LECTURE 13 March 4^{th}, 2025

PART II Fundamental Quantum Algorithms

$\boxed{\text{Today}}$ QFT and 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 $\quad |x\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{s=0}^{N-1} \omega_N^{xs} |s\rangle$

E.g (N=4)
$$QFT_4 = \frac{1}{\sqrt{4}} \begin{bmatrix} \omega_4^0 & \omega_4^0 & \omega_4^0 & \omega_4^0 \\ \omega_4^0 & \omega_4^1 & \omega_4^2 & \omega_4^3 \\ \omega_4^0 & \omega_4^2 & \omega_4^4 & \omega_4^6 \\ \omega_4^0 & \omega_4^3 & \omega_4^6 & \omega_4^9 \end{bmatrix}$$
can express mod 4 since $\omega_4^4 = 1$

QFT_N can be implemented with $O(n^2)$ 1 and 2 qubit gates for $N=2^n$

Let's see how to do this by example, Say $N = 16$

We want to implement $|x\rangle \xrightarrow{DFT_{16}} \frac{1}{\sqrt{16}} \sum_{s=0}^{N-1} \omega_{16}^{sx} |s\rangle$ where $\omega_{16} = e^{\frac{2\pi i}{16}} := \omega$

$$DFT_{16}|x\rangle = \frac{1}{4}\left(|0000\rangle + \omega^x |0001\rangle + \omega^{2x} |0010\rangle + \omega^{3x}|0011\rangle + \dots + \omega^{15x}|1111\rangle\right)$$

Is this state entangled? No!

$$= \underbrace{\left(\frac{|0\rangle + \omega^{8x}|1\rangle}{\sqrt{2}}\right)}_{|s_3\rangle} \otimes \underbrace{\left(\frac{|0\rangle + \omega^{4x}|1\rangle}{\sqrt{2}}\right)}_{|s_2\rangle} \otimes \underbrace{\left(\frac{|0\rangle + \omega^{2x}|1\rangle}{\sqrt{2}}\right)}_{|s_1\rangle} \otimes \underbrace{\left(\frac{|0\rangle + \omega^{x}|1\rangle}{\sqrt{2}}\right)}_{|s_0\rangle}$$

Compare this to the following step in Simon's algorithm:

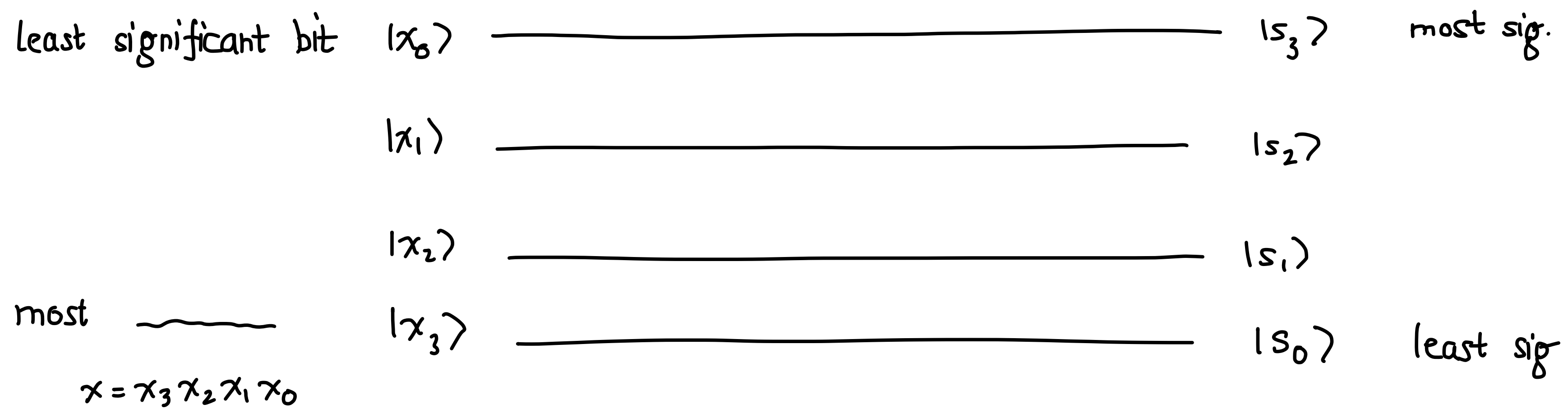
$$H^{\otimes n}|x\rangle = \underset{\substack{\uparrow \\ \text{if } x_2=1}}{|+\rangle \otimes |-\rangle} \otimes \underset{\substack{\uparrow \\ \text{if } x_3=0}}{|+\rangle} \otimes \dots$$

output qubit i depends only on input qubit x

For QFT, each output qubit depends on all n-input qubits

We will do the transform qubit-by-qubit

It will be very convenient to reverse the order



One can do $\frac{n}{2}$ SWAP gates to reverse the order at the end

To do the 0^{th} wire, we need to get $\frac{|0\rangle + \omega^{8x}|1\rangle}{\sqrt{2}}$ ← Seems like this depends on all 4 qubits of x

Notice, $\omega^8 = \omega_{16}^8 = (-1)$

so, $\omega^{8x} = (-1)^x$ and it only depends on whether x is even or odd, i.e. on x_0

So, we want $\frac{|0\rangle + (-1)^{x_0}|1\rangle}{\sqrt{2}} = H|x_0\rangle$

To do the 1^{st} wire, we need to get $\frac{|0\rangle + \omega^{4x}|1\rangle}{\sqrt{2}}$ ← Seems like this depends on all 4 qubits of x again

$\omega^4 = i$, so $\omega^{4x} = i^x$ ← only depends on x mod 4 i.e. x_0 and x_1

$$\omega^{4x} = \omega_{16}^{4(x_0 + 2x_1 + \cancel{4x_2} + \cancel{8x_3})}$$ since $16x_2, 32x_3 = 0$

$$= \omega^{4x_0} \cdot \omega^{8x_1} = (\omega^4)^{x_0} (-1)^{x_1}$$

So, the $|1\rangle$ state should pick up phase (-1) if $x_1 = 1$ ← Hadamard

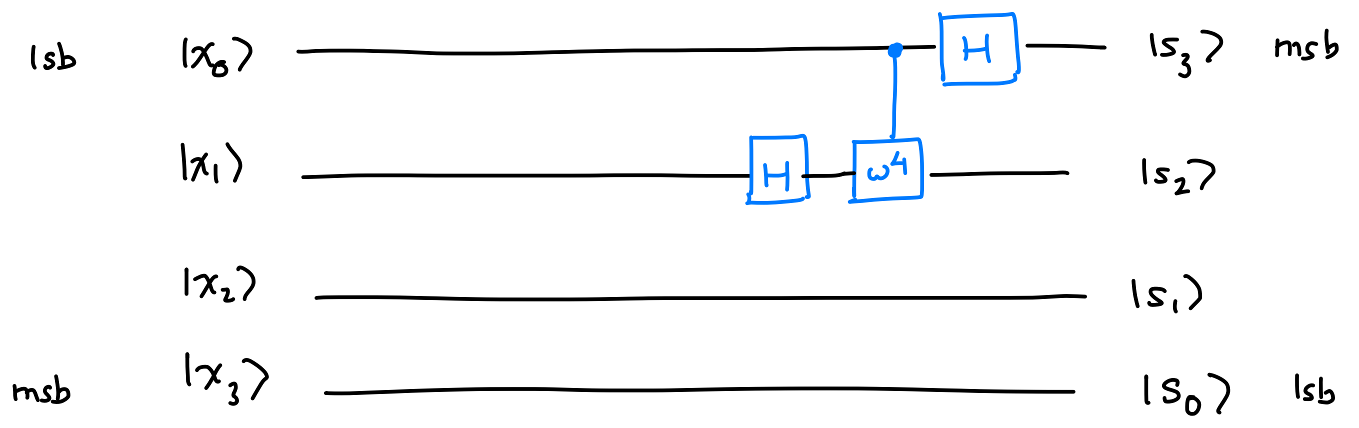
should also pick up phase ω^4 if $x_0 = 1$

"controlled - ω^4" gate, control qubit $= x_0$

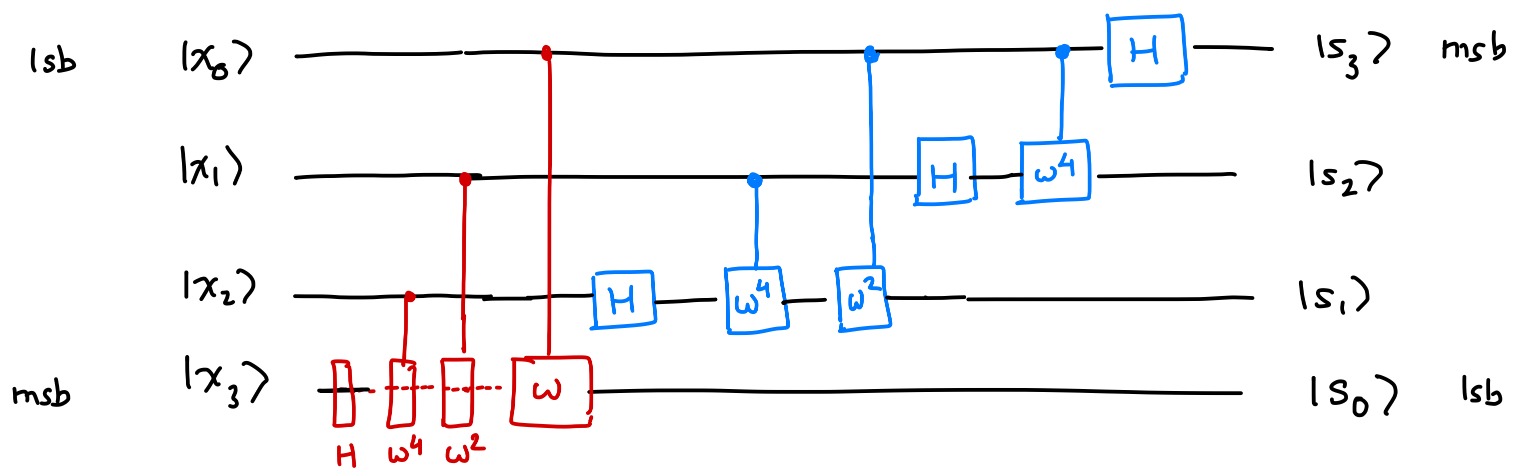
$|00\rangle \longrightarrow |00\rangle \qquad |10\rangle \longrightarrow \omega^4 |10\rangle$

$|01\rangle \longrightarrow |01\rangle \qquad |11\rangle \longrightarrow \omega^4 |11\rangle$

$$\begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & \omega^4 \end{bmatrix}$$



Rest is similar, in the end we have



Total gates : $1 + 2 + 3 + 4 + \cdots + n = O(n^2)$

$\boxed{\text{Final Remarks}}$ For general n, say $n = 1000$ $\quad \omega_{2^n}$ is the controlled 2^{1000}-th root of unity phase shift gate

We cannot build this accurately in practice

In general, not realistic for 2^k root of unity for $k \geq 30$

Luckily, it's not a problem!

$\boxed{\text{FACT}}$ Suppose we delete all gates where $k \geq \log\left(\frac{n}{\varepsilon}\right)$ E.g. $k=30$, $\varepsilon = 1\%$

Then, the resulting circuit

- "ε approximates" DFT_N $\rightarrow$ success probability of Shor's algorithm only goes down by ε
- remaining gates can be built since they have large phases
- only $O(n \log(\frac{n}{\varepsilon}))$ gates remain $\leftarrow$ Near linear size? Way more efficient!

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

$\mathbb{Z}_N$ = 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

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

$0^2 = 0$ $\quad 2^2 = 0$

$1^2 = 1$ $\quad 3^2 = 1$

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

$\uparrow$ 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

$\underbrace{\qquad\qquad}_{p}\ \underbrace{\qquad\qquad}_{p}\ \underbrace{\qquad\qquad}_{p}$

$N = 12$
$= 4$

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 $f : \mathbb{Z}_Q \rightarrow$ COLORS

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

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

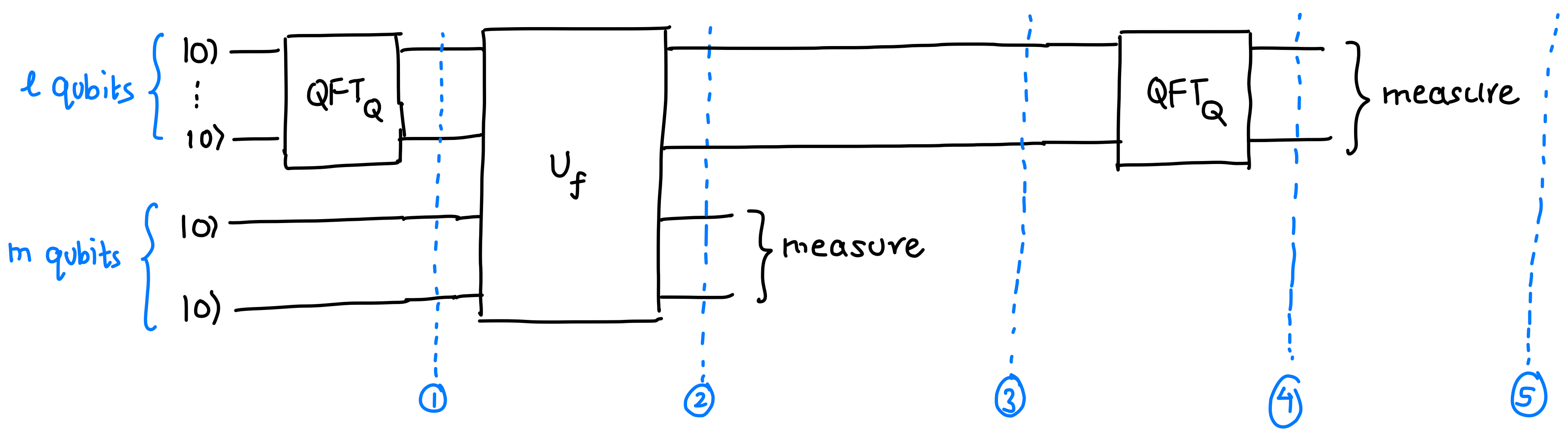
Moreover, the values $f(0), \dots f(p-1)$ are assumed to be distinct

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

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

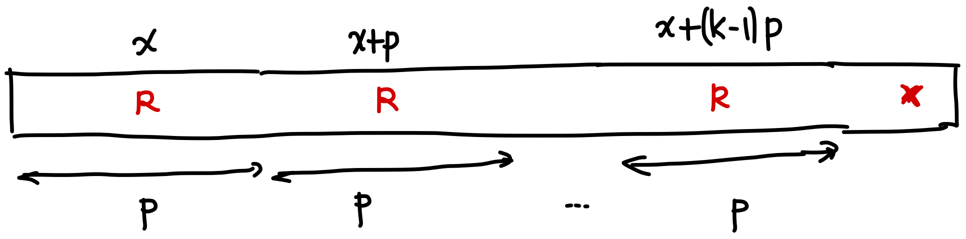
Note: Here we could have applied $H^{\otimes \ell}$ as well since

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

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

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

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

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 $\underbrace{\sum_{j=0}^{K-1} \left(\omega_Q^{bp}\right)^j}_{\text{Sum of roots of unity}}$

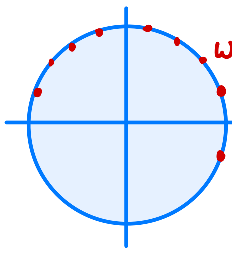
Sum of roots of unity $\omega_Q^{bp} = \omega$ ← This is ω_Q^r

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

where $r = bp \mod Q$

- 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

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

$b = \frac{Q}{P} \cdot \mathbb{Z}$

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

Overall, we get that the state at time 4 is

$$\frac{1}{\sqrt{KQ}} \sum_{b=0}^{Q-1} \omega_Q^{bx} \underbrace{\left(\sum_{j=0}^{K-1} \omega_Q^{bjp} \right)}_{= k \text{ if } \frac{bp}{Q} \text{ is an integer}} |b\rangle$$

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

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

$\hookrightarrow$ an integer

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

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

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

$\ell_1 R, \ell_2 R, \ell_3 R, \ldots$ e.g. say $R = 7$

$14, 49, \ldots$

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

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

NEXT TIME + RSA Cryptosystem and Shor's Factoring Algorithm