Quanten-Fourier-Transformation

Einleitung
1. Reelle Fourierreihen
2. Fouriertransformation
3. Diskrete Fouriertransformation (DFT)
4. Fast Fouriertransformation (FFT)
5. Quantum-Fouriertransformation
Quellen

H. Brandenburg

Einleitung

Die Quantum-Fouriertransformation bildet die Grundlage für das Faktorisierungsverfahren von Shor.

Dazu werden wir zunächst die Grundlagen dieses Verfahrens betrachten.

Grundsätzlich dient die Fourierreihen-Entwicklung, resp. die Fourier-transformation dazu eine Funktion in eine Darstellung in einem Funktionenraum zu transformieren. Dieses Verfahren findet zum Beispiel eine Anwendung in der Bildbearbeitung, wo man anhand der Fouriertransformierten neben der Periode einer Funktion auch leicht deren Amplitude ablesen kann.

Dazu suchen wir zunächst eine Basis, d.h. eine Anzahl von linear unabhängigen Vektoren welche den Raum aufspannen.

1. Reelle Fourierreihen

Die Funktionen 1, cos(kx), sin(kx) [k >0] bilden ein Orthogonalsystem im Raum der integrierbaren 2π - periodischen Funktionen.

D.h. u.a. $\int_{-\pi}^{\pi} \cos(jx)\sin(kx)dx = 0 \quad j \neq k$

und $\int_{-\pi}^{\pi} \cos^2(kx)dx = \int_{-\pi}^{\pi} \sin^2(kx)dx = \pi \qquad k > 0$

Dieser Raum wird durch unendlich viele dieser Vektoren aufgespannt, mithin bildet das Orthogonalsystem eine Basis für den Raum der integrierbaren 2π - periodischen Funktionen.

Damit lässt sich die Fourierreihen-Entwicklung wie folgt beschreiben:

Def: Die reelle Fourier-Reihe einer reellen 2π - periodischen Funktion f ist die Entwicklung nach obigen Orthogonalsystem:

$$f(x) = \frac{a_0}{2} + \sum_{k=1}^{\infty} (a_k \cos(kx) + b_k \sin(kx))$$

mit:

$$a_k = \frac{1}{\pi} \int_{-\pi}^{\pi} f(t) \cos(kt) dt \qquad k \geq 0$$

$$b_k = \frac{1}{\pi} \int_{-\pi}^{\pi} f(t) \sin(kt) dt \qquad k \geq 1$$

Bem: Da es in der Praxis nicht möglich ist solche unendlichen Reihen vollständig zu berechnen, verwendet man lediglich die ersten n Reihenglieder. Dabei wird die Funktion desto genauer aproximiert je größer n ist, also je mehr Reihenglieder verwendet werden.

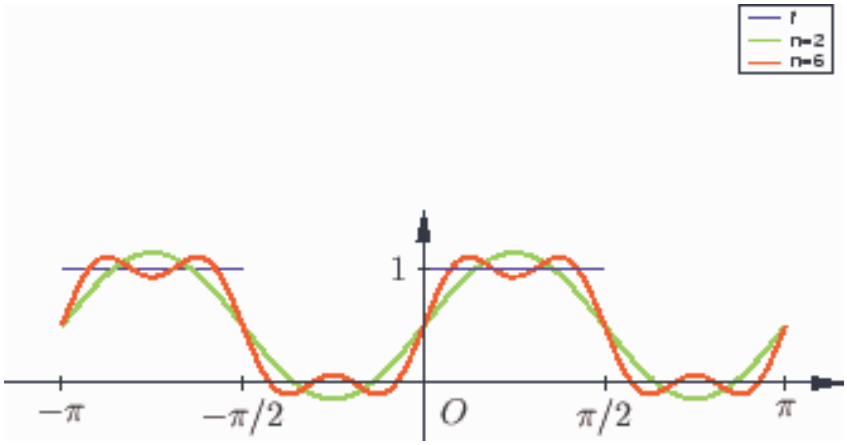
Bsp:
Gegeben sei folgende zwischen 0 und 1 alternierende Funktion:

$$f(x) = \begin{cases} 1, x \in \left[-\pi, \frac{-\pi}{2}\right) \cup \left[0, \frac{\pi}{2}\right) \\ 0, x \in \left[\frac{-\pi}{2}, 0\right) \cup \left[\frac{\pi}{2}, \pi\right) \end{cases}$$

damit ist die Fourierreihe von f:

$$f \sim \frac{1}{2} + \frac{4}{\pi} \sum_{m=0}^{\infty} \frac{\sin((4m+2)x)}{4m+2} = \frac{1}{2} + \frac{4}{\pi} \left(\frac{\sin(2x)}{2} + \frac{\sin(6x)}{6} + \ldots \right)$$

In Abb.1 ist diese Reihe für die Fälle n = 2 und n = 6 dargestellt.



[Abb.1]

Anm: Dieses Verfahren lässt sich auch auf Funktion mit einer Periode ungleich π anwenden.
Die Fourierreihe einer h-periodischen Funktion f erhält man durch eine lineare Transformation auf das Intervall $[-\pi, \pi]$.

2. Fouriertransformation

Betrachten wir nun allgemein komplexe Funktionen. Im entsprechenden Funktionenraum bilden die Funktionen $e_k(x) = e^{ikx}$ ein Orthogonalsystem.

Def: Die Fourier-Transformation einer komplexen Funktion f wird beschrieben durch:

$$f(t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} F(\omega) e^{i\omega t} d\omega \quad \text{und}$$

$$F(\omega) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} f(t) e^{-i\omega t} dt$$

wobei F als die Fouriertransformierte von f bezeichnet wird.

Dabei lassen sich nicht alle komplexen Funktionen transformieren. Es gelten folgende Einschränkungen:

Satz von Dirichlet-Jordan: Die Fourier-Transformierte F von f existiert, wenn die folgenden Kriterien allesamt erfüllt sind:

a) Die Funktion f ist absolut integrierbar, d.h.

$$\int_{-\infty}^{\infty} |f(t)|\, dt < \infty$$

b) Jedes Intervall enthält nur endlich viele Stellen $t_0 < t_1 < t_2 < ... < t_m$, wobei der Real- und Imaginärteil der Funktion f in allen offenen Teilintervallen (t_i, t_{i+1}) monoton und stetig ist.

c) An allen Stellen t existieren die beiden einseitigen Grenzwerte.

Genauer gilt für die inverse Transformation an allen Stellen t folgende Gleichung:

$$\lim_{\varepsilon \to 0^+} \left(\frac{f(t_i + \varepsilon) + f(t_i - \varepsilon)}{2} \right) = \frac{1}{\sqrt{2 \cdot \pi}} \cdot \int_{-\infty}^{\infty} F(\omega) \cdot e^{i \cdot \omega \cdot t}\, d\omega$$

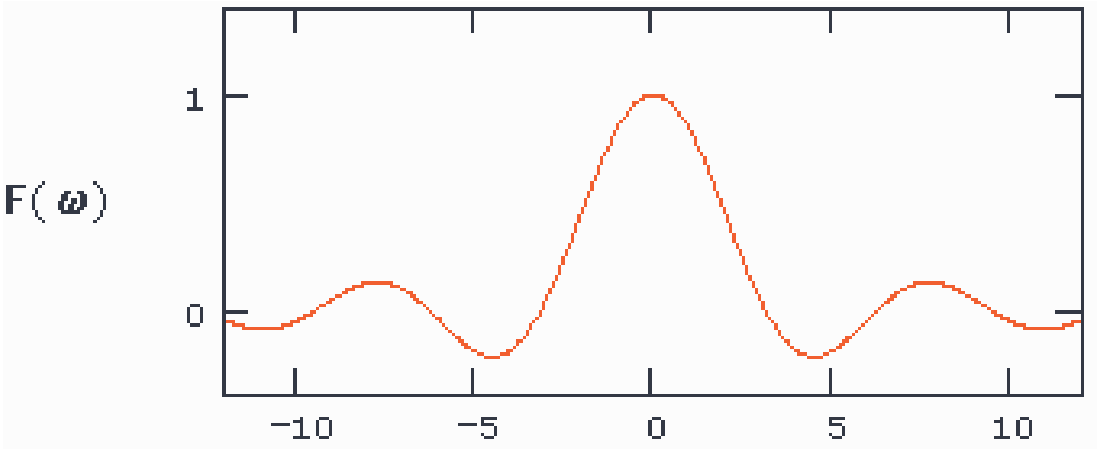
Bsp:

$$f(t) = \begin{bmatrix} \sqrt{\frac{\pi}{2}} & \text{für} \quad (-1 \le x \le 1) \\ 0 & \text{für} \quad (x < -1), (x > 1) \end{bmatrix}$$

=>

$$F(\omega) = \frac{1}{\sqrt{2 \cdot \pi}} \cdot \int_{-1}^{1} \sqrt{\frac{\pi}{2}} \cdot e^{-i \cdot \omega \cdot t}\, dt = \begin{pmatrix} \frac{\sin(\omega)}{\omega} & \text{für} \quad \omega \neq 0 \\ 1 & \text{für} \quad \omega = 0 \end{pmatrix}$$

siehe Abb.2



[Abb.2]

3. Diskrete Fouriertransformation

Im folgenden werden wir keine (stetigen) Funktionen, sondern (diskrete) Vektoren betrachten.

Def:
Eine komplexe Zahl ω heißt n-te Einheitswurzel falls $\omega^n=1$ ist;
Sie sei bezeichnet als ω_n .
Ist weiterhin $\omega_n=1$ und $\omega_k \neq 1$ (n<k) so heißt ω primitive n-te Einheitswurzel.

Durch bilden der Potenzen der Einheitswurzel: $\omega^j_n = e^{\frac{2\pi ij}{n}}$
Erhält man die Fourier-Matrix $F_n=(\omega_n{}^{jk})$

Nach einer Normierung $F_n \rightarrow F_n/\sqrt{n}$ ist sie überdies unitär.

Damit ist für einen Vektor $x = (x_0,x_1,...,x_{n-1})$ die Transformierte: $y(y_0,y_1,...,y_{n-1}) = F_n x$, mithin also:

$$y_k = \sum_{j=0}^{n-1} x_j (\omega_n)^{jk} = \sum_{j=0}^{n-1} e^{\frac{2\pi ijk}{n}} x_j$$

Der Aufwand für diese Berechnung ist $O(n^3)$; kann aber durch spezielle Verfahren noch ein wenig gesenkt werden.

Dabei werden viele Schritte mehrfach gemacht, daher wird als Vereinfachung die Fast-Fouriertransformation angewandt.

4. Fast-Fouriertransformation (FFT)

Bei der FFT wird versucht, die Fouriertransformation rekursiv durchzuführen. Dazu wird der zu transformierende Vektor x in zwei Hälften zerlegt, welche separat zu transformieren sind, und die Ergebnisse werden anschließend wieder zusammengefasst.

Sei n gerade. Dann kann $x = (x_0,x_1,...,x_{n-1})$ zerlegt werden in

$x^{even} := (x_0, x_2,...,x_{n-2}) = (x_0^{even}, x_1^{even},...,x_{n/2-1}^{even})$ und
$x^{odd} := (x_1, x_3,...,x_{n-1}) = (x_0^{odd}, x_1^{odd},...,x_{n/2-1}^{odd})$.

Nun wird FFT auf x^{even} und x^{odd} angewandt:

$$y_k^{even} = \sum_{j=0}^{\frac{n}{2}-1} e^{\frac{2\pi ijk}{n/2}} x_{2j} \text{ bzw. } y_k^{odd} = \sum_{j=0}^{\frac{n}{2}-1} e^{\frac{2\pi ijk}{n/2}} x_{2j+1}$$

Die Ergebnisse werden dann zusammengefasst:

Sei zunächst k = 0,...,n/2 :

$$y_k = \sum_{j=0}^{n-1} x_j (\omega_n)^{jk} = \sum_{j=0}^{\frac{n}{2}-1} x_{2j} (\omega_n)^{2jk} + \sum_{j=0}^{\frac{n}{2}-1} x_{2j+1} (\omega_n)^{(2j+1)k}$$

$$= \sum_{j=0}^{\frac{n}{2}-1} x_{2j} (\omega_{\frac{n}{2}})^{jk} + \sum_{j=0}^{\frac{n}{2}-1} x_{2j+1} (\omega_{\frac{n}{2}})^{jk} \omega_n^{\ k}$$

$$= y_k^{\ even} + y_k^{\ odd} \omega_n^{\ k}$$

ähnlich erhält man für den Rest:

$$y_{\frac{n}{2}+k} = y_k^{\ even} - y_k^{\ odd} \omega_n^{\ k}$$

Der Aufwand für diese (rekursive) Berechnung ist O(n log n).

Quantum-Fouriertransformation (QFT)

Ziel: Transformierung eines Qubits j in einen Überlagerungszustand:

$$|j\rangle \xrightarrow{QFT} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i j k}{N}} |k\rangle$$

Die Linearkombination $\sum_{k=0}^{N-1} x_j |j\rangle$ wird dabei mit Hilfe der klassischen DFT transformiert:

$$\sum_{k=0}^{N-1} x_j |j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \sum_{k=0}^{N-1} e^{\frac{2\pi i j k}{N}} |k\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} x_j e^{\frac{2\pi i j k}{N}} |k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} y_k |k\rangle$$

Dabei ist $(y_0,y_1,...,y_{N-1}) = DFT(x_0,x_1,...,x_{N-1})$.

Durch Anwendung der (unitären) Fouriermatrix F_N erhält man die Kurzschreibweise $QFT(|j\rangle) = F_N |j\rangle$.

Festlegungen:

Sei nun $N=2^n$; damit lässt sich das Qubit $|j\rangle$ darstellen als

$$|j\rangle = \left|\underbrace{0110..11}_{n}\right\rangle = |j_1, j_2, ..., j_n\rangle \text{ mit } j_i \in \{0,1\}.$$

Desweiteren bedeute nun $.j_l j_{l+1} ... j_n$, $j_i \in \{0,1\}$:

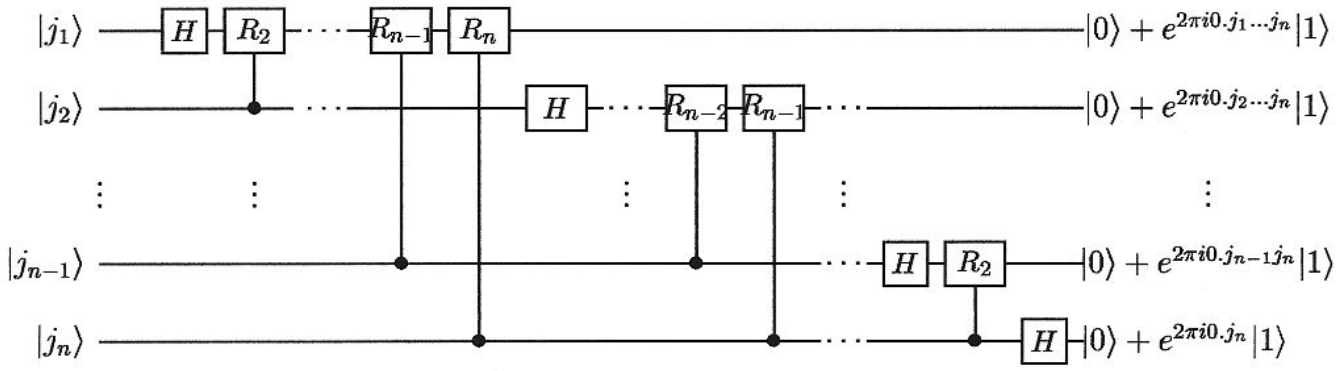
$j_l \frac{1}{2} + j_{l+1} \frac{1}{4} + ... + j_n \frac{1}{2^{n-l+1}}$, also die Binärbruchentwicklung von j.

Z.B. .011= 1/4 + 1/8 = 3/8

Beh: Die Quantum-Fouriertransformation lässt sich darstellen als

$$QFT(|j\rangle) = (|0\rangle + e^{2\pi i 0.j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle)...(|0\rangle + e^{2\pi i 0.j_1 ... j_n}|1\rangle)\frac{1}{\sqrt{N}}$$

Dies wird als Produktdarstellung bezeichnet.
Aus ihr kann ein effizienter Quantenschaltkreis für die QFT abgeleitet werden.



R_k bezeichne die unitäre Transformation $R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\left(\frac{2\pi i}{2^k}\right)} \end{pmatrix}$, welche nur dann ausgeführt wird, wenn $|j_k\rangle = 1$ ist, sowie H die Hadamard-Transformation.

Bew.: (Beh.) Sei $|j_1 j_2 .. j_n\rangle$ gegeben. Durch die Hadamard-Transformation auf $|j_1\rangle$ ergibt sich der Zustand:

$H|j_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0.j_1}|1\rangle)|j_2 .. j_n\rangle$ da $e^{2\pi i 0.j_1} = -1$ für j_1=1 bzw 1 für j_1=0.

Das Gatter R_2 wird nun in Abhängigkeit von $|j_2\rangle$ ausgeführt; man erhält als Folgezustände die beiden Alternativen

$\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0.j_1}|1\rangle)|j_2 .. j_n\rangle$,falls j_2=0

$\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0.j_1 j_2}|1\rangle)|j_2 .. j_n\rangle$,falls j_2=1 (*)

da im Fall j_2=0 $0.j_1 = 0.j_1 j_2$ ist, kann der Folgezustand allgemein durch (*) beschrieben werden.

Nach Anwendung aller kontrolierten R_i-Gatter bis R_n, ergibt sich der Zustand $\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0.j_1 \ldots j_n}|1\rangle)|j_2 .. j_n\rangle$.

Dies wird analog für die restliche Qubits durchgeführt und durch Vertauschung der Reihenfolge erhält man die gewünschte Produktdarstellung.

Diese Schaltung benötigt damit $\sum_{i=1}^{n} i = \frac{n(n-1)}{2} = O(n^2)$ „kleine“ Gatter.

<u>Noch zu zeigen:</u> Produktdarstellung enspricht der QFT

Analog zur FFT entwickeln wir eine rekursive Darstellung der QFT.

Erinnerung: $QFT(|j\rangle) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i j k}{N}} |k\rangle$

Wir definieren die Bitstrings $\hat{j} = j_2 \cdots j_n$ und $j' = j_1 \cdots j_{n-1}$.

Damit läst sich die QFT schreiben als:

$$QFT(|j\rangle) = \frac{1}{\sqrt{N}} \sum_{k' \in \{0,1\}^{n-1}} e^{\frac{2\pi i j k' 0}{N}} |k'0\rangle + e^{\frac{2\pi i j k' 1}{N}} |k'1\rangle,$$

wobei k'0 und k'1 als konkatenierte Bitstrings zu verstehen sind.

Da *bin*(x0)=2*bin*(x) und *bin*(x1)=2*bin*(x)+1 ist, erhält man

$$QFT(|j\rangle) = \frac{1}{\sqrt{N}} \sum_{k' \in \{0,1\}^{n-1}} e^{\frac{2\pi i j k'}{N/2}} |k'0\rangle + e^{\frac{2\pi i j (2k'+1)}{N}} |k'1\rangle$$

[wegen $ab(|x\rangle \otimes |y\rangle) = a|x\rangle \otimes b|y\rangle = |ax\rangle \otimes |by\rangle$]

$$= \underbrace{\frac{1}{\sqrt{N}} \sum_{k' \in \{0,1\}^{n-1}} e^{\frac{2\pi i j k'}{N/2}} |k'\rangle}_{=\sqrt{2} QFT_{\frac{N}{2}}(|\hat{j}\rangle)} \left(|0\rangle + e^{\frac{2\pi i j}{N}} |1\rangle \right).$$

Die in den Klammer behauptete Gleichheit gilt, da

$$e^{\frac{2\pi i j k'}{N/2}} = e^{\frac{2\pi i j_1 \hat{j} k'}{N/2}} = e^{\frac{2\pi i (2^{n-1} j_1 + \hat{j}) k'}{N/2}} = \underbrace{e^{\frac{2\pi i 2^{n-1} j_1 k'}{N/2}}}_{=1} e^{\frac{2\pi i \hat{j} k'}{N/2}} = e^{\frac{2\pi i \hat{j} k'}{N/2}}.$$

Damit gilt:

$$\frac{1}{\sqrt{N/2}} \sum_{k' \in \{0,1\}^{n-1}} e^{\frac{2\pi i \hat{j} k'}{N}} |k'\rangle \left(\frac{|0\rangle + e^{2\pi i . j} |1\rangle}{\sqrt{2}} \right) = QFT_{\frac{N}{2}}(|\hat{j}\rangle) \left(\frac{|0\rangle + e^{2\pi i . j} |1\rangle}{\sqrt{2}} \right),$$

und mit $\sqrt{N} = 2^{\frac{n}{2}} = \left(\sqrt{2}\right)^n$ die Behauptung.

Quellen:

Jacobo Toran: Vorlesung Quantencomputer; Mitschrift von Jan Paul Buchwald; Universität Ulm 2003

App/Höllig: Mathematik-Online-Kurs: Fourier-Analysis - Fourier-Reihen - Kosinus- und Sinusreihen
http://mo.mathematik.uni-stuttgart.de/kurse/kurs19/

Oliver Bräunling: Kleine mathematische Sammlung
http://www.mathe.braunling.de/

http://iti.fh-flensburg.de/lang/algorithmen/fft/