

(141)

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

Consider $n=2$

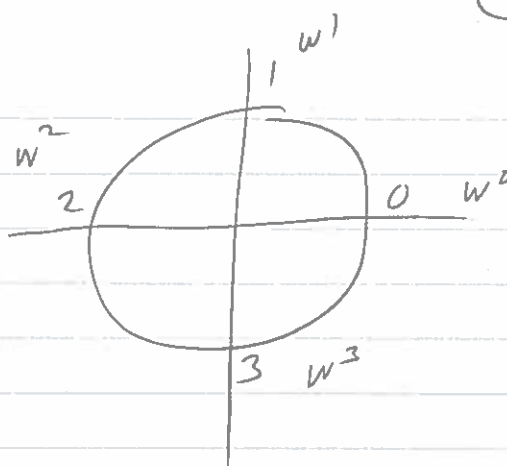
$$|x\rangle \rightarrow \frac{1}{\sqrt{4}} \left[e^{2\pi i / 4 \cdot 0 \cdot x} |0\rangle + e^{2\pi i / 4 \cdot 1 \cdot x} |1\rangle + e^{2\pi i / 4 \cdot 2 \cdot x} |2\rangle + e^{2\pi i / 4 \cdot 3 \cdot x} |3\rangle \right]$$

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

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

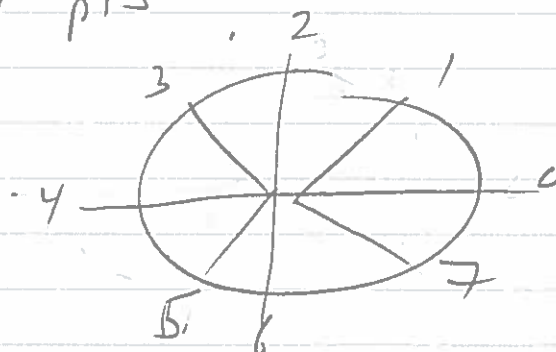
(142)

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



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

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



$n=3$ 8 samples

each is an 8th root of unity

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

are all 1

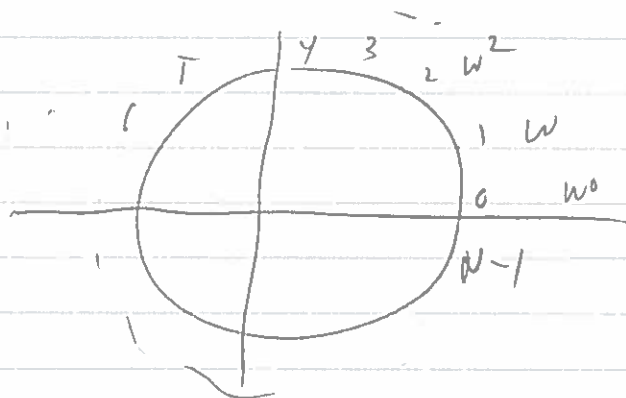
By linearity

$$\text{QFT}_1(\alpha_0 | 10 \rangle + \alpha_1 | 11 \rangle) =$$

$$\alpha_0 \text{QFT}_1(| 10 \rangle) + \alpha_1 \text{QFT}_1(| 11 \rangle)$$

GFT n qubits $N = 2^n$

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



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

is a unique N^{th}
 root of unity

$$\begin{aligned} \left(e^{2\pi i K / N} \right)^N &= e^{2\pi i \frac{KN}{N}} \\ &= \left(e^{2\pi i} \right)^K \\ &= 1^K \end{aligned}$$

These are discrete samples of the
 unit complex circle
 Larger N gives more samples

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

(143.1)

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

Row j Col k entry = w^{jk}

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

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

Lets look at QFT_4 applied to

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

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

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

$$\begin{bmatrix} \end{bmatrix} \begin{bmatrix} \end{bmatrix}$$

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
related
 $i\pi/2$
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?

$$\frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \quad \begin{matrix} 1/4 & |0\rangle \\ 1/4 & |1\rangle \\ 1/4 & |2\rangle \\ 1/4 & |3\rangle \end{matrix} \quad \frac{1}{2} \begin{pmatrix} 1 \\ i \\ -1 \\ -i \end{pmatrix} \quad \begin{matrix} S \\ A \\ M \\ E \end{matrix}$$

Fourier sampling - compute & measure
is the same!

QFT_N is unitary
Prime columns are orthonormal

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

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

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

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

(143.5)

If same column $i=j$

$$\langle F_i | F_j \rangle = \frac{1}{N} \sum_{k=0}^{N-1} \omega^{0k} = 1$$

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

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

$$\begin{aligned} \sum_{k=0}^{N-1} r^k \\ = \frac{r^N - 1}{r - 1} \end{aligned}$$

$$\omega^N = 1 \quad \text{so} \quad (\omega^N)^{(j-i)} = 1$$

so series produces 0

□

LINEAR SHIFT

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

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

(143.5)

If same column $i=j$

$$\langle F_i | F_j \rangle = \frac{1}{N} \sum_{k=0}^{N-1} \omega^{0k} = 1$$

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

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

$$\begin{aligned} & \sum_{k=0}^{N-1} r^k \\ &= \frac{r^N - 1}{r - 1} \end{aligned}$$

$$\omega^N = 1 \text{ so } (\omega^N)^{(j-i)} = 1$$

so series produces 0

□

LINEAR SHIFT

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

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

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

$$\text{QFT}_4(|f(x)\rangle) = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \end{pmatrix}$$

$$\text{QFT}_4(|f(x+1)\rangle) = \begin{pmatrix} \beta_0 \\ -i\beta_1 \\ -\beta_2 \\ i\beta_3 \end{pmatrix}$$

We saw this specifically for

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

It can be shown

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

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

143.7

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

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

$$\text{QFT}_4 \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \end{pmatrix}$$

$\downarrow d=1$

$$\text{Then } \text{QFT} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_0 \end{pmatrix} = \begin{pmatrix} w^1 \beta_0 \\ w^2 \beta_1 \\ w^3 \beta_2 \\ \beta_3 \end{pmatrix}$$

Identical under measurement
because

$$|w^k| = 1 \text{ always}$$

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

can be basis
state or NOT



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

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

How hard is QFT_N It's phase estimation backwards

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

$$n = \log N \quad \text{so} \quad O(n^2) = O(\log^2 N)$$

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

QFT exponentially better!

Catch you don't get $\beta_1 \dots \beta_{n-1}$ separately

you get a superposition

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

Nature computes $\beta_1 \dots \beta_{n-1}$ but won't share it with you!

Periodic states

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

\downarrow mps
 $m-1$
 \uparrow period \uparrow shift

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

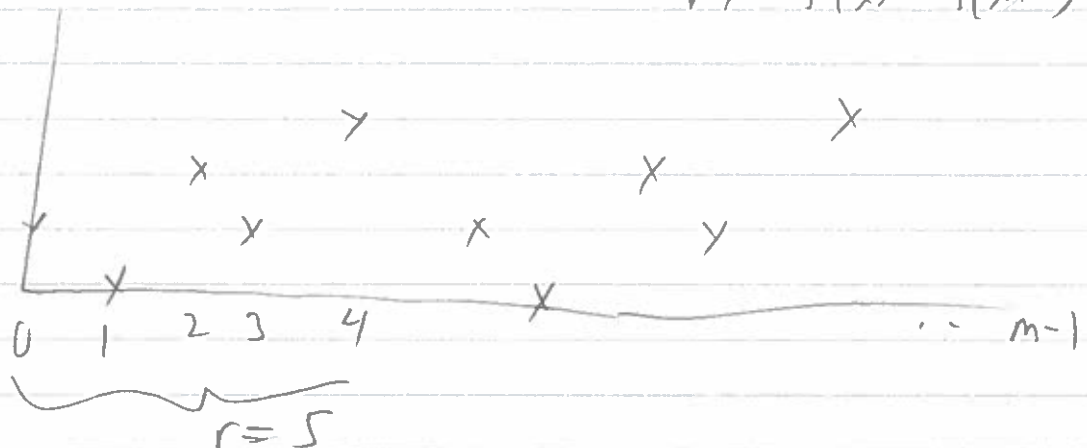
$$|\phi_{5,2}\rangle = \frac{1}{\sqrt{3}} (|2\rangle + |7\rangle + |12\rangle)$$

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

Find r

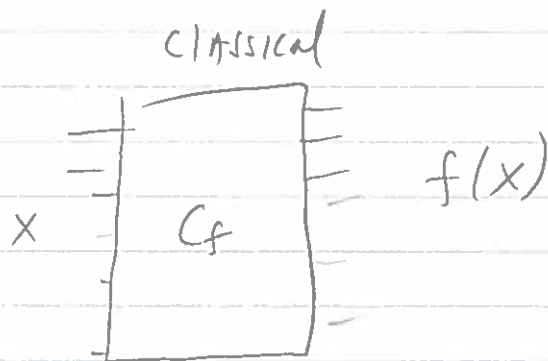
Quantum Factoring Shor's Alg [Vazirani]

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



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

Note - within a period f is 1:1
Assume r divides m (^{for now})
 $\frac{m}{r} \gg r$ $m \gg r^2$
 $\forall x \ f(x) = f(x+r)$



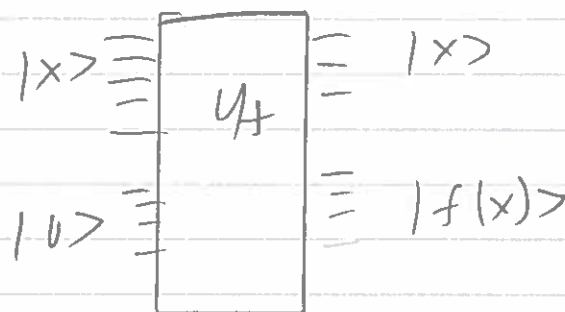
Need to see
many repeats
of the period

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. (\pm think $1/2$)
 Still, 256 dis number - too big!

Quantum Alg



Usual trick set up uniform superposition
 of all inputs

Output is then the superposition

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

(QFT)

x

2	0
0	0
0	2
0	0
0	0
2	0
0	0
0	2
0	0
0	0
2	0
0	0
0	2
0	0
0	1
2	0

$2 > 0$

shift up
later show
doesn't matter

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

(148)

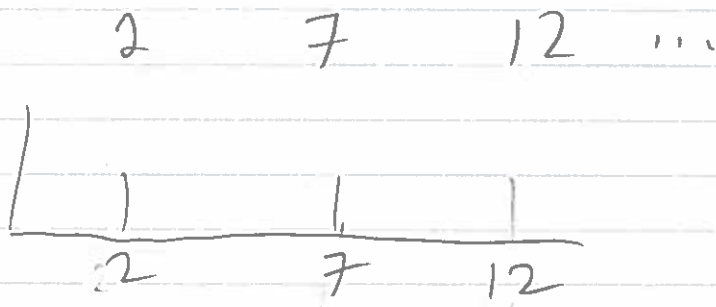
Now measure bottom qubits
to see some $f(x)$, say $f(a) = 4$

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

After measuring bottom, top is

$$\frac{1}{\sqrt{2}} \sum_{x=0}^{m-1} \alpha_x |x\rangle \quad \begin{array}{l} \alpha_x = 0, f(x) \neq 4 \\ \alpha_x > 0, f(x) = 4 \end{array}$$

In an example



I wish I could sample 2 of these
but I can only sample 1

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

I would like to see the distances
between the above pos. amplitudes.
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

linear 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

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