Quantum nonexpander problem is quantum-Merlin-Arthur-complete

The MIT Faculty has made this article openly available. Please share how this access benefits you. Your story matters.

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>As Published</td>
<td><a href="http://dx.doi.org/10.1103/PhysRevA.87.042317">http://dx.doi.org/10.1103/PhysRevA.87.042317</a></td>
</tr>
<tr>
<td>Publisher</td>
<td>American Physical Society</td>
</tr>
<tr>
<td>Version</td>
<td>Final published version</td>
</tr>
<tr>
<td>Citable link</td>
<td><a href="http://hdl.handle.net/1721.1/88738">http://hdl.handle.net/1721.1/88738</a></td>
</tr>
<tr>
<td>Terms of Use</td>
<td>Article is made available in accordance with the publisher’s policy and may be subject to US copyright law. Please refer to the publisher’s site for terms of use.</td>
</tr>
</tbody>
</table>
Quantum nonexpander problem is quantum-Merlin-Arthur-complete

Adam D. Bookatz,†,‡ Stephen P. Jordan,1,§ Yi-Kai Liu,2,† and Pawel Wocjan3,‡

1Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, Massachusetts, USA
2National Institute of Standards and Technology, Gaithersburg, Maryland, USA
3Mathematics Department & Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, Massachusetts, USA

(Received 16 December 2012; published 15 April 2013)

A quantum expander is a unital quantum channel that is rapidly mixing, has only a few Kraus operators, and can be implemented efficiently on a quantum computer. We consider the problem of estimating the mixing time (i.e., the spectral gap) of a quantum expander. We show that the problem of deciding whether a quantum channel is not rapidly mixing is a complete problem for the quantum Merlin-Arthur complexity class. This has applications to testing randomized constructions of quantum expanders and studying thermalization of open quantum systems.

DOI: 10.1103/PhysRevA.87.042317 PACS number(s): 03.67.–a, 89.70.Eg

I. INTRODUCTION

A quantum expander is a unital quantum channel that is rapidly mixing. This means that with repeated applications of the channel, every quantum state is rapidly contracted to the maximally mixed state, which is the unique fixed point. In addition, a quantum expander has only a small number of Kraus operators, each of which is described by an efficient quantum circuit. Quantum expanders are quantum analogs of expander graphs, which play a prominent role in computer science and discrete mathematics [1]. The idea of quantum expanders was introduced in [2,3]. Since then, several explicit constructions of quantum expanders have been discovered, and quantum expanders have found various applications in quantum information theory, such as constructing quantum states with unusual entanglement properties and simulating thermalization in quantum systems [4–9].

Here we study the problem of estimating the mixing rate of a quantum expander. Given a quantum channel \( \Phi \) of the above form (a small number of Kraus operators, specified by quantum circuits), this problem is to estimate the spectral gap of \( \Phi \). This problem arises in connection with randomized constructions of quantum expanders [9], where with high probability one obtains a good expander, but it is not obvious how to test that a particular instance of the construction is in fact good. In addition, this problem can be viewed as a special case of a more general question: given an open quantum system, determine whether it thermalizes, and on what time scale. (The behavior of a quantum expander is roughly equivalent to that of a quantum system with a particular weak coupling to a bath of harmonic oscillators.)

Formally, we define the “quantum nonexpander problem” (which is the complement of the above problem), and we give evidence that this problem is computationally intractable: We prove that it is QMA-complete. Here QMA (quantum Merlin-Arthur) is a complexity class that is a quantum analog of NP (nondeterministic polynomial time) [10–12]. Proving that a problem is QMA-complete implies that it is equivalent (up to polynomial-time reductions) to all other QMA-complete problems [11,13–19], a survey of which can be found in [20]. In particular, this implies that the problem cannot be solved in polynomial time (unless QMA = BQP). Furthermore, this implies that our original problem, the “quantum expander problem”, is complete for the complexity class co-QMA (where co-QMA is the class of all problems whose complements are in QMA); hence the “quantum expander problem” cannot be in QMA (unless QMA = co-QMA). In other words, when a channel \( \Phi \) is not a quantum expander, there is an efficiently verifiable quantum proof of that fact; but when \( \Phi \) is a quantum expander, there is no way of giving an efficiently verifiable quantum proof.

II. PRELIMINARIES

A. The quantum nonexpander problem

We use the definition of explicit quantum expanders due to Ben-Aroya, Schwartz, and Ta-Shma [4]. For an \( n \)-dimensional Hilbert space \( \mathcal{H} \), let \( L(\mathcal{H}) \) denote the space of linear operators from \( \mathcal{H} \) to itself. A superoperator \( \Phi : L(\mathcal{H}) \to L(\mathcal{H}) \) is admissible if it is a completely positive and trace-preserving map. An admissible superoperator is unitary if \( \Phi(I) = I \), where \( I = \frac{1}{n} \mathbb{1} \) is the maximally mixed state on \( \mathcal{H} \) (where \( I \) is the identity operator on \( \mathcal{H} \)). A unital superoperator is \( D \)-regular if \( \Phi = \frac{1}{D} \sum \Phi_d \), and for \( d = 1, \ldots, D \), \( \Phi_d(X) = U_d X U_d^\dagger \), where the \( U_d \) are unitary transformations on \( \mathcal{H} \). The unitaries \( U_d \) are called the operation elements (or Kraus operators) of \( \Phi \), and \( D \) is called the degree of \( \Phi \). A \( D \)-regular superoperator is explicit if each of its operation elements can be implemented by a quantum circuit of size \( \log(N) \), where \( N \) is the dimension of \( \mathcal{H} \).

Definition 1 (quantum expander). A \( D \)-regular superoperator \( \Phi : L(\mathcal{H}) \to L(\mathcal{H}) \) is a \( \kappa \)-contractive expander if for all \( A \in L(\mathcal{H}) \) that are orthogonal to \( I \) with respect to the Hilbert-Schmidt inner product, that is, \( \text{Tr}(\Phi A) = 0 \), it holds that

\[
\| \Phi(A) \|_F \leq \kappa \| A \|_F. \tag{1}
\]

Here the Frobenius norm is given by \( \| A \|_F = \sqrt{\sum_{i,j} |a_{ij}|^2} \), where \( a_{ij} \) are the entries of the matrix \( A \). The quantity \( 1 - \kappa \) is called the spectral gap of \( \Phi \).
Remark 1. The motivation for this definition can easily be seen from the following argument. A good quantum expander $\Phi$ rapidly sends any density matrix $\rho$ to the maximally mixed state $I$. Because $\text{Tr}[\rho] = \text{Tr}[I] = 1$ we can always write $\rho = I + A$ where $\text{Tr}[A] = 0$. The requirement of Eq. (1) therefore formalizes the idea of $\Phi$ bringing $\rho$ towards $I$ by rapidly killing off the $A$ term. In this context Eq. (1) is equivalent to demanding that $\|\Phi(\rho) - I\|_F \leq \kappa \|\rho - I\|_F$, which clearly encapsulates the idea of $\Phi$ rapidly sending density matrices towards the maximally mixed state. Note that in this argument $A = \rho - I$ is Hermitian; however, it can be shown that if Eq. (1) applies for traceless Hermitian matrices, it also applies for traceless matrices in general, thus justifying Definition 1.

We consider the problem of estimating the mixing time of a quantum expander. Formally, we study the following decision problem:

Definition 2 (quantum nonexpander problem). Fix some encoding such that each string $x \in \{0,1\}^n$ specifies the following: an explicit $D$-regular superoperator $\Phi: (\mathbb{C}^2)^{\otimes m} \rightarrow (\mathbb{C}^2)^{\otimes m}$, with operation elements $U_1, \ldots, U_D$, and two parameters $\alpha > \beta$.

We will consider instances which satisfy the following promises: $m$ and $D$ are upper-bounded by (fixed) polynomials in $|x|$; the parameters $\alpha$ and $\beta$ are polynomially separated, i.e., they satisfy $\alpha - \beta \geq \frac{1}{\sqrt{|x|}}$ for some (fixed) polynomial $q$; and the operation elements $U_1, \ldots, U_D$ are given as quantum circuits of size at most $r(|x|)$ for some (fixed) polynomial $r$.

The “quantum nonexpander” problem is the task of deciding which of the following is correct, given the promise that exactly one of them is correct:

(1) $\Phi$ is not an $\alpha$-contractive expander (YES case).
(2) $\Phi$ is a $\beta$-contractive expander (NO case).

B. Thermalization of open quantum systems

To motivate the “quantum nonexpander” problem, we now describe a connection between that problem and the study of thermalization in open quantum systems. We show an example of a quantum system coupled to a bath, where the system thermalizes and the relaxation time is determined by the spectral gap of a certain quantum expander.

Let the system consist of $m$ qubits, and fix some unitary transformations $U_a$ (for $a = 1, \ldots, D$) which act on $(\mathbb{C}^2)^{\otimes m}$. Let the bath consist of a large number of harmonic oscillators, with annihilation operators $b^\dagger_{a k}$ (for $a = 1, \ldots, D$ and $k \in \Omega$, where $\Omega$ is some large set). Let the total Hamiltonian be

$$H = H_S + \varepsilon H_I + H_B,$$

where the system Hamiltonian is $H_S = 0$, the bath Hamiltonian is

$$H_B = \sum_k \sum_a \omega_k b^\dagger_{a k} b_{a k},$$

and the interaction Hamiltonian is

$$H_I = \sum_a (U_a \otimes f_a) + (U^\dagger_a \otimes f^\dagger_a),$$

where the operators $f_a$ are defined by $f_a = \frac{1}{\sqrt{|a|}} \sum_k b_{a k}$.

In the weak-coupling limit ($\varepsilon \to 0$), the time evolution of the system is described by a master equation [21]. Suppose the bath is in a thermal state, $\rho_B = (1/Z_B) \exp(-H_B/T)$. Then the master equation takes the following form:

$$\frac{d}{dt} \rho_S(t) = R_0 \sum_a (U_a \rho_S(t) U^\dagger_a - \rho_S(t)) + R_1 \sum_a (U^\dagger_a \rho_S(t) U_a - \rho_S(t)),$$

where $\rho_S(t)$ is the state of the system at time $t$, and $R_0$ and $R_1$ are positive real numbers. Equation (5) has two special features: There is no contribution from a “Lamb shift” Hamiltonian, and the dissipator is in diagonal form with Lindblad operators which are unitary. (See Appendix 1 for the derivation of this equation.)

Now define the quantum channel

$$\Phi(\rho) = \frac{R_0}{(R_0 + R_1)D} \sum_a U_a \rho U^\dagger_a + \frac{R_1}{(R_0 + R_1)D} \sum_a U^\dagger_a \rho U_a.$$

This channel $\Phi$ is a (nonuniform) mixture of unitary operations. In the special case where the set of unitaries $\{U_a \mid a = 1, \ldots, D\}$ is closed with respect to the adjoint operation (i.e., for every $1 \leq a \leq D$, there exists some $1 \leq \beta \leq D$ such that $U_a = U^\dagger_{\beta}$), the channel $\Phi$ can be written as

$$\Phi(\rho) = \frac{1}{D} \sum_a U^\dagger_a \rho U_a;$$

hence $\Phi$ is a $D$-regular superoperator, as described in the definition of a quantum expander.

The master equation can now be rewritten in terms of $\Phi$:

$$\frac{d}{dt} \rho_S(t) = (R_0 + R_1)D (\Phi - I)[\rho_S(t)],$$

where $I$ denotes the identity channel. We can solve for $\rho_S(t)$:

$$\rho_S(t) = \exp[t(R_0 + R_1)D(\Phi - I)][\rho_S(0)].$$

Thus the system converges to the maximally mixed state as $t \to \infty$, and the rate of convergence depends on the spectral gap of $\Phi$. More precisely, write $\rho_S(t) = \tilde{I} + A(t)$ where $A(t)$ is traceless. Then it can be verified that

$$\|A(t)\|_F \leq \exp[-t(R_0 + R_1)D(1 - \kappa)]\|A(0)\|_F.$$
Arthur to accept with high probability, but if \( x \notin L \) then Arthur will reject all states with high probability. QMA is a quantum analog of MA, which is the probabilistic analog of NP.

**Definition 3** \([\text{QMA}(a,b)]\). A language \( L \) is in \( \text{QMA}(a,b) \) if for each \( x \in \{0,1\}^* \) one can efficiently generate a quantum circuit \( V \) with the following properties:

1. \( V \) acts on the Hilbert space \( \mathcal{W} \otimes \mathcal{A} \), where
   \[ \mathcal{W} = (\mathbb{C}^2)^{\otimes n}, \quad \mathcal{A} = (\mathbb{C}^2)^{\otimes n}, \]
   and the functions \( n_w, n_a : \mathbb{N} \to \mathbb{N} \) grow at most polynomially in \( |x| \).
2. \( V \) consists of \( s(|x|) \) elementary gates where the function \( s : \mathbb{N} \to \mathbb{N} \) grows at most polynomially in \( |x| \).
3. If \( x \in L \) (YES case) then there exists a witness state \( |\psi\rangle \in \mathcal{W} \) such that
   \[ \| PV |\psi\rangle \|_F^2 \geq a. \]  
4. If \( x \notin L \) (NO case) then for all states \( |\psi\rangle \in \mathcal{W} \) we have that
   \[ \| PV |\psi\rangle \|_F^2 \leq b. \]

Here \( \mathcal{W} \) and \( \mathcal{A} \) are the witness and ancilla registers, respectively, and \( P = \{1\} \{1\} \{1\} \) projects onto the subspace of the first qubit of \( \mathcal{W} \otimes \mathcal{A} \) being in the state \( |1\rangle \). The state \( |0\rangle = |00\ldots0\rangle \) is the all-zeros state on \( \mathcal{A} \).

Observe that \( V, \mathcal{W}, A, n_x, n_y, \) and \( P \) depend on \( x \); however, to avoid unnecessarily complicated notation, we do not indicate this explicitly.

**Remark 2.** It is conventional to define QMA = QMA(2/3,1/3). However, the complexity class QMA(\(a,b\)) is highly insensitive to the particular values of \( a \) and \( b \). In fact, even if \( a \) and \( b \) are functions of the problem size \( n \), it remains true that QMA(\(a(n),b(n)\)) = QMA provided \( a(n) - b(n) \geq \frac{1}{p(n)} \) for some polynomial \( p \). It is always possible to achieve that \( a = 1 - \varepsilon \) and \( b = \varepsilon \) by increasing the size of the circuit by a factor \( \text{polylog}(1/\varepsilon) \) and increasing \( n_x \) by \( \text{polylog}(1/\varepsilon) \) qubits, with no change in \( n_w \) [22,23].

## III. QUANTUM NONEXPANDER IS IN QMA

We now show that the problem defined in Definition 2 is in QMA. We first consider the YES case. In this case, Merlin has to convince Arthur that there exists a traceless matrix \( A \) such that

\[ \| \Phi(A) \|_F \geq \alpha \| A \|_F. \]  

We may assume without loss of generality that \( \| A \|_F = 1 \). Clearly, Merlin cannot directly send the matrix \( A \) because it is an exponentially large matrix. Instead, he can send the quantum certificate

\[ |\psi_A\rangle = \sum_{i,j=1}^{N} a_{ij} |i\rangle \otimes |j\rangle \]

encoding the matrix \( A \). We show that \( |\psi_A\rangle \) can serve as a witness making it possible to convince Arthur that the inequality in Eq. (8) holds.

Arthur’s verification protocol makes use of the following facts:

\[ \| \Phi(A) \|_F^2 = \langle \psi_A | \psi_A \rangle, \quad \text{Tr}[A] = \sqrt{N} \langle \varphi | \psi_A \rangle, \]

and

\[ W = \frac{1}{D} \sum_{d=1}^{D} U_d \otimes \overline{U}_d, \]

where \( U_d \) denotes the complex conjugate of \( U_d \).

First, to check whether \( \text{Tr}[A] = 0 \), Arthur verifies that \( |\psi_A\rangle \) is orthogonal to \( |\varphi\rangle \). Second, to estimate the contractive factor, Arthur estimates the expectation value \( \langle \psi_A | W^\dagger W | \psi_A \rangle \) of \( W^\dagger W \). For \( d = 1, \ldots, D \), define the unitaries

\[ V_{d,e} = (U_d^\dagger \otimes U_e^\dagger)(U_e \otimes \overline{U}_d). \]

Note that \( V_{d,e} = V_{e,d}^\dagger \) and \( V_{d,d} = 1 \). The expectation value can be expressed as

\[ \langle \psi_A | W^\dagger W | \psi_A \rangle = \frac{1}{D} \sum_{d,e} \langle \psi_A | V_{d,e} | \psi_A \rangle \]

\[ \leq \frac{1}{D} + \sum_{d,e} \text{Re} \langle \psi_A | V_{d,e} | \psi_A \rangle. \]

Arthur can estimate the values \( \text{Re} \langle \psi_A | V_{d,e} | \psi_A \rangle \) using the Hadamard test (shown in Fig. 1, since it will output 1 with probability Pr(1) = \( \frac{1}{2} (1 + \text{Re} \langle \psi_A | V_{d,e} | \psi_A \rangle) \)). From this Arthur can calculate \( \langle \psi_A | W^\dagger W | \psi_A \rangle = \| \Phi(A) \|_F^2 \) and ensure it exceeds \( \alpha^2 \).

Now consider the NO case. In this case, Arthur’s first measurement projects the state \( |\psi_A\rangle \) onto the subspace orthogonal to \( |\varphi\rangle \); and by definition, all states \( |\psi_A\rangle \) in that subspace must satisfy

\[ \langle \psi_A | W^\dagger W | \psi_A \rangle \leq \| \Phi(A) \|_F^2 \leq \beta^2. \]

This shows that Merlin cannot cheat, that is, make Arthur believe that there exists a quantum state with contraction greater or equal to \( \alpha \), provided that Arthur estimates the expected value sufficiently well and with sufficiently high probability of confidence.

As in the original definition of QMA in [11], we may assume that Arthur has multiple copies of the quantum certificate \( |\psi\rangle \) so that we can estimate the expected value sufficiently well. Using the powerful technique of in-place amplification [22], we can transform a quantum circuit requiring \( |\psi\rangle^{\otimes k} \) into one that requires only a single copy of \( |\psi\rangle \).

## IV. SOME TECHNICAL TOOLS

### A. The Frobenius norm

In the proof that quantum nonexpander is QMA-hard we will frequently make use of the Frobenius norm; we therefore present some useful facts about this norm here. If \( B \) is a matrix
with entries $b_{ij}$, then the Frobenius norm is defined as
\[
\|B\|_F = \sqrt{\text{Tr}[B^†B]} = \sqrt{\sum_{ij} |b_{ij}|^2}.
\]  

(9)

We have the following identities: $\|A \otimes B\|_F = \|A\|_F \|B\|_F$, $\text{Tr}[A \otimes B] = \text{Tr}[A] \text{Tr}[B]$, and of course $\text{Tr}[A + B] = \text{Tr}[A] + \text{Tr}[B]$. If $|\psi\rangle$ and $|\phi\rangle$ are pure states then
\[
\|\psi\langle\phi\|_F = \sqrt{\langle\psi|\psi\rangle\langle\phi|\phi\rangle} = \|\psi\|_F \|\phi\|_F.
\]

(10)

Note that $\|0\rangle\langle 0\|_F = \|1\rangle\langle 1\|_F = 1$.

In this paper we denote the Pauli matrices on one qubit by $\sigma_i$, with $\sigma_0 = 1$, $\sigma_1 = \sigma_x$, $\sigma_2 = \sigma_y$, and $\sigma_3 = \sigma_z$. Consider any traceless matrix $A$ that acts on some space $\mathbb{C}^d \otimes \mathbb{C}^2$, where we will refer to the second subspace (i.e., single-qubit subspace) as the indicator qubit register. Because the Pauli matrices $\sigma_i$ form a basis for the matrices acting on the indicator qubit register, we can decompose $A$ as $\sum_{i=0}^3 A_i \otimes \sigma_i$, where $A_i$ are matrices on the combined multiqubit subspace (the witness and ancilla registers that we will see later). Because $\sigma_i$ are traceless for $i = 1, 2, 3$, the traceless condition on $A$ therefore becomes $\text{Tr}[A_0] = 0$. Moreover, because the Pauli matrices are orthogonal with respect to the trace inner product and all satisfy $\|\sigma_i\|_F^2 = 2$, we have $\|\sum_i A_i \otimes \sigma_i\|_F^2 = \sum_i \|A_i \otimes \sigma_i\|_F^2 = 2 \sum_i \|A_i\|_F^2$, giving the inequality
\[
\left\|\sum_{i=0}^3 A_i \otimes \sigma_i\right\|_F \geq \sqrt{2}\|A_0\|_F.
\]

(11)

A quantum operation $G$ is called a pinching operator if $G(B) = \sum_i PBP$ where $P$ is nonoverlapping projectors with $\sum_i P = 1$. Pinching operators are trace preserving,
\[
\text{Tr}\left[\sum_i PBP\right] = \text{Tr}[B],
\]

(12)

and moreover (by the pinching inequality) cannot increase Frobenius norm:
\[
\left\|\sum_i PBP\right\|_F \leq \|B\|_F.
\]

(13)

It should be noted that a quantum expander $E$ is also norm-nonincreasing,
\[
\|E(B)\|_F \leq \|B\|_F,
\]

(14)

and similarly for any projector $P$,
\[
\|PBP\|_F \leq \|B\|_F.
\]

(15)

B. Controlled expanders

The remainder of our paper will make repeated use of controlled expanders, which we introduce here. If $U$ is a unitary gate, we use the notation $\Lambda U$ to indicate a controlled-$U$ operation.

Definition 4 (controlled expander). Let $F$ be a quantum expander with operation elements $\{U_i : i = 1 \ldots m\}$ so that $F(B) = \sum_{i=1}^m U_i B U_i^†$. The controlled expander $\Lambda F$ is defined to be the $m$-regular superoperator whose operation elements are the controlled unitaries $\{\Lambda U_i : i = 1 \ldots m\}$.

More explicitly, consider two registers, a control register and a target register, and suppose that an expander $F$ acts on the target register as $F(B) = \sum_{i=1}^m U_i B U_i^†$. Decompose the control register into two orthogonal subspaces, and let $Q$ and $P$ be projectors onto these two subspaces (so $Q + P = 1$ and $PQ = QP = 0$). Suppose that the controlled operations $\Lambda U_i$ are to be applied when the control register is in the subspace corresponding to $P$; thus $\Lambda U_i = P \otimes U_i + Q \otimes 1$. Consider a matrix $A \otimes B$, where $A$ and $B$ act on the control and target registers, respectively. Then the controlled expander $\Lambda F$, with operation elements $\Lambda U_i$, acts on $A \otimes B$ as
\[
\Lambda F(A \otimes B) = \sum_{i=1}^m [(\Lambda U_i)(A \otimes B)(\Lambda U_i^†)]
\]
\[
= \sum_{i=1}^m [P \otimes U_i + Q \otimes 1](A \otimes B)(P \otimes U_i^†)
\]
\[
+ Q \otimes 1
\]
\[
= \sum_{i=1}^m [PAP \otimes U_i BU_i^† + PAQ \otimes U_i B]
\]
\[
+ QAP \otimes BU_i^† + QAQ \otimes B
\]
\[
= PAP \otimes \left(\sum_{i=1}^m U_i BU_i^†\right)
\]
\[
+ PAQ \otimes \left(\sum_{i=1}^m U_i\right) B
\]
\[
+ QAP \otimes B \left(\sum_{i=1}^m U_i^†\right) + QAQ \otimes B.
\]

(16)

Note that if we impose on $F$ the requirement that
\[
\sum_i U_i = 0,
\]

(17)

then we obtain
\[
\Lambda F(A \otimes B) = PAP \otimes F(B) + QAQ \otimes B,
\]

(18)

which is how we would naturally desire a controlled expander to act. Unfortunately, unlike Eq. (18), Eq. (16) has additional cross-terms whose elimination would greatly simplify our future analysis.

We will, however, freely assume that Eq. (17) is satisfied, justified by the following observation. If necessary, we may always increase the set of operation elements of $F$ from $\{U_i : i = 1 \ldots m\}$ to $\{U_i : i = 1 \ldots m\} \cup \{-U_i : i = 1 \ldots m\}$. Such a change has no effect on the original expander $F$; the expander $F(B) = \sum_{i=1}^m (U_i BU_i^†)$ is invariant under $U_i \leftrightarrow -U_i$, even though the controlled expander $\Lambda F(B) = \sum_{i=1}^m (\Lambda U_i B \Lambda U_i^†)$ is not necessarily invariant under $U_i \leftrightarrow -U_i$. Thus, with only a factor of two overhead in the number of unitaries, we may satisfy the condition of Eq. (17), thereby eliminating the undesired cross-terms; as such, Eq. (18) may effectively be taken as the definition of a controlled expander.

A concrete example of a controlled expander—and one of particular importance in this paper—is the controlled complete depolarizer. Throughout this paper we use $\mathcal{D}$ to denote the
complete depolarizing channel on a single qubit, which is
normally defined to apply a unitary from \{1, X, Y, Z\} with
uniform probability 1/4. To ensure that Eq. (17) is satisfied,
we therefore define the effect of \( D \) on a matrix \( \sigma \) to be
\[
D(\sigma) = \frac{1}{8} \sum_{W} W \sigma W = \frac{1}{2} \text{Tr}[\sigma],
\]
where the sum is over \( W \in \{1, X, Y, Z, -1, -X, -Y, -Z\} \).
and the second one only if the top output is zero. The controlled \( E \)
expander is applied only if the bottom qubit is one. Note that this
figure is not a true circuit because \( D \) and \( E \) are quantum expanders,
ot unitary gates.

\[
\Lambda D(\Lambda \otimes \sigma) = PAP \otimes \frac{1}{2} \text{Tr}[\sigma] + QAQ \otimes \sigma.
\]

Although controlled expanders are not actually quantum
gates, we will nevertheless include them in circuit diagrams.
If \( \Lambda F(B) = \frac{\Lambda}{8} \sum (\Lambda U_i B A U_i^\dagger) \) then the circuit in Fig. 2 is to
be interpreted as applying an element selected uniformly at
random from the set \( \{\Lambda U_i\} \) (or equivalently, as applying to
the target register a unitary selected uniformly at random from
the set \( \{U_i\} \) but only if the control register is in the
appropriate state). As a final remark note that although a controlled
expander is a unital map, it is not itself a good expander (first,
because depending on the control qubit, the operator might not
do anything at all, and second, because even when the operator
does act, it only expands on the subspace of the target, not the
entire space). For example, note that \( |0\rangle\langle 0| \otimes |0\rangle\langle 0| \)
is not contracted at all by the controlled complete depolarizer \( \Lambda D \),
thus indicating that \( \Lambda D \) is not a good expander.

V. QUANTUM NONEXPANDER IS QMA-HARD

A. Outline of the proof
Let \( L \) be any language in QMA(\( \frac{\epsilon}{2}, \frac{1}{2} \)). We show that the
quantum nonexpander problem is QMA-hard by reducing \( L \)
to a quantum nonexpander problem. Specifically, let \( x \) be an
|\( x \)-bit problem instance whose inclusion in \( L \), or lack thereof,
we wish to determine. Because \( L \in \text{QMA} \) we have access to a
verifier circuit satisfying Eqs. (6) and (7) acting on a witness
space of \( n_w = \text{poly}(|x|) \) qubits and some ancilla space.
For reasons that will become apparent later, we now use QMA
amplification to give that \( L \in \text{QMA}(a,b) \) for polynomially
separated \( a \) and \( b \), where
\[
a > 0.99 \quad \text{and} \quad b < (0.1)^{-2(n_w+1)}.\]

Note from Remark 2 that this can be done without increasing
the size of the witness space of the verifier. Let the resulting
QMA(\( a,b \)) verifier circuit be called \( V \), which acts on the same
witness space of \( n_w = \text{poly}(|x|) \) qubits and some ancilla space
of \( n_a = \text{poly}(|x|) \) ancilla qubits. Merlin can provide Arthur a
valid (with high probability) witness if and only if \( x \in L \).

Let \( \mathcal{E} \) be an explicit \( \kappa_\mathcal{E} \)-contracting expander of degree \( D_\mathcal{E} \)
acting on \( n_w + n_a \) qubits, where \( \kappa_\mathcal{E} < 0.1 \) and \( D_\mathcal{E} \) is constant
(independent of \( |x| \)). Such expanders are known to exist, as
we outline in Appendix 2 using Ref. [24]. Using \( V \) and \( \mathcal{E} \), we create a quantum expander \( \Phi \) that is bad if \( x \in L \) but good
if \( x \notin L \); indeed, we will present polynomially separated (in
fact, constant) \( \alpha \) and \( \beta \) such that \( \Phi \) is a \( \beta \)-contracting expander
if \( x \notin L \) but is not an \( \alpha \)-contracting expander if \( x \in L \).
The circuit for \( \Phi \) is shown in Fig. 3, which we now describe in
detail.

The map \( \Phi \) acts on three registers, which from top to bottom
are the witness register (of \( n_w \) qubits), the ancilla register (of
\( n_a \) qubits), and an additional single-qubit register we call the
indcator qubit register. The circuit is realized by composing
the following three maps:
(1) the ancilla verifier,
(2) the witness verifier,
(3) the controlled \( \mathcal{E} \).

The basic idea is that if \( x \in L \) then Merlin can provide a
valid witness and properly initialized ancillae that will pass
the verifiers and not be mixed by the final controlled expander
(indicating that our quantum expander is bad); conversely,
if \( x \notin L \) then no matter what witness and ancilla qubits
Merlin provides, the indicator qubit will be depolarized and
consequently his state will be well mixed by the final controlled
expander (indicating our expander to be good).

We now provide a detailed description of the three different
maps and their purposes.

(1) The ancilla verifier is the first gate in Fig. 3. It is
the controlled expander \( \Lambda_{\text{anc}} \mathcal{D} \), which applies the complete
depolarizer \( D \) to the indicator qubit register only if any of the
ancilla bits are 1 (i.e., if they are not all 0). More technically, it is
\[
\Lambda_{\text{anc}} \mathcal{D}(B) = \frac{1}{8} \sum_{W} \Lambda_{\text{anc}} W B \Lambda_{\text{anc}} W^\dagger
\]
(with \( W \in \{1, X, Y, Z, -1, -X, -Y, -Z\} \)), where \( \Lambda_{\text{anc}} W \) is
the gate shown in Fig. 4. Note that \( \Lambda_{\text{anc}} W \) requires a controlled-
(\( W \) gate controlled by \( n_a \) qubits, which can be implemented
with \( n_a^2 \) gates using no extra work qubits [25]. (It is important
that the implementation not require work qubits, because we demand that there be no internal ancillae; our expander must be an expander on the entire space, not just a subspace.) Intuitively, if the ancilla qubits are not initialized to be all 0’s, the verifier will depolarize the indicator qubit, whence the term ancilla verifier.

(2) The witness verifier consists of the next three operations in Fig. 3. First, $V$ operates on the witness and ancilla registers, with its output on the top qubit (with $|1\rangle$ signifying that the witness is valid, $|0\rangle$ signifying that it is invalid); the lower multiqubit register of $n_w+n_a-1$ qubits contains the rest of $V$’s output (required by reversibility). A controlled-depolarizer then acts on the indicator qubit, conditioned upon the top qubit being $|0\rangle$ (i.e., failing the witness verification). The effects of $V$ are then uncomputed with $V^\dagger$. At this point, intuitively, the indicator qubit has been depolarized if and only if the input failed either the ancilla verifier or the witness verifier (or both).

(3) Finally, the last operation, which is the controlled expander $A_{\text{ind}}E$, acts, conditioned on whether the indicator qubit is $|1\rangle$. Intuitively, if the input was $|\psi\rangle \otimes |0\rangle \otimes |0\rangle$, with the indicator qubit initialized to $|0\rangle$, with the ancilla qubits initialized to $|0\rangle = |00\ldots0\rangle$, and with $|\psi\rangle$ a valid witness (for $x \in L$), then the indicator qubit will remain $|0\rangle$ and nothing will happen; if, on the other hand, the witness/ancillae failed any of the verifiers, thus depolarizing the indicator qubit to be $\frac{1}{2} (I+1) = \frac{1}{2} |0\rangle \langle 0| + \frac{1}{2} |1\rangle \langle 1|$, then $E$ will act on the top registers, resulting in a highly mixed output (across all three registers).

Note that because $E$ is an explicit $D_2$-regular expander (where $D_\infty$ is a constant), $\Phi$, being the composition of two explicit $8$-regular superoperators and $A E$, is manifestly explicit and $64 D_2$-regular (i.e., of constant degree). We now proceed to show that $\Phi$ is indeed a good expander if $x \not\in L$ (the NO case) but not if $x \in L$ (the YES case).

B. Analysis of NO case

First, consider the case in which $x \not\in L$. We wish to show that $\Phi$ is a good expander, and therefore by Eq. (1), that it sufficiently decreases the Frobenius norm of any input traceless matrix. As discussed earlier, we may therefore take the input state to be $\sum_{i=3}^{3} A_i \otimes \sigma_i$ for some matrices $A_i$ with $\text{Tr}[A_0] = 0$, where $\sigma_i$ are the Pauli matrices on the indicator qubit register.

Both the witness and ancilla verifiers are controlled depolarizers, and we can analyze each of them in the same way using projection operators that act on some subspace of the system; specifically, we will use $Q = \sum_{\phi_{\text{passes}}} |\phi\rangle \langle \phi|$ that projects onto the states that pass the verifier and $P = \sum_{\phi_{\text{fails}}} |\phi\rangle \langle \phi|$ that projects onto the states that fail it. For the ancilla verifier, these are $Q_a = |00\ldots00\rangle \langle 00\ldots00|_{\text{anc}}$ (more properly written as $Q_a = 1_{\text{wit}} \otimes |00\ldots00\rangle \langle 00\ldots00|_{\text{anc}} \otimes 1_{\text{ind}}$) and $P_a = \mathbb{I} - Q_a = \sum_{x \neq 00\ldots00} |x\rangle \langle x|_{\text{anc}}$. For the witness verifier, $Q_w = V^\dagger |0\rangle \langle 0| (1_{\log V} + |0\rangle \langle 0|)$ (so that $P_w + Q_w = \mathbb{I}$). Here the subscript $\text{top}$ is used to indicate the top qubit register output from $V$.

Applying Eq. (19) and linearity, the effect of a verifier unit on the input state $\sum_{i=0}^{3} A_i \otimes \sigma_i$ is therefore

$$F \left( \sum_{i=0}^{3} A_i \otimes \sigma_i \right) = \sum_{i=0}^{3} \left[ PA_i P \otimes \frac{\text{Tr}[\sigma_i]}{2} + QA_i Q \otimes \sigma_i \right] = PA_i P \otimes \mathbb{I} + \sum_{i=0}^{3} QA_i Q \otimes \sigma_i.$$ By linearity, it is easy to see that the effect of two such verifier units—the ancilla verifier with projectors $\{P_a, Q_a\}$ and witness verifier with projectors $\{P_w, Q_w\}$—is

$$F_w \circ F_a \left( \sum_{i=0}^{3} A_i \otimes \sigma_i \right) = \left( P_w P_a P_a P_a + Q_w Q_a Q_a Q_a + P_w Q_a Q_a P_a \right) \otimes \mathbb{I} + \sum_{i=0}^{3} Q_a A_i Q_a Q_w \otimes \sigma_i = \sum_{p} P A_p P^\dagger \otimes \mathbb{I} + \sum_{i=1}^{3} Q A_i Q^\dagger \otimes \sigma_i,$$ where the first sum is over $P \in \{P_w P_a, P_a Q_a, Q_a P_a, P_a Q_a Q_a\}$ and where $Q$ is the single product $Q = Q_w Q_a$ and $Q^\dagger = Q_a Q_w$. Notice that the $i = 0$ term (involving $\sigma_0 = I$) in the second sum has been transferred to the first sum, thereby allowing the first sum to include all possible projection combinations.

We can rewrite this as

$$F_w \circ F_a \left( \sum_{i=0}^{3} A_i \otimes \sigma_i \right) = C(A_0) \otimes 1 + \sum_{i=1}^{3} Q A_i Q^\dagger \otimes \sigma_i,$$

where

$$C(A_0) = \sum_{p} P A_p P^\dagger = \sum_{R_w = P_w, Q_w} R_w \left( \sum_{R_a = P_a, Q_a} R_a A_0 R_a \right) R_w = (G_w \circ G_a)(A_0)$$ is the composition of the pinching operators $G_j(B) = P_j B P_j + Q_j B Q_j$ applied to $A_0$. 

042317-6
Since $C$ is the composition of pinching operators, Eqs. (12) and (13), along with Eq. (11), tell us
\[ \text{Tr}[C(A_0)] = \text{Tr}[A_0] = 0 \] (21)
and
\[ \| C(A_0) \|_F \leq \| A_0 \|_F \leq \frac{1}{\sqrt{2}} \left\| \sum_i A_i \otimes \sigma_i \right\|_F. \] (22)

We are now ready to apply the final controlled expander, which by Eq. (18), with $P = |1\rangle\langle 1|$ and $Q = |0\rangle\langle 0|$, has the effect
\[ \Lambda \mathcal{E}(B \otimes b) = \mathcal{E}(B) \otimes |1\rangle\langle 1| b \langle 1 | + B \otimes |0\rangle\langle 0| b |0\rangle. \]

Applying this to the state Eq. (20) we conclude that the effect of the map in Fig. 3 on the initial traceless matrix $\sum_{i=0} A_i \otimes \sigma_i$ is
\[ \Phi \left( \sum_{i=0} A_i \otimes \sigma_i \right) = C(A_0) \otimes |0\rangle\langle 0| + \mathcal{E} \left( C(A_0) \right) \otimes |1\rangle\langle 1| + Q A_3 Q_1 \otimes |0\rangle\langle 0| - \mathcal{E}(Q A_3 Q_1) \otimes |1\rangle\langle 1|. \]

To show that $\Phi$ is a good quantum expander, we must show that it sufficiently decreases the Frobenius norm of its traceless input. Since $\mathcal{E}$ is a $\kappa_c$-contractive expander and $C(A_0)$ is traceless [see Eq. (21)] we are guaranteed that
\[ \| \mathcal{E}(C(A_0)) \|_F \leq \kappa_c \| C(A_0) \|_F. \] (23)

Applying the triangle inequality and Eqs. (14), (22), and (23), we therefore have
\[ \left\| \Phi \left( \sum_{i=0} A_i \otimes \sigma_i \right) \right\|_F \leq \| C(A_0) \|_F + \mathcal{E}(C(A_0)) \|_F + \mathcal{E}(Q A_3 Q_1) \|_F \leq 1 + \kappa_c \| C(A_0) \|_F + 2 \| Q A_3 Q_1 \|_F \leq \frac{1}{\sqrt{2}} \left\| \sum_{i=0} A_i \otimes \sigma_i \right\|_F + 2 \| Q A_3 Q_1 \|_F. \] (24)

Note that we cannot make a claim similar to Eq. (23) for $\mathcal{E}(Q A_3 Q_1)$ because $Q A_3 Q_1$ need not be traceless.

In QMA(1, 0) we are guaranteed that provided the ancillae are initialized to be all 0’s, no witness can pass the verifier (for a NO instance). Mathematically, this guarantee is equivalent to saying that $Q \equiv 0$. Consequently, the $Q A_3 Q_1$ vanishes and we are done. In QMA(a, b), however, we must upper bound $\| Q A_3 Q_1 \|_F$, which we now proceed to do.

Because $x \notin L \in \text{QMA}(a, b)$ we are assured that for any purported witness $|\psi\rangle$,
\[ \| Q_w |\psi\rangle \langle 0| \| \leq \sqrt{b}. \] (25)

Because $Q_w$ projects onto the $|0\rangle \langle 0|$ ancilla subspace, we may write
\[ Q_w A_3 Q_w = \sum_{|\psi_1\rangle, |\psi_2\rangle} c(\psi_1, \psi_2)|\psi_1\rangle\langle \psi_2| \otimes |0\rangle \langle 0|. \]

where $\{ |\psi_i\rangle \}$ is any orthonormal basis of the witness subspace.

Note that because the witness register consists of $n_w$ qubits, $c(\psi_1, \psi_2)$ can be regarded as a matrix with dimension $N = 2^{n_w} \times 2^{n_w}$. Thus using the triangle inequality and Eqs. (10) and (25),
\[ \| Q A_3 Q_1 \|_F = \left\| \sum_{|\psi_1\rangle, |\psi_2\rangle} c(\psi_1, \psi_2) Q_w |\psi_1\rangle \langle \psi_2| \langle 0| Q_w \right\|_F \leq \sum_{|\psi_1\rangle, |\psi_2\rangle} |c(\psi_1, \psi_2)| \| Q_w |\psi_1\rangle \langle 0| Q_w \|_F = \sum_{|\psi_1\rangle, |\psi_2\rangle} |c(\psi_1, \psi_2)| \| Q_w |\psi_1\rangle \langle 0| Q_w |\psi_2\rangle \|_F \leq \sum_{|\psi_1\rangle, |\psi_2\rangle} |c(\psi_1, \psi_2)| b. \]

The matrix $c$ has $2^{n_w} \times 2^{n_w}$ elements, so its 1-norm and 2-norm are related by
\[ \sum_{|\psi_1\rangle, |\psi_2\rangle} |c(\psi_1, \psi_2)| \leq 2^{n_w} \sqrt{\sum_{|\psi_1\rangle, |\psi_2\rangle} |c(\psi_1, \psi_2)|^2} = 2^{n_w} \| Q_w A_3 Q_1 \|_F. \]

But by Eqs. (11) and (15),
\[ \| Q_w A_3 Q_1 \|_F \leq \| A_3 \|_F \leq \frac{1}{\sqrt{2}} \sum_{i=0}^3 A_i \otimes \sigma_i \|_F; \]

thus we conclude,
\[ \| Q A_3 Q_1 \|_F \leq \frac{2^{n_w}}{\sqrt{2}} \sum_{i=0}^3 A_i \otimes \sigma_i \|_F. \] (26)

Although $2^{n_w}$ is exponential in $n_w$, recall that $b$ was chosen so that $2^{n_w+1} b \leq 0.1$. We conclude from Eqs. (24) and (26) that $\Phi$ is a $\beta$-contractive expander,
\[ \left\| \Phi \left( \sum_{i=0} A_i \otimes \sigma_i \right) \right\|_F \leq \beta \left\| \sum_{i=0} A_i \otimes \sigma_i \right\|_F, \] (27)
with
\[ \beta = \frac{1 + \kappa_c + 2^{n_w+1} b}{\sqrt{2}} < 0.85. \] (28)

C. Analysis of YES case

Now consider the case in which $x \in L$. Since $L \in \text{QMA}(a, b)$ there exists a valid witness $|\psi\rangle$ such that
\[ \| Q_w |\psi\rangle \langle 0| \|_F \geq a. \] (29)

From this witness we construct the density matrix $\Psi = |\psi\rangle \langle \psi| \otimes |0\rangle \langle 0| \otimes |0\rangle \langle 0|$. Because $\Psi$ passes the ancilla verifier unchanged and the witness verifier with very little change, $\Psi$ is almost a fixed point of our expander $\Phi$ [and indeed, for QMA(1, 0) it is a fixed point]; intuitively, therefore, $\Phi$ is a poor expander. The matrix $I = \sum_{i=0}^3 A_i \otimes \sigma_i$ is certainly a fixed point (for any unitary map); therefore the traceless matrix
\[ A = \Psi - I = |\psi\rangle \langle \psi| \otimes |0\rangle \langle 0| \otimes |0\rangle \langle 0| - \frac{1}{2^{n_w+n_w+1}} 1 \]
is also expected to change very little under $\Phi$. By showing this to be the case, we will show that $\Phi$ is not an $\alpha$-contractive expander for an $\alpha$ that is polynomially separated from the $\beta$ found in the NO case.
Using an analysis similar to the previous case, it is easy to see that the effect of our circuit on $\Psi$ is

$$
\Psi = |\psi\rangle\langle\psi| \otimes |0\rangle\langle0| + \frac{1}{2} P_w(|\psi\rangle\langle\psi| \otimes |0\rangle\langle0|) + \frac{1}{2} P_w(|\psi\rangle\langle\psi| \otimes |0\rangle\langle0|) Q_w \otimes \{0\} |0\rangle
$$

controlled $\mathcal{E}$

$$
\frac{1}{2} \mathcal{E}[P_w(|\psi\rangle\langle\psi| \otimes |0\rangle\langle0|) P_w] \otimes |1\rangle\langle1| + \frac{1}{2} P_w(|\psi\rangle\langle\psi| \otimes |0\rangle\langle0|) P_w \otimes |0\rangle + \frac{1}{2} P_w(|\psi\rangle\langle\psi| \otimes |0\rangle\langle0|) Q_w \otimes \{0\} |0\rangle.
$$

Note that the three final terms are mutually orthogonal because $|0\rangle\langle0| \otimes \{1\} = 0$ and $P_w Q_w = 0$. Consequently, we have

$$
\|\Phi(\Psi)\|^2_F = \frac{1}{2} \|\mathcal{E}[P_w(|\psi\rangle\langle\psi| \otimes |0\rangle\langle0|) P_w] \|_F^2 + \frac{1}{2} \|P_w(|\psi\rangle\langle\psi| \otimes |0\rangle\langle0|) P_w \|_F^2 + \|Q_w(|\psi\rangle\langle\psi| \otimes |0\rangle\langle0|) Q_w \|_F^2 \\
\geq \|Q_w(|\psi\rangle\langle\psi| \otimes |0\rangle\langle0|) Q_w \|_F^2 = \|Q_w(|\psi\rangle\langle\psi|) Q_w \|_F^2 \\
\geq a^2 - \frac{1}{2n_w + \alpha^2} \|A\|^2_F.
$$

(30)

where we have used Eqs. (10) and (29).

Now, because $\Psi$ is a pure state density matrix, $\|A\|^2_F = \|\Psi - I\|^2_F = \text{Tr}[\Psi^2] + \text{Tr}[\tilde{F}^2] - 2\text{Tr}[\Psi \tilde{F}]$, using Eq. (9), so that

$$
\|A\|^2_F = 1 - \frac{1}{2n_w + \alpha^2}.
$$

(31)

Thus, using that $\Phi$ is linear and trace-preserving, that $\Phi(\tilde{I}) = \tilde{I}$, and Eqs. (30) and (31), we have

$$
\|\Phi(A)\|^2_F = \|\Phi(\Psi) - \Phi(\tilde{I})\|^2_F
\geq \text{Tr}[\Phi(\Psi)^2] - \text{Tr}[\Phi(\Psi) \tilde{F}]
\geq \|\Phi(\Psi)\|^2_F + \text{Tr}[\tilde{F}^2] - 2\text{Tr}[\Psi \tilde{F}]
\geq a^2 - \frac{1}{2n_w + \alpha^2} \|A\|^2_F.
$$

where in the last inequality we have used from Eq. (31) that for $n_w \geq 1$ we have $\frac{1}{8} < \|A\|^2_F < 1$. Thus we conclude that $\Phi$ is not an $\alpha$-contractive expander,

$$
\|\Phi(A)\|^2_F > \alpha \|A\|^2_F.
$$

(32)

with

$$
\alpha = \sqrt{1 - \frac{1}{2n_w + \alpha^2}} > 0.98.
$$

(33)

Note that $\alpha$ and $\beta$ are constants, and therefore certainly polynomially separated.

VI. CONCLUSION

We have presented a computational problem, quantum nonexpander, and proved that it is QMA-complete. This gives some insight into the computational complexity of estimating mixing rates of quantum channels and open quantum systems.

In contrast to the plethora of natural NP-complete problems, very few problems have been shown to be QMA-complete. We hope that it may be possible to find new QMA-complete problems, using reductions from the quantum nonexpander problem.

ACKNOWLEDGMENTS

This work was supported in part by the US Department of Energy under cooperative research agreement Contract DE-FG02-05ER41360, as well as by the National Science Foundation Science and Technology Center for Science of Information under Grant No. CCF-0939370. P.W. gratefully acknowledges the support from NSF CAREER Award No. CCF-0746600. Contributions to this work by NIST, an agency of the US government, are not subject to US copyright.

APPENDIX

1. Master equation for a quantum system coupled to a bath

In this section we derive the master equation (5), given the system-bath Hamiltonian specified in (2)–(4). We follow the arguments of Secs. 3.3 and 3.4 in [21].

First, define new operators $A_{\sigma} \alpha$ and $B_{\sigma} \alpha$ (for $\alpha = 1, \ldots, D$ and $\sigma = 0, 1$):

$$
A_{\sigma} \alpha = \frac{1}{\sqrt{2}} (-i)^{\sigma} [U_{\alpha}(-1)^{\sigma} U_{\alpha}^{\dagger}],
$$

$$
B_{\sigma} \alpha = \frac{1}{\sqrt{2}} i^{\sigma} \left[ f_{\alpha}(-1)^{\sigma} f_{\alpha}^{\dagger} \right].
$$

Then we can write the interaction Hamiltonian in the form

$$
H_I = \sum_{\alpha, \sigma} A_{\sigma} \alpha \otimes B_{\sigma} \alpha.
$$

This form is convenient because $A_{\sigma} \alpha$ and $B_{\sigma} \alpha$ are Hermitian. In the weak-coupling limit ($\epsilon \rightarrow 0$), one gets the following master equation (Eq. 3.140 in [21], simplified using the fact that $H_S = 0$):

$$
\frac{d}{dt} \rho_{\Sigma}(t) = -i[H_{LS}, \rho_{\Sigma}(t)] + \mathcal{D}(\rho_{\Sigma}(t)),
$$

(A1)

where $H_{LS}$ is the “Lamb shift” Hamiltonian and $\mathcal{D}$ is the dissipator,

$$
H_{LS} = \sum_{\alpha, \sigma} S_{\alpha, \sigma, \tau} A_{\sigma, \tau} A_{\sigma, \tau}^{\dagger}.
$$

and the coefficients $S_{\alpha, \sigma, \tau}$ and $\gamma_{\alpha, \sigma, \tau}$ are given by

$$
S_{\alpha, \sigma, \tau} = \frac{1}{2} \left( \Gamma_{\alpha, \tau} + \Gamma_{\alpha, \tau}^{*} \right), \quad \gamma_{\alpha, \sigma, \tau} = \Gamma_{\alpha, \tau} + \Gamma_{\alpha, \tau}^{*},
$$

where $\Gamma_{\alpha, \tau}$ are the one-sided Fourier transforms (evaluated at frequency $0$) of the bath correlation functions,

$$
\Gamma_{\alpha, \tau} = \int_{0}^{\infty} ds \langle B_{\alpha, \tau}(s) B_{\tau}(0) \rangle, \quad B_{\alpha, \tau}(t) = e^{iH_S t} B_{\alpha, \tau} e^{-iH_S t}.
$$

42317-8
We can evaluate the bath correlation functions, using the fact that the bath is in a thermal state at temperature $T$. After some algebra, we get

$$
\langle B_{\sigma}(s)B_{\beta}(0) \rangle = \frac{1}{2} i^\sigma i^\tau \frac{1}{\Omega} \sum_{kk'} (e^{-is\omega_k} (b_{ak}b_{pk'}) + (-1)^\sigma e^{is\omega_k} (b_{ak}b_{pk'}) + (-1)^\sigma e^{is\omega_k} (b_{ak}b_{pk'}) + (-1)^\tau e^{is\omega_k} (b_{ak}b_{pk'})
$$

where $N(\omega_k) = \frac{1}{\exp(\omega_k/T) - 1}$. We take a continuum limit, replacing the sum $\frac{1}{2\Omega} \sum_k$ by an integral $\int_\Omega dk$; this amounts to using a bath with infinitely many modes, and is necessary to obtain irreversible behavior of the system.

We then substitute the above expression into the definition of $\Gamma_{a\bar{a}\sigma\bar{\sigma}}$:

$$
\Gamma_{a\bar{a}\sigma\bar{\sigma}} = \frac{1}{2} i^\sigma i^\tau \delta_{a\bar{a}} \int_0^\infty ds \int_\Omega dk (-1)^\sigma e^{is\omega_k} N(\omega_k) + e^{-is\omega_k} (-1)^\tau [1 + N(\omega_k)]).
$$

We can simplify the above formula by exchanging the integrals and using the identity $\int_0^\infty ds e^{-i\lambda s} = \pi \delta(x) - iP(\frac{1}{x})$, where $\delta(x)$ is the Dirac distribution and $P(\frac{1}{x})$ is the Cauchy principal value (equation 3.202 in [21]). We then get

$$
\Gamma_{a\bar{a}\sigma\bar{\sigma}} = \frac{1}{2} i^\sigma i^\tau \delta_{a\bar{a}} \left( (-1)^\sigma \pi N(0) + (-1)^\tau iP \int_\Omega \frac{N(\omega_k)}{\omega_k} dk + (-1)^\tau \pi [1 + N(0)] - (-1)^\tau iP \int_\Omega \frac{1 + N(\omega_k)}{\omega_k} dk \right).
$$

In particular, $\Gamma_{a\bar{a}\sigma\bar{\sigma}}$ can be written in the form

$$
\Gamma_{a\bar{a}\sigma\bar{\sigma}} = \frac{1}{2} i^\sigma i^\tau \delta_{a\bar{a}} ((-1)^\sigma Q_0 + (-1)^\tau Q_1),
$$

where the coefficients $Q_0$ and $Q_1$ are complex numbers with positive real part.

We can now calculate the “Lamb shift” Hamiltonian $H_{L.S}$ as follows:

$$
S_{a\bar{a}\sigma\bar{\sigma}} = \frac{1}{2i} \frac{1}{2} i^\sigma i^\tau \delta_{a\bar{a}} ((-1)^\sigma (Q_0 - Q_0^*) + (-1)^\tau (Q_1 - Q_1^*)),
$$

$$
H_{L.S} = \frac{Q_0 - Q_0^*}{4i} \sum_a \left( \sum_\sigma i^\sigma (-1)^\sigma A_{a\sigma}^\dagger \right) \left( \sum_\tau i^\tau A_{a\tau} \right) + \frac{Q_1 - Q_1^*}{4i} \sum_a \left( \sum_\sigma i^\sigma A_{a\sigma}^\dagger \right) \left( \sum_\tau i^\tau (-1)^\tau A_{a\tau} \right)
$$

$$
= \frac{Q_0 - Q_0^*}{4i} \sum_a \sqrt{2} U_a U_a^\dagger \frac{Q_0^* - Q_0}{4i} \sum_a \sqrt{2} U_a U_a^\dagger = \frac{Q_0 - Q_0^*}{2i} D I + \frac{Q_1 - Q_1^*}{2i} D I.
$$

So $H_{L.S}$ is a multiple of the identity, and it contributes nothing when we substitute it into the master equation (A1).

Finally we can calculate the dissipator $D$. First, 

$$
\gamma_{a\bar{a}\sigma\bar{\sigma}} = \frac{1}{2} i^\sigma i^\tau \delta_{a\bar{a}} ((-1)^\sigma (Q_0 + Q_0^*) + (-1)^\tau (Q_1 + Q_1^*)).
$$

We substitute this into the definition of $D$, and simplify it in the same way as we did for $H_{L.S}$. This yields

$$
D(\rho_S) = (Q_0 + Q_0^*) \sum_a (U_a \rho_S U_a^\dagger - \rho_S) + (Q_1 + Q_1^*) \sum_a (U_a \rho_S U_a^\dagger - \rho_S).
$$

Note that $Q_0 + Q_0^*$ and $Q_1 + Q_1^*$ are positive real numbers. We substitute this into the master equation (A1). This completes our proof of (5).

2. Controlled expanders

In this section, we outline how we obtain the requisite controlled expander $\Lambda E$ needed for Sec. V. We use the results of Ben-Aroya, Schwartz, and Ta-Shma [24], whose Theorems 4.3 and 4.6 give the following result.

Theorem A1. There exists an integer $D_0$ such that for every $D > D_0$ and for every integer $t > 0$, there exists an explicit $\lambda_t$-contractive expander of degree $D^2$ on a space of dimension $D^h$ where $\lambda_t \leq \lambda + c \lambda^2$ with $c$ a constant and $\lambda = \frac{4D^r}{D}$. We will additionally use the following result, which follows directly from the definition. Here we use the notation that $F^r$ denotes the $r$-fold composition of $F$.

Proposition A1. If $F$ is a $\lambda$-contractive expander of degree $D$ on a space of size $N$, then for any positive integer $r$, $F^r$ is a $\lambda^r$-contractive expander of degree $D^r$ on a space of size $N$.

In Sec. V we require an $\kappa E$-contractive expander $E$ with $\kappa E \leq 0.1$ on a space of size $N = 2^{2n + \gamma_n}$, where $N$ is actually allowed to exceed $2^{2n + \gamma_n}$ since we can always have...
extra input ancillae that do nothing but are acted upon by the final controlled expander $\Lambda E$.

Fix $D$ to be any power of 2 larger than $D_0$. Then $\lambda = \frac{4\sqrt{D-1}}{D} < 1$ is fixed. Let $r$ be such that $(\lambda + c\lambda^2)^r \leq 0.1$. Let $t = \left\lceil \frac{n_w+n_a}{8 \log_2 D} \right\rceil = \frac{n_w+n_a+n_{\text{extra}}}{8 \log_2 D}$ for some $n_{\text{extra}} < 8 \log_2 D$. Using the above theorem we are guaranteed the existence of a $\lambda^r$-contractive expander of degree $D^{2r}$ on a space of size $D^{8t} = 2^{n_w+n_a+n_{\text{extra}}}$, where $D$ and $r$ are constants and $\lambda^r \leq 0.1$.