Necessity of Superposition of Macroscopically Distinct States for Quantum Computational Speedup

Akira Shimizu* and Akihisa Ukena
Department of Basic Science, University of Tokyo, 3-8-1 Komaba, Tokyo 153-8902, Japan

Yuichiro Matsuzaki
Department of Basic Science, University of Tokyo, 3-8-1 Komaba, Tokyo 153-8902, Japan and
Department of Material, University of Oxford, OX1 3PH, United Kingdom
(Dated: September 28, 2010)

For quantum computation, we investigate the conjecture that superposition of macroscopically distinct states is necessary for large quantum speedup. Although this conjecture was supported for a circuit-based quantum computer performing Shor's factoring algorithm (A. Ukena and A. Shimizu, Phys. Rev. A **69**, 022301 (2004)), it needs to be generalized in order to apply to wide classes of algorithms and/or other models (such as measurement-based quantum computers). To treat such general cases, we first generalize the indices for superposition of macroscopically distinct states. We then generalize the conjecture, using the generalized indices, in such a way that it is applicable unambiguously to general models if a quantum algorithm achieves exponential speedup. Based on this generalized conjecture, we further extend the conjecture to Grover's quantum search algorithm, whose speedup is large but quadratic. It is shown that this extended conjecture is also correct for Grover's algorithm. Since Grover's algorithm is a representative algorithm for unstructured problems, the present result further supports the conjecture.

PACS numbers: 03.67.Lx, 03.67.Mn

I. INTRODUCTION

We consider quantum speedup for solving computational problems of size L bits, such as the factoring problem (for which L is the size of the number to be factored) and the search problem (L is the size of the solution space). In the well-known quantum algorithms of Shor [1, 2] and Grover [3], such problems are solved using quantum computers whose number of qubits $\mathcal{L} \geq L$ [1–4]. Since quantum speedup becomes relevant for large L, such quantum computers are many-body quantum systems with a large number of qubits $\mathcal{L}$. Since there are many types (and corresponding measures or indices) of entanglement for many-body systems [5–13], it is interesting to explore which types of entanglement are relevant to large quantum speedup over classical computations [14–21].

This issue has been studied extensively, particularly on Shor's factoring algorithm [1, 2] and Grover's quantum search algorithm [3]. For example, Parker and Plenio demonstrated that the bipartite entanglement as measured by the logarithmic negativity is an intrinsic part of Shor's algorithm [14]. Shimoni, Shapiro and Biham showed that highly entangled states are generated in both algorithms [15, 16]. Orús and Latorre studied scaling of entanglement in three algorithms including Shor's and Grover's [17].

For general algorithms, a few necessary conditions were derived for computational speedup over classical computations. Jozsa and Linden showed that for exponential speedup a state is necessary which cannot be factored into a direct product of states of at most a constant number of qubits [18]. Vidal showed that a necessary condition for exponential speedup is that the amount of the bipartite entanglement between one part and the rest of the qubits increases with L [19].

We note that one can get a stricter condition by taking the product of these and other necessary conditions, which may be obtained by studying other types of entanglement. Such a stricter condition would lead to deeper understanding of quantum computations. Hence, it is important to seek for more conditions which are necessary for quantum computational speedup.

As a possible necessary condition, one of the authors conjectured that superposition of macroscopically distinct states would be necessary for quantum computational speedup (Ref. [20] and Sec. III). Although 'superposition of macroscopically distinct states' was only ambiguously defined until recently, clear definition and the corresponding index p ($1 \leq p \leq 2$) for pure states were proposed in Refs. [11, 12], according to which a pure state has superposition

*Electronic address: shmz@ASone.c.u-tokyo.ac.jp; URL: http://as2.c.u-tokyo.ac.jp

of macroscopically distinct states if and only if $p = 2$. The generalization to mixed states was made in Ref. [22], in which p is generalized to an index q ($1 \leq q \leq 2$) ; a mixed state has superposition of macroscopically distinct states if and only if $q = 2$. For pure states, $p = 2$ implies $q = 2$ and vice versa [22]. [For mixed states, p is undefined.]

The entanglement possessed by superposition of macroscopically distinct states is totally different from bipartite entanglement which was studied in the previous works [18, 19]. [Hence, it was called 'macroscopic entanglement' in Refs [12, 13, 22, 23]. However, we do not use this term in this paper because the same term is used in other senses by other authors.] For example, some pure states with $p = 2$ (such as the GHZ state) have very small bipartite entanglement whereas some other states with $p = 1$ (such as energy eigenstates of many-body chaotic systems) have very large bipartite entanglement [12, 13]. Therefore, *simultaneous* requirement (for quantum computational speedup) of the superposition of macroscopically distinct states *and* large bipartite entanglement is much stronger than the requirement of either one of them.

For a circuit-based quantum computer performing Shor's factoring algorithm [1, 2], we obtained results that support the above conjecture in the previous paper [21]. It is interesting to study the correctness of the conjecture in other algorithms and/or other models (such as measurement-based quantum computers). To explore such general cases unambiguously, however, the conjecture needs to be generalized. For example, quantum states in quantum computers are not only *inhomogeneous* but also *dependent on instances* (i.e., different for different questions of a given problem). Since the indices p and q assumed a family of similar states that are spatially homogeneous, the conjecture (which was based on p or q) is not strictly applicable to such a general family of states, in its original form.

Furthermore, since Shor's algorithm is a representative quantum algorithm for solving structured problems [4], it is very interesting to study whether the conjecture is correct in the case of quantum algorithms for solving *unstructured* problems. However, the quantum speedup achieved by Grover's quantum search algorithm [3], which is a representative algorithm for unstructured problems [4], is not exponential but quadratic. The conjecture, in its original form, did not assume speedup of such a degree.

In this paper, we first generalize the indices p and q to treat general algorithms and models. We then generalize the conjecture, using the generalized indices, in such a way that it is applicable unambiguously to general models if a quantum algorithm achieves exponential speedup. Based on this generalized conjecture, we further extend the conjecture to the quadratic speedup of Grover's quantum search algorithm. It is shown that this extended conjecture is also correct for Grover's algorithm. To show details of evolution of superposition of macroscopically distinct states, we also perform numerical simulations of a quantum computer that performs Grover's quantum search algorithm.

This paper is organized as follows. In Sec. II, we generalize the indices p and q. Section III is devoted to generalize and further extend the conjecture. Analytic results for Grover's quantum search algorithm are given in Sec. IV, where we will prove that the extended conjecture is correct for Grover's algorithm. We present results of numerical simulations of a quantum computer that performs Grover's quantum search algorithm in Sec. V. Discussions and summary are given in Sec. VI.

II. INDICES OF SUPERPOSITION OF MACROSCOPICALLY DISTINCT STATES

The indices of superposition of macroscopically distinct states were proposed and studied for pure states in Refs. [11, 12, 23], and for mixed states in Ref. [22]. To study these indices for states in quantum computers, we here generalize their definitions, because, as will be illustrated explicitly in Secs. IV and V, quantum states in quantum computers are not only inhomogeneous but also dependent on instances. Here, an *instance* is a particular question of a given problem. The physical meanings and implications of the indices will also be described briefly in this section.

A. Index for a family of pure states

Let $|\psi_\nu(L)\rangle$'s be pure states of a system of size L, which are labeled by an index ν, e.g., as $|\psi_1(L)\rangle, |\psi_2(L)\rangle, |\psi_3(L)\rangle, \cdots$. For each value of L, the range of ν is given, for example as $\nu = 1, 2, \ldots, 2^L$. In a quantum computer which solves a decision problem, L corresponds to the size of a certain register, which is usually proportional to the size of the input of the problem, and ν labels various inputs (see later sections). We do *not* assume that $\langle\psi_\nu(L)|\psi_{\nu'}(L)\rangle = 0$ for $\nu \neq \nu'$. We consider a family F of $|\psi_\nu(L)\rangle$'s,

$$F \equiv \{|\psi_\nu(L)\rangle \mid \text{all } \nu\text{'s, all } L\}, \tag{1}$$

which we abbreviate to $\{|\psi_\nu(L)\rangle\}_{L,\nu}$.

In general, a quantum computer consists of a large number of small quantum systems, such as qubits, which are distributed spatially. We call each small quantum system a *site*, and an operator acting on a single site a *local operator*.

To avoid mathematical complexities, we limit ourselves to the case where every local operator is bounded (i.e., its norm is finite).

Let $\hat{a}(l)$ be a local operator on site l. We normalize it as $\|\hat{a}(l)\| = 1$. Although this normalization condition might look too restrictive at first sight, it actually imposes only a weak restriction that makes the maximization operation in Eq. (5) well-defined [24], as discussed in Appendix A.

Note that we can use either $\|\hat{a}\|_E$ or $\|\hat{a}\|_H$ as the operator norm $\|\hat{a}\|$, where

$$\|\hat{a}\|_E \equiv \sup_{\||\psi\rangle\|=1} \|\hat{a}|\psi\rangle\|, \tag{2}$$

$$\|\hat{a}\|_H \equiv \sqrt{(\hat{a},\hat{a})}, \tag{3}$$

and $(\hat{a},\hat{b}) \equiv \mathrm{Tr}(\hat{a}^\dagger\hat{b})$ denotes the inner product of operators $\hat{a}$ and $\hat{b}$. In fact, both definitions give the same value of the index p, because $\|\hat{a}(l)\|_E \le \|\hat{a}(l)\|_H \le \sqrt{d}\|\hat{a}(l)\|_E$ and $\|\hat{a}(l)\|_H/\sqrt{d} \le \|\hat{a}(l)\|_E \le \|\hat{a}(l)\|_H$, where d is the dimension of the Hilbert space of a single site.

By the same symbol $\hat{a}(l)$ we also denote $\hat{a}(l) \otimes \bigotimes_{l'(\neq l)} \hat{1}(l')$, which is an operator on the Hilbert space $\mathcal{H}$ of the total system, where $\hat{1}(l')$ is the identity operator acting on site l'. Using this notation, we define an *additive operator* $\hat{A}(L)$ as the sum of local operators [11, 22];

$$\hat{A}(L) = \sum_{l=1}^{L} \hat{a}(l) \quad (\|\hat{a}(l)\| = 1). \tag{4}$$

Here, we do *not* assume that $\hat{a}(l')$ $(l' \neq l)$ is a spatial translation of $\hat{a}(l)$.

To simplify notation, we express the expectation value in $|\psi_\nu(L)\rangle$ as $\langle\cdot\rangle_{L\nu}$. We also use the symbols O, Ω, Θ to describe asymptotic behaviors according to Ref. [4], as summarized in Appendix B. Furthermore, as described in Appendix B, a family $\{f_\nu(L)\}_{L,\nu}$ of non-negative functions of L is said to be $\overline{\Theta}(g(L))$ if $f_\nu(L)$ is $\Theta(g(L))$ *for almost every* ν, i.e., apart from possible exceptional ν's whose measure (i.e., the number of such ν's divided by the total number of ν's) vanishes as L goes to infinity.

For each state $|\psi_\nu(L)\rangle$, consider fluctuation $\langle\Delta\hat{A}(L)^\dagger\Delta\hat{A}(L)\rangle_{L\nu}$, where $\Delta\hat{A}(L) \equiv \hat{A}(L) - \langle\hat{A}(L)\rangle_{L\nu}$. Its magnitude depends on $\hat{A}(L)$, i.e., on the choice of $\hat{a}(l)$'s. Since $\|\hat{A}(L)\|$ is upper-bounded, there exists the maximum value, $\max_{\hat{A}(L)}\langle\Delta\hat{A}(L)^\dagger\Delta\hat{A}(L)\rangle_{L\nu}$. The maximum value is taken for some additive operator $\hat{A}_{\max}(L)$, which we call the *most fluctuating additive operator*. Using the maximum value, which depends on L and ν, we define the index p of the family F $(= \{|\psi_\nu(L)\rangle\}_{L,\nu})$ as the positive number (if it exists) that satisfies

$$\max_{\hat{A}(L)} \langle\psi_\nu(L)|\Delta\hat{A}(L)^\dagger\Delta\hat{A}(L)|\psi_\nu(L)\rangle = \overline{\Theta}(L^p). \tag{5}$$

Note that p does not necessarily exist for a general family. If p exists for a given family, we can show (see Appendix C) that

$$1 \le p \le 2. \tag{6}$$

When a family $\{|\psi_\nu(L)\rangle\}_{L,\nu}$ has $p = 2$ (or $p = 1$, etc), we also say simply that 'almost every state $|\psi_\nu(L)\rangle$ has $p = 2$ (or $p = 1$, etc).'

The present definition of p contains those of the previous works, Refs. [11–13, 23], as special cases. In fact, Refs. [11, 12, 23] treated homogeneous states, for which $|\psi(L+1)\rangle$ was simply defined as the enlarged state of $|\psi(L)\rangle$. For example, when $|\psi(L)\rangle = |00\cdots0\rangle + |11\cdots1\rangle$ with L sites, then $|\psi(L+1)\rangle = |000\cdots0\rangle + |111\cdots1\rangle$ with $(L+1)$ sites. According to the present general definition of p, such a case corresponds to a family whose members for each L are identical, i.e., $|\psi_\nu(L)\rangle = |\psi(L)\rangle$ for all ν. Moreover, Ref. [13] treated energy eigenstates of homogeneous chaotic systems. Since *each* energy eigenstate is *inhomogeneous* spatially, this case is different from the case of homogeneous states. According to the present definition of p, it corresponds to a family composed of all energy eigenstates in a certain energy interval. Therefore, p defined here is a natural generalization of p of the previous works, Refs. [11–13, 23].

The physical meaning of the present p is basically the same as the p of these previous works. That is, almost every state of a family with $p = 2$ contains superposition of states with macroscopically distinct values of some additive operator(s) [11–13, 23]. We call such an additive operator(s) a *macroscopically-fluctuating additive operator(s)* of the state (or family). For example, when $|\psi_\nu(L)\rangle = |00\cdots0\rangle + |11\cdots1\rangle$ for all ν then its macroscopically-fluctuating additive operator is $\sum_l \hat{\sigma}_z(l)$, which corresponds to the z component of the total magnetization of a

magnetic substance. Since additive operators are macroscopic dynamical variables [11, 22], two (or more) states are macroscopically distinct from each other if they have macroscopically distinct values of an additive operator. Therefore, one can state definitely that a state with $p = 2$ contains superposition of macroscopically distinct states.

To illustrate how p is useful and necessary for identifying such superposition, we give a few simple examples in Appendix D.

In the present general definition of p, a macroscopically-fluctuating additive operator(s) of a given family can be different for different L and ν, unlike the case of homogeneous states treated in Refs. [11, 12, 23]. Therefore, we can say the following: *For a given family of pure states, if there exists a family of additive operators*

$$\{\hat{A}_\nu(L) \mid \textit{all } \nu\textit{'s, all } L\} \tag{7}$$

such that

$$\langle \Delta\hat{A}_\nu(L)^\dagger \Delta\hat{A}_\nu(L)\rangle_{L\nu} = \overline{\Theta}(L^2), \tag{8}$$

then the family has $p = 2$. This means that almost all states of the family contain superposition of states that have macroscopically distinct values of some additive operator(s).

It is worth mentioning that there often exist two or more families of such operators, even for a family of homogeneous states [12, 23].

B. Index for a family of mixed states

The index p, which is defined only for pure states, is sufficient for the concrete analyses in Secs. IV and V. However, to state our conjecture in a general form, we need a more general index which is applicable to mixed states. For example, measurement-based quantum computers [25, 26] often have a larger number of qubits than corresponding circuit-based computers. Hence, in such computers, superposition of macroscopically distinct states might appear as a mixed state of a subset of qubits [27]. Fortunately, generalization of p to mixed states has been made in Ref. [22], in which a generalized index q was proposed for homogeneous mixed states. We here generalize it to families of more general mixed states in order to apply q to wide classes of quantum computers.

For an additive operator $\hat{A}(L)$, as given by Eq. (4), and a projection operator $\hat{\eta}$ on $\mathcal{H}$, satisfying $\hat{\eta}^2 = \hat{\eta}$, we define the following Hermitian operator;

$$\hat{C}_{\hat{A}\hat{\eta}} \equiv [\hat{A}, [\hat{A}, \hat{\eta}]] = \hat{A}^2\hat{\eta} - 2\hat{A}\hat{\eta}\hat{A} + \hat{\eta}\hat{A}^2. \tag{9}$$

For a family $\{\hat{\rho}_\nu(L)\}_{L,\nu}$ of mixed states, which are not necessarily homogeneous spatially, we define the index q as the positive number (if it exists) that satisfies

$$\max\left\{L,\ \max_{\hat{A},\hat{\eta}}\langle C\rangle_{L\nu}\right\} = \overline{\Theta}(L^q), \tag{10}$$

where $\max_{\hat{A},\hat{\eta}}$ is taken over all possible choices of $\hat{A}$ and $\hat{\eta}$. If this q exists for a given family we can show (by slightly generalizing the proof in Ref. [22]) that

$$1 \le q \le 2. \tag{11}$$

We say a family $\{\hat{\rho}_\nu(L)\}_{L,\nu}$ of mixed states contains superposition of macroscopically distinct states if and only if q exists and $q = 2$. We also say that almost every $\hat{\rho}_\nu(L)$ of such a family contains superposition of macroscopically distinct states. For pure states, this is consistent with the corresponding statement based on p, because we can show (following the proof in Ref. [22]) that for pure states $p = 2$ implies $q = 2$ and vice versa.

The case of Ref. [22] corresponds to the special case where $\hat{\rho}_\nu(L)$'s are homogeneous and independent of ν and $\hat{\rho}_\nu(L+1)$ is simply the enlarged state of $\hat{\rho}_\nu(L)$. In such a case, q defined here reduces to q of Ref. [22].

C. Properties of states with $p = 2$ or $q = 2$

As application of general theory of Ref. [11], the index p was studied for many-magnon states in Ref. [12], for energy eigenstates of many-body chaotic systems in Ref. [13], and for typical many-body states in Ref. [23]. Comparison with a measure of bipartite entanglement were also made in these references. Most importantly, many states were

found (such as energy eigenstates of a chaotic system) such that they are almost maximally entangled in the bipartite measure but their p is minimum, $p = 1$. Many other states (such as the GHZ state) are also found such that their p is maximum, $p = 2$, but their bipartite entanglement is small. Therefore, the aspect of entanglement which is detected by p or q is completely different from that detected by the bipartite measure. Furthermore, it has been shown in Ref. [22] that a family of states with $q = 2$ has a strong L-point correlation, which is $\Theta(L)$ times larger than that of any separable states. Note that any measure of bipartite entanglement can*not* detect such a strong L-point correlation for mixed states. On the other hand, the index q does not detect entanglement generated by a small number of Bell pairs, whereas measures of bipartite entanglement do. These facts demonstrate that *the index q is complementary to the measures of bipartite entanglement*.

Note that p is calculated from *two-point* correlations because fluctuation of an additive operator is the sum of two-point correlations;

$$\langle \Delta \hat{A}(L)^\dagger \Delta \hat{A}(L) \rangle_{L\nu} = \sum_{l=1}^{L} \sum_{l'=1}^{L} \langle \Delta \hat{a}(l)^\dagger \Delta \hat{a}(l') \rangle_{L\nu}. \tag{12}$$

However, this does *not* mean that p is related *only* to two-point correlations, because, as mentioned above, pure states with $p = 2$ have $q = 2$, which means a strong L-point correlation. That is, given the knowledge that a family consists of pure states one can say that if the family has $p = 2$ then it has a strong L-point correlation.

It was shown in Ref. [11] that p is directly related to fundamental stabilities of many-body states against decoherence and local measurements. Regarding decoherence by weak noises, it was shown that for any state with $p = 1$ its decoherence rate Γ by *any* noises *never* exceeds $O(L)$. For a state with $p = 2$, on the other hand, it is possible in principle to construct a noise or environment that makes Γ of the state $\Theta(L^2)$. However, this does *not* necessarily mean that such a fatal noise or environment does exist in real physical systems; it depends on physical situations [11]. A more fundamental stability is the stability against local measurements, which was proposed and defined in Refs. [11, 28]. From the theorem proved there, we can say that a state with $p = 2$ is *unstable* against local measurements, i.e., there exists a *local* observable by measurement of which the state changes drastically [29].

Furthermore, a quite singular property was proved rigorously in Ref. [11]; any *pure* state with $p = 2$ in a *finite* system of size L does *not* approach a pure state in an *infinite* system as $L \to \infty$. For readers who are not familiar with quantum theory of infinite systems [30], we give a brief explanation for this fact in Appendix E.

These observations indicate that states with $p = 2$ or $q = 2$ are quite anomalous many-body states. This led to the conjecture of Ref. [20], which will be generalized in Sec. III of the present paper.

D. Efficient method of identifying superposition of macroscopically distinct states

Evaluation of a measure or index of entanglement often becomes intractable for large L. Fortunately, this is not the case for p because there is an efficient method of calculating p [12, 13, 23]. Since this method assumed homogeneous states, we here generalize it to study general families of pure states.

In this subsection, the dimension d of the local Hilbert space is arbitrary, and we employ $\|\hat{a}\|_H$ defined by Eq. (3) as the operator norm $\|\hat{a}\|$.

Let $\{\hat{b}_0(l), \hat{b}_1(l), \cdots, \hat{b}_D(l)\}$ be a complete orthonormal basis set of operators on site l, where $\hat{b}_0(l) = \hat{1}(l)/\sqrt{d}$ and $D \equiv d^2 - 1$. We expand $\hat{a}(l)$ as

$$\hat{a}(l) = \sum_{\alpha=0}^{D} c_{l\alpha} \hat{b}_\alpha(l), \quad \sum_{\alpha=0}^{D} |c_{l\alpha}|^2 = 1, \tag{13}$$

where the latter equality comes from $\|\hat{a}(l)\|_H = 1$. Let $\Delta\hat{a}(l) \equiv \hat{a}(l) - \langle \hat{a}(l) \rangle_{L\nu}$ and $\Delta\hat{b}_\alpha(l) \equiv \hat{b}_\alpha(L) - \langle \hat{b}_\alpha(L) \rangle_{L\nu}$. Note that $\Delta\hat{b}_\alpha(l)$'s, unlike $\hat{b}_\alpha(l)$'s, are *not* necessarily orthogonal to each other.

Since $\Delta\hat{b}_0(l) = 0$, terms with $\alpha = 0$ do not contribute to $\Delta\hat{A}(L) = \sum_l \Delta\hat{a}(l)$, i.e., it can be expanded as

$$\Delta \hat{A}(L) = \sum_{l=1}^{L} \sum_{\alpha=1}^{D} c_{l\alpha} \Delta \hat{b}_\alpha(l), \quad \sum_{\alpha=1}^{D} |c_{l\alpha}|^2 \le 1. \tag{14}$$

As a result, $\sum_l \sum_{\alpha=1}^{D} |c_{l\alpha}|^2 \le L$. Since this normalization is not convenient, we temporarily consider another operator

$\Delta\hat{A}'$ whose expansion coefficients are *normalized*;

$$\Delta\hat{A}'(L) = \sum_{l=1}^{L}\sum_{\alpha=1}^{D} c'_{l\alpha}\Delta\hat{b}_\alpha(l), \quad \sum_{l=1}^{L}\sum_{\alpha=1}^{D}|c'_{l\alpha}|^2 = L. \tag{15}$$

Here, we do *not* require that $\sum_{\alpha=1}^{D}|c'_{l\alpha}|^2 = 1$ for every l. The fluctuation of such an operator is calculated as

$$\langle\Delta\hat{A}'(L)^\dagger\Delta\hat{A}'(L)\rangle_{L\nu} = \sum_{l=1}^{L}\sum_{\alpha=1}^{D}\sum_{l'=1}^{L}\sum_{\alpha'=1}^{D} c'^{*}_{l\alpha}c'_{l'\alpha'}V_{l\alpha,l'\alpha'}(L,\nu) \tag{16}$$

for each $|\psi_\nu(L)\rangle$. Here, for $\alpha,\alpha' = 1,2,\cdots,D$ and $l,l' = 1,2,\cdots,L$, we have defined

$$V_{l\alpha,l'\alpha'}(L,\nu) \equiv \langle\Delta\hat{b}^\dagger_\alpha(l)\Delta\hat{b}_{\alpha'}(l')\rangle_{L\nu}, \tag{17}$$

which can be regarded as elements of a $DL\times DL$ Hermitian matrix, which we call the *variance-covariance matrix* (VCM). Therefore, for each $|\psi_\nu(L)\rangle$,

$$\max_{\hat{A}'(L)}\langle\Delta\hat{A}'(L)^\dagger\Delta\hat{A}'(L)\rangle_{L\nu} = e_{\max}(L,\nu)L, \tag{18}$$

where $e_{\max}(L,\nu)$ is the maximum eigenvalue of the VCM. This and Eq. (5) suggest that the following index p_e should be useful:

$$e_{\max}(L,\nu) = \overline{\Theta}(L^{p_e-1}). \tag{19}$$

In fact, we can show (see Appendix F) that *if $p_e = 2$ then $p = 2$ and vice versa*. For a family of homogeneous states, in particular, we can show that $p = p_e$ for every value of p (see the last paragraph of Appendix F). Hence, *one can identify states with $p = 2$ by calculating* $e_{\max}(L,\nu)$. This can be done in time Poly(L) because the VCM is a $DL\times DL$ matrix.

Furthermore, if $p_e = 2$ we can find a macroscopically-fluctuating additive operator from the eigenvector(s) $\{c'^{\,\nu}_{l\alpha\,\max}(L)\}$ of the VCM corresponding to $e_{\max}(L,\nu)$, as follows. If we normalize $\{c'^{\,\nu}_{l\alpha\,\max}(L)\}$ as

$$\sum_{l=1}^{L}\sum_{\alpha=1}^{D}|c'^{\,\nu}_{l\alpha\,\max}(L)|^2 = L, \tag{20}$$

then the operator

$$\Delta\hat{A}'^{\nu}_{\max}(L) \equiv \sum_{l=1}^{L}\sum_{\alpha=1}^{D} c'^{\,\nu}_{l\alpha\,\max}(L)\Delta\hat{b}_\alpha(l) \tag{21}$$

takes the form of Eq. (15), and it fluctuates macroscopically;

$$\langle\Delta\hat{A}'^{\nu\dagger}_{\max}(L)\Delta\hat{A}'^{\nu}_{\max}(L)\rangle_{L\nu} = e_{\max}(L,\nu)L = \overline{\Theta}(L^2). \tag{22}$$

As shown in Appendix F, if we put

$$C_\nu(L) \equiv \max_l\left(\sum_{\alpha=1}^{D}|c'^{\,\nu}_{l\alpha\,\max}(L)|^2\right), \tag{23}$$

then $C_\nu(L) = \overline{\Omega}(L^0)$ if $p_e = 2$. Therefore, the following operator (which clearly takes the form of Eq. (14))

$$\Delta\hat{A}^{\nu}_{\max}(L) \equiv \sum_{l=1}^{L}\sum_{\alpha=1}^{D} c^{\nu}_{l\alpha\,\max}(L)\Delta\hat{b}_\alpha(l), \quad c^{\nu}_{l\alpha\,\max}(L) \equiv \frac{c'^{\,\nu}_{l\alpha\,\max}(L)}{\sqrt{C_\nu(L)}}, \tag{24}$$

also fluctuates macroscopically;

$$\langle\Delta\hat{A}^{\nu\dagger}_{\max}(L)\Delta\hat{A}^{\nu}_{\max}(L)\rangle_{L\nu} = e_{\max}(L,\nu)L/C_\nu(L) = \overline{\Theta}(L^2). \tag{25}$$

We can then construct an additive operator $\hat{A}^{\nu}_{\max}(L)$ easily from $\Delta\hat{A}^{\nu}_{\max}(L)$, by going from Eq. (14) back to Eq. (13). Although $\hat{A}^{\nu}_{\max}(L)$ is not uniquely determined from $\Delta\hat{A}^{\nu}_{\max}(L)$ (as discussed in Appendix A), this non-uniqueness does not cause any difficulty because p is defined only through the fluctuation.

III. CONJECTURE ON QUANTUM COMPUTATION

The conjecture of Ref. [20] is roughly that superposition of macroscopically distinct states should be *necessary* for large quantum speedup. We now generalize it to treat wide classes of algorithms and models.

We consider decision problems because most computational problems can be reduced, with polynomial overheads, to some decision problems. The number of bits or qubits in a computer is allowed to be Poly(L), where L denotes the size of the input measured in bits. To be definite, we assume that a quantum computer is composed of qubits (i.e., two-level quantum systems) which are separated spatially to each other. That is, if we use the terms of the general discussions of the previous section, each qubit is located on its own site.

We consider the time complexity of problems, allowing both quantum and classical algorithms to have a bounded probability of error. In doing so, we assume a classical probabilistic Turing machine as a counterpart of a quantum computer.

A. Exponential Speedup

To establish notation and to exclude possible ambiguity, we first define exponential speedup, according to convention, as follows.

We consider problems which are *not* in BPP (Bounded-error Probabilistic Polynomial time). For a given (decision) problem, we denote an instance (input) by $i(L,\nu)$, where ν labels different instances (inputs) of size L. The computational time depends not only on L but also on ν. For a given classical computer C and for a given quantum computer Q, let $T_C(L,\nu)$ and $T_Q(L,\nu)$, respectively, be computational time for an instance $i(L,\nu)$, with a bounded probability of error being allowed.

Since we are considering a decision problem which is *not* in BPP, for any classical computer C there exists a set of infinitely many instances that cannot be solved in polynomial time. That is,

$$T_C(L,\nu) > \mathrm{Poly}(L) \text{ for some infinitely many instances.} \tag{26}$$

Here, $T_C(L,\nu) > \mathrm{Poly}(L)$ means that $T_C(L,\nu) = \Omega(P(L))$ for any polynomial $P(L)$. For a quantum computer Q solving such a problem, we say Q achieves *exponential speedup* if

$$T_Q(L,\nu) = \mathrm{Poly}(L) \text{ for all } \nu. \tag{27}$$

According to this definition, Shor's algorithm [1] achieves exponential speedup (if the factoring is not in BPP). On the other hand, *the Deutsch-Jozsa algorithm [31] does not achieve exponential speedup* because the Deutsch's problem *is* in BPP.

B. Extra qubits and redefinition of local sites

In a quantum computer there can exist many qubits (such as ancilla qubits) which are not directly related to quantum computational speedup. For example, one can replace a classical circuit that assists a quantum computer with a quantum circuit. Then, the size of the quantum computer becomes larger than the original one. It is clear that in the enlarged quantum computer only the original part is relevant to quantum computational speedup.

Therefore, *we allow looking only at a subsystem of a quantum computer* in order to find out a relevant part, whose state (according to our conjecture) would have $q = 2$.

Furthermore, one can add extra qubits and circuits to a quantum computer without increasing $T_Q(L,\nu)$ more than a Poly(L) factor. For example, to implement quantum error correction [32, 33] one can replace each qubit with a logical qubit, which is composed of n qubits, where, e.g., $n = 9$ for the Shor code [32]. In such a case, correlation between two qubits is turned into correlation between two *logical* qubits, i.e., correlation among $2n$ qubits. As a result, it is possible that a state with $q = 2$ of the original computer is changed into another state with $q < 2$. However, such nonessential decrease of q may be recovered by regarding each *logical* qubit as a 'local site'.

Generally, in systems which are composed of discrete sites, a local site (which may be, say, a quantum dot) physically has a finite spatial dimension. A set of several neighboring sites also has a finite dimension. Hence, the definition of a 'local site' is to a great extent arbitrary. It is therefore possible and reasonable to redefine a set of neighboring sites as a new single site [29].

In quantum computers, there is further arbitrariness because it is possible to swap the states of two distant qubits, paying only polynomial overhead.

From these observations, *we allow all possible redefinition of local sites* (accordingly, the number of local sites is changed) by regarding two or more qubits, however distant they are, as a local site.

C. Generalized conjecture

In order to apply to wide classes of algorithms and models, we generalize the conjecture of Ref. [20] as follows.

For a decision problem which is not in BPP, consider a quantum computer solving it. If the quantum computer achieves exponential speedup, then states having $q = 2$, whose size is $\Omega(L)$, appear during computation, for some set H of infinitely many instances;

$$H \equiv \{i(L,\nu) \mid \text{some infinitely many } (L,\nu)\text{'s}\} \tag{28}$$

if 'local sites' of the quantum computer are appropriately defined.

This generalized conjecture can be rephrased as follows. *After defining local sites appropriately, look at a certain subsystem which is composed of $\Omega(L)$ local sites of the quantum computer. Let $\hat{\rho}_k(L,\nu)$ be the reduced density operator of such a subsystem at the k-th step of the quantum computation. Take some function $k_*(L,\nu)$, which takes positive integral values, of L and ν. For some set H of infinitely many instances (Eq. (28)), consider the following family of states;*

$$F_{k_*}(H) \equiv \{\hat{\rho}_{k_*}(L,\nu) \mid \textit{all } \nu \textit{ and } L \textit{ such that } i(L,\nu) \in H\}. \tag{29}$$

If the quantum computer achieves exponential speedup, one can find an appropriate definition of local sites, a function $k_*(L,\nu)$, and a set H, such that $q = 2$ for the family $F_{k_*}(H)$.

We will explain physical meaning of the set H in the next subsection.

D. Physical meaning of the set H

If the above conjecture is correct, we can show that H contains some infinitely many instances which cannot be solved in polynomial time by any classical computer. That is, *H contains infinitely many 'hard' instances.* This can be seen using reduction to absurdity as follows.

Suppose that the conjecture is correct but H did *not* contain infinitely many instances which satisfy inequality (26). Then, there would exist a classical computer that solves all instances in H in time Poly(L). By attaching this classical computer to Q as a pre-processor, one could obtain another fast quantum computer Q'. However, states having $q = 2$ would not appear in Q' at all, in contradiction to the conjecture. Therefore, H must contain infinitely many instances which satisfy inequality (26), if our conjecture is correct.

Note that H is *not* uniquely determined for a given problem because an appropriate subset of H can be another H. To confirm the above conjecture, it is sufficient to find *one* of many possible H's.

The set H is closely related to a 'complexity core' [34–37]. A *complexity core* (or, polynomial complexity core) $\mathcal{C}$ was defined by Lynch [34] as an infinite collection of instances such that every algorithm solving the problem using a deterministic Turing machine needs more than polynomial time almost everywhere on $\mathcal{C}$. [Note that $\mathcal{C}$ is not uniquely determined for a given problem because an appropriate subset of $\mathcal{C}$ is also a complexity core [34–37].] His idea has been generalized to complexity classes other than P in Refs. [35–37]. Intuitively, a complexity core is a set of 'hard' instances. The above-mentioned fact shows that *H includes a complexity core as a subset.* Hence, our conjecture claims roughly that *states with $q = 2$ appear for infinitely many instances in a complex core.*

E. Remarks on the conjecture

Before going further, we make a few remarks.

The conjecture does *not* claim that states with $q = 2$ would be *sufficient* for exponential speedup; it rather claims that they are *necessary.* Hence, if states with $q = 2$ appear in some quantum algorithm, it does not necessarily mean that the algorithm achieves exponential speedup.

Moreover, even when a quantum computer does achieve exponential speedup, the conjecture does *not* claim that *all* states with $q = 2$ appearing in the computer would be relevant to exponential speedup. In fact, we already showed in Ref. [21] that although the final state $|\psi_{\rm DFT}\rangle$ of the computation (before the final measurement) has $p = 2$ (hence $q = 2$) it is irrelevant to exponential speedup.

Furthermore, for some states with $q = 2$ of size L (such as the GHZ state), one can construct a quantum circuit that converts a product state into such a state only in $\Theta(L)$ steps *if the target state with $q = 2$ is known beforehand* (i.e., when one constructs the circuit). This fact has *nothing* to do with our conjecture. The point is that in quantum computation the state that appears at, e.g., the middle point of the computation is *unknown* when the circuit is constructed, because the state varies considerably according to the instances.

Finally, we note that the results of Ref. [21] can be understood more clearly according to the present generalized conjecture. For example, it was shown in Ref. [21] that states with $p = 2$ does not appear when $r = 2^n$, where $n = 1, 2, 3, \cdots$ and r is the least positive integer which satisfies $\mathsf{x}^r \equiv 1 \pmod{\mathsf{N}}$. [$\mathsf{N}$ is a positive integer to be factored, and x a random integer co-prime to N which satisfies $0 < \mathsf{x} < \mathsf{N}$ [1, 2, 21].] This fact does *not* conflict with the conjecture. In fact, according to the generalized conjecture, one can exclude the instances with $r = 2^n$ from H, or, even if one includes such instances in H, such rare instances do not affect the generalized index p of Sec. II A because it is defined not by Θ but by $\overline{\Theta}$.

F. Further extention to Grover's quantum search algorithm

Shor's factoring algorithm [1] is a representative algorithm for structured problems [4]. For this algorithm, Ref. [21] supported the above conjecture.

On the other hand, a representative algorithm for unstructured problems is Grover's quantum search algorithm [3, 4]. Hence, it is tempting to examine the conjecture in Grover's algorithm. However, we cannot apply the conjecture (even in the above generalized form) directly to Grover's algorithm because Eq. (27) is not satisfied, i.e., it does not achieve exponential speedup. Nevertheless, it is often argued that the quadratic speedup of Grover's algorithm is significant [4]. Furthermore, Grover's algorithm is known to be optimal, i.e., no quantum algorithm is faster than Grover's algorithm by more than a Poly(L) factor in solving the search problem [4]. It is therefore very interesting to examine the conjecture, if possible, for Grover's algorithm. To make it possible, we here extend the conjecture further to Grover's algorithm. Its correctness for Grover's algorithm will be proved in the next section.

Grover's search problem is the problem of finding a solution to the equation $f_L(x) = 1$ among $N = 2^L$ possibilities, where $f_L(x)$ is a function, $f_L : \{0,1\}^L \mapsto \{0,1\}$. Let M be the number of solutions, and $x_1, \cdots, x_M$ be the solutions. For each L, the solutions specify an instance. That is, $(x_1, \cdots, x_M)$ corresponds to ν, which labels instances as $i(L, \nu)$. According to convention, we regard the number of oracle calls as the computational time.

In extending the conjecture, we note that the degree of quantum speedup depends on the magnitude of M [see Sec. IV B]. We here consider the case where

$$M = O(2^{mL}) \quad (0 < m < 1), \tag{30}$$

where m is a constant, independent of L. In this case, the degree of quantum speedup is similar to the case of $M = 1$ [see Sec. IV B], and hence seems significant.

We extend the conjecture of Sec. III C simply by replacing the condition *'if the quantum computer achieves exponential speedup'* with the relaxed condition *'if the quantum computer achieves exponential speedup or it solves the quantum search problem using Grover's algorithm for the case of Eq. (30)'*.

IV. ANALYTIC RESULTS FOR GROVER'S QUANTUM SEARCH ALGORITHM

In this section, we show that the extended conjecture of Sec. III F is correct for Grover's algorithm.

A. Notation

We first introduce notation. We assume that $N(= 2^L) \gg M$ (the number of solutions), because otherwise classical computers could solve the problem quickly.

It seems obvious that an index register, composed of L qubits, is relevant to Grover's algorithm. We therefore look only at the index register, although additional quantum circuits would be present in real quantum computers (see discussions in Sec. III C). For each instance $i(L, \nu)$, where $\nu = (x_1, \cdots, x_M)$ (see Sec. III F), we put

$$|\alpha(L,\nu)\rangle \equiv \frac{1}{\sqrt{N-M}} \sum_{x\,(\neq x_1,\cdots,x_M)} |x\rangle, \tag{31}$$

$$|\beta(L,\nu)\rangle \equiv \frac{1}{\sqrt{M}} \sum_{x\,(=x_1,\cdots,x_M)} |x\rangle. \tag{32}$$

Then the state $|\psi_0(L)\rangle$ just after the first Hadamard transformation (HT) (see Sec. V A) is represented as [4]

$$\begin{aligned} |\psi_0(L)\rangle &= |\rightarrow\rightarrow\cdots\rightarrow\rangle \\ &= \cos\frac{\theta}{2}\,|\alpha(L,\nu)\rangle + \sin\frac{\theta}{2}\,|\beta(L,\nu)\rangle, \end{aligned} \tag{33}$$

where $|\rightarrow\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$, and the angle θ is given by

$$\cos\frac{\theta}{2} = \sqrt{\frac{N-M}{N}}. \tag{34}$$

Let $\hat{O}(L,\nu)$ be the oracle operator;

$$\hat{O}(L,\nu)|x\rangle = \begin{cases} -|x\rangle & (x = x_1, \cdots, x_M), \\ |x\rangle & (\text{otherwise}). \end{cases} \tag{35}$$

The Grover iteration

$$\hat{G}(L,\nu) = \left[2|\psi_0(L)\rangle\langle\psi_0(L)| - \hat{I}(L)\right]\hat{O}(L,\nu) \tag{36}$$

performs the rotation by angle θ in the direction $|\alpha(L,\nu)\rangle \to |\beta(L,\nu)\rangle$ in the two-dimensional subspace spanned by $|\alpha(L,\nu)\rangle$ and $|\beta(L,\nu)\rangle$. The state $|\psi_k(L,\nu)\rangle$ after k $(= 0, 1, 2, \cdots)$ iterations is therefore given by [4]

$$\begin{aligned} |\psi_k(L,\nu)\rangle &= \hat{G}(L,\nu)^k|\psi_0(L)\rangle \\ &= \cos\left(\frac{2k+1}{2}\theta\right)|\alpha(L,\nu)\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\beta(L,\nu)\rangle. \end{aligned} \tag{37}$$

Hence, by repeating the Grover iteration

$$R(L) \equiv \left\lceil \left(\arccos\sqrt{M/N}\right)/\theta \right\rceil \simeq \left\lceil \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rceil \tag{38}$$

times, the state evolves into $|\psi_{R(L)}(L,\nu)\rangle \simeq |\beta(L,\nu)\rangle$. Here, $\lceil a \rceil$ denotes the smallest integer among those larger than or equal to a. By observing this state in the computational basis, one can find a solution to the search problem with probability $\gtrsim 1/2$. The range of k is thus

$$0 \le k \le R. \tag{39}$$

B. M dependence of degree of speedup

According to convention, we regard the number of oracle calls as the computational time. Then, apart from Poly(L) factors,

$$T_Q(L,\nu) = R(L) = \Theta\left(\sqrt{N/M}\right) \tag{40}$$

for all instances. In contrast, for classical computers there exist infinitely many instances (as $L \to \infty$) such that

$$T_C(L,\nu) = \Theta(N/M). \tag{41}$$

The quadratic speedup of $T_Q(L,\nu)$ over $T_C(L,\nu)$ is significant when M is small enough (such as $M = \text{Poly}(L)$). On the other hand, *no* quantum speedup is achieved when M is too large such as $M = N/\text{Poly}(L)$ because then classical computers can solve the problem efficiently.

To be specific, we limit ourselves to the case of Eq. (30), i.e., where $M = O(2^{mL})$ [m is independent of L and $0 < m < 1$], because almost all interesting applications of Grover's algorithm would belong to this case. For example, this includes the case of $M = \text{Poly}(L)$, whereas the uninteresting case of $M = N/\text{Poly}(L)$ is excluded.

When $M = O(2^{mL})$, we find

$$T_C(L,\nu) = \Theta\left(2^{(1-m)L}\right) \tag{42}$$

for some infinitely many instances, and

$$T_Q(L,\nu) = \Theta\left(\sqrt{2^{(1-m)L}}\right) \tag{43}$$

for all instances. This quadratic speedup seems to be as significant as that of $M = 1$.

C. Family of states to evaluate q or p

As discussed above, the degree of speedup depends on how the number of solutions M behaves asymptotically as a function of L. For clarity, we treat different asymptotic forms of M separately when investigating our extended conjecture.

Suppose that we are given a functional form of M, which asymptotically satisfies inequality (30), such as $M = L^2$. Then, it will turn out that the set of all instances is an appropriate choice of H of Sec. III C;

$$H = \{i(L,\nu) \mid \text{all } L,\ \text{all } \nu\}. \tag{44}$$

To construct a family of states $F_{k_*}(H)$, Eq. (29), we specify the number k_* as follows. Since Grover's algorithm simply repeats the Grover iteration $R(L)$ times, it seems natural to take $k_* = \lceil R(L)/2 \rceil$. More generally, it seems reasonable to take

$$k_* = \lceil R(L)/s \rceil, \tag{45}$$

where s is a positive constant independent of L. It will turn out that this choice of k_* is indeed appropriate. A family of states $F_{k_*}(H)$ is thus constructed, for a given k_*, as

$$F_{k_*}(H) = \{|\psi_{k_*}(L,\nu)\rangle \mid \text{all } L,\ \text{all } \nu\}. \tag{46}$$

Since all states of this family are pure states, we will evaluate the index p rather than q.

D. When $M = 1$

When $M = 1$, Eq. (31) reduces to $|\alpha(L,\nu)\rangle = |\psi_0(L)\rangle + O(1/\sqrt{N}) = |\psi_0(L)\rangle + O(1/2^{L/2})$, whereas Eq. (32) reduces to $|\beta(L,\nu)\rangle = |x_1\rangle$. Since $|\psi_0(L)\rangle$ and $|x_1\rangle$ are product states, we find that $p = 1$ for (the families composed, respectively, of) $|\psi_0(L)\rangle$, $|\alpha(L,\nu)\rangle$ and $|\beta(L,\nu)\rangle$. Hence, $p = 1$ for (the families of) the initial and final states.

For intermediate states $|\psi_k(L,\nu)\rangle$'s of interest, it is convenient to investigate $\hat{M}_x \equiv \sum_l \hat{\sigma}_x(l)$ (which corresponds to the x component of the total magnetization of magnetic substances). Note here that in order to show that $p = 2$ it is sufficient to find *one* additive observable (which in this case is $\hat{M}_x$) which fluctuates macroscopically. From Eq. (37), we find

$$\langle\psi_k(L,\nu)|\hat{M}_x|\psi_k(L,\nu)\rangle = \cos^2\left(\frac{2k+1}{2}\theta\right) L + O(1), \tag{47}$$

$$\langle\psi_k(L,\nu)|\hat{M}_x^2|\psi_k(L,\nu)\rangle = \cos^2\left(\frac{2k+1}{2}\theta\right) L^2 + O(L). \tag{48}$$

Hence,

$$\langle\psi_k(L,\nu)|(\Delta\hat{M}_x)^2|\psi_k(L,\nu)\rangle = \frac{1}{4}\sin^2\left((2k+1)\theta\right) L^2 + O(L). \tag{49}$$

For all states in the family $F_{k_*}(H)$ of Eq. (46), we thus find

$$\langle\psi_{k_*}(L,\nu)|(\Delta\hat{M}_x)^2|\psi_{k_*}(L,\nu)\rangle \simeq \frac{1}{4}\sin^2\left(\frac{\pi}{s}\right) L^2 + O(L). \tag{50}$$

Since s is independent of L, the right-hand side is $\Theta(L^2)$, and thus $p = 2$ for this family.

E. When $M = \mathbf{Poly}(L)$

We now consider the case where $M \geq 2$. In this case, unlike the case of $M = 1$, $|\beta(L,\nu)\rangle$ has $p = 2$ for some instances.

For example, suppose that $M = 2$ and the two solutions for some instance ν are $x_0 \equiv 1010\cdots10$ and $x_1 \equiv 0101\cdots01$. Then, $p = 2$ for $|\beta(L,\nu)\rangle = (|x_0\rangle + |x_1\rangle)/\sqrt{2}$ (i.e., for the family $\{|\beta(L,\nu)\rangle \mid \text{all } L\}$), because $\langle\beta(L,\nu)|(\Delta\hat{M}_z^{\rm st})^2|\beta(L,\nu)\rangle = \Omega(L^2)$. Here, $\hat{M}_z^{\rm st} \equiv \sum_l (-1)^l \hat{\sigma}_z(l)$, which corresponds to the z component of the staggered magnetization of antiferromagnets. On the other hand, if $x_0 \equiv 0000\cdots00$ and $x_1 \equiv 0000\cdots01$ for another instance ν' then $p = 1$ for $|\beta(L,\nu')\rangle = (|x_0\rangle + |x_1\rangle)/\sqrt{2}$.

Therefore, *when $M \geq 2$, p of the final state depends on the instance, i.e., on the nature of the solutions.* (On the other hand, it is clear that $p = 1$ for the initial state.)

To compute p of states in intermediate stages of computation for $M > 2$, we first consider the case where $M = \mathrm{Poly}(L)$. In this case, Eq. (49) still holds for $|\psi_k(L,\nu)\rangle$ with $k \geq 1$, and thus the discussion following Eq. (49) also holds. Therefore, we again find that $p = 2$ for the family $F_{k_*}(H)$ of Eq. (46).

We can obtain the same conclusion when $M = O(2^{L^\kappa})$, where κ is a constant independent of L and $0 < \kappa < 1$. Instead of showing this, we shall derive the same conclusion when M is even larger in the next subsection.

F. When $M = \Theta(2^{mL})$

We now study the case where

$$M = \Theta(2^{mL}) \quad (0 < m < 1), \tag{51}$$

where m is independent of L. This is the upper limit of M that satisfies condition (30).

As mentioned above, p of the final state depends on the nature of the solutions (whereas $p = 1$ for the initial state). Since this might not be trivial when M is as large as $\Theta(2^{mL})$, we give an example for $M = 2^{L/2} = \sqrt{N}$. Suppose that the solutions for some instance ν are as follows; $x_j = j$ for $j = 1, 2, \ldots, \frac{1}{2}\sqrt{N}$ whereas x_j's for $j \geq \frac{1}{2}\sqrt{N} + 1$ are multiples of $2\sqrt{N}$ (less than N). Then

$$\begin{aligned} |\beta(L,\nu)\rangle &= \frac{1}{\sqrt{2M}} \sum_{y=1}^{\frac{1}{2}\sqrt{N}} |00\cdots 0y\rangle + \frac{1}{\sqrt{2M}} \sum_{z=0}^{\frac{1}{2}\sqrt{N}-1} |z0\cdots 00\rangle \\ &= \frac{1}{\sqrt{2}}|00\cdots 0 \to\to \cdots \to\rangle + \frac{1}{\sqrt{2}}|\to\to \cdots \to 00\cdots 0\rangle + O(1/\sqrt{N}). \end{aligned} \tag{52}$$

Since $\langle\beta(L,\nu)|(\Delta\hat{M'}_x)^2|\beta(L,\nu)\rangle = O(L^2)$, where $\hat{M'}_x \equiv \sum_{l=1}^{L/2} \hat{\sigma}_x(l) + \sum_{l=L/2+1}^{L} \hat{1}(l)$, we find that $p = 2$ for this state. By contrast, if $x_j = j$ for all j for another instance ν', then $|\beta(L,\nu')\rangle = |00\cdots \to\to \cdots \to\rangle$, for which $p = 1$.

To compute p of states in intermediate stages of computation, we note that $|\alpha(L,\nu)\rangle = |\psi_0(L)\rangle + O(2^{-(1-m)L/2})$ when $M = \Theta(2^{mL})$. Hence, abbreviating $|\psi_k(L,\nu)\rangle, |\alpha(L,\nu)\rangle, |\beta(L,\nu)\rangle$ to $|\psi_k\rangle, |\alpha\rangle, |\beta\rangle$, respectively, we find

$$\langle\psi_k|\hat{M}_x|\psi_k\rangle = \cos^2\left(\frac{2k+1}{2}\theta\right)\langle\alpha|\hat{M}_x|\alpha\rangle + \sin^2\left(\frac{2k+1}{2}\theta\right)\langle\beta|\hat{M}_x|\beta\rangle + O(1), \tag{53}$$

$$\langle\psi_k|\hat{M}_x^2|\psi_k\rangle = \cos^2\left(\frac{2k+1}{2}\theta\right)\langle\alpha|\hat{M}_x^2|\alpha\rangle + \sin^2\left(\frac{2k+1}{2}\theta\right)\langle\beta|\hat{M}_x^2|\beta\rangle + O(1), \tag{54}$$

which yield

$$\begin{aligned} \langle\psi_k|(\Delta\hat{M}_x)^2|\psi_k\rangle &= \cos^2\left(\frac{2k+1}{2}\theta\right)\langle\alpha|(\Delta\hat{M}_x)^2|\alpha\rangle + \sin^2\left(\frac{2k+1}{2}\theta\right)\langle\beta|(\Delta\hat{M}_x)^2|\beta\rangle \\ &+ \frac{1}{4}\sin^2((2k+1)\theta)\big(\langle\alpha|\hat{M}_x|\alpha\rangle - \langle\beta|\hat{M}_x|\beta\rangle\big)^2 + O(L). \end{aligned} \tag{55}$$

As shown in Appendix G, $\langle\alpha|\hat{M}_x|\alpha\rangle = L + O(1)$ and $\langle\beta|\hat{M}_x|\beta\rangle = KL$, where K is independent of L and $0 < K < 1$. Hence, for k_* of Eq. (45), we find $\langle\psi_{k_*}|(\Delta\hat{M}_x)^2|\psi_{k_*}\rangle = O(L^2)$. Therefore, $p = 2$ for the family $F_{k_*}(H)$ of Eq. (46).

We have thus proved that the extended conjecture of Sec. III F is correct for Grover's algorithm.

G. Intermediate values of p

As the quantum computation proceeds (i.e., as k is increased), p increases from 1 for the initial state $|\psi_0(L)\rangle$ to 2 for $|\psi_{k_*}(L,\nu)\rangle$. In the transient steps, p takes intermediate values between 1 and 2.

Such intermediate values are taken also, e.g., by states of quantum many-body systems at critical points of continuous phase transitions, where two-point correlation functions decay according to power laws as a function of the distance between two points. Hence, one might expect some universal properties of p, as critical exponents in continuous phase transitions have.

For states of quantum computers in the transient steps, however, the intermediate values of p are not universal; they depend on details such as the nature of the solutions. Since we are not interested in such non-universal values of p in this paper, we have focused on the universal result, which is directly related to our conjecture, that $p = 2$ for the family composed of $|\psi_{k_*}(L,\nu)\rangle$'s.

V. EVOLUTION OF QUANTUM CORRELATIONS IN GROVER'S QUANTUM SEARCH ALGORITHM

As summarized in Sec. II, the index p is calculated from two-point correlations of local operators. For pure states, $p = 2$ if they have two-point correlations of $\overline{\Theta}(1)$ between $\Theta(L^2)$ pairs of sites. [As discussed in Sec. II C, for pure states such strong two-point correlations imply a strong L-point correlation.] As discussed in Sec. II D, the existence of such correlations can be detected by the asymptotic behavior (as $L \to \infty$) of the maximum eigenvalue $e_{\max}$ of the VCM, because, roughly speaking, $Le_{\max}$ is proportional to the number of pairs of sites whose correlation is of $\overline{\Theta}(1)$ [38].

Although p is simpler and more convenient for stating the conjecture, $e_{\max}$ has more detailed information about two-point correlations. [For example, a state with $e_{\max} = L$ has stronger two-point correlations than one with $e_{\max} = L/10$, whereas both states have $p = 2$.] It is therefore interesting to study how $e_{\max}$ evolves as the computation proceeds from a small value (corresponding to $p = 1$) at the initial state to larger values. It describes how two-point correlations evolves (until a strong L-point correlation develops for $p = 2$, as discussed in Sec. II C).

In this section, to investigate the evolution of $e_{\max}$, we simulate numerically a quantum computer that performs Grover's algorithm. In the simulation, we study more states than those studied in the previous section, where we have studied $|\psi_k(L,\nu)\rangle = \hat{G}^k(L,\nu)|\psi_0(L)\rangle$ $(k = 0, 1, 2, \cdots, R(L))$. In actual quantum computations, the Grover iteration $\hat{G}(L,\nu)$ may be realized, e.g., as a series of local and pair-wise operations [4]. Hence, many intermediate states appear between the computational steps corresponding to $|\psi_k(L,\nu)\rangle$ and $|\psi_{k+1}(L,\nu)\rangle$. Although it was sufficient to investigate $|\psi_k(L,\nu)\rangle$'s for confirming the conjecture, we also study such intermediate states to see more details.

We simulate two cases, $M = 1$ and $M = 2$, because these cases are most fundamental. The solution(s) x_1 (and x_2) is chosen randomly. We have confirmed that this random choice of a solution(s) makes no significant difference on the results of the numerical simulations presented below.

A. Formulation of simulation

We explain our simulation for the case of $M = 1$. Simulation for $M = 2$ has also been performed similarly.

Since $M = 1$, we can simply take $\nu = x_1$. As in the previous section, we consider the index register composed of L qubits. The register is initially set to be in the following product state;

$$|\psi_{\rm init}(L)\rangle = |00\cdots0\rangle. \tag{56}$$

Firstly, the HT is performed by successive applications of the Hadamard gate on individual qubits, and the quantum state evolves into $|\psi_0(L)\rangle$ of Eq. (33). Then we apply the Grover iteration $\hat{G}(L,\nu)$, which consists of two HTs, an oracle operation $\hat{O}(L,\nu)$, and a conditional phase shift $\hat{P}(L)$ [4];

$$\hat{P}(L)|x\rangle = \begin{cases} |00\cdots0\rangle & (x = 0), \\ -|x\rangle & (x > 0). \end{cases} \tag{57}$$

Each HT requires L operations of the Hadamard gate. The oracle $\hat{O}(L,\nu)$ requires its own workspace qubits and computational time. However, since the oracle is not a proper part of the Grover's algorithm, we simulate the operation of $\hat{O}(L,\nu)$ as a one-step operation, and its workspace is not included in the simulation. The execution of $\hat{P}(L)$ requires $\Omega(L)$ pairwise unitary operations. For simplicity, however, we simulate $\hat{P}(L)$ as a one-step operation. Hence, each Grover iteration is simulated by $2L + 2$ steps of operations.

After application of the Grover iterations $R(L)$ times, the state $|\psi_0(L)\rangle$ evolves into

$$\hat{G}^{R(L)}(L,\nu)|\psi_0(L)\rangle = |\psi_{R(L)}(L,\nu)\rangle \simeq |\beta(L,\nu)\rangle = |x_1\rangle. \tag{58}$$

Finally, by observing this state one can obtain the solution x_1 with a sufficiently high probability. We do not simulate this measurement process. The total computational time (steps) $T_Q(L,\nu)$ in our simulation is thus

$$T_Q(L,\nu) = L + (2L + 2)R(L) = \Theta(L\sqrt{2^L}) \tag{59}$$

for all ν. This is larger than $T_Q(L,\nu)$ of Sec. IV only by a polynomial factor. For each instance ν, $T_Q(L,\nu)$ different states, including $|\psi_k(L,\nu)\rangle$'s of Sec. IV, appear during computation.

In our conjecture, we have allowed (i) looking only at a subsystem and (ii) all possible redefinition of local sites. For the present model of a quantum computer, however, we have confirmed (from the following results and the results of the previous section) that they are unnecessary. That is, in the present model, we can confirm the extended conjecture by simply calculating the index p of states of the index register.

To find states with $p = 2$, we calculate $e_{\max}(L,\nu)$ of Sec. II D. By plotting the L dependence of $e_{\max}(L,\nu)$, we can determine the value of p_e through Eq. (19). When states with $p_e = 2$ are found, they have $p = 2$ because, as discussed in Sec. II D, if $p_e = 2$ then $p = 2$ (and vice versa). We will also plot how $e_{\max}(L,\nu)$ (for fixed L) grows and decays as the quantum computation proceeds because it is instructive and impressive.

In defining the VCM of Eq. (17), we take $\hat{b}_\alpha(l) = \hat{\sigma}_\alpha(l)$ (Pauli operator on site l and $\alpha = 1, 2, 3$), i.e,

$$V_{l\alpha,l'\alpha'}(L,\nu) \equiv \langle \Delta\hat{\sigma}_\alpha(l)\Delta\hat{\sigma}_{\alpha'}(l')\rangle_{L\nu}. \tag{60}$$

In the following, for the sake of conciseness, we will often denote $e_{\max}(L,\nu)$, $V_{l\alpha,l'\alpha'}(L,\nu)$, and so on simply by $e_{\max}$, $V_{l\alpha,l'\alpha'}$, and so on.

B. Results of simulation for $M = 1$

Figure 1 plots evolution of $e_{\max}$ for $L = 8, 9, 10, 12, 14$ and $M = 1$, when $x_1 = 19, 388, 799, 1332, 9875$, respectively. It is seen that on the whole the curves are exponentially expanded along the horizontal axis as L is increased.

Figure 2 is a magnification from the 1st to 40th steps for $L = 8$, whereas a magnification from the 1005th to 1155th steps for $L = 14$ is shown in Fig. 3.

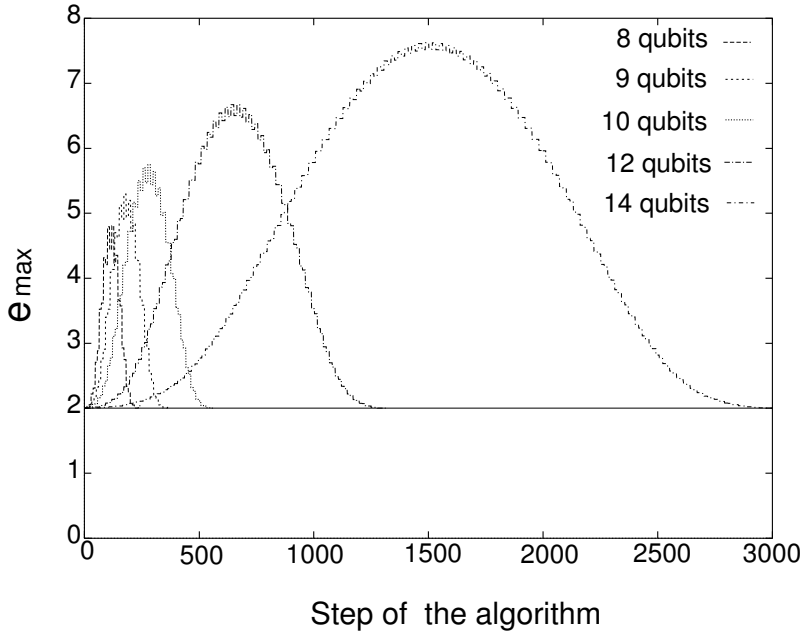

FIG. 1: The maximum eigenvalue $e_{\max}$ of the VCM of quantum states appearing in Grover's quantum search algorithm for $L = 8, 9, 10, 12, 14$ when $x_1 = 19, 388, 799, 1332, 9875$, respectively, as functions of the step of the algorithm. The horizontal line represents the value of $e_{\max}$ for product states, $e_{\max} = 2$.

It is seen that $e_{\max} = 2.00$ for all states from $|\psi_{\rm init}\rangle$ to $|\psi_0\rangle$, i.e., during the initial HT (from the 1st to 8th steps in Fig. 2, denoted as 'HT'). This is because all these states are product states, for which we can easily show that $e_{\max} = 2$ (Appendix H). When the stage of Grover iterations begins, $e_{\max}$ grows gradually, as seen from Figs. 1 and 2. In each Grover iteration, Figs. 2 and 3 show that $e_{\max}$ changes when the oracle operator $\hat{O}$ is operated, whereas it is kept constant during the subsequent HT. Then, it changes again when $\hat{P}$ is operated, whereas it is kept constant again during the subsequent HT. As the Grover iterations are repeated, $e_{\max}$ (hence, quantum correlation) continues to increase as a whole, until it takes the maximum value after about $R(L)/2$ times applications of $\hat{G}$. Further applications

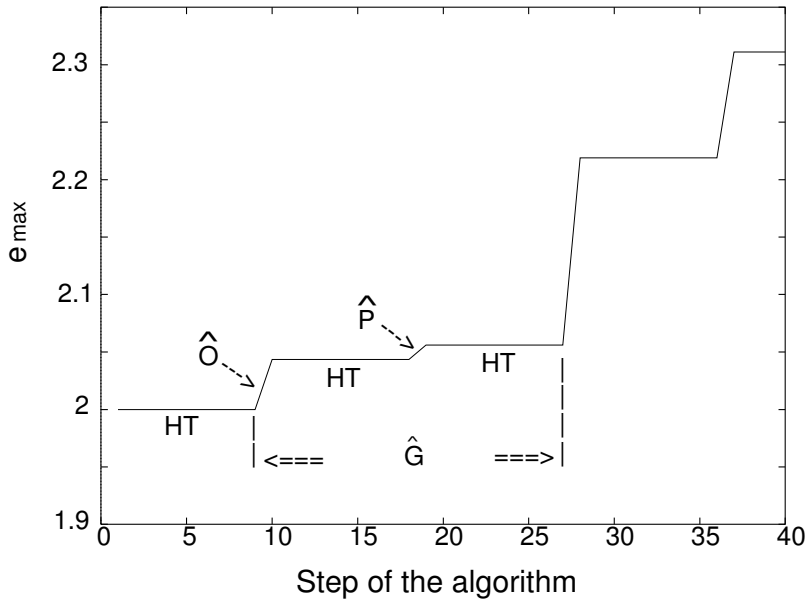

FIG. 2: A magnification of Fig. 1, from the 1st to 40th steps for $L = 8$. Here, $\hat{O}$ and $\hat{P}$ represent the oracle operation and conditional phase shift, respectively, in a single Grover iteration $\hat{G}$.

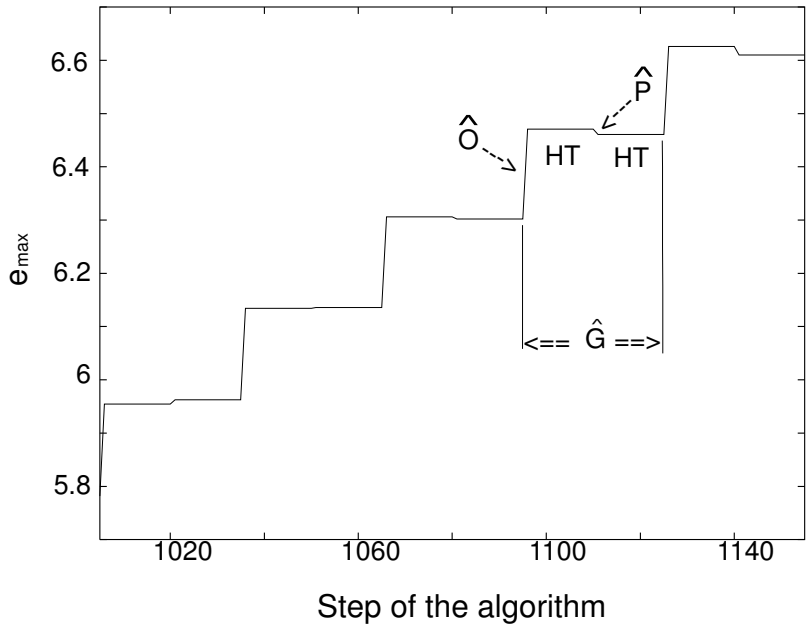

FIG. 3: A magnification of Fig. 1, from the 1005th to 1155th steps for $L = 14$. Here, $\hat{O}$ and $\hat{P}$ represent the oracle operation and conditional phase shift, respectively, in a single Grover iteration $\hat{G}$.

of $\hat{G}$ reduce $e_{\max}$, as seen from Fig. 1, toward $e_{\max} \simeq 2.00$ for $|\psi_{R(L)}\rangle$, which is approximately a product state as seen from Eq. (58).

These results indicate that our construction of the family of states, Eqs. (45) and (46), is natural. Although we have already shown in Sec. IV that $p = 2$ for such a family, it is instructive to plot $e_{\max}(L, \nu)$ of $|\psi_{k_*}(L, \nu)\rangle$ as a function of L when the solution x_1 is randomly chosen (i.e., an instance ν is randomly chosen) for each L. Figure 4 plots $e_{\max}$'s of $|\psi_{\lceil R/2 \rceil}\rangle$, $|\psi_{\lceil R/3 \rceil}\rangle$ and $|\psi_{\lceil R/4 \rceil}\rangle$ for such randomly-chosen x_1 as functions of L. [We have confirmed that almost identical curves are obtained for other choices of x_1 as well.] Since $e_{\max}$'s tend to be proportional to L

for large L, we can confirm that $p = p_e = 2$.

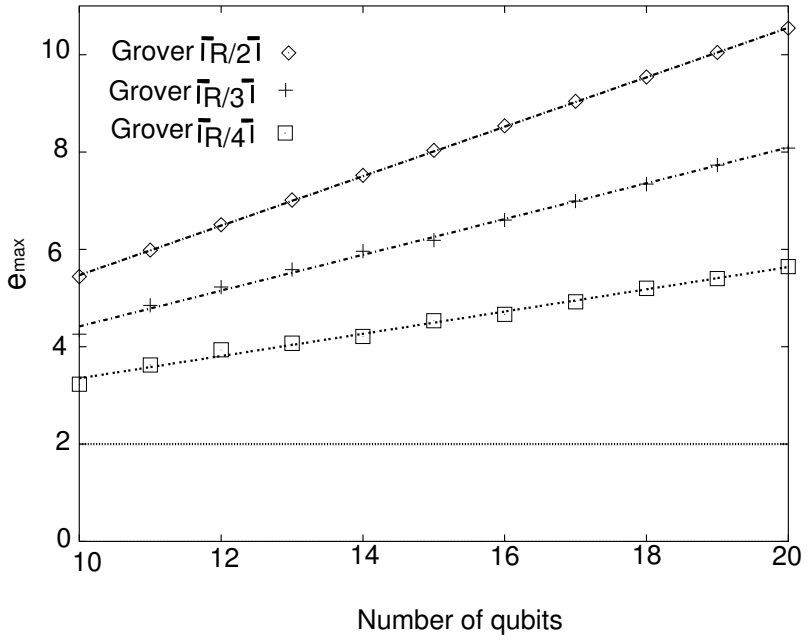

FIG. 4: $e_{\max}$'s of $|\psi_{\lceil R/2 \rceil}\rangle$ (diamonds), $|\psi_{\lceil R/3 \rceil}\rangle$ (crosses) and $|\psi_{\lceil R/4 \rceil}\rangle$ (squares), as functions of L. They all show that $p = p_e = 2$. The dotted lines are the guides to the eyes, whereas the horizontal line represents the value of $e_{\max}$ for product states, $e_{\max} = 2$.

C. Results of simulation for $M = 2$

When $M = 2$, the result of Sec. IV E indicates that $p = 2$ for most states in the Grover iteration processes whereas p of the *final* state depends on the nature of the solutions. Figure 5 illustrates this clearly, where we have plotted evolution of $e_{\max}$ for two cases, $p = 2$ (profile 1) and $p = 1$ (profile 2) for the final state. For $|\psi_{\lceil R/2 \rceil}\rangle$, $|\psi_{\lceil R/3 \rceil}\rangle$ and $|\psi_{\lceil R/4 \rceil}\rangle$, on the other hand, we obtain results similar to Fig. 4 for both cases. Hence, $p = 2$ for these states. This result visualizes how our extended conjecture holds when $M \geq 2$.

VI. DISCUSSIONS AND SUMMARY

We have studied the conjecture that superposition of macroscopically distinct states would be necessary for significant speedup of quantum computers over classical computers. This conjecture was previously supported for a circuit-based quantum computer performing Shor's factoring algorithm. To treat general algorithms and models, we have generalized the indices p and q for superposition of macroscopically distinct states. We then generalize the conjecture in such a way that it is applicable unambiguously to general models if a quantum algorithm achieves an exponential speedup. We further extend the conjecture to the speedup achieved by Grover's quantum search algorithm. This extended conjecture is proved to be correct for Grover's algorithm. Since Grover's and Shor's algorithms are representative ones for unstructured and structured problems, respectively, the present results and the results of Ref. [21] support strongly the conjecture. To see details, we have also presented, by numerical simulation, how quantum correlation evolves and the superposition of macroscopically distinct states develops as the computation proceeds.

Jozsa and Linden previously showed that entanglement over a cluster whose size is larger than $O(1)$ is necessary for an exponential speedup [18]. For $p = 2$, on the other hand, entanglement over a cluster whose size is larger than $O(L)$ is necessary [11, 12]. The present conjecture imposes a stronger condition in this sense.

Moreover, Vidal showed that a necessary condition for an exponential speedup is that the amount of the bipartite entanglement between one part and the rest of the qubits increases with L [19]. The bipartite entanglement which was

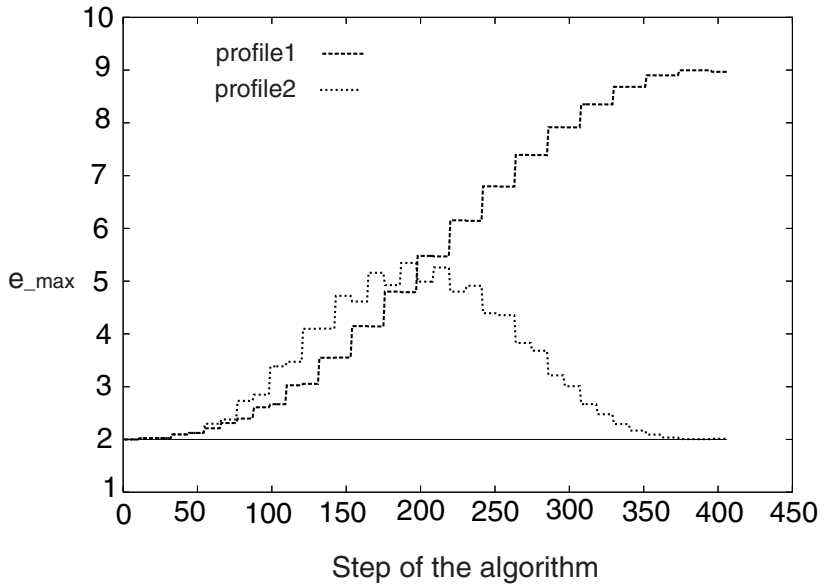

FIG. 5: The maximum eigenvalue $e_{\max}$ of the VCM of quantum states appearing in Grover's quantum search algorithm for $L = 10$ and $M = 2$, when $x_1 = 2, x_2 = 1023$ (profile 1) and when $x_1 = 511, x_2 = 512$ (profile 2), as functions of the step of the algorithm. The horizontal line represents the value of $e_{\max}$ for product states, $e_{\max} = 2$.

studied by him is totally different from the entanglement possessed by superposition of macroscopically distinct states. Therefore, the *simultaneous* requirement (for speedup over classical computations) of Vidal's condition and *and* the present conjecture is much stronger than the requirement of either one of them. That is, for quantum speedups *both* superposition of macroscopically distinct states *and* a sufficient amount of the bipartite entanglement are necessary.

It is also interesting to explore relation between our results and the problem of time-optimal quantum evolution [39, 40]. In the latter case the optimal evolution requires large fluctuation of Hamiltonian, while in the former fast quantum computations require states with large fluctuations of additive operators. This suggests a possible relation between the quantum speedup and the optimal evolution [40].

Acknowledgments

We thank M. Koashi and A. Hosoya for valuable discussions. This work was supported by PRESTO, Japan Science and Technology Corporation, by Grant-in-Aid for Scientific Research No. 18-11581, and by KAKENHI No. 22540407.

Appendix A: On the restriction that $\|\hat{a}(l)\| = 1$

Suppose that $\hat{A} = \sum_l \hat{a}(l)$ is an additive operator. In the present paper, we have required that $\|\hat{a}(l)\| = 1$. To understand technical details about this, the following examples would be helpful.

ex.1 The operator $\hat{A}_1'' \equiv \sum_l \hat{a}(l)/2$ is *not* an additive operator according to the present definition, because the norm of the local operators is not unity. However, by simply multiplying $\hat{A}_1''$ by 2, we can obtain an additive operator $\hat{A}_1 \equiv 2\hat{A}_1''$ $(= \hat{A})$. Fluctuations of $\hat{A}_1$ and $\hat{A}_1''$ differ only by a constant factor.

ex.2 The operator $\hat{A}_2'' \equiv \sum_{l=\text{odd}} \hat{a}(l)$ is *not* an additive operator according to the present definition, because the norm of the local operators for even l vanishes. However, this operator has the same fluctuation as the additive operator $\hat{A}_2 \equiv \sum_{l=\text{odd}} \hat{a}(l) + \sum_{l=\text{even}} \hat{1}(l)$.

ex.3 The operator $\hat{A}_3'' \equiv \sum_l \left(1 + \frac{(-1)^l}{2}\right) \hat{a}(l)$ is *not* an additive operator according to the present definition. However, there always exist real numbers $\alpha, \beta(l)$ such that $\hat{a}_3(l) \equiv \alpha \left(1 + \frac{(-1)^l}{2}\right) \hat{a}(l) + \beta(l)\hat{1}(l)$ has unit norm for every l. Then, $\hat{A}_3 \equiv \sum_l \hat{a}_3(l)$ is an additive operator, and fluctuations of $\hat{A}_3$ and $\hat{A}_3''$ differ only by a constant factor.

Therefore, operators like $\hat{A}_1'', \hat{A}_2'', \hat{A}_3''$ are essentially included (as $\hat{A}_1, \hat{A}_2, \hat{A}_3$, respectively) when taking $\max_{\hat{A}(L)}$ in Eq. (5).

The point is that one can modify $\hat{A}_1'', \hat{A}_2'', \hat{A}_3''$ in such a way that fluctuations of the modified operators $\hat{A}_1, \hat{A}_2, \hat{A}_3$ (which are additive operators) have the same order of magnitude as those of $\hat{A}_1'', \hat{A}_2'', \hat{A}_3''$. Note that this modification is *not* unique. For example, from $\hat{A}_1''$ one can also construct an additive operator $2\hat{A}_1'' - \hat{a}(1) + \hat{1}(1) = \hat{1}(1) + \sum_{l\geq 2} \hat{a}(l)$, which has the same order of fluctuation as $\hat{A}_1$. This non-uniqueness does not cause any difficulty because p and q are defined by the order of magnitude of fluctuations.

Appendix B: asymptotic notation

Let $f(L)$ and $g(L)$ be non-negative functions of a positive variable L. Following Ref. [4], we use the following asymptotic notation:

$$f(L) = O(g(L)) \;\Leftrightarrow\; f(L) \leq Kg(L), \tag{B1}$$
$$f(L) = \Omega(g(L)) \;\Leftrightarrow\; Jg(L) \leq f(L), \tag{B2}$$
$$f(L) = \Theta(g(L)) \;\Leftrightarrow\; Jg(L) \leq f(L) \leq Kg(L), \tag{B3}$$

as $L \to \infty$, where J, K are some positive constants.

Let $f_\nu(L)$'s be non-negative functions, which are labeled by an index ν, of a positive variable L. We consider a family that consists of these functions, i.e., a family of real values, $\{f_\nu(L)\}_{L,\nu}$. Assuming that the number of possible values of ν increases to infinity as $L \to \infty$, we use the following asymptotic notation:

$$f_\nu(L) = \overline{O}(g(L)) \;\Leftrightarrow\; f_\nu(L) = O(g(L)) \text{ for almost every } \nu, \tag{B4}$$
$$f_\nu(L) = \overline{\Omega}(g(L)) \;\Leftrightarrow\; f_\nu(L) = \Omega(g(L)) \text{ for almost every } \nu, \tag{B5}$$
$$f_\nu(L) = \overline{\Theta}(g(L)) \;\Leftrightarrow\; f_\nu(L) = \Theta(g(L)) \text{ for almost every } \nu. \tag{B6}$$

For example, if $\nu = 1, 2, \ldots, 2^L$ for each L and $f_\nu(L) = L^2(1 + \sin L)(1/L + 1/L^\nu)$, then $f_\nu(L) = \overline{\Theta}(L^2)$, whereas it is *not* $\Theta(L^2)$.

Appendix C: Range of p

In this appendix, we show that $1 \leq p \leq 2$. As the operator norm $\|\hat{a}\|$, we employ $\|\hat{a}\|_E$, defined by Eq. (2), in this Appendix. Since $\left\langle \left(\Delta \hat{A}(L)\right)^2 \right\rangle_{L\nu} \leq \left\langle \hat{A}(L)^2 \right\rangle_{L\nu} \leq L^2$, we find that $p \leq 2$. To prove that $p \geq 1$, we use the following Lemma;

Lemma: For any state, which can be a mixed state, there always exists an local operator $\hat{a}_*(l)$ which satisfies

$$\|\hat{a}_*(l)\|_E = 1 \text{ and } \langle \Delta\hat{a}_*(l)^\dagger \Delta\hat{a}_*(l)\rangle = 1, \tag{C1}$$

Proof: For a given state $\hat{\rho}(L)$, its local density operator $\hat{\rho}_l \equiv \mathrm{Tr}_{l'(\neq l)}\hat{\rho}(L)$ can be diagonalized as

$$\hat{\rho}_l = \sum_{j=1}^{d} w_j(l)|j,l\rangle\langle j,l|, \quad \sum_{j=1}^{d} w_j(l) = 1, \tag{C2}$$

where $\{|j,l\rangle\}_j$ is a complete orthonormal set of site l. Take

$$\hat{a}_*(l) = \sum_{j=\mathrm{odd}} (|j,l\rangle\langle j+1,l| + h.c.) \quad (\text{where } \langle d+1,l| \equiv \langle 1,l|), \tag{C3}$$

which is a non-Hermitian local operator with $\|\hat{a}_*(l)\|_E = 1$. Since $\mathrm{Tr}\,[\hat{\rho}(L)\hat{a}_*(l)] = 0$ and

$$\hat{a}_*(l)^\dagger \hat{a}_*(l) = \sum_{j=1}^{d} |j,l\rangle\langle j,l| = \hat{1}(l), \tag{C4}$$

we find that $\langle \Delta\hat{a}_*(l)^\dagger \Delta\hat{a}_*(l)\rangle = 1$. ■

Using this Lemma, we now show the following theorem, from which it is obvious that $p \geq 1$.
Theorem: For any state, which can be a mixed state, there always exists an additive operator which satisfies

$$\langle \Delta \hat{A}(L)^\dagger \Delta \hat{A}(L) \rangle \geq L. \tag{C5}$$

Proof: We use the induction method. We define

$$\hat{A}(k) \equiv \sum_{l=1}^{k} \hat{a}(l) \quad (\|\hat{a}(l)\| = 1), \tag{C6}$$

for $1 \leq k \leq L$. When $k = 1$, the above Lemma shows that there exists $\hat{A}(1)$ such that $\langle \Delta \hat{A}(1)^\dagger \Delta \hat{A}(1) \rangle \geq 1$. Now, assume that there exists $\hat{A}(k)$ such that $\langle \Delta \hat{A}(k)^\dagger \Delta \hat{A}(k) \rangle \geq 1$. From the above Lemma, there exists a local operator $\hat{a}_*(k+1)$ on site $k+1$ such that $\|\hat{a}_*(k+1)\| = 1$ and $\langle \Delta \hat{a}_*(k+1)^\dagger \Delta \hat{a}_*(k+1) \rangle = 1$. So, construct $\hat{A}(k+1)$ as

$$\hat{A}(k+1) = \hat{A}(k) + \hat{a}_*(k+1). \tag{C7}$$

Then,

$$\langle \Delta \hat{A}(k+1)^\dagger \Delta \hat{A}(k+1) \rangle = \langle \Delta \hat{A}(k)^\dagger \Delta \hat{A}(k) \rangle + \left\{ \langle \Delta \hat{A}(k)^\dagger \Delta \hat{a}_*(k+1) \rangle + c.c. \right\} + 1. \tag{C8}$$

Therefore, if $\left\{ \langle \Delta \hat{A}(k)^\dagger \Delta \hat{a}_*(k+1) \rangle + c.c. \right\} \geq 0$ then $\langle \Delta \hat{A}(k+1)^\dagger \Delta \hat{A}(k+1) \rangle \geq k+1$. If, on the other hand, $\left\{ \langle \Delta \hat{A}(k)^\dagger \Delta \hat{a}_*(k+1) \rangle + c.c. \right\} < 0$ then reconstruct $\hat{A}(k+1)$ as

$$\hat{A}(k+1) = \hat{A}(k) - \hat{a}_*(k+1). \tag{C9}$$

This gives $\langle \Delta \hat{A}(k+1)^\dagger \Delta \hat{A}(k+1) \rangle \geq k+1$. ■

Appendix D: Simple examples of states with $p = 2$ and $p = 1$

To explain why p is useful and necessary, we give a few simple examples of homogeneous states.

For the GHZ or 'cat' state, $|\psi_{\rm cat}(L)\rangle \equiv (|00\cdots0\rangle + |11\cdots1\rangle)/\sqrt{2}$, a heuristic discussion would be sufficient to judge that it contains superposition of macroscopically distinct states, because it is simply superposition of *two* macroscopically distinct states and their coefficients do *not* vanish as $L \to \infty$.

By contrast, heuristic discussions will be ambiguous for the following state;

$$|\psi_{\rm dw}(L)\rangle \equiv \frac{1}{\sqrt{L-1}} \left(|100\cdots00\rangle + |110\cdots00\rangle + |111\cdots00\rangle + \cdots + |111\cdots10\rangle \right), \tag{D1}$$

where 'DC' stands for domain wall (see below). This is superposition of L states, each state differs from the preceeding state *only in a single qubit*, and the weight of each state *vanishes* in the $L \to 0$ limit.

Even for such a state, by using the index p we can easily judge whether superposition of macroscopically distinct states is contained. In fact, we can show that $p = 2$ for $|\psi_{\rm dw}\rangle$, hence it does contain superposition of macroscopically distinct states. Physically, this state is superposition of single-domain-wall states. That is, let $|j; j+1\rangle$ be the state which has a domain wall between sites j and $j+1$, then

$$|\psi_{\rm dw}(L)\rangle = \frac{1}{\sqrt{L-1}} \sum_{j=1}^{L-1} |j; j+1\rangle \tag{D2}$$

Since the domain wall is clearly a macroscopic object, this state contains superposition of macroscopically distinct states. This can also be understood by rewriting $|\psi_{\rm dw}\rangle$ as

$$|\psi_{\rm dw}(L)\rangle = \frac{1}{\sqrt{L-1}} \sum_{j=1}^{L/2-1} |j; j+1\rangle + \frac{1}{\sqrt{L-1}} \sum_{j=L/2}^{L-1} |j; j+1\rangle, \tag{D3}$$

$$= \frac{1}{\sqrt{2}} [\text{a state whose domain wall is located in the left half}] + \frac{1}{\sqrt{2}} [\text{a state whose domain wall is located in the right half}]. \tag{D4}$$

The two states in this expression are clearly distinct macroscopically.

On the other hand, the 'W state' $|\psi_{\rm W}(L)\rangle \equiv \frac{1}{\sqrt{L}}\left(|100\cdots0\rangle + |010\cdots0\rangle + \cdots + |000\cdots1\rangle\right)$ has $p = 1$, hence it does *not* contain superposition of macroscopically distinct states [11, 12]. This is reasonable because the W state corresponds to normal states in condense-matter physics, such as a Frenkel exciton excited in an insulating solid [21].

Since both the W state and product states have $p = 1$, they belong to the same class with respect to superposition of macroscopically distinct states. In contrast, states with $p = 2$ are extremely abnormal in view of many-body physics, as discussed in Sec. II C and Ref. [11].

Regarding the index q for mixed states, see Ref. [22] for several examples.

Appendix E: Approach of a pure state with $p = 2$ to a mixed state as $L \to \infty$

It was proved rigorously that any *pure* state with $p = 2$ in a *finite* system of size L does *not* approach pure states in an *infinite* system as $L \to \infty$ [11]. Although this might sound strange to the reader who is not familiar with quantum theory of infinite systems [30], its physics can be understood as follows.

In quantum theory of finite systems, all possible representations are equivalent (unitary equivalence). In quantum theory of infinite systems, in contrast, many representations can exist which are *not* equivalent to each other [30]. Among two or more inequivalent representations, we have to choose one that is suitable for describing the physical states of interest [30]. This makes the quantum theory of infinite systems much different from that of finite systems. The above strange fact comes from this great difference.

As the simplest example, consider a cat state $|\psi(L)\rangle \equiv (|00\cdots0\rangle + |11\cdots1\rangle)/\sqrt{2}$ of size L. If L is finite, there exist observables that have non-vanishing matrix elements between $|00\cdots0\rangle$ and $|11\cdots1\rangle$. The expectation values of such observables discriminate between the pure state $|\psi(L)\rangle$ and the mixed state $\rho(L) \equiv (|00\cdots0\rangle\langle00\cdots0| + |11\cdots1\rangle\langle11\cdots1|)/2$. If we take the $L \to \infty$ limit, however, the quantum theory of infinite systems requires that every observables should be a function of field operators within a *finite* region in an infinite space [30]. As a result, there are no observables that have non-vanishing matrix elements between the $L \to \infty$ limits of $|00\cdots0\rangle$ and $|11\cdots1\rangle$. This implies that $\lim_{L\to\infty}|\psi(L)\rangle$ is not a pure state. Here, the rigorous definition of pure states in Ref. [30] are used instead of the (over)simplified definition $\hat{\rho}^2 = \hat{\rho}$, because the latter can be used only for (an irreducible representation for) finite systems.

More mathematically speaking, if $|\psi(L)\rangle$ has $p = 2$ then $\lim_{L\to\infty}|\psi(L)\rangle$ is not a vector state of an irreducible representation. For details, see Ref. [11] and references cited therein.

Appendix F: Equivalence of $p_e = 2$ and $p = 2$

In this appendix, we show that if $p_e = 2$ then $p = 2$ and vice versa. For simplicity, we will omit 'ν' and '(L)', i.e., we will abbreviate $\hat{A}'(L), |\psi_\nu(L)\rangle, C_\nu(L)$ and so on to $\hat{A}', |\psi\rangle, C$ and so on, respectively. We first note that

$$\left\|\Delta\hat{A}'|\psi\rangle\right\|^2 = \left\|\sum_{l=1}^{L}\sum_{\alpha=1}^{D} c'_{l\alpha}\Delta\hat{b}_\alpha(l)|\psi\rangle\right\|^2 \le \left[\sum_{l=1}^{L}\sum_{\alpha=1}^{D}|c'_{l\alpha}|^2\right]\left[\sum_{l=1}^{L}\sum_{\alpha=1}^{D}\left\|\Delta\hat{b}_\alpha(l)|\psi\rangle\right\|^2\right] \le L\overline{O}(L), \tag{F1}$$

from which $p_e \le 2$. Here, we have used the inequality $\sum_k \left|\sum_j x_j y_{jk}\right|^2 \le \sum_k \sum_j |x_j|^2 \sum_{j'} |y_{j'k}|^2 = \sum_j |x_j|^2 \sum_{j'}\sum_k |y_{j'k}|^2$, which holds for arbitrary complex numbers x_j, y_{jk}. On the other hand, it is clear from the definitions that

$$p \le p_e. \tag{F2}$$

Therefore, if $p = 2$ then $p_e = 2$.

To show the inverse, we assume that $p_e = 2$, i.e., Eq. (22) holds. Without loss of generality, we also assume that $\max_{l,\alpha}|c'_{l\alpha\,\max}|^2 = |c'_{11\,\max}|^2$. It is clear from Eq. (20) that

$$|c'_{11\,\max}|^2 \le L. \tag{F3}$$

Our purpose is to show that

$$|c'_{11\,\max}|^2 = \overline{O}(L^0) \tag{F4}$$

because it yields $C = \overline{O}(L^0)$, which gives Eq. (25) (implying $p = 2$). Equation (22) can be rewritten as

$$\sum_{\alpha,\alpha'=1}^{D} c'^{*}_{1\alpha\,\max} c'_{1\alpha'\,\max} V_{1\alpha,1\alpha'} + \left(\sum_{l=2}^{L} \sum_{\alpha,\alpha'=1}^{D} c'^{*}_{l\alpha\,\max} c'_{1\alpha'\,\max} V_{l\alpha,1\alpha'} + c.c. \right) + \sum_{l,l'=2}^{L} \sum_{\alpha,\alpha'=1}^{D} c'^{*}_{l\alpha\,\max} c'_{l'\alpha'\,\max} V_{l\alpha,l'\alpha'} = \overline{O}(L^2) \tag{F5}$$

The first term is positive (because the VCM is a non-negative Hermitian matrix) and $\leq \overline{O}(L)$. The second term is estimated as

$$\begin{aligned} \left| \sum_{l=2}^{L} \sum_{\alpha,\alpha'=1}^{D} c'^{*}_{l\alpha\,\max} c'_{1\alpha'\,\max} V_{l\alpha,1\alpha'} \right| &\leq D|c'_{11\,\max}| \left| \sum_{l=2}^{L} \sum_{\alpha=1}^{D} c'^{*}_{l\alpha\,\max} \right| \max_{l,\alpha,\alpha'} |V_{l\alpha,1\alpha'}| \\ &\leq D|c'_{11\,\max}| \sqrt{D(L-1)} \sqrt{L} \max_{l,\alpha,\alpha'} |V_{l\alpha,1\alpha'}| \\ &\leq |c'_{11\,\max}| \overline{O}(L) \leq \overline{O}(L^{3/2}), \end{aligned} \tag{F6}$$

where we have used inequality (F3) and $|\vec{x} \cdot \vec{1}| \leq |\vec{x}||\vec{1}| = n|\vec{x}|$, which holds for an arbitrary n-dimensional vector $\vec{x}$. Therefore, the third term of Eq. (F5) should be

$$\sum_{l,l'=2}^{L} \sum_{\alpha,\alpha'=1}^{D} c'^{*}_{l\alpha\,\max} c'_{l'\alpha'\,\max} V_{l\alpha,l'\alpha'} = \overline{O}(L^2). \tag{F7}$$

On the other hand, let

$$c'_{l\alpha} \equiv \frac{1}{\sqrt{1 - \sum_{\alpha=1}^{D} |c'_{l\alpha\,\max}|^2 / L}} c'_{l\alpha\,\max}, \tag{F8}$$

then the following operator, which does not involve an operator on site 1, takes the form of Eq. (15);

$$\Delta \hat{A}' \equiv \sum_{l=2}^{L} \sum_{\alpha=1}^{D} c'_{l\alpha} \Delta \hat{b}_{\alpha}(l). \tag{F9}$$

We therefore have, using Eqs. (F6) and (F7),

$$\begin{aligned} 0 &\leq \langle \Delta \hat{A}'^{\nu\dagger}_{\max} \Delta \hat{A}'^{\nu}_{\max} \rangle_{L\nu} - \langle \Delta \hat{A}'^{\nu\dagger} \Delta \hat{A}'^{\nu} \rangle_{L\nu} \\ &\leq \sum_{\alpha,\alpha'=1}^{D} c'^{*}_{1\alpha\,\max} c'_{1\alpha'\,\max} V_{1\alpha,1\alpha'} + \left(\sum_{l=2}^{L} \sum_{\alpha,\alpha'=1}^{D} c'^{*}_{l\alpha\,\max} c'_{1\alpha'\,\max} V_{l\alpha,1\alpha'} + c.c. \right) \\ &\quad - \frac{|c'_{11\,\max}|^2}{L} \sum_{l,l'=2}^{L} \sum_{\alpha,\alpha'=1}^{D} c'^{*}_{l\alpha\,\max} c'_{l'\alpha'\,\max} V_{l\alpha,l'\alpha'} \\ &\leq |c'_{11\,\max}|^2 \overline{O}(L^0) + |c'_{11\,\max}| \overline{O}(L) - \frac{|c'_{11\,\max}|^2}{L} \overline{O}(L^2) \\ &\leq |c'_{11\,\max}| \left[|c'_{11\,\max}| \overline{O}(L^0) + \overline{O}(L) - |c'_{11\,\max}| \overline{O}(L) \right]. \end{aligned} \tag{F10}$$

Therefore, Eq. (F4) should be satisfied because otherwise the last line would become negative in contradiction with the first line.

For a family of homogeneous states, in particular, $p = p_e$ for every value of p, because in this case the VCM has the translational invariance and thus an eigenvector corresponding to $e_{\max}$ is also translational invariant. [Even when $e_{\max}$ is a degenerate eigenvalue, one can construct a translational-invariant eigenvector by taking linear combination of eigenvectors corresponding to $e_{\max}$.] From Eq. (20), this means $C = \overline{O}(L^0)$ for the additive operator that is composed of such an eigenvector, and thus $p \geq p_e$. From inequality (F2), this yields $p = p_e$.

Appendix G: Proof of $\langle \beta | \hat{M}_x | \beta \rangle = kL$ $(0 < k < 1)$ for $M = 2^{mL}$

In this appendix, we prove $\langle \beta | \hat{M}_x | \beta \rangle = KL$ $(0 < K < 1)$ for $M = 2^{mL}$ where K is independent of L. We use the following lemma:

Lemma: There exists a real number K independent of L such that $2^{(1-m)}(1-K)^{1-K}K^K > 1$ and $\frac{1}{2} < K < 1$.
Proof: Consider the following function;

$$f(k) = (1-m)\log 2 + k\log k + (1-k)\log(1-k) \ \ (\frac{1}{2} \leq k < 1), \tag{G1}$$

where $0 < m < 1$. Since $f(\frac{1}{2}) = -m\log 2 < 0$, $f(k) \to (1-m)\log 2 > 0$ $(k \to 1)$, and the function $f(k)$ is continuous at $\frac{1}{2} \leq k < 1$, we can apply a intermediate-value theorem and therefore there exists a real number K such that $f(K) > 0$ and $1/2 < K < 1$. ■

Now, we prove $\langle\beta|\hat{M}_x|\beta\rangle = kL$ $(0 < k < 1)$ for $M = 2^{mL}$. Let $P(M_x = -L+2j)$ be the probability of getting a value $-L+2j$ when one performs the measurement of $\hat{M}_x$ where $j = 0, 1, \cdots, L$. It is represented as

$$P(M_x = -L+2j) = \sum_{\nu} \left|\langle M_x = -L+2j, \nu|\beta\rangle\right|^2 \leq \binom{L}{j} \max_{\nu}[\ \left|\langle M_x = -L+2j, \nu|\beta\rangle\right|^2\ ], \tag{G2}$$

where $|M_x = L-j, \nu\rangle$ is an eigenstate of $\hat{M}_x$, and $\nu = 1, 2, \cdots, \binom{L}{j}$ labels degenerate eigenstates. Since

$$\left|\langle M_x = -L+2j, \nu|\beta\rangle\right| \leq \frac{1}{\sqrt{M}} \sum_{n=1}^{M} \left|\langle M_x = -L+2j, \nu|x_n\rangle\right| \leq \sqrt{\frac{M}{2^L}}, \tag{G3}$$

we have, using Stirling's formula $n! \sim \sqrt{2\pi n}(\frac{n}{e})^n$,

$$P(M_x = -L+2j) \leq \binom{L}{j}\frac{M}{2^L} \sim \frac{1}{\sqrt{2\pi j(1-\frac{j}{L})}\{2^{(1-m)}(1-\frac{j}{L})^{1-\frac{j}{L}}(\frac{j}{L})^{\frac{j}{L}}\}^L}. \tag{G4}$$

From the above Lemma, there exists a real number K independent of L such that $2^{(1-m)}(1-K)^{1-K}K^K > 1$ and $\frac{1}{2} < K < 1$. Hence,

$$L^n P(M_x = -L+2j) \to 0 \ \ (KL \leq j \leq L) \ \text{ as } L \to \infty, \tag{G5}$$

where n is independent of L. This yields

$$\langle\beta|\hat{M}_x|\beta\rangle \to \sum_{j=0}^{KL-1} (-L+2j)P(M_x = -L+2j) \tag{G6}$$

as $L \to \infty$, from which we conclude that $\langle\beta|\hat{M}_x|\beta\rangle \leq KL$ for large L. ■

Appendix H: Maximum eigenvalue of the VCM for product states

In this appendix, we show that $e_{\max} = 2$ for a product state, $|\psi\rangle = \bigotimes_{l=1}^{L} |\phi_l\rangle_l$, where $|\phi_l\rangle_l$ denotes a state of the qubit at site l $(= 1, 2, \cdots, L)$. The VCM of such a state is block-diagonal;

$$\begin{pmatrix} \boldsymbol{V}_1 & 0 & \cdots & \cdots & 0 \\ 0 & \boldsymbol{V}_2 & 0 & \cdots & \cdots \\ \vdots & 0 & \boldsymbol{V}_3 & 0 & \cdots \\ \vdots & \vdots & & \cdots & \cdots \\ 0 & \cdots & \cdots & 0 & \boldsymbol{V}_L \end{pmatrix}, \tag{H1}$$

where $\boldsymbol{V}_l$ is a 3×3 matrix whose $\alpha\beta$ element $(\alpha, \beta = x, y, z)$ is given by

$$(V_l)_{\alpha\beta} = \langle\phi_l|\hat{\sigma}_\alpha(l)\hat{\sigma}_\beta(l)|\phi_l\rangle - \langle\phi_l|\hat{\sigma}_\alpha(l)|\phi_l\rangle\langle\phi_l|\hat{\sigma}_\beta(l)|\phi_l\rangle. \tag{H2}$$

Therefore, $e_{\max}$ is given by the maximum one among the maximum eigenvalues of $\boldsymbol{V}_l$'s. By a unitary transformation of this 3×3 matrix such that $|\phi_l\rangle$ becomes an eigenstate of the transformed $\hat{\sigma}_z(l)$, we can transform $\boldsymbol{V}_l$ into

$$\boldsymbol{V}_l = \begin{pmatrix} 1 & i & 0 \\ -i & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}. \tag{H3}$$

Since the maximum eigenvalue of this matrix is 2, we find that $e_{\max} = 2$.

---

[1] 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.
[2] A. Ekert and R. Jozsa, Rev. Mod. Phys., **68**, 733 (1996).
[3] Lov K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[5] C. H. Bennett, S. Popescu, D. Rohrlich, J. A. Smolin, and A. V. Thapliyal, Phys. Rev. A **63**, 012307 (2000).
[6] A. Miyake and M. Wadati, Phys. Rev. A **64**, 042317 (2001).
[7] D. A. Meyer and N. R. Wallach J. Math. Phys. **43**(9), 4273 (2002).
[8] J. K. Stockton, J. M. Geremia, A. C. Doherty, and H. Mabuchi, Phys. Rev. A **67**, 022112 (2003).
[9] O. F. Syljuasen, Phys. Rev. A **68**, 060301 (2003).
[10] F. Verstraete, M. Popp, and J. I. Cirac, Phys. Rev. Lett. **92**, 027901 (2004).
[11] A. Shimizu and T. Miyadera, Phys. Rev. Lett. **89**, 270403 (2002). In this reference, states with $p = 2$ are called anomalously fluctuating states.
[12] T. Morimae, A. Sugita and A. Shimizu, Phys. Rev. A **71**, 032317 (2005).
[13] A. Sugita and A. Shimizu, J. Phys. Soc. Jpn. 74 (2005) 1883.
[14] S. Parker and M. B. Plenio, J. Mod. Optics **49**, 1325 (2002).
[15] Y. Shimoni, D. Shapiro and O. Biham, Phys. Rev. A **69**, 062303 (2004).
[16] Y. Shimoni, D. Shapiro and O. Biham, Phys. Rev. A **72**, 062308 (2005).
[17] R. Orús and J. Latorre, Phys. Rev. A **69**, 052308 (2004).
[18] R. Jozsa and N. Linden, Proc. R. Soc. London, Ser. A **459**, 2011 (2003)
[19] G. Vidal, Phys. Rev. Lett. **91**, 147902 (2003).
[20] A. Shimizu, talk presented at The 4th Symposium on Quantum Effects and Related Physical Phenomena (December 20-21, 2000, Tokyo, Japan); A. Shimizu and T. Miyadera, in *Proceedings of the 56th annual meeting of the Physical Society of Japan* (Physical Society of Japan, 2001), paper no. 28pYN-6.
[21] A. Ukena and A. Shimizu, Phys. Rev. A **69**, 022301 (2004).
[22] A. Shimizu and T. Morimae, Phys. Rev. Lett. **95**, 090401 (2005).
[23] T. Morimae and A. Shimizu, Phys. Rev. A **74**, 052111 (2006).
[24] For homogeneous states, it is obvious that $\hat{A}(L)$ should be homogeneously extended with increasing L. For example, if $\hat{A}(L) = \sum_{l=1}^{L} \hat{\sigma}_z(l)$ for some L, then $\hat{A}(L')$ for another L' ($\neq L$) should be $\sum_{l=1}^{L'} \hat{\sigma}_z(l)$. For this reason, the condition $\|\hat{a}(l)\| = 1$ was not imposed in Refs. [11, 12, 23]. On the other hand, we do *not* require here that $\hat{a}(l)$ is independent of L, because the independence is not well-defined when treating general families of states.
[25] R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).
[26] D. Gross, J. Eisert, N. Schuch, D. Perez-Garcia, Phys. Rev. A **76**, 052315 (2007).
[27] This expectation has been confirmed for one-way quantum computers by Y. Matsuzaki and A. Shimizu, unpublished.
[28] Y. Matsuzaki and A. Shimizu, in *Proceedings of the 61st annual meeting of the Physical Society of Japan* (Physical Society of Japan, 2006), paper no. 28aSA-4.
[29] One can also apply the theories of Refs. [11, 22] to n-point correlations, if n (≥ 3) is independent of the system size L and if the n points can be divided into two groups $1, 2$ in such a way that the maximum distance ℓ_i ($i = 1, 2$) between two points in each group is independent of L. In fact, let $\ell \equiv \max_i \ell_i$, and regard each ℓ neighboring sites as a new site. The original lattice composed of L sites then becomes a new lattice composed of L/ℓ new sites. Then, the original n-point correlations become two-point correlations of the new lattice, and the theories of Refs. [11, 22] are applicable to the new lattice. By interpreting the results in terms the original sites, one obtains the corresponding results for the n-point correlations.
[30] See, e.g., R. Haag, *Local Quantum Physics* (Springer, Berlin, 1992).
[31] D. Deutsch and R. Jozsa, Proc.Royal Soc. London A **439**, 553 (1992).
[32] P. W. Shor, Phys. Rev. A **52** R2493.
[33] J. Preskill, Proc. R. Soc. London, Ser. A **454**, 385 (1998), and references cited therein.
[34] N. Lynch, J. Assoc. Comput. Mach. **22**, 341 (1975).
[35] P. Orponen and U. Schöning, Mathematical Foundations of Computer Science 1984 (Springer, Berlin, 1984), pp. 452-458.
[36] S. Even, A. L. Selman and Y. Yacobi, J. Assoc. Comput. Mach. **32**, 205 (1985).
[37] R. V. Book and D-Z. Du, J. Assoc. Comput. Mach. **34**, 718 (1987).
[38] Strictly speaking, this picture is not necessarily correct because when quantum states are strongly inhomogeneous $Le_{\max}$ is not necessarily proportional to the number of pairs of sites whose correlation is of $\overline{\Theta}(1)$. Fortunatelly, however, this picture is good for most instances in our simulations.
[39] A. Carlini et al., Phys. Rev. Lett. **96**, 060503 (2006), and references cited therein.
[40] A. Hosoya, private communication.