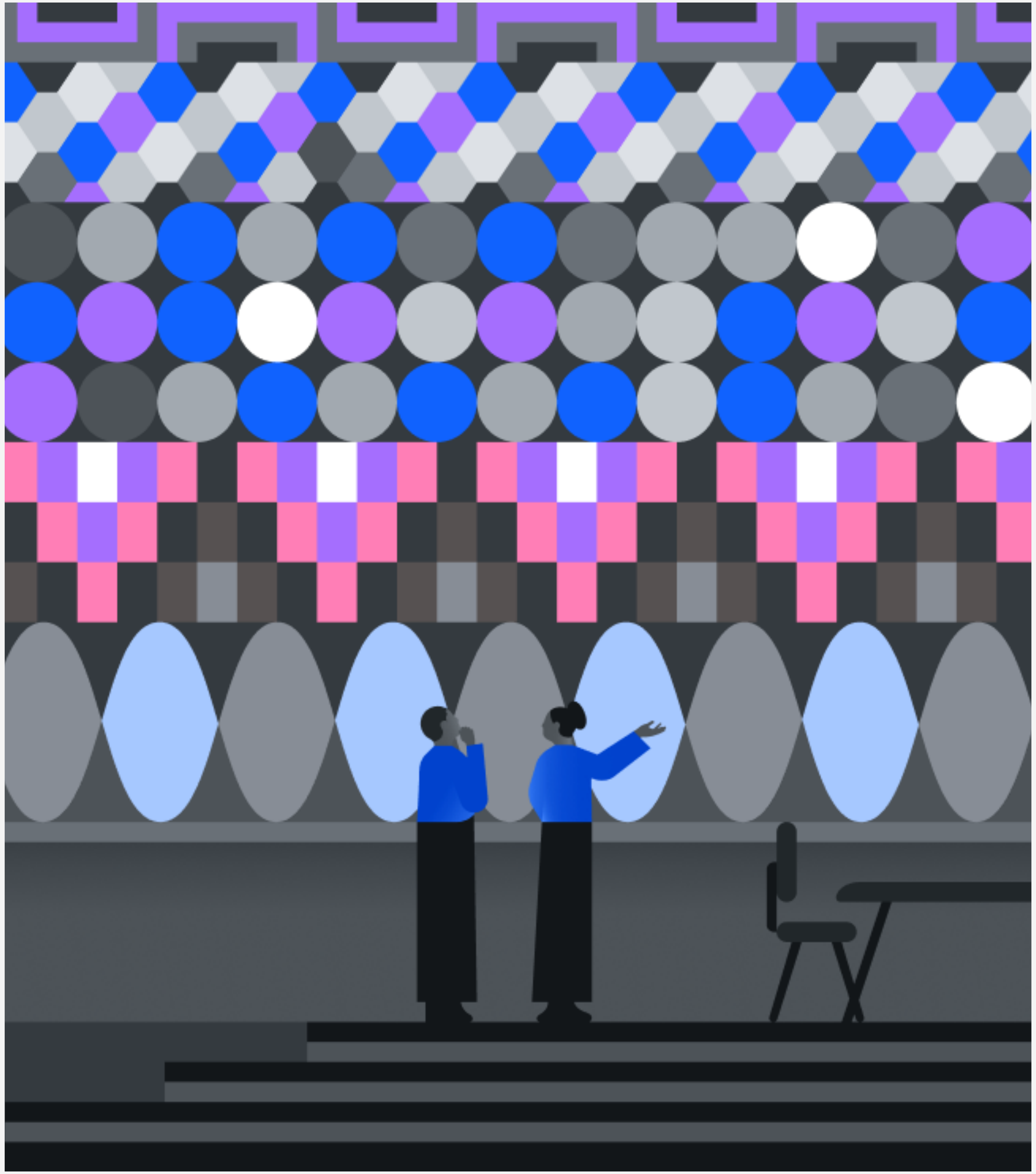
Understanding quantum information and computation

By John Watrous

Lesson 7

Phase estimation and factoring



IBM

Spectral theorem for unitary matrices

The *spectral theorem* is an important fact in linear algebra. Here is a statement of a special case of this theorem, for *unitary matrices.*

Spectral theorem for unitary matrices

Suppose U is an $N \times N$ unitary matrix.

There exists an orthonormal basis $\{|\psi_1\rangle, \ldots, |\psi_N\rangle\}$ of vectors along with complex numbers

$$\lambda_1 = e^{2\pi i\theta_1}, \; \ldots, \; \lambda_N = e^{2\pi i\theta_N}$$

such that

$$U = \sum_{k=1}^{N} \lambda_k |\psi_k\rangle\langle\psi_k|$$

Spectral theorem for unitary matrices

Spectral theorem for unitary matrices

Suppose U is an $N \times N$ unitary matrix.

There exists an orthonormal basis $\{|\psi_1\rangle, \ldots, |\psi_N\rangle\}$ of vectors along with complex numbers

$$\lambda_1 = e^{2\pi i\theta_1}, \ \ldots, \ \lambda_N = e^{2\pi i\theta_N}$$

such that

$$U = \sum_{k=1}^{N} \lambda_k |\psi_k\rangle\langle\psi_k|$$

Each vector $|\psi_k\rangle$ is an *eigenvector* of U having *eigenvalue* λ_k:

$$U|\psi_k\rangle = \lambda_k|\psi_k\rangle = e^{2\pi i\theta_k}|\psi_k\rangle$$

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

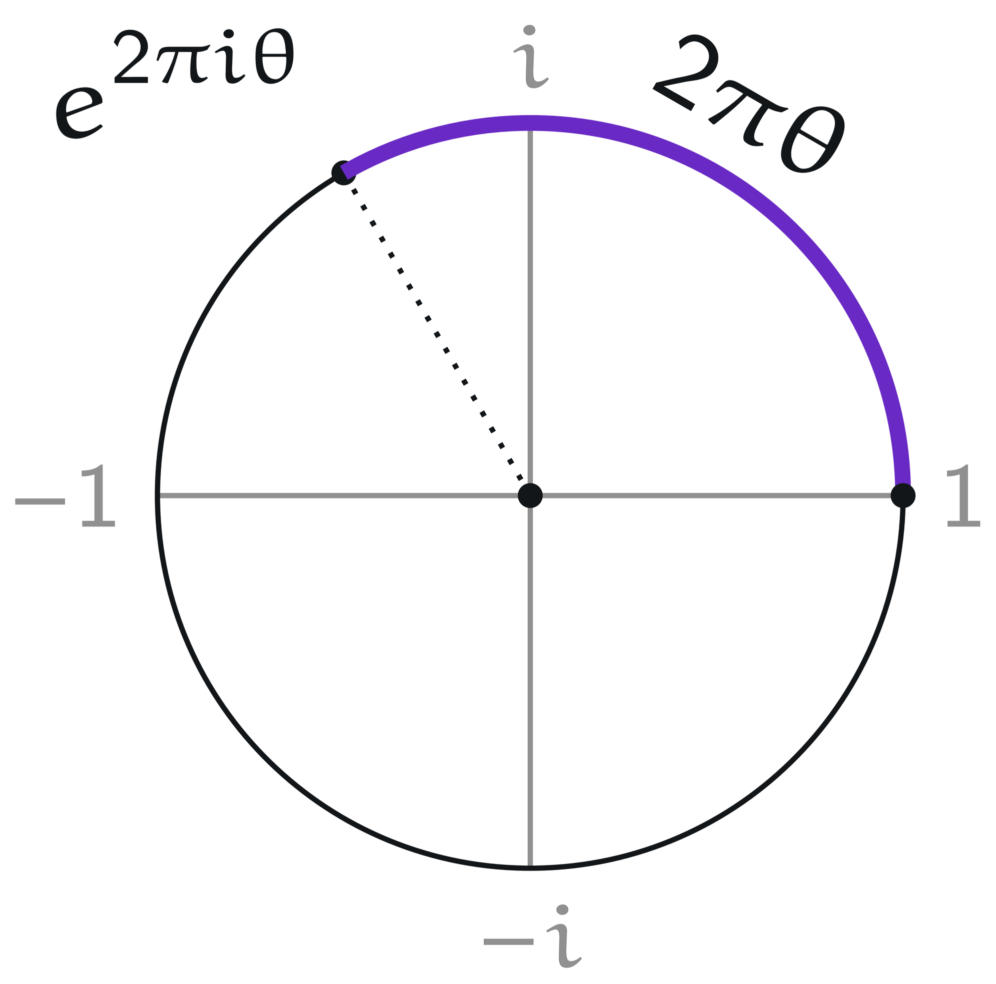
Phase estimation problem

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 θ by a fraction

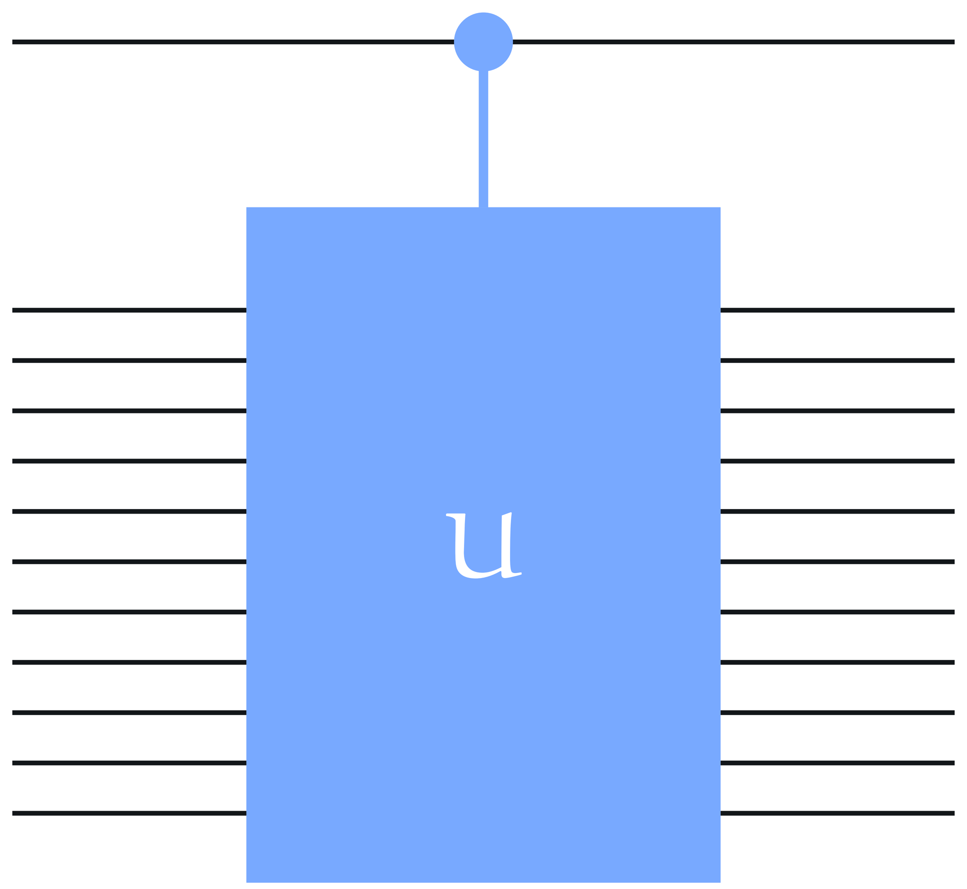
$$\theta \approx \frac{y}{2^m}$$

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

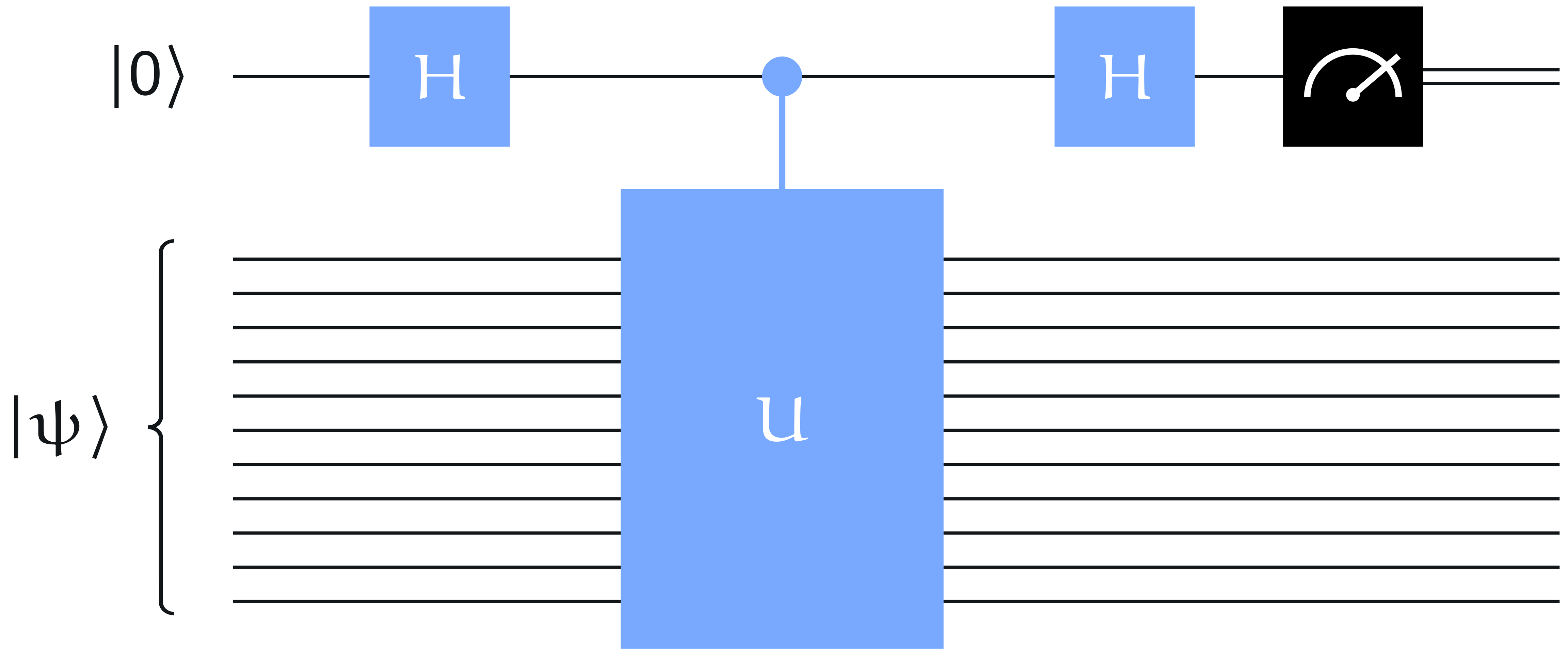
This approximation is taken “modulo 1.”

Warm-up: using the phase kickback

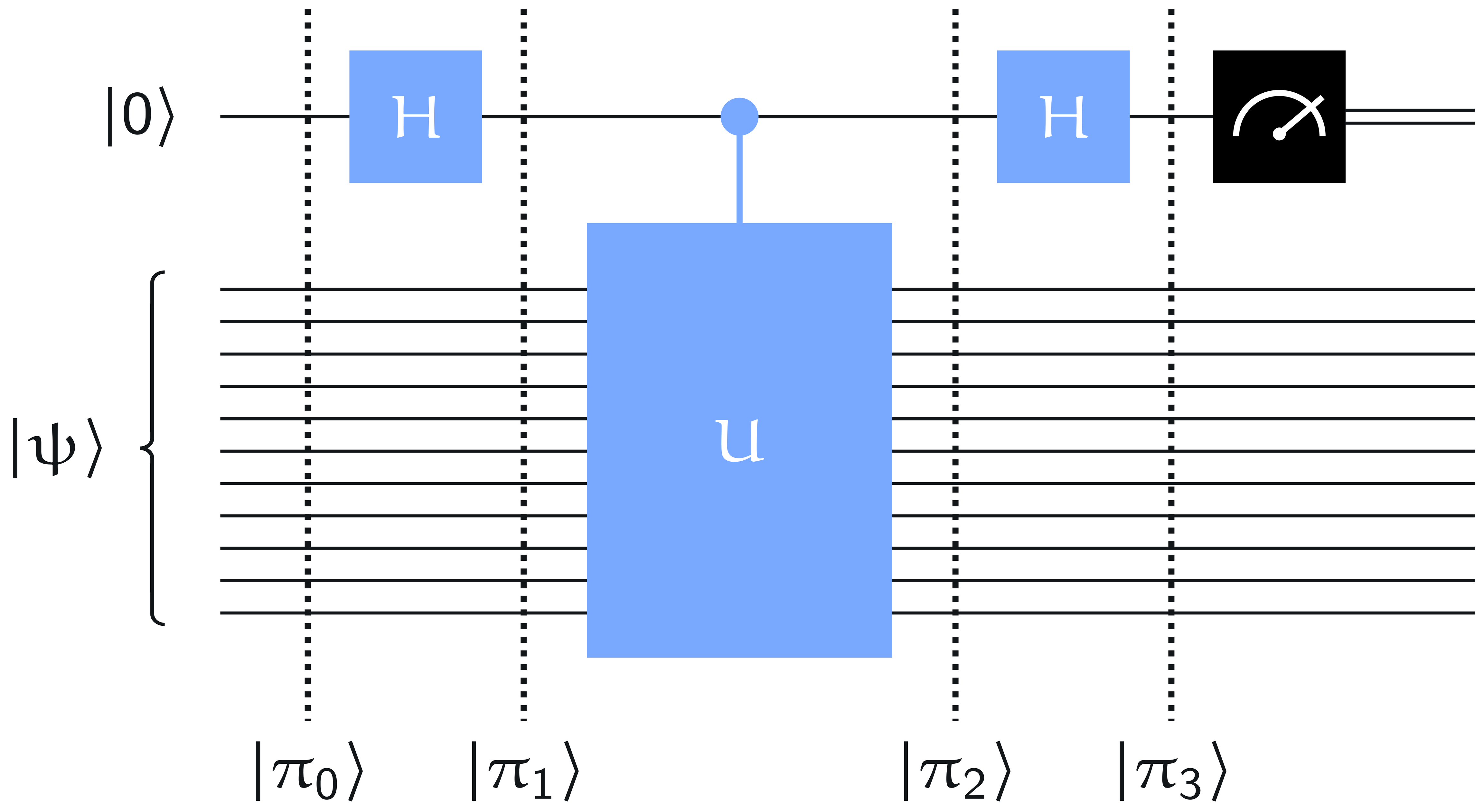
Given a circuit for U, we can create a circuit for a controlled-U operation:



Let's consider this circuit:



Warm-up: using the phase kickback

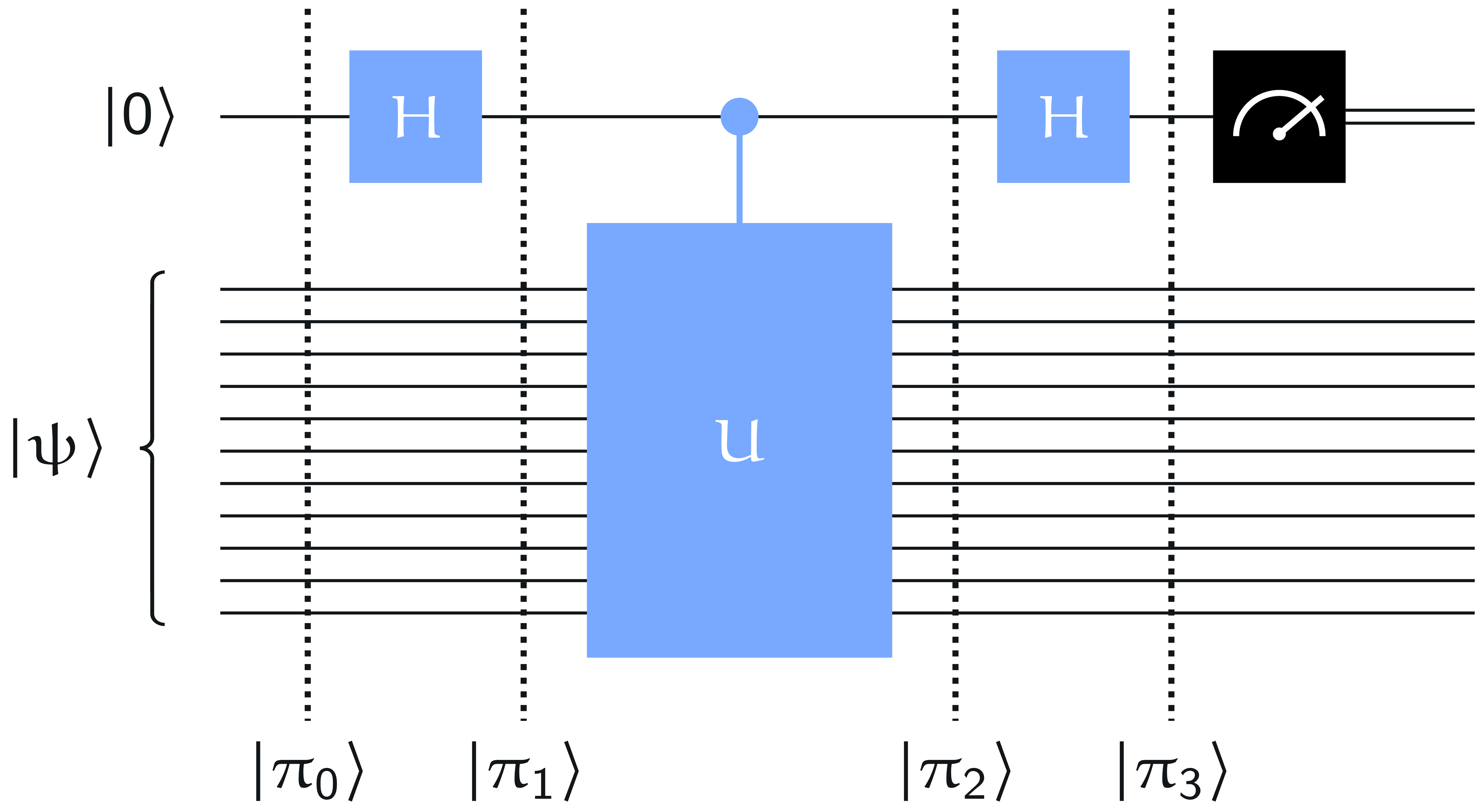


$$|\pi_0\rangle = |\psi\rangle|0\rangle$$

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

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

Warm-up: using the phase kickback



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

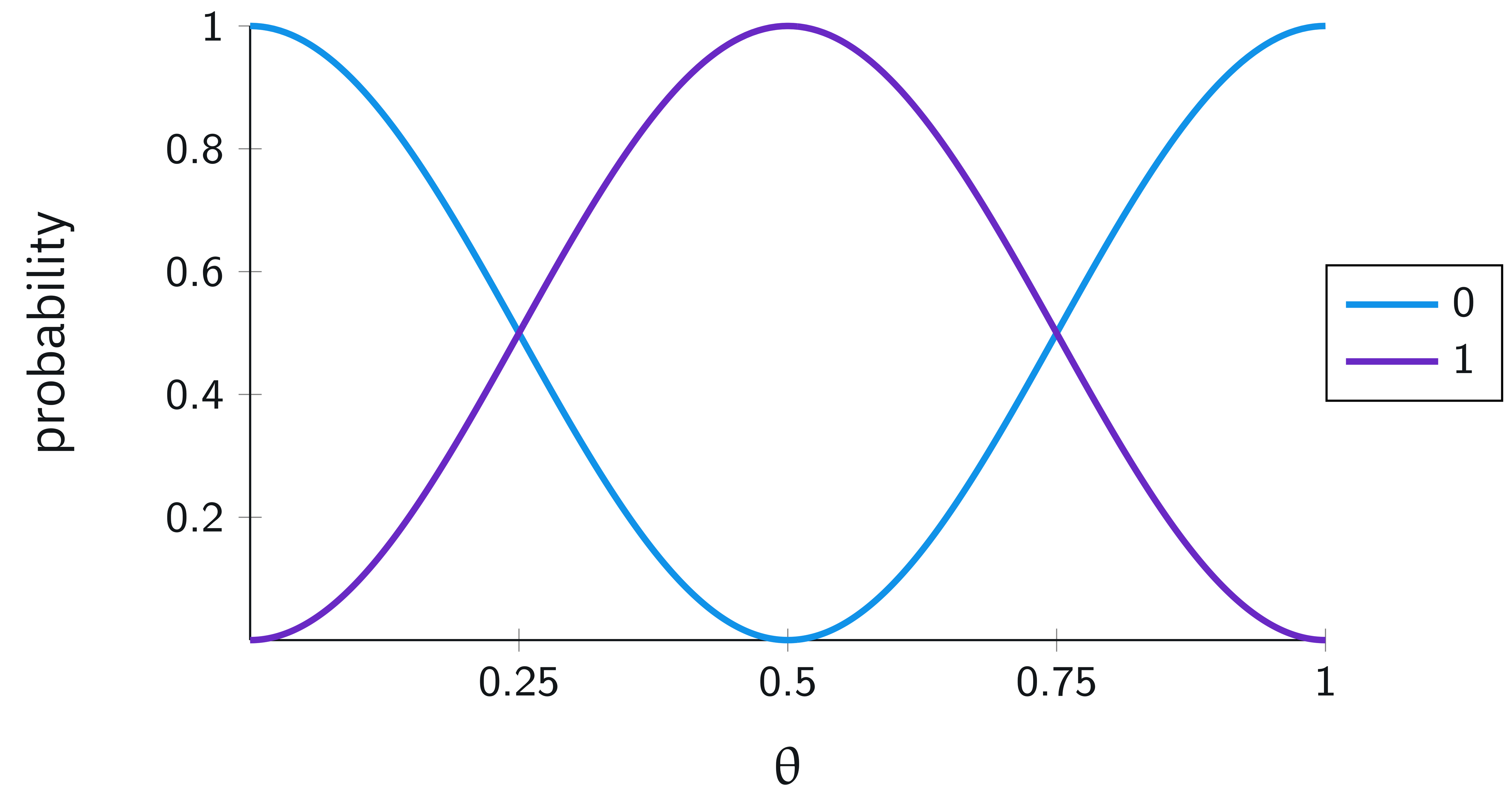
$$|\pi_3\rangle = |\psi\rangle \otimes \left(\frac{1 + e^{2\pi i\theta}}{2}|0\rangle + \frac{1 - e^{2\pi i\theta}}{2}|1\rangle \right)$$

Warm-up: using the phase kickback

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

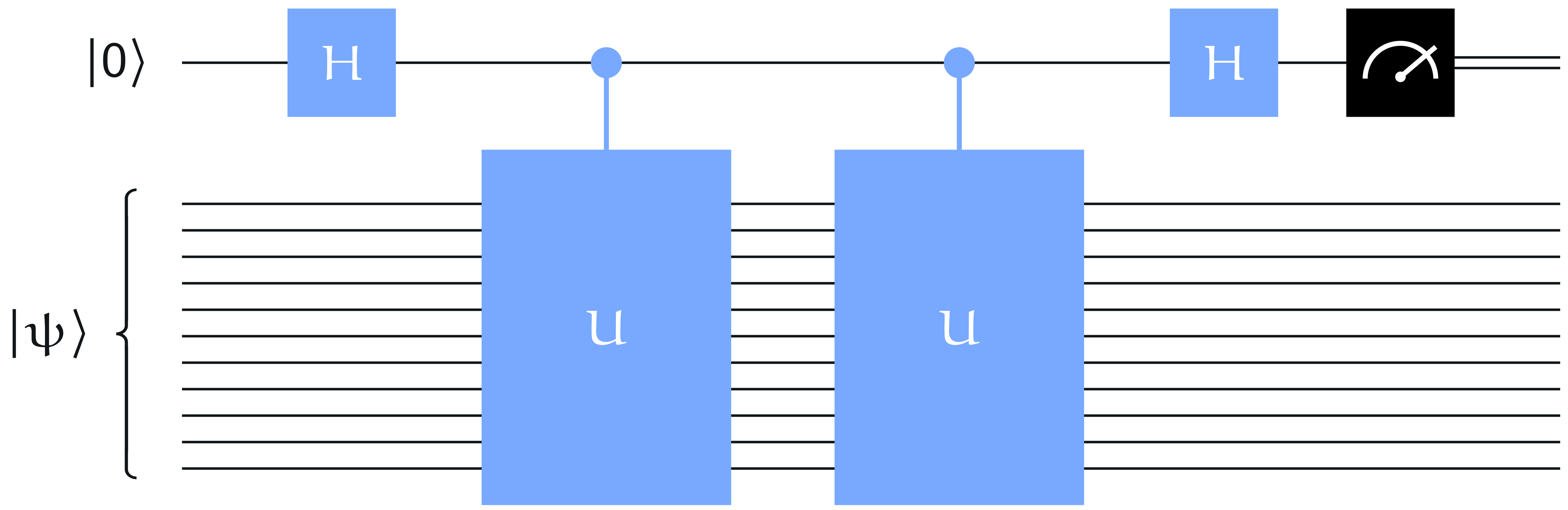
Measuring the top qubit yields the outcomes 0 and 1 with these probabilities:

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

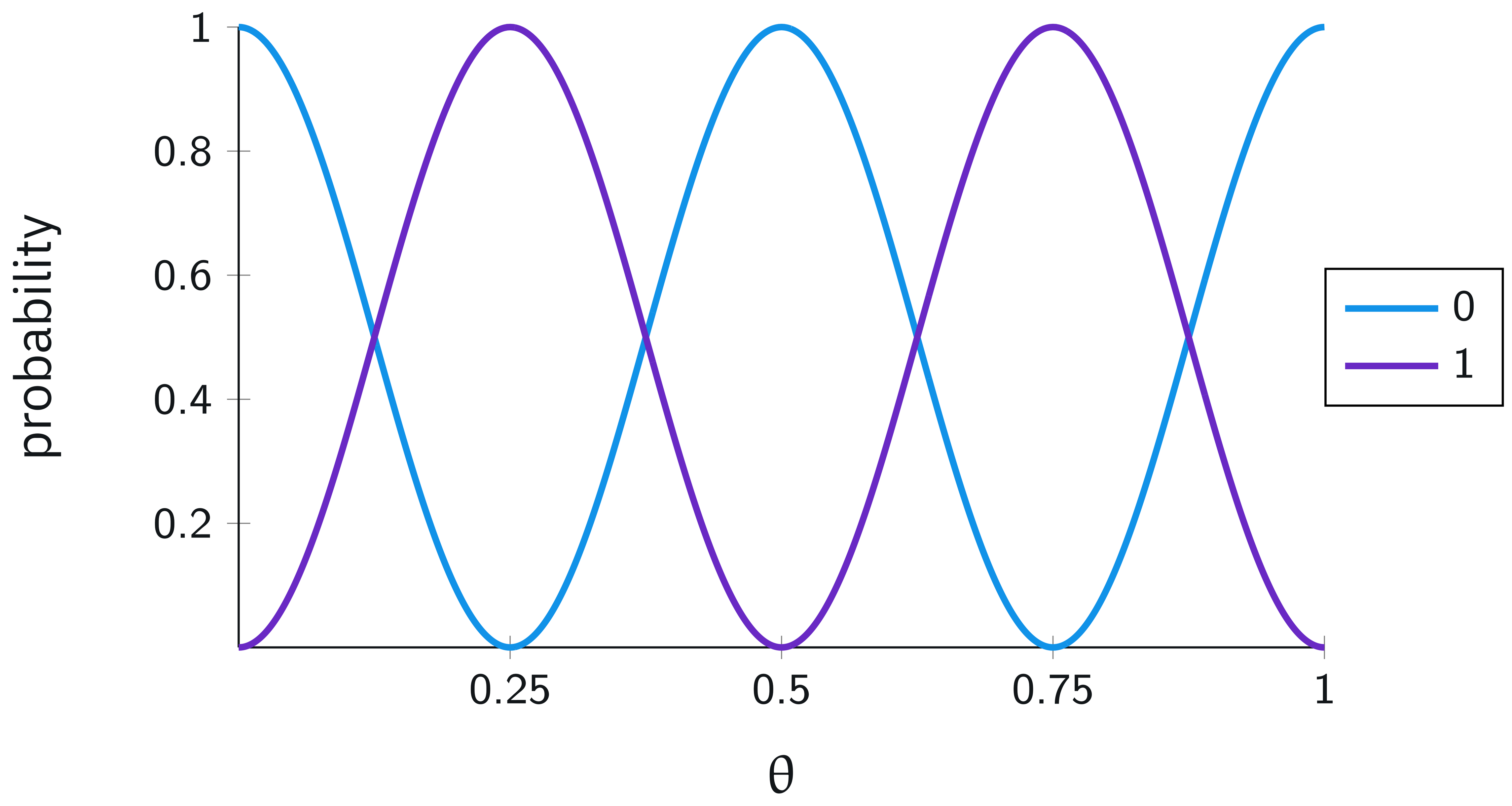


Iterating the unitary operation

How can we learn more about θ? One possibility is to apply the controlled-U operation twice (or multiple times):

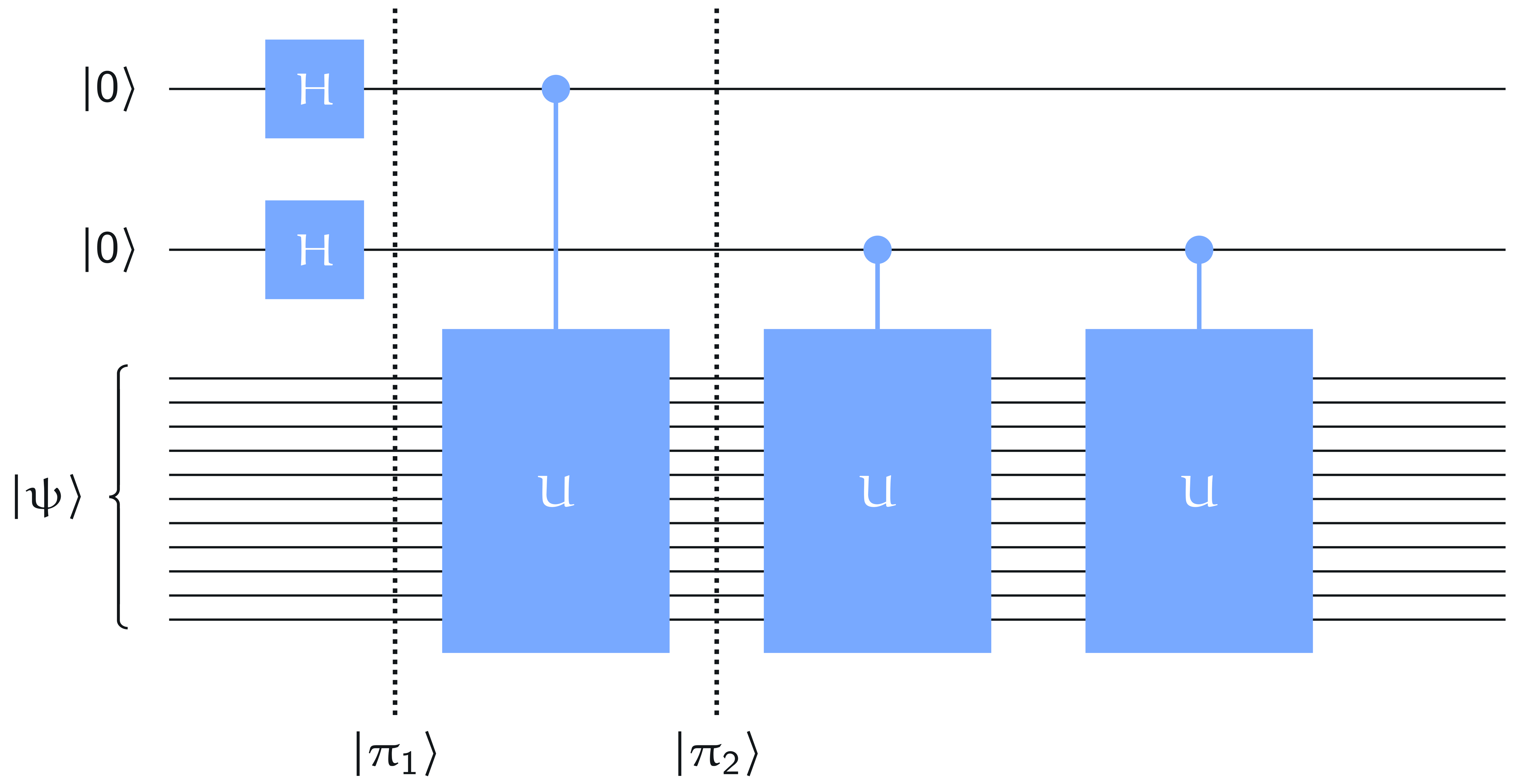


Performing the controlled-U operation twice has the effect of squaring the eigenvalue:



Two control qubits

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

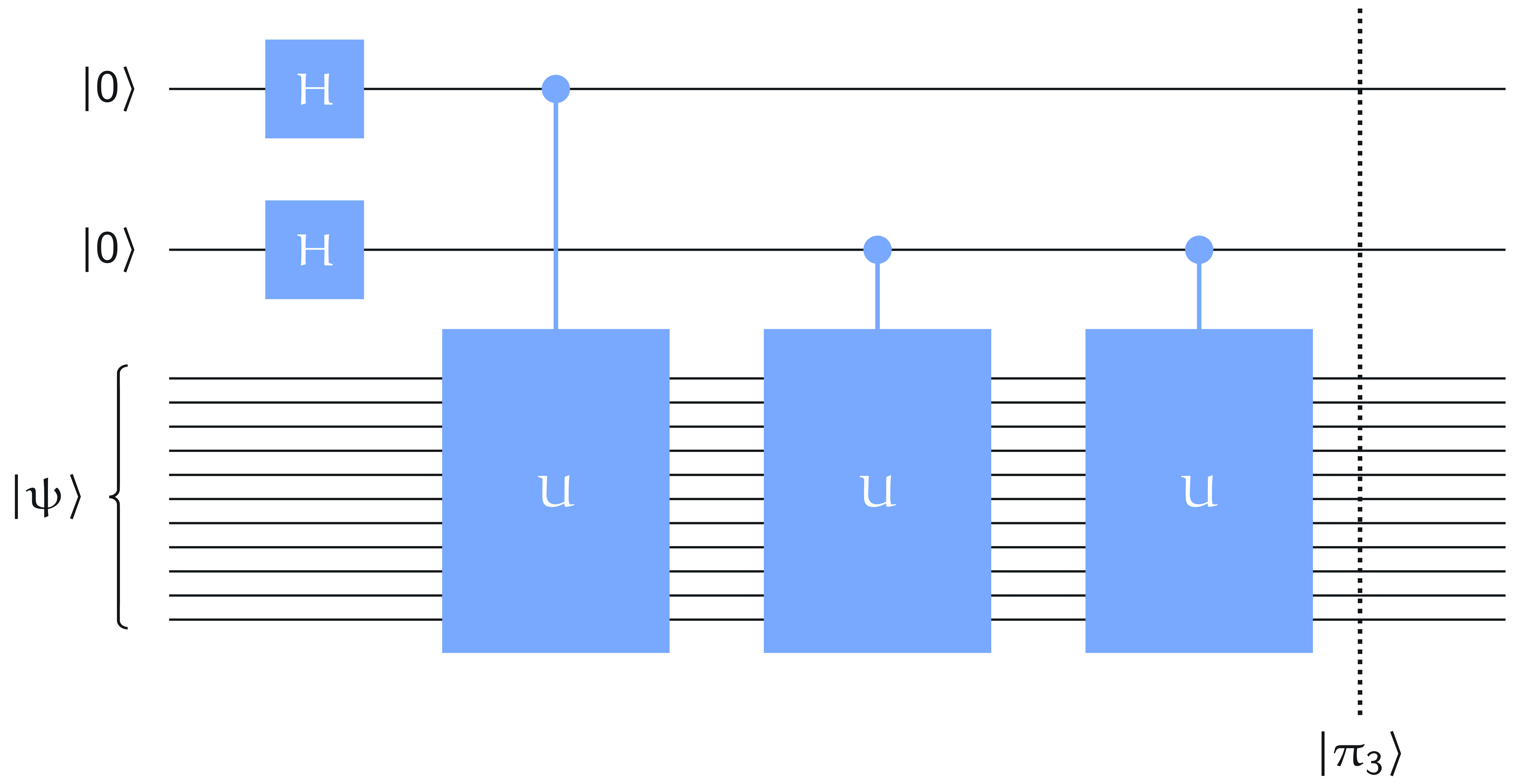


$$|\pi_1\rangle = |\psi\rangle \otimes \frac{1}{2} \sum_{a_0=0}^{1} \sum_{a_1=0}^{1} |a_1 a_0\rangle$$

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

Two control qubits

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



$$
\begin{aligned}
|\pi_3\rangle &= |\psi\rangle \otimes \frac{1}{2} \sum_{a_0=0}^{1} \sum_{a_1=0}^{1} e^{2\pi i (2a_1 + a_0)\theta} |a_1 a_0\rangle \\
&= |\psi\rangle \otimes \frac{1}{2} \sum_{x=0}^{3} e^{2\pi i x \theta} |x\rangle
\end{aligned}
$$

Two control qubits

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

What can we learn about θ 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

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

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

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

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

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

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

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.

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

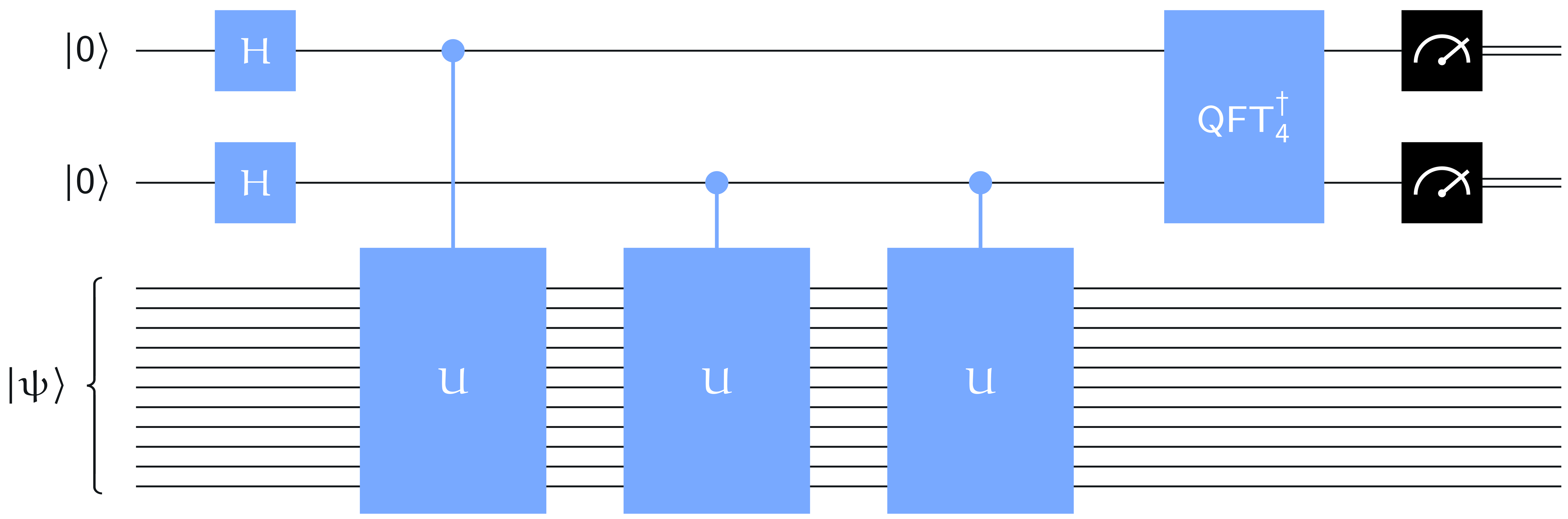
Two-qubit phase estimation

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

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

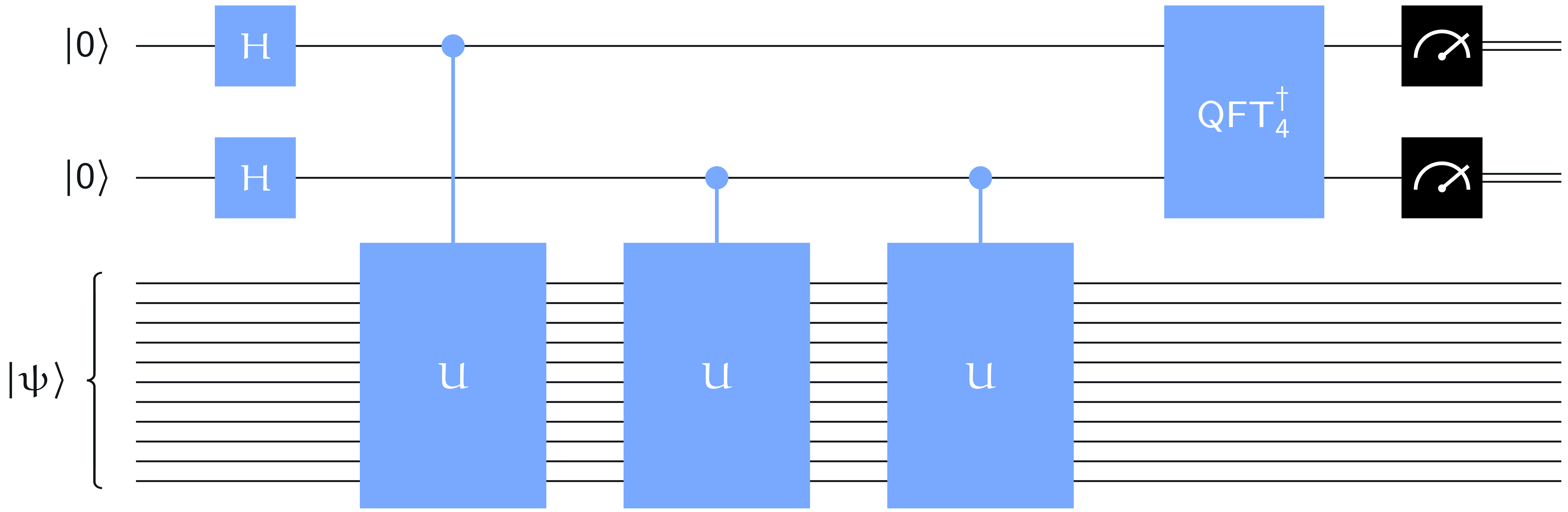
When we think about this matrix as a unitary operation, we call it the *quantum Fourier transform.*

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

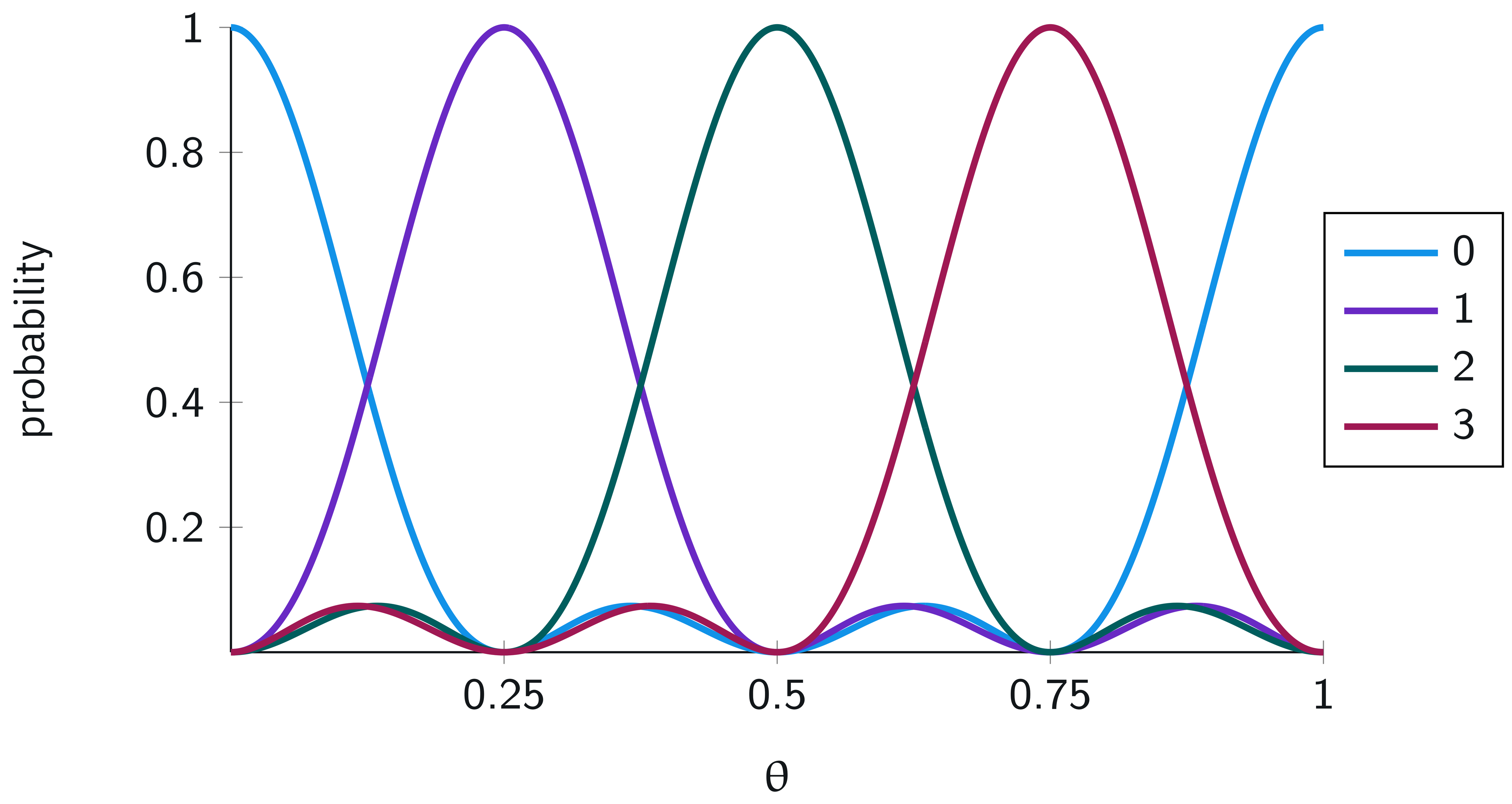


Two-qubit phase estimation

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 θ:



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

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

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

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

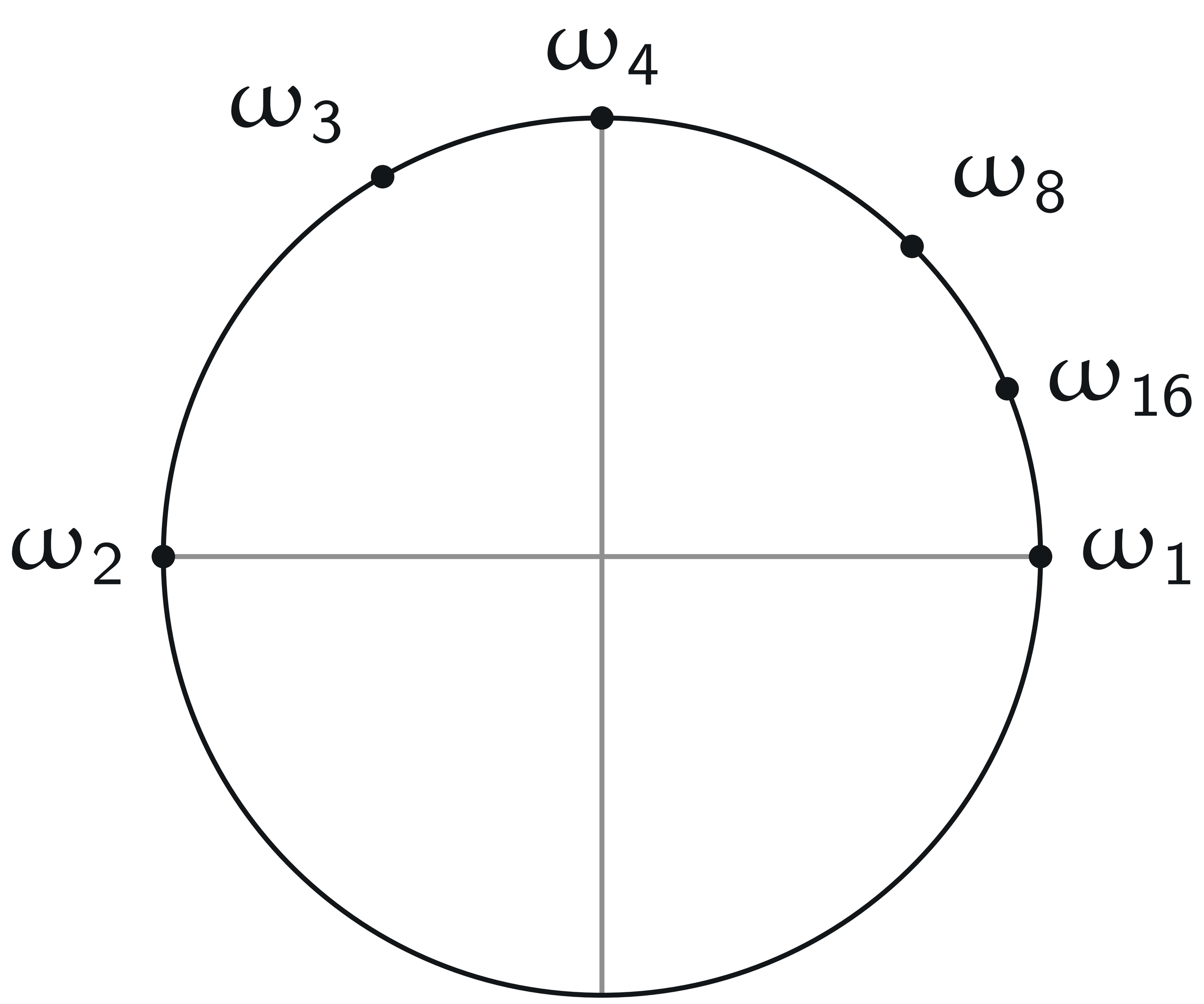
Quantum Fourier transform

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

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

Useful shorthand notation:

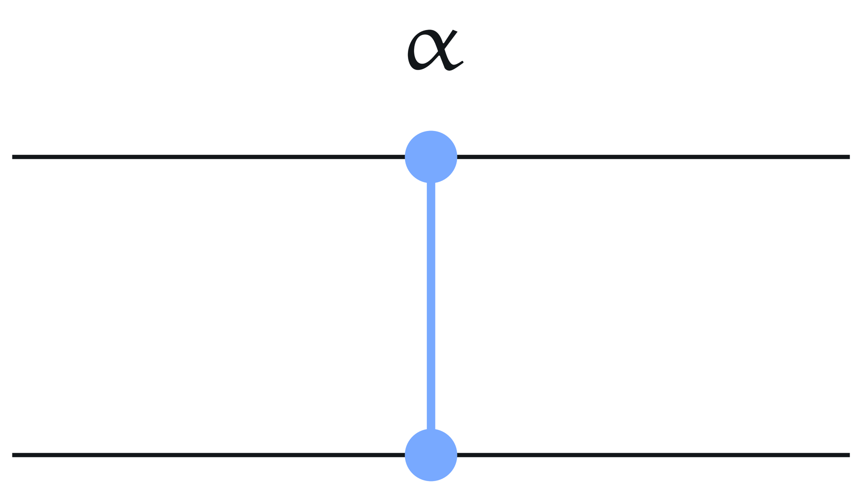
$$\omega_N = e^{\frac{2\pi i}{N}} = \cos\left(\frac{2\pi}{N}\right) + i \sin\left(\frac{2\pi}{N}\right)$$



Circuits for the QFT

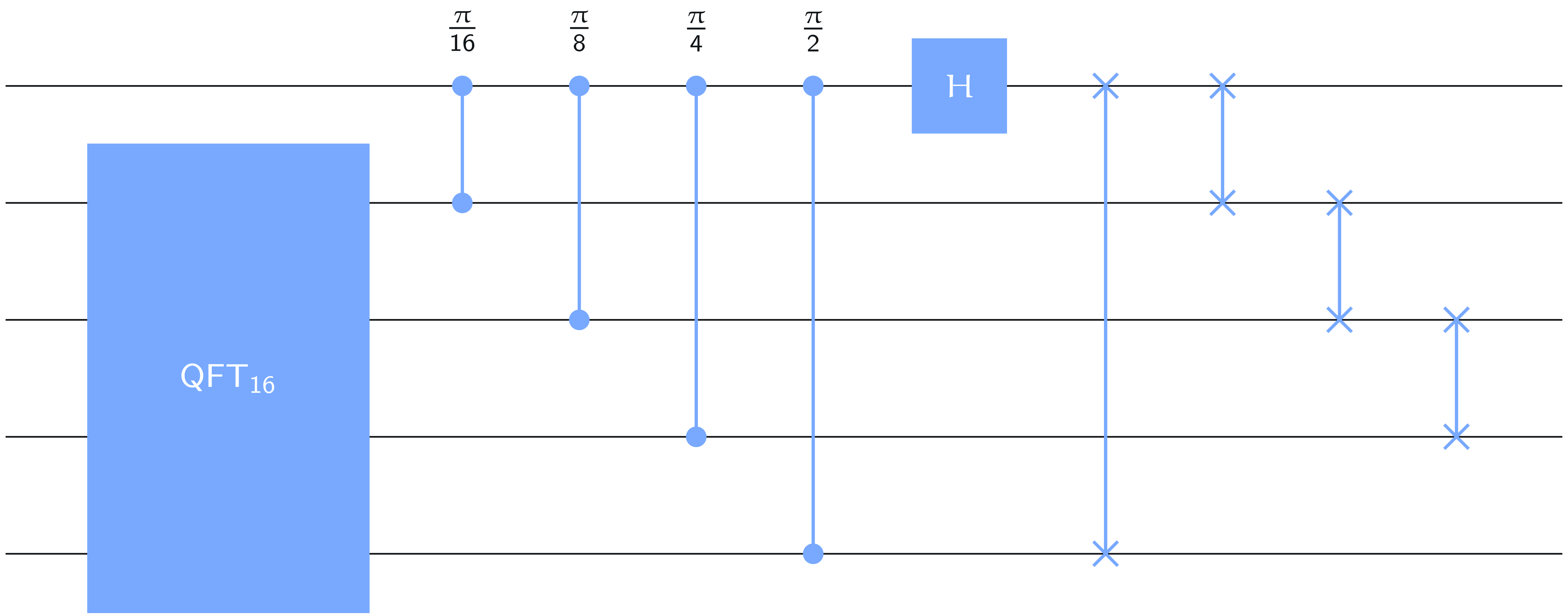
We can implement QFT_N efficiently with a quantum circuit when N is a power of 2.

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 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

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

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

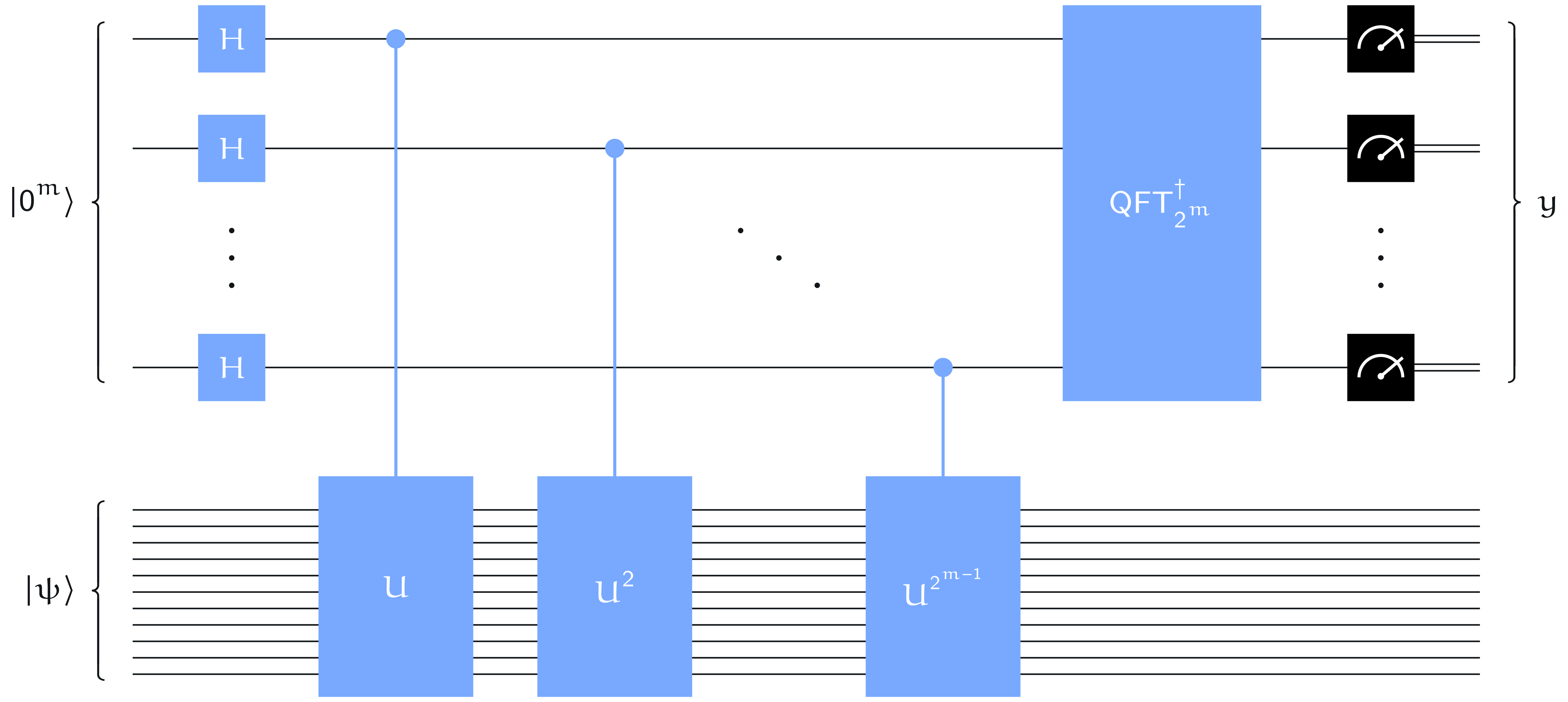
$$s_m = \sum_{k=1}^{m} (2k - 1) = m^2$$

Additional remarks:

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

Phase estimation procedure

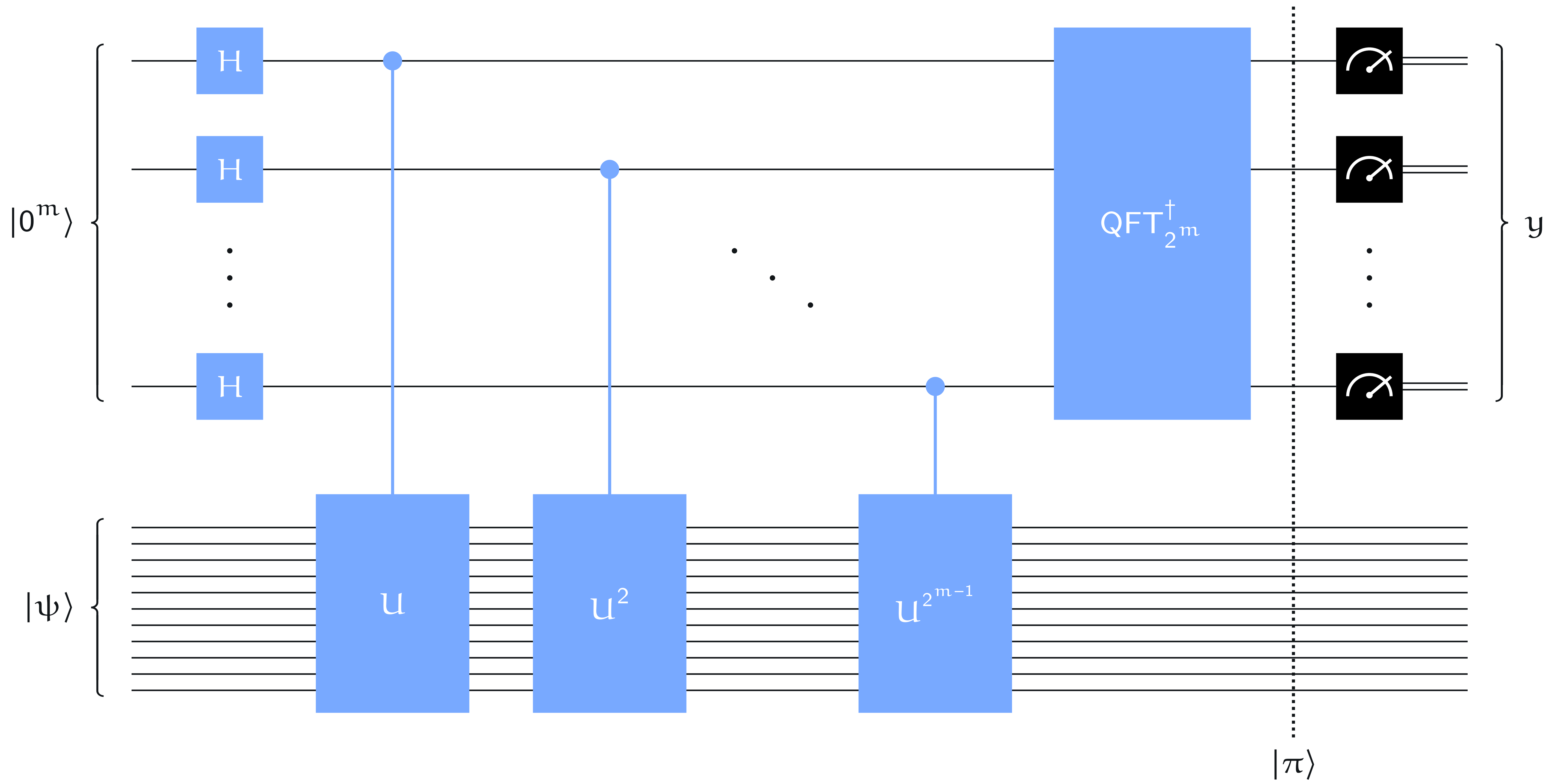
The general phase-estimation procedure, for any choice of m:



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



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

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

Phase estimation procedure

Best approximations

Suppose $y/2^m$ is the *best approximation* to θ:

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

Then the probability to measure y will relatively high:

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

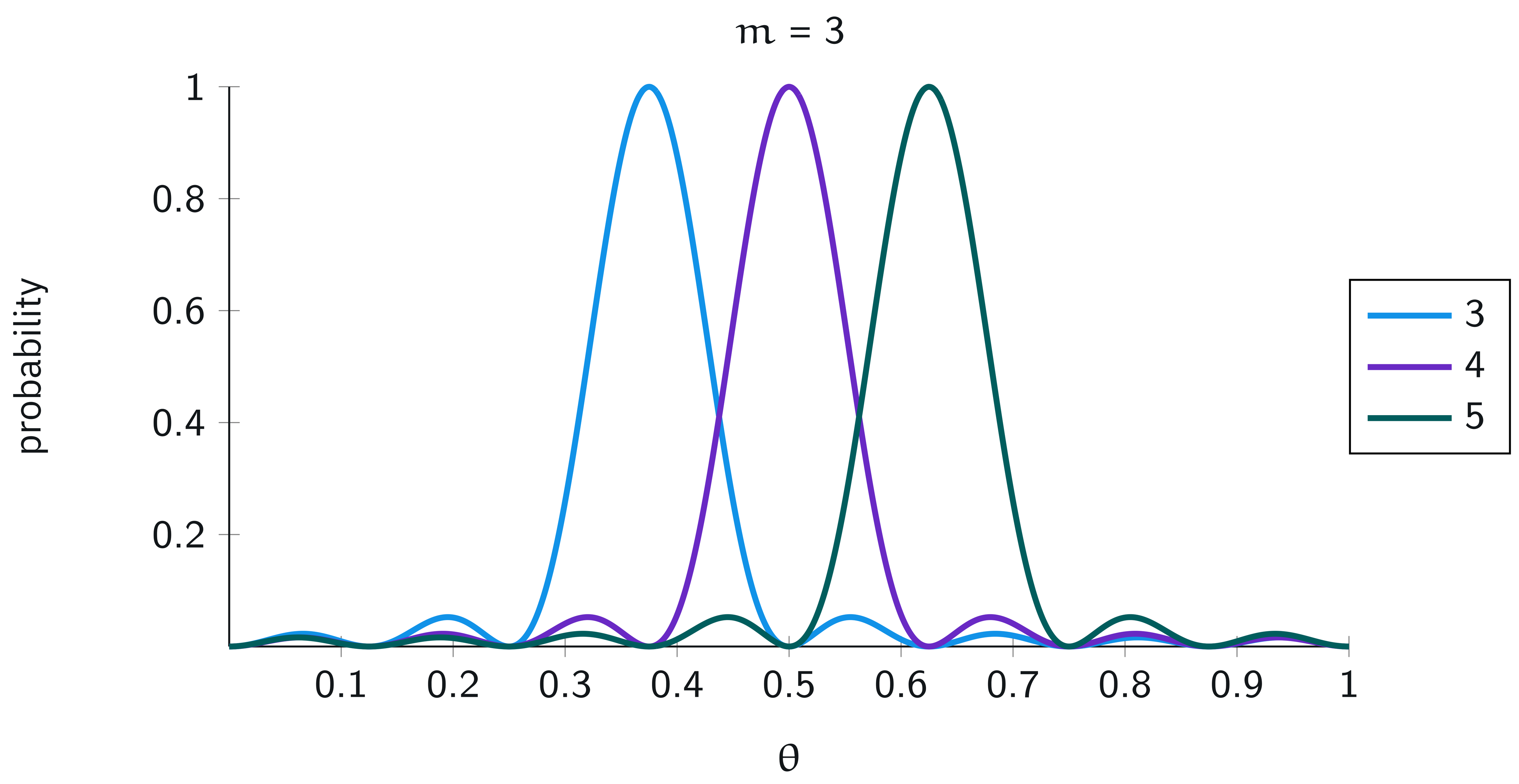
Worse approximations

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

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

Then the probability to measure y will be relatively low:

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



Phase estimation procedure

Best approximations

Suppose $y/2^m$ is the *best approximation* to θ:

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

Then the probability to measure y will relatively high:

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

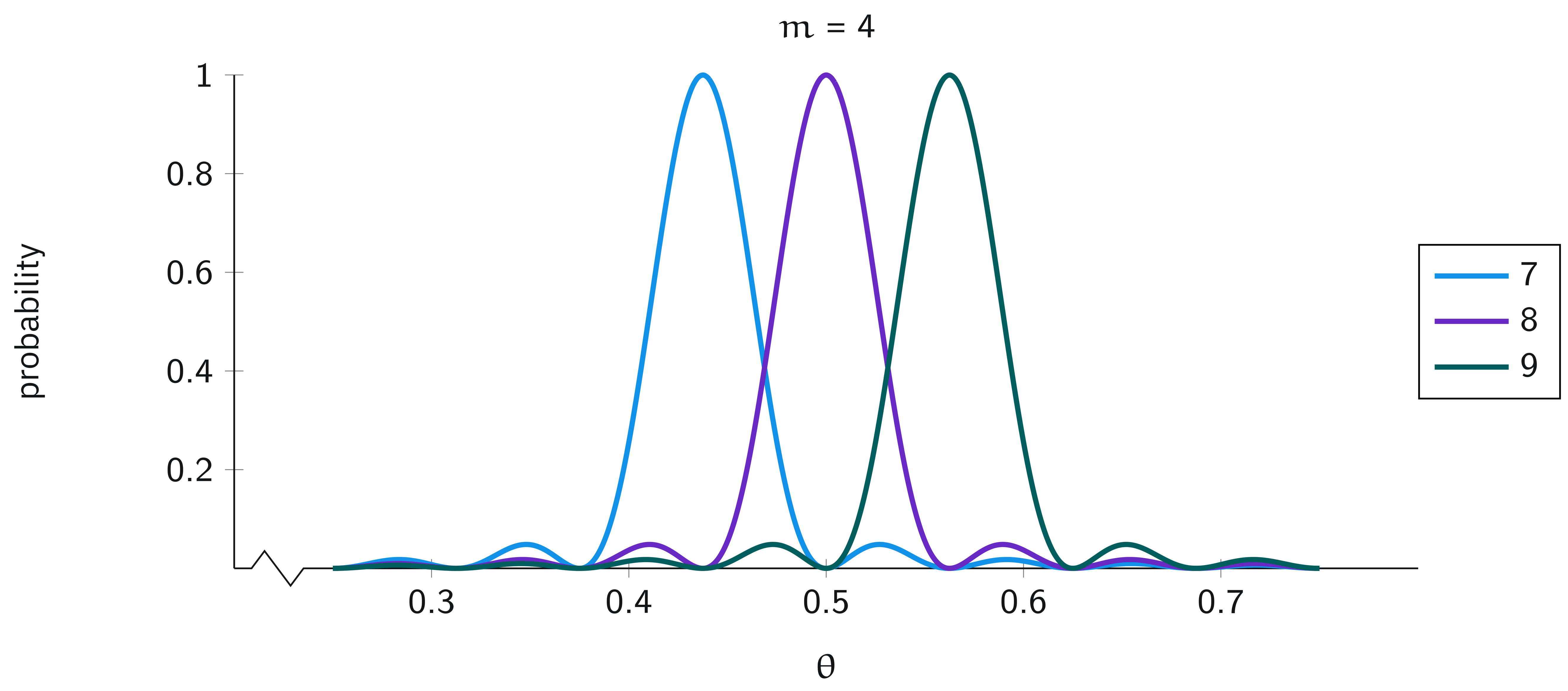
Worse approximations

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

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

Then the probability to measure y will be relatively low:

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



Phase estimation procedure

Best approximations

Suppose $y/2^m$ is the *best approximation* to θ:

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

Then the probability to measure y will relatively high:

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

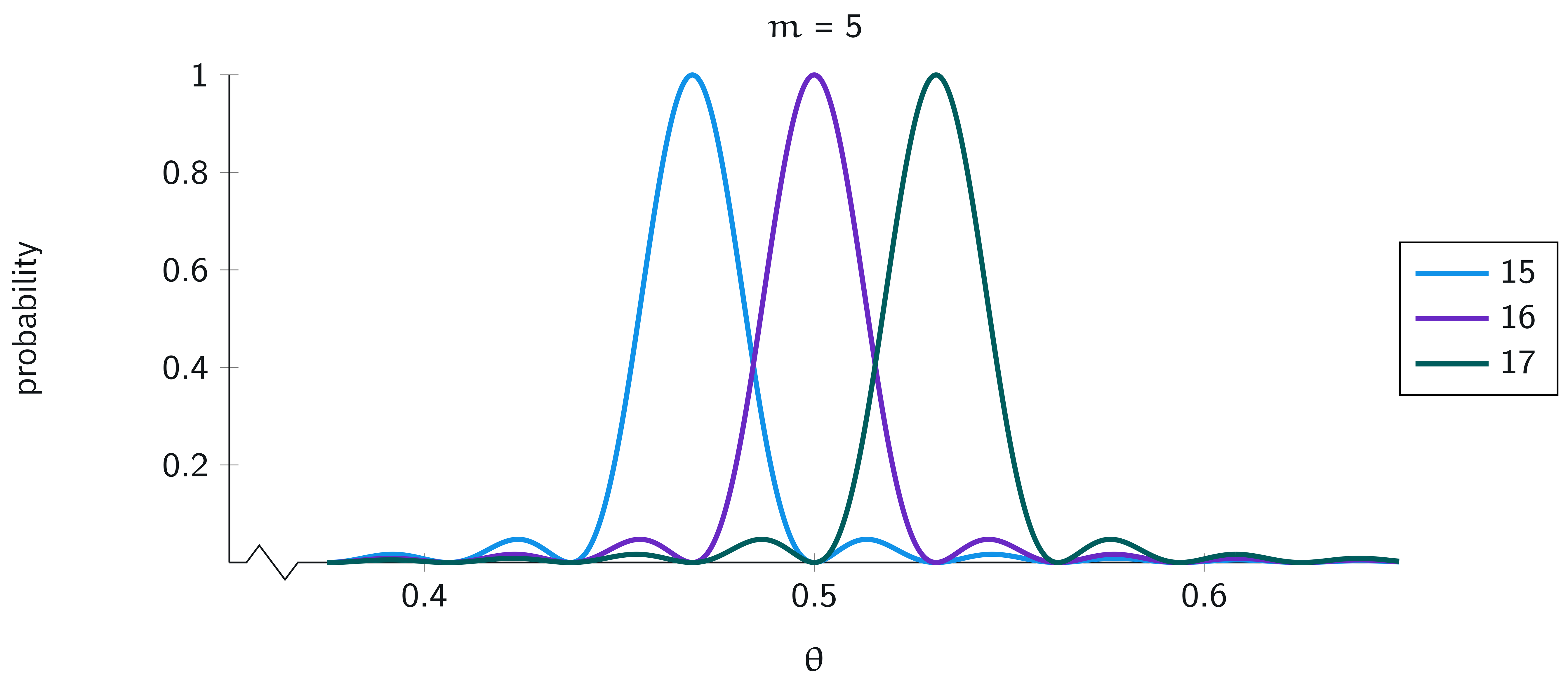
Worse approximations

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

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

Then the probability to measure y will be relatively low:

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



Phase estimation procedure

Best approximations

Suppose $y/2^m$ is the *best approximation* to θ:

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

Then the probability to measure y will relatively high:

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

Worse approximations

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

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

Then the probability to measure y will be relatively low:

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

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.)

The order-finding problem

For each positive integer N we define

$$\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$$

For instance, $\mathbb{Z}_1 = \{0\}$, $\mathbb{Z}_2 = \{0,1\}$, $\mathbb{Z}_3 = \{0,1,2\}$, and so on.

We can view arithmetic operations on $\mathbb{Z}_N$ as being defined modulo N.

Example

Let $N = 7$. We have $3 \cdot 5 = 15$, which leaves a remainder of 1 when divided by 7.

This is often expressed like this:

$$3 \cdot 5 \equiv 1 \pmod{7}$$

We can also simply write $3 \cdot 5 = 1$ when it's clear we're working in $\mathbb{Z}_7$.

The elements $a \in \mathbb{Z}_N$ that satisfy $\gcd(a, N) = 1$ are special.

$$\mathbb{Z}_N^* = \{a \in \mathbb{Z}_N : \gcd(a, N) = 1\}$$

Example

$$\mathbb{Z}_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$$

The order-finding problem

Fact

For every $a \in \mathbb{Z}_N^*$ there must exist a positive integer k such that $a^k = 1$. The smallest such k is called the *order* of a in $\mathbb{Z}_N^*$.

Example

For $N = 21$, these are the smallest powers for which this works:

$$\begin{array}{cccc} 1^1 = 1 & 5^6 = 1 & 11^6 = 1 & 17^6 = 1 \\ 2^6 = 1 & 8^2 = 1 & 13^2 = 1 & 19^6 = 1 \\ 4^3 = 1 & 10^6 = 1 & 16^3 = 1 & 20^2 = 1 \end{array}$$

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.

Order-finding by phase-estimation

To connect the order-finding problem to phase estimation, consider a system whose classical state set is $\mathbb{Z}_N$.

For a given element $a \in \mathbb{Z}_N^*$, define an operation as follows:

$$M_a |x\rangle = |ax\rangle \qquad (\text{for each } x \in \mathbb{Z}_N)$$

This is a *unitary operation* — but only because $\gcd(a, N) = 1$!

Example

Let $N = 15$ and $a = 2$. The operation M_a has this action:

$$\begin{array}{lll}
M_2|0\rangle = |0\rangle & M_2|5\rangle = |10\rangle & M_2|10\rangle = |5\rangle \\
M_2|1\rangle = |2\rangle & M_2|6\rangle = |12\rangle & M_2|11\rangle = |7\rangle \\
M_2|2\rangle = |4\rangle & M_2|7\rangle = |14\rangle & M_2|12\rangle = |9\rangle \\
M_2|3\rangle = |6\rangle & M_2|8\rangle = |1\rangle & M_2|13\rangle = |11\rangle \\
M_2|4\rangle = |8\rangle & M_2|9\rangle = |3\rangle & M_2|14\rangle = |13\rangle
\end{array}$$

Order-finding by phase-estimation

To connect the order-finding problem to phase estimation, consider a system whose classical state set is $\mathbb{Z}_N$.

For a given element $a \in \mathbb{Z}_N^*$, define an operation as follows:

$$M_a|x\rangle = |ax\rangle \qquad \text{(for each } x \in \mathbb{Z}_N\text{)}$$

This is a *unitary operation* — but only because $\gcd(a, N) = 1$!

Main idea

The *eigenvalues* of M_a are closely connected with the *order* of a.

By approximating certain eigenvalues with enough precision using phase estimation, we'll be able to compute the order.

Eigenvectors and eigenvalues

This is an eigenvector of M_a:

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

The associated eigenvalue is 1:

$$M_a|\psi_0\rangle = \frac{|a\rangle + |a^2\rangle + \cdots + |a^r\rangle}{\sqrt{r}} = \frac{|a\rangle + \cdots + |a^{r-1}\rangle + |1\rangle}{\sqrt{r}} = |\psi_0\rangle$$

To identify more eigenvectors, first recall that

$$\omega_r = e^{2\pi i/r}$$

This is another eigenvector of M_a:

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

Eigenvectors and eigenvalues

$$
\begin{aligned}
M_a|\psi_1\rangle &= \frac{|a\rangle + \omega_r^{-1}|a^2\rangle + \cdots + \omega_r^{-(r-1)}|a^r\rangle}{\sqrt{r}}\\
&= \frac{\omega_r|1\rangle + |a\rangle + \omega_r^{-1}|a^2\rangle + \cdots + \omega_r^{-(r-2)}|a^{r-1}\rangle}{\sqrt{r}}\\
&= \omega_r\left(\frac{|1\rangle + \omega_r^{-1}|a\rangle + \omega_r^{-2}|a^2\rangle + \cdots + \omega_r^{-(r-1)}|a^{r-1}\rangle}{\sqrt{r}}\right)\\
&= \omega_r|\psi_1\rangle
\end{aligned}
$$

Additional eigenvectors can be identified by similar reasoning...

For each $j \in \{0, \ldots, r-1\}$, this is an eigenvector of M_a:

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

$$
M_a|\psi_j\rangle = \omega_r^j|\psi_j\rangle
$$

A convenient eigenvector

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

$$M_a|\psi_1\rangle = \omega_r|\psi_1\rangle = e^{2\pi i \frac{1}{r}}|\psi_1\rangle$$

Suppose we're given $|\psi_1\rangle$ as a quantum state. We can attempt to learn r as follows:

1. Perform phase estimation on the state $|\psi_1\rangle$ and a quantum circuit implementing M_a. The outcome is an approximation $y/2^m \approx 1/r$.
2. Output $2^m/y$ rounded to the nearest integer:

$$\text{round}\left(\frac{2^m}{y}\right) = \left\lfloor \frac{2^m}{y} + \frac{1}{2} \right\rfloor$$

How much precision do we need to correctly determine r?

$$\left|\frac{y}{2^m} - \frac{1}{r}\right| \le \frac{1}{2N^2} \qquad \Longrightarrow \qquad \text{round}\left(\frac{2^m}{y}\right) = r$$

Choosing $m = 2\lg(N) + 1$ in phase estimation makes such an approximation likely.

A random eigenvector

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

$$M_a|\psi_j\rangle = \omega_r^j|\psi_1\rangle = e^{2\pi i \frac{j}{r}}|\psi_1\rangle$$

Suppose we're given $|\psi_j\rangle$ as a quantum state for a *random choice* of $j \in \{0, \ldots, r-1\}$. We can attempt to learn j/r as follows:

1. Perform phase estimation on the state $|\psi_j\rangle$ and a quantum circuit implementing M_a. The outcome is an approximation $y/2^m \approx j/r$.
2. Among the fractions u/v in lowest terms satisfying $u, v \in \{0, \ldots, N-1\}$ and $v \neq 0$, output the one closest to $y/2^m$. This can be done efficiently using the *continued fraction algorithm.*

How much precision do we need to correctly determine $u/v = j/r$?

$$\left|\frac{y}{2^m} - \frac{j}{r}\right| \leq \frac{1}{2N^2} \qquad \Rightarrow \qquad \frac{u}{v} = \frac{j}{r}$$

Choosing $m = 2\lg(N) + 1$ for phase estimation makes such an approximation likely.
We might get unlucky: j could have common factors with r.

A random eigenvector

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

$$M_a|\psi_j\rangle = \omega_r^j|\psi_1\rangle = e^{2\pi i \frac{j}{r}}|\psi_1\rangle$$

Suppose we're given $|\psi_j\rangle$ as a quantum state for a *random choice* of $j \in \{0, \ldots, r-1\}$. We can attempt to learn j/r as follows:

1. Perform phase estimation on the state $|\psi_j\rangle$ and a quantum circuit implementing M_a. The outcome is an approximation $y/2^m \approx j/r$.
2. Among the fractions u/v in lowest terms satisfying $u, v \in \{0, \ldots, N-1\}$ and $v \neq 0$, output the one closest to $y/2^m$. This can be done efficiently using the *continued fraction algorithm.*

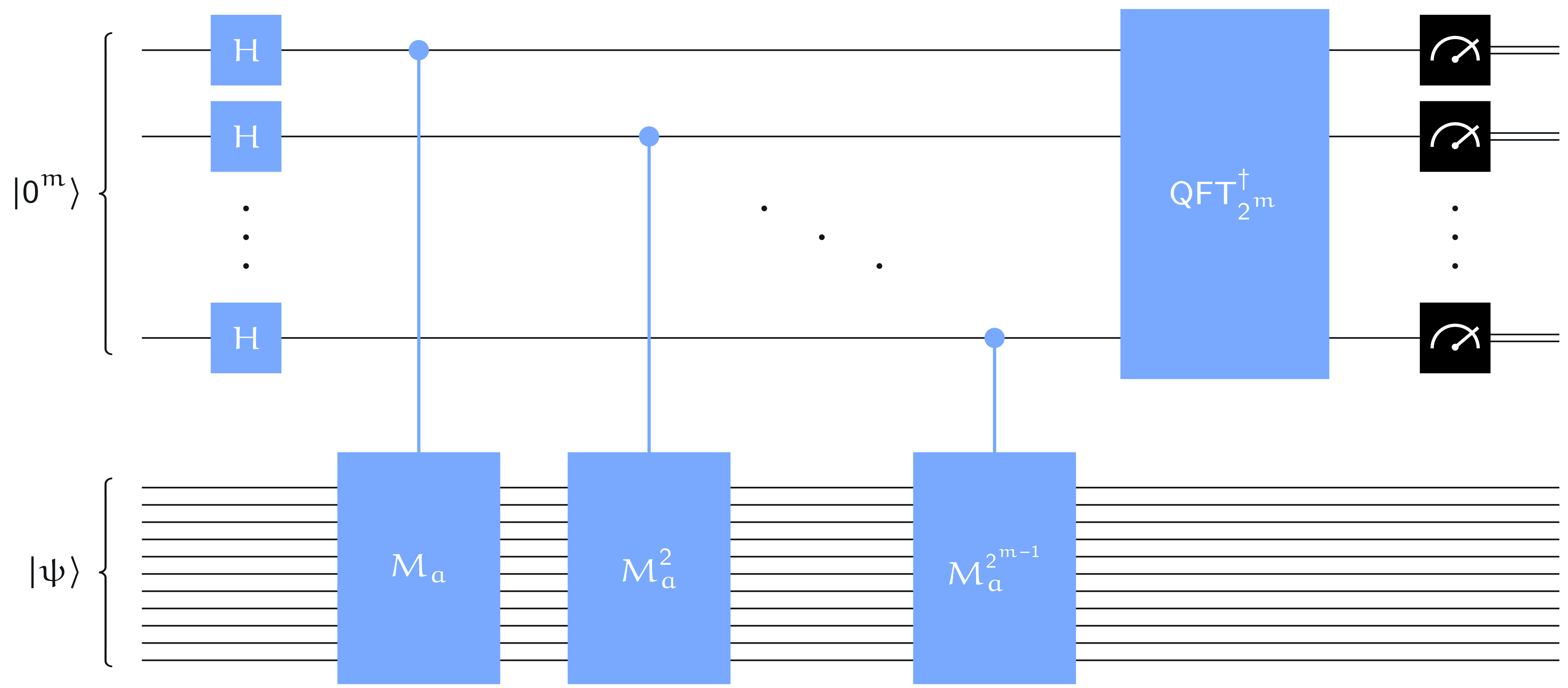
How much precision do we need to correctly determine $u/v = j/r$?

$$\left|\frac{y}{2^m} - \frac{j}{r}\right| \leq \frac{1}{2N^2} \qquad \Rightarrow \qquad \frac{u}{v} = \frac{j}{r}$$

If we can draw *independent samples,* for $j \in \{0, \ldots, r-1\}$ is chosen uniformly, we can recover r with high probability by computing the *least common multiple* of the values of v we observed.

Implementation

To find the order of $a \in \mathbb{Z}_N^*$, we apply phase estimation to the operation M_a. Let's measure the cost as a function of $n = \lg(N)$.



Cost for each controlled unitary

Using the techniques from Lesson 6, we can implement M_a at cost $O(n^2)$.

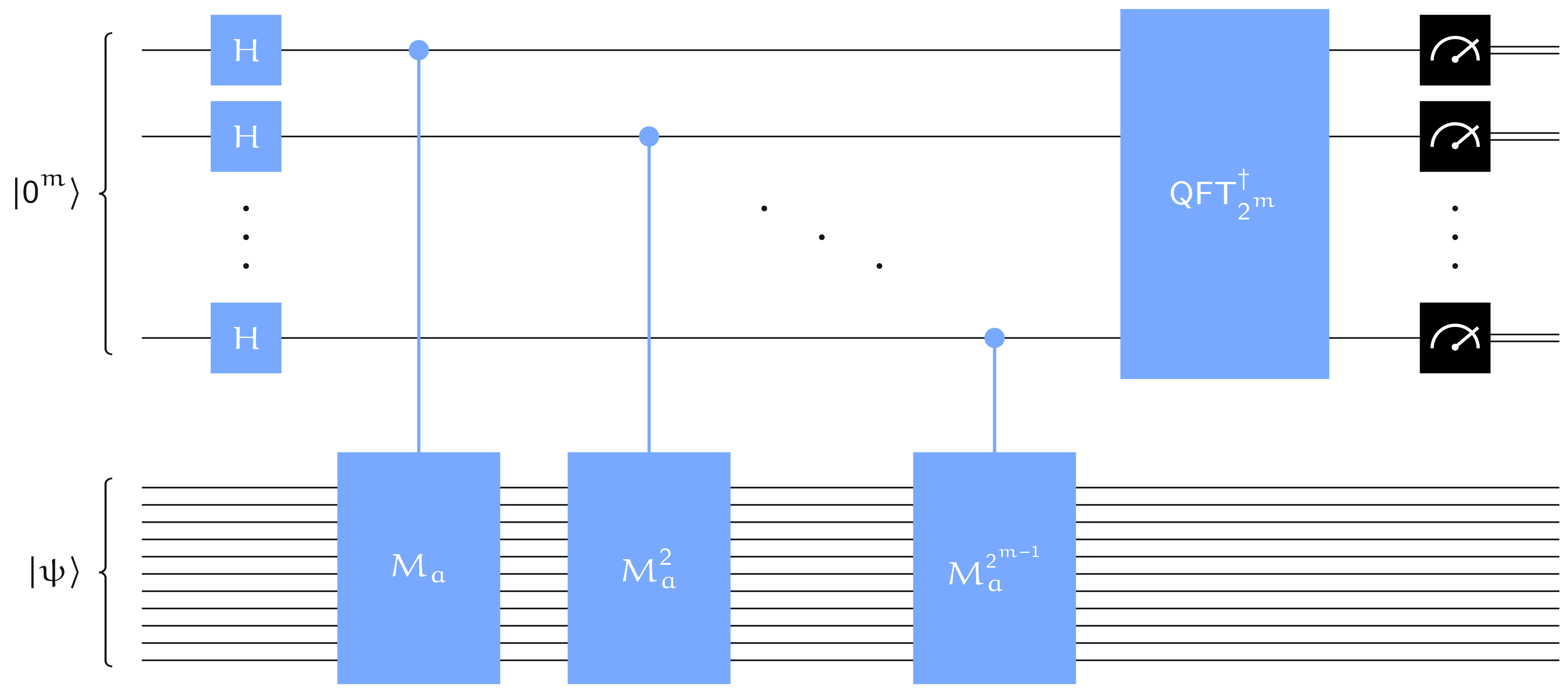
We need to implement M_a^k for each $k = 1, 2, 4, 8, \ldots, 2^{m-1}$. Each M_a^k can be implemented as follows:

Compute $b = a^k \pmod N$.
Use a circuit for M_b.

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

Implementation

To find the order of $a \in \mathbb{Z}_N^*$, we apply phase estimation to the operation M_a. Let's measure the cost as a function of $n = \lg(N)$.

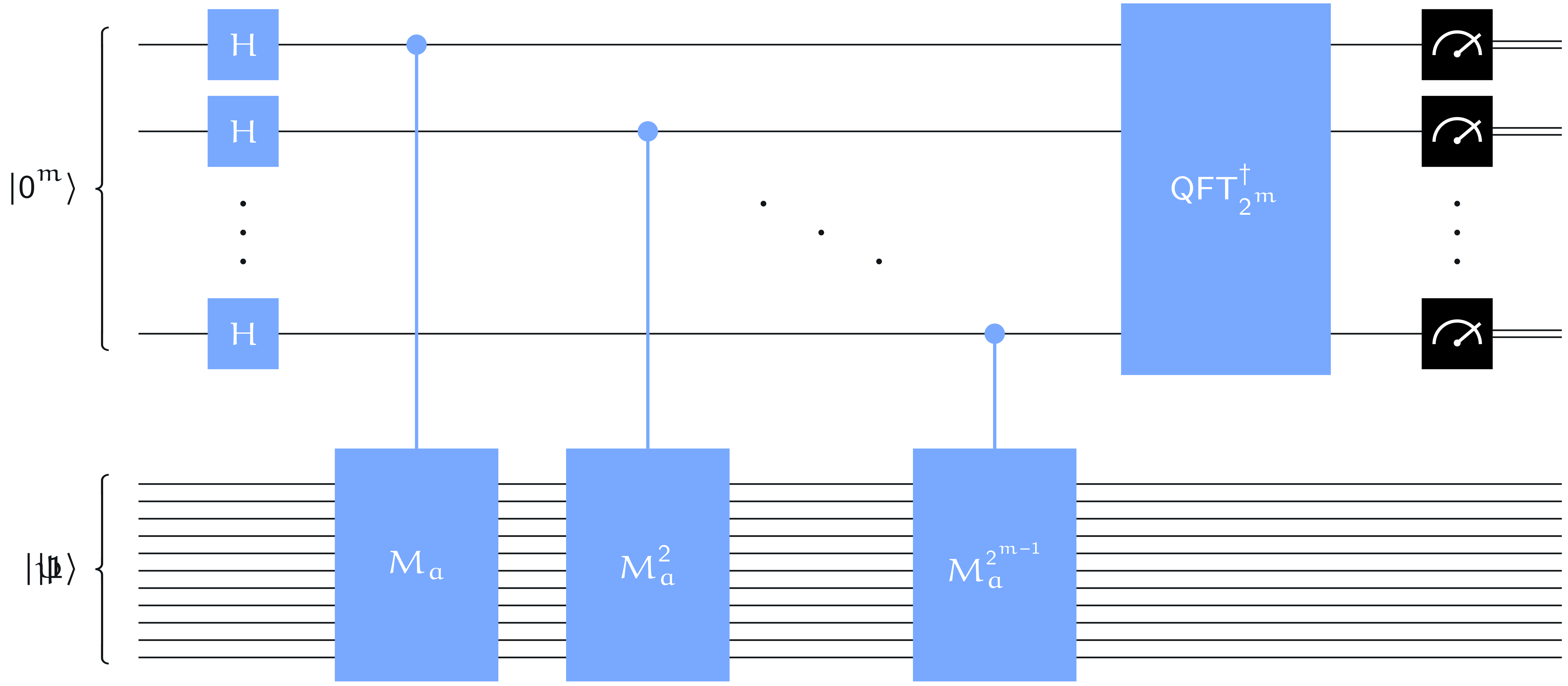


Cost for phase estimation

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

Total cost: $O(n^3)$

Implementation



Remaining issue: getting one of the eigenvectors $|\psi_0\rangle, \ldots, |\psi_{r-1}\rangle$.

Solution: replace the eigenvector $|\psi\rangle$ with the state $|1\rangle$.

This works because of the following equation:

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

The outcome is the same as if we chose $j \in \{0, 1, \ldots, r-1\}$ uniformly and used $|\psi\rangle = |\psi_j\rangle$.

Factoring through order-finding

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

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.

Main idea

1. By the definition of the order, we know that $a^r \equiv 1 \pmod{N}$.

$$a^r \equiv 1 \pmod{N} \qquad \Longleftrightarrow \qquad N \text{ divides } a^r - 1$$

2. If r is even, then

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

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