Arbitrary phases in quantum amplitude amplification

Peter Høyer*
BRICS,† Department of Computer Science, University of Aarhus, Ny Munkegade, Building 540, DK-8000 Aarhus C, Denmark
(Received 30 May 2000; published 11 October 2000)

We consider the use of arbitrary phases in quantum amplitude amplification, which is a generalization of quantum searching. We prove that the phase condition in amplitude amplification is given by $\tan(\varphi/2) = \tan(\phi/2)(1-2a)$, where ϕ and φ are the phases used and where a is the success probability of the given algorithm. Thus the choice of phases depends nontrivially and nonlinearly on the success probability. Utilizing this condition, we give methods for constructing quantum algorithms that succeed with certainty and for implementing arbitrary rotations. We also conclude that phase errors of order up to $1/\sqrt{a}$ can be tolerated in amplitude amplification.

PACS number(s): 03.67.Hk

I. INTRODUCTION

Most quantum algorithms developed so far are based on two techniques: Quantum Fourier transforms and amplitude amplification. The latter technique is a generalization of Grover's quantum algorithm for searching an unordered database [1], and it allows a quadratic speedup over any classical algorithm for many computational problems. Since amplitude amplification is fundamental for quantum algorithms it has received a great deal of attention. This includes a study of its robustness to errors and modifications. In particular, the effects of using arbitrary phases in amplitude amplification have been studied in a sequence of papers by Long *et al.* [2–5].

In this paper, we also consider the question of when arbitrary phases can be utilized in amplitude amplification. Our results complement the results of Long *et al.* who are primarily interested in the question of how large phase errors we can tolerate and still obtain a quantum algorithm for searching that succeeds with *high probability*. We are primarily interested in the question of what restrictions we need to put on the two angles used in amplitude amplification and still obtain quantum algorithms that succeed with *certainty*.

To illustrate our results, consider a database of size N with a unique marked element. In each iteration of Grover's algorithm, we rotate the phase of some states by angles ϕ and φ, respectively. The main result in Refs. [2–5] is that if the two angles differ by at most $c/\sqrt{N}$ for some appropriate constant c, that is, if $|\varphi-\phi| \leq c/\sqrt{N}$, then we can still find the marked element with high probability using only $\Theta(\sqrt{N})$ iterations. Our main result is that if the two angles satisfy the equation $\tan(\varphi/2) = \tan(\phi/2)(1-2/N)$ then we can find the marked element with certainty using only $\Theta(\sqrt{N})$ iterations. Together with the result of Long *et al.*, this provides a description of the use of arbitrary phases for bounded-error and exact quantum algorithms. It is possible to rederive the main result of Long *et al.* from our results by considering the case $\phi=\varphi$ an approximation to the perfect case $\tan(\varphi/2) = \tan(\phi/2)(1-2/N)$. (See Secs. III–V below for rigorous statements.)

We thus prove that there is phase condition in amplitude amplification, and that this condition is not that the phases are equal, but that they satisfy the trigonometric equation mentioned above. We believe that our approach is intuitive and that it yields short and straightforward proofs.

II. AMPLITUDE AMPLIFICATION

Amplitude amplification is a generalization of Grover's quantum searching algorithm that allows a speed up of many classical algorithms. The heart of amplitude amplification is an operator $\mathbf{Q}$ defined similarly to the operator used in Grover's algorithm [1]. We refer the reader to Ref. [6] and the references therein for a through introduction to amplitude amplification. Here we give only a concise description of the objects we require.

Let $\mathcal{H}$ be Hilbert space of dimension N and let $\{|0\rangle,\ldots,|N-1\rangle\}$ be an orthonormal basis for $\mathcal{H}$. Let $\mathcal{A}$ be a unitary operator on $\mathcal{H}$. We may think of $\mathcal{A}$ as a quantum algorithm that uses no measurements. Let $\chi:\{0,\ldots,N-1\}\to\{0,1\}$ be a Boolean function. We say that a basis state $|x\rangle$ is *good* if $\chi(x)=1$, and otherwise we say that $|x\rangle$ is *bad*. Given two angles $0\leq\phi,\varphi<2\pi$, define

$$\mathbf{Q}=\mathbf{Q}(\mathcal{A},\chi,\phi,\varphi)=-\mathcal{A}\mathbf{S}_0(\phi)\mathcal{A}^{-1}\mathbf{S}_\chi(\varphi). \tag{1}$$

Here, the operator $\mathbf{S}_\chi(\varphi)$ conditionally changes the phase of the amplitudes of the good states,

$$|x\rangle\mapsto\begin{cases} e^{\iota\varphi}|x\rangle & \text{if } \chi(x)=1 \\ |x\rangle & \text{if } \chi(x)=0. \end{cases} \tag{2}$$

Similarly, the operator $\mathbf{S}_0(\phi)$ multiplies the amplitude by a factor of $e^{\iota\phi}$, if and only if, the state is the zero state $|0\rangle$. Here and elsewhere we use ι to denote the principal square root of -1.

Let $|\Psi\rangle=\mathcal{A}|0\rangle$ denote the superposition obtained by applying algorithm $\mathcal{A}$ on the initial state $|0\rangle$. Let $|\Psi_1\rangle = \mathbf{P}_{\text{good}}|\Psi\rangle$, where $\mathbf{P}_{\text{good}}=\Sigma_{x:\chi(x)=1}|x\rangle\langle x|$ denotes the projection onto the subspace spanned by the good basis states,

*Email address: hoyer@brics.dk
†Basic Research in Computer Science, Center of the Danish National Research Foundation.

and similarly let $|\Psi_0\rangle = \mathbf{P}_{\text{bad}}|\Psi\rangle$ where $\mathbf{P}_{\text{bad}} = \Sigma_{x:\chi(x)=0}|x\rangle\langle x|$. Let $a = \langle\Psi_1|\Psi_1\rangle$ denote the probability that a measurement of $|\Psi\rangle = \mathcal{A}|0\rangle$ yields a good state, and let $b = \langle\Psi_0|\Psi_0\rangle$ denote the probability that a measurement of $|\Psi\rangle$ yields a bad state. We then have that $|\Psi\rangle = |\Psi_1\rangle + |\Psi_0\rangle$ and $1 = a + b$. Finally, let angle θ be so that $0 \leqslant \theta \leqslant \pi/2$ and $a = \sin^2(\theta)$.

As an example, for $N = 2^n$, we obtain Grover's searching algorithm [1] by setting $\mathcal{A}$ to be the Walsh-Hadamard transform on n qubits, letting $\chi(x)$ be 1, if and only if, the database holds a 1 at position x, and picking phases $\phi = \varphi = \pi$. If the database contains a 1 at t different positions then $a = t/N$.

The operator $\mathbf{Q}$ implements a unitary operation on the subspace spanned by $|\Psi_1\rangle$ and $|\Psi_0\rangle$. This subspace has dimension 2 if $0 < a < 1$. With respect to the ordered orthonormal basis $(1/\sqrt{a}|\Psi_1\rangle, 1/\sqrt{b}|\Psi_0\rangle)$, we can represent $\mathbf{Q} = \mathbf{Q}(\mathcal{A}, \chi, \phi, \varphi)$ by the 2×2 unitary matrix

$$M = \begin{bmatrix} -\{(1-e^{\imath\phi})a + e^{\imath\phi}\} & (1-e^{\imath\phi})\sqrt{a}\sqrt{1-a}\,e^{\imath\varphi} \\ (1-e^{\imath\phi})\sqrt{a}\sqrt{1-a} & \{(1-e^{\imath\phi})a - 1\}e^{\imath\varphi} \end{bmatrix}. \tag{3}$$

If $\phi = \varphi = \pi$, then this simplifies to [7]

$$M = \begin{bmatrix} \cos(2\theta) & -\sin(2\theta) \\ \sin(2\theta) & \cos(2\theta) \end{bmatrix}. \tag{4}$$

That is, if we pick $\phi = \varphi = \pi$, then each application of $\mathbf{Q}$ implements a rotation by angle 2θ. A natural question then is, what happens if at least one of the two angles ϕ and φ is not equal to π?

III. ARBITRARY ROTATIONS

Consider the matrix M defined by Eq. (3). Our primary objective is to ensure that the diagonal elements of M are equal.

Theorem 1 (Optimal angles)—*Suppose $\phi \neq \pi$. Then the two diagonal elements of M are equal, if and only if,*

$$\tan(\varphi/2) = \tan(\phi/2)(1-2a), \tag{5}$$

where matrix M is defined by Eq. (3).

Equation (5) expresses the phase condition we want to impose on ϕ and φ. It can be proven straightforwardly using standard identities of the trigonometric functions as follows. The two diagonal elements of M are equal, if and only if,

$$-\{(1-e^{\imath\phi})a + e^{\imath\phi}\} = \{(1-e^{\imath\phi})a - 1\}e^{\imath\varphi},$$

if and only if,

$$(e^{\imath\phi} - 1)a(e^{\imath\varphi} + 1) = e^{\imath\phi} - e^{\imath\varphi}.$$

Dividing by $2\imath e^{\imath(\phi+\varphi)/2}$ on both sides, this is equivalent to requiring that

$$2a\sin\left(\frac{\phi}{2}\right)\cos\left(\frac{\varphi}{2}\right) = \sin\left(\frac{\phi-\varphi}{2}\right). \tag{6}$$

By applying the identity $\sin(x-y) = \sin(x)\cos(y) - \sin(y)\cos(x)$, Eq. (6) can be rewritten as

$$\sin\left(\frac{\varphi}{2}\right)\cos\left(\frac{\phi}{2}\right) = \sin\left(\frac{\phi}{2}\right)\cos\left(\frac{\varphi}{2}\right)(1-2a),$$

which holds, if and only if,

$$\tan\left(\frac{\varphi}{2}\right) = \tan\left(\frac{\phi}{2}\right)(1-2a).$$

Theorem 1 follows.

We now show how to implement arbitrary rotations (up to certain phase factors) by appropriate choices of ϕ and φ. Let $0 \leqslant \vartheta < 2\pi$ be any angle for which $|\sin(\vartheta)| \leqslant \sin(2\theta)$. First we pick angle ϕ so that the absolute value of the lower left entry of M equals $|\sin(\vartheta)|$. Then we pick angle φ so that Eq. (5) holds. This ensures that the two diagonal elements of M are equal. With these choices of ϕ and φ, matrix M can thus be written in the form

$$H = e^{\imath v}\begin{bmatrix} 1 & \\ & e^{\imath u} \end{bmatrix}\begin{bmatrix} \cos(\vartheta) & -\sin(\vartheta) \\ \sin(\vartheta) & \cos(\vartheta) \end{bmatrix}\begin{bmatrix} 1 & \\ & e^{-\imath u} \end{bmatrix} \tag{7}$$

for some angles $0 \leqslant u, v < 2\pi$. We denote this matrix by H. Here and elsewhere, missing matrix entries are assumed equal to 0.

To summarize, we have just shown that for all a $(0 < a < 1)$ and for all angles ϑ $(0 \leqslant \vartheta < 2\pi)$ so that $|\sin(\vartheta)| \leqslant \sin(2\theta)$, there exist angles $0 \leqslant \phi, \varphi < 2\pi$ so that $M = H$ for some angles $0 \leqslant u, v < 2\pi$, where M is given by Eq. (3) and H by Eq. (7). Matrix H represents a rotation by angle ϑ, which is conjugated by a conditional phase change by angle u, up to a global phase factor of $e^{\imath v}$.

For many applications, applying H will be equally good to applying a rotation by angle ϑ. For instance, we can use H to implement arbitrary rotations as follows. Suppose a is known. Let w be any angle $(0 \leqslant w < 2\pi)$. We implement a rotation by angle w as follows. First, we check if w is a multiple of 2θ. If so, we simply just apply $\mathbf{Q}(\mathcal{A}, \chi, \pi, \pi)$ a total number of $w/(2\theta)$ times and stop [7]. Otherwise, we compute the smallest integer m larger than $w/(2\theta)$ and we set $\vartheta = w/m$. Then we find angles ϕ and φ so that $M = H$, and we compute the angles u and v. With these choices of angles, we can factorize the rotation by angle w as

$$\begin{bmatrix} \cos(w) & -\sin(w) \\ \sin(w) & \cos(w) \end{bmatrix} = e^{-\imath m v}\begin{bmatrix} 1 & \\ & e^{-\imath u} \end{bmatrix} M^m \begin{bmatrix} 1 & \\ & e^{\imath u} \end{bmatrix}. \tag{8}$$

Thus, to implement a rotation by angle w, we first apply a conditional phase change of the bad states by angle u. Then we apply $\mathbf{Q}(\mathcal{A}, \chi, \phi, \varphi)$ a total number of m times, apply a conditional phase change of the bad states by angle $-u$, and finally apply a global phase change by angle $-mv$.

IV. OBTAINING SUCCESS PROBABILITY 1

We now show that if we pick nontrivial angles ϕ and φ so that Eq. (5) holds, then we can find a good solution with

certainty. That is, we can use any set of angles $(\phi,\varphi) \neq (0,0)$ for which Eq. (5) holds.

Let angle $0 \leq \vartheta \leq \pi/2$ be defined so that $\sin(\vartheta) = |\sin(\phi/2)\sin(2\theta)|$. Since ϕ and φ satisfy Eq. (5), we can write $\mathbf{Q}(\mathcal{A},\chi,\phi,\varphi)$ in the form

$$e^{\iota v}\begin{bmatrix} 1 & \\ & e^{\iota u} \end{bmatrix}\begin{bmatrix} \cos(\vartheta) & -\sin(\vartheta) \\ \sin(\theta) & \cos(\vartheta) \end{bmatrix}\begin{bmatrix} 1 & \\ & e^{-\iota u} \end{bmatrix} \tag{9}$$

for some angles $0 \leq u,v < 2\pi$. That is, operator $\mathbf{Q}(\mathcal{A},\chi,\phi,\varphi)$ implements a rotation by angle ϑ, up to phase factors.

Our idea for finding a good solution with certainty is as follows: Let $m = (\pi/2 - \theta)/\vartheta$ and $\theta_{\text{init}} = \pi/2 - m\vartheta$. Then $-\theta < \theta_{\text{init}} \leq \theta$. We first set up a superposition representing the initial angle θ_{init}. This is possible since $|\theta_{\text{init}}| \leq \theta$. Then we apply operator $\mathbf{Q}(\mathcal{A},\chi,\phi,\varphi)$ a total number of m times and finally we measure. This produces a good solution with certainty. Let $|\Psi_{\text{init}}\rangle$ denote the state $\sin(\theta_{\text{init}})/\sqrt{a}|\Psi_1\rangle + \cos(\theta_{\text{init}})/\sqrt{1-a}|\Psi_0\rangle$. A realization of this idea is as follows:

(1) Apply $\mathcal{A}$ on the first register of the initial state $|0\rangle|0\rangle|0\rangle$, producing the state $|\Psi\rangle|0\rangle|0\rangle$.

(2) Apply function χ on the first and second registers. That is, apply the mapping $|x\rangle|z\rangle \rightarrow |x\rangle|z \oplus \chi(x)\rangle$ for $z \in \{0,1\}$, producing the state $|\Psi_1\rangle|1\rangle|0\rangle + |\Psi_0\rangle|0\rangle|0\rangle$. (Recall that $|\Psi\rangle = |\Psi_1\rangle + |\Psi_0\rangle$.)

(3) Let $\gamma = [\cos(\theta)/\sin(\theta)][\sin(\theta_{\text{init}})/\cos(\theta_{\text{init}})]$. Note that $|\gamma| \leq 1$ since $|\theta_{\text{init}}| \leq \theta \leq \pi/2$. Rotate the third register conditionally to the second register holding a 1, producing the state $|\Psi_1\rangle|1\rangle(\gamma|0\rangle + \sqrt{1-\gamma^2}|1\rangle) + |\Psi_0\rangle|0\rangle|0\rangle$, which we can rewrite as $(\gamma|\Psi_1\rangle|1\rangle + |\Psi_0\rangle|0\rangle)|0\rangle + \beta|\Psi_1\rangle|1\rangle|1\rangle$, where $\beta = \sqrt{1-\gamma^2}$.

(4) Apply function χ on the first and second registers, producing the state $(\gamma|\Psi_1\rangle + |\Psi_0\rangle)|0\rangle|0\rangle + \beta|\Psi_1\rangle|0\rangle|1\rangle$, which is equal to $\alpha|\Psi_{\text{init}}\rangle|0\rangle|0\rangle + \beta|\Psi_1\rangle|0\rangle|1\rangle$, where $\alpha = \cos(\theta)/\cos(\theta_{\text{init}})$.

(5) Now swap the contents of the first and second registers conditionally to that the third register contains a 1, producing the state $\alpha|\Psi_{\text{init}}\rangle|0\rangle|0\rangle + \beta|0\rangle|\Psi_1\rangle|1\rangle$.

(6) We are now ready to rotate the first register by angle $m\vartheta$. First apply the operator $\mathbf{S}_\chi(u)$ on the first register, producing the state $\alpha\{e^{\iota u}\sin(\theta_{\text{init}})/\sqrt{a}|\Psi_1\rangle + \cos(\theta_{\text{init}})/\sqrt{1-a}|\Psi_0\rangle\}|0\rangle|0\rangle + \beta|0\rangle|\Psi_1\rangle|1\rangle$.

(7) Apply operator $\mathbf{Q}(\mathcal{A},\chi,\phi,\varphi)$ a total number of m times on the first register, producing the state $\alpha\{e^{\iota(u+vm)}/\sqrt{a}|\Psi_1\rangle\}|0\rangle|0\rangle + \beta|E'\rangle|\Psi_1\rangle|1\rangle$, for some state $|E'\rangle$.

(8) Finally, swap the contents of the first two registers conditionally to that the third register contains a 1, producing the final tensor product state $|\Psi_1\rangle|E'\rangle_{2,3}$, for some state $|E'\rangle_{2,3}$ that represents the joint state of registers 2 and 3.

We may summarize this section by saying that for fixed known rotational angle ϑ, we can modify the angle of the initial state so that we succeed with certainty.

V. THE PHASE CONDITION

Our condition that $\tan(\varphi/2) = \tan(\phi/2)(1-2a)$ implies unfortunately that ϕ and φ depend nontrivially on a. Put formally, for all angles $0 < \phi < 2\pi$ so that $\phi \neq \pi$, the following holds: For all angles $0 \leq \varphi < 2\pi$ with $\varphi \neq \pi$, there exists a unique $a \in \Re$ so that Eq. (5) holds, and for all $0 \leq a \leq 1$, there exists a unique angle $0 \leq \varphi < 2\pi$ so that Eq. (5) holds. If the success probability a is known in advance, then for any angle ϕ we may want to pick, we can easily compute the angle φ to use. However, if a is not known, then this is not possible unless $\phi \in \{0,\pi\}$. Thus for angles $\phi \notin \{0,\pi\}$, we need to know a to compute φ so that Eq. (5) holds.

If we do not know a in advance, then a subsidiary strategy could be to utilize a set of angles (ϕ,φ) so that Eq. (5) almost holds. If a is small then we could, for example, approximate φ by ϕ. In the papers [2–5], Long *et al.* consider the question of when arbitrary phases can be utilized successfully in quantum searching. Their conclusion is that the angles have to equal $(\phi = \varphi)$ ''to construct an efficient quantum search algorithm'' [8]. Our condition that $\tan(\varphi/2) = \tan(\phi/2)(1-2a)$ is obviously different from their condition (that $\phi = \varphi$) whenever $0 < a < 1$ and $\phi \notin \{0,\pi\}$. The explanation for these different results is that Long *et al.* consider when the quantum search algorithm succeeds with high probability, whereas we, in the previous section, consider when the quantum search algorithm succeeds with certainty. In particular, all our calculations are exact. A main proof technical idea used by Long *et al.* for example in Ref. [3] is approximations of the type $K_1 \approx e^{K_2}$ for 2×2 matrices K_1 and K_2.

Long *et al.* [3,4] prove their result via an $\mathbf{SO}(3)$ rotational interpretation of operator $\mathbf{Q}(\mathcal{A},\chi,\phi,\varphi)$. We now reprove the theorem of Long *et al.* that if we use phases $\phi = \varphi$, then we can find a good solution with high probability. The main idea in our alternative proof is to consider the case $\phi = \varphi$, an approximation to the perfect case in which Eq. (5) holds, and then lower bound how well this approximation works. We do that by upper bounding the norm of the difference of two operators. This idea provides a short and straightforward proof.

Lemma 1 (equal angles)—*Let* $0 < \phi < \pi$. *Let angle* $0 < \vartheta \leq \pi/2$ *be so that* $\sin(\vartheta) = \sin(\phi/2)\sin(2\theta)$. *Let* $m = \lceil \pi/(2\vartheta) - \frac{1}{2} \rceil$ *and let* $\mathbf{Q}' = \mathbf{Q}(\mathcal{A},\chi,\phi,\phi)$. *Then*

$$|\langle \Psi_1'|\mathbf{Q}'^m \mathcal{A}|0\rangle| \geq 1 - a(2 + 4\pi^2 m), \tag{10}$$

where $|\Psi_1'\rangle = 1/\sqrt{a}|\Psi_1\rangle$.

Let angle $-\pi < \varphi < \pi$ be so that $\tan(\varphi/2) = \tan(\phi/2)(1-2a)$. Then $|\phi - \varphi| \leq 2\pi a$. Let $\mathbf{Q} = \mathbf{Q}(\mathcal{A},\chi,\phi,\varphi)$ and let $\mathcal{H}$ denote the Hilbert space that $\mathbf{Q}$ and $\mathbf{Q}'$ act upon. Let $\|\cdot\|$ denote the operator norm on $\mathcal{H}$ defined by $\|O\| = \sup\{|O|\Gamma\rangle| : ||\Gamma\rangle| = 1\}$ for any operator O on $\mathcal{H}$. Then

$$\|\mathbf{Q}' - \mathbf{Q}\| = \left\| \begin{bmatrix} 1 & \\ & e^{\iota\phi} \end{bmatrix} - \begin{bmatrix} 1 & \\ & e^{\iota\varphi} \end{bmatrix} \right\| = |1 - e^{\iota(\phi-\varphi)}| \leq 4\pi^2 a, \tag{11}$$

and thus $\|\mathbf{Q}'^m - \mathbf{Q}^m\| \leq 4\pi^2 a m$.

By definition of m we have that $|m\vartheta-\pi/2|\leq\vartheta/2\leq\theta$, so $\sin(m\vartheta)\geq\sqrt{1-a}$ and hence $|\langle\Psi_1'|\mathbf{Q}'^m|\Psi\rangle|\geq 1-2a$. Thus,

$$|\langle\Psi_1'|\mathbf{Q}'^m|\Psi\rangle|\geq|\langle\Psi_1'|\mathbf{Q}^m|\Psi\rangle|-4\pi^2am \geq 1-a(2+4\pi^2m). \quad (12)$$

Lemma 1 follows.

If we measure the state $\mathbf{Q}'^m\mathcal{A}|0\rangle$, then the outcome is good with probability at least $1-4a(1+2\pi^2m)$, which is at least $1-4a(\pi^3/\vartheta+11)$. The probability of measuring a bad state is thus upper bounded by $4\pi^3a/\vartheta+44a$, which is $O(\sqrt{a}/\phi)$ for $0<a\leq 1$ and $0<\phi<\pi$. Theorem 2 follows.

Theorem 2 (equal angles)—*Let $\mathcal{A}$ be any quantum algorithm that uses no measurements. Let a denote the success probability of $\mathcal{A}$ and let angle $0<\theta\leq\pi/2$ be so that $\sin^2(\theta)=a$. Let ϕ be any angle so that $\theta\leq\phi<\pi$. Let $m=\lceil\pi/(2)\vartheta-\frac{1}{2}\rceil$, where angle $0<\vartheta\leq\pi/2$ is so that $\sin(\vartheta)=\sin(\phi/2)\sin(2\theta)$. Let $\mathbf{Q}'=\mathbf{Q}(\mathcal{A},\chi,\phi,\phi)$. Then a measurement of $\mathbf{Q}'^m\mathcal{A}|0\rangle$ will provide a good solution with probability $1-O(\sqrt{a}/\phi)$.*

Theorem 2 relies on two properties: First, that operator $\mathbf{Q}(\mathcal{A},\chi,\phi,\phi)$ approximates operator $\mathbf{Q}=\mathbf{Q}(\mathcal{A},\chi,\phi,\varphi)$ sufficiently well. Secondly, that each application of $\mathbf{Q}$ implements a rotation by a sufficiently large angle ϑ. Any set of angles (ϕ,φ) so that these two properties are fulfilled will provide a quantum amplitude amplification scheme. In general, the closer we pick the rotational angle ϑ to the maximal angle 2θ, the worse the approximation for $\mathbf{Q}$ we can allow ourselves to use, and vice versa. In the next theorem, which is proven almost identically to Theorem 2, we express one way of capturing this duality.

Theorem 3 (any angles)—*Let $\mathcal{A}$ be any quantum algorithm that uses no measurements. Let a denote the success probability of $\mathcal{A}$ and let angle $0<\theta\leq\pi/2$ be so that $\sin^2(\theta)=a$. Let $0<\phi<\pi$ and $-\pi<\varphi'<\pi$ be given angles. Let $m=\lceil\pi/(2\vartheta)-\frac{1}{2}\rceil$, where angle $0<\vartheta\leq\pi/2$ is so that $\sin(\vartheta)=\sin(\phi/2)\sin(2\theta)$. Let $-\pi<\varphi<\pi$ be defined so that $\tan(\varphi/2)=\tan(\phi/2)(1-2a)$ and let $\delta=|\varphi'-\varphi|$. Let $\mathbf{Q}'=\mathbf{Q}(\mathcal{A},\chi,\phi,\varphi')$ denote our approximation to $\mathbf{Q}(\mathcal{A},\chi,\phi,\varphi)$. Then a measurement of $\mathbf{Q}'^m\mathcal{A}|0\rangle$ will provide a good solution with error probability at most $4a+\epsilon$, provided $\delta\leq\epsilon\phi\sqrt{a}\sqrt{3}/[2\pi^2(\sqrt{3}+\pi)]$.*

The above theorem put bounds on the error $\delta=|\varphi'-\varphi|$ that we can tolerate to still obtaining a quantum algorithm that succeeds with high probability. Suppose ϕ is a constant, say $\phi=\pi/10$, then whenever δ is at most $c\sqrt{a}$, for some appropriate constant c, the above algorithm finds a good solution with bounded error probability. Furthermore, if δ is at most $O(a)$, as it is if we pick $\varphi'=\phi$, then the error probability drops to being in $O(\sqrt{a})$. Thus, the smaller the error in the choice of angles from the perfect case as expressed by Eq. (5), the smaller is the error probability of the algorithm.

Theorem 3 is similar to the main result in Ref. [5] where it is proven that for quantum searching, the distance $|\phi-\varphi|$ must be at most of order $1/\sqrt{N}$ for finding the marked element with constant success probability. Our result generalizes their result as it measures the error probability of the overall algorithm in terms of the distance from the perfect case in which Eq. (5) holds. The case $\phi=\varphi$ is already an approximation, which by itself introduces an error in δ in the order of $\Theta(a)$. In addition, Theorem 3 includes the cases that the angles ϕ and φ are not constants but depend on a. However, the main benefit of Theorem 3 is that it is easy to prove once one is given Theorem 1. Essentially, the proof of Theorem 3 reduces to bounding the distance between the two operators $\mathbf{Q}(\mathcal{A},\chi,\phi,\varphi)$ and $\mathbf{Q}(\mathcal{A},\chi,\phi,\varphi')$.

VI. CONCLUSION

Amplitude amplification is besides quantum Fourier transforms the most successfully used tool in quantum algorithms. It is a generalization of Grover's quantum searching algorithm and it allows a quadratic speed up of many algorithms.

We prove that the phase condition in amplitude amplification can be expressed by the equation $\tan(\varphi/2)=\tan(\phi/2)(1-2a)$, where a denotes the success probability of the original algorithm. We show how to implement arbitrary rotations and how to boost quantum algorithms to succeed with certainty by utilizing angles (ϕ,φ) that satisfy the above equation. In both cases, the number of iterations required increases linearly in the inverse of angle ϕ. For instance, if we choose $\phi=\pi/c$ for some constant $c>1$, then we require $\Theta(c/\sqrt{a})$ iterations to find a solution with certainty.

Whenever the success probability a is not known *a priori*, we can approximate the above trigonometric equation by the linear equation $\phi=\varphi$. This case has been studied by Long *et al.* [2–5] and in particular, they have shown that equal angles can be utilized in quantum searching. By considering the case $\phi=\varphi$ an approximation to the perfect case $\tan(\varphi/2)=\tan(\phi/2)(1-2a)$, we can reprove the main results by Long *et al.*

ACKNOWLEDGMENTS

I am grateful to Gilles Brassard and Richard Cleve for comments.

[1] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[2] G. L. Long, W. L. Zhang, Y. S. Li, and L. Niu, Commun. Theor. Phys. **32**, 335 (1999).
[3] G. L. Long, Y. S. Li, W. L. Zhang, and L. Niu, Phys. Lett. A **262**, 27 (1999).
[4] G. L. Long, C. C. Tu, Y. S. Li, W. L. Zhang, and H. Y. Yan, *A Novel SO(3) Picture for Quantum Searching*, 1999, available at Los Alamos e-print archive as http://arXiv.org/abs/quant-ph/9911004.
[5] G. L. Long, Y. S. Li, W. L. Zhang, and C. C. Tu, Phys. Rev. A

61, 042305 (2000).
[6] G. Brassard, P. Høyer, M. Mosca, and A. Tapp, *Quantum Amplitude Amplification and Estimation*, available at Los Alamos e-print archive as http://arXiv.org/abs/quant-ph/0005055.
[7] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, Fortschr. Phys. **46**, 493 (1998).
[8] See, for example, the first paragraph on page 042305-2 in Ref. [5]. Please note that the notation used in Refs. [2–5] is slightly different from ours: their θ denotes our φ, and their φ denotes our ϕ.