Input: vector $\vec{v}$ or function $f: \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$

Output: $F_m \vec{v}$ or $\hat{f}: \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$

Formula for new coefficients:

$$(F_m V)_n = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} V_k \omega_m^{nk}$$

or

$$\hat{f}(n) = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} f(k) \omega_m^{nk}$$

Computer

Demo

Runtime?

Classical: discrete fourier transform via matrix multiplication

$$O(m^2)$$

Fast Fourier Transform : $O(m \log(m))$

Quantum Fourier Transform: F_m is a unitary matrix

$m = 2^n$
n qubits
can store
$0 = 00000\cdots0$
up to
$m-1 = 111\cdots1$

$$\sum_{x=0}^{m-1} f(x)|x\rangle \longmapsto \sum_{y=0}^{m-1} \hat{f}(y)|y\rangle$$

$$= \frac{1}{\sqrt{m}} \sum_{y=0}^{m-1} \left(\sum_{k=0}^{m-1} \omega_m^{yk} f(k) \right) |y\rangle$$

Can be implemented with $O(\log_2^2(m))$ gates

(H and a controlled phase gates)

QFT of a periodic state

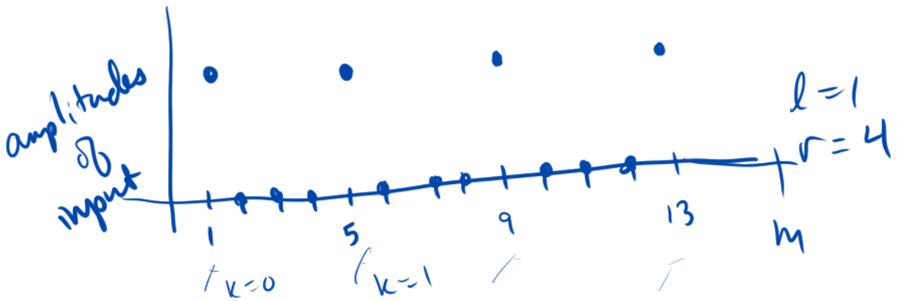
$$\text{Input:}\quad \frac{1}{\sqrt{m/r}} \sum_{k=0}^{m/r-1} |\ell + kr\rangle$$

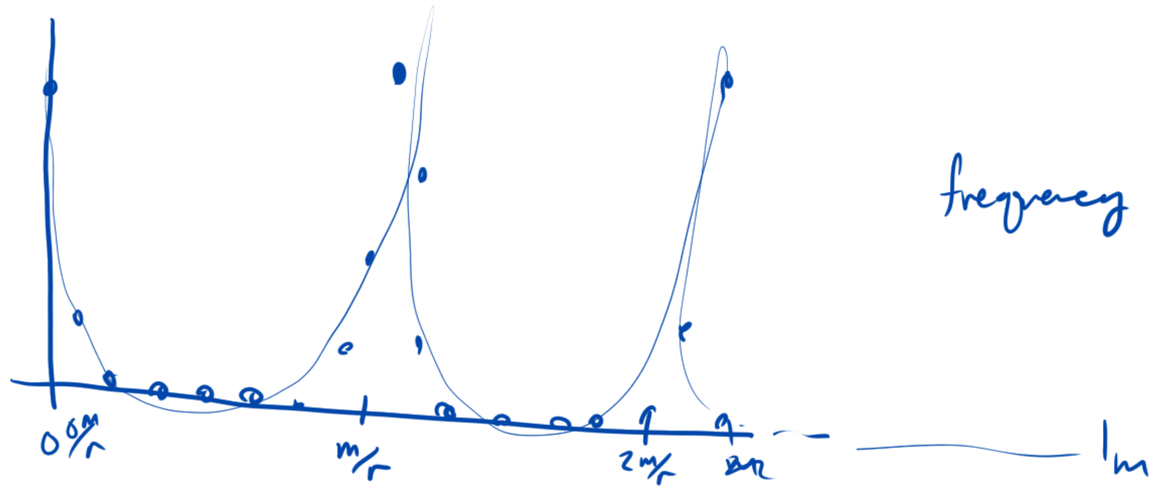
$m = 2^n$

$r \mid m$

↑ period

$$\xrightarrow{QFT_m} \frac{1}{\sqrt{m}\sqrt{m/r}} \sum_{y=0}^{m-1} \left(\sum_{k=0}^{m/r-1} \omega_m^{(\ell+kr)y} \right) |y\rangle$$

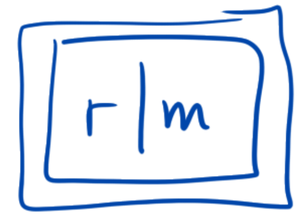


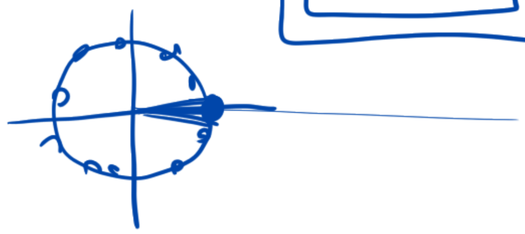


QFT reminder:

$$\sum_{x=0}^{m-1} \alpha_x |x\rangle \longmapsto \frac{1}{\sqrt{m}} \sum_{y=0}^{m-1} \left(\sum_{k=0}^{m-1} \alpha_k \omega_m^{ky} \right) |y\rangle$$

Amplitude @ $|y\rangle$ is $\frac{1}{\sqrt{m}\sqrt{m/r}} \sum_{k=0}^{m/r-1} \omega_m^{(\ell+kr)y}$





If $y = 0, \frac{m}{r}, 2\frac{m}{r}, 3\frac{m}{r}, \ldots$ i.e. $y \in \frac{m}{r}\mathbb{Z}$.

$$\text{ampl} = \frac{1}{\sqrt{m}\sqrt{m/r}} \omega_m^{\ell y} \sum_{k=0}^{m/r-1} \omega_m^{kry}$$

$$= \frac{1}{\sqrt{m}\sqrt{m/r}} \omega_m^{\ell y} \left(\frac{m}{r}\right)$$

$$|\text{ampl}|^2 = \frac{1}{r}$$

$kry \in km\mathbb{Z} \subseteq m\mathbb{Z}$

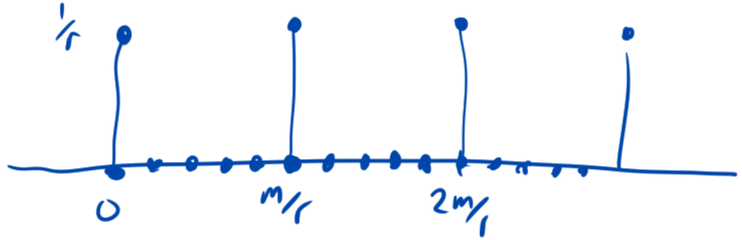
so

$\omega_m^{kry} = (\omega_m^m)^{\text{integer}} = 1^{\text{integer}} = 1$

So: $|\text{ampl}|^2 = \frac{1}{r}$ @ the r positions $y = 0, \frac{m}{r}, \frac{2m}{r}, \ldots$

Since $\sum |\text{ampl}|^2 = 1$, the rest must be 0.

output of QFT



If $m/r \notin \mathbb{Z}$?

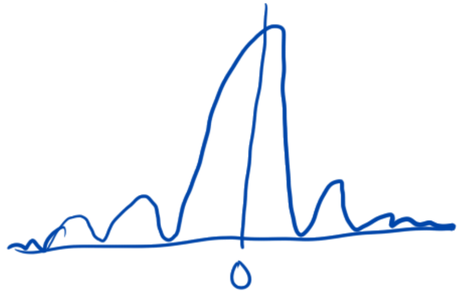
Amplitude @ $|y\rangle$ is $\frac{1}{\sqrt{m}\sqrt{s}} \sum_{k=0}^{s-1} \omega_m^{(\ell+kr)y}$ where $s = \lfloor \frac{m}{r} \rfloor$ or $\lfloor \frac{m}{r} \rfloor + 1$

$$|\text{ampl}|^2 = \frac{1}{sm} \left| \sum_{k=0}^{s-1} \omega_m^{kry} \right|^2$$

$$= \frac{1}{sm} \left| \frac{1 - \omega_m^{rys}}{1 - \omega_m^{ry}} \right|^2$$

$$= \frac{1}{sm} \left| \frac{\sin\left(\frac{2\pi rys}{m}\right)}{\sin\left(\frac{2\pi ry}{m}\right)} \right|^2$$

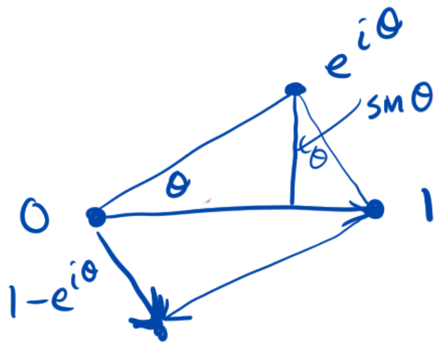
$$= \frac{1}{sm} \left| \frac{\sin(\theta s)}{\sin(\theta)} \right|^2 \quad \text{where } \theta = \frac{2\pi ry}{m}$$



peaks @ $\theta \to 2\pi\mathbb{Z}$

$y \to \frac{m}{r}\mathbb{Z}$

$\frac{y}{m} \to \frac{\mathbb{Z}}{r}$



Observation / Bottom Line:

output has magnitude peaks @ $\frac{m}{r}\mathbb{Z}$

and the offset (ℓ) is absorbed into the phase not magnitude.

Computer Demo

Computer Demo

Factoring N

Recall: If we can find $x \in \mathbb{Z}/N\mathbb{Z}$ s.t. $x^2 \equiv 1$, $x \not\equiv \pm 1 \pmod N$ then we can factor N, by $\gcd(x-1, N)$ or $\gcd(x+1, N)$.

Ex. $N = 15$ $\quad \varphi(15) = 8$

	1	α	α^2	α^3	α^4	α^5	α^6	α^7	$(\alpha^8 = 1)$
$\alpha = 2$	1	2	4	8	1				
$\alpha = 13$	1	13	11	7	1				
$\alpha = 11$	1	11	1						

mult. order = 4 of 2

$\alpha^4 = 1$
$\alpha^2 = 4$
$((\alpha^2)^2 = 1)$

Idea: Take a random α, find $\alpha^r = 1$
If r is even, compute $\alpha^{r/2}$
If $\alpha^{r/2} \not\equiv \pm 1$, we win
since $(\alpha^{r/2})^2 \equiv 1$
So take $\gcd(\alpha^{r/2} + 1, N)$

Finding mult. order of α ⇓ factoring!

Shor's Algorithm

classical (1) Take a random α mod N, $\alpha \neq 0$.

quantum (2) Find the order of r in $(\mathbb{Z}/N\mathbb{Z})^*$.

classical (3) Check if r is even, and $\alpha^{r/2} \not\equiv \pm 1 \pmod{N}$. } Luck (If not, change α, try again.)

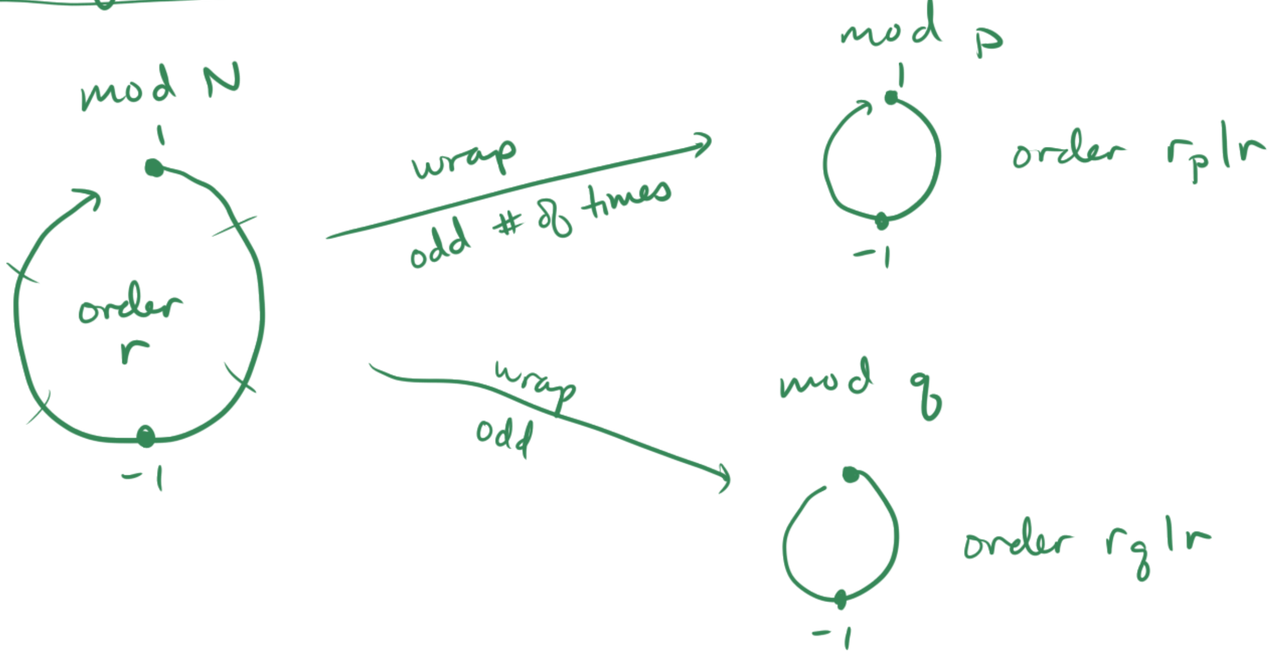
classical (4) If so, take $\gcd(\alpha^{r/2} - 1, N)$.

Proposition Let $N = pq$, p, q odd primes.

Then $\text{Prob}\left(\text{ord}(x) \text{ is even and } x^{\frac{\text{ord}(x)}{2}} \not\equiv -1 \pmod N \right) \geq \frac{1}{2}$ as x ranges over $(\mathbb{Z}/N\mathbb{Z})^*$.

Proof. Suppose $\text{ord}(x)$ is even and $x^{\frac{\text{ord}(x)}{2}} \equiv -1 \pmod N$.

Mult. dyn. of x:



-1 appears in a cycle mod p

$\iff x^{r/2} \equiv -1 \equiv g^{\frac{p-1}{2}}$

$\iff x = g^s$ where $s \mid \frac{p-1}{2}$.

$p - 1 = 2^{\sim}(\text{odd})$

This occurs at most $\frac{1}{2}$ of the time.

So at most $\frac{1}{4}$ of the residues of $(\mathbb{Z}/N\mathbb{Z})^*$ have this property mod p & mod q i.e. land in this case.