The Effect of Sample Property on Optimum Search by Quantum Computing

Hamed Edalati Fard, Majid Vafaei Jahan, Mehrdad Jalali
Department of Computer Engineering
Mashad Branch, Islamic Azad University
Mashad, Iran
hamed.edalati@gmail.com, VafaeiJahan@mshdiau.ac.ir, mehrdadjalali@ieee.org

***Abstract*—Quantum computers are designed based on quantum mechanics. They have special features such as entanglement and parallelism, which do not exist in classic mechanics-based computers. Therefore, quantum algorithms have their own privilege for solving some problems compare to classic ones such as finding the minimum value of a function in optimization problems. For instance, finding the minimum of *N* elements in quantum method is faster than classic method. In this case, having information about *N* elements of distribution does not reduce the cost of finding the minimum value in classic method due to linear search of each element. But in quantum method, all elements are simultaneously considered as well as distribution information, which is related to the whole elements. This distribution information effectively influences on finding the minimum value. Numerical simulations show having mean and variance of *N* elements can reduces the cost of minimum finding through quantum method by %40. Furthermore, it is shown the greater variance causes less cost.**

Keywords- optimization; quantum search; adaptive search; sample distribution; mean; variance.

I. INTRODUCTION

The concept of quantum computers was presented in early 1980s. These types of computers are like classic computers with this difference that their base of working is quantum mechanics instead of classic one . In late 1980s and early 1990s, it was shown that quantum computer power in solving some specific problems is higher than classic computers. In 1994, Shor showed that a quantum computer can solve the known problem of "decomposition of an integer number *N* to prime factors" in a time order of polynomial *log N*. Whereas, for this problem about classic computers, there is no efficient known algorithm [1]. In 1996, Grover presented an algorithm could find an element among *N* unordered elements with the time order of O(√*N*). The equivalent classic algorithm of this action is of order O(*N*) [2]. By using this capability, a quantum algorithm for finding the minimum element between *N* elements is presented that is of order O(√*N*) versus time order O(*N*) of its equivalent classic algorithm. The main core of this algorithm is Grover's Search (GS) which in proper times is called in this algorithm. In this text, it is shown that by knowing mean and variance of *N* elements and using it in quantum algorithm of finding minimum, it could reduce search cost. In section II, some primal concepts of quantum computations are presented. GS which has an extensive application in most quantum computation has been completely described in section III. GS application in optimization problems is studied in section IV. In section V, it is shown that by applying mean and variance of sample's distribution, it is possible to reduce the cost of finding minimum. Section VI is composed of simulation results of a quantum algorithm of finding minimum. Conclusion is presented in section VII.

II. PRIMAL CONCEPTS OF QUANTUM COMPUTATIONS

In this section, some primal concepts of quantum computations are presented [4]. The basic unit of information in quantum computing is called qubit, which is the abbreviation of quantum bit. A bit can be 0 or 1 in a usual computer. A qubit can also be in $|0\rangle$ or $|1\rangle$. Furthermore, it can take a state called superposition. This state is a linear combination of states $|0\rangle$ and $|1\rangle$. If this state is called $|\psi\rangle$, a superposition is written as:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{1}$$

Here α and β are complex numbers such that:

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2}$$

Since, a qubit can be a superposition of states $|0\rangle$ and $|1\rangle$, whenever a measurement to be done, the same result wouldn't be reached. In fact, when a qubit is measured, only it can be found in one of the states $|0\rangle$ or $|1\rangle$. Quantum mechanic laws tell us absolute squares of α and β in (1)

would be the probability of finding a qubit in state $|0\rangle$ or $|1\rangle$. In other words,

$|\alpha|^2$ gives us the probability of finding $|\psi\rangle$ in state $|0\rangle$.

$|\beta|^2$ gives us the probability of finding $|\psi\rangle$ in state $|1\rangle$.

Because the information unit in quantum computation is qubit, a range in which quantum computations are located in mathematical concept is a vector space. This expresses that quantum states to behave mathematically as same as physics vectors. Therefore, vector space is applied here. Vectors of this space often have common fundamental properties of physics vectors, such as having a length. Showing information in a vector form of basic states, gives an important capability to quantum computers. This capability called quantum parallelism causes quantum algorithms rate to increase in comparison with other classic algorithms. A quantum register like an n bit classic register is an array of n qubits. A quantum system can be manipulated by using quantum gates. In fact, these gates are unitary matrices that are imposed on quantum states (vectors). Each quantum computation consists of three following parts:

1. Preparing a quantum register in an initial well defined state $|\psi_0\rangle$.
2. Manipulating the initial state $|\psi_0\rangle$ by using a sequence of gates until final state $|\psi_f\rangle$ to be reached.
3. Measuring the final state $|\psi_f\rangle$.

III. GROVER QUANTUM SEARCHING ALGORITHM

Let n be a positive integer number and $S=\{0,1\}^n$, such that the domain length to be $N=2^n$. It is supposed $h: S \to \{0,1\}$. We wish to find a point $u \in S$ that $h(u)=1$. Also, it is supposed that h is an oracle. It means that recognition about is just possible by sampling (evaluating) it and there is no information about its structure.

By classic computations, the logic function *h* can be implemented as a sub-procedure. For instance, a classic logic circuit that has taken a sequence of bits as a representative of a point in *S*, results in its dependent value of *h*. This sub-procedure can be performed successfully on all points of *S* until a considered point to be found. This classic program needs an average of *N/2* evaluations to find a determined *p* point.

In quantum computing, the circuit implementing *h* (using gates that work with qubits) inputs and outputs superpositions. Hence, many feasible solutions would be observed in an instance. On a quantum computer, observing the output, changes the output value to a classic bit sequence. This action is done with respect to a specified probability distribution by superposition. Thereafter, without a need to use a loop on *N* points of *S*, a quantum computer can work on a superposition of these *N* points.

Algorithm(1): Grover quantum search algorithm.

1. Initialize the system to the distribution: $\left(\frac{1}{\sqrt{N}},\frac{1}{\sqrt{N}},\frac{1}{\sqrt{N}},\ldots,\frac{1}{\sqrt{N}}\right)$, i.e. there is the same Amplitude for be in each of the N states.
2. Repeat the following unitary operations $O(\sqrt{N})$ times:
   (a) Let the system be in any state S:
   In case $C(S)=1$, rotate the phase by π radians;
   In case $C(S)=0$, leave the system unaltered.
   (b) Apply the diffusion transtorm D which is defined by matrix D as follows:
   $$D_{ij}=\frac{2}{N} \text{ if } i \neq j \quad \& \quad D_{ii}=-1+\frac{2}{N}$$
   This diffusion transform, D, can be implemented as $D=WRW$, where R the rotation matrix & W the Walsh-Hadamard Transform Matrix are defined as follows:
   $$R_{ij}=0 \text{ if } i \neq j;$$
   $$R_{ii}=1 \text{ if } i=0;$$
   $$R_{ii}=-1 \text{ if } i \neq 0$$
   $W_{ij}=2^{-n/2}(-1)^{\bar{i}.\bar{j}}$ where $\bar{i}$ is the binary representation of i, and $\bar{i}.\bar{j}$ denotes the bitwise dot product of the two n bit strings $\bar{i}$ and $\bar{j}$.
3. Sample the resulting state. In case $C(S_v)=1$ there is a unique state S_v such that the final state is S_v with the probability of at least $\frac{1}{2}$.

The set of considered points is represented by $M=\{u \in S | h(u)=1\}$ and the number of these objective points is represented *t*. We may or may not be aware of the value of *t*. Grover introduced the "Grover's rotation" operator, which incorporates the oracle for *h* and provides a means of implementing a certain phase-space rotation of the states of a quantum system encoding points in the domain *S*. By repeating these rotations, it can reach from a state with equal amplitude state (which is simple to prepare within a quantum computer) toward the states encoding the unknown marked points. More details are given in [2, 5, 6]. A Grover search with *r* rotations performs *r* times Grover's rotation operator on a superposition of those states with the same domains, then the output is observed.

Most of the performed operations in implementing Grover rotation operator is related to requesting from oracle, so the cost of a Grover search with *r* rotations is considered equivalent to the cost of *r* requests from oracle. The output is a point of *S*, and if someone wants to know whether the resulting output is in *M* or not, one more request from oracle (for operating on that point) gives function's value of *h*.

Maybe, applied oracle computations in GS seem vague. From computer science researchers' point of view, an oracle is just a fictitious mathematical device that permits them to estimate the computational cost of some algorithms with respect to "the number of oracle recalls". For GS, it allows them comparing relative costs of classic unstructured search and quantum unstructured search with respect to the number of oracle recalls. During implementing unstructured search on real problems, oracle, which has an explicit pre-awareness of solution is replaced with a studying and testing procedure of a polynomial (or better) order. This studying and testing procedure recognizes solutions implicitly through properties which a correct solution should have had. These studying and testing procedures can be different completely from one problem to another. So the use of the oracle in GS is really only a proxy for such a testing procedure in which, we assume, arbitrarily, that there is a unit cost per call to the oracle [7].

A. *Some points about GS*

1) Grover showed [2] if exactly one point is being considered, in this case, for finding that point, only $\pi/4\sqrt{N}$ rotations are required.

2) Optimality of GS was proven in [8]. It means that any other quantum algorithms which are being applied for unstructured search have to perform oracle recall at least to the times of oracle recall in GS.

3) Implementing this algorithm in contrast to other quantum algorithms is simpler. Because, Walsh-Hadamard transformation and conditional phase change operator are used in it, which implementing them is simpler to necessary transformations in other algorithms.

4) It is shown that for obtaining to a correct result, number of GS iterations has to be exactly $\pi/4\sqrt{N}$ [5], otherwise the probability of finding the correct solution decreases. In figure (1), the oscillations of GS success probability by increasing the number of iterations is shown [7]. This figure is a result of searching an objective option among 2^{10} options. As it is observed, the first high probability of success is reached after $\pi/4\sqrt{2^{10}} \approx 25$ iterations of the algorithm and after that this probability decreases.

5) In quantum unstructured search, if *k* objective options are being looked for among *N* options (*k* is known), then GS has to be performed exactly $\pi/4\sqrt{N/k}$ times until reaching success [5]. If *k* is unknown, but it is known that $k \geq k_0$, $\pi/4\sqrt{N/k_o}$ iterations of GS for reaching the success is enough.

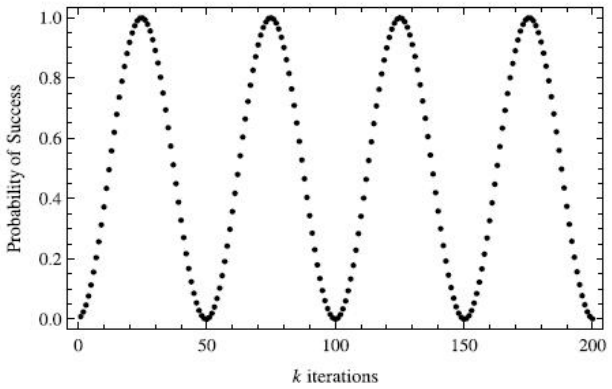

Figure 1. The probability of success as a function of the number of steps of amplitude amplification for a problem having one solution amongst 2^{10} possibilities.[7]

IV. GS APPLICATION IN GLOBAL OPTIMIZATION

Quantum computing have a high capability for increasing efficacy of stochastic global optimization methods. GS could be used for solving a specific optimization problem of "finding global minimum" [10]. With the assumption of an objective function $f : S \to \Re$ and a point like $X \in S$ with $f(X)=Y$, improvement region for function *f* is defined as:

$$IR_f = \{w \in S : f(w) < Y\} \tag{3}$$

It is trivial that $|S| > |IR_f|$. Therefore, the probability of finding minimum in an improvement region is more than the region *S*.

$$\frac{1}{|S|} < \frac{1}{|IR_f|} \tag{4}$$

If a sequence of improvement regions is generated, at last an improvement region is generated whose members are the minimum value of function *f*. for generating these improvement regions, it is possible to use GS. GS needs an oracle; a quantum circuit which to be able categorizes points $w \in S$ from the aspect of belonging to objective set [11]. The logic function $h(w)=(f(w)<y)$ would be this oracle. In fact, *h* is simply a quantum circuit of a black box whose output at a point w in *S* (or a hyper state of these points) is defined as:

$$h(w) = \begin{cases} 1 & ; \quad f(w) < y \\ 0 & ; \quad f(w) \geq y \end{cases} \tag{5}$$

If GS uses above oracle, the output before measurement is an improvement region and after measurement is a random point of the improvement region.

This method is called Grover adaptive search (GAS) method [6]. At first, the algorithm selects a sample from the domain uniformly and assesses the objective function at that point. At each subsequence of iterations, the algorithm evaluates the objective function at the determined point by GS. GS uses the best observed function value so far as the threshold. This algorithm is given as a semi-code here [10]:

Algorithm(2): Grover Adaptive Search (GAS).

1. Generate X_1 uniformly in S, and set $Y_1 = f(X_1)$.
2. For $n = 1,2,\ldots$ until a termination condition is met, do:
   (a) Perform a Grover search of r_n rotations on f with threshold Y_n, and denote the outputs by x and y.
   (b) If $y < Y_n$, set $X_{n+1} = x$, $Y_{n+1} = y$,
   Otherwise, set $X_{n+1} = X_n$, $Y_{n+1} = Y_n$.

GAS is compatible with a developed adaptive search framework [12, 13, 14, 15, 16]. It has been proven that this framework is useful for studying convergence theory of stochastic global optimization methods. Hypothesis of all adaptive algorithms is that improvement points can be found. GS can find existing points of an unknown objective set by an oracle. This capability of GAS is resulted from making an objective oracle for the current improvement region at every iteration. In this method, a sequence of domain's points is generated that were distributed uniformly in the previous improvement region. This sequence converges too fast to global optimum. Actually, all the algorithm work is done in the last step, when GS is performed by a threshold a little larger than the global minimum [10].

V. EFFECT OF SAMPLE DISTRIBUTION IN OPTIMIZATION

For finding the minimum element among *N* numbers in classic case, if it is known that the minimum point has been repeated *t* times through elements, this information doesn't have any effect on the cost of finding the minimum. In quantum case, with the mentioned assumption, the cost of finding the minimum decreases from $O(\sqrt{N})$ to $O(\sqrt{N/t})$. It can conclude that by having general information of sample, it is possible to decrease search cost. In GAS algorithm, first, by selecting a random element between *N* elements, an objective region is generated. At each of iterations of GAS, objective region becomes smaller until this region to have only one element, which is that objective element. The proposed method in improving the cost of executing GAS algorithm is that instead of a random element, an element to be selected that to accelerate the convergence of objective function toward the objective elements. For this reason, the mean difference and the variance are used as the estimations for the minimum element. According to definition of mean and variance the primary objective region to the objective region generated randomly would be smaller. Therefore, the cost of finding minimum will decrease. Since, computing the variance and mean for applying in finding the minimum increases the algorithm total cost of finding the minimum, this approach for problems in which the variance and the mean of samples are given as the initial data or problem assumptions would be very effective. This method is called improved Grover adaptive search (IGAS). Semi-code of this algorithm is as following in algorithm (3).

Assuming $S_1,S_2,\ldots$ is a sequence of generated improvement regions by GAS and $T_1,T_2,\ldots$ is a sequence of generated improvement regions by IGAS. Because threshold value Y_i in IGAS to GAS is accounted for a better approximation of the minimum element, so the probability of finding the minimum in T_i would be higher than S_i, and the sequence $\{T_n\}$ would converge sooner than $\{S_n\}$. Consequently, by assumption of having the mean and variance of *N* numbers, the cost of finding the minimum of these *N* numbers by IGAS method would have less cost than GAS method.

Algorithm(3): Improved Grover Adaptive Search (IGAS).

1. Set $Y_1 = mean(S) - \mathrm{var}(S)$.
2. For $n = 1,2,\ldots$ until a termination condition is met, do:
   (a) Perform a Grover search of r_n rotations on f with threshold Y_n, and denote the outputs by x and y.
   (b) If $y < Y_n$, set $X_{n+1} = x$, $Y_{n+1} = y$,
   Otherwise, set $X_{n+1} = X_n$, $Y_{n+1} = Y_n$.

VI. NUMERICAL SIMULATION

Computer simulation as a method has been accepted in many science and engineering fields. Today computers can be applied for simulating relatively small quantum computers (about 24 qubits). For this reason, nowadays, quantum computation theoretical ideas cannot be performed like executed numerical computations on current supercomputers. Current computers can be an abstract model of an ideal quantum computer from the simulation aspect. Moreover, they are able to simulate the hardware physical functions of a quantum computer [17].

In order to simulate a quantum multi-part system while the parts have interactions with each other, problems will grow exponentially alongside the growing quantum system. This has been clearly obvious in quantum statistical mechanics and also quantum chemistry. In fact, this phenomenon imposed a question for Feynman that what kind of computer is required to prevail over exponential growth? He concluded that only a quantum computer can simulate itself thoroughly [18]. Therefore, most of the performed simulation on the theoretical studies or even implementation emphasize the small scales [19-24], since the purpose is presenting the potentials and capabilities of quantum computations.

In GS based algorithms, the cost of an algorithm is determined with the number of GS's rotations. Since GS is the main core of the quantum algorithm for finding the minimum, without a quantum computer only by using a classic computer and also considering the number of rotations, it is possible to obtain the cost of executing the algorithm. Therefore, in order to compare two methods GAS and IGAS for finding the minimum, the number of rotations in each method is required. In this case, the number of rotations has been obtained by numerical simulation with MATLAB on a classic computer.

A. *Simulation results*

1) Simulating by a fixed sample

A random sample of $N=2^n$ (n is the number of qubits and $2\leq n\leq 12$) with normal distribution $N(0,1)$ is generated and GAS and IGAS algorithms for finding the minimum on this sample are executed for 100 times. The search cost for every algorithm is considered the number of rotations done for finding the minimum. The average number of required rotations for finding the quantum minimum is given in figure 2.

2) Simulating with different samples

GAS and IGAS algorithms are performed 100 times on samples having $N=2^n$ (n is the number of qubits and $2\leq n\leq 12$) generated elements of normal distribution $N(0,1)$. The average number of required rotations for finding the quantum minimum is represented as the average cost of GAS and IGAS algorithm separately in figure 3.

As the figures 2 and 3 show, on average the number of rotations in IGAS is %40 less than GAS. In another word, the cost of finding the minimum with IGAS algorithm is about %40 less than GAS algorithm's.

3) Simulating with constant mean and variable variance

$N=1024$ random numbers with normal distribution of mean 0 and variance between 0, 1 to 2 are generated for 1000 times and GAS, and IGAS algorithms are performed on them in order to find the minimum, which the results are given in figure 4.

VII. CONCLUSIONS

GS time order is $O(\sqrt{N})$ by using this algorithm, especially in finding the minimum. GAS is one of the quantum algorithms for finding the minimum applies GS as the main core. The proposed IGAS algorithm uses the difference of mean and variance instead of selecting the threshold element randomly. IGAS to GAS spends less cost to find the minimum in the first step, because in the first step, its objective set would be smaller than GAS's which it leads to accelerate converging to the minimum element to GAS.

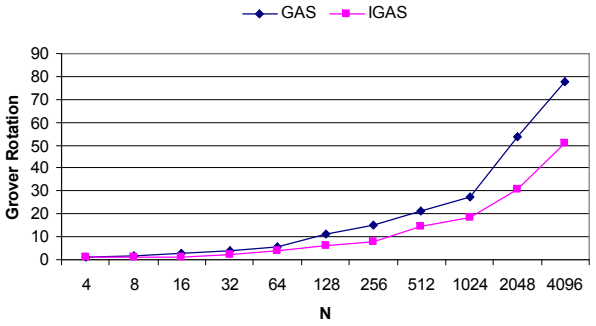

Figure 2. Comparing the average cost of finding the minimum element among N constant element of GAS and IGAS.

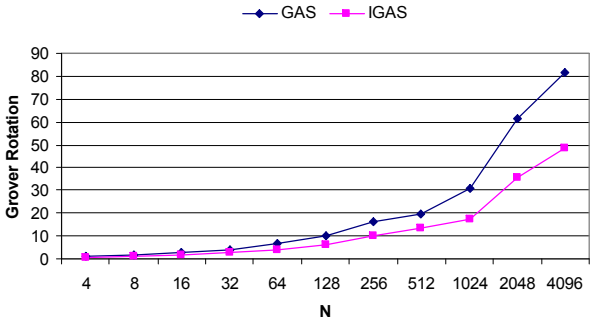

Figure 3. Comparing the average cost of finding the minimum element among N elements of GAS and IGAS.

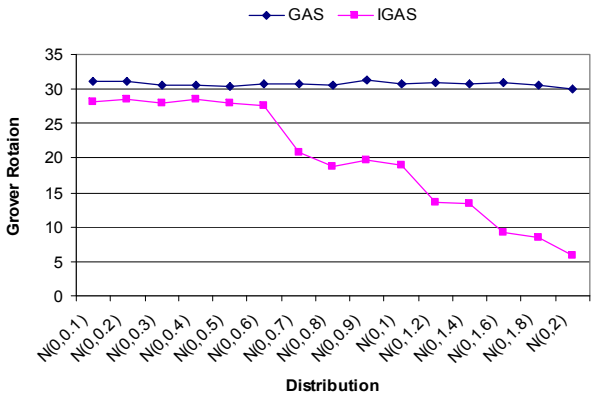

Figure 4. Comparing the average cost of GAS and IGAS for N=1024 elements with constant mean and variable variance.

Numerical simulations show that the cost is decreased around %40 of GAS's cost. This result confirms the proposed idea in IGAS for improving the cost of performing the algorithm of finding the quantum minimum.

In addition, it is observed that more dispersions of elements (larger variance), less cost in finding the minimum by IGAS, whereas, this dispersion has no effect on finding the minimum by GAS. Unlike, classic algorithms that the searched being sample distribution don't affect on the cost of finding the minimum, by using the quantum algorithms and

sample distribution characteristics, it can decrease the search cost of finding the minimum which is important in optimization problems.

Applying IGAS algorithm is not sufficient while mean and variance are not available since computing the mean and variance are costly. While data are too much, IGSA algorithm can be applied by using statistical sampling methods and estimating mean and variance. Determining the efficiency and improvement of IGAS algorithm can be considered in the future. Moreover, because the normal distribution of mean 0 has been used in simulations, the question about the effect of sample distribution type can be studied in later works.

REFERENCES

[1] P. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring", Proc. 35th Annu. IEEE Symp. Foundations of Computer Science, IEEE, 1994, pp. 124–134.

[2] L. K. Grover,"A Fast Quantum Mechanical Algorithm for Database Search", Proc. 28th Annual ACM Symposium on the Theory of Computing, Philadelphia, 1996, pp. 212–219.

[3] C. Durr and P. Hoyer, "A Quantum Algorithm for Finding the Minimum", Available from: http://lanl.arxiv.org/abs/quant-ph/9607014, 1996. [Accessed 7 May 2011].

[4] D. McMahan, Quantum Computing Explained, John Wiley & Sons, 2008.

[5] M. Boyer, G. Brassard, P. Hoyer & A. Tapp, "Tight Bounds on Quantum Searching", 4th Workshop on Physics and Computation, 1996, pp.36-43.

[6] D. W. Bulger, W. P. Baritompa, and G. R. Wood, "Implementing Pure Adaptive Search with Grover's Quantum Algorithm", Journal of Optimization Theory and Application, Volume. 116, No. 3, 2003, pp. 517–529.

[7] C.P. Wiliams, Explorations in Quantum Computing, London: Springer-Verlag, 2010.

[8] C.Zalka, "Grover's Quantum Searching Algorithm is Optimal", Physical Review A, Volume. 60, No. 4, 1999, pp. 2746–2751.

[9] A. Andris, "Quantum Search Algorithms", ACM SIGACT News, Volume. 35, No. 2, 2004, pp. 22-35.

[10] W.P. Baritompa, D.W.Bulger and G.R.Wood , "Grover's Quantum Algorithm Applied to Global Optimization", SIAM Journal on Optimization, Volume. 15, No. 4, 2005, pp. 1170–1184.

[11] L. K. Grover, "A Framework for Fast Quantum Mechanical Algorithms", Proc. 30th Annual ACM Symposium on the Theory of Computing, Dallas, 1998, pp. 53–62.

[12] Z. B. Zabinsky and R. L. Smith, "Pure Adaptive Search in Global Optimization", Journal Mathematical Programming, Volume. 53, No. 3, 1992, pp. 323–338.

[13] G. R. Wood, Z. B. Zabinsky, and B. P. Kristinsdottir, "Hesitant Adaptive Search: The Distribution of the Number of Iterations to Convergence", Journal Mathematical Programming, Volume. 89, No. 3, 2001, pp. 479–486.

[14] D. W. Bulger, D. L. J. Alexander, W. P. Baritompa, G. R. Wood, and Z. B. Zabinsky, "Expected Hitting Time for Backtracking Adaptive Search", Optimization, Volume. 53, No. 2, 2004, pp. 189–202.

[15] Z. B. Zabinsky, G. R. Wood, M. A. Steel, and W. P. Baritompa, "Pure Adaptive Search for Finite Global Optimization", Journal Mathematical Programming, Volume. 69, No.3, 1995, pp. 443–448.

[16] D. W. Bulger and G. R. Wood, "Hesitant Adaptive Search for Global Optimization",Journal Mathematical Programming, Volume. 81, No. 1, 1998, pp. 89–102.

[17] H. De Raedt, K. Michielsen, "Computational Methods for Simulating Quantum Computers", In Handbook of Theoretical and Computational Nanotechnology, Volume. 3, pp. 2-48, American Scientific Publishers, 2004.

[18] R. Feynman, "Simulating Physics with Computers", International Journal of Theoretical Physics, Volume. 21, No. 6–7, 1982, pp. 467–488.

[19] J Bang, S Yoo, J Lim, J Ryu,C Lee, J Lee ,"Quantum Heuristic Algorithm for Traveling Salesman Problem" , Available from: http://arxiv.org/abs/1004.4124v1, 2010. [Accessed 7 May 2011].

[20] H.R. Moser, "The Quantum Mechanical Solution of the Traveling Salesman Problem", Physica E, Volume. 16, 2003, pp 280–285.

[21] T Hogg, D Portnov, "Quantum Optimization", Information Sciences, Volume. 128, 2000, pp 181-197.

[22] L.R.U. Manssur, R. Portugal, "Stochastic Simulation of Grover's Algorithm", Available from: http://arxiv.org/abs/quant-ph/0301077, 2003. [Accessed 7 May 2011].

[23] G.V. López, T. Gorin, L. Lara , "Quantum Computation in a Ising Spin Chain Taking into Account Second Neighbor Couplings ", International Journal of Theoretical Physics, Volume 47, No. 6, 2008 , pp. 1641–1653.

[24] G.V. López , L. Lara ,"Numerical simulation of a Controlled-Controlled-Not (CCN) quantum gate in a chain of three interacting nuclear spins system", Available from: http://arxiv.org/abs/quant-ph/0608147v2, 2006. [Accessed 7 May 2011].