- Shor's algorithm (Factoring → Period Finding)
- Hassidim-Harrow-Lloyd's algorithm (Q Linear System Algorithm)
- Grover's algorithm (Search)

Shor's algorithm:

PERIOD FINDING

input: Integer m, a s.t. $1 \le a < m$, $GCD(a,m) = 1$ (a and m are coprime)

output: The smallest $r > 0$ s.t. $a^r \equiv 1 \pmod m$.

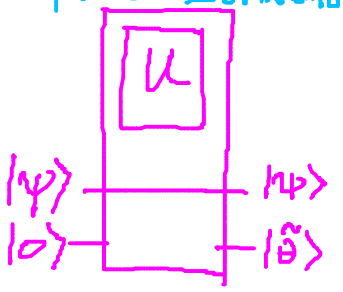
PHASE ESTIMATION

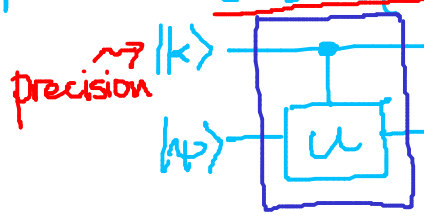
input: A unitary matrix U, eigenvector $|\psi\rangle$ of U

output: The eigenvalue $e^{2\pi i \theta}$ of U corresponding to $|\psi\rangle$

that is $U|\psi\rangle = e^{i\theta}|\psi\rangle$. Output: $\tilde{\theta} = \frac{\theta}{2\pi}$, $\tilde{\theta} \in [0,1)$

phase estimator = CTRL-U (controlled U) + QFT + $H^{\otimes n}$





$U|\psi\rangle = e^{2\pi i \tilde{\theta}}|\psi\rangle$

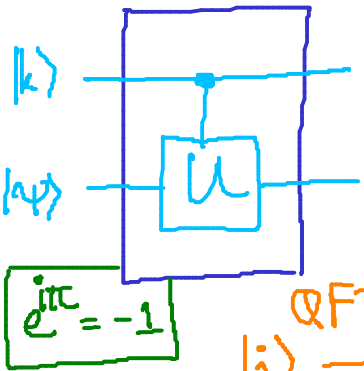
CTRL-U: $|k\rangle|\psi\rangle \mapsto e^{2\pi i k\tilde{\theta}}|k\rangle|\psi\rangle$

$\frac{1}{\sqrt{2^n}}\sum_k |k\rangle|\psi\rangle \to \frac{1}{\sqrt{2^n}}\sum_k e^{2\pi i k\tilde{\theta}}|k\rangle|\psi\rangle$

say k is an n-bit integer

$k \in \{0,1\}^n$

$\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}|k\rangle$



$= \left[\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1} e^{\frac{2\pi i k(\tilde{\theta}2^n)}{2^n}}|k\rangle\right]|\psi\rangle$ (*)

ex: $n=1$, 1-bit integers

$|j\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}\sum_{k=0}^{1} e^{\pi i jk}|k\rangle$

$= \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^j|1\rangle\right)$

$|0\rangle \to \frac{|0\rangle+|1\rangle}{\sqrt{2}}$

$|1\rangle \to \frac{|0\rangle-|1\rangle}{\sqrt{2}}$

QFT: $|j\rangle \to \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1} \omega_{2^n}^{jk}|k\rangle$, $j \doteq \tilde{\theta}2^n$, $\omega_{2^n} \doteq e^{2\pi i/2^n}$

QFT^{-1}

$|\tilde{\theta}2^n\rangle$

$0 \le \tilde{\theta} < 1$: $\tilde{\theta} = 0.b_1b_2\ldots b_nb_{n+1}\ldots$

$2\tilde{\theta} = b_1.b_2b_3\ldots$

$2^2\tilde{\theta} = b_1b_2.b_3b_4\ldots$

$2^n\tilde{\theta} = [b_1b_2\ldots b_n].b_{n+1}\ldots$

ignore fractional part

n-bit approximation to $\tilde{\theta}$

PERIOD FINDING: find r s.t.

N, a: $a^0 \to a^1 \to a^2 \to a^3 \to \dots \to a^r = 1$, $a^{r+1} = a^1$, $a^{r+2} = a^2$, $a^{r+3} = a^3$, $\dots$, $a^{2r} = 1$, $\dots$ $\dots$

$U = M_{a,m}$ (mod m) $|a\rangle \to |a^2\rangle \to |1\rangle$ $\quad M_{a,m}: |x\rangle \to |a^x\rangle$ (mod m)

? $|\psi_0\rangle = \frac{1}{\sqrt{r}}\left(|1\rangle + |a\rangle + \dots + |a^{r-1}\rangle\right)$ $\quad a^r \equiv 1 \pmod m$

$U|\psi_0\rangle = \omega_r^0 |\psi_0\rangle$ $\quad |\psi_0\rangle$ is an eigenvector of U with eigenvalue 1

? $|\psi_1\rangle = \frac{1}{\sqrt{r}}\left(|1\rangle + \omega_r^{-1}|a\rangle + \omega_r^{-2}|a^2\rangle + \dots + \omega_r^{-(r-1)}|a^{r-1}\rangle\right)$ $\quad \omega_r = e^{2\pi i/r}$ r^{th} principal root of unity

$U|\psi_1\rangle = \frac{1}{\sqrt{r}}\left(|a\rangle + \omega_r^{-1}|a^2\rangle + \omega_r^{-2}|a^3\rangle + \dots + \omega_r|1\rangle\right)$

$= \omega_r \frac{1}{\sqrt{r}}\left(\omega_r^{-1}|a\rangle + \omega_r^{-2}|a^2\rangle + \dots + |1\rangle\right)$ $\quad \omega_r^{-(r-1)} = \omega_r^{-r+1} = \omega_r$

$= \omega_r^1 |\psi_1\rangle$

$\boxed{\omega_r^r = 1}$

$|\psi_j\rangle = \frac{1}{\sqrt{r}}\left(|1\rangle + \omega_r^{-j}|a\rangle + \omega_r^{-2j}|a^2\rangle + \dots\right) \Rightarrow U|\psi_j\rangle = \omega_r^j |\psi_j\rangle$ $\quad j = 0, 1, \dots, r-1$

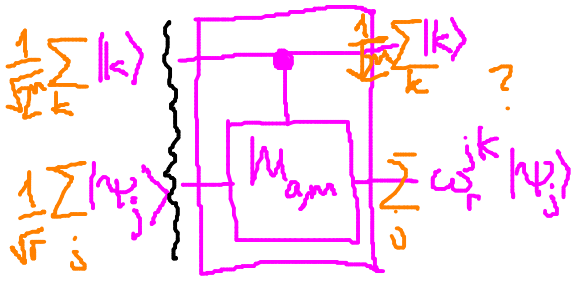
Fact:

$\frac{1}{\sqrt{r}}\left(|\psi_0\rangle + |\psi_1\rangle + \dots + |\psi_{r-1}\rangle\right) = |1\rangle$

$1 + \omega_r + \omega_r^2 + \dots + \omega_r^{r-1} = \frac{\omega_r^r - 1}{\omega_r - 1} = 0$ $\quad \omega_r \neq 1$

geometric series

$M_{a,m}$: $|x\rangle \to |ax \pmod m\rangle$



$\frac{1}{\sqrt{2^n}}\sum_k |k\rangle \otimes \frac{1}{\sqrt{r}}\sum_j |\psi_j\rangle = \frac{1}{\sqrt{2^n r}} \sum_{k,j} |k\rangle|\psi_j\rangle$

$C\text{-}M_{a,m}$ $\longrightarrow \frac{1}{\sqrt{2^n r}} \sum_{k,j} \omega_r^{jk} |k\rangle|\psi_j\rangle$

$= \frac{1}{\sqrt{r}} \sum_j \left[\frac{1}{\sqrt{2^n}} \sum_k e^{\frac{2\pi i k \tilde{j}}{2^n}} |k\rangle \right] |\psi_j\rangle$ $\quad \tilde{j}$: $\frac{j}{r} \approx \frac{\tilde{j}}{2^n}$

QFT^{-1} $\longrightarrow \frac{1}{\sqrt{r}} \sum_j |\tilde{j}\rangle |\psi_j\rangle$ $\quad \tilde{j}$: measure

details missing! (Mike & Ike book)

n-bit approximation of $\frac{j}{r}$

$\tilde{j} = \frac{j}{r} \times 2^n$ $\quad$ fraction $\quad j = 0, 1, \dots, r-1$

$0 \leq \frac{j}{r} < 1$

if j, r are coprime then we can recover r

Harrow-Hassidim-Lloyd algorithm: [See Aaronson's article]

input: A, Hermitian matrix ($n \times n$), invertible; vector $|b\rangle \in \mathbb{R}^n$

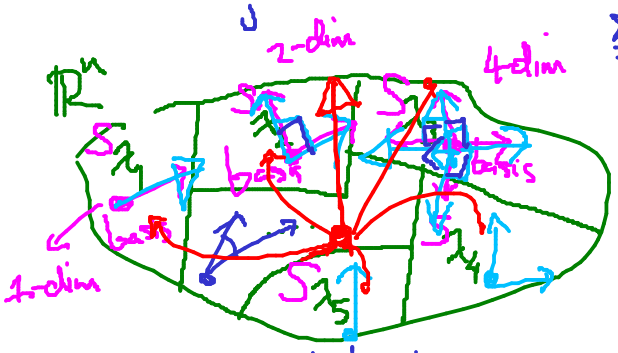
output: The vector $|x\rangle$ s.t. $A|x\rangle = |b\rangle \Rightarrow |x\rangle = A^{-1}|b\rangle$

Say the eigenvectors + eigenvalues of A: $A|\psi_j\rangle = \lambda_j |\psi_j\rangle$

$$|b\rangle = \sum_j c_j |\psi_j\rangle$$

Spectral decomposition: projection matrix onto the eigenspace of λ_j

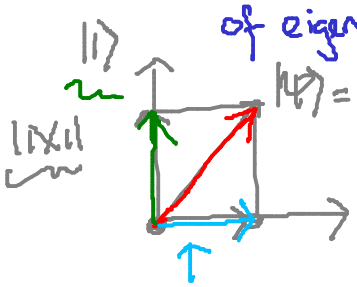
$$\star\star \quad A = \sum_j \lambda_j \underbrace{|\psi_j\rangle\langle\psi_j|}_{\text{outer product of } |\psi_j\rangle \text{ with itself}}$$



orthonormal basis of eigenvectors

$$S_{\lambda_j} = \sum |\psi\rangle\langle\psi|$$

$\{$ eigenvectors with eigenvalue λ_j



$$|0\rangle\langle 0|\psi\rangle = \overline{|0\rangle\langle 0|}\left(a|0\rangle + b|1\rangle\right) = a|0\rangle\underbrace{\langle 0|0\rangle}_{1} + b|0\rangle\underbrace{\langle 0|1\rangle}_{0} = a|0\rangle$$

nice f

$$A \overset{\downarrow}{=} \sum_j \lambda_j |\psi_j\rangle\langle\psi_j| \Rightarrow f(A) = \sum_j f(\lambda_j)|\psi_j\rangle\langle\psi_j|$$

1) $f(x) = e^{ix}$:

$$\underbrace{e^{iA}}_{\| \text{ finite Sum}} = \sum_j e^{i\lambda_j}|\psi_j\rangle\langle\psi_j|$$

$$I + iA + \frac{(iA)^2}{2!} + \frac{(iA)^3}{3!} + \cdots$$

infinite series

2) $f(x) = \frac{1}{x} = x^{-1}$

$$A^{-1} = \sum_j \frac{1}{\lambda_j}|\psi_j\rangle\langle\psi_j|$$

$\forall j: \lambda_j \neq 0 \Leftrightarrow A$ invertible nonsingular

Assume $A = \sum_j \lambda_j |\psi_j\rangle\langle\psi_j|$

A Hermitian $\Rightarrow e^{iAt}$ unitary

$|\psi_j\rangle, \lambda_j$ $\quad$ $|\psi_j\rangle, e^{i\lambda_j t}$

HHL:

$$\underbrace{e^{iAt}}_{\| \sum c_j|\psi_j\rangle}|b\rangle|0\rangle \to \sum_j c_j e^{i\lambda_j t}|\psi_j\rangle|0\rangle$$

$$\to \sum_j c_j e^{i\lambda_j t}|\psi_j\rangle|\lambda_j t\rangle \to \sum_j c_j e^{i\lambda_j t}|\psi_j\rangle|\lambda_j t\rangle$$

$i\lambda_j t$: Cancel; $\lambda_j t$: zero

$$A^{-1} = \sum_j \lambda_j^{-1}|\psi_j\rangle\langle\psi_j|$$

$$A^{-1}|b\rangle = \sum_j \lambda_j^{-1}\langle\psi_j|b\rangle|\psi_j\rangle$$

Phase Estimation; uncompute trick; ignore; measure?

$$\sum_j \frac{c_j}{\lambda_j}|\psi_j\rangle|0\rangle = \underbrace{A^{-1}|b\rangle}_{|x\rangle}|0\rangle \qquad |x\rangle = \sum_j x_j|j\rangle$$

$|x_j|^2$