Gurbaaz Singh Nandra
06/11/2022 (190349)

CS682A : Assignment

1. (a) $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ with eigenvalues $= \pm 1$
and eigenvectors $= |+\rangle, |-\rangle$

By diagonalisation of matrix, $X = PDP^{-1}$

$$X = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{-1}$$

(Note: P is constructed using eigenvectors of X)

Let square root of $X = B$, then $B = PD^{1/2}P^{-1}$

$$\Rightarrow B = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \sqrt{1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{-1}$$

$$= \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & -1/2 \end{pmatrix}$$

$$= \frac{1}{2} \begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$$

$$\left[B^2 = PD^{1/2}P^{-1}PD^{1/2}P^{-1} = P(D^{1/2})^2P^{-1} = PDP^{-1} = X \right]$$

Action of B on basis:

$$|0\rangle \longrightarrow \frac{1}{2}\begin{pmatrix} 1+i \\ 1-i \end{pmatrix} = \frac{1}{\sqrt{2}}(|+\rangle + i|-\rangle)$$

$$|1\rangle \longrightarrow \frac{1}{2}\begin{pmatrix} 1-i \\ 1+i \end{pmatrix} = \frac{1}{\sqrt{2}}(|+\rangle - i|-\rangle)$$

We know that S (phase gate) $= \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

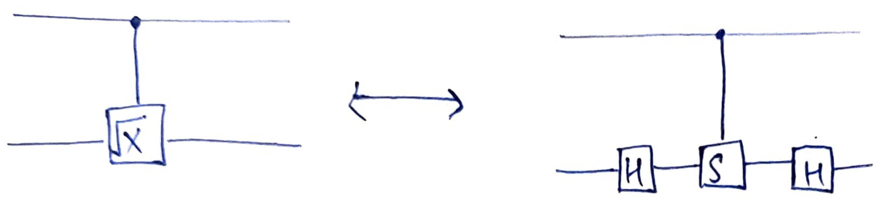
Hence, we can implement $B = \sqrt{X}$ using S-gate and H-gate as follows on the basis states

$$|0\rangle \xrightarrow{H} \frac{|0\rangle + |1\rangle}{\sqrt{2}} \xrightarrow{S} \frac{|0\rangle + i|1\rangle}{\sqrt{2}} \xrightarrow{H} \frac{|+\rangle + i|-\rangle}{\sqrt{2}}$$

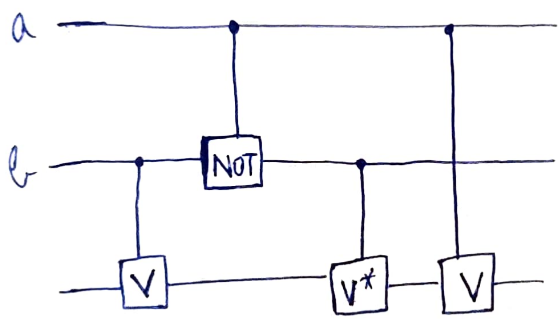
$$|1\rangle \xrightarrow{H} \frac{|0\rangle - |1\rangle}{\sqrt{2}} \xrightarrow{S} \frac{|0\rangle - i|1\rangle}{\sqrt{2}} \xrightarrow{H} \frac{|+\rangle - i|1\rangle}{\sqrt{2}}$$

That is, $\sqrt{X} \equiv HSH$

Circuit of controlled version of $\sqrt{X}$ using C-S gate :



(b) A CC-U gate can be implemented using CNOT, CV and CV* gate as :-



We can easily see that output at non-control wire is $V^b (V^*)^{b \oplus a} V^a$. Let us verify that the circuit is indeed CC-U :-

I : $a = 0$ and $b = 0$

No control gate is applied. Therefore U is not applied.

II : $a = 0$ and $b = 1$

In this case, first CV is applied and then CV^* is applied. Second CV and CNOT gate are not applied. ∴ Final action on non-control wire $= VV^* = I$, since $V = \sqrt{U}$

Therefore, net action $\neq U$

III: $a=1$ and $b=0$

In this case, first CV is not applied. But as the result of CNOT gate, b becomes 1 and then ~~second~~ CV^* is applied, followed by second CV^*. Net action on non-control wires is again $V^*V = I \neq U$.

IV: $a=1$ and $b=1$

In this case, first CV is applied. As a result of CNOT gate, b becomes 0 and CV^* is not applied. Finally CV is applied.

Net action $= VV = U$

$\therefore$ Given circuit implements the functionality of CCU gate.

---

2. (a) Order r is the smallest non-zero integer s.t.

$a^r \bmod n = 1$, where $a = 2, n = 15$

We get order of 2; $r = 4$

Since r is not odd and $2^{4/2} = 4 \neq \pm 1 \bmod 15$

We find $b = a^{r/2} = 4$ and find non trivial factors from $\gcd(b \pm 1, n)$

$= \gcd(4 \pm 1, 15)$

$= \gcd(3, 15)$ and $\gcd(5, 15)$

$= 3$ and 5

And we break from the iterative loop.

(b) Use quantum phase estimation on unitary operator

$$U|y\rangle = |ay \bmod n\rangle$$
$$= |2y \bmod 15\rangle$$

$y \in Z_{15}^*$ and y is a basis of $\mathbb{C}^{16}$

Eigenvectors :

$$|U_s\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{2\pi i j s/r} |2^j \bmod 15\rangle$$

Since $|1\rangle$ basis state is a superposition of these eigenstates, i.e.

$|1\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |U_s\rangle$, we apply QPE on U using $|1\rangle$, and

measure a phase $\phi = s/r$

$$|0,1\rangle \xrightarrow{H^{\otimes 4} \otimes I} \frac{1}{\sqrt{16}} \sum_{j=0}^{15} |j,1\rangle \xrightarrow{CU^j} \frac{1}{\sqrt{16}} \sum_{j=0}^{15} |j\rangle \frac{1}{\sqrt{r}} \sum e^{\frac{2\pi i j s}{r}} |U_s\rangle$$

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |2^k s/r\rangle |U_s\rangle \xleftarrow{IQFT} \frac{1}{r} \sum_{s=0}^{r-1} \frac{1}{\sqrt{16}} \sum_{j=0}^{15} e^{\frac{-2\pi i j s}{r}} |j\rangle |U_s\rangle$$

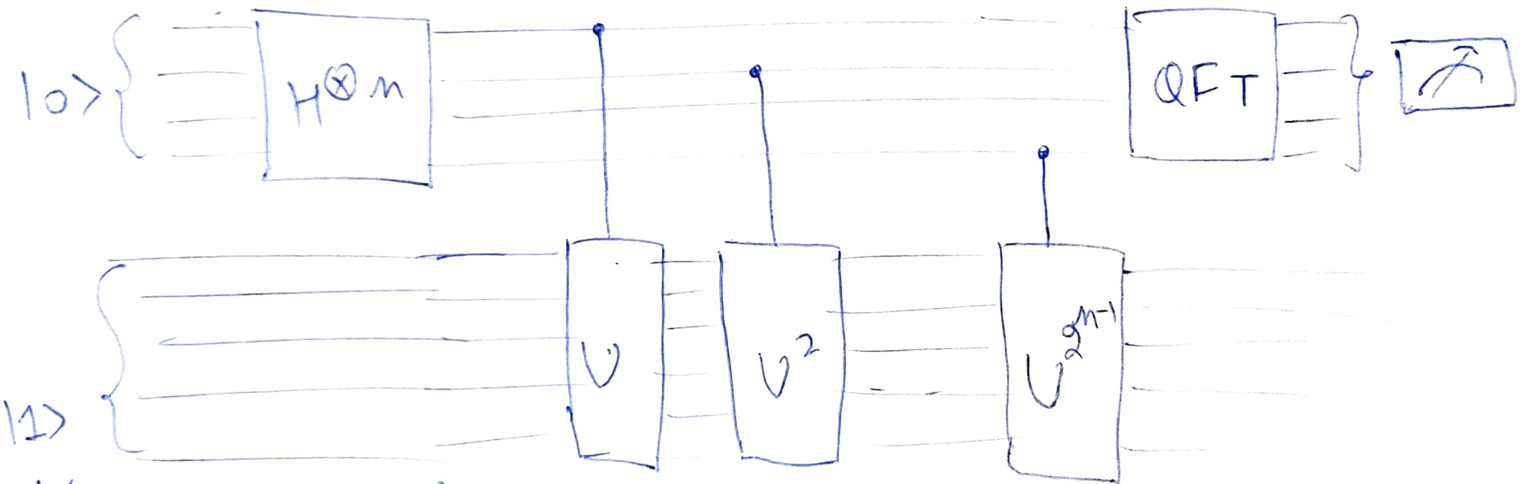
On measuring first qubit, we get s/r

Since $r = 4$, s can take values $0, 1, 2, 3$

As s & r are coprime, we have 50% probability $(1/4, 3/4)$ of obtaining correct s/r.

As a next step, we simply have to use continued fraction to obtain s and r, and check if r is correct.

Circuit for Order finding :



$= \frac{1}{\sqrt{r}}(|u_0\rangle + |u_1\rangle \ldots + |u_{r-1}\rangle)$

3. $a^s = b \bmod n$

Let $f(x_1, x_2) = b^{x_1} a^{x_2} \bmod n$ be a HSP

Then

$\cancel{f(x_1, x_2+s) = b^{x_1+s} a^{x_2} \bmod n}$

$$f(x_1, x_2) = b^{x_1} a^{x_2-s} a^{s} \bmod n$$

$$= b^{x_1} a^{x_2-s} b \bmod n$$

$$= b^{x_1+1} a^{x_2-s} \bmod n$$

$$= f(x_1+1, x_2-s)$$

$$= f(x_1+2, x_2-2s)$$

$$\vdots$$

and so on. is periodic.

Group $:= (\mathbb{Z}, \mathbb{Z})$

Hidden subgroup $:= (\mathbb{Z}, -s\mathbb{Z})$

(4.) (a) To show: $|\tilde{x}\rangle$ is an eigenvector of U with eigenvalue $e^{i2\pi x/m}$

i.e. $U|\tilde{x}\rangle = e^{i2\pi x/m}|\tilde{x}\rangle$

$$|\tilde{x}\rangle = \frac{1}{\sqrt{m}}\sum_{y=0}^{m-1} e^{i2\pi xy/m}|y\rangle \quad \text{———} \quad (1)$$

$$U|\tilde{x}\rangle = \frac{1}{\sqrt{m}}\left(\sum_{y=0}^{m-1} e^{\frac{i2\pi xy}{m}} U|y\rangle\right)$$

since $0 \leq y < m$, $U|y\rangle = |y-1 \bmod m\rangle$

$$U|\tilde{x}\rangle = \frac{1}{\sqrt{m}}\left(\sum_{y=0}^{m-1} e^{\frac{i2\pi xy}{m}}|y-1 \bmod m\rangle\right)$$

Substituting $t = y-1 \bmod m$, we get

$$U|\tilde{x}\rangle = \frac{1}{\sqrt{m}}\left(\sum_{t=0}^{m-1} e^{\frac{i2\pi x(t+1)}{m}}|t\rangle\right)$$

$$= \frac{1}{\sqrt{m}} e^{\frac{i2\pi x}{m}}\left(\sum_{t=0}^{m-1} e^{\frac{i2\pi xt}{m}}|t\rangle\right)$$

$$= e^{i2\pi x/m}\left(\frac{1}{\sqrt{m}}\sum_{t=0}^{m-1} e^{\frac{i2\pi xt}{m}}|t\rangle\right)$$

$$= e^{\frac{i2\pi x}{m}}|\tilde{x}\rangle \qquad \text{(From (1))}$$

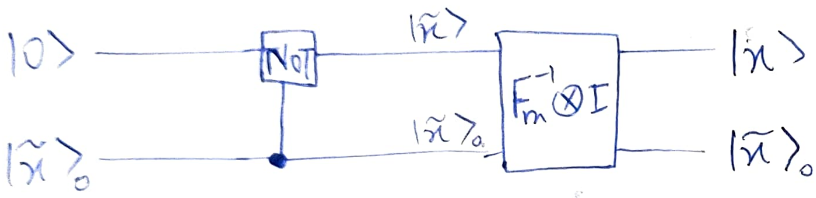
Hence proved.

(b) Convert $|0\rangle|\tilde{x}\rangle$ to $|x\rangle|\tilde{x}\rangle$.

We can perform the given conversion with applying the following sets of gates

i) CNOT with $|\tilde{x}\rangle_0$ as control qubit

ii) Fourier Inverse $(F_m^{-1} \otimes I)$

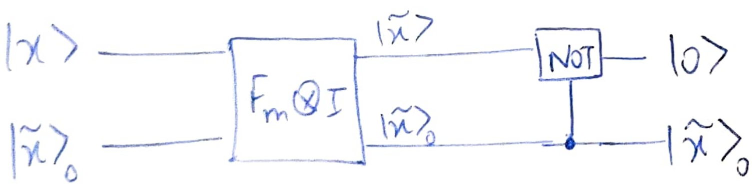


[Note that $|0\rangle$ and $|\tilde{x}_0\rangle$ are not single qubits but a set of qubits, and CNOT is actually from one set of qubits to other, mapped in a one-to-one fashion.]

(c) We know that Quantum gates are reversible, hence we can perform the opposite conversion of $|x\rangle|\tilde{x}\rangle$ to $|0\rangle|\tilde{x}\rangle$ as

i) Fourier $(F_m \otimes I)$

ii) CNOT with $|\tilde{x}\rangle_0$ as control qubit



[Circuits have been simplified for easy visualisation]

5.

(a) Query complexity of algorithm consists of two sub-parts of queries:-

i. Picking l random elements and query them all takes l queries.

ii. Grover search on remaining $n-l$ elements to check if a value collides with one of these l values. For one marked element, i.e. $f(x) = f(y)$ for exactly one x in remaining $n-l$ and y in l ~~elemen~~ queried elements, grover search takes $O(\sqrt{n-l})$ query complexity. In general, for t marked elements, grover search takes $O\left(\sqrt{\frac{n-l}{t}}\right)$, which is upper bounded by $O(\sqrt{n})$.

$\therefore$ Total query complexity of algorithm $= l + O(\sqrt{n})$

(b) For the success probability of previous algorithm, it is sufficient to calculate success probability of worst case, i.e., when failure probability is the highest. This case would be when there exists only one pair of repeating elements, and failure of algorithm would occur if both equal elements are in the set of remaining $n-l$ elements.

$$\therefore\ p(\text{failure}) = \frac{{}^{n-2}C_l}{{}^{n}C_l}$$

$$p(\text{success}) = 1 - p(\text{failure}) = 1 - \frac{{}^{n-2}C_l}{{}^{n}C_l}$$

$$= 1 - \frac{(n-2)!}{(n-2-\ell)!\,\cancel{\ell!}} \cdot \frac{(n-\ell)!\,\cancel{\ell!}}{n!}$$

$$= 1 - \frac{(n-\ell-1)(n-\ell)}{n(n-1)}$$

$$= \frac{\cancel{n^2} - \cancel{n} - \cancel{n^2} + \ell n + \ell n - \ell^2 + \cancel{n} - \ell}{n^2 - n}$$

$$= \frac{\ell(2n-\ell-1)}{n(n-1)}$$

We know that in grover search, given $p(\text{success}) = p$, we need to iterate the algorithm $\frac{1}{\sqrt{p}}$ times for constant success probability. Therefore,

$$\#\text{ iterations} = \sqrt{\frac{n(n-1)}{\ell(2n-\ell-1)}}$$

(c) Choose $\ell = \sqrt{n}$, we get

$$p(\text{success}) = \frac{\sqrt{n}(2n - \sqrt{n} - 1)}{n(n-1)} = \frac{\sqrt{n}}{n}\left(\frac{2(n-1)}{n-1} - \frac{(\sqrt{n}-1)}{n-1}\right)$$

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

since $n \geq 1$ and hence $2 - \frac{1}{\sqrt{n}+1} > 1$

$\therefore$ Total query complexity

$= (\#\text{ iterations})(\text{query complexity of single search})$

$$= \frac{1}{\sqrt{p}} \left(\ell + O\sqrt{n} \right) \Big|_{\ell = \sqrt{n}}$$

$$= O(n^{1/4}) \left(n^{1/2} + O(n^{1/2}) \right)$$

$$= O(n^{1/4 + 1/2})$$

$$= O(n^{3/4})$$