Theoretical and Mathematical Physics, **144**(3): 1279–1287 (2005)

PHASE CONDITION FOR THE GROVER ALGORITHM

D.-F. Li,* X.-X. Li,† and H.-T. Huang‡

For the Grover algorithm, we derive the exact formula of the norm of the amplitude in the marked state in a sine-function form and use this formula to derive the necessary and sufficient phase condition $\sin\Delta \le |\beta|$ *for this algorithm with arbitrary phase rotations. We show that the condition of identical rotation angles* $\theta = \phi$*, which is a special case of our condition, is a sufficient but not necessary phase condition.*

Keywords: Grover algorithm, quantum search algorithm, phase condition

1. Introduction

Quantum algorithms standardly use two techniques: Fourier transforms [1] and amplitude amplification. The Grover search algorithm is based on the latter. The problem addressed by the Grover algorithm is to find a marked term (or *target* term in [2]) in an unsorted database of size N. To accomplish this, a quantum computer needs $O\big(\sqrt{N}\big)$ queries using the Grover algorithm [3]. In Grover's original version [3], the algorithm consists of a sequence of unitary operations on a pure state, i.e., the algorithm is $Q = -I_0^{(\pi)} W I_\tau^{(\pi)} W$, where W is the Walsh–Hadamard transformation and $I_x^{(\pi)} = I - 2|x\rangle|\langle x|$, which inverts the amplitude in the state $|x\rangle$; here, $I_0^{(\pi)}$ and $I_\tau^{(\pi)}$ invert the amplitudes in the respective initial and marked basis states $|0\rangle$ and $|\tau\rangle$. To extend his original algorithm, Grover [2] replaced the Walsh–Hadamard transformation with any quantum mechanical operation and thus obtained the quantum search algorithm $Q = -I_\gamma^{(\pi)} U^{-1} I_\tau^{(\pi)} U$, where U is any unitary operation and U^{-1} is the adjoint (the complex conjugate of the transpose) of U. Boyer et al. gave analytic expressions for the amplitude of the states for the original Grover algorithm with the Walsh–Hadamard transformation and the inversion of the amplitudes and established tight bounds on quantum searching [4]. To generalize the Grover algorithm further, we must allow amplitudes to be rotated by arbitrary phases, not just be inverted. An example is the quantum algorithm $Q = -I_\gamma^{(\theta)} U^{-1} I_\tau^{(\phi)} U$, where θ and ϕ are the rotation angles of the amplitude phases in the respective initial basis state $|\gamma\rangle$ and marked basis state $|\tau\rangle$. Recently, several authors have contributed to general quantum search algorithms with any unitary operations and arbitrary phase rotations [5]–[10].

For general quantum search algorithms, the following problems must be solved:

1. What is the amplitude in the marked state after k applications of Q?
2. What are the rotation angles in the initial and marked basis states to reach the marked state from the initial state? This problem is called the *phase condition*.
3. What is the optimum number of iteration steps to find the marked state?
4. Which of the general algorithms is the most efficient?

*Department of Mathematical Sciences, National Laboratory for Artificial Intellect at Tsinghua University, Tsinghua University, Beijing, China, e-mail: dli@math.tsinghua.edu.cn.

†Department of Computer Science, Wayne State University, Detroit, Mich., USA.

‡Electrical Engineering and Computer Science Department, University of Michigan, Ann Arbor, Mich., USA.

Translated from Teoreticheskaya i Matematicheskaya Fizika, Vol. 144, No. 3, pp. 472–483, September, 2005. Original article submitted October 26, 2003; revised March 4, 2005.

Our motivation for this paper is as follows. Since Grover presented the phase condition, several authors discussed this condition. To find the marked state with certainty, Long et al. presented a matching condition: identical rotation angles $\theta = \phi$ [5]. Høyer next gave the phase condition $\tan(\theta/2) = \tan(\phi/2)(1-2a)$ [7]. Biham et al. then used a recursive equation to study the quantum search algorithm and reported that for different rotation angles $\theta \neq \phi$, the algorithm fails to enhance the probability of measuring a marked state and that for the algorithm to be applicable, the two rotation angles must therefore be equal, $\theta = \phi$ [9]. It follows from the conclusion of Biham et al. that identical rotation angles $\theta = \phi$ is a necessary and sufficient phase condition. At least four papers reported identical rotation angles as the phase condition [5], [8], [9]. It then becomes an open question what the necessary and sufficient phase condition is for the Grover algorithm with arbitrary phase rotations. In this paper, we present the phase condition $\sin\Delta \leq |\beta|$, which is necessary and sufficient for finding the marked state, and thus solve the phase condition problem posed by Grover in [2]. We also indicate that the condition of identical rotation angles $\theta = \phi$, which is a special case of our condition, is sufficient but not necessary to find the marked state. Using the exact phase condition, we can construct quantum algorithms with arbitrary rotations that succeed with certainty.

This paper is organized as follows. In Sec. 3, we derive the exact expression for the norm of the amplitude in the marked state in a sine-function form. In Sec. 4, we use this exact formula to present the necessary and sufficient phase condition for the Grover algorithm with arbitrary phase rotations. In Sec. 5, we show that identical rotation angles $\theta = \phi$ is a sufficient but not necessary phase condition for finding the marked state.

2. The Grover algorithm with arbitrary phase rotations

The original Grover search algorithm [3] was presented for the following search problem. In an unsorted database containing N items, there is one item with a known property. We want to find the item (called the marked term). To retrieve the marked term from N terms, the original Grover search algorithm repeats the following unitary operations alternately: a phase rotation R_1 and an inversion about the average D. Furthermore, Grover showed that the inversion about the average takes the form $D = WR_2W$, where R_2 is the phase rotation matrix. Grover then presented the quantum search algorithm [2]: $Q = -I_\gamma^{(\pi)} U^{-1} I_\tau^{(\pi)} U$, where U is any unitary operator, $|\gamma\rangle$ is the initial basis state, $|\tau\rangle$ is the marked basis state, and $I_x^{(\pi)} = I - 2|x\rangle|\langle x|$, which inverts the amplitude in the state $|x\rangle$. When $U^{-1} = U = W$ and $|\gamma\rangle = |0\rangle$, this reduces to the original Grover search algorithm. Furthermore, Grover derived the property

$$Q \begin{pmatrix} |\gamma\rangle \\ U^{-1}|\tau\rangle \end{pmatrix} = \begin{pmatrix} 1-4|U_{\tau\gamma}|^2 & 2U_{\tau\gamma} \\ -2U_{\tau\gamma}^* & 1 \end{pmatrix} \begin{pmatrix} |\gamma\rangle \\ U^{-1}|\tau\rangle \end{pmatrix},$$

where $U_{\tau\gamma} = \langle\tau|U|\gamma\rangle$ and $U_{\tau\gamma}^* = \langle\gamma|U|\tau\rangle$, which is the complex conjugate of $U_{\tau\gamma}$ (see expression (6) in [2]). He interpreted this property as follows: Q preserves the two-dimensional vector space spanned by $|\gamma\rangle$ and $U^{-1}|\tau\rangle$.

The Grover algorithm finds the marked state $|\tau\rangle$ among N states using the amplitude amplification technique. It starts with the initial basis state $|\gamma\rangle$ and applies the operator Q $O\big(\sqrt{N}\big)$ times. The initial basis state $|\gamma\rangle$ is then transformed to $U^{-1}|\tau\rangle$. The last application of U to $U^{-1}|\tau\rangle$ leads to the marked state $|\tau\rangle$. To compute $Q^k|\gamma\rangle$, we must take into account that Q preserves the two-dimensional vector space spanned by $|\gamma\rangle$ and $U^{-1}|\tau$. It follows from this property that $Q|\gamma\rangle = \big(1-4|U_{\tau\gamma}|^2\big)|\gamma\rangle + 2U_{\tau\gamma}\big(U^{-1}|\tau\rangle\big)$. We assume that $Q^k|\gamma\rangle = a_k|\gamma\rangle + b_k\big(U^{-1}|\tau\rangle\big)$. We can then evaluate $Q^{k+1}|\gamma\rangle = Q\big(Q^k|\gamma\rangle\big) = a_kQ|\gamma\rangle + b_kQ\big(U^{-1}|\tau\rangle\big)$ if we again take into account that Q preserves the two-dimensional vector space spanned by $|\gamma\rangle$ and $U^{-1}|\tau\rangle$. This property of the operator Q guarantees the success of the search algorithm.

In 1999, Long presented the search algorithm [5]

$$Q = -I_\gamma U^{-1} I_\tau U, \qquad I_\gamma = I - (-e^{i\theta}+1)|\gamma\rangle|\langle\gamma|, \qquad I_\tau = I - (-e^{i\phi}+1)|\tau\rangle|\langle\tau|.$$

When $\theta = \phi = \pi$, $U^{-1} = U = W$, and $|\gamma\rangle = |0\rangle$, it reduces to the Grover algorithm. Long showed that Q preserves the two-dimensional vector space spanned by $|\gamma\rangle$ and $U^{-1}|\tau\rangle$ (see expression (4) in [5]). In 2000, Høyer defined the search algorithm $Q = -AS_0(\phi)A^{-1}S_\chi(\varphi)$ and proved that Q preserves the two-dimensional vector space spanned by $1/\sqrt{a}\,|\psi_1\rangle$ and $1/\sqrt{b}\,|\psi_0\rangle$ (see expression (3) in [7]).

In [6], we introduced the search algorithm

$$Q = -I_\gamma U^{-1} I_\tau U, \qquad I_\gamma = I - 2\cos\theta e^{i\theta}|\gamma\rangle|\langle\gamma|, \qquad I_\tau = I - 2\cos\phi e^{i\phi}|\tau\rangle|\langle\tau|,$$

where θ and ϕ are real. When $\theta = \phi = 0$, it reduces to the Grover algorithm [2]. We showed that Q preserves the vector space spanned by $|\gamma\rangle$ and $U^{-1}|\tau\rangle$:

$$Q\begin{pmatrix} |\gamma\rangle \\ U^{-1}|\tau\rangle \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \lambda & \delta \end{pmatrix}\begin{pmatrix} |\gamma\rangle \\ U^{-1}|\tau\rangle \end{pmatrix},$$

where

$$\begin{aligned} &\alpha = -1 + 2\cos\theta e^{i\theta} - 4\cos\theta e^{i\theta}\cos\phi e^{i\phi}|U_{\tau\gamma}|^2, \qquad \beta = 2U_{\tau\gamma}\cos\phi e^{i\phi}, \\ &\lambda = 2\cos\theta e^{i\theta}(1 - 2\cos\phi e^{i\phi})U^*_{\tau\gamma}, \qquad \delta = 2\cos\phi e^{i\phi} - 1. \end{aligned} \tag{1}$$

After k applications of Q in this algorithm, as soon as the state $U^{-1}|\tau\rangle$ is attained, the next application of U sets the state of the quantum computer to $|\tau\rangle$, the marked state.

In this paper, all discussions and derivations are based on this algorithm. The results obtained in this paper also hold for the Grover, Høyer, and Long et al. algorithms and for any quantum search algorithm that preserves a two-dimensional vector space if the result depends only on α, β, λ, and δ.

3. The exact formula for the amplitude

For a quantum search algorithm Q, the key problem is to determine the amplitude in the marked state after k applications of Q. In this section, we derive an exact formula for the amplitude in a sine-function form. Let $Q|\gamma\rangle = \alpha|\gamma\rangle + \beta\big(U^{-1}|\tau\rangle\big)$, $Q\big(U^{-1}|\tau\rangle\big) = \lambda|\gamma\rangle + \delta\big(U^{-1}|\tau\rangle\big)$, and $Q^k|\gamma\rangle = a_k|\gamma\rangle + b_k\big(U^{-1}|\tau\rangle\big)$, where a_k and b_k are the amplitudes in the respective initial state $|\gamma\rangle$ and marked state $U^{-1}|\tau\rangle$.

In [6], we showed that $b_k = \beta r_k$. When $\beta = 0$ ($\cos\phi = 0$), we just have $|b_k| = 0$, and the quantum algorithm becomes useless. We therefore assume that $\beta \neq 0$ ($\cos\phi \neq 0$).

3.1. A simpler recursive formula for the amplitude b_k. The recursive formulas for a_k and b_k obtained in [6] are $a_{k+1} = (\alpha a_k + \lambda b_k)$ and $b_{k+1} = (\beta a_k + \delta b_k)$. We note that the recursive formulas for a_k and b_k contain the respective terms b_k and a_k. We can propose a simpler recursive formula $b_{k+1} = \beta(\alpha a_{k-1} + \lambda b_{k-1}) + \delta b_k = (\alpha+\delta)b_k + (\beta\lambda - \alpha\delta)b_{k-1}$. Clearly, the formula for b_{k+1} does not contain the term a_k. We can also derive a simpler recursive formula for the amplitude a_k: $a_{k+1} = (\alpha+\delta)a_k + (\beta\lambda - \alpha\delta)a_{k-1}$. Here, $a_k = r_{k+1} - \delta r_k$ because $b_{k+1} = \beta r_{k+1}$.

Because $b_k = \beta r_k$ and β does not contain k, we only need to derive the exact formula for r_k in a sine-function form. We first derive the recursive formula for r_k. After computing $b_1 = \beta$ and $b_2 = \beta(\alpha+\delta)$, we obtain $r_1 = 1$, $r_2 = \alpha + \delta$, and $r_{k+1} = (\alpha+\delta)r_k + (\beta\lambda - \alpha\delta)r_{k-1}$. For the Grover algorithm, $r_1 = 1$, $r_2 = \alpha + 1$, and $r_{k+1} = (\alpha+1)r_k - r_{k-1}$.

3.2. The expression for r_k. Clearly, $z^2-(\alpha+\delta)z+(\alpha\delta-\beta\lambda)$ is the characteristic polynomial of the algorithm Q relative to the basis. Then, $\det Q=\alpha\delta-\beta\lambda=\det\bigl(-I_\gamma^{(x)}U^{-1}I_\tau^{(y)}U\bigr)=e^{i(x+y)}$, where x and y are the real rotation angles.

Let $r_{k+1}=(z_1+z_2)r_k-z_1z_2r_{k-1}$, where $z_1+z_2=\alpha+\delta$ and $z_1z_2=\alpha\delta-\beta\lambda$, i.e., z_1 and z_2 are the eigenvalues of Q. We then obtain $(z_1-z_2)r_{k+1}=z_1^{k+1}-z_2^{k+1}$ (see Appendix A for the detailed derivation). From Result 6 in Appendix B, we know that $z_1\ne z_2$ if $\cos\phi\ne0$. Therefore, $r_{k+1}=(z_1^{k+1}-z_2^{k+1})/(z_1-z_2)$.

Let $z_1=\rho_1e^{i\psi_1}$ and $z_2=\rho_2e^{i\psi_2}$, where $\rho_1>0$ and $\rho_2>0$. Because $|z_1z_2|=1$, we have $\rho_1\rho_2=1$. Let $\rho_1=\rho$. Then $\rho_2=1/\rho$, $z_1+z_2=2\bigl(\cos(\theta-\phi)-2|U_{\tau\gamma}|^2\cos\theta\cos\phi\bigr)e^{i(\theta+\phi)}$, and $(\rho^2-1)\sin\bigl(\psi_1-(\theta+\phi)\bigr)=0$. We note that $\psi_1+\psi_2=2(\theta+\phi)$.

There are two cases.

Let $\rho\ne1$. Then $\sin\bigl(\psi_1-(\theta+\phi)\bigr)=0$, and we obtain $\psi_1=\psi_2$. Let $z_1=\rho e^{i\psi}$. Then $z_2=e^{i\psi}/\rho$, $z_1+z_2=(\rho+1/\rho)e^{i\psi}$, and Results 4 and 5 in Appendix B imply that $2<\rho+1/\rho=|\alpha+\delta|\le2$. Therefore, $\rho\ne1$ is impossible.

Let $\rho=1$, $z_1=e^{i\psi_1}$, and $z_2=e^{i\psi_2}$. Then $r_k=\sin(k\Delta)\,e^{i(k-1)(\theta+\phi)}/\sin\Delta$, where $\Delta=(\psi_1-\psi_2)/2$. We next compute Δ. Clearly,

$$z_1+z_2=2\cos\frac{\psi_1-\psi_2}{2}\,e^{i(\psi_1+\psi_2)/2}.$$

Let $p=|U_{\tau\gamma}|$. We then obtain $\Delta=\arccos\bigl(\cos(\theta-\phi)-2p^2\cos\theta\cos\phi\bigr)=\arccos\bigl(e^{-i(\theta+\phi)}\operatorname{tr}Q\bigr)$, where $\operatorname{tr}Q$ is the trace of Q (see Result 2 in Appendix B). Because $\cos\phi\ne0$, we conclude that $\psi_1\ne\psi_2$. Without loss of generality, we let $\psi_1>\psi_2$. Then

$$\sin\Delta=\sqrt{1-\frac{|\alpha+\delta|^2}{4}}=\sqrt{1-\bigl(\cos(\theta-\phi)-2p^2\cos\theta\cos\phi\bigr)^2}>0.$$

3.3. The exact formula for the amplitude b_k. Obviously,

$$b_k=\beta r_k=2p\cos\phi\,e^{i((k-1)(\theta+\phi)+\phi)}\sin(k\Delta)/\sin\Delta,$$

and for each application of the Grover algorithm, the phase of the amplitude in the marked state increases by $\theta+\phi$. From the above definition of Δ, we then have $|b_k|=|\beta|\,|\sin(k\Delta)|/\sin\Delta$, where $|\beta|=2p|\cos\phi|$.

Remark 1. The formula for b_k holds for the Grover, Long et al., and Høyer algorithms and for any other quantum search algorithm that preserves a two-dimensional vector space.

The expression for b_k can be simplified for identical rotation angles $\theta=\phi$ and for the Grover algorithm. Let $|b_k|=|\beta|\,|\sin(k\Delta)|/\sin\Delta$, where

$$\Delta=\frac{\psi_1-\psi_2}{2},\qquad \psi_1-\psi_2=\arccos\bigl\{2(1-2p^2\cos^2\phi)^2-1\bigr\},$$

$$\sin\Delta=2p|\cos\phi|\sqrt{1-p^2\cos^2\phi}\,.$$

In [5], using many transformations, the authors derived the approximate formula for the amplitude in the marked state.

We consider the Grover algorithm $Q=-I_\gamma^{(\pi)}U^{-1}I_\tau^{(\pi)}U$. In this case, it is easy to see that $\alpha=1-4|U_{\tau\gamma}|^2$, $\beta=2U_{\tau\gamma}$, $\lambda=-2U_{\tau\gamma}^*$, and $\delta=1$ and that the characteristic equation in Sec. 3.2 becomes $z^2-(\alpha+1)z+1=0$. We let the characteristic roots be $z_1=e^{i\xi}$ and $z_2=e^{-i\xi}$. Then

$$\cos\xi=1-2p^2,\qquad z_1^k-z_2^k=2i\sin(k\xi),\qquad r_k=\frac{\sin(k\xi)}{\sin\xi},$$

which can also be obtained using the formulas in Sec. 3.2 by letting $\psi_1=\xi$ and $\psi_2=-\xi$. Finally, we have

$$b_k=\beta\frac{\sin(k\xi)}{\sin\xi},\qquad |b_k|=2p\frac{|\sin(k\xi)|}{|\sin\xi|}.$$

4. The necessary and sufficient phase condition

We deduce a necessary and sufficient phase condition to be imposed on arbitrary phase rotations in order to find the marked state with certainty.

4.1. The necessary and sufficient phase condition $\sin\Delta \le |\beta|$.

Theorem. *An algorithm can find the marked state with certainty, i.e., there exists a number k such that $|b_k| = 1$, if and only if*

$$\sin\Delta = \sqrt{1 - \frac{|\alpha+\delta|^2}{4}} = \sqrt{1 - \big(\cos(\theta-\phi) - 2p^2\cos\theta\cos\phi\big)^2} \le |\beta|.$$

Proof. If $|b_k| = 1$, i.e., $|b_k| = |\beta|\,|\sin(k\Delta)|/\sin\Delta = 1$ for some k, then $|\sin(k\Delta)| = \sin\Delta/|\beta|$. Clearly, $\sin\Delta/|\beta| \le 1$. Therefore, $\sin\Delta \le |\beta|$. Let k_o be the optimum number of iteration steps to find the marked state with certainty. Then

$$k_\mathrm{o} = \frac{1}{\Delta}\arcsin\frac{\sin\Delta}{|\beta|}, \tag{2}$$

where $|b_{k_\mathrm{o}}| = 1$.

Conversely, if $\sin\Delta \le |\beta|$ and k_o is given by (2), then $|b_{k_\mathrm{o}}| = |\beta|\,|\sin k_\mathrm{o}\Delta|/\sin\Delta = 1$. The proof is complete.

The phase condition can be also written as $2\sqrt{1-|\beta|^2} \le |\operatorname{tr} Q|$. The phase condition holds for the Long et al. and Høyer algorithms and for any other quantum search algorithm that preserves a two-dimensional vector space.

From the general phase condition, we obtain two corollaries, whose proofs are in Appendix C. These corollaries are convenient for verifying whether an algorithm satisfies the phase condition. We recall that $p = |U_{\tau\gamma}|$.

Corollary 1. *Let $p < 1/2$ and θ and ϕ either lie in the same quadrant or satisfy $|\theta-\phi| < \pi/2$ and $\cos\theta\cos\phi < 0$. Then $\sin\Delta \le |\beta|$, and the algorithm can find the marked state with certainty if and only if*

$$|\theta-\phi| \le \arccos\big(2p^2\cos\theta\cos\phi + \sqrt{1-4p^2\cos^2\phi}\,\big).$$

Corollary 2. *Let θ and ϕ either lie in the same quadrant or satisfy $\cos\theta\cos\phi < 0$ and $\sin\theta\sin\phi < 0$. Then $\sin\Delta > |\beta|$, and the algorithm cannot find the marked state with certainty if $\big|\sin(\theta-\phi)\big| > |\beta|$.*

4.2. The optimum number of iteration steps. In the case of identical rotation angles $\theta = \phi$, we can reduce the optimum number k_o of iteration steps. In this case,

$$k_\mathrm{o} = \frac{\arcsin\sqrt{1-p^2\cos^2\phi}}{\arcsin\big(2p|\cos\phi|\sqrt{1-p^2\cos^2\phi}\,\big)}.$$

Let $p\cos\phi = \sin\xi$. Then $k_\mathrm{o} = (\pi-2\xi)/4\xi = \pi/4\xi - 1/2$. When $\phi = 0$, we have $p = \sin\xi$, and k_o is just the optimum number of iteration steps for the Grover algorithm in [2]. Moreover, let $p = \sqrt{1/N}$. Then $k_\mathrm{o} = (\pi-2\theta)/4\theta$ is the optimum number of iteration steps for the original Grover algorithm when $\sin^2\theta = 1/N$ [4]. In [5], the authors obtained an approximate formula for the optimum number of iterations for identical rotation angles. There, the authors set $U_{\tau\gamma} = e^{i\zeta}\sin\beta$. Then $\sin\beta = p$, which is also different from $\sin\xi = p\cos\phi$.

Let $p = 1/\sqrt{N}$, where $N = 2^{10}$. The exact optimum numbers of iterations are collected in Table 1. For the original Grover algorithm, the optimum number of iterations is 24.625.

Table 1

ϕ	$4\pi/9$	$5\pi/12$	$\pi/3$	$\pi/4$	$\pi/5$	$\pi/6$	$\pi/8$	$\pi/10$	$\pi/15$
k_{o}	144.21	96.590	49.763	35.037	30.561	28.516	26.699	25.922	25.515

Remark 2. If the phase condition $\sin\Delta \le |\beta|$ is satisfied, then the optimum number of iteration steps to find the marked state with certainty is given by (2). Taking the phase condition into account, we obtain $0 < k_{\mathrm{o}}\Delta = \arcsin(\sin\Delta/|\beta|) \le \pi/2$. Hence, for $0 < k\Delta \le k_{\mathrm{o}}\Delta \le \pi/2$, we have $|\sin(k\Delta)| = \sin(k\Delta)$ and $|b_k| = |\beta|\sin(k\Delta)/\sin\Delta$. Therefore, $|b_k|$, considered as a function of k, increases strictly monotonically as k increases from zero to k_{o}.

5. Identical rotation angles are not necessary

In this section, we show that the condition of identical rotation angles $\theta = \phi$ is sufficient but not necessary for finding the marked state with certainty.

5.1. Identical rotation angles condition is sufficient. Given $\theta = \phi$, we have

$$\sin\Delta = 2p|\cos\phi|\sqrt{1 - p^2\cos^2\phi}$$

and consequently $\sin\Delta/|\beta| = \sqrt{1 - p^2\cos^2\phi} \le 1$. Therefore, for $\theta = \phi$, the phase condition in Sec. 4 implies that the quantum algorithm Q can find the marked state with certainty in all cases except $I_\gamma = I_\tau = I$.

5.2. Identical rotation angles condition is not necessary. We present examples demonstrating that the condition $\theta = \phi$ is not necessary and that we can choose nonidentical rotation angles for finding the marked state with certainty if these angles satisfy the phase condition in Sec. 4.

Example 1. Let $\phi = 0$. Then $\sin\Delta \le |\beta|$, and the algorithm can find the marked state with certainty if and only if $|\sin\theta| \le 2p^2/|1 - 2p^2|$.

Indeed, the phase condition at $\phi = 0$ gives

$$\frac{\sin\Delta}{|\beta|} = \frac{\sqrt{1 - (1 - 2p^2)^2\cos^2\theta}}{2p} \le 1,$$

which is equivalent to $|\sin\theta| \le 2p^2/|1 - 2p^2|$.

For instance, for $p = 0.5$, $\phi = 0$, and $\theta = \pi/3$, we have $\sin\pi/3 < 2p^2/|1 - 2p^2| = 1$, and the phase condition is therefore satisfied. In this case, $k_{\mathrm{o}} = 1$.

Example 2. We assume that $\theta = 0$. It is then easy to show that $\sin\Delta \le |\beta|$ if and only if $\cos^2\phi \ge 1/(1 + 4p^4)$.

Examples 1 and 2 demonstrate that the condition of identical rotation angles $\theta = \phi$ is not necessary for finding the marked state with certainty; nevertheless, identical rotation angles $\theta = \phi$ is an important case of the phase condition.

Acknowledgments. The authors thank Cheng Guo for the helpful discussion about the simpler recursive formula for the amplitudes.

This work was supported in part by the NSFC (Grant No. 60433050), the basic research fund of Tsinghua University (Grant No. JC2003043), and the State Key Laboratory of Intelligence Technology and System.

Appendix A

Starting from the recursive relation $r_{k+1} = (\alpha+\delta)r_k + (\beta\lambda - \alpha\delta)r_{k-1}$, we can derive the exact formula for b_k in a sine-function form. Let

$$r_{k+1} = (z_1 + z_2)r_k - z_1 z_2 r_{k-1}, \tag{3}$$

where $z_1 + z_2 = \alpha + \delta$ and $z_1 z_2 = -(\beta\lambda - \alpha\delta)$. We note that $r_1 = 1$ and $r_2 = \alpha + \delta = z_1 + z_2$. Then $r_{k+1} = z_1 r_k + z_2 r_k - z_1 z_2 r_{k-1}$, and we obtain

$$r_{k+1} - z_1 r_k = z_2 r_k - z_1 z_2 r_{k-1} = z_2(r_k - z_1 r_{k-1}), \tag{4}$$

$$r_{k+1} - z_2 r_k = z_1 r_k - z_1 z_2 r_{k-1} = z_1(r_k - z_2 r_{k-1}). \tag{5}$$

Using (4), we obtain

$$r_{k+1} - z_1 r_k = z_2(r_k - z_1 r_{k-1}) = z_2^2(r_{k-1} - z_1 r_{k-2}) = \cdots = z_2^{k-1}(r_2 - z_1 r_1),$$

and therefore

$$r_{k+1} - z_1 r_k = z_2^{k-1}(r_2 - z_1 r_1). \tag{6}$$

Analogously, taking (5) into account, we obtain

$$r_{k+1} - z_2 r_k = z_1^{k-1}(r_2 - z_2 r_1). \tag{7}$$

Hence,

$$\begin{aligned} z_1 r_{k+1} - z_2 r_{k+1} &= z_1^k(r_2 - z_2 r_1) - z_2^k(r_2 - z_1 r_1) = \\ &= z_1^k(z_1 + z_2 - z_2) - z_2^k(z_1 + z_2 - z_1) = z_1^{k+1} - z_2^{k+1}. \end{aligned}$$

We note that $r_2 = z_1 + z_2$ and $r_1 = 1$.

From Result 6 in Appendix B, we have $z_1 \neq z_2$ if $\cos\phi \neq 0$, and therefore

$$r_{k+1} = \frac{z_1^{k+1} - z_2^{k+1}}{z_1 - z_2}.$$

Appendix B

Several results are collected here. First, α, β, λ, and δ in (1) can be rewritten as

$$\begin{aligned} &\alpha = e^{i2\theta} - (e^{i2\theta} + 1)(e^{i2\phi} + 1)|U_{\tau\gamma}|^2, \qquad \beta = (e^{i2\phi} + 1)U_{\tau\gamma}, \\ &\lambda = -e^{i2\phi}(e^{i2\theta} + 1)U_{\tau\gamma}^*, \qquad \delta = e^{i2\phi}. \end{aligned}$$

Then we have

$$\begin{aligned} &\beta\lambda = -e^{i2\phi}(e^{i2\phi} + 1)(e^{i2\theta} + 1)|U_{\tau\gamma}|^2, \\ &\alpha\delta = e^{i2\phi}\big(e^{i2\theta} - (e^{i2\theta} + 1)(e^{i2\phi} + 1)|U_{\tau\gamma}|^2\big). \end{aligned}$$

Result 1. $\alpha\delta - \beta\lambda = e^{i2(\theta+\phi)}$ (we recall that we set $p = |U_{\tau\gamma}|$).

Result 2.

$$\alpha + \beta = e^{i2\theta} + e^{i2\phi} - 4\cos\theta\cos\phi e^{i(\theta+\phi)}p^2 =$$

$$= 2\big(\cos(\theta-\phi) - 2p^2\cos\theta\cos\phi\big)e^{i(\theta+\phi)} =$$

$$= 2\big((1-2p^2)\cos\theta\cos\phi + \sin\theta\sin\phi\big)e^{i(\theta+\phi)}.$$

Result 3. $\big|\cos(\theta-\phi) - 2p^2\cos\theta\cos\phi\big| \le 1$, and the equality holds if and only if $\cos\theta = \cos\phi = 0$.

Proof. We note that $\cos(\theta-\phi) - 2p^2\cos\theta\cos\phi = (1-2p^2)\cos\theta\cos\phi + \sin\theta\sin\phi$, and $|1-2p^2| < 1$ if $0 < p < 1$. If $\cos\theta\cos\phi = 0$, then clearly $\big|(1-2p^2)\cos\theta\cos\phi + \sin\theta\sin\phi\big| \le 1$. We prove that $\big|(1-2p^2)\cos\theta\cos\phi + \sin\theta\sin\phi\big| < 1$ if $\cos\theta\cos\phi \ne 0$. There are several cases.

Case 1.1. Let $\cos\theta\cos\phi > 0$ and $0 < p < \sqrt{2}/2$. Then

$$0 < 1-2p^2 < 1, \qquad 0 < (1-2p^2)\cos\theta\cos\phi < \cos\theta\cos\phi,$$

$$\sin\theta\sin\phi < (1-2p^2)\cos\theta\cos\phi + \sin\theta\sin\phi < \cos(\theta-\phi) \le 1.$$

Therefore, $\big|(1-2p^2)\cos\theta\cos\phi + \sin\theta\sin\phi\big| < 1$.

Case 1.2. Let $\cos\theta\cos\phi > 0$ and $\sqrt{2}/2 \le p < 1$. Then

$$-1 < 1-2p^2 \le 0, \qquad -\cos\theta\cos\phi < (1-2p^2)\cos\theta\cos\phi \le 0,$$

$$-\cos(\theta+\phi) < (1-2p^2)\cos\theta\cos\phi + \sin\theta\sin\phi \le \sin\theta\sin\phi.$$

We also have $\big|(1-2p^2)\cos\theta\cos\phi + \sin\theta\sin\phi\big| < 1$.

Case 2.1. Let $\cos\theta\cos\phi < 0$ and $0 < p < \sqrt{2}/2$. Then

$$0 < 1-2p^2 < 1, \qquad \cos\theta\cos\phi < (1-2p^2)\cos\theta\cos\phi < 0,$$

$$\cos(\theta-\phi) < (1-2p^2)\cos\theta\cos\phi + \sin\theta\sin\phi < \sin\theta\sin\phi.$$

We also have $\big|(1-2p^2)\cos\theta\cos\phi + \sin\theta\sin\phi\big| < 1$.

Case 2.2. Let $\sqrt{\cos\theta\cos\phi} < 0$ and $\sqrt{2}/2 \le p < 1$. Then

$$-1 < 1-2p^2 \le 0, \qquad 0 \le (1-2p^2)\cos\theta\cos\phi < -\cos\theta\cos\phi,$$

$$\sin\theta\sin\phi \le (1-2p^2)\cos\theta\cos\phi + \sin\theta\sin < -\cos(\theta+\phi).$$

We also have $\big|(1-2p^2)\cos\theta\cos\phi + \sin\theta\sin\phi\big| < 1$.

Therefore, if $\cos\theta\cos\phi \ne 0$, then $\big|(1-2p^2)\cos\theta\cos\phi + \sin\theta\sin\phi\big| < 1$.

We now prove the second part. If $\big|(1-2p^2)\cos\theta\cos\phi + \sin\theta\sin\phi\big| = 1$, then we obviously have $\cos\theta\cos\phi = 0$ and $|\sin\theta\sin\phi| = 1$. Then $|\sin\theta| = |\sin\phi| = 1$ and consequently $\cos\theta = \cos\phi = 0$.

Conversely, if $\cos\theta = \cos\phi = 0$, then $|\sin\theta| = |\sin\phi| = 1$ and $\big|(1-2p^2)\cos\theta\cos\phi + \sin\theta\sin\phi\big| = 1$. This completes the proof.

Result 4. $|\alpha+\beta| = 2\big|\cos(\theta-\phi) - 2p^2\cos\theta\cos\phi\big| \le 2$, which follows trivially from Results 2 and 3.

Result 5. We assume that $\rho > 0$. Then $\rho + 1/\rho \ge 2$, and the equality holds if and only if $\rho = 1$.

Result 6. Let $z_1 + z_2 = \alpha + \beta$ and $z_1 z_2 = \alpha\delta - \beta\lambda$. Then $z_1 \ne z_2$ if $\beta \ne 0$ ($\cos\phi \ne 0$).

Proof. We suppose that $z_1 = z_2$ and $z_1 = z_2 = \rho e^{i\psi}$. Because $|z_1 z_2| = 1$, we obtain $\rho = 1$ and $|\alpha+\beta| = 2$, i.e., $\big|\cos(\theta-\phi) - 2p^2\cos\theta\cos\phi\big| = 1$. Result 3 in Appendix B then implies that $\cos\theta = \cos\phi = 0$. This contradicts the condition that $\cos\phi \ne 0$.

Appendix C

Proof of Corollary 1. If θ and ϕ are in the same quadrant, then

$$\cos(\theta-\phi)-2p^2\cos\theta\cos\phi=(1-2p^2)\cos\theta\cos\phi+\sin\theta\sin\phi>0.$$

If $|\theta-\phi|<\pi/2$ and $\cos\theta\cos\phi<0$, then $\cos(\theta-\phi)>0$ and $\cos(\theta-\phi)-2p^2\cos\theta\cos\phi>0$.

Necessity. If $\sin\Delta\le|\beta|$, then

$$\sqrt{1-\big(\cos(\theta-\phi)-2p^2\cos\theta\cos\phi\big)^2}\le|\beta|,\qquad 1-4p^2\cos^2\phi\le\big(\cos(\theta-\phi)-2p^2\cos\theta\cos\phi\big)^2.$$

Under our conditions,

$$\sqrt{1-4p^2\cos^2\phi}\le|\cos(\theta-\phi)-2p^2\cos\theta\cos\phi|=\cos(\theta-\phi)-2p^2\cos\theta\cos\phi.$$

Hence, $|\theta-\phi|\le\arccos\big(2p^2\cos\theta\cos\phi+\sqrt{1-4p^2\cos^2\phi}\big)$.

Sufficiency. Clearly, $\cos(\theta-\phi)\ge\sqrt{1-4p^2\cos^2\phi}+2p^2\cos\theta\cos\phi$. If $\cos(\theta-\phi)-2p^2\cos\theta\cos\phi>0$, then it follows from Result 3 in Appendix B that $4p^2\cos^2\phi\ge1-\big(\cos(\theta-\phi)-2p^2\cos\theta\cos\phi\big)^2\ge0$. Therefore, $\sin\Delta\le|\beta|$. This completes the proof.

It was shown in [6] that if $|\theta-\phi|<|\beta|$, then the algorithm Q finds the marked state with certainty. This is the first-order approximate phase condition. Below, we analyze the case where $|\theta-\phi|>|\beta|$.

Proof of Corollary 2. We note that if θ and ϕ are in the same quadrant, then we have

$$1-\big(\cos(\theta-\phi)-2p^2\cos\theta\cos\phi\big)^2=$$

$$=\sin^2(\theta-\phi)+4p^2\cos\theta\cos\phi\big((1-p^2)\cos\theta\cos\phi+\sin\theta\sin\phi\big)>\sin^2(\theta-\phi)$$

under the conditions of the corollary. Therefore, if $\big|\sin(\theta-\phi)\big|>|\beta|$, then $\sin\Delta>|\beta|$. This completes the proof.

REFERENCES

1. P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in: *Proc. 35th Ann. Symp. on Foundations of Computer Science* (Santa Fe, New Mexico, November 20–22, 1994, S. Goldwasser, ed.), Los Alamos, Calif., IEEE Computer Society Press (1994), p. 124.
2. L. K. Grover, *Phys. Rev. Lett.*, **80**, 4329 (1998).
3. L. K. Grover, *Phys. Rev. Lett.*, **79**, 325 (1997).
4. M. Boyer, G. Brassard, P. Høyer, and A. Tapp, *Fortschr. Phys.*, **46**, 493 (1998).
5. G. L. Long, Y. S. Li, W. L. Zhang, and Li Niu, *Phys. Lett. A*, **262**, 27 (1999).
6. Dafa Li and Xinxin Li, *Phys. Lett. A*, **287**, 304 (2001); quant-ph/0105035 (2001).
7. P. Høyer, *Phys. Rev. A*, **62**, 052304 (2000).
8. G. L. Long, Y. S. Li, W. L. Zhang, and C. C. Tu, *Phys. Rev. A*, **61**, 042305 (2000); G. L. Long, *Phys. Rev. A*, **64**, 022307 (2001).
9. E. Biham, O. Biham, D. Biron, M. Grassl, D. A. Lidar, and D. Shapira, *Phys. Rev. A*, **63**, 012310 (2000).
10. Dafa Li, Xinxin Li, H. Huang, and Xiangrong Li, *Phys. Rev. A*, **66**, 044304 (2002).