The Quantum Fourier Transform and Its Applications

The Quantum Fourier Transform

discrete FT $y_k = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} x_j e^{\frac{2\pi}{N} ijk}$

QFT $|j\rangle = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{\frac{2\pi}{N} ijk}|k\rangle$

QFT is unitary:

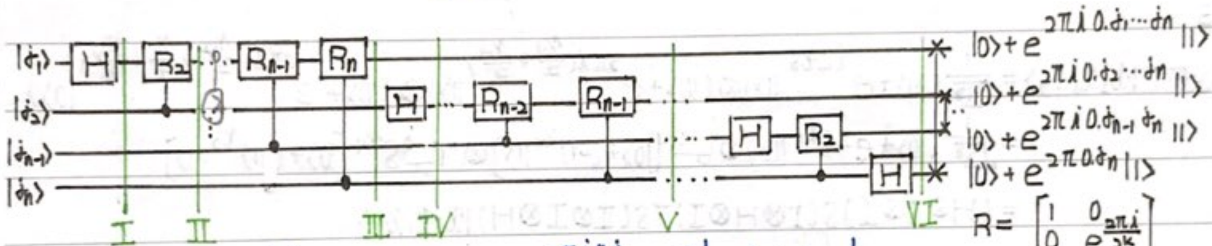
$$\langle m|j\rangle = \frac{1}{N}\sum_{k,n=0}^{N-1} e^{-\frac{2\pi}{N} imn} e^{\frac{2\pi}{N} ijk}\langle n|k\rangle = \frac{1}{N}\sum_{k,n=0}^{N-1} e^{-\frac{2\pi}{N} imn} e^{-\frac{2\pi}{N} ijk}\delta_{n,k}$$

$$= \frac{1}{N}\sum_{k=0}^{N-1} e^{\frac{2\pi i}{k}(j-m)k} = \delta_{j,m}$$

For $N=2^n$, $|00\cdots0\rangle$, $|00\cdots0\rangle \to \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1} e^{\frac{2\pi}{2^n} ik\cdot 0}|k\rangle = \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}|k\rangle$

define $j = j_1 2^{n-1} + j_2 2^{n-2} + \dots + j_n 2^0$ $\quad 0.j_l j_{l+1}\cdots j_m = \frac{1}{2} j_l + \frac{1}{4} j_{l+1} + \dots + \frac{1}{2^{m-l+1}} j_m$

$$\Rightarrow |j_1\cdots j_n\rangle \to \frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)\cdots(|0\rangle + e^{2\pi i 0.j_1 j_2\cdots j_n}|1\rangle)}{\sqrt{2^n}}$$



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

I $\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0.j_1}|1\rangle)|j_2\cdots j_n\rangle$ $\qquad e^{2\pi i 0.j_1} = {-1 \atop +1}$ when $j_1 = {1 \atop 0}$

II $\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0.j_1 j_2}|1\rangle)|j_2\cdots j_n\rangle$

III $\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0.j_1 j_2\cdots j_n}|1\rangle)|j_2\cdots j_n\rangle$

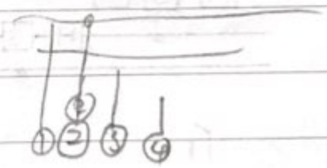
IV $\frac{1}{2}(|0\rangle + e^{2\pi i 0.j_1 j_2\cdots j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_2}|1\rangle)|j_3\cdots j_n\rangle$

V $\frac{1}{2}(|0\rangle + e^{2\pi i 0.j_1\cdots j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_2\cdots j_n}|1\rangle)|j_3\cdots j_n\rangle$

VI $\frac{1}{\sqrt{2^n}}(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle)\cdots(|0\rangle + e^{2\pi i 0.j_1\cdots j_n}|1\rangle)$

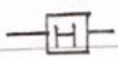
c t

(3,0)
(3,1)
(3,2)
(1,3)



$n=1$

QFT$|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i x}|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle)$ $\qquad \begin{cases} x=0 & \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \\ x=1 & \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \end{cases}$ H gate



NO.

DATE / /

n=2

$$QFT|x\rangle = QFT|x_1x_0\rangle = \frac{1}{2}\sum_{y=0}^{3} e^{\frac{1}{4}2\pi i x(2y_1+y_0)}|y_1y_0\rangle = \frac{1}{2}\sum_{y_1} e^{\frac{1}{2}2\pi i x y_1}|y_1\rangle \otimes \sum_{y_0} e^{\frac{1}{4}2\pi i x y_0}|y_0\rangle$$

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

$$= \frac{1}{2}(|0\rangle + e^{\pi i(2x_1+x_0)}|1\rangle) \otimes (|0\rangle + e^{\frac{1}{2}i\pi(2x_1+x_0)}|1\rangle)$$

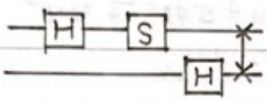
$$= \frac{1}{2}(|0\rangle + e^{i\pi x_0}|1\rangle) \otimes (|0\rangle + e^{\frac{3\pi}{\pi}ix_1} e^{\frac{1}{2}\pi i x_0}|1\rangle)$$

$$= \frac{1}{2}(|0\rangle + e^{\pi i x_0}|1\rangle) \otimes e^{\frac{1}{2}\pi i x_0}(|0\rangle + e^{\pi i x_1})|1\rangle$$

$$= \frac{1}{2}(|0\rangle + (-1)^{x_0}|1\rangle \otimes S^{x_0}(|0\rangle + (-1)^{x_1}|1\rangle)$$

$$S^{x_0}\begin{cases} x_0=0, & I \\ x_0=1 & e^{\frac{1}{2}\pi i}\end{cases}$$

$$\Rightarrow (H\otimes I)CS(I\otimes H)|x_0,x_1\rangle = (H\otimes I)CS(I\otimes H)\,SWAP|x_1x_0\rangle$$



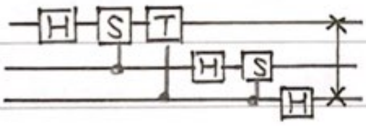
n=3

$$QFT|x_2x_1x_0\rangle = \frac{1}{\sqrt{2^3}}(|0\rangle + e^{i\pi x_0}|1\rangle) \otimes (|0\rangle + e^{2\pi i(\frac{x_1}{2}+\frac{x_0}{4})}|1\rangle) \otimes (|0\rangle + e^{2\pi i(\frac{x_2}{2}+\frac{x_1}{4}+\frac{x_0}{8})}|0\rangle)$$

$$= \frac{1}{\sqrt{2^3}}(|0\rangle + (-1)^{x_0}|1\rangle) \otimes S^{x_0}[|0\rangle + (-1)^{x_1}|1\rangle] \otimes T^{x_0}S^{x_1}[|0\rangle + (-1)^{x_2}|1\rangle]$$

$$= (H\otimes I\otimes I)S(I\otimes H\otimes I)TS(I\otimes I\otimes H)|x_0x_1x_2\rangle$$

$$= (H\otimes I\otimes I)S(I\otimes H\otimes I)TS(I\otimes I\otimes H)\,SWAP|x_2x_1x_0\rangle$$

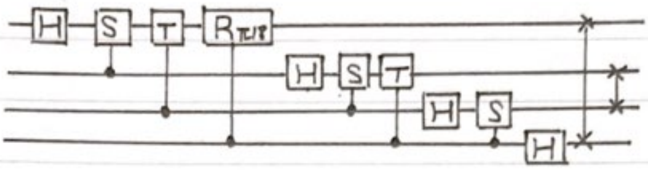


$$\frac{1}{\sqrt{8}}\begin{bmatrix} 1 & & & \cdots & & & & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ \vdots & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ \vdots & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{bmatrix}$$

NO.

DATE / /

$n=4$



for n bite, need $\frac{n(n+1)}{2}$ gates are required plut SWAP $\Rightarrow O(n^2)$
at most $\frac{n}{2}$ SWAP

classical FT $O(n2^n)$

Inverse QFT

inverse discrete FT $x_i = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{-\frac{2\pi}{N} ijk} y_k$

then $|x\rangle = \sum_{j=0}^{N-1} x_i |j\rangle = \sum_{j=0}^{N-1} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{-\frac{2\pi}{N} ijk} |j\rangle$

$= \sum_{k=0}^{N-1} y_k \left(\sum_{j=0}^{N-1} \frac{1}{\sqrt{N}} e^{-\frac{2\pi}{N} ijk} |j\rangle \right)$

$|k\rangle \to \sum_{j=0}^{N-1} \frac{1}{\sqrt{N}} e^{-\frac{2\pi}{N} ijk} |j\rangle = \frac{1}{\sqrt{2^n}} (|0\rangle + e^{-2\pi i 0.k_n} |1\rangle) \otimes (|0\rangle + e^{-2\pi i 0.k_{n-1} k_n} |1\rangle) \cdots\cdots$

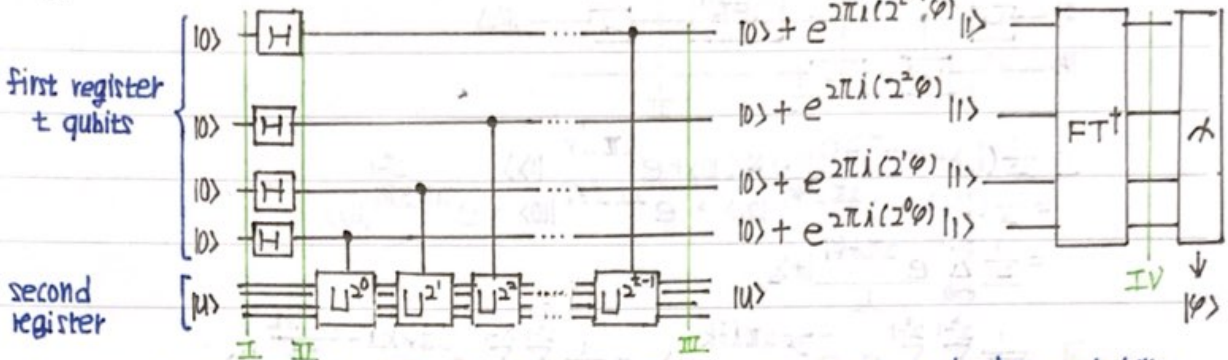
just change the input into the output and vice-versa

NO.

DATE

Phase Estimation

suppose $\underset{\text{unitary}}{U}|u\rangle = e^{2\pi i\varphi}|u\rangle$ estimate φ



choose t depends on the number of digits of accuracy we wish and what probability we wish the phase estimation procedure to be successful

u as many qubits as is necessary to store $|u\rangle$

$$\frac{1}{\sqrt{2^t}}(|0\rangle+e^{2\pi i 2^{t-1}\varphi}|1\rangle)(|0\rangle+e^{2\pi i 2^{t-2}\varphi}|1\rangle)\cdots(|0\rangle+e^{2\pi i 2^0\varphi}|1\rangle) = \frac{1}{\sqrt{2^t}}\sum_{k=0}^{2^t-1} e^{2\pi i\varphi k}|k\rangle$$

$$|j\rangle|u\rangle \to |j\rangle U^{j_n 2^0}\cdots U^{j_3 2^{n-3}}U^{j_2 2^{n-2}}U^{j_1 2^{n-1}}|u\rangle = |j\rangle U^{j_1 2^{n-1}}U^{j_2 2^{n-2}}\cdots U^{j_n 2^0}|u\rangle$$
$$= |j\rangle U^{j_1 j_2 j_3\cdots j_n}|u\rangle = |j\rangle U^{j}|u\rangle$$

$$\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1} e^{2\pi i\varphi j}|j\rangle|u\rangle \to |\tilde{\varphi}\rangle|u\rangle$$

I $|0\rangle|u\rangle$

II $\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|u\rangle$

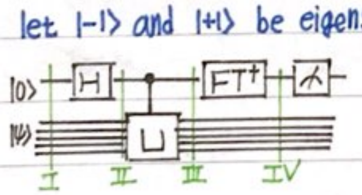
III $\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle U^j|u\rangle = \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1} e^{2\pi i j\varphi_u}|j\rangle|u\rangle$

IV $|\tilde{\varphi}_u\rangle|u\rangle$

V $\tilde{\varphi}_u$

Example U with eigenvalues ±1

let $|-1\rangle$ and $|+1\rangle$ be eigenstates of U with eigenvalues ±1



$|\psi\rangle = \sum_{j=\pm1} C_j|j\rangle$

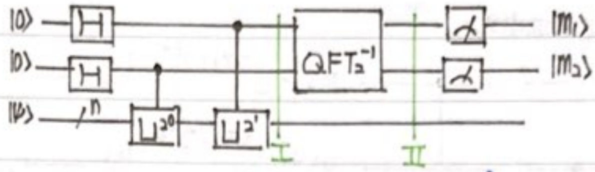
I $\sum_{j=\pm1} C_j|0\rangle|j\rangle$

II $\sum_{j=\pm1} C_j\frac{1}{\sqrt{2}}\sum_{k=0,1}|k\rangle|j\rangle$

III $\sum_{j=\pm1} C_j\frac{1}{\sqrt{2}}(|0\rangle+e^{2\pi i\varphi_j}|1\rangle)|j\rangle$

IV $\sum_{j=\pm1} C_j|\varphi_j\rangle|j\rangle$

Example



$$\text{I}\quad \frac{1}{2}(|0\rangle + e^{2\pi 2\varphi i}|1\rangle)\otimes(|0\rangle + e^{2\pi 2^0\varphi i}|1\rangle)$$

$$= \frac{1}{2}(|00\rangle + e^{2\pi 2^0\varphi i}|01\rangle + e^{2\pi 2^1\varphi i}|10\rangle + e^{2\pi \overset{2^2-1}{3}\varphi i}|11\rangle)$$

$$= \frac{1}{2}\sum_{j=0}^{2^2-1} \underbrace{e^{2\pi j\varphi i}}_{a_j}|j\rangle_2$$

$$\text{II}\quad \frac{1}{\sqrt{2^2}}\sum_{j=0}^{2^2-1}\sum_{k=0}^{2^2-1} a_k e^{-\frac{1}{2^2}2\pi i jk}|j\rangle_2 = \frac{1}{4}\sum_{j=0}^{2^2-1}\sum_{k=0}^{2^2-1} e^{2\pi\varphi k i - \frac{2\pi i jk}{2^2}}|j\rangle_2$$

$$= \frac{1}{4}\sum_{j=0}^{3}\sum_{k=0}^{3} e^{-\frac{2\pi k i}{2^2}(j-2^2\varphi)}|j\rangle_2$$

$$\Rightarrow \frac{1}{2^m}\sum_{j=0}^{2^m-1}\sum_{k=0}^{2^m-1} e^{-\frac{2\pi k i}{2^m}(\overset{l}{j}-2^m\varphi)}|j\rangle_m \otimes |\varphi\rangle \text{ --- (1)}$$

choose $c = [2^m\varphi + \frac{1}{2}]$ let $d = \left|\frac{2^m\varphi - c}{2^m}\right| = \left|\varphi - \frac{c}{2^m}\right|$

$$(1) = \frac{1}{2^m}\sum\sum e^{-\frac{2\pi k i}{2^m}(j-c)} e^{2\pi d k i}|j\rangle_m$$

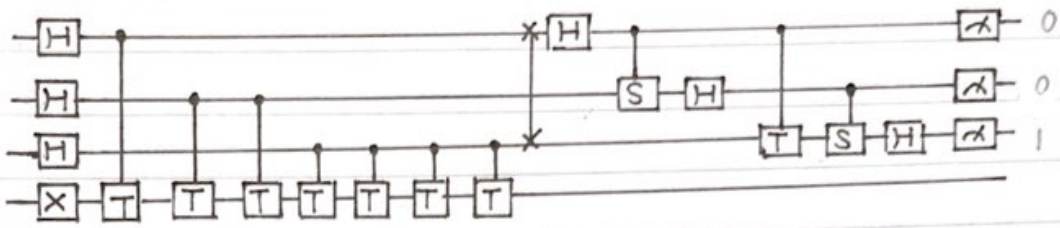
$$P(c) = \left|\frac{1}{2^m}\sum_{k=0}^{2^m-1} e^{-\frac{2\pi k i}{2^m}(c-c)} e^{2\pi d k i}\right|^2 = \left|\frac{1}{2^m}\sum e^{2\pi d k i}\right|^2 = \frac{1}{2^{2m}}\left|\sum_{k=0}^{2^m-1} e^{2\pi d k i}\right|^2$$

if $d=0$, $P(c)=1$ when $\varphi = \frac{c}{2^m}$ is a rational number

if $d\neq 0$ $P = \frac{4}{\pi^2}$

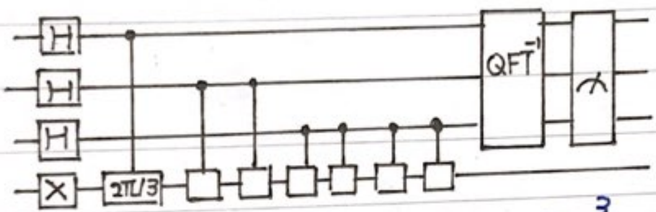
	$j=0$	$j=1$	$j=2$	$j=3$
$k=0$	$\|00\rangle$	$\|01\rangle$	$\|10\rangle$	$\|11\rangle$
$k=1$	$e^{+\frac{1}{2}\pi i 4\varphi}\|00\rangle$	$e^{+\frac{1}{2}\pi i(1-4\varphi)}\|01\rangle$	$e^{\frac{1}{2}\pi(2-4\varphi)}\|10\rangle$	$e^{\frac{1}{2}\pi(3-4\varphi)}\|11\rangle$
$k=2$	$e^{+\pi i 4\varphi}\|00\rangle$	$e^{\pi i(1-4\varphi)}\|01\rangle$	$e^{\pi i(2-4\varphi)}\|10\rangle$	$e^{\pi i(3-4\varphi)}\|11\rangle$
$k=3$	$e^{+\frac{3}{2}\pi i 4\varphi}\|00\rangle$	$e^{\frac{3}{2}\pi i(1-4\varphi)}\|01\rangle$	$e^{\frac{3}{2}\pi i(2-4\varphi)}\|10\rangle$	$e^{\frac{3}{2}\pi i(3-4\varphi)}\|11\rangle$

for example : $T|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = e^{\frac{i\pi}{4}} |1\rangle$, $\varphi = \frac{1}{8}$



$j = \frac{1}{2^0} = 8\varphi$, $\varphi = \frac{1}{8}$

a gate which $\varphi = \frac{1}{3}$



69.7% $011 \Rightarrow 3$, $j = 3 = 8\varphi$, $\varphi = \frac{3}{8}$

16.8% $010 \Rightarrow 2$, $j = 2 = 8\varphi$, $\varphi = \frac{1}{4}$

Applications: Order-Finding and Factoring

Order-finding

for positive integers x and N with no common factors and $x<N$, then $x^r = 1 \pmod N$, $r \le N$ (order of x mod N)

for example $x=5$, $N=21$ $\gcd(a,N)=1$

$$5 \div 21 = 0 \cdots 5 \qquad 5^4 \div 21 = 29 \cdots 16$$
$$5^2 \div 21 = 1 \cdots 4 \qquad 5^5 \div 21 = \cdots 17 \Rightarrow r=6$$
$$5^3 \div 21 = 5 \cdots 20 \qquad 5^6 \div 21 = \cdots 1$$
$$5^7 \div 21 = \cdots 5$$

$f_x(a) = x^a \bmod N$, $f_x(a) = f_x(a+r)$

$x^r \equiv 1 \bmod N \Rightarrow x^r - 1 \equiv 0 \bmod N$, $(x^{\frac{r}{2}}-1)(x^{\frac{r}{2}}+1) = 0 \bmod N \Rightarrow r$ be even

define $U|y\rangle = |xy \bmod N\rangle$ $\qquad U^2|y\rangle = |x^2 y \bmod N\rangle$

define $|u_s\rangle = \frac{1}{\sqrt r}\sum_{k=0}^{r-1} e^{-\frac{2\pi i s k}{r}} |x^k \bmod N\rangle$

$$U|u_s\rangle = U\left(\frac{1}{\sqrt r}\sum_{k=0}^{r-1} e^{-\frac{2\pi k i s}{r}} |a^{k+1} \bmod N\rangle\right) = \frac{1}{\sqrt r}\sum_{k=0}^{r-1} e^{-\frac{2\pi k s i}{r}} |a^{k+1} \bmod N\rangle$$
$$= \frac{1}{\sqrt r}\sum_{k=0}^{r-1} e^{-\frac{2\pi k s i}{r}} |a^{k+1} \bmod N\rangle = \frac{1}{\sqrt r}\sum_{k=0}^{r-1} e^{-\frac{2\pi (k+1-1) s i}{r}} |a^{k+1} \bmod N\rangle$$
$$= \frac{1}{\sqrt r}\sum_{k=0}^{r-1} e^{-\frac{2\pi (k+1) s i}{r}} e^{-\frac{2\pi (-1) s i}{r}} |a^{k+1} \bmod N\rangle = e^{\frac{2\pi i s}{r}} \frac{1}{\sqrt r}\sum_{k=0}^{r-1} e^{\frac{2\pi (k+1) s i}{r}}$$
$$= e^{\frac{2\pi i s}{r}} |u_s\rangle$$

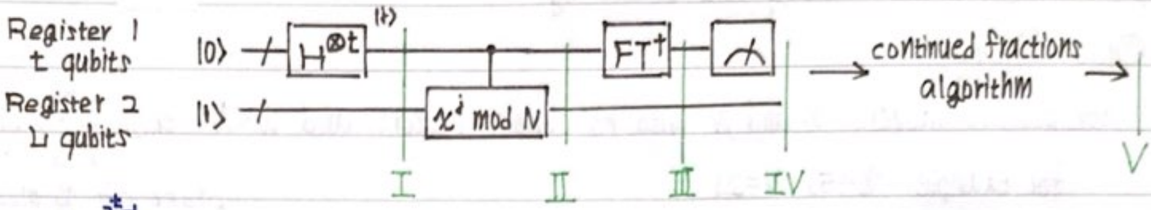
$$\frac{1}{\sqrt r}\sum_{s=0}^{r-1} |u_s\rangle = \frac{1}{\sqrt r}\sum_{s=0}^{r-1} e^{\frac{2\pi i s k}{r}} |u_s\rangle = \frac{1}{r}\sum_{s=0}^{r-1}\sum_{k'=0}^{r-1} \underbrace{e^{\frac{2\pi i s}{r}(k-k')}}_{r\delta_{kk'}} |x^{k'} \bmod N\rangle$$

or $\frac{1}{r}\sum\underbrace{\sum e^{-\frac{2\pi i s k}{r}}}_{r\delta_{k0}}$

$$= \sum_{k'=0}^{r-1} \delta_{kk'} |x^{k'} \bmod N\rangle = |x^k \bmod N\rangle$$
$$= |x^0 \bmod N\rangle = |1\rangle \text{ if } k'=0$$

we wish to compute the transformation

$$|z\rangle|y\rangle \rightarrow |z\rangle U^{z_t 2^{t-1}} \cdots U^{z_1 2^0}|y\rangle = |z\rangle|x^{z_t 2^{t-1}} \times \cdots \times x^{z_1 2^0} y \bmod N\rangle$$
$$= |z\rangle|x^z y \bmod N\rangle$$



I $\quad \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|1\rangle$

II $\quad \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|x^j \bmod N\rangle \approx \frac{1}{\sqrt{r2^t}}\sum_{s=0}^{r-1}\sum_{j=0}^{2^t-1} e^{\frac{2\pi i s j}{r}}|j\rangle|u_s\rangle$

III $\quad \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|\widetilde{s/r}\rangle|u_s\rangle$

IV $\quad \widetilde{\frac{s}{r}}$

V $\quad r$

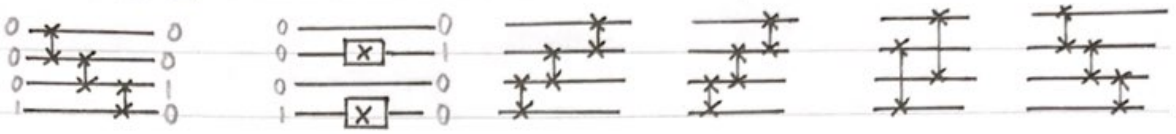
NO.

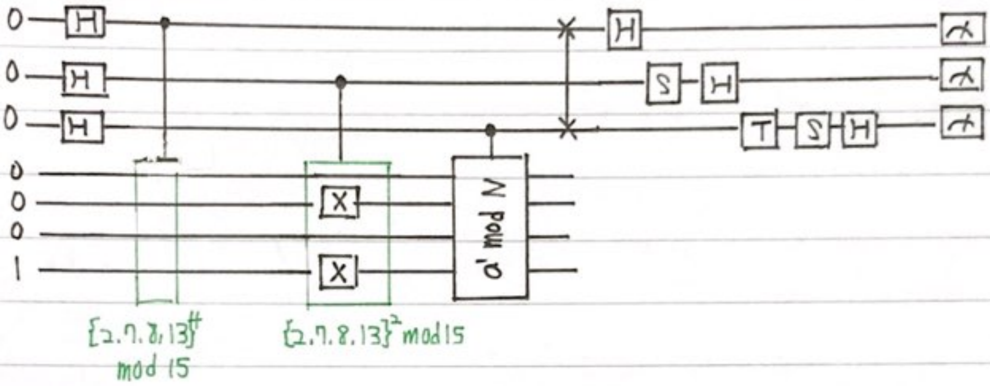
DATE

Application : factoring

for example $N=15$

$2^1 \bmod 15 = 2$ $\quad$ $2^2 \bmod 15 = 4$ $\quad$ 7^1 md 15 $\quad$ 8^1 mod 15 $\quad$ 11^1 mod 15 $\quad$ 13^1 mod 15





II : $\frac{1}{\sqrt{2^t}}\sum_{k=0}^{2^t-1}|k\rangle|x^k \bmod N\rangle = \frac{1}{\sqrt{2^t}}(|0\rangle|1\rangle+|1\rangle|7\rangle+|2\rangle|4\rangle+|3\rangle|13\rangle+|4\rangle|1\rangle+|5\rangle|7\rangle+|6\rangle|4\rangle+\cdots)$

IV maybe $\sqrt{\frac{4}{2^t}}(|2\rangle \underbrace{+}_{4} |6\rangle \underbrace{+}_{4} |10\rangle \underbrace{+}_{4} |14\rangle \underbrace{+}_{4} \cdots) \Rightarrow r=4$

$4 \div 2 = 2$, $\gcd[(7^2-1),15]=3$
$\gcd(7^2+1, 15)=5$ $\Rightarrow 15 = 5 \times 3$ (if $N=7$)