Fixed-Point Quantum Search

Lov K. Grover*

Bell Laboratories, Lucent Technologies, 600-700 Mountain Avenue, Murray Hill, New Jersey 07974, USA

(Received 11 April 2005; published 3 October 2005)

The quantum search algorithm consists of an iterative sequence of selective inversions and diffusion type operations, as a result of which it is able to find a state with desired properties (target state) in an unsorted database of size N in only $\sqrt{N}$ queries. This is achieved by designing the iterative transformations in a way that each iteration results in a small rotation of the state vector in a two-dimensional Hilbert space that includes the target state; if we choose the right number of iterative steps, we will stop just at the target state. This Letter shows that by replacing the selective inversions by selective phase shifts of $\frac{\pi}{3}$, the algorithm preferentially converges to the target state irrespective of the step size or number of iterations. This feature leads to robust search algorithms and also to new schemes for quantum control and error correction.

DOI: 10.1103/PhysRevLett.95.150501 PACS numbers: 03.67.Lx

I. Introduction.—"Quantum searching is like cooking a souffle. You put the state obtained by quantum parallelism in a 'quantum oven' and let the desired answer rise slowly. Success is almost guaranteed if you open the oven at just the right time. But the souffle is very likely to fall—the amplitude of the correct answer drops to zero—if you open the oven too early. Furthermore, the souffle could burn if you overcook it; strangely, the amplitude of the desired state starts shrinking after reaching its maximum." [1]

Search algorithms can be described as a rotation of the state vector in two-dimensional Hilbert space defined by the initial (s) and the target (t) vectors. As we describe later, any iterative quantum procedure *has* to be an iterative rotation in state space where each iteration causes the same amount of rotation. In the original quantum search algorithm, the state vector uniformly goes from the initial to the target, and unless we stop when it is right at the target, it will drift away. For many applications, including an unsorted database search, this leads to a square-root speedup over the corresponding classical algorithm. One limitation of these algorithms is that, to perform optimally, they need precise knowledge of certain problem parameters, e.g., the number of target states.

This Letter shows that by replacing the selective phase inversions in quantum search by suitable phase shifts we can get an algorithm that always gives an improvement. As shown in Fig. 1, when a single iteration derived from any unitary operator U is applied, the state vector *always* moves closer to the target state (Sec. III). By recurring this basic iteration, we develop an algorithm with multiple applications of U that converges monotonically to the target (Sec. IV). This leads to variants of quantum searching that are robust to changes in the parameters (Secs. VI and VII). Also, this immediately leads to schemes for reducing certain kinds of errors in quantum computing (Sec. VIII).

II. A different kind of quantum search.—Consider the transformation $UR_sU^\dagger R_tU$ applied to $|s\rangle$:

$$UR_sU^\dagger R_tU|s\rangle, \tag{1}$$

$$R_s = I - \left[1 - \exp\left(i\frac{\pi}{3}\right)\right]|s\rangle\langle s|,$$

$$R_t = I - \left[1 - \exp\left(i\frac{\pi}{3}\right)\right]|t\rangle\langle t|.$$

R_t and R_s denote selective phase shifts of the respective state(s) by $\frac{\pi}{3}$. Note that if we were to change these phase shifts from $\frac{\pi}{3}$ to π, we would get one iteration of the amplitude amplification algorithm [2,3].

The next section shows that if U drives the state vector from a source (s) to a target (t) state with a probability of $(1 - \epsilon)$, i.e., $\|U_{ts}\|^2 = (1 - \epsilon)$, then the transformation (1) drives the state vector from the source to the same target state with a probability of $(1 - \epsilon^3)$. The deviation from the t state has hence fallen from ϵ to ϵ^3.

The striking aspect of this result is that it holds for *any* kind of deviation from the t state. Unlike the standard amplitude amplification algorithm which would greatly overshoot the target state when ϵ is small (Fig. 1), the new algorithm will always move towards the target. As shown in Sec. VI, this can be used to develop algorithms that are more robust to variations in the problem parameters.

Connections to control and error correction might already be evident. Let us say that we are trying to drive a system from an s state/subspace to a t state/subspace. The

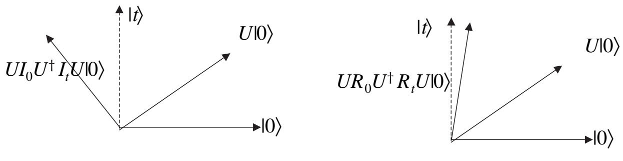

FIG. 1. In amplitude amplification (left), the state vector overshoots the target state; in the algorithm of this Letter (right), the state vector always moves towards the target.

transformation that we have available for this is U, which drives it from s to t with a probability $\|U_{ts}\|^2$ of $(1-\epsilon)$; i.e., the probability of error in this transformation is ϵ. Then the composite transformation $UR_sU^\dagger R_tU$ will reduce the error to ϵ^3.

This technique is applicable whenever the transformations U, $U^\dagger$, R_s, and R_t can be implemented. This will be the case when errors are systematic errors or slowly varying errors, e.g., due to environmental degradation of some component. This would not apply to errors that come about as a result of sudden disturbances from the environment. It is further assumed that the transformation U can be inverted with exactly the same error (illustrated in Sec. VII). Traditionally, quantum error correction is carried out at the single qubit level where individual errors are corrected, each error being corrected in a separate way. With the machinery of this Letter, errors can be corrected without ever needing to identify the error syndrome.

III. Analysis.—We analyze the effect of the transformation $UR_sU^\dagger R_tU$ when it is applied to the $|s\rangle$ state. As mentioned in the previous section, R_t and R_s denote selective phase shifts of the respective state(s) by $\frac{\pi}{3}$ (t for target, s for source). We show that if $\|U_{ts}\|^2 = (1-\epsilon)$, then

$$\|\langle t|UR_sU^\dagger R_tU|s\rangle\|^2 = (1-\epsilon^3). \tag{2}$$

In the rest of this section, the greek alphabet θ will be used to denote $\frac{\pi}{3}$. Start with $|s\rangle$ and apply the operations U, R_s, $U^\dagger$, R_t, and U. Analyzing the effect of the operations, one by one, just as in the original quantum search algorithm [4], it leads to the following superposition:

$$U|s\rangle[e^{i\theta} + \|U_{ts}\|^2(e^{i\theta}-1)^2] + |t\rangle U_{ts}(e^{i\theta}-1).$$

To calculate the deviation of this superposition from $|t\rangle$, consider the amplitude of the above superposition in non-target states. The probability is given by the absolute square of the corresponding amplitude:

$$(1-\|U_{ts}\|^2)\|[e^{i\theta} + \|U_{ts}\|^2(e^{i\theta}-1)^2]\|^2.$$

Substituting $\|U_{ts}\|^2 = (1-\epsilon)$, the above quantity becomes ϵ^3.

IV. Recursion.—A few years after the invention of the quantum search algorithm [4], it was generalized to a much larger class of applications known as the amplitude amplification algorithms [2,3]. In these algorithms, the amplitude produced in a particular state t by starting from a state s and applying a unitary operation U can be *amplified* by successively repeating the sequence of operations: $Q = I_sU^\dagger I_tU$. Here I_s and I_t denote selective inversions of the s and t states, respectively. For later reference, note that the amplitude amplification transformation with four I_t's is

$$U(I_sU^\dagger I_tU)(I_sU^\dagger I_tU)(I_sU^\dagger I_tU)(I_sU^\dagger I_tU). \tag{3}$$

Unlike the amplitude amplification transformation, it is not possible to iterate the transformation (1) $UR_sU^\dagger R_tU$ to obtain larger rotations of the state vector. Instead longer sequences have to be formed by recursion as follows. Define the transformation U_{m+1} by the recursion:

$$U_{m+1} = U_mR_sU_m^\dagger R_tU_m, \qquad U_0 = U. \tag{4}$$

Unlike amplitude amplification, it is *not* simple to write down the precise operation sequence for U_m with large m without working out the full recursion. Recursion for each m is different and there is no simple structure. Let us illustrate this for U_2:

$$\begin{aligned} U_0 = U, \qquad U_1 &= U_0R_sU_0^\dagger R_tU_0 = UR_sU^\dagger R_tU \\ U_2 &= U_1R_sU_1^\dagger R_tU_1 \\ &= (UR_sU^\dagger R_tU)R_s(UR_sU^\dagger R_tU)^\dagger R_t(UR_sU^\dagger R_tU) \\ &= U(R_sU^\dagger R_tU)(R_sU^\dagger R_t^\dagger U)(R_s^\dagger U^\dagger R_tU)(R_sU^\dagger R_tU). \end{aligned} \tag{5}$$

The corresponding transformation for amplitude amplification is (3).

It is straightforward to show that if $\|U_{ts}\|^2 = 1-\epsilon$, then $\|U_{m,ts}\|^2 = 1-\epsilon^{3^m}$. Expressed as a function of the number of queries (q_m) $\|U_{m,ts}\|^2 = 1-\epsilon^{2q_m+1}$. The failure probability hence falls as ϵ^{2q_m+1} after q_m queries [5]; this is similar to a classical algorithm where the probability of failure falls as ϵ^{q+1} after q queries (a classical algorithm is discussed in Sec. VI).

V. Fixed point of algorithm.—First, note that the standard amplitude amplification algorithm (3) and the phase-shift algorithm (5), both have some selective operations performed on the t state, and so from an information theoretic point of view there is no violation in having fixed points. However, unitarity would be violated if there was any kind of accumulation at the target state due to repetition of the same transformation. This is because any unitary transformation has all eigenvalues of modulus unity and so any iteration is inherently periodic.

In amplitude amplification (3), exactly the same transformation is repeated and so unitarity does not permit any fixed point. In the phase-shift algorithm (5), which is similar to amplitude amplification, the transformation repeated in each step is slightly different due to the presence of each of the four operations R_s, R_t, $R_s^\dagger$, $R_t^\dagger$ and it hence gets around the condition regarding repetition of identical unitary operators that prevents amplitude amplification from having a fixed point.

Very recently a novel algorithm for obtaining fixed points in iterative quantum transformations by periodic measurements has been discovered [6].

VI. Quantum searching amidst uncertainty.—The original quantum search algorithm [4] considered the problem of finding a marked item in a large unsorted database with minimum queries to the database. For this type of problem, it is usually acceptable to reach a point in state space somewhere in the neighborhood of the solution and spend a few queries to fine-tune the answer. However, there are other important problems where the additional queries create a significant overhead and need to be minimized, e.g., when we are limited to a single query and have to find the answer with a probability approaching unity. One field in which this type of problem occurs is in pattern recognition and image analysis where each query requires a lot of signal processing and the consequences of making an error are catastrophic.

VII. The problem.—Consider the situation where a large fraction of the items in a database are marked, but the precise fraction of marked items is not known. The goal is to find a single marked item with as high a probability as possible in a single query to the database. For concreteness, say some unknown fraction $(1 - \epsilon)$ of the items is marked, with ϵ uniformly distributed in the range $(0, \epsilon_0)$ with equal probability. The search algorithm returns an item; if it is a marked item the algorithm succeeds, else if it is unmarked, the algorithm fails. In this Letter we show that the probability of failure for the new scheme is $O(\epsilon_0^3)$, whereas that of the best (possible) classical scheme and that of the best known quantum schemes are both $O(\epsilon_0^2)$.

A. Classical algorithm. The best classical algorithm is to select a random state and see if it is a t state (one query). If yes, return this state; if no, pick another random state and return that without any query. The probability of failure is equal to that of not getting a single t state in two random picks, i.e., ϵ^2. Since ϵ is uniformly distributed in the range $(0, \epsilon_0)$, the overall failure probability is $\frac{\int_0^{\epsilon_0} \epsilon^2 d\epsilon}{\int_0^{\epsilon_0} d\epsilon} = \frac{1}{3}\epsilon_0^2$.

B. Quantum searching. Boyer *et al.* [7] first described in detail an algorithm that succeeds with probability approaching 1, regardless of the number of solutions (it is a classical algorithm that uses quantum searching as a subroutine; of course, it can be made fully quantum). The first quantum algorithm to be able to search an unstructured database in a single query with a success probability approaching 1 was given by Mosca [8].

Mosca observed that the quantum counting algorithm of [7] (based on the original searching algorithm) produces a solution with probability converging to 1/2. One easily converts this to an algorithm with probability of success converging to 1/4. Thus by using this algorithm as a subroutine in another quantum search, we get success probability converging to 1. (This appears to be based on the observation in [7] that an algorithm that succeeds with probability exactly 1/4 can be amplified to one with success probability exactly 1 using only one quantum search iterate.) In other words, the technique Mosca uses is to take a search algorithm that succeeds with probability $1/4 - X$ and then use one quantum search iteration to map it to an algorithm that succeeds with probability $(1 - 12X^2 - 16X^3)$. Using this scheme, if the fraction of marked states of the database is $1 - \epsilon$, one can easily obtain a marked state with a probability of error of $1 - \frac{3}{4}\epsilon^2 - \frac{1}{4}\epsilon^3$ by means of a single quantum query. The overall failure probability in this case becomes $\frac{\int_0^{\epsilon_0}[(3/4)\epsilon^2+(1/4)\epsilon^3]d\epsilon}{\int_0^{\epsilon_0} d\epsilon} = \frac{1}{4}\epsilon_0^2 + \frac{1}{16}\epsilon_0^3$.

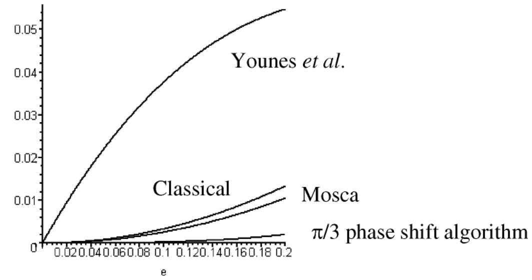

FIG. 2. Comparison of the failure probability of the $\pi/3$ phase-shift algorithm with a classical algorithm [8,9] when the fraction of unmarked states (ϵ_0) varies between 0 and 0.2.

A recent quantum search based algorithm for this problem is by Younes *et al.* [9]. This finds a solution with a probability of $(1 - \cos\theta)(\frac{\sin^2(q+1)\theta}{\sin^2\theta} + \frac{\sin^2 q\theta}{\sin^2\theta})$, where $q =$ number of queries and $\theta = \arccos\epsilon$ [Eq. (59) from [9]]. When $q = 1$, the success probability becomes $(1 - \epsilon) \times (1 + 4\epsilon^2)$, and hence the probability of error becomes $\epsilon - 4\epsilon^2 + 4\epsilon^3$. The overall failure probability becomes $\frac{\int_0^{\epsilon_0}(\epsilon - 4\epsilon^2 + 4\epsilon^3)d\epsilon}{\int_0^{\epsilon_0} d\epsilon} = (\frac{1}{2}\epsilon_0 - \frac{4}{3}\epsilon_0^2 + \epsilon_0^3)$. It should be pointed out that this algorithm is designed to give its best performance not around ϵ close to 0 but over a broad range for ϵ varying between 0.0 and 0.5.

C. New algorithm.—As in the quantum search algorithm, encode the N items in the database in terms of $\log_2 N$ qubits. The algorithm consists of applying the transformation $WR_{\bar{0}}WR_tW$ to $|\bar{0}\rangle$ (W denotes the Walsh-Hadamard Transformation and $\bar{0}$ is the state with all qubits set to 0). After this an observation is made which makes the system collapse into a basis state.

In order to analyze the performance of this algorithm, note that this algorithm is a special case of the phase-shift transformation $UR_sU^\dagger R_tU$ (1) applied to $|s\rangle$ which has already been analyzed in Sec. III. The algorithm follows from (1), by substituting the W-H transform (W) for U and the $\bar{0}$ state (state with all qubits in the 0 state) for s. Then $\|U_{ts}\|^2$ is the fraction of marked items which is $1 - \epsilon$. ϵ

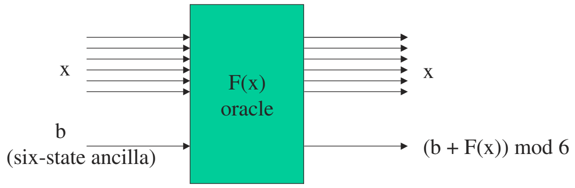

FIG. 3 (color online). By setting the six-state ancilla, b, to the superposition $\frac{1}{\sqrt{6}}(|0\rangle + |1\rangle\omega + |2\rangle\omega^2 + |3\rangle\omega^3 + |4\rangle\omega^4 + |5\rangle\omega^5)$, where $\omega = \exp(-\frac{i\pi}{3})$, we get a $\frac{\pi}{3}$ phase shift of the states for which $F(x) = 1$ relative to those for which $F(x) = 0$.

lies in the range $(0, \epsilon_0)$. Therefore after applying the transformation $WR_{\bar{0}}WR_tW$ to $|\bar{0}\rangle$, the probability of being in a non-t state becomes ϵ^3; i.e., the overall failure probability becomes $\frac{\int_0^{\epsilon_0} \epsilon^3 d\epsilon}{\int_0^{\epsilon_0} d\epsilon} = \frac{1}{4}\epsilon_0^3$.

The performance of the algorithm is graphically illustrated in Fig. 2. In [5], it will be shown that the performance of the phase-shift algorithm of this Letter for the types of problems discussed in this section is asymptotically optimal.

VIII. Quantum control and error correction.—Let us say that we want to implement a certain transformation U to drive the system into a t state (or subspace) with certainty. However, when U is applied to s, the probability of reaching t is only $(1 - \epsilon)$; i.e., U produces an error of ϵ. The analysis of Sec. III shows that if we can apply the composite operation $UR_sU^\dagger R_tU$ to $|s\rangle$, then we can reduce the error from ϵ to ϵ^3. This implementation thus depends on our ability to efficiently apply the operations U, R_s, $U^\dagger$, and R_t. Similar transformations occur in the context of *self-correcting pulses* and have been extensively studied in NMR. This connection will be developed further in [10] where a threshold condition is derived and it is shown how to eliminate errors module by module.

Quantum gates being reversible, we assume that we can apply $U^\dagger$ as easily (note that this must reuse the same or very similar hardware as what U did so as to keep the error exactly the same). For systematic errors and slowly varying random errors, this can probably be achieved since we assume that the circuit parameters stay fixed in time. R_s and R_t require us to selectively shift the phases of certain states. Shifting the phase of a state is as easy as identifying the presence of the state (Fig. 3). This leads to a number of different control and error-correction schemes, depending on the type of error to be corrected. To summarize, the error-correction technique requires the following conditions to be satisfied: (i) In case we are correcting errors in a transformation, U, we should be able to apply U twice and $U^\dagger$ once. These transformations must be applied with exactly the same error as in the original U. (ii) We should have a submodule to distinguish the signal part of the output wave function from the error. This is necessary to carry out R_t. (iii) Finally, we assume the ability to perform noiseless R_t and R_s operations. Reference [10] shows in detail how the methodology of this Letter can be used to design elementary (one and two qubit gates) that perform precisely even in the presence of small errors in R_s and R_t.

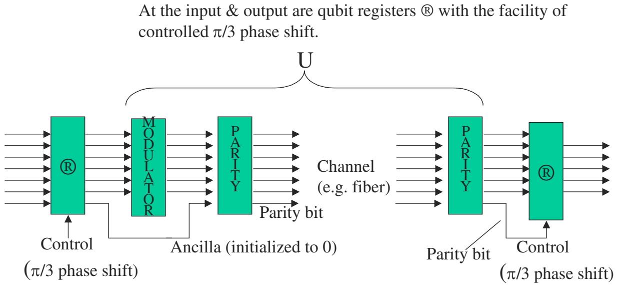
At the input & output are qubit registers ® with the facility of controlled π/3 phase shift.
U
®
MODULATOR
PARITY
Parity bit
Channel
(e.g. fiber)
PARITY
®
Control
(π/3 phase shift)
Ancilla (initialized to 0)
Parity bit
Control
(π/3 phase shift)

FIG. 4 (color online). Redundancy, in the form of a parity bit, helps to detect, and *correct*, single bit-flip errors.

We illustrate this error-correction procedure with a simple example (Fig. 4). Consider the problem of transmitting classical information over a quantum channel. Although the channel is quantum, the information of interest is classical. Therefore the only portion of the errors that are of concern are the amplitude errors (i.e., bit-flip errors); we do not care about the phase. It is well known that by adding a single parity bit, we will be able to identify the presence of single bit-flip errors. To correct these would normally require additional bits. By making use of the error-correction scheme of this Letter, we show how to *correct* single bit-flip errors using just a single parity qubit using two U and one $U^\dagger$ transformations. The quantum nature of the scheme enables us to *correct* the error without using any additional qubits.

Reference [10] discusses some more realistic examples which demonstrate the advantage of this scheme.

IX. Conclusion.—The variant of quantum searching discussed in this Letter supplements the original search algorithm by providing a scheme that permits a fixed point and hence moves towards a target state in a more directed way. This new scheme leads to a robust quantum scheme for quantum searching that is within a constant factor of the most efficient possible [5]. Also it naturally leads to schemes for error correction. Recently, the algorithm has been implemented using NMR [11].

Research was partly supported by NSA, ARDA, and ARO under Contract No. DAAG55-98-C-0040.

*Electronic address: lkgrover@bell-labs.com

[1] G. Brassard, Science **275**, 627 (1997).
[2] G. Brassard and P. Hoyer, *Proceedings of the 5th Israeli Symposium on the Theory of Computing Systems (ISTCS), Ramat-Gan, Israel, 1997*, quant-ph/9704027, pp. 12–23.
[3] L. K. Grover, Phys. Rev. Lett. **80**, 4329 (1998).
[4] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[5] S. Chakraborty, J. Radhakrishnan, and N. Raghunathan, "Bounds on Error-Reduction with Few Quantum Queries," in Proceedings of RANDOM & APPROX, Berkeley, California, 2005 (Springer-Verlag, Berlin, to be published).
[6] T. Tulsi, L. Grover, and A. Patel, quant-ph/0505007.
[7] M. Boyer *et al.*, quant-ph/9605034; Fortschr. Phys. **46**, 493 (1998).
[8] M. Mosca, Theor. Comput. Sci. **264**, 139 (2001).
[9] Ahmed Younes *et al.*, quant-ph/0312022.
[10] B. Reichardt and L. K. Grover, quant-ph/0506242 [Phys. Rev. A (to be published)].
[11] L Xiao and J. Jones, Phys. Rev. A **72**, 032326 (2005).