Available online at www.sciencedirect.com

SciVerse ScienceDirect

Energy Procedia 16 (2012) 1701 – 1706

Energy Procedia

2012 International Conference on Future Energy, Environment, and Materials

Progress of Grover Quantum Search Algorithm

Linlin Luan[1,2] , Zhijie Wang [1],Sanming Liu[1]

[1]*School of Electrical Engineering Shanghai DianJi University*
Shanghai200240,China
2、*School of Information Science & Engineering East China University of Science and Technology*
Shanghai200237, China

Abstract

Grover quantum search algorithm access the unsorted database *O(N)* times, however, the probability of acquiring solutions usually falls with the increase of the number of solutions, the reason of which is analyzed. To improve the performance of converging and optimizing for the intelligent optimization, some quantum evolutionary algorithms are proposed by domestic and foreign scholars. In this paper, a lot of improved Grover quantum search algorithms are introduced in detail.

Keywords: Grover algorithm; quantum searching; quantum computing

1. Introduction

Grover quantum search algorithm was proposed by Grover in 1996 Grover. Grover's quantum search algorithm[1] is one of the most important developments in quantum computation. Since quantum mechanical system can simultaneously be in multiple Schrodinger cat states and carry out multiple tasks at the same time, for searching a marked state in an unordered list, it achieves quadratic speedup over classical search algorithms. This algorithm can significantly improves the efficiency of search. However this algorithm still has some defects. With the target number increases, the probability of getting the right result is drastically reduced. To improve the success probability of this algorithm scholars have proposed several improvements of the Grover algorithm. The basic idea of most of these improvement are from phase rotation and weighted target to construct a new iteration operator.

doi:10.1016/j.egypro.2012.01.263

2. Grover's algorithm

2.1 Algorithm

Let a system have $N=2^n$ States which are labeled $S^1.S^2...S^N$. These 2^n states are represented as n bit strings. Let there be a unique state, say S_v, that satisfies the condition $C(S_v) = 1$, whereas for all other states S, $C(S) = 0$ (assume that for any state S, the condition $C(S)$ can be evaluated in unit time). The problem is to identify the state S_v.

1) Initialize the system to the distribution:, $\left(1/\sqrt{N}, 1/\sqrt{N}, 1/\sqrt{N}, \cdots 1/\sqrt{N}\right)$, i.e. there is the same amplitude to be in each of the N states. This distribution can be obtained in $O(logN)$ steps .

2) Repeat the following unitary operations $O(N)$ times:

a) Let the system be in any state S: Incase $C(S)$=1 ,rotate the phase by radians; In case $C(S)$=0, leave the system unaltered.

b) Apply the diffusion transform D which is defined by the matrix D as follows: $D_{ij} = 2/\sqrt{N}$ if $i \neq j$ and $D_{ij}=-1+2/\sqrt{N}$ This diffusion transform ,D, can be implemented as D=WRW, where R the rotation matrix and W the Walsh-Hadamard Transform Matrix are defined as follows: R_{ij}=0 if $i \neq j$; R_{ij}=1 if i=0; $R_{ij} = -1$ if $i \neq 0$.

3) Sample the resulting state. In case $C(S_v)$=1 there is a unique state S_v with a probability of at least $\frac{1}{2}$.

2.2 search problem[2]

Let M denotes the number of matches within the search space such as $1 \le M \le N$ and for simplicity and without loss of generality we can assume that $N=2^n$.Solution set is Ω , $|\alpha\rangle = 1/\sqrt{N-M} \sum_{x\notin\Omega} |x\rangle$, $|\beta\rangle = 1/M \sum_{x\in\Omega} |x\rangle$. For convenience, $\lambda = M/N$, $\theta = \arcsin\sqrt{\lambda}$,the initial state of the system can be described as:

$$|\phi\rangle = \cos\theta|\alpha\rangle + \sin\theta|\beta\rangle \qquad (2.2.1)$$

The algorithms require number R of iteration is:

$$\mathrm{R=CI}\left(\arccos\sqrt{\lambda}\Big/\left(2\arcsin\sqrt{\lambda}\right)\right) \qquad (2.2.2)$$

After Grover was called R times the initial state changes into：

$$G^R|\phi\rangle = \cos(2R+1)\arcsin\sqrt{\lambda}\,|\alpha\rangle + \sin((2R+1)\arcsin\sqrt{\lambda}\,|\beta\rangle \qquad (2.2.3)$$

Therefore the successful probability of Grover search algorithm is[13]:

$$\mathrm{P}=\sin^2\left(\left(2R+1\right)\arcsin\sqrt{\lambda}\right) \qquad (2.2.4)$$

From the formulas 2.2.1 and 2.2.4, when $\lambda \in (0.14645, 0.50)$, R=1; when $\lambda = 0.14645$, P=0.85356;当 $\lambda = 0.50, P=0.5$. Therefore the successful probability of the general Grover search algorithm can obtain the maximum on the point $\lambda = 0.25$, then decrease rapidly. When $\lambda = 0.5$,the probability down to the minimum 0.5. Then R=0, the algorithm is disabled. So when λ is large ,the rapid decline in the probability of success is the main problem of the general Grover search algorithm

The improved algorithm based on $\pi/2$ phase The main problem of Grover algorithm : The size of the two phase rotation are equal to π in the algorithm , as λ increases, when it is larger, the probability of success is in decline. First people change the fixed phase value π in the twice phase rotations into arbitrary values, then determine the a new phase matching conditions by exploring the relationship between the values of each phase rotation and the probability of obtain the correct results. According the results, people proposed a new phase matching conditions is: set the twice phase rotation values are equal to, $\pi/2$ but in the opposite directions.

2.3 A Improvement of phase-matching conditions

The general form of the two phase shift operators are:

$$U = I - (1-e^{j\partial}) \sum_{m=1}^{M} |\tau_m\rangle\langle\tau_m| \qquad (3.1.1)$$

$$V = (1 - e^{j\beta})|\varphi\rangle\langle\varphi| + e^{j\beta}\, I \qquad (3.1.2)$$

Theorem 1 : The operators defined by the formulas 3.1.1 and 3.2.2 are unitary operators.
Theorem 2 :When $\lambda > 1/3$,set $\alpha = \beta = \pi/2$,only need one search to make the probability of success reach $P \geq 25/27$.
By Theorem 2, the improved algorithm of the two phase shift operators can be crystallized as:

$$U=I-(1-i)\sum_{m=1}^{M} |\tau_m\rangle\langle\tau_m| \qquad (3.1.3)$$

$$V=(1+i)|\varphi\rangle|\varphi\rangle-iI \qquad (3.1.4)$$

We can prove that when $1/3 < \lambda < 1$,the improved algorithm is superior to the general Grover algorithm.

3. The Grover algorithm based on adaptive phase rotation

The probability of success of the standard Grover search algorithm is difficult to achieve 100%. Only when the database is infinite, the probability of success can be equal to 100%. So professor Long G L et al proposed a modified Grover algorithm [5], which can make P reach 100%. The key to the improved algorithm is that, first step is reverse the phase for make it a phase rotation angle related to the size of the database which can changes with the searching database size. Then iterate the phase rotation angle to iteration operator. The phase rotation angle is: [7-9]

$$\begin{aligned}\phi = \theta &= 2\arcsin\left[\sin\left[\frac{\pi}{4J+6}\right]\Big/\sin\beta\right] \\ &= 2\arcsin\left[\sin\left[\frac{\pi}{4J+5}\right]N^{1/2}\right]\end{aligned} \qquad (4.1)$$

Where: $J \geq J_{op}$, J_{op} is the iterations,

$$J_{op} = \left[\frac{\pi/2-\beta}{2\beta}\right] = \left[\frac{\pi}{4\beta} - \frac{1}{2}\right]$$

$$\beta = \arcsin\left[(1/N)^{1/2}\right]$$

According to Professor Long G L, Professor Li P C proposed a new adaptive phase rotation strategy [11].

In the search engines, the value of the phase rotation angle is determined by $\lambda = M/N$. The minimum of the probability of general Grover algorithm is 0.5, but the adaptive phase rotation can make it equal to 1 constantly.

Theorem 5: In the Grover algorithm ,the set number of marked states is M, the number of the total state is N, and $\lambda = M/N$,the search engines is $G=-HI_0H^{+}I_s$.

（1） When $1/4 \le \lambda \le 1$, there is a unique $\alpha = \arccos((2\lambda - 1)/2\lambda)$,only need one Grover iteration the probability of success is P=1.

（2） When $(3-\sqrt{5})/8 < \lambda < 1/4$, there is a unique $\alpha = \arccos(1-(3-\sqrt{5})/4\lambda)$, only need two steps Grover iteration, the probability of success is P=1.

According theorem 5, when the number of target state is more than $(3\text{-}\sqrt{5})/8$ percents of the total state number, it takes at most two steps of iterations to obtain search target with probability 1 using the new adaptive phase rotation strategy. And when the number of target state is less than $(3\text{-}\sqrt{5})/8$ percents of the total state, the probability will be high than 93.3% if we adapting the original phase rotation.

4. The quantum search algorithm of using a local diffusion operator

In 2003,Younes who from the University of Birmingham proposed a local diffusion operator using quantum search algorithm, the algorithm in the mean operator inversion operation is not carried out in all space, but the introduction of the local diffusion operator makes the means of the operator only in the local space. Theoretical analysis and experiments show that the algorithm has excellent performance, especially for multi-object search problems. The probability of success is at least 84.72%.

Local diffusion operator

Definition of local diffusion operator Y, Applied Y to the system of n +1 quantum bits system, the operator can be described as

$$Y=H^{\otimes n} \otimes I\ (2|0\rangle\langle 0|\text{-}I)\ H^{\otimes n} \otimes I \qquad (5.1.1)$$

Applied Y to the system having P（P=n+1） states the system can change into:

$$\sum_{j=0}^{P\text{-}1} \sigma_k |k\rangle = \sum_{j=0}^{N-1} \alpha_j (|j\rangle \otimes \langle 0|) + \sum_{j=0}^{N\text{-}1} \beta_j (|j\rangle \otimes |1\rangle) \qquad (5.1.2)$$

When K is even, $\alpha_j = \sigma_k$,when K is odd, $\beta_j = \sigma_k$ .The system applied to Y can change into：

$$Y\ (\sum_{k=0}^{P\text{-}1} \sigma_k |k\rangle) = \sum_{j=0}^{N\text{-}1} (2|\alpha\rangle\text{-}a_j(|j\rangle \otimes |0\rangle)\text{-}\sum_{j=0}^{N\text{-}1} \beta_j (|j\rangle \otimes |1\rangle) \qquad (5.1.3)$$

where $\langle\alpha\rangle = \frac{1}{N}\sum_{j=0}^{N\text{-}1} \alpha_j$ is the mean rate of the subspace $\sum_{j=0}^{N-1} \alpha_j (|j\rangle \otimes |0\rangle)$ .Therefore the function of the local diffusion operator Y is implementing a mean reversal in the space $\sum_{j=0}^{N-1} \alpha_j (|j\rangle \otimes |0\rangle)$,and only change the sign of the magnitude in space $\sum_{j=0}^{N\text{-}1} \beta_j (|j\rangle \otimes |1\rangle$.

The probability of success after q steps iterations of Younes algorithm is:

$$P_s^q = (1\text{-}\cos\theta)\left(\sin^2(q+1)\,\theta/\sin^2\theta + \sin^2 q\theta/\sin^2\theta\right) \qquad (5.1.4)$$

Where $\cos\theta$=1- M/N ; $0 < \theta \le \pi/2$; Iteration steps is: q=$\left(\pi/2\sqrt{2}\right)\sqrt{N/M}$.

5. Grover algorithm based on objective weighting

Li P C proposed the Grover algorithm based on objective weighting in 2008. This algorithm is to give different weights according the importance of the target, and then express search targets as a quantum superposition state, and then construct a new Grover algorithm based on the quantum superposition state.

5.1 Structure of the Target quantum superposition state

Set $|q_1\rangle, |q_2\rangle, \ldots |q_M\rangle$ is the M target quantum states, $\Omega = \{q_1, q_2, \cdots q_M\}$; $\omega_1, \omega_2, \cdots \omega_M (\omega_i \ge 0)$ is the weights of the its target, and $\sum_i^M \omega_i = 1$. he Target quantum superposition state is:

$$|q\rangle \sum b_i |i\rangle = \begin{cases} \sum \sqrt{\omega_i} |i\rangle & i \in \Omega \\ 0|i\rangle & i \notin \Omega \end{cases} \qquad (6.1.1)$$

Where b_i is probability amplitude of each state in the target superposition state.

5.2 The construction of iteration operator [15]

The form of Oracle operators is： $O = I\text{-}2|q\rangle\langle q|$, Hadamard transform and the phase shift operator is: $U_S = I\text{-}2|\varphi\rangle\langle\varphi|$

5.3 Performance analysis of algorithms

Theorem 6: After t times search, the target weighted probability of success of Grover algorithm is not less than the square of superposition of the system state and the target point within the plot, that is:

$$P^t \ge \left(\langle q|\varphi\rangle^{(t)}\right)^2 .$$

The probability of success of each goal are equal in General Grover algorithm, we can't search for the more important goals on the larger probability. And weighted Grover algorithm was able to search the important goal with greater probability, which is the advantage of weighted Grover algorithm.

6. Outlooks

Although the Grover search algorithm has many flaws and shortcomings, it has important significance in the early development of quantum algorithms. Currently, Grover algorithm has attracted extensive attention and has become a challenging area of research. It is generally accepted that the following aspects need further exploration and research.

Acknowledgment

This work is supported by Natural Science of Foundation of Shanghai (09ZR1420600), Talent Development of Foundation of Shanghai (Grant No. 2009027), Project supported by the National Natural Science Foundation of China (Grant No. 61075092), Innovation Program of Shanghai District Technology Commission (2010MH035) (2010MH054) and Key Subject of foundation of Shanghai Education Committee (J51901).

References

[1] GROVER L K. A fast quantum mechanical algorithm for database search [C]//Proc. of the 28th annual ACM Symp on Theory of Computing. New York, USA: ACM Press, 1996. 6: 212-219.

[2] NIELSEN M A, CHUANG I L Quantum computation and quantum information [M]. London: Cambridge University Press, 2000.

[3] Zhao Qianchuan translation, quantum computing and quantum information, Beijing, Tsinghua University Press, 2004

[4] LI P C, LI S Y. Phase matching in Grover's algorithm [J]. Physics Letter A, 2007, 366(1-2): 42-46.

[5] Long Guilu. Grover algorithm with zero theoretical failure rate [J]. Phys Rev. 2001, A 64(2): 022307.

[6] Long Guilu. Phase matching in quantum searching and the improved grover algorithm [J]. Nuclear Phys Rcv, 2004, 2(2): 114-116.

[7] Long Guilu,Xiao Li． General phase matching condition for quantum searching [J] Phys Lett, 2002, A294(4 / 3): 143—152.

[8] Zhong Cheng, Zhao Yuehua. Introduction to Information Security [M], Wuhan: Wuhan exhaust, the 2006.

[9] YOUNES A. Quantum search algorithm with more reliable behavior using partial diffusion [J]. Quant-ph/0312022: 1-27.

[10] Li Shiyong, Li Panchi. Quantum Computation and Quantum Optimization Algorithm [M]. Harbin: Harbin Institute of Technology Press, 2009.5 [12] LI P C, LI S Y. A Grover quantum searching algorithm based on the weighted targets [J]. Journal of Systems Engineering Electronics, 2008, 19(2): 363-369.

[11] Long Guilu .Graver algorithm with zero theoretical failure rate [J]． Phys Rev,2001,A64(2)：022307．

[12] Li Shiyong, Li Panchi.Weighted quantum search algorithm and its phase-matching conditions of [J]. Computer Physics, 2008, (05) -0623-08 [16] Nielsen M A,Chuang I L． Quantum computation and quantum information[M]． London：Cambridge University Press,2000.248—255． G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.