Grover's Search Algorithm
(1996)

0	0	0	0	0	1	0	0
1	2	3			a		N

N elements

To find index a such that $f(a) = 1$

Goal is to search for a single element $a_1, a_2, \ldots a_N$ does there exist an x such that $a_x = y$

I want to find "a" such that

$f(a) = 1$ $\quad f(x) = 0$ for all other $x \neq a$

Input :- n bits "N" possible

Output : a single bit 0 or 1

bits n

$N = 2$

Marked entry

$f(x) = 1$ at some $x = x_0$ and for other inputs the value of $f(x) = 0$

Goal :- To find x_0 for which $f(x_0) = 1$

→ classically how much time would it take $O(N)$

Can we do better?

In a quantum setting, you can do this task $O(\sqrt{N})$

→ An oracle $f: \{N\} \to \{0,1\}$ $N = 2^n$

$\{0,1\}^n$

for every input. $\boxed{\text{Find } a \text{ s.t } f(a) = 1}$

$x \to \boxed{U_f} \to f(x)$

$$\boxed{U_f |x, y\rangle = |x, y \oplus f(x)\rangle}$$

$$U_f |x, 0\rangle = |x, f(x)\rangle$$

$$U_f |x, 1\rangle = |x, 1 \oplus f(x)\rangle = |x, \overline{f(x)}\rangle$$

ancilla qubit

$$\boxed{|y\rangle = |-\rangle} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\boxed{U_f |x, -\rangle = (-1)^{f(x)} |x, -\rangle} \quad — \quad 1$$

Start with $\boxed{|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle}$

$N = 2^n$

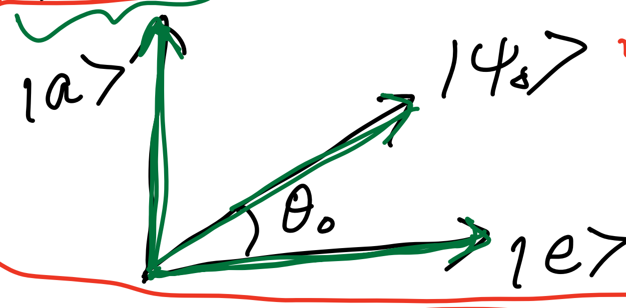
Assume that $f(a) = 1$
$f(x) = 0 \quad \forall\ x \neq a$

$$|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle$$

$$= \frac{1}{\sqrt{N}} \left[|a\rangle + \sum_{x \neq a} |x\rangle \right]$$

$$= \frac{1}{\sqrt{N}} |a\rangle + \frac{\sqrt{N-1}}{\sqrt{N}} \underbrace{\left[\frac{\sum_{x \neq a} |x\rangle}{\sqrt{N-1}} \right]}_{|e\rangle}$$

$$|\psi_0\rangle = \frac{1}{\sqrt{N}} |a\rangle + \sqrt{1 - \frac{1}{N}}\, |e\rangle \quad \text{— (1)}$$



$$\cos\theta_0 = |\langle e|\psi_0\rangle|$$

$$= \sqrt{1 - \frac{1}{N}}$$

$$\sin\theta_0 = \frac{1}{\sqrt{N}}$$

$$|\psi_0\rangle = \sin\theta_0\, |a\rangle + \cos\theta_0\, |e\rangle \quad (1)$$

If N is very large, θ_0 is very small

Oracle

$$U_f |x, -\rangle = (-1)^{f(x)} |x, -\rangle \quad — (*)$$

$f(x) = 0$
$\forall\, x \neq a$
$f(a) = 1$

$$U_f |a, -\rangle = (-1)^{f(a)} |x, -\rangle$$

$$U_f |a, -\rangle = -|a, -\rangle \quad — (2)$$

$$U_f |e, -\rangle = U_f \left| \frac{\sum_{x \neq a} |x\rangle}{\sqrt{N-1}}, -\right\rangle$$

$$= (-1)^{0} \left| \sum_{x \neq a} \frac{|x\rangle}{\sqrt{N-1}}, -\right\rangle$$

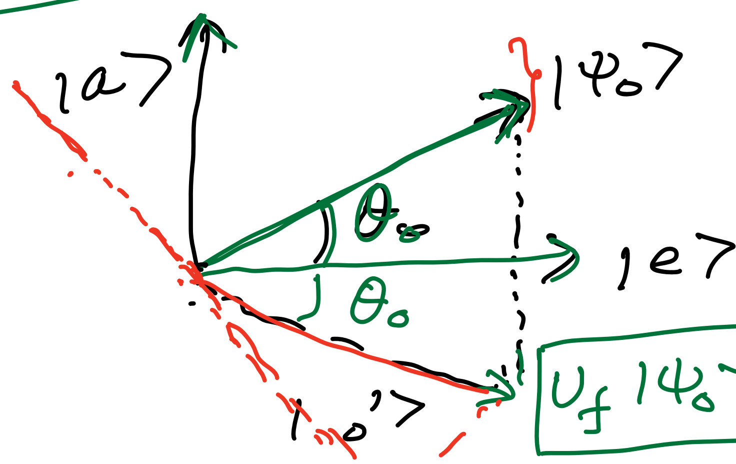
$$U_f |e, -\rangle = |e, -\rangle \quad — (3)$$

$$U_f |\psi_0, -\rangle = U_f \left| \sin\theta_0 |a\rangle + \cos\theta_0 |e\rangle, -\right\rangle$$

$$= \sin\theta_0 \{ -|a, -\rangle \} + \cos\theta_0 |e, -\rangle$$

$$\boxed{U_f |\psi_0\rangle = -\sin\theta_0 |a\rangle + \cos\theta_0 |e\rangle}$$

$U_f |\psi_0\rangle \longrightarrow$



$$\boxed{U_f |\psi_0\rangle = R_{|e\rangle} |\psi_0\rangle}$$

Q: Can we achieve rotation closer to $|a\rangle$ through reflection?

→ can achieve this from 2 consecutive reflections!

$$|\psi_0\rangle = \sin\theta_0 |a\rangle + \cos\theta_0 |e\rangle$$

$$\boxed{U_f|\psi_0\rangle = -\sin\theta_0 |a\rangle + \cos\theta_0 |e\rangle}$$

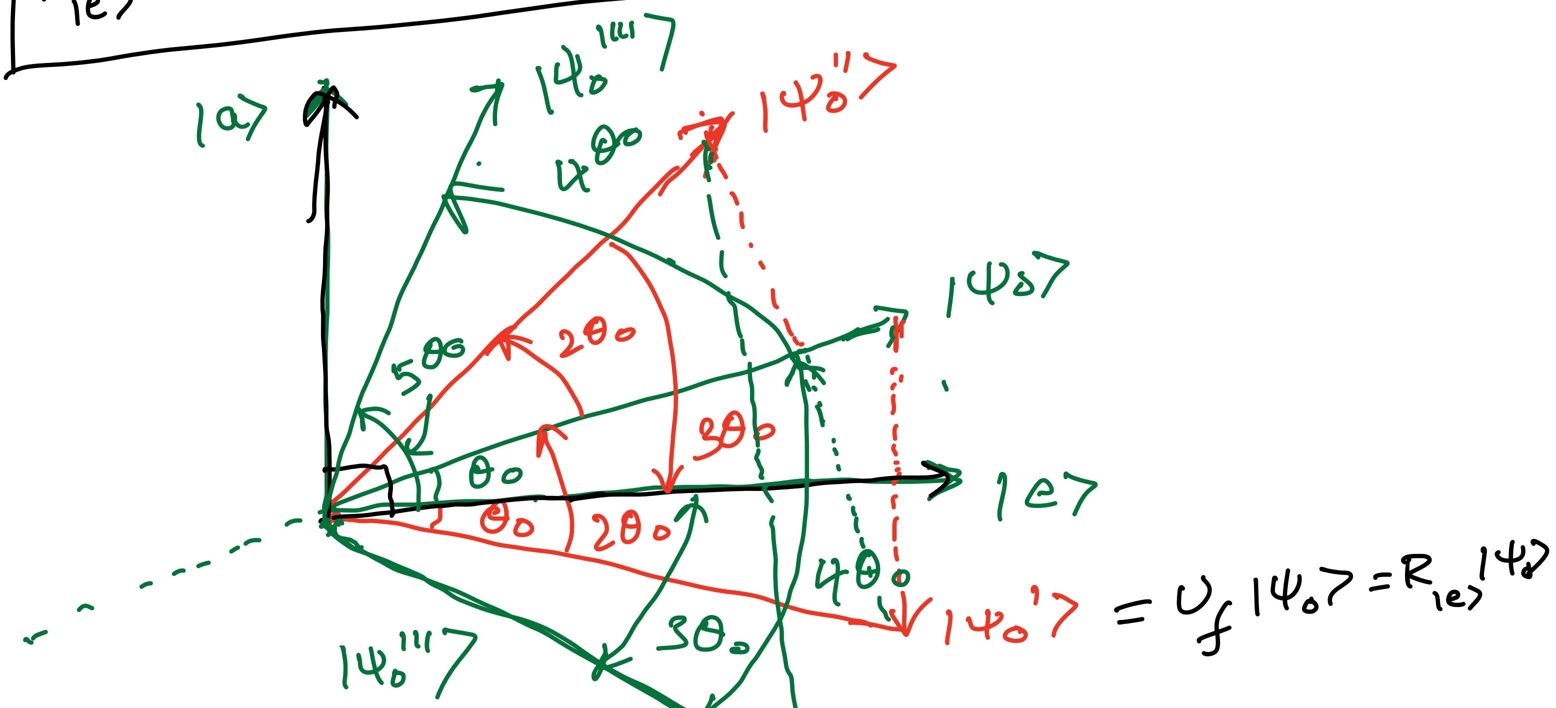
$$R_{|e\rangle}|\psi_0\rangle = (I - 2|a\rangle\langle a|)|\psi_0\rangle$$

$$= (|\psi_0\rangle - 2|a\rangle\langle a|\psi_0\rangle)$$

$|\psi$

$$= (\sin\theta_0 |a\rangle + \cos\theta_0 |e\rangle - 2|a\rangle[\sin\theta_0])$$

$$\boxed{R_{|e\rangle}|\psi_0\rangle = -\sin\theta_0 |a\rangle + \cos\theta_0 |e\rangle} \rightarrow |\psi_0'\rangle$$



$$|\psi_0''\rangle = R_{|\psi_0\rangle}|\psi_0'\rangle = \sin 3\theta_0\,|a\rangle + \cos 3\theta_0\,|e\rangle$$

$$|\psi_0''\rangle = R_{|\psi_0\rangle}R_{|e\rangle}|\psi_0\rangle = \underbrace{\sin 3\theta_0\,|a\rangle + \cos 3\theta_0\,|e\rangle}$$

$$G = R_{|\psi_0\rangle}R_{|e\rangle}$$

$$|\psi_0'''\rangle = R_{|e\rangle}\left[R_{|\psi_0\rangle}R_{|e\rangle}|\psi_0\rangle\right]$$

$$= R_{|e\rangle}|\psi_0''\rangle$$

$$= -\sin 3\theta_0\,|a\rangle + \cos 3\theta_0\,|e\rangle$$

$$R_{|\psi_0\rangle}|\psi_0'''\rangle = \sin 5\theta_0\,|a\rangle + \cos 5\theta_0\,|e\rangle$$

$G \rightarrow$ Grover operator

$$R_{|\psi_0\rangle}R_{|e\rangle} = R_{|\psi_0\rangle}U_f$$

$$G^k|\psi_0\rangle = \sin(\underbrace{(2k+1)\theta_0}) |a\rangle + \underbrace{\cos((2k+1)\theta_0)}|e\rangle$$

$$(2k+1)\theta_0 \approx \frac{\pi}{2}$$

$$(2k+1)\theta_0 = \frac{\pi}{2} \Rightarrow 2k\theta_0 + \theta_0 = \frac{\pi}{2}$$

$$\Rightarrow \quad 2k\theta_0 = \frac{\pi}{2} - \theta_0$$

$$\sin\theta_0 = \frac{1}{\sqrt{N}}$$

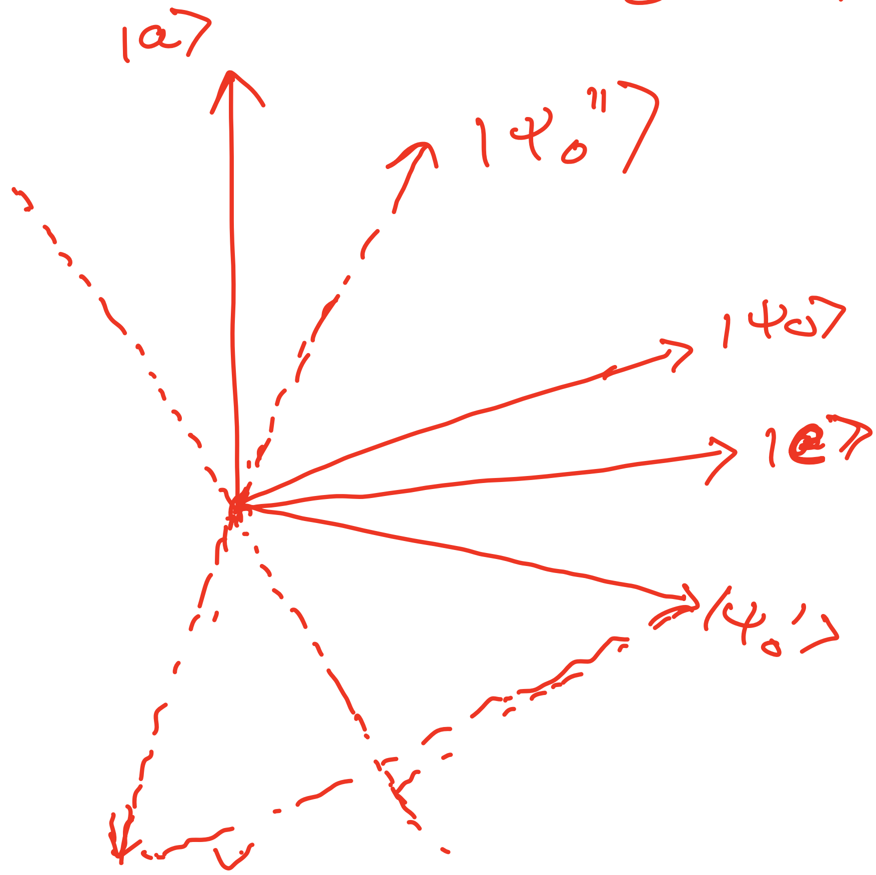
$$\Rightarrow \quad k = \underbrace{\frac{\pi}{4\theta_0} - \frac{1}{2}}$$

$$\sin\theta_0 \simeq \theta_0$$

$$\theta_0 \simeq 1/\sqrt{N}$$

$$K \simeq \frac{\sqrt{N}\,\pi}{4}$$

$$O(\sqrt{N})$$



$$\boxed{R_{|\psi_0\rangle} = -(I - 2|\psi_0\rangle\langle\psi_0|)}$$

$$\boxed{R_{|\psi_0\rangle} = 2|\psi_0\rangle\langle\psi_0| - I}$$

$$\boxed{R_{|\psi_0\rangle} = H^{\otimes n}(2|0^{\otimes n}\rangle\langle 0^{\otimes n}| - I)H^{\otimes n}}$$

$$H^{\otimes n}|0^{\otimes n}\rangle = |\psi_0\rangle \qquad (H^{\otimes n})^{\dagger}(H^{\otimes n}) = I$$

$$|0^{\otimes n}\rangle = (H^{\otimes n})^{\dagger}|\psi_0\rangle$$

$$= H^{\otimes n}|\psi_0\rangle$$

$$\boxed{R_{|\psi_0\rangle} = \left[2\,\underbrace{H^{\otimes n}|0^{\otimes n}\rangle}\langle 0^{\otimes n}| - H^{\otimes n}\right]H^{\otimes n}}$$

$$= \left[2|\psi_0\rangle\underbrace{\langle 0^{\otimes n}|} - \underbrace{H^{\otimes n}}\right]\underbrace{H^{\otimes n}}$$

$$\boxed{R_{|\psi_0\rangle} = 2\underbrace{|\psi_0\rangle}\langle\psi_0| - I}$$

Amplitude amplification

$|\psi_0\rangle$ which is prepared by oracle U_{ψ_0} ie $\boxed{U_{\psi_0}|0^n\rangle = |\psi_0\rangle}$

$$|\psi_0\rangle = \sqrt{p_0}\,|\psi_{good}\rangle + \sqrt{1-p_0}\,|\psi_{bad}\rangle$$

Grover's algorithm kind of approach can be used to amplify the coefficient in front of $|\psi_{good}\rangle$ i.e one can devise a quantum circuit similar to Grover's algorithm to construct states which have large overlap $|\psi_{good}\rangle$

$$\boxed{G = R_{\psi_0} R_{good}}$$

Quantum Phase Estimation

Phase estimation

$U \rightarrow$ unitary operator

$|\psi\rangle \rightarrow$ eigenvector of U

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

$$\theta = 2\pi\phi \quad , \quad \phi \in [0, 1)$$

$$U|\psi\rangle = e^{i2\pi\phi}|\psi\rangle$$

Given Given Estimate ϕ?

$$\underset{\sim}{Q}\,\underset{\sim}{x} = \lambda\,\underset{\sim}{x}$$

$$x^{+}Q\,x = \lambda\,x^{+}x$$

$$\lambda = \frac{x^{+}Qx}{x^{+}x}$$

Quantum Phase Estimation Algo :→

(I) Hadamard Test

$\Downarrow$

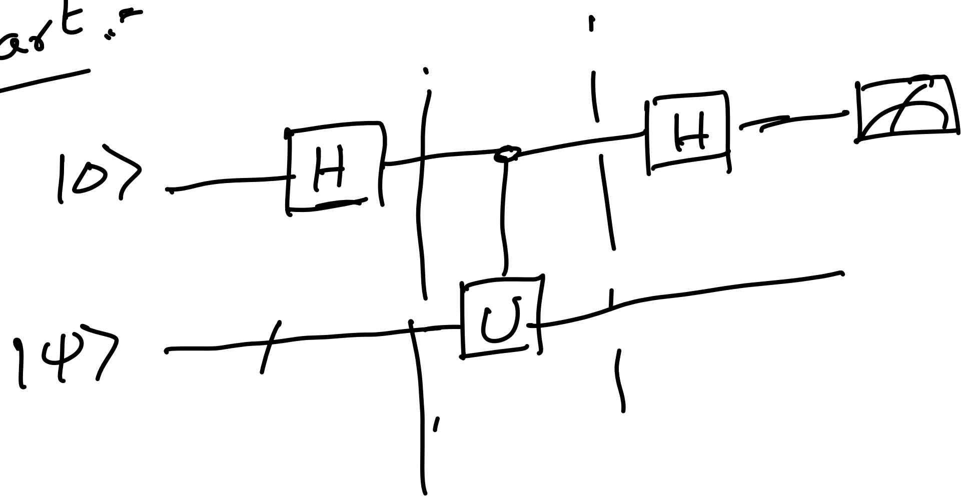
Compute expectation value of unitary operator with respect to a state $\langle\psi|U|\psi\rangle$ ↳ complex number

Since U is unitary this quantity

$\langle\psi|U|\psi\rangle$ is a complex number

and one needs to measure real and imaginary part of $\langle\psi|U|\psi\rangle$ separately!

Real part :-



$$\mathrm{Re}\,\langle\psi|U|\psi\rangle$$

$$|0\rangle\otimes|\psi\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes|\psi\rangle$$

$$\Big\downarrow \; c\text{-}U$$

$$\frac{1}{\sqrt{2}}\left(|0\rangle\otimes|\psi\rangle + |1\rangle\otimes U|\psi\rangle\right)$$

$$\Big\downarrow \; H\otimes I$$

$$\frac{1}{\sqrt{2}}\left(|+\rangle\otimes|\psi\rangle + |-\rangle\otimes U\psi\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes|\psi\rangle + \frac{1}{\sqrt{2}}(|0\rangle-|-\rangle)\otimes U|\psi\rangle\right)$$

$$= \frac{1}{2}\left[|0\rangle\otimes(|\psi\rangle+U|\psi\rangle)\right] + \frac{1}{2}\left[|1\rangle\otimes(|\psi\rangle-U|\psi\rangle)\right]$$

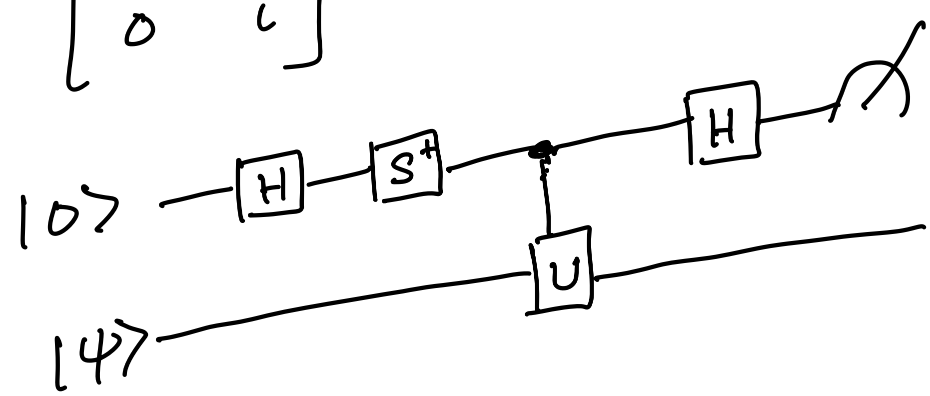
Probability of measuring qubit 0 to be in state $|0\rangle$

$$\boxed{p(0) = \frac{1}{2}\left(1+\mathrm{Re}\langle\psi|U|\psi\rangle\right)}$$

$|\psi\rangle + U|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

To define the imaginary part

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$ phase Gate



$$\frac{1}{2}\left[|0\rangle \otimes (|\psi\rangle - iU|\psi\rangle)\right] + \frac{1}{2}\left[|1\rangle \otimes (|\psi\rangle + iU|\psi\rangle)\right]$$

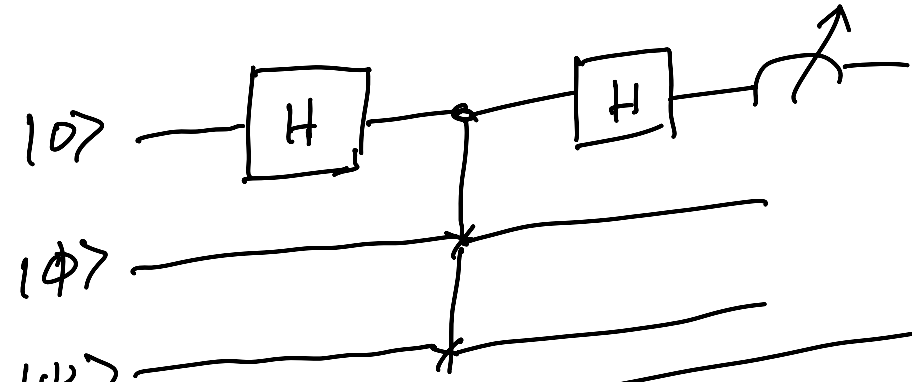
Probability of measuring qubit 0 (1st qubit) to be in State $|0\rangle$

$$p(0) = \frac{1}{2}\left(1 + \mathrm{Im}(\langle\psi|U|\psi\rangle)\right)$$

Combining the results from two circuits we obtain the estimate to $\langle\psi|U|\psi\rangle$

<u>Overlap estimate</u> :- (Application of Hadamard test)

Swap test $\rightarrow$ estimate overlap of two quantum state $|\langle\phi|\psi\rangle|$

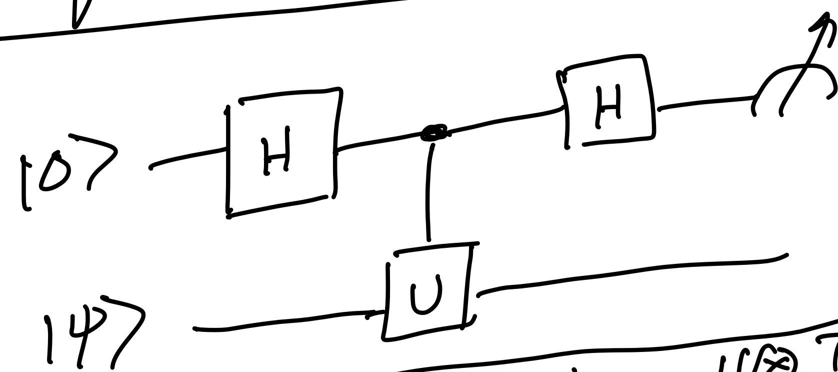


$$\boxed{p(0) = \frac{1}{2}\left(1+|\langle\phi|\psi\rangle|^2\right)}$$

1st Qubit to be in state $|0\rangle$

Single qubit phase estimation

$|\psi\rangle$ is an eigen vector of "U"



$$|0\rangle\otimes|\psi\rangle \boxed{\xrightarrow{H\otimes I} \quad \xrightarrow{c-U} \quad \xrightarrow{H\otimes I}}$$

$$\downarrow$$

$$\frac{1}{2}\Big(|0\rangle\otimes(|\psi\rangle+U|\psi\rangle) + |1\rangle\otimes(|\psi\rangle-U|\psi\rangle)\Big)$$

Probability of measuring 1^{st} qubit to be state $|1\rangle$

$$p(1) = \frac{1}{2}\left(1 - \mathrm{Re}\langle\psi|U|\psi\rangle\right)$$

$$= \frac{1}{2}\left(1 - \cos(2\pi\phi)\right)$$

$$\phi = \pm \frac{\cos^{-1}(1 - 2p(1))}{2\pi}$$

$p(1)$ is close to 0 or 1 or somewhere in between

The number of samples needed is $O(1/\varepsilon^2)$ where ε is the precision to determine "ϕ"

QPE $\rightarrow$ Can we do better than $O(1/\varepsilon^2)$ sampling to estimate ϕ?