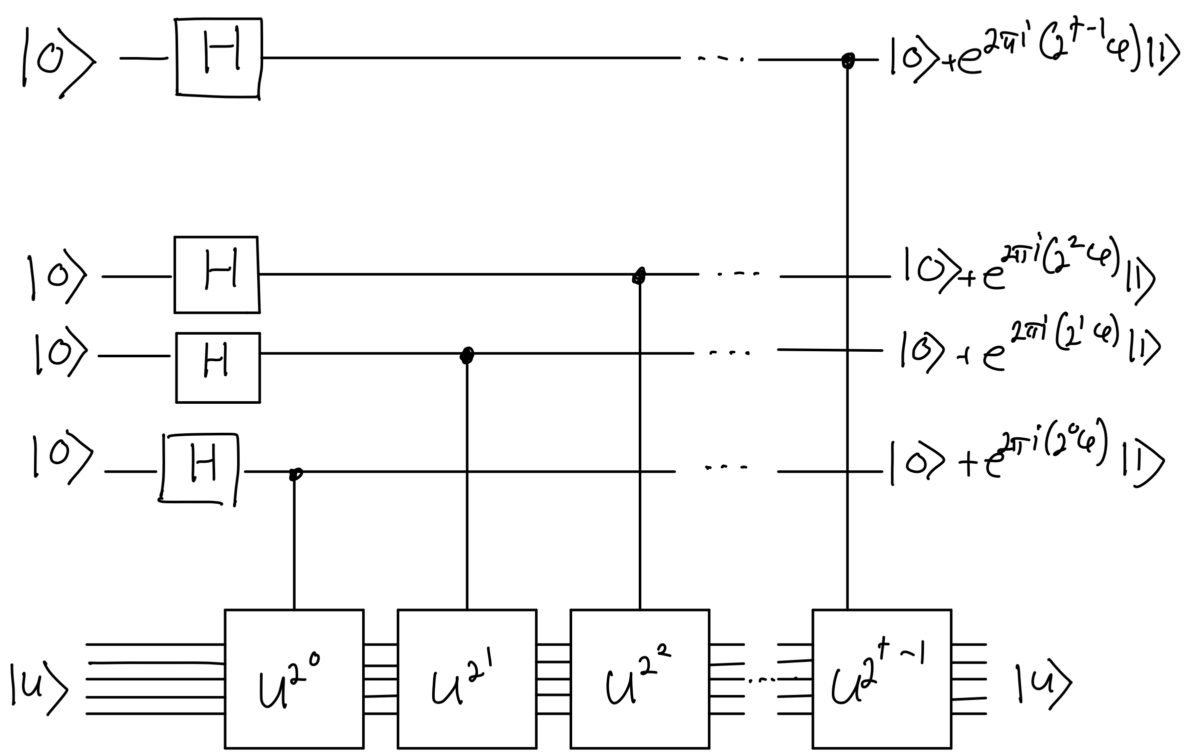
Phase estimation

Suppose a unitary operator U has an eigenvector $|u\rangle$ with eigenvalue $e^{2\pi i \varphi}$

goal: estimate φ

→ use two registers:

- first register contains t registers (t controls accuracy)
- second register has as many qubits as necessary to store $|u\rangle$



The final state of the first register is easily seen to be:

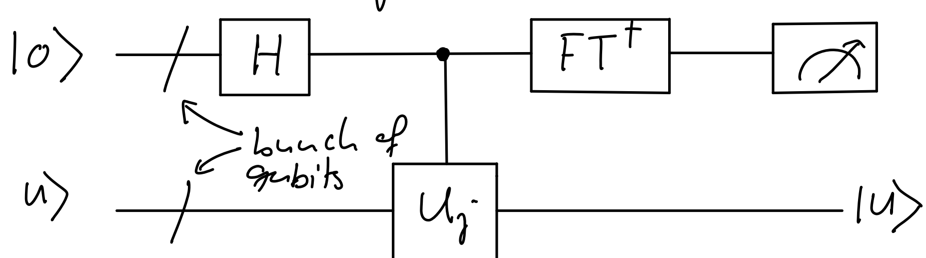
$$\frac{1}{2^{t/2}}\left(|0\rangle + e^{2\pi i 2^{t-1}\varphi}|1\rangle\right)\left(|0\rangle + e^{2\pi i 2^{t-2}\varphi}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 2^{0}\varphi}|1\rangle\right)$$

$$= \frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1} e^{2\pi i \varphi k}|k\rangle \qquad (*)$$

Now apply the "inverse" quantum Fourier trf. on first register.

→ can be implemented in $O(t^2)$ steps (see last lecture)

schematically:



explanation: suppose $\varphi = 0.\varphi_1\ldots\varphi_t$

→ then state (*) can be written as:

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

But this is the product rep. of QFT!

$\longrightarrow$ applying the inverse Fourier trf. gives us therefore

$$|\varphi\rangle = |\varphi_1 \dots \varphi_t\rangle$$

$\longrightarrow$ we just have to measure spin along the Z-basis to read off φ!

In general, one only arrives at an estimate $\tilde{\varphi}$ of the exact phase:

$$\frac{1}{2^{t/2}} \sum_{j=0}^{2^t-1} e^{2\pi i \varphi j} |j\rangle |u\rangle \xrightarrow[\text{QFT}]{\text{inv.}} |\tilde{\varphi}\rangle |u\rangle$$

<u>Performance and requirements:</u>

Let b be the integer in the range 0 to $2^t - 1$ such that $\frac{b}{2^t} = 0.b_1 \cdots b_t$ is the best t bit approximation to φ which is less than φ.

$\longrightarrow$ $\delta \equiv \varphi - b/2^t$ satisfies $0 \leq \delta \leq 2^{-t}$

Applying the inverse quantum Fourier transform to state $(**)$ produces the state

$$\frac{1}{2^t}\sum_{k,\ell=0}^{2^t-1} e^{-\frac{2\pi i k\ell}{2^t}} e^{2\pi i \varphi k}|\ell\rangle \qquad (1)$$

Let α_ℓ be the amplitude of $|(b+\ell)(\text{mod } 2^t)\rangle$,

$$\alpha_\ell \equiv \frac{1}{2^t}\sum_{k=0}^{2^t-1}\left(e^{2\pi i(\varphi-(b+\ell)/2^t)}\right)^k$$

(simply shift ℓ by b in (1))

$$= \frac{1}{2^t}\left(\frac{1-e^{2\pi i(2^t\varphi-(b+\ell))}}{1-e^{2\pi i(\varphi-(b+\ell)/2^t)}}\right)$$

$$= \frac{1}{2^t}\left(\frac{1-e^{2\pi i(2^t\delta-\ell)}}{1-e^{2\pi i(\delta-\ell/2^t)}}\right)$$

Suppose the outcome of the final measurement is m.

→ aim to obtain a bound for probability of $|m-b|>e$ for tolerance e.

→ $$p(|m-b|>e) = \sum_{-2^{t-1}<\ell\leq-(e+1)}|\alpha_\ell|^2 + \sum_{e+1\leq\ell\leq 2^{t-1}}|\alpha_\ell|^2 \qquad (2)$$

But for any θ, $|1-\exp(i\theta)|\leq 2$, so

$$|\alpha_\ell| \leq \frac{2}{2^t|1-e^{2\pi i(\delta-\ell/2^t)}|}$$

$$\leq \frac{1}{2^{t+1}(\delta+\ell/2^t)} \qquad \text{(exercise)} \quad (3)$$

Combining (2) and (3) gives:

$$p(|m-b|>e) \leq \frac{1}{4}\left[\sum_{\ell=-2^{t-1}+1}^{-(e+1)} \frac{1}{(\ell-2^t\delta)^2} + \sum_{\ell=e+1}^{2^t-1} \frac{1}{(\ell-2^t\delta)^2}\right]$$

Recalling that $0 \leq 2^t\delta \leq 1$, we obtain

$$p(|m-b|>e) \leq \frac{1}{4}\left[\sum_{\ell=-2^{t-1}+1}^{-(e+1)} \frac{1}{\ell^2} + \sum_{\ell=e+1}^{2^{t-1}} \frac{1}{(\ell-1)^2}\right]$$

$$\leq \frac{1}{2} \sum_{\ell=e}^{2^{t-1}-1} \frac{1}{\ell^2}$$

$$\leq \frac{1}{2} \int_{e-1}^{2^{t-1}-1} \frac{1}{\ell^2}\, d\ell$$

$$= \frac{1}{2(e-1)}$$

Suppose we wish to approximate φ to an accuracy 2^{-n}, that is, we choose $e = 2^{t-n}-1$. By making use of $t = n+p$ qubits in phase estimation algorithm

$$\longrightarrow p(\text{accurate approximation}) \geq 1 - \underbrace{\frac{1}{2(2^p-2)}}_{=:\,\varepsilon}$$

$$\longrightarrow \quad t = n + \left\lceil \log\left(2+\frac{1}{2\varepsilon}\right)\right\rceil$$

Application: order-finding

For positive integers x and N, $x < N$, with no common factors, the "order" of x modulo N is defined to be the least positive integer, r, such that $x^r = 1 \pmod{N}$.

$\longrightarrow$ "order-finding" is hard problem on classical computer
(no algorithm polynomial in $O(L)$ for $L \equiv \lceil \log(N) \rceil$ known)

quantum algorithm:
Define unitary operator U by

$$U|y\rangle \equiv |xy \,(\mathrm{mod}\, N)\rangle$$

with $y \in \{0,1\}^L$

$\rightarrow$ simple calculation shows

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

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

check: $$U|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi i s k}{r}\right] |x^{k+1} \bmod N\rangle$$

$$= \exp\left[\frac{2\pi i s}{r}\right] |u_s\rangle \quad \checkmark$$

→ phase estimation gives with high accuracy corresponding eigenvalues $\exp(2\pi i s/r)$

→ can read off r

exercise : show that U is unitary

two requirements :

1) need efficient implementation of controlled-U^{2^j} operation

2) preparation of state r

→ 1) : Modular exponentiation

wish to compute the trf

$$|z\rangle|y\rangle \mapsto |z\rangle U^{z_t 2^{t-1}} \cdots U^{z_1 2^0}|y\rangle$$

$$= |z\rangle|x^{z_t 2^{t-1}} \times \cdots \times x^{z_1 2^0} y \pmod N\rangle$$

→ equivalent to multiplying contents of second register by "modular exponential" $x^z \pmod N$ where z is the content of first register

→ 2) : preparing $|u_s\rangle$ requires that we know r, out of question

use the following trick:

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle \qquad \text{(exercise)}$$

→ use $t = 2L + 1 + \lceil \log(2 + \frac{1}{2\varepsilon}) \rceil$ qubits in first register and prepare second register in state $|1\rangle$

→ will obtain estimate of phase $\varphi \approx \frac{s}{r}$ accurate to $2L+1$ bits, with probability $\geq (1-\varepsilon)/r$.