Grover algorithm with zero theoretical failure rate

G. L. Long
Department of Physics, Tsinghua University, Beijing 100084, People's Republic of China;
Key Laboratory for Quantum Information and Measurements, Ministry of Education, Beijing 100084, People's Republic of China;
Institute of Theoretical Physics, Chinese Academy of Sciences, Beijing 100080, People's Republic of China;
and Center of Atomic, Molecular and Nanosciences, Tsinghua University, Beijing 100084, People's Republic of China
(Received 3 February 2001; published 11 July 2001)

In a standard Grover's algorithm for quantum searching, the probability of finding the marked item is not exactly 1. In this paper we present a modified version of Grover's algorithm that searches a marked state with full successful rate. The modification is done by replacing the phase inversion by phase rotation through angle ϕ. The rotation angle is given analytically to be $\phi=2\arcsin(\sin[\pi/(4J+6)]/\sin\beta)$, where $\sin\beta=1/\sqrt{N}$, N is the number of items in the database, and J is any integer equal to or greater than the integer part of $[(\pi/2)-\beta]/(2\beta)$. Upon measurement at the $(J+1)$th iteration, the marked state is obtained with certainty.

DOI: 10.1103/PhysRevA.64.022307 PACS number(s): 03.67.Lx, 89.70.+c, 89.20.Ff

Grover's quantum search algorithm [1] is an important development in quantum computation. It achieves square-root speedup over classical algorithms in unsorted database searching. It has extensive applications, because many problems, for instance deciphering the DES encryption scheme, can be reduced to this problem [2]. Starting from an evenly distributed state, the Grover algorithm searches the database with

$$j_{op}=[(\pi/2-\beta)/(2\beta)], \tag{1}$$

or $j_{op}+1$ number of times, whichever of $[2(j_{op}+1)+1]\beta$ and $(2j_{op}+1)\beta$ is closest to $\pi/2$. Here $\beta=\arcsin(1/\sqrt{N})$ and [ ] means taking the integer part. N is the number of items in the database. Maximum probability is achieved when measurement is made at the optimal iteration step, and it is

$$P_{max}=\sin^2[(2j_{op}+1)\beta]\cong 1. \tag{2}$$

It equals 1 if $(2j_{op}+1)\beta=\pi/2$. This condition is usually approximately satisfied. This can be seen from Table I where values of j_{op}, $(2j_{op}+1)\beta$ for N are given. The deviation $(2j_{op}+1)\beta$ from $\pi/2$ is on the order of $1/\sqrt{N}$. This small deviation becomes negligible when the dimension of the quantum database becomes very large, for instance in deciphering the DES code where $N=2^{56}$ the deviation is only 3×10^{-9}. The standard Grover algorithm has already achieved high probability, and in most potential applications it is sufficient.

However, in problems where certainty is vital, especially when the dimension is not so big, using a searching algorithm with certainty becomes important. Meanwhile constructing such a quantum search algorithm itself is an interesting issue. In this paper we present such a modified Grover algorithm.

In fact, two such algorithms already exist. One is given by Brassard *et al.* [3] where the generalized algorithm searches the database j_{op} iterations with the standard Grover algorithm, and then run one more iteration with a modified algorithm whose step is smaller. Høyer gave another generalization [4], where certainty is achieved by modifying the Grover algorithm and making change to the initial distribution. Our algorithm here complements with these algorithms. In addition, the present algorithm materializes one earlier anticipation [5]. It was pointed out that when the phase inversions are replaced by arbitrary rotations in Grover's algorithm [6], a quantum search algorithm with a smaller iteration can be constructed. Zalka anticipated that this could be used to achive certainty in quantum searching [5] by running a quantum searching algorithm with a smaller step so that at an integer number of iteration, the quantum computer state vector is exactly the marked state. Our algorithm here is just such an algorithm.

The generalized Grover algorithm here starts from the evenly distributed state

$$\begin{aligned}|\psi_i\rangle&=\frac{1}{\sqrt{N}}\sum_i|j\rangle\\&=\frac{1}{\sqrt{N}}(|0\rangle+|1\rangle+\cdots+|\tau\rangle+\cdots+|N-1\rangle)\\&=\sin\beta|1\rangle+\cos\beta|2\rangle,\end{aligned} \tag{3}$$

TABLE I. Examples of j_{op} and $(2j_{op}+1)\beta$.

$N=$	2	4	8	100	1000	10^4	10^6	10^8	10^{10}	2^{56}
j_{op}	0	1	1	7	24	78	784	7853	78539	210828713
$\frac{(2j_{op}+1)\beta}{\frac{\pi}{2}}$	$\frac{1}{2}$	1	0.69016	0.956528	0.986617	0.99951	0.998857	0.999939	0.999996	0.999999997

TABLE II. Examples of $j_{op}+1$ and ϕ.

$N=$	2	4	8	16	100	1000	10^4	10^6	10^8	10^{10}
$j_{op}+1$	1	1	2	3	8	25	79	785	7854	78540
$\frac{\phi}{\pi}$	$\frac{1}{2}$	1	0.677007	0.698709	0.748018	0.854022	0.90089	0.989752	0.992688	0.9973

and the searching operator is

$$Q=-WI_0WI_\tau = \begin{bmatrix} -e^{i\phi}(1+(e^{i\phi}-1)\sin^2\beta) & -(e^{i\phi}-1)\sin\beta\cos\beta \\ -e^{i\phi}(e^{i\phi}-1)\sin\beta\cos\beta & -e^{i\phi}+(e^{i\phi}-1)\sin^2\beta \end{bmatrix}, \tag{4}$$

where the matrix expression is written in the following basis:

$$|1\rangle=|\tau\rangle,$$

$$|2\rangle=\frac{1}{\sqrt{N-1}}\sum_{i\neq\tau}|i\rangle \tag{5}$$

and

$$I_\tau=I+(e^{i\phi}-1)|\tau\rangle\langle\tau|, \qquad I_0=I+(e^{i\phi}-1)|0\rangle\langle 0|, \tag{6}$$

where

$$\phi=2\arcsin\left(\frac{\sin\left(\frac{\pi}{4J+6}\right)}{\sin\beta}\right), \qquad J\geqslant J_{op}. \tag{7}$$

Here the two-phase rotations are equal which is required by the phase-matching condition [7,8]. Certainty quantum searching is achieved by measuring the quantum computer at $J+1$ iteration. In a standard Grover algorithm, $\phi=\pi$. In Table II we gave the angle ϕ for some values of N. It is seen that in general the phase rotations are very close to π. We see that at small N, the deviation of ϕ to π is big, and it decreases when N becomes large. The certainty of the algorithm can be examined by direct computation. We will give the detailed derivation of this result in the $SO(3)$ picture of the quantum searching algorithm [9].

Equation (7) has a real solution for $J\geqslant j_{op}$, otherwise the solution will be complex. An integer $J\geqslant j_{op}$ fixes a phase rotation that searches the marked state with certainty in $J+1$ steps. The lower bound j_{op} tells us that it cannot be faster than the standard Grover algorithm. J can be chosen to be j_{op}, or an integer larger than j_{op} for convenience.

In the following part, we show the above result and give the expression for the probability during the searching process. We do this in the $SO(3)$ picture introduced recently [9]. In this picture, the quantum search operator (4) corresponds to a rotation in space

$$R_Q=\begin{bmatrix} R_{11} & R_{12} & R_{13} \\ R_{21} & R_{22} & R_{23} \\ R_{31} & R_{32} & R_{33} \end{bmatrix}, \tag{8}$$

where

$$R_{11}=\cos\phi(\cos^2 2\beta\cos\phi+\sin^2 2\beta)+\cos 2\beta\sin^2\phi),$$

$$R_{12}=\cos\phi\sin\phi(\cos 2\beta-1),$$

$$R_{13}=-\cos\phi\sin 4\beta\sin^2\frac{\phi}{2}+\sin 2\beta\sin^2\phi,$$

$$R_{21}=-\cos 2\beta\cos\phi\sin\phi+\left(\cos^2\frac{\phi}{2}-\cos 4\beta\sin^2\frac{\phi}{2}\right)\sin\phi,$$

$$R_{22}=\cos^2\phi+\cos 2\beta\sin^2\phi,$$

$$R_{23}=-\cos\phi\sin 2\beta\sin\phi-\sin 4\beta\sin^2\frac{\phi}{2}\sin\phi,$$

$$R_{31}=-\sin 4\beta\sin^2\frac{\theta}{2},$$

$$R_{32}=\sin 2\beta\sin\phi,$$

$$R_{33}=\cos^2 2\beta+\cos\phi\sin^2 2\beta.$$

The above rotation is a rotation about the following axis:

$$\vec{l}=\begin{pmatrix} \cos\frac{\phi}{2} \\ \sin\frac{\phi}{2} \\ \cos\frac{\phi}{2}\tan\beta \end{pmatrix}, \tag{9}$$

through an angle α

$$\alpha=4\arcsin\left[\sin\left(\frac{\phi}{2}\right)\sin\beta\right]. \tag{10}$$

State vector $|\psi\rangle=(a+bi)|1\rangle+(c+di)|2\rangle$ is represented by the polarization vector

$$\vec{r}_\psi = \langle\psi|\vec{\sigma}|\psi\rangle = \begin{pmatrix} 2(ac+bd) \\ 2(-bc+ad) \\ a^2+b^2-c^2-d^2 \end{pmatrix}, \tag{11}$$

where $\vec{\sigma}=\sigma_x\vec{i}+\sigma_y\vec{j}+\sigma_z\vec{k}$, and $\vec{i}$, $\vec{j}$, and $\vec{k}$ are the unit vectors along the x, y, and z axes. The initial state $|\psi_i\rangle$ and the marked state $|\tau\rangle$ are represented by

$$\vec{r}_i = \begin{pmatrix} \sin(2\beta) \\ 0 \\ -\cos(2\beta) \end{pmatrix}, \quad \vec{r}_f = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}. \tag{12}$$

Now we want to find out the angle that we must rotate to shift $\vec{r}_i$ to $\vec{r}_f$. The equation for a line passing through the origin and parallel to the rotational axis is

$$\frac{x}{\cos\frac{\phi}{2}} = \frac{y}{\sin\frac{\phi}{2}} = \frac{z}{\cos\frac{\phi}{2}\tan\beta}, \tag{13}$$

and the equation for the plane passing through $(0,0,1)^T$ and normal to the rotational axis is

$$x\cos\frac{\phi}{2} + y\sin\frac{\phi}{2} + (z-1)\cos\frac{\phi}{2}\tan\beta = 0. \tag{14}$$

The intersecting point of Eqs. (13) with (14) is

$$\vec{r}_o = \begin{pmatrix} c\cos^2\left(\frac{\phi}{2}\right)\tan\beta \\ c\sin\left(\frac{\phi}{2}\right)\cos\left(\frac{\phi}{2}\right)\tan\beta \\ c\cos^2\left(\frac{\phi}{2}\right)\tan^2\beta \end{pmatrix}, \tag{15}$$

where $c=1/(1+\cos^2\phi/2\tan^2\beta)$. The angle ω between $\vec{r}_i-\vec{r}_0$ and $\vec{r}_f-\vec{r}_0$ is the angle we have to rotate in a given number of iterations. Using

$$(\vec{r}_i-\vec{r}_o)\cdot(\vec{r}_f-\vec{r}_o) = |\vec{r}_i-\vec{r}_0||\vec{r}_f-\vec{r}_0|\cos\omega, \tag{16}$$

we find that

$$\cos\omega = -\cos^2\beta - \cos\phi\sin^2\beta = \cos(2\arccos x), \tag{17}$$

where

$$x = \sin\left(\frac{\phi}{2}\right)\sin\beta. \tag{18}$$

Certainty in finding the marked state is achieved if angle ω is $J+1$ times of the basic rotation angle α:

$$\omega = 2\arccos(x) = (J+1)\alpha = 4(J+1)\arcsin(x). \tag{19}$$

Using the trigonometric relation $\arcsin x+\arccos x=\pi/2$, we obtain

$$\omega = 2\left(\frac{\pi}{2}-\arcsin x\right) = 4(J+1)\arcsin(x).$$

This gives the result of Eq. (7). Equation (7) has real solutions for $J \geqslant j_{op}$. $J=j_{op}$ is the minimum in most cases. In the cases of $N=4$ and $N=1$, $J=j_{op}-1$ itself is a solution.

The probability for finding the marked state during the searching can be obtained easily. In the $SO(3)$ picture, the polarization vector at a given iteration is obtained by a simple geometric argument,

$$\vec{r}_j = \vec{r}_i\cos\omega + \vec{l}_n(\vec{l}_n\cdot\vec{r}_i)(1-\cos\omega) + (\vec{l}_n\otimes\vec{r}_i)\sin\omega, \tag{20}$$

where $\vec{l}_n$ is the rotational axis (9) normalized to unity. Using Eq. (11), the state vector can be determined easily. The probability for finding the marked state is $(z+1)/2$.

We can also write out the expressions in the $U(2)$ formalism. After diagonalization, the Q operator can be written as

$$Q = T\Lambda T^\dagger,$$

where

$$T = \frac{1}{\sqrt{N_T}}\begin{pmatrix} e^{-i(\phi/2)}\left[\cos\left(\frac{\phi}{2}\right)\sin\beta+\cos\beta'\right] & -\cos\beta \\ \cos\beta & e^{i(\phi/2)}\left[\cos\left(\frac{\phi}{2}\right)\sin\beta+\cos\beta'\right] \end{pmatrix},$$

$$\Lambda = \begin{pmatrix} -e^{i(\phi+2\beta')} & 0 \\ 0 & -e^{i(\phi-2\beta')} \end{pmatrix},$$

$$\beta' = \alpha/4 = \arcsin\left[\sin\left(\frac{\phi}{2}\right)\sin\beta\right],$$

$$N_T = \cos^2\beta + \left[\cos\left(\frac{\phi}{2}\right)\sin\beta+\cos\beta'\right]^2.$$

Successive operations of Q can be written analytically through

$$Q^n = T\Lambda^n T^\dagger.$$

In summary, a Grover algorithm with certainty is present. Together with the algorithms in Refs. [3] and [4], there are three choices of the quantum searching algorithm for finding the marked state with certainty. Our algorithm may be appreciated in cases where the dimension is not big and certainty is important, and in cases where preparation of the initial state and the change of the experimental setting during the computation process are difficult.

This work is supported by the Major State Basic Research Developed Program Grant No. G200077400, the China National Natural Science Foundation Grant No. 60073009, the Fok Ying Tung Education Foundation, and the Excellent Young University Teachers' Fund of Education Ministry of China.

[1] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[2] G. Brassard, Science **275**, 627 (1997).
[3] G. Brassard, P. Høyer, M. Mosca, and A. Tapp, e-print quant-ph/0005055.
[4] P. Høyer, Phys. Rev. A **62**, 052304 (2001).
[5] G. Zalka, e-print quant-ph/9902049.
[6] L. K. Grover, Phys. Rev. Lett. **80**, 4329 (1998).
[7] G. L. Long, Y. S. Li, W. L. Zhang, and L. Niu, Phys. Lett. A **262**, 27 (1999).
[8] Note that the phase condition in Ref. [4] is different from this one, because his initial state is different.
[9] G. L. Long *et al.*, J. Phys. A **34**, 867 (2001). Also in e-print quant-ph/9911004.