Introduction to Quantum Information and Computing - Lecture 6

Shrikara A, Arnav Negi, Kriti Gupta, Manav Shah, Mohammed Shamil, Shiven Sinha, Swayam Agarwal, Vineeth Bhat, Yash Adivarekar

21st February, 2023

1 Quantum Search - Grover's Algorithm

Quantum search algorithms provide quadratic speedup compared to classical algorithms. That is if it takes classical algorithms $O(N)$ steps to run, it would take a quantum algorithm $O(\sqrt{N}$ steps to run with a high probability of success.

1.1 Problem Statement

Let us have a set X of $N = 2^n$ elements

$$X = \{x_1, x_2, ..., x_N\}$$

and a Boolean function $f : X \to \{0, 1\}$. x_i are bitstrings of length n.
Find elements $x* \in X$ such that $f(x*) = 1$.

The classical algorithm to solve this would always need $O(N)$ queries to the function f.

It's complexity is $O(N) = O(2^n)$ both in the average case and the worst case classically. However the quantum approach allows us to speed this up quadratically. This is achieved as shown below.

1.2 The Quantum Approach

We have seen in previous lectures the following observation:

$$H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{N}} \sum_{z \in 0,1^n} |z\rangle$$

Hence the Hadamard gate when applied to $|0\rangle^{\otimes n}$ converts it to an equal superposition of all states in the computational basis. Now from now on let $|S\rangle = \frac{1}{\sqrt{N}} \sum_{z \in 0,1^n} |z\rangle$.

We now introduce a phase kickback oracle:

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

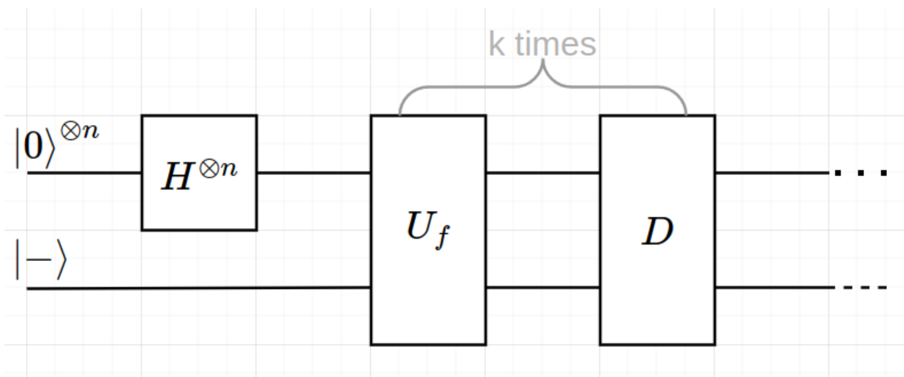
This gate will flip the phase of $|x\rangle$ for all $x*$, else it will keep the state unchanged. Applying this to our state $|S\rangle$:

$$U_f |S\rangle = \frac{1}{\sqrt{N}}(\sum_{x \notin x*} |x\rangle - \sum |x*\rangle)$$

So only phase of $|x*\rangle$ is flipped.

1.3 The algorithm

The grover's algorithm is then defined as follows:



$$G = (DU_f)^k |S\rangle$$

for a suitable k. D is a gate that is called the diffuser. We now rewrite $|S\rangle$ as follows:

$$|S\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle$$

$$= \frac{1}{\sqrt{N}}(\sum_{x' : f(x')=1} |x'\rangle + \sum_{x'' : f(x'')=1} |x'\rangle)$$

Now let, $|\{x : f(x) = 1\}| = M$. Define the following:

$$|\omega\rangle = \frac{1}{\sqrt{M}} \sum_{x' : f(x')=1} |x'\rangle$$

$$|S\omega\rangle = \frac{1}{\sqrt{N-M}} \sum_{x'' : f(x'')=0} |x''\rangle$$

Then,

$$|S\rangle = \frac{\sqrt{M}}{\sqrt{N}}|\omega\rangle + \frac{\sqrt{N-M}}{\sqrt{N}}|S\omega\rangle$$

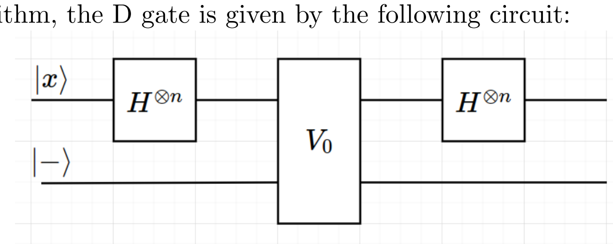
Now we see that, $\langle S\omega|\omega\rangle = 0$, so the basis $\{|\omega\rangle, |S\omega\rangle\}$ forms an orthonormal set.

Let $sin(\theta/2) = \sqrt{\frac{M}{N}}$ and $cos(\theta/2) = \sqrt{\frac{N-M}{N}}$.
So,

$$|S\rangle = sin(\theta/2)|\omega\rangle + cos(\theta/2)|S\omega\rangle$$
$$U_f|S\rangle = -sin(\theta/2)|\omega\rangle + cos(\theta/2)|S\omega\rangle$$

1.4 D Gate

In the algorithm, the D gate is given by the following circuit:



The V_0 gate performs a controlled phase shift. If $|x\rangle = |0\rangle^{\otimes n}$ then no phase shift happens, else the phase is flipped.

This gives:

$$V_0 = 2|0\rangle^{\otimes n}\langle 0|^{\otimes n} - \mathbb{I}$$

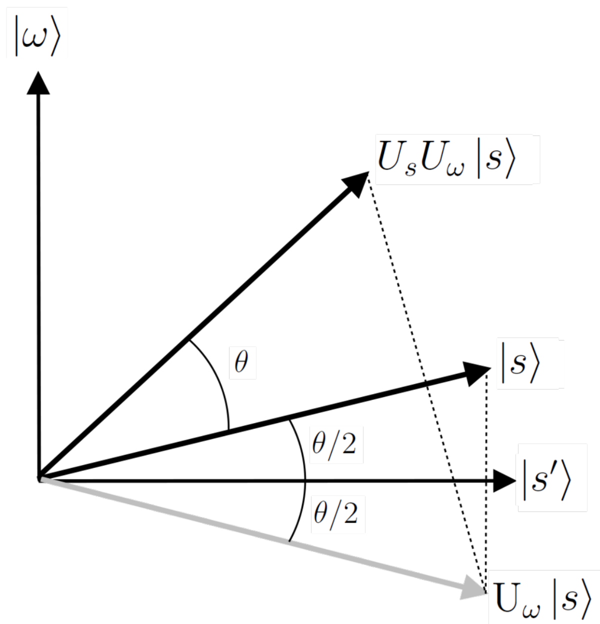
we can also write,

$$V_0 : |x\rangle \to (-1)^{OR(x_1,x_2,\ldots)}|x\rangle$$

since if at least one bit is non 0, there is a phase kickback. So,

$$\begin{gathered} D = H^{\otimes n}V_0H^{\otimes n} \\ = 2H^{\otimes n}|0\rangle^{\otimes n}\langle 0|^{\otimes n}H^{\otimes n} - H^{\otimes n}\mathbb{I}H^{\otimes n} \\ = 2|S\rangle\langle S| - (H^2)^{\otimes n} \\ = 2|S\rangle\langle S| - \mathbb{I} \end{gathered}$$

1.5 Working of the algorithm



In the above diagram of the algorith, the U_f gate flips the state along the axis for $|S\omega\rangle$ and the D gate flips it across the state $|S\rangle$. The combined effect is a rotation by angle of θ counter clockwise on the diagram. Hence the state's overlap with the solution state ω increases.

However then for the algorithm to work we must have $M << N$. This would mean θ is considerably smaller than $\pi/2$. Then to get maximum overlap, we take k as follows:

$$\theta/2 + k\theta \approx \pi/2$$