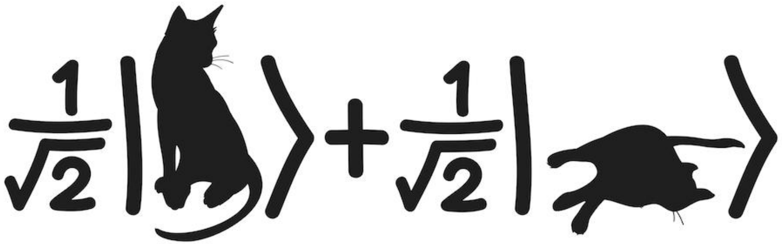
Quantum Mechanics & Quantum Computation



Umesh V. Vazirani

University of California, Berkeley

Lecture 13: Quantum Fourier Transform

Period Finding

Fourier transform

$\omega = e^{2\pi i/N}$

$$F_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \cdots & \omega^{(N-1)^2} \end{pmatrix}$$

$$(F_N)_{jk} = \omega^{jk}$$

$$\frac{1}{\sqrt{N}}\begin{pmatrix} 1 & - & - & 1 \\ 1 & \omega & - - & \omega^{N-1} \\ 1 & & & \\ \vdots & & & \\ 1 & \omega^{N-1} & - - - & \omega^{(N-1)^2} \end{pmatrix}\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{N-1} \end{pmatrix}$$

$\boxed{\nearrow}$ see k wp $|\beta_k|^2$

Convolution - multiplication property of F.T.

$$F_N\left(\sum_j \alpha_j |j\rangle\right) = \sum_k \beta_k |k\rangle$$

<u>Shift</u>

$$\frac{1}{\sqrt{N}}\begin{pmatrix} 1 & - & - - & 1 \\ 1 & \omega & - - & \omega^{N-1} \\ 1 & & & \\ \vdots & & & \\ 1 & \omega^{N-1} & - - - & \end{pmatrix}\begin{pmatrix} \alpha_{N-1} \\ \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-2} \end{pmatrix} = \begin{pmatrix} 1 & \beta_0 \\ \omega & \beta_1 \\ \omega^2 & \vdots \\ \vdots & \vdots \\ \omega^{N-1} & \beta_{N-1} \end{pmatrix}$$

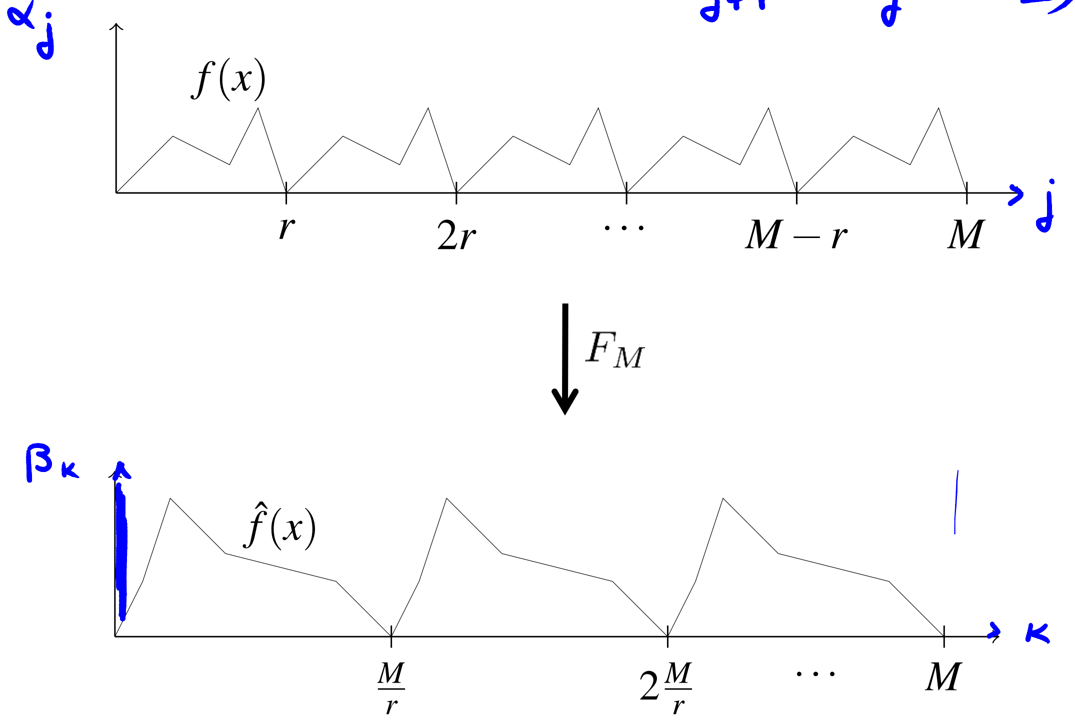
$\boxed{\nearrow}$ see k wp. $|\beta_k|^2$

Quantum Fourier Sampling:

Fourier transform

$$F_M\left(\sum_{j=0}^{M-1}\alpha_j|j\rangle\right) = \sum_{k=0}^{M-1}\beta_k|k\rangle$$

$$\alpha_{j+r}=\alpha_j \quad \Rightarrow \quad \beta_{k+\frac{M}{r}}=\beta_k$$



$$F_M\left(\frac{1}{\sqrt{M}}\sum_{j=0}^{M-1}|j\rangle\right)$$

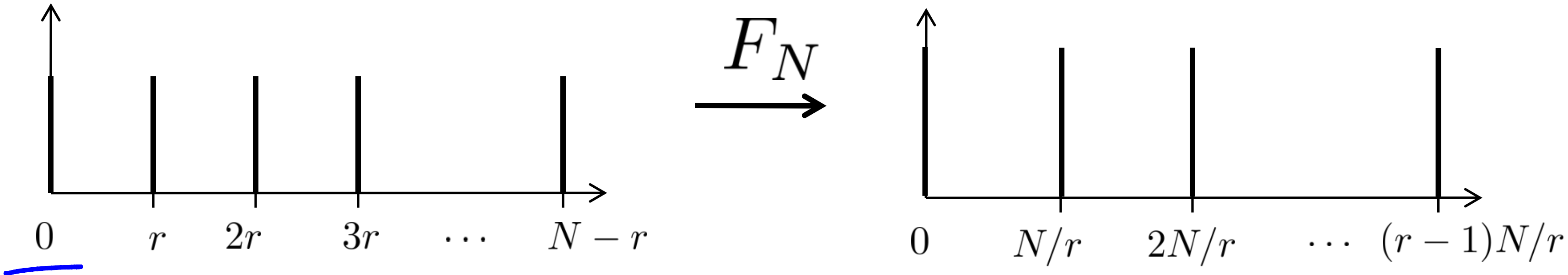
$$= \underline{|0\rangle}$$

$r=\underline{1} \qquad \frac{M}{r}=M$

Fourier transform

r/N

We will prove a special case:



$$\sqrt{\frac{r}{N}}\left(|0\rangle + |r\rangle + |2r\rangle + \cdots + |N-r\rangle\right) \xrightarrow{F_N} \frac{1}{\sqrt{r}}\left(|0\rangle + \left|\frac{N}{r}\right\rangle + \left|\frac{2N}{r}\right\rangle + \cdots \left|\frac{(r-1)N}{r}\right\rangle\right)$$

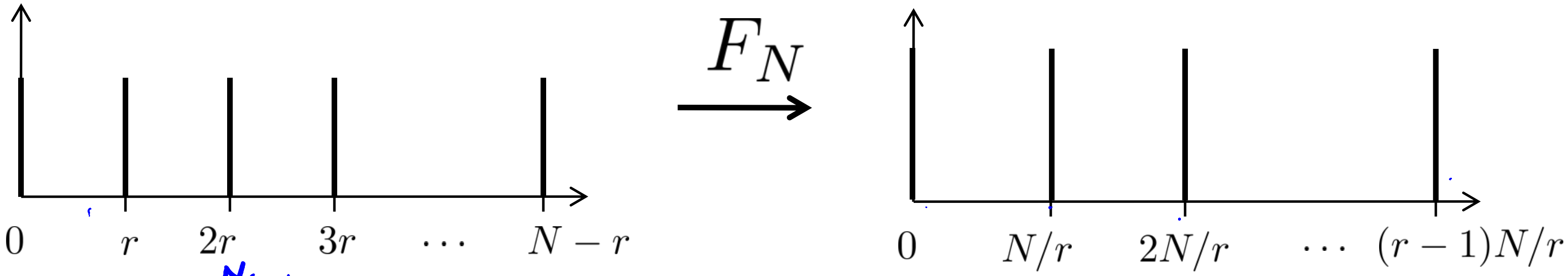
$$|0\rangle \xrightarrow{F_N} \frac{1}{\sqrt{N}}\left(|0\rangle + |1\rangle + |2\rangle + \cdots + |N-1\rangle\right)$$

$$\frac{1}{\sqrt{N}}\begin{pmatrix}1 & 1 & \cdots & 1\\ 1 & \omega & \cdots & \omega^{N-1}\\ \vdots & \omega^2 & \cdots & \\ 1 & \omega^{N-1} & \cdots & \end{pmatrix}\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix} = \frac{1}{\sqrt{N}}\begin{pmatrix}1\\1\\\vdots\\1\end{pmatrix} =$$

Fourier transform

$r \mid N$

We will prove a special case:



$$\sqrt{\frac{r}{N}} \sum_{j=0}^{N/r-1} |jr\rangle \xrightarrow{F_N} \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \left|k\frac{N}{r}\right\rangle$$

$$F_N = \frac{1}{\sqrt{N}} \begin{array}{cc} & y \\ x & \begin{pmatrix} \omega^{xy} \end{pmatrix} \end{array}$$

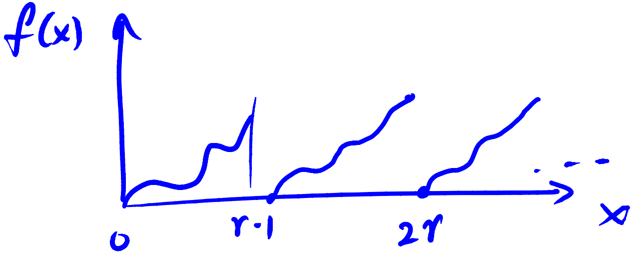
$$\sum_{j=0}^{N/r-1} \sqrt{\frac{r}{N}} \frac{1}{\sqrt{N}} \omega^{jrkN/r}$$

$$= \frac{\sqrt{r}}{N} \sum_{j=0}^{N/r-1} \omega^{jkN} = \frac{\sqrt{r}}{N} \times \frac{N}{r} = \frac{1}{\sqrt{r}}$$

Period Finding:

$$f : \{0, 1, \dots, N-1\} \to S$$

f is periodic with period r/N.



$$f(x) = f(x + r \pmod N)$$

Given a black box or C_f.

Determine r.

$$x \longrightarrow \boxed{C_f} \longrightarrow f(x)$$

Period finding

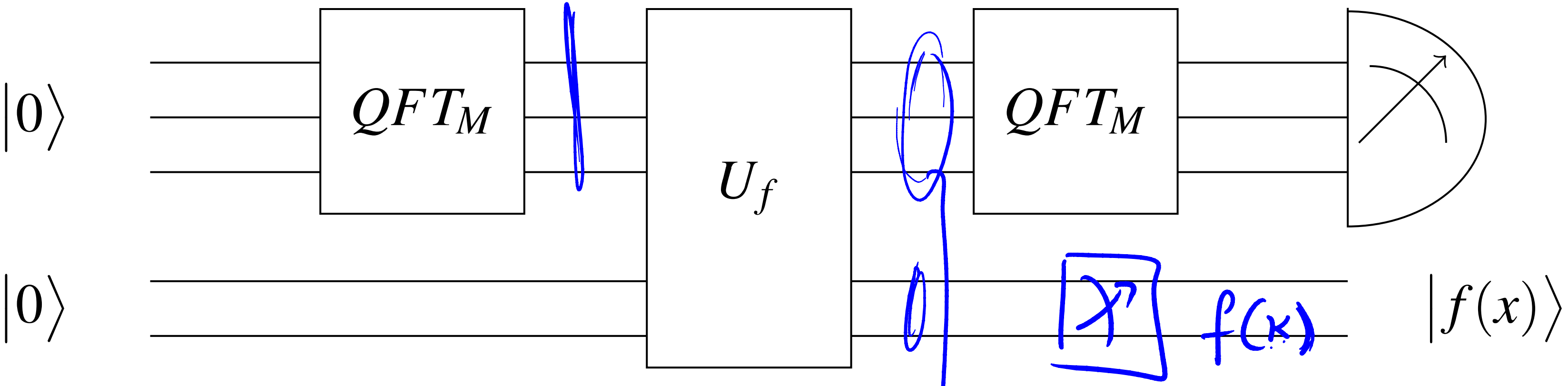
$f: \{0, \dots, M-1\} \to S$

$r \mid M$

$f(x) = f(x+r)$

$\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle$

$\sum_{x=0}^{M-1} |x\rangle |f(x)\rangle$

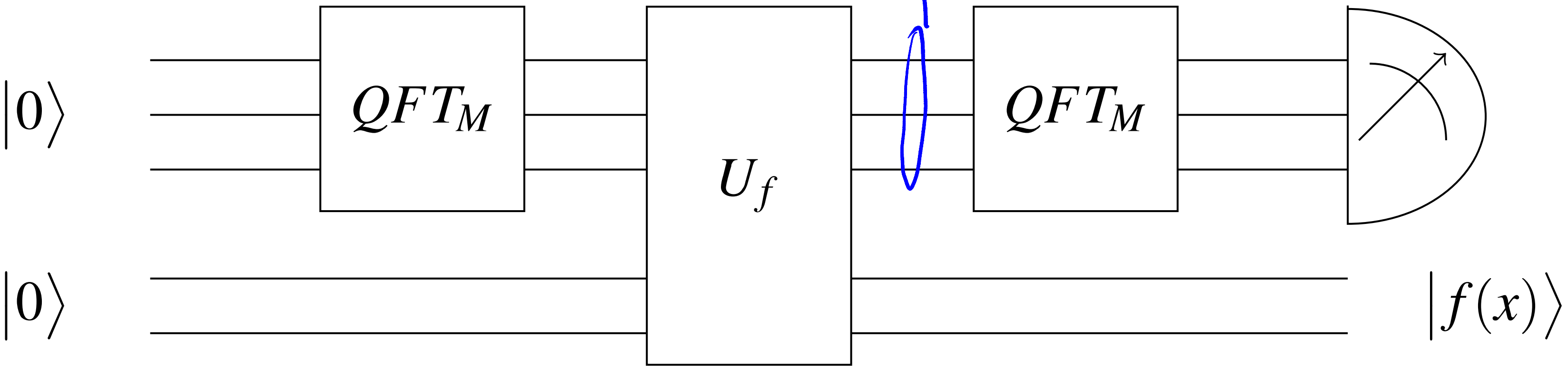


$$\frac{1}{\sqrt{M}} \begin{pmatrix} 1 & \cdots & & 1 \\ 1 & \omega & \cdots & \\ \vdots & & & \\ 1 & \omega^{N-1} & \cdots & \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \frac{1}{\sqrt{M}} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$$

$$\sqrt{\frac{r}{M}} \left(|k\rangle + |k+r\rangle + |k+2r\rangle + \cdots + |k+M-r\rangle \right)$$

Period finding

$$\sqrt{\frac{r}{M}} \sum_{j=0}^{\frac{M}{r}-1} |jr+\cancel{k}\rangle \xrightarrow{QFT_M} \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} \left|l \frac{M}{r}\right\rangle$$



$s \frac{M}{r}$ where $s \in_R \{0, 1, \ldots, r-1\}$

<u>Repeat</u> GCD $= \frac{M}{r}$