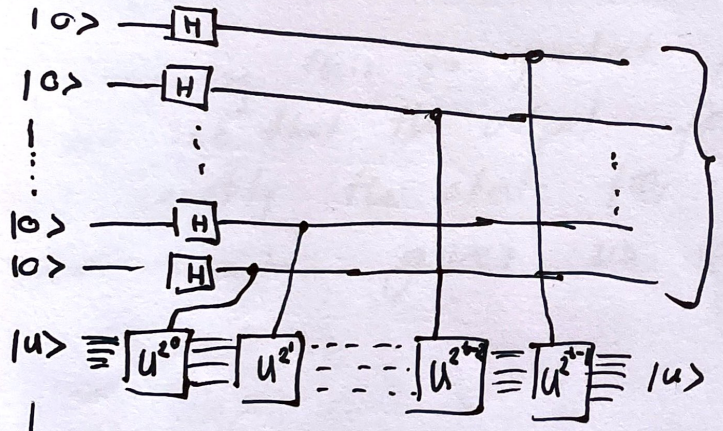
Quantum Phase Estimation:

Suppose a unitary operator U has an eigenvector $|u\rangle$ and the corresponding eigenvalue $e^{2\pi i\varphi}$ where φ is unknown. The goal of phase estimation algorithm is to find (estimate) φ. We assume we are capable of preparing state $|u\rangle$ and performing controlled U^{2^j} operations where j is a nonnegative integer. Phase estimation is not complete algorithm but used as a subroutine in many quantum algorithms.



$|0\rangle^{\otimes t}|u\rangle \xrightarrow{\text{After H gates}} \frac{1}{2^{n/2}}(|0\rangle+|1\rangle)^{\otimes n}|u\rangle \xrightarrow[\text{controlled } U^{2^0} \text{ to } n\text{th qubit}]{\text{Applying}} \frac{1}{2^{1/2}}\left(|0\rangle(|\quad\rangle + |1\rangle e^{2\pi i 2^0\varphi}|u\rangle\right)\otimes \frac{1}{2^{\frac{n-1}{2}}}(|0\rangle+|1\rangle)^{\otimes n-1}$

since $U|u\rangle = e^{2\pi i\varphi}|u\rangle$

$U^{2^j}|u\rangle = e^{2\pi i 2^j}|u\rangle$

$= \frac{1}{2^{1/2}}\left(|0\rangle + |1\rangle e^{2\pi i 2^0\varphi}\right)|u\rangle \otimes \frac{1}{2^{\frac{n-1}{2}}}(|0\rangle+|1\rangle)^{\otimes n-1}$

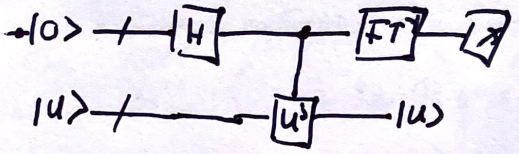
Then applying the remainder $n-1$ controlled U gates

$\Rightarrow \frac{1}{2^{n/2}}\left(|0\rangle + e^{2\pi i 2^{n-1}\varphi}|1\rangle\right)\left(|0\rangle + e^{2\pi i 2^{n-2}\varphi}|1\rangle\right)$

$\cdots\cdots \left(|0\rangle + e^{2\pi i 2^1\varphi}|1\rangle\right)\left(|0\rangle + e^{2\pi i 2^0\varphi}|1\rangle\right)$

$= \frac{1}{2^{n/2}}\underbrace{\left(|0\rangle + e^{2\pi i 2^0\varphi}|1\rangle\right)}_{n\text{th qubit}} \otimes (|0\rangle+|1\rangle)^{\otimes n-1}|u\rangle$

The second stage is to apply inverse fourier transform.

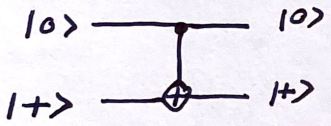


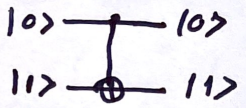
Suppose $\varphi = 0.\varphi_1\varphi_2\ldots\varphi_t$ then the resulting state from the first stage of phase estimation,

$$\frac{1}{2^{t/2}}\left(|0\rangle + e^{2\pi i 0.\varphi_t}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.\varphi_{t-1}\varphi_t}|1\rangle\right)\ldots\left(|0\rangle + e^{2\pi i 0.\varphi_1\varphi_2\ldots\varphi_t}|1\rangle\right)$$

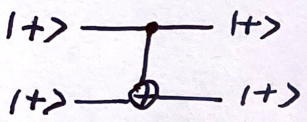
Comparing this to product form of Fourier transform we see that the output from the second stage is exactly the state $|\varphi_1\ldots\varphi_t\rangle$, therefore the measurement gives us φ exactly.

Phase Kickback:





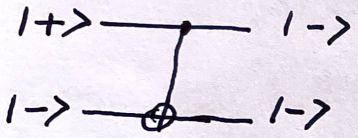
$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



$$|++\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

$$\downarrow CNOT$$

$$\frac{1}{2}(|00\rangle + |01\rangle + |11\rangle + |10\rangle) = |++\rangle \quad (\text{no change})$$



$$|+-\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

$$\downarrow CNOT$$

$$\frac{1}{2}(|00\rangle - |01\rangle + |11\rangle - |10\rangle) = |--\rangle$$

Due to our classical computing background we often rely on standard basis vectors $|0\rangle$ and $|1\rangle$, but when we are dealing with qubits it is better to realize qubits are not limited to those states and can be in a superposition of them.

Quantum order finding:

For positive integers x and N, $x < N$ with no common factors, the order of x modulo N is defined as the least positive integer, r, such that $x^r = 1 \pmod N$. Then, the order finding problem is determining the order of a given x and N.

example

$x = 5$, $N = 21 \Rightarrow 5^r = 1 \pmod{21}$

$\Rightarrow$
$5^1 = 5 = 5 \pmod{21}$
$5^2 = 25 = 4 \pmod{21}$
$5^3 = 125 = 20 \pmod{21}$
$5^4 = 625 = 16 \pmod{21}$
$5^5 = 3125 = 17 \pmod{21}$
$5^6 = 15625 = 1 \pmod{21}$ ✓ $\Rightarrow \boxed{r = 6}$

This is a hard problem using a classical computer since there are no algorithms known to solve the problem, using resources polynomial in $O(L)$ where $L = \log N$, is the number of bits needed to specify N.

quantum order finding is phase estimation applied to the unitary operator:

$$U|y\rangle \equiv |xy \pmod N\rangle$$

where $y \in \{0,1\}^L$, assume when $N \le y \le 2^L - 1$

then $xy \pmod N = y$ that is U only nontrivial when $0 \le y \le N-1$.

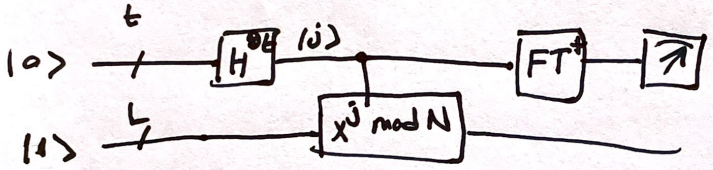
$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i s k}{r}} |x^k \bmod N\rangle$$

for integer $0 \le s \le r-1$ are eigenstates of U since

$$|U|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i s k}{r}} |x^{k+1} \bmod N\rangle$$

$$= e^{\frac{2\pi i s}{r}} |u_s\rangle$$

Using the phase estimation we can obtain the corresponding eigenvalues $e^{\frac{2\pi i s}{r}}$ and with some more work we can obtain the order (r).



Inputs:
- A black-box $U_{x,N}$ which transforms $|j\rangle|k\rangle \to |j\rangle|x^j k \bmod N\rangle$ (for a x co-prime to a L-bit number N)
- $t = 2L + 1 + \lceil \log(2 + \frac{1}{2\epsilon}) \rceil$ qubits initialized to zero
- L qubits initialized to $|1\rangle$.

Outputs: the least integer $r > 0$ s.t. $x^r = 1 \pmod N$

Runtime: $O(L^3)$ operations, succeeds with probability $Q(1)$

1. $|0\rangle|1\rangle$ % initialize
2. $\frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|1\rangle$ % create superposition
3. $\frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|x^j \bmod N\rangle$ % apply $U_{x,N}$
   $\approx \frac{1}{\sqrt{r 2^t}} \sum_{s=0}^{r-1} \sum_{j=0}^{2^t-1} e^{2\pi i s j / r} |j\rangle|u_s\rangle$
4. $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |s/r\rangle|u_s\rangle$ % apply inverse FT to first t qubits
5. ~~s~~ s/r % measure the first qubit
6. obtain r (via continued fractions algorithm)