
ITC
Enduring Value
classmate
MARVEL
AVENGERS
© Marvel
NO TREE FROM NATURAL FOREST
FOREST SAFE
WAS CUT TO MAKE THIS NOTEBOOK

soorajss1729@gmail.com
+91-9400635788

INDEX

(10)

NAME: SOORAJ.S. STD.: SEC.: ROLL NO.: SUB.:

S. No.	Date	Title	Page No.	Teacher's Sign / Remarks
		QUANTUM COMPUTATION		
		& QUANTUM INFORMATION		
		- Nielsen & Chuang		

DYC0221907 D

6 QUANTUM SEARCH ALGORITHMS

Suppose we are given a map containing many cities, and wish to determine the shortest route passing thro' all cities on the map. A simple algorithm to find this route is to search all possible routes thro' the cities, keeping a running record of which route has the shortest length.

On a classical computer, if there are N possible routes, it takes $O(N)$ operations to determine the shortest route using this method.

There is a quantum search algorithm, sometimes known as Grover's algorithm, which enables this search method to be sped up substantially, requiring only $O(\sqrt{N})$ operations.

The Quantum Search Algorithm

(Grover's algorithm)

The oracle

Suppose we wish to search thro' a search space of N elements. Rather than search the elements directly, we concentrate on the index to those elements, which is just a number in the range 0 to $N-1$.

For convenience we assume $N = 2^n$, so the index can be stored in n bits, and that the search problem has exactly M solutions, with $1 \le M \le N$.

A particular instance of the search problem can conveniently be represented by a function f, which takes as i/p an integer x, in the range 0 to $N-1$. By definition,

$f(x) = 1$ if x is a solution to the search problem.

$f(x) = 0$ if x is not a solution to the search problem.

Suppose,

we are supplied with a quantum oracle, with the ability to recognize solutions to the search problem. This recognition is signalled by making use of an oracle qubit.

The oracle is a unitary operator O, defined by its action on the computational basis :

$$|x\rangle|q\rangle \xrightarrow{O} |x\rangle|q \oplus f(x)\rangle$$

where $|x\rangle$ is the index register

$\oplus$ denotes addition modulo 2

and the oracle qubit $|q\rangle$ is a single qubit which is flipped if $f(x) = 1$, and is unchanged otherwise.

We can check whether x is a solution to our search problem by preparing $|x\rangle|0\rangle$, applying the oracle, and checking to see if the oracle qubit has been flipped to $|1\rangle$.

In the quantum search algorithm it is useful to apply the oracle with the oracle qubit initially in the state $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$, just as was done in the Deutsch-Jozsa algorithm.

If x is not a solution to the search problem, appying the oracle to the state $|x\rangle\frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$ does not change the state.

If x is a solution to the search problem, then $|0\rangle$ and $|1\rangle$ are interchanged by the action of the oracle, giving a final state $-|x\rangle\frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$.

The action of the oracle is:

$$|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \xrightarrow{O} |x\rangle\left(\frac{|0\rangle\oplus|f(x)\rangle-|1\rangle\oplus|f(x)\rangle}{\sqrt{2}}\right)$$

$$= |x\rangle\left(\frac{|f(x)\rangle-|\overline{f(x)}\rangle}{\sqrt{2}}\right)$$

$$= (-1)^{f(x)}|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

The state of the oracle qubit is not changed, which remains $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ throughout the quantum search algorithm, and therefore be omitted from further discussion of the algorithm.

With this convention, the action of the oracle may be written:

$$|x\rangle \xrightarrow{O} (-1)^{f(x)} |x\rangle$$

$\Rightarrow$ The oracle marks the solutions to the search problem, by shifting the phase of the solution.

There is a distinction b/w knowing the solution to a search problem, and being able to recognize the solution. The crucial point is that it is possible to recognize the solution without necessarily being able to know the solution.

- For an N item search problem with M solutions, we need to only apply the search oracle $O(\sqrt{N/M})$ times in order to obtain a solution, on a quantum computer.

- There are many computational problems in which it's difficult to find a solution, but relatively easy to verify a solution.

Ex:- We can easily verify a solution to a sudoku by checking all the rules are satisfied. For these problems, we can create a function f that takes a proposed solution x, and returns $f(x)=0$ if x is not a solution $(x \neq z)$ and $f(x)=1$ for a valid solution $(x=z)$. Our oracle can then be described as:

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

and the oracle's matrix will be a diagonal matrix of the form:

$$O = \begin{bmatrix} (-1)^{f(0)} & 0 & \cdots & 0 \\ 0 & (-1)^{f(1)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & (-1)^{f(N-1)} \end{bmatrix}$$

☐ The Grover Iteration - Geometric Visualization

* Exactly 1 solution

Grover's algorithm depends on a key concept known as the Grover iteration, G. Each application of G will ask the oracle how close the current state is to a solution.

Each object is encoded in integers $1, \dots, N$, which we'll write equivalently as $0, 1, \dots, N-1$.

We do this to encode the integers in binary by $x \in \{0,1\}^n$, where $n = \log_2 N$ is integral by assumption that N is a power of 2.
So, our solution will be some bit string z, which we don't know.

We have no idea what the solution z is other than it is one of the bit strings $x \in \{0,1\}^n$. As far as we are concerned, every bit string is equally probable to be the solution. We should thus start in the equal superposition state,

$$|\phi\rangle := \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

where,

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

Since $|\phi\rangle$ is an equal superposition over all bit strings, it includes the correct bit string, say z.

$$|\phi\rangle = \frac{1}{\sqrt{2^n}} \Big(|wrong\rangle + |wrong\rangle + \cdots + |wrong\rangle + |z\rangle + |wrong\rangle + \cdots + |wrong\rangle \Big)$$

If we measure in the computational basis now, we would have merely $1/2^n$ probability of getting the correct bit string, which is very small for large n. In other words, we'd just be guessing!

We want some way to increase, or amplify, this probability. This is the goal of the Grover iteration, which achieves this in a clever way.

The overlap of the correct string $|z\rangle$ with our initial guess is exponentially small in the # of qubits n:

$$\langle z|\phi\rangle = \frac{1}{\sqrt{2^n}}$$

⇒ Geometrically, the state $|\phi\rangle$ is nearly orthogonal to $|z\rangle$. It is exactly orthogonal in the limiting case $n \to \infty$, and for all practical purposes, for large enough n we can consider them to be essentially orthogonal.

- If the two states $|\phi\rangle$ and $|z\rangle$ were exactly orthogonal, Grover's algorithm would fail.

The angle b/w $|\phi\rangle$ and the vector exactly orthogonal to $|z\rangle$ is,

$$\Delta := \frac{\pi}{2} - \cos^{-1}\frac{1}{\sqrt{2^n}} = \sin^{-1}\frac{1}{\sqrt{2^n}} \approx \frac{1}{\sqrt{2^n}}$$

where we used the small angle approximation which is valid for large n.

The Grover iteration, geometrically, consists of the following steps:

① Reflect about the correct solution $|z\rangle$.

$$R_z := 2|z\rangle\langle z| - I$$

② Reflect about the equal superposition state (initial guess) $|\phi\rangle$.

$$R_\phi := 2|\phi\rangle\langle\phi| - I$$

These 2 reflections rotate any state vector $|\psi\rangle$ closer to the correct state $|z\rangle$.

Consider the effect of the Grover iteration $G := R_\phi R_z$ on the initial state $|\phi\rangle$.

$$R_z|\phi\rangle = (2|z\rangle\langle z| - I)|\phi\rangle$$
$$= \frac{2}{\sqrt{2^n}}|z\rangle - |\phi\rangle \qquad \left(\langle z|\phi\rangle = \frac{1}{\sqrt{2^n}} \right.$$

$$R_\phi R_z|\phi\rangle = R_\phi\left(\frac{2}{\sqrt{2^n}}|z\rangle - |\phi\rangle\right)$$
$$= (2|\phi\rangle\langle\phi| - I)\left(\frac{2}{\sqrt{2^n}}|z\rangle - |\phi\rangle\right)$$
$$= \left(\frac{4}{2^n} - 1\right)|\phi\rangle - \frac{2}{\sqrt{2^n}}|z\rangle$$

tor

$$\sin \Delta = \frac{1}{\sqrt{2^n}}$$

$\therefore$

The Grover iteration $G := R_\phi R_z$ has the effect,

$$\boxed{G|\phi\rangle = \left(4\sin^2\Delta - 1\right)|\phi\rangle - 2\sin\Delta\,|z\rangle}$$

where $N := 2^n$ and n is the # of qubits.

$\Rightarrow$ the amplitude of $|z\rangle$ is increased after applying the Grover iteration.

* The probability of measuring $|z\rangle$ before the Grover iteration,

$$P = |\langle z|\Phi\rangle|^2 = \frac{1}{2^n}$$

The probability of measuring $|z\rangle$ after the Grover iteration,

$$
\begin{aligned}
P_G &= |\langle z|G|\Phi\rangle|^2 \\
&= \left|(4\sin^2\Delta - 1)\langle z|\Phi\rangle - 2\sin\Delta\langle z|z\rangle\right|^2 \\
&= \left|(4\sin^2\Delta - 1)\frac{1}{\sqrt{2^n}} - 2\sin\Delta\right|^2 \\
&= \frac{1}{2^n}\left(16\sin^4\Delta - 8\sin^2\Delta + 1\right) + 4\sin^2\Delta - \frac{4\sin\Delta}{\sqrt{2^n}}\left(4\sin^2\Delta - 1\right) \\
&= \frac{1}{2^n} + \frac{16\sin^4\Delta}{2^n} - \frac{16}{\sqrt{2^n}}\sin^3\Delta + \left(4 - \frac{8}{2^n}\right)\sin^2\Delta + \frac{4\sin\Delta}{\sqrt{2^n}} \\
&= \frac{1}{2^n} + \frac{16\sin^4\Delta}{2^n} + \left(4 - \frac{8}{2^n}\right)\sin^2\Delta - \frac{4}{\sqrt{2^n}}\sin\Delta\left(4\sin^2\Delta - 1\right) \\
&= \frac{1}{2^n} + \frac{16\sin^4\Delta}{2^n} + \left(4 - \frac{8}{2^n}\right)\sin^2\Delta + \frac{4\sin\Delta}{\sqrt{2^n}}\left(1 - 4\sin^2\Delta\right)
\end{aligned}
$$

$$\sin\Delta = \frac{1}{\sqrt{2^n}} \quad \text{and} \quad n \to \infty$$

$$4 - \frac{8}{2^n} > 0 \Rightarrow \left(4 - \frac{8}{2^n}\right)\sin^2\Delta > 0$$

$$\frac{4\sin\Delta}{\sqrt{2^n}}\left(1 - 4\sin^2\Delta\right) = \frac{4}{2^n}\left(1 - \frac{4}{2^n}\right) > 0$$

$$\Rightarrow \quad P_G = \left|\langle z|G|\phi\rangle\right|^2 > \frac{1}{2^n} = \left|\langle z|\phi\rangle\right|^2$$

* $G|\phi\rangle$ and $-G|\phi\rangle$ produce the same probability distribution and are thus the same state upto global phase.

* The angle θ b/w $|\phi\rangle$ and $-G|\phi\rangle$ is such that

$$\cos\theta = \langle\phi|(-G)|\phi\rangle = 1 - 2\sin^2\Delta = \cos 2\Delta$$

Proof.

$$-G|\phi\rangle = -(4\sin^2\Delta - 1)|\phi\rangle + 2\sin\Delta|z\rangle$$

$$\langle\phi|-G|\phi\rangle = -(4\sin^2\Delta - 1) + 2\sin\Delta\langle\phi|z\rangle$$

$$= -4\sin^2\Delta + 1 + \frac{2\sin\Delta}{\sqrt{2^n}}$$

$$\sin\Delta = \frac{1}{\sqrt{2^n}}$$

$$= -4\sin^2\Delta + 1 + 2\sin^2\Delta = \underline{\underline{1 - 2\sin^2\Delta}}$$

$\therefore$

The angle b/w $|\phi\rangle$ and $-G|\phi\rangle$ is 2Δ.

Here is the eureka! moment.

We started with a vector $|\phi\rangle$ that had angle Δ relative to $|z^\perp\rangle$. After applying the Grover iteration we ended up with a vector $-G|\phi\rangle$ which has angle 2Δ relative to $|\phi\rangle$.

$\Longrightarrow -G|\phi\rangle$ has angle 3Δ relative to $|z^\perp\rangle$

$\therefore$

The effect of the Grover iteration is to move the initial vector an angle 2Δ closer to the correct vector.

The Grover iteration G has this effect on any vector, not just $|\phi\rangle$, as long as that vector is not $|z^{\perp}\rangle$ upto global phase.

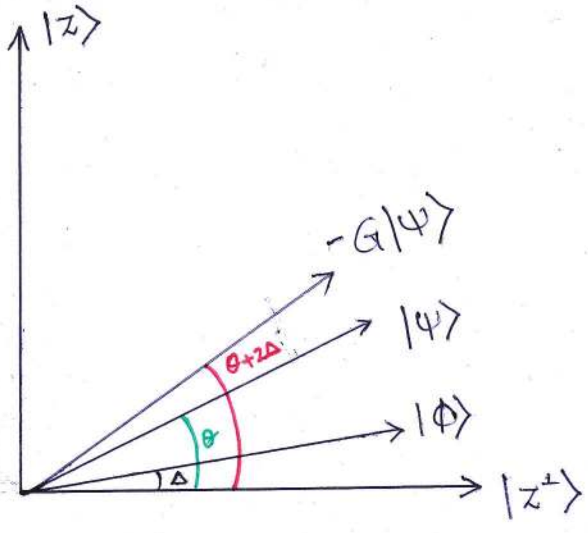
- Grover's algorithm is simply $G^k|\Phi\rangle$ for some integer k.

Effect of Grover iteration

Let $|\psi\rangle$ be any state such that $\langle z^{\perp}|\psi\rangle =: \cos\theta \neq 0$.
Then, the angle b/w $|z\rangle$ and $G|\Phi\rangle$ (modulo a global phase) is :

$$\cos^{-1}\langle z|G|\Phi\rangle = \theta + 2\Delta$$

where $\Delta := \sin^{-1}\frac{1}{\sqrt{N}} \approx \frac{1}{\sqrt{N}}$



The Quantum Complexity

Grover's algorithm is simply $G^k|\Phi\rangle$ for some integer k. The # of times we need to implement k is precisely the (oracle) complexity of the algorithm.

We want our state to be as close to the vector $|z\rangle$ as possible.

The angle b/w $G^k|\Phi\rangle$ and $|z^\perp\rangle$ (i.e., our final state after k iterations of G) is :

$$\theta_k := \Delta + 2k\Delta = (2k+1)\Delta$$

We would like this angle θ_k to be $\frac{\pi}{2} - \Delta$.

Setting $\theta_k = \frac{\pi}{2} - \Delta$,

$$(2k+1)\Delta = \frac{\pi}{2} - \Delta$$

$$\Longrightarrow \quad 2(k+1)\Delta = \pi/2$$

$$\therefore \quad \boxed{k = \frac{\pi}{4\Delta} - 1}$$

$$\Delta := \sin^{-1}\left(1/\sqrt{N}\right) \approx 1/\sqrt{N}$$

$$\boxed{k \approx \frac{\pi}{4}\sqrt{N} - 1}$$

We want k to be an integer because we're going to apply G an integer # of times.

So we round k to an integer. However, the farthest k can be from an integer is one-half.

Let θ_{k^*} be the optimal angle, and let θ_k be the angle we rotate by after rounding k^* to the closest integer k.

$$|k-k^*| \leq 1/2$$

$$|\theta_k - \theta_{k^*}| = 2|k-k^*|\Delta \leq \Delta$$

$\therefore$ The effect of rounding error is:

$$\theta_k = \theta_{k^*} \pm \Delta$$

$\Rightarrow$ We are at worst an angle Δ away from $|z\rangle$ at the end of Grover's algorithm.

Angle b/w $|z\rangle$ and $G^k|\phi\rangle$ is Δ.

For the worst case when the final angle is Δ away from optimal, the probability of success is :

$$P(\text{measure } |z\rangle) = \left|\langle z|G^k|\phi\rangle\right|^2$$

$$= \cos^2\Delta = 1 - \sin^2\Delta = 1 - \frac{1}{N}$$

The Complexity of Grover's algorithm

For large N, after

$$k := \text{round}\left(\frac{\pi}{4}\sqrt{N} - 1\right)$$

applications of the Grover's iteration $G := R_\phi R_z$ to the initial state $|\phi\rangle$, the probability of measuring the correct solution is

$$p\left(\text{measure } |z\rangle\right) = 1 - \frac{1}{N}$$

* M solutions

The equal superposition state is,

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

Let's define normalized states,

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{x}'' |x\rangle$$

$$|\beta\rangle = \frac{1}{\sqrt{M}} \sum_{x}' |x\rangle$$

where $\sum_x''$ indicates a sum over all x which are not solutions to the search problem, and $\sum_x'$ indicates a sum over all x which are solutions to the search problem.

The initial state $|\psi\rangle$ may be re-expressed as:

$$|\psi\rangle = \sqrt{\frac{N-M}{N}}\,|\alpha\rangle + \sqrt{\frac{M}{N}}\,|\beta\rangle$$

So the initial state of the quantum computer is in the space spanned by $|\alpha\rangle$ and $|\beta\rangle$.

The Grover iteration can be defined by the operator,

$$G = \left(2|\psi\rangle\langle\psi| - I\right)O$$

where the oracle operation O performs a reflection about the vector $|\alpha\rangle$ in the plane defined by $|\alpha\rangle$ and $|\beta\rangle$. That is,

$$O\left(a|\alpha\rangle + b|\beta\rangle\right) = a|\alpha\rangle - b|\beta\rangle$$

Similarly,

$2|\psi\rangle\langle\psi| - I$ also performs a reflection in the plane defined by $|\alpha\rangle$ and $|\beta\rangle$, about the vector $|\psi\rangle$.

$$Ref(\theta)\, Ref(\phi) = \begin{bmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{bmatrix} \begin{bmatrix} \cos 2\phi & \sin 2\phi \\ \sin 2\phi & -\cos 2\phi \end{bmatrix}$$

$$= \begin{bmatrix} \cos[2(\theta-\phi)] & -\sin[2(\theta-\phi)] \\ \sin[2(\theta-\phi)] & \cos[2(\theta-\phi)] \end{bmatrix} = Rot\,[2(\theta-\phi)]$$

$\Longrightarrow$ The product of two reflections is a rotation.

$\therefore$ The state $G^k|\psi\rangle$ remains in the space spanned by $|\alpha\rangle$ and $|\beta\rangle$ for all k.

Let $\cos\theta/2 = \langle\alpha|\psi\rangle = \sqrt{\frac{N-M}{N}}$

$$\Rightarrow |\psi\rangle = \cos\theta/2\,|\alpha\rangle + \sin\theta/2\,|\beta\rangle$$

$$O|\psi\rangle = \cos\theta/2\,|\alpha\rangle - \sin\theta/2\,|\beta\rangle$$

$$G|\psi\rangle = (2|\psi\rangle\langle\psi| - I)\,O|\psi\rangle$$

$\langle\psi|\alpha\rangle = \cos\theta/2$ & $\langle\psi|\beta\rangle = \sin\theta/2$

$$= (2|\psi\rangle\langle\psi| - I)(\cos\theta/2\,|\alpha\rangle - \sin\theta/2\,|\beta\rangle)$$

$$= 2\cos^2\theta/2\,|\psi\rangle - 2\sin^2\theta/2\,|\psi\rangle - \cos\theta/2\,|\alpha\rangle + \sin\theta/2\,|\beta\rangle$$

$$= 2\cos\theta\,|\psi\rangle - \cos\theta/2\,|\alpha\rangle + \sin\theta/2\,|\beta\rangle$$

$$= 2\cos\theta\cos\theta/2\,|\alpha\rangle + 2\cos\theta\sin\theta/2\,|\beta\rangle - \cos\theta/2\,|\alpha\rangle + \sin\theta/2\,|\beta\rangle$$

$$= \cos\theta/2\left(2\cos\theta - 1\right)|\alpha\rangle + \sin\theta/2\left(2\cos\theta + 1\right)|\beta\rangle$$

$$= \cos\theta/2\left(4\cos^2\tfrac{\theta}{2} - 3\right)|\alpha\rangle + \sin\theta/2\left(-4\sin^2\tfrac{\theta}{2} + 3\right)|\beta\rangle$$

$$= \left(4\cos^3\theta/2 - 3\cos\theta/2\right)|\alpha\rangle + \left(3\sin\theta/2 - 4\sin^3\theta/2\right)|\beta\rangle$$

$$\sin 3x = 3\sin x - 4\sin^3 x$$

$$\cos 3x = 4\cos^3 x - 3\cos x$$

$$G|\psi\rangle = \cos\frac{3\theta}{2}|\alpha\rangle + \sin\frac{3\theta}{2}|\beta\rangle$$

$\Longrightarrow$ The rotation angle is in fact θ.

The continued application of G takes the state to,

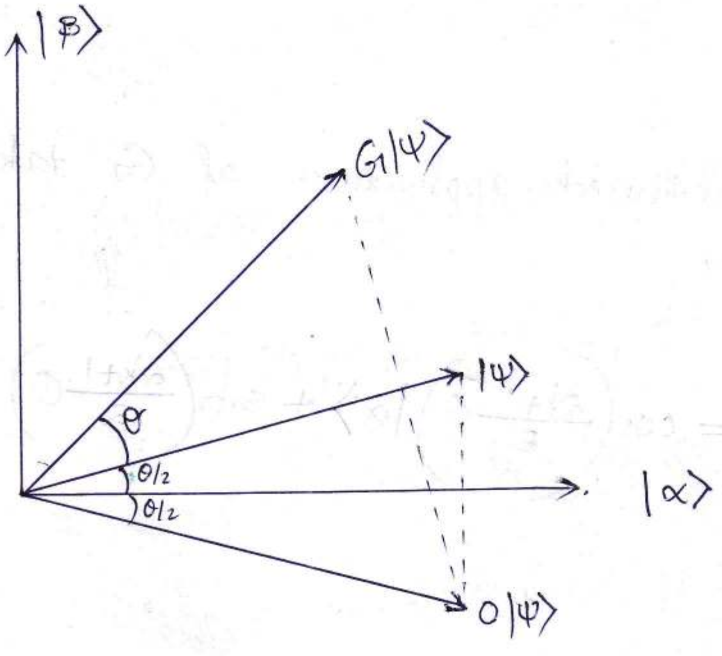
$$G^k|\psi\rangle = \cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle$$

$\therefore$

G is a rotation in the 2D space spanned by $|\alpha\rangle$ and $|\beta\rangle$, rotating the space by θ radians per application of G.

Repeated application of the Grover iteration rotates the state vector close to $|\beta\rangle$.

When this occurs, an observation in the computational basis produces with high probability one of the outcomes superposed in $|\beta\rangle$, that is, a solution to the search problem!



nned

by

ation

the

sed

* In the $|\alpha\rangle, |\beta\rangle$ basis the Grover iteration can be written as,

$$G = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

where θ is a real # in the range 0 to $\pi/2$ (assuming for simplicity that $M \le N/2$; this limitation will be lifted shortly), chosen so that

$$\sin\theta = \frac{2\sqrt{M(N-M)}}{N}$$

$$\cos\theta/2 = \langle\alpha|\psi\rangle = \sqrt{\frac{N-M}{N}}$$

$$\Rightarrow \sin\theta/2 = \sqrt{1 - \frac{N-M}{N}} = \sqrt{\frac{M}{N}}$$

$$\sin\theta = 2\sin\theta/2 \cos\theta/2 = 2 * \sqrt{\frac{M}{N}}\sqrt{\frac{N-M}{N}} = \frac{2\sqrt{M(N-M)}}{N}$$

Assuming that $M \le N/2 \Rightarrow \frac{M}{N} \le 1/2 \Rightarrow \sin\theta/2 \le 1/\sqrt{2}$.

$$\Rightarrow \theta/2 \le \pi/4 \Rightarrow \underline{\underline{\theta \le \frac{\pi}{2}}}$$

Performance

How many times must the Grover iteration be repeated in order to rotate $|\psi\rangle$ near $|\beta\rangle$?

The initial state of the system is,

$$|\psi\rangle = \sqrt{\frac{N-M}{N}}\,|\alpha\rangle + \sqrt{\frac{M}{N}}\,|\beta\rangle$$

$$= \cos \theta/2\,|\alpha\rangle + \sin \theta/2\,|\beta\rangle$$

$$\frac{\pi}{2} - \frac{\theta}{2} = \frac{\pi}{2} - \sin^{-1}\sqrt{M/N} = \cos^{-1}\sqrt{M/N}$$

$\therefore$ Rotating thro' $\arccos\sqrt{M/N}$ radians takes the system to $|\beta\rangle$.

Let $CI(x)$ denote the integer closest to the real number x, where by convention we round halves down; Example : $CI(3.5) = 3$.

$$\sin\theta/2 = \sqrt{M/N} \leq 1/\sqrt{2} \implies \theta/2 \leq \pi/4 .$$

$$\boxed{|x - CI(x)| \leq 1/2 \Rightarrow \text{angle}, \delta \leq \theta/2 \leq \pi/4}$$

$\therefore$ Repeating the Grover iteration

$$\boxed{R = CI\left(\frac{\arccos\sqrt{M/N}}{\theta}\right)}$$

times rotates $|\psi\rangle$ to within an angle $\theta/2 \leq \pi/4$ of $|\beta\rangle$.

$$\theta/2 \le \pi/4 \implies \cos\theta/2 \ge 1/\sqrt{2}$$

$$\boxed{P(\text{measure } |\beta\rangle) \ge \cos^2(\theta/2) = 1 - \sin^2\theta/2 \ge \frac{1}{2} \\ = 1 - \frac{M}{N}}$$

$\therefore$

Observation of the state in the computational basis then yields a solution to the search problem with probability at least $1/2$.

For specific values of M and N it is possible to achieve a much higher probability of success.

For example,

when $M \leq N$

$$\theta \approx \sin\theta = \frac{2\sqrt{M(N-M)}}{N} \approx 2\sqrt{\frac{M}{N}}$$

The angular error in the final state is at most $\frac{\theta}{2} \approx \sqrt{\frac{M}{N}}$,

giving a probability of error of at most M/N

$$R = CI\left(\frac{\arccos\sqrt{M/N}}{\theta}\right)$$

Note that,

R depends on the # of solutions M but not on the identity of those solutions, so provided we know M we can apply the quantum search algorithm.

We can even remove the need for a knowledge of M in applying the search algorithm, which will be explained in the section 6.3- Quantum Counting.

$$R = CI\left(\frac{\arccos\sqrt{M/N}}{\theta}\right) \quad — (6.15)$$

The form (6.15) is useful as an exact expression for the # of oracle calls used to perform the quantum search algorithm, but it coould be useful to have a simpler expression summarizing the essential behavior of R.

The ceiling function maps x to the least integer greater than or equal to x, denoted $\lceil x \rceil$ or ceil(x).

Ex:- $\lceil 2.4 \rceil = 3$, $\lceil -2.4 \rceil = -2$

$$\frac{\pi}{2} - \frac{\theta}{2} = \frac{\pi}{2} - \sin^{-1}\sqrt{M/N} = \cos^{-1}\sqrt{M/N}$$

$$\Longrightarrow \cos^{-1}\sqrt{M/N} \leq \pi/2$$

$$\therefore R = CI\left(\frac{\arccos\sqrt{M/N}}{\theta}\right) \leq \left\lceil \frac{\pi/2}{\theta} \right\rceil$$

$$\Longrightarrow R \leq \left\lceil \frac{\pi}{2\theta} \right\rceil$$

So a lower bound on θ will give an upper bound on R.

$f(x) = \sin x - x$, $0 \leq x \leq \pi/2$.

$$f'(x) = \cos x - 1 \Longrightarrow \begin{array}{l} f'(0) = 1-1 = 0 \\ f'(\pi/2) = 0-1 = -1 \end{array}$$

$f''(x) = -\sin x < 0$ $\Big\}$ $f(x)$ is a decreasing funtion. in $[0,\pi/2]$.

$$\left.\begin{array}{l} f(0) = 0 \\ f(\pi/2) = 1-\pi/2 < 0 \end{array}\right\}. \quad f(x) = \sin x - x \leq 0$$

$$\underline{\underline{\sin x \leq x}} \Longrightarrow \frac{\sin x}{x} \leq 1$$

Lemma

Assume that $M \leq N/2$,

$$\sqrt{\frac{M}{N}} \leq 1/\sqrt{2} \Rightarrow \sin\theta/2 \leq 1/\sqrt{2}$$

$$\frac{\theta}{2} \leq \pi/4 \Rightarrow \theta \leq \pi/2.$$

Lemma $\Rightarrow$ $\frac{\theta}{2} \geq \sin\frac{\theta}{2} = \sqrt{M/N}$

$$\Rightarrow \underline{\theta \geq 2\sqrt{M/N}}$$

from which we obtain an elegant upper bound on the # of iterations required,

$$R \leq \left\lceil \frac{\pi}{4}\sqrt{N/M} \right\rceil$$

$\Rightarrow$ $R = O(\sqrt{N/M})$ Grover iterations (and thus oracle calls) must be performed in order to obtain a solution to the search problem with high probability, a quadratic improvement over the $O(N/M)$ oracle calls required classically.

The Procedure

The algorithm makes use of a single n qubit register.

The goal of the algorithm is to find a solution to the search problem, using the smallest possible # of applications of the oracle.

The oracle is a unitary operator O, defined by its action on the computational basis:

$$|x\rangle|q\rangle \xrightarrow{O} |x\rangle|q \oplus f(x)\rangle$$

where, $|q\rangle$: oracle qubit, which is flipped if $f(x) = 1$, and is unchanged otherwise.

The function f takes as input an integer x, in the range 0 to $N-1$ such that

$f(x) = 1$ if x is a solution to the search problem.

$f(x) = 0$ if x is not a solution to the search problem.

The action of the oracle is,

$$|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \xrightarrow{O} |x\rangle\left(\frac{|0\rangle\oplus|f(x)\rangle-|1\rangle\oplus|f(x)\rangle}{\sqrt{2}}\right)$$

$$= |x\rangle\left(\frac{|f(x)\rangle-|\overline{f(x)}\rangle}{\sqrt{2}}\right)$$

$$= (-1)^{f(x)}|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

The state of the oracle qubit remains $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ throughout the quantum search algorithm, & therefore be omitted from further discussions.

with this convention, the action of the oracle may be written as:

$$|x\rangle \xrightarrow{O} (-1)^{f(x)}|x\rangle$$

$\Rightarrow$ The oracle marks the solutions to the search problem, by shifting the phase of the solution.

The algorithm begins with the computer in the state $|0\rangle^{\otimes n}$. The Hadamard transform is used to put the computer in the equal superposition state,

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

which can be reexpressed as,

$$|\psi\rangle = \sqrt{\frac{N-M}{N}}\,|\alpha\rangle + \sqrt{\frac{M}{N}}\,|\beta\rangle$$

where, $$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{x}'' |x\rangle$$

$$|\beta\rangle = \frac{1}{\sqrt{M}} \sum_{x}' |x\rangle$$

and $\sum_{x}'$ indicates a sum over all x which are solutions to the search problem, and $\sum_{x}''$ indicates a sum over all x which are not solutions to the search problem.

So the initial state of the quantum computer is in the space spanned by $|\alpha\rangle$ and $|\beta\rangle$.

The quantum search algorithm consists of repeated application of a quantum sub routine, known as the Grover iteration or Grover iteration, G.

$$G = \left(2|\psi\rangle\langle\psi| - I\right) O$$

$$= H^{\otimes n}\left(2|0\rangle\langle 0| - I\right) H^{\otimes n} O$$

where, the oracle operation O performs a reflection about the vector $|\alpha\rangle$ in the plane defined by $|\alpha\rangle$ and $|\beta\rangle$.

i.e, $O\left(a|\alpha\rangle + b|\beta\rangle\right) = a|\alpha\rangle - b|\beta\rangle$

$2|\psi\rangle\langle\psi| - I$ also performs a reflection in the plane defined by $|\alpha\rangle$ and $|\beta\rangle$, about the vector $|\psi\rangle$.

---

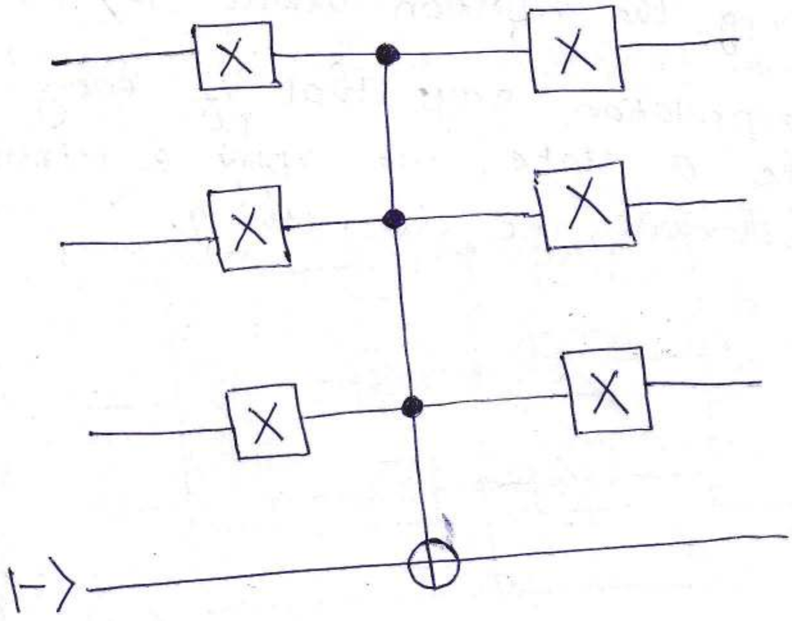
* The Householder matrix for a reflection about the hyperplane $\perp$ to a unit vector $\hat{u}$ is:

$$H = I - 2\hat{u}\hat{u}^{\dagger}$$

The key insight to implementing G is actually the intuitive interpretation of reflections:

Do nothing to the ‖el component, and add a minus sign to the ⊥r component.

Fig:- A quantum circuit that implements a reflection about $|0\rangle^{\otimes n}$, ie, the unitary $R_0 := I - 2|0\rangle\langle 0|$. Here $n=3$, ~~and~~ a single ancilla in the $|-\rangle$ state is utilized for any n. The multicontrolled Toffoli gate can be constructed from standard Toffoli gates.



Considering the reflection about $|0\rangle^{\otimes n}$.

The interpretation says that if every qubit is in the 0 state, we apply a minus sign. Otherwise, we do nothing.

We can modify the reflection about $|0\rangle$, to reflect about any state $|v\rangle$.

$$R_v := I - 2|v\rangle\langle v| = I - 2V|0\rangle\langle 0|V^\dagger$$

where V is a unitary operator which prepares $|v\rangle$ from the ground state. i.e., $V|0\rangle = |v\rangle$.

Fig:- A quantum circuit for performing the reflection $R_v = I - 2|v\rangle\langle v|$ where $|v\rangle = V|0\rangle$

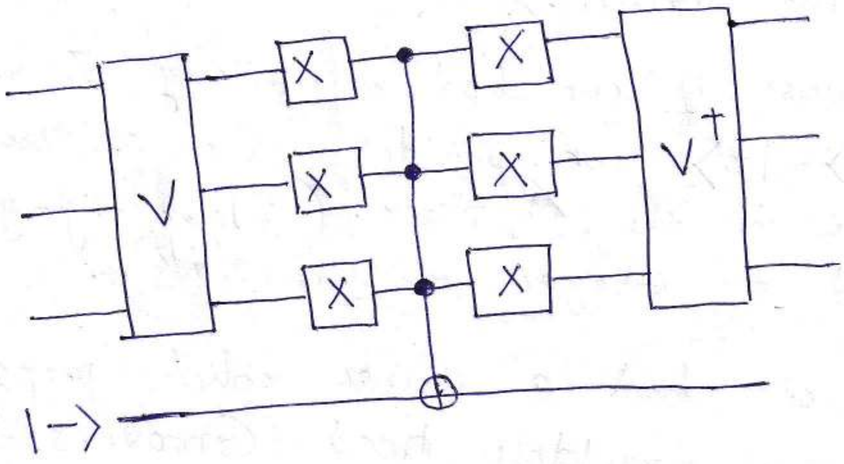
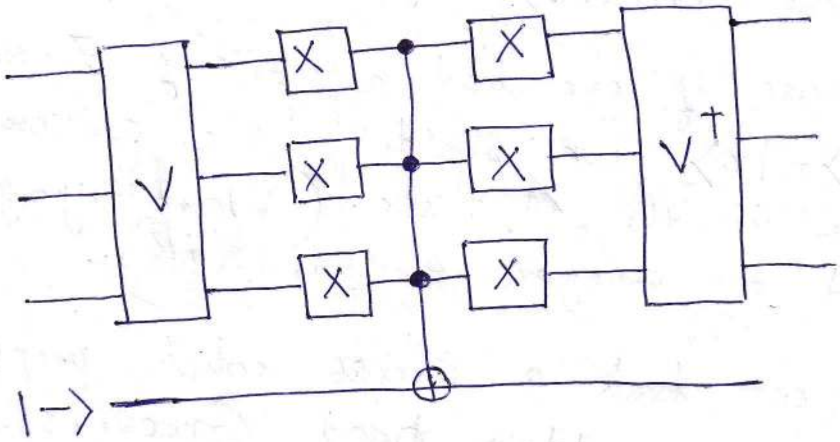


Fig:- A quantum circuit for performing the reflection $R_v := I - 2|v\rangle\langle v|$ where $|v\rangle = V|0\rangle$



We can not implement the reflection about the solution state $|z\rangle$ in the same manner as in the circuit.

Because, if we had a unitary Z such that $Z|0\rangle = |z\rangle$, we wouldn't have a problem to solve in the 1st place. (We're trying to find an integer $z \in \{1, 2, \dots, N\}$).

If we had a circuit which prepared $|z\rangle$, we wouldn't need Grover's algorithm!

All we are allowed is the Quantum oracle which acts on a state of $n = \log N$ qubits and sets an ancilla qubit to be $|1\rangle$ if the register is a solution to the search problem. This is precisely what we want to implement the reflection about $|z\rangle$.

We simply act with the oracle O on the i/p register and ancilla to perform the reflection, $R_z = I - 2|z\rangle\langle z|$.

The Grover iteration G may be brocken up into 4 steps:

① Apply the Oracle O

② Apply the Hadamard transfoom $H^{\otimes n}$

③ Perform a conditional phase shift on the computer, with every computational Basis except $|0\rangle$, receiving a phase shift of -1.

$$|x\rangle \longrightarrow -(-1)^{\delta_{x0}} |x\rangle$$

④ Apply the Hadamard transform $H^{\otimes n}$

- The unitary operator corresponding to the phase shift in the Grover iteration is $2|0\rangle\langle 0| - I$.

Each of the operations in the Grover iteration may be efficiently implemented on a quantum computer.

The Grover iteration requires only a single oracle call. The combined effect of steps 2, 3 and 4 is:

$$H^{\otimes n}\left(2|0\rangle\langle 0|-I\right)H^{\otimes n} = 2|\psi\rangle\langle\psi| - I$$

where $|\psi\rangle$ is the equally weighted superposition of states. Thus the Grover iteration G may be written, $G = \left(2|\psi\rangle\langle\psi|-I\right)O$.

gle
steps

position
G

Ex: 6.2 Show that the operation $(2|\psi\rangle\langle\psi| - I)$ applied to a general state $\sum_k \alpha_k |k\rangle$

produces

$$\sum_k \left[-\alpha_k + 2\langle\alpha\rangle\right]|k\rangle$$

where $\langle\alpha\rangle = \sum_k \frac{\alpha_k}{N}$ is the mean value of the α_k. For this reason, $(2|\psi\rangle\langle\psi| - I)$ is sometimes referred to as the inversion about mean operation.

Algorithm : Quantum Search

Inputs : ① A black box oracle O which performs the transformation, $O|x\rangle|q\rangle = |x\rangle|q \oplus f(x)\rangle$ where $f(x) = 0$ for all $0 \le x < 2^n$ except x_0, for which $f(x_0) = 1$

② $n+1$ qubits in the state $|0\rangle$

Outputs : x_0

Runtime : $O(\sqrt{2^n})$ operations. Succeeds with probability $O(1)$.

Procedure :

① $|0\rangle^{\otimes n}|0\rangle$ — initial state

② $\rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$ — apply $H^{\otimes n}$ to the 1st n qubits, and HX to the last qubit.

③ $\left[(2|\psi\rangle\langle\psi| - I)O\right]^R \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$ — apply the Grover iteration $R \approx \frac{\pi\sqrt{2^n}}{4}$ times.

$\approx |x_0\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$

④ $\longrightarrow x_0$ — measure the 1st n qubits.

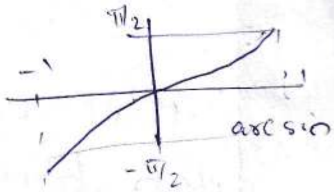
What happens when more than half the items are solutions to the search problem, i.e., $M \geq N/2$?

$$\sin \theta/_2 = \sqrt{\frac{N-M}{N}} \quad \& \quad \cos \theta/_2 = \sqrt{\frac{M}{N}}$$

$$\sin\theta = 2\sin\theta/_2 \cos\theta/_2$$

$$= 2 * \sqrt{\frac{N-M}{N}} * \sqrt{\frac{M}{N}} = \frac{2\sqrt{M(N-M)}}{N}$$

$$\Longrightarrow \quad \theta = \arcsin\left(\frac{2\sqrt{M(N-M)}}{N}\right)$$



$M = N/2$: $\theta = \sin^{-1}(1) = \pi/2$

$M = N$: $\theta = \sin^{-1}(0) = 0$

$\Rightarrow$ The angle θ gets smaller as M varies from $N/2$ to N. As a result, the # of iterations needed by the search algorithm increases with M, for $M \geq N/2$.

Intuitively, this is a silly property for a search algorithm to have: we expect that it should become easier to find a solution to the problem as the # of solutions increases.

(ii) If M is known in advance to be larger than $N/2$.

then we can just randomly pick an item from the search space, and then check that it is a solution using the oracle. This approach has a success probability at least $1/2$, and only requires one consultation with the oracle.

It has the disadvantage that we may not know the # of solutions M in advance.

Intuitively, this is a silly property for a search algorithm to have: We expect that it should become easier to find a solution to the problem as the # of solutions increases.

(i) If M is known in advance to be larger than $N/2$.

then we can just randomly pick an item from the search space, and then check that it is a solution using the oracle. This approach has a success probability at least $1/2$, and only requires one consultation with the oracle.

It has the disadvantage that we may not know the # of solutions M in advance.

(ii) If it isn't known whether $M \geq N/2$

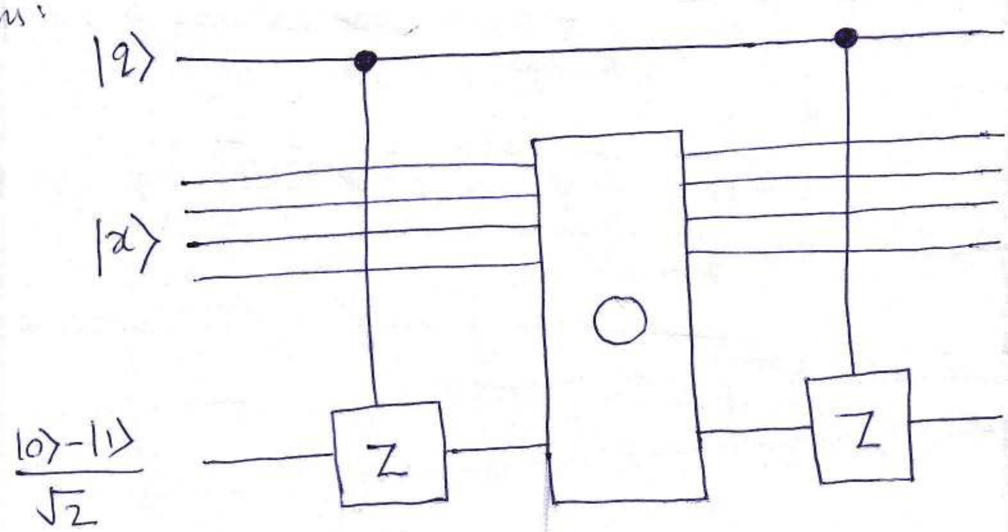
The idea is to double the # of elements in the search space by adding N extra items to the search space, none of which are solutions. This is effected by adding a single qubit $|q\rangle$ to the search index, doubling the # of items to be searched to $2N$.

A new augmented oracle O' is constructed which marks an item only if it is a solution to the search problem and the extra bit is set to zero. The new search problem has only M solutions out of $2N$ entries. So running the search algorithm with the new oracle O', at most $R = \frac{\pi}{4}\sqrt{\frac{2N}{M}}$ calls to O' are required, and it follows that $\Theta\left(\sqrt{N/M}\right)$ calls to 0 are required to perform the search.

search.

Ex: 6.5 Show that the augmented oracle O' may be constructed using one application of O, and elementary quantum gates, using the extra qubit $|q\rangle$.

Ans:



Z gate (Phase flip matrix)

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$$

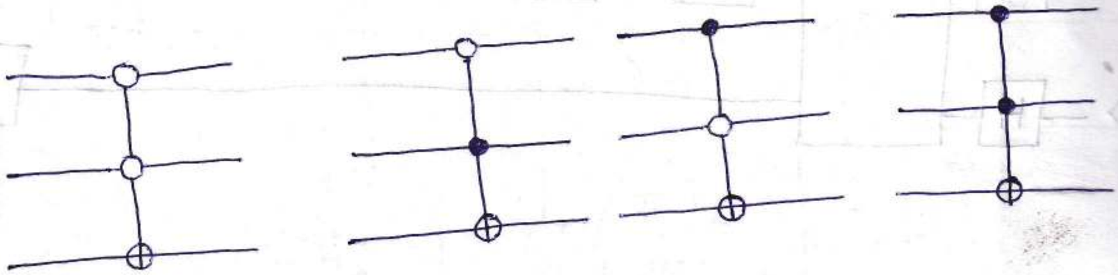
$$\left[\begin{aligned} Z|0\rangle &= |0\rangle \\ Z|1\rangle &= -|1\rangle \end{aligned}\right.$$

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

Quantum Search → a two-bit example

Search space size, $N = 4$

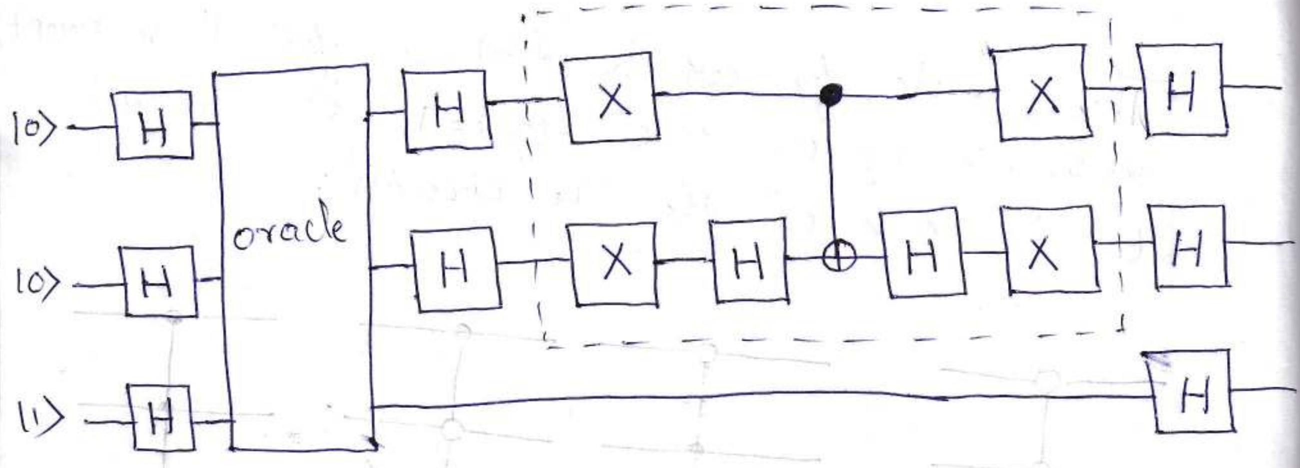
The oracle, for which $f(x) = 0$ for all x except $x = x_0$, in which case $f(x_0) = 1$, can be taken to be one of the 4 circuits:



corresp. to $x_0 = 0, 1, 2,$ or 3 from left to right, where the ~~top~~ two qubits carry the query x, and the bottom qubit carries the oracle's response.

We need to identify which one among the four.

The quantum circuit which performs the initial Hadamard transforms & a single Grover iteration G is :



The gates in the dotted box perform the conditional phase shift operation $2|00\rangle\langle 00| - I$.

How many times must we repeat G to obtain x_0 ?

$$R = CI\left(\frac{\arccos\sqrt{M/N}}{\theta}\right)$$

Repeating Grover iteration R number of times rotates $|\psi\rangle$ to within an angle $\theta/2 \le \pi/4$ of $|\beta\rangle$, the superposition of all solutions to the search problem.

$M = 1,\ N = 4$

$$R = CI\left(\frac{\arccos 1/2}{\theta}\right) = CI\left(\frac{\pi}{3\theta}\right)$$

$$= CI(1) = 1$$

$$\sin\theta = \frac{2\sqrt{M(N-M)}}{N} = \frac{2\sqrt{3}}{4} = \sqrt{3}/2 \implies \theta = \pi/3$$

$\rightarrow$ Only exactly one iteration is required to perfectly obtain x_0.

In the geometric picture, our initial state $|\psi\rangle = \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)$ is 30° from $|\alpha\rangle$, and a single rotation by $\theta = 60^\circ$ moves $|\psi\rangle$ to $|\beta\rangle$.

Measurement of the top two qubits gives x_0, after using the oracle only once.

In contrast, a classical computer - or classical circuit - try to differentiate b/w the 4 oracles would require on average 2.25 oracle queries!

Quantum Counting

How quickly can we determine the # of solutions, M, to an N item search problem, if M is not known in advance ?

On a classical computer it takes $\Theta(N)$ consultation with an oracle to determine M.

On a quantum computer it is possible to estimate the # of solutions much more quickly than is possible on a classical computer by combining the Grover iteration with the phase estimation technique based upon the quantum Fourier transform.

This has some important applications :

(1st) If we can estimate the # of solutions quickly then it is also possible to find a solution quickly, even if the # of solutions is unknown, by 1st counting the # of solutions, and then applying the quantum search algorithm to find a solution.

(2nd) Quantum counting allows us to decide whether or not a solution even exists, depending on whether the # of solutions is zero, or non-zero.

pending
or

Ex: 6.13 Consider a classical algorithm for the counting problem which samples uniformly and independently, k times from the search space; and let $X_1, \ldots, X_k$ be the results of the oracle calls, that is, $X_j = 1$ if the j^{th} oracle call revealed a solution to the problem, and $X_j = 0$ if the j^{th} oracle call did not reveal a solution to the problem. This algorithm returns the estimate $S = N \times \sum_j X_j/k$ for the # of solutions to the search problem. Show that the standard deviation in S is $\Delta S = \sqrt{M(N-M)/k}$. Prove that to obtain a probability at least $3/4$ of estimating M correctly in within an accuracy $\sqrt{M}$ for all values of M we must have $k = \Omega(N)$.

Ans: S: estimate of the # of solutions to the search problem obtained

$$Var(s) = E[s^2] - \left(E[s]\right)^2$$

$$E(S) = E\left(N \times \sum_j \frac{X_j}{k}\right)$$

$$= \frac{N}{k} E\left(\sum_j X_j\right)$$

$$= \frac{N}{k} \sum_j E(X_j)$$

$$= \frac{N}{k} \sum_j \frac{M}{N}$$

$$= \frac{N}{k} \times \frac{kM}{N} = M$$

Binomial trial & each done independently.

$$E(X_j) = 1 \times P(X_j = 1) + 0 \times P(X_j = 0)$$
$$= P(X_j = 1) = M/N$$

$\therefore$

s is an unbiased estimator of M.

where we have used:

① For a random variable X with a finite list $x_1, \dots, x_k$ of possible outcomes, each of which (respectively) has probability $p_1, \dots, p_k$ of occurring. The expectation value of X is defined as:

$$E[X] = x_1 p_1 + \dots + x_k p_k = \sum_{j=1}^{k} x_j p_j$$

which can be interpreted as a weighted average of the x_j value, with weights given by their probabilities p_j.

② For any random variables X and Y, and a constant 'a', we have

$$E(X+Y) = E(X) + E(Y)$$

$$E(aX) = aE(X)$$

③ The expected value of a Binomial distribution is np.

Proof

II $P(X=k) = \binom{n}{k} p^k (1-p)^{n-k}$

$$E[X] = \sum_{k=0}^{n} k\, P(X=k)$$

$$= \sum_{k=0}^{n} k \binom{n}{k} p^k (1-p)^{n-k}$$

$$= \sum_{k=1}^{n} k \frac{n!}{(n-k)!\, k!} p^k (1-p)^{n-k}$$

Factoring out np,

$$= np \sum_{k=1}^{n} \frac{(n-1)!}{(n-k)!\,(k-1)!} \times p^{k-1} (1-p)^{n-k}$$

$$= np \sum_{k=1}^{n} \binom{n-1}{k-1} p^{k-1} (1-p)^{n-k}$$

$$= np \sum_{k-1=0}^{n-1} \binom{n-1}{k-1} p^{k-1} (1-p)^{n-k}$$

$$= np \sum_{j=0}^{m} \binom{m}{j} p^j (1-p)^{m-j} = np$$

where, $j = k-1 \Rightarrow k: 1 \to n \Rightarrow j: 0 \to m$

$m = n-1$

$$(x+y)^m = \sum_{j=0}^{m} \binom{m}{j} x^j y^{m-j}$$

$$\Rightarrow (p+(1-p))^m = 1 = \sum_{j=0}^{m} \binom{m}{j} p^j (1-p)^{m-j}$$

$\boxed{2}$ Let $B_i = 1$ if we have a success on the ith trial, and 0 otherwise.

Then the number X of successes is:

$$X = B_1 + B_2 + \cdots + B_n.$$

By the linearity of expectation,

$$E(X) = E(B_1 + B_2 + \cdots + B_n) = E(B_1) + E(B_2) + \cdots + E(B_n)$$

$$E(B_i) = 1 \times P + 0 \times (1-P) = P$$

$$\Rightarrow E(X) = \underbrace{P + P + \cdots + P}_{n \text{ times}} = \underline{\underline{nP}}$$

$$E(s^2) = E\left[\left(N \times \sum_{j=1}^{k} \frac{X_j}{k}\right)^2\right]$$

$$= \frac{N^2}{k^2} E\left(\sum_{j=1}^{k} X_j\right)^2$$

$$= \frac{N^2}{k^2} E\left(\sum_{i=1}^{k} X_i \times \sum_{j=1}^{k} X_j\right)$$

$$= \frac{N^2}{k^2} E\left(\sum_{i=1}^{k} \sum_{j=1}^{k} X_i X_j\right)$$

$$= \frac{N^2}{k^2} \sum_{i=1}^{k} \sum_{j=1}^{k} E\left(X_i X_j\right)$$

case 1 : $i = j$

$$E(X_i X_i) = E(X_i^2) = 1^2 \times P(X_i = 1) + 0 \times P(X_i = 0)$$

$$= P(X_i = 1)$$

$$= \frac{M}{N}$$

Case 2: $i \neq j$

$$E(X_i X_j) = 1 \times 1 \times P(X_i = 1, X_j = 1) + 1 \times 0 \times P(X_i = 1, X_j = 0)$$
$$+ 0 \times 1 \times P(X_i = 0, X_j = 1) + 0 \times 0 \times P(X_i = 0, X_j = 0)$$

$$= P(X_i = 1, X_j = 1)$$

$$= P(X_i = 1) P(X_j = 1)$$

$$= \frac{M}{N} \times \frac{M}{N} = \frac{M^2}{N^2}$$

Case 1 happens k times $\Rightarrow$ case 2 must happen $k^2 - k$ times.

$\therefore$

$$E(S^2) = \frac{N^2}{k^2} \sum_{i=1}^{k} \sum_{j=1}^{k} E(X_i X_j)$$

$$= \frac{N^2}{k^2} \left[k \frac{M}{N} + (k^2 - k) \frac{M^2}{N^2} \right]$$

$$= \frac{MN}{k} + M^2 - \frac{M^2}{k}$$

$$Var(S) = E(S^2) - (E(S))^2$$

$$= \frac{MN}{k} + \cancel{M^2} - \frac{M^2}{k} - \cancel{M^2}$$

$$= \frac{M(N-M)}{k}$$

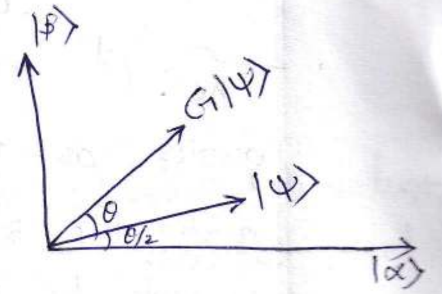
$$s.d(S) = \Delta S = \sqrt{M(N-M)/k}$$

Quantum Counting

Quantum counting is an application of the phase estimation procedure to estimate the eigenvalues of the Grover iteration, G, which in turn enables us to determine the # of solutions M to the search problem.

In the $|\alpha\rangle, |\beta\rangle$ basis :

$$G = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$



Suppose $|a\rangle$ and $|b\rangle$ are the two eigenvectors of the Grover iteration in the space spanned by $|\alpha\rangle$ and $|\beta\rangle$.

Let θ be the angle of rotation determined by the Grover iteration.

The corresponding eigenvalues are $e^{i\theta}$ and $e^{i(2\pi-\theta)}$.

For ease of analysis it is convenient to assume that the oracle has been augmented, expanding the size of the search space to $2N$ and ensuring that $\sin^2 \theta/2 = M/2N$.

The function of the phase estimation circuit used for quantum counting is to estimate θ to m bits of accuracy, with a probability of success at least $1-\epsilon$.
The 1^{st} register contains $t = m + \log_2\left(2 + \frac{1}{2\epsilon}\right)$ qubits, as per the phase estimation algorithm, and the 2^{nd} register contains $n+1$ qubits, enough to implement the Grover iteration on the augmented search space.

$N = 2^n \implies 2N = 2^{n+1}$

The state of the 2^{nd} register is initialized to an equal superposition of all possible inputs $\sum_x |x\rangle$ By a Hadamard transform.

This state is a superposition of the eigenstates $|a\rangle$ and $|b\rangle$.

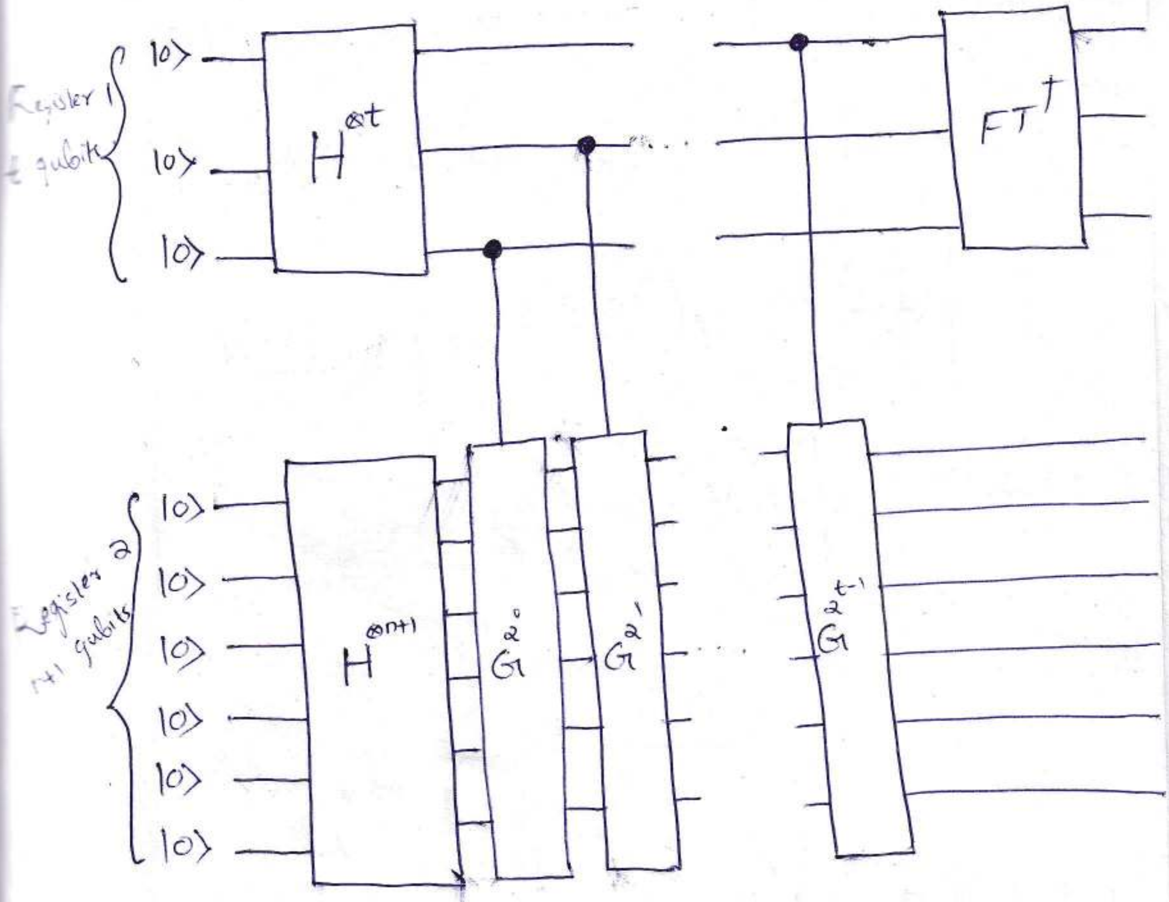
So the phase estimation circuit gives us an estimate of θ or $2\pi-\theta$ accurate to within $|\Delta\theta| \leq 2^{-m}$, with probability at least $1-\epsilon$.

Furthermore,

an estimate for $2\pi-\theta$ is clearly equivalent to an estimate of θ with the same level of accuracy, so effectively the phase estimation algorithm determines θ to an accuracy 2^{-m} with probability $1-\epsilon$.

$\therefore$ Using the equation $\sin^2 \theta/2 = M/2N$ and our estimate for θ, we obtain an estimate of the # of solutions, M.

nd
mate



* Circuit for performing approximate quantum counting on a quantum computer.

— How large an error, ΔM, is there in the estimate ?

$$\sin^2(\theta/2) = M/2N$$

$$\frac{|\Delta M|}{2N} = \left| \sin^2\left(\frac{\theta+\Delta\theta}{2}\right) - \sin^2(\theta/2) \right|$$

$$= \left(\sin\left(\frac{\theta+\Delta\theta}{2}\right) + \sin\theta/2\right) \left|\sin\left(\frac{\theta+\Delta\theta}{2}\right) - \sin(\theta/2)\right|$$

$$\frac{dy}{dx} = \lim_{\Delta x \to 0} \frac{f(x+\Delta x) - f(x)}{\Delta x}$$

$$\frac{d}{d\theta}\sin\theta/2 = \cos\theta/2 = \lim_{\Delta\theta/2 \to 0} \frac{\sin\left(\frac{\theta+\Delta\theta}{2}\right) - \sin(\theta/2)}{\Delta\theta/2} \leq 1$$

Calculus $\Longrightarrow \left|\sin\left(\frac{\theta+\Delta\theta}{2}\right) - \sin(\theta/2)\right| \leq |\Delta\theta|/2$

$$|a| - |b| \leq |a - b|$$

$$\left|\sin\left(\frac{\theta+\Delta\theta}{2}\right)\right| - \left|\sin\left(\theta/2\right)\right| \leq \left|\sin\left(\frac{\theta+\Delta\theta}{2}\right) - \sin\left(\theta/2\right)\right|$$

$$\sin\theta/2 = \sqrt{M/2N} > 0$$

$$\left|\sin\left(\frac{\theta+\Delta\theta}{2}\right)\right| - \sin\theta/2 \leq \left|\sin\left(\frac{\theta+\Delta\theta}{2}\right) - \sin\left(\theta/2\right)\right| \leq |\Delta\theta|/2$$

$$\Longrightarrow \left|\sin\left(\frac{\theta+\Delta\theta}{2}\right)\right| < \sin\left(\theta/2\right) + |\Delta\theta|/2$$

$$\therefore \quad \sin\left(\frac{\theta+\Delta\theta}{2}\right) + \sin\left(\theta/2\right) < 2\sin\theta/2 + |\Delta\theta|/2$$

and

$$\left|\sin\left(\frac{\theta+\Delta\theta}{2}\right) - \sin\left(\theta/2\right)\right| \leq \frac{|\Delta\theta|}{2}$$

$$\frac{|\Delta M|}{2N} < \left(2\sin\left(\theta/2\right) + \frac{|\Delta\theta|}{2}\right)\frac{|\Delta\theta|}{2}$$

Substituting $\sin^2 \theta/2 = M/2N$ and $|\Delta\theta| \leq 2^{-m}$,

$$\frac{|\Delta M|}{2N} < \left(2 \times \sqrt{M/2N} + \frac{1}{2^{m+1}}\right) 2^{-m-1}$$

$$\boxed{|\Delta M| < \left(\sqrt{2MN} + \frac{N}{2^{m+1}}\right) 2^{-m}}$$

Example

Suppose we choose $m = \lceil n/2 \rceil + 1$ and $\epsilon = 1/6$.

$$t = m + \log_2\left(2 + \frac{1}{2\epsilon}\right)$$
$$= \lceil n/2 \rceil + 1 + \log_2(2+3)$$
$$= \lceil n/2 \rceil + 1 + \log_2(5)$$
$$\approx \lceil n/2 \rceil + 3$$

$\log_2 4 < \log_2 5 < \log_2 8$

$\frac{n}{2} \le \lceil n/2 \rceil < \frac{n}{2} + 1$

$\frac{n}{2} + 3 < t < \frac{n}{2} + 5$

$$\#\{\text{Grover iterations}\} = 1 + 2^1 + 2^2 + \cdots + 2^{t-1}$$
$$= 2^t - 1$$
$$= 2^{\lceil n/2 \rceil + 1 + \log_2 5} - 1$$

$$2^{\frac{n}{2}+1+\log_2 4} - 1 < 2^{\lceil n/2 \rceil + 1 + \log_2 5} - 1 < 2^{\frac{n}{2}+1+1+\log_2 8} - 1$$

$$2^{\frac{n}{2}+3} - 1 < 2^{\lceil n/2 \rceil + 1 + \log_2 5} - 1 < 2^{\frac{n}{2}+5} - 1$$

$$2^3 \cdot 2^{n/2} - 1 < 2^{\lceil n/2 \rceil + 1 + \log_2 5} - 1 < 2^5\, 2^{n/2} - 1$$

$$2^3 \sqrt{N} - 1 < 2^{\lceil n/2 \rceil + 1 + \log_2 5} - 1 < 2^5 \sqrt{N} - 1$$

$\Longrightarrow$ The algorithm requires $\Theta(\sqrt{N})$ Grover iterations, and thus $\Theta(\sqrt{N})$ oracle calls.

$$|\Delta M| < \left(\sqrt{2MN} + \frac{N}{2^{m+1}}\right) 2^{-m}$$

$N = 2^n$

& $m = \left\lceil \frac{n}{2} \right\rceil + 1 > \frac{n}{2} + 1 \implies \frac{n}{2} + 1 - m < 0$

$\implies 2\left(\frac{n}{2} + 1 - m\right) - 1 < -1 < 0$

$$|\Delta M| < \left(\sqrt{2M \times 2^n} + \frac{2^n}{2^{m+1}}\right) 2^{-m} = \left(\sqrt{\frac{M}{2} \times 2^{n+2}} + 2^{n-m-1}\right) 2^{-m}$$

$$= \left(\sqrt{M/2} \times 2^{\frac{n}{2}+1} + 2^{n-m-1}\right) 2^{-m}$$

$$= \sqrt{M/2} \times 2^{\frac{n}{2}+1-m} + \frac{1}{4} \times 2^{n-2m+1}$$

$$= \sqrt{M/2} \times 2^{\frac{n}{2}+1-m} + \frac{1}{4} \times 2^{2\left(\frac{n}{2}+1-m\right)-1}$$

$$|\Delta M| < \sqrt{M/2} + 1/4 = O(\sqrt{M})$$

The example just described serves double duty as an algorithm for determining whether a solution to the search problem exists at all, i.e., whether $M=0$ or $M \neq 0$.

If $M=0$ we have $|\Delta M| < 1/4$, so the algorithm must produce the estimate zero with probability at least $1-\epsilon = 1-\frac{1}{6} = 5/6$.

Conversely,
If $M \neq 0$ then it is easy to verify that the estimate for M is not equal to 0 with probability at least $5/6$.

Another application of quantum counting is to find a solution to a search problem when the number M of solutions is unknown.

The difficulty in applying the quantum search algorithm is that the # of times to repeat the Grover iteration, depends on knowing the # of solutions M, since

$R \leq \left\lceil \frac{\pi}{4} \sqrt{N/M} \right\rceil$

This problem can be alleviated by using the quantum counting algorithm to 1st estimate θ and M to high accuracy using phase estimation, and then apply the quantum search algorithm, repeating the Grover iteration a # of times determined by $R = CI\left(\frac{\arccos\sqrt{M/N}}{\theta}\right)$, with the estimates for θ and M obtained by phase estimation substituted to determine R.

Another application of quantum counting is to find a solution to a search problem when the number M of solutions is unknown.

The difficulty in applying the quantum search algorithm is that the # of times to repeat the Grover iteration, depends on knowing the # of solutions M, since

$$R \leq \left\lceil \frac{\pi}{4}\sqrt{N/M} \right\rceil$$

This problem can be alleviated by using the quantum counting algorithm to 1st estimate θ and M to high accuracy using phase estimation, and then apply the quantum search algorithm, repeating the Grover iteration a # of times determined by $R = CI\left(\frac{\arccos\sqrt{M/N}}{\theta}\right)$, with the estimates for θ and M obtained by phase estimation substituted to determine R.

$$|\psi\rangle = \cos \theta/2 \, |\alpha\rangle + \sin \theta/2 \, |\beta\rangle$$

where $\cos \theta/2 = \sqrt{\frac{N-M}{N}}$ & $\sin \theta/2 = \sqrt{M/N}$

Assuming $M \leq N/2 \Rightarrow \frac{M}{N} = \frac{1}{2} \Rightarrow \sqrt{\frac{M}{N}} = \frac{1}{\sqrt{2}} = \sin \theta/2$

$$0 \leq \theta/2 \leq \pi/4 \implies 0 \leq \theta \leq \pi/2$$

$$|x - CI(x)| \leq \frac{1}{2} \Rightarrow \text{angle, } \delta \leq \frac{\theta}{2} \leq \frac{\pi}{4}$$

$\therefore$ The Grover iterations rotates the initial state $|\psi\rangle$ by θ a few times, such that $|\psi\rangle$ will be rotated to within an angle $\theta/2 \leq \pi/4$ of $|\beta\rangle$.

Using the Quantum Counting algorithm to get an estimate of $\theta \approx \theta + \Delta\theta$ and thus $M \approx M + \Delta M$ which is the # of solutions.

The corresponding error to our initial state $|\psi\rangle$ is $\Delta\theta/2$.

Since, $\frac{\theta}{2} \leq \frac{\pi}{4}$, the maximum error tied to the initial state $|\psi\rangle$ is,

$$\text{Max. Initial Error} = \frac{\pi}{4} \times \frac{|\Delta\theta/2|}{\theta/2} = \frac{\pi}{4} \frac{|\Delta\theta|}{\theta}$$

Grover iterations will rotate $|\psi\rangle$ close to $|\beta\rangle$ with the maximum angular separation being $\pi/4$ irrespective of the value of the initial angle which is $\dfrac{\theta + \Delta\theta}{2}$.

$\therefore$

The total maximum angular error (accounting for the offset of $\Delta\theta/2$ in the initial state $|\psi\rangle$) from $|\beta\rangle$ in this case is,

$$\text{Total max. angular error} = \frac{\pi}{4} + \text{Max. Initial Error}$$

$$= \frac{\pi}{4} + \frac{\pi}{4}\frac{|\Delta\theta|}{\theta}$$

$$= \frac{\pi}{4}\left(1 + \frac{|\Delta\theta|}{\theta}\right)$$

So,

Choosing $m = \lceil \frac{n}{2} \rceil + 1$,

$$|\Delta\theta| \le 2^{-m} = \frac{1}{2^m}$$

$$m = \lceil \frac{n}{2} \rceil + 1 \ge \frac{n}{2} + 1 \implies 2^m \ge 2^{\frac{n}{2}+1}$$

$$\implies |\Delta\theta| \le 2^{-m} \le 2^{-\frac{n}{2}-1} = \frac{1}{2 \cdot 2^{n/2}}$$

$\boxed{\text{Lemma :}}$ $\sin x \le x$ when $0 \le x \le \frac{\pi}{2}$

Proof

$f(x) = \sin x - x$, $0 \le x \le \pi/2$

$f'(x) = \cos x - 1 \implies f'(0) = 1 - 1 = 0$ & $f'(\pi/2) = -1$

$f''(x) = -\sin x < 0$ } $f(x)$ is a decreasing function in $[0, \pi/2]$.

$f(0) = 0$

$f(\pi/2) = 1 - \frac{\pi}{2} < 0$ } $f(x) = \sin x - x \le 0$

$\therefore \sin x \le x$

Lemma $\Rightarrow \frac{\theta}{2} \geq \sin\theta/_2$ since $0 \leq \theta/_2 \leq \pi/_4$

$$\Rightarrow \frac{1}{\theta} \leq \frac{1}{\sin\theta}$$

$$\theta/_2 \geq \sin\theta/_2 = \sqrt{\frac{M}{2N}} \geq \sqrt{\frac{1}{2N}} \Longrightarrow \theta/_2 \geq \frac{1}{\sqrt{2N}} = \frac{1}{\sqrt{2} * 2^{n/2}}$$

$$\frac{|\Delta\theta|}{\theta} = \frac{|\Delta\theta|}{2 * \theta/_2} \leq \frac{1/_{2 * \cancel{2^{n/2}}}}{1/_{\sqrt{2} * \cancel{2^{n/2}}}} = \frac{1}{\sqrt{2}} \leq \frac{1}{2}$$

If $M \leq N/_2$, then $\sin\theta/_2 = \sqrt{M/_N} \leq \sqrt{1/_{2N}}$

$$\Rightarrow \theta/_2 \geq \frac{1}{\sqrt{N}} = \frac{1}{2^{n/2}}.$$

$$\Rightarrow \frac{|\Delta\theta|}{\theta} = \frac{|\Delta\theta|}{2 * \theta/_2} \leq \frac{1/_{2 * 2^{n/2}}}{1/_{2^{n/2}}} = \frac{1}{2}$$

$$\therefore \frac{\pi}{4}\left(1 + \frac{|\Delta\theta|}{\theta}\right) = \frac{\pi}{4}\left(1 + \frac{1}{2}\right) = \frac{\pi}{4} * \frac{3}{2} = 3\pi/_8$$

which is the max. angular error.

$$\boxed{\begin{array}{l} P(\text{measure } |\beta\rangle) \geq \sin^2(\pi/_2 - \theta/_2) = \cos^2\theta/_2 \\ \text{where, } \theta/_2 \text{ is the angle b/w } G^k|\psi\rangle \text{ and } |\beta\rangle. \end{array}}$$

The corresp. success probability is at least $\cos^2(3\pi/_8) \approx 0.15$ for the search algorithm.

The probability of obtaining an estimate of θ this accurate is $5/6$.

$\therefore$ The total probability of obtaining a solution to the search problem is,

$$\frac{5}{6} \times \cos^2\left(3\pi/8\right) \approx 0.12$$

a probability which may quickly be boosted close to 1 by a few repetitions of the combined counting-search procedure.

FEEDBACK ? SUGGESTIONS ?
Quality Manager, ITC Ltd.- ESPB,
ITC Centre, 5th Floor,
760, Anna Salai, Chennai. 600 002.
classmate@itc.in **18004253242**
(Toll-Free from MTNL/BSNL lines)

A quality product marketed by

Enduring Value

Exercise Book
172 Pages
(Total Pages Include Index & Printed Information)

Size : 24 x 18 cm

MRP Rs. 48.00
Inclusive of all taxes

Batch: C/AE/FT
02000222

8 902519 00222

©ITC Limited

Type of Ruling :
Unruled