Assignment-4

Name:- Shreyas M.L

Date: 25/05/2020

Shreyas

Sem :- II

Course Name :- FQC

Reg No :- 190913012

Roll No :- 11

Branch :- CSE

Shor's Algorithm

$N = 15 \quad a = 7$

1> Create 2 quantum registers

Reg 1 :- $(|\psi_1\rangle)$: $k = 3$ qubits representing the number 0 to 7 $(\leq N/2)$

Reg 2 :- $(|\psi_2\rangle)$: $m = 4$ qubits representing the number 0 to 15 $(\leq N)$

$\gcd(7, 15) = 1$

2> Initialize all 7 (3+4) qubits to $|0\rangle$

$|\psi\rangle = |0000000\rangle = |\psi_1\rangle|\psi_2\rangle = |000\rangle|0000\rangle$

Apply Hadamard gate to each of the 3 qubits in $|000\rangle$

i.e $|\psi\rangle = \left(\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \cdot \frac{1}{\sqrt{2}}(|0\rangle|1\rangle) \cdot \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\right)|0000\rangle$

3> $|\psi\rangle = \frac{1}{\sqrt{8}}\left(|\underbrace{000}_{0}\rangle + |\underbrace{001}_{1}\rangle + |\underbrace{010}_{2}\rangle + \ldots + |\underbrace{111}_{7}\rangle\right)|0000\rangle$

$|\psi\rangle = \left(\frac{1}{\sqrt{8}} \sum_{K=0}^{7} |k\rangle\right)|0000\rangle$

4> The values of $f(x)$ for $a = 7$ $\quad f(x) = 7^x \bmod 15$

x	0	1	2	3	4	5	6	7
$f(x)$	1	7	4	13	1	7	4	13

5) The result ~~of~~ $f(x) = a^x \bmod N$ for all x in first register $(0..7)$ is in the second register

$$|\psi\rangle = \frac{1}{\sqrt{8}}\Big(\underset{0}{|000\rangle}\underset{1}{|0001\rangle} + \underset{1}{|001\rangle}\underset{7}{|0111\rangle} + \underset{2}{|010\rangle}\underset{4}{|0100\rangle} + \underset{3}{|011\rangle}\underset{13}{|1101\rangle}$$
$$+ \underset{4}{|100\rangle}\underset{1}{|0001\rangle} + \underset{5}{|101\rangle}\underset{7}{|0111\rangle} + \underset{6}{|110\rangle}\underset{4}{|0100\rangle} + \underset{7}{|111\rangle}\underset{13}{|1101\rangle}$$

Combining like terms

$$|\psi\rangle = \frac{1}{\sqrt{8}}\Big(\Big[\big(\underset{0}{|000\rangle} + \underset{4}{|100\rangle}\Big]\underset{1}{|001\rangle} + \Big[\underset{1}{|001\rangle} + \underset{5}{|101\rangle}\Big]\underset{7}{|0111\rangle}$$
$$+ \Big[\underset{2}{|010\rangle} + \underset{6}{|110\rangle}\Big]\underset{4}{|0100\rangle} + \Big[\underset{3}{|011\rangle} + \underset{7}{|111\rangle}\,|\underset{13}{1101\rangle}\Big]\Big)$$

6) Register 1 contains ~~r of~~ period r of intrest but only for identical measurement results of register $\underline{4}$

- The distance b/w components (0,4 or 1,5 or 2,6 or 3,7) in 1st register single state of the 2nd register <u></u>r is even

7) The factors of $N = 15$ are $p = GCD(N, a^{r/2}+1)$

$$= \boxed{GCD(15, 50) = 5}$$

$$q = GCD(N, a^{r/2}-1) = \boxed{GCD(15, 48) = 3}$$

$\therefore$ Factors are 5 and 3

Shreyas