$\beta^{\rightarrow}$ is imaginary conjugate it flips only i sign

$3 + 3i = 3 - 3i$

Inverse of U is U^+ unitary matrix

Qubit

$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ how much in 0 state / how much in 1 state

normally use dirac notation

$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ i \end{pmatrix} = \boxed{\alpha |0\rangle + \beta |1\rangle}$

Bloch sphere 3d sphere, $|0\rangle$ & $|1\rangle$ z axis

x axis = + − y axis = ± i

Logic gates flip around the x, y, or z gate

$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ inverse matrix = gate

Ex) $Y|\psi\rangle = Y\left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right)$

(applying Y gate) $= \frac{\sqrt{3}}{2} Y|0\rangle + \frac{1}{2} Y|1\rangle)$

$= \frac{\sqrt{3}}{2} Y \begin{pmatrix} 0 \\ i \end{pmatrix} + \frac{1}{2} Y \begin{pmatrix} -i \\ 0 \end{pmatrix}$

$= \sqrt{3}/2\, Y\, i \begin{pmatrix} 0 \\ i \end{pmatrix} - \frac{1}{2} Y\, i \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

X = NOT

Y = NOT + phase twist

Phase (bloch sphere) rotating around z axis

- doesnt change prob of α or β

on equator is $\pm i, +, -$ state

important for hadamard gate

Hadamard Gate $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

0 state goes to + visa versa

1 state goes to −

$H|0\rangle = +$ $H|1\rangle = -$

S & T Phase Gates (adds phase of e^{i-})

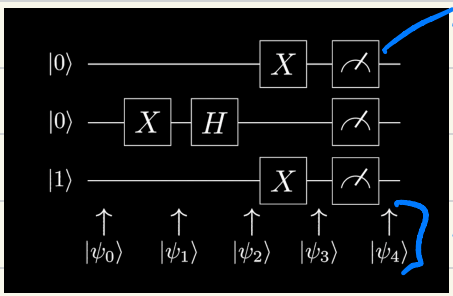
$S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix}$ $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

$S^\dagger$ & $T^\dagger$ are inverse of S & T

Tensor prod $|0\rangle \otimes |0\rangle = |00\rangle$

↳ combine multiple quantum systems into 1

Quantum Circuit



measuring qubit

diff pts during algo

$\psi_0 = 001$

$\psi_1 = 011$

$\psi_2 = 0 - 1 = \frac{1}{\sqrt{2}}(001 - 011)$

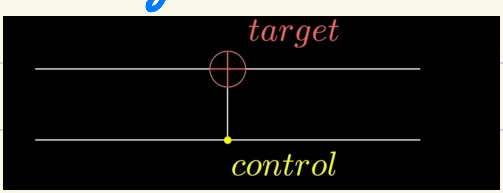
$\psi_3 = \frac{1}{\sqrt{2}}(100 - 110)$

ψ_4 = measure

$|100\rangle$ 50%

$|110\rangle$ 50%

CNOT gate (toffol: similar)



if control is a 1 then x gate put on target

else nothing

Measuring Single Qubit prob

$|\psi\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$

Prob of first Qubit as 0 = $\frac{1}{2}^2 + \frac{1}{2}^2 = 1/2$

Entanglement ⭐

$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ Bell state where there are 2 qubits, they can either both be 0 or 1

Once we measure a 0, we know $|\psi_2\rangle = |00\rangle$

bc there is no 01 or 10 in system

& visa versa w/ 1

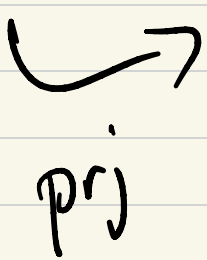
(By measuring one, yk the other) = Entanglement

↳ if can't be factored into individual qubits then is entangled

Ex above is max entangled

$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{4}|01\rangle + \frac{1}{4}|10\rangle + \frac{1}{\sqrt{2}}|11\rangle$

measuring first qubit 1 vs 0 will change what $|\psi\rangle$ collapses to (partial entangle)

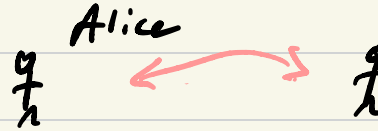


Send quantum info using classical bits

Entanglement demo

How quantum tele actually works

Theory:



Already have a max entangled qubit (ebit)

Joint state of all qubits

$$= \frac{1}{\sqrt{2}}\left(\alpha_0\left(|0\rangle_B|0\rangle_A + |1\rangle_B|1\rangle_A\right)|0\rangle_Q + \alpha_1(\ldots)|1\rangle_Q\right.$$

(just expanding on the max entangled bell state)

$$|\Phi^+\rangle_{BA} = \frac{1}{\sqrt{2}}\left(|0_B 0_A\rangle + |1_B 1_A\rangle\right)$$

Ebit ★

apply Cnot on Alice

$= CNOT(Q, A)$

CNOT Gate (control, target)

INPUT		OUTPUT (Q, A)	
Control	Target	Control	Target
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

$$= \frac{1}{\sqrt{2}}\left(\text{didnt change bc input} + \alpha_1\left(|0\rangle_B|1\rangle_A + |1\rangle_B|0\rangle_A\right)|1\rangle_Q\right.$$

only right side changes bc $Q=1$

$|\rangle_B$ doesnt change bc CNOT applied to only A

Apply H gate →

Hadamard Gate

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Apply H

left side → to get right

$$= \frac{1}{2}\Big[(\alpha_0|0\rangle_B + \alpha_1|1\rangle_B)|0\rangle_A|0\rangle_Q + (\alpha_0|0\rangle_B - \alpha_1|1\rangle_B)|0\rangle_A|1\rangle_Q$$
$$+ (\alpha_1|0\rangle_B + \alpha_0|1\rangle_B)|1\rangle_A|0\rangle_Q + (-\alpha_1|0\rangle_B + \alpha_0|1\rangle_B)|1\rangle_A|1\rangle_Q\Big]$$

4 diff states

for ex, if Alice 0 & 0 then bob $|\alpha_0|0\rangle_B$

same for others

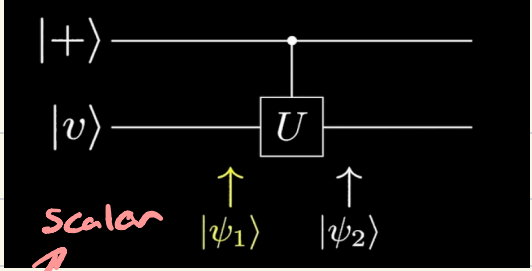
Alice calls bob

Based on Alice outcome she conveys instructions to bob on what to do w/his qubit

Bob may need to do X, Z, X&Z gate

Final] Alice destroys quantum info w her and have it appear with bob bc entanglement

Phase kickback —



$|v\rangle$ is eigenvector of U so $U|v\rangle = e^{i\theta}|v\rangle$

scalar

refresh lin alg - eigenvalue multiplied w/ eigenvector to stretch or flip but direction is same.

For quantum same thing but instead of stretch its phase (rotation around z-axis)

back to kickback - looking at circuit

$|\psi_1\rangle = |+\rangle|v\rangle$ $(|+\rangle = |0\rangle + |1\rangle/\sqrt{2})$

plug in $\approx |v_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle|v\rangle + |1\rangle|v\rangle)$

$|\psi_2\rangle = CU|\psi_1\rangle = \frac{1}{\sqrt{2}}(CU|0\rangle|v\rangle + CU|1\rangle|v\rangle)$

$= \frac{1}{\sqrt{2}}(|0\rangle|v\rangle + e^{i\theta}|1\rangle|v\rangle)$ sub in

only qubit 1 affected bc that's when CU on

$= \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle)|v\rangle$

Being kickedback- eigenphase that U applies to its eigenvector

V can be ignored bc it gets factored out anyway (makes kick back possible). Kickback is bc V is unchanged, U's affect goes to control qubit's phase

Phase kickback (used in phase estimation) basically where applying control-target system like CNOT (conceptually) but instead of target being affected its the control that changes

---

Phase kickback Qiskit math

`qc.x(target_v)` start w/ 0 & apply X to get 1

1 is important bc we later say $U = Z$

$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ so $Z|1\rangle = |-1\rangle = e^{i\pi}|1\rangle$

$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ so $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix} = -1\begin{pmatrix} 0 \\ 1 \end{pmatrix} = -|1\rangle$

(1 is eigenstate of Z w/ eigenval of -1)

`qc.cz(control_plus, target_v)` Phase Kick part

if control = 0 do nun, else apply Z to target

Superdense coding - Sending 2 bits of info with 1 qubit (w/ entanglement)

Max entangled ex Alice & Bob

A needs to alter $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

If she wants to send 00 to Bob

↳ Do nothing

Send 01 X gate needed

Send 10 Z gate

Send 11 X, Z gates

Bell State

↓ Bob applies CNOT (1st qubit control) then hadamard to get what alice wanted to send

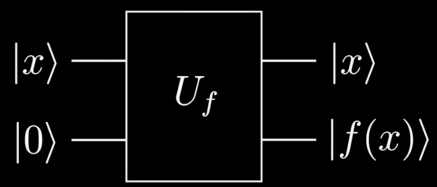
Send classical info using quantum entanglement (mirror of tele)

Alice is encoding the msg

Function on QC – must be reversable

Standard Quantum Function/Oracle

Set $y = |0\rangle$:

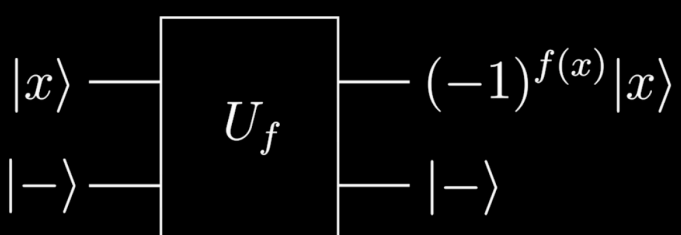


$$U_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle$$

Backbone of all algo

Phase Oracle

$$U_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$$



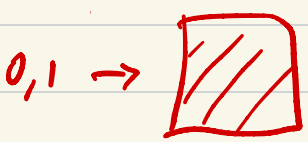
allows for quantum speed up

Deutsch Algo

- Constant fn returns the same bit always
  ex) $f(0) = f(1)$

x	fx
0	1
1	1

- Balanced return 0 for half of inputs
  ex) NOT or identity t-table



black box ex
we dont know
what goes on inside

Classical
we would need 2 queres to tell
if constant or balanced

quantum
only 1 query

↳ if $f(0) = f(1)$
$= |\psi_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
$= |+\rangle$

then $H|+\rangle$ & $H|-\rangle$
$= |0\rangle$ $= |1\rangle$

if $f(0) \neq f(1)$
$= |\psi_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
$= |-\rangle$

if machine
return 1 then
yk $f(0) \neq f(1)$ ex

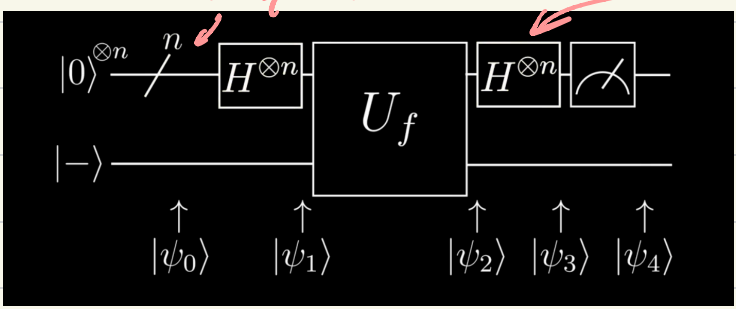
Deutsch Jozsa algo

$f: \{0,1\}^n \to \{0,1\}$

same but for any num of n inputs

Classical needs $2^{n-1}+1$ queries worst case

Quantum only need 1 query again



Flow

$\psi_0 = 0^{\otimes n} |-\rangle$

$\psi_1 = H^{\otimes n} |0^{\otimes n}\rangle$ so many $|+\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$

ψ_2 = distribute $U_f \approx \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} U_f |x\rangle |-\rangle$

$U_f |x\rangle |-\rangle$ is phase oracle form so $= (-1)^{f_x} |x\rangle |-\rangle$

$= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle$

ψ_3 = apply $H^{\otimes n}$ on x like how we did ε for $H|0$, $H|x$ is $\frac{1}{\sqrt{2^n}} \sum_{z \in \{0,1\}^n} (-1)^{x \cdot z} |z\rangle$

If f is Constant:	If f is Balanced:
Amplitude of $\|00\ldots0\rangle = \pm 1$	Amplitude of $\|00\ldots0\rangle = 0$
$\implies$ Prob of measuring $\|00\ldots0\rangle = 1$	$\implies$ Prob of measuring $\|00\ldots0\rangle = 0$

If we measure the $|00\ldots0\rangle$ state then f is constant. If we measure any other state then f is balanced

Bernstein Vazarani algo

given n bits & outputting single bit
↳ the fn, $f(x) = x \cdot s \pmod 2$

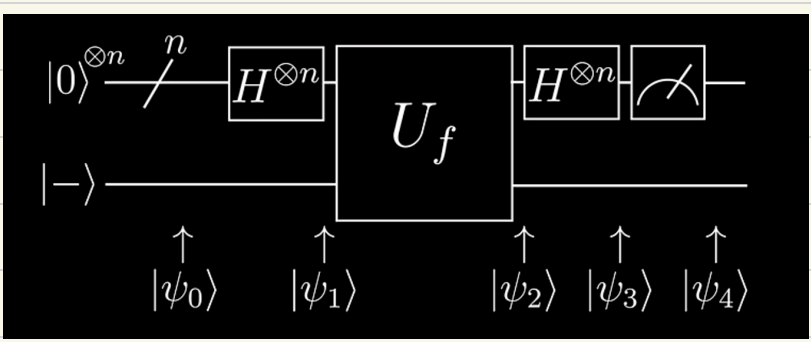
s is secret str to find

Classical O(n): s = 101

$f(x_1, x_2, x_3) = (1 \cdot x_1 + 0 \cdot x_2 + 1 \cdot x_3)$

so each query ex f(100) will give 1 bit of s so need n times

Quantum approach O(1)



Same circuit as D-J algo

BV algo pt 2

Same steps $\psi_0 - \psi_2$ from DJ algo

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle|-\rangle$$ sub $f(x)$ for $x \cdot s$

$$|\psi_3\rangle = H^{\otimes n} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{s \cdot x} |x\rangle$$

$$= \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot s} \left[\sum_{x \in \{0,1\}^n} (-1)^{x \cdot z} |z\rangle \right]$$

distribute $-1^{x \cdot s}$ into next part to get

$$|\psi_3\rangle = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} \sum_{z \in \{0,1\}^n} (-1)^{(s+z) \cdot x} |z\rangle$$

$(s+z) \cdot x \approx s_i \oplus z_i$ XOR

$|\psi_4\rangle$ = amplitute of $|s\rangle$ state when $|z\rangle = |s\rangle$

$$= \frac{1}{2^n} \sum_{x \in (0,1)^n} (-1)^{(s+s) \cdot x}$$

$s+s = s$ XOR $s = 0$

bc $0 \oplus 0 = 0$ & $1 \oplus 1 = 0$

$$= \frac{1}{2^n} \sum_{x \in (0,1)^n} 1 \qquad \sum_{x \in \{0,1\}^n} 1 = 2^n$$

$$= \frac{1}{2^n} 2^n$$

$= 1$ Prob of measuring s after applying algo is 1

So only 1 query

Quantum Fourier Transform

Binary into QFT $|101\rangle$ (5) for ex

1 block for each digit in 101, so 3
↳ each block is qubit

Work backward w/ first being $\frac{n}{8} \cdot 2\pi$

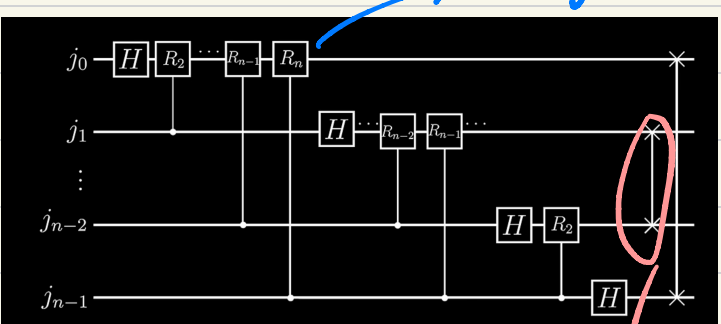
So $5/8 \cdot 2\pi = 10\pi/8 = 5\pi/4$ radian

Second ×2 ~ $5\pi/4 \cdot 2 = \pi/2$ radian

Third ×2 ~ $\pi/2 \cdot 2 = \pi$ radian

$QFT|101\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi}|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi/2}|1\rangle \ldots)$

QFT circuit → R_k gate = $\begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$

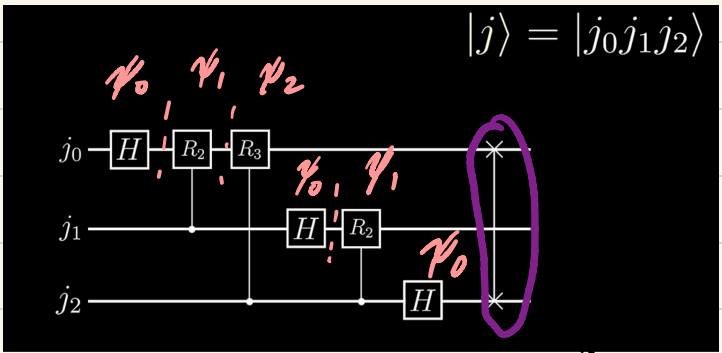


Only apply if control is 1

Swap gate to swap states of 2 qubits bc ans prints backward

QFT is a phase reader bascially, used in QPE an Shors but not sum like BV

QFT pt 2, 3 bit example



individual flow first

$-1^{j_0} = e^{2\pi i\left(\frac{j_0}{2}\right)}$

j_0 $\gamma_0 = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{j_0}|1\rangle\right)$

$\gamma_1 = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i(j_0/2)}\, e^{\left(\frac{2\pi i}{2^3}\right) j_1}|1\rangle\right)$

$= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(j_0/2 + j_1/4\right)}|1\rangle\right)$

only apply R to 1 state

γ_2 = same j mult $e^{\left(\frac{2\pi i}{2^3}\right) j_2}$ to $|1\rangle$

final j_0

$$R_3 R_2 H|j_0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{j_0}{2} + \frac{j_1}{4} + \frac{j_2}{8}\right)}|1\rangle\right)$$

j_1 & j_2 same thing w/ $HR_2|j_1\rangle$ & $H|j_2\rangle$

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{j_0}{2} + \frac{j_1}{4} + \frac{j_2}{8}\right)}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{j_1}{2} + \frac{j_2}{4}\right)}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{j_2}{2}\right)}|1\rangle\right)$$

(j_0, j_1, j_2)

$$QFT|j\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{j_2}{2}\right)}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{j_1}{2} + \frac{j_2}{4}\right)}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\left(\frac{j_0}{2} + \frac{j_1}{4} + \frac{j_2}{8}\right)}|1\rangle\right)$$

after swap

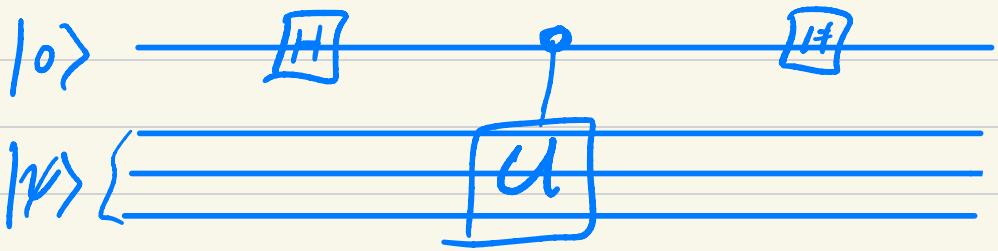
Encoded the value of j into the phase of the qubits. Like the bloch sphere ex in the prev page. So if you try 101 again you will get j2=1, j1=0, j0 = 1

→ use Inverse QFT to get 101

Formula

$$QFT|j\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n - 1} e^{\frac{2\pi i j k}{2^n}}|k\rangle$$

QPE (1 qubit QPE ex)



kickback recap - Eigenstate is $|\psi\rangle$ (target)

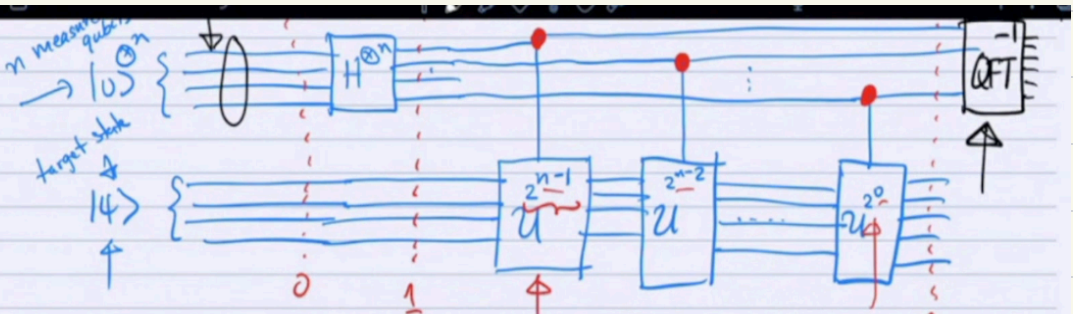
Eigenvalue is $e^{i\theta}$ (phase)

- Control qubit starts in $|0\rangle$, Hadamard → superposition ✅
- U acts on $|\psi\rangle$ (target) ✅
- $|\psi\rangle$ **must be an eigenstate of** U ✅
- Eigenvalue is a phase: $U|\psi\rangle = e^{i\theta}|\psi\rangle$ ✅
- Phase **kicks back** onto the control, **state doesn't change** ✅
- Second Hadamard turns phase into a measurable probability ✅

multi state ex QPE is finding digits (binary) of phase θ

each U gate is finding one digit to kick back

increases precision



QPE pt2

After all U gates, phase is encoded to unscramble, use IQFT to turn phase into bits. Then just measure & done.

Shor's - factoring num $N = p \cdot q$

(p & q are large prime)

Classically - huge exponential $O(n)$

Quantum $O(n^3)$

Steps) $N = pq$

no common divisors

1] pick num a that's coprime w/ N

2] find order (period) r of fn $a^r \pmod N$

$=$ smallest r s.t. $a^r \equiv 1 \pmod N$

3] if r is even good (prob $\frac{1}{2}$ by factor)

$x \equiv a^{r/2} \pmod N$

if $x+1 \not\equiv 0 \pmod N$

$\{p, q\}$ (atleast one) is contained in $\gcd(x+1, N)$ $\gcd(x-1, N)$

Shor's algorithm uses quantum phase estimation to find the period of modular exponentiation, which classically reveals the prime factors of a large

$f(x) = a^x \bmod N$, repeats every r steps

The repeats are visualized into frequencies which is the phase

Shors put simply - Solves the real problem related to encryption(done by multiplying two large primes) which is hard to do classically. Shor's uses phase via period finding to help factor large composite numbers efficiently.

"Repetition in the function causes phases to add up; the QFT converts that phase alignment into a measurable frequency, which reveals the

Code flow - pick random num -> construct periodic modular exponentation fn -> superposition -> measure to isolate period -> apply QFT to extract period -> use classical to get factors

building fn whose outputs repeat where repetition depends on the hidden factors of N

($a^x \bmod N$ is fn)

Grovers

Given large unlabeled search space, finding the wanted item in O(sqrt(n)) instead of brute force classical O(n).

Assuming you have a checker that will output - for 1 or no change for 0 (oracle)

Flow -

Putting everything into superposition w H gate to make vector equally probable. Black box oracle which marks correct ans w/negative sign (flipping the phase). By repeatedly reflecting on the state that was negatively marked then the amplitude gets closer and closer to the correct ans. (3 blue 1 black video ex). So when we collapse its super likely to be the correct ans.

Bonus - Grover is a structural geo procedure meaning it works inside a Hilbert Space

Algorithm description

Grover's algorithm

1. *Initialize:* set n qubits to the state $H^{\otimes n}|0^n\rangle$.
2. *Iterate:* apply the Grover operation t times (for t to be specified later).
3. *Measure:* a standard basis measurement yields a candidate solution.

The Grover operation is defined like this:

$$G = H^{\otimes n} Z_{OR} H^{\otimes n} Z_f$$

Z_f is the phase query gate for f and Z_{OR} is the phase query gate for the n-bit OR function.