$$= \frac{1}{\sqrt{2^n}} \Big(e^{2\pi i/2^n \, 0 \cdot x} |0\rangle$$
$$+ e^{2\pi i/2^n \, 1 \cdot x} |1\rangle$$
$$+ e^{2\pi i/2^n \, 2 \cdot x} |2\rangle$$
$$\vdots$$
$$+ e^{2\pi i/2^n \, (2^n - 1) x} |2^n - 1\rangle \Big)$$

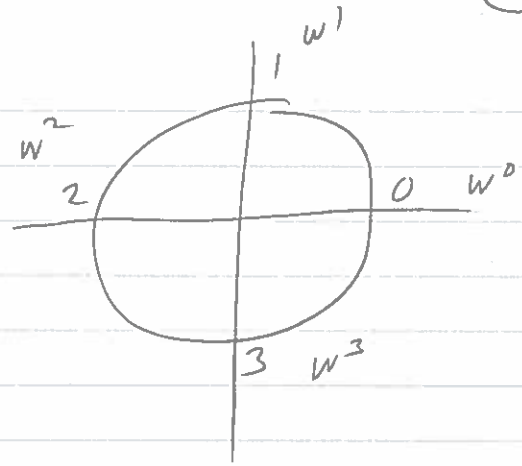
Consider $n = 2$

$$|x\rangle \to \frac{1}{\sqrt{4}} \Big[e^{2\pi i/4 \, 0 \cdot x} |0\rangle$$
$$+ e^{2\pi i/4 \, 1 \cdot x} |1\rangle$$
$$+ e^{2\pi i/4 \, 2 \cdot x} |2\rangle$$
$$+ e^{2\pi i/4 \, 3 \cdot x} |3\rangle \Big]$$

Define $w = e^{2\pi i/4} = i$

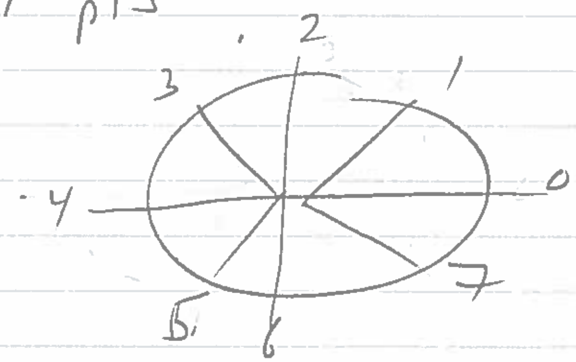
$$|x\rangle \to \frac{1}{\sqrt{4}} \Big[i^{0 \cdot x} |0\rangle + i^{1 \cdot x} |1\rangle$$
$$+ i^{2 \cdot x} |2\rangle + i^{3 \cdot x} |3\rangle \Big]$$

$w = e^{2\pi i/4}$



$n=2$ Samples the unit complex circle in 4 pts

$w = e^{2\pi i/8}$



$n=3$ 8 samples

each is an 8^{th} root of unity

$x^8 = 1$ $\left(e^{2\pi i/8}\right)^{8}$, 1, 2, ...

are all 1

By linearity

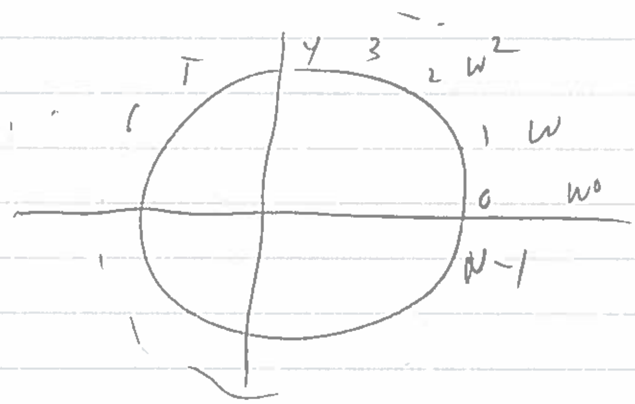
$QFT_1(\alpha_0|0\rangle + \alpha_1|1\rangle) =$

$\alpha_0 \, QFT_1(|0\rangle) + \alpha_1 \, QFT(|1\rangle)$

QFT $\quad n$ qubits $\quad N = 2^n$

ω is primitive N^{th} root of unity

$= e^{2\pi i/N}$



$e^{2\pi i\, K/N} \quad K = 0, 1, \ldots N-1$

is a unique N^{th} root of unity

$$\left(e^{2\pi i\, K/N}\right)^N = e^{2\pi i \frac{KN}{N}}$$

$$= \left(e^{2\pi i}\right)^K$$

$$= 1^K$$

These are discrete samples of the unit complex circle

Larger N gives more samples

143.1

$w = e^{2\pi i/N}$ [edX]

$$QFT_N = \frac{1}{\sqrt{N}} \begin{pmatrix} w^0 & w^0 & w^0 & w^0 & \cdots & w^0 \\ w^0 & w^1 & w^2 & w^3 & \cdots & w^{N-1} \\ w^0 & w^2 & w^4 & w^6 & \cdots & w^{2(N-1)} \\ w^0 & w^3 & w^6 & w^9 & \cdots & w^{3(N-1)} \\ \vdots & & & & & \\ w^0 & w^{N-1} & w^{2(N-1)} & w^{3(N-1)} & \cdots & w^{(N-1)(N-1)} \end{pmatrix}$$

Row j Col k entry $= w^{jk}$

QFT_4 $\quad w = e^{2\pi i/4} = i$

$$QFT_4 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

Lets look at QFT_4 applied to

$$|f\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \qquad |g\rangle = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |h\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$QFT_4(|f\rangle) = \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\begin{bmatrix} \quad & \quad \end{bmatrix} \begin{bmatrix} \\ \\ \\ \end{bmatrix}$$

How close, similar, are these vectors

$|f\rangle$ very similar to top row, Not at all to the others

Measure of $QFT_4(|f\rangle)$ is $|0\rangle$

QFT$_4$($|g\rangle$) selects column 0

$$= \frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

QFT$_4$($|h\rangle$) selects col 1

$$= \frac{1}{2} \begin{pmatrix} 1 \\ i \\ -1 \\ -i \end{pmatrix}$$

How are these related

$e^{i\pi/2}$ phase shift each

Notes

1) Columns of QFT$_4$ are orthogonal, No similarity
2) Columns have magnitude 1

so QFT$_4$ is unitary - can be quantum computed

3) Inputs with lots of 0s (large spread) have QFT with narrow spread & vice versa

$|g\rangle$ and $|h\rangle$ differ by a phase shift

but measurements of their QFT are differ by relative phase shift

143.4

Does ~~that~~ matter on measurement?

$$\frac{1}{2}\begin{pmatrix}1\\1\\1\\1\end{pmatrix} \qquad \begin{matrix}1/4 & |0\rangle\\1/4 & |1\rangle\\1/4 & |2\rangle\\1/4 & |3\rangle\end{matrix} \qquad \frac{1}{2}\begin{pmatrix}1\\i\\-1\\-i\end{pmatrix}$$

S
A
M
E

Fourier sampling - compute & measure is the same!

QFT_N is unitary
Prove columns are orthonormal

$$F_i = \begin{pmatrix}1\\w^{i\cdot 1}\\w^{i\cdot 2}\\\vdots\\w^{i\cdot(N-1)}\end{pmatrix} \qquad F_j = \begin{pmatrix}1\\w^{j\cdot 1}\\w^{j\cdot 2}\\\vdots\\w^{j\cdot(N-1)}\end{pmatrix}$$

$$\langle F_i | F_j \rangle = 1/N \sum_{k=0}^{N-1} \overline{w^{ik}} \cdot w^{jk}$$

$$= 1/N \sum_{k=0}^{N-1} w^{-ik} \cdot w^{jk}$$

$$= 1/N \sum_{k=0}^{N-1} w^{(j-i)k}$$

If same column $i=j$

$$\langle F_i|F_j\rangle = 1/N \sum_{K=0}^{N-1} w^{0K} = 1$$

If not, $i \neq j$, treat inner product as a geometric series

$$1/N \sum_{K=0}^{N-1} \omega^{(j-i)K} = 1/N \frac{w^{N(j-i)}-1}{w^{j-i}-1}$$

$$\boxed{\sum_{K=0}^{N-1} r^K = \frac{r^N-1}{r-1}}$$

$w^N = 1$ so $(w^N)^{(j-i)} = 1$

so series produces 0

$\square$

LINEAR SHIFT

The linear shift of a state vector causes (only) a relative phase shift of its DFT

Ex $|f(x)\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix}$

143.6

$$|f(x+1)\rangle = \begin{pmatrix}\alpha_1\\ \alpha_2\\ \alpha_3\\ \alpha_0\end{pmatrix}$$

$$QFT_4\left(|f(x)\rangle\right) = \begin{pmatrix}\beta_0\\ \beta_1\\ \beta_2\\ \beta_3\end{pmatrix}$$

$$QFT_4\left(|f(x+1)\rangle\right) = \begin{pmatrix}\beta_0\\ -i\beta_1\\ -\beta_2\\ i\beta_3\end{pmatrix}$$

We saw this specifically for

$|f(x)\rangle = \begin{pmatrix}1\\1\\1\\1\end{pmatrix}$ previously

It can be shown

if $|\hat{f}(x)\rangle$ is the QFT_N of $|f(x)\rangle$

then the QFT_N of $|f(x+d)\rangle$

$= |\hat{f}(x)\rangle$ with each component having phase multiplier $e^{2\pi/N \times d}$

Since $w = e^{2\pi i/N}$

entry x is phase shifted by $w^{x \cdot d}$

$$QFT_4 \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \end{pmatrix}$$

$d = 1$

$$\text{then } QFT \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_0 \end{pmatrix} = \begin{pmatrix} w^0 & \beta_0 \\ w & \beta_1 \\ w^2 & \beta_2 \\ w^3 & \beta_3 \end{pmatrix}$$

Identical under measurement because $|w^x| = 1$ always

$$\begin{pmatrix} & QFT_N & \end{pmatrix}\begin{pmatrix}\alpha_0\\ \vdots \\ \alpha_{N-1}\end{pmatrix} = \begin{pmatrix}\beta_0\\ \vdots\\ \beta_{N-1}\end{pmatrix}$$

can be basis state or NOT

$\sum_{j=0}^{N-1} \alpha_j |j\rangle$ $\qquad$ $\sum_{j=0}^{N-1} \beta_j |j\rangle$

How hard is QFT_N It's phase estimation backwards

Complexity can be $O(n^2)$ $\quad$ n qubits
close to $O(n)$ if work hard

$n = \log N$ so $O(n^2) = O(\log^2 N)$

By comparison FFT $O(N^2)$ time
better $O(N \log N)$ time

QFT exponentially better!

<u>Catch</u> you don't get $\beta_0 \ldots \beta_{x-1}$ separately

You get a superposition

When you measure, you see $|j\rangle$ with probability $|\beta_j|^2$

Nature computes $\beta_0 \ldots \beta_{x-1}$ but won't share it with you!

Periodic States

$$|\phi_{r,b}\rangle = \frac{1}{\sqrt{m}} \sum_{z=0}^{m-1} |zr+b\rangle$$

reps

period shift

Example $r=5$ $b=2$ $m=3$

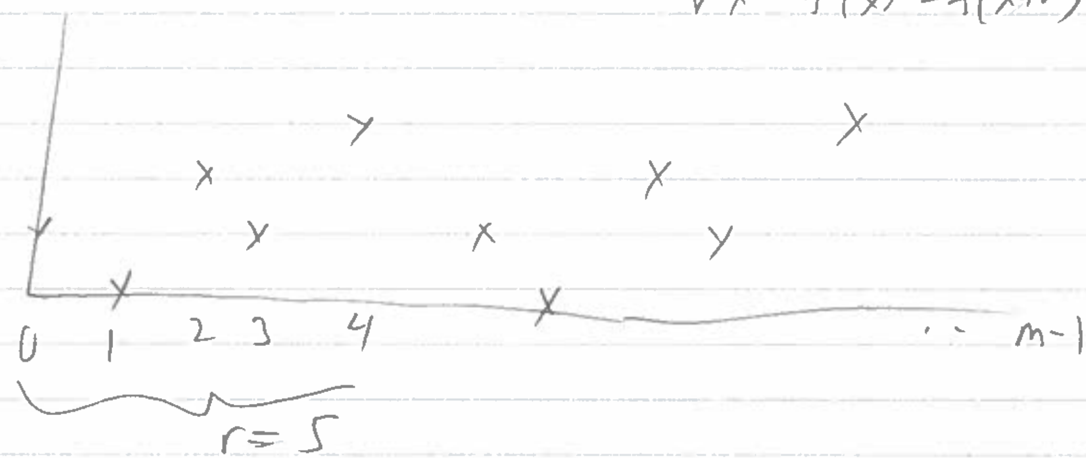
$$|\phi_{5,2}\rangle = \frac{1}{\sqrt{3}}\left(|2\rangle + |7\rangle + |12\rangle\right)$$

Given $m \cdot r$ (15)
Random b in $[0, r)$

Find r

Quantum Factoring Shor's Alg [Vazirani]

Main idea: find the period of a function
$\forall x \quad f(x) = f(x+r)$

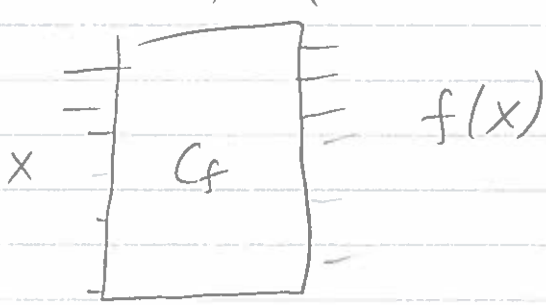


$m = 100$, $m/r = 20$ repeats of pattern

Note - within a period f is 1:1
Assume r divides m (for now)
$m/r \gg r \quad m \gg r^2$

$\forall x \quad f(x) \neq f(x+r)$

classical



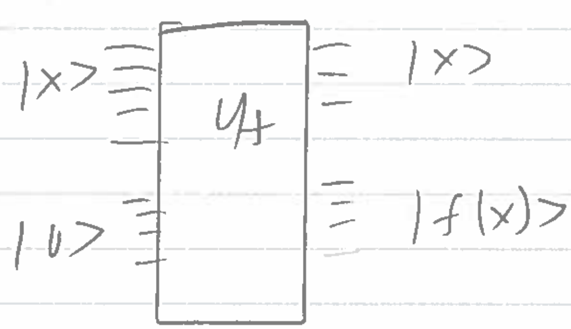
Need to see many repeats of the period

Now, suppose m is really large, say 1000 dig number
so r is 500 dig number

Find r?

Classically try finding $f(x)=f(y)$
Certainly $r+1$ tries yields one duplicate
Randomly, $\sqrt{r}$ inputs suffice to see collision → birthday paradox w/ high prob. (I think 1/2),
Still, 250 dig number – too big!

Quantum Alg



Usual trick set up uniform superposition of all inputs

Output is then the superposition

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

$$\begin{pmatrix} & & \\ & QFT & \\ & & \end{pmatrix} \times \begin{matrix} \alpha & 0 \\ 0 & 0 \\ 0 & \alpha \\ 0 & 0 \\ 0 & 0 \\ \alpha & 0 \\ 0 & 0 \\ 0 & \alpha \\ 0 & 0 \\ 0 & 0 \\ \alpha & 0 \\ 0 & 0 \\ 0 & \alpha \\ 0 & 0 \\ 0 & 0 \\ \alpha & 0 \end{matrix} \qquad \alpha > 0$$

shift up
later show
doesn't matter

We get as the output
the sum of colums 0, 5, 10, 15

Now measure bottom qubits
to see <u>some</u> $f(a)$, say $f(a) = 4$

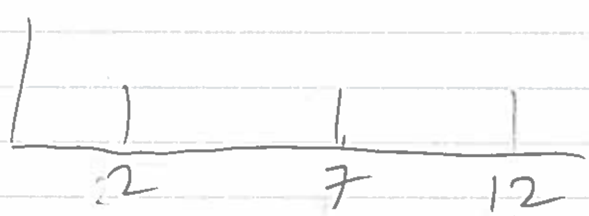
Many x's have $f(x) = 4$
but they are all 5 apart

After measuring bottom, top is

$$\frac{1}{\sqrt{?}} \sum_{x=0}^{m-1} \alpha_x |x\rangle \qquad \alpha_x = 0,\ f(x) \neq 4 \qquad \alpha_x > 0,\ f(x) = 4$$

In our example

2   7   12 ...



I wish I could sample 2 of these
but I can only sample <u>1</u>

And if I run the circuit so far
again, I probably won't get $a \mid f(a) = 4$

I would like to see the distances
between the above pos ampl. BASES
In every run of the circuit they are 5 apart

From what we saw before,
a QF sample of

2 7 12 ...

is the same as

0 5 10

<u>linear</u> shift doesn't matter

Turns out

If f is periodic with period r over $M = 2^n$ samples

then $\hat{f}$ (QFT(f)) is periodic with period M/r

We had $r = 5$ $m = 100$
so $\hat{f}$ is periodic w/ period 20

So

$$f = \sqrt{r/m} \sum_{j=0}^{m/r - 1} |jr\rangle$$

$$= \sum_{x=0}^{m-1} \begin{cases} \sqrt{r/m}\,|x\rangle & \text{if } x = 0 \bmod r \\ 0\,|x\rangle & \text{otherwise} \end{cases}$$