Lecture 15: Period-Finding: Simon's Algorithm over $\mathbb{Z}_N$.

(This lecture is basically a carbon copy of Lecture 13 – Simon's Alg – but over $\mathbb{Z}_N$.)

The setup: Given access to quantum circuit Q_F implementing $F: \mathbb{Z}_N \to \text{COLORS}$.

$N = 2^n$ $\quad$ COLORS $\cong \{0,1\}^m$

Promised F is "L-periodic":

$\forall X \;\; F(X) = F(X+L) = F(X+2L) = F(X+3L) = \dots$

& "otherwise colors distinct" ($F(X) = F(Y)$
$\Rightarrow Y - X$ is mult. of L)

e.g. $L = 4$:

F	R	G	B	Y	R	G	B	Y	R	---	Y
	0	1	2	3	4	5	-	-	-	-	$N-1$

Task: find L,
(using few quantum gates & few applications of Q_F)

Dopey issue: L-periodicity $\Rightarrow L$ divides $\underset{2^n}{\overset{\shortparallel}{N}}$

$\Rightarrow L \in \{1, 2, 4, 8, \ldots, 2^{n-1}\}$

(Only n possibilities, so classically: easy to try them all.)

(Mollifying remarks:)

Rem. 1: For today's alg., no need to assume $N = 2^n$ → except when implementing DFT_N.

(And not even then, technically. And there are some N with $\approx N^{\frac{1}{\log\log N}}$ divisors — a ton!)

Rem. 2: We'll see Simon's Alg. still basically works even if $L \nmid N$ and L-periodicity fails at the "mod N wraparound".

((Shor '94 proved all these results from today's lecture & the previous one. With them in hand, the quantum factoring alg. is basically done, thanks to known number theory algorithms from ~40 years ago.))

[Let's do it!] Usual "quantum Fourier sampling" paradigm:

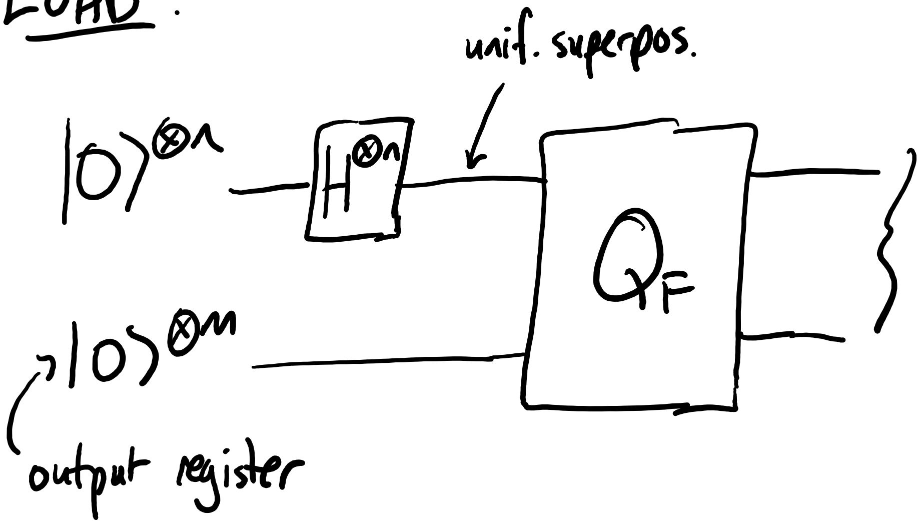
- "Load" F into quantum state
- Discrete Fourier Transform

Measure

↳ gives "clue" about L

(Repeat ≈ 4 times, get enough clues to learn L.)

<u>LOAD</u>:



$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |F(x)\rangle$$

$$\text{e.g. } \frac{1}{\sqrt{N}} \Big(|0\rangle|R\rangle + |1\rangle|G\rangle + |2\rangle|B\rangle + |3\rangle|Y\rangle + |4\rangle|R\rangle + \cdots \Big)$$

Finally: Measure output (color) register.

(As discussed in Simon's Alg., technically don't need to do this...)

Each color used $\frac{N}{L}$ times.

$\Rightarrow$ each color appears on measurement readout w/ prob. $\frac{1}{L}$.

Conditioned on readout $C^* \in$ COLORS, state collapses to...

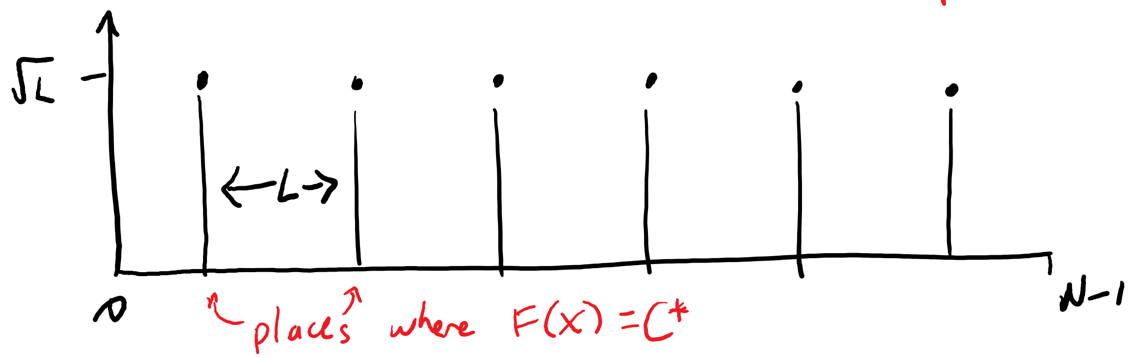
$$\underbrace{(\text{normalizing factor})}_{\sqrt{\frac{L}{N}}} \cdot \sum_{X : F(X) = C^*} |X\rangle \cancel{|C^*\rangle}$$ discardable

$=: |g_{C^*}\rangle$ for what function $g_{C^*} : \mathbb{Z}_N \to \mathbb{R}$?

$$g_{C^*}(X) = \begin{cases} \sqrt{L} & \text{if } F(X) = C^* \\ 0 & \text{else.} \end{cases}$$

($\sqrt{L}$ times the "indicator function for $F = C^*$".
Don't be alarmed that g_{C^*}'s values are sometimes > 1. Recall: $|g\rangle$ a quantum state iff average value of $|g|^2$ is 1.)

State now $|g_{c^*}\rangle$: [[g_{c^*} is an L-periodic "spike train".]]



[[Rotate, Compute, rotate.]]

$$\Big\downarrow \mathrm{DFT}_N$$

[[$O(n^2)$ quantum gates, or $O(n \log^{n}/\varepsilon)$ if approximating.]]

new state: $\displaystyle\sum_{s=0}^{N-1} \hat{g}_{c^*}(s)\,|s\rangle$

[[Strength of discrete cosine χ_s in g_{c^*}.]]

Measure

[[We'll think about these Fourier coeffs soon.]]

Readout "s" $\in \{0, 1, \ldots, N-1\}$ with prob. $|\hat{g}_{c^*}(s)|^2$.

[[Hopefully gives a "clue" about L.]]

Pleasing Claim: $|\widehat{g_{C^*}}(S)|^2$ doesn't depend on C^*!

[Great! Means we don't have to worry about what the color measurement is. Equiv., can pretend $C^* = F(0)$, We saw this same phenomenon in Simon's Alg..]

Lemma: (on HW7, #5, in $\mathbb{F}_2^n$ case)

If $f: \mathbb{Z}_N \to \mathbb{C}$, $y \in \mathbb{Z}_N$, define (translated function)

$f^{+y}: \mathbb{Z}_N \to \mathbb{C}$ by $f^{+y}(x) = f(x+y)$.

Then $\widehat{f^{+y}}(S) = \hat{f}(S) \cdot \underbrace{(\text{some } N^{th} \text{ root of } 1)}_{\text{magnitude } 1.}$

(goes away when you put $|\cdot|$ on both sides)

Proof:

$$\widehat{f^{+y}}(S) = \operatorname*{avg}_{x=0}^{N-1} \{ \chi_s(x)^* f^{+y}(x) \} = \operatorname*{avg}_{x} \{ \chi_s(x)^* f(x+y) \}.$$

Change vbl: $z = x+y$, $\Rightarrow x = z-y$. As x runs thru $0 \ldots N-1$, so too does z.

Hence it's $= \operatorname*{avg}_{z=0}^{N-1} \{ \chi_s(z-y)^* f(z) \}$

(by "character" ppty.)

$$= \operatorname*{avg}_{z} \{ \chi_s(-y)^* \chi_s(z)^* f(z) \} = \underbrace{\chi_s(-y)^*}_{\omega_N^{s \cdot y}} \cdot \hat{f}(S). \blacksquare$$

$\therefore$ May assume $C^* = F(0)$, hence g_{c^*} is the simplest L-periodic "spike train":

$$g(x) = \begin{cases} \sqrt{L} & \text{if } x \in \{0, L, 2L, 3L \ldots\} \\ 0 & \text{else} \end{cases}$$

["subgroup of $\mathbb{Z}_N$ generated by L"]

Claim: (mentioned last time) $\hat{g} : \mathbb{Z}_N \to \mathbb{C}$ is (simplest) $\frac{N}{L}$-periodic spike train:

$$\hat{g}(s) = \begin{cases} \frac{1}{\sqrt{L}} & \text{if } s \in \{0, \frac{N}{L}, \frac{2N}{L}, \frac{3N}{L}, \ldots\} \\ 0 & \text{else} \end{cases}$$

(Why is that the normalizing constant? We know...)

$$|g\rangle \xmapsto{DFT_N} \sum_{s=0}^{N-1} \hat{g}(s) |s\rangle$$

quantum state,

$$\Rightarrow \sum_s |\hat{g}(s)|^2 = 1$$

[$\hat{g}$ has L nonzero vals, so each is $\frac{1}{\sqrt{L}}$.]

So DFT gets us to

$$\frac{1}{\sqrt{L}} \sum_{s:\ s\cdot L \equiv 0 \bmod N} |s\rangle.$$

[[Compare with Simon! Same, except "s•L" was the $\mathbb{F}_2^n$ - dot product!]]

$\Rightarrow$ Measuring will read out a <u>random</u> $s \in \{0, M, 2M, 3M, \ldots N-M\}$.

[[All L multiples of $M = \frac{N}{L}$ less than N]]

where $M := \frac{N}{L}$.

[[color Multiplicity]]

Great "clue". We'll see: from a few multiples can discover M, hence $L = N/M$.

Theorem: For $g(X) = \begin{cases} \sqrt{L} & \text{if } X \in \{0, L, 2L, 3L, \dots\} \\ 0 & \text{else} \end{cases}$,

$$\hat{g}(S) = \begin{cases} \frac{1}{\sqrt{L}} & \text{if } S \in \{0, M, 2M, 3M, \dots\} \quad \left(M = \frac{N}{L}\right) \quad (*) \\ 0 & \text{else.} \quad (**) \end{cases}$$

Proof: A trick: We know (unitarity) that $\sum_S |\hat{g}(S)|^2 = 1$. So if we verify $(*)$, we already have $L \cdot \left|\frac{1}{\sqrt{L}}\right|^2 = 1$ squared-amplitude, so $(**)$ follows!

Verifying $(*)$: $\hat{g}(S) = \underset{X=0}{\overset{N-1}{\text{avg}}} \{\chi_S(X)^* g(X)\}$ $\quad \frac{1}{N}\sum_X$

$$= \frac{\sqrt{L}}{N} \sum_{X=0,L,2L,\dots} \chi_S(X)^* \leftarrow \omega_N^{-X \cdot S}$$

$$= \frac{\sqrt{L}}{N} \cdot M \cdot \underset{j=0}{\overset{M-1}{\text{avg}}} \left\{ \omega_N^{-\boxed{(jL) \cdot S}} \right\}$$

If $S \in \{0, M, 2M, \dots\}$
$= (jL) \cdot kM$
$= jk \cdot LM$
$= jk \cdot N$

$$= \frac{1}{\sqrt{L}} \cdot \underset{j=0}{\overset{M-1}{\text{avg}}} \{ \underbrace{\omega_N^{-jkN}}_{1^{-jk} = 1} \} = \frac{1}{\sqrt{L}} \cdot \text{avg}\{1\} = 1/\sqrt{L}. \blacksquare$$

Summary: Given Q_F for L-periodic
$F : \mathbb{Z}_N \to$ COLORS . . .

LOAD F: n H's, 1 Q_F :)

DFT_N : $\leq n^2$ gates :)

measure : Gives uniformly random

$S \in \{0, M, 2M, 3M, \ldots\}$,

$M = N/L$. (Much easier to finish, compared to Simon: just 2 repetitions, not $n-1$.)

Claim: Repeat twice, to get
$k_1 M$, $k_2 M$ for
random $0 \leq k_1, k_2 < L$ . . . .
good chance of learning M . . .
and hence $L = N/M$.

[You know N, so just do an n-bit division: $\leq n^2$ classical steps. :)]

[How to learn M from random multiples of M? GCD!]

$$\gcd(k_1 M, k_2 M) = \underbrace{\gcd(k_1, k_2)}\cdot M$$

if 1, you're in luck.

[We'll show there's a decent chance k_1, k_2 have GCD = 1. "In practice, would just take 10 or 20 random multiples of M and GCD them all → very high probability to get M.]

(Recall: HW2, #8, classically can do GCD of n-bit #'s in $\approx n^2$ steps.) (Or $\tilde{O}(n)$ with very sophisticated alg.)

Claim: (On HW6, #8, but I'll repeat it.)

For k_1, k_2 random from $\{0, 1, 2, \ldots, L-1\}$,

$\Pr[\gcd(k_1, k_2) = 1] \geq 5\%$. (Actually, $\approx 55\%$.)

(Implies: expected ≤ 20 (indeed, ≤ 2) repetitions of whole alg. to get gcd $= 1$.)

Proof: $\Pr[k_1, k_2 \text{ both} \neq 0] = \text{high}$.

Even if $L = 2$, it's $\geq \frac{1}{4}$.

We'll show $\Pr_{k_1, k_2 \sim \{1, 2, \ldots, L-1\}} [\gcd(k_1, k_2) = 1] \geq 20\%$. ← no 0

Fix a prime P. If $P | k_1$ and $P | k_2$ → bad, gcd $\geq P$.

$\Pr[P | k_1, k_2] = \Pr[P | k_1]^2 \leq \frac{1}{P^2}$.

[[$\leq \frac{1}{P}$ frac. of #'s in $\{1, 2, \ldots, L\}$ are in $\{P, 2P, 3P, \ldots\}$]]

If no bad P: gcd $= 1$.

$$\Pr[\text{any bad } P] \underset{\text{union bound}}{\leq} \Pr[2 | k_1, k_2] + \Pr[3 | k_1, k_2] + \cdots$$

$$\leq \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{5^2} + \frac{1}{7^2} + \frac{1}{11^2} + \cdots$$

(numerical fact) $\approx .45$. $\therefore \Pr[\text{good}] \geq .55$.

Elementary bound:

$$\leq \frac{1}{2^2} + \frac{1}{3^2} + \left(\frac{1}{5^2} + \frac{1}{6^2} + \cdots + \frac{1}{9^2}\right) + \left(\frac{1}{10^2} + \cdots + \frac{1}{19^2}\right) + \left(\frac{1}{20^2} + \cdots + \frac{1}{39^2}\right) + \cdots$$

$$\leq \frac{1}{4} + \frac{1}{9} + 5 \cdot \frac{1}{5^2} + 10 \cdot \frac{1}{10^2} + 20 \cdot \frac{1}{20^2} + \cdots$$

$$= \frac{1}{4} + \frac{1}{9} + \frac{1}{5}\left(1 + \frac{1}{2} + \frac{1}{4} + \cdots\right)$$

$$= \frac{1}{4} + \frac{1}{9} + \frac{2}{5} = .25 + .111\cdots + .4$$

$$= .76111\cdots \leq 80\%$$

$$\therefore \Pr[\text{good} : \gcd = 1] \geq 20\%. \quad \blacksquare$$

What if L doesn't divide N?

F: $\underset{0\ 1\ 2\qquad\qquad\qquad\qquad\qquad N-1}{\boxed{RGBYRGBY\text{-----}RGB}}$

Now $M = N/L$ not an integer!

Each color used ~~M times~~ ?

$\lfloor M \rfloor$ or $\lceil M \rceil$ times.

Each value $0, M, 2M, 3M, \ldots$ read out with prob. $\frac{1}{L}$ when measuring S?

Claim: For each value $0, \lfloor M \rceil, \lfloor 2M \rceil, \lfloor 3M \rceil, \ldots$

(where $\lfloor \alpha \rceil :=$ nearestInteger(α)),

read out with prob. $\geq \frac{.4}{L}$.

(So... a solid 40% of your samples are of the form NearestInt(random mult of M).

That'll be good enough for Shor....)

Proof Sketch: Measured color C^* occurs some M' times, either $\lfloor M \rfloor$ or $\lceil M \rceil$.

Before: $\Pr[\text{read out } S] = |\hat{g}_{c^*}(S)|^2 = |\hat{g}(S)|^2$,

where $\hat{g}(S) = \frac{1}{\sqrt{L}} \operatorname*{avg}_{j=0}^{M-1} \{\omega_N^{-jL\cdot S}\}$.

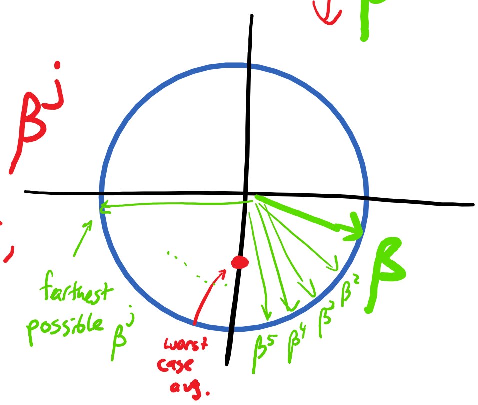
Now (I assure you...): $\Pr[\text{read out } S] =$

$$\cancel{\frac{1}{L}} \; \frac{M'}{N} \cdot \left| \operatorname*{avg}_{j=0}^{M'-1} \left\{ \omega_N^{-jL\cdot S} \right\} \right|^2.$$

Before: $S = kM \Rightarrow \omega_N^{-jL\cdot S} = (\omega_N^{-kL\cdot M})^j = (\omega_N^{-kN})^j = 1^j$.

Now: $S = \lfloor k\hat{M} \rceil \Rightarrow \omega_N^{-jL\cdot S} = \left(\omega_N^{-L(kM \pm \frac{1}{2})}\right)^j = \left(\omega_N^{-\frac{1}{2}L \dots \frac{1}{2}L}\right)^j \downarrow \beta^j$

difference is in range $[-\frac{1}{2}, \frac{1}{2}]$



(β is pretty close to 1. We're averaging β^j over $j = 0, 1, 2, \dots, \approx M = \frac{N}{L}$. At worst, β is $\omega_N^{\pm \frac{1}{2} L}$, so last averaged val. is $\approx (\omega_N^{\pm L/2})^{N/L} = \omega_N^{\pm N/2} \longrightarrow$ can't make it all the way around to get avg. ≈ 0. Worst case, avg is $\approx \pm .63i$. Squared magnitude $\geq .4$.)