A Modification of Grover’s Quantum Search Algorithm

I. Ashraf[1], T. Mahmood[2], V. Lakshminarayanan[3]

[1]Department of Physics, Quaid-i-Azam University
Islamabad, 45320, Pakistan

[2]Department of Physics, Hazara University Mansehra, Pakistan

[3]School of Optometry, Department of Physics and Electrical Engineering, University of Waterloo
200 University Avenue West, Waterloo, Ontario N2l 3G1Canada

[1]drimrana@comsats.net.pk; [2]tmabbasi2004@yahoo.com; [3]vengu@uwaterloo.ca

Abstract-**We propose a quantum search method based on Grover’s algorithm. This algorithm is described and we show that to search for a single marked element from an unsorted search space of *N* elements, the number of queries are required using this algorithm $O\left(N^{1/3}\right)$ when compared to $O(\sqrt{N})$ for the Grover algorithm.**

Keywords-Quantum Search Algorithm; Grover’s Technique; Sub-register

I. INTRODUCTION

A computation is a physical process. It may be performed by a piece of electronics, on an abacus, or in our brain. But it is a process that takes place in nature and as such, it is subject to the laws of physics. Application of principles of quantum mechanics in the development of techniques for computation and information processing has given birth to the science of quantum computation. According to Feynman [1], the computers based on laws of quantum mechanics instead of classical physics could be used to model quantum mechanical systems and other large scale computations. Quantum computers are machines that rely on quantum phenomena such as quantum interference and quantum entanglement in order to perform the computation [2-4].

The quantum mechanically produced computers will speedup certain computations dramatically. But one of the main difficulties of quantum computers is that de-coherence destroys the information in the superposition of states contained in a quantum computer, thus making long computations impossible. It has been shown [5] how to reduce the effect of de-coherence for information stored in quantum memory. Quantum computers offer an essential speed advantage over classical computers [6]. Some recent reviews [7, 8] have attempted to explain how a quantum computer differs from a classical, conventional computer.

In order to solve a particular problem, computers, be it classical ones or quantum, follow a precise set of instructions called an algorithm. But the kinds of search algorithms that can be run on a quantum computer are qualitatively different from those that run on classical computers [9].

Over the past years, several quantum algorithms have emerged. Some are exponentially faster than their best classical counterparts [10]; others are polynomial-faster [11]. While a polynomial speed up less than we would like ideally, quantum search has proven to be considerably more versatile than the quantum algorithms exhibiting exponential speedups.

In this paper we propose a fast quantum search algorithm inspired by Grover’s search algorithm [11]. It has shown that using the same technique as Grover’s algorithm but by dividing the register with $N = 2^n$ elements into $M = 2^{\left\lfloor \frac{n}{3} \right\rfloor}$ sub-registers, we can find a marked element in $O\left(\left[\ (\pi+2)/4\ \right]N^{1/3}\right)$ steps instead of $O\left(\sqrt{N}\right)$ as in Grover’s algorithm.

The contents of this paper can be summarized as follows. Section II describes the Grover’s quantum search algorithm for an unsorted database. In Sec. III, we give the details of our fast quantum search algorithm based on the idea of sub-registers. In the last section, we will explain and discuss our results.

II. GROVER’S QUANTUM SEARCH ALGORITHM

Quantum mechanics can speed up range of search applications over unsorted data. Consider a search problem having an unsorted database containing *N* elements, out of which just one element satisfies a given condition that it is marked. The problem is to find this marked element. Once an element is examined, it is possible to tell whether or not it satisfies the condition in one-step. However, there do not exist any sorting on the database that would aid its selection. Classically, searching an unsorted database requires linear search, i.e, examine the items in database one by one. One has to keep track of the examined elements so that it is not checked again. To find marked elements with a probability of 50% any classical algorithm, deterministic or probabilistic, will need to access the database a minimum of 0.5 *N* times (and *N* times in the worst case). Quantum mechanical systems can be in a superposition of states and simultaneously examine multiple elements; therefore, it can speed up the search. Grover’s quantum search algorithm shows that by using the same amount of hardware as in the classical case, but having input and output in superposition of states, we can find an element in $O\left(\sqrt{N}\right)$ quantum mechanical steps instead of $O\left(N\right)$ classical steps. It provides a quadratic speedup over its classical counterpart, which is considerable when *N* is large. Grover’s algorithm is probabilistic in the sense that it gives the correct answer with high probability.

III. MODIFIED QUANTUM SEARCH ALGORITHM

Consider a search space *D* of $N = 2^n$ elements. If there is a single marked element in this search space, we can find that element by applying $O\left(\sqrt{N}\right)$ number of Grover's iteration on *D*. Assume that there is no marked element in the search space. A basic question arises. "What will be the number of oracle queries required to know about the absence of the marked element in the search space?" Before doing Grover's iteration, we have to initialize the search space, that is, to create equal superposition of states. It is done by applying the Walsh- Hadamard operator *H*. For a single qubit, it is represented by the following matrix:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{1}$$

i.e., a bit in state $|0\rangle$ is transformed into a superposition in two states: $\left(1/\sqrt{2}, 1/\sqrt{2}\right)$. Similarly a bit in state $|1\rangle$ is transformed to $\left(1/\sqrt{2}, -1/\sqrt{2}\right)$; i.e., the magnitude of the amplitude in each state is $1/\sqrt{2}$, but the phase of amplitude in the state $|1\rangle$ is inverted. For a search space of dimension $N = 2^n$, we can perform *H* on each bit independently in sequence thus changing the state of the system. This superposition can be obtained in $O(\log N)$ steps. The matrix representing this operation will be of dimension 2^n x 2^n. If all *n* bits are in state $|0\rangle$, the resultant configuration will have identical amplitude of $2^{-n/2}$ in each of the 2^n states. Now start with Grover's iteration:

$$Q = -H^{\otimes n} R_0^{\pi} H^{\otimes n} R_{f(x)=1}^{\pi} \tag{2}$$

Each quantum mechanical step consists of an elementary unitary operation. The phase transformation operator R_0^{π} , rotates the state $|00...0\rangle$ by π radians. For single qubit state, it takes the form:

$$R_0^{\pi} = -|0\rangle\langle 0| + \sum_{x \neq 0} |x\rangle\langle x| \tag{3}$$

While the function of phase rotation operator $R_{f(x)=1}^{\pi}$ is to rotate the marked element by a phase of π radians and is defined by

$$R_{f(x)=1}^{\pi} = \sum_x (-1)^{f(x)} |x\rangle\langle x| \tag{4}$$

If there is no marked element, the phase rotation operator is just an identity operator i.e.

$$R_{f(x)=1}^{\pi} = \sum_x |x\rangle\langle x| = I \tag{5}$$

Grover's iteration reduces to

$$Q' = -H^{\otimes n} R_0^{\pi} H^{\otimes n} \tag{6}$$

Now if we apply Q' on the search space, with same amplitude of all the elements, it has no effect and the search space remains in an equal superposition of states. Hence it may be concluded that by using a single query it can be found whether the marked element is present or not in the search space. Our fast quantum search algorithm is based on this observation. In this algorithm, we split the main register into small sub-registers. First we look for the sub-register that contains the marked element by linear search method. Once we find the sub-register containing the marked element, then we have to apply Grover's iteration only on that sub-register and as result we require less number of queries to reach the desired element as compared to the Grover's original quantum search algorithm.

In order to describe the operation of the algorithm we first introduce a register, $|x\rangle = |x_1, x_2 \cdots x_n\rangle$, of *n*-qubits, and an ancillary qubit, $|q\rangle$ .We also introduce a quantum oracle, a unitary operator *O*. The oracle performs the following unitary operation on computational basis states of the register $|0\rangle$ and of the ancillary $|q\rangle$. That is,

$$O|x\rangle|q\rangle = |x\rangle|q \oplus f(x)\rangle \tag{7}$$

Where $\oplus$ denotes the addition modulo 2. The oracle recognizes marked state in the sense that if $|x\rangle$ is a marked element of the search space, $f(x)$ =1, the oracle flips the ancillary qubit from $|0\rangle$ to $|1\rangle$ and vice versa, while for unmarked state the ancillary is unchanged. Thus, the only effect of the oracle is to apply a phase of -1 if *x* is a marked state and no phase change if *x* is unmarked.

A. *The Algorithm*

This algorithm can be summarized as follows:

Inputs: 1- A black box oracle *O*, whose action is defined by Eq. (7)

2- *n* +1 qubits in the state $|x\rangle\ |0\rangle_q$.

Output: 1- A candidate for a marked $|m\rangle$.

B. *Procedure*

1-Initialize the system to the superposition $\left(1/\sqrt{N}, 1/\sqrt{N}, \cdots 1/\sqrt{N} \right)$; that is amplitude of all states is same. It is done by applying Hadamard gate to each qubit in the register, and the gate *HX* to the ancilla, where *X* is the NOT-gate. The matrices are written with respect to the computational basis$\left(|0\rangle,\ |1\rangle \right)$. The resulting state is

$$\frac{1}{\sqrt{N}} \sum_x |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)_q \tag{8}$$

This superposition can be obtained in $O\left(\log N\right)$ steps.

2- Split the register $\left|x\right\rangle=\left|x_1,x_2\cdots x_n\right\rangle$ into M numbers of equal size sub-registers, such that $\left|x\right\rangle=\left|y_1,y_2\cdots y_M\right\rangle$.

3- Search the sub-register having the marked element. It is done by applying Grover's iteration Eq. (1) on each sub-register one by one. First, apply the Grover's iteration on sub-register y_1 and select y_1, if the amplitude of elements is changed. Reject it if remains in equal superposition state. Continue this process successively on the sub-registers of the register $\left|x\right\rangle$, until a sub-register is found in which the amplitude of one element is changed. On average, selection of desired sub-register requires $M/2$ oracle queries.

4-Apply Grover's iterations on the selected sub-register k times, where $k=\frac{\pi}{4}\sqrt{N/M}$ and at this point the probability of finding the marked state will be a maximum. Now the total number of queries required to search the marked state is given by

$$k=\frac{\pi}{4}\sqrt{\frac{N}{M}}+\frac{M}{2} \tag{9}$$

5- Measure the selected sub-register in the computational basis.

From Eq.(7), it is clear that in step-2 the precise number of sub-registers is important. Table 1 shows the required number of queries, for different numbers of sub-registers and for different sizes of registers.

TABLE I NUMBER OF QUERIES REQUIRED FOR DIFFERENT SIZED REGISTERS AND NUMBER OF SUB-REGISTERS (SEE TEXT FOR DETAILS)

N0. of Sub-register	No. of queries required for different size of register											
	2^9	2^{10}	2^{11}	2^{12}	2^{13}	2^{14}	2^{15}	2^{16}	2^{17}	2^{18}	2^{19}	2^{20}
2^1	13.56	18.76	26.12	36.53	51.24	72.05	101.48	143.10	201.96	285.20	402.92	569.40
2^2	10.88	14.56	19.76	27.12	37.53	52.24	73.05	102.48	144.10	202.96	286.20	403.92
2^3	10.28•	12.88•	16.56•	21.76	29.12	39.53	54.24	75.05	104.48	146.10	204.96	288.20
2^4	12.44	14.28	16.88	20.56•	25.76•	33.12•	43.53	58.24	79.05	108.48	150.10	208.96
2^5	19.14	20.44	22.28	24.88	28.56	33.76	41.12•	51.53•	66.24•	87.05	116.48	158.10
2^6	-	-	-	38.28	40.88	44.56	49.76	57.12	67.53	82.24•	103.05•	132.48•
2^7	-	-	-	-	-	-	76.56	81.76	89.12	99.53	114.24	135.05
2^8	-	-	-	-	-	-	-	-	-	153.12	163.53	178.24

Analysis shows that required numbers of queries are minimum for the number of sub-registers $M=2^{\lfloor n/3\rfloor}$, where, $\left[n/3\right]$ is the smallest integer value. Hence, each sub-register will be consisting of elements $2^{n-\lfloor n/3\rfloor}$.

Now Eq. (9) takes the form

$$k=\frac{\pi}{4}\sqrt{\frac{N}{2^{\lfloor n/3\rfloor}}}+\frac{2^{\lfloor n/3\rfloor}}{2} \tag{10}$$

As $N=2^n$, so

$$k=\frac{\pi}{4}\sqrt{\frac{N}{2^{\lfloor n/3\rfloor}}}+\frac{2^{\lfloor n/3\rfloor}}{2}=\frac{\pi+2}{4}\left(N\right)^{1/3} \tag{11}$$

The above relation gives good results if the number of qubits n in the search space is a multiple of 3. There is little discrepancy in the result when n is not multiple of 3. It is due to the fact that we take smallest integer value of $\left[{}^{n}\!/_{3}\right]$ in selecting the number of sub-registers. This discrepancy can be removed by introducing a factor μ in the Eq. (11) that is

$$k=\frac{\pi+2}{4}\mu\left(N\right)^{1/3} \tag{12}$$

Analysis shows that the value of μ is

$\mu=0.9943027$ for $n=1,4,7,10,\cdots$

$\mu=1.0144727$ for $n=2,5,8,11,\cdots$

Hence, our Algorithm requires fewer queries as compared to Grover's algorithm, a comparison that is illustrated in Fig. (1).

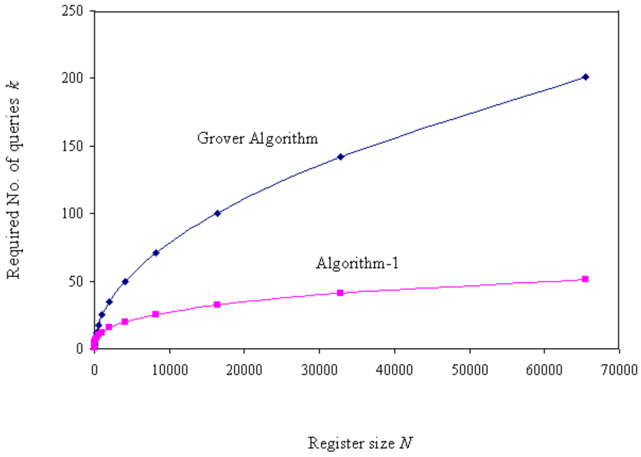

Fig. 1 Performance of Grover's algorithm and the one described in this paper

A comparison of Grover's algorithm and our modified algorithm is given below:

GROVER'S ALGORITH

1	Search Space of dimensions $N=2^n$
2	Register with n-qubits: $\left|x\right\rangle=\left|x_1,x_2\cdots x_n\right\rangle$
3	Prepare the initial state by applying Walsh-Hadamard operator in $O\left(\log N\right)$ steps
4	Apply Grover's Iteration $Q=-H^{\otimes n}R_0^{\pi}H^{\otimes n}R_{f(x)=1}^{\pi}$ to find marked element
5	$k=\frac{\pi}{4}\sqrt{N}$ number of total queries needed to find marked element
6	Measure the final state

MODIFIED ALGORITH

1	Search Space of dimensions $N=2^n$

2	Register with n-qubits: $\left\|x\right\rangle = \left\|x_1, x_2 \cdots x_n\right\rangle$
3	Prepare the initial state by applying Walsh-Hadamard operator in $O\left(\log N\right)$ steps
4	Split the register in $M = 2^{\lfloor n/3 \rfloor}$ numbers of sub-registers: $\left\|x\right\rangle = \left\|y_1, y_2 \cdots y_M\right\rangle$
5	Each sub-register will have $2^{n-\lfloor n/3 \rfloor}$ number of elements
6	Apply Grover's iteration $Q = -H^{\otimes n} R_0^{\pi} H^{\otimes n} R_{f(x)=1}^{\pi}$ on each sub-register
7	$M/2$ number of queries needed to find the sub-register with marked element
8	Apply Grover's iteration $Q = -H^{\otimes n} R_0^{\pi} H^{\otimes n} R_{f(x)=1}^{\pi}$ to the selected sub-register $k = \frac{\pi}{4}\sqrt{N/M}$ times
9	$k = \frac{\pi + 2}{4}\left(N\right)^{1/3}$ number of total queries needed to find marked element
10	Measure the selected sub-register

IV. RESULTS AND DISCUSSION

Consider a search space of dimension $N= 2^n$. In order to find the marked element one needs $O\left(\sqrt{N}\right)$ number of queries, in its exact form $\frac{\pi}{4}\sqrt{N}$ queries. Now if we divide the register in M numbers of sub- registers, one of the sub register will have a marked element. If for example there is no marked element, the Phase Rotation Operator will just be an identity operator, application of Grover's iteration will have no effect, and search space will remain in an equal superposition of states. But if we have a marked element only one application of Grover's iteration, on M sub-registers, will allow us identify the sub-register having the marked element. Because only the sub-register has marked element, the Phase rotation operator will change the phase of marked state by π and one application of Grover's iteration will increase the amplitude of marked state. This process is like a linear search, and on average by $M/2$ queries we can identify the sub-register with the marked element. Now we have to apply Grover's iteration only on the selected sub-register $\frac{\pi}{4}\sqrt{N/M}$ times. It is found that the required numbers of queries are a minimum if the number of sub-registers is $2^{\lfloor n/3 \rfloor}$, where [n/3] is the smallest integer value. It can be explained with the help of Table 1. The first column of the table shows number of sub-register from 2^1 to 2^8, while first row indicates the size of register, which starts from 2^9 to 2^{20}, all other rows show the number of queries required for different sizes of the register. In the fourth row, for the number of sub- register equal to 2^3, number of queries are 10.28 for size of register 2^9 , 12.88 for 2^{10} and 16.56 for 2^{11}, second, third and forth columns respectively. These are the minimum values for the sizes of the register. The size of register 2^9 means n=9 which implies M=9/3 =3, while n=10 means M=10/3= 3.33 and similarly for n=11. For n=12 we get M= 12/3= 4 and one can see from forth row, for sub register M= 2^4, that number of queries are minimum for size of register 2^{12}, 2^{13} and 2^{14}, given in columns 5, 6 and 7, respectively. These minimum queries terms are highlighted with * as a superscript on each term. Hence, we can say if the number of n is a multiple of 3, then we get accurate result; but if it is not a multiple, then there is a little discrepancy which is removed by introducing a factor of μ in Eq. (12).

V. CONCLUSIONS

We studied the effect of Grover's iteration on a search space, with same amplitude of all elements concluding that by using a single query it can be known whether marked element is present or not in the search space. Based on this finding, we have proposed a fast quantum search algorithm. It has been shown that by using the same technique as Grover's algorithm but dividing the register with N elements into M sub-registers, we can find a marked element in $O\left(\left[\,(\pi+2)/4\,\right]N^{1/3}\right)$ steps instead of $O\left(\sqrt{N}\right)$ as in Grover's algorithm.

REFERENCES

[1] R. P. Feynman, *Int.J. Theor. Phys.* 21, 467-488 (1982).

[2] A. Elitzur and L. Vaidman, *Found. Phys.* 23, 987-997 (1993).

[3] D. P. Divincenzo, *Science*, 270, 255-261 (1995).

[4] V. Sahni and V. Lakshminarayanan, "*Quantum Information Science*", Tata McGraw Hill, New Delhi, (2010).

[5] P.W. Shor, *Phys. Rev.* A 52, 2493-2496, (1995).

[6] A. Barenco, *quant-ph*/9612014, (1996).

[7] L.K. Grover, Am. *J. Phys.* 69, 769-777 (2001).

[8] N.D. Mermin, Am. *J. Phys*. 71, 23-30 (2003).

[9] L.K. Grover, in Proceedings of the "*Twenty-Eight Annual Symposium on the Theory of Computing*", Philadelphia, Pennsylvania (ACM Press, New York) 212-218, (1996).

[10] P.W. Shor, in proceedings of the Symposium on the foundations of Computer Science, 1994, Los Alamitos, California (IEEE Computer Society Press, New York) 124-134, (1994).

[11] L.K. Grover, *Phys. Rev. Lett.* 79(2), 235-243, (1997).

Imrana Asharf is working as an Associate Professor at the Department of Physics, Quaid -i-Azam Uuniversity, Islamabad. She has done her PhD in the field of Quantum Optics. The title of her thesis is "QUANTUM THEORY OF THE TWO-PHOTON MICROMASER AND LASER ". She is winner of ICO/ICTP Prize for year 2004. She is a regular visitor of ICTP and has been a Regular Associate at ICTP from 2000 -2008 and recently awarded Senior Associate-ship at ICTP from year 2012 to 2017. From past many years she is actively involved in Preparatory school to the Winter College on Optics at ICTP. Her area of interest is Quantum Optics, Atom optics and Quantum Information.

Mr. Tariq Mahmood has done his M.Phil under the supervision of Dr. Imrana Ashraf from Department of Physics, Quaid-i-Azam University, Islamabad Pakistan. Title of his Thesis is "STUDY OF GROVER'S QUANTUM SEARCH ALGORITHM". He has permanent position at Department of Physics, Hazara University Mansehra, Pakistan, as Lecturer since April, 2006. Presently he is enrolled as PhD student in the Institute of Theoretical Physics, Leibniz University Hannover Germany. His area of research is: Quantum Algorithms, Quantum Channels, Quantum Cryptography.

V. Lakshminaryanan is currently a full professor of optometry (vision science), physics and electrical and computer engineering at the University of Waterloo. He is also an associate of the Michigan Center for Theoretical Physics at Ann Arbor. He has held research/ teaching positions at the University of California at Berkeley and Irvine campuses as well as the University of Missouri. He has been a KITP Scholar at the Kavli institute for Theoretical Physics at Santa Barbara. He is a fellow of the American Physical Society, American Association for the Advancement of Science, Optical Society of America, SPIE-The international society for optical engineering, etc. He has received numerous awards and honors, most recently the Educator award from SPIE and the Optics medal from the Optical Society of India. He is currently a topical editor or section editor for Optics Letters, Journal of Modern Optics, and American Journal of Bioengineering. He has published widely in areas ranging from biomedical engineering, quantum chemistry, vision science, ophthalmology as well as optical physics.