CSCE 785
10/26/2023

Shor's Algo (cont)
QFT

What I saw: Prob $= (-\frac{1}{2})^2 + \underbrace{(\frac{i}{2})^2}_{\text{must take } |\cdot|} = \frac{1}{4} \overset{+}{\cancel{-}} \frac{1}{4} = 0$ ✗

Last time: DFT_m unitary: $[DFT]_{jk} = \omega^{jk}/\sqrt{m}$

$[0 \le i, j < m]$

$$\boxed{\omega = e^{2\pi i/m}}$$

$[DFT^*]_{jk} = [DFT]_{kj}^* = (\omega^{kj})^*$

$\omega^* = \omega^{-1}$

$$[DFT_m^* DFT_m]_{jk} = \frac{1}{m}\sum_{l=0}^{m-1} [DFT_m^*]_{jl}[DFT]_{lk}$$

$$= \frac{1}{m}\sum_l (\omega^*)^{lj}\omega^{lk} = \frac{1}{m}\sum_l \omega^{-lj}\omega^{lk}$$

$$= \frac{1}{m}\sum_l \omega^{l(k-j)}$$

$j=k$: $= \frac{1}{m}\sum_l \omega^0 = \frac{1}{m}\sum_l 1 = 1 = \delta_{jk}$

$j \ne k$: $= \frac{1}{m}\sum_{l=0}^{m-1} (\underbrace{\omega^{k-j}}_{\ne 1})^l = \frac{1}{m}\left(\frac{(\omega^{k-j})^m - 1}{\omega^{k-j} - 1}\right)$

$$= \frac{1}{m}\left(\frac{(\omega^m)^{k-j} - 1}{\omega^{k-j} - 1}\right) = \frac{1}{m}\left(\frac{1-1}{\omega^{k-j} - 1}\right) = 0 = \delta_{jk}$$

$\therefore DFT_m^* DFT = I_m$ $\therefore DFT_m$ is unitary //

<u>Def</u>: The n-qubit <u>Quantum Fourier Transform</u>

is $QFT_n = DFT_{2^n}$ $\boxed{m = 2^n}$

For now: we identify an $x \in \{0,1\}^n$ with its binary representation in $\mathbb{Z}_{2^n}$

0^n — 0
$0^{n-1}1$ — 1
$0^{n-2}10$ — 2
$\vdots$
1^n — $2^n - 1$

Shorthand: define for $x \in \mathbb{Z}$

$$e_n(x) := \exp(2\pi i x / 2^n)$$
$$= \exp(2\pi i / 2^n)^x$$

Basic properties

$$e_n(x+y) = e_n(x) e_n(y)$$
$$e_n(0) = 1 = e_n(2^n)$$
$$e_n(x) = e_n(x \bmod 2^n)$$
$$e_n(x) = e_{n+1}(2x)$$
$$\cancel{e_{n+r}(x) =}$$
$$e_n(x) = e_{n+r}(2^r x)$$
(more generally)

For any $x \in \mathbb{Z}_{2^n}$,

$$QFT_n |x\rangle := \frac{1}{2^{n/2}} \sum_{y \in \mathbb{Z}_{2^n}} e_n(xy) |y\rangle$$

$$= \frac{1}{2^{n/2}} \left(|0\rangle + e_1(x)|1\rangle\right) \otimes \left(|0\rangle + e_2(x)|1\rangle\right) \otimes \cdots$$

$$\cdots \otimes \left(|0\rangle + e_n(x)|1\rangle\right)$$

$$= \frac{1}{2^{n/2}} \bigotimes_{k=1}^{n} \left(|0\rangle + e_k(x)|1\rangle\right)$$ [Proof: Exercise]

Shor's Algorithm

Input: $N > 1$ (the modulus) and $a \in \mathbb{Z}_N^*$
Output: ord(a) in $\mathbb{Z}_N$ with "high" probability

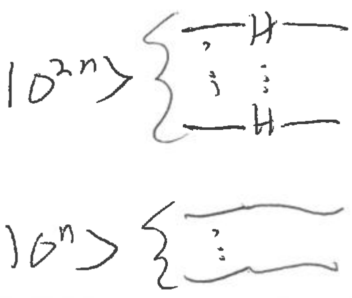
1. Let $n = \lceil \lg N \rceil$ $\quad \boxed{\lg = \log_2}$

   [an n-qubit register is big enough to hold N and any element of $\mathbb{Z}_N$.]

2. Initialize a 2n-qubit register to $|0^{2n}\rangle$ and an n-qubit register to $|0^n\rangle$

3. Apply $H^{\otimes 2n}$ to the 1^{st} register to get

$$(H^{\otimes 2n} \otimes I)(|0^{2n}\rangle \otimes |0^n\rangle) = \frac{1}{2^n} \sum_{x \in \mathbb{Z}_{2^{2n}}} |x\rangle \otimes |0^n\rangle$$



4. Apply a "classical" quantum circuit for modular exponentiation (mod N):

$$\frac{1}{2^n} \sum_{x \in \mathbb{Z}_{2^{2n}}} |x\rangle \otimes |0^n\rangle \longmapsto \overbrace{\frac{1}{2^n} \sum_x |x\rangle \otimes |a^x \bmod N\rangle}^{|\varphi\rangle}$$

[think: a, N are hardcoded into our circuit]

5. (Optional) Measure the 2nd register, get some value $w \in \mathbb{Z}_N$ (ignored):

$$\text{some normalization factor} \sum_{\substack{x \in \mathbb{Z}_{2^{2n}} \\ \text{such that} \\ a^x \bmod N = w}} |x\rangle$$

forgetting 2nd register

6. Apply QFT_{2n} to the first (now only) register:

Get

$$\bigcirc \sum_x QFT_{2n} |x\rangle = \bigcirc \sum_x \sum_{y \in \mathbb{Z}_{2^{2n}}} e_{2n}(xy) |y\rangle$$

7. Measure the first register, getting some $y \in \mathbb{Z}_{2^{2n}}$

8. Find smallest coprime integers k and $r > 0$ such that

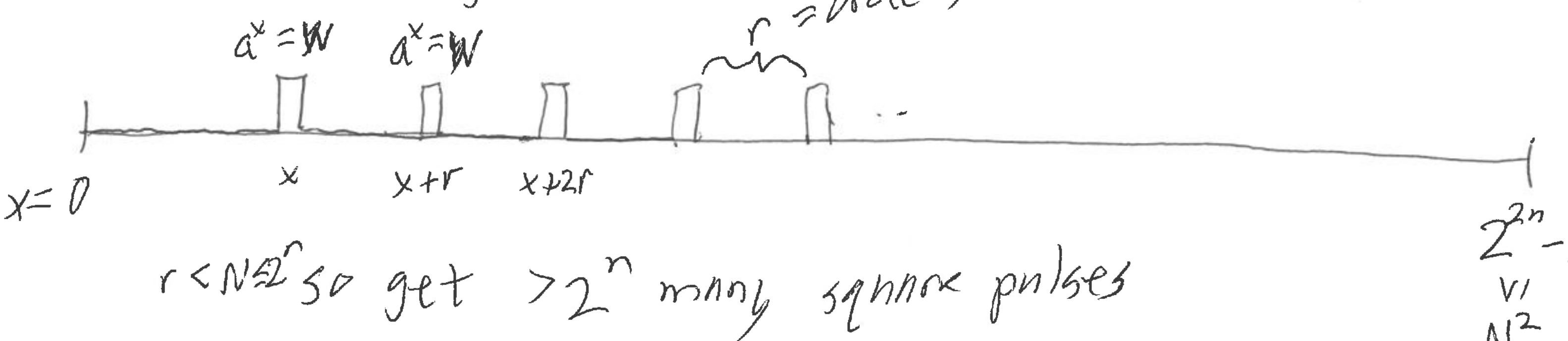
$$\left| \frac{y}{2^{2n}} - \frac{k}{r} \right| \leq 2^{-2n-1} = \frac{1}{2 \cdot 2^{2n}}$$

[Good rational approx to $y/2^{2n}$]

9. Classically compute $a^r \bmod N$
   If result is 1, output r.
   Otherwise "go back to the drawing board"
   Repeat the whole algo.

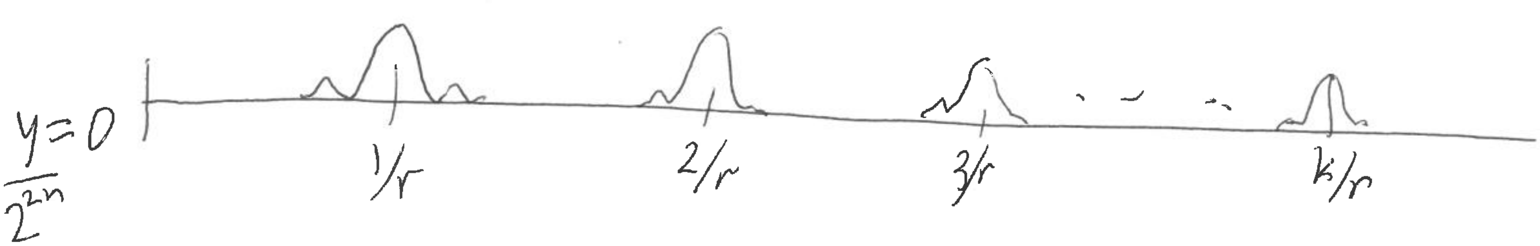
Signal processing intuition: x — 0 to $2^{2n}-1$
"time"

Think of the coeff on $|x\rangle$ after step 5 as the "signal"

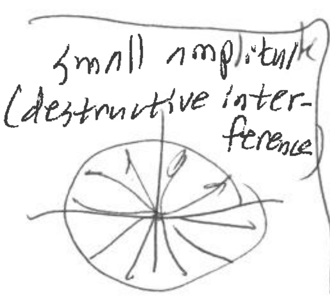


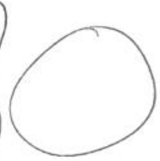
$r < N \leq 2^n$ so get $> 2^n$ many square pulses

$\Downarrow$ QFT [step 6]



State after step 6:





$$\sum_{y\in\mathbb{Z}_{2^{2n}}} \Bigg(\sum_{\substack{x\in\mathbb{Z}_{2^{2n}} \\ \text{s.t.} \\ a^x = w \pmod N}} e_{2n}(xy)\Bigg)|y\rangle$$