Lecture 14 - The Fourier Transform for $\mathbb{Z}_N$ ← integers modulo N

Recap: Lec. 12: The Fourier Transform for $\mathbb{F}_2^n$ ← $\{0,1\}^n$ with XOR operation

Decomposes $g : \{0,1\}^n \to \mathbb{C}$

into "strengths" of XOR functions

$$\chi_s(x) = (-1)^{s \cdot x} \leftarrow \text{dot prod. in } \mathbb{F}_2^n$$

$$|g\rangle = \sum_{s \in \{0,1\}^n} \hat{g}(s)\, |\chi_s\rangle$$

Lec. 13: Simon's Alg.

Given Q_F implementing an

"L-periodic" $F : \{0,1\}^n \to$ COLORS

$$F(x+L) = F(x) \quad \forall x$$

(and distinct otherwise)

with only $\approx n$ uses of Q_F,

determines L.

Today: The Fourier Transform for $\mathbb{Z}_N$

integers mod N

Decomposes $g: \mathbb{Z}_N \to \mathbb{C}$

into "strengths" of .... "discrete (co)sines"

$\chi_0 : \mathbb{Z}_N \to \mathbb{C}, \ \chi_1, \chi_2, \ldots, \chi_{N-1}$

Orthonormal functions/vectors.

$$\chi_s(x) = \omega_N^{s \cdot x}$$

product (mod N)

ints mod N

primitive N^{th} root of unity, $e^{2\pi i/N}$

Crucial: When $N = 2^n$, this Fourier Transform

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

"strength" of $|\chi_s\rangle$ in $|g\rangle$

computable with $\approx n^2$ 1- & 2-qubit gates

[In fact, to super-high accuracy, all you need, with $O(n \log n)$ gates.

Can also do it when N not a power of 2, but annoying, so we won't. See [Hales-Hallgren '00.]]

Next lec: Simon's Alg, but for $\mathbb{Z}_N$.

$F: \mathbb{Z}_N \to$ COLORS has

$\forall x \quad F(x) = F(x+L) = F(x+2L) = \cdots$

mod N (distinct o/w)

for some L (dividing N).

Using only ≈ 3 applications of Q_F, finds L.

Classically ... hard
not, for stupid reason:

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

only n possibilitees. [[Easy to check w/ $\approx n$ apps of Q_F.]]

Later: Still works even if $L \ll N$ doesn't divide $N \Rightarrow F$ not quite L-periodic.

Shor: Apply to F like $F(x) = A^x \bmod M$

[[For randomly chosen A. Can build Q_F for this ourselves!]]

Result helps to factor M!

Further lec: Generalize quantum Fourier transform to other "groups" G beyond $\mathbb{F}_2^n$, $\mathbb{Z}_N$, ... ?

(And also Simon's Alg. to "H-periodic" functions on the group, where H is a subgroup of G...)

Again: associate $f: \mathbb{Z}_N \to \mathbb{C}$ to

<u>vector</u> $|f\rangle = \frac{1}{\sqrt{N}} \begin{bmatrix} f(0) \\ f(1) \\ \vdots \\ f(N-1) \end{bmatrix} \in \mathbb{C}^N.$

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

A quantum state $\rightarrow$ if & only if $\operatorname*{avg}_{0 \le x < N} \{|f(x)|^2\} = 1.$

Want N "pattern functions" $\chi_0, \chi_1, \ldots, \chi_{N-1} : \mathbb{Z}_N \to \mathbb{C}$

such that $|\chi_0\rangle, \ldots, |\chi_{N-1}\rangle$ are <u>orthonormal</u> basis vectors.

(Inverse) Fourier Transform:

unitary $U = \begin{pmatrix} | & | & & | \\ |\chi_0\rangle & |\chi_1\rangle & \cdots & |\chi_{N-1}\rangle \\ | & | & & | \end{pmatrix}.$

(Fourier Transform: given any $|g\rangle$, finds its coeffs in χ-basis.)

(Well, I actually already told you the χ's, but let's try to "find" them. Kind of uses some "group theory", actually.)

Cool feature of XOR pattern fcns $\chi_s = (-1)^{s \cdot x}$?

$\mathbb{F}_2^n$ dot prod.

$$\boxed{\chi_s(x+y) = \chi_s(x)\chi_s(y)}$$

$\oplus$: XOR, $+$ in $\mathbb{F}_2^n$

Why? $\chi_s(x+y) = (-1)^{s\cdot(x+y)}$

$= (-1)^{s\cdot x + s \cdot y}$

$= (-1)^{s\cdot x}(-1)^{s\cdot y} = \chi_s(x)\chi_s(y)$

[χ_s is a "character" of the group.]

Want the same for $\chi_s : \mathbb{Z}_N \to \mathbb{C}$.

• Need $\chi_s(X+0) = \chi_s(X)\chi_s(0)$

$\|$

$\chi_s(X)$ $\Rightarrow \chi_s(0) = 1$ $\forall s$.

(Unless $\chi_s(X) = 0$ for all X, but that's undesirable.)

• Need $\chi_s(\underbrace{X + X + \cdots + X}_{N \text{ times}}) = \chi_s(X)\chi_s(X)\cdots\chi_s(X) = \chi_s(X)^N$

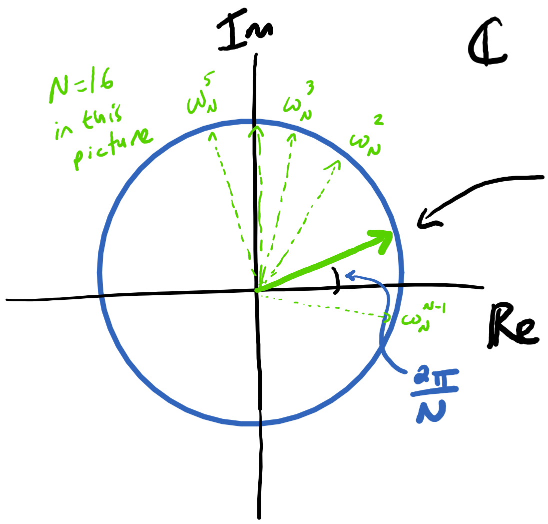
$= 0 \bmod N$

$\|$

$\chi_s(0) = 1$

$\Rightarrow \chi_s(X)$ an N^{th} root of unity!

[So in this $\mathbb{Z}_N$ world, <u>every</u> $\chi_s(x)$ value must be an N^{th} root of unity. So for $N > 2$, complex numbers are <u>forced</u> on us. This is really the one & only place where we need/want to go to complex numbers/amplitudes. If it weren't for this, we'd have stuck with real amplitudes for basically the whole course!]



$\mathbb{C}$

$$\omega_N := e^{2\pi i/N} = \cos\frac{2\pi}{N} + i\sin\frac{2\pi}{N}$$

"primitive" N^{th} root ("first") of unity.

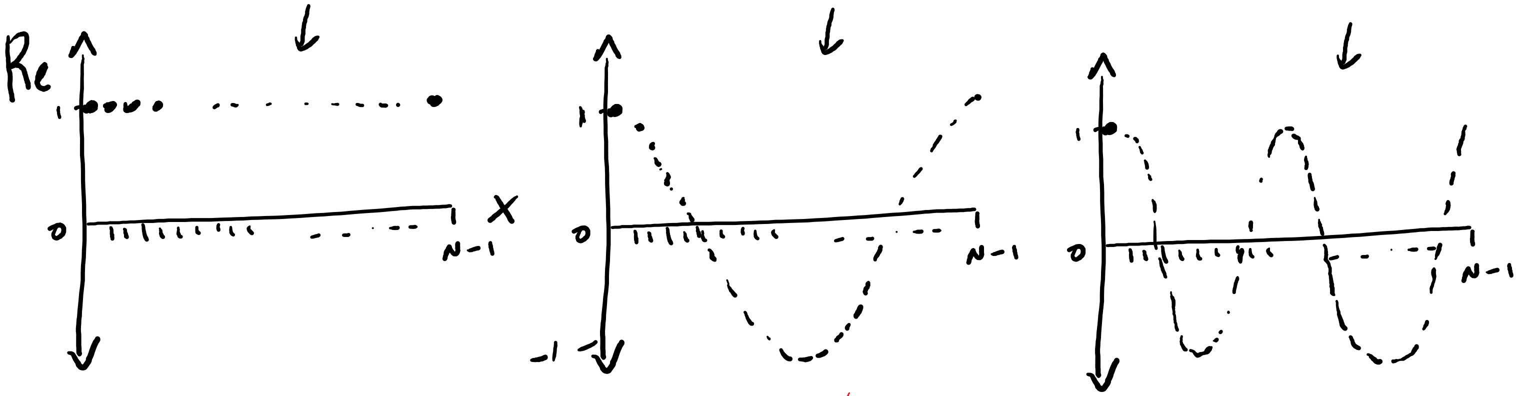
All others are

$$1 = \omega_N^0, \ldots, \omega_N^2, \omega_N^3, \ldots, \omega_N^{N-1}$$

def: For $0 \le s < N$,

$$\chi_s(x) = \omega_N^{s \cdot x} \leftarrow \text{mult. mod } N$$

eg: $\chi_0(x) \equiv 1$, $\chi_1(x) = \omega_N^{x}$, $\chi_2(x) = \omega_N^{2x}$



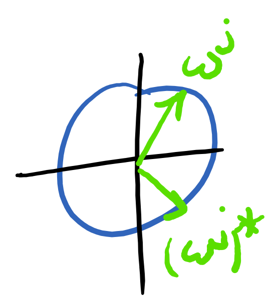
(like a discrete cosine wave)

Facts

- $\chi_0(x) = 1 \quad \forall x$ [[Just like in Boolean/Hadamard case. Implies $DFT_N|00\cdots0\rangle$ = uniform superpos, again]]

- $\chi_s(x)^* = \left(\omega_N^{s \cdot x}\right)^*$

$$= \omega_N^{-s \cdot x} = \chi_{-s}(x)$$



- $\chi_s(x) = \omega_N^{s \cdot x} = \chi_x(s)$ ((A little weird, but helps compute $DFT_N^\dagger$.))

Key fact: $|\chi_0\rangle, |\chi_1\rangle, \ldots, |\chi_{N-1}\rangle$ are orthonormal (like in Boolean case)

(I'll show you how to build the (inv.) DFT, which has these vectors as its columns, from quantum gates → indirect proof it's unitary, hence χ_S's are orthonormal!)

proof. $\langle \chi_T | \chi_S \rangle = \underset{0 \le X < N}{\text{avg}} \{ \chi_T(X)^* \chi_S(X) \}$

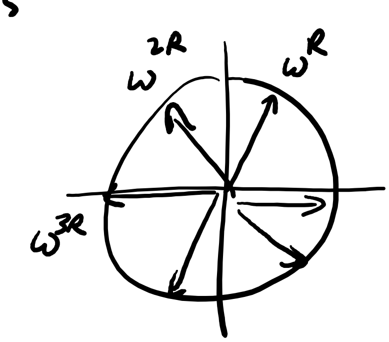
$$\chi_T(X)^* \chi_S(X) = \chi_{-T}(X)\chi_S(X) = \chi_{S-T}(X)$$

if $S=T$, it's $\underset{X}{\text{avg}}\{\chi_0(X)\} = \underset{X}{\text{avg}}\{1\} = 1$ ✓

if $S \ne T$, so $R := S-T \ne 0$, it's

$$\underset{0 \le X < N}{\text{avg}} \{ \omega_N^{R \cdot X} \}$$

$$= 0 \quad ✓$$



(on Hmwk. Sum a geometric series, or think about symmetries.)

$\therefore$
$$\begin{bmatrix} | & & | \\ |\chi_0\rangle & \cdots & |\chi_{N-1}\rangle \\ | & & | \end{bmatrix} \text{ is unitary.}$$

Standard Basis $\longmapsto$ χ-basis

↑ Inverse DFT, actually

e.g. $N=4$:

$DFT_N^{-1} = DFT_N^{\dagger} =$

$$\frac{1}{\sqrt{4}} \begin{array}{c c} & \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{array}{c} 0 \\ 1 \\ 2 \\ 3 \end{array} & \begin{bmatrix} \omega_4^0 & \omega_4^0 & \omega_4^0 & \omega_4^0 \\ \omega_4^0 & \omega_4^1 & \omega_4^2 & \omega_4^3 \\ \omega_4^0 & \omega_4^2 & \omega_4^4 & \omega_4^6 \\ \omega_4^0 & \omega_4^3 & \omega_4^6 & \omega_4^9 \end{bmatrix} \end{array}$$

$\to$ can take expons mod 4, $\because \omega_N^4 = 1$

DFT_N: take conj. transpose:
= put neg. signs in expons

$$\therefore DFT_N |x\rangle = \sum_{s=0}^{N-1} \chi_s(x)^* |s\rangle$$

(cols. of conjug. transpose)

χ-Basis $\xrightarrow[DFT_N]{}$ Standard Basis

$$|g\rangle \longmapsto \sum_s \hat{g}(s)|s\rangle$$

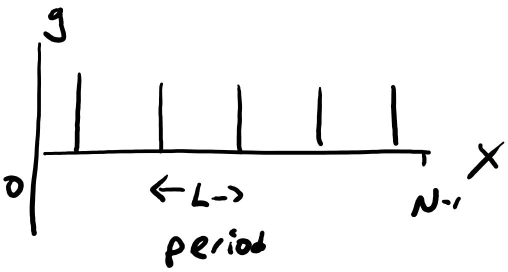
"strength" of $|\chi_s\rangle$ in $|g\rangle$, namely

$$\langle \chi_s | g \rangle$$

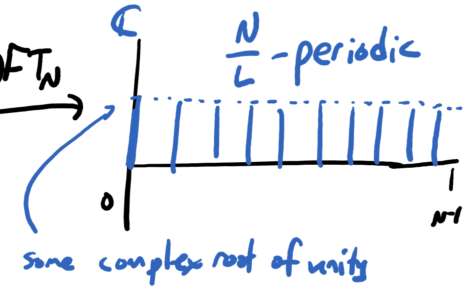
$$= \underset{0 \le x < N}{\text{avg}} \{\chi_s(x)^* g(x)\}$$

$$= \underset{x}{\text{avg}} \{\omega_N^{-s \cdot x} g(x)\}$$

Key fact for next time:



$\xrightarrow{DFT_N}$



Implementing DFT_N, $N=2^n$, with

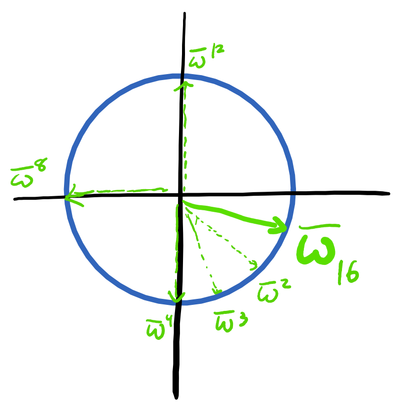
$\frac{n(n+1)}{2} \leq n^2$ quantum gates (1- & 2-qubit gates)

By example ☺ Say $n=4 \Rightarrow N=16$.

To implement: $$|x\rangle \xmapsto{DFT_{16}} \frac{1}{\sqrt{16}} \sum_{s=0}^{15} \chi_s(x)^* |s\rangle$$

$$\overline{\omega}_{16}^{\,s\cdot x} = \omega_{16}^{-s\cdot x}$$

where $\overline{\omega}_{16} = e^{-2\pi i/16}$



So for $0 \leq x < 16$,

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

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

CLAIM

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

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

[[E.g., if 1st qubit is a 1 in (*), should pick up a phase of $\overline{\omega}^{8}$.]]

Result is <u>unentangled</u>!!

Compare Hadamard FT: $H^{\otimes n}|x\rangle = |+\rangle \otimes |-\rangle \otimes \dots$

if $x_1 = 0$ if $x_2 = 1$

[[Challenge, though: each output qubit depends on all n input qubits $x_0 x_1 \dots x_{n-1}$. Seemingly.]]

(Will do the transformation qubit-by-qubit. Very convenient to output qubits in <u>reverse</u> order.)

$x = x_3x_2x_1x_0$

((can do ≈½ SWAPs at end if you like)

To do 0^{th} wire:

Need to get $\left(\frac{|0\rangle + \bar{\omega}^{8x}|1\rangle}{\sqrt{2}} \right)$.

(Seems like depends on all 4 qubits of x? No!)

$\bar{\omega}^8 = \omega_{16}^{-8} = (-1)$. $\therefore$ $\bar{\omega}^{8x} = (-1)^x$, only depends on if x even/odd; i.e., on x_0.

It's $\left(\frac{|0\rangle + (-1)^{x_0}|1\rangle}{\sqrt{2}} \right) = \underline{H|x_0\rangle}$!

To do 1st wire:

Need to get $\left(\dfrac{|0\rangle + \bar{\omega}^{4x}|1\rangle}{\sqrt{2}} \right)$.

(Seems like depends on all 4 qubits of x? No!)

$\bar{\omega}^4 = (-i)$. $\therefore \bar{\omega}^{4x} = (-i)^x =$ only depends on $x \bmod 4$; i.e., on x_0, x_1

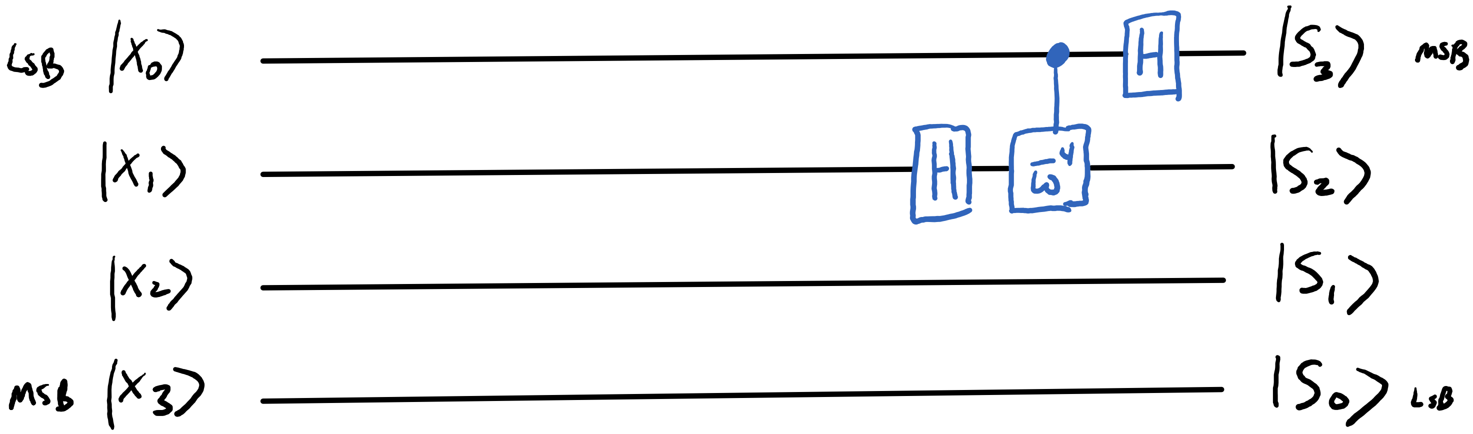
$$\bar{\omega}^{4x} = \bar{\omega}_{16}^{4(x_0 + 2x_1 \cancel{+4x_2} \cancel{+8x_3})} \qquad \because 16x_2, 32x_2 \equiv 0 \bmod 16$$

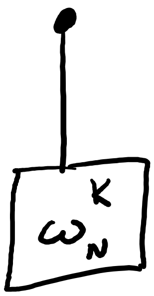
$$= \bar{\omega}^{4x_0} \cdot \bar{\omega}^{8x_1} = (\bar{\omega}^4)^{x_0} (-1)^{x_1}.$$

$|1\rangle$ should pick up phase (-1) if $x_1 = 1$: H!

Should also pick up phase $\bar{\omega}^4$ if $x_0 = 1$:

"controlled - $\bar{\omega}^4$"
x_0





: Some 2-qubit gate

$$\begin{array}{c|cccc} & 00 & 01 & 10 & 11 \\ \hline 00 & & & & \\ 01 & & \multicolumn{2}{c}{\left[\begin{matrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & \omega_N^k \end{matrix}\right]} & \\ 10 & & & & \\ 11 & & & & \end{array}$$

(Rest is similar...)

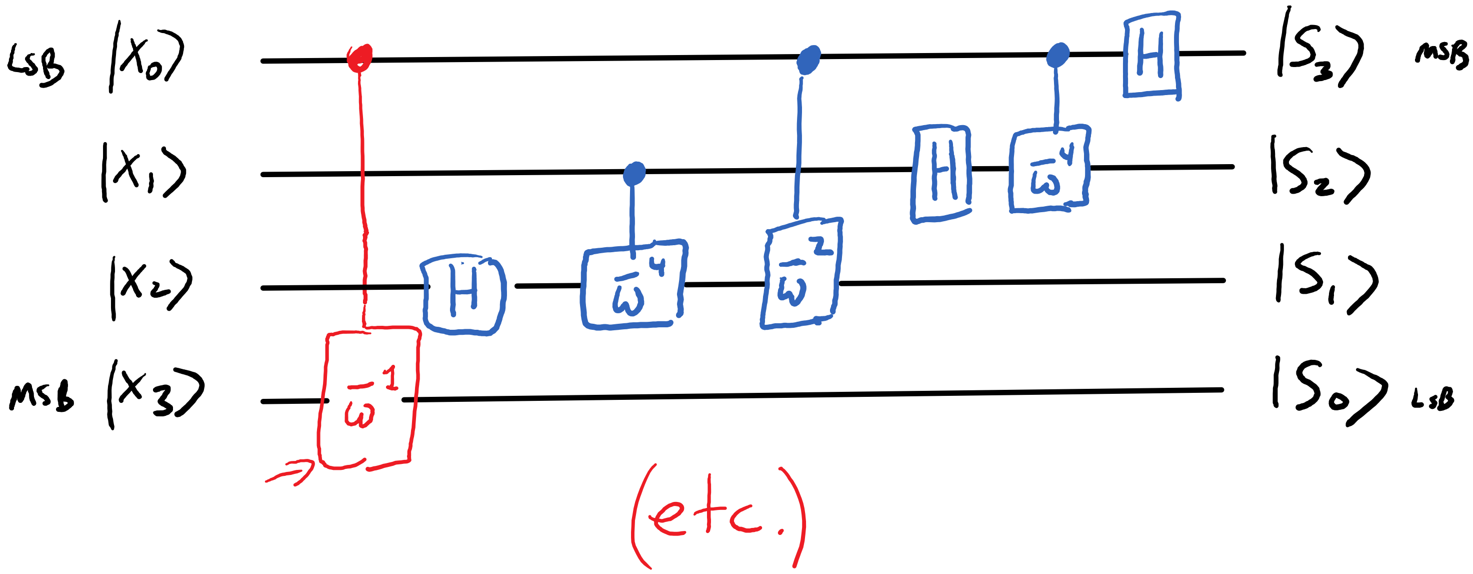
To do 2nd wire:

Need to get $\left(\dfrac{|0\rangle + \bar{\omega}^{2x}|1\rangle}{\sqrt{2}} \right)$.

$$\bar{\omega}^{2x} = \bar{\omega}_{16}^{\,2(x_0 + 2x_1 + 4x_2 + \cancel{8x_3})}$$

$$= \left(\bar{\omega}^2\right)^{x_0} \cdot \left(\bar{\omega}^4\right)^{x_1} \cdot \left(\cancel{\bar{\omega}^8}^{\,(-1)}\right)^{x_2}$$

- $|1\rangle$ picks up phase (-1) if $x_2 = 1$: H!
- " " " " $\bar{\omega}^4$ if $x_1 = 1$: contr'd $\bar{\omega}^4$
- " " " " $\bar{\omega}^2$ " $x_0 = 1$: contr'd $\bar{\omega}^2$.



Total gates: $1+2+3+4+\dots+n$

$$= \frac{n(n+1)}{2} \leq n^2.$$

MSB $|x_3\rangle$ —$\boxed{\bar{\omega}^{1}}$———————— $|s_0\rangle$ LSB

(Final remark: For general n, e.g. $n=1000$, this gate is $\bar{\omega}_{2^n}^{1}$, the controlled-$(2^{-1000})^{th}$ root of unity phase shift. Physically implem'd with a quartz plate 2^{-1000} cm thick, or by firing a laser for 2^{-1000} sec?!? Impossible to accurately build. In general, the controlled gates that control across k wires are using $\bar{\omega}_{2^n}^{2^{n-k-1}} = e^{-2^k \pi i}$. Not realistic for $k \geq 30$, say.

Luckily, it's okay! Fact: suppose you delete all gates where $k \geq \log(n/\varepsilon)$. (e.g. 30) (e.g. $\varepsilon = 1\%$)

Then resulting circuit:

- "ε-approximates" DFT_N $\rightarrow$ success prob. of Shor's alg. only goes down by ε.
- ☺ Remaining gates have plausible phases.
- ☺ Only $O(n \log(n/\varepsilon))$ remaining gates — way more efficient!)