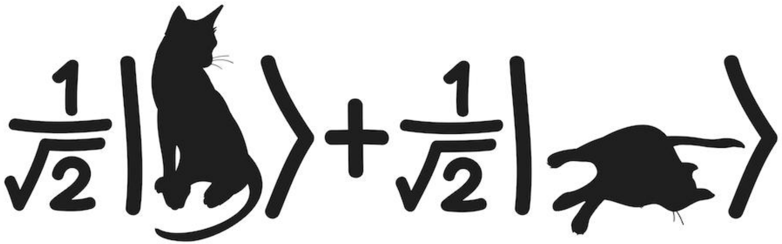
Quantum Mechanics & Quantum Computation



Umesh V. Vazirani
University of California, Berkeley

Lecture 14: Quantum Factoring

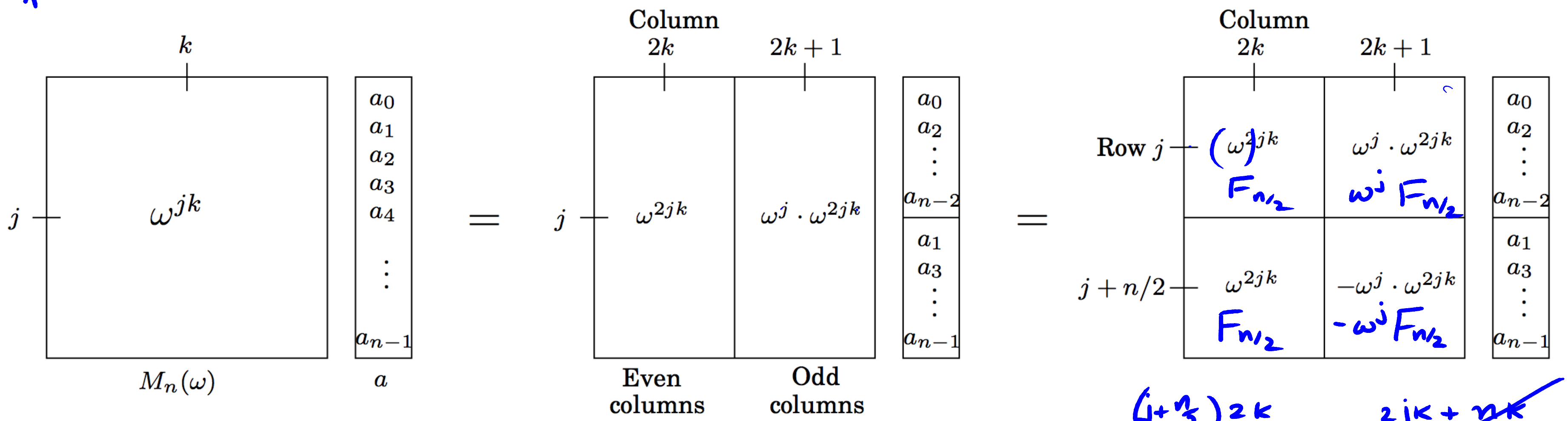
QFT Circuit

$\omega^n = 1$ $\quad \omega = e^{2\pi i/n}$

$= \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$.

$$
\begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ \vdots \\ b_{n-1} \end{bmatrix}
=
\begin{bmatrix}
1 & 1 & 1 & \cdots & 1 \\
1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\
1 & \omega^2 & \omega^4 & \cdots & \omega^{2(n-1)} \\
 & & \vdots & & \\
1 & \omega^j & \omega^{2j} & \cdots & \omega^{(n-1)j} \\
 & & \vdots & & \\
1 & \omega^{(n-1)} & \omega^{2(n-1)} & \cdots & \omega^{(n-1)(n-1)}
\end{bmatrix}
\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix}
$$

F_n



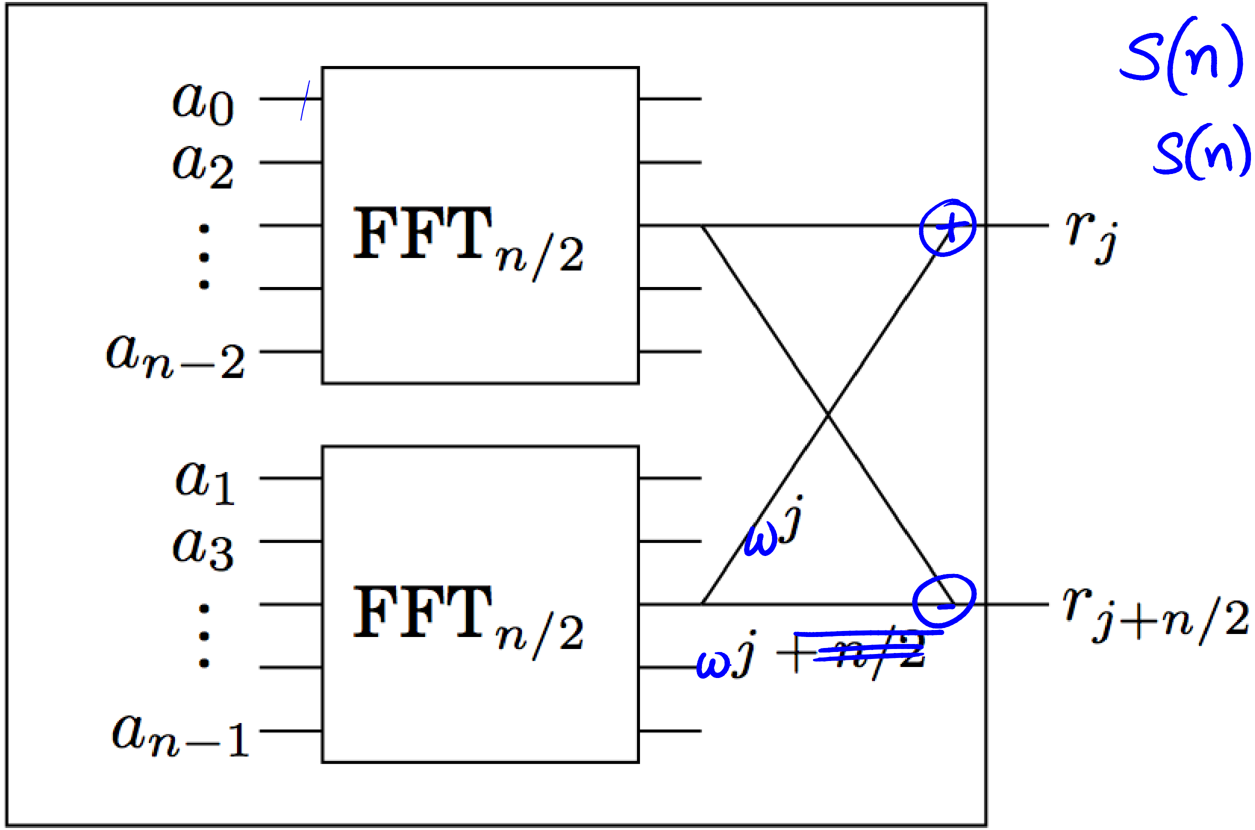
$$\omega^{(j+\frac{n}{2})2k} = \omega^{2jk + \cancel{nk}}$$

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

$$\omega^2 = e^{2\pi i/(n/2)}$$

$$\begin{array}{r} \text{Row } j \\ \\ \\ j+n/2 \end{array} \begin{bmatrix} M_{n/2} \begin{bmatrix} a_0 \\ a_2 \\ \vdots \\ a_{n-2} \end{bmatrix} + \omega^j M_{n/2} \begin{bmatrix} a_1 \\ a_3 \\ \vdots \\ a_{n-1} \end{bmatrix} \\ \\ M_{n/2} \begin{bmatrix} a_0 \\ a_2 \\ \vdots \\ a_{n-2} \end{bmatrix} - \omega^j M_{n/2} \begin{bmatrix} a_1 \\ a_3 \\ \vdots \\ a_{n-1} \end{bmatrix} \end{bmatrix}$$

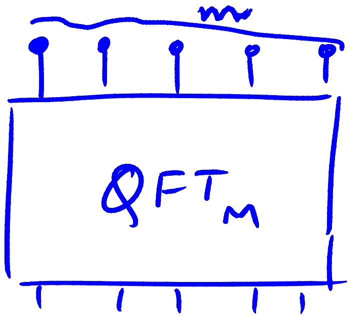
$\mathbf{FFT}_n$ **(input:** $a_0, \ldots, a_{n-1}$**, output:** $r_0, \ldots, r_{n-1}$**)**



$S(n) = 2S(\frac{n}{2}) + O(n)$

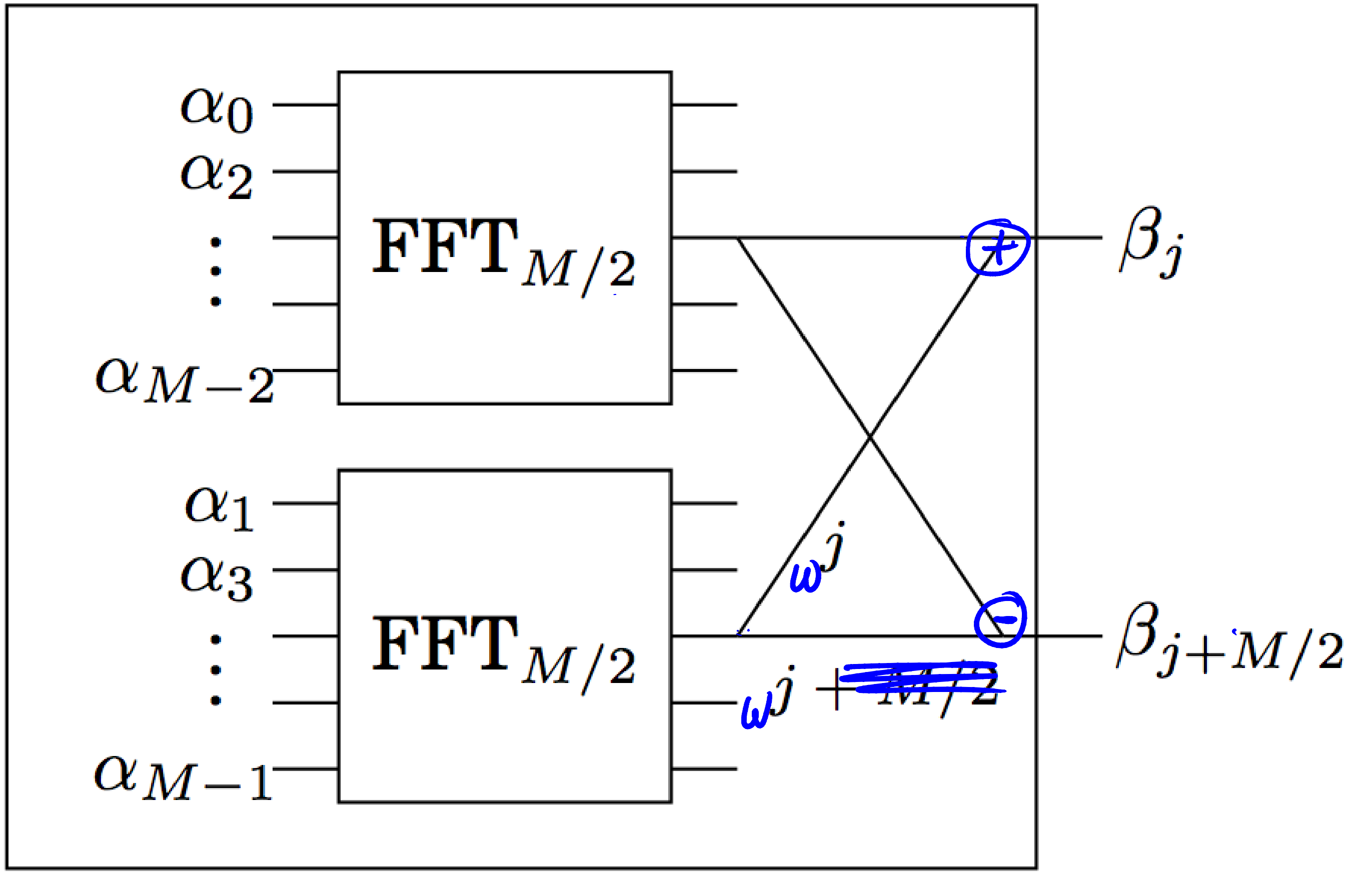
$S(n) = O(n \lg n)$

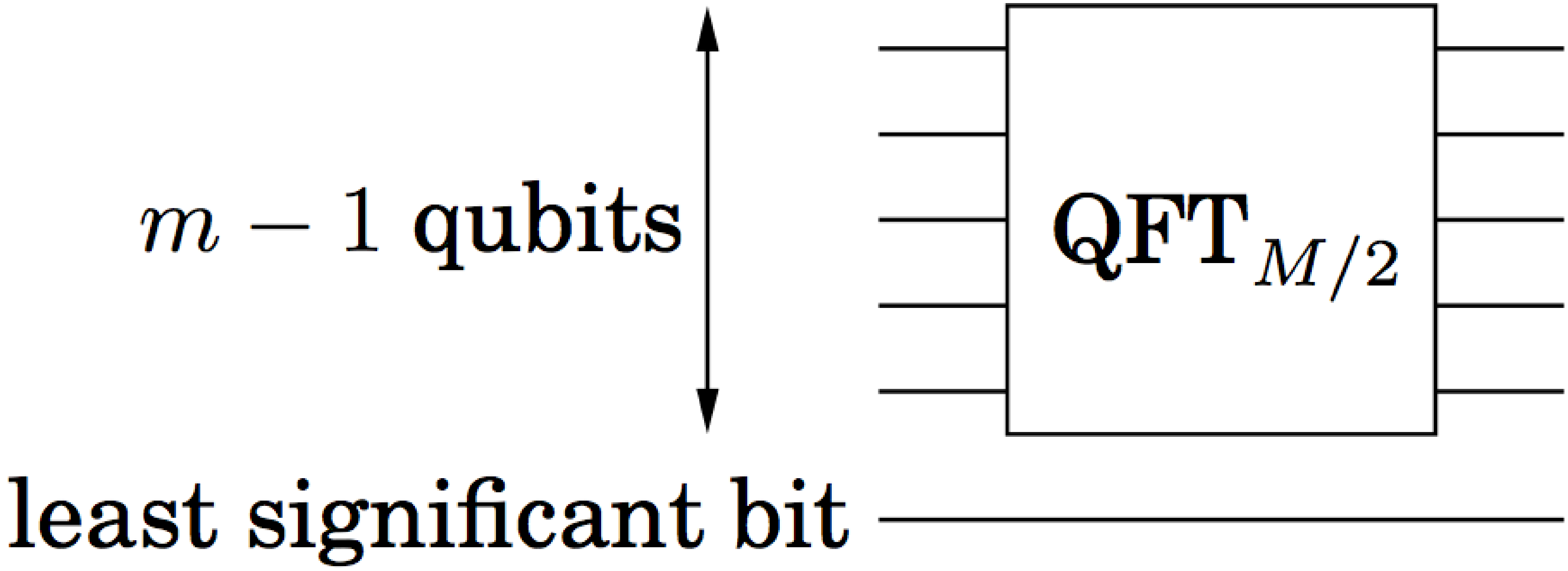
$M = 2^m$

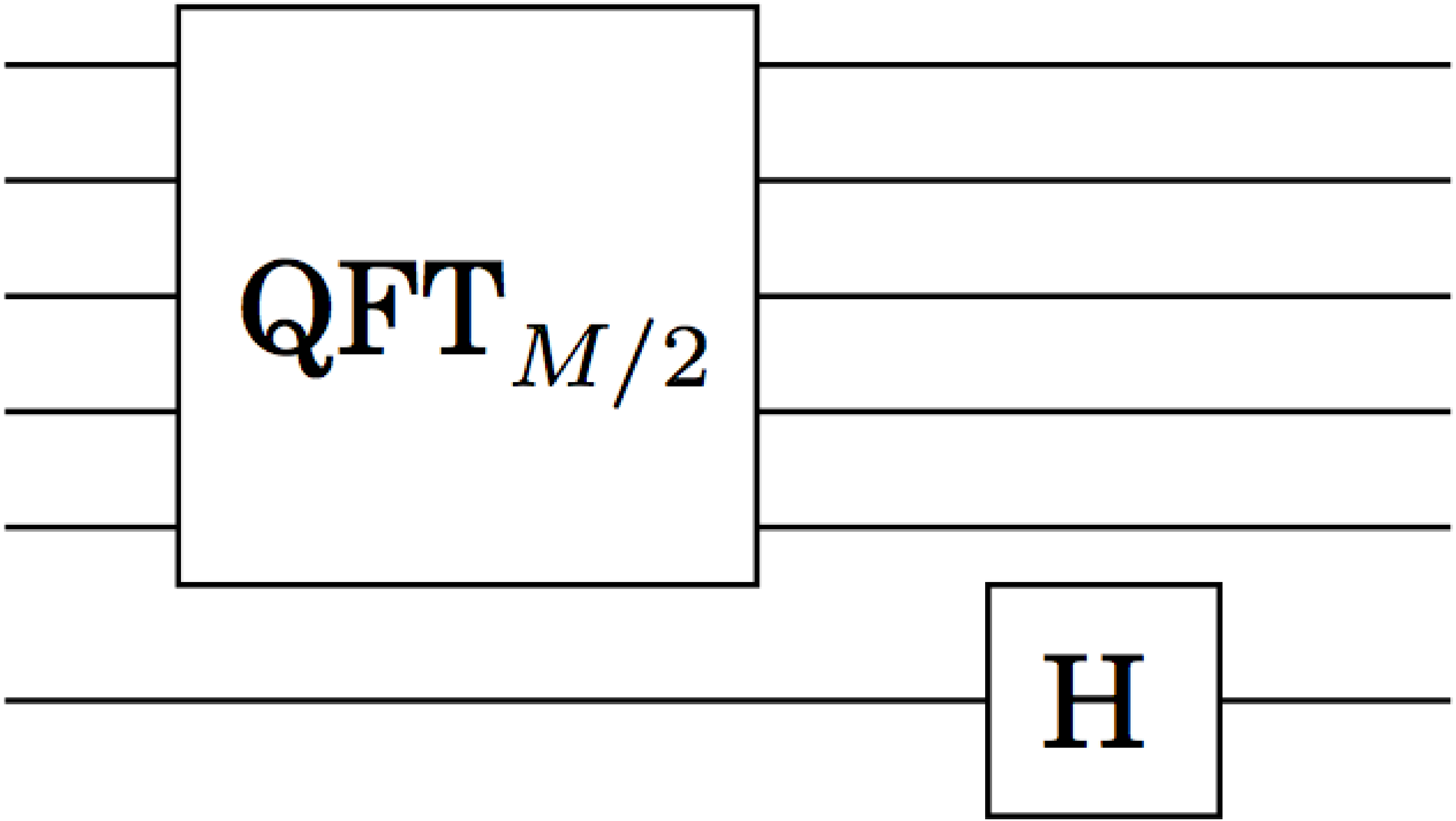


$$
\begin{bmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \vdots \\ \beta_{M-1} \end{bmatrix}
= \frac{1}{\sqrt{M}}
\begin{bmatrix}
1 & 1 & 1 & \cdots & 1 \\
1 & \omega & \omega^2 & \cdots & \omega^{M-1} \\
1 & \omega^2 & \omega^4 & \cdots & \omega^{2(M-1)} \\
 & \vdots & & & \\
1 & \omega^j & \omega^{2j} & \cdots & \omega^{(M-1)j} \\
 & \vdots & & & \\
1 & \omega^{(M-1)} & \omega^{2(M-1)} & \cdots & \omega^{(M-1)(M-1)}
\end{bmatrix}
\begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{M-1} \end{bmatrix}
$$

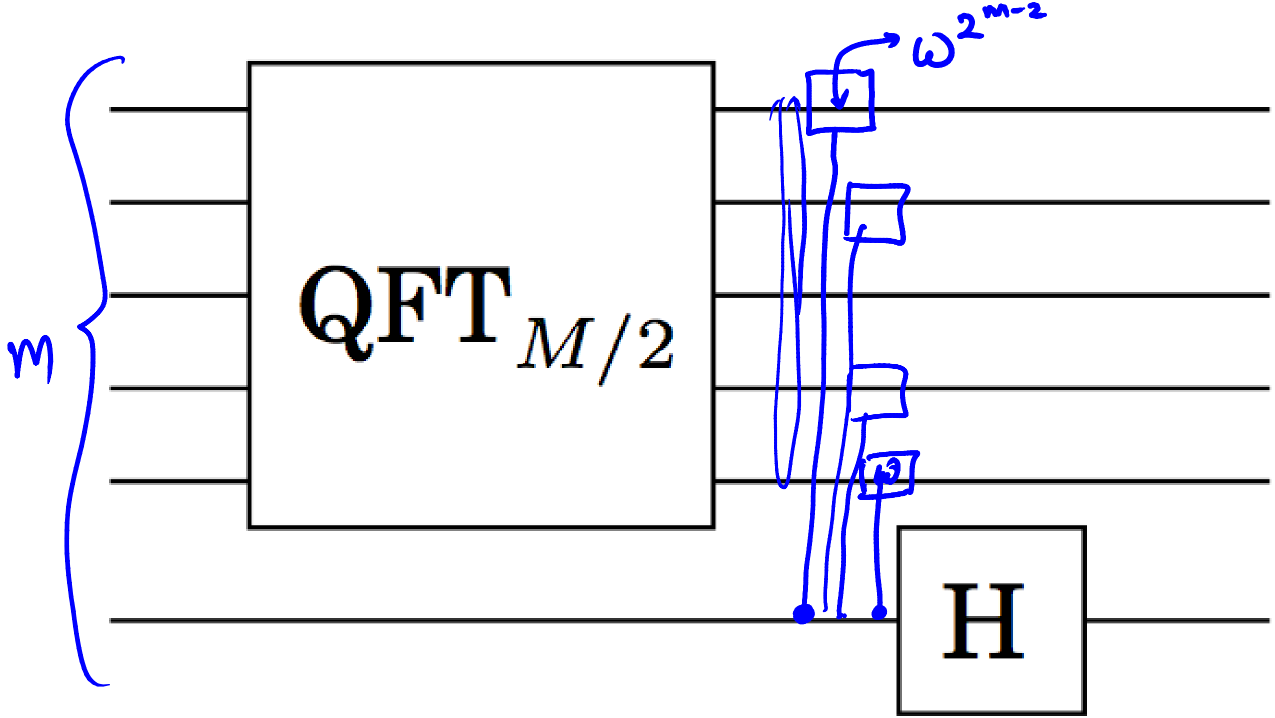
$\mathbf{FFT}_M$ (input: $\alpha_0, \ldots, \alpha_{M-1}$, output: $\beta_0, \ldots, \beta_{M-1}$)




$m-1$ qubits
$\mathbf{QFT}_{M/2}$
least significant bit



$QFT_{M/2}$
H



$$S(m) = S(m-1) + O(m)$$

$$S(m) = O(m^2)$$

$$M = 2^m$$

$$S = O(\log^2 M)$$

$$\omega^{j} = \omega^{\underline{j_{m-2}} j_{m-3} \cdots j_0} = \omega^{j_{m-2} \cdot 2^{m-2}} \times \omega^{j_{m-3} 2^{m-3}} \cdots \omega^{j_0 \cdot 2^0}$$