Name = Harshit Yadav

Semester = 2

Section = Mtech CSE

Branch = mtech

Roll/Reg No = 190913017

Subject name = FQC

Signature =

Date = May 25, 2020

Assignment = 4

1) For the following combination a, N apply shor's Alg find the factor of N = , N = 15, a = 7
show all working including state of two register after each calculation

① $\alpha = 7$, $N = 15$

GCD $(7, 15) = 1$

② Determining Q

$$n^2 \le Q \le 2N^2$$

let us consider 2 quantum registers

R_1 $(|\psi_1\rangle)$: $K = 3$ qubits for representing the number 0 to 7 $(\le N/2$

R_2 $(|\psi_2\rangle)$: $m = 4$ qubits for representing the number 0 to 15 $(\le N)$

Initializing all 7 (3+4) qubits to $|0\rangle$

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

Randomize the first register apply Hadamard gate to each of 3 qubits in $|000\rangle$

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$$
$$|0000\rangle$$

$$|\psi\rangle = \frac{1}{\sqrt{8}}(|000\rangle+|001\rangle+|010\rangle+|011\rangle+|100\rangle+$$
$$|101\rangle+|110\rangle+|111\rangle)|0000\rangle$$

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

x	0	1	2	3	4	5	6	7
$f(x) = 7^x \bmod 15$	1	7	4	13	1	7	4	13

the result of simultaneous evaluation of $f(x) = a^x \bmod N$ (here $7^x \bmod 15$) for all x in 1st register (0 -- 7) is in 2nd register

$$|\psi\rangle = \frac{1}{\sqrt{8}}(|000\rangle|001\rangle + |001\rangle|111\rangle + |010\rangle|100\rangle + |011\rangle|1101\rangle$$
$$+ |100\rangle|001\rangle + |101\rangle|111\rangle + |110\rangle|100\rangle +$$
$$|111\rangle|1101\rangle)$$

$$\psi\rangle = \frac{1}{\sqrt{8}}((|000\rangle + |100\rangle)|001\rangle + (|001\rangle + |101\rangle)$$
$$|111\rangle + (|010\rangle + |110\rangle)|100\rangle + (|011\rangle +$$
$$|111\rangle)|1101\rangle)$$

Register 1 contains now the period r, but only for identical measurement results in register 2

The $\boxed{\text{period } r = 4}$ is the distance between
since r = even $x^{r/2} \bmod nf - 1$
((0,4), (1,5), (2,6), (3,7)) in the 1st register
for a single state of 2nd register

the factor of N=15 are

$p = GCD(a^{r/2}+1, N)$ | $q = GCD(a^{r/2}-1, N)$, $r=4$

$p = GCD(50, 15)$ | $q = GCD(48, 15)$

$\underline{p=5}$ | $\underline{q=3}$

$N = p * q \Rightarrow 15 = \underline{5*3}$

Fatoras are (5 and 3)