A SIMPLE EXPLANATION OF SEARCH TECHNIQUE IN QUANTUM FRAMEWORK

Shaktikanta Nayak1, Sitakanta Nayak1 and J.P. Singh2
1PhD student, Department of Management Studies, Indian Institute of Technology, Roorkee
2Professors, Department of Management Studies, Indian Institute of Technology, Roorkee,
Uttarakhand, India
shakti302@gmail.com1, purieskay@gmail.com2, jpsiitr@gmail.com3

Abstract: The quantum search takes advantage of quantum parallelism to construct superposition of all possible states and then increase the probability amplitude of the solution state. This is the distinguishing characteristics of quantum search strategy. The objective of a classical search algorithm is to diminish the amplitude of target state where as a quantum search algorithm tries to amplify the amplitude of the target state. The term amplification indicates to increase the probability of the target state. This paper attempts to explain two central ideas of Grover’s quantum search algorithm that amplify the probability of the target state, the inversion about the mean and phase inversion, in a simplified way with a concrete example.

Key words: Database search, Quantum computing, Quantum algorithm, Grover’s search algorithm,

INTRODUCTION

Information storage and retrieval are the most important applications of database systems. In a brute force search technique the worst case time complexity to locate an item is \( O(N) \) where, \( N \) is the size of the data base. Binary search technique is an improved algorithm for searching which is based upon sorting. The worst case time complexity to locate an item using this technique is \( O(\log N) \). Suppose telephone number of a person is the key instead of his name and we want to find the name of the person. In this case binary search is not possible to search this unsorted database. The major drawback of binary search is the sorting. In real world we have certain problems which have to be searched in an efficient way without sorting. Is there any technique which can search more efficiently than the best known classical search techniques with less computing time? The answer is a new search algorithm which is based upon principles of quantum computing, the computing inspired by quantum mechanics [14].

The idea to introduce quantum principles in computing was first given by Feynman [3, 4]. Nowadays quantum computing is a promising research field with vast application in cryptography and security, artificial neural networks [15,16], algorithm, information processing etc. All the important quantum algorithms discovered to date perform tasks exponentially faster than their classical counterparts. Deutsch’s algorithm [5] is designed to solve the problem of identifying whether a binary function is constant or balanced. Its running time is \( O(n) \) while classical counterpart of this method requires \( O(2^n) \) running time. Simon’s algorithm [6] is designed for finding the periodicity of a function that is guaranteed to possess a periodic element. Shor’s algorithm [7] used for prime factorization, finds the prime factors of very large numbers in a polynomial time for which the best known classical algorithm requires exponential time. Finally the most important algorithm for our discussion called Grover’s search algorithm [8, 9], which is based upon the principles of quantum computing [10–13], is meant for searching an unsorted database in \( O(\sqrt{N}) \) times, where as a classical search algorithm takes \( O(N) \) times. Searching is a real world problem for which quantum algorithm provides the performance that is classically impossible. The quantum search technique takes the advantage of quantum parallelism to construct superposition of all possible values of the states and then increase the probability amplitude of the solution state.

This parallelism provides the distinction between classical and quantum algorithmic strategies. For an example the objective of a classical algorithm is to reduce the amplitude of non target states, where as a quantum search algorithm tries to amplify the amplitude of the target states. Here the term amplification indicates to increase the probability of the target state. The main idea of quantum search technique is to rotate the state vector from an initial state to a final state (target) in a two-dimensional Hilbert space. The algorithm is iterative and each iteration causes same amount of rotation. The speedup is achieved due to the quantum parallelism and the probability, which is the square of the amplitude. In this paper, a detailed analysis of the mechanism of the above said transformations is done in both classical and quantum context. Grover’s algorithm has been demonstrated for a data base of size sixteen. Finally a comparison is made between classical and quantum search.

PHASE INVERSION AND INVERSION ABOUT THE MEAN

Definition Of Mean:
Suppose we have a set of integers \( X = \{x_i\} \) where \( i = 1, 2, \ldots N \), with mean

\[
\text{mean} = \frac{1}{N} \sum_{i=1}^{N} x_i
\]
Defination of inversion about the mean:
The classical inversion about the mean is denoted by $Y$, transforms $x_i$ to $x_i'$:

$$Y: x_i \rightarrow x_i' \text{ with}$$

$$x_i' = \bar{x} + (x - x_i)$$

$$= 2\bar{x} - x_i$$

(2)

EXAMPLE-1 (INVERSION ABOUT THE MEAN)
Suppose we have a set of eight integers $X = \{34, 66, 47, 63, 54, 28, 42, 48\}$
The average is $\bar{x} = \frac{1}{8} \sum_{i=1}^{8} x_i = 49$

Graphically representation of eight integers with average 49:

![Graphical representation of eight integers with average 49](image)

In figure-1 the amplitude of vertical bars are proposal to the modulus of the numbers. The transformation of individual integers about the mean is $\bar{x} = 49$

The transformation of individual integers is given below:

$$34 \rightarrow 98 - 34 = 64, 66 \rightarrow 98 - 66 = 32, 47 \rightarrow 98 - 47 = 51, 63 \rightarrow 98 - 63 = 35$$

$$54 \rightarrow 98 - 54 = 44, 28 \rightarrow 98 - 28 = 70, 42 \rightarrow 98 - 42 = 56, 58 \rightarrow 98 - 58 = 40$$

Graphically representation of inversion about the mean:

![Graphical representation of inversion about the mean](image)

EXAMPLE-2 (Inversion About The Mean And Phase Inversion):
Next, let us level the 8 items with complex numbers of equal amplitude $x_i = \frac{1}{\sqrt{8}}$ and impose the condition that after each transformation the sum of the squares of the modulus of the complex numbers to be one. Suppose there are eight numbers and we want to search sixth number. Assume that there is an oracle (a black box) which is capable to invert the phase of the complex number and identify the item we are searching for. Gradually we will notice that the repeated application of phase inversion and inversion about the mean will amplify the amplitude of the desired state and will decrease the amplitude of other states.

![Graphical representation of phase inversion of the sixth element](image)

STEP-0
Initially all the 8 numbers are of equal amplitude shown in the figure below.

Graphical representation of eight complex numbers with equal amplitude $\frac{1}{\sqrt{8}}$:

![Graphical representation of eight complex numbers with equal amplitude](image)

Calculate the new mean from the phase inversion figure-3 of STEP-0:

$$\bar{x} = \frac{1}{8} \sum_{i=1}^{8} x_i = \frac{1}{8} \left[ 7 \times \frac{1}{\sqrt{8}} - \frac{1}{\sqrt{8}} \right]$$

$$= \frac{3}{4\sqrt{8}}$$

(3)

Calculate the new inversion about the mean using the formula using equation (2)

$$x_1' = x_2' = x_3' = x_4' = x_5' = x_7' = x_8' = 2 \times \frac{3}{4\sqrt{8}} - \frac{1}{\sqrt{8}}$$

$$= \frac{1}{2\sqrt{8}}$$

(4)

and

$$x_6' = 2 \times \frac{3}{4\sqrt{8}} + \frac{1}{\sqrt{8}}$$

$$= \frac{5}{2\sqrt{8}}$$

(5)

The inversion about the mean amplifies the amplitude of the sixth item we are searching for and reduce the amplitude of the rest seven items. This can be visualized graphically as follows:

Again make a second time phase inversion of the sixth item which is shown graphically:

![Graphical representation of phase inversion of the sixth element](image)
STEP-2

When we are going for a second phase inversion of the sixth item we have to find a new inversion about the mean. Hence the new mean will be:

$$\bar{x}' = \frac{1}{8} \sum_{i=1}^{8} x_i = \frac{1}{8} \left[ 7 \times \frac{1}{2\sqrt{8}} - \frac{5}{2\sqrt{8}} \right]$$

$$= \frac{1}{8\sqrt{8}}$$

(6)

The inversion about the mean using the formula will be

$$x_1'' = x_2'' = x_3'' = x_4'' = x_5'' = x_7'' = x_8''$$

$$= 2 \times \frac{1}{8\sqrt{8}} - \frac{1}{4\sqrt{8}}$$

and

$$x_6'' = 2 \times \frac{1}{8\sqrt{8}} + \frac{5}{2\sqrt{8}}$$

$$= \frac{11}{4\sqrt{8}}$$

(8)

The second time inversion about the mean amplifies the amplitude of the sixth item more than previous and reduces more the amplitude of the rest of the seven items than before. This can be visualized graphically below:

```
Figure-5
```

From the above discussion we can analyse, without going into the detail of the Grover search algorithm, the effect of inversion about the mean with phase inversion considering set of eight complex numbers $x_i$ to be the probability amplitude of the basis states of the Hilbert space. The initial state of a system with eight elements:

$$|\Psi\rangle = x_1|000\rangle + x_2|001\rangle + x_3|010\rangle + x_4|011\rangle + x_5|100\rangle + x_6|101\rangle + x_7|110\rangle + x_8|111\rangle$$

(9)

The probability amplitude of the sixth element $|101\rangle$ is $1/8 = 0.125$

After two iterations of phase inversion followed by inversion about the mean the final state will be:

$$|\Psi\rangle'' = x_1'|000\rangle + x_2'|001\rangle + x_3'|010\rangle + x_4'|011\rangle + x_5'|100\rangle + x_6'|101\rangle + x_7'|110\rangle + x_8'|111\rangle$$

(10)

If we measure the probability amplitude of the sixth element $|101\rangle$ will be $(\frac{11}{4\sqrt{8}})^2 = \frac{121}{128} = 0.97227$. Hence in conclusion the concept of inversion about mean with phase inversion increases the probability amplitude of the desired state with decreasing amplitude of other states. In other words the probability of finding the desired state is tending towards one compared with other states. Here we have applied the inversion twice which means the number of iteration took place for two times.

OUTLINE OF GROVER’S SEARCH METHOD

Let us consider an unstructured database with $N = 2^n$ elements which are numbered 0 to $N - 1$. Grover’s algorithm uses two registers where the first register contains $n$-qubits to hold the address of the label in binary form. The second register holds the oracle qubit. Apply $n$-dimensional Hadamard gate to create $|\Psi\rangle$, an equal superposition of the indices of all items in the database. Apply Grover operator $G$ for $O(\sqrt{N})$ times on $|\Psi\rangle$. Where $G$ consists of oracle $U_f$ followed by an inversion about the mean $D_\Psi$. Hence $G = D_\Psi U_f = (2|\Psi\rangle\langle\Psi| - I)U_f$. Finally measure the state $|\Psi\rangle$.

```
DIAGRAM:
```

```
Figure-6
```
STEP 0
Initialize first register and second register in the state \(|0^{\otimes n}\) and \(|1\rangle\) respectively.

STEP 1
Apply \(n\)-dimensional Hadamard gate to first and \(1\)-dimensional Hadamard gate to second register respectively.

STEP 2
Apply Grover operator \(G\) for \(O(\sqrt{N})\) times on step-1
- Apply oracle \(U_f\) (Phase inversion)
- Apply \(D_\varphi = 2|\Psi\rangle\langle\Psi| - I\) (Amplitude amplification)

DIAGRAM:

First Register

Initialization to \(|0\rangle\) and second register initialized to \(|1\rangle\)

STEP 3
Measure the result

EXECUTION

Find the eleventh record from a given database of size sixteen. i.e. \(N = 2^4 = 16\), so we need a register of length \(n = 4\) bits. The number of iterations \(k = \text{round}\left(\frac{\pi}{4}\sqrt{N}\right) = \text{round}\left(\frac{\pi}{4}\sqrt{16}\right) = 3\). Refer Grover circuit in fig-7 and Grover algorithm steps for execution of the problem.

So we will modify the state \(|\Psi\rangle\) as follows:

\[
|\Psi\rangle = \frac{1}{\sqrt{16}} \left[ \sum_{x=0}^{15} |x\rangle + |1011\rangle \right]
\]

Where,

\[
|\Phi\rangle = \frac{1}{\sqrt{15}} \sum_{x=1}^{15} |x\rangle
\]

\[
= \frac{1}{\sqrt{15}} \left[ |0000\rangle + |0001\rangle + |0010\rangle + |0011\rangle + |0100\rangle + |0101\rangle + |0110\rangle + |0111\rangle + |1000\rangle + |1001\rangle + |1010\rangle + |1011\rangle + |1100\rangle + |1101\rangle + |1110\rangle + |1111\rangle \right]
\]

Therefore

\[
|\Psi\rangle = \frac{\sqrt{15}}{\sqrt{16}} |\Phi\rangle + \frac{1}{\sqrt{16}} |1011\rangle
\]

First iteration

Apply the oracle operator \(U_f\):
\[
|\Psi_0\rangle = U_f(|\Phi\rangle - \rangle) = \frac{\sqrt{15}}{\sqrt{16}} U_f(|\Phi\rangle - \rangle) + \frac{1}{\sqrt{16}} U_f(|1011\rangle - \rangle)
\]

\[
|\Psi_0\rangle = \frac{\sqrt{15}}{\sqrt{16}} |\Phi\rangle - \rangle - \frac{1}{\sqrt{16}} |1011\rangle - \rangle
\]

Hence

\[
|\Psi_1\rangle = \frac{\sqrt{15}}{\sqrt{16}} |\Phi\rangle - \rangle - \frac{1}{\sqrt{16}} |1011\rangle - \rangle
\]

Similarly the second and third iterations will be carried out as follows:

**Second iteration:**

Apply the oracle operator \(U_f\):

\[
|\Psi_2\rangle = |2\Psi\rangle(|\Psi\rangle - I) = \frac{3}{4} |\Psi\rangle + \frac{1}{2} |1011\rangle
\]

\[
|\Psi_2\rangle = \frac{3}{16} \sum_{x=0}^{15} |x\rangle + \frac{11}{16} |1011\rangle
\]

**Third iteration:**

Apply the oracle operator \(U_f\):

\[
|\Psi_3\rangle = |2\Psi\rangle(|\Psi\rangle - I)|\Psi_2\rangle = \frac{5}{64} \sum_{x=0}^{15} |x\rangle + \frac{61}{64} |1011\rangle
\]

Finally calculate the probability of the target state \(|1011\rangle\)

\[
P = \frac{251}{256}^2 \approx 0.96
\]

Hence finding the probability of the desired state \(|1011\rangle\) is around 96%. From this we can conclude that the oracle requires three iterations to execute the algorithm. In order to execute the same problem classically we need eight queries in an average.

**CONCLUSION**

In this paper, a simple explanation of inversion about the mean and phase inversion is made considering a register of four qubits. The limitation of the algorithm is that it terminates earlier before reaching the target state due to some error factor. A comparison between quantum and classical search algorithm is given below.

<table>
<thead>
<tr>
<th>ALGORITHM</th>
<th>QUANTUM</th>
<th>CLASSICAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executes on</td>
<td>Quantum computer</td>
<td>Classical computer</td>
</tr>
<tr>
<td>Uses</td>
<td>Qubits</td>
<td>Bits</td>
</tr>
<tr>
<td>Number of operations</td>
<td>(O(\sqrt{N}))</td>
<td>(O(N))</td>
</tr>
<tr>
<td>Nature</td>
<td>Probabilistic</td>
<td>Generally Non-probabilistic</td>
</tr>
<tr>
<td>Implementation</td>
<td>Quantum Gates</td>
<td>Classical Gates</td>
</tr>
</tbody>
</table>

**REFERENCE**


