau die Hälfte aller Elemente von G die Behauptung mit $u = v$ erfüllt ist. Damit bleiben für die übrigen u höchstens die Hälfte aller Elemente übrig. Die Elemente g^k, mit $k = 1, 3, \ldots, m-1$, also k ungerade, sind genau die Elemente, die den Faktor 2^v in ihrer Ordnung haben müssen, da sie keine 2 in dem k haben. Das sind genau die Hälfte aller Elemente von G. □

Den Beweis des folgenden Satzes überlassen wir den Algebralehrbüchern. Man sieht aber leicht selbst, dass Z_8^* nicht zyklisch ist, im Unterschied zu Z_4^*.

Satz 4 *Ist $p \geq 3$, eine Primzahl $\alpha \geq 1$, dann ist $Z_{p^\alpha}^*$ mit der Multiplikation eine zyklische Gruppe.*

Für welche Elemente $x \in \mathbb{Z}_{p^\alpha}$ gilt $x \notin \mathbb{Z}_{p^\alpha}^*$? Das sind $x = 0 \cdot p, 1 \cdot p, 2 \cdot p, 3 \cdot p, \ldots, p^\alpha - p = (p^{\alpha-1} - 1) \cdot p$. Das sind genau $p^{\alpha-1}$ viele Elemente. (Jedes $p-$te Element von $\mathbb{Z}_{p^\alpha}$ ist Vielfaches von p). Also $\#\mathbb{Z}_{p^\alpha}^* = p^\alpha - p^{\alpha-1} = p^{\alpha-1} \cdot (p-1)$. Also ist $\mathbb{Z}_{p^\alpha}^*$, $p \geq 3$ eine zyklische Gruppe mit einer geraden Anzahl von Elementen.

Beweis von Satz 1: Wir kürzen ab, $q_i = p_i^{\alpha_i}$ Sei $a \in \mathbb{Z}_M^*$ und sei $a_k = a \mod q_k$. Dann ist der Isomorphismus des chinesischen Restsatzes $f(a) = (a_1, \ldots, a_k)$ und $a_i \in \mathbb{Z}_{q_i}^*$. Sei $S_i = \text{Ord}_{q_i}(a_i)$ und $R = \text{Ord}_M(a)$. Dann ist $R = \text{kgV}(S_1, \ldots, S_k)$. Sei für $u_i \geq 0$ 2^{u_i} die Zweierpotenz in der Primfaktorzerlegung von S_i. Wir zeigen: Wenn nicht alle u_i gleich

sind, so gilt die Behauptung des Satzes für a. Sei o.B.d.A. in u_1 das kleinste der u_i und u_2 das größte. Dann ist $u_1 < u_2$ und die Zweierpotenz in R ist gerade 2^{u_2}. Also ist R gerade und wir betrachten $\frac{R}{2}$. (Sicherlich ist $a^{\frac{R}{2}} \mod M \neq 1$). Was ist mit $a_1^{\frac{R}{2}}$? Da $u_1 < u_2$ ist, ist immer noch $a_1^{\frac{R}{2}} \mod q_1 = 1$. Was ist mit $a_2^{\frac{R}{2}}$? Es ist $a_2^{\frac{R}{2}} \mod q_2 \neq 1$, einfach da ein Faktor von 2 an der Ordnung fehlt. Aber es ist $a_2^{\frac{R}{2}} \mod q_2$ Lösung der Gleichung $x \cdot x = 1 \mod q_2$. Also da $\mathbb{Z}_{q_2}^*$ zyklisch ist (!), gibt es nur eine weitere Lösung außer der 1. Es gilt $(q_2-1)\cdot(q_2-1) = 1 \mod q_2$. Also muss $a_2^{\frac{R}{2}} = -1 \mod q_2$ sein. Und der ganz konkrete Wert ist $q_2 - 1$. Es ist $a_2^{\frac{R}{2}} \in Z_M^*$.

Wir schauen uns $\left(a^{\frac{R}{2}} - 1\right) \mod M$ an.

Es ist $\left(a^{\frac{R}{2}} - 1\right) \mod q_1 = 0$ und $\left(a^{\frac{R}{2}} - 1\right) = -2 \mod q_2$.

Der konkrete Wert ist $\left(a^{\frac{R}{2}} - 1\right) \mod q_2 = q_2 - 2$.

Es ist $q_2 - 2 \neq 0 \mod q_2$, da alle $p_i \geq 3$. (Sonst wäre $q_2 = 2$ möglich).

Es ist $f\left(a^{\frac{R}{2}} - 1\right) = (0, q_2 - 2, \dots)$.

Also $\left(a^{\frac{R}{2}} - 1\right) \notin \mathbb{Z}_M^*$ und $\left(a^{\frac{R}{2}} - 1\right) \mod M \neq 0$.

Also ist ggT$\left(a^{\frac{R}{2}} - 1, M\right) \neq 1$ und $\neq M$.

Wir zählen die $\#(a_1, \dots, a_k)$ wie oben, so dass alle u_i gleich sind. Es kann a_1 beliebig aus $\mathbb{Z}_{q_1}$ sein. Sei 2^{u_1} die Zweierpotenz in der Ordnung von a_1. Dann müssen die anderen a_i so sein, dass $u_i = u_1$ ist. Also kommen für a_i $2 \leq i \leq k$ höchstens die Hälfte der Elemente von $\mathbb{Z}_{q_i}^*$ in Frage. Also $\#(a_1, \dots, a_k)$, sodass alle u_i gleich sind, ist $\leq \frac{1}{2^{k-1}} \cdot \#\mathbb{Z}_{q_1}^* \times \mathbb{Z}_{q_2}^* \times \cdots \times \mathbb{Z}_{q_k}^* = \frac{1}{2^{k-1}} \cdot \#\mathbb{Z}_M^*$. □

10.3 Zusammenfassung

Wir lassen insgesamt folgendes Programm laufen:

Eingabe: M (Gesucht ist ein Teiler von M, wenn er denn existiert.)

1. Test: M gerade? Wenn ja, Teiler 2 und Schluss.
2. Test: $M = q^k$ für ein $q \geq 2$ und $k \geq 2$? Wenn ja Ausgabe von q und Schluss.
   Jetzt geht es erst richtig los.
3. Erzeuge a zufällig $1 \leq a \leq M - 1$.

4. Test: ggT$(a, M) > 1$. Ausgabe des ggT und Schluss.
5. Ermittle $R = \text{Ord}_M(a)$ mit dem Quantenalgorithmus.
6. Falls R ungerade Schluss, ohne Teiler zu finden.
7. Berechne $a^{\frac{R}{2}} - 1 \mod M$. Teste, ob ggT$(a^{\frac{R}{2}} - 1, M \neq 1$ und $\neq M$.
   Ausgabe des ggT als Teiler.

Das Programm ist mit Wahrscheinlichkeit $\varepsilon > 0$ erfolgreich, wie sich aus unseren Betrachtungsn ergibt. Test 2. ist effizient machbar und das Quantenprogramm zu zufälligem a ist auch effizient konstruierbar (Multiplikation mit a).

Damit ist die Sache soweit fertig.

11 Simons Problem

Simons Problem ist das erste Problem, bei dem durch einen Quantenalgorithmus ein exponentieller Laufzeitgewinn zu erzielen ist $\left(\text{d.h. von } \geq c \cdot n \text{ auf } \geq 2^{c \cdot n} \text{ auf } \leq n^k \left(\frac{log 2^{cn}}{c}\right)^k\right)$.

Vorher hatten wir

Deutsches Algorithmus: 1 Aufruf von f (oder U_f) weniger.

Deutsch Josza:

- klassisch deterministisch, dann $2^{n-1} + 1$ zu 1 Aufruf
- klassisch randomisiert $\geq C \geq 2$ zu 1 Aufruf

Also zu randomisierten Algorithmen noch nicht so tolle Verbesserungen.

Wir betrachten hier:

$$\mathbb{Z}_2^k = \{0,1\} = \left\{ \begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix} \right\} | b_i \in \{0,1\}$$

als abelsche Gruppe mit 2^k Elementen.

Null = 0-Vektor

$$-\begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix}, \text{ da } 1+1=0+0=0$$

Wir betrachten eine Untergruppe bestehend aus 2 Elementen,

$$D = 0, 1, y = \begin{pmatrix} y_1 \\ \vdots \\ y_k \end{pmatrix} \neq \begin{pmatrix} y_1 \\ \vdots \\ y_k \end{pmatrix} \text{ fest.}$$

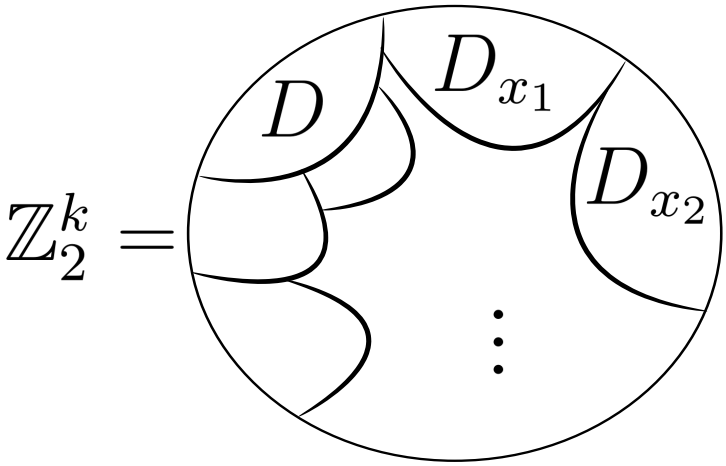
Wir betrachten die Restklassen von D.

Das sind alle Teilmengen $D_x = \{x + y, x \neq 0\} = x + D$ von $\mathbb{Z}_2^k$.

Für $x \neq x'$ gilt $D_x = D_{x'}$ oder $D_x \cap D_{x'} = \emptyset$.

Da auf jeden Fall $x \in D_x$ ist, liefern uns die D_x eine Partition von $\mathbb{Z}_2^k$.

Fig. 1. Die Partitionen von Z_2^k



Es gibt genau $\frac{2^k}{2} = 2^{k-1}$ verschiedene Restklassen. Wir geben jeder Restklasse einen eindeutigen Namen. Dazu nehmen wir uns eine Funktion $f : \mathbb{Z}_2^k \to \mathbb{Z}_2^{k-1}$ mit $f(x) = f(x')$

$\Leftrightarrow x, x'$ in derselben Restklasse

$\Leftrightarrow x = x'$ oder $x - x' = x + x' = y$. (Erinnerung $y \neq 0$).

Das algorithmische Problem ist nun:

Gegeben ein solches f, gesucht ist die Untermenge D, also das y. Wie geht man da ran? Wenn wir $x \neq x'$ mit $f(x) = f(x')$ haben, ist $y = x + x'$. Also x, x' suchen.

Deterministisch finden wir solche Elemente x, x', sicher indem die Funktion f an $2^{k-1} + 1$ Argumenten ausgewertet wird. Der folgende Quantenalgorithmus hat Laufzeit $\mathcal{O}(k^3)$.

Zunächst muss f so transformiert werden, dass es durch einen Quantenalgorithmus implementiert werden kann. Die Funktion $f_\oplus : \{0,1\}^k, \times \{0,1\}^{k-1} \to \{0,1\}^k \times \{0,1\}^{k-1}$ ist gegeben durch $b_1 \dots b_k c_1 \dots c_{k_1} \to b_1 \dots b_k$

$c_1 \dots c_{k-1} \oplus f(b_1 - b_k)$,

wobei für $f(b_1 - b_k) = d_1 - d_{k-1}$

$c_1 - c_{k-1} \oplus f(b_1 - b_k) := c_1 \oplus d_1 \dots c_{k-1} \oplus d_{k-1}$ ist, also koordinatenweises esklusives Oder. Es ist $f_\oplus$ bijektiv. Wir haben einen Quantenalgorithus für die Matrix U_f (die $f_\oplus$ berechnet).

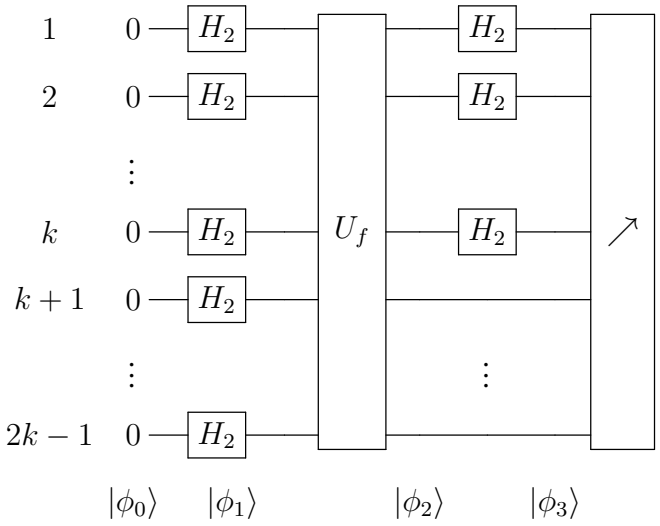
Es ist

$$U_f|b_1 - b_k 0 \dots 0\rangle = \underbrace{|b_1 \dots b_k d_1 \dots d_{k-1}\rangle}_{\text{gleich}}$$
$$\text{und}$$
$$U_f|b_1' - b_k' 0 \dots 0\rangle = \overbrace{|b_1' \dots b_k' d_1 \dots d_{k-1}\rangle}^{\text{gleich}}$$

gdw. $b_1 - b_k = b_1' - b_k'$ oder $\begin{pmatrix} b_1' \\ \vdots \\ b_k' \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix} + y$ unterschiedlich aus einer Restklasse.

Der Algorithmus ist denkbar einfach. Der Hauptbestandteil ist folgender Quantenalgorithmus:

Programm 6



$\phi\Phi$ Jetzt der ganze Algoritmus:

Der Quantenalgorithmus wird l-mal ausgeführt. Von den Messergebnissen verwahren wir immer die Bits $1, \ldots, k$.

$$\begin{aligned} &1.\text{ Messung} : a_{1,1} \ldots a_{1,k} \\ &\qquad\vdots \\ &l.\text{ Messung} : a_{l,1} \ldots a_{l,k} \end{aligned}$$

Wir konstruieren die Matrix $A = (a_{i,j})_{1 \le i \le l, 1 \le j \le k}$.

Wir sehen sie als lineare Abbildung $A : \mathbb{Z}_2^k \to \mathbb{Z}_2^l$.

Wir betrachten das Gleichungssystem $A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$.

Dieses hat die Lösung $\begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ und die Lösung y.

Wir ermitteln alle Lösungen dieses Systems. Sind das nur 2 Stück, so ist y das gesuchte $y =$ die Lösung $\neq \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$.

Hier wird der Gaußsche Algorithmus zur Lösung von linearen Gleichungssystemen aufgerufen.

Schauen wir uns zunächst den Quantenalgorithmus an. Wir verwenden die Bezeichnungen $|\phi_i\rangle$ aus dem Bild. $|\phi_0\rangle = |0 \dots 00 \dots 0\rangle$.

$$\begin{aligned} |\phi_1\rangle &= \frac{1}{\sqrt{2^k}} \left(\sum_{b_1,\dots,b_k} |b_1 \dots b_k\rangle \right) \otimes |0 \dots 0\rangle \\ &= \frac{1}{\sqrt{2^k}} \sum_{b_1,\dots,b_k} \Big| b_1, \dots, b_k \underbrace{0 \dots 0}_{\text{Platz für das Ergebnis}} \Big\rangle \end{aligned}$$

$|\phi_2\rangle = \frac{1}{\sqrt{2^k}} \cdot \sum_{b_1 \dots b_k} |b_1, \dots, b_k f\left(b_1 \dots b_k\right)\rangle$ (Quantenalgorithmus)

In der ausgegeben Darstellung von ϕ_2 sehen wir gut: an jedem $b_1 \dots b_k$ hängt der Funktionswert $f\left(b_1 \dots b_k\right)$.

Man kann aber auch von den Funktionswerten aus gucken: An jedem $c_1 \dots c_{k-1}$ hängen genau die beiden $\begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix}$ und $\begin{pmatrix} b'_1 \\ \vdots \\ b'_k \end{pmatrix}$ mit $\phi \begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix} = \begin{pmatrix} b'_1 \\ \vdots \\ b'_k \end{pmatrix}$ also genau eine Restlasse $D_x = x + D$.

Damit ist

$$|\phi_2\rangle = \frac{1}{\sqrt{2^k}} \cdot \sum_{c_1 \dots c_{k-1}} \sum_{b_1 \dots b_k} |b_1 \dots b_k c_1 \dots c_{k-1}\rangle \text{ mit } f\left(b_1 \dots b_k\right) = c_1 \dots c_{k-1}.$$

Die innere Summe besteht für jedes $c_1 \dots c_{k-1}$ aus 2 Summanden:

$|b_1 \dots b_k c_1 \dots c_{k_1}\rangle + |(b_1 \dots b_k \oplus y_1 \dots y_k)\, c_1 \dots c_{k-1}\rangle$, wobei $y = \begin{pmatrix} y_1 \\ \dots \\ y_k \end{pmatrix}$ und $\oplus$ die einfache Vektoraddition ist. An $c_1 \dots c_{k-1}$ hängen die beiden Elemente aus der Restklasse mit Namen $c_1 \dots c_{k-1}$. Bezeichnen wir diese mit $D_{\bar{c}}$, $\bar{c} = c_1 \dots c_{k-1}$. Also $D_{0\dots0}$ bis $D_{1\dots1}$ enthält jede Restklasse genau einmal.

Also $D_{0\dots0}$ bis $D_{1\dots1}$ enthält jede Restklasse genau einmal. Also

$$|\phi_2\rangle = \frac{1}{\sqrt{2^k}} \cdot \sum_{c_1 \dots c_{k-1}} \left(\left(\sum_{b_1 \dots b_k \in D_{c_1 \dots c_{k-1}}} |b_1 \dots b_k\rangle \right) \oplus |c_1 \dots c_{k-1}\rangle \right)$$

Bezeichnen wir $\bar{c} = c_1 \dots c_{k-1}$, dann

$$|\phi_3\rangle = \frac{1}{\sqrt{2^k}} \sum_{\bar{c}} \left(\left(\sum_{b_1 \dots b_k \in D_{\bar{c}}} H|b_1\rangle \oplus \dots \oplus H|b_k\rangle \right) \oplus \bar{c} \right)$$

Wir sehen und sie innere Summe an. Ein typisches $D_{\bar{c}}$ ist

$$D_{\bar{c}} = \left\{ b_1 \dots b_k, b_1 \dots b_k \oplus \underbrace{y_1 \dots y_k}_{\text{Das gesuchte y.}} \right\}$$

Es ist

$$\begin{aligned} H_2|b\rangle &= \frac{1}{\sqrt{2}} (-1)^{b\cdot 0} |0\rangle + (-1)^{b\cdot 1} |1\rangle \\ &= \frac{1}{\sqrt{2}} \sum_{c=0,1} (-1)^{b\cdot c} |c\rangle. \end{aligned}$$

Also ist $H_2|b_1\rangle \oplus \dots \oplus H_2|b_k\rangle$

$$= \frac{1}{2^k} \cdot \sum_{a_1 \ldots a_k} (-1)^{b_1 a_1} |a_1\rangle \oplus \ldots \oplus (-1)^{b_k a_k} |a_k\rangle$$
$$= \frac{1}{2^k} \cdot \sum (-1)^{b_1 a_1 + \ldots + b_k a_k} |a_1 \ldots a_k\rangle$$

Interpretation von $(-1)^{b_1 a_1 + \ldots + b_k a_k}$:
$b_1 \ldots b_k \widehat{=} \{i | 1 \leq i \leq, b_i = 1\}$,
$a_1 \ldots a_k$ analog. Dann $b_1 a_1 + \ldots + b_k a_k = \#\left(\{i | b_i = 1\} \bigcap \{i | a_i = 1\}\right)$
$(-1)^{\sum_{a_i b_i}} = 1$, wenn der Schnitt gerade ist, -1 bei ungerade.

$$H_2|b_1 \oplus y_1\rangle \oplus \ldots \oplus H_2|b_k \oplus y_k\rangle$$
$$= \frac{1}{2^k} \sum_{a_1 \ldots a_k} (-1)^{\sum a_i (b_i \oplus y_i)} |a_1 \ldots a_k\rangle$$
$$\vdots$$
$$= \frac{1}{2^k} \sum_{a_1 \ldots a_k} (-1)^{\sum a_i (b_i + y_i)} |a_1 \ldots a_k\rangle$$
$$= \frac{1}{2^k} \sum_{a_1 \ldots a_k} (-1)^{\sum a_i b_i} \cdot (-1)^{\sum a_i y_i} |a_1 \ldots a_k\rangle$$

Damit ist

$$H_2|b_1\rangle \oplus \ldots \oplus H_2|b_k\rangle + H_2|b_1 \oplus y_1\rangle \oplus \ldots \oplus H_2|b_k \oplus y_k\rangle$$
$$= \frac{1}{\sqrt{2^k}} \cdot \sum_{a_1 \ldots a_k} (-1)^{\sum a_i b_i} \cdot 2|a_1 \ldots a_k\rangle$$
$$(-1)^{\sum a_i y_i} = 1$$

Hier wird das y langsam sichtbar. Es haben alle die $a_1 \ldots a_k$, die mit $y = y_1 \ldots y_k$ eien Amplitude $\neq 0$, genauer $\pm \frac{2}{\sqrt{2^k}}$.

Dabei ist $(b_1, \ldots, b_k)$ ein festes der beiden Elemente aus $D_{\bar{c}}$. Da $\sum_{a_i y_i}$, gerade ist, ist auch egal welches. Der Faktor bleibt gleich. Der gesamt Zustand $|\phi_3\rangle$ hat $2^{k-1} \cdot 2^{k-1} = 2^{2k-2}$ Einträge mit Amlitude $\pm\frac{2}{2^k}$.

Nach dem Messen bekommen wir ein $a_1 \ldots a_k c_1 \ldots c_{k-1}$ mit $\sum a_i y_i$ gerade mit Wahrscheinlichkeit $\frac{1}{2^{2k-2}}$.