Portland State U

F, 05/08/2020

S′20 CS 410/510

Intro to quantum computing

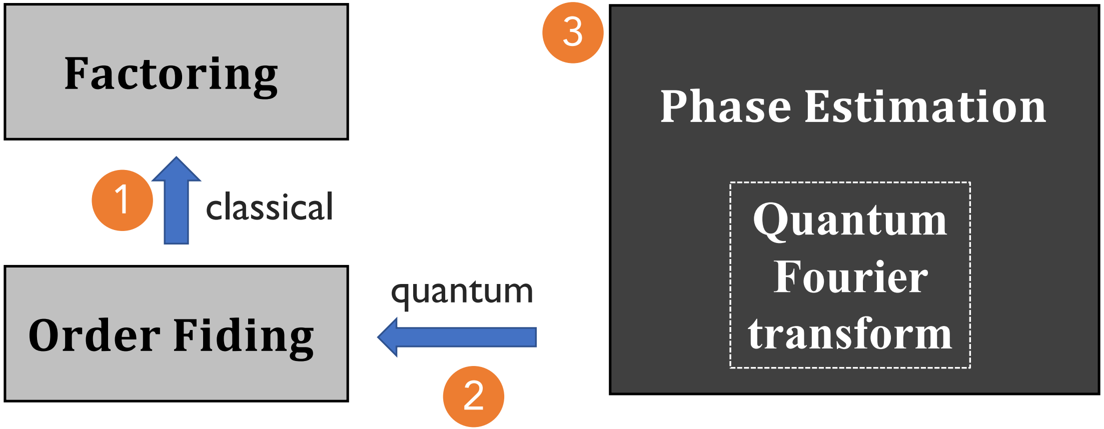
Fang Song

Week 6

- Phase estimation
- Quantum Fourier transform

Credit: based on slides by Richard Cleve

Recall: quantum factorization algorithm



- Last week: 1 & 2 (treating PE as black-box)
- Today: 3 open up PE and QFT

Phase estimation (eigenvalue est.) [Kitaev'94]

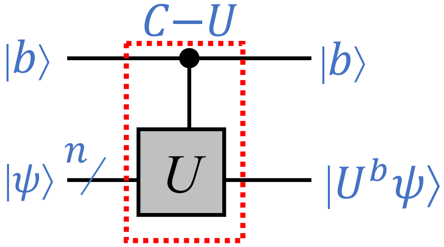
Input:

- Unitary operation U (described by a quantum circuit).
- A quantum state $|\psi\rangle$ that is an eigenvector of U: $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$.

Output: An approximation to $\theta \in [0,1)$.

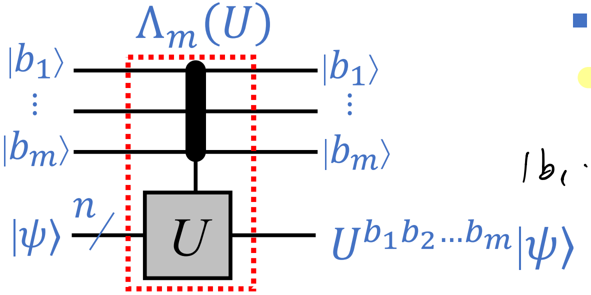
- A central tool in quantum algorithm design
  - Order finding
  - QFT ($\mathbb{Z}_m$)
  - Hidden subgroup problem
  - Quantum linear system solver
  - Quantum simulation
  - …

Generalized controlled unitary



- $C\!-\!U = \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}$ $\quad CNOT = \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix}$

$k \leftarrow b_1 \cdots b_m \quad 2^{m-1} \cdot b_1 + 2^{m-2} b_2 + \dots + b_m$



- $\Lambda_m(U)$ on $m+n$ qubits
  $|k\rangle|\psi\rangle \mapsto |k\rangle U^k|\psi\rangle, k \in \{0,1,\dots,2^m-1\}$

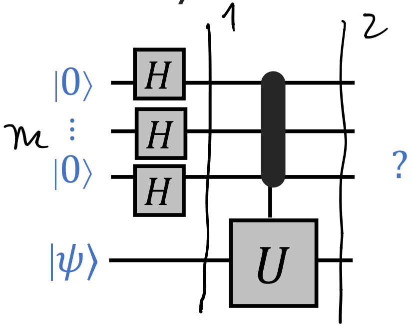
$|b_1 \cdots b_m\rangle$

$$\Lambda_m(U) = \begin{pmatrix} I & 0 & 0 & \dots & 0 \\ 0 & U & 0 & \dots & 0 \\ 0 & 0 & U^2 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & U^{2^m-1} \end{pmatrix}$$

- $b_1 b_2 \dots b_m$ base-2 representation of integers
- Identify $\{000, 001, 010, 011, 100, 101, 110, 111\} = \{0, 1, 2, 3, 4, 5, 6, 7\}$

Phase estimation algorithm

- Assume a quantum circuit for $\Lambda_m(U)$ is given
  - May be difficult to construct from a circuit for U



$U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$

$$|0^m\rangle|\psi\rangle$$

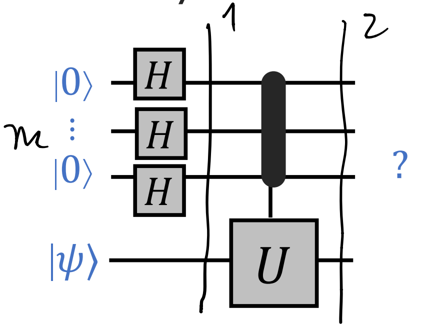
$$\xrightarrow[1]{H^{\otimes m}\otimes \mathbb{1}} \frac{1}{\sqrt{2^m}}\sum_{k=0}^{2^m-1}|k\rangle\,|\psi\rangle$$

$$\xrightarrow[2]{\Lambda_m(U)} \frac{1}{\sqrt{2^m}}\sum_{k=0}^{2^m-1}\Lambda_m(U)\big(|k\rangle|\psi\rangle\big)$$

$$= \frac{1}{\sqrt{2^m}}\sum_{k=0}^{2^m-1}|k\rangle U^k|\psi\rangle$$

Phase estimation algorithm

- Assume a quantum circuit for $\Lambda_m(U)$ is given
  - May be difficult to construct from a circuit for U



$$= \frac{1}{\sqrt{2^m}} \left(\sum_{k=0}^{2^m-1} |k\rangle U^k |\psi\rangle \right)$$

$$= \frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} |k\rangle e^{2\pi i k\theta} |\psi\rangle$$

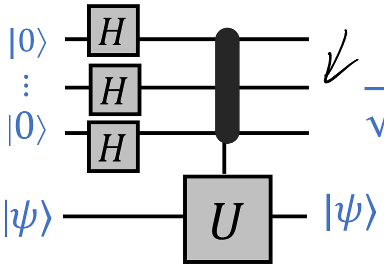
$$U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$$

$$|\psi\rangle \xmapsto{U} e^{2\pi i\theta}|\psi\rangle \xmapsto{U} (e^{2\pi i\theta})^2 |\psi\rangle$$

$$= e^{2\pi i 2\theta} |\psi\rangle$$

Phase estimation algorithm cont'd

- A special case: $\theta = \frac{j}{2^m}$ for some $j \in \{0,1,\ldots,2^m-1\}$



$$\frac{1}{\sqrt{2^m}}\sum_{k=0}^{2^m-1} e^{2\pi i k\theta}|k\rangle$$

$\theta = j/2^m$

$e^{2\pi i\, k\cdot j/2^m}$

$2^m = M,\ e^{2\pi i/2^m} = \omega_M$

Let $|\phi_j\rangle := \frac{1}{\sqrt{2^m}}\sum_{k=0}^{2^m-1} \omega_M^{kj}|k\rangle$ $(\omega_M := e^{\frac{2\pi i}{2^m}})$

- Determining j $\Leftrightarrow$ distinguishing between $|\phi_j\rangle$

Phase estimation algorithm cont'd

How to distinguishing between $|\phi_j\rangle, j \in \{0, \dots, 2^m - 1\}$?

$$|\phi_j\rangle := \frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} \omega_M^{kj} |k\rangle \ (\omega_M := e^{\frac{2\pi i}{2^m}})$$

- Observation. $\{|\phi_j\rangle\}$ orthonormal
- Pf. $\langle \phi_j | \phi_{j'} \rangle = \left(\sum_k \omega_M^{-kj} \langle k|\right)\left(\sum_{k'=0}^{2^m-1} \omega_M^{k'j'} |k'\rangle\right)$ $|\phi_{j'}\rangle$

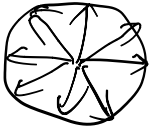
$j \neq j'$

$\left(\frac{1}{\sqrt{2}}\langle 0|\right)\left(\frac{1}{\sqrt{3}} + \frac{1}{\sqrt{3}}\right)|0\rangle$

$\left(\langle 0| + \langle 1|\right)\left(2|0\rangle + 3|1\rangle\right) = \sum_k \sum_{k'} \omega_M^{k'j'} \cdot W_M^{-kj} \langle k | k' \rangle$

$= \delta_{kk'} = \begin{cases} 1 & \text{if } k = k' \\ 0 & \text{o.w.} \end{cases}$

$= \sum_{k=0}^{M-1} \omega_M^{k(j'-j)} = 0$



Phase estimation algorithm cont'd

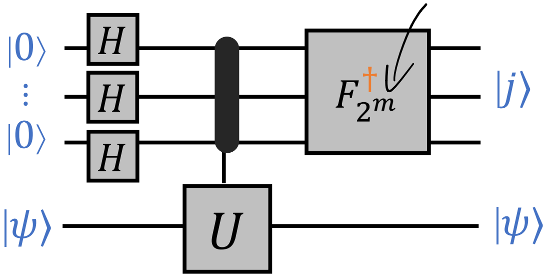
- $\{|\phi_j\rangle\}$ orthonormal ➔ $\exists$ unitary $F: |j\rangle \mapsto |\phi_j\rangle = \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} \omega_M^{kj} |k\rangle$, $M = 2^m$

$$
\begin{array}{cc}
 & \begin{array}{ccccc} j=0 & j=1 & & j & \end{array} \\
F_M = \frac{1}{\sqrt{M}} & \begin{pmatrix}
1 & 1 & 1 & \cdots & 1 \\
1 & \omega & \omega^2 & \cdots & \omega^{M-1} \\
1 & \omega^2 & \omega^4 & |\phi_j\rangle & \omega^{2(M-1)} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \omega^{M-1} & \omega^{2(M-1)} & \cdots & \omega^{(M-1)(M-1)}
\end{pmatrix}
\end{array}
$$

$F^{-1}: |\phi_j\rangle \mapsto |j\rangle$

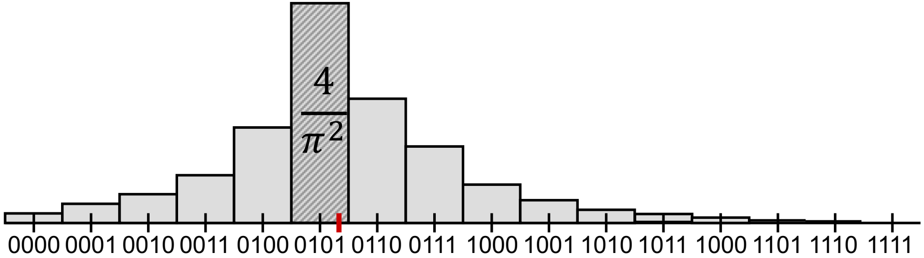
Phase estimation algorithm cont'd

- Special case $\theta = \frac{j}{2^m} = 0.j_1 j_2 \dots j_m$.



- General $\theta = 0.j_1 j_2 \dots j_m j_{m+1} \cdots$

➔Measure $j = j_1 j_2 \dots j_m$ (m-bit approximation of θ) with prob. at lest $\frac{4}{\pi^2} \approx 0.4$.



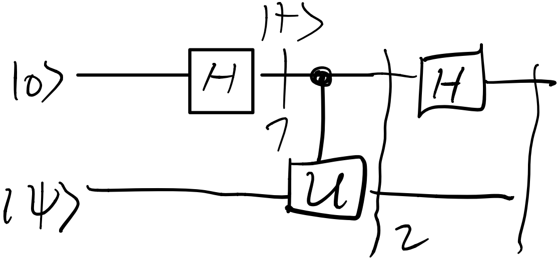
Ex. $\theta = 1/3 = 0.0101010101010101 \dots$

$UU^{\dagger} = \mathbb{I}$

$U^{\dagger} = U^{-1}$

Exercise

1. Let U be a unitary on one qubit, and $|\psi\rangle$ is an eigenvector with eigenvalue either 1 or -1. Can you design a quantum algorithm to determine the eigenvalue? How many gates do you need?



if $\lambda = 1$ $|0\rangle$

$\lambda = -1$ $|1\rangle$

$$|+\rangle|\psi\rangle \xmapsto{C\text{-}U} |0\rangle|\psi\rangle + |1\rangle|\psi\rangle$$

$$= |0\rangle|\psi\rangle + |1\rangle\lambda|\psi\rangle$$

$$= (|0\rangle + \lambda|1\rangle)|\psi\rangle$$

2: $\lambda = 1$ $\quad |+\rangle \xmapsto{H} |0\rangle$

$\lambda = -1$ $\quad |-\rangle \quad\quad |1\rangle$

$$(-1(|0\rangle - |1\rangle) = |1\rangle$$

What about F_M

- Discrete Fourier transform

$$\begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{M-1} \end{pmatrix} \mapsto \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{M-1} \end{pmatrix} = F_M \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{M-1} \end{pmatrix}$$

$$F_M = \frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(M-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{M-1} & \omega^{2(M-1)} & \cdots & \omega^{(M-1)(M-1)} \end{pmatrix}$$

$$y_j = \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} \omega_M^{kj} x_k$$

Applications everywhere: signal processing, optics, crystallography, geology, astronomy …

- Quantum Fourier transform $\mathrm{QFT}_M \; |j\rangle \mapsto |\phi_j\rangle = \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} \omega_M^{kj} \, |k\rangle$

$$\sum_{j=0}^{M-1} x_j |j\rangle \mapsto \sum_{j=0}^{M-1} y_j |j\rangle, y_j = \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} \omega_M^{kj} x_k$$

Computing F_M

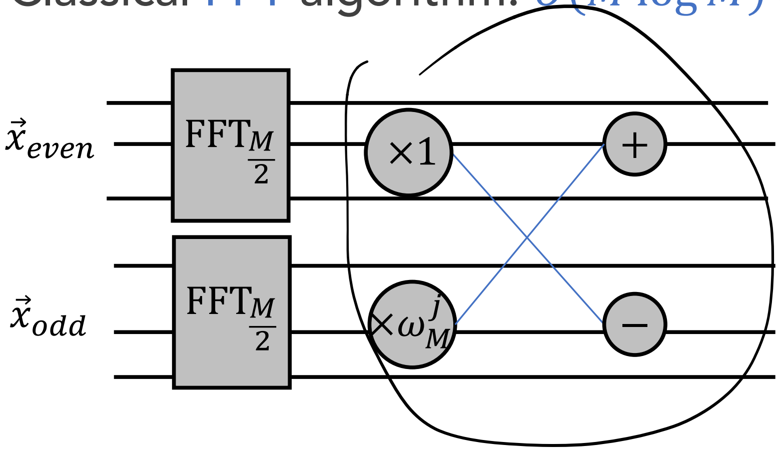
- Naïve matrix multiplication $O(M^2)$
- Classical FFT algorithm: $O(M \log M)$ arithmetic operations

$$F_M = \frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(M-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{M-1} & \omega^{2(M-1)} & \cdots & \omega^{(M-1)(M-1)} \end{pmatrix}$$

$$\begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{M-1} \end{pmatrix} \mapsto \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{M-1} \end{pmatrix} = F_M \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{M-1} \end{pmatrix} = \begin{pmatrix} F_{M/2} \begin{pmatrix} x_0 \\ x_2 \\ \vdots \\ x_{M-2} \end{pmatrix} & \omega_M^j F_{M/2} \begin{pmatrix} x_1 \\ x_3 \\ \vdots \\ x_{M-1} \end{pmatrix} \\ F_{M/2} \begin{pmatrix} x_0 \\ x_2 \\ \vdots \\ x_{M-2} \end{pmatrix} & -\omega_M^j F_{M/2} \begin{pmatrix} x_1 \\ x_3 \\ \vdots \\ x_{M-1} \end{pmatrix} \end{pmatrix}$$

Computing F_M cont'd

- Classical FFT algorithm: $O(M \log M)$ arithmetic operations



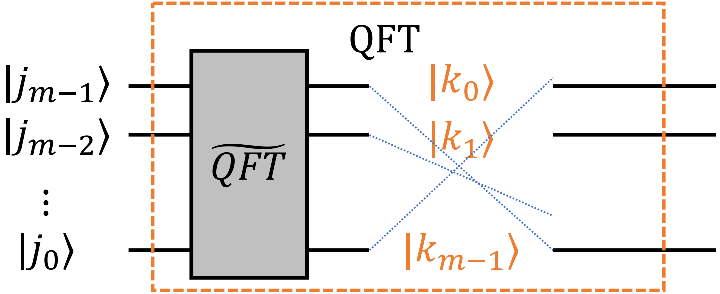
- $T(M) = 2T(M/2) + O(M) = O(M \log M)$ [Think of Merge Sort]

Quantum Fourier Transform

- ∃ QFT circuit of size $O(m^2)$ [$\log^2 M$ vs. FFT $M \log M$]

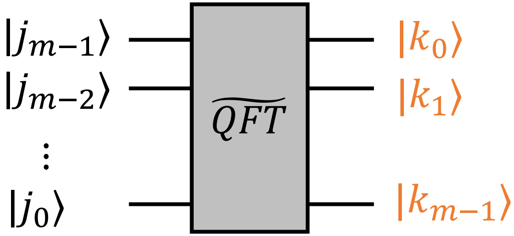
$j = 2^{m-1} \cdot j_{m-1} + 2^{m-2} \cdot j_{m-2} + \cdots + 2^0 \cdot j_0$ $\quad k_{m-1} k_{m-2} \cdots k_0$

- Let's implement $\widetilde{QFT}_M |j_{m-1} j_{m-2} \dots j_0\rangle = \frac{1}{\sqrt{M}} \sum_k \omega_M^{kj} |k_0 k_1 \dots k_{m-1}\rangle$
  - i.e. reverse the order of the output qubits of QFT



Quantum Fourier Transform cont'd

- $\widetilde{QFT}_M |\overbrace{j_{m-1}j_{m-2}\dots j_0}\rangle = \frac{1}{\sqrt{M}}\sum_k \omega_M^{kj}\, |\overbrace{k_0 k_1 \dots k_{m-1}}\rangle$ $\quad M = 2^m$



$$\widetilde{QFT}_2 |b\rangle = \frac{1}{\sqrt{2}} \sum_{k=0}^{1} \omega_2^{j\cdot k} |k\rangle$$

$$\parallel$$

$$H \qquad = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^b |1\rangle\right)$$

$\cdot\, m \geq 2$

$\cdot\; j' = j_{m-1} j_{m-2} \cdots j_1 = \lfloor j/2 \rfloor$

$\widetilde{QFT}_{M/2}$

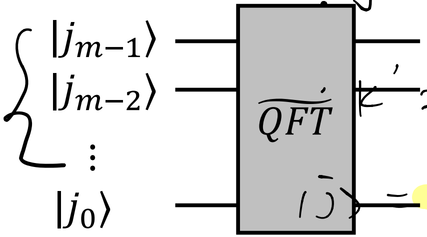
$\cdot\; k' = k_{m-2} k_{m-3} \cdots k_0 = k - 2^{m-1} k_{m-1}$

$$|j\rangle = |j'\rangle |j_0\rangle \xmapsto{\widetilde{QFT}_{M/2}} \frac{1}{\sqrt{2^{m-1}}} \sum_{k'=0}^{M/2-1} \omega_M^{j'\cdot k'} |k'_0 \cdots k'_{m-2}\rangle |j_0\rangle$$

Quantum Fourier Transform cont'd

- $\widetilde{QFT}_M |\overbrace{j_{m-1} j_{m-2} \dots j_1}^{j'} j_0\rangle = \frac{1}{\sqrt{M}} \sum_k \omega_M^{kj} |k_0 \overbrace{k_1 \dots k_{m-1}}\rangle$ $\quad M = 2^m$

$j' = j_{m-1} j_{m-2} \cdots j_1 = \lfloor j/2 \rfloor$



$k' = k_{m-2} k_{m-3} \cdots k_0 = k - 2^{m-1} k_{m-1}$

$|j'\rangle |j_0\rangle \xmapsto{\widetilde{QFT}_{M/2}} \frac{1}{\sqrt{2^{m-1}}} \sum_{k'=0}^{M/2-1} \omega_{M/2}^{j' \cdot k'} |k'_0 \cdots k'_{m-2}\rangle |j_0\rangle$

$m \geq 2$

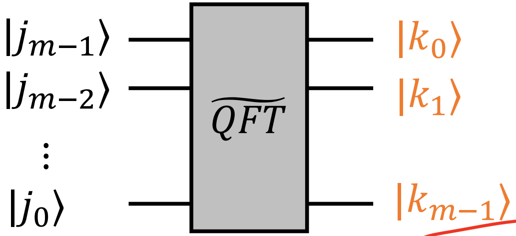
$= \frac{1}{\sqrt{M/2}} \sum_{k'=0}^{M/2-1} \omega_M^{j'k'} |k'_0 \cdots k'_{m-2}\rangle |j_0\rangle$

$\widetilde{QFT}_{M/2}$

$\xmapsto{C\text{-}R_k} \sum_{k'} \omega_{M/2}^{j'k'} \, \omega_M^{k'_0 \cdot j_0} \cdot \omega_{M/2}^{k'_1 j_0} \cdots\cdots \omega_4^{k'_{m-2} \cdot j_0} |k'_0 \cdots k'_{m-2}\rangle |j_0\rangle$

Quantum Fourier Transform cont'd

- $\widetilde{QFT}_M |j_{m-1} j_{m-2} \dots j_0\rangle = \frac{1}{\sqrt{M}} \sum_k \omega_M^{kj} \, |k_0 k_1 \dots k_{m-1}\rangle$



$$\omega_{M/2} = e^{2\pi i / M/2} = e^{(2\pi i \cdot 2/M)} = \left(e^{2\pi i/M}\right)^2 = \omega_M^2$$

$$\xrightarrow{C\text{-}R_k} \sum_{k'} \boxed{\omega_{M/2}^{j'k'} \; \omega_M^{k_0' \cdot j_0} \cdot \omega_{M/2}^{k_1' j_0} \cdots\cdots \omega_4^{k_{m-2}' \cdot j_0}} \, |k_0' \cdots k_{m-2}'\rangle |j_0\rangle$$

$QFT_{M/2}$

$$= \sum_{k'} \omega_M^{2 \cdot j'k' + k_0' j_0 + 2k_1' j_0 + \cdots + j_0 (2^{m-2} k_{m-2}')}$$

$| \;\rangle | \;\rangle$

Scratch

- $j' = j_{m-1} j_{m-2} \cdots j_1 = \lfloor j/2 \rfloor$
- $k' = k_{m-2} k_{m-3} \cdots k_0 = k - 2^{m-1} k_{m-1}$

$2 \cdot j' \cdot k' + k_0' \cdot j_0 + 2 k_1' j_0 + \cdots + j_0 (2^{m-2} \cdot k_{m-2}')$

$$\sum_{k'} \omega_M \qquad |k_0' k_1' \cdots k_{m-2}'\rangle |j_0\rangle$$

$$= \sum_{k'=0}^{M/2-1} \omega_M^{jk'} |k_0' k_1' \cdots k_{m-2}'\rangle |j_0\rangle$$

$H(|j_0\rangle) = |0\rangle + (-1)^{j_0} |1\rangle$

$$= \sum_{k'=0}^{M/2-1} \sum_{k_{m-1}=0}^{1} \omega_M^{jk'} (-1)^{k_{m-1} j_0} |k_0' \cdots k_{m-2}'\rangle |k_{m-1}\rangle$$

$= (-1)^{k_{m-1} \cdot j}$

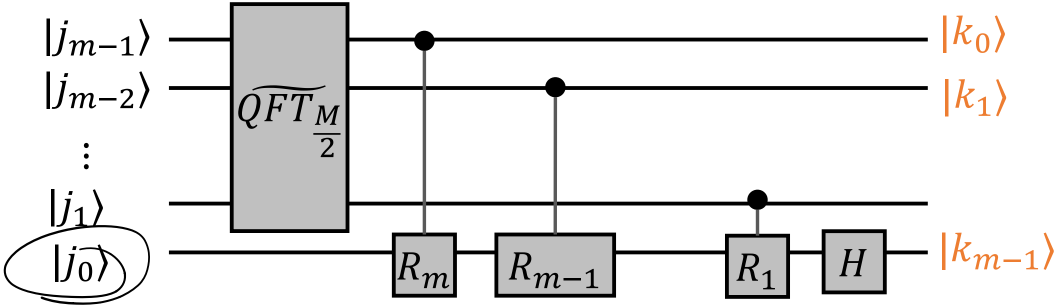
$(-1) = \omega_M^{M/2}$

$$= \sum_{k'} \sum_{k_{m-1}} \omega_M^{jk' + j(2^{m-1} \cdot k_{m-1})} |k_0' \cdots k_{m-2}'\rangle |k_{m-1}\rangle$$

$\quad \,// \,\omega_M^{jk} \qquad |k_0 k_1 \cdots k_{m-1}\rangle$

Quantum Fourier Transform cont'd

- $\widetilde{QFT}_M |j_{m-1} j_{m-2} \dots j_0\rangle = \frac{1}{\sqrt{M}} \sum_k \omega_M^{kj} \, |k_0 k_1 \dots k_{m-1}\rangle$



$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$$

$R_k: |0\rangle \longmapsto |0\rangle$

$|1\rangle \longmapsto e^{2\pi i/2^k} |1\rangle$

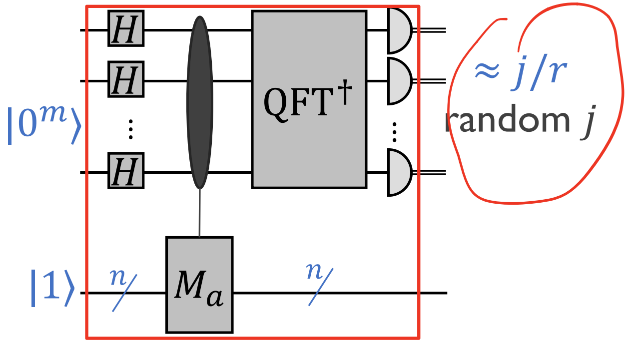
? $k=1$

- $T(m) = T(m-1) + O(m) = O(m^2)$

Revisit quantum order finding algorithm

- QFT ✓ $\quad n = \lceil \log N \rceil$
- $\Lambda_m(M_a): |k\rangle|x\rangle \mapsto |k\rangle|a^k x \bmod N\rangle$
  - Modular exponentiation takes time $O(mn^2)$
  - $m = O(n)$ suffices to recover r

➔ Circuit size $poly(n)$



$$|1\rangle = |00 \dots 1\rangle = \frac{1}{\sqrt{r}} \Sigma |\psi_j\rangle$$

- NB. Read about continued fraction if curious
  https://people.eecs.berkeley.edu/~vazirani/s09quantum/notes/lecture4.pdf

Summary

Factoring $\xleftarrow{\text{classical}}$ **Order Fiding** $\longleftarrow$ **Phase Estimation** 

Exercise

1. Let $\vec{x} = \left(\frac{1}{\sqrt{2}}, 0, 0, \frac{i}{\sqrt{2}}\right)$. Compute $\vec{y} = F_4 \vec{x}$ using FFT

2. Draw the QFT circuit that implements F_4

Scratch