Dominant gate imperfection in Grover's quantum search algorithm

Gui Lu Long,[1,2,3,*] Yan Song Li,[1] Wei Lin Zhang,[1] and Chang Cun Tu[1]
[1]*Department of Physics, Tsinghua University, Beijing 100084, People's Republic of China*
[2]*Institute of Theoretical Physics, Chinese Academy of Sciences, Beijing 100080, People's Republic of China*
[3]*Center of Nuclear Theory, National Laboratory of Heavy Ion Physics, Lanzhou 730000, People's Republic of China*
(Received 5 October 1999; published 10 March 2000)

It is found that systematic errors in phase inversions and random errors in Hadmard-Walsh transformations are the dominant gate imperfection in Grover's quantum search algorithm. They lead to reductions in the maximum probability of the marked state and affect the efficiency of the algorithm. Given the degree of inaccuracy, we find that to guarantee a half-rate of success, the size of the database should be on the order of $O(1/\delta^2)$, where δ is the uncertainty.

PACS number(s): 03.67.Lx, 89.70.+c

I. INTRODUCTION

Grover's quantum search algorithm is a remarkable achievement in quantum computing [1]. There has been intense interest in Grover's quantum search algorithm recently [2–18]. It uses only two simple gate operations, controlled phase rotations and Hadamard transformations. It has been successfully demonstrated in solution NMR bulk quantum computers with a few qubits [2,3]. However, the inevitable quantum state decoherence and gate inaccuracies can introduce errors [18,19], which accumulate throughout the computation and make long computation unreliable, while in order to find the marked state with high probability, it still requires an exponential number of iterations. Thus, the error probability of the complete algorithm may be as exponentially large as the error probability of each iteration. In other words, even with small imperfection per step, large scale quantum search may be difficult.

Fortunately, recent study of quantum error correction shows that in principle, whenever the noise rates are below a constant threshold, an arbitrarily long quantum operation can be performed reliably through *fault-tolerant quantum computation* [20]. Experimentally, different types of faults can occur with different rates and will affect the efficiencies of the algorithm differently. For example, the effects of quantum state decoherence and operational errors on the efficiency of quantum algorithms have been studied in [21] with ion trap quantum computers. A good understanding of the effect on the algorithms from different noise can help us look for specific potential physical realizations of quantum computers.

In this paper, we address the problem of influences of different imperfect gate operations in the quantum search algorithm, in the absence of decoherence and error corrections. We have found that systematic phase mismatching and random errors in the Walsh-Hadmard transformation are the dominant gate imperfections affecting the algorithm. They lead to exponential reduction in the maximum success probability. To ensure a large success rate in a quantum searching machine, the size of the database should be limited. This limitation is due to the intrinsic vulnerability of the algorithm to imperfect gate operation. Fault tolerant quantum computation can reduce gate imperfection and decoherence. This will ease the demand on gate perfection. However, quantum error correction also uses useful resources. In practice, one has to take into account the balance between available resources and the size of the database.

The paper is organized as follows. Section II is devoted to the description of different error models in phase mismatching and the corresponding simulation results. In Sec. III, we present the consequences of imperfect Hadamard transformations. Section IV gives a short summary.

II. EFFECTS OF IMPERFECT PHASE INVERSIONS

Grover's algorithm consists of essentially four steps in an iteration [5]: (1) a Walsh-Hadamard transformation $U=W$; (2) a phase inversion of the prepared state $|\gamma\rangle, I_\gamma = I - 2|\gamma\rangle\langle\gamma|$, where usually $|\gamma\rangle = |0\rangle$; (3) a phase inversion of the marked state $|\tau\rangle, I_\tau = I - 2|\tau\rangle\langle\tau|$; and (4) an inverse of the Walsh-Hadamard transformation $U^{-1}=W$ (W is self-inverse). The operator for one Grover iteration is $Q = -I_\gamma U^{-1} I_\tau U$.

In this section, we focus on the imperfections in phase inversions and therefore choose U to be the ideal Hadamard transformation. We consider the imperfections in the phase inversion to be *systematic*, that is,

$$I_\gamma = I - (1-e^{i\theta})|\gamma\rangle\langle\gamma|,$$
$$I_\tau = I - (1-e^{i\varphi})|\tau\rangle\langle\tau|, \tag{1}$$

where $\theta = \pi + \theta_0, \varphi = \pi + \varphi_0$ with θ_0 and φ_0 *constant* and small. When $\theta_0 = \varphi_0 = 0$, we recover the original Grover's algorithm. The generalized quantum search algorithm is a rotation in a two-dimensional space spanned by $|\gamma\rangle$ and $|\tau\rangle$. In the following orthonormal basis:

$$|1\rangle = \frac{(|\gamma\rangle - U_{\tau\gamma} U^{-1}|\tau\rangle)}{\sqrt{1-|U_{\tau\gamma}|^2}},$$
$$|2\rangle = U^{-1}|\tau\rangle, \tag{2}$$

*Electronic address: gllong@mail.tsinghua.edu.cn where $U_{\tau\gamma}=\langle\tau|U|\gamma\rangle=1/\sqrt{N}$, the operator Q is represented by

$$\begin{pmatrix} -e^{i\theta}-|U_{\tau\gamma}|^2(1-e^{i\theta}) & (1-e^{i\theta})U_{\tau\gamma}\sqrt{1-|U_{\tau\gamma}|^2} \\ e^{i\varphi}(1-e^{i\theta})U^*_{\tau\gamma}\sqrt{1-|U_{\tau\gamma}|^2} & -e^{i\varphi}[1-(1-e^{i\theta})|U_{\tau\gamma}|^2] \end{pmatrix}. \tag{3}$$

Let $\delta=\theta-\varphi=\theta_0-\varphi_0$. It has been shown that to construct an efficient quantum search algorithm, the phase matching requirement $\theta=\varphi$ must be observed [22,23] [it is much easier to see this phase matching condition in an SO(3) picture [24]]. However due to imperfections in gate operations, this phase matching requirement cannot be strictly satisfied. In the following, we show that nonzero constant δ results in exponential reduction in the maximum success probability of Grover's algorithm asymptotically.

Since both θ_0 and φ_0 are small, by dropping off an overall phase, we approximate Q as

$$Q \doteq \cos\delta I + i\sin\delta\sigma_z + i\beta'\sigma_y + o(\beta'), \tag{4}$$

where σ_x, σ_y, and σ_z are Pauli operators and I is the identity operator in dimension 2. $\beta'=2\beta+O(\theta_0\beta)=2\beta+o(\beta)$ with $\beta=(\sqrt{N-1})/N$. For small δ, we can further simplify operator Q as

$$Q\approx I+iG\approx e^{iG},$$

with $G=\sin\delta\sigma_z+\beta'\sigma_y$. Using $G^2=(\delta^2+\beta'^2)I$, we obtain

$$Q^j=\begin{bmatrix} \cos j\lambda+i\dfrac{\delta\sin j\lambda}{\lambda} & \dfrac{\beta'\sin j\lambda}{\lambda} \\ -\dfrac{\beta'\sin j\lambda}{\lambda} & \cos j\lambda-i\dfrac{\delta\sin j\lambda}{\lambda} \end{bmatrix}, \tag{5}$$

with $\lambda=\sqrt{\delta^2+\beta'^2}$. Then, starting from the prepared state $|\gamma\rangle=\sqrt{1-|U_{\tau\gamma}|^2}|1\rangle+U_{\tau\gamma}|2\rangle=\cos\beta|1\rangle+\sin\beta|2\rangle\approx|1\rangle$, after j number of iterations, the norm of the amplitude of the marked state in the quantum computer is

$$|B_j|\approx\frac{\beta'}{\lambda}\sin(j\lambda) \tag{6}$$

and the maximum probability of the marked state in the algorithm is

$$P_{max}\approx\frac{\beta'^2}{\beta'^2+\delta^2}\leqslant 1. \tag{7}$$

Therefore, for large N, Grover's algorithm is efficient only when $\delta=0$. When $\delta\neq 0$, we find

$$P_{max}\approx\frac{\beta'^2}{\delta^2}\sim\frac{4}{N\delta^2}. \tag{8}$$

Thus, P_{max} decreases linearly with N or exponentially with $n=\log_2 N$. This concludes our proof that systematic phase mismatching results in exponential reduction in the success probability and consequently gives an upper bound on the size of the database. If a half-rate of success is required, that is $P_{max}\geqslant 1/2$, N cannot exceed $8/\delta^2$.

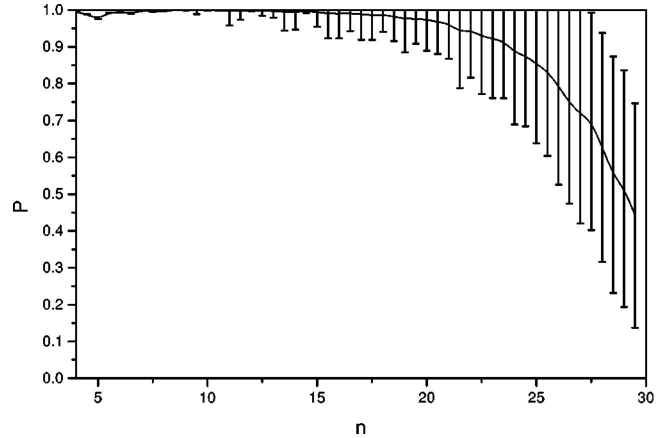

FIG. 1. The maximum probability of finding the marked state P vs $n=\log_2 N$ for EM2 where only random errors exist. The standard deviation $s=0.01$. The central line is the average over 500 simulations for each point.

So far, we have assumed that the errors in the phase inversions are systematic such that δ is constant. We now extend this simple error model (EM1) to another two error models. The second error model (EM2) assumes that δ in each step is a Gaussian random variable with mean $\delta_0=0$ and standard deviation s. Such an error is conventionally defined as *random* error. Finally, we let δ be a Gaussian random variable with mean $\delta_0\neq 0$ and standard deviation s (EM3). The exact effects of EM2 and EM3 are difficult to compute analytically due to their randomness. Hence, we only present the simulation results. We vary $n=\log_2 N$ and run the algorithm with sufficient number of iterations so that a maximum probability is found. Since δ in EM2 and EM3 are random variables, we adopt the *random sampling* technique in the simulation. The relationships between the maximum success rate and the size of the database are shown in Fig. 1 and Fig. 2 for EM2 and EM3, respectively. For comparison, we also provide the simulation result from EM1 in Fig. 3.

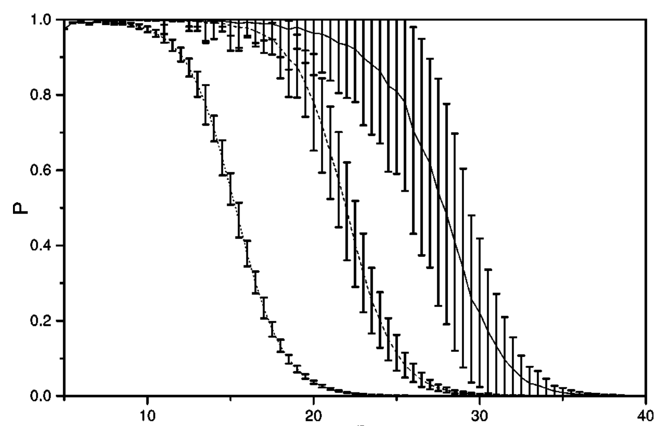

FIG. 2. The same as Fig. 1 for EM3 where both random and systematic errors exist. $s=0.01$. Solid line for $\delta_0=0.01$, short dashed line for $\delta_0=0.001$, and dotted line for $\delta_0=0.0001$.

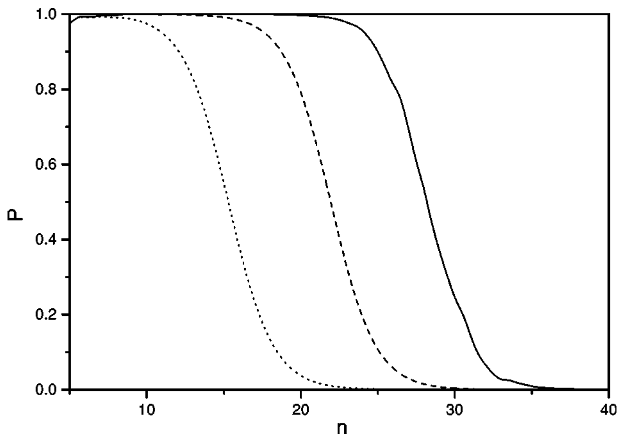

FIG. 3. The same as Fig. 1 for EM1 where only systematic error in the phase inversions exists. N is the size of the database and $\beta = 1/\sqrt{N}$. Solid line for $\delta_0 = 0.01$, short dashed line for $\delta_0 = 0.001$ and dotted line for $\delta_0 = 0.0001$.

Our simulation results are consistent with mathematical predictions. First, both systematic and random errors cause reduction in the maximum probability. Second, the success probability drops quickly after a transition point, which is determined by the error parameters δ_0 and s. When n is large, the probability decreases exponentially. Third, the different effects of systematic errors and random errors also meet our expectations. Mathematically, systematic errors cause the error amplitudes to grow exponentially with the number of gates applied; while random errors cause the error probabilities to grow linearly. This difference is clearly demonstrated in our simulation results. Figure 1 shows that random errors give a much larger transition point than systematic errors. Figure 2 shows that the average success probability from EM3 is nearly identical to that of EM1 except for some small fluctuations.

It is shown in this section that systematic errors in the phase inversions lead to reduction in the maximum probability of finding the marked state. Random errors also affect this success rate, but in a lesser degree. In practice, we should make δ_0 as small as possible. However, due to imperfection, nonzero δ_0 inevitably occur. For instance, systematic errors arise from imperfect calibration and inhomogeneity in the radio frequency pulses in NMR realization. Random errors are always present in a realistic environment. These errors will reduce the maximum probability of the algorithm. To make an estimate of the combined effect of systematic and random errors (EM3), we assume that random errors affect the algorithm just like the systematic errors. Then we can treat $\Delta = 2\delta$ as the uncertainty due to both systematic errors and random errors and use this to derive an upper bound for the size of a quantum database: *any phase inversion operation is imperfect, there is an uncertainty, and this uncertainty sets an upper bound on the size of the database N*. For a half-rate of success, the dimension of the database should be less than $64/\Delta^2$.

III. IMPERFECT HADAMARD TRANSFORMATION

Hadmard-Walsh transformations are also subject to errors. To study the effect of the imperfect Hadmard-Walsh transformation, let us take $\delta = 0$ in Eq. (5). Then the maximum probability for finding the marked state is approximately $\sin^2(2j\beta)$ for perfect unitary transformation. For a perfect Hadamard-Walsh transformation, $\beta = \arcsin(|U_{\tau\gamma}|)$, and $|U_{\tau\gamma}| = \sqrt{1/N}$. For systematic errors in the Hadmard-Walsh transformation, the matrix elements of U are no longer equal to $\sqrt{1/N}$. If $|U_{\tau\gamma}|$ is larger than $\sqrt{1/N}$, then the algorithm will require fewer steps in reaching the desired state compared with the standard Grover's algorithm. If $|U_{\tau\gamma}|$ is smaller than $\sqrt{1/N}$, the algorithm will require more steps of iteration. In this case, the searching algorithm can still give a probability quite close to unity. But if one makes a measurement at the normal optimal number of iterations, one gets a reduction in the success rate. This difficulty can be overcome by using the algorithm several times with measurements made around the optimal number of iterations, which is similar to the method used in Ref. [12].

Here, we give a simple interpretation of why Grover's algorithm is optimal. The rigorous proof has been given in Ref. [11]. Grover's algorithm can be seen as a rotation of the state vector in a two-dimensional space spanned by $|\tau\rangle$ and $|\gamma\rangle$. Each iteration rotates an angle $\lambda = \beta' = 2\sin(\theta/2)\beta$. $\theta = \phi = \pi$ gives the largest angle $2\beta = 2\arcsin(|U_{\tau\gamma}|)$. So one has to choose phase inversions to make the algorithm efficient. As for the unitary transformation U, at first glance one may be tempted to think that a larger $|U_{\tau\gamma}|$ will constitute a faster search algorithm. However, since U is unitary, its matrix elements satisfy the normalization relation $\Sigma_\tau |U_{\tau\gamma}|^2 = 1$, where τ runs through all the N basis states. The mean value of the matrix element is $\sqrt{1/N}$. If some of the matrix elements are larger than this average, some other matrix elements will be less than this average. In other words, while making the search for some marked states in fewer steps, the modified algorithm has to search the rest of the basis states in more steps. In contrast, the original Grover's algorithm searches all possible marked states with the same optimal number of iterations. Together with its simpleness and ease of implementation, the Walsh-Hadamard transformation is the best choice.

We discuss the effects of random errors in the Walsh-Hadamard transformation in a simple model. In this case, the algorithm is no longer a simple rotation in two dimensions. Though in each iteration, the operator can be approximately written as

$$Q = \begin{pmatrix} \cos\beta & \sin\beta \\ -\sin\beta & \cos\beta \end{pmatrix}, \tag{9}$$

the basis states in each iteration have been changed, that is, the two-dimensional space in each iteration is no longer the same. This is apparent from inspecting the expressions in Eq. (2). Suppose in the first iteration that the unitary transformation is U and in the following iteration the operator becomes V. Then after the first iteration, the state vector of the quantum computer is

$$|\psi_1\rangle = \cos\beta|1\rangle - \sin\beta|2\rangle \approx \cos\beta|1'\rangle - \sin\beta U^{-1}V|2'\rangle, \tag{10}$$

where $|1'\rangle$ and $|2'\rangle$ are obtained from Eq. (2) by substituting U with V. Because $U \neq V, U^{-1}V$ is no longer the identity operator. Expanding $U^{-1}V|2'\rangle = (U^{-1}V)_{22}|2'\rangle + \cdots$, we see that the Grover search operator acts only on the subspace spanned by $|1'\rangle$ and $|2'\rangle$, and the other terms are leaked out of the two-dimensional space. To make an estimate, let us assume that in each iteration, $(U^{-1}V)_{22}|2'\rangle \approx (1-\delta_1)|2\rangle +$ higher order terms. Then in this model, the matrix for a Grover search operator becomes

$$Q = \begin{pmatrix} \cos\beta & \sin\beta(1-\delta_1) \\ -\sin\beta & \cos\beta(1-\delta_1) \end{pmatrix}. \tag{11}$$

Starting from initial state $|\gamma\rangle \approx |1\rangle$, after j iterations, the amplitude of the state $|2\rangle$ becomes

$$\left| \left(1 - \frac{j-1}{2}\delta_1 \right) \sin(j\beta) \right|, \tag{12}$$

where only first order in δ_1 is retained. With the optimal number of iterations, $j \approx \pi\sqrt{N}/4, \sin(j\beta) \approx 1$, the success rate is

$$P \approx \left(1 - \frac{\pi\sqrt{N}\delta_1}{8} \right)^2 \approx 1 - \frac{\pi\sqrt{N}\delta_1}{4}. \tag{13}$$

For a half-success rate, one must have $N \leqslant 4/\pi^2\delta_1^2$, which is similar to the limitation on the size of the database in the phase inversion inaccuracies. However, the mechanism is different. Here the random errors play a more important role than the systematic errors, whereas in the phase inversion case, it is just the opposite.

IV. SUMMARY

In summary, we find that the dominating gate imperfections in Grover's algorithm are the systematic phase mismatching and the random errors in the Walsh-Hadmard transformation. Using the results obtained in this work, it is easy to understand the simulation results of Ref. [21]. In Fig. 1(a) of [21] (the results with only random errors in both phase inversions and Hadmard transformation), we see that the peak in the probability curve drops down as random errors grow. But the position of the peak is relatively fixed. Random errors in the phase inversion do not affect the algorithm very seriously. Random errors in the Hadmard transformation reduce the maximum probability. The optimal iteration number remains more or less the same. When there are only systematic errors as shown in Fig. 2(b) of Ref. [21], we see a drop in the maximum probability and also a shifting of the peak position to the left. The drop in maximum probability is caused by systematic phase mismatching. The shift of the peak position is due to the systematic errors in the Walsh-Hadmard transformation.

These gate inaccuracies set an upper bound on the size of the database. We estimate that the upper bound is inversely proportional to the quadrature of the uncertainty in the phase mismatching or in the Walsh-Hadmard transformation. In real quantum computation, imperfect gate operations exist all the time at a constant rate while decoherence increases rapidly with computing time. At the early stage of a quantum computation, gate imperfection is dominant in affecting a quantum algorithm. As the computation continues, decoherence increases and then dominates. Suitable quantum correction codes and in particular fault-tolerant quantum computation can reduce the decoherence and gate inaccuracies and ease the stringent requirement on gate accuracies. The limitations on the quantum data size can then be greatly relieved. However, quantum error correction also uses useful resources. In pratice, one has to make a balance between the extent of quantum error correction and the size of the quantum database.

ACKNOWLEDGMENTS

Encouragement from Professor Haoming Chen and Hongzhou Sun and helpful discussions with Dr. C. Zalka are gratefully acknowledged. We thank Dr. Bisset for a careful reading of the manuscript. This work was supported in part by the China National Natural Science Foundation Grant No. 19775026, the Fok Ying Tung Education Foundation, and the Education Ministry of China.

[1] L.K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[2] J.A. Jones, M. Mosca, and R.H. Hansen, Nature (London) **393**, 344 (1998).
[3] I.L. Chuang, N. Gershenfeld, and M. Kubinec, Phys. Rev. Lett. **80**, 3408 (1998).
[4] L.K. Grover, Phys. Rev. Lett. **79**, 4709 (1997).
[5] Lov K. Grover, Phys. Rev. Lett. **80**, 4329 (1998).
[6] G. Brassard, Science **275**, 627 (1997).
[7] G. Brassard, P. Hφyer, and A. Tapp, e-print quant-ph/9805082.
[8] Liping Fu, Li Xiao, Jun Luo, and Xizhi Zheng, Chin. J. Magn. Res. **16**, 341 (1999).
[9] C. Bennett *et al.*, SIAM J. Comput. **26**, 1510 (1997).
[10] M. Boyer, G. Brassard, P. Hφyer, and A. Tapp, Fortschr. Phys. **46**, 493 (1998).
[11] C. Zalka, e-print quant-ph/9711070.
[12] C. Zalka, e-print quant-ph/9902049.
[13] D. Biron *et al.*, e-print quant-ph/9801066.
[14] A. Kumar Pati, e-print quant-ph/9807067.

[15] Y. Ozhigov, e-print quant-ph/9904039.
[16] R. Gingrich, C. P. Williams, and N. Cerf, e-print quant-ph/9904049.
[17] R. Josza, e-print quant-ph/9901021.
[18] Sixia Yu and Chang-pu Sun, e-print quant-ph/9903075.
[19] I.L. Chuang, R. Laflamme, P.W. Shor, and W.H. Zurek, Science **270**, 1633 (1995).
[20] J. Preskill, Proc. R. Soc. London, Ser. A **454**, 385 (1998).
[21] K. Obenland and A.M. Despain, e-print quant-ph/9804038.
[22] G.L. Long, W.L. Zhang, Y.S. Li, and L. Niu, Commun. Theor. Phys. **32**, 335 (1999).
[23] G.L. Long, Y.S. Li, W.L. Zhang, and L. Niu, Phys. Lett. A **262**, 27 (1999).
[24] G.L. Long, C.C. Tu, Y.S. Li, W.L. Zhang, and H.Y. Yan, e-print quant-ph/9911004.