Week 5

Review

- Operations on quantum states are norm-preserving (Unitary)

  $\rightarrow \quad U^{\dagger} = U^{-1} \Rightarrow U^{\dagger}U = UU^{\dagger} = I$

- Unitary operations for a single qubit are rotations on the surface of Bloch sphere

- Eigenvalues and eigenvectors of unitary matrices (or operations) are special.

  $\rightarrow \quad U|x\rangle = \lambda_x |x\rangle$ → eigenvector

  ↑ eigenvalue always of the form $e^{i\theta}$

  → for two distinct λ_x and λ_y :

  $\lambda_x = \lambda_y$: $|x\rangle$ and $|y\rangle$ are orthogonal

  $\langle x|y\rangle = 0$

- Shor's Algorithm:

  $f(x) = f(y)$ for $x \neq y$ iff $|x-y| = np$

  ↖ period

Classically : $O\left(e^{c \cdot n^{1/3} \cdot (\log n)^{2/3}}\right)$

n bits needed to describe the period

Quantum : $O(n^2 \log n \cdot \log\log n)$

↳ A little better than $O(n^3)$

→ QFT and modular exponentiation are the building blocks of <u>Shor's Algo.</u> → Quantum Phase Estimation

→ Factorisation $\xleftrightarrow{\text{similar}}$ periodicity

* QFT: A change of basis from computational basis to Fourier basis.

Comp: $M_0 = \langle 0|0\rangle$ $\quad M_1 = \langle 1|1\rangle$

Fourier: $M_+ = \langle +|+\rangle$ $\quad M_- = \langle -|-\rangle$

$|\tilde{0}\rangle = |+\rangle ; \ |\tilde{1}\rangle = |-\rangle$

→ 1 Qubit QFT is Hadamard gate.

→ For n qubits, we have $N = 2^n$ basis states

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

$|y\rangle$ corres. to binary notation of y

Fourier basis

ex: $QFT|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi \cdot 1}|1\rangle\right) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}$

→ Notation: $|y\rangle$ is actually $\underbrace{|y_1 y_2 \cdots y_n\rangle}$ Binary version of y

$$\therefore \sum_{y=0}^{n} \rightarrow \sum_{y_0=0}^{1} \sum_{y_1=0}^{1} \cdots \sum_{y_n=0}^{1}$$

$$\therefore |x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle \otimes \cdot \otimes |x_n\rangle = |x\rangle$$

$$\Big\downarrow \text{QFT}$$

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

ex: $n = 3$ qubits $\longrightarrow$ $N = 2^3 = 8$

$$|x\rangle = |5\rangle = |101\rangle = |1\rangle \otimes |0\rangle \otimes |1\rangle$$

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

→ $|x_k\rangle \longrightarrow |0\rangle + e^{\frac{2\pi i x}{2^k}} |1\rangle$ [QFT]

- Phase is qubit dependent
- Terms with more +more 1's occur more and more → ex : $|011\rangle$ ($|101\rangle$, $|110\rangle$ terms would need 2 phase terms

* $H|x_k\rangle = \left(|0\rangle + e^{\frac{2\pi i x_k}{2}}|1\rangle\right)/\sqrt{2}$

if x_k 0 or 1

$e^{\frac{2\pi i x_k}{2}}$: $x_k = 0 \rightarrow 1$; $x_k = 1 \rightarrow -1$

* $UROT_k |x_j\rangle = e^{\frac{2\pi i}{2^k} x_j} |x_j\rangle$

$UROT$: Unitary rotation

controlled rotation $\rightarrow$ $x_j = 0 \Rightarrow e^{\frac{2\pi i}{2^k} x_j} |x_j\rangle = |0\rangle$

$x_j = 1 \Rightarrow e^{\frac{2\pi i}{2^k} x_j} |x_j\rangle = e^{\frac{2\pi i}{2^k}} |x_j\rangle$

For 1 qubit $\rightarrow$ $UROT_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{bmatrix}$

applying a phase if $|1\rangle$ (on)

* Quantum Phase Estimation:

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

an eigenvector of U

→ QPE corresponds to measuring the global phase of a state

→ Assuming that we have the capacity to prepare a given $|\psi\rangle$ and apply U to it:

$$QPE|0\rangle|\psi\rangle = \frac{1}{2}\left[|0\rangle(1+e^{i\theta_\psi}) + |1\rangle(1-e^{i\theta_\psi})\right]|\psi\rangle$$

→ After a lot of measurements, we can estimate θ_ψ based on the $|0\rangle$ and $|1\rangle$ meas. on first qubit

$$\rightarrow \quad U^{2^x}|\psi\rangle = U^{2^x-1}\, U|\psi\rangle$$
$$= U^{2^x-1}\, e^{i\theta_\psi}|\psi\rangle$$
$$= e^{i\theta_\psi + i\theta_\psi}\, U^{2^x-2}|\psi\rangle$$
$$= e^{x i\theta_\psi}|\psi\rangle$$

→ If we use n qubits for meas. instead of 1:

$$QPE\,|0\rangle^{\otimes n}|\psi\rangle = \left(\frac{1}{\sqrt{2}}\right)^n \left(|0\rangle + e^{i\theta_\psi 2^{n-1}}|1\rangle\right) \otimes \left(|0\rangle + e^{i\theta_\psi 2^{n-2}}|1\rangle\right) \otimes \cdots \left(|0\rangle + e^{i\theta_\psi 2^{0}}|1\rangle\right)|\psi\rangle$$

→ QPE is same as QFT except:

$$\theta_\psi \longrightarrow \frac{\theta_\psi}{2^n} 2\pi$$

QFT phase   QPE phase

$$\rightarrow (QFT^{-1})(QPE)\,|0\rangle^{\otimes n}|\psi\rangle = |2^n\theta_\psi\rangle|\psi\rangle$$

This factor increases the amplitude for phase estimate