Exactness of the original Grover search algorithm

Zijian Diao*
Mathematics Department, Ohio University Eastern Campus, St. Clairsville, Ohio 43950, USA

(Received 13 August 2010; published 15 October 2010)

It is well-known that when searching one out of four, the original Grover's search algorithm is exact; that is, it succeeds with certainty. It is natural to ask the inverse question: If we are not searching one out of four, is Grover's algorithm definitely not exact? In this article we give a complete answer to this question through some rationality results of trigonometric functions.

DOI: 10.1103/PhysRevA.82.044301 PACS number(s): 03.67.Hk

I. INTRODUCTION

Grover's algorithm [1] is one of the most significant quantum algorithms [2]. It provides a quadratic speedup for the unsorted database search problem by amplifying the probability amplitude of the search target. When it was first discovered, like most quantum algorithms, it was considered a probabilistic algorithm; that is, it may fail with certain (albeit small) probability. Currently, several schemes have been proposed to make this algorithm exact, either by fine-tuning the amplitude amplification operator [3–6] or by dynamical modification of the oracle function encoding the database [7]. The study of exact quantum algorithms bears importance in both practical applications and theoretical research of quantum information science.

It is straightforward to verify that, when searching one target out of a database of four entries, the original Grover's algorithm is exact; that is, it succeeds with certainty. Is this the only case of exactness, excluding the trivial search of a database full of search targets? We provide a rigorous analysis to confirm this conjecture in this article. Reference [5] derives an elegant phase condition for the amplitude amplification operator, which is sufficient to ensure search with certainty. Unfortunately, the phase shift π in the original Grover's algorithm is exactly what is ruled out in the assumption of this condition (cf. [5, Theorem 1]). So the discussion there cannot be readily applied. Furthermore, our emphasis here deals with the opposite direction to that used in [5]. We fix the phase shift (π) first, then analyze whether the search is exact under varying initial success probability.

In the following sections we limit our discussion mostly to the original Grover's algorithm, which searches for a single target. It can be generalized in a straightforward fashion to the multiple-target case [8,9] with the same essential ingredients. Similar arguments apply with minimal modification.

II. ORIGINAL GROVER'S ALGORITHM

In this section we briefly review the procedure of the original Grover's algorithm. The problem dealt by the original Grover's algorithm is as follows: Given an unsorted database containing N items, $N \geqslant 1$, how does one locate one particular target item? Mathematically, the database is represented by an oracle function $f(x)$, with $x \in \{1,2,\ldots,N\}$, defined by

$$f(x) = \begin{cases} 0 & \text{if} \quad x \neq w \\ 1 & \text{if} \quad x = w \end{cases}, \tag{1}$$

where w is the search target. Grover's algorithm utilizes the amplitude amplification operator $\mathcal{G} = \mathcal{I}_s\mathcal{I}$, defined by

$$\mathcal{I}|x\rangle = (-1)^{f(x)}|x\rangle, \tag{2}$$

or, equivalently,

$$\mathcal{I} = \mathbb{I} - 2|w\rangle\langle w|, \tag{3}$$

and

$$\mathcal{I}_s = 2|s\rangle\langle s| - \mathbb{I}, \tag{4}$$

where $|s\rangle = \frac{1}{\sqrt{N}}(\sum_{x=1}^{N}|x\rangle)$, the uniform superposition (the average) of all possible basis states, and $\mathbb{I}$ is the identity operator. $\mathcal{I}$ is the selective sign-flipping operator, which selectively flips the sign of the target state $|w\rangle$. $\mathcal{I}_s$ is the inversion around the average operator, which reflects a given state vector around $|s\rangle$.

The procedure of Grover's algorithm is as follows:

(1) prepare the initial state vector $|s\rangle$;

(2) apply $\mathcal{G}$ on $|s\rangle$ for an appropriate number of times (approximately $\frac{\pi}{4}\sqrt{N}$ times if N is very large);

(3) measure the final state, which yields the target state $|w\rangle$ with high probability.

The effect of the amplitude amplification operator, $\mathcal{G}$, and why this algorithm works, can be best explained by a geometric visualization (see Fig. 1) on the plane spanned by $|s\rangle$ and $|w\rangle$. When applied to a state vector $|v\rangle$, the selective sign-flipping operator $\mathcal{I}$ flips the sign of the component of $|v\rangle$ in the direction of $|w\rangle$, but leaves all other components unchanged. So the pure effect is a reflection of $|v\rangle$ about $|w^{\perp}\rangle$, the orthogonal vector to $|w\rangle$. When applied to a state vector $|v\rangle$, the inversion around the average operator $\mathcal{I}_s$ leaves the component in the direction of $|s\rangle$ unchanged, but flips the signs of all the other components. So the pure effect is a reflection of $|v\rangle$ about $|s\rangle$. If we start from $|s\rangle$, one application of $\mathcal{G} = \mathcal{I}_s\mathcal{I}$ reflects $|s\rangle$ first about $|w^{\perp}\rangle$ and then about $|s\rangle$, hence rotates $|s\rangle$ toward $|w\rangle$ by an angle of 2θ, where θ is the initial angle between $|s\rangle$ and $|w^{\perp}\rangle$ with $\sin\theta = \cos(\frac{\pi}{2} - \theta) = \langle s|w\rangle = \frac{1}{\sqrt{N}}$.

It can be explicitly computed [10, p. 252] that, after n iterations,

$$\mathcal{G}^n|s\rangle = \sin[(2n+1)\theta]|w\rangle + \cos[(2n+1)\theta]|w^{\perp}\rangle. \tag{5}$$

*diao@ohio.edu

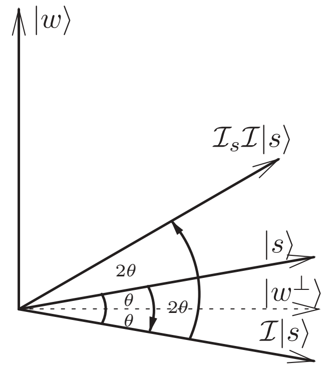

FIG. 1. Geometric visualization of Grover's algorithm.

So the success probability p_n is $\sin^2[(2n+1)\theta]$. When $n = \frac{\pi}{4\theta} - \frac{1}{2}$, $(2n+1)\theta = \frac{\pi}{2}$, and $p_n = 1$. A measurement after n steps yields $|w\rangle$ with certainty. However, $\frac{\pi}{4\theta} - \frac{1}{2}$ is not necessarily an integer, so the optimal strategy is choosing n to be either $\lceil \frac{\pi}{4\theta} - \frac{1}{2} \rceil$ or $\lfloor \frac{\pi}{4\theta} - \frac{1}{2} \rfloor$ such that $(2n+1)\theta$ is the closest to $\frac{\pi}{2}$ in order to maximize p_n. The consequence is that p_n is close, but not equal, to 1, which explains the probabilistic nature of the algorithm.

III. EXACTNESS OF THE ORIGINAL GROVER'S ALGORITHM

In this section we fully resolve the exactness of the original Grover's algorithm. Let us start from the special case of searching one out of four. Now $\sin\theta = \frac{1}{2}$, $\theta = \frac{\pi}{6}$. After one iteration, $p_1 = \sin(3\theta) = \sin\frac{\pi}{2} = 1$. We can find the target with certainty after one oracle query (cf. Fig. 2). It is obvious that in order for the algorithm to be exact, it is necessary for θ to be a rational multiple of π.

The analysis in the rest of this section is motivated by [11, Chapter 4] and follows the same line of presentation. Let us start from a basic result about the rational roots of polynomials, adapted from [12, Proposition 11, p. 308]. First we define a polynomial to be monic if its leading coefficient is 1.

Lemma 1. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a monic polynomial with integer coefficients. Then every rational root of $f(x)$ is an integer.

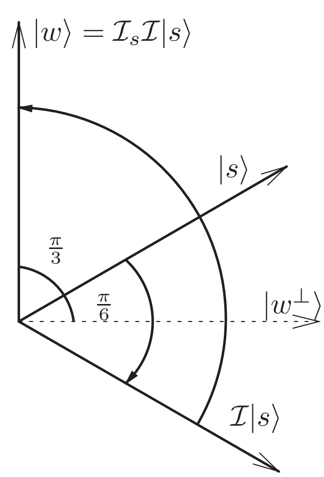

FIG. 2. Geometric visualization when searching one out of four.

Proof. Suppose $x = \frac{A}{B}$, with A and B being relative prime and $B > 0$, is a rational root of $f(x)$. Thus,

$$\frac{A^n}{B^n} + a_{n-1}\frac{A^{n-1}}{B^{n-1}} + \cdots + a_1\frac{A}{B} + a_0 = 0, \tag{6}$$

$$A^n + a_{n-1}A^{n-1}B + \cdots + a_1 A B^{n-1} + a_0 B^n = 0, \tag{7}$$

$$B(a_{n-1}A^{n-1} + \cdots + a_1 A B^{n-2} + a_0 B^{n-1}) = -A^n. \tag{8}$$

From (8), we have $B \mid A^n$, but A and B are relatively prime, so $B = 1$. Therefore, $x = A$ is an integer. ■

The following rationality result of trigonometric functions is adapted from [13]. We use $\mathbb{Q}$ to denote the set of rational numbers.

Lemma 2. There exists a sequence of monic polynomials f_n with integer coefficients such that $f_n(2\cos\phi) = 2\cos(n\phi)$, for all $n = 1, 2, \ldots$.

Proof. Let us construct this sequence of polynomials inductively by $f_0(x) = 2$, $f_1(x) = x$, and $f_n(x) = x f_{n-1}(x) - f_{n-2}(x)$. Clearly all f_n's except f_0 are monic and all their coefficients are integers. Also, f_0 and f_1 satisfy the cosine property. Assume that $f_n(2\cos\phi) = 2\cos(n\phi)$ for all indices up to n. It is easy to verify that $f_{n+1}(2\cos\phi) = 2\cos\phi\, f_n(2\cos\phi) - f_{n-1}(2\cos\phi) = 4\cos\phi\cos(n\phi) - 2\cos[(n-1)\phi] = 2\cos[(n+1)\phi]$, which completes the induction proof. ■

Theorem 1. The only rational values for $\cos(r\pi)$ with $r \in \mathbb{Q}$ are 0, $\pm\frac{1}{2}$, and ± 1.

Proof. If $r \in \mathbb{Q}$, there exists a non-negative integer n such that nr is an integer. Let f_n be the polynomial constructed in Lemma 2. $f_n[2\cos(r\pi)] = 2\cos(nr\pi) = \pm 2$, so $2\cos(r\pi)$ is a root of the polynomial $f_n(x) \pm 2$. Lemma 1 tells us that if $2\cos(r\pi)$ is a rational number, then $2\cos(r\pi)$ has to be an integer, that is, 0, ± 1, or ± 2. Hence, the only rational values of $\cos(r\pi)$ are 0, $\pm\frac{1}{2}$, and ± 1. ■

Now we are in the position to prove our main result.

Main Theorem 1. Excluding the trivial search of a database full of search targets, the original Grover's algorithm is exact if and only if searching one out of four.

Proof. In order to succeed with certainty after a number of iterations, the geometric interpretation of Grover's algorithm imposes the restriction that the angle θ must be a rational multiple of π, that is, of the form $r\pi$, where $r \in \mathbb{Q}$. On the other hand, $\sin^2\theta = \frac{1}{N}$ ($\frac{t}{N}$ in the multitarget case, where t is the number of targets) is a rational number, and so is $\cos(2\theta) = 1 - 2\sin^2\theta = 1 - \frac{2}{N}$ ($1 - \frac{2t}{N}$ in the multitarget case). However, the only possible rational values of $\cos(2\theta)$ are 0, $\pm\frac{1}{2}$, and ± 1, when $\theta = r\pi$, $r \in \mathbb{Q}$. Let us analyze these five values one by one.

(1) When $\cos(2\theta) = 1$, $\sin^2\theta = 0$. This is the trivial search for a nonexisting target.

(2) When $\cos(2\theta) = -1$, $\sin^2\theta = 1$. This is the trivial search of a database where all the entries are targets.

(3) When $\cos(2\theta) = 0$, $\sin^2\theta = \frac{1}{2}$, and $\theta = \frac{\pi}{4}$. The success probability after n iteration is $\sin^2[(2n+1)\theta] = \sin^2\frac{(2n+1)\pi}{4} = \frac{1}{2}$, which is never 1.

(4) When $\cos(2\theta) = -\frac{1}{2}$, $\sin^2\theta = \frac{3}{4}$, and $\theta = \frac{\pi}{3}$. The success probability after n iteration is $\sin^2(2n+1)\theta = \sin^2\frac{(2n+1)\pi}{3}$, which is never 1 (0 if $3 \mid 2n+1$ and $\frac{3}{4}$ if $3 \nmid 2n+1$).

(5) When $\cos(2\theta) = \frac{1}{2}$, $\sin^2\theta = \frac{1}{4}$, so $\theta = \frac{\pi}{6}$. This is the familiar case of searching one out of four. One iteration yields the search target with certainty.

Out of these, the exactness result in this theorem follows naturally. ■

As the final remark, if postmeasurement processing is allowed, there is one more special case where exactness can be achieved. When there are three search targets in a database with four entries, the success probability is 0 after one iteration (cf. Case 4 in the proof of Main Theorem 1 with $n = 1$). If we measure at this point, we are bound to discover the only nontarget in the database. To complete the search successfully, choosing any of the other three entries will do. However, this strategy cannot be extended to similar scaled-up three out of four cases. If there are more than one nontargets, we can determine and rule out only one of them after the measurement. Choosing any of the remaining entries does not necessarily yield a target anymore.

IV. DISCUSSION

We have rigorously shown that searching one out of four is the only nontrivial case where the original Grover's algorithm is exact. It would be interesting to generalize the same kind of reasoning to the generalized Grover's search with arbitrary phase shifts, in particular the phase shifts of the form $r\pi$ with $r \in \mathbb{Q}$, since they are easier to implement in practice. We conjecture that a thorough analysis based on rationality observations will provide us with similar results.

ACKNOWLEDGMENTS

This work is supported by the Ohio University Research Committee Award and Faculty Research Activity Fund. The author also thanks Peter Høyer and Barry Sanders for helpful comments and the Institute for Quantum Information Science at University of Calgary, where part of the draft was prepared.

[1] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[2] A. Ambainis, e-print arXiv:quant-ph/0609168v1.
[3] G. Brassard, P. Høyer, and A. Tapp, in *Proceedings of the 25th International Colloquium on Automata, Languages and Programming* (Springer, New York, 1998), Vol. 1443 of *Lecture Notes in Computer Science*, p. 820.
[4] D.-P. Chi and J. Kim, in *Lecture at First NASA International Conference on Quantum Computing and Quantum Communications* (Springer, Berlin, 1998).
[5] P. Høyer, Phys. Rev. A **62**, 052304 (2000).
[6] G.-L. Long, Phys. Rev. A **64**, 022307 (2001).
[7] G. Chen and Z. Diao, e-print arXiv:quant-ph/0011109v3.
[8] G. Chen, S. Fulling, and J. Chen, in *Mathematics of Quantum Computation*, edited by R. Brylinski and G. Chen (CRC Press, Boca Raton, FL, 2002), Chap. 6, p. 135.
[9] G. Chen and S. Sun, in *Mathematics of Quantum Computation*, edited by R. Brylinski and G. Chen (CRC Press, Boca Raton, FL, 2002), Chap. 7, p. 161.
[10] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).
[11] J. Rotman, *Journey into Mathematics: An Introduction to Proofs* (Prentice Hall, Upper Saddle River, NJ, 1998).
[12] D. Dummit and R. Foote, *Abstract Algebra*, 3rd ed. (Wiley, New York, 2004).
[13] I. Niven and H. S. Zuckerman, *An Introduction to the Theory of Numbers* (Wiley, New York, 1972).