

RESEARCH PAPER

Available Online at www.jgrcs.info

A SIMPLE EXPLANATION OF SEARCH TECHNIQUE IN QUANTUM FRAMEWORK

Shaktikanta Nayak^{*1}, Sitakanta Nayak¹ and J.P.Singh²

¹PhD student, Department of Management Studies, Indian Institute of Technology, Roorkee

² Professors, Department of Management Studies, Indian Institute of Technology, Roorkee, Uttarakhand, India

shakti302@gmail.com¹, purieskay@gmail.com², jpsitr@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 data base system. 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 data base. The major drawback of binary search is the sorting then searching. 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 crypto graphy and security, artificial neural network [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. The Grover's algorithm is based upon two transformations: Inversion about the mean and Phase inversion. Repeated applications of these two transformations increase the probability amplitude of the desired state with high accuracy. 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

Defination Of Mean:

Suppose we have a set of integers $X = \{x_i\}$ where $i = 1, 2, \dots, N$, with mean

$$\bar{x} = \frac{1}{N} \sum_{i=1}^N x_i \quad (1)$$

Definition of inversion about the mean:

The classical inversion about the mean is denoted by Y , transforms x_i to x_i' :

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

$$\begin{aligned} x_i' &= \bar{x} + (\bar{x} - x_i) \\ &= 2\bar{x} - x_i \end{aligned} \quad (2)$$

EXAMPLE-1 (INVERSION ABOUT THE MEAN)

Suppose we have a set of eight integers $X = \{34, 66, 47, 63, 54, 28, 42, 58\}$

The average is $\bar{x} = \frac{1}{8} \sum_{i=1}^8 x_i = 49$

Graphically representation of eight integers with average 49:



Figure- 1. Set of eight integers with average = 49

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:

$$\begin{aligned} 34 &\rightarrow 98 - 34 = 64, & 66 &\rightarrow 98 - 66 = 32, & 47 &\rightarrow 98 - 47 = 51, \\ 47 &= 51, & 63 &\rightarrow 98 - 63 = 35, \\ 54 &\rightarrow 98 - 54 = 44, & 28 &\rightarrow 98 - 28 = 70, & 42 &\rightarrow 98 - 42 = 56, \\ 42 &= 56, & 58 &\rightarrow 98 - 58 = 40 \end{aligned}$$

Graphical representation of inversion about the mean:

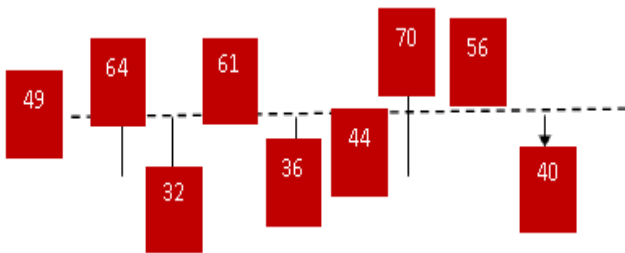


Figure-2 Graphical Representation of Inversion about Mean

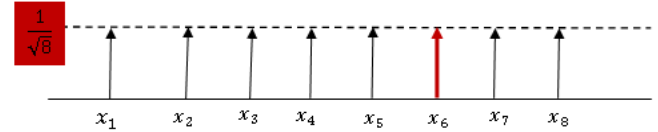
Example-2(Inversion About The Mean And Phase Inversion):

Next, let us level the N items with complex numbers of equal amplitude $x_i = \frac{1}{\sqrt{N}}$ 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.

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 Phase inversion of the sixth element:

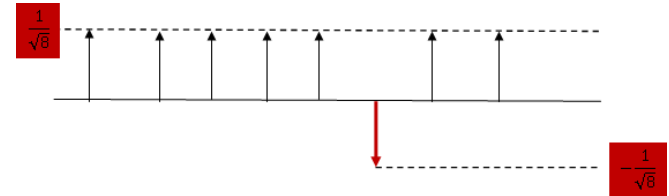


Figure-3

STEP-1

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

$$\begin{aligned} \bar{x} &= \frac{1}{8} \sum_{i=1}^8 x_i = \frac{1}{8} \left[7 \times \frac{1}{\sqrt{8}} - \frac{1}{\sqrt{8}} \right] \\ &= \frac{3}{4\sqrt{8}} \end{aligned} \quad (3)$$

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

$$\begin{aligned} x_1' = x_2' = x_3' = x_4' = x_5' = x_7' = x_8' &= 2 \times \frac{2}{4\sqrt{8}} - \frac{1}{\sqrt{8}} \\ &= \frac{1}{2\sqrt{8}} \end{aligned} \quad (4)$$

and

$$\begin{aligned} x_6' &= 2 \times \frac{3}{4\sqrt{8}} + \frac{1}{\sqrt{8}} \\ &= \frac{5}{2\sqrt{8}} \end{aligned} \quad (5)$$

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:

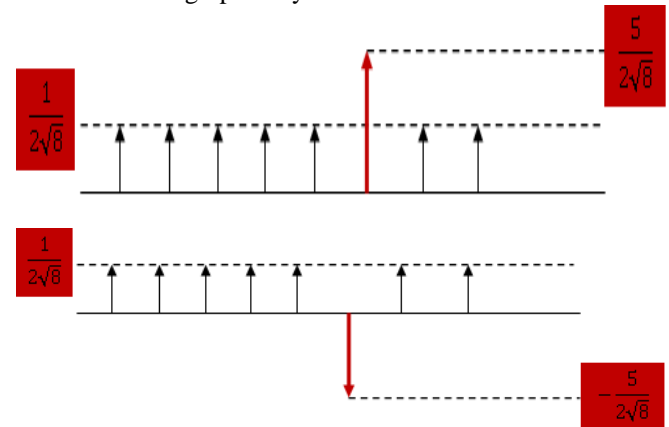


Figure-4

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:

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

$$= \frac{1}{8\sqrt{8}} \quad (6)$$

The inversion about the mean using the formula will be

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

$$= 2 \times \frac{1}{8\sqrt{8}} - \frac{1}{2\sqrt{8}} = -\frac{1}{4\sqrt{8}} \quad (7)$$

and

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

$$= \frac{11}{4\sqrt{8}} \quad (8)$$

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:

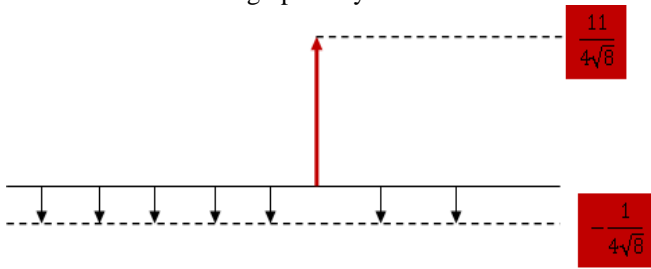


Figure-5

From the above discussion we can analyse, without going in to 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:

DIAGRAM:

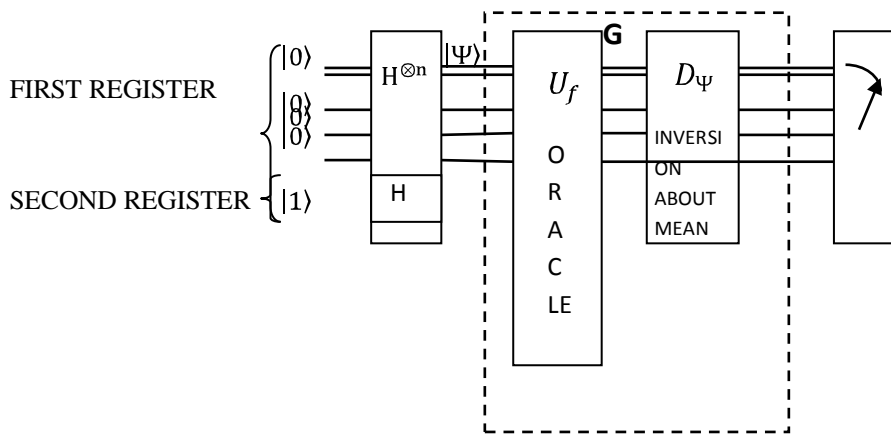


Figure-6

$$|\Psi\rangle = x_1|000\rangle + x_2|001\rangle + x_3|010\rangle + x_4|011\rangle + x_5|100\rangle$$

$$+ x_6|101\rangle + x_7|110\rangle + x_8|111\rangle \quad (9)$$

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:

$$|\Psi''\rangle = x_1''|000\rangle + x_2''|001\rangle + x_3''|010\rangle + x_4''|011\rangle + x_5''|100\rangle$$

$$+ x_6''|101\rangle + x_7''|110\rangle + x_8''|111\rangle \quad (10)$$

If we measure the probability amplitude of the sixth element $|101\rangle$ will be $\left(\frac{11}{4\sqrt{8}}\right)^2 = \frac{121}{128} = 0.97227$. 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_Ψ . Hence $G = D_\Psi U_f = (2|\Psi\rangle\langle\Psi| - I)U_f$. Finally measure the state $|\Psi\rangle$.

STEP-0

Initialize first register and second register in the state $|0\rangle^{\otimes n}$ 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 $D_\Psi = 2|\Psi\rangle\langle\Psi| - I$ (Amplitude amplification)

DIAGRAM:

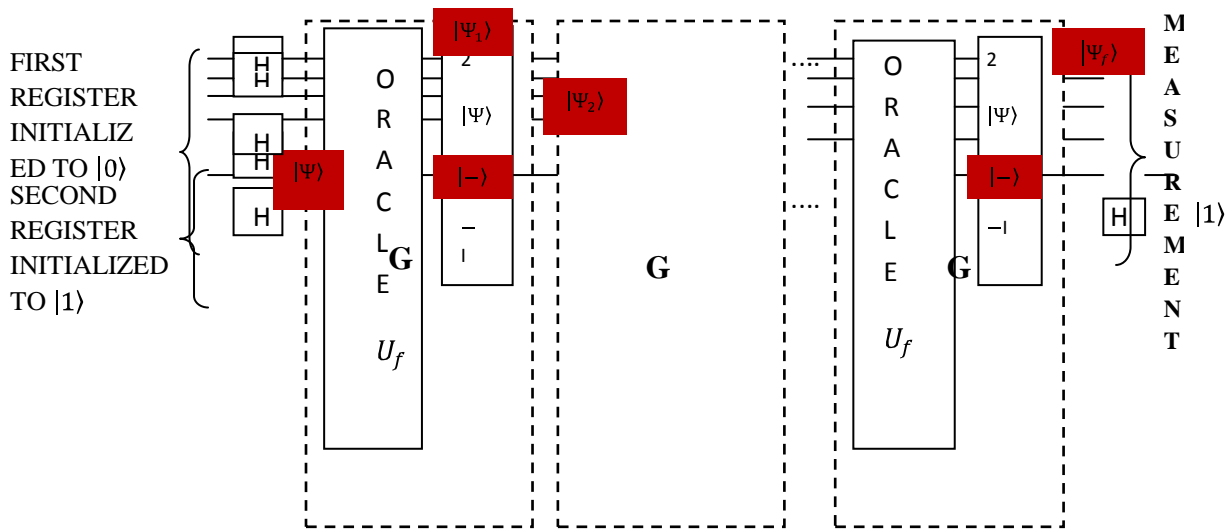


Figure- 7 Grover Circuit for $n = 4$

We will start by putting four qubits in the first register and one qubit in the second register respectively.

STEP-0

Then initialize the first register to be in the state $|0000\rangle$ and second register to be $|1\rangle$

STEP-1

Apply the Hadamard operator to the first register:

$$|\Psi\rangle = H^{\otimes 4} |0000\rangle = (H|0\rangle)^{\otimes 4} = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right]^{\otimes 4}$$

$$= \frac{1}{\sqrt{2^4}} \sum_{x=0}^{2^4-1} |x\rangle = \frac{1}{\sqrt{16}} \sum_{x=0}^{15} |x\rangle$$

$$|\Psi\rangle = \frac{1}{\sqrt{16}} \{ |0000\rangle + |0001\rangle + |0010\rangle + |0011\rangle + |0100\rangle + |0101\rangle + |0110\rangle + |0111\rangle + |1000\rangle + |1001\rangle + |1010\rangle + |1011\rangle + |1100\rangle + |1101\rangle + |1110\rangle + |1111\rangle \}$$

Apply the Hadamard operator to the second register:

$$|-\rangle = H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

STEP-2

Apply Grover operator G for 3 times and stop when $|1011\rangle = 11$ is reached:

We want to find the 11th item that is $|1011\rangle = 11$

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:

$$|\Psi\rangle = \frac{1}{\sqrt{16}} \left[\sum_{\substack{x=0 \\ x \neq 11}}^{15} |x\rangle + |1011\rangle \right]$$

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

Where,

$$|\Phi\rangle = \frac{1}{\sqrt{15}} \sum_{\substack{x=0 \\ x \neq 11}}^{15} |x\rangle$$

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

Therefore

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

First iteration

Apply the oracle operator U_f :

$$\begin{aligned}
 |\Psi_1\rangle|-\rangle &= U_f(|\Psi\rangle|-\rangle) \\
 &= \frac{\sqrt{15}}{\sqrt{16}}U_f[|\Phi\rangle|-\rangle] + \frac{1}{\sqrt{16}}U_f[|1011\rangle|-\rangle] \\
 &= \frac{\sqrt{15}}{\sqrt{16}}|\Phi\rangle|-\rangle - \frac{1}{\sqrt{16}}|1011\rangle|-\rangle
 \end{aligned}$$

Hence

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

$$\begin{aligned}
 |\Psi_1\rangle &= \frac{1}{\sqrt{16}}\{ |0000\rangle + |0001\rangle + |0010\rangle + |0011\rangle \\
 &\quad + |0100\rangle + |0101\rangle + |0110\rangle + |0111\rangle \\
 &\quad + |1000\rangle + |1001\rangle + |1010\rangle - |1011\rangle \\
 &\quad + |1100\rangle + |1101\rangle + |1110\rangle + |1111\rangle \}
 \end{aligned}$$

Using state $|\Phi\rangle$ we can write $|\Psi_1\rangle$ as:

$$|\Psi_1\rangle = \frac{1}{4} \sum_{\substack{x=0 \\ x \neq 11}}^{15} |x\rangle - \frac{1}{4} |1011\rangle$$

Apply the inversion operator $(2|\Psi\rangle\langle\Psi| - I)$:

$$|\Psi_2\rangle = [2|\Psi\rangle\langle\Psi| - I]|\Psi_1\rangle = \frac{3}{4}|\Psi\rangle + \frac{1}{2}|1011\rangle$$

$$\Rightarrow |\Psi_2\rangle = \frac{3}{16} \sum_{\substack{x=0 \\ x \neq 11}}^{15} |x\rangle + \frac{11}{16}|1011\rangle$$

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

Second iteration:

Apply the oracle operator U_f :

$$\begin{aligned}
 |\Psi_3\rangle|-\rangle &= U_f(|\Psi_2\rangle|-\rangle) = \frac{3}{4}|\Psi\rangle - \frac{7}{8}|1011\rangle \\
 &= \frac{3}{16} \sum_{\substack{x=0 \\ x \neq 11}}^{15} |x\rangle - \frac{11}{16}|1011\rangle
 \end{aligned}$$

Apply the inversion operator $(2|\Psi\rangle\langle\Psi| - I)$:

$$|\Psi_4\rangle = [2|\Psi\rangle\langle\Psi| - I]|\Psi_3\rangle = \frac{5}{64} \sum_{\substack{x=0 \\ x \neq 11}}^{15} |x\rangle + \frac{61}{64}|1011\rangle$$

Third iteration:

Apply the oracle operator U_f :

$$|\Psi_5\rangle|-\rangle = U_f(|\Psi_4\rangle|-\rangle) = \frac{5}{16}|\Psi\rangle - \frac{33}{32}|1011\rangle$$

Apply the inversion operator $(2|\Psi\rangle\langle\Psi| - I)$:

$$|\Psi_f\rangle = [2|\Psi\rangle\langle\Psi| - I]|\Psi_5\rangle = -\frac{13}{256}|x\rangle + \frac{251}{256}|1011\rangle$$

STEP-4

Measure the state $|\Psi_f\rangle$

Finally calculate the probability of the target state $|1011\rangle$

$$\begin{aligned}
 P &= \left| \frac{251}{256} \right|^2 \\
 &\cong 0.96
 \end{aligned} \tag{11}$$

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: 1

ALGORITHM	QUANTUM	CLASSICAL
Executes on	Quantum computer	Classical computer
Uses	Qubits	Bits
Number of operations	$O(\sqrt{N})$	$O(N)$
Nature	Probabilistic	Generally Non probabilistic
Implementation	Quantum Gates	Classical Gates

REFERENCE

- [1]. Yao A C, Bentley J. An almost optimal algorithm for unbounded searching. Information Processing Letters, 1976, 5: 82-87
- [2]. Yao A C, Yao F. The complexity of searching an ordered random table. In: Proceedings of 17th IEEE Symposium on Foundations of Computer Science. Houston, Texas: 1976, 222-227
- [3]. R. Feynman. Simulating physics with computers. Internat. J. Theoret. Phys., 21:467-488, 1982.
- [4]. R. Feynman. Quantum mechanical computers. Optics News, 11:11-21, February 1985.
- [5]. D. Deutsch. Quantum theory, the church-Turing principle and the universal quantum computer. Proc. Roy. Soc. London Ser. A, 400:97-117, 1985.
- [6]. D. Simon. On the power of quantum computation. SIAM J. Comp., 26(5):1474-1483, 1997. preliminary version in Proc. 26th ACM Symposium. on Theory of Computing (STOC), pages 116-123, 1994.
- [7]. P.W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comp., 26(5):1484-1509, 1997. Preliminary version in Proceedings of the 35th Ann. IEEE Symposium on the Foundations of Computer Science (FOCS), pages 124-134, 1994
- [8]. Grover L K. A fast quantum mechanical algorithm for database search. In: Proceedings of 28th Annual ACM Symposium on Theory of Computing. New York: ACM, 1996, 212-219

- [9]. Grover L K. Quantum mechanics helps in searching for a needle in a haystack. Phys. Rev. Lett., 1997, 79(2): 325–328
- [10]. M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, UK, 2000.
- [11]. J. Gruska, Quantum computing, McGraw-Hill, 1999
- [12]. J. Preskill. Quantum information and computation, Lecture notes.
<http://www.theory.caltech.edu/people/preskill/ph229/>, 1998.
- [13]. M. Nakahara and T. Ohmi, *Quantum Computing: From Linear Algebra to Physical Realizations*, (Taylor and Francis, 2008).
- [14]. P. A. M. Dirac, *Principles of Quantum Mechanics* (4th ed.), (Clarendon Press, 1981)
- [15]. Shaktikanta Nayak, Sitakanta Nayak, J.P.Singh, “An Introduction to Quantum Neural Computing”, Journal of Global Research in Computer science.Vol-2, No-8, August-2011.
- [16]. Sitakanta Nayak, Shaktikanta Nayak, J.P Singh, “Quantum Concepts in Neural Computation”, Proceedings of the International Conference on Soft Computing for problem Solving 2011, Advances in Intelligent and Soft Computing ,Vol. 130, pp. 395–400 , Springer India.