Effects of dynamical phases in Shor's factoring algorithm with operational delays

L. F. Wei,[1,2] Xiao Li,[3,4] Xuedong Hu,[1,5] and Franco Nori[1,*]
[1]*Frontier Research System, The Institute of Physical and Chemical Research (RIKEN), Wako-shi, Saitama, 351-0198, Japan*
[2]*Institute of Quantum Optics and Quantum Information, Department of Physics, Shanghai Jiaotong University, Shanghai 200030, China*
[3]*Department of Physics, Shanghai Jiaotong University, Shanghai 200030, China*
[4]*Department of Physics, PMB 179, 104 Davey Laboratory, Penn State University, University Park, Pennsylvania 16802-6300, USA*
[5]*Department of Physics, University at Buffalo, SUNY, Buffalo New York 14260-1500, USA*
(Received 5 May 2003; revised manuscript received 15 July 2004; published 22 February 2005)

Ideal quantum algorithms usually assume that quantum computing is performed continuously by a sequence of unitary transformations. However, there always exist idle finite time intervals between consecutive operations in a realistic quantum computing process. During these delays, *coherent errors* will accumulate from the dynamical phases of the superposed wave functions. Here we explore the sensitivity of Shor's quantum factoring algorithm to such errors. Our results clearly show a severe sensitivity of Shor's factorization algorithm to the presence of delay times between successive unitary transformations. Specifically, in the presence of these coherent errors, the probability of obtaining the correct answer decreases exponentially with the number of qubits of the work register. A particularly simple phase-matching approach is proposed in this paper to *avoid* or suppress these coherent errors when using Shor's algorithm to factorize integers. The robustness of this phase-matching condition is evaluated analytically and numerically for the factorization of several integers: 4, 15, 21, and 33.

DOI: 10.1103/PhysRevA.71.022317 PACS number(s): 03.67.Lx

I. INTRODUCTION

Building a practical quantum information processor has attracted considerable interest during the past decade [1]. With the resources provided by quantum mechanics, such as superposition and entanglement, a quantum computer could achieve a significant speedup for certain computational tasks. The most prominent example is Shor's factoring algorithm [2,3], which allows an exponential speedup over the known classical algorithms. The proposed quantum algorithms are constructed assuming that all quantum operations can be performed precisely. In reality, any physical realization of such a computing process must treat various errors arising from various noise and imperfections (see, e.g., [4]). Physically, these errors can be distinguished as two different kinds: incoherent and coherent errors. The incoherent errors originate from the coupling of the quantum information processor to an uncontrollable external environment, which is stochastic and results in decoherence. Coherent errors usually arise from nonideal quantum gates which lead to unitary but nonideal temporal evolutions of a quantum computer. So far, most previous works (see, e.g., [5–9]) have been concerned with quantum errors arising from the decoherence due to interactions with the external environment and external operational imperfections. Here, we focus instead on internal ones. The coherent errors we consider here are related to the *intrinsic* dynamical evolution of the qubits *between* operations.

A quantum computing process generally consists of a sequence of quantum unitary operations. These transformations are usually applied to the superposition states so that the quantum computer evolves from an input initial state to the desired final state. If the two qubit levels have different energies, as is usually the case, the superposition wave function of the quantum register undergoes fast coherent oscillations during the finite time delay between two consecutive operations. These oscillation, if not controlled, can spoil the correct computational results expected from the ideal quantum algorithms, where operational delays are neglected.

In principle, these coherent errors can be either (1) avoided by tuning the relevant energy splittings of the qubits to zero [10,11] or (2) eliminated by introducing a "natural" phase induced by using a stable continuous reference oscillation for each quantum transition in the computing process [12]. Indeed, a possible approach to study the present problem could consider the use of simple error-avoidance schemes, such as encoding each logical qubit in two physical qubits via $|0\rangle \rightarrow |01\rangle + |10\rangle$, $|1\rangle \rightarrow |01\rangle - |10\rangle$ so that both states have the same energy. We prefer to use our (quite different) approach presented here because it does not involve increasing the number of physical qubits to encode a logical qubit. This increase can involve increased complexity in the device and in its operation. Also note that qubits in solid-state systems are never truly identical (in contrast with trapped ions). Nonidentical qubits limit the applicability of the above encoding approach. Without using a few physical qubits to encode a logical qubit, we show in the present work that the discussed coherence errors can be efficiently avoided by a phase-matching strategy, by setting the total delay between successive operations On the other hand, experimentally—for example, in NMR systems (see, e.g., [3,13])—the above coherence errors were usually corrected by introducing two

*Permanent address: Center of Theoretical Physics, Physics Department, Center for the Study of Complex Systems, University of Michigan, Ann Arbor, Michigan 48109-1120, USA.

additional operations before and after the delay to reverse each undesired free evolution.

In this paper we perform a quantitative assessment of the effects of the dynamical phases in Shor's algorithm by realistically assuming that operational delays, between successive unitary transformations, exist throughout the computation. We explore a phase-matching approach to deal with the dynamical phase problem. We show that coherent "errors" due to these phases, acquired by the dynamical evolution of the superposed wave function during the operational delays, may be avoided by properly setting the *total* delay. We then carefully evaluate the robustness of such a phase-matching condition, focusing on its dependence on the number of qubits, the length of the delay, and the fluctuations in the qubit energy splitting. Our discussions are in the context of Shor's algorithm, but can be extended to other quantum algorithms, such as the phase estimation and other algorithms [14]. For simplicity and clarity, here we assume that the influence of the environmental decoherence and the gate imperfections on the computing process are negligible.

The paper is organized as follows. In Sec. II, we present a decomposition of Shor's algorithm and explain how we incorporate the dynamical phases into the realization of this algorithm. The usual decompositions of quantum algorithms into consecutive elementary gates are strictly limited by the short decoherence time. Here, we reconstruct the standard Shor's algorithm out of four functional unitary transformations and only consider the operational delays between these larger building blocks. We assume that each block can be exactly performed by only one-time evolution as a multiqubit gate (see, e.g., [15,16]), avoiding the existing idle time inside it. It is shown that the effects of dynamical phases are not negligible, even in this primary or "coarse-grained" decomposition. In Sec. III, we analytically and numerically evaluate several examples to illustrate the phase-matching condition and establish a clear relationship between this condition and the equivalence of the Schrödinger picture and the interaction picture description of a physical system. We also demonstrate the robustness of the phase-matching condition by varying the number of qubits involved, the delay duration, and distribution of qubit energy splitting. Finally, in Sec. IV we present some conclusions and discussions from our numerical studies.

II. FOUR-BLOCK DECOMPOSITION OF SHOR'S ALGORITHM WITH OPERATIONAL DELAYS

We study the dynamical phase problem in the context of Shor's factoring algorithm. In Shor's algorithm [2], the factorization of a given number N is based on calculating the period of the function $f(x)=a^x \bmod N$ quantum mechanically for a randomly selected number a $(1<a<N)$ coprime with N. Here $y \bmod N$ is the remainder when y is divided by N. The order r of $a \bmod N$ is the smallest integer r such that $a^r \bmod N=1$. Once r is known, factors of N are obtained by calculating the greatest common divisor of N and $y^{r/2}\pm 1$. A quantum computer can find r efficiently by a series of quantum operations on two quantum registers W and A. One is the work register W with L qubits, in which the job of finding the order is done, while the values of the function $f(x)$ are stored in the auxiliary register A with L' qubits. The sizes of the work and auxiliary registers are chosen as the integers satisfying the inequalities $N^2<q=2^L<2N^2$ and $2^{L'-1}<N<2^{L'}$. Here q is the Hilbert space dimension of the work register.

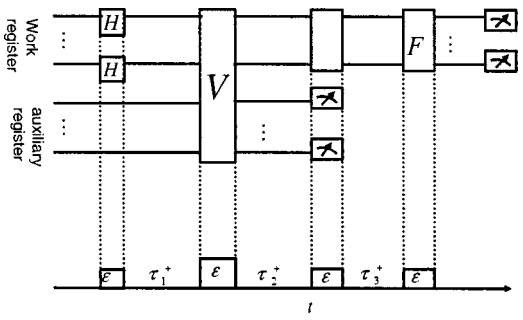

FIG. 1. Quantum circuit for implementing Shor's algorithm with time delays $\tau_j^+(j=1,2,3)$ between the successive operations. Here H refers to a Hadamard gate, while F refers to a quantum Fourier transformation. Each block operation is assumed to be exactly performed in a very short time interval ε (so that phases accumulated during the operations are either accounted for by the operations themselves or simply neglected).

As shown in Fig. 1, a realistic implementation of Shor's algorithm can be decomposed into the following unitary transformations.

(1) Initialize the work register in an equal-weight superposition of all the logical states and the auxiliary register in its logical ground state $|0\rangle_A$. Initially, each work qubit is in its logical ground state $|0\rangle$. Assuming that a Hadamard gate H is applied to each qubit in the work register at one time, the computational initial state of the system becomes

$$|\Psi(0)\rangle = \frac{1}{\sqrt{q}}\sum_{j=0}^{q-1} |j\rangle_W \otimes |0\rangle_A.$$

Here, the subindex W stands for the work register state and the subindex A for the auxiliary register. After a finite-time delay τ_1 and right before the second unitary transformation is applied, the initial state $|\Psi(0)\rangle$ of the whole system evolves to

$$|\Psi(\tau_1)\rangle = \frac{1}{\sqrt{q}}\sum_{j=0}^{q-1} e^{-iE_j\tau_1}|j\rangle_W \otimes e^{-iE_0\tau_1}|0\rangle_A, \qquad (1)$$

with E_j being the energy of state $|j\rangle$ and $\hbar=1$. Here, $\tau_m(m=1,2,3,\ldots)$ denotes the time interval between the $(m-1)$th and mth unitary operations. $\tau_m^+=\tau_m+\epsilon$ with $\epsilon \ll \tau_m$ being the operational time of the mth unitary transformation, here assumed to be extremely small compared to other time scales. In other words, τ_m^+ refers to the time interval between the end of $(m-1)$th operation and the end of the mth operation. In what follows, the global dynamical phase $\exp(-iE_0\tau_1)$ will be omitted as it does not have any physical meaning.

(2) Calculate the function $f_{N,a}(j)=a^j \bmod N$ and then entangle the work $\{|j\rangle_W\}$ and auxiliary registers $|f_{a,N}(s)\rangle_A$ by applying a joint operation $\hat{V}$. After another finite-time delay τ_2 before the next step (i.e., the third unitary transformation),

the entangled state of the whole system becomes

$$|\Psi(\tau_1^+ + \tau_2)\rangle = \frac{1}{\sqrt{q}}\sum_{s=0}^{r-1} |\psi\rangle_W \otimes |\phi\rangle_A, \tag{2}$$

where

$$|\phi\rangle_A = \exp[-iE_{f_{a,N}(s)}\tau_2]|f_{a,N}(s)\rangle_A$$

and

$$|\psi\rangle_W = \sum_{l=0}^{w} \exp[-iE_{(lr+s)}(\tau_1^+ + \tau_2)]|lr+s\rangle_W,$$

with $w=[(q-s-1)/r]$ being the largest integer less than $(q-s-1)/r$. The dynamical phases of the qubits in the work register, before and after the joint operation $\hat{V}$, can be added directly, as this operator is diagonal in the logical basis.

(3) Measure the auxiliary register $|\phi\rangle_A$ in its computational basis $\{|j\rangle_A\}$. After this operation, the state of the whole system becomes $|\Psi(\tau_1^+ + \tau_2^+)\rangle = |\psi(\tau_1^+ + \tau_2^+)\rangle_W \otimes |\phi(\tau_1^+ + \tau_2^+)\rangle_A$. In other words, the work and auxiliary registers disentangle and the work register collapses to one of its periodic states $|\psi(\tau_1^+ + \tau_2^+)\rangle_W$.

For example, if the measurement on the auxiliary register $|\phi\rangle_A$ gives a value $A_s = a^s \bmod N$, then the work register immediately becomes

$$|\psi(\tau_1^+ + \tau_2^+)\rangle_W = \frac{1}{\sqrt{w+1}}\sum_{l=0}^{w} \exp[-iE_{(lr+s)}(\tau_1^+ + \tau_2^+)]|lr+s\rangle_W.$$

After the third unitary transformation is applied, there is a third time delay τ_3. The state $|\psi(\tau_1^+ + \tau_2^+)\rangle_W$ now evolves to

$$|\psi(\tau_1^+ + \tau_2^+ + \tau_3)\rangle_W = \frac{1}{\sqrt{w+1}}\sum_{l=0}^{w} \exp[-iE_{(lr+s)}(\tau_1^+ + \tau_2^+ + \tau_3)] \times |lr+s\rangle_W. \tag{3}$$

Because of the collapse of the wave function $|\Psi(\tau_1^+ + \tau_2)\rangle$ in Eq. (2), the dynamical phases accumulated by the wave function $|\phi\rangle_A$ of the auxiliary register do not affect the algorithm anymore, as the relevant phase $\exp[-iE_{f_{a,N}(s)}\tau_2^+]$ becomes a global phase.

(4) Perform the fourth unitary transformation: the quantum Fourier transform (F transformation) on the work register $|\psi\rangle_W$, so that information regarding the order r of $a \bmod N$ (i.e., the smallest integer r such that $a^r \bmod N = 1$) can be more easily extracted. After the F transformation the state of the work register becomes

$$|\psi(\tau)\rangle_W = \frac{1}{\sqrt{q}}\sum_{k=0}^{q-1} g(k)|k\rangle_W,$$

with

$$\tau = \tau_1^+ + \tau_2^+ + \tau_3^+$$

being the time after applying the fourth unitary transformation and

$$g(k) = \frac{\exp(2\pi isk/q)}{\sqrt{w+1}}\sum_{l=0}^{w} \exp\left[-iE_{(lr+s)}\tau + 2\pi ilk\frac{l}{q}\right].$$

After another delay time τ_4—i.e., right before applying the fifth unitary transformation—the work register evolves into

$$|\psi(\tau+\tau_4)\rangle_W = \frac{1}{\sqrt{q}}\sum_{k=0}^{q-1} g(k)e^{-iE_k\tau_4}|k\rangle_W. \tag{4}$$

(5) Finally, we carry out a measurement on the work register in the computational basis $\{|j\rangle_W\}$ and derive the desired order r satisfying the condition $a^r \bmod N = 1$. This measurement yields the state $|k\rangle_W$ with probability

$$P(k) = \frac{1}{q(w+1)}\left|\sum_{l=0}^{w} \exp\left[-iE_{(lr+s)}\tau + 2\pi ilk\frac{r}{q}\right]\right|^2, \tag{5}$$

which is independent of the free evolution during the last delay τ_4. Notice that here $P(k)$ only depends on the *total* effective delay time $\tau = \tau_1^+ + \tau_2^+ + \tau_3^+$, but *not* directly on the *individual* time intervals τ_m, $m=1,2,3,4$.

In this decomposition of Shor's algorithm we have included time delays only in between the various unitary operations, which were implemented by independently using various one-time evolutions [15,16]. Note that only the delays from the initial Hadamard gates to the finishing Fourier transformation may result in physical effects. Fortunately, all the operators during these delays are either diagonal or at least not affecting the phase accumulation. Therefore, the phases in each qubit simply add up.

If each unitary transformation is itself composed of several consecutive steps, with delays between these internal steps, we assume these delays to be negligible. This condition implies that the internal time delays occurring between steps within each unitary operation should be so short that their accumulated phases are negligible. Such a condition is possibly difficult to satisfy experimentally. However, our results below show that even under such a restrictive condition the interference effects due to dynamical phases between successive unitary transformation are already too significant to be ignored.

For the ideal situation without any delay ($\tau_m \equiv 0$), the probability distribution $P(k)$ in Eq. (5) reduces to that in the original Shor's algorithm [2]. However, Eq. (5) clearly shows that the expected probabilistic distribution may be strongly modified by the interferences due to the dynamical phases of the superposition wave function, which would consequently lead to a lower probability for obtaining the desired final output.

III. EFFECTS OF DYNAMICAL PHASES

In order to study the effects of dynamical phases, we need to compute $P(k)$. The probability $P(k)$ in Eq. (5) can be computed if the energies $E_{(lr+s)}$ for the various states $|lr+s\rangle_W$ involved are known exactly. These will be computed below.

A. Phase-matching condition for eliminating the coherent errors due to operational delays

As a first approximation we assume that all qubits in a quantum computer system possess identical energy spectra. Such an approximation is valid for naturally identical systems like trapped ions. In this ideal case, when all the qubits have the same energy splitting between ground and excited states, different quantum states with the same number of excited qubits will acquire the same dynamical phase. For example, the four-qubit states $|1_3 0_2 0_1 0_0\rangle$ and $|0_3 0_2 0_1 1_0\rangle$ would acquire the same dynamical phase $\exp(-i3\epsilon_0 t - i\epsilon_1 t)$ during a delay time t. Here ϵ_0 and ϵ_1 are the energies of a single qubit corresponding to the ground state $|0\rangle$ and the excited state $|1\rangle$, respectively. Under this approximation, Eq. (5) can be rewritten as

$$P(k) = \frac{1}{q(w+1)} \left| \sum_{l=0}^{w} \exp\left[2\pi i l k \frac{r}{q}\right] \exp[-i m_l \tau \Delta] \right|^2,$$
$$\Delta = \epsilon_1 - \epsilon_0, \tag{6}$$

where Δ is the qubit energy splitting and m_l is the number of qubits in the logical state $|1\rangle$ for the number state $|lr+s\rangle_W$. A global factor $\exp[-iL\varepsilon_0\tau]$ has been neglected. Obviously, when the *total* effective delay time $\tau(\tau=\tau_1^+ + \tau_2^+ + \tau_3^+)$ satisfies the phase-matching condition

$$\tau\Delta = (\epsilon_1 - \epsilon_0)\tau = 2n\pi, \quad n = 1,2,3,\ldots, \tag{7}$$

the above probability distribution $P(k)$ equals that of an ideal computation process with $\tau\Delta = 0$, as m_l is always an integer number. This implies that *the interference due to the fast evolution of the dynamical phases can be suppressed periodically* so that the correct results are obtained at the delay points indicated in Eq. (7).

Physically, this phase-matching condition is related to the transformation of the wave function from the interaction to the Schrödinger pictures. Theoretical derivations (see, e.g., [17]) for realizing quantum computation are usually in the interaction picture, in which the Hamiltonian for the qubit free evolution does not appear and the oscillation of the superposed wave function does not exist. More specifically, if a system Hamiltonian $\hat{H}$ can be written as a sum of a free oscillator part and an interaction part $\hat{H} = \hat{H}_0 + \hat{V}$, so that the time-dependent Schrödinger equation can be written as (in the so-called Schrödinger picture where operators are time independent while states evolve with time)

$$i\hbar \frac{\partial}{\partial t} |\psi_S(t)\rangle = (\hat{H}_0 + \hat{V}) |\psi_S(t)\rangle,$$

one can introduce the interaction picture wave function $|\psi_S(t)\rangle = \exp(-i\hat{H}_0 t/\hbar)|\psi_I(t)\rangle$, which satisfies

$$i\hbar \frac{\partial}{\partial t} |\psi_I(t)\rangle = \hat{V}_I |\psi_I(t)\rangle,$$

where $\hat{V}_I = \exp(i\hat{H}_0 t/\hbar)\hat{V}\exp(-i\hat{H}_0 t/\hbar)$. Now that $\hat{H}_0$ has been eliminated from the Schrödinger equation, it seems that dynamical phases due to the qubit free evolution would have no effect. However, at the end of a calculation, physical measurements have to be performed to read out the computational results, and these measurements are generally performed in the laboratory frame (the Schrödinger picture), in which the dynamical phases reappear. More specifically, the measurement of an observable $\hat{O}$ can be expressed as $\langle\psi_S(t)|\hat{O}|\psi_S(t)\rangle = \langle\psi_I(t)|\exp(i\hat{H}_0 t/\hbar)\hat{O}\exp(-i\hat{H}_0 t/\hbar)|\psi_I(t)\rangle = \langle\psi_I(t)|\hat{O}_I(t)|\psi_I(t)\rangle$. In other words, if we prefer calculating the expectation value of a time-independent operator, it has to be done in the Schrödinger picture. If $|\psi_I(\tau)\rangle = \Sigma_j \alpha_j |j\rangle$ is the desired final state, the Schrödinger picture final state would take the form

$$|\psi_S(\tau)\rangle = \sum_j \alpha_j e^{-iE_j\tau}|j\rangle = \sum_j \alpha_j e^{-im_l\tau\Delta}|j\rangle. \tag{8}$$

Therefore, the phase-matching condition (7) would render the phases $\exp[-im_l\tau\Delta] = 1$, so that it enforces the equivalence of the interaction picture and Schrödinger picture states, which ensures that the coherent error arising from the free evolution during the delay can be effectively eliminated.

In what follows, we illustrate our discussion with a few instances of Shor's algorithm.

B. Analytical example for factoring a small composite number

Let us first consider the factorization of the smallest composite number 4, which uses a two-qubit work register, a two-qubit auxiliary register, and $a=3$. After going through the four steps of Shor's algorithm as discussed above, the final work register state [Eq. (4)] is

$$|\psi(\tau+\tau_4)\rangle_W = \frac{1}{\sqrt{2}}\left\{\frac{1}{\sqrt{2}}(|0_1\rangle_W + e^{-i\tau_4\Delta}|1_1\rangle_W) \otimes \frac{1}{\sqrt{2}}[\zeta|0_0\rangle_W + \xi e^{-i\tau_4\Delta}|1_0\rangle_W]\right\}$$
$$= \frac{1}{\sqrt{8}}[\zeta|0\rangle_W + \xi|1\rangle_W + e^{-i\tau_4\Delta}\zeta|2\rangle_W + e^{-i\tau_4\Delta}\xi|3\rangle_W], \tag{9}$$

with $\zeta = 1 + e^{-i\tau\Delta}$ and $\xi = 1 - e^{-i\tau\Delta}$. Here, $|\alpha_k\rangle_W$ refers to the logical states (with $\alpha = 0,1$) of the kth (with $k=0,1$) qubit in the work register. In the other hand, $|0\rangle_W = |0_1 0_0\rangle_W$, $|1\rangle_W = |0_1 1_0\rangle$, $|2\rangle_W = |1_1 0_0\rangle$, and $|3\rangle_W = |1_1 1_0\rangle_W$.

To derive Eq. (9), the measurement on the auxiliary register is the projection $\hat{P}_A = |1\rangle_A\langle 1|_A$. Measuring the work register in the computational basis, the state (9) collapses to the expected one: either $|0\rangle_W$ or $|2\rangle_W$, with probability $p_e = |\zeta|^2 = [1+\cos(\tau\Delta)]/4$. This implies that the desired results ($p_e = 1/2$) are obtained only if the phase-matching condition (7) is satisfied. Equation (9) also shows that the dynamical phase acquired by each qubit after the Fourier transform does not result in any measurable physical effect.

C. Numerical examples for factoring a few integers

To quantitatively evaluate the effects of the dynamical phases when running Shor's algorithm, we introduce two

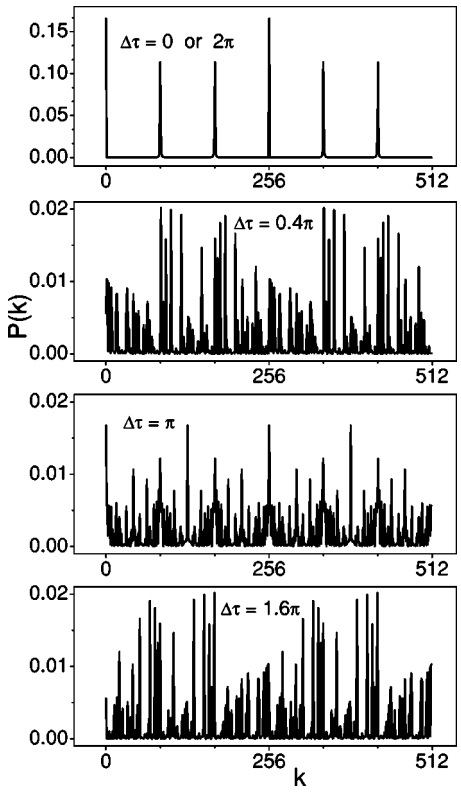

FIG. 2. The probability $P(k)$ [see Eq. (6)] of observing values of k for different values of $\tau\Delta=(\epsilon_1-\epsilon_0)\tau=0$, 0.4π, π, 1.6π, and 2π, given $N=21$, $q=512$, $a=5$, and the expected order $r=6$. Here, τ is the total effective delay time between unitary operations. The correct outputs are obtained when the phase-matching condition $\tau\Delta=2\pi$ (or the ideal case $\tau\Delta=0$) is satisfied. The probabilities of obtaining the correct outputs far from the phase-matching conditions are very low. (See the second, third, and fourth panels. Note the different scales for the vertical axes.) Indeed, as shown in the bottom three panels, many incorrect results are produced when the phase-matching condition given by Eq. (7) is not enforced.

delay-dependent functions: $p_e(k_e)$ is used to quantify the probability of obtaining the correct result k_e and

$$P_e=\sum_{k_e} p_e(k_e) \tag{10}$$

is the probability of computing all the correct outputs. $P_e=1$ for an ideal computation process and for practical quantum computers at the phase-matching time intervals consistent with Eq. (7). For other delays not satisfying Eq. (7) wrong results ($k\neq k_e$) can be obtained so that $P_e<1$.

We now run the algorithm to factorize $N=21$ with $a=5$ using nine work qubits. Figure 2 shows the various outputs and the corresponding probabilities for different delay times τ: $\tau\Delta=0$, 0.4π, π, 1.6π, and 2π. It is seen from Fig. 2 that, when the phase-matching condition (7) is satisfied, the computed results are identical to that of an ideal computation process with $\tau\Delta=0$. Note in Fig. 2 that the maximum value of $P(k)\approx 0.2$ at the matching condition and $P(k)<0.02$ away from it.

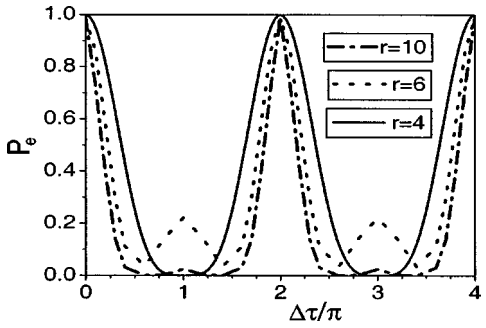

FIG. 3. The probability P_e of obtaining the correct results versus $\Delta\tau=(\epsilon_1-\epsilon_0)\tau$ for running Shor's factoring algorithm in the presence of delays. The lines for $r=4$, 6, 10 correspond to the cases where 4, 9, 11 work qubits, given $q=16$, 512, 2048, are used to factorize $N=15$, 21, 33 with $a=13$, 5, 5, respectively. Note that the expected outputs can be obtained at the phase-matching points: $\Delta\tau=2\pi, 4\pi$.

We plot the delay-dependent P_e in Fig. 3 for several examples: factorizing $N=15$, 21, and 33, with $a=13$, 5, and 5, and when using 4, 9, and 11 work qubits, respectively. As is shown in Fig. 3, the correct results are always obtained at the phase-matching time intervals given by Eq. (7). For other delay cases, especially near the delay points satisfying the condition $\tau\Delta=(\epsilon_1-\epsilon_0)\tau=(2n-1)\pi$, the correct results cannot be obtained (for the case where the expected order is a power of two; see, e.g., the solid line for $r=4$ in Fig. 3) or may be obtained with very low probabilities P_e (for the cases where the order r cannot divide the given q exactly; see, e.g., the lines for $r=6$, 10 in Fig. 3). Of course, the dynamical oscillations can also be suppressed by trivially setting up individual delays τ_m as $\tau\Delta_m=2n\pi$. The key observation here is that *only the total delay time*, instead of the duration for every delay, *needs to be accurately chosen to avoid the coherent dynamical phase error*.

Classically, higher precision is usually obtained by using more computational bits. However, this is not necessarily the case in practical quantum computation. Indeed, for Shor's algorithm, after taking into consideration the influence of the time delays between consecutive operations, the more qubits are used, the *lower* the computational efficiency. For example, if we use a work register with four qubits to factor 15, a desired final state—e.g., $|0000\rangle$—is obtained with the probability

$$p_e^{(4)}(0)=\frac{1}{2^4}[6+8\cos(\tau\Delta)+2\cos(2\tau\Delta)]. \tag{11}$$

If the delays are set as $\tau\Delta=5\pi/3$ [rather than the phase-matching points (7)], we have $p_e^{(4)}(0)=9/2^4$. With a five-qubit work register, the probability of obtaining one of the expected results (e.g., $|00000\rangle$) is

$$p_e^{(5)}(0)=\frac{1}{2^5}[20+30\cos(\tau\Delta)+12\cos(2\tau\Delta)+2\cos(3\tau\Delta)], \tag{12}$$

which reduces to $p_e^{(5)}(0)=27/2^5$ $[<p_e^{(4)}(0)]$ for the same delay of $\tau\Delta=5\pi/3$. This feature is clearly demonstrated in Fig.

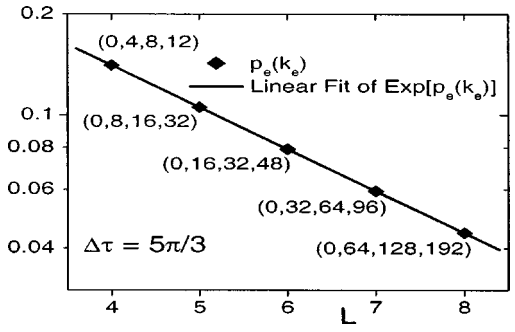

FIG. 4. The probability $p_e^{(L)}(k_e)$ of obtaining one of the correct results versus the number L of work qubits used to run the quantum algorithm factorizing $N=15$ in the presence of a delay $\Delta\tau=(\epsilon_1-\epsilon_0)\tau=5\pi/3$. The straight line shows that this probability $p_e^{(L)}(k_e)$ decreases exponentially with the number L of qubits used. The points on the line show the probability of obtaining one of the correct outputs $k_e=(0,4,8,12)$ for four-qubit, (0, 8, 16, 24) for five-qubit, (0, 16, 32, 48) for six-qubit, (0, 32, 64, 96) for seven-qubit, and (0, 64, 128, 192) for eight-qubit cases, respectively.

4, which shows that *the probability of obtaining any one of the correct results decreases exponentially when increasing the number of qubits of the work register*. Such a scenario is to be expected, since the number of possible outputs in the final measurement increases exponentially with the number of the work register qubits, which makes the constructive interference in Eq. (5) for the probability $P(k)$ harder to achieve if $\tau\Delta$ deviates from the phase-matching condition (7). At the exact points when $(\epsilon_1-\epsilon_0)\tau=2n\pi$, the constructive interference of the superposition wave functions ensures that the computational accuracy is independent of the number of qubits involved.

D. Effect of energy splitting inhomogeneity

In the previous calculations shown above, we have assumed that all qubits possess an identical energy splitting $\Delta=\epsilon_1-\epsilon_0$. In reality, especially for solid-state quantum systems such as the Josephson junction qubits and quantum dot trapped spins, different qubits will have slightly *different* energy splittings due to system inhomogeneity, in contrast to ions, which are perfectly identical. The logical states with the same energy in the "identical qubit" assumption (e.g., $|1_30_20_10_0\rangle$ and $|0_30_20_11_0\rangle$) may now have slightly different energies. A critical question then is how robust the phase-matching condition (7) is for a system of multiple qubits with fluctuations in the qubit energy splittings. Here we provide quantitative answers to this important question by numerically simulating Shor's algorithm assuming a Gaussian distribution for the qubit energy splittings. In other words, the energy splitting Δ_j of the jth qubit is chosen randomly according to the distribution function

$$P(\Delta_j)=\frac{1}{\sqrt{2\pi}\sigma}\exp\left[-\frac{(\Delta_j-\langle\Delta\rangle)^2}{2\sigma^2}\right] \tag{13}$$

around an average value $\langle\Delta\rangle$ and width σ. Thus, near the delay condition set at $\langle\Delta\rangle\tau=2\pi$, we have

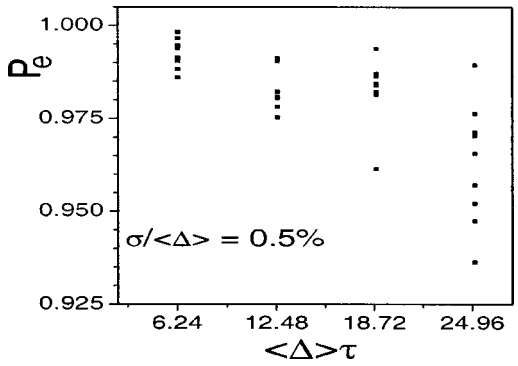

FIG. 5. The probabilities P_e (for factorizing $N=15$ using eight work qubits) of obtaining the correct results for different phase-matching cases: $\langle\Delta\rangle\tau=2\pi$, 4π, 6π, 8π, with a common Gaussian energy splitting fluctuation with $\sigma/\langle\Delta\rangle=0.5\%$. Note that this probability P_e is higher at the phase-matching points with shorter total delay time τ.

$$P(k)=\frac{1}{q(w+1)}\left|\sum_{l=0}^{w}\exp\left[2\pi ilk\frac{r}{q}\right]\exp[-im_l\tau(\langle\Delta\rangle+\delta)]\right|^2$$
$$\simeq\frac{1}{q(w+1)}\left|\sum_{l=0}^{w}\exp\left[2\pi ilk\frac{r}{q}\right]\left(1-im_l\frac{\delta}{\langle\Delta\rangle}\tau\right)\right|^2. \tag{14}$$

This fluctuation results in a small deviation of the probability near the phase-matching points. Figure 5 shows that the probability of obtaining correct answers decreases as the total time delay τ increases. Also, Fig. 6 shows the dependence of P_e on the width of the qubit energy splitting distribution σ, with the delay condition set at $\langle\Delta\rangle\tau=2\pi$. As expected, a quantum computer runs with higher efficiencies for shorter time delays τ and for narrower distributions $P(\Delta_j)$ of energy splittings. In essence, here we study an effect similar to inhomogeneous broadening, which is not a true dephasing effect. This is consistent with our focus in this paper on the coherent errors instead of the incoherent ones.

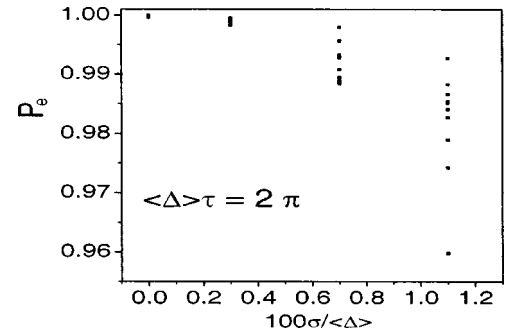

FIG. 6. The probabilities P_e (for factorizing $N=15$ using eight work qubits) of obtaining the correct results for different fluctuations of energy splittings: $\sigma/\langle\Delta\rangle=0.01\%$, 0.3%, 0.7%, 1.1%, with a common phase-matching point: $\langle\Delta\rangle\tau=2\pi$. Note that the probability at the phase-matching point is still sufficiently high, even if the energy splittings of the qubits exist with certain fluctuations around the average value $\langle\Delta\rangle$.

IV. CONCLUSIONS AND DISCUSSIONS

When a real quantum computer performs a computational task, there must be unavoidable time intervals between consecutive unitary operations. During these delays, the wave function of a system with nonzero free Hamiltonian would acquire relative dynamical phases, if the two states for each qubit have different energies. These dynamical phases lead to fast oscillations in the total wave function and modify the desired quantum interference required by quantum algorithms, which in turn reduce the probability of obtaining correct computational results.

Here we have studied the effects of the dynamical phases in running a quantum algorithm (more specifically, Shor's factoring algorithm). We point out that a phase-matching condition can potentially help allieviate the interference problems caused by the dynamical phases, and this condition is closely related to establishing the equivalence between quantum states in the Schrödinger picture and the interaction picture through a quantum computation process. In the presence of coherent phase errors, we have demonstrated that the probability of obtaining the correct answer decreases exponentially with increasing number of qubits of the work register. In addition, Shor's algorithm fails for the worst case scenario of $\tau\Delta=(2n-1)\pi$ if the expected order r is a power of 2. We have further shown that the phase-matching condition studied here is quite robust in the presence of small fluctuations in the qubit energy splittings. Unlike the refocusing technique in NMR experiments [3], which deals with unwanted evolutions due to uncontrolled qubit interaction, we have shown here that by properly setting the *total* effective delay, the unwanted oscillations of the superposed wave functions due to the free Hamiltonians of the bare qubits can be effectively suppressed; thus, the desired output can be obtained without additional operations. This implies that the quantum computing may be performed in an effective interaction picture, in which coherent errors arising from the free evolution of the bare qubits during the operational delay can be automatically avoided.

We emphasize that the present simplified approach only treats the delays between two sequential functional operations and neglects those inside these transforms. In fact, each functional transform, which is actually equivalent to a multiqubit gate, can be, in principle, implemented exactly by using only one-time evolution [15,16]. This "coarse-grained" one-step implementation implies that the evolutions relating to the various parts of the total Hamiltonian have been well controlled. Therefore, the operational delays, relating only to the free evolution ruled by the free Hamiltonian of the bare physical qubits, within each one of these larger functional building blocks are assumed to be zero. Also, the dynamical phases acquired by the superposed wave functions can be added up for the operational delays before and after each functional transformation. Therefore, the phase-matching condition (7) exists for the *total* delay.

The present calculation is done assuming that Shor's algorithm is accomplished in five lumped steps. A simple analysis can prove that, even if using an actual elementary gate array model—e.g., shown in Fig. 7 (for implementing the initializations by using the Hadamard gates and the quantum Fourier transformation)—the proposed phase-matching conditions (in terms of the total delay time instead of individual delay times of each operational delay) for avoiding the coherent phase errors are still valid. The key is that only two elementary nondiagonal operations (i.e., $\hat{R}_x$ in Hadamard gates) are applied to each qubit in the work register (see Fig. 7). The qubit is in a product state before the first nondiagonal $\hat{R}_x$ gate, while the delays after the second nondiagonal $\hat{R}_x$ in the corresponding Hadamard gate do not affect the results of projective measurement [see, e.g., Eq. (9)]. Therefore, the dynamical phases acquired in different effective operational delays accumulate even when the operational delays inside the functional steps are considered.

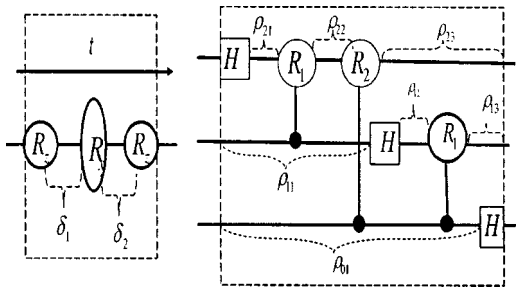

FIG. 7. Quantum circuits formed by the elementary single- and two-qubit logic gates for performing (a) Hadamard gate for one qubit and (b) a quantum Fourier transformation for three-qubit. Here, $\delta_l(l=1,2,\ldots)$ and ρ_{kl} $(k=0,1,2,\ldots)$ refer to the operational delays inside them, respectively. In the logical basis, the single-qubit gate $\hat{R}_z=\exp(i\pi\sigma_z/4)$ and the two-qubit controlled-phase gate $R_k=|00\rangle\langle 00|+|01\rangle\langle 01|+|10\rangle\langle 10|+\exp(2i\pi/2^k)|11\rangle\langle 11|$ are diagonal, while the single-qubit $\hat{R}_x=\exp(i\pi\sigma_x/4)$ is not.

In the present approach, we have assumed that every qubit in the work register has the same waiting time τ_j^+ for each effective operational delay. In practice, this assumption is not necessary. Indeed, in the elementary gate array model, the waiting times for different qubits would have been different. However, the phase-matching condition (7) needs only a slight modification in this case, so that it becomes a condition for each qubit [14]: $\tau_k\Delta_k=2n_k\pi$, $k=1,2,\ldots$, $n_k=1,2,\ldots$ for each qubit. Here, Δ_k and τ_k are the energy splitting and *total* controllable effective delay of the kth qubit in the work register, respectively.

Our discussion has assumed that all operations in the algorithm act on the pure quantum states of the two registers. In fact, in the framework of the phase estimation algorithm, Shor's algorithm can also be efficiently achieved with just one initial pure control qubit and a supply of initial mixed $\log_2 N$ qubits [18,19]. Correspondingly, numerical simulations in Ref. [20] showed that the algorithm is still efficient enough if the random incoherence noise is only allowed to act on the mixed qubits. However, an exponential drop-off in the efficiency of the algorithm was found, if the incoherence noise is allowed to act on the pure state of the control qubit. The above discussion, on the effect of dynamical phases, can also be applied to this implementation. An oscillating factor related to the operational delay of the control qubit can also be introduced to describe the relevant dynamical phase effect.

Finally, let us emphasize the differences between coherent errors due to dynamical phases, considered in this study, and incoherent errors due to qubit decoherence. The way a quantum algorithm is influenced by incoherent errors is very different from that by the coherent errors we discussed above. In short, coherent errors do not cause information loss, so that there can be a "revival" of the information when correct computational results can be obtained again after a period of time. Our analytical results, Eqs. (6) and (9), as well as the numerical simulations, Figs. 2 and 3, clearly show that the success probability, after one run of a quantum algorithm, oscillates with the dynamical phase $\tau\Delta$. On the other hand, decoherence leads to a decrease of the success probability of computing by a decohering factor—e.g., an exponentially decreasing factor of $\exp(-L^2t/\tau_d)$ for the fastest decoherence of an L-qubit system [21]. Here, τ_d and t are the decoherence time of a single qubit and the computation time, respectively. In other words, the incoherent errors due to decoherence lead to irreversible loss of information and have to be fixed by quantum error correction and/or decoherence-free encoding [22]. Phenomenologically [23], the systematic unitary errors due to dynamical phases accumulate in the same manner in deviating from the required quantum operations. These coherent errors may modify the required quantum interference, but they do not destroy the coherence of the quantum register [12]. Meanwhile, decoherence is intrinsically random and therefore leads to a slower but irreversible growth of incoherent errors with increasing computing time. Overcoming one type of error is not enough to guarantee the successful running of quantum algorithms. Indeed, the results presented in this paper demonstrate that, even in the absence of decoherence, the dynamical phases of the qubits still have to be taken into consideration in order to successfully implement Shor's algorithm.

ACKNOWLEDGMENTS

This work was supported in part by the National Security Agency (NSA) and Advanced Research and Development Activity (ARDA) under Air Force Office of Research (AFOSR) Contract No. F49620-02-1-0334 and by National Science Foundation Grant No. EIA-0130383.

[1] See, e.g., M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, (Cambridge University Press, Cambridge, England, 2000); C. H. Bennett and D. P. DiVincenzo, Nature (London) **44**, 247 (2000); A. Ekert and R. Josza, Rev. Mod. Phys. **68**, 733 (1996); A. M. Steane, Rep. Prog. Phys. **61**, 117 (1998).

[2] P. Shor, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, edited by Shafi Goldwasser (IEEE Computer Society Press, New York, 1994), p. 124.

[3] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, R. Cleve, and I. L. Chuang, Nature (London) **414**, 883 (2001); Phys. Rev. Lett. **85**, 5452 (2000).

[4] M. Mussinger, A. Delgado, and G. Alber, New J. Phys. **2**, 191 (2000).

[5] P. W. Shor, Phys. Rev. A **52**, R2493 (1995); A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).

[6] C. Miquel, J. P. Paz, and R. Perazzo, Phys. Rev. A **54**, 2605 (1996); E. Knill, R. Laflamme, and W. H. Zurek, Science **279**, 342 (1998); M. B. Plenio and P. L. Knight, Phys. Rev. A **53**, 2986 (1996).

[7] See, e.g., D. A. Lidar, I. L. Chuang, and K. B. Whaley, Phys. Rev. Lett. **81**, 2594 (1998); P. Zanardi and M. Rasetti, *ibid.* **79**, 3306 (1997).

[8] G. L. Long, Y. S. Li, W. L. Zhang, and C. C. Tu, Phys. Rev. A **61**, 042305 (2000); J. Chin. Chem. Soc. (Taipei) **48**, 449 (2001); X. Hu and S. Das Sarma, Phys. Rev. A **66**, 012312 (2002).

[9] M. B. Plenio and P. L. Knight, Proc. R. Soc. London, Ser. A **453**, 2017 (1997).

[10] Y. Makhlin, G. Schön, and A. Shnirman, Nature (London) **398**, 305 (1999).

[11] M. Feng, Phys. Rev. A **63**, 052308 (2001).

[12] G. P. Berman, G. D. Doolen, and V. I. Tsifrinovish, Phys. Rev. Lett. **84**, 1615 (2000).

[13] N. A. Gershenfeld and I. L. Chuang, Science **275**, 350 (1997); D. G. Cory, A. F. Fahmy, and T. F. Havel, Proc. Natl. Acad. Sci. U.S.A. **94**, 1634 (1997).

[14] L. F. Wei and F. Nori, J. Phys. A **37**, 4607 (2004).

[15] L. F. Wei and F. Nori, Europhys. Lett. **65**, 1 (2004); , Phys. Lett. A **320**, 131 (2003).

[16] A. O. Niskanen, J. J. Vartiainen, and M. M. Salomaa, Phys. Rev. Lett. **90**, 197901 (2003); X. Wang, A. Sørensen, and K. Mølmer, *ibid.* **86**, 3907 (2001); J. F. Du, M. J. Shi, J. H. Wu, X. Y. Zhou, and R. D. Han, Phys. Rev. A **63**, 042302 (2001); F. Yamaguchi, C. P. Master, and Y. Yamamoto, e-print quant-ph/0005128.

[17] J. I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995); L. F. Wei, S. Y. Liu, and X. L. Lei, Phys. Rev. A **65**, 062316 (2002); T. Sleator and H. Weinfurter, Phys. Rev. Lett. **74**, 4087 (1995).

[18] M. B. Plenio and P. L. Knight, Phys. Rev. A **53**, 2986 (1996); S. Schneider and G. J. Milburn, *ibid.* **59**, 3766 (1999); **57**, 3748 (1998).

[19] S. Parker and M. B. Plenio, Phys. Rev. Lett. **85**, 3049 (2000).

[20] S. Parker and M. B. Plenio, J. Mod. Opt. **49**, 1325 (2002).

[21] C. P. Sun, H. Zhan, and X. F. Liu, Phys. Rev. A **58**, 1810 (1998); G. M. Palma, K. A. Suominen, and A. K. Ekert, Proc. R. Soc. London, Ser. A **452**, 567 (1996).

[22] See, e.g., C. D'Helon and G. J. Milburn, Phys. Rev. A **56**, 640 (1997).

[23] See, e.g., G. Benenti, G. Casati, and G. Strini, *Principles of Quantum Computation and Information* (World Scientific, Singapore, 2004), Vol. I, Chap. 3.