Yining Hua

HW 4

1. NC5.10 Order of x $\Rightarrow$ find the smallest possible r that let $x^r \equiv 1 \bmod N$, when $x=5$, $N=21$.

Start with a guess that $r=2$ | $x^2 = 25$.

then $x^2 \bmod 21 = 25 \bmod 21$

$= (25-21) \bmod 21$

$= 4$. ...

Continue trying like this we get

$x^1 \bmod 21 = 5$

$x^2 \bmod 21 = 4$

$x^3 \bmod 21 = -1$

$x^4 \bmod 21 = -5$

$x^5 \bmod 21 = -4$

$x^6 \bmod 21 = 1$.

$\therefore$ When $r = 1$ we find the smallest possible r, which is 6.

2. NC.5.11. Show that the order of x satisfies $r \leq N$.

$x^r = 1 \bmod N$, $r = \{0, 1, 2, \cdots N\}$.

$N+1$ elements.

Since there are at most N elements that modulo N, in the $N+1$ elements of r must exist 2 at least 2 possible values of r that are equal to each other. Let these 2 values of r be m and n. then we have

$0 \leq m < n \leq N$. $x^m \equiv x^n \bmod N$.

$\therefore x^{n-m} \bmod N = 1.$

Since r is the first number to let $x^r \bmod N = 1$,

$$x^r \le x^{n-m} \le x^N$$

$$\therefore r \le n-m \le N$$

$$\therefore r \le N. \qquad \square$$

3. Known: A subroutine that factors any B to P.Q.
Want: An algorithm that finds the order of $A \in \mathbb{Z}_B^*$.

$\mathbb{Z}_B^*$ is a group b/c it fulfill the 3 properties of group.

$$\mathbb{Z}_B^* = \{ x \in \mathbb{Z}_B \mid \gcd(x, B) = 1 \}, \quad x := x \bmod B$$

1. → Order of A: find $\gcd(A, \mathbb{Z}_B^*) \pm 1$.
2. → According to the Lagrange's Theorem, for an infinite group G and its subgroup H,
$|H| \mid |G| \Rightarrow$ the cardinality of H devides that of G.

For the associativity,
$a \bmod (b \bmod c) = (a \bmod b) \bmod c$
$\therefore \surd$

$\therefore$ Known the subroutine that factors B, we assume that it factors B into $p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_n^{a_n}$, with p_i as prime numbers and a_i as its power.

* Then we only need to find $|\mathbb{Z}_B^*|$, and try out all possible combinations of divisors of A till we find the one that divides $|\mathbb{Z}_B^*|$.

2. Find $|\mathbb{Z}_B^*|$.

According to Euler's product formula $\varphi(n) = n \prod_{p \mid n} (1 - \frac{1}{p})$.
we can find $|\mathbb{Z}_B^*|$, which is $\varphi(B)$

↙ cardinality of $\mathbb{Z}_B^*$. ↓ number of relative primes to B.

Therefore, factoring and order-finding are of equivalent complexity.

4.NC5.6 $|x\rangle \to |x+y \bmod 2^n\rangle$ $0 \le x < 2^n$. y fixed constant

what QFT does by definition : $|j\rangle \to \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} |k\rangle$

$(N = 2^n)$

(1st QFT) $\therefore |x\rangle \xrightarrow{QFT} \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{\frac{2\pi i kx}{2^n}} |k\rangle$

(phase shift) $\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{\frac{2\pi i kx}{2^n}} |k\rangle \xrightarrow{\text{phase shift}} \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{\frac{2\pi i k(x+y)}{2^n}}$

$e^{\frac{2\pi i kx}{2^n}} \cdot e^{\frac{2\pi i ky}{2^n}}$

$\therefore$ This phase shift converts $|k\rangle$ into $e^{\frac{2\pi i ky}{2^n}} |k\rangle$

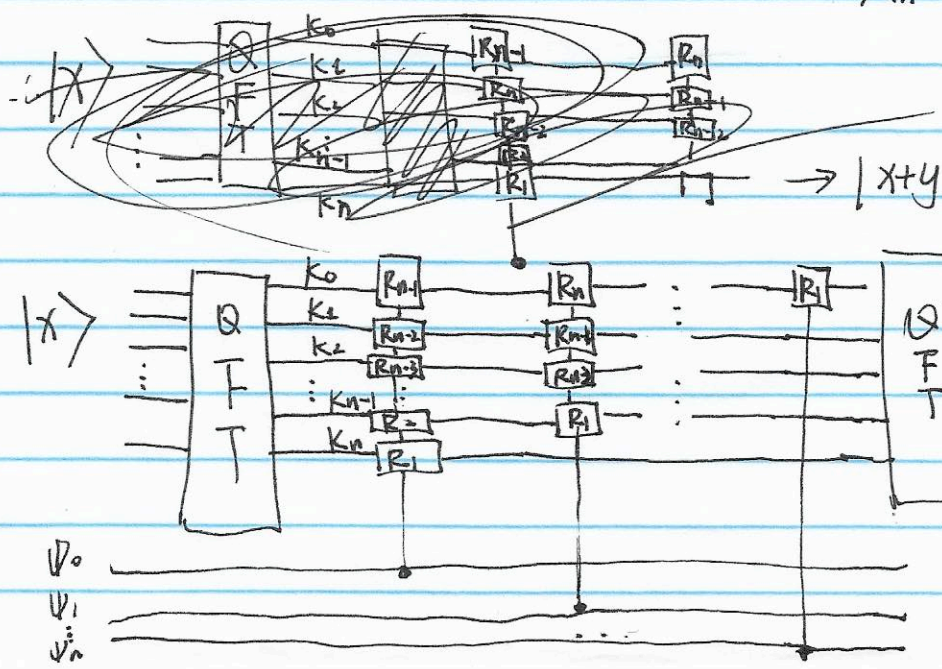
Since k, y in binary. $\Rightarrow \begin{cases} k = \sum_{j=0}^{n} k_j 2^j \\ y = \sum_{k=0}^{n} y_k 2^k \end{cases} \Rightarrow ky = \sum_{j=0}^{n} \sum_{k=0}^{n} 2^{j+k} k_j y_k$

$\therefore$ We need a unitary operator that transforms $|k_j\rangle$ into

$$\prod_k e^{\frac{2\pi i y_k k_j}{2^{n-k-j}}} |k_j\rangle$$

↳ For each k_j (qubit), apply a R_{n-j-k} gate on it (controlled by y_k)

$$R_n = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^n}} \end{pmatrix}$$



5. NC 6.2

$$2|\psi\rangle\langle\psi| - I)\left(\sum_k a_k |k\rangle\right)$$

~~$\sum_k 2 a_k |\psi\rangle\langle\psi|k\rangle - a_k|k\rangle$~~

$$= \sum_k \left(2a_k |\psi\rangle\langle\psi|k\rangle - a_k|k\rangle\right)$$

(6.4)
$$= \sum_k \left(2a_k \left(\frac{1}{N^{1/2}} \sum_{x=0}^{N-1} \langle x|k\rangle - a_k|k\rangle\right)\right)$$

↓

replace this with $\sum_{ij} |i\rangle\langle j|$. $\quad \frac{1}{\sqrt{N}} \cdot \frac{1}{\sqrt{N}} = \frac{1}{N}$

↑ it's gone b/c it's replaced w $|i\rangle\langle j|$. → ~~double 1~~

$$\therefore = \sum_k \left(2a_k \left(\frac{1}{N} \sum_{ij} |i\rangle\langle j|k\rangle - a_k|k\rangle\right)\right)$$

$$= \frac{1}{N} \sum_i |i\rangle \delta_{jk} \quad \hookrightarrow 1.$$

$$= \frac{1}{N} \sum_i |i\rangle$$

$$\therefore = \sum_k \left(2a_k \frac{1}{N} \sum_i |i\rangle - a_k|k\rangle\right)$$

~~$= \sum_k \left(2a_k \frac{1}{N} \sum_k |k\rangle - a_k|k\rangle\right)$~~

~~$= \sum_k a_k$~~

$$= 2\sum_k a_k \frac{1}{N} \sum_i |i\rangle - \sum_k a_k|k\rangle$$

$$= \sum_k 2\frac{a_k}{N} \sum_k |k\rangle - \sum_k a_k|k\rangle$$

$\langle a\rangle$

~~$= \sum_k \langle a\rangle |k\rangle - \sum_k a_k|k\rangle$~~

$$= \sum_k \left(2\langle a\rangle - a_k\right)|k\rangle. \quad \square.$$

// $|i\rangle, |k\rangle$ in the same orthonormal basis.