Parallel quantum computing in a single ensemble quantum computer

Gui Lu Long[1,2,3,4] and L. Xiao[1,2]
[1]*Department of Physics, Tsinghua University, Beijing 100084, China*
[2]*Key Laboratory For Quantum Information and Measurements, Beijing 100084,China*
[3]*Center for Atomic and Molecular Nanosciences, Tsinghua University, Beijing 100084, China*
[4]*Center for Quantum Information, Tsinghua University, Beijing 100084, China*
(Received 26 September 2002; published 6 May 2004)

We propose a parallel quantum computing mode for ensemble quantum computer. In this mode, some qubits are in pure states while other qubits are in mixed states. It enables a single ensemble quantum computer to perform "single-instruction-multidata" type of parallel computation. Parallel quantum computing can provide additional speedup in Grover's algorithm and Shor's algorithm. In addition, it also makes a fuller use of qubit resources in an ensemble quantum computer. As a result, some qubits discarded in the preparation of an effective pure state in the Schulman-Varizani and the Cleve-DiVincenzo algorithms can be reutilized.

DOI: 10.1103/PhysRevA.69.052303 PACS number(s): 03.67.Lx, 03.67.Hk, 89.70.+c

I. INTRODUCTION

Quantum computer realization schemes can be classified into single-quantum-computer type where only a single quantum system is used, e.g., the trap ion [1], and ensemble-quantum-computer (EQC) type such as the liquid nuclear magnetic rosonance (NMR) scheme [2,3] and the solid-state scheme [4], where many copies of quantum systems are used. A quantum computer uses superposition of states and possesses quantum parallelism which provides enormous computing power. It achieves exponential speedup over existing classical computing algorithms in prime factorization [5] and simulating quantum systems [6]. However for some problems the speedup is not exponential. For instance, Grover's algorithm [7], shown optimal [8], achieves square-root speedup for unsorted database search. In some other problems, quantum computer cannot achieve any speedup [9]. It is natural to explore additional speedup by making quantum computers work in parallel, as in classical computation. By running many identical quantum computers in parallel, an unsorted database search can be speeded up greatly [10,11]. Using Liouville space computation [12], exponentially fast search can be achieved [13,14]. The speedup is achieved by using more resources. EQC is a potential place to exploit this parallelism because there are many molecules in it. Each molecule is potentially a single quantum computer, and an EQC is potentially a collection of that number of quantum computers. At present, an EQC is used as a single quantum computer using effective pure state technique [2,3], apart from the lack of projective measurement. Though preparing effective pure state is tedious, Cleve and DiVincenzo [15], Schulman and Vazirani [16] have proposed efficient algorithms to produce a portion of qubits in a pure state and discard some qubits in the completely mixed states.

In this paper, we introduce the idea of parallel quantum computing (PQC) in a single EQC. In the PQC a subset of qubits is prepared in pure state while the other qubits in mixed state. On one hand, this enables the "single-instruction-multidata" type of parallel computation in a single EQC for additional speedup, for example, for the Grover and the Shor algorithms. On the other hand, the PQC uses qubits in mixed state and makes a full use of the qubit resources. For instance, those qubits discarded in the Cleve-DiVincenzo [15] and the Schulman-Vazirani [16] algorithms can now be reused. The PQC is the classical parallel operation of many single quantum computers.

II. LIOUVILLE SPACE ENSEMBLE COMPUTING

In 1998, Mádi, Brüswchweiler, and Ernst proposed the Liouville space computer in which quantum operations and classical algorithm are combined [12]. The parallel quantum computing mode we proposed here is a generalization of the Liouville space computation. We briefly review the Liouville space computation in this section. In a NMR ensemble system, the state can be represented by density operators which are linear combinations of direct products of spin-polarization operators [17,12]. In a strong external magnetic field, the eigenstates of the Zeeman Hamiltonian,

$$|\phi_{in}\rangle = |001\cdots 01\rangle = |\alpha\alpha\beta\cdots\alpha\beta\rangle, \tag{1}$$

are mapped on states in the spin Liouville space,

$$\sigma_{in} = |\phi\rangle\langle\phi| = I_1^{\alpha} I_2^{\alpha} I_3^{\beta} \cdots I_{n-1}^{\alpha} I_n^{\beta}, \tag{2}$$

where

$$I_k^{\alpha} = |\alpha^k\rangle\langle\alpha^k| = \frac{1}{2}(\mathbf{1}_k + 2I_{kz}) = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \tag{3}$$

$$I_k^{\beta} = |\beta^k\rangle\langle\beta^k| = \frac{1}{2}(\mathbf{1}_k - 2I_{kz}) = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \tag{4}$$

represent, respectively, the spin-up and spin-down state of the spin. A Liouville space computation is performed by using a mixed state, which is a linear combination of the basis states in Eq. (2),

$$\rho = \sum_{j=1}^{M} \sigma_j, \tag{5}$$

where M gives a restriction for the range of basis states to be included.

The Brüswchweiler algorithm [13] is a Liouville space computing algorithm. Like the Grover algorithm, it finds a marked state in an unsorted database. Suppose the oracle is a computable function f. It has the following property: $f(x)=0$ for all x except $x=z$, and z is the item we want to find out for which $f(z)=1$. In Liouville space computation and the Brüswchweiler algorithm, an ancilla bit is used and its state is represented by I_0. The output of the oracle is stored on the ancilla bit I_0, whose state is prepared in the α state at the beginning. The output of f can be represented by an expectation value of I_{0z} for a pure state,

$$f = F(I_0^{\alpha}\sigma_{in}) = \frac{1}{2} - \mathrm{Tr}(U_f I_0^{\alpha}\sigma_{in}U_f^{+}I_{0z}). \tag{6}$$

If σ_{in} happens to satisfy the oracle, then I_0^{α} is changed to I_0^{β}. This gives the value of the trace equal to $-1/2$, and hence f equals to 1. The input of f can be a mixed state of the form $\rho=\Sigma_{j=1}^{N}\ I_0^{\alpha}\ \sigma_j$, where σ_j is one of the form in Eq. (2):

$$f = \sum_{j=1}^{N} F(I_0^{\alpha}\ \sigma_j) = F\left(\sum_{j=1}^{N} I_0^{\alpha}\ \sigma_j\right) + \frac{N-1}{2}. \tag{7}$$

The oracle is applied simultaneously to all the components in the NMR ensemble. The oracle operation is quantum mechanical. The essential feature of the Brüswchweiler algorithm is as follows: suppose that the unsorted database has $N=2^n$ number of items. We need n-qubit system to represent these 2^n items. The algorithm contains n oracle queries each followed by a measurement.

(1) Each time $I_0^{\alpha}I_k^{\alpha}$ $(k=1,2,...,n)$ is prepared. In fact, the input state $I_0^{\alpha}\cdots\mathbf{1}\cdots I_k^{\alpha}\cdots\mathbf{1}\cdots$ is a highly mixed state [12]. This Liouville operator actually represents the 2^{n-1} number of items encoded in mixed state:

$$\begin{aligned} I_0^{\alpha}I_k^{\alpha} &= I_0^{\alpha}(I_1^{\alpha}+I_1^{\beta})(I_2^{\alpha}+I_2^{\beta})\cdots(I_n^{\alpha}+I_n^{\beta}) \\ &= \sum_{\gamma_1,\gamma_2,...,\gamma_{k-1},\gamma_k,\gamma_{k+1},...,\gamma_n=\alpha,\beta} I_0^{\alpha}I_1^{\gamma_1}I_2^{\gamma_2}\cdots I_{k-1}^{\gamma_{k-1}}I_k^{\alpha}I_{k+1}^{\gamma_{k+1}}\cdots I_n^{\gamma_n} \\ &= \sum_{i_1,i_2,...,i_{k-1},i_{k+1},...,i_n=0,1} |i_1 i_2\cdots i_{k-1}0 i_{k+1}\cdots i_n\rangle \\ &\quad \times\langle i_1 i_2\cdots i_{k-1}0 i_{k+1}\cdots i_n|, \end{aligned} \tag{8}$$

where the identity operators have been omitted for clarity. This mixed state contains half the number of items in the database. The kth bit is set to α. The other half of the database with kth bit equal to β(or 1) is not included.

(2) Applying the oracle function to the system. As seen in Eq. (7), the operation is done simultaneously to all the basis states. If kth bit of the marked state is 0, then the marked state is contained in Eq. (8). One of the 2^n terms in Eq. (8) satisfies the oracle and the oracle changes the sign of the ancilla bit from α to β. If one measures the spin of ancilla spin after the function f, the value will be $f=(2^n-1)(1/2)+1/2-(2^n-2)(1/2)=1$. If the kth bit of the marked state is 1, then the state (8) will not contain the marked item. Upon the operation of the function f, there is no flip in the ancilla bit. A measurement on the ancilla bit's spin I_{0z} will yield $f=(1/2)(2^n-1)+1/2-(2^n)(1/2)=0$. However, without obtaining the value of f, we can know the marked state by measuring the ancilla bit's spin. If one measures the spin of ancilla spin after the oracle, the value will be $(2^{n-1}-1)(1/2)-1/2=N/4-1$ for the kth bit of the marked state being 0. If the kth bit of the marked state is 1, then the state (8) will not contain the marked item. Upon the operation of the oracle, there is no flip in the ancilla bit. A measurement on the ancilla bit's spin I_{0z} will yield $(1/2)(2^{n-1})=N/4$. Therefore by measuring the ancilla bit's spin, one actually reads out the kth bit of the marked state.

(3) By repeating the above procedure for k from 1 to n, one can find out each bit value of the marked state.

Brüswchweiler algorithms have been implemented in a 3-qubit NMR systems [18,19]. The Brüswchweiler algorithm has been applied to global optimization problem [20]. In fact, using the Liouville space computation, the unsorted database search algorithm can achieve its ultimate optimum, a single query. By putting all a NMR ensemble in a complete mixed state, a single query is sufficient to find all the marked items satisfying an oracle [14]. It has been demonstrated experimentally in a 7-qubit NMR system recently [21].

It is worth pointing the salient features of Liouville space computer. First, all the computational operations are quantum mechanical. The operations are exactly the same as those in quantum computer. Second, classical parallelism is introduced in Liouville space computing since different components may carry different computation tasks at the same time. Third, there is no quantum superposition of the basis states in Liouville space computation. Because of this, the Liouville space computer can be replaced by an ensemble of reversible computers, which can in principle be implemented by classical reversible Turing machines. In the parallel quantum computing proposed in this paper, we generalize the Liouville space computer to allow quantum superposition of the computational basis states to perform computation. We will see that the effective pure state quantum computation and the Liouville space computation can be viewed as two extremes of the parallel quantum computation.

III. PARALLEL QUANTUM COMPUTING

We introduce notations first. We call a term in a superposed state as a component, for instance $|\psi_0\rangle$ in $a|\psi_0\rangle+b|\psi_1\rangle$; a term in a density matrix a constituent, for instance, $|\psi_0\rangle\langle\psi_0|$ in $p_0|\psi_0\rangle\langle\psi_0|+p_1|\psi_1\rangle\langle\psi_1|+p_2|\psi_2\rangle\langle\psi_2|$. We can divide an n number qubits system into two parts, one with n_1 qubits and the other with n_2 qubits, and $n_1+n_2=n$. The state of this n-qubit system may be represented by $|j_1,j_2\rangle$, where $|j_1\rangle$ is the first n_1 qubit state and $|j_2\rangle$ is the latter n_2 qubits state. We can also combine the two parts to represent the state as $|j_{12}\rangle\equiv|j_1 j_2\rangle$. We use interchangeably binary and decimal representations. For instance, a 4-qubit state with $n_1=n_2=2$ can be represented as $|01,10\rangle=|0110\rangle=|1,2\rangle=|6\rangle$, where the first and third are in the separated binary and decimal forms,

whereas the second and fourth are in the combined binary and decimal forms, respectively.

We then describe the ensemble measurement which is a generalization of that used in Liouville space computation [12,18]. Assume that an EQC can detect the transition signal from a single molecule. For a molecule with $n+1$ qubits, one qubit is used as the ancilla qubit and is labeled 0. The Hamiltonian of the ancilla qubit is

$$H = \omega_0 I_{0z} + \sum_{k>0} 2\pi J_{0k} I_{0z} I_{kz}, \tag{9}$$

where J_{0k} is the J-coupling constant between the ancilla and the kth qubit. I_{jz} is the z component of the spin operator for the jth qubit. The transition frequency of the ancilla qubit depends on the state of the remaining n qubits. If the ancilla qubit transition occurs with n qubits in state $|i_1 i_2 \cdots i_n\rangle$, its transition frequency is then $\omega_0 + \Sigma_{k=1}^{n} \pi J_{0k}(-1)^{i_k}$. This transition produces a peak in the ancilla qubit spectrum. For instance, the n-qubit state $|i_1 i_2 \cdots i_n\rangle = |00\cdots 0\rangle$ corresponds to the highest frequency $\omega_0 + \Sigma_{k=1}^{n} \pi J_{0k}$, and the state $|i_1 i_2 \cdots i_n\rangle = |11\cdots 1\rangle$ corresponds to the lowest frequency $\omega_0 - \Sigma_{k=1}^{n} \pi J_{0k}$. Thus one can tell the state of the n qubits $|i_1 i_2 \cdots i_n\rangle$ by looking at this sign of the multiplet component. Moreover, the ancilla qubit state itself is represented by the spectral peak direction. If the ancilla qubit is in the $|0\rangle(|1\rangle)$ state before transition, then the spectral peak is upward (downward). The state in the PQC can be a superposition of basis states, say $\Sigma_{j_2=0}^{N_2-1} c_{j_1,j_2}|j_1,j_2\rangle$. In this state the first n_1 qubits are in $|j_1\rangle$ and the latter n_2 qubits are in superposed state of the n_2 register. When we measure the ancilla qubit, we will observe only one transition. The transition frequency is random in one of the frequencies corresponding to the n_2-qubit states in states $|0\rangle, \cdots, |N_2-1\rangle$, because the n-qubit state will collapse into one of N_2 basis states $|j_1,j_2\rangle = |j_1 j_2\rangle$ randomly with probability $|c_{j_1,j_2}|^2$. When the superposed state is transformed into a single basis state, the transition frequency will be definite and determined by Eq. (9). This ancilla qubit spectrum method will serve as the ensemble measurement throughout this paper. It can tell the ancilla qubit state by the peak direction and the n-qubit state by the transition frequency.

Our quantum computer model is an EQC with $N_1 = 2^{n_1}$ molecules. Each molecule can be operated and measured. It has $n+m+1$ qubits. They are divided into three parts: one ancilla qubit, a function register with m qubits, and an argument register with n qubits. The argument register is further divided into two parts: one part with n_1 qubits called n_1 register and another part with n_2 qubits called n_2 register, and $n = n_1 + n_2$. In general before a computation, the function register and ancilla qubit are prepared in the pure state $|0\rangle$. The argument register is in a mixed state with N_1 constituent. Each constituent is characterized by the state of the n_1 register. The n_2 register in a given constituent is in a superposed state of its $N_2 = 2^{n_2}$ basis states. The density operator of the ensemble is

$$\rho = \frac{1}{N_1} \sum_{j_1=0}^{N_1-1} \left[\sum_{j_2=0}^{N_2-1} c_{j_1,j_2} |0,j_1,j_2\rangle \right] \left[\sum_{j_2=0}^{N_2-1} c^*_{j_1,j_2} \langle 0,j_1,j_2| \right], \tag{10}$$

where in $|i,j_1,j_2\rangle$, i, j_1, and j_2 are the states for the function, the n_1 and the n_2 registers, respectively, and $\Sigma_{j_2=0}^{N_2-1} |c_{j_1,j_2}|^2 = 1$. The ancilla qubit state is not written out explicitly. In this EQC, there are N_1 constituents and N_1 molecules. Each molecule is in a different state, $\Sigma_{j_2=0}^{N_2-1} c_{j_1,j_2}|0,j_1,j_2\rangle$, which is a superposition of N_2 number of computational basis states. In general, a quantum computation performs unitary transformations on both the argument and the function registers. Denoting this transformation as U_c, the quantum computation on state (10) will be

$$\rho \to \rho_c = U_c \rho U_c^{-1} = \frac{1}{2^{n_1}} \sum_{j_1=0}^{N_1-1} \left[\sum_{j_2=0}^{N_2-1} c_{j_1,j_2} U_c |0,j_1,j_2\rangle \right] \times \left[\sum_{j_2=0}^{N_2-1} c^*_{j_1,j_2} \langle 0,j_1,j_2| U_c^\dagger \right]. \tag{11}$$

An ensemble measurement is then performed to read out the result.

The quantum computation represented in Eq. (11) on the ensemble (10) is defined as the parallel quantum computing. In fact it is N_1 quantum computers working in parallel. The computation instruction U_c is the same for all molecules, but the databases, numbers represented by different molecules, are different. Hence, the PQC is the single-instruction-multidata type of parallel computation in classical computation. The state (10) is the most general initial state, and in most applications the following simplified state is sufficient: the n_1 register in the complete mixed state $\Sigma_{j_1=0}^{N_1-1} (1/N_1)|j_1\rangle\langle j_1|$ and the n_2 register in the equally weighted superposed state $\Sigma_{j_2=0}^{N_2-1} \sqrt{1/N_2}|j_2\rangle$. In this case, $c_{j_1,j_2} = 1/\sqrt{N_2}$ for all possible j_1 and j_2.

IV. PARALLELIZING THE GROVER ALGORITHM AND THE SHOR ALGORITHM

Application of the PQC to the Grover algorithm is studied in this section. Suppose the marked state is $|j_1^0 j_2^0\rangle$. Then only one qubit is required for the function register in this algorithm. This qubit is also used as the ancilla qubit for the ensemble measurement. Preparing the function register in the $|0\rangle$ state, the n_2 register in the equally weighted superposed state, and the n_1 register in the complete mixed state, we have then

$$\rho = \frac{1}{N_1} \sum_{j_1=0}^{N_1-1} \left[\sqrt{\frac{1}{N_2}} \sum_{j_2=0}^{N_2-1} |0,j_1,j_2\rangle \right] \left[\sqrt{\frac{1}{N_2}} \sum_{j_2=0}^{N_2-1} \langle 0,j_1,j_2| \right]. \tag{12}$$

In this way, we divide the database into N_1 subdatabases, each with N_2 items. Apply a zero-failure rate Grover algorithm [22] to the ensemble with J iterations, where $J-1$ is the integer part of $[(\pi/2)-\beta]/(2\beta)$ and is approximately

$\pi\sqrt{N_2}/4$ and $\beta=\arcsin 1/\sqrt{N_2}$. In this modified Grover algorithm, each iteration consists of four steps: (1) apply the query to the whole n-qubit argument register and on condition that the query is satisfied, rotates the phase of the marked state through angle $\phi=2\arcsin[\sqrt{N_2}\sin\pi/(4J+6)]$ (ϕ is slightly smaller than π); (2) make a Hadmard transformation on the n_2 register; (3) make a phase rotation through angle ϕ on the $|0\cdots0\rangle$ basis state of the n_2 register; (4) make a Hadmard transformation on the n_2 register again. If a subdatabase does not contain the marked state, the above operation does not produce any observable effect. The constituent that contains the marked item has its n_1 register in state $|j_1^0\rangle$. The modified Grover algorithm transforms its n_2 register from the equally weighted superposed state into a single state $|j_2^0\rangle$ so that the constituent is in the marked state $|j_1^0 j_2^0\rangle$. At the end of the modified Grover algorithm, one makes a further query and on condition that the query is satisfied, makes a flip on the function register. The density matrix becomes

$$\rho_f=\left(\frac{1}{N_1}\right)|0\rangle\langle 0|\sum_{j_1\neq j_1^0}\left[\sum_{j_1=0}^{N_1-1}\sqrt{\frac{1}{N_2}}|j_1 j_2\rangle\right]\times\left[\sum_{j_1=0}^{N_1-1}\sqrt{\frac{1}{N_2}}\langle j_1 j_2|\right]+\left(\frac{1}{N_1}\right)|1\rangle\langle 1||j_1^0 j_2^0\rangle\langle j_1^0 j_2^0|.$$

Finally, by measuring the ancilla qubit, one obtains N_1 transition peaks in the spectrum, each from a constituent. For those constituents without the marked item, each peak is upward and its transition frequency is random in one of those corresponding states $|j_1 0\rangle$, …, $|j_1 N_2-1\rangle$. The constituent with the marked item is in a unique state and produces a downward peak with definite frequency corresponding to the state $|j_1^0 j_2^0\rangle$. It finds the marked state with certainty.

The number of queries is about $\pi\sqrt{N_2}/4=\pi\sqrt{N/N_1}/4$. This is only $1/\sqrt{N_1}$ of that a standard Grover algorithm requires. This is so because there are N_1 single quantum computers searching in parallel, each in a reduced database with only $N/N_1=N_2$ items. It requires $\pi\sqrt{N/N_1}/4$ steps for each single quantum computer to complete the search. In one extreme $n_1=0$, there is only a single molecule, the number of query is $\pi\sqrt{N}/4$, which is just that for the standard Grover algorithm. On the other extreme, if $n_1=n$, $n_2=0$, the EQC contains $N=2^n$ molecules in completely mixed state, only a single query is needed. This is just the Liouville space computing fetching the algorithm proposed recently [14]. In Liouville space computation [12], no superposition of the computational basis states is used. Each molecule can also be viewed as a reversible classical computer that can be realized quantum mechanically [23], or simply be implemented directly using classical Turing machine with three tapes [24]. If $n_1=n-1$ and $n_2=1$, the algorithm finds the marked item with just two queries. Clearly, the speedup is achieved at the expense of more molecules. The number of queries N_q and the number of molecules N_1 satisfy $N_q^2\times N_1=\text{const}$.

If we fix the number of molecules in an EQC, say at N_E, then in order that each constituent is occupied by at least one molecule, n_1 cannot be larger than $\log_2 N_E$, otherwise there will be constituents without any occupying molecules. We assume that the qubit number n is very large, $N_E\leqslant 2^n$. The maximum value for n_1 is $\log_2 N_E$. A natural estimate of the bound is to set $N_E=N_A$, the Avogadro constant. This sets to $n_1\leqslant 79$. In principle, we can vary n_1 from 0 to $\log_2 N_E$ so that the functioning of the EQC changes. When $n_1=0$, all N_E molecules are in the same pure state and the EQC works as a single quantum computer. Most NMR EQC quantum computation experiments done so far manage to get this effect using the effective pure state technique. When $n_1=1$, the ensemble is divided into two subensembles each with $N_E/2$ molecules. Each subensemble works as a single quantum computer. The whole ensemble works as two single quantum computers in parallel. When $n_1=\log_2 N_E$, the ensemble works as N_E single quantum computers working in parallel.

In the above discussion, a single molecule and an ensemble of many molecules in pure state are all treated as a single quantum computer. We point here that the EQC can do more by implementing the parallel operation proposed in Refs. [10,11]. In these works, the Grover algorithm is run on some k identical quantum computers in parallel. It is equivalent to repeating the algorithm in a single quantum computer k times. We call this parallel algorithm as repetition parallel algorithm (RPA). For instance, in Ref. [10], by running one iteration of Grover's algorithm on k number of identical quantum computers simultaneously and then measuring these quantum computers simultaneously, the marked state can be found by picking out the one most quantum computers point to. Because the marked state will appear $9k/N$ times in the outcome, whereas any other state appears k/N times. When $k=O(N\ln N)$, the probability that the marked state occurs more than any other state approaches unity. In Ref. [11], k identical quantum computers are searching in parallel. In each quantum computer, the probability for finding marked state is amplified. Because there are k quantum computers, by using the majority-vote rule, one needs less iterations on each quantum computer. The speedup scales as $O(\sqrt{k})$. The extent of speedup is the same as the PQC algorithm. But there are several differences between the PQC and the RPA:

(1) In the PQC, the database for each quantum computer is reduced from N to N/N_1, whereas in repetition parallelism, the database size is always N.

(2) In the PQC, some n_1 qubits are in mixed state, whereas in the RPA, all qubits are in pure states. This gives the PQC the advantage to make a fuller use of qubit resources as we will explain later.

(3) The PQC algorithm has full success rate whereas the RPA is probabilistic. To overcome fluctuation, it requires more resource than that in the PQC. For instance, for single query searching, the PQC algorithm requires N molecules whereas the algorithm in Ref. [10] requires $O(N\ln N)$ molecules.

Shor's algorithm can also be run in the PQC. The aim is to find the period r of a^x mod N_b. We need two registers, one argument register with n qubits where $N_b^2<2^n<2N_b^2$ and one function register with similar size. We divide the argument register into n_1 qubits in the complete mixed state, and n_2 qubits in pure state. The ensemble is prepared in state described by Eq. (12). We perform a^x mod N_b and store the

results in the function register. After performing Fourier transform on only the n_2 register, the states in the n_2 register becomes identical in all constituents. By measuring the n_2 register using an ancilla qubit, the period in the n_2 register N_2/r can be found. The speedup is achieved due to two factors. First, the Fourier transform is done on a smaller space in the n_2 register, and it requires only $O(n_2^2)$ steps as compared with $O(n^2)$ steps in standard Shor algorithm. Second, there are N_1 constituents, therefore there are N_1 transitions by a single ensemble measurements. In standard Shor algorithm, several runs of the algorithm are required. In the PQC, this can be reduced by a factor of $1/N_1$. We illustrate this in a simple example with $N_b=15$, $a=7$, $n=8$, $n_1=2$, $n_2=6$. Shor's algorithm in a single quantum computer yields the following state $|\psi\rangle=(|0\rangle+|64\rangle+|128\rangle+\cdots)(|1\rangle+|7\rangle+|4\rangle+|13\rangle)$, and the period in the argument register is $q/r=64$, where $q=256$. With the PQC, the resulting state is $\rho=[(|1\rangle+|7\rangle+|4\rangle+|13\rangle)][([00]+[01]+[10]+[11])|[(|0\rangle+|16\rangle+|32\rangle+|48\rangle)]$, where the square bracketed quantities denote the corresponding density operator, e.g., $[00]$ and $[(|1\rangle+|7\rangle+\cdots)]$. Upon measurement, four transitions from the n_2 register appear, and this is equivalent to running the algorithm with six qubits four times. But for the PQC operation of Shor's algorithm, there is a restriction on n_1: it should not be large, otherwise the Fourier transformation in n_2 qubits will not achieve the desired destructive interference.

V. IMPLEMENTATION WITH REALISTIC NMR ENSEMBLES AND THE NOTION OF A LOGICAL MOLECULE

In reality, some number, say N_E, of molecules has to be used as a logical molecule. A logical molecule can be viewed as the minimum number of molecules that acts as a single quantum computer. Then a molecule in the preceding discussion should be understood as a logical molecule. The number of logical molecules in an EQC is N_s/N_E, where N_s is the total number of molecules in the ensemble. In practice, a NMR EQC contains a large number of molecules, say 10^{16}. Though with effective pure state technique, the number of molecules contributing to quantum computation is reduced, there are still 10^{10}. This is much more than that needed for a logical molecule. Thus in ensemble quantum computation with effective pure state technique, it is possible to see the effect of repetition parallelism. Indeed, it has been pointed out that in ensemble quantum computation, unsorted database search can be faster than Grover algorithm [25] by trading space resources with time resources, a reflection of the repetition parallelism. In implementing the PQC, effective pure state technique can also be used to prepare the n_2+m+1 qubits in pure state.

A logical molecule is in fact a subensemble of molecules in the same pure state. Hence the difference between a single molecule and a logical molecule is essentially the difference between a single molecule and an ensemble of molecules in the same pure state. The minimum number of molecules required for a logical molecule depends on the measurement sensitivity. In the following, we explain the differences between a logical molecule and a single molecule in a measuring process, in an example with three qubits, one qubit as the ancilla qubit and the other two qubits as working qubits. Here the first qubit is the ancilla qubit.

(1) If the two working qubits are in a computational basis state $|0i_1i_2\rangle$, where i_1, i_2 are either 0 or 1, then there is only a single transition for the ancilla qubit, $|0\ i_1\ i_2\rangle\rightarrow|1\ i_1\ i_2\rangle$. In this circumstance, there is no difference between a single molecule and a logical molecule except that the intensity of the transition from the logical molecule is N_E times of that for a single molecule, where N_E is the number of molecules in a logical molecule.

(2) When the two working qubits are in a superposed state, for example, $|0\rangle(|01\rangle+|10\rangle)/\sqrt{2}$(the first ket $|0\rangle$ represents the state of the ancilla qubit), then there will be two transition possibilities for the ancilla qubit. One is from $|0\ 0\ 1\rangle$ to $|1\ 0\ 1\rangle$ with 50% probability and the other is from $|0\ 1\ 0\rangle$ to $|1\ 1\ 0\rangle$ also with 50% probability. For a single molecule, there will be only one transition, either the first or the second. For a logical molecule, both transitions will occur. Half of the molecules will experience transition $|0\ 0\ 1\rangle\rightarrow|1\ 0\ 1\rangle$ and the other half will go through transition $|0\ 1\ 0\rangle\rightarrow|1\ 1\ 0\rangle$. We should see two transitions, each with an intensity of $N_E/2$ times of that from a single molecule.

(3) When there are more components in the superposed state of the working qubits, say N_c, there will be N_c transition lines in the ancilla qubit spectrum with a reduced intensity, N_E/N_c times of that for a single molecule. Then the minimum number of molecules N_E for a logical molecule is to make N_E/N_c times of the transition from a single molecule detectable in experiments. In quantum algorithms, N_c is usually very small, for instance, it is equal to 1 in the Grover algorithm. Thus the minimum number of molecules in a logical molecule is only a multiple of the minimum number of molecules producing a detectable transition signal when each molecule makes the same transition.

(4) According to Ladd *et al.* [4], N_E is of the order of $O(10^5)$ for present-day technology. With the development of technology, this number could be further reduced. But it is important to note that this number is more or less a constant for quantum algorithms, for instance the Grover algorithm, and it scales more or less as a constant with the number of qubits in the molecule. For example, if the apparatus can detect the simultaneous transition of 10^5 molecules, then for Grover algorithm with three qubits we need 10^5 molecules as a logical molecule unit, and with ten qubits we need the same number of molecules as a logical molecule unit. As this number is more or less fixed, to utilize the benefit of the classical parallelism discussed in our paper, one can simply add more molecules in the ensemble as long as it is feasible in the experiment. A logical molecule is in fact a subensemble of molecules in the same pure state. Hence the difference between a single molecule and a logical molecule is essentially the difference between a single molecule and an ensemble of molecules in the same pure state, which has been discussed in the literatures. The minimum number of molecules required for a logical molecule depends on the measurement sensitivity.

(5) From this discussion, we see that as long as each component in an ensemble can be detected, there is no need

for the number of molecules in each component to be equal. This property makes the parallel quantum computing flexible in practical implementation.

VI. DISCUSSION AND SUMMARY

The PQC uses mixed state in general. One can take advantage of this to make a full use of the qubit resources in EQC. In the Cleve-DiVincenzo [15] and the Schulman-Vazirani [16] algorithms, $O(n)$ qubits are prepared in pure state while some qubits [$O(\sqrt{n})$ in Ref. [15] and $O(n)$ in Ref. [16]] have to be in the completely mixed state and be discarded. In the PQC, these qubits can be reused. This gives a natural criteria for dividing n into n_1 and n_2. We can use these discarded qubits as the n_1 register. This increases considerably the number of qubits usable in an EQC.

As is common to all NMR ensemble computing schemes, the effective pure state [2,3] ensemble quantum computing and the Liouville space computing [12], the PQC uses the free decay signals for the measurement, hence the PQC requires a sensitivity that is exponential in the number of qubits. The difference between the effective pure state ensemble-quantum-computing scheme and the Liouville space computing and the PQC in the aspect of measurement is that some transitions are suppressed in the effective pure state quantum computing, only one or a few spectral lines are retained, while in the Liouville space computing and the PQC nearly all transition lines are collected. To recognize the computing result, it is necessary to identify the frequency of the transition spectral lines. There are altogether 2^n number of transitions, hence it scales exponentially with the number of qubits n.

It is worth pointing that there are different interpretations of the density matrix for a mixed state. In this work and our previous work [14,18,26], we have used the ensemble average definition, which is called proper mixed state, by d'Espgnat [27]. In this interpretation, in a given instant, the state of a molecule in an ensemble is in a definite quantum state. But if we take an average over all the ensembles, an "average" molecule in the ensemble has a probability distribution in the set of pure states. We use this picture as an approximation to a NMR ensemble within a time period of the dephasing time T_2, i.e., within a period of time T_2, a molecule is approximately in a definite pure quantum state. Another interpretation of a mixed state is that a molecule in an ensemble is not in a definite pure quantum state at any given instant because of its entanglement with the environment. This interpretation has been used, for instance in Ref. [28]. When the number of molecules in an ensemble is small, these two different interpretations of mixed state can make a difference in the outcome for the PQC. In the first interpretation, because a molecule in an ensemble is in a definite quantum state, it remains in a definite quantum pure state during the process of computation. For example, if there are 2^n molecules in an ensemble and each molecule is in a different computational basis states $|i_1 i_2 \cdots i_n\rangle$, where n is the number of qubits in each molecule, then the ensemble is represented by density matrix proportional to a $2^n \times 2^n$ unit matrix. In each state, there is a molecule in that state. In the second interpretation, each molecule in an ensemble itself is not in a pure quantum state at a given instant. For instance, for an ensemble with 2^n molecules described by the same unit density matrix, at a given instant each molecule has $1/2^n$ probability to be in one of 2^n computational basis states. There is some probability that some computational state is not occupied by any molecules in the ensemble at some instant. However, when the number of molecules in the ensemble is much larger than 2^n, then it is certain that every computational basis state is occupied by some molecules. In this case, the two different interpretations of the mixed state leads to identical results. For realistic NMR ensemble, there are huge numbers of molecules in an ensemble, and the number of qubits is much small compared to this number. Hence the two different interpretations of a mixed state do not affect the parallel quantum computing mode we proposed. It is worth pointing that there are still different views about the interpretation of mixed state, and these are closely related to fundamental issues in quantum mechanics. For instance, the first postulate in quantum mechanics reads "the state of the particle is represented by a vector $|\psi(t)\rangle$ in a Hilbert space" [29]. Mixed state (or ensemble) is introduced in quite a number of textbooks, for instance, by Shankar [29] and Ka [30]. Whether a mixed state is only a mathematical tool for describing a quantum system with insufficient information or it is indeed a physical state, and how good a mixed state describes a NMR ensemble are interesting questions and need further attention. These issues need heavy involvement and we leave it to a separate publication.

ACKNOWLEDGMENTS

This work was supported by the National Fundamental Research Program Grant No. 001CB309308, China National Natural Science Foundation Grants Nos. 60073009, 10325521, the Hang-Tian Science Fund, and the SRFDP program of Education Ministry of China. Helpful discussions with Professor A. Zeilinger, Dr. J. W. Pan, Dr. C. Brukner, Dr. Ian Glendinning are gratefully acknowledged. We are also grateful to Professor William K. Wootters for helpful communications and comments.

[1] J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995).
[2] D. G. Cory, A. F. Fahmy, and T. F. Havel, Proc. Natl. Acad. Sci. U.S.A. **94**, 1634 (1997).
[3] N. A. Gershenfeld and I. L. Chuang, Science **275**, 350 (1997).
[4] T. D. Ladd *et al.*, Phys. Rev. Lett. **89**, 017901 (2002).
[5] Peter W. Shor, in *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science* (IEEE, New York, 1994), pp. 124–134.

[6] S. Lloyd, Science **273**, 1073 (1996).
[7] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[8] M. Boyer, G. Brassard, P. Hoyer, and A. Tapp, Fortschr. Phys. **46**, 493 (1998).
[9] DiVincenzo and D. Loss, J. Magn. Magn. Mater. **200**, 202 (1999), and references therein.
[10] L. K. Grover, Phys. Rev. Lett. **79**, 4709 (1998).
[11] R. M. Gingrich, C. P. Williams, and N. J. Cerf, Phys. Rev. A **61**, 052313 (2000).
[12] Z. L. Mádi, R. Brüswchweiler, and R. R. Ernst, J. Chem. Phys. **109**, 10603, (1998).
[13] R. Brüsuchweiler, Phys. Rev. Lett. **85**, 4815 (2000).
[14] L. Xiao and G. L. Long, Phys. Rev. A **66**, 052320 (2002).
[15] R. Cleve and D. P. DiVincenzo, Phys. Rev. A **54**, 2636 (1996).
[16] L. J. Schulman and U. Vazirani, in *Proceedings of 31'st ACM STOC (Symp. Theory of Computing)* (ACM, New York, 1999), p. 322.
[17] R. R. Ernst, G. Bodenhausen, and A. Wokaun, *Principles of Nuclear Magnetic Resonance in One and Two Dimensions* (Oxford University Press, Oxford, 1987).
[18] L. Xiao, G. L. Long, H. Y. Yan, and Y. Sun, J. Chem. Phys. **117**, 3310 (2002).
[19] X. Yang, D. Wei, J. Luo, and X. Miao, Phys. Rev. A **66**, 042305 (2002).
[20] V. Protopopescu, C. DHelon, and J. Barhen, J. Phys. A **36**, L399 (2003).
[21] G. L. Long and L. Xiao, J. Chem. Phys. **119**, 8473 (2003).
[22] G. L. Long, Phys. Rev. A **64**, 022307 (2001).
[23] P. Benioff, Phys. Rev. Lett. **48**, 1581 (1982).
[24] C. H. Bennett, IBM J. Res. Dev. **17**, 525 (1973).
[25] D. Collins, Phys. Rev. A **65**, 052321 (2002).
[26] G. L. Long *et al.*, Commun. Theor. Phys. **38**, 305 (2002).
[27] B. d'Espgnat, *Veiled Reality: An Analysis of Present-day Quantum Mechanical Concepts* (Addison-Wesley, Reading, MA, 1995).
[28] Arvind and D. Collins, Phys. Rev. A **68**, 052301 (2003).
[29] R. Shankar, *Principles of Quantum Mechanics* (Plenum, New York, 1980).
[30] Xing-Lin Ka, *Advanced Quantum Mechanics* (Higher Education Press, 1999).