Grover's Algorithm

Instrumentation And Applied Physics
Indian Institute Of Science

Name:	Akshay Ranchhod Patil
Student Number:	19353
Research Centre:	Advanced Quantum Technology Lab
Research Project Title:	Grover's Algorithm
Instructor:	Dr.Balaaditya Suri

1 Abstract

Finding an object/string of interest from a large pile of unstructured objects is what we know as a search.Using a quantum Algorithm for this search is what we call a 'Quantum Search'.Classically to find a string or an object of interest from large pile of objects it takes on an average N/2 queries to oracle whereas Grover's Algorithm does it in O$\sqrt{N}$ queries to the oracle.Grover Algorithm uses the principle of Quantum Mechanics mainly 'Entanglement' and 'Superposition' and exploits the fact that probability of measurement is square of the amplitude which is the main factor responsible for quadratic speedup compared to classical available algorithms.

In this report I will give a detailed theoretical explanation of Grover's Algorithm and its implementation for 3 Qubits on IBM Quantum Simulator as well as IBM Quantum Computer using a database oracle which will again use 3 Qubits to encode the given classical data,followed by a brief discussion on the results observed.

2 Introduction to Grover Algorithm

Grover's Algorithm is a Quantum Algorithm used for 'searching an unsorted database' with $N = 2^n$ elements in O$\sqrt{N}$ time.

Grover's Problem $\rightarrow$ We are given a set of N objects x=[1,2,...,N].By using encoding of database we can map these objects into $[0,1]^n$ strings.We are also given Quantum Circuit or Oracle U_f that implements function f which maps these N strings which are each n bits into [0,1] i.e. $N = 2^n$. We have to find x (winning state) for which f(x)=1. There are two cases to Grover's Problem - 1.Single Object Finding 2.Multiple Objects Finding. Second Case will be briefly discussed at the end of the introduction.For now lets focus on case of f(x)=1 for exactly one string i.e first case.

For any Quantum Algorithm end states are always classical.Lets start with a classical state $|\Psi_1\rangle$=$|00...0\rangle$=$|0\rangle^{\otimes n}$ Now to convert this classical state tensor product in to a uniform superposition of states we apply Quantum Fourier Transform also known as Hadamard Transform.This first step of converting the input classical strings into a superposition of strings is called 'initialization'.

1.First Step of Algorithm-
Initialization: $H^{\otimes n}|\Psi_1\rangle = H^{\otimes n}|0\rangle^{\otimes n}$=

$$\frac{1}{\sqrt{N}}\begin{bmatrix}1 & 1 & \cdots & 1\\ 1 & 1 & \cdots & 1\\ \vdots & \vdots & \ddots & \vdots\\ 1 & 1 & \cdots & 1\end{bmatrix}_{N\times N}\begin{bmatrix}1\\0\\\vdots\\0\end{bmatrix}_{N\times 1} = \frac{1}{\sqrt{N}}\begin{bmatrix}1\\1\\\vdots\\1\end{bmatrix}_{N\times 1} = \frac{1}{\sqrt{N}}\sum_{x=1}^{N}|x\rangle = |s\rangle$$

2.Second Step of Algorithm
After the step of initialization comes the step of phase inversion in which phase inversion of winning state is carried out by using the phase oracle U_f.Phase inversion is a process of introducing a global phase factor of -1 to the winning state $|w\rangle$ (lets say).

A Phase oracle operator U_f flips the sign of the winning state and keeps the remaining states orthogonal to $|w\rangle$ as it is.

Basic Function of Phase Operator :U_f: $|x\rangle\otimes|y\rangle \rightarrow |x\rangle\otimes|y \oplus f(x)\rangle$

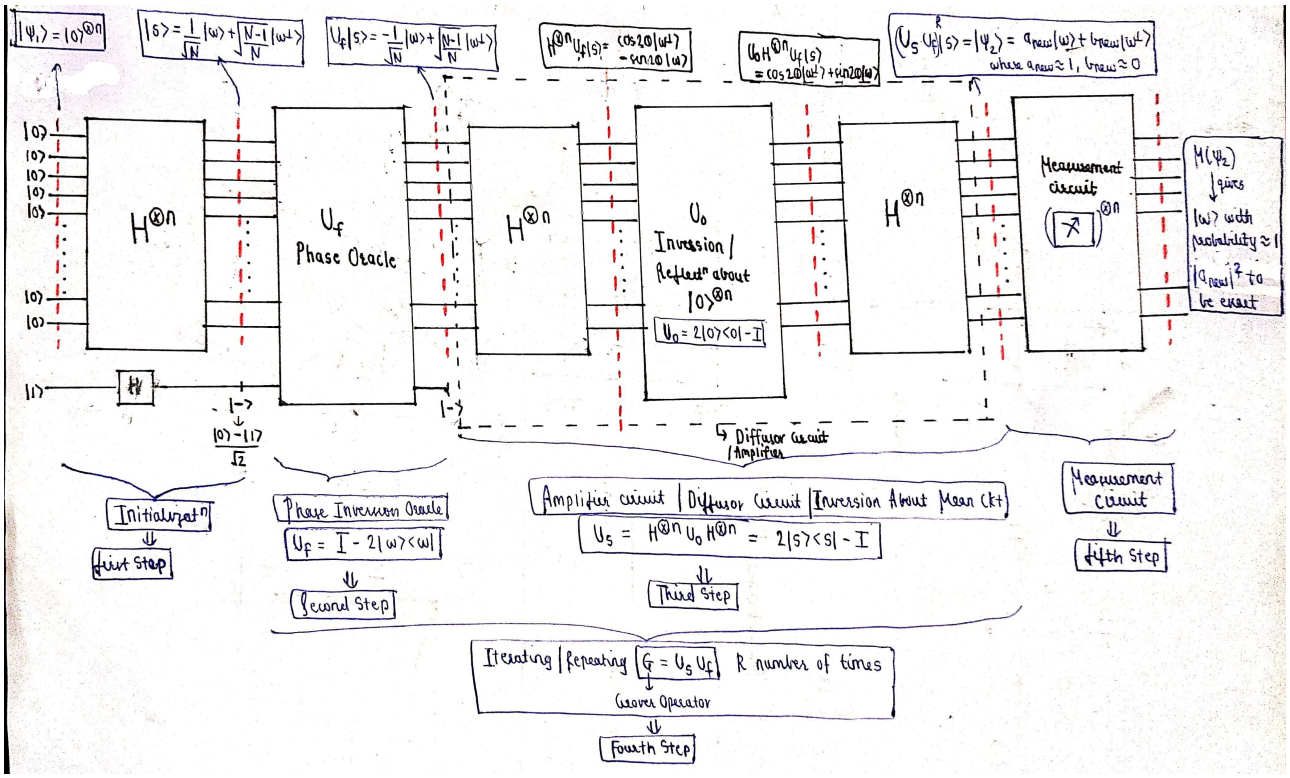

Figure 1: Quantum Circuit For Grover's Algorithm

if f(x)=1 then if y=0 then y$\oplus f(x) = 1$
if y=1 then y$\oplus f(x) = 1$
i.e U_f flips the value of y
U_f: $|x\rangle \otimes |-\rangle \rightarrow (-1)^{f(x)} |x\rangle \otimes |-\rangle$
Now if we apply U_f on $|s\rangle$
$U_f \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle = \frac{1}{\sqrt{N}} \sum_{x=1}^{N} (-1)^{f(x)} |x\rangle$ where f(x)=0 for $x \neq w$ and f(x)=1 for $x = w$

Note - By using maths manipulation We can write the uniform superposition state as the sum of winning state and all states orthogonal to winning state.

$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle = \frac{\sqrt{N-1}}{\sqrt{N}} |w^{\perp}\rangle + \frac{1}{\sqrt{N}} |w\rangle \rightarrow |s\rangle = a|w\rangle + b|w^{\perp}\rangle \rightarrow |s\rangle = \sin\theta\ |w\rangle + \cos\theta\ |w^{\perp}\rangle$

where $|w^{\perp}\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq w} |x\rangle$ $a = \sin\theta = \frac{1}{\sqrt{N}}$, $b = \cos\theta = \frac{\sqrt{N-1}}{\sqrt{N}}$

Now , $U_f|s\rangle = \frac{\sqrt{N-1}}{\sqrt{N}} |w^{\perp}\rangle - \frac{1}{\sqrt{N}} |w\rangle = -a|w\rangle + b|w^{\perp}\rangle \rightarrow U_f|s\rangle = -\sin\theta\ |w\rangle + \cos\theta\ |w^{\perp}\rangle$[h]

Hence if we represent a space such that our winning state $|w\rangle$ is along vertical axis and all the remaining states i.e states orthogonal to $|w\rangle$ as horizontal axis (more accurately a plane) and a uniform superposition vector $|s\rangle$ that satisfies $\sin\theta\ |w\rangle + \cos\theta\ |w^{\perp}\rangle$ equation in a 2D plane then $U_f|s\rangle$ is nothing but a reflection operation of $|s\rangle$ about $|w^{\perp}\rangle$ in the 2D plane in Figure 2.

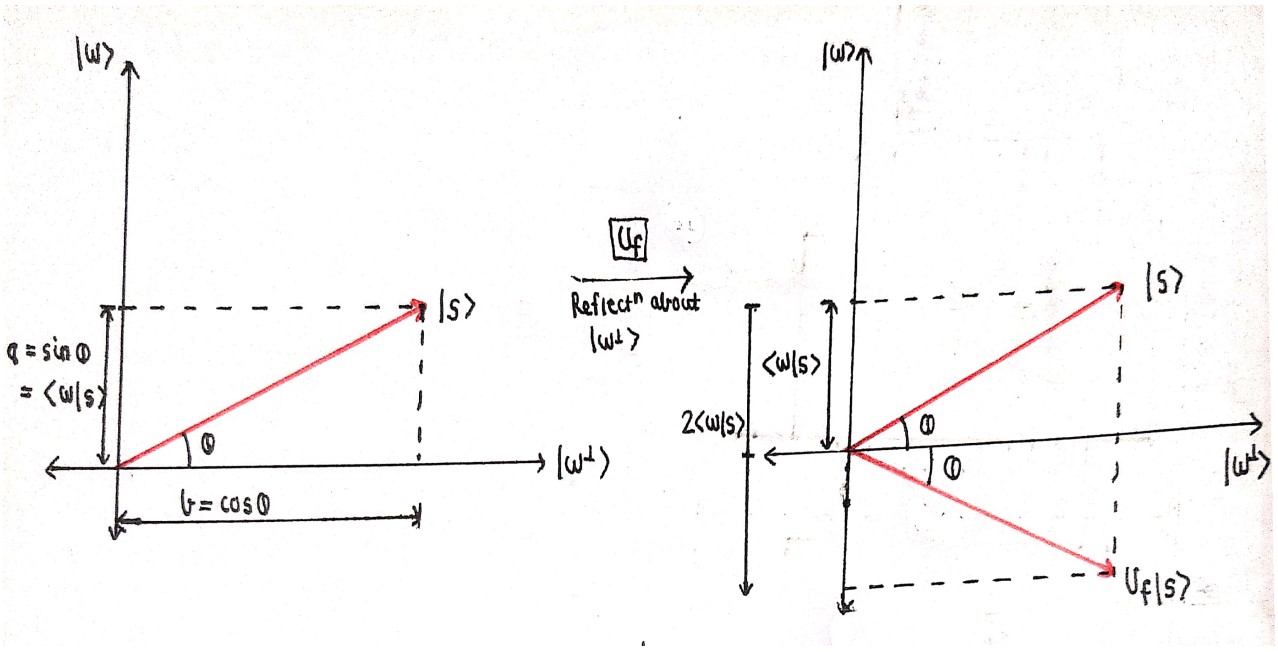

Figure 2: Visualization Of U_f operation in 2D plane i.e Reflection about $|w^{\perp}\rangle$

In Matrix form U_f= $\begin{bmatrix} (-1)^{f(x)} & 0 & \cdots & 0 \\ 0 & (-1)^{f(x)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & (-1)^{f(x)} \end{bmatrix}_{N\times N}$

where f(x)=0 for $x \neq w$ and f(x)=1 for $x = w$

Note-Here as $|x\rangle$ and $|-\rangle$ are not entangled hence for simplicity we can take U_f to be $N \times N$ matrix acting on $|x\rangle$ and keep the $|-\rangle$ state as it is in output

Hence we can define the phase inversion oracle operator as U_f= I-2$|w\rangle\langle w|$

Verification: $U_f|w\rangle$= (I-2$|w\rangle\langle w|$)$|w\rangle$=$|w\rangle$- 2$|w\rangle$=-$|w\rangle$ → Phase inversion of winning state

$U_f|w^{\perp}\rangle$= (I-2$|w\rangle\langle w|$)$|w^{\perp}\rangle$=$|w^{\perp}\rangle$ → Keeping the orthogonal states to $|w\rangle$ as it is

$U_f|s\rangle$= (I-2$|w\rangle\langle w|$)$|s\rangle$=-a$|w\rangle$+ b$|w\rangle$ → Reflection of the uniform superposition state $|s\rangle$ about $|w^{\perp}\rangle$

We can also understand this reflection operation by drawing Amplitude vs State diagram. As shown in figure 3 when U_f acts on uniform superposition state $|s\rangle$ then only the amplitude of the winning state flips its sign and remaining amplitudes stay as it is i.e we get

$U_f\,|s\rangle$= $\frac{-1}{\sqrt{N}}\,|w\rangle$+$\sqrt{N-1}\frac{}{\sqrt{N}}\,|w^{\perp}\rangle$

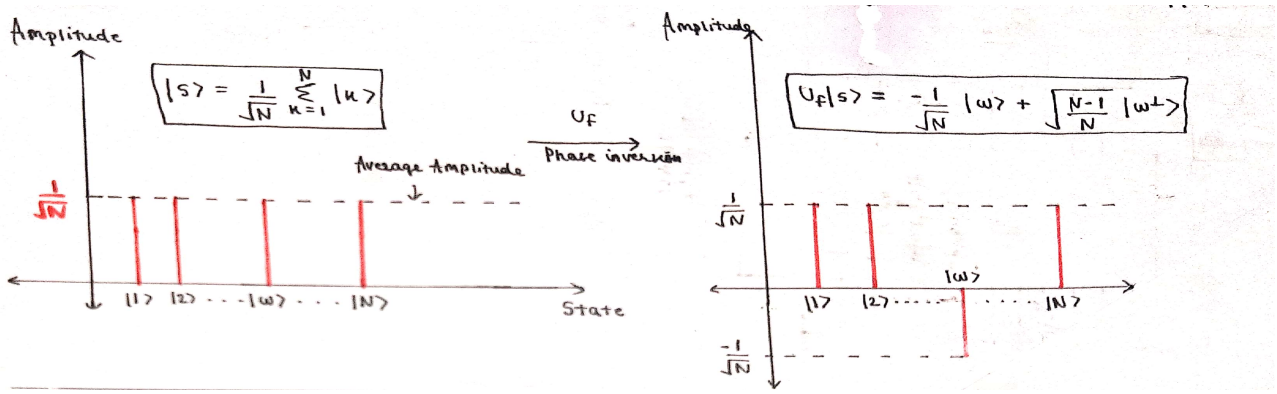

Figure 3: Visualization Of U_f operation from Amplitude vs State Graph i.e Phase Inversion of the winning state $|w\rangle$

3.Third Step Of Algorithm

Once our winning state is marked/phase inverted now comes the step of marked state amplification.We are free to choose this operator unlike the phase oracle operator.What we conventionally use is a diffuser operator which does an inversion about mean operation or reflection about $|s\rangle$ in the 2D plane of all the states including our marked winning state.But since the winning state is already phase inverted when we perform its inversion about mean its amplitude increases manyfolds (by $2/\sqrt{N}$ to be exact) compared to remaining orthogonal states which increases the probability that measurement at end of our Quantum Circuit gives $|w\rangle$

Explaination of the Diffusor Circuit

We follow a 3 step process for achieving this reflection about $|s\rangle$

Step 1 - Transform the uniform superpostion state $|s\rangle$ into $|0\rangle^{\otimes n}$ by using $H^{\otimes n}$

Step 2- Reflection about $|0\rangle^{\otimes n}$ by using a Unitary Transformation U_0

Step 3- Transform $|0\rangle^{\otimes n}$ into $|s\rangle$ by using inverse Hadamard Transform

By using above 3 steps as a basis guideline let us define and derive the diffuser/Amplitude Operator

U_s= $H^{\otimes n}U_0H^{\otimes n}$

Define U_0= $\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 \end{bmatrix}_{N\times N} \longrightarrow$ Leaves the $|0\rangle^{\otimes n}$ state as it is and inverts all the remaining states about $|0\rangle^{\otimes n}$

U_0=2$|0\rangle^{\otimes n}\langle 0|^{\otimes n}$- I

Now U_s becomes U_s= $H^{\otimes n}$(2$|0\rangle^{\otimes n}\langle 0|^{\otimes n}$- I)$H^{\otimes n}$=$H^{\otimes n}$($\begin{bmatrix} 2 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}$ - I)$H^{\otimes n}$

=$H^{\otimes n}$ $\begin{bmatrix} 2 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}$ $H^{\otimes n}$ - $H^{\otimes n}$I$H^{\otimes n}$ = $\frac{1}{\sqrt{N}}\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{bmatrix}\begin{bmatrix} 2 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}\frac{1}{\sqrt{N}}\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{bmatrix}$ - I

= $\begin{bmatrix} 2/N-1 & 2/N & \cdots & 2/N \\ 2/N & 2/N-1 & \cdots & 2/N-1 \\ \vdots & \vdots & \ddots & \vdots \\ 2/N & 2/N & \cdots & 2/N-1 \end{bmatrix} \longrightarrow$ Diffuser Operator in Matrix Form

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

Proof of why U_s is reflection about mean:

Consider U_s acting on U_f $|s\rangle$ then in matrix form the equation becomes,

$\begin{bmatrix} 2/N-1 & 2/N & \cdots & 2/N \\ 2/N & 2/N-1 & \cdots & 2/N-1 \\ \vdots & \vdots & \ddots & \vdots \\ 2/N & 2/N & \cdots & 2/N-1 \end{bmatrix}\begin{bmatrix} \frac{1}{\sqrt{N}} \\ \frac{1}{\sqrt{N}} \\ \vdots \\ \frac{-1}{\sqrt{N}} \\ \vdots \\ \frac{1}{\sqrt{N}} \end{bmatrix}_{N\times 1} = \begin{bmatrix} 2/\sqrt{N}(1-(2/N))-(1/\sqrt{N})) \\ 2/\sqrt{N}(1-(2/N))-(1/\sqrt{N})) \\ \vdots \\ 2/\sqrt{N}(1-(2/N))+(1/\sqrt{N})) \\ \vdots \\ 2/\sqrt{N}(1-(2/N))-(1/\sqrt{N})) \end{bmatrix}_{N\times 1} = \begin{bmatrix} 2\mu-(1/\sqrt{N}) \\ 2\mu-(1/\sqrt{N}) \\ \vdots \\ 2\mu+(1/\sqrt{N}) \\ \vdots \\ 2\mu-(1/\sqrt{N}) \end{bmatrix}$

where μ=Average Amplitude after one iteration=$\frac{1}{\sqrt{N}}(1-(\frac{2}{N}))$

Verification : $U_s|s\rangle$= (2 $|s\rangle\langle s|$- I)$|s\rangle$= $|s\rangle \rightarrow$ superposition state remains as it is under U_s

$U_s(U_f|s\rangle)$= (2 $|s\rangle\langle s|$- I)$(U_f|s\rangle)$= (2$|s\rangle\langle s|$- I)(-a $|w\rangle + b\left|w^{\perp}\right\rangle$) = $-a(2\ |s\rangle\langle s|$- I) $|w\rangle + b(2\ |s\rangle\langle s|$- I) $\left|w^{\perp}\right\rangle$

=-a(2$|s\rangle\langle s|w\rangle - |w\rangle) + b(2\ |s\rangle\left\langle s|w^{\perp}\right\rangle - \left|w^{\perp}\right\rangle)$

$\langle s|w\rangle = a\langle w|w\rangle + b\left\langle w^{\perp}|w\right\rangle = a$ (as we are working in 2D real space we can take $a = a^*$ and $b = b^*$)

$\left\langle s|w^{\perp}\right\rangle = b$ (Similarly)

= 2(b$^2 - a^2$) $|s\rangle + a\,|w\rangle - b\left|w^{\perp}\right\rangle$

Now putting $|s\rangle$= a$|w\rangle$+b$\left|w^{\perp}\right\rangle$ we get $U_s(U_f|s\rangle)$= (2ab$^2 - 2a^3 + a)|w\rangle$+(2$b^3 - 2ba^2 - b$) $\left|w^{\perp}\right\rangle$

Now putting $a = sin\theta$ and $b = cos\theta$ and solving we approximately get $U_s(U_f|s\rangle)$=sin3$\theta\,|w\rangle + cos3\theta\left|w^{\perp}\right\rangle$ i.e which proves that U_s acting on $(U_f|s\rangle)$ is a reflection operation about s vector.

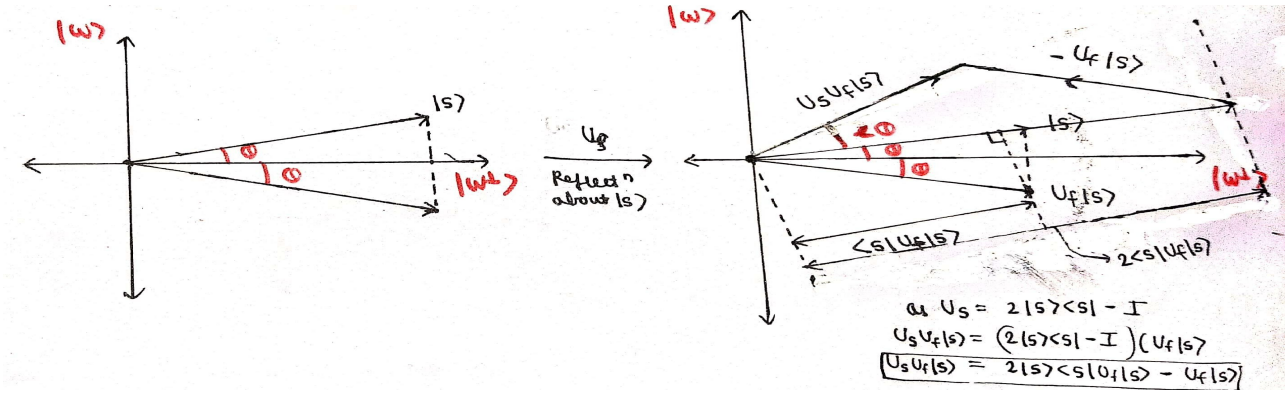

Figure 4: Visualization of U_s acting on $U_f\ |s\rangle$
i.e Reflection of $U_f\ |s\rangle$ about $|w^{\perp}\rangle$

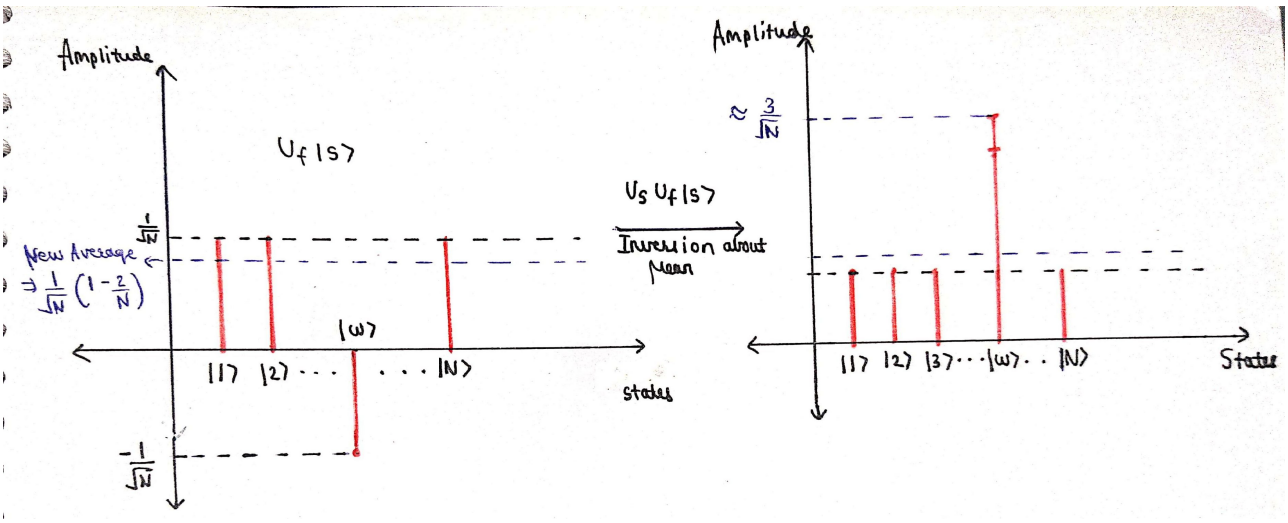

Figure 5: Visualization of U_s acting on $U_f\ |s\rangle$
i.e Reflection of $U_f\ |s\rangle$ about $|w^{\perp}\rangle$

As shown in Figure 4 U_s acting on $U_f|s\rangle$ is nothing but a reflection operation that reflects $U_f|s\rangle$ vector about $|s\rangle$ hence the final state after third step of Grover's Algorithm is

$U_s U_f|s\rangle = sin3\theta|w\rangle + cos3\theta|w^{\perp}\rangle$

Also as shown in Figure 5 U_s acting on $U_f|s\rangle$ can also be interpreted as inversion operation of amplitudes of all states about mean amplitude.As $U_f|w\rangle$ inverts the phase of $|w\rangle$,when the inverted winning state is reflected about mean it reflects by an amplitude of $2/\sqrt{N}$ i.e its amplitude now becomes $3/\sqrt{N}$.Hence we have achieved the purpose of amplifying the winning state by applying the Grover operator.

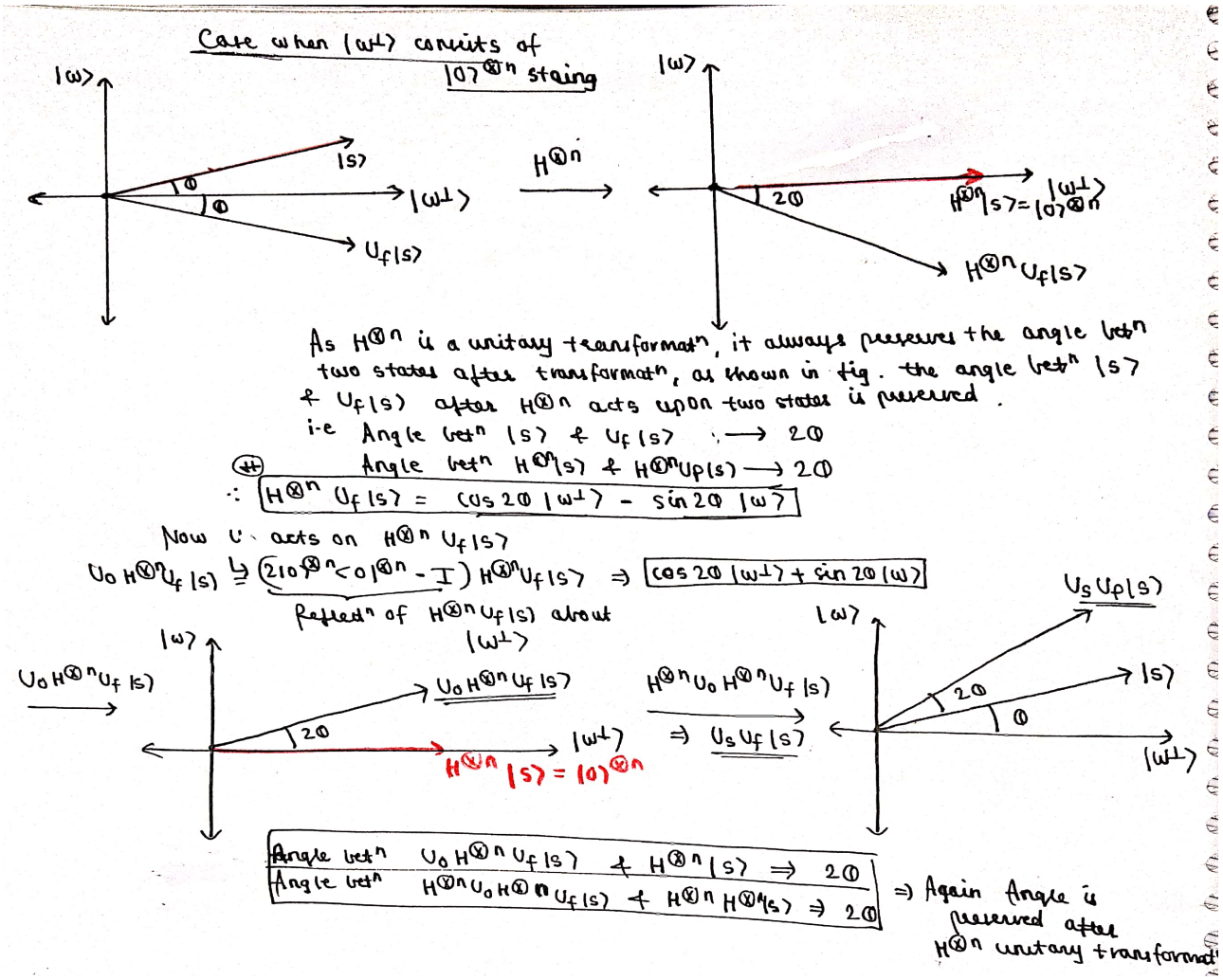

Figure 6: Step by step Visualization of U_s acting on $U_f\ |s\rangle$
i.e Reflection of $U_f\ |s\rangle$ about $|w^{\perp}\rangle$
(Arrived at this explaination after Discussion With Guru Krushna Anurag Sahoo Prasad)

4.Fourth Step of Algorithm

The $U_s(U_f|s\rangle)$ is called as Grover Operator. As we have already applied Grover operator once, we have achieved amplitude amplification by $2/\sqrt{N}$ or the rotation of $|s\rangle$ *by* 2θ.Hence now if we measure the end state there is higher probability that measured state is $|w\rangle$ but to achieve a success probability closer to 1 ,we should perform Grover Operator optimal number of times which is given by $2R\theta + \theta = \pi/2$ where $2R\theta$ is total rotation of $|s\rangle$ in anticlockwise direction(as per our figure) after R iterations of Grover Operator and θ is the initial angle $|s\rangle$ makes with $|w^{\perp}\rangle$ before application of Grover Operator.

draw figure/graph of how vector s varies after each iteration

Optimum Number of Iterations R :

$2R\theta + \theta \approx \pi/2 \rightarrow$ R= $\pi/4\theta$ - 1/2 $\rightarrow$ R= $\pi/4sin^{-1}(1/\sqrt{N}) - 1/2 \rightarrow$ For Large N using linear approximation $\sin^{-1}(1/\sqrt{N}) \approx (1/\sqrt{N}) \rightarrow$ R$\approx (\pi/4)\sqrt{N} = O(\sqrt{N}) \rightarrow$ Quadratic Speedup

If we apply Grover Operator R times i.e $(U_s U_f|s\rangle)^R$ then the initially uniform superposition state vector $|s\rangle$ aligns itself with $|w\rangle$ with angle deviation no larger than θ. The number of iterations R is of the order of $O(\sqrt{N})$. This is due to the fact that in quantum mechanics probabilities are squares of amplitudes i.e. R quantum queries increase the success probability quadratically in R as opposed to only linear rise in classical R queries.

5.Fifth Step of Algorithm

Now after successful theorization of first four steps only the last step of measuring the output state of our Quantum Circuit remains.

Circuit output state→ $|\psi_2\rangle$ =H$^{\otimes n}$(U_s($U_f|s\rangle$))^R $|\psi_1\rangle = a_{new}|w\rangle + b_{new}|w^\perp\rangle$
where $a_{new} \approx 1$ and $b_{new} \approx 0$
Measurement of Output State→ $M(|\psi_2\rangle)$ gives $|w\rangle$ with probability nearly equal to 1 ($sin^2(\theta_{new})$ to be exact) and $|w^\perp\rangle$ with probability nearly equal to 0 ($cos^2(\theta_{new})$ to be exact)

As shown in figure 6 after R iterations of the Grover's Operator we get a state very close to winning state $|w\rangle$.But R as is calculated from $R \approx (\pi/4)\sqrt{N}$,it can come out as a non integer value but we cannot perform non integer iterations.Hence we round off to the nearest integer due to which there is some error angle ϕ between winning state $|w\rangle$ and ($U_sU_f|s\rangle$)^R.Hence the probablity of success after R iterations becomes $cos^2\phi$.Now the error angle at max can be θ because if its more than θ then we can perform one more iteration to make it less than or equal to θ.Hence the worst probability of success .i.e probability that measurement gives winning state $|w\rangle$ is $cos^2\theta$= $\frac{N-1}{N}$. Now from amplitude point of view if we perform the first iteration of Grover Operator then the amplitude of the winning state increases by $2/\sqrt{N}$ i.e the new amplitude of winning state is $3/\sqrt{N}$.

Increase in Amplitude per iteration $\frac{1}{\sqrt{N}} \xrightarrow{R=1} \frac{3}{\sqrt{N}} \xrightarrow{R=2} \frac{5}{\sqrt{N}} \cdots\cdots \xrightarrow{R=\frac{1}{2\sqrt{N}}} \frac{1}{\sqrt{2}} \cdots\cdots \xrightarrow{R=(\pi/4)\sqrt{N}} \approx 1$

Hence as the we apply Grover Operator R times we increase the amplitude of state $|w\rangle \approx 1$ and therefore the amplitude of the remaining states by normalization criteria is $1-\sqrt{1}$=0.

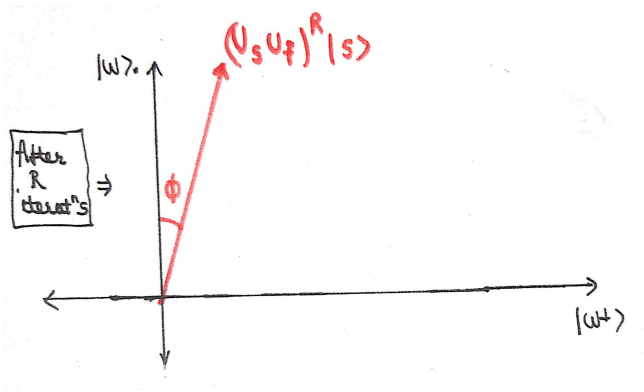

Figure 7: Visualization of U_sU_f after R iterations on 2D plane

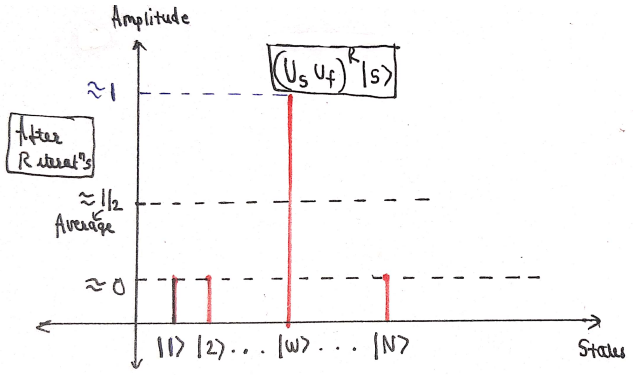

Figure 8: Visualization of U_sU_f after R iterations on Amplitude vs State Diagram

3 Summary of Grover's Algorithm

1.First Step - Initialization- Transformation of N strings each of n bits into uniform superposition of states by using Hadamard Transform.
2.Second Step- Marking the winning state by using the phase oracle U_f i.e.in simple terms adding a negative global phase to the winning state.
3.Third Step- Amplification of the amplitude of the marked state by using the inversion about mean approach which gives a diffusion operator U_s

4.Fourth Step- Repeating/Iterating the Grover Operator= $U_f U_s$ R number of times where R$\approx (\pi/4)\sqrt{N}$
5.Fifth Step- Measuring the output state $|\psi_2\rangle$ which on measurement should give winning state with a probability close to 1.

4 Multiple Winning States

If the number of winning states are greater than 1 i.e M>1 then we can define the winning state $|w\rangle$ and all the states orthogonal to winning states i.e $|w^{\perp}\rangle$ as

$|w\rangle = \frac{1}{\sqrt{M}} \sum_{j=1}^{M} |w_j\rangle$ and $|w^{\perp}\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \neq (w_1,\ldots,w_M)} |w_j\rangle$

Now we can define the superposition state as

$|s\rangle = \frac{\sqrt{M}}{\sqrt{N}}|w\rangle + \frac{\sqrt{N-M}}{\sqrt{N}}|w^{\perp}\rangle = sin\theta|w\rangle + cos\theta|w^{\perp}\rangle$

Number of Grover Operator Iterations $\rightarrow$

R= π/(4sin$^{-1}(\sqrt{M}\frac{}{\sqrt{N}})$) - (1/2) = O($\frac{\sqrt{N}}{\sqrt{M}}$)

As angle θ is larger for M>1 when compared to M=1,the superposition state $|s\rangle$ takes only O($\frac{\sqrt{N}}{\sqrt{M}}$) quantum queries to the oracle to align itself to the M winning states $|w\rangle$.Hence when number of winning strings are greater than 1 we require less quantum queries as well as less time to find the required set of winning states from the given set of strings by a factor $\sqrt{M}$.Classically we still need O(N/M) queries to the oracle to find the marked set of strings/objects.

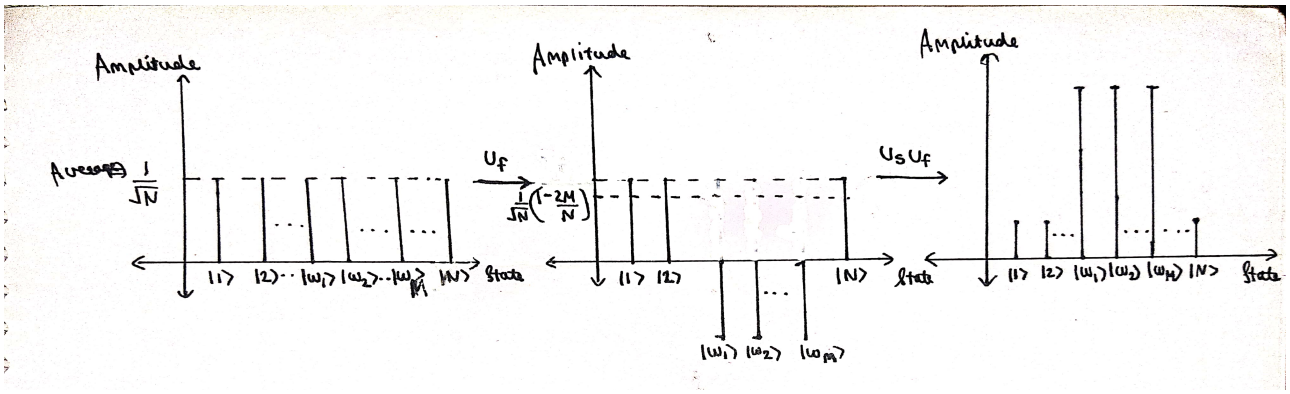

Figure 9: Multiple Winning States Amplitude vs State Diagram

5 Optimality Of Grover's Theorem

To check the optimality of any Quantum Algorithm there are two criterions -

1.Time Optimality

2.Query Optimality

Here,I will not go in to detailed proofs of the optimality of Grover's Algorithm but just introduce its notion. For finding the time taken for a unstructured database search by Grover Algorithm we have to see the time evolution of effective Hamiltonian of the Grover Algorithm.As given in Dr.Apoorva Patel's paper the effective time independent Hamiltonian takes the geodesic(shortest) route on bloch sphere when we go from state $|s\rangle$ to $|w\rangle$ implying that Grover's Algorithm is time wise optimal. One can find the optimal time required for Grover's Algorithm to search the string is O($\sqrt{N}$).

Note- Adiabatic Quantum Search which takes evolution of the time dependent Hamiltonian also follows geodesic route on bloch sphere and takes time of order O($\sqrt{N}$) implying no other Hamiltonian exist which can give better results and also no other algorithm exists (till date) which can give better time wise results unless we apply specific problem oriented algorithms.

As for the query complexity it is shown in Preskill's Notes that optimal Query for Quantum Search is O($\sqrt{N}$) and Grover's Algorithm achieves the optimal success probability in O($\sqrt{N}$) queries.

6 Quantum Complexity And Possible Applications of Grover's Algorithm

The Grover's Algorithm provides quadratic speedup over classical for unstructured database search. The optimality of Grover's Algorithm implies that NP class problems is not a subset of BQP (class of problems that are efficiently solvable by quantum computers known as Bounded error Polynomial). This also implies that a quantum computer cannot solve all the problems intractable to classical computers.

NP complete/NP Hard problems are presently intractable by classical computers but an optimal solution can be provided by approximating the problem to a solvable framework.Finding a solution to NP complete problems can be viewed as 'search problem'.Example of such class of problems are 'The Travelling Salesman Problem','Satisfiability (SAT) Problem' etc.All the NP complete problems can be thought of as an equivalent of 'SAT' problem.So once you have a exact solution to 'SAT' problem you can solve all the problems in NP complete class.It can also be able to give us an answer to millennium problem of whether P=NP or $P \neq NP$. As shown in Grover's Algorithm by using the principles of Quantum Mechanics mainly the Entanglement and Superposition i.e.Quantum Parallelism the optimal speedup that we can achieve for exhaustive search is quadratic.A quadratic speedup is an advantage which may be useful for variety of NP class problems but unlike an exponential speedup it cannot cross the bridge from intractability to solvability i.e a verbal argument of NP is not a subset of BQP. As the universe works on the laws of quantum Physics,a quantum computer is as good as the nature itself.So therefore within the laws of Quantum Physics we cannot construct a computer better than quantum computer which can efficiently solve all complexity classes of problems unless it turns out that laws of physics need modification in the light of future discoveries.

Possible (Far-fetched) Applications Of Grover's Algorithm -

1.Solving Chess Completely i.e whatever move black makes white always wins i.e searching for the best moves possible for both white and black.But the complexity of chess is so vast that a mere quadratic speedup cannot do it in finite time.(at least exponential speedup is needed for exhaustive search to achieve this task in finite time which is not possible in present).Of course AI's such as Alphazero, Leela chess zero exists which can give not the best but optimal moves for each position that arises in chess.

2.Travelling Salesman Problem

The traveling salesman problem is an NP Hard Problem of finding the shortest route possible. In simpler terms, given a number of interconnected cities, with certain distances between them, is there a route of less than m kilometers for which the salesman can visit every city? By applying Grover's Algorithm it is possible to complete the search for the route less than m Kms in O($\frac{1}{\sqrt{N}}$) steps.For M different solutions of m the time complexity for Grover's Algorithm is With Grover's algorithm it is possible to complete a search for a route of less than m kilometers in steps rather than an average of (which is O(N)) steps for the classical case. If we have M different solutions for m then the time complexity for Grover's algorithm is O($\frac{\sqrt{N}}{\sqrt{M}}$).

3. SAT 4.SUDOKU etc...

So basically all optimization problems of the NP complete class can be viewed as an exhaustive search problems and for achieving a quadratic speedup to exhaustive search we can apply Grover's Algorithm . But a mere quadratic speedup cannot give tractability to these problems but only help in finding the optimal solutions faster compared to classical ones.

7 Practical Implementation Of Grover's Algorithm on Quantum Computer

Again lets follow a step by step approach-

1.First Step- Initialization -

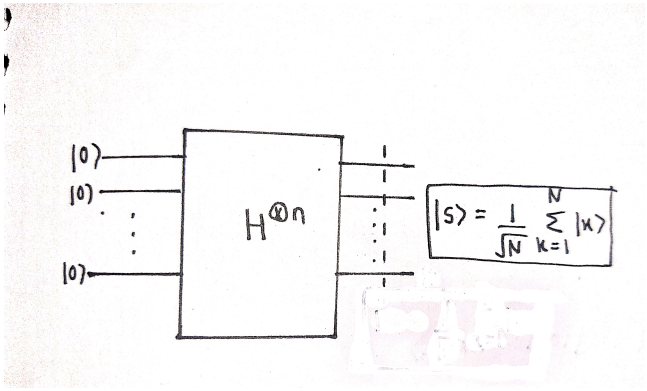

Figure 10: Initialization Circuit

As Hadamard Gate is Universal Gate Operation it is available ready made on IBM computer for implementation so no need to discuss it any further.

2.Second Step- Phase Inversion Oracle

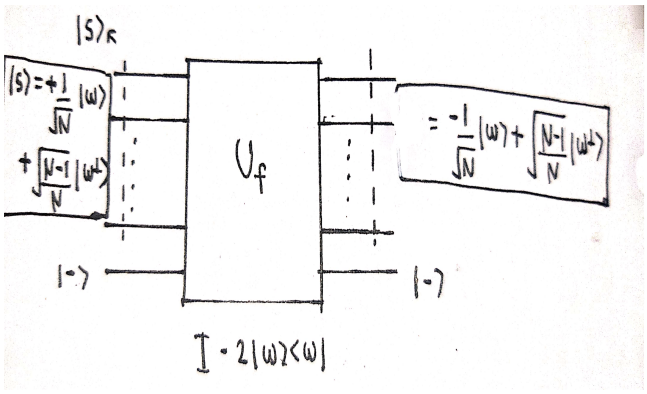

Figure 11: Theoritical Phase Oracle U_f circuit

As U_f oracle depends on our winning state $|w\rangle$,the practical circuit that performs this operation on Quantum Computer also depends on the winning state.Hence if we change the winning state the circuit that performs the phase iversion operation also changes. Hence lets take an example of 3 Qubit system to understand the practical implementation of phase inversion.

Number of States $N = 2^3 = 8$ After the step of initialization the state is

$|s\rangle$=(|000⟩+|001⟩+|010⟩+|011⟩+|100⟩+|101⟩+|110⟩+|111⟩)/$\sqrt{8}$

If we want to find the winning state $|000\rangle$ then the circuit of implementation will be as shown in figure 11

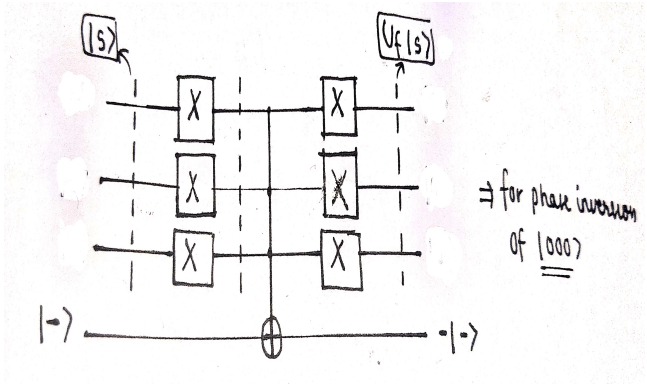

Figure 12: Phase inversion ckt for $|000\rangle$

Note- This circuit will only flip the sign of $|000\rangle$ and will leave the remaining states as it is.

The Basic Function of X gate is to rotate the state by 180 degrees on Bloch sphere about x axis or by 90 degrees in Hilbert Space.

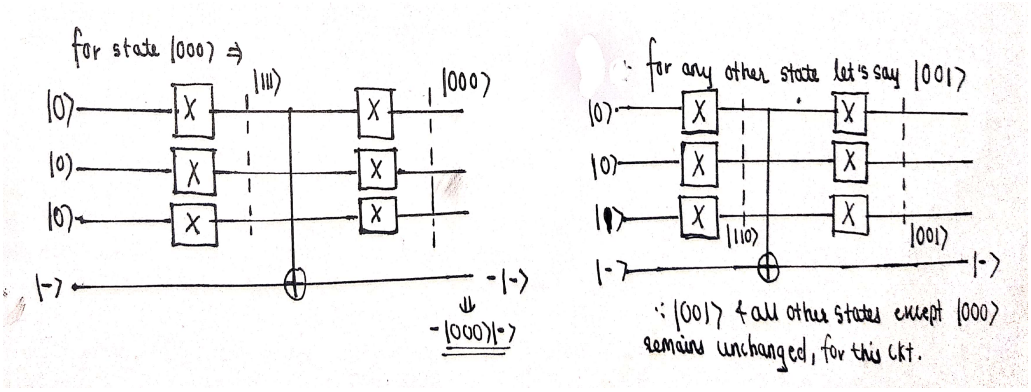

Figure 13: Working of Phase inversion circuit for state $|000\rangle$ and any other state

X=Pauli X Matrix=$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \rightarrow X\ |0\rangle$=$|1\rangle$ and X$|1\rangle$=$|0\rangle$ hence it also known as bit flip gate.

The Basic Function of $C^{n-1}NOT$ is to flip the target bit if and only if all the n-1 control bits are 1.

In Matrix Form, C-NOT matrix=$\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$

Similarly,$C^{n-1}NOT$ matrix=$\begin{bmatrix}1 & 0 & \cdots & 0 & 0\\ 0 & 1 & \cdots & 0 & 0\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & \cdots & 0 & 1\\ 0 & 0 & \cdots & 1 & 0\end{bmatrix}_{N\times N}$

Now that we know the basics of X Gate and $C^{n-1}NOT$ Gate.Lets get back to our example. Consider only the winning state $|w\rangle$=$|000\rangle$ then

X$^{\otimes 3}$($|0^{\otimes 3}\rangle$) $\rightarrow 1^{\otimes 3}$

Now as all the target bits are 1 the C^3NOT acting on $|-\rangle$ = ($|0\rangle$-$|1\rangle$)/$\sqrt{2}$ gives ($|1\rangle$-$|0\rangle$)/$\sqrt{2}$ i.e -$|-\rangle$.Hence our winning state now is -$|111\rangle|-\rangle$.Note- As $|-\rangle$ and $|111\rangle$ are not an entangled states we can assign the negative sign obtained for $|-\rangle$ to $|111\rangle$. Now to revert back to our original winning state again apply $X^{\otimes 3}$ as X gate is an inverse of itself $X^{\otimes 3}(-\ |1^{\otimes 3}\rangle) \rightarrow -0^{\otimes 3}$. Hence we have successfully marked the winning states.One can verify that the remaining states are unchanged when input to the circuit.

$U_f|s\rangle$= (-$|000\rangle$+$|001\rangle$+$|010\rangle$+$|011\rangle$+$|100\rangle$+$|101\rangle$+$|110\rangle$+$|111\rangle$)/$\sqrt{8}$

One can also verify that $X^{\otimes 3}$[C^3NOT]$X^{\otimes 3}$= U_f=$\begin{bmatrix}-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1\end{bmatrix}_{8\times 8}$ which implies that theory is equivalent to practical implementation of U_f

Scaling Up the Circuit of Phase Inversion for n Qubits

The General Concept for implementing U_f for n qubits is as follows, Consider the uniform superposition state $|s\rangle$= $\frac{1}{\sqrt{N}}\sum_{x=1}^{N}|x\rangle$= $\frac{\sqrt{N-1}}{\sqrt{N}}\ |w^{\perp}\rangle$ + $\frac{1}{\sqrt{N}}\ |w\rangle$.

Now to mark the winning state $|w\rangle$ which consists of some bit string lets say $|1001000110.....\rangle$, we just have to make 0 bits in the string to be 1 by applying X gate on that register and keeping 1 bit as it is or applying identity to 1,followed by $C^{n-1}NOT$ to flip the sign of the state $|-\rangle$ followed by again applying X gates on the those bits which 0 at the start to revert its present 1 state back to 0,thus we get our winning state phase inverted as shown in the figure 13.

Practical implementation of U_f for any winning state $|w\rangle$ can be thought as applying X gate to m bits of $|w\rangle$ that are 0 and keeping the remaining n-m bits as it is i.e applying an identity operator on remaining n-m bits to make the $C^{n-1}NOT$ gate flip the sign of state $|-\rangle$,then again applying X gate to m bits of $|w\rangle$ that are 0 and keeping the remaining n-m bits as it is to recover our original winning state.

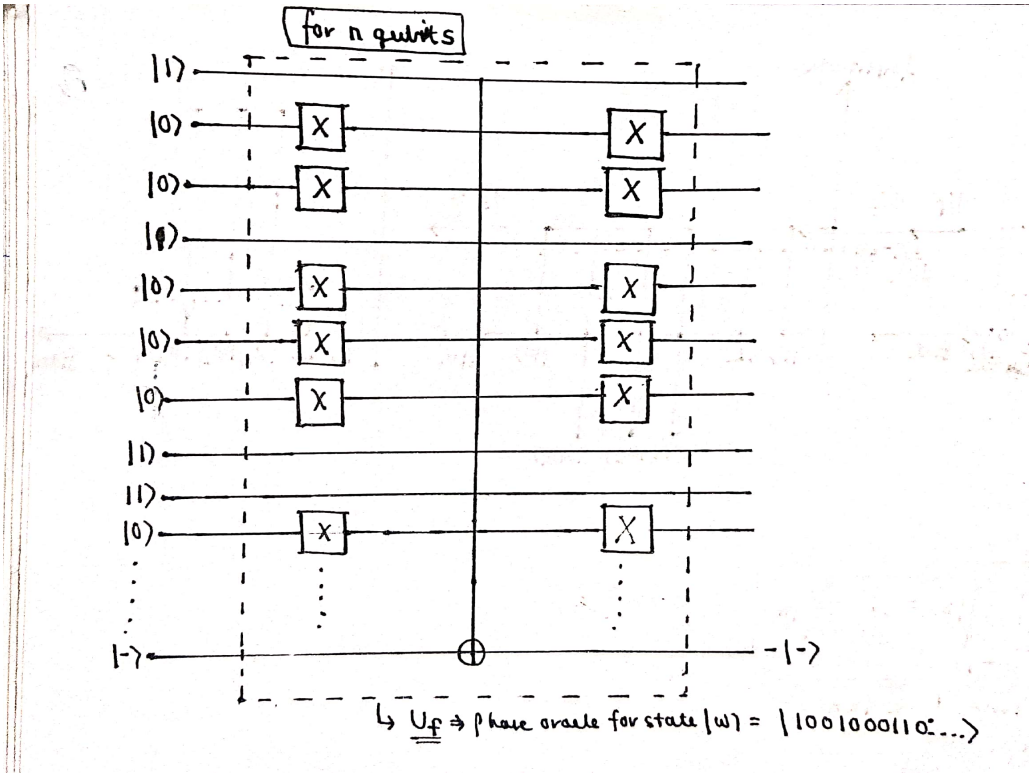

Figure 14: Phase inversion circuit for n qubits of specific winning state $|w\rangle$

Note- We can directly implement X gate on Qiskit and also by using the command mcx[control bits,targets bits] one can easily implement $C^{n-1}NOT$ gate and thus I will not go into details of converting the multiple CNOT gate into Toffoli Gate $(C^2NOTgate)$.

Third Step - Amplification Operation or Inversion about Mean Operation or Diffusion Operation

Again lets take a simple 3 Qubit system before scaling it upto n qubits system.

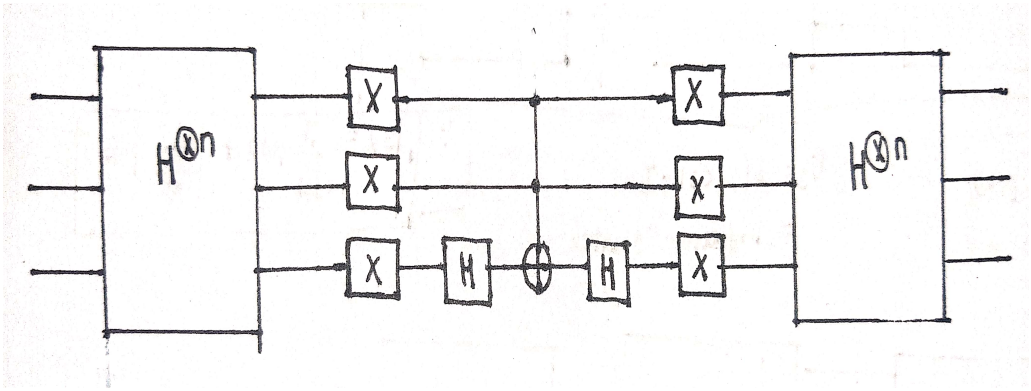

Figure 15: Diffusor/Amplifier Circuit for 3 Qubits

Let our input state be $|s\rangle$=(|000⟩+|001⟩+|010⟩+|011⟩+|100⟩+|101⟩+|110⟩+|111⟩)/$\sqrt{8}$ $|s\rangle$= and let our winning state be $|010\rangle$ then $U_f|s\rangle|s\rangle$=(|000⟩+|001⟩-|010⟩+|011⟩+|100⟩+|101⟩+|110⟩+|111⟩)/$\sqrt{8}$.Now when we apply Hadamard Transform to this state then the state becomes $H^{\otimes 3}U_f|s\rangle$=(|+ + +⟩+|+ + −⟩-|+ − +⟩+|+ − −⟩+|− + +⟩

We ignore the amplitude for now and just visualize how our input state progresses in the diffusor circuit.So lets begin!

We know that X acting on $|+\rangle$ gives $|+\rangle$ and X acting on $|-\rangle$ gives -$|-\rangle$. Now we are applying X gates to all the registers then the state becomes ($|+++\rangle$-$|++-\rangle$+$|+-+\rangle$+$|+--\rangle$-$|-++\rangle$+$|-+-\rangle$+$|--+\rangle$-$|---\rangle$)

Now we are applying HXH on the last bit of each state i.e we are flipping the last bit of each state from $|+\rangle$ to $|-\rangle$ or vice-versa in the above superposed state,then the state becomes ($|++-\rangle$-$|+++\rangle$+$|+--\rangle$+$|+-+\rangle$-$|-++\rangle$+$|-+-\rangle$+$|+++\rangle$+$|---\rangle$-$|--+\rangle$)

Now we are reversing the gates to get similar structure to our input state.Applying X gates to all the registers then the state becomes (-$|++-\rangle$-$|+++\rangle$-$|+-+\rangle$+$|+--\rangle$+$|-++\rangle$+$|-+-\rangle$+$|++-\rangle$+$|---\rangle$+$|--+\rangle$)

Now applying the inverse Hadamard Operation, we get the state

$U_fU_s|s\rangle$= $5/2\sqrt{8}$($|010\rangle$)+$1/2\sqrt{8}$ ($|000\rangle$+$|001\rangle$+$|011\rangle$+$|100\rangle$+$|101\rangle$+$|110\rangle$+$|111\rangle$).

Hence now if we measure the state we get $|010\rangle$ with probability $(5/2\sqrt{8})^2$ and remaining states with probability $((1/2\sqrt{8})^2$ Now lets figure out in matrix notation from where is the amplitude amplification coming in to picture.

$$U_s\text{=H}^{\otimes 3}(X^{\otimes 2}\otimes[(\text{X}_3H_3)(C^2NOT(H_3X_3)]\otimes X^{\otimes 2})H^{\otimes 3} = \begin{bmatrix} -3/4 & 1/4 & \cdots & 1/4 \\ 1/4 & -3/4 & \cdots & 1/4 \\ \vdots & \vdots & \ddots & \vdots \\ 1/4 & 1/4 & \cdots & -3/4 \end{bmatrix}_{8\times 8}$$

$$\text{Now } U_sU_f|s\rangle = \begin{bmatrix} -3/4 & 1/4 & \cdots & 1/4 \\ 1/4 & -3/4 & \cdots & 1/4 \\ \vdots & \vdots & \ddots & \vdots \\ 1/4 & 1/4 & \cdots & -3/4 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{8}} \\ \frac{1}{\sqrt{8}} \\ \frac{-1}{\sqrt{8}} \\ \vdots \\ \frac{1}{\sqrt{8}} \end{bmatrix} = \begin{bmatrix} \frac{1}{2\sqrt{8}} \\ \frac{1}{2\sqrt{8}} \\ \frac{5}{2\sqrt{8}} \\ \vdots \\ \frac{1}{2\sqrt{8}} \end{bmatrix}$$

Thus we have successfully achieved an amplification of amplitude of winning state practically.

Scaling the Amplication Circuit for n qubits

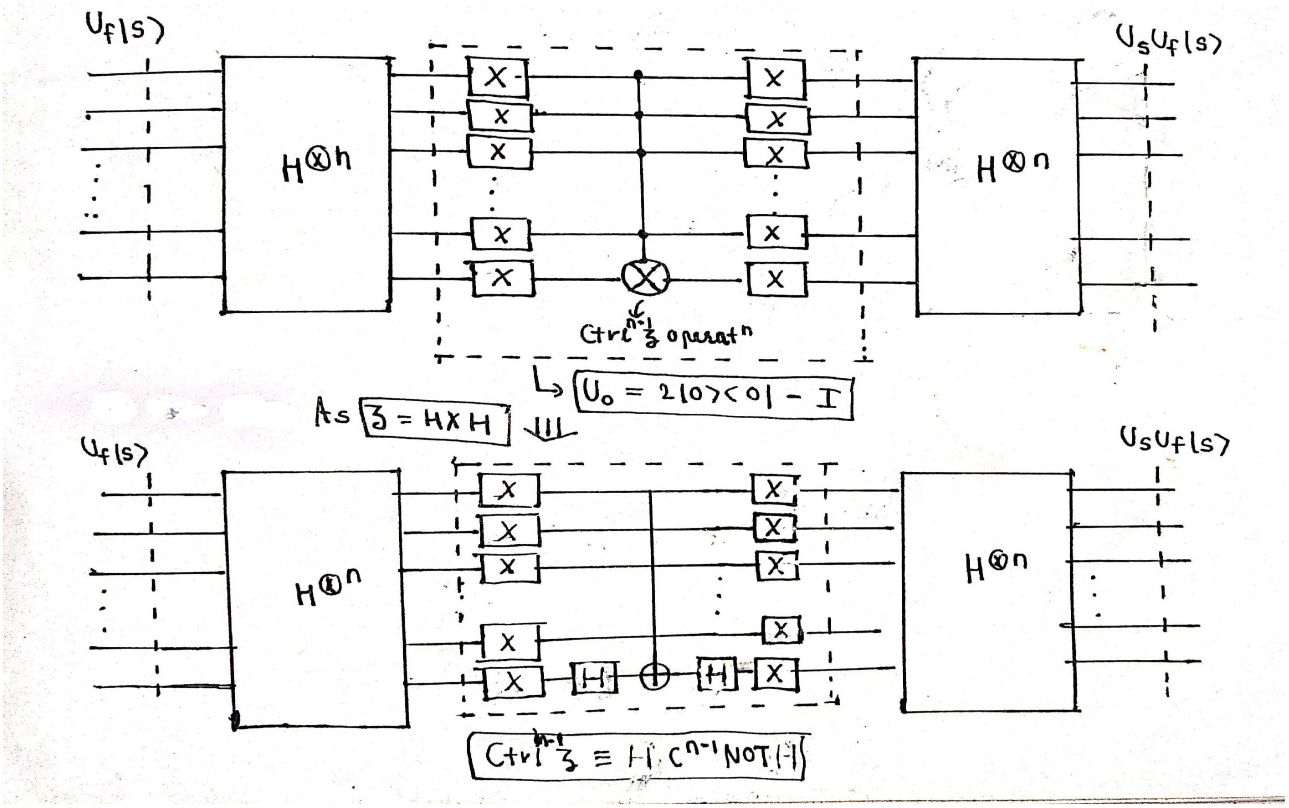

Figure 16: General Diffusor/Amplifier Circuit for n Qubits

Now for scaling the amplification circuit for n qubits as shown in the figure 15 we can write the cicuit for U_s in one line as,

U_s=H$^{\otimes n}$($X^{\otimes n-1}\otimes$[(X$_n H_n$)($C^{n-1}NOT$($H_n X_n$)]$\otimes X^{\otimes n-1}$)$H^{\otimes n}$ = $\begin{bmatrix} 2/N-1 & 2/N & \cdots & 2/N \\ 2/N & 2/N-1 & \cdots & 2/N-1 \\ \vdots & \vdots & \ddots & \vdots \\ 2/N & 2/N & \cdots & 2/N-1 \end{bmatrix}_{N\times N}$

One can verify the L.H.S (Theoritical Requirement)=R.H.S (Practical Realization) for 2 or 3 Qubit system just to get the clearer picture.

Fourth Step - Repeatition

Repeating the Grover Operator R times so that ($U_s U_f|s\rangle$) vector aligns itself with the winning state.

Grover circuit can be written as

G$^R H^{\otimes n}|0\rangle = ((\mathrm{U}_s U_f)^R (H^{\otimes n})|0\rangle^{\otimes n}$

= [[(H$^{\otimes n}$)$X^{\otimes n-1}\otimes$[(X$_n H_n$)($C^{n-1}NOT$($H_n X_n$)]$\otimes X^{\otimes n-1}$)($H^{\otimes n}$))[$X|0\rangle$,I$|1\rangle$]$^{\otimes n}$C^{n-1}NOT[$X|0\rangle$,I$|1\rangle$]$^{\otimes n}$]^R($H^{\otimes n}$)] $|0\rangle^{\otimes n}$

where $[0,1]^{\otimes n}$ is winning string and X gates are applied for 0 bits and Identity is applied to 1 bit of the winning string.

Fifth Step -Measurement of Output State

We can directly write a code to measure output state of the Grover circuit.Hence no need to discuss it further as the content will the same as discussed in Introduction.

8 Grover's Code on Github

I have implemented Grover's Circuit for 3 Qubits using a Database Oracle to Encode which again uses 3 Qubits plus 1 Qubit for Marking Gate so in total using 7 Qubits.

Link for My circuit implementation of Grover's Algorithm on IBM simulator and IBM Quantum Processor of 7 Qubits-

Implementation Of Grover's Algorithm on IBM Quantum Simulator and Quantum Processor using Qiskit

9 Results Detailed Summary (In Progress)

There are in general four types of errors/noises in practical quantum circuits-

A.Input State Creation Error-

Error caused when state created at the input i.e (lets say) $|0\rangle$ does not have fidelity equal to 1 i.e there is some error angle between exact state $|0\rangle$ and created state $|0\rangle$

B.Measurement Error-

Error caused in the measurement of output state.Measurement errors can be mitigated on qiskit. Both input and measurement errors independent of depth and width of the cicuit hence can be clubbed together as SPAM (State Preparation and Measurement Errors).

C.Gate Fidelity Error-

Errors caused when the actual output state of implemented gate differs from expected theoritical ideal output state by certain rotation on bloch sphere.This error occur due to coherent noise as well as the incoherent noise associated with the gates.As this error is due to the gates giving a different output state than theoretically expected ,it depends on the depth of the circuit.Depth of the circuit is nothing but the estimate of total number of gates used in the circuit.Hence as the number of gates used in the circuit increases this error increases quadratically for coherent noise and linearly for incoherent noise whose proof can be shown by simple linear algebra which I will not go into.

D.Projection Noise/Error-

In Ideal case we can perform the number of shots infinitely on identical quantum systems to get the ideal expected value of measurement,but practically we can perform only limited number of shots on near identical prepared quantum systems,hence we get the Projection error.

Due to the above four types of errors/noises mainly, the results given by IBM Quantum simulator which can be considered as ideal quantum computer is different than IBM Quantum Computer as observed in Figure 16 and 17.

As my implemented Grover quantum circuit contains 2714 number of gates(as shown in Figure 18 i.e the depth of circuit is too large for the present NISQ (Noisy Intermediate Scale Quantum Computing) era's Quantum Computer to handle efficiently and give us the desired ideal output.Fault

Error Correction Quantum Computing era is the answer to achieve a noise free system which hopefully will come in the near future due to extensive ongoing research in the field.

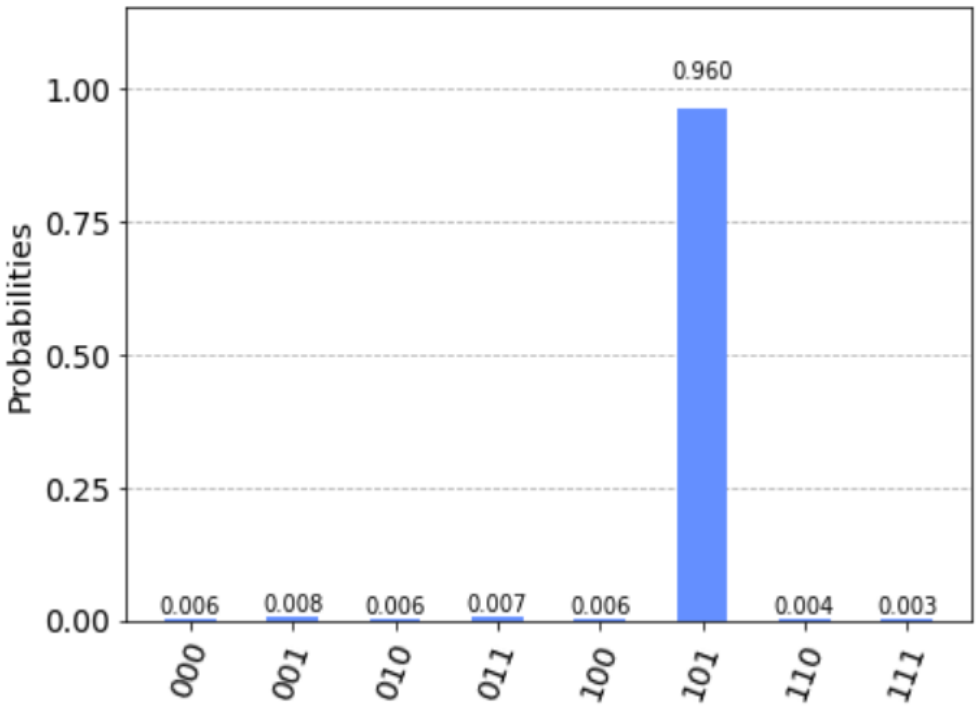

Figure 17: Results on IBM Quantum Simulator

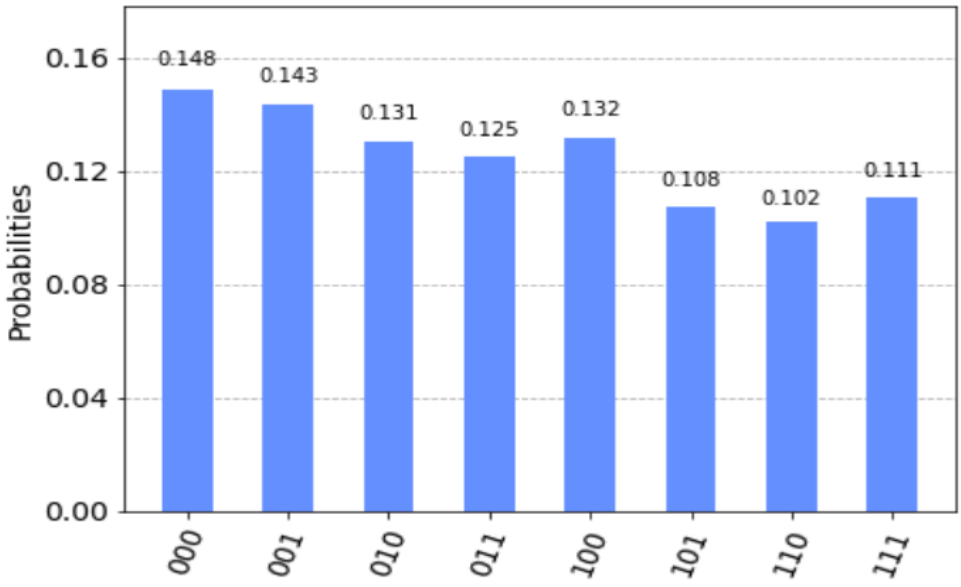

Figure 18: Results on IBM Quantum Processor

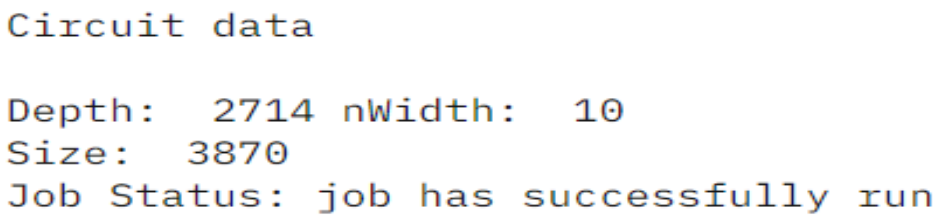

Figure 19: My implemented Grover Circuit's Depth and width

10 References

A.Youtube Videos -

1.Grover's Algorithm: Lecture 18 of Quantum Computation at CMU by Ryan O'Donnell (bit complicated to understand but a fresh perspective)

2.Quantum Search By 'Umesh Vazirani' (explained the nuances in much simpler terms with proper maths)

3.Quantum Search By 'John Preskill' (all explainations in one video)

4.'Introduction to Quantum Computing And Quantum Hardware' Lectures 6 and 7 by Qiskit.

5.Grover's Theorem Simplified by 'Sundarappan Kathiresan'.

B.Reference Books-

1.'Quantum Computing from the Ground Up' by Riley Tipton Perry

2.'Computing With Quantum Cats' from Colossus to Qubits by John Gribbin

3.'John Preskill's' Notes on Quantum Computation

4.'Quantum Computing for Computer Scientists' by Noson S. Yanofsky and Mirco A. Mannucci

5.'Quantum Computing since Democritus' by Scott Aaronson

6.'Quantum Computer Science- An Introduction' by N. David Mermin

7.'Quantum Information, Computation and Cryptography - An Introduction Survey of Theory,Technology and Experiments by Fabio Benatti,Mark Fennes,Roberto Floreanini and Dimitri Petritis

8.'Quantum Computation and Quantum Information' by Micheal A. Nelson and Isaac L.Chuang

9.Dr.Aproova Patel's Assignment's 4 and 5 (My Solutions)

10.'Quantum Computing in Practice with Qiskit and IBM Quantum Experience' by Hassi Norton (Best of the best books for Qiskit)

C.Research Papers

1.'Searching a Quantum Database with Grover's Search Algorithm by Ben Klain

2.'Optimisation of Quantum Hamiltonian Evolution: From Two Projection Operators to Local Hamiltonians'by Apoorva Patel and Anjani Priyadarsini