Nam Nguyen

Question 1

- When the first qubit is $|0\rangle$ we do not apply U

  $|1\rangle$ we apply U on $|\varphi\rangle$

then output state is

$$\alpha|0\rangle|\varphi\rangle + \beta|1\rangle U|\psi\rangle$$

$$= \alpha|0\rangle|\varphi\rangle + \beta|1\rangle e^{2\pi i\omega}|\varphi\rangle$$

$$= \left(\alpha|0\rangle + \beta e^{2\pi i\omega}|1\rangle\right)|\varphi\rangle$$

- $J \leq 1$ with $J = 0 \Rightarrow U^{2^J} = U^{2^0} = U$

  then output state is $|\phi\rangle = \left(\alpha|0\rangle + \beta e^{2\pi i\omega}|1\rangle\right)|\varphi\rangle$

$J = 1 \Rightarrow U^{2^J} = U^2$, then $U^2|\varphi\rangle = e^{2\pi i \cdot 2\omega}|\varphi\rangle$

thus, output state is $\left(\alpha|0\rangle + \beta e^{2\pi i(2\omega)}|1\rangle\right)|\varphi\rangle$

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

$$= \frac{1}{\sqrt{2^2}} \left(e^{2\pi i w \cdot 0} |0\rangle + e^{2\pi i w} |1\rangle + e^{2\pi i 2w} |2\rangle + e^{2\pi i 3w} |3\rangle \right)$$

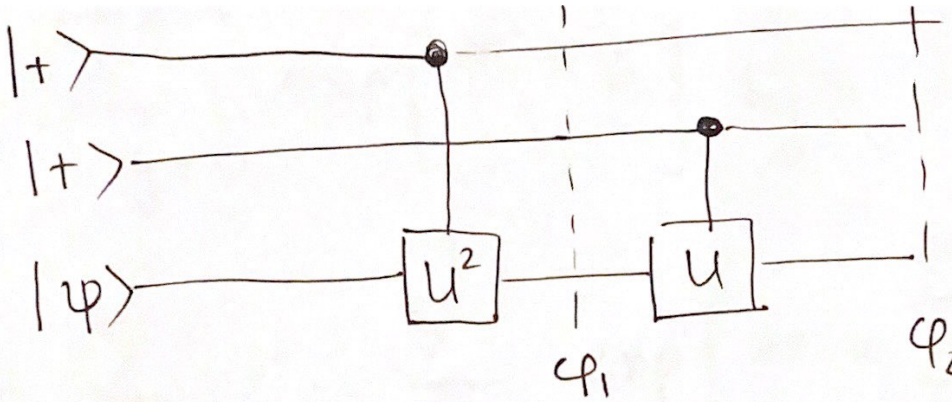
$$= \frac{1}{\sqrt{2^2}} \left[|00\rangle + e^{2\pi i w} |01\rangle + e^{2\pi i 2w} |10\rangle + e^{2\pi i 3w} |11\rangle \right]$$

$$= \frac{1}{\sqrt{2^2}} \left[\left(|0\rangle \left(|0\rangle + e^{2\pi i w} |1\rangle \right) + e^{2\pi i 2w} |1\rangle \left(|0\rangle + e^{2\pi i w} |1\rangle \right) \right) \right.$$

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

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

•



We have $|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$

$$|\varphi_1\rangle = \frac{|0\rangle + e^{2\pi i (2\omega)}|1\rangle}{\sqrt{2}}\,|\varphi\rangle$$

$$|\varphi_2\rangle = \left(\frac{|0\rangle + e^{2\pi i (2\omega)}|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + e^{2\pi i \omega}|1\rangle}{\sqrt{2}}\right)|\varphi\rangle$$

by previous part $\frac{1}{\sqrt{2^2}}\sum_{y=0}^{2^2-1} e^{2\pi i \omega y}|y\rangle$ ← superposition over 2 qubits

thus the output state is $\frac{1}{\sqrt{2^2}}\sum_{y=0}^{2^2-1} e^{2\pi i \omega y}|y\rangle|\varphi\rangle$

$$\bullet \quad \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} \exp\left[2\pi i \omega y\right] |y\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{y_1=0}^{1} \cdots \sum_{y_n=0}^{1} \exp\left(2\pi i \omega \sum_{l=1}^{n-1} y_l 2^l\right) |y_1 \cdots y_n\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{y_1=0}^{1} \cdots \sum_{y_n=0}^{1} \bigotimes_{l=1}^{n-1} e^{2\pi i \omega y_l 2^l} |y_l\rangle$$

$$= \frac{1}{\sqrt{2^n}} \bigotimes_{l=0}^{n-1} \left[\sum_{y_l=0}^{1} e^{2\pi i \omega y_l 2^l} |y_l\rangle \right]$$

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

$$= \frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{2\pi i \omega} |1\rangle\right) \left(|0\rangle + e^{2\pi i \omega 2^1} |1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i \omega 2^{n-1}} |1\rangle\right)$$

thus; RHS $= \left(\frac{|0\rangle + e^{2\pi i 2^{n-1}\omega}|1\rangle}{\sqrt{2}}\right) \cdots \left(\frac{|0\rangle + e^{2\pi i \omega}|1\rangle}{\sqrt{2}}\right)$

- At slice 1; output state is

$$|\varphi_1\rangle = \frac{|0\rangle + e^{2\pi i (2^{n-1} w)} |1\rangle}{\sqrt{2}} |\varphi\rangle$$

→ At slice 2; the output is

$$(CU^{2^{n-2}})\left(|+\rangle^{\otimes n} |\varphi_1\rangle\right)$$

$$= \frac{|0\rangle + e^{2\pi i 2^{n-2} w} |1\rangle}{\sqrt{2}} \cdot \frac{|0\rangle + e^{2\pi i 2^{n-1} w} |1\rangle}{\sqrt{2}} |\varphi\rangle$$

→ At the end of the circuit we have

$$\left(\frac{|0\rangle + e^{2\pi i (2^{n-1} w)} |1\rangle}{\sqrt{2}}\right) \cdots \left(\frac{|0\rangle + e^{2\pi i (w)} |1\rangle}{\sqrt{2}}\right) |\varphi\rangle$$

$$//$$

$$\left(\text{by previsous part}\right) \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n - 1} e^{2\pi i w y} |y\rangle \quad |\varphi\rangle$$

Question2

- If $s \geq N$; $U_a = I$, thus for $|s\rangle \neq |s'\rangle$

  then trivially $I|s\rangle \neq I|s'\rangle$

  $\Leftrightarrow U_a|s\rangle \neq U_a|s'\rangle$

If $s < N$; for $|s\rangle \neq |s'\rangle$ (*)

$U_a|s\rangle = |sa \bmod N\rangle$

$U_a|s'\rangle = |s'a \bmod N\rangle$

Suppose $U_a|s\rangle = U_a|s'\rangle \Leftrightarrow |sa \bmod N\rangle = |s'a \bmod N\rangle$

$\Leftrightarrow (s-s')a \bmod N \equiv 0$

a is invertible , then there exist b, s.t. $ab \bmod N = 1$

thus $a \bmod N$ cannot $= 0$

thus $(s-s') \bmod N \equiv 0$, and $s, s' < N$

then $|s\rangle = |s'\rangle$ (contradict with (*)) $\Rightarrow U|s\rangle \neq U|s'\rangle$

- Show that U_a is unitary.

We have for $0 \leq z, z' \leq N-1$

$$\langle z' | U_a^\dagger U_a | z \rangle = \left(\langle z' | U_a^\dagger \right) \left(U_a | z \rangle \right)$$

$$= \langle z'a \bmod N \mid za \bmod N \rangle$$

Since a is invertible modulo N

then if $z'a \equiv za \bmod N$

$$\Rightarrow \quad z' \equiv z \bmod N$$

$$\Rightarrow \langle z' | U_a^\dagger U_a | z \rangle = \langle z'a | za \rangle = \langle z' | z \rangle$$

$$\Rightarrow \quad U_a^\dagger U_a = \underline{I}$$

- $\left(U_a^\dagger U_a \right) U_a^{-1} = U_a^{-1} \Leftrightarrow U_a^\dagger \underbrace{\left(U_a U_a^{-1} \right)}_{\underline{I}} = U_a^{-1}$

$$\Leftrightarrow \quad U_a^\dagger \underline{I} = U_a^{-1} \Leftrightarrow U_a^\dagger = U_a^{-1} \Rightarrow U_a U_a^{-1} = U_a U_a^\dagger = \underline{I}$$

- With $|u_k\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-2\pi i \frac{k}{r} s} |a^s \bmod N\rangle$

we have $U_a |u_k\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-2\pi i \frac{k}{r} s} |a^{s+1} \bmod N\rangle$

$= \exp\left[\frac{2\pi i k}{r}\right] \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-2\pi i \frac{k}{r} s} |a^s \bmod N\rangle$

$= |u_k\rangle$

thus, $U_a |u_k\rangle = \exp\left[\frac{2\pi i k}{r}\right] |u_k\rangle$

thus; $|u_k\rangle$ is an eigenvector of U_a

with corresponding eigenvalue $\exp\left[\frac{2\pi i k}{r}\right]$

- $\langle 1 | \left(\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |u_k\rangle \right)$

$$= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \langle 1 | u_k \rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \langle 1 | I | u_k \rangle$$

$$= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \left(\langle 1 | u_a^\dagger \right) \left(u_a | u_k \rangle \right)$$

$$= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \left(u_a | 1 \rangle \right)^\dagger \lambda_k | u_k \rangle$$

$$= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \langle a \cdot 1 \bmod N | \exp\left[\frac{2\pi i k}{r} \right] \left(\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \exp(\right.$$

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

$$= \frac{1}{r} \sum_{k=0}^{r-1} \exp\left[\frac{2\pi i k}{r} \right] \sum_{s=0}^{r-1} e^{-\frac{2\pi i k}{r} s} \langle a \bmod N | a^s \bmod N \rangle$$

if $S \neq 1 \rightarrow \langle a \bmod N | a^S \bmod N \rangle = 0$

$$\Rightarrow RHS = \frac{1}{r} \sum_{k=0}^{r-1} \exp\left[\frac{2\pi i k}{r}\right] \exp\left[-\frac{2\pi i k \cdot 1}{r}^{S}\right]$$

$\langle a \bmod N | \overset{1}{a} \bmod N \rangle$

$$= \frac{1}{r} \sum_{k=0}^{r-1} \exp(0) = \frac{1}{r} \sum_{k=0}^{r-1} \overset{1}{1} = \frac{r}{r} = 1$$

- We have $\langle 1 | \left(\frac{1}{\sqrt{r}} \sum_{k=0}^{r} |u_k\rangle \right) = 1$

Let $\frac{1}{\sqrt{r}} \sum_{k=0}^{r} |u_k\rangle = |b\rangle \Rightarrow \langle 1|b\rangle = 1$

~~so $\langle 1|b\rangle = 1 = \langle 1|1\rangle$~~

If $|b\rangle \neq |1\rangle \Rightarrow \langle 1|b\rangle \neq \langle 1|1\rangle = 1$

contradict with $\langle 1|b\rangle = 1$; thus $|b\rangle = |1\rangle$

• With initial state $|0\rangle^{\otimes n} |1\rangle$

the state at the first slice is the superposition of $|0\rangle^{\otimes n}$ and $|1\rangle$, thus

$$|\varphi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{J=0}^{2^n-1} |J\rangle |1\rangle$$

(superposition)

So if we apply U_a on $|\varphi_1\rangle$; we have the state before QFT^{-1} is

$$|\varphi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{J=0}^{2^n-1} |J\rangle |a^J \bmod N\rangle$$

Now, we need to prove that

$$\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{2\pi i s k}{r}\right] |u_k\rangle = |a^s \bmod N\rangle$$

In fact; $\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{2\pi i s k}{r}\right] |u_k\rangle$

$$= \frac{1}{\sqrt{r}} \sum_{s';k=0}^{r-1} \exp\left(-\frac{2\pi i k (s'-s)}{r}\right) |a^{s'} \bmod N\rangle$$

then $\sum_{k=0}^{r-1} \exp\left(-\frac{2\pi i k (s'-s)}{r}\right)$

$$= \begin{cases} \sum_{k=0}^{r-1} \exp(0) & \text{if } s' = s \\ \frac{1 - e^{-2\pi i (s'-s)}}{1 - e^{\frac{-2\pi i (s'-s)}{r}}} & s' \neq s \end{cases}$$

$$= \begin{cases} \sum_{k=0}^{r-1} 1 = r & \text{if } s' = s \\ 0 & \text{if } s' \neq s \end{cases}$$

Thus; LHS $= \sum_{s'=0}^{r-1} \delta_{s's} \, |a^{s'} \bmod N\rangle$

$= |a^{s} \bmod N\rangle$

$\left(\text{since} \sum_{k=0}^{r-1} \exp\left(-\frac{2\pi i s k}{r}\right) = r\delta_{s0} \right)$

Thus, we have proved that $\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{2\pi i s k}{r}} |u_k\rangle = |a^k \bmod N\rangle$

then $|\varphi_2\rangle = \frac{1}{\sqrt{r2^n}} \sum_{k=0}^{r-1} \sum_{j=0}^{2^n-1} e^{\frac{2\pi i s k}{r}} |j\rangle |u_k\rangle$

$= \frac{1}{\sqrt{r}} \cdot \frac{1}{\sqrt{2^n}} \sum_{k=0}^{r-1} \sum_{j=0}^{2^n-1} e^{\frac{2\pi i s k}{r}} |j\rangle |u_k\rangle$

$= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |\tilde{s}/r\rangle |u_s\rangle$

So the final state after QFT_n^{-1}

is $|\varphi_3\rangle = (QFT_n^{-1})\,|\varphi_2\rangle$

$$= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \left|\widetilde{k/r}\right\rangle |u_k\rangle$$

- measuring the first register yields $\widetilde{\frac{k}{r}}$

We can reconstruct r by apply continud fractions algorithm.

Suppose that $\varphi \simeq \frac{k}{r}$ is $2L+1$ bits

then $\left|\frac{k}{r} - \varphi\right| \leq \frac{1}{2^{2L+1}} \leq \frac{1}{2r^2}$ since $r \leq N \leq 2^L$

thus $\frac{k}{r}$ is a convergent of the continue fractions for $\varphi = \frac{\widetilde{k}}{r}$

thus $\frac{k}{r}$ can be computed in $O(L^3)$