Grover's Search Algorithm

Abhay Saxena

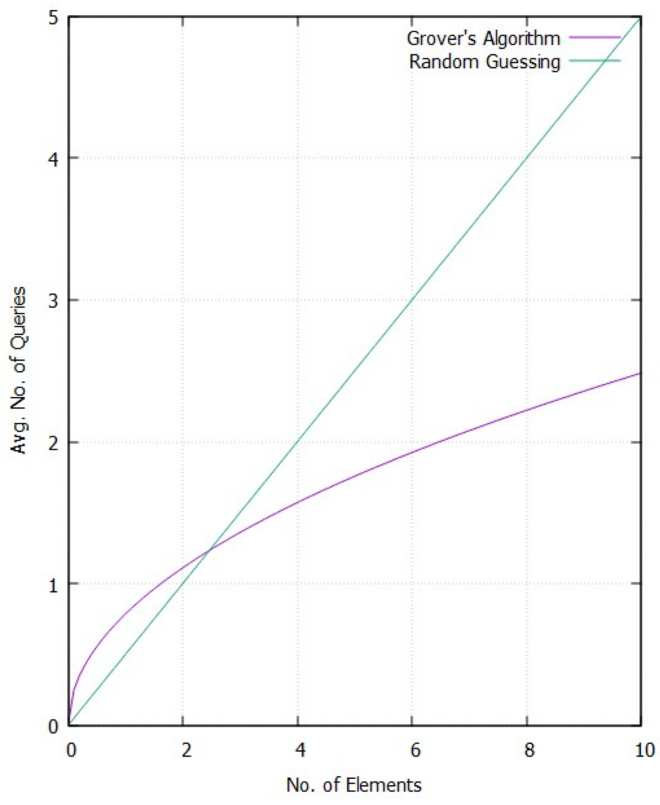
Problem

- Phone directory containing N names arranged in completely random order (unstructured data).
- Aim is to find a particular person’s phone no.
- Best way to do it classically is to simply go though every single n^{th} entry until we reach the name being searched (average number of database queries grows linearly)
- However it could be done in less no. of steps using quantum computers

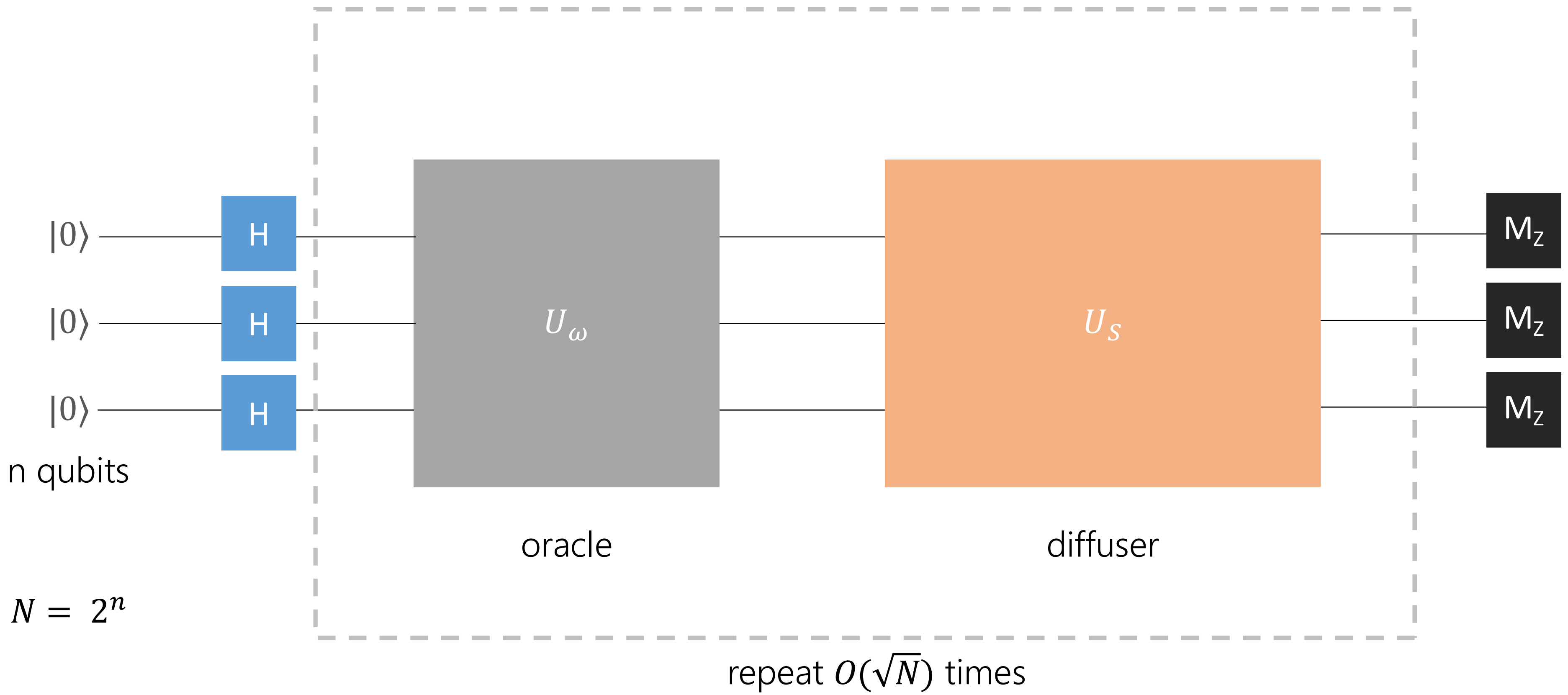
Name	No.
Sharad	12345678
Gowtham	87654321
Sagnik	12348765
Ananya	56784321
Pranav	56781234

Searching for a Needle in a Haystack

- Quantum mechanics can speed up a range of search applications over unsorted data.
- by having the input and output in superpositions of states, we can find an object in $O(\sqrt{N})$ (approx π√N/4) quantum mechanical steps instead of $O(N)$ (approx N/2) classical steps.



Basic structure



Overview

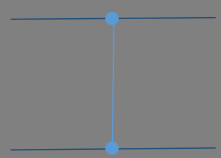
Ultimately we are trying to input all possible states in a superposition to this quantum circuit and trying to maximize the probability of getting output as out desired selected element(s).

- First we create an equal superposition of every possible input to the oracle. We can create this superposition by applying a H-gate to each qubit. We'll call this equal superposition state $|s\rangle$
- Then we run U_ω on this superpostition state. Oracle holds the table of elements and is used for querying data.
- Finally we apply diffuser operator which works along with oracle to magnify the amplitude of desired results

Oracle

- In order to simplify the database to a set of rules in bits for input and output we define certain blackboxes which input a possible
- it basically rotates the current state around perpendicular to $|\omega\rangle$.
- we can even use Toffoli gate to implement our desired oracle from classic oracles making its reversible version.

```
#just a simple oracle for ω = |11>
oracle = QuantumCircuit(2)
oracle.cz(0,1)  # not for |00>,|10>,|01>
oracle.draw()
```



$$U_\omega = I - 2|\omega\rangle\langle\omega|$$

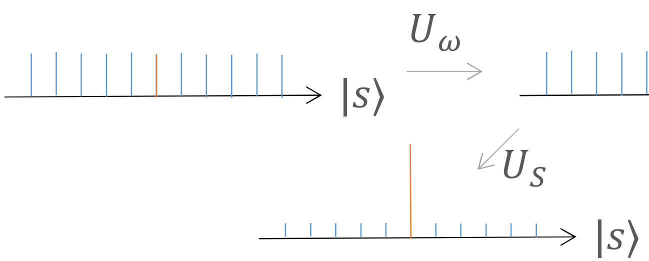
$$\text{let } N = 2^n \text{ such that there are } n \text{ qubits}$$

$$|\omega\rangle = \frac{1}{\sqrt{no.\ of\ items\ in\ k}}\sum_{x\in k}|x\rangle$$

$$\text{where } k \text{ is set of desired outcomes}$$

Diffuser

- In order to increase the magnitude of all the states with phase change due to oracle (i.e desired elements), we use diffuser which amplifies their probability and reduce the probability of others
- It basically rotates current state around the perpendicular to $|s\rangle$



$$U_S = 2|s\rangle\langle s| - I$$

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

$$U_s \sum_i a_i|i\rangle = \sum_i (2\langle a\rangle - a_i)|i\rangle$$

for arbitrary state

$$\langle\omega|s\rangle = \frac{\sqrt{k}}{\sqrt{N}}$$

$$R_g = U_S U_\omega$$

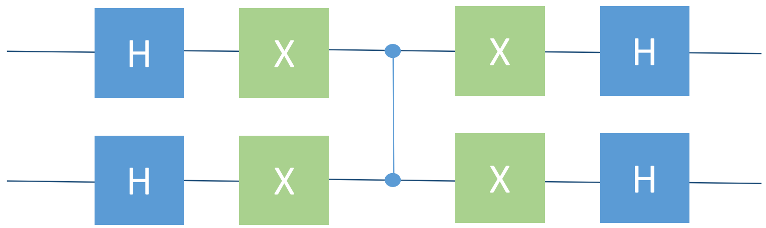
where R_g is Grover's Operator to be repeated $O(\sqrt{N})$ times

2 qubit diffuser

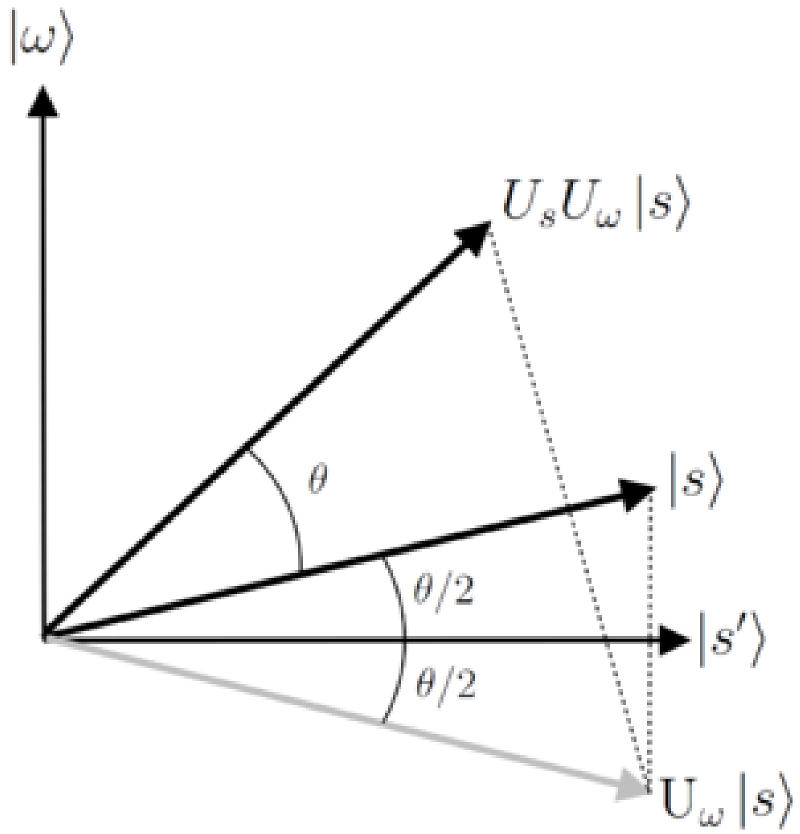
$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- to imitate the effect of reflection around the state $|s\rangle$, we simply create a transformation map $|s\rangle \rightarrow |11\rangle$ as we know an operator which reflects araound $|11\rangle$.
- so in short, we create $|s\rangle$ from $|00\rangle$ by h gates
- then do the transformation $|s\rangle \rightarrow |11\rangle$.
- reflect around $|11\rangle$ using cz.
- do the transformation $|11\rangle \rightarrow |s\rangle$.
- undo the H gate by applying it again.

```
diffuser.cz(0,1)
diffuser.x([0,1])
diffuser.h([0,1])
diffuser.draw()
grover = grover.compose(oracle)
grover = grover.compose(diffuser)
grover.measure_all()
```



Geometric interpretation



Calculation no. of iterations

- $Angle\ btw.\ |s\rangle\ and\ |\omega\rangle = \frac{\pi}{2} - \frac{\theta}{2}$
- if we want to reach $|\omega\rangle$ in m iterations, we need $m \times\ \theta\ = \frac{\pi}{2} - \frac{\theta}{2}$
- $m = \frac{\pi}{2\theta} - \frac{1}{2}$
- $as\ |s\rangle = \frac{1}{\sqrt{N}}(\ |0\rangle\ +\ \ |1\rangle + \ldots +\ |\omega\rangle + \ldots |N-1\rangle)$ for the case that *even if there is just one solution state in* $|\omega\rangle$ *we can say,*
- $sin(\frac{\theta}{2}) = \frac{1}{\sqrt{N}}\ so,\ \frac{\theta}{2} \approx \frac{1}{\sqrt{N}}$ rad$(\approx \frac{\sqrt{k}}{\sqrt{N}}\ for\ k\ elements\ in\ |\omega\rangle)$
- *Hence, no. of iterations* $m \approx \frac{\pi}{4}\sqrt{N}$
- *interestingly no quantum Turig machine can do it in less than O(√N) iterations*