

Lecture 3 - Shor's Algorithm I - QFT and QPE

Roadmap - (1) Qubits & Quantum states

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}; |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}; X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$|4\rangle = a|0\rangle + b|1\rangle$$

$$\langle 0|4\rangle = a; \langle 1|4\rangle = b;$$

$$\text{Prob(meas 0)} = \|a\|^2; \text{Prob(meas 1)} = \|b\|^2$$

$$\|a\|^2 + \|b\|^2 = 1 \Rightarrow 2 \text{ implications}$$

(1) Operations on quantum states need to preserve norm to 1

$$\rightarrow \text{Norm-preserving matrices} = \text{unitary} (\Rightarrow U^+ = U^{-1})$$

$$\Rightarrow U^+ U = U U^+ = I$$

(2) For a single qubit, can think of ^{unitary} gates as rotations on the surface of the Bloch sphere.

(3) Eigenvalues and eigenvectors of unitary matrices are special.

$$(a) U|x\rangle = \lambda_x|x\rangle$$

$$\Rightarrow \langle x|U^+ = \langle x|\lambda_x^*$$

$$\langle x|x\rangle = 1 = \langle x|U^+U|x\rangle = \langle x|\lambda_x^*\lambda_x|x\rangle = |\lambda_x|^2 \langle x|x\rangle = |\lambda_x|^2$$

$$\Rightarrow |\lambda_x|^2 = 1 \Rightarrow \lambda_x = e^{i\theta} \text{ for some } \theta$$

\Rightarrow eigenvalues of U are of the form $e^{i\theta}$

$$(b) U|x\rangle = \lambda_x|x\rangle \text{ if } \lambda_x \neq \lambda_y, \text{ then}$$

$$U|y\rangle = \lambda_y|y\rangle \quad \langle x|y\rangle = \langle x|U^+U|y\rangle = \lambda_x^* \lambda_y \langle x|y\rangle$$

$$\lambda_x \neq \lambda_y \Rightarrow \langle x|y\rangle = 0$$

eigvecs of diff eigenvals
are orthonormal

$$\Rightarrow \langle x|y\rangle (1 - \lambda_x^* \lambda_y) = 0$$

$$\text{multiply by } \lambda_x \Rightarrow \langle x|y\rangle (\lambda_y - \lambda_x) = 0$$

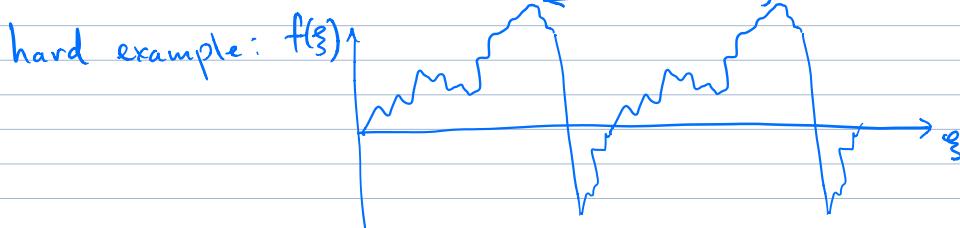
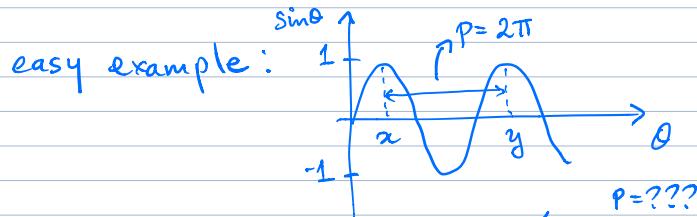
$$\text{and use } |\lambda_x|^2 = 1 \Rightarrow \langle x|y\rangle (\lambda_y - \lambda_x) = 0$$

- Also covered - Deutsch-Josza algorithm
 - constant / balanced function in one shot
- Grover's algorithm
 - unstructured search in N items with $O(\sqrt{N})$

Today: Preliminaries for Shor's algorithm

famous algorithm

Problem: given a function that is periodic, find its period.
strict definition: $f(x) = f(y)$ for $x \neq y$ iff $|x - y| = kP$



classically: $O(\exp cn^{1/3}(\log n)^{2/3})$
 p has n bits

quantum: Shor's algorithm : $O(n^2(\log n)(\log \log n))$
little faster than $O(n^3)$

Reason why this works: (1) quantum Fourier transform
(2) modular exponentiation

Implication: difficulty of factoring on a classical computer is basis for security (more tomorrow)

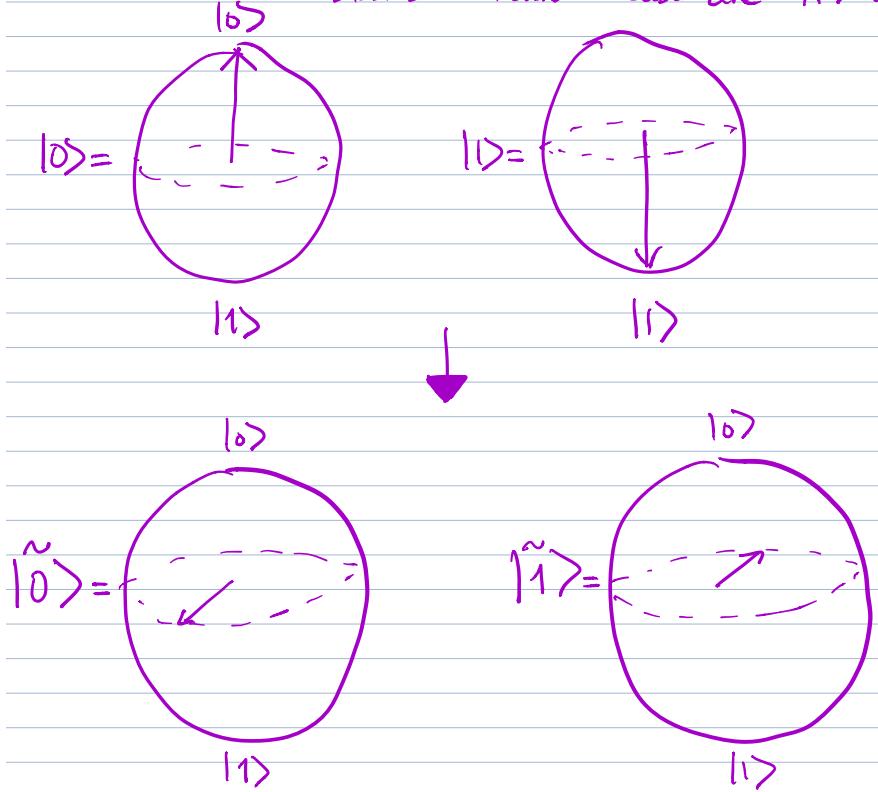
Today - Quantum Fourier Transform,
Quantum Phase Estimation

(Shor's algorithm is really QPE in disguise)

QFT is effectively a change of basis from the computational basis to a Fourier basis.

e.g.: 1 qubit: states in computational basis are $|0\rangle$ and $|1\rangle$

states in Fourier basis are $|+\rangle$ and $|-\rangle$



multiple qubits: go to Qiskit demo

- notice that we are going from basis on the two poles of the Bloch sphere to a basis on the equatorial plane.

Building the quantum circuit that applies QFT

(1) Show QFT rigorously

(2) Show circuit to implement QFT expression

(1) n qubits $\Rightarrow 2^n$ basis states. Define $N = 2^n$. Then,

$$\begin{aligned} |\tilde{x}\rangle &= \text{QFT } |x\rangle \\ &\stackrel{\substack{\uparrow \\ \text{Fourier basis}}}{=} \stackrel{\substack{\uparrow \\ \text{Computational basis}}}{=} \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{2\pi i}{N} xy} |y\rangle \quad [\text{analogous to inverse discrete Fourier transform}] \end{aligned}$$

e.g.: 1-qubit case $[\Rightarrow N=2]$

$$\begin{aligned} |\tilde{0}\rangle &= \frac{1}{\sqrt{2}} \sum_{y=0}^1 e^{\frac{2\pi i}{2} (0)y} |y\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^1 |y\rangle \\ &= \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \end{aligned}$$

$$\begin{aligned} |\tilde{1}\rangle &= \frac{1}{\sqrt{2}} \sum_{y=0}^1 e^{\frac{2\pi i}{2} (1)y} |y\rangle = \frac{1}{\sqrt{2}} \left(e^{\frac{2\pi i}{2} (0)} |0\rangle + e^{\frac{2\pi i}{2} (1)} |1\rangle \right) \\ &= \frac{1}{\sqrt{2}} (|0\rangle + (-1)|1\rangle) \\ &= \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \end{aligned}$$

A note on notation: for multiple qubits, e.g. $n=3$,

$$|\tilde{x}\rangle = \frac{1}{\sqrt{8}} \sum_{y=0}^7 e^{\frac{2\pi i}{8} xy / 2^3} |y\rangle \quad \hookrightarrow \text{e.g. } |y\rangle = |4\rangle \Leftrightarrow |100\rangle$$

$$4 = 2^2(1) + 2^1(0) + 2^0(0)$$

$$\frac{4}{2^3} = \frac{2^2(1) + 2^1(0) + 2^0(0)}{2^3}$$

$$\begin{aligned}
 |\tilde{x}\rangle &= \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{2\pi i x y}{N}} |y\rangle \quad y = [y_0, y_1, \dots, y_{n-1}] \\
 &= \frac{1}{\sqrt{N}} \sum_{y_0=0}^1 \sum_{y_1=0}^1 \dots \sum_{y_{n-1}=0}^1 e^{\frac{2\pi i x}{N} \sum_{k=1}^n y_k 2^{n-k}} |y_k\rangle \\
 &= \frac{1}{\sqrt{N}} \sum_{y_0, y_1, \dots, y_{n-1}} \bigotimes_{k=1}^n e^{\frac{2\pi i x}{N} 2^{n-k} y_k} |y_k\rangle \\
 &= \frac{1}{\sqrt{N}} \bigotimes_{k=1}^n \left[|0\rangle + e^{\frac{2\pi i x}{N} 2^{n-k}} |1\rangle \right] \\
 &= \frac{1}{\sqrt{N}} \bigotimes_{k=1}^n \left[|0\rangle + e^{\frac{2\pi i x}{2^k}} |1\rangle \right]
 \end{aligned}$$

$$k=1 \text{ term: } |0\rangle + e^{\frac{2\pi i x}{2}} |1\rangle$$

$$k=2 \text{ term: } |0\rangle + e^{\frac{2\pi i x}{4}} |1\rangle$$

$$\text{notice: } x = [x_0, x_1, x_2, \dots, x_{n-1}]$$

$$\frac{x}{2} = 0.x_1 x_2 \dots x_{n-1}$$

$$\frac{x}{4} = 00x_1 x_2 \dots x_{n-2}$$

Final form:

$$\frac{1}{\sqrt{N}} \left(|0\rangle + e^{\frac{2\pi i x}{2}} |1\rangle \right) \otimes \left(|0\rangle + e^{\frac{2\pi i x}{4}} |1\rangle \right) \otimes \dots$$

went from

$$|x_0, x_1, \dots, x_{n-1}\rangle$$

Example:

$$n = 3 \text{ qubits} \Rightarrow N = 2^3 = 8$$

$$|\alpha\rangle = |5\rangle$$
$$\text{QFT}|\alpha\rangle = \frac{1}{\sqrt{8}} \left(|0\rangle + e^{2\pi i \frac{5}{2}} |1\rangle \right) \otimes \left(|0\rangle + e^{2\pi i \frac{5}{4}} |1\rangle \right)$$
$$\otimes \left(|0\rangle + e^{2\pi i \frac{5}{8}} |1\rangle \right)$$

$$\text{Notice: } 2\pi i \left(\frac{5}{2}\right) = 2\pi i \left(\frac{2^2}{2} + \frac{1}{2}\right)$$
$$= 2\pi i \left(2 + \frac{1}{2}\right)$$

since $e^{2\pi i z} = 1$ for any integer z ,

$$e^{2\pi i \left(\frac{5}{2}\right)} = e^{2\pi i \left(2 + \frac{1}{2}\right)} = e^{2\pi i \left(\frac{1}{2}\right)} = e^{\pi i} = -1$$

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

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

let's write $y = \sum_{k=1}^{n-k} y_k 2^k$

$$y = y_1 \dots y_n \\ = 2^{n-1} y_1 + \dots + 2^0 y_n$$

then $y/2^n = \sum_{k=1}^n y_k / 2^k$ and we have

$$|\tilde{x}\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i x \sum_{k=1}^n y_k / 2^k} |y_1 y_2 \dots y_n\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \prod_{k=1}^n e^{2\pi i x y_k / 2^k} |y_1 y_2 \dots y_n\rangle$$

remember, $\sum_{y=0}^{N-1} = \sum_{y_1=0}^1 \sum_{y_2=0}^1 \dots \sum_{y_n=0}^1$

$$\begin{aligned} |\tilde{x}\rangle &= \frac{1}{\sqrt{N}} \left(|0\rangle + e^{\frac{2\pi i x}{2^1}} |1\rangle \right) \otimes \left(|0\rangle + e^{\frac{2\pi i x}{2^2}} |1\rangle \right) \otimes \\ &\quad \dots \left(|0\rangle + e^{\frac{2\pi i x}{2^n}} |1\rangle \right) \end{aligned}$$

Notice that we went from

$$|x\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \dots \otimes |x_n\rangle$$

to

$$|\tilde{x}\rangle = \frac{1}{\sqrt{N}} \left(|0\rangle + e^{\frac{2\pi i x}{2^1}} |1\rangle \right) \otimes \left(|0\rangle + e^{\frac{2\pi i x}{2^2}} |1\rangle \right) \otimes \dots \otimes \left(|0\rangle + e^{\frac{2\pi i x}{2^n}} |1\rangle \right)$$

The Quantum Circuit that implements QFT

Notice that we went from

$$|\alpha\rangle = |\alpha_1\rangle \otimes |\alpha_2\rangle \otimes \dots \otimes |\alpha_n\rangle \text{ to}$$

$$|\tilde{\alpha}\rangle = \frac{1}{\sqrt{N}} (|0\rangle + e^{\frac{2\pi i \alpha_1}{2^n}} |1\rangle) \otimes (|0\rangle + e^{\frac{2\pi i \alpha_2}{2^n}} |1\rangle) \otimes \dots \otimes (|0\rangle + e^{\frac{2\pi i \alpha_n}{2^n}} |1\rangle)$$

each qubit went from $|\alpha_k\rangle$ to $|0\rangle + e^{\frac{2\pi i \alpha_k}{2^n}} |1\rangle$.

Two observations:

(1) $|\tilde{\alpha}\rangle$ contains terms like

$$\begin{aligned} &|00\dots 00\rangle \\ &e^{\frac{2\pi i \alpha_1}{2^n}} |00\dots 01\rangle \\ &e^{\frac{2\pi i \alpha_2}{2^n}} |00\dots 10\rangle \\ &e^{\frac{2\pi i \alpha_n}{2^n}} |10\dots 00\rangle \end{aligned}$$

$$e^{2\pi i \left[\frac{\alpha_1}{2} + \frac{\alpha_2}{2^2} + \dots + \frac{\alpha_n}{2^n} \right]}$$

(2) $e^{\underbrace{\dots}_{2\pi i \frac{\alpha_1}{2^1} + 2\pi i \frac{\alpha_2}{2^2} + 2\pi i \frac{\alpha_3}{2^3} + \dots + 2\pi i \frac{\alpha_n}{2^n}}} |1111\dots 1111\rangle$

$$\downarrow e^{\frac{2\pi i \alpha_1}{2^1}} e^{\frac{2\pi i \alpha_2}{2^2}} e^{\frac{2\pi i \alpha_3}{2^3}} \dots e^{\frac{2\pi i \alpha_n}{2^n}}$$

Hints:

- phase is qubit-dependent
- need to add up more components with more "1"s

Two ingredients needed:

$$(1) H |\alpha_k\rangle = \begin{cases} \xrightarrow{x_k=0} (|0\rangle + |1\rangle)/\sqrt{2} \\ \xrightarrow{x_k=1} (|0\rangle - |1\rangle)/\sqrt{2} \end{cases}$$

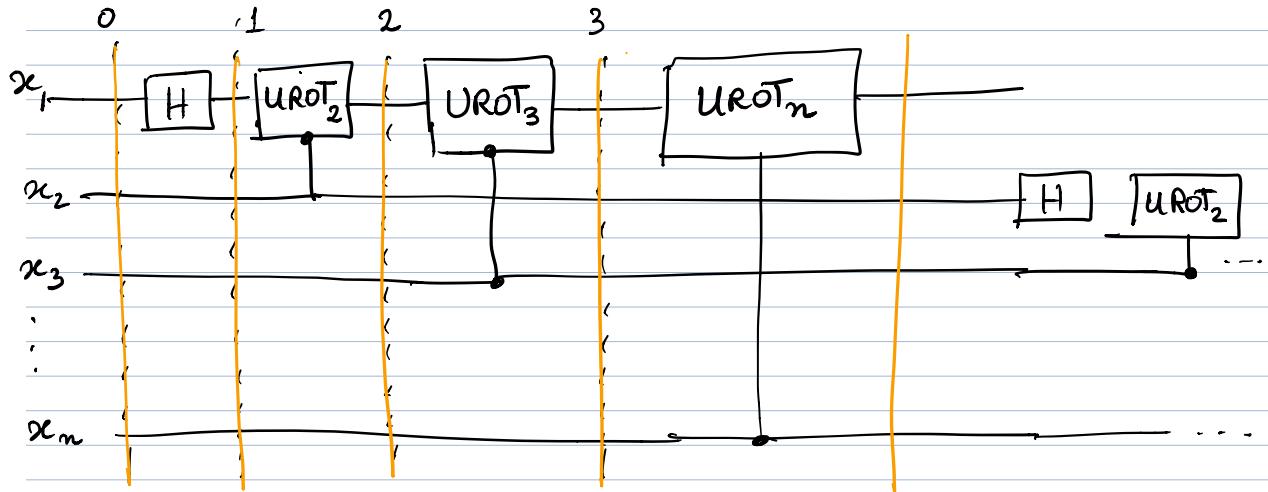
$$= (|0\rangle + e^{\frac{\pi i \alpha_k}{2}} |1\rangle)/\sqrt{2}$$

$$= e^{\frac{2\pi i \alpha_k}{2}}$$

$$(2) UROT_k |\alpha_j\rangle = e^{\frac{2\pi i \alpha_j}{2^k}} |\alpha_j\rangle$$

$$\Rightarrow UROT_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i \alpha_j}{2^k}} \end{bmatrix}$$

\uparrow applies phase $e^{\frac{2\pi i \alpha_j}{2^k}}$



Step 0: $|x_1 x_2 \dots x_n\rangle$

$$\text{step 1: } [|0\rangle + e^{\frac{2\pi i}{2} x_1} |1\rangle] \otimes |x_2 \dots x_n\rangle$$

$$\text{step 2: } [|0\rangle + e^{\frac{2\pi i}{2^2} x_2} e^{\frac{2\pi i}{2^1} x_1} |1\rangle] \otimes \dots$$

$$\text{step 3: } [|0\rangle + e^{\frac{2\pi i}{2^3} x_3} e^{\frac{2\pi i}{2^2} x_2} e^{\frac{2\pi i}{2^1} x_1} |1\rangle] \otimes \dots$$

$$\text{step } n: [|0\rangle + \underbrace{e^{\frac{2\pi i}{2^n} x_n} \dots e^{\frac{2\pi i}{2^1} x_1}}_{\text{in curly braces}} |1\rangle] \otimes \dots$$

$$\exp \left[2\pi i \left(\frac{x_n}{2^n} + \frac{x_{n-1}}{2^{n-1}} + \dots + \frac{x_1}{2^1} \right) \right]$$

$$\text{recall: } x = 2^{n-1}x_1 + 2^{n-2}x_2 + \dots + 2^0 x_n$$

$$\Rightarrow \frac{x_n}{2^n} + \dots + \frac{x_1}{2^1} = \frac{x}{2^n}$$

$$\Rightarrow \text{term above is } \exp \left[2\pi i \frac{x}{2^n} \right]$$

$$\Rightarrow \text{after step } n: [|0\rangle + e^{\frac{2\pi i}{2^n} x} |1\rangle] \otimes |x_2 x_3 \dots x_n\rangle$$

↗
reversed order from derived form, but OK otherwise.

Part II: Quantum Phase Estimation

- Here, we will use QFT to do a very useful thing.

Problem: Recall that a unitary matrix has eigenvalues of the form $e^{i\theta}$ and that it has eigenvectors that form an orthonormal basis

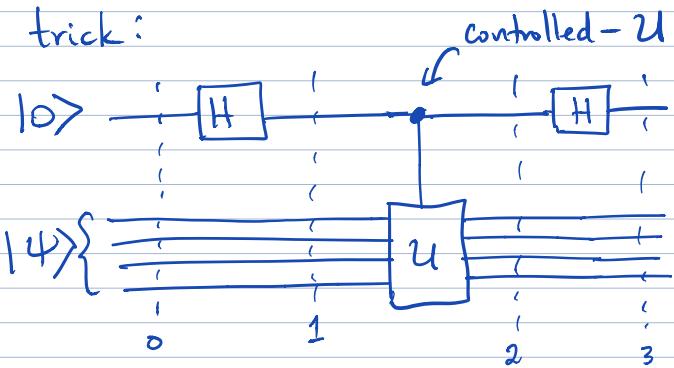
$$U|\psi\rangle = e^{i\theta_4}|4\rangle$$

Can we extract θ_4 given the ability to prepare $|4\rangle$?

Solution: Yes. Use QPE.

Why do we care? - Hamiltonian evolution operator is unitary
→ implications for q. simulation.

QPE trick:



step 0: $|0\rangle|4\rangle$

step 1: $\frac{1}{\sqrt{2}}(|0\rangle|4\rangle + |1\rangle|4\rangle)$

step 2: $\frac{1}{\sqrt{2}}(|0\rangle|4\rangle + |1\rangle e^{i\theta_4}|4\rangle)$

$$\text{step 3: } \frac{1}{2} [(|0\rangle + |1\rangle)|4\rangle + e^{i\theta_4}(|0\rangle - |1\rangle)|4\rangle]$$

$$= \frac{1}{2} [|0\rangle(1 + e^{i\theta_4}) + |1\rangle(1 - e^{i\theta_4})] |4\rangle$$

measure qubit 0:

$$\text{prob } \left| \frac{1+e^{i\theta_4}}{2} \right|^2 \Rightarrow \text{measure 0}$$

$$\text{prob } \left| \frac{1-e^{i\theta_4}}{2} \right|^2 \Rightarrow \text{measure 1}$$

← almost $\frac{1}{2}$ each but
with small shift

$$\text{if } \theta_4 > 0, \text{ prob}[0] = \cos^2\left(\frac{\theta_4}{2}\right)$$

$$\text{prob}[1] = \sin^2\left(\frac{\theta_4}{2}\right) \sim$$

To measure θ precisely using this bit of information, need to do lots of measurements.

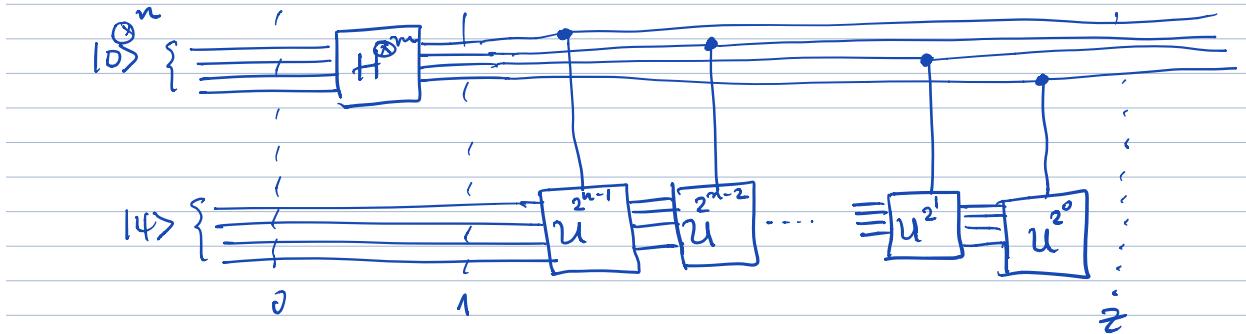
$$\text{eg: } \theta_4 = 1^\circ \Rightarrow \text{prob}[0], \text{prob}[1] = \{0.9999, 7.615 \times 10^{-5}\}$$

$$\theta_4 = 10^\circ \Rightarrow \sim = \{0.9924, 0.007596\}$$



↑ not a good idea to try to measure with such low precision.

Better solution: use multiple qubits to measure the phase.



step 0: $|0\rangle^{\otimes n} |4\rangle$

step 1: $\frac{1}{(\sqrt{2})^n} (|0\rangle + |1\rangle)^{\otimes n} |4\rangle$

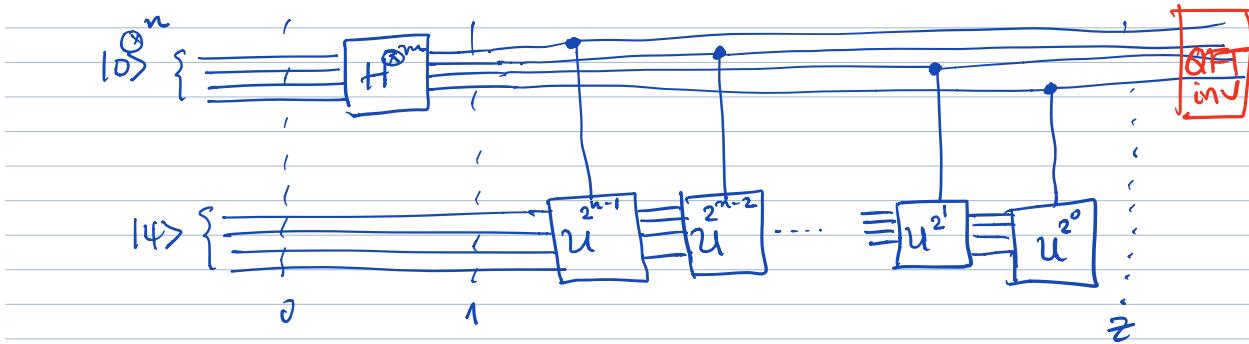
$$\begin{aligned} \text{Before proceeding, note: } u^{2^x} |4\rangle &= u^{2^{x-1}} u |4\rangle \\ &= u^{2^{x-1}} e^{i\theta_4} |4\rangle \\ &\vdots \\ &= e^{i\theta_4 2^x} |4\rangle \end{aligned}$$

step 2: $\left(\frac{1}{\sqrt{2}}\right)^n (|0\rangle + e^{i\theta_4 2^{m-1}} |1\rangle) \otimes (|0\rangle + e^{i\theta_4 2^{m-2}} |1\rangle) \otimes \dots (|0\rangle + e^{i\theta_4 2^0} |1\rangle)$

vs QFT:

$$\tilde{|x\rangle} = \frac{1}{\sqrt{2^n}} (|0\rangle + e^{\frac{2\pi i x}{2^1}} |1\rangle) \otimes (|0\rangle + e^{\frac{2\pi i x}{2^2}} |1\rangle) \otimes \dots (|0\rangle + e^{\frac{2\pi i x}{2^n}} |1\rangle)$$

the form is the same, but $\theta_4 \rightarrow 2\pi \frac{x_4}{2^n}$, so do inverse QFT



Measurement should yield $2^n \times \left(\frac{1}{2\pi}\right) \theta$