# Quantum Fourier Transform.

Note Title 4/17/2012

The discrete Fourier transform takes as input a vector of $N$ complex numbers $(x_0, \ldots, x_{N-1})$ and outputs the transformed data, a vector of complex numbers $(y_0, y_1, \ldots, y_{N-1})$. defined as:

$$\hat{\alpha}_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} w^{j \cdot k} \alpha_j \qquad (w \equiv e^{2\pi/N})$$

One of the early discoveries in quantum algorithms was that a quantum computer can calculate the Fourier transform very efficiently when the vector is encoded as a set of amplitudes in a quantum state. Note that this does not mean that there is a quantum algorithm to compute the classical Fourier transform more efficiently since the vector is only accessible via quantum measurement, but the quantum Fourier transform has been an important component in many quantum algorithms.

Before discussing the QFT (quantum Fourier transform), we will review the classical discrete Fourier transform.

The DFT can be seen as matrix multiplication by the $N \times N$ matrix:

$$DFT_N = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & w & w^2 & \cdots & w^{N-1} \\ \vdots & w^2 & w^4 & & w^{2(N-1)} \\ \vdots & & & & \\ 1 & w^{N-1} & & & w^{(N-1)(N-1)} \end{bmatrix}$$

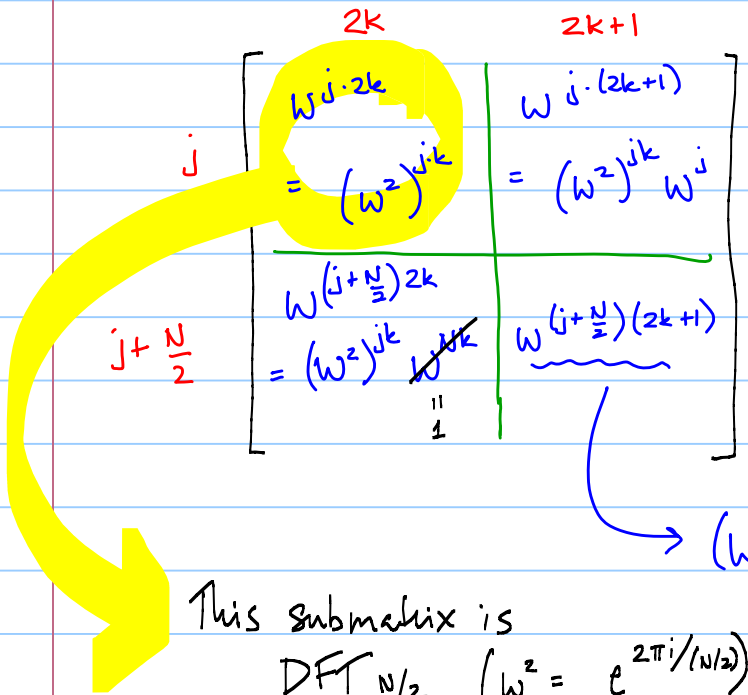
if rows + columns are numbered $0 \ldots N-1$ then

$$[DFT_N]_{jk} = w^{jk}$$

Thus, the time to compute the DFT is at most the time to multiply an $N \times N$ matrix by a length $N$ vector ($O(N^2)$).

The Fast Fourier Transform (FFT) exploits structure in the matrix to compute the Fourier transform more efficiently.

Reorganize the columns of $DFT_N$ so that the columns with an even index appear before the columns with an odd index. The entries in the input vector need to be reorganized accordingly: (assume $N$ is a power of 2)


$0 \le k \le \frac{N}{2}-1$

$0 \le j \le \frac{N}{2}-1$

$(w^2)^{jk} \underbrace{w^{Nk}}_{=1} \cdot w^j \cdot \underbrace{w^{N/2}}_{=-1} = -(w^2)^{jk} w^j$

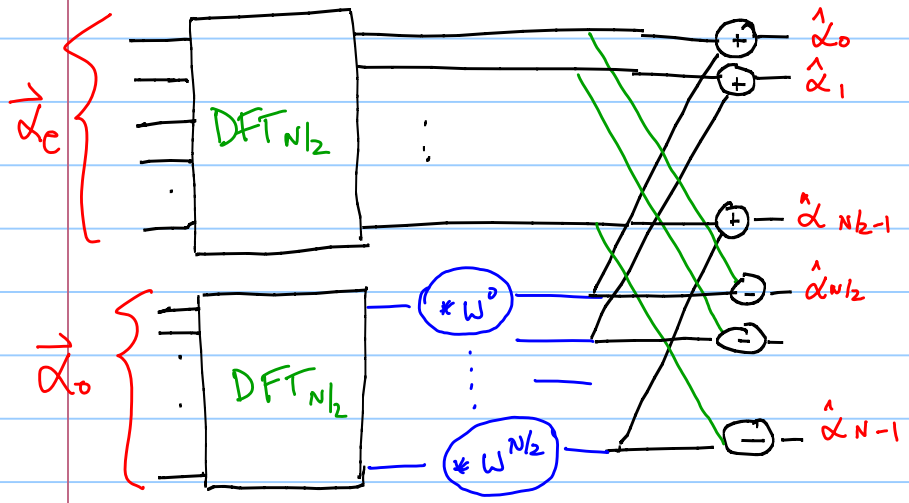
This submatrix is $DFT_{N/2}$ $(w^2 = e^{2\pi i/(N/2)})$.

$$\begin{bmatrix} (W^2)^{jk} & W^j (W^2)^{jk} \\ (W^2)^{jk} & -W^j (W^2)^{jk} \end{bmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_2 \\ \vdots \\ \alpha_{N-2} \\ \alpha_1 \\ \alpha_3 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} \begin{matrix} \} \vec{\alpha}_e \\ \\ \\ \\ \} \vec{\alpha}_o \end{matrix} = \begin{pmatrix} \hat{\alpha}_0 \\ \hat{\alpha}_1 \\ \vdots \\ \hat{\alpha}_{N/2-1} \\ \hat{\alpha}_{N/2} \\ \vdots \\ \hat{\alpha}_{N-1} \end{pmatrix}$$

$(DFT_{N/2})_j \triangleq$ row $j$ of $DFT_{N/2}$

For $0 \le l \le \frac{N}{2}-1$ $\quad y_l = \vec{\alpha}_e \cdot (DFT_{N/2})_l + \left[\vec{\alpha}_o (DFT_{N/2})_l\right] w^j$

$y_{\frac{N}{2}+l} = \vec{\alpha}_e \cdot (DFT_{N/2})_l - \left[\vec{\alpha}_o (DFT_{N/2})_l\right] w^j$




Complexity for $N$ is $S(N)$

$S(N) = 2S(N/2) + O(N)$

$\Rightarrow S(N)$ is $O(N \log N)$

## Quantum Fourier Transform

$\underline{QFT}\ |\psi\rangle = |\hat{\psi}\rangle$

$QFT$ $N \times N$ matrix.

$|\psi\rangle = \sum_{j=0}^{N-1} \alpha_j |j\rangle$

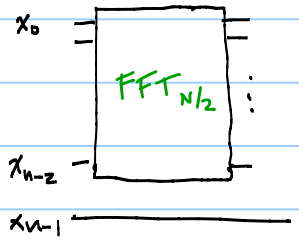
↳ if $N$ is a power of 2 this state is represented by an $n$ bit string

$|\hat{\psi}\rangle = \sum_{k=0}^{N-1} \hat{\alpha}_k |k\rangle$

$\hat{\alpha}_k = \sum_{j=0}^{N-1} w^{jk} \alpha_j$

We use the least significant bit to separate between the odd and even numbers

Perform FFT on the $(n-1)$ most significant bits




If least significant bit is 1, multiply by $w^j$:

$$|j\rangle|0\rangle \longrightarrow |j\rangle|0\rangle$$
$$|j\rangle|1\rangle \longrightarrow w^j|j\rangle|1\rangle$$

Note that $w^j = w^{j_0} \cdot w^{j_1 \cdot 2} w^{j_2 4} \cdots w^{2^{n-2} j_{n-2}}$

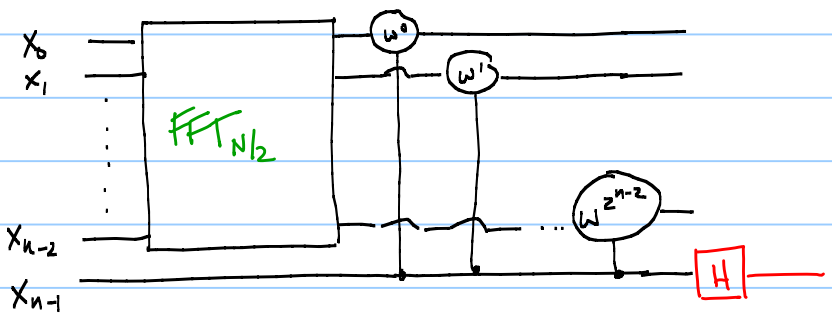
For $k = 0$ to $\log(N/2) - 1$

if ($k^{th}$ bit $= 1$) $\wedge$ (least significant bit $= 1$)

multiply by $w^{2^k}$

$$\begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & w^{2^k} \end{bmatrix}$$

applied to qubits $k$ and $n-1$.




Now need:

$$|j\rangle|0\rangle \longrightarrow \frac{1}{\sqrt{2}}(|j\rangle|0\rangle + |j\rangle|1\rangle)$$
$$|j\rangle|1\rangle \longrightarrow \frac{1}{\sqrt{2}}(|j\rangle|0\rangle - |j\rangle|1\rangle)$$

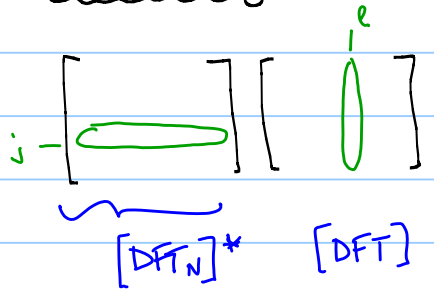
} this is H

$2^n = N$ $\qquad S(n) = S(n-1) + O(n)$

$S(n)$ is $O(n^2)$ $\qquad O(\log^2 N)$

## Properties of DFT:

### DFT is Unitary:




$$= \sum_k (W^{-1})^{jk} W^{kl} = \sum_k \left[W^{l-j}\right]^k = \delta_{lj}$$

$$DFT_N^{-1} = DFT_N^{*} = \left[DFT_N\right]^{T*} = DFT_N^{\dagger}$$

↳ $DFT_N$ is symmetric.

### Fourier Transform converts between Translation + Phase:

$$|\alpha\rangle = \sum_{x=0}^{N-1} \alpha_x |x\rangle \qquad \text{Define } |\alpha_{+j}\rangle = \sum_{x=0}^{N-1} \alpha_x |x+j\rangle \quad \text{(translation)}$$

Now take Fourier transform of $|\alpha_{+j}\rangle$ to get $|\hat{\alpha}_{+j}\rangle$:

$$|\hat{\alpha}_{+j}\rangle = \sum_{y=0}^{N-1} \sum_{x=0}^{N-1} \alpha_x W^{(x+j)y} |y\rangle$$

$$= \sum_{y=0}^{N-1} W^{jy} \underbrace{\sum_{x=0}^{N-1} \alpha_x W^{xy}}_{\hat{\alpha}_y} |y\rangle = \sum_{y=0}^{N-1} W^{jy} \hat{\alpha}_y |y\rangle$$

⇒ Suppose $r$ divides $N$ evenly.

Define $|\phi_r\rangle = \sqrt{\frac{r}{N}} \sum_{k=0}^{\frac{N}{r}-1} |kr\rangle$

$\alpha_x = \sqrt{\frac{r}{N}}$ for $x$, multiple of $r$.

$\alpha_x = 0$ otherwise.

Claim: $DFT_N |\phi_r\rangle = |\phi_{N/r}\rangle$

$$\hat{\alpha}_y = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} w^{xy} \alpha_x = \frac{1}{\sqrt{N}} \sum_{k=0}^{\frac{N}{r}-1} w^{kry} \sqrt{\frac{r}{N}}$$

Case 1: $y$ is a multiple of $N/r$ : $y = j \cdot N/r$

$$\hat{\alpha}_y = \frac{1}{\sqrt{N}} \sum_{k=0}^{\frac{N}{r}-1} w^{k \cdot r \cdot j \frac{N}{r}} \sqrt{\frac{r}{N}} = \frac{1}{\sqrt{N}} \sum_{k=0}^{\frac{N}{r}-1} \underbrace{w^{jkN}}_{=1} \sqrt{\frac{r}{N}}$$

$$= \frac{1}{\sqrt{N}} \frac{N}{r} \sqrt{\frac{r}{N}} = \frac{1}{\sqrt{r}}$$

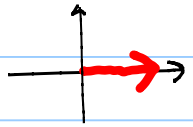
Since there are $r$ multiples of $N/r$ the magnitude squared of these amplitudes sum to 1 and the rest of the amplitudes ($y$ not a multiple of $N/r$) must be 0

Case 2 $y$ not a multiple of $N/r$ $\hat{\alpha}_y = 0$. ← total amplitude sq for multiples of $N/r$ already equal 1.

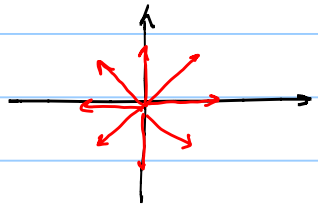
$$DFT |\phi_r\rangle = \sum_{k=0}^{r-1} \sqrt{\frac{1}{r}} \left|k \tfrac{N}{r}\right\rangle$$

More intuitively look at: $\sum_{k=0}^{\frac{N}{r}-1} (w^{yr})^k = \hat{\alpha}_y = 0$.

If $y$ is a multiple of $N/r$ $w^{yr} = 1$ & all the amplitudes in the sum line up:



If $y$ is not a multiple of $N/r$ the amplitudes in the sum cancel:



For factoring, we will be interested in the following subproblem:

Suppose we have a periodic superposition with a shift:

$$\sqrt{r/N} \sum_{k=0}^{N/r-1} |kr + \ell\rangle$$ we want to find $r$

We can't measure directly because $\ell$ is arbitrary. We may have many copies of this state but all with different offset $\ell$.

If we apply the QFT then the shifting factor $\ell$ just adds a phase (and effectively drops out).

By the other property, we get $|\phi_{N/r}\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |k\, N/r\rangle$

If we measure this now we get $\frac{kN}{r}$ where $k$ is chosen at random from $\{0, \ldots, r-1\}$

Let $q = kN/r$. We know both $q$ & $N$. Furthermore,

$$q/N = k/r.$$

If $\gcd(k, r) = 1$ then $N / \gcd(q, N) = r$.

The probability of selecting a $k$ that is relatively prime to $r$ is $\frac{\varphi(r)}{r}$ which is known to be at least $\frac{1}{c \log\log r}$ for some constant $c$.

Our situation is a little more complicated than this since $r$ will not divide $N$ perfectly. We will have:

$$|\phi_r\rangle = \frac{1}{\sqrt{s}} \sum_{k=0}^{s-1} |kr\rangle \qquad s = \lfloor N/r \rfloor$$

$$QFT|\phi_r\rangle = \sum_a \hat{\alpha}_a |a\rangle \qquad \hat{\alpha}_a = \frac{1}{\sqrt{sN}} \sum_{k=0}^{s-1} w^{kra}$$

We want to find the values for $a$ where the $w^{kra}$ line up in a single direction. When we had the case where $r$ divides $N$ perfectly, for the $r$ multiples of $N/r$, the amplitudes all lined up at 1. We have the following approximate version:

Claim: For every $k \in \{0,1,\ldots,r-1\}$ there is an $a$ such that $|ar - kN| \leq r/2$ and for these values of $a$, $\hat{\alpha}_a \geq c/\sqrt{r}$ for some constant $c$.

Note that this means we can find an $a$ such that $|ar - kN| \leq r/2$ and $\gcd(k,r)$ with probability at least $\frac{1}{c \log\log r}$.

Before we prove the claim, let's discuss how it will be used (more details on that later).

We have $|ar - kN| \leq r/2$. We know $a$ & $N$ and we want to find $r$.

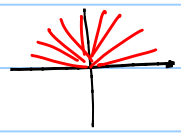
Rearranging $\left|\frac{a}{N} - \frac{k}{r}\right| \leq \frac{1}{2N}$ for some integer $k$ relatively prime to $r$.

We have a very good approximation of $k/r$ we will use properties of rational numbers and continued fractions to find $r$.

**Proof of Claim:** Suppose $|ar - kN| \le r/2$ (will assume wlog $0 \le ar - kN \le r/2$)

$$\hat{\alpha}_a = \frac{1}{\sqrt{sN}} \sum_{\ell=0}^{s-1} w^{\ell r a}$$

$ar \le r/2 \bmod N$, $0 \le \ell \le N/r$ } $w^{\ell ar}$ all lie in:



($\frac{N}{2r}$ of them)

Half of these are within $\pi/4$ of the $\uparrow$ direction.
They contribute at least $1/\sqrt{2}$ to the $\uparrow$ direction.
Total component in $\uparrow$ direction is at least

$$\frac{1}{\sqrt{sN}} \quad \frac{N}{2r} \quad \frac{1}{\sqrt{2}} = \frac{1}{2\sqrt{2}\sqrt{r}} \qquad (s \sim N/r)$$

Now for any value of $kN$, there are at least $r$ consecutive integers that lie in the range $kN \pm r/2$. At least one of them must be a multiple of $r$.