Portland State U

F, 05/08/2020

# S'20 CS 410/510

# Intro to quantum computing

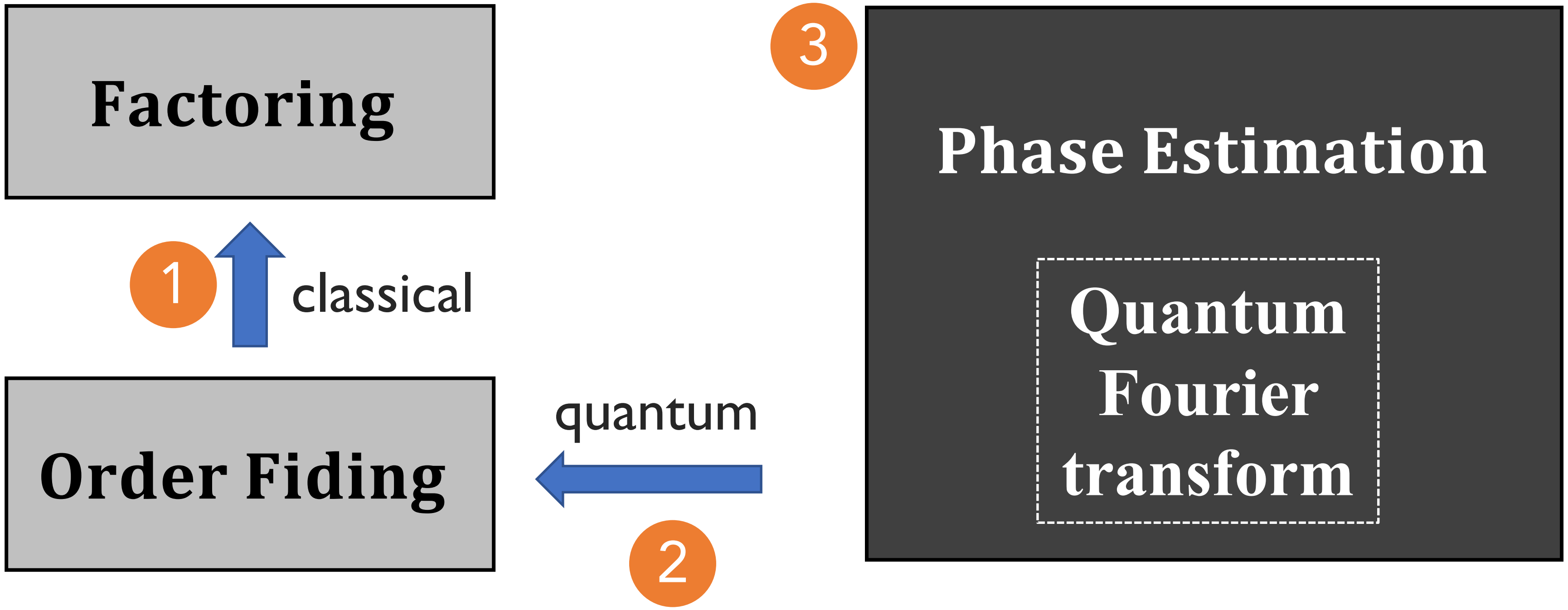
Fang Song

## 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]

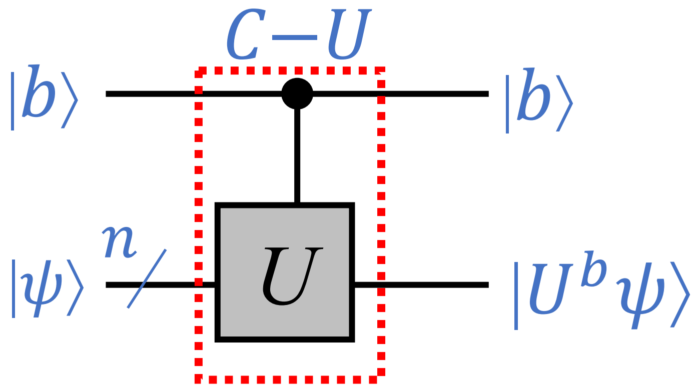
Input:

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

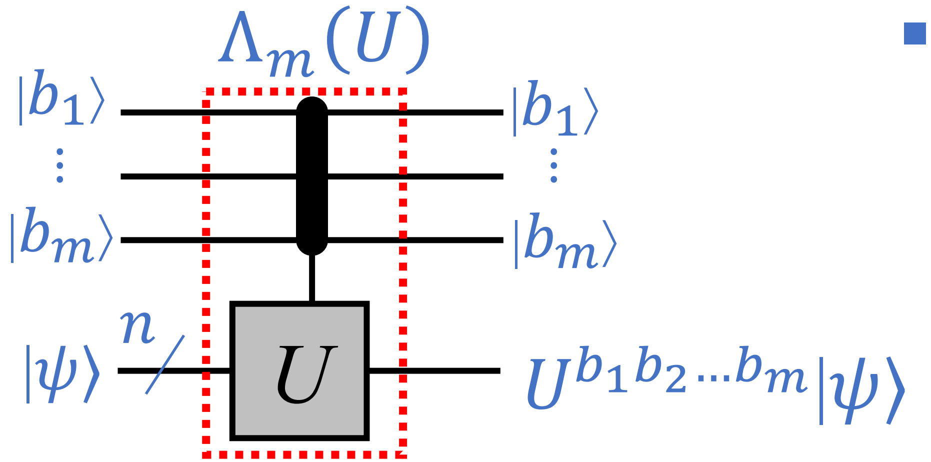
Output: An approximation to $\theta \in [0, 1)$.

- 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




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



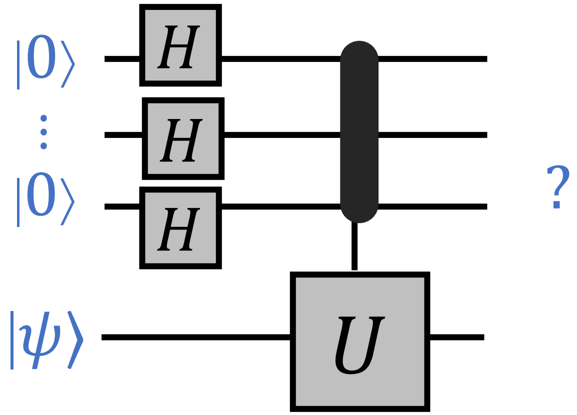

- $\Lambda_m(U)$ on $m+n$ qubits
  $|k\rangle|\psi\rangle \mapsto |k\rangle U^k|\psi\rangle, k \in \{0,1,\dots,2^m-1\}$

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

- $b_1 b_2 \dots b_m$ 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

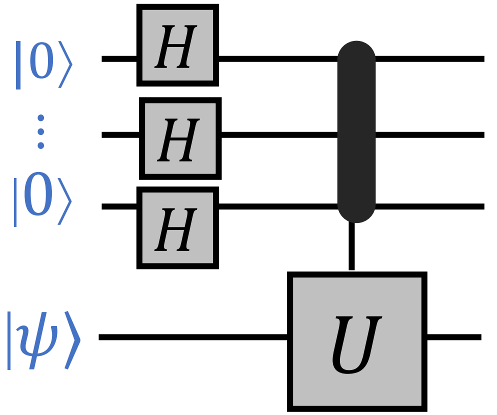
- Assume a quantum circuit for $\Lambda_m(U)$ is given
  - May be difficult to construct from a circuit for $U$




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

# Phase estimation algorithm cont'd

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




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

$|\psi\rangle$

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 $|\phi_j\rangle, j \in \{0, \ldots, 2^m - 1\}$?

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

- Observation. $\{|\phi_j\rangle\}$ orthonormal
- Pf. $\langle\phi_j|\phi_{j'}\rangle =$

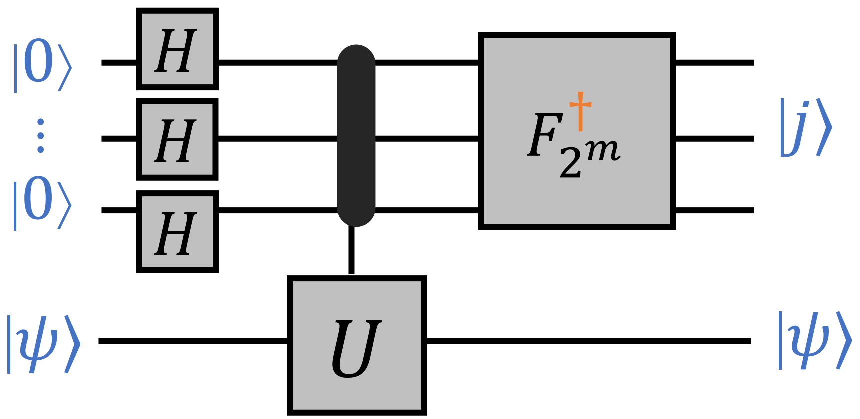
# Phase estimation algorithm cont'd

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

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

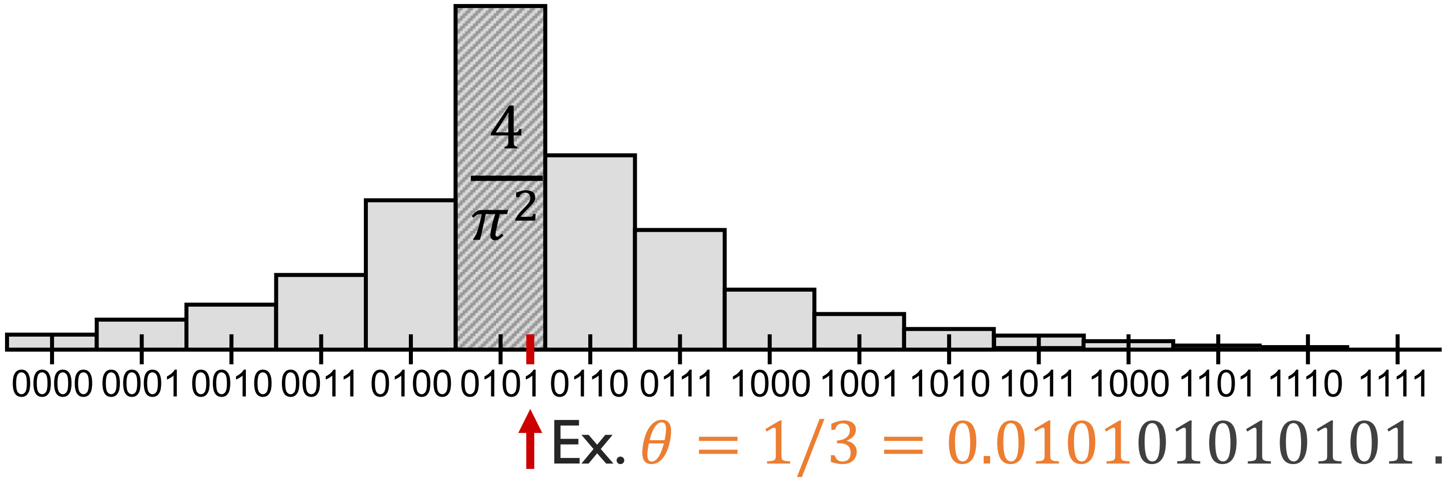
# Phase estimation algorithm cont'd

- Special case $\theta = \frac{j}{2^m} = 0.j_1j_2\dots j_m$.




- General $\theta = 0.j_1j_2\dots j_mj_{m+1}\cdots$

➔Measure $j = j_1j_2\dots j_m$ ($m$-bit approximation of $\theta$) with prob. at lest $\frac{4}{\pi^2} \approx 0.4$.




Ex. $\theta = 1/3 = 0.0101010101\dots$

# 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?

# 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 $F_M$

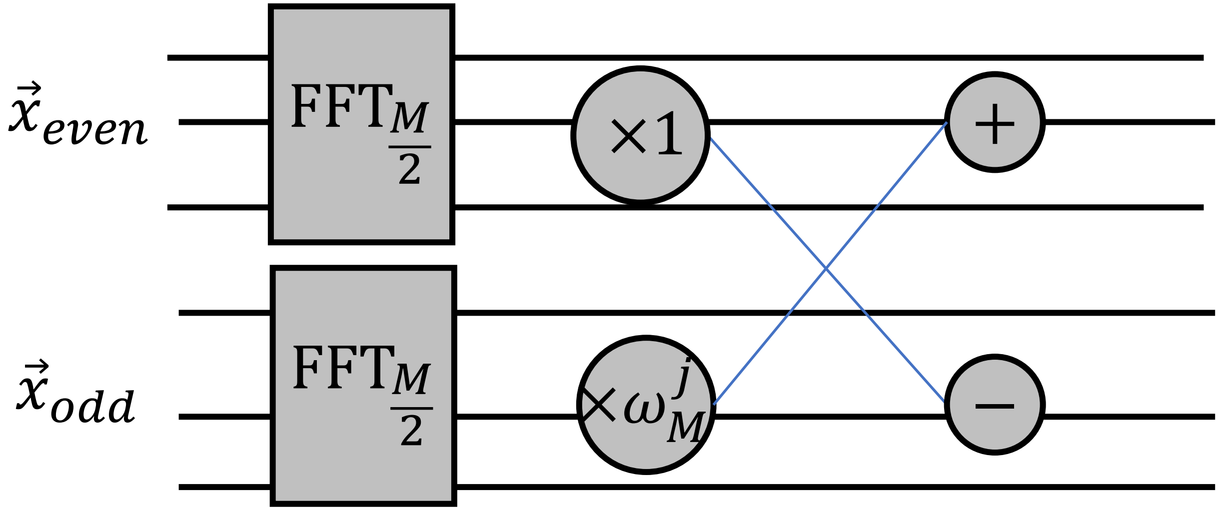
- Naïve matrix multiplication $O(M^2)$
- Classical FFT algorithm: $O(M \log M)$ arithmetic operations

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

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

# Computing $F_M$ cont'd

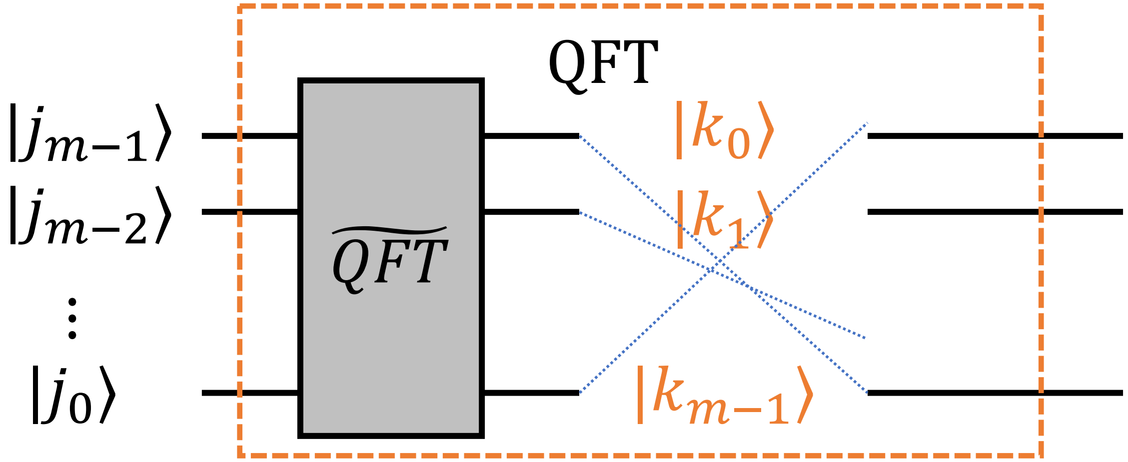
- Classical FFT algorithm: $O(M \log M)$ arithmetic operations




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

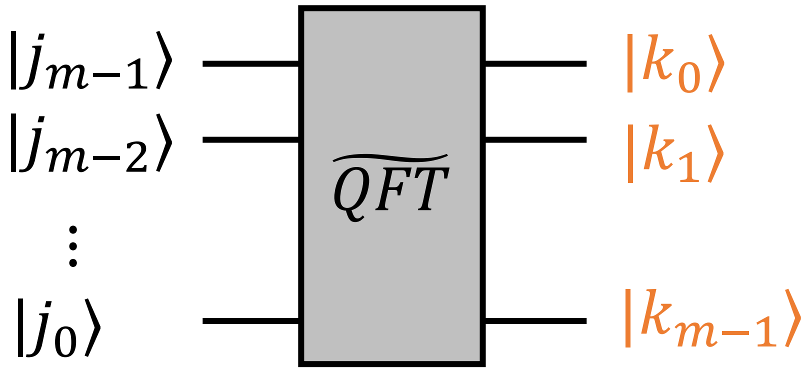
# Quantum Fourier Transform

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



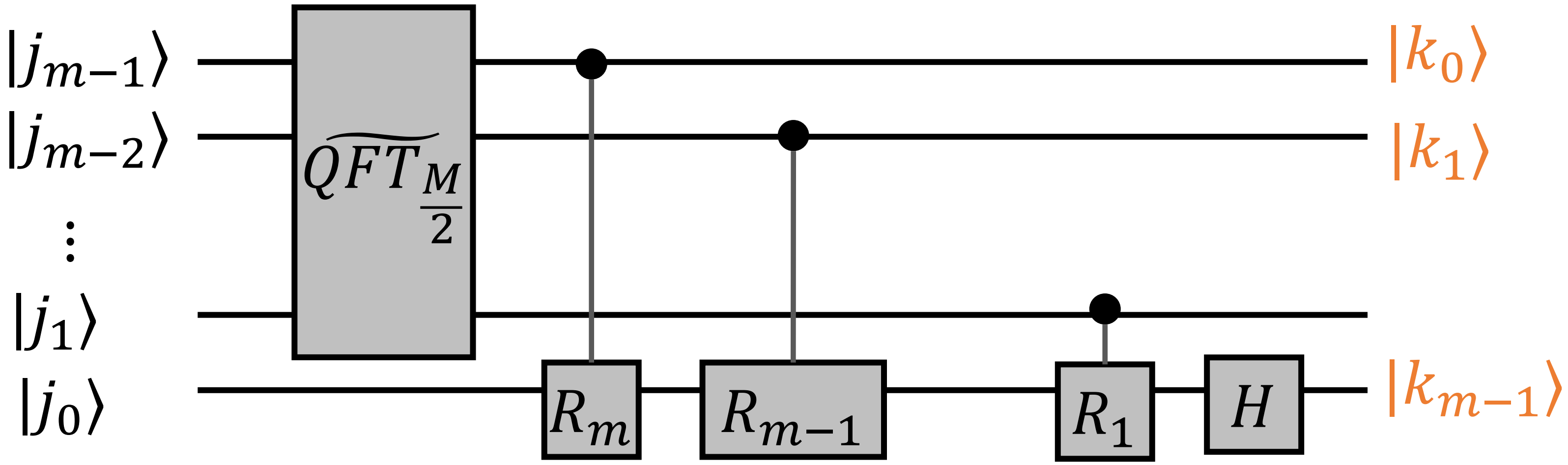
# Quantum Fourier Transform cont'd

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



# Quantum Fourier Transform cont'd

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



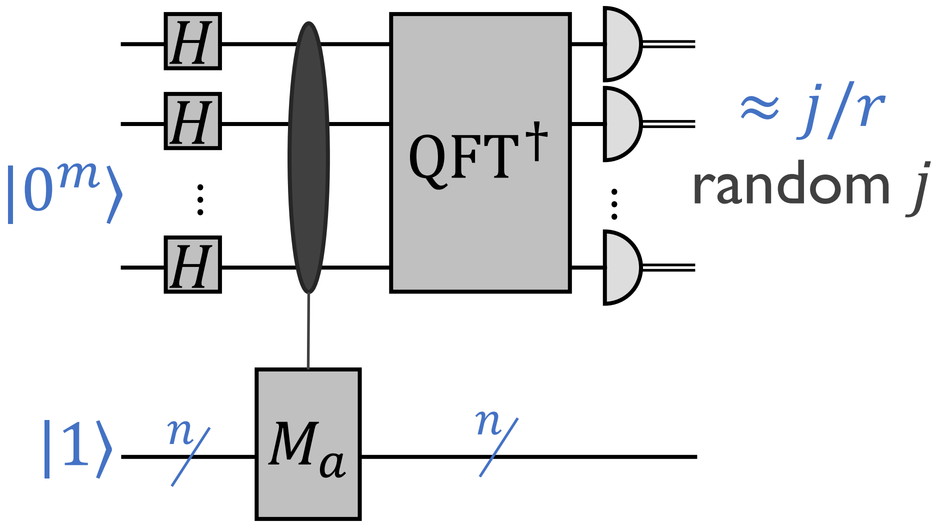

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$$

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

# Revisit quantum order finding algorithm

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

➔ Circuit size $poly(n)$




$$|1\rangle = |00\ldots1\rangle = \frac{1}{\sqrt{r}}\Sigma|\psi_j\rangle$$

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

# Summary

# 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