LECTURE 13 October 3rd, 2023

PART II Fundamental Quantum Algorithms

$\boxed{\text{Today}}$ Period finding over $\mathbb{Z}_N$

RECAP Quantum Fourier Transform for $N = 2^n$

$$|0\rangle \xrightarrow{QFT_N} \frac{1}{\sqrt{N}} \sum_{s=0}^{N-1} |s\rangle$$

0th root of unity $\quad |1\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{s=0}^{N-1} \omega_N^{s} |s\rangle \quad$ where $\omega_N = e^{2\pi i/N}$ is the primitive N^{th} root of unity

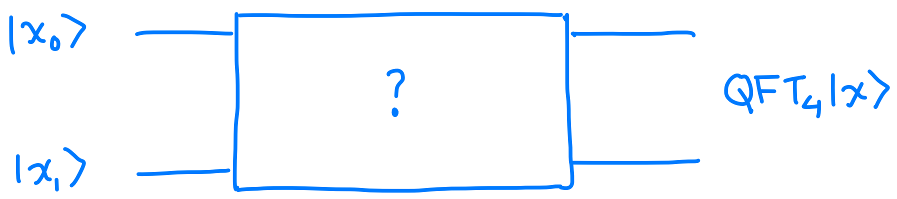
1st root of unity $\quad |2\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{s=0}^{N-1} \omega_N^{2s} |s\rangle$

$\vdots$

(N-1)st root of unity $\quad |x\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{s=0}^{N-1} \omega_N^{xs} |s\rangle$

Last time we saw that QFT_N can be implemented with $O(n^2)$ 1 and 2 qubit gates

Exercise (in-class) Give a circuit implementing QFT_4



Our motivation for considering QFT was the following

In Simon's Algorithm, we used a quantum subroutine that gave us linear equations describing our period

We will use QFT in a similar way to design a quantum subroutine that will give us a "clue" about periods over integers modulo N

In the next lecture, we will use these clues to design an algorithm for factoring

Period finding over $\mathbb{Z}_N$

$f : \mathbb{Z}_N \longrightarrow$ COLORS $\qquad \mathbb{Z}_N$ = integers modulo N

One can think of f as an array of length N

R	G	B	Y	R	G	B	Y	R	G	B	Y

$\mathbb{Z}_4 = \{0,1,2,3\}$

$0^2 = 0 \qquad 2^2 = 0$

$1^2 = 1 \qquad 3^2 = 1$

We will assume that we have "black-box" or "query access" to f

$$U_f |x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$$ where y has m-qubits

Note that in Shor's algorithm we will be able to implement this black-box unitary ourselves

We will assume that f is periodic

Periodic means that $f(x) = f(x+p)$ for all $x \in \mathbb{Z}_N$ where $p \neq 0$ and divides N

addition mod N

So, $f(0) = f(p) = f(2p) = \dots = f(kp)$ where $k = \frac{N}{p}$ is integer

$f(1) = f(p+1) = f(2p+1) = \dots = f(kp+1)$ and so on

E.g

R	G	B	Y	R	G	B	Y	R	G	B	Y

p p p

$N = 12$

$= 4$

Moreover, the values $f(0), \dots f(p-1)$ are assumed to be distinct

Compared to Simon's problem, there is a lot of periodicity here and we will see it

Let's try to design a quantum subroutine that will give us a "clue" about the period s

Quantum Subroutine (similar to Simon's algorithm)

For controlling the errors later, we shall need $p \ll \sqrt{N}$ so we first do the following

Pick a number $Q = 2^\ell$ such that $Q \in (N^2, 2N^2]$ and extend $f : \mathbb{Z}_Q \to$ COLORS

f on this bigger space may only be Almost-Periodic but we will able to handle it

$\boxed{\text{Almost-periodic}}$ $f(x) = f(x+p) = f(x+2p) = \dots = f(x+kp)$ if $x + kp < Q$

E.g

R	G	B	Y	R	G	B	Y	R	G	B

$Q = 12$

$p = 4$

The array does not wrap perfectly

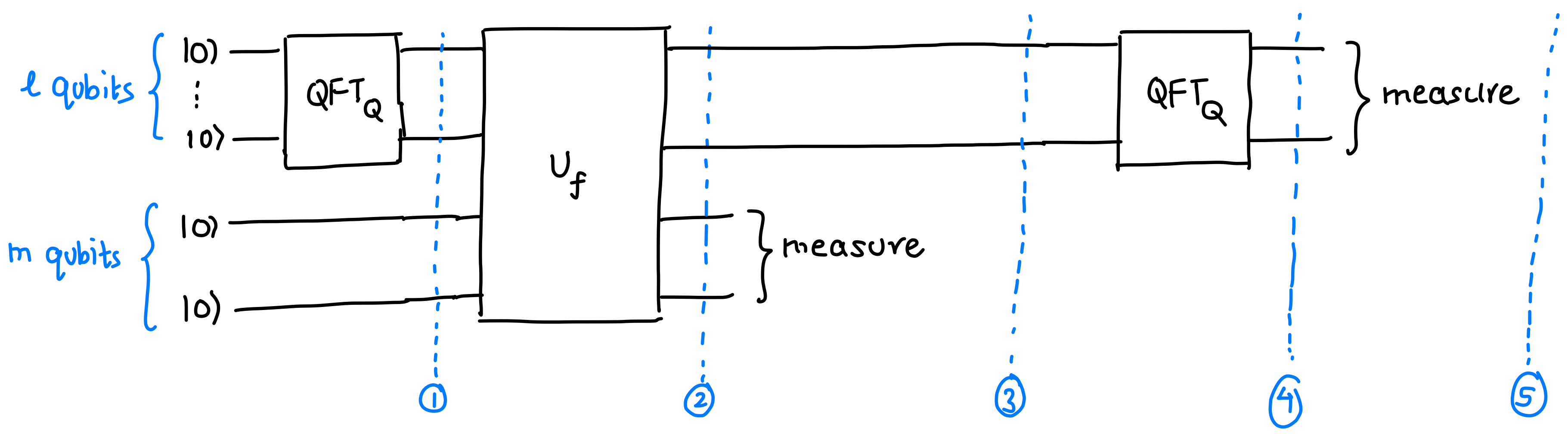
Moreover, the values $f(0), \dots f(p-1)$ are assumed to be distinct

① Prepare the state $\frac{1}{\sqrt{Q}} \sum_{x \in \mathbb{Z}_Q} |x\rangle|0^m\rangle \xrightarrow[U_f]{\text{Apply}} \frac{1}{\sqrt{Q}} \sum_{x \in \mathbb{Z}_Q} |x\rangle \underbrace{|f(x)\rangle}_{\text{COLOR}}$

② Measure the COLOR

③ Apply QFT_Q to the remaining qubits and measure them

\# gates $(\log Q)^2 = (\log N)^2$



State at time ① $= \left(QFT_Q |0\cdots0\rangle\right) \otimes |0\rangle^{\otimes m}$

$$= \frac{1}{\sqrt{Q}} \sum_{x \in \mathbb{Z}_Q} |x\rangle \otimes |0\rangle^{\otimes m}$$

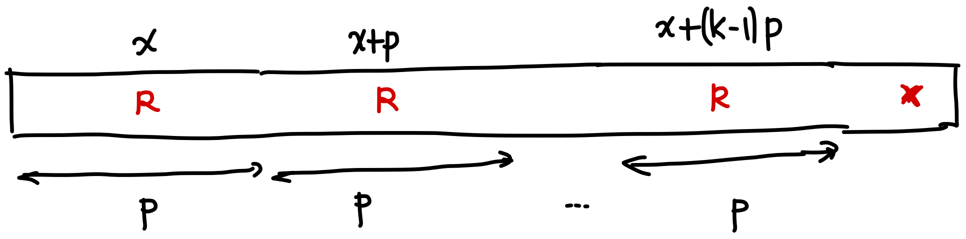
Note: Here we could have applied $H^{\otimes \ell}$ as well since

$$H^{\otimes \ell} |0\cdots0\rangle = \frac{1}{\sqrt{Q}} \sum_{x \in \mathbb{Z}_Q} |x\rangle$$

State at time ② $= \frac{1}{\sqrt{Q}} \sum_{x \in \mathbb{Z}_Q} |x\rangle |f(x)\rangle$

State at time ③ is obtained by measuring the COLOR

Suppose we measure R, then the state only contains amplitudes on terms where R occurs



Let k = # times R appears $= \left\lfloor \frac{Q}{p} \right\rfloor$ or $\left\lfloor \frac{Q}{p} \right\rfloor + 1$

if f on bigger space is still periodic, $k = \frac{Q}{p}$

Then, the state collapses to

$$\frac{1}{\sqrt{k}} \left(|x\rangle + |x+p\rangle + \ldots + |x+kp\rangle \right) \otimes |R\rangle \qquad \text{where } f(x) = R$$

$$= \left(\frac{1}{\sqrt{k}} \sum_{j=0}^{k} |x+jp\rangle \right) \otimes \underbrace{|R\rangle}$$

ignore what happens to this from now on

Applying the QFT, the state of the first ℓ qubits at time ④ is

$$\frac{1}{\sqrt{K}} \sum_{j=0}^{K-1} \frac{1}{\sqrt{Q}} \sum_{b=0}^{Q-1} \omega_Q^{b(x+jp)} |b\rangle$$

$$= \frac{1}{\sqrt{KQ}} \sum_{b=0}^{Q-1} \sum_{j=0}^{K-1} \omega_Q^{b(x+jp)} |b\rangle$$

$$= \frac{1}{\sqrt{KQ}} \sum_{b=0}^{Q-1} \omega_Q^{bx} \left(\sum_{j=0}^{K-1} \omega_Q^{bjP} \right) |b\rangle$$

RECALL

$$|x\rangle \xrightarrow{QFT_Q} \frac{1}{\sqrt{Q}} \sum_{b=0}^{Q-1} \omega^{bx} |b\rangle$$

where $\omega_Q = e^{2\pi i/Q}$

What's going on with this state ?

Let's first start with the easy case where f is also periodic on the bigger space
This happens when p divides Q

Now, the question is

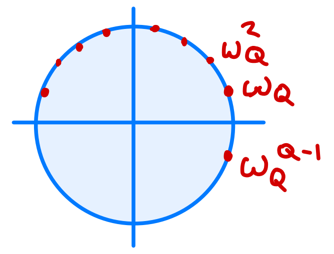
- Which basis states have large amplitudes ? ← Constructive Interference
- Which ones have small or zero amplitudes ? ← Destructive Interference

Let us look at $\underbrace{\sum_{j=0}^{K-1} \left(\omega_Q^{bp}\right)^j}$

Sum of roots of unity $\omega_Q^{bp} = \omega$ ← This is ω_Q^r where $r = bp \bmod Q$

$1 + \omega + \omega + \dots + \omega^{k-1}$

- If $r = 0$, we sum the trivial root k times
  Constructive interference if $\frac{bp}{Q}$ is integer



If $r \neq 0$, since $1 + \omega_N + \omega_N^2 + \dots + \omega_N^{N-1} = 0$ for some N^{th}-root of unity
and since we go around the circle an integer # of times

$\Rightarrow$ the sum evaluates to 0

Destructive interference if $\frac{bp}{Q}$ is not an integer

$\frac{bp}{Q} \in \mathbb{Z}$

$b = \frac{Q}{p} \cdot z$

Overall, we get that the state at time 4 is

$$\frac{1}{\sqrt{KQ}} \sum_{b=0}^{Q-1} \omega_Q^{bx} \underbrace{\left(\sum_{j=0}^{K-1} \omega_Q^{bjP} \right)} |b\rangle$$

$= k$ if $\frac{bp}{Q}$ is an integer which happens for $b = 0, \frac{Q}{p}, \frac{2Q}{p}, \dots, \frac{(p-1)Q}{p}$

$$= \sqrt{\frac{K}{Q}} \left(\sum_{l=0}^{p-1} \omega_Q^{l \cdot \frac{Q}{p} \cdot x} \left| l \frac{Q}{p} \right\rangle \right)$$

If we measure it, we get a random integer b that is a multiple of $\boxed{\frac{Q}{p}}$ ↱ an integer

i.e, we get $b = \frac{\ell Q}{p}$ where $\ell \in \{0, \dots p-1\}$ is uniformly chosen and $\frac{Q}{p}$ is an integer, say R

$\boxed{\text{Note}}$ The algorithm knows Q because we picked it and b which is the outcome of the measurement

But it does not know $\underline{\ell \text{ or } p}$ e.g. if $b = 3 \cdot \frac{Q}{17}$ or $b = 6 \cdot \frac{Q}{34}$

If we do this several times, we get random samples

$$\ell_1 R, \ \ell_2 R, \ \ell_3 R, \dots$$

e.g. say $R = 7$

14, 49, ...

If ℓ_i and ℓ_j are coprime, i.e. $\gcd(\ell_i, \ell_j) = 1$

$$\Rightarrow \gcd(\ell_i R, \ell_j R) = R$$

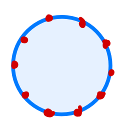
The largest common factor between $\ell_i R$ and $\ell_j R$ is R

Of course, the algorithm does not know ℓ_i's but if we do this many times and take gcd of all pairs and say take the minimum, we will succeed with high probability

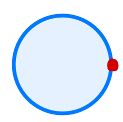
$\boxed{\text{Hard case}}$ When $\frac{Q}{p}$ is not an integer which is what happens when function is almost-periodic

Previously (when $\frac{Q}{p}$ was integer)

$$\frac{1}{\sqrt{KQ}} \sum_{b=0}^{Q-1} \omega_Q^{bx} \underbrace{\left(\sum_{j=0}^{K-1} \omega_Q^{bjp} \right)}_{= \begin{cases} 0 & \text{if } b \neq \text{multiple of } \frac{Q}{p} \\ \text{OR} & \\ k & \text{if } b = \text{multiple of } \frac{Q}{p} \end{cases}} |b\rangle$$



sum roots around circle

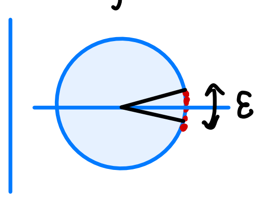


sum trivial root

Now, (when $\frac{Q}{p}$ is not an integer) we will mostly see constructive interference if $k =$ nearest-integer(multiple of $\frac{Q}{p}$) [integer]

and destructive interference if $k \neq$ nearest-integer(multiple of $\frac{Q}{p}$)

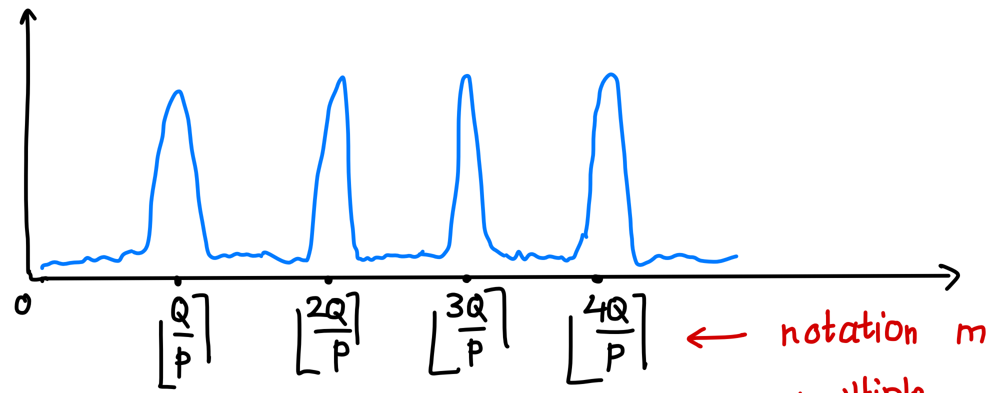
Basically, constructive interference occurs because :



we sum over complex values $e^{i 2\pi \varepsilon}$ where $\varepsilon \approx 0$ so the values are close to 1 destructive interference occurs because again the values almost cancel out

$$\frac{1}{\sqrt{KQ}} \sum_{b=0}^{Q-1} \underbrace{\omega_Q^{bx}\left(\sum_{j=0}^{K-1} \omega_Q^{bjp}\right)}_{:=\alpha_b} |b\rangle$$

If we plot $|\alpha_b|$ it now looks like (this is what matters for measurement)



← notation means nearest integer multiple

If we measure, with high probability we will output an integer $b_1 = \lfloor \ell_1 \frac{Q}{p} \rfloor$

Final thing that remains to do : if we get $b_1 = \lfloor \ell_1 \frac{Q}{p} \rceil$, $b_2 = \lfloor \ell_2 \frac{Q}{p} \rceil$, $b_3 = \lfloor \ell_3 \frac{Q}{p} \rceil$

how do we find p ? Next time

$\boxed{\text{NEXT TIME}}$ + RSA Cryptosystem and Shor's Factoring Algorithm