Analysis and Simulation of Grover's Search Algorithm

Zhuang Jiayu, Zhao Junsuo, Xu Fanjiang, Hu Haiying, and Qiao Peng

***Abstract*—A quantum computation problem of quantum search is discussed in this paper. Grover's search algorithm, the most commonly used quantum search algorithm, is introduced in details. The flow of quantum search algorithm and the quantum circuit model are shown. And the error of the search value, as well as the probability of measurement, is analyzed. For further research we simulated the Grover's search algorithm in classical computer. By quantum simulator the probability distribution of the measuring result of search value is presented and the computational efficiency is discussed. The simulation result demonstrates the effectiveness of the proposed algorithm.**

***Index Terms*—Quantum computation, quantum search algorithm, grover's algorithm.**

I. Introduction

In the past few decades, we have gained more and more ability to access massive amounts of information and to make use of computers to store, analyse and manage this data. Recent studies have shown the great progress towards the physical realization of a quantum computer. Deutsch [1], [2] systematically described the first universal quantum computer that is accepted by now. In 1982, Benioff [3] studied the question whether quantum computer was more computationally powerful than a conventional classical Turing machine. He mapped the operation of a reversible Turing machine onto the quantum system and thus exhibited the first quantum-mechanical model of computation, which discovered the potential power of quantum computer. In 1994, American scientist Peter Shor [4] proposed an algorithm that factor a large integer in polynomial time, which is the first practical quantum algorithm.

In 1996, Grover [5], [6] proposed an algorithm that provides a speedup of $\sqrt{N}$ in order of magnitude than classic algorithm in searching an unsorted database. Although the purpose of Grover's algorithm is usually described as "searching a database", it may be more accurate to describe it as "inverting a function". Quantum computation and quantum information is the study of the information processing task that can be accomplished using quantum mechanical system. Quantum computation has many features that differ from classical computing in that quantum state has the characteristic of coherence and entanglement.

Grover's algorithm can also be used for estimating the mean and median of a set of numbers, and for solving the collision problem. In addition, it can be used to solve NP-complete problems by performing exhaustive searches over the set of possible solutions. This would result in a considerable speedup over classical solutions, even though it does not provide the "holy grail" of a polynomial-time solution.

Manuscript received July 9, 2013; revised December 3, 2013.

Zhuang Jiayu, Zhao Junsuo, Xu Fanjiang, and Qiao Peng are with the Science and Technology on Integrated Information System Laboratory, Institute of Software Chinese Academy of Sciences, Beijing, China (e-mail: jiayu@ iscas.ac.cn, junsuo@ iscas.ac.cn, fanjiang@ iscas.ac.cn, qiaopeng@ iscas.ac.cn).

Hu Haiying is with Shanghai Engineering Center for Microsatellites, Chinese Academy of Sciences, Shanghai, China.

II. Quantum Oracle

Grover's search algorithm dealt with a single object search in large unsorted database [7].

Consider the unstructured search of an unknown number a of items in a large unsorted database of size 2^n and there is an index to those elements which is just a number in the range 0 to $2^n - 1$.

A particular instance of the search problem can conveniently be represented by a function f, which takes as input an integer $x(0 \le x \le 2^n - 1)$. By definition, $f(x)$=1 if x is a solution to the search problem and $f(x)$=0 if x is not a solution to the search problem.

Suppose there is a quantum black box which can transform the quantum state x into $f(x)$. The quantum black box[8] is a unitary operation, defined by its action on the computational basis:

$$U: |x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$$

where $|x\rangle$ is the index register, $\oplus$ denotes addition modulo 2, and the Oracle qubit $|y\rangle$ is a single qubit which is flipped if $f(x) = 1$ and is unchanged otherwise.

If $|y\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, the action of the Oracle is:

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

This transform will showed in geometry projection is:

$$U_a = I - 2|a\rangle\langle a|$$

where a is the data which will be searched in Oracle.

III. The Procedure of Grover's Search Algorithm

In 1996, Grover discovered the quantum algorithm for identifying a target element in an unstructured search universe of N items in approximately $\pi/4\sqrt{N}$ queries to a quantum oracle. For classical search using a classical oracle, the search complexity is clearly of order $N/2$. It has been proven that this square-root speed-up is the best attainable performance gain by any quantum algorithm [9].

In Grover's algorithm [10], only $O(\sqrt{N})$ steps are needed. Grover's algorithm has two registers: n qubits in the first one and one qubit in the second. The first step is to create a superposition of all 2^n computational basis states. This is

achieved by initializing the first register in the state and applying the operator $H^{\otimes n}$, where H is the Hadamard gate.

Grover's search algorithm begins with the initialized state $|0\rangle^{\otimes n}$. Then the Hadamard transform is used to $|0\rangle^{\otimes n}$:

$$|s\rangle = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle$$

We create a unitary operator:

$$U_s = 2|s\rangle\langle s| - I$$

In geometry, it means any vector v immovability in the direction of $|s\rangle$ and reversed in the perpendicular direction of $|s\rangle$. The unitary operator $U = U_a U_s$ is defined. Apply U to any vector $|x\rangle$ is:

$$|\langle a|s\rangle| = \frac{1}{\sqrt{2^n}} = \sin\theta$$

where $|s\rangle$ will considered to be the vector which rotate $|a^{\perp}\rangle$ with θ.

The Grover's algorithm can be consisting as the follow steps:

1) Consider an initial state: $|0\rangle^{\otimes n}$.
2) Apply the Hadamard gate on the first n qubits to get a uniform superposition of all possible arguments.
3) Apply the oracle f. Note that the information on fare included in the $(n+1)^{th}$ qubit,
4) 4) Apply against the Hadamard gate,
5) 5) Do an observation [11].

The quantum circuit representation of the Grover's algorithm is shown in Fig. 1.

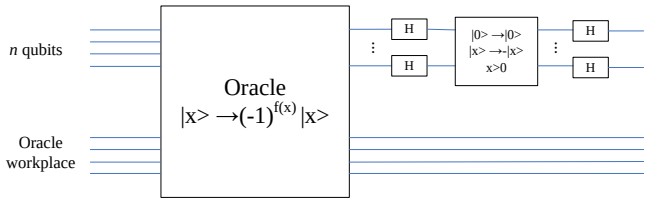


Fig. 1. Circuit of Grover's algorithm.

In fact, the Grover iteration can be regarded as a rotation in the 2-D space spanned by the starting vector $|s\rangle$.

Quantum procedure:

$$|x'\rangle = U_a |x\rangle$$

$$|x''\rangle = U_s |x'\rangle$$

The intersection angle between $|x\rangle$ and $|x''\rangle$ is $2\theta (2\theta = \alpha + \beta)$. The geometric characterization of Grover's algorithm is shown in Fig. 2.

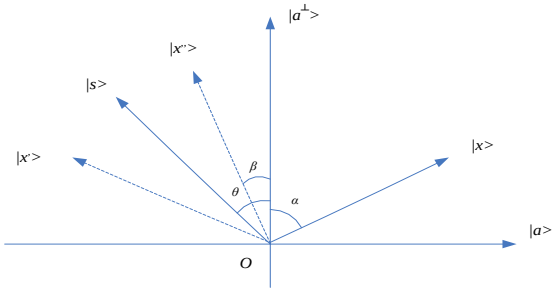


Fig. 2. Geometric characterization.

In Fig. 2, $|x\rangle$ is an arbitrary state vector, $|s\rangle$ is a prepared state with equipobability quantum state, $|a\rangle$ is the data which will be searched in Oracle, $|a^{\perp}\rangle$ is the state vector which perpendicular to $|a\rangle$.

If $x = s$, then $|s''\rangle = U_s U_a |s\rangle$. The intersection angle between $|a^{\perp}\rangle$ and $|s''\rangle$ *is* $\theta + 2\theta$, it is a solution of one Grover iteration. When m steps Grover iterations were applied to the quantum state, the intersection angle between $|a^{\perp}\rangle$ and $|s^m\rangle$ is $\theta + 2m\theta$. If $\theta + 2m\theta = \frac{\pi}{2}$, the probability of observing the result is 1. So,

$$\theta + 2m\theta = (2m+1) \cdot sin^{-1}\frac{1}{\sqrt{2^n}} = \frac{\pi}{2}$$

$$m = \frac{\pi}{4\, sin^{-1}\frac{1}{\sqrt{2^n}}} - \frac{1}{2} = O(\sqrt{2^n})$$

IV. Performance of Grover's Algorithm

After m steps Grover iterations, the state vector $|s\rangle$ is rotated to the position of $(2m+1)\theta$. In order to get the solution ($|a\rangle$) by measurement with higher probability, the intersection angle should close to $\pi/2$.

$$\left|\frac{\pi}{2} - (2m+1)\theta\right| = \delta$$

$$\left|m - (\frac{\pi}{4\theta} - \frac{1}{2})\right| = \frac{\delta}{2\theta}$$

$$m = (\frac{\pi}{4\theta} - \frac{1}{2}) \pm \frac{\delta}{2\theta}$$

$$m \approx \frac{\pi}{4}\sqrt{2^n}$$

where m is the iteration steps, θ is state intersection angle and δ is error.

The probability of observing $|a\rangle$ is :

$$p(a) = sin^2(2m+1)\theta$$

$$p(a) = 1 - cos^2[(2m+1)\theta]$$

$$p(a) = 1 - sin^2\left[\frac{\pi}{2} - (2m+1)\theta\right]$$

$$p(a) = 1 - sin^2(\delta) = cos^2(\delta)$$

It shows the Grover's algorithm search the Oracle in $O(\sqrt{2^n})$ times in order to obtain a solution, on a quantum computer.

V. Simulation

The correctness of Grover's search algorithm is easily verified. But the Grover's search algorithm processed in quantum computer seemed very difficult. It is a better way with classical computer simulation to do further research in Grover's search algorithm. We proposed a quantum computation emulator [12], [13] in classical computer which satisfies the requirements of quantum computer. Conventional quantum algorithms can be operated in this simulation system. In this paper, the simulation aimed to analyses the relationship between the accuracy and probability of observing in Grover's search algorithm. The Orcale can be written in n-qubit in Grover's algorithm. We

will get all the possible states by measuring the output qubit.

Build such an Oracal with 2^{10} irregular records for testing. This simulation will find a particular data a_0 in the Oracal. The numerical simulation can simulate the Grover iteration. In the simulation we can get the probability distribution of quantum state of output from 1 to 2^{10} which is shown in Fig. 3.

It shows in Fig. 3 with three different curves representing the probability distribution of quantum state after the different number of Grover iterations. In Fig. 3, we will get the objective value more than 99.99% after 25 times (integer part of $\frac{\pi}{4}\cdot\sqrt{2^{10}}$) Grover iterations , but not more than 70% after 16 times iterations and to be worse after 8 times iterations.

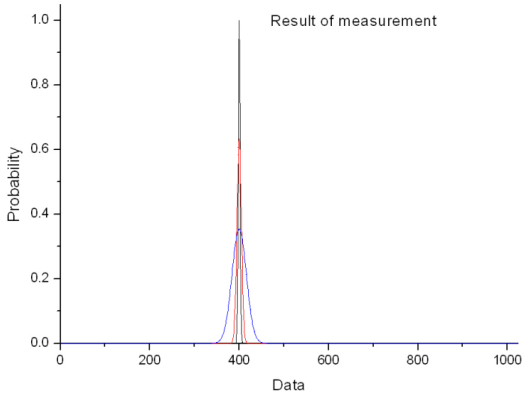


Fig. 3. The probability distribution of different Grover iterations.

Fig. 4 is mainly about the different Grover iterations effect on the probability of Grover search which in the same Oracle. As it is shown, the more closer to the $\frac{\pi}{4}\cdot\sqrt{2^n}$ iterations the higher probability to get the objective by quantum measurement.

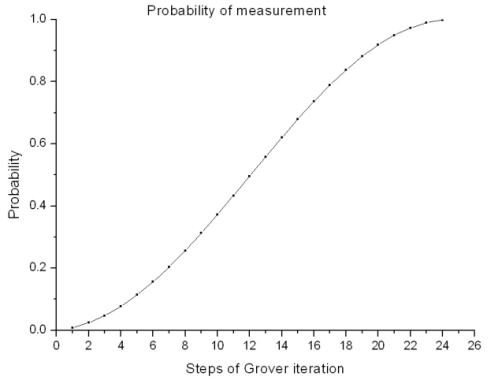


Fig. 4. The probability of different Grover iterations.

VI. Conclusion

In this paper, we have presented an application of quantum algorithm in the quantum information processing system. We have analyzed, in particular, the basic concept of Grover's search algorithm and its implementation in the case of *n*-qubits system. The simulation of Grover's algorithm shows it is an efficient and effective search algorithm. The author believes Grover's search algorithm leave much more to be improved.

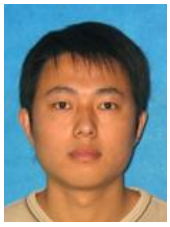
In future, our work focuses on the quantum search algorithm of muti-objective.

Acknowledgment

It is my pleasure to thank my colleagues, Zhao Junsuo, for helping me organize and consolidate my original ideas as well as for giving me insight along every step of the editing and writing process. I would also like to thank Zhang Wenjun for organizing the academic discussion about quantum computation this year.

References

[1] D. Deutsch, "Quantum theory, the church-turing principle and the universal quantum computer," *Proc. Royal Soc. Lond. A*, vol. 400, no. 1818, pp. 97-117, 1985.
[2] D. Deutsch, "Quantum computational networks," *Proc. Roy. Soc. Lond.* A, vol. 439, pp. 553-558, 1992.
[3] P. Benioff, "The computer as a physical stystem: a microscopic quantum mechanical hamiltonian model of computers as represented by turing machines," *Journal of Statistical Physics*, vol. 22, pp. 563-591, 1982.
[4] P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," in *Proc. 35th Annual Symposium on Foundations of Computer Science*, New Mexico: IEEE Computer Society Press, 1994, pp. 124-134.
[5] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annual ACM Symposium on the Theory of Computing*, 1996, pp. 212-129.
[6] G. L. K. Grover, "Quantum mechanics helps in searching for a needle in haystack," *Phys. Rev. Lett.*, vol. 79, pp. 325-328, 1997.
[7] C. H. Bennett, E. Bernstein, G. Brassard, and U. V. Vazirani, "Strength and weaknesses of quantum computing," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1510-1523, Octorber 1997.
[8] M. Boyer, G. Brassard, P. Hoeyer, and A. Tapp, "Tight bounds on quantum computing," in *Proc. 4th Workshop on Physics and Computation*, 1996, pp. 36-43.
[9] C. Zalka, "Grover's quantum searching is optimal," *Phys. Rev. A*, vol. 60, pp. 2746, 1999.
[10] M. A. Nilelsen and L. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge Univ. Press, 2000.
[11] B. C. Sanders and G. J. Milburn, "Optimal quantum measurements for phase *estimation*," *Phys. Rev. Lett*., vol. 75, pp. 2944-2947, 1995
[12] R. Feynman, "Quantum mechanical computers," *Science*, vol. 273, no. 5278, pp. 1073-1078, 1996.
[13] I. Buluta and F. Nori, "Quantum simulators," *Science*, vol. 326, no. 5949, pp. 108-111, 2009.



Zhuang Jiayu was born in Jiangsu, China in 1982. The author is a researcher in Institute of Software Chinese Academy of Sciences who interested in the research of information processing and quantum computation.