Week 3:
Quantum Search

→ Classical: $O(n)$ Grover: $\frac{\pi}{4}\sqrt{n}$

$= O(\sqrt{n})$

* Grover's algorithm:

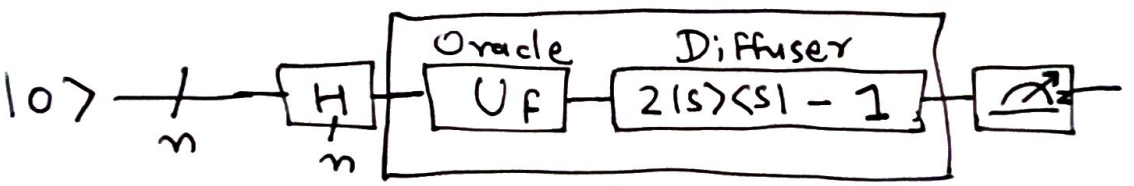
(1) create an equal superposition of all $|0\rangle$ qubits to $|s\rangle$ by applying H gate to every qubit: $\frac{\Sigma_x |x\rangle}{\sqrt{N}}$; $|x\rangle = |x_1, x_2, \ldots x_n\rangle$; $N = 2^n$

(equal likelyhood of each poss sol^n stat)

(N: Search space)

(2) The next step involves running the oracle circuit (U_{oracle}) on these qubits.

(3) Run a diffuser or diffusion operator (U_s)



Repeat $\frac{\pi}{4}\sqrt{N}$ times: Grover iterations

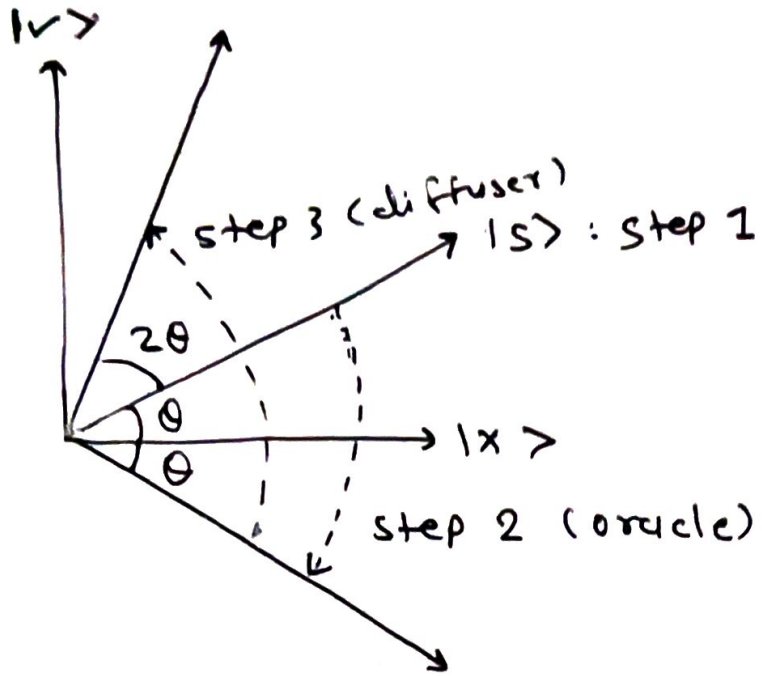
→ $|v\rangle = \frac{1}{\sqrt{n}}$ (|state 1⟩ + ⋯ |state n⟩) : q-qubits

$|x\rangle = \frac{1}{\sqrt{q-n}}$ (|state 1'⟩ + ⋯ |state (q−n)'⟩) : q-qubits

eg: $|v\rangle = \frac{1}{\sqrt{3}}(|000\rangle + |011\rangle + |101\rangle)$

$|x\rangle = \frac{1}{\sqrt{5}}(\ldots)$ | x > = [1/sqrt(5)] (rest of the states)

[1]



$a|x\rangle + b|v\rangle$

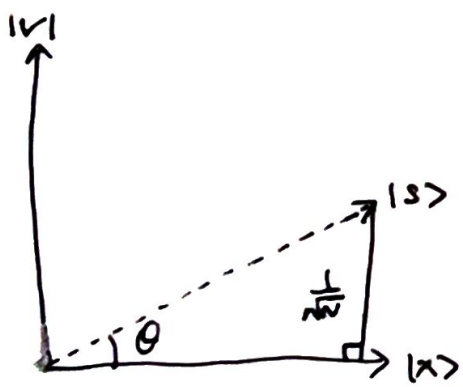
↓ oracle

$a|x\rangle - b|v\rangle$

↑ phase inversion of solution states

→ initially $|s\rangle$ is closer to $|x\rangle$. If most states are not the solutions, as we repeat steps 2 and 3, the $|s\rangle$ gets transformed to states closer and closer to $|v\rangle$.

[2]



$\sin\theta = \frac{1}{\sqrt{N}}$

$\therefore$ small angle approx

$\theta \approx \frac{1}{\sqrt{N}}$

→ Each subsequent diffuser rotn of 2θ ref [1]

$2\theta = \frac{2}{\sqrt{N}} \Longrightarrow$ no. of iterations needed $= \boxed{\frac{\pi}{2} \div \frac{2}{\sqrt{N}}}$

Imaginary

* $|\psi\rangle = \sqrt{1-p}\,|0\rangle + \underbrace{e^{i\phi}}\sqrt{p}\,|1\rangle$

global phase (undetectable) (imaginary)

arbitrary phase shift

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle)$$

* Let's say we have a search function $F(x)$ such as:

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

ancilla qubit (or) check qubit

$f(x)$: 0 if not a soln; 1 if a soln

More generally,

$$U_f |x\rangle|z\rangle = |x\rangle|z \oplus f(x)\rangle$$

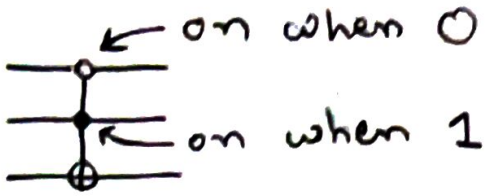
$\oplus$ is add mod 2

→ Sometimes a quantum circuit that computes $f(x)$ may give intermediate states as well:

eg. $|x\rangle|0\rangle|0\rangle \longrightarrow |x\rangle|s(x)\rangle|w(x)\rangle$

$|s(x)\rangle$: desired; $|w(x)\rangle$: not desired; garb: garbage

we want $|x\rangle|0\rangle \longrightarrow |x\rangle|s(x)\rangle$ only.



A more complicated controlled gate

- After $\frac{\pi}{4}\sqrt{N}$ iterations :

The prob. of measuring the correct O/P:

$$1 - \frac{1}{N}$$

This means for large N, prob. increases!

→ It is a good practise to verify the solution observed through the oracle and rerun the algorithm if a non-solution is observed.

→ If some values x are known to not be part of $|v\rangle$, $|x\rangle$ can be removed from the initial superpos^n $|s\rangle$ to reduce the search space.

→ Increase in the $|v\rangle$ state amplitudes can be though of, in terms of constructive and distructive interference: 'Quantum Parallelism' - related with uncomputation.