Appearance and stability of anomalously fluctuating states in Shor's factoring algorithm

Akihisa Ukena* and Akira Shimizu†
Department of Basic Science, University of Tokyo, 3-8-1 Komaba, Tokyo 153-8902, Japan
(Received 1 August 2003; published 2 February 2004)

We analyze quantum computers which perform Shor's factoring algorithm, paying attention to asymptotic properties as the number L of qubits is increased. Using numerical simulations and a general theory of the stabilities of many-body quantum states, we show the following: Anomalously fluctuating states (AFSs), which have anomalously large fluctuations of additive operators, appear in various stages of the computation. For large L, they decohere at anomalously great rates by weak noises that simulate noises in real systems. Decoherence of some of the AFSs is fatal to the results of the computation, whereas decoherence of some of the other AFSs does not have strong influence on the results of the computation. When such a crucial AFS decoheres, the probability of getting the correct computational result is reduced approximately proportional to L^2. The reduction thus becomes anomalously large with increasing L, even when the coupling constant to the noise is rather small. Therefore, quantum computations should be improved in such a way that all AFSs appearing in the algorithms do not decohere at such great rates in the existing noises.

DOI: 10.1103/PhysRevA.69.022301 PACS number(s): 03.67.Lx, 03.67.Pp, 03.65.Yz

I. INTRODUCTION

Quantum computers are considered to be more efficient than classical computers in solving certain problems [1–4]. Since the efficiency of computation becomes relevant only when the size N of the input is huge, the efficiency is defined in terms of the asymptotic behavior of the number Q of the computational steps as the size N of the input is increased. To study the asymptotic behavior, one must take the data size large but finite. Since larger N generally requires a larger number L of qubits as $L \sim \log N$, L of a relevant quantum computer becomes large but finite. Therefore, a relevant quantum computer is a many-body quantum system with large but finite degrees of freedom, $1 \ll L < +\infty$.

In the conventional many-body physics, one is usually interested in states that approach as $L \to \infty$ a ''vacuum'' state and finite excitations on it. This means that one is usually uninterested in other states of finite systems. In a quantum computer, on the other hand, various states are generated according to the algorithm and the input. It is therefore expected that some of them would be very different from states that are treated in the conventional many-body physics. It is very interesting to reveal physical properties of such ''anomalous'' states as well as their roles in quantum computations.

For quantum states of general systems with large but finite degrees of freedom, Shimizu and Miyadera (SM) recently studied the stabilities against weak noises, against weak perturbations from environments, and against local measurements [5]. By fully utilizing the locality of the theory, they obtained the general and universal results: the stabilities of quantum states are determined by long-distance correlations between local operators. As measures of the long-range correlations of quantum states, SM employed the ''cluster property,'' which plays a fundamental role in field theory [6], and the ''fluctuations of additive operators,'' which will be explained in the following section. If a pure state has anomalously large fluctuation of an additive operator(s), then the state has a long-distance correlation(s). Such a state does not have the cluster property, and is quite anomalous in many-body physics. Such anomalies are directly related to the stabilities of the quantum states.

Since the stability of quantum states against noises has been considered as a key to realizing quantum computers [7–9], it is interesting to apply the general theory by SM to quantum computers. In this paper, we analyze quantum computers performing Shor's factoring algorithm [2–4] using the general theory by SM and numerical simulations. We show that anomalous states, which have anomalously large fluctuations of additive operators, appear during the computation. For large L, they decohere at anomalously great rates in the presence of long-wavelength noises, while for small L the decoherence rates are of the same order of magnitude as those of normal states. The decoherence of some of the anomalous states, not all of them, results in the reduction of the success probability of the computation. Therefore, the decoherence of such anomalous states is crucial to Shor's factoring algorithm with huge inputs.

II. SUMMARY OF THE GENERAL THEORY OF THE DECOHERENCE RATES OF QUANTUM STATES IN SYSTEMS OF LARGE BUT FINITE DEGREES OF FREEDOM

SM [5] studied stabilities of quantum states of general systems of large but finite degrees of freedom. Among three kinds of stabilities discussed by them, we focus on the stability against weak classical noises; namely, we focus on the decoherence due to weak classical noises.

As compared with general many-body systems, quantum computers are often assumed to have the following special properties (although they are not necessary): (a) The system Hamiltonian is assumed to be negligible, so that quantum states of a quantum computer do not evolve unless the com-

*Email address: ukena@ASone.c.u-tokyo.ac.jp
†Email address: shmz@ASone.c.u-tokyo.ac.jp

puter is subjected to external operations and/or noises. (b) Qubits are assumed to be located on a one-dimensional lattice. In this section, we summarize the result of SM for the decoherence rate Γ, assuming these special properties.

A. Normalized additive operator

We consider a quantum computer that is composed of L ($\gg 1$) qubits which are located on sites of a one-dimensional lattice with a unit lattice constant. Let $\hat{a}(\ell)$ be a *local operator* at site $\ell(=1,2,\ldots,L)$, which for qubit systems is a polynomial of the Pauli operators $\hat{\sigma}_x(\ell),\hat{\sigma}_y(\ell),\hat{\sigma}_z(\ell)$, acting on the qubit at ℓ. Such a polynomial becomes a linear combination of the identity operator $\hat{1}(\ell)$ and $\hat{\sigma}_x(\ell),\hat{\sigma}_y(\ell),\hat{\sigma}_z(\ell)$ because of the su(2) algebra. We define a *normalized additive operator* $\hat{A}$ by

$$\hat{A}=\frac{1}{L}\sum_{\ell=1}^{L}\hat{a}(\ell), \tag{1}$$

which is the normalized one of the "additive operator" defined in Ref. [5]. For example, if we take

$$\hat{a}(\ell)=(-1)^{\ell}\hat{\sigma}_z(\ell), \tag{2}$$

then $\hat{A}$ is the z component of the "staggered magnetization," which has a finite expectation value when the system has an antiferromagnetic order.

Note that normalized additive operators are macroscopic operators. Thermodynamics assumes that fluctuations of any macroscopic observables are $o(V^2)$ for pure phases [5], where V is the volume of the system. However, this is *not* necessarily satisfied by pure quantum states of finite macroscopic systems [5,10–12], as will be described in the following.

B. L dependence of quantum states

In order to discuss L dependences of properties of quantum states, some rule is necessary that defines L dependence of quantum states. The simplest one of such a rule is that the quantum states are homogeneously extended with increasing L. For example, consider a superposition of two Néel states,

$$\frac{1}{\sqrt{2}}|1010\ldots10\rangle+\frac{1}{\sqrt{2}}|0101\ldots01\rangle, \tag{3}$$

where $|1\rangle$ and $|0\rangle$ denote the spin-up and -down states, respectively. To increase L of this state, one can simply add two spins as $(1/\sqrt{2})|1010\ldots1010\rangle+(1/\sqrt{2})|0101\ldots0101\rangle$. Unfortunately, states in quantum computers do not have such simple homogeneity. However, they are homogeneous in a broad sense because states with a larger L (which is necessary for a larger input N) and states with a smaller L are both generated according to the same algorithm. As a result, both of them have similar structures, as will be demonstrated explicitly in Sec. V D. This allows us to analyze the asymptotic behaviors of properties of states in quantum computers as $N\to\infty$.

C. Normally and anomalously fluctuating states

As a measure of correlations between distant qubits for a system of many qubits, SM [5] proposed the use of fluctuations of additive operators. We here summarize their proposal in terms of *normalized* additive operators.

Consider a pure state $|\psi\rangle$, and put

$$\Delta\hat{A}\equiv\hat{A}-\langle\psi|\hat{A}|\psi\rangle. \tag{4}$$

We focus on the L dependence of the fluctuation $\langle\psi|(\Delta\hat{A})^2|\psi\rangle$ for $L\gg 1$, and define an index p by

$$\langle\psi|(\Delta\hat{A})^2|\psi\rangle=O(L^{p-2}). \tag{5}$$

The value of p depends on both $\hat{A}$ and $|\psi\rangle$. For example, if the correlation between $\hat{a}(\ell)$ and $\hat{a}(\ell')$ for large $|\ell-\ell'|$ is negligibly small for $|\psi\rangle$, then $p=1$ for the normalized additive operator $\hat{A}$ which is composed of $\hat{a}(\ell)$ as Eq. (1).

For a given $|\psi\rangle$, if the maximum value of p (among those of all normalized additive operators) is unity, $|\psi\rangle$ is called a normally fluctuating state (NFS). It is easy to show that any separable state is a NFS. Note however that *the inverse is not necessarily true*. For example, $|100\ldots0\rangle,|010\ldots0\rangle,\ldots,|000\ldots1\rangle$ are all separable states, hence are NFSs. Their superposition

$$\frac{1}{\sqrt{L}}[|100\cdots0\rangle+|010\cdots0\rangle+|001\cdots0\rangle+\cdots+|000\cdots1\rangle]$$
$$\equiv|W\rangle \tag{6}$$

is also a NFS, but nonseparable.

On the other hand, if there is a normalized additive operator(s) $\hat{A}$ for which $p=2$, then the pure state $|\psi\rangle$ is called an anomalously fluctuating state (AFS) because the fluctuation of $\hat{A}$ is anomalously large. In this case, $\hat{a}(\ell)$ and $\hat{a}(\ell')$, which compose $\hat{A}$, are strongly correlated even when $|\ell-\ell'|\sim L$. Since AFSs are pure states, this indicates that AFSs are entangled *macroscopically* [5]. This entanglement is macroscopic because one cannot turn a NFS into an AFS by adding a small ($\sim L^0$) number of Bell pairs. Note, in particular, that the state $|W\rangle$ of Eq. (6) *is* entangled, but *not* macroscopically entangled, hence is not an AFS but a NFS. In this way, the value of p can be taken as a quantitative measure of *macroscopic* entanglement.

A simple example of an AFS is the state of Eq. (3), for which $\langle\psi|(\Delta\hat{A})^2|\psi\rangle=1$ for the staggered magnetization defined by Eqs. (1) and (2). Another simple example of an AFS is

$$\frac{1}{\sqrt{2}}|000\ldots0\rangle+\frac{1}{\sqrt{2}}|111\ldots1\rangle\equiv|C\rangle, \tag{7}$$

for which the fluctuation of the "magnetization" $\hat{M}_z \equiv (1/L)\Sigma_\ell \hat{\sigma}_z(\ell)$ is anomalously large; $\langle C|(\Delta \hat{M}_z)^2|C\rangle = 1$.

From the viewpoints of many-body physics and experiments, the index p seems a natural measure of macroscopic entanglement. In ferromagnets, for example, $|C\rangle$ is quite anomalous because it is a superposition of two states that have different values of the macroscopic variable $\hat{M}_z$. Such a state is usually discarded in many-body physics for many reasons. One reason is that it is very hard to generate such a state experimentally. Another reason is that such a state is not allowed as a pure state in the limit of infinite degrees of freedom, $L \to \infty$ [5]. On the other hand, $|W\rangle$ is a normal state which can easily be generated experimentally, although it is sometimes classified as a strongly entangled state in quantum information theory. In insulating solids, for example, the state vector of a many-body state in which a Frenkel exciton is excited on the ground state takes the form of $|W\rangle$; namely, in many-body physics $|W\rangle$ is just an ordinary state in which a single quasiparticle is excited on the ground state. Since many-body physics is directly related to (and has been tested by) experiments, a normal (abnormal) state in many-body physics is also a normal (abnormal) state in experiments. Therefore, our measure of macroscopic entanglement seems natural from the viewpoints of many-body physics and experiments. Considering that quantum computers should be fabricated from real materials, this indicates also that our measure would be suitable for discussing realization of quantum computers. Furthermore, an efficient method of computing p for general states has been developed in Ref. [13], whereas some of the other measures are hard to compute for general states. This is also an advantage of the present measure [14].

Although states with $1 < p < 2$ are possible [15], we focus on two classes of states, NFSs ($p=1$) and AFSs ($p=2$), in this paper.

D. Decoherence rate

We consider the decoherence rate Γ of states of quantum computers. For the origin of the decoherence, we assume a weak classical noise $f(\ell,t)$, acting on every site ℓ, with vanishing average $\overline{f(\ell,t)} = 0$. The case of a weak perturbation from the environment can be treated in a similar manner. We assume that $\overline{f(\ell,t)f(\ell',t')}[=\overline{f(\ell',t')f(\ell,t)}]$ depends only on $|\ell-\ell'|$ and $|t-t'|$. We denote the spectral intensity of $f(\ell,t)$ by $g(k,\omega)$, which is non-negative by definition. Here, k takes discrete values from $-\pi$ to π with separation $2\pi/L$ [16], whereas ω takes continuous values. The autocorrelation function can be expressed as

$$\overline{f(\ell,t)f(\ell',t')} = \sum_k \int \frac{d\omega}{2\pi} g(k,\omega) e^{ik(\ell-\ell')-i\omega(t-t')}. \tag{8}$$

Since physical interactions must be local, the interaction between the qubit system and the noise should be the sum of local interactions:

$$\hat{H}_{\rm int}(t) = \lambda \sum_{\ell=1}^{L} f(\ell,t)\hat{a}(\ell), \tag{9}$$

where λ is a positive constant and $\hat{a}(\ell)$ is a local operator at site ℓ. Since increasing λ is equivalent to increasing the amplitude of the noise, λ may be interpreted as the noise amplitude times the coupling constant. We shall therefore take f to have a normalized amplitude, as Eq. (39), and vary the noise amplitude by varying λ.

Assuming this local interaction and a short correlation time for the noise, SM showed that for $L \gg 1$ the decoherence rate Γ of a pure state $|\psi\rangle$ is directly related to fluctuations of additive operators. In terms of *normalized* additive operators, their formula reads

$$\Gamma \simeq \lambda^2 L^2 \sum_k g(k) \langle \psi | \Delta \hat{A}_k^\dagger \Delta \hat{A}_k | \psi \rangle. \tag{10}$$

Here, $g(k)$ is an average value of $g(k,\omega)$ [5] and $\Delta \hat{A}_k \equiv \hat{A}_k - \langle \psi | \hat{A}_k | \psi \rangle$, where

$$\hat{A}_k \equiv \frac{1}{L} \sum_{\ell=1}^{L} \hat{a}(\ell) e^{-ik\ell}. \tag{11}$$

For quantum computers, $g(k) \simeq g(k,0)$ because the system Hamiltonian is negligible. Note that $\hat{A}_k$ is a normalized additive operators, where $\hat{a}(\ell)e^{-ik\ell}$ of Eq. (11) corresponds to $\hat{a}(\ell)$ of Eq. (1). Hence, formula (10) shows that Γ of a pure state $|\psi\rangle$ of a quantum computer is determined by the fluctuation of a normalized additive operator that is composed of the local operators in $\hat{H}_{\rm int}$. Note that the formula of a pioneering work by Palma *et al.* [8] is a special case of the above general formula.

E. Fragility

We say that a quantum state is "fragile" if its decoherence rate Γ is anomalously great in such a way that

$$\Gamma \sim K L^{1+\delta}, \tag{12}$$

where K is a function of microscopic parameters, such as λ, and δ is a positive constant. This is an anomalous situation in which the decoherence rate *per qubit*, $\Gamma/L \sim K L^{\delta}$, grows with increasing L. For a nonfragile state (for which $\delta=0$), in contrast, $\Gamma/L \sim K$ is independent of L, in consistency with the naive expectation. This is a normal situation in which the total decoherence rate Γ is simply the sum of local decoherence rates.

For large L, fragile quantum states decohere much faster than nonfragile states because Γ becomes anomalously great, even when the coupling constant between the system and the noise is small.

F. Nonfragility of all NFSs and fragility of some AFSs

When $|\psi\rangle$ is a NFS, $\langle \psi | \Delta \hat{A}_k^\dagger \Delta \hat{A}_k | \psi \rangle \le O(1/L)$ for any $\hat{A}_k$, hence

$$\Gamma \lesssim \lambda^2 O(L) \sum_k g(k). \tag{13}$$

Since $\Sigma_k g(k) = \int \overline{f(x,t) f(x,0)} dt$ does not depend on L, we find that NFSs never become fragile under weak perturbations from any random noises [5].

When $|\psi\rangle$ is an AFS, on the other hand, $\langle \psi | \Delta \hat{A}_k^\dagger \Delta \hat{A}_k | \psi \rangle = O(L^0)$ for some $\hat{A}_k$, i.e., for some local operator $\hat{a}(x)$ and some wave number $k = k_0$. Hence, if $\hat{H}_{\rm int}$ has a term that is composed of such $\hat{a}(x)$'s, then

$$\Gamma \simeq \lambda^2 O(L^2) g(k_0) + \lambda^2 O(L) \sum_{k(\neq k_0)} g(k). \tag{14}$$

In this case, the AFS becomes fragile if $g(k_0) = O(L^{-1+\delta})$, where $\delta > 0$; namely, for an AFS, there *can* exist weak classical noises or weak perturbations from environments that make the AFS fragile. Whether such a noise or environment *really* exists in a quantum computer system depends on physical situations.

Although SM also considered a more fundamental instability of AFSs (i.e., instability against local measurements), the fragility is sufficient for the purpose of the present paper.

III. CONJECTURES ON QUANTUM COMPUTERS

From the general results summarized in the preceding section, we are led to the following conjectures on quantum computers [34].

A. Quantum computers should utilize AFSs

Entanglement has been considered to be essential to efficient quantum computations [1–4,17,18]. To discuss the efficiency of computation, one must study the asymptotic behavior of the computational time as $N \to \infty$. It is natural to consider that more entanglement is required for larger N. Since AFSs are entangled macroscopically, we are led to the following conjecture, which we call conjecture (i): In performing an algorithm that is much more efficient than any classical algorithms, a quantum computer should utilize AFSs in some stages of the computation.

Although the use of entanglement in quantum computations was somehow confirmed in the previous works [17,18], the magnitude of entanglement for large L can be defined in various ways. As a quantitative measure of entanglement, we propose here to use the asymptotic behavior, Eq. (5), of fluctuations of normalized additive operators. This enables us not only to identify macroscopically entangled states for large L, but also to estimate their decoherence rates using formulas (10), (13), and (14).

B. Some of AFSs appearing during quantum computation would be fragile

If conjecture (i) is the case, the results of Sec. II F lead us to the second conjecture, which we call conjecture (ii): Some of the AFSs appearing during quantum computation would be fragile under realistic weak classical noises or weak perturbations from environments.

For example, suppose that electromagnetic noises at 4 K is the dominant noise. If the physical dimension of a quantum computer is less than 1 cm, then $g(k)$ of the electromagnetic noises behaves as follows [16]:

$$g(k) \simeq \begin{cases} O(L^0) & (k=0) \\ O(1/L) & (k \geqslant 2\pi/L). \end{cases} \tag{15}$$

Therefore, according to Eq. (14), AFSs with $k_0 = 0$ becomes fragile (with $\delta = 1$), whereas AFSs with $k_0 \geqslant 2\pi/L$ are nonfragile; namely, if AFSs with $k_0 = 0$ appear during the computation, they are fragile in electromagnetic noises at 4 K.

C. Fragility of some AFSs should be fatal to quantum computation

If a fragile AFS is used in the quantum computation, it decoheres at an anomalously great rate as given by Eq. (12) with $\delta > 0$. Since quantum coherence is considered to be important in quantum computations, we are further led to the third conjecture, which we call conjecture (iii): The anomalously fast decoherence of such a fragile AFS(s) should be fatal to a quantum computation, and the quantum computation would become impossible for large L even if the coupling constant between the system and the noise or environment is small, unless error correcting codes (ECC) [19–22] and/or a decoherence-free subspace (DFS) [23–25] were successfully used. Since such efficient ECC and/or a DFS against all existing noises would not be easy to realize (see Sec. VIII E), improvements of the algorithm seem necessary; namely, if possible, one should implement the algorithm in such a way that only AFSs that are not fragile in existing noises are used.

In this paper, we study these conjectures by analyzing quantum computers performing Shor's factoring algorithm.

IV. QUICK SUMMARY OF SHOR'S FACTORING ALGORITHM

To study the conjectures raised in the preceding section, we perform numerical simulations on Shor's factoring algorithm [2,3], which is believed to be much (exponentially) faster than any classical algorithms. In order to establish notations, we summarize in this section the main part, which we will simulate, of the algorithm.

In order to factor an integer N, we use two quantum registers R_1 and R_2, which are called the first and second registers, respectively. They are composed of L_1 and L_2 qubits, respectively, where

$$2 \log N \leqslant L_1 < 2 \log N + 1, \tag{16}$$

$$\log N \leqslant L_2 < \log N + 1. \tag{17}$$

Here, log denotes $\log_2$. The total number of qubits is $L_1 + L_2 \equiv L$. The state of each qubit is described by a vector of a Hilbert space spanned by two basis states, $|0\rangle$ and $|1\rangle$. As a computational basis of register R_k, we take the set of the tensor products of the basis states of L_k qubits:

$$|a_1,a_2,\ldots,a_{L_k}\rangle^{(k)} \equiv |a\rangle^{(k)}. \tag{18}$$

Here, $a_\ell = 0$ or 1 ($\ell = 1,2,\ldots,L_k$) and $a \equiv \Sigma_{\ell=1}^{L_k} a_\ell 2^{\ell-1}$, for example, $|0\rangle^{(1)} = |00\cdots0\rangle^{(1)}$, $|1\rangle^{(1)} = |10\cdots0\rangle^{(1)}$, and $|2^{L_1}-1\rangle^{(1)} = |11\cdots1\rangle^{(1)}$. The initial state is taken as the following separable state:

$$|0\rangle^{(1)}|1\rangle^{(2)} \equiv |\psi_{\mathrm{init}}\rangle. \tag{19}$$

First, the Hadamard transformation is performed by successive unitary transformations on individual qubits of R_1, yielding

$$\frac{1}{\sqrt{2^{L_1}}} \sum_{a=0}^{2^{L_1}-1} |a\rangle^{(1)}|1\rangle^{(2)} \equiv |\psi_{\mathrm{HT}}\rangle. \tag{20}$$

Then, we take randomly an integer x ($\mathsf{x}<N$) that is coprime to N [26], and perform the modular exponentiation by successive pairwise unitary transformations, yielding

$$\frac{1}{\sqrt{2^{L_1}}} \sum_{a=0}^{2^{L_1}-1} |a\rangle^{(1)}|\mathsf{x}^a \bmod N\rangle^{(2)} \equiv |\psi_{\mathrm{ME}}\rangle. \tag{21}$$

Finally, the discrete Fourier transformation (DFT) is performed by successive pairwise unitary transformations, yielding

$$\frac{1}{2^{L_1}} \sum_{a=0}^{2^{L_1}-1} \sum_{c=0}^{2^{L_1}-1} \exp\left(\frac{2\pi i}{2^{L_1}} ca\right) |\overline{c}\rangle^{(1)}|\mathsf{x}^a \bmod N\rangle^{(2)}$$
$$\equiv |\psi_{\mathrm{final}}\rangle. \tag{22}$$

Here, $\overline{c}$ is the number that is obtained by reading the bits of c in the reversed order [3]. This completes the main part of Shor's factoring algorithm, and no more quantum computation is necessary. Since one can read $\overline{c}$ reversely, the final state $|\psi_{\mathrm{final}}\rangle$ is practically equivalent to

$$\frac{1}{2^{L_1}} \sum_{a=0}^{2^{L_1}-1} \sum_{c=0}^{2^{L_1}-1} \exp\left(\frac{2\pi i}{2^{L_1}} ca\right) |c\rangle^{(1)}|\mathsf{x}^a \bmod N\rangle^{(2)}.$$

The amplitude of $|\psi_{\mathrm{final}}\rangle$ has dominant peaks at basis states $|c\rangle^{(1)}$ satisfying

$$-\frac{r}{2} \le \overline{c}r \bmod 2^{L_1} \le \frac{r}{2}, \tag{23}$$

where r ($<N$) is the "order" of $\mathsf{x} \bmod N$ [2,3]. By performing a measurement that diagonalizes the computational basis $\{|c\rangle^{(1)}\}$ of R_1, one can obtain a value of c satisfying inequality (23) with the probability greater than $4/\pi^2$. When such an integer c is obtained, one can find uniquely for each c, using the continued fraction expansion of $\overline{c}/2^{L_1}$, a fraction c'/r that satisfies

$$\left|\frac{\overline{c}}{2^{L_1}} - \frac{c'}{r}\right| \le \frac{1}{2^{L_1+1}}, \tag{24}$$

where c' is an integer. If c' happens to be coprime to r, one can know the value of r. In other cases, where c' is not coprime to r or c does not satisfy inequality (23), one would obtain wrong results for r or could not obtain c' satisfying inequality (24). Whether the obtained value of r is correct or not can be checked easily by calculating $\mathsf{x}^r \bmod N$ using a classical computer. When the correct value of r is not obtained, one can perform the algorithm again. It is known that one can successfully obtain the correct value by repeating the algorithm $O(\log N)$ times. When r is thus obtained, one can know a factor of N with the probability greater than 1/2. Therefore, one can factor N efficiently by repeating the algorithm.

V. NUMERICAL SIMULATION WITHOUT NOISE

In order to study conjecture (i), we perform numerical simulations without noise in this section.

A. Simplification and the number of computational steps

The process of the modular exponentiation $|\psi_{\mathrm{HT}}\rangle \to |\psi_{\mathrm{ME}}\rangle$ costs $O(L_1^3)$ steps [2,3]. Since it will turn out that R_1 takes a major role, we simplify operations on R_2 in our numerical simulations; namely, we represent the process $|\psi_{\mathrm{HT}}\rangle \to |\psi_{\mathrm{ME}}\rangle$ as the product of L_1 controlled unitary transformations $U^{a_\ell 2^{\ell-1}}$ ($\ell = 1,2,\ldots,L_1$), which is described in Box 5.2 of Ref. [4]. Since $U^{a_\ell 2^{\ell-1}}$ can be decomposed into $O(L_1^2)$ pairwise unitary transformations, the states appearing during the modular exponentiation in our simulations correspond to L_1 representative states out of $O(L_1^3)$ states. As a result of this simplification, the total number Q of computational steps, from $|\psi_{\mathrm{init}}\rangle$ to $|\psi_{\mathrm{final}}\rangle$, in our simulation becomes

$$Q = 2L_1 + \frac{L_1(L_1+1)}{2}. \tag{25}$$

Here, L_1 comes from the Hadamard transformation and another L_1 from the modular exponentiation, whereas $L_1(L_1+1)/2$ comes from the discrete Fourier transformation. This Q is smaller than $O(L_1^3)$ steps of a real computation because of the above simplification.

We denote the time interval between subsequent computational steps by τ. Although τ depends on the hardware of the quantum computer, this dependence does not matter in the following discussions because we are only interested in the N dependence, which is the only crucial factor in discussing the exponential speedup. The total computational time, starting from $|\psi_{\mathrm{init}}\rangle$ and ending with the measurement of $|\psi_{\mathrm{final}}\rangle$, is given by

$$\tau_{\mathrm{total}} = (Q+1)\tau. \tag{26}$$

B. Choice of normalized additive operators

To judge that a quantum state is *not* an AFS, fluctuations of *all* normalized additive operators have to be investigated. On the other hand, to judge that a state *is* an AFS, it is sufficient to find out *one* normalized additive operator $\hat{A}$ for which $\langle \Delta \hat{A}^2 \rangle = O(L^0)$. In order to confirm conjecture (i), it is therefore sufficient to find out *one* $\hat{A}$ for which a quantum state(s) appearing in the computational process has an anomalously large fluctuation, $\langle \Delta \hat{A}^2 \rangle = O(L^0)$.

As normalized additive operators, we here consider the "magnetization" in three directions $\alpha = x,y,z$, for the total and the individual registers, which are defined by

$$\hat{M}_\alpha = \frac{1}{L} \sum_{\ell \in R_1, R_2} \hat{\sigma}_\alpha(\ell) \tag{27}$$

and

$$\hat{M}^{(k)}{}_\alpha = \frac{1}{L_k} \sum_{\ell \in R_k} \hat{\sigma}_\alpha(\ell), \tag{28}$$

respectively. The maximum value of $\langle (\Delta \hat{M}_\alpha)^2 \rangle$ is unity, which is taken, e.g., by the following AFS:

$$\frac{1}{\sqrt{2}} |0\rangle^{(1)} |0\rangle^{(2)} + \frac{1}{\sqrt{2}} |2^{L_1} - 1\rangle^{(1)} |2^{L_2} - 1\rangle^{(2)}. \tag{29}$$

For separable states, on the other hand, $\langle (\Delta \hat{M}_\alpha)^2 \rangle$ becomes as small as $\langle (\Delta \hat{M}_\alpha)^2 \rangle \leq 1/L$. This is consistent with the fact that any separable state is a NFS. For example, $|\psi_{\rm init}\rangle$ is a separable state, for which $\langle (\Delta \hat{M}_\alpha)^2 \rangle \leq 1/L$ for all three directions $\alpha = x,y,z$.

C. Anomalously fluctuating states are used in Shor's algorithm

We evaluate fluctuations of $\hat{M}_\alpha$ and $\hat{M}^{(1)}{}_\alpha$ for all states appearing in Shor's factoring algorithm, for various values of N and x. We assume in this section that noises are absent, because our purpose in this section is to find out AFSs.

Figure 1 shows the change of $\langle (\Delta \hat{M}_\alpha)^2 \rangle$ along the steps of the algorithm when $N = 21$, $L_1 = 10$, $L_2 = 5$, $\mathsf{x} = 2$, for which $r = 6$. It is seen that $\langle (\Delta \hat{M}_\alpha)^2 \rangle$'s remain smaller than $1/L = 1/15 \simeq 0.067$ until the Hadamard transformation is finished. This is consistent with the fact that any separable state is a NFS (although the inverse is not necessarily true), because all states during the Hadamard transformation are separable states [see, e.g., Eq. (61)]. In the modular exponentiation processes, on the other hand, $\langle (\Delta \hat{M}_x)^2 \rangle$ grows quickly, until it becomes 0.227, which is significantly greater than $1/L$, when the modular exponentiation is finished. During the DFT, $\langle (\Delta \hat{M}_x)^2 \rangle$ decreases gradually, whereas $\langle (\Delta \hat{M}_z)^2 \rangle$ grows in turn until it becomes 0.109, which is significantly greater than $1/L$, at the final stage of the DFT.

To examine which register is responsible for the large fluctuations, we investigate W_α ($\alpha = x,y,z$) that is defined by

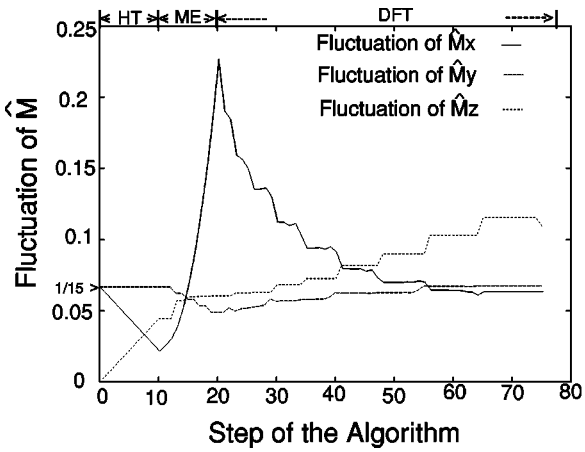

FIG. 1. $\langle (\Delta \hat{M}_\alpha)^2 \rangle$ of every state appearing in Shor's factoring algorithm when $N = 21$, $L_1 = 10$, $L_2 = 5$, $\mathsf{x} = 2$, for which $r = 6$.

$$W_\alpha \equiv \frac{\langle (\Delta \hat{M}_\alpha^{(1)})^2 \rangle}{\langle (\Delta \hat{M}_\alpha)^2 \rangle} = \frac{\langle (\Delta \hat{M}_\alpha^{(1)})^2 \rangle}{\left\langle \left(\frac{L_1}{L} \Delta \hat{M}_\alpha{}^{(1)} + \frac{L_2}{L} \Delta \hat{M}_\alpha{}^{(2)} \right)^2 \right\rangle}. \tag{30}$$

If the first register gives dominant contribution to the fluctuation, we expect that

$$W_\alpha \simeq \left(\frac{L}{L_1} \right)^2 = 2.25. \tag{31}$$

In Fig. 2, we plot the change of $\langle (\Delta \hat{M}_\alpha^{(1)})^2 \rangle$ along the steps of the algorithm. Comparing Fig. 1 with Fig. 2, we find that $W_x = 2.03$ for $|\psi_{\rm ME}\rangle$ and $W_z = 2.05$ for $|\psi_{\rm final}\rangle$. Since these values of W_α are close to $(L/L_1)^2$, we conclude that R_1 gives the dominant contribution.

In order to judge whether the states are AFSs or not, we also investigate the L dependence of the fluctuations. Since R_1 gives dominant contributions, we calculate $\langle (\Delta \hat{M}_\alpha^{(1)})^2 \rangle$ for a larger system with $N = 513$, $L_1 = 20$, $L_2 = 10$, $\mathsf{x} = 26$, for which $r = 6$. Figure 3 plots $\langle (\Delta \hat{M}_\alpha^{(1)})^2 \rangle$ in this case. By

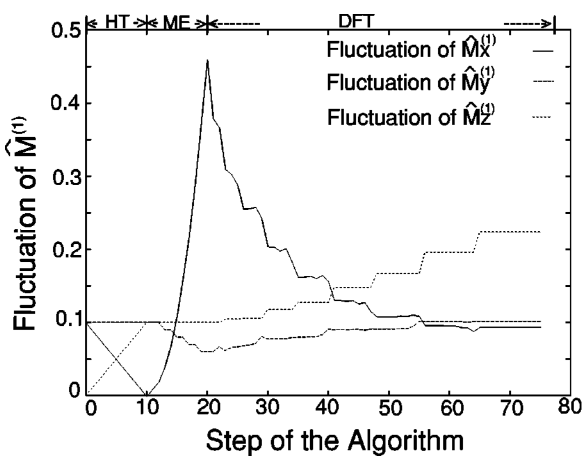

FIG. 2. $\langle (\Delta \hat{M}_\alpha^{(1)})^2 \rangle$ of every state appearing in Shor's factoring algorithm when $N = 21$, $L_1 = 10$, $L_2 = 5$, $\mathsf{x} = 2$, for which $r = 6$.

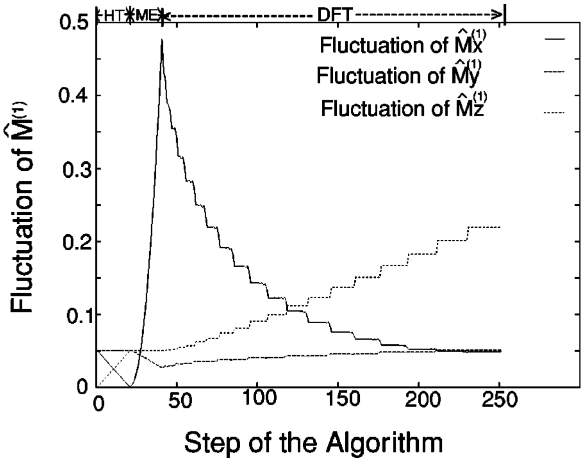

FIG. 3. $\langle(\Delta\hat{M}_\alpha^{(1)})^2\rangle$ of every state appearing in Shor's factoring algorithm when $N=513$, $L_1=20$, $L_2=10$, $\mathsf{x}=26$, for which $r=6$.

comparing this figure with Fig. 2, we find that $\langle(\Delta\hat{M}_x^{(1)})^2\rangle$ for $|\psi_{\rm ME}\rangle$ is almost independent of L_1. In fact, $\langle\psi_{\rm ME}|(\Delta\hat{M}_x^{(1)})^2|\psi_{\rm ME}\rangle$ is 0.460 and 0.477 in Figs. 2 and 3, respectively. We also find that $\langle(\Delta\hat{M}_z^{(1)})^2\rangle$ is almost independent of L_1 for $|\psi_{\rm final}\rangle$. In fact, $\langle\psi_{\rm final}|(\Delta\hat{M}_z^{(1)})^2|\psi_{\rm final}\rangle$ is 0.223 and 0.219 in Figs. 2 and 3, respectively. On the other hand, other fluctuations have different dependences on L_1; for example, $\langle(\Delta\hat{M}_x^{(1)})^2\rangle$ for $|\psi_{\rm final}\rangle$ in Fig. 3 is nearly half of that in Fig. 2. Moreover, $\langle(\Delta\hat{M}_y^{(1)})^2\rangle$'s of all states in Fig. 3 are nearly half of those in Fig. 2.

From these observations, we conclude that $|\psi_{\rm ME}\rangle$ and $|\psi_{\rm final}\rangle$ are AFSs, which have anomalously large fluctuations of $\hat{M}_x$ and $\hat{M}_z$, respectively. Although this does not exclude the possibility that some other states could also be AFSs, identification of the above AFSs are sufficient for the purpose of the present paper. Namely, we have confirmed conjecture (i) when $(N,\mathsf{x})=(21,2)$ and $(513,26)$, both for which $r=6$.

We also performed numerical simulations for other values of (N,x), for which r takes various values from 2 to 20. We found that AFSs appear for all cases except when r becomes an integral power of 2, i.e., except when $r=2,4,8,16$; namely, we have confirmed conjecture (i) apart from the exceptional cases. Since such exceptional cases seem to be unimportant in quantum computation, we consider a typical case $(N,\mathsf{x})=(21,2)$ in the following sections.

D. Similarity of states with different values of *L*

From Figs. 2 and 3, it is seen that states of different values of L have similar properties; namely, states in quantum computers are homogeneous in a broad sense, because states with a larger L (which is necessary for larger inputs) and states with a smaller L are both generated according to the same algorithm. This allows us to analyze the L dependence of the properties of quantum states in the quantum computers.

VI. MODELING AND THEORETICAL BASIS OF QUANTUM COMPUTERS SUBJECT TO NOISES

In order to examine conjectures (ii) and (iii), we investigate in the following sections effects of weak perturbations from classical noises on quantum computers. In this section, we describe the modeling and theoretical basis.

A. Model of noises

We consider classical noises f_x, f_y, f_z, which act on the qubits through the following interaction Hamiltonian:

$$\hat{H}_{\rm int}=\sum_{\alpha=x,y,z}\lambda_\alpha\sum_{\ell=1}^{L} f_\alpha(\ell,t)\hat{\sigma}_\alpha(\ell). \tag{32}$$

Since the computational basis is taken as Eq. (18), f_x and f_y are called "bit-flip noises" because they induce transitions between different basis states, whereas f_z is called a "phase-shift noise" because it induces phase shifts of the basis states.

In this paper, we consider long-wavelength noises, whose spectral intensities behave as Eq. (15); namely, we take $f_\alpha(\ell,t)$ to be independent of ℓ:

$$f_\alpha(\ell,t)=f_\alpha(t). \tag{33}$$

For simplicity, we assume that

$$\lambda_x=\lambda_y=\lambda_z\equiv\lambda, \tag{34}$$

$$\overline{f_\alpha(t)}=0, \tag{35}$$

$$\overline{f_\alpha(t)f_\beta(t')}=\delta_{\alpha,\beta}\overline{f_\alpha(t)f_\alpha(t')}, \tag{36}$$

which seem natural in many physical situations. Here, the overline denotes the average over the ensemble of the noises:

$$\overline{\cdots}=\lim_{n_\nu\to\infty}\frac{1}{n_\nu}\sum_{\nu=1}^{n_\nu}\cdots, \tag{37}$$

where ν labels realizations $(1,2,\ldots,n_\nu)$ of the noises. From Eqs. (33) and (34), the interaction reduces to the simple form

$$\hat{H}_{\rm int}(t)=\lambda L\sum_{\alpha=x,y,z} f_\alpha(t)\hat{M}_\alpha. \tag{38}$$

To simulate some real systems [27–29], $f_\alpha(t)$ is assumed to have the $1/f$ spectrum [30],

$$f_\alpha(t)=\sum_\omega \frac{1}{\sqrt{\omega\tau}}\cos[\omega t+\theta_\alpha(\omega)], \tag{39}$$

where $\theta_\alpha(\omega)$ is a random phase, which distributes uniformly in $(-\pi,\pi]$ for each ω, and the summation is taken over discrete values of ω in the interval $\omega_{\rm low}\leqslant\omega\leqslant\omega_{\rm high}$ with separations $\Delta\omega=2\pi/\tau_{\rm total}$. Here, $\omega_{\rm low}$ and $\omega_{\rm high}$ are low- and high-frequency cutoffs, respectively.

In real systems, noises act continuously over the whole computational time $\tau_{\rm total}$. However, we wish to study effects of noises *on each state* in the computation. Therefore, we assume that the computation is perfectly performed until the mth step, and that the noises act between the mth and $(m+1)$th steps. By calculating changes of the quantum states and of the computational results in this case, we can analyze effects of the noises on each state.

For this purpose, we take $\omega_{\rm low}=\Delta\omega$ because the variation at such a low frequency is negligible during the time interval τ of one step. Regarding $\omega_{\rm high}$, we take $\omega_{\rm high}\simeq 4.1\times 2\pi/\tau$, where the fractional factor 4.1 is taken in order to avoid possible troubles which may occur by setting $\omega_{\rm high}$ as an integral multiple of $2\pi/\tau$. We have confirmed that effects of higher-frequency components are negligible.

B. Fidelity and decoherence

Before presenting results of numerical simulations in the following section, we present in this section a theoretical basis for analyzing the numerical results.

As explained in Sec. II D, λ can be interpreted as the noise amplitude times the coupling constant. We are interested in the case of small λ, because otherwise it is obvious that the quantum computation would fail. We therefore assume that λ is small enough so that its lowest-order contribution is dominant [see, e.g., Eq. (41) below]. Note, however, that the numerical results presented in the following section include all orders in λ. Since numerical simulations are possible only for relatively small L, we will draw general conclusions by using complementally both the numerical results and the analytic results of this section.

Suppose that the computation is perfectly performed until the mth step; namely, the state $|\psi_m\rangle$ that is obtained just after the mth step is exactly the state prescribed by the algorithm. When the noises act between the mth and $(m+1)$th steps, the state evolves into

$$|\psi_m'\rangle=|\psi_m\rangle+\frac{1}{i\hbar}\int_0^\tau dt\hat{H}_{\rm int}(t)|\psi_m\rangle + \frac{1}{(i\hbar)^2}\int_0^\tau dt\int_0^t dt'\hat{H}_{\rm int}(t)\hat{H}_{\rm int}(t')|\psi_m\rangle+\cdots. \tag{40}$$

We are interested in the density operator $\hat{\rho}_m'$ that is the average of $|\psi_m'\rangle\langle\psi_m'|$ over the ensemble of the noises. From Eqs. (35), (36), (38), and (40), we obtain

$$\hat{\rho}_m'\equiv\overline{|\psi_m'\rangle\langle\psi_m'|}=\hat{\rho}_m-\frac{\lambda^2L^2}{2\hbar^2}\sum_\alpha C_\alpha(\tau)(\hat{M}_\alpha^2\hat{\rho}_m+\hat{\rho}_m\hat{M}_\alpha^2 - 2\hat{M}_\alpha\hat{\rho}_m\hat{\rho}_m\hat{M}_\alpha)+O(\lambda^3). \tag{41}$$

Here, $\hat{\rho}_m\equiv|\psi_m\rangle\langle\psi_m|$, and $C_\alpha(\tau)$ is an integral of the autocorrelation function of the noise,

$$C_\alpha(\tau)\equiv 2\int_0^\tau dt\int_0^t dt'\overline{f_\alpha(t)f_\alpha(t')}=\int_0^\tau dt\int_0^\tau dt'\overline{f_\alpha(t)f_\alpha(t')} =\overline{\left(\int_0^\tau f_\alpha(t)dt\right)^2}. \tag{42}$$

As a measure of deviation of $\hat{\rho}_m'$ from the ideal one $\hat{\rho}_m$, we consider the fidelity that is defined by

$$F_m\equiv{\rm Tr}[\rho_m\rho_m']. \tag{43}$$

This is not necessarily a good measure of decoherence, because it can be reduced even when $\hat{\rho}_m'$ happens to be a pure state. As a measure of decoherence, we consider the α entropy of $\alpha=2$,

$$S_m\equiv-\ln({\rm Tr}[(\rho_m')^2]). \tag{44}$$

To see the relation between F_m and S_m, let us represent Eq. (41) as $\hat{\rho}_m'=\hat{\rho}_m+\lambda^2\hat{\eta}_m+O(\lambda^3)$. Then we obtain

$$S_m=-2\lambda^2{\rm Tr}[\hat{\rho}_m\hat{\eta}_m]+O(\lambda^3), \tag{45}$$

$$F_m=1+\lambda^2{\rm Tr}[\hat{\rho}_m\hat{\eta}_m]+O(\lambda^3). \tag{46}$$

We thus find

$$S_m=2(1-F_m)+O(\lambda^3). \tag{47}$$

Therefore, to $O(\lambda^2)$, the reduction of the fidelity is directly related to the increase of the entropy, i.e., to the decoherence. Since we are interested in the case of small λ, this perturbative relation should hold. We thus simply call the reduction of the fidelity 'decoherence'' in the following discussions.

Inserting Eq. (41) into Eq. (43), we obtain a simple formula, which is correct up to $O(\lambda^2)$,

$$F_m=1-\frac{\lambda^2L^2}{\hbar^2}\sum_\alpha C_\alpha(\tau)\langle\psi_m|(\Delta\hat{M}_\alpha)^2|\psi_m\rangle, \tag{48}$$

where $\Delta\hat{M}_\alpha\equiv\hat{M}_\alpha-\langle\psi_m|\hat{M}_\alpha|\psi_m\rangle$. It is seen that, to $O(\lambda^2)$, F_m decreases in proportion to L^2 and to the fluctuations of magnetizations, in accordance with the general result, Eq. (10). It is also seen that the noises in three directions f_x, f_y, f_z contribute additively to F_m. We can therefore calculate effects of f_x, f_y, f_z independently.

The decoherence rate (per step) Γ_m of $|\psi_m\rangle$ is given by

$$\Gamma_m\equiv\frac{S_m}{2\tau}, \tag{49}$$

where the factor of 2 has been inserted for convenience. From Eqs. (47) and (48), we obtain a formula for Γ_m:

$$\Gamma_m=\frac{\lambda^2L^2}{\hbar^2}\sum_\alpha\frac{C_\alpha(\tau)}{\tau}\langle\psi_m|(\Delta\hat{M}_\alpha)^2|\psi_m\rangle, \tag{50}$$

which is correct up to $O(\lambda^2)$. This formula is a special case of the general result of SM, Eq. (10), except for the extra factor $C_\alpha(\tau)/\tau$. The case of $\alpha = z$ of the above formula agrees also with the result of Ref. [8], except for the extra factor. The extra factor appears because the $1/f$ noise, Eq. (39), does not satisfy the assumption of short-time correlation. Since the extra factor is independent of the state of the qubit system, it can be considered as a constant when comparing decoherence rates of different states.

C. Fragility of anomalously fluctuating states

When $|\psi_m\rangle$ is a NFS, $\langle\psi_m|(\Delta\hat{M}_\alpha)^2|\psi_m\rangle \leqslant O(1/L)$ by definition. Formula (50) then yields

$$\Gamma_m \leqslant \lambda^2 O(L). \tag{51}$$

Therefore, NFSs never become fragile. When $|\psi_m\rangle$ is an AFS that has been found in Sec. V C, on the other hand, $\langle\psi_m|(\Delta\hat{M}_\alpha)^2|\psi_m\rangle = O(L^0)$ for $\alpha = x$ or z. If the noise component f_α for such α is present, formula (50) yields

$$\Gamma_m = \lambda^2 O(L^2), \tag{52}$$

hence the AFS becomes fragile (with $\delta = 1$).

These results are consistent with conjecture (ii) and with the more general results that are summarized in Sec. II F. It is important to note the following fact, which is obtained from Eqs. (51) and (52):

$$\frac{(\text{decoherence rate of fragile AFSs})}{(\text{decoherence rate of NFSs})} \geqslant O(L). \tag{53}$$

This ratio becomes $\gg 1$ when $L \gg 1$, i.e., when the input N is huge. Therefore, the decoherence rate of the quantum computer is almost determined by the decoherence rates of the fragile AFSs. These points will be studied more in detail using numerical simulations in the following section.

Note also that decoherence does not necessarily reduce the success probability of the computation. We will also study this point in the following section.

VII. RESULTS OF NUMERICAL SIMULATIONS WITH NOISES

In this section, we present results of numerical simulations of Shor's factoring algorithm when noises act on a quantum computer. As explained in Sec. V C, we take $N = 21$, $L_1 = 10$, $L_2 = 5$, $\mathrm{x} = 2$, for which $r = 6$ and $Q = 75$.

A. Decoherence

In Fig. 4, we show a two-dimensional plot of the fidelity versus the fluctuation of $\hat{M}_z$ for all steps, i.e., $(\langle\psi_m|(\Delta\hat{M}_z)^2|\psi_m\rangle, F_m)$ for all m, when only a phase-shift noise is present, i.e., when f_z is given by Eq. (39) whereas $f_x = f_y = 0$. Each point in the figure corresponds to a state appearing in the algorithm. The parameter λ is taken as $0.0015\hbar/\tau$. Regarding a bit-flip noise, we show in Fig. 5 a two-dimensional plot of the fidelity versus the fluctuation of $\hat{M}_x$ when f_x is given by Eq. (39) whereas $f_y = f_z = 0$ for $\lambda = 0.0015\hbar/\tau$. A similar plot (not shown) has been obtained if we plot $(\langle\psi_m|(\Delta\hat{M}_y)^2|\psi_m\rangle, F_m)$ when f_y is given by Eq. (39) whereas $f_x = f_z = 0$. This is reasonable because both f_x and f_y are bit-flip noises.

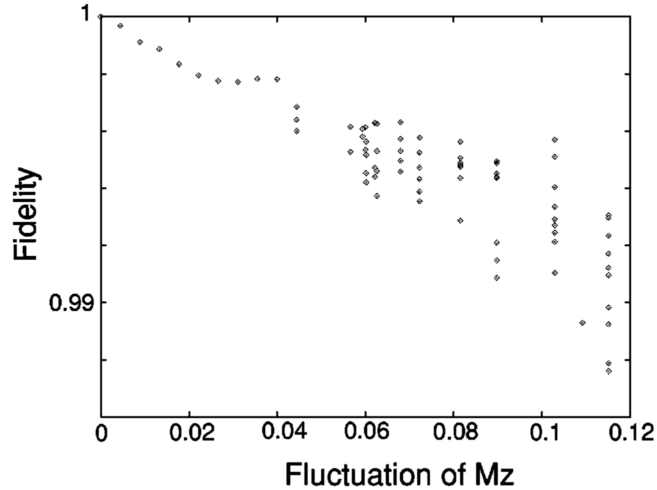

FIG. 4. Fidelity vs $\langle(\Delta\hat{M}_z)^2\rangle$ in the presence of a phase-shift noise f_z when $N = 21$, $\mathrm{x} = 2$, and $\lambda = 0.0015\hbar/\tau$. The average over noise realizations has been taken over 40 samples.

Figures 4 and 5 show that F decreases, on an average, in proportion to the fluctuation of the normalized additive operator to which the noise couples via $\hat{H}_{\rm int}(t)$ of Eq. (38). Distributions around the average curve are due to the fact that the number n_ν of noise samples is not very large; $n_\nu = 40$. Therefore, formula (48) has been confirmed. Hence, formulas (50)–(52) have also been confirmed.

In these figures, states with larger fluctuations are more likely to be AFSs. In particular, the states with the largest fluctuations in Figs. 4 and 5 are $|\psi_{\rm final}\rangle$ and $|\psi_{\rm ME}\rangle$, respectively, which have been identified as AFSs in Sec. V C. Although L is rather small ($L = 15$) in this simulation, we can extrapolate the results to the case of larger L using formulas (50)–(52). (See discussions in Sec. VII D.) It is then clear that conjecture (ii) is correct.

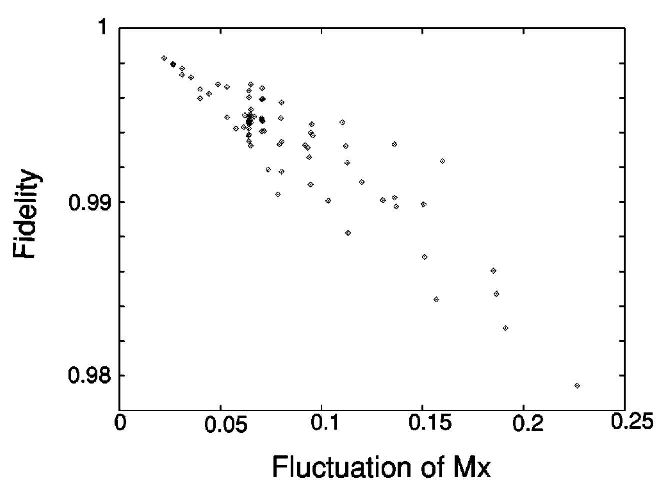

FIG. 5. Fidelity vs $\langle(\Delta\hat{M}_x)^2\rangle$ in the presence of a bit-flip noise f_x when $N = 21$, $\mathrm{x} = 2$, and $\lambda = 0.0015\hbar/\tau$. The average over noise realizations has been taken over 40 samples.

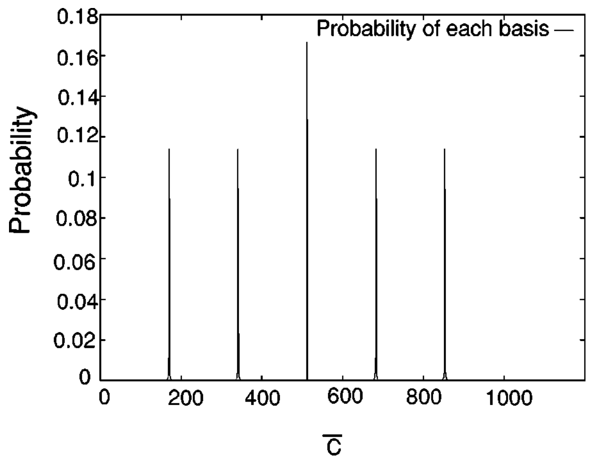

FIG. 6. Probability distribution of finding a basis state $|c\rangle^{(1)}$ at the end of the algorithm when $N=21$, $x=2$, and $\lambda=0$. The horizontal axis is the bit reversal $\overline{c}$ of c.

B. Success probability

Generally speaking, decoherence of a particular state does not necessarily lead to false results of the quantum computation. For example, as will be discussed in Sec. VII E, decoherence of $|\psi_{\rm final}\rangle$ by the phase-shift noise f_z does not reduce the probability of getting the correct value of r at all. Therefore, in this section we investigate effects of the noises on the computational result for each state.

For this purpose, we calculate the *success probability T* that is defined as the probability of finding in the final state a basis state which gives the correct value of r. In Shor's factoring algorithm, one performs measurement, which diagonalize the computational basis, on the final state $|\psi_{\rm final}\rangle$. When noises are absent, for example, we plot in Fig. 6 the probability of finding each basis state in $|\psi_{\rm final}\rangle$. Each dominant peak is accompanied by side peaks, as shown in Fig. 7, which is a magnification of Fig. 6. If the basis state with $c=\overline{171}$ or $\overline{853}$ happens to be obtained, one can successfully obtain the correct value of $r=6$, where the overbar denotes the bit reversal. The other basis states do not give the correct

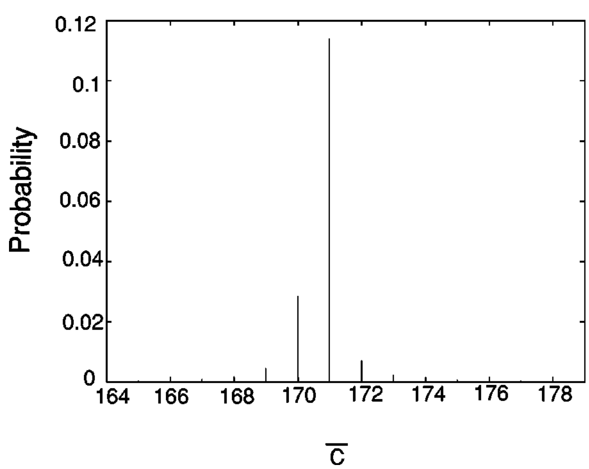

FIG. 7. A magnification of Fig. 6 around a dominant peak at $\overline{c}=171$.

value. For example, if one obtains $c=\overline{512}$, which corresponds to the central peak in Fig. 6, then c' satisfying inequality (24) is $c'=3$. Since c' is not coprime to $r=6$, it gives a wrong result as $r=2$. Whether the result is correct or not can be checked efficiently using a classical computer. Furthermore, if one obtains $c=\overline{170}$, which corresponds to the highest side peak associated with the dominant peak at $c=\overline{171}$ in Fig. 7, then there is no c' satisfying inequality (24). Therefore, T is given in the case of $N=21$, $x=2$ by

$$T=P(\overline{171})+P(\overline{853}), \tag{54}$$

where $P(c)$ denotes the probability of finding in the final state a basis state $|c\rangle^{(1)}$.

It is essential to exclude $P(c)$'s of the basis states corresponding to the other peaks. In fact, we found that some of such excluded $P(c)$'s sometimes *increase* with increasing the strength of noises. Hence, we would have obtained unphysical results if we included them in the success probability.

It is evident from Eq. (54) that $T<1$ even in the absence of the noises. If we denote T in the absence of noises by $T_{\rm clean}$, it is evaluated for the case of Fig. 6 as $T_{\rm clean}=0.227\,97$. When noises act on the quantum computer, T would become smaller than $T_{\rm clean}$,

$$T=\epsilon T_{\rm clean}, \tag{55}$$

where $\epsilon\leqslant 1$. For a successful quantum computation, the factor ϵ should be kept larger than some threshold value $\epsilon_{\rm th}$ (see Sec. VIII A):

$$\epsilon\geqslant\epsilon_{\rm th}. \tag{56}$$

Consider now the case where noises act *only* between the mth and $(m+1)$th steps. We denote the success probability in this case by T_m. By investigating T_m and F_m for each m, we can study effects of the noises on the computational results for each state $|\psi_m\rangle$. In real situations, noises act continuously throughout all steps. Hence, the success probability in real situations is less than any T_m:

$$T\leqslant\min_m T_m. \tag{57}$$

Therefore, the following condition is *necessary* for a successful quantum computation:

$$\min_m\frac{T_m}{T_{\rm clean}}\geqslant\epsilon_{\rm th}. \tag{58}$$

C. Relation between the success probability and decoherence

In Figs. 8 and 9, we plot the relation between the fidelity F_m and the success probability T_m when $\lambda=0.0015\hbar/\tau$ for a bit-flip noise [$f_x\neq 0$, given by Eq. (39), whereas $f_y=f_z=0$] and a phase-shift noise [$f_x=f_y=0$, whereas $f_z\neq 0$, given by Eq. (39)], respectively; namely, (F_m,T_m) are plotted for all m.

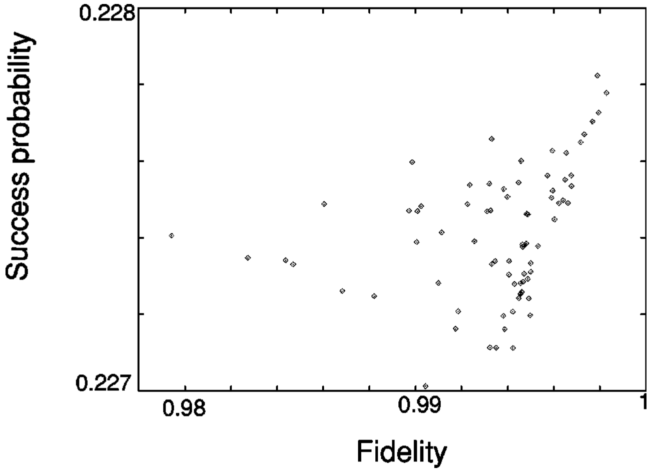

FIG. 8. The success probability vs the fidelity in the presence of a bit-flip noise f_x when $N=21$, $\chi=2$, and $\lambda=0.0015\hbar/\tau$. The average over noise realizations has been taken over 40 samples.

It is seen that for most states their decoherence results in the reduction of the success probability, as might be expected. If we define the *rate of the reduction of the success probability per decoherence* by

$$r_m \equiv \frac{T_{\text{clean}} - T_m}{1 - F_m}, \tag{59}$$

then it is found that r_m varies from state to state.

We notice that there are exceptional states located at the top of Fig. 9, for which the phase-shift noise does not reduce the success probability. These are states which appear in the latter part of the DFT. This means that quantum coherence among basis states of these states is unnecessary for quantum computation. This may be understood by considering effects of the phase-shift noise on the final state $|\psi_{\text{final}}\rangle$. In order to estimate r, one will perform measurement on this state, which diagonalizes the computational basis. This means that one will not measure the relative phases among basis states. Therefore, decoherence of the relative phases in $|\psi_{\text{final}}\rangle$ does not change the computational result at all. This point will be discussed again later in Sec. VII E.

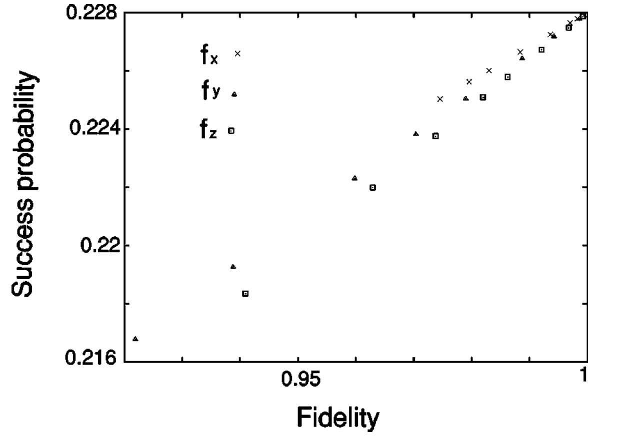

FIG. 10. The success probability vs the fidelity of $|\psi_{\text{HT}}\rangle$, which is a typical NFS, for various strengths of the noises f_x, f_y, f_z. The average over noise realizations has been taken over 200 samples.

D. An AFS is crucial

We now investigate differences between effects of noises on NFSs and those on AFSs. For this purpose, we investigate effects of noises on $|\psi_{\text{HT}}\rangle$, which is a typical NFS, and those on $|\psi_{\text{ME}}\rangle$, which is a typical AFS.

Figures 10 and 11 plot (F_m, T_m) for $|\psi_m\rangle = |\psi_{\text{HT}}\rangle$ and for $|\psi_m\rangle = |\psi_{\text{ME}}\rangle$, respectively, for various values of λ ranging from $0.000\,75\hbar/\tau$ to $0.006\hbar/\tau$. The crosses represent the case of a bit-flip noise with $f_x \neq 0$, given by Eq. (39), whereas $f_y = f_z = 0$. The triangles represent the case of another bit-flip noise with $f_y \neq 0$, given by Eq. (39), whereas $f_x = f_z = 0$. On the other hand, the squares in the figures represent the case of a phase-shift noise with $f_z \neq 0$, given by Eq. (39), whereas $f_x = f_y = 0$.

It is found that both F_m and T_m decrease with increasing λ. As a result, (F_m, T_m) of either state composes a monotonic curve, although the data scatter slightly around the average curve because the average over noise realizations has

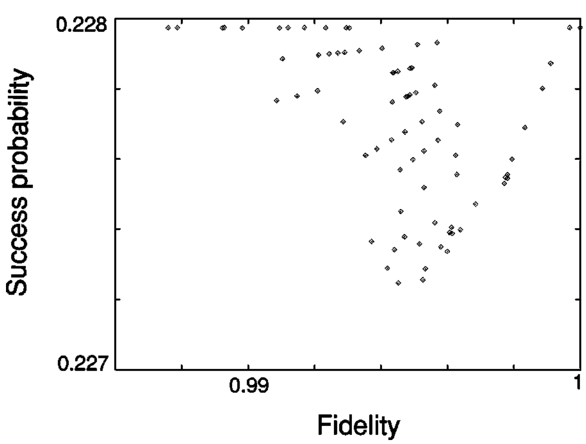

FIG. 9. The success probability vs the fidelity in the presence of a phase-shift noise f_z when $N=21$, $\chi=2$, and $\lambda=0.0015\hbar/\tau$. The average over noise realizations has been taken over 40 samples.

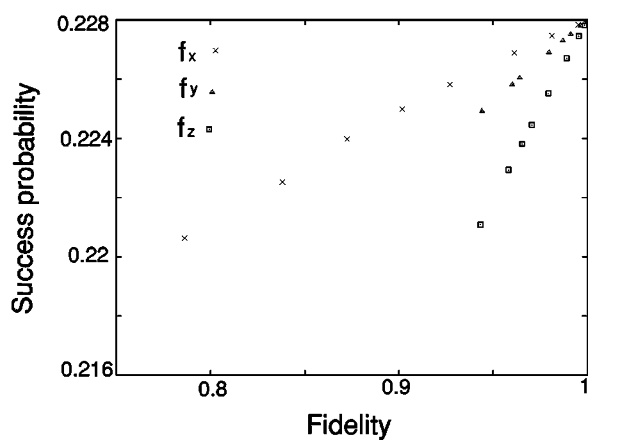

FIG. 11. The success probability vs the fidelity of $|\psi_{\text{ME}}\rangle$, which is a typical AFS, for various strengths of the noises f_x, f_y, f_z. The average over noise realizations has been taken over 200 samples.

been taken over a finite number ($n_\nu = 200$) of samples. The average curves are almost straight for such small λ as assumed in the numerical simulations; namely, for small λ,

$$r_m \simeq \text{const, independent of } \lambda, \text{ for each noise and } m, \tag{60}$$

where r_m is defined by Eq. (59).

For $|\psi_{\rm HT}\rangle$, the rate r_m takes similar values for the three noises. Regarding each of F_m and T_m, on the other hand, the magnitudes of their reductions by f_x are smaller than those by f_y or f_z. This may be understood by noting that $|\psi_{\rm HT}\rangle$ can be rewritten simply as

$$|\psi_{\rm HT}\rangle = |+x,+x,\ldots,+x\rangle^{(1)}|1\rangle^{(2)}, \tag{61}$$

where $|+x,+x,\ldots,+x\rangle^{(1)}$ denotes the simultaneous eigenstate of $\hat{\sigma}_x(1),\hat{\sigma}_x(2),\ldots,\hat{\sigma}_x(L_1)$ with the eigenvalues $+1,+1,\ldots,+1$. It is then clear that the state of R_1 is not changed by f_x which couples to $\hat{\sigma}_x(\ell)$ through the interaction (32), because f_x induces only a random phase factor $e^{i\theta}$ as $|+x,+x,\ldots,+x\rangle^{(1)} \to e^{i\theta}|+x,+x,\ldots,+x\rangle^{(1)}$, which means no change in the quantum state. Hence, the reductions of F_m and T_m of $|\psi_{\rm HT}\rangle$ occur only through the decoherence of the state of R_2, and thus the reductions become small.

For $|\psi_{\rm ME}\rangle$, the reduction of F_m by f_x is larger than that by f_y or f_z. This can be understood from Eq. (48): Through the interaction (38), f_x couples to $\hat{M}_x$, which has an anomalously large fluctuation for this state, whereas f_y and f_z couple to $\hat{M}_y$ and $\hat{M}_z$, respectively, which have normal fluctuations. Therefore, it is confirmed again that the reduction of F_m is simply determined by the fluctuation of $\hat{M}_\alpha$ to which the noise couples. Regarding T_m, on the other hand, there is no significant difference between the magnitudes of the reductions by f_x and f_z, whereas the reduction by f_y is smaller. As a result, r_m takes different values for the three noises.

It seems reasonable to assume that in real systems noises in all directions coexist with similar magnitudes, because noises are uncontrollable, random objects. Then, it may be tempting from Figs. 10 and 11 to say that the effects on the computational result of the noises acting on $|\psi_{\rm HT}\rangle$ and those acting on $|\psi_{\rm ME}\rangle$ would be of the same order of magnitudes. However, to study the performance of computations, we must consider how the effects of noises scale as L is increased. Although L is not so large ($L=15$) in Figs. 10 and 11, it will be much larger in practical applications. In order to satisfy condition (58) for larger L, λ should be made smaller. Suppose that one somehow reduces λ with increasing L in such a way that $1-F_m$ for $|\psi_{\rm HT}\rangle$ is kept constant. According to Eq. (51), this means the following scaling rule:

$$\lambda^2 \propto 1/L. \tag{62}$$

However, according to Eq. (52), $1-F_m$ for $|\psi_{\rm ME}\rangle$ scales in this case as $1-F_m \propto L$. Then, since T_m is a monotonically decreasing function with decreasing F_m, as seen from Fig. 11 and Eq. (60) [31], it is expected that T_m is greatly reduced, approaching zero, with increasing L. Therefore, condition (58) would be violated in practical applications, for which L is large, if λ is scaled as Eq. (62).

This argument is applicable also to other AFSs and NFSs that appear during quantum computations. Therefore, $\min_m T_m$ on the left-hand side of condition (58) is T_m of an AFS, and it is necessary that

$$\lambda^2 \leq O(1/L^2), \tag{63}$$

which is much severer than the naive one (62). This supports conjecture (iii); namely, we conclude that the bottleneck of the quantum computations is the anomalously fast decoherence of AFSs, which appear during quantum computations.

Note that inequality (63) is *not* a sufficient condition, but a necessary condition. We will discuss a sufficient condition in Sec. VIII.

E. Some AFSs may be noncrucial

We have shown that the decoherence of *one* of AFSs appearing in Shor's factoring algorithm is crucial, in consistency with conjecture (iii). Note however that this does *not* mean that decoherence of *all* AFSs appearing in the algorithm were crucial.

For example, consider the final state $|\psi_{\rm final}\rangle$, which has an anomalously large fluctuation of $\hat{M}_z$, whereas the fluctuations of $\hat{M}_x$ and $\hat{M}_y$ take normal values. When a phase-shift noise with $f_z \neq 0, f_x = f_y = 0$ acts on this state, it evolves into

$$|\psi'_{\rm final}\rangle = \frac{1}{2^{L_1}} \sum_{a=0}^{2^{L_1}-1} \sum_{c=0}^{2^{L_1}-1} \exp\left(\frac{2\pi i}{2^{L_1}} ca + i\,\theta(c,a)\right) |\bar{c}\rangle^{(1)} |\mathrm{x}^a \mod N\rangle^{(2)}, \tag{64}$$

where $\theta(c,a)$ is a phase, which depends on c,a, and the noise. Since the probability $P(c)$ of finding a base $|c\rangle^{(1)}$ does not depend on this random phase, T_m for this state is not reduced at all by the phase-shift noise, whereas the fidelity F_m is reduced in proportion to L^2. Therefore, unlike $|\psi_{\rm ME}\rangle$, the anomalously fast decoherence of $|\psi_{\rm final}\rangle$ is not crucial. T_m of this state is reduced only by f_x or f_y, in proportion to L.

VIII. DISCUSSIONS

A. A sufficient condition on λ

Inequality (63) is not a sufficient condition, but a necessary condition. In this section, we discuss a sufficient condition.

In real situations, noises act continuously throughout the computation, as discussed in Sec. VII B. Hence, the success probability T in real situations may be given by

$$T \simeq T_{\rm clean} \prod_m \frac{T_m}{T_{\rm clean}}. \tag{65}$$

For a sufficiently small λ, since $T_{\rm clean} - T_m \propto \lambda^2$, this may be approximated by

$$T \simeq T_{\text{clean}} \exp\left(-\sum_m \frac{T_{\text{clean}} - T_m}{T_{\text{clean}}} \right)$$
$$= T_{\text{clean}} \exp\left[-\lambda^2 \left(\sum_{m \in \text{crucial AFSs}} O(L^2) + \sum_{m \in \text{noncrucial AFSs and NFSs}} O(L) \right) \right]. \tag{66}$$

We have already identified that $|\psi_{\text{ME}}\rangle$ is a crucial AFS. It seems reasonable to assume that AFSs appearing before and after this state, having anomalously large fluctuations of $\hat{M}_x$, should also be crucial AFSs. Figures 1–3 suggest that the number of such AFSs is roughly proportional to the total number of computational steps, Q. As described in Sec. V A, $Q = O(L_1^n) = O(L^n)$, where $n=2$ in our simulation, whereas $n=3$ in an actual computation. Hence, for large L, we can estimate roughly as

$$T \simeq T_{\text{clean}} \exp[-\lambda^2 O(L^{n+2})]. \tag{67}$$

Hence, ϵ defined by Eq. (55) is roughly given by

$$\epsilon \simeq \exp[-\lambda^2 O(L^{n+2})]. \tag{68}$$

To get a successful result within a time of poly($\log N$) $=$poly(L), where poly denotes a polynomial, the lowest allowable value ϵ_{th} of ϵ should be

$$\epsilon_{\text{th}} = 1/\text{poly}(L). \tag{69}$$

Therefore, a sufficient condition would be

$$\lambda^2 = O\left(\frac{\log(L)}{L^{n+2}} \right). \tag{70}$$

For any value of n, we stress that the required condition for λ becomes L ($\gg 1$) times severer due to the appearance of AFSs than the case where only NFSs appear during the computation, and conjecture (iii) has been confirmed.

B. Possible meaning of the appearance of a noncrucial AFS

It seems that macroscopic entanglement is necessary for the exponential speedup over classical computers in performing computation with huge inputs, because otherwise the quantum computation would be able to be simulated efficiently by classical computers. Since AFSs have macroscopic entanglement, they seem necessary for the exponential speedup.

We have shown that both $|\psi_{\text{ME}}\rangle$ and $|\psi_{\text{final}}\rangle$ in Shor's factoring algorithm are AFSs. In agreement with the general theory of SM [5], the decoherence rates of these states become anomalously great as the number L of qubits is increased. However, we have also shown that the anomalously fast decoherence of $|\psi_{\text{final}}\rangle$ is not crucial, i.e., does not reduce the success probability, whereas that of $|\psi_{\text{ME}}\rangle$ is crucial. This may indicate that the use of an AFS in the final stage would be dispensable, whereas the use of an AFS in the modular exponentiation stage would be indispensable, to Shor's factoring algorithm; namely, it might be possible to modify the algorithm in such a way that it does not use an AFS in the final stage, while keeping the number Q of computational steps as $Q = \text{poly}(\log N) = \text{poly}(L)$. On the other hand, it would be impossible to modify the algorithm in such a way that it does not use an AFS in the modular exponentiation stage, while keeping $Q = \text{poly}(\log N)$. This interesting point will be a subject of future studies.

C. A possible method of fighting against anomalously fast decoherence of crucial AFSs

If the use of an AFS in the modular exponentiation stage is indeed indispensable to Shor's algorithm, we must find a way of fighting against the anomalously fast decoherence of such crucial AFSs. A possible solution may be the use of ECC [19–22] and/or a DFS [23–25], which will be mentioned in Sec. VIII E. We here point out another possible solution.

We note that, according to formula (14), an AFS becomes fragile only when the spectrum density of the noise behaves as $g(k_0) = O(L^{-1+\delta})$ with $\delta > 0$. That is, when $|\psi\rangle$ is an AFS for which $\langle \psi | \Delta \hat{A}_{k_0}^\dagger \Delta \hat{A}_{k_0} | \psi \rangle = O(L^0)$, and when the spectrum density of the noise at $k = k_0$ behaves as $g(k_0) = O(L^{-1+\delta})$, then $|\psi\rangle$ becomes fragile if $\delta > 0$ or nonfragile if $\delta \leq 0$. For example, if the physical dimension of the quantum computer is 1 cm, and if the wavelengths of all noises are longer than 1 cm, the spectral densities of the noises behave like Eq. (15). In such long-wavelength noises, AFSs with $k_0 = 0$ become fragile, whereas AFSs with $k_0 \gg 1\,\text{cm}^{-1}$ are nonfragile. Therefore, we would be able to avoid anomalously fast decoherence in such long-wavelength noises if we can improve the algorithm in such a way that crucial AFSs are replaced with other AFSs with $k_0 \gg 1\,\text{cm}^{-1}$.

For example, we have shown that $|\psi_{\text{ME}}\rangle$ is a crucial AFS that is fragile in a long-wavelength, bit-flip noise. In order to realize quantum computers with large L, one should improve the algorithm in such a way that $|\psi_{\text{ME}}\rangle$ is replaced with another AFSs with $k_0 \gg 1\,\text{cm}^{-1}$. Since the construction of such an improved algorithm is beyond the scope of the present paper, we will study it elsewhere.

D. Possibilities of other AFSs and other noises

As normalized additive operators, we have only examined the "magnetizations" $\hat{M}_\alpha$ and $\hat{M}_\alpha^{(1)}$ with $\alpha = x, y, z$. This is sufficient for the purpose of the present paper, as explained in Sec. V B. However, it would be interesting to find out all AFSs used in the algorithm. To do this, we must study fluctuations of *all* normalized additive operators. A convenient method of doing this has recently been proposed by Sugita and Shimizu, and has been applied to quantum chaotic systems [13]. It would be very interesting to apply their method to quantum computers, and thereby make a complete list of anomalous states used in the quantum computation.

To examine the anomalously fast decoherence of AFSs with anomalously large fluctuations of $\hat{M}_\alpha$, we have considered long-wavelength noises. In real systems, it seems reasonable to assume that many different noises and/or components (wavelengths, frequencies, and directions) coexist. It would be necessary to examine effects of all existing noises to realize a quantum computer with a huge number L of qubits, because, as we have shown in this paper, for huge L some noises can be crucial even if its strength is much weaker than other noises.

These points will be subjects of future studies.

E. Uses of error correcting codes and/or a decoherence-free subspace

We have studied Shor's factoring algorithm without ECC [19–22] or error avoiding using a DFS [23–25]; namely, we have studied "bare" characteristics of quantum computers performing Shor's algorithm.

Regarding the use of a DFS, it will be effective for fighting against the long-wavelength noises f_α that are considered in this paper. However, as mentioned in the preceding section, many different noises and/or components would coexist in real systems. It is not clear whether a DFS can be constructed efficiently in such a realistic case, because the number of extra qubits that are necessary to construct a DFS is increased as the number of different noises and/or components is increased [23,24]. Also, at present, we do not have definite conclusions on the efficiency of ECC in such a realistic case. We can, however, say that the improvement of the bare characteristics is crucial in practical applications, because if the bare characteristics are bad, then ECC would become much complicated and large scale. Such a computer system would be impractical.

Therefore, we think that all of ECC, a DFS, and the improvement of the bare characteristics should be necessary to realize a quantum computer that accept huge inputs.

F. Various definitions of decoherence

The decoherence and decoherence rate can be defined in many different ways. The definition of Γ_m of the present paper, Eq. (49), is one of many possible definitions. Fortunately, however, we are interested in the case of small λ in this paper. In such a case, we can obtain similar conclusions for many different definitions of the decoherence rate. Indeed, we have shown in Sec. VI B that the loss of fidelity and the increase of the α entropy agree with each other for small λ.

Note, however, that the situation could be different if one employed some definitions used in condensed-matter physics. In condensed-matter physics, decoherence is often discussed with respect to a particular quantity, such as the line shape [32] and a nonequilibrium noise [33]. In quantum information theory, on the other hand, the decoherence is usually defined with respect to all possible observable. The decoherence in the latter sense can take place without any change of the (expectation) value of a particular quantity. This point should be considered when using rich results of condensed-matter physics.

IX. SUMMARY AND CONCLUSIONS

With the help of the general theory of stabilities of many-body quantum states by SM [5], we have studied properties of quantum states in quantum computers that perform Shor's factoring algorithm [2]. Since the efficiency of computation becomes relevant only when the size N of the input is huge, we focus on asymptotic behaviors as the number L $[=O(\log N)]$ of qubits is increased.

Following the general theory by SM, we have paid attention to fluctuations of normalized additive operators, which are the sums of local operators, as defined by Eq. (1). If fluctuation $\langle \psi|(\Delta\hat{A})^2|\psi\rangle$ of every normalized additive operator $\hat{A}$ is $O(1/L)$ or less for a pure state $|\psi\rangle$, we call it a normally fluctuating state (NFS). Any separable state is a NFS, whereas the inverse is not necessarily true. On the other hand, if there is a normalized additive operator whose fluctuation is $O(L^0)$ for a pure state $|\psi\rangle$, we call $|\psi\rangle$ an anomalously fluctuating state (AFS). Since AFSs have such anomalously large fluctuations, they are entangled macroscopically. We have pointed out in Sec. II C that the use of fluctuations of normalized additive operators as a measure of macroscopic entanglement seems natural from the viewpoints of many-body physics and experiments.

By performing numerical simulations of Shor's factoring algorithm, we have found that AFSs appear during the computation, although the initial state is a NFS. For example, the state $|\psi_{\rm ME}\rangle$ just after the modular exponentiation process is an AFS, which has anomalously large fluctuation of $\hat{M}_x$. Here, $\hat{M}_x$ is the $\alpha = x$ component of $\hat{M}_\alpha$ that is defined by Eq. (27), which corresponds to the magnetization of a spin system. The final state $|\psi_{\rm final}\rangle$, which is obtained by a discrete Fourier transform, is also an AFS, which has anomalously large fluctuation of $\hat{M}_z$ (the $\alpha = z$ component of $\hat{M}_\alpha$).

According to the general theory by SM, the asymptotic behavior, as L is increased, of the decoherence rate Γ of a quantum state is directly related to fluctuations of normalized additive operators: Γ of a NFS never exceeds $O(L)$ in any weak classical noises, whereas Γ of an AFS can be either $O(L^2)$ or less, depending on the spectral densities of the noises. An AFS with an anomalously great decoherence rate $\Gamma = O(L^{1+\delta})$, where $\delta > 0$, is said to be fragile. We have shown that AFSs which we have found in Shor's algorithm become fragile, $\Gamma = O(L^2)$, in long-wavelength noises with a $1/f$ spectrum, which simulate noises in some real systems. Therefore, for large L, the decoherence rate of a quantum computer performing Shor's factoring algorithm is determined by the decoherence rates of the fragile AFSs that appear during the computation.

Since decoherence of particular states does not necessarily lead to false results of the quantum computation, we examine whether the anomalously fast decoherence of the fragile AFSs leads to anomalously large degradation of the result of computation. To do this, we have investigated effects of the noises on the computational results for each state. We have found that the anomalously fast decoherence, $\Gamma = O(L^2)$, of $|\psi_{\rm ME}\rangle$ leads to anomalously large reduction, approximately proportional to L^2, of the success probability T, which is defined as the probability of getting the correct result of computation. We have concluded that the anomalously fast decoherence of such crucial AFSs becomes a bottleneck of quantum computers performing Shor's factoring algorithm.

This does not however mean that all AFSs appearing in the algorithm are crucial. For example, the anomalously fast decoherence, $\Gamma = O(L^2)$, of $|\psi_{\text{final}}\rangle$ does not lead to a large reduction of *T*. In this sense, $|\psi_{\text{final}}\rangle$ is a noncrucial AFS in Shor's factoring algorithm.

It seems that macroscopic entanglement is necessary for the exponential speedup over classical computers in performing computation with huge inputs, because otherwise the quantum computation would be able to be simulated efficiently by classical computers. Since AFSs have macroscopic entanglement, they seem necessary for the exponential speedup. This does not however mean that all AFSs in an algorithm written naively are necessary. For Shor's factoring algorithm, our results suggest that a crucial AFS $|\psi_{\text{ME}}\rangle$ is necessary whereas a noncrucial AFS $|\psi_{\text{final}}\rangle$ may be able to be replaced with a NFS. In order to realize quantum computers with large *L*, one should improve the algorithm in such a way that necessary but fragile AFSs are replaced with other AFSs that are nonfragile in real noises. To do this, formula (14) will be useful, from which one can estimate Γ of an AFS. Since error correcting codes and decoherence-free subspaces are not almighty, we think that one must also utilize such optimization to realize a quantum computer that accepts huge inputs.

ACKNOWLEDGMENTS

We thank T. Miyadera for fruitful discussions and comments. This work was supported by Grant-in-Aid for Scientific Research.

[1] D. Deutsch, Proc. R. Soc. London, Ser. A **400**, 97 (1985).
[2] P.W. Shor, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, edited by S. Goldwasser (IEEE Computer Society, Los Alamitos, CA, 1994), p. 124.
[3] A. Ekert and R. Jozsa, Rev. Mod. Phys. **68**, 733 (1996).
[4] M.A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[5] A. Shimizu and T. Miyadera, Phys. Rev. Lett. **89**, 270403 (2002).
[6] R. Haag, *Local Quantum Physics* (Springer, Berlin, 1992).
[7] W.G. Unruh, Phys. Rev. A **51**, 992 (1995).
[8] G.M. Palma, K.-A. Suominen, and A.K. Ekert, Proc. R. Soc. London, Ser. A **452**, 567 (1996).
[9] C. Miquel, J.P. Paz, and R. Perazzo, Phys. Rev. A **54**, 2605 (1996).
[10] P. Horsh and W. von der Linden, Z. Phys. B: Condens. Matter **72**, 181 (1988).
[11] T. Koma and H. Tasaki, J. Stat. Phys. **76**, 745 (1994).
[12] A. Shimizu and T. Miyadera, Phys. Rev. E **64**, 056121 (2001).
[13] A. Sugita and A. Shimizu, e-print quant-ph/0309217.
[14] On the other hand, a disadvantage of the present measure of entanglement is that it can only be applied to pure states.
[15] For example, a ground state in which a continuous symmetry is broken often takes such a value of *p* because of the Nambu-Goldstone modes.
[16] Since the noise amplitude outside the qubit system is irrelevant, the spatial Fourier transform is taken over $\ell = 1,2,\ldots,L$ to define $g(k,\omega)$, hence *k* takes discrete values with separation $2\pi/L$.
[17] A. Miyake and M. Wadati, Phys. Rev. A **64**, 042317 (2001).
[18] R. Jozsa and N. Linden, e-print quant-ph/0201143.
[19] P.W. Shor, Phys. Rev. A **52**, R2493 (1995).
[20] A. Ekert and C. Macchiavello, Phys. Rev. Lett. **77**, 2585 (1996).
[21] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
[22] J. Preskill, Phys. Today **52**(6), 24 (1999).
[23] P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).
[24] D.A. Lidar, I.L. Chuang, and K.B. Whaley, Phys. Rev. Lett. **81**, 2594 (1998).
[25] D. Kielpinski *et al.*, Science **291**, 1013 (2001).
[26] One can check whether x is coprime to *N* easily by a classical computer.
[27] M. Covington, M.W. Keller, R.L. Kautz, and J.M. Martinis, Phys. Rev. Lett. **84**, 5192 (2000).
[28] R.L. Kautz, M.W. Keller, and J.M. Martinis, Phys. Rev. B **62**, 15888 (2000).
[29] Y. Nakamura, Yu.A. Pashkin, T. Yamamoto, and J.S. Tsai, Phys. Rev. Lett. **88**, 047901 (2002).
[30] $1/f$ noises do not strictly satisfy the assumptions of Ref. [5]. This does not cause any difficulty in the present paper, as discussed at the end of Sec. VI B.
[31] Although the relation between $T_{\text{clean}} - T_m$ and $1 - F_m$ becomes nonlinear for larger λ and/or larger *L*, we confirmed that the relation is still monotonic.
[32] P.W. Anderson and P.R. Weiss, Rev. Mod. Phys. **25**, 269 (1953).
[33] A. Shimizu and M. Ueda, Phys. Rev. Lett. **69**, 1403 (1992); **86**, 3694(E) (2001).
[34] A Shimizu, talk presented at the 4th Symposium on Quantum Effects and Related Physical Phenomena, Tokyo, Japan, 2000 (unpublished); A Shimizu and T. Miyadera, in *Proceedings of the 56th Annual Meeting of the Physical Society of Japan* (Physical Society of Japan, Tokyo, 2001), paper no. 28pYN-6.