Lecture 3 – Shor's Algorithm I – QFT and QPE

Roadmap – (1) Qubits & Quantum states

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}; \quad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}; \quad X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

$$\langle 0|\psi\rangle = a; \quad \langle 1|\psi\rangle = b;$$

$$\text{Prob}(\text{meas } 0) = \|a\|^2; \quad \text{Prob}(\text{meas } 1) = \|b\|^2$$

$$\|a\|^2 + \|b\|^2 = 1 \Rightarrow \text{2 implications}$$

(1) Operations on quantum states need to preserve norm to 1

→ Norm-preserving matrices = unitary ($\Rightarrow U^\dagger = U^{-1}$)

$\Rightarrow U^\dagger U = UU^\dagger = I$

→ $|\det(U)| = 1$

(2) For a single qubit, can think of unitary gates as rotations on the surface of the Bloch sphere.

(3) Eigenvalues and eigenvectors of unitary matrices are special.

(a) $U|x\rangle = \lambda_x|x\rangle$

$\Rightarrow \langle x|U^\dagger = \langle x|\lambda_x^*$

$$\langle x|x\rangle = 1 = \langle x|U^\dagger U|x\rangle = \langle x|\lambda_x^*\lambda_x|x\rangle = |\lambda_x|^2\langle x|x\rangle = |\lambda_x|^2$$

$\Rightarrow |\lambda_x|^2 = 1 \Rightarrow \lambda_x = e^{i\theta}$ for some θ

$\Rightarrow$ eigenvalues of U are of the form $e^{i\theta}$

(b) $U|x\rangle = \lambda_x|x\rangle$ if $\lambda_x \neq \lambda_y$, then

$U|y\rangle = \lambda_y|y\rangle$ $\quad \langle x|y\rangle = \langle x|U^\dagger U|y\rangle = \lambda_x^*\lambda_y\langle x|y\rangle$

$\Rightarrow \langle x|y\rangle(1 - \lambda_x^*\lambda_y) = 0$

multiply by λ_x and use $|\lambda_x|^2 = 1$ $\Rightarrow \langle x|y\rangle(\lambda_x - \lambda_y) = 0$

$\lambda_x \neq \lambda_y \Rightarrow \langle x|y\rangle = 0$ eigvecs of diff eigvals are orthonormal

- Also covered - Deutsch - Josza algorithm
  - constant / balanced function in one shot
- Grover's algorithm
  - unstructured search in N items with $O(\sqrt{N})$

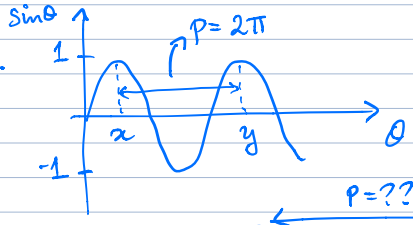
Today: Preliminaries for Shor's algorithm

famous algorithm

Problem: given a function that is periodic, find its period. period

strict definition: $f(x) = f(y)$ for $x \neq y$ iff $|x - y| = kp$

easy example:



hard example: $f(\xi)$

classically: $O(\exp c \cdot n^{1/3}(\log n)^{2/3})$

p has n bits

quantum: Shor's algorithm: $O(n^2(\log n)(\log\log n))$

little faster than $O(n^3)$

Reason why this works: (1) quantum Fourier transform

(2) modular exponentiation

Implication: difficulty of factoring on a classical computer is basis for security (more tomorrow)

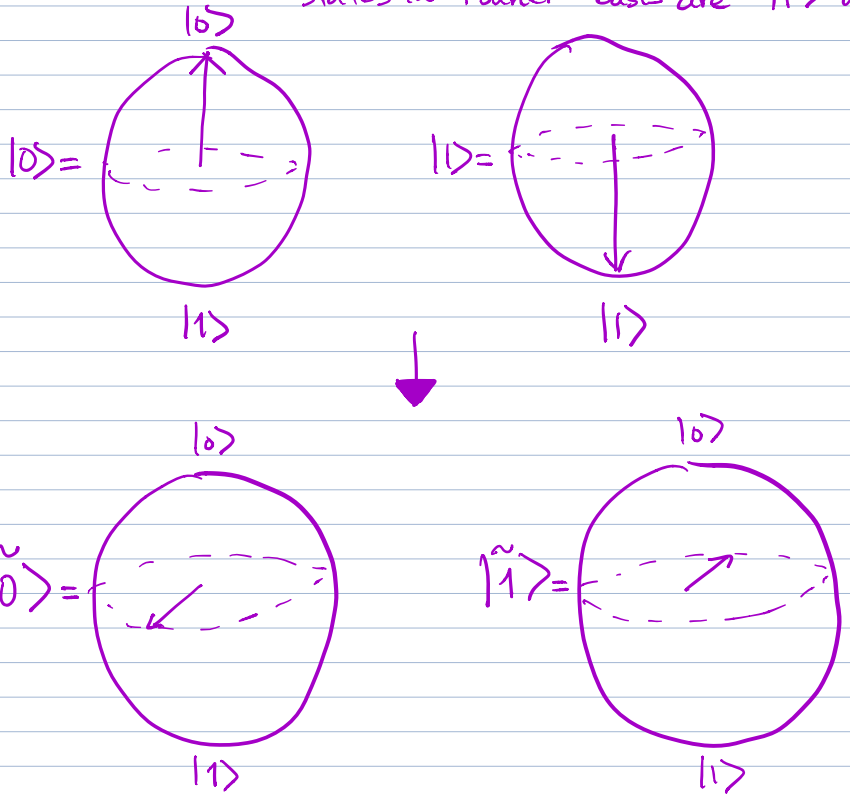
Today – Quantum Fourier Transform, Quantum Phase Estimation

(Shor's algorithm is really QPE in disguise)

QFT is effectively a change of basis from the computational basis to a Fourier basis.

eg: 1 qubit: states in computational basis are $|0\rangle$ and $|1\rangle$

states in Fourier basis are $|+\rangle$ and $|-\rangle$



multiple qubits: go to Qiskit demo

– notice that we are going from basis on the two poles of the Bloch sphere to a basis on the equatorial plane.

Building the quantum circuit that applies QFT

(1) Show QFT rigorously

(2) Show circuit to implement QFT expression

(1) n qubits $\Rightarrow$ 2^n basis states. Define $N \equiv 2^n$. Then,

$$|\tilde{x}\rangle \equiv QFT\,|x\rangle$$

($|\tilde{x}\rangle$: Fourier basis; $|x\rangle$: Computational basis)

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

[analogous to inverse discrete Fourier transform]

eg: 1-qubit case $[\Rightarrow N = 2]$

$$|\tilde{0}\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} e^{\frac{2\pi i (0)\cdot y}{2}} |y\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} |y\rangle$$

$$= \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

$$|\tilde{1}\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} e^{\frac{2\pi i (1)\cdot y}{2}} |y\rangle = \frac{1}{\sqrt{2}} \left(e^{\frac{2\pi i (0)}{2}} |0\rangle + e^{\frac{2\pi i \cdot 1}{2}} |1\rangle \right)$$

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

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

A note on notation: for multiple qubits, eg $n = 3$,

$$|\tilde{x}\rangle = \frac{1}{\sqrt{8}} \sum_{y=0}^{7} e^{2\pi i x y / 2^3} |y\rangle$$

↳ eg $|y\rangle = |4\rangle \Leftrightarrow |100\rangle$

$4 = 2^2(1) + 2^1(0) + 2^0(0)$

$4/2^3 = \frac{2^2(1) + 2^1(0) + 2^0(0)}{2^3}$

$$|\tilde{x}\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{2\pi i x y}{N}} |y\rangle \qquad y = [y_1 y_2 y_3 \cdots y_n] = 2^{n-1} y_1 + \cdots + 2^{n-n} y_n$$

$$= \frac{1}{\sqrt{N}} \sum_{y_1=0}^{1} \sum_{y_2=0}^{1} \cdots \sum_{y_n=0}^{1} e^{\frac{2\pi i x}{N} \sum_{k=1}^{n} y_k 2^{n-k}} |y_k\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_{y_1, y_2, \ldots, y_n} \bigotimes_{k=1}^{n} e^{\frac{2\pi i x 2^{n-k}}{N} y_k} |y_k\rangle$$

$$= \frac{1}{\sqrt{N}} \bigotimes_{k=1}^{n} \left[|0\rangle + e^{\frac{2\pi i x}{N} 2^{n-k}} |1\rangle \right]$$

$$= \frac{1}{\sqrt{N}} \bigotimes_{k=1}^{N} \left[|0\rangle + e^{2\pi i x 2^{-k}} |1\rangle \right]$$

$k=1$ term: $|0\rangle + e^{2\pi i \frac{x}{2}} |1\rangle$

$k=2$ term: $|0\rangle + e^{2\pi i \frac{x}{4}} |1\rangle$

notice: $x = [x_1 x_2 x_3 \cdots x_n]$

$$\frac{x}{2} = 0.x_1 x_2 \cdots x_{n-1}$$

$$\frac{x}{4} = 00 x_1 x_2 \cdots x_{n-2}$$

Final form:

$$\frac{1}{\sqrt{N}} \left(|0\rangle + e^{2\pi i \frac{x}{2}} |1\rangle\right) \otimes \left(|0\rangle + e^{2\pi i \frac{x}{4}} |1\rangle\right) \otimes \cdots \left(|0\rangle + e^{2\pi i \frac{x}{2^n}} |1\rangle\right)$$

went from $|x_1 x_2 \cdots x_n\rangle$ to

Example:

$n = 3$ qubits $\Rightarrow N = 2^3 = 8$

$|x\rangle = |5\rangle$

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

Notice: $2\pi i\left(\frac{5}{2}\right) = 2\pi i\left(\frac{2^2}{2} + \frac{1}{2}\right)$

$= 2\pi i\left(2 + \frac{1}{2}\right)$

since $e^{2\pi i z} = 1$ for any integer z,

$$e^{2\pi i\left(\frac{5}{2}\right)} = e^{2\pi i\left(2+\frac{1}{2}\right)} = e^{2\pi i\left(\frac{1}{2}\right)} = e^{\pi i} = -1$$

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

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

Let's write $y = \sum_{k=1}^{n} y_k 2^{n-k}$ $\qquad y = y_1 \cdots y_n = 2^{n-1} y_1 + \cdots + 2^0 y_n$

then $y/2^n = \sum_{k=1}^{n} y_k / 2^k$ and we have

$$|\tilde{x}\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i x \sum_{k=1}^{n} y_k/2^k} |y_1 y_2 \cdots y_n\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \prod_{k=1}^{n} e^{2\pi i x y_k/2^k} |y_1 y_2 \cdots y_n\rangle$$

remember, $\sum_{y=0}^{N-1} = \sum_{y_1=0}^{1} \sum_{y_2=0}^{1} \cdots \sum_{y_n=0}^{1}$

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

Notice that we went from

$|x\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle$ to

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

The Quantum Circuit that implements QFT

Notice that we went from

$|x\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle$ to

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

each qubit went from $|x_k\rangle$ to $|0\rangle + e^{2\pi i x/2^k}|1\rangle$.

Two observations:

(1) $|\tilde{x}\rangle$ contains terms like

$|00\cdots00\rangle$

$e^{2\pi i x/2^n}|00\cdots01\rangle$

$e^{2\pi i x/2^{n-1}}|00\cdots10\rangle$

$e^{2\pi i x/2^1}|10\cdots00\rangle$

(2) $e^{2\pi i \left[\frac{x}{2} + \frac{x}{2^2} + \cdots + \frac{x}{2^n}\right]}|1111\cdots1111\rangle$

$\hookrightarrow e^{\frac{2\pi i x}{2^1}} e^{\frac{2\pi i x}{2^2}} e^{\frac{2\pi i x}{2^3}} \cdots e^{\frac{2\pi i x}{2^n}}$

Hints:
- phase is qubit-dependent
- need to add up more components with more "1"s

Two ingredients needed:

(1) $H|x_k\rangle = \begin{cases} x_k=0 \to (|0\rangle + |1\rangle)/\sqrt{2} \\ x_k=1 \to (|0\rangle - |1\rangle)/\sqrt{2} \end{cases}$

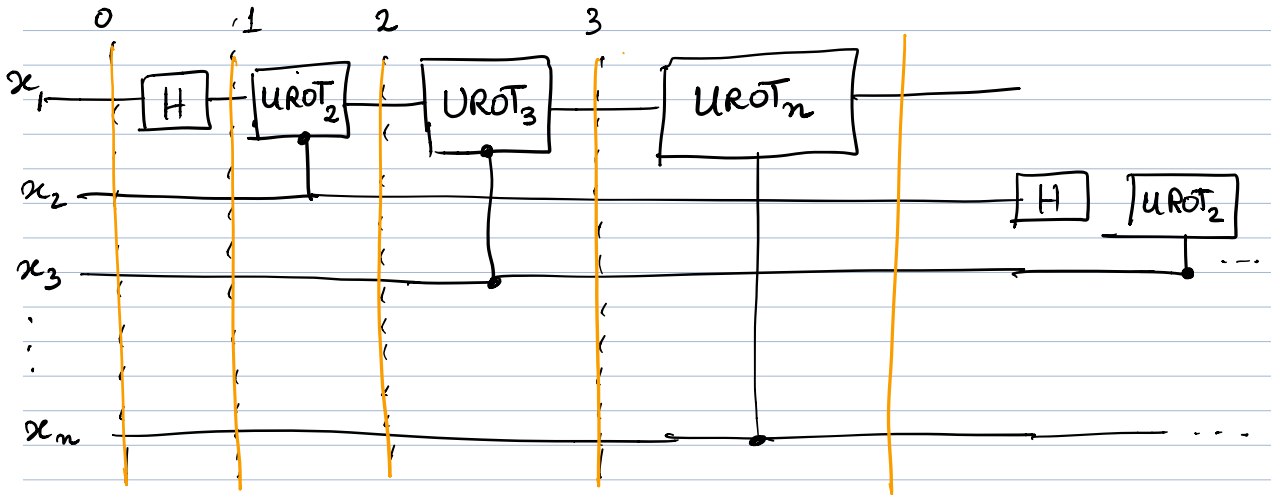
(x_k: 0 or 1)

$= (|0\rangle + \underbrace{e^{\pi i x_k}}_{= e^{\frac{2\pi i x_k}{2}}}|1\rangle)/\sqrt{2}$

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

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

applies phase $e^{2\pi i/2^k}$



step 0: $|x_1 x_2 \dots x_n\rangle$

step 1: $\left[|0\rangle + e^{\frac{2\pi i}{2} x_1} |1\rangle\right] \otimes |x_2 \dots x_n\rangle$

step 2: $\left[|0\rangle + e^{\frac{2\pi i}{2^2} x_2} e^{\frac{2\pi i}{2^1} x_1} |1\rangle\right] \otimes$

step 3: $\left[|0\rangle + e^{\frac{2\pi i}{2^3} x_3} e^{\frac{2\pi i}{2^2} x_2} e^{\frac{2\pi i}{2^1} x_1} |1\rangle\right] \otimes$

step n: $\left[|0\rangle + \underbrace{e^{\frac{2\pi i}{2^n} x_n} \cdots e^{\frac{2\pi i}{2^1} x_1}}_{\exp\left[2\pi i \left(\frac{x_n}{2^n} + \frac{x_{n-1}}{2^{n-1}} + \cdots + \frac{x_1}{2^1}\right)\right]} |1\rangle\right] \otimes$

recall: $x = 2^{n-1} x_1 + 2^{n-2} x_2 + \cdots + 2^0 x_n$

$\Rightarrow \frac{x_n}{2^n} + \cdots + \frac{x_1}{2^1} = \frac{x}{2^n}$

$\Rightarrow$ term above is $\exp\left[2\pi i \frac{x}{2^n}\right]$

$\Rightarrow$ after step n: $\left[|0\rangle + e^{\frac{2\pi i x}{2^n}} |1\rangle\right] \otimes |x_2 x_3 \dots x_n\rangle$

reversed order from derived form, but OK otherwise.