An *SO*(3) picture for quantum searching

2001 J. Phys. A: Math. Gen. 34 861

(http://iopscience.iop.org/0305-4470/34/4/312)

J. Phys. A: Math. Gen. **34** (2001) 861–866 www.iop.org/Journals/ja PII: S0305-4470(01)13674-7

An $SO(3)$ picture for quantum searching

Gui Lu Long[1,2,3], **Chang Cun Tu**[1], **Yan Song Li**[1], **Wei Lin Zhang**[1] **and Hai Yang Yan**[1]

[1] Department of Physics, Tsinghua University, Beijing 100084, People's Republic of China
[2] Institute of Theoretical Physics, Chinese Academy of Sciences, Beijing 100080, People's Republic of China
[3] Key Laboratory for Quantum Information and Measurements, Ministry of Education, People's Republic of China

Received 28 April 2000

Abstract

An $SO(3)$ picture of the generalized Grover quantum searching algorithm is constructed. In this picture, various aspects of quantum searching, the phase matching requirement in particular, are easily understood. It also offers a simple quantitative description of quantum searching. Exact formulae for the rotation angle and rotational axis are given. The probability of finding the marked state is just the projection of the state vector onto the z-axis in this picture. Applications of the picture to the standard Grover algorithm and to a generalized quantum search algorithm with arbitrary phase rotations are given.

PACS number: 0367L

Grover's quantum search [1] is one of the most celebrated quantum computing algorithms. It was shown that the Hadmard transformation in the algorithm can be replaced by almost any arbitrary unitary transformation [2]. It has been shown that the algorithm is optimal [3]. The original algorithm used an evenly distributed initial state. Later the algorithm was generalized to arbitrary initial amplitude distribution [4]. It has many important applications, for instance, in the Simon problem [5] and quantum counting [6]. Since Grover's algorithm involves only simple gate operations, it has been realized in two qubits [7,8] and three-qubit NMR systems [9].

Two points have to be made when applying Grover's algorithm. First, one has to make the measurement at the right optimal iteration number, otherwise the probability of finding the marked item will decrease. This is known as over-cooking. Secondly, the algorithm in Grover's original algorithm does not usually transform the state vector of the quantum computer to the marked state exactly; in other words, the searching is not 100% successful. To avoid this, one requires that in the last iteration the standard Grover searching engine be replaced by one that uses a step less than the standard Grover algorithm so that the state vector of the quantum computer is exactly the marked state. In addition, in many applications of the quantum search algorithm, one needs to use specifically a quantum search algorithm that has shorter steps. Thus it is important to construct a quantum search algorithm with arbitrary phase rotations. It has been found recently [11–13] that the algorithm has strange behaviours when the phase rotations in the algorithm are generalized. There is a requirement of phase matching in the two rotations in the algorithm; that is, the phase rotation of the marked state and phase rotation in the inversion about average must be matched.

There is an $SU(2)$ picture given by Grover [2] and Yu and Sun [14] to explain the searching process of quantum searching. However, in a generalized quantum searching algorithm, in particular when the phase rotations are generalized, this $SU(2)$ picture is no longer helpful. We need a clear physical picture to understand the algorithm and to apply the algorithm with ease. In this paper, we present a novel $SO(3)$ picture for the generalized quantum search algorithm. By exploiting the relation between $SO(3)$ and $SU(2)$, the process of quantum search is clearly transparent. Using this picture, it is very easy to calculate the probability of the algorithm at any stage of the quantum searching.

First, let us briefly recall the generalized quantum search algorithm. The operator for quantum search can be written as $Q = -I_\gamma U^{-1} I_\tau U$, where $|\tau\rangle$ is the marked state and $|\gamma\rangle$ is the prepared state, usually $|\gamma\rangle = |0\rangle$. It should be pointed that the minus sign in the Q operator has no physical significance, and is left there because of tradition. For arbitrary phase rotations, $I_\gamma = I - (-\mathrm{e}^{\mathrm{i}\theta} + 1)|\gamma\rangle\langle\gamma|$ and $I_\tau = I - (-\mathrm{e}^{\mathrm{i}\phi} + 1)|\tau\rangle\langle\tau|$. In the basis where $|1\rangle = U^{-1}|\tau\rangle$ and $|2\rangle = -(|\gamma\rangle - U_{\tau\gamma}U^{-1}|\tau\rangle)/\sqrt{1 - |U_{\tau\gamma}|^2}$, Q can be written as

$$Q = \begin{pmatrix} -\mathrm{e}^{-\mathrm{i}\frac{\phi}{2}}\left(\cos\frac{\theta}{2} + \mathrm{i}\cos 2\beta \sin\frac{\theta}{2}\right) & -\mathrm{i}\mathrm{e}^{-\mathrm{i}\frac{\phi}{2}} \sin 2\beta \sin\frac{\theta}{2} \\ -\mathrm{i}\mathrm{e}^{\mathrm{i}\frac{\phi}{2}} \sin 2\beta \sin\frac{\theta}{2} & -\mathrm{e}^{\mathrm{i}\frac{\phi}{2}}\left(\cos\frac{\theta}{2} - \mathrm{i}\cos 2\beta \sin\frac{\theta}{2}\right) \end{pmatrix} \tag{1}$$

where we have written $U_{\tau\gamma} = \mathrm{e}^{\mathrm{i}\xi}\sin\beta$ (in Grover's original algorithm, $U_{\tau\gamma} = \frac{1}{\sqrt{N}}$, $\xi = 0$ and $\sin\beta = \frac{1}{\sqrt{N}}$), and again an overall phase factor has been neglected. A quantum circuit for realizing the generalized quantum search algorithm is shown in figure 1 for a three-qubit system. In order to facilitate the phase rotations, we need two auxiliary qubits: one is prepared in $|0\rangle + \mathrm{e}^{\mathrm{i}\theta}|1\rangle$ and the other in $|0\rangle + \mathrm{e}^{\mathrm{i}\phi}|1\rangle$. Beginning from the prepared initial state $|000\rangle$ from the left, the algorithm carries firstly the unitary transformation U, then phase rotation $I_{\gamma=0}$ is carried out. Here the cross in the multiply controlled rotation means that the rotation is carried out when the control qubit is $|0\rangle$, and a small circle in the controlled rotation means carrying out the rotation in the target qubit when the control qubit is in $|1\rangle$. Then the inverse of the unitary transformation U is carried in each of the three work qubits. After that the phase rotation I_τ is carried. Here in the illustration, the marked state is $|\tau = 100\rangle$. This finishes one iteration in the quantum searching procedure. Then the state vector is redirected to the left for the next iteration. For each marked state, one has to make an appropriate I_τ layout in the circuit. This is equivalent to typing into the quantum computer the 'telephone number' of whom we want to find. A misunderstanding may occur here. One might wonder why we do not design a circuit that will transform the state vector of the machine into the marked state at just one iteration. Certainly, one can design such a transformation for each given marked state. However each given marked state has a distinct series of operation instruction. To realize such a quantum searching machine, one has to build up all the operation instruction sets for each of the N basis state. This is equivalent to sorting the quantum database, which clearly shows no advantage over classical searching algorithms. While in a quantum algorithm, though the number of states is also N, we need not prepare an operation instruction set for each τ, because the construction of the I_τ part of the circuit is done by a set of simple rules: a cross if the binary expression of the number in that position is zero and a circle if it is a one. This part can be done easily, for instance by a classical computer.

Now let us construct the $SO(3)$ picture. It is easy to check that $\det(Q) = 1$, and Q is an element of the $SO(3)$ group. As is well known, each unitary matrix u in the $SU(2)$ group corresponds to a rotation R_u in the $SO(3)$ group [10]. Here operator Q corresponds to the

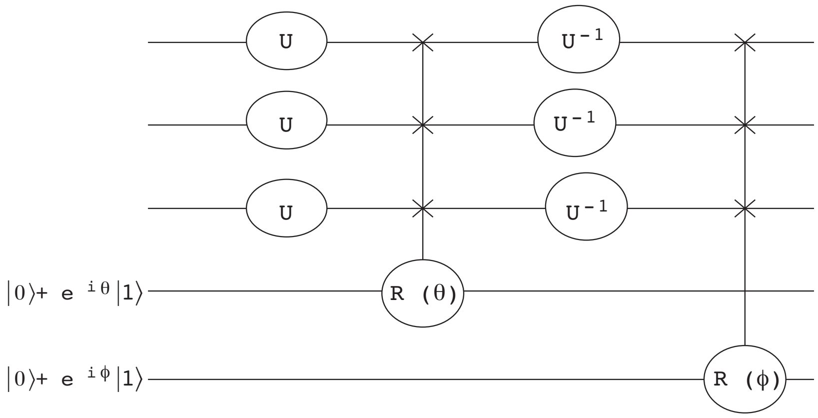

Figure 1. A quantum circuit for a three-qubit quantum searching with arbitrary phase rotations.

rotation

$$\begin{pmatrix} R_{11} & R_{12} & R_{13} \\ R_{21} & R_{22} & R_{23} \\ R_{31} & R_{32} & R_{33} \end{pmatrix} \tag{2}$$

where

$$\begin{aligned}
R_{11} &= \cos\phi(\cos^2 2\beta\cos\theta + \sin^2 2\beta) + \cos 2\beta \sin\theta\sin\phi \\
R_{12} &= \cos 2\beta\cos\phi\sin\theta - \cos\theta\sin\phi \\
R_{13} &= -\cos\phi\sin 4\beta\sin^2\frac{\theta}{2} + \sin 2\beta\sin\theta\sin\phi \\
R_{21} &= -\cos(2\beta)\cos\phi\sin\theta + \left(\cos^2\frac{\theta}{2} - \cos 4\beta\sin^2\frac{\theta}{2}\right)\sin\phi \\
R_{22} &= \cos\theta\cos\phi + \cos 2\beta\sin\theta\sin\phi \\
R_{23} &= -\cos\phi\sin 2\beta\sin\theta - \sin 4\beta\sin^2\frac{\theta}{2}\sin\phi \\
R_{31} &= -\sin 4\beta\sin^2\frac{\theta}{2} \\
R_{32} &= \sin 2\beta\sin\theta \\
R_{33} &= \cos^2 2\beta + \cos\theta\sin^2 2\beta.
\end{aligned}$$

We represent a spinor in $SU(2)$ which describes the state of the quantum computer, $\Psi = (a + b\mathrm{i})|1\rangle + (c + d\mathrm{i})|2\rangle = \begin{pmatrix} a + b\mathrm{i} \\ c + d\mathrm{i} \end{pmatrix}$, by a vector in R^3

$$\boldsymbol{r} = \Psi^\dagger\boldsymbol{\sigma}\Psi = \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2(ac + bd) \\ 2(-bc + ad) \\ a^2 + b^2 - c^2 - d^2 \end{pmatrix}. \tag{3}$$

The probability of finding the marked state is equal to the square of the magnitude of the coefficient of $|1\rangle$,

$$P = a^2 + b^2 = (z + 1)/2 \tag{4}$$

where z is the third component of this polarization vector. This simple equation gives a very clear picture of the probability of finding the marked state in the algorithm. For

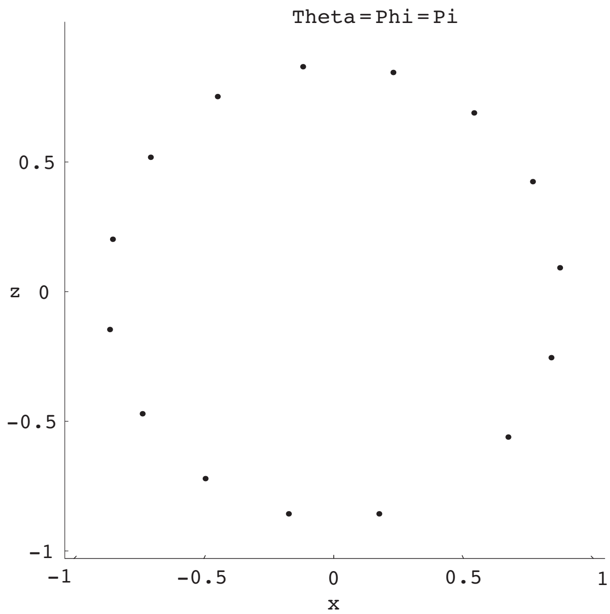

Figure 2. The trace of the vector state tip for Grover's algorithm.

instance, the evenly distributed state $\Psi_o = (\frac{1}{\sqrt{N}}, \frac{\sqrt{N-1}}{\sqrt{N}})^T$, corresponds to vector $\boldsymbol{r}_o = (2\sqrt{1-\frac{1}{N}}\sqrt{\frac{1}{N}}, 0, -1+\frac{2}{N})^T$, which is nearly parallel to the $-z$-axis when N is large. The marked state $\psi_a = (1, 0)^T$, corresponds to $\boldsymbol{r}_a = (0, 0, 1)^T$, which is on the $+z$-axis. The process of quantum searching in this $SO(3)$ picture is to rotate the state vector from a position nearly parallel to $-z$ to the $+z$-axis.

The effect of a step in a generalized quantum search can be characterized by a rotation about a rotational axis in space. The rotational axis of (3) can be found by solving the eigenvalue problem, $R_u\boldsymbol{l} = \boldsymbol{l}$. This gives

$$\boldsymbol{l} = \begin{pmatrix} \cot\frac{\phi}{2} \\ 1 \\ -\cot 2\beta\cot\frac{\phi}{2} + \cot\frac{\theta}{2}\csc 2\beta \end{pmatrix}. \tag{5}$$

The rotational angle in an iteration is given by

$$\alpha = \arccos\left[\frac{1}{4}(\cos 4\beta + 3)\cos\theta\cos\phi + \sin^2 2\beta\left(\frac{1}{2}\cos\phi - \sin^2\frac{\theta}{2}\right) + \cos 2\beta\sin\theta\sin\phi\right]. \tag{6}$$

As a simple application, we discuss Grover's algorithm. Here $\theta = \phi = \pi$, the rotation axis is exactly the y-axis and the rotational angle is equal to the maximum value of 4β (note that this corresponds a rotation angle of 2β in the $SU(2)$ space). The state vector $\boldsymbol{r}$ is rotated within the x–z-plane from the $-z$- to the $+z$-axis, where the marked state achieves maximum probability. The number of steps required to reach the $+z$-axis is $\frac{\pi-2\beta}{\alpha} \approx 0.785\sqrt{N} - 0.5 \approx 0.785\sqrt{N}$, which is exactly what has been given by Grover. The tip of the state vector $\boldsymbol{r}$ spans a circle in the x–z-plane as shown in figure 2. In particular, we notice that this circle is a meridian.

Now we look at the general case with arbitrary θ and ϕ. If we require that the quantum search algorithm find the marked state with certainty, this $SO(3)$ framework gives exactly the

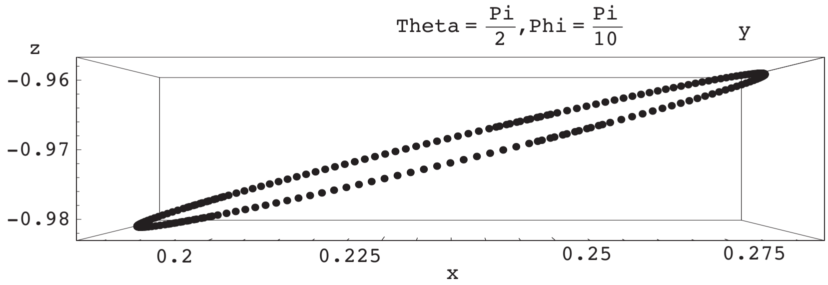

Figure 3. Three-dimensional plot of the trace of the vector state tip when the phase mismatches.

phase matching requirement found in [12]. Here the trace of the tip of the state vector $\boldsymbol{r}$ is also a circle. The state vector spans a cone with the top at the origin. During the rotation, the vector $\boldsymbol{r} - \boldsymbol{r}_o$ is orthogonal to the rotational axis $\boldsymbol{l}$ at any time: $(\boldsymbol{r} - \boldsymbol{r}_o) \cdot \boldsymbol{l} = 0$. When the state vector passes through the $+z$-axis, $(0, 0, 1)^T$ must be in the trace. Then the algorithm can find the marked item with certainty. By solving equation $\boldsymbol{r} - \boldsymbol{r}_a \cdot \boldsymbol{l} = 0$, we have $\cot\frac{\phi}{2} = \cot\frac{\theta}{2}$, or $\phi = \theta$, the phase matching requirement. Now we can look at the difference between the standard Grover algorithm and the generalized quantum search algorithm with phase matching. In a general case, the rotational axis is

$$\boldsymbol{l} = \begin{pmatrix} \cos\frac{\phi}{2} \\ \sin\frac{\phi}{2} \\ \cos\frac{\phi}{2}\tan\beta \end{pmatrix} \tag{7}$$

which is not the y-axis. In general, the circle spanned by the state vector is no longer a meridian, unless $\cos\frac{\phi}{2} = 0$. The rotation angle is

$$\alpha = \arccos\left\{2\left[(\cos 2\beta - 1)\sin^2\frac{\phi}{2} + 1\right]^2 - 1\right\}. \tag{8}$$

Thus the generalized algorithm can find the marked state with more iteration steps. However, the algorithm cannot reach the $-z$-axis, which means that the probability of finding the marked state at any stage is greater than zero.

From the exact formulae in the $SO(3)$ picture, it is easy to obtain the approximate formulae derived in [12]. If N is very large,

$$\boldsymbol{l} \approx \begin{pmatrix} \cos\frac{\phi}{2} \\ \sin\frac{\phi}{2} \\ 0 \end{pmatrix}$$

which is in the x–y-plane, and the initial state vector is nearly the $-z$-axis. The trace of the tip of the state vector is a circle in the x–z-plane. The circle spanned by the state vector is approximately a meridian. Each iteration rotates the state vector an angle α given by (11). To first order in β, $\alpha \approx 4\beta\sin\frac{\phi}{2}$, which corresponds a rotation of $2\beta\sin\frac{\phi}{2}$ in $SU(2)$. The number of steps required to search the marked state is larger than that in the original version, as given in [12].

When $\theta \neq \phi$, the trace the tip of the state vector is still a circle, but it is very tilted. In figure 3, it is drawn for the case of $\theta = \frac{\pi}{2}$, $\phi = \frac{\pi}{10}$. Here we see the rotating axis is nearly the z-axis and the circle spanned by the state vector tip is nearly parallel to the x–y-plane. The amplitude of the marked state cannot reach unity; neither can it reach zero. This explains naturally the intriguing narrowly bounded behaviour of the algorithm we have found in [11].

It is seen that to achieve a useful quantum search algorithm, the phase matching requirement $\theta = \phi$ must be satisfied. With equation (8), it is convenient to calculate the exact amount of phase rotation in a specific algorithm. This phase matching condition is also easy to implement experimentally. The two auxiliary qubits can be combined for a search algorithm with phase matching, saving useful qubit resources.

To summarize, we have given a novel $SO(3)$ picture of the quantum search algorithm. In this picture, the effect of quantum search is clearly displayed. The status of the quantum search algorithm at any stage can be given exactly. In this picture, the phase matching requirement is clearly understood. With these results, it is convenient to apply the quantum search algorithm to other quantum algorithms. The results here can be generalized to multiple-item searching directly. It will be interesting to generalize the picture to other cases, for example, quantum searching with arbitrary initial amplitudes.

Acknowledgments

The authors thank Professor Y D Zhang for helpful discussions. Partial support from China National Natural Science Foundation, the Ministry of Education, the FoK Ying Tung Education Foundation and the Basic Research Fund of Tsinghua University are gratefully acknowledged.

References

[1] Grover L K 1997 *Phys. Rev. Lett.* **79** 325
[2] Grover L K 1997 *Phys. Rev. Lett.* **79** 4709
[3] Zalka C 1999 *Phys. Rev.* A **60** 2746
[4] Biham E, Biham O, Biron D, Grassl M and Lidar D A 1999 *Phys. Rev.* A **60** 2742
[5] Brassard G and Höyer P 1998 *Lecture Notes in Computer Science* vol 1443 (Demark: Aaborg) pp 820–31
[6] Brassard G, Höyer P and Tapp A 1997 *5th Israeli Symp. on Theory of Computing and Systems (ISTCS'97)* (Piscataway, NJ: IEEE Computer Society Press) pp 12–23
[7] Chuang I L, Gershenfeld N and Kubinee M 1998 *Phys. Rev. Lett.* **80** 3408
[8] Jones J A, Mosca M and Hansen R H 1998 *Nature* **393** 344
[9] Vandersypen L M K *et al* 2000 *Appl. Phys. Lett.* **76** 646
[10] Han Q Z and Sun H Z 1987 *Group Theory* (Peking University Press)
Sun H Z and Han Q Z 1999 *Lie Algebras and Lie Superalgebras and Their Applications in Physics* (Beijing: Peking University Press)
[11] Long G L *et al* 1999 *Commun. Theor. Phys.* **32** 335
[12] Long G L *et al* 1999 *Phys. Lett.* A **262** 27
[13] Long G L *et al* 2000 *Phys. Rev.* A **61** 042305
[14] Yu S and Sun C P 1999 *Preprint* quant-ph/990375