Quantum Computation: Zusammenfassung der 7. Vorlesung (28.11.08)

2.2 *Die Quantenfouriertransformation*

Der unter dem Namen “Fast Fourier Transformation” bekannte klassische Algorithmus, der die diskrete Fourientransformation implementiert, ist reversibel und kann unmittelbar als unitärer Quantenalgorithmus aufgefasst werden. Der Schaltkreis enthält nur unitäre Gatter, die wir schon betrachtet haben.

Definition: Die lineare Abbildung des $\mathbf{C}^M$

$$c_k \longmapsto \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} e^{-\frac{2\pi i}{M} kj} c_j \quad (k = 0, 1, 2, \ldots, (M-1))$$

heißt diskrete Fouriertransformation. In der Quanteninformationstheorie wird dagegen für ein N-Qubitsystem, d.h. für $M = 2^N$, die dazu inverse Transformation im $\mathbf{C}^{2^N}$ mit Quantenfourientransformation bezeichnet:

$$\mathbf{F_N} : c_k \longmapsto \hat{c}_k := \frac{1}{\sqrt{2^N}} \sum_{j=0}^{2^N-1} e^{\frac{2\pi i}{2^N} kj} c_j \quad (k = 0, 1, 2, \ldots, (2^N - 1)).$$

Man kann direkt zeigen, dass die Matrixelemente der diskreten Fouriertransformation eine unitäre Matrix bilden. Da wir uns nur für die Quantenfouriertranstormation interessieren, können wir uns dies ersparen, denn in diesem Fall ist es eine direkte Folge der Tensorproduktdarstellung, die wir nun herleiten werden. Zuvor noch eine Bemerkung zur Nomenklatur: Für $\psi \in \mathbf{C}^{2^N}$ bezeichnen wie die Quantenfouriertransformierte mit

$$\hat{\psi} = (|0)\ |1)\ |2)\ \ldots\ |2^N - 1))((\mathbf{F_N}_{kj})) \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ \cdot \\ \cdot \\ c_{2^N-1} \end{pmatrix},$$

und es gilt

$$\begin{aligned}
\hat{\psi} &= (|0) \; |1) \; |2) \; \ldots \; |2^N-1)) \begin{pmatrix} \hat{c}_0 \\ \hat{c}_1 \\ \hat{c}_2 \\ . \\ . \\ \hat{c}_{2^N-1} \end{pmatrix} \\
&= (|\hat{0}) \; |\hat{1}) \; |\hat{2}) \; \ldots \; |2^N \hat{-} 1)) \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ . \\ . \\ c_{2^N-1} \end{pmatrix} .
\end{aligned}$$

Ebenso kann man auch die inverse Quantenfourientransformierte,

$$\breve{\varphi} = (|0) \; |1) \; |2) \; \ldots \; |2^N-1))((\overline{\mathbf{F_N}_{kj}})) \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ . \\ . \\ c_{2^N-1} \end{pmatrix} ,$$

auf verschiedene Weise schreiben:

$$\begin{aligned}
\breve{\varphi} &= (|0) \; |1) \; |2) \; \ldots \; |2^N-1)) \begin{pmatrix} \breve{c}_0 \\ \breve{c}_1 \\ \breve{c}_2 \\ . \\ . \\ \breve{c}_{2^N-1} \end{pmatrix} \\
&= (|\breve{0}) \; |\breve{1}) \; |\breve{2}) \; \ldots \; |2^N \breve{-} 1)) \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ . \\ . \\ c_{2^N-1} \end{pmatrix} .
\end{aligned}$$

Wegen der Symmetrie von $\mathbf{F}_{\mathbf{N}kj}$ in der Computerbasis ist $\mathbf{F}^{+}_{\mathbf{N}kj} = \overline{\mathbf{F}_{\mathbf{N}}}_{kj}$.

Mit $j = 2^{N-1}x_1 + 2^{N-2}x_2 + \cdots + 2^0 x_N$ ist

$$\begin{aligned}
|\hat{k}) &= \frac{1}{\sqrt{2^N}} \sum_{j=0}^{2^N-1} e^{\frac{2\pi i}{2^N}kj}|j) \\
&= \frac{1}{\sqrt{2^N}} \sum_{x_1=0}^{1} \sum_{x_2=0}^{1} \cdots \sum_{x_N=0}^{1} e^{\frac{2\pi i}{2^N}k(2^{N-1}x_1+2^{N-2}x_2+\cdots+2^0x_N)} \bigotimes_{l=1}^{N} |x_l > \\
&= \frac{1}{\sqrt{2^N}} \sum_{x_1=0}^{1} \sum_{x_2=0}^{1} \cdots \sum_{x_N=0}^{1} e^{2\pi i k(\frac{x_1}{2}+\frac{x_2}{4}+\cdots+\frac{x_N}{2^N})} \bigotimes_{l=1}^{N} |x_l > \\
&= \frac{1}{\sqrt{2^N}} \sum_{x_1=0}^{1} \sum_{x_2=0}^{1} \cdots \sum_{x_N=0}^{1} \bigotimes_{l=1}^{N} e^{2\pi i k\frac{x_l}{2^l}} |x_l > \\
&= \frac{1}{\sqrt{2^N}} (\sum_{x_1=0}^{1} e^{2\pi i k\frac{x_1}{2}} |x_1 >) \otimes (\sum_{x_2=0}^{1} e^{2\pi i k\frac{x_2}{4}} |x_2 >) \otimes \cdots \otimes \sum_{x_N=0}^{1} e^{2\pi i k\frac{x_N}{2^N}} |x_N > \\
&= \frac{1}{\sqrt{2^N}} \bigotimes_{l=1}^{N} (|0 > + \ e^{2\pi i k\frac{x_l}{2^l}} |1 >).
\end{aligned}$$

Sei nun $k = 2^{N-1}y_1 + 2^{N-2}y_2 - \cdots + y_N$, dann ist

$$2\pi i k \frac{x_l}{2^l} = 2\pi i x_l (2^{N-(l+1)}y_1 + \cdots + y_{N-l} + \frac{y_{N-(l-1)}}{2} \cdots + \frac{y_N}{2^l}),$$

denn für $N - (l + j) = 0$ ist $j = N - l$. Schreibt man

$$0, y_{N-(l-1)} y_{N-(l-2)} \ldots y_N := \frac{y_{N-(l-1)}}{2} + \frac{y_{N-(l-2)}}{4} + \cdots + \frac{y_N}{2^l},$$

dann ist

$$|\hat{k}) = \frac{1}{\sqrt{2^N}} \bigotimes_{l=1}^{N} (|0 > + \ e^{2\pi i \, 0, y_{N-(l-1)} y_{N-(l-2)} \cdots y_N} |1 >),$$

weil $e^{2\pi i Z} = 1$ für $Z \in \mathbf{Z}$, und ebenso

$$|\breve{k}) = \frac{1}{\sqrt{2^N}} \bigotimes_{l=1}^{N} (|0 > + \ e^{-2\pi i \, 0, y_{N-(l-1)} y_{N-(l-2)} \cdots y_N} |1 >).$$

Damit ist

$$
\begin{aligned}
\mathbf{F_N} &= \sum_{j=0}^{2^N-1} |\hat{j})(j| \\
&= \frac{1}{\sqrt{2^N}} \sum_{j=0}^{2^N-1} \left(\bigotimes_{l=1}^{N} (|0> + \; e^{2\pi i \, 0,x_{N-(l-1)}x_{N-(l-2)}\dots x_N} |1>) \right) (j|
\end{aligned}
$$

und mithin

$$
\begin{aligned}
\mathbf{F_N}^+ &= \sum_{j'=0}^{2^N-1} |j')(\hat{j}'| \\
&= \frac{1}{\sqrt{2^N}} \sum_{j'=0}^{2^N-1} |j') \left(\bigotimes_{l=1}^{N} (<0| + \; e^{-2\pi i \, 0,x'_{N-(l-1)}x'_{N-(l-2)}\dots x'_N} <1|) \right),
\end{aligned}
$$

wobei $|j') = |x'_1 x'_2 \dots x'_N >$ ist. Folglich ist

$$
\begin{aligned}
\mathbf{F_N}\mathbf{F_N}^+ &= \frac{1}{2^N} \sum_{j=0}^{2^N-1} \left(\bigotimes_{l=1}^{N} (|0> + \; e^{2\pi i \, 0,x_{N-(l-1)}x_{N-(l-2)}\dots x_N} |1>) \right) \\
&\qquad \left(\bigotimes_{l=1}^{N} (<0| + \; e^{-2\pi i \, 0,x_{N-(l-1)}x_{N-(l-2)}\dots x_N} <1|) \right) \\
&= \frac{1}{2^N} \sum_{j=0}^{2^N-1} \bigotimes_{l=1}^{N} (|0><0| + |1><1|) = \mathbf{1}.
\end{aligned}
$$

$\mathbf{F_N}$ ist also unitär und damit sind $\{|\hat{k})\}$ und $\{|\breve{k})\}$ Orthonormalbasen im $\mathbf{C}^{2^N}$. Wie die Tensorproduktdarstellung zeigt, bestehen diese Basen, wie die Computerbasis, aus unverschränkten Zuständen.