Quantum Fourier Transform

$x_i \longrightarrow y_j$ $\quad (i, j = 0, 1, 2, \ldots N-1$, $N = 2^n)$

$$y_j = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} e^{2\pi i x_j / N} x_i$$

or

$$\boxed{y_j = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} \omega^{x_j} x_i}$$

$$\begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{N-1} \end{pmatrix} = \frac{1}{\sqrt{N}} \begin{pmatrix} \omega^{0.0} & \omega^{0.1} & \cdots & \omega^{0.(N-1)} \\ \omega^{1.0} & \omega^{1.1} & \cdots & \omega^{1.(N-1)} \\ \vdots & & & \\ \omega^{(N-1).0} & \omega^{(N-1).1} & \cdots & \omega^{(N-1)^2} \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{pmatrix}$$

$$|\psi\rangle = \sum_x a_x |x\rangle$$

$$|\phi\rangle = U_{QFT} |\psi\rangle$$

$$\begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{N-1} \end{pmatrix} \xrightarrow{QFT} \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{N-1} \end{pmatrix}$$

$$\sum_x a_x |x\rangle \xrightarrow{QFT} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} a_x \frac{e^{2\pi i (xy)/N}}{\sqrt{N}} |y\rangle$$

Find QFT $\left\{ \dfrac{|0\rangle - |1\rangle}{\sqrt{2}} \right\}$

$\dfrac{|0\rangle - |1\rangle}{\sqrt{2}} = |\psi\rangle$ ← one qubit state

$n = 1$

$N = 2^n = 2$

$$U = \frac{1}{\sqrt{2}} \begin{pmatrix} \omega^0 & \omega^0 \\ \omega^0 & \omega^1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\omega^1 = e^{2\pi i/2} = e^{\pi i} = -1$$

$$H|+\rangle \longrightarrow |1\rangle$$

$$QFT\left\{\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right\} = |1\rangle$$

2. Find QFT of

$$|\psi\rangle = \sqrt{\frac{2}{N}} \sum_{x=0}^{N-1} \cos\left(\frac{2\pi x}{N}\right) |x\rangle$$

Solution

$$|\tilde{x}\rangle = \sum_x \sum_y a_x \frac{e^{2\pi i x y/N}}{\sqrt{N}} |y\rangle$$

$$U_{QFT}|\psi\rangle = \sqrt{\frac{2}{N}} \sum_{x=0}^{N-1} \cos\left(\frac{2\pi x}{N}\right) \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i x y/N} |y\rangle$$

$$= \frac{\sqrt{2}}{N} \sum_{y=0}^{N-1} \left(\sum_{x=0}^{N-1} \cos\left(\frac{2\pi x}{N}\right) e^{2\pi i x y/N} \right) |y\rangle$$

$$= \alpha_y |y\rangle$$

$$\frac{\sqrt{2}}{N} \sum_{x=0}^{N-1} \cos\left(\frac{2\pi x}{N}\right) e^{2\pi i x y/N}$$

$$= \sum_{x=0}^{N-1} \frac{\sqrt{2}}{N} \left[\frac{e^{2\pi i x/N} + e^{-2\pi i x/N}}{2} \right] e^{2\pi i x y/N}$$

$$= \frac{\sqrt{2}}{N} \sum_{x=0}^{N-1} \frac{e^{2\pi i x (y+1)/N} + e^{2\pi i x (y-1)/N}}{2}$$

1st term

$$A = \sum_{x=0}^{N-1} e^{2\pi i x (y+1)/N}$$

If $y = N-1$ then

$$A = \sum_{x=0}^{N-1} e^{2\pi i x} = \sum_{x=0}^{N-1} 1 = N$$

If $y \neq N-1$

$$A = 0$$

$$A = \begin{cases} N & y = N-1 \\ 0 & y \neq N-1 \end{cases}$$

Again $$B = \sum_{x=0}^{N-1} e^{2\pi i x (y-1)/N}$$

$y = 1$ $\quad B = N \; ; \; y = 1$

$\quad = 0 \; ; \; y \neq 1$

$$\frac{\sqrt{2}}{N} \sum_{x=0}^{N-1} \cos\left(\frac{2\pi x}{N}\right) e^{2\pi i x y/N}$$

$$= \frac{\sqrt{2}}{2N} \left(\underset{=}{A} + B \right)$$

$$= \frac{1}{\sqrt{2}N} \left\{ \begin{matrix} 0 & y \neq N-1 \\ N & y = N-1 \end{matrix} + \begin{matrix} 0 & y \neq 1 \\ N & y = 1 \end{matrix} \right\}$$

$$= \frac{1}{\sqrt{2}N} \begin{cases} N & \text{if } y = N-1 \text{ or } 1 \\ 0 & \text{if } y \neq N-1 \text{ or } 1 \end{cases}$$

Thus, $$\alpha_y = \frac{1}{\sqrt{2}} \left[\delta_{y,1} + \delta_{y,N-1} \right]$$

$$U_{QFT}|\psi\rangle = \frac{1}{\sqrt{2}}\left[\delta_{y,1} + \delta_{y,N-1}\right]|y\rangle$$

$$= \frac{1}{\sqrt{2}}\left[|1\rangle + |N-1\rangle\right]$$

3. Say $|\psi\rangle = \dfrac{|00\rangle + |01\rangle}{\sqrt{2}}$ is subjected to QFT after which the first qubit is measured. What is the probability of getting the state $|0\rangle$?

$n = 2, \quad N = 4$

Solution $|\psi\rangle = \dfrac{|00\rangle + |01\rangle}{\sqrt{2}} \equiv \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$

{ For simplicity I take
$|00\rangle \to |0\rangle$
$|01\rangle \to |1\rangle$

Here $n=2, \quad N = 4$

$$|\phi\rangle = U_{QFT}|\psi\rangle$$

$$= \sum_y \left(\sum_x a_x \frac{e^{2\pi i xy/N}}{\sqrt{N}} \right)|y\rangle = \sum_{y=0}^{3} \alpha_y |y\rangle$$

$$= \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle + \alpha_3|3\rangle$$

$$\equiv \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle$$

$$\alpha_y = \sum_{x=0}^{3} a_x \frac{e^{2\pi i xy/4}}{2}$$

$(y=0)$ $\quad \alpha_0 = \dfrac{a_0 + a_1 + a_2 + a_3}{2}$

$\Rightarrow$ The co-efficient of the state $|0\rangle = |00\rangle$ is $\alpha_0 = \dfrac{a_0 + a_1 + a_2 + a_3}{2}$

$$= \frac{1}{2}\left[\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} + 0 + 0\right]$$

$$= \frac{1}{\sqrt{2}}$$

$(y=1)$ $$\alpha_1 = \sum_{x=0}^{3} a_x \frac{e^{2\pi i x \cdot 1/4}}{2} = \frac{1}{2}\sum_{x=0}^{3} a_x e^{\pi i x/2}$$

$$= \frac{1}{2}\left(a_0 + a_1 e^{i\pi/2} + a_2 e^{2\pi i/2} + a_3 e^{3\pi i/2}\right)$$

$$= \frac{1}{2}\left(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}\, i\right) \qquad (a_2 = a_3 = 0)$$

So, the co-efficient of the state $|1\rangle = |01\rangle$ is

$$\alpha_1 = \frac{1}{2\sqrt{2}}(1+i)$$

$(y=2)$ $$\alpha_2 = \sum_{x=0}^{3} a_x \frac{e^{2\pi i x \cdot 2/4}}{2} = \sum_{x=0}^{3} a_x e^{\pi i x}$$

$$= \frac{1}{2}\left(a_0 + a_1 e^{\pi i} + a_2 e^{2\pi i} + a_3 e^{3\pi i}\right)$$

$$= \frac{1}{2}\left(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}(-1)\right) \qquad (a_2 = a_3 = 0)$$

$$= 0$$

$(y=3)$ $$\alpha_3 = \sum_{x=0}^{3} a_x \frac{e^{2\pi i x \cdot 3/4}}{2}$$

$$= \frac{1}{2}\left(a_0 + a_1 e^{3\pi i/2} + a_2 e^{3\pi i} + a_3 e^{9\pi i/2}\right)$$

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

$$= \frac{1}{2\sqrt{2}}(1-i)$$

Thus,

$$|\phi\rangle = U_{QFT}\,|\psi\rangle$$

$$= \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle$$

(Note: $00 \to 0$, $01 \to 1$, $10 \to 2$, $11 \to 3$)

$$\boxed{|\phi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{2\sqrt{2}}(1+i)\,|01\rangle + \frac{1}{2\sqrt{2}}(1-i)\,|11\rangle}$$

This is normalized!

So, the probability of getting the qubit $|0\rangle$ as a result of measurement is

$$\left|\frac{1}{\sqrt{2}}\right|^2 + \left|\frac{1}{2\sqrt{2}}(1+i)\right|^2$$

$$= \frac{1}{2} + \frac{1}{8} \times 2 = \frac{1}{2} + \frac{1}{4}$$

$$= \frac{6}{8} = \frac{3}{4} \;//$$

Shore's Factorization algorithm

$N = pq$ where p and q are primes

Euclid agorithm $\sqrt{N}$ steps

$$29083 = 229 \times 127$$

- Factorization : very hard
- checking : very easy

Euclid's algorithm

Say, we have two numbers 'a' and 'b'

Find the greatest common divisor of 'a' and 'b' (g.c.d)

say g.c.d. of $(a, b) = c$

$a = mc$
$b = nc$ m, n are integers

Say a is divided by b and remainder is r :

$$r = a - bq \quad , b < a$$

$$\begin{array}{r|l} & q \\ b & a \\ & bq \\ \hline & r \end{array}$$

c also divides r :

$$\frac{r}{c} = \frac{a}{c} - \frac{b}{c} q = m - nq$$

In Euclid's algorithm

(i) Start with a long division

$$\frac{a}{b} = q_1 \text{ , say}$$

remainder $r_1 = a - bq_1$

$$\frac{b}{r_1} = q_2$$

$$r_2 = b - q_2 r_1$$

$$q_3 = \frac{r_1}{r_2}$$

$$\vdots$$

$$\boxed{q_{n+1} = \frac{r_{n-1}}{r_n}}$$

If there is no remainder, then $r_n = c$

$a = 75$

$b = 24$

Shor suggested that one should solve an equivalent problem.

This equivalent problem is called period finding.

↳ QFT

Period finding

1. Choose a random number m such that $m < N$

- m should be coprime with N

$\Downarrow$

m and N don't have any common factor bet^n them

$g.c.d(m, N) = 1$

$N = 21$

$m \neq 6$

2. Find various powers of m corresponding to N

Define function $f : N \rightarrow N$ such that

$$F_N(a) = m^a \bmod N$$

The smallest value of a $(= p)$ for which

$$m^p = 1 \bmod N$$

is called the period of this function.

Say $N = 21$

1. Choose $m = 2$

2.
$$2^1 = 2$$
$$2^2 = 4$$
$$2^3 = 8$$
$$2^4 = 16 = 16 \bmod 21$$
$$2^5 = 32 = 11 \bmod 21$$
$$2^6 = 64 = 1 \bmod 21$$

period $= 6$

choosing $m = 2$ for $N = 21$
we find the period $p = 6$.

$m \in \{2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$