Quantum Computing Assignment 10 - Group 18

Rallabhandi, Anand Krishna Mustafa, Syed Husain
, Mohammed Kamran

January 25, 2021

Exercise 10.1

(Reduction of Factoring to Order Finding)

(a) As per the algorithm for "Reduction of Factoring to Order Finding" the first two steps state the following:
Step-1 : If N is even, return the factor 2.
Step-2 : Determine whether $N = a^b$ for integers $a \geq 1$ & $b \geq 2$ (using a classical algorithm) and if so return the factor a.

Given N=221, the first step does not return 2 as N is not even.
$a_{b=2}$: $221^{\frac{1}{2}} = 14.866$, $a_{b=3}$: $221^{\frac{1}{3}} = 6.046$, $a_{b=4}$: $221^{\frac{1}{4}} = 2.943$, $a_{b=5}$: $221^{\frac{1}{5}} = 2.458$,
$a_{b=6}$: $221^{\frac{1}{6}} = 2.162$
Since none of the values of "a" obtained above lie in the set of Integers, hence Step-2 does not return the factor "a".

For Step-3 of the Factoring Algorithm we randomly choose $x = 55$, such that $1 \leq x \leq N-1$, when $N = 221$.
For Step-4 we compute order **r** of x modulo N.
$55^0 \equiv 1 \bmod 221$,$55^1 \equiv 55 \bmod 221$, $55^2 \equiv 152 \bmod 221$, $55^3 \equiv 183 \bmod 221$,
$55^4 \equiv 120 \bmod 221$, $55^5 \equiv 191 \bmod 221$, $55^6 \equiv 118 \bmod 221$, $55^7 \equiv 81 \bmod 221$,
$55^8 \equiv 35 \bmod 221$, $55^9 \equiv 157 \bmod 221$, $55^{10} \equiv 16 \bmod 221$, $55^{11} \equiv 217 \bmod 221$,
& $55^{12} \equiv 1 \bmod 221$
$\therefore$ Order **r** of 55 mod 221 is **12**
Step-5 : If r is even & $x^{\frac{r}{2}} \neq -1$ mod N, then compute $gcd(x^{\frac{r}{2}} - 1, N)$ and $gcd(x^{\frac{r}{2}} + 1, N)$, one of which must be a non-trivial factor, and return this factor; otherwise the algorithm fails.

$55^{\frac{12}{2}} = 55^6 \equiv 118 \bmod 221$, hence $55^6 \neq -1 \bmod 221$.
Computing $gcd(55^6 - 1, 221) = 13$
Computing $gcd(55^6 + 1, 221) = 17$
$\therefore$ The prime factorization of N=221, is given by $221 = 13 \times 17$

(b) Consider $N = 15$ as input to the Order finding subroutine. All composite numbers smaller than 15 are multiples of 2, ie; 4, 6, 8, 10, 12, & 14. The only odd composite less than 15 is 9. Since $9 = 3^2$, 15 is the smallest number for which order-finding subroutine is required.

Exercise 10.2

(**Quantum Operations & Amplitude Damping**)

(a) $$\sum_{k\epsilon\{0,1\}} E_k^\dagger E_k = \begin{pmatrix}1 & 0\\ 0 & \sqrt{1-\gamma}\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & \sqrt{1-\gamma}\end{pmatrix} + \begin{pmatrix}0 & 0\\ \sqrt{\gamma} & 0\end{pmatrix}\begin{pmatrix}0 & \sqrt{\gamma}\\ 0 & 0\end{pmatrix}$$
$$= \begin{pmatrix}1 & 0\\ 0 & 1-\gamma\end{pmatrix} + \begin{pmatrix}0 & 0\\ 0 & \gamma\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \equiv I$$

Hence Proved

(b) Controlled-$R_y(\theta)$ Gate $\equiv \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & \cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2})\\ 0 & 0 & \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2})\end{pmatrix}$

Flipped CNOT GATE $\equiv \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\end{pmatrix}$

$$U_{AD} = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\end{pmatrix}\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & \cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2})\\ 0 & 0 & \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2})\end{pmatrix} = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 0 & \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2})\\ 0 & 0 & \cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2})\\ 0 & 0 & 1 & 0\end{pmatrix}$$

(c) For $\gamma = \sin^2(\frac{\theta}{2})$

$$E_0 = \begin{pmatrix}1 & 0\\ 0 & \cos(\frac{\theta}{2})\end{pmatrix} \;\&\; E_1 = \begin{pmatrix}0 & \sin(\frac{\theta}{2})\\ 0 & 0\end{pmatrix}$$

For $(E_0)_{l,m} = \langle l, 0|U_{AD}|m, 0\rangle$:

$$(E_0)_{0,0} = \langle 00|U_{AD}|00\rangle = \begin{pmatrix}1 & 0 & 0 & 0\end{pmatrix}\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 0 & \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2})\\ 0 & 0 & \cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2})\\ 0 & 0 & 1 & 0\end{pmatrix}\begin{pmatrix}1\\0\\0\\0\end{pmatrix} = 1$$

$$(E_0)_{0,1} = \langle 00|U_{AD}|10\rangle = \begin{pmatrix}1 & 0 & 0 & 0\end{pmatrix}\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 0 & \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2})\\ 0 & 0 & \cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2})\\ 0 & 0 & 1 & 0\end{pmatrix}\begin{pmatrix}0\\0\\1\\0\end{pmatrix} = 0$$

$$(E_0)_{1,0} = \langle 10|U_{AD}|00\rangle = \begin{pmatrix}0 & 0 & 1 & 0\end{pmatrix}\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 0 & \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2})\\ 0 & 0 & \cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2})\\ 0 & 0 & 1 & 0\end{pmatrix}\begin{pmatrix}1\\0\\0\\0\end{pmatrix} = 0$$

$$(E_0)_{1,1} = \langle 10|U_{AD}|10\rangle = \begin{pmatrix}0 & 0 & 1 & 0\end{pmatrix}\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 0 & \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2})\\ 0 & 0 & \cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2})\\ 0 & 0 & 1 & 0\end{pmatrix}\begin{pmatrix}0\\0\\1\\0\end{pmatrix} = \cos(\frac{\theta}{2})$$

For $(E_1)_{l,m} = \langle l,1|U_{AD}|m,0\rangle$:

$$(E_1)_{0,0} = \langle 01|U_{AD}|00\rangle = \begin{pmatrix}0 & 1 & 0 & 0\end{pmatrix}\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 0 & \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2})\\ 0 & 0 & \cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2})\\ 0 & 0 & 1 & 0\end{pmatrix}\begin{pmatrix}1\\0\\0\\0\end{pmatrix} = 0$$

$$(E_1)_{0,1} = \langle 01|U_{AD}|10\rangle = \begin{pmatrix}0 & 1 & 0 & 0\end{pmatrix}\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 0 & \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2})\\ 0 & 0 & \cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2})\\ 0 & 0 & 1 & 0\end{pmatrix}\begin{pmatrix}0\\0\\1\\0\end{pmatrix} = \sin(\frac{\theta}{2})$$

$$(E_1)_{1,0} = \langle 11|U_{AD}|00\rangle = \begin{pmatrix}0 & 0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 0 & \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2})\\ 0 & 0 & \cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2})\\ 0 & 0 & 1 & 0\end{pmatrix}\begin{pmatrix}1\\0\\0\\0\end{pmatrix} = 0$$

$$(E_1)_{1,1} = \langle 11|U_{AD}|10\rangle = \begin{pmatrix}0 & 0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 0 & \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2})\\ 0 & 0 & \cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2})\\ 0 & 0 & 1 & 0\end{pmatrix}\begin{pmatrix}0\\0\\1\\0\end{pmatrix} = 0$$

Values of $(E_0)_{l,m}$ & $(E_1)_{l,m}$ are in agreement with Eq. (2)