# Foundational Quantum Algorithms

Part 2

## Phase estimation and Shor's algorithm

John Watrous
IBM

# Eigenvectors and eigenvalues

Suppose $M$ is an $N \times N$ matrix, $|\psi\rangle$ is a non-zero $N$-dimensional vector, and $\lambda$ is a complex number such that

$$M|\psi\rangle = \lambda|\psi\rangle$$

Then the $|\psi\rangle$ is an *eigenvector* of $M$ and $\lambda$ is its associated *eigenvalue.*

Relevant facts about *unitary matrices:*

- Every unitary matrix has an orthonormal basis of eigenvectors. (This is true more generally for *normal matrices* — which are matrices that commute with their own conjugate transpose.)
- Every eigenvalue of a unitary matrix lies on the complex unit circle $\{\alpha \in \mathbb{C} : |\alpha| = 1\}$.

That is, for every $N \times N$ unitary matrix $U$, there exists an orthonormal basis $\{|\psi_0\rangle, \ldots, |\psi_{N-1}\rangle\}$ along with real numbers $\theta_0, \ldots, \theta_{N-1} \in [0, 1)$ such that

$$U|\psi_k\rangle = e^{2\pi i\theta_k}|\psi_k\rangle \qquad \text{(for each } k = 0, \ldots, N-1\text{)}$$

# Phase estimation problem

In the phase estimation problem, we're given two things:

1. A description of a *unitary quantum circuit* on $n$ qubits.
2. An $n$-qubit *quantum state* $|\psi\rangle$.

We're *promised* that $|\psi\rangle$ is an eigenvector of the unitary operation $U$ described by the circuit, and our goal is to approximate the corresponding eigenvalue.

**Phase estimation problem**

Input: A unitary quantum circuit for an $n$-qubit operation $U$ and an $n$ qubit quantum state $|\psi\rangle$

Promise: $|\psi\rangle$ is an eigenvector of $U$

Output: An approximation to the number $\theta \in [0, 1)$ satisfying

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

# Phase estimation problem

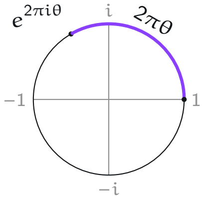
**Phase estimation problem**

Input: A unitary quantum circuit for an $n$-qubit operation $U$ and an $n$ qubit quantum state $|\psi\rangle$

Promise: $|\psi\rangle$ is an eigenvector of $U$

Output: An approximation to the number $\theta \in [0,1)$ satisfying

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




We can approximate $\theta$ by a fraction

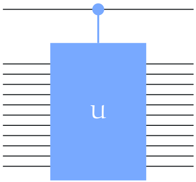
$$\theta \approx \frac{y}{2^m}$$

for $y \in \{0, 1, \ldots, 2^m - 1\}$.

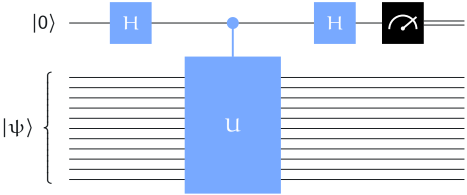
This approximation is taken "modulo 1."

# Warm-up: using the phase kickback

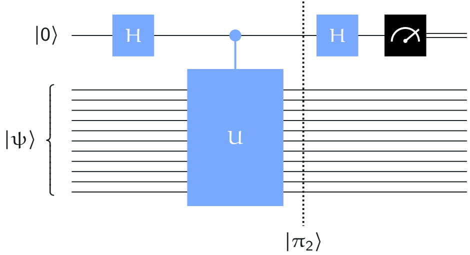
Given a circuit for $\mathsf{U}$, we can create a circuit for a controlled-$\mathsf{U}$ operation:




Let's consider this circuit:



# Warm-up: using the phase kickback

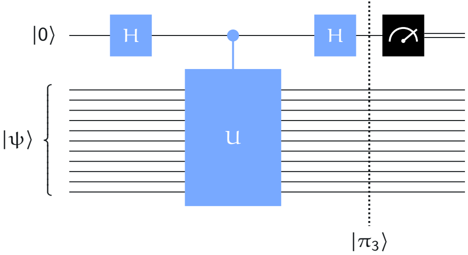



$$|\pi_0\rangle = |\psi\rangle|0\rangle$$

$$|\pi_1\rangle = \frac{1}{\sqrt{2}}|\psi\rangle|0\rangle + \frac{1}{\sqrt{2}}|\psi\rangle|1\rangle$$

$$|\pi_2\rangle = \frac{1}{\sqrt{2}}|\psi\rangle|0\rangle + \frac{1}{\sqrt{2}}(U|\psi\rangle)|1\rangle = |\psi\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{e^{2\pi i\theta}}{\sqrt{2}}|1\rangle\right)$$

# Warm-up: using the phase kickback




$$|\pi_2\rangle = |\psi\rangle \otimes \left( \frac{1}{\sqrt{2}} |0\rangle + \frac{e^{2\pi i \theta}}{\sqrt{2}} |1\rangle \right)$$

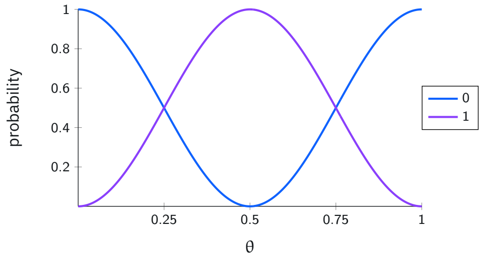
$$|\pi_3\rangle = |\psi\rangle \otimes \left( \frac{1 + e^{2\pi i \theta}}{2} |0\rangle + \frac{1 - e^{2\pi i \theta}}{2} |1\rangle \right)$$

# Warm-up: using the phase kickback

$$|\psi\rangle \otimes \left( \frac{1 + e^{2\pi i \theta}}{2} |0\rangle + \frac{1 - e^{2\pi i \theta}}{2} |1\rangle \right)$$

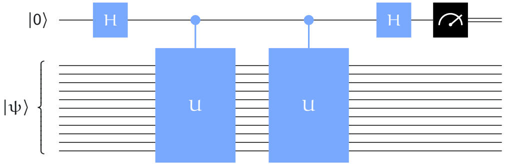
Measuring the top (i.e., rightmost) qubit yields the outcomes 0 and 1 with these probabilities:

$$p_0 = \left| \frac{1 + e^{2\pi i \theta}}{2} \right|^2 = \cos^2(\pi\theta) \qquad p_1 = \left| \frac{1 - e^{2\pi i \theta}}{2} \right|^2 = \sin^2(\pi\theta)$$

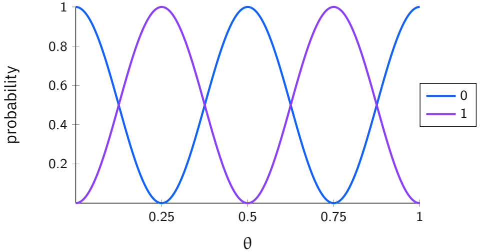


# Iterating the unitary operation

How can we learn more about $\theta$? One possibility is to apply the controlled-$U$ operation twice:

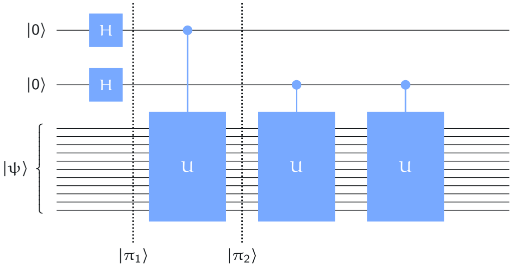



Performing the controlled-$U$ operation twice has the effect of squaring the eigenvalue:



# Two control qubits

Let's use two control qubits to perform the controlled-$U$ operations — and then we'll see how best to proceed.

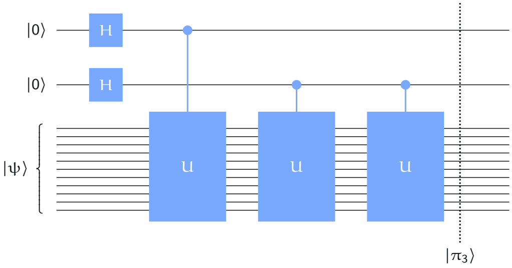



$$|\pi_1\rangle = |\psi\rangle \otimes \frac{1}{2} \sum_{a_0=0}^{1} \sum_{a_1=0}^{1} |a_1 a_0\rangle$$

$$|\pi_2\rangle = |\psi\rangle \otimes \frac{1}{2} \sum_{a_0=0}^{1} \sum_{a_1=0}^{1} e^{2\pi i a_0 \theta} |a_1 a_0\rangle$$

# Two control qubits

Let's use two control qubits to perform the controlled-$U$ operations — and then we'll see how best to proceed.




$$|\pi_3\rangle = |\psi\rangle \otimes \frac{1}{2}\sum_{a_0=0}^{1}\sum_{a_1=0}^{1} e^{2\pi i(2a_1+a_0)\theta}|a_1 a_0\rangle$$

$$= |\psi\rangle \otimes \frac{1}{2}\sum_{x=0}^{3} e^{2\pi i x\theta}|x\rangle$$

# Two control qubits

$$\frac{1}{2}\sum_{x=0}^{3} e^{2\pi i x\theta}|x\rangle$$

What can we learn about $\theta$ from this state? Suppose we're promised that $\theta = \frac{y}{4}$ for $y \in \{0, 1, 2, 3\}$. Can we figure out which one it is?

Define a two-qubit state for each possibility:

$$|\phi_y\rangle = \frac{1}{2}\sum_{x=0}^{3} e^{2\pi i \frac{xy}{4}}|x\rangle$$

$$|\phi_0\rangle = \frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle + \frac{1}{2}|2\rangle + \frac{1}{2}|3\rangle$$

$$|\phi_1\rangle = \frac{1}{2}|0\rangle + \frac{i}{2}|1\rangle - \frac{1}{2}|2\rangle - \frac{i}{2}|3\rangle$$

$$|\phi_2\rangle = \frac{1}{2}|0\rangle - \frac{1}{2}|1\rangle + \frac{1}{2}|2\rangle - \frac{1}{2}|3\rangle$$

$$|\phi_3\rangle = \frac{1}{2}|0\rangle - \frac{i}{2}|1\rangle - \frac{1}{2}|2\rangle + \frac{i}{2}|3\rangle$$

These vectors are *orthonormal* — so they can be discriminated perfectly by a projective measurement.

# Two control qubits

$$|\phi_y\rangle = \frac{1}{2}\sum_{x=0}^{3} e^{2\pi i \frac{xy}{4}} |x\rangle$$

$$\begin{aligned}
|\phi_0\rangle &= \frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle + \frac{1}{2}|2\rangle + \frac{1}{2}|3\rangle \\
|\phi_1\rangle &= \frac{1}{2}|0\rangle + \frac{i}{2}|1\rangle - \frac{1}{2}|2\rangle - \frac{i}{2}|3\rangle \\
|\phi_2\rangle &= \frac{1}{2}|0\rangle - \frac{1}{2}|1\rangle + \frac{1}{2}|2\rangle - \frac{1}{2}|3\rangle \\
|\phi_3\rangle &= \frac{1}{2}|0\rangle - \frac{i}{2}|1\rangle - \frac{1}{2}|2\rangle + \frac{i}{2}|3\rangle
\end{aligned}$$

$$V = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

These vectors are *orthonormal* — so they can be discriminated perfectly by a projective measurement.

$$\{|\phi_0\rangle\langle\phi_0|,\ |\phi_1\rangle\langle\phi_1|,\ |\phi_2\rangle\langle\phi_2|,\ |\phi_3\rangle\langle\phi_3|\}$$

The unitary matrix $V$ whose *columns* are $|\phi_0\rangle, |\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle$ has this action:

$$V|y\rangle = |\phi_y\rangle \quad \text{(for every } y \in \{0,1,2,3\})$$

# Two control qubits

$$|\phi_y\rangle = \frac{1}{2}\sum_{x=0}^{3} e^{2\pi i \frac{xy}{4}} |x\rangle$$

$$\begin{aligned}
|\phi_0\rangle &= \frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle + \frac{1}{2}|2\rangle + \frac{1}{2}|3\rangle \\
|\phi_1\rangle &= \frac{1}{2}|0\rangle + \frac{i}{2}|1\rangle - \frac{1}{2}|2\rangle - \frac{i}{2}|3\rangle \\
|\phi_2\rangle &= \frac{1}{2}|0\rangle - \frac{1}{2}|1\rangle + \frac{1}{2}|2\rangle - \frac{1}{2}|3\rangle \\
|\phi_3\rangle &= \frac{1}{2}|0\rangle - \frac{i}{2}|1\rangle - \frac{1}{2}|2\rangle + \frac{i}{2}|3\rangle
\end{aligned}$$

$$V = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

The unitary matrix $V$ whose *columns* are $|\phi_0\rangle$, $|\phi_1\rangle$, $|\phi_2\rangle$, $|\phi_3\rangle$ has this action:

$$V|y\rangle = |\phi_y\rangle \quad \text{(for every } y \in \{0,1,2,3\}\text{)}$$

We can identify $y$ by performing the inverse of $V$ then a standard basis measurement.

$$V^\dagger|\phi_y\rangle = |y\rangle \quad \text{(for every } y \in \{0,1,2,3\}\text{)}$$

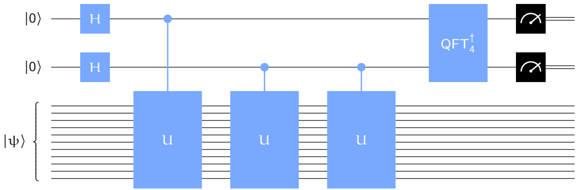
# Two-qubit phase estimation

$$\mathrm{QFT}_4 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

This matrix is associated with the *discrete Fourier transform* (for 4 dimensions).

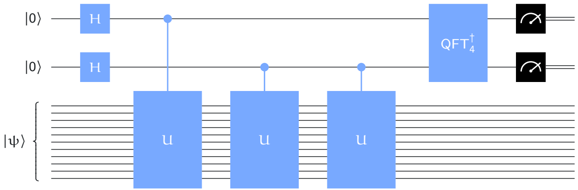
When we think about this matrix as a unitary operation, we call it the *quantum Fourier transform.*

The complete circuit for learning $y \in \{0, 1, 2, 3\}$ when $\theta = y/4$:

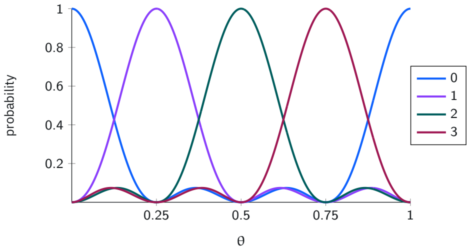


# Two-qubit phase estimation

The complete circuit for learning $y \in \{0, 1, 2, 3\}$ when $\theta = y/4$:




The outcome probabilities when we run the circuit, as a function of $\theta$:



# Quantum Fourier transform

The quantum Fourier transform is defined for each positive integer $N$ as follows.

$$\mathrm{QFT}_N = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} e^{2\pi i \frac{xy}{N}} |x\rangle\langle y|$$

$$\mathrm{QFT}_N |y\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{2\pi i \frac{xy}{N}} |x\rangle$$

**Example**

$$\mathrm{QFT}_1 = \begin{pmatrix} 1 \end{pmatrix}$$

# Quantum Fourier transform

The quantum Fourier transform is defined for each positive integer $N$ as follows.

$$\mathrm{QFT}_N = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} e^{2\pi i \frac{xy}{N}} |x\rangle\langle y|$$

$$\mathrm{QFT}_N |y\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{2\pi i \frac{xy}{N}} |x\rangle$$

Example

$$\mathrm{QFT}_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = H$$

# Quantum Fourier transform

The quantum Fourier transform is defined for each positive integer $N$ as follows.

$$
\begin{aligned}
\mathrm{QFT}_N &= \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} e^{2\pi i \frac{xy}{N}} |x\rangle\langle y| \\
\mathrm{QFT}_N |y\rangle &= \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{2\pi i \frac{xy}{N}} |x\rangle
\end{aligned}
$$

Example

$$
\mathrm{QFT}_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \frac{-1+i\sqrt{3}}{2} & \frac{-1-i\sqrt{3}}{2} \\ 1 & \frac{-1-i\sqrt{3}}{2} & \frac{-1+i\sqrt{3}}{2} \end{pmatrix}
$$

# Quantum Fourier transform

The quantum Fourier transform is defined for each positive integer $N$ as follows.

$$\mathrm{QFT}_N = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} e^{2\pi i \frac{xy}{N}} |x\rangle\langle y|$$

$$\mathrm{QFT}_N |y\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{2\pi i \frac{xy}{N}} |x\rangle$$

Example

$$\mathrm{QFT}_4 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

# Quantum Fourier transform

The quantum Fourier transform is defined for each positive integer $N$ as follows.

$$\mathrm{QFT}_N = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} e^{2\pi i \frac{xy}{N}} |x\rangle\langle y|$$

$$\mathrm{QFT}_N |y\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{2\pi i \frac{xy}{N}} |x\rangle$$

Example

$$\mathrm{QFT}_8 = \frac{1}{2\sqrt{2}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \frac{1+i}{\sqrt{2}} & i & \frac{-1+i}{\sqrt{2}} & -1 & \frac{-1-i}{\sqrt{2}} & -i & \frac{1-i}{\sqrt{2}} \\ 1 & i & -1 & -i & 1 & i & -1 & -i \\ 1 & \frac{-1+i}{\sqrt{2}} & -i & \frac{1+i}{\sqrt{2}} & -1 & \frac{1-i}{\sqrt{2}} & i & \frac{-1-i}{\sqrt{2}} \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & \frac{-1-i}{\sqrt{2}} & i & \frac{1-i}{\sqrt{2}} & -1 & \frac{1+i}{\sqrt{2}} & -i & \frac{-1+i}{\sqrt{2}} \\ 1 & -i & -1 & i & 1 & -i & -1 & i \\ 1 & \frac{1-i}{\sqrt{2}} & -i & \frac{-1-i}{\sqrt{2}} & -1 & \frac{-1+i}{\sqrt{2}} & i & \frac{1+i}{\sqrt{2}} \end{pmatrix}$$

# Quantum Fourier transform

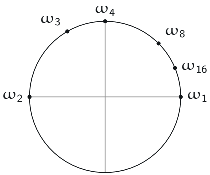
The quantum Fourier transform is defined for each positive integer $N$ as follows.

$$\mathrm{QFT}_N = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} e^{2\pi i \frac{xy}{N}} |x\rangle\langle y| = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \omega_N^{xy} |x\rangle\langle y|$$

$$\mathrm{QFT}_N |y\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{2\pi i \frac{xy}{N}} |x\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \omega_N^{xy} |x\rangle$$

Useful notation:

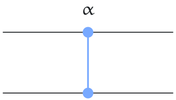
$$\omega_N = e^{\frac{2\pi i}{N}} = \cos\left(\frac{2\pi}{N}\right) + i \sin\left(\frac{2\pi}{N}\right)$$



# Circuits for the QFT

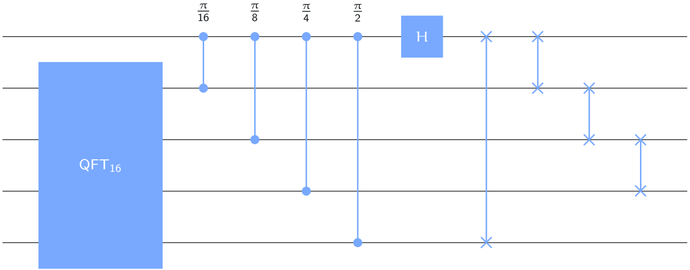
We can implement $\mathrm{QFT}_N$ efficiently with a quantum circuit when $N$ is a power of 2.

The implementation makes use of *controlled-phase* gates:

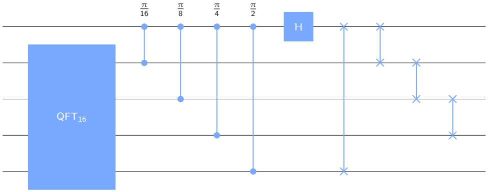



$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\alpha} \end{pmatrix}$$

The implementation is *recursive* in nature. As an example, here is the circuit for $\mathrm{QFT}_{32}$:



# Circuits for the QFT




Cost analysis

Let $s_m$ denote the number of gates we need for $m$ qubits.

- For $m = 1$, a single Hadamard gate is required.
- For $m \geq 2$, these are the gates required:

  $s_{m-1}$ gates for the QFT on $m - 1$ qubits
  $m - 1$ controlled phase gates
  $m - 1$ swap gates
  1 Hadamard gate

$$s_m = \begin{cases} 1 & m = 1 \\ s_{m-1} + 2m - 1 & m \geq 2 \end{cases}$$

# Circuits for the QFT

Cost analysis

Let $s_m$ denote the number of gates we need for $m$ qubits.

- For $m = 1$, a single Hadamard gate is required.
- For $m \geq 2$, these are the gates required:

  $s_{m-1}$ gates for the QFT on $m - 1$ qubits
  $m - 1$ controlled phase gates
  $m - 1$ swap gates
  1 Hadamard gate

$$s_m = \begin{cases} 1 & m = 1 \\ s_{m-1} + 2m - 1 & m \geq 2 \end{cases}$$

This is a *recurrence relation* with a closed-form solution:

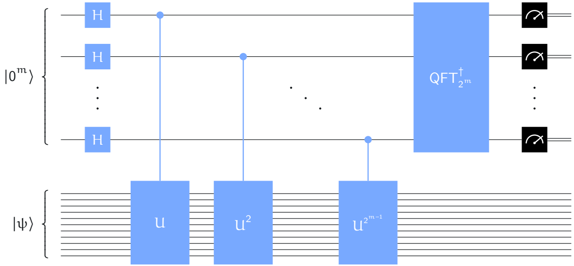
$$s_m = \sum_{k=1}^{m} (2k - 1) = m^2$$

Additional remarks:

- The number of swap gates can be reduced.
- Approximations to $\mathrm{QFT}_{2^m}$ can be done at lower cost (and lower depth).

# Phase estimation procedure

The general phase-estimation procedure, for any choice of $m$:

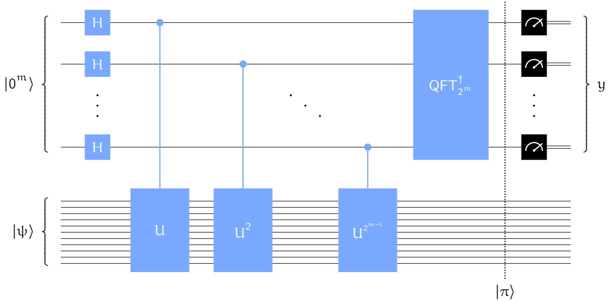



**Warning**

If we perform each $U^k$-operation by repeating a controlled-$U$ operation $k$ times, increasing the number of control qubits $m$ comes at a *high cost.*

# Phase estimation procedure

The general phase-estimation procedure, for any choice of $m$:




$$|\pi\rangle = |\psi\rangle \otimes \frac{1}{2^m} \sum_{y=0}^{2^m-1} \sum_{x=0}^{2^m-1} e^{2\pi i x(\theta - y/2^m)} |y\rangle$$

$$p_y = \left| \frac{1}{2^m} \sum_{x=0}^{2^m-1} e^{2\pi i x(\theta - y/2^m)} \right|^2$$

# Phase estimation procedure

$$p_y = \left| \frac{1}{2^m} \sum_{x=0}^{2^m-1} e^{2\pi i x(\theta - y/2^m)} \right|^2$$

## Best approximations

Suppose $y/2^m$ is a *best approximation* to $\theta$:

$$\left| \theta - \frac{y}{2^m} \right|_1 \leq 2^{-(m+1)}$$

The probability to measure $y$ will be high:

$$p_y \geq \frac{4}{\pi^2} \approx 0.405$$

## Worse approximations

Suppose there's a *better approximation* to $\theta$ between $y/2^m$ and $\theta$:

$$\left| \theta - \frac{y}{2^m} \right|_1 \geq 2^{-m}$$

The probability to measure $y$ will be lower:

$$p_y \leq \frac{1}{4}$$

# Phase estimation procedure

**Best approximations**

Suppose $y/2^m$ is a *best approximation* to $\theta$:

$$\left|\theta - \frac{y}{2^m}\right|_1 \leq 2^{-(m+1)}$$

The probability to measure $y$ will be high:

$$p_y \geq \frac{4}{\pi^2} \approx 0.405$$

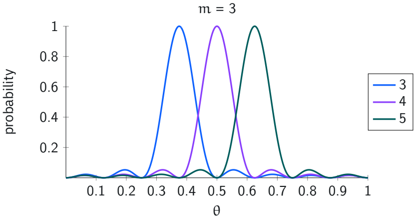
**Worse approximations**

Suppose there's a *better approximation* to $\theta$ between $y/2^m$ and $\theta$:

$$\left|\theta - \frac{y}{2^m}\right|_1 \geq 2^{-m}$$

The probability to measure $y$ will be lower:

$$p_y \leq \frac{1}{4}$$



# Phase estimation procedure

## Best approximations

Suppose $y/2^m$ is a *best approximation* to $\theta$:

$$\left|\theta - \frac{y}{2^m}\right|_1 \leq 2^{-(m+1)}$$

The probability to measure $y$ will be high:

$$p_y \geq \frac{4}{\pi^2} \approx 0.405$$

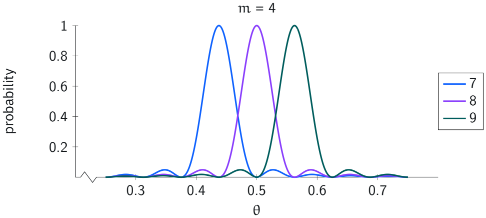
## Worse approximations

Suppose there's a *better approximation* to $\theta$ between $y/2^m$ and $\theta$:

$$\left|\theta - \frac{y}{2^m}\right|_1 \geq 2^{-m}$$

The probability to measure $y$ will be lower:

$$p_y \leq \frac{1}{4}$$



# Phase estimation procedure

## Best approximations

Suppose $y/2^m$ is a *best approximation* to $\theta$:

$$\left|\theta - \frac{y}{2^m}\right|_1 \leq 2^{-(m+1)}$$

The probability to measure $y$ will be high:

$$p_y \geq \frac{4}{\pi^2} \approx 0.405$$

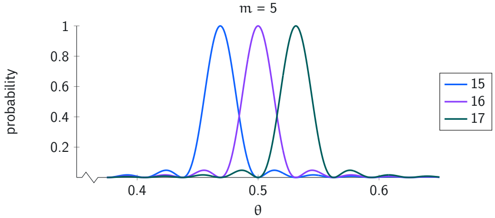
## Worse approximations

Suppose there's a *better approximation* to $\theta$ between $y/2^m$ and $\theta$:

$$\left|\theta - \frac{y}{2^m}\right|_1 \geq 2^{-m}$$

The probability to measure $y$ will be lower:

$$p_y \leq \frac{1}{4}$$



# Phase estimation procedure

## Best approximations

Suppose $y/2^m$ is a *best approximation* to $\theta$:

$$\left|\theta - \frac{y}{2^m}\right|_1 \leq 2^{-(m+1)}$$

The probability to measure $y$ will be high:

$$p_y \geq \frac{4}{\pi^2} \approx 0.405$$

## Worse approximations

Suppose there's a *better approximation* to $\theta$ between $y/2^m$ and $\theta$:

$$\left|\theta - \frac{y}{2^m}\right|_1 \geq 2^{-m}$$

The probability to measure $y$ will be lower:

$$p_y \leq \frac{1}{4}$$

To obtain an approximation $y/2^m$ that is *very likely* to satisfy

$$\left|\theta - \frac{y}{2^m}\right|_1 < 2^{-m}$$

we can run the phase estimation procedure using $m$ control qubits *several times* and take $y$ to be the *mode* of the outcomes. (The eigenvector $|\psi\rangle$ is unchanged by the procedure and can be reused as many times as needed.)

# Order-finding and factoring

### Order-finding problem

Input: Positive integers $a$ and $N$ with $\gcd(a, N) = 1$.

Output: The smallest positive integer $r$ such that $a^r \equiv 1 \pmod{N}$

No efficient classical algorithm for this problem is known — an efficient algorithm for order-finding implies an efficient algorithm for integer factorization.

### Factor-finding method

1. Choose $a \in \{2, \ldots, N-1\}$ at random.
2. Compute $d = \gcd(a, N)$. If $d \geq 2$ then output $d$ and stop.
3. *Compute the order* $r$ of $a$ modulo $N$.
4. If $r$ is even, then compute $d = \gcd(a^{r/2} - 1, N)$. If $d \geq 2$, output $d$ and stop.
5. If this step is reached, the method has failed.

This method succeeds in finding a factor of $N$ with probability at least $1/2$, provided $N$ is odd and not a prime power.

# Order-finding and factoring

## Factor-finding method

1. Choose $a \in \{2, \dots, N-1\}$ at random.
2. Compute $d = \gcd(a, N)$. If $d \geq 2$ then output $d$ and stop.
3. *Compute the order* $r$ of $a$ modulo $N$.
4. If $r$ is even, then compute $d = \gcd(a^{r/2} - 1, N)$. If $d \geq 2$, output $d$ and stop.
5. If this step is reached, the method has failed.

## Main idea

By the definition of the order we know that $a^r \equiv 1 \pmod{N}$, so $N$ divides $a^r - 1$.
If $r$ is even, then

$$a^r - 1 = (a^{r/2} + 1)(a^{r/2} - 1)$$

Each prime dividing $N$ must therefore divide either $(a^{r/2} + 1)$ or $(a^{r/2} - 1)$.
For a random $a$, at least one of the prime factors of $N$ is likely to divide $(a^{r/2} - 1)$.

# Order-finding by phase-estimation

Assume $N$ is a positive integer, and let $n$ be the number of bits required to express $N - 1$ in binary notation.

For every positive integer $a$ satisfying $\gcd(a, N) = 1$, define an $n$-qubit unitary operation as follows for $x = 0, \ldots, 2^n - 1$ written in binary:

$$M_a|x\rangle = \begin{cases} |ax \bmod N\rangle & 0 \leq x < N \\ |x\rangle & N \leq x < 2^n \end{cases}$$

This is a *unitary operation* — but only because $\gcd(a, N) = 1$! We can build quantum circuits for these operations using $O(n^2)$ gates.

Main idea

We'll perform phase estimation $M_a$.

The *eigenvalues* of $M_a$ are closely connected with the *order* of $a$ modulo $N$. By approximating the eigenvalues with enough precision, we can determine the order.

# Order-finding by phase-estimation

$$M_a|x\rangle = \begin{cases} |ax \bmod N\rangle & 0 \le x < N \\ |x\rangle & N \le x < 2^n \end{cases}$$

What are (some of) the eigenvectors and eigenvalues of $M_a$?

Notation:

- Let $r$ denote the order of $a$ modulo $N$. (We're trying to find $r$.)
- Every expression in a ket is taken modulo $N$.

Also recall that $\omega_r = e^{2\pi i/r}$.

$$|\psi_0\rangle = \frac{|1\rangle + |a\rangle + \cdots + |a^{r-1}\rangle}{\sqrt{r}} \qquad M_a|\psi_0\rangle = |\psi_0\rangle \qquad \theta = 0$$

# Order-finding by phase-estimation

$$M_a|x\rangle = \begin{cases} |ax \bmod N\rangle & 0 \leq x < N \\ |x\rangle & N \leq x < 2^n \end{cases}$$

What are (some of) the eigenvectors and eigenvalues of $M_a$?

Notation:

- Let $r$ denote the order of $a$ modulo $N$. (We're trying to find $r$.)
- Every expression in a ket is taken modulo $N$.

Also recall that $\omega_r = e^{2\pi i/r}$.

$$|\psi_1\rangle = \frac{|1\rangle + \omega_r^{-1}|a\rangle + \cdots + \omega_r^{-(r-1)}|a^{r-1}\rangle}{\sqrt{r}} \qquad M_a|\psi_1\rangle = \omega_r|\psi_1\rangle \qquad \theta = \frac{1}{r}$$

# Order-finding by phase-estimation

$$M_a|x\rangle = \begin{cases} |ax \bmod N\rangle & 0 \leq x < N \\ |x\rangle & N \leq x < 2^n \end{cases}$$

What are (some of) the eigenvectors and eigenvalues of $M_a$?

Notation:

- Let $r$ denote the order of $a$ modulo $N$. (We're trying to find $r$.)
- Every expression in a ket is taken modulo $N$.

Also recall that $\omega_r = e^{2\pi i/r}$.

$$|\psi_j\rangle = \frac{|1\rangle + \omega_r^{-j}|a\rangle + \cdots + \omega_r^{-j(r-1)}|a^{r-1}\rangle}{\sqrt{r}} \qquad M_a|\psi_j\rangle = \omega_r^j|\psi_j\rangle \qquad \theta = \frac{j}{r}$$

# Order-finding by phase-estimation

$$M_a|x\rangle = \begin{cases} |ax \bmod N\rangle & 0 \leq x < N \\ |x\rangle & N \leq x < 2^n \end{cases}$$

$$|\psi_j\rangle = \frac{|1\rangle + \omega_r^{-j}|a\rangle + \cdots + \omega_r^{-j(r-1)}|a^{r-1}\rangle}{\sqrt{r}} \qquad M_a|\psi_j\rangle = \omega_r^j|\psi_j\rangle \qquad \theta = \frac{j}{r}$$

We won't actually create any of these eigenvectors to use in phase estimation. Instead, we'll use the state $|1\rangle$ (meaning the $n$-bit binary representation of 1).

Here's the key equation that makes this work:

$$|1\rangle = \frac{|\psi_0\rangle + \cdots + |\psi_{r-1}\rangle}{\sqrt{r}}$$

The result is equivalent to *randomly selecting* one of the eigenvectors $|\psi_0\rangle, \ldots, |\psi_{N-1}\rangle$. We obtain an approximation to $j/r$ for a random $j \in \{0, \ldots, N-1\}$.

# Order-finding by phase-estimation

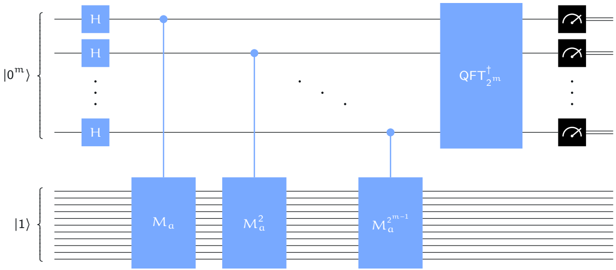
$$M_a|x\rangle = \begin{cases} |ax \bmod N\rangle & 0 \le x < N \\ |x\rangle & N \le x < 2^n \end{cases}$$

$$|\psi_j\rangle = \frac{|1\rangle + \omega_r^{-j}|a\rangle + \cdots + \omega_r^{-j(r-1)}|a^{r-1}\rangle}{\sqrt{r}} \qquad M_a|\psi_j\rangle = \omega_r^j|\psi_j\rangle \qquad \theta = \frac{j}{r}$$

The result is equivalent to *randomly selecting* one of the eigenvectors $|\psi_0\rangle, \ldots, |\psi_{N-1}\rangle$. We obtain an approximation to $j/r$ for a random $j \in \{0, \ldots, N-1\}$.

By using sufficiently high precision ($m = 2n$ bits of precision suffice) and repeating a small number of times, the order $r$ can be recovered with high probability.

# Implementation




**Cost for controlled unitary operations**

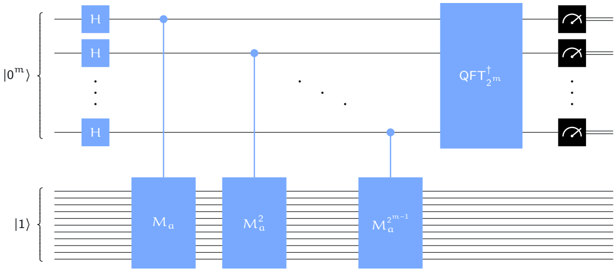
Each $M_a^k$ for each $k = 1, 2, 4, 8, \ldots, 2^{m-1}$ can be implemented as follows:

Compute $b = a^k \bmod N$ using the power algorithm (also called repeated squaring).

Use a circuit for $M_b$ in place of $M_a^k$.

The cost to implement each $M_b = M_a^k$ is $O(n^2)$.

# Implementation




**Total cost for phase estimation**

- $m$ Hadamard gates: cost $O(n)$
- $m$ controlled unitary operations: cost $O(n^3)$
- Quantum Fourier transform: cost $O(n^2)$

Total cost: $O(n^3)$

Thank you for your attention!