Week 6

→ A complex amplitude coefficient α:

$$\alpha_0 = A_0 e^{i(2\pi \underbrace{ft}_{\omega} + \phi_0)}$$

$|A_0|^2$ is the prob. of measure.

α_0 corresponding to the 0^{th} qubit

ϕ_0 initial phase

ft Frequency of the wave and the time passed

- A reminder that $e^{i\theta}$ part is just a phase, so it doesn't affect the measurement prob. directly.
- But the phases can be utilized in the form of constructive / destructive interference. [using superpos^n + entanglement]

→ Fourier Transform can be used to decompose an arbitrary wave function into its components of pure orthogonal (fourier basis) functions.
(for quantum)

$$\text{computational basis} \xrightarrow{QFT} \text{Fourier basis}$$

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

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

$$\vdots$$

$$\left(|0\rangle + e^{\frac{2\pi i}{2^n} x} |1\rangle\right) \equiv |\tilde{x}\rangle$$

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

→ Fourier basis is a way of encoding information in phases.

→ Phase estimation converts the phase information into amplitudes, which can be measured using many observations.

$$\rightarrow (ABC)^{\dagger} = C^{\dagger} B^{\dagger} A^{\dagger}$$

* Shor's Algo

$5 \div 3$ = quotient = 1 and remainder = 2

$5 \equiv 2 \pmod 3$ [5 and 2 are equivalent in modulo 3]

ex:

$x = 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9$

$x \equiv 1 \quad 2 \quad 0 \quad 1 \quad 2 \quad 0 \quad 1 \quad 2 \quad 0 \pmod 3$

$x \equiv y \pmod 3 \Rightarrow x = 3k + y$ for $k \in \mathbb{Z}$

int

→ Periodicity of modular arithmetic:

$x \equiv y \pmod N$ means $y \in \{0, \dots, N-1\}$

⇒ The Protocol: $N = pq$

(1) Pick a number "a" that is coprime with N.

(2) Find the 'order' r of the function $a^r \pmod N$

$=$ smallest r s.t. $a^r \equiv 1 \pmod N$

[see next page]

(3) if r is even :

$x \equiv a^{r/2} \pmod{N}$

if $x+1 \not\equiv 0 \pmod{N}$:

out of $\{p, q\}$, at least one is contained in $\left\{ \begin{array}{l} \gcd(x+1, N), \\ \gcd(x-1, N) \end{array} \right\}$

else: find another a

ex: Factoring 15

$\rightarrow 15 = [1\ 1\ 1\ 1]$ (four bits)

step-1: $a = 13$

step-2: find the period r in

$13^r \pmod{15}$

x in $r = 0, 1, 2, 3, \cdots, 13^x \pmod{15}$

$= 1, 13, 4, 7, 1, \ldots$

$\boxed{r = 4}$

$\therefore a^r \equiv 1 \pmod{N} \Rightarrow 4 = r$

step-3: $x = a^{r/2} \pmod{N} = 13^{4/2} \pmod{15}$

$= 4 \pmod{15}$

$x+1 = 4+1 = 5 \pmod{15}$

$\gcd(x+1, N) = \gcd(5, 15) = 5$

$\gcd(x-1, N) = \gcd(3, 15) = 3$

$\{p, q\} = \{3, 5\}$

→ By solving the periodicity r s.t.

$$a^r \equiv 1 \pmod{N},$$

we can find the factors of N.

* $f_{a,N}(x) \equiv a^x \pmod{N}$

$$U|y\rangle = |ay \bmod N\rangle$$

$$|x\rangle|w\rangle \xrightarrow{f_{a,N}} |x\rangle|w \oplus f_{a,N}(x)\rangle$$

→ Why $a^{r/2} \pmod{N} = x$ and sol^n could be a gcd of $\{x+1, N\}$ or/and $\{x-1, N\}$?

$$a^r \bmod N = 1$$

$$\therefore (a^r - 1) \bmod N = 0$$

$$(a^r - 1) = (a^{r/2} - 1)(a^{r/2} + 1)$$

↑
here, we need r to be even, else retry.