# Fourier Transform Properties - page 1

Wednesday, November 7, 2018 5:17 PM

$DFT_N \equiv$ Fourier Transform mod N

Fourier Transform Converts between Translation + Phase.

$$|\psi\rangle = \sum_{x=0}^{N-1} \alpha_x |x\rangle \qquad |\psi_{+j}\rangle = \sum_{x=0}^{N-1} \alpha_x |x+j \bmod N\rangle$$

(translation).

$$(\alpha_0, \alpha_1\ \alpha_2\ \alpha_3) \overset{+1}{\Longrightarrow} (\alpha_3, \alpha_0, \alpha_1, \alpha_2)$$

Take FT of $|\psi_{+j}\rangle$ to get $|\hat{\psi}_{+j}\rangle$

$$|\hat{\psi}_{+j}\rangle = \sum_{y=0}^{N-1} \underbrace{\sum_{x=0}^{N-1} \frac{\alpha_x\, \omega^{(x+j)y}}{\sqrt{N}}} |y\rangle$$

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

$$= \sum_{y=0}^{N-1} \omega^{jy}\, \hat{\alpha}_y |y\rangle$$

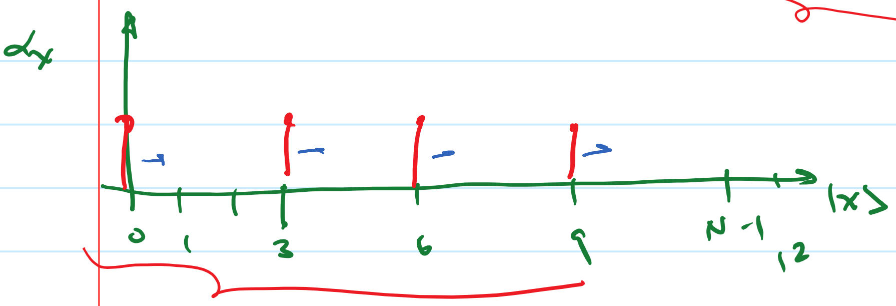
+j

# Fourier Transform Properties - page 2

Thursday, November 8, 2018 12:49 PM

Suppose $r$ divides $N$ evenly.

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




$\alpha_x = \sqrt{\frac{r}{N}}$ if $x$ is a multiple of $r$

$\alpha_x = 0$ otherwise.

Claim: $DFT_N |\phi_r\rangle = |\phi_{N/r}\rangle = \sum \hat{\alpha}_y |y\rangle$

$$\hat{\alpha}_y = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \omega^{x \cdot y} \alpha_x = \frac{1}{\sqrt{N}} \sum_{k=0}^{\frac{N}{r}-1} \omega^{kr \cdot y} \sqrt{\frac{r}{N}}$$

$j\frac{N}{r}$

Case 1: $y$ is a multiple of $\frac{N}{r}$. $y = j \cdot \frac{N}{r}$

$$= \frac{1}{\sqrt{N}} \cdot \sqrt{\frac{r}{N}} \sum_{k=0}^{\frac{N}{r}-1} \underbrace{\omega^{kr(jN/r)}} = \frac{\sqrt{r}}{N} \cdot \frac{N}{r}$$

$r \cdot \left(\frac{1}{\sqrt{r}}\right)^2$

$\omega^{N \cdot j \cdot k} = 1$

$= 1/\sqrt{r}$

Note that since there are $r$ multiples of $N/r$ the sum of the squares of the amplitudes sum to 1. $\Rightarrow$ ($y$ not a multiple of $N/r$ $\hat{\alpha}_y = 0$).

# Fourier Transform Properties - page 3

Thursday, November 8, 2018 12:56 PM

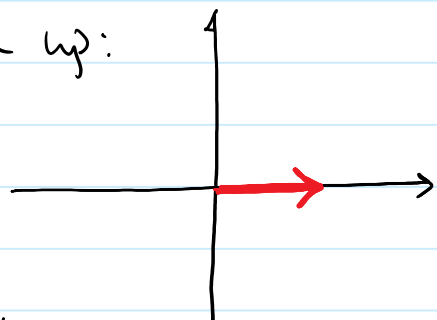
Case 2: $y$ not a multiple of $N/r \Rightarrow \hat{\alpha}_y = 0$.

$$\Rightarrow \quad DFT_N |\Phi_r\rangle = \sum_{k=0}^{r-1} \frac{1}{\sqrt{r}} \left|k \cdot \frac{N}{r}\right\rangle$$

More intuitively look at: $\displaystyle\sum_{k=0}^{\frac{N}{r}-1} \left(\omega^{yr}\right)^k$

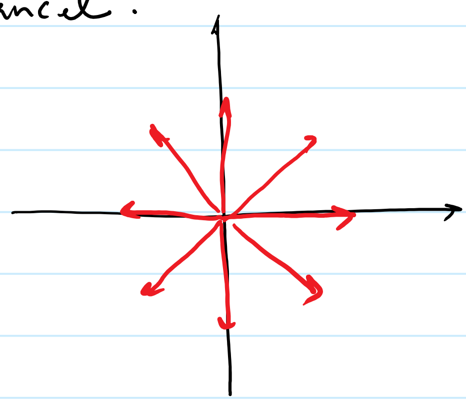
If $y$ is a multiple of $\frac{N}{r}$ $\omega^{yr} = 1$.

All the vectors in the sum line up:



If $y$ is not a multiple of $N/r$.
$\omega^{yr} = \omega^{jr}$ for $0 < j < N-1$.

All the vectors in the sum cancel:



# Fourier Transform Properties - page 4

Thursday, November 8, 2018 1:03 PM

For factoring, we are interested in the following subproblem:

Suppose we have a periodic superposition with a shift:

$$\sqrt{\frac{r}{N}} \sum_{k=0}^{\frac{N}{r}-1} |kr+\underline{\ell}\rangle \Rightarrow \text{Find } r$$

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

$|\phi_r \text{ w/ offset } \ell\rangle$

$\downarrow$ FFT

$|\phi_{N/r}\rangle$

If we apply the QFT then the offset $\ell$ becomes a phase and effectively drops out.

DFT$_N$ yields $\displaystyle \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} w^{\ell \cdot k \cdot N/r} |k \cdot \tfrac{N}{r}\rangle$

If we measure, we get $k \cdot \frac{N}{\underline{r}} = q$.

where k is chosen at random from $\{0, 1, .., r-1\}$

# Fourier Transform Properties - page 5

Thursday, November 8, 2018 1:12 PM

Let $q = \frac{kN}{r}$ We know $q$ and $N$.

$\frac{q}{N} = \frac{k}{r}$ If $\gcd(k, r) = 1$

$$\gcd(N, q) = \gcd\left(N, \frac{kN}{r}\right) = \frac{N}{r}.$$

$N/r$ evenly divides $N$ + $q$

So $\gcd(N, q) = a \cdot N/r$.

Suppose $a > 1$.

$a\frac{N}{r}$ evenly divides $N$ and $q$.

$$r = \frac{N}{\gcd(N, q)}.$$

$\frac{N}{a\frac{N}{r}} = \frac{r}{a} \Rightarrow a | r$

$\frac{kN/r}{aN/r} = \frac{k}{a} \Rightarrow a | k$.

$\gcd(k, r) \neq 1$.

The probability of Selecting a $k$ that is relatively prime to $r$ is:

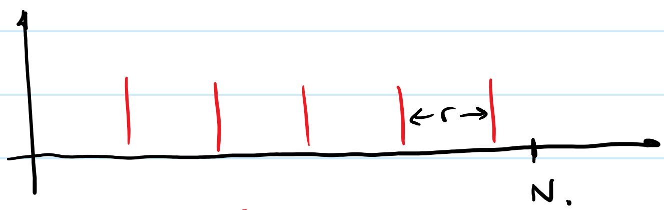
$$\frac{\phi(r)}{r} \geq \frac{1}{c \log \log r}$$

# Fourier Transform Properties - page 6

Thursday, November 8, 2018 1:21 PM

Our situation is a little more complicated since r will not divide N perfectly.

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




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

We want to find the values where the $w^{kra}$ line up in a single direction.

For the case where $r|N$ these were multiples of $\frac{N}{r}$.

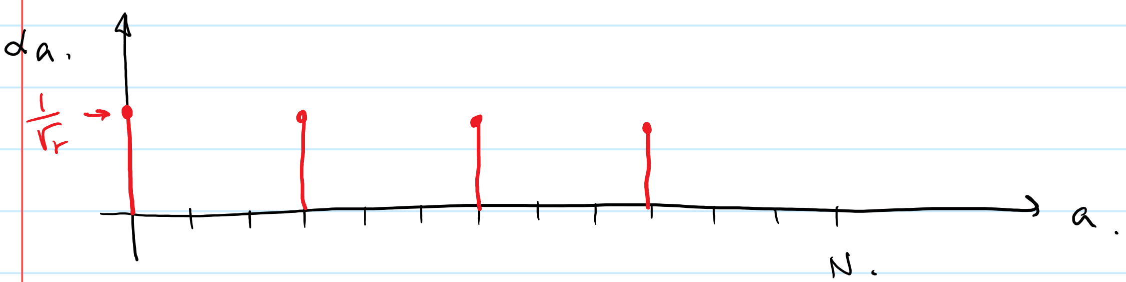
Friday, November 9, 2018 11:24 AM

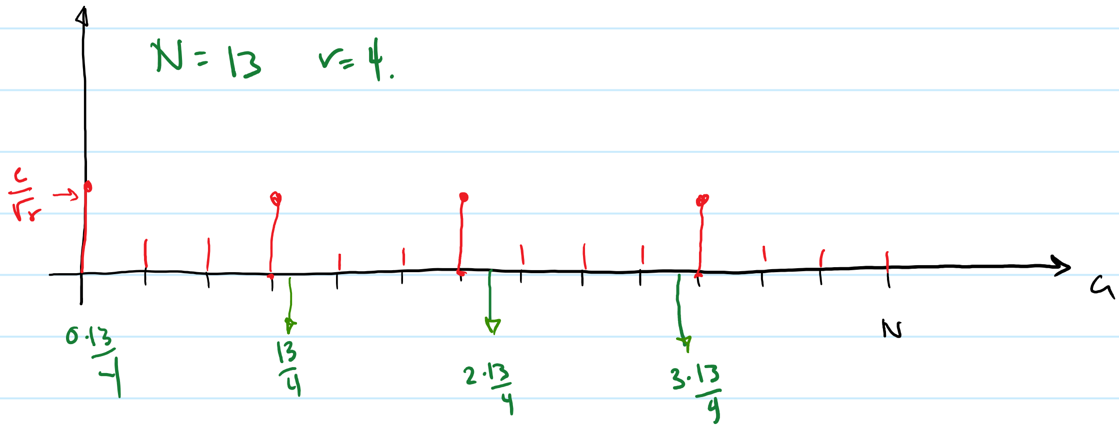
Here's an approximate version:

Claim: For every $k \in \{0, 1, .., r-1\}$ there is a unique $a_k$ such that $|a_k \cdot r - kN| \le r/2$ and $|\hat{\alpha}_{a_k}| \ge c/\sqrt{r}$ for some constant $c$.

$a_k = \frac{kN}{r} \pm \delta \qquad \delta \le 1/2.$

For $r|N$: $N = 12 \quad r = 4.$




If we measure $|a\rangle$ probability of getting an $a_j$

$$= \sum_{j=0}^{r-1} |\hat{\alpha}_{a_k}|^2 \ge r \cdot \left(\frac{c}{\sqrt{r}}\right)^2 \ge c^2$$

Probability of getting $a_k$ where $\gcd(k,r) = 1$ is $\Omega\left(\frac{1}{\log \log r}\right)$

# Fourier Transform Properties - page 8

Thursday, November 8, 2018 3:48 PM

With probability $\geq \Omega\left(\frac{1}{\lg \lg r}\right)$ can get a

such that $|ar - kN| \leq r/2$ and $\gcd(k, r) = 1$.

We know a and N and we want to find r.

$$\left|\frac{a}{N} - \frac{k}{r}\right| \leq \frac{1}{2N}.$$

for some int k
$\gcd(k,r) = 1$.

We know $\frac{a}{N}$ which is a good approximation of $\frac{k}{r}$. Will use properties of rational numbers and continued fractions to recover r.

# Fourier Transform Properties - page 9

Thursday, November 8, 2018 3:52 PM

**Claim:** For every $k \in \{0, 1, .., r-1\}$ there is a unique $a_k$ such that $|a_k r - kN| \le r/2$. $|\hat{\alpha}_{a_k}| \ge c/\sqrt{r}$ for some constant $c$.

**Proof** $a_k = k\frac{N}{r}$ rounded to the nearest int.

Since $N/r > 1$, each $a_k$ will be unique.

$$\left|a_k - \frac{kN}{r}\right| \le 1/2 \Rightarrow |a_k \cdot r - kN| \le r/2$$

Now to determine $\hat{\alpha}_{a_k}$:

W.l.o.g. assume $0 \le ar - kN \le r/2$.

$$\hat{\alpha}_a = \frac{1}{\sqrt{sN}} \sum_{l=0}^{s-1} (w^{ra})^l$$

$ar \bmod N = d \le r/2$.

$0 \le l < N/r$

$$w^{ra} = w^d = e^{\frac{2\pi i}{N} \cdot d}$$

$\theta < \frac{\pi}{(N/r)}$

$$\hat{\alpha}_a = \frac{1}{\sqrt{sN}} \sum_{l=0}^{s-1} e^{l \cdot \theta i}$$

$0 \le l < \frac{N}{r} - 1$

$\theta < \pi/(N/r)$.

# Fourier Transform Properties - page 10

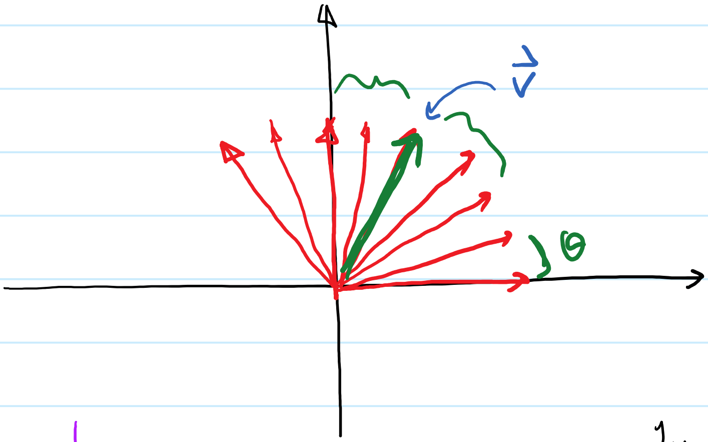
Friday, November 9, 2018 12:03 PM

these angles are all in the range $0 \ldots \pi$.

$$\hat{\alpha}_a = \frac{1}{\sqrt{SN}} \sum_{l=0}^{S-1} e^{l \cdot \theta i}$$

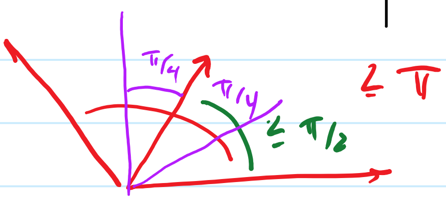
$0 \le l < \frac{N}{r} - 1$

$\theta < \pi/(N/r)$.




Take middle angle. $\vec{v}$

$\sim \theta \cdot \frac{N}{2r}$




1. All vectors have a positive component in $\vec{v}$ direction.

2. At least half of the vectors are within $\pi/4$ of $\vec{v}$.

3. At least half of the vectors have magnitude $\ge 1/\sqrt{2}$ in the direction of $\vec{v}$.

$$\left| \sum_{l=0}^{S-1} e^{l\theta i} \right| \ge \frac{N}{2r} \cdot \frac{1}{\sqrt{2}}$$

$$\hat{\alpha}_a \ge \frac{1}{\sqrt{N/r}\sqrt{N}} \cdot \frac{N}{2r} \cdot \frac{1}{\sqrt{2}} \ge \frac{1/2\sqrt{2}}{\sqrt{r}}.$$