Quantum Computation:
Zusammenfassung der 6. Vorlesung (03.06.2011)

2 *Quantenalgorithmen*

2.1.1 *Der Deutsch Algorithmus*

Um festzustellen, ob ein vorgelegtes 1-Bitgatter einen reversiblen monadischen Wahrheitswertfunktor F implementiert oder nicht, muss man klassisch zwei Versuche machen: Man muss $F(0)$ und $F(1)$ ermitteln. Ist der Funktor unitär implementiert, dann gelingt es mit dem Deutschalgorithmus, die Antwort auf diese Frage mit nur einem Versuch zu erhalten. Das besondere dabei ist, dass man bei klassischer Vorgehensweise dazu das Gatter bestimmen muß, was man bei quantenmechanischer Vorgehensweise aber mit Hilfe des Überlagerungsprinzips umgehen kann.

Eine geeignete Überlagerung der Basiszustände von zwei Qubits erhält man mit

$$\left.\begin{array}{l} |0>-\boxed{H}- \\ \\ |1>-\boxed{H}- \end{array}\right\} (|00>\ \ |01>\ \ |10>\ \ |11>) \begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{-1} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

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

Damit folgt aufgrund der Linearität von U_F

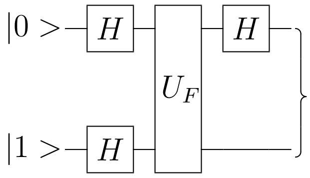
$$\left.\begin{array}{lcl} |0>-\boxed{H}- & & - \\ & \boxed{U_F} & \\ |1>-\boxed{H}- & & - \end{array}\right\} \frac{1}{2}(|0F(0)> -|0(1\oplus F(0))> +|1F(1)> -|1(1\oplus F(1))>)$$

$$= \frac{1}{2}(|0> \otimes(-1)^{F(0)}(|0> -|1>) + |1> \otimes(-1)^{F(1)}(|0> -|1>)$$

$$= \frac{1}{2}((-1)^{F(0)}|0> +(-1)^{F(1)}|1>) \otimes (|0> -|1>)$$

$$= (-1)^{F(0)}\frac{1}{\sqrt{2}}(|0> +(-1)^{F(0)+F(1)}|1>) \otimes \frac{1}{\sqrt{2}}(|0> -|1>).$$

Wegen $H\frac{1}{\sqrt{2}}(|0> + |1>) = |0>$ und $H\frac{1}{\sqrt{2}}(|0> - |1>) = |1>$ gilt schließlich:

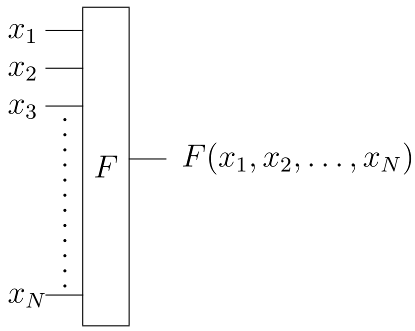


$$(-1)^{F(0)} \begin{cases} |0> \otimes \frac{1}{\sqrt{2}}(|0> - |1>) & \text{falls } F(0) = F(1) \\ |1> \otimes \frac{1}{\sqrt{2}}(|0> - |1>) & \text{falls } F(0) \neq F(1) \end{cases}$$

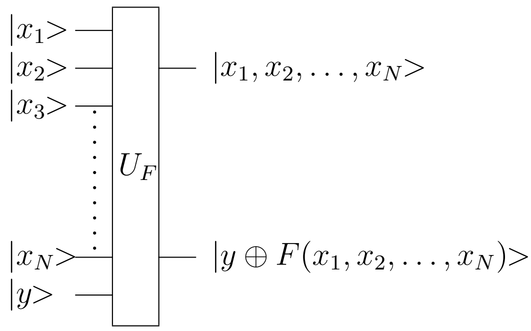
Eine Messung der Observablen $|1 >< 1|$ am ersten Qubit mit dem Ergebnis "0" zeigt also an, dass das unbekannte Gatter irreversibel ist. Falls die Messung das Ergebis "1" liefert, ist das unbekannte Gatter reversibel.

2.1.2 *Der Deutsch-Jozsa-Algorithmus*

Eine Verallgemeinerung des Deutsch-Algorithmus auf eine Klasse N-adischer Wahrheitswertfunktoren ist der Deutsch-Jozsa-Algorithmus: Der vorgelegte Funktor $F : \{0,1\}^N \to \{0,1\}$ muß entweder konstant oder gleichgewichtet sein, wobei letzteres bedeutet, dass der Funktor für 2^{N-1} Eingaben wahr und für 2^{N-1} Eingaben falsch ist. Der Algorithmus zeigt dann, welcher der beiden Fälle vorliegt. Für $N = 1$ reduziert sich diese Fragestellung auf die des Deutschalgorithmus. Als unbekanntes Gatter diese Klasse sei vorgelegt



und



sei die unitäre Implementation. Für die Multiqubit-Basiszustände hatten wir schon die Bezeichnung $|k) = |x_1 x_2 \ldots x_N>$, wobei k die Dezimalzählung ist, eingeführt, von der wir jetzt Gebrauch machen. Der Übersicht halber indizieren wir die Elemente der Computerbasis in Dezimalzählung in $\mathbf{C}^N$

vorübergehend mit der Anzahl der Dualstellen: $|k)_N \in \mathbf{C}^N$. Mit

$$H|0)_1 = H|0>= \frac{1}{\sqrt{2}}(|0>+|1>) = \frac{1}{\sqrt{2}}(|0)_1 + |1)_1) == \frac{1}{\sqrt{2}}\sum_0^{2-1}|k)_1$$

als Induktionsanfang und

$$H^{\otimes N}|0)_N = \frac{1}{\sqrt{2^N}}\sum_0^{2^N-1}|k)_N$$

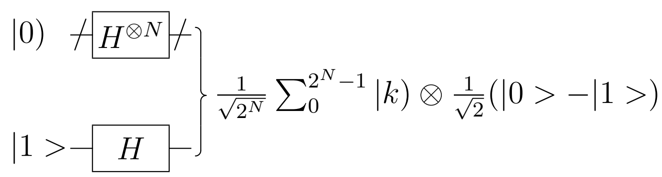
als Induktionsannahme ist zunächst

$$\begin{aligned} H^{\otimes(N+1)}|0)_{N+1} &= (H^{\otimes N}\otimes H)(|0)_N \otimes |0>) \\ &= \frac{1}{\sqrt{2^N}}\sum_0^{2^N-1}|k)_N \otimes \frac{1}{\sqrt{2}}(|0>)+|1>) \\ &= \frac{1}{\sqrt{2^{N+1}}}(\sum_0^{2^N-1}(|k)_N \otimes (|0>)+\sum_0^{2^N-1}(|k)_N \otimes |1>)). \end{aligned}$$

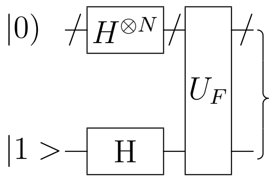
Bedenkt man nun, dass $|k)_N \otimes |z>=|k')_{N+1}$ mit $k' = 2^N x_1 + 2^{N-1}x_2 + \cdots + 2x_N + z = 2k + x$ ist, dann sthen in der ersten Summe der letzten Gleichung die Summanden mit ungeradem k' und in der zweiten die Summanden mit geradem k' von

$$H^{\otimes(N+1)}|0)_{N+1} = \frac{1}{\sqrt{2^{N+1}}}\sum_0^{2^{N+1}-1}|k')_{N+1}$$

was die Induktionsannahme bestätigt. Analog zum Deutsch-Algorithmus (Spezialfall $N = 1$) wird eine geeignete Überlagerung der Basiszustände durch



erzeugt und die Linearität von U_F liefert



$$\frac{1}{\sqrt{2^{N+1}}}\sum_0^{2^N-1}(|k)\otimes(|F(k)>-|1\oplus F(k)>)$$

$$= \frac{1}{\sqrt{2^{N+1}}}\sum_0^{2^N-1}(-1)^{F(k)}(|k)\otimes(|0>-|1>).$$

Um die Wirkung von $H^{\otimes N}$ auf einen beliebigen Basisvektor berauszubekommen, führen wir für $k=\sum_1^N 2^{N-i}x_i$ und $l=\sum_1^N 2^{N-i}y_i$ das "innere Produkt"

$$k\cdot l := \sum_1^N x_i y_i$$

ein. Offenbar gilt (Induktionsvoraussetzung)

$$< x|H|y >= \frac{1}{\sqrt{2}}(-1)^{xy}$$

und behaupten für $|k)=|x_1x_2\ldots x_N>$ und $|l)=|y_1y_2\ldots y_N>$ (Induktionsannahme)

$$(k|H^{\otimes N}|l) = \frac{1}{\sqrt{2^N}}(-1)^{k\cdot l}.$$

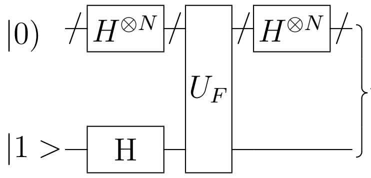
Diese Formel wird mit dem Induktionsbeweis

$$\begin{aligned}
(k'|H^{\otimes(N+1)}|l') &= < x_1x_2\ldots x_Nx_{N+1}|H^{\otimes(N+1)}|y_1y_2\ldots y_Ny_{N+1}> \\
&= (k|H^{\otimes N}|l) < x_{N+1}|H|y_{N+1}> \\
&= \frac{1}{\sqrt{2^{N+1}}}(-1)^{k\cdot l}(-1)^{x_{N+1}y_{N+1}} = \frac{1}{\sqrt{2^{N+1}}}(-1)^{\sum_1^{N+1}x_jy_j} \\
&= \frac{1}{\sqrt{2^{N+1}}}(-1)^{k'\cdot l'}
\end{aligned}$$

bestätigt. Damit ist

$$H^{\otimes N}|l) = \sum_{k=0}^{2^N-1}|k)(k|H^{\otimes N}|l) = \sum_{k=0}^{2^N-1}\frac{1}{\sqrt{2^N}}(-1)^{k\cdot l}|k)$$

und



$$\frac{1}{2^N\sqrt{2}} \sum_{k,l=0}^{2^N-1} (-1)^{k\cdot l+F(k)} |l) \otimes (|0> -|1>)$$

$$= \frac{1}{2^N\sqrt{2}} (|0) \otimes \sum_{k=0}^{2^N-1} (-1)^{F(k)} (|0> -|1>)$$

$$+ \sum_{l=1}^{2^N-1} \sum_{k=0}^{2^N-1} (-1)^{k\cdot l+F(l)} |l) \otimes (|0> -|1>)).$$

Die resultierende Wellenfunktion besteht so aus zwei zueinander orthogonalen Anteilen , von denen der erste genau dann verschwindet, wenn F gleichgewichtet ist. Ist F konstant dann ist der erste Anteil der Einheitsvektor $\pm|0> \otimes \frac{1}{\sqrt{2}}(|0> -|1>)$ und der zweite muss verschwinden. Liefert die Messung von $|0><0|$ am ersten System "1", dann ist F konstant, liefert sie "0" dann ist F gleichgewichtet (equilibrated).