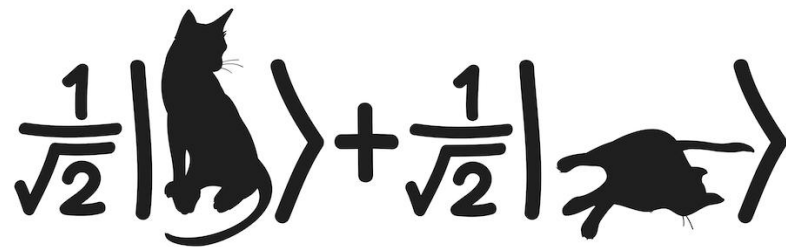


Quantum Mechanics & Quantum Computation

Umesh V. Vazirani

University of California, Berkeley



Lecture 14: Quantum Factoring

QFT Circuit

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

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

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

Γ_n

$$\begin{array}{c}
 \begin{array}{|c|} \hline k \\ \hline \end{array} \\
 \begin{array}{|c|} \hline \omega^{jk} \\ \hline \end{array} \\
 \begin{array}{|c|} \hline j \\ \hline \end{array}
 \end{array}
 M_n(\omega)
 \begin{array}{|c|} \hline a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ \vdots \\ a_{n-1} \\ \hline \end{array}
 a
 =
 \begin{array}{c}
 \begin{array}{|c|} \hline \text{Column} \\ 2k \\ \hline \end{array} \\
 \begin{array}{|c|} \hline \omega^{2jk} \\ \hline \end{array} \\
 \begin{array}{|c|} \hline j \\ \hline \end{array}
 \end{array}
 \begin{array}{c}
 \begin{array}{|c|} \hline \text{Column} \\ 2k+1 \\ \hline \end{array} \\
 \begin{array}{|c|} \hline \omega^j \cdot \omega^{2jk} \\ \hline \end{array} \\
 \begin{array}{|c|} \hline j \\ \hline \end{array}
 \end{array}
 \begin{array}{|c|} \hline a_0 \\ a_2 \\ \vdots \\ a_{n-2} \\ \hline a_1 \\ a_3 \\ \vdots \\ a_{n-1} \\ \hline \end{array}
 =
 \begin{array}{c}
 \begin{array}{|c|} \hline \text{Column} \\ 2k \\ \hline \end{array} \\
 \begin{array}{|c|} \hline (\omega^j)^{jk} \\ \hline \end{array} \\
 \begin{array}{|c|} \hline \text{Row } j \\ \hline \end{array}
 \end{array}
 \begin{array}{c}
 \begin{array}{|c|} \hline \text{Column} \\ 2k+1 \\ \hline \end{array} \\
 \begin{array}{|c|} \hline \omega^j \cdot \omega^{2jk} \\ \hline \end{array} \\
 \begin{array}{|c|} \hline j \\ \hline \end{array}
 \end{array}
 \begin{array}{|c|} \hline a_0 \\ a_2 \\ \vdots \\ a_{n-2} \\ \hline a_1 \\ a_3 \\ \vdots \\ a_{n-1} \\ \hline \end{array}$$

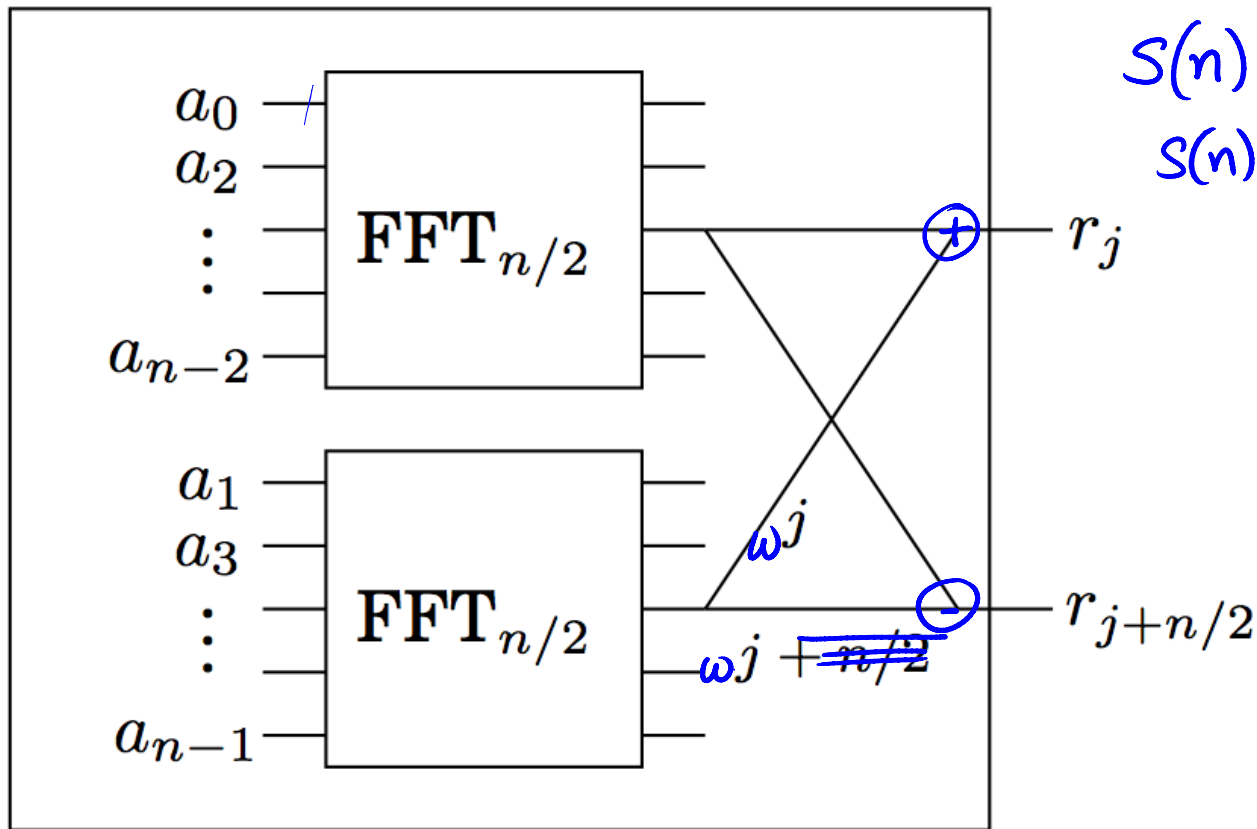
$$\omega^{(j+\frac{n}{2})2k} = \omega^{2jk} \cdot \omega^{nk}$$

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

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

$$\begin{array}{c}
 \text{Row } j \\
 \\
 j + n/2
 \end{array}
 \left[\begin{array}{cc}
 \begin{array}{c} \boxed{F_{n/2}} \\ \\ \boxed{M_{n/2}} \end{array} & \begin{array}{c} \boxed{\begin{array}{c} a_0 \\ a_2 \\ \vdots \\ a_{n-2} \end{array}} \\ \\ \boxed{\begin{array}{c} a_0 \\ a_2 \\ \vdots \\ a_{n-2} \end{array}} \end{array}
 \right.
 + \omega^j \left[\begin{array}{cc}
 \boxed{M_{n/2}} & \boxed{\begin{array}{c} a_1 \\ a_3 \\ \vdots \\ a_{n-1} \end{array}} \\ \\
 \boxed{M_{n/2}} & \boxed{\begin{array}{c} a_1 \\ a_3 \\ \vdots \\ a_{n-1} \end{array}}
 \end{array}
 \right.
 \left. - \omega^j \left[\begin{array}{cc}
 \boxed{M_{n/2}} & \boxed{\begin{array}{c} a_1 \\ a_3 \\ \vdots \\ a_{n-1} \end{array}} \right.
 \right.
 \left. \right]$$

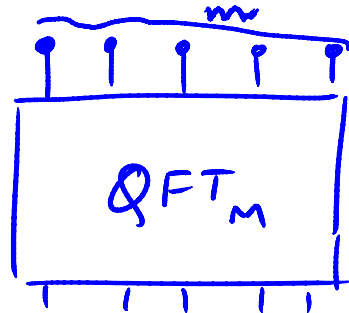
FFT_n (input: $a_0, \dots, a_{n-1}$, output: $r_0, \dots, r_{n-1}$)



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

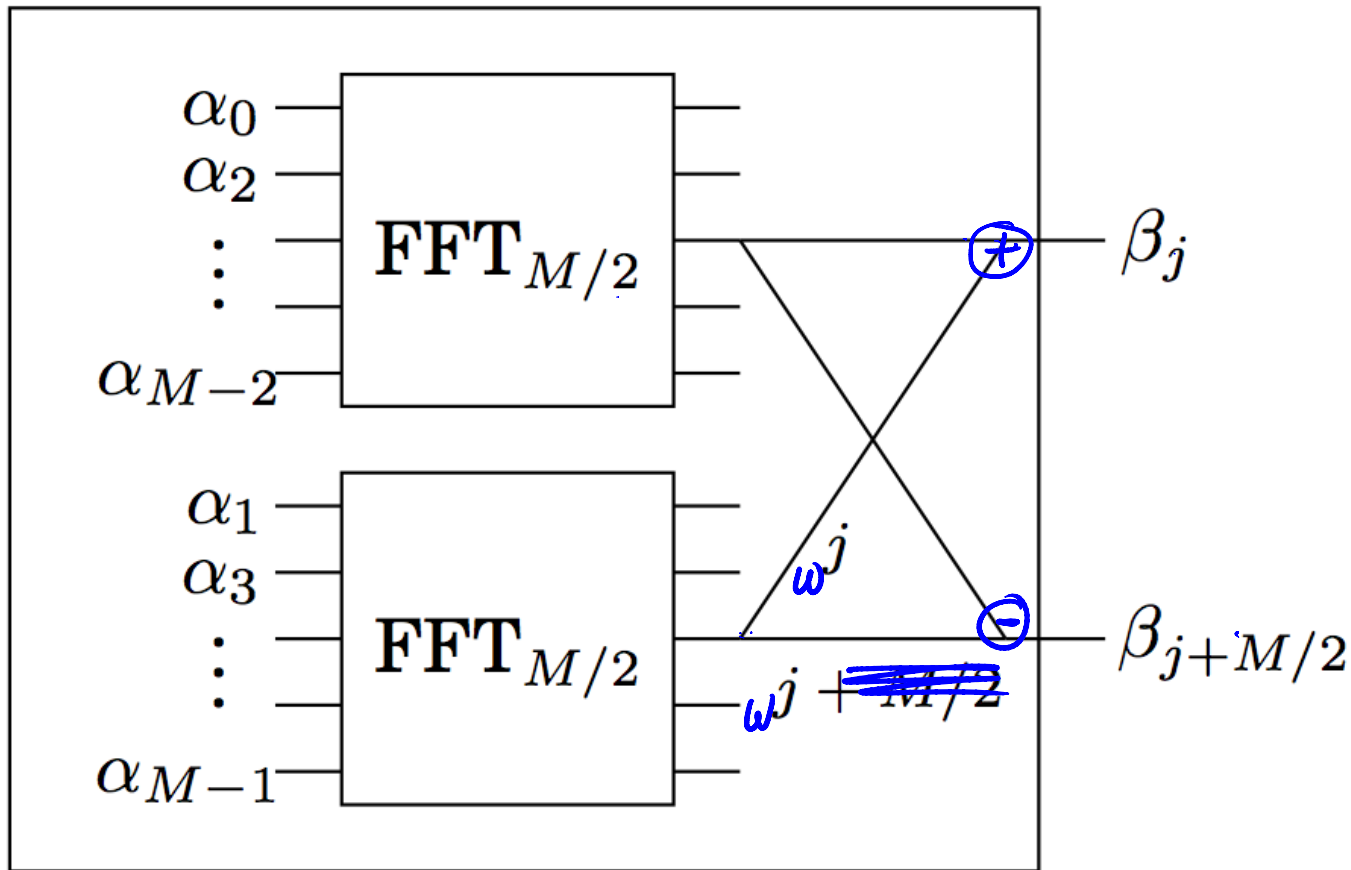
$$S(n) = O(n \lg n)$$

$$M = 2^m$$



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

FFT_M (input: $\alpha_0, \dots, \alpha_{M-1}$, output: $\beta_0, \dots, \beta_{M-1}$)



$m - 1$ qubits



least significant bit

